مبانی جبر مجرد

(همراه با آزمایشگاه‌های کامپیوتر)

ویـــــرایـــــش دوم

تالیف

بیژن طائری

دانشکده علوم ریاضی

دانشگاه صنعتی اصفهان

در راستای حمایت از دانشجویان و تسهیل دسترسی به منابع آموزشی، با مساعدت ناشر محترم تصمیم گرفتم ویرایش دوم کتاب را به صورت رایگان در وبسایت خود قرار دهم. هدف من از این اقدام فراهم کردن فرصتی برای یادگیری و رشد علمی دانشجویان عزیز است.
لطفا نظرات و پیشنهادهای خود را برای من ارسال کنید.

فهرست مطالب

فهرست مطالب ت

مقدمه ث

فصل ۱ مجموعه، رابطه ۱
۱.۱ مجموعه . . . ۱
۲.۱ رابطه . . . ۵
۳.۱ مجموعه‌های جزئاً مرتب . . . ۹
۴.۱ استقرا . . . ۱۱
۵.۱ توابع . . . ۱۴
۶.۱ عمل دوتایی . . . ۲۳
۷.۱ جایگشت‌ها . . . ۲۵

فصل ۲ اعداد صحیح ۳۵
۱.۲ تجزیه در اعداد صحیح . . . ۳۵
۲.۲ اعداد صحیح به پیمانه‌ی n، $\mathbb{Z}_n$ . . . ۴۲

فصل ۳ گروه‌ها ۴۹
۱.۳ خواص مقدماتی گروه‌ها . . . ۴۹
۲.۳ مرتبه، گروه‌های دوری . . . ۵۸
۳.۳ همریختی . . . ۶۲
۴.۳ زیرگروه . . . ۶۶
۵.۳ تولید گروه‌ها، گروه‌های متناهیاً تولید شده . . . ۷۰
۶.۳ چند زیرگروه مهم . . . ۷۴
۷.۳ زیرگروه‌های مشخصه و نرمال . . . ۷۷
۸.۳ هم‌مجموعه‌ها، قضیه‌ی لاگرانژ . . . ۸۳
۹.۳ گروه‌های خارج‌قسمتی . . . ۹۱
۱۰.۳ قضایای یکریختی . . . ۹۵

فصل ۴ حاصل‌ضرب گروه‌ها ۹۹
۱.۴ حاصل‌ضرب مستقیم گروه‌ها . . . ۹۹
۲.۴ حاصل‌ضرب نیم‌مستقیم . . . ۱۰۵

فصل ۵ عمل گروه و قضایای سیلو ۱۰۹
۱.۵ عمل گروه روی مجموعه . . . ۱۰۹
۲.۵ عمل چپ منظم گروه روی خودش . . . ۱۱۲
۳.۵ عمل گروه به صورت مزدوجی . . . ۱۱۶
۴.۵ قضایای سیلو . . . ۱۱۹

فصل ۶ گروه‌های آبلی متناهیاً تولید شده ۱۲۵
۱.۶ گروه‌های آبلی متناهی . . . ۱۲۵
۲.۶ ساختار گروه‌های آبلی متناهیاً تولید شده . . . ۱۳۰

فصل ۷ سری زیر گروه‌ها ۱۳۷
۱.۷ گروه‌های حل‌پذیر . . . ۱۳۷
۲.۷ گروه‌های پوچ‌توان . . . ۱۴۱
۳.۷ زیرگروه فراتینی . . . ۱۴۷
۴.۷ سری ترکیبی . . . ۱۵۰
۵.۷ گروه‌های چند دوری و حل‌پذیر . . . ۱۵۶

فصل ۸ گروه‌های آزاد ۱۶۱
۱.۸ خواص اساسی گروه‌های آزاد . . . ۱۶۱

فصل ۹ مباحثی در نظریه‌ی گروه‌ها ۱۶۷
۱.۹ گروه‌هایی که اجتماع زیرگروه‌های سره‌شان هستند . . . ۱۶۷
۲.۹ تعداد مرکز سازها در یک گروه . . . ۱۷۸
۳.۹ مساله‌ای احتمالاتی در گروه‌ها . . . ۱۸۲
۴.۹ مساله‌ی n- جایگشت‌پذیری . . . ۱۸۸

فصل ۱۰ حلقه‌ها ۱۹۷
۱.۱۰ خواص مقدماتی حلقه‌ها . . . ۱۹۷
۲.۱۰ زیرحلقه . . . ۲۰۵
۳.۱۰ همریختی . . . ۲۰۸
۴.۱۰ ایدآل، حلقه‌ی خارج‌قسمتی . . . ۲۱۲
۵.۱۰ میدان کسرهای یک دامنه‌ی صحیح . . . ۲۱۹
۶.۱۰ تولید ایدآل‌ها . . . ۲۲۱
۷.۱۰ ایدآل‌های ماکسیمال و اول . . . ۲۲۴

فصل ۱۱ حلقه‌ی چندجمله‌ای‌ها ۲۳۱
۱.۱۱ خواص مقدماتی چندجمله‌ای‌ها . . . ۲۳۱
۲.۱۱ تجزیه‌ی چندجمله‌ای‌ها روی یک میدان . . . ۲۳۸
۳.۱۱ یکتایی تجزیه . . . ۲۴۵
۴.۱۱ حلقه‌های چندجمله‌ای‌های خارج‌قسمتی روی یک میدان . . . ۲۴۹

فصل ۱۲ تجزیه در دامنه‌های صحیح ۲۵۵
۱.۱۲ تجزیه و تحویل‌ناپذیرها . . . ۲۵۵
۲.۱۲ عناصر اول و تحویل‌ناپذیر . . . ۲۵۷
۳.۱۲ دامنه‌های تجزیه‌ی یکتا . . . ۲۶۰
۴.۱۲ تجزیه‌ی چندجمله‌ای‌ها روی یک UFD . . . ۲۶۳
۵.۱۲ دامنه‌های اقلیدسی . . . ۲۶۶
۶.۱۲ برخی حلقه‌های اعداد صحیح مرتبه‌ی دوم . . . ۲۶۸

فصل ۱۳ مدول‌ها و فضاهای برداری ۲۷۳
۱.۱۳ مدول‌ها . . . ۲۷۳
۲.۱۳ زیرمدول . . . ۲۷۴
۳.۱۳ قضایای یکریختی . . . ۲۷۵
۴.۱۳ مدول‌های آزاد متناهیاً تولید شده . . . ۲۷۷

فصل ۱۴ میدان‌ها ۲۸۳
۱.۱۴ توسیع‌های جبری . . . ۲۸۳
۲.۱۴ توسیع‌های تجزیه . . . ۲۹۱
۳.۱۴ میدان‌های متناهی . . . ۲۹۶
۴.۱۴ توسیع‌های جداپذیر . . . ۳۱۰
۵.۱۴ گروه گالوای توسیع . . . ۳۱۲
۶.۱۴ چندجمله‌ای‌های دایره‌بر و قضیه‌ی ودربُرن . . . ۳۱۹
۷.۱۴ توسیع‌های نرمال . . . ۳۲۵
۸.۱۴ قضیه‌ی اساسی نظریه‌ی گالوا . . . ۳۲۸
۹.۱۴ حل‌پذیری چندجمله‌ای‌ها با رادیکال . . . ۳۳۶
۱۰.۱۴ساخت‌پذیری هندسی . . . ۳۴۱

فصل ۱۵ کاربردی از جبر (کدگذاری) ۳۴۹
۱.۱۵ کدهای خطی . . . ۳۴۹
۲.۱۵ کدگشایی کدهای خطی . . . ۳۵۶
۳.۱۵ چند برنامه‌ی مفید به چند GAP . . . ۳۶۸
۴.۱۵ کدهای دوری . . . ۳۷۱
۵.۱۵ کدهای BCH . . . ۳۸۹
۶.۱۵ کدهای مانده‌ای درجه‌ی دوم . . . ۳۹۶

فصل ۱۶ آزمایشگاه‌های GAP ۴۰۵
۱.۱۶ آشنایی با GAP، آزمایشگاه اول . . . ۴۰۵
۲.۱۶ لیست‌ها در GAP، آزمایشگاه دوم . . . ۴۰۹
۳.۱۶ توابع در GAP، آزمایشگاه سوم . . . ۴۱۱
۴.۱۶ مجموعه، رابطه، و تابع در GAP، آزمایشگاه چهارم . . . ۴۱۳
۵.۱۶ اعمال بیشتر روی مجموعه‌ها و لیست‌ها در GAP، آزمایشگاه پنجم . . . ۴۱۷
۶.۱۶ جایگشت‌ها در GAP، آزمایشگاه ششم . . . ۴۱۹
۷.۱۶ اعداد صحیح در GAP، آزمایشگاه هفتم . . . ۴۲۴
۸.۱۶ مقدمه‌ای بر گروه‌ها در GAP، آزمایشگاه هشتم . . . ۴۲۹

۹.۱۶ تعدادی گروه دیگر در GAP، آزمایشگاه نهم ۴۳۳
۱۰.۱۶ همریختی در GAP، آزمایشگاه دهم ۴۳۷
۱۱.۱۶ زیر گروه‌ها در GAP، آزمایشگاه یازدهم ۴۴۱
۱۲.۱۶ هم‌مجموعه‌ها و گروه‌های خارج قسمتی در GAP، آزمایشگاه دوازدهم ۴۴۴
۱۳.۱۶ حاصل‌ضرب مستقیم و نیم‌مستقیم در GAP، آزمایشگاه سیزدهم ۴۴۶
۱۴.۱۶ عمل گروه در GAP، آزمایشگاه چهاردهم ۴۵۰
۱۵.۱۶ زیرگروه‌های سیلو در GAP، آزمایشگاه پانزدهم ۴۵۴
۱۶.۱۶ سری زیر گروه‌ها در GAP، آزمایشگاه شانزدهم ۴۵۵
۱۷.۱۶ حلقه‌ها در GAP، آزمایشگاه هفدهم ۴۵۹
۱۸.۱۶ حلقه‌ی چندجمله‌ای‌ها در GAP، آزمایشگاه هجدهم ۴۶۵
۱۹.۱۶ مدول‌ها و فضاهای برداری در GAP، آزمایشگاه نوزدهم ۴۶۹
۲۰.۱۶ میدان‌ها در GAP، آزمایشگاه بیستم ۴۷۴

فهرست مراجع ۴۸۵

راهنمایی برای حل برخی از تمرین‌ها ۴۸۷

واژه‌نامه فارسی-انگلیسی ۵۴۵

فهرست اسامی خاص ۵۵۳

فهرست نمادها ۵۵۷

نمایه ۵۶۲

مقدمه

با وجود کتب فارسی (نه چندان زیاد) و منابع فراوان به زبان‌های دیگر در جبر مجرد، اندیشه‌ی من از تدوین کتابی دیگر تکرار مکررات کلیشه‌ای نیست. بلکه که سعی من در بیان سلیقه‌ها و علاقه‌های شخصی در نحوه‌ی ارائه‌ی دروس جبر است. سعی کرده‌ام که علاوه بر پوشش مطالبی که دانشجوی جبر مجرد باید بداند، او را به سمت تفکر بیشتر و بسط مطالب سوق دهم. با آوردن تعدادی آزمایشگاه کامپیوتر به زبان برنامه نویسی GAP سعی کرده‌ام تا دانشجو با محاسبه در جبر مجرد نیز آشنا شود، تا بتوانند مطالب را برای خود ملوس‌تر کند. نخستین برخورد یک دانشجو با جبر مجرد ممکن است زیاد خوش‌آیند نباشد. زیرا بر خلاف برخی دروس دیگر دانشگاهی که دانشجو از دبیرستان با آن ها آشنا شده، هیچ گونه زمینه‌ی ذهنی، به‌جز در موارد بسیار جزئی در درس مبانی ریاضیات، در این مبحث ندارد . مثالی می‌آوریم. دانشجوی درس آنالیز از قبل آشنایی زیادی با این درس دارد و در دبیرستان با مفاهیم مقدماتی حسابان و انجام محاسبه در آن آشنا شده است. در ابتدای ورود به دانشگاه و در دروس ریاضی عمومی با مفاهیم آنالیز بیشتر مانوس می‌شود. در نهایت با اخذ درس آنالیز با زمینه‌ی ذهنی نسبتاً خوب آماده‌ی پذیرش درس است. اما وضعیت در جبر مجرد کاملاً فرق می‌کند. دانشجو هیچ گونه زمینه آی از جبر مجرد ندارد و گذار او از واقعیت به تجرید مشکل است. اگر انتظار داشته باشیم که یک دانشجو پس از گذراندن درس جبر مجرد مفاهیم مقدماتی آن را بداند و از طرف دیگر با تفکر انتزاعی آشنا شود، نمی‌توان مطالعه را چند بار، یک بار به صورت محاسبه‌ای، یک بار قدری مجردتر، و در نهایت مبحث اصلی را در یک یا دو درس به دانشجو ارائه کرد. بنابراین وظیفه‌ی دانشجو و مدرس در اولین درس جبر قدری دشوار است. دانشجو باید با سخت کوشی و مدرس با حوصله‌ی زیاد یک‌دیگر را یاری دهند. معمولاً به مرور زمان کارها آسان‌تر می‌شود.

در این کتاب در فصل اول ، مجموعه، رابطه و مفاهیم وابسته به آن‌ها از قبیل توابع، رابطه‌های هم‌ارزی، لم زُرن و اصل انتخاب، اعمال دوتایی و جایگشت‌ها؛ در فصل دوم خواص اعداد صحیح، اعداد اول و رابطه‌های هم‌نهشتی آورده شده‌اند. در فصلهای سوم تا هشتم مفاهیم مقدماتی نظریه‌ی گروه‌ها و قضیه‌های اساسی از قبیل قضیه‌ی لاگرانژ، قضیه‌ی یکریختی، قضایای سیلو، ... بررسی شده‌اند. در فصل نهم تعدادی از مباحث تحقیقی نظریه‌ی گروه‌ها که با ابزار مقدماتی ارئه‌ی شده در فصل‌های قبل قابل بررسی‌اند، آورده شده‌اند. در فصل‌های دهم تا دوازدهم مفاهیم مقدماتی نظریه‌ی حلقه‌ها، آورده شده‌اند. در فصل سیزدهم مفاهیم مقدماتی مدول‌ها و فضای برداری، برای درک مطالب فصل چهارده‌ام که به نظریه‌ی میدان اختصاص دارد ، آورده شده‌اند. در فصل چهارده‌ام نظریه‌ی میدان‌ها و نظریه‌ی گالوا و مفاهیم اساسی وابسته به آن ها بررسی شده‌اند. در نهایت در فصل پانزدهم کاربردی از جبر، یعنی نظریه‌ی کد گذاری، ارائه و بررسی شده است.

پیش‌نیاز خاصی برای کتاب فرض نشده است، به جز در برخی از موارد که آشنایی مختصری از جبر خطی که دانشجو از دبیرستان آن‌ها را می‌داند، یا می‌تواند در هنگام مطالعه‌ی این کتاب از کتب موجود جبر خطی برای آشنایی با آن‌ها استفاده کند.

انتهای اثبات قضیه‌ها و حل مثال‌ها را با علامت □ مشخص شده است. در پایان هر بخش تعدادی تمرین آورده شده ، که پاسخ یا راهنمایی برای حل برخی از آن‌ها در پایان کتاب ارائه شده است. به نظر من بهتر است دانشجو قبل از مراجعه به آخر کتاب برای دیدن را راهنمایی یا پاسخ، به قدر کافی روی حل مساله فکر کند. چرا که ممکن است راه حل متاسب‌تری برای حل آن بیابید. به هر حال در تمرین‌های چند فصل اول کتاب راهنمایی بیشتری برای حل مساله‌ها و در بسیاری از موارد حل کامل آورده شده؛ که به تدریج از تعداد آن ها کاسته شده است. برای تمرین‌های موجود در آزمایشگاه‌های GAP پاسخ یا راهنمایی در انتهای کتاب آورده نشده است.

برای درس جبر ۱، بخش ۱۱ از فصل ۱، بخش ۳ از فصل ۲، فصل ۳ به طور کامل، بخش ۱ از فصل ۴، بخشهای ۱ تا ۵ از فصل ۱۰؛ برای درس جبر ۲، فصل ۵ به طور کامل، بخشهای ۱ تا ۳ از فصل ۷، از فصل ۱۰ بخش ۶ تا آخر، فصل ۱۱ و ۱۲ به طور کامل؛ و برای درس جبر ۳، فصل ۱۳ و ۱۴ به طور کامل؛ را پیشنهاد می‌کنم. فصل ۱۵ را می‌توان در یک درس به نام نظریه‌ی مقدماتی کدگذاری ارائه کرد. در صورتی که دانشجو قبلاً درس جبر ۳ را گذرانده باشد دو واحد، و در غیر این صورت، همراه با بررسی مختصر فصل ۱۱ و بخش‌های ۱، ۲، ۳، ۶ از

فصل ۱۴، سه واحد برای ارائه آن مناسب به نظر می‌رسد. دانشجویان کارشناسی ارشد در دروس جبر پیشرفته و نظریه‌ی گروه‌ها می‌تواند بخش ۲ از فصل ۴، فصل ۶، بخشهای ۳ تا آخر از فصل ۷، و فصل ۸ و ۹ را به صورت کمک درسی استفاده نماید.

برخی از همکاران و دانشجویان تعدادی از اشکالات کتاب را قبل از چاپ به من گوشزد کرده‌اند، از جمله آقای دکتر علی ایرانمنش ویراستار علمی کتاب، آقای دکتر حسین خبازیان (در فصل ۱۴)، خانم دکتر عاطفه قربانی (در مباحث مربوط به جبر ۱)، دانشجوی دکتری ریاضی خانم شادی عسکری (در مباحث مربوط به جبر ۱)، دانشجویان کارشناسی ریاضی آقایان رضا سبحانی (بازخوانی متن اولیه و نهایی)، محمد رضا گورابی، و خانم‌ها سیما سلطانی، لیلی شهریاری، که از آن‌ها و سایر دانشجویانی که در طول تدریس چندساله‌ی کتاب سبب تکمیل برخی ایده‌ها شدند، تشکر می‌کنم. هم‌چنین از خانم شهلا دولتشاهی کارشناس ارشد ادبیات فارسی، به خاطر تذکر برخی نکات دستور زبان فارسی، تشکر می‌کنم. کار آنان باعث شد کتابی بهتر از آن چه که ممکن بود نوشته شود، تالیف کنم.

سعی بسیار کرده‌ام تا اشکالی در کتاب نباشد. اما قطعاً اشکالاتی در کتاب وجود دارد که از دید من پنهان مانده است، تذکر آن‌ها و هم‌چنین ارائه‌ی نقطه نظرات از جانب همکاران، دانشجویان، و خوانندگان عزیز مایه‌ی خوشحالی من خواهد شد.

بر خود لازم می‌دانم که از شورای انتشارات دانشگاه صنعتی اصفهان به خصوص آقای دکتر امیر مظفر امینی ریاست مرکز نشر به خاطر حسن نظر و همکاری صمیمانه در چاپ کتاب تشکر کنم. هم‌چنین از کارکنان مرکز نشر دانشگاه به خاطر همکاری موثر در مراحل چاپ کتاب، به ویژه آقایان ناصر مجاهد و ابراهیم قلمی به خاطر ارائه‌ی نظرات مفید در جهت بهبود کیفیت چاپ کتاب و پیگیری‌های امور چاپ، تشکر کنم. پس از چاپ کتاب در سال ۱۳۸۲، افتخار کتاب برگزیده سال ۱۳۸۳ دانشگاه تهران کسب شد.

در ویرایش جدید کتاب سعی شده که ایرادهای نگارشی و علمی تا حد امکان برطرف شود. هم‌چنین همه‌ی آزمایشگاه‌های آشنایی با GAP که در بخش‌های مختلف پراکنده بودند، در یک فصل مجزا گردآوری شده‌اند. در این مرحله آقای سعید حمیدی دانشجوی دکتری ریاضی در یافتن تعدادی از ایرادهای کتاب به من کمک کرده‌اند، که از ایشان تشکر می‌کنم.

در راستای حمایت از دانشجویان و تسهیل دسترسی به منابع آموزشی، با مساعدت ناشر محترم تصمیم گرفتم ویرایش دوم کتاب را به صورت رایگان در وبسایت خود قرار دهم. هدف من از این اقدام فراهم کردن فرصتی برای یادگیری و رشد علمی دانشجویان عزیز است.
لطفا نظرات و پیشنهادهای خود را برای من ارسال کنید.

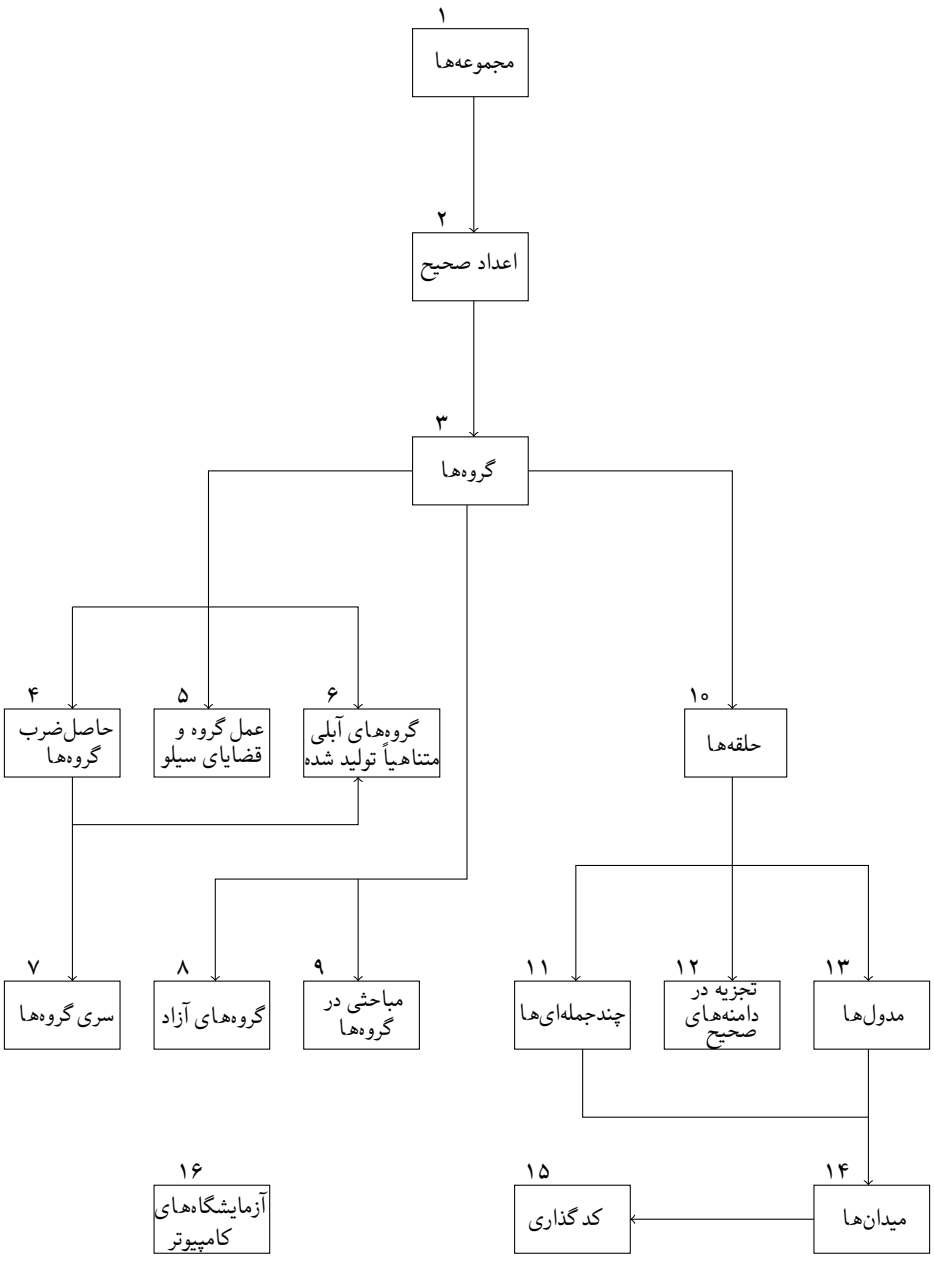
بیژن طائری

شهریور ۱۳۸۲، آذر ۱۴۰۳

دانشکده علوم ریاضی
دانشگاه صنعتی اصفهان

b.taeri@iut.ac.ir
https://taeri.iut.ac.ir/

وابستگی فصل‌های کتاب در نمودار زیر داده شده است.



فصل ۱

مجموعه، رابطه

هدف این فصل مرور مختصر برخی از خواص آشنای مجموعه‌ها، روابط، و توابع است. با این که اغلب این خواص برای خواننده آشنا هستند، مفاهیم معین و نتایج اساسی برای فهم فصل‌های بعد بررسی می‌شوند.

۱.۱ مجموعه

قصد ما بر این نیست که به روش اصل موضوعی با نظریه‌ی مجموعه‌ها برخورد کنیم، بلکه نگرش شهودی به این موضوع داریم. بنابراین مجموعه را گردآیه‌ای از اشیا تلقی می‌کنیم. اگر مجموعه‌ی S داده شده و x عضوی از S باشد می‌نویسیم $x \in S$ و اگر x عضو S نباشد می‌نویسیم $x \notin S$. مجموعه‌ی A را زیرمجموعه‌ی S گوییم هرگاه هر عضو A عضو S باشد؛ در این حالت می‌نویسیم $A \subseteq S$ و می‌گوییم A مشمول در S، یا S شامل A است. اگر $A \subseteq S$ و $S \subseteq A$ گوییم S برابر A است و می‌نویسیم $A = S$، در غیر این صورت می‌نویسیم $A \neq S$. اگر $A \subseteq S$ و $A \neq S$ می‌نویسیم $A \subset S$ و می‌گوییم A به طور سره در S قرار دارد یا A یک زیرمجموعه‌ی سره‌ی S است.
واضح است که هر مجموعه‌ی S زیرمجموعه‌ای از خودش است، یعنی $S \subseteq S$.
مجموعه‌ی تهی یا خالی مجموعه‌ای است که هیچ عضوی ندارد. این مجموعه را با $\emptyset$ نشان می‌دهیم. به ازای هر مجموعه‌ی A، داریم $\emptyset \subseteq A$.
این رابطه به انتفای مقدم درست است، در واقع تهی عضوی ندارد که بودن یا نبودن آن‌را در A بررسی کنیم.
مجموعه‌های اعداد از مجموعه‌های مهم هستند که آن‌ها را با نمادهای زیر نشان می‌دهیم

$\mathbb{N}$: مجموعه‌ی اعداد طبیعی
$\mathbb{Z}$: مجموعه‌ی اعداد صحیح (مثبت، منفی و صفر)
$\mathbb{Q}$: مجموعه‌ی اعداد گویا ($\frac{m}{n}$، m و n اعداد صحیح، $n \neq ۰$)
$\mathbb{R}$: مجموعه‌ی اعداد حقیقی
$\mathbb{C}$: مجموعه‌ی اعداد مختلط

گاهی اوقات برای توصیف مجموعه، اعضای آن‌را فهرست می‌کنیم مثلاً:

$$\mathbb{N} = \{۱, ۲, ۳, \ldots\}$$

یا

$$A = \{۱, ۲, ۳\}.$$

گاهی اوقات نیز با ذکر خواص اعضای مجموعه، آن‌را توصیف می‌کنیم مثلاً:

$$\mathbb{N} = \{x \mid x \in \mathbb{Z},\ \ x > ۰\} = \{x \in \mathbb{Z} \mid x > ۰\}$$

یا

$$A = \{x \in \mathbb{N} \mid ۱ \leq x \leq ۳\}.$$

به طور کلی اگر گزاره‌ی $P(x)$ و مجموعه‌ی S داده شده باشند، نماد

$$A = \{x \mid x \in S,\ \ P(x)\} \quad \text{یا} \quad A = \{x \in S \mid P(x)\}$$

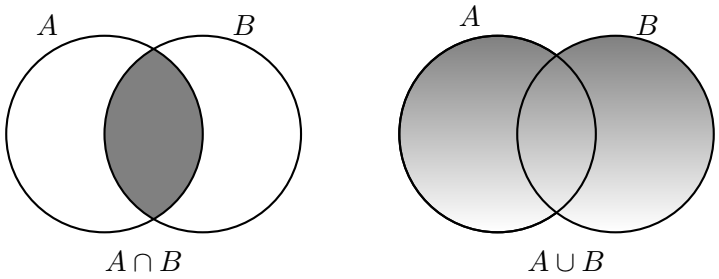
مجموعه‌ی اعضایی از S را مشخص می‌کند که خاصیت P را دارند، یعنی $a \in A$ اگر و تنها اگر $P(a)$ درست باشد. این روش را روش انتزاعی گوییم. البته استفاده‌ی آزادانه از گزاره‌ی $P(x)$ ممکن است باعث مشکلاتی شود. در انتهای بخش به این مطلب باز خواهیم گشت.
اگر A و B دو مجموعه باشند، اجتماع آن‌ها را با $A \cup B$ نشان می‌دهیم و به صورت زیر تعریف می‌کنیم

$$A \cup B = \{x \mid x \in A \text{ یا } x \in B\}.$$

بنابراین $x \in A \cup B$ اگر و تنها اگر $x \in A$ یا $x \in B$ (یا هر دو). بنا به تعریف داریم : $A \subseteq A \cup B$ و $B \subseteq A \cup B$.
هرگاه A و B دو مجموعه باشند اشتراک آن‌ها را با $A \cap B$ نشان می‌دهیم و عبارت است از

$$A \cap B = \{x \mid x \in A,\ \ x \in B\}.$$

پس $x \in A \cap B$ اگر و تنها اگر $x \in A$ و $x \in B$. بنا به تعریف داریم $A \cap B \subseteq A$ و $A \cap B \subseteq B$.
اجتماع و اشتراک را می‌توان با استفاده از شکلی مثل شکل ۱.۱ نشان داد. ناحیه‌ی هاشور خورده مجموعه‌ی مورد نظر است.



شکل ۱.۱: اجتماع و اشتراک دو مجموعه

مثلاً اگر $A = \{۱, ۲, ۳, ۴\}$ و $B = \{۳, ۴, ۵, ۶\}$، آنگاه داریم

$$A \cup B = \{۱, ۲, ۳, ۴, ۵, ۶\}, \qquad A \cap B = \{۳, ۴\}.$$

دو مجموعه‌ی A و B را مجزا گوییم هرگاه $A \cap B = \emptyset$. اجتماع و اشتراک را می‌توان برای تعداد متناهی مجموعه تعریف کرد: اگر $A_۱$، $A_۲$، ...، A_n، n مجموعه باشند اجتماع آن‌ها را با $A_۱ \cup A_۲ \cup \cdots \cup A_n$ یا $\bigcup_{i=۱}^{n} A_i$ نشان می‌دهیم و عبارت است از

$$\bigcup_{i=۱}^{n} A_i = \{x \mid \exists i,\ \ ۱ \le i \le n,\ \ x \in A_i\}$$

(علامت $\exists$ یعنی وجود دارد.) و اشتراک آن‌ها را با $A_۱ \cap A_۲ \cap \cdots \cap A_n$ یا $\bigcap_{i=۱}^{n} A_i$ نشان می‌دهیم که عبارت است از

$$\bigcap_{i=۱}^{n} A_i = \{x \mid \forall i,\ \ ۱ \le i \le n,\ \ x \in A_i\}$$

(علامت $\forall$ یعنی به ازای هر).
فرض کنید $\mathscr{A}$ گردآیه‌ای از مجموعه‌ها باشد. مجموعه‌ی I را یک مجموعه‌ی اندیس برای $\mathscr{A}$ گوییم هرگاه به ازای هر $\alpha \in I$، مجموعه‌ی $A_\alpha \in \mathscr{A}$ وجود داشته باشد و علاوه بر آن $\mathscr{A} = \{A_\alpha \mid \alpha \in I\}$. $\mathscr{A}$ را مجموعه‌ی اندیس‌دار گوییم. مثلاً اگر A_n فاصله‌ی باز

$\left(-\frac{۱}{n},\frac{۱}{n}\right)$ باشد، یعنی $A_n=\left\{x\in\mathbb{R}\mid -\frac{۱}{n}<x<\frac{۱}{n}\right\}$، آنگاه $\mathbb{N}$ یک مجموعه‌ی اندیس برای $\mathscr{A}=\{A_n\mid n\in\mathbb{N}\}$ است. اجتماع مجموعه‌ی اندیس‌دار $\mathscr{A}=\{A_\alpha\mid \alpha\in I\}$ را با $\bigcup\mathscr{A}$ یا $\bigcup_{\alpha\in I}A_\alpha$ نشان می‌دهیم و عبارت است از

$$\bigcup\mathscr{A}=\bigcup_{\alpha\in I}A_\alpha=\{x\mid \exists\alpha\in I,\ \ x\in A_\alpha\}$$

و اشتراک آن را با $\bigcap\mathscr{A}$ یا $\bigcap_{\alpha\in I}A_\alpha$ نشان می‌دهیم و به صورت زیر تعریف می‌کنیم

$$\bigcap\mathscr{A}=\bigcap_{\alpha\in I}A_\alpha=\{x\mid \forall\alpha\in I,\ \ x\in A_\alpha\}.$$

مثلاً اگر $\mathscr{A}=\left\{\left(-\frac{۱}{n},\frac{۱}{n}\right)\mid n\in\mathbb{N}\right\}$، آنگاه

$$\bigcup\mathscr{A}=\bigcup_{n\in\mathbb{N}}\left(-\frac{۱}{n},\frac{۱}{n}\right)=\bigcup_{n=۱}^{\infty}\left(-\frac{۱}{n},\frac{۱}{n}\right)=(-۱,۱)$$

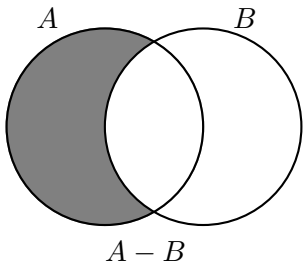
و

$$\bigcap\mathscr{A}=\bigcap_{n\in\mathbb{N}}\left(-\frac{۱}{n},\frac{۱}{n}\right)=\bigcap_{n=۱}^{\infty}\left(-\frac{۱}{n},\frac{۱}{n}\right)=\{۰\}.$$

اگر دو مجموعه‌ی A و B داده شده باشند مکمل یا تفاضل B نسبت به A که با $A-B$ نشان داده می‌شود عبارت است از

$$A-B=\{x\mid x\in A,\quad x\notin B\}.$$

شکل ۲.۱، تفاضل دو مجموعه‌ی A و B را توصیف می‌کند. مثلاً اگر $A=\{۱,۲,۳,۴\}$ و $B=\{۳,۴,۵,۶\}$، آنگاه $A-B=\{۱,۲\}$.



شکل ۲.۱: تفاضل دو مجموعه

اگر X مجموعه‌ای دلخواه باشد، مجموعه‌ی توانی X را با $\mathscr{P}(X)$ نشان می‌دهیم و عبارت است از مجموعه‌ی همه‌ی زیرمجموعه‌های X، یعنی :

$$\mathscr{P}(X)=\{A\mid A\subseteq X\}.$$

مثلاً اگر $X=\{۱,۲,۳\}$، آنگاه

$$\mathscr{P}(X)=\{\emptyset,\{۱\},\{۲\},\{۳\},\{۱,۲\},\{۱,۳\},\{۲,۳\},\{۱,۲,۳\}\}.$$

اکنون مفهوم زوج مرتب‌را، که پایه و اساس همه‌ی ریاضیات است، تعریف می‌کنیم:

تعریف ۱.۱.۱. فرض کنید A و B دو مجموعه‌ی ناتهی باشند و $x\in A$ و $y\in B$. زوج مرتب (x,y) عبارت است از مجموعه‌ی $\{\{x\},\{x,y\}\}$. x را مولفه‌ی اول و y را مولفه‌ی دوم زوج مرتب (x,y) گوییم.

مجموعه‌ی همه‌ی زوج‌های مرتب که مولفه‌ی اول‌شان در A و مولفه‌ی دوم شان در B است را حاصل‌ضرب دکارتی A و B گوییم و با $A \times B$ نشان می‌دهیم. پس

$$A \times B = \{(x, y) \mid x \in A, y \in B\}.$$

نکته اساسی این است که دو زوج مرتب وقتی و فقط وقتی با هم مساوی‌اند که مولفه‌های آن‌ها مساوی باشند : فرض کنید $(a, b), (x, y) \in A \times B$. ادعا می‌کنیم

$$(x, y) = (a, b) \Longleftrightarrow x = a \text{ و } y = b.$$

ابتدا فرض می‌کنیم $x = a$ و $y = b$. در این صورت $\{\{x\}, \{x, y\}\} = \{\{a\}, \{a, b\}\}$، بنابراین $(x, y) = (a, b)$.
برای اثبات عکس مطلب فرض می‌کنیم $(x, y) = (a, b)$. در این صورت طبق تعریف داریم $\{\{x\}, \{x, y\}\} = \{\{a\}, \{a, b\}\}$.
اکنون چون $\{\{x\}, \{x, y\}\} \in \{x\}$، داریم $\{\{x\}, \{x, y\}\} \in \{\{a\}, \{a, b\}\}$. بنابراین $\{x\} = \{a\}$ یا $\{x\} = \{a, b\}$. اگر $\{x\} = \{a\}$، آنگاه داریم $\{a, b\} = \{x, y\}$. از این‌رو $x = a$ و $y = b$. اگر $\{x\} = \{a, b\}$، آنگاه باید داشته باشیم $\{x, y\} = \{a\}$. از این‌رو $x = a = b$ و $x = y = a$. پس در این حالت $x = y = a = b$ و ادعای ما ثابت شد.
مثلاً اگر $A = \{۱, ۲, ۳\}$ و $B = \{۳, ۴\}$، آنگاه

$$A \times B = \{(۱, ۳), (۱, ۴), (۲, ۳), (۲, ۴), (۳, ۳), (۳, ۴)\}.$$

اگر $\mathbb{R}$ مجموعه‌ی اعداد حقیقی باشد $\mathbb{R} \times \mathbb{R}$ همان صفحه‌ی اقلیدسی است.
در ابتدای این بخش گفتیم که برای تعریف مجموعه از طریق توصیف خاصیت یا روش انتزاعی، دو چیز مورد نیاز است. اول مجموعه‌ای مثل S موسوم به مجموعه‌ی مرجع و دوم گزاره‌ای مثل $P(x)$. در این صورت $\{x \in S \mid P(x)\}$ گردآیه‌ی اشیایی از S را مشخص می‌کند که گزاره‌ی $P(x)$ برای آن‌ها درست است. اما روند استفاده‌ی آزادانه از گزاره‌ی $P(x)$ ممکن است باعث مشکلاتی شود. مثال بعدی که به پارادکس راسل معروف است این مشکل را نشان می‌دهد. این مثال را برتراند راسل در سال ۱۹۰۲ برای گوتلوپ فرگه فرستاد و در سال ۱۹۰۳ منتشر شد. این مثال را مستقلاً ارنست زرملو نیز کشف کرد.

مثال ۲.۱.۱. مجموعه‌ای که شامل همه‌ی مجموعه‌ها باشد وجود ندارد.

حل فرض کنید حکم درست نباشد. فرض کنید M مجموعه‌ای شامل همه‌ی مجموعه‌ها باشد. A را مجموعه‌ی همه‌ی اعضایی از M در نظر بگیرید که عضو خودشان نیستند، یعنی $A = \{x \in M \mid x \notin x\}$. بنابراین A شامل مجموعه‌هایی است که گزاره‌ی $P(x) : \ x \notin x$ در مورد آن‌ها درست است. برای خود A دو حالت پیش می‌آید.
حالت اول : $A \in A$. در این حالت چون A باید در گزاره‌ی $P(x) : \ x \notin x$ صدق کند داریم $A \notin A$ که تناقض است.
حالت دوم : $A \notin A$. در این حالت چون A نباید در گزاره‌ی $P(x) : \ x \notin x$ صدق کند داریم $A \in A$، که دوباره تناقض است.
بنابراین هر دو حالت به تناقض منجر شد. پس M نمی‌تواند مجموعه باشد. □

با این حال ، اگر صحبت از گردایه‌ی همه‌ی مجموعه‌ها را به طور کامل کنار بگذاریم مشکل کوچکی به وجود می‌آید. این گردایه نمی‌تواند مجموعه باشد اما چه موقعیتی می‌توان به آن داد؟ برای رفع این مشکل مفهوم رده یا کلاس را معرفی می‌کنیم.یک رده گردآیه‌ای از اشیا است. رده‌ی A را مجموعه گوییم هرگاه رده‌ای مثل B وجود داشته باشد که $A \in B$. بنابراین مجموعه نوع خاصی از رده است. رده‌ای را که مجموعه نباشد رده‌ی سره گوییم. پس مجموعه یک رده‌ی "کوچک" است، اما رده‌ی سره بسیار "بزرگ" (مثل رده‌ی همه‌ی مجموعه‌ها) است. رده‌های دیگری که مجموعه نیستند نیز وجود دارند.

تمرین‌ها

۱. برای مجموعه‌های $A = \{x, y, z\}$ و $B = \{y, w\}$ هر کدام از مجموعه‌های $A \cup B$، $A \cap B$، $A - B$، $B - A$، $A \times B$، $\mathscr{P}(A)$، را مشخص کنید

۲. فرض کنید X، B، A مجموعه باشند. اگر $A \subseteq B$، نشان دهید $A \cap X \subset B \cap X$ و $A \cup X \subset B \cup X$.

۳. ثابت کنید
(الف) $A \subseteq B$ اگر و تنها اگر $A \cap B = A$.
(ب) $A \subseteq B$ اگر و تنها اگر $A \cup B = B$.

۴. فرض کنید X، B، A مجموعه باشند. اگر $A \cap X = B \cap X$ و $A \cup X = B \cup X$، ثابت کنید $A = B$.

۵. فرض کنید C، B، A مجموعه باشند. ثابت کنید
(الف) $A \cup B = B \cup A$ و $A \cap B = B \cap A$.
(ب) $A \cup (B \cup C) = (A \cup B) \cup C$ و $A \cap (B \cap C) = (A \cap B) \cap C$.
(ج) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$، به طور کلی اگر $\{B_\alpha\}_{\alpha \in I}$ خانواده‌ای از مجموعه‌ها باشد، $A \cap (\bigcup_{\alpha \in I} B_\alpha) = \bigcup_{\alpha \in I} (A \cap B_\alpha)$.
(د) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$، به طور کلی اگر $\{B_\alpha\}_{\alpha \in I}$ خانواده‌ای از مجموعه‌ها باشد، $A \cup (\bigcap_{\alpha \in I} B_\alpha) = \bigcap_{\alpha \in I} (A \cup B_\alpha)$.

۶. قوانین دمورگان را ثابت کنید:
(الف) $S - (A \cup B) = (S - A) \cap (S - B)$، به طور کلی $\{A_\alpha\}_{\alpha \in I}$ خانواده‌ای از مجموعه‌ها باشد، $S - \bigcup_{\alpha \in I} A_\alpha = \bigcap_{\alpha \in I} (S - A_\alpha)$.
(ب) $S - (A \cap B) = (S - A) \cup (S - B)$، به طور کلی $\{A_\alpha\}_{\alpha \in I}$ خانواده‌ای از مجموعه‌ها باشد، $S - \bigcap_{\alpha \in I} A_\alpha = \bigcup_{\alpha \in I} (S - A_\alpha)$.

۷. ثابت کنید
(الف) $A \times (B \cap C) = (A \times B) \cap (A \times C)$.
(ب) $A \times (B \cup C) = (A \times B) \cup (A \times C)$.
(ج) $(A \cap B) \times ((X - A) \cap (X - B)) = (A \times (X - A)) \cap (B \times (X - B))$.

۲.۱ رابطه

برخی ریاضیات را علم مطالعه‌ی رابطه‌ها تعریف (یا توصیف) می‌کنند. چون رابطه مجموعه‌ای از زوجهای مرتب است، اولین نتیجه‌ی مهم را از مفهوم زوج مرتب به دست می‌آوریم.

تعریف ۱.۲.۱. یک رابطه‌ی دوتایی یا به طور ساده یک رابطه‌ی R از مجموعه‌ی A به مجموعه‌ی B زیرمجموعه‌ی از $A \times B$ است.

اگر R رابطه‌ای از مجموعه‌ی A به مجموعه‌ی B باشد و $(x, y) \in R$، می‌نویسیم xRy. اگر xRy، گاهی اوقات می‌گوییم x با y در رابطه است. اگر $A = B$ می‌گوییم R یک رابطه‌ی دوتایی روی A است.

مثال ۲.۲.۱. مجموعه‌ی اعداد حقیقی $\mathbb{R}$ را در نظر بگیرید. اگر

$$R = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x \leq y\}$$

آنگاه R یک رابطه‌ی دوتایی روی $\mathbb{R}$ است. □

اگر R رابطه‌ای از مجموعه‌ی A به مجموعه‌ی B باشد. با نگاه کردن به عناصر R می‌توانیم دریابیم که چه عناصری از A با چه عناصری از B نسبت به R در رابطه‌اند. این عناصر A که با عضوی از B در رابطه‌اند زیرمجموعه‌ی از A را تشکیل می‌دهند که دامنه‌ی R نام دارد و عناصر B که عناصری از A با آن‌ها در رابطه است زیرمجموعه‌ی از B را می‌سازند که به برد R موسوم است. به طور دقیق‌تر:

تعریف ۳.۲.۱. فرض کنید R رابطه‌ای از مجموعه‌ی A به مجموعه‌ی B باشد. دامنه‌ی R را که با $\operatorname{dom} R$ نشان می‌دهیم عبارت است از

$$\operatorname{dom} R = \{x \in A \mid \exists y \in B, \ \ (x, y) \in R\}.$$

برد R که با $\operatorname{ran} R$ نشان می‌دهیم عبارت است از

$$\operatorname{ran} R = \{y \in B \mid \exists x \in A,\ \ (x,y) \in R\}.$$

مثال ۴.۲.۱. اگر $A = \{۱,۲,۳,۴\}$ و $B = \{۳,۴,۵\}$، $R \subseteq A \times B$ را با

$$R = \{(۱,۳),(۱,۴),(۲,۵),(۲,۳)\}$$

تعریف می‌کنیم. در این صورت $\operatorname{dom} R = \{۱,۲\}$ و $\operatorname{ran} R = \{۳,۴,۵\}$. □

یکی از روابط مهم رابطه‌ی هم‌ارزی است:

تعریف ۵.۲.۱. فرض کنید R یک رابطه‌ی دوتایی روی مجموعه‌ی A باشد. R را
(الف) بازتابی می‌نامیم هرگاه برای هر $x \in A$، xRx.
(ب) متقارن می‌نامیم هرگاه برای هر $x,y \in A$، از xRy نتیجه می‌شود yRx.
(ج) ترایا می‌نامیم هرگاه برای هر $x,y,z \in A$، از xRy و yRz نتیجه شود xRz.

تعریف ۶.۲.۱. رابطه‌ی دوتایی R را روی مجموعه‌ی A رابطه‌ی هم‌ارزی می‌نامیم هرگاه بازتابی، متقارن و ترایا باشد.

مثال ۷.۲.۱. فرض کنید $A = \{۱,۲,۳,۴,۵\}$. در این صورت رابطه‌ی

$$R = \{(۱,۱),(۲,۲),(۳,۳),(۴,۴),(۵,۵),(۱,۲),(۲,۱)\}$$

یک رابطه‌ای هم‌ارزی روی A است. □

اگر R یک رابطه‌ی هم‌ارزی روی مجموعه‌ی A باشد و $x \in A$، مجموعه‌ی اعضایی از A که با x در رابطه‌اند را با $\bar{x}$ یا $[x]$ یا $\operatorname{class}(x)$ نشان می‌دهیم و رده‌ی هم‌ارزی شامل x گوییم:

$$\bar{x} = \{y \in A \mid xRy\}.$$

در قضیه‌ی زیر خواص اساسی رده‌های هم‌ارزی را ثابت می‌کنیم.

قضیه ۸.۲.۱. فرض کنید R رابطه‌ای هم‌ارزی روی A باشد. در این صورت داریم
(الف) به ازای هر $x \in A$، $\bar{x} \neq \emptyset$.
(ب) اگر $x,y \in A$، آنگاه xRy اگر و تنها اگر $\bar{x} = \bar{y}$.
(ج) به ازای هر $x,y \in A$ یا $\bar{x} = \bar{y}$ یا $\bar{x} \cap \bar{y} = \emptyset$.
(د) $A = \bigcup_{x \in A} \bar{x}$، یعنی A اجتماع رده‌های هم‌ارزی است.

اثبات. (الف) چون R بازتابی است، xRx. بنابراین $x \in \bar{x}$ و $\bar{x} \neq \emptyset$.
(ب) فرض کنید xRy. ثابت می‌کنیم $\bar{y} = \bar{x}$. عضو $z \in \bar{y}$ را در نظر می‌گیریم، پس yRz. چون xRy و yRz و R ترایا است، داریم xRz، یعنی $z \in \bar{x}$. پس $\bar{y} \subseteq \bar{x}$. حال چون xRy و R متقارن است، yRx و بنا به مطلبی که هم اکنون ثابت شد $\bar{x} \subseteq \bar{y}$. پس $\bar{x} = \bar{y}$.
برعکس اگر $\bar{y} = \bar{x}$، آنگاه چون $y \in \bar{y} = \bar{x}$ پس xRy.
(ج) اگر $\bar{x} \cap \bar{y} \neq \emptyset$ ثابت می‌کنیم $\bar{y} = \bar{x}$. فرض کنید $z \in \bar{x} \cap \bar{y}$. پس xRz و yRz. چون R متقارن است، zRy و چون R ترایا است xRy. بنابراین طبق (ب) $\bar{x} = \bar{y}$.
(د) فرض کنید $x \in A$. در این صورت $x \in \bar{x} \subseteq \bigcup_{x \in A} \bar{x}$ و $\bigcup_{x \in A} \bar{x} \subseteq A$. به علاوه چون $\bar{x} \subseteq A$ به ازای هر $x \in A$، پس $\bigcup_{x \in A} \bar{x} \subseteq A$. بنابراین $A = \bigcup_{x \in A} \bar{x}$. □

قضیه‌ی ۸.۲.۱، می‌گوید که رده‌های هم‌ارزی مجموعه‌ی A را افراز می‌کنند. ابتدا مفهوم افراز را بیان می‌کنیم:

تعریف ۹.۲.۱. فرض کنید A مجموعه باشد. گردآیه‌ی $\mathscr{P}$ از زیرمجموعه‌های ناتهی A را افراز A گوییم، هرگاه
(الف) به ازای هر $B, C \in \mathscr{P}$، یا $B = C$ یا $B \cap C = \emptyset$.
(ب) $A = \bigcup_{B \in \mathscr{P}} B$.

مثال ۱۰.۲.۱. (الف) فرض کنید $A = \{۱, ۲, ۳, ۴, ۵, ۶\}$. قرار می‌دهیم $A_۱ = \{۱\}$، $A_۲ = \{۲, ۴, ۶\}$، و $A_۳ = \{۳, ۵\}$، آنگاه $A = A_۱ \cup A_۲ \cup A_۳$، $A_۱ \cap A_۲ = \emptyset$، $A_۱ \cap A_۳ = \emptyset$ و $A_۲ \cap A_۳ = \emptyset$. بنابراین $\mathscr{P} = \{A_۱, A_۲, A_۳\}$ افرازی از A است.
(ب) مجموعه‌ی اعداد صحیح $\mathbb{Z}$ را در نظر بگیرید. اگر A و B، به ترتیب، مجموعه‌ی اعداد زوج و فرد باشند، آنگاه $A \cap B = \emptyset$ و $A \cup B = \mathbb{Z}$. پس $\{A, B\}$ یک افراز $\mathbb{Z}$ است. □

اگر R رابطه‌ی هم‌ارزی دلخواهی روی مجموعه‌ی A باشد، بنا به قضیه‌ی ۸.۲.۱،

$$\mathscr{P} = \{\bar{x} \mid x \in A\}$$

یک افراز A است.
دیدیم از رابطه‌ی هم‌ارزی یک افراز حاصل می‌شود. عکس مطلب نیز درست است:

قضیه ۱۱.۲.۱. فرض کنید $\mathscr{P}$ یک افراز مجموعه‌ی A باشد. رابطه‌ی R را روی A به صورت زیر تعریف می‌کنیم: $x, y \in A$ در رابطه‌اند اگر و تنها اگر به یک عضو $\mathscr{P}$ متعلق باشد، یعنی

$$\forall x, y \in A, \quad xRy \iff \exists B \in \mathscr{P}, \quad x, y \in B.$$

در این صورت R رابطه‌ای هم‌ارزی روی A است و رده‌های هم‌ارزی آن دقیقاً عناصر $\mathscr{P}$ هستند.

اثبات. چون $\mathscr{P}$ افراز A است، $A = \bigcup_{B \in \mathscr{P}} B$. فرض کنید $x \in A$ عضو دلخواهی باشد. پس عضو $B \in \mathscr{P}$ وجود دارد که $x \in B$.
چون $x, x \in B$، داریم xRx و R بازتابی است. حال فرض کنید xRy. پس عضو $B \in \mathscr{P}$ وجود دارد که $x, y \in B$. چون $y, x \in B$، داریم yRx و R متقارن است. در نهایت فرض کنید xRy و yRz. پس اعضای $B, C \in \mathscr{P}$ وجود دارند که $x, y \in B$ و $y, z \in C$.
چون $y \in B \cap C$، داریم $B \cap C \neq \emptyset$. به علاوه، چون $\mathscr{P}$ افراز است، $B = C$. بنابراین $x, z \in B = C$ و xRz. بنابراین R ترایا است. پس ثابت کرده‌ایم R رابطه‌ی هم‌ارزی روی A است.
حال نشان می‌دهیم رده‌های هم‌ارزی R دقیقاً عناصر $\mathscr{P}$ هستند. فرض کنید $x \in A$. چون $A = \bigcup_{B \in \mathscr{P}} B$، عضو $B \in \mathscr{A}$ وجود دارد که $x \in B$. ادعا می‌کنیم $\bar{x} = B$. فرض کنید $u \in \bar{x}$. پس uRx و چون $x \in B$، داریم $u \in B$. بنابراین $\bar{x} \subseteq B$. برعکس فرض کنید $y \in B$. چون $x \in B$، داریم xRy، یعنی $y \in \bar{x}$. بنابراین $B \subseteq \bar{x}$.
در نهایت توجه کنید که اگر $C \in \mathscr{P}$، آنگاه به ازای هر $u \in C$ داریم $C = \bar{u}$. در نتیجه رده‌های هم‌ارزی دقیقاً عناصر $\mathscr{P}$ هستند. □

رابطه‌ی R که در قضیه‌ی ۱۱.۲.۱، ساخته شد را رابطه‌ی هم‌ارزی روی A القا شده توسط افراز $\mathscr{P}$ گوییم.
اگر R رابطه‌ی هم‌ارزی دلخواهی روی مجموعه‌ی A باشد، مجموعه‌ی همه‌ی رده‌های هم‌ارزی را با A/R نشان می‌دهیم. بنابراین

$$A/R = \{\bar{a} \mid a \in A\}.$$

A/R را مجموعه‌ی خارج قسمتی گوییم. بنا به قضیه‌ی ۸.۲.۱، A/R یک افراز A است.
با استفاده از رابطه‌های موجود می‌توان رابطه‌های جدیدی ساخت. مثلاً اگر رابطه‌های R و S از مجموعه‌ی A به مجموعه‌ی B داده شده باشند، می‌توانیم رابطه‌های $R \cap S$، $R \cup S$، $R - S$، $(A \times B) - S$ را به طریق متعارف بسازیم. در همه‌ی روابط فوق دامنه و برد زیرمجموعه‌هایی به ترتیب از A و B هستند. در صورتی که برد رابطه‌ی R زیرمجموعه‌ی دامنه‌ی رابطه‌ی S باشد می‌توان رابطه‌ای دیگر موسوم به ترکیب R و S ساخت:

تعریف ۱۲.۲.۱. فرض کنید R رابطه‌ای از مجموعه‌ی A به مجموعه‌ی B و S رابطه‌ای از B به مجموعه‌ی C باشد. ترکیب R و S که با $S \circ R$ نشان داده می‌شود رابطه‌ای از A به C است و به صورت زیر تعریف می‌شود:

$$x(S \circ R)y \iff \exists z \in B, \quad xRz, \ \ zSy,$$

یعنی

$$S \circ R = \{(x,y) \mid \exists z \in B,\ \ xRz,\ \ zSy\}.$$

اگر R رابطه‌ای روی مجموعه‌ی A باشد، رابطه‌ی R^n را برای هر $n \in \mathbb{N}$ به صورت بازگشتی تعریف می‌کنیم:

$$\begin{aligned} R^{۱} &= R \\ R^n &= R \circ R^{n-۱}, \quad n \geq ۱. \end{aligned}$$

تعریف ۱۳.۲.۱. اگر R رابطه‌ای از A به B باشد، وارون R را که با $R^{-۱}$ نشان می‌دهیم رابطه‌ای از B به A است و به صورت زیر تعریف می‌شود

$$\forall x \in B, \quad \forall y \in A, \quad xR^{-۱}y \iff yRx.$$

بنابراین طبق تعریف

$$R^{-۱} = \{(x,y) \mid yRx\}.$$

در قضیه‌ی بعدی شرط لازم و کافی برای این که یک رابطه‌ی دوتایی رابطه‌ای هم‌ارزی باشد به دست می‌آوریم.

قضیه ۱۴.۲.۱. فرض کنید R یک رابطه روی مجموعه‌ی A باشد. در این صورت R یک رابطه‌ی هم‌ارزی روی A است اگر و تنها اگر سه شرط زیر برقرار باشد

(الف) $\Delta \subseteq R$، که در آن $\Delta = \{(x,x) \mid x \in A\}$.

(ب) $R = R^{-۱}$.

(ج) $R \circ R \subseteq R$.

اثبات. ($\Longleftarrow$) فرض کنید R رابطه‌ی هم‌ارزی روی A باشد. فرض کنید $(x,x) \in \Delta$، که در آن $x \in A$. چون R بازتابی است، داریم $(x,x) \in R$. بنابراین $\Delta \subseteq R$. پس (الف) برقرار است. حال فرض کنید $(x,y) \in R$. چون R متقارن است، $(y,x) \in R$ و بنا به تعریف $R^{-۱}$، $(x,y) \in R^{-۱}$. بنابراین $R \subseteq R^{-۱}$. از طرف دیگر فرض کنید $(x,y) \in R^{-۱}$. پس $(y,x) \in R$. چون R متقارن است، $(x,y) \in R$. بنابراین $R^{-۱} \subseteq R$. در نتیجه $R = R^{-۱}$ و (ب) ثابت شد. در نهایت فرض کنید $(x,y) \in R \circ R$. بنابراین $z \in A$ وجود دارد که $(x,z) \in R$ و $(z,y) \in R$. چون R ترایا است، $(x,y) \in R$. پس $R \circ R \subseteq R$ و (ج) برقرار است.
($\Longrightarrow$) فرض کنید (الف)، (ب) و (ج) برقرار باشند. به ازای هر $x \in A$ بنا به (الف)، $(x,x) \in \Delta \subseteq R$ و R بازتابی است. حال فرض کنید $(x,y) \in R$، پس بنا به (ب)، $(x,y) \in R^{-۱}$. بنابراین $(y,x) \in R$ و R متقارن است. در نهایت فرض کنید $(x,y) \in R$ و $(y,z) \in R$. در این صورت $(x,z) \in R \circ R$ و بنا به (ج) $(x,z) \in R$. بنابراین R ترایا است. پس ثابت شد که R رابطه‌ی هم‌ارزی است. □

تمرین‌ها

۱. کدام رابطه‌ی $\sim$ در زیر رابطه‌ی هم‌ارزی روی مجموعه‌ی A است.

(الف) $A = \{-۲, -۱, ۰, ۱, ۲\}$، $a \sim b$ اگر و تنها اگر $a^۳ - a = b^۳ - b$.

(ب) $A = \mathbb{Z}$، $a \sim b$ اگر و تنها اگر $a \leq b$.

(ج) $A = \mathbb{R} \times \mathbb{R}$، $(x,y) \sim (x_۱, y_۱)$ اگر و تنها اگر $y - ۳x = y_۱ - ۳x_۱$.

۲. فرض کنید $A = \{۱, ۲, ۳, ۴, ۵, ۶\}$ و $R = \{(a,b) \in A \times A \mid a + b \leq ۹\}$.

(الف) اعضای R را فهرست کنید، دامنه و برد R را بیابید.

(ب) آیا $\Delta \subseteq R$، که در آن $\Delta = \{(x,x) \mid x \in A\}$؟

(ج) آیا $R = R^{-۱}$؟

(د) آیا $R \circ R \subseteq R$؟

۳. همه‌ی روابط هم‌ارزی روی مجموعه‌ی $A = \{a, b, c\}$ را بیابید.

۴. همه‌ی افرازهای $A = \{۱, ۲, ۳, ۴\}$ را بیابید.

۵. اگر $R_۱$ و $R_۲$ رابطه‌هایی روی مجموعه‌ی S باشند، کدامیک از قضیه‌های زیر درست هستند؟ در صورت درستی، آن را ثابت کنید و در غیر این صورت مثال نقض بیاورید.
(الف) اگر $R_۱$ و $R_۲$ بازتابی باشند، آنگاه $R_۱ \circ R_۲$ بازتابی است.
(ب) اگر $R_۱$ و $R_۲$ متقارن باشند، آنگاه $R_۱ \circ R_۲$ متقارن است.
(ج) اگر $R_۱$ و $R_۲$ ترایا باشند، آنگاه $R_۱ \circ R_۲$ ترایا است.
(د) اگر $R_۱$ ترایا باشد، آنگاه $R_۱ \circ R_۲$ ترایا است.
(هـ) اگر $R_۱$ ترایا باشد، آنگاه $R_۱^{-۱}$ نیز ترایا است.

۶. فرض کنید $R_۱$ و $R_۲$ رابطه‌های متقارن روی مجموعه‌ی A باشند. نشان دهید $R_۱ \circ R_۲$ متقارن است اگر و تنها اگر $R_۱ \circ R_۲ = R_۲ \circ R_۱$.

۷. فرض کنید R رابطه‌ای بازتابی و ترایا روی مجموعه‌ی A باشد. نشان دهید $R \cap R^{-۱}$ رابطه‌ی هم‌ارزی است.

۳.۱ مجموعه‌های جزئاً مرتب

در بخش قبل رابطه‌های دوتایی و خواص اساسی آن‌ها را مطالعه کردیم. رابطه‌هایی را در نظر گرفتیم که بازتابی، متقارن، و ترایا هستند. در این بخش رابطه‌هایی را در نظر می‌گیریم که بازتابی و ترایا هستند و در خاصیت دیگری که پاد متقارن نامیده می‌شود صدق می‌کنند. با تعریف زیر شروع می‌کنیم.

تعریف ۱.۳.۱. رابطه‌ی R روی یک مجموعه‌ی A را رابطه‌ی ترتیب جزیی گوییم هرگاه
(الف) به ازای هر $a \in A$، $(a, a) \in R$، (یعنی R بازتابی باشد)
(ب) به ازای هر $a, b \in A$ از $(a, b) \in R$ و $(b, a) \in R$ نتیجه شود $a = b$ (یعنی R پاد متقارن باشد)
(ج) به ازای هر $a, b, c \in A$ اگر $(a, b) \in R$ و $(b, c) \in R$، آنگاه $(a, c) \in R$، (یعنی R ترایا باشد).

بنابراین طبق تعریف، رابطه‌ی بازتابی، پاد متقارن و ترایا روی مجموعه‌ی A، ترتیب جزیی روی A نامیده می‌شود.

مثال ۲.۳.۱. رابطه‌ی R روی $\mathbb{Z}$ با $(a, b) \in R$ اگر و تنها اگر $a \leq b$، رابطه‌ی ترتیب جزیی است. □

اگر $a, b \in \mathbb{Z}$ $(a, b \in \mathbb{N})$. گوییم a، b را در $\mathbb{Z}$ $(\mathbb{N})$ عاد می‌کند و می‌نویسیم $a|b$، هرگاه عدد $k \in \mathbb{Z}$ $(k \in \mathbb{N})$ وجود داشته باشد که $b = ak$.

مثال ۳.۳.۱. نشان دهید رابطه‌ی R روی $\mathbb{N}$ با $(a, b) \in R$ اگر و تنها اگر در $\mathbb{N}$، $a|b$، رابطه‌ی ترتیب جزیی است.

حل فرض کنید $a \in \mathbb{N}$. چون $a = ۱a$ داریم $a|a$ و $(a, a) \in R$. پس R بازتابی است. اکنون اگر $(a, b), (b, a) \in R$، آنگاه $a|b$ و $b|a$. پس $m, n \in \mathbb{N}$ وجود دارند که $b = an$ و $a = bm$. در نتیجه $a = bm = anm$ و بنابراین $nm = ۱$. چون m و n اعداد صحیح مثبت هستند ، داریم $m = n = ۱$. پس $a = b$ و R پاد متقارن است. در نهایت فرض کنید $(a, b) \in R$، (b, c). بنابراین در $\mathbb{N}$، $a|b$، $b|c$ و اعداد $m, n \in \mathbb{N}$ وجود دارند که $b = an$ و $c = bm$. در نتیجه $c = bm = anm$. چون $nm \in \mathbb{N}$، $a|c$. پس $(a, c) \in R$ و R ترایا است.
در نتیجه R ترتیب جزیی روی $\mathbb{N}$ است. □

مثال ۴.۳.۱. نشان دهید رابطه‌ی R روی $\mathbb{Z}$ با $(a, b) \in R$ اگر و تنها اگر در $\mathbb{Z}$، $a|b$، رابطه‌ی ترتیب جزیی نیست.

حل می‌توان دید R بازتابی و ترایا است. چون $(-۲)(-۱) = ۲$ و $۲(-۱) = -۲$ داریم $(۲, -۲) \in R$ و $(-۲, ۲) \in R$، اما $-۲ \neq ۲$. پس R پاد متقارن نیست. □

مثال ۵.۳.۱. فرض کنید S مجموعه‌ای دلخواه باشد. رابطه‌ی $\subseteq$ روی $\mathscr{P}(S)$، مجموعه‌ی توانی S، رابطه‌ی ترتیب جزیی است. □

یک رابطه‌ی ترتیب جزیی روی مجموعه‌ی S را معمولاً با $\leq$ نشان می‌دهیم و به جای $(a,b) \in \leq$ می‌نویسیم $a \leq b$. اگر $a \leq b$ و $a \neq b$ می‌نویسیم $a < b$. اگر $\leq$ یک رابطه‌ی ترتیب جزیی روی S باشد، گوییم S یک مجموعه‌ی جزئاً مرتب است و می‌نویسیم $(S, \leq)$. اگر S مجموعه‌ی جزئاً مرتب باشد، $a, b \in S$ را قابل مقایسه گوییم هرگاه $a \leq b$ یا $b \leq a$. یک مجموعه‌ی جزئاً مرتب $(S, \leq)$ را مجموعه‌ی مرتب خطی یا زنجیر گوییم هرگاه به ازای هر $x, y \in S$، یا $x \leq y$ یا $y \leq x$. بنابراین یک زنجیر مجموعه‌ای جزئاً مرتب است که هر دو عضو آن قابل مقایسه باشند.

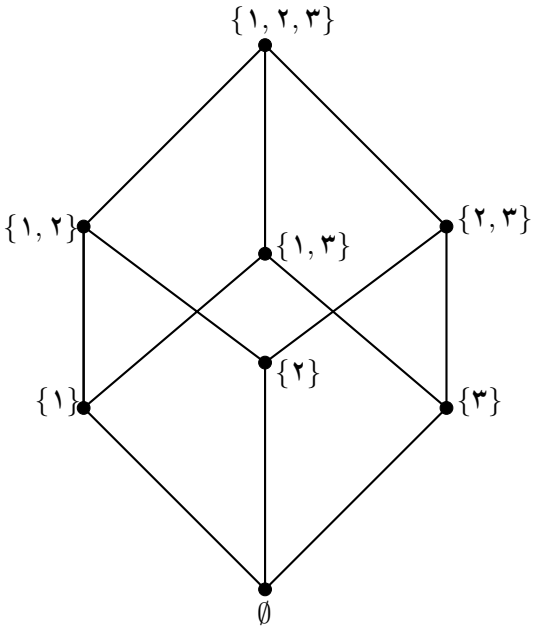
مثال ۶.۳.۱. (الف) $\mathbb{Z}$ به همراه رابطه‌ی "کوچک‌تر یا مساوی" معمولی، $\leq$، یک زنجیر است.
(ب) $\mathbb{N}$ به همراه رابطه‌ی تقسیم پذیری زنجیر نیست، زیرا $۵ \nmid ۳$ و $۳ \nmid ۵$.
(ج) اگر S مجموعه‌ای با بیش از یک عضو باشد، $\mathscr{P}(S)$ به همراه رابطه‌ی "شمول" معمولی $\subseteq$، زنجیر نیست، زیرا اگر $a, b \in S$ دو عضو متمایز باشند، آنگاه $\{a\} \not\subseteq \{b\}$ و $\{b\} \not\subseteq \{a\}$. □

فرض کنید $(S, \leq)$ مجموعه‌ی جزئاً مرتب باشد. $a \in S$ را عضو ماکسیمال S گوییم هرگاه از $a \leq b$ نتیجه شود $a = b$. بنابراین a ماکسیمال است هرگاه عضو $b \in S$ وجود نداشته باشد که $a < b$. عضو $a \in S$ را عضو می‌نیمال S گوییم هرگاه از $b \leq a$ نتیجه شود $b = a$. بنابراین a می‌نیمال است هرگاه عضو $b \in S$ وجود نداشته باشد که $b < a$. عضو $a \in S$ را عضو ماکسیمم S گوییم هرگاه برای هر $b \in S$ داشته باشیم $b \leq a$. عضو $a \in S$ عضو می‌نیمم S گوییم هرگاه برای هر $b \in S$ داشته باشیم $a \leq b$. واضح است که هر عضو ماکسیمم (می‌نیمم) عضو ماکسیمال (می‌نیمال) نیز هست.

مثال ۷.۳.۱. اگر $S = \{۱, ۲, ۳\}$، آنگاه

$$\mathscr{P}(S) = \{\emptyset, \{۱\}, \{۲\}, \{۳\}, \{۱, ۲\}, \{۱, ۳\}, \{۲, ۳\}, \{۱, ۲, ۳\}\}.$$

$(\mathscr{P}(S), \subseteq)$ یک مجموعه‌ی جزئاً مرتب است. نمودار این رابطه در شکل ۳.۱ داده شده است.



شکل ۳.۱: نمودار یک مجموعه‌ی جزئاً مرتب

$S = \{۱, ۲, ۳\}$ عضو ماکسیمم $\mathscr{P}(S)$ و $\emptyset$ عضو می‌نیمم $\mathscr{P}(S)$ است. فرض کنید $T = \{\{۱\}, \{۲\}, \{۳\}, \{۱, ۲\}, \{۱, ۳\}, \{۲, ۳\}\}$ مجموعه‌ی همه‌ی زیرمجموعه‌های ناتهی و سره‌ی S باشد. در این صورت $(T, \subseteq)$ مجموعه‌ی جزئاً مرتب است. در این مجموعه اعضای می‌نیمال عبارت‌اند از $\{۱\}$، $\{۲\}$ و $\{۳\}$ و اعضای ماکسیمال عبارت‌اند از $\{۴, ۳\}$، $\{۱, ۳\}$ و $\{۱, ۲\}$. هم‌چنین T عضو ماکسیمم و می‌نیمم ندارد. □

فرض کنید $(S, \leq)$ مجموعه‌ی جزئاً مرتب باشد و $X \subseteq S$. عضو $a \in S$ کران بالای X می‌نامیم هرگاه برای هر $x \in X$، $x \leq a$. $b \in S$ را کران پایین X می‌نامیم هرگاه برای هر $x \in X$، $b \leq x$. قضیه‌ی بعدی که به لم زُرن معروف است از قضیه‌های مهم در نظریه‌ی مجموعه‌هاست و کاربردهای فراوانی در سایر شاخه‌های ریاضیات دارد. این قضیه با اصل موضوع انتخاب معادل است و بررسی آن را می‌توان در کتاب مرجع [۲] یافت.

قضیه ۸.۳.۱. (لم زُرن) اگر هر زنجیر در مجموعه‌ی جزئاً مرتب $(S, \leq)$ یک کران بالا در S داشته باشد، آنگاه S دارای یک عضو ماکسیمال است. □

لم زُرن را کوراتوفسکی در مقاله‌ای به سال ۱۹۲۲ برای اولین بار بیان کرد. لم زُرن با اصل موضوع انتخاب، که یکی از اصول مهم نظریه‌ی مجموعه‌هاست، معادل است. اهمیت لم زُرن در این حقیقت نهفته است که برای بسیاری از کاربردها در ریاضیات مناسبت دارد. برای مثال، در جبر خطی اثبات این که هر فضای برداری دارای پایه است نیاز به صورتی از اصل موضوع انتخاب دارد ، و لم زُرن صورتی مناسب برای استفاده در این کار است (فرض کنید $\mathscr{A}$ خانواده‌ای از همه‌ی مجموعه‌های مستقل خطی باشد، در این صورت یک عضو ماکسیمال یک پایه است). به طریق مشابه در اثبات وجود ایدآل سره‌ی ماکسیمال در یک حلقه یکدار یا در اثبات وجود زیرگروه آبلی ماکسیمال در یک گروه، لم زُرن ابزار مناسبی را فراهم می‌کند.
می‌توان بحثی به صورت زیر انجام داد که درستی لم را توجیه کند. S نمی‌تواند تهی باشد، چون $\emptyset$ یک زنجیر است و بنابراین $\bigcup \emptyset = \emptyset \in S$. ممکن است $\emptyset$ ماکسیمال نباشد، پس می‌توان یک مجموعه‌ی بزرگ‌تر انتخاب کرد. اگر این مجموعه نیز ماکسیمال نباشد، می‌توان مجموعه‌ی بزرگ‌تر دیگری انتخاب کرد. بعد از تعداد نامتناهی مرحله، حتی اگر نتوان یک مجموعه‌ی ماکسیمال یافت حداقل یک زنجیر به وجود آمده است. بنابراین می‌توان اجتماع آن را در نظر گرفت و ادامه داد. روند فوق را تنها موقعی متوقف می‌کنیم که به یک مجموعه‌ی ماکسیمال رسیده باشیم. پس اگر به اندازه کافی صبور باشیم، به چنین مجموعه‌ای خواهیم رسید.

تمرین‌ها

۱. برای هر یک از مجموعه‌های جزئاً مرتب زیر نمودار ترتیب جزئی را رسم کنید.
(الف) $(\{a \in \mathbb{N} \mid a|۲۰\}, \leq)$، که در آن $\leq$ رابطه‌ی تقسیم پذیری است.
(ب) $(\mathbb{N}, \leq)$، که در آن $\leq$ رابطه‌ی ترتیب متعارف است.
(ج) $(\mathscr{P}(A), \subseteq)$، که در آن $A = \{۱, ۲, ۳, ۴\}$.
(د) $(\mathscr{P}(A) - \{\emptyset\}, \subseteq)$، که در آن $A = \{۱, ۲, ۳\}$.

۲. رابطه‌ای مثال بزنید که پاد متقارن باشد ولی بازتابی نباشد.

۳. نشان دهید $(\mathbb{R}, \leq)$ مجموعه‌ی جزئاً مرتب نیست، که در آن $a \leq b$ یعنی $d \in \mathbb{R}$ وجود دارد که $b = ad$.

۴. فرض کنید $\leq_۱$ و $\leq_۲$ دو رابطه‌ی ترتیب جزیی روی مجموعه‌ی A باشند. آیا $\leq_۲ \cap \leq_۱$ رابطه‌ی ترتیب جزیی روی A است؟

۵. اگر $(A, \leq_۱)$ و $(B, \leq_۲)$ مجموعه‌های جزئاً مرتب باشند، نشان دهید $(A \times B, \leq)$ مجموعه‌ای جزئاً مرتب است، که در آن $(a, b) \leq (c, d)$ اگر و تنها اگر $a \leq_۱ c$ و $b \leq_۲ d$.

۴.۱ استقرا

در فصل بعد خواص مجموعه‌ی اعداد صحیح را به طور مفصل بررسی می‌کنیم. اما برای ادامه‌ی این فصل به معرفی یک اصل مهم، به نام اصل استقرای ریاضی ، نیاز داریم. این اصل معادل با اصل خوش‌ترتیبی است. اثبات بسیاری از نتایج جبر مبتنی بر خاصیت اساسی زیر از اعداد صحیح موسوم به اصل خوش‌ترتیبی است:

اصل خوش‌ترتیبی. هر زیرمجموعه‌ی ناتهی از $\mathbb{N}$ کوچک‌ترین عضو دارد ، یعنی اگر $\emptyset \neq S \subseteq \mathbb{N}$، آنگاه $x \in S$ وجود دارد که به ازای هر $y \in S$، $x \leq y$.

فرض کنید $S \subseteq \mathbb{N}$ در خواص زیر صدق می‌کند
(الف) عضوی مثل $n_۰$ در S وجود دارد.

(ب) برای هر $n \in \mathbb{N}$ که $n \geq n_۰$، اگر $n \in S$، آنگاه $n + ۱ \in S$.
نشان می‌دهیم $\{n \in \mathbb{N} \mid n \geq n_۰\} \subseteq S$. فرض کنید $T = \{n \in \mathbb{N} \mid n \geq n_۰\}$ و $T \not\subseteq S$. در این صورت $a \in T$ وجود دارد که $a \notin S$. پس $T_۱ = \{n \in T \mid n \notin S\}$ زیرمجموعه‌ی ناتهی $\mathbb{N}$ است. بنابراین بنا به اصل خوش‌ترتیبی ، $T_۱$ کوچک‌ترین عضو دارد ، مثلاً m. پس $m \in T$ و $m \notin S$. چون $m \in T$، $m \geq n_۰$. اگر $m = n_۰$، آنگاه بنا به (الف)، $m \in S$ که تناقض است. پس $m > n_۰$ و $m - ۱ \geq n_۰$. بنابراین $m - ۱ \in T$. اکنون چون m کوچک‌ترین عضو $T_۱$ است، $m - ۱ \in S$. پس بنا به (ب)، $m = (m - ۱) + ۱ \in S$، که تناقض است. در نتیجه $T \subseteq S$.
بنابراین از اصل خوشترتیبی، یکی از خاصیت‌های مهم اعداد صحیح موسوم به اصل استقرای ریاضی نتیجه می‌شود:

قضیه ۱.۴.۱. (اصل استقرای ریاضی) فرض کنید $S \subseteq \mathbb{N}$، $n_۰ \in S$. فرض کنید S در یکی از شرایط زیر صدق می‌کند.
(الف) به ازای هر $n \in \mathbb{N}$ که $n \geq n_۰$، اگر $n \in S$، آنگاه $n + ۱ \in S$.
(ب) به ازای هر $n \in \mathbb{N}$، اگر $m < n$، $m \in S$، آنگاه $n \in S$. در این صورت

$$\{n \in \mathbb{N} \mid n \geq n_۰\} \subseteq S. \qquad \square$$

قسمت (الف) قضیه را ثابت کردیم و قسمت (ب) را به عنوان تمرین به خواننده واگذار می‌کنیم.
گزاره‌ی زیر، گزاره‌ای آشناست:

$$۱ + ۲ + \cdots + n = \frac{n(n+۱)}{۲}, \quad n \geq ۱.$$

این گزاره را به استقرا ثابت می‌کنیم. فرض کنید $S(n)$ گزاره‌ی زیر باشد:

$$S(n): \quad ۱ + ۲ + \cdots + n = \frac{n(n+۱)}{۲}, \quad n \geq ۱.$$

هرگاه سمت راست گزاره با سمت چپ آن مساوی باشد این گزاره درست است. فرض کنید $S = \{n \in \mathbb{N} \mid S(n) \text{ درست }\}$. نشان می‌دهیم $S = \mathbb{N}$. اکنون داریم

$$۱ = \frac{۱ \cdot (۱+۱)}{۲},$$

یعنی $S(۱)$ درست است و بنابراین $۱ \in S$. فرض کنید $n \in \mathbb{N}$ و $S(n)$ درست باشد، یعنی $n \in S$. نشان می‌دهیم $S(n+۱)$ درست است. داریم

$$S(n+۱): \quad ۱ + ۲ + \cdots + n + (n+۱) = \frac{(n+۱)(n+۲)}{۲}.$$

سمت چپ را در نظر می‌گیریم

$$\begin{aligned} ۱ + ۲ + \cdots + n + (n+۱) &= \frac{n(n+۱)}{۲} + (n+۱) \\ &= \frac{(n+۱)(n+۲)}{۲} \end{aligned}$$

(چون $S(n)$ درست است). بنابراین $S(n+۱)$ درست است و $n + ۱ \in S$. بنا به اصل استقرای ریاضی $S = \mathbb{N}$. این مطلب ادعای ما را ثابت می‌کند: به ازای هر $n \in \mathbb{N}$،

$$۱ + ۲ + \cdots + n = \frac{n(n+۱)}{۲}.$$

اثبات با استفاده از اصل استقرا سه مرحله دارد :
مرحله‌ی اول : نشان دهید $n_۰ \in S$، یعنی نشان دهید به ازای یک $n_۰ \in \mathbb{N}$، گزاره‌ی $S(n_۰)$ درست است.
مرحله‌ی دوم: فرض استقرا را بنویسید: n عدد صحیحی است که $n \geq n_۰$ و $n \in S$، یعنی به ازای عدد صحیح n که $n \geq n_۰$، $S(n)$ درست است (یا k عدد صحیح است که $n_۰ < k \leq n$ و $S(k)$ درست است).
مرحله‌ی سوم: نشان دهید $n + ۱ \in S$، یعنی $S(n+۱)$ درست است.

مثال ۲.۴.۱. نشان دهید برای هر $n \geq ۳$، $۲n + ۱ \leq ۲^n$.

حل فرض کنید $S(n)$ گزاره‌ی

$$S(n): \quad ۲n + ۱ \leq ۲^n, \quad n \geq ۳$$

باشد. ابتدا باید درستی گزاره‌ی $S(۳)$ را بررسی کنیم. فرض کنید $n = ۳$. چون $۲^n = ۲^۳ = ۸$ و $۲n + ۱ = ۲ \times ۳ + ۱ = ۷$، پس $S(۳)$ درست است. حال فرض کنید به ازای یک $n \geq ۳$، $S(n)$ درست باشد، یعنی به ازای یک $n \geq ۳$، $۲n + ۱ \leq ۲^n$. گزاره‌ی $S(n + ۱)$ را در نظر می‌گیریم :

$$S(n + ۱): \quad ۲(n + ۱) + ۱ \leq ۲^{n+۱}.$$

داریم

$$\begin{aligned} ۲(n + ۱) + ۱ &= (۲n + ۱) + ۲ \\ &\leq ۲^n + ۲, \quad (\text{چون } S(n) \text{ درست است}) \\ &\leq ۲^n + ۲^n, \quad (\text{چون } ۲ \leq ۲^n, n \geq ۳) \\ &= ۲^{n+۱} \end{aligned}$$

پس $S(n + ۱)$ درست است و به استقرا به ازای هر $n \geq ۳$، $۲n + ۱ \leq ۲^n$. □

اصل استقرا ابزار بسیار مفیدی در ریاضیات است و از آن در سرتاسر کتاب استفاده می‌کنیم.

تمرین‌ها

۱. با استفاده از استقرای ریاضی اتحادهای زیر را ثابت کنید.

(الف) $۱^۲ + ۲^۲ + \cdots + n^۲ = \frac{n(n+۱)(۲n+۱)}{۶}$، $n \geq ۱$.

(ب) $۱ + ۵ + ۹ + \cdots + (۴n - ۳) = n(۲n - ۱)$، $n \geq ۱$.

(ج) $\frac{۱}{۲!} + \frac{۲}{۳!} + \frac{۳}{۴!} + \cdots + \frac{n}{(n+۱)!} = ۱ - \frac{۱}{(n+۱)!}$، $n \geq ۱$.

(د) $\frac{۱}{۱ \times ۲} + \frac{۱}{۲ \times ۳} + \cdots + \frac{۱}{n \times (n+۱)} = \frac{n}{n+۱}$، $n \geq ۱$.

(هـ) $۱ \times ۲ + ۲ \times ۳ + \cdots + n(n+۱) = \frac{n(n+۱)(n+۲)}{۳}$، $n \geq ۱$.

۲. قضیه‌های داده شده را به استقرا ثابت کنید.

(الف) به ازای هر $n \in \mathbb{N}$، $n < ۲^n$.

(ب) به ازای هر $n \in \mathbb{N}$، که $n \geq ۴$، $۲^n \geq n^۲$.

(ج) به ازای هر $n \in \mathbb{N}$، که $n \geq ۷$، $n! \geq n^۳$.

۳. فرض کنید n و r اعداد صحیح باشند به طوری‌که $۰ < r \leq n$ ضرایب دوجمله‌ای عبارت است از $\binom{n}{r} = \frac{n!}{r!(n-r)!}$. نشان دهید

(الف) $\binom{n}{r} = \binom{n}{n-r}$

(ب) $\binom{n}{r} + \binom{n}{r-۱} = \binom{n+۱}{r}$ (اتحاد پاسکال).

(ج) قضیه‌ی دوجمله‌ای را ثابت کنید: $(a+b)^n = \sum_{k=۰}^{n} \binom{n}{k} a^k b^{n-k}$ ، a و b اعداد حقیقی و $n \in \mathbb{N}$.

۴. اگر S مجموعه‌ای n عضوی باشد، نشان دهید $|\mathscr{P}(S)| = ۲^n$.

۵.۱ توابع

مفهوم تابع، همچون مجموعه، نقش اساسی در ریاضیات دارد. تابع حالت خاصی از رابطه است. توابع به ما کمک می‌کنند که ارتباط بین ساختارهای جبری متفاوت را مطالعه کنیم. در این بخش خواص اساسی توابع را مرور می‌کنیم. به طور شهودی تابع تناظر خاصی بین اعضای یک مجموعه و اعضای مجموعه‌ای دیگر است. به طور دقیق‌تر تابع زیرمجموعه‌ی مشخصی از زوجهای مرتب است.

تعریف ۱.۵.۱. فرض کنید A و B مجموعه باشند. رابطه‌ی f از A به B را تابع (یا نگاشت) از A به B گوییم، هرگاه
(الف) $\operatorname{dom} f = A$
(ب) به ازای هر $(x_۱, y_۱), (x, y) \in f$، از $x = x_۱$ نتیجه شود $y = y_۱$.

هرگاه شرط (ب)، در تعریف فوق، در مورد رابطه‌ای مثل f برقرار باشد گوییم f خوش‌تعریف (یا تک‌مقداری) است. اگر f تابعی از A به B باشد، می‌نویسیم $f : A \longrightarrow B$. اگر $(x, y) \in f$ معمولاً می‌نویسیم $y = f(x)$. y را تصویر x تحت f و x را پیش تصویر y تحت f گوییم. نماد $f(x)$ را اولین بار کلرو (۱۷۳۴) ابداع کرد و اویلر به طور گسترده از آن استفاده نمود. دیریکله تعریف مرسوم تابع را ارائه کرد.
فرض کنید $f : A \longrightarrow B$. در این صورت f زیرمجموعه‌ی از $A \times B$ است طوری که به ازای هر $x \in A$، عضو یکتای y وجود دارد که $(x, y) \in f$. پس می‌توانیم یک تابع را به عنوان قاعده‌ای که به هر عضو x از A دقیقاً یک عضو y از B را نظیر می‌کند تصور کنیم. برای این که نشان دهیم رابطه‌ی f از A به B یک تابع است، ابتدا باید نشان دهیم دامنه‌ی f برابر A است. سپس نشان دهیم f خوش تعریف یا تک‌مقداری است. یعنی اگر در A، $x = y$، آنگاه در B، $f(x) = f(y)$.

مثال ۲.۵.۱. فرض کنید $f \subseteq \mathbb{R} \times \mathbb{R}$ و $f = \{(x, ۳x + ۱) \mid x \in \mathbb{R}\}$. در این صورت $\operatorname{dom} f = \mathbb{R}$. به وضوح f خوش تعریف و بنابراین تابع است. □

مثال ۳.۵.۱. فرض کنید $f \subseteq \mathbb{Q} \times \mathbb{Z}$ و

$$f = \left\{ \left(\frac{a}{b}, a \right) \mid a, b \in \mathbb{Z},\ \ b \neq ۰ \right\}.$$

ابتدا توجه کنید $\operatorname{dom} f = \mathbb{Q}$. پس f در اولین شرط تابع صدق می‌کند. اکنون $\left(\frac{۲}{۳}, ۲\right) \in f$ و $\left(\frac{۴}{۶}, ۴\right) \in f$ و $\frac{۴}{۶} = \frac{۲}{۳}$. اما $f\left(\frac{۴}{۶}\right) = ۴ \neq ۲ = f\left(\frac{۲}{۳}\right)$. بنابراین f خوش تعریف نیست، یعنی f تابعی از $\mathbb{Q}$ به $\mathbb{Z}$ نیست. □

اکنون تساوی دو تابع را بررسی می‌کنیم. فرض کنید $f : A \longrightarrow B$ و $g : A \longrightarrow B$ دو تابع باشند. در این صورت $f, g \subseteq A \times B$. فرض کنید $f = g$. عضو دلخواه $x \in A$ را در نظر می‌گیریم. پس $(x, f(x)) \in f = g$. هم‌چنین $(x, g(x)) \in g$. چون g تابع است، داریم $f(x) = g(x)$. اکنون فرض کنید به ازای هر $x \in A$، $f(x) = g(x)$. اگر $(x, y) \in f$، آنگاه $y = f(x) = g(x)$. پس $(x, y) \in g$. این یعنی $f \subseteq g$. به طریق مشابه $g \subseteq f$ و بنابراین $f = g$. پس دو تابع $f : A \longrightarrow B$ و $g : A \longrightarrow B$ برابرند اگر و تنها اگر به ازای هر $x \in A$، $f(x) = g(x)$.

تعریف ۴.۵.۱. فرض کنید f تابعی از مجموعه‌ی A به مجموعه‌ی B باشد. در این صورت
(الف) f را یک‌به‌یک گوییم، هر گاه به ازای هر $x_۱, x_۲ \in A$ از $f(x_۱) = f(x_۲)$ نتیجه شود $x_۱ = x_۲$.
(ب) f را پوشا گوییم هرگاه $\operatorname{ran} f = B$. یعنی به ازای هر $y \in B$ عضو $x \in A$ وجود داشته باشد که $f(x) = y$.

بنابراین f یک‌به‌یک است اگر و تنها اگر هر عضو B حداکثر یک پیش تصویر داشته باشد. هم‌چنین f پوشاست اگر و تنها اگر هر عضو B حداقل یک پیش تصویر داشته باشد.
فرض کنید A مجموعه‌ای ناتهی باشد. تابع $\mathrm{id}_A : A \longrightarrow A$ با ضابطه‌ی $\mathrm{id}_A(x) = x$، به ازای هر $x \in A$، تابعی یک‌به‌یک و پوشا از A به A است. id_A را تابع همانی روی A گوییم.
فرض کنید A و B مجموعه باشند و $f : A \longrightarrow B$. در این صورت $f^{-۱}$ رابطه‌ای از B به A است، یعنی $f^{-۱} \subseteq B \times A$. هم‌چنین طبق تعریف، $(x, y) \in f$ اگر و تنها اگر $(y, x) \in f^{-۱}$. $f^{-۱}$ چه موقع تابع است؟ در واقع f یک‌به‌یک است اگر و تنها اگر $f^{-۱}$ تابع باشد :

قضیه ۵.۵.۱. فرض کنید A و B مجموعه باشند. در این صورت $f : A \longrightarrow B$ یک‌به‌یک است اگر و تنها اگر f^{-1} تابعی از $\mathrm{Im}\, f$ به A باشد. در این حالت f^{-1} یک‌به‌یک است. به علاوه f پوشاست اگر و تنها اگر f^{-1} پوشا باشد.

اثبات. ابتدا فرض کنید f^{-1} تابع باشد و $f(x_1) = y = f(x_2)$. در این صورت $(x_1, y), (x_2, y) \in f$ و $(y, x_1), (y, x_2) \in f^{-1}$. چون f^{-1} تابع است، $x_1 = x_2$. بنابراین f یک‌به‌یک است.
برعکس فرض کنید f تابع یک‌به‌یک باشد. اگر $(y, x_1), (y, x_2) \in f^{-1}$، آنگاه طبق تعریف داریم $(x_1, y), (x_2, y) \in f$، یعنی $f(x_1) = y = f(x_2)$. چون f یک‌به‌یک است، $x_1 = x_2$. پس f^{-1} تابع است.
حال فرض کنید f یک‌به‌یک باشد. اگر $f^{-1}(y_1) = x = f^{-1}(y_2)$، آنگاه $f(x) = y_1$ و $f(x) = y_2$. چون f تابع است، $y_1 = y_2$. بنابراین f^{-1} یک‌به‌یک است.
اکنون فرض کنید تابع f پوشاست. نشان می‌دهیم f^{-1} نیز پوشاست. اگر $a \in A$، آنگاه $f(a) = b \in B$. پس طبق تعریف، $f^{-1}(b) = a$. در نتیجه f^{-1} پوشاست. به طریق مشابه اگر f^{-1} پوشا باشد نتیجه می‌گیریم که f نیز پوشاست. □

فرض کنید $f : A \longrightarrow B$ و $\emptyset \neq X \subseteq A$. تحدید f با X که با $f|_X$ نشان داده می‌شود عبارت است از

$$f\,|_X = \{(x, f(x)) \mid x \in X\}.$$

پس برای $x \in X$، $(f|_X)(x) = f(x)$. توجه کنید $f|_X$ همان تابع f است جز این که آن را برای دامنه‌ی کوچک‌تر X در نظر گرفته‌ایم.
اگر $g : X \longrightarrow B$ و A مجموعه‌ای شامل X باشد. تابع $f : A \longrightarrow B$ را توسیع g به A می‌نامیم هرگاه $f|_X = g$.
فرض کنید A، B و C مجموعه باشند، $f : A \longrightarrow B$ و $g : B \longrightarrow C$. یادآوری می‌کنیم ترکیب f و g به صورت زیر تعریف می‌شود

$$g \circ f = \{(x, z) \in A \times C \mid \exists y \in B,\ \ (x, y) \in f,\ \ (y, z) \in g\}$$

یا با نمادگذاری متعارف

$$g \circ f = \{(x, z) \in A \times C \mid \exists y \in B,\ \ y = f(x),\ \ z = f(y)\}.$$

فرض کنید $(x, z) \in g \circ f$، یعنی $(g \circ f)(x) = z$. بنا به تعریف ترکیب توابع، $y \in B$ وجود دارد که $f(x) = y$ و $g(y) = z$. پس

$$z = g(y) = g(f(x)).$$

بنابراین $(g \circ f)(x) = g(f(x))$. توجه کنید اگر $f : A \longrightarrow B$ یک‌به‌یک و پوشا باشد، آنگاه طبق قضیه‌ی ۵.۵.۱، $f^{-1} : B \longrightarrow A$ تابع است. پس $y = f(x)$ اگر و تنها اگر $x = f^{-1}(y)$. بنابراین داریم

$$f^{-1}(f(x)) = f^{-1}(y) = x \qquad \text{و} \qquad f(f^{-1}(y)) = f(x) = y,$$

این یعنی $f \circ f^{-1} = \mathrm{id}_B$ و $f^{-1} \circ f = \mathrm{id}_A$. در قضیه‌ی بعدی تعدادی از خواص ترکیب توابع را بررسی می‌کنیم.

قضیه ۶.۵.۱. فرض کنید $f : A \longrightarrow B$ و $g : B \longrightarrow C$. در این صورت
(الف) $g \circ f : A \longrightarrow C$، یعنی $g \circ f$ تابعی از A به C است.
(ب) اگر f و g یک‌به‌یک باشند، آنگاه $g \circ f$ یک‌به‌یک است.
(ج) اگر f و g پوشا باشند، آنگاه $g \circ f$ پوشاست.

اثبات. (الف) فرض کنید $x \in A$. چون f تابع است و $x \in A$، عضو $y \in B$ وجود دارد که $y = f(x)$. حال چون g تابع است و $y \in B$، عضو $z \in C$ وجود دارد که $g(y) = z$. بنابراین $(g \circ f)(x) = g(f(x)) = g(y) = z$، یعنی $(x, z) \in g \circ f$. پس $x \in \mathrm{dom}\,(g \circ f)$. از این‌رو $A \subseteq \mathrm{dom}\,(g \circ f)$. اما $\mathrm{dom}\,(g \circ f) = A$ و بنابراین $g \circ f$ خوش تعریف است. فرض کنید $(x, z) \in g \circ f$ و (x, z_1)، که در آن $x \in A$ و $z, z_1 \in C$. بنا به تعریف ترکیب توابع، اعضای $y_1 \in B$ و y وجود دارند که $y = f(x)$، $z = g(y)$، $y_1 = f(x)$، و $z_1 = g(y_1)$. چون f تابع است، $y = y_1$ و چون g تابع است، $z = z_1$. پس $g \circ f$ خوش تعریف است.

(ب) فرض کنید $x_۱, x_۲ \in A$ و $(g \circ f)(x_۱) = (g \circ f)(x_۲)$. بنابراین، طبق تعریف، داریم $g(f(x_۱)) = g(f(x_۲))$. چون g یک‌به‌یک است، $f(x_۱) = f(x_۲)$. چون f یک‌به‌یک است، $x_۱ = x_۲$. از این‌رو $g \circ f$ یک‌به‌یک است.
(ج) فرض کنید $z \in C$. چون g پوشاست، عضو $y \in B$ وجود دارد که $z = g(y)$. اکنون چون f پوشاست عضو $x \in A$ وجود دارد که $y = f(x)$. بنابراین

$$(g \circ f)(x) = g(f(x)) = g(y) = z$$

و $g \circ f$ پوشاست. □

قضیه ۷.۵.۱. فرض کنید $f : A \longrightarrow B$، $g : B \longrightarrow C$، و $h : C \longrightarrow D$. در این صورت $h \circ (g \circ f) = (h \circ g) \circ f$، یعنی ترکیب توابع شرکت‌پذیر است.

اثبات. ابتدا توجه کنید که $h \circ (g \circ f) : A \longrightarrow D$ و $(h \circ g) \circ f : A \longrightarrow D$. برای هر $x \in A$، داریم

$$\begin{aligned} [h \circ (g \circ f)](x) &= h((g \circ f))(x) \\ &= h(g(f(x))) \\ &= (h \circ g)(f(x)) \\ &= [(h \circ g) \circ f](x). \end{aligned}$$

پس $h \circ (g \circ f) = (h \circ g) \circ f$. □

فرض کنید A و B مجموعه باشند. A و B را هم‌توان (یا هم‌عدد) گوییم و می‌نویسیم $A \approx B$، هرگاه تابع یک‌به‌یک و پوشا از A به B وجود داشته باشد، یعنی عناصر A و B در تناظر یک‌به‌یک باشند.

مثال ۸.۵.۱. اگر $A = \{x \in \mathbb{R} \mid -۱ < x < ۱\}$، آنگاه $A \approx \mathbb{R}$.

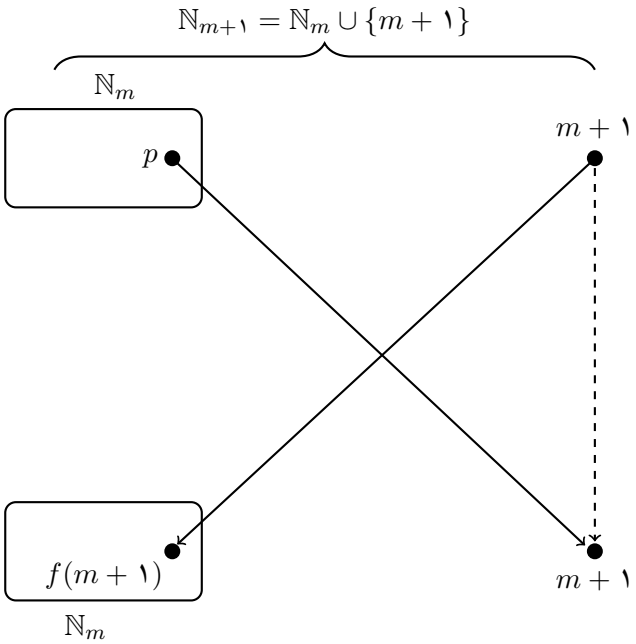
حل تابع $f : A \longrightarrow \mathbb{R}$ با ضابطه‌ی $f(x) = \tan^{-۱}\left(\pi \frac{x}{۲}\right)$ یک تابع یک‌به‌یک و پوشاست. پس $A \approx \mathbb{R}$. □

برای هر k مجموعه‌ی $\mathbb{N}_k$ را برابر مجموعه‌ی اولین k عدد طبیعی تعریف می‌کنیم، یعنی $\mathbb{N}_k = \{۱, ۲, ۳, \ldots, k\}$. مجموعه‌ی A را متناهی گوییم هرگاه به ازای kای با $\mathbb{N}_k$ هم‌توان باشد. در این حالت گوییم A، k عضو دارد و می‌نویسیم $|A| = k$. اگر $f : \mathbb{N}_k \longrightarrow A$ یک‌به‌یک و پوشا باشد، آنگاه $A = \{a_۱, \ldots, a_k\}$ که در آن $a_i = f(i)$. A را نامتناهی گوییم هرگاه A متناهی نباشد. آیا $|A|$ عدد منحصر به فرد است؟ آیا $|A|$ را می‌توان برای مجموعه‌های نامتناهی نیز تعریف کرد؟ جواب هر دو سوال مثبت است. در ادامه به این سوال‌ها پاسخ می‌دهیم. ابتدا به قضیه‌ی نیاز داریم که به اصل لانه کبوتری معروف است. به زبان عامیانه این اصل می‌گوید اگر m کبوتر در کمتر از m لانه کبوتر قرار داده شوند، آنگاه در بعضی از لانه کبوترها باید بیش از یک کبوتر باشد.

قضیه ۹.۵.۱. (اصل لانه کبوتری) فرض کنید m عدد طبیعی باشد. در این صورت به ازای هر $k < m$، $\mathbb{N}_m$ با $\mathbb{N}_k$ هم‌توان نیست.

اثبات. فرض کنید f تابعی یک‌به‌یک از مجموعه‌ی $\mathbb{N}_m$ به مجموعه‌ی $\mathbb{N}_m$ باشد. نشان می‌دهیم $\operatorname{ran} f$ برابر تمام مجموعه‌ی $\mathbb{N}_m$ است (و زیرمجموعه‌ی سره‌ای از $\mathbb{N}_m$ نیست). این کار برای اثبات قضیه کافی است. از استقرا روی m استفاده می‌کنیم. اگر $m = ۱$، آنگاه تنها یک تابع از $\{۱\} = \mathbb{N}_۱$ به $\mathbb{N}_۱$ وجود دارد ، که یک‌به‌یک و پوشا نیز هست. فرض کنید حکم برای m درست باشد و تابع یک‌به‌یک $f : \mathbb{N}_{m+۱} \longrightarrow \mathbb{N}_{m+۱}$ را در نظر بگیرید. باید ثابت کنیم $\operatorname{ran} f = \mathbb{N}_{m+۱}$. تابع تحدید $f|_{\mathbb{N}_m} : \mathbb{N}_m \longrightarrow \mathbb{N}_{m+۱}$ یک‌به‌یک است. دو حالت رخ می‌دهد.
حالت اول : $m + ۱ \notin \operatorname{ran}(f|_{\mathbb{N}_m})$، یعنی $\operatorname{ran}(f|_{\mathbb{N}_m}) \subseteq \mathbb{N}_m$. در این حالت طبق فرض استقرا $\operatorname{ran} f|_{\mathbb{N}_m} = \mathbb{N}_m$. به علاوه چون f یک‌به‌یک است تنها مقدار ممکن برای $f(m + ۱)$ عدد $m + ۱$ است. بنابراین

$$\operatorname{ran} f = \mathbb{N}_m \cup \{m + ۱\} = \mathbb{N}_{m+۱}.$$



شکل ۴.۱: با تعویض دو مقدار f، $\hat{f}$ به دست می‌آید.

حالت دوم : $m+1 \in \operatorname{ran}(f|_{\mathbb{N}_m})$. در این حالت عدد $p \leq m$ وجود دارد که $f(p) = m+1$. اکنون تابع $\hat{f} : \mathbb{N}_{m+1} \longrightarrow \mathbb{N}_{m+1}$ را به صورت زیر تعریف می‌کنیم:

$$\begin{aligned} \hat{f}(p) &= f(m+1) \\ \hat{f}(m+1) &= f(p) \\ \hat{f}(x) &= f(x) \quad \forall x \in \mathbb{N}_{m+1} - \{p, m+1\} \end{aligned}$$

(شکل ۴.۱ را ببینید)
در واقع دو مقدار f را تغییر می‌دهیم تا از حالت اول برای تابع جدید استفاده کنیم. $\hat{f}$ تابعی یک‌به‌یک است و $\operatorname{ran}(\hat{f}|_{\mathbb{N}_m}) \subseteq \mathbb{N}_m$. پس طبق حالت اول $\operatorname{ran}\hat{f} = \mathbb{N}_{m+1}$. اما $\operatorname{ran} f = \operatorname{ran}\hat{f} = \mathbb{N}_{m+1}$.
بنابراین در هر حالت ، $\operatorname{ran} f = \mathbb{N}_{m+1}$. □

نتیجه ۱۰.۵.۱. هیچ مجموعه‌ی متناهی با زیرمجموعه‌ی سره‌ای از خودش هم‌توان نیست.

اثبات. فرض کنید برخلاف حکم تابع یک‌به‌یک و پوشای f بین A و زیرمجموعه‌ی سره از A وجود داشته باشد. تابع مرکب $g \circ f \circ g^{-1}$ را در نظر بگیرید. این تابع مرکب $\mathbb{N}_m$ را به $\mathbb{N}_m$ تصویر می‌کند و بنا به قضیه‌ی ۶.۵.۱، یک‌به‌یک است. به علاوه برد آن زیر مجموعه‌ای سره از $\mathbb{N}_m$ چون C است. (اگر $a \in A - \operatorname{ran} f$، آنگاه $g(a) \in \mathbb{N}_m - C$.) بنابراین $\mathbb{N}_m$ با C هم‌توان است، که این با اصل لانه کبوتری در تناقض است. □

نتیجه ۱۱.۵.۱. (الف) هر مجموعه‌ای که با زیرمجموعه‌ی سره‌ای از خودش هم‌توان باشد نامتناهی است.
(ب) مجموعه‌ی $\mathbb{N}$ نامتناهی است.

اثبات. قسمت (الف) در نتیجه قبل ثابت شد.
قسمت (ب) بلافاصله از قسمت (الف) نتیجه می‌شود، زیرا تابع $f : \mathbb{N} \longrightarrow \mathbb{N} - \{1\}$ با ضابطه‌ی $f(n) = n+1$ یک‌به‌یک و پوشاست. □

نتیجه ۱۲.۵.۱. هر مجموعه‌ی متناهی A به ازای یک عدد منحصر به فرد طبیعی k با $\mathbb{N}_k$ هم‌توان است.

اثبات. فرض کنید به ازای اعداد طبیعی m و k، $A \approx \mathbb{N}_m$ و $A \approx \mathbb{N}_k$. در این صورت داریم $\mathbb{N}_m \approx \mathbb{N}_k$، یعنی $m = k$. □

به ازای مجموعه‌ی متناهی A، عدد منحصر به فرد $k \in \mathbb{N}$ که $A \approx \mathbb{N}_k$ را عدد اصلی A گوییم و آن را به طور مختصر با $|A|$ نشان می‌دهیم. به عنوان مثال، به ازای هر $k \in \mathbb{N}$، $|\mathbb{N}_k| = k$ و اگر a، b، c، و d همگی اشیای متمایز باشند، آنگاه $|\{a, b, c, d\}| = ۴$، زیرا $\{a, b, c, d\} \approx \mathbb{N}_۴$.

در مورد عدد اصلی مجموعه‌های نامتناهی چه می‌توان گفت؟ عدد $|A|$، تعداد اعضای مجموعه‌ی متناهی A را اندازه می‌گیرد. "اعداد" را می‌خواهیم که به طور مشابه تعداد اعضای مجموعه‌های نامتناهی را اندازه‌گیری کند. این کار را با استفاده از قضیه‌ی زیر انجام می‌دهیم.

قضیه ۱۳.۵.۱. رابطه‌ی هم‌توانی $\approx$ رابطه‌ی هم‌ارزی روی رده‌ی همه‌ی مجموعه‌هاست.

اثبات. به ازای هر مجموعه‌ی A تابع همانی $\mathrm{id}_A : A \longrightarrow A$ یک‌به‌یک و پوشاست. پس $A \approx A$ و $\approx$ بازتابی است. حال اگر $A \approx B$، تابع یک‌به‌یک و پوشای $f : A \longrightarrow B$ وجود دارد. بنا به قضیه‌ی ۵.۵.۱، $f^{-۱} : B \longrightarrow A$ یک‌به‌یک و پوشاست. بنابراین $B \approx A$ و $\approx$ متقارن است. در نهایت اگر $A \approx B$ و $B \approx C$، توابع یک‌به‌یک و پوشای $f : A \longrightarrow B$ و $g : B \longrightarrow C$ وجود دارند. بنا به قضیه‌ی ۶.۵.۱، تابع $g \circ f : A \longrightarrow C$ یک‌به‌یک و پوشاست. پس $A \approx C$ و $\approx$ ترایا است. □

فرض کنید A مجموعه باشد. رده‌ی هم‌ارزی شامل A را عدد اصلی A گوییم و با $|A|$ نشان می‌دهیم. بنابراین $A \approx B$ اگر و تنها اگر $|A| = |B|$. به ازای هر عدد صحیح $k \geq ۰$، عدد k را با عدد اصلی آن یکی در نظر می‌گیریم و قرار می‌دهیم $|\mathbb{N}_k| = k$. عدد اصلی مجموعه‌های متناهی همگی اعداد طبیعی هستند. مجموعه‌ی اعداد طبیعی $\mathbb{N}$ متناهی نیست. عدد اصلی $\mathbb{N}$ را با

$$|\mathbb{N}| = \aleph_۰$$

نشان می‌دهیم، نامی که اولین بار کانتور به آن داد. نماد $\aleph$ اولین حرف الفبای عبری، "الف"، است. در حالت کلی، برای عدد اصلی λ، مجموعه‌های زیادی مثل A وجود دارند که $|A| = \lambda$ ($\lambda = ۰$ یک حالت استثنایی است.) در واقع، به ازای هر عدد اصلی ناصفر λ، رده‌ی

$$\mathbf{K}_\lambda = \{X \mid |X| = \lambda\}$$

متشکل از مجموعه‌های با عدد اصلی λ به قدری بزرگ است که نمی‌تواند یک مجموعه باشد (تمرین ۱۵). مجموعه‌هایی که عدد اصلی آن‌ها λ است خیلی شبیه‌اند، اعضای چنین دو مجموعه‌ای ممکن است متفاوت باشند اما تعداد اعضای آن‌ها همواره برابر λ است. به ویژه اگر X مجموعه‌ی متناهی با عدد اصلی λ باشد، آنگاه همه‌ی اعضای رده‌ی فوق نیز متناهی هستند؛ در این حالت λ یک عدد اصلی متناهی است. در غیر این صورت λ یک عدد اصلی نامتناهی است. بنابراین اعداد اصلی متناهی دقیقاً اعداد طبیعی هستند. $\aleph_۰$ یک عدد اصلی نامتناهی است، هم‌چنین $|\mathbb{R}|$، $|\mathscr{P}(\mathbb{R})|$، و غیره نیز نامتناهی‌اند.

تعریف ۱۴.۵.۱. فرض کنید $f : A \longrightarrow B$

(الف) f را از چپ وارون‌پذیر گوییم هرگاه تابع $g : B \longrightarrow A$ وجود داشته باشد که $g \circ f = \mathrm{id}_A$. تابع g را وارون چپ f گوییم.

(ب) f را از راست وارون‌پذیر گوییم هرگاه تابع $h : B \longrightarrow A$ وجود داشته باشد که $f \circ h = \mathrm{id}_B$. تابع h را وارون راست f گوییم.

تابع f را وارون‌پذیر گوییم هرگاه هم وارون چپ و هم وارون راست داشته باشد. قضیه‌ی بعدی برای تعیین این که f وارون چپ یا راست دارد یا وارون‌ناپذیر است مفید است.

قضیه ۱۵.۵.۱. فرض کنید $f : A \longrightarrow B$. در این صورت

(الف) f یک‌به‌یک است اگر و تنها اگر f از چپ وارون‌پذیر باشد.

(ب) f پوشاست اگر و تنها اگر f از راست وارون‌پذیر باشد.

(ج) f یک‌به‌یک و پوشاست اگر و تنها اگر f وارون‌پذیر باشد.

اثبات. (الف) ($\Longrightarrow$) فرض کنید f وارون چپ داشته باشد. تابع $g : B \longrightarrow A$ وجود دارد که $g \circ f = \mathrm{id}_A$.

برای اثبات یک‌به‌یک بودن f فرض کنید $x, y \in A$ طوری باشند که $f(x) = f(y)$. در این صورت $g(f(x)) = g(f(y))$، یعنی $(g \circ f)(x) = (g \circ f)(y)$. در نتیجه $\mathrm{id}_A(x) = \mathrm{id}_A(y)$، یعنی $x = y$. بنابراین f یک‌به‌یک است.

($\Longleftarrow$) فرض کنید f یک‌به‌یک باشد. پس برای هر $y \in B$ یا $y \notin \operatorname{ran} f$ (یعنی y پیش تصویر ندارد) یا $y \in \operatorname{ran} f$، در این حالت عضو یکتای $x_y \in A$ وجود دارد که $f(x_y) = y$. عضو دلخواه $a \in A$ را ثابت در نظر گرفته و به ازای هر $y \in B$ تعریف می‌کنیم

$$g(y) = \begin{cases} a & y \notin \operatorname{ran} f \\ x_y & y \in \operatorname{ran} f, \quad f(x_y) = y \end{cases}$$

در واقع چون f یک‌به‌یک است، f^{-1} تابع است. اما دامنه‌ی f^{-1} ممکن است کوچک‌تر از B باشد. بنابراین برای این که وارون چپ را روی همه‌ی B تعریف کنیم روی $\operatorname{ran} f$، g را برابر f^{-1} و بیرون از $\operatorname{ran} f$، g را مقدار ثابت a تعریف می‌کنیم. بنا به تعریف g، $\operatorname{dom} g = B$. برای اثبات خوش‌تعریفی g، عناصر $y_1, y_2 \in B$ را در نظر بگیرید که $y_1 = y_2$. آن‌گاه $y_1 = y_2$ یا در $\operatorname{ran} f$ نیست یا در $\operatorname{ran} f$ هست، که در این حالت اعضای یکتای $x_{y_1}, x_{y_2} \in A$ وجود دارند که $f(x_{y_1}) = y_1$ و $f(x_{y_2}) = y_2$. فرض کنید $y_1 = y_2 \notin \operatorname{ran} f$. در این صورت $g(y_1) = a = g(y_2)$. حال فرض کنید اعضای یکتای $x_{y_1}, x_{y_2} \in A$ وجود دارند که $f(x_{y_1}) = y_1$ و $f(x_{y_2}) = y_2$. پس $g(y_1) = x_{y_1}$ و $g(y_2) = x_{y_2}$. چون $y_1 = y_2$ داریم $f(x_{y_1}) = f(x_{y_2})$. چون f یک‌به‌یک است، $x_{y_1} = x_{y_2}$ و بنا بر این $g(y_1) = g(y_2)$. این یعنی g خوش تعریف است. حال نشان می‌دهیم $g \circ f = \mathrm{id}_A$. فرض کنید $u \in A$ و به ازای یک $v \in B$، $f(u) = v$. بنا به تعریف g، $g(v) = u$. بنابراین

$$(g \circ f)(u) = g(f(u)) = g(v) = u = \mathrm{id}_A(u).$$

پس $g \circ f = \mathrm{id}_A$.

(ب) ($\Longrightarrow$) فرض کنید f از راست وارون‌پذیر باشد. پس تابع $g : B \longrightarrow A$ وجود دارد که $f \circ g = \mathrm{id}_B$. فرض کنید $y \in B$. قرار می‌دهیم $x = g(y) \in A$. داریم

$$y = \mathrm{id}_B(y) = (f \circ g)(y) = f(g(y)) = f(x),$$

یعنی f پوشاست.

($\Longleftarrow$) برعکس فرض کنید f پوشاست. اگر $y \in B$ عضو $x \in A$ وجود دارد که $f(x) = y$. قرار می‌دهیم $A_y = \{x \in A \mid f(x) = y\}$. بنابراین $A_y \neq \emptyset$. به ازای هر $y \in B$ عضو $x_y \in A_y$ را انتخاب می‌کنیم. تابع $h : B \longrightarrow A$ را با $h(y) = x_y$، به ازای هر $y \in B$، تعریف می‌کنیم. فرض کنید $y \in B$، در این صورت

$$(f \circ h)(y) = f(h(y)) = f(x_y) = y = \mathrm{id}_B(y).$$

بنابراین $f \circ h = \mathrm{id}_B$ و f از راست وارون‌پذیر است.

(ج) مطلب از (الف) و (ب) حاصل می‌شود. □

فرض کنید $f : A \longrightarrow B$ وارون‌پذیر باشد. فرض کنید g وارون چپ f و h وارون راست f باشند. در این صورت $g \circ f = \mathrm{id}_A$ و $f \circ h = \mathrm{id}_B$. داریم

$$g = g \circ \mathrm{id}_B = g \circ (f \circ h) = (g \circ f) \circ h = \mathrm{id}_A \circ h = h.$$

بنابراین اگر f وارون‌پذیر باشد، آن‌گاه وارون چپ و راست آن یکی هستند. این مطلب هم‌چنین ثابت می‌کند وارون f در صورت وجود یکتاست و همان f^{-1} است.

در اثبات قسمت (ب) قضیه‌ی فوق گفته شد که چون $A_y \neq \emptyset$، به ازای هر $y \in B$ عضو $x_y \in A_y$ را انتخاب می‌کنیم. این نحوه‌ی انتخاب به چه صورت است؟ چون هیچ‌گونه وجه تمایزی بین اعضای A_y وجود ندارد و A_y و تعداد آن‌ها ممکن است نامتناهی باشند در این‌جا برای انتخاب x_y مشکل داریم. اما این مشکل با استفاده از اصل موضوع انتخاب، که یکی از اصول مهم نظریه‌ی مجموعه‌ها است، برطرف می‌شود. یکی از صورت‌های اصل موضوع انتخاب عبارت است از:

به ازای هر رابطه‌ی R، یک تابع $h \subseteq R$ وجود دارد که $\operatorname{dom} h = \operatorname{dom} R$.

حال می‌توان با استفاده از اصل موضوع انتخاب اثبات قضیه را پیگیری کرد. به ازای $R = f^{-1}$، طبق اصل موضوع انتخاب تابع $g \subseteq f^{-1}$ وجود دارد که $\operatorname{dom} g = \operatorname{dom} f^{-1}$. پس $g \circ f = \mathrm{id}_A$.

در مورد این اصل پس از تعریف حاصل‌ضرب دکارتی نامتناهی به طور مفصل بحث می‌کنیم. اکنون تعریف حاصل‌ضرب دکارتی را به خانواده‌ی دلخواه $\{A_\alpha \mid \alpha \in I\}$، که در آن I یک مجموعه‌ی اندیس است، تعمیم می‌دهیم. ابتدا فرض کنید $I = \{۱, ۲\}$ و

$$S = \{f \mid f : I \to A \cup B,\ \ f(۱) \in A,\ \ f(۲) \in B\}.$$

بنابراین هر تابع $f \in S$ زوج مرتب $(f(۱), f(۲)) \in A \times B$ را تعریف می‌کند. برعکس اگر $x \in A$ و $y \in B$ داده شده باشد تابع $f \in S$ را با $f(۱) = x$ و $f(۲) = y$ تعریف می‌کنیم. در این صورت زوج مرتب (x, y) یک تابع $f \in S$ را تعریف می‌کنند. بنابراین یک تناظر یک‌به‌یک بین عناصر S و $A \times B$ وجود دارد. با الهام از این واقعیت، حاصل‌ضرب دکارتی $\{A_\alpha \mid \alpha \in I\}$ را تعریف می‌کنیم. حاصل‌ضرب دکارتی خانواده‌ی $\{A_\alpha \mid \alpha \in I\}$ از مجموعه‌ها را که با $\prod_{\alpha\in I} A_\alpha$ نشان می‌دهیم، برابر مجموعه‌ی

$$\{f \mid f : I \to \bigcup_{\alpha\in I} A_\alpha,\quad f(\alpha) \in A_\alpha,\quad \forall \alpha \in I\}$$

تعریف می‌کنیم. فرض کنید $f \in \prod_{\alpha\in I} A_\alpha$. در این صورت به ازای هر $\alpha \in I$، $f(\alpha) \in A_\alpha$. به ازای هر $\alpha \in I$، قرار می‌دهیم $x_\alpha = f(\alpha)$. معمولاً از $(x_\alpha)_{\alpha\in I}$ به جای f استفاده می‌کنیم، یعنی یک عضو نوعی از $\prod_{\alpha\in I} A_\alpha$ را با $(x_\alpha)_{\alpha\in I}$ نشان می‌دهیم که در آن $x_\alpha \in A_\alpha$، به ازای هر $\alpha \in I$. $(x_\alpha)_{\alpha\in I}$ را یک دنباله با اندیس I یا به طور ساده یک دنباله می‌نامیم. فرض کنید $I = \{۱, ۲, \ldots, n\}$ مجموعه‌ای متناهی باشد. در این صورت حاصل‌ضرب دکارتی $\prod_{\alpha\in I} A_\alpha$ را با

$$A_۱ \times A_۲ \times \cdots \times A_n$$

نشان می‌دهیم. یک عضو نوعی از $A_۱ \times A_۲ \times \cdots \times A_n$ را با $(x_۱, x_۲, \ldots, x_n)$ نشان می‌دهیم که در آن $x_i \in A$، $i = ۱, ۲, \ldots, n$. عناصر $A_۱ \times A_۲ \times \cdots \times A_n$ را n- تایی‌های مرتب می‌نامیم. برای دو n- تایی $(x_۱, x_۲, \ldots, x_n) = (y_۱, y_۲, \ldots, y_n)$، داریم $(x_۱, x_۲, \ldots, x_n), (y_۱, y_۲, \ldots, y_n) \in A_۱ \times \cdots \times A_n$ اگر و تنها اگر به ازای هر i، $x_i = y_i$.

سوالی که مطرح می‌شود این است که اگر $\{A_\alpha\}_{\alpha\in I}$ خانواده‌ای نامتناهی از مجموعه‌ها باشد آیا $\prod_{\alpha\in I} A_\alpha \neq \emptyset$؟ یعنی آیا به ازای هر $\alpha \in I$، می‌توان عضوی مثل x_α را انتخاب کرد و در نهایت عضو $(x_\alpha)_{\alpha\in I}$ در $\prod_{\alpha\in I} A_\alpha$ را به دست آورد؟ پاسخ این مطلب اصل انتخاب است که در بالا نیز اشاره شد. اصل موضوع انتخاب یکی از اصوا مهم نظریه‌ی مجموعه‌ها است و صورت‌های معادل زیادی دارد. یکی از صورت‌های معادل این اصل که قبلاً گفته شد عبارت است از: به ازای هر رابطه‌ی R، یک تابع $f \subseteq R$ وجود دارد که $\operatorname{dom} f = \operatorname{dom} R$. صورت معادل دیگر از اصل موضوع انتخاب عبارت است از :

حاصل‌ضرب دکارتی مجموعه‌های ناتهی همواره ناتهی است. یعنی، اگر $\{A_\alpha\}_{\alpha\in I}$ خانواده‌ای نامتناهی از مجموعه‌ها باشد، تابع f با دامنه‌ی I وجود دارد که به ازای هر $\alpha \in I$، $f(\alpha) \in A_\alpha$.

لم زُرن نیز که قبلاً بیان شد یک از صورت های معادل اصل انتخاب است. به دلایل تاریخی اصل موضوع انتخاب وضعیتی بی‌مانند دارد. در ابتدا تعدادی از ریاضی‌دانان این اصل موضوع را رد می‌کردند. چون این اصل موضوع وجود یک مجموعه را بدون این که مشخص کند دقیقاً چه چیزی در آن است ادعا می‌کرد. تا این حد این اصل موضوع نسبت به سایر اصول کمتر "ساختنی" است. به تدریج این اصل موضوع شگفت‌انگیز مورد قبول واقع شد (حداقل اغلب ریاضی‌دانانی که متمایل به پذیرش منطق کلاسیک بودند آن را پذیرفتند). اما این اصل موضوع تصویری تیره را از روزهایی که کاملاً پذیرفته نشده بود یدک می‌کشد. بنابراین هر وقت از اصل موضوع انتخاب استفاده می‌شود، متداول است که به طور صریح نامی از آن آورده شود (چنین اقدامی را در باره سایر اصول موضوع که به نحوی مورد گسترده مورد استفاده قرار می‌گیرند ولی به‌ندرت ذکری از آن‌ها می‌شود، روا نمی‌دارند). بدون استفاده از اصل موضوع انتخاب، هنوز می‌توانیم ثابت کنیم که به ازای یک مجموعه‌ی متناهی I، اگر به ازای هر $\alpha \in I$، $A_\alpha \neq \emptyset$، آنگاه یک تابع f با دامنه‌ی I وجود دارد که به ازای هر $\alpha \in I$، $f(\alpha) \in A_\alpha$. اما برای یک مجموعه‌ی نامتناهی I، اصل موضوع انتخاب لازم است (اگر هفت انتخاب داشته باشیم، می‌توانیم صریحاً به هر کدام اشاره کنیم؛ اما برای $\aleph_۰$ انتخاب این کار ممکن نیست). به ویژه اگر یک چیز انتخاب کنیم، نیازی به اصل موضوع انتخاب نداریم (این را تذکر می‌دهیم به خاطر این که بعضی اشخاص به محض شنیدن نام اصل موضوع انتخاب واکنش منفی نشان می‌دادند.) برای مثال، فرض کنید $A \neq \emptyset$. پس $y_۰$ی در A وجود دارد ؛ می‌توان از $y_۰$ برای بحث‌های بیشتر استفاده کرد (برای نشان دادن این که، مثلاً یک زیرمجموعه‌ی تک

عضوی $\{y_0\}$ از A وجود دارد.) از اصل موضوع انتخاب در این مورد استفاده نمی‌شود، حتی اگر عبارت به صورت "می‌توان یک عضو ثابت y_0 در A انتخاب کرد" بیان شود. به عنوان دومین مثال، فرض کنید، R رابطه‌ای باشد که به ازای هر x در دامنه‌ی R، y_0ی وجود دارد که xRy_0. می‌توان نتیجه گرفت که به ازای هر x در $\operatorname{dom} R$ یک مجموعه‌ی تک عضوی $\{y_0\}$ مشمول در $\{t \mid xRt\}$ وجود دارد هنوز از اصل موضوع انتخاب استفاده نکرده‌ایم. چیزی که اصل موضوع انتخاب برای آن لازم است این است که بگوییم، به ازای هر x در $\operatorname{dom} R$ یک y_x وجود دارد که xRy_x، و سپس همه‌ی این y_xها را در یک مجموعه قرار می‌دهیم، مثلاً،

$$\{y_x \mid x \in \operatorname{dom} R\}.$$

این کار در عمل انتخاب‌های زیادی را باعث می‌شود: به ازای هر x در $\operatorname{dom} R$، که ممکن است مجموعه‌ای نامتناهی باشد (یک انسان نمیتواند تعدادی نامتناهی عمل را انجام دهد. اما اصل موضوع انتخاب بیان می‌کند که علی‌رغم محدودیت‌های عملی، یک مجموعه که با تعداد نامتناهی انتخاب، در تئوری، ساخته می‌شود وجود دارد.) وضعیت دیگری که می‌توان از اصل موضوع انتخاب اجتناب کرد وقتی است که دقیقاً معین کنیم چه اشیائی را می‌خواهیم انتخاب کنیم. مثلاً، می‌توان بدون استفاده از اصل موضوع انتخاب نشان داد، یک تابع از مجموعه‌ی همه‌ی زیرمجموعه‌های ناتهی $\mathbb{N}$ به $\mathbb{N}$ وجود دارد. یعنی ، تابع $f : \mathscr{P}(\mathbb{N}) - \{\emptyset\} \longrightarrow \mathbb{N}$ را برای هر $\emptyset \neq A \subseteq \mathbb{N}$ با ضابطه‌ی

$$f(A) = A \text{ کوچک‌ترین عضو}$$

تعریف می‌کنیم. نکته مهم در این‌جا این است که می‌توانیم عبارتی بنویسیم که عضو انتخابی A را تعریف کند. اگر مثلاً جای $\mathbb{N}$ را با $\mathbb{R}$ عوض کنیم، هیچ امکانی برای تعریف روشی که اعداد را از زیرمجموعه‌های ناتهی و دلخواه $\mathbb{R}$ انتخاب کند وجود ندارد. مثال زیر منسوب به راسل است: اگر $\aleph_0$ جفت کفش داشته باشیم، می‌توانیم از هر جفت یک لنگه کفش را بدون استفاده از اصل موضوع انتخاب برگزینیم. به سادگی می‌توان مثلاً کفش پای چپ را از هر زوج انتخاب کرد. اما اگر $\aleph_0$ جفت جوراب داشته باشیم برای برگزیدن یک لنگه جوراب از هر جفت باید از اصل موضوع انتخاب استفاده کنیم. زیرا تفاوت معینی بین دو لنگه جوراب در هر جفت نیست.

این بخش را با بررسی مختصر مفهوم مجموعه‌های شمارا به پایان می‌بریم. مجموعه‌ی A شمارا گوییم هرگاه یا متناهی یا با $\mathbb{N}$ هم‌توان باشد. در غیر این صورت A را ناشمارا گوییم. بنابراین اگر مجموعه‌ی A شمارا باشد، آنگاه یا $A = \{a_1, a_2, \ldots, a_k\}$ یا $A = \{a_1, a_2, \ldots\}$. برای مثال مجموعه‌ی اعداد طبیعی $\mathbb{N}$، مجموعه‌ی اعداد صحیح $\mathbb{Z}$، و مجموعه‌ی اعداد گویا $\mathbb{Q}$ همگی مجموعه‌های شمارای نامتناهی هستند. اما مجموعه‌ی اعداد حقیقی $\mathbb{R}$ ناشمارا است. به وضوح هر زیرمجموعه‌ی یک مجموعه‌ی شمارا، شمارا است؛ و اگر A و B مجموعه‌های شمارا باشند، آنگاه $A \cup B$ و $A \times B$ شمارا هستند. از طرف دیگر به ازای هر مجموعه‌ی نامتناهی A مجموعه‌ی زیرمجموعه‌های A، یعنی $\mathscr{P}(A)$، ناشمارا است. جزئیات اثبات قضیه‌ی بعدی را به عنوان تمرین واگذار می‌کنیم.

قضیه ۱.۵.۱۶. اجتماع شمارا از مجموعه‌های شمارا، شمارا است؛ یعنی اگر به ازای هر $n \in \mathbb{N}$، A_n مجموعه‌ای شمارا باشد، آنگاه $\bigcup_{i=1}^{\infty} A_n$ شمارا است.

اثبات. به ازای هر $n \in \mathbb{N}$، A_n مجموعه‌ای شمارا است. بنابراین یا A_n متناهی است و $A_n = \{a_{n1}, a_{n2}, \ldots, a_{nm}\}$؛ یا A_n نامتناهی است و $A_n = \{a_{n1}, a_{n2}, a_{n3}, \ldots\}$. تابع $f : \bigcup_{n=1}^{\infty} A_n \longrightarrow \mathbb{N} \times \mathbb{N}$ با ضابطه‌ی $f(a_{ij}) = (i, j)$ یک تابع یک‌به‌یک است (شکل ۵.۱ را ببینید). چون $\mathbb{N} \times \mathbb{N}$ شمارا است، $\bigcup_{i=1}^{\infty} A_n$ نیز شمارا است. □

تمرین‌ها

۱. اگر $\mathbb{Q}_{pos}$ مجموعه‌ی اعداد گویای مثبت باشد تعیین کنید کدام $f : \mathbb{Q}_{pos} \longrightarrow \mathbb{Q}$ خوش تعریف است:

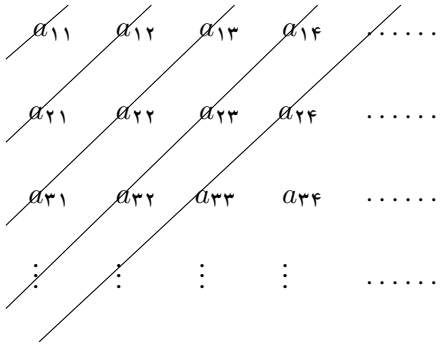
(الف) $f\left(\frac{m}{n}\right) = n$ (ب) $f\left(\frac{m}{n}\right) = \frac{m-n}{m+n}$

(ج) $f\left(\frac{m}{n}\right) = m+n$ (د) $f\left(\frac{m}{n}\right) = \frac{5n+7m}{3m+n}$

۲. برای توابع $f : \mathbb{Z} \longrightarrow \mathbb{Z}$ در زیر،یک وارون چپ و یک وارون راست بیابید (در صورت وجود)

(الف) $f(x) = x+2$ (ب) $f(x) = 2x$

(ج) $f(x) = \begin{cases} x & x \text{ زوج} \\ x+1 & x \text{ فرد} \end{cases}$ (د) $f(x) = \begin{cases} \frac{x}{2} & x \text{ زوج} \\ x & x \text{ فرد} \\ 2x+1 & \end{cases}$



شکل ۵.۱: اجتماع شمارا از مجموعه‌های شمارا، شمارا است.

۳. توابع $f : \mathbb{Q}_{pos} \longrightarrow \mathbb{R}$ و $g : \mathbb{R} \longrightarrow \mathbb{R}$ با ضابطه‌های $f(x) = ۱ + \frac{۱}{x}$، برای هر $x \in \mathbb{Q}_{pos}$، و $g(x) = x + ۱$، برای هر $x \in \mathbb{R}$، مفروضند. $g \circ f$ را بیابید.

۴. فرض کنید $f : A \longrightarrow B$ تابع باشد. رابطه‌ی R را روی A با aRb اگر و تنها اگر $f(a) = f(b)$ تعریف می‌کنیم. نشان دهید R رابطه‌ی هم‌ارزی است.

۵. فرض کنید R رابطه‌ی هم‌ارزی روی مجموعه‌ی A باشد و $f : A \longrightarrow A$. نشان دهید تابع $\bar{f} : A/R \longrightarrow A/R$ وجود دارد که $\bar{f}(\bar{a}) = \overline{f(a)}$ اگر و تنها اگر از $(x, y) \in R$ نتیجه شود $(f(x), f(y)) \in R$.

۶. فرض کنید X و Y مجموعه باشند و $T \subseteq X$. اگر $f : X \longrightarrow Y$، تصویر T تحت f عبارت است از $f(T) = \{f(x) \mid x \in T\}$. فرض کنید $A, B \subseteq X$. نشان دهید :
(الف) $f(A \cup B) = f(A) \cup f(B)$.
(ب) $f(A \cap B) \subseteq f(A) \cap f(B)$.
(ج) اگر f یک‌به‌یک باشد، آنگاه $f(A - B) \subseteq f(A) - f(B)$.

۷. فرض کنید X و Y مجموعه باشند و $f : X \longrightarrow Y$. ثابت کنید f یک‌به‌یک است اگر و تنها اگر برای هر دو زیرمجموعه‌ی ناتهی A و B از X داشته باشیم $f(A \cap B) = f(A) \cap f(B)$.

۸. فرض کنید X و Y مجموعه باشند و $S \subseteq Y$. اگر $f : X \longrightarrow Y$، آنگاه تصویر وارون S تحت f را با $f^{-۱}(S) = \{x \in X \mid f(x) \in S\}$ تعریف می‌کنیم. فرض کنید $A, B \subseteq Y$. نشان دهید
(الف) $f^{-۱}(A \cup B) = f^{-۱}(A) \cup f^{-۱}(B)$.
(ب) $f^{-۱}(A \cap B) = f^{-۱}(A) \cap f^{-۱}(B)$.
(ج) $f^{-۱}(A - B) = f^{-۱}(A) - f^{-۱}(B)$.

۹. (قضیه‌ی شرودر-برنشتاین) فرض کنید A و B مجموعه باشند. اگر به ازای یک زیرمجموعه‌ی Y از B، $A \approx Y$ و به ازای یک زیرمجموعه‌ی X از A، $B \approx X$، ثابت کنید $A \approx B$.

۱۰. نشان دهید تابع $f : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$ با ضابطه‌ی $f(m, n) = ۲^m(۲n + ۱) - ۱$ یک‌به‌یک و پوشاست.

۱۱. نشان دهید مجموعه‌های زیر هم‌توان هستند
(الف) $\mathbb{Z}$، $۲\mathbb{Z}$، $(k\mathbb{Z} = \{kn \mid n \in \mathbb{Z}\})$.
(ب) $۵\mathbb{Z}$، $۷\mathbb{Z}$.
(ج) $\mathbb{Z}$، $\mathbb{Q}$.
(د) $\mathbb{R}_{pos} = \{x \in \mathbb{R} \mid x > ۰\}$، $S = \{x \in \mathbb{R} \mid ۰ < x < ۱\}$.
(هـ) $\mathbb{R}$، $\mathbb{R}_{pos}$.
(و) $A = \{x \in \mathbb{R} \mid ۰ \leq x \leq ۱\}$، $B = \{x \in \mathbb{R} \mid ۶ \leq x \leq ۹\}$.

۱۲. یک تابع یک‌به‌یک و پوشا از فاصله‌ی بسته‌ی $A = \{x \in \mathbb{R} \mid ۰ \leq x \leq ۱\}$ به فاصله‌ی باز $B = \{x \in \mathbb{R} \mid ۰ < x < ۱\}$

بیابید که اعداد گویا را به اعداد گویا و اعداد اصم را به اعداد اصم تصویر کند.

۱۳. نشان دهید $\mathbb{N} \not\approx \mathbb{R}$.

۱۴. به ازای هر مجموعه‌ی X نشان دهید $X \not\approx \mathscr{P}(X)$.

۱۵. فرض کنید λ یک عدد اصلی ناصفر باشد. نشان دهید $\mathbf{K}_\lambda = \{X \mid |X| = \lambda\}$ مجموعه نیست.

۱۶. نشان دهید
(الف) هر زیرمجموعه‌ی یک مجموعه‌ی شمارا، شمارا است.
(ب) اگر A و B مجموعه‌های شمارا باشند، آنگاه $A \cup B$ و $A \times B$ شمارا هستند.
(ج) به ازای هر مجموعه‌ی نامتناهی A مجموعه‌ی زیرمجموعه‌های A، یعنی $\mathscr{P}(A)$، ناشمارا است.

۱۷. (الف) فرض کنید $\mathscr{A}$ گردآیه‌ای از غیر مستدیر غیر متقاطع در صفحه باشد. نشان دهید $\mathscr{A}$ شمارا است.
(ب) فرض کنید $\mathscr{B}$ گردآیه‌ای از دایره‌ها غیر متقاطع در صفحه باشد. آیا لزوماً $\mathscr{B}$ شمارا است؟

۱۸. یک مجموعه‌ی $\mathscr{A}$ از فاصله‌های باز در $\mathbb{R}$ بیابید که هر عدد گویا به یکی از آن فاصله‌ها تعلق داشته باشد، اما $\bigcup \mathscr{A} \neq \mathbb{R}$.

۱۹. فرض کنید A مجموعه‌ای از اعداد حقیقی مثبت باشد. اگر عدد b وجود داشته باشد که مجموع اعضای هر زیرمجموعه‌ی متناهی A از b کمتر باشد، نشان دهید A شمارا است.

۶.۱ عمل دوتایی

مفهوم عمل دوتایی در جبر مجرد بسیار مهم است. در تمامی کتاب مجموعه‌هایی را به همراه یک یا چند عمل دوتایی در نظر می‌گیریم. در اینجا، عمل دوتایی را تعریف و چند خاصیت مهم آن را بررسی می‌کنیم.

تعریف ۱.۶.۱. فرض کنید A مجموعه‌ای ناتهی باشد. یک تابع از $A \times A$ به A را یک عمل دوتایی روی A گوییم.

یک عمل دوتایی به ازای هر زوج مرتب (x, y) از عناصر $x, y \in A$ عضوی از A را نظیر می‌کند. مثلاً، $+$ یک عمل دوتایی روی $\mathbb{Z}$ است که به زوج $(۲, ۳)$ عدد ۵ را نظیر می‌کند. اگر $* : A \times A \longrightarrow A$ یک عمل دوتایی روی مجموعه‌ی A باشد، معمولاً به جای $*(a, b)$ می‌نویسیم $a * b$. چون تصویر $*$ زیرمجموعه‌ی از A است، می‌گوییم A تحت $*$ بسته است. $\mathbb{Z}$ تحت عمل $+$ بسته است، زیرا اگر دو عدد صحیح را با هم جمع کنیم عدد صحیحی به دست خواهیم آورد. چون $۲, ۵ \in \mathbb{N}$ و $-۳ = ۲ - ۵ \notin \mathbb{N}$، می‌بینیم که $-$ (تفریق) عمل دوتایی روی $\mathbb{N}$ نیست. پس $\mathbb{N}$ تحت $-$ بسته نیست.

تعریف ۲.۶.۱. $(n + ۱)$- تایی $(A, *_۱, \ldots, *_n)$ را ساختار جبری می‌نامیم، هرگاه A مجموعه‌ی ناتهی و $*_۱$، $*_۲$،... $*_n$، اعمال دوتایی روی A باشند. A را مجموعه‌ی زمینه‌ی ساختار می‌نامیم.

تعریف ۳.۶.۱. فرض کنید $(A, *)$ یک ساختار جبری باشد.
(الف) $*$ را شرکت‌پذیر گوییم هرگاه به ازای هر $a, b, c \in A$،

$$a * (b * c) = (a * b) * c.$$

(ب) $*$ را تعویض‌پذیر گوییم هرگاه به ازای هر $a, b \in A$،

$$a * b = b * a.$$

(ج) عضو $e \in A$ را عضو همانی یا عضو بی‌اثر گوییم هرگاه به ازای هر $a \in A$،

$$e * a = a * e = a.$$

مثال ۴.۶.۱. ساختار جبری $(\mathbb{Z}, +)$ را در نظر بگیرید. چون جمع اعداد صحیح هم شرکت‌پذیر و هم تعویض‌پذیر است، پس $+$ هم شرکت‌پذیر و هم تعویض‌پذیر است. □

مثال ۵.۶.۱. فرض کنید X مجموعه‌ای ناتهی باشد. فرض کنید A مجموعه‌ی همه‌ی توابع روی X باشد، یعنی

$$A = \{f \mid f : X \longrightarrow X\}.$$

چون ترکیب دو تابع دوباره تابع است، $(A, \circ)$ ساختار جبری است. چون ترکیب توابع شرکت‌پذیر است، $\circ$ شرکت‌پذیر است. □

مثال بعد نشان می‌دهد که یک ساختار جبری ممکن است نه شرکت‌پذیر باشد و نه تعویض‌پذیر.

مثال ۶.۶.۱. ساختار جبری $(\mathbb{Z}, -)$ را در نظر بگیرید، که در آن $-$ نشان دهنده عمل تفریق روی $\mathbb{Z}$ است. آنگاه $۱ - (۳ - ۲) = ۲ - ۳ = ۰ \neq -۲ = (۱ - ۳) - ۲$، یعنی $-$ شرکت‌پذیر نیست. هم‌چنین چون $۳ - ۲ \neq ۲ - ۳$، $-$ تعویض‌پذیر نیز نیست. □

راهی مناسب برای تعریف عمل دوتایی روی یک مجموعه‌ی متناهی A استفاده از یک جدول عمل یا ضرب است. مثلاً فرض کنید $A = \{e, a, b\}$. عمل دوتایی $*$ را روی A با جدول عمل زیر تعریف می‌کنیم

$*$	e	a	b
e	e	a	b
a	a	a	a
b	b	a	a

توجه کنید $e * a = a = a * e$، $e * b = b = b * e$، و $e * e = e = e * e$. پس e عضو همانی $(A, *)$ است. □

قضیه ۷.۶.۱. عضو همانی یک ساختار جبری $(A, *)$ (در صورت وجود) یکتاست.

اثبات. فرض کنید e و $e_۱$ دو همانی برای $(A, *)$ باشند. چون e همانی است، به ازای هر $a \in A$، $a * e = e * a = a$. به ویژه برای $a = e_۱$ داریم

$$e_۱ * e = e * e_۱ = e.$$

اکنون چون $e_۱$ همانی است، به ازای هر $a \in A$، $a * e_۱ = a$. به ویژه برای $a = e$ داریم

$$e * e_۱ = e_۱ * e = e_۱.$$

بنابراین از دو معادله‌ی بالا نتیجه می‌گیریم که $e = e_۱$. □

تمرین‌ها

معین کنید کدامیک، اعمال دوتایی‌اند، شرکت‌پذیری و تعویض‌پذیری، اعمال را بررسی کنید. کدامیک عضو همانی دارند.

۱. $(\mathbb{N}, *)$، که در آن به ازای هر $x, y \in \mathbb{N}$، $x * y = x^y$
۲. $(\mathbb{Z}, *)$، که در آن به ازای هر $x, y \in \mathbb{Z}$، $x * y = x + y + ۱$
۳. $(\mathbb{R}, *)$، که در آن به ازای هر $x, y \in \mathbb{R}$، $x * y = \min\{x, y\}$
۴. $(\mathbb{R}, *)$، که در آن به ازای هر $x, y \in \mathbb{R}$، $x * y = \max\{x, y\}$
۵. $(\mathbb{R}, *)$، که در آن به ازای هر $x, y \in \mathbb{R}$، $x * y = |x| + |y|$

۷.۱ جایگشت‌ها

نظریه‌ی گروه‌های جایگشتی یکی از قدیمی‌ترین شاخه‌های نظریه‌ی گروه‌ها است. منشاء آن به یافتن فرمول‌هایی برای به دست آوردن ریشه‌های چندجمله‌ای‌ها با استفاده از رادیکال‌ها برمی‌گردد. لاگرانژ، رافینی، و کُشی اولین کسانی بودند که با گروه‌های جایگشتی کار کردند. مطالعه‌ی هدف‌مند کُشی از گروه‌های جایگشتی بین سال‌های ۱۸۱۵ تا ۱۸۴۵ را منشاء نظریه‌ی گروه‌های مجرد می‌دانند. بسیاری از نتایج و مفاهیم این بخش به کُشی منسوب است.
مطالعه‌ی گروه‌های جایگشتی را با تعریف این که " یک جایگشت چیست؟" شروع می‌کنیم. فرض کنید X یک مجموعه باشد. هر تابع دوسویی از X به X را یک جایگشت روی X گوییم. مجموعه‌ی همه‌ی جایگشت‌ها روی X را با S_X، یا $\mathrm{Sym}\,(X)$، نشان می‌دهیم. S_X را با عمل ترکیب توابع در نظر می‌گیریم. خواص زیر را داریم.
(الف) ترکیب دو جایگشت روی X مجدداً یک جایگشت روی X است.
(ب) ترکیب توابع شرکت‌پذیر است.
(ج) تابع همانی $\mathrm{id}_X : X \longrightarrow X$ یک جایگشت است.
(د) هر جایگشت روی X وارون پذیر است و وارون آن یک جایگشت روی X است.
اگر $\alpha, \beta \in S_X$ به جای $\alpha \circ \beta$ می‌نویسیم $\alpha\beta$. وقتی می‌گوییم حاصل‌ضرب دو جایگشت، منظور همان ترکیب دو جایگشت است. می‌توان خواص S_X را به طور مجرد توصیف کرد:

تعریف ۱.۷.۱. مجموعه‌ی ناتهی G را به همراه عمل دوتایی $*$ یک گروه می‌نامیم، هرگاه
(الف) به ازای هر $a, b, c \in G$، $(a * b) * c = a * (b * c)$، یعنی عمل $*$ شرکت‌پذیر باشد.
(ب) عضو $e \in G$ وجود داشته باشد که به ازای هر $a \in G$، $a * e = e * a = a$. e را عضو همانی یا عضو بی‌اثر گوییم.
(ج) به ازای هر $a \in G$ عضو $b \in G$ وجود داشته باشد که $a * b = b * a = e$. b را وارون a گوییم.
به علاوه اگر به ازای هر $a, b \in G$ داشته باشیم $a * b = b * a$، گوییم گروه G تعویض‌پذیر (یا آبلی، به افتخار آبلی، ریاضی‌دان نروژی) است. $|G|$ را مرتبه‌ی G می‌نامیم.

بنابراین S_X همراه با عمل ترکیب توابع یک گروه است. در حالتی که $X = \{x_۱, \ldots, x_n\}$ متناهی باشد S_X را با S_n، یا $\mathrm{Sym}(n)$ نشان می‌دهیم و آن را گروه متقارن روی n حرف گوییم. هم‌چنین در این حالت معمولاً به جای نوشتن x_iها از اعداد استفاده می‌کنیم: $X = \{۱, ۲, \ldots, n\}$.

مثال ۲.۷.۱. اگر $|X| \geq ۳$ ثابت کنید گروه S_X ناآبلی است.

حل فرض کنید $a, b, c \in X$ سه عضو متمایز باشند. جایگشت‌های α و β را به صورت زیر تعریف می‌کنیم

$$\alpha(a) = b, \quad \alpha(b) = a, \quad \alpha(x) = x, \ \ \forall x \neq a, b$$
$$\beta(b) = c, \quad \beta(c) = b, \quad \beta(x) = x, \ \ \forall x \neq b, c.$$

پس

$$\beta\alpha(a) = \beta(b) = c, \quad \alpha\beta(a) = \alpha(a) = b$$

و بنابراین $\alpha\beta \neq \beta\alpha$. □

برای این که خواص جایگشت‌ها را راحت‌تر بررسی کنیم ابتدا نمادهایی را معرفی می‌کنیم که با استفاده از آن ها کار با جایگشت‌ها ساده‌تر است. اگر α جایگشتی روی مجموعه‌ی $X_n = \{۱, ۲, \ldots, n\}$ باشد، آن‌گاه

$$\alpha = \{(۱, \alpha(۱)), (۲, \alpha(۲)), \ldots, (n, \alpha(n))\}.$$

(یادآوری می‌کنیم که یک تابع $f : A \longrightarrow A$ زیرمجموعه‌ی از $A \times A$ است.) گاهی اوقات مناسب است که جایگشت را با نماد زیر نشان دهیم

$$\alpha = \begin{pmatrix} ۱ & ۲ & ۳ & \cdots & n \\ \alpha(۱) & \alpha(۲) & \alpha(۳) & \cdots & \alpha(n) \end{pmatrix}.$$

این نماد به کُشی منسوب است و آن را نماد دو سطری می‌نامیم. در سطر اول اعضای X_n را فهرست می‌کنیم و در سطر دوم زیر هر عضو $x \in X_n$، تصویر آن ، یعنی $\alpha(x)$، را می‌نویسیم.

مثال ۳.۷.۱. فرض کنید $n = ۴$ و جایگشت α روی $X_۴$ را با $\alpha(۱) = ۲$، $\alpha(۲) = ۴$، $\alpha(۳) = ۳$، $\alpha(۴) = ۱$، تعریف می‌کنیم. در این صورت با استفاده از نماد دو سطری می‌توان α را به صورت زیر نوشت:

$$\alpha = \begin{pmatrix} ۱ & ۲ & ۳ & ۴ \\ ۲ & ۴ & ۳ & ۱ \end{pmatrix}. \qquad \square$$

فرض کنید $n = ۷$ و

$$\alpha = \begin{pmatrix} ۱ & ۲ & ۳ & ۴ & ۵ & ۶ & ۷ \\ ۱ & ۳ & ۴ & ۶ & ۷ & ۲ & ۵ \end{pmatrix}, \quad \beta = \begin{pmatrix} ۱ & ۲ & ۳ & ۴ & ۵ & ۶ & ۷ \\ ۲ & ۵ & ۳ & ۱ & ۷ & ۶ & ۴ \end{pmatrix}$$

دو جایگشت روی $X_۷$ باشند. $\alpha\beta$ را محاسبه می‌کنیم. بنا به تعریف، به ازای هر $x \in X_۷$، $(\alpha\beta)(x) = \alpha(\beta(x))$. پس

$$(\alpha\beta)(۱) = \alpha(\beta(۱)) = \alpha(۲) = ۳,$$
$$(\alpha\beta)(۲) = \alpha(\beta(۲)) = \alpha(۵) = ۷$$

و غیره. از این روند روشن است که وقتی مثلاً می‌خواهیم $(\alpha\beta)(۱)$ را محاسبه کنیم، با β شروع می‌کنیم و با α تمام می‌کنیم و به صورت زیر می‌خوانیم: ۱ به ۲ می‌رود (تحت β) و ۲ به ۳ می‌رود (تحت α) و بنابراین ۱ به ۳ می‌رود (تحت $\alpha\beta$). این روند را به صورت زیر نشان می‌دهیم:

$$\begin{array}{ll} ۱ \xrightarrow{\beta} ۲ \xrightarrow{\alpha} ۳ & ۱ \xrightarrow{\alpha\beta} ۳ \\ ۲ \xrightarrow{\beta} ۵ \xrightarrow{\alpha} ۷ & ۲ \xrightarrow{\alpha\beta} ۷ \\ ۳ \xrightarrow{\beta} ۳ \xrightarrow{\alpha} ۴ & ۳ \xrightarrow{\alpha\beta} ۴ \\ ۴ \xrightarrow{\beta} ۱ \xrightarrow{\alpha} ۱ & ۴ \xrightarrow{\alpha\beta} ۱ \\ ۵ \xrightarrow{\beta} ۷ \xrightarrow{\alpha} ۵ & ۵ \xrightarrow{\alpha\beta} ۵ \\ ۶ \xrightarrow{\beta} ۶ \xrightarrow{\alpha} ۲ & ۶ \xrightarrow{\alpha\beta} ۲ \\ ۷ \xrightarrow{\beta} ۴ \xrightarrow{\alpha} ۶ & ۷ \xrightarrow{\alpha\beta} ۶. \end{array}$$

پس

$$\alpha\beta = \begin{pmatrix} ۱ & ۲ & ۳ & ۴ & ۵ & ۶ & ۷ \\ ۳ & ۷ & ۴ & ۱ & ۵ & ۲ & ۶ \end{pmatrix}.$$

مثال ۴.۷.۱. فرض کنید $n = ۶$ و α و β دو جایگشت روی $X_۶$ باشند که به صورت زیر تعریف شده‌اند

$$\alpha = \begin{pmatrix} ۱ & ۲ & ۳ & ۴ & ۵ & ۶ \\ ۳ & ۱ & ۴ & ۶ & ۵ & ۲ \end{pmatrix} \quad \text{و} \quad \beta = \begin{pmatrix} ۱ & ۲ & ۳ & ۴ & ۵ & ۶ \\ ۱ & ۳ & ۵ & ۴ & ۲ & ۶ \end{pmatrix}.$$

ابتدا $\alpha\beta$ را محاسبه می‌کنیم. داریم $۳ \xrightarrow{\alpha} ۱ \xrightarrow{\beta} ۱$، یعنی ، $۳ \xrightarrow{\alpha\beta} ۱$. به طریق مشابه $۴ \xrightarrow{\alpha\beta} ۲$، $۵ \xrightarrow{\alpha\beta} ۳$، $۶ \xrightarrow{\alpha\beta} ۴$، $۱ \xrightarrow{\alpha\beta} ۵$، $۲ \xrightarrow{\alpha\beta} ۶$. پس

$$\alpha\beta = \begin{pmatrix} ۱ & ۲ & ۳ & ۴ & ۵ & ۶ \\ ۳ & ۴ & ۵ & ۶ & ۱ & ۲ \end{pmatrix}.$$

به طریق مشابه برای $\beta\alpha$؛ ۵ $\xrightarrow{\beta}$ ۳ $\xrightarrow{\alpha}$ ۱، یعنی ، ۵ $\xrightarrow{\beta\alpha}$ ۱ و غیره در این حالت با α شروع و با β تمام می‌کنیم. توجه کنید که

$$\beta\alpha = \begin{pmatrix} ۱ & ۲ & ۳ & ۴ & ۵ & ۶ \\ ۵ & ۱ & ۴ & ۶ & ۲ & ۳ \end{pmatrix}.$$

دقت کنید $\alpha\beta \neq \beta\alpha$. □

فرض کنید $X = \{x_۱, x_۲, \ldots, x_n\}$ مجموعه‌ای n عضوی باشد. می‌خواهیم تعداد جایگشت‌های روی X را تعیین کنیم. اگر $\alpha \in S_X$، آن‌گاه برای $\alpha(۱)$ ، n انتخاب داریم. چون α یک‌به‌یک است برای تعریف $\alpha(۲)$، $n-۱$ انتخاب داریم. با ادامه این روند برای تعریف $\alpha(n-۱)$، ۲ انتخاب و در نهایت برای تعریف $\alpha(n)$، ۱ انتخاب داریم. پس تعداد راه‌های تعریف توابع یک‌به‌یک از X به X برابر است با

$$n \cdot (n-۱) \cdot (n-۲) \cdots ۲ \cdot ۱ = n!.$$

هر تابع یک‌به‌یک از یک مجموعه‌ی متناهی به خودش پوشا نیز هست، پس تعداد جایگشت‌های روی X دقیقاً $n!$ است. بنابراین ثابت کرده‌ایم $|S_n| = n!$.

مثال ۵.۷.۱. مجموعه‌ی اعضای $S_۳$، عبارت است از

$$S_۳ = \left\{ \begin{pmatrix} ۱ & ۲ & ۳ \\ ۱ & ۲ & ۳ \end{pmatrix}, \begin{pmatrix} ۱ & ۲ & ۳ \\ ۲ & ۱ & ۳ \end{pmatrix}, \begin{pmatrix} ۱ & ۲ & ۳ \\ ۳ & ۲ & ۱ \end{pmatrix}, \begin{pmatrix} ۱ & ۲ & ۳ \\ ۱ & ۳ & ۲ \end{pmatrix}, \right.$$
$$\left. \begin{pmatrix} ۱ & ۲ & ۳ \\ ۲ & ۳ & ۱ \end{pmatrix}, \begin{pmatrix} ۱ & ۲ & ۳ \\ ۳ & ۱ & ۲ \end{pmatrix} \right\}.$$ □

چنان که در مثال بالا دیدیم حاصل‌ضرب دو جایگشت دلخواه لزوماً تعویض‌پذیر نیست. اما در حالتی که دو جایگشت مجزا باشند، حاصل‌ضرب آن‌ها تعویض‌پذیر است. جایگشت‌های مجزا را در زیر تعریف می‌کنیم:

تعریف ۶.۷.۱. فرض کنید $\alpha \in S_X$ و $x \in X$. اگر $\alpha(x) \neq x$ گوییم α، x را حرکت می‌دهد و اگر $\alpha(x) = x$ گوییم α، x را ثابت نگه می‌دارد.

تعریف ۷.۷.۱. فرض کنید $\alpha, \beta \in S_X$. فرض کنید به ازای هر $x \in X$، اگر α، x حرکت دهد، β، x را ثابت نگه دارد و اگر β، x حرکت دهد، α، x را ثابت نگه دارد ، یعنی

$$\alpha(x) \neq x \Longrightarrow \beta(x) = x$$
$$\beta(x) \neq x \Longrightarrow \alpha(x) = x.$$

در این صورت α و β را مجزا گوییم.

به عنوان مثال فرض کنید سه جایگشت α، β، γ، در $S_۵$ به صورت زیر تعریف شده باشند :

$$\alpha = \begin{pmatrix} ۱ & ۲ & ۳ & ۴ & ۵ \\ ۳ & ۱ & ۵ & ۴ & ۲ \end{pmatrix}, \quad \beta = \begin{pmatrix} ۱ & ۲ & ۳ & ۴ & ۵ \\ ۱ & ۲ & ۵ & ۴ & ۳ \end{pmatrix}, \quad \gamma = \begin{pmatrix} ۱ & ۲ & ۳ & ۴ & ۵ \\ ۲ & ۱ & ۳ & ۴ & ۵ \end{pmatrix}.$$

ملاحظه کنید که α، ۴ را ثابت نگه می‌دارد و ۱، ۲، ۳، و ۵ را حرکت می‌دهد. β، ۱، ۲ و ۴ را ثابت نگه می‌دارد و ۳ و ۵ را حرکت می‌دهد. γ، ۳، ۴، و ۵ را ثابت نگه می‌دارد و ۱، و ۲ حرکت می‌دهد. پس β و γ مجزا هستند اما α و β مجزا نیستند. هم‌چنین α و γ مجزا نیستند. حال نشان می‌دهیم حاصل‌ضرب جایگشت‌های مجزا تعویض‌پذیر است:

قضیه ۸.۷.۱. اگر $\alpha, \beta \in S_X$ دو جایگشت مجزا باشند، آن‌گاه $\alpha\beta = \beta\alpha$.

اثبات. فرض کنید $x \in X$ عضو دلخواهی باشد. اگر هم α، و هم β، x را ثابت نگه دارند، آنگاه

$$\beta\alpha(x) = \beta(x) = x = \alpha(x) = \alpha\beta(x).$$

اگر α، x را حرکت دهد، یعنی $\alpha(x) \neq x$، آنگاه چون α یک‌به‌یک است، $\alpha(\alpha(x)) \neq \alpha(x)$. بنابراین α، $\alpha(x)$ را نیز حرکت می‌دهد. از طرف دیگر α و β مجزا هستند ، پس β هم x و هم $\alpha(x)$ را ثابت نگه می‌دارد ، یعنی $\beta(x) = x$ و $\beta\alpha(x) = \alpha(x)$. بنابراین

$$\alpha\beta(x) = \alpha(x) = \beta\alpha(x).$$

به همین نحو اگر β، x را حرکت دهد داریم $\alpha\beta(x) = \beta\alpha(x)$. این رابطه به ازای هر $x \in X$ درست است، بنابراین $\alpha\beta = \beta\alpha$. □

تعریف ۹.۷.۱. $\alpha \in S_X$ را یک دور به طول r یا r- دور گوییم هرگاه اعضای $x_1, \ldots, x_r \in X$ وجود داشته باشند که برای هر $x \neq x_i$، $i = 1, \ldots r$، داشته باشیم $\alpha(x) = x$ و هم‌چنین

$$\alpha(x_1) = x_2, \quad \alpha(x_2) = x_3, \quad \ldots, \quad \alpha(x_{r-1}) = x_r, \quad \alpha(x_r) = x_1.$$

در این صورت می‌نویسیم $\alpha = (x_1\ x_2\ \cdots\ x_r)$.

توجه کنید اگر $\alpha = (x_1\ x_2\ \cdots\ x_r)$ یک r- دور باشد، می‌توان نوشت

$$\begin{aligned} \alpha = (x_1\ x_2\ \cdots\ x_r) &= (x_2\ x_3 \cdots x_r\ x_1) \\ &= (x_3\ x_4\ \cdots\ x_r\ x_1\ x_2) \\ &= (x_r\ x_1\ x_2\ \cdots\ x_{r-1}). \end{aligned}$$

یک دور به طول ۲ را ترانهش گوییم.

مثال ۱۰.۷.۱. جایگشت $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 7 & 1 & 6 & 5 & 2 & 3 \end{pmatrix}$ را با نماد دور بنویسید.

حل می‌توان نوشت $\alpha = (3\ 7\ 2\ 6\ 4\ 1)$. توجه کنید که α، ۵ را ثابت نگه می‌دارد. □

مثال ۱۱.۷.۱. تنها دور به طول ۱ جایگشت همانی (1) است. □

مثال ۱۲.۷.۱. از مثال ۵.۷.۱، داریم

$$S_3 = \{(1), (1\ 2\ 3), (1\ 3\ 2), (1\ 2), (1\ 3), (2\ 3)\}.$$

پس هر عضو S_3 دور است. اما در حالت کلی همه‌ی اعضای S_n دور نیستند. □

مثال ۱۳.۷.۱. جایگشت

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 1 & 7 & 6 & 10 & 4 & 2 & 5 & 9 & 8 \end{pmatrix}$$

در S_{10} را در نظر بگیرید. از ۱ شروع می‌کنیم، و عمل α را از ۱ به صورت زیر دنبال می‌کنیم: $\alpha : 1 \to 3 \to 7 \to 2 \to 1$. بنابراین یک دور حاصل می‌شود: $(2\ 7\ 3\ 1)$. اکنون با عضو دیگری در دور بالا نیست شروع می‌کنیم، مثلاً $\alpha : 4 \to 6 \to 4$؛ بنابراین دور دیگری حاصل می‌شود: $(6\ 4)$. اما هنوز ۵ استفاده نشده است، پس با ۵ شروع می‌کنیم: $\alpha : 5 \to 10 \to 8 \to 5$ که دور $(8\ 10\ 5)$ را به دست می‌دهد. در نهایت تنها عضو باقیمانده ۹ است که α آن را ثابت نگه می‌دارد و دور متناظر آن (9) است که همان جایگشت همانی است. بنابراین $\alpha = (2\ 7\ 3\ 1)(6\ 4)(8\ 10\ 5)(9)$، که اگر از جایگشت همانی صرف‌نظر کنیم خواهیم داشت

$$\alpha = (2\ 7\ 3\ 1)(6\ 4)(8\ 10\ 5).$$

ملاحظه کنید که α دور نیست اما حاصل‌ضرب دورهای مجزا است. □

برای عکس کردن عمل یک دور، یعنی برای یافتن وارون یک جایگشت دوری، کافی است آن را در جهت مخالف بنویسیم. یعنی اگر $\alpha = (x_1\ x_2\ \cdots\ x_{r-1}\ x_r)$ یک r- دور در S_n باشد، آنگاه α^{-1} نیز یک r- دور است و $\alpha^{-1} = (x_r\ x_{r-1}\ \cdots\ x_2\ x_1)$.
استفاده از نماد دور بسیار ساده‌تر از نماد دو سطری است. اما وقتی از نماد دور استفاده می‌کنیم دو نکته را باید در نظر داشته باشیم. اول این که یک جایگشت دوری را می‌توان با نماد دوری به صورت های متفاوتی نوشت. مثلاً $\alpha = (۲\ ۴\ ۳\ ۱)$ در $S_۴$ را می‌توان به صورت های $(۳\ ۲\ ۱\ ۴) = (۲\ ۱\ ۴\ ۳) = (۴\ ۳\ ۲\ ۱)$ نوشت. البته این مطلب در صورت آگاهی از آن اشکالی پیش نمی‌آورد.
دومین نکته را با یک مثال توضیح می‌دهیم: اگر $\alpha = (۱\ ۴\ ۲)$، آنگاه α در $S_۴$ است (که ۳ را ثابت نگه می‌دارد)؟ یا در $S_۵$ (که ۳ و ۵ را ثابت نگه می‌دارد)؟ با قرار داد زیر این نکته نیز هیچ مشکلی پیش نمی‌آورد.

قرارداد: هر جایگشت در S_n را می‌توان به عنوان تابعی از $\mathbb{N}$ به $\mathbb{N}$ (یعنی عضوی از $S_{\mathbb{N}}$) در نظر گرفت که عناصر $n+۱$، $n+۲$، ... را ثابت نگه می‌دارد. بنابراین

$$S_n = \{\alpha \in S_{\mathbb{N}} \mid \forall j > n,\ \ \alpha(j) = j\}.$$

پس $S_۱ \subset S_۲ \subset S_۳ \subset \cdots$. این قرار داد را در تمامی کتاب استفاده می‌کنیم. با استفاده از روش مثال ۱۳.۷.۱، نشان می‌دهیم که هر جایگشت دلخواه را می‌توان به صورت حاصلضرب جایگشت‌های مجزا نوشت. اکنون نحوه‌ی یافتن تجزیه را تشریح می‌کنیم. ابتدا توان‌های یک جایگشت را تعریف می‌کنیم. اگر $\alpha \in S_X$ و n عدد طبیعی باشد، α^n را برابر n بار ترکیب α با خودش تعریف می‌کنیم، یعنی $\alpha^n = \underbrace{\alpha\alpha\cdots\alpha}_{n\ \text{بار}}$. به علاوه تعریف می‌کنیم: $\alpha^{\circ} = \mathrm{id}_X$ و $\alpha^{-n} = (\alpha^{-1})^n$. بنابراین به ازای هر عدد صحیح $m \in \mathbb{Z}$، α^m را تعریف کرده‌ایم. به عنوان مثال اگر $\alpha = (۳\ ۷\ ۲\ ۶\ ۴\ ۱)$، آنگاه

$$\alpha^۲ = (۱\ ۶\ ۷)(۲\ ۳\ ۴), \quad \alpha^۳ = (۱\ ۲)(۳\ ۶)(۴\ ۷),$$
$$\alpha^۴ = (۱\ ۷\ ۶)(۲\ ۴\ ۳), \quad \alpha^۵ = (۱\ ۳\ ۷\ ۲\ ۶\ ۴), \quad \alpha^۶ = (۱),$$

و

$$\alpha^{-۲} = (۱\ ۷\ ۶)(۲\ ۴\ ۳), \quad \alpha^{-۳} = (۱\ ۲)(۳\ ۶)(۴\ ۷),$$
$$\alpha^{-۴} = (۱\ ۶\ ۷)(۲\ ۳\ ۴), \quad \alpha^{-۵} = (۱\ ۴\ ۶\ ۲\ ۷\ ۳), \quad \alpha^{-۶} = (۱).$$

اگر $\alpha \in S_X$ جایگشت دلخواهی باشد، رابطه‌ی $\sim$ را روی X به صورت زیر تعریف می‌کنیم:

$$x \sim y \iff \exists k \in \mathbb{Z},\ \ \alpha^k(x) = y.$$

این رابطه یک رابطه‌ی هم‌ارزی روی X است. زیرا برای هر $x \in X$،

$$\alpha^{\circ}(x) = \mathrm{id}_X(x) = x.$$

پس $x \sim x$ و رابطه‌ی $\sim$ بازتابی است. حال اگر $x, y \in X$ و $x \sim y$، آنگاه $k \in \mathbb{Z}$ وجود دارد که $\alpha^k(x) = y$. بنابراین $\alpha^{-k}\alpha^k(x) = \alpha^{-k}(y)$. در نتیجه $x = \alpha^{-k}(y)$، یعنی $y \sim x$ و رابطه‌ی $\sim$ متقارن است. در نهایت اگر $x, y, z \in X$ طوری باشند که $x \sim y$ و $y \sim z$، داریم $\alpha^k(x) = y$ و $\alpha^l(y) = z$ که در آن $l, k \in \mathbb{Z}$. بنابراین $\alpha^{l+k}(x) = \alpha^l\alpha^k(x) = \alpha^l(y) = z$. پس $x \sim z$ و $\sim$ ترایا است. در نتیجه $\sim$ رابطه‌ای هم‌ارزی روی X است. رده‌های هم‌ارزی این رابطه را مدارهای α گوییم. مدار α شامل $x \in X$ را با $\mathrm{orb}_\alpha(x)$ نشان می‌دهیم، پس

$$\begin{aligned}\mathrm{orb}_\alpha(x) &= \{y \in X \mid \exists k \in \mathbb{Z},\ \ \alpha^k(x) = y\} \\ &= \{\alpha^k(x) \mid k \in \mathbb{Z}\}.\end{aligned}$$

توجه کنید که اگر x، α را ثابت نگه دارد هر توانی از α نیز x را ثابت نگه می‌دارد. بنابراین در این حالت $\mathrm{orb}_\alpha(x) = \{x\}$، یعنی مدار x تحت α تک عضوی است. در صورتی که $\alpha = (x_1\ x_2\ \cdots\ x_r)$،یک $r-$ دور باشد، آنگاه

$$\alpha(x_1) = x_2, \quad \alpha^۲(x_1) = x_3, \quad \ldots, \quad \alpha^{r-1}(x_1) = x_r$$

و $\mathrm{orb}_\alpha(x_1) = \{x_1, \ldots, x_r\}$. در نتیجه یک جایگشت غیر همانی دور است اگر و تنها اگر فقط یک مدار با بیش از یک عضو داشته باشد (یعنی تنها یک مدار نابدیهی داشته باشد). یک دور، r- دور است هرگاه تنها مدار نابدیهی آن دقیقاً r عضو داشته باشد. اگر X مجموعه‌ای متناهی باشد و $\alpha \in S_X$، مدارهای α یک افراز X را تشکیل می‌دهند. فرض کنید X_1، ...، X_m مدارهای α باشند. در این صورت با توجه به تعریف رابطه‌ی $\sim$ داریم $\alpha(X_i) = X_i$. هم‌چنین $\alpha|_{X_i}$ یک دور به طول $|X_i|$ است. حال اگر X_1، ...، X_m مدارهای نابدیهی α باشند، بحث بالا می‌گوید $\alpha|_{X_i}$ یک دور است. اگر به ازای هر $i = 1, \ldots, m$، جایگشت $\alpha_i \in S_X$ را جایگشتی تعریف کنیم که روی X_i برابر α باشد و هر عضو دیگر را ثابت نگه دارد ، آنگاه هر α_i یک دور در S_X است. به علاوه α_iها مجزا هستند و $\alpha = \alpha_1\alpha_2\cdots\alpha_m$ (چرا؟). پس تجزیه‌ی مورد نظر حاصل می‌شود.
در قضیه‌ی بعد علاوه بر این که اثبات دیگری از وجود تجزیه یک جایگشت به حاصل‌ضرب دورهای مجزا ارائه می‌کنیم، نشان می‌دهیم این تجزیه (صرف‌نظر از ترتیب دورها) یکتا است.

قضیه ۱۴.۷.۱. هر جایگشت نابدیهی برابر حاصل‌ضرب دورهای مجزا با طول بزرگ‌تر یا مساوی ۲ است. این تجزیه بجز در ترتیب نوشتن دورها یکتاست.

اثبات. فرض کنید حکم درست نباشد. پس بنا به اصل خوشترتیبی کوچک‌ترین عدد طبیعی n وجود دارد که حکم قضیه در S_n برقرار نیست. توجه کنید $n \geq 2$ و بنا به خاصیت n، قضیه برای S_{n-1} درست است. چون S_n در حکم قضیه صدق نمی‌کند جایگشت $\alpha \in S_n$ وجود دارد که به حاصل‌ضرب دورهای مجزا تجزیه نمی‌شود. اگر $\alpha(n) = n$، آنگاه $\alpha \in S_{n-1}$، که تناقض است. پس فرض کنید $\alpha(n) \neq n$. چون α پوشاست $m \in \{1, 2, \ldots, n-1\}$ وجود دارد که $\alpha(m) = n$. قرار می‌دهیم $\sigma = (m\ n)$ و جایگشت $\gamma = \alpha\sigma$ را در نظر می‌گیریم. چون $\sigma^2 = (1)$ داریم $\gamma\sigma = \alpha\sigma^2 = \alpha$. به علاوه $\gamma(n) = \alpha\sigma(n) = \alpha(m) = n$ و $\gamma \in S_{n-1}$. در نتیجه، بنا به خاصیت n، γ حاصل‌ضرب دورهای مجزا است. دو حالت وجود دارد
(الف) $\gamma(m) = m$. در این حالت γ و σ مجزا هستند (زیرا $\gamma(n) = n$) و چون $\alpha = \sigma\gamma$، حکم ثابت است.
(ب) $\gamma(m) \neq m$. در این حالت دقیقاً یک دور در تجزیه‌ی γ، m را حرکت می‌دهد. بنابراین می‌توان نوشت

$$\gamma = \beta(m\ k_1\ k_2\ \cdots\ k_r),$$

که در آن β حاصل‌ضرب ضربی از جایگشت‌های مجزا است و m و k_1، k_2،...، k_r را ثابت نگاه می‌دارند (پس n را ثابت نگاه می‌دارند، زیرا $\gamma(n) = n$). در نهایت به سادگی می‌توان تحقیق کرد که

$$\alpha = \gamma\sigma = \beta(m\ k_1\ k_2\ \cdots\ k_r)(m\ n) = \beta(m\ n\ k_1\ k_2\ \cdots\ k_r)$$

تجزیه‌ی α به دورهای مجزا است و این تناقض است.
حال یکتایی تجزیه را ثابت می‌کنیم. فرض کنید حکم قضیه درست نباشد، پس جایگشت

$$\alpha = \alpha_1\alpha_2\cdots\alpha_m = \beta_1\beta_2\cdots\beta_k \qquad (1)$$

با دو تجزیه به دورهای مجزا با طول بزرگ‌تر یا مساوی ۲ وجود دارد که $\max\{m, k\}$ می‌نیمم است. اگر α، x را حرکت دهد، آنگاه یکی از α_iها و یکی از β_i باید x را حرکت دهند چون جایگشت‌های مجزا تعویض می‌شوند با تغییر اندیس‌ها می‌توانیم فرض کنیم α_1 و β_1، x را حرکت می‌دهند. در نتیجه برای $i \neq 1$، α_i و β_i و بنابراین توان‌های آن ها x را ثابت نگه می‌دارند. به ازای هر عدد صحیح مثبت t داریم

$$\alpha^t(x) = \alpha_1^t(x).$$

به همین نحو $\alpha^t(x) = \beta_1^t(x)$. در نتیجه

$$\alpha_1^t(x) = \alpha^t(x) = \beta_1^t(x).$$

چون α_1 و β_1 دور هستند و تنها یک مدار نابدیهی دارند با توجه به رابطه‌ی فوق طول مدار آن ها مساوی است و مثلاً هر دو r- دور هستند و

$$\beta_1 = (\beta_1(x)\ \beta_1^2(x)\ \cdots\ \beta_1^{r-1}(x)), \quad \alpha_1 = (\alpha_1(x)\ \alpha_1^2(x)\ \cdots\ \alpha_1^{r-1}(x)).$$

در نتیجه $\alpha_۱ = \beta_۱$ و با حذف آن‌ها از طرفین تساوی (۱) داریم

$$\alpha_۲ \cdots \alpha_m = \beta_۲ \cdots \beta_k.$$

پس دو تجزیه برای $\alpha_۲ \cdots \alpha_m$ با تعداد عوامل کمتر از $\max\{m,k\}$ داریم ، که این متناقض با می‌نیمم بودن $\max\{m,k\}$ است. این تناقض نشان می‌دهد تجزیه‌ی یک جایگشت به دورهای مجزا (صرف‌نظر از ترتیب دورها) یکتا است. □

تجزیه‌ی یک جایگشت به دورهای مجزا را تجزیه‌ی دوری آن گوییم.

مثال ۱۵.۷.۱. تجزیه‌ی دوری همه‌ی عناصر $S_۴$ را فهرست کنید.

حل $۲۴ = ۴!$ عضو $S_۴$ عبارتند از

$$(۱)$$
$$(۱\ ۲), (۱\ ۳), (۱\ ۴), (۲\ ۳), (۲\ ۴), (۳\ ۴)$$
$$(۱\ ۲\ ۳), (۱\ ۳\ ۲), (۱\ ۲\ ۴), (۱\ ۴\ ۲), (۱\ ۴\ ۳), (۱\ ۳\ ۴), (۲\ ۳\ ۴), (۲\ ۴\ ۳)$$
$$(۱\ ۲\ ۳\ ۴), (۱\ ۲\ ۴\ ۳), (۱\ ۳\ ۲\ ۴), (۱\ ۳\ ۴\ ۲), (۱\ ۴\ ۲\ ۳), (۱\ ۴\ ۳\ ۲)$$
$$(۱\ ۲)(۳\ ۴), (۱\ ۳)(۲\ ۴), (۱\ ۴)(۲\ ۳),$$

در جدول زیر شکل تجزیه‌ی دوری اعضای $S_۴$ و تعداد آن ها مشخص شده‌اند

ساختار دوری		تعداد
$(\times)$	۱	$= ۱$
$(\times\times)$	$\frac{۴ \times ۳}{۲}$	$= ۶$
$(\times\times\times)$	$\frac{۴ \times ۳ \times ۲}{۳}$	$= ۸$
$(\times\times\times\times)$	$\frac{۴ \times ۳ \times ۲ \times ۱}{۴}$	$= ۶$
$(\times\times)(\times\times)$	$\frac{۱}{۲}\left(\frac{۴ \times ۳}{۲} \times \frac{۲ \times ۱}{۲}\right)$	$= ۳$
		$۲۴ = ۴!$

در جدول زیر شکل تجزیه‌ی دوری (ساختار دوری) اعضای $S_۵$ و تعداد آن ها مشخص شده‌اند

ساختار دوری		تعداد
$(\times)$	۱	$= ۱$
$(\times\times)$	$\frac{۵ \times ۴}{۲}$	$= ۱۰$
$(\times \times \times)$	$\frac{۵ \times ۴ \times ۳}{۳}$	$= ۲۰$
$(\times \times \times\times)$	$\frac{۵ \times ۴ \times ۳ \times ۲}{۴}$	$= ۳۰$
$(\times \times \times \times \times)$	$\frac{۵!}{۵}$	$= ۲۴$
$(\times\times)(\times \times \times)$	$\frac{۵ \times ۴}{۲} \times \frac{۳ \times ۲ \times ۱}{۳}$	$= ۲۰$
$(\times\times)(\times\times)$	$\frac{۱}{۲}\left(\frac{۵ \times ۴}{۲} \times \frac{۳ \times ۲}{۲}\right)$	$= ۱۵$
		$\overline{۱۲۰ = ۵!}$

نتیجه ۱۶.۷.۱. هر جایگشت در S_n را می‌توان بر حسب حاصل‌ضرب ترانهش‌ها نوشت.

اثبات. با توجه به قضیه‌ی ۱۴.۷.۱، کافی است ثابت کنیم هر r- دور را می‌توان بر حسب حاصل‌ضرب ترانهش‌ها نوشت. اگر $r = ۱$، آنگاه

$$(x_۱) = (x_۱\ x_۲)(x_۱\ x_۲)$$

و اگر $r > ۱$، آنگاه می‌توان نوشت

$$(x_۱\ x_۲\ x_۳\ \cdots\ x_r) = (x_۱\ x_r)(x_۱\ x_{r-۱})\cdots(x_۱\ x_۲). \qquad \square$$

نوشتن یک جایگشت بر حسب حاصل‌ضرب ترانهش‌ها یکتا نیست، مثلاً

$$(۱\ ۲\ ۳) = (۱\ ۳)(۱\ ۲), \quad (۱\ ۲\ ۳) = (۲\ ۳)(۱\ ۲)(۱\ ۳)(۲\ ۳).$$

اما زوج یا فرد بودن تعداد ترانهش‌ها یکتاست. یعنی اگر یک جایگشت را بتوان بر حسب تعداد زوج (یا فردی) ترانهش تجزیه کرد، آنگاه در هر تجزیه آن به حاصل‌ضرب ترانهش‌ها همواره تعداد زوجی (یا فردی) ترانهش ظاهر می‌شود:

قضیه ۱۷.۷.۱. هیچ جایگشتی در S_n، $n \geq ۲$، را نمی‌توان هم به صورت حاصل‌ضرب تعداد زوجی ترانهش و هم به صورت تعداد فردی ترانهش تجزیه کرد.

اثبات. ابتدا حالت جایگشت همانی را در نظر می‌گیریم در این حالت $(۱) = (۱\ ۲)(۱\ ۲)$ و ثابت می‌کنیم در هر تجزیه (۱) به ترانهش‌ها تعداد زوجی ترانهش وجود دارد. اگر α_i، برای $i = ۱, ۲, \ldots, k$، ترانهش باشد و $(۱) = \alpha_۱\alpha_۲\cdots\alpha_k$، باید نشان دهیم k زوج است. عدد m را که حداقل در یکی از ترانهش‌های α_i آمده است انتخاب می‌کنیم و فرض می‌کنیم از چپ به راست اولین ترانهش باشد که m را حرکت می‌دهد. بدیهی است که $j \neq k$ (زیرا در غیر این صورت (۱)، m را ثابت نگه نمی‌دارد). اکنون $\alpha_j\alpha_{j+۱}$ باید به یکی از صورت های زیر باشد.

$$(m\ x)(m\ x) = (۱) \qquad (*)$$
$$(m\ x)(m\ y) = (x\ m\ y) = (x\ y)(x\ m)$$
$$(m\ x)(y\ z) = (y\ z)(m\ x)$$
$$(m\ x)(x\ y) = (y\ m\ x) = (y\ x)(y\ m).$$

اگر به جای $\alpha_j\alpha_{j+1}$ مقدار را از یکی از تساوی‌های فوق قرار دهیم یا از ترانهش‌های موجود دو تا کم می‌شود و یا اولین وقوع m یک مرحله به سمت راست حرکت داده می‌شود. با تکرار این عمل سرانجام باید به حالت (*) برسیم و دو تا از ترانهش‌های موجود کم می‌شود. با انجام این کار برای همه‌ی اعدادی که در ترانهش‌های تجزیه‌ی (۱) ظاهر شده‌اند و حذف همه‌ی آن ها دیده می‌شود که در هر مرحله دو ترانهش حذف می‌شود. پس k باید زوج باشد.
اکنون در حالت کلی، اگر دو تجزیه‌ی $\alpha = \alpha_1\alpha_2\cdots\alpha_r = \beta_1\beta_2\cdots\beta_s$ به ترانهش‌ها برای جایگشت α در نظر بگیریم، آنگاه داریم

$$(1) = \alpha\alpha^{-1} = \alpha_1\alpha_2\cdots\alpha_r\beta_s^{-1}\beta_{s-1}^{-1}\cdots\beta_1^{-1}.$$

چون هر ترانهش با وارون خود مساوی است

$$(1) = \alpha_1\alpha_2\cdots\alpha_r\beta_s\beta_{s-1}\cdots\beta_1.$$

پس بنا به مرحله‌ی قبل، $r+s$ باید زوج باشد، یعنی یا r و s هر دو زوج و یا هر دو فرد هستند. □

تعریف ۱۸.۷.۱. یک جایگشت را زوج گوییم هرگاه در تجزیه‌ی آن به حاصل‌ضرب ترانهش‌ها تعداد زوجی ترانهش ظاهر شود و در غیر این صورت آن را فرد گوییم.

مجموعه‌ی همه‌ی جایگشت‌های زوج در S_n را با A_n نشان می‌دهیم.

مثال ۱۹.۷.۱. نشان دهید تعداد جایگشت‌های زوج و فرد در S_n، $n \geq 2$، برابر هستند و نتیجه بگیرید $|A_n| = \frac{1}{2}n!$.

حل فرض کنید T مجموعه‌ی جایگشت‌های فرد در S_n باشد. یک ترانهش دلخواه، مثلاً $\sigma = (1\ 2)$، را در نظر می‌گیریم. تابع $f : A_n \longrightarrow T$ را با ضابطه‌ی $f(\alpha) = \alpha\sigma$ تعریف می‌کنیم. چون ترانهش‌ها فرد هستند و حاصل‌ضرب یک جایگشت فرد و یک جایگشت زوج، فرد است، f خوش تعریف است. f یک‌به‌یک است، زیرا اگر $f(\alpha) = f(\beta)$ آنگاه $\alpha\sigma = \beta\sigma$ و در نتیجه $\alpha = \beta$. حال اگر $\gamma \in T$، آنگاه $\gamma\sigma \in A_n$ و $f(\gamma\sigma) = \gamma\sigma\sigma = \gamma$. پس f پوشا نیز هست. بنابراین $|A_n| = |T|$. به ویژه چون $A_n \cap T = \emptyset$ و $S_n = A_n \cup T$ داریم

$$n! = |S_n| = |A_n| + |T| = |A_n| + |A_n|.$$

بنابراین $|A_n| = \frac{1}{2}n!$. □

A_n تحت عمل ترکیب جایگشت‌ها گروه است. زیرا جایگشت همانی زوج است؛ وارون یک جایگشت زوج و حاصل‌ضرب دو جایگشت زوج، زوج است. A_n را گروه متناوب از درجه‌ی n گوییم. داریم $A_3 = \{(1), (1\ 2\ 3), (1\ 3\ 2)\}$. هر عضو غیرهمانی A_3 یک ۳- دور است. این مطلب برای A_n در حالت کلی درست نیست. اما با استفاده از ۳- دورها می‌توان همه‌ی اعضای A_n را به دست آورد. در واقع هر عضو غیرهمانی A_n به صورت حاصل‌ضرب تعداد زوجی ترانهش است و هر زوج ترانهش را می‌توان به صورت حاصل‌ضرب ۳- دورها نوشت:یک جفت ترانهش یا به صورت $(a\ b)(a\ c)$ است که در آن a، b، c متمایزند و یا به صورت $(a\ b)(c\ d)$ که در آن a، b، c، d متمایزند نوشت و داریم

$$(a\ b)(a\ c) = (a\ c\ b), \qquad (a\ b)(c\ d) = (a\ d\ c)(a\ b\ c).$$

پس هر عضو A_n را می‌توان به صورت حاصل‌ضرب ۳- دورها نوشت.

تمرین‌ها

۱. جایگشت‌های

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 4 & 3 & 5 \end{pmatrix},\ \beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 1 & 5 & 2 \end{pmatrix},\ \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 2 & 1 & 4 \end{pmatrix}$$

را به دورهای مجزا تجزیه و عبارت‌های زیر را محاسبه کنید
(الف) $\alpha\beta$ (ب) $\beta\alpha$ (ج) $\alpha\beta\sigma^{-1}$
(د) $\sigma\alpha^2$ (هـ) $\beta\alpha\beta^{-1}$ (و) $\beta^2\sigma^{-2}$

۲. جایگشت‌های زیر را به دورهای مجزا تجزیه کنید.

(الف) $\begin{pmatrix} ۱ & ۲ & ۳ & ۴ & ۵ & ۶ & ۷ & ۸ & ۹ \\ ۴ & ۷ & ۹ & ۸ & ۲ & ۱ & ۶ & ۳ & ۵ \end{pmatrix}$

(ب) $\begin{pmatrix} ۱ & ۲ & ۳ & ۴ & ۵ & ۶ & ۷ & ۸ & ۹ \\ ۳ & ۸ & ۹ & ۵ & ۲ & ۱ & ۶ & ۴ & ۷ \end{pmatrix}$

(ج) $\begin{pmatrix} ۱ & ۲ & ۳ & ۴ & ۵ & ۶ & ۷ & ۸ & ۹ \\ ۶ & ۴ & ۸ & ۹ & ۳ & ۱ & ۷ & ۵ & ۲ \end{pmatrix}$

(د) $(۱\ ۶\ ۳)(۷\ ۱\ ۳\ ۵\ ۷)(۶\ ۷)(۵\ ۱\ ۲\ ۳\ ۴)$.

۳. ساختار دوری، و توازن (زوج یا فرد بودن) اعضای $S_۶$ را مشخص کنید.

۴. زوج یا فرد بودن جایگشت‌های زیر را مشخص کنید.

(الف) $(۲\ ۶)(۲\ ۳\ ۴)(۵\ ۱\ ۲)$ (ب) $(۳\ ۶\ ۷\ ۱)(۳\ ۲)(۵\ ۱\ ۲)$.

۵. فرض کنید n و m اعداد صحیح مثبت باشند و $m \mid n$. اگر $\alpha \in S_n$ یک n- دور باشد نشان دهید α^m حاصل‌ضرب m دور به طول $\dfrac{n}{m}$ است.

۶. اگر X یک مجموعه‌ی دلخواه و $A = \{a_۱, \ldots, a_m\}$ و $B = \{b_۱, \ldots, b_m\}$ زیرمجموعه‌های X باشند، نشان دهید جایگشت $\sigma \in S_X$ وجود دارد که به ازای هر $۱ \le i \le m$، $\sigma(a_i) = b_i$.

۷. اگر $\sigma = (a_۱\ a_۲\ \cdots\ a_m)$ یک دور به طول m و τ یک جایگشت دلخواه در S_n باشند، ثابت کنید $\tau\sigma\tau^{-۱} = (\tau(a_۱)\ \tau(a_۲)\ \cdots\ \tau(a_m))$.

۸. دو جایگشت $\alpha, \beta \in S_n$ را مزدوج گوییم هرگاه جایگشت $\tau \in S_n$ وجود داشته باشد که $\tau\alpha\tau^{-۱} = \beta$.
(الف) از مساله‌ی قبل نتیجه بگیرید دو دور در S_n مزدوج‌اند اگر و تنها اگر طول یکسان داشته باشند.
(ب) نشان دهید دو جایگشت در S_n مزدوج‌اند اگر و تنها اگر تجزیه‌ی دوری یکسان داشته باشند.

۹. نشان دهید :
(الف) هر عضو S_n را می‌توان به صورت حاصل‌ضرب ترانهش‌های $(۱\ i)$ نوشت که در آن $۲ \le i \le n$.
(ب) هر عضو S_n را می‌توان به صورت حاصل‌ضرب ترانهش‌های $(i\ i+۱)$ نوشت که در آن $۱ \le i \le n-۱$.

۱۰. نشان دهید :
(الف) هر عضو A_n را می‌توان به صورت حاصل‌ضرب ۳- دورهای $(۱\ i\ j)$ نوشت که در آن $۲ \le i, j \le n$، $i < j$.
(ب) هر عضو A_n را می‌توان به صورت حاصل‌ضرب ۳- دورهای $(۱\ ۲\ i)$ نوشت که در آن $۳ \le i \le n$.

فصل ۲

اعداد صحیح

استفاده از حساب نقش به سزایی در پیشرفت تمدن بشری داشته است. حتی جوامع اولیه‌ی بشری نیز به شمارش اشیاء نیاز داشتند و اصطلاحاتی برای اعداد ۱، ۲، ۳، . . . را بسط دادند. به موازات پیشرفت تمدن بشری نیاز به توسعه‌ی شمارش برای تجارت، جنگ، تقویم، و غیره احساس شد. به این دلیل روش‌هایی برای ثبت اعداد ابداع شدند که غالباً (اما نه همیشه) شاید به خاطر تعداد انگشتان، بر مبنای گروه‌هایی از ۱۰ بودند. برخی از سیستم‌های عددی برای اعمالی مثل جمع و ضرب محاسبه نبودند (مثل اعداد رومی) و برخی دیگر مثل اعداد بابلی بر مبنای عدد ۶۰ بودند.
در این فصل فرض می‌کنیم خواننده با اعداد صحیح و خواص مقدماتی اعمال روی آن ها آشنا است و با استفاده از آن حقایق بیشتری را نظیر تقسیم پذیری و اعداد اول به دست می‌آوریم. سرتاسر جبر مجرد، مجموعه‌ی اعداد صحیح مثال‌هایی استاندارد هستند و در واقع برخی تجرید سازی‌های جبری از اعداد صحیح ناشی می‌شوند. در این جا بر آن نیستیم که ساختار اعداد صحیح را به صورت اصل موضوعی بررسی کنیم. خواص اساسی آن‌ها را می‌پذیریم. مثلاً اگر m و n اعداد صحیح باشند و $n < m$، آنگاه عدد صحیح $t \in \mathbb{Z}$ وجود دارد که $m = n + t$.
در فصل پیش اصل استقرای ریاضی و اصل خوشترتیبی را بررسی کردیم. در این فصل، برخی خواص مهم دیگر اعداد صحیح را مرور و اثبات می‌کنیم.

۱.۲ تجزیه در اعداد صحیح

مجموعه‌ی اعداد صحیح به راه‌های متفاوتی در این کتاب استفاده می‌شود: به عنوان منشاء اصلی مثال‌هایی از ساختارهای جبری؛ برای بیان تعاریف و اثبات قضایا (معمولاً به استقرا)؛ و به عنوان یک الگوی سازگار برای ساختارهای کلی‌تر. برای اغلب این موارد به خواص اعداد صحیح از جمله جمع، ضرب، و ترتیب اعداد صحیح نیاز داریم. هم‌چنین از خواص دیگری از قبیل تقسیم پذیری و اعداد اول استفاده می‌کنیم که در این بخش به این مفاهیم می‌پردازیم. ابتدا یکی از خواص مهم اعداد یعنی الگوریتم تقسیم را با استفاده از اصل خوشترتیبی ثابت می‌کنیم:

قضیه ۱.۱.۲. (الگوریتم تقسیم) اگر $a, b \in \mathbb{Z}$، $b \neq 0$، آنگاه اعداد صحیح یکتای q و r وجود دارند که $a = qb + r$، $0 \leq r < |b|$.

اثبات. ابتدا فرض کنید $b > 0$. پس $b \geq 1$. مجموعه‌ی

$$S = \{a - ub \mid u \in \mathbb{Z},\ \ a - ub \geq 0\}$$

را در نظر می‌گیریم. چون $b \geq 1$، داریم $a - (-|a|)b = a + |a|b \geq 0$. بنابراین $a - (-|a|)b \in S$. بنابراین S مجموعه‌ی ناتهی از اعداد صحیح نامنفی است. در نتیجه بنا به اصل خوشترتیبی S کوچک‌ترین عضو دارد ، مثلاً r. چون $r \in S$ داریم $r \geq 0$ و به ازای یک $q \in \mathbb{Z}$، $r = a - qb$. در نتیجه $a = qb + r$. باید نشان دهیم که $r < |b|$. فرض کنید برخلاف آن $r \geq |b| = b$. در این صورت

$$a - (q + 1)b = (a - qb) - b = r - b \geq 0.$$

پس $r - b \in S$ که تناقض است، زیرا r کوچک‌ترین عضو S است و $r - b < r$. بنابراین $r < |b|$. بنابراین قضیه در حالت $b > 0$ ثابت شد.
حال فرض کنید $b < 0$. در این صورت $|b| > 0$ و بنا به بحث فوق اعداد صحیح q' و r وجود دارند که $a = q'|b| + r$. $0 \leq r \leq |b|$.

چون $b < ۰$، $|b| = -b$. بنابراین $a = -q'b + r$. با قرار دادن $q = -q'$ داریم $a = qb + r$، $۰ \leq r < |b|$ و حکم ثابت است. حال نشان می‌دهیم q و r یکتا هستند. فرض کنید اعداد صحیح q و r' نیز وجود دارند که $۰ \leq r' < |b|$، و

$$a = qb + r = q'b + r'.$$

در این صورت

$$r' - r = (q - q')b$$

و در نتیجه

$$|r' - r| = |q - q'||b|.$$

اکنون $-|b| < -r \leq ۰$ و $۰ \leq r' < |b|$. بنابراین با جمع این نامساوی‌ها داریم

$$-|b| < r' - r < |b|,$$

یا $|r' - r| < |b|$. پس

$$۰ \leq |q - q'| < ۱.$$

چون $q - q'$ عدد صحیح است داریم $|q - q'| = ۰$. از این‌رو $|r - r'| = ۰$. بنابراین $q - q' = ۰$ و $r - r' = ۰$. در نتیجه r و q یکتا هستند. □

در قضیه‌ی فوق q را خارج قسمت و r را باقیمانده‌ی تقسیم a بر b گوییم.

نتیجه ۲.۱.۲. برای هر دو عدد صحیح a و b که $b > ۰$، اعداد صحیح یکتای q و r وجود دارند که $a = qb + r$، $۰ \leq r < b$. □

فرض کنید $a, b \in \mathbb{Z}$ و $a \neq ۰$. یادآوری می‌کنیم که گوییم a، b را عاد می‌کند یا a یک شمارنده‌های b است و می‌نویسیم $a|b$، هرگاه عدد صحیح $q \in \mathbb{Z}$ وجود داشته باشد که $b = aq$. اگر a، b را عاد نکند می‌نویسیم $a \nmid b$.

تعریف ۳.۱.۲. فرض کنید $a, b \in \mathbb{Z}$. عدد ناصفر d را بزرگ‌ترین مقسوم‌علیه مشترک a و b گوییم و می‌نویسیم $d = \gcd\{a, b\}$ یا $d = (a, b)$، هرگاه

(الف) $d \geq ۱$.

(ب) $d|a$ و $d|b$.

(ج) برای هر $c \in \mathbb{Z}$ هرگاه $c|a$ و $c|b$، آنگاه $c|d$.

اگر d و d' دو بزرگ‌ترین مقسوم‌علیه مشترک a و b باشند، آنگاه $d|d'$ و $d'|d$. بنابراین اعداد صحیح u و v وجود دارند که $d' = du$ و $d = d'v$. از این‌رو $d = duv$، که نتیجه می‌دهد $uv = ۱$. چون $d \neq ۰$. پس $u = v = ۱$ یا $u = v = -۱$. بنابراین $d' = \pm d$ و بزرگ‌ترین مقسوم‌علیه مشترک یکتاست. قضیه‌ی بعد، وجود بزرگ‌ترین مقسوم‌علیه مشترک هر دو عدد ناصفر را ثابت می‌کند.

قضیه ۴.۱.۲. اگر $a, b \in \mathbb{Z}$ ناصفر باشند، آنگاه بزرگ‌ترین مقسوم‌علیه مشترک d از a و b وجود دارد. به علاوه اعداد $m, n \in \mathbb{Z}$ وجود دارند که $d = ma + nb$.

اثبات. فرض کنید

$$S = \{ta + sb \mid t, s \in \mathbb{Z},\ \ ta + sb > ۰\}.$$

در این صورت به ازای $t = a$، $s = b$ داریم $a^۲ + b^۲ > ۰$ و $a^۲ + b^۲ \in S$. بنابراین $S \neq \emptyset$. بنا به اصل خوشترتیبی، S کوچک‌ترین عضو دارد ، مثلاً d. چون $d \in S$، اعداد $m, n \in \mathbb{Z}$ وجود دارند که $d = ma + nb$. ادعا می‌کنیم $d = \gcd\{a, b\}$. ابتدا ثابت می‌کنیم $d|a$، $d|b$. چون $d \neq ۰$ بنا به الگوریتم تقسیم اعداد صحیح q و r وجود دارند که $۰ \leq r < d$ و $a = qd + r$. بنابراین

$$\begin{aligned} r &= a - qd \\ &= a - q(ma + nb), \qquad (d = ma + nb) \\ &= (۱ - qm)a + (-qn)b. \end{aligned}$$

اگر $r > ۰$، آنگاه $r \in S$ و این متناقض با $r < d$ است. بنابراین $r = ۰$. در نتیجه $a = qd$ و $d|a$. به طریق مشابه $d|b$.
حال اگر $c \in \mathbb{N}$ وجود داشته باشد که $c|a$ و $c|b$، آنگاه $c|(ma + nb)$ (بنا به تمرین ۲) و $c|d$. بنابراین $d = \gcd\{a, b\}$. □

اگر a و b اعداد صحیح ناصفر باشند بنا به قضیه‌ی ۴.۱.۲، $d = \gcd\{a, b\}$ وجود دارد و $m, n \in \mathbb{Z}$ وجود دارند که $d = ma + nb$. اعداد صحیح m و n یکتا نیستند. زیرا مثلاً $\gcd\{۲, ۶\} = ۲$ و $۶(۱) + ۴(-۱) = ۲$ و $۶(۵) + ۴(-۷) = ۲$. قضیه‌ی ۴.۱.۲، وجود $\gcd\{a, b\}$ و اعداد m و n را ثابت می‌کند اما نحوه‌ی یافتن آن‌ها را مشخص نمی‌کند. حال نشان می‌دهیم که چگونه می‌توان این اعداد را یافت. فرض کنید $a, b \in \mathbb{Z}$ ناصفر باشند. بنا به الگوریتم تقسیم اعداد $q_۱, r_۱ \in \mathbb{Z}$ وجود دارند که

$$a = q_۱b + r_۱, \quad ۰ \le r_۱ < |b|.$$

اگر $r_۱ \neq ۰$، آنگاه بنا به الگوریتم تقسیم اعداد $q_۲, r_۲ \in \mathbb{Z}$ وجود دارند که

$$b = q_۲r_۱ + r_۲, \quad ۰ \le r_۲ < r_۱.$$

اگر $r_۲ \neq ۰$، مجدداً بنا به الگوریتم تقسیم، اعداد $q_۳, r_۳ \in \mathbb{Z}$ وجود دارند که

$$r_۱ = q_۳r_۲ + r_۳, \quad ۰ \le r_۳ < r_۲.$$

چون $r_۱ > r_۲ > r_۳ \ge ۰$، با ادامه این روند درنهایت اعداد صحیح q_k، $q_{k+۱}$ و $r_k > ۰$ را خواهیم یافت که

$$\begin{aligned} r_{k-۲} &= q_k r_{k-۱} + r_k, \quad ۰ < r_k < r_{k-۱} \\ r_{k-۱} &= q_{k+۱} r_k + ۰. \end{aligned}$$

ادعا می‌کنیم r_k (یعنی آخرین باقیماندهی ناصفر) بزرگ‌ترین مقسوم‌علیه مشترک a و b است. چون $r_k|r_{k-۱}$ و $r_{k-۲} = q_k r_{k-۱} + r_k$ پس $r_k|r_{k-۲}$ (بنا به تمرین ۲(ب)). با ادامه این روند خواهیم داشت $r_k|r_۱$ و $r_k|r_۲$. بنابراین $r_k|b$، زیرا $b = q_۲r_۱ + r_۲$. چون $r_k|b$ و $r_k|r_۱$ و $a = q_۱b + r_۱$ داریم $r_k|a$. پس r_k یک مقسوم‌علیه مشترک a و b است. حال فرض کنید c عدد صحیحی باشد که $c|a$ و $c|b$. چون $r_۱ = a - qb$ داریم $c|r_۱$. چون $c|r_۱$ و $c|b$ و $r_۲ = b - q_۲r_۱$، داریم $c|r_۲$. با ادامه این روند خواهیم داشت $c|r_k$. بنابراین $r_k = \gcd\{a, b\}$. اکنون به صورت زیر، اعداد صحیح $m, n \in \mathbb{Z}$ را می‌یابیم که $r_k = ma + nb$:

$$\begin{aligned} r_k &= r_{k-۲} + r_{k-۱}(-q_k) \\ &= r_{k-۲} + [r_{k-۳} + r_{k-۲}(-q_{k-۱})](-q_k) \\ &= r_{k-۳}(-q_k) + r_{k-۲}(۱ - q_{k-۱}q_k) \quad \text{(ساده سازی)} \end{aligned}$$

با استفاده از $r_{k-۲} = r_{k-۴} + r_{k-۳}(-q_{k-۲})$ و تکرار جای‌گذاری‌ها، درنهایت به ازای اعداد صحیح m و n به رابطه‌ی $r_k = ma + nb$ خواهیم رسید. این روند به الگوریتم اقلیدسی موسوم است. روند فوق را با یک مثال تشریح می‌کنیم:

مثال ۵.۱.۲. $\gcd\{۴۵, ۱۲۶\}$ را بیابید.

حل داریم

$$\begin{aligned} ۱۲۶ &= ۲ \times ۴۵ + ۳۶ \\ ۴۵ &= ۱ \times ۳۶ + ۹ \\ ۳۶ &= ۴ \times ۹ + ۰. \end{aligned}$$

بنابراین $\gcd\{۴۵, ۱۲۶\} = ۹$. هم‌چنین داریم

$$\begin{aligned} ۹ &= ۴۵ - ۱ \times ۳۶ \\ &= ۴۵ - ۱ \times [۱۲۶ - ۲ \times ۴۵] \\ &= ۳ \times ۴۵ + (-۱) \times ۱۲۶. \end{aligned}$$

بنابراین $m = ۳$، $n = -۱$ و $۹ = ۴۵m + ۱۲۶n$. □

تعریف ۶.۱.۲. دو عدد صحیح a و b را نسبت به هم اول گوییم هرگاه $\gcd\{a,b\} = ۱$.

اگر $\gcd\{a,b\} = ۱$، آنگاه طبق قضیه‌ی ۴.۱.۲، اعداد صحیح m و n وجود دارند که $ma + nb = ۱$. بر عکس فرض کنید اعداد صحیح m و n وجود داشته باشند که $ma + nb = ۱$. اگر $d = \gcd\{a,b\}$، آنگاه $d|a$ و $d|b$. پس $d|(ma + nb)$ و $d|۱$. در نتیجه $d = ۱$. بنابراین ثابت کرده‌ایم:

قضیه ۷.۱.۲. $a, b \in \mathbb{Z}$ نسبت به هم اول‌اند اگر و تنها اگر اعداد $m, n \in \mathbb{Z}$ وجود داشته باشند که $ma + nb = ۱$. □

نتیجه ۸.۱.۲. اگر $a, b \in \mathbb{Z}$ و $d = \gcd\{a,b\}$، آنگاه $\frac{a}{d}$ و $\frac{b}{d}$ نسبت به هم اول‌اند. □

قضیه ۹.۱.۲. فرض کنید a، b، c اعداد صحیح ناصفر باشند. اگر $\gcd\{a,b\} = ۱$ و $a|bc$، آنگاه $a|c$.

اثبات. چون $\gcd\{a,b\} = ۱$، اعداد صحیح m و n وجود دارند که $ma + nb = ۱$. بنابراین $c = mac + nbc$. چون $a|a$ و $a|bc$ ، داریم $a|c$. □

تعریف ۱۰.۱.۲. عدد صحیح $p > ۱$ را عدد اول گوییم هرگاه شمارنده‌های آن تنها ± ۱ و $\pm p$ باشند.

نتیجه ۱۱.۱.۲. (لم اقلیدس) فرض کنید $a, b \in \mathbb{Z}$ ناصفر باشند و p عدد اول. اگر $p|ab$، آنگاه $p|a$ یا $p|b$.

اثبات. اگر $p|a$ حکم ثابت است. پس فرض کنید $p \nmid a$. چون تنها شمارنده‌های مثبت p ، برابر ۱ و p هستند ، پس $\gcd\{p,a\} = ۱$. بنابراین، طبق قضیه‌ی ۹.۱.۲، $p|b$. □

بنابراین به استقرا می‌توان ثابت کرد

نتیجه ۱۲.۱.۲. اگر $a_۱, a_۲, \ldots, a_n \in \mathbb{Z}$ و p عدد اول باشد که $p|a_۱a_۲\cdots a_n$، آنگاه $۱ \le i \le n$ وجود دارد که $p|a_i$. □

قضیه ۱۳.۱.۲. (قضیه‌ی اساسی حساب) هر عدد صحیح $n > ۱$ را می‌توان به طور منحصر به فرد (مگر در ترتیب عوامل) به صورت حاصل‌ضرب اعداد اول تجزیه کرد، یعنی اعداد اول (نه لزوماً متمایز) $p_۱$، $p_۲$، ...، p_r وجود دارند که $n = p_۱p_۲\cdots p_r$ و اگر $n = q_۱q_۲\cdots q_s$ که در آن q_iها اعداد اول‌اند. آنگاه $r = s$، پس از تعویض ترتیب q_jها، $p_i = q_i$ برای هر $۱ \le i \le s$.

اثبات. ابتدا وجود تجزیه را به استقرا روی n نشان می‌دهیم. اگر $n = ۲$، آنگاه n اول است و چیزی برای اثبات نیست. حال فرض کنید هر عدد صحیح k که $۲ \le k < n$ را بتوان به حاصل‌ضرب اعداد اول تجزیه کرد. اگر n عدد اول باشد، چیزی برای اثبات نیست. پس فرض کنید n عدد اول نباشد. بنابراین به ازای دو عدد صحیح b، a، که $۱ < a < n$ و $۱ < b < n$ داریم $n = ab$. اکنون بنا به فرض استقرا a و b به صورت حاصل‌ضرب اعداد اول تجزیه می‌شوند، یعنی n به صورت حاصل‌ضرب اعداد اول تجزیه می‌شود.
یکتایی تجزیه نیز به استقرا ثابت می‌کنیم. اگر $n = ۲$ چیزی برای اثبات نیست. فرض کنید یکتایی تجزیه برای همه‌ی اعداد k که $۲ \le k < n$ برقرار باشد و

$$n = p_۱p_۲\cdots p_r = q_۱q_۲\cdots q_s$$

دو تجزیه‌ی n به حاصل‌ضرب اعداد اول باشد. اگر n اول باشد چون تنها شمارنده‌های مثبت n، اعداد ۱ و n هستند ، باید داشته باشیم $r = s = ۱$. بنابراین $n = p_۱ = q_۱$ و تجزیه یکتاست. پس فرض کنید n اول نباشد. از این رو $r > ۱$ و $s > ۱$. چون

$$\frac{n}{p_۱} = p_۲\cdots p_r$$

عدد صحیح است. از طرفی چون $p_۱|q_۱\cdots q_s$، عدد $۱ \le i \le s$ وجود دارد که $p_۱|q_i$. با تعویض ترتیب q_i می‌توان فرض کرد $i = ۱$ و بنابراین $p_۱|q_۱$. چون $q_۱$ اول است و $p_۱ > ۱$. داریم $q_۱ = p_۱$. پس $n = p_۱p_۲\cdots p_r = p_۱q_۲\cdots q_s$ و

$$\frac{n}{p_۱} = p_۲\cdots p_r = q_۲\cdots q_s.$$

بنا به فرض استقرا $r = s$ و پس از تعویض ترتیب q_iها (در صورت لزوم) $p_i = q_i$ برای $۱ \le i \le s$ و حکم ثابت است. □

اگر $n \geq ۲$ عدد صحیح باشد، قضیه‌ی اساسی حساب می‌گوید n را می‌توان به طور منحصر به فرد به صورت

$$n = p_۱^{n_۱} \cdots p_r^{n_r}$$

تجزیه کرد، که در آن p_iها اعداد اول متمایزند و $n_i \geq ۱$.

نتیجه ۱۴.۱.۲. اگر $n < -۱$ عدد صحیح باشد، آنگاه n را می‌توان به صورت یکتای $n = -p_۱p_۲ \cdots p_r$ تجزیه کرد که در آن p_iها اعداد اول هستند. □

قضیه ۱۵.۱.۲. (اقلیدس) تعداد نامتناهی عدد اول وجود دارد.

اثبات. فرض کنید برخلاف حکم تعداد متناهی عدد اول $p_۱$، $p_۲$، ...، p_n وجود داشته باشند. قرار می‌دهیم

$$m = p_۱p_۲ \cdots p_n + ۱.$$

چون $m \geq ۲$، بنا به قضیه‌ی اساسی حساب عدد اول p وجود دارد که $p|m$. اگر $۱ \leq i \leq n$ وجود داشته باشد که $p = p_i$، آنگاه p، $m - p_۱p_۲ \cdots p_n = ۱$ را عاد می‌کند، که تناقض است. پس p با هیچ‌کدام از $p_۱$، ...، p_n برابر نیست و بنابراین $n + ۱$ عدد اول متمایز داریم که تناقض است. □

در قضیه‌ی بعد نشان می‌دهیم که شمارنده‌های مثبت $n = p_۱^{n_۱}p_۲^{n_۲} \cdots p_r^{n_r}$ دقیقاً به صورت $d = p_۱^{d_۱} \cdots p_r^{d_r}$، هستند که در آن $۰ \leq d_i \leq n_i$.

قضیه ۱۶.۱.۲. فرض کنید $n \in \mathbb{N}$ و $n = p_۱^{n_۱}p_۲^{n_۲} \cdots p_r^{n_r}$ تجزیه‌ی n به عوامل اول باشد، که در آن p_iها اعداد اول متمایز هستند و $n_i \geq ۱$ برای هر i. اگر d شمارنده مثبتی از n باشد، آنگاه $d = p_۱^{d_۱} \cdots p_r^{d_r}$، در آن $۰ \leq d_i \leq n_i$ برای هر i.

اثبات. بنا به لم اقلیدس شمارنده‌های اول d در مجموعه‌ی $\{p_۱, p_۲, \ldots, p_r\}$ هستند و بنا به قضیه‌ی اساسی حساب d نمی‌تواند شامل توانی از p_i بزرگ‌تر از n_i باشد. □

با استفاده از قضیه‌ی اساسی حساب می‌توان بزرگ‌ترین مقسوم‌علیه مشترک و کوچک‌ترین مضرب مشترک هر تعداد عدد صحیح را به دست آورد. ابتدا این مفاهیم را تعریف می‌کنیم. فرض کنید $a_۱$، $a_۲$، ...، a_n اعداد صحیح باشند. بزرگ‌ترین مقسوم‌علیه مشترک $a_۱$، $a_۲$، ...، a_n که با $\gcd\{a_۱, \ldots, a_n\}$ یا $(a_۱, \ldots, a_n)$ نشان داده می‌شود عبارت است از عدد صحیح مثبت d که اولاً مقسوم‌علیه مشترک a_i باشد $۱ \leq i \leq n$، یعنی $d|a_i$، $۱ \leq i \leq n$. ثانیاً مضرب هر مقسوم‌علیه مشترک a_iها باشد یعنی اگر $c|a_i$، $۱ \leq i \leq n$، آنگاه $c|d$.
کوچک‌ترین مضرب مشترک $a_۱$، ...، a_n که با $\operatorname{lcm}\{a_۱, \ldots, a_n\}$، یا $[a_۱, \ldots, a_n]$ نشان داده می‌شود عبارت است از عدد صحیح مثبت m که اولاً مضرب مشترک a_i باشد، $۱ \leq i \leq n$ یعنی $a_i|n$، $۱ \leq i \leq n$. ثانیاً مقسوم‌علیه هر مضرب مشترک a_iها باشد، یعنی اگر $a_i|u$، $۱ \leq i \leq n$، آنگاه $m|u$.
مثلاً $\gcd\{۴, ۱۲, ۱۰\} = ۲$، $\operatorname{lcm}\{۴, ۶, ۱۰\} = ۶۰$. بزرگ‌ترین مقسوم‌علیه مشترک و کوچک‌ترین مضرب مشترک برای هر تعداد عدد صحیح همواره وجود دارند، و در واقع مثل حالت وجود و یکتایی gcd برای دو عدد می‌توان عمل کرد. در مثال بعد نحوه‌ی پیدا کردن gcd و lcm را با استفاده از قضیه‌ی اساسی حساب تشریح می‌کنیم.

مثال ۱۷.۱.۲. $d = \gcd\{۱۲, ۲۰, ۱۸\}$ و $m = \operatorname{lcm}\{۱۲, ۲۰, ۱۸\}$ را بیابید.

حل ابتدا اعداد داده شده را به عوامل اول تجزیه می‌کنیم:

$$\begin{aligned} ۱۲ &= ۲^۲ \times ۳^۱ \times ۵^۰ \\ ۲۰ &= ۲^۲ \times ۳^۰ \times ۵^۱ \\ ۱۸ &= ۲^۱ \times ۳^۲ \times ۵^۰. \end{aligned}$$

به ازای اعداد صحیح a، b و c داریم $d = ۲^a ۳^b ۵^c$. داریم $a \leq ۱$، زیرا $d|۱۸$. $b = c = ۰$، زیرا $d|۲۰$ و $d|۱۲$. بنابراین $d = ۲$ بزرگ‌ترین عدد ممکن است. به طریق مشابه به ازای اعداد صحیح k، r، s، t داریم $m = ۲^r ۳^s ۵^t \times k$، که در آن $k \geq ۱$ عاملی است که

اعداد اول غیر از ۲،۳، و ۵ را دارد. اکنون $r \geq ۲$ زیرا $۲|m$ (یا زیرا $۲۰|m$)، $s \geq ۲$ زیرا $۱۸|m$ و $t > ۱$ زیرا $۲۰|m$. پس کوچک‌ترین عدد ممکن عبارت است از $m = ۲^۲ \times ۳^۲ \times ۵^۱ = ۸۰$. □

مثال قبل، قضیه‌ی زیر را پیشنهاد می‌کند که اثبات آن به خواننده، واگذار می‌شود.

قضیه ۱۸.۱.۲. فرض کنید $\{a, b, c, \ldots\}$ مجموعه‌ای متناهی از اعداد صحیح مثبت باشد،

$$\begin{aligned} a &= p_۱^{a_۱} p_۲^{a_۲} \cdots p_r^{a_r} \\ b &= p_۱^{b_۱} p_۲^{b_۲} \cdots p_r^{b_r} \\ c &= p_۱^{c_۱} p_۲^{c_۲} \cdots p_r^{c_r} \\ \vdots &\ \ \vdots \ \ \ \vdots \end{aligned}$$

که در آن p_iها اعداد اولی هستند که حداقل یکی از a، b، c، ... را عدد می‌کنند. در این صورت داریم

$$\begin{aligned} \gcd\{a, b, c, \ldots\} &= p_۱^{k_۱} p_۲^{k_۲} \cdots p_r^{k_r} \\ \operatorname{lcm}\{a, b, c, \ldots\} &= p_۱^{m_۱} p_۲^{m_۲} \cdots p_r^{m_r} \end{aligned}$$

که در آن $k_i = \min\{a_i, b_i, c_i, \ldots\}$، $m_i = \max\{a_i, b_i, c_i, \ldots\}$ به ازای هر i. □

نتیجه ۱۹.۱.۲. اگر $a, b \in \mathbb{N}$، آنگاه $\operatorname{lcm}\{a, b\} \cdot \gcd\{a, b\} = ab$.

اثبات. با استفاده از قضیه‌ی ۱۸.۱.۲، و این مطلب که برای اعداد صحیح m و n،

$$\max\{m, n\} + \min\{m, n\} = m + n,$$

حکم را می‌توان ثابت کرد. □

تعریف ۲۰.۱.۲. فرض کنید n عدد صحیح مثبت باشد، تعداد اعداد کوچک‌تر یا مساوی n که نسبت به n اول‌اند را با $\varphi(n)$ نشان می‌دهیم، یعنی

$$\varphi(n) = |\{m \in \mathbb{N} \mid m \leq n, \ \ \gcd\{m, n\} = ۱\}|.$$

$\varphi(n)$ را تابع فی اویلر می‌نامیم.

مثلاً $\varphi(۲) = ۱$، $\varphi(۳) = ۲$، $\varphi(۴) = ۲$؛ و اگر p عدد اول باشد، $\varphi(p) = p - ۱$. به طور کلی $\varphi(p^n) = p^n - p^{n-۱}$:

قضیه ۲۱.۱.۲. اگر p عدد اول باشد و $n \in \mathbb{N}$، آنگاه $\varphi(p^n) = p^n \left(۱ - \frac{۱}{p}\right)$.

اثبات. اگر $۱ \leq a \leq p^n$ و $\gcd\{a, p^n\} \neq ۱$، آنگاه چون p عددی اول است، $p|a$. بنابراین عدد k وجود دارد که $a = kp$. اما به ازای هر $۱ \leq k \leq p^{n-۱}$، $p \leq kp \leq p^n$. پس $p^{n-۱}$ عدد بین ۱ و p^n وجود دارند که نسبت به p^n اول نیستند. از این‌رو تعداد اعدادی که بین ۱ و p^n قرار دارند و نسبت به p^n اول‌اند عبارت است از

$$\varphi(p^n) = p^n - p^{n-۱} = p^n \left(۱ - \frac{۱}{p}\right). \qquad \square$$

تمرین‌ها

۱. قضیه‌های زیر را به استقرا ثابت کنید.
(الف) به ازای هر $n \in \mathbb{N}$، $۷^n - ۱$ ، ۶ را عاد می‌کند.
(ب) به ازای هر $n \in \mathbb{N}$، $۵^{۲n} + ۳$ ، ۴ را عاد می‌کند.

۲. فرض کنید a و b، c و d اعداد صحیح باشند و $a \neq ۰$. ثابت کنید
(الف) اگر $a|b$، آنگاه $a|bc$.
(ب) اگر $b \neq ۰$، $a|b$ و $b|c$، آنگاه به ازای هر $m, n \in \mathbb{Z}$، $a|(mb + nc)$.
(ج) اگر $a, b > ۰$ و $a|b$، آنگاه $a \leq b$.
(د) اگر $ac \neq ۰$ و $ac|bc$، آنگاه $a|b$.

۳. فرض کنید p عدد اول باشد، و m و n اعداد صحیح و r عدد صحیح مثبت. اگر $p^r|mn$ و $p \nmid m$ نشان دهید ، $p^r|n$.

۴. فرض کنید $a, b, c \in \mathbb{N}$، نشان دهید $\gcd\{ab, ac\} = a \gcd\{b, c\}$.

۵. به ازای هر $a, b, c \in \mathbb{N}$ اگر $\gcd\{a, b\} = ۱$ و $\gcd\{a, c\} = ۱$، نشان دهید $\gcd\{a, bc\} = ۱$.

۶. فرض کنید $a, b, c \in \mathbb{N}$. اگر $\gcd\{a, b\} = ۱$، $a|c$ و $b|c$، نشان دهید $ab|c$.

۷. اگر $a, b \in \mathbb{N}$، نشان دهید $\gcd\{a, b\} = \gcd\{a, a + b\}$.

۸. نشان دهید تعداد نامتناهی عدد اول به صورت $۶n - ۱$ وجود دارند، $n \geq ۲$.

۹. در هر حالت $\gcd\{m, n\}$ را بیابید و آن را بر حسب ترکیب خطی m و n بیان کنید.
(الف) $m = ۷۲$، $n = ۴۲$ (ب) $m = ۴۱$، $n = ۲۵$
(ج) $m = ۳۲۷$، $n = ۵۴$ (د) $m = ۳۲۷$، $n = ۲۹$
(هـ) $m = -۲۳۱$، $n = ۱۵۰$ (و) $m = ۷۲$، $n = -۱۷۵$.

۱۰. نشان دهید هر دو عدد فرد متوالی نسبت به هم اول‌اند.

۱۱. اگر p عدد اول باشد، نشان دهید به ازای هر n یا $p|n$ یا $\gcd\{p, n\} = ۱$.

۱۲. بزرگ‌ترین مقسوم‌علیه مشترک و کوچک‌ترین مضرب مشترک اعداد زیر را بیابید.
(الف) ۱۱۰، ۷۳۵ (ب) ۱۰۱، ۱۱۳ (ج) ۱۳۹، ۲۷۸

۱۳. فرض کنید $m, n \in \mathbb{N}$ و $\gcd\{m, n\} = ۱$. اگر $d|mn$ نشان دهید اعداد $m_۱$، $n_۱$ وجود دارند که $d = m_۱n_۱$ طوری که $m_۱|m$ و $n_۱|n$.

۱۴. تمرین ۱۳، را بدون فرض $\gcd\{m, n\} = ۱$ انجام دهید.

۱۵. اگر $a, b \in \mathbb{N}$ نشان دهید اعداد $u, v \in \mathbb{N}$ وجود دارند طوری که $u|a$، $v|b$، $\gcd\{u, v\} = ۱$ و $\operatorname{lcm}\{u, v\} = ab$.

۱۶. اگر q عدد گویایی باشد که $q^۲$ عدد صحیح است، نشان دهید q عدد صحیح است.

۱۷. (الف) نشان دهید هر عدد اول $p > ۲$ به صورت $p = ۴k + ۱$ یا $p = ۴k + ۳$ است.
(ب) اثبات قضیه‌ی ۱۵.۱.۲، را تغییر دهید و نشان دهید تعداد نامتناهی عدد اول به صورت $۴k + ۳$ وجود دارد.

۱۸. فرض کنید $m, n \in \mathbb{N}$.
(الف) فرض کنید $m = qn + r$، که در آن $q \in \mathbb{Z}$، r و $۰ \leq r < n$. نشان دهید $k \in \mathbb{Z}$ وجود دارد که $۲^{m-۱} = k(۲^n - ۱) + (۲^r - ۱)$، که در آن $۰ \leq ۲^r - ۱ \leq ۲^n - ۱$.
(ب) اگر $\gcd\{m, n\} = d$ نشان دهید $\gcd\{۲^m - ۱, ۲^n - ۱\} = ۲^d - ۱$.

۲.۲ اعداد صحیح به پیمانه‌ی n، $\mathbb{Z}_n$

فرض کنید n یک عدد طبیعی ثابت باشد. رابطه‌ی هم‌نهشتی به پیمانه‌ی n روی $\mathbb{Z}$ را چنین تعریف می‌کنیم.

$$\forall a, b \in \mathbb{Z}, \quad a \equiv b \mod n \iff n|(b-a).$$

بنابراین اگر b، a اعداد صحیح باشند، می‌گوییم a هم‌نهشت با b به پیمانه‌ی n است و می‌نویسیم $a \equiv b \mod n$، هرگاه $n|(b-a)$، یعنی $k \in \mathbb{Z}$ وجود داشته باشد که $b - a = nk$.
اگر $a \in \mathbb{Z}$، آنگاه $a - a = n \times ۰$، یعنی $a \equiv b \mod n$ بازتابی است. اگر $a, b \in \mathbb{Z}$ و $a \equiv b \mod n$، آنگاه $k \in \mathbb{Z}$ وجود دارد که $b - a = nk$. بنابراین $a - b = n(-k)$، یعنی $b \equiv a \mod n$ و $\equiv$ متقارن است. اگر $a, b, c \in \mathbb{Z}$ و $a \equiv b \mod n$ و $b \equiv c \mod n$، آنگاه $k_۱, k_۲ \in \mathbb{Z}$ وجود دارند که $b - a = nk_۱$ و $c - b = nk_۲$. بنابراین $c - a = n(k_۱ + k_۲)$ و $\equiv$ ترایا است. در نتیجه رابطه‌ی هم‌نهشتی به پیمانه‌ی n روی $\mathbb{Z}$ یک رابطه‌ی هم‌ارزی است. اگر $a \in \mathbb{Z}$، رده‌ی هم‌ارزی شامل a را با $\bar{a}$ نشان می‌دهیم. پس

$$\begin{aligned} \bar{a} &= \{b \in \mathbb{Z} \mid a \equiv b \mod n\} \\ &= \{b \in \mathbb{Z} \mid \exists k \in \mathbb{Z}, \quad b = a + nk\} \\ &= \{a + nk \mid k \in \mathbb{Z}\}. \end{aligned}$$

هم‌چنین مجموعه‌ی رده‌های هم‌ارزی یک افراز $\mathbb{Z}$ را به دست می‌دهند، به ویژه

$$\bar{a} = \bar{b} \iff a \equiv b \mod n.$$

بنابراین n رده‌ی هم‌ارزی متمایز وجود دارد : $\bar{۰}$، $\bar{۱}$، ...، $\overline{n-۱}$. در واقع اگر a عدد صحیح دلخواهی باشد، آنگاه بنا به الگوریتم تقسیم اعداد صحیح r و q وجود دارند که $a = qn + r$ و $۰ \le r \le n-۱$. در نتیجه $n|(a-r)$ و $a \equiv r \mod n$، یعنی $\bar{a} = \bar{r}$.
بنابراین هر رده هم‌ارزی در فهرست $\bar{۰}$، $\bar{۱}$، ...، $\overline{n-۱}$ قرار دارد. به علاوه این رده‌های هم‌ارزی نیز متمایزند. زیرا اگر $\bar{r} = \bar{s}$، که در آن $۰ \le r, s \le n-۱$ و مثلاً $r \le s$، آنگاه $n|(s-r)$ و $۰ \le s - r \le n-۱$، که نتیجه می‌دهد $r = s$.
اگر $\bar{a}$ یک رده‌ی هم‌ارزی باشد عضو a را یک نماینده‌ی این رده گوییم. بنابراین ۰ یک نماینده‌ی $\bar{۰}$ است. هم‌چنین مثلاً $\bar{n} = \bar{۰}$، پس n نیز یک نماینده‌ی $\bar{n} = \bar{۰}$ است. مجموعه‌ی رده‌های هم‌ارزی را با $\mathbb{Z}_n$ نشان می‌دهیم، یعنی

$$\mathbb{Z}_n = \{\bar{۰}, \bar{۱}, \ldots, \overline{n-۱}\}$$

و آن را مجموعه‌ی رده‌های مانده‌ای به پیمانه‌ی n می‌نامیم. بنابراین $|\mathbb{Z}_n| = n$.

مثال ۱.۲.۲. عناصر $\overline{۷۹}$ و $\overline{-۶۶}$ را در $\mathbb{Z}_۶ = \{\bar{۰}, \bar{۱}, \bar{۲}, \bar{۳}, \bar{۴}, \bar{۵}\}$ مشخص کنید.

حل چون $۷۹ \equiv ۱ \mod ۶$ و $-۶۶ \equiv ۰ \mod ۶$ داریم $\bar{۱} = \overline{۷۹}$ و $\bar{۰} = \overline{-۶۶}$. □

مثال ۲.۲.۲. در $\mathbb{Z}_n$ نشان دهید $\bar{a} = \bar{۰}$ اگر و تنها اگر $n|a$.

حل داریم $\bar{a} = \bar{۰}$ اگر و تنها اگر $a \equiv ۰ \mod n$ اگر و تنها اگر $n|a$. □

روی $\mathbb{Z}_n$ یک عمل جمع تعریف می‌کنیم: برای هر $\bar{a}, \bar{b} \in \mathbb{Z}_n$ تعریف می‌کنیم

$$\bar{a} + \bar{b} = \overline{a+b}.$$

آیا تعریف فوق واقعاً یک عمل دوتایی است؟ یعنی آیا جمع فوق خوش تعریف است؟ در واقع بله. ثابت می‌کنیم عمل جمع بستگی به انتخاب نماینده از رده‌های هم‌ارزی ندارد ، یعنی ثابت می‌کنیم اگر $\bar{a} = \bar{a}_۱$ و $\bar{b} = \bar{b}_۱$، آنگاه $\overline{a+b} = \overline{a_۱ + b_۱}$. چون $\bar{a} = \bar{a}_۱$، عضو $r \in \mathbb{Z}$ وجود دارد که $a - a_۱ = rn$. به همین نحو عضو $s \in \mathbb{Z}$ وجود دارد که $b - b_۱ = sn$. با جمع دو رابطه‌ی اخیر داریم

$$(a - a_۱) + (b - b_۱) = (r+s)n$$

یا

$$(a+b)-(a_۱+b_۱)=(r+s)n.$$

این یعنی $a+b\equiv a_۱+b_۱ \mod n$ و $\overline{a+b}=\overline{a_۱+b_۱}$. به عنوان مثال در $\mathbb{Z}_۶$ داریم $\bar{۲}+\bar{۳}=\bar{۵}=\bar{۸}=\bar{۱}$ و در $\mathbb{Z}_۷$ داریم $\bar{۵}+\bar{۳}=\bar{۸}=\bar{۱}$. حال که خوش‌تعریفی عمل جمع ثابت شد به راحتی می‌توان قضیه‌ی زیر را ثابت کرد.

قضیه ۳.۲.۲. اگر $n\geq ۲$ عدد صحیح ثابتی باشد، آنگاه به ازای همه‌ی اعداد صحیح a، b و c قضیه‌های زیر در $\mathbb{Z}_n$ برقرارند.
(الف) $\bar{a}+\bar{b}=\bar{b}+\bar{a}$. یعنی عمل جمع در $\mathbb{Z}_n$ تعویض‌پذیر است.
(ب) $\bar{a}+(\bar{b}+\bar{c})=(\bar{a}+\bar{b})+\bar{c}$. یعنی عمل جمع در $\mathbb{Z}_n$ شرکت‌پذیر است.
(ج) $\bar{a}+\bar{۰}=\bar{a}$. یعنی $\bar{۰}$ عضو بی‌اثر عمل جمع در $\mathbb{Z}_n$ است.
(د) $\bar{a}+\overline{-a}=\bar{۰}$. یعنی برای هر عضو، عضو قرینه (عضو وارون نسبت به عمل جمع) در $\mathbb{Z}_n$ وجود دارد.

اثبات. (ب) را ثابت می‌کنیم. اثبات سایر قسمت‌ها به طور مشابه است و به عنوان تمرین واگذار می‌شود. شرکت‌پذیری در $\mathbb{Z}_n$ با استفاده از شرکت‌پذیری در $\mathbb{Z}$ ثابت می‌شود:

$$\begin{aligned}\bar{a}+(\bar{b}+\bar{c}) &= \bar{a}+\overline{b+c}\\ &= \overline{a+(b+c)}\\ &= \overline{a+b}+\bar{c}\\ &= (\bar{a}+\bar{b})+\bar{c}.\end{aligned}$$

پس عمل جمع روی $\mathbb{Z}_n$ شرکت‌پذیر است. □

روی $\mathbb{Z}_n$ یک عمل ضرب نیز تعریف می‌شود:

$$\bar{a}\bar{b}=\overline{ab}.$$

مثل قبل ثابت می‌شود عمل ضرب خوش تعریف است: اگر $\bar{a}=\bar{a_۱}$ و $\bar{b}=\bar{b_۱}$، آنگاه به ازای $r,s\in\mathbb{Z}$ داریم $a=a_۱+rn$ و $b=b_۱+sn$. در نتیجه

$$ab=a_۱b_۱+(a_۱s+b_۱r+srn)n.$$

بنابراین $ab\equiv a_۱b_۱ \mod n$، یعنی $\overline{ab}=\overline{a_۱b_۱}$. حال که خوش‌تعریفی عمل ضرب ثابت شد به راحتی می‌توان قضیه‌ی زیر را ثابت کرد.

قضیه ۴.۲.۲. اگر $n\geq ۲$ عدد صحیح ثابتی باشد، آنگاه به ازای همه‌ی اعداد صحیح a، b و c قضیه‌های زیر در $\mathbb{Z}_n$ برقرارند.
(الف) $\bar{a}\bar{b}=\bar{b}\bar{a}$، یعنی عمل ضرب در $\mathbb{Z}_n$ تعویض‌پذیر است.
(ب) $\bar{a}(\bar{b}\bar{c})=(\bar{a}\bar{b})\bar{c}$، یعنی عمل ضرب در $\mathbb{Z}_n$ شرکت‌پذیر است.
(ج) $\bar{a}\bar{۱}=\bar{a}$، یعنی $\bar{۱}$ عضو بی‌اثر عمل ضرب در $\mathbb{Z}_n$ است
(د) $\bar{a}(\bar{b}+\bar{c})=\bar{a}\bar{b}+\bar{a}\bar{c}$، یعنی عمل ضرب نسبت به عمل جمع در $\mathbb{Z}_n$ توزیع‌پذیر است. □

قضیه ۵.۲.۲. اگر $\bar{a}\in\mathbb{Z}_n$، آنگاه $\bar{۰}=\bar{a}\bar{۰}=\bar{۰}\bar{a}$.

اثبات. طبق قانون توزیع‌پذیری داریم $\bar{a}\bar{۰}+\bar{a}\bar{۰}=\bar{a}(\bar{۰}+\bar{۰})=\bar{a}\bar{۰}$. اگر به طرفین تساوی اخیر $-\bar{a}\bar{۰}$ را اضافه کنیم خواهیم داشت $\bar{a}\bar{۰}=\bar{۰}$. چون ضرب تعویض‌پذیر است، داریم $\bar{a}\bar{۰}=\bar{۰}\bar{a}=\bar{۰}$، که حکم را ثابت می‌کند. □

توجه کنید مشابه قسمت (د) قضیه‌ی ۳.۲.۲، برای عمل ضرب لزوماً برقرار نیست. یعنی ممکن است عضوی از $\mathbb{Z}_n$ نسبت به عمل ضرب وارون نداشته باشد، یعنی برای هر $\bar{a}\in\mathbb{Z}_n$ لزوماً عضو $\bar{b}\in\mathbb{Z}_n$ وجود ندارد که $\bar{a}\bar{b}=\bar{۱}$. به عنوان مثال $\bar{۰}$ در $\mathbb{Z}_n$ وارون ندارد (زیرا $\bar{۱}\neq\bar{۰}=\bar{۰}\bar{a}$). عضو $\bar{a}\in\mathbb{Z}_n$ را وارون‌پذیر گوییم هرگاه $\bar{b}\in\mathbb{Z}_n$ وجود داشت باشد که $\bar{a}\bar{b}=\bar{۱}$. آیا همه اعضای $\mathbb{Z}_n$ (به‌جز $\bar{۰}$) وارون

دارند؟ در واقع در حالت کلی نه؟ مثلاً در $\mathbb{Z}_۴$ عضو $\bar{۲}$ وارون ندارد. زیرا اگر $\bar{۲}\bar{a} = \bar{۱}$، آنگاه $\bar{۲}(\bar{۲}\bar{a}) = \bar{۲}\bar{۱} = \bar{۲}$ و $\bar{۴}\bar{a} = \bar{۰}$، یعنی $\bar{۲}$، که تناقض است. باید ببینیم که در $\mathbb{Z}_n$ چه موقع یک عضو وارون‌پذیر است. فرض کنید $\bar{a} \in \mathbb{Z}_n$ داریم

$$\begin{aligned} \bar{a} \text{ وارون‌پذیر} &\iff \exists \bar{b} \in \mathbb{Z}_n,\ \bar{b}\bar{a} = \bar{۱} \\ &\iff \exists b \in \mathbb{Z},\ n|(۱ - ba) \\ &\iff \exists b, k \in \mathbb{Z},\ ba + kn = ۱ \\ &\iff \gcd\{a, n\} = ۱ \end{aligned}$$

پس ثابت کرده‌ایم:

قضیه ۶.۲.۲. $\bar{a} \in \mathbb{Z}_n$ وارون پذیر است اگر و تنها اگر $\gcd\{a, n\} = ۱$. □

مجموعه‌ی اعضای وارون‌پذیر $\mathbb{Z}_n$ را با $\mathbb{Z}_n^\times$ نشان می‌دهیم. طبق قضیه‌ی ۶.۲.۲، داریم

$$\mathbb{Z}_n^\times = \{\bar{a} \in \mathbb{Z}_n \mid \gcd\{a, n\} = ۱\}.$$

مثلاً

$$\mathbb{Z}_۲^\times = \{\bar{۱}\}, \quad \mathbb{Z}_۳^\times = \{\bar{۱}, \bar{۲}\}, \quad \mathbb{Z}_۴^\times = \{\bar{۱}, \bar{۳}\}, \quad \mathbb{Z}_۵^\times = \{\bar{۱}, \bar{۲}, \bar{۳}, \bar{۴}\}, \quad \dots$$

بنابراین ثابت کردیم که $\mathbb{Z}_n$ همراه با عمل جمع،یک گروه متناهی با مرتبه‌ی n و $\mathbb{Z}_n^\times$ همراه با عمل ضرب، یک گروه متناهی با مرتبه‌ی $\varphi(n)$ است.
اکنون جدول ضرب و جمع $\mathbb{Z}_۶ = \{\bar{۰}, \bar{۱}, \bar{۲}, \bar{۳}, \bar{۴}, \bar{۵}\}$ را در نظر بگیرید

$+$	$\bar{۰}$	$\bar{۱}$	$\bar{۲}$	$\bar{۳}$	$\bar{۴}$	$\bar{۵}$
$\bar{۰}$	$\bar{۰}$	$\bar{۱}$	$\bar{۲}$	$\bar{۳}$	$\bar{۴}$	$\bar{۵}$
$\bar{۱}$	$\bar{۱}$	$\bar{۲}$	$\bar{۳}$	$\bar{۴}$	$\bar{۵}$	$\bar{۰}$
$\bar{۲}$	$\bar{۲}$	$\bar{۳}$	$\bar{۴}$	$\bar{۵}$	$\bar{۰}$	$\bar{۱}$
$\bar{۳}$	$\bar{۳}$	$\bar{۴}$	$\bar{۵}$	$\bar{۰}$	$\bar{۱}$	$\bar{۲}$
$\bar{۴}$	$\bar{۴}$	$\bar{۵}$	$\bar{۰}$	$\bar{۱}$	$\bar{۲}$	$\bar{۳}$
$\bar{۵}$	$\bar{۵}$	$\bar{۰}$	$\bar{۱}$	$\bar{۲}$	$\bar{۳}$	$\bar{۴}$

$\times$	$\bar{۰}$	$\bar{۱}$	$\bar{۲}$	$\bar{۳}$	$\bar{۴}$	$\bar{۵}$
$\bar{۰}$	$\bar{۰}$	$\bar{۰}$	$\bar{۰}$	$\bar{۰}$	$\bar{۰}$	$\bar{۰}$
$\bar{۱}$	$\bar{۰}$	$\bar{۱}$	$\bar{۲}$	$\bar{۳}$	$\bar{۴}$	$\bar{۵}$
$\bar{۲}$	$\bar{۰}$	$\bar{۲}$	$\bar{۴}$	$\bar{۰}$	$\bar{۲}$	$\bar{۴}$
$\bar{۳}$	$\bar{۰}$	$\bar{۳}$	$\bar{۰}$	$\bar{۳}$	$\bar{۰}$	$\bar{۳}$
$\bar{۴}$	$\bar{۰}$	$\bar{۴}$	$\bar{۲}$	$\bar{۰}$	$\bar{۴}$	$\bar{۲}$
$\bar{۵}$	$\bar{۰}$	$\bar{۵}$	$\bar{۴}$	$\bar{۳}$	$\bar{۲}$	$\bar{۱}$

این دو جدول تفاوتهای زیادی را که بین محاسبه در $\mathbb{Z}_۶$ و $\mathbb{Z}$ وجود دارد را نشان می‌دهند. مثلاً ۰، ۱ در $\mathbb{Z}$ تنها عناصر $k \in \mathbb{Z}$ هستند که در خاصیت $k^۲ = k$ صدق می‌کنند. اما در $\mathbb{Z}_۶$ این عناصر عبارت‌اند از $\bar{۰}$، $\bar{۱}$، $\bar{۳}$، $\bar{۴}$. تفاوت دیگر این است که در $\mathbb{Z}$ قانون حذف برقرار است، یعنی اگر $ab = ac$ و $a \neq ۰$، آنگاه $b = c$. اما در $\mathbb{Z}_۶$ این خاصیت برقرار نیست، زیرا مثلاً در $\mathbb{Z}_۶$ داریم $\bar{۵} \cdot \bar{۴} = \bar{۲} \cdot \bar{۴}$ و $\bar{۴} \neq \bar{۰}$ اما $\bar{۵} \neq \bar{۲}$. در $\mathbb{Z}$ اگر $ab = ۰$، آنگاه یا $a = ۰$ یا $b = ۰$. اما در $\mathbb{Z}_۶$ این خاصیت برقرار نیست، زیرا مثلاً در $\mathbb{Z}_۶$ داریم $\bar{۲} \cdot \bar{۳} = \bar{۰}$ اما $\bar{۲} \neq \bar{۰}$ و $\bar{۳} \neq \bar{۰}$.

مثال ۷.۲.۲. باقیمانده تقسیم $۴^{۱۱۹}$ بر ۷ را بیابید.

حل باید عدد r را طوری بیابیم که $۰ \leq r \leq ۶$ و $۴^{۱۱۹} \equiv r \mod ۷$. این محاسبه را در $\mathbb{Z}_۷$ انجام می‌دهیم. چون ، در $\mathbb{Z}_۷$، $\bar{۴}^{۲} = \bar{۲}$ داریم $\bar{۴}^{۳} = \bar{۸} = \bar{۱}$. با در نظر گرفتن این مطلب ۱۱۹ را بر ۳ تقسیم می‌کنیم: $۱۱۹ = ۳ \times ۳۹ + ۲$. پس

$$\bar{۴}^{۱۱۹} = \bar{۴}^{۳ \times ۳۹ + ۲} = (\bar{۴}^{۳})^{۳۹} \times \bar{۴}^{۲} = \bar{۱}^{۳۹} \times \bar{۲} = \bar{۲}.$$

بنابراین $۴^{۱۱۹} \equiv ۲ \mod ۷$ و با باقیمانده مورد نظر ۲ است. □

مثال ۸.۲.۲. با یافتن وارون $\overline{۱۶}$ در $\mathbb{Z}_{۳۵}$ معادله‌ی $\overline{۱۶}x = \bar{۹}$ را در $\mathbb{Z}_{۳۵}$ حل کنید.

حل چون ۱۶ و ۳۵ نسبت به هم اول‌اند پس وارون $\overline{۱۶}$ در $\mathbb{Z}_{۳۵}$ وجود دارد. با استفاده از الگوریتم اقلیدسی داریم

$$۳۵ = ۲ \times ۱۶ + ۳ \quad و \quad ۱۶ = ۵ \times ۳ + ۱.$$

پس $۳۵ \times ۵ - ۱۶ \times ۱۱ = ۱۶ - ۵(۳۵ - ۲ \times ۱۶) = ۱$. بنابراین $۱۶ \times ۱۱ \equiv ۱ \mod ۳۵$، و $\overline{۱۱}$ وارون $\overline{۱۶}$ در $\mathbb{Z}_{۳۵}$ است. اکنون دو طرف معادله‌ی $\overline{۱۶}x = \overline{۹}$ را در $\overline{۱۱}$ ضرب می‌کنیم و به دست می‌آوریم $\overline{۱۶}x = \overline{۹} \times \overline{۱۱}$؛ یعنی $x = \overline{۹۹} = \overline{۲۹}$. □

مثال ۹.۲.۲. دستگاه معادله‌ی زیر را در $\mathbb{Z}_{۱۱}$ حل کنید

$$\begin{cases} \bar{۵}x + \bar{۸}y = \bar{۲} \\ \bar{۳}x + \bar{۲}y = \bar{۱}. \end{cases}$$

حل روش متعارف حذفی در حل دستگاه را به کار می‌بریم. برای حذف y معادله‌ی دوم را در $\bar{۴}$ ضرب می‌کنیم و به دست می‌آوریم

$$x + \bar{۸}y = \bar{۴}.$$

(توجه کنید $\bar{۱}x = x$ زیرا $x \in \mathbb{Z}_{۱۱}$). معادله‌ی اخیر را از معادله‌ی اول کم می‌کنیم و به دست می‌آوریم $\bar{۴}x = -\bar{۲} = \bar{۹}$. اکنون چون $\bar{۳}$ وارون $\bar{۴}$ در $\mathbb{Z}_{۱۱}$ است،با ضرب معادله‌ی اخیر در $\bar{۳}$ داریم $x = \bar{۳} \times \bar{۹} = \bar{۵}$. سپس با استفاده این نتیجه در معادله‌ی دوم داریم

$$\bar{۲}y = \bar{۱} - \bar{۳}x = \bar{۱} - \bar{۳} \times \bar{۵} = -\overline{۱۴} = \bar{۸}.$$

در نهایت چون $\bar{۶}$ وارون $\bar{۲}$ است، داریم $y = \bar{۶} \times \bar{۸} = \bar{۴}$. □

فرض کنید a عددی حقیقی باشد، اگر $\left(\frac{۱}{۲}a\right)^۲$ را به عبارت $x^۲ + ax$ اضافه کنیم مربع کامل خواهد شد:

$$x^۲ + ax + \left(\frac{۱}{۲}a\right)^۲ = \left(x + \frac{۱}{۲}a\right)^۲.$$

این روند را کامل کردن مربع گوییم، و هرگاه $\bar{۲}$ در $\mathbb{Z}_n$ وارون داشته باشد (یعنی وقتی n فرد باشد) این کار را در $\mathbb{Z}_n$ نیز می‌توان انجام داد.

مثال ۱۰.۲.۲. معادله‌ی $x^۲ + \bar{۳}x + \bar{۹} = \bar{۵}$ را در $\mathbb{Z}_{۱۳}$ حل کنید.

حل ابتدا $\bar{۹}$ را از دو طرف معادله کم می‌کنیم:

$$x^۲ + \bar{۳}x = -\bar{۹} = \bar{۴}.$$

چون $\bar{۷}$ وارون $\bar{۲}$ در $\mathbb{Z}_{۱۳}$ است، با اضافه کردن $\overline{۱۲} = \bar{۸}^۲ = (\bar{۳} \times \bar{۷})^۲$ به دو طرف تساوی، در سمت چپ مربع را کامل می‌کنیم:

$$x^۲ + \bar{۳}x + \overline{۱۲} = \bar{۴} + \overline{۱۲} \quad یا \quad (x + \bar{۸})^۲ = \bar{۳}.$$

اکنون با امتحان ۱۳ عضو $\mathbb{Z}_{۱۳}$ می‌بینیم تنها دو عضو $\bar{۴}$ و $\bar{۹} = -\bar{۴}$ ریشه‌ی دوم $\bar{۳}$ هستند. در نتیجه $x + \bar{۸} = \bar{۴}$ یا $x + \bar{۸} = \bar{۹}$. پس $x = \bar{۱}$ و $x = \bar{۹}$ جواب‌های معادله‌اند. □

توجه کنید در مثال قبل دو جواب برای معادله به دست آوردیم و دلیل آن این بود که $\bar{۳}$ در $\mathbb{Z}_{۱۳}$ تنها دو "ریشه‌ی دوم" دارد : $\bar{۴}$ و $\bar{۹} = -\bar{۴}$.
اما حالت های دیگر نیز امکانپذیر است: در $\mathbb{Z}_۷$، $\bar{۳}$ ریشه‌ی دوم ندارد ، اما در $\mathbb{Z}_{۲۷}$، $\bar{۹}$ شش تا ریشه‌ی دوم دارد ، $\bar{۳}$ و $\overline{۲۴} = -\bar{۳}$، $\bar{۶}$ و $\overline{۲۱} = -\bar{۶}$، و درنهایت $\overline{۱۲}$ و $\overline{۱۵} = -\overline{۱۲}$.
اعداد صحیح ۱ و -۱ تنها عناصر $\mathbb{Z}$ هستند که وارون دارند (زیرا اگر $k \neq ۱, -۱$، $\frac{۱}{k}$ در $\mathbb{Z}$ نیست). از طرف دیگر هر عدد حقیقی ناصفر x در $\mathbb{R}$ وارون دارد : $\frac{۱}{x}$. در قضیه‌ی بعد وضعیت را در $\mathbb{Z}_n$ بررسی می‌کنیم.

قضیه ۱۱.۲.۲. به ازای هر عدد صحیح $n \geq ۲$ شرایط زیر معال‌اند.
(الف) هر عضو $\bar{a} \neq \bar{۰}$ در $\mathbb{Z}_n$ وارون دارد.
(ب) اگر در $\mathbb{Z}_n$، $\bar{a}\bar{b} = \bar{۰}$، آنگاه $\bar{a} = \bar{۰}$ یا $\bar{b} = \bar{۰}$.
(ج) n اول است.

اثبات. ثابت می‌کنیم (الف)$\Longleftarrow$(ب)، (ب)$\Longleftarrow$(ج)، و (ج)$\Longleftarrow$(الف)
(الف)$\Longleftarrow$(ب) فرض کنید (الف) درست باشد و در $\mathbb{Z}_n$، $\bar{a}\bar{b} = \bar{۰}$. اگر $\bar{a} = \bar{۰}$ چیزی برای اثبات نیست. پس فرض کنید $\bar{a} \neq \bar{۰}$. طبق فرض $\bar{a}$ وارون دارد ، مثلاً $\bar{c}\bar{a} = \bar{۱}$. با ضرب کردن $\bar{c}$ در دو طرف تساوی $\bar{a}\bar{b} = \bar{۰}$ داریم $\bar{c}\bar{a}\bar{b} = \bar{c}\bar{۰} = \bar{۰}$؛ یعنی $\bar{b} = \bar{۰}$.
(ب)$\Longleftarrow$(ج) اگر n اول نباشد می‌توان نوشت $n = ab$، که در آن $۲ \leq a \leq n$ و $۲ \leq b \leq n$. اما در این صورت، $\bar{a}\bar{b} = \bar{n} = \bar{۰}$، که در آن $\bar{a} \neq \bar{۰}$ و $\bar{b} \neq \bar{۰}$ و این تناقض با (ب) است. پس ادعای اول نبودن n درست نیست.
(ج)$\Longleftarrow$(الف) اگر n اول باشد و $\bar{a} \neq \bar{۰}$، آنگاه $\gcd\{a, n\} = ۱$ (زیرا در غیر این صورت $\gcd\{a, n\} = n$، و $n|a$). بنابراین اعداد صحیح b، c وجود دارند که $۱ = ba + cn$. پس $ba \equiv ۱ \mod n$ و در نتیجه $\bar{b}\bar{a} = \bar{۱}$، یعنی $\bar{a}$ وارون‌پذیر است. □

قضیه ۱۲.۲.۲. (قضیه‌ی فرما) اگر p عدد اول باشد، آنگاه به ازای هر عدد صحیح a داریم

$$a^p \equiv a \mod p.$$

در واقع به ازای هر عدد صحیح a که نسبت به p اول است داریم $a^{p-۱} \equiv ۱ \mod p$.

اثبات. باید نشان دهیم در $\mathbb{Z}_p$، $\bar{a}^p = \bar{a}$. چون این رابطه برای $\bar{a} = \bar{۰}$ درست است، کافی است نشان دهیم در $\mathbb{Z}_p$، برای $\bar{a} \neq \bar{۰}$، $\bar{a}^{p-۱} = \bar{۱}$. اما اگر $\bar{a} \neq \bar{۰}$، آنگاه $\bar{a}$ در $\mathbb{Z}_p$ وارون دارد ، مثلاً $\bar{b}\bar{a} = \bar{۱}$. اکنون همه‌ی اعضای ناصفر $\mathbb{Z}_p$ را در $\bar{a}$ ضرب می‌کنیم:

$$\bar{a}\bar{۱}, \bar{a}\bar{۲}, \ldots, \bar{a}\overline{p-۱}.$$

همه این عناصر متمایزند (زیرا پس از ضرب $\bar{a}\bar{r} = \bar{a}\bar{s}$ در $\bar{b}$ نتیجه می‌شود $\bar{r} = \bar{s}$) و هیچ‌کدام برابر $\bar{۰}$ نیستند. پس

$$\{\bar{a}\bar{۱}, \bar{a}\bar{۲}, \ldots, \bar{a}\overline{p-۱}\} = \{\bar{۱}, \bar{۲}, \ldots, \overline{p-۱}\}.$$

به ویژه حاصل‌ضرب اعضای مجموعه‌های فوق برابرند:

$$\bar{a}^{p-۱}\bar{۱}\bar{۲}\cdots\overline{p-۱} = \bar{۱}\bar{۲}\cdots\overline{p-۱}.$$

اما $\bar{۱}\bar{۲}\cdots\overline{p-۱}$ در $\mathbb{Z}_p$ وارون دارد (تمرین ۷ را ببینید). بنابراین با ضرب تساوی در وارون آن داریم $\bar{a}^{p-۱} = \bar{۱}$. □

معمولاً وقتی در $\mathbb{Z}_n$ کار می‌کنیم به‌جای $\bar{a}$ می‌نویسیم a. بنابراین مثلاً $\mathbb{Z}_۵$ را به صورت $\mathbb{Z}_۵ = \{۰, ۱, ۲, ۳, ۴\}$ می‌نویسیم، و تساویهایی مثل $۲ = ۴ \times ۳$ و $۰ = ۳ + ۲$ را در $\mathbb{Z}_۵$ داریم. البته هرگاه که بیم ابهام در محاسبه‌ها باشد از همان نماد $\bar{a}$ استفاده می‌کنیم.

تمرین‌ها

۱. همه اعداد صحیح $k \geq ۲$ را بیابید که در $k^۲ \equiv ۵k \mod ۱۵$ صدق می‌کنند.
۲. باقیمانده تقسیم دو عدد داده شده را بیابید
(الف) $۱۰^{۵۱۵}$ بر ۷ (ب) $۸^{۳۹۱}$ بر ۵
(ج) $۷^{۳۴۸}$ بر ۱۱ (د) $۳^{۳۲۳}$ بر ۷
۳. نشان دهید به ازای هر عدد صحیح a، ۷ شمارنده‌ها $a^۳ + ۲$ نیست.
۴. نشان دهید به ازای هر عدد صحیح a، در $\mathbb{Z}_۶$ داریم $\bar{a}^۳ = \bar{a}$.

۵. معادله‌های زیر را، در صورت امکان، حل کنید.
(الف) $\bar{۹}=\overline{۱۳}x$، در $\mathbb{Z}_{۳۵}$. (ب) $\overline{۱۲}=\bar{۷}x$، در $\mathbb{Z}_{۲۵}$.
(ج) $\overline{۱۶}=\overline{۱۱}x$، در $\mathbb{Z}_{۲۰}$. (د) $\overline{۱۴}=\bar{۹}x$، در $\mathbb{Z}_{۱۶}$.

۶. اگر $\bar{a}$ در $\mathbb{Z}_n$ وارون داشته باشد و $\bar{a}\bar{b}=\bar{a}\bar{c}$، نشان دهید $\bar{b}=\bar{c}$.

۷. اگر $\bar{a_۱}$، $\bar{a_۲}$، ...، $\bar{a_k}$ در $\mathbb{Z}_n$ وارون داشته باشند نشان دهید $\bar{a_۱}\bar{a_۲}\cdots\bar{a_k}$ نیز در $\mathbb{Z}_n$ وارون دارد.

۸. معادله‌های زیر را، در صورت امکان، حل کنید.

(الف) $\begin{cases}\bar{۳}x+\bar{۴}y=\bar{۱}\\ \bar{۲}x+\ y=\bar{۱}\end{cases}$ در $\mathbb{Z}_۷$ (ب) $\begin{cases}\bar{۳}x+\bar{۲}y=\bar{۱}\\ \bar{۵}x+\ y=\bar{۱}\end{cases}$ در $\mathbb{Z}_{۱۱}$

(ج) $\begin{cases}\bar{۳}x+\bar{۴}y=\bar{۱}\\ \bar{۲}x+\ y=\bar{۱}\end{cases}$ در $\mathbb{Z}_۵$ (د) $\begin{cases}\bar{۳}x+\bar{۲}y=\bar{۱}\\ \bar{۵}x+\ y=\bar{۱}\end{cases}$ در $\mathbb{Z}_۷$

(هـ) $\begin{cases}\bar{۳}x+\bar{۴}y=\bar{۱}\\ \bar{۲}x+\bar{۳}y=\bar{۴}\end{cases}$ در $\mathbb{Z}_۵$ (و) $\begin{cases}\bar{۳}x+\bar{۲}y=\bar{۱}\\ \bar{۵}x+\ y=\bar{۴}\end{cases}$ در $\mathbb{Z}_۷$

۹. جواب معادله‌های زیر را، در صورت وجود، بیابید.
(الف) $x^۲+\bar{۵}x+\bar{۴}=\bar{۰}$، در $\mathbb{Z}_۷$. (ب) $\bar{۲}x^۲+\bar{۳}x+\bar{۱}=\bar{۰}$، در $\mathbb{Z}_۵$.
(ج) $x^۲+\bar{۴}x+\bar{۳}=\bar{۰}$، در $\mathbb{Z}_۵$. (د) $x^۲+\bar{۶}x+\bar{۵}=\bar{۰}$، در $\mathbb{Z}_۹$.

۱۰. فرض کنید $p\geq ۳$ عدد اول باشد. نشان دهید هر عضو $\mathbb{Z}_p$ ریشه‌ی $(p-۲)$ام دارد.

۱۱. فرض کنید p عدد اول باشد.
(الف) اگر در $\mathbb{Z}_p$، $x^۲=\bar{۱}$، نشان دهید $x=\bar{۱}$ یا $x=-\bar{۱}$.
(ب) قضیه‌ی ویلسون را ثابت کنید: $(p-۱)!\equiv -۱ \mod p$.

۱۲. (الف) فرض کنید p عدد اول به صورت $p=۴n+۱$ باشد و $x=\frac{p-۱}{۲}!$. ثابت کنید در $\mathbb{Z}_p$، $x^۲=-\bar{۱}$.
(ب) فرض کنید p عدد اول به صورت $۴n+۳$ باشد. نشان دهید معادله‌ی $x^۲=-\bar{۱}$ در $\mathbb{Z}_p$ جواب ندارد.

۱۳. (الف) فرض کنید رابطه‌ی $a^n\equiv a \mod n$ به ازای همه‌ی اعداد صحیح a برقرار باشد. نشان دهید n باید آزاد از مربع (یعنی حاصل‌ضرب اعداد اول متمایز) باشد.
(ب) نشان دهید به ازای هر عدد صحیح a داریم $a^{۵۶۱}\equiv a \mod ۵۶۱$.

فصل ۳

گروه‌ها

در این فصل خواص اساسی گروه‌ها را به صورت مجرد بررسی می‌کنیم. نظریه‌ی گروه‌ها از قدیمی‌ترین شاخ‌های جبر است. منشاء آن از نظریه‌ی ریشه‌ی چندجمله‌ای‌هاست. ابتدای قرن نوزدهم میلادی ریاضی‌دانان فرمول‌هایی برای محاسبه‌ی ریشه‌های چندجمله‌ای‌های درجه‌ی سه و چهار (شبیه فرمول ریشه‌ی چندجمله‌ای‌های درجه‌ی دو) با استفاده از رادیکال‌ها به دست آوردند. معروف‌ترین ریاضی‌دانان آن زمان برای پیدا کردن فرمولی برای ریشه‌های چندجمله‌ای‌های درجه‌ی پنج تلاش می‌کردند. هنگامی که نیلز هنریک آبل (۱۸۲۹ – ۱۸۰۲) ثابت کرد چنین فرمولی وجود ندارد باعث حیرت فراوان شد. در همین سال‌ها اواریست گالوا (۱۸۳۲ – ۱۸۱۱) نشان داد که به هر چندجمله‌ای درجه n یک گروه جایگشتی از ریشه‌های چندجمله‌ای متناظر می‌شود او ثابت کرد که یک چندجمله‌ای با استفاده از رادیکال‌ها حل‌پذیر است اگر و تنها اگر این گروه خاصیت معینی (که اکنون آن را گروه حل‌پذیر می‌نامیم) داشته باشد. به ویژه این حقیقت که گروه A_n متشکل از همه‌ی جایگشت‌های زوج روی n حرف برای $n \geq ۵$ حل‌پذیر نیست، نتیجه می‌دهد که فرمولی برای چندجمله‌ای‌های با درجه $n \geq ۵$ وجود ندارد. این کارها به شاخه‌ای از جبر که هم اکنون به نظریه‌ی گالوا معروف است منجر شد. کار گالوا تا پس از مرگش در سن ۲۰ سالگی نافهمیده باقی‌مانده بود. گالوا با گروه‌های جایگشتی کار می‌کرد. سپس در سال ۱۸۴۵ آرتور کیلی (۱۸۹۰ – ۱۸۲۱) مفهوم گروه مجرد را فرمول‌بندی کرد. در این فصل و فصل‌های ۴ تا ۹ نظریه‌ی گروه‌های مجرد را بررسی می‌کنیم. نظریه‌ی مجرد گروه‌ها از این حیث مزیت دارد که خواص گروه‌ها را به طور مجرد و بدون وابستگی به مثلاً جایگشت‌ها، بررسی می‌کند. بنابراین بر هر گروهی قابل استفاده است. البته گروه‌های جایگشتی از مثال‌های مهم هستند.

۱.۳ خواص مقدماتی گروه‌ها

در دو فصل قبل با مفهوم گروه آشنا شده‌ایم. گروه جایگشت‌ها روی یک مجموعه را در فصل ۱ و گروه اعداد صحیح به پیمانه‌ی n را در فصل ۲ بررسی کردیم. اکنون می‌خواهیم خواص گروه‌ها را به طور کلی و به صورت مجرد بررسی کنیم. اگر G مجموعه‌ای ناتهی و $*$ عمل دوتایی روی G باشد طوری که برای هر $a, b, c \in G$ داشته باشیم

$$(a * b) * c = a * (b * c) \qquad \text{(خاصیت شرکت‌پذیری)}$$

$(G, *)$ یا به طور مختصر G را نیم‌گروه گوییم. نیم‌گروه G را مونوئید گوییم هرگاه عضو $e \in G$ وجود داشته باشد که برای هر $a \in G$

$$a * e = e * a = a \qquad \text{(وجود عضو همانی)}$$

عضو e را عضو همانی یا عضو بی‌اثر (دو طرفی) G می‌نامیم. مونویید G را گروه گوییم هرگاه برای هر عضو $a \in G$ عضو $b \in G$ وجود داشته باشد که

$$a * b = b * a = e.$$

b را وارون یا معکوس (دو طرفی) a می‌نامیم و با $a^{-۱}$ نشان می‌دهیم.
نیم‌گروه $(G, *)$ را آبلی یا تعویض‌پذیر گوییم هرگاه برای هر $a, b \in G$

$$a * b = b * a.$$

مرتبه‌ی گروه $(G,*)$ عبارت است از عدد اصلی $|G|$. G را متناهی (یا نامتناهی) گوییم هرگاه $|G|$ متناهی (یا نامتناهی) باشد.

مثال ۱.۱.۳. $\mathbb{Z}$، $\mathbb{Q}$، $\mathbb{R}$ و $\mathbb{C}$ تحت عمل جمع گروه‌های آبلی نامتناهی هستند. □

مثال ۲.۱.۳. $\mathbb{Q}-\{0\}$، $\mathbb{R}-\{0\}$، $\mathbb{C}-\{0\}$ تحت عمل ضرب گروه‌های آبلی نامتناهی هستند. در حالی‌که $\mathbb{Z}-\{0\}$ تحت عمل ضرب گروه نیست. □

اگر $(A,*)$ یک مونوییدِ باشد، مجموعه‌ی اعضای وارون‌پذیر A تحت $*$ یک گروه تشکیل می‌دهند (چرا؟) این گروه را با $A^\times$ نشان می‌دهیم. مثلاً تحت عمل ضرب متعارف داریم:

$$\mathbb{Q}^\times=\mathbb{Q}-\{0\},\quad \mathbb{R}^\times=\mathbb{R}-\{0\},\quad \mathbb{C}^\times=\mathbb{C}-\{0\},\quad \mathbb{Z}^\times=\{1,-1\}.$$

مثال ۳.۱.۳. اگر n عدد صحیح مثبت ثابت باشد، مجموعه‌ی رده‌های مانده‌ای یعنی $\mathbb{Z}_n$ تحت عمل جمع $\bar{a}+\bar{b}=\overline{a+b}$ یک گروه آبلی متناهی با مرتبه‌ی n است. هم‌چنین مجموعه‌ی $\mathbb{Z}_n^\times=\{\bar{a}\in\mathbb{Z}_n \mid \gcd\{a,n\}=1\}$ متشکل از اعضای وارون‌پذیر $\mathbb{Z}_n$ تحت عمل ضرب $\bar{a}\,\bar{b}=\overline{ab}$ یک گروه آبلی با مرتبه‌ی $\varphi(n)$ است، که در آن φ تابع فی اویلر است. □

مثال ۴.۱.۳. فرض کنید X مجموعه‌ی ناتهی باشد. مجموعه‌ی $\mathrm{Map}(X,X)$ متشکل از همه‌ی توابع از X به X تحت عمل ترکیب توابع یک مونوییدِ است. عضو همانی $\mathrm{Map}(X,X)$ تابع همانی $\mathrm{id}_X:X\longrightarrow X$ است. توجه کنید مجموعه‌ی اعضای وارون‌پذیر $\mathrm{Map}(X,X)$ همان S_X متشکل از همه‌ی جایگشت‌های روی X است، یعنی $\mathrm{Map}(X,X)^\times=S_X$. اگر $|X|=n$، آن‌گاه $|\mathrm{Map}(X,X)|=n^n$ و $|S_X|=n!$. □

قبل از آن که مثال‌های بیشتری از گروه بیاوریم تعدادی از خواص اولیه را ثابت می‌کنیم. ابتدا متذکر می‌شویم که اگر $(G,*)$ مونوئید باشد، عضو همانی e یکتاست (قضیه‌ی ۶.۱ در صفحه‌ی ۲۴ را ببینید). اکنون یک خاصیت مهم در گروه‌ها که به قوانین حذف معروف است را ثابت می‌کنیم:

قضیه ۵.۱.۳. فرض کنید $(G,*)$ گروه باشد.
(الف) قوانین حذف در G برقرارند، یعنی به ازای هر $a,b,c\in G$

$$a*b=a*c\Longrightarrow b=c \qquad \text{(حذف از چپ)}$$
$$a*b=c*b\Longrightarrow a=c \qquad \text{(حذف از راست)}$$

(ب) به ازای هر عضو $a\in G$ عضو وارون آن یعنی a^{-1} یکتاست.
(ج) برای هر $a\in G$ داریم $(a^{-1})^{-1}=a$.
(د) به ازای هر $a,b\in G$ داریم $(a*b)^{-1}=b^{-1}*a^{-1}$.
(هـ) به ازای هر $a,b\in G$ معادلات $a*x=b$ و $y*a=b$ در G جواب یکتا دارند به طور مشخص $x=a^{-1}*b$ و $y=b*a^{-1}$.

اثبات. (الف) برای اثبات قانون حذف از چپ می‌نویسیم

$$\begin{aligned} b &= e*b\\ &= (a^{-1}*a)*b\\ &= a^{-1}*(a*b)\\ &= a^{-1}*(a*c)\\ &= (a^{-1}*a)*c\\ &= e*c\\ &= c. \end{aligned}$$

در واقع مثل این است که بر طرفین تساوی $a*b=a*c$ عضو a^{-1} را از چپ اثر داده‌ایم

$$a^{-1}*(a*b)=a^{-1}*(a*c)$$

که نتیجه می‌دهد

$$(a^{-1}*a)*b=(a^{-1}*a)*c.$$

و بنابراین $e*b=e*c$ یا $b=c$.
اثبات قانون حذف از راست به طریق مشابه انجام می‌شود.
(ب) اگر a' و a^{-1} وارون a باشند داریم $a*a^{-1}=e$ و $a*a'=e$. پس $a*a'=a*a^{-1}$. طبق قانون حذف از چپ $a'=a^{-1}$، که حکم (ب) را ثابت می‌کند.
(ج) چون $a*a^{-1}=a^{-1}*a=e$ پس a وارون a^{-1} است، یعنی $a=(a^{-1})^{-1}$.
(د) چون

$$\begin{aligned}(a*b)*(b^{-1}*a^{-1}) &= ((a*b)*b^{-1})*a^{-1}\\ &= (a*(b*b^{-1}))*a^{-1}\\ &= (a*e)*a^{-1}\\ &= a*a^{-1}\\ &= e\end{aligned}$$

و به طریق مشابه $(b^{-1}*a^{-1})*(a*b)=e$، داریم $(a*b)^{-1}=b^{-1}*a^{-1}$.
(هـ) $x=a^{-1}*b$ جوابی از معادله‌ی $a*x=b$ است، زیرا

$$a*(a^{-1}*b)=(a*a^{-1})*b=e*b=b.$$

این جواب یکتاست زیرا

$$\begin{aligned}a*x=b &\implies a^{-1}*(a*x)=a^{-1}*b\\ &\implies (a^{-1}*a)*x=a^{-1}*b\\ &\implies e*x=a^{-1}*b\\ &\implies x=a^{-1}*b.\end{aligned}$$

در واقع چون همه‌ی مراحل بالا برگشت پذیر است نتیجه می‌شود که $x=a^{-1}*b$ جواب معادله نیز هست. به همین نحو می‌توان معادله‌ی $y*a=b$ را بررسی کرد. □

قضیه ۶.۱.۳. (تعمیم قانون شرکت‌پذیری) فرض کنید $(G,*)$ یک نیم‌گروه باشد. اگر a_1، a_2، ...، a_n اعضای دل‌خواهی از G باشند، آن‌گاه مقدار $a_1*a_2*\cdots*a_n$ مستقل از پرانتزگذاری است.

اثبات. به طور استقرایی فرض کنید $\prod_{i=1}^{1}a_i=a_1$ و $\prod_{i=1}^{k}a_i=\left(\prod_{i=1}^{k-1}a_i\right)*a_k$. پس مثلاً $\Pi_{i=1}^{2}a_i=(\Pi_{i=1}^{1}a_i)*a_2=(a_1)*a_2=a_1*a_2$ و $\prod_{i=1}^{3}a_i=\left(\prod_{i=1}^{2}a_i\right)*a_3=(a_1*a_2)*a_3$ و $\prod_{i=1}^{4}a_i=\left(\prod_{i=1}^{3}a_i\right)*a_4=((a_1*a_2)*a_3)*a_4$ و غیره. به استقرا روی n ثابت می‌کنیم هر پرانتزگذاری مقدار $a_1*a_2*\cdots*a_n$ برابر $\prod_{i=1}^{n}a_i$ است. برای $n=1,2,3$ محاسبات بالا و قانون شرکت‌پذیری این مطلب را نتیجه می‌دهند. فرض کنید به ازای هر $k<n$ هر پرانتزگذاری دلخواه $a_1*a_2*\cdots*a_n$ را با $(a_1*a_2*\cdots*a_n)$ نشان دهیم. این پرانتزگذاری به دو زیر حاصل‌ضرب مثلاً $(a_1*\cdots*a_k)*(a_{k+1}*\cdots*a_n)$ شکسته می‌شود.

طبق فرض استقرا $(a_۱ * \cdots * a_k)$ برابر عضو منحصر به فرد $x = \prod_{i=۱}^{k} a_i$ از G است. پس

$$\begin{aligned}(a_۱ * \cdots * a_n) &= (a_۱ * \cdots * a_k) * (a_{k+۱} * \cdots * a_n)\\ &= x * (a_{k+۱} * \cdots * a_n)\\ &= (x * (a_{k+۱} * \cdots * a_{n-۱})) * a_n \quad \text{(فرض استقرا)}\\ &= ((a_۱ * \cdots * a_k) * (a_{k+۱} * \cdots * a_{n-۱})) * a_n\\ &= \left(\prod_{i=۱}^{n-۱} a_i\right) * a_n \quad \text{(فرض استقرا)}\\ &= \prod_{i=۱}^{n} a_i\end{aligned}$$

و حکم ثابت است. □

هرگاه $(G, *)$ یک مونویید باشد معمولاً از نوشتن عمل دوتایی $*$ صرف نظر می‌کنیم و عبارت $a * b$ را به طور ساده و به صورت نماد ضربی ab می‌نویسیم. هم‌چنین در این حالت عضو همانی را با e یا ۱ نشان می‌دهیم. گاهی اوقات عمل دوتایی را با استفاده از نماد جمع به صورت $a + b$ می‌نویسیم. این نمادگذاری معمولاً در حالتی به‌کار می‌رود که G آبلی باشد. در این حالت عضو همانی را با ۰ و وارون a را با $-a$ نشان می‌دهیم. $-a$ را قرینه‌ی a گوییم.
اگر G نیم‌گروه باشد، $a \in G$ و $n \in \mathbb{N}$ تعریف می‌کنیم

$$a^n = \underbrace{aa \cdots a}_{n \text{ بار}},$$

که این تعریف در صورتی گروه مورد نظر گروه جمعی باشد به صورت زیر است

$$na = \underbrace{a + a + \cdots + a}_{n \text{ بار}}.$$

علاوه بر آن اگر G مونویید باشد تعریف می‌کنیم $a^۰ = e$ (و در نماد جمعی $۰a = ۰$). درنهایت اگر G گروه باشد، به ازای هر $n \in \mathbb{N}$ تعریف می‌کنیم $a^{-n} = (a^{-۱})^n$ (در نماد جمعی $(-n)a = n(-a)$). در واقع عمل توان در یک گروه برای اعداد صحیح نامنفی (همانند اثبات قضیه‌ی ۶.۱.۳) به صورت استقرایی تعریف می‌شود:

$$a^۰ = e, \quad a^۱ = a, \quad a^n = a^{n-۱}a.$$

در جدول زیر قوانین متناظر توان و ضرایب در نمادهای ضربی و جمعی آورده شده‌اند. برخی از قوانین در تمرین ۹ آورده شده‌اند. توجه کنید در حالتی که گروه جمعی باشد معمولاً گروه را آبلی در نظر می‌گیریم و na یک ضریب از a گوییم.

در گروه جمعی	در گروه ضربی
$۰a = ۰$	$a^۰ = ۱$
$۱a = ۱$	$a^۱ = a$
$(-۱)a = -a$	$a^{(-۱)} = a^{-۱}$
$(n+m)a = na + ma$	$a^{n+m} = a^n a^m$
$n(a+b) = na + nb$	$(ab)^n = a^n b^n$ ($ab = ba$ اگر)
$n(ma) = (nm)a$	$(a^m)^n = a^{mn}$

در این‌جا چند مثال دیگر از گروه می‌آوریم.

مثال ۷.۱.۳. فرض کنید $V_۴ = \{e, a, b, c\}$ مجموعه‌ای متشکل از چهار عضو باشد. حاصل‌ضرب در $V_۴$ را با جدول زیر تعریف می‌کنیم

$*$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

بنابراین

$$a^۲ = b^۲ = c^۲ = e, \quad ab = c, \quad ac = b, \quad bc = a, \quad ex = xe = x, \ \ \forall x \in V_۴.$$

به سادگی می‌توان دید که $V_۴$ یک گروه آبلی مرتبه‌ی ۴ است که آن‌را ۴-گروه کلاین گوییم. □

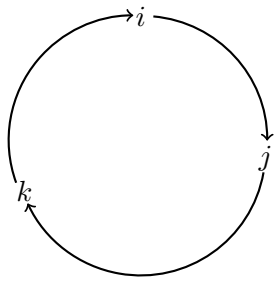
مثال ۸.۱.۳. گروه چهارگان (کواترنیونی) $Q_۸$ به صورت زیر تعریف می‌شود

$$Q_۸ = \{۱, -۱, i, -i, j, -j, k, -k\}$$

که در آن حاصل‌ضرب اعضا به صورت زیر است

$$(-۱)^۲ = ۱, \ \ ۱a = a۱ = a, \ \ (-۱)a = a(-۱) = -a, \ \ a = i, j, k,$$
$$ij = k, \ \ ji = -k, \ \ ki = j, \ \ ik = -j, \ \ jk = i, \ \ kj = -i,$$
$$i^۲ = j^۲ = k^۲ = -۱,$$
$$a(-b) = (-a)b = (-۱)ab, \ \ a = i, j, k.$$

به خاطر سپردن عمل ضرب ساده است. با در نظر گرفتن شکل ۱.۳،



شکل ۱.۳: عمل ضرب در گروه کواترنیونی

حاصل‌ضرب دو عضو متوالی در جهت عقربه‌های ساعت، عضو دیگر و در جهت عکس عقربه‌های ساعت قرینه‌ی عضو دیگر را به دست می‌دهد. اثبات شرکت‌پذیری عمل قدری طولانی است ولی اثبات خواص دیگر گروه ساده است و به عنوان تمرین واگذار می‌شود. $Q_۸$ یک گروه ناآبلی مرتبه‌ی ۸ است. □

مثال ۹.۱.۳. فرض کنید U دایره‌ی واحد، یعنی

$$U = \{z \in \mathbb{C} \mid |z| = ۱\},$$

باشد. در این صورت به سادگی دیده می‌شود U به همراه عمل ضرب متعارف اعداد مختلط یک گروه است. □

مثال ۱۰.۱.۳. اگر n عدد طبیعی باشد، مجموعه‌ی ریشه‌های nام واحد را در نظر می‌گیریم:

$$C_n = \{z \in \mathbb{C} \mid z^n = ۱\}.$$

C_n تحت ضرب اعداد مختلط یک گروه است. اگر $w = e^{\frac{۲\pi i}{n}}$، آنگاه به راحتی می‌توان دید C_n یک گروه مرتبه‌ی n است و

$$C_n = \{۱, w, w^۲, \ldots, w^{n-۱}\}.$$ □

مثال ۱۱.۱.۳. فرض کنید p عددی اول باشد. یکی از گروه‌های مهم، گروه گروه شبه دوری است که آن را به صورت زیر تعریف می‌کنیم

$$C_{p^\infty} = \{z \in \mathbb{C} \mid \exists n \in \mathbb{N},\ z^{p^n} = ۱\}.$$

در واقع C_{p^∞} شامل همه‌ی ریشه‌های p^nام واحد (به ازای هر n) است. به سادگی دیده می‌شود که C_{p^∞} تحت ضرب اعداد مختلط یک گروه نامتناهی است. توجه کنید مجموعه‌های

$$C_{p^n} = \{z \in \mathbb{C} \mid z^{p^n} = ۱\}, \quad n = ۱, ۲, \dots$$

همگی زیرمجموعه‌های C_{p^∞} هستند و به وضوح داریم

$$C_p \subset C_{p^۲} \subset \cdots$$

و هم‌چنین

$$C_{p^\infty} = \bigcup_{n=۱}^{\infty} C_{p^n}.$$

بنابراین C_{p^∞} اجتماع زنجیر صعودی از گروه‌های C_{p^n}، $n \geq ۱$ است که هر کدام زیرمجموعه‌ی سره C_{p^∞} هستند. □

مثال ۱۲.۱.۳. فرض کنید $n \geq ۳$ و P_n یک n ضلعی منتظم باشد که مرکز آن مبدا مختصات است. یک تابع دوسویی $\varphi : \mathbb{R}^۲ \longrightarrow \mathbb{R}^۲$ که P_n را حفظ کند یعنی $\varphi(P_n) = P_n$ یک تقارن P_n نامیده می‌شود. در هندسه نشان داده می‌شود که تقارن‌های P_n عبارت‌اند از : n چرخش مبداء به اندازه‌ی

$$\frac{۲k\pi}{n}, \quad k = ۰, ۱, ۲, \dots, n-۱$$

و n بازتاب که
(الف) اگر n فرد باشد، نسبت به خطوطی که هر راس را به وسط ضلع مقابل وصل می‌کند.
(ب) اگر n زوج باشد، نسبت به خطوطی که دو راس مقابل و یا وسط دو ضلع مقابل را به هم وصل می‌کند.
بنابراین تقارن‌های P_n دقیقاً $۲n$ تا هستند. مجموعه‌ی این چرخش‌ها و بازتاب‌ها تحت عمل ترکیب توابع یک گروه ناآبلی تشکیل می‌دهند که آن را گروه دووجهی از مرتبه‌ی $۲n$ می‌نامیم و با $D_{۲n}$ نشان می‌دهیم. اگر ρ چرخش مبداء به اندازه‌ی $\frac{۲\pi}{n}$ و ε یک بازتاب دلخواه در $D_{۲n}$ باشد، به سادگی می‌توان دید

$$\rho^n = \varepsilon^۲ = (\rho\varepsilon)^۲ = ۱.$$

پس

$$D_{۲n} = \{۱, \rho, \rho^۲, \dots, \rho^{n-۱}, \varepsilon, \rho\varepsilon, \rho^۲\varepsilon, \dots, \rho^{n-۱}\varepsilon\}.$$

مثلاً گروه تقارن‌های مثلث متساوی‌الاضلاع عبارت است از

$$D_۶ = \{۱, \rho, \rho^۲, \varepsilon, \rho\varepsilon, \rho^۲\varepsilon\}$$

که در آن ρ چرخش به اندازه‌ی $\frac{۲\pi}{۳}$ و ε بازتاب دلخواه (مثلاً نسبت به محور yها) است. یعنی اگر A، B، و C سه راس مثلث باشند،

$$\begin{aligned} \rho : A &\mapsto B & \varepsilon : A &\mapsto A \\ B &\mapsto C & B &\mapsto C \\ C &\mapsto A & C &\mapsto B. \end{aligned}$$

یک میدان مجموعه‌ای مثل F است به همراه دو عمل جمع و ضرب که (الف) $(F,+)$ گروه آبلی باشد (عضو همانی جمع را با ۰ نشان می‌دهیم)، (ب) داشته باشیم $F^\times = F - \{۰\}$ و $F^\times$ تحت عمل ضرب گروه آبلی باشد، و (ج) قانون توزیع‌پذیری برقرار باشد :

$$\forall a,b,c \in F,\ \ a(b+c) = ab + ac.$$

$\mathbb{Q}$، $\mathbb{R}$، $\mathbb{C}$ مثال‌هایی از میدانهای نامتناهی هستند. میدانهای متناهی نیز وجود دارند، مثلاً اگر p عدد اول باشد، $\mathbb{Z}_p$ یک میدان متناهی با مرتبه‌ی p است.
فرض کنید F یک میدان و $n > ۱$ یک عدد صحیح مثبت باشد. مجموعه‌ی ماتریس‌های $n \times n$ با درایه‌های در F را با $M_n(F)$ نشان می‌دهیم. جمع متعارف دو ماتریس $n \times n$، $A = [a_{ij}]$ و $B = [b_{ij}]$ با درایه‌های در F به صورت درایه‌ای انجام می‌شود:

$$A + B = [a_{ij}] + [b_{ij}] = [a_{ij} + b_{ij}].$$

$M_n(F)$ تحت عمل جمع متعارف ماتریس‌ها یک گروه است. عضو همانی آن ماتریس $n \times n$ است که همه‌ی درایه‌های آن صفر است، این ماتریس را ماتریس صفر می‌نامیم. قرینه‌ی ماتریس $A = [a_{ij}]$ عبارت است از $-A = [-a_{ij}]$.
روی $M_n(F)$ یک عمل ضرب نیز تعریف می‌شود ضرب متعارف دو ماتریس $n \times n$، $A = [a_{ij}]$ و $B = [b_{ij}]$ به صورت زیر است:

$$AB = [a_{ij}][b_{ij}] = [c_{ij}], \quad c_{ij} = \sum_{k=۱}^{n} a_{ik}b_{kj}.$$

$M_n(F)$ تحت عمل ضرب متعارف ماتریس‌ها یک مونویید است. عضو همانی $M_n(F)$ تحت عمل ضرب ماتریس همانی $I = [d_{ij}]$ است که روی قطر آن ۱ و سایر درایه‌های آن صفر است، یعنی $d_{ii} = ۱$ و برای $i \neq j$، $d_{ij} = ۰$. $M_n(F)$ تحت عمل ضرب متعارف ماتریس‌ها گروه نیست. مجموعه‌ی اعضای وارون‌پذیر $M_n(F)$، یعنی $(M_nF)^\times$، را با $\mathrm{GL}_n(F)$ نشان می‌دهیم و آن را گروه خطی عمومی از درجه‌ی n می‌نامیم. پس

$$\mathrm{GL}_n(F) = \{A \in M_nF \mid \det A \neq ۰\}$$

تحت عمل ضرب متعارف ماتریس‌ها یک گروه غیرآبلی است. عضو همانی آن ماتریس همانی $n \times n$ یعنی I است. وارون ماتریس A ماتریس معکوس آن ، یعنی $A^{-۱}$ است. یک زیرمجموعه‌ی مهم $\mathrm{GL}_n(F)$ که خود تحت ضرب متعارف ماتریس‌ها گروه است، گروه خطی خاص متشکل از ماتریس‌های با دترمینان ۱ است:

$$\mathrm{SL}_n(F) = \{A \in \mathrm{GL}_n(F) \mid \det A = ۱\}.$$

اگر F یک میدان و V فضای برداری روی F باشد مجموعه‌ی همه‌ی تبدیل‌های خطی از V به V را با $L(V,V)$ نشان می‌دهیم. $L(V,V)$ تحت عمل جمع متعارف توابع یک گروه است. اما تحت عمل ترکیب توابع گروه نیست. مجموعه‌ی اعضای وارون‌پذیر $L(V,V)$، یعنی $L(V,V)^\times$، را با گروه خطی عمومی گوییم و با $\mathrm{GL}(V)$ نشان می‌دهیم. پس

$$\mathrm{GL}(V) = \{\theta \in L(V,V) \mid \ \theta \text{ وارون پذیر}\}$$

تحت عمل ترکیب توابع یک گروه است.

مثال ۱۳.۱.۳. فرض کنید $G = \{a \in \mathbb{R} \mid -۱ < a < ۱\}$، عمل $*$ روی G را به صورت زیر تعریف می‌کنیم

$$a * b = \frac{a+b}{۱+ab}, \quad \forall a,b \in G.$$

نشان دهید $(G,*)$ یک گروه است.

حل فرض کنید $a,b \in G$، ابتدا نشان می‌دهیم $a * b \in G$. چون $-۱ < a,b < ۱$ پس $a^۲ < ۱$ و $b^۲ < ۱$. بنابراین $(۱-a^۲)(۱-b^۲) > ۰$ و در نتیجه $۱ - a^۲ - b^۲ + a^۲b^۲ > ۰$. اکنون

$$(۱+ab)^۲ - (a+b)^۲ = ۱ + a^۲b^۲ + ۲ab - a^۲ - b^۲ - ۲ab = ۱ - a^۲ - b^۲ + a^۲b^۲ > ۰.$$

در نتیجه $\left(\frac{a+b}{1+ab}\right)^2 < 1$ و $a*b \in G$. حال نشان می‌دهیم $*$ خوش تعریف است. اگر $a,b,c,d \in G$ و $(a,b)=(c,d)$، آن‌گاه $a=c$ و $b=d$. پس

$$a*b=\frac{a+b}{1+ab}=\frac{c+d}{1+cd}=c*d$$

و $*$ خوش تعریف است. برای اثبات شرکت‌پذیری فرض کنید $a,b,c \in G$. داریم

$$(a*b)*c=\frac{a+b}{1+ab}*c=\frac{\frac{a+b}{1+ab}+c}{1+\frac{a+b}{1+ab}c}=\frac{a+b+c+abc}{1+ab+ac+bc}.$$

به طریق مشابه

$$a*(b*c)=\frac{a+b+c+abc}{1+ab+ac+bc}.$$

بنابراین $(a*b)*c=a*(b*c)$، یعنی $*$ شرکت‌پذیر است.
اکنون چون $0 \in G$ و

$$0*a=\frac{0+a}{1+0a}=a, \quad a*0=\frac{a+0}{1+a0}=a.$$

پس 0 همانی است. اگر $a \in G$، آن‌گاه $-a \in G$ و

$$-a*a=\frac{-a+a}{1+(-a)a}=0, \quad a*(-a)=0,$$

یعنی $-a$ وارون a است. پس $(G,*)$ گروه است. □

مثال ۱۴.۱.۳. اگر G یک گروه باشد و $a,b \in G$ طوری باشند که $ab=ba^{-1}$ و $ba=ab^{-1}$، نشان دهید $a^4=b^4=1$.

حل طبق فرض داریم $ab=ba^{-1}$. محاسبه می‌کنیم

$$\begin{aligned} ab=ba^{-1} &\implies b^{-1}aba=b^{-1}ba^{-1}a \\ &\implies b^{-1}aba=1 \\ &\implies b^{-1}aab^{-1}=1 \quad (ba=ab^{-1} \text{ چون}) \\ &\implies a^2=b^2. \end{aligned}$$

بنابراین $a^2=b^2$. اکنون مجدداً از $ab=ba^{-1}$ داریم

$$\begin{aligned} ab=ba^{-1} &\implies b^{-1}ab=a^{-1} \\ &\implies (b^{-1}ab)^2=a^{-2} \\ &\implies b^{-1}a^2b=a^{-2} \\ &\implies b^{-1}b^2b=b^{-2} \quad (a^2=b^2 \text{ چون}) \\ &\implies b^4=1. \end{aligned}$$

بنابراین $b^4=1$. درنهایت چون $a^2=b^2$ نتیجه می‌گیریم که $a^4=b^4=1$. □

این بخش را با مثالی از نحوه‌ی ساختن گروه جدید با استفاده از گروه‌های دلخواه داده شده به پایان می‌بریم.

مثال ۱۵.۱.۳. فرض کنید $G_۱$، $G_۲$، ...، G_k، k گروه دلخواه باشند حاصل‌ضرب دکارتی $G_۱ \times G_۲ \times \cdots \times G_k$ با عمل زیر به گروه تبدیل می‌شود که آن را حاصل‌ضرب مستقیم $G_۱$، ...، G_k گوییم. به ازای هر دو عضو دلخواه $(h_۱, \ldots, h_k)$ و $(g_۱, \ldots, g_k)$ از $G_۱ \times \cdots \times G_k$ تعریف می‌کنیم

$$(g_۱, \ldots, g_k)(h_۱, \ldots, h_k) = (g_۱h_۱, \ldots g_kh_k).$$

عضو بی‌اثر $G_۱ \times \cdots \times G_k$ عبارت است از $(۱_{G_۱}, \ldots, ۱_{G_k})$ و وارون $(g_۱, \ldots, g_k)$ عبارت است از $(g_۱^{-۱}, \ldots, g_k^{-۱})$.

تمرین‌ها

۱. فرض کنید G نیم‌گروه باشد و (الف) عضو $e \in G$ وجود دارد که برای هر $a \in G$، $ea = a$ (e همانی چپ) و (ب) به ازای هر $a \in G$ عضو b وجود دارد که $ba = e$ (وارون چپ). ثابت کنید G گروه است.

۲. آیا اگر یک نیم‌گروه همانی چپ داشته باشد و هر عضو آن وارون راست داشته باشد می‌توان نتیجه گرفت که گروه است؟

۳. هرگاه در نیم‌گروه G قوانین حذف برقرار باشند و برای هر $a \in G$ عضو $e_a \in G$ وجود داشته باشد که $ae_a = e_aa = a$، نشان دهید G مونوئید است.

۴. ثابت کنید هر نیم‌گروه متناهی که قوانین حذف در آن برقرار باشند گروه است.

۵. فرض کنید $G = \mathbb{Q} - \{-۱\}$. نشان دهید $(G, *)$ یک گروه است، که در آن

$$a * b = a + b + ab, \quad \forall a, b \in G.$$

۶. اگر $G = \{۱, a, b, c, d\}$ گروه باشد، جدول ضرب داده شده را کامل کنید:

(الف)

$*$	۱	a	b	c	d
۱	۱	a	b	c	d
a	a				
b	b		c	d	
c	c				
d	d				

(ب)

$*$	۱	a	b	c	d
۱	۱	a	b	c	d
a	a		۱	b	
b	b				
c	c				
d	d				

۷. فرض کنید y و x دو عضو گروه G باشند. نشان دهید $xy = yx$ اگر و تنها اگر $x^{-۱}y^{-۱}xy = ۱$ اگر و تنها اگر $y^{-۱}xy = x$.

۸. فرض کنید a، b دو عضو گروه G باشند که $ab = ba$. ثابت کنید به ازای هر عدد صحیح n داریم $(ab)^n = a^nb^n$.

۹. فرض کنید G گروه باشد و $a \in G$. نشان دهید به ازای همه‌ی اعداد صحیح m و n:
(الف) $a^ma^n = a^{m+n}$ (در نماد جمعی : $ma + na = (m + n)a$).
(ب) $(a^m)^n = a^{mn}$ (در نماد جمعی : $n(ma) = (mn)a$).

۱۰. فرض کنید a، b دو عضو یک گروه، و n، r اعداد طبیعی باشند. ثابت کنید
(الف) $(a^{-۱}ba)^n = a^{-۱}b^na$.
(ب) اگر $a^{-۱}ba = b^r$، آنگاه $a^{-n}ba^n = b^{r^n}$.

۱۱. اگر در گروه G به ازای هر $a \in G$ داشته باشیم $a^۲ = e$ (یعنی $a^{-۱} = a$) ثابت کنید G آبلی است.

۱۲. فرض کنید G گروه متناهی باشد. ثابت کنید عدد طبیعی m وجود دارد که برای هر $a \in G$، $a^m = ۱$.

۱۳. فرض کنید $n > ۱$ عددی صحیح باشد. گروه G را n-آبلی گوییم هرگاه برای هر $a, b \in G$، $(ab)^n = a^nb^n$. اگر G، n-آبلی باشد ثابت کنید
(الف) $(ab)^{n-۱} = b^{n-۱}a^{n-۱}$.

(ب) $a^n b^{n-1} = b^{n-1} a^n$.

(ج) $(a^{-1} b^{-1} ab)^{n(n-1)} = 1$.

۱۴. فرض کنید G گروه باشد. عضو $g^{-1} x g$ را مزدوج x (توسط g) نامیم و رابطه‌ی تزویج $\sim$ را روی G چنین تعریف می‌کنیم: $x \sim y$ اگر و تنها اگر y مزدوج x باشد. نشان دهید رابطه‌ی تزویج رابطه‌ی هم‌ارزی است. رده‌ی هم‌ارزی شامل x را با $\mathrm{orb}(x)$ نشان می‌دهیم و آن را رده‌ی مزدوجی x می‌نامیم.

۱۵. رده‌های مزدوجی D_{2n} را برای n زوج و فرد بیابید.

۱۶. عضو a در نیم‌گروه S را خودتوان گوییم هرگاه $a^2 = a$. اگر S نیم‌گروه باشد و $a \in S$، $a^m = a^n$ $(m, n \in \mathbb{N})$. نشان دهید توانی از a خودتوان است.

۱۷. فرض کنید S یک نیم‌گروه متناهی باشد، نشان دهید S یک عضو خودتوان دارد.

۱۸. فرض کنید G یک نیم‌گروه متناهی با عضو همانی باشد. نشان دهید G گروه است اگر و تنها اگر G تنها یک عضو خودتوان داشته باشد.

۱۹. فرض کنید S نیم‌گروه باشد. نشان دهید S گروه است اگر و تنها اگر به ازای هر $a \in S$، $aS = S$ و $Sa = S$، که در آن $aS = \{as \mid s \in S\}$ و $Sa = \{sa \mid s \in S\}$.

۲۰. اگر در یک گروه داشته باشیم $a^6 = 1$ و $ab = ba^3$، نشان دهید $a^2 = 1$ و $ab = ba$.

۲۱. فرض کنید a، b اعضایی از یک گروه باشند و $b^{-1} a^2 b = a^3$ و $a^{-1} b^2 a = b^3$. نشان دهید $a = b = 1$.

۲۲. فرض کنید a، b اعضایی از یک گروه باشند و $a^4 = 1$ و $a^2 b = ba$. نشان دهید $a = 1$.

۲۳. اگر در یک گروه داشته باشیم $a^6 = 1$ و $ab = ba^2$، نشان دهید $a^3 = 1$ و $aba = b$.

۲۴. فرض کنید S یک نیم‌گروه باشد. نشان دهید S یک گروه است اگر و تنها اگر به ازای هر $a \in S$ عضو یکتای $b \in S$ وجود داشته باشد که $aba = a$.

۲۵. فرض کنید F یک میدان و $n \geq 2$ عدد صحیح باشد. اگر E_{ij} نشان ماتریسی در $\mathrm{Mat}_n(F)$ باشد که درایه (i, j) آن برابر ۱ و سایر درایه‌ها برابر صفر است، تحقیق کنید که $E_{ij} E_{kl} = \delta_{jk} E_{il}$، که در آن δ_{jk} دلتای کرونکر است. نشان دهید به ازای هر $a \in F$ ماتریس $I + aE_{ij}$، $i \neq j$، وارون‌پذیر است و وارون آن را بیابید.

۲۶. اگر F یک میدان باشد $n \geq 2$، نشان دهید گروه $\mathrm{GL}_n(F)$ آبلی نیست.

۲.۳ مرتبه، گروه‌های دوری

در این بخش مفهوم مرتبه و گروه‌های دوری و خواص اساسی آن‌ها را بررسی می‌کنیم.

تعریف ۱.۲.۳. فرض کنید G گروه باشد و $a \in G$. اگر عدد طبیعی m وجود داشته باشد که $a^m = 1$، گوییم مرتبه a متناهی است و کوچک‌ترین عدد طبیعی m با این خاصیت را مرتبه‌ی a گوییم و می‌نویسیم $O(a) = m$. در صورتی که چنین mای وجود نداشته باشد گوییم مرتبه‌ی a برابر بی‌نهایت است و می‌نویسیم $O(a) = \infty$.

مثال ۲.۲.۳. در هر گروه G داریم $O(e) = 1$. □

مثال ۳.۲.۳. مرتبه‌ی هر عضو غیرهمانی در ۴-گروه کلاین برابر ۲ است. مرتبه‌ی هر عضو مخالف ± 1 در Q_8 برابر چهار است. هم‌چنین در Q_8 مرتبه‌ی -1 برابر ۲ است. □

مثال ۴.۲.۳. در گروه ضربی $\mathbb{Q}^\times = \mathbb{Q} - \{0\}$ مرتبه‌ی عضو -1 برابر ۲ و مرتبه‌ی هر عضو مخالف ± 1 نامتناهی است. □

مثال ۵.۲.۳. در گروه ضربی $\mathbb{C}^\times = \mathbb{C} - \{0\}$ مرتبه‌ی عضو z متناهی است اگر و تنها اگر در معادله‌ی $z^n = 1$ (به ازای nای) صدق کند، یعنی یک ریشه‌ی nام واحد باشد. □

مثال ۶.۲.۳. جایگشت (۳ ۲ ۱) را در نظر بگیرید، چون

$$(۱\ ۲\ ۳)^۲ = (۱\ ۳\ ۲)$$

و

$$(۱\ ۲\ ۳)^۳ = (۱\ ۲\ ۳)(۱\ ۲\ ۳)^۲ = (۱\ ۲\ ۳)(۱\ ۳\ ۲) = (۱),$$

نتیجه می‌گیریم $O((۱\ ۲\ ۳)) = ۳$. به همین نحو

$$O((۱\ ۳\ ۲)) = ۳, \quad \text{و} \quad O((۱\ ۲)) = O((۱\ ۳)) = O((۲\ ۳)) = ۲.$$

به طور کلی مرتبه‌ی هر دور به طول r برابر r است. □

گروه G را تاب‌دار گوییم هرگاه مرتبه‌ی هر عضو آن متناهی باشد. گروه G را بی‌تاب گوییم هرگاه مرتبه‌ی هر عضو غیرهمانی نامتناهی باشد. اگر عدد طبیعی n وجود داشته باشد که به ازای هر $a \in G$، $a^n = e$، گوییم نمای G متناهی است. کوچک‌ترین عدد طبیعی n با این خاصیت را نمای G می‌نامیم و آن را با $\exp(G)$ نشان می‌دهیم. در صورتی که چنین عددی وجود نداشته باشد گوییم نمای G نامتناهی است و می‌نویسیم $\exp(G) = \infty$. واضح است که نمای هر گروه بی‌تاب نامتناهی است.

مثال ۷.۲.۳. در گروه‌های جمعی $\mathbb{Z}$، $\mathbb{Q}$، $\mathbb{R}$ و $\mathbb{C}$ مرتبه‌ی هر عضو ناصفر نامتناهی است. پس این گروه‌ها بی‌تاب هستند. C_{p^∞} یک گروه نامتناهی و تاب‌دار است. توجه کنید نمای همه‌ی گروه‌های فوق نامتناهی است. □

فرض کنید G یک گروه و $a \in G$ عضوی با مرتبه‌ی n باشد. پس n کوچک‌ترین عدد طبیعی است که $a^n = e$. حال اگر m عدد صحیح دلخواهی باشد که $a^m = e$، بنا به الگوریتم تقسیم اعداد صحیح q و r وجود دارند که $m = nq + r$ که در آن $۰ \le r < n$. با توجه به تمرین ۹ صفحه‌ی ۵۷، می‌توان نوشت:

$$e = a^m = a^{nq+r} = a^{nq}a^r = (a^n)^q a^r = e^q a^r = ea^r = a^r.$$

از این‌رو $a^r = e$. اگر $r \neq ۰$، آنگاه $۰ < r < n$ و $a^r = e$. این متناقض با خاصیت n است. پس $r = ۰$ و $m = nq$. بنابراین ثابت کرده‌ایم:

قضیه ۸.۲.۳. فرض کنید G گروه باشد و $a \in G$. اگر $O(a) = n$ و $m \in \mathbb{Z}$ طوری باشد که $a^m = e$، آنگاه $n|m$. □

نتیجه ۹.۲.۳. اگر $\alpha \in S_n$ و $\alpha = \alpha_۱ \cdots \alpha_r$ تجزیه‌ی α به دورهای مجزا باشد، آنگاه مرتبه‌ی α برابر کوچک‌ترین مضرب مشترک مرتبه‌ی دورهاست.

اثبات. چون دورهای مجزا با هم تعویض می‌شوند، به ازای هر $m \in \mathbb{Z}$ داریم

$$\alpha^m = \alpha_۱^m \cdots \alpha_r^m.$$

در نتیجه $\alpha^m = (۱)$ اگر و تنها اگر به ازای هر $۱ \le i \le r$، $\alpha_i^m = (۱)$ اگر و تنها اگر به ازای هر i، $O(\alpha_i) \mid m$. چون $O(\alpha)$ کوچک‌ترین عدد طبیعی با این خاصیت است، $O(\alpha) = \operatorname{lcm}\{O(\alpha_i) \mid ۱ \le i \le r\}$. □

با استفاده از روش اثبات قضیه‌ی ۸.۲.۳، می‌توان دید که اگر $O(a) = n$، آنگاه توان‌های متمایز a عبارت‌اند از e، a، $a^۲$، ...، $a^{n-۱}$. از طرف دیگر اگر $O(a) = \infty$، آنگاه همه‌ی توان‌های a متمایزند. زیرا اگر مثلاً $a^k = a^t$ و $k > t$، آنگاه $a^{k-t} = e$. یعنی $O(a) < \infty$ که تناقض است.

قضیه‌ی بعدی ارتباط بین مرتبه‌ی یک عضو و مرتبه‌ی توان‌های آن را مشخص می‌کند.

قضیه ۱۰.۲.۳. فرض کنید G گروه باشد و $a \in G$ طوری که $O(a) = n$. اگر $k \in \mathbb{Z}$، آنگاه $O(a^k) = \dfrac{n}{\gcd\{n, k\}}$.

اثبات. قرار می‌دهیم $d=\gcd\{n,k\}$. فرض کنید $O(a^k)=t$، نشان می‌دهیم $\frac{n}{d}\Big|t$ و $t\Big|\frac{n}{d}$. چون $e=(a^k)^t=a^{kt}$، بنا به قضیه‌ی ۸.۲.۳، $n|kt$. بنابراین $\frac{n}{d}\Big|\frac{k}{d}t$. چون $\gcd\left\{\frac{n}{d},\frac{k}{d}\right\}=1$، داریم $\frac{n}{d}\Big|t$.
اکنون داریم

$$(a^k)^{\frac{n}{d}}=(a^n)^{\frac{k}{d}}=e^{\frac{k}{d}}=e.$$

پس مجدداً، بنا به قضیه‌ی ۹.۱.۲، $t\Big|\frac{n}{d}$. در نتیجه $t=\frac{n}{d}$ و حکم ثابت است. □

نتیجه ۱۱.۲.۳. اگر a عضوی از مرتبه‌ی n در گروه G باشد و $k|n$، آنگاه $O(a^k)=\frac{n}{k}$. □

مثال ۱۲.۲.۳. اگر در گروه $\mathbb{C}^\times$ قرار دهیم $w=e^{\frac{۲\pi i}{۸}}$، آنگاه $O(w)=۸$. در نتیجه

$$O(w^۲)=\frac{۸}{\gcd\{۸,۲\}}=۴,\quad O(w^۳)=\frac{۸}{\gcd\{۸,۳\}}=۸,$$
$$O(w^۴)=\frac{۸}{\gcd\{۸,۴\}}=۲,\quad O(w^۵)=\frac{۸}{\gcd\{۸,۵\}}=۸,$$
$$O(w^۶)=\frac{۸}{\gcd\{۸,۶\}}=۴,\quad O(w^۷)=\frac{۸}{\gcd\{۸,۷\}}=۸.$$ □

اگر G گروه باشد و $a\in G$، داریم $a^{-۱}\in G$. چون G نسبت به ضرب بسته است، همه‌ی توان‌های مثبت و منفی a در G قرار دارند. در واقع مجموعه‌ی همه‌ی توان‌های a تحت عمل ضرب تعریف شده در G یک گروه تشکیل می‌دهند (توجه کنید که $a^۰=۱$، و $a^ma^n=a^{m+n}$) که آن را گروه تولید شده توسط a گوییم و با $\langle a\rangle$ نشان می‌دهیم. a را مولد $\langle a\rangle$ گوییم:

$$\langle a\rangle=\{a^n\mid n\in\mathbb{Z}\}\qquad\text{(در نماد ضربی)}$$
$$\langle a\rangle=\{na\mid n\in\mathbb{Z}\}\qquad\text{(در نماد جمعی)}$$

گروه G را دوری گوییم هرگاه عضوی چون $a\in G$ وجود داشته باشد که $G=\langle a\rangle$. مثلاً

$$C_n=\{z\in\mathbb{C}\mid z^n=۱\}$$

یک گروه دوری است و $C_n=\left\langle e^{\frac{۲\pi i}{n}}\right\rangle$.
هرگاه $G=\langle a\rangle$ یک گروه دوری متناهی از مرتبه‌ی n باشد، داریم $O(a)=n$. در نتیجه $G=\langle a^k\rangle$ اگر و تنها اگر $O(a^k)=n$ اگر و تنها اگر $n=\frac{n}{\gcd\{n,k\}}$ اگر و تنها اگر $\gcd\{n,k\}=۱$. بنابراین یک گروه دوری از مرتبه‌ی n، $\varphi(n)$ تا مولد دارد ، که در آن φ تابع فی اویلر است.

مثال ۱۳.۲.۳. مولدهای $C_۸=\langle w\rangle$ $(w=e^{\frac{۲\pi i}{۸}})$ عبارت‌اند از : w، $w^۳$، $w^۵$، $w^۷$. □

مثال ۱۴.۲.۳. در گروه جمعی $\mathbb{Z}$ داریم

$$\langle ۱\rangle=\{n\mid n\in\mathbb{Z}\}=\mathbb{Z}.$$

پس $\mathbb{Z}$ یک گروه دوری است و ۱ مولدی از آن است. به علاوه

$$\langle -۱\rangle=\{n(-۱)\mid n\in\mathbb{Z}\}=\mathbb{Z}.$$

بنابراین -۱ نیز مولدی از $\mathbb{Z}$ است. □

آیا $\mathbb{Z}$ مولد دیگری به‌جز ۱ و -۱ دارد ؟ جواب سوال منفی است: هرگاه $G=\langle a\rangle$ یک گروه دوری نامتناهی باشد در این صورت a^k مولدی از G است اگر و تنها اگر $G=\langle a^k\rangle$ اگر و تنها اگر $a=a^{kk_۱}$ اگر و تنها اگر $a^{kk_۱-۱}=۱$ اگر و تنها اگر $kk_۱=۱$. پس مولدهای G عبارت‌اند از a و $a^{-۱}$.

مثال ۱۵.۲.۳. در گروه جمعی $\mathbb{Z}_n$، چون $O(\bar{1}) = n$، داریم

$$\langle \bar{1} \rangle = \{m\bar{1} \mid m \in \mathbb{Z}\} = \mathbb{Z}_n.$$

پس $\mathbb{Z}_n$ گروه دوری است و $\bar{1}$ مولدی از آن. به علاوه $\bar{a}$ مولدی از $\mathbb{Z}_n$ است اگر و تنها اگر $O(\bar{1}) = O(\bar{a})$. اما

$$O(\bar{a}) = O(a\bar{1}) = \frac{n}{\gcd\{n, a\}}.$$

بنابراین $\bar{a}$ مولدی از $\mathbb{Z}_n$ است اگر و تنها اگر $\gcd\{a, n\} = 1$. □

مثال ۱۶.۲.۳. ثابت کنید گروه جمعی $\mathbb{Q}$ دوری نیست.

حل فرض کنید $\mathbb{Q}$ دوری باشد، مثلاً $\mathbb{Q} = \left\langle \frac{r}{s} \right\rangle$، که در آن $\gcd\{r, s\} = 1$. عدد دلخواه k را طوری در نظر می‌گیریم که $k > s$. چون $\frac{1}{k} \in \mathbb{Q}$، $n \in \mathbb{Z}$ وجود دارد که $\frac{1}{k} = n\frac{r}{s}$. در نتیجه $s = krn$ و $k|s$ که تناقض است. پس $\mathbb{Q}$ دوری نیست. □

تمرین‌ها

۱. مرتبه‌ی اعضای Q_8 را بیابید.

۲. مرتبه‌ی هر عضو و هم‌چنین مولدهای گروه‌های C_{12}، C_{15}، C_{17}، C_{38} را بیابید.

۳. مرتبه‌ی هر عضو و هم‌چنین مولدهای گروه‌های $\mathbb{Z}_{12}$، $\mathbb{Z}_{15}$، $\mathbb{Z}_{17}$، $\mathbb{Z}_{38}$ را بیابید.

۴. مرتبه‌ی هر عضو گروه‌های $\mathbb{Z}_{12}^{\times}$، $\mathbb{Z}_{15}^{\times}$، $\mathbb{Z}_{17}^{\times}$، $\mathbb{Z}_{38}^{\times}$ را بیابید. کدامیک از این گروه‌ها دوری هستند.

۵. فرض کنید a، b دو عضو یک گروه باشند. اگر $a^{-1}ba = b^2$ و $O(a) = 3$، $O(b)$ را بیابید.

۶. فرض کنید a, b دو عضو با مرتبه‌ی متناهی در گروه G باشند و $ab = ba$. نشان دهید $O(ab) < \infty$.

۷. ماتریس‌های $a = \begin{bmatrix} 1 & 1 \\ 0 & -1 \end{bmatrix}$ و $b = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$ در $\mathrm{GL}_2(\mathbb{R})$ را در نظر بگیرید. ثابت کنید $O(a) = O(b) = 2$ و $O(ab) = \infty$. (این مطلب را با تمرین ۶ مقایسه کنید.)

۸. ماتریس‌های $a = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$ و $b = \begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix}$ در $\mathrm{GL}_2(\mathbb{R})$ را در نظر بگیرید. ثابت کنید $O(a) = 4$، $O(b) = 3$ و $O(ab) = \infty$.

۹. اعضای $\mathrm{GL}_2(\mathbb{Z}_2)$ را مشخص کرده و مرتبه‌ی آن‌ها را بیابید.

۱۰. اگر F میدان متناهی با مرتبه‌ی q باشد نشان دهید

$$|\mathrm{GL}_n(F)| = (q^n - 1)(q^n - q)\cdots(q^n - q^{n-1}).$$

۱۱. اگر x, y دو عضو یک گروه باشند نشان دهید
(الف) $O(x) = O(x^{-1})$ (ب) $O(x) = O(y^{-1}xy)$.
(ج) $O(xy) = O(yx)$.

۱۲. فرض کنید a عضوی از یک گروه G باشد، $O(a) = n_1n_2$، و $\gcd\{n_1, n_2\} = 1$. نشان دهید اعضای $a_1, a_2 \in G$ وجود دارند که $O(a_1) = n_1$، $O(a_2) = n_2$، و $a = a_1a_2 = a_2a_1$. به علاوه نشان دهید a_1 و a_2 با شرایط فوق یکتا هستند. تعمیم مساله چیست؟

۱۳. ثابت کنید هر گروه با مرتبه‌ی زوج عضوی از مرتبه‌ی دو دارد.

۱۴. فرض کنید $G = (\mathbb{R} - \{۰\}) \times \mathbb{R}$. عمل $*$ روی G را با

$$(a, b) * (c, d) = (ac, b + d)$$

به ازای هر $(a, b), (c, d) \in G$ تعریف می‌کنیم. نشان دهید
(الف) $(G, *)$ گروه است.
(ب) G دقیقاً یک عضو مرتبه‌ی ۲ دارد.
(ج) G عضو مرتبه‌ی ۳ ندارد.

۱۵. مرتبه‌ی جایگشت‌های داده شده را بیابید.

(الف) $\begin{pmatrix} ۱ & ۲ & ۳ & ۴ & ۵ & ۶ & ۷ & ۸ & ۹ \\ ۴ & ۷ & ۹ & ۸ & ۲ & ۱ & ۶ & ۳ & ۵ \end{pmatrix}$

(ب) $\begin{pmatrix} ۱ & ۲ & ۳ & ۴ & ۵ & ۶ & ۷ & ۸ & ۹ \\ ۳ & ۸ & ۹ & ۵ & ۲ & ۱ & ۶ & ۴ & ۷ \end{pmatrix}$

(ج) $\begin{pmatrix} ۱ & ۲ & ۳ & ۴ & ۵ & ۶ & ۷ & ۸ & ۹ \\ ۶ & ۴ & ۸ & ۹ & ۳ & ۱ & ۷ & ۵ & ۲ \end{pmatrix}$

(هـ) $(۱\ ۲\ ۳\ ۴\ ۵)(۶\ ۷)(۱\ ۳\ ۵\ ۷)(۱\ ۶\ ۳)$

(و) $(۱\ ۲\ ۵)(۲\ ۳\ ۴)(۲\ ۶)$

(ز) $(۱\ ۲\ ۵)(۲\ ۳)(۱\ ۷\ ۶\ ۳)$.

۱۶. فرض کنید $\alpha = (x_۱\ x_۲\ \cdots\ x_r)$ یک r-دور باشد. ثابت کنید اگر $۱ \le i \le r$ داریم $\alpha^i(x_j) = x_k$، که در آن k باقی‌مانده تقسیم $i + j$ بر r است (یعنی $k \equiv i + j \bmod r$، $۱ \le k \le r$). نتیجه بگیرید $O(\alpha) = r$.

۱۷. اگر $\alpha = (۱\ ۲\ ۳\ \cdots\ r)$، نشان دهید α^i، r-دور است اگر و تنها اگر $\gcd\{i, r\} = ۱$.

۱۸. فرض کنید p عدد اول باشد و $\alpha \in S_n$. نشان دهید $O(\alpha) = p$ اگر و تنها اگر تجزیه‌ی دوری α حاصل‌ضرب p- دورهای مجزا باشد. با ارائه‌ی مثالی نشان دهید که اگر p عدد اول نباشد حکم درست نیست.

۱۹. فرض کنید a, b دو عضو یک گروه باشند. اگر $ab = ba$، $O(a) = n$، و $O(b) = m$ نشان دهید $(ab)^k = ۱$ که در آن $k = \operatorname{lcm}\{n, m\}$. (مرتبه‌ی ab ممکن است کمتر از k باشد، مثلاً فرض کنید $b = a^{-۱}$.) اگر $\langle a \rangle \cap \langle b \rangle = \{۱\}$ ثابت کنید $O(ab) = k$.

۲۰. نشان دهید $\exp(S_n) = \operatorname{lcm}\{۲, ۳, ۴, \ldots, n\}$.

۲۱. اگر b و a دو عضو گروه آبلی G با مرتبه‌های n و m باشند، نشان دهید G عضوی از مرتبه‌ی $\operatorname{lcm}\{m, n\}$ دارد.

۲۲. فرض کنید H و K دو گروه دوری متناهی با مرتبه‌های m و n باشند. نشان دهید $H \times K$ دوری است اگر و تنها اگر $\gcd\{m, n\} = ۱$.

۲۳. فرض کنید m و n دو عدد طبیعی باشند که نسبت به هم اول‌اند. اگر φ تابع فی اویلر باشد، نشان دهید $\varphi(mn) = \varphi(m)\varphi(n)$.

۲۴. (قضیه‌ی باقیمانده چینی) فرض کنید $n_۱$، $n_۲$، ...، n_k اعداد صحیح مثبت باشند. اگر اعداد صحیح $m_۱$، $m_۲$، ...، m_k داده شده باشند، نشان دهید عدد $m \in \mathbb{Z}$ وجود دارد که به ازای هر $i = ۱, ۲, \ldots, k$، $m_i \equiv m \bmod n_i$ اگر و تنها اگر $\gcd\{n_۱, n_۲, \ldots, n_k\} = ۱$.

۳.۳ همریختی

یکی از ابزارهای مهم برای بررسی ارتباط بین ساختارهای جبری، همریختی است. چگونه می‌توان بین دو ساختار جبری ارتباطی برقرار کرد؟ اول از همه یک تابع بین اعضای دو گروه ارتباطی برقرار می‌کند. اما چگونه می‌توان اعمال این دو گروه را به هم مرتبط کرد. این در صورتی است که تابع مورد نظر خاصیت دیگری داشته باشد، و آن حفظ اعمال بین دو گروه است. یعنی تصویر حاصل‌ضرب دو عضو در گروه اول ،

تحت تابع، برابر حاصل‌ضرب تصویرهای آن‌ها در گروه دوم باشد. در واقع اگر G و H دو گروه باشند تابع $f : G \longrightarrow H$ را همریختی می‌نامیم، هرگاه برای هر $x, y \in G$ داشته باشیم

$$f(xy) = f(x)f(y).$$

هرگاه همریختی f یک‌به‌یک باشد آن‌را تکریختی و اگر پوشا باشد آن‌را برووریختی و اگر یک‌به‌یک و پوشا باشد آن‌را یکریختی گوییم. اگر $f : G \longrightarrow H$ یکریختی باشد گوییم G با H یکریخت است و می‌نویسیم

$$G \cong H.$$

به سادگی می‌توان نشان داد (نشان دهید) که وارون یک یکریختی دوباره یکریختی است، بنابراین اگر $G \cong H$، آنگاه $H \cong G$. در واقع می‌توان ثابت کرد (ثابت کنید) که رابطه‌ی $\cong$ روی رده‌ی همه‌ی گروه‌ها یک رابطه‌ی هم‌ارزی است.

مثال ۱.۳.۳. تابع $\ln : \mathbb{R}^{\times}_{pos} \longrightarrow \mathbb{R}$ یکریختی است، که در آن $\mathbb{R}^{\times}_{pos}$ گروه ضربی اعداد حقیقی مثبت است. در واقع $\ln$ از $\mathbb{R}^{\times}_{pos}$ به $\mathbb{R}$ یک‌به‌یک و پوشا است و هم‌چنین

$$f(x) = \ln x, \quad f(xy) = \ln xy = \ln x + \ln y = f(x) + f(y),$$

یعنی f همریختی نیز هست. بنابراین $\mathbb{R} \cong \mathbb{R}^{\times}_{pos}$. □

مثال ۲.۳.۳. تابع $\exp : \mathbb{R} \longrightarrow \mathbb{R}^{\times}_{pos}$ یکریختی است، زیرا

$$g(x) = \exp(x), \quad g(x+y) = e^{x+y} = e^x \cdot e^y = g(x)g(y)$$

و $\exp$ یک‌به‌یک و پوشاست. در واقع $\exp$ و $\ln$ وارون یکدیگرند. □

مثال ۳.۳.۳. تابع $|\cdot| : \mathbb{C}^{\times} \longrightarrow \mathbb{R}^{\times}_{pos}$ (قدر مطلق) همریختی است، زیرا به ازای هر $z, w \in \mathbb{C}$ داریم

$$|zw| = |z||w|.$$

این تابع پوشاست. اما یک‌به‌یک نیست، زیرا $|-۱| = |۱| = ۱$. □

مثال ۴.۳.۳. فرض کنید H و K دو گروه باشند. تابع $\pi_۱ : H \times K \longrightarrow H$ با ضابطه‌ی $\pi_۱(h,k) = h$ یک همریختی پوشا است، که آن را همریختی تصویر (روی مولفه‌ی اول) می‌نامیم. به همین نحو همریختی تصویر روی مولفه‌ی دوم تعریف می‌شود. هم‌چنین تابع $\iota_۱ : H \longrightarrow H \times K$ با ضابطه‌ی $\iota_۱(h) = (h, ۱)$ یک همریختی یک‌به‌یک است، که آن را همریختی جادهی (مولفه‌ی اول) می‌نامیم. به همین نحو می‌توان همریختی جادهی مولفه‌ی دوم را تعریف کرد. □

اکنون تعدادی از خواص مقدماتی همریختیها را می‌یابیم.

قضیه ۵.۳.۳. اگر $f : G \longrightarrow H$ همریختی باشد، آنگاه
(الف) $f(۱_G) = ۱_H$
(ب) برای هر $x \in G$ و هر $n \in \mathbb{Z}$ داریم $f(x^n) = f(x)^n$.

اثبات. (الف) چون f همریختی است داریم

$$f(۱_G) = f(۱_G ۱_G) = f(۱_G)f(۱_G).$$

چون در H قانون حذف برقرار است داریم

$$۱_H = f(۱_G).$$

(ب) برای $n \geq ۰$ به استقرا روی n حکم را ثابت می‌کنیم. اگر $n = ۰$، آنگاه طبق تعریف و قسمت (الف) داریم

$$f(x^{۰}) = f(۱_G) = ۱_H = f(x)^{۰}.$$

حال اگر $n > ۰$ و قضیه برای $n - ۱$ درست باشد، می‌توان نوشت

$$f(x^n) = f\left(x^{n-۱}x\right) = f\left(x^{n-۱}\right) f(x) = f(x)^{n-۱} f(x) = f(x)^n$$

و حکم برای هر $n > ۰$ برقرار است. اکنون ثابت می‌کنیم $f\left(x^{-۱}\right) = f(x)^{-۱}$. چون

$$۱_H = f(۱_G) = f\left(xx^{-۱}\right) = f(x) f\left(x^{-۱}\right).$$

بنا به یکتایی وارون داریم

$$f(x)^{-۱} = f\left(x^{-۱}\right).$$

حال اگر $n < ۰$ داریم

$$f(x^n) = f\left(\left(x^{-n}\right)^{-۱}\right) = \left[f\left(x^{-n}\right)\right]^{-۱} = \left[f(x)^{-n}\right]^{-۱} = f(x)^n$$

و حکم به ازای هر $n \in \mathbb{Z}$ ثابت شد. □

قضیه ۶.۳.۳. اگر $G = \langle g \rangle$ یک گروه دوری نامتناهی باشد، آنگاه $G \cong \mathbb{Z}$.

اثبات. تابع $\psi : \mathbb{Z} \longrightarrow G$ را با ضابطه‌ی $\psi(n) = g^n$، به ازای هر $n \in \mathbb{Z}$، تعریف می‌کنیم. ψ همریختی است، زیرا به ازای هر $m, n \in \mathbb{Z}$،

$$\psi(m+n) = g^{m+n} = g^m \cdot g^n = \psi(m)\psi(n).$$

ψ یک‌به‌یک است، زیرا اگر $\psi(n) = \psi(m)$، آنگاه $g^n = g^m$ یا $g^{n-m} = ۱$. چون $O(g) = \infty$ باید داشته باشیم $n - m = ۰$ یا $n = m$. ψ پوشاست، زیرا هر عضو $G = \langle g \rangle$ به ازای یک $n \in \mathbb{Z}$ به صورت g^n است. بنابراین $\psi(n) = g^n$. در نتیجه ψ یکریختی است و $G \cong \mathbb{Z}$. □

قضیه ۷.۳.۳. اگر $G = \langle g \rangle$ یک گروه دوری از مرتبه‌ی n باشد، آنگاه $G \cong C_n$.

اثبات. اگر $w = e^{\frac{۲\pi i}{n}}$، می‌دانیم $C_n = \langle w \rangle$. تابع $\psi : G \longrightarrow C_n$ را با ضابطه‌ی $\psi(g^k) = w^k$ را در نظر می‌گیریم. ψ خوش تعریف است، زیرا

$$g^k = g^m \Longrightarrow g^{k-m} = ۱ \Longrightarrow n|(k-m) \Longrightarrow w^{k-m} = ۱ \Longrightarrow w^k = w^m.$$

چون مراحل بالا برگشت پذیر است ψ یک‌به‌یک نیز هست. هم‌چنین به وضوح ψ همریختی پوشا نیز هست. پس ψ یکریختی است و $G \cong C_n$. □

اگر G گروه باشد یک همریختی از G به G را یک درون‌ریختی G گوییم. مجموعه‌ی همه‌ی درون‌ریختی‌های G را با $\operatorname{End} G$ نشان می‌دهیم. $\operatorname{End} G$ تحت عمل ترکیب توابع مونویید است. همریختی همانی $\mathrm{id}_G : G \longrightarrow G$ عضو همانی $\operatorname{End} G$ است. یکریختی از G به G را خودریختی گوییم. مجموعه‌ی همه‌ی خودریختی‌های G را با $\operatorname{Aut} G$ نشان می‌دهیم. $\operatorname{Aut} G$ تحت عمل ترکیب توابع یک گروه است، در واقع $\operatorname{Aut} G = (\operatorname{End} G)^\times$. در قضیه‌ی بعدی گروه خودریختی‌های $\mathbb{Z}$ و $\mathbb{Z}_n$ را می‌یابیم، که از آن جا گروه خودریختی‌های هر گروه دوری معین می‌شود (تمرین ۱۲ را ببینید).

قضیه ۸.۳.۳. (الف) $\operatorname{Aut} \mathbb{Z} \cong \mathbb{Z}^\times$ (ب) $\operatorname{Aut} \mathbb{Z}_n \cong \mathbb{Z}_n^\times$

اثبات. (الف) اگر $f : \mathbb{Z} \longrightarrow \mathbb{Z}$ یک خودریختی باشد در این صورت، بنا به قضیه‌ی ۵.۳.۳، برای هر $n \in \mathbb{Z}$ داریم $f(n) = nf(۱)$. چون $۱ \in \mathbb{Z}$ و f پوشاست، عضو $m \in \mathbb{Z}$ وجود دارد که $f(m) = ۱$. در نتیجه $mf(۱) = ۱$. بنابراین $f(۱) = ۱$ یا $f(۱) = -۱$. اگر $f(۱) = ۱$ داریم $f(n) = n$، برای هر n. پس f خودریختی همانی است. اگر $f(۱) = -۱$ داریم $f(n) = -n$. بنابراین $|\operatorname{Aut} \mathbb{Z}| = ۲$ و $\operatorname{Aut} \mathbb{Z} \cong \mathbb{Z}^\times$.

(ب) فرض کنید $\bar{a} \in \mathbb{Z}_n^\times$. تابع $f_a : \mathbb{Z}_n \longrightarrow \mathbb{Z}_n$ را با ضابطه‌ی $f_a(\bar{x}) = \overline{ax}$ تعریف می‌کنیم. f_a خوشتعریف و یک‌به‌یک است، زیرا

$$\bar{x} = \bar{y} \Longleftrightarrow \bar{a}\bar{x} = \bar{a}\bar{y} \Longleftrightarrow \overline{ax} = \overline{ay} \Longleftrightarrow f_a(\bar{x}) = f_a(\bar{y}).$$

f_a همریختی است، زیرا

$$f_a(\bar{x}+\bar{y}) = f_a(\overline{x+y}) = \overline{a(x+y)} = \overline{ax} + \overline{ay} = f_a(\bar{x}) + f_a(\bar{y}).$$

اکنون نشان می‌دهیم که تابع f_a پوشاست. عضو دلخواه $\bar{y} \in \mathbb{Z}_n$ را در نظر می‌گیریم. چون $\gcd\{a,n\} = ۱$، اعداد صحیح r و s وجود دارند که $ra + sn = ۱$. پس $\overline{ar} = \bar{۱}$ و داریم $\overline{ary} = \bar{y}$. بنابراین $f_a(\bar{r}\bar{y}) = \bar{y}$. در نتیجه $f_a \in \operatorname{Aut}\mathbb{Z}_n$. حال اگر $\bar{a} = \bar{b}$ به ازای هر $\bar{x} \in \mathbb{Z}_n$ داریم $\bar{a}\bar{x} = \bar{b}\bar{x}$ و بنابراین $f_a(\bar{x}) = f_b(\bar{x})$ برای هر $\bar{x} \in \mathbb{Z}_n$. پس $f_a = f_b$. بنابراین $f : \mathbb{Z}_n^\times \longrightarrow \operatorname{Aut}\mathbb{Z}_n$ با ضابطه‌ی $f(\bar{a}) = f_a$ خوش تعریف است. f یک‌به‌یک است، زیرا

$$f(\bar{a}) = f(\bar{b}) \Longrightarrow f_a = f_b \Longrightarrow f_a(\bar{۱}) = f_b(\bar{۱}) \Longrightarrow \bar{a} = \bar{b}.$$

f همریختی است، زیرا برای هر $\bar{x} \in \mathbb{Z}_n$

$$f_{ab}(\bar{x}) = \overline{abx} = f_a(\bar{b}\bar{x}) = f_a f_b(\bar{x}).$$

پس $f_{ab} = f_a f_b$ و $f(\bar{a}\bar{b}) = f(\bar{a})f(\bar{b})$. درنهایت برای هر $\psi \in \operatorname{Aut}\mathbb{Z}_n$، قرار می‌دهیم $\bar{a} = \psi(\bar{۱})$. به راحتی می‌توان دید $\bar{a} \in \mathbb{Z}_n^\times$ و $f_a = \psi$. در نتیجه f پوشاست. □

برای هر گروه دلخواه می‌توان، با استفاده از رابطه‌ی مزدوجی، خودریختی‌هایی موسوم به داخلی ساخت. خودریختی داخلی گروه G به صورت زیر تعریف می‌شود. اگر $g \in G$، تابع $\tau_g : G \longrightarrow G$ را با ضابطه‌ی $\tau_g(x) = gxg^{-۱}$ خودریختی داخلی G گوییم. τ_g یک‌به‌یک است، زیرا

$$\tau_g(x) = ۱ \Longrightarrow gxg^{-۱} = ۱ \Longrightarrow x = ۱.$$

τ_g پوشاست، زیرا برای هر $y \in G$ داریم

$$\tau_g(g^{-۱}yg) = g(g^{-۱}yg)g^{-۱} = y.$$

τ_g همریختی است، زیرا برای هر $x, y \in G$ داریم

$$\tau_g(xy) = g(xy)g^{-۱} = \left(gxg^{-۱}\right)\left(gyg^{-۱}\right) = \tau_g(x)\tau_g(y).$$

ملاحظه کنید $\tau_g = \mathrm{id}_G$ اگر و تنها اگر برای هر $x \in G$، $\tau_g(x) = x$ اگر و تنها اگر برای هر $x \in G$، $gxg^{-۱} = x$ اگر و تنها اگر $xg = gx$. پس $\tau_g = \mathrm{id}_G$ اگر و تنها اگر g با تمامی اعضای G تعویض شود.

تمرین‌ها

۱. فرض کنید $f : G \longrightarrow H$ یک همریختی و $a \in G$ عضوی با مرتبه‌ی متناهی باشد. ثابت کنید
(الف) $O(f(a)) | O(a)$.
(ب) اگر f یک‌به‌یک باشد، آن‌گاه $O(f(a)) = O(a)$.

۲. فرض کنید $f : \langle a\rangle \longrightarrow H$ همریختی باشد. ثابت کنید $f(\langle a\rangle) = \langle f(a)\rangle$.

۳. نشان دهید (الف) $\mathbb{R}^\times \ncong \mathbb{C}^\times$ (ب) $\mathbb{Z} \ncong \mathbb{Q}$ (ج) $\mathbb{Q}^\times \ncong \mathbb{Q}$
(د) $\mathbb{R}^\times \ncong \mathbb{R}$ (هـ) $\mathbb{R} \ncong \mathbb{Q}$ (و) $D_۸ \ncong Q_۸$.

۴. اگر $|X| = |Y|$، ثابت کنید $S_X \cong S_Y$.

۵. اگر G گروه باشد، نشان دهید $\operatorname{Aut} G$ تحت عمل ترکیب توابع گروه است.

۶. ثابت کنید نگاشت $f : G \longrightarrow G$ با ضابطه‌ی $f(g) = g^{-۱}$ همریختی است اگر و تنها اگر G آبلی باشد.

۷. ثابت کنید نگاشت $f : G \longrightarrow G$ با ضابطه‌ی $f(g) = g^۲$ همریختی است اگر و تنها اگر G آبلی باشد.

۸. اگر گروه G عضوی چون g داشته باشد که $g^۲ \neq ۱$، نشان دهید $\operatorname{Aut} G \neq \{۱\}$.

۹. فرض کنید G گروهی متناهی باشد و $f \in \operatorname{Aut} G$ تنها عضو همانی را ثابت نگه دارد. ثابت کنید $G = \{a^{-۱} f(a) \mid a \in G\}$.

۱۰. فرض کنید G گروهی متناهی و $f \in \operatorname{Aut} G$ یک خودریختی مرتبه‌ی دو باشد که تنها عضو همانی را ثابت نگه دارد. ثابت کنید G آبلی و از مرتبه‌ی فرد است.

۱۱. ثابت کنید (الف) $\operatorname{Aut} S_۳ \cong S_۳$. (ب) $\operatorname{Aut} V_۴ \cong S_۳$.

۱۲. اگر $G \cong H$ نشان دهید $\operatorname{Aut} G \cong \operatorname{Aut} H$. آیا عکس مطلب درست است؟

۱۳. نشان دهید $\mathrm{GL}_۲(\mathbb{Z}_۲) \cong S_۳$.

۱۴. اگر H آبلی [دوری] و $f : G \longrightarrow H$ همریختی یک‌به‌یک باشد، نشان دهید G آبلی [دوری] است.

۱۵. اگر G آبلی [دوری] و $f : G \longrightarrow H$ همریختی پوشا باشد، نشان دهید H آبلی [دوری] است.

۱۶. فرض کنید V یک فضای برداری با بعد n (n عدد طبیعی) روی میدان $\mathbb{Z}_p$ باشد، ثابت کنید $\operatorname{Aut} V \cong \mathrm{GL}_n(\mathbb{Z}_p)$.

۱۷. فرض کنید p عددی اول و G یک گروه آبلی باشد و به ازای هر $g \in G$ داشته باشیم $g^p = ۱$. ثابت کنید $G \cong V$، که در آن V یک فضای برداری روی $\mathbb{Z}_p$ است. نتیجه بگیرید اگر G متناهی باشد آن‌گاه به ازای عدد طبیعی nی داریم $|G| = p^n$.

۱۸. فرض کنید F یک میدان باشد. ثابت کنید تابع $f : \mathrm{GL}_n(F) \longrightarrow \mathrm{GL}_n(F)$ با ضابطه‌ی $f(x) = (x^{-۱})^t$ یک خودریختی است (y^t ترانهاده‌ی y است).

۱۹. اگر F یک میدان باشد ثابت کنید $F \ncong F^\times$.

۲۰. اگر G گروهی با بیش از دو عضو باشد ثابت کنید $\operatorname{Aut} G \neq \{۱\}$.

۴.۳ زیرگروه

برخی از گروه‌های مهم زیرمجموعه‌هایی از گروه‌های دیگر هستند. بنابراین به زیرمجموعه‌هایی مثل H از گروه G توجه داریم که خودشان گروه باشند. چنین Hای را زیرگروه G گوییم. به طور دقیق‌تر فرض کنید G یک گروه باشد. اگر H زیرمجموعه‌ی ناتهی از G باشد که تحت عمل ضرب تعریف شده در G و تحت وارون بسته باشد، یعنی برای هر $x, y \in H$ داشته باشیم $xy \in H$ و $x^{-۱} \in H$، آن‌گاه H را زیرگروه G گوییم و می‌نویسیم $H \leq G$. اگر $H \leq G$ و $H \neq G$ می‌نویسیم $H < G$ و می‌گوییم H زیرگروه سره‌ی G است. توجه کنید اگر $H \leq G$، آن‌گاه H تحت عمل تعریف شده در G یک گروه است. چون $H \neq \emptyset$ عضو $x_۰ \in H$ وجود دارد. پس $x_۰^{-۱} \in H$ و $۱ = x_۰ x_۰^{-۱} \in H$. در نتیجه $۱ \in H$. خاصیت شرکت‌پذیری نیز به وضوح در H برقرار است.

مثال ۱.۴.۳. داریم $\mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R} \leq \mathbb{C}$، $C_{p^n} \leq C_{p^\infty}$. به ازای هر $n \geq ۱$، داریم $\mathrm{SL}_n(F) \leq \mathrm{GL}_n(F)$. هم‌چنین اگر F میدان باشد، آن‌گاه $\square$

هر گروه G حداقل دو زیرگروه، $\{۱\}$، و G، دارد که آن‌ها را زیرگروه‌های بدیهی G گوییم. در صورتی که H زیرمجموعه‌ی ناتهی و متناهی از یک گروه باشد برای این که H زیرگروه G باشد کافی است تحت ضرب بسته باشد. این مطلب محتوای قضیه‌ی زیر است.

قضیه ۲.۴.۳. فرض کنید G گروه باشد. اگر H زیرمجموعه‌ی ناتهی و متناهی از G باشد که تحت عمل ضرب تعریف شده در G بسته است، آن‌گاه $H \leq G$.

اثبات. باید ثابت کنیم H نسبت به داشتن وارون بسته است. فرض کنید $x \in H$. چون H نسبت به ضرب بسته است، همه‌ی توان‌های مثبت x یعنی

$$x, x^۲, x^۳, \ldots$$

همگی در H قرار دارند. چون H متناهی است، به ازای i و jای که $i \neq j$ داریم $x^i = x^j$. فرض کنید، مثلاً $j < i$. پس با فرض $n = i - j$ داریم $۱ = x^n \in H$. توجه کنید که $n \geq ۱$، بنابراین $x^{-۱} = x^{n-۱} \in H$ و اثبات کامل است. $\square$

مثال ۳.۴.۳. فرض کنید $f : G \longrightarrow H$ همریختی باشد و $K \leq H$. نشان دهید $f^{-1}(K)$ زیرگروهی از G است.

حل چون K زیرگروه H است، با توجه به قضیه‌ی ۵.۳.۳، داریم $f(1_G) = 1_H \in K$، یعنی $1_G \in f^{-1}(K)$. از طرف دیگر اگر $x, y \in f^{-1}(K)$، آنگاه $f(x) \in K$ و $f(y) \in K$. در نتیجه

$$f(xy) = f(x)f(y) \in K, \quad f(x^{-1}) = f(x)^{-1} \in K.$$

پس $xy \in f^{-1}(K)$ و $x^{-1} \in f^{-1}(K)$. □

به ویژه اگر $K = \{1_H\}$ زیرگروه بدیهی H باشد، آنگاه

$$f^{-1}(\{1_H\}) = \{x \in G \mid f(x) = 1_H\}$$

زیرگروهی از G است که آن را هسته‌ی f گوییم و با $\ker f$ نشان می‌دهیم.

مثال ۴.۴.۳. فرض کنید G و H گروه باشند. نشان دهید همریختی $f : G \longrightarrow H$ یک‌به‌یک است اگر و تنها اگر $\ker f = \{1_G\}$.

حل فرض کنید f همریختی یک‌به‌یک باشد و $f(x) = 1_H$. در این صورت چون $f(1_G) = 1_H$، داریم $x = 1_G$. پس $\ker f = \{1_G\}$. برعکس اگر $\ker f = \{1_G\}$ آنگاه f یک‌به‌یک است، زیرا

$$\begin{aligned} f(x) = f(y) &\implies f(x)f(y)^{-1} = 1_H \\ &\implies f(x)f(y^{-1}) = 1_H \\ &\implies f(xy^{-1}) = 1_H \\ &\implies xy^{-1} \in \ker f \\ &\implies xy^{-1} = 1_G \\ &\implies x = y. \end{aligned}$$ □

اگر $f : G \longrightarrow H$ همریختی باشد و $K \leq G$ به راحتی می‌توان دید (تمرین ۷ را ببینید) که $f(K)$ زیرگروهی از H است. به ویژه $f(G) = \operatorname{Im} f$ زیرگروه H است. اگر $f : G \longrightarrow H$ همریختی یک‌به‌یک باشد، آنگاه $G \cong \operatorname{Im} f$. پس G با زیرگروهی از H یکریخت است. در این حالت گوییم G در H نشانده شده و می‌نویسیم $G \hookrightarrow H$ و f را یک جادهی گوییم.
گروه خودریختی‌های $\operatorname{Aut} G$ یک زیرگروه مهم دارد و آن $\operatorname{Inn} G$ متشکل از خودریختی‌های داخلی است. چون $\mathrm{id}_G = \tau_1 \in \operatorname{Inn} G$ داریم $\operatorname{Inn} G \neq \emptyset$. حال اگر $\tau_g, \tau_h \in \operatorname{Inn} G$ به ازای هر $x \in G$ داریم

$$(\tau_g\tau_h)(x) = \tau_g\left(hxh^{-1}\right) = g\left(hxh^{-1}\right)g^{-1} = (gh)x(gh)^{-1} = \tau_{gh}(x).$$

بنابراین $\tau_g\tau_h = \tau_{gh} \in \operatorname{Inn} G$. هم‌چنین

$$\tau_g\tau_{g^{-1}} = \tau_{gg^{-1}} = \tau_1 \quad \text{و} \quad \tau_{g^{-1}}\tau_g = \tau_{g^{-1}g} = \tau_1,$$

بنابراین $\tau_g^{-1} = \tau_{g^{-1}} \in \operatorname{Inn} G$. از این‌رو $\operatorname{Inn} G \leq \operatorname{Aut} G$.
یادآوری می‌کنیم $\tau_g(x) = x$ اگر و تنها اگر برای هر $x \in G$، $gxg^{-1} = x$ اگر و تنها اگر $xg = gx$. پس $\tau_g = \mathrm{id}_G$ اگر و تنها اگر g با تمامی اعضای G تعویض شود. بنابراین $\operatorname{Inn} G = \{\mathrm{id}_G\}$ اگر و تنها اگر G آبلی باشد.
یادآوری می‌کنیم در صورتی که یک عضو g را از یک گروه G در اختیار داشته باشیم با استفاده از توان‌های آن یک زیرگروه به دست می‌آید که آن را زیرگروه دوری تولید شده توسط g گوییم. تعریف می‌کنیم

$$\langle g \rangle = \{g^n \mid n \in \mathbb{Z}\} \qquad \text{(در نماد ضربی)}$$
$$\langle g \rangle = \{ng \mid n \in \mathbb{Z}\} \qquad \text{(در نماد جمعی)}$$

$\langle g\rangle$ یک زیرگروه G است. به علاوه $\langle g\rangle$ کوچک‌ترین زیرگروه از G شامل g است، زیرا اگر $H \leq G$ و $g \in H$، آنگاه چون H زیرگروه G است، برای هر $n \in \mathbb{Z}$ داریم $g^n \in H$. پس $\langle g\rangle \subseteq H$. g را مولد $\langle g\rangle$ می‌نامیم.
در ادامه این بخش ساختار گروه‌های دوری را بررسی می‌کنیم. ابتدا ثابت می‌کنیم هر زیرگروه یک گروه دوری، دوری است.

قضیه ۵.۴.۳. فرض کنید $G = \langle g\rangle$ یک گروه دوری باشد و $H \leq G$. آنگاه H دوری است. به طور مشخص $H = \langle g^m\rangle$ که در آن m کوچک‌ترین عدد صحیح مثبت است که $g^m \in H$.

اثبات. اگر $H = \{۱\}$ چیزی برای اثبات نیست. پس فرض کنیم $a \in H \neq ۱$ وجود داشته باشد. چون $a \in H \leq \langle g\rangle$ پس به ازای یک $n \in \mathbb{Z}$، داریم $g^n = a \in H$. اگر $n < ۰$، آنگاه $g^{-n} = a^{-۱} \in H$. پس توان مثبتی از g در H قرار دارد. فرض کنید m کوچک‌ترین عدد صحیح مثبتی باشد که $g^m \in H$. ادعا می‌کنیم $H = \langle g^m\rangle$. چون $g^m \in H$ داریم $\langle g^m\rangle \subseteq H$. حال اگر $x \in H$ چون $x \in \langle g\rangle$، به ازای یک $n \in \mathbb{Z}$ داریم $x = g^n$. بنا به الگوریتم تقسیم اعداد صحیح r و q وجود دارند که $n = mq + r$ و $۰ \leq r < m$. بنابراین

$$x = g^n = g^{mq+r} = (g^m)^q g^r.$$

باید ثابت کنیم $r = ۰$. اگر $r \neq ۰$، آنگاه

$$g^r = (g^{mq})^{-۱} x \in H$$

که این خلاف انتخاب m است. پس $r = ۰$. از این‌رو $x = (g^m)^q$؛ یعنی $x \in \langle g^m\rangle$. بنابراین $H \subseteq \langle g^m\rangle$. در نتیجه $H = \langle g^m\rangle$. □

مثال ۶.۴.۳. چون $\mathbb{Z} = \langle ۱\rangle$ دوری است پس هر زیرگروه $\mathbb{Z}$ دوری است. اگر $H \leq \mathbb{Z}$، آنگاه $H = \langle k\rangle = k\mathbb{Z}$ که در آن k کوچک‌ترین عدد صحیح مثبت است که $k = k۱ \in H$. بنابراین همه‌ی زیر گروه‌های $\mathbb{Z}$ عبارت‌اند از

$$\{۰\},\ \mathbb{Z},\ ۲\mathbb{Z},\ ۳\mathbb{Z},\ \ldots. \qquad \square$$

قضیه ۷.۴.۳. فرض کنید $G = \langle g\rangle$ یک گروه دوری متناهی از مرتبه‌ی n باشد. اگر $s|n$، آنگاه G یک زیرگروه یکتا از مرتبه‌ی s دارد.

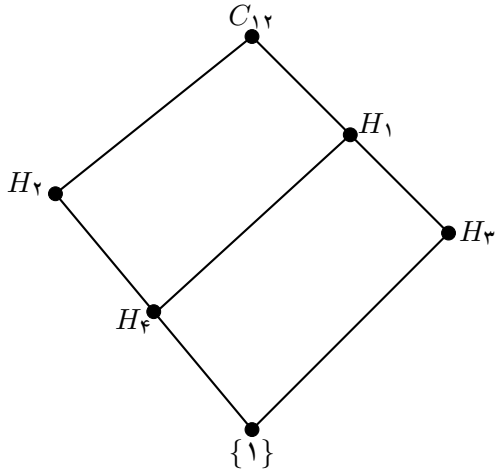
اثبات. چون $O(g^{\frac{n}{s}}) = sk$، $H = \left\langle g^{\frac{n}{s}}\right\rangle$ زیرگروهی از G با مرتبه‌ی s است. حال ثابت می‌کنیم H یکتا زیرگروه G از مرتبه‌ی s است. اگر $K \leq G$ و $|K| = s$، آنگاه بنا به قضیه‌ی ۵.۴.۳، عدد m وجود دارد که $K = \langle g^m\rangle$. چون $O(g^m) = s$ داریم $g^{ms} = ۱$. بنابراین $n|ms$ و $\frac{n}{s}\Big| m$. پس $K = \left\langle g^{\frac{n}{s}}\right\rangle$ و در نتیجه $g^m \in \left\langle g^{\frac{n}{s}}\right\rangle = K \subseteq H$. اکنون چون H و K متناهی‌اند و $|H| = |K|$، داریم $H = K$. □

اگر $w = e^{\frac{۲\pi i}{n}}$، آنگاه $C_n = \langle w\rangle$ گروه دوری از مرتبه‌ی n است. پس هر زیرگروه آن دوری است و به ازای هر s که $s|n$ زیرگروه یکتای $H_s = \left\langle w^{\frac{n}{s}}\right\rangle$ را داریم.

مثال ۸.۴.۳. اگر $w = e^{\frac{۲\pi i}{۱۲}}$، آنگاه $C_{۱۲} = \langle w\rangle$ یک گروه دوری مرتبه‌ی ۲۱ است. همه‌ی زیرگروه‌های $C_{۱۲}$ عبارت‌اند از

$$\begin{aligned}
C_{۱۲} = \langle w\rangle = \left\langle w^{۵}\right\rangle = \left\langle w^{۷}\right\rangle = \left\langle w^{۱۱}\right\rangle &\quad : \text{زیرگروه مرتبه‌ی } ۱۲\\
H_۱ = \left\langle w^{۲}\right\rangle = \left\langle w^{۱۰}\right\rangle &\quad : \text{زیرگروه مرتبه‌ی } ۶\\
H_۲ = \left\langle w^{۳}\right\rangle = \left\langle w^{۹}\right\rangle &\quad : \text{زیرگروه مرتبه‌ی } ۴\\
H_۳ = \left\langle w^{۴}\right\rangle = \left\langle w^{۸}\right\rangle &\quad : \text{زیرگروه مرتبه‌ی } ۳\\
H_۴ = \left\langle w^{۶}\right\rangle &\quad : \text{زیرگروه مرتبه‌ی } ۲\\
\langle ۱\rangle &\quad : \text{زیرگروه مرتبه‌ی } ۱
\end{aligned}$$

زیرگروه‌های $C_{۱۲}$ و ارتباط بین آن‌ها را می‌توان با شکل ۲.۳، که نمودار زیرگروه‌های آن نامیده می‌شود مشخص کرد.



شکل ۲.۳: نمودار زیرگروه‌های $C_{۱۲}$.

تمرین‌ها

۱. نشان دهید زیرگروه‌های سره $Q_۸$ و $V_۴$ دوری هستند ، اما این گروه‌ها دوری نیستند.

۲. ثابت کنید هر دو زیرگروه $\mathbb{Q}$ اشتراک نابدیهی دارند.

۳. نشان دهید هیچ گروهی را نمی‌توان به صورت اجتماع دو زیرگروه نابدیهی و متمایز نوشت. گروهی بیابید که اجتماع سه زیرگروه نابدیهی و متمایز باشد.

۴. اگر G گروه آبلی باشد، ثابت کنید مجموعه‌ی عناصر با مرتبه‌ی متناهی G یک زیرگروه تشکیل می‌دهند.

۵. فرض کنید g عضوی از یک گروه با مرتبه‌ی $n \geq ۱$ باشد. نشان دهید گروه دوری تولید شده توسط g برابر $\{۱, g, g^۲, \ldots, g^{n-۱}\}$ است.

۶. اگر $H \leq G$، $g \in G$، $O(g) = n$، $g^m \in H$، و $\gcd\{m, n\} = ۱$ ثابت کنید $g \in H$.

۷. اگر $f : G \longrightarrow H$ همریختی باشد و $K \leq G$ ثابت کنید $f(K) \leq H$.

۸. فرض کنید

$$G = \left\{ \begin{bmatrix} a & b \\ ۰ & c \end{bmatrix} \middle| \, a, b, c \in \mathbb{R}, ac \neq ۰ \right\}, H = \left\{ \begin{bmatrix} ۱ & b \\ ۰ & ۱ \end{bmatrix} \middle| \, b \in \mathbb{R} \right\}.$$

ثابت کنید $H \leq G \leq \mathrm{GL}_۲(\mathbb{R})$، و $H \cong \mathbb{R}$. عناصر مرتبه‌ی دو در G را بیابید.

۹. فرض کنید X, Y دو زیر مجموعه‌ی گروه G باشند. تعریف می‌کنیم

$$XY = \{xy \mid y \in X,\ y \in Y\}$$

و $X\{y\}$ را با Xy نشان می‌دهیم. هرگاه H، K دو زیرگروه از G باشند، نشان دهید در حالت کلی ممکن است HK زیرگروه G نباشد.

۱۰. فرض کنید H و K دو زیرگروه G باشند. ثابت کنید $HK \leq G$ اگر و تنها اگر $HK = KH$.

۱۱. اگر H، K، N زیر زیرگروه‌هایی از گروه G باشند که $H \leq K$، $H \cap N = K \cap N$، و $HN = KN$. نشان دهید $H = K$.

۱۲. فرض کنید K، H دو زیرگروه G باشند و به ازای $x, y \in G$ داشته باشیم $Hx = Ky$. نشان دهید $H = K$.

۱۳. اگر $\{H_i\}_{i \in I}$ خانواده‌ای از زیر گروه‌های G باشد ثابت کنید $\bigcap_{i \in I} H_i \leq G$.

۱۴. همه‌ی زیرگروه‌های $\mathbb{Z}_{۱۵}$، $\mathbb{Z}_{۳۰}$، و $\mathbb{Z}_۷$ $\mathbb{Z}_{۳۸}$، $C_{۱۲}$، $C_{۱۵}$، $C_۷$، و $C_{۳۸}$ را بیابید.

۱۵. نشان دهید هر زیرگروه سره‌ی C_{p^∞} دوری است.

۱۶. فرض کنید G گروهی باشد که اگر $J < H \leq G$، آنگاه $J \trianglelefteq H$. نشان دهید G تاب‌دار است. مثالی از چنین گروهی ارائه کنید.

۱۷. اگر $H_1 \leq H_2 \leq \cdots$ یک زنجیر صعودی از زیر گروه‌های G باشد ثابت کنید $\bigcup_{n=1}^{\infty} H_n \leq G$.

۱۸. فرض کنید $S_{\mathbb{N}}$ گروه همه‌ی جایگشت‌ها روی مجموعه‌ی اعداد طبیعی باشد. یادآوری می‌کنیم به ازای هر n، $S_n = \{\alpha \in S_{\mathbb{N}} \mid \forall j > n,\ \ \alpha(j) = j\}$. نشان دهید
(الف) $G = \bigcup_{n=1}^{\infty} S_n$ یک گروه است و اعضای آن را توصیف کنید.
(ب) به ازای هر $n \in \mathbb{N}$، G زیرگروه‌های دوری از مرتبه‌ی n دارد ؛ اما به ازای هر عدد اول p زیرگروهی یکریخت با C_{p^∞} ندارد.

۱۹. (ددکیند) فرض کنید H، K، L زیر زیرگروه‌هایی از گروه G باشند و $K \subseteq L$. ثابت کنید $HK \cap L = (H \cap L)K$.

۲۰. فرض کنید $H < G$ و $g \in G$. نشان دهید $H(g^{-1}Hg) \subset G$.

۲۱. اگر G گروهی باشد که $|G| > 1$ و هیچ زیرگروه نابدیهی نداشته باشد، ثابت کنید G دوری، متناهی، و از مرتبه‌ی عددی اول است.

۲۲. ثابت کنید هر گروه نامتناهی تعداد نامتناهی زیرگروه دارد.

۲۳. فرض کنید گروه G حداقل یک زیرگروه نابدیهی داشته باشد. ثابت کنید G دوری نامتناهی است اگر و تنها اگر با هر زیرگروه غیرهمانی‌اش یکریخت باشد.

۲۴. فرض کنید G گروه نابدیهی باشد. زیرگروه سره M از G را زیرگروه ماکسیمال گوییم هرگاه هیچ زیرگروه K وجود نداشته باشد که $M < K < G$. نشان دهید در یک گروه متناهی هر زیرگروه سره در یک زیرگروه ماکسیمال قرار دارد.

۲۵. نشان دهید C_{p^∞} زیرگروه ماکسیمال ندارد.

۲۶. اگر V فضای برداری نابدیهی روی یک میدان F باشد، ثابت کنید $\mathrm{GL}(V) \leq \mathrm{Aut}\, V$

۵.۳ تولید گروه‌ها، گروه‌های متناهیاً تولید شده

می‌توان بحث گروه دوری تولید شده توسط یک عضو را تعمیم داد. فرض کنید X زیرمجموعه‌ی ناتهی از گروه G باشد. اگر زیرگروهی از G شامل X باشد، چون نسبت به ضرب و وارون بسته است، همه‌ی توان‌های مثبت و منفی اعضای X و هم‌چنین همه‌ی حاصل‌ضرب‌های اعضای X را دربر دارد. بنابراین گروه تولید شده توسط X را برابر همه‌ی حاصل‌ضرب‌های توان‌های اعضای X تعریف می‌کنیم:

$$\langle X\rangle = \{x_1^{n_1}x_2^{n_2}\cdots x_k^{n_k} \mid k \in \mathbb{N},\quad n_i \in \mathbb{Z},\quad x_i \in X\} \quad \text{(در نماد ضربی)}$$

$$\langle X\rangle = \{n_1x_1 + n_2x_2 + \cdots + n_kx_k \mid k \in \mathbb{N}, n_i \in \mathbb{Z}, x_i \in X\} \quad \text{(در نماد جمعی)}$$

به سادگی دیده می‌شود $\langle X\rangle$ زیرگروه G است. در واقع $\langle X\rangle$ کوچک‌ترین زیرگروه G، شامل X است. X را مجموعه‌ی مولد برای $\langle X\rangle$ گوییم. وقتی که $X = \emptyset$، قرار داد می‌کنیم $\langle X\rangle = \{1\}$. اگر $X = \{a_1, \ldots, a_m\}$ زیرمجموعه‌ی متناهی از گروه G باشد، گروه تولید شده توسط X را با $\langle a_1, \ldots, a_m\rangle$ نشان می‌دهیم و آن را زیرگروه متناهیاً تولید شده گوییم.

مثال ۱.۵.۳. گروه Q_8 دوری نیست و داریم

$$Q_8 = \langle i, j\rangle = \langle i, k\rangle = \langle k, j\rangle\,.$$

بنابراین حداقل دو عضو برای تولید Q_8 لازم است. □

مثال ۲.۵.۳. ۴-گروه کلاین $V_4 = \{e, a, b, c\}$ دوری نیست و داریم

$$V_4 = \langle a, b\rangle = \langle b, c\rangle = \langle a, c\rangle\,.$$

بنابراین حداقل دو عضو برای تولید V_4 لازم است. □

مـثـال ۳.۵.۳. هـر دور $\alpha = (x_1\ x_2\ \cdots\ x_r)$ در S_n را مـی‌تـوان بـه صـورت حـاصـل‌ضـرب تـرانـهـش‌هـا نـوشـت: $\alpha = (x_1\ x_r)\cdots(x_1\ x_3)(x_1\ x_2)$. چون هر جایگشت در S_n به صورت حاصل‌ضرب دورهای مجزا نوشته می‌شود، ترانهش‌ها S_n را تولید می‌کنند. □

مثال ۴.۵.۳. یک مجموعه‌ی مولد برای گروه ضربی $\mathbb{Q}^{\times}_{pos} = \{x \in \mathbb{Q} \mid x > 0\}$ بیابید.

حل فرض کنید $\frac{r}{s} \in \mathbb{Q}^{\times}_{pos}$. اعداد صحیح مثبت r و s را به حاصل‌ضرب عوامل اول تجزیه می‌کنیم: $r = p_1^{n_1}p_2^{n_2}\cdots p_k^{n_k}$ و $s = p_1^{m_1}p_2^{m_2}\cdots p_k^{m_k}$، که در آن p_i، iامین عدد اول است و $m_i \geq 0$ و n_i. (فرض کرده‌ایم که $p_1 < p_2 < \cdots$ دنباله اعداد اول به ترتیب صعودی باشند، پس ممکن است بعضی از n_iها و m_iها صفر باشند). از این‌رو داریم

$$\frac{r}{s} = \frac{p_1^{n_1}p_2^{n_2}\cdots p_k^{n_k}}{p_1^{m_1}p_2^{m_2}\cdots p_k^{m_k}} = p_1^{n_1-m_1}p_2^{n_2-m_2}\cdots p_k^{n_k-m_k}.$$

بنابراین

$$\frac{r}{s} \in \langle \{p \mid p \text{ عدد اول}\} \rangle .$$

پس

$$\mathbb{Q}^{\times}_{pos} = \langle \{p \mid p \text{ عدد اول}\} \rangle$$

و $\{p \mid p \text{ عدد اول}\}$ یک مجموعه‌ی مولد برای گروه ضربی $\mathbb{Q}^{\times}_{pos}$ است. □

حال سوال این است که آیا یک مجموعه‌ی متناهی می‌تواند $\mathbb{Q}^{\times}_{pos}$ را تولید کند؟ این مطلب در تمرین‌ها خواسته شده است.

مثال ۵.۵.۳. توابع $\varepsilon : \mathbb{R} \longrightarrow \mathbb{R}$ و $\tau : \mathbb{R} \longrightarrow \mathbb{R}$ را با ضابطه‌های

$$\tau(x) = x + 1, \quad \varepsilon(x) = -x$$

در نظر بگیرید. واضح است که ε و τ توابع دوسویی‌اند، یعنی $\varepsilon, \tau \in S_{\mathbb{R}}$. گروه تولید شده توسط ε و τ را گروه دووجهی نامتناهی گوییم و با D_∞ نشان می‌دهیم

$$D_\infty = \langle \varepsilon, \tau \rangle .$$

می‌خواهیم شکل اعضای D_∞ را بیابیم. به ازای هر $x \in \mathbb{R}$ داریم

$$\varepsilon^2(x) = \varepsilon(\varepsilon(x)) = \varepsilon(-x) = x,$$

یعنی $O(\varepsilon) = 2$ و $\varepsilon^2 = 1$. از طرف دیگر به ازای هر $0 \neq n \in \mathbb{Z}$ و هر $x \in \mathbb{R}$ داریم

$$\tau^n(x) = x + n \neq x,$$

یعنی $O(\tau) = \infty$. اکنون به ازای هر $x \in \mathbb{R}$ داریم

$$\varepsilon\tau(x) = \varepsilon(x + 1) = -(x + 1) = -x - 1 = \tau^{-1}(-x) = \tau^{-1}\varepsilon(x).$$

بنابراین $\varepsilon\tau = \tau^{-1}\varepsilon$ و به ازای هر $n \in \mathbb{Z}$، $\varepsilon\tau^n = \tau^{-n}\varepsilon$. پس

$$D_\infty = \{\varepsilon^n\tau^m \mid \quad n \in \{0, 1\},\ \ m \in \mathbb{Z}\}. \qquad \square$$

اگر گروهی با دو عضو مرتبه‌ی ۲ تولید شود آن را گروه دووجهی گوییم. چون $D_{2n} = \langle \varepsilon, \varepsilon\rho \rangle$ و $D_\infty = \langle \varepsilon, \varepsilon\tau \rangle$، D_{2n} و D_∞ گروه‌های دووجهی هستند.

ممکن است به نظر بیاید که هر زیرگروه یک گروه متناهیاً تولید شده حتماً متناهیاً تولید شده است. اما این مطلب درست نیست. برای ارائه‌ی یک مثال ابتدا ثابت می‌کنیم:

قضیه ۶.۵.۳. اگر $G_1 < G_2 < G_3 < \cdots$ زنجیری سره از زیرگروه‌های یک گروه G باشد، آنگاه $H = \bigcup_{i=1}^{\infty} G_i$ زیرگروه G است و متناهیاً تولید شده نیست.

اثبات. به سادگی می‌توان دید که H زیرگروه G است (تمرین ۱۷ از صفحه‌ی ۷۰). حال نشان می‌دهیم H متناهیاً تولید شده نیست. فرض کنید چنین نباشد و $H = \langle h_1, \ldots, h_n \rangle$. چون $h_i \in H = \bigcup_{i=1}^{\infty} G_i$، به ازای هر $i = 1, \ldots, n$، عدد $m_i \in \mathbb{N}$ وجود دارد که $h_i \in G_{m_i}$. قرار می‌دهیم $m = \max\{m_1, \ldots, m_n\}$، پس $h_1, \ldots, h_n \in G_m$ و $H = \langle h_1, \ldots, h_n \rangle \subseteq G_m$. بنابراین $G_{m+1} \subseteq H = G_m$، که تناقض است. □

مثال ۷.۵.۳. فرض کنید G گروه ضربی تولید شده توسط ماتریس‌های $x = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ و $y = \begin{bmatrix} 2 & 0 \\ 0 & 1 \end{bmatrix}$ در $\mathrm{GL}_2(\mathbb{R})$ و H مجموعه‌ی همه‌ی ماتریس‌های در G باشد که درایه روی قطر اصلی‌شان برابر ۱ است. نشان دهید H زیرگروه G است و متناهیاً تولید شده نیست.

حل به سادگی می‌توان دید به ازای هر $n \in \mathbb{Z}$،

$$x^n = \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix} \quad \text{و} \quad y^n = \begin{bmatrix} 2^n & 0 \\ 0 & 1 \end{bmatrix}.$$

به ازای هر عدد صحیح $n \geq 0$، قرار می‌دهیم $x_n = y^{-n} x y^n$ و $H_n = \langle x_n \rangle$. پس

$$\begin{aligned} x_n &= \begin{bmatrix} 2^{-n} & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 2^n & 0 \\ 0 & 1 \end{bmatrix} \\ &= \begin{bmatrix} 1 & 2^{-n} \\ 0 & 1 \end{bmatrix}. \end{aligned}$$

هم‌چنین به سادگی می‌توان دید، به ازای هر $m \in \mathbb{Z}$،

$$x_n^m = \begin{bmatrix} 1 & m2^{-n} \\ 0 & 1 \end{bmatrix}.$$

چون $x_n = x_{n+1}^2 \in H_{n+1}$، داریم $H_n \leq H_{n+1}$. از طرف دیگر $x_{n+1} \notin H_n$، زیرا اگر به ازای یک $m \in \mathbb{Z}$ داشته باشیم $x_{n+1} = x_n^m$، آنگاه $2^{-(n+1)} = m2^{-n}$، یعنی $m = 2^{-1}$ که تناقض است. بنابراین، به ازای هر عدد صحیح $n \geq 0$، H_n زیرگروه سره‌ی H_{n+1} است. در نتیجه زنجیر سره‌ی $H_0 < H_1 < H_2 < \cdots$ از زیرگروه‌های G را داریم. بنا به قضیه‌ی ۶.۵.۳، $K = \bigcup_{n=0}^{\infty} H_n$ زیرگروه G است و متناهیاً تولید شده نیست. حال ثابت می‌کنیم $H = K$. به ازای هر $n \in \mathbb{N}$، طبق تعریف H، داریم $H_n \subseteq H$. بنابراین $K \subseteq H$. از طرف دیگر هر عضو $u \in G$ به صورت

$$\begin{aligned} u &= x^{n_1} y^{m_1} \cdots x^{n_k} y^{m_k} \\ &= \begin{bmatrix} 2^{m_1+\cdots+m_k} & n_1 + n_2 2^{m_1} + n_3 2^{m_1+m_2} \cdots + n_k 2^{m_1+\cdots+m_{k-1}} \\ 0 & 1 \end{bmatrix} \end{aligned}$$

است، که در آن $k \in \mathbb{N}$، و $n_i, m_i \in \mathbb{Z}$، $i = 1, \ldots, k$. بنابراین $u \in H$ اگر و تنها اگر $m_1 + \cdots + m_k = 0$. در این حالت داریم

$$\begin{aligned} u &= x^{n_1} y^{n_2} \cdots x^{n_k} y^{n_k} \\ &= \begin{bmatrix} 1 & n_1 + n_2 2^{m_1} + n_3 2^{m_1+m_2} \cdots + n_k 2^{m_1+\cdots+m_{k-1}} \\ 0 & 1 \end{bmatrix} \\ &= \begin{bmatrix} 1 & n_1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & n_2 2^{m_2} \\ 0 & 1 \end{bmatrix} \cdots \begin{bmatrix} 1 & n_k 2^{m_1+\cdots+m_{k-1}} \\ 0 & 1 \end{bmatrix} \\ &= x_0^{n_1} x_{r_1}^{s_1} x_{r_2}^{s_2} \cdots x_{r_k}^{s_k} \in K, \end{aligned}$$

که در آن (به ازای هر $i = ۱, ۲, \dots, k$) اگر $m_۱ + \cdots + m_{i-۱} \leq ۰$، آنگاه $s_i = n_i$ و $r_i = -(m_۱ + \cdots + m_{i-۱})$؛ اگر $m_۱ + \cdots + m_{i-۱} > ۰$، آنگاه $r_i = ۰$ و $s_i = n_i(۲^{m_۱ + \cdots + m_{i-۱}})$. پس $H = K$. □

تمرین‌ها

۱. اگر $f : G \longrightarrow H$ همریختی باشد و $X \subseteq G$ ثابت کنید $f(\langle X \rangle) = \langle f(X) \rangle$.

۲. فرض کنید X زیرمجموعه‌ای دلخواه از گروه G باشد، ثابت کنید

$$\langle X \rangle = \bigcap \{H \mid X \subseteq H \leq G\}.$$

۳. فرض کنید $H < G$، نشان دهید $\langle G - H \rangle = G$.

۴. نشان دهید هر زیرگروه متناهیاً تولید شده $\mathbb{Q}$ دوری است و نتیجه بگیرید $\mathbb{Q}$ متناهیاً تولید شده نیست.

۵. زیرگروهی از $\mathbb{Q}$ به‌جز $\mathbb{Q}$ ارائه کنید که دوری نباشد.

۶. ثابت کنید گروه ضربی اعداد گویای مثبت، $\mathbb{Q}^{\times}_{pos}$، متناهیاً تولید شده نیست.

۷. نشان دهید ، C_{p^∞} متناهیاً تولید شده نیست.

۸. ثابت کنید هر گروه متناهیاً تولید شده زیرگروه ماکسیمال دارد (راهنمایی: لم زُرن).

۹. ماتریس‌های $a = \begin{bmatrix} ۱ & ۱ \\ ۰ & ۱ \end{bmatrix}$ و $b = \begin{bmatrix} ۲ & ۰ \\ ۰ & ۱ \end{bmatrix}$ در $\mathrm{GL}_۲(\mathbb{R})$ را در نظر بگیرید. ثابت کنید $bab^{-۱} = a^۲$ و نتیجه بگیرید $\langle a, b \rangle = \{b^\alpha a^\beta b^\gamma \mid \alpha, \beta, \gamma \in \mathbb{Z}\}$.

۱۰. ماتریس‌های $a = \begin{bmatrix} ۱ & ۰ \\ ۰ & -۱ \end{bmatrix}$ و $b = \begin{bmatrix} ۱ & ۱ \\ ۰ & -۱ \end{bmatrix}$ در $\mathrm{GL}_۲(\mathbb{R})$ را در نظر بگیرید. ثابت کنید $\langle a, b \rangle \cong D_\infty$.

۱۱. نشان دهید (الف) $S_n = \langle (۱\ i) \mid ۲ \leq i \leq n \rangle$.

(ب) $S_n = \langle (i\ i+۱) \mid ۱ \leq i \leq n-۱ \rangle$.

(ج) $S_n = \langle (۱\ ۲), (۱\ ۲\ ۳\ \cdots\ n) \rangle$.

۱۲. نشان دهید (الف) $A_n = \langle (۱\ i\ j) \mid ۲ \leq i, j \leq n,\ i \neq j \rangle$.

(ب) $A_n = \langle (۱\ ۲\ i) \mid ۳ \leq i \leq n \rangle$.

۱۳. اگر هر زیرگروه متناهیاً تولید شده‌ی گروه G دوری باشد، G را موضعاً دوری گوییم. نشان دهید

(الف) $\mathbb{Q}$ موضعاً دوری است.

(ب) هر گروه موضعاً دوری آبلی است.

(ج) اگر G اجتماع زنجیر صعودی از زیرگروه‌های موضعاً دوری باشد، آنگاه G موضعاً دوری است.

۱۴. فرض کنید $\alpha : \mathbb{R} \longrightarrow \mathbb{R}$ و $\beta : \mathbb{R} \longrightarrow \mathbb{R}$ توابعی باشند که، به ازای هر $x \in \mathbb{R}$، $\alpha(x) = x + ۱$ و $\beta(x) = ۲x$.

(الف) نشان دهید α و β جایگشت هستند ، یعنی $\alpha, \beta \in S_{\mathbb{R}}$.

(ب) نشان دهید ، به ازای هر $x \in \mathbb{R}$، $\beta^n(x) = ۲^n x$.

(ج) به ازای هر $n \in \mathbb{N}$، فرض کنید $\alpha_n = \beta^{-n}\alpha\beta^n$ و نشان دهید ، به ازای هر $x \in R$، $\alpha_n(x) = x + ۲^{-n}$.

(د) فرض کنید H_n زیرگروه تولید شده توسط α_n در $S_{\mathbb{R}}$ باشد، یعنی $H_n = \langle \alpha_n \rangle$. ثابت کنید $H_n < H_{n+۱}$. نتیجه بگیرید $H = \bigcup_{n=۱}^{\infty} H_n$ زیرگروه $G = \langle \alpha, \beta \rangle$ است و متناهیاً تولید شده نیست.

۶.۳ چند زیرگروه مهم

اکنون چند زیرگروه مهم از گروه را معرفی می‌کنیم. این زیر گروه‌ها در بررسی ساختار گروه نقش اساسی دارند. فرض کنید G یک گروه باشد و $x \in G$. مرکزساز x در G را که با $C_G(x)$ نشان می‌دهیم مجموعه‌ی همه‌ی اعضای G است که با x تعویض می‌شوند، یعنی

$$C_G(x) = \{g \in G \mid xg = gx\}.$$

چون $x۱ = ۱x$، داریم $۱ \in C_G(x)$. از طرف دیگر اگر $g, h \in C_G(x)$، آنگاه

$$x(gh) = (xg)h = (gx)h = g(xh) = g(hx) = (gh)x.$$

پس $gh \in C_G(x)$. هم‌چنین چون $xg = gx$ داریم

$$g^{-۱}(xg)g^{-۱} = g^{-۱}(gx)g^{-۱}.$$

در نتیجه $g^{-۱}x = xg^{-۱}$ و $g^{-۱} \in C_G(x)$. بنابراین $C_G(x) \leq G$.

مثال ۱.۶.۳. مرکزساز $\alpha = (۱\ ۲\ ۳)$ در $S_۴$، یعنی $C_{S_۴}(\alpha)$ را بیابید.

حل فرض کنید $\beta \in C_{S_۴}(\alpha)$، در این صورت $\beta\alpha\beta^{-۱} = \alpha$. بنا به تمرین ۷ از صفحه‌ی ۳۴، $(\beta(۱)\ \beta(۲)\ \beta(۳)) = (۱\ ۲\ ۳)$. پس تنها ۳ امکان وجود دارد $\beta = (۱)$، $\beta = (۱\ ۲\ ۳)$، $\beta = (۱\ ۳\ ۲)$. بنابراین $C_G(\alpha) = \langle\alpha\rangle$. □

به طور کلی اگر X زیرمجموعه‌ای دلخواه و ناتهی از G باشد مرکزساز X در G عبارت است از

$$C_G(X) = \{g \in G \mid \forall x \in X, \quad xg = gx\}.$$

چون اشتراک هر دسته از زیرگروه‌های G مجدداً زیرگروه است، $C_G(X) = \bigcap_{x\in X} C_G(x)$ نیز زیرگروه G است. هرگاه H زیرگروه آبلی از G باشد به سادگی می‌توان دید $H \leq C_G(H)$. اگر $K \leq C_G(H)$ گوییم K، H را مرکزی می‌کند.
مرکز G عبارت است از $C_G(G)$ که آن را با $Z(G)$ نشان می‌دهیم

$$Z(G) = \{a \in G \mid \forall x \in G, \quad xa = ax\}.$$

واضح است که $C_G(a) = G$ اگر و تنها اگر $a \in Z(G)$. هم‌چنین واضح است که G آبلی است اگر و تنها اگر $Z(G) = G$.

مثال ۲.۶.۳. داریم $Z(Q_۸) = \{۱, -۱\}$ و $C_{Q_۸}(i) = \{\pm۱, \pm i\} = \langle i\rangle$. □

مثال ۳.۶.۳. فرض کنید X مجموعه‌ای دلخواه با بیش از دو عضو باشد، نشان دهید $Z(S_X) = \{\mathrm{id}_X\}$.

حل اگر $\alpha \in S_X$ جایگشت غیرهمانی باشد، آنگاه یک $x_۱ \in X$ را حرکت می‌دهد، یعنی $\alpha(x_۱) = x_۲ \neq x_۱$. چون $|X| > ۲$ عضو $x_۳ \in X$ متمایز از $x_۱$ و $x_۲$ را اختیار می‌کنیم و جایگشت $\beta \in S_X$ را چنین تعریف می‌کنیم

$$\beta(x_۲) = x_۳, \quad \beta(x_۳) = x_۲, \quad \beta(x) = x, \quad \forall x \in X, \ x \neq x_۲, x_۳,$$

یعنی $\beta = (x_۲\ x_۳)$. در این صورت

$$\alpha\beta(x_۱) = \alpha(x_۱) = x_۲, \quad \beta\alpha(x_۱) = \beta(x_۲) = x_۳.$$

چون $x_۲ \neq x_۳$، $\alpha\beta \neq \beta\alpha$. □

در بحث مرکزساز یک عضو می‌توان به‌جای یک عضو از یک زیرمجموعه‌ی ناتهی و دلخواه X از G استفاده کرد. در این صورت نرمال‌ساز X به دست می‌آید. نرمال‌ساز X در G را که با $N_G(X)$ نشان می‌دهیم عبارت است از

$$N_G(X) = \{g \in G \mid gX = Xg\}$$

که در آن

$$gX = \{gx \mid x \in X\}, \quad Xg = \{xg \mid x \in X\}.$$

اگر قرار دهیم

$$g^{-1}Xg = \{g^{-1}xg \mid x \in X\}$$

می‌توان نوشت

$$N_G(X) = \{g \in G \mid g^{-1}Xg = X\}.$$

$g^{-1}Xg$ را مزدوج X تحت g گوییم. به سادگی می‌توان دید که رابطه‌ی تزویج روی زیرمجموعه‌های ناتهی G یک رابطه‌ی هم‌ارزی است. هرگاه $H \leq G$ به سادگی می‌توان دید $H \leq N_G(H)$. اگر $K \leq N_G(H)$ گوییم K، H را نرمال می‌کند.

مثال ۴.۶.۳. اگر G گروه آبلی باشد و $H \leq G$، آنگاه $N_G(H) = G$. □

مثال ۵.۶.۳. در Q_8 قرار می‌دهیم $H = \langle i \rangle$ و داریم $N_{Q_8}(H) = Q_8$. □

مثال ۶.۶.۳. نرمال‌ساز A_n در S_n را می‌یابیم. اگر $\alpha \in S_n$، آنگاه برای هر $\beta \in A_n$ جایگشت $\alpha^{-1}\beta\alpha$ زوج است و در A_n قرار دارد ، یعنی $\alpha^{-1}A_n\alpha \subseteq A_n$. از طرف دیگر برای هر $\beta \in A_n$، چون $\alpha^{-1}\beta\alpha \in A_n$، داریم ، $\beta = \alpha(\alpha^{-1}(\beta\alpha))\alpha^{-1} \in \alpha A_n\alpha^{-1}$ یعنی $A_n \subseteq \alpha A_n\alpha^{-1}$. بنابراین برای هر $\alpha \in S_n$، داریم $\alpha A_n\alpha^{-1} = A_n$، یعنی $S_n \subseteq N_{S_n}(A_n)$. پس $N_{S_n}(A_n) = S_n$. □

یکی دیگر از زیرگروه‌های مهم یک گروه زیرگروه مشتق است. ابتدا مفهوم تعویض‌گر را بیان می‌کنیم. اگر G گروه باشد و $x, y \in G$، آنگاه

$$[x, y] = x^{-1}y^{-1}xy$$

را تعویض‌گر x و y گوییم. ملاحظه کنید

$$[x, y] = 1 \iff xy = yx.$$

پس x و y تعویض می‌شوند اگر و تنها اگر تعویض‌گر آن‌ها بدیهی باشد. زیرگروه تولید شده توسط همه‌ی تعویض‌گرهای $[x, y] = x^{-1}y^{-1}xy$ که در آن $x, y \in G$ را زیرگروه مشتق G گوییم و با G' نشان می‌دهیم:

$$G' = \langle [x, y] \mid x, y \in G \rangle .$$

مثال ۷.۶.۳. ثابت کنید گروه G آبلی است اگر و تنها اگر $G' = \{1\}$.

حل فرض کنید G آبلی باشد. به ازای هر $x, y \in G$ داریم $xy = yx$. پس $[x, y] = 1$ و

$$G' = \langle [x, y] \mid x, y \in G \rangle = \langle 1 \rangle = \{1\}.$$

بر عکس فرض کنید $G' = \{1\}$. به ازای هر $x, y \in G$ داریم $[x, y] \in G' = \{1\}$. پس $[x, y] = 1$، یعنی $xy = yx$. بنابراین G آبلی است. □

مثال ۸.۶.۳. در Q_8 داریم

$$[i, j] = i^{-1}j^{-1}ij = (-i)(-j)ij = kk = -1.$$

به همین نحو

$$[i, k] = [j, k] = [j, i] = [k, i] = [k, j] = -1$$

که از آن جا نتیجه می‌شود $Q_8' = \{\pm 1\}$. □

در حالت کلی اگر H و K زیرگروه‌هایی از G باشند، تعویض‌گر H و K عبارت است از

$$[H,K]=\langle [h,k]\mid h\in H, k\in K\rangle .$$

بنابراین

$$G'=[G,G].$$

می‌توان روند مشتق‌گیری را تعمیم داد و $(G')'=G''$، $(G'')'=G'''$، ... را تعریف کرد: قرار می‌دهیم $G^{(0)}=G$ و اگر $G^{(i)}$ تعریف شده باشد تعریف می‌کنیم

$$G^{(i+1)}=(G^{(i)})'.$$

پس $G^{(1)}=G'$، $G^{(2)}=G''$، $G^{(3)}=G'''$ و غیره. پس دنباله‌ای از زیرگروه‌های G به دست می‌آید که آن را سری مشتق G گوییم:

$$G=G^{(0)}\geq G'\geq G''\geq \cdots .$$

اگر به ازای nای داشته باشیم $G^{(n)}=\{1\}$، یعنی سری مشتق به $\{1\}$ ختم شود، گوییم گروه G حل‌پذیر است. کوچک‌ترین nای که $G^{(n)}=\{1\}$ را طول حل‌پذیری G گوییم. به وضوح هر گروه آبلی، حل‌پذیر با طول حل‌پذیری ۱ است. اگر G گروه حل‌پذیر با طول حل‌پذیری ۲ باشد آن‌را فراآبلی گوییم.

مثال ۹.۶.۳. Q_8 یک گروه فرا آبلی است. زیرا $Q_8'=\{\pm 1\}$ و $Q_8''=\{1\}$. □

تمرین‌ها

۱. D_{2n}' و D_∞' را بیابید و نشان دهید D_{2n} و D_∞ حل‌پذیر هستند.

۲. $Z(D_\infty)$ را بیابید.

۳. فرض کنید $n\geq 3$ عدد صحیح باشد. ثابت کنید اگر n فرد باشد، $Z(D_{2n})=\{1\}$ و اگر n زوج باشد، $Z(D_{2n})=\{1,\rho^{\frac{n}{2}}\}$.

۴. اگر F میدان باشد و $n\geq 1$، مرکز $\mathrm{GL}_n(F)$ را بیابید.

۵. فرض کنید G گروه باشد و $x,y\in G$. اگر $xy\in Z(G)$، نشان دهید $yx\in Z(G)$.

۶. نشان دهید S_3، S_4 ، و $\mathrm{GL}_2(\mathbb{Z}_2)$حل‌پذیرند.

۷. نشان دهید هر زیرگروه یک گروه حل‌پذیر ، حل‌پذیر است.

۸. فرض کنید G یک گروه باشد طوری که $|G'|=m$. ثابت کنید هر رده مزدوجی G حداکثر m عضو دارد.

۹. نشان دهید گروه ماتریس‌های بالا مثلثی وارون‌پذیر با درایه‌های در میدان دلخواه F، حل‌پذیر است.

۱۰. اگر y و x در گروه G مزدوج باشند، نشان دهید $C_G(x)$ و $C_G(y)$ نیز مزدوج‌اند.

۱۱. فرض کنید مرکز گروه G نامتناهی باشد و به ازای هر دو زیر مجموعه‌ی نامتناهی X و Y از G اعضای $x\in X$ و $y\in Y$ وجود داشته باشند که $xy=yx$، ثابت کنید G آبلی است.

۱۲. فرض کنید G گروهی نامتناهی باشد و $n\in\mathbb{N}$. اگر در هر زیر مجموعه‌ی نامتناهی X از G عضو $x\in X$ وجود داشته باشد که $x^n=1$. ثابت کنید به ازای هر $g\in G$ داریم $g^n=1$.

۱۳. فرض کنید G گروهی نامتناهی باشد و برای هر $x\in G$ و هر زیرگروه نامتناهی H از G، مرکزساز x در H نامتناهی باشد، یعنی $|C_H(x)|=\infty$. ثابت کنید به ازای هر $g\in G$ زیرگروه نامتناهی و آبلی A از G وجود دارد که $g\in A$.

۱۴. اگر G گروه ناآبلی باشد، ثابت کنید عضوی چون $x\in G-Z(G)$ وجود دارد که $O(x)>2$.

۷.۳ زیرگروه‌های مشخصه و نرمال

فرض کنید G یک گروه باشد و $H \leq G$. گوییم H در G کاملاً پایا است هرگاه تحت درون‌ریختی‌های G پایا باشد، یعنی برای هر $\alpha \in \operatorname{End} G$، $\alpha(H) \subseteq H$. گوییم H در G مشخصه است و می‌نویسیم $H \operatorname{char} G$ هرگاه تحت خودریختی‌های G پایا باشد، یعنی برای هر $\alpha \in \operatorname{Aut} G$، $\alpha(H) \subseteq H$. هم‌چنین H را در G نرمال گوییم و می‌نویسیم $H \trianglelefteq G$ هرگاه تحت خودریختی‌های داخلی G پایا باشد، یعنی برای هر $g \in G$، $\tau_g(H) \subseteq H$ یا $gHg^{-1} \subseteq H$. اگر $H \trianglelefteq G$ و $H \neq G$ می‌نویسیم $H \lhd G$. واضح است که اگر H کاملاً پایا باشد، آن‌گاه مشخصه نیز هست و اگر H مشخصه باشد، آن‌گاه نرمال نیز هست.

مثال ۱.۷.۳. هر گروه G دو زیرگروه کاملاً پایای بدیهی $\{1\}$ و G دارد. پس این زیر گروه‌ها مشخصه و نرمال نیز هستند. □

مثال ۲.۷.۳. اگر G گروه باشد ثابت کنید $Z(G)$ در G مشخصه است.

حل فرض کنید $\alpha \in \operatorname{Aut} G$ و $x \in Z(G)$. به ازای هر $a \in G$ ثابت می‌کنیم $\alpha(x)a = a\alpha(x)$. چون α پوشاست، عضو $b \in G$ وجود دارد که $\alpha(b) = a$. پس

$$\begin{aligned} \alpha(x)a &= \alpha(x)\alpha(b) \\ &= \alpha(xb) \\ &= \alpha(bx) \\ &= \alpha(b)\alpha(x) \\ &= a\alpha(x), \end{aligned}$$

یعنی $Z(G)$ در G مشخصه است. □

در دو مثال بعدی شرایط معادل با نرمال بودن یک زیرگروه را بررسی می‌کنیم:

مثال ۳.۷.۳. ثابت کنید $H \trianglelefteq G$ اگر و تنها اگر به ازای هر $g \in G$، $gHg^{-1} = H$.

حل فرض کنید $H \trianglelefteq G$. اگر $g \in G$ عضو دلخواهی باشد داریم $g^{-1} \in G$. پس $(g^{-1})H(g^{-1})^{-1} \subseteq H$، یعنی $g^{-1}Hg \subseteq H$ یا $H \subseteq gHg^{-1}$. از طرفی طبق تعریف، $gHg^{-1} \subseteq H$. بنابراین $gHg^{-1} = H$.
عکس مطلب واضح است. □

مثال ۴.۷.۳. ثابت کنید $H \trianglelefteq G$ اگر و تنها اگر به ازای هر $g \in G$ و به ازای هر $h \in H$ داشته باشیم $ghg^{-1} \in H$.

حل فرض کنید $H \trianglelefteq G$. طبق تعریف برای هر $g \in G$، $gHg^{-1} \subseteq H$. پس برای هر $g \in G$ و هر $h \in H$ داریم $ghg^{-1} \in gHg^{-1} = H$. برعکس اگر برای هر $g \in G$ و هر $h \in H$ داشته باشیم $ghg^{-1} \in H$، آن‌گاه $gHg^{-1} \subseteq H$. بنابراین $H \trianglelefteq G$. □

مثال ۵.۷.۳. هر زیرگروه یک گروه آبلی، نرمال است. در واقع اگر H زیرگروهی از گروه G باشد، آن‌گاه برای هر $a \in G$ و هر $h \in H$ داریم

$$aha^{-1} = aa^{-1}h = h \in H.$$

در نتیجه $H \trianglelefteq G$. □

مثال ۶.۷.۳. $A_n \trianglelefteq S_n$، زیرا به ازای هر $\alpha \in S_n$ و $\beta \in A_n$ داریم $\alpha\beta\alpha^{-1} \in A_n$. □

مثال ۷.۷.۳. نشان دهید اگر $f : G \longrightarrow H$ همریختی باشد، آن‌گاه $\ker f \trianglelefteq G$.

حل می‌دانیم $\ker f \leq G$. اکنون برای هر $g \in G$ و هر $x \in \ker f$ داریم

$$f\left(gxg^{-1}\right) = f(g)f(x)f\left(g^{-1}\right) = f(g)1_H f(g)^{-1} = 1_G.$$

پس $gxg^{-1} \in \ker f$، یعنی $\ker f \trianglelefteq G$. □

اگر $f : G \longrightarrow H$ همریختی باشد و $a \in G$، آنگاه بنا به تمرین ۱ از صفحه‌ی ۷۳، $f\left(\langle a\rangle\right) = \langle f(a)\rangle$ به ویژه

$$\begin{aligned} g\langle a\rangle g^{-1} &= \tau_g(\langle a\rangle) \\ &= \langle \tau_g(a)\rangle \\ &= \left\langle gag^{-1}\right\rangle. \end{aligned}$$

از این نکته در مثال بعد استفاده می‌کنیم.

مثال ۸.۷.۳. در گروه Q_8 و زیرگروه $H = \langle i\rangle$ از آن داریم

$$jHj^{-1} = \left\langle jij^{-1}\right\rangle = \langle -jij\rangle = \langle -i\rangle = \langle i\rangle = H$$

و

$$kHk^{-1} = \left\langle kjk^{-1}\right\rangle = \langle -kjk\rangle = \langle -i\rangle = \langle i\rangle = H.$$

پس $jHj^{-1} = H$ و $kHk^{-1} = H$. از طرفی برای هر $h \in H$ نیز به وضوح $hHh^{-1} = H$. از این‌رو برای هر $a \in Q_8$ داریم $a^{-1} = H$. بنابراین $H \trianglelefteq Q_8$. می‌توان ثابت کرد که (ثابت کنید) هر زیرگروه Q_8 در Q_8 نرمال است. □

اگر $K \leq H \leq G$، آنگاه $K \leq G$، یعنی زیرگروه بودن خاصیت ترایا دارد. نرمال بودن خاصیت ترایا ندارد (تمرین ۲ را ببینید). اما داریم

مثال ۹.۷.۳. اگر $K \operatorname{char} H \trianglelefteq G$، آنگاه $K \trianglelefteq G$.

حل فرض کنید $g \in G$. چون $H \trianglelefteq G$ داریم $\tau_g(H) = H$. بنابراین $\psi_g = \tau_g|_H$ یک خودریختی از H است. حال چون $K \operatorname{char} H$، $\psi_g(K) \subseteq K$، یعنی $g^{-1}Kg \subseteq K$. بنابراین $K \trianglelefteq G$. □

مثال ۱۰.۷.۳. اگر G گروه باشد، آنگاه $\operatorname{Inn} G \trianglelefteq \operatorname{Aut} G$.

حل قبلاً دیده‌ایم (در صفحه‌ی ۶۷) که $\operatorname{Inn} G \leq \operatorname{Aut} G$. باید ثابت کنیم برای هر $g \in G$ و هر $\alpha \in \operatorname{Aut} G$، $\alpha\tau_g\alpha^{-1} \in \operatorname{Inn} G$. به ازای هر $x \in G$ داریم

$$\begin{aligned} \left(\alpha\tau_g\alpha^{-1}\right)(x) &= \alpha\left(\tau_g\left(\alpha^{-1}(x)\right)\right) \\ &= \alpha\left(g\alpha^{-1}(x)g^{-1}\right) \\ &= \alpha(g)\alpha\alpha^{-1}(x)\alpha\left(g^{-1}\right) \\ &= \alpha(g)x\alpha(g)^{-1} \\ &= \tau_{\alpha(g)}(x). \end{aligned}$$

بنابراین $\alpha\tau_g\alpha^{-1} = \tau_{\alpha(g)} \in \operatorname{Inn} G$. در نتیجه $\operatorname{Inn} G \trianglelefteq \operatorname{Aut} G$. □

تعریف ۱۱.۷.۳. نابدیهی نداشته باشد.

اگر G گروه دوری متناهی با مرتبه‌ی عدد اول باشد، آنگاه G گروه ساده است. در واقع گروه آبلی G ساده است اگر و تنها اگر به ازای یک عدد اول p، $G \cong \mathbb{Z}_p$. می‌خواهیم نشان دهیم A_n، $n \geq 5$ گروه ناآبلی ساده است. برای اثبات این مطلب به قدری مقدمه نیاز داریم. از تمرین ۷ از صفحه‌ی ۳۴، یادآوری می‌کنیم که اگر $\sigma = (a_1\ a_2\ \cdots\ a_m)$ یک دور به طول m و τ یک جایگشت دلخواه در S_n باشند، آنگاه $\tau\sigma\tau^{-1} = (\tau(a_1)\ \tau(a_2)\ \cdots\ \tau(a_m))$.

قضیه ۱۲.۷.۳. اگر $n \geq ۵$ و $H \trianglelefteq A_n$ شامل یک سه دور باشد، آنگاه $H = A_n$.

اثبات. فرض کنید $(a\ b\ c) \in H$. کافی است ثابت کنیم هر سه دور در H است. سه دور دلخواه $(i\ j\ k)$ را در نظر می‌گیریم و جایگشت $\sigma \in S_n$ را با $\sigma(a) = i$، $\sigma(b) = j$، $\sigma(c) = k$، تعریف می‌کنیم (تمرین ۶ صفحه‌ی ۳۴ را ببینید). پس طبق تمرین ۷ از صفحه‌ی ۳۴، داریم

$$\sigma(a\ b\ c)\sigma^{-۱} = (\sigma(a)\ \sigma(b)\ \sigma(c)) = (i\ j\ k).$$

اگر $\sigma \in A_n$ چون $H \trianglelefteq A_n$، داریم $(i\ j\ k) \in H$ و اثبات کامل است. پس فرض کنید $\sigma \notin A_n$. در این صورت σ جایگشت فرد است. چون $n \geq ۵$، دو حرف متمایز u و w را طوری انتخاب می‌کنیم که $u, w \notin \{a, b, c\}$. اکنون چون $\sigma(u\ w) \in A_n$ و $H \trianglelefteq A_n$، داریم $\sigma(u\ w)(a\ b\ c)(\sigma(u\ w))^{-۱} \in H$. پس

$$\begin{aligned} \sigma(u\ w)(a\ b\ c)(\sigma(u\ w))^{-۱} &= \sigma(u\ w)(a\ b\ c)(u\ w)\sigma^{-۱} \\ &= \sigma(a\ b\ c)\sigma^{-۱} \\ &= (\sigma(a)\ \sigma(b)\ \sigma(c)) \\ &= (i\ j\ k) \in H. \end{aligned}$$

بنابراین $H = A_n$. □

قضیه ۱۳.۷.۳. اگر $n \geq ۵$، آنگاه A_n ساده است.

اثبات. فرض کنید $H \trianglelefteq A_n \neq \{(۱)\}$. عضو $(۱) \neq \sigma \in H$ را طوری اختیار می‌کنیم که در بین عناصر غیر همانی H کم‌ترین حرف را حرکت دهد، مثلاً m حرف. چون σ ترانهش نیست، $m \geq ۳$. اگر $m = ۳$ آنگاه σ یک $۳-$ دور است. بنابراین، طبق قضیه‌ی ۱۲.۷.۳، $H = A_n$. ثابت می‌کنیم فرض $m \geq ۴$ به تناقض منجر می‌شود. فرض کنید $\sigma = \sigma_۱\sigma_۲\cdots\sigma_k$ تجزیه‌ی σ به دورهای مجزا باشد، دو حالت وجود دارد.

حالت اول. اگر برای هر $i = ۱, \ldots, k$، σ_i ترانهش باشد. در این حالت $k \geq ۲$. فرض کنید $\sigma_۱ = (a\ b)$ و $\sigma_۲ = (c\ d)$. چون $n \geq ۵$، حرف u وجود دارد که $u \notin \{a, b, c, d\}$. قرار می‌دهیم $\alpha = (c\ d\ u)$. چون $\alpha \in A_n$ و $H \trianglelefteq A_n$، داریم $\sigma' = \sigma^{-۱}\alpha\sigma\alpha^{-۱} \in H$. جایگشت σ' حرف a را به a و حرف b را به b می‌برد، زیرا

$$\sigma'(a) = \sigma^{-۱}\alpha\sigma\alpha^{-۱}(a) = \sigma^{-۱}\alpha\sigma(a) = \sigma^{-۱}\alpha(b) = \sigma^{-۱}(b) = a$$

و

$$\sigma'(b) = \sigma^{-۱}\alpha\sigma\alpha^{-۱}(b) = \sigma^{-۱}\alpha\sigma(b) = \sigma^{-۱}\alpha(a) = \sigma^{-۱}(a) = b.$$

به علاوه $\sigma' \neq (۱)$، زیرا

$$\sigma'(d) = \sigma^{-۱}\alpha\sigma\alpha^{-۱}(d) = \sigma^{-۱}\alpha\sigma(c) = \sigma^{-۱}\alpha(d) = \sigma^{-۱}(u) \neq d = \sigma^{-۱}(c).$$

حال ثابت می‌کنیم که σ' حرف کمترین نسبت به σ حرکت می‌دهد. اگر برای هر حرف w که $w \notin \{a, b, c, d, u\}$ و $\sigma(w) = w$، آنگاه $\sigma'(w) = w$، زیرا هم α و هم σ، w را ثابت نگه می‌دارد. از طرف دیگر σ' دو حرف a, b را نیز ثابت نگه می‌دارد. پس تعداد حروفی که σ' حرکت می‌دهد کمتر از تعداد حروفی است که σ حرکت می‌دهد، که متناقض با انتخاب σ است و این حالت به تناقض منجر می‌شود.

حالت دوم. اگر یک دور به طول بیشتر یا مساوی ۳ در تجزیه σ ظاهر شود. چون جایگشت‌های مجزا تعویض می‌شوند بدون کم شدن کلیت مساله فرض می‌کنیم طول $\sigma_۱$ بیشتر یا مساوی ۳ باشد. $\sigma_۱ = (a\ b\ c\ \cdots)$. اگر $m = ۴$، آنگاه چون طبق حالت اول σ حاصل‌ضرب دو ترانهش نیست، یک ۴- دور و جایگشت فرد است که این تناقض است. بنابراین $m \geq ۵$ و σ حداقل ۵ حرف را حرکت می‌دهد. فرض کنیم w و u طوری باشند که σ آنها حرکت دهد و $u, w \notin \{a, b, c\}$. قرار می‌دهیم $\alpha = (c\ u\ w)$. چون $H \trianglelefteq A_n$، $\sigma' = \sigma^{-۱}\alpha\sigma\alpha^{-۱} \in H$. داریم $\sigma'(b) = \sigma^{-۱}(u) \neq b$، پس $\sigma' \neq (۱)$. به علاوه σ'، a را ثابت نگه می‌دارد ، زیرا

$$\sigma'(a) = \sigma^{-۱}\alpha\sigma\alpha^{-۱}(a) = \sigma^{-۱}\alpha\sigma(a) = \sigma^{-۱}\alpha(b) = \sigma^{-۱}(b) = a.$$

اکنون ثابت می‌کنیم که σ' حرف کمترین نسبت به σ حرکت می‌دهد. اگر برای هر حرف v که $v \notin \{a, b, c, u, w\}$ و $\sigma(v) = v$، آنگاه $\sigma'(v) = v$، زیرا هم α و هم σ، v را ثابت نگه می‌دارند. پس σ' حرف کمترین نسبت به σ حرکت می‌دهد که این تناقض است. بنابراین $m = ۳$ و حکم ثابت است. □

گروه ساده را گروهی تعریف کردیم که زیرگروه نرمال نابدیهی ندارد. پس اگر گروهی که زیرگروه نابدیهی و پایا تحت خودریختی‌های داخلی نداشته باشد، ساده است. بنابراین تعریف زیر به طور طبیعی مطرح می‌شود.

تعریف ۱۴.۷.۳. گروه نابدیهی G را مشخصاً ساده گوییم هرگاه زیرگروه مشخصه‌ی نابدیهی نداشته باشد.

گروه‌های ساده یقیناً مشخصاً ساده هستند، اما یک گروه مشخصاً ساده لزوماً ساده نیست. در واقع با استفاده از قضیه‌ی ۱۸.۷.۳، که در ادامه ثابت می‌کنیم، می‌توان گروه‌های غیرساده‌ی فراوانی ساخت که مشخصاً ساده باشند. یک شرط کافی و مهم را برای این که یک زیرگروه مشخصاً ساده باشد بیان می‌کنیم. شرط کافی برای این که زیرگروهی از یک گروه مشخصاً ساده باشد این است که ماکسیمال نرمال باشد. ابتدا زیرگروه ماکسیمال نرمال را دقیقاً تعریف می‌کنیم:

تعریف ۱۵.۷.۳. فرض کنید $H \trianglelefteq G > \{۱\}$. گوییم H زیرگروه ماکسیمال نرمال از G است هرگاه زیرگروه نرمال K از G وجود نداشته باشد که $H < K < \{۱\}$.

قضیه ۱۶.۷.۳. اگر H زیرگروه ماکسیمال نرمال G باشد، آنگاه H مشخصاً ساده است.

اثبات. فرض کنید L زیرگروه مشخصه‌ای از H باشد. چون $L \operatorname{char} H \trianglelefteq G$، طبق مثال ۹.۷.۳، $L \trianglelefteq G$. به علاوه چون $L \leq H$ و H زیرگروه ماکسیمال نرمال G است، یا $L = \{۱\}$ و یا $L = H$. بنابراین H مشخصاً ساده است. □

توصیف گروه‌های مشخصاً ساده در حالت کلی کمی مشکل است؛ این توصیف در مرجع [۱۳] صفحه‌ی ۲۷۱ داده شده:یک گروه متناهی نابدیهی مشخصاً ساده است اگر و تنها اگر حاصلضرب مستقیم تعداد متناهی گروه ساده‌ی یکریخت با یکدیگر باشد. اما گروه آبلی متناهی مشخصاً ساده را به راحتی می‌توان توصیف کرد. ابتدا به تعریف زیر نیاز داریم

تعریف ۱۷.۷.۳. گروه آبلی G را آبلی مقدماتی گوییم هرگاه عدد اول p وجود داشته باشد که به ازای هر $a \in G$، $a^p = ۱$.

بنابراین گروه آبلی G یک گروه آبلی مقدماتی است هرگاه نمای G عدد اول p باشد، یعنی $\exp G = p$. ابتدا ساختار گروه‌های آبلی مقدماتی را به دست می‌آوریم. در دو قضیه‌ی بعد برای سادگی کار گروه‌های آبلی را به صورت گروه جمعی در نظر می‌گیریم.

قضیه ۱۸.۷.۳. فرض کنید G گروه آبلی باشد. در این صورت G آبلی مقدماتی است اگر و تنها اگر عدد اول p و فضای برداری V روی $\mathbb{Z}_p$ وجود داشته باشد که $G \cong (V, +)$.

اثبات. فرض کنید G آبلی مقدماتی باشد. پس عدد اول p وجود دارد که به ازای هر $a \in G$، $pa = ۰$. فضای برداری V روی $\mathbb{Z}_p$ را به صورت زیر تعریف می‌کنیم: (الف) عناصر V همان عناصر G هستند. (ب) حاصل جمع دو عضو V را همان حاصل جمع‌شان در در G تعریف می‌کنیم. (ج) به ازای هر $\bar{m} \in \mathbb{Z}_p$ و $a \in G$، حاصلضرب اسکالر $\bar{m}a$ را برابر عضو $ma \in G$ تعریف می‌کنیم. این حاصلضرب اسکالری خوش تعریف است. زیرا اگر $\bar{m} = \bar{n}$، آنگاه $p|(m-n)$. پس $(m-n)a = ۰$ و $ma = na$، یعنی $\bar{m}a = \bar{n}a$. اکنون به سادگی می‌توان تحقیق کرد که V یک فضای برداری روی $\mathbb{Z}_p$ است؛ و به وضوح $G \cong (V, +)$.
بر عکس اگر V یک فضای برداری روی $\mathbb{Z}_p$ باشد و $G \cong (V, +)$، آنگاه $(V, +)$ یک گروه آبلی است. به علاوه، چون به ازای هر $v \in V$، $pv = ۰$، $(V, +)$ آبلی مقدماتی است. چون $G \cong (V, +)$، G نیز آبلی مقدماتی است. □

حال می‌توانیم ساختار گروه‌های آبلی متناهی مشخصاً ساده را توصیف کنیم:

قضیه ۱۹.۷.۳. فرض کنید G یک گروه آبلی متناهی نابدیهی باشد. در این صورت G مشخصاً ساده است اگر و تنها اگر آبلی مقدماتی باشد.

اثبات. فرض کنید G گروه آبلی مقدماتی باشد. بنا به قضیه‌ی ۱۸.۷.۳، عدد اول p و فضای برداری V روی $\mathbb{Z}_p$ وجود دارد که $G \cong (V, +)$. چون G متناهی است، V متناهی است. فرض کنید W یک زیرگروه نابدیهی مشخصه‌ی $(V, +)$ باشد و $۰ \neq w \in W$. بنابراین پایه‌ای از V شامل w وجود دارد. پس اگر $v \in V$، آنگاه تبدیل خطی $\theta : V \longrightarrow V$ وجود دارد که $\theta(w) = v$. چون $\theta \in \operatorname{Aut}(V, +)$ و W در $(V, +)$ مشخصه است، داریم $v = \theta(w) \in W$. پس $W = V$ و $(V, +)$ مشخصاً ساده است.

بر عکس فرض کنید G مشخصاً ساده باشد. فرض کنید p عدد اولی باشد که G یک عضو از مرتبه‌ی p دارد (چرا چنین عدد اولی وجود دارد؟) و قرار دهید

$$A = \{a \in G \mid pa = ۰\}.$$

چون G آبلی است، $A \leq G$. اگر $\psi \in \operatorname{Aut} G$ و $a \in A$، آنگاه

$$p\psi(a) = \psi(pa) = \psi(۰) = ۰,$$

یعنی $\psi(a) \in A$. بنابراین A در G مشخصه است. چون G مشخصاً ساده است و $A \neq \{۰\}$، داریم $G = A$. پس G آبلی مقدماتی است. □

این بخش را با تاریخچه‌ای در باره‌ی گروه‌های ساده به پایان می‌بریم. مفهوم گروه ساده را گالوا در سال ۱۸۳۰ معرفی کرد. ساده بودن A_n برای گالوا امری مسلم بود زیرا در اثبات او از حل‌ناپذیری چندجمله‌ای‌های با درجه‌ی بیشتر یا مساوی ۵، از این مطلب استفاده کرد. اما اولین اثبات از ساده بودن A_n را ژردان در سال ۱۸۷۰ ارائه کرد. کلاین اولین شخصی بود که ثابت کرد گروهی ساده از مرتبه‌ی ۱۶۸ وجود دارد.
مساله‌ی تعیین این که در یک فاصله‌ی داده شده چه اعدادی می‌توانند مرتبه‌ی گروه‌های ساده باشند به سال ۱۸۹۲ برمی‌گردد. در این سال هولدر این کار را تا عدد ۲۰۰ انجام داد. استدلال‌های او برای اعداد صحیح ۱۴۴ و ۱۸۰ به تنهایی ۱۰۰ صفحه بود. اما اهمیت گروه‌های ساده در نظریه‌ی گروه‌ها از حیث چیست؟ این گروه‌ها همانند اعداد اول در نظریه‌ی اعداد یا عناصر در شیمی هستند، یعنی آن‌ها زیربنای اصلی همه‌ی گروه‌ها هستند. این زیربناهای اساسی را می‌توان به صورت زیر تعیین کرد. فرض کنید G یک گروه متناهی باشد و زیرگروه نرمال $G_۱$ از $G = G_۰$ را با مرتبه‌ی ماکسیمم انتخاب کنید. در این صورت $G_۰/G_۱$ ساده است. (مفهوم گروه خارج قسمتی $G_۰/G_۱$ را بعداً، در بخش ۱۳، بررسی می‌کنیم و نشان می‌دهیم که $G_۰/G_۱$ ساده است اگر و تنها اگر $G_۱$ زیرگروه با مرتبه‌ی ماکسیمم باشد) سپس زیرگروه نرمال $G_۲$ از $G_۱$ را با مرتبه‌ی ماکسیمم انتخاب کنید. در این صورت $G_۱/G_۲$ نیز ساده است، این روند را تا رسیدن به $G_n = \{۱\}$ ادامه می‌دهیم. گروه‌های ساده‌ی $G_n/G_۲$، $G_۱/G_۲$، ...، $G_{n-۱}/G_n$ را عوامل ترکیبی G می‌نامیم و دنباله‌ی گروه‌های

$$G = G_۰ > G_۱ > \cdots > G_n = \{۱\}$$

را یک سری ترکیبی برای G می‌نامیم (فصل ۷ را ببینید). ژردان و هولدر ثابت کردند که این عوامل مستقل از انتخاب زیرگروه‌های نرمال در فرایند بالا است. به مفهومی معین، یک گروه را می‌توان از عوامل ترکیبی‌اش دوباره ساخت و خواص زیادی از گروه را با استفاده از خواص عوامل ترکیبی‌اش به دست آورد. این مطلب و این حقیقت را که تعداد زیادی از سوالات درباره‌ی گروه‌های متناهی را می‌توان (به استقرا) به سوالاتی در مورد گروه‌های ساده تبدیل کرد اهمیت تعیین همه‌ی گروه‌های متناهی ساده را واضح می‌کند.
همانطور که قبلاً ذکر شد $\mathbb{Z}_p$، (p عدد اول) خانواده‌ی نامتناهی گروه‌های آبلی ساده هستند. در واقع هر گروه آبلی ساده با یکی از این گروه‌ها یکریخت است. اما متاسفانه راهی ساده برای توصیف گروه‌های ناآبلی ساده وجود ندارد. بهترین کاری که در این جا می‌توانیم انجام دهیم ارائه‌ی چند مثال و ذکر جملاتی در مورد چگونگی کشف آن‌ها است. A_n برای $n \geq ۵$، خانواده‌ای نامتناهی از گروه‌های ناآبلی ساده است. ساده بودن این گروه‌ها را اولین بار گالوا ملاحظه کرد. کشف بعدی را ژردان در سال ۱۸۷۰ انجام داد. او ثابت کرد چهار خانواده‌ی نامتناهی از گروه‌های ماتریسی ساده روی میدان $\mathbb{Z}_p$ (p عدد اول) وجود دارد. یکی از این خانواده‌ها گروه خارج قسمتی

$$\mathrm{PSL}(n, \mathbb{Z}_p) = \mathrm{SL}(n, \mathbb{Z}_p)/Z(\mathrm{SL}(n, \mathbb{Z}_p))$$

است (به‌جز وقتی که $n = ۲$ و $p = ۲$ یا $p = ۳$ است). بین سال‌های ۱۸۹۲ و ۱۹۰۵ لئونارد دیکسون ریاضی‌دان آمریکایی نتایج ژردان را برای میدانهای متناهی دلخواه تعمیم داد و خانواده‌های جدید دیگری از گروه‌های ساده را کشف کرد. تقریباً در خلال همین زمان‌ها میلر و کول نشان دادند که خانواده‌ای متشکل از ۵ گروه ساده که اولین بار ماتیو در سال ۱۸۶۱ توصیف کرده بود، گروه‌های ساده هستند. چون این پنج گروه به خانواده‌ای نامتناهی از گروه‌های ساده مثل A_n یا گروه‌های ماتریسی روی میدان‌های متناهی منجر نمی‌شود، آن‌ها را پراکنده می‌نامیم.
در دهه‌ی ۱۹۵۰ نتایج مهم دیگری به دست آمد. در این دهه خانواده‌های جدید بسیاری از گروه‌های ساده به دست آمدند و مراحل اولیه‌ی راه طویل و پرپیچ و حمی که به رده‌بندی کامل همه‌ی گروه‌های ساده‌ی متناهی منجر شد پایه‌گذاری شد. اولین مرحله وقتی بود که ریچارد براوئر ملاحظه کرد که مرکزساز یک عضو مرتبه‌ی ۲ ابزاری بسیار مهمی برای مطالعه‌ی گروه‌های ساده است. چند سال بعد جان تامپسون، در رساله‌ی

دکتری خود ایده‌ای قاطع برای مطالعه‌ی نرمال‌سازهای زیرگروه‌های با مرتبه توانی از عدد اول معرفی کرد. در اوایل ۱۹۶۰، فیت و تامپسون قضیه‌ی بسیار مهم خود را ثابت کردند که می‌گوید مرتبه‌ی هر گروه ناآبلی ساده متناهی زوج است. شخصی که اولین بار این خاصیت را در سال ۱۹۰۰ حدس زد ویلیام برن ساید ریاضی‌ان مشهور انگلیسی بود. اثبات قضیه‌ی فیت- تامپسون یک جلد کامل از حدود ۲۵۵ صفحه‌ی ژورنالی را که در آن چاپ شد اوایل کرد. این نتیجه محرکی برای رده‌بندی گروه‌های ساده متناهی فراهم کرد. یعنی برنامه‌ای که همه‌ی گروه‌های ساده را کشف کند و ثابت کند چیز بیشتر برای یافتن وجود ندارد. در دهه‌ی ۱۹۶۰، روش‌هایی را که در اثبات قضیه‌ی فیت- تامپسون معرفی شده بود، تعدادی از ریاضی‌دانان توسعه داند. به علاوه در خلال سال‌های ۱۹۶۶ و ۱۹۷۵، نوزده گروه پراکنده‌ی جدید کشف شد. علی‌رغم موفقیت‌های جالبی که در تحقیقات نظریه‌ی گروه‌های ساده رخ داد دهه‌ی ۱۹۶۰ در حالی به پایان رسید که بسیاری از ریاضی‌دانان رده‌بندی گروه‌های ساده را ناممکن می‌دانستند. بدبینان از گروه‌های ساده پراکنده که ممکن بود همه‌ی تلاش‌ها را با شکست مواجه کند بیم داشتند. دیگرانی که خوشبین بودند، پیش‌بینی می‌کردند که این مهم در دهه‌ی ۱۹۹۰ انجام شود. دهه‌ی ۱۹۷۰ در حالی آغاز شد که تامپسون به خاطر سهم عمده‌اش در نظریه‌ی گروه‌های ساده ، جایزه‌ی فیلدز را دریافت کرد. این جایزه بزرگ‌ترین جایزه‌ای است که یک ریاضی‌دان می‌تواند به آن برسد.

در طی چند سال سه پیش‌آمد بسیار بزرگ رخ داد که درنهایت منجر به رده‌بندی گروه‌های ساده شد. ابتدا تامپسون مقاله‌ای بسیار مهم در نظریه‌ی گروه‌های ساده، مقاله‌ی N- گروه‌ها، را چاپ کرد. در آن مقاله تامپسون تعداد زیادی روش اساسی را معرفی کرد و مدلی برای رده‌بندی خانواده‌ای وسیعی از گروه‌های ساده به دست آورد. سپس دانیل گورنشتاین طرحی کامل از رده‌بندی را در سلسله دروسی در دانشگاه شکاگو در سال ۱۹۷۲ ارائه کرد. در آن جا برنامه‌ای با قدری اثبات طراحی شد. حال فوجی از محققین، نقشه‌ی جنگی و یک فرمانده داشتند. اما این فوج هنوز به سلاح‌های بهتری نیاز داشتند. پس از آن سومین توسعه مهم پدید آمد: تضمین مایکل اشباخه. در یک سری مقاله‌ی خیره کننده، اشباخه بینش خود و روش تامپسون را که در دهه‌ی ۱۹۶۰ تعمیم داده شده بود، و دید هندسی را که برند فیشر از متقدمین آن بود ترکیب کرد و به نتیجه‌ی برجسته‌ای رسید. در واقع اشباخه و دیگرآن در سال ۱۹۷۶ چنین پیشرفت‌هایی را انجام دادند تا بر هر کسی معلوم شود که به اندازه‌ی کافی روش برای تکمیل رده‌بندی گروه‌های ساده در اختیار ما است و تنها جزئیات اثبات باقی‌مانده است.

دهه‌ی ۱۹۸۰ در حالی آغاز شد که جایزه‌ی کول، جایزه‌ی انجمن ریاضی آمریکا، به اشباخه تعلق گرفت. در نهایت ۲۰ سال جنگ رده‌بندی گروه‌های ساده ، وقتی که گورنشتاین در اجتماع ۱۹۸۱ در یک اجتماع انجمن ریاضی آمریکا اعلام کرد که همه‌ی گروه‌های ساده رده‌بندی شده‌اند و اکنون فهرست کامل همه‌ی گروه‌های متناهی ساده در اختیار ما است، پایان گرفت. اثبات این که این لیست کامل است، حدود ۱۰۰۰۰ صفحه ژورنال است.

آخرین گروه ساده‌ی پراکنده را رابرت گریس به دست آورد. این گروه به هیولا معروف است و مرتبه‌ی آن حدود 8×10^{53} است. هیولا، بزرگ‌ترین گروه پراکنده‌ی ساده ، گروه چرخش‌ها با بعد ۱۹۶۸۸۳ است و هر عضو آن را با یک ماتریس 1966883×1966883 می‌توان نشان داد.

تعداد گروه‌های ساده پراکنده برابر ۲۶ است. امیل ماتیو ۵ تا از این گروه‌ها را در سال ۱۸۶۰ پیدا کرد و ۲۱ تای باقی در طی سال‌های ۱۹۶۵ تا ۱۹۷۵ کشف شدند. جانکو، کانوی، و فیشر هرکدام ۳ گروه پراکنده را پیدا کردند. برخی محققین گروه‌های ساده عبارت‌اند از: امیل ماتیو، کول، میلر، لئونارد دیکسون، دیودونه، چولی، براوئر، دانیل گورنشتاین.

تمرین‌ها

۱. ثابت کنید هر زیرگروه یک گروه آبلی نرمال است. آیا عکس مطلب درست است؟

۲. نشان دهید نرمال بودن خاصیت ترایا ندارد.

۳. اگر $H \operatorname{char} K \operatorname{char} G$ نشان دهید $H \operatorname{char} G$.

۴. اگر H, K زیرگروه‌های گروه G باشند و $H \trianglelefteq G$، نشان دهید $HK \leq G$. (تمرین ۹ صفحه‌ی ۶۹، را ببینید.)

۵. اگر H, K زیرگروه‌های نرمال گروه G باشند و $H \cap K = \{1\}$. ثابت کنید به ازای هر $h \in H$ و $k \in K$، $hk = kh$.

۶. اگر $H \trianglelefteq G$ و $|H| = 2$ ثابت کنید $H \leq Z(G)$.

۷. اگر $N \trianglelefteq G$ و $G' \cap N = \{1\}$ ثابت کنید $N \leq Z(G)$.

۸. ثابت کنید هر زیرگروه یک گروه دوری مشخصه است.

۹. فرض کنید $n \geq ۳$ و گروه دووجهی از مرتبه‌ی $۲n$، یعنی $D_{۲n}$، را در نظر بگیرید. اگر $H = \langle \rho \rangle$ ثابت کنید مرتبه‌ی هر عضو $D_{۲n} - H$ برابر ۲ است. نتیجه بگیرید H تنها زیرگروه دوری $D_{۲n}$ از مرتبه‌ی n است؛ بنابراین مشخصه است.

۱۰. گروه دووجهی نامتناهی، یعنی D_∞، را در نظر بگیرید. اگر $K = \langle \tau \rangle$ ثابت کنید مرتبه‌ی هر عضو $D_\infty - K$ برابر ۲ است. آیا K در D_∞ مشخصه است؟

۱۱. نشان دهید گروه آبلی G ساده است اگر و تنها اگر عدد اول p وجود داشته باشد که $G \cong \mathbb{Z}_p$.

۱۲. نشان دهید گروه حل‌پذیر G ساده است اگر و تنها اگر عدد اول p وجود داشته باشد که $G \cong \mathbb{Z}_p$.

۱۳. اگر $H, K \leq G$ ثابت کنید $[H, K] \trianglelefteq \langle H, K \rangle$، که در آن $\langle H, K \rangle = \langle H \cup K \rangle$.

۱۴. فرض کنید H زیرگروهی از گروه G باشد. ثابت کنید $H \trianglelefteq G$ اگر و تنها اگر H اجتماعی از رده‌های مزدوجی عناصر G باشد.

۱۵. فرض کنید $G_۱ \leq G_۲ \leq \cdots$ زنجیری از زیرگروه‌های یک گروه G باشد. اگر به ازای هر i، G_i ساده باشد، نشان دهید $\bigcup_{i=۱}^{\infty} G_i$ یک گروه ساده است.

۱۶. یک گروه ساده‌ی نامتناهی بیابید.

۱۷. فرض کنید $H \leq G$. (یا درون نرمال یا هسته) H در G را که با H_G نشان می‌دهیم عبارت است از اشتراک همه‌ی مزدوج‌های H، یعنی $H_G = \bigcap_{g \in G} g^{-۱} H g$. ثابت کنید $H_G \trianglelefteq G$ و H_G بزرگ‌ترین زیرگروه یکتای نرمال G است که در H قرار دارد.

۱۸. فرض کنید $H \leq G$. بستار نرمال H در G را که با H^G نشان می‌دهیم عبارت است از $H^G = \bigcap \{N \mid H \subseteq N \trianglelefteq G\}$، یعنی اشتراک همه‌ی زیرگروه‌های نرمال G که شامل H هستند. ثابت کنید
(الف) $H^G \trianglelefteq G$ و H^G کوچک‌ترین زیرگروه یکتای نرمال G، شامل H است.
(ب) $H^G = \langle g^{-۱} h g \mid g \in G,\ h \in H \rangle$.
(ج) $H^G = H[H, G]$.

۱۹. فرض کنید H زیرگروه ماکسیمال نرمال G باشد. نشان دهید یا $Z(H) = \{۱\}$ یا H آبلی است.

۲۰. نشان دهید گروه جمعی $\mathbb{Z}$ زیرگروه ماکسیمال نرمال ندارد.

۲۱. فرض کنید H زیرگروه ماکسیمال نرمال G باشد. اگر H دوری باشد نشان دهید H متناهی و از مرتبه‌ی عدد اول است.

۲۲. اگر F یک میدان باشد، نشان دهید گروه آبلی جمعی $(F, +)$ مشخصاً ساده است.

۸.۳ هم‌مجموعه‌ها، قضیه‌ی لاگرانژ

در بخش ۴.۳ نشان دادیم در یک گروه دوری متناهی مرتبه‌ی هر زیرگروه مرتبه‌ی گروه را عاد می‌کند. این مطلب در حالت کلی نیز درست است. در واقع قضیه‌ی لاگرانژ می‌گوید که در یک گروه متناهی مرتبه‌ی هر زیرگروه مرتبه‌ی گروه را عاد می‌کند. لاگرانژ این قضیه را سال‌ها پیش از ظهور نظریه‌ی گروه‌ها موقعی که روی جایگشت‌های ریشه چندجمله‌ای‌ها کار می‌کرد در سال ۱۷۷۰ ثابت کرد. قضیه‌ی لاگرانژ قضیه‌ی مهم در نظریه‌ی گروه‌های متناهی است. در این بخش این قضیه را ثابت می‌کنیم. ابتدا به بحثی کشاف برای توجیه کارهای‌مان نیاز داریم.
اگر n عدد صحیح مثبت باشد می‌دانیم رابطه‌ی هم‌نهشتی به پیمانه‌ی n رابطه‌ای هم‌ارزی روی $\mathbb{Z}$ است

$$\forall a, b \in \mathbb{Z}, \quad a \equiv b \mod n \iff n | (b - a).$$

این رابطه را می‌توان چنین بیان کرد

$$a \equiv b \mod n \iff b - a \in n\mathbb{Z}.$$

در واقع دو عضو در گروه $\mathbb{Z}$ هم‌نهشت به پیمانه‌ی n هستند هرگاه تفاضل آن‌ها در زیرگروه $n\mathbb{Z}$ قرار گیرد. می‌توان این مطلب را تعمیم داد.
فرض کنید G یک گروه باشد و $H \leq G$؛ رابطه‌ی $\sim$ روی G را به صورت زیر تعریف می‌کنیم

$$a \sim b \iff a^{-۱} b \in H \quad (-a + b \in H \text{ در نماد جمعی})$$

$\sim$ یک رابطه‌ی هم‌ارزی است: چون $a^{-1}a = e \in H$ پس $\sim$ بازتابی است. اگر $a \sim b$، آنگاه $a^{-1}b \in H$. بنابراین $b^{-1}a = (a^{-1}b)^{-1} \in H$، یعنی $b \sim a$ و پس $\sim$ متقارن است. اگر $a \sim b$ و $b \sim c$، آنگاه $a^{-1}b \in H$ و $b^{-1}c \in H$. پس $a^{-1}c = (a^{-1}b)(b^{-1}c) \in H$ و $a \sim c$؛ یعنی $\sim$ ترایا است. بنابراین $\sim$ یک رابطه‌ی هم‌ارزی است و G به رده‌های هم‌ارزی افراز می‌شود. گاهی اوقات، با الهام از رابطه‌ی هم‌نهشتی به پیمانه‌ی n در $\mathbb{Z}$، رابطه‌ی $a \sim b$ را با $a \equiv_\ell b \mod H$ نشان می‌دهیم و آن را هم‌نهشتی به پیمانه‌ی H می‌نامیم. اگر رده‌ی هم‌ارزی شامل a را با $\bar{a}$ نشان دهیم، داریم

$$\begin{aligned}
\bar{a} &= \{b \in G \mid a \sim b\} \\
&= \{b \in G \mid a^{-1}b \in H\} \\
&= \{b \in G \mid \exists h \in H, \quad a^{-1}b = h\} \\
&= \{b \in G \mid \exists h \in H, \quad b = ah\} \\
&= \{ah \in G \mid h \in H\} \\
&= aH.
\end{aligned}$$

$aH = \{ah \mid h \in H\}$ را یک هم‌مجموعه‌ی چپ H در G گوییم. بنابراین هم مجموعه‌های چپ H در G، G را افراز می‌کنند. یعنی $G = \bigcup_{a \in G} aH$ و هر دو هم مجموعه‌ی متمایز اشتراک تهی دارند. اگر aH و bH دو هم‌مجموعه باشند، آنگاه طبق خواص رابطه‌ی هم‌ارزی

$$aH = bH \iff a \sim b \iff a^{-1}b \in H.$$

بنابراین

$$aH = H \iff a \in H.$$

اگر $X = \{aH \mid a \in G\}$ مجموعه‌ی همه‌ی هم مجموعه‌های چپ H در G باشد، $|X|$ را شاخص H در G گوییم و با $|G : H|$ نشان می‌دهند. مجموعه‌ی T را یک پیمایش چپ H در G می‌گویند هرگاه از هر هم‌مجموعه یک و تنها یک عضو را داشته باشد. بنابراین اگر T یک پیمایش چپ H در G باشد، $|T| = |X| = |G : H|$. به راحتی می‌توان ثابت کرد عدد اصلی هر دو هم مجموعه‌ی چپ H در G برابر است:

مثال ۱.۸.۳. اگر $H \leq G$ و $a \in G$، نشان دهید $|aH| = |H|$.

حل تابع $f : H \longrightarrow aH$ با ضابطه‌ی $f(h) = ah$ دوسویی است. □

قضیه‌ی بعدی با وجود ساده بودن از قضیه‌های مهم در نظریه‌ی گروه‌های متناهی است.

قضیه ۲.۸.۳. (قضیه‌ی لاگرانژ) اگر G یک گروه متناهی باشد و $H \leq G$، آنگاه $|G : H| = \frac{|G|}{|H|}$، به ویژه $|H| \mid |G|$.

اثبات. فرض کنید a_1H، ...، a_nH هم‌مجموعه‌های متمایز چپ H در G باشند. در این صورت $G = \bigcup_{i=1}^{n} a_iH$، و به ازای هر $i \neq j$، $a_iH \cap a_jH = \emptyset$. بنابراین

$$|G| = \left|\bigcup_{i=1}^{n} a_iH\right| = \sum_{i=1}^{n} |a_iH| = \sum_{i=1}^{n} |H| = n|H|.$$

پس $n = \frac{|G|}{|H|}$. چون $n = |G : H|$، اثبات کامل است. □

نتیجه ۳.۸.۳. اگر G گروه متناهی و $a \in G$، آنگاه $O(a) \mid |G|$. □

نتیجه ۴.۸.۳. اگر G گروه متناهی و $n = |G|$، آنگاه به ازای هر $a \in G$ داریم $a^n = e$.

اثبات. اگر $O(a) = m$، آنگاه $m|n$. بنابراین $t \in \mathbb{N}$ وجود دارد که $n = mt$. پس

$$a^n = a^{mt} = (a^m)^t = e^t = e \qquad .\square$$

نتیجه ۵.۸.۳. اگر G گروه متناهی و از مرتبه‌ی عدد اول p باشد، آنگاه G دوری است و زیرگروه نابدیهی ندارد.

اثبات. اگر $H \leq G$، آنگاه طبق قضیه‌ی لاگرانژ $|H| \mid p$. پس $|H| = ۱$ یا $|H| = p$. در نتیجه $H = \{۱\}$ یا $H = G$. پس G زیرگروه نابدیهی ندارد. حال اگر $a \in G$ ، $a \neq ۱$، آنگاه $\{۱\} \neq \langle a \rangle \leq G$. بنابراین $\langle a \rangle = G$ و G دوری است. □

نتیجه ۶.۸.۳. اگر $a \in \mathbb{Z}$، $n \in \mathbb{N}$، و $\gcd\{a, n\} = ۱$، آنگاه $a^{\varphi(n)} \equiv ۱ \mod n$، که در آن φ تابع فی اویلر است. به ویژه اگر p عدد اول باشد، $a^p \equiv a \mod n$.

اثبات. $\mathbb{Z}_n^\times$ را در نظر می‌گیریم. می‌دانیم $|\mathbb{Z}_n^\times| = \varphi(n)$. پس $\bar{a}^{\varphi(n)} = \bar{۱}$. در نتیجه $a^{\varphi(n)} \equiv ۱ \mod n$. □

عکس قضیه‌ی لاگرانژ درست نیست. یعنی اگر G گروه متناهی باشد و $m \mid |G|$، آنگاه ممکن است G زیرگروهی از مرتبه‌ی m نداشته باشد :

مثال ۷.۸.۳. $A_۴$ زیرگروه مرتبه‌ی ۶ ندارد.

حل توجه کنید $|A_۴| = ۱۲$ و $۶ | ۱۲$.
اثبات اول : اثبات را به برهان خلف انجام می‌دهیم فرض کنید $H \leq A_۴$ و $|H| = ۶$. اگر $\alpha \in A_۴$ عضو دلخواه مرتبه‌ی ۳ باشد. چون $|A_۴ : H| = ۲$ پس حداکثر دو هم‌مجموعه از هم مجموعه‌های H، αH و $\alpha^۲ H$ متمایزند. اما تساوی هر جفت از این ها ایجاب می‌کند که $\alpha \in H$. پس هر عضو مرتبه‌ی ۳ از $A_۴$ در H قرار دارد. اما $A_۴$ هشت عضو مرتبه‌ی ۳ دارد.
اثبات دوم : اگر $|H| = ۶$ چون مرتبه‌ی $|H|$ زوج است عضوی از مرتبه‌ی ۲ مثل β در H وجود دارد. چون $A_۴$، ۳ عضو مرتبه‌ی ۲ دارد پس حداقل دو عضو مرتبه‌ی ۳ از $A_۴$ در H قرار دارند. اگر α یکی از آن‌ها باشد، داریم $\alpha\beta\alpha^{-۱} \in H$ و $O(\alpha\beta\alpha^{-۱}) = ۲$. اگر $\alpha\beta\alpha^{-۱} = \beta$، آنگاه α و β با هم تعویض می‌شوند و $O(\alpha\beta) = ۶$. اما عضو مرتبه‌ی ۶ در $A_۴$ وجود ندارد ، پس $\alpha\beta\alpha^{-۱} = \gamma$ که در آن γ عضو دیگری از مرتبه‌ی ۲ است. بنابراین $\beta\gamma \in H$. پس هر سه عضو مرتبه‌ی ۲ از $A_۴$ در H قرار دارند، یعنی $V_۴ \leq H$ که متناقض قضیه‌ی لاگرانژ است. □

مشابه هم‌مجموعه‌های چپ می‌توان هم‌مجموعه‌ی راست را تعریف کرد. در واقع رابطه‌ی $\sim$ (که گاهی اوقات با $\equiv_r \mod H$ نشان داده می‌شود) به صورت زیر تعریف می‌شود

$$\forall a, b \in G, \quad a \sim b \ \ (a \equiv_r b \mod H) \iff ba^{-۱} \in H$$

رابطه‌ای هم‌ارزی است. رده‌ی هم‌ارزی شامل a، که آنرا هم‌مجموعه‌ی راست H در G می‌نامیم، به صورت است که در آن $Ha = \{ha \mid h \in H\}$. بنا به تعریف

$$Ha = Hb \iff ba^{-۱} \in H.$$

بنابراین $a \in H$ اگر و تنها اگر $Ha = H$. هم‌چنین به سادگی می‌توان دید $|Ha| = |H|$.

مثال ۸.۸.۳. اگر $X = \{aH \mid a \in G\}$ و $Y = \{Ha \mid a \in G\}$ به ترتیب مجموعه‌ی هم مجموعه‌های چپ و راست H در G باشند، آنگاه $|X| = |Y|$.

حل تابع $f : X \longrightarrow Y$ با ضابطه‌ی $f(aH) = Ha^{-۱}$، خوش‌تعریف، یک‌به‌یک و پوشاست. در واقع

$$aH = bH \iff a^{-۱}b \in H \iff b^{-۱}(a^{-۱})^{-۱} \in H \iff Ha^{-۱} = Hb^{-۱}.$$

این یعنی f تابع خوش تعریف و یک‌به‌یک است. پوشا بودن f نیز واضح است. بنابراین $|Y| = |X| = |G : H|$. □

توجه کنید که اگر H زیرگروهی از گروه G باشد، آنگاه H در G نرمال است اگر و تنها اگر به ازای هر $g \in G$، $g^{-۱}Hg = H$. بنابراین H در G نرمال است اگر و تنها اگر به ازای هر $g \in G$، $Hg = gH$.

مثال ۹.۸.۳. ثابت کنید هر زیرگروه با شاخص ۲ نرمال است.

حل فرض کنید $N \leq G$، $|G : N| = ۲$. باید به ازای هر $g \in G$، ثابت کنیم $Ng = gN$. اگر $g \in N$، آنگاه $Ng = N$ و $gN = N$، یعنی $Ng = gN$. حال اگر $g \notin N$، آنگاه gN، N دو هم‌مجموعه‌ی چپ متمایز در G هستند. پس $G = N \cup gN$ و $G - N = gN$. به همین نحو Ng، N دو هم مجموعه‌ی راست متمایز در G هستند؛ پس $G = N \cup Ng$ و $G - N = Ng$. بنابراین

$$gN = G - N = Ng.$$

از این‌رو $N \trianglelefteq G$. □

مثال ۱۰.۸.۳. چون $|S_n : A_n| = ۲$، داریم $A_n \trianglelefteq S_n$. □

مثال ۱۱.۸.۳. در $D_{۲n} = \langle \rho, \varepsilon \rangle$، چون $|D_{۲n} : \langle \rho \rangle| = ۲$، داریم $\langle \rho \rangle \trianglelefteq D_{۲n}$. □

رابطه‌ی مزدوجی رابطه‌ی هم‌ارزی روی یک گروه G است (تمرین ۱۴ از صفحه‌ی ۵۸ را ببینید). برای $x \in G$، رده‌ی هم‌ارزی شامل x رده‌ی مزدوجی گوییم و عبارت است از

$$\mathrm{orb}(x) = \{g^{-۱}xg \mid g \in G\}.$$

مثال ۱۲.۸.۳. فرض کنید x عضوی از گروه G باشد. ثابت کنید تعداد مزدوج‌های x در G برابر شاخص مرکزساز x در G است، یعنی $|G : C_G(x)| = |\mathrm{orb}(x)|$.

حل تابع f از مجموعه‌ی هم مجموعه‌های راست $C_G(x)$ در G به مجموعه‌ی مزدوج‌های x در G را با $f(C_G(x)g) = g^{-۱}xg$ تعریف می‌کنیم. f خوش تعریف و یک‌به‌یک است، زیرا

$$\begin{aligned} C_G(x)g_۱ = C_G(x)g_۲ &\iff g_۱g_۲^{-۱} \in C_G(x) \\ &\iff g_۱g_۲^{-۱}x = xg_۱g_۲^{-۱} \\ &\iff g_۲^{-۱}xg_۲ = g_۱^{-۱}xg_۱ \\ &\iff f((C_G(x)g_۲) = f(C_G(x)g_۱). \end{aligned}$$

پوشا بودن f نیز واضح است. بنابراین $|G : C_G(x))| = |\mathrm{orb}(x)|$. □

توجه می‌کنیم که $|G : C_G(x)| = ۱$ اگر و تنها اگر $x \in Z(G)$. پس $|\mathrm{orb}(x)| = ۱$ اگر و تنها اگر $x \in Z(G)$. حال فرض کنید $\mathrm{orb}(x_۱)$، ...، $\mathrm{orb}(x_k)$، $\mathrm{orb}(y_۱)$، ...، $\mathrm{orb}(y_m)$ همه‌ی رده‌های مزدوجی متمایز G باشند طوری که $|\mathrm{orb}(x_i)| = ۱$ برای $i = ۱, \ldots, k$ و $|\mathrm{orb}(y_i)| \geq ۲$ برای $i = ۱, \ldots, m$. آنگاه داریم

$$\begin{aligned} |G| &= \sum_{i=۱}^{k} |\mathrm{orb}(x_i)| + \sum_{i=۱}^{m} |\mathrm{orb}(y_i)| \\ &= k + \sum_{i=۱}^{m} |G : C_G(y_i)|. \end{aligned}$$

چون $k = |Z(G)|$ داریم

$$|G| = |Z(G)| + \sum_{i=۱}^{m} |G : C_G(y_i)|.$$

معادله‌ی اخیر را معادله‌ی رده‌ای G گوییم.
به عنوان کاربردی از معادله‌ی رده‌ای ثابت می‌کنیم هر گروه متناهی از مرتبه‌ی p^n، (p عدد اول) مرکز نابدیهی دارد.

قضیه ۱۳.۸.۳. فرض کنید G گروه و p عدد اول باشد. اگر $|G| = p^n$، آنگاه $Z(G) \neq \{۱\}$.

اثبات. معادله‌ی رده‌ای G را در نظر می‌گیریم. فرض کنید $\mathrm{orb}(y_۱)$، $\mathrm{orb}(y_۲)$، ...، $\mathrm{orb}(y_m)$ همه‌ی رده‌های مزدوجی متمایز و نابدیهی (با بیش از ۱ عضو) G باشند. چون $|G : C_G(y_i)|$ بزرگ‌تر از ۱ و بنا به قضیه‌ی لاگرانژ مقسوم علیه‌ای از $|G| = p^n$ است، داریم $p \mid |G : C_G(y_i)|$. پس $p \mid \sum_{i=۱}^{m} |G : C_G(y_i)|$. بنابراین

$$p \left| \left(|G| - \sum_{i=۱}^{m} |G : C_G(y_i)| \right) ; \right.$$

یعنی $p \mid |Z(G)|$ و $|Z(G)| > ۱$. □

نتیجه ۱۴.۸.۳. اگر $|G| = p^n$ (p عدد اول و $n > ۱$)، آنگاه G ساده نیست.

اثبات. طبق قضیه‌ی ۱۳.۸.۳، می‌دانیم $Z(G) \neq \{۱\}$. اگر $Z(G) < G$، آنگاه $Z(G)$ یک زیرگروه نرمال نابدیهی از G است. پس فرض کنید $G = Z(G)$. پس G آبلی است و هر زیرگروه آن نرمال است. حال اگر G هیچ زیرگروه نابدیهی نداشته باشد، بنا به تمرین ۲۱ از صفحه‌ی ۷۰، G دوری با مرتبه‌ی عدد اول است، یعنی $|G| = p$، که تناقض است. پس G حداقل یک زیرگروه نابدیهی دارد که قطعاً در G نرمال است (چون G آبلی است). □

اگر H و K دو زیرگروه از گروه G باشند، تعریف می‌کنیم

$$HK = \{hk \mid h \in H, k \in K\}.$$

در حالت کلی لزومی ندارد که HK زیرگروه G باشد. بدون توجه به این مطلب $|HK|$ را می‌توان یافت. در واقع داریم

قضیه ۱۵.۸.۳. اگر H و K دو زیرگروه از گروه متناهی G باشند، آنگاه

$$|HK| = \frac{|H||K|}{|H \cap K|}.$$

اثبات. داریم

$$HK = \bigcup_{h \in H} hK \qquad (۱)$$

تعداد هم مجموعه‌های متمایز در اجتماع رابطه‌ی (۱) را می‌شماریم. اگر $a, b \in H$، آنگاه

$$aK = bK \iff a^{-۱}b \in H \cap K \iff a(H \cap K) = b(H \cap K).$$

بنابراین تعداد $|H : H \cap K|$ هم‌مجموعه در اجتماع رابطه‌ی (۱) متمایزند. یعنی اگر $\{h_۱(H \cap K)$، ...، $h_t(H \cap K)\}$ مجموعه‌ی همه‌ی هم مجموعه‌های چپ متمایز $H \cap K$ در H باشد، داریم

$$HK = \bigcup_{i=۱}^{t} h_i K.$$

اکنون چون در اجتماع فوق هم‌مجموعه‌ها متمایزند، داریم

$$\begin{aligned} |HK| &= \left|\bigcup_{i=1}^{t} h_iK\right| \\ &= \sum_{i=1}^{t} |h_iK| \\ &= \sum_{i=1}^{t} |K| \\ &= t|K| \\ &= |H : H\cap K||K| \\ &= \frac{|H||K|}{|H\cap K|}. \end{aligned}$$ □

قضیه ۱۶.۸.۳. فرض کنید $K \le H \le G$. اگر T یک پیمایش چپ H در G و U یک پیمایش چپ K در H باشد، آنگاه TU یک پیمایش چپ K در G است، به ویژه $|G : K| = |G : H||H : K|$.

اثبات. چون $G = \bigcup_{t\in T} tH$ و $H = \bigcup_{u\in U} uK$، داریم

$$G = \bigcup_{t\in T} tH = \bigcup_{t\in T} t\left(\bigcup_{u\in U} uK\right) = \bigcup_{tu\in TU} tuK.$$

حال نشان می‌دهیم هم‌مجموعه‌های tuK مجزا هستند. اگر $tuK = t'u'K$ که در آن $t, t' \in T$ و $u, u' \in U$، آنگاه $(tu)^{-1}t'u' \in K$ و در نتیجه $u^{-1}t^{-1}t'u' \in K$. اما $K \le H$. پس $u^{-1}t^{-1}t'u' \in H$. چون $u, u' \in H$ داریم $t^{-1}t' \in H$. بنابراین $tH = t'H$. اما T یک پیمایش چپ H در G است. پس $t = t'$. در نتیجه $u^{-1}u' \in K$ و $uK = u'K$. چون U پیمایش K در H است داریم $u = u'$. پس ثابت شد TU یک پیمایش چپ K در G است. به ویژه

$$|G : K| = |TU| = |T||U| = |G : H||H : K|.$$ □

قضیه ۱۷.۸.۳. (لم پوانکاره) اگر H و K زیرگروه‌هایی از گروه G باشند، آنگاه داریم

$$|G : H\cap K| \le |G : H||G : K|.$$

اگر $|G : H| = m$ و $|G : K| = n$، طوری باشند که $\gcd\{m, n\} = 1$، آنگاه تساوی برقرار است.

اثبات. اگر $X = \{aH \mid a \in G\}$ و $Y = \{aK \mid a \in G\}$ به ترتیب مجموعه‌ی هم مجموعه‌های چپ H و K در G باشند، تابع f را از مجموعه‌ی هم مجموعه‌های $H\cap K$ در G به $X \times Y$ چنین تعریف می‌کنیم:

$$f(a(H\cap K)) = (aH, aK).$$

f خوش تعریف و یک‌به‌یک است، زیرا

$$\begin{aligned} a(H\cap K) = b(H\cap K) &\iff a^{-1}b \in H\cap K \\ &\iff a^{-1}b \in H,\ \ a^{-1}b \in K \\ &\iff aH = bH,\ \ aK = bK \\ &\iff (aH, aK) = (bH, bK). \end{aligned}$$

بنابراین

$$|G : H \cap K| \leq |X \times Y| = |X||Y| = |G : H||G : K| \tag{۲}$$

حال فرض کنید $|G : H| = m$ و $|G : K| = n$. طبق رابطه‌ی (۲)، $|G : H \cap K|$ متناهی است و کوچک‌تر یا مساوی mn. اکنون داریم $H \cap K \leq H \leq G$ و بنا به قضیه‌ی ۱۶.۸.۳،

$$|G : H \cap K| = |G : H||H : H \cap K|.$$

بنابراین $m \mid |G : H \cap K|$. به همین صورت داریم $n \mid |G : H \cap K|$. از این‌رو $\operatorname{lcm}\{m, n\} \mid |G : H \cap K|$. اما چون $\gcd\{m, n\} = ۱$ داریم $\operatorname{lcm}\{m, n\} = mn$. بنابراین $|G : H \cap K| = |G : K||G : H|$ و اثبات کامل است. □

ثابت کردیم که هر زیرگروه با شاخص ۲ نرمال است. این مطلب به طور کلی هم درست است: اگر p کوچک‌ترین عدد اولی باشد که $|G|$ را عاد می‌کند، آنگاه هر زیرگروه با شاخص p نرمال است. اینک می‌خواهیم اثباتی مقدماتی از این مطلب را انجام دیدیم. بعداً (در فصل ۵) این مطلب با استفاده از عمل گروه روی مجموعه نیز ثابت خواهد شد. ابتدا یک لم ثابت می‌کنیم:

لم ۱۸.۸.۳. فرض کنید H و K زیرگروه‌های G باشند. اگر L یک هم مجموعه‌ی چپ H در G و $R_۱$ و $R_۲$ دو هم‌مجموعه‌ی راست K در G باشند که $L \cap R_۱ \neq \emptyset$ و $L \cap R_۲ \neq \emptyset$، آنگاه $|L \cap R_۲| = |L \cap R_۱|$.

اثبات. فرض کنید $x \in L \cap R_۱$ و $y \in L \cap R_۲$. پس

$$L = xH = yH, \quad R_۱ = Kx, \quad R_۲ = Ky$$

و در نتیجه

$$L \cap R_۱ = xH \cap Kx = (xHx^{-۱} \cap K)x \tag{۳}$$
$$L \cap R_۲ = yH \cap Ky = (yHy^{-۱} \cap K)y \tag{۴}$$

چون $xH = yH$، داریم

$$xHx^{-۱} = yHx^{-۱} = y(Hx^{-۱}) = yHy^{-۱},$$

زیرا

$$\begin{aligned} xH = yH &\iff x^{-۱}y \in H \\ &\iff y^{-۱}x \in H \\ &\iff Hx^{-۱} = Hy^{-۱}. \end{aligned}$$

بنابراین از (۳) و (۴)، و این که $xHx^{-۱} = yHy^{-۱}$ نتیجه می‌گیریم

$$\begin{aligned} L \cap R_۱ &= (xHx^{-۱} \cap K)x, \\ L \cap R_۲ &= (xHx^{-۱} \cap K)y. \end{aligned}$$

پس $L \cap R_۱$ و $L \cap R_۲$ هر دو هم مجموعه‌های یک زیرگروه G، یعنی $xHx^{-۱} \cap K$، هستند و بنابراین تعداد اعضای‌شان برابر است. □

قضیه ۱۹.۸.۳. اگر p کوچک‌ترین عدد اولی باشد که $|G|$ را عاد می‌کند، آنگاه هر زیرگروه H از G با شاخص p، نرمال است.

اثبات. فرض کنید $g \in G$. اگر $g \in H$، آنگاه $gH = Hg$ و حکم ثابت است. پس فرض کنید $g \notin H$؛ یعنی $gH \cap H = \emptyset$. پس تعداد هم مجموعه‌های راست که با gH اشتراک دارند کوچک‌تر یا مساوی $p-1$ است. با توجه به لم ۱۸.۸.۳، تعداد عناصر این اشتراکها یعنی $gH \cap R_i$ مقدار ثابتی مثل c است. بنابراین

$$|H| = |gH| = \sum_{gH \cap R_i \neq \emptyset} |gH \cap R_i| = ck.$$

پس $k \mid |H|$ و در نتیجه $k \mid |G|$. چون p کوچک‌ترین عدد اول شمارنده $|G|$ است و $k \leq p-1$. بنابراین $k = 1$. پس تنها یک هم مجموعه‌ی راست با gH اشتراک دارد. چون $gH \cap Hg \neq \emptyset$، با توجه به این که هم مجموعه‌های H در G، G را افراز می‌کنند، $gH = Hg$. □

تمرین‌ها

۱. فرض کنید H و K زیرگروه‌های متناهی از گروه G باشند و $\gcd\{|H|, |K|\} = 1$. ثابت کنید $H \cap K = \{1\}$.

۲. فرض کنید $n, m \in \mathbb{N}$. ثابت کنید $n \mid \varphi(m^n - 1)$، که در آن φ تابع فی اویلر است.

۳. فرض کنید G گروهی متناهی باشد و $H, K \leq G$. نشان دهید
(الف) $|\langle H, K\rangle : K| \geq |H : H \cap K|$ (که در آن $\langle H, K\rangle = \langle H \cup K\rangle$).
(ب) اگر $|G : K| > \frac{1}{2}|H : H \cap K|$ آنگاه $G = \langle H, K\rangle$.

۴. فرض کنید K و H دو زیرگروه G باشند. ثابت کنید
(الف) $|H : H \cap K| \leq |G : K|$.
(ب) اگر G متناهی باشد، آنگاه $|H : H \cap K| = |G : K|$ اگر و تنها اگر $G = HK$.

۵. فرض کنید K و H زیرگروه‌هایی از گروه متناهی G باشند، که شاخص‌های‌شان در G نسبت به هم اولند، یعنی $\gcd\{|G : K|, |G : H|\} = 1$. ثابت کنید $G = HK$.

۶. فرض کنید $M < G$ و $|G : M| = p$، که در آن p عدد اول است. نشان دهید M زیرگروه ماکسیمال G است.

۷. فرض کنید $|G| = p^n m$، که در آن p عدد اول است و $p \nmid m$. اگر H و K دو زیرگروه G باشند که $|H| = p^n$ و $|K| = p^s$، که در آن $0 \leq s \leq n$ و $K \not\subseteq H$، نشان دهید HK زیرگروه G نیست.

۸. ثابت کنید تعداد مزدوج‌های زیر مجموعه‌ی X از گروه G برابر است با $|G : N_G(X)|$.

۹. فرض کنید G گروه متناهی باشد. اگر $k(G)$ نشان دهنده تعداد رده‌های مزدوجی G باشد، نشان دهید
(الف) $k(G) = 2$ اگر و تنها اگر $G \cong \mathbb{Z}_2$.
(ب) $k(G) = 3$ اگر و تنها اگر $G \cong \mathbb{Z}_3$ یا $G \cong S_3$.

۱۰. فرض کنید G گروهی متناهی، و $f \in \operatorname{Aut} G$ طوری باشد که بیش از $\frac{3}{4}$ عناصر G را به وارون‌های‌شان تصویر می‌کند. ثابت کنید به ازای هر $g \in G$، $f(g) = g^{-1}$. بنابراین G آبلی است. گروهی متناهی مثال بزنید که یک خودریختی آن دقیقاً $\frac{3}{4}$ عناصر را به وارون‌های‌شان تصویر کند.

۱۱. فرض کنید n عددی صحیح باشد.
(الف) فرض کنید G گروهی دوری از مرتبه‌ی n باشد. به ازای هر شمارنده s از n، G_s را زیرگروه یکتای G از مرتبه‌ی s بگیرید. ثابت کنید $G_s = \{x \in G \mid x^s = 1\}$.
(ب) نشان دهید $\sum_{s \mid n} \varphi(s) = n$، که در آن φ تابع فی اویلر است.
(ج) فرض کنید G گروهی از مرتبه‌ی n باشد که به ازای هر شمارنده s از n، حداکثر یک زیرگروه مرتبه‌ی s دارد. ثابت کنید G دوری است.

۱۲. اگر G گروه متناهیاً تولید شده و H زیرگروهی با شاخص متناهی در G باشد. ثابت کنید H متناهیاً تولید شده است.

۱۳. فرض کنید $G = \langle g_1, g_2, \ldots, g_k \rangle$ گروهی متناهیاً تولید شده باشد و $|G'| = m$. ثابت کنید $|G : Z(G)| \leq m^k$.

۱۴. فرض کنید G گروه متناهی باشد و $H \leq G$. ثابت کنید

(الف) $\left| \bigcup_{g \in G} g^{-1} H g \right| \leq 1 + |G| - |G : H|$. بنابراین اجتماع مزدوج‌های یک زیرگروه سره زیر مجموعه‌ی سره‌ی G است.

(ب) اگر H از هر رده‌ی مزدوجی حداقل یک عضو داشته باشد، آنگاه $G = H$.

۱۵. اگر G گروه باشد FC-مرکز G را برابر مجموعه‌ی همه عناصر G که رده‌ی مزدوجی آن ها متناهی است تعریف می‌کنیم:

$$FC(G) = \{x \in G \mid |G : C_G(x)| < \infty\}.$$

ثابت کنید $FC(G) \leq G$.

۱۶. اگر $G = FC(G)$ یعنی هر عضو G تعداد متناهی مزدوج داشته باشد، G را FC- گروه گوییم. ثابت کنید هر زیرگروه یک FC- گروه، FC- گروه است.

۱۷. فرض کنید G یک FC- گروه متناهیاً تولید شده باشد. ثابت کنید $|G : Z(G)| < \infty$.

۱۸. اگر $|G : Z(G)| < \infty$، ثابت کنید G، FC- گروه است.

۱۹. فرض کنید G گروه متناهی و p کوچک‌ترین عدد اول شمارنده $|G|$ باشد. ثابت کنید اگر $k(G) > \frac{|G|}{p}$، آنگاه $Z(G) \neq \{1\}$. ($k(G)$ تعداد رده‌های مزدوجی G است.)

۲۰. اگر G گروهی متناهی و ناآبلی باشد، نشان دهید $k(G) > |Z(G)| + 1$.

۲۱. فرض کنید n عدد طبیعی باشد. ثابت کنید گروه G با $|G| = n$ و $|G : Z(G)| = 4$ وجود دارد اگر و تنها اگر $8|n$.

۹.۳ گروه‌های خارج‌قسمتی

در بخش ۸.۳، دیدیم که به ازای هر زیرگروه از گروه G دو افراز از G وجود دارد: مجموعه‌ی هم مجموعه‌های چپ و مجموعه‌ی هم مجموعه‌های راست. اولین بار این دو افراز را گالوا در سال ۱۸۳۱ در نظر گرفت. گالوا دو افراز را "سره" نامید اگر عناصر نظیر هر دو افراز با هم برابر باشند، یعنی هم مجموعه‌های چپ و راست با هم مساوی باشند. چنین زیرگروه‌های هم اکنون نرمال نامیده می‌شوند. گالوا نشان داد که حل‌پذیر ی چندجمله‌ای‌ها با استفاده از رادیکالها با مفهوم یک زیرگروه نرمال از گروه جایگشتی ریشه‌ها و گروهی که با استفاده از این زیرگروه نرمال ساخته می‌شود (این گروه را هم اکنون گروه خارج‌قسمتی گوییم) مربوط است. ژردان زیرگروه نرمال به صورت معمول امروزی را (بدون ذکر کلمه نرمال) تعریف کرد. در این بخش گروه‌های خارج‌قسمتی را که با استفاده از زیرگروه‌های نرمال ساخته می‌شوند بررسی می‌کنیم. ابتدا بحثی کشاف برای توجیه مطالب ارائه می‌کنیم.

اگر n عدد طبیعی باشد می‌دانیم $\mathbb{Z}_n = \{\bar{0}, \bar{1}, \ldots, \overline{n-1}\}$ متشکل از رده‌های هم‌ارزی رابطه‌ی هم‌نهشتی به پیمانه‌ی n یک گروه تشکیل می‌دهند. در واقع همانطور که دیدیم رده‌های هم‌ارزی فوق در واقع هم مجموعه‌های چپ $n\mathbb{Z}$ در $\mathbb{Z}$ هستند ، یعنی

$$\bar{a} = a + n\mathbb{Z}.$$

جمع دو رده‌ی هم‌ارزی به صورت زیر است

$$\bar{a} + \bar{b} = \overline{a+b}$$

یعنی

$$(a + n\mathbb{Z}) + (b + n\mathbb{Z}) = (a + b) + n\mathbb{Z}.$$

آیا به طور کلی اگر G گروه دلخواه باشد و $H \leq G$، مجموعه‌ی $\{aH \mid a \in G\}$ متشکل از هم مجموعه‌های چپ H در G تحت

$$(aH)(bH) = abH$$

یک گروه تشکیل می‌دهند؟ اولین قدم بررسی خوش‌تعریفی عمل است. حال ببینیم چه موقع عمل فوق خوش تعریف است. در واقع برای خوش‌تعریفی باید ثابت کنیم اگر $aH = a_۱H$ و $bH = b_۱H$، آنگاه $(aH)(bH) = (a_۱H)(b_۱H)$. یعنی $abH = a_۱b_۱H$، یعنی $(ab)^{-۱}a_۱b_۱ \in H$. چون $aH = a_۱H$ و $bH = b_۱H$، اعضای $h, k \in H$ وجود دارند که $a = a_۱h$ و $b = b_۱k$. اکنون

$$(ab)^{-۱}a_۱b_۱ = b^{-۱}a^{-۱}a_۱b_۱ = k^{-۱}b_۱^{-۱}h^{-۱}a_۱^{-۱}a_۱b_۱ = k^{-۱}b_۱^{-۱}h^{-۱}b_۱$$

چون $k \in H$ شرط لازم و کافی برای این که عبارت فوق در H باشد این است که $b_۱^{-۱}h^{-۱}b_۱ \in H$. این شرط، در صورتی که H در G نرمال باشد، به وضوح برقرار است. بنابراین قضیه زیر را داریم.

قضیه ۱.۹.۳. اگر $H \trianglelefteq G$، آنگاه مجموعه‌ی هم مجموعه‌های چپ H در G تحت

$$(aH)(bH) = abH$$

یک گروه تشکیل می‌دهد.

اثبات. چون H در G نرمال است، بحث پیش از قضیه نشان می‌دهد که عمل ضرب هم‌مجموعه‌ها خوش تعریف است. اکنون به ازای همه هم‌مجموعه‌های cH، bH، aH داریم

$$(aHbH)cH = (abH)cH = (ab)cH = a(bc)H = aH(bHcH),$$

یعنی عمل شرکت‌پذیر است. هم‌چنین

$$(aH)(۱H) = a۱H = aH, \quad (۱H)(aH) = ۱aH = aH,$$

یعنی $۱H = H$ عضو همانی است. به علاوه

$$(aH)(a^{-۱}H) = aa^{-۱}H = ۱H = H,$$

و

$$(a^{-۱}H)(aH) = a^{-۱}aH = ۱H = H,$$

یعنی $(aH)^{-۱} = a^{-۱}H$. بنابراین مجموعه‌ی هم مجموعه‌های چپ H در G تحت ضرب متعارف هم‌مجموعه‌ها یک گروه تشکیل می‌دهد. □

در حالتی که $N \trianglelefteq G$ مجموعه‌ی هم مجموعه‌های چپ N در G را با G/N نشان می‌دهیم و آن را گروه خارج‌قسمتی می‌نامیم.

مثال ۲.۹.۳. اگر n عدد طبیعی باشد، چون $\mathbb{Z}$ یک گروه آبلی است $n\mathbb{Z} \trianglelefteq \mathbb{Z}$. پس $\mathbb{Z}/n\mathbb{Z}$ تحت عمل جمع هم‌مجموعه‌ها یک گروه است:

$$(a + n\mathbb{Z}) + (b + n\mathbb{Z}) = (a + b) + n\mathbb{Z}.$$

چون $\bar{a} = a + n\mathbb{Z}$، داریم $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n$. □

به عنوان کاربردی از قضیه‌ی لاگرانژ، گروه‌های خارج‌قسمتی، و معادله‌ی رده‌ای، قضیه‌ای معروف موسوم به قضیه‌ی کُشی را ثابت می‌کنیم: اگر عدد اول p مرتبه‌ی گروه G را عاد کند، آنگاه G عضوی از مرتبه‌ی p دارد. قضیه‌ی خاصی حالت خاصی از قضیه‌ی سیلو است که در فصل ۵ آن‌را به تفصیل بررسی می‌کنیم. ابتدا حالتی را که گروه G آبلی باشد در نظر می‌گیریم :

قضیه ۳.۹.۳. (قضیه‌ی کُشی برای گروه‌های آبلی) فرض کنید G گروه آبلی متناهی و p عدد اول باشد. اگر $p \mid |G|$، آنگاه G عضوی از مرتبه‌ی p دارد.

اثبات. قضیه را به استقرا روی $|G|$ اثبات می‌کنیم. اگر $|G| = ۱$، حکم به انتفای مقدم برقرار است: p مرتبه‌ی G را عاد نمی‌کند. حال فرض کنید قضیه برای همه‌ی زیرگروه‌هایی که مرتبه‌ی آن‌ها از $|G|$ کمتر است، درست باشد. اگر G زیرگروه نابدیهی نداشته باشد، آنگاه G دوری با مرتبه‌ی عددی اول است (تمرین ۲۱ از صفحه‌ی ۷۰). چون $p \mid |G|$، داریم $|G| = p$. بنابراین همه‌ی $p - ۱$ عضو نابدیهی G در حکم قضیه صدق می‌کنند. پس فرض کنید G زیرگروه نابدیهی مثل K داشته باشد. اگر $p \mid |K|$، آنگاه طبق فرض استقرا K و بنابراین G عضوی از مرتبه‌ی p دارد. پس فرض کنید $p \nmid |K|$. چون G آبلی است، $K \trianglelefteq G$ و می‌توان G/K را تشکیل داد. توجه کنید چون $۱ < K < G$، $۱ < |G/K| < |G|$. اکنون $|G| = |G/K||K|$ را عاد می‌کند و $|K|$ را عاد نمی‌کند، پس $p \mid |G/K|$. بنابراین طبق فرض استقرا G/K عضوی چون xK با مرتبه‌ی p دارد. فرض کنید $|K| = m$. ادعا می‌کنیم $y = x^m$ عضوی از مرتبه‌ی p است. چون $O(xK) = p$، داریم $x^p \in K$. بنا به نتیجه‌ی قضیه‌ی لاگرانژ، $y^p = x^{mp} = ۱$. پس $O(y) \mid p$. اگر $O(y) = ۱$، داریم $x^m = y = ۱$. چون $\gcd\{p, |K|\} = ۱$، اعداد صحیح $c_۱$ و $c_۲$ وجود دارند که $c_۱p + c_۲m = ۱$. بنابراین

$$x = x^{۱} = x^{c_۱p}x^{c_۲m} = x^{c_۱p} \in K,$$

که نتیجه می‌دهد $xK = K$ و این خلاف $O(xK) = p$ است. پس $O(y) = p$ و حکم ثابت است. □

اکنون حالت کلی را در نظر می‌گیریم.

قضیه ۴.۹.۳. (قضیه‌ی کُشی) فرض کنید G گروه متناهی و p عدد اول باشد. اگر $p \mid |G|$، آنگاه G عضوی از مرتبه‌ی p دارد.

اثبات. به استقرا روی G عمل می‌کنیم. در حالت $|G| = ۱$ چیزی برای اثبات نیست. فرض کنید $|G| > ۱$ و قضیه برای زیرگروه‌هایی که مرتبه‌هایشان از $|G|$ کمتر است درست باشد. فرض کنید $\text{orb}(y_۱)$، ...، $\text{orb}(y_m)$ همه‌ی رده‌های مزدوجی متمایز و نابدیهی G باشند. معادله‌ی رده‌ای G را در نظر می‌گیریم:

$$|G| = |Z(G)| + \sum_{i=۱}^{m} |G : C_G(y_i)|.$$

به ازای هر $i = ۱, ۲, \ldots, m$، داریم $|G : C_G(y_i)| > ۱$. بنابراین $C_G(y_i)$ زیرگروه سره‌ای از G است. اگر به ازای یک i، $p \mid |C_G(y_i)|$، آنگاه بنا به فرض استقرا $C_G(y_i)$ و بنابراین G عضوی از مرتبه‌ی p دارد. پس فرض کنید به ازای هر $i = ۱, ۲, \ldots, m$، $p \nmid |C_G(y_i)|$. چون به ازای هر $i = ۱, ۲, \ldots, m$، $p \mid |G : C_G(y_i)||C_G(y_i)| = |G|$ را عدد می‌کند و $|C_G(y_i)|$ را عاد نمی‌کند، به ازای هر $i = ۱, ۲, \ldots, m$، داریم $p \mid |G : C_G(y_i)|$. در نتیجه p، $|G| - \sum_{i=۱}^{m} |G : C_G(y_i)| = |Z(G)|$ را عاد می‌کند. پس طبق قضیه‌ی کُشی برای گروه‌های آبلی $Z(G)$ و بنابراین G عضوی از مرتبه‌ی p دارد. □

اگر $H \trianglelefteq G$، آنگاه $\pi : G \longrightarrow G/H$ با ضابطه‌ی $\pi(g) = gH$ یک همریختی پوشاست که آن را همریختی طبیعی گوییم. واضح است که $\ker \pi = H$. بنابراین $H \trianglelefteq G$ اگر و تنها اگر H هسته‌ی یک همریختی از G به گروه دیگر باشد.
حال سوالی که مطرح است این است که زیرگروه‌های یک گروه خارج‌قسمتی به چه صورت هستند؟ قضیه‌ی بعدی این سوال را پاسخ می‌دهد.

قضیه ۵.۹.۳. فرض کنید $N \trianglelefteq G$، آنگاه هر زیرگروه G/N به صورت K/N است که در آن $N \subseteq K \leq G$. به علاوه $K/N \trianglelefteq G/N$ اگر و تنها اگر $K \trianglelefteq G$.

اثبات. همریختی طبیعی $\pi : G \longrightarrow G/N$ را در نظر می‌گیریم. فرض کنید X زیرگروهی از G/N باشد. می‌دانیم $K = \pi^{-۱}(X)$ زیرگروهی از G است (مثال ۳.۴.۳). داریم

$$g \in \pi^{-۱}(X) \iff \pi(g) \in X \iff gN \in X.$$

پس $K = \pi^{-۱}(X) = \{g \in G \mid gN \in X\} \leq G$. برای هر $a \in N$ داریم $aN = N \in X$. بنابراین $N \subseteq K \leq G$ و در واقع $K/N = X$. حال اگر X در G/N نرمال باشد، آنگاه به سادگی می‌توان دید که $K = \pi^{-۱}(X)$ نیز در G نرمال است.
برعکس فرض کنید K زیرگروهی از G و شامل N باشد. چون N در G نرمال است، در K نیز نرمال است. بنابراین داریم $N \trianglelefteq K$ و $K/N = \pi(K) \leq G/N$ (تمرین ۷ از صفحه‌ی ۶۹ را ببینید) و اگر $K \trianglelefteq G$، آنگاه $K/N = \pi(K) \trianglelefteq G/N$. □

تمرین‌ها

۱. فرض کنید $H \leq G$. اگر مجموعه‌ی هم مجموعه‌های چپ H در G تحت عمل متعارف یک گروه تشکیل دهند، ثابت کنید $H \trianglelefteq G$.

۲. فرض کنید $H \trianglelefteq G$ و $|G : H| = n$. ثابت کنید به ازای هر $g \in G$ داریم $g^n \in H$. نشان دهید اگر H در G نرمال نباشد، این نتیجه الزاماً درست نیست.

۳. فرض کنید $H \trianglelefteq G$ و $|G/H| = n$. اگر $g \in G$ و به ازای یک $m \in \mathbb{Z}$ داشته باشیم $g^m \in H$ و $\gcd\{m, n\} = ۱$، نشان دهید $g \in H$.

۴. فرض کنید $K \trianglelefteq G$ و $|K| = m$. اگر $x \in G$ و n عدد صحیح مثبت باشد که $\gcd\{m, n\} = ۱$، ثابت کنید
(الف) اگر $O(x) = n$، آنگاه $O(xK) = n$.
(ب) اگر $O(xK) = n$، آنگاه عضو $y \in G$ وجود دارد که $O(y) = n$ و $xK = yK$.

۵. فرض کنید p عددی اول باشد. اگر مرتبه‌ی هر عضو گروه G توانی از p باشد، یعنی به ازای هر $a \in G$ عدد m وجود داشته باشد که $O(a) = p^m$، G را p- گروه می‌نامیم. ثابت کنید G یک p- گروه است اگر و تنها اگر عدد صحیح $n \geq ۰$ وجود داشته باشد که $|G| = p^n$.

۶. اگر $G/Z(G)$ دوری باشد ثابت کنید G آبلی است. نتیجه بگیرید که هر گروه مرتبه‌ی $p^۲$ آبلی است (p عدد اول).

۷. فرض کنید G گروه مرتبه‌ی p^n باشد (p عدد اول و $n > ۱$). به استقرا روی n نشان دهید هر زیرگروه مرتبه‌ی $p^{n-۱}$ در G نرمال است.

۸. فرض کنید G گروه آبلی از مرتبه‌ی n باشد و $m|n$. به استقرا روی n نشان دهید G زیرگروهی از مرتبه‌ی m دارد.

۹. فرض کنید $K \leq H \leq G$ و $K \operatorname{char} G$. اگر $H/K \operatorname{char} G/K$، نشان دهید $H \operatorname{char} G$.

۱۰. اگر H زیرگروه نرمال گروه حل‌پذیر G باشد، نشان دهید G/Hحل‌پذیر است.

۱۱. فرض کنید H زیرگروه نرمال گروه G باشد. اگر H و G/H حل‌پذیر باشند نشان دهید Gحل‌پذیر است.

۱۲. فرض کنید G یک گروه متناهی باشد، $H \leq G$، $N \trianglelefteq G$، و $(|H|, |G : N|) = ۱$. ثابت کنید $H \leq N$.

۱۳. فرض کنید G گروه باشد.
(الف) نشان دهید G/G' آبلی است؛ به طور کلی نشان دهید اگر $H \trianglelefteq G$، آنگاه G/H آبلی است اگر و تنها اگر $G' \leq H$.
(ب) اگر مرتبه‌ی هر عضو G' متناهی باشد (G' تاب‌دار)، آنگاه عناصر با مرتبه‌ی متناهی در G یک زیرگروه تشکیل می‌دهند.

۱۴. اگر $|G| = p^n$، آنگاه یک سری

$$G = G_۰ \supset G_۱ \supset G_۲ \supset \cdots \supset G_n = \{۱\}$$

از زیرگروه‌های G وجود دارد که $G_i \trianglelefteq G$ و $|G_i/G_{i+۱}| = p$ به ازای هر i.

۱۵. (قضیه‌ی اول سیلو) با استفاده از معادله‌ی رده‌ای ثابت کنید که اگر $|G| = p^n m$، که در آن p عدد اول است و $p \nmid m$، آنگاه G زیرگروهی از مرتبه‌ی p^n دارد.

۱۶. فرض کنید H زیرگروه سره‌ای از $\mathbb{Q}$ باشد. نشان دهید
(الف) $\mathbb{Q}/H$ نامتناهی است. (ب) $\mathbb{Q}/H$ دوری نیست.

۱۷. نشان دهید $\mathbb{Q}$ زیرگروه ماکسیمال ندارد.

۱۸. نشان دهید $\mathbb{R}$ زیرگروه ماکسیمال ندارد.

۱۹. فرض کنید G گروهی ناآبلی باشد و $|G| = p^۳$ (که در آن p عددی اول است)، نشان دهید $|Z(G)| = p$ و $k(G) = p^۲ + p - ۱$.

۲۰. فرض کنید H زیرگروهی از گروه متناهی G باشد. ثابت کنید
(الف) اگر $H \trianglelefteq G$، آنگاه $k(G/H) \leq k(G) - j + ۱$، که در آن j تعداد رده‌های مزدوجی عناصر G است که در H قرار دارند.

(ب) اگر G ناآبلی و $G/Z(G)$ آبلی باشد، آنگاه

$$k(G) \geq |G/Z(G)| + |Z(G)| - ۱.$$

۲۱. ثابت کنید هر گروه خارج‌قسمتی یک FC- گروه، FC- گروه است.

۲۲. اگر G گروهی متناهی باشد و $x \in G$، ثابت کنید $|G/G'| \leq |C_G(x)|$.

۲۳. اگر G یک FC- گروه باشد، نشان دهید $G/Z(G)$ یک FC- گروه تاب‌دار است.

۲۴. اگر $|G/Z(G)| = n$ ثابت کنید

(الف) G حداکثر $n^۲$ تعویض‌گر دارد.

(ب) به ازای هر $x, y \in G$ داریم $[x, y]^{n+۱} = [x, y^۲][y^{-۱}xy, y]^{n-۱}$.

(ج) هر عضو G' را می‌توان به صورت حداکثر $n^۳$ تعویض‌گر نوشت.

(د) G' متناهی است و در حقیقت $|G'| \leq n^{۲n^۳}$.

۲۵. اگر در گروه نامتناهی G هر زیرگروه نابدیهی شاخص متناهی داشته باشد، ثابت کنید G دوری است.

۲۶. (الف) فرض کنید G یک گروه آبلی و $x_n \in G$، $n = ۱, ۲, \ldots$، اعضای G باشند طوری که $O(x_۱) = p$، و به ازای هر $n = ۱, ۲, \ldots$، $x_{n+۱}^p = x_n$. ثابت کنید $\langle x_n \mid n \geq ۱ \rangle \cong C_{p^\infty}$.

(ب) فرض کنید p عدد اول باشد و به ازای هر $n \in \mathbb{N}$، T_{p^n} گروه تولید شده توسط $\frac{۱}{p^n} + \mathbb{Z}$ در گروه جمعی $\mathbb{Q}/\mathbb{Z}$ باشد:

$T_{p^n} = \left\langle \frac{۱}{p^n} + \mathbb{Z} \right\rangle$. قرار می‌دهیم $\mathbb{Z}_{p^\infty} = \bigcup_{n=۱}^{\infty} T_{p^n}$. نشان دهید $\mathbb{Z}_{p^\infty} \cong C_{p^\infty}$.

۱۰.۳ قضایای یکریختی

قبلاً دیده‌ایم که اگر $\psi : G \longrightarrow H$ همریختی باشد، آنگاه $\ker \psi \trianglelefteq G$ و گروه خارج‌قسمتی $G/\ker \psi$ را می‌توان تشکیل داد. این گروه با ψ و G چه ارتباطی دارد؟ در واقع قضیه‌ی اول یکریختی، که هم اکنون ثابت می‌کنیم، می‌گوید این گروه با $\operatorname{Im} \psi$ یکریخت است:

قضیه ۱.۱۰.۳. (قضیه‌ی اول یکریختی) اگر $\psi : G \longrightarrow H$ همریختی باشد، آنگاه $G/\ker \psi \cong \operatorname{Im} \psi$

اثبات. تابع $\bar{\psi} : G/\ker \psi \longrightarrow \operatorname{Im} \psi$ را به صورت زیر تعریف می‌کنیم

$$\bar{\psi}(g \ker \psi) = \psi(g).$$

$\bar{\psi}$ خوش تعریف و یک‌به‌یک است، زیرا

$$\begin{aligned} g_۱ \ker \psi = g_۲ \ker \psi &\iff g_۱^{-۱} g_۲ \in \ker \psi \\ &\iff \psi(g_۱^{-۱} g_۲) = ۱ \\ &\iff \psi(g_۱)^{-۱} \psi(g_۲) = ۱ \\ &\iff \psi(g_۱) = \psi(g_۲) \\ &\iff \bar{\psi}(g_۱ \ker \psi) = \bar{\psi}(g_۲ \ker \psi). \end{aligned}$$

$\bar{\psi}$ همریختی است، زیرا ψ همریختی است. پوشا بودن $\bar{\psi}$ نیز واضح است. □

مثال ۲.۱۰.۳. ثابت کنید $U \cong \mathbb{R}/\mathbb{Z}$ که در آن U دایره‌ی واحد است.

حل تابع $\psi : \mathbb{R} \longrightarrow U$ با ضابطه‌ی $\psi(x) = e^{۲\pi ix}$ را در نظر می‌گیریم. ψ همریختی است زیرا

$$\psi(x+y) = e^{۲\pi i(x+y)} = e^{۲\pi ix}e^{۲\pi iy} = \psi(x)\psi(y).$$

هسته‌ی ψ را می‌یابیم

$$x \in \ker\psi \iff \psi(x) = ۱ \iff e^{۲\pi ix} = ۱ \iff x = n, \quad n \in \mathbb{Z}.$$

پس $\ker\psi = \mathbb{Z}$. از طرف دیگر به وضوح ψ پوشاست، یعنی $\operatorname{Im}\psi = U$. از این‌رو بنا به اولین قضیه‌ی یکریختی $\mathbb{R}/\mathbb{Z} \cong U$. □

مثال ۳.۱۰.۳. ثابت کنید $\mathbb{R}^\times/C_۲ \cong \mathbb{R}^\times_{pos}$.

حل تابع $\psi : \mathbb{R}^\times \longrightarrow \mathbb{R}^\times_{pos}$ را با ضابطه‌ی $\psi(x) = |x|$ یک همریختی پوشاست. داریم

$$x \in \ker\psi \iff \psi(x) = ۱ \iff |x| = ۱ \iff x = \pm ۱.$$

پس $\ker\psi = C_۲$ و بنا به قضیه‌ی اول یکریختی $\mathbb{R}^\times/C_۲ \cong \mathbb{R}^\times_{pos}$. □

مثال ۴.۱۰.۳. ثابت کنید $\mathbb{C}^\times/\mathbb{R}^\times_{pos} \cong U$.

حل تابع $\psi : \mathbb{C}^\times \longrightarrow U$ با ضابطه‌ی $\psi(z) = \dfrac{z}{|z|}$ را در نظر می‌گیریم. ψ همریختی پوشا با هسته‌ی $\mathbb{R}^\times_{pos}$ است. پس حکم از اولین قضیه‌ی یکریختی نتیجه می‌شود. □

مثال ۵.۱۰.۳. فرض کنید G گروه دلخواه باشد. ثابت کنید $G/Z(G) \cong \operatorname{Inn} G$.

حل ابتدا توجه کنید که با ازای هر $g, h \in G$ و به ازای هر $x \in G$ داریم

$$\tau_{gh}(x) = (gh)x(gh)^{-۱} = g(hxh^{-۱})g^{-۱} = \tau_g(hxh^{-۱}) = \tau_g\tau_h(x).$$

پس $\tau_{gh} = \tau_g\tau_h$. با توجه به این نکته تابع $\psi : G \longrightarrow \operatorname{Inn} G$ را با $\psi(g) = \tau_g$ تعریف می‌کنیم. ψ همریختی است، زیرا

$$\psi(g_۱g_۲) = \tau_{(g_۱g_۲)} = \tau_{g_۱g_۲} = \tau_{g_۱}\tau_{g_۲} = \psi(g_۱)\psi(g_۲).$$

هسته‌ی ψ برابر $Z(G)$ است، زیرا

$$g \in \ker\psi \iff \psi(g) = ۱ \iff \tau_g = ۱ \iff g \in Z(G).$$

از طرف دیگر به وضوح ψ پوشاست. از این‌رو بنا به قضیه‌ی اول یکریختی

$$G/Z(G) \cong \operatorname{Inn} G. \qquad \square$$

قضیه ۶.۱۰.۳. (قضیه‌ی دوم یکریختی) اگر $H \leq G$ و $K \trianglelefteq G$، آنگاه $H \cap K \trianglelefteq H$ و $\dfrac{H}{H \cap K} \cong \dfrac{HK}{K}$

اثبات. تابع $\psi : H \longrightarrow HK/K$ را با ضابطه‌ی $\psi(h) = hK$ در نظر می‌گیریم به وضوح ψ همریختی است. اگر $h_۱k_۱K \in HK/K$، آنگاه داریم $\psi(h_۱) = h_۱K = h_۱k_۱K$، یعنی ψ پوشاست. هسته‌ی ψ را می‌یابیم

$$h \in \ker\psi \iff \psi(h) = ۱_{HK/K} \iff hK = K \iff h \in K.$$

بنابراین $\ker\psi = H \cap K$ و $H \cap K \trianglelefteq H$. از این‌رو بنا به قضیه‌ی اول یکریختی داریم $H/(H \cap K) \cong HK/K$. □

قضیه ۷.۱۰.۳. (قضیه‌ی سوم یکریختی) اگر $N \trianglelefteq G$ و $K \trianglelefteq G$ و $N \subseteq K$، آنگاه $\dfrac{G/N}{K/N} \cong G/K$.

اثبات. تابع $\psi : G/N \longrightarrow G/K$ را با ضابطه‌ی $\psi(gN) = gK$ در نظر می‌گیریم. ψ خوش تعریف است، زیرا

$$\begin{aligned} g_1N = g_2N &\implies g_1^{-1}g_2 \in \mathbb{N} \\ &\implies g_1^{-1}g_2 \in K \ \ (N \subseteq K) \\ &\implies g_1K = g_2K \\ &\implies \psi(g_1N) = \psi(g_2N). \end{aligned}$$

ψ به وضوح همریختی و پوشا نیز هست. حال هسته‌ی ψ را می‌یابیم:

$$\begin{aligned} gN \in \ker\psi &\iff \psi(gN) = 1_{G/K} \\ &\iff gK = K \\ &\iff g \in K. \end{aligned}$$

پس هسته‌ی ψ عبارت است از $\ker\psi = \{gN \in G/N \mid g \in K\} = K/N$. بنابراین طبق قضیه‌ی اول یکریختی $\frac{G/N}{K/N} \cong G/K$.

تمرین‌ها

۱. فرض کنید G گروهی ناآبلی باشد. ثابت کنید $\operatorname{Aut} G$ دوری نیست.

۲. نشان دهید گروه متناهی G وجود ندارد که $\operatorname{Aut} G$ دوری با مرتبه‌ی فرد بیش از ۱ باشد.

۳. اگر $H \leq G$ ثابت کنید $C_G(H) \trianglelefteq N_G(H)$ و $N_G(H)/C_G(H)$ با زیرگروهی از $\operatorname{Aut} H$ یکریخت است.

۴. فرض کنید K زیرگروه نرمالی با مرتبه‌ی p از گروه متناهی G باشد، که در آن p کوچک‌ترین عدد اول شمارنده $|G|$ است. ثابت کنید $K \leq Z(G)$.

۵. فرض کنید G گروه نامتناهی باشد که هیچ گروه خارج‌قسمتی نابدیهی ندارد. ثابت کنید هر زیرگروه متناهی و نرمال G آبلی است و در مرکز G قرار دارد.

۶. فرض کنید A و B دو زیرگروه آبلی از گروه ناآبلی و متناهی G باشند و p کوچک‌ترین عدد اول شمارنده‌ی مرتبه‌ی G. اگر $|G : A| = |G : B| = p$، نشان دهید $\operatorname{Inn} G$ گروه آبلی و غیر دوری با مرتبه‌ی p^2 است.

۷. فرض کنید H زیرگروه نرمال و متناهی از گروه G باشد، طوری که $G/H \cong \mathbb{Z}$. نشان دهید G زیرگروه نرمال نامتناهی با شاخص متناهی دارد.

فصل ٤

حاصل‌ضرب گروه‌ها

۱.۴ حاصل‌ضرب مستقیم گروه‌ها

فرض کنید H و K دو گروه دلخواه باشند. حاصل‌ضرب دکارتی $H \times K$ را در نظر می‌گیریم. یادآوری می‌کنیم که با عمل ضرب مولفه‌ای این حاصل‌ضرب دکارتی به یک گروه تبدیل می‌شود: در واقع برای هر $h_۱, h_۲ \in H$ و $k_۱, k_۲ \in K$ تعریف می‌کنیم

$$(h_۱, k_۱)(h_۲, k_۲) = (h_۱h_۲, k_۱k_۲).$$

شرکت‌پذیری در $H \times K$ با استفاده از شرکت‌پذیری در H و K ثابت می‌شود:

$$\begin{aligned}
[(h_۱, k_۱)(h_۲, k_۲)](h_۳, k_۳) &= (h_۱h_۲, k_۱k_۲)(h_۳, k_۳) \\
&= ((h_۱h_۲)h_۳, (k_۱k_۲)k_۳)) \\
&= (h_۱(h_۲h_۳), (k_۱(k_۲k_۳)) \\
&= (h_۱, k_۱)(h_۲h_۳, k_۲k_۳) \\
&= (h_۱, k_۱)[(h_۲, k_۲)(h_۳, k_۳)].
\end{aligned}$$

عضو بی‌اثر $H \times K$ عبارت است از $(۱_H, ۱_K)$، زیرا

$$(h, k)(۱_H, ۱_K) = (h۱_H, k۱_K) = (h, k)$$

و

$$(۱_H, ۱_K)(h, k) = (۱_Hh, ۱_Kk) = (h, k).$$

وارون $(h, k) \in H \times K$ برابر $(h^{-۱}, k^{-۱})$ است، زیرا

$$(h, k)(h^{-۱}, k^{-۱}) = (hh^{-۱}, kk^{-۱}) = (۱_H, ۱_K),$$

و

$$(h^{-۱}, k^{-۱})(h, k) = (h^{-۱}h, k^{-۱}k) = (۱_H, ۱_K).$$

بنابراین $H \times K$ با عمل ضرب مولفه‌ای یک گروه است. $H \times K$ را حاصل‌ضرب مستقیم (خارجی) H و K گوییم. به عنوان مثال در گروه $Q_۸ \times \mathbb{Z}$ داریم

$$(i, ۳)(j, ۴) = (ij, ۳ + ۴) = (k, ۷).$$

در حالتی که هر دو گروه H و K آبلی جمعی باشند گاهی اوقات به جای $H \times K$ می‌نویسیم $H \oplus K$ و می‌گوییم حاصل‌جمع مستقیم H و K.

مثال ۱.۱.۴. داریم $\mathbb{C} \cong \mathbb{R} \oplus \mathbb{R}$. زیرا تابع $\varphi : \mathbb{C} \longrightarrow \mathbb{R} \oplus \mathbb{R}$ با ضابطه‌ی

$$\varphi(a + ib) = (a, b)$$

یکریختی از $\mathbb{C}$ به $\mathbb{R} \oplus \mathbb{R}$ است. □

مثال ۲.۱.۴. داریم $\mathbb{C}^\times \cong \mathbb{R}^\times_{pos} \times U$، که در آن $U = \{z \in \mathbb{C} \mid |z| = ۱\}$ دایره‌ی واحد و $\mathbb{R}_{pos}$ گروه ضربی مجموعه‌ی اعداد حقیقی مثبت است. در اینجا تابع $\varphi : \mathbb{C}^\times \longrightarrow \mathbb{R}^\times_{pos} \times U$ با ضابطه‌ی

$$\varphi(z) = \left(|z|, \frac{z}{|z|}\right)$$

از $\mathbb{C}^\times$ به $\mathbb{R}^\times_{pos} \times U$ یکریختی است. □

اکنون فرض کنید گروه‌های دلخواه H و K داده شده باشند و گروه $H \times K$ را در نظر بگیرید. فرض کنید

$$\overline{H} = \{(h, ۱) \mid h \in H\} = H \times \{۱\}, \quad \overline{K} = \{(۱, k) \mid k \in K\} = \{۱\} \times K.$$

در این صورت $\overline{H}$ و $\overline{K}$ زیرگروه‌های $H \times K$ هستند و $\overline{H} \cong H$ و $\overline{K} \cong K$. در واقع توابع $\iota_۱ : H \longrightarrow H \times K$، با $\iota_۱(h) = (h, ۱)$ برای هر $h \in H$ و $\iota_۲ : K \longrightarrow H \times K$، با $\iota_۲(k) = (۱, k)$، برای هر $k \in K$، همریختی‌های یک‌به‌یک هستند و $\iota_۱(H) = \overline{H}$ و $\iota_۲(K) = \overline{K}$. به علاوه هر عضو $a = (h, k) \in H \times K$ به صورت یکتای $a = (h, ۱)(۱, k)$ نوشته می‌شود. هم‌چنین اعضای $\overline{H}$ و $\overline{K}$ تعویض می‌شوند، یعنی اگر $x = (h, ۱) \in \overline{H}$ و $y = (۱, k) \in \overline{K}$، آنگاه $xy = yx$. عکس این مطلب نیز درست است. در واقع اگر G گروهی باشد که دارای دو زیرگروه H و K است طوری که هر عضو $g \in G$ به صورت یکتای $g = hk$ با $h \in H$ و $k \in K$ نوشته شود. اعضای H و K با هم تعویض شوند، آنگاه $G \cong H \times K$. در این حالت گوییم G حاصل‌ضرب مستقیم (داخلی) H و K است و می‌نویسیم $G = H \times K$. برای اثبات مطلب اخیر تابع $\varphi : G \longrightarrow H \times K$ را با ضابطه‌ی

$$\varphi(hk) = (h, k)$$

تعریف می‌کنیم. چون هر عضو $g \in G$ به صورت یکتای $g = hk$ نوشته می‌شود φ خوش تعریف است. به سادگی می‌توان دید φ همریختی یک‌به‌یک و پوشاست. پس حاصل‌ضرب مستقیم داخلی و خارجی به مفهوم یکریختی یکی هستند. توجه کنید که

مثال ۳.۱.۴. در گروه $V_۴ = \{e, a, b, c\}$ داریم $V_۴ = \langle a \rangle \times \langle b \rangle$. □

قضیه ۴.۱.۴. اگر H و K زیرگروه‌های G باشند، آنگاه G حاصل‌ضرب مستقیم H و K است اگر و تنها اگر $H, K \trianglelefteq G$ و $G = HK$ و $H \cap K = \{۱\}$.

اثبات. ابتدا فرض کنید $G = H \times K$. فرض کنید $h \in H$ و $g = ab \in G$، که در آن $a \in H$ و $b \in K$. در این صورت

$$\begin{aligned} g^{-۱}hg &= b^{-۱}a^{-۱}hab \\ &= a^{-۱}hab^{-۱}b \quad \text{(چون عناصر } K, H \text{ تعویض می‌شوند)} \\ &= a^{-۱}ha \in H. \end{aligned}$$

پس $H \trianglelefteq G$. به همین نحو $K \trianglelefteq G$. طبق تعریف حاصل‌ضرب مستقیم داخلی، هر عضو $g \in G$ به صورت (یکتای) $g = hk$، که در آن $h \in H$ و $k \in K$، نوشته می‌شود. از این‌رو $G = HK$. در نهایت فرض کنید $a \in H \cap K$. چون $H \in ۱$ و $K \in ۱$ و $a = ۱a = a۱$، بنا به یکتایی تجزیه‌ی a به حاصل‌ضرب عضوی از H و عضوی از K داریم $a = ۱$. پس $H \cap K = \{۱\}$.
بر عکس فرض کنید $G = HK$، $H, K \trianglelefteq G$، و $H \cap K = \{۱\}$. فرض کنید $h \in H$ و $k \in K$. چون $H \trianglelefteq G$، $k^{-۱}hk \in H$. بنابراین $h^{-۱}k^{-۱}hk \in H$. به علاوه چون $K \trianglelefteq G$، $h^{-۱}k^{-۱}h \in K$ و بنابراین $h^{-۱}k^{-۱}hk \in K$. در نتیجه $h^{-۱}k^{-۱}hk \in H \cap K = \{۱\}$ و $hk = kh$. پس هر عضو H با هر عضو K تعویض می‌شود. حال فرض کنید $g \in G$. طبق فرض

$G = HK$. پس $h \in H$ و $k \in K$ وجود دارند که $g = hk$. باید ثابت کنیم h و k منحصر به فرد هستند. اگر $g = h_۱k_۱$، که در آن $h_۱ \in H$ و $k_۱ \in K$، آن‌گاه $g = hk = h_۱k_۱$. از این‌رو $h_۱^{-۱}h = k_۱k^{-۱} \in H \cap K$. بنابراین $h = h_۱$ و $k = k_۱$. پس هر عضو $g \in G$ به صورت یکتای $g = hk$ نوشته می‌شود. در نتیجه طبق تعریف، $G = H \times K$. □

تعریف حاصل‌ضرب مستقیم (داخلی، خارجی) را می‌توان به تعداد دلخواهی از گروه‌ها تعمیم داد. ابتدا این کار را برای تعداد متناهی انجام می‌دهیم. فرض کنید $G_۱$، $G_۲$، ...، G_k، k گروه دلخواه باشند، حاصل‌ضرب دکارتی $G_۱ \times G_۲ \times \cdots \times G_k$ با عمل ضرب مولفه‌ای به گروه تبدیل می‌شود که آن را حاصل‌ضرب مستقیم (خارجی) $G_۱$، ...، G_k گوییم: برای هر دو عضو دلخواه $(h_۱, \ldots, h_k)$ و $(g_۱, \ldots, g_k)$ از $G_۱ \times \cdots \times G_k$ تعریف می‌کنیم

$$(g_۱, \ldots, g_k)(h_۱, \ldots, h_k) = (g_۱h_۱, \ldots, g_kh_k).$$

عضو بی‌اثر $G_۱ \times \cdots \times G_k$ عبارت است از $(۱_{G_۱}, \ldots, ۱_{G_k})$ و وارون $(g_۱, \ldots, g_k)$ عبارت است از $(g_۱^{-۱}, \ldots, g_k^{-۱})$. هرگاه $G_۱, \ldots, G_k$ همگی گروه‌های جمعی باشند به جای $G_۱ \times \cdots \times G_k$ می‌نویسیم $G_۱ \oplus \cdots \oplus G_k$. به ازای هر i، تابع $\iota_i : G_i \longrightarrow G_۱ \times \cdots \times G_k$ با ضابطه‌ی $\iota(a) = (۱, \ldots, a, \ldots, ۱)$، که در آن a در iامین مولفه است سایر مولفه‌ها صفرند، یک همریختی یک‌به‌یک است؛ که آن را همریختی جادهی مولفه iام گوییم. $\operatorname{Im} \iota_i$ عبارت است از

$$\begin{aligned} \iota_i(G_i) &= \{(g_۱, \ldots, g_k) \in G_۱ \times \cdots \times G_k \mid g_j = ۱, \quad \forall j \neq i\} \\ &= \{۱\} \times \cdots \times \{۱\} \times G_i \times \{۱\} \times \cdots \times \{۱\}. \end{aligned}$$

چون تصویر یک زیرگروه تحت همریختی زیرگروه است، $\iota_i(G)$ زیرگروه $G_۱ \times \cdots \times G_k$ است. به علاوه چون ι_i یک‌به‌یک است داریم $G_i \cong \iota_i(G_i)$. هم‌چنین هر عضو $(g_۱, \ldots, g_k)$ از $G_۱ \times \cdots \times G_k$ به صورت یکتا بر حسب حاصل‌ضرب اعضای $\iota_k(G), \ldots, \iota_۱(G)$ نوشته می‌شود، زیرا

$$(g_۱ \ldots, g_k) = (g_۱, ۱, \ldots, ۱) \cdots (۱, \ldots, ۱, g_k) = \iota_۱(g_۱) \cdots \iota_k(g_k).$$

در نهایت اعضای $\iota_i(G)$ و $\iota_j(G)$ برای $i \neq j$ دوبه‌دو با هم تعویض می‌شوند؛ زیرا اگر $a \in G_i$ و $b \in G_j$، و مثلاً $i < j$، آن‌گاه

$$\begin{aligned} \iota_i(a)\iota_j(b) &= (۱, \ldots, ۱, a, ۱, \ldots, ۱)(۱, \ldots, ۱, b, ۱, \ldots, ۱) \\ &= (۱, \ldots, ۱, a, ۱, \ldots, b, ۱ \ldots, ۱) \\ &= (۱, \ldots, ۱, b, ۱, \ldots, ۱)(۱, \ldots, ۱, a, ۱, \ldots, ۱) \\ &= \iota_j(b)\iota_i(a). \end{aligned}$$

متناظر هر حاصل‌ضرب مستقیم همریختی‌های دیگری موسوم به همریختی‌های تصویر وجود دارند: به ازای هر $i = ۱, ۲, \ldots, k$، تابع $\pi_i : G_۱ \times \cdots \times G_k \longrightarrow G_i$ با ضابطه‌ی $\pi_i(g_۱, \ldots, g_k) = g_i$ یک همریختی پوشاست، که آن را همریختی تصویر روی مولفه‌ی iام گوییم. هسته‌ی π_i عبارت است از

$$\ker \pi_i = \{(g_۱, \ldots, g_k) \in G_۱ \times \cdots \times G_k \mid g_i = ۱\}.$$

حال فرض کنید G گروهی دلخواه باشد. اگر $H_۱$، ...، H_k زیرگروه‌هایی از G باشند که هر عضو $g \in G$ به صورت یکتای $g = a_۱, \ldots a_k$ نوشته شود، که در آن $a_i \in H_i$ و به علاوه عناصر H_i و H_j برای $i \neq j$ دوبه‌دو تعویض شوند، گوییم G حاصل‌ضرب مستقیم داخلی $H_۱$، ...، H_k است و می‌نویسیم $G = H_۱ \times \cdots \times H_k$. توجه کنید در این حالت G با حاصل‌ضرب مستقیم خارجی $H_۱$، ...، H_k یکریخت است. در واقع تابع $\varphi : H_۱ \times \cdots \times H_k \longrightarrow G$ با ضابطه‌ی $\varphi(a_۱, \ldots, a_k) = a_۱ \cdots a_k$ یکریختی است. پس $G \cong H_۱ \times \cdots \times H_k$.

اثبات قضیه‌ی بعد را به عنوان تمرین واگذار می‌کنیم.

قضیه ۵.۱.۴. اگر $H_۱$، ...، H_k زیرگروه‌های G باشند، آنگاه $G = H_۱ \times \cdots \times H_k$ اگر و تنها اگر
(الف) $G = H_۱H_۲ \cdots H_k$.
(ب) برای هر $i = ۱, \ldots, k$، $H_i \trianglelefteq G$.
(ج) برای هر $i = ۱, \ldots, k$، $H_i \cap \left\langle \bigcup_{\substack{j=۱ \\ j \neq i}}^{k} H_j \right\rangle = \{۱\}$.

توجه کنید که اگر G حاصل‌ضرب مستقیم داخلی $H_۱$، ...، H_k باشد، آنگاه H_iها زیرگروه‌های نرمال G هستند. اما حاصل‌ضرب خارجی $H_۱ \times \cdots \times H_k$ شامل هیچ‌کدام از H_i ها نیست، اما به ازای هر i، شامل یک کپی یکریخت با H_i، یعنی $\iota_i(H_i)$ است.
اکنون مطالب فوق را تعمیم می‌دهیم. فرض کنید I یک مجموعه‌ی اندیس و $\{G_i\}_{i \in I}$ خانواده‌ای از گروه‌ها باشد. یادآوری می‌کنیم حاصل‌ضرب دکارتی $\prod_{i \in I} G_i$ عبارت است از مجموعه‌ی همه‌ی دنباله‌های $(a_i)_{i \in I}$ که در آن $a_i \in G_i$ به ازای هر i:

$$\prod_{i \in I} G_i = \{(a_i)_{i \in I} \mid a_i \in G_i, \quad \forall i \in I\}.$$

$\prod_{i \in I} G_i$ تحت عمل ضرب مولفه‌ای

$$(a_i)_{i \in I}(b_i)_{i \in I} = (a_i b_i)_{i \in I}$$

یک گروه است، عضو بی‌اثر آن دنباله $(c_i)_{i \in I}$ است که به ازای هر $i \in I$، $c_i = ۱$. وارون دنباله $(a_i)_{i \in I}$ عبارت است از $(a_i^{-۱})_{i \in I}$.
این گروه را با $\mathrm{Cr}_{i \in I} G_i$ نیز نشان می‌دهیم.
فرض کنید $u = (a_i)_{i \in I}$ دنباله دلخواهی در $\mathrm{Cr}_{i \in I} G_i$ باشد. تکیه‌گاه u را که با $\mathrm{supp}(u)$ نشان می‌دهیم عبارت است از

$$\mathrm{supp}(u) = \{j \in I \mid a_j \neq ۱\}.$$

قضیه ۶.۱.۴. فرض کنید $u = (a_i)_{i \in I}$ و $v = (b_i)_{i \in I}$ دنباله‌های دلخواهی در $\mathrm{Cr}_{i \in I} G_i$ باشند. در این صورت
(الف) $\mathrm{supp}(u) = \mathrm{supp}(u^{-۱})$
(ب) $\mathrm{supp}(uv) \subseteq \mathrm{supp}(u) \cup \mathrm{supp}(v)$
(ج) $\mathrm{supp}(v^{-۱}uv) = \mathrm{supp}(u)$

اثبات. اثبات قضیه بسیار ساده است، در واقع چون $a_j \neq ۱$ اگر و تنها اگر $a_j^{-۱} \neq ۱$. (الف) واضح است. اگر $a_j b_j \neq ۱$، آنگاه یا $a_j \neq ۱$ یا $b_j \neq ۱$. بنابراین (ب) واضح است. در نهایت چون $b_j^{-۱} a_j b_j \neq ۱$ اگر و تنها اگر $a_j \neq ۱$ ، (ج) واضح است. □

مجموعه‌ی همه‌ی دنباله‌های در $\mathrm{Cr}_{i \in I} G_i$ با تکیه‌گاه متناهی را با $\mathrm{Dr}_{i \in I} G_i$ نشان می‌دهیم:

$$\mathrm{Dr}_{i \in I} G_i = \{(a_i)_{i \in I} \in \mathrm{Cr}_{i \in I} G_i \mid |\mathrm{supp}((a_i)_{i \in I})| < \infty\}.$$

قضیه‌ی بالا نشان می‌دهد که $\mathrm{Dr}_{i \in I} G_i$ زیرگروه نرمال $\mathrm{Cr}_{i \in I} G_i$ است. $\mathrm{Dr}_{i \in I} G_i$ را حاصل‌ضرب مستقیم (خارجی) خانواده‌ی $\{G_i\}_{i \in I}$ گوییم. در حالتی که G_i ها همگی گروه‌های آبلی و جمعی باشند حاصل‌ضرب مستقیم (خارجی) آن‌ها را با $\oplus_{i \in I} G_i$ نشان می‌دهیم. در این حالت $\oplus_{i \in I} G_i$ یک گروه آبلی و جمعی است. در حالتی که $I = \{۱, ۲, \ldots, n\}$ ، را با $G_۱ \times \cdots \times G_n$ $\mathrm{Cr}_{i \in I} G_i = \mathrm{Cr}_{i=۱}^{n} G_i$ (یا در حالتی که همه‌ی G_i گروه‌ها جمعی و آبلی باشند با $G_۱ \oplus \cdots \oplus G_n$) نشان می‌دهیم.
به ازای هر $j \in I$، تابع $\iota_j : G_j \longrightarrow \mathrm{Dr}_{i \in I} G_i$ با ضابطه‌ی $\iota_j(a) = (a_i)_{i \in I}$، که در آن a در jامین مولفه است، یعنی $a_i = \begin{cases} ۱ & i \neq j \\ a & i = j \end{cases}$، یک همریختی یک‌به‌یک است. ι_j را جادهی مولفه‌ی jام گوییم. چون ι_j یک‌به‌یک است $\iota_j(G_j)$ زیرگروهی از $\mathrm{Dr}_{i \in I} G_i$ و یکریخت با G_j است:

$$G_j \cong \iota_j(G_j) = \{(a_i)_{i \in I} \in \mathrm{Dr}_{i \in I} G_i \mid a_i = ۱, \quad \forall i \neq j\}.$$

در حالتی که $I = \{۱, ۲, \dots, n\}$، داریم

$$G_j \cong \iota_j(G_j) = \{۱\} \times \cdots \times \{۱\} \times G_j \times \{۱\} \times \cdots \times \{۱\}.$$

فرض کنید $(a_i)_{i\in I} \in \iota_j(G_j)$ و $(b_i)_{i\in I} \in \iota_k(G_k)$. پس برای هر $i \neq j$، داریم $a_i = ۱$ و برای هر $i \neq k$ داریم $b_i = ۱$. در نتیجه، به ازای هر $i \in I$، $a_ib_i = b_ia_i$. بنابراین حاصل‌ضرب $(a_i)_{i\in I}$ و $(b_i)_{i\in I}$ تعویض‌پذیر است. پس اعضای $\iota_j(G_j)$ و $\iota_k(G_k)$ برای $j \neq k$ دوبه‌دو با یکدیگر تعویض می‌شوند. به علاوه هر عضو $\mathrm{Dr}_{i\in I}G_i$ به صورت یکتا برحسب اعضای $\iota_j(G_j)$، $j \in I$، نوشته می‌شود. زیرا فرض کنید $(a_i)_{i\in I} \in \mathrm{Dr}_{i\in I}G_i$. در این صورت $j_۱, \dots, j_n \in I$ وجود دارند که اگر $i \notin \{j_۱, \dots, j_n\}$، آن‌گاه $a_i = ۱$. فرض کنید u_{j_k} دنباله‌ای باشد که مولفه‌ی j_kام برابر a_{j_k} و مولفه‌های دیگر برابر ۱ است، یعنی $u_{j_k} = (b_i)_{i\in I}$ و b_i. پس داریم $b_i = \begin{cases} ۱ & i \neq j_k \\ a_{j_k} & i = j_k \end{cases}$

$$(a_i)_{i\in I} = u_{j_۱}u_{j_۲}\cdots u_{j_n}$$

و به وضوح این نحوه‌ی نوشتن $(a_i)_{i\in I}$ برحسب اعضای $\iota_j(G_j)$، $i \in I$ یکتاست.
متناظر حاصل‌ضرب مستقیم همریختی‌هایی موسوم به همریختی‌های تصویر وجود دارند: به ازای هر $j \in I$، تابع $\pi_j : \mathrm{Dr}_{i\in I}G_i \longrightarrow G_j$ با ضابطه‌ی $\pi_j((a_i)_{i\in I}) = a_j$ یک همریختی پوشا است که آن را همریختی تصویر روی مولفه‌ی jام گوییم. توجه کنید:

$$\ker \pi_j = \{(a_i)_{i\in I} \in \mathrm{Dr}_{i\in I}G_i \mid a_j = ۱\}.$$

اکنون فرض کنید G گروهی دلخواه باشد و $\{H_i\}_{i\in I}$ خانواده‌ای از زیرگروه‌های G، طوری که هر عضو $۱ \neq g \in G$ به صورت یکتای $g = a_{j_۱}a_{j_۲}\cdots a_{j_n}$ نوشته شود، که در آن $a_{j_k} \in H_{j_k}$، $a_{j_k} \neq ۱$، $k = ۱, \dots, n$. به علاوه عناصر H_j و H_k برای $j \neq k$ دوبه‌دو تعویض می‌شوند. گوییم G حاصل‌ضرب مستقیم (داخلی) خانواده‌ی $\{H_i\}_{i\in I}$ است. در این حالت تابع $\varphi : \mathrm{Dr}_{i\in I}H_i \longrightarrow G$ با ضابطه‌ی $\varphi((a_i)_{i\in I}) = a_{j_۱}, \dots a_{j_n}$، که در آن برای هر $i \notin \{j_۱, \dots, j_n\}$، $a_i = ۱$،یکریختی است، پس $G \cong \mathrm{Dr}_{i\in I}H_i$. هرگاه G حاصل‌ضرب مستقیم داخلی $\{H_i\}_{i\in I}$ باشد، می‌نویسیم $G = \mathrm{Dr}_{i\in I}H_i$. توجه کنید که اگر G حاصل‌ضرب مستقیم داخلی $\{H_i\}_{i\in I}$ باشد، آن‌گاه H_iها زیرگروه‌های نرمال G هستند. اما حاصل‌ضرب خارجی $\mathrm{Dr}_{i\in I}H_i$ شامل هیچ‌کدام از H_jها نیست، بلکه که به ازای هر j، شامل یک کپی یکریخت با H_j، یعنی $\iota_j(H_j)$ است.

قضیه ۷.۱.۴. اگر $\{H_i\}_{i\in I}$ خانواده‌ای از زیرگروه‌های G باشند، آن‌گاه $G = \mathrm{Dr}_{i\in I}H_i$ اگر و تنها اگر
(الف) $G = \langle \bigcup_{i\in I} H_i \rangle$.
(ب) به ازای هر $i \in I$، $H_i \trianglelefteq G$.
(ج) به ازای هر $j \in I$، $H_j \cap \left\langle \bigcup_{\substack{i\in I \\ i\neq j}} H_j \right\rangle = \{۱\}$.

اثبات. ($\Longleftarrow$) فرض کنید $G = \mathrm{Dr}_{r\in I}H_i$. اگر $h \in H_j$ و $a = a_{j_۱}\cdots a_{j_n} \in G$، که در آن $a_{j_k} \in H_{j_k}$، آن‌گاه چون اعضای H_j و H_k برای $j \neq k$ با یکدیگر تعویض می‌شوند، بدون کم شدن از کلیت می‌توان فرض کرد، مثلاً $a_{j_۱} \in H_j$. حال داریم

$$\begin{aligned} a^{-۱}ha &= a_{j_n}^{-۱}\cdots a_{j_۱}^{-۱}ha_{j_۱}\cdots a_{j_n} \\ &= a_{j_۱}^{-۱}ha_{j_۱}a_{j_۲}^{-۱}a_{j_۲}\cdots a_{j_n}^{-۱}a_{j_n} \\ &= a_{j_۱}^{-۱}ha_{j_۱} \in H_j, \end{aligned}$$

پس $H_j \trianglelefteq G$. طبق تعریف حاصل‌ضرب مستقیم داخلی، هر عضو $a \in G$ به صورت (یکتای) $a = a_{j_۱}\cdots a_{j_n}$، که در آن $a_{j_k} \in H_{j_k}$، نوشته می‌شود، یعنی $G = \langle \bigcup_{i\in I} H_i \rangle$. در نهایت فرض کنید $a \in H_j \cap \left\langle \bigcup_{\substack{i\in I \\ i\neq j}} H_j \right\rangle$. پس $a = a_{j_۱}\cdots a_{j_k}$، که در آن $a_{j_k} \in H_{j_k}$ و $j_k \neq j$. در نتیجه $a^{-۱}a_{j_۱}\cdots a_{j_k} = ۱$ و بنا به یکتایی تجزیه‌ی ۱ به صورت حاصل‌ضرب اعضای $\{H_i\}_{i\in I}$، داریم $a = a_{j_۱} = \cdots = a_{j_k} = ۱$ و $H_j \cap \left\langle \bigcup_{\substack{i\in I \\ i=j}} H_j \right\rangle = \{۱\}$.

($\Longrightarrow$) چون به ازای هر $j \in I$، $H_j \cap \left\langle \bigcup_{\substack{i\in I\\ i\neq j}} H_j \right\rangle = \{۱\}$، به ویژه به ازای هر $i \neq j$ داریم $H_i \cap H_j = \{۱\}$. به علاوه چون H_i و H_j در G نرمال هستند ، نتیجه می‌شود که اعضای H_i و H_j دوبه‌دو با یکدیگر تعویض می‌شوند. حال فرض کنید $۱ \neq a \in G$. بنا به (الف) اعضای $۱ \neq a_{j_k} \in H_{j_k}$، $k = ۱, \ldots, n$ وجود دارند که $a = a_{j_۱} \cdots a_{j_n}$. باید ثابت کنیم این تجزیه یکتاست. فرض کنید $a = b_{i_۱} b_{i_۲} \cdots b_{i_m}$، که در آن $k = ۱, \ldots, m, b_{i_k} \in H_{i_k}$. به سادگی و به استقرا روی $\max\{m, n\}$ با استفاده از (ج) می‌توان ثابت کرد $m = n$ و پس از تعویض اندیس‌ها $b_{i_k} = a_{i_k}$. جزئیات کار را به خواننده واگذار می‌کنیم. □

تمرین‌ها

۱. اگر $m, n \in \mathbb{N}$ و $\gcd\{m, n\} = ۱$، ثابت کنید $C_m \times C_n \cong C_{mn}$.

۲. ثابت کنید $\mathbb{Q}^\times \cong \mathbb{Q}^\times_{pos} \times C_۲$.

۳. فرض کنید $n > ۱$ عدد صحیح و $n = p_۱^{m_۱} p_۲^{m_۲} \cdots p_k^{m_k}$ تجزیه n به عوامل اول باشد. اگر $k > ۱$، نشان دهید $C_n \cong C_{p_۱^{m_۱}} \times \cdots \times C_{p_k^{m_k}}$. در این حالت C_n را تجزیه پذیر گوییم. نشان دهید C_{p^m} تجزیه پذیر نیست، یعنی به حاصل‌ضرب مستقیم دو زیر گروه نابدیهی خود تجزیه نمی‌شود.

۴. ثابت کنید مرکز $A_۴ \times \mathbb{Z}_۲$ کاملاً پایا نیست.

۵. نشان دهید $\mathrm{Aut}\,(\mathbb{Z} \oplus \mathbb{Z}_۴) \cong D_۸$.

۶. فرض کنید n عدد صحیح مثبت و F یک میدان باشد، طوری که هر $a \in F$ ریشه‌ی nام منحصر بفرد داشته باشد، یعنی به ازای هر $h \in F$، عضو یکتای $b \in F$ وجود داشته باشد که $b^n = a$. ثابت کنید $\mathrm{GL}_n(F) \cong F^\times \times \mathrm{SL}_n(F)$، که در آن $\mathrm{SL}_n(F)$ زیر گروه $\mathrm{GL}_n(F)$ متشکل از همه‌ی ماتریس‌های با دترمینان ۱ است. (به ویژه این مطلب برای $F = \mathbb{R}$ و n فرد درست است.)

۷. فرض کنید F یک میدان و n عدد صحیح مثبت باشد. نشان دهید مجموعه‌ی H متشکل از همه‌ی ماتریس‌های وارون پذیر قطری $n \times n$ با درایه‌های در F زیرگروهی از $\mathrm{GL}_n(F)$ است و $H \cong \underbrace{F^\times \times \cdots \times F^\times}_{n \text{ بار}}$.

۸. فرض کنید $G = H \times K$. ثابت کنید G حل‌پذیر است اگر و تنها اگر H و K حل‌پذیر باشند.

۹. فرض کنید $G = H \times K$. ثابت کنید
(الف) یک همریختی یک‌به‌یک از $(\mathrm{Aut}\, H) \times (\mathrm{Aut}\, K)$ به $\mathrm{Aut}\, G$ وجود دارد.
(ب) اگر H و K در G مشخصه باشند، آنگاه $(\mathrm{Aut}\, H) \times (\mathrm{Aut}\, K) \cong \mathrm{Aut}\, G$.
(ج) اگر همریختی نابدیهی از H به K و از K به H وجود نداشته باشد، آنگاه $(\mathrm{Aut}\, H) \times (\mathrm{Aut}\, K) \cong \mathrm{Aut}\, G$.

۱۰. فرض کنید $n > ۱$ عدد صحیح و $n = p_۱^{m_۱} p_۲^{m_۲} \cdots p_k^{m_k}$ تجزیه‌ی n به عوامل اول باشد. نشان دهید
(الف) $\mathbb{Z}_n \cong \mathbb{Z}_{p_۱^{m_۱}} \times \cdots \times \mathbb{Z}_{p_k^{m_k}}$. (ب) $\mathbb{Z}_n^\times \cong \mathbb{Z}^\times_{p_۱^{m_۱}} \times \cdots \times \mathbb{Z}^\times_{p_k^{m_k}}$.

۱۱. فرض کنید G یک گروه آبلی متناهی باشد. نشان دهید زیرگروه‌های $H_۱$، $H_۲$، ...، H_k از G وجود دارند که $G = H_۱ \times H_۲ \times \cdots \times H_k$.

۱۲. اگر $G = H_۱ \times H_۲ \times \cdots \times H_r$ یک حاصل‌ضرب مستقیم داخلی باشد و برای هر $i = ۱, ۲, \ldots r$، $K_i \leq H_i$ و $K_i \trianglelefteq G$، نشان دهید $K = K_۱ K_۲ \cdots K_r$ یک حاصل‌ضرب مستقیم است و

$$\frac{G}{K} = \frac{H_۱}{K_۱} \times \frac{H_۲}{K_۲} \times \cdots \times \frac{H_r}{K_r}.$$

این مطلب را برای حاصل‌ضرب دکارتی (و حاصل‌ضرب مستقیم) یک خانواده‌ی دلخواه از گروه‌ها تعمیم دهید.

۱۳. فرض کنید $G = G_۱ \times G_۲ \times \cdots \times G_r$ یک حاصل‌ضرب مستقیم داخلی باشد. اگر $G = H_۱ H_۲ \cdots H_r$ که در آن $H_i \leq G_i$، $i = ۱, ۲, \ldots, r$، آنگاه $H_i = G_i$، $i = ۱, ۲, \ldots, r$.

۱۴. نشان دهید $Z(G_۱ \times G_۲ \times \cdots \times G_r) = Z(G_۱) \times Z(G_۲) \times \cdots \times Z(G_r)$.

۱۵. نشان دهید (الف) $\mathrm{Aut}\,(\underbrace{\mathbb{Z}\times\cdots\times\mathbb{Z}}_{n\text{ بار}})\cong \mathrm{GL}_n(\mathbb{Z})$.

(ب) $\mathrm{Aut}\,(\underbrace{\mathbb{Z}_{p^m}\times\cdots\times\mathbb{Z}_{p^m}}_{n\text{ بار}})\cong \mathrm{GL}_n(\mathbb{Z}_{p^m})$.

۲.۴ حاصل‌ضرب نیم‌مستقیم

فرض کنید H و K دو زیرگروه نرمال گروه G باشند. اگر $G=HK$ و $H\cap K=\{1\}$، آنگاه $G=H\times K$ حاصل‌ضرب مستقیم (داخلی) H و K است. اگر شرایط فوق را اندکی ضعیف‌تر کنیم نوع دیگری از حاصل‌ضرب گروه‌ها، موسوم به حاصل‌ضرب نیم‌مستقیم (داخلی) به‌دست می‌آید. آن وقتی است که یکی از زیرگروه‌های H یا K لزوماً نرمال نیستند.

تعریف ۱.۲.۴. فرض کنید G گروه باشد و $H,K\leq G$، G را حاصل‌ضرب نیم‌مستقیم (داخلی) H توسط K گوییم و می‌نویسیم $G=H\rtimes K$، هرگاه

(الف) $H\trianglelefteq G$

(ب) $H\cap K=\{1\}$

(ج) $G=HK$

اگر G حاصل‌ضرب نیم‌مستقیم H توسط K باشد، آنگاه چون $G=HK$، هر عضو $g\in G$ به صورت $g=hk$ نوشته می‌شود، که در آن $h\in H$ و $k\in K$. این طریقه‌ی نوشتن یکتاست، زیرا $H\cap K=\{1\}$. بنابراین تا این‌جا حاصل‌ضرب مستقیم و نیم‌مستقیم فرقی ندارند. اما تفاوت آن‌ها در چیست؟ در حاصل‌ضرب مستقیم اعضای H و K با یکدیگر تعویض می‌شوند، اما این مطلب لزوماً برای حاصل‌ضرب نیم‌مستقیم برقرار نیست. اگر $G=H\times K$، حاصل‌ضرب مستقیم (داخلی) H و K باشد، آنگاه عمل ضرب در G به صورت زیر است

$$(h_1k_1)(h_2k_2)=(h_1h_2)(k_1k_2).$$

اما اگر $G=H\rtimes K$ عمل ضرب در G به چه صورت است؟ برای یافتن نحوه‌ی ضرب از نرمال بودن H در G استفاده می‌کنیم:

$$(h_1k_1)(h_2k_2)=(h_1k_1)(h_2k_1^{-1}k_1k_2)=h_1(k_1h_2k_1^{-1})k_1k_2=h_3k_3,$$

که در آن $h_3=h_1k_1h_2k_1^{-1}\in H$ و $k_3=k_1k_2\in K$.

مثال ۲.۲.۴. نشان دهید گروه دووجهی D_{2n} حاصل‌ضرب نیم‌مستقیم دو زیرگروه است.

حل داریم $D_{2n}=\langle\rho,\varepsilon\rangle$ که در آن $\rho^n=\varepsilon^2=1$، و $\varepsilon\rho=\rho^{-1}\varepsilon$. چون $\langle\rho\rangle\trianglelefteq D_{2n}$، $\langle\rho\rangle\cap\langle\varepsilon\rangle=\{1\}$ و

$$\langle\rho\rangle\langle\varepsilon\rangle=\{1,\rho,\cdots,\rho^{n-1},\varepsilon,\varepsilon\rho,\cdots,\varepsilon\rho^{n-1}\}=D_{2n}$$

پس D_{2n} حاصل‌ضرب نیم‌مستقیم $\langle\rho\rangle$ توسط $\langle\varepsilon\rangle$ است. □

همانند مثال فوق گروه دووجهی نامتناهی $D_\infty=\langle\tau,\varepsilon\rangle$، حاصل‌ضرب نیم‌مستقیم $\langle\tau\rangle$ توسط $\langle\varepsilon\rangle$ است.

مثال ۳.۲.۴. چون $A_3\trianglelefteq S_3$ و $A_3\cap\langle(1\ 2)\rangle=\{(1)\}$ و $S_3=A_3\langle(1\ 2)\rangle$، پس S_3 حاصل‌ضرب نیم‌مستقیم A_3 توسط $\langle(1\ 2)\rangle$ است. □

حال فرض کنید $G=H\rtimes K$ حاصل‌ضرب نیم‌مستقیم (داخلی) H توسط K باشد. به ازای هر $k\in K$، قرار می‌دهیم $\varphi_k=\tau_k|_H$، که در آن τ_k خودریختی داخلی القا شده توسط k است. چون $H\trianglelefteq G$، داریم $\tau_k(H)=H$. پس $\varphi_k\in\mathrm{Aut}\,H$ و تابع $\varphi:K\longrightarrow\mathrm{Aut}\,H$ با ضابطه‌ی $\varphi(k)=\varphi_k$، به ازای هر $k\in K$، خوش تعریف است. به ازای هر $a,b\in K$ و هر $h\in H$ داریم

$$\varphi_{ab}(h)=(ab)h(ab)^{-1}=abhb^{-1}a^{-1}=\varphi_a\left(bhb^{-1}\right)=\varphi_a(\varphi_b(h)).$$

بنابراین به ازای هر $a, b \in K$ داریم

$$\varphi(ab) = \varphi_{ab} = \varphi_a\varphi_b = \varphi(a)\varphi(b).$$

پس φ همریختی است. در نتیجه ثابت کردیم که اگر $G = H \rtimes K$ حاصل‌ضرب نیم‌مستقیم (داخلی) H توسط K باشد، آنگاه یک همریختی $\varphi : K \longrightarrow \operatorname{Aut} H$ وجود دارد. در این حالت عمل ضرب در G را می‌توان به صورت زیر نوشت:

$$(h_1k_1)(h_2k_2) = (h_1k_1h_2k_1^{-1})(k_1k_2) = (h_1\varphi_{k_1}(h_2))(k_1k_2).$$

پس عمل ضرب در $G = HK$ تنها بستگی به عمل ضرب در H، عمل ضرب در K و همریختی φ بستگی دارد. بنابراین این عمل را می‌توان بر حسب H و K توصیف کرد. با استفاده از این تعبیر حاصل‌ضرب نیم‌مستقیم داخلی می‌توانیم حاصل‌ضرب نیم‌مستقیم خارجی را تعریف کنیم. فرض کنید H و K دو گروه دلخواه باشند و $\varphi : K \longrightarrow \operatorname{Aut} H$ یک همریختی باشد. فرض کنید G مجموعه‌ی همه‌ی زوج‌های مرتب (h, k) باشد که در آن $h \in H$ و $k \in K$. با الهام از عمل ضرب در حاصل‌ضرب نیم‌مستقیم داخلی، عمل ضرب در G را به صورت زیر تعریف می‌کنیم:

$$(h_1, k_1)(h_2, k_2) = (h_1\varphi_{k_1}(h_2), k_1k_2),$$

که در آن برای سادگی، تصویر $k \in K$ تحت φ را با φ_k نشان داده‌ایم. این حاصل‌ضرب، G را به یک گروه با مرتبه‌ی $|G| = |H||K|$ تبدیل می‌کند. برای اثبات شرکت‌پذیری به طریق زیر عمل می‌کنیم: به ازای هر $(a, x), (b, y), (c, z) \in G$ داریم

$$\begin{aligned}
[(a,x)(b,y)](c,z) &= (a\varphi_x(b), xy)(c,z) \\
&= (a\varphi_x(b)\varphi_{xy}(c), xyz) \\
&= (a\varphi_x(b)\varphi_x(\varphi_y(c), xyz) \\
&= (a\varphi_x(b\varphi_y(c)), xyz) \\
&= (a,x)(b\varphi_y(c), yz) \\
&= (a,x)[(b,y)(c,z)].
\end{aligned}$$

عضو بی‌اثر G عبارت است از $(۱, ۱)$، زیرا

$$\begin{aligned}
(h,k)(۱,۱) &= (h\varphi_k(۱), k۱) = (h۱, k) = (h,k) \\
(۱,۱)(h,k) &= (۱\varphi_۱(h), ۱k) = (۱h, k) = (h,k).
\end{aligned}$$

فرض کنید $(a, x) \in G$ وارون (h, k) باشد، داریم

$$(۱, ۱) = (h,k)(a,x) = (h\varphi_k(a), kx).$$

بنابراین $h\varphi_k(a) = ۱$ و $kx = ۱$. پس $x = k^{-۱}$ و $\varphi_k(a) = h^{-۱}$ و بنابراین $a = \varphi_{k^{-۱}}(h^{-۱})$. در نتیجه وارون (h, k) عبارت است از

$$(\varphi_{k^{-۱}}(h^{-۱}), k^{-۱}).$$

گروه G را که هم اکنون ساخته شد، حاصل‌ضرب نیم‌مستقیم (خارجی) H توسط K نسبت به φ گوییم و با $G = H \rtimes_\varphi K$ نشان می‌دهیم. در حالتی که بیم ابهام نباشد. از نوشتن φ صرف‌نظر می‌کنیم و می‌نویسیم $G = H \rtimes K$.
حاصل‌ضرب نیم‌مستقیم داخلی و خارجی چه ارتباطی با یکدیگر دارند؟ قضیه‌ی بعد این مطلب را روشن می‌کند.

قضیه ۴.۲.۴. فرض کنید H و K دو گروه و $\varphi : K \longrightarrow \operatorname{Aut} H$ همریختی باشد. اگر $G = H \rtimes_\varphi K$ حاصل‌ضرب نیم‌مستقیم خارجی H توسط K نسبت به φ باشد، آنگاه زیرگروه‌های $\overline{H}$ و $\overline{K}$ از G وجود دارند که G حاصل‌ضرب مستقیم داخلی $\overline{H}$ توسط $\overline{K}$ است.

اثبات. قرار می‌دهیم $\overline{H} = \{(h, ۱) \mid h \in H\}$ و $\overline{K} = \{(۱, k) \mid k \in K\}$. به ازای هر $a, b \in H$ داریم

$$(a, ۱)(b, ۱) = (a\varphi_۱(b), ۱) = (ab, ۱)$$

و به ازای هر $x, y \in K$ داریم

$$(۱, x)(۱, y) = (۱\varphi_x(۱), xy) = (۱, xy).$$

از روابط فوق نتیجه می‌شود که $\overline{H}$ و $\overline{K}$ زیرگروه‌های G هستند. به علاوه، داریم $H \cong \overline{H}$ و $K \cong \overline{K}$. هم‌چنین توجه کنید که $\overline{H} \cap \overline{K} = \{(۱, ۱)\}$ و $G = \overline{H}\,\overline{K}$. حال ثابت می‌کنیم $\overline{H} \trianglelefteq G$. داریم

$$\begin{aligned}(۱, k)(h, ۱)(۱, k^{-۱}) &= [(۱, k)(h, ۱)](۱, k^{-۱}) \\ &= (\varphi_k(h), k)(۱, k^{-۱}) \\ &= (\varphi_k(h)\varphi_k(۱), kk^{-۱}) \\ &= (\varphi_k(h), ۱) \in \overline{H}.\end{aligned}$$

پس $\overline{H}$ در G نرمال است. از این‌رو G حاصل‌ضرب مستقیم (داخلی) $\overline{H}$ توسط $\overline{K}$ است. □

فرض کنید $G = H \rtimes_\varphi K$ حاصل‌ضرب نیم‌مستقیم (خارجی) H توسط K نسبت به φ باشد. در قضیه‌ی ۴.۲.۴، دیدیم اگر $\overline{H} = \{(h, ۱) \mid h \in G\}$ و $\overline{K} = \{(۱, k) \mid k \in K\}$، آنگاه $H \cong \overline{H}$ و $K \cong \overline{K}$ و G حاصل‌ضرب مستقیم $\overline{H}$ توسط $\overline{K}$ است. اگر H را با $\overline{H}$ و K را با $\overline{K}$ یکی در نظر بگیریم و G را به صورت

$$G = \{hk \mid h \in H,\ \ k \in K\}$$

بنویسیم، آنگاه $G \trianglelefteq H$، و $H \cap K = \{۱\}$. هم‌چنین به ازای هر $h \in H$، هر $k \in K$ داریم $khk^{-۱} = \varphi_k(h)$. پس φ_k تحدید خودریختی داخلی القا شده توسط k به H است.
حاصل‌ضرب نیم‌مستقیم راهی مناسب برای تعریف گروه‌های جدید است:

مثال ۵.۲.۴. فرض کنید H یک گروه آبلی دلخواه و هم‌چنین $K = \langle x\rangle \cong C_۲$ یک گروه دوری مرتبه‌ی ۲ باشد. همریختی $\varphi : K \longrightarrow \operatorname{Aut} H$ را با ضابطه‌ی $\varphi(x) = \varphi_x$، $\varphi_x(h) = h^{-۱}$ تعریف می‌کنیم. (چون H آبلی است $\varphi_x : H \longrightarrow H$ با ضابطه‌ی $\varphi_x(h) = h^{-۱}$ خودریختی از H است). فرض کنید $G = H \rtimes_\varphi K$. آنگاه H زیرگروه با شاخص ۲ در G است، زیرا $|G : H| = \dfrac{|G|}{|H|} = \dfrac{|H||K|}{|H|} = |K| = ۲$. به علاوه به ازای هر $h \in H$،

$$xhx^{-۱} = h^{-۱}$$

به ویژه اگر $H = \langle y\rangle$ و $O(y) = n$، آنگاه $G = HK = \langle x, y\rangle$، و $x^۲ = ۱$، $xyx^{-۱} = y^{-۱}$. بنابراین $G \cong D_{۲n}$. اگر $H = \langle y\rangle$ و $O(y) = \infty$، آنگاه $G \cong D_\infty$. □

مثال فوق را می‌توان تعمیم داد:

مثال ۶.۲.۴. فرض کنید H گروه آبلی دلخواه و $K = \langle x\rangle \cong C_{۲n}$ یک گروه دوری مرتبه‌ی $۲n$ باشد. همریختی $\varphi : K \longrightarrow \operatorname{Aut} H$ را با $\varphi_x(h) = h^{-۱}$ تعریف می‌کنیم. در $G = H \rtimes_\varphi K$ به ازای هر $h \in H$ داریم $xhx^{-۱} = h^{-۱}$ و $x^۲hx^{-۲} = h$. پس $x^۲ \in Z(G)$. به ویژه اگر $H = \langle y\rangle$ و $O(y) = ۳$ و $K \cong C_۴$، آنگاه G یک گروه ناآبلی مرتبه‌ی ۱۲ است، که با $A_۴$ یا $D_{۱۲}$ یکریخت نیست (زیرا G یک زیرگروه نرمال مرتبه‌ی ۳ دارد ولی $A_۴$ و $D_{۱۲}$ زیرگروه نرمال مرتبه‌ی ۳ ندارند). □

تمرین‌ها

۱. نشان دهید گروه کواترنیونی Q_8 حاصل‌ضرب نیم‌مستقیم دو زیرگروه سره‌ی خود نیست.

۲. فرض کنید $G = H \rtimes_\varphi K$. نشان دهید $G = H \times K$ اگر و تنها اگر $\varphi : K \longrightarrow \operatorname{Aut} H$ همریختی بدیهی باشد، یعنی $\varphi(k) = \mathrm{id}_H$، به ازای هر $k \in K$.

۳. فرض کنید H گروه باشد و $K = \operatorname{Aut} H$؛ همریختی همانی $\varepsilon : K \longrightarrow \operatorname{Aut} H$ را با $\varepsilon(\alpha) = \alpha$ در نظر بگیرید. حاصل‌ضرب نیم‌مستقیم H توسط $K = \operatorname{Aut} H$ نسبت به ε را هولومورف H گوییم و با $\operatorname{Hol} H = H \rtimes_\varepsilon \operatorname{Aut} H$ نشان می‌دهیم.
(الف) عمل ضرب در $\operatorname{Hol} H$ را تشریح کنید.
(ب) نشان دهید $H \trianglelefteq \operatorname{Hol} H$.
(ج) نشان دهید $\operatorname{Hol} C_3 \cong S_3$

۴. فرض کنید H یک گروه و K زیرگروهی از $\operatorname{Aut} H$ باشد. همریختی شمولی $i : K \longrightarrow \operatorname{Aut} H$ را با $i(\alpha) = \alpha$ در نظر بگیرید. حاصل‌ضرب نیم‌مستقیم $H \rtimes_i K$، H توسط K نسبت به i را هولومورف نسبی H گوییم.
(الف) نشان دهید $H \trianglelefteq H \rtimes_i K \leq \operatorname{Hol} H$.
(ب) اگر A گروه آبلی با عضوی مثل b باشد که $b^2 \neq 1$. خودریختی $\eta \in \operatorname{Aut} A$ با ضابطه‌ی $\eta(a) = a^{-1}$ را در نظر می‌گیریم. در این صورت $\eta^2 = 1$، $\eta \neq 1$. هولومورف نسبی $A \langle \eta \rangle$ از A را گروه دووجهی تعمیم یافته گوییم و با $\operatorname{Dih} A$ نشان می‌دهیم. ثابت کنید اگر $n \geq 3$، $\operatorname{Dih} C_n \cong D_{2n}$ و $\operatorname{Dih} \mathbb{Z} \cong D_\infty$.

۵. فرض کنید A گروه آبلی باشد و به ازای یک $b \in A$، $b^2 \neq 1$. قرار دهید $D = \operatorname{Dih} A$. نشان دهید
(الف) مرتبه‌ی هر عضو $D - A$ برابر ۲ است.
(ب) $Z(D) = \{a \in A \mid a^2 = 1\}$.
(ج) $A\mathrm{char}\, D$.
(د) $\operatorname{Aut} D \cong \operatorname{Hol} A$.

۶. فرض کنید $G = H \rtimes_\varphi K$. نشان دهید
(الف) $C_K(H) = \ker \varphi$.
(ب) $C_H(K) = N_H(K)$.

۷. فرض کنید $G = \operatorname{Hol}(C_2 \times C_2)$.
(الف) ثابت کنید $\operatorname{Aut}(C_2 \times C_2) \cong S_3$ و نتیجه بگیرید $|G| = 24$.
(ب) نشان دهید $G \cong S_4$.

۸. آیا S_n حاصل‌ضرب نیم‌مستقیم دو زیرگروه سره‌ی خودش است؟

فصل ۵

عمل گروه و قضایای سیلو

۱.۵ عمل گروه روی مجموعه

یکی از مفاهیم مهم در نظریه‌ی گروه‌ها مفهوم عمل یک گروه G بر یک ساختار جبری است، که نمایش G نسبت به آن ساختار نامیده می‌شود و آن وقتی است که یک همریختی از G به گروه خودریختی‌های آن ساختار وجود داشته باشد. در حالتی که X یک مجموعه‌ی دلخواه باشد می‌توان X را به عنوان یک ساختار جبری بدون هیچ عملی در نظر گرفت. در این حالت گروه خودریختی‌های X همان مجموعه‌ی توابع یک‌به‌یک و پوشا از X به X یعنی S_X است. گوییم G روی مجموعه‌ی X (از چپ) عمل می‌کند، هرگاه یک همریختی $\varphi : G \longrightarrow S_X$ وجود داشته باشد φ را یک نمایش جایگشتی G گوییم.
گوییم G روی گروه H عمل می‌کند هرگاه همریختی $\varphi : G \longrightarrow \operatorname{Aut} H$ وجود داشته باشد. گوییم G روی فضای برداری V عمل می‌کند هرگاه همریختی $\varphi : G \longrightarrow \mathrm{GL}(V)$ وجود داشته باشد، φ را نمایش خطی G نامیم. حالت اخیر، تعریف پایه‌ی شاخه‌ای مهم از نظریه‌ی گروه‌ها موسوم به نظریه‌ی نمایش گروه‌ها است.
در اینجا نمایش جایگشتی گروه‌ها را بررسی می‌کنیم. فرض کنید X یک مجموعه‌ی دلخواه، G یک گروه، و $\varphi : G \longrightarrow S_X$ یک نمایش جایگشتی G باشد. چون φ همریختی است، به ازای هر g_1 و g_2 در G داریم

$$\varphi(g_1 g_2) = \varphi(g_1)\varphi(g_2).$$

پس به ازای هر $x \in X$ خواهیم داشت

$$\varphi(g_1 g_2)(x) = \varphi(g_1)(\varphi(g_2)(x)).$$

معمولاً از نوشتن φ صرف‌نظر می‌کنیم و می‌نویسیم

$$(g_1 g_2) \cdot x = g_1 \cdot (g_2 \cdot x).$$

هم‌چنین چون $\varphi(1) = \mathrm{id}_X$ داریم

$$\varphi(1)(x) = \mathrm{id}_X(x) = x,$$

یعنی برای هر $x \in X$، $1 \cdot x = x$. بنابراین اگر همریختی $\varphi : G \longrightarrow S_X$ وجود داشته باشد، آن‌گاه تابع $\cdot : G \times X \longrightarrow X$ وجود دارد که به ازای هر $x \in X$ و به ازای هر $g_1, g_2 \in G$،

$$(g_1 g_2) \cdot x = g_1(g_2 \cdot x), \qquad 1 \cdot x = x.$$

بر عکس اگر تابع

$$\begin{aligned} \cdot : G \times X &\longrightarrow X \\ (g, x) &\mapsto g \cdot x \end{aligned}$$

با دو خاصیت فوق وجود داشته باشد، آنگاه نگاشت $\rho : G \longrightarrow S_X$ با ضابطه‌ی $\rho(g) = \rho_g$ که در آن $\rho_g : X \longrightarrow X$، $\rho_g(x) = g \cdot x$ یک همریختی است. اولاً $\rho_g \in S_X$، زیرا

$$\begin{aligned} \rho_g(x) = \rho_g(y) &\implies g \cdot x = g \cdot y \\ &\implies g^{-1} \cdot (g \cdot x) = g^{-1} \cdot (g \cdot y) \\ &\implies (g^{-1}g) \cdot x = (g^{-1}g) \cdot y \\ &\implies 1 \cdot x = 1 \cdot y \\ &\implies x = y, \end{aligned}$$

یعنی ρ_g یک‌به‌یک است. ρ_g پوشا نیز هست، زیرا به ازای هر $y \in X$ داریم

$$\rho_g\left(g^{-1} \cdot y\right) = g \cdot \left(g^{-1} \cdot y\right) = \left(gg^{-1}\right) \cdot y = 1 \cdot y = y.$$

ثانیاً به ازای هر $g_1, g_2 \in G$، داریم

$$\begin{aligned} \forall x \in X, \ (\rho_{g_1}\rho_{g_2})(x) &= \rho_{g_1}(\rho_{g_2}(x)) \\ &= \rho_{g_1}(g_2 \cdot x) \\ &= g_1 \cdot (g_2 \cdot x) \\ &= (g_1 g_2) \cdot x \\ &= \rho_{g_1 g_2}(x). \end{aligned}$$

بنابراین $\rho_{g_1 g_2} = \rho_{g_1}\rho_{g_2}$، یعنی

$$\rho(g_1 g_2) = \rho_{g_1 g_2} = \rho_{g_1}\rho_{g_2} = \rho(g_1)\rho(g_2)$$

و ρ همریختی است.

مثال ۱.۱.۵. فرض کنید G گروه و X مجموعه‌ی دلخواهی باشد. برای هر $g \in G$ و هر $x \in X$ تعریف می‌کنیم $g \cdot x = x$. این تعریف منجر به عمل گروه G روی X می‌شود که آن را عمل بدیهی گوییم. نمایش جایگشتی متناظر آن $\rho : G \longrightarrow S_X$ است که در آن $\rho(g) = \mathrm{id}_X$ به ازای هر $g \in G$. □

مثال ۲.۱.۵. اگر X یک مجموعه باشد، S_X به طور طبیعی روی X به صورت زیر عمل می‌کند: برای هر $\alpha \in S_X$ و برای هر $x \in X$ تعریف می‌کنیم $\alpha \cdot x = \alpha(x)$. نمایش جایگشتی متناظر آن همریختی همانی $\mathrm{id} : S_X \longrightarrow S_X$ (به ازای هر $\alpha \in S_X$، $\mathrm{id}(\alpha) = \alpha$) است. □

عمل G روی X را صادق گوییم هرگاه همریختی متناظر آن یک‌به‌یک باشد. $\ker\varphi$ را هسته‌ی عمل گوییم. ملاحظه کنید طبق قضیه‌ی اول یکریختی $G/\ker\varphi \cong \mathrm{Im}\,\varphi \leq S_X$. قبل از این‌که مثال‌های بیشتری بیاوریم قدری از خواص عمل گروه را می‌یابیم. فرض کنید گروه G روی مجموعه‌ی X (از چپ) عمل کند. رابطه‌ی $\sim$ را روی X چنین تعریف می‌کنیم

$$x \sim y \iff \exists g \in G, \quad y = g \cdot x.$$

این رابطه یک رابطه‌ی هم‌ارزی است. چون $1 \cdot x = x$، $x \sim x$ برای هر $x \in X$، یعنی $\sim$ بازتابی است. حال اگر $x \sim y$، آنگاه به ازای یک $g \in G$ داریم $y = g \cdot x$. در نتیجه

$$x = 1 \cdot x = (g^{-1}g) \cdot x = g^{-1} \cdot (g \cdot x) = g^{-1} \cdot y.$$

پس $x \sim y$، یعنی $\sim$ متقارن است. در نهایت اگر $x \sim y$ و $y \sim z$، آنگاه به ازای $g_۱, g_۲ \in G$ داریم $y = g_۱ \cdot x$ و $z = g_۲ \cdot y$. در نتیجه

$$z = g_۲ \cdot y = g_۲ \cdot (g_۱ \cdot x) = (g_۲ g_۱) \cdot x.$$

یعنی $x \sim z$. بنابراین $\sim$ ترایا است.
رده‌ی هم‌ارزی شامل x را مدار x گوییم و با $\mathrm{orb}_G(x)$ (یا $\bar{x}$) نشان می‌دهیم. بنابراین

$$\begin{aligned} \mathrm{orb}_G(x) &= \{y \in X \mid x \sim y\} \\ &= \{y \in X \mid \exists g \in G, \quad y = g \cdot x\} \\ &= \{g \cdot x \mid g \in G\}. \end{aligned}$$

اکنون می‌خواهیم $|\mathrm{orb}_G(x)|$ را محاسبه کنیم. برای این منظور باید مجموعه‌ی اعضای G که x را ثابت نگه می‌دارند را در نظر بگیریم. این مجموعه را با $\mathrm{stab}_G(x)$ یا G_x نشان می‌دهیم و ثابت ساز x در G نامیم:

$$\mathrm{stab}_G(x) = \{g \in G \mid g \cdot x = x\}.$$

$\mathrm{stab}_G(x)$ زیرگروهی از G است. چون $۱ \cdot x = x$، $۱ \in \mathrm{stab}_G(x)$. هم‌چنین اگر $g_۱, g_۲ \in \mathrm{stab}_G(x)$، آنگاه

$$(g_۱ g_۲) \cdot x = g_۱ \cdot (g_۲ \cdot x) = g_۱ \cdot x = x$$

و

$$g_۱ \cdot x = x \Longrightarrow g_۱^{-۱} \cdot (g_۱ \cdot x) = g_۱^{-۱} \cdot x \Longrightarrow ۱ \cdot x = g^{-۱} \cdot x \Longrightarrow x = g_۱^{-۱} \cdot x.$$

پس $g_۱ g_۲$ و $g_۱^{-۱}$ هر دو در $\mathrm{stab}_G(x)$ قرار دارند. اکنون توجه کنید که

$$\begin{aligned} g \in \ker \varphi &\iff \varphi(g) = \mathrm{id}_X \\ &\iff \forall x \in X, \ \ \varphi(g)(x) = \mathrm{id}_X(x) \\ &\iff \forall x \in X, \ \ g \cdot x = x \\ &\iff \forall x \in X, \ \ g \in \mathrm{stab}_G(x) \\ &\iff g \in \bigcap_{x \in X} \mathrm{stab}_G(x). \end{aligned}$$

بنابراین $\ker \varphi = \bigcap_{x \in X} \mathrm{stab}_G(x)$.
حال نشان می‌دهیم $|\mathrm{orb}_G(x)| = |G : \mathrm{stab}_G(x)|$. اگر $T = \{gG_x \mid g \in G\}$ مجموعه‌ی هم مجموعه‌های چپ $G_x = \mathrm{stab}_G(x)$ در G باشد، تابع $f : \mathrm{orb}_G(x) \longrightarrow T$ را با ضابطه‌ی $f(g \cdot x) = gG_x$ تعریف می‌کنیم. f خوش تعریف و یک‌به‌یک است زیرا

$$\begin{aligned} g_۱ \cdot x = g_۲ \cdot x &\iff x = (g_۱^{-۱} g_۲) \cdot x \\ &\iff g_۱^{-۱} g_۲ \in G_x \\ &\iff g_۲ G_x = g_۱ G_x \\ &\iff f(g_۲ \cdot x) = f(g_۱ \cdot x). \end{aligned}$$

به وضوح f پوشا نیز هست.
عمل G را روی X ترایا گوییم هرگاه یک مدار داشته باشد و عمل را منظم گوییم هرگاه ترایا بوده و برای هر $x \in X$، $\mathrm{stab}_G(x) = \{۱\}$.
واضح است که هر عمل منظم، عمل صادق نیز هست، زیرا $\ker \varphi = \bigcap_{x \in X} \mathrm{stab}_G(x)$. توجه کنید

$$\mathrm{orb}_G(x) = \{x\} \iff \forall g \in G, \quad g \cdot x = x \iff \mathrm{stab}_G(x) = G.$$

مجموعه‌ی تمام اعضایی از X که مدارشان یک عضوی است را مجموعه‌ی نقاط ثابت X می‌نامیم و با X_f نشان می‌دهیم:

$$\begin{aligned} X_f &= \{x \in X \mid \mathrm{orb}_G(x) = \{x\}\} \\ &= \{x \in X \mid \mathrm{stab}_G(x) = G\} \\ &= \{x \in X \mid \forall g \in G, \quad g \cdot x = x\}. \end{aligned}$$

حال فرض کنید G گروه متناهی باشد. فرض کنید

$$\mathrm{orb}_G(y_1), \ldots, \mathrm{orb}_G(y_r), \mathrm{orb}_G(x_1), \ldots, \mathrm{orb}_G(x_k)$$

همه‌ی رده‌های هم‌ارزی متمایز X باشند طوری که $|\mathrm{orb}_G(y_i)| = 1$ و $|\mathrm{orb}_G(x_i)| \geq 2$. پس $X_f = \{y_1, \ldots, y_r\}$. چون X اجتماع مجزای مدارها است داریم

$$|X| = |X_f| + \sum_{i=1}^{k} |\mathrm{orb}_G(x_i)|.$$

بنابراین قضیه‌ی مهم زیر را ثابت کرده‌ایم

قضیه ۳.۱.۵. با نمادهای بالا داریم

$$|X| = |X_f| + \sum_{i=1}^{k} |G : \mathrm{stab}_G(x_i)|.$$

به ویژه اگر G یک p- گروه متناهی باشد، آنگاه به ازای هر $i = 1, 2, \ldots, k$، p شمارنده‌ای از $|G : \mathrm{stab}_G(x_i)|$ است، پس $p \mid (|X| - |X_f|)$ و $p \left| \sum_{i=1}^{k} |G : \mathrm{stab}_G(x_i)| \right.$. □

۲.۵ عمل چپ منظم گروه روی خودش

اگر G گروه باشد، G روی $X = G$ از چپ عمل می‌کند:

$$\forall g \in G, \ \ \forall x \in G, \ \ g \cdot x = gx \tag{1}$$

که در آن gx نشان دهنده‌ی ضرب دو عضو g و x در گروه G است. برای هر $x \in G$ و برای هر $g_1, g_2 \in G$ داریم

$$(g_1 g_2) \cdot x = (g_1 g_2)x = g_1(g_2 x) = g_1 \cdot (g_2 \cdot x)$$

و

$$1 \cdot x = 1x = x.$$

پس رابطه‌ی (۱) عمل گروه G را روی G مشخص می‌کند. همریختی متناظر این عمل عبارت است از $\rho : G \longrightarrow S_G$ که در آن $\rho(g) = \rho_g \in S_G$ و $\rho_g(x) = gx$. این عمل ترایا است. زیرا اگر $x \in G$ عضو دلخواهی باشد، آنگاه به ازای هر $y \in G$، $y^{-1}x \in G$ و

$$y = (yx^{-1}) \cdot x \in \mathrm{orb}_G(x).$$

بنابراین $\mathrm{orb}_G(x) = G$، که نشان می‌دهد عمل فوق ترایا است. از طرف دیگر

$$\begin{aligned} g \in \mathrm{stab}_G(x) &\iff g \cdot x = x \\ &\iff gx = x \\ &\iff g = 1. \end{aligned}$$

پس برای هر $x \in X$، $\mathrm{stab}_G(x) = \{۱\}$. در نتیجه عمل فوق منظم است. به این دلیل عمل فوق را عمل چپ منظم G روی خودش و همریختی متناظر را نمایش جایگشتی چپ منظم G گوییم. چون $\rho : G \longrightarrow S_G$ یک‌به‌یک است، پس G با زیرگروهی از S_G یکریخت است. این نتیجه به قضیه‌ی کیلی موسوم است.

مثال ۱.۲.۵. نمایش جایگشتی چپ منظم ۴-گروه کلاین $G = \{e, a, b, c\}$ را بیابید.

حل به ازای هر $g \in G$ جایگشت $\rho_g \in S_G$ متناظر آن‌را می‌یابیم. می‌دانیم که به ازای هر $x \in G$، $\rho_g(x) = gx$. پس

$$\rho_e = \begin{pmatrix} e & a & b & c \\ e & a & b & c \end{pmatrix}, \quad \rho_a = \begin{pmatrix} e & a & b & c \\ a & e & c & b \end{pmatrix},$$
$$\rho_b = \begin{pmatrix} e & a & b & c \\ b & c & e & a \end{pmatrix}, \quad \rho_c = \begin{pmatrix} e & a & b & c \\ c & b & a & e \end{pmatrix}.$$

بنابراین

$$\rho_e = (e), \quad \rho_a = (e\ a)(b\ c), \quad \rho_b = (e\ b)(a\ c), \quad \rho_c = (e\ c)(a\ b).$$

اگر اعضای e، a، b، c را به ترتیب با اعداد ۱، ۲، ۳، ۴ نام‌گذاری کنیم، آنگاه

$$G \cong \{(۱), (۱\ ۲)(۳\ ۴), (۱\ ۳)(۲\ ۴), (۱\ ۴)(۲\ ۳)\}.$$

بنابراین G با زیر گروهی از $S_۴$ یکریخت است. □

مثال ۲.۲.۵. اگر $|G| = ۲m$، که در آن $m > ۱$ عدد صحیح مثبت فرد است، آنگاه G یک زیرگروه نرمال از مرتبه‌ی m دارد. بنابراین G ساده نیست.

حل فرض کنید $\rho : G \longrightarrow S_G$ نمایش جایگشتی عمل چپ منظم G روی خودش باشد: $\rho(g) = \rho_g \in S_G$، $\rho_g(x) = gx$. می‌دانیم ρ یک‌به‌یک است و $G \cong \mathrm{Im}\,\rho \leq S_G$. چون مرتبه‌ی G زوج است، عضوی از مرتبه‌ی ۲ مثل g دارد. اکنون داریم $\rho_g(x) = gx$ و $\rho_g(gx) = g^۲x = x$. پس ρ_g حاصل‌ضرب ترانهش‌هایی به صورت $(x\ gx)$ است. چون $|G| = ۲m$، تعداد ترانهش‌هایی که در تجزیه‌ی ρ_g ظاهر می‌شوند برابر m است. در نتیجه ρ_g جایگشت فرد است. بنابراین $H = \mathrm{Im}\,\rho$ شامل جایگشت فرد ρ_g است. تابع

$$f : H \longrightarrow \{-۱, ۱\}$$

را با ضابطه‌ی

$$f(\sigma) = \begin{cases} ۱ & \sigma \text{ زوج} \\ -۱ & \sigma \text{ فرد} \end{cases}$$

تعریف می‌کنیم. در این صورت f یک همریختی پوشاست و بنا به قضیه‌ی اول یکریختی

$$H/\ker f \cong \{-۱, ۱\}.$$

بنابراین $|\ker f| = ۲$ و $۲m = |G| = |H| = |\ker f|\,m$. این یعنی H زیرگروه نرمال از مرتبه‌ی m و بنابراین G زیرگروه نرمال از مرتبه‌ی m دارد. □

فرض کنید G گروه باشد. می‌توان عمل ضرب از چپ G روی خودش را برای ضرب از راست نیز تعریف کرد. در واقع G روی $X = G$ با ضرب وارون از راست عمل می‌کند:

$$\forall g \in G, \ \ \forall x \in G, \ \ g \cdot x = xg^{-۱},$$

که در آن $xg^{-۱}$ نشان دهنده‌ی ضرب دو عضو x و $g^{-۱}$ در گروه G است. برای هر $x \in G$ و برای هر $g_۱, g_۲ \in G$ داریم

$$(g_۱g_۲) \cdot x = x(g_۱g_۲)^{-۱} = x(g_۲^{-۱}g_۱^{-۱}) = (xg_۲^{-۱})g_۱^{-۱} = g_۱ \cdot (g_۲ \cdot x)$$

و

$$۱ \cdot x = x۱^{-۱} = x۱ = x.$$

بنابراین G با ضرب وارون از راست روی خودش عمل می‌کند. توجه کنید تعریف $g \cdot x = xg$ لزوماً به یک عمل منجر نمی‌شود (چرا؟). اکنون عمل ضرب از چپ گروه را تعمیم می‌دهیم. فرض کنید H زیرگروهی از گروه G و $X = \{xH \mid x \in G\}$ مجموعه‌ی هم مجموعه‌های چپ H در G باشد. در این صورت G روی X از چپ عمل می‌کند:

$$\forall g \in G, \quad \forall xH \in X, \quad g \cdot xH = gxH$$

که در آن gxH هم‌مجموعه‌ی چپ H شامل gx است. این مشاهده به تعریف یک عمل منجر می‌شود، زیرا به ازای هر $g_۱, g_۲ \in G$ و به ازای هر $xH \in X$ داریم

$$(g_۱g_۲) \cdot xH = (g_۱g_۲)xH = g_۱(g_۲x)H = g_۱ \cdot (g_۲ \cdot xH)$$

و

$$۱ \cdot xH = ۱xH = xH.$$

نمایش جایگشتی متناظر عبارت است از $\rho : G \longrightarrow S_X$ با ضابطه‌ی $\rho(g) = \rho_g$ که در آن $\rho_g \in S_X$ و $\rho_g(xH) = gxH$. داریم

$$\begin{aligned} g \in \mathrm{stab}_G(xH) &\iff g \cdot (xH) = xH \\ &\iff gxH = xH \\ &\iff x^{-۱}gx \in H \\ &\iff g \in xHx^{-۱}. \end{aligned}$$

بنابراین

$$\mathrm{stab}_G(xH) = xHx^{-۱}.$$

در نتیجه

$$\ker \rho = \bigcap_{x \in G} \mathrm{stab}_G(xH) = \bigcap_{x \in G} xHx^{-۱}$$

و $\bigcap_{x \in G} xHx^{-۱}$ یک زیرگروه نرمال از G است که آن را با H_G نشان می‌دهیم و هسته‌ی H در G نامیم. H_G بزرگ‌ترین زیرگروه نرمال G است که در H قرار دارد. در واقع اگر $K \trianglelefteq G$ و $K \leq H$، آنگاه به ازای هر $x \in G$ داریم $K = xKx^{-۱} \leq xHx^{-۱}$. پس $K \leq \bigcap_{x \in G} xHx^{-۱} = H_G$. در حالتی که $H = \{۱\}$ عمل چپ G روی هم مجموعه‌های چپ H در G همان عمل چپ منظم G روی خودش است. با استفاده از عمل G روی هم مجموعه‌های چپ یک زیرگروه دو قضیه‌ی مهم بعد را ثابت می‌کنیم.

قضیه ۳.۲.۵. اگر H زیر گروهی با شاخص متناهی در G باشد، آنگاه زیر گروه نرمال K از G وجود دارد که $K \leq H$ و G/K متناهی است.

اثبات. فرض کنید X مجموعه‌ی هم مجموعه‌های چپ H در G، و $\rho : G \longrightarrow S_X$ نمایش جایگشتی عمل G روی X باشد. فرض کنید $K = H_G$ هسته‌ی ρ باشد، بنا به قضیه‌ی اول یکریختی داریم $G/K \cong \mathrm{Im}\,\rho \leq S_X$. حال اگر $|G : H| = n$، آنگاه $S_X \cong S_n$. پس G/K با زیرگروهی از S_n یکریخت و بنابراین متناهی است. چون H شامل $K = H_G$ است، حکم ثابت است. □

قضیه ۴.۲.۵. اگر H زیرگروهی با شاخص $n > ۱$ از گروه متناهی G باشد طوری که $|G| \nmid n!$، آنگاه G ساده نیست.

اثبات. فرض کنید برخلاف حکم که G ساده باشد. فرض کنید X مجموعه‌ی هم مجموعه‌های چپ H در G، و $\rho : G \longrightarrow S_X \cong S_n$ نمایش جایگشتی عمل G روی X باشد. چون G ساده است، $H_G = \ker \rho = \{۱\}$ و G با زیرگروهی از S_n یکریخت است. به ویژه $|G|$ مرتبه‌ی S_n، یعنی $n!$ را عاد می‌کند، که متناقض با فرض است. □

می‌دانیم اگر $H \leq G$ و $|G : H| = ۲$، آنگاه $H \trianglelefteq G$. اکنون این نتیجه را تعمیم می‌دهیم:

قضیه ۵.۲.۵. فرض کنید G گروه متناهی باشد. اگر $H \leq G$ و $|G : H| = p$، که در آن p کوچک‌ترین عدد اولی است که مرتبه‌ی G را می‌شمارد، آنگاه $H \trianglelefteq G$.

اثبات. اگر $\rho : G \longrightarrow S_p$ نمایش جایگشتی عمل G روی هم مجموعه‌های چپ H در G باشد، می‌دانیم $\ker \rho = H_G$ یک زیرگروه نرمال از G است که در H قرار دارد. چون $G/H_G \hookrightarrow S_p$، داریم $|G/H_G| \mid p!$. اما $H_G \subseteq H \subseteq G$، که نتیجه می‌دهد

$$\begin{aligned} |G : H_G| &= |G : H||H : H_G| \\ &= p|H : H_G|. \end{aligned}$$

بنابراین $p \mid |G : H_G|$، یعنی $p \mid (p-1)!$. چون $|H : H_G|$ شمارنده‌ای از $|G|$ است و همه‌ی شمارنده‌های اول $(p-1)!$ از p کمتر هستند، $|H : H_G| = 1$. یعنی $H = H_G$ و $H \trianglelefteq G$. □

قضیه ۶.۲.۵. اگر G یک گروه نامتناهی و متناهیاً تولید شده باشد، آنگاه به ازای هر عدد صحیح مثبت n، G تعداد متناهی زیرگروه با شاخص n دارد.

اثبات. فرض کنید $G = \langle g_1, \ldots, g_m \rangle$ و H زیرگروهی با شاخص n در G باشد. نمایش جایگشتی $\rho : G \longrightarrow S_n$ متناظر با عمل G روی هم مجموعه‌های چپ H در G را در نظر می‌گیریم. داریم $\ker \rho = H_G$. هر همریختی $\varphi : G \longrightarrow S_n$ با معلوم بودن $\varphi(g_1)$، ...، $\varphi(g_m)$ کاملاً مشخص می‌شود. چون S_n متناهی است، تعداد متناهی همریختی از G به S_n وجود دارد. بنابراین تعداد متناهی زیرگروه نرمال از G می‌تواند به عنوان هسته‌ی این زیرگروه‌های با شاخص n وجود داشته باشد. به علاوه هر چنین زیرگروه نرمال K می‌تواند هسته‌ی تعداد متناهی زیرگروه با شاخص n در G باشد، زیرا G/K متناهی است و بنابراین تعداد متناهی زیرگروه دارد. پس G تعداد متناهی زیرگروه با شاخص n دارد. □

قضیه ۷.۲.۵. فرض کنید H زیرگروهی با شاخص متناهی در یک گروه نامتناهی و متناهیاً تولید شده G باشد. در این صورت زیرگروه مشخصه‌ی K از G وجود دارد که $K \leq H$ و G/K متناهی است.

اثبات. فرض کنید $|G : H| = n$. بنا به قضیه‌ی ۶.۲.۵، G تعداد متناهی زیرگروه با شاخص n دارد مثلاً، $H = H_1$، H_2، ...، H_r. قرار می‌دهیم

$$K = \bigcap_{i=1}^{r} H_i.$$

هر خودریختی G هر زیرگروه شاخص n را به زیرگروه با شاخص n می‌برد. پس هر H_i را به H_j می‌برد، بنابراین K را به K می‌برد ، یعنی K مشخصه است. در نهایت بنا به لم پوانکاره

$$|G : K| = \left| G : \bigcap_{i=1}^{r} H_i \right| \leq \prod_{i=1}^{r} |G : H_i| < \infty.$$

بنابراین شاخص K نیز متناهی است. □

در دو قضیه‌ی فوق شرط متناهیاً تولید شده بودن لازم است. مثلاً گروه جمعی $\mathbb{Z}_p \oplus \mathbb{Z}_p \oplus \cdots$ را در نظر بگیرید، که یک فضای برداری با بعد نامتناهی روی $\mathbb{Z}_p$ است. این گروه متناهیاً تولید شده نیست، به ازای هر n، تعداد نامتناهی زیرگروه با شاخص n دارد و به علاوه مشخصاً ساده است (چرا؟).

فرض کنید $H \leq G$ و $X = \{xH \mid x \in G\}$ مجموعه‌ی هم مجموعه‌های چپ H در G باشد. H نیز روی X با ضرب از چپ عمل می‌کند:

$$\forall h \in H, \ \ \forall Hx \in X, \ \ h \cdot xH = hxH.$$

در واقع عمل H روی X همان تحدید عمل G روی X به H است. مجموعه‌ی اعضایی که مدارشان یک عضوی است را می‌یابیم:

$$\begin{aligned} X_f &= \{xH \in X \mid h \cdot xH = xH, \quad \forall h \in H\} \\ &= \{xH \in X \mid x^{-1}hx \in H, \quad \forall h \in H\} \\ &= \{xH \in X \mid x^{-1}Hx \subseteq H\}. \end{aligned}$$

قضیه ۸.۲.۵. اگر H زیر گروهی از G گروه متناهی باشد طوری که $|H| = p^r$، که در آن p عددی اول است، آنگاه داریم $|G : H| \equiv |N_G(H) : H| \mod p$. به ویژه اگر $p \mid |G : H|$، داریم $p \mid |N_G(H) : H|$، که نتیجه می‌دهد $H < N_G(H)$.

اثبات. عمل H روی $X = \{xH \mid x \in G\}$ هم‌مجموعه‌های چپ H در G را در نظر می‌گیریم. اگر X_f مجموعه‌ی مدارهای یک عضوی و $\mathrm{orb}_H(x_1H)$، ...، $\mathrm{orb}_H(x_kH)$ مدارهای متمایز با بیش از دو عضو باشند، با توجه به قضیه‌ی ۳.۱.۵، داریم

$$|X| = |X_f| + \sum_{i=1}^{k} |H : \mathrm{stab}_H(x_iH)|.$$

چون $|H| = p^r$، به ازای هر $i = 1, 2, \ldots, r$ داریم $p \mid |H : \mathrm{stab}_H(x_iH)|$. بنابراین $p \mid \sum_{i=1}^{r} |H : \mathrm{stab}_H(x_iH)|$ و $p|(|X| - |X_f|)$. در نتیجه $|X| \equiv |X_f| \mod p$. در بحث پیش از قضیه دیدیم $xH \in X_f$ اگر و تنها اگر $x^{-1}Hx \subseteq H$. چون H متناهی است، $|x^{-1}Hx| = |H|$. پس $x^{-1}Hx = H$ و

$$X_f = \{xH \mid x \in N_G(H)\} = \frac{N_G(H)}{H}$$

و $|X_f| = |N_G(H) : H|$. از طرف دیگر داریم $|X| = |G : H|$. از این‌رو $|G : H| \equiv |X_f| \mod p$. اگر $p \mid |G : H|$، آنگاه $p \mid |N_G(H) : H|$ و $H < N_G(H)$. □

۳.۵ عمل گروه به صورت مزدوجی

یکی دیگر از اعمال مهم گروه عمل به صورت مزدوجی است. این عمل ممکن است روی خود گروه یا به طور کلی‌تر روی هر زیر گروه نرمال از گروه، یا مثلاً روی زیر مجموعه‌های گروه باشد. در این‌جا عمل گروه را روی خودش با مزدوجی معرفی می‌کنیم. اگر G گروه باشد، آنگاه G روی خودش به صورت مزدوجی عمل می‌کند:

$$\forall x \in G, \quad \forall g \in G, \quad g \cdot x = gxg^{-1}.$$

زیرا به ازای هر g_1 و g_2 در G و هر $x \in G$ داریم

$$\begin{aligned} (g_1g_2) \cdot x &= (g_1g_2)x(g_1g_2)^{-1} \\ &= g_1(g_2xg_2^{-1})g_1^{-1} \\ &= g_1(g_2 \cdot x)g_1^{-1} \\ &= g_1 \cdot (g_2 \cdot x) \end{aligned}$$

و

$$1 \cdot x = 1x1^{-1} = x.$$

مدار x عبارت است از

$$\mathrm{orb}_G(x) = \{g \cdot x \mid g \in G\} = \{gxg^{-1} \mid g \in G\}$$

که همان رده‌ی مزدوجی x است. ثابت‌ساز x عبارت است از

$$\begin{aligned}\mathrm{stab}_G(x) &= \{g \in G \mid gxg^{-1} = x\}\\ &= \{g \in G \mid gx = xg\}\\ &= C_G(x)\end{aligned}$$

که همان مرکزساز x در G است. مجموعه‌ی اعضایی که مدارشان یک عضوی است را به دست می‌آوریم

$$X_f = \{x \in G \mid \mathrm{stab}_G(x) = G\} = \{x \in G \mid C_G(x) = G\} = Z(G).$$

اگر $\mathrm{orb}_G(x_k), \ldots, \mathrm{orb}_G(x_1)$ همه رده‌های هم‌ارزی متمایز $X = G$ باشند، آنگاه بنا به قضیه‌ی ۳.۱.۵، داریم

$$|G| = |X| = |X_f| + \sum_{i=1}^{k} |G : \mathrm{stab}_G(x_i)| = |Z(G)| + \sum_{i=1}^{k} |G : C_G(x_i)|$$

که همان معادله‌ی رده‌ای است.
همریختی $\tau : G \longrightarrow S_G$، با ضابطه‌ی $\tau(g) = \tau_g$ که در آن τ_g یک جایگشت روی G است و $\tau_g(x) = gxg^{-1}$، به ازای هر $x \in G$، نمایش جایگشتی متناظر عمل G روی G به صورت مزدوجی است. به علاوه

$$\ker \tau = \bigcap_{x \in G} \mathrm{stab}_G(x) = \bigcap_{x \in G} C_G(x) = Z(G).$$

دقت کنید $\mathrm{Im}\,\tau = \mathrm{Inn}\,G$. پس بنا به اولین قضیه‌ی یکریختی $G/Z(G) \cong \mathrm{Inn}\,G$. این نتیجه قبلاً در صفحه‌ی ۹۶ نیز به دست آمده است.
در برخی از کتاب‌ها، به خصوص کتاب‌هایی که مخصوص نظریه‌ی گروه‌ها نوشته شده، تصویر نقطه x تحت تابع f به صورت $(x)f$ یا x^f نوشته می‌شود. بنابراین عمل ترکیب توابع از چپ به راست انجام می‌شود. در این حالت اگر f و g دو تابع باشند تصویر x تحت تابع مرکب $f \circ g$ عبارت است از $g(f(x))$. یکی از مواردی که در این تعریف باید دقت شود هنگام عمل یک گروه بر یک مجموعه است. در این‌جا اگر گروه G روی مجموعه‌ی X عمل کند، برای نشان دادن عمل $g \in G$ روی $x \in X$ می‌نویسیم $x \cdot g$ و می‌گوییم G از راست روی X عمل می‌کند. به ازای هر $g \in G$، تابع $\varphi_g : X \longrightarrow X$ با ضابطه‌ی $(x)\varphi_g = x \cdot g$ یک جایگشت روی X است. از طرفی به ازای هر $g_1, g_2 \in G$ و به ازای هر $x \in X$ داریم

$$(x)\varphi_{g_1 g_2} = x \cdot (g_1 g_2) = (x \cdot g_1) \cdot g_2 = ((x)\varphi_{g_1})\varphi_{g_2},$$

یعنی تابع $\varphi : G \longrightarrow S_X$ یک همریختی است. در واقع شرط لازم و کافی برای این که G از راست روی X عمل کند این است که همریختی $\varphi : G \longrightarrow S_X$ وجود داشته باشد.
بنابراین در این‌جا گروه G با ضرب از راست ، ضرب وارون از چپ، و به صورت مزدوجی $x \cdot g = g^{-1}xg$، روی خودش عمل می‌کند.

تمرین‌ها

۱. نشان دهید گروه جمعی $\mathbb{R}$ روی مجموعه‌ی اعداد مختلط $\mathbb{C}$ به صورت زیر عمل می‌کند

$$\forall a \in \mathbb{R},\ \ \forall z \in \mathbb{C},\ \ a \cdot z = ez.$$

این عمل را از نظر هندسی توصیف کرده و مدارها و ثابت‌سازها را بیابید.

۲. فرض کنید G روی X عمل می‌کند. اگر K هسته‌ی عمل باشد، نشان دهید G/K به صورت طبیعی و صادقانه روی X عمل می‌کند.

۳. فرض کنید $H \leq G$. مجموعه‌ی X را طوری بیابید که G روی X عمل کند و به ازای یک $x \in X$، $\mathrm{stab}_G(x) = H$.

۴. فرض کنید G گروه و X مجموعه‌ی ناتهی باشد. اگر G روی X عمل کند، نشان دهید به ازای هر $g \in G$ و $x \in X$، داریم $\mathrm{stab}_G(g \cdot x) = g\,\mathrm{stab}_G(x)\,g^{-1}$.

۵. فرض کنید G یک p- گروه متناهی باشد و $H \trianglelefteq G$. با استفاده از عمل G روی H به صورت مزدوجی نشان دهید $H \cap Z(G) \neq \{1\}$.

۶. فرض کنید G یک گروه با مرتبه‌ی p^n باشد (p عدد اول و n عدد صحیح مثبت). نشان دهید هر زیرگروه با شاخص p در G نرمال است.

۷. نمایش جایگشتی چپ منظم گروه دووجهی D_8 را بیابید.

۸. نمایش جایگشتی چپ منظم گروه $\mathrm{GL}_2(\mathbb{Z}_2)$ را بیابید.

۹. نمایش جایگشتی گروه دووجهی D_8 را روی هم مجموعه‌های چپ $\langle \varepsilon \rangle$ در D_8 بیابید.

۱۰. فرض کنید H و K زیرگروه‌هایی از گروه دلخواه G باشند (G لزوماً متناهی نیست). اگر $|G : H|$ و $|G : K|$ متناهی و نسبت به هم اول باشند، نشان دهید داریم $|G : H \cap K| = |G : H||G : K|$ و $G = HK$.

۱۱. فرض کنید H و K زیرگروه‌هایی از گروه دلخواه G (نه لزوماً متناهی) باشند. اگر $|G : K| < \infty$، نشان دهید $G = HK$ اگر و تنها اگر $|H : H \cap K| = |G : K|$.

۱۲. فرض کنید G یک p- گروه متناهی باشد. نشان دهید تعداد زیرگروه‌های غیر نرمال G مضربی از p است.

۱۳. فرض کنید G یک p- گروه متناهی باشد. نشان دهید تعداد زیرگروه‌های مرتبه‌ی p^k با تعداد زیرگروه‌های نرمال از مرتبه‌ی p^k به پیمانه‌ی p هم‌نهشت است.

۱۴. فرض کنید K اشتراک همه‌ی زیرگروه‌های شاخص p در یک p- گروه متناهی G باشد. نشان دهید $K \trianglelefteq G$ و G/K آبلی است. هم‌چنین مرتبه‌ی هر عضو غیرهمانی G/K برابر p است.

۱۵. فرض کنید $H, K \leq G$. نشان دهید K به تعداد $|H : H \cap N_G(K)|$ مزدوج متمایز به صورت hKh^{-1}، $h \in H$ دارد.

۱۶. فرض کنید $H, K \leq G$. با استفاده از عمل $H \cap K$ روی $H \times K$ که با $a \cdot (h, k) = (ha^{-1}, ak)$ داده می‌شود ثابت کنید $|HK||H \cap K| = |H||K|$.

۱۷. فرض کنید $H, K \leq G$. در این صورت $H \times K$ روی G با

$$(h, k) \cdot x = hxk^{-1}$$

عمل می‌کند.
(الف) نشان دهید رابطه‌ی بالا یک عمل را معرفی می‌کند و مدار $x \in G$ برابر است با HxK (که آن را هم مجموعه‌ی مضاعف گوییم).
(ب) نشان دهید $\mathrm{stab}_{H\times K}(x)| = |H \cap xKx^{-1}| = |x^{-1}Hx \cap K|$.
(ج) قضیه‌ی فروبنیوس را ثابت کنید: اگر $Hx_1K, \ldots, Hx_nK$ هم‌مجموعه‌های مضاعف متمایز باشند، آن‌گاه

$$|G| = \sum_{i=1}^{n} \frac{|H||K|}{|x_i^{-1}Hx_i \cap K|}.$$

۱۸. نشان دهید $\mathrm{GL}_2(\mathbb{R})$ روی $\mathbb{R}^2$ به صورت زیر عمل می‌کند

$$\begin{bmatrix} a & b \\ c & a \end{bmatrix} \cdot (x, y) = (ax + by, cx + dy).$$

۱۹. فرض کنید G گروه متناهی، $|G| = mn$، و $\rho : G \longrightarrow S_G$ نمایش جایگشتی عمل چپ منظم G باشد. اگر $g \in G$ و $O(g) = n$، نشان دهید $\rho(g)$ حاصلضرب m تا n- دور است. نتیجه بگیرید $\rho(g)$ فرد است اگر و تنها اگر $O(g)$ زوج و $|G|/O(g)$ فرد باشد.

۲۰. فرض کنید G روی X عمل می‌کند. نشان دهید
(الف) اگر عمل ترایا باشد و به ازای یک $x \in X$، $\text{stab}_G(x) = \{۱\}$، آنگاه عمل منظم است.
(ب) اگر G آبلی و عمل صادق و ترایا باشد، آنگاه عمل منظم است.

۲۱. فرض کنید گروه متناهی G به طور ترایا روی مجموعه‌ی متناهی X عمل می‌کند و $|X| = n$، آنگاه $|G|$ مضربی از n است. هم‌چنین $|G| = n$ اگر و تنها اگر عمل منظم باشد.

۲۲. فرض کنید $G = \text{GL}_۲(\mathbb{Z}_۳)$ و $K = Z(G)$. قرار می‌دهیم

$$H = \left\{ \left[\begin{array}{cc} a & b \\ ۰ & c \end{array} \right] \middle| a, b, c \in \mathbb{Z}_۳, \ \ ac \neq ۰ \right\}.$$

نشان دهید
(الف) $K \leq H \leq G$ و $|H| = ۱۲$.
(ب) $K = \bigcap_{x \in G} xHx^{-۱}$.
(ج) $G/K \cong S_۴$.

۲۳. نشان دهید $\text{GL}_۲(\mathbb{Z}_۳)$ حل‌پذیر است.

۲۴. فرض کنید G گروه متناهی باشد و $H \leq G$ طوری است که

$$\forall x \in G, \ \ x \notin H \Longrightarrow H \cap xHx^{-۱} = \{۱\}.$$

ثابت کنید $|H|$ و $|G : H|$ نسبت به هم اول‌اند.

۲۵. فرض کنید H زیرگروهی از گروه G باشد، با تعریف یک عمل مناسب نشان دهید $N_G(H)/C_G(H) \hookrightarrow \text{Aut}\, H$.

۴.۵ قضایای سیلو

در این بخش قضایای سیلو را ، که از قضیه‌های مهم در گروه‌های متناهی هستند. ثابت می‌کنیم. اولین قضیه‌ی سیلو، عکس قضیه‌ی لاگرانژ در یک حالت خاص است. آن وقتی است که عدد شمارنده مرتبه‌ی گروه توانی از یک عدد اول باشد. از تمرین ۵ صفحه‌ی ۹۴ یادآوری می‌کنیم که گروه G را p- گروه (p عدد اول) می‌نامیم، هرگاه مرتبه‌ی هر عضو G توانی از p باشد. به علاوه بنا به همان تمرین، گروه متناهی G یک p- گروه است اگر و تنها اگر $|G|$ توانی از p باشد. قضیه‌ی زیر را می‌توان با استفاده از معادله‌ی رده‌ای ثابت کرد، و در تمرین ۱۵ از صفحه‌ی ۹۴، این کار خواسته شده است. در این‌جا اثبات دیگری ارائه می‌کنیم.

قضیه ۱.۴.۵. فرض کنید G گروه متناهی باشد. اگر p عدد اول باشد و $p^k \mid |G|$، که در آن $k \geq ۰$ عدد صحیح است، آنگاه G زیرگروهی از مرتبه‌ی p^k دارد.

اثبات. به استقرا روی k قضیه را ثابت می‌کنیم. اگر $k = ۰$ چیزی برای اثبات نیست و اگر $k = ۱$ حکم از قضیه‌ی کُشی (قضیه‌ی ۴.۹.۳ از صفحه‌ی ۹۳) ثابت است. فرض کنید $k > ۱$ و قضیه برای همه زیرگروه‌هایی که $p^{k-۱}$ مرتبه‌ی آن‌ها را می‌شمارد درست باشد. بنا به فرض استقرا زیرگروه H از G با مرتبه‌ی $p^{k-۱}$ وجود دارد. چون $p \mid |G : H|$، بنا به قضیه‌ی ۸.۲.۵، داریم $p \mid |N_G(H) : H|$. بنا به قضیه‌ی کُشی زیرگروه K/H از $N_G(H)/H$ با مرتبه‌ی p وجود دارد. بنابراین

$$|K| = |K/H||H| = pp^{k-۱} = p^k$$

و K زیر گروهی از G با مرتبه‌ی p^k است. □

نتیجه ۲.۴.۵. (قضیه‌ی اول سیلو) اگر $|G| = p^n m$، که در آن p عدد اول است و $p \nmid m$، آنگاه G زیرگروهی از مرتبه‌ی p^n دارد.

اگر $|G| = p^n m$ که در آن p عدد اول است و $p \nmid m$، هر زیرگروه مرتبه‌ی p^n را p- زیرگروه سیلوی G نامیم. مجموعه‌ی p- زیرگروه‌های سیلو را با $\mathrm{Syl}_p(G)$ نشان می‌دهیم. قضیه‌ی اول سیلو می‌گوید $\mathrm{Syl}_p(G) \neq \emptyset$. یک p- زیرگروه سیلوی P از گروه متناهی G یک p- زیرگروه G با ماکسیمم مرتبه‌ی ممکن است. توجه کنید به ازای هر $g \in G$، gPg^{-1} نیز یک p- زیرگروه سیلوی G است، زیرا $|gPg^{-1}| = |P|$. عکس مطلب نیز درست است: هر p- زیرگروه سیلوی G با P مزدوج است. در واقع چیز بیشتری می‌توانیم ثابت کنیم: هر p- زیرگروه G در یک مزدوج P قرار دارد (و در نتیجه در یک p- زیرگروه سیلو واقع است).

قضیه ۳.۴.۵. فرض کنید G گروه متناهی باشد و $|G| = p^n m$، که در آن p عدد اول است و $p \nmid m$. فرض کنید $P \in \mathrm{Syl}_p(G)$. اگر H یک p- زیرگروه دلخواه G باشد، آنگاه به ازای یک $g \in G$، $H \leq gPg^{-1}$.

اثبات. فرض کنید $X = \{xP \mid x \in G\}$ مجموعه‌ی هم مجموعه‌های چپ P در G باشد. در این صورت H روی X با $h \cdot xP = hxP$ عمل می‌کند. داریم $|X| = |G : P| = m$ و $p \nmid |X|$ را عاد نمی‌کند. چون H یک p- گروه است، طبق قضیه‌ی ۳.۱.۵، $p \nmid (|X| - |X_f|)$، که در آن X_f مجموعه‌ی اعضای X است که مدارشان یک عضوی است. بنابراین $X_f \neq \emptyset$. فرض کنید $gP \in X_f$. پس به ازای هر $h \in H$، $h \cdot gP = gP$. بنابراین به ازای هر $h \in H$ داریم $g^{-1}hg \in P$. و این یعنی $H \subseteq gPg^{-1}$. □

حال اگر H را یک p- زیرگروه سیلوی G در نظر بگیریم خواهیم داشت:

نتیجه ۴.۴.۵. (قضیه‌ی دوم سیلو) اگر G گروه متناهی باشد هر دو p- زیرگروه سیلوی G در G مزدوج‌اند. به بیان دیگر عمل G روی $\mathrm{Syl}_p(G)$ به صورت مزدوجی، ترایا است. □

چون یک زیرگروه G در G نرمال است اگر و تنها اگر با همه‌ی مزدوج‌هایش برابر باشد، داریم :

نتیجه ۵.۴.۵. فرض کنید G گروه متناهی باشد و $P \in \mathrm{Syl}_p(G)$. در این صورت P در نرمال است اگر و تنها اگر یکتا p- زیرگروه سیلوی G باشد. □

مثال ۶.۴.۵. فرض کنید K یک زیرگروه نرمال از گروه متناهی G باشد. در این صورت یک زیرگروه K، p- زیرگروه سیلوی K است اگر و تنها اگر به صورت $P \cap K$ باشد، که در آن P یک p- زیرگروه سیلوی G است، یعنی

$$\mathrm{Syl}_p(K) = \{P \cap K \mid P \in \mathrm{Syl}_p(G)\}.$$

حل فرض کنید $P \in \mathrm{Syl}_p(G)$. چون $P \cap K \leq P$، $P \cap K$ یک p- زیرگروه K است. به علاوه p،

$$|G : P| = |G : PK||PK : P|$$

را عاد نمی‌کند. از این رو $p \nmid |PK : P|$. اما $|PK : P| = |K : P \cap K|$، که نتیجه می‌دهد $p \nmid |K : P \cap K|$ و این یعنی $P \cap K \in \mathrm{Syl}_p(K)$ (توجه کنید چون $K \trianglelefteq G$ داریم $PK \leq G$).
حال اگر $T \in \mathrm{Syl}_p(K)$، آنگاه چون $P \cap K \in \mathrm{Syl}_p(K)$، طبق قضیه‌ی دوم سیلو، به ازای یک $k \in K$ داریم $k(P \cap K)k^{-1} = T$ و $kPk^{-1} \cap K = T$. kPk^{-1} یک مزدوج P و از این رو یک p- زیرگروه سیلوی G است. بنابراین حکم ثابت است. □

مثال ۷.۴.۵. فرض کنید G گروه متناهی باشد. یک زیرگروه G/K یک p- زیرگروه سیلوی G/K است اگر و تنها اگر به صورت PK/K باشد که در آن P یک p- زیرگروه سیلوی G است، یعنی

$$\mathrm{Syl}_p(G/K) = \{PK/K \mid P \in \mathrm{Syl}_p(G)\}.$$

حل بنا به قضیه‌ی دوم یکریختی داریم $PK/K \cong P/P \cap K$. پس PK/K یک p- زیرگروه G/K است. از طرف دیگر p، $|G : P| = |G : PK||PK : P|$ را عاد نمی‌کند. پس p، $|G : PK|$ را عاد نمی‌کند و بنابراین $|G/K : PK/K| = |G : PK|$ را عاد نمی‌کند. در نتیجه $PK/K \in \mathrm{Syl}_p(G/K)$.
حال اگر $T/K \in \mathrm{Syl}_p(G/K)$، چون $PK/K \in \mathrm{Syl}_p(G/K)$ بنا به قضیه‌ی دوم سیلو به ازای یک $gK \in G/K$ داریم

$gK(PK/K)(gK)^{-1} = T/K$، که نتیجه می‌دهد $(gPg^{-1})K/K = T/K$. چون $H = gPg^{-1} \in \mathrm{Syl}_p(G)$، حکم ثابت است. □

حال می‌خواهیم تعداد p- زیرگروه‌های سیلوی متمایز یک گروه متناهی G، یعنی $|\mathrm{Syl}_p(G)|$ را بیابیم. فرض کنید n_p تعداد p-زیرگروه‌های سیلوی متمایز G باشد. اگر P یک p- زیرگروه سیلوی G باشد، طبق قضیه‌ی دوم سیلو، هر زیرگروه سیلوی G با P در G مزدوج است. پس $n_p = |G : N_G(P)|$. از طرف دیگر اگر $|G| = p^n m$ که در آن $p \nmid m$، آنگاه چون $P \leq N_G(P) \leq G$، داریم

$$\begin{aligned} |G : P| &= |G : N_G(P)||N_G(P) : P| \\ &= n_p|N_G(P) : P|. \end{aligned}$$

چون $|G : P| = m$، داریم $n_p|m$.
اکنون ویژگی مهم n_p را ثابت می‌کنیم:

قضیه ۸.۴.۵. (قضیه‌ی سوم سیلو) اگر $|G| = p^n m$، که در آن p یک عدد اول است که $p \nmid m$، آنگاه $n_p \equiv ۱ \mod p$

اثبات. فرض کنید $X = \mathrm{Syl}_p(G)$، در این صورت $n_p = |X|$. p- زیرگروه سیلوی $P \in X$ را ثابت در نظر می‌گیریم. P روی X با مزدوجی عمل می‌کند. بنا به قضیه‌ی ۳.۱.۵، $p|(|X| - |X_f|)$ که در آن X_f مجموعه‌ی اعضای X است که مدارشان یک عضوی است. چون $|X| = n_p$، پس کافی است ثابت کنیم $X_f = \{P\}$. چون

$$X_f = \{Q \in X \mid \forall a \in P,\ \ aQ^{-1}a = P\},$$

واضح است که $P \in X_f$. حال اگر $Q \in X_f$، آنگاه $P \subseteq N_G(Q)$. بنابراین P و Q هر دو p- زیرگروه‌های سیلوی $N_G(Q)$ هستند (چون p- زیرگروه‌هایی با مرتبه‌ی ماکسیمم‌اند) چون $Q \trianglelefteq N_G(Q)$، پس بنا به نتیجه ۵.۴.۵، $Q = P$. بنابراین، همان طور که می‌خواستیم $X_f = \{P\}$. □

مثال ۹.۴.۵. اگر G یک گروه باشد و $|G| = pq$، که در آن p و q اعداد اول متمایز هستند طوری که $q \not\equiv ۱ \mod p$، آنگاه p- زیرگروه سیلوی G در G نرمال است.

حل بنا به قضایای سیلو $n_p|q$، $n_p \equiv ۱ \mod p$. اگر $n_p = q$، آنگاه $q \equiv ۱ \mod p$ که خلاف فرض است. پس $n_p = ۱$ و p-زیرگروه سیلوی G یکتا و در G نرمال است. □

مثال ۱۰.۴.۵. اگر $|G| = pq$ (p و q اعداد اول متمایز)، آنگاه G ساده نیست.

حل بدون کم شدن از کلیت مساله می‌توان فرض کرد $p > q$. پس $p > q > q - ۱$ و $p \nmid q - ۱$. پس طبق مثال ۹.۴.۵، p- زیرگروه سیلوی G در G نرمال است. □

مثال ۱۱.۴.۵. اگر $|G| = pq$ (که در آن p و q اعداد اول متمایزند) و $p \not\equiv ۱ \mod q$ و $q \not\equiv ۱ \mod p$، آنگاه G دوری است.

حل اگر $P \in \mathrm{Syl}_p(G)$ و $Q \in \mathrm{Syl}_q(G)$. طبق مثال قبل $P \trianglelefteq G$ و $Q \trianglelefteq G$. از طرفی چون $|P \cap Q|$ هم p و هم q را می‌شمارد، $|P \cap Q| = ۱$، یعنی $P \cap Q = \{۱\}$. بنابراین $|PQ| = |P||Q| = pq = |G|$ که نتیجه می‌دهد $G = PQ$. بنابراین $G = P \times Q$. چون P و Q دوری‌اند و مرتبه‌هایشان نسبت به هم اول است، G نیز دوری است. □

مثال ۱۲.۴.۵. نشان دهید هر گروه مرتبه‌ی $p^۲q^۲$ ساده نیست (p و q اعداد اول متمایز).

حل فرض کنید $|G| = p^۲q^۲$. بدون کم شدن از کلیت مساله می‌توان فرض کرد $p > q$. داریم $n_p|q^۲$. پس $n_p = ۱$ یا $n_p = q$ یا $n_p = q^۲$. اگر $n_p = ۱$، آنگاه p- زیرگروه سیلوی G نرمال و مساله حل است. حالت $n_p = q$ ممکن نیست، زیرا $p > q$ و $n_p = ۱ + kp$. بنابراین فرض کنید $n_p = q^۲$. چون $n_p \equiv ۱ \mod p$، داریم $q^۲ \equiv ۱ \mod p$، یعنی $p|(q^۲ - ۱)$. بنابراین $p|(q - ۱)$ یا $p|(q + ۱)$. چون $p > q$، حالت اول امکان ندارد ، و $p|(q + ۱)$. بنابراین $q + ۱ \geq p > q$ و $q + ۱ = p$. پس $p = ۳$ و $q = ۲$ و $|G| = ۳۶$. اما در این صورت شاخص هر ۳- زیرگروه سیلو برابر ۴ است. بنابراین همریختی $\rho : G \longrightarrow S_۴$ وجود دارد. این همریختی یک‌به‌یک نیست زیرا $|G| = ۳۶$ و $|S_۴| = ۴!$. بنابراین $\ker \rho \trianglelefteq G$. □

مثال ۱۳.۴.۵. اگر $|G| = p^۲q$، که در آن p و q اعداد اول متمایزند، آنگاه یا p- زیرگروه سیلوی G و یا q- زیرگروه سیلوی G در G نرمال است. بنابراین G ساده نیست.

حل فرض کنید برخلاف حکم $n_p > ۱$ و $n_q > ۱$. چون $n_p|q$، داریم $n_p = q$. از طرفی $n_p = ۱ + kp$ (به ازای یک $k > ۰$). پس $q = n_p = ۱ + kp > p$. هم‌چنین $n_q|p^۲$، که نتیجه می‌دهد $n_q = p$ یا $n_q = p^۲$. چون هر عضو مرتبه‌ی q در G یک زیرگروه مرتبه‌ی q تولید می‌کند که q- زیرگروه سیلوی G نیز هست و اشتراک هر دو زیرگروه متمایز G از مرتبه‌ی q بدیهی است، تعداد اعضای مرتبه‌ی q در G برابر است با

$$n_q(q - ۱).$$

بنابراین اگر $n_q = p^۲$، آنگاه دقیقاً

$$p^۲q - p^۲(q - ۱) = p^۲$$

عضو G از مرتبه‌ی q نیستند. اما در این صورت چون مرتبه‌ی هیچ عضو یک p- زیرگروه سیلوی P از G برابر q نیست و $|P| = p^۲$، نتیجه می‌شود که P باید یک p- زیرگروه سیلوی یکتا G باشد. این تناقض با $n_p > ۱$ است. پس $n_q = p$. حال چون $n_q = ۱ + rq$، $r > ۰$، نتیجه می‌شود که $p = n_q = ۱ + rq > q$ که متناقض با $q > p$ است. □

مثال ۱۴.۴.۵. فرض کنید G گروه و r، q، p اعداد اول متمایز باشند. اگر $|G| = pqr$، آنگاه یکی از زیرگروه‌های سیلوی G در G نرمال است. بنابراین G ساده نیست.

حل بدون کم شدن از کلیت مساله می‌توان فرض کرد $p > q > r$. فرض کنید بر خلاف حکم $n_p > ۱$، n_q، و n_r. چون مرتبه‌ی هر p- زیرگروه سیلوی G برابر p است، اشتراک هر دو p- زیرگروه سیلوی متمایز G بدیهی است. پس تعداد اعضای مرتبه‌ی p برابر است با $n_p(p - ۱)$. به طریق مشابه تعداد اعضای مرتبه‌ی q برابر $n_q(q - ۱)$ و تعداد اعضای مرتبه‌ی r برابر $n_r(r - ۱)$ است. بنابراین

$$|G| = pqr \geq ۱ + n_p(p - ۱) + n_q(q - ۱) + n_r(r - ۱).$$

بنا به قضیه‌ی سوم سیلو $n_p|qr$، که نتیجه می‌دهد $n_p = q$، یا $n_p = r$ یا $n_p = qr$. چون $n_p = ۱ + k_۱p$، $(k_۱ > ۰)$ و $n_p = ۱ + k_۱p > p > q > r$، دو حالت اول رخ نمی‌دهند. بنابراین $n_p = qr$. هم‌چنین $n_q|pr$، که نتیجه می‌دهد $n_q = r$، یا $n_q = p$ یا $n_q = pr$. چون $n_q = ۱ + k_۲q$، $(k_۲ > ۰)$ و $n_q = ۱ + k_۲q > q > r$، حالت اول رخ نمی‌دهند و داریم $n_q \geq p$. در نهایت داریم $n_r|pq$. پس n_r برابر q، یا p، و یا pq است. در هر حالت $n_r \geq q$. بنابراین

$$pqr \geq ۱ + qr(p - ۱) + p(q - ۱) + q(r - ۱),$$

این یعنی $(p - ۱)(q - ۱) \geq ۰$، که نتیجه‌ای قطعاً نادرست است. □

مثال ۱۵.۴.۵. اگر $|G| = ۲^۵ \times ۳$، نشان دهید G یک زیرگروه نرمال از مرتبه‌ی ۳۲ یا ۱۶ دارد.

حل داریم $n_۲|۳$ و $n_۲ = ۱ + ۲k$. پس $n_۲ = ۱$ یا $n_۲ = ۳$. اگر $n_۲ = ۱$، آنگاه ۲- زیرگروه سیلوی G زیرگروه نرمال مرتبه‌ی ۳۲ دارد. پس فرض کنید $n_۲ = ۳$. فرض کنید P و Q در ۲- زیرگروه سیلوی G باشند. ادعا می‌کنیم $|P \cap Q| = ۱۶$. چون $P \neq Q$ و $|P| \mid |P|$ $|P \cap Q|$ پس $|P \cap Q|$ برابر ۲، ۴، ۸ یا ۱۶ است. اگر $|P \cap Q| \leq ۸$، آنگاه

$$|PQ| = \frac{|P||Q|}{|P \cap Q|} \geq \frac{۳۲ \times ۳۲}{۸} = ۱۲۸ > ۹۶ = |G|$$

که تناقض است. پس $|P \cap Q| = ۱۶$. چون $|P : P \cap Q| = ۲$ و $|Q : P \cap Q| = ۲$، $P \cap Q$ در P و Q نرمال است. پس $P, Q \leq N_G(P \cap Q)$ و $PQ \leq N_G(P \cap Q)$. بنابراین

$$|N_G(P \cap Q)| \geq |PQ| = \frac{|P||Q|}{|P \cap Q|} = \frac{۳۲ \times ۳۲}{۱۶} = ۶۴.$$

چون $N_G(P \cap Q) \leq G$ و $|G| = ۹۶$، $|N_G(P \cap Q)| = ۹۶$. پس $N_G(P \cap Q) = G$. بنابراین $P \cap Q \trianglelefteq G$. □

مثال ۱۶.۴.۵. نشان دهید هر گروه مرتبه‌ی ۲۵۵ دوری است.

حل فرض کنید $|G| = ۲۵۵ = ۳ \times ۵ \times ۱۷$ و $P \in \mathrm{Syl}_{۱۷}(G)$. چون $n_{۱۷}|۱۵$ و $n_{۱۷} = ۱ + ۱۷k$، $n_{۱۷} = ۱$. پس $P \trianglelefteq G$. اکنون چون، بنا به تمرین ۳ از صفحه‌ی ۹۷،

$$\frac{G}{C_G(P)} = \frac{N_G(P)}{C_G(P)} \hookrightarrow \mathrm{Aut}\, P$$

و $\mathrm{Aut}\, P = \mathrm{Aut}\, \mathbb{Z}_{۱۷} \cong \mathbb{Z}_{۱۷}^{\times}$، داریم $|G/C_G(P)| \mid ۱۶$. چون $|G/C_G(P)| \mid ۲۵۵$ و $\gcd\{۲۵۵, ۱۶\} = ۱$، داریم $G = C_G(P)$. در نتیجه $P \leq Z(G)$ و $|Z(G)| \mid ۱۷$. بنابراین $|Z(G)|$ برابر ۱۷، ۵۱، یا ۸۵ و یا ۲۵۵ است. در نتیجه $|G/Z(G)|$ برابر ۱۵ یا ۵ یا ۳ و یا ۱ است. اما در این صورت $G/Z(G)$ دوری است، که نتیجه می‌دهد G آبلی است. بنابراین همه‌ی زیرگروه‌های G در G نرمال هستند. به ویژه اگر $P \in \mathrm{Syl}_{۱۷}(G)$، $Q \in \mathrm{Syl}_{۵}(G)$، $R \in \mathrm{Syl}_{۳}(G)$، آنگاه $P = \langle a \rangle$، $Q = \langle b \rangle$ و $R = \langle c \rangle$ در G نرمال هستند. به راحتی می‌توان دید $O(abc) = ۲۵۵$. پس $G = \langle abc \rangle$ دوری است. □

مثال ۱۷.۴.۵. (این مثال به فصل ۴، حاصل‌ضرب دکارتی گروه‌ها، نیاز دارد) فرض کنید G یک گروه متناهی با مرتبه‌ی $p_۱^{n_۱} p_۲^{n_۲} \cdots p_k^{n_k}$ باشد، که در آن p_iها اعداد اول متمایز و n_iها اعداد صحیح مثبت هستند. اگر به ازای هر $i = ۱, ۲, \ldots, k$، p_i- زیرگروه سیلوی G یکتا باشد، نشان دهید G برابر حاصل‌ضرب مستقیم زیرگروه‌های خودش است.

حل فرض کنید به ازای هر $i = ۱, ۲, \ldots, k$، P_i یکتا p_i- زیرگروه سیلوی G باشد. بنابراین $P_i \trianglelefteq G$. چون مرتبه‌ی $P_۱$ و $P_۲$ نسبت به هم اول‌اند ، $P_۱ \cap P_۲ = \{۱\}$، که نتیجه می‌دهد

$$|P_۱ P_۲| = \frac{|P_۱||P_۲|}{|P_۱ \cap P_۲|} = |P_۱||P_۲| = p_۱^{n_۱} p_۲^{n_۲}.$$

چون $P_۱$ و $P_۲$ در G نرمال‌اند، $P_۱P_۲$ زیرگروهی از G است. اکنون چون مرتبه‌ی $P_۱P_۲$ و $P_۳$ نسبت به هم اول‌اند، $P_۱P_۲ \cap P_۳ = \{۱\}$ و داریم

$$|P_۱ P_۲ P_۳| = \frac{|P_۱P_۲||P_۳|}{|P_۱P_۲ \cap P_۳|} = |P_۱P_۲||P_۳| = p_۱^{n_۱} p_۲^{n_۲} p_۳^{n_۳}.$$

پس به استقرا می‌توان ثابت کرد که $P_۱P_۲ \cdots P_k$ زیرگروهی از G با مرتبه‌ی $p_۱^{n_۱} p_۲^{n_۲} \cdots p_k^{n_k}$ است. بنابراین، داریم $G = P_۱P_۲ \cdots P_k$. به علاوه به ازای هر $j = ۱, ۲, \ldots, k$، مرتبه‌های P_j و $P_۱ \cdots P_{j-۱}P_{j+۱} \cdots P_k$ نسبت به هم اول‌اند، و اشتراک‌شان بدیهی است. در نتیجه $G = P_۱ \times \cdots \times P_k$. □

این بخش را اثبات این که $A_۵$ تنها گروه ساده با مرتبه‌ی ۶۰ است، به پایان می‌بریم.

قضیه ۱۸.۴.۵. اگر G گروه ساده با مرتبه‌ی ۶۰ باشد، آنگاه $G \cong A_۵$.

اثبات. فرض کنید $P \in \mathrm{Syl}_{۲}(G)$. پس $n_۲ = |G : N_G(P)|$. به علاوه از $n_۲|۱۵$ نتیجه می‌شود $n_۲$ برابر ۳ یا ۵ و یا ۱۵ است.
حالت اول : $n_۲ = ۳$. چون شاخص $N_G(P)$ در G برابر ۳ است، عمل G روی هم‌مجموعه‌های $N_G(P)$ در G منجر به نمایش جایگشتی $\rho : G \to S_۳$ می‌شود. چون G ساده است، $\ker \rho = \{۱\}$. این تناقض است زیرا $|G| = ۶۰$ و $|S_۳| = ۶$.
حالت دوم : $n_۲ = ۱۵$. اگر برای هر دو ۲- زیرگروه سیلوی متمایز P و Q داشته باشیم $P \cap Q = \{۱\}$. آنگاه تعداد عناصر غیرهمانی در ۲- زیرگروه‌های سیلوی G برابر $۱۵ \times (۴ - ۱) = ۴۵$ است. اما چون $n_۵ = ۶$، تعداد عناصر مرتبه‌ی ۵ برابرند با $۶ \times (۵ - ۱) = ۲۴$. از این دو ۶۹ عضو به دست می‌آید، این خلاف $|G| = ۶۰$ است. پس دو ۲- زیرگروه سیلوی P و Q از G وجود دارند که $|P \cap Q| = ۲$. فرض کنید $M = N_G(P \cap Q)$. چون P و Q آبلی‌اند، $P, Q \leq M$. چون G ساده است $M \neq G$. پس $|M| \mid ۴$ و $|M| > ۴$ (در غیر این صورت $P = M = Q$). چون $|M| \mid ۶۰$ و $|M| > ۴$ داریم $|M| = ۲۰$ یا $|M| = ۱۲$. اگر $|M| = ۲۰$، آنگاه $|G : M| = ۳$ و یک همریختی $\rho : G \to S_۳$ وجود دارد. چون G ساده است، $\ker \rho = \{۱\}$. این تناقض است زیرا $|G| = ۶۰$ و $|S_۳| = ۶$. از این‌رو $|M| = ۱۲$. در نتیجه $|G : M| = ۵$ و یک همریختی $\rho : G \to S_۵$ وجود دارد. چون G ساده است، $\ker \rho = \{۱\}$ و $G \cong \mathrm{Im}\, \rho \leq S_۵$. G را با تصویرش در $S_۵$ یکی در نظر می‌گیریم و فرض می‌کنیم $G \leq S_۵$. چون $|S_۵ : G| = ۲$ و $A_۵$ تنها زیرگروه S با شاخص ۲ است، $G = A_۵$. این تناقض است زیرا $n_۲(A_۵) = ۵$.

حالت سوم: $n_۲ = ۵$. مانند استدلال حالت دوم ، همریختی $\rho : G \to S_۵$ وجود دارد و $\ker \rho = \{۱\}$ و $G \cong \operatorname{Im} \rho \leq S_۵$. G را با تصویرش در $S_۵$ یکی در نظر می‌گیریم و فرض می‌کنیم $G \leq S_۵$. چون $|S_۵ : G| = ۲$ و $A_۵$ تنها زیرگروه S با شاخص ۲ است، $G = A_۵$. □

تمرین‌ها

۱. اگر $K \trianglelefteq G$، نشان دهید G یک p- گروه است اگر و تنها اگر K و G/K هر دو p- گروه باشند.

۲. نشان دهید هر گروه مرتبه‌ی ۱۷۵ آبلی است.

۳. نشان دهید اگر $|G|$ یکی از اعداد زیر باشد، آنگاه گروه G ساده نیست.
(الف) ۵۶ (ب) ۷۲ (ج) ۶۵ (د) ۱۲۵ (هـ) ۴۶۲
(و) ۲۰۰ (ز) ۵۲ (ح) ۷۵ (ط) ۱۵۰ (ی) ۱۴۴

۴. اگر $|G| = ۳۸۵$ نشان دهید ۷- زیرگروه سیلوی G در $Z(G)$ قرار دارد و ۱۱- زیرگروه سیلوی G نرمال است.

۵. ثابت کنید که اگر $|G| \leq ۱۰۰$ و G گروه ناآبلی ساده باشد، آنگاه $G \cong A_۵$.

۶. فرض کنید مرتبه‌ی گروه G برابر ۴۵۵ باشد. نشان دهید G دوری است.

۷. اگر $|G| = p^۲q$ و $p^۲ \not\equiv ۱ \mod q$ و $q \not\equiv ۱ \mod p$ نشان دهید G آبلی است.

۸. فرض کنید $|G| = p^m r$ و $p \nmid r$، که در آن p عدد اول است و $r \geq ۰$. اگر G گروه ساده باشد، ثابت کنید $p^m | (r-۱)!$.

۹. گروه ساده از مرتبه‌ی ۵×۲^m وجود ندارد $(m \geq ۱)$.

۱۰. فرض کنید K اشتراک همه‌ی p- زیرگروه‌های سیلوی گروه متناهی G باشد. نشان دهید K در G نرمال است و هر p- زیرگروه نرمال G را در بر دارد.

۱۱. (استدلال فراتینی) اگر H زیرگروه نرمال متناهی از گروه G باشد و $P \in \operatorname{Syl}_p(H)$، آنگاه $G = HN_G(P)$.

۱۲. فرض کنید P یک p- زیرگروه سیلوی گروه متناهی G باشد. نشان دهید هر $K \leq G$ که $N_G(P) \leq K$ داریم $N_G(K) = K$.

۱۳. فرض کنید P یک p- زیرگروه سیلوی گروه متناهی G باشد، طوری که $N_G(P) = P$، آنگاه به ازای هر $Q \in \operatorname{Syl}_p(G)$، داریم $N_G(Q) = Q$.

۱۴. فرض کنید P یک p- زیرگروه سیلوی نرمال گروه متناهی G و $\varphi : G \longrightarrow G$ یک همریختی باشد. نشان دهید $\varphi(P) \leq P$.

۱۵. نشان دهید اگر H یک زیرگروه نرمال مرتبه‌ی p^k در گروه متناهی G باشد، آنگاه H در هر p- زیرگروه سیلوی G قرار دارد.

۱۶. فرض کنید G گروه متناهی و $P \in \operatorname{Syl}_p(G)$ طوری باشد که $N_G(P) = P$. نشان دهید G/G' یک p- گروه است.

۱۷. فرض کنید G گروهی متناهی باشد که به ازای هر n حداکثر n عضو متمایز از مرتبه‌ی n دارد. نشان دهید G دوری است.

۱۸. نشان دهید هر خودریختی $S_۴$ داخلی است و نتیجه بگیرید $\operatorname{Aut} S_۴ \cong S_۴$.

۱۹. فرض کنید G گروه متناهی باشد و $|G| = p^n m$، که در آن p عدد اول است و $\gcd\{p, m\} = ۱$. اگر $n_p = ۱ + p$، نشان دهید $|\bigcap_{P \in \operatorname{Syl}_p(G)} P| = p^{n-۱}$

فصل ۶

گروه‌های آبلی متناهیاً تولید شده

یکی از هدف‌های جبر مجرد (و دیگر بخش‌های ریاضیات) این است که رده‌ای مهم از ساختارهای جبری را در نظر بگیرد و نشان دهد هر عضو این رده را می‌توان به صورت الگوریتمی بر حسب اعضای ساده و شناخته شده ساخت. در این فصل این کار را برای گروه‌های آبلی متناهیاً تولید شده انجام می‌دهیم: هر گروه آبلی متناهیاً تولید شده با حاصل‌ضرب تعداد متناهی گروه دوری یکریخت است. چون گروه‌های دوری کاملاً شناخته شده هستند ، این نتیجه از اولین نمونه‌ها در قضایائی از این نوع محسوب می‌شود، و الگویی برای متخصصین جبر است که آن را به راه‌های متفاوتی توسعه دهند.

۱.۶ گروه‌های آبلی متناهی

در این بخش نشان می‌دهیم که هر گروه آبلی متناهی با حاصل‌ضرب تعداد متناهی زیرگروه دوری منحصر به فرد با مرتبه‌ی توانی از اعداد اول یکریخت است. فرض کنید G یک گروه و p یک عدد اول باشد. قرار می‌دهیم

$$G(p) = \{g \in G \mid \exists k \geq ۰,\ \ g^{p^k} = ۱\}.$$

در حالتی که G آبلی باشد $G(p)$ یک زیرگروه G است. اگر $g \in G$ و به ازای یک $k \geq ۰$، $g^{p^k} = ۱$، آنگاه $O(g)|p^k$ و $O(g)$ نیز توانی از p است. پس

$$G(p) = \{g \in G \mid \exists k \geq ۰,\ \ O(g) = p^k\}.$$

$G(p)$ را مولفه‌ی اولیه‌ی گروه G می‌نامیم. قضیه‌ی بعدی را می‌توان با استفاده از قضایای سیلو و این که G حاصل‌ضرب مستقیم زیرگروه‌های سیلوی خودش است ثابت کرد. اما در این‌جا اثبات دیگری ارائه می‌کنیم.

قضیه ۱.۱.۶. (قضیه‌ی تجزیه‌ی اولیه) فرض کنید G یک گروه آبلی متناهی باشد. اگر $|G| = p_۱^{n_۱} p_۲^{n_۲} \cdots p_k^{n_k}$، که در آن p_iها اعداد اول متمایزند و $n_i \geq ۰$، $i = ۱, \ldots, k$، آنگاه

$$G = G(p_۱) \times \cdots \times G(p_k).$$

اثبات. فرض کنید $n = p_۱^{n_۱} p_۲^{n_۲} \cdots p_k^{n_k}$. به ازای هر $i = ۱, \ldots, k$، قرار می‌دهیم $m_i = n/p_i^{n_i}$. چون $\gcd\{m_۱, m_۲, \ldots, m_k\} = ۱$، اعداد صحیح $c_۱$، $c_۲$، ...، c_k وجود دارند که

$$۱ = c_۱ m_۱ + \cdots + c_k m_k.$$

بنابراین برای هر $g \in G$ داریم

$$g = g^{۱} = g^{c_۱ m_۱ + \cdots + c_k m_k} = g^{c_۱ m_۱} \cdots g^{c_k m_k}.$$

به علاوه $g^{c_i m_i} \in G(p_i)$، زیرا $(g^{c_i m_i})^{p_i^{n_i}} = g^{n c_i} = ۱$. بنابراین

$$G = G(p_۱) G(p_۲) \cdots G(p_k).$$

حال فرض کنید

$$g \in [G(p_1)\cdots G(p_{r-1})G(p_{r+1})\cdots G(p_k)] \cap G(p_r).$$

چون $g \in G(p_r)$، داریم $g^u = 1$، که در آن u توانی از p_r است. هم‌چنین چون

$$g \in G(p_1)\cdots G(p_{r-1})G(p_{r+1})\cdots G(p_k),$$

داریم $g^v = 1$، که در آن v حاصل‌ضرب ضربی از توان‌های p_1، ...، p_{r+1}، p_{r-1}، ...، p_k است. چون $\gcd\{u,v\} = 1$، داریم $g = 1$. بنابراین

$$G = G(p_1) \times \cdots \times G(p_k). \qquad \square$$

نتیجه ۲.۱.۶. با نمادهای بالا داریم $|G(p_i)| = p_i^{n_i}$.

اثبات. چون $G(p_i)$ یک p_i- گروه است، پس m_i وجود دارد که $|G(p_i)| = p_i^{m_i}$. اما بنا به قضیه‌ی ۱.۱.۶، داریم

$$|G| = |G(p_1)||G(p_2)|\cdots|G(p_k)| = p_1^{m_1}p_2^{m_2}\cdots p_k^{m_k}.$$

چون $|G| = n = p_1^{n_1}p_2^{n_2}\cdots p_k^{n_k}$، بنا به یکتایی تجزیه به عوامل اول ، داریم $m_i = n_i$. $\square$

نتیجه ۳.۱.۶. اگر $n = p_1^{n_1}\cdots p_k^{n_k}$، p_iها اعداد اول متمایزند، آنگاه

$$\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{n_1}} \oplus \cdots \oplus \mathbb{Z}_{p_k^{n_k}}.$$

اثبات. $\mathbb{Z}_n(p_i)$ یک گروه دوری است (زیرگروهی از $\mathbb{Z}_n$ است) و مرتبه‌اش $p_i^{n_i}$ است، پس $\mathbb{Z}_n(p_i) \cong \mathbb{Z}_{p_i^{n_i}}$. $\square$

نتیجه ۴.۱.۶. فرض کنید G گروه آبلی باشد و $|G| = p_1^{n_1}p_2^{n_2}\cdots p_k^{n_k}$ (p_iها اعداد اول متمایز هستند). اگر $G = G_1 \times G_2 \times \cdots \times G_k$، که در آن G_i، یک p_i- گروه است، آنگاه $G_i = G(p_i)$.

مثال ۵.۱.۶. مولفه‌های اولیه‌ی $\mathbb{Z}_{12} \oplus \mathbb{Z}_{15} \oplus \mathbb{Z}_{90}$ را بیابید.

حل با استفاده از نتیجه‌ی ۳.۱.۶، به طور جداگانه برای $\mathbb{Z}_{12}$ و $\mathbb{Z}_{15}$ و $\mathbb{Z}_{90}$ داریم

$$\begin{aligned} G &= \mathbb{Z}_{12} \oplus \mathbb{Z}_{15} \oplus \mathbb{Z}_{90} \\ &\cong (\mathbb{Z}_4 \oplus \mathbb{Z}_3) \oplus (\mathbb{Z}_3 \oplus \mathbb{Z}_5) \oplus (\mathbb{Z}_2 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_5) \\ &\cong (\mathbb{Z}_2 \oplus \mathbb{Z}_4) \oplus (\mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_9) \oplus (\mathbb{Z}_5 \oplus \mathbb{Z}_5). \end{aligned}$$

پس همه‌ی مولفه‌های اولیه‌ی گروه G عبارت‌اند از

$$G(5) \cong \mathbb{Z}_5 \oplus \mathbb{Z}_5, \quad G(3) \cong \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_9, \quad G(2) \cong \mathbb{Z}_2 \oplus \mathbb{Z}_4. \qquad \square$$

فرض کنید G گروه آبلی متناهی باشد، در این صورت بنا به قضیه‌ی تجزیه‌ی اولیه ۱.۱.۶، G حاصل‌ضرب مستقیم p- گروه‌ها است. اکنون با در نظر گرفتن p- گروه‌های آبلی تجزیه‌ی G را بیشتر بررسی می‌کنیم. از اینجا به بعد برای راحتی کار همه‌ی گروه‌های آبلی مورد بحث را به صورت جمعی در نظر می‌گیریم.

لم ۶.۱.۶. فرض کنید G یک p- گروه آبلی متناهی باشد. اگر $a \in G$ عضوی با مرتبه‌ی ماکسیمم باشد، آنگاه زیرگروه H وجود دارد که $G = \langle a \rangle \oplus H$.

اثبات. فرض کنید $O(a)=p^n$. در این صورت طبق فرض به ازای هر $g\in G$، که $O(g)=p^k$، آنگاه $k\leq n$. بنابراین به ازای هر $g\in G$، $p^ng=۰$. داریم $\langle a\rangle\cap\{۰\}=\{۰\}$. چون G متناهی است زیرگروه H از G با مرتبه‌ی ماکسیمم طوری وجود دارد که $\langle a\rangle\cap H=\{۰\}$. اگر ثابت کنیم $G=\langle a\rangle+H$، حکم ثابت است. فرض کنید چنین نباشد و $\langle a\rangle+H<G$. پس عضو $b\in G$ وجود دارد که $b\notin\langle a\rangle+H$. فرض کنید t کوچک‌ترین عدد صحیح مثبت باشد که $p^tb\notin\langle a\rangle+H$ (این عدد وجود دارد، زیرا اگر $O()=p^r$، آنگاه $p^rb=۰\in\langle a\rangle+H$). قرار می‌دهیم $g=p^tb$. پس $g\notin\langle a\rangle+H$ و $pg\in\langle a\rangle+H$. از این‌رو $h\in H$ و $m\in\mathbb{Z}$ وجود دارند که $pg=ma+h$. چون $p^ng=۰$ داریم

$$p^ng=p^{n-۱}ma+p^{n-۱}h.$$

بنابراین

$$p^{n-۱}ma=-p^{n-۱}h\in\langle a\rangle\cap H=\{۰\}.$$

پس $p^{n-۱}ma=۰$. چون $O(a)=p^n$ داریم $p^n|p^{n-۱}m$ و $p|m$. در نتیجه $k\in\mathbb{Z}$ وجود دارد که $m=kp$. چون $pg=ma+h$، داریم

$$p(g-ka)=pg-ma=h\in H.$$

اما چون $g\notin\langle a\rangle+H$، داریم $g-ka\notin H$. از این‌رو $H<\langle g-ka\rangle+H$ و بنا به انتخاب H،

$$\langle a\rangle\cap[\langle g-ka\rangle+H]\neq\{۰\}.$$

بنابراین

$$۰\neq\ =s(g-ka)+h_۱,\quad r,s\in\mathbb{Z},\quad h_۱\in H.$$

اکنون دو حالت تشخیص می‌دهیم:

حالت اول : $p|s$. در این حالت $s=k_۱p$، که در آن $k_۱\in\mathbb{Z}$. چون $p(g-ka)\in H$، داریم

$$۰\neq\ =k_۱p(g-ka)+h_۱\in H$$

که تناقض است، زیرا $\langle a\rangle\cap H=\{۰\}$.

حالت دوم : $p\nmid s$. در این صورت $\gcd\{p,s\}=۱$ و اعداد $u,v\in\mathbb{Z}$ وجود دارند که $up+vs=۱$. چون $pg\in\langle a\rangle+H$ داریم

$$g=۱\cdot g=upg+vsg=upg+v(ra+ska-h_۱)\in\langle a\rangle+H$$

که تناقض است. بنابراین هر دو حالت به تناقض منجر شد. بنابراین $G=\langle a\rangle+H$ و اثبات کامل است. □

قضیه ۷.۱.۶. (فروبنیوس-استیکلبرگر) گروه آبلی G متناهی است اگر و تنها اگر حاصل‌ضرب جمع مستقیم تعداد متناهی گروه دوری با مرتبه‌ی توانی از اعداد اول باشد.

اثبات. با توجه به قضیه‌ی تجزیه‌ی اولیه ۱.۱.۶، کافی است حالتی را در نظر بگیریم که G یک p- گروه باشد. فرض کنید $a\in G$ عضوی با مرتبه‌ی ماکسیمم باشد. طبق لم ۶.۱.۶، $H\leq G$ وجود دارد که $G=\langle a\rangle\oplus H$. اکنون چون H یک p- گروه است، می‌توان به استقرا عمل کرده و حکم قضیه را به دست آورد. □

اکنون یکتایی تجزیه‌ی یک p- گروه را به حاصل‌جمع مستقیم گروه‌های دوری ثابت می‌کنیم:

قضیه ۸.۱.۶. فرض کنید G یک p- گروه آبلی متناهی و

$$G=G_۱\oplus G_۲\oplus\cdots\oplus G_r$$

تجزیه‌ی G به زیرگروه‌های دوری باشد که در آن $|G_۱|\geq|G_۲|\geq\cdots\geq|G_r|$، آنگاه این تجزیه یکتاست، یعنی اگر $G=H_۱\oplus H_۲\oplus\cdots\oplus H_s$ تجزیه‌ی دیگری از G به زیرگروه‌های دوری باشد که $|H_۱|\geq|H_۲|\geq\cdots\geq|H_s|$، آنگاه $r=s$ و $H_i\cong G_i$، به ازای هر i.

اثبات. تعریف می‌کنیم

$$G[p] = \{g \in G \mid pg = ۰\}.$$

به سادگی می‌توان دید $G[p] \leq G$؛ و هم‌چنین $G[p] = G_۱[p] \oplus \cdots \oplus G_r[p]$ و $|G_i[p]| = p$ به ازای هر i، پس $|G[p]| = p^r$. به طریق مشابه با استفاده از تجزیه‌ی $G = H_۱ \oplus \cdots \oplus H_s$ داریم $|G[p]| = p^s$. پس $r = s$. حال نشان می‌دهیم $H_i \cong G_i$. به استقرا روی i، کافی است نشان دهیم $|H_i| = |G_i|$ (زیرا G_i و H_i دوری‌اند). فرض کنید $|G| = p^n$. به استقرا روی n عمل می‌کنیم. حالت‌های $n = ۰$ و $n = s$ واضح هستند. تعریف می‌کنیم

$$pG = \{pg \mid g \in G\}.$$

در این صورت به سادگی می‌توان دید که $pG \leq G$. هم‌چنین $pG = pG_۱ \oplus \cdots \oplus pG_r$ و به علاوه $pG_i = \{۰\}$ اگر و تنها اگر $|G_i| = p$ و در غیر این صورت $|pG_i| = \frac{|G_i|}{p}$. پس فرض کنید k طوری باشد که $pG = pG_۱ \oplus \cdots \oplus pG_k$ و $|G_{k+۱}| = \cdots = |G_r| = p$. به طریق مشابه $pG = pH_۱ \oplus \cdots \oplus pH_m$، که $|H_{m+۱}| = \cdots = |H_s| = p$. چون $|pG| < |G|$ از فرض استقرا داریم $k = m$ و $|G_i| = |H_i|$، برای $۱ \leq i \leq k$. پس $|G_i| = |H_i|$، به ازای هر i و حکم ثابت است. □

در قضیه‌ی ۸.۱.۶، داریم $|G_i| = p^{n_i}$ (به ازای یک i). پس بنا به قضیه‌ی ۸.۱.۶، اگر G آبلی باشد و $|G| = p^n$، آنگاه اعداد یکتای (وابسته به G) $n_۱ \geq n_۲ \geq \cdots \geq n_r \geq ۱$ وجود دارند که $n = n_۱ + n_۲ + \cdots + n_r$ و

$$G \cong \mathbb{Z}_{p^{n_۱}} \oplus \mathbb{Z}_{p^{n_۲}} \oplus \cdots \oplus \mathbb{Z}_{p^{n_r}}.$$

در این حالت گوییم G از نوع $(n_۱, n_۲, \ldots, n_r)$ است و اعداد $p^{n_۱}$، $p^{n_۲}$، ...، p^{n_r} را شمارنده‌های مقدماتی گروه G می‌نامیم. $(n_۱, n_۲, \ldots, n_r)$ یک افراز n نامیده می‌شود.

مثال ۹.۱.۶. همه‌ی گروه‌های آبلی از مرتبه‌ی $p^۴$ را رده‌بندی کنید.

حل این رده‌بندی عبارت است از

نوع	گروه
(۴)	$\mathbb{Z}_{p^۴}$
$(۳, ۱)$	$\mathbb{Z}_{p^۳} \oplus \mathbb{Z}_p$
$(۲, ۲)$	$\mathbb{Z}_{p^۲} \oplus \mathbb{Z}_{p^۲}$
$(۲, ۱, ۱)$	$\mathbb{Z}_{p^۲} \oplus \mathbb{Z}_p \oplus \mathbb{Z}_p$
$(۱, ۱, ۱, ۱)$	$\mathbb{Z}_p \oplus \mathbb{Z}_p \oplus \mathbb{Z}_p \oplus \mathbb{Z}_p$.

پس ۵ گروه غیر یکریخت آبلی مرتبه‌ی $p^۴$ وجود دارد. □

مثال ۱۰.۱.۶. همه‌ی گروه‌های آبلی از مرتبه‌ی $p^۲q^۳$ را بیابید (p و q اعداد اول متمایز).

حل اگر $|G| = p^۲q^۳$، آنگاه $G \cong G(p) \oplus G(q)$، که در آن $|G(p)| = p^۲$، $|G(q)| = q^۳$. پس همه‌ی نوع‌های ممکن برای $G(p)$ عبارت‌اند از (۲) و $(۱, ۱)$. همه‌ی نوع‌های ممکن برای $G(q)$ عبارت‌اند از (۳)، $(۲, ۱)$ و $(۱, ۱, ۱)$. بنابراین ۶ گروه آبلی از مرتبه‌ی $p^۲q^۳$ وجود دارند:

$$\mathbb{Z}_{p^۲} \oplus \mathbb{Z}_{q^۳} \qquad \mathbb{Z}_p \oplus \mathbb{Z}_p \oplus \mathbb{Z}_{q^۳}$$
$$\mathbb{Z}_{p^۲} \oplus \mathbb{Z}_{q^۲} \oplus \mathbb{Z}_q \qquad \mathbb{Z}_p \oplus \mathbb{Z}_p \oplus \mathbb{Z}_{q^۲} \oplus \mathbb{Z}_q$$
$$\mathbb{Z}_{p^۲} \oplus \mathbb{Z}_q \oplus \mathbb{Z}_q \oplus \mathbb{Z}_q \qquad \mathbb{Z}_p \oplus \mathbb{Z}_p \oplus \mathbb{Z}_q \oplus \mathbb{Z}_q \oplus \mathbb{Z}_q.$$

□

می‌دانیم اگر G گروه دوری از مرتبه‌ی n باشد، آنگاه به ازای هر شمارنده‌ی d از n زیرگروهی یکتا از مرتبه‌ی d دارد. اکنون این مطلب را برای گروه‌های آبلی متناهی ثابت می‌کنیم:

قضیه ۱۱.۱.۶. اگر G یک گروه آبلی از مرتبه‌ی n باشد و $m|n$، $(m > ۰)$، آنگاه G زیرگروهی از مرتبه‌ی m دارد.

اثبات. اگر $n = ۱$، آنگاه $m = ۱$ و $\{۰\}$ یک زیرگروه مرتبه‌ی m است. پس فرض کنید $n > ۱$. بنا به قضیه‌ی ۱.۱.۶، اعداد اول $p_۱$، $p_۲$، ...، p_k، و اعداد صحیح مثبت $n_۱$، $n_۲$، ...، n_k وجود دارند که

$$G \cong \mathbb{Z}_{p_۱^{n_۱}} \oplus \mathbb{Z}_{p_۲^{n_۲}} \oplus \cdots \oplus \mathbb{Z}_{p_k^{n_k}}.$$

پس $n = p_۱^{n_۱} \cdots p_k^{n_k}$. چون $m|n$، اعداد صحیح $۰ \leq m_i \leq n_i$، برای $i = ۱, ۲, \ldots, k$ وجود دارد که $m = p_۱^{m_۱} p_۲^{m_۲} \cdots p_k^{m_k}$. چون $p_i^{m_i} | p_i^{n_i}$ به ازای هر i، بنا به قضیه‌ی ۷.۴.۳، از صفحه‌ی ۶۸، گروه دوری $\mathbb{Z}_{p_i^{n_i}}$ زیرگروه یکتای G_i از مرتبه‌ی $p_i^{m_i}$، به ازای هر i، دارد. پس $G_۱ + G_۲ + \cdots + G_k = G_۱ \oplus G_۲ \oplus \cdots \oplus G_k$ زیرگروهی از $\mathbb{Z}_{p_۱^{n_۱}} \oplus \mathbb{Z}_{p_۲^{n_۲}} \oplus \cdots \oplus \mathbb{Z}_{p_k^{n_k}}$ با مرتبه‌ی $m = p_۱^{m_۱} p_۲^{m_۲} \cdots p_k^{m_k}$ است. بنابراین، به سادگی، نتیجه می‌شود G زیرگروهی از مرتبه‌ی m دارد. □

قضیه ۱۲.۱.۶. دو p- گروه آبلی از مرتبه‌ی p^n، n عدد صحیح مثبت، یکریخت هستند اگر و تنها اگر نوع یکسان داشته باشند.

اثبات. فرض کنید G و H دو p^n- گروه آبلی با مرتبه‌ی p باشند. ابتدا فرض کنید G و H نوع یکسان $(n_۱, n_۲, \ldots, n_k)$ داشته باشند، که در آن $n = n_۱ + \cdots + n_k$ و $n_۱ \geq n_۲ \geq \cdots \geq n_k > ۰$. در این صورت $G \cong \mathbb{Z}_{p^{n_۱}} \oplus \cdots \oplus \mathbb{Z}_{p^{n_k}}$ و $H \cong \mathbb{Z}_{p^{n_۱}} \oplus \cdots \oplus \mathbb{Z}_{p^{n_k}}$. بنابراین $G \cong H$.
اکنون فرض کنید $H \cong G$ و $f : G \longrightarrow H$ یکریختی باشد. طبق قضیه‌ی ۱.۱.۶، داریم $G = G_۱ \oplus G_۲ \oplus \cdots \oplus G_k$، که در آن $G_i \cong \mathbb{Z}_{p^{n_i}}$، $۱ \leq i \leq k$، و $n_۱ \geq n_۲ \geq \cdots \geq n_k > ۰$. هم‌چنین $H = H_۱ \oplus \cdots \oplus H_t$، که در آن $H_j \cong \mathbb{Z}_{p_j^m}$، $۱ \leq j \leq t$، و $m_۱ \geq m_۲ \geq \cdots \geq m_t > ۰$. اکنون چون $f^{-۱}(H_i)$ زیرگروه مرتبه‌ی p^{n_i} از G و $f^{-۱}(H_۱) \oplus \cdots \oplus f^{-۱}(H_t)$ است، بنا به قضیه‌ی ۸.۱.۶، $t = k$ و $p^{m_i} = |f^{-۱}(H_i)| = p^{n_i}$، $۱ \leq i \leq k$، یعنی $m_i = n_i$ و نوع G و H یکی است. □

مثال ۱۳.۱.۶. فرض کنید H و G گروه‌های آبلی باشند.
(الف) اگر $f : G \longrightarrow H$ یک همریختی باشد، نشان دهید به ازای هر عدد اول p، $f(G(p)) \subseteq H(p)$.
(ب) $G \cong H$ اگر و تنها اگر به ازای هر عدد اول p، $G(p) \cong H(p)$.

حل (الف) فرض کنید $a \in G(p)$. در این صورت به ازای یک $k \geq ۰$، $p^k a = ۰$. پس $f(p^k a) = p^k f(a) = ۰$ و $f(a) \in H(p)$. بنابراین $f(G(p)) \subseteq H(p)$.
(ب) فرض کنید $G \cong H$ و $f : G \longrightarrow H$ یکریختی باشد. فرض کنید p عدد اول دلخواهی باشد ؛ طبق (الف) $f|_{G(p)} : G(p) \longrightarrow H(p)$ همریختی یک‌به‌یک است. نشان می‌دهیم $f|_{G(p)}$ پوشاست. فرض کنید $h \in H(p)$. چون f پوشاست، $a \in G$ وجود دارد که $f(a) = h$. به علاوه چون $h \in H(p)$، عدد $k \geq ۰$ وجود دارد که $p^k h = ۰$. بنابراین $f(p^k a) = p^k f(a) = p^k h = ۰$ و $p^k a \in \ker f = \{۰\}$. در نتیجه $a \in G(p)$. بنابراین $f|_{G(p)} : G(p) \longrightarrow H(p)$ یکریختی است و $G(p) \cong H(p)$. برعکس فرض کنید به ازای هر p، $G(p) \cong H(p)$. با استفاده از قضیه‌ی ۱.۱.۶، داریم

$$G = G(p_۱) \oplus G(p_۲) \oplus \cdots \oplus G(p_k)$$
$$H = H(p_۱) \oplus H(p_۲) \oplus \cdots \oplus H(p_k).$$

طبق فرض، $G(p_i) \cong H(p_i)$ به ازای هر i. پس یکریختی $f_i : G(p_i) \longrightarrow H(p_i)$ وجود دارد. تابع $f : G \longrightarrow H$ را با

$$f(g_۱ + g_۲ + \cdots + g_k) = f_۱(g_۱) + f_۲(g_۲) + \cdots + f_k(g_k)$$

تعریف می‌کنیم. در این صورت f یکریختی است و $G \cong H$. □

۲.۶ ساختار گروه‌های آبلی متناهیاً تولید شده

در این بخش گروه‌های آبلی متناهیاً تولید شده را در نظر می‌گیریم. ثابت می‌کنیم چنین زیرگروه‌هایی با حاصل‌جمع مستقیم گروه‌های دوری یکریخت هستند. فرض کنید G یک گروه آبلی باشد. زیرمجموعه‌ی X از G را مستقل خطی گوییم، هرگاه اگر $x_۱, \dots, x_n \in X$ اعضای متمایز X باشند و $k_۱, \dots, k_n \in \mathbb{Z}$ از

$$k_۱x_۱ + k_۲x_۲ + \cdots + k_nx_n = ۰$$

نتیجه شود، $k_۱ = k_۲ = \cdots = k_n = ۰$. زیرمجموعه‌ی را که مستقل خطی نباشد وابسته‌ی خطی گوییم. یک مجموعه‌ی مولد و مستقل خطی برای گروه آبلی G یک پایه گوییم. بنابراین X پایه‌ای برای گروه آبلی G است، هرگاه مستقل خطی بوده و هر عضو $a \in G$ را بتوان به صورت $a = k_۱x_۱ + \cdots + k_nx_n$ نوشت، که در آن $n \in \mathbb{N}$، $k_i \in \mathbb{Z}$ و $x_i \in X$. به سادگی می‌توان دید که زیر مجموعه‌ی X از گروه آبلی G پایه‌ای برای G است اگر و تنها اگر هر عضو $a \in G$ را بتوان به صورت منحصر به فرد $a = k_۱x_۱ + \cdots + k_nx_n$ نوشت، که در آن $n \in \mathbb{N}$، $۰ \neq k_i \in \mathbb{Z}$ و $x_i \in X$ (یعنی اگر $a = r_۱y_۱ + \cdots + r_my_m$، که در آن $n \in \mathbb{N}$، $۰ \neq r_i \in \mathbb{Z}$ و $y_i \in X$، آنگاه $n = m$ و پس از تعویض اندیس‌ها، در صورت لزوم، $k_i = r_i$ و $x_i = y_i$). گروه آبلی F را گروه آبلی آزاد گوییم هرگاه پایه‌ای داشته باشد. گروه آبلی F را گروه آبلی آزاد متناهیاً تولید شده گوییم هرگاه پایه‌ای متناهی داشته باشد.
فرض کنید I یک مجموعه‌ی اندیس باشد؛ به ازای هر $i \in I$، قرار می‌دهیم $G_i = \mathbb{Z}$. پس $\oplus_{i\in I}G_i = \oplus_{i\in I}\mathbb{Z}$ یک گروه آبلی است. به ازای هر $j \in I$، دنباله‌ی $e_j = (a_i)_{i\in I}$ را طوری در نظر می‌گیریم مولفه‌ی jام آن برابر ۱ و هر مولفه‌ی دیگر آن ۰ باشد، یعنی $a_i = \begin{cases} ۰ & i \neq j \\ ۱ & i = j \end{cases}$. پس e_j عضوی از $\oplus_{i\in I}\mathbb{Z}$ است. فرض کنید $u = (b_i)_{i\in I}$ عضو دلخواهی از $\oplus_{i\in I}\mathbb{Z}$ باشد. بنابراین $j_۱, \dots, j_n \in I$ وجود دارند که به ازای هر $i \in I$ که $i = \{j_۱, \dots, j_n\}$، $b_i = ۰$. در نتیجه

$$u = (b_i)_{i\in I} = b_{j_۱}e_{j_۱} + \cdots + b_{j_n}e_{j_n}.$$

این یعنی $X = \{e_j \mid j \in I\}$ یک مجموعه‌ی مولد برای $\oplus_{i\in I}\mathbb{Z}$ است. علاوه بر این X مستقل خطی است، زیرا اگر

$$b_{j_۱}e_{j_۱} + \cdots + b_{j_n}e_{j_n} = (۰)_{i\in I},$$

آنگاه به ازای هر k، مولفه‌ی j_kام سمت چپ تساوی برابر b_{j_k} و مولفه‌ی j_kام سمت راست تساوی برابر ۰ است. پس به ازای هر k، $b_{j_k} = ۰$. بنابراین ثابت کردیم $\oplus_{i\in I}\mathbb{Z}$ یک گروه آبلی آزاد با پایه‌ی $\{e_j \mid j \in I\}$ است.
حال فرض کنید X مجموعه‌ای دلخواه باشد. X را به عنوان مجموعه‌ی اندیس انتخاب می‌کنیم. پس گروه آبلی $\oplus_{x\in X}\mathbb{Z}$ یک گروه آبلی آزاد روی $Y = \{e_x \mid x \in X\}$ است. به وضوح $|Y| = |X|$. بنابراین به ازای هر مجموعه‌ی X یک گروه آبلی آزاد با پایه‌ای مثل Y وجود دارد که $|Y| = |X|$.

قضیه ۱.۲.۶. فرض کنید F گروه آبلی باشد. قضیه‌های زیر معادل‌اند
(الف) F گروه آبلی آزاد است.
(ب) F حاصل‌جمع مستقیم (داخلی) زیرگروه‌های دوری نامتناهی است.

اثبات. (الف) $\Longrightarrow$ (ب) فرض کنید X پایه‌ای برای F باشد. عضو دلخواه $x \in X$ را در نظر می‌گیریم. اگر به ازای یک $n \in \mathbb{Z}$، $nx = ۰$، آنگاه چون X مستقل خطی است، داریم $n = ۰$. پس $O(x) = \infty$ و $\langle x\rangle$ یک زیرگروه دوری نامتناهی است. چون X پایه‌ای برای F است، هر عضو $a \in F$ را می‌توان به صورت منحصر به فرد $a = k_۱x_۱ + \cdots + k_nx_n$ نوشت، که در آن $n \in \mathbb{N}$، $۰ \neq k_i \in \mathbb{Z}$ و $x_i \in X$. از این‌رو F حاصل‌جمع مستقیم خانواده زیرگروه‌های $\{\langle x\rangle\}_{x\in X}$ است: $F = \oplus_{x\in X}\langle x\rangle$.
(ب) $\Longrightarrow$ (الف) فرض کنید $F = \oplus_{i\in I}G_i$، که در آن ، به ازای هر $i \in I$، $G_i = \langle a_i\rangle$ گروه دوری نامتناهی است. چون F حاصل‌جمع مستقیم خانواده زیرگروه‌های $\{G_i\}_{i\in I}$ است، هر عضو $a \in F$ را می‌توان به صورت منحصر به فرد $a = k_۱a_۱ + \cdots + k_na_n$ نوشت، که در آن $n \in \mathbb{N}$، $۰ \neq k_i \in \mathbb{Z}$. این یعنی $X = \{a_i \mid i \in I\}$ پایه‌ای برای F است و F گروه آبلی آزاد است. □

برای تعریف همریختی از یک گروه آبلی آزاد به گروه آبلی دیگر کافی است آن را روی یک پایه‌ی آزاد تعریف کنیم. این مطلب محتوای قضیه‌ی بعد است.

قضیه ۲.۲.۶. فرض کنید F یک گروه آبلی آزاد با پایه‌ی X باشد. اگر G یک گروه آبلی دلخواه باشد، آنگاه هر تابع $g : X \longrightarrow G$ را می‌توان به یک همریختی یکتای $f : F \longrightarrow G$ توسعه داد، یعنی همریختی یکتای $f : F \longrightarrow G$ وجود دارد که $f|_X = g$، یعنی $f(x) = g(x)$ به ازای هر $x \in X$.

اثبات. چون X پایه‌ای برای F است، هر عضو $a \in F$ را می‌توان به صورت منحصر بفرد $a = k_1x_1 + \cdots + k_nx_n$ نوشت، که در آن $x_i \in X$ و $k_i \in \mathbb{Z}$. اگر تابع $f : F \longrightarrow G$ بخواهد همریختی باشد و $f(x) = g(x)$، به ازای هر $x \in X$، باید داشته باشیم

$$\begin{aligned} f(a) &= f(k_1x_1 + \cdots + k_nx_n) \\ &= k_1f(x_1) + \cdots + k_nf(x_n) \\ &= k_1g(x_1) + \cdots + k_ng(x_n). \end{aligned}$$

پس تابع $f : F \longrightarrow G$ را با ضابطه‌ی

$$f(a) = k_1g(x_1) + \cdots + k_ng(x_n)$$

تعریف می‌کنیم. نشان می‌دهیم f همریختی است. اگر $a = k_1x_1 + \cdots + k_nx_n$ و $b = r_1x_1 + \cdots + r_nx_n$ اعضایی از F باشند، که در آن $k_i, r_i \in \mathbb{Z}$ و $x_i, y_i \in X$، (با اضافه کردن $0x_i$ به a یا b، در صورت لزوم) داریم

$$\begin{aligned} f(a+b) &= f(k_1x_1 + \cdots + k_nx_n + r_1x_1 + \cdots + r_nx_n) \\ &= f((k_1 + r_1)x_1 + \cdots + (k_n + r_n)x_n) \\ &= (k_1 + r_1)g(x_1) + \cdots + (k_n + r_n)g(x_n) \\ &= k_1g(x_1) + \cdots + k_ng(x_n) + r_1g(x_1) + \cdots + r_ng(x_n) \\ &= f(k_1x_1 + \cdots + k_nx_n) + f(r_1x_1 + \cdots + r_nx_n) \\ &= f(a) + f(b). \end{aligned}$$

به علاوه f یکتاست. زیرا اگر $h : F \longrightarrow G$ همریختی دیگری باشد که به ازای هر $x \in X$، $h(x) = g(x)$، آنگاه به ازای هر $a = k_1x_1 + \cdots + k_nx_n \in G$ داریم

$$\begin{aligned} f(a) &= k_1g(x_1) + \cdots + k_ng(x_n) && (f \text{ طبق تعریف}) \\ &= k_1h(x_1) + \cdots + k_nh(x_n) && (g(x_i) = h(x_i) \text{ چون}) \\ &= h(k_1x_1 + \cdots + k_nx_n) && (h \text{ چون همریختی است}) \\ &= h(a). \end{aligned}$$

بنابراین $f = h$. □

نتیجه ۳.۲.۶. هر گروه آبلی G تصویر همریخت یک گروه آبلی آزاد است.

اثبات. فرض کنید X یک مجموعه‌ی مولد برای G باشد (G بزرگ‌ترین مجموعه‌ی مولد برای G است). فرض کنید F یک گروه آبلی آزاد با پایه‌ای مثل Y باشد که $|X| = |Y|$. در این صورت تابع یک‌به‌یک و پوشای $g : Y \longrightarrow X$ وجود دارد. بنا به قضیه‌ی قبل همریختی یکتای $f : G \longrightarrow F$ وجود دارد که به ازای هر $y \in Y$، $f(y) = g(y)$. چون $G = \langle X \rangle$ و g پوشاست، نتیجه می‌شود که f پوشاست. بنابراین $G \cong F/\ker f$ و G تصویر همریخت گروه آبلی آزاد F است. □

مثال ۴.۲.۶. برای هر $n \in \mathbb{N}$، $\mathbb{Z}_n$ تصویر همریخت $\mathbb{Z}$ است، زیرا $\mathbb{Z}_n \cong \mathbb{Z}/n\mathbb{Z}$. □

برای یک گروه آبلی آزاد پایه‌های متفاوت زیادی وجود دارد. مثلاً $\{(1,0),(0,1)\}$ و $\{(1,1),(0,-1)\}$ دو پایه‌ی متفاوت برای $\mathbb{Z} \oplus \mathbb{Z}$ هستند. اما تعداد عناصر پایه عددی منحصر به فرد است. این مطلب را در حالتی که گروه آبلی آزاد یک پایه‌ی متناهی داشته باشد، ثابت می‌کنیم. اما متذکر می‌شویم که این مطلب در حالت کلی درست است (صفحه‌ی ۲۷ از کتاب مرجع [۵] را ببینید).

قضیه ۵.۲.۶. فرض کنید F یک گروه آبلی آزاد متناهیاً تولید شده باشد. در این صورت هر دو پایه‌ی F تعداد عناصر یکسانی دارند.

اثبات. فرض کنید X پایه‌ای برای F با k عضو و Y پایه‌ای برای F با r عضو باشند. پس $F \cong \underbrace{\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}}_{k \text{ بار}}$. اکنون $2F \leq F$ و $2F \cong \underbrace{2\mathbb{Z} \oplus \cdots \oplus 2\mathbb{Z}}_{k \text{ بار}}$. در نتیجه، بنا به تمرین ۱۲، از صفحه‌ی ۱۰۴،

$$\frac{F}{2F} \cong \underbrace{\frac{\mathbb{Z}}{2\mathbb{Z}} \oplus \cdots \oplus \frac{\mathbb{Z}}{2\mathbb{Z}}}_{k \text{ بار}} \cong \underbrace{\mathbb{Z}_2 \oplus \cdots \oplus \mathbb{Z}_2}_{k \text{ بار}}$$

که نتیجه می‌دهد $|F/2F| = 2^k$. به طریق مشابه، چون Y پایه‌ای با r عضو برای F است، $|F/2F| = 2^r$. در نتیجه $2^k = 2^r$ و $k = r$. □

فرض کنید F گروه آبلی آزاد متناهیاً تولید شده باشد. تعداد عناصر پایه‌ی F را که به طور یکتا تعیین می‌شود رتبه‌ی F گوییم و با $\operatorname{rank}(F)$ نشان می‌دهیم.

چون هر گروه آبلی متناهیاً تولید شده تصویر همریخت یک گروه آبلی آزاد با رتبه‌ی متناهی است، برای تعیین ساختار گروه‌های آبلی متناهیاً تولید شده ابتدا باید زیرگروه‌های گروه آبلی آزاد را بررسی کنیم. برای انجام این کار ابتدا به لم زیر نیاز داریم که اثبات آن ساده است و به عنوان تمرین واگذار می‌شود.

لم ۶.۲.۶. فرض کنید F یک گروه آبلی آزاد با رتبه‌ی k باشد. اگر $\{x_1, x_2, \ldots, x_k\}$ پایه‌ای برای F باشد و $n \in \mathbb{Z}$، آنگاه به ازای هر $1 \leq i, j \leq k$، $i \neq j$،

$$\{x_1, x_2, \ldots, x_{j-1}, x_j + nx_i, x_{j+1}, \ldots, x_k\}$$

نیز پایه‌ای برای F است. □

گروه $\mathbb{Z}$ را در نظر بگیرید $\mathbb{Z}$ گروه آبلی آزاد از رتبه‌ی ۱ با پایه‌ی $\{1\}$ است. هر زیرگروه ناصفر $\mathbb{Z}$ نیز (به ازای یک $n \in \mathbb{N}$) به صورت $n\mathbb{Z}$، و بنابراین آزاد و با پایه‌ی $\{n\}$ است. این نتیجه را در قضیه بعد تعمیم می‌دهیم. در واقع ثابت می‌کنیم زیرگروه‌های ناصفر یک گروه آبلی آزاد با رتبه‌ی متناهی، آزاد هستند و پایه‌ی هر زیرگروه ناصفر را می‌توان با استفاده از پایه‌ی گروه آبلی آزاد یافت. متذکر می‌شویم که این مطلب در حالت کلی درست است (صفحه‌ی ۷۹ از کتاب مرجع [۱۲] را ببینید) ولی ما آن را در حالتی که رتبه‌ی F متناهی باشد، ثابت می‌کنیم.

قضیه ۷.۲.۶. فرض کنید F گروه آبلی آزاد با رتبه‌ی k، $\{0\} \neq H \leq F$ باشد. در این صورت پایه‌ای مثل $\{x_1, x_2, \ldots, x_k\}$ برای F و عدد صحیح r، $(1 \leq r \leq k)$ و اعداد صحیح مثبت m_1، m_2، ...، m_r وجود دارند طوری که $m_{i-1} | m_i$، $2 \leq i \leq r$ طوری که $\{m_1 x_1, m_2 x_2, \ldots, m_r x_r\}$ پایه‌ای برای H است.

اثبات. به استقرا روی k عمل می‌کنیم. اگر $k = 1$، آنگاه $F = \langle x_1 \rangle$ و چون هر زیرگروه یک گروه دوری، دوری است H نیز دوری است. پس $m_1 > 0$ وجود دارد که $H = \langle m_1 x_1 \rangle$. حال فرض کنید مساله برای همه‌ی گروه‌های آبلی آزاد با رتبه‌ی کمتر از k درست باشد. فرض کنید S مجموعه‌ی همه‌ی اعداد طبیعی m باشد که به ازای آن‌ها پایه‌ی $\{y_1, \ldots, y_k\}$ برای F و اعداد صحیح n_2، n_3، ...، n_k وجود داشته باشد که $my_1 + n_2 y_2 \cdots + n_k y_k \in H$؛ یعنی S برابر مجموعه‌ی زیر است

$$S = \{m \in \mathbb{N} \mid \exists \{y_1, \ldots, y_k\} \text{ پایه‌ی } F \text{ و } \exists n_2, n_3, \ldots, n_k \in \mathbb{Z}, \\ my_1 + n_2 y_2 + \cdots + n_k y_k \in H\}.$$

چون $H \neq \{0\}$، $S \neq \emptyset$. پس S کوچک‌ترین عضو دارد ، مثلاً m_1. بنابراین طبق خاصیت S، پایه‌ی $\{y_1, y_2, \ldots, y_k\}$ از F و اعداد صحیح n_2، n_3، ...، n_k وجود دارند که $h = m_1 y_1 + n_2 y_2 + \cdots + n_k y_k \in H$. به علاوه برای هر پایه‌ی $\{z_1, z_2, \ldots z_k\}$ از F، اگر اعداد صحیح s_1، s_2، ...، s_k وجود داشته باشند که $s_1 > 0$ و

$$s_1 z_1 + s_2 z_2 + \cdots + s_k z_k \in H,$$

آنگاه $m_۱ \leq s_۱$. اکنون بنا به الگوریتم تقسیم اعداد صحیح r_i و q_i وجود دارند طوری که

$$n_i = m_۱q_i + r_i, \quad ۰ \leq r_i < m_۱, \quad i = ۲, ۳, \ldots, k.$$

بنابراین

$$h = m_۱(y_۱ + q_۲y_۲ + \cdots + q_ky_k) + r_۲y_۲ + \cdots + r_ky_k.$$

قرار می‌دهیم $x_۱ = y_۱ + q_۲y_۲ + \cdots + q_ky_k$. چون $\{x_۱, y_۲, \ldots, y_k\}$، و هر مجموعه‌ای که با تعویض ترتیب عناصر این مجموعه به دست بیاید، پایه‌ای برای Y است، بنا به انتخاب $m_۱$، باید داشته باشیم $r_i = ۰$، $۱ \leq i \leq k$. بنابراین $m_۱x_۱ = h \in H$. فرض کنید $K = \langle y_۲, \ldots, y_k\rangle$. در این صورت K گروه آبلی آزاد با رتبه‌ی $k - ۱$ است و $F = \langle x_۱\rangle \oplus K$. ادعا می‌کنیم $H = \langle m_۱x_۱\rangle \oplus (H \cap K)$. فرض کنید $a \in H$. پس اعداد صحیح t_i، $۱ \leq i \leq k$، وجود دارند که $a = t_۱x_۱ + t_۲y_۲ + \cdots + t_ky_k$. بنا به الگوریتم تقسیم اعداد صحیح $q_۱$ و $r_۱$ وجود دارند که $t_۱ = q_۱m_۱ + r_۱$، $۰ \leq r_۱ \leq m_۱$. در نتیجه

$$r_۱x_۱ + t_۲y_۲ + \cdots + t_ky_k = a - q_۱m_۱x_۱ \in H.$$

بنابراین، بنا به انتخاب $m_۱$، $r_۱ = ۰$. از این‌رو $t_۲y_۲ + \cdots + t_ky_k \in H$ و

$$a = q_۱(m_۱x_۱) + t_۲y_۲ + \cdots + t_ky_k \in \langle m_۱x_۱\rangle + (H \cap K).$$

اکنون چون $F = \langle x_۱\rangle \oplus K$ داریم

$$H = \langle m_۱x_۱\rangle \oplus (H \cap K).$$

اگر $H \cap K = \{۰\}$، آنگاه $H = \langle m_۱x_۱\rangle$ و مساله حل است. فرض کنید $H \cap K \neq \{۰\}$. بنابراین $H \cap K$ زیرگروه ناصفری از گروه آبلی آزاد K است. در نتیجه بنا به فرض استقرا، پایه‌ی $\{x_۲, \ldots, x_k\}$ از K و اعداد صحیح مثبت r، $m_۲$، $\ldots$، m_k وجود دارند که $\{m_۲x_۲, \ldots, m_kx_k\}$ پایه‌ای برای $H \cap K$ و $m_{i-۱} | m_i$، $۲ \leq i \leq r$. اکنون $\{x_۱, \ldots, x_k\}$ پایه‌ای برای F و $\{m_۱x_۱, \ldots, m_kx_k\}$ پایه‌ای برای H است. تنها تحقیق $m_۱ | m_۲$ باقی‌مانده است. بنا به الگوریتم تقسیم، اعداد صحیح r و q وجود دارند که $m_۲ = qm_۱ + r$، $۰ \leq r < m_۱$. اکنون چون $\{x_۲, x_۱ + qx_۲, x_۳, \ldots, x_k\}$ پایه‌ای برای F است و

$$x_۲ + m_۱(x_۱ + qx_۲) = m_۱x_۱ + m_۲x_۲ + ۰x_۳ + \cdots + ۰x_k \in H,$$

بنا به خاصیت $m_۱$، $r = ۰$. بنابراین $m_۱ | m_۲$. □

قضیه‌ی بعدی به قضیه‌ی اساسی گروه‌های آبلی متناهیاً تولید شده موسوم است.

قضیه ۸.۲.۶. اگر $G \neq \{۰\}$ گروه آبلی متناهیاً تولید شده باشد، آنگاه G با حاصل‌جمع مستقیم تعداد متناهی گروه‌های دوری یکریخت است، که مرتبه‌ی جمع‌وندهای متناهی (در صورت وجود)، به ترتیب، برابر $m_۱$، $m_۲$، $\ldots$، m_r است؛ با $m_۱ > ۱$ و $m_i | m_{i+۱}$، $۱ \leq i \leq r - ۱$.

اثبات. فرض کنید G، k مولد داشته باشد. بنا به نتیجه ۳.۲.۶، G تصویر همریخت یک گروه آبلی آزاد F با رتبه‌ی k است. پس $K \leq F$ وجود دارد که $G \cong F/K$. اگر $K = \{۰\}$ در این صورت $G \cong F \cong \underbrace{\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}}_{k}$. حال فرض کنید $K \neq \{۰\}$. بنا به قضیه‌ی ۷.۲.۶، پایه‌ی $\{x_۱, x_۲, \ldots, x_k\}$ برای F و عدد صحیح r، $۱ \leq r \leq k$، و اعداد صحیح مثبت $m_۱$، $m_۲$، $\ldots$، m_r با $m_{i-۱} | m_i$، $۲ \leq i \leq r$ وجود دارند و $\{m_۱x_۱, \ldots, m_rx_r\}$ پایه‌ای برای K است. اکنون $F = \langle x_۱\rangle \oplus \cdots \oplus \langle x_۲\rangle$ و $K = \langle m_۱x_۱\rangle \oplus \cdots \oplus \langle m_rx_r\rangle$. بنا به تمرین ۱۲ از صفحه‌ی ۱۰۴، داریم

$$\begin{aligned} G \cong F/K &\cong \frac{\langle x_۱\rangle}{\langle m_۱x_۱\rangle} \oplus \cdots \oplus \frac{\langle x_r\rangle}{\langle m_rx_r\rangle} \oplus \langle x_{r+۱}\rangle \oplus \cdots \oplus \langle x_k\rangle \\ &\cong \mathbb{Z}_{m_۱} \oplus \cdots \oplus \mathbb{Z}_{m_r} \oplus \mathbb{Z} \oplus \cdots \oplus \mathbb{Z}. \end{aligned}$$

□

فرض کنید G گروه آبلی باشد. در این صورت مجموعه‌ی $T(G)$ متشکل از عناصر با مرتبه‌ی متناهی در G یک زیرگروه G است، که آن را زیرگروه تاب‌دار G گوییم. به علاوه $G/T(G)$ بی‌تاب است. زیرا اگر $a+T(G)\in G/T(G)$ و $n\in\mathbb{Z}$ طوری باشند که $n(a+T(G))=T(G)$، آنگاه $na\in T(G)$ و مرتبه‌ی na متناهی است؛ یعنی مرتبه‌ی a متناهی است. پس $a\in T(G)$. از این‌رو $G/T(G)$ بی‌تاب است.

با استفاده از قضیه‌ی اساسی گروه‌های آبلی متناهیاً تولید شده ۸.۲.۶، قضیه‌ی بعدی به راحتی ثابت می‌شود که آن را به عنوان تمرین واگذار می‌کنیم.

قضیه ۹.۲.۶. گروه آبلی متناهیاً تولید شده $G\neq\{0\}$، بی‌تاب است اگر و تنها اگر G گروه آبلی آزاد متناهیاً تولید شده باشد. □

بنابراین اگر G گروه آبلی متناهیاً تولید شده باشد، آنگاه $G/T(G)$ گروه آبلی آزاد متناهیاً تولید شده است.

قضیه ۱۰.۲.۶. فرض کنید G گروه آبلی متناهیاً تولید شده باشد. در این صورت گروه آبلی آزاد متناهیاً تولید شده F وجود دارد که $G=T(G)\oplus F$.

اثبات. چون $G/T(G)$ گروه آبلی آزاد متناهیاً تولید شده است، پایه‌ی

$$\{a_1+T(G),\dots,a_k+T(G)\}$$

برای آن وجود دارد. قرار می‌دهیم $F=\langle a_1,\dots,a_k\rangle$ و ادعا می‌کنیم که $\{a_1,\dots,a_k\}$ پایه‌ای برای F است. تنها باید ثابت کنیم این مجموعه مستقل خطی است. اگر $n_i\in\mathbb{Z}$ و $n_1a_1+\cdots+n_ka_k=0$، آنگاه $n_1(a_1+T(G))+\cdots+n_k(a_k+T(G))=T(G)$ و چون $\{a_1+T(G),\dots,a_k+T(G)\}$ پایه‌ای برای $G/T(G)$ است، $n_i=0$، $1\leq i\leq k$. بنابراین F آزاد است. ادعا می‌کنیم $G=T\oplus F$. فرض کنید $g\in G$، در این صورت $g+T(G)\in G/T(G)$. بنابراین اعداد صحیح m_1، ...، m_k وجود دارند که $g+T(G)=m_1(a_1+T(G))+\cdots+m_k(a_k+T(G))$.
بنابراین $g-(m_1a_1+\cdots+m_ka_k)\in T(G)$ و در نتیجه $g\in T(G)+F$ و $G=T+F$. هم‌چنین چون $T(G)$ تاب‌دار و F بی‌تاب است، $T(G)\cap F=\{0\}$. بنابراین $G=T(G)\oplus F$. □

اکنون یکتایی تجزیه‌ی یک گروه آبلی آزاد متناهیاً تولید شده را ثابت می‌کنیم:

قضیه ۱۱.۲.۶. فرض کنید F یک گروه آبلی متناهیاً تولید شده باشد ؛ که در آن F گروه آبلی آزاد با رتبه‌ی r و G_i، $2\leq i\leq r$، گروه دوری مرتبه‌ی m_i است که $m_{i-1}|m_i$. در این صورت اعداد r و m_1، ...، m_s به طور یکتا معین می‌شوند.

اثبات. به وضوح شمول $G_1\oplus\cdots\oplus G_s\subseteq T(G)$ برقرار است. ادعا می‌کنیم که تساوی برقرار است. به ازای هر عضو دلخواه $g\in T(G)$، اعضای $g_1\in G$ و $x\in F$ وجود دارند که $g=g_1+\cdots+g_s+x$. بنابر این $g-(g_1+\cdots+g_s)=x\in T(G)\cap F=\{0\}$ و $g=g_1+\cdots+g_s\in G_1\oplus\cdots\oplus G_s$. در نتیجه داریم $T(G)=G_1\oplus\cdots\oplus G_s$. اکنون چون

$$G/T(G)=\frac{T(G)+F}{T(G)}\cong\frac{F}{T\cap P}=\frac{F}{\{0\}}\cong F,$$

$r=\operatorname{rank}(F)=\operatorname{rank}(G/T(G))$ به طور یکتا توسط G تعیین می‌شود. حال فرض کنید p_1، ...، p_t اعداد اول متمایزی باشند که حداقل یکی از اعداد m_1، m_2، ...، m_s را عدد می‌کنند. می‌نویسیم

$$m_i=p_1^{m_{i1}}p_2^{m_{i2}}\cdots p_t^{m_{it}}\ ,\ m_{ij}\geq 0.$$

در این صورت $G_i\cong\mathbb{Z}_{p_1^{m_{i1}}}\oplus\mathbb{Z}_{p_2^{m_{i2}}}\oplus\cdots\oplus\mathbb{Z}_{p_t^{m_{it}}}$ ، که در آن $\mathbb{Z}_{p_i^0}=\{0\}$. بنابراین مولفه‌ی p_j- اولیه‌ی $T(G)$ عبارت است از

$$T(p_j)=\mathbb{Z}_{p_j^{m_{1j}}}\oplus\mathbb{Z}_{p_j^{m_{2j}}}\oplus\cdots.$$

نوع این گروه عبارت است از $(m_{1j},m_{2j},\dots)$، و بنابراین G به طور یکتا اعداد صحیح m_{ij} و بنابراین m_i را مشخص می‌کند. □

تمرین‌ها

۱. فرض کنید G گروه آبلی باشد، p عدد اول و $n \in \mathbb{Z}$، نشان دهید :
(الف) $G[n] = \{g \in G | ng = ۰\}$ زیرگروه G است.
(ب) $nG = \{ng | g \in G\}$ زیرگروه G است.
(ج) $G(p) = \{g \in G \mid \exists s \geq ۰, \quad O(g) = p^s\}$ زیرگروه G است.
(د) $G/G[n] \cong nG$.

۲. گروه‌های آبلی با مرتبه‌های داده را رده‌بندی کنید.
(الف) ۹ (ب) ۱۶ (ج) ۲۷ (د) ۳۲ (هـ) ۶۰
(و) ۸۰ (ز) ۱۰۸ (ح) ۲۴۰ (ی) ۵۴۰ (ک) ۳۲۴

۳. گروه‌های آبلی با مرتبه‌ی داده شده را رده‌بندی کنید (p، q، r اعداد اول متمایز)
(الف) $p^۵$، (ب) $p^۶$ (ج) $pq^۲$، (د) $p^۲q^۲$
(هـ) $p^۳q^۲$ (و) $p^۲q^۳r^۴$ (ز) $p^۵qr^۲$

۴. نوع و شمارنده‌های مقدماتی مولفه‌های گروه‌های زیر را بیابید.
(الف) $\mathbb{Z}_{۱۲} \oplus \mathbb{Z}_{۶۵} \oplus \mathbb{Z}_{۲۷}$ (ب) $\mathbb{Z}_{۱۰} \oplus \mathbb{Z}_{۳۰} \oplus \mathbb{Z}_{۱۲۰}$

۵. فرض کنید $G = H \oplus K$ و $H \leq G_۱ \leq G$. نشان دهید $G_۱ = H \oplus (G_۱ \cap K)$.

۶. نشان دهید یک گروه آبلی متناهی دوری است اگر و تنها اگر هر مولفه‌ی اولیه‌ی آن دوری باشد.

۷. نشان دهید یک گروه آبلی مرتبه‌ی ۸ دوری است اگر و تنها اگر فقط یک زیرگروه مرتبه‌ی ۲ داشته باشد.

۸. فرض کنید G گروه آبلی باشد و $|G| = p_۱p_۲ \cdots p_n$، که در آن p_i ها اعداد اول متمایزند. نشان دهید G دوری است.

۹. اگر G گروه آبلی متناهی باشد و $n \mid |G|$، نشان دهید G یک زیرگروه با شاخص n دارد.

۱۰. فرض کنید G یک p- گروه آبلی متناهی و $k \geq ۱$ عدد صحیح باشد.
(الف) اگر G دوری مرتبه‌ی p^n باشد، نشان دهید

$$|p^kG| = \begin{cases} p^k & k \leq n \\ p^n & k > n \end{cases}, \; |G[p^k]| = \begin{cases} p^{n-k} & k \leq n \\ ۱ & k > n \end{cases}$$

(ب) اگر $G = G_۱ \oplus \cdots \oplus G_r$، نشان دهید

$$G[p^k] = G_۱[p^k] \oplus \cdots \oplus G_r[p^k] \quad \text{و} \quad p^kG = p^kG_۱ \oplus \cdots \oplus p^kG_r.$$

(ج) اگر نوع G، $(n_۱, n_۲, \ldots, n_r)$ باشد، نشان دهید نوع $G[p]$، $(\underbrace{۱, ۱, \ldots, ۱}_{r})$ است و در صورتی که $pG \neq \{۰\}$، نشان دهید نوع pG عبارت است از $(n_۱ - ۱, n_۲ - ۱, \ldots, n_s - ۱)$، که $n_s > ۱$، $n_{s+۱} = \cdots = n_r = ۱$.

۱۱. فرض کنید G یک p- گروه آبلی متناهی با نوع $(n_۱, n_۲, \ldots, n_r)$ باشد.
(الف) $|G[p]| = p^r$؛ یعنی تعداد عناصر مرتبه‌ی p برابر $p^r - ۱$ است.
(ب) فرض کنید s تعداد iهایی باشد که $n_i > ۱$ (احتمالاً $s = ۰$) نشان دهید $G[p^۲] = p^{r+s}$. یعنی G، $p^r(p^s - ۱)$ عضو مرتبه‌ی $p^۲$ دارد.

۱۲. اگر G و H دو گروه آبلی متناهی باشند که تعداد عناصر آن‌ها از مرتبه‌ی m، به ازای هر m، برابر است، نشان دهید $G \cong H$.

۱۳. اگر G و H گروه‌های آبلی متناهی باشند و $G \oplus G \cong H \oplus H$ نشان دهید $G \cong H$.

۱۴. اگر G و H و K گروه‌های آبلی متناهی باشند و $G \oplus H \cong G \oplus K$ نشان دهید $H \cong K$.

۱۵. فرض کنید G گروه آبلی باشد و $|G| = mn$، که در آن $\gcd\{m, n\} = ۱$. نشان دهید $G = mG \oplus nG$.

۱۶. نشان دهید هر زیرگروه یک گروه آبلی متناهیاً تولید شده مجدداً متناهیاً تولید شده است.

۱۷. فرض کنید G یک گروه آبلی متناهیاً تولید شده و بی‌تاب باشد. نشان دهید G گروه آبلی آزاد است.

۱۸. نشان دهید گروه جمعی $\mathbb{Q}$ گروه آبلی آزاد نیست.

۱۹. ثابت کنید گروه ضربی $\mathbb{Q}^{\times}$ یک گروه آبلی آزاد است.

فصل ۷

سری زیر گروه‌ها

با مفهوم سری برای گروه در فصل‌های قبل آشنا شده‌ایم. به خصوص سری‌هایی مثل سری مشتق متناظر با گروه‌های حل‌پذیرند. در این فصل سری زیر گروه‌ها را بررسی کرده و رده‌هایی مهم از گروه‌ها را معرفی و خواص آن‌ها را بررسی می‌کنیم.

۱.۷ گروه‌های حل‌پذیر

در این بخش گروه‌های حل‌پذیر را بررسی می‌کنیم. اغلب نتایج این بخش قبلاً به عنوان تمرین، در فصل ۳، مطرح شده‌اند. یادآوری می‌کنیم که اگر G گروه باشد و $z, y \in G$، آنگاه تعویض‌گر x و y عبارت است از

$$[x, y] = x^{-1}y^{-1}xy.$$

چون

$$[x, y] = 1 \iff xy = yx,$$

x و y تعویض می‌شوند اگر و تنها اگر تعویض‌گر آن‌ها بدیهی باشد.

مثال ۱.۱.۷. اگر x و y دو عضو یک گروه G باشند، نشان دهید $[x, y]^{-1} = [y, x]$. بنابراین معکوس یک تعویض‌گر مجدداً تعویض‌گر است.

حل $[x, y]^{-1} = (x^{-1}y^{-1}xy)^{-1} = y^{-1}x^{-1}yx = [y, x]$. □

یادآوری می‌کنیم که زیرگروه مشتق گروه G زیرگروه تولید شده توسط همه‌ی تعویض‌گرهای $[x, y] = x^{-1}y^{-1}xy$، که در آن $x, y \in G$، است که با G' نشان داده می‌شود: $G' = \langle [x, y] \mid x, y \in G \rangle$؛ و در حالت کلی اگر H و K زیرگروه‌هایی از G باشند $[H, K] = \langle [h, k] \mid h \in H, k \in K \rangle$ تعویض‌گر H و K نامیده می‌شود.

مثال ۲.۱.۷. اگر H و K دو زیرگروه G باشند و $\alpha \in \operatorname{End} G$، آنگاه

$$\alpha([H, K]) = [\alpha(H), \alpha(K)].$$

حل فرض کنید $h \in H$ و $k \in K$. داریم

$$\alpha([h, k]) = \alpha\left(h^{-1}k^{-1}hk\right) = \alpha(h)^{-1}\alpha(k)^{-1}\alpha(h)\alpha(k) = [\alpha(h), \alpha(k)].$$

بنابراین تصویر هر تعویض‌گر تحت هر همریختی α مجدداً تعویض‌گر است، این یعنی هر مولد $\alpha([H, K])$ مولدی از $[\alpha(H), \alpha(K)]$ و هر مولد $[\alpha(H), \alpha(K)]$ مولدی از $\alpha([H, K])$ است. از این‌رو $\alpha([H, K]) = [\alpha(H), \alpha(K)]$. به طور دقیق‌تر، اگر داشته باشیم، $v = u_1^{n_1}u_2^{n_2}\cdots u_k^{n_k} \in [H, K]$، که در آن u_iها تعویض‌گر و n_iها اعداد صحیح هستند، آنگاه چون α همریختی است، داریم $\alpha(v) = \alpha(u_1)^{n_1}\alpha(u_2)^{n_2}\cdots\alpha(u_k)^{n_k}$ و بنابراین

$\alpha([H,K]) \leq [\alpha(H),\alpha(K)]$. بر عکس فرض کنید $v = u_1^{n_1}u_2^{n_2}\cdots u_k^{n_k}$ عضوی از $[\alpha(H),\alpha(K)]$ باشد، که در آن $u_i = [\alpha(h_i),\alpha(k_i)]$، $h_i \in H$، $k_i \in K$. چون $u_i = [\alpha(h_i),\alpha(k_i)] = \alpha([h_i,u_i]) \in \alpha([H,K])$، و $\alpha([H,K])$ زیرگروه G است، داریم $v = u_1^{n_1}u_2^{n_2}\cdots u_k^{n_k} \in \alpha([H,K])$. پس $\alpha([H,K)) = [\alpha(H),\alpha(K)]$. □

یادآوری می‌کنیم که سری مشتق G عبارت است است

$$G = G^{(0)} \geq G' \geq G'' \geq \cdots \geq G^{(n)} \geq G^{(n+1)} \geq \cdots,$$

که در آن $G^{(i+1)} = (G^{(i)})'$، پس $G^{(1)} = G'$، $G^{(2)} = G''$، $G^{(3)} = G'''$ و غیره. در نهایت یادآوری می‌کنیم که G را حل‌پذیر گوییم، اگر به ازای nای داشته باشیم $G^{(n)} = \{1\}$، بنابراین دنباله‌ای از زیرگروه‌های G به دست یعنی سری مشتق به $\{1\}$ ختم شود، و کوچک‌ترین nای که $G^{(n)} = \{1\}$ را طول حل‌پذیری G گوییم.

مثال ۳.۱.۷. نشان دهید گروه نابدیهی حل‌پذیر G ساده است اگر و تنها اگر عدد اول p وجود داشته باشد که $G \cong \mathbb{Z}_p$.

حل فرض کنید G گروه حل‌پذیر و ساده باشد. پس عدد صحیح مثبت d وجود دارد که $G^{(d)} = \{1\}$. اگر $G' = G$، آنگاه به ازای هر $n \in \mathbb{N}$ داریم $G^{(n)} = G$. به ویژه $G^{(d)} = G = \{1\}$، که تناقض است. پس G' زیرگروه سره‌ای از G است. چون G ساده و G' زیرگروه نرمال سره‌ای از G است، $G' = \{1\}$. بنابراین G آبلی است. چون هر زیرگروه یک گروه آبلی، نرمال است، G هیچ زیرگروه نابدیهی ندارد. از این‌رو بنا به تمرین ۲۱ از صفحه‌ی ۷۰، G دوری، متناهی و از مرتبه‌ی عددی اول ، مثل p است، این یعنی $G \cong \mathbb{Z}_p$.
عکس مطلب واضح است. □

اکنون تعدادی از خواص گروه‌های حل‌پذیر را می‌یابیم. اثبات این خواص در فصل ۳ به عنوان تمرین مطرح شده بود. اگر رده‌ای از گروه‌ها (مثلاً رده‌ی گروه‌های حل‌پذیر) در اختیار داشته باشیم، گروه‌های این رده همگی یک خاصیت $\mathcal{P}$ (مثلاً هر گروهی که در رده‌ی گروه‌های حل‌پذیر باشد خاصیت حل‌پذیری دارد) دارند. به طور طبیعی سه سوال در مورد این رده مطرح می‌شود:
(الف) آیا اگر G یک گروه با خاصیت $\mathcal{P}$ باشد، زیرگروه‌های آن نیز خاصیت $\mathcal{P}$ را دارند؟
(ب) آیا اگر G یک گروه با خاصیت $\mathcal{P}$ باشد، گروه‌های خارج‌قسمتی آن نیز چنین هستند؟
(ج) آیا این رده تحت توسیع بسته است؛ یعنی اگر N زیرگروه نرمال گروه G باشد طوری که N و G/N هر دو خاصیت $\mathcal{P}$ را دارند، آیا G نیز واجد خاصیت $\mathcal{P}$ است؟
جواب هر سه سوال فوق در مورد گروه‌های حل‌پذیر مثبت است.

قضیه ۴.۱.۷. اگر G حل‌پذیر باشد، آنگاه هر زیرگروه G حل‌پذیر است.

اثبات. چون G حل‌پذیر است عدد طبیعی d وجود دارد که $G^{(d)} = \{1\}$. فرض کنید $H \leq G$. داریم (تمرین ۴ را ببینید)

$$H' = [H,H] \leq [G,G] = G'.$$

در نتیجه به صورت استقرایی می‌توان ثابت کرد به ازای هر $n \in \mathbb{N}$،

$$H^{(n)} \leq G^{(n)}.$$

پس $H^{(d)} \leq G^{(d)} = \{1\}$ و $H^{(d)} = \{1\}$، این یعنی H حل‌پذیر است. به علاوه ثابت کرده‌ایم که طول حل‌پذیری H کوچکتر یا مساوی طول حل‌پذیری G است. □

مثال ۵.۱.۷. اگر F میدان دلخواهی باشد $\mathrm{GL}_n(F)$ برای $n \geq 3$ حل‌پذیر نیست.

حل فرض کنید E_{ij} ماتریسی $n \times n$ باشد که درایه‌های i,j آن برابر ۱ و سایر درایه‌ها صفر باشد. در این صورت $E_{ij}E_{jt} = E_{it}$ و برای $j \neq k$، داریم $E_{ij}E_{kt} = 0$. به علاوه $(I + E_{ij})^{-1} = I - E_{ij}$. اکنون فرض کنید $H = \langle I + E_{ij} \mid i \neq j \rangle$. اندیس‌های

متمایز i، j و k را اختیار می‌کنیم. داریم

$$\begin{aligned}[I+E_{ik}, I+E_{kj}] &= (I+E_{ik})^{-1}(I+E_{kj})^{-1}(I+E_{ik})(I+E_{kj}) \\ &= (I-E_{ik})(I-E_{ij})(I+E_{ik})(I+E_{xj}) \\ &= (I-E_{kj}-E_{ik}+E_{ij})(I+E_{kj}+E_{ik}+E_{ij}) \\ &= I+E_{ij},\end{aligned}$$

که نتیجه می‌دهد $I+E_{ij} \in H'$ و $H \subseteq H'$. در نتیجه $H = H' = H''$ و به طور کلی، به استقرا، به ازای n داریم $H = H^{(n)} \neq \{1\}$. بنابراین H حل‌پذیر نیست و $\mathrm{GL}_n(F)$ نیز، بنا به قضیه‌ی قبل، می‌تواند حل‌پذیر نباشد. □

مثال ۶.۱.۷. فرض کنید G گروه باشد. ثابت کنید به ازای هر n، $G^{(n)}$ یک زیرگروه کاملاً پایای G و بنابراین در G مشخصه است.

حل به استقرا روی n عمل می‌کنیم. برای $n = 0$ داریم $G^{(0)} = G$ و چیزی برای اثبات نیست. حال فرض کنید $n > 0$ و $G^{(n)}$ زیرگروه کاملاً پایای G باشد و $\alpha \in \mathrm{Aut}\, G$. بنا به مثال ۲.۱.۷ و فرض استقرا داریم

$$\begin{aligned}\alpha\left(G^{(n+1)}\right) &= \alpha\left(\left[G^{(n)}, G^{(n)}\right]\right) \\ &= \left[\alpha\left(G^{(n)}\right), \alpha\left(G^{(n)}\right)\right] \leq \left[G^{(n)}, G^{(n)}\right] = G^{(n+1)}.\end{aligned}$$

پس به ازای هر $n \in \mathbb{N}$، $G^{(n)}$ زیرگروه کاملاً پایای G است. □

قضیه ۷.۱.۷. هر گروه خارج‌قسمتی یک گروه حل‌پذیر، حل‌پذیر است.

اثبات. فرض کنید G گروه باشد و $N \trianglelefteq G$. در این صورت

$$\begin{aligned}(G/N)' &= [G/N, G/N] \\ &= \langle [aN, bN] \,|\, aN, bN \in G/N \rangle \\ &= \langle [a,b]N \mid a, b \in G \rangle \\ &= \frac{G'N}{N}.\end{aligned}$$

پس به استقرا می‌توان ثابت کرد

$$(G/N)^{(n)} = \frac{G^{(n)}N}{N}.$$

بنابراین اگر G حل‌پذیر باشد و $G^{(n)} = \{1\}$، آنگاه

$$(G/N)^{(n)} = \frac{G^{(n)}N}{N} = \frac{N}{N} = \{N\},$$

یعنی G/N حل‌پذیر است. به علاوه ثابت کرده‌ایم طول حل‌پذیری G/N کوچک‌تر یا مساوی با طول حل‌پذیری G است. □

رده‌ی گروه‌های حل‌پذیر نسبت به توسیع بسته است، یعنی

قضیه ۸.۱.۷. فرض کنید G گروه باشد و $N \trianglelefteq G$. اگر N و G/N حل‌پذیر باشند، آنگاه G نیز حل‌پذیر است.

اثبات. چون G/N حل‌پذیر است، عدد n وجود دارد که $(G/N)^{(n)} = \{N\}$. بنابراین $\frac{G^{(n)}N}{N} = \{N\}$، یعنی $G^{(n)}N = N$ و $G^{(n)} \leq N$. اکنون چون N حل‌پذیر است، $G^{(n)}$ حل‌پذیر است و عدد d وجود دارد که $(G^{(n)})^{(d)} = \{1\}$. این یعنی $G^{(n+d)} = \{1\}$. این یعنی G حل‌پذیر است. □

فرض کنید G گروه باشد. بنا به مثال ۶.۱.۷، G' زیرگروه کاملاً پایای G است. پس G' در G نرمال است و می‌توان گروه خارج‌قسمتی G/G' را تشکیل داد. این گروه آبلی است:

قضیه ۹.۱.۷. فرض کنید G گروه باشد و $H \trianglelefteq G$. در این صورت G/H آبلی است اگر و تنها اگر $G' \leq H$. به ویژه G/G' آبلی است.

اثبات. فرض کنید $H \trianglelefteq G$. به ازای هر $x, y \in G$ داریم

$$\begin{aligned} x^{-1}y^{-1}xy \in H &\iff (yx)^{-1}xy \in H \\ &\iff xyH = yxH \\ &\iff xHyH = yHxH. \end{aligned}$$

بنابراین اگر $G' \leq H$، آنگاه $[x, y] \in G' \leq H$ و حالت ($\Longrightarrow$) در رابطه‌ی بالا نشان می‌دهد که G/H آبلی است. به ویژه، با قرار دادن G' به جای H، G/G' آبلی است. حال اگر G/H آبلی باشد. حالت ($\Longleftarrow$) در رابطه‌ی بالا نشان می‌دهد که هر مولد G' در H قرار دارد و بنابراین $G' \leq H$. □

یک سری (از G به $\{1\}$ یا از $\{1\}$ به G) عبارت است از زنجیر

$$G = G_0 \trianglerighteq G_1 \trianglerighteq \cdots \trianglerighteq G_n = \{1\}$$

از زیرگروه‌های G که در آن G_{i+1} در G_i نرمال است. گروه خارج‌قسمتی G_i/G_{i+1} را یک عامل سری گوییم. سری آبلی گوییم هرگاه عوامل آن آبلی باشد. به ازای هر i، طبق قضیه‌ی ۹.۱.۷، $G^{(i)}/G^{(i+1)}$ آبلی است. بنابراین سری

$$G = G^{(0)} \trianglerighteq G^{(1)} \trianglerighteq G^{(2)} \trianglerighteq \cdots$$

سری نرمال (یعنی یک سری که جملات آن در G نرمال هستند) است که عوامل آن آبلی‌اند. اگر G حل‌پذیر باشد، آنگاه به ازای nای داریم $G^{(n)} = \{1\}$. پس در این حالت سری

$$G = G^{(0)} \trianglerighteq G^{(n)} \trianglerighteq \cdots \trianglerighteq G^{(n)} = \{1\}$$

یک سری با عوامل آبلی است.
شرط لازم و کافی برای این که G حل‌پذیر باشد این است که یک سری آبلی برای G وجود داشته باشد. در واقع فرض کنید یک سری آبلی برای G وجود داشته باشد. به استقرا نشان می‌دهیم $G^{(i)} \leq G_i$. برای $i = 0$ واضح است. حال اگر $G^{(i)} \leq G_i$، آنگاه چون G_i/G_{i+1} آبلی است، داریم $G_i' \leq G_{i+1}$. پس

$$G^{(i+1)} = (G^{(i)})' \leq G_i' \leq G_{i+1},$$

و به استقرا به $G^{(i)} \leq G_i$. چون برای $i = n$ داریم $G^{(n)} = \{1\}$، G حل‌پذیر است.

تمرین‌ها

۱. نشان دهید $\mathrm{GL}_2(\mathbb{Z}_3)$ حل‌پذیر است.

۲. فرض کنید H، K دو زیرگروه نرمال گروه G باشند. ثابت کنید $[H, K] \leq H \cap K$.

۳. اگر $H, K \leq G$، ثابت کنید $[H, K] \trianglelefteq \langle H, K \rangle$.

۴. اگر $H_1 \leq H$ و $K_1 \leq K$، نشان دهید $[H_1, K_1] \leq [H, K]$.

۵. فرض کنید $G = H \times K$، نشان دهید
الف) اگر $h_1, h_2 \in H$ و $k_1, k_2 \in K$، آنگاه

$$[(h_1, k_1), (h_2, k_2)] = ([h_1, h_2], [k_1, k_2]).$$

(ب) اگر $H_1, H_2 \leq H$ و $K_1, K_2 \leq K$، آنگاه

$$[H_1 \times K_1, H_2 \times K_2] = [H_1, H_2] \times [K_1, K_2].$$

نتیجه بگیرید $G' = H' \times K'$ و $G^{(n)} = H^{(n)} \times K^{(n)}$.

۶. فرض کنید p، q، و r اعداد اول باشند. نشان دهید هر گروه با مرتبه‌ی (الف) pqr (ب) $p^۲q$ (ج) $p^۲q^۲$ حل‌پذیر است.

۷. فرض کنید G حل‌ناپذیر باشد و $|G| \leq ۱۰۰$، نشان دهید $G \cong A_۵$.

۸. اگر G حل‌ناپذیر باشد و $|G| \leq ۲۰۰$، نشان دهید $|G|$ برابر ۶۰، ۱۲۰، ۱۶۸، یا ۱۸۰ است.

۹. گروه‌های حل‌ناپذیر با مرتبه‌های ۶۰، ۱۲۰، ۱۶۸، و ۱۸۰ ارائه کنید.

۱۰. فرض کنید z، y، x عناصری از یک گروه و n عددی صحیح باشد. ثابت کنید
(الف) $[xy, z] = y^{-۱}[x, z]y[y, z]$ (ب) $[x, yz] = [x, z]z^{-۱}[x, y]z$
(ج) $[x^{-۱}, y] = x[x, y]^{-۱}x^{-۱}$
(د) اگر $[x, y] \in Z(\langle x, y\rangle)$، آنگاه $[x^n, y] = [x, y]^n$

۱۱. فرض کنید H، K، N زیرگروه‌های نرمال گروه G باشند. نشان دهید
(الف) $[H, G] \leq H$.
(ب) $[HK, N] = [H, N][K, N]$.

۱۲. اگر $K_i \trianglelefteq G$، برای $i = ۱, ۲, \ldots, n$ و هر G/K_i حل‌پذیر باشد نشان دهید $G/\bigcap_{i=۱}^{n} K_i$ حل‌پذیر است.

۱۳. اگر H و K دو زیرگروه حل‌پذیر از گروه G باشند و $H \trianglelefteq G$. نشان دهید HK زیرگروه حل‌پذیر G است.

۱۴. نشان دهید موارد زیر برای گروه متناهی $G \neq \{۱\}$ معادل‌اند.
(الف) G حل‌پذیر است.
(ب) هر زیرگروه نرمال غیرهمانی G،یک گروه خارج‌قسمتی آبلی غیرهمانی دارد.
(ج) هر گروه خارج‌قسمتی غیرهمانی G، زیرگروه آبلی نرمال غیرهمانی دارد.

۱۵. اگر $G \neq \{۱\}$ حل‌پذیر باشد، نشان دهید
(الف) G یک گروه خارج‌قسمتی غیرهمانی آبلی دارد.
(ب) G یک زیرگروه آبلی نرمال غیرهمانی دارد.

۱۶. فرض کنید M یک زیرگروه ماکسیمال گروه حل‌پذیر G باشد. نشان دهید $|G : M|$ یا نامتناهی است یا توانی از یک عدد اول.

۲.۷ گروه‌های پوچ‌توان

رده‌ی مهم دیگری از گروه‌ها، رده‌ی گروه‌های پوچ‌توان است. در این بخش خواص اساسی این گروه‌ها را بررسی می‌کنیم. ابتدا زیرگروه‌هایی مهم از گروه داده شده، که به جملات سری مرکزی پائینی معروف‌اند را معرفی می‌کنیم. فرض کنید G یک گروه باشد. قرار می‌دهیم $\Gamma_۱(G) = G$ و به ازای $n \geq ۱$ تعریف می‌کنیم $\Gamma_{n+۱}(G) = [\Gamma_n(G), G]$. پس

$$\begin{aligned} \Gamma_۲(G) &= [\Gamma_۱(G), G] = [G, G] = G' \\ \Gamma_۳(G) &= [\Gamma_۲(G), G] = [G', G] \\ &\vdots \quad \vdots \quad \vdots \end{aligned}$$

بنابراین یک دنباله‌ی

$$G = \Gamma_۱(G) \geq \Gamma_۲(G) \geq \Gamma_۳(G) \geq \cdots$$

از زیرگروه‌های G را داریم. دنباله‌ی فوق را سری مرکزی پائینی G گوییم. دلیل این که چرا به آن مرکزی گوییم در ادامه بحث مشخص می‌شود. در صورتی که به ازای یک n، داشته باشیم $\Gamma_{n+۱}(G) = \{۱\}$ گوییم گروه G پوچ‌توان است. کوچک‌ترین n با این خاصیت را رده‌ی پوچ‌توانی G گوییم. توجه کنید

$$G'' = [G', G'] \leq [G', G] = \Gamma_۳(G).$$

پس به طور استقرایی می‌توان ثابت کرد به ازای هر n، $G^{(n)} \leq \Gamma_{n+1}(G)$. اما لزوماً $G^{(n)}$ با $\Gamma_n(G)$ مساوی نیست. چون $G^{(n)} \leq \Gamma_{n+1}(G)$، هر گروه پوچ‌توان، حل‌پذیر است اما عکس آن درست نیست.

مثال ۱.۲.۷. اگر $G \neq \{1\}$ یک گروه پوچ‌توان باشد، نشان دهید مرکز G نابدیهی است.

حل فرض کنید رده‌ی پوچ‌توانی G برابر c باشد. در این صورت $\Gamma_{c+1}(G) = \{1\}$ و $\Gamma_c(G) \neq \{1\}$. نشان می‌دهیم $\Gamma_c(G) \leq Z(G)$. اگر $u \in \Gamma_c(G)$، آنگاه به ازای هر $g \in G$ داریم

$$[u, g] \in [\Gamma_c(G), G] = \Gamma_{c+1}(G) = \{1\}.$$

بنابراین $[u, g] = 1$ و $ug = gu$. پس $u \in Z(G)$. چون $u \in \Gamma_c(G)$ دلخواه بود، $\Gamma_c(G) \leq Z(G)$. □

مثال ۲.۲.۷. نشان دهید S_3 حل‌پذیر است ولی پوچ‌توان نیست.

حل چون $Z(S_3) = \{(1)\}$، طبق مثال ۱.۲.۷، S_3 پوچ‌توان نیست. اما به سادگی می‌توان دید که $S_3' = A_3$ و $A_3 = \{(1)\}$. پس S_3 یک گروه فراآبلی است. □

قضیه ۳.۲.۷. هر زیرگروه یک گروه پوچ‌توان، پوچ‌توان است.

اثبات. فرض کنید G گروه باشد و $H \leq G$. به استقرا ثابت می‌کنیم $\Gamma_i(H) \subseteq \Gamma_i(G)$. برای $i = 1$ مساله واضح است. زیرا $\Gamma_1(H) = H \subseteq G = \Gamma_1(G)$. فرض کنید $\Gamma_i(H) \subseteq \Gamma_i(G)$. داریم

$$\Gamma_{i+1}(H) = [\Gamma_i(H), H] \subseteq [\Gamma_i(G), G] = \Gamma_{i+1}(G).$$

پس به استقرا ثابت شد برای هر i، $\Gamma_i(H) \subseteq \Gamma_i(G)$. اکنون چون G پوچ‌توان است، به ازای یک c داریم $\Gamma_{c+1}(G) = \{1\}$، که نتیجه می‌دهد $\Gamma_{c+1}(H) \subseteq \Gamma_{c+1}(G) = \{1\}$. بنابراین H پوچ‌توان است. □

دیدیم اگر K زیرگروه نرمال G باشد که K و G/K حل‌پذیرند، آنگاه G نیز حل‌پذیر است. این مطلب در مورد گروه‌های پوچ‌توان درست نیست، یعنی رده‌ی گروه‌های پوچ‌توان تحت توسیع بسته نیست. مثلاً A_3 و S_3/A_3 هر دو پوچ‌توان هستند ، اما S_3 پوچ‌توان نیست، زیرا $Z(S_3) = \{1\}$. ولی قضیه‌ی زیر را در مورد حاصل‌ضرب گروه‌های پوچ‌توان داریم.

قضیه ۴.۲.۷. اگر H و K دو گروه پوچ‌توان باشند، آنگاه $H \times K$ نیز پوچ‌توان است.

اثبات. به استقرا ثابت می‌کنیم $\Gamma_i(H \times K) = \Gamma_i(H) \times \Gamma_i(K)$. برای $i = 1$ مساله واضح است. حال فرض کنید مساله برای i برقرار باشد و حالت $i + 1$ را در نظر می‌گیریم. طبق فرض استقرا و تمرین ۵ از بخش قبل داریم

$$\begin{aligned} \Gamma_{i+1}(H \times K) &= [\Gamma_i(H \times K), H \times K] \\ &= [\Gamma_i(H) \times \Gamma_i(K), H \times K] \\ &= [\Gamma_i(H), H] \times [\Gamma_i(K), K] \\ &= \Gamma_{i+1}(H) \times \Gamma_{i+1}(K). \end{aligned}$$

حال اگر $\Gamma_{c+1}(H) = \{1\}$ و $\Gamma_{d+1}(K) = \{1\}$، قرار می‌دهیم $t = \max\{c, d\}$. پس $\Gamma_{t+1}(H) = \{1\}$ و $\Gamma_{t+1}(K) = \{1\}$. در نتیجه $\Gamma_{t+1}(H \times K) = \{(1, 1)\}$ و $H \times K$ پوچ‌توان است. □

نتیجه ۵.۲.۷. فرض کنید G_1، G_2، ...، G_r گروه‌های پوچ‌توان باشند. در این صورت $G_1 \times G_2 \times \cdots \times G_r$ پوچ‌توان است.

مثال ۶.۲.۷. فرض کنید G گروه باشد. ثابت کنید به ازای هر n، $\Gamma_n(G)$ یک زیرگروه کاملاً پایای G و بنابراین در G مشخصه است.

حل به استقرا روی n عمل می‌کنیم. برای $n = ۱$ داریم $\Gamma_۱(G) = G$ و چیزی برای اثبات نیست. حال فرض کنید $\Gamma_n(G)$ کاملاً پایا باشد و $\alpha \in \operatorname{End} G$. بنا به مثال ۲.۱.۷ و فرض استقرا، داریم

$$\begin{aligned} \alpha\left(\Gamma_{n+۱}(G)\right) &= \alpha([\Gamma_n(G), G]) \\ &= [\alpha(\Gamma_n(G)), \alpha(G)] \leq [\Gamma_n(G), G] = \Gamma_{n+۱}(G). \end{aligned}$$

پس $\Gamma_{n+۱}(G)$ کاملاً پایا است. □

قضیه ۷.۲.۷. هر گروه خارج‌قسمتی یک گروه پوچ‌توان، پوچ‌توان است.

اثبات. اگر G گروه باشد و $K \trianglelefteq G$، به استقرا ثابت می‌کنیم $\Gamma_i(G/K) = \dfrac{\Gamma_i(G)K}{K}$. برای $i = ۱$ حکم واضح است زیرا $\Gamma_۱\left(\dfrac{G}{K}\right) = \dfrac{G}{K} = \dfrac{\Gamma_۱(G)K}{K}$. اکنون فرض کنید $\Gamma_i(G/K) = \dfrac{\Gamma_i(G)K}{K}$، داریم

$$\begin{aligned} \Gamma_{i+۱}(G/K) &= [\Gamma_i(G/K), G/K] \\ &= \left[\frac{\Gamma_i(G)K}{K}, \frac{G}{K}\right] \\ &= \frac{[\Gamma_i(G), G]K}{K} \\ &= \frac{\Gamma_{i+۱}(G)K}{K}. \end{aligned}$$

پس به استقرا، به ازای هر i، $\Gamma_i(G/K) = \dfrac{\Gamma_i(G)K}{K}$. چون $\Gamma_{c+۱}(G) = \{۱\}$ داریم

$$\Gamma_{c+۱}(G/K) = \frac{\Gamma_{c+۱}(G)K}{K} = \frac{K}{K} = \{K\}$$

و G/K پوچ‌توان است. □

اگر G گروه باشد چون $Z(G)$ در G نرمال است، می‌توان گروه خارج $G/Z(G)$ را تشکیل داد. چون $Z(G/Z(G))$ زیرگروهی نرمال از $G/Z(G)$ است پس زیرگروه نرمال K از G وجود دارد که $Z(G/Z(G)) = K/Z(G)$. K را مرکز دوم G گوییم و با $Z_۲(G)$ نشان می‌دهیم. به همین نحو می‌توان $G/Z_۲(G)$ را تشکیل داد و چون $Z(G/Z_۲(G))$ زیرگروه نرمال $G/Z_۲(G)$ است، زیرگروه نرمال $Z_۳(G)$ از G وجود دارد که $Z(G/Z_۲(G)) = Z_۳(G)/Z_۲(G)$، و این روند را می‌توان ادامه داد. در واقع به طور استقرایی تعریف می‌کنیم: ابتدا قرار می‌دهیم $Z_۰(G) = \{۱\}$ و اگر زیرگروه نرمال $Z_n(G)$ از G ساخته شده باشد زیرگروه نرمال $Z_{n+۱}(G)$ را از G طوری انتخاب می‌کنیم که $Z(G/Z_n(G)) = Z_{n+۱}(G)/Z_n(G)$. پس دنباله‌ی

$$\{۱\} = Z_۰(G) \leq Z_۱(G) \leq \cdots$$

از زیرگروه‌های نرمال G به دست می‌آید، که آن را سری مرکزی بالایی G گوییم. توجه کنید که داریم $Z(G/\{۱\}) = Z_۱(G)/\{۱\}$، یعنی $Z_۱(G) = Z(G)$.

به طور کلی سری

$$۱ = G_۰ \leq G_۱ \leq \cdots$$

از زیرگروه‌های G را سری مرکزی گوییم هرگاه $G_i \trianglelefteq G$ و $G_{i+۱}/G_i \leq Z(G/G_i)$، برای هر i. در قضیه‌ی بعد یک محک مهم برای مرکزی بودن یک سری را ثابت می‌کنیم.

قضیه ۸.۲.۷. سری $\{۱\} = G_۰ \leq G_۱ \leq \cdots \leq G_n = G$ مرکزی است اگر و تنها اگر به ازای هر i، $[G_{i+۱}, G] \leq G_i$.

اثبات. اگر سری داده شده مرکزی باشد، آنگاه $G_i \trianglelefteq G$ و $G_{i+1}/G_i \leq Z(G/G_i)$، به ازای هر i. پس به ازای هر $x \in G_{i+1}$ و هر $y \in G$ داریم

$$[xG_i, yG_i] = G_i,$$

یعنی

$$[x, y]G_i = G_i$$

و

$$[x, y] \in G_i,$$

که نتیجه می‌دهد

$$[G_{i+1}, G] \leq G_i.$$

برعکس فرض کنید به ازای هر i، $[G_{i+1}, G] \leq G_i$. اگر $x \in G_{i+1}$ و $y \in G$، داریم

$$x^{-1}y^{-1}xy = [x, y] \in G_i.$$

به ویژه چون $G_i \leq G_{i+1}$، داریم $x^{-1}y^{-1}xy \in G_{i+1}$ و $y^{-1}xy \in G_{i+1}$ (زیرا $x \in G_{i+1}$). پس $G_{i+1} \trianglelefteq G$. به علاوه چون به ازای هر $x \in G_{i+1}$ و هر $y \in G$، $[x, y] \in [G_{i+1}, G] \leq G_i$، داریم $[xG_i, yG_i] = G_i$. بنابراین $xG_i \in Z(G/G_i)$، یعنی $G_{i+1}/G_i \leq Z(G/G_i)$. پس سری داده شده مرکزی است. □

چون

$$[\Gamma_i(G), G] = \Gamma_{i+1}(G),$$

طبق قضیه‌ی ۸.۲.۷، سری مرکزی پایینی

$$G = \Gamma_1(G) \geq \Gamma_2(G) \geq \cdots$$

یک سری مرکزی است. بنابراین اگر G پوچ‌توان باشد سری مرکزی برای آن وجود دارد. بر عکس اگر یک سری مرکزی برای G وجود داشته باشد، از قضیه‌ی بعد می‌توان نتیجه گرفت که G پوچ‌توان است. هم‌چنین قضیه‌ی بعد ارتباط بین سری‌های مرکزی بالایی و پائینی را با سری‌های مرکزی دلخواه مشخص می‌کند.

قضیه ۹.۲.۷. اگر $\{1\} = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_n = G$ یک سری مرکزی برای گروه G باشد، آنگاه به ازای هر i، $\Gamma_{n-i+1}(G) \leq G_i \leq Z_i(G)$.

اثبات. ابتدا به استقرا روی i، نشان می‌دهیم $G_i \leq Z_i(G)$. برای $i = 0$ حکم واضح است فرض کنید $i > 0$ و $G_{i-1} \leq Z_{i-1}(G)$. در این صورت، بنا به تمرین ۱۱ از صفحه‌ی ۱۴۱، فرض قضیه و فرض استقرا، داریم

$$[G_iZ_{i-1}(G), G] \leq [G_i, G][Z_{i-1}(G), G] \leq G_{i-1}Z_{i-1}(G) = Z_{i-1}(G).$$

بنابراین

$$\frac{G_iZ_{i-1}(G)}{Z_{i-1}(G)} \leq Z\left(\frac{G}{Z_{i-1}(G)}\right) = \frac{Z_i(G)}{Z_{i-1}(G)},$$

که نتیجه می‌دهد $G_iZ_{i-1}(G) \leq Z_i(G)$، یعنی $G_i \leq Z_i(G)$.
اکنون به استقرا روی j نشان می‌دهیم $\Gamma_{j+1}(G) \leq G_{n-j}$. مساله به ازای $j = 0$ واضح است. فرض کنید $j > 0$ و $\Gamma_j(G) \leq G_{n-(j-1)}$. طبق قضیه‌ی ۸.۲.۷، داریم

$$[G_{n-(j-1)}, G] \leq G_{n-j}.$$

بنابراین

$$\Gamma_{j+1}(G) = [\Gamma_j(G), G] \leq [G_{n-(j-1)}, G] \leq G_{n-j}.$$

پس به ازای هر j، داریم $\Gamma_{j+1}(G) \leq G_{n-j}$. به ویژه برای $j = n - i$ داریم $\Gamma_{n-i+1}(G) \leq G_i$. □

اگر c کوچک‌ترین عددی باشد که $Z_c(G) = G$، آنگاه در قضیه‌ی ۹.۲.۷، با انتخاب $G_i = Z_i(G)$ برای $i = 0, 1, 2, \ldots, c$ و $n = c$ داریم (به ازای $i = 0$)

$$\Gamma_{c+1}(G) = \Gamma_{c-0+1}(G) \leq G_0 = Z_0(G) = \{1\}.$$

پس $\Gamma_{c+1}(G) = \{1\}$. حال ادعا می‌کنیم c کوچک‌ترین عددی است که $\Gamma_{c+1}(G) = \{1\}$. فرض کنید برخلاف ادعا، $\Gamma_d(G) = \{1\}$ که در آن $d \leq c$. در این صورت با انتخاب $G_i = \Gamma_{d-i+1}(G)$ برای $i = 0, 1, \ldots, d$ و $n = d$ در قضیه‌ی ۹.۲.۷، داریم

$$\Gamma_{d-i+1}(G) = G_i \leq Z_i(G)$$

و به ازای $i = d$ داریم $G = \Gamma_1(G) \leq Z_d(G) = G$. بنابراین $Z_d(G) = G$، که خلاف انتخاب c است. همین استدلال نشان می‌دهد، اگر c کوچک‌ترین عددی باشد که $\Gamma_{c+1}(G) = \{1\}$، آنگاه c کوچک‌ترین عددی است که $Z_c(G) = G$.

قضیه ۱۰.۲.۷. اگر G گروهی باشد که $|G| = p^n$، که در آن p عدد اول است، آنگاه G پوچ‌توان است.

اثبات. به استقرا روی $|G|$ قضیه را ثابت می‌کنیم. اگر $|G| = 1$ چیزی برای اثبات نیست. فرض کنید $|G| > 1$ و قضیه برای همه‌ی گروه‌های با مرتبه‌ی کمتر از $|G|$ برقرار باشد. طبق قضیه‌ی ۱۳.۸.۳ از صفحه‌ی ۸۶، $Z(G) \neq \{1\}$. چون $Z(G) \trianglelefteq G$، می‌توان گروه خارج‌قسمتی $G/Z(G)$ را تشکیل داد. طبق فرض استقرا $G/Z(G)$ پوچ‌توان است. بنابراین سری مرکزی

$$\{Z(G)\} = \frac{G_1}{Z(G)} \leq \frac{G_2}{Z(G)} \leq \cdots \leq \frac{G_m}{Z(G)} = \frac{G}{Z(G)} \tag{1}$$

برای $\dfrac{G}{Z(G)}$ وجود دارد. توجه کنید $G_1 = Z(G)$ و $G_m = G$. سری

$$\{1\} = G_0 \leq G_1 \leq \cdots \leq G_m = G \tag{2}$$

را در نظر می‌گیریم. ثابت می‌کنیم سری (۲) مرکزی است. چون سری (۱) مرکزی است، بنا به قضیه‌ی ۸.۲.۷، به ازای هر $0 \leq i < n$، داریم

$$\left[\frac{G_{i+1}}{Z(G)}, \frac{G}{Z(G)}\right] \leq \frac{G_i}{Z(G)},$$

که نتیجه می‌دهد

$$\frac{[G_{i+1}, G]Z(G)}{Z(G)} \leq \frac{G_i}{Z(G)}.$$

بنابراین $[G_{i+1}, G] \leq G_i$ و بنا به قضیه‌ی ۸.۲.۷، سری (۲) یک سری مرکزی برای G است. در نتیجه G پوچ‌توان است. □

اکنون تعدادی شرط لازم و کافی را برای این که یک گروه متناهی، پوچ‌توان باشد ارائه می‌کنیم.

قضیه ۱۱.۲.۷. اگر $G \neq \{1\}$ گروه متناهی باشد موارد زیر معادل هستند.
(الف) G پوچ‌توان است.
(ب) اگر $H < G$، آنگاه $H < N_G(H)$.
(ج) هر زیرگروه ماکسیمال نرمال است.
(هـ) هر زیرگروه سیلوی G نرمال است.
(و) G حاصل‌ضرب مستقیم زیرگروه‌های سیلوی خودش است.

اثبات. (الف) $\Longleftarrow$ (ب) چون G پوچ‌توان است، عدد c وجود دارد که $Z_c(G)=G$. چون $H<G$ داریم $Z_0(G)=\{1\}\subseteq H$ و $Z_c(G)=G\not\subseteq H$. پس عدد $k\geq 0$ وجود دارد که $Z_k(G)\subseteq H$، اما $Z_{k+1}(G)\not\subseteq H$. اکنون عضو $a\in Z_{k+1}(G)-H$ را انتخاب می‌کنیم. داریم

$$aZ_k(G)\in \frac{Z_{k+1}(G)}{Z_k(G)}=Z\left(\frac{G}{Z_k(G)}\right).$$

بنابراین برای هر $h\in H$،

$$aZ_k(G)hZ_k(G)=hZ_k(G)aZ_k(G).$$

پس $hah^{-1}a^{-1}\in Z_k(G)\subseteq H$، یعنی $aha^{-1}\in H$. از این‌رو $aHa^{-1}\subseteq H$ و $a\in N_G(H)$.
(ب) $\Longleftarrow$ (ج) فرض کنید M زیرگروه ماکسیمال G باشد. چون $M\leq N_G(M)\leq G$ و بنا به فرض $M<N_G(M)$، داریم $N_G(M)=G$ و $M\trianglelefteq G$.
(ج) $\Longleftarrow$ (هـ) فرض کنید $P\in \mathrm{Syl}_p(G)$. اگر P در G نرمال نباشد، داریم $N_G(P)\neq G$. بنابراین زیرگروه ماکسیمال M شامل $N_G(P)$ وجود دارد. چون $P\leq N_G(P)\leq M$ و طبق فرض $M\trianglelefteq G$، به ازای هر $a\in G$، داریم $M=aMa^{-1}\leq aPa^{-1}$. بنابراین P و aPa^{-1} هر دو p- زیرگروه سیلوی M هستند و بنابراین در M مزدوج‌اند. پس عضو $x\in M$ وجود دارد که $P=xaPa^{-1}x^{-1}$. در نتیجه $xa\in N_G(P)$ و $a\in N_G(P)$. چون $a\in G$ دلخواه بود، $G=M$، که این تناقض است.
(هـ) $\Longleftarrow$ (و) فرض کنید $|G|=p_1^{n_1}p_2^{n_2}\cdots p_r^{n_r}$ و P_1، P_2، ...، P_r زیرگروه‌های سیلوی متمایز G باشند که طبق فرض همگی نرمال‌اند. چون مرتبه‌ی P_1 و P_2 نسبت به هم اول‌اند، $P_1\cap P_2=\{1\}$، که نتیجه می‌دهد

$$|P_1P_2|=\frac{|P_1||P_2|}{|P_1\cap P_2|}=|P_1||P_2|=p_1^{n_1}p_2^{n_2}.$$

چون P_1 و P_2 در G نرمال‌اند، P_1P_2 زیرگروهی از G است. اکنون چون مرتبه‌های P_1P_2 و P_3 نسبت به هم اول هستند ، داریم $P_1P_2\cap P_3=\{1\}$ و

$$|P_1P_2P_3|=\frac{|P_1P_2||P_3|}{|P_1P_2\cap P_3|}=|P_1P_2||P_3|=p_1^{n_1}p_2^{n_2}p_3^{n_3}.$$

پس ، به صورت استقرایی، می‌توان ثابت کرد که $P_1P_2\cdots P_r$ زیرگروهی از G با مرتبه‌ی $p_1^{n_1}p_2^{n_2}\cdots p_k^{n_r}$ است. بنابراین $G=P_1P_2\cdots P_r$. به علاوه به ازای هر $j=1,2,\ldots,r$، مرتبه‌های P_j و $P_1\cdots P_{j-1}P_{j+1}\cdots P_r$ نسبت به هم اول‌اند، و به ویژه اشتراک‌شان بدیهی است. در نتیجه $G=P_1\times\cdots\times P_r$.
(و) $\Longleftarrow$ (الف) طبق قضیه‌ی ۱۰.۲.۷، هر p- گروه متناهی پوچ‌توان است و بنا به قضیه‌ی ۴.۲.۷ صفحه‌ی ۱۴۲، حاصل‌ضرب مستقیم گروه‌های پوچ‌توان، پوچ‌توان است. این حکم را ثابت می‌کند. □

لازم است که تذکر دهیم شرایط (ب)-(و) در قضیه‌ی قبل برای گروه‌های نامتناهی ضعیف‌تر از پوچ‌توانی است (فصل ۱۲ از کتاب مرجع [۱۲] را ببینید).
اکنون با استفاده از قضیه‌ی قبل ثابت می‌کنیم که عکس قضیه‌ی لاگرانژ برای گروه‌های پوچ‌توان درست است:

مثال ۱۲.۲.۷. فرض کنید G گروه پوچ‌توان متناهی با مرتبه‌ی n باشد. اگر m عدد طبیعی باشد که $m|n$، آنگاه G زیرگروهی از مرتبه‌ی m دارد.

حل فرض کنید $n=p_1^{n_1}p_2^{n_2}\cdots p_k^{n_k}$ و $m=p_1^{m_1}p_2^{m_2}\cdots p_k^{m_k}$ تجزیه‌های n و m به عوامل اول باشد. طبق قضیه‌ی ۱۱.۲.۷، $G\cong P_1\times P_2\times\cdots\times P_k$، که در آن $P_i\in \mathrm{Syl}_{p_i}(G)$، $i=1,2,\ldots,k$. بنا به قضیه‌ی ۱.۴.۵، به ازای هر $i=1,2,\ldots,k$، زیرگروه‌های H_i از P_i با مرتبه‌ی $p_i^{m_i}$ وجود دارد. قرار می‌دهیم $H=H_1\times H_2\times\cdots\times H_k$. در این صورت H زیرگروهی از $P_1\times P_2\times\cdots\times P_k$ با مرتبه‌ی $m=p_1^{m_1}p_2^{m_2}\cdots p_k^{m_k}$ است. پس H با زیرگروهی از مرتبه‌ی m در G یکریخت است. □

تمرین‌ها

۱. اگر G پوچ‌توان باشد، نشان دهید برای هر $\{1\}\neq H\leq G$، $Z(H)\neq\{1\}$. نشان دهید عکس مطلب درست نیست.

۲. آیا گروه ماتریس‌های ۲ × ۲ بالا مثلثی وارون پذیر با درایه‌های در میدان دلخواه F پوچ‌توان است؟

۳. نشان دهید $D_{۲n}$ پوچ‌توان است اگر و تنها اگر به ازای یک k، $n = ۲^k$.

۴. اگر G پوچ‌توان باشد و $\{۱\} \neq H \trianglelefteq G$، نشان دهید $H \cap Z(G) \neq \{۱\}$.

۵. فرض کنید G گروه باشد. ثابت کنید به ازای هر i، $Z_i(G)$ در G مشخصه است.

۶. فرض کنید G پوچ‌توان باشد. اگر K یک زیرگروه نرمال ماکسیمال G باشد، نشان دهید $K \leq Z(G)$.

۷. فرض کنید H زیرگروه ماکسیمال نرمال G باشد. نشان دهید یا $Z(H) = \{۱\}$ یا H آبلی است.

۸. نشان دهید گروه جمعی $\mathbb{Z}$ زیرگروه ماکسیمال نرمال ندارد.

۹. فرض کنید K و L دو زیرگروه متمایز نرمال ماکسیمال گروه G باشند. ثابت کنید $KL \cong K \times L$.

۱۰. نشان دهید گروه متناهی G پوچ‌توان است اگر و تنها اگر عناصرi که مرتبه‌هایشان نسبت به هم اول است، تعویض شوند.

۱۱. نشان دهید گروه متناهی G پوچ‌توان است اگر و تنها اگر به ازای هر شمارنده‌ی m از $|G|$ یک زیرگروه نرمال مرتبه‌ی m داشته باشد.

۱۲. فرض کنید مرکز گروه G بی‌تاب باشد. نشان دهید هر عامل سری مرکزی بالایی G، یعنی $Z_{k+۱}k(G)/Z_k(G)$، بی‌تاب است. نتیجه بگیرید برای $i > j$، $Z_i(G)/Z_j(G)$ بی‌تاب است، به ویژه $G/Z(G)$ بی‌تاب است.

۱۳. فرض کنید G گروه پوچ‌توان باشد و $\exp(Z(G)) = n$. نشان دهید نمای G متناهی است و n^c را عاد می‌کند، که در آن c رده‌ی پوچ‌توانی G است.

۱۴. فرض کنید G گروه دلخواه باشد. زیرگروه آبلی و نرمال H از G زیرگروه آبلی نرمال ماکسیمال گوییم، هرگاه به ازای هر زیرگروه آبلی نرمال K که $H \leq K \leq G$، داشته باشیم $K = H$ یا $K = G$.
(الف) نشان دهید G،یک زیرگروه آبلی نرمال ماکسیمال (نه لزوماً سره) دارد.
(ب)فرض کنید گروه G پوچ‌توان باشد. اگر H زیرگروه آبلی نرمال ماکسیمال G باشد، نشان دهید $C_G(H) = H$، و نتیجه بگیرید اگر $|H| < \infty$، آنگاه $|G| < \infty$.

۳.۷ زیرگروه فراتینی

در این بخش زیرگروه فراتینی از یک گروه را بررسی می‌کنیم. یاد آوری می‌کنیم که زیرگروه M از G را ماکسیمال است هرگاه $M < G$ و هیچ زیرگروه K وجود نداشته باشد که $M < K < G$. هر گروه متناهی و به طور کلی هر گروه متناهیاً تولید شده زیرگروه ماکسیمال دارد (تمرین ۸ صفحه‌ی ۷۳ را ببینید). اگر $G \neq \{۱\}$ یک گروه باشد اشتراک همه‌ی زیرگروه‌های ماکسیمال G را زیرگروه فراتینی G گوییم و با $\Phi(G)$ نشان می‌دهیم

$$\Phi(G) = \bigcap \{M \mid M \text{ زیرگروه ماکسیمال } G\}.$$

در صورتی که G زیرگروه ماکسیمال نداشته باشد تعریف می‌کنیم $\Phi(G) = G$.

مثال ۱.۳.۷. زیرگروه‌های ماکسیمال $Q_۸$ عبارت‌اند از $\langle i\rangle$، $\langle j\rangle$، و $\langle k\rangle$، بنابراین

$$\Phi(Q_۸) = \langle i\rangle \cap \langle j\rangle \cap \langle k\rangle = \{۱, -۱\}. \qquad \square$$

مثال ۲.۳.۷. زیرگروه‌های ماکسیمال $\mathbb{Z}$ عبارت‌اند از $p\mathbb{Z}$، p عدد اول. بنابراین

$$\Phi(\mathbb{Z}) = \bigcap_{p \text{ اول}} p\mathbb{Z} = \{۰\}. \qquad \square$$

مثال ۳.۳.۷. اگر $G = \langle a\rangle$ و $O(a) = p^n$، که در آن p عدد اول است، آنگاه $\langle a^p\rangle$ یکتا زیرگروه ماکسیمال G است. بنابراین $\Phi(G) = \langle a^p\rangle$. $\square$

عضو g در گروه G را عضو نامولد G گوییم، هرگاه بتوان آن را از هر مجموعه‌ی مولد G حذف کرد ؛ یعنی اگر $G = \langle X \cup \{g\}\rangle$، آنگاه $G = \langle X\rangle$. یکی از خواص اساسی $\Phi(G)$ این است که اعضای آن دقیقاً مجموعه‌ی عناصر نامولد G هستند. برای اثبات این مطلب به لم زیر نیاز داریم.

لم ۴.۳.۷. اگر g عضوی از گروه دلخواه G باشد و $H \leq G$ طوری که $g \notin H$، آنگاه زیرگروه M از G وجود دارد که نسبت به دو شرط $H \leq M$ و $g \notin M$ ماکسیمال است.

اثبات. با استفاده از لم زُرن حکم را ثابت می‌کنیم. مجموعه‌ی

$$S = \{K \mid K \leq G,\ \ x \notin K\}$$

را با رابطه‌ی شمول $\subseteq$ در نظر می‌گیریم. $(S, \subseteq)$ یک مجموعه‌ی جزئاً مرتب است. ابتدا توجه کنید که چون $H \in S$ داریم $S \neq \emptyset$. فرض کنید $\mathscr{C}$ یک زنجیر در S باشد. قرار می‌دهیم $T = \bigcup\{K \mid K \in \mathscr{C}\}$. بنابراین، به ازای هر $K \in \mathscr{C}$، $K \subseteq T$؛ یعنی T یک کران بالا برای $\mathscr{C}$ است. به سادگی می‌توان دید $T \leq G$ و $x \notin T$، یعنی $T \in S$. پس بنا به لم S دارای یک عضو ماکسیمال مثل K است. این حکم را ثابت می‌کند. □

اکنون ثابت می‌کنیم $\Phi(G)$ متشکل از اعضای نامولد G است.

قضیه ۵.۳.۷. اگر G گروهی دلخواه باشد، آنگاه $x \in \Phi(G)$ اگر و تنها اگر x عضو نامولد G باشد.

اثبات. فرض کنید $g \in \Phi(G)$. اگر برخلاف حکم g عضو نامولد G نباشد، مجموعه‌ی $X \subseteq G$ وجود دارد که $G = \langle X \cup \{g\}\rangle$. چون $G \neq \langle X\rangle$، داریم $g \notin X$ و بنا به لم ۴.۳.۷، زیرگروه M از G وجود دارد که نسبت به دو شرط $\langle X\rangle \leq M$ و $g \notin M$ ماکسیمال است. اگر $M < H \leq G$، آنگاه $g \in H$ و $H = G$. بنابراین M زیرگروه ماکسیمال G است. اکنون چون $g \in \Phi(G) \subseteq M$، داریم $g \in M$. بنابراین $G = \langle X \cup \{g\}\rangle \subseteq M$، که تناقض است. برعکس فرض کنید g عضو نامولد i از G باشد. زیرگروه ماکسیمال دلخواه M از G را در نظر می‌گیریم. پس $M \leq \langle M \cup \{g\}\rangle \leq G$ و چون M ماکسیمال است، یا $\langle M \cup \{g\}\rangle = G$ یا $\langle M \cup \{g\}\rangle = M$. حالت اول امکان ندارد ، زیرا $M < G$ و g عضو نامولد G است. در حالت دوم داریم $x \in M$. از این‌رو g در همه‌ی زیرگروه‌های ماکسیمال G قرار دارد ، یعنی $g \in \Phi(G)$. □

فرض کنید M یک زیرگروه ماکسیمال گروه G باشد و $\alpha \in \operatorname{Aut} G$. در این صورت $\alpha(M)$ نیز زیرگروه ماکسیمال G است. برای اثبات این مطلب فرض کنید $\alpha(M) \leq N \leq G$. بنابراین $\alpha^{-1}(\alpha(M)) \leq \alpha^{-1}(N) \leq \alpha^{-1}(G)$. چون α یک‌به‌یک و پوشاست، نتیجه می‌گیریم $M \leq \alpha^{-1}(N) \leq G$. اکنون چون M زیر گروه ماکسیمال G است، $\alpha^{-1}(N) = G$ یا $\alpha^{-1}(N) = M$. مجدداً چون α یک‌به‌یک و پوشاست، $N = \alpha(G) = G$ یا $N = \alpha(M)$. از این‌رو $\alpha(M)$ زیرگروه ماکسیمال G است. بنابراین قضیه‌ی زیر را داریم :

قضیه ۶.۳.۷. اگر G گروه باشد، آنگاه $\Phi(G)$ زیرگروه مشخصه G است.

اثبات. فرض کنید $\alpha \in \operatorname{Aut} G$. اگر M زیرگروه ماکسیمال G باشد، آنگاه $\alpha^{-1}(M)$ در $\alpha^{-1}(G) = G$ ماکسیمال است (زیرا $\alpha^{-1} \in \operatorname{Aut} G$) و $\Phi(G) \subseteq \alpha^{-1}(M)$. بنابراین $\alpha(\Phi(G)) \subseteq M$، برای هر زیرگروه ماکسیمال M. پس $\alpha(\Phi(G)) \subseteq \Phi(G)$.□

قضیه ۷.۳.۷. فرض کنید $\Phi(G) \leq H \trianglelefteq G$. اگر H متناهی و $H/\Phi(G)$ پوچ‌توان باشد، آنگاه H پوچ‌توان است. به ویژه اگر $\Phi(G)$ متناهی باشد، پوچ‌توان است.

اثبات. فرض کنید P یک p- زیرگروه سیلوی H باشد. ثابت می‌کنیم $P \trianglelefteq H$. قرار می‌دهیم $K = P\Phi(G)$. چون $\dfrac{H}{\Phi(G)}$ گروه متناهی و پوچ‌توان است، p- زیرگروه سیلوی آن، یعنی $K/\Phi(G)$ یکتا و بنابراین مشخصه است. اکنون چون $K \operatorname{char} H \trianglelefteq G$، نتیجه می‌گیریم که $K \trianglelefteq G$. حال اگر $a \in G$، آنگاه $aPa^{-1} \subseteq aKa^{-1} = \Phi(G)$. پس P و aPa^{-1} دو p- زیرگروه سیلوی K هستند و بنابراین در $P\Phi(G)$ مزدوج‌اند. پس عضو $x \in K$ وجود دارد که $P = xaPa^{-1}x^{-1}$. از این‌رو $xa \in N_G(P)$ و $a \in KN_G(P)$. چون a دلخواه بود،

$$G = KN_G(P) = \Phi(G)PN_G(P) = \Phi(G)N_G(P),$$

یعنی $G = \langle \Phi(G), N_G(P) \rangle$. چون $\Phi(G)$ مجموعه‌ی نامولدهای G است، داریم $G = \langle N_G(P) \rangle = N_G(P)$، یعنی $P \trianglelefteq G$، به ویژه $P \trianglelefteq \Phi(G)$. بنابراین هر زیرگروه سیلوی $\Phi(G)$ نرمال است و طبق قضیه‌ی ۱۱.۲.۷، $\Phi(G)$ پوچ‌توان است. □

در قضیه‌ی بعدی یک شرط معادل پوچ‌توانی را برای گروه‌های متناهی، با استفاده از زیرگروه فراتینی ثابت می‌کنیم.

قضیه ۸.۳.۷. فرض کنید G گروه متناهی باشد. در این صورت G پوچ‌توان است اگر و تنها اگر $G' \leq \Phi(G)$.

اثبات. ($\Longleftarrow$) فرض کنید $G' \leq \Phi(G)$. با توجه به قضیه‌ی ۱۱.۲.۷، کافی است ثابت کنیم هر زیرگروه ماکسیمال G نرمال است. فرض کنید M زیرگروه ماکسیمال دلخواهی باشد. چون $G' \leq \Phi(G) \leq M$، $M \trianglelefteq G$ (زیرا اگر $g \in G$، $a \in M$، آنگاه $a^{-1} \in M$ و چون $a^{-1}g^{-1}ag \in G' \leq M$، $g^{-1}ag \in M$).
($\Longrightarrow$) اکنون فرض کنید G پوچ‌توان باشد. زیرگروه ماکسیمال دلخواه M از G را در نظر می‌گیریم. بنا به قضیه‌ی ۱۱.۲.۷، $M \trianglelefteq G$. از این‌رو $|G/M|$ عددی اول و G/M آبلی است، که نتیجه می‌دهد $G' \leq M$. پس $G' \leq \Phi(G)$. □

قضیه‌ی فوق بیان می‌کند که برای گروه‌های متناهی شرط $G' \leq \Phi(G)$ معادل پوچ‌توانی است. اما این شرط برای گروه‌های نامتناهی بسیار ضعیف است. زیرا ممکن است یک گروه نامتناهی زیرگروه ماکسیمال نداشته باشد، و بنابراین شرط $G' \leq \Phi(G) = G$ برقرار است. برای دیدن مطالب بیشتری در این رابطه به فصل ۱۲ از کتاب مرجع [۱۲] مراجعه کنید.

تمرین‌ها

۱. $\Phi(G)$ را بیابید هرگاه (الف) $G = D_8$ (ب) $G = D_{12}$ (ج) $G = D_{14}$

۲. فرض کنید G گروه ناآبلی باشد و $|G| = p^3$، که در آن p عدد اول است. نشان دهید $\Phi(G) = G' = Z(G)$ و $|Z(G)| = p$.

۳. فرض کنید $O(a) = p_1^{m_1} \cdots p_r^{m_r}$ (p_iها اعداد اول متمایزند و $m_i \in \mathbb{N}$) نشان دهید $\Phi(\langle a \rangle) = \langle a^m \rangle$، که در آن $m = p_1 p_2 \cdots p_r$.

۴. اگر G گروه متناهی پوچ‌توان و G/G' دوری باشد، نشان دهید G دوری است.

۵. فرض کنید G گروه متناهی باشد و $K \trianglelefteq G$. نشان دهید $K \leq \Phi(G)$ اگر و تنها اگر هیچ زیرگروه سره‌ی H وجود نداشته باشد که $G = HK$.

۶. اگر G یک p- گروه متناهی باشد، نشان دهید $\Phi(G) = \{1\}$ اگر و تنها اگر G آبلی مقدماتی باشد.

۷. اگر G گروه متناهی باشد و $H \trianglelefteq G$. نشان دهید $\Phi(H) \leq \Phi(G)$.

۸. فرض کنید $G = H \times K$، که در آن H، K زیرگروه‌های گروه G هستند. نشان دهید
(الف) هر زیرگروه ماکسیمال G شامل H به صورت $H \times L$ است که در آن L زیرگروه ماکسیمال K است.
(ب) اگر $K \neq \{1\}$، آنگاه اشتراک همه‌ی زیرگروه‌های ماکسیمال G که شامل H هستند برابر $H \times \Phi(K)$ است.
(ج) نتیجه بگیرید $\Phi(H \times K) = \Phi(H) \times \Phi(K)$.

۹. فرض کنید G گروه متناهی باشد.
(الف) اگر M زیرگروه ماکسیمال G باشد نشان دهید $Z(G) \leq M$ یا $G' \leq M$. (ب)نشان دهید $Z(G) \cap G' \leq \Phi(G)$.

۱۰. اگر G گروه متناهی باشد، نشان دهید تعداد مولدهای G و $G/\Phi(G)$ برابر است.

۱۱. فرض کنید $K \trianglelefteq G$، نشان دهید
(الف) $\dfrac{\Phi(G)K}{K} \leq \Phi\left(\dfrac{G}{K}\right)$
(ب) اگر $K \leq \Phi(G)$، آنگاه $\Phi(G)/K = \Phi(G/K)$
(ج) $\Phi(G/\Phi(G)) = \{\Phi(G)\}$.

۱۲. فرض کنید G یک p- گروه متناهی باشد. نشان دهید $\Phi(G) = G'G^p$، که در آن $G^p = \langle g^p \mid g \in G \rangle$.

۱۳. اگر A زیرگروه آبلی و نرمال گروه G باشد که $\Phi(G) \cap A = \{۱\}$، نشان دهید زیرگروه H از G وجود دارد که $G = HA$ و $H \cap A = \{۱\}$.

۱۴. نشان دهید هر زیرگروه ماکسیمال گروه G نرمال است اگر و تنها اگر $G' \leq \Phi(G)$.

۴.۷ سری ترکیبی

یادآوری می‌کنیم که یک سری برای گروه G عبارت است از زنجیر

$$G = G_۰ \geq G_۱ \geq \cdots \geq G_n = \{۱\}$$

از زیرگروه‌های G، که در آن $G_{i+۱} \trianglelefteq G_i$ به ازای هر $i = ۰, \ldots, n-۱$. G_iها را جملات سری و گروه‌های خارج‌قسمتی $G_i/G_{i+۱}$ را عوامل سری گوییم. چون $G_{i+۱} \trianglelefteq G_i$ معمولاً سری بالا را به صورت

$$G = G_۰ \trianglerighteq G_۱ \trianglerighteq \cdots \trianglerighteq G_n = \{۱\}$$

می‌نویسیم. توجه کنید لزومی ندارد که G_i ها در G نرمال باشند. هرگاه هر جمله سری در G نرمال باشد سری را سری نرمال گوییم. به علاوه با حذف جملات تکراری می‌توانیم فرض کنیم $G_i \neq G_{i+۱}$. در این حالت سری را به صورت

$$G = G_۰ \rhd G_۱ \rhd \cdots \rhd G_n = \{۱\}$$

می‌نویسیم و گاهی اوقات آن را سری سره گوییم. هم‌چنین n را طول سری گوییم.

مثال ۱.۴.۷. به ازای هر گروه G، $G \trianglerighteq \{۱\}$ یک سری برای G است و تنها عامل آن $G/\{۱\} \cong G$ است. □

مثال ۲.۴.۷. فرض کنید $V_۴ = \{(۱), (۱\ ۲)(۳\ ۴), (۱\ ۳)(۲\ ۴), (۱\ ۴)(۲\ ۳)\}$ و $K = \{(۱), (۱\ ۲)(۳\ ۴)\}$. در این صورت $A_۴ \rhd V_۴ \rhd K \rhd \{(۱)\}$ یک سری برای $A_۴$ است. عوامل آن $A_۴/V_۴ \cong C_۳$، $V_۴/K \cong C_۲$، $K/\{(۱)\} \cong C_۲$ هستند. توجه کنید K در $A_۴$ نرمال نیست. □

یکی از حالت‌های جالب وقتی است که عوامل سری ساده باشند. در این حالت سری ترکیبی به دست می‌آید.

تعریف ۳.۴.۷. سری $G = G_۰ \rhd G_۱ \rhd \cdots \rhd G_n = \{۱\}$ را سری ترکیبی برای گروه G گوییم، هرگاه همه‌ی عوامل آن یعنی $G_i/G_{i+۱}$ ساده باشند. عدد n را طول سری ترکیبی گوییم. در صورتی که $G = \{۱\}$ طول سری ترکیبی آن را برابر صفر می‌گیریم.

مثال ۴.۴.۷. گروه G ساده است اگر و تنها اگر یک سری ترکیبی به‌طول ۱ داشته باشد $G \rhd \{۱\}$.

مثال ۵.۴.۷. هر گروه متناهی سری ترکیبی دارد. این مطلب برای وقتی $G = \{۱\}$ درست است. اگر $G \neq \{۱\}$ می‌نویسیم $G = G_۰$ و یک زیرگروه ماکسیمال $G_۱$ از $G_۰$ را انتخاب می‌کنیم ($G_۱$ وجود دارد چون G متناهی است) اکنون $G_۰/G_۱$ ساده است و چون $|G_۱| < |G|$، به استقرا روی $|G|$ سری ترکیبی برای $G_۱$ وجود دارد ، مثلاً $G_۱ \rhd G_۲ \rhd \cdots \rhd G_n = \{۱\}$ سری ترکیبی برای G باشد. در نتیجه سری

$$G = G_۰ \rhd G_۱ \rhd \cdots \rhd G_n = \{۱\}$$

یک سری ترکیبی برای G است. □

در مثال ۵.۴.۷، شرط متناهی بودن را نمی‌توان حذف کرد. مثلاً $\mathbb{Z}$ گروه نامتناهی است که سری ترکیبی ندارد ، زیرا هیچ زیرگروه ساده‌ی نابدیهی ندارد. اما برای گروه‌های آبلی داشتن سری ترکیبی معادل با متناهی بودن است: هر گروه آبلی G سری ترکیبی دارد اگر و تنها اگر G متناهی باشد. در واقع اگر G متناهی باشد، طبق مثال ۵.۴.۷، G سری ترکیبی دارد. برعکس اگر گروه آبلی G سری ترکیبی $G = G_۰ \rhd G_۱ \rhd \cdots \rhd G_n = \{۱\}$ داشته باشد، آنگاه چون هر $G_i/G_{i+۱}$ آبلی ساده است، متناهی با مرتبه‌ی اول است. اکنون

$G_{n-1}/G_n = G_n/\{1\}$ متناهی است، G_{n-1} متناهی است. چون G_{n-2}/G_{n-1} و G_{n-1} متناهی هستند ، G_{n-2} نیز متناهی است و

$$|G_{n-2}| = \left|\frac{G_{n-2}}{G_{n-1}}\right| |G_{n-1}| = \left|\frac{G_{n-2}}{G_{n-1}}\right| \left|\frac{G_{n-1}}{G_n}\right|.$$

حال به استقرا فرض کنید $G_{n-(i-1)}$ متناهی باشد. چون $\dfrac{G_{n-i}}{G_{n-(i-1)}}$ متناهی است، G_{n-i} متناهی است و

$$\begin{aligned} |G_{n-i}| &= \left|\frac{G_{n-i}}{G_{n-(i-1)}}\right| |G_{n-(i-1)}| \\ &= \left|\frac{G_{n-i}}{G_{n-(i-1)}}\right| \left|\frac{G_{n-(i-1)}}{G_{n-(i-2)}}\right| \cdots \left|\frac{G_{n-1}}{G_n}\right|. \end{aligned}$$

به ویژه برای $i = n$ داریم $G = G_0$ متناهی است و

$$|G| = |G_0| = \left|\frac{G_0}{G_1}\right| \left|\frac{G_1}{G_2}\right| \cdots \left|\frac{G_{n-1}}{G_n}\right|.$$

مثال ۶.۴.۷. اگر p عدد اول باشد و $|G| = p^n$. در این صورت طبق قضیه‌ی ۱.۴.۵، $G_0 = G$ یک زیرگروه مرتبه‌ی p^{n-1} مثل G_1 دارد. و طبق قضیه‌ی ۵.۲.۵، $G_0 \rhd G_1$. چون $|G_0/G_1| = p$، $G_0/G_1 \cong C_p$ ساده است. اکنون به استقرا روی n، G_1 یک سری ترکیبی با عوامل یکریخت با C_p دارد : $G_1 \rhd G_2 \rhd \cdots \rhd G_n = \{1\}$ که در این صورت $G = G_0 \rhd G_1 \rhd G_2 \rhd \cdots \rhd G_n = \{1\}$ یک سری ترکیبی برای G با عوامل یکریخت با C_p است. □

یک گروه ممکن است سره‌های ترکیبی متفاوتی داشته باشد. مثلاً در $\mathbb{Z}_{12}$ سری‌هایی که می‌توانیم تشکیل دهیم عبارت‌اند از

$$\begin{aligned} &\mathbb{Z}_{12} \rhd \langle\bar{6}\rangle \rhd \{\bar{0}\} \\ &\mathbb{Z}_{12} \rhd \langle\bar{3}\rangle \rhd \langle\bar{6}\rangle \rhd \{\bar{0}\} \\ &\mathbb{Z}_{12} \rhd \langle\bar{2}\rangle \rhd \langle\bar{4}\rangle \rhd \{\bar{0}\} \\ &\mathbb{Z}_{12} \rhd \langle\bar{2}\rangle \rhd \langle\bar{6}\rangle \rhd \{\bar{0}\}. \end{aligned}$$

عوامل سری اول عبارت‌اند از

$$\mathbb{Z}_{12}/\langle\bar{6}\rangle \cong \mathbb{Z}_6, \quad \langle\bar{6}\rangle/\{\bar{0}\} \cong \mathbb{Z}_2.$$

عوامل سری دوم عبارت‌اند از

$$\mathbb{Z}_{12}/\langle\bar{3}\rangle \cong \mathbb{Z}_3, \quad \frac{\langle\bar{3}\rangle}{\langle\bar{6}\rangle} \cong \mathbb{Z}_2, \quad \langle\bar{6}\rangle/\{\bar{0}\} = \mathbb{Z}_2,$$

و غیره. به جز سری اول همه‌ی سری‌های دیگر سری ترکیبی‌اند. اگر عوامل سری سوم و چهارم را نیز بیابیم می‌بینیم که در مجموعه‌ی $\{\mathbb{Z}_2, \mathbb{Z}_2, \mathbb{Z}_3\}$ قرار دارند. اگر در سری اول بین $\mathbb{Z}_{12}$ و $\langle\bar{6}\rangle$ زیرگروه $\langle\bar{3}\rangle$ را قرار دهیم یک سری ترکیبی که همان سری دوم باشد به دست می‌آید. این مطالب را به طور کلی ثابت می‌کنیم. یعنی مجموعه‌ی عوامل سری‌های ترکیبی برای گروه G مساوی‌اند و اگر G سری ترکیبی داشته باشد، و هر سری برای G را می‌توان به یک سری ترکیبی توسعه داد.

تعریف ۷.۴.۷. فرض کنید G گروه و

$$G = G_0 \trianglerighteq G_1 \trianglerighteq \cdots \trianglerighteq G_{n-1} \trianglerighteq G_n = \{1\} \tag{۳}$$

یک سری برای G باشد. یک تظریف این سری عبارت است از سری

$$G = H_0 \trianglerighteq H_1 \trianglerighteq \cdots \trianglerighteq H_{m-1} \trianglerighteq H_m = \{1\} \tag{۴}$$

که در آن $n \leq m$، و اعداد صحیح مثبت $j_0 < j_1 < \cdots < j_n \leq m$ وجود داشته باشند که $G_i = H_{j_i}$، برای $i = 0, 1, \ldots, n$.
یعنی سری (۳) را بتوان با حذف تعدادی از جملات (۴) به دست آورد. سری (۴) را تظریف سرهی (۳) گوییم، هرگاه حداقل به ازای یک $j \in \{0, 1, \ldots, m\}$ داشته باشیم $G_i \neq H_j$، $i = 0, 1, \ldots, n$.

مثال ۸.۴.۷. سری

$$\mathbb{Z} \rhd 6\mathbb{Z} \rhd 12\mathbb{Z} \rhd 48\mathbb{Z} \rhd \{0\}$$

برای $\mathbb{Z}$ را در نظر بگیرید، یک تظریف سره‌ی این سری، عبارت است از

$$\mathbb{Z} \rhd 2\mathbb{Z} \rhd 6\mathbb{Z} \rhd 12\mathbb{Z} \rhd 24\mathbb{Z} \rhd 48\mathbb{Z} \rhd \{0\}. \qquad \square$$

مثال ۹.۴.۷. سری

$$\mathbb{Z}_{12} \rhd \langle \bar{3} \rangle \rhd \langle \bar{6} \rangle \rhd \langle \bar{0} \rangle$$

برای $\mathbb{Z}_{12}$ را در نظر بگیرید. این سری یک تظریف سره برای سری $\langle \bar{0} \rangle \rhd \langle \bar{6} \rangle \rhd \mathbb{Z}_{12}$ است. اما تظریف سره برای سری $\langle \bar{0} \rangle \rhd \langle \bar{4} \rangle \rhd \langle \bar{2} \rangle \rhd \mathbb{Z}_{12}$ نیست. $\square$

قضیه ۱۰.۴.۷. یک سری برای G سری ترکیبی است اگر و تنها اگر تظریف سره نداشته باشد.

اثبات. فرض کنید

$$G = G_0 \rhd G_1 \rhd \cdots \rhd G_0 = \{1\} \qquad (5)$$

یک سری ترکیبی برای G باشد. چون G_{i+1} زیرگروه نرمال ماکسیمال G_i است، هیچ زیرگروه نرمال G_i شامل G_{i+1} وجود ندارد. یعنی هیچ زیرگروه $H \lhd G_i$ وجود ندارد که $G_i \lhd H \lhd G_{i+1}$. پس هیچ تظریف سره‌ای برای سری (۵) وجود ندارد.
برعکس فرض کنید سری (۵) یک سری باشد که تظریف سره ندارد. اگر (۵) سری ترکیبی نباشد. پس یک زیرگروه G_{i+1} در سری (۵) وجود دارد که زیرگروه نرمال ماکسیمال G_i نیست. پس یک زیرگروه H وجود دارد طوری که $H_i < H < H_{i+1}$ و $H \lhd H_i$. بنابراین یک تظریف سره برای سری (۵) به دست می‌آید که تناقض است.

تعریف ۱۱.۴.۷. دو سری

$$G = G_0 \rhd G_1 \rhd G_2 \rhd \cdots \rhd G_n = \{1\}$$

و

$$G = H_0 \rhd H_1 \rhd H_2 \rhd \cdots \rhd H_m = \{1\}$$

را معادل گوییم هرگاه تناظر یک‌به‌یکی بین عوامل نابدیهی آن‌ها وجود داشته باشد طوری که عوامل متناظر یکریخت باشند.

مثال ۱۲.۴.۷. دو سری

$$\mathbb{Z} \rhd 4\mathbb{Z} \rhd 12\mathbb{Z} \rhd 24\mathbb{Z} \rhd 120\mathbb{Z} \rhd \{0\} \qquad (6)$$

$$\mathbb{Z} \rhd 2\mathbb{Z} \rhd 8\mathbb{Z} \rhd 24\mathbb{Z} \rhd 120\mathbb{Z} \rhd \{0\} \qquad (7)$$

را در نظر بگیرید. عوامل سری‌های (۶) عبارت‌اند از

$$\mathbb{Z}/4\mathbb{Z} \cong \mathbb{Z}_4, \quad 4\mathbb{Z}/12\mathbb{Z} \cong \mathbb{Z}_3, \quad 12\mathbb{Z}/24\mathbb{Z} \cong \mathbb{Z}_2,$$
$$24\mathbb{Z}/120\mathbb{Z} \cong \mathbb{Z}_5, \quad 120\mathbb{Z}/\{0\} \cong \mathbb{Z}$$

و عوامل سری (۷) عبارت‌اند از

$$\mathbb{Z}/2\mathbb{Z} \cong \mathbb{Z}_2, \quad 2\mathbb{Z}/8\mathbb{Z} \cong \mathbb{Z}_4, \quad 8\mathbb{Z}/24\mathbb{Z} \cong \mathbb{Z}_3,$$
$$24\mathbb{Z}/120\mathbb{Z} \cong \mathbb{Z}_5, \quad 120\mathbb{Z}/\{0\} \cong \mathbb{Z}$$

بنابراین سری‌های (۶) و (۷) معادل‌اند. $\square$

قضیه ۱۳.۴.۷. (لم پروانه‌ای زاسنهاوس) فرض کنید H_{i+1} و H_i و K_{j+1} و K_j زیرگروه‌های گروه G باشند طوری که H_{i+1} در H_i و K_{j+1} در K_j نرمال‌اند. در این صورت $H_{i+1}(H_i \cap K_{j+1})$ زیرگروه نرمال $H_{i+1}(H_i \cap K_j)$ و $K_{j+1}(H_{i+1} \cap K_j)$ زیرگروه نرمال $K_{j+1}(H_i \cap K_j)$ است. به علاوه

$$\frac{H_{i+1}(H_i \cap K_j)}{H_{i+1}(H_i \cap K_{j+1})} \cong \frac{K_{j+1}(H_i \cap K_j)}{K_{j+1}(H_{i+1} \cap K_j)}.$$

اثبات. چون $K_{j+1} \trianglelefteq K_j$ و $H_i \cap K_j \leq K_j$، داریم

$$H_i \cap K_{j+1} = (H_i \cap K_j) \cap K_{j+1} \trianglelefteq H_i \cap K_j.$$

به همین نحو $H_{i+1} \cap K_j \trianglelefteq H_i \cap K_j$. از این‌رو

$$J = (H_i \cap K_{j+1})(H_{i+1} \cap K_j) \trianglelefteq H_i \cap K_j.$$

اکنون تابع $f : H_{i+1}(H_i \cap K_j) \longrightarrow (H_i \cap K_j)/J$ را با ضابطه‌ی $f(ha) = Ja$ تعریف می‌کنیم، که در آن $h \in H_{j+1}$، $a \in H_i \cap K_j$ (توجه کنید هر عضو $x \in H_{i+1}(H_i \cap K_j)$ را می‌توان به صورت $x = ha$ نوشت که در آن $h \in H_{i+1}$، $a \in H_i \cap K_j$). f خوشتعریف است، زیرا اگر $h_1, h_2 \in H_{i+1}$، $a_1, a_2 \in H_i \cap K_j$، آن‌گاه

$$\begin{aligned} h_1a_1 = h_2a_2 &\Longrightarrow h_2^{-1}h_1 = a_2a_1^{-1} \in H_{i+1} \cap (H_i \cap K_j) = H_{i+1} \cap K_j \subseteq J \\ &\Longrightarrow a_2a_1^{-1} \in J \\ &\Longrightarrow Ja_1 = Ja_2 \\ &\Longrightarrow f(h_1a_1) = f(h_2a_2). \end{aligned}$$

f همریختی است، زیرا

$$\begin{aligned} f((h_1a_1)(h_2a_2)) &= f((h_1a_1h_2a_1^{-1})(a_1a_2)) \\ &= Ja_1a_2 \\ &= (Ja_1)(Ja_2) \\ &= f(h_1a_1)f(h_2a_2). \end{aligned}$$

توجه کنید چون $H_{i+1} \lhd H_i$، $h_1(a_1h_2a_1^{-1}) \in H_{i+1}$. پوشا بودن f واضح است. اکنون هسته‌ی f را می‌یابیم؛ چون

$$ha \in \ker f \Longleftrightarrow f(ha) = J \Longleftrightarrow Ja = J \Longleftrightarrow a \in J,$$

داریم

$$\ker f = H_{i+1}J = H_{i+1}(H_{i+1} \cap K_j)(H_i \cap K_{j+1}) = H_{i+1}(H_i \cap K_{j+1}),$$

که بنا به قضیه‌ی اول یکریختی نتیجه می‌دهد

$$\frac{H_{i+1}(H_i \cap K_j)}{H_{i+1}(H_i \cap K_{j+1})} \cong \frac{H \cap K}{J}.$$

بنا به تقارن

$$\frac{K_{j+1}(H_i \cap K_j)}{K_{j+1}(H_{i+1} \cap K_j)} \cong \frac{H \cap K}{J}.$$

این حکم را ثابت می‌کند. □

قضیه ۱۴.۴.۷. (قضیه‌ی شرایر) هر دو سری

$$G = H_۰ \rhd H_۱ \rhd H_۲ \rhd \cdots \rhd H_{n-۱} \rhd H_n = \{۱\} \quad (۸)$$

$$G = K_۰ \rhd K_۱ \rhd K_۲ \rhd \cdots \rhd K_{m-۱} \rhd K_m = \{۱\} \quad (۹)$$

تظریفهای معادل دارند.

اثبات. بین هر H_i و $H_{i+۱}$ زیرگروه‌های $H_{i+۱}(H_i \cap K_j)$، $j = ۰, ۱, ۲, \ldots, m$ را قرار می‌دهیم. بنا به لم زاسنهاوس این کار منجر به یک تظریف (۸) با mn رابطه‌ی شمول (نه لزوماً متمایز) می‌شود. بین هر K_j و $K_{j+۱}$ نیز زیرگروه‌های $K_{j+۱}(K_j \cap H_i)$، $i = ۰, ۱, \ldots, n$ را قرار می‌دهیم. این کار نیز به یک تظریف (۹) با mn رابطه‌ی شمول منجر می‌شود. تظریف‌های نهایی عبارت‌اند از

$$\cdots \rhd H_{i+۱}(H_i \cap K_j) \rhd H_{i+۱}(H_i \cap K_{j+۱}) \rhd \cdots$$

و

$$\cdots \rhd K_{j+۱}(K_j \cap H_i) \rhd K_{j+۱}(K_j \cap H_{i+۱}) \rhd \cdots .$$

بنا به لم زاسنهاوس داریم

$$\frac{H_{i+۱}(H_i \cap K_j)}{H_{i+۱}(H_i \cap K_{j+۱})} \cong \frac{K_{j+۱}(K_j \cap H_i)}{K_{j+۱}(K_j \cap H_{i+۱})}.$$

که حکم را ثابت می‌کند. □

قضیه ۱۵.۴.۷. (ژردان–هولدر) هر دو سری ترکیبی برای یک گروه معادل هستند.

اثبات. طبق قضیه‌ی شرایر هر دو سری ترکیبی G تظریف‌های معادل دارند. یک سری ترکیبی هیچ تظریف سره‌ای ندارد. پس یک سری ترکیبی با هر تظریف خود معادل است. در نتیجه هر دو سری ترکیبی یک گروه معادل هستند. □

بنا به قضیه‌ی ژردان–هولدر ، اگر G یک سری ترکیبی با طول n داشته باشد، آنگاه طول هر سری ترکیبی برای G باید n باشد. عدد n را طول ترکیبی G می‌نامیم و با $\ell(G)$ نشان می‌دهیم.

نتیجه ۱۶.۴.۷. (قضیه‌ی اساسی حساب) هر عدد صحیح مثبت بزرگ‌تر از ۲ به صورت یکتا به عوامل اول تجزیه می‌شود.

اثبات. فرض کنید $n > ۱$ عدد صحیح باشد. گروه $\mathbb{Z}_n$ را در نظر می‌گیریم. چون $\mathbb{Z}_n$ گروه متناهی است، سری ترکیبی دارد. فرض کنید

$$\mathbb{Z}_n = H_۰ \rhd H_۱ \rhd H_۲ \rhd \cdots \rhd H_{k-۱} \rhd H_k = \{۰\}$$

یک سری ترکیبی برای $\mathbb{Z}_n$ باشد. چون عوامل $H_i/H_{i+۱}$ گروه‌های آبلی ساده‌اند، مرتبه‌ی هر یک از آن‌ها عددی اول است، مثلاً $|H_i/H_{i+۱}| = p_i$. اکنون

$$n = |\mathbb{Z}_n| = |H_۰/H_۱||H_۱/H_۲| \cdots |H_{k-۱}/H_k| = p_۱p_۲ \cdots p_n.$$

یکتایی این تجزیه از معادل بودن سری‌های ترکیبی حاصل‌ضرب می‌شود. □

دو سری ترکیبی

$$\mathbb{Z}_{۳۰} \rhd \langle \bar{۵} \rangle \rhd \langle \bar{۱۰} \rangle \rhd \{\bar{۰}\},$$
$$\mathbb{Z}_{۳۰} \rhd \langle \bar{۲} \rangle \rhd \langle \bar{۶} \rangle \rhd \{\bar{۰}\}$$

را برای $\mathbb{Z}_{۳۰}$ در نظر بگیرید. داریم

$$\mathbb{Z}_{۳۰}/\langle \bar{۵} \rangle \cong \mathbb{Z}_۵ \ncong \mathbb{Z}_{۳۰}/\langle \bar{۲} \rangle \cong \mathbb{Z}_{۱۵}$$

اما یکریختی‌های زیر را داریم

$$\begin{aligned}\mathbb{Z}_{۳۰}/\langle\bar{۵}\rangle &\cong \langle\bar{۶}\rangle/\langle\bar{۵}\rangle \cong \mathbb{Z}_{۵}\\ \mathbb{Z}_{۳۰}/\langle\bar{۲}\rangle &\cong \langle\bar{۵}\rangle/\langle\bar{۱۰}\rangle \cong \mathbb{Z}_{۲}\\ \mathbb{Z}_{۳۰}/\langle\bar{۶}\rangle &\cong \langle\bar{۱۰}\rangle/\langle\bar{۵}\rangle \cong \mathbb{Z}_{۳}\end{aligned}$$

این بخش را با معرفی و بررسی مختصر سری‌های نرمال به پایان می‌بریم. در قضیه‌ی ۱۰.۴.۷، دیدیم که سری

$$G = G_۰ \trianglerighteq G_۱ \trianglerighteq \cdots \trianglerighteq G_۰ = \{۱\} \qquad (۱۰)$$

سری ترکیبی است اگر و تنها اگر تظریف سره نداشته باشد. در یک سری برای گروه G لزومی ندارد که جملات در G نرمال باشند. سری (۱۰) را سری نرمال گوییم هرگاه هر جمله سری در G نرمال باشد، یعنی به ازای هر $i = ۱, ۲, \ldots, n$، $G_i \trianglelefteq G$.یک سری نرمال که هیچ تظریف سره‌ای به سری نرمال دیگر نداشته باشد را سری اصلی گوییم. عوامل یک سری اصلی برای G را عوامل اصلی G می‌نامیم. توجه کنید هر گروه متناهی سری اصلی دارد. زیرا اگر G متناهی باشد، فرایند تظریف سری سره‌ی نرمال باید پس از تعداد متناهی مرحله به سری اصلی برای G منجر شود.
برخلاف عوامل ترکیبی، عوامل اصلی لزوماً گروه‌های ساده نیستند. مثلاً $A_۴$ را در نظر بگیرید، ۴-گروه کلاین V، تنها زیرگروه نرمال $A_۴$ است. پس

$$A_۴ \trianglerighteq V \trianglerighteq \{(۱)\}$$

یک سری اصلی برای $A_۴$ است. در این سری عامل اصلی $A_۴/V \cong C_۳$ ساده است. اما عامل اصلی دیگر ، یعنی $V \cong V/\{(۱)\}$ ساده نیست.

قضیه ۱۷.۴.۷. فرض کنید یک سری اصلی برای گروه G وجود دارد و H، K دو زیرگروه نرمال از G با $K < H$ باشند. در این صورت H/K عامل اصلی G است اگر و تنها اگر H/K زیرگروه ماکسیمال نرمال G/K باشد.

اثبات. فرض کنید H/K یک عامل اصلی برای G باشد. اگر $L/K \trianglelefteq G/K$ و $L/K < H/K$، آنگاه $L \trianglelefteq G$ و $K \leq L < H$. چون H/K عامل اصلی است، $K = L$. پس H/K زیرگروه ماکسیمال G/K است.
برعکس اگر H/K زیرگروه ماکسیمال G/K باشد، آنگاه یک سری اصلی برای G وجود دارد که H و K از جملات آن هستند (مشابه مثال ۵.۴.۷ عمل کنید). اگر L جمله‌ی دیگری از این سری اصلی باشد طوری که $K < L < H$، آنگاه $L/K \trianglelefteq G/K$ و $L/K < H/K$. این مطلب خلاف ماکسیمال نرمال بودن H/K در G/K است. پس هیچ جمله‌ای از سری اصلی بین H و K قرار ندارد. بنابراین H/K یک عامل اصلی برای G است. □

اگر G سری اصلی داشته باشد، بنا به قضیه‌ی ۱۷.۴.۷، هر عامل اصلی H/K از G زیرگروه ماکسیمال نرمال G/K است و بنابراین، طبق قضیه‌ی ۱۶.۷.۳ از صفحه‌ی ۸۰، مشخصاً ساده است.

تمرین‌ها

۱. در حالت‌های زیر طول ترکیبی و عوامل ترکیبی گروه داده شده را بیابید.
(الف) $C_۸$ (ب) $C_{۱۲}$ (ج) $D_۸$ (د) $A_۴$ (هـ) $Q_۸$

۲. نشان دهید C_{p^n} ($n \geq ۱$ عدد صحیح و p عدد اول)، دقیقاً یک سری ترکیبی دارد.

۳. همه‌ی سری‌های ترکیبی گروه‌های زیر را بیابید.
(الف) $\mathbb{Z}_{۲۰}$ (ب) $C_{۲۴}$ (ج) $C_{۳۰}$ (د) $S_۳$
(هـ) $S_۴$ (و) $\mathbb{Z}_۲ \times \mathbb{Z}_۲$ (ز) $C_۸ \times C_۴$

۴. دو گروه متناهی غیر یکریخت مثال بزنید که عوامل ترکیبی آن ها یکی باشد.

۵. فرض کنید $K \trianglelefteq G$، $G = G_0 \trianglerighteq G_1 \trianglerighteq \cdots \trianglerighteq G_n = \{1\}$ یک سری برای G باشد و
(الف) نشان دهید $K = K \cap G_0 \trianglerighteq K_1 \cap G_1 \trianglerighteq \cdots \trianglerighteq K \cap G_n = \{1\}$ یک سری برای K است و عامل $(K \cap G_i)/(K \cap G_{i+1})$ با زیرگروه نرمالی از G_i/G_{i+1} یکریخت است.
(ب) نشان دهید $G/K = \frac{G_0K}{K} \trianglerighteq \frac{G_1K}{K} \trianglerighteq \cdots \trianglerighteq \frac{G_nK}{K} = \{K\}$ یک سری برای G/K است و عامل $[G_iK/K]/[G_{i+1}K/K]$، یک تصویر همریختی از G_i/G_{i+1} است.

۶. اگر K زیرگروه نرمالی از G باشد، نشان دهید G سری ترکیبی دارد اگر و تنها اگر K و G/K سری ترکیبی داشته باشند. به علاوه در این صورت
(الف) $\ell(G) = \ell(K) + \ell(G/K)$، که در آن $\ell(G)$ طول ترکیبی G است.
(ب) عوامل ترکیبی G دقیقاً عوامل ترکیبی K و G/K هستند.
(ج) G یک سری ترکیبی شامل K دارد.

۷. نشان دهید گروه‌های G و H سری ترکیبی دارند. اگر و تنها اگر $G \times H$ نیز سری ترکیبی داشته باشد و در این حالت $\ell(G \times H) = \ell(G) + \ell(H)$. این مطلب را برای n گروه تعمیم دهید.

۸. فرض کنید G گروه آبلی با مرتبه‌ی $p_1^{n_1}p_2^{n_2}\cdots p_r^{n_r}$ باشد، که در آن p_i ها اعداد اول متمایزند. نشان دهید $\ell(G) = n_1 + n_2 + \cdots + n_r$.

۹. فرض کنید G گروه و H، K زیرگروه‌های نرمال ماکسیمال G باشند. نشان دهید $H \cap K$ زیرگروه نرمال ماکسیمال هم H و هم K است. به علاوه $\frac{H}{H \cap K} \cong \frac{G}{K}$ و $\frac{K}{H \cap K} \cong \frac{G}{H}$.

۱۰. قضیه‌ی ژردان–هولدر به استقرا و با استفاده از مثال‌های ۵، ۶ و ۹ اثبات کنید.

۱۱. فرض کنید $n = p_1^{n_1}p_2^{n_2}\cdots p_r^{n_r}$، که در آن p_iها اعداد اول متمایزند و $n_i \geq 1$.
(الف) نشان دهید C_n دقیقاً r زیرگروه نرمال ماکسیمال دارد.
(ب) اگر $m = n_1 + n_2 + \cdots + n_r$ نشان دهید C_n، $\frac{m!}{n_1!n_2!\cdots n_r!}$ سری ترکیبی دارد.

۱۲. فرض کنید $n = p_1^{n_1}p_2^{n_2}\cdots p_r^{n_r}$، طول ترکیبی D_{2n} را بیابید.

۱۳. نشان دهید موارد زیر برای گروه متناهی G معادل‌اند.
(الف) G حل‌پذیر است.
(ب) برای هر $\{1\} \neq H \leq G$، $H' < H$.
(ج) همه‌ی عوامل ترکیبی G آبلی‌اند.

۱۴. فرض کنید $|G| = p_1^{m_1}\cdots p_s^{m_s}$ (که در آن p_iها اعداد اول متمایزند و $m_i \in \mathbb{N}$). نشان دهید G حل‌پذیر است اگر و تنها اگر طول ترکیبی G برابر $\sum_{j=1}^{s} m_j$ باشد.

۱۵. نشان دهید یک گروه متناهی حل‌پذیر است اگر و تنها اگر سری ترکیبی داشته باشد.

۱۶. نشان دهید موارد زیر برای گروه متناهی G معادل هستند.
(الف) G حل‌پذیر است.
(ب) مرتبه‌ی هر عامل ترکیبی G عدد اول است.
(ج) هر عامل اصلی G آبلی مقدماتی است.

۵.۷ گروه‌های چند دوری و حل‌پذیر

دیدیم هر گروه حل‌پذیر ، پوچ‌توان است و عکس آن درست نیست. در این بخش رده‌های دیگری از گروه‌ها را معرفی می‌کنیم که شامل گروه‌های حل‌پذیر هستند. یک گروه را چند دوری گوییم، هرگاه یک سری با عوامل دوری داشته باشد. پس گروه G چند دوری است، هرگاه

سری

$$G = G_۰ \trianglerighteq G_۱ \trianglerighteq \cdots \trianglerighteq G_n = \{۱\} \tag{۱۱}$$

وجود داشته باشد که به ازای هر $i = ۱, ۲, \ldots, n-۱$، $G_i/G_{i+۱}$ دوری است. یک گروه را حل‌پذیر گوییم، هرگاه یک سری نرمال با عوامل دوری داشته باشد. بنابراین گروه G حل‌پذیر است، هرگاه یک سری مثل (۱۱) وجود داشته باشد که به ازای هر $i = ۱, ۲, \ldots, n$، $G_i \trianglelefteq G$ و به ازای هر $i = ۱, ۲, \ldots, n-۱$، $G_i/G_{i+۱}$ دوری باشد. توجه کنید هر گروه حل‌پذیر ، چند دوری است و هر گروه چند دوری حل‌پذیر است.

مثال ۱.۵.۷. نشان دهید گروه متناوب $A_۴$ یک گروه چند دوری و بنابراین حل‌پذیر است، اما حل‌پذیر نیست.

حل فرض کنید

$$V = \{(۱), (۱\ ۲)(۳\ ۴), (۱\ ۳)(۲\ ۴), (۱\ ۴)(۲\ ۳)\},$$

۴-گروه کلاین باشد و زیرگروه $H = \{(۱), (۱\ ۲)(۳\ ۴)\}$ از V را در نظر می‌گیریم. در این صورت سری $A_۴ \trianglerighteq V \trianglerighteq H \trianglerighteq \{(۱)\}$ یک سری با عوامل دوری است، زیرا $A_۴/V \cong C_۳$، $V/H \cong C_۲$ و $H/\{(۱)\} \cong C_۲$. بنابراین $A_۴$ چند دوری است. اما $A_۴$ حل‌پذیر نیست، زیرا تنها سری نرمال برای $A_۴$ سری $A_۴ \trianglerighteq V \trianglerighteq H\{(۱)\}$ است که عامل $V/\{(۱)\} \cong C_۲ \times C_۲$ دوری نیست. □

هر گروه متناهی حل‌پذیر چند دوری است. زیرا ، بنا به تمرین ۱۶ از بخش قبل، مرتبه‌ی عوامل ترکیبی هر گروه متناهی حل‌پذیر عدد اول است. بنابراین گروه متناهی حل‌پذیر است اگر و تنها اگر چند دوری باشد. پس گروهی حل‌پذیر که چند دوری نباشد باید گروه نامتناهی باشد (تمرین ۶ را ببینید).

قضیه ۲.۵.۷. اگر G گروهی چند دوری و

$$G = G_۰ \trianglerighteq G_۱ \trianglerighteq \cdots \trianglerighteq G_n = \{۱\}$$

یک سری با عوامل دوری به طول n (n عدد صحیح مثبت) برای G باشد، آنگاه

(الف) G یک گروه n مولدی است.

(ب) برای هر زیرگروه و هر گروه خارج‌قسمتی G یک سری به طول حداکثر n با عوامل دوری وجود دارد. بنابراین همه‌ی زیر گروه‌ها و گروه‌های خارج‌قسمتی G چند دوری و n مولدی هستند.

اثبات. (الف) چون عوامل سری دوری هستند ، به ازای هر $i = ۰, ۱, ۲, \ldots, n-۱$، $x_i \in G_i$ وجود دارد که $G_i/G_{i+۱} = \langle x_i G_{i+۱}\rangle$. بنابراین $G_i = \langle G_{i+۱}, x_i\rangle$ و

$$G = G_۰ = \langle G_۱, x_۰\rangle = \langle G_۲, x_۱, x_۰\rangle = \cdots = \langle x_{n-۱}, \ldots, x_۱, x_۰\rangle .$$

(ب) فرض کنید H زیرگروهی از G باشد. چون $G_{i+۱} \trianglelefteq G_i$، داریم $H \cap G_{i+۱} \trianglelefteq H$؛ پس $H \cap G_{i+۱} H = H \cap G_{i+۱} \cap G_i \trianglelefteq H \cap G_i$. بنا به دومین قضیه‌ی یکریختی داریم

$$\frac{H \cap G_i}{H \cap G_{i+۱}} = \frac{H \cap G_i}{(H \cap G_i) \cap G_{i+۱}} \cong \frac{(H \cap G_i)G_{i+۱}}{G_{i+۱}} \leq \frac{G_i}{G_{i+۱}}.$$

بنابراین، چون $G_i/G_{i+۱}$ دوری است، هر عامل سری

$$H = H \cap G = H \cap G_۰ \trianglerighteq H \cap G_۱ \trianglerighteq \cdots \trianglerighteq H \cap G_n = \{۱\}$$

دوری است. پس سری فوق یک سری با طول n و عوامل دوری برای H است.

اکنون فرض کنید $H \trianglelefteq G$. چون $G_{i+۱} \trianglelefteq G_i$ داریم $G_{i+۱}H \trianglelefteq G_i H$. بنا به قضیه‌ی دوم و سوم یکریختی داریم

$$\frac{G_i H}{G_{i+۱}H} = \frac{G_i G_{i+۱} H}{G_{i+۱}H} \cong \frac{G_i}{G_i \cap G_{i+۱}H} \cong \frac{G_i/G_{i+۱}}{(G_i \cap G_{i+۱}H)/G_{i+۱}}.$$

بنابراین، چون G_i/G_{i+1} دوری است، هر عامل سری

$$\frac{G}{H} = \frac{G_0}{H} \trianglerighteq \frac{G_1 H}{H} \trianglerighteq \frac{G_2 H}{H} \trianglerighteq \cdots \trianglerighteq \frac{G_n H}{H} = \{H\}$$

دوری است. پس سری فوق یک سری با طول n و عوامل دوری برای G/H است. □

رده‌ی گروه‌های چند دوری تحت توسیع بسته است، یعنی :

قضیه ۳.۵.۷. فرض کنید H زیرگروه نرمالی از گروه G باشد. اگر H و G/H چند دوری باشند، آنگاه G چند دوری است.

اثبات. طبق فرض سری‌های

$$H = H_0 \trianglerighteq H_1 \trianglerighteq \cdots \trianglerighteq H_r = \{1\}$$

و

$$\frac{G}{H} = \frac{G_0}{H} \trianglerighteq \frac{G_1}{H} \trianglerighteq \cdots \trianglerighteq \frac{G_s}{H} = \{H\}$$

با عوامل دوری برای H و G/H وجود دارند. چون $G_{i+1}/H \trianglelefteq G_i/H$، $G_{i+1} \trianglelefteq G_i$. اکنون سری

$$G = G_0 \trianglerighteq G_1 \trianglerighteq \cdots \trianglerighteq G_s \trianglerighteq H_0 \trianglerighteq H_1 \trianglerighteq \cdots \trianglerighteq H_r = \{1\}$$

یک سری برای G با عوامل دوری است، زیرا به ازای هر $i = 1, 2, \ldots, s-1$ و به ازای هر $j = 1, 2, \ldots, r$ عوامل

$$\frac{G_i}{G_{i+1}} \cong \frac{G_i/H}{G_{i+1}/H}, \quad \frac{G_s}{H_0} = \frac{G_s}{H}, \quad \frac{H_j}{H_{j+1}}$$

دوری هستند. □

قضیه ۴.۵.۷. فرض کنید G گروه متناهیاً تولید شده با n مولد باشد. قضیه‌های زیر معادل هستند.
(الف) هر زیرگروه نرمال G متناهیاً تولید شده و حل‌پذیر است.
(ب) G چند دوری است.
(ج) هر زیرگروه G متناهیاً تولید شده و حل‌پذیر است.

اثبات. (الف) $\Longleftarrow$ (ب) چون G حل‌پذیر است عدد m وجود دارد که $G^{(m)} = \{1\}$. طبق فرض به ازای هر i، $G^{(i)}$ متناهیاً تولید شده است. به صورت استقرایی ثابت می‌کنیم $G^{(m-i)}$، $i = 0, 1, 2, \ldots, m$. چند دوری است. به ازای $i = 0$ داریم $G^{(m)} = \{1\}$ و چیزی برای اثبات نیست. به ازای $i = 1$، $G^{(m-1)}$ گروه آبلی متناهیاً تولید شده است. پس بنا به تمرین ۱، $G^{(m-1)}$ چند دوری است. فرض کنید $G^{(m-i)}$ چند دوری باشد. چون $G^{(m-i-1)}$ متناهیاً تولید شده است، گروه $G^{(m-i-1)}/G^{(m-i)}$ آبلی متناهیاً تولید شده است و بنا به تمرین ۱، چند دوری است. بنابراین ، بنا به قضیه‌ی ۳.۵.۷، $G^{(m-i-1)}$ چند دوری است. به ویژه، به ازای $i = m$، $G^{(m-m)} = G^{(0)} = G$ چند دوری است.
(ب) $\Longleftarrow$ (ج) بنا به قضیه‌ی ۲.۵.۷، واضح است.
(ج) $\Longleftarrow$ (الف) واضح است. □

اکنون گروه‌های حل‌پذیر را بررسی می‌کنیم. اثبات قضیه‌ی زیر را که مشابه اثبات قسمت (ب) قضیه‌ی ۲.۵.۷، است به عنوان تمرین واگذار می‌کنیم.

قضیه ۵.۵.۷. اگر G گروه حل‌پذیر باشد، آنگاه هر زیرگروه و هر گروه خارج‌قسمتی G حل‌پذیر است.

رده‌ی گروه‌های حل‌پذیر تحت توسیع بسته نیست. زیرا مثلاً $A_4/V \cong C_3$ و V (V، ۴-گروه کلاین است) حل‌پذیرند و A_4 حل‌پذیر نیست. اما قضیه‌ی زیر را در مورد گروه‌های حل‌پذیر داریم.

قضیه ۶.۵.۷. اگر H و K حل‌پذیر باشند، آنگاه $G = H \times K$ نیز حل‌پذیر است.

اثبات. طبق فرض سری‌های

$$H = H_۰ \trianglerighteq H_۱ \trianglerighteq \cdots \trianglerighteq H_r = \{۱\}$$

و

$$K = K_۰ \trianglerighteq K_۱ \trianglerighteq \cdots \trianglerighteq K_s = \{۱\}$$

با عوامل دوری برای H و K وجود دارند طوری که $H_i \trianglelefteq H$ و $K_i \trianglelefteq K$. اکنون چون به ازای هر $H_i \trianglelefteq H$ و $K_i \trianglelefteq K$ به ازای هر $i = ۱, ۲, \ldots, s$، داریم $H \times K_i \trianglelefteq H \times K$ و به ازای هر $i = ۱, ۲, \ldots, r$، داریم $H_i \times \{۱\} \trianglelefteq H \times K$. پس سری

$$G = H \times K = H \times K_۰ \trianglerighteq H \times K_۱ \trianglerighteq \cdots \trianglerighteq H \times K_s = H \times \{۱\} = H_۰ \times \{۱\}$$

$$\trianglerighteq H_۱ \times \{۱\} \trianglerighteq \cdots \trianglerighteq H_r \times \{۱\} = \{۱\} \times \{۱\} = \{(۱, ۱)\}$$

یک سری با جملات نرمال در G است. به علاوه عوامل سری دوری هستند ، زیرا

$$\frac{H \times K_i}{H \times K_{i+۱}} \cong \frac{H}{H} \times \frac{K_i}{K_{i+۱}} \cong \frac{K_i}{K_{i+۱}}, \quad \frac{H_i \times \{۱\}}{H_{i+۱}} \times \{۱\} \cong \frac{H_i}{H_{i+۱}}.$$

بنابراین $G = H \times K$، حل‌پذیر است. □

تمرین‌ها

۱. فرض کنید G گروه آبلی n مولدی، n عدد صحیح مثبت، باشد. نشان دهید G چند دوری است و همه‌ی زیرگروه‌های G گروه‌های n مولدی هستند.

۲. فرض کنید G گروه متناهی باشد. ثابت کنید G حل‌پذیر است اگر و تنها اگر مرتبه‌ی هر عامل اصلی آن عدد اول باشد.

۳. نشان دهید هر گروه پوچ‌توان متناهی حل‌پذیر است. با ارائه‌ی یک مثال نشان دهید گروه حل‌پذیر متناهی وجود دارد که پوچ‌توان نیست.

۴. فرض کنید G گروه چند دوری باشد. نشان دهید تعداد عوامل دوری نامتناهی در هر سری با عوامل دوری برای G مستقل از سری است و بنابراین فقط به G بستگی دارد. این عدد را طول هرش (Hirsh) گوییم و با $h(G)$ نشان می‌دهیم.

۵. فرض کنید K زیرگروهی از گروه چند دوری G باشد. نشان دهید
(الف) اگر $K \trianglelefteq G$، آنگاه $h(G) = h(G/K) + h(K)$.
(ب) K متناهی است اگر و تنها اگر $h(K) = ۰$.
(ج) $h(G) = h(K)$ اگر و تنها اگر $|G : K|$ متناهی باشد.

۶. به ازای هر $i \geq ۱$، گروه دوری $\langle a_i \rangle$ را در نظر بگیرید و قرار دهید $A = \mathrm{Dr}_{i=۱}^{\infty} \langle a_i \rangle$. خودریختی $\alpha \in \mathrm{Aut}\, A$ را با $\alpha(a_i) = a_{i+۱}$، $i \geq ۱$ در نظر بگیرید و حاصل‌ضرب نیم‌مستقیم $G = A \rtimes \langle \alpha \rangle$ را تشکیل دهید. نشان دهید G یک گروه دو مولدی حل‌پذیر با مولدهای $a_۱$ و α است؛ اما زنجیر سره $\{۱\} < \langle a_۱ \rangle < \langle a_۱, a_۲ \rangle < \cdots$ از زیرگروه‌های G وجود دارد. نتیجه بگیرید G چند دوری نیست.

فصل ۸
گروه‌های آزاد

۱.۸ خواص اساسی گروه‌های آزاد

یک مساله در نظریه‌ی گروه‌ها ساختن گروه‌های جدید با استفاده از یک مجموعه‌ی داده شده است. داده شده است. در فصل ۶ مساله‌ی ساختن گروه آبلی آزاد روی یک مجموعه را بررسی کردیم. دیدیم به ازای هر مجموعه‌ی X یک گروه آبلی آزاد روی X وجود دارد. اکنون می‌خواهیم با استفاده از مجموعه‌ی X داده شده ، گروهی مثل G بسازیم که X مجموعه‌ی مولد آن باشد و اعضای G در معادله‌های از پیش تعیین شده‌ای صدق کنند. در واقع قبلاً دیده‌ایم که برخی گروه‌ها را با استفاده از مولدهای‌شان و تعدادی معادله که شامل مولدهاست می‌توان توصیف کرده و شکل همه‌ی اعضای آن‌ها را یافت. به عنوان مثال گروه دووجهی از مرتبه‌ی $2n$ ، D_{2n} با استفاده از مولدهاش ε، ρ و معادله‌های $\rho^n = \varepsilon^2 = (\rho\varepsilon)^2 = 1$ کاملاً توصیف می‌شود. در این حالت می‌نویسیم

$$D_{2n} = \langle \rho, \varepsilon \mid \rho^2 = \varepsilon^2 = (\rho\varepsilon)^2 = 1 \rangle .$$

هر یک عبارت‌های $\rho^n = 1$، $\varepsilon^n = 1$، $(\rho\varepsilon)^2 = 1$ را یک رابطه روی مجموعه‌ی مولد $\{\rho, \varepsilon\}$ می‌نامیم. این نحوه‌ی توصیف D_{2n} را نمایش آن می‌نامیم. به عنوان مثال دیگر یک نمایش برای گروه دووجهی نامتناهی D_∞ عبارت است

$$D_\infty = \langle \tau, \varepsilon \mid \varepsilon^2 = (\varepsilon\tau)^2 = 1 \rangle .$$

اگر X مجموعه‌ای ناتهی و R مجموعه‌ای از روابط روی X باشد، سوالی که مطرح است این است که آیا گروهی مانند G وجود دارد که X آن را تولید کند و R مجموعه‌ای از روابط در G باشد که اعضای G با استفاده از مجموعه‌ی مولد X و روابط در R کاملاً توصیف شود، یعنی آیا گروه G وجود دارد که

$$G = \langle X \mid R \rangle ?$$

در این بخش می‌خواهیم به این سوال پاسخ مثبت دهیم. ابتدا حالت $R = \emptyset$ را در نظر می‌گیریم، یعنی مجموعه‌ای چون X گروه G را تولید کند و هیچ رابطه‌ای روی X وجود نداشته باشد. این مطلب منجر به تعریف مفهوم گروه آزاد روی X می‌شود. فرض کنید X مجموعه‌ای دلخواه باشد. ثابت می‌کنیم گروهی وجود دارد که X مجموعه‌ی مولد آن باشد. مجموعه‌ای مثل Y طوری انتخاب می‌کنیم که $X \cap Y = \emptyset$ و $|X| = |Y|$. چون $|X| = |Y|$ یک تابع دوسویی از X به Y وجود دارد. تصویر $x \in X$ را تحت این تابع با x^{-1} نشان می‌دهیم. هم‌چنین تصویر $y \in Y$ تحت معکوس این تابع را با y^{-1} نشان می‌دهیم. بنابراین $(x^{-1})^{-1} = x$. به این دلیل به جای Y می‌نویسیم X^{-1} و x^{-1} را وارون x گوییم.یک مجموعه‌ی بک عضوی را طوری اختیار می‌کنیم که در $X \cup X^{-1}$ قرار نداشته باشد و آن را $\{1\}$ می‌نامیم. قرار می‌دهیم $1^{-1} = 1$ و به ازای هر $u \in X \cup X^{-1}$، $u^1 = u$. یک واژه روی X دنباله‌ای مثل

$$(x_1, x_2, x_3, \ldots)$$

است که در آن $x_i \in X \cup X^{-1} \cup \{1\}$، طوری که عدد n (وابسته به دنباله) وجود دارد که برای هر $i \geq n$، $x_i = 1$. بنابراین می‌توانیم تصور کنیم که یک واژه حاصل‌ضرب متناهی از اعضای X و وارون‌های‌شان است (تکرار مجاز است). اکنون برای این که نمایش یک واژه یکتا باشد تنها واژه‌هایی را در نظر می‌گیریم که ۱ بین حروف قرار می‌گیرد و دو حرف متوالی وارون هم نباشند مثلاً به جای واژه‌ی $b1b1aa^{-1}b$، واژه‌ی bb را در نظر بگیریم.

تعریف ۱.۱.۸. واژه‌ی $(x_1, x_2, x_3, \ldots)$ را واژه‌ی کاهشی گوییم هرگاه
(الف) به ازای هر $x_i \neq 1$ داشته باشیم $x_{i+1} \neq x_i^{-1}$.
(ب) اگر به ازای یک k، داشته باشیم $x_k = 1$، آنگاه برای هر $i \geq k$، $x_i = 1$.

واژه‌ی $(1, 1, 1, \ldots)$ را واژه‌ی تهی می‌نامیم و با 1 نشان می‌دهیم. اکنون نمادگذاری را ساده می‌کنیم و به جای واژه‌ی کاهشی $(x_1^{\varepsilon_1}, x_2^{\varepsilon_2}, \ldots, x_n^{\varepsilon_n}, 1, 1, 1, \ldots)$، که در آن $x_i \in X$ و $\varepsilon_i = \pm 1$، می‌نویسیم $x_1^{\varepsilon_1} x_2^{\varepsilon_2} \cdots x_n^{\varepsilon_n}$. توجه کنید بنا به تعریف، واژه‌های کاهشی $x_1^{\varepsilon_1} x_2^{\varepsilon_2} \cdots x_n^{\varepsilon_n}$ و $y_1^{\delta_1} y_2^{\delta_2} \cdots y_m^{\delta_m}$ برابرند اگر و تنها اگر $n = m$ و به ازای هر $1 \leq i \leq n$، $\varepsilon_i = \delta_i$ و $x_i = y_i$. فرض کنید $F = F(X)$ مجموعه‌ی همه‌ی واژه‌ها کاهشی روی X باشد و با استفاده از تابع یک‌به‌یک

$$x \mapsto (x, 1, 1, 1, \ldots)$$

X را به عنوان زیرمجموعه‌ای از $F(X)$ در نظر می‌گیریم.
اکنون یک عمل دوتایی روی $F(X)$ تعریف می‌کنیم. در واقع برای ضرب دو واژه‌ی کاهشی $u = x_1^{\varepsilon_1} x_2^{\varepsilon_2} \cdots x_n^{\varepsilon_n}$ و $v = y_1^{\delta_1} y_2^{\delta_2} \cdots y_m^{\delta_m}$ کافی است که دو واژه را کنار هم بگذاریم:

$$uv = x_1^{\varepsilon_1} x_2^{\varepsilon_2} \cdots x_n^{\varepsilon_n} y_1^{\delta_1} y_2^{\delta_2} \cdots y_m^{\delta_m}.$$

اما یک مشکل وجود دارد. آیا واژه‌ی حاصل کاهشی است؟ در واقع اگر مثلاً $\varepsilon_n = 1$ و $\delta_1 = -1$ و $x_n = y_1$، قطعاً واژه‌ی حاصل کاهشی نیست. برای این که واژه‌ی کاهشی به دست بیاوریم باید حروف مجاور که وارون یکدیگر هستند را حذف کنیم. فرض کنید مثلاً $n \leq m$ و k را بزرگ‌ترین عدد صحیح بگیرید که $0 \leq k \leq n$، و $x_{n-j}^{\varepsilon_{n-j}} \neq y_{j+1}^{-\delta_{j+1}}$، برای هر $j = 0, 1, \ldots, k-1$. در این صورت حاصل‌ضرب واژه‌ها کاهشی u و v به صورت زیر تعریف می‌شود:

$$(x_1^{\varepsilon_1} \cdots x_n^{\varepsilon_n})(y_1^{\delta_1} \cdots y_m^{\delta_m}) = \begin{cases} x_1^{\varepsilon_1} \cdots x_{n-k}^{\varepsilon_{n-k}} y_{k+1}^{\delta_{k+1}} \cdots y_m^{\delta_m} & k < n \\ y_{n+1}^{\delta_{n+1}} \cdots y_m^{\delta_m} & k = n < m \\ 1 & k = n = m. \end{cases}$$

در حالتی که $n > m$ عمل ضرب را به طریق مشابه تعریف می‌کنیم.

قضیه ۲.۱.۸. با نمادهای بالا $F = F(X)$ یک گروه است.

اثبات. به وضوح 1 عضو همانی است و وارون واژه‌ی کاهشی $x_1^{\varepsilon_1} x_2^{\varepsilon_2} \cdots x_n^{\varepsilon_n}$ واژه‌ی کاهشی $x_n^{-\varepsilon_n} x_{n-1}^{-\varepsilon_{n-1}} \cdots x_1^{-\varepsilon_1}$ است. برای اثبات شرکت‌پذیری به طریق زیر عمل می‌کنیم. به ازای هر $x \in X \cup X^{-1} \cup \{1\}$ تابع $\varphi_x : F \longrightarrow F$ را با

$$\varphi_x(x_1^{\varepsilon_1} x_2^{\varepsilon_2} \cdots x_n^{\varepsilon_n}) = \begin{cases} x x_1^{\varepsilon_1} x_2^{\varepsilon_2} \cdots x_n^{\varepsilon_n} & x_1^{\varepsilon_1} \neq x^{-1} \\ x_2^{\varepsilon_2} x_3^{\varepsilon_3} \cdots x_n^{\varepsilon_n} & x_1^{\varepsilon_1} = x^{-1} \end{cases}$$

تعریف می‌کنیم. چون $\varphi_{x^{-1}} \varphi_x = \varphi_1$ تابع همانی روی F است، φ_x یک جایگشت روی F است. فرض کنید H زیرگروه S_F، گروه متقارن روی F، باشد که توسط همه‌ی φ_x تولید می‌شود:

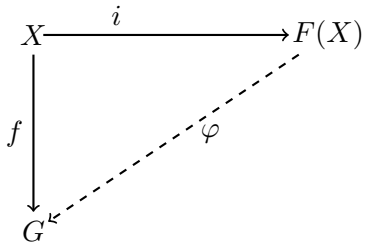
$$H = \langle \varphi_x \mid x \in X \cup X^{-1} \cup \{1\} \rangle \leq S_F.$$

به وضوح نگاشت $\psi : F \longrightarrow H$ با ضابطه‌ی

$$\psi(x_1^{\varepsilon_1} x_2^{\varepsilon_2} \cdots x_n^{\varepsilon_n}) = \varphi_{x_1}^{\varepsilon_1} \varphi_{x_2}^{\varepsilon_2} \cdots \varphi_{x_n}^{\varepsilon_n}$$

یک تابع دوسویی است و به ازای هر $u, v \in F$، $\psi(uv) = \psi(u)\psi(v)$. چون H گروه و در نتیجه شرکت‌پذیر است، $F(X)$ نیز چنین است. □

تعریف ۳.۱.۸. گروه $F(X)$ را گروه آزاد روی مجموعه‌ی X گوییم. یک گروه F را گروه آزاد گوییم هرگاه مجموعه‌ی X وجود داشته باشد که $F = F(X)$. X را یک مجموعه‌ی مولدهای آزاد (یا پایه‌ی آزاد) برای F گوییم. $|X|$ را رتبه‌ی F می‌نامیم.



شکل ۱.۸: نمودار تعویض‌پذیر است.

برای تعریف همریختی از یک گروه آزاد به گروه دلخواه کافی است این همریختی را روی پایه‌ی آزاد F تعریف کنیم. این اساسی‌ترین خاصیت گروه آزاد است. این خاصیت را خاصیت جهانی گروه آزاد گوییم.

قضیه ۴.۱.۸. فرض کنید $F(X)$ گروه آزاد روی X باشد و $i : X \longrightarrow F(X)$ تابع شمول ($i(x) = x$، به ازای هر $x \in X$). اگر G یک گروه و $f : X \longrightarrow G$ یک تابع باشد، آنگاه همریختی یکتای $\varphi : F(X) \longrightarrow G$ وجود دارد که $\varphi(x) = f(x)$، به ازای هر $x \in X$، یعنی نمودار ۱.۸ تعویض‌پذیر است. بنابراین هر تابع $f : X \longrightarrow G$ را می‌توان به یک همریختی $\varphi : F(X) \longrightarrow G$ توسعه داد.

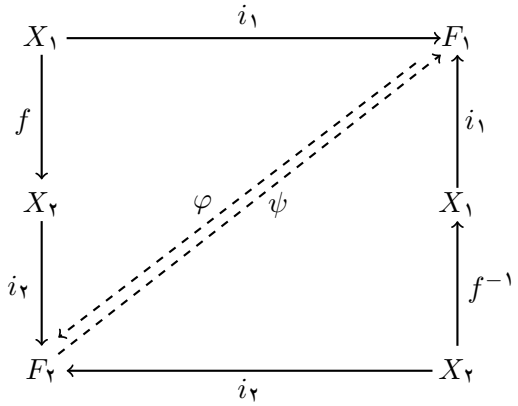
اثبات. چنین φ باید در $\varphi(x_1^{\varepsilon_1} x_2^{\varepsilon_2} \cdots x_n^{\varepsilon_n}) = f(x_1)^{\varepsilon_1} f(x_2)^{\varepsilon_2} \cdots f(x_n)^{\varepsilon_n}$ صدق کند. بنابراین تابع $\varphi : F(X) \longrightarrow G$ را با $\varphi(1) = 1$ و برای واژه‌ی ناتهی $x_1^{\varepsilon_1} \cdots x_n^{\varepsilon_n}$ به صورت بالا تعریف می‌کنیم. چون G گروه است و $\varepsilon_i = \pm 1$، و $f(x_i) \in G$، حاصل‌ضرب $f(x_1)^{\varepsilon_1} f(x_2)^{\varepsilon_2} \cdots f(x_n)^{\varepsilon_n}$ عضوی از G است، یعنی φ خوش تعریف است. اثبات همریختی بودن φ را به عنوان تمرین واگذار می‌کنیم. حال فرض کنید $g : F(X) \longrightarrow G$ همریختی دیگری باشد که به ازای هر $x \in X$، $g(x) = f(x)$، آنگاه

$$\begin{aligned} g\left(x_1^{\varepsilon_1} x_2^{\varepsilon_2} \cdots x_n^{\varepsilon_n}\right) &= g\left(x_1^{\varepsilon_1}\right) g\left(x_2^{\varepsilon_2}\right) \cdots g\left(x_n^{\varepsilon_n}\right) \\ &= g(x_1)^{\varepsilon_1} g(x_2)^{\varepsilon_2} \cdots g(x_n)^{\varepsilon_n} \\ &= f(x_1)^{\varepsilon_1} f(x_2)^{\varepsilon_2} \cdots f(x_n)^{\varepsilon_n} \\ &= \varphi\left(x_1^{\varepsilon_1} x_2^{\varepsilon_2} \cdots x_n^{\varepsilon_n}\right). \end{aligned}$$

بنابراین $g = \varphi$ و φ یکتاست. □

نتیجه ۵.۱.۸. اگر F_1 گروه آزاد روی X_1 و F_2 گروه آزاد روی X_2 باشند و $|X_1| = |X_2|$، آنگاه $F_1 \cong F_2$. به ویژه هر دو گروه آزاد روی یک مجموعه یکریخت هستند.

اثبات. چون $|X_1| = |X_2|$ تابع دوسویی $f : X_1 \longrightarrow X_2$ وجود دارد. نمودارهای ۲.۸

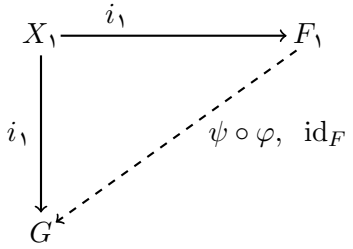


شکل ۲.۸: نمودارها تعویض‌پذیر هستند.

را در نظر بگیرید. چون $i_۱ \circ f^{-۱} : X_۲ \longrightarrow F_۱$ و $i_۲ \circ f : X_۱ \longrightarrow F_۲$ تابع هستند ، بنا به قضیه‌ی ۴.۱.۸، همریختی‌های یکتای $\varphi : F_۱ \longrightarrow F_۲$ و $\psi : F_۲ \longrightarrow F_i$ وجود دارند که نمودارهای ۲.۸، تعویض‌پذیرند. یعنی $\varphi \circ i_۱ = i_۲ \circ f$ و $\psi \circ i_۲ = i_۱ \circ f^{-۱}$، پس داریم

$$(\psi \circ \varphi) \circ i_۱ = \psi \circ (\varphi \circ i_۱) = \psi \circ (i_۲ \circ f) = (\psi \circ i_۲) \circ f = (i_۱ \circ f^{-۱}) \circ f = i_۱ .$$

از طرفی همریختی همانی $\mathrm{id}_{F_۱} : F_۱ \longrightarrow F_۱$ نیز در شرط $\mathrm{id}_{F_۱} \circ i_۱ = i_۱$ صدق می‌کند. بنابراین نمودار ۳.۸ هم به ازای همریختی



شکل ۳.۸: نمودار تعویض‌پذیر است.

$\varphi \circ \psi$ و هم به ازای همریختی $\mathrm{id}_{F_۱}$ تعویض‌پذیر است. بنا به قضیه‌ی ۴.۱.۸، $\psi \circ \varphi = \mathrm{id}_{F_۱}$. به همین نحو $\varphi \circ \psi = \mathrm{id}_{F_۲}$. پس φ و ψ همریختی‌های یک‌به‌یک و پوشا باشند و $F_۱ \cong F_۲$. □

نتیجه ۶.۱.۸. هر گروه دلخواه G تصویر همریخت یک گروه آزاد است.

اثبات. فرض کنید X یک مجموعه‌ی مولد دلخواه برای G باشد (G بزرگ‌ترین مجموعه‌ی مولد برای G است). گروه آزاد $F(X)$ روی X را در نظر می‌گیریم. فرض کنید $i_۱ : X \longrightarrow F$ و $i_۲ : X \longrightarrow G$ نگاشت‌های شمول باشند. بنا به قضیه‌ی ۴.۱.۸، همریختی یکتای $\varphi : F \longrightarrow G$ وجود دارد که $\varphi \circ i_۱ = i_۲$. این همریختی پوشاست، زیرا $G = \langle X \rangle$. در واقع اگر $u = x_۱^{\varepsilon_۱} \cdots x_n^{\varepsilon_n} \in G$، که در آن $x_i \in X$ و $\varepsilon_i = \pm ۱$، آنگاه

$$\begin{aligned} \varphi(x) &= \varphi(x_۱^{\varepsilon_۱} \cdots x_n^{\varepsilon_n}) \\ &= \varphi(x_۱)^{\varepsilon_۱} \cdots (x_n)^{\varepsilon_n} \\ &= \varphi(i_۱(x_۱))^{\varepsilon_۱} \cdots \varphi(i_n(x_n))^{\varepsilon_n} \\ &= i_۲(x_۱)^{\varepsilon_۱} \cdots i_۲(x_n)^{\varepsilon_n} \\ &= x_۱^{\varepsilon_۱} \cdots x_n^{\varepsilon_n} \\ &= u. \end{aligned}$$

اگر $N = \ker \varphi$، آنگاه $G = F/N$ و حکم ثابت است. □

در نتیجه ۶.۱.۸، دیدیم که هر گروه دلخواه را می‌توان از تصویر همریخت یک گروه آزاد به دست آورد. توصیف یک گروه به عنوان چنین تصویر همریخت را نمایش گروه نامیم. به طور دقیق‌تر فرض کنید X یک مجموعه‌ی مولد برای گروه G باشد. گروه آزاد F روی X و همریختی پوشای $\pi : F \longrightarrow G$ را در نظر می‌گیریم. اگر $N = \ker \pi$، آنگاه $F/N \cong G$. یک نمایش برای G عبارت است از زوج $\langle X, R \rangle$، که در آن R مجموعه‌ای از واژه‌ها در F است طوری که بستار نرمال $\langle R \rangle$ در F، (کوچک‌ترین زیرگروه نرمال F شامل $\langle R \rangle$، تمرین ۱۸ از صفحه‌ی ۸۳ را ببینید) برابر $\ker \pi$ باشد، یعنی $\langle R \rangle^F = \ker \pi$. عناصر X را مولدها و عناصر R را روابط G می‌نامیم و می‌نویسیم

$$G = \langle X \mid R \rangle .$$

اگر $X = \{x_۱, \ldots, x_n\}$ و $R = \{w_۱, \ldots, w_m\}$ می‌نویسیم

$$G = \langle x_۱, \ldots, x_n \mid w_۱ = w_۲ = \cdots = w_m = ۱ \rangle .$$

اگر مثلاً $w = w_۱ w_۲^{-۱}$ به جای $w = ۱$ می‌نویسیم $w_۱ = w_۲$.

قضیه ۷.۱.۸. (قضیه‌ی ون دایک) فرض کنید G و H زیرگروه‌هایی با نمایش‌های، به ترتیب، $\pi : F \longrightarrow G$ و $\varphi : F \longrightarrow H$ باشند طوری که هر رابطه‌ی π رابطه‌ی از φ نیز باشد (یعنی $\ker \pi \subseteq \ker \varphi$). در این صورت نگاشت $\psi : G \longrightarrow H$ با ضابطه‌ی $\psi(g) = \psi(\pi(u)) = \varphi(u)$ یک همریختی پوشا است.

اثبات. اگر $g \in G$، آنگاه به ازای یک $u \in F$ داریم $\pi(u) = g$. پس تابع $\psi : G \longrightarrow H$ را با ضابطه‌ی $\psi(g) = \psi(\pi(u)) = \varphi(u)$ تعریف می‌کنیم. ψ خوشتعریف است، زیرا اگر $\pi(u) = g = \pi(u_1)$، آنگاه $\pi(u^{-1}u_1) = 1$ و $u^{-1}u_1 \in \ker \pi \leq \ker \varphi$. پس $\varphi(u^{-1}u_1) = 1$ یا $\varphi(u) = \varphi(u_1)$. ψ پوشاست، زیرا به ازای هر $h \in H$، عضو $v \in F$ وجود دارد که $\varphi(v) = h$ و بنابراین $\psi(\pi(v)) = \varphi(v) = h$. در نگاشت ψ همریختی است، زیرا

$$\psi(\pi(u)\pi(v)) = \psi(\pi(uv)) = \varphi(uv) = \varphi(u)\varphi(v) = \psi(\pi(u))\psi(\pi(v)).$$

بنابراین ψ همریختی پوشاست. □

مثال ۸.۱.۸. نشان دهید $S_3 \cong D_6$.

حل می‌دانیم $D_6 = \langle \rho, \varepsilon \mid \rho^3 = \varepsilon^2 = 1 \rangle$، $\varepsilon\rho = \rho^{-1}\varepsilon$. اکنون در S_3 قرار می‌دهیم $x = (1\ 2\ 3)$ و $y = (1\ 2)$، آنگاه $x^3 = 1$، $y^2 = 1$ و $yx = x^{-1}y$. بنابراین بنا به قضیه‌ی ون دایک، همریختی $\varphi : D_6 \longrightarrow S_3$ وجود دارد که $\varphi(\rho) = x$ و $\varphi(\varepsilon) = y$. چون x و y، S_3 را تولید می‌کنند، φ پوشاست. چون مرتبه‌ی S_3 و D_6 هر دو ۶ است پس φ یک‌به‌یک نیز هست. پس φ یکریختی است و $S_3 \cong D_6$. □

تمرین‌ها

۱. نشان دهید مرتبه‌ی هر عضو نابدیهی در گروه آزاد، نامتناهی است.

۲. نشان دهید گروه آزاد با رتبه‌ی ۱ با $\mathbb{Z}$ یکریخت است.

۳. فرض کنید G گروه باشد و $X \subseteq G$. اگر هر عضو $g \in G$ به صورت یکتای $g = x_1^{n_1}x_2^{n_2}\cdots x_k^{n_k}$، نوشته شود که در آن $x_i \in X$، $k \geq 0$، $n_i \neq 0$، و $x_i \neq x_{i+1}$ نشان دهید G گروه آزاد روی X است.

۴. نشان دهید مرکز یک گروه آزاد، با رتبه‌ی بیش از یک، بدیهی است.

۵. نشان دهید یک گروه آبلی آزاد است اگر و تنها اگر دوری نامتناهی باشد.

۶. فرض کنید $z \in \mathbb{C}$ طوری باشد که $|z| \geq 2$. نشان دهید گروه تولید شده توسط ماتریس‌های

$$x = \begin{bmatrix} 1 & 0 \\ z & 1 \end{bmatrix} \quad \text{و} \quad y = \begin{bmatrix} 1 & z \\ 0 & 1 \end{bmatrix}$$

گروه آزاد روی $\{x, y\}$ است.

۷. فرض کنید H یک زیرگروه با شاخص متناهی در گروه آزاد F باشد. نشان دهید اشتراک هر زیرگروه نابدیهی F با H نابدیهی است.

۸. نماد ∞ را در نظر می‌گیریم و فرض می‌کنیم $\frac{1}{0} = \infty$، $\frac{1}{\infty} = 0$، ...
(الف) فرض کنید $a, b, c, d \in \mathbb{C}$ طوری باشند که $ad \neq bc$. نشان دهید تابع $\lambda(a, b, c, d) : \mathbb{C} \cup \{\infty\} \longrightarrow \mathbb{C} \cup \{\infty\}$ با ضابطه‌ی

$$\lambda(a, b, c, d)(z) = \frac{az + b}{cz + d}, \quad \forall z \in \mathbb{C} \cup \{\infty\}$$

یک جایگشت است. $\lambda(a, b, c, d)$ را تبدیل خطی کسری می‌نامیم.
(ب) جایگشت‌های $\psi, \varphi : \mathbb{C} \cup \{\infty\} \longrightarrow \mathbb{C} \cup \{\infty\}$ با ضابطه‌های

$$\psi(z) = \frac{z}{2z + 1} \quad \text{و} \quad \varphi(z) = z + 2$$

را در نظر گرفته نشان دهید $F = \langle \varphi, \psi \rangle$ یک گروه آزاد روی $\{\varphi, \psi\}$ است.

۹. (الف) نشان دهید مجموعه‌ی همه‌ی تبدیل‌های خطی کسری $\mathbb{C}$ تحت عمل یک گروه تشکیل می‌دهند (زیرگروه گروه جایگشت‌ها روی $\mathbb{C} \cup \{\infty\}$).
(ب) نشان دهید ضابطه‌ی

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \mapsto \lambda(a, b, c, d)$$

یک همریختی از $\mathrm{GL}_۲(\mathbb{C})$ به گروه تبدیلهای خطی کسری $\mathbb{C}$ را مشخص می‌کند و تحت این همریختی ماتریس‌های $A = \begin{bmatrix} ۱ & ۰ \\ ۲ & ۱ \end{bmatrix}$ و $B = \begin{bmatrix} ۱ & ۲ \\ ۰ & ۱ \end{bmatrix}$ به ترتیب به φ و ψ (در تمرین قبل) تصویر می‌شوند. نتیجه بگیرید $\langle A, B \rangle$ گروه آزاد روی مجموعه‌ی $\{A, B\}$ است.

۱۰. فرض کنید F یک گروه آزاد و G، H گروه‌های دلخواه باشند. اگر $\alpha : F \longrightarrow H$ یک همریختی و $\beta : G \longrightarrow H$ یک همریختی پوشا باشد، ثابت کنید یک همریختی $\gamma : F \longrightarrow G$ وجود دارد که $\beta\gamma = \alpha$.

۱۱. نشان دهید یک نمایش برای گروه کواترنیونی مرتبه‌ی ۸ به صورت زیر است

$$Q_۸ = \left\langle x, y \mid x^۲ = y^۲ \ , \ x^{-۱}yx = y^{-۱} \right\rangle .$$

۱۲. نشان دهید یک نمایش برای گروه دووجهی نامتناهی عبارت است از

$$D_۸ = \left\langle x, y \mid x^۲ = y^۲ = ۱ \right\rangle .$$

۱۳. نشان دهید یک نمایش برای $S_۳$ عبارت است از

$$S_۳ = \left\langle x, y \mid x^۲ = y^۳ = (xy)^۲ = ۱ \right\rangle .$$

۱۴. نشان دهید $\mathrm{Aut}\, Q_۸ \cong S_۴$.

۱۵. نشان دهید $\mathrm{Aut}\, D_۸ \cong D_۸$.

فصل ۹

مباحثی در نظریه‌ی گروه‌ها

در این فصل می‌خواهیم چند مبحث مقدماتی از نظریه‌ی گروه‌ها را مطرح کنیم. این مباحث به طور طبیعی از فصل‌های قبل ناشی می‌شوند. در این فصل هیچ تمرینی ارائه نمی‌کنیم؛ بلکه می‌خواهیم دانشجو درباره‌ی بسط و تعمیم مطالعه و ارائه سوال‌های جدید فکر کند. در پایان هر بخش تعدادی مرجع برای مطالعه‌ی بیشتر آورده‌ایم.

۱.۹ گروه‌هایی که اجتماع زیرگروه‌های سره‌شان هستند

قبلاً دیده‌ایم (تمرین ۳ صفحه‌ی ۶۹) که یک گروه را نمی‌توان به صورت اجتماع دو زیرگروه سره‌اش نوشت. هم‌چنین گروه کواترنیونی Q_8، از مرتبه‌ی ۸ را می‌توان به صورت اجتماع سه زیرگروه سره‌اش نمایش داد. سوالی که به طور طبیعی مطرح می‌شود این است که چه زیرگروه‌هایی را می‌توان به صورت اجتماع سه زیرگروه سره‌شان نمایش داد؟
فرض کنید A، B و C سه زیرگروه سره‌ی گروه G باشند طوری که

$$G = A \cup B \cup C$$

می‌خواهیم ساختار G را معین کنیم. ابتدا توجه می‌کنیم که مثلاً اگر $A \subseteq B$، آنگاه $G = B \cup C$، و این امکان ندارد. پس هیچ‌کدام از زیرگروه‌های A، B و C شامل دیگری نیستند. این تجزیه را تجزیه‌ی نابدیهی برای G گوییم. برای تعیین ساختار G به چند مرحله نیاز داریم. ابتدا نشان می‌دهیم اشتراک هر دو زیرگروه حتماً زیرگروه دیگر را قطع می‌کند، یعنی

لم ۱.۱.۹. $(A \cap B) - C = (A \cap C) - B = (B \cap C) - A = \emptyset$.

اثبات. چون تجزیه‌ی G به زیرگروه‌های A، B و C نابدیهی است عضو $x \in C - (A \cup B)$ وجود دارد. حال فرض کنید $a \in (A \cap B) - C$. چون $ax \in G = A \cup B \cup C$، سه حالت پیش می‌آید:

$$\begin{aligned} ax \in A &\Longrightarrow x \in A \qquad (a \in A \text{ چون}) \\ ax \in B &\Longrightarrow x \in B \qquad (a \in B \text{ چون}) \\ ax \in C &\Longrightarrow x \in C \qquad (x \in C \text{ چون}) \end{aligned}$$

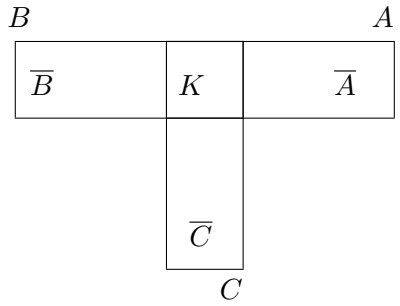
بنابراین هر سه حالت به تناقض می‌انجامد. در نتیجه $(A \cap B) - C = \emptyset$. به همین نحو $(A \cap C) - B = \emptyset$ و $(B \cap C) - A = \emptyset$. □

بنابراین وضعیت سه زیرگروه A، B و C به شکل ۱.۹ است. از این‌جا به بعد نمادهای زیر را اختیار می‌کنیم

$$\overline{A} = A - (B \cup C), \;\; \overline{B} = B - (A \cup C), \;\; \overline{C} = C - (A \cup B), \;\; K = A \cap B \cap C.$$

توجه کنید که تساوی‌های زیر برقرارند

$$A = \overline{A} \cup K, \;\; B = \overline{B} \cup K, \;\; C = \overline{C} \cup K.$$



شکل ۱.۹: وضعیت سه زیرگروه که اجتماع‌شان گروه را می‌پوشاند.

لم ۲.۱.۹. همه‌ی مجموعه‌های $\overline{A}$، $\overline{B}$ و $\overline{C}$ نسبت به داشتن وارون بسته‌اند.

اثبات. فرض کنید $a \in \overline{A}$. در این صورت $a \notin B$ و $a \notin C$. چون B و C زیرگروه هستند ، $a^{-1} \notin B$ و $a^{-1} \notin C$. پس $a^{-1} \in A$ و $a^{-1} \in \overline{A}$. به همین نحو مجموعه‌های دیگر نیز نسبت به وارون بسته‌اند. □

لم ۳.۱.۹. اگر $a \in \overline{A}$ و $b \in \overline{B}$، آنگاه $ab \in \overline{C}$.
اگر $b \in \overline{B}$ و $c \in \overline{C}$، آنگاه $bc \in \overline{A}$.
اگر $a \in \overline{A}$ و $c \in \overline{C}$، آنگاه $ac \in \overline{C}$.

اثبات. اگر $ab \in A \cup B$ دو حالت پیش می‌آید

$$ab \in A \Longrightarrow b \in A \qquad (\text{چون } a \in A)$$
$$ab \in B \Longrightarrow a \in B \qquad (\text{چون } b \in B)$$

بنابراین هر دو حالت منجر به تناقض می‌شود. از این‌رو $ab \notin A \cup B$ و $ab \in \overline{C}$. به همین نحو سایر گزاره‌ها ثابت می‌شوند. □

لم ۴.۱.۹. اگر $x, y \in \overline{A}$، آنگاه $xy \in K$.

اثبات. داریم $xy \in A = \overline{A} \cup K$. فرض کنید $xy \in \overline{A}$. عضو دلخواه $b \in \overline{B}$ را اختیار می‌کنیم و bxy را در نظر می‌گیریم. چون $x \in \overline{A}$ و $b \in \overline{B}$، طبق لم ۳.۱.۹، داریم $bx \in \overline{C}$. مجدداً طبق لم ۳.۱.۹، داریم $(bx)y \in \overline{B}$. از طرف دیگر چون $xy \in \overline{A}$ و $b \in \overline{B}$، طبق لم ۳.۱.۹، داریم $b(xy) \in \overline{C}$. در نتیجه $bxy \in \overline{B} \cap \overline{C} = \emptyset$، که تناقض است. پس $xy \in A \cap B \cap C$. □

لم ۵.۱.۹. $K = A \cap B \cap C$ زیرگروه نرمال G است.

اثبات. چون K برابر اشتراک زیرگروه‌هایی از G است، $K \leq G$. حال فرض کنید $k \in K$ و $x \in G$. اگر $x \in K$، چون K زیرگروه است، $x^{-1}kx \in K$. پس فرض کنید مثلاً $x \in \overline{A}$، بنا به لم ۲.۱.۹، داریم $x^{-1} \in \overline{A}$. اکنون داریم $kx \in A = \overline{A} \cup K$. اگر $kx \in K$، آنگاه چون K زیرگروه G است، $x \in K$ که تناقض است. پس $kx \in \overline{A}$. حال بنا به لم ۴.۱.۹، داریم $x^{-1}kx \in K$ و $K \trianglelefteq G$. □

لم ۶.۱.۹. اگر $a \in \overline{A}$، آنگاه $aK = \overline{A}$.
اگر $b \in \overline{B}$، آنگاه $bK = \overline{B}$.
اگر $c \in \overline{C}$، آنگاه $cK = \overline{C}$.

اثبات. فرض کنید $k \in K$. پس $ak \in A = \overline{A} \cup K$. اگر $ak \in K$، آنگاه $a \in K$ که تناقض است پس $ak \in \overline{A}$. بنابراین $aK \subseteq \overline{A}$.
حال فرض کنید $a \in \overline{A}$. بنا به لم ۲.۱.۹، $a^{-1} \in \overline{A}$. بنا به لم ۴.۱.۹، $a^{-1}x \in K$. در نتیجه $x \in aK$ و $\overline{A} \subseteq aK$. □

اکنون آماده‌ایم تا زیرگروه‌هایی را که اجتماع سه زیرگروه سره‌شان هستند را توصیف کنیم:

قضیه ۷.۱.۹. گروه G اجتماع (نابدیهی) سه زیرگروه سره‌ی خودش است اگر و تنها اگر G تصویر همریخت ۴-گروه کلاین، V، باشد.

اثبات. ($\Longleftarrow$) فرض کنید $G = A \cup B \cup C$ تجزیه‌ی نابدیهی G به سه زیرگروه سره‌اش باشد. قرار می‌دهیم $K = A \cap B \cap C$. طبق لم ۵.۱.۹، $K \trianglelefteq G$. برای هر $a \in \overline{A}$، طبق لم ۶.۱.۹، داریم $aK = \overline{A}$. به همین نحو، طبق لم ۶.۱.۹،

$$\begin{aligned} b \in B - (A \cup C) &\implies bK = B - (A \cup C) \\ c \in C - (A \cup B) &\implies cK = C - (A \cup B) \end{aligned}$$

بنابراین $\frac{G}{K} = \{K, aK, bK, cK\}$، که در آن $a \in \overline{A}$، $b \in \overline{B}$ و $c \in \overline{C}$. از طرف دیگر طبق لم ۳.۱.۹، $ab \in \overline{C}$. بنابراین

$$(aK)(bK) = (ab)K = C - (A \cup B) = cK.$$

به همین نحو $(aK)(cK) = bK$ و $(bK)(cK) = aK$. بنابراین $G/K \cong V$.
($\Longrightarrow$) حال فرض کنید G تصویر همریخت V باشد. پس زیرگروه نرمال K وجود دارد که

$$\frac{G}{K} = \{K, aK, bK, cK\} \cong V.$$

اکنون $\{K, aK\} \leq \frac{G}{K}$. اما $\{K, aK\} = \frac{A}{K}$ که در آن $A = K \cup aK$، که نتیجه می‌دهد A زیرگروهی از G است. به همین نحو $B = bK \cup K$ و $C = cK \cup K$ زیرگروه‌هایی از G هستند و

$$G = K \cup aK \cup bK \cup cK = A \cup B \cup C,$$

که حکم را ثابت می‌کند. □

نتیجه ۸.۱.۹. اگر گروه متناهی G اجتماع (نابدیهی) سه زیرگروه سره‌ی خودش باشد، آنگاه $|G| = ۴m$. □

توجه کنید عکس نتیجه i فوق درست نیست. زیرا گروه دوری $\mathbb{Z}_{۴m}$ اجتماع سه زیرگروه سره‌ی خودش نیست. گروهی که اجتماع نابدیهی سه زیرگروه سره‌ی خودش باشد، گروه ۳-مجموع گوییم. سوالی که در مورد گروه‌های ۳-مجموع مطرح می‌شود وضعیت ساختار زیرگروه‌های ظاهر شده در تجزیه است. می‌خواهیم این مطلب را بررسی کنیم. اگر $G = A \cup B \cup C$ تجزیه‌ی نابدیهی G به زیرگروه‌های سره باشد می‌نویسیم $G \longrightarrow \{A, B, C\}$. در این نمادگذاری به جای A، B و C از گروه‌های یکریخت با آن‌ها نیز استفاده می‌کنیم.

مثال ۹.۱.۹. ۴-گروه کلاین، V، تجزیه‌ای به صورت $V \longrightarrow \{C_۲, C_۲, C_۲\}$ دارد. □

مثال ۱۰.۱.۹. پنج گروه مرتبه‌ی ۸ وجود دارند: $C_۴ \times C_۲$، $C_۲ \times C_۲ \times C_۲$، $C_۸$، $D_۸$، $Q_۸$. به‌جز $C_۸$، همه‌ی این گروه‌ها را می‌توان به صورت اجتماع سه زیرگروه نابدیهی‌شان نوشت، این تجزیه‌ها به صورت زیر است

$$\begin{aligned} D_۸ &\longrightarrow \{C_۴, V, V\}, \qquad Q_۸ \longrightarrow \{C_۴, C_۴, C_۴\}, \\ C_۲ \times C_۴ &\longrightarrow \{C_۴, C_۴, V\}, \qquad C_۲ \times C_۲ \times C_۲ \longrightarrow \{V, V, V\}. \end{aligned}$$

حل داریم $D_۸ = \{۱, \rho, \rho^۲, \rho^۴, \varepsilon, \varepsilon\rho, \varepsilon\rho^۲, \varepsilon\rho^۳\}$. قرار می‌دهیم

$$\begin{aligned} A &= \langle \rho \rangle \cong \{۱, \rho, \rho^۲, \rho^۳\} \cong C_۴ \\ B &= \langle \rho^۲, \varepsilon \rangle = \{۱, \varepsilon\rho^۲, \varepsilon\rho^۲\} \cong V \\ C &= \langle \rho^۲, \varepsilon\rho \rangle = \{۱, \varepsilon\rho, \rho^۲, \varepsilon\rho^۳\} \cong V. \end{aligned}$$

در نتیجه $D_۸ = A \cup B \cup C$ و $D_۸ \longrightarrow \{C_۴, V, V\}$.
برای $Q_۸ = \{\pm ۱, \pm i, \pm j, \pm k\}$ قرار می‌دهیم

$$\begin{aligned} A &= \langle i \rangle = \{\pm ۱, \pm i\} \cong C_۴ \\ B &= \langle j \rangle = \{\pm ۱, \pm j\} \cong C_۴ \\ C &= \langle k \rangle = \{\pm ۱, \pm k\} \cong C_۴. \end{aligned}$$

پس $Q_۸ = A \cup B \cup C$ و $Q_۸ \longrightarrow \{C_۴, C_۴, C_۴\}$.
اکنون فرض کنید $G = \langle a, b \mid ab = ba, a^۲ = b^۴ = ۱ \rangle \cong C_۲ \times C_۴$. بنابراین

$$G = \{۱, a, b, b^۲, b^۳, ab, ab^۲, ab^۳\}.$$

قرار می‌دهیم

$$\begin{aligned} A &= \langle b \rangle = \{۱, b, b^۲, b^۳\} \cong C_۴ \\ B &= \langle ab^۳ \rangle = \{۱, ab^۳, b^۲, ab\} \cong C_۴ \\ C &= \langle a, ab^۲ \rangle = \{۱, a, ab^۲, b^۲\} \cong V. \end{aligned}$$

پس $D_۸ = A \cup B \cup C$ و $D_۸ \longrightarrow \{C_۴, C_۴, V\}$. □

مثال ۱۱.۱.۹. نشان دهید گروه دووجهی مرتبه‌ی $۴m$، $D_{۴m}$،یک گروه سه مجموع است و تجزیه‌ی آن را بیابید.

حل داریم

$$D_{۴m} = \langle \rho, \varepsilon \mid \rho^{۲m} = \varepsilon^۲ = ۱, \ \ \rho\varepsilon = \varepsilon\rho^{-۱} \rangle.$$

قرار می‌دهیم $K = \langle \rho^۲ \rangle = \{۱, \rho^۲, \ldots, \rho^{۲(m-۱)}\}$. توجه کنید $K \trianglelefteq D_{۴m}$ و

$$\frac{D_{۴m}}{K} = \{K, \rho K, \varepsilon K, \varepsilon\rho K\} \cong V.$$

پس بنا به قضیه‌ی ۷.۱.۹، $D_{۴m}$ یک گروه سه مجموع است. طبق اثبات قضیه‌ی ۷.۱.۹، قرار می‌دهیم

$$\begin{aligned} A &= \rho K \cup K = \{۱, \rho^۳, \rho^۵, \ldots, \rho^{۲m-۱}, \rho^۲, \rho^۴, \ldots, \rho^{۲(m-۱)}\} \\ &= \langle \rho \rangle \cong C_{۲m} \\ B &= \varepsilon K \cup K = \{۱, \varepsilon\rho^۲, \varepsilon\rho^۴, \cdots, \varepsilon\rho^{۲(m-۱)}, \rho^۲, \rho^۴, \ldots, \rho^{۲(m-۱)}\} \\ &= \langle \rho^۲, \varepsilon\rho^۲ \rangle \cong D_{۲m} \\ C &= \varepsilon\rho K \cup K = \{۱, \varepsilon\rho^۳, \varepsilon\rho^۳, \varepsilon\rho^۵, \ldots, \varepsilon\rho^{۲m-۱}, \rho^۲, \rho^۴, \ldots, \rho^{۲(m-۱)}\} \\ &= \langle \rho^۲, \varepsilon\rho^۳ \rangle \cong D_{۲m}. \end{aligned}$$

بنابراین $D_{۴m} \longrightarrow \{C_{۲m}, D_{۲m}, D_{۲m}\}$. □

آیا یک گروه ۳-مجموع می‌تواند تجزیه‌های متفاوت داشته باشد ؟ پاسخ مثبت است:

مثال ۱۲.۱.۹. نشان دهید دو تجزیه‌ی متفاوت به صورت زیر برای $C_۲ \times D_۸$ وجود دارد.

$$\begin{aligned} C_۲ \times D_۸ &\longrightarrow \{C_۲ \times C_۴, D_۸, D_۸\} \\ C_۲ \times D_۸ &\longrightarrow \{C_۲ \times C_۴, C_۲ \times C_۲ \times C_۲, C_۲ \times C_۲ \times C_۲\}. \end{aligned}$$

حل داریم

$$\begin{aligned} C_۲ \times D_۸ = \{&(۱,۱), (۱,\rho), (۱,\rho^۲), (۱,\rho^۳), (x,۱), (x,\rho), (x,\rho^۲), (x,\rho^۳), (۱,\varepsilon), \\ &(۱,\varepsilon\rho), (۱,\varepsilon\rho^۲), (۱,\varepsilon\rho^۳), (x,\varepsilon), (x,\varepsilon\rho), (x,\varepsilon\rho^۲), (x,\varepsilon\rho^۳)\}. \end{aligned}$$

قرار می‌دهیم $K = \langle (۱,\rho) \rangle = \{(۱,۱), (۱,\rho), (۱,\rho^۲), (۱,\rho^۳)\}$. به وضوح داریم $K \trianglelefteq C_۲ \times D_۸$ و

$$\frac{C_۲ \times D_۸}{K} = \{K, (۱,\varepsilon\rho)K, (x,\rho)K, (x,\varepsilon)K\} \cong V.$$

بنابراین (طبق اثبات قضیه‌ی ۷.۱.۹)

$$\begin{aligned} A &= K \cup (1, \varepsilon\rho)K \\ &= \{(1,1),(1,\rho),(1,\rho^2),(1,\rho^3),(1,\varepsilon\rho),(1,\varepsilon\rho^2),(1,\varepsilon\rho^3),(1,\varepsilon)\} \\ &\cong C_2 \times C_4 \\ B &= K \cup (x,\rho)K \\ &= \{(1,1),(1,\rho),(1,\rho^2),(1,\rho^3),(x,\rho),(x,\rho^2),(x,\rho^3)\} \cong D_8 \\ C &= K \cup (x,\varepsilon)K \\ &= \{(1,1),(1,\rho),(1,\rho^2),(1,\rho^3),(x,\varepsilon),(x,\varepsilon\rho),(x,\varepsilon\rho^2),(x,\varepsilon\rho^3)\} \\ &\cong D_8. \end{aligned}$$

در نتیجه $C_2 \times D_8 \longrightarrow \{C_2 \times C_4, D_8, D_8\}$. حال اگر قرار دهیم

$$K = \langle (x,1),(1,\rho^2)\rangle = \{(1,1),(x,1),(x,\rho^2),(x,\rho^2)\},$$

به طریق مشابه خواهیم داشت $\frac{C_2 \times D_8}{K} \cong V$، و تجزیه‌ی بعدی حاصل می‌شود. □

سوال دیگر ی که مطرح است این است: آیا دو گروه ۳-مجموع با تجزیه‌های یکسان می‌توانند نایکریخت باشند؟ مثال بعد به این سوال پاسخ مثبت می‌دهد.

مثال ۱۳.۱.۹. فرض کنید $G = \langle a,b,c \mid a^2 = b^2 = c^2 = 1, abc = cab = bca\rangle$. در این صورت G گروهی از مرتبه‌ی ۱۶ است که $G \ncong C_2 \times D_8$ و

$$G \longrightarrow \{C_2 \times C_4, D_8, D_8\}.$$

حل به راحتی می‌توان دید

$$G = \{1, a, b, c, ab, (ab)^2, , ca, bc, cb, abc, acb, aba, aca, bab\}.$$

توجه کنید

$$aba = cbc, \quad aca = bcb, \quad (ab)^2 = (ba)^2 = (ac)^2 = (ca)^2 = (abc)^2.$$

قرار می‌دهیم

$$K = \langle a, bab\rangle = \{1, a, bab, (ab)^2\}.$$

داریم $K \trianglelefteq G$ و

$$\frac{G}{K} = \{K, bK, cK, bcK\} \cong V.$$

بنابراین G گروهی ۳-مجموع است. داریم

$$\begin{aligned} bK &= \{b, ba, ab, aba\}, & A &= K \cup bK \cong D_8 \\ cK &= \{c, ca, ac, bcb\}, & B &= K \cup cK \cong D_8 \\ bcK &= \{bc, abc, acb, cb\}, & C &= K \cup bcK \cong C_2 \times C_4, \end{aligned}$$

و $G \longrightarrow \{C_2 \times C_4, D_8, D_8\}$. از طرف دیگر چون تعداد اعضای مرتبه‌ی ۲ در G برابر ۴ است و تعداد اعضای مرتبه‌ی ۲ در $C_2 \times D_8$ برابر ۱۱ Ta است، $G \ncong C_2 \times D_8$. □

یک زیرگروه در تجزیه‌ی یک گروه ۳-مجموع می‌تواند آبلی، $\mathscr{A}$، یا ناآبلی، $\mathscr{N}$، باشد. بنابراین چهار نوع تجزیه برای یک گروه ۳-مجموع ممکن است: $\{\mathscr{A},\mathscr{A},\mathscr{A}\}$، $\{\mathscr{A},\mathscr{A},\mathscr{N}\}$، $\{\mathscr{A},\mathscr{N},\mathscr{N}\}$، و $\{\mathscr{N},\mathscr{N},\mathscr{N}\}$. اما حالت $\{\mathscr{A},\mathscr{A},\mathscr{N}\}$ نمی‌تواند اتفاق بیافتد. این مطلب در لم بعدی نشان داده شده است.

لم ۱۴.۱.۹. فرض کنید $G = A \cup B \cup C$ یک تجزیه‌ی نابدیهی برای گروه G باشد. اگر A و B آبلی باشند، آنگاه C نیز آبلی است.

اثبات. چون $K = A \cap B \cap C \subseteq A$، K آبلی است. فرض کنید $c_۱, c_۲ \in \overline{C}$، داریم $\frac{G}{K} = \{K, aK, bK, cK\} \cong V$، که در آن $a \in \overline{A}$، $b \in \overline{B}$ و $c \in \overline{C}$، هر عضو دلخواهی هستند. چون $abK = (aK)(bK) = c_۱K$ عضو $k_۱ \in K$ وجود دارد که $c_۱ = abk_۱$. به همین نحو چون $abK = c_۲K$، عضو $k_۲ \in K$ وجود دارد که $c_۲ = abk_۲$. در نتیجه، چون A، B و K آبلی‌اند، داریم

$$c_۱c_۲ = (abk_۱)(abk_۲) = (abk_۲)(abk_۱) = c_۲c_۱,$$

یعنی اعضای $\overline{C}$ با یکدیگر تعویض می‌شوند. به همین صورت اعضای $\overline{C}$ و K با یکدیگر تعویض می‌شوند. پس $C = \overline{C} \cup K$ آبلی است. □

مثال بعدی نشان می‌دهد که سه تجزیه‌ی دیگر امکانپذیر هستند.

مثال ۱۵.۱.۹. (الف) تجزیه‌ی $Q_۸ \longrightarrow \{C_۴, C_۴, C_۴\}$ به صورت $G \longrightarrow \{\mathscr{A}, \mathscr{A}, \mathscr{A}\}$ است.
(ب) تجزیه‌ی $D_{۱۲} \longrightarrow \{C_۶, S_۳, S_۳\}$ به صورت $G \longrightarrow \{\mathscr{A}, \mathscr{N}, \mathscr{N}\}$ است.
(ج) تجزیه‌ی $S_۳ \times V \longrightarrow \{D_{۱۲}, D_{۱۲}, D_{۱۲}\}$ به صورت $G \longrightarrow \{\mathscr{N}, \mathscr{N}, \mathscr{N}\}$ است.

حل (الف) واضح است.
(ب) قرار می‌دهیم $K = \langle \rho^۲ \rangle = \{۱, \rho^۲, \rho^۴\}$. داریم $K \trianglelefteq D_{۱۲}$ و

$$\frac{G}{K} = \{K, \rho^۳K, \varepsilon K, \varepsilon\rho^۳K\} \cong V.$$

به علاوه

$$\begin{aligned} A &= K \cup \rho^۳K = \{۱, \rho^۲, \rho^۴, \rho^۳, \rho^۵, \rho\} \cong C_۶ \\ B &= K \cup \varepsilon K = \{۱, \rho^۲, \rho^۴, \varepsilon, \varepsilon\rho^۲, \varepsilon\rho^۴\} \cong S_۳ \\ C &= K \cup \varepsilon\rho^۳K = \{۱, \rho^۲, \rho^۴, \varepsilon\rho^۳, \varepsilon\rho^۵, \varepsilon\rho\} \cong S_۳. \end{aligned}$$

(ج) قرار می‌دهیم $K = S_۳ \times \{۱\}$. پس $K \trianglelefteq S_۳ \times V$ و

$$\frac{S_۳ \times V}{K} = \{K, (۱, a)K, (۱, b)K, (۱, ab)K\} \cong V.$$

به علاوه

$$\begin{aligned} A &= K \cup (۱, a)K \cong D_{۱۲} \\ B &= K \cup (۱, b)K \cong D_{۱۲} \\ C &= K \cup (۱, ab)K \cong D_{۱۲}. \end{aligned}$$

بنابراین در هر سه مورد تجزیه‌های مورد نظر به دست آمد. □

لم و مثال قبل را در قضیه‌ی زیر جمع‌بندی می‌کنیم.

قضیه ۱۶.۱.۹. هر تجزیه‌ی یک گروه ۳-مجموع به یکی از صورت های زیر است

$$\{\mathscr{A}, \mathscr{A}, \mathscr{A}\}, \quad \{\mathscr{A}, \mathscr{N}, \mathscr{N}\}, \quad \{\mathscr{N}, \mathscr{N}, \mathscr{N}\}. \qquad \square$$

اکنون حالتی را در نظر می‌گیریم که گروه ۳-مجموع به گروه‌های آبلی تجزیه شود.

قضیه ۱۷.۱.۹. اگر $G = A \cup B \cup C$ تجزیه‌ی گروه ۳-مجموع ناآبلی G باشد، آنگاه $G \longrightarrow \{\mathscr{A}, \mathscr{A}, \mathscr{A}\}$ اگر و تنها اگر $A \cap B \cap C = Z(G)$.

اثبات. قرار می‌دهیم $K = A \cap B \cap C$. ابتدا فرض کنید A، B و C آبلی باشند. چون $G = A \cup B \cup C$، داریم $K \subseteq Z(G)$. حال نشان می‌دهیم $\overline{A} \cap Z(G) = \emptyset$. فرض کنید $a \in \overline{A} \cap Z(G)$. بنا به لم ۲.۱.۹، $a^{-1} \in \overline{A}$. به ازای هر $c \in \overline{C}$، بنا به لم ۳.۱.۹، داریم $a^{-1}c \in \overline{B}$. پس $b \in \overline{B}$ وجود دارد که $a^{-1}c = b$، یعنی $c = ab$. در نتیجه برای هر $b_1 \in B$ داریم $b_1c = cb_1$ (زیرا $a \in Z(G)$ و B آبلی است). بنابراین هر دو عضو $\overline{B}$ و $\overline{C}$ با یکدیگر تعویض می‌شوند چون $K \leq Z(G)$، $B = \overline{B} \cup K$ و $C = \overline{C} \cup K$، همه‌ی عضوهای B و C با یکدیگر تعویض می‌شوند.
به علاوه به ازای هر $a \in \overline{A}$، چون $ak = a_1k$، عضو $k \in K$ وجود دارد که $a_1 = ak$. بنابراین به ازای هر $b_1 \in B$، $a_1b_1 = b_1a_1$، (زیرا $K \leq Z(G)$ و $a \in Z(G)$). پس عضوهای A و B نیز با یکدیگر تعویض می‌شوند. به طریق مشابه عضوهای A و C نیز با یکدیگر تعویض می‌شوند. بنابراین G آبلی است. این تناقض است. پس $\overline{A} \cap Z(C) = \emptyset$. به همین صورت $\overline{B} \cap Z(G) = \emptyset$ و $\overline{C} \cap Z(G) = \emptyset$. بنابراین $Z(G) \subseteq A \cap B \cap C = K$. □

قضیه ۱۸.۱.۹. اگر $G = A \cap B \cup C$ تجزیه‌ی نابدیهی گروه ۳-مجموع G باشد، که در آن A آبلی و B و C ناآبلی‌اند، آنگاه $Z(G) \subseteq A$.

اثبات. فرض کنید $K = A \cap B \cap C$، نشان می‌دهیم $\overline{B} \cap Z(G) = \emptyset$. فرض کنید چنین نباشد و $b \in \overline{B} \cap Z(G)$. به ازای هر $b_1 \in \overline{B}$، چون $bK = b_1K$، عضو $k \in K$ وجود دارد که $b_1 = bk$. چون $B = \overline{B} \cup K$، و K آبلی است و $b \in Z(G)$ پس B آبلی است، که تناقض است. پس $\overline{B} \cap Z(G) = \emptyset$. به طریق مشابه $\overline{C} \cap Z(G) = \emptyset$. بنابراین $Z(G) \subseteq A$. □

مثال ۱۹.۱.۹. برای $G = D_{12} \longrightarrow \{C_6, S_3, S_3\}$، داریم $\overline{A} \cap Z(G) = \emptyset$. □

از قضایای ۱۷.۱.۹ و ۱۸.۱.۹، نتیجه می‌گیریم که اگر G دارای تجزیه‌ی $\{A, B, C\}$ از نوع $\{\mathscr{A}, \mathscr{N}, \mathscr{N}\}$ باشد، آنگاه یا $Z(G)$ به طور سره از $K = A \cap B \cap C$ قرار دارد یا حداکثر عناصری از $A - (B \cap C)$ را نیز شامل می‌شود. در حالتی که تجزیه‌ی G از نوع $\{\mathscr{N}, \mathscr{N}, \mathscr{N}\}$ باشد در مورد $Z(G)$ چه می‌توان گفت؟ فرض کنید $G = A \cup B \cup C$ تجزیه‌ی نابدیهی گروه ۳-مجموع G باشد که در آن A، B و C ناآبلی هستند. اگر $\overline{A} \cap Z(G) = \emptyset$ و $\overline{B} \cap Z(G) = \emptyset$، آنگاه $\overline{C} \cap Z(G) = \emptyset$. زیرا در غیر این صورت $Z(G) = (Z(G) \cap A) \cup (Z(G) \cap B)$ که تجزیه‌ی گروه $Z(G)$ به دو زیرگروه سره است. پس این امکان وجود دارد که $Z(G)$ شامل عناصرا از $\overline{A}$، $\overline{B}$ و $\overline{C}$ باشد. در این حالت $Z(G)$ لزوماً گروه ۳-مجموع با تجزیه‌ی $Z(G) = (Z(G) \cap A) \cup (Z(G) \cap B) \cup (Z(G) \cap C)$ است. وجود چنین تجزیه‌ای ایجاب می‌کند که $K = A \cap B \cap C$ ناآبلی است. زیرا اگر K آبلی باشد، آنگاه مثلاً ثابت می‌شود B آبلی است. روش اثبات مشابه قضیه‌ی ۷.۱.۹، است: فرض کنید $b \in [B - (A \cup B)] \cap Z(G)$. به ازای هر $\overline{B}$ $b_1 \in$، چون $bk = b_1k$، عضو $k \in K$ وجود دارد که $b_1 = bk$. چون $B = \overline{B} \cup K$ و K آبلی است و $b \in Z(G)$، نتیجه می‌شود که B آبلی است.

مثال ۲۰.۱.۹. در تجزیه‌ی $S_3 \times V \longrightarrow \{D_{12}, D_{12}, D_{12}\}$ به سادگی می‌توان دید که هیچ‌کدام از مجموعه‌های $\overline{A} \cap Z(G)$، $\overline{B} \cap Z(G)$ و $\overline{C} \cap Z(G)$ تهی نیستند. □

اکنون تعمیم ایده‌ی نمایش G به صورت اجتماع نابدیهی ۳-زیرگروه را در نظر می‌گیریم.

تعریف ۲۱.۱.۹. گروه G را یک گروه n-مجموع گوییم هرگاه بتوان آن را به صورت اجتماع n زیرگروه سره‌اش و نه تعداد کمتر از n نوشت در این حالت می‌نویسیم $\sigma(G) = n$.

بنابراین گروه G، n-مجموع است اگر و تنها اگر زیرگروه‌های سره‌ی H_1، ...، H_n از G وجود داشته باشند که $G = \bigcup_{i=1}^{n} H_i$ و $H_j \nsubseteq \bigcup_{\substack{i=1 \\ i \neq j}} H_i$ و به علاوه نتوان G را به صورت اجتماع تعداد کمتر از n زیرگروه نوشت. یک گروه دوری را نمی‌توان به صورت اجتماع زیرگروه‌های سره‌اش نوشت، زیرا هیچ زیرگروه سره‌ای که شامل مولد گروه باشد وجود ندارد. برای سادگی کار وقتی که G گروه دوری باشد قرار داد می‌کنیم $\sigma(G) = \infty$. از این جا به بعد همه‌ی گروه‌های مورد بررسی را متناهی فرض می‌کنیم.
فرض کنید G گروه n-مجموع باشد و $G = \bigcup_{i=1}^{n} H_i$، که در آن به ازای هر i، H_i زیرگروه سره‌ی G است. به علاوه می‌توانیم فرض کنیم

هر H_i زیرگروه ماکسیمال G است، زیرا در یک گروه متناهی هر زیرگروه سره در یک زیرگروه ماکسیمال قرار می‌گیرد. که می‌توان در تجزیه‌ی G به اجتماع n- زیرگروه سره زیرگروه‌های ماکسیمال را جایگزین کرد و مجدداً یک تجزیه‌ی به اجتماع n زیرگروه سره و ماکسیمال به دست آورد. به علاوه در تمامی بحث فرض می‌کنیم H_i ها طوری مرتب شده‌اند که شاخصهای آن‌ها به ترتیب صعودی باشد، یعنی

$$|G : H_۱| \leq |G : H_۲| \leq \cdots \leq |G : H_n|.$$

بنابراین

$$|H_۱| \geq |H_۲| \geq \cdots \geq |H_n|.$$

قضیه ۲۲.۱.۹. فرض کنید $G = \bigcup_{i=۱}^{n} H_i$، با قراردادهای بالا داریم $|G| \leq \sum_{i=۲}^{n} |H_i|$ و تساوی برقرار است اگر و تنها اگر (الف) برای $i \neq ۱$، $H_۱H_i = G$ و (ب) برای $i \neq j$، $H_i \cap H_j \subseteq H_۱$.

اثبات. تعداد عناصر H_i که در $H_۱$ قرار ندارند برابر است با

$$\begin{aligned} |H_i| - |H_۱ \cap H_i| &= |H_i| - \frac{|H_۱||H_i|}{|H_۱H_i|} \\ &\leq |H_i| - \frac{|H_۱||H_i|}{|G|} = |H_i|\left(۱ - \frac{|H_۱|}{|G|}\right) \end{aligned} \quad (۱)$$

بنابراین

$$\begin{aligned} |G| = \left|\bigcup_{i=۱}^{n} H_i\right| &\leq |H_۱| + \sum_{i=۲}^{n}(|H_i| - (|H_۱ \cap H_i|)) \\ &\leq |H_۱| + \left(۱ - \frac{|H_۱|}{|G|}\right)\sum_{i=۲}^{n}|H_i|. \end{aligned} \quad (۲)$$

که از آن نامساوی مورد نظر $|G| \leq \sum_{i=۲}^{n} |H_i|$ حاصل‌ضرب می‌شود. تساوی برقرار است اگر و تنها اگر در هر دو نامساوی مراحل بالا تساوی برقرار باشد. در (۱) تساوی برقرار است اگر و تنها اگر $|G| = |H_۱H_i|$، یعنی $G = H_۱H_i$. در (۳) تساوی برقرار است اگر و تنها اگر هیچ دو زیرگروهی عضو مشترکی نداشته باشند که در $H_۱$ نیز نباشد، یعنی $H_i \cap H_j \subseteq H_۱$، برای هر $i \neq j$. □

لم ۲۳.۱.۹. فرض کنید $\sigma(G) = n$ و $G = \bigcup_{i=۱}^{n} H_i$. با استفاده از قراردادهای بالا داریم $|G : H_۲| \leq n - ۱$.

اثبات. طبق قضیه‌ی ۲۲.۱.۹، داریم $|G| \leq |H_۲| + \cdots + |H_n|$. چون

$$|H_۱| \geq |H_۲| \geq \cdots \geq |H_n|$$

داریم

$$\frac{|G|}{|H_۲|} \leq ۱ + \frac{|H_۳|}{|H_۲|} + \cdots + \frac{|H_n|}{|H_۲|} \leq \underbrace{۱ + \cdots + ۱}_{(n-۱)\text{ بار}} = n - ۱. \qquad \square$$

نتیجه ۲۴.۱.۹. $\sigma(G) = ۳$ اگر و تنها اگر G حداقل دو زیرگروه با شاخص ۲ داشته باشد.

اثبات. فرض کنید $G = H_۱ \cup H_۲ \cup H_۳$. با قراردادهای بالا و با استفاده از لم ۲۳.۱.۹، داریم $|G : H_۲| \leq ۲$. چون $H_۲ < G$، $|G : H_۲| = ۲$. از طرف دیگر چون $|G : H_۱| \leq |G : H_۲| = ۲$، داریم $|G : H_۱| = ۲$. بنابراین $H_۱$ و $H_۲$ دو زیرگروه با شاخص ۲ هستند. برعکس اگر G دو زیرگروه $H_۱$ و $H_۲$ با شاخص ۲ داشته باشد، آنگاه $H_۱$ و $H_۲$ در G نرمال‌اند. در نتیجه $N = H_۱ \cap H_۲$ در G نرمال است. چون

$$\frac{G}{N} = \frac{G}{H_۱ \cap H_۲} \hookrightarrow \frac{G}{H_۱} \times \frac{G}{H_۲} \cong C_۲ \times C_۲.$$

بنابراین $\frac{G}{N} \cong C_۲ \times C_۲$ و G گروه ۳-مجموع است. □

نتیجه ۲۵.۱.۹. گروه G با $\sigma(G) = ۲$ وجود ندارد.

اثبات. فرض کنید $G = H_۱ \cup H_۲$، با قراردادهای بالا داریم $|G : H_۲| \leq ۱$، یعنی $G = H_۲$ که تناقض است. □

قضیه ۲۶.۱.۹. G یک گروه ۴-مجموع است اگر و تنها اگر $\sigma(G) \neq ۳$ و G حداقل دو زیرگروه با شاخص ۳ داشته باشد.

اثبات. ($\Longleftarrow$) فرض کنید $G = \bigcup_{i=۱}^{۴} H_i$. با نمادهای بالا داریم $|G : H_۲| \leq ۳$. اگر $|G : H_۲| = ۲$، آنگاه $|G : H_۱| = ۲$ و بنا به نتیجه‌ی ۲۴.۱.۹، C گروه ۳-مجموع است، که تناقض است. پس $|G : H_۲| = ۳$.
بنا به قضیه‌ی ۲۲.۱.۹، داریم $|G| \leq |H_۲| + |H_۳| + |H_۴|$ و

$$۱ \leq \frac{|H_۲|}{|G|} + \frac{|H_۳|}{|G|} + \frac{|H_۴|}{|G|}.$$

چون $|G : H_۲| = ۳$ داریم

$$\frac{۲}{۳} \leq \frac{۱}{|G : H_۳|} + \frac{۱}{|G : H_۴|}.$$

چون $|G : H_۴| \leq |G : H_۲| \leq |G : H_۲| = ۳$، تنها حالت ممکن این است که $|G : H_۳| = |G : H_۴| = ۳$.
($\Longrightarrow$) اکنون فرض کنید $\sigma(G) \neq ۳$ و G دو زیرگروه A و B با شاخص ۳ داشته باشد. دو حالت وجود دارد.
حالت اول. $A \trianglelefteq G$ و $B \trianglelefteq G$. در این حالت $N = A \cap B \trianglelefteq G$ و چون A و B در G ماکسیمال هستند.

$$\frac{G}{N} = \frac{G}{A \cap B} \cong \frac{G}{A} \times \frac{G}{B} \cong C_۳ \times C_۳$$

در نتیجه $\sigma(G) = ۴$. زیرا اگر $G/N \cong C_۳ \times C_۳$، آنگاه

$$\frac{G}{N} = \{N, xN, x^۲N, yN, y^۲N, xyN, x^۲y^۲N, xy^۲N, x^۲yN\}.$$

قرار می‌دهیم

$$\begin{aligned} H_۱ &= \langle x \rangle N = N \cup xN \cup x^۲N \\ H_۲ &= \langle y \rangle N = N \cup yN \cup y^۲N \\ H_۳ &= \langle xy \rangle N = N \cup xyN \cup x^۲y^۲N \\ H_۴ &= \langle x^۲y \rangle N = N \cup x^۲yN \cup xy^۲N. \end{aligned}$$

در نتیجه $G = H_۱ \cup H_۲ \cup H_۳ \cup H_۴$. چون $\sigma(G) \neq ۳$ خواهیم داشت $\sigma(G) = ۴$.
حالت دوم. $A \not\trianglelefteq G$. چون $|G : A| = ۳$، عمل G روی هم مجموعه‌های چپ A در G یک همریختی $\rho : G \longrightarrow S_۳$ به دست می‌دهد. به علاوه $\ker \rho = A_G \leq A$. از طرف دیگر چون $A \leq N_G(A) \leq G$ و A ماکسیمال است و در G نرمال نیست، $A = N_G(A)$. بنابراین تعداد مزدوج‌های A در G برابر $|G : N_G(A)| = |G : A| = ۳$ است. اگر A، $xAx^{-۱}$ و $yAy^{-۱}$ مزدوج‌های متمایز A باشند، داریم $\ker \rho = A_G = A \cap xAx^{-۱} \cap yAy^{-۱}$، بنابراین A/A_G و $xAx^{-۱}/A_G$ و $yAy^{-۱}/A_G$ سه زیرگروه متمایز هم مرتبه از G/A_G هستند. پس G/A_G نمی‌تواند دوری باشد. چون $G/A_G = G/\ker \rho$ با زیرگروهی از $S_۳$ یکریخت است و دوری نیست، $G/A_G \cong S_۳$. از این‌رو $\sigma(G) = ۴$. زیرا اگر $G/N \cong S_۳$، که در آن $N = A_G$، آنگاه

$$\frac{G}{N} = \{N, xN, yN, zN, uN, u^۲N\}.$$

قرار می‌دهیم

$$\begin{aligned} H_۱ &= \langle x \rangle N = N \cup xN \\ H_۲ &= \langle y \rangle N = N \cup yN \\ H_۳ &= \langle z \rangle N = N \cup zN \\ H_۴ &= \langle u \rangle N = N \cup uN \cup u^۲N. \end{aligned}$$

در نتیجه $G = H_۱ \cup H_۲ \cup H_۳ \cup H_۴$. چون $\sigma(G) \neq ۳$ خواهیم داشت $\sigma(G) = ۴$. □

برای بررسی گروه‌های ۵-مجموع به قدری مقدمه نیاز داریم. ابتدا یک لم ساده را ثابت می‌کنیم:

لم ۲۷.۱.۹. اگر H زیرگروه ماکسیمال گروه G باشد، آنگاه یا H دقیقاً $|G : H|$ تا مزدوج دارد یا $H \trianglelefteq G$ و $|G : H|$ عدد اول است.

اثبات. داریم $H \leq N_G(H) \leq G$. چون H ماکسیمال است، دو حالت پیش می‌آید.
حالت اول. $H = N_G(H)$. در این حالت به تعداد $|G : H| = |G : N_G(H)|$ مزدوج برای H وجود دارد.
حالت دوم. $G = N_G(H)$. در این حالت $H \trianglelefteq G$ و چون H ماکسیمال است، G/H زیرگروه نابدیهی ندارد و $|G/H|$ عدد اول است. □

لم ۲۸.۱.۹. اگر $N \trianglelefteq G$، آنگاه $\sigma(G) \leq \sigma(G/N)$.

اثبات. فرض کنید $\frac{G}{N} = \bigcup_{i=۱}^{n} \frac{H_i}{N}$. چون $N \trianglelefteq G$، به ازای هر i، $H_iN \leq G$. به علاوه $G = \bigcup_{i=۱}^{n} H_iN$، که نتیجه می‌دهد $\sigma(G) \leq \sigma(G/N)$. □

قضیه ۲۹.۱.۹. اگر G یک p-گروه غیر دوری باشد، آنگاه $\sigma(G) = p + ۱$.

اثبات. فرض کنید $G = \bigcup_{i=۱}^{n} H_i$، که در آن $n = \sigma(G)$. با قراردادهای بالا داریم $|G : H_۲| \leq n - ۱ = \sigma(G) - ۱$. چون شاخص هر زیرگروه سره حداقل برابر p است، داریم $p \leq \sigma(G) - ۱$. پس $\sigma(G) \geq p + ۱$.
حال نشان می‌دهیم $\sigma(G) \leq p + ۱$. ابتدا فرض کنید G گروه آبلی غیر دوری باشد. در این صورت G حاصل‌ضرب مستقیم دو p-گروه آبلی است. بنابراین G گروه خارج‌قسمتی G/N یکریخت با $C_p \times C_p$ دارد. از این‌رو

$$\sigma(G) \leq \sigma(G/N) = \sigma(C_p \times C_p) = p + ۱.$$

اکنون حالت کلی را در نظر بگیرید. فرض کنید $|G| = p^k$، $k \geq ۲$. برای حالت $k = ۲$، $G \cong C_p \times C_p$ آبلی است و حکم ثابت است. در $k \geq ۳$؛ اگر G آبلی باشد، حکم از مرحله‌ی قبل ثابت است. در غیر این صورت $G/Z(G)$ یک p-گروه غیر دوری با مرتبه‌ی کمتر از $|G|$ است. پس بنا به فرض استقرا و لم قبل داریم $\sigma(G) \leq \sigma(G/Z(G)) \leq p + ۱$. □

لم ۳۰.۱.۹. اگر p عدد اول باشد $\sigma(C_p \times C_p) = p + ۱$.

اثبات. چون شاخص هر زیرگروه سره‌ی $C_p \times C_p$ برابر p است، بنا به لم ۲۸.۱.۹، داریم $\sigma(C_p \times C_p) \geq p + ۱$. اگر a و b مولدهای گروه $G = C_p \times C_p$ باشند، آنگاه G اجتماع $p + ۱$ زیرگروه دوری $\langle ab^i \rangle$، $۱ \leq i \leq p - ۱$ و $\langle b \rangle$ است، یعنی $\sigma(G) \leq p + ۱$. □

قضیه ۳۱.۱.۹. گروه G، ۵-مجموع است اگر و تنها اگر $\sigma(G) \neq ۳, ۴$ و G یک زیرگروه ماکسیمال با شاخص ۴ داشته باشد.

اثبات. ($\Longleftarrow$) فرض کنید $G = \bigcup_{i=۱}^{۵} H_i$. با قراردادهای بالا داریم $|G : H_۲| \leq ۴$. اگر $|G : H_۲| = ۲$، آنگاه $|G : H_۱| = ۲$ و بنا به قضیه‌ی ۲۴.۱.۹، $\sigma(G) = ۳$ که تناقض است. فرض کنید $|G : H_۲| = ۳$. با استفاده از قضیه‌ی ۱۷.۱.۹، داریم $|G| \leq |H_۲| + |H_۳| + |H_۴| + |H_۵|$، که نتیجه می‌دهد

$$۱ \leq \frac{|H_۲|}{|G|} + \frac{|H_۳|}{|G|} + \frac{|H_۴|}{|G|} + \frac{|H_۵|}{|G|}.$$

چون $|G : H_۲| = ۳$،

$$\frac{۲}{۳} \leq \frac{۱}{|G : H_۳|} + \frac{۱}{|G : H_۴|} + \frac{۱}{|G : H_۵|}.$$

در نتیجه $|G : H_۳| \leq ۴$. زیرا اگر $|G : H_۳| > ۴$، آنگاه

$$\frac{۵}{۱۲} < \frac{۱}{|G : H_۴|} + \frac{۱}{|G : H_۵|} + \frac{۱}{|G : H_۳|} < \frac{۱}{۴}.$$

چون $|G:H_۵| \leq |G:H_۴| \leq |G:H_۳| < ۴$، داریم $۵ < |G:H_۲| \leq |G:H_۵|$ و $\frac{۲}{۵} \leq \frac{۵}{۱۲}$ که تناقض است. بنابراین $|G:H_۳| \leq ۴$. اگر $|G:H_۳| = ۳$، آنگاه بنا به قضیه‌ی ۲۶.۱.۹، $\sigma(G) = ۴$ که تناقض است پس $|G:H_۳| = ۴$ و حکم ثابت است.

($\Longleftarrow$) فرض کنید $\sigma(G) \neq ۳, ۴$ و B یک زیرگروه ماکسیمال G با شاخص ۴ باشد. چون شاخص B در G عدد اول نیست، $B \not\trianglelefteq G$. پس بنا به لم ۲۷.۱.۹، B دقیقاً چهار مزدوج در G دارد. از طرف دیگر عمل G روی هم مجموعه‌های چپ B در G منجر به همریختی $\rho : G \longrightarrow S_۴$ با $\ker \rho = B_G = \bigcap_{g \in G} gBg^{-۱}$ می‌شود. چون $\frac{G}{B_G}$ با زیرگروهی از $S_۴$ یکریخت است و $\frac{B}{B_G}$ زیرگروهی از $\frac{G}{B_G}$ با شاخص ۴ است، پس $|G/B_G|$ برابر ۸، ۲۱ یا ۴۲ است. به علاوه G/B_G دوری نیست زیرا ۴ زیرگروه به صورت K/B_G با مرتبه‌های یکسان دارد ، که در آن K یک مزدوج دلخواه از B است.

اگر $|G/B_G| = ۸$، آنگاه بنا به قضیه‌ی ۲۹.۱.۹، $\sigma(G/B_G) = ۳ = ۲ + ۱$. اما بنا به لم ۲۸.۱.۹، $۴ < \sigma(G) \leq \sigma(G/B_G) = ۳$ که تناقض است. اگر $|G/B_G| = ۲۴$، آنگاه $G/B_G \cong S_۴$. اما $\frac{S_۴}{V} \cong S_۳$ که در آن V، ۴-گروه کلاین است. پس بنا به لم ۲۸.۱.۹، $۴ < \sigma(G) \leq \sigma(G/B_C) = \sigma(S_۴) \leq \sigma(S_۴/V) = \sigma(S_۳) = ۴$ که مجدداً تناقض است. بنابراین تنها حالت ممکن $|G/B_G| = ۱۲$ است. چون تنها زیرگروه مرتبه ۲۱ از $S_۴$ برابر $A_۴$ است. در نتیجه بنا به لم ۲۸.۱.۹، $۵ = \sigma(G) \leq \sigma(G/B_G) = \sigma(A_۴) = ۵$، که نتیجه می‌دهد $\sigma(G) = ۵$ و حکم ثابت است. □

از این جا تا انتهای این بخش، به قضایای سیلو، در فصل ۵، و گروه‌های پوچ‌توان، در فصل ۷، نیاز داریم. چون یک گروه پوچ‌توان متناهی G حاصل‌ضرب مستقیم زیرگروه‌های سیلو است. بنا به قضیه‌ی ۲۹.۱.۹، می‌توان $\sigma(G)$ را تعیین کرد مشروط به این که $\sigma(H \times K)$ را بیابیم.

لم ۳۲.۱.۹. اگر H و K گروه باشند، آنگاه $\sigma(H \times K) \leq \min\{\sigma(H), \sigma(K)\}$.

اثبات. بنا به لم ۲۸.۱.۹، داریم

$$\sigma(H \times K) \leq \sigma\left(\frac{H \times K}{\{۱\} \times K}\right) = \sigma(H)$$

و

$$\sigma(H \times K) \leq \sigma\left(\frac{H \times K}{H \times \{۱\}}\right) = \sigma(K). \qquad \square$$

لم ۳۳.۱.۹. فرض کنید H و K گروه باشند و $\gcd\{|H|, |K|\} = ۱$، آنگاه داریم $\sigma(H \times K) = \min\{\sigma(H), \sigma(K)\}$.

اثبات. چون $\gcd\{|H|, |K|\} = ۱$ و $G = H \times K$ دوری است اگر و تنها اگر H و K هر دو دوری باشند. پس اگر $H \times K$ دوری باشد، چیز i برای اثبات نیست. فرض کنید $\sigma(G) = n$. ابتدا ادعا می‌کنیم هر زیرگروه G به صورت $X \times Y$ است که در آن $X \leq H$ و $Y \leq K$. فرض کنید $T \leq G = H \times K$. قرار می‌دهیم $X = \{x \in H \mid (h, ۱) \in T\}$ و $Y = \{k \in K \mid (۱, k) \in T\}$. در این صورت $T = X \times Y$. زیرا اگر $(x, y) \in T$، که در آن $O(x) = n$ و $O(y) = m$، آنگاه چون $\gcd\{m, n\} = ۱$، اعداد صحیح r و s وجود دارند که $rn + sm = ۱$. بنابراین

$$(x, y) = (x, y)^{rn+sm} = (x, y)^{sm}(x, y)^{rn} = (x^{sm}, ۱)(۱, y^{rn}) \in X \times Y.$$

بنابراین هر زیرگروه ماکسیمال $X \times Y$ از $G = H \times K$ باید به صورت $H \times Y$، یا $X \times K$ باشد که در آن Y زیرگروه ماکسیمال K و X زیرگروه ماکسیمال H است. در نتیجه

$$G = \left(\bigcup_{i=۱}^{p} H \times Y_i\right) \cup \left(\bigcup_{j=۱}^{q} X_j \times K\right) = G_۱ \cup G_۲,$$

که در آن $p + q = n$، $p \geq ۰$، و $q \geq ۰$. نشان می‌دهیم $p = ۰$ یا $q = ۰$. اگر $q \neq ۰$، آنگاه $G_۱ \neq G$. پس عضو $(h_۱, k_۱) \in G$ وجود دارد که $(h_۱, k_۱) \notin G_۱$. بنابراین به ازای هر i، $(h_۱, k_۱) \notin H \times Y_i$. چون $h_۱ \in H$، به ازای هر i، $k_۱ \notin Y_i$. پس به ازای هر $h \in H$، $(h, k_۱) \notin G_۱$. زیرا در غیر این صورت به ازای یک r داریم $(h, k_۱) \in H \times Y_r$ یعنی $k_۱ \in Y_r$ که تناقض است. در نتیجه به

ازای هر $h \in H$، داریم $(h, k_۱) \in G_۲$. اما در این صورت به ازای هر $h \in H$ و هر $k \in K$ داریم $(h, k) \in G_۲$، یعنی $G = G_۲$ و $p = ۰$. در نتیجه

$$G = G_۲ = \bigcup_{j=۱}^{n} (X_j \times K) = \left(\bigcup_{j=۱}^{n} X_j \right) \times K.$$

بنابراین $H = \bigcup_{j=۱}^{n} X_j$ و $\sigma(H) \leq n = \sigma(G)$. به همین نحو اگر $p \neq ۰$ داریم $q = ۰$. پس $\sigma(K) \leq n = \sigma(G)$. □

نتیجه ۳۴.۱.۹. اگر G یک گروه غیر دوری پوچ‌توان باشد، آنگاه $\sigma(G) = p + ۱$، که در آن p کوچک‌ترین عدد اولی است که p-زیرگروه سیلوی G دوری نیست.

اثبات. داریم $G = P_۱ \times \cdots \times P_r$، که در آن $P_۱$، ...، P_r زیرگروه‌های سیلوی متمایز G هستند. با توجه به لم ۳۳.۱.۹، داریم $\sigma(G) = \min\{\sigma(P_۱), \ldots, \sigma(P_r)\}$ و حکم از قضیه‌ی ۲۹.۱.۹، به دست می‌آید. □

لم ۳۵.۱.۹. اگر H و K زیرگروه‌های نرمال G باشند، آنگاه

$$\frac{HK}{H \cap K} \cong \frac{H}{H \cap K} \times \frac{K}{H \cap K}.$$

اثبات. تابع $\varphi : HK \longrightarrow \dfrac{H}{H \cap K} \times \dfrac{K}{H \cap K}$ خوش‌تعریف، همریختی، پوشا، و با هسته‌ی $H \cap K$ است. بنابراین حکم از قضیه‌ی اول یکریختی نتیجه می‌شود. □

تعدادی مرجع برای مطالعه‌ی بیشتر

1. M. Bruckheimer, A. C. Bryan and A. Muir. *Groups which are the union of three subgroups,* Amer. Math. Monthly **77** (1970) 52-75.
2. J. H. E. Cohn. *On n-sum groups,* Math. Scand. **44** (1994) 44-58.
3. S. Haber and A. Rosentield. *Groups as unions of proper subgroups,* Amer. Math. Monthly **66** (1959) 491-494.
4. M. J. Tomkinson. *Groups covered by finitely many cosets or subgroups,* Comm. Algebra. **15** (1987) 845-859.
5. M. J. Tomkinson. *Groups as the union of proper subgroups,* Math. Scand. **81** (1997) 191-198.

۲.۹ تعداد مرکز سازها در یک گروه

اگر G یک گروه متناهی باشد، تعداد مرکزسازهای عناصر G چند تا است. G آبلی است اگر و تنها اگر برای هر $x \in G$، $G = C_G(x)$. پس G آبلی است اگر و تنها اگر تعداد مرکزسازهای عناصر G برابر ۱ باشد. تعریف می‌کنیم

$$\#\mathrm{cent}(G) = |\{C_G(x) \mid x \in G\}|.$$

پس G آبلی است اگر و تنها اگر $\#\mathrm{cent}(G) = ۱$. اگر $Y_۱ = C_G(۱) = G$، $Y_۲ = C_G(y_۲)$، ...، $Y_t = C_G(y_t)$، همه‌ی مرکزسازهای متمایز G باشند، آنگاه داریم $G = \bigcup_{i=۲}^{t} Y_i$. زیرا اگر $x \in G$ و $C_G(x) \neq G$، آنگاه $C_G(x) \in \{Y_۲, \ldots, Y_t\}$؛ از این‌رو به ازای یک i، $C_G(x) = C_G(y_i)$ و $x \in C_G(y_i)$. پس G اجتماع مرکزسازهای سره‌اش است. اما چیزی بیشتر می‌توان گفت:

قضیه ۱.۲.۹. فرض کنید $\{x_۱, \dots, x_n\}$ زیرمجموعه‌ی با اندازه‌ی ماکسیمم از عناصر دوبه‌دو تعویض ناشونده‌ی گروه G باشد. در این صورت

(الف) $G = \bigcup_{i=۱}^{n} C_G(x_i)$.

(ب) $Z(G) = \bigcap_{i=۱}^{n} C_G(x_i)$.

اثبات. (الف) اگر $x \in G - (\bigcup_{i=۱}^{n} C_G(x_i))$، آنگاه به ازای هر $۱ \leq i \leq n$، $x \notin C_G(x_i)$. از این‌رو $\{x_۱, \dots, x_n, x\}$ مجموعه‌ای از عناصر دو بدو تعویض ناشونده با اندازه‌ی $n+۱$ است، که این خلاف فرض است.

(ب) از یک طرف واضح است که $Z(G) \subseteq \bigcap_{i=۱}^{n} C_G(x_i)$. از طرف دیگر اگر عضوی مثل $a \in (\bigcap_{i=۱}^{n} C_G(x_i)) - Z(G)$ وجود داشته باشد، آنگاه عضو $b \in G$ وجود دارد که $ab \neq ba$. به ازای هر $۱ \leq i \leq n$ تعریف می‌کنیم

$$y_i = \begin{cases} x_i & \text{اگر } [x_i, b] \neq ۱ \\ ax_i & \text{اگر } [x_i, b] = ۱. \end{cases}$$

در این صورت $\{y_۱, \dots, y_n, b\}$ مجموعه‌ای از عناصر دو بدو تعویض ناشونده، با اندازه‌ی $n+۱$ است. این خلاف با ماکسیمال بودن n است. □

فرض کنید G یک گروه متناهی نابدیهی باشد. دیدیم G اجتماع مرکزسازهای سره‌ی خود است. اگر $\#\mathrm{cent}(G) = ۲$، آنگاه G اجتماع یک زیرگروه سره‌ی خودش است، که ممکن نیست. اگر $\#\mathrm{cent}(G) = ۳$، آنگاه G اجتماع دو زیرگروه سره‌اش است، که ممکن نیست، پس $\#\mathrm{cent}(G) \geq ۴$. آیا گروه G با $\#\mathrm{cent}(G) = ۴$ وجود دارد؟ بله، در واقع:

مثال ۲.۲.۹. نشان دهید $\#\mathrm{cent}(D_۸) = ۴$ و $\#\mathrm{cent}(Q_۸) = ۴$.

حل فرض کنید $G = D_۸$. داریم $Z(G) = \{۱, \rho^۲\}$ و

$$\begin{aligned} C_G(۱) &= C_G(\rho^۲) = G, \quad C_G(\rho^i) = \langle \rho \rangle, \quad i = ۱, ۲, ۳ \\ C_G(\varepsilon) &= C_G(\varepsilon\rho^۲) = \{۱, \varepsilon, \varepsilon\rho^۲, \rho^۳\} \\ C_G(\varepsilon\rho) &= C_G(\varepsilon\rho^۳) = \{۱, \varepsilon\rho, \varepsilon\rho^۳, \rho^۲\}. \end{aligned}$$

پس $\#\mathrm{cent}(G) = ۴$.

حال فرض کنید $G = Q_۸$. داریم $Z(G) = \{\pm ۱\}$ و

$$\begin{aligned} &C_G(۱) = C_G(-۱) = G, \quad C_G(\pm i) = \langle i \rangle, \\ &C_G(\pm j) = \langle j \rangle, \quad C_G(\pm k) = \langle k \rangle. \end{aligned}$$

بنابراین $\#\mathrm{cent}(G) = ۴$. □

قضیه ۳.۲.۹. فرض کنید G گروه باشد. در این صورت $\#\mathrm{cent}(G) = ۴$ اگر و تنها اگر $G/Z(G) \cong V$، که در آن V، ۴- گروه کلاین است.

اثبات. ($\Longleftarrow$) فرض کنید $X_۱ = C_G(x_۱)$، $X_۲ = C_G(x_۲)$ و $X_۳ = C_G(x_۳)$ مرکزسازهای سره‌ی G باشند. پس $G = X_۱ \cup X_۲ \cup X_۳$، این اجتماع نابدیهی است، زیرا G اجتماع دو زیرگروه سره‌ی خود نیست. بنابراین با توجه به قضیه‌ی ۷.۱.۹، $G/K \cong V$ که در آن $K = X_۱ \cap X_۲ \cap X_۳$. اما $Z(G) = C_G(x_۱) \cap C_G(x_۲) \cap C_G(x_۳) = K$، بنابراین $G/Z(G) \cong V$.

($\Longrightarrow$) فرض کنید $G/Z(G) \cong V$. قرار می‌دهیم $K = Z(G)$. طبق فرض عناصر a، b و c در G وجود دارند که $G/K = \{K, aK, bK, cK\} \cong V$. بنابراین $A = K \cup aK$، $B = K \cup bK$ و $C = K \cup cK$ زیرگروه‌های سره‌ای از G هستند. توجه کنید

$$G = K \cup aK \cup bK \cup cK.$$

عضو دلخواه $xk \in G$ را در نظر می‌گیریم، که در آن $x \in \{a, b, c\}$ و $k \in K$. فرض کنید X زیرگروه متناظر x باشد. در این صورت داریم

$$X \subseteq C_G(xk) \subset G,$$

و

$$۲ = |G : X| = |G : C_G(xk)||C_G(xk) : X|, \quad |G : C_G(xK)| \neq ۱.$$

بنابراین $C_G(xk) = X$. در نتیجه هر مرکزساز سره‌ی G، دقیقاً یکی از زیرگروه‌های A، B، C است. این یعنی $\#\text{cent}(G) = ۴$. □

مثال ۴.۲.۹. $\#\text{cent}(D_{۲m})$ را بیابید.

حل داریم

$$G = D_{۲m} = \{۱, \rho, \rho^۲, \ldots, \rho^{m-۱}, \varepsilon, \varepsilon\rho, \ldots, \varepsilon\rho^{m-۱}\}.$$

دو حالت در نظر می‌گیریم.

حالت اول. m فرد. در این حالت داریم $Z(D_{۲m}) = \{۱\}$ و

$$G = C_G(۱), \quad C_G(\rho^i) = \langle\rho\rangle, \quad C_G(\varepsilon\rho^i) = \{۱, \varepsilon\rho^i\}, \quad = ۰, ۱, \ldots, m-۱.$$

در نتیجه $\#\text{cent}(D_{۲m}) = m + ۲$.

حالت دوم. m زوج. در این حالت داریم $Z(D_{۲m}) = \left\{۱, \rho^{\frac{m}{۲}}\right\}$ و

$$G = C_G(۱) = C_G(\rho^{\frac{m}{۲}}), C_G(\rho^i) = \langle\rho\rangle,$$
$$C_G(\varepsilon\rho^i) = C_G(\varepsilon\rho^{i+\frac{m}{۲}}) = \{۱, \varepsilon\rho^i, \varepsilon\rho^{i+\frac{m}{۲}}, \rho^{\frac{m}{۲}}\}, i = ۰, ۱, \ldots, \frac{m}{۲} - ۱.$$

در نتیجه $\#\text{cent}(D_{۲m}) = \frac{m}{۲} + ۲$.

بنابراین

$$\#\text{cent}(D_{۲m}) = \begin{cases} m + ۲ & m \text{ فرد} \\ \frac{m}{۲} + ۲ & m \text{ زوج.} \end{cases}$$

پس در هر حالت $\#\text{cent}(D_{۲m})$ به دست آوردیم. □

نتیجه ۵.۲.۹. به ازای هر $n \geq ۴$، گروه G با $\#\text{cent}(G) = n$ وجود دارد.

اثبات. فرض کنید n فرد باشد، قرار می‌دهیم $m = n - ۲$. طبق مثال ۴.۲.۹،

$$\#\text{cent}(D_{۲m}) = m + ۲ = n.$$

حال فرض کنید n زوج باشد، قرار می‌دهیم $m = ۲(n - ۲)$. طبق مثال ۴.۲.۹،

$$\#\text{cent}(D_{۲m}) = \frac{m}{۲} + ۲ = n. \qquad \square$$

در قضیه‌ی ۳.۲.۹، دیدیم اگر $G/Z(G) \cong C_۲ \times C_۲$، آنگاه $\#\text{cent}(G) = ۴$. اکنون این قضیه را تعمیم می‌دهیم:

قضیه ۶.۲.۹. اگر $\frac{G}{Z(G)} \cong C_p \times C_p$، ($p$ عدد اول) آنگاه $\#\text{cent}(G) = p + ۲$.

اثبات. فرض کنید $K = Z(G)$. چون

$$\frac{G}{K} = \{x^i y^j K \mid ۰ \leq i, j \leq p-۱\} \cong C_p \times C_p,$$

فقط $p+۱$ زیرگروه متمایز غیربدیهی

$$\langle yK \rangle, \quad \langle x^i yK \rangle, \quad i = ۱, ۲, \ldots, p$$

را داریم. در نتیجه

$$H = \bigcup_{j=۰}^{p-۱} y^j K, \quad H_i = \bigcup_{j=۰}^{p-۱} (x^i y^j) K$$

زیرگروه‌هایی متمایز و غیربدیهی G هستند و

$$G = H \cup H_۱ \cup H_۲ \cup \cdots \cup H_p.$$

اگر $uk \in G$، که در آن $u \in \{x^i y^j | ۱ \leq i \leq p, ۱ \leq j \leq p-۱\}$، $k \in K$ و X زیرگروه متناظر u باشد، آنگاه داریم

$$X \subseteq C_G(uk) \subset G,$$

و

$$p = |G : X| = |G : C_G(uk)||C_G(uk) : X|, \quad |G : C_G(uk)| \neq ۱.$$

بنابراین $C_G(uk) = X$. از این‌رو هر مرکزساز سره‌ی G، دقیقاً یکی از زیرگروه‌های H، $H_۱$، ...، H_p است. این یعنی $\#\text{cent}(G) = p+۲$. □

تعداد مرکزسازهای گروه G را که $\frac{G}{Z(G)} \cong C_p \times C_p$ را تعیین کردیم. در اثبات قضیه‌ی ۶.۲.۹، تنها از این نکته استفاده شد که $C_p \times C_p$، $p+۱$ زیرگروه سره‌ی نابدیهی دارد و شاخص هر زیرگروه سره‌ی عدد اول p است. چون $D_{۲p}$، (p عدد اول فرد)، نیز $p+۱$ زیرگروه نابدیهی دارد و شاخص هر زیرگروه سره‌ی آن عدد اول است، داریم :

قضیه ۷.۲.۹. فرض کنید p عدد اول فرد باشد و $\frac{G}{Z(G)} \cong D_{۲p}$. در این صورت $\#\text{cent}(G) = p+۲$. □

اکنون حالتی را در نظر می‌گیریم که $\frac{G}{Z(G)}$ ناآبلی است. کوچک‌ترین گروه ناآبلی $S_۳$ است، پس حالت $\frac{G}{Z(G)} \cong S_۳$ را در نظر می‌گیریم. چون $S_۳$، ۴ زیرگروه نابدیهی دارد و شاخص هر زیرگروه سره‌ی آن عدد i اول است، خواهیم داشت

قضیه ۸.۲.۹. اگر $\frac{G}{Z(G)} \cong S_۳$، آنگاه $\#\text{cent}(G) = ۵$. □

دیدیم که اگر $\frac{G}{Z(G)} \cong C_۳ \times C_۳$ یا $\frac{G}{Z(G)} \cong S_۳$، آنگاه $\#\text{cent}(G) = ۵$. نشان می‌دهیم عکس مطلب نیز درست است.

قضیه ۹.۲.۹. اگر $\#\text{cent}(G) = ۵$ آنگاه $\frac{G}{Z(G)} \cong C_۳ \times C_۳$ یا $\frac{G}{Z(G)} \cong S_۳$.

اثبات. فرض کنید $\{x_۱, x_۲, \ldots x_r\}$ مجموعه‌ای با اندازه‌ی ماکسیمال از اعضای دو بدو تعویض ناشونده‌ی G باشد. قرار می‌دهیم $X_i = C_G(x_i)$ و $\beta_i = |G : X_i|$. طبق قضیه‌ی ۱.۲.۹، $G = \bigcup_{i=۱}^{r} X_i$ و $Z(G) = \bigcap_{i=۱}^{r} X_i$. فرض کنید X_iها طوری مرتب شده‌اند که $\beta_۱ \leq \beta_۲ \leq \cdots \leq \beta_r$. به وضوح $۴ \leq r \leq ۳$.

حالت اول. $r = ۳$. در این حالت $G = X_۱ \cup X_۲ \cup X_۳$ و G یک گروه ۳-مجموع است، و $\frac{G}{K} \cong C_۲ \times C_۲$ که در آن $K = X_۱ \cap X_۲ \cap X_۳ = Z(G)$. بنابراین طبق قضیه‌ی ۷.۲.۹، $\#\text{cent}(G) = ۴$ که تناقض است.

حالت دوم. $r = ۴$ در این حالت طبق قضیه‌ی ۲۳.۱.۹، داریم $\beta_۲ \leq ۴ - ۱ = ۳$. پس $\beta_۲ = ۲$ یا $\beta_۲ = ۳$ اگر $\beta_۲ = ۲$،

آنگاه $\beta_1 = ۲$. بنابراین X_1 و X_2 دو زیرگروه نرمال با شاخص ۲ در G هستند. پس طبق قضیه‌ی ۲۴.۱.۹، $\sigma(G) = ۳$. بنابراین از اجتماع $G = X_1 \cup X_2 \cup X_3 \cup X_4$ یکی از X_iها را می‌توان حذف کرد. اگر مثلاً $X_1 \subseteq X_2 \cup X_3 \cup X_4$. آنگاه به ازای یک i، $C_G(x_1) \subseteq C_G(x_i)$، یعنی x_1 و x_i تعویض می‌شوند، که تناقض است. پس $\beta_2 = ۳$. طبق قضیه‌ی ۲۲.۱.۹، $|G| \leq |X_2| + |X_3| + |X_4|$، که نتیجه می‌دهد

$$\frac{۲}{۳} \leq \frac{۱}{\beta_3} + \frac{۱}{\beta_4}$$

چون $\beta_4 \leq \beta_3 \leq \beta_2 \leq ۳$، تنها حالت ممکن وقتی است که $\beta_3 = \beta_4 = ۳$. بنابراین در قضیه‌ی ۲۲.۱.۹، تساوی برقرار است. در نتیجه $X_1 X_i = G$ و $X_i \cap X_j \subseteq X_1$. پس $Z(G) = X_1 \cap X_2$ چون $\beta_1 \leq \beta_2 = ۳$، دو حالت برای β_1 پیش می‌آید: $\beta_1 = ۲, ۳$. در هر حالت بنا به لم پوانکاره داریم

$$\left|\frac{G}{Z(G)}\right| = |G : X_1 \cap X_2| \leq |G : X_1||G : X_2| \leq ۹.$$

بنابراین $\frac{G}{Z(G)}$ گروهی غیر دوری کمتر یا مساوی ۹ است. از طرف دیگر $G = X_1 X_2$ و $|G : X_2| = ۳$. بنابراین $\left|\frac{G}{X_1 \cap X_2}\right| = ۳$. پس ۹ یا ۶ $= \left|\frac{G}{Z(G)}\right|$، که نتیجه می‌دهد $\frac{G}{Z(G)} \cong S_3$ یا $C_3 \times C_3$. □

تعدادی مرجع برای مطالعه‌ی بیشتر

1. A. R. Ashrafi. *On finite groups with a given number of centralizers,* Algebra Colloq. **7**:2 (2000) 139-146.
2. A. R. Ashrafi. *Counting the centralizers of some finte groups,* Korean J. Comput. & Appl. Math. **7**:1 (2000) 115-124.
3. S. M. Belcastro and G. J. Sherman. *On counting centralizers in finite groups,* Math. Mag. **67** (1994) 366-374.
4. S. Camp Mora. *Locally finite groups with two normalizers,* Comm. Algebra. **28**(11) (2000) 5475-5480.
5. M. D. Perez Ramos. *Groups with two normalizers,* Arch. Math. **50** (1988) 199-203.

۳.۹ مساله‌ای احتمالاتی در گروه‌ها

احتمال تعویض شدن دو عضو در یک گروه متناهی چقدر است؟ این مساله ممکن است به ذهن هر دانشجویی که جبر و احتمال را مطالعه می‌کند خطور کند. این مساله را می‌توانیم به صورت زیر حل کنیم. فرض کنید G گروه متناهی باشد. باید تعداد حالت ممکن را بر تعداد اعضای فضای نمونه تقسیم کنیم. حالت ممکن زوجهایی از عناصر G مثل x و y هستند که $xy = yx$. پس قرار می‌دهیم

$$C = \{(x, y) \in G \times G \mid xy = yx\}.$$

در نتیجه احتمال تعویض شدن دو عضو در G عبارت است از

$$\mathrm{pr}(G) = \frac{|C|}{|G|^2}.$$

اکنون می‌خواهیم $|C|$ را بیابیم. اگر $x \in G$ عضو دلخواهی باشد، آنگاه

$$(x, y) \in C \iff xy = yx \iff y \in C_G(x).$$

بنابراین

$$|C| = \sum_{x \in G} |C_G(x)|.$$

به ازای هر $g \in G$ داریم $C_G(gxg^{-1}) = gC_G(x)g^{-1}$. پس اگر $x, y \in G$ مزدوج باشند $C_G(x)$ و $C_G(y)$ نیز مزدوج‌اند. فرض کنید $\text{orb}(x_1)$، $\text{orb}(x_2)$، ...، $\text{orb}(x_k)$ مجموعه‌ی همه‌ی رده‌های مزدوجی متمایز G باشد. چون تعداد اعضای زیرگروه‌های مزدوج برابر است، داریم

$$\begin{aligned}
|C| &= \sum_{x \in G} |C_G(x)| \\
&= \sum_{i=1}^{k} \sum_{x \in \text{orb}(x_i)} |C_G(x)| \\
&= \sum_{i=1}^{k} \sum_{x \in \text{orb}(x_i)} |C_G(x_i)| \\
&= \sum_{i=1}^{k} \text{orb}(x_i)|C_G(x_i)| \\
&= \sum_{i=1}^{k} |G : C_G(x_i)||C_G(x_i)| \\
&= \sum_{i=1}^{k} |G| \\
&= k|G|.
\end{aligned}$$

پس

$$\text{pr}(G) = \frac{|C|}{|G|^2} = \frac{k}{|G|}.$$

بنابراین اگر G گروه متناهی باشد احتمال تعویض شدن دو عضو در G برابر است با

$$\text{pr}(G) = \frac{k(G)}{|G|},$$

که در آن $k(G)$ تعداد رده‌های مزدوجی G است.
واضح است که G آبلی است اگر و تنها اگر $\text{pr}(G) = 1$. اگر G گروه ناآبلی باشد $\text{pr}(G)$ تا چه اندازه بزرگ است. فرض کنید $\text{orb}(x_1)$، ...، $\text{orb}(x_t)$ همه‌ی رده‌های مزدوجی متمایز نابدیهی G باشند. معادله‌ی رده‌ای را می‌نویسیم

$$|G| = |Z(G)| + \sum_{i=1}^{t} |\text{orb}(x_i)|.$$

اگر p کوچک‌ترین عدد اولی باشد که $p \mid |G|$، آنگاه

$$|\text{orb}(x_i)| = |G : C_G(x_i)| \geq p, \quad i = 1, 2, \ldots, t.$$

بنابراین

$$|G| - |Z(G)| = \sum_{i=1}^{t} |\text{orb}(x_i)| \geq tp.$$

پس

$$k(G) = |Z(G)| + t \leq |Z(G)| + \frac{|G| - Z(G)|}{p}$$

یا

$$k(G) \leq \frac{|G|}{p} + |Z(G)|\frac{p-۱}{p}.$$

اما چون G ناآبلی است، $\frac{G}{Z(G)}$ دوری نیست. بنابراین داریم $|G/Z(G)| \geq p^۲$، یعنی $|Z(G)| \leq \frac{|G|}{p^۲}$. از این‌رو

$$k(G) \leq \frac{|G|}{p} + \frac{|G|}{p^۳}(p-۱) = |G|\frac{p^۲ + p - ۱}{p^۳}$$

و در نتیجه (چون $p \geq ۲$)

$$\mathrm{pr}(G) = \frac{k(G)}{|G|} \leq \frac{p^۲ + p - ۱}{p^۳} \leq \frac{۵}{۸} \qquad (۳)$$

بنابراین ثابت کرده‌ایم:

قضیه ۱.۳.۹. فرض کنید G گروه متناهی باشد. در این صورت G ناآبلی است اگر و تنها اگر $\mathrm{pr}(G) \leq \frac{۵}{۸}$. □

سوالی که مطرح می‌شود این است که آیا گروهی مثل G با $\mathrm{pr}(G) = \frac{۵}{۸}$ وجود دارد ؟ جواب مثبت است. در واقع

مثال ۲.۳.۹. داریم $\mathrm{pr}(Q_۸) = \mathrm{pr}(D_۸) = \frac{۵}{۸}$.

حل رده‌های مزدوجی متمایز $D_۸$ عبارت‌اند از

$$\mathrm{orb}(۱) = \{۱\},\ \ \mathrm{orb}(\rho) = \mathrm{orb}(\rho^۳) = \{\rho, \rho^۳\},\ \ \mathrm{orb}(\rho^۲) = \{\rho^۲\},$$
$$\mathrm{orb}(\varepsilon) = \mathrm{orb}(\varepsilon\rho^۲) = \{\varepsilon, \varepsilon\rho^۲\},\ \ \mathrm{orb}(\varepsilon\rho) = \mathrm{orb}(\varepsilon\rho^۳) = \{\varepsilon\rho, \varepsilon\rho^۳\}.$$

پس $k(D_۸) = ۵$ و $\mathrm{pr}(D_۸) = \frac{۵}{۸}$.
به همین نحو رده‌های مزدوجی متمایز $Q_۸$ عبارت‌اند از

$$\mathrm{orb}(۱) = \{۱\},\ \ \mathrm{orb}(-۱) = \{-۱\},\ \ \mathrm{orb}(i) = \{\pm i\},$$
$$\mathrm{orb}(j) = \{\pm j\},\ \ \mathrm{orb}(k) = \{\pm k\}.$$

بنابراین $k(Q_۸) = ۵$ و $\mathrm{pr}(Q_۸) = \frac{۵}{۸}$. □

قضیه ۳.۳.۹. اگر H و K گروه‌های متناهی باشند، آنگاه $\mathrm{pr}(H \times K) = \mathrm{pr}(H)\mathrm{pr}(K)$.

اثبات. فرض کنید $G = H \times K$ و $(h,k) \in G$؛ داریم

$$\begin{aligned}
\mathrm{orb}(h,k) &= \{(x,y)(h,k)(x,y)^{-۱} \mid (x,y) \in G\} \\
&= \{(h_۱k_۱, h_۲k_۲)(h,k)(h_۱k_۱, h_۲k_۲)^{-۱} \mid h_i \in H, k_i \in K\} \\
&= \{(h_۱hh_۱^{-۱}, k_۱kk_۱^{-۱}) \mid h_۱ \in H, k_۱ \in K\} \\
&= \mathrm{orb}(h) \times \mathrm{orb}(k),
\end{aligned}$$

که در سطر سوم از این که اعضای H و K با یکدیگر تعویض می‌شوند استفاده کرده‌ایم. بنابراین تابع یک‌به‌یک و پوشا از مجموعه‌ی مدارهای $H \times K$ حاصل‌ضرب دکارتی مجموعه‌ی مدارهای H و مجموعه‌ی مدارهای K داریم. از این‌رو $k(H \times K) = k(H)k(K)$ و در نتیجه $\mathrm{pr}(H \times K) = \mathrm{pr}(H)\mathrm{pr}(K)$. □

سوال دیگری که مطرح است این است که ساختار گروه G با $\mathrm{pr}(G) = \frac{۵}{۸}$ چیست؟ با توجه به روند بالا، تساوی در (۳) برقرار است اگر و تنها اگر $p = ۲$، $|G/Z(G)| = ۴$، $|\mathrm{orb}(x_i)| = ۲$، $i = ۱, ۲, \ldots, t$. فرض کنید $|Z(G)| = ۲^n m$، که در آن $n \geq ۰$، و $m \nmid ۲$. پس $|G| = ۲^{n+۲} m$. چون $Z(G)$ آبلی است، زیرگروهی مثل A از مرتبه‌ی m دارد. چون $A \leq Z(G)$، $A \trianglelefteq G$. فرض کنید $P \in \mathrm{Syl}_۲(G)$. چون $n_۲ = ۱ + ۲k$ و $n_۲ | m$ و $\gcd\{n, ۲\} = ۱$، $n_۲ = ۱$. از این‌رو $P \trianglelefteq G$. به علاوه چون $|A| = m$ و $|P| = ۲^{n+۲}$، $\gcd\{m, ۲\} = ۱$، $P \cap A = ۱$. در نتیجه $G = P \times A$ و

$$\frac{۵}{۸} = \mathrm{pr}(G) = \mathrm{pr}(P \times A) = \mathrm{pr}(P)\mathrm{pr}(A) = \mathrm{pr}(P).$$

به وضوح $|P/Z(P)| = ۴$. بنابراین ثابت کرده‌ایم:

قضیه ۴.۳.۹. اگر G گروه متناهی باشد، آنگاه $\mathrm{pr}(G) = \frac{۵}{۸}$ اگر و تنها اگر $G = P \times A$، که در آن P یک ۲-گروه، A گروه آبلی است و $|A| \nmid ۲$ و $|P/Z(P)| = ۴$. □

اگر G گروه باشد، $x, y \in G$، آنگاه $xy = yx$ اگر و تنها اگر $\langle x, y\rangle$ آبلی باشد. بنابراین

$$\mathrm{pr}(G) = \frac{|(x, y) \in G \times G \mid \quad \text{آبلی} \quad \langle x, y\rangle\}|}{|G|^۲}.$$

این مطلب را می‌توان برای هر خاصیت دیگر تعمیم داد. مثلاً تعریف می‌کنیم

$$\mathrm{prcyc}(G) = \frac{|(x, y) \in G \times G \mid \quad \text{دوری} \quad \langle x, y\rangle\}|}{|G|^۲}.$$

بنابراین $\mathrm{prcyc}(G)$ احتمال دوری بودن گروه تولید شده توسط دو عضو G را مشخص می‌کند. اگر $\langle x, y\rangle$ دوری باشد، آنگاه $\langle x, y\rangle$ آبلی است، بنا به قضیه‌ی ۱.۳.۹،

$$\mathrm{prcyc}(G) \leq \mathrm{pr}(G) \leq \frac{۵}{۸}.$$

از طرف دیگر همان طور که انتظار می‌رود داریم :

قضیه ۵.۳.۹. $\mathrm{prcyc}(G) = ۱$ اگر و تنها اگر G دوری باشد.

اثبات. ابتدا توجه کنید که $\mathrm{prcyc}(G) = ۱$ اگر و تنها اگر هر زیرگروه دو مولدی G دوری باشد. اگر G دوری باشد هر زیرگروه G نیز دوری است، پس $\mathrm{prcyc}(G) = ۱$. برعکس اگر $\mathrm{prcyc}(G) = ۱$، آنگاه به وضوح G آبلی است. به استقرا روی $|G|$ ثابت می‌کنیم G دوری است. حالت $|G| = ۱$ بدیهی است. حال اگر G هیچ زیرگروه نابدیهی نداشته باشد، آنگاه G دوری است. پس فرض کنید $۱ < H < G$. چون G آبلی است، $H \trianglelefteq G$. گروه‌های H و $\frac{G}{H}$ را در نظر می‌گیریم. داریم $|H| < |G|$ و $\frac{|G|}{|H|} < |G|$ و به وضوح $\mathrm{prcyc}(H) = ۱$ و $\mathrm{prcyc}\left(\frac{G}{H}\right) = ۱$. پس ، بنا به فرض استقرا، H و $\frac{G}{H}$ دوری هستند : $H = \langle h\rangle$ و $\frac{G}{H} = \langle gH\rangle$. بنابراین $G = \langle g, h\rangle$. اما طبق فرض هر زیرگروه دو مولدی G دوری است. بنابراین G دوری است. □

قضیه ۶.۳.۹. اگر H و K دو گروه دلخواه باشند، آنگاه

$$\mathrm{prcyc}(H \times K) \leq \mathrm{prcyc}(H)\mathrm{prcyc}(K).$$

اثبات. اگر $\langle (x_۱,y_۱),(x_۲,y_۲)\rangle$ دوری باشد، آنگاه $(x,y)\in H\times K$ و اعداد صحیح نامنفی $n_۱$ و $n_۲$ وجود دارند که $(x,y)^{n_i}=(x_i,y_i)$. پس $x^{n_i}=x_i$ و $y^{n_i}=y_i$ و

$$\begin{aligned}\langle x_۱,x_۲\rangle &= \langle x^{n_۱},x^{n_۲}\rangle=\langle x^m\rangle\\ \langle y_۱,y_۲\rangle &= \langle y^{n_۱},y^{n_۲}\rangle=\langle y^m\rangle\end{aligned}$$

که در آن $m=\gcd\{n_۱,n_۲\}$. بنابراین حکم ثابت است. □

در حالتی که G ناآبلی باشد، دیدیم $\operatorname{prcyc}(G)\le \operatorname{pr}(G)\le \frac{۵}{۸}$. می‌خواهیم ثابت کنیم به ازای هر گروه متناهی G، $\operatorname{prcyc}(G)\le \frac{۵}{۸}$. باید حالتی که G آبلی باشد را در نظر بگیریم. ابتدا توجه کنید چون G آبلی است حاصل‌ضرب مستقیم زیرگروه‌های سیلوی خودش است، بنا به قضیه‌ی ۶.۳.۹، داریم

$$\operatorname{prcyc}(G)\le \prod_{p||G|}\operatorname{prcyc}(H_p)$$

که در آن p عدد اول و H_p، p- زیرگروه سیلوی G است. بنابراین اگر حداقل به ازای یک p، $\operatorname{prcyc}(H_p)\le \frac{۵}{۸}$، حکم ثابت می‌شود. چون G غیر دوری است، حداقل یک عدد اول مثل q وجود دارد که H_q دوری نیست. بنابراین H_q به صورت $C_{q^k}\times C_{q^m}\times A$ است، که در آن $۱\le k\le m$.

لم ۷.۳.۹. $\operatorname{prcyc}\left(C_{q^k}\times C_{q^k}\right)\le \frac{۵}{۸}$، ($q$ عدد اول ، $k\ge ۱$).

اثبات. فرض کنید $(a,b),(c,d)\in C_{q^k}\times C_{q^k}$ و $\langle (a,b),(c,d)\rangle$ دوری باشد. دو حالت پیش می‌آید.
حالت اول. مرتبه‌ی (a,b) برابر q^k باشد. چون q^k بیشترین مرتبه‌ی ممکن یک عضو در $C_{q^k}\times C_{q^k}$ است، نتیجه می‌گیریم که $(c,d)\in\langle (a,b)\rangle$. بنابراین تعداد $q^{۲k}-q^{۲k-۲}$ انتخاب برای (a,b) و تعداد q^k انتخاب برای (c,d) داریم ، یعنی تعداد $(q^{۲k}-q^{۲k-۲})q^k$ انتخاب برای (a,b) و (c,d) داریم.
حالت دوم. مرتبه‌ی (a,b) کوچکتر از q^k باشد. در این حالت تعداد $q^{۲k-۲}$ انتخاب برای (a,b) و تعداد حداکثر $q^{۲k}$ انتخاب برای (c,d) داریم. بنابراین حداکثر تعداد $q^{۲k-۲}q^{۲k}$ انتخاب برای (a,b) و (c,d) داریم. در نتیجه

$$\begin{aligned}\operatorname{prcyc}(C_{q^k}\times C_{q^k}) &\le \frac{(q^{۲k}-q^{۲k-۲})q^k+q^{۲k-۲}q^{۲k}}{q^{۴k}}\\ &= \frac{۱}{q^۲}+\left(۱-\frac{۱}{q^۲}\right)\left(\frac{۱}{q^k}\right)\\ &\le \frac{۱}{۴}+\frac{۳}{۴}\cdot\frac{۱}{۲}\\ &= \frac{۵}{۸}.\end{aligned}$$

□

آیا گروه G با $\operatorname{prcyc}(G)=\frac{۵}{۸}$ وجود دارد ؟ جواب مثبت است: به سادگی می‌توان دید $\operatorname{prcyc}(C_۲\times C_۲)=\frac{۵}{۸}$.

لم ۸.۳.۹. اگر $\operatorname{prcyc}\left(C_{q^k}\times C_{q^m}\right)\le\frac{۵}{۸}$، آنگاه $\operatorname{prcyc}\left(C_{q^k}\times C_{q^{m+۱}}\right)\le\frac{۵}{۸}$.

اثبات. فرض کنید $(a,b),(c,d)\in C_{q^k}\times C_{q^{m+۱}}$ و $\langle (a,b),(c,d)\rangle$ دوری باشد. مشابه لم ۷.۳.۹، برای شمارش تعداد چنین زیرگروه‌هایی سه حالت را در نظر می‌گیریم.
حالت اول. مرتبه‌ی (c,d) و (a,b) هر دو کمتر یا مساوی q^m باشد. مجموعه‌ی همه‌ی چنین اعضایی را به صورت زوج مرتب در نظر می‌گیریم

$$C=\{((a,b),(c,d))\mid O(a,b),O(c,d)\le m,\ \text{دوری}\ \langle (a,b),(c,d)\rangle\}$$

قرار می‌دهیم

$$H = \bigcup C.$$

اکنون فرض کنید B تصویر H در $C_{q^{m+1}}$ باشد، یعنی $H \subseteq \langle A\rangle \times \langle B\rangle$. بنابراین $\langle B\rangle$ زیرگروه دوری $C_{q^{m+1}}$ است و عضوی از مرتبه‌ی q^{m+1} ندارد. در نتیجه $\langle B\rangle \cong C_{q^j}$، $j \leq m$، که نتیجه می‌دهد $\langle A\rangle \times \langle B\rangle$ با زیرگروهی از $C_{q^k} \times C_{q^m}$ یکریخت است. پس $|C| \leq \frac{5}{8} q^{2(k+m)}$، بنا به فرض.

حالت دوم. مرتبه‌ی (a,b) برابر q^{m+1} باشد. در این حالت چون $(c,d) \in \langle (a,b)\rangle$، تعداد $q^{k+m+1} - q^{k+m}$ انتخاب برای (a,b) و a^{m+1} انتخاب برای (c,d) داریم. در نتیجه تعداد $q^{k+2m+2} - q^{k+2m+1}$ انتخاب برای $((a,b),(c,d))$ داریم.

حالت سوم. مرتبه‌ی (a,b) کمتر یا مساوی q^m و مرتبه‌ی (c,d) برابر q^{m+1} باشد. در این حالت تعداد $q^{k+m+1} - q^{k+m}$ انتخاب برای (c,d) و چون مرتبه‌ی (a,b) کمتر از q^m است و $(a,b) \in \langle (c,d)\rangle$، تعداد q^m انتخاب برای (a,b) داریم. پس تعداد $q^{k+2m+1} - q^{k+2m}$ انتخاب برای $((a,b),(c,d))$ داریم. اکنون داریم

$$\begin{aligned}
\mathrm{prcyc}(C_{q^k} \times C_{q^{m+1}}) &\leq \frac{\frac{5}{8} q^{2(k+m)} + q^{k+2m+2} - q^{k+2m}}{q^{2(k+m+1)}} \\
&= \frac{5}{8}\frac{1}{q^2} + \frac{1}{q^k} - \frac{1}{q^{k+2}} \\
&\leq \frac{5}{8}\frac{1}{2^2} + \frac{1}{2^k} - \frac{1}{2^{k+2}} \\
&\leq \frac{5}{8}\frac{1}{2^2} + \frac{1}{2} - \frac{1}{2^3} \\
&= \frac{17}{32} \leq \frac{5}{8}.
\end{aligned}$$

که حکم را ثابت می‌کند. □

بنابراین $\mathrm{prcyc}(H_q) \leq \frac{5}{8}$ و ثابت کرده‌ایم

قضیه ۹.۳.۹. اگر G گروه ناآبلی باشد، آنگاه $\mathrm{prcyc}(G) \leq \frac{5}{8}$. □

تعدادی مرجع برای مطالعه‌ی بیشتر

1. W. H. Gustafson. *What is the probability that two group elements commute?,* Amer. Math. Monthly **80** (1973) 1031-1037.
2. J. E. Fulman, M. D. Galloy, G. J. Sherman and J. M. Vanderkam. *Counting nilpotent pairs in finite groups,* ARS Cominatoria **54** (2000) 161-178.
3. D. M. Patrick, G. J. Sherman, C. A. Sugar and E. K. Wepsic. *What is the probability of generating a cyclic subgroup,* ISM Bull. **31** (1993) 22-27.
4. G. J. Sherman. *Wath is the probabilty an automorphism fixes a group element,* Amer. Math. Monthly **82** (1975) 261-264.
5. G. J. Sherman. *A probabilistic estimate of invariance for groups,* Amer. Math. Monthly **85** (1978) 361-363.
6. G. J. Sherman. *Trying to do group theory with undergraduates and computers,* J. Symbolic Comput. **23** (1997) 577-587.
7. W. Shi. *Quotient of the group order and the number of conjugacy classes,* Southeast Asian Bull. Math. **22** (1998) 301-305.

۴.۹ مساله‌ی n- جایگشتپذیری

یک روند تعمیم مفهوم تعویض شدن دو عضو، مفهوم n- جایگشتپذیری است. فرض کنید G گروه باشد، n- تایی $(x_۱, \dots, x_n)$ از عناصر G را n- جایگشتپذیر می‌نامیم هرگاه جایگشت غیرهمانی $\sigma \in S_n$ وجود داشته باشد که

$$x_۱x_۲\cdots x_n = x_{\sigma(۱)}x_{\sigma(۲)}\cdots x_{\sigma(n)}.$$

گروه G را n- جایگشتپذیر گوییم هرگاه هر n تایی از عناصر G، n- جایگشتپذیر باشد، بنابراین گروه G، ۲- جایگشتپذیر است اگر و تنها اگر G آبلی باشد.

مثال ۱.۴.۹. اگر G گروهی باشد که $|G'| = ۲$، آنگاه G، ۳- جایگشتپذیر است.

حل فرض کنید $x, y, t \in G$. اگر $[x, y] = ۱$، آنگاه $xyt = yxt$ و حکم ثابت است. پس فرض کنید $[x, y] \neq ۱$. چون $|G'| = ۲$، $G' = \{۱, [x, y]\}$. اکنون چون G/G' آبلی است،

$$xytG' = tyxG'.$$

پس $a \in G'$ وجود دارد که $xyt = tyxa$. اگر $a = ۱$ حکم ثابت است و اگر $a \neq ۱$، آنگاه $a = [x, y]$. پس

$$xyt = tyxa = tyxx^{-۱}y^{-۱}xy = txy,$$

یعنی G، ۳- جایگشتپذیر است. □

مثال ۲.۴.۹. گروه کواترنیونی $Q_۸$ گروهی ۳- جایگشتپذیر است، زیرا $Q_۸' = \{\pm ۱\}$. □

قضیه ۳.۴.۹. فرض کنید H زیرگروهی از گروه G باشد. اگر H، r- جایگشتپذیر باشد و $|G : H| = m$، آنگاه G، rm جایگشتپذیر است.

اثبات. قرار می‌دهیم $n = rm$. n عضو دلخواه $x_۱$، $x_۲$، ...، x_n، از G را در نظر می‌گیریم. $n + ۱ = rm + ۱$ هم‌مجموعه‌های

$$H,\ x_۱H,\ x_۱x_۲H,\ x_۱x_۲x_۳H,\ \dots,\ x_۱x_۲\cdots x_nH$$

را در نظر می‌گیریم. چون $|G : H| = m$ و $n = rm$، بنا به اصل لانه کبوتری $r + ۱$ عدد صحیح $i_۱$، $i_۲$، ...، $i_{r+۱}$ وجود دارند که $۰ \leq i_۱ \leq i_۲ \leq \cdots \leq i_{r+۱} \leq n$ و

$$x_۱x_۲\cdots x_{i_۱}H = x_۱x_۲\cdots x_{i_۲}H = \cdots = x_۱x_۲\cdots x_{i_{r+۱}}H$$

(اگر $i_۱ = ۰$، اولین هم‌مجموعه برابر H است). بنابراین r عضو

$$a_j = x_{i_j+۱}x_{i_j+۲}, \dots, x_{i_j+۱}, \quad j = ۱, ۲, \dots, r$$

عضو H، r- جایگشتپذیر است جایگشت غیرهمانی $\sigma \in S_n$ وجود دارد که

$$a_۱a_۲\cdots a_r = a_{\sigma(۱)}a_{\sigma(۲)}\cdots a_{\sigma(r)},$$

در نتیجه

$$\begin{aligned} x_۱x_۲\cdots x_n &= x_۱x_۲\cdots x_{i_۱}a_۱\cdots a_r x_{i_{r+۱}+۱}\cdots x_n \\ &= x_۱x_۲\cdots x_{i_۱}a_{\sigma(۱)}\cdots a_{\sigma(r)}x_{i_{r+۱}+۱}\cdots x_n, \end{aligned}$$

که نشان می‌دهد G، n جایگشتپذیر است. □

مثال ۱.۴.۹، را می‌توان تعمیم داد:

قضیه ۴.۴.۹. فرض کنید G گروه باشد. اگر G' متناهی با مرتبه‌ی m باشد، آنگاه G، $(m+۱)$- جایگشتپذیر است.

اثبات. قرار می‌دهیم $n = m + ۱$ و n عضو دلخواه $x_۱$، $x_۲$، ...، x_n از G را در نظر می‌گیریم. چون G/G' آبلی است به ازای هر $۲ \leq j \leq n$،

$$x_۱x_۲\cdots x_nG' = (x_nx_{n-۱}\cdots x_{j+۱}x_j)(x_۱x_۲\cdots x_{j-۱})G'.$$

بنابراین به ازای هر $۲ \leq j \leq n$، عضو $d_j \in G'$ وجود دارد که

$$x_۱x_۲\cdots x_n = (x_nx_{n-۱}\cdots x_{j+۱}x_j)(x_۱x_۲\cdots x_{j-۱})d_j.$$

اگر به ازای یک j، داشته باشیم $d_j = ۱$ حکم ثابت است. بنابراین فرض کنید به ازای هر j، $d_j \neq ۱$. چون $|G' - \{۱\}| = m - ۱ = n - ۲$، بنا به اصل لانه کبوتری اعداد صحیح r و s وجود دارند که $۲ \leq r \leq s \leq n$ و $d_r = d_s$. بنابراین

$$\begin{aligned} x_۱x_۲\cdots x_n &= (x_nx_{n-۱}\cdots x_{r+۱}x_r)(x_۱x_۲\cdots x_{r-۱})d \\ &= (x_nx_{n-۱}\cdots x_{s+۱}x_s)(x_۱x_۲\cdots x_{s-۱})d. \end{aligned}$$

از این‌رو

$$(x_nx_{n-۱}\cdots x_{r+۱}x_r)(x_۱x_۲\cdots x_{r-۱}) = (x_nx_{n-۱}\cdots x_{s+۱}x_s)(x_۱x_۲\cdots x_{s-۱})$$

که نتیجه می‌دهد

$$x_۱x_۲\cdots x_{r-۱} = (x_{r-۱}x_r\cdots x_s)(x_۱x_۲\cdots x_{s-۱}).$$

بنابراین با ضرب $x_rx_{r+۱}\cdots x_n$ از سمت راست در تساوی اخیر نتیجه حاصل می‌شود. □

اگر G گروهی باشد که $|G'| \leq ۲$، آنگاه بنا به قضیه ۴.۴.۹، G، ۳- جایگشتپذیر است. می‌خواهیم نشان دهیم عکس مطلب نیز برقرار است. به قدری مقدمه نیاز داریم.

لم ۵.۴.۹. فرض کنید G گروه ۳- جایگشتپذیر باشد. در این صورت به ازای هر $x \in G$ داریم $x^۲ \in Z(G)$.

اثبات. عضو دلخواه $y \in G$ را در نظر می‌گیریم و ثابت می‌کنیم $x^۲y = yx^۲$. قرار می‌دهیم $x_۱ = x$، $x_۲ = y$ و $x_۳ = x^۲$. چون G، ۳- جایگشتپذیر است، برای $x_۱x_۲x_۳ = xyx^۲$ پنج حالت پیش می‌آید:

$$\begin{aligned} x_۱x_۲x_۳ = x_۱x_۳x_۲ &\implies xyx^۲ = xx^۲y \Longrightarrow yx^۲ = x^۲y \\ x_۱x_۲x_۳ = x_۳x_۱x_۲ &\implies xyx^۲ = x^۲xy \Longrightarrow yx^۲ = x^۲y \\ x_۱x_۲x_۳ = x_۳x_۲x_۱ &\implies xyx^۲ = x^۲yx \Longrightarrow yx = xy \\ x_۱x_۲x_۳ = x_۲x_۱x_۳ &\implies xyx^۲ = yxx^۲ \Longrightarrow xy = yx \\ x_۱x_۲x_۳ = x_۲x_۳x_۲ &\implies xyx^۲ = yx^۲x \Longrightarrow xy = yx \end{aligned}$$

که در هر پنج حالت نتیجه‌ی مورد نظر حاصل می‌شود. □

لم ۶.۴.۹. اگر G گروهی باشد که به ازای هر $x \in G$، $x^۲ \in Z(G)$، آنگاه $G' \leq Z(G)$ و به ازای هر $x, y \in G$، $[x, y]^۲ = ۱$.

اثبات. طبق فرض مرتبه‌ی هر عضو غیرهمانی $G/Z(G)$ برابر ۲ است. بنابراین $G/Z(G)$ آبلی است. در نتیجه $G' \leq Z(G)$. اکنون چون $x^۲ \in Z(G)$ و $[x, y] \in Z(G)$، داریم

$$۱ = [x^۲, y] = x^{-۱}[x, y]x[x, y] = [x, y][x, y] = [x, y]^۲$$

و حکم ثابت است. □

لم ۷.۴.۹. قضیه‌های زیر برای گروه G معادل‌اند
(الف) $|G'| \leq ۲$
(ب) به ازای هر $x \in G - Z(G)$، $|G : C_G(x)| = ۲$.

اثبات. (الف) $\Longleftarrow$ (ب) چون $x \notin Z(G)$، $|G : C_G(x)| > ۱$. از طرف دیگر اگر $\text{orb}(x)$ رده‌ی مزدوجی شامل x باشد، آنگاه $|\text{orb}(x)| = |G : C_G(x)|$. داریم $x^{-۱}\text{orb}(x) \leq G'$، که نتیجه می‌دهد

$$|G : C_G(x)| = |\text{orb}(x)| = |x^{-۱}\text{orb}(x)| \leq |G'| \leq ۲$$

بنابراین $|G : C_G(x)| = ۲$.
(ب) $\Longleftarrow$ (الف) فرض کنید $[x_۱, y_۱] \neq ۱$ و $[x_۲, y_۲] \neq ۱$. که در آن $x_i, y_i \in G$. عضو دلخواه $t \in C_G$ را طوری می‌گیریم که $t \notin C_G(x_i)$، $i = ۱, ۲$ را در نظر بگیرید. چون شاخص $C_G(x_i)$ در G برابر ۲ است و $y_i \notin C_G(x_i)$ داریم $y_i C_G(x_i) = t^{-۱}C_G(x_i)$ و $ty_i \in C_G(x_i)$. از طرف دیگر چون ، طبق فرض، $|G : C_G(y_i)| = ۲$، پس $C_G(y_i) \trianglelefteq G$ و $\frac{G}{C_G(y_i)}$ آبلی است. از این‌رو

$$\begin{aligned} ۱ = [ty_i, x_i] &= y_i^{-۱}[t, x_i]y_i[y_i, x_i] \\ &= [t, x_i][y_i, x_i] \quad (G' \leq C_G(x_i) \text{ چون}) \\ &= x_۱[t, x_۱]x_۱^{-۱}[x_۲, t] \\ &= [t, x_۱][t, x_۲]^{-۱} \\ &= [x_۱, y_۱][x_۲, y_۲]^{-۱}, \end{aligned}$$

و $[x_۱, y_۱] = [x_۲, y_۲]$. بنابراین $|G'| \leq ۲$. □

قضیه ۸.۴.۹. اگر G گروه ناآبلی ۳- جایگشتپذیر باشد، آنگاه $|G'| = ۲$.

اثبات. ابتدا توجه کنید بنا به لم‌های ۵.۴.۹ و ۶.۴.۹، داریم $G' \leq Z(G)$. پس برای هر $g \in G$، $G' \leq Z(G) \leq C_G(g)$. از این‌رو $C_G(g) \trianglelefteq G$. حال فرض کنید حکم قضیه درست نباشد. بنا به لم ۷.۴.۹، عضو $y \in G - Z(G)$ وجود دارد که $|G : C_G(y)| \neq ۲$. به ازای هر $x \in G - C_G(y)$، بنا به لم ۵.۴.۹، داریم $x^۲ \in Z(G)$. بنابراین

$$\frac{C_G(y)\langle x\rangle}{C_G(y)} \cong \frac{\langle x\rangle}{C_G(y) \cap \langle x\rangle} = \frac{\langle x\rangle}{\langle x^۲\rangle} \cong C_۲,$$

یعنی شاخص $C_G(y)$ در $C_G(y)\langle x\rangle$ برابر ۲ است. از این‌رو $C_G(y)\langle x\rangle \neq G$. دو حالت وجود دارد.
حالت اول. عضو $x \in G - C_G(y)$ وجود دارد که $C_G(x) \nsubseteq C_G(y)\langle x\rangle$. در این حالت عضو $t \in C_G(x) - C_G(y)\langle x\rangle$ را اختیار می‌کنیم. بنابراین $[xy, t] \neq ۱$ و $[xt, y] \neq ۱$. چون G، ۳- جایگشتپذیر است پنج حالت برای $x_۱ = x$، $x_۲ = y$ و $x_۳ = t$ پیش می‌آید.
(الف) $xyt = yxt$ (ب) $xyt = xty$ (ج) $xyt = txy$
(د) $xyt = ytx$ (H) $xyt = tyx$
در حالت (الف) داریم $xy = yx$. در حالت (ب) داریم $yt = ty$ و در حالت (ج) چون $t \in C_G(x)$ داریم $[xy, t] = ۱$. در حالت (د) چون $t \in C_G(x)$ داریم ، $xy = yx$. پس حالت‌های (الف) - (د) رخ نمی‌دهند. اگر (هـ) برقرار باشد، $xyt = tyx$، داریم $x^۲yt = xtyx$. چون $x^۲ \in Z(G)$ و $t \in C_G(x)$ داریم $ytx^۲ = txyx$ یا $ytx = txy$، یعنی $[xt, y] = ۱$ که امکان ندارد.
حالت دوم. به ازای هر $y \in G$، که $|G : C_G(y)| > ۲$ و هر $x \in G - C_G(y)$، داشته باشیم $C_G(x) < C_G(y)\langle x\rangle$. در این حالت عضو $t \in G - C_G(y)\langle x\rangle$ را اختیار می‌کنیم. اگر $[xy, t] = ۱$، طبق فرض این حالت داریم $xy \in C_G(t) < \langle C_G(y), t\rangle$ و $x \in \langle C_G(y), t\rangle$؛ پس $c \in C_G(y)$ و $m \in \mathbb{Z}$ وجود دارند که $x = ct^m$. از این‌رو $[x, y] = [ct^m, y] = [t, y]^m$ (توجه کنید $[t, y] \in G' \leq Z(G)$). چون $[x, y] \neq ۱$، با استفاده از لم ۷.۴.۹، داریم $[x, y] = [t, y]$. بنابراین $tx^{-۱} \in C_G(y)$ که نتیجه می‌دهد

$t \in C_G(y) \langle x \rangle$، این تناقض است. پس $[xy,t] \neq ۱$.
حال چون G، ۳- جایگشتپذیر است برای $x_۱ = x$، $y_۲ = y$ و $x_۳ = t$ پنج حالت (الف) - (هـ) مثل بالا پیش می‌آید. در حالت (الف) داریم $xy = yx$، در حالت (ب) داریم $yt = ty$. پس (الف) و (ب) امکان ندارند. در حالت (ج) داریم $[xy,t] = ۱$ که امکان ندارد. در حالت (د) داریم $yt \in C_G(x) < \langle C_G(y), x \rangle$ که نتیجه می‌دهد $t \in C_G(y) \langle x \rangle$، و این امکان ندارد. در نهایت فرض کنید حالت (هـ) برقرار باشد. با ضرب طرفین رابطه در xt داریم ، $xtxyt = xttyx$. چون $t^۲ \in Z(G)$، داریم $xtxyt = xyxt^۲$، که نتیجه می‌دهد $[xy,xt] = ۱$، یعنی $xy \in C_G(xt)$. از $C_G(x) < \langle C_G(y), x \rangle$ نتیجه می‌شود $|G : C_G(x)| \neq ۲$؛ و چون $xt \notin C_G(x)$، بنا به فرض این حالت داریم

$$xy \in C_G(xt) < C_G(x) \langle xt \rangle = C_G(x) \langle t \rangle .$$

بنابراین $y \in \langle C_G(x), t \rangle$. پس $c \in C_G(x)$ و $m \in \mathbb{Z}$ وجود دارند که $y = ct^m$. از این‌رو $[x,y] = [x,ct^m] = [x,t]^m$ (توجه کنید $[x,t] \in G' \leq Z(G)$). چون $[x,y] \neq ۱$، با استفاده از لم ۷.۴.۹، داریم $[x,y] = [x,t]$. بنابراین

$$ty^{-۱} \in C_G(x) < \langle C_G(y), x \rangle .$$

در نتیجه $t \in \langle C_G(y), x \rangle$ که تناقض است. □

حال فرض کنید G گروه متناهی باشد. تاکنون ثابت کرده‌ایم موارد زیر معادل‌اند
(۱) G، ۳- جایگشتپذیر است.
(۲) $|G'| \leq ۲$.
(۳) به ازای هر $x \in G$، یا $C_G(x) = G$ یا $|C_G(x)| = \frac{|G|}{۲}$.
(۴) اندازه‌ی هر رده‌ی مزدوجی برابر ۱ یا ۲ است.
بنابراین این شرایط رابطه‌ای بین ۳- جایگشتپذیری و احتمال تعویض شدن دو عضو را برقرار می‌کند. می‌خواهیم این ارتباط را فرمول‌بندی کنیم. توجه کنید چون اندازه‌ی هر رده‌ی مزدوجی گروه ۳- جایگشتپذیر G برابر ۱ یا ۲ است بنا به معادله‌ی رده‌ای داریم $|G| = t + ۲r$، که در آن $t = |Z(G)|$ و r تعداد رده‌های مزدوجی متمایز نابدیهی است. بنابراین

$$\frac{|G|}{k(G)} = \frac{t+۲r}{t+r} = ۱ + \frac{r}{t+r} < ۲$$

در نتیجه اگر G گروه ۳- جایگشتپذیر باشد، آنگاه

$$\mathrm{pr}(G) = \frac{k(G)}{|G|} > \frac{۱}{۲}$$

سوالی که مطرح می‌شود این است که آیا عکس مطلب فوق درست است؟ می‌خواهیم به این سوال پاسخ مثبت بدهیم. ابتدا به قدری مقدمه نیاز داریم.

لم ۹.۴.۹. فرض کنید $x,y \in G$ و $|G : C_G(x)| = ۲$ و $C_G(y) \cap (G - C_G(x)) = \emptyset$، آنگاه داریم $|G : C_G(xy)| \geq |G : C_G(y)|$.

اثبات. فرض کنید $\mathrm{orb}(y) = \{g_۱ y g_۱^{-۱}, g_۲ y g_۲^{-۱}, \ldots, g_n y g_n^{-۱}\}$
رده‌ی مزدوجی شامل y باشد. ادعا می‌کنیم g_iها را می‌توان از $C_G(x)$ انتخاب کرد. اگر این ادعا درست نباشد، داریم $C_G(y)g_i \subseteq G - C_G(x)$. بنابراین، چون $|G : C_G(x)| = ۲$، داریم $G - C_G(x) = C(x)g_i$. در نتیجه $C_G(y) \subseteq C_G(x)$، که متناقض با فرض است. پس می‌توانیم فرض کنیم برای هر i، $g_i \in C_G(x)$. از این‌رو $\varphi : \mathrm{orb}(y) \longrightarrow \mathrm{orb}(xy)$ با ضابطه‌ی $\varphi(g_i y g_i^{-۱}) = x(g_i y g_i^{-۱})$، خوش تعریف و یک‌به‌یک است. این حکم را ثابت می‌کند. □

لم ۱۰.۴.۹. اگر G، ۳- جایگشتپذیر نباشد، آنگاه $|G : Z(G)| \geq ۶$.

اثبات. اگر $|G : Z(G)|$ برابر ۱، ۲، ۳، یا ۵ باشد، آنگاه $G/Z(G)$ دوری است. پس G آبلی است. اگر $|G : Z(G)| = ۴$ و $x \in G - Z(G)$، آنگاه $Z(G) \subseteq C_G(x) \subseteq G$ که نتیجه می‌دهد $|G : C_G(x)| = ۲$. بنابراین G، ۳- جایگشتپذیر است. □

لم ۱۱.۴.۹. فرض کنید G گروه متناهی باشد و

$$\begin{aligned} X &= \{x \in G \mid |G : C_G(x)| \geq ۳\}, \\ Y &= \{x \in G \mid |G : C_G(x)| = ۲\}, \\ Z &= \{x \in G \mid |G : C_G(x)| = ۱\}. \end{aligned}$$

اگر تعداد عناصری که شاخص مرکزسازشان در G حداقل برابر ۳ است، حداقل $۳|Z|$ باشد، آنگاه $\mathrm{pr}(G) \leq \frac{۱}{۲}$.

اثبات. داریم

$$\begin{aligned} C &= \{(x,y) \in G \times G \mid xy = yx\} \\ &= k(G)|G| \\ &\leq (|X|/۳ + |Y|/۲ + |Z|) \cdot |G| \\ &= (|Z| + (|X| - ۳|Z|)/۳ + |Y|/۲ + |Z|) \cdot G \\ &\leq (|Z| + (|X| - ۳|Z|)/۲ + |Y|/۲ + |Z|) \cdot |G| \\ &= (|X| + |Y| + |Z|)|G|/۲ \\ &= |G|^۲/۲. \end{aligned}$$

بنابراین

$$\mathrm{pr}(G) = \frac{|C|}{|G|^۲} \leq \frac{۱}{۲}. \qquad \square$$

قضیه ۱۲.۴.۹. اگر G گروه متناهی باشد و $\mathrm{pr}(G) > \frac{۱}{۲}$، آنگاه G، ۳- جایگشتپذیر است.

اثبات. فرض کنید چنین نباشد. با نمادهای لم ۱۱.۴.۹، داریم $X \neq \emptyset$. عضو $g \in X$ را اختیار می‌کنیم و قرار می‌دهیم $n = |G : C_G(g)|$. آنگاه $Z \cup Zg \subseteq C_G(g)$ و داریم $(Z \cup Zg) \cap Y = \emptyset$، که نتیجه می‌دهد $|C_G(g) \cap Y| \leq \frac{|G|}{n} - ۲|Z|$. در نتیجه

$$|(G - C_G(g)) \cap Y| \geq |Y| - \frac{|G|}{n} + ۲|Z|.$$

اگر $x \in (G - C_G(g)) \cap Y$، آنگاه $|G : C_G(x)| = ۲$ و

$$C_G(g) \cap (G - C_G(g)) \neq \emptyset.$$

لم ۱۱.۴.۹، نتیجه می‌دهد $|G : C_G(xg)| \geq |G : C_G(g)| \geq ۳$. بنابراین $C_G(g) \cap (G - C_G(x)) = \emptyset$. در نتیجه $G - C_G(g) \cap Y \subseteq X$، در واقع چون $Zg \subseteq X \cap C_G(g)$، داریم $(G - C_G(g)) \cap Y \subset X - Zg$. بنابراین

$$|X| - |Z| = |X - Zg| \geq |(G - C_G(g)) \cap Y| \geq |Y| - \frac{|G|}{n} + ۲|Z|,$$

یعنی

$$|X| \geq |Y| - \frac{|G|}{n} + ۳|Z| \qquad (۴)$$

با توجه به لم ۱۱.۴.۹ و رابطه (۴) اگر نشان دهیم $|Y| \geq |G|/۳$ مساله حل است. پس فرض کنید $|Y| < \frac{|G|}{۳}$. در این حالت لم ۱۱.۴.۹، نتیجه می‌دهد $|X| > \frac{|G|}{۲}$. بنابراین $|X| > ۳|Z|$ و حکم ثابت است. $\square$

یک تعمیم طبیعی مفهوم n- جایگشتپذیری مفهوم n- بازنویس‌پذیری است. مجموعه‌ی $\{x_۱, x_۲, \dots, x_n\}$ از عناصر G را بازنویس‌پذیر گوییم هرگاه جایگشت‌های متمایز $\sigma \in S_n$ و τ وجود داشته باشند که

$$x_{\sigma(۱)}x_{\sigma(۲)}\cdots x_{\sigma(n)} = x_{\tau(۱)}x_{\tau(۲)}\cdots x_{\tau(n)}.$$

گروه G را n- بازنویس‌پذیر گوییم هرگاه هر زیرمجموعه‌ی n عضوی آن بازنویس‌پذیر باشد. واضح است که هر گروه n- جایگشتپذیر ، n- بازنویس‌پذیر نیز هست.

قضیه ۱۳.۴.۹. فرض کنید G گروه متناهی باشد. اگر $|G| \leq |Z(G)| + n!$، آنگاه G، n- بازنویس‌پذیر است.

اثبات. فرض کنید بر خلاف حکم که G، n- بازنویس‌پذیر نباشد. بنابراین زیرمجموعه‌ی n عضوی $\{x_۱, x_۲, \dots, x_n\}$ از G وجود دارد که به ازای هر $n!$ انتخابهای متمایز برای σ در S_n، عناصر $x_{\sigma(۱)}x_{\sigma(۲)}, \dots x_{\sigma(n)}$ همگی متمایزند، یعنی

$$|\{x_{\sigma(۱)}x_{\sigma(۲)}\cdots x_{\sigma(n)} \mid \sigma \in S_n\}| = n!.$$

اگر به ازای یک $\rho \in S_n$، $x_{\rho(۱)}x_{\rho(۲)}\cdots x_{\rho(n)} \in Z(G)$، آنگاه به خصوص داریم

$$x_{\rho(۱)}(x_{\rho(۱)}x_{\rho(۲)}\cdots x_{\rho(n)}) = (x_{\rho(۱)}x_{\rho(۲)}\cdots x_{\rho(n)})x_{\rho(۱)}.$$

با حذف $x_{\rho(۱)}$ از سمت چپ تساوی فوق و با قرار دادن $\tau(i) = \rho(i+۱)$، برای $۱ \leq i \leq n$ و $\tau(n) = \rho(۱)$، به دست می‌آید

$$x_{\rho(۱)}x_{\rho(۲)}\cdots x_{\rho(n)} = x_{\tau(۱)}x_{\tau(۲)}\cdots x_{\tau(n)}.$$

که خلاف انتخاب $\{x_۱, x_۲, \dots, x_n\}$ است. پس

$$Z(G) \cap \{x_{\sigma(۱)}x_{\sigma(۲)}\cdots x_{\sigma(n)} \mid \sigma \in S_n\} = \emptyset$$

که نتیجه می‌دهد $|Z(G)| + n! < |G|$. این متناقض با فرض است. توجه کنید بنا به انتخاب مجموعه‌ی $\{x_۱, \dots, x_n\}$، $x_۱ \notin Z(G)$؛ پس در رابطه‌ی فوق نامساوی اکید است. □

نتیجه ۱۴.۴.۹. فرض کنید G گروه متناهی باشد و $|G| \leq n!$. در این صورت G، n- بازنویس‌پذیر است. □

بنابراین S_n، n- بازنویس‌پذیر است. مشابه قضیه ۳.۴.۹، می‌توان نشان داد:

قضیه ۱۵.۴.۹. فرض کنید H زیرگروهی با شاخص m در گروه G باشد. اگر H، r بازنویس‌پذیر باشد، آنگاه G، mr- بازنویس‌پذیر است.

اثبات. قرار می‌دهیم $n = mr$، n عضو $x_۱$، $x_۲$، ...، x_n از G را در نظر می‌گیریم. هم مجموعه‌های

$$H,\ \ x_۱H,\ \ x_۱x_۲H,\ \ x_۱x_۲x_۳H,\ \ \dots,\ \ x_۱x_۲\cdots x_nH$$

را در نظر می‌گیریم. چون $|G : H| = m$ و $n = rm$، بنا به اصل لانه کبوتری $r+۱$ عدد صحیح $i_۱$، $i_۲$، ...، $i_{r+۱}$ وجود دارند که $۰ \leq i_۱ \leq i_۲ \leq \cdots \leq i_{r+۱} \leq n$ و

$$x_۱x_۲\cdots x_{i_۱}H = x_۱x_۲\cdots x_{i_۲}H = \cdots = x_۱x_۲\cdots x_{i_{r+۱}}H$$

(اگر $i_۱ = ۰$ اولین هم‌مجموعه برابر H است). بنابراین r عضو

$$a_j = x_{i_{j+۱}}x_{i_{j+۱}}\cdots x_{i_{j+۱}}, \quad j = ۱, ۲, \dots, r,$$

به H تعلق دارند. چون H، r- بازنویس‌پذیر است، جایگشت‌های متمایز $\sigma, \tau \in S_n$ وجود دارند که

$$a_{\sigma(۱)}a_{\sigma(۲)}\cdots a_{\sigma(n)} = a_{\tau(۱)}a_{\tau(۲)}\cdots a_{\tau(n)}.$$

در نتیجه

$$x_۱x_۲\cdots x_{i_۱}a_{\sigma(۱)}\cdots a_{\sigma(r)}x_{i_{r+۱}+۱}\cdots x_n = x_۱\cdots x_{t_۱}a_{\tau(۱)}\cdots a_{\tau(r)}x_{i_{r+۱}+۱}\cdots x_n,$$

که نشان می‌دهد G، n- بازنویس‌پذیر است. □

قضیه ۱۶.۴.۹. اگر G گروهی باشد که $|G'| < n!$، آنگاه G، n- بازنویس‌پذیر است.

اثبات. فرض کنید $x_۱$، $x_۲$، ...، x_n عناصر G باشند. چون G/G' آبلی است، به ازای هر $\sigma \in S_n$ داریم

$$x_۱x_۲\cdots x_nG' = x_{\sigma(۱)}x_{\sigma(۲)}\cdots x_{\sigma(n)}G'.$$

پس $d_\sigma \in G'$ وجود دارد که $x_{\sigma(۱)}x_{\sigma(۲)}\cdots x_{\sigma(n)} = x_۱x_۲\cdots x_nd_\sigma$. اگر به ازای یک σ، $d_\sigma = ۱$، حکم ثابت است. پس فرض کنید به ازای هر $\sigma \in S_n$، $d_\sigma \neq ۱$. چون $|G'| < n!$، بنا به اصل لانه کبوتری جایگشت‌های متمایز $\sigma, \tau \in S_n$ وجود دارند که $d_\sigma = d_\tau$. بنابراین

$$x_{\sigma(۱)}x_{\sigma(۲)}\cdots x_{\sigma(n)} = x_{\tau(۱)}x_{\tau(۲)}\cdots x_{\tau(n)}.$$

پس G، n- بازنویس‌پذیر است. □

تعدادی مرجع برای مطالعه‌ی بیشتر

1. A. Abdollahi, A. Mohammadi Hassanabadi and B. Taeri. *A property equivalent to n-permutability,* J. Algebra **221** (1999) 570-578.
2. A. Abdollahi, A. Mohammadi Hassanabadi and B. Taeri. *An n-rewritability criterion for infinite groups,* Comm. Algebra **29**(4) (2001) 1571-1581.
3. M. Bianchi, R.Brandl and A. Mauri. *On the 4-permutational property,* Arch. Math. **48** (1987) 281-285.
4. R. D. Blyth. *Rewriting products of group elements I,* J. Algebra **116** (1988) 506-521.
5. R. D. Blyth. *Rewriting products of group elements II,* J. Algebra **119** (1988) 252-259.
6. R. D. Blyth and A. Rhemtulla. *Rewritable products in FC-by-finite groups,* Canad. J. Math, **XLI** No 2, (1988) 369-384.
7. R. D. Blyth and D. J. S. Robinson. *Insoluble groups with the rewriting property P_8,* J. pure and applied Alg. **72** (1991) 251-263.
8. R. D. Blyth and D. J. S. Robinson. *Recent progress on rewritability in groups,* Group Theory Proceeding of the 1987 Singapore Conference, (de Gruyter, Berlin, 1989).
9. R. D. Blyth and D. J. S. Robinson. *Solution of the solubility problem for rewritable groups,* J. London Math. Soc. **2** (1990) 438-444.
10. R. Brandl. *General bounds for permutability in finite groups,* Arch. Math. **53** (1989) 245-249.
11. M. Curzio, P. Longobardi and M. Maj. *Su di problema combinatoria in teoria dei gruppi,* Atti. Acc. Lincei. Rend. fis. VIII, **LXXIV** (1983) 136-142.
12. M. Curzio, P. Longobardi, M. Maj and A. Rhemtulla. *Groups with many rewritable products,* Proc. Amer. Math. Soc. **115** Number 4, August (1992) 931-934.
13. M. Curzio, P. Longobardi, M. Maj and D. J. S. Robinson. *A permutational property of groups,* Arch.Math. **44** (1985) 385-389.
14. J. S. Ellenberg, G. J. Sherman, L. M. Smithline, C. A. Sugar and E. K. Wepsic. *The combinatorics of rewritability in finite groups,* Proc. Ohiao State-Denison Conf. (Editors: S. Surinder and R. Solomon.) Singapore: World Scientific (1993) 250-261.

15. J. Lennox, A. Mohammadi Hassanabadi and J. Wiegold. *Some commutativity criteria,* Rend. Sem. Mat. Univ. Padova, **84** (1990) 135-141.

16. J. L. Leavitt, G. J. Sherman and M. E. Walker. *Rewritability in finite groups,* Amer. Math. Monthly **99** (1992) 442-452.

17. J. Lennox, A. Mohammadi Hassanabadi and J. Wiegold. *Some commutativity criteria II,* Rend. Sem. Mat. Univ. Padova, **86** (1991) 207-211.

18. P. Longobardi and M. Maj. *On groups in which every product of four elements can be reordered,* Arch. Math. **49** (1987) 273-276.

19. P. Longobardi, M. Maj and S. E. Stonehewer. *The classification of groups in which every product of four elements can be reordered,* Rend. Sem. Mat. Univ. Padova **93** (1995) 253-261.

20. P. Longobardi, M. Maj and S. E. Stonehewer. *Finite 2-groups in which every product of four elements can be reordered,* Illinois J. Math. **35** (1991) 198-214.

21. M. Maj. *Some remarks on groups with permutable subgroup products,* Comm. Algebra **17** (10) (1989) 2539-2555.

22. M. Maj. *On the derived length of groups with some permutational property,* J. Algebra, **136** (1991) 86-91.

23. M. Maj and S. E. Stonehewer. *Non-nilpotent groups in which every product of four elements can be reordered,* Canad. J. Math. **XLII** No. 6, (1990) 1053-1066.

24. F. Menegazzo. *A property equivalent to commutativity,* Rend. Sem. Mat. Univ. Padova, c**87** (1992).

25. A. Mohammadi Hassanabadi and A. Rhemtulla. *Criteria for commutativity in large groups.* Canad. Math. Bull. **XX(Y)** (1998), 1-6.

26. A. Mohammadi Hassanabadi. *A property equivalent to permutabilty for groups,* Rend. Sem. Mat. Univ. Padova, **100** (1998), 137-142.

27. C. Mitchell, C. College and G. J. Sherman. *Counting triples in finite groups,* Congressus Numerantium **109** (1995) 129-134.

28. A. Restivo and C. Reutenauer. *On the Burnside problem for semigroups,* J. Algebra **89** (1984) 102-104.

فصل ۱۰

حلقه‌ها

تاکنون ساختارهای جبری را مطالعه کرده‌ایم که یک عمل دوتایی روی آن‌ها تعریف شده. اما حتماً توجه کرده‌اید که روی برخی از ساختارها اعمال دوتایی دیگری نیز می‌توان تعریف کرد. مثلاً روی مجموعه‌ی اعداد صحیح، مجموعه‌ی اعداد گویا، مجموعه‌ی اعداد حقیقی، مجموعه‌ی اعداد مختلط، و مجموعه‌ی اعداد صحیح به پیمانه‌ی n، دو عمل جمع و ضرب متعارف وجود دارند. هر کدام از این مجموعه‌ها نسبت به عمل جمع گروه آبلی و نسبت به عمل ضرب نیم‌گروه هستند ، و به علاوه قوانین توزیع‌پذیری نیز در آن‌ها برقرار است. این ساختارها را حلقه می‌نامیم. در این فصل خواص مقدماتی حلقه‌ها را بررسی می‌کنیم.

۱.۱۰ خواص مقدماتی حلقه‌ها

مجموعه‌ی ناتهی R را به همراه دو عمل دوتایی به نام‌های جمع و ضرب $(+, \cdot)$ حلقه گوییم، هرگاه $(R, +)$ یک گروه آبلی و $(R, \cdot)$ یک نیم‌گروه باشد و هم‌چنین قوانین توزیع‌پذیری برقرار باشند، یعنی برای هر $a, b, c \in R$،

$$\begin{aligned} a \cdot (b + c) &= (a \cdot b) + (a \cdot c) \\ (b + c) \cdot a &= (b \cdot a) + (c \cdot a). \end{aligned}$$

عضو بی‌اثر جمع R را با ۰ و وارون جمعی (قرینه‌ی) $a \in R$ را با $-a$ نشان می‌دهیم. بنابراین سه تایی $(R, +, \cdot)$ را حلقه گوییم هرگاه R مجموعه‌ای ناتهی ، و $+$ و $\cdot$ دو عمل دوتایی روی R باشند که در شرایط زیر صدق کنند:

(الف) برای هر $a, b, c \in R$، $(a + b) + c = a + (b + c)$

(ب) به ازای هر $a, b \in R$، $a + b = b + a$

(ج) عضوی مثل $0 \in R$ وجود دارد که برای هر $a \in R$، $a + 0 = a$.

(د) به ازای هر $a \in R$ عضوی چون $-a \in R$ وجود دارد که $a + (-a) = 0$

(هـ) به ازای هر $a, b, c \in R$، $(a \cdot b) \cdot c = a \cdot (b \cdot c)$

(و) به ازای هر $a, b, c \in R$، $a \cdot (b + c) = a \cdot b + a \cdot c$

(ز) به ازای هر $a, b, c \in R$، $(b + c) \cdot a = (b \cdot a) + (c \cdot a)$

۰ را عضو صفر حلقه‌ی $(R, +, \cdot)$ گوییم. معمولاً به جای $a \cdot b$ می‌نویسیم ab و به جای $a + (-b)$ می‌نویسیم $a - b$. هم‌چنین به جای $(a \cdot b) + c$ می‌نویسیم $ab + c$، به جای $(a \cdot b) + (-(a \cdot c))$ می‌نویسیم $ab - ac$. به علاوه، معمولاً به جای این که بگوییم $(R, +, \cdot)$ حلقه است می‌گوییم R حلقه است.

تعریف ۱.۱.۱۰. حلقه‌ی R را تعویض‌پذیر گوییم، هرگاه عمل ضرب در R تعویض‌پذیر باشد، یعنی به ازای هر $a, b \in R$ داشته باشیم $ab = ba$. حلقه‌ای را که تعویض‌پذیر نباشد تعویض‌ناپذیر می‌نامیم.

در یک حلقه‌ی R عضو $e \in R$ را عضو همانی گوییم هرگاه برای هر $a \in R$، $a = ea = ae$. پس عضو همانی (در صورت وجود)، عضو همانی نیم‌گروه $(R, \cdot)$ و بنابراین یکتاست. عضو همانی R را (در صورت وجود) با ۱ یا 1_R نشان می‌دهیم.

تعریف ۲.۱.۱۰. حلقه‌ی R را یکدار گوییم هرگاه عضو همانی داشته باشد.

فرض کنید R حلقه‌ای یکدار (با عضو همانی ۱) باشد ؛ عضو $a \in R$ را وارون‌پذیر (یکه) گوییم هرگاه نسبت به عمل ضرب وارون داشته باشد، یعنی عضو $b \in R$ وجود داشته باشد که $ab = ba = ۱$. وارون a (در صورت وجود) یکتاست و آن را با $a^{-۱}$ نشان می‌دهیم. می‌دانیم مجموعه‌ی اعضای وارون‌پذیر R یک گروه ضربی است که آن را با $R^\times$ نشان می‌دهیم. حلقه‌ی R را نابدیهی گوییم هرگاه $R \neq \{۰\}$، یعنی R بیش از یک عضو داشته باشد.
اکنون مثال‌هایی از حلقه می‌آوریم.

مثال ۳.۱.۱۰. $\mathbb{Z}$، $\mathbb{Q}$، $\mathbb{R}$ و $\mathbb{C}$ همگی تحت عمل جمع و ضرب معمولی اعداد ، حلقه‌های تعویض‌پذیر و یکدار هستند و هم‌چنین داریم $\mathbb{Z}^\times = \{-۱, ۱\}$، $\mathbb{Q}^\times = \mathbb{Q} - \{۰\}$، $\mathbb{R}^\times = \mathbb{R} - \{۰\}$، و $\mathbb{C}^\times = \mathbb{C} - \{۰\}$. □

حلقه‌ی یکدار R را حلقه‌ی تقسیم گوییم هرگاه هر عضو ناصفرv وارون‌پذیر باشد. یک حلقه‌ی تقسیم تعویض‌پذیر را میدان گوییم.

مثال ۴.۱.۱۰. اگر n عدد صحیح مثبت باشد، $\mathbb{Z}_n$ به همراه عمل جمع و ضرب به پیمانه‌ی n حلقه‌ی تعویض‌پذیر و یکدار است و داریم $\mathbb{Z}_n^\times = \{\bar{a} \in \mathbb{Z}_n \mid \gcd\{a, n\} = ۱\}$. □

مثال ۵.۱.۱۰. اگر $n > ۱$ عدد صحیح باشد، $n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}$ به همراه عمل جمع و ضرب متعارف، یک حلقه‌ی تعویض‌پذیر است که یکدار نیست. □

مثال ۶.۱.۱۰. فرض کنید R حلقه باشد و $n \geq ۱$،یک ماتریس $n \times n$ روی R یک ماتریس به صورت

$$A = [a_{ij}] = \begin{bmatrix} a_{۱۱} & a_{۱۲} & \cdots & a_{۱n} \\ a_{۲۱} & a_{۲۲} & \cdots & a_{۲n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n۱} & a_{n۲} & \cdots & a_{nn} \end{bmatrix}$$

است، که در آن هر a_{ij} عضو R است، و آن را درایه‌ی (i, j)، A گوییم. مجموعه‌ی همه‌ی ماتریس‌های $n \times n$ روی R را با $M_n(R)$ نشان می‌دهیم. اگر $A = [a_{ij}]$ و $B = [b_{ij}]$ عناصری از $M_n(R)$ باشند، تعریف می‌کنیم

$$\begin{aligned} A = B &\iff a_{ij} = b_{ij}, \quad \forall i, j \\ A + B &= [a_{ij} + b_{ij}] \\ AB &= [c_{ij}], \quad c_{ij} = \sum_{k=۱}^{n} a_{i_k} b_{k_j}, \quad \forall i, j. \end{aligned}$$

به راحتی می‌توان دید $M_n(R)$ تحت عمل جمع و ضرب ماتریسی که در بالا تعریف شد یک حلقه است. □

صفر $M_n(R)$ ماتریس صفر است، $[۰] = ۰$ که هر درایه آن صفر است. قرینه‌ی $A = [a_{ij}]$ عبارت است از $-A = [-a_{ij}]$، قوانین شرکت‌پذیری و توزیع‌پذیری از قوانین متناظر در R نتیجه می‌شوند. هرگاه R یکدار باشد $M_n(R)$ نیز یکدار است. عضو همانی آن ماتریس همانی $n \times n$،

$$I = \begin{bmatrix} ۱ & ۰ & \cdots & ۰ \\ ۰ & ۱ & \cdots & ۰ \\ \vdots & \vdots & \ddots & \vdots \\ ۰ & ۰ & \cdots & ۱ \end{bmatrix}$$

است، که روی قطر آن ۱، سایر درایه‌ها صفر است. $M_n(R)$ را حلقه‌ی ماتریس‌های $n \times n$ روی R گوییم. اگر $n \geq ۲$، و R حلقه‌ای باشد که عمل ضرب در R نابدیهی است، حتی اگر R تعویض‌پذیر باشد، $M_n(R)$ تعویض‌ناپذیر است. اگر عمل ضرب در حلقه‌ی R نابدیهی باشد دو عضو $a, b \in R$ وجود دارند که $ab \neq ۰$، داریم

$$\begin{bmatrix} ۰ & b \\ ۰ & ۰ \end{bmatrix} \begin{bmatrix} a & ۰ \\ ۰ & ۰ \end{bmatrix} = \begin{bmatrix} ۰ & ۰ \\ ۰ & ۰ \end{bmatrix} \neq \begin{bmatrix} ۰ & ab \\ ۰ & ۰ \end{bmatrix} = \begin{bmatrix} a & ۰ \\ ۰ & ۰ \end{bmatrix} \begin{bmatrix} ۰ & b \\ ۰ & ۰ \end{bmatrix}.$$

پس $M_۲(R)$ تعویض‌پذیر نیست. به همین نحو $M_n(R)$، $n \geq ۲$، تعویض‌پذیر نیست.

مثال ۷.۱.۱۰. $M_۲(\mathbb{Z}_۲)$ یک حلقه‌ی تعویض‌ناپذیر با ۱۶ عضو است. □

مثال ۸.۱.۱۰. اگر R حلقه باشد و $n \geq ۱$، یک چندجمله‌ای درجه n با ضرایب در R عبارتی به صورت

$$f(x) = a_۰ + a_۱x + a_۲x^۲ + \cdots + a_nx^n = \sum_{i=۰}^{n} a_ix^i$$

است، که در آن x یک متغیر است و $a_۰, a_۱, \ldots, a_n \in R$ و $a_n \neq ۰$. مجموعه‌ی همه‌ی چندجمله‌ای‌ها با ضرایب در R را با $R[x]$ نشان می‌دهیم. اگر

$$f(x) = a_۰ + a_۱x + \cdots + a_nx^n \quad \text{و} \quad g(x) = b_۰ + b_۱x + \cdots + b_mx^m$$

عناصری از $R[x]$ باشند، آن‌گاه

$$f(x) = g(x) \iff n = m, \quad a_i = b_i, \quad \forall i.$$

جمع و ضرب دو چند جمله‌ای به طریق متعارف انجام می‌شود. برای ارائه یک فرمول با اضافه کردن $۰x^i$، $i = n+۱, \ldots, m$ به $f(x)$ یا با اضافه کردن $۰x^i$، $i = m+۱, \ldots, n$ به $g(x)$ (در صورت لزوم) فرض می‌کنیم $n = m$. اکنون می‌توانیم یک فرمول برای جمع و ضرب $f(x)$ و $g(x)$ ارائه کنیم:

$$f(x) + g(x) = \sum_{i=۰}^{n}(a_i + b_i)x^i$$
$$f(x)g(x) = \sum_{i=۰}^{m+n} c_ix^i, \quad c_i = \sum_{k=۰}^{i} a_kb_{i-k}, \quad \forall i$$

به راحتی می‌توان دید $R[x]$ تحت عمل جمع و ضرب چندجمله‌ای‌ها که در بالا تعریف شد یک حلقه است. □

مثال ۹.۱.۱۰. فرض کنید X مجموعه‌ای ناتهی و R حلقه‌ای دلخواه باشد. مجموعه‌ی همه‌ی توابع از X به R را با $\mathrm{Map}(X, R)$ نشان می‌دهیم. $\mathrm{Map}(X, R)$ با عمل جمع و ضرب نقطه‌وار که به صورت زیر تعریف می‌شود یک حلقه است: اگر f و g دو عضو $\mathrm{Map}(X, R)$ باشند، تعریف می‌کنیم

$$f + g : X \longrightarrow R, \qquad (f + g)(x) = f(x) + g(x), \ \ \forall x \in X$$
$$f \cdot g : X \longrightarrow R, \qquad (f \cdot g)(x) = f(x)g(x), \ \ \forall x \in X.$$

عضو صفر $\mathrm{Map}(X, R)$ تابع ثابت $\theta : X \longrightarrow R$ است که با $\theta(x) = ۰$، به ازای هر $x \in X$، تعریف می‌شود. قرینه‌ی $f \in \mathrm{Map}(X, R)$ تابع $-f : X \longrightarrow R$ است که با $(-f)(x) = -f(x)$، به ازای هر $x \in X$، تعریف می‌شود. اگر R حلقه‌ی یکدار باشد، آن‌گاه $\mathrm{Map}(X, R)$ نیز یکدار است و تابع $\tau : X \longrightarrow R$ با ضابطه‌ی $\tau(x) = ۱$، به ازای هر $x \in X$، عضو همانی آن است. □

مثال ۱۰.۱.۱۰. اگر $R_۱$، $R_۲$، ...، R_n حلقه باشند حاصل‌ضرب دکارتی آن‌ها، یعنی $R_۱ \times R_۲ \times \cdots \times R_n$ تحت اعمال جمع و ضرب مولفه‌ای یک حلقه است:

$$(r_۱, r_۲, \ldots r_n) + (s_۱, s_۲, \ldots s_n) = (r_۱ + s_۱, r_۲ + s_۲, \ldots r_n + s_n)$$
$$(r_۱, r_۲, \ldots r_n) \cdot (s_۱, s_۲, \ldots s_n) = (r_۱s_۱, r_۲s_۲, \ldots, r_ns_n).$$

$R_۱ \times R_۲ \times \cdots \times R_n$ تعویض‌پذیر است اگر و تنها اگر هر R_i تعویض‌پذیر باشد. عضو صفر آن $(۰, ۰, \ldots ۰)$ است. اگر هر R_i یکدار باشد، آن‌گاه $R_۱ \times \cdots \times R_n$ نیز یکدار است و $(۱, ۱, \ldots ۱)$ عضو همانی آن است. □

مثال ۱۱.۱.۱۰. اگر i، j، k عناصر Q_8، گروه کواترنیونی، باشند و R حلقه‌ای دلخواه باشد، مجموعه‌ی

$$Q_R = \{\alpha_1 + \alpha_2 i + \alpha_3 j + \alpha_4 k \mid \alpha_i \in R\}$$

تحت عمل جمع و ضرب متعارف یک حلقه است، که آن را حلقه‌ی کواترنیونی گوییم. $Q_{\mathbb{Q}}$ را حلقه‌ی کواترنیونی گویا، و $Q_{\mathbb{R}}$ را حلقه‌ی کواترنیونی حقیقی گوییم. □

اگر R حلقه باشد چون R یک گروه آبلی جمعی است، قوانین توان صورت دیگری دارند و به صورت ضرایب نوشته می‌شوند: اگر $n \in \mathbb{Z}$، $na \in R$. در زیر قوانین متناظر توان و ضرایب آورده شده‌اند:

در گروه جمعی	در گروه ضربی
$0a = 0$	$a^0 = 1$
$1a = a$	$a^1 = a$
$(-1)a = -a$	$a^{(-1)} = a^{-1}$
$(n+m)a = na + ma$	$a^{n+m} = a^n a^m$
$n(a+b) = na + nb$	$(ab)^n = a^n b^n$ ($ab = ba$ اگر)
$n(ma) = (nm)a$	$(a^m)^n = a^{mn}$

اکنون برخی خواص مقدماتی حلقه‌ها را ثابت می‌کنیم. ابتدا توجه کنید که اگر R یک حلقه باشد، برای هر $a \in R$ داریم $0a = (0+0)a = 0a + 0a$. پس $0a = 0$.

قضیه ۱۲.۱.۱۰. اگر R حلقه باشد و $a, b, c \in R$، آنگاه

(الف) $a(-b) = (-a)b = -(ab)$.

(ب) $(-a)(-b) = ab$.

(ج) $a(b-c) = ab - ac$ و $(b-c)a = ba - ca$.

(د) به ازای هر $m, n \in \mathbb{Z}$، $(ma)(nb) = (mn)(ab)$.

اثبات. (الف) چون

$$(-a)b + ab = (-a+a)b = 0b = 0 = -(ab) + ab,$$

داریم $(-a)b = -(ab)$. به طریق مشابه $a(-b) = -(ab)$.

(ب) بنا به (الف) $(-a)(-b) = a(-(-b)) = ab$.

(ج) چون $b - c = b + (-c)$، بنا به (الف) داریم ،

$$a(b-c) = a(b+(-c)) = ab + a(-c) = ab + (-(ac)) = ab - ac.$$

به طریق مشابه $(b-c)a = ba - ca$.

(د) ابتدا نشان می‌دهیم، به ازای هر $n \in \mathbb{Z}$، $a(nb) = n(ab)$. به ازای $n = 0$ حکم واضح است، زیرا $a0 = 0$. اگر به ازای $n \geq 0$ برقرار باشد، آنگاه

$$a[(n+1)b] = a(nb + b) = a(nb) + ab = n(ab) + ab = (n+1)ab.$$

پس به استقرا برای $n \geq 0$ داریم $a(nb) = n(ab)$. اگر $n < 0$، آنگاه $-n = m$، که $m > 0$. بنابراین

$$\begin{aligned} a(nb) &= a((-m)b) \\ &= a(-(mb)) \\ &= -[a(mb)] \\ &= -[m(ab)] \\ &= (-m)(ab) \\ &= n(ab). \end{aligned}$$

بنابراین به ازای هر $n \in \mathbb{Z}$ نشان دادیم، $a(nb) = n(ab)$.
به همین نحو می‌توان نشان داد به ازای هر $n \in \mathbb{Z}$، $(na)b = n(ab)$. □

نتیجه ۱۳.۱.۱۰. اگر R حلقه‌ای یکدار باشد، آنگاه $R \neq \{۰\}$ اگر و تنها اگر ۰ و ۱ عناصر متمایز باشند.

اثبات. فرض کنید $R \neq \{۰\}$؛ عضو $a \in R$، $a \neq ۰$ را در نظر می‌گیریم. اگر $۰ = ۱$، آنگاه $a = a۱ = a۰ = ۰$، که تناقض است. پس $۰ \neq ۱$. عکس مطلب واضح است، زیرا R حداقل دو عضو متمایز ۰ و ۱ را دارد. □

اکنون قضیه‌ی دوجمله‌ای را برای حلقه‌ها ثابت می‌کنیم.

قضیه ۱۴.۱.۱۰. (قضیه‌ی دوجمله‌ای) فرض کنید a و b عناصری از حلقه‌ی یکدار R باشند که تعویض شوند، یعنی $ab = ba$. در این صورت به ازای هر $n \in \mathbb{N}$ داریم

$$\begin{aligned}(a+b)^n &= \sum_{k=۰}^{n} \binom{n}{k} a^{n-k}b^k \\ &= \binom{n}{۰}a^n + \binom{n}{۱}a^{n-۱}b + \cdots + \binom{n}{n-۱}ab^{n-۱} + \binom{n}{n}b^n.\end{aligned}$$

اثبات. به استقرا روی n عمل می‌کنیم. به ازای $n = ۱$، داریم

$$\sum_{k=۰}^{۱} \binom{۱}{k} a^{۱-k}b^k = \binom{۱}{۰}a + \binom{۱}{۱}b = a + b.$$

پس حکم به ازای $n = ۱$ برقرار است. اکنون فرض کنید قضیه برای $n \geq ۱$ برقرار باشد، داریم

$$\begin{aligned}(a+b)^{n+۱} &= (a+b)(a+b)^n \\ &= (a+b)\sum_{k=۰}^{n} \binom{n}{k} a^{n-k}b^k \\ &= \sum_{k=۰}^{n} \binom{n}{k} a^{n-k+۱}b^k + \sum_{k=۰}^{n} \binom{n}{k} a^{n-k}b^{k+۱} \\ &= a^{n+۱} + \sum_{k=۱}^{n} \binom{n}{k} a^{n-k+۱}b^k + \sum_{k=۰}^{n-۱} \binom{n}{k} a^{n-k}b^{k+۱} + b^{n+۱}\end{aligned}$$

با تبدیل k به $k - ۱$ در مجموع دوم و با استفاده از اتحاد پاسکال پاسکال (تمرین ۳ از صفحه‌ی ۱۳ را ببینید) داریم

$$\begin{aligned}(a+b)^{n+۱} &= a^{n+۱} + \sum_{k=۱}^{n} \binom{n}{k} a^{n-k+۱}b^k + \sum_{k=۱}^{n} \binom{n}{k-۱} a^{n-k+۱}b^k + b^{n+۱} \\ &= a^{n+۱} + \sum_{k=۱}^{n} \left[\binom{n}{k} + \binom{n}{k-۱}\right] a^{n-k+۱}b^k + b^{n+۱} \\ &= \sum_{k=۰}^{n+۱} \binom{n+۱}{k} a^{n+۱-k}b^k. \qquad \square\end{aligned}$$

قضیه‌ی دوجمله‌ای، در حالتی که حلقه‌ی R یکدار نباشد، نیز درست است. در این حالت ، برای اجتناب از جملات $b^۰$ و $a^۰$، جملات اول و آخر مجموع را جداگانه می‌نویسیم. یعنی اگر $a, b \in R$ و $ab = ba$، آنگاه داریم

$$(a+b)^n = a^n + \sum_{k=۱}^{n-۱} \binom{n}{k} a^{n-k}b^k + b^n.$$

گاهی اوقات پیش می‌آید که در یک حلقه حاصل‌ضرب دو عضو ناصفر برابر صفر باشد، مثلاً در حلقه‌ی $\mathbb{Z}_۶$ داریم $\bar{۳}\bar{۲} = \bar{۰}$. این وضعیت را با تعریف زیر مشخص می‌کنیم.

تعریف ۱۵.۱.۱۰. عضو ناصفر a در حلقه‌ی R را مقسوم‌علیه چپ [راست] صفر گوییم هرگاه عضو ناصفر $b \in R$ وجود داشته باشد که $ab = ۰$ [$ba = ۰$].یک مقسوم‌علیه صفر عضوی از R است که هم مقسوم‌علیه راست صفر و هم مقسوم‌علیه چپ صفر باشد.

اگر R حلقه‌ی یکدار باشد، یک مقسوم‌علیه صفر نمی‌تواند وارون‌پذیر باشد. زیرا اگر $a \in R$ مقسوم‌علیه صفر باشد، عضو ناصفر $b \in R$ وجود دارد که $ab = ۰$. حال اگر a وارون‌پذیر باشد، آنگاه

$$b = ۱b = (a^{-۱}a)b = a^{-۱}(ab) = a^{-۱}۰ = ۰,$$

که تناقض است. بنابراین مقسوم‌علیه صفر، وارون‌پذیر نیست و یا به طور معادل عضو وارون‌پذیر مقسوم‌علیه صفر نیست.

مثال ۱۶.۱.۱۰. در حلقه‌ی $\mathbb{Z}_n$، عضو $\bar{a}$ مقسوم‌علیه صفر است اگر و تنها $\bar{a}$ وارون‌پذیر نباشد و $a \neq ۰$، یعنی $\gcd\{a, n\} \neq ۱$.

حل در بحث پیش از مثال دیدیم یک مقسوم‌علیه صفر وارون‌پذیر نیست. پس اگر $\bar{a} \in \mathbb{Z}_n$ مقسوم‌علیه صفر باشد، آنگاه $\bar{a}$ وارون‌پذیر نیست. بنابراین $\gcd\{a, n\} \neq ۱$.
برعکس اگر $\gcd\{a, n\} = d > ۱$، آنگاه اعداد صحیح r و s وجود دارند که $a = rd$ و $n = sd$. پس $nr = sdr = sa$ و $\overline{nr} = \overline{sa}$. بنابراین $\bar{s}\bar{a} = \bar{۰}$. چون $۱ < s < n$، $\bar{s} \neq \bar{۰}$. پس $\bar{a}$ مقسوم‌علیه صفر است. □

تعریف ۱۷.۱.۱۰. حلقه‌ی تعویض‌پذیر و یکدار R را دامنه‌ی صحیح یا ID (مخفف Integral Domain) می‌نامیم هرگاه مقسوم‌علیه صفر نداشته باشد.

هر میدان یک دامنه‌ی صحیح است. به ویژه $\mathbb{Q}$، $\mathbb{R}$، $\mathbb{C}$، $\mathbb{Z}_p$، (p عدد اول) دامنه‌های صحیح هستند. عکس مطلب درست نیست مثلاً $\mathbb{Z}$ دامنه‌ی صحیح است و میدان نیست.

مثال ۱۸.۱.۱۰. حلقه‌ی $M_۲(\mathbb{Z})$ دامنه‌ی صحیح نیست. زیرا $M_۲(\mathbb{Z})$ مقسوم‌علیه صفر دارد، مثلاً

$$\begin{bmatrix} ۰ & ۱ \\ ۰ & ۰ \end{bmatrix}\begin{bmatrix} ۱ & ۰ \\ ۰ & ۰ \end{bmatrix} = \begin{bmatrix} ۰ & ۰ \\ ۰ & ۰ \end{bmatrix}.$$

به علاوه $M_۲(\mathbb{Z})$ تعویض‌پذیر هم نیست. □

مثال ۱۹.۱.۱۰. فرض کنید $(R, +)$ یک گروه آبلی باشد. عمل ضرب روی R را با $ab = ۰$، به ازای هر $a, b \in R$، تعریف می‌کنیم. در این صورت $(R, +, \cdot)$ یک حلقه است که آن را حلقه‌ی صفر گوییم. اگر R بیش از یک عضو داشته باشد، R حلقه‌ای تعویض‌پذیر است و یکدار نیست و هر عضو ناصفرش مقسوم‌علیه صفر است. □

فرض کنید حلقه‌ی R مقسوم‌علیه چپ صفر نداشته باشد. در این صورت R مقسوم علیه راست صفر نیز ندارد. زیرا اگر $a \in R$ یک مقسوم‌علیه راست صفر باشد، آنگاه عضو ناصفر $b \in R$ وجود دارد که $ba = ۰$، این یعنی b مقسوم علیه چپ صفر است، که تناقض است.
حال فرض کنید اعضای $a, b, c \in R$ طوری باشند که $ab = ac$ و $a \neq ۰$. در این صورت $ab - ac = ۰$ و $a(b - c) = ۰$. چون R مقسوم‌علیه چپ صفر ندارد و $a \neq ۰$، داریم $b - c = ۰$، یعنی $b = c$. در نتیجه قانون حذف از چپ برقرار است. قانون حذف از راست نیز برقرار است، زیرا اگر $a, b, c \in R$ طوری باشند که $ba = ca$ و $a \neq ۰$، آنگاه $(b - c)a = ۰$ و چون R مقسوم‌علیه چپ صفر ندارد، $b - c = ۰$، یعنی $b = c$.
به طریق مشابه اگر R مقسوم علیه راست صفر نداشته باشد، آنگاه مقسوم‌علیه چپ صفر نیز ندارد و قوانین حذف از چپ و راست در R برقرارند.
اکنون فرض کنید یکی از قوانین حذف، مثلاً حذف از چپ، برقرار باشد. فرض کنید a عضو ناصفری از R باشد و $b \in R$. اگر $ab = ۰$، آنگاه $ab = a۰$ و بنا به قانون حذف از چپ $b = ۰$. اگر $ba = ۰$ و $b \neq ۰$، آنگاه $ba = b۰$ و بنا به قانون حذف از چپ داریم $a = ۰$ که تناقض است. پس $b = ۰$. بنابراین اگر قانون حذف از چپ در R برقرارند باشد، آنگاه R مقسوم‌علیه صفر ندارد و قانون حذف از راست نیز برقرار است.

به طریق مشابه اگر قانون حذف از راست در R برقرار باشد، آنگاه R مقسوم‌علیه صفر ندارد و قانون حذف از چپ نیز برقرار است.

قضیه ۲۰.۱.۱۰. هر حلقه‌ی متناهی R با بیش از یک عضو که مقسوم‌علیه چپ یا راست صفر نداشته باشد، یک حلقه‌ی تقسیم است.

اثبات. ابتدا ثابت می‌کنیم R عضو بی‌اثر دارد. عضو دلخواه $a \in R \neq ۰$ را در نظر می‌گیریم. عناصر مجموعه‌ی $aR = \{ar \mid r \in R\}$ دوبه‌دو متمایزند، زیرا اگر $ar_۱ = ar_۲$، چون $a \neq ۰$ و طبق فرض قانون حذف از چپ برقرار است، داریم $r_۱ = r_۲$. پس تعداد اعضای aR دقیقاً برابر تعداد اعضای R است، یعنی $|aR| = |R|$. چون $aR \subseteq R$ و R متناهی است، $aR = R$. اکنون چون $a \in R = aR$، عضو $x_۰ \in R$ وجود دارد که $a = ax_۰$. در نتیجه $a(x_۰a) = (ax_۰)a = aa$ و با حذف a از طرفین تساوی داریم $x_۰a = a$. بنابراین $x_۰a = ax_۰ = a$.
حال ادعا می‌کنیم که $x_۰$ عضو همانی R است. عضو دلخواه $b \in R$ را در نظر بگیرید. چون $(bx_۰)a = b(x_۰a) = ba$، با حذف a از طرفین تساوی داریم $bx_۰ = b$. به همین نحو چون $a(x_۰b) = (ax_۰)b = ab$، داریم $x_۰b = b$.
پس $x_۰ = ۱$ عضو همانی R است. حال عضو دلخواه $a \in R \neq ۰$ را در نظر می‌گیریم چون $۱ \in R = aR$ پس عضو $y \in R$ وجود دارد که $ay = ۱$. با ضرب طرفین تساوی اخیر در a از سمت راست داریم $aya = a$. با حذف a از سمت چپ داریم $ya = ۱$. بنابراین $ay = ya = ۱$ و a وارون‌پذیر است. در نتیجه R یک حلقه‌ی تقسیم است. □

نتیجه ۲۱.۱.۱۰. هر حلقه‌ی تعویض‌پذیر و متناهی با بیش از یک عضو که مقسوم‌علیه صفر ندارد، یک میدان است. □

در نتیجه‌ی فوق شرط تعویض‌پذیری زاید است. در واقع هر حلقه‌ی متناهی که مقسوم‌علیه چپ و راست صفر نداشته باشد تعویض‌پذیر و در نتیجه میدان است. این قضیه‌ای عمیق از ودربرن است و اثبات آن مشکل‌تر است. اثباتی از این قضیه را در فصل ۱۴ ارائه می‌کنیم.

نتیجه ۲۲.۱.۱۰. هر دامنه‌ی صحیح متناهی میدان است. □

فرض کنید R حلقه باشد. گاهی اوقات بیش می‌آید که مرتبه‌ی اعضای $(R, +)$ متناهی (با یک کران) باشد، مثلاً در حلقه‌ی $\mathbb{Z}_۶$ داریم $\bar{۶}\bar{a} = \bar{۰}$، به ازای هر $\bar{a} \in \mathbb{Z}_۶$. این مشاهده به تعریف زیر منجر می‌شود.

تعریف ۲۳.۱.۱۰. اگر برای حلقه‌ی R عدد طبیعی n وجود داشته باشد که برای هر $a \in R$، $na = ۰$، (یعنی مرتبه‌ی جمعی اعضای R همگی متناهی و یک کران n داشته باشند) گوییم مشخصه‌ی R ناصفر است و کوچک‌ترین عدد طبیعی واجد این خاصیت را مشخصه‌ی R گوییم. در صورتی که چنین عددی وجود نداشته باشد گوییم مشخصه‌ی R صفر است. مشخصه‌ی R را با $\operatorname{char} R$ نشان می‌دهیم.

به عنوان مثال مشخصه‌ی $\mathbb{Z}_n$ برابر n و مشخصه‌های $\mathbb{Z}$، $\mathbb{Q}$، $\mathbb{R}$ و $\mathbb{C}$ برابر صفرند.

قضیه ۲۴.۱.۱۰. اگر R حلقه‌ی یکدار باشد، آنگاه $\operatorname{char} R = n > ۰$ اگر و تنها اگر n کوچک‌ترین عدد طبیعی باشد که $n۱_R = ۰$.

اثبات. ($\Longleftarrow$) اگر $\operatorname{char} R = n > ۰$، آنگاه به ازای هر $a \in R$ داریم $na = ۰$، به ویژه $n۱_R = ۰$. اگر $۰ < m < n$ طوری باشد که $m۱_R = ۰$، آنگاه به ازای هر $a \in R$ داریم

$$ma = m(۱_R a) = (m۱_R)a = ۰a = ۰$$

که متناقض با خاصیت n است. پس n کوچک‌ترین عدد طبیعی است که $n۱_R = ۰$.
($\Longrightarrow$) فرض کنید n کوچک‌ترین عدد طبیعی باشد که $n۱_R = ۰$. به ازای هر $a \in R$ داریم

$$na = n(۱_R a) = (n۱_R)a = ۰a = ۰.$$

پس n کوچک‌ترین عدد طبیعی است که به ازای هر $a \in R$، $na = ۰$. □

نتیجه ۲۵.۱.۱۰. در دامنه‌ی صحیح R همه‌ی عناصر ناصفر مرتبه‌ی جمعی یکسان دارند. اگر $\operatorname{char} R = ۰$، این مرتبه برابر ∞ است؛ و اگر $\operatorname{char} R = n > ۰$ این مرتبه برابر n است.

اثبات. ابتدا فرض کنید $\operatorname{char} R = n > ۰$. بنا به تعریف، به ازای هر $a \in R$، $na = ۰$. پس به ازای هر $a \in R$، $O(a) < \infty$. اگر $O(a) = m$ داریم $m|n$. از طرف دیگر

$$۰ = ma = m(۱_R a) = (m۱_R)a.$$

چون R دامنه‌ی صحیح است، $a \neq ۰$. پس $m۱_R = ۰$. به علاوه چون n کوچک‌ترین عدد طبیعی است که $n۱_R = ۰$. داریم $n \leq m$. بنابراین $n = m$.

حال فرض کنید $\operatorname{char} R = ۰$. اگر مرتبه‌ی عضو ناصفری از R مثل a متناهی باشد، یعنی به ازای یک $m \in \mathbb{N}$، $ma = ۰$، آنگاه $۰ = ma = (m۱_R)a$. چون R دامنه‌ی صحیح است، $m۱_R = ۰$ که تناقض است. پس به ازای هر $a \neq ۰$، $O(a) = \infty$. □

نتیجه ۲۶.۱.۱۰. دامنه‌ی صحیح R مشخصه‌ی مثبت دارد اگر و تنها اگر به ازای یک عضو ناصفر $a \in R$ و به ازای یک $n \in \mathbb{N}$ داشته باشیم $na = ۰$. □

قضیه ۲۷.۱.۱۰. مشخصه‌ی دامنه‌ی صحیح R یا صفر است و یا عددی اول.

اثبات. اگر $\operatorname{char} R = n > ۰$ و $n = n_۱n_۲$، آنگاه

$$۰ = n۱_R = (n_۱n_۲)۱_R = (n_۱۱_R)(n_۲۱_R)$$

چون R دامنه‌ی صحیح است، داریم $n_۱۱_R = ۰$ یا $n_۲۱_R = ۰$. چون n کوچک‌ترین عددی است که $n۱_R = ۰$، پس یکی از $n_۱$، $n_۲$ برابر ۱ و دیگری برابر n است، یعنی n عددی اول است. □

تمرین‌ها

۱. اگر R حلقه باشد و به ازای هر $a, b \in R$، $ab = a + b$ نشان دهید $R = \{۰\}$.

۲. فرض کنید R حلقه‌ی یکدار باشد و $a \in R$. اگر a و $a - ۱$ وارون‌پذیر باشند، نشان دهید $a^{-۱} - ۱$ نیز وارون‌پذیر است.

۳. فرض کنید R حلقه‌ی یکدار و بدون مقسوم‌علیه چپ و راست صفر باشد و $a, b \in R$. ثابت کنید:
(الف) $ab = ۱$ اگر و تنها اگر $ba = ۱$.
(ب) اگر $a^۲ = ۱$، آنگاه $a = ۱$ یا $a = -۱$.

۴. اگر R حلقه باشد و به ازای هر $a \in R$ $a \neq ۰$ عضو یکتای $b \in R$ وجود داشته باشد که $aba = a$ ثابت کنید
(الف) R مقسوم‌علیه (چپ و راست) صفر ندارد.
(ب) R یکدار است.
(ج) R حلقه‌ی تقسیم است.

۵. فرض کنید R حلقه‌ای متناهی باشد. ثابت کنید $\operatorname{char} R > ۰$ و $\operatorname{char} R$ برابر کوچک‌ترین مضرب مشترک مرتبه‌ی اعضای $(R, +)$ است.

۶. مشخصه‌ی حلقه‌های زیر را بیابید.
(الف) $\mathbb{Z}_n \times \mathbb{Z}_m$ (ب) $M_n(\mathbb{Z}_m)$ (ج) $\mathbb{Z} \times \mathbb{Z}_n$.

۷. اگر R حلقه‌ی تعویض‌پذیر و یکدار و $f(x) = a_۰ + a_۱x + \cdots + a_nx^n$ یک چندجمله‌ای در $R[x]$ باشد؛ ثابت کنید $f(x)$ مقسوم‌علیه صفر است اگر و تنها اگر $b \neq ۰$ وجود داشته باشد که $bf(x) = ۰$.

۸. (الف) در حلقه‌ی R نشان دهید $(a + b)(a - b) = a^۲ - b^۲$ اگر و تنها اگر $ab = ba$.
(ب) در حلقه‌ی R نشان دهید $(a + b)^۲ = a^۲ + ۲ab + b^۲$ اگر و تنها اگر $ab = ba$.

۹. (الف) اگر در یک حلقه‌ی یکدار $a^۳ = ۱$ و $ab + ba = ۱$، نشان دهید $a^۲ = ۱$.
(ب) اگر در یک حلقه‌ی یکدار $ab = a$ و $ba = b$، نشان دهید $a^۲ = a$ و $b^۲ = b$.

۱۰. فرض کنید R حلقه‌ی یکدار باشد و $a, b \in R$. نشان دهید $ab + ۱$ یکه است اگر و تنها اگر $ba + ۱$ یکه باشد.

۱۱. فرض کنید R یک حلقه باشد، نشان دهید $R(i) = \{a + ib \mid a, b \in R\}$ با اعمال زیر حلقه است

$$(a + ib) + (c + id) = a + c + i(b + d)$$
$$(a + ib)(c + id) = (ac - bd) + i(ad + bc).$$

۱۲. اگر $F = \{۰, ۱, a, b\}$ میدان باشد جدول ضرب و جمع F را بنویسید.

۱۳. اگر F میدان متناهی باشد و $|F| = q$. نشان دهید به ازای هر $a \in F$، $a^q = a$.

۱۴. نشان دهید میدان مرتبه‌ی ۶ وجود ندارد.

۲.۱۰ زیرحلقه

زیرمجموعه‌ی ناتهی S از حلقه‌ی R را زیرحلقه‌ی R می‌نامیم، هرگاه S به همراه عمل جمع و ضرب تعریف شده در R یک حلقه باشد. بنابراین S زیرحلقه‌ی R است اگر و تنها اگر زیرگروه جمعی R بوده و تحت عمل ضرب بسته باشد، یعنی به ازای هر $a, b \in S$ داشته باشیم $a - b \in S$ و $ab \in S$. اگر R میدان باشد و S تحت وارون نیز بسته باشد گوییم S زیرمیدان R است. بنابراین زیرمجموعه‌ی ناتهی S از میدان F را زیرمیدان F می‌نامیم، هرگاه به ازای $a, b \in S$، $a - b \in S$ و $ab \in S$ و $a^{-۱} \in S$ (برای $a \neq ۰$).

مثال ۱.۲.۱۰. اگر $n > ۱$ عدد صحیح باشد، $n\mathbb{Z}$ یک زیر حلقه‌ی $\mathbb{Z}$ است. □

مثال ۲.۲.۱۰. اگر R یک حلقه باشد و $a \in R$، آنگاه $C_R(a) = \{x \in R \mid xa = ax\}$، (مرکز ساز a) یک زیرحلقه‌ی R است. $C_R(a) \neq \emptyset$ زیرا $a \in C_R(a)$. حال اگر $x, y \in C_R(a)$، آنگاه

$$(x - y)a = xa - ya = ax - ay = a(x - y)$$

و

$$(xy)a = x(ya) = x(ay) = (xa)y = a(xy).$$

بنابراین $xy, x - y \in C_R(a)$. □

مثال ۳.۲.۱۰. اگر R یک حلقه باشد، مرکز R را که با $\mathrm{Cent}(R)$ نشان می‌دهیم یک زیرحلقه‌ی R است:

$$\mathrm{Cent}(R) = \{a \in R \mid \forall x \in R,\ \ ax = xa\}.$$

توجه کنید $۰ \in \mathrm{Cent}(R)$ و $\mathrm{Cent}(R) = \bigcap_{a \in R} C_R(a)$. به طور کلی اشتراک هر تعداد زیرحلقه دوباره زیرحلقه است. □

مثال ۴.۲.۱۰. اگر R حلقه‌ای دلخواه باشد، و

$$T_۲(R) = \begin{bmatrix} R & R \\ ۰ & R \end{bmatrix} = \left\{ \begin{bmatrix} a & b \\ ۰ & c \end{bmatrix} \middle| \, a, b, c \in R \right\}.$$

نشان دهید $T_۲(R)$، که آن را حلقه‌ی ماتریس‌های بالا مثلثی ۲ × ۲ روی R می‌نامیم، یک زیرحلقه‌ی $M_۲(R)$ است.

حل به وضوح ماتریس ۲ × ۲ صفر در $T_۲(R)$ قرار دارند، پس $T_۲(R) \neq \emptyset$.

حال اگر $A = \begin{bmatrix} a & b \\ ۰ & c \end{bmatrix}$ و $B = \begin{bmatrix} p & q \\ ۰ & r \end{bmatrix}$ دو عضو $T_۲(R)$ باشند، آنگاه

$$A - B = \begin{bmatrix} a - p & b - q \\ ۰ & c - r \end{bmatrix} \in T_۲(R), \quad AB = \begin{bmatrix} ap & aq + br \\ ۰ & cr \end{bmatrix} \in T_۲(R).$$

بنابراین $T_۲(R)$ زیرحلقه‌ی $M_۲(R)$ است. □

عضو e در حلقه‌ی R را خودتوان گوییم هرگاه $e = e^۲$. به عنوان مثال در هر حلقه‌ی یکدار R، اعضای ۰ و ۱ خودتوان هستند. هم‌چنین مثلاً $\begin{bmatrix} ۰ & ۱ \\ ۰ & ۱ \end{bmatrix}$ و $\begin{bmatrix} ۱ & ۱ \\ ۰ & ۰ \end{bmatrix}$ دو عضو خودتوان در $M_۲(R)$ هستند ، که در آن R یک حلقه‌ی یکدار است. به عنوان مثال دیگر اعضای $\bar{۳}$ و $\bar{۴}$ در $\mathbb{Z}_۶$ خودتوان هستند. اگر e عضوی خودتوان در حلقه‌ی یکدار R باشد، آن‌گاه $(۱-e)^۲ = ۱-e-e+e^۲ = ۱-e-e+e = ۱-e$. پس $e-۱$ نیز خودتوان است. هم‌چنین $e(۱-e) = (۱-e)e = ۰$.

قضیه ۵.۲.۱۰. اگر e عضوی خودتوان در حلقه‌ی R باشد، آن‌گاه $eRe = \{ere \mid r \in R\}$ یک زیرحلقه‌ی یکدار R با عضو همانی e است. به علاوه

$$eRe = \{a \in R \mid ea = a = ae\}.$$

اثبات. چون $e = e۰e \in eRe$، $eRe \neq \emptyset$. حال اگر $ese, ere \in eRe$، آن‌گاه

$$ere - ese = e(r-s)e \in eRe, \quad (ere)(ese) = e(res)e \in eRe.$$

از این‌رو eRe زیرحلقه‌ی R است. به علاوه چون $e = eee \in eRe$، $e \in eRe$. هم‌چنین به ازای هر $ere \in eRe$ داریم $e(ere) = ere = (ere)e$. پس e عضو همانی eRe است و $eRe \subseteq \{a \in R \mid ae = a = ea\}$. از طرف دیگر اگر $a \in R$ و $ae = a = ea$، آن‌گاه $a = eae \in eRe$. پس $eRe = \{a \in R \mid ae = a = ea\}$. □

مثال ۶.۲.۱۰. عضو $e = (۰, ۱)$ در حلقه‌ی $R^۲ = R \times R$ عضوی خودتوان است و $eRe = \{(۰, r) \mid r \in R\}$، حلقه‌ای یکدار با عضو همانی $e = (۰, ۱)$ است. به همین ترتیب عضو $e = \begin{bmatrix} ۱ & ۰ \\ ۰ & ۰ \end{bmatrix}$ در حلقه‌ی $R = M_۲(R)$ خودتوان است و $eRe = \left\{ \begin{bmatrix} r & ۰ \\ ۰ & ۰ \end{bmatrix} \middle| \, r \in R \right\}$ حلقه‌ای یکدار با عضو همانی $e = \begin{bmatrix} ۱ & ۰ \\ ۰ & ۰ \end{bmatrix}$ است. □

عضو a در حلقه‌ی R را پوچ‌توان می‌نامیم، هرگاه عدد صحیح مثبت n وجود داشته باشد که $a^n = ۰$. عضو صفر در هر حلقه پوچ‌توان است. به عنوان مثال اعضای $\bar{۲}$، $\bar{۴}$، و $\bar{۶}$ در حلقه‌ی $\mathbb{Z}_۸$ پوچ‌توان هستند. هم‌چنین اعضای $\begin{bmatrix} ۰ & r \\ ۰ & ۰ \end{bmatrix}$ و $\begin{bmatrix} ۰ & ۰ \\ r & ۰ \end{bmatrix}$ در حلقه‌ی $M_۲(R)$، (R حلقه‌ی دلخواه) و $\begin{bmatrix} \bar{۱} & \bar{۱} \\ \bar{۱} & \bar{۱} \end{bmatrix}$ در حلقه‌ی $M_۲(\mathbb{Z}_۲)$ پوچ‌توان هستند.

مثال ۷.۲.۱۰. اگر عضو a در حلقه‌ی یکدار R پوچ‌توان باشد، آن‌گاه $a-۱$ و $a+۱$ وارون‌پذیر هستند.

حل چون a پوچ‌توان است، عدد صحیح $n \geq ۱$ وجود دارد که $a^n = ۰$. فرض کنید n کوچک‌ترین عدد صحیح مثبت باشد که $a^n = ۰$. اعضای $u = ۱ + a + a^۲ + \cdots + a^{n-۱}$ و $v = ۱ - a + a^۲ - \cdots + (-۱)^{n-۱}a^{n-۱}$ در حلقه‌ی R را در نظر می‌گیریم. داریم

$$u(۱-a) = (۱ + a + \cdots + a^{n-۱})(۱-a) = ۱ - a^n = ۱$$
$$v(۱+a) = (۱ - a + \cdots + (-۱)^{n-۱}a^{n-۱})(۱+a) = ۱ + (-۱)^{n-۱}a^n = ۱$$

و به همین نحو $u(a-۱) = ۱$ و $(a+۱)v = ۱$. پس $a-۱$ و $a+۱$ وارون‌پذیرند. □

مثال ۸.۲.۱۰. فرض کنید R حلقه‌ای تعویض‌پذیر باشد. مجموعه‌ی اعضای پوچ‌توان R را با $N(R)$ نشان می‌دهیم: $N(R) = \{a \in R \mid \exists n \in \mathbb{N}, \ a^n = ۰\}$. نشان دهید $N(R)$ زیر حلقه‌ی R است. $N(R)$ را رادیکال پوچ می‌نامیم.

حل چون $۰^۱ = ۰$، $۰ \in N(R)$. بنابراین $N(R) \neq \emptyset$. فرض کنید $a, b \in N(R)$. پس اعداد صحیح مثبت n، m وجود دارند که $a^n = ۰$، و $b^m = ۰$. به ازای هر $j > n$ داریم

$$a^j = a^n a^{n-j} = ۰a^{n-j} = ۰$$

و به همین نحو به ازای هر $j > m$ داریم $b^j = ۰$. در نتیجه به ازای هر $k = ۱, ۲, \ldots, m$ داریم $a^{m+n-k}b^k = ۰b^k = ۰$ و به ازای هر $k = m, m+۱, \ldots, m+n$ داریم $a^{m+n-k}b^k = a^{m+n-k}۰ = ۰$. پس اگر قرار دهیم $c = m + n$، بنا به قضیه‌ی دوجمله‌ای، خواهیم داشت

$$(a+b)^c = a^c + \sum_{k=۱}^{c-۱} \binom{c}{k} a^{c-k}b^k + b^c = ۰,$$

و $a + b \in N(R)$. به علاوه چون $(ab)^n = a^n b^n = ۰b^n = ۰$، $ab \in N(R)$. پس $N(R)$ زیرحلقه‌ی R است. □

تمرین‌ها

۱. فرض کنید R یک حلقه و $R/\mathrm{Cent(R)}$ به عنوان گروه جمعی دوری باشد. نشان دهید R تعویض‌پذیر است.

۲. نشان دهید در حلقه‌ی تعویض‌پذیر و یکدار مجموع یک عضو پوچ‌توان و یک عضو وارون‌پذیر، وارون‌پذیر است.

۳. نشان دهید $\bar{a} \in \mathbb{Z}_n$ پوچ‌توان است اگر و تنها اگر هر شمارنده‌ی اول n، شمارنده‌ی اول a نیز باشد. اعضای پوچ‌توان $\mathbb{Z}_{۳۸}$ و $\mathbb{Z}_{۱۴۶}$ را بیابید.

۴. همه‌ی اعضای خودتوان $\mathbb{Z}_n$ را توصیف کنید و اعضای خودتوان $\mathbb{Z}_{۳۸}$ و $\mathbb{Z}_{۱۴۶}$ را بیابید.

۵. فرض کنید حلقه‌ی R عضو پوچ‌توان ناصفر نداشته باشد. نشان دهید هر عضو خودتوان R در مرکز R قرار دارد.

۶. حلقه‌ای که هر عضو آن خودتوان باشد را حلقه‌ی بولی می‌نامیم. ثابت کنید هر حلقه‌ی بولی تعویض‌پذیر است.

۷. فرض کنید R حلقه‌ای یکدار باشد و برای هر $a \neq ۱$ و $b \neq ۱$ در R رابطه‌ی $ab^۲ = ab$ برقرار باشد. نشان دهید R تعویض‌پذیر است.

۸. فرض کنید R یک حلقه باشد و $a \in R$. اگر a پوچ‌توان نباشد و $a - a^۲$ پوچ‌توان باشد، نشان دهید R عضو خودتوان ناصفر دارد.

۹. (الف) اگر در حلقه‌ی R داشته باشیم $a^m = a^n$ (m، n اعداد صحیح متمایز). نشان دهید توانی از a خودتوان است.
(ب) در حلقه‌ی متناهی R توانی از هر عضو، خودتوان است.

۱۰. در حالت‌های زیر نشان دهید در حلقه‌ی یکدار R، $ab = ۱$ نتیجه می‌دهد $ba = ۱$.
(الف) R متناهی باشد.
(ب) هر عضو خودتوان R در مرکز R باشد.

۱۱. اگر R یک حلقه و $e \in R$ عضوی خودتوان باشد، نشان دهید ، به ازای هر $r \in R$، (الف) $re - ere$ و $er - ere$ پوچ‌توان هستند.
(ب) $e + re - ere$ و $e + er - ere$ خودتوان هستند.

۱۲. فرض کنید e عضوی خودتوان از حلقه‌ی یکدار R باشد. نشان دهید شرایط زیر معادل هستند.
(الف) e در مرکز R قرار دارد.
(ب) e با هر عضو خودتوان تعویض می‌شود.
(ج) e با هر عضو پوچ‌توان تعویض می‌شود.
(د) e با هر عضو وارون‌پذیر تعویض می‌شود.

۱۳. فرض کنید R حلقه و m عدد صحیح مثبت ثابت باشد. اگر به ازای هر $a \in R$ داشته باشیم $a^{۲m} = a$، نشان دهید به ازای هر $a \in R$، $۲a = ۰$.

۱۴. فرض کنید G گروه آبلی باشد. نشان دهید

$$R = \begin{bmatrix} \mathbb{Z} & G \\ ۰ & \mathbb{Z} \end{bmatrix} = \left\{ \begin{bmatrix} n & a \\ ۰ & m \end{bmatrix} \;\middle|\; n, m \in \mathbb{Z},\ \ a \in G \right\}$$

تحت عمل جمع و ضرب متعارف ماتریس‌ها، حلقه است. یکه‌ها، پوچ‌توان‌ها و خودتوان‌های R را بیابید.

۱۵. اگر F میدان باشد، و $|F| = ۸$ و K زیرمیدانی از F باشد نشان دهید $K = F$ یا $K = \{۰, ۱\}$. در حالتی $|F| = ۱۶$ چه می‌توان گفت؟

۱۶. نشان دهید $\mathbb{Q}[i] = \{a + ib \mid a, b \in \mathbb{Q}\}$ زیرمیدان $\mathbb{C}$ است.

۱۷. (الف) نشان دهید $\mathbb{Q}[i\sqrt{۵}] = \{a + ib \mid a, b \in \mathbb{Q}\}$ زیرمیدان $\mathbb{C}$ است.
(ب) نشان دهید $\mathbb{Z}[i\sqrt{۵}] = \{n + mi\sqrt{۵} \mid n, m \in \mathbb{Z}\}$ زیرحلقه‌ی $\mathbb{C}$ است و یکه‌های آن را بیابید.

۱۸. اگر به ازای هر a در حلقه‌ی R داشته باشیم $a^۲ + a \in \mathrm{Cent}(R)$ ثابت کنید R تعویض‌پذیر است.

۱۹. اگر برای هر a در حلقه‌ی R داشته باشیم $a^۳ = a$ نشان دهید R تعویض‌پذیر است.

۲۰. فرض کنید R حلقه باشد و $a \in R$، $a^۲ = ۰$. ثابت کنید برای هر $x \in R$، $ax + xa$ با a تعویض می‌شود.

۲۱. فرض کنید در حلقه‌ی R برای هر $a \in R$ داشته باشیم $a^۴ = a$. ثابت کنید R تعویض‌پذیر است.

۲۲. فرض کنید R حلقه‌ای باشد که عضو پوچ‌توان ناصفر ندارد. نشان دهید اگر اعضای $a_۱, a_۲, \ldots, a_n \in R$ طوری باشند که $a_۱a_۲\cdots a_n = ۰$، آنگاه به ازای هر $\sigma \in S_n$، $a_{\sigma(۱)}a_{\sigma(۲)}\cdots a_{\sigma(n)} = ۰$.

۲۳. فرض کنید R حلقه‌ی تعویض‌پذیر و یکدار و $f(x) = a_۰ + a_۱x + \cdots + a_nx^n$ یک چندجمله‌ای در $R[x]$ باشد. ثابت کنید
(الف) $f(x)$ وارون‌پذیر است اگر و تنها اگر $a_۰$ وارون‌پذیر و $a_۱$، ...، a_n پوچ‌توان باشند.
(ب) $f(x)$ پوچ‌توان است اگر و تنها اگر $a_۰$، $a_۱$، ...، a_n پوچ‌توان باشند.

۲۴. (الف) نشان دهید $\mathbb{Z}[\sqrt{۲}] = \{n + m\sqrt{۲} \mid n, m \in \mathbb{Z}\}$ زیرحلقه‌ای از $\mathbb{C}$ است.
(ب) اگر a_k تخمینی برای $\sqrt{۲}$ باشد می‌دانیم (روش نیوتن) که $a_{k+۱} = \dfrac{a_k^۲ + ۲}{۲a_k}$ تخمین بهتری است. با استفاده از این مطلب نشان دهید $\mathbb{Z}[\sqrt{۲}]$ تعداد نامتناهی یکه دارد.

۲۵. فرض کنید $\mathbb{Z}[w] = \{n + mw \mid n, m \in \mathbb{Z}\}$ که در آن $w \in \mathbb{C} - \mathbb{Q}$ و $w^۲ \in \mathbb{Z}$. به ازای هر $a = n + mw \in \mathbb{Z}[w]$ قرار می‌دهیم $a^* = n - mw$ و $N(a) = n^۲ - w^۲m^۲$. نشان دهید
(الف) $\mathbb{Z}[w]$ زیرحلقه‌ی $\mathbb{C}$ و بنابراین دامنه‌ی صحیح است.
(ب) در $\mathbb{Z}[w]$، $n + mw = n_۱ + m_۱w_۱$ اگر و تنها اگر $n = n_۱$ و $m = m_۱$.
به علاوه برای هر $a, b \in \mathbb{Z}[w]$ نشان دهید.
(ج) $a^{**} = a$، $(ab)^* = a^*b^*$ و برای هر $r, s \in \mathbb{Z}$، $(ra + sb)^* = ra^* + sb^*$
(د) $N(a) = aa^*$، و $N(ab) = N(a)N(b)$.
(هـ) $a \in \mathbb{Z}[w]$ یکه است اگر و تنها اگر $N(a) = \pm ۱$.

۳.۱۰ همریختی

در این بخش مفاهیم همریختی و یکریختی برای حلقه را معرفی می‌کنیم. این مفاهیم شبیه همریختی و یکریختی برای گروه‌ها هستند.

تعریف ۱.۳.۱۰. فرض کنید R و S دو حلقه باشند، تابع $f : R \longrightarrow S$ را همریختی (حلقه‌ای) گوییم هرگاه برای هر $a, b \in R$ داشته باشیم

$$\begin{aligned} f(a+b) &= f(a) + f(b) \\ f(ab) &= f(a)f(b). \end{aligned}$$

به علاوه اگر f یک‌به‌یک و پوشا نیز باشد، f را یکریختی (حلقه‌ای) نامیم و گوییم R و S یکریخت‌اند و می‌نویسیم $R \cong S$. یک همریختی یک‌به‌یک و پوشا از حلقه‌ی R به خودش را خودریختی R گوییم. مجموعه‌ی خودریختی‌های حلقه‌ی R را با $\mathrm{Aut}\, R$ نشان می‌دهیم.

هرگاه $f : R \longrightarrow S$ همریختی حلقه‌ای باشد، آنگاه f یک همریختی بین گروه‌های جمعی R و S است. پس به ازای هر $n \in \mathbb{Z}$ و هر

$a \in R$ داریم $f(na) = nf(a)$. به ویژه $f(0) = 0$ و $f(-a) = -f(a)$. هم‌چنین هسته‌ی f، یعنی

$$\ker f = \{a \in R \mid f(a) = 0\}$$

یک زیرگروه جمعی R است. چون برای هر $a, b \in \ker f$ داریم $f(ab) = f(a)f(b) = 0$، $\ker f$ زیرحلقه‌ی R است. یادآوری می‌کنیم $\ker f = \{0\}$ اگر و تنها اگر f یک‌به‌یک باشد.

مثال ۲.۳.۱۰. تابع $f : \mathbb{Z} \longrightarrow \mathbb{Z}_n$ با ضابطه‌ی $f(a) = \bar{a}$ یک همریختی حلقه‌ای پوشا با هسته‌ی $\ker f = n\mathbb{Z}$ است. □

مثال ۳.۳.۱۰. اگر R حلقه‌ای یکدار باشد تابع $f : \mathbb{Z} \longrightarrow R$ با ضابطه‌ی $f(m) = m1_R$ یک همریختی حلقه‌ای با هسته‌ی $\ker f = \{m \in \mathbb{Z} \mid m1_R = 0\}$ است. بنابراین اگر $\operatorname{char} R = 0$، آن‌گاه $\ker f = \{0\}$ و f یک‌به‌یک است. اگر $\operatorname{char} R = n$، آن‌گاه $\ker f = n\mathbb{Z}$ و f یک‌به‌یک نیست. □

مثال ۴.۳.۱۰. فرض کنید R حلقه‌ای یکدار باشد و $|R| = p$، p عدد اول. نشان دهید $R \cong \mathbb{Z}_p$، که در آن جمع و ضرب در $\mathbb{Z}_p$ به طور معمول و به پیمانه‌ی p انجام می‌شود.

حل تابع $f : \mathbb{Z}_p \longrightarrow R$ را با $f(\bar{m}) = m1_R$ تعریف می‌کنیم. f خوش تعریف و یک‌به‌یک است، زیرا

$$\begin{aligned} \bar{m} = \bar{n} &\iff m \equiv n \mod p \\ &\iff p|(m-n) \\ &\iff (m-n)1_R = 0 \\ &\iff m1_R = n1_R. \end{aligned}$$

توجه کنید چون مرتبه‌ی R عدد اول است، گروه جمعی R دوری و هر عضو ناصفر آن مولدی از R است، به ویژه $O(1_R) = p$. اکنون به سادگی می‌توان دید که f یکریختی حلقه‌ای است. بنابراین $R \cong \mathbb{Z}_p$. □

اگر R حلقه‌ای با p عضو باشد، آن‌گاه گروه جمعی R یک گروه دوری است و هر عضو ناصفر آن مولدی از R است. در مثال بالا دیدیم که اگر R یکدار باشد، آن‌گاه $R \cong \mathbb{Z}_p$. حال اگر R یکدار نباشد. نشان می‌دهیم R حلقه‌ی صفر است. یعنی برای هر $a, b \in R$، $ab = 0$. فرض کنید $0 \neq a \in R$، آن‌گاه $R = \langle a \rangle = \{0, a, 2a, \ldots, (p-1)a\}$. کافی است نشان دهیم $a^2 = 0$. فرض کنید چنین نباشد و $a^2 \neq 0$. چون $a^2 \in R$، عدد $0 < j \leq p-1$ وجود دارد که $a^2 = ja$. پس به ازای هر $n \in \mathbb{N}$، داریم $a^n = j^{n-1}a$. بنا به قضیه‌ی فرما $j^{p-1} \equiv 1 \mod p$. بنابراین $a^p = j^{p-1}a = a$. برای هر $0 \leq k \leq p-1$ داریم $a^{p-1}(ka) = ka^p = ka$. از این‌رو a^{p-1} عضو همانی ضربی R است، که متناقض با فرض است.

مثال ۵.۳.۱۰. نشان دهید

$$R = \left\{ \begin{bmatrix} a & b \\ -b & a \end{bmatrix} \middle| \, a, b \in \mathbb{R} \right\}$$

حلقه‌ای یکریخت با حلقه‌ی اعداد مختلط، $\mathbb{C}$، است.

حل به راحتی می‌توان دید R زیرحلقه‌ای از $M_2(\mathbb{R})$ است. اکنون تابع $f : R \longrightarrow \mathbb{C}$ را با ضابطه‌ی

$$f\left(\begin{bmatrix} a & b \\ -b & a \end{bmatrix} \right) = a + ib$$

تعریف می‌کنیم. f یک‌به‌یک است زیرا $a+ib=a'+ib'$، در $\mathbb{C}$، نتیجه می‌دهد $a=a'$ و $b=b'$. هم‌چنین به وضوح f پوشاست. به علاوه

$$\begin{aligned} f\left(\begin{bmatrix} a & b \\ -b & a \end{bmatrix}+\begin{bmatrix} a' & b' \\ -b' & a' \end{bmatrix}\right) &= f\left(\begin{bmatrix} a+a' & b+b' \\ -(b+b') & a+a' \end{bmatrix}\right) \\ &= (a+a')+i(b+b') \\ &= (a+ib)+(a'+ib') \\ &= f\left(\begin{bmatrix} a & b \\ -b & a \end{bmatrix}\right)+f\left(\begin{bmatrix} a' & b' \\ -b' & a' \end{bmatrix}\right) \end{aligned}$$

و

$$\begin{aligned} f\left(\begin{bmatrix} a & b \\ -b & a \end{bmatrix}\begin{bmatrix} a' & b' \\ -b' & a' \end{bmatrix}\right) &= f\left(\begin{bmatrix} aa'-bb' & ab'+ba' \\ -ba'-ab' & aa'-bb' \end{bmatrix}\right) \\ &= (aa'-bb')+i(ab'+ba') \\ &= (a+ib)(a'+ib') \\ &= f\left(\begin{bmatrix} a & b \\ -b & a \end{bmatrix}\right) f\left(\begin{bmatrix} a' & b' \\ -b' & a' \end{bmatrix}\right). \end{aligned}$$

پس f یکریختی است. □

مثال ۶.۳.۱۰. نشان دهید حلقه‌های $R=\left\{\begin{bmatrix} a & b \\ ۰ & a \end{bmatrix}\middle| a,b\in\mathbb{Z}_۲\right\}$ و $\mathbb{Z}_۲\times\mathbb{Z}_۲$ یکریخت نیستند، اما به عنوان گروه‌های جمعی یکریخت هستند.

حل عضو ناصفر $r=\begin{bmatrix} ۰ & ۱ \\ ۰ & ۰ \end{bmatrix}$ در R در رابطه‌ی $r^۲=۰$ صدق می‌کند. فرض کنید $f:R\longrightarrow\mathbb{Z}_۲\times\mathbb{Z}_۲$ یکریختی حلقه‌ای باشد. اگر $s=f(r)$، آن‌گاه

$$s^۲=f(r)^۲=f(r^۲)=f(۰)=۰.$$

اما $s^۲=۰$ در $\mathbb{Z}_۲\times\mathbb{Z}_۲$ نتیجه می‌دهد $s=۰$. پس $s=f(r)=۰$. چون f یک‌به‌یک است، داریم $r=۰$، که تناقض است. از این رو R و $\mathbb{Z}_۲\times\mathbb{Z}_۲$ به عنوان حلقه یکریخت نیستند. اما به سادگی می‌توان دید تابع $g:R\longrightarrow\mathbb{Z}_۲\times\mathbb{Z}_۲$ با ضابطه‌ی $g\left(\begin{bmatrix} a & b \\ ۰ & a \end{bmatrix}\right)=(a,b)$ یک یکریختی بین گروه‌های جمعی R و $\mathbb{Z}_۲\times\mathbb{Z}_۲$ است. □

مثال ۷.۳.۱۰. نشان دهید معادله‌ی $x^۳-۵x^۲-x-۱۷=۰$ در $\mathbb{Z}$ جواب ندارد.

حل همریختی $f:\mathbb{Z}\longrightarrow\mathbb{Z}_۵$ را با $f(a)=\bar{a}$ در نظر می‌گیریم. اگر $n\in\mathbb{Z}$ جوابی از معادله باشد، داریم $n^۳-۵n^۲-n-۱۷=۰$. با اثر دادن f به دو طرف تساوی و استفاده از خاصیت همریختی بودن f داریم $\bar{n}^۳-\bar{۵}\bar{n}^۲-\bar{n}-\overline{۱۷}=۰$، که نتیجه می‌دهد $\bar{n}^۳-\bar{n}-\bar{۲}=۰$. اما $\bar{n}\in\mathbb{Z}_۵=\{\bar{۰},\bar{۱},\bar{۲},\bar{۳},\bar{۴}\}$ و می‌بینیم هیچ‌کدام از اعضای $\mathbb{Z}_۵$ در معادله‌ی فوق صدق نمیکنند، که تناقض است. □

مثال ۸.۳.۱۰. نشان دهید $x^۳-۶y^۳=۳$ در $\mathbb{Z}$ جواب ندارد.

حل تلاش اول ما این است که همانند مثال قبل معادله را به پیمانه‌ی ۶ تحویل کنیم. در $\mathbb{Z}_۶$ به دست بیاوریم: $\bar{x}^۲=\bar{۳}$. اما این معادله در $\mathbb{Z}_۶$ جواب $\bar{x}=\bar{۳}$ دارد. اگر در $\mathbb{Z}_۷$ عمل کنیم، معادله به صورت $\bar{x}^۳+\bar{y}^۳=\bar{۳}$ در می‌آید. چون

$$\bar{۲}^۳=\bar{۴}^۳=\bar{۱},\quad \bar{۳}^۳=\bar{۵}^۳=\bar{۶}^۳=\bar{۶},$$

تنها مکعب‌ها در $\mathbb{Z}_۷$ عبارت‌اند از $\bar{۰}$، $\bar{۱}$ و $\bar{۶}$ و مجموع دوبه‌دوی آن‌ها عبارت است از $\bar{۰}$، $\bar{۱}$، $\bar{۲}$، $\bar{۵}$ و یا $\bar{۶}$. چون $\bar{۳}$ در این فهرست نیست، این معادله در $\mathbb{Z}_۷$ جواب ندارد. پس معادله‌ی داده شده در $\mathbb{Z}$ جواب ندارد. □

تمرین‌ها

۱. (الف) مثالی از یک همریختی حلقه‌ای بزنید که R و S یکدار باشند و $f(۱_R) \neq ۱_S$.
(ب) اگر $f : R \longrightarrow S$ همریختی پوشای حلقه باشد و R و S یکدار باشند، نشان دهید $f(۱_R) = ۱_S$.
(ج) اگر $f : R \longrightarrow S$ همریختی حلقه‌ای باشد و R و S یکدار باشند و عضو وارون‌پذیر $u \in R$ وجود داشته باشد که $f(u)$ عضوی وارون‌پذیر از S باشد، نشان دهید $f(۱_R) = ۱_S$ و $f(u^{-۱}) = f(u)^{-۱}$.

۲. فرض کنید $f : R \longrightarrow S$ همریختی حلقه‌ای باشد که $f \neq ۰$. اگر R یکدار بوده و S مقسوم‌علیه چپ [راست] صفر نداشته باشد. ثابت کنید S یکدار است و $f(۱_R) = ۱_S$.

۳. اگر R حلقه باشد، نشان دهید $\operatorname{Aut} R$ (مجموعه‌ی همریختی‌های حلقه‌ای یک‌به‌یک و پوشا از R به R) تحت عمل ترکیب توابع گروه است.

۴. نشان دهید $f : \mathbb{Z}_n \longrightarrow \mathbb{Z}_m$ با ضابطه‌ی $f(\bar{a}) = k\bar{a}$، k عدد صحیح ثابت، همریختی حلقه‌ای است اگر و تنها اگر $m|kn$ و $m|(k^۲ - k)$.

۵. آیا همریختی حلقه‌ای پوشا از $\mathbb{Z}_{۲۴}$ به $\mathbb{Z}_۷$ وجود دارد؟ از $\mathbb{Z}_۶$ به $\mathbb{Z}_{۱۱}$ چطور ؟

۶. نشان دهید حلقه‌های $۲\mathbb{Z}$ و $۳\mathbb{Z}$ یکریخت نیستند.

۷. نشان دهید معادله‌ی $x^۳ - ۸x^۲ + ۵x + ۳ = ۰$ در $\mathbb{Z}$ ریشه ندارد.

۸. نشان دهید معادله‌ی $m^۳ + ۱۴n^۳ = ۱۲$ در $\mathbb{Z}$ جواب ندارد.

۹. نشان دهید معادله‌ی $۷m^۲ + ۱۱n^۲ = ۹$ در $\mathbb{Z}$ جواب ندارد.

۱۰. نشان دهید $n^۳ + (n+۱)^۳ + (n+۲)^۳ = k^۲ + ۱$ در $\mathbb{Z}$ جواب ندارد.

۱۱. فرض کنید $\mathbb{Q}$ حلقه‌ی اعداد گویا و R حلقه‌ای دلخواه باشد. اگر $f, g : \mathbb{Q} \longrightarrow R$ همریختی‌های حلقه‌ای باشند که $f|_{\mathbb{Z}} = g|_{\mathbb{Z}}$، نشان دهید $f = g$.

۱۲. فرض کنید R حلقه‌ای دلخواه باشد. قرار می‌دهیم $S = R \times \mathbb{Z}$ و جمع و ضرب روی S را به صورت زیر تعریف می‌کنیم: به ازای هر $a, b \in R$، و $m, n \in \mathbb{Z}$.

$$\begin{aligned}(a,m) + (b,n) &= (a+b, m+n),\\ (a,m)\cdot(b,n) &= (ab + na + mb, mn)\end{aligned}$$

نشان دهید حلقه‌ی S یکدار است و $R \hookrightarrow S$ (یعنی یک همریختی یک‌به‌یک از R به S وجود دارد). بنابراین هر حلقه‌ی دلخواه را می‌توان در حلقه‌ای یکدار نشاند.

۱۳. فرض کنید R حلقه‌ای با مشخصه‌ی $n > ۰$ باشد؛ $S = R \times \mathbb{Z}_n$ را در نظر بگیرید. جمع و ضرب روی S را به صورت زیر تعریف می‌کنیم: به ازای هر $(b, \bar{t}), (a, \bar{m}) \in S$

$$\begin{aligned}(a,\bar{m}) + (b,\bar{t}) &= (a+b, \overline{m+t})\\ (a,\bar{m})\cdot(b,\bar{t}) &= (ab + \bar{m}a + \bar{t}b, \overline{mt})\end{aligned}$$

نشان دهید S حلقه‌ی یکدار است و $\operatorname{char} S = n$. هم‌چنین $R \hookrightarrow S$.

۴.۱۰ ایدآل، حلقه‌ی خارج‌قسمتی

اگر R یک حلقه و I یک زیرگروه جمعی R باشد، چون R گروه جمعی آبلی است، I به عنوان زیرگروه جمعی R، در R نرمال است. پس می‌توان گروه جمعی $R/I = \{a + I \mid a \in R\}$ را تشکیل داد که در آن جمع هم‌مجموعه‌ها به صورت متعارف انجام می‌شود:

$$(a + I) + (b + I) = (a + b) + I \qquad \forall a, b \in R.$$

سوالی که مطرح است این است که آیا می‌توان با استفاده از عمل ضرب R یک عمل ضرب در R/I تعریف کرد و آن را به یک حلقه تبدیل نمود؟ یعنی آیا اگر تعریف کنیم

$$(a + I)(b + I) = ab + I$$

یک عمل ضرب خوش تعریف به دست می‌آوریم؟ حال ببینیم که رابطه‌ی بالا چه مجموع یک عمل خوش تعریف را به دست می‌دهد. فرض کنید $a + I = a' + I$ و $b + I = b' + I$. پس $x = a - a' \in I$ و $y = b - b' \in I$. برای این که عمل فوق خوش تعریف باشد باید داشته باشیم $ab + I = a'b' + I$، یعنی $ab - a'b' \in I$. داریم

$$\begin{aligned} ab - a'b' &= ab - (a - x)(b - y) \\ &= ab - ab + ay + xb - xy \\ &= ay + xb - xy. \end{aligned}$$

در صورتی که هر سه جمله‌ی ay، xb، و xy در I باشند، آنگاه $ab - a'b' \in I$ و عمل تعریف شده خوش تعریف است. بنابراین اگر به ازای هر $r \in R$ و هر $x \in I$، داشته باشیم $rx \in I$ و $xr \in I$، آنگاه سه جمله‌ی فوق در I هستند. پس عمل تعریف شده خوش تعریف است. بنابراین تعریف زیر را ارائه می‌کنیم.

تعریف ۱.۴.۱۰. زیرگروه جمعی I از حلقه‌ی R را ایدآل چپ [راست] R گوییم، هرگاه به ازای هر $r \in R$ و هر $x \in I$ داشته باشیم $rx \in I$ [$xr \in I$]. I را ایدآل (دوطرفی) R گوییم، هرگاه هم ایدآل راست و هم ایدآل چپ باشد.

بنابراین اگر I ایدآل R باشد، آنگاه عمل ضرب هم‌مجموعه‌ها در R/I،

$$(a + I)(b + I) = ab + I$$

یک عمل خوش تعریف است. پس به راحتی قضیه‌ی زیر را می‌توان ثابت کرد که اثبات آن را به عنوان تمرین واگذار می‌کنیم.

قضیه ۲.۴.۱۰. اگر I ایدآل حلقه‌ی R باشد، آنگاه R/I تحت عمل جمع و ضرب هم مجموعه‌ها یک حلقه است: به ازای هر $a, b \in R$

$$\begin{aligned} (a + I) + (b + I) &= (a + b) + I \\ (a + I)(b + I) &= ab + I. \end{aligned}$$ □

اگر I ایدآل حلقه‌ی R باشد، R/I را حلقه‌ی خارج‌قسمتی گوییم. هرگاه I زیرگروه جمعی R بوده و ضرب متعارف هم‌مجموعه‌ها در گروه جمعی R/I خوش تعریف باشد، آنگاه I یک ایدآل R است (چرا؟). توجه کنید هر ایدآل یک زیرحلقه است، اما عکس آن لزوماً درست نیست. دو مثال بعد این مطلب را نشان می‌دهند.

مثال ۳.۴.۱۰. $\mathbb{Z}$ زیرحلقه‌ای از $\mathbb{Q}$ است اما ایدآل $\mathbb{Q}$ نیست. □

مثال ۴.۴.۱۰. حلقه‌ی ماتریس‌های ۲×۲ با درایه‌های حقیقی، یعنی $M = M_۲(\mathbb{R})$، را در نظر بگیرید. در این صورت $\mathrm{Cent}(M) = \left\{ \begin{bmatrix} a & ۰ \\ ۰ & a \end{bmatrix} \middle| a \in \mathbb{R} \right\}$ یک زیرحلقه‌ی M است ولی ایدآل M نیست. □

اگر $f : R \longrightarrow S$ همریختی حلقه‌ای باشد، آنگاه $\ker f$ یک ایدآل R است. زیرا $\ker f$ یک زیرگروه جمعی R است و به علاوه برای هر $a \in R$ و هر $x \in \ker f$ داریم

$$\begin{aligned} f(ax) &= f(a)f(x) = f(a)۰ = ۰ \\ f(xa) &= f(x)f(a) = ۰f(a) = ۰, \end{aligned}$$

یعنی $xa, ax \in \ker f$. از این‌رو $\ker f$ یک ایدآل R است. از طرف دیگر $f(R) = \operatorname{Im} f$ یک زیرحلقه‌ی S است، اما ممکن است ایدآل نباشد (بررسی این مطالعه در تمرین‌ها خواسته شده است).

مثال ۵.۴.۱۰. فرض کنید R یک حلقه باشد. $\{۰\}$ و R دو ایدآل R هستند که آن‌ها را ایدآل‌های بدیهی R گوییم. ایدآل‌های دیگر R را نابدیهی نامیم. □

ایدآل I از حلقه‌ی R را ایدآل سره گوییم، هرگاه $I \neq R$. اکنون مثالی می‌آوریم که در یک حلقه ممکن است ایدآل چپ، ایدآل راست نباشد و برعکس.

مثال ۶.۴.۱۰. حلقه‌ی $M_۲(\mathbb{Z})$ را در نظر بگیرید و قرار دهید

$$I = \left\{ \begin{bmatrix} a & ۰ \\ b & ۰ \end{bmatrix} \middle| \, a, b \in \mathbb{Z} \right\}, \quad J = \left\{ \begin{bmatrix} a & b \\ ۰ & ۰ \end{bmatrix} \middle| \, a, b \in \mathbb{Z} \right\}$$

چون $\begin{bmatrix} ۰ & ۰ \\ ۰ & ۰ \end{bmatrix} \in I$، داریم $I \neq \emptyset$. فرض کنید $\begin{bmatrix} a & ۰ \\ b & ۰ \end{bmatrix}, \begin{bmatrix} c & ۰ \\ d & ۰ \end{bmatrix} \in I$ و $\begin{bmatrix} x & y \\ z & w \end{bmatrix} \in M_۲(\mathbb{Z})$، آنگاه

$$\begin{bmatrix} a & ۰ \\ b & ۰ \end{bmatrix} - \begin{bmatrix} c & ۰ \\ d & ۰ \end{bmatrix} = \begin{bmatrix} a-c & ۰ \\ b-d & ۰ \end{bmatrix} \in I$$

و

$$\begin{bmatrix} x & y \\ z & w \end{bmatrix} \begin{bmatrix} a & ۰ \\ b & ۰ \end{bmatrix} = \begin{bmatrix} xa+yb & ۰ \\ za+wb & ۰ \end{bmatrix} \in I.$$

بنابراین I یک ایدآل چپ $M_۲(\mathbb{Z})$ است. اکنون چون $\begin{bmatrix} ۰ & ۱ \\ ۰ & ۰ \end{bmatrix} \in M_۲(\mathbb{Z})$ و $\begin{bmatrix} ۱ & ۰ \\ ۱ & ۰ \end{bmatrix} \in I$ و

$$\begin{bmatrix} ۱ & ۰ \\ ۱ & ۰ \end{bmatrix} \begin{bmatrix} ۰ & ۱ \\ ۰ & ۰ \end{bmatrix} = \begin{bmatrix} ۰ & ۱ \\ ۰ & ۱ \end{bmatrix} \notin I$$

نتیجه می‌شود I ایدآل راست $M_۲(\mathbb{Z})$ نیست. به طریق مشابه J ایدآل راست $M_۲(\mathbb{Z})$ است و ایدآل چپ نیست. □

قضیه ۷.۴.۱۰. اگر R حلقه‌ای یکدار و I ایدآل (چپ، راست یا دوطرفی) از R باشد که شامل یک عضو وارون‌پذیر u است، آنگاه $I = R$.

اثبات. فرض کنید مثلاً I ایدآل چپ باشد، چون $u^{-۱} \in R$، $۱_R = u^{-۱}u \in I$. پس برای هر $a \in R$ داریم $a = a۱_R \in I$. بنابراین $I = R$. □

نتیجه ۸.۴.۱۰. یک حلقه‌ی تقسیم، به ویژه یک میدان، ایدآل (چپ، راست یا دوطرفی) نابدیهی ندارد. □

عکس نتیجهی بالا، در حالت ایدآل دوطرفی، درست نیست، زیرا حلقه‌هایی وجود دارند که ایدآل دوطرفی ندارند ولی حلقه‌ی تقسیم نیستند (تمرین ۶ را ببینید). اما در حالت ایدآل چپ یا راست درست است:

قضیه ۹.۴.۱۰. اگر R حلقه‌ای یکدار باشد که ایدآل چپ (یا راست) نابدیهی نداشته باشد، آنگاه R حلقه‌ی تقسیم است.

اثبات. فرض کنید $a \in R$، $a \neq ۰$. قرار می‌دهیم $Ra = \{ra \mid r \in R\}$. به سادگی می‌توان دید Ra یک ایدآل چپ R است. چون $a = ۱a \in Ra$، Ra ایدآل چپ ناصفر R است. چون R ایدآل چپ نابدیهی ندارد ، $R = Ra$. اکنون چون $۱ \in R = Ra$، $b \in R$ وجود دارد که $ba = ۱$. پس هر عضو $۰ \neq a \in R$ وارون چپ دارد. فرض کنید $۰ \neq a \in R$ و b وارون چپ a باشد، یعنی $ba = ۱$. در این صورت $b \neq ۰$. پس وارون چپ b وجود دارد. فرض کنید c وارون چپ b باشد، یعنی $cb = ۱$. با ضرب طرفین $ba = ۱$ از چپ در c داریم $cba = c$. چون $cb = ۱$، $a = c$. بنابراین $ab = ۱$ و $ba = ۱$. پس b وارون دوطرفی a است. بنابراین R حلقه‌ی تقسیم است. □

اگر p یک عدد اول باشد، آنگاه بنا به تعریف، به ازای هر $k = ۱, ۲, \ldots, p-۱$ داریم $\binom{p}{k} = \frac{p!}{k!(p-k)!}$، یعنی

$$p! = \binom{p}{k} k!(p-k)!.$$

p عبارت سمت راست تساوی فوق، یعنی $\binom{p}{k}k!(p-k)!$ را عاد می‌کند. بنا به لم اقلیدس، یا $p \mid \binom{p}{k}$ یا $p \mid k!(p-k)!$. اما چون $۱ \leq k \leq p-۱$ و $۱ \leq p-k \leq p-۱$ حالت دوم رخ نمیدهد. بنابراین $p \mid \binom{p}{k}$. این مطلب در اثبات قضیه‌ی مهم زیر به کار می‌آید.

قضیه ۱۰.۴.۱۰. اگر R حلقه‌ای تعویض‌پذیر با مشخصه‌ی عدد اول p باشد، آنگاه تابع $\varphi : R \longrightarrow R$ با ضابطه‌ی $\varphi(a) = a^p$ یک همریختی حلقه‌ای است (که آن را درون‌ریختی فروبنیوس گوییم). اگر R میدان متناهی باشد، آنگاه φ یکریختی است (که آن را خودریختی فروبنیوس می‌نامیم.)

اثبات. فرض کنید $a, b \in R$. چون R تعویض‌پذیر است،

$$\varphi(ab) = (ab)^p = a^p b^p = \varphi(a)\varphi().$$

هم‌چنین داریم

$$\varphi(a+b) = a^p + \sum_{k=۱}^{p-۱} \binom{p}{k} a^{p-k}b^k + b^p.$$

چون برای هر $k = ۱, ۲, \ldots, p-۱$، $p \mid \binom{p}{k}$ و مشخصه‌ی R برابر p است، داریم $\binom{p}{k}a^{p-k}b^k = ۰$، $k = ۱, ۲, \ldots, p-۱$. بنابراین

$$\varphi(a+b) = a^p + b^p = \varphi(a) + \varphi()$$

و φ همریختی حلقه‌ای است. اگر R میدان باشد، ایدآل نابدیهی ندارد ، پس $\ker \varphi = \{۰\}$؛ یعنی φ یک‌به‌یک است. اگر R متناهی باشد φ پوشا نیز هست. پس φ خودریختی است. □

فرض کنید I ایدآل حلقه‌ی R باشد، تابع $\pi : R \longrightarrow R/I$ با ضابطه‌ی $\pi(a) = a + I$ یک همریختی پوشای حلقه‌ای است که همریختی طبیعی نامیده می‌شود. به وضوح $\ker \pi = I$. پس I ایدآل حلقه‌ی R است اگر و تنها اگر هسته‌ی یک همریختی از R به حلقه‌ای دیگر باشد. قضیه‌ی زیر را به سادگی و با استفاده از قضیه‌ی مشابه در گروه‌ها می‌توان ثابت کرد.

قضیه ۱۱.۴.۱۰. اگر I ایدآل حلقه‌ی R باشد، آنگاه ایدآل‌های R/I دقیقاً به صورت J/I هستند که در آن J یک ایدآل R است و $I \subseteq J$. □

قضیه ۱۲.۴.۱۰. (قضیه‌ی اول یکریختی) اگر $f : R \longrightarrow S$ همریختی حلقه‌ای باشد، آنگاه $R/\ker f \cong \operatorname{Im} f$.

اثبات. طبق قضیه‌ی اول یکریختی برای گروه‌ها می‌دانیم تابع $\bar{f} : R/\ker f \longrightarrow \operatorname{Im} f$ با ضابطه‌ی $\bar{f}(a + \ker f) = f(a)$ یک همریختی یک‌به‌یک و پوشای گروهی است. پس کافی است ثابت کنیم $\bar{f}$، عمل ضرب را حفظ می‌کند. برای هر $a, b \in R$ داریم

$$\begin{aligned} \bar{f}((a+\ker f)(b+\ker f)) &= \bar{f}(ab + \ker f) \\ &= f(ab) \\ &= f(a)f(b) \\ &= \bar{f}(a+\ker f)\bar{f}(b+\ker f). \end{aligned}$$

بنابراین $\bar{f}$ همریختی حلقه‌ای نیز هست. □

قضیه ۱۳.۴.۱۰. (قضیه‌ی دوم یکریختی) اگر I و J ایدآل‌های حلقه‌ی R باشند، آنگاه $\frac{I+J}{J} \cong \frac{I}{I\cap J}$. □

قضیه ۱۴.۴.۱۰. (قضیه‌ی سوم یکریختی) اگر I، J ایدآل‌های حلقه‌ی R باشند و $I \subseteq J$، آنگاه $\frac{R/I}{J/I} \cong R/J$. □

در مثال ۳.۳.۱۰، دیدیم که اگر R حلقه‌ای یکدار باشد تابع $f : \mathbb{Z} \longrightarrow R$ با ضابطه‌ی $f(k) = k1_R$ همریختی است. توجه کنید $\operatorname{Im} f = \{k1_R \mid k \in \mathbb{Z}\} = \mathbb{Z}1_R$ زیرحلقه‌ای از R است. بنا به قضیه‌ی اول یکریختی $\mathbb{Z}/\ker f \cong \mathbb{Z}1_R$. هرگاه $\operatorname{char} R = 0$، آنگاه $\ker f = \{0\}$ و f یک‌به‌یک است. پس $\mathbb{Z} \cong \mathbb{Z}1_R$. اگر $\operatorname{char} R = n$، آنگاه $\ker f = n\mathbb{Z}$ و $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}1_R$. پس در حالتی که $\operatorname{char} R = 0$، آنگاه R زیرحلقه‌ای یکریختی با $\mathbb{Z}$ دارد و در حالتی که $\operatorname{char} R = n$، آنگاه R زیرحلقه‌ای یکریخت با $\mathbb{Z}_n$ دارد.
حالت مهم وقتی است که R میدان باشد. در این حالت زیرحلقه‌ی S از R زیرمیدان نامیده می‌شود، هرگاه S میدان باشد یا به طور معادل برای هر $a \in S$، $a^{-1} \in S$. حال اگر R میدان باشد مشخصه‌ی R یا صفر است و یا عدد اول p، اگر $\operatorname{char} R = p$، R زیرمیدانی یکریخت با $\mathbb{Z}_p$ دارد ، اگر $\operatorname{char} R = 0$، زیرحلقه‌ی $\mathbb{Z}1_R$ با $\mathbb{Z}$ یکریخت است. در این حالت قرار می‌دهیم

$$Q = \{ab^{-1} \mid a, b \in \mathbb{Z}1_R, b \neq 0\},$$

به سادگی می‌توان دید Q زیر میدان R و $\varphi : \mathbb{Q} \longrightarrow Q$ با ضابطه‌ی

$$\varphi\left(\frac{m}{n}\right) = (m1_R)(n1_R)^{-1}$$

یکریختی حلقه‌ای است. بنابراین R زیرمیدانی یکریخت با $\mathbb{Q}$ دارد. به خاطر این نتیجه $\mathbb{Z}_p$ و $\mathbb{Q}$ را میدانهای اول گوییم.

مثـال ۱۵.۴.۱۰. فـرض کـنـیـد I ایـدآلـی از حـلـقـه‌ی R بـاشـد، نـشـان دهـیـد $M_n(I)$ ایـدآلـی از $M_n(R)$ اسـت و $M_n(R/I) \cong M_n(R)/M_n(I)$.

حل به خاطر سادگی در محاسبه ها می‌نویسیم $\bar{a} = a + I$؛ بنابراین اگر همریختی طبیعی $\pi : R \longrightarrow R/I$ را در نظر بگیریم ، داریم $\pi(a) = \bar{a}$، برای هر $a \in R$. اکنون تابع $\varphi : M_n(R) \longrightarrow M_n(R/I)$ را با $\varphi([a_{ij}]) = [\overline{a_{ij}}]$ تعریف می‌کنیم. فرض کنید $[a_{ij}], [b_{ij}] \in M_n(R)$، داریم

$$\begin{aligned}
\varphi([a_{ij}] + [b_{ij}]) &= \varphi([a_{ij} + b_{ij}]) \\
&= [\overline{a_{ij} + b_{ij}}] \\
&= [\overline{a_{ij}} + \overline{b_{ij}}] \\
&= [\overline{a_{ij}}] + [\overline{b_{ij}}] \\
&= \varphi([a_{ij}]) + \varphi([b_{ij}])
\end{aligned}$$

و

$$\begin{aligned}
\varphi\left([a_{ij}][b_{ij}]\right) &= \varphi\left(\left[\sum_{k=1}^{n} a_{ik}b_{k_j}\right]\right) \\
&= \left[\overline{\sum_{k=1}^{n} a_{ik}b_{k_j}}\right] \\
&= \left[\sum_{k=1}^{n} \overline{a_{ik}}\ \overline{b_{k_j}}\right] \\
&= [\overline{a_{ij}}][\overline{b_{ij}}] \\
&= \varphi([a_{ij}])\varphi([b_{ij}]).
\end{aligned}$$

در نتیجه φ همریختی حلقه‌ای است. به وضوح φ پوشاست. هم‌چنین $\ker\varphi = M_n(I)$، زیرا $[a_{ij}] \in \ker\varphi$ اگر و تنها اگر $a_{ij} \in I$، به ازای هر i، j. در نتیجه حکم از قضیه‌ی اول یکریختی به دست می‌آید. □

در ادامه این بخش حاصل‌ضرب حلقه‌ها را بررسی می‌کنیم. برای استقلال این بحث از فصل ۴، همه‌ی مفاهیم مورد نیاز را می‌آوریم. فرض کنید I یک مجموعه‌ی اندیس و $\{R_i\}_{i\in I}$ خانواده‌ای از حلقه‌ها باشد. یادآوری می‌کنیم حاصل‌ضرب دکارتی $\prod_{i\in I} R_i$ عبارت است از مجموعه‌ی همه‌ی دنباله‌های $(r_i)_{i\in I}$ که در آن $r_i \in R_i$ به ازای هر i:

$$\prod_{i\in I} R_i = \{(r_i)_{i\in I} \mid r_i \in R_i, \quad \forall i \in I\}.$$

$\prod_{i\in I} R_i$ تحت عمل جمع و ضرب مولفه‌ای

$$(r_i)_{i\in I} + (s_i)_{i\in I} = (r_i + s_i)_{i\in I}$$
$$(r_i)_{i\in I}(s_i)_{i\in I} = (r_i s_i)_{i\in I}$$

یک حلقه است، عضو بی‌اثر آن دنباله‌ی $(c_i)_{i\in I}$ است که به ازای هر $i \in I$، $c_i = 0$. قرینه‌ی دنباله‌ی $(r_i)_{i\in I}$ عبارت است از $(-r_i)_{i\in I}$. گاهی اوقات این حلقه را با $\mathrm{Cr}_{i\in I}R_i$ نشان می‌دهیم. فرض کنید $u = (r_i)_{i\in I}$ دنباله‌ی دلخواهی در $\prod_{i\in I} R_i$ باشد. تکیه‌گاه u را که با $\mathrm{supp}(u)$ نشان می‌دهیم عبارت است از

$$\mathrm{supp}(u) = \{j \in I \mid r_j \neq 0\}.$$

قضیه‌ی زیر را می‌توان به سادگی اثبات کرد.

قضیه ۱۶.۴.۱۰. اگر $u = (r_i)_{i\in I}$ و $v = (s_i)_{i\in I}$ دنباله‌های دل‌خواهی در $\prod_{i\in I} R_i$ باشند، آن‌گاه
(الف) $\mathrm{supp}(u) = \mathrm{supp}(-u)$.
(ب) $\mathrm{supp}(u+v) \subseteq \mathrm{supp}(u) \cup \mathrm{supp}(v)$.
(ج) $\mathrm{supp}(uv) \subseteq \mathrm{supp}(u) \cap \mathrm{supp}(v)$. □

مجموعه‌ی همه‌ی دنباله‌های در $\prod_{i\in I} R_i$ با تکیه‌گاه متناهی را با $\oplus_{i\in I}R_i$ یا $\mathrm{Dr}_{i\in I}R_i$ نشان می‌دهیم:

$$\oplus_{i\in I}R_i = \{(r_i)_{i\in I} \in \mathrm{Cr}_{i\in I}R_i \mid |\mathrm{supp}((r_i)_{i\in I})| < \infty\}.$$

قضیه‌ی فوق نشان می‌دهد که $\oplus_{i\in I}R_i$ یک ایدآل $\prod_{i\in I} R_i$ است. $\oplus_{i\in I}R_i$ را حاصل‌ضرب مستقیم (خارجی) خانواده‌ی $\{R_i\}_{i\in I}$ گوییم. در حالتی که $I = \{1, 2, \ldots, n\}$، $\prod_{i\in I} R_i$ و $\oplus_{i\in I}R_i$ با هم مساوی هستند که آن‌ها را با $R_1 \oplus \cdots \oplus R_n$ یا $\oplus_{i=1}^n R_i$ نشان می‌دهیم.
به ازای هر $j \in I$، تابع $\iota_j : R_j \to \oplus_{i\in I}R_i$ با ضابطه‌ی $\iota_j(a) = (r_i)_{i\in I}$، که در آن a در jامین مولفه و هر مولفه‌ی دیگر صفر است، یعنی $r_i = \begin{cases} 0 & i \neq j \\ a & i = j \end{cases}$، یک همریختی یک‌به‌یک است. ι_j را جادهی مولفه‌ی jام گوییم. چون ι_j یک‌به‌یک است $\iota_j(R_j)$ زیرحلقه‌ای از $\oplus_{i\in I}R_i$ و یکریخت با R_j است:

$$R_j \cong \iota_j(R_j) = \{(r_i)_{i\in I} \in \oplus_{i\in I}R_i \mid r_i = 0, \quad \forall i \neq j\}.$$

توجه کنید $\iota_j(R_j)$ در واقع یک ایدآل $\oplus_{i\in I}R_i$ است.
در حالتی که $I = \{1, 2, \ldots, n\}$، داریم

$$R_j \cong \iota_j(R_j) = \{0\} \oplus \cdots \oplus \{0\} \oplus R_j \oplus \{0\} \oplus \cdots \oplus \{0\}.$$

هر عضو $\oplus_{i\in I}R_i$ به صورت یکتا بر حسب اعضای $\iota_j(R_j)$، $j\in I$، نوشته می‌شود. زیرا فرض کنید $(r_i)_{i\in I}\oplus_{i\in I}R_i$. در این صورت $j_1,\dots,j_n\in I$ وجود دارد که اگر $i\notin\{j_1,\dots,j_n\}$، آن‌گاه $r_i=0$. فرض کنید u_{j_k} دنباله‌های باشد که مولفه‌ی j_kام آن برابر r_{j_k} و هر مولفه‌ی دیگر برابر ۰ است، یعنی $u_{j_k}=(s_i)_{i\in I}$ و $s_i=\begin{cases}0 & i\neq j_k\\ r_{j_k} & i=j_k\end{cases}$. پس داریم

$$(r_i)_{i\in I}=u_{j_1}+u_{j_2}+\cdots+u_{j_n}$$

و به وضوح این نحوه نوشتن $(r_i)_{i\in I}$ بر حسب اعضای $\iota_j(R_j)$، $i\in I$ یکتاست.
به ازای هر $j\in I$ تابع $\pi_j:\oplus_{i\in I}R_i\to R_j$ با ضابطه‌ی $\pi_j((r_j)_{i\in I})=r_j$ یک همریختی پوشا است که آن را همریختی تصویر روی مولفه‌ی jام گوییم. توجه کنید که داریم

$$\ker\pi_j=\{(r_i)_{i\in I}\in\oplus_{i\in I}R_i\mid r_j=0\}.$$

حال فرض کنید R حلقه‌ای دلخواه باشد و $\{S_i\}_{i\in I}$ خانواده‌ای از ایدآل‌های R، طوری که هر عضو $0\neq r\in R$ به صورت یکتای $r=r_{j_1}+r_{j_2}+\cdots+r_{j_n}$ نوشته شود، که در آن $0\neq r_{j_k}\in S_{j_k}$، $k=1,\dots,n$.
در این حالت گوییم R حاصل‌جمع مستقیم (داخلی) خانواده $\{S_i\}_{i\in I}$ است. به سادگی می‌توان ثابت کرد:

قضیه ۱۰.۴.۱۷. اگر $\{S_i\}_{i\in I}$ خانواده‌ای از ایدآل‌های R باشند، آن‌گاه R حاصل‌جمع مستقیم $\{S_i\}_{i\in I}$ است اگر و تنها اگر
(الف) $R=\left(\bigcup_{i\in I}S_i\right)$.
(ب) به ازای هر $j\in I$، $S_j\cap\left(\bigcup_{\substack{i\in I\\ i\neq j}}S_j\right)=\{0\}$.

اثبات. ($\Longleftarrow$) فرض کنید $R=\oplus_{i\in I}S_i$. طبق تعریف حاصل‌جمع مستقیم داخلی، هر عضو $a\in R$ به صورت (یکتای) $a=r_{j_1}+\cdots+r_{j_n}$، که در آن $r_{j_k}\in S_{j_k}$، نوشته می‌شود، پس $R=\left(\bigcup_{i\in I}S_i\right)$. حال فرض کنید $a\in S_j\cap\left(\bigcup_{\substack{i\in I\\ i\neq j}}S_j\right)$. بنابراین $a=r_{j_1}+\cdots+r_{j_k}$، که در آن $r_{j_k}\in S_{j_k}$ و $j_k\neq j$. در نتیجه داریم $0=-a+r_{j_1}+\cdots+r_{j_k}$ و بنا به یکتایی تجزیه‌ی ۰ به صورت حاصل‌جمع اعضای $\{S_i\}_{i\in I}$، داریم $a=r_{j_1}=\cdots=r_{j_k}=0$. پس $S_j\cap\left(\bigcup_{\substack{i\in I\\ i=j}}S_j\right)=\{0\}$.
($\Longrightarrow$) فرض کنید $0\neq a\in R$. بنا به (الف) اعضای $0\neq r_{j_k}\in S_{j_k}$، $k=1,\dots,n$ وجود دارند که $a=r_{j_1}+\cdots+r_{j_n}$. باید ثابت کنیم این تجزیه یکتاست. فرض کنید $a=b_{i_1}+b_{i_2}+\cdots+b_{i_m}$، که در آن $b_{i_k}\in S_{i_k}$، $k=1,\dots,m$. به سادگی و به استقرا روی $\max\{m,n\}$ با استفاده از (ب) می‌توان ثابت کرد $m=n$ و پس از تعویض اندیس‌ها $b_{i_k}=r_{i_k}$. جزئیات کار را به خواننده واگذار می‌کنیم. □

فرض کنید حلقه‌ی R حاصل‌جمع مستقیم خانواده‌ی ایدآل‌های $\{S_i\}_{i\in I}$ باشد. چون به ازای هر $j\in I$، $S_j\cap\left(\bigcup_{\substack{i\in I\\ i\neq j}}S_j\right)=\{0\}$، به ویژه به ازای هر $i\neq j$ داریم $S_i\cap S_j=\{0\}$. با توجه به این نکته و این که S_jها ایدآل R هستند ، به سادگی می‌توان دید تابع $\varphi:\oplus_{i\in I}S_i\to R$ با ضابطه‌ی $\varphi((r_i)_{i\in I})=r_{j_1}+\ldots+r_{j_n}$، که در آن برای هر $i\notin\{j_1,\dots,j_n\}$، $r_i=0$، عمل ضرب را حفظ می‌کند. به علاوه به سادگی می‌توان دید φ یکریختی حلقه‌ای است، بنابراین $R\cong\oplus_{i\in I}S_i$. هرگاه R حاصل‌جمع مستقیم داخلی $\{S_i\}_{i\in I}$ باشد، می‌نویسیم $R=\oplus_{i\in I}S_i$. توجه کنید که اگر R حاصل‌جمع مستقیم داخلی $\{S_i\}_{i\in I}$ باشد، آن‌گاه S_iها ایدآل‌هایی از R هستند ، اما حاصل‌جمع مستقیم خارجی $\oplus_{i\in I}S_i$ شامل هیچ‌کدام از S_jها نیست، بلکه که به ازای هر j، شامل یک کپی یکریخت با S_j، یعنی $\iota_j(S_j)$ است.

تمرین‌ها

۱. فرض کنید $f:R\longrightarrow S$ همریختی حلقه‌ای و I یک ایدآل R و J یک ایدآل S باشند. ثابت کنید
(الف) $f^{-1}(J)$ یک ایدآل R شامل $\ker f$ است.
(ب) اگر f پوشا باشد $f(I)$ ایدآل S است.
(ج) با ارائه‌ی مثالی نشان دهید شرط پوشا بودن در (ب) لازم است.

۲. فرض کنید R حلقه‌ای یکدار باشد و $A = [a_{ij}] \in M_n(R)$. هرگاه E_{ij} ماتریسی باشد که درایه‌های (i,j) آن برابر ۱ و سایر درایه‌ها صفر باشد، تحقیق کنید:
(الف) سطر iام ماتریس $E_{ij}A$ برابر سطر jام A و سایر سطرهای آن صفر است.
(ب) ستون jام ماتریس AE_{ij} برابر ستون iام A و سایر ستون‌های آن صفر است.
(ج) درایه‌ی (p,j) ماتریس $E_{pq}AE_{ij}$ برابر a_{qi} و سایر درایه‌های آن برابر صفر هستند ، یعنی $E_{pq}AE_{ij} = a_{qi}E_{pj}$.

۳. فرض کنید R حلقه‌ی یکدار باشد. نشان دهید R ایدآل چپ نابدیهی ندارد اگر و تنها اگر ایدآل راست نابدیهی نداشته باشد.

۴. فرض کنید R حلقه‌ای یکدار باشد. اگر I_n ماتریس همانی باشد نشان دهید $\mathrm{Cent}(M_n(R)) = \{aI_n \mid a \in \mathrm{Cent}(R)\}$.

۵. فرض کنید R حلقه‌ی یکدار باشد. نشان دهید هر ایدآل دوطرفی $M_n(R)$ به صورت $M_n(J)$ است که در آن J یک ایدآل R است.

۶. اگر R حلقه‌ی تقسیم باشد نشان دهید $M_n(R)$ حلقه‌ی ساده است (یعنی ایدآل نابدیهی ندارد).

۷. فرض کنید R حلقه‌ی یکدار و L_j مجموعه‌ی همه‌ی ماتریس‌های در $M_n(R)$ باشد که ستون jام آن‌ها عناصر دلخواهی از R و سایر ستون‌های آن‌ها صفرند. نشان دهید L_j ایدآل چپ $M_n(R)$ است و به ازای هر i، $L_j = M_n(R)E_{ij}$.

۸. فرض کنید R حلقه‌ای بدون مقسوم‌علیه صفر باشد، و هر زیرحلقه‌ی R یک ایدآل از R باشد. ثابت کنید R تعویض‌پذیر است. مثالی از چنین حلقه‌ای ارائه کنید.

۹. فرض کنید $N(R)$ مجموعه‌ی عناصر پوچ‌توان حلقه‌ی تعویض‌پذیر R باشد. نشان دهید $N(R)$ یک ایدآل R است و $R/N(R)$ عضو پوچ‌توان ندارد.

۱۰. (الف) نشان دهید اجتماع دو ایدآل، لزوماً ایدآل نیست.
(ب) اگر $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$ زنجیری از ایدآل‌های حلقه‌ی R باشد، ثابت کنید $\bigcup_{k=1}^{\infty} I_k$ ایدآلی از R است.

۱۱. نشان دهید تنها یک همریختی حلقه‌ای ناصفر از $\mathbb{R}$ به $\mathbb{C}$ وجود دارد.

۱۲. اگر $\varphi : \mathbb{R} \longrightarrow \mathbb{R}$ خودریختی باشد، نشان دهید φ همانی است.

۱۳. نشان دهید تنها دو همریختی حلقه‌ای از $\mathbb{R}$ به $\mathbb{R}$ وجود دارد.

۱۴. نشان دهید هر زیرگروه جمعی حلقه‌ی یکدار R ایدآل R است اگر و تنها اگر $R \cong \mathbb{Z}$ یا به ازای یک $n \geq 1$، $R \cong \mathbb{Z}_n$.

۱۵. فرض کنید R حلقه‌ی یکدار و گروه جمعی $(R,+)$ دوری باشد. نشان دهید $R \cong \mathbb{Z}$ یا به ازای یک $n \geq 1$، $R \cong \mathbb{Z}_n$.

۱۶. (قضیه‌ی باقیمانده چینی) فرض کنید I و J ایدآل‌هایی از حلقه‌ی یکدار R باشند. اگر $I + J = R$، نشان دهید $\dfrac{R}{I \cap J} \cong \dfrac{R}{I} \times \dfrac{R}{J}$.

۱۷. فرض کنید F میدان باشد. نشان دهید ایدآل‌های نابدیهی حلقه‌ی $R = \begin{bmatrix} F & F \\ 0 & F \end{bmatrix}$ عبارت‌اند از $\begin{bmatrix} F & F \\ 0 & 0 \end{bmatrix}$، $\begin{bmatrix} F & 0 \\ 0 & F \end{bmatrix}$. همه‌ی تصاویر همریختی R را بیابید.

۱۸. فرض کنید R حلقه‌ای تعویض‌پذیر و یکدار و ناشمارا باشد طوری که به ازای هر ایدآل $I \neq \{0\}$ حلقه‌ی خارج‌قسمتی R/I شمارا باشد. ثابت کنید R دامنه‌ی صحیح است.

۱۹. فرض کنید حلقه‌ی R دقیقاً دو ایدآل (دو طرفی) داشته باشد. اگر $u \in R$ وجود داشته باشد که به ازای هر $x \in R$، $ux = x$، نشان دهید R یکدار است و $u = 1_R$.

۲۰. فرض کنید R یک حلقه‌ی تعویض‌پذیر و بدون مقسوم‌علیه صفر باشد. نشان دهید R با زیرحلقه‌ای از یک دامنه‌ی صحیح یکریخت است.

۲۱. فرض کنید F یک میدان نامتناهی و زیرحلقه‌ای از حلقه‌ی R باشد. اگر A، A_1، ...، A_n ایدآل‌هایی از R باشند که $A \subseteq \bigcup_{i=1}^{n} A_i$، نشان دهید $1 \leq j \leq n$ وجود دارد که $A \subseteq A_j$.

۲۲. فرض کنید R حلقه‌ای باشد که به ازای هر $a \in R$ عدد صحیح $n > 1$ وجود داشته باشد $a^n = a$. نشان دهید هر ایدآل راست

(چپ) R یک ایدآل دوطرفی است.

۲۳. حلقه‌ی یکدار R را حلقه‌ی موضعی گوییم، هرگاه مجموعه‌ی $J(R)$ متشکل از نایکه‌های R یک ایدآل باشد.
(الف) نشان دهید هر حلقه‌ی تقسیم R، موضعی است. $J(R)$ را توصیف کنید.
(ب) نشان دهید اگر R موضعی باشد، آنگاه $R/J(R)$ حلقه‌ی تقسیم است.
(ج) فرض کنید R موضعی باشد. اگر $I \subseteq J(R)$ ایدآلی از R باشد، نشان دهید R/I حلقه‌ی موضعی است و $J(R/I) = \{r + I \mid r \in J(R)\}$.
(هـ) نشان دهید $\mathbb{Z}_{p^n}$ (p عدد اول)، موضعی است و $J(\mathbb{Z}_{p^n})$ را توصیف کنید.
(و) نشان دهید اگر R موضعی باشد، هیچ ایدآل سره R شامل $J(R)$ وجود ندارد.

۲۴. فرض کنید $\mathbb{Z}_{(p)} = \left\{ \frac{m}{n} \;\middle|\; m \in \mathbb{Z},\ n \in \mathbb{N},\ p \not| n \right\}$ (p عدد اول)، نشان دهید
(الف) $\mathbb{Z}_{(p)}$ دامنه‌ی صحیح است.
(ب) $J(\mathbb{Z}_{(p)}) = \left\{ \frac{m}{n} \in \mathbb{Z}_{(p)} \;\middle|\; p|m \right\}$ و $\mathbb{Z}_{(p)}$ حلقه‌ی موضعی است، به علاوه $\mathbb{Z}_{(p)}/J(\mathbb{Z}_{(p)}) \cong \mathbb{Z}_p$.
(ج) اگر $I \neq \{0\}$ ایدآلی از $\mathbb{Z}_{(p)}$ باشد، آنگاه $I = (p^k)$، که در آن $k \geq 0$ کوچک‌ترین عدد صحیح است که $p^k \in I$.

۵.۱۰ میدان کسرهای یک دامنه‌ی صحیح

در این بخش نشان می‌دهیم هر دامنه‌ی صحیح با زیرحلقه‌ای از یک میدان یکریخت است. ایده‌ی ما از دامنه‌ی صحیح $\mathbb{Z}$ و میدان $\mathbb{Q}$ ناشی می‌شود. هر عضو $\mathbb{Q}$ به صورت $\frac{a}{b}$ است، که در آن $a, b \in \mathbb{Z}$ و $b \neq 0$. یک عضو $\mathbb{Q}$ را کسر می‌نامیم. دو کسر $\frac{a}{b}$ و $\frac{c}{d}$ وقتی و فقط وقتی مساوی‌اند که $ad = bc$. بنابراین از این ایده می‌توان استفاده کرد و به طور کلی در یک دامنه‌ی صحیح عمل کرد. فرض کنید R دامنه‌ی صحیح دلخواهی باشد. رابطه‌ی $\sim$ را روی

$$X = R \times (R - \{0\}) = \{(a, b) \mid a, b \in R,\ \ b \neq 0\}$$

به صورت زیر تعریف می‌کنیم

$$(a, b) \sim (c, d) \iff ad = bc.$$

چون $ab = ba$، $(a, b) \sim (a, b)$، یعنی $\sim$ بازتابی است. اگر $(a, b) \sim (c, d)$، آنگاه $ad = bc$. چون R تعویض‌پذیر است، $cb = ba$. پس $(c, d) \sim (a, b)$ و $\sim$ متقارن است. حال اگر $(a, b) \sim (c, d)$ و $(c, d) \sim (r, s)$، آنگاه $ad = bc$ و $cs = dr$. چون R تعویض‌پذیر است داریم

$$asd = (ad)s = (bc)s = b(cs) = b(dr) = bdr.$$

چون $d \neq 0$ و R دامنه‌ی صحیح است با حذف d از طرفین تساوی فوق به دست می‌آوریم $as = br$ بنابراین $(a, b) \sim (r, s)$. در نتیجه $\sim$ ترایا است.
از این‌رو $\sim$ رابطه‌ی هم‌ارزی روی X است. رده‌ی هم‌ارزی شامل (a, b) را با $\frac{a}{b}$ نشان می‌دهیم:

$$\begin{aligned} \frac{a}{b} &= \{(c, d) \mid c, d \in R,\ \ d \neq 0,\ \ (a, b) \sim (c, d)\} \\ &= \{(c, d) \mid c, d \in R,\ \ d \neq 0,\ \ ad = bc\} \end{aligned}$$

و داریم

$$\frac{a}{b} = \frac{c}{d} \iff (a, b) \sim (c, d) \iff ad = bc.$$

مجموعه‌ی همه‌ی رده‌های هم‌ارزی را با $Q(R)$ نشان می‌دهیم:

$$Q(R) = \left\{ \frac{a}{b} \;\middle|\; a, b \in R,\ \ b \neq 0 \right\}.$$

جمع و ضرب در $Q(R)$ را به صورت زیر تعریف می‌کنیم:

$$\frac{a}{b}+\frac{c}{d}=\frac{ad+bc}{bd},\quad \frac{a}{b}\frac{c}{d}=\frac{ac}{bd}.$$

نشان می‌دهیم جمع و ضرب خوش تعریف است. فرض کنید $\frac{a}{b}=\frac{a'}{b'}$ و $\frac{c}{d}=\frac{c'}{d'}$. پس $ab'=ba'$ و $cd'=dc'$. باید نشان دهیم $\frac{ad+bc}{bd}=\frac{a'd'+b'c'}{b'd'}$، یعنی باید نشان دهیم $(ad+bc)b'd'=(a'd'+b'c')bd$. داریم

$$\begin{aligned}(ad+bc)b'd' &= adb'd'+bcb'd'\\ &= (ab')dd'+(cd')bb'\\ &= (ba')dd'+(dc')bb'\\ &= a'd'bd+b'c'bd\\ &= (a'd'+b'c')bd.\end{aligned}$$

پس خوش‌تعریفی جمع ثابت شد. به همین نحو می‌توان خوش‌تعریفی ضرب را ثابت کرد. حال می‌توان نشان داد $Q(R)$ میدان است. مثلاً برای اثبات شرکت‌پذیری جمع محاسبه می‌کنیم:

$$\begin{aligned}\frac{a}{b}+\left(\frac{c}{d}+\frac{r}{s}\right) &= \frac{a}{b}+\frac{cs+rd}{ds}\\ &= \frac{a(ds)+(cs+rd)b}{b(ds)}\\ &= \frac{(ad+bc)s+r(bd)}{(bd)s}\\ &= \frac{ad+bc}{bd}+\frac{r}{s}\\ &= \left(\frac{a}{b}+\frac{c}{d}\right)+\frac{r}{s}.\end{aligned}$$

با انجام محاسبات مشابه می‌توان نشان داد $Q(R)$ یک حلقه‌ی تعویض‌پذیر است. اگر $a\neq 0$ عضوی از R باشد، آنگاه عضو صفر در $Q(R)$ عبارت است از $\frac{0}{a}=\frac{0}{1}$. قرینه‌ی $\frac{a}{b}$ عبارت است از $\frac{-a}{b}$. عضو همانی R، عبارت است از $\frac{1}{1}=\frac{a}{a}$، اگر $\frac{a}{b}$ عضوی ناصفر در $Q(R)$ باشد، آنگاه $a\neq 0$. بنابراین $\frac{a}{b}\in Q(R)$ و $\frac{a}{b}\frac{b}{a}=\frac{ab}{ba}=1$، یعنی $\frac{b}{a}=\left(\frac{a}{b}\right)^{-1}$. بنابراین $Q(R)$ میدان است.

حال تابع $\varphi : R\longrightarrow Q(R)$ را با ضابطه‌ی $\varphi(a)=\frac{a}{1}$، به ازای هر $a\in R$، تعریف می‌کنیم. φ همریختی حلقه‌ای است، زیرا برای هر $a,b\in R$ داریم

$$\begin{aligned}\varphi(a+b)&=\frac{a+b}{1}=\frac{a}{1}+\frac{b}{1}=\varphi(a)+\varphi(b)\\ \varphi(ab)&=\frac{ab}{1}=\frac{a}{1}\frac{b}{1}=\varphi(a)\varphi(b).\end{aligned}$$

φ یک‌به‌یک است، زیرا اگر $\varphi(a)=\varphi(b)$، آنگاه $\frac{a}{1}=\frac{b}{1}$ و $a=b$. از این‌رو

$$R\cong \operatorname{Im}\varphi=\{\varphi(a)\mid a\in R\}=\left\{\frac{a}{1}\;\middle|\; a\in R\right\}.$$

پس R با زیرحلقه‌ی $\left\{\frac{a}{1}\mid a\in R\right\}$ از $Q(R)$ یکریخت است. معمولاً R را با تصویر آن در $Q(R)$ یکی می‌گیریم و قرار می‌دهیم $a=\frac{a}{1}$، بنابراین R را به عنوان زیرحلقه‌ای از $Q(R)$ در نظر می‌گیریم. $Q(R)$ را میدان کسرهای R گوییم. اگر $\frac{a}{1}$ را با a یکی در نظر بگیریم، آنگاه $\frac{a}{b}=\frac{a}{1}\frac{1}{b}=ab^{-1}$. پس $Q(R)=\{ab^{-1}\mid a,b\in R,\ \ b\neq 0\}$.

تمرین‌ها

۱. فرض کنید R دامنه‌ی صحیح و Q میدان کسرهای آن باشد. نشان دهید Q کوچک‌ترین میدان شامل R است یعنی اگر F میدان باشد و $R \subseteq F$، آنگاه زیر میدان K از F وجود دارد که $R \subseteq K$ و $K \cong Q$.

۲. فرض کنید $m \in \mathbb{Z}$ مربع کامل نباشد. نشان دهید $\mathbb{Z}[\sqrt{m}]$ دامنه‌ی صحیح است و میدان کسرهای آن را در حالت $m > ۰$ و $m < ۰$ توصیف کنید.

۳. فرض کنید Q میدان کسرهای دامنه‌ی صحیح R باشد و $\alpha \in \operatorname{Aut} R$. نشان دهید خودریختی یکتای $\bar{\alpha} \in \operatorname{Aut} Q$ وجود دارد که به ازای هر $r \in R$، $\bar{\alpha}(r) = \alpha(r)$.

۴. فرض کنید R یک حلقه باشد. $S \subseteq R$ را مجموعه‌ی بسته‌ی ضربی گوییم، نسبت به ضرب بسته باشد، یعنی اگر $a, b \in S$، آنگاه $ab \in S$. فرض کنید S یک زیر مجموعه‌ی بسته‌ی ضربی حلقه‌ی تعویض‌پذیر R باشد.
(الف) نشان دهید رابطه‌ی $\sim$ روی $R \times S$ که به صورت زیر تعریف می‌شود یک رابطه‌ی هم‌ارزی است:

$$(a, s) \sim (b, t) \iff \exists u \in S, \quad u(ta - sb) = ۰.$$

(ب) اگر $\frac{a}{s}$ رده‌ی هم‌ارزی شامل $(a, s) \in R \times S$ باشد، نشان دهید مجموعه‌ی همه‌ی رده‌های هم‌ارزی تحت اعمال

$$\frac{a}{s} + \frac{b}{t} = \frac{at + sb}{st}, \quad \frac{a}{s}\frac{b}{t} = \frac{ab}{st}$$

یک حلقه‌ی تعویض‌پذیر است. این حلقه را حلقه‌ی کسرهای R نسبت به S می‌نامیم و با $S^{-۱}R$ یا R_S نشان می‌دهیم.
(ج) اگر $S \ni ۰$، نشان دهید $S^{-۱}R$ تنها یک عضو دارد و اگر $S = R - \{۰\}$ و R دامنه‌ی صحیح باشد، آنگاه $S^{-۱}R$ میدان کسرهای R است.

۵. فرض کنید R حلقه‌ی تعویض‌پذیر و یکدار باشد. عضو $s \in R$ را نامقسوم علیه صفر گوییم، هرگاه از $as = ۰$ نتیجه شود $a = ۰$. فرض کنید $S \subseteq R$ مجموعه‌ای از نامقسوم‌های صفر باشد و $۱ \in S$. نشان دهید S مجموعه‌ی بسته‌ی ضربی است و $S^{-۱}R$ را توصیف کنید.

۶.۱۰ تولید ایدآل‌ها

در این بخش مطالبی در مورد تولید ایدآل‌ها مطرح می‌کنیم. متناظر با هر زیرمجموعه‌ی ناتهی از یک حلقه می‌توان ایدآل‌های چپ، راست یا دوطرفی تعریف کرد:

قضیه ۱.۶.۱۰. فرض کنید X زیرمجموعه‌ی ناتهی از حلقه‌ی R باشد. در این صورت
(الف) $RX = \{\sum_{i=۱}^{n} r_i x_i \mid n \in \mathbb{N},\ r_i \in R,\ x_i \in X\}$ یک ایدآل چپ R است.
(ب) $XR = \{\sum_{i=۱}^{n} x_i r_i \mid n \in \mathbb{N},\ r_i \in R,\ x_i \in X\}$ یک ایدآل راست R است.
(ج) $RXR = \{\sum_{i=۱}^{n} r_i x_i s_i \mid n \in \mathbb{N},\ r_i,\ s_i \in R,\ x_i \in X\}$ یک ایدآل دوطرفی R است.

اثبات. اثبات قضیه بسیار ساده است. به عنوان مثال (الف) را ثابت و قسمت‌های (ب) و (ج) را به عنوان تمرین واگذار می‌کنیم. چون $X \neq \emptyset$، $x \in X$ وجود دارد. پس $۰x = ۰ \in RX$ و $RX \neq \emptyset$. حال فرض کنید $a = \sum_{i=۱}^{n} r_i x_i \in RX$، $b = \sum_{i=۱}^{m} s_i y_i \in RX$ و $r \in R$، که در آن $y_i, x_i \in X$، $r_i, s_i \in R$، و $m, n \in \mathbb{N}$. داریم

$$a - b = \sum_{i=۱}^{n} r_i x_i - \sum_{i=۱}^{m} s_i y_i = \sum_{i=۱}^{m+n} r_i x_i \in RX,$$

که در آن $x_{n+i} = y_i$ و $r_{n+i} = -s_i$، $i = ۱, ۲, \ldots, m$. پس RX زیرگروه جمعی R است. هم‌چنین داریم

$$ra = r\sum_{i=۱}^{n} r_i x_i = \sum_{i=۱}^{n} (rr_i) x_i \in RX.$$

در نتیجه RX ایدآل چپ R است. □

اگر X زیرمجموعه‌ی ناتهی از حلقه‌ی R باشد و R یکدار باشد، آنگاه برای هر $x \in X$ داریم $x = 1x \in RX$. پس $X \subseteq RX$. بنابراین در حالتی که R یکدار باشد RX یک ایدآل چپ شامل X است. به همین نحو اگر R یکدار باشد XR و RXR ایدآل‌های راست و دوطرفی شامل X هستند. اما اگر R یکدار نباشد لزومی ندارد که RX شامل X باشد. می‌خواهیم ایدآل چپی را بیابیم که شامل X است. اگر I ایدآل چپ از R باشد که شامل X است، آنگاه برای هر $x_1, \ldots, x_k \in X$ داریم $x_1, \ldots, x_k \in I$. پس برای هر $n_1, \ldots, n_k \in \mathbb{Z}$، $\sum_{i=1}^{k} n_i x_i \in I$. با این ایده تعریف می‌کنیم:

$$\mathbb{Z}X = \left\{ \sum_{i=1}^{k} n_i x_i \;\middle|\; k \in \mathbb{N},\ \ n_i \in \mathbb{Z},\ \ x_i \in X \right\}.$$

اکنون برای هر زیرمجموعه‌ی ناتهی X از یک حلقه ایدآل‌های چپ، راست ، و یا دوطرفی شامل X را به دست می‌آوریم:

قضیه ۲.۶.۱۰. اگر X زیرمجموعه‌ی ناتهی از حلقه‌ی R باشد، آنگاه
(الف) $RX + \mathbb{Z}X$ ایدآل چپ R شامل X است.
(ب) $XR + \mathbb{Z}X$ ایدآل راست R شامل X است.
(ج) $XR + RX + RXR + \mathbb{Z}X$ ایدآل دوطرفی R شامل X است.

اثبات. اثبات قضیه ساده است. (الف) را ثابت می‌کنیم و اثبات سایر قسمت‌ها را به عنوان تمرین واگذار می‌کنیم. فرض کنید $a = \sum_{i=1}^{k} n_i x_i \in \mathbb{Z}X$، $b = \sum_{i=1}^{t} m_i y_i$، که در آن $x_i, y_i \in X$، $m_i, n_i \in \mathbb{Z}$، و $k, t \in \mathbb{N}$. داریم

$$a - b = \sum_{i=1}^{k} n_i x_i - \sum_{i=1}^{t} m_i y_i = \sum_{i=1}^{k+t} n_i x_i \in \mathbb{Z}X$$

که در آن $n_{i+k} = -m_i$، و $x_{k+i} = y_i$، $i = 1, 2, \ldots, t$.
حال اگر $r \in R$ داریم

$$ra = r \sum_{i=1}^{k} n_i x_i = \sum_{i=1}^{k} r(n_i x_i) = \sum_{i=1}^{k} (n_i r) x_i \in RX.$$

پس بنا به قضیه‌ی ۱.۶.۱۰، $RX + \mathbb{Z}X$ ایدآل چپ R است. برای هر $x \in X$ چون $x = 1x \in \mathbb{Z}X$، $x \in RX + \mathbb{Z}X$. پس $RX + \mathbb{Z}X$ ایدآل چپ R شامل X است. □

فرض کنید X زیرمجموعه‌ی ناتهی R باشد. اگر I یک ایدآل چپ شامل X باشد، آنگاه به ازای هر $x_1, \ldots, x_k \in X$ و به ازای هر $r_1, \ldots, r_k \in R$، داریم $\sum_{i=1}^{k} r_i x_i \in I$. بنابراین هر عضو RX در I قرار دارد و $RX \subseteq I$. هم‌چنین برای هر $n_1, \ldots, n_k \in \mathbb{Z}$ داریم $\sum_{i=1}^{k} n_i x_i \in I$. پس هر عضو $\mathbb{Z}X$ نیز در I قرار دارد و $\mathbb{Z}X \subseteq I$. در نتیجه $RX + \mathbb{Z}X \subseteq I$. بنابراین $RX + \mathbb{Z}X$ کوچک‌ترین ایدآل چپ R شامل X است.
فرض کنید X زیرمجموعه‌ی از حلقه‌ی R باشد. ایدآل چپ تولید شده توسط X که آن را با $(X)_\ell$ نشان می‌دهیم عبارت است از کوچک‌ترین ایدآل چپ R شامل X، یعنی

$$(X)_\ell = \bigcap \{I \mid X \subseteq I,\ \ R \text{ ایدآل چپ } I\}.$$

به همین نحو ایدآل راست تولید شده توسط X، $(X)_r$، و ایدآل تولید شده توسط X، (X)، را تعریف می‌کنیم:

$$(X)_r = \bigcap \{I \mid X \subseteq I,\ \ R \text{ ایدآل راست } I\}$$

$$(X) = \bigcap \{I \mid X \subseteq I,\ \ R \text{ ایدآل } I\}.$$

واضح است که اگر $X = \emptyset$، آنگاه $(\emptyset) = (\emptyset)_\ell = (\emptyset)_r = \{0\}$. اگر $X \neq \emptyset$ قضیه‌ی ۲.۶.۱۰، و بحث بالا نشان می‌دهد که $(X)_\ell = RX + \mathbb{Z}X$ و به همین صورت $(X)_r = XR + \mathbb{Z}X$. در حالتی که R یکدار باشد $(X)_\ell = RX$، $(X)_r = XR$ و $(X) = XR + RX + RXR$. اگر $X = \{x_1, \ldots, x_k\}$،
ایدآل چپ تولید شده توسط X را با $(x_1, \ldots, x_k)_\ell$ نشان می‌دهیم. در این حالت $(X)_\ell$ را ایدآل چپ با تولید متناهی می‌نامیم. به همین نحو $(x_1, \ldots, x_k)_r$ و $(x_1, \ldots, x_k)$ را ، به ترتیب، ایدآل‌های راست و دوطرفی متناهیاً تولید شده می‌نامیم. اگر $X = \{x\}$، آنگاه $(x)_\ell$ را ایدآل اصلی چپ تولید شده توسط x می‌نامیم، $(x)_r$ را ایدآل اصلی راست تولید شده توسط x و (x) را ایدآل اصلی تولید شده توسط x می‌نامیم. بنابراین

$$\begin{aligned}
(x)_\ell &= Rx + \mathbb{Z}x = \{rx + nx \mid r \in R, \ \ n \in \mathbb{Z}\} \\
(x)_r &= xR + \mathbb{Z}x = \{xr + nx \mid r \in R, \ \ n \in \mathbb{Z}\} \\
(x) &= Rx + xR + RxR + \mathbb{Z}x \\
&= \left\{ rx + xs + nx + \sum_{i=1}^{k} r_i x s_i \;\middle|\; r, s, r_i, s_i \in R, \ \ n \in \mathbb{Z} \right\}.
\end{aligned}$$

اگر R یکدار باشد

$$(x)_\ell = Rx, \quad (x)_r = xR, \quad (x) = Rx + xR + RxR.$$

توجه کنید مجموعه‌های $Rx = \{rx \mid r \in R\}$ و $xR = \{xr \mid r \in R\}$ ایدآل‌های چپ و راست از R هستند حتی اگر R یکدار نباشد. ولی لزوماً Rx و یا xR شامل x نیستند.
حلقه‌ی تعویض‌پذیر و یکدار R را حلقه‌ی ایدآل اصلی گوییم، هرگاه هر ایدآل آن اصلی باشد. اگر حلقه‌ی ایدآل اصلی دامنه صحیح نیز باشد آن را دامنه‌ی ایدآل اصلی یا PID می‌نامیم. به عنوان مثال $\mathbb{Z}$ یک PID است.

مثال ۳.۶.۱۰. فرض کنید $R = 2\mathbb{Z}$ حلقه‌ی اعداد صحیح زوج باشد. در این صورت R یکدار نیست. داریم $2R = R2 = \{0, \pm 4, \pm 8, \ldots\} = \{r2 + n2 \mid r \in R, n \in \mathbb{Z}\} = (2)$ و $2 \in (2)$. اما 2 شامل $\{0, \pm 2, \pm 4, \ldots\}$ نیست. □

اگر I و J ایدآل‌های چپ (راست یا دوطرفی) R باشند حاصل‌ضرب دو ایدآل I و J را به صورت زیر تعریف می‌کنیم

$$IJ = \left\{ \sum_{i=1}^{n} a_i b_i \;\middle|\; n \in \mathbb{N}, \quad a_i \in I, \ \ b_i \in J \right\}.$$

به راحتی می‌توان دید IJ یک ایدآل چپ (راست یا دوطرفی) R است. به علاوه اگر I ایدآل چپ و J ایدآل راست باشند. به سادگی دیده می‌شود که IJ یک ایدآل (دوطرفی) است. هم‌چنین به صورت استقرایی تعریف می‌کنیم

$$\begin{aligned}
I^1 &= I \\
I^n &= II^{n-1}, \quad n > 1.
\end{aligned}$$

تعریف ۴.۶.۱۰. فرض کنید I ایدآلی از حلقه‌ی R باشد.
الف) I را ایدآل پوچ می‌نامیم، هرگاه هر عضو I پوچ‌توان باشد.
b) I را ایدآل پوچ‌توان می‌نامیم، هرگاه عدد صحیح مثبت n وجود داشته باشد $I^n = \{0\}$.

مثال ۵.۶.۱۰. در حلقه‌ی $\mathbb{Z}_8$، ایدآل $I = \{\bar{0}, \bar{4}\}$ ایدآل پوچ و ایدآل پوچ‌توان است:

$$I^2 = \left\{ \sum_{i=1}^{k} a_i b_i \;\middle|\; a_i, \ \ b_i \in I, \ \ k \in \mathbb{N} \right\} = \{0\},$$

زیرا $8 | a_i b_i$. □

واضح است که هر ایدآل پوچ‌توان، ایدآل پوچ نیز هست. اما عکس مطلب درست نیست، مثال بعد این مطلب را نشان می‌دهد.

مثال ۶.۶.۱۰. فرض کنید p عدد اول ثابتی باشد. فرض کنید R مجموعه‌ی همه‌ی دنباله‌های $(a_n)_{n=1}^{\infty}$، با جمله‌های در $\mathbb{Z}_{p^n}$، باشد که عدد m (وابسته به دنباله‌ی (a_n)) وجود دارد که $a_n = \bar{0}$، برای هر $n \geq m$؛ یعنی $R = \mathrm{Dr}_{n=1}^{\infty}\mathbb{Z}_{p^n}$. عمل جمع و ضرب روی R به صورت زیر است

$$\begin{aligned}(a_n) + (b_n) &= (a_n + b_n)\\ (a_n)(b_n) &= (a_n b_n),\end{aligned}$$

برای هر $(b_n), (a_n) \in R$. R یک حلقه‌ی تعویض‌پذیر است. عضو صفر آن دنباله‌ی (a_n) است که برای هر n، $a_n = \bar{0}$. قرینه‌ی دنباله‌ی (a_n) عبارت است از دنباله‌ی $(-a_n)$. عضو $\bar{p} \in \mathbb{Z}_{p^n}$ پوچ‌توان است، زیرا $\bar{p}^n = \overline{p^n} = \bar{0}$. پس برای هر $\bar{r} \in \mathbb{Z}_{p^n}$، $\bar{p}\bar{r}$ پوچ‌توان است. در نتیجه هر عضو $\bar{p}\mathbb{Z}_{p^n}$ پوچ‌توان است. فرض کنید

$$I = \{(\bar{p}a_1, \bar{p}a_2, \ldots, \bar{p}a_n, 0, 0, \ldots) \in R \mid n \in \mathbb{N}, a_i \in \mathbb{Z}_{p^i}, i = 1, \ldots, n\}.$$

I یک ایدآل R است و به علاوه هر عضو I پوچ‌توان است. اکنون نشان می‌دهیم I پوچ‌توان نیست. فرض کنید چنین نباشد، پس عدد صحیح مثبت m وجود دارد که $I^m = \{0\}$. دنباله‌ی (a_n) که $a_n = \bar{p}$ برای $i = 1, 2, \ldots, m+1$، و $a_n = \bar{0}$ برای هر $n \geq m+2$، عضوی از I است. داریم $(a_n)^m = (\bar{0}, \bar{0}, \ldots, \bar{0}, \bar{p}^m, 0, 0, \ldots)$، که در آن $(m+1)$امین جملهi دنباله‌ی $\bar{p}^m$ است و سایر جملات $\bar{0}$. چون $\bar{p}^m$ در $\mathbb{Z}_{p^{m+1}}$ ناصفر است، داریم $(a_n)^m \neq 0$، $(a_n)^m \in I^m = \{0\}$ که تناقض است. پس I پوچ‌توان نیست. □

تمرین‌ها

۱. فرض کنید $R = \mathbb{Z}[i]$. در هر حالت R/I را توصیف کنید
(الف) $I = (i)$ (ب) $I = (1 - i)$
(ج) $I = (1 + 2i)$ (د) $I = (1 + 3i)$.

۲. فرض کنید I، J و K ایدآل‌های حلقه‌ی R باشند. نشان دهید
(الف) $IJ \subseteq I \cap J$ (ب) $I(J + K) = IJ + IK$
(ج) $(J + K)I = JI + KI$ (د) $I(JK) = (IJ)K$.

۳. فرض کنید $m, n \in \mathbb{Z}$. نشان دهید $(m, n) = (m) + (n) = (d)$، که در آن $d = \gcd\{m, n\}$ و $(m) \cap (n) = (q)$، که در آن $q = \mathrm{lcm}\{m, n\}$.

۴. فرض کنید R حلقه‌ی تعویض‌پذیر باشد که ایدآل نابدیهی ندارد. نشان دهید یا R میدان است یا حلقه‌ی صفر است، یعنی به ازای هر $a, b \in R$، $ab = 0$؛ در این حالت $(R, +)$ یک گروه دوری با مرتبه‌ی عدد اول است.

۵. فرض کنید R حلقه باشد و $R^2 \neq \{0\}$. ثابت کنید R حلقه‌ی تقسیم است اگر و تنها اگر ایدآل چپ نابدیهی نداشته باشد.

۶. فرض کنید R حلقه‌ای یکدار و هر ایدآل R اصلی باشد. اگر $f : R \longrightarrow R$ یک همریختی پوشا باشد، ثابت کنید f یکریختی است.

۷. نشان دهید هر دامنه‌ی صحیح که تعداد متناهی ایدآل داشته باشد، میدان است.

۷.۱۰ ایدآل‌های ماکسیمال و اول

در این بخش همواره فرض می‌کنیم حلقه‌های مورد بررسی نابدیهی‌اند ، یعنی بیش از یک عضو دارند. یادآوری می‌کنیم که اگر I یک ایدآل چپ و J یک ایدآل راست حلقه‌ی R باشند، آنگاه

$$IJ = \left\{ \sum_{j=1}^{n} a_j b_j \;\middle|\; a_j \in I,\ \ b_j \in J,\ \ n \in \mathbb{N} \right\}$$

یک ایدآل (دوطرفی) R است. بنابراین چون $aR = \{ar \mid r \in R\}$ یک ایدآل راست R است، $R(aR)$ یک ایدآل R است که آن را با RaR نشان می‌دهیم. پس

$$\begin{aligned} RaR &= \left\{ \sum_{j=1}^{n} r_j y_j \;\middle|\; r_j \in R,\ \ y_j \in aR,\ \ n \in \mathbb{N} \right\} \\ &= \left\{ \sum_{j=1}^{n} r_j a s_j \;\middle|\; r_j, s_j \in R,\ \ n \in \mathbb{N} \right\} \end{aligned}$$

یک ایدآل دوطرفی R است.

تعریف ۱.۷.۱۰. ایدآل سره‌ی P از حلقه‌ی R را ایدآل اول می‌نامیم، هرگاه برای هر دو ایدآل I و J از R که $IJ \subseteq P$ نتیجه شود $I \subseteq P$ یا $J \subseteq P$.

قضیه‌ی بعدی یک شرط لازم و کافی برای اول بودن یک ایدآل را با استفاده از عناصر حلقه به دست می‌دهد.

قضیه ۲.۷.۱۰. ایدآل سره‌ی P از حلقه‌ی R ایدآل اول است اگر و تنها اگر برای هر $a, b \in R$، از $aRb \subseteq P$ نتیجه شود $a \in P$ یا $b \in P$.

اثبات. ($\Longleftarrow$) فرض کنید P ایدآل اول باشد و $aRb \subseteq P$، که در آن $a, b \in R$. قرار می‌دهیم $I = RaR$ و $J = RbR$، آنگاه I و J ایدآل‌هایی از حلقه‌ی R هستند. به علاوه

$$IJ = (RaR)(RbR) \subseteq R(aRb)R \subseteq RPR \subseteq P.$$

چون P اول است، یا $I \subseteq P$ و یا $J \subseteq P$. فرض کنید $I \subseteq P$. اکنون داریم $(a)^{۳} \subseteq R = I \subseteq P$ (چرا؟). چون P ایدآل اول است. $(a) \subseteq P$ و بنابراین $a \in P$. به طریق مشابه اگر $J \subseteq P$ نتیجه می‌شود $b \in P$.
($\Longrightarrow$) فرض کنید P ایدآلی باشد که در شرط قضیه صدق می‌کند. فرض کنید I و J ایدآل‌هایی از حلقه‌ی R باشند که $IJ \subseteq P$. اگر $I \nsubseteq P$، آنگاه عضو $a \in I$ وجود دارد که $a \notin P$. فرض کنید $b \in J$؛ چون $aRb = (aR)b \subseteq IJ \subseteq P$، طبق فرض $a \in P$ یا $b \in P$. اما چون $a \notin P$، داریم $b \in P$ و بنابراین $J \subseteq P$. □

نتیجه ۳.۷.۱۰. فرض کنید R حلقه‌ای دلخواه و P ایدآل سره‌ای از R باشد. اگر به ازای هر $a, b \in R$ از $ab \in P$ نتیجه شود $a \in P$ یا $b \in P$، آنگاه P اول است.

اثبات. اگر $a, b \in R$ و $aRb \subseteq P$، آنگاه $aab \in P$. طبق فرض، یا $aa \in P$ یا $b \in P$. اگر $aa \in P$ از فرض نتیجه می‌شود $a \in P$. پس در هر حال یا $a \in P$ یا $b \in P$. از این‌رو طبق قضیه‌ی ؟؟، P ایدآل اول R است. □

در حالتی که R حلقه‌ی تعویض‌پذیر باشد عکس نتیجه ۳.۷.۱۰، نیز درست است:

نتیجه ۴.۷.۱۰. فرض کنید R حلقه‌ای تعویض‌پذیر باشد. ایدآل سره‌ی P از R ایدآل اول است اگر و تنها اگر به ازای هر $a, b \in R$ از $ab \in P$ نتیجه شود $a \in P$ یا $b \in P$.

اثبات. ($\Longrightarrow$) بنا به نتیجه‌ی ۳.۷.۱۰، واضح است.
($\Longleftarrow$) فرض کنید P ایدآل اول R باشد و $ab \in P$، که در آن $a, b \in R$. چون P ایدآل است $abR \subseteq P$. از این که R تعویض‌پذیر است، داریم $aRb = abR$. اکنون چون P اول است، طبق قضیه‌ی ۲.۷.۱۰، یا $a \in P$ یا $b \in P$. □

درحالتی که R حلقه‌ی تعویض‌پذیر نباشد، نتیجه‌ی ۴.۷.۱۰، لزوماً درست نیست. در واقع فرض کنید D یک حلقه‌ی تقسیم باشد و $R = M_n(D)$. بنا به تمرین ۵ از صفحه‌ی ۲۱۸، هر ایدآل S به صورت $M_n(J)$ است، که در آن J یک ایدآل D است. اما D هیچ ایدآل نابدیهی ندارد. پس R ایدآل نابدیهی ندارد. بنابراین $\{۰\}$ ایدآل اول R است. اما R مقسوم‌علیه صفر دارد ، زیرا مثلاً $E_{۱۱}E_{۲۱} = ۰$، که در آن E_{ij} ماتریسی است که درایه‌ی (i, j) آن برابر ۱ و سایر درایه‌ها صفر است. پس $\{۰\}$ ایدآل اولی از R است که در حکم نتیجه ۴.۷.۱۰، صدق نمیکند. بنابراین اگر حلقه‌ی R تعویض‌پذیر نباشد، نتیجه‌ی ۴.۷.۱۰ درست نیست.

مثال ۵.۷.۱۰. ایدآل $\{۰\}$ یک ایدآل اول $\mathbb{Z}$ است. زیرا اگر $a,b\in\mathbb{Z}$ و $ab=۰$، آنگاه $a=۰$ یا $b=۰$. □

مثال ۶.۷.۱۰. در حلقه‌ی $\mathbb{Z}$، ایدآل $n\mathbb{Z}$، $(n\geq ۱)$ ایدآل اول است اگر و تنها اگر n عدد اول باشد.

حل فرض کنید $n\mathbb{Z}$ اول باشد و $n=ab$، در این صورت $ab=n\in n\mathbb{Z}$. چون $n\mathbb{Z}$ ایدآل اول $\mathbb{Z}$ است و $\mathbb{Z}$ تعویض‌پذیر است، یا $a\in n\mathbb{Z}$ و یا $b\in n\mathbb{Z}$. اگر $a\in n\mathbb{Z}$، آنگاه عضو $m\in\mathbb{Z}$ وجود دارد که $a=nm$. بنابراین $n=ab=nmb$. در نتیجه $mb=۱$. پس $b=a=n$. به همین نحو اگر $b\in n\mathbb{Z}$ نتیجه می‌شود $a=۱$ و $b=n$. بنابراین n عدد اول است.
برعکس اگر n عدد اول باشد، ثابت می‌کنیم $n\mathbb{Z}$ ایدآل اول است. فرض کنید $ab\in n\mathbb{Z}$، یعنی $n|ab$. چون n اول است، $n|a$ یا $n|b$. اگر $n|a$، آنگاه $a\in n\mathbb{Z}$ و اگر $n|b$، آنگاه $b\in n\mathbb{Z}$، و حکم ثابت است. □

مفهوم عدد اول را می‌توان تعمیم داد و آن را در هر حلقه‌ی تعویض‌پذیر دلخواهی تعریف کرد. اگر R یک حلقه‌ی تعویض‌پذیر باشد و $a,b\in R$، $a\neq ۰$، گوییم a، b را عاد می‌کند و می‌نویسیم $a|b$، هرگاه $c\in R$ وجود داشته باشد که $b=ac$. عضو ناصفر و نایکه‌ی p در حلقه‌ی تعویض‌پذیر R را عضو اول گوییم، هرگاه برای هر $a,b\in R$ از $p|ab$ نتیجه شود $p|a$ یا $p|b$. مثال قبل را می‌توان تعمیم داد و آن را برای هر دامنه‌ی ایدآل اصلی ثابت کرد:

قضیه ۷.۷.۱۰. اگر R یک PID و P یک ایدآل ناصفر از R باشد، آنگاه P اول است اگر و تنها اگر عضوی اول P را تولید کند.

اثبات. $(\Longleftarrow)$ چون R یک PID است و $P\neq\{۰\}$ عضو ناصفر $p\in R$ وجود دارد که $P=(p)$. چون $P\neq R$، p وارون‌پذیر نیست. فرض کنید $a,b\in R$ طوری باشند که $p|ab$. در این صورت عضو $c\in R$ وجود دارد که $ab=pc$. پس $ab\in P$. چون P ایدآل اول است و R تعویض‌پذیر است، یا $a\in P$ و یا $b\in P$. بنابراین یا $p|a$ یا $p|b$. پس p عضو اول است.
$(\Longrightarrow)$ بر عکس فرض کنید $P=(p)$ که در آن p عضوی اول از R است. چون p نایکه است، $P\neq R$. فرض کنید $a,b\in R$ و $ab\in P$. در این صورت $p|ab$. چون p اول است، $p|a$ یا $p|b$. پس $a\in P$ یا $b\in P$ و بنابراین (p) اول است. □

قضیه ۸.۷.۱۰. اگر R حلقه‌ای تعویض‌پذیر و یکدار و P ایدآلی از R باشد، آنگاه P ایدآل اول است اگر و تنها اگر R/P دامنه‌ی صحیح باشد.

اثبات. $(\Longleftarrow)$ چون R حلقه‌ی تعویض‌پذیر و یکدار است، R/P حلقه‌ی تعویض‌پذیر و یکدار است. چون $P\neq R$، داریم $۱\notin P$ و بنابراین $۱+P\neq ۰+P$. بنابراین R/P حلقه‌ای نابدیهی است. نشان می‌دهیم R/P مقسوم‌علیه صفر ندارد. اگر $a+P,b+P\in R/P$ و $(a+P)(b+P)=۰+P$، آنگاه داریم $ab+P=۰+P$، یعنی $ab\in P$. چون P ایدآل اول است، $a\in P$ یا $b\in P$، یعنی $a+P=۰+P$ یا $b+P=۰+P$. پس R/P مقسوم‌علیه صفر ندارد و R/P دامنه‌ی صحیح است.
$(\Longrightarrow)$ اگر $a,b\in R$ و $ab\in P$، آنگاه داریم $۰+P=ab+P=(a+P)(b+P)$. از این‌رو $a+P=۰+P$ یا $b+P=۰+P$. بنابراین $a\in P$ یا $b\in P$. در نتیجه P ایدآل اول است. □

تعریف ۹.۷.۱۰. ایدآل M از حلقه‌ی R را ایدآل ماکسیمال می‌نامیم، هرگاه $M\neq R$ و ایدآل I از R وجود نداشته باشد که $M\subset I\subset R$.

قضیه ۱۰.۷.۱۰. اگر M یک ایدآل حلقه‌ی تعویض‌پذیر و یکدار R باشد، آنگاه M ایدآل ماکسیمال R است اگر و تنها اگر R/M میدان باشد.

اثبات. $(\Longrightarrow)$ فرض کنید M ایدآل ماکسیمال باشد. چون R حلقه‌ی یکدار است و $۱\notin M$، R/M نیز حلقه‌ی یکدار است. با توجه به قضیه‌ی ۹.۴.۱۰، کافی است ثابت کنیم R/M ایدآل نابدیهی ندارد. اگر J/M ایدآلی از R/M باشد، آنگاه J ایدآلی از R است و $M\subseteq J\subseteq R$. چون M ماکسیمال است، یا $M=J$ یا $R=J$. در نتیجه یا $J/M=\{M\}$ و یا $J/M=R/M$. پس R/M ایدآل نابدیهی ندارد.
$(\Longleftarrow)$ بر عکس فرض کنید R/M میدان باشد. در این صورت $R\neq M$. اگر J ایدآلی از R باشد که $M\subseteq J\subseteq R$. در این صورت J/M ایدآلی از R/M است. بنا به نتیجه‌ی ۸.۴.۱۰، R/M ایدآل نابدیهی ندارد. پس $J/M=\{M\}$ یا $J/M=R/M$، یعنی $J=M$ یا $J=R$. بنابراین M ایدآل ماکسیمال است. □

چون هر میدان دامنه‌ی صحیح است، هر ایدآل ماکسیمال در حلقه‌ی تعویض‌پذیر و یکدار، ایدآل اول نیز هست. اما عکس مطلب لزوماً درست نیست، مثلاً ایدآل $\{۰\}$ در حلقه‌ی تعویض‌پذیر و یکدار $\mathbb{Z}$ اول است اما ماکسیمال نیست، زیرا $\mathbb{Z}/\{۰\} \cong \mathbb{Z}$ دامنه‌ی صحیح است ولی میدان نیست. به عنوان مثال دیگر حلقه‌ی $R = \mathbb{Z} \times \mathbb{Z} = \{(a,b) \mid a,b \in \mathbb{Z}\}$ را با جمع و ضرب متعارف در نظر بگیرید. در این صورت $I = \mathbb{Z} \times \{۰\} = \{(a,۰) \mid a \in \mathbb{Z}\}$ ایدآل اول است اما ماکسیمال نیست، زیرا $I \subset \mathbb{Z} \times ۲\mathbb{Z} \subset R$.

مثال ۱۱.۷.۱۰. حلقه‌ی تعویض‌پذیر و بدون یک $R = ۲\mathbb{Z}$ را در نظر بگیرید. ایدآل تولید شده توسط ۴، یعنی

$$(۴) = ۴R + ۴\mathbb{Z} = \{۸k + ۴m \mid k,m \in \mathbb{Z}\}$$

را در نظر بگیرید. (۴) در R ماکسیمال است اما اول نیست، زیرا $(۴) \in ۲ \times ۲$ و $۲ \notin (۴)$. □

فرض کنید I ایدآل حلقه‌ی تعویض‌پذیر و یکدار R باشد. اگر M/I ایدآلی از حلقه‌ی تعویض‌پذیر و یکدار R/I باشد، آنگاه M/I یک ایدآل اول (ماکسیمال) است اگر و تنها اگر $\frac{R/I}{M/I} \cong R/M$. دامنه‌ی صحیح (میدان) باشد. بنابراین ایدآل‌های اول (ماکسیمال) R/I به صورت M/I هستند که در آن M یک ایدآل اول (ماکسیمال) R است و $I \subseteq M$. به عنوان حالت خاص حلقه‌ی تعویض‌پذیر و یکدار $\mathbb{Z}_۶ = \mathbb{Z}/۶\mathbb{Z}$ را در نظر بگیرید. تنها ایدآل‌های ماکسیمال $\mathbb{Z}$ که شامل $۶\mathbb{Z}$ هستند عبارت‌اند از $۲\mathbb{Z}$ و $۳\mathbb{Z}$ (توجه کنید $n\mathbb{Z} \subseteq m\mathbb{Z}$ اگر و تنها اگر $m|n$). پس ایدآل‌های ماکسیمال $\mathbb{Z}_۶$ عبارت‌اند از :

$$\frac{۳\mathbb{Z}}{۶\mathbb{Z}} = ۳\mathbb{Z}_۶ = \{\bar{۰}, \bar{۳}\}, \quad \frac{۲\mathbb{Z}}{۶\mathbb{Z}} = ۲\frac{\mathbb{Z}}{۶\mathbb{Z}} = ۲\mathbb{Z}_۶ = \{\bar{۰}, \bar{۲}, \bar{۴}\}$$

مثال ۱۲.۷.۱۰. فرض کنید R حلقه‌ی توابع پیوسته حقیقی روی فاصله‌ی بسته $[۰, ۱]$ باشد. نشان دهید اگر $۰ \leq c \leq ۱$ عددی ثابت باشد، آنگاه $I = \{f \in R \mid f(c) = ۰\}$ یک ایدآل ماکسیمال R است. در تمرین ۱۹، خواسته شده که نشان دهید ، هر ایدآل ماکسیمال R به این صورت است.

حل تابع $\varphi : R \longrightarrow \mathbb{R}$ را با ضابطه‌ی $\varphi(f) = f(c)$ تعریف می‌کنیم. به وضوح φ همریختی پوشا با هسته‌ی I است. پس ، بنا به قضیه‌ی اول یکریختی، $R/I \cong \mathbb{R}$. بنابراین R/I میدان است و طبق قضیه‌ی ۱۰.۷.۱۰، I ایدآل ماکسیمال R است. □

قضیه ۱۳.۷.۱۰. اگر R یک دامنه‌ی ایدآل اصلی باشد، آنگاه ایدآل ناصفر P، $(P \neq R)$ اول است اگر و تنها اگر ماکسیمال باشد.

اثبات. $(\Longrightarrow)$ هر ایدآل ماکسیمال در حلقه‌ی تعویض‌پذیر و یکدار اول است.
$(\Longleftarrow)$ چون P ایدآل ناصفر اول است و $P \neq R$ و R دامنه‌ی ایدآل اصلی است، بنا به قضیه‌ی ۷.۷.۱۰، عضو اول $p \in R$ وجود دارد که $P = (p)$. فرض کنید $R \subseteq (a) \subseteq (p)$. چون $p \in (p) \subseteq (a)$، عضو $b \in R$ وجود دارد که $p = ab$، به ویژه $p|ab$. چون p اول است، $p|a$ یا $p|b$. اگر $p|a$، آنگاه $(p) \subseteq (a)$ و بنابراین $(a) = (p)$. اگر $p|b$، آنگاه $c \in R$ وجود دارد که $b = cp$. پس $p = ab = acp$. چون R دامنه‌ی صحیح است داریم $ac = ۱$. بنابراین a وارون‌پذیر است، که نتیجه می‌دهد $(a) = R$. در نتیجه (p) ایدآل ماکسیمال است. □

حال نشان می‌دهیم در هر حلقه‌ی یکدار ایدآل ماکسیمال وجود دارد :

قضیه ۱۴.۷.۱۰. اگر R حلقه‌ای یکدار باشد، آنگاه هر ایدآل سره‌ی R در یک ایدآل ماکسیمال قرار دارد.

اثبات. از لم زُرن استفاده می‌کنیم. فرض کنید I ایدآل سره‌ی از R باشد و مجموعه‌ی

$$\mathscr{A} = \{J \mid I \subseteq J, \ \ J \text{ ایدآل سره‌ی } R\}$$

را در نظر بگیرید. چون $I \in \mathscr{A}$، $A \neq ۰$. به علاوه $\mathscr{A}$ همراه با رابطه‌ی شمول یک مجموعه‌ی جزئا مرتب است. نشان می‌دهیم هر زنجیر در $\mathscr{A}$ کران بالا در $\mathscr{A}$ دارد. فرض کنید $\mathscr{B} = \{J_\lambda\}_{\lambda \in \Lambda}$ یک زنجیر در $\mathscr{A}$ باشد. چون $I \subseteq J_\lambda$، برای هر $\lambda \in \Lambda$، داریم $I \subseteq \bigcup_{\lambda \in \Lambda} J_\lambda$. حال نشان می‌دهیم $\bigcup_{\lambda \in \Lambda} J_\lambda$ ایدآلی از R است. فرض کنید $a,b \in \bigcup_{\lambda \in \Lambda} J_\lambda$. در این صورت به ازای $\lambda, \mu \in \Lambda$ داریم $a \in J_\lambda$ و $b \in J_\mu$. چون $\mathscr{B}$ زنجیر است، یا $J_\lambda \subseteq J_\mu$ یا $J_\mu \subseteq J_\lambda$. فرض کنید مثلاً $J_\lambda \subseteq J_\mu$، بنابراین $a,b \in J_\mu$. چون J_μ ایدآل است، $a - b \in J_\mu \subseteq \bigcup_{\lambda \in \Lambda} J_\lambda$. اگر $r \in R$، آنگاه $ra, ar \in J_\lambda \subseteq \bigcup_{\lambda \in \Lambda} J_\lambda$. در نتیجه $\bigcup_{\lambda \in \Lambda} J_\lambda$ ایدآل R است. ادعا

می‌کنیم $\bigcup_{\lambda\in\Lambda} J_\lambda \neq R$. اگر چنین نباشد، به ازای یک $\lambda \in \Lambda$ داریم $1 \in J_\lambda$، که ممکن نیست زیرا $J_\lambda \neq R$. پس $\bigcup_{\lambda\in\Lambda} J_\lambda$ یک کران بالای $\mathscr{B}$ است که در $\mathscr{A}$ قرار دارد. بنابراین بنا به لم زُرن، عضوی ماکسیمال چون M در $\mathscr{A}$ وجود دارد. حال نشان می‌دهیم M ایدآل ماکسیمال است. اگر J ایدآلی از R باشد که $M \subset J \subset R$، آنگاه $J \in \mathscr{A}$ و بنابراین M در $\mathscr{A}$ ماکسیمال نیست که تناقض است. پس چنین Jای وجود ندارد و M ایدآل ماکسیمال است. □

نتیجه ۱۵.۷.۱۰. اگر R حلقه‌ی یکدار باشد و $a \in R$، آنگاه a در یک ایدآل ماکسیمال R قرار دارد اگر و تنها اگر a نایکه باشد.

اثبات. فرض کنید a نایکه باشد، پس $(a) \subset R$ و بنا به قضیه‌ی ۱۴.۷.۱۰، ایدآل ماکسیمال M از R وجود دارد که $(a) \subseteq M$. در نتیجه $a \in (a) \subseteq M$. برعکس اگر $a \in M$، آنگاه چون M ایدآل ماکسیمال است $M \neq R$. بنابراین a یکه نیست. □

نتیجه ۱۶.۷.۱۰. اگر R حلقه‌ای یکدار باشد، آنگاه R یک ایدآل ماکسیمال دارد.

اثبات. چون $\{0\}$ یک ایدآل سره است، بنا به قضیه‌ی ۱۴.۷.۱۰، ایدآل ماکسیمال M از R وجود دارد که $\{0\} \subseteq M$. □

تعریف ۱۷.۷.۱۰. اگر R حلقه‌ای تعویض‌پذیر و یکدار باشد، رادیکال ژاکوبسون را که با $J(R)$ نشان می‌دهیم عبارت است از

$$J(R) = \bigcap\{M \mid R \text{ ایدآل ماکسیمال } M\}.$$

توجه کنید اگر حلقه‌ی تعویض‌پذیر و یکدار R تنها یک ایدآل ماکسیمال ، مثلاً M، داشته باشد، آنگاه هر عضو نایکه R در M قرار دارد (بنا به قضیه‌ی ۱۴.۷.۱۰). از طرف دیگر چون M سره است، هر عضو M نایکه است. پس $J(R) = M$ دقیقاً مجموعه‌ی عناصر نایکه R است. برعکس اگر مجموعه‌ی I متشکل از عناصر نایکه R یک ایدآل R باشد، آنگاه I ایدآل ماکسیمال R و تنها ایدآل ماکسیمال است. زیرا عناصر هر ایدآل سره‌ی J نایکه هستند و بنابراین هر ایدآل سره‌ی R در I قرار دارد. در نتیجه در یک حلقه‌ی تعویض‌پذیر و یکدار تنها یک ایدآل ماکسیمال وجود دارد اگر و تنها اگر مجموعه‌ی عناصر نایکه ایدآل باشد. این حلقه‌ها را موضعی می‌نامیم (تمرین ۲۳ از صفحه‌ی ۲۱۹ را ببینید). قضیه‌ی بعدی $J(R)$ را بر حسب عناصر R توصیف می‌کند.

قضیه ۱۸.۷.۱۰. اگر R حلقه‌ی تعویض‌پذیر و یکدار باشد و $y \in R$، آنگاه $y \in J(R)$ اگر و تنها اگر به ازای هر $x \in R$، $1 - xy$ در R یکه باشد.

اثبات. فرض کنید $y \in J(R)$ و عضو $x \in R$ وجود داشته باشد که $1 - xy$ یکه نباشد. پس ایدآل ماکسیمال M از R وجود دارد که $1 - xy \in M$. چون $y \in J(R)$ داریم $y \in M$. در نتیجه $xy \in M$ که نتیجه می‌دهد

$$1 = 1 - xy + xy \in M,$$

که تناقض است. پس $1 - xy$ یکه است.
برعکس فرض کنید به ازای هر $x \in R$، $1 - xy$ یکه باشد. اگر $y \notin J(R)$، آنگاه ایدآل ماکسیمال M از R وجود دارد که $y \notin M$. در این صورت $M + Ry$ ایدآلی از R است که $M \subset M + Ry$. چون M ماکسیمال است باید داشته باشیم $M + Ry = R$. اکنون چون $1 \in R$، عضو $a \in M$ و $r \in R$ وجود دارد که $1 = a + ry$. در نتیجه $1 - ry = a \in M$. بنا به فرض $a = 1 - ry$ یکه است، این تناقض است، زیرا $M \neq R$. در نتیجه $y \in J(R)$. □

نتیجه ۱۹.۷.۱۰. فرض کنید R حلقه‌ی تعویض‌پذیر و یکدار باشد. در این صورت 0 تنها عضو خودتوان $J(R)$ است.

اثبات. فرض کنید $y \in J(R)$ عضو خودتوان باشد. اکنون $1 - y = 1 - y1$ عضوی یکه است. پس $u \in R$ وجود دارد که $(1 - y)u = 1$. با ضرب y در طرفین رابطه‌ی اخیر و توجه به این نکته که $y = y^2$، داریم

$$y = y(1 - y)u = (y - y^2)u = (y - y)u = 0.$$

بنابراین $y = 0$. □

نتیجه ۲۰.۷.۱۰. اگر R حلقه‌ی تعویض‌پذیر و یکدار باشد، آنگاه $J(R)$ شامل همه‌ی ایدآل‌های پوچ است.

اثبات. فرض کنید I یک ایدآل پوچ R باشد. پس هر عضو I پوچ‌توان است. بنابراین به ازای هر $a \in I$ و هر $r \in R$، ar پوچ‌توان است. در نتیجه بنا به تمرین ۲، از صفحه‌ی ۲۰۷، به ازای هر $r \in R$، $1 - ar$ وارون‌پذیر است. از این‌رو $a \in J(R)$ و $I \subseteq J(R)$. □

تمرین‌ها

۱. فرض کنید $f : R \longrightarrow S$ همریختی حلقه‌ای پوشا باشد. ثابت کنید
(الف) اگر J ایدآل اول S باشد، $f^{-1}(J)$ یک ایدآل اول R شامل $\ker f$ است.
(ب) اگر I ایدآل اول R شامل $\ker f$ باشد، $f(I)$ ایدآل اول S است.
(ج) مطالب فوق را در مورد ایدآل‌های ماکسیمال بررسی کنید.

۲. ثابت کنید در یک حلقه‌ی بولی ایدآل‌های اول ، ماکسیمال هستند.

۳. فرض کنید R حلقه‌ی تعویض‌پذیر و یکدار باشد و برای هر $a \in R$، عدد صحیح $n > 1$ وجود داشته باشد که $a^n = a$. ثابت کنید هر ایدآل اول R ماکسیمال است.

۴. ثابت کنید مجموعه‌ی متشکل از صفر و همه‌ی مقسوم‌علیههای صفر در یک حلقه تعویض‌پذیر و یکدار، شامل حداقل یک ایدآل اول است.

۵. اگر $N(R)$ ایدآل همه‌ی عناصر پوچ‌توان حلقه‌ی تعویض‌پذیر و یکدار R باشد، ثابت کنید $N(R)$ برابر اشتراک همه‌ی ایدآل‌های اول R است.

۶. فرض کنید R حلقه‌ی تعویض‌پذیر و یکدار باشد. اگر هر ایدآل R اول باشد، نشان دهید R میدان است.

۷. فرض کنید R حلقه‌ی تعویض‌پذیر و یکدار، و I ایدآلی از R باشد. اگر P ایدآل اول I باشد، ثابت کنید P ایدآل R است.

۸. نشان دهید ایدآل (x) در $\mathbb{Z}[x]$ اول است، اما ماکسیمال نیست.

۹. نشان دهید $\mathbb{Z} \times \mathbb{Z}$ ۵$\mathbb{Z} \times \mathbb{Z}$ ایدآل ماکسیمال است.

۱۰. فرض کنید $I = \{f(x) \in \mathbb{Z}[x] \mid 3 | f(0)\}$، نشان دهید I ایدآل اول است. آیا I ماکسیمال است؟

۱۱. فرض کنید $n > 1$ عدد صحیح باشد. نشان دهید $J(\mathbb{Z}_n) = \{0\}$ اگر و تنها اگر n آزاد از مربع باشد. (عدد صحیح مثبت n را آزاد از مربع گوییم، هرگاه $n = p_1 p_2 \cdots p_k$، که در آن p_iها اعداد اول متمایزند.)

۱۲. فرض کنید I یک ایدآل حلقه R باشد.
(الف) نشان دهید پوچ‌ساز I در R، که با

$$\operatorname{ann}_R(I) = \{r \in R \mid = ar = 0, \ \ \forall a \in I\}$$

تعریف می‌شود،یک ایدآل R است.
(ب) اگر I تعویض‌پذیر باشد و $\operatorname{ann}_R(I) = \{0\}$، نشان دهید R تعویض‌پذیر است. نتیجه بگیرید اگر $I \neq \{0\}$ ایدآل اول و تعویض‌پذیر باشد، آنگاه R تعویض‌پذیر است.

۱۳. فرض کنید R حلقه‌ی تعویض‌پذیر و یکدار باشد. اگر I یک ایدآل R و P_1، ...، P_n ایدآل‌های اول R باشند طوریکه $I \subseteq \bigcup_{i=1}^{n} P_i$، نشان دهید $1 \leq j \leq n$ وجود دارد که $I \subseteq P_j$.

۱۴. فرض کنید R حلقه‌ی تعویض‌پذیر و یکدار، و P ایدآل اولی از R باشد، نشان دهید
(الف) $S = R - P$ مجموعه‌ی بسته‌ی ضربی است. (تمرین ۴ از صفحه‌ی ۲۲۱ را ببینید.)
(ب) $S^{-1}R$ یک حلقه‌ی موضعی است. این حلقه را موضعی سازی R در P گوییم و با R_P نشان می‌دهیم.
(ج) اگر R دامنه‌ی صحیح باشد، آنگاه R_P زیرحلقه‌ای از Q است، که در آن Q میدان کسرهای R است.

۱۵. اگر R حلقه‌ی تعویض‌پذیر باشد و $R^2 = R$ (به ویژه اگر R یکدار باشد)، نشان دهید هر ایدآل ماکسیمال، اول است.

۱۶. فرض کنید S یک زیرمجموعه‌ی بسته‌ی ضربی از حلقه‌ی تعویض‌پذیر و یکدار R باشد و $0 \notin S$. نشان دهید مجموعه‌ی متشکل از همه‌ی ایدآل‌های R که با S اشتراک ندارند، یعنی $\mathscr{A} = \{I \mid I \cap S = \emptyset \quad R$ ایدآل $I\}$، یک عضو ماکسیمال دارد که لزوماً ایدآل اول است.

۱۷. فرض کنید هر ایدآل چپ در حلقه‌ی یکدار R ایدآل راست باشد. اگر P یک ایدآل سره‌ی R باشد، ثابت کنید P ایدآل اول R است

اگر و تنها اگر از $ab \in P$، $(a, b \in R)$ نتیجه شود $a \in P$ یا $b \in P$.

۱۸. فرض کنید R حلقه‌ای یکدار و هر ایدآل چپ R ایدآل راست نیز باشد. نشان دهید اشتراک همه‌ی ایدآل‌های اول با مجموعه‌ی عناصر پوچ‌توان R برابر است.

۱۹. فرض کنید R حلقه‌ی توابع پیوسته حقیقی روی فاصله‌ی بسته‌ی $[۰, ۱]$ باشد. اگر M ایدآل ماکسیمال R باشد، ثابت کنید عدد حقیقی $۰ \leq \alpha \leq ۱$ وجود دارد که $M = \{f \in R \mid f(\alpha) = ۰\}$ (قدری آنالیز نیاز دارد).

فصل ۱۱

حلقه‌ی چندجمله‌ای‌ها

۱.۱۱ خواص مقدماتی چندجمله‌ای‌ها

رده‌ی بسیار مهمی از حلقه‌ها، حلقه‌ی چندجمله‌ای‌ها است. با چندجمله‌ای‌ها آشنا هستیم. می‌توانیم تصور کنیم یک چندجمله‌ای یک عبارت به صورت $a_0 + a_1x + \cdots + a_nx^n$ است، که در آن x یک نماد، a_iها اعضای یک حلقه‌اند، یا می‌توانیم چندجمله‌ای را به عنوان یک تابع $f(x) = a_0 + a_1x + \cdots + a_nx^n$ تصور کنیم. اما وقعاً چندجمله‌ای چنین چیزهایی است؟ نماد x چیست؟ چرا دو چندجمله‌ای $a_0 + a_1x + \cdots + a_nx^n$ و $b_0 + b_1x + \cdots + b_mx^m$ مساوی‌اند اگر و تنها اگر $n = m$ و $a_i = b_i$، $i = 1, \ldots, m$؟ می خواهیم به این سوالات پاسخ دهیم و خواص اساسی چندجمله‌ای‌ها را بررسی کنیم. ابتدا تعریف دقیقاً چندجمله‌ای را ارائه می‌کنیم.

تعریف ۱.۱.۱۱. به ازای هر حلقه‌ی دلخواه R، $R[x]$ را مجموعه‌ی همه‌ی دنباله‌های نامتناهی $(a_0, a_1, a_2, \ldots)$، با $a_i \in R$، $i = 0, 1, 2, \ldots$، که عدد صحیح n (وابسته به دنباله‌ی $(a_0, a_1, a_2, \ldots)$) وجود دارد که برای هر $k \geq n$، $a_k = 0$، در نظر می‌گیریم. عناصر $R[x]$ را چندجمله‌ای‌های روی R گوییم.

جمع و ضرب را روی $R[x]$ به صورت زیر تعریف می‌کنیم:

$$(a_0, a_1, a_2, \ldots) + (b_0, b_1, b_2, \ldots) = (a_0 + b_0, a_1 + b_1, a_2 + b_2, \ldots)$$

$$(a_0, a_1, a_2, \ldots)(b_0, b_1, b_2, \ldots) = (c_0, c_1, c_2, \ldots),$$

که در آن

$$c_j = \sum_{i=0}^{j} a_i b_{j-i}, \quad j = 0, 1, 2, \ldots.$$

تحقیق این که $R[x]$ با اعمال فوق حلقه است، چندان مشکل نیست و به خواننده واگذار می‌شود. توجه کنید عضو صفر $R[x]$ دنباله‌ی $(0, 0, 0, \ldots)$ و قرینه‌ی $(a_0, a_1, a_2, \ldots)$ دنباله‌ی $(-a_0, -a_1, -a_2, \ldots)$ است. $R[x]$ را حلقه‌ی چندجمله‌ای‌ها روی R گوییم. اگر R تعویض‌پذیر باشد، به وضوح $R[x]$ نیز تعویض‌پذیر است. اگر R یکدار باشد، آنگاه $R[x]$ نیز یکدار با عضو همانی $(1, 0, 0, 0, \ldots)$ است. نگاشت $a \mapsto (a, 0, 0, \ldots)$ یک همریختی یک‌به‌یک از R به $R[x]$ است. پس R را می‌توان با یکی گرفتن تصویر آن تحت نگاشت فوق، به عنوان زیرحلقه‌ای از $R[x]$ در نظر گرفت. بنابراین تمایزی بین a و $(a, 0, 0, \ldots)$ قائل نمی‌شویم.
اکنون می‌خواهیم نمادگذاری بالا را به نمادهای آشنای قبلی تبدیل کنیم. اگر $(a, 0, 0, \ldots)$ را با $ax^0 = a$، $(0, a, 0, \ldots)$ را با ax^1، $(0, 0, a, 0, \ldots)$ را با ax^2 و ... نشان دهیم، آنگاه داریم

$$\begin{aligned}(a_0, a_1, a_2, \ldots, a_n, 0, 0, \ldots) &= (a_0, 0, 0, \ldots) + (0, a_1, 0, 0, \ldots) + \\ &\quad \cdots + (0, 0, \ldots, 0, a_n, 0, \ldots) \\ &= a_0 + a_1x + \cdots + a_nx^n.\end{aligned}$$

نماد x را یک متغیر روی R و عناصر a_0، a_1، ...، a_n را ضرایب $a_0 + a_1x + \cdots + a_nx^n$ می‌نامیم. چون دو دنباله‌ی $(a_0, a_1, \ldots)$ و $(b_0, b_1, \ldots)$ مساوی‌اند اگر و تنها اگر به ازای هر i، $a_i = b_i$، دو چندجمله‌ای $a_0 + a_1x + \cdots + a_nx^n$ و

$b_۰ + b_۱x + \cdots + b_mx^m$ مساوی‌اند اگر و تنها اگر $n = m$ و $a_i = b_i$، $i = ۱, ۲, \ldots, n$.

اگر R یکدار باشد، می‌توانیم x را به عنوان عضوی از $R[x]$ در نظر بگیریم و این کار را با یکی گرفتن $۱x$ با x یعنی $(۰, ۱, ۰, \ldots)$ انجام می‌دهیم.
می‌توان تحقیق کرد که تعریف جمع و ضرب دو چندجمله‌ای همان جمع و ضرب آشنای چندجمله‌ای‌هاست. پس وقتی R یکدار باشد، داریم

$$\begin{aligned} ax &= (a, ۰, ۰, \ldots)(۰, ۱, ۰, \ldots) \\ &= (۰, a, ۰, \ldots) \\ &= (۰, ۱, ۰, \ldots)(a, ۰, ۰, \ldots) \\ &= xa. \end{aligned}$$

پس وقتی R یکدار باشد، $x \in \mathrm{Cent}(R[x])$.

تعریف ۲.۱.۱۱. فرض کنید R یک حلقه باشد. اگر $f(x) = a_۰ + a_۱x + \cdots + a_nx^n$، $a_n \neq ۰$، یک چندجمله‌ای در $R[x]$ باشد، آنگاه n را درجه‌ی چندجمله‌ای $f(x)$ گوییم و با $\deg f(x)$ نشان می‌دهیم. a_n را ضریب پیشروی $f(x)$ می‌نامیم. اگر R یکدار باشد و $a_n = ۱$، $f(x)$ را چندجمله‌ای تکین گوییم.

چندجمله‌ای‌های درجه‌ی صفر در $R[x]$ دقیقاً اعضای $R - \{۰\}$ هستند. $۰ \in R[x]$ درجه‌ای ندارد؛ یعنی درجه‌ی چندجمله‌ای صفر را تعریف نمی‌کنیم. عناصر R را چندجمله‌ای‌های ثابت یا اسکالر گوییم.

قضیه ۳.۱.۱۱. فرض کنید R یک حلقه و $f(x) = a_۰ + a_۱x + \cdots + a_nx^n$، $a_n \neq ۰$، $g(x) = b_۰ + b_۱x + \cdots + b_mx^m$، $b_m \neq ۰$، دو چندجمله‌ای ناصفر در $R[x]$ باشند.
(الف) اگر $f(x)g(x) \neq ۰$، آنگاه $\deg f(x)g(x) \leq \deg f(x) + \deg g(x)$ و تساوی وقتی برقرار است که $a_nb_m \neq ۰$. به ویژه اگر R مقسوم‌علیه صفر نداشته باشد $R[x]$ نیز مقسوم‌علیه صفر ندارد.
(ب) اگر $f(x) + g(x) \neq ۰$، آنگاه

$$\deg(f(x) + g(x)) \leq \max\{\deg f(x), \deg g(x)\}.$$

اثبات. (الف) داریم $f(x)g(x) = a_۰b_۰ + (a_۰b_۱ + a_۱b_۰)x + \cdots + a_nb_mx^{n+m}$.
اگر $f(x)g(x) \neq ۰$، آنگاه حداقل یکی از ضرایب $f(x)g(x)$ ناصفر است. اگر $a_nb_m \neq ۰$، آنگاه داریم

$$\deg f(x)g(x) = n + m = \deg f(x) + \deg g(x)$$

و اگر $a_nb_m = ۰$، آنگاه $\deg f(x)g(x) < \deg f(x) + \deg g(x)$.
(ب) اگر مثلاً $\deg f(x) > \deg g(x)$، آنگاه

$$\deg(f(x) + g(x)) = \deg f(x) = \max\{\deg f(x), \deg g(x)\}.$$

حال فرض کنید $\deg f(x) = \deg g(x)$. چون $f(x) + g(x) \neq ۰$ داریم

$$\deg(f(x) + g(x)) \leq \deg f(x) = \deg g(x) = \max\{\deg f(x), \deg g(x)\}.$$

قضیه ۴.۱.۱۱. اگر R یک حلقه‌ی تعویض‌پذیر و یکدار باشد، آنگاه $R[x]$ نیز حلقه‌ی تعویض‌پذیر و یکدار است.

اثبات. فرض کنید $f(x) = a_۰ + a_۱x + \cdots + a_nx^n$ و $g(x) = b_۰ + b_۱x + \cdots + b_mx^m$ دو عضو $R[x]$ باشند. در این صورت

$$f(x)g(x) = c_۰ + c_۱x + \cdots + c_tx^t \quad \text{و} \quad g(x)f(x) = d_۰ + d_۱x + \cdots + d_sx^s,$$

که در آن $c_j = \sum_{i=۰}^{j} a_i b_{j-i}$ و $d_j = \sum_{i=۰}^{j} b_{j-i} a_i$. چون R تعویض‌پذیر است به ازای هر $j = ۰, ۱, ۲, \ldots$ داریم

$$c_j = a_۰b_j + a_۱b_{j-۱} + \cdots + a_jb_۰ = b_۰a_j + b_۱a_{j-۱} + \cdots + b_ja_۰ = d_j.$$

بنابراین $f(x)g(x) = g(x)f(x)$ و در نتیجه $R[x]$ تعویض‌پذیر است. چون R یکدار است، $۱ \in R[x]$ و به ازای هر $f(x) \in R[x]$، $f(x)۱ = ۱f(x) = f(x)$. از این‌رو $R[x]$ حلقه‌ی تعویض‌پذیر و یکدار است. □

مثال ۵.۱.۱۱. فرض کنید $f(x) = ۱ + ۲x^۲$ و $g(x) = ۱ + ۳x$ دو چندجمله‌ای در $\mathbb{Z}_۶[x]$ باشند. در این صورت

$$f(x) + g(x) = ۲ + ۳x + ۲x^۲ \quad \text{و} \quad f(x)g(x) = ۱ + ۳x + ۲x^۲$$

و

$$\deg f(x)g(x) = ۲ < ۳ = \deg f(x) + \deg g(x).$$

اگر $h(x) = ۵ + ۴x^۲$، آنگاه $f(x) + h(x) = ۰$. بنابراین $\deg(f(x) + h(x))$ تعریف نشده است. □

قضیه ۶.۱.۱۱. قضیه‌ی (الگوریتم تقسیم) فرض کنید R حلقه‌ی یکدار و $f(x)$، $g(x)$ دو چندجمله‌ای در $R[x]$ باشند. اگر ضریب پیشرو ی $g(x)$ در R یکه باشد، آنگاه چندجمله‌ای‌های یکتای $r(x), q(x) \in R[x]$ وجود دارند که

$$f(x) = q(x)g(x) + r(x),$$

که در آن $r(x) = ۰$ یا $\deg r(x) < \deg g(x)$.

اثبات. اگر $f(x) = ۰$ یا $\deg f(x) < \deg g(x)$، آنگاه قرار می‌دهیم $q(x) = ۰$ و $r(x) = f(x)$. پس فرض می‌کنیم $\deg f(x) \geq \deg g(x)$ و قضیه را به استقرا روی $\deg f(x) = n$ ثابت می‌کنیم. اگر $\deg f(x) = ۰$، آنگاه $\deg f(x) = \deg g(x)$. در این حالت قرار می‌دهیم $q(x) = f(x)g(x)^{-۱}$ و $r(x) = ۰$. اکنون فرض کنید قضیه برای همه‌ی چندجمله‌ای‌های با درجه‌ی کمتر از n برقرار باشد و $f(x) = a_۰ + a_۱x + \cdots + a_nx^n$ و $g(x) = b_۰ + b_۱x + \cdots + b_mx^m$، $a_n, b_m \neq ۰$، و $n \geq m$. درجه‌ی چندجمله‌ای

$$f_۱(x) = f(x) - a_nb_m^{-۱}x^{n-m}g(x)$$

کمتر از n است، زیرا ضرایب x^n برابر است با $a_n - (a_nb_m^{-۱})b_m = ۰$. بنابراین بنا به فرض استقرا، چندجمله‌ای‌های $q_۱(x), r_۱(x) \in R[x]$ وجود دارند که

$$f_۱(x) = q_۱(x)g(x) + r_۱(x),$$

که در آن $r_۱(x) = ۰$ یا $\deg r_۱(x) < \deg g(x)$. اگر در معادله‌ی فوق به جای $f_۱(x)$ مقدار را قرار دهیم داریم

$$f(x) - a_nb_m^{-۱}x^{n-m}g(x) = q_۱(x)g(x) + r_۱(x),$$

یعنی

$$f(x) = (q_۱(x) + a_nb_m^{-۱}x^{n-m})g(x) + r_۱(x).$$

با فرض $q(x) = q_۱(x) + a_nb_m^{-۱}x^{n-m}$ و $r(x) = r_۱(x)$ نمایش مورد نظر برای $f(x)$ حاصل‌ضرب شده است. حال ثابت می‌کنیم $q(x)$ و $r(x)$ یکتا هستند. فرض کنید چندجمله‌ای‌های $r_۲(x) \in R[x]$ و $q_۲(x)$ نیز وجود دارند که

$$f(x) = q(x)g(x) + r(x) = q_۲(x)g(x) + r_۲(x)$$

که در آن $r_۲(x) = ۰$ یا $\deg r_۲(x) < \deg g(x)$. داریم

$$r(x) - r_۲(x) = (q_۲(x) - q(x))g(x).$$

اگر $r(x) \neq r_۲(x)$، چون ضریب پیشرو ی $g(x)$ یکه است داریم

$$\deg((q_۲(x) - q(x))g(x)) = \deg(q_۲(x) - q(x)) + \deg g(x) \geq \deg g(x).$$

از این‌رو

$$\deg(r(x) - r_۲(x)) \geq \deg g(x)$$

که ممکن نیست، زیرا $\deg r(x), \deg r_۲(x) < \deg g(x)$. پس $r(x) = r_۲(x)$. بنابراین

$$۰ = (q_۲(x) - q(x))g(x).$$

حال اگر $q_۲(x) \neq q(x)$، چون b_m یکه است درجه‌ی سمت راست تساوی تعریف شده و بزرگ‌تر یا مساوی صفر است، در صورتی که درجه‌ی سمت چپ تساوی تعریف نشده که تناقض است، پس $q_۲(x) = q(x)$. □

چندجمله‌ای‌های $q(x)$ و $r(x)$ در قضیه‌ی ۶.۱.۱۱، را به ترتیب خارج قسمت و باقیمانده تقسیم $f(x)$ بر $g(x)$ می‌نامیم.

تعریف ۷.۱.۱۱. فرض کنید R حلقه باشد و $f(x) = a_۰ + a_۱x + \cdots + a_nx^n \in R[x]$. به ازای هر $r \in R$ تعریف می‌کنیم

$$f(r) = a_۰ + a_۱r + \cdots + a_nr^n.$$

گوییم r یک ریشه و یا یک صفر $f(x)$ است هرگاه $f(r) = ۰$.

در تعریف فوق می‌توانیم این چنین تصور کنیم که به جای x در $f(x)$، عضو r را قرار داده‌ایم و این گذاری را مقدار $f(x)$ در r بنامیم.

مثال ۸.۱.۱۱. اگر $f(x) = ۵ + ۴x - ۲x^۲ + x^۳$ و $g(x) = (x - ۱)(x^۲ + ۱)$ چندجمله‌ای‌هایی در $\mathbb{Z}[x]$ باشند، آن‌گاه

$$f(۳) = ۵ + (۴ \times ۳) - (۲ \times ۹) + ۲۷ = ۲۶$$

و

$$g(۳) = (۳ - ۱)(۳^۲ + ۱) = ۲۰.$$ □

مثال ۹.۱.۱۱. چندجمله‌ای $f(x) = x^۳ - x \in \mathbb{Z}_۶[x]$ را در نظر بگیرید. نشان دهید به ازای هر $a \in \mathbb{Z}_۶$، $f(a) = ۰$.

حل در $\mathbb{Z}_۶$ داریم

$$\begin{aligned} &f(۰) = ۰, \quad f(۱) = ۱ - ۱ = ۰, \quad f(۲) = ۸ - ۲ = ۶ = ۰, \\ &f(۳) = ۲۷ - ۳ = ۲۴ = ۰, \quad f(۴) = ۶۴ - ۴ = ۶۰ = ۰, \\ &f(۵) = ۱۲۵ - ۵ = ۱۲۰ = ۰. \end{aligned}$$

پس به ازای هر $a \in \mathbb{Z}_۶$، $f(a) = ۰$. □

از الگوریتم تقسیم مکرراً استفاده می‌کنیم. اگرچه آن را برای حلقه‌ی دلخواه یکدار ثابت کردیم. اما این الگوریتم بیشتر موقعی موثر است که حلقه‌ی R تعویض‌پذیر و یکدار باشد. دلیل این مطلب را تشریح می‌کنیم: فرض کنید چندجمله‌ای $f(x) = a_۰ + a_۱x + \cdots + a_nx^n \in R[x]$ داده شده باشد و $a \in R$، می‌خواهیم قادر باشیم که a را به جای x قرار دهیم و عضو $f(a) = a_۰ + a_۱a + \cdots + a_na^n \in R$ را به دست بیاوریم. اما باید برای انجام این کار دقت کنیم. فرض کنید a و b دو عضو در حلقه‌ی یکدار باشند و چندجمله‌ای $f(x) = (x - a)(x + b)$ را در نظر بگیرید. داریم

$$f(a) = (a - a)(a + b) = ۰(a + b) = ۰.$$

چون R یکدار است، به ازای هر $r \in R$، $rx = xr$، پس $f(x) = x^۲ + (b - a)x - ab$ و

$$۰ = f(a) = a^۲ + (b - a)a - ab = ba - ab$$

که قطعاً وقتی $ab \neq ba$ بی معنی است. در واقع چون حلقه‌ی R یکدار است، رابطه $xr = rx$ به ازای هر $r \in R$ برقرار است. پس جایگذاری $x = a$ در $f(x)$ وقتی صحیح است که a با تمامی ضرایب $f(x)$ تعویض شود. بنابراین اگر جایگذاری $x = a$ در هر چندجمله‌ای معنی داشته باشد، باید a در مرکز R باشد. در این حالت مشکلی پیش نمی‌آید.

تعریف ۱۰.۱.۱۱. فرض کنید R حلقه‌ای یکدار باشد، $f(x), g(x) \in R[x]$ و $g(x) \neq 0$. گوییم $g(x)$، $f(x)$ را عاد می‌کند یا $g(x)$ عاملی از $f(x)$ است و می‌نویسیم $g(x)|f(x)$ اگر $q(x) \in R[x]$ وجود داشته باشد که $f(x) = q(x)g(x)$.

قضیه ۱۱.۱.۱۱. اگر R حلقه‌ای تعویض‌پذیر و یکدار باشد و $f(x) \in R[x]$ و $a \in R$، آنگاه $q(x) \in R[x]$ وجود دارد که

$$f(x) = (x - a)q(x) + f(a).$$

اثبات. بنا به الگوریتم تقسیم با $g(x) = x - a$، چندجمله‌ای‌های یکتای $q(x), r(x) \in R[x]$ وجود دارند که $f(x) = (x - a)q(x) + r(x)$، که در آن $r(x) = 0$ یا $\deg r(x) < 1$. پس $r(x)$ چندجمله‌ای ثابت است؛ مثلاً $r(x) = d$. با قرار دادن a به جای x داریم $f(a) = (a - a)q(a) + d = d$ و حکم ثابت است. □

نتیجه ۱۲.۱.۱۱. فرض کنید R حلقه‌ی تعویض‌پذیر و یکدار باشد، $f(x) \in R[x]$ و $a \in R$. در این صورت a ریشه‌ای از f است اگر و تنها اگر $(x - a)|f(x)$.

اثبات. فرض کنید a ریشه‌ای از $f(x)$ باشد. بنا به قضیه‌ی ۱۱.۱.۱۱، و با توجه به این که $f(a) = 0$، داریم $f(x) = (x - a)q(x)$، یعنی $(x - a)|f(x)$. برعکس فرض کنید $(x - a)|f(x)$. پس چندجمله‌ای $q(x) \in R[x]$ وجود دارد که $f(x) = (x - a)q(x)$. بنابراین $f(a) = (a - a)q(a) = 0$ و a ریشه‌ای از f است. □

اگر R حلقه‌ی یکدار باشد و $a \in \mathrm{Cent}(R)$ نگاشت

$$\varphi_a : R[x] \longrightarrow R$$
$$\varphi_a[f(x)] = f(a)$$

را نگاشت مقدارياب (یا همریختی مقدارياب) گوییم. φ_a پوشاست، زیرا به ازای هر $b \in R$، داریم $\varphi_a[x + (b - a)] = b$. نشان می‌دهیم φ_a همریختی حلقه‌ای است. فرض کنید $f(x), g(x) \in R[x]$. با اضافه کردن جملات $0x^i$ (در صورت لزوم) به $f(x)$ یا $g(x)$ فرض می‌کنیم $f(x) = a_0 + a_1x + \cdots + a_nx^n$ و $g(x) = b_0 + b_1x + \cdots + b_nx^n$. داریم $f(x) + g(x) = (a_0 + b_0) + (a_1 + b_1)x + \cdots + (a_n + b_n)x^n$. بنابراین

$$\begin{aligned}
\varphi_a[f(x) + g(x)] &= (a_0 + b_0) + (a_1 + b_1)a + \cdots + (a_n + b_n)a^n \\
&= (a_0 + a_1a + \cdots + a_na^n) + (b_0 + b_1a + \cdots + b_na^n) \\
&= \varphi_a[f(x)] + \varphi_a[g(x)].
\end{aligned}$$

بنابراین φ_a جمع را حفظ می‌کند. اکنون $f(x) = c_0 + c_1x + \cdots + c_tx^t$ که در آن $c_k = \sum_{i=0}^{k} a_ib_{k-i}$. چون a در مرکز R قرار دارد ، داریم

$$\begin{aligned}
\varphi_a[f(x)]\varphi_a[g(x)] &= (a_0 + a_1a + \cdots + a_na^n)(b_0 + b_1a + \cdots + b_na^n) \\
&= a_0b_0 + (a_0b_1a + a_1ab_0) + \\
&\qquad (a_0b_2a^2 + a_1ab_1a + a_2a^2b_0) + \cdots + a_nb_na^{2n} \\
&= a_0b_0 + (a_0b_1 + a_1b_0)a + (a_0b_2 + a_1b_1 + a_2b_0)a^2 \\
&\qquad + \cdots + a_nb_na^{2n} \\
&= \varphi_a[f(x)g(x)],
\end{aligned}$$

یعنی φ_a ضرب را نیز حفظ می‌کند. بنابراین یک همریختی حلقه‌ای است. در اغلب کاربردها می‌خواهیم به ازای هر $a \in R$ و هر $f(x) \in R[x]$ مقدار $f(x)$ را در a بیابیم. این موفعی معنی دارد که R تعویض‌پذیر باشد، پس معمولاً R را تعویض‌پذیر فرض می‌کنیم.
حال فرض کنید R حلقه‌ای تعویض‌پذیر و یکدار باشد و $a \in R$. هسته‌ی همریختی مقدارباب عبارت است از

$$\ker \varphi_a = \{f(x) \in R[x] \mid f(a) = ۰\}.$$

چون $\ker \varphi_a$ ایدآل $R[x]$ است و $x - a \in \ker \varphi_a$، به ازای هر $g(x) \in R[x]$ داریم $(x-a)g(x) \in \ker \varphi_a$. بنابراین ایدآل تولید شده توسط $x - a$ در $\ker \varphi_a$ واقع است، یعنی $(x - a) \subseteq \ker \varphi_a$. حال اگر $g(x) \in \ker \varphi_a$. چندجمله‌ای $q(x) \in R[x]$ وجود دارد که $g(x) = (x - a)q(x) + g(a)$. اما $g(a) = ۰$، که نتیجه می‌دهد $g(x) \in (x - a)$. بنابراین $\ker \varphi_a = (x - a)$.

قضیه ۱۳.۱.۱۱. اگر R دامنه‌ای صحیح و $f(x) \in R[x]$ یک چندجمله‌ای ناصفر با درجه‌ی n باشد، آنگاه $f(x)$ در R حداکثر n ریشه دارد .

اثبات. به استقرا روی n حکم را ثابت می‌کنیم. اگر $n = ۰$، آنگاه $f(x)$ چندجمله‌ای ثابت است، مثلاً $f(x) = c \neq ۰$. در این حالت $f(x)$ ریشه‌ای ندارد. حال فرض کنید قضیه برای همه‌ی چندجمله‌ای‌های با درجه‌ی کمتر از n درست باشد، و $n > ۰$. اگر $f(x)$ در R ریشه ای نداشته باشد، قضیه ثابت است. پس فرض کنید $f(x)$ ریشه ای مثل $r \in R$ داشته باشد. بنا به نتیجه i ۱۲.۱.۱۱، $q(x) \in R[x]$ وجود دارد که $f(x) = (x - r)q(x)$. چون R دامنه‌ی صحیح است، $n = \deg f(x) = \deg(x - r) + \deg q(x)$ و $\deg q(x) = n - ۱$. اگر $f(x)$ ریشه‌ی دیگری مثل $r_۱ \in R$ داشته باشد، آنگاه $۰ = f(r_۱) = (r_۱ - r)q(r_۱)$. چون $r_۱ \neq r$ و R دامنه‌ی صحیح است، $q(r_۱) = ۰$، یعنی $r_۱$ ریشه‌ای از $q(x)$ است. در نتیجه هر ریشه‌ی دیگر $f(x)$ ریشه‌ای از $q(x)$ است. برعکس چون $f(x) = (x - r)q(x)$ هر ریشه‌ی $q(x)$ نیز ریشه‌ای از $f(x)$ است. بنا به فرض استقرا $q(x)$ حداکثر $n - ۱$ ریشه دارد. پس $f(x)$ حداکثر n ریشه دارد. □

به عنوان کاربردی از قضیه‌ی ۱۳.۱.۱۱، ثابت می‌کنیم گروه ضربی متشکل از اعضای ناصفر هر میدان متناهی دوری است. ابتدا به یک لم نیاز داریم ، که در مساله‌ی ۱۱، صفحه‌ی ۹۰، مطرح شده است. اما در این جا می‌خواهیم اثباتی دیگر ارائه‌ی کنیم:

لم ۱۴.۱.۱۱. فرض کنید G گروه متناهی با مرتبه‌ی n باشد، طوری که به ازای هر d که $d \mid n$، حداکثر یک زیر گروه از مرتبه‌ی d دارد. در این صورت G دوری است.

اثبات. فرض کنید $|G| = p_۱^{m_۱} p_۲^{m_۲} \cdots p_k^{m_k}$، که در آن p_iها اعداد اول متمایز و m_iها اعداد صحیح مثبت باشند. فرض کنید P_i، $۱ \leq i \leq k$، p_i-زیرگروه سیلوی G باشد. طبق فرض G حداکثر یک زیر گروه مرتبه‌ی $p_i^{m_i}$ دارد. پس P_i یکتا زیرگروه G از مرتبه‌ی $p_i^{m_i}$ است. بنابراین به ازای هر i، $۱ \leq i \leq k$، P_i در G نرمال است. پس G حاصل‌ضرب مستقیم زیر گروه‌های سیلوی خودش است، یعنی $G = P_۱ \times P_۲ \times \cdots \times P_k$. بنابراین اگر ثابت کنیم هر زیرگروه سیلوی G دوری است، نتیجه می‌شود که G دوری است. فرض کنید P یک p-زیرگروه دلخواه G با $|P| = p^m$ باشد. فرض کنید P دوری نباشد. طبق قضیه‌ی سیلو زیرگروه H با $|H| = p^{m-۱}$ وجود دارد. عضو دلخواه $a \in P - H$ را اختیار می‌کنیم. فرض کنید $O(a) = p^s$. در این صورت طبق قضیه‌ی سیلو H زیر گروهی مثل K از مرتبه‌ی p^s دارد. طبق فرض K یکتا زیرگروه G از مرتبه‌ی p^s است. از این‌رو $a \in \langle a \rangle = K \subseteq H$ که تناقض است. □

قضیه ۱۵.۱.۱۱. فرض کنید F میدان باشد. اگر G زیرگروه متناهی از گروه ضربی $F^\times$ باشد، آنگاه G دوری است. به ویژه اگر F متناهی باشد، آنگاه $F^\times$ دوری است.

اثبات. فرض کنید $|G| = n$. ثابت می‌کنیم G به ازای هر d که $d \mid n$، حداکثر یک زیرگروه از مرتبه‌ی d دارد. فرض کنید H و K دو زیرگروه G با مرتبه‌ی d باشند. اگر $a \in H$ یا $a \in K$، بنا به قضیه‌ی لاگرانژ، $a^d = ۱$. پس هر عضو $a \in H \cup K$ ریشه‌ای از چندجمله‌ای $f(x) = x^d - ۱ \in F[x]$ است. چون F دامنه‌ی صحیح است، $f(x)$ حداکثر d ریشه در F دارد. حال اگر $H \neq K$، آنگاه $|H \cup K| > d$، و تعداد ریشه‌های $f(x)$ بیش از d خواهد شد. پس $H = K$. □

این بخش را با معرفی مختصر حلقه‌ی چندجمله‌ای‌های n متغیره به پایان می‌بریم. فرض کنید $x_۱$ یک متغیر روی حلقه‌ی R باشد. می‌توان حلقه‌ی $R[x_۱]$ متشکل از چندجمله‌ای‌های با متغیر $x_۱$ و ضرایب در R را تشکیل داد. اکنون $R[x_۱]$ یک حلقه است. فرض کنید $x_۲$ یک متغیر روی حلقه‌ی $R[x_۱]$ باشد. $R[x_۱][x_۲]$ متشکل از چندجمله‌ای‌های با متغیر $x_۲$ و ضرایب در $R[x_۱]$ را تشکیل داد. این حلقه را

حلقه‌ی چندجمله‌ای‌های دو متغیره روی R می‌نامیم و با $R[x_۱, x_۲]$ نشان می‌دهیم.یک عضو دلخواه $R[x_۱, x_۲] = R[x_۱][x_۲]$ عبارت است از

$$u = a_۰(x_۱) + a_۱(x_۱)x_۲ + a_۲(x_۱)x_۲^۲ + \cdots + a_n(x_۱)x_۲^n = \sum_{j=۰}^{n} a_j(x_۱)x_۲^j,$$

که در آن $n \in \mathbb{N}$ و $a_j(x_۱) \in R[x_۱]$. چون به ازای هر j داریم $a_j(x_۱) = \sum_{i=۰}^{m} r_{ij}x_۱^i$، که در آن $m \in \mathbb{N}$ و $r_{ij} \in R$ (با اضافه کردن جملات $۰x_۱^i$، در صورت لزوم، به $a_j(x_۱)$ها فرض می‌کنیم توان $x_۱$ در $a_j(x_۱)$، به ازای هر j، برابر m است). بنابراین یک عضو دلخواه $R[x_۱, x_۲]$ به صورت

$$\begin{aligned} u &= \sum_{i=۰}^{m} r_{i۰}x_۱^i + \left(\sum_{i=۰}^{m} r_{i۱}x_۱^i\right)x_۲ + \\ &\quad \left(\sum_{i=۰}^{m} r_{i۲}x_۱^i\right)x_۲^۲ + \cdots + \left(\sum_{i=۰}^{m} r_{in}x_۱^i\right)x_۲^n \\ &= \sum_{i=۰}^{m}\sum_{j=۰}^{n} r_{ij}x_۱^i x_۲^j \\ &= \sum_{i,j} r_{ij}x_۱^i x_۲^j. \end{aligned}$$

بنابراین

$$R[x_۱, x_۲] = \left\{ \sum_{i,j} r_{ij}x_۱^i x_۲^j \;\middle|\; r_{ij} \in R \right\}.$$

به طور کلی می‌توان $R[x_۱, \ldots, x_n]$ را به صورت استقرایی تعریف کرد:

$$R[x_۱, x_۲, \ldots, x_n] = R[x_۱, x_۲, \ldots, x_{n-۱}][x_n].$$

مثل $R[x_۱, x_۲]$ می‌توان نشان داد

$$R[x_۱, x_۲, \ldots, x_n] = \left\{ \sum_{i_۱, i_۲, \ldots, i_n} r_{i_۱ i_۲ \cdots i_n} x_۱^{i_۱} x_۲^{i_۲} \cdots x_n^{i_n} \;\middle|\; r_{i_۱ i_۲ \cdots i_n} \in R \right\}.$$

تمرین‌ها

۱. $f(x) + g(x)$ و $f(x)g(x)$ را در هر حالت محاسبه کنید
(الف) در $\mathbb{Z}_۵[x]$، $f(x) = ۳ + ۲x + x^۲ + ۴x^۳$، $g(x) = ۱ + x^۲ + x^۳$
(ب) در $\mathbb{Z}_۷[x]$، $f(x) = ۵ + ۲x + x^۲ + x^۳$، $g(x) = ۲ + x + x^۲$

۲. نشان دهید در $\mathbb{Z}_p[x]$، p عدد اول ، داریم $(۱ + x)^p = ۱ + x^p$.

۳. چه تعداد چندجمله‌ای درجه‌ی n، در $\mathbb{Z}_m[x]$ وجود دارند. چه تعداد شان تکین هستند.

۴. (الف) همه‌ی ریشه‌های $(x - ۴)(x - ۵)$ را در $\mathbb{Z}_۶$ و $\mathbb{Z}_۳$ بیابید.
(ب) همه‌ی ریشه‌های $x - x^۳$ را در $\mathbb{Z}_۶$ و $\mathbb{Z}_۴$ بیابید.

۵. $x^۳ - ۴x + ۵$ را بر $۲x + ۱$ در $\mathbb{Q}[x]$ تقسیم کنید. چرا این تقسیم را نمیتوان در $\mathbb{Z}$ انجام داد.

۶. در هر حالت در $R[x]$ بنویسید $g(x) = q(x)f(x) + r(x)$ که در آن $r(x) = ۰$ یا $\deg r(x) < \deg f(x)$.
(الف) $g(x) = x^۵ + ۴x^۴ + x^۳ + ۵x^۲ + x + ۲$، $f(x) = x^۲ + x + ۱$ $R = \mathbb{Z}_۶$.

(ب) $g(x) = x^5 + 2x^4 + x^2 + x + 4$، $f(x) = x^2 + x + 2$، $R = \mathbb{Z}_7$.
(ج) $g(x) = 3x^3 + 2x^2 - x + 1$، $f(x) = x^2 + 2$، $R = \mathbb{Z}_8$.

۷. کدامیک از چندجمله‌ای‌های $x - 1$، $x + 1$، $x - 2$ عاملی از $x^4 - 2x^3 - x^2 + 3x - 2$ در $\mathbb{Z}[x]$ هستند.

۸. به ازای چه عدد اول p، $x + 2$ عاملی از $f(x) = 5x^4 - 3x^3 + 3x^2 + 4x - 1$ در $\mathbb{Z}_p[x]$ است.

۹. نشان دهید قضیه‌ی ۱۱.۱.۱۱، در حالتی که R تعویض‌ناپذیر باشد، درست نیست.

۱۰. (الف) نشان دهید $\mathbb{Z}_4[x]$ نامتناهی عضو یکه و نامتناهی عضو پوچ‌توان دارد.
(ب) عضوی از $\mathbb{Z}_4[x]$ بیابید که نه یکه و نه پوچ‌توان باشد.

۱۱. در حالت‌های زیر نشان دهید برای چندجمله‌ای $f(x) \in R[x]$، $f(a) = 0$ به ازای هر $a \in R$.
(الف) $f(x) = x^p - x$، $R = \mathbb{Z}_p$ (راهنمایی: قضیه‌ی فرما)
(ب) $f(x) = x^5 - x$، $R = \mathbb{Z}_{10}$
(ج) $f(x) = x^p - x$، $R = \mathbb{Z}_{2p}$، ($p > 2$ عدد اول)
(د) $f(x) = x^p - x$، $R = \mathbb{Z}_{3p}$، ($p > 3$ عدد اول)

۱۲. چندجمله‌ای $f(x) \in \mathbb{Z}_n[x]$ با درجه‌ی n بیابید که برای هر $a \in \mathbb{Z}_n$، $f(a) = 0$.

۱۳. فرض کنید p عدد اول باشد. نشان دهید در $\mathbb{Z}_p[x]$ داریم

$$x^p - x = x(x-1)(x-2)\cdots(x-p+1).$$

۱۴. ریشه‌های گویای $f(x)$ را در $\mathbb{Q}[x]$ بیابید. $f(x)$ را تا حد امکان در $\mathbb{Q}[x]$ تجزیه کنید
(الف) $f(x) = 4x^4 + x^3 - 3x^2 + 4x - 3$
(ب) $f(x) = 4x^4 + 4x^3 + 3x^2 - x - 1$
(ج) $f(x) = x^4 - x^3 - x^2 - x - 2$
(د) $f(x) = x^5 - x^4 + x^3 - x^2 + x - 1$
(هـ) $f(x) = x^4 - \frac{5}{2}x^3 + \frac{5}{2}x^2 - \frac{5}{2}x + \frac{3}{2}$

۱۵. فرض کنید R دامنه‌ی صحیح و $f(x)$ و $g(x)$ چندجمله‌ای‌های در $R[x]$ باشند که یا صفرند و یا درجه‌ی آن‌ها حداکثر n است. اگر $n + 1$ عضو متمایز a_1، ...، a_{n+1} وجود داشته باشند که $f(a_i) = g(a_i)$، $i = 1, \ldots, n + 1$ نشان دهید $f(x) = g(x)$.

۱۶. نشان دهید ایدآل $(2, x)$ در $\mathbb{Z}[x]$ اصلی نیست؛ و نتیجه بگیرید $\mathbb{Z}[x]$ دامنه‌ی ایدآل اصلی نیست.

۱۷. نشان دهید $\mathbb{Z}_p$ را می‌توان در یک میدان نامتناهی نشاند.

۱۸. فرض کنید I ایدآلی از حلقه‌ی R باشد و $\bar{I} = \{f[x] \in R[x] \mid f(0) \in I\}$. نشان دهید $\bar{I}$ ایدآلی از $R[x]$ است و $R[x]/\bar{I} \cong R/I$.

۱۹. فرض کنید R حلقه‌ی یکدار باشد. ثابت کنید $R[x]/(x) \cong R$.

۲۰. فرض کنید F میدان و $\alpha : F[x] \longrightarrow F[x]$ یک خودریختی باشد طوری که برای هر $a \in F$، $\alpha(a) = a$. نشان دهید اعضای $a, b \in F$ وجود دارند که $\alpha(x) = ax + b$.

۲.۱۱ تجزیه‌ی چندجمله‌ای‌ها روی یک میدان

اگر F یک میدان باشد، چندجمله‌ای ناصفر $p(x) \in F[x]$ را چندجمله‌ای تحویل‌ناپذیر روی F (یا روی $F[x]$) می‌نامیم هرگاه
(الف) $\deg p(x) \geq 1$.
(ب) اگر در $F[x]$، $p(x) = f(x)g(x)$، آنگاه یا $\deg f(x) = 0$ آیا $\deg g(x) = 0$.
شرط (الف) بیان می‌کند که یک چندجمله‌ای تحویل‌ناپذیر یکه نیست (شبیه شرط اول بودن در $\mathbb{Z}_p$ که $p \geq 2$، برای هر عدد اول p).

مثال ۱.۲.۱۱. فرض کنید F یک میدان باشد، نشان دهید چندجمله‌ای‌های خطی روی F تحویل‌ناپذیرند.

حل فرض کنید $p(x) = ax + b \in F[x]$، $a \neq 0$ و در $F[x]$، $p(x) = f(x)g(x)$. چون F دامنه‌ی صحیح است، $1 = \deg p(x) = \deg f(x) + \deg g(x)$. چون $\deg f(x) \geq 0$ و $\deg g(x) \geq 0$ اعداد صحیح هستند یکی از آن‌ها باید برابر صفر باشد. □

فرض کنید F میدان باشد. اگر $p(x)$ در $F[x]$ تحویل‌ناپذیر باشد و $a \in F$، $a \neq 0$، آنگاه $ap(x)$ در F تحویل‌ناپذیر است. زیرا اگر در $F[x]$، $ap(x) = f(x)g(x)$، آنگاه $p(x) = (a^{-1}f(x))g(x)$. چون $p(x)$ تحویل‌ناپذیر است، یا $\deg g(x) = 0$ یا $\deg f(x) = \deg[a^{-1}f(x)] = 0$. پس $ap(x)$ برای هر $a \in F$، $a \neq 0$ تحویل‌ناپذیر است. اکنون به ویژه اگر a ضریب پیشرو ی $p(x)$ باشد، آنگاه $a^{-1}p(x)$ یک چندجمله‌ای تکین تحویل‌ناپذیر است. بنابراین، در $F[x]$، معمولاً بدون کم شدن چیزی از کلیت با چندجمله‌ای‌های تکین تحویل‌ناپذیر کار می‌کنیم.
هر چندجمله‌ای خطی در $F[x]$ به صورت $p(x) = ax + b$، $a \neq 0$ است و بنابراین ریشه‌ی آن در F، عبارت است از $a^{-1}b$.
چندجمله‌ای‌های تحویل‌ناپذیر با درجه‌ی بیشتر یا مساوی ۲ نمی‌تواند در F ریشه‌ای داشته باشند. اثبات قضیه‌ی بعد ساده است.

قضیه ۲.۲.۱۱. فرض کنید F میدان باشد و $p(x) \in F[x]$، $\deg p(x) \geq 2$.
(الف) اگر $p(x)$ روی F تحویل‌ناپذیر باشد، آنگاه $p(x)$ در Fریشه‌ای ندارد.
(ب) اگر $\deg p(x)$ برابر ۲ یا ۳ باشد، آنگاه $p(x)$ روی F تحویل‌ناپذیر است اگر و تنها اگر $p(x)$ در F ریشه‌ای نداشته باشد.

اثبات. (الف) اگر $a \in F$ ریشه‌ای از $p(x)$ باشد، آنگاه $p(a) = 0$ و بنا به نتیجه‌ی ۱۲.۱.۱۱، $q(x) \in F[x]$ وجود دارد که $p(x) = (x - a)q(x)$. چون $\deg p(x) \geq 2$ و $\deg q(x) \geq 1$، $p(x)$ تحویل‌پذیر است، که این متناقض با فرض است.
(ب) فرض کنید $p(x) = f(x)g(x)$ ریشه‌ای در F نداشته باشد. در این صورت $f(x)$ و $g(x)$ نیز ریشه‌ای در F ندارند و بنابراین $\deg f(x) \neq 1$ و $\deg g(x) \neq 1$. اما چون $\deg p(x) = \deg f(x) + \deg g(x)$ برابر ۲ و یا ۳ است باید یا $\deg f(x) = 0$ و یا $\deg g(x) = 0$. در نتیجه $p(x)$ تحویل‌ناپذیر است. عکس مطلب از (الف) نتیجه می‌شود. □

مثال ۳.۲.۱۱. $x^2 + 1$ روی $\mathbb{R}[x]$ تحویل‌ناپذیر است زیرا ریشه‌ای در $\mathbb{R}$ ندارد. □

مثال ۴.۲.۱۱. (الف) $f(x) = x^2 + x + 1 \in \mathbb{Z}_2[x]$ روی $\mathbb{Z}_2$ تحویل‌ناپذیر است، زیرا $f(0) = 1$ و $f(1) = 1$. بنابراین $f(x)$ روی $\mathbb{Z}_2$ ریشه ای ندارد.
(ب) $g(x) = x^3 + 2x + 1 \in \mathbb{Z}_3[x]$ روی $\mathbb{Z}_3$ تحویل‌ناپذیر است زیرا $g(0) = 1$، $g(1) = 1$، $g(2) = 1$. بنابراین $g(x)$ روی $\mathbb{Z}_2$ ریشه‌ای ندارد. □

قضیه‌ی ۲.۲.۱۱، برای چندجمله‌ای‌های با درجه‌ی بیش از ۳ درست نیست، مثلاً

$$f(x) = x^4 + 3x^2 + 2 = (x^2 + 1)(x^2 + 2)$$

روی $\mathbb{R}$ تحویل‌پذیر است ولی هیچ ریشه‌ای در $\mathbb{R}$ ندارد.

قضیه ۵.۲.۱۱. فرض کنید $f(x) = a_0 + a_1x + \cdots + a_nx^n \in \mathbb{Z}[x]$، که در آن $a_0 \neq 0$، $a_n \neq 0$. اگر $\frac{c}{d} \in \mathbb{Q}$ ریشه‌ای از $f(x)$ باشد که $\gcd\{c, d\} = 1$، آنگاه

$$c|a_0, \quad d|a_n.$$

اثبات. داریم $f\left(\frac{c}{d}\right) = a_0 + a_1\frac{c}{d} + \cdots + a_n\left(\frac{c}{d}\right)^n = 0$. با ضرب طرفین تساوی در d^n به دست می‌آوریم

$$0 = a_0d^n + a_1cd^{n-1} + \cdots + a_{n-1}c^{n-1}d + a_nc^n$$

چون c در همه‌ی جملات تساوی بجز اولین ظاهر شده، $c|a_0d^n$. پس $c|a_0$، زیرا $\gcd\{c, d^n\} = 1$. به طریق مشابه $d|a_n$. □

مثال ۶.۲.۱۱. اگر m عدد صحیح مثبت باشد که مربع هیچ عدد صحیح نیست. نشان دهید $\sqrt{m}$ گویا نیست.

حل اگر $\sqrt{m}=\frac{c}{d}$ عدد گویا باشد، باید در چندجمله‌ای $x^۲-m\in\mathbb{Z}[x]$ صدق کند. بنا به قضیه‌ی ۵.۲.۱۱، $c|m$ و $d|۱$، یعنی $d=\pm ۱$. بنابراین $\sqrt{m}=\pm c$. پس m مربع عدد صحیح است. این متناقض با فرض است. □

وقتی در مورد تحویل‌ناپذیری بحث می‌کنیم میدان ضرایب چندجمله‌ای باید مشخص باشد. مثلاً چندجمله‌ای $f(x)=x^۲-۲$ روی $\mathbb{Q}$ تحویل‌ناپذیر و روی $\mathbb{R}$ تحویل‌پذیر است؛ زیرا $f(x)=(x-\sqrt{۲})(x+\sqrt{۲})$ و $\sqrt{۲}\notin\mathbb{Q}$.
اگر F یک میدان باشد، چندجمله‌ای‌های تحویل‌ناپذیر در $F[x]$ مشابه عناصر اول $\mathbb{Z}$ هستند. چون هیچ راهی برای مشخص کردن همه‌ی اعداد اول وجود ندارد ، هر توصیف کامل برای همه‌ی چندجمله‌ای‌های تحویل‌ناپذیر در $F[x]$ بسیار مشکل به نظر می‌آید (البته در صورتی که چنین توصیفی وجود داشته باشد). اما در حالتی که $F=\mathbb{C}$ یا $F=\mathbb{R}$ چنین توصیفی وجود دارد. این توصیف به قضیه‌ی تعمیمی که اولین بار در سال ۹۹۷۱ گاوس آن را در پایان نامه دکتری خود ثابت کرد بستگی دارد، آن قضیه‌ی اساسی جبر است:

قضیه ۷.۲.۱۱. (قضیه‌ی اساسی جبر) اگر $f(x)\in\mathbb{C}[x]$ یک چندجمله‌ای غیرثابت باشد، آنگاه $f(x)$ ریشه‌ای در $\mathbb{C}$ دارد. □

تاکنون اثبات ساده‌ای از این قضیه انجام نشده است و اغلب اثبات‌های انجام شده مبتنی بر زوش‌های آنالیزی هستند. در فصل ۱۴ بخش ۷ اثباتی جبری از این قضیه را ارائه می‌کنیم. با استفاده از قضیه‌ی اساسی جبر می‌توان توصیف کامل چندجمله‌ای‌های تحویل‌ناپذیر در $\mathbb{C}[x]$ را به دست آورد:

قضیه ۸.۲.۱۱. (الف) اگر $f(x)\in\mathbb{C}[x]$ و $\deg f(x)=n\geq ۱$، آنگاه $f(x)$ به صورت زیر روی $\mathbb{C}$ کاملا تجزیه می‌شود

$$f(x)=a(x-a_۱)(x-a_۲)\cdots(x-a_n)$$

که در آن a ضریب پیشرو ی $f(x)$ است و $a_۱$، $a_۲$، ...، a_n ریشه‌های (نه لزوماً متمایز) $f(x)$ روی $\mathbb{C}$ هستند.
(ب) تنها چندجمله‌ای‌های تحویل‌ناپذیر روی $\mathbb{C}$ چندجمله‌ای‌های خطی هستند.

اثبات. (الف) به استقرا روی $n=\deg f(x)$ حکم را ثابت می‌کنیم. اگر $n=۱$، آنگاه $f(x)=ax+b=a(x+a^{-۱}b)$ و بنابراین $a_۱=-a^{-۱}b$. حال فرض کنید $n>۱$ و قضیه برای همه‌ی چندجمله‌ای‌های با درجه‌ی کمتر از n درست باشد. بنا به قضیه‌ی اساسی جبر ریشه‌ی $a_۱$ از $f(x)$ وجود دارد و بنابراین چندجمله‌ای $q(x)$ وجود دارد که $f(x)=(x-a_۱)q(x)$ که در آن $\deg q(x)=n-۱$. بنا به فرض استقرا $q(x)$ به صورت $g(x)=a(x-a_۲)\cdots(x-a_n)$ است. پس $f(x)=a(x-a_۱)(x-a_۲)\cdots(x-a_n)$ که به صورت مورد نظر است.
(ب) از قسمت (الف) واضح است. □

قضیه‌ی اساسی جبر وجود ریشه‌های یک چندجمله‌ای مختلط را تضمین می‌کند، اما روشی برای یافتن آن‌ها ارائه نمی‌دهد. در حالت کلی یافتن ریشه‌ها مشکل است.
فرض کنید $q(x)=ax^۲+bx+c$، $a\neq ۰$،یک چندجمله‌ای درجه‌ی ۲ حقیقی باشد. ریشه‌های $q(x)$ از فرمول درجه‌ی دوم

$$u=\frac{۱}{۲a}\left[-b\pm\sqrt{b^۲-۴ac}\right]$$

داده می‌شوند. عبارت $b^۲-۴ac$ را دلتای $q(x)$ گویند. اگر $q(x)$ تحویل‌ناپذیر باشد، آنگاه ریشه‌ی حقیقی ندارد. بنابراین $b^۲-۴ac<۰$ و دو ریشه‌ی غیرحقیقی مختلط، که مزدوج یکدیگر هستند ، برای $q(x)$ وجود دارد :

$$u=\frac{۱}{۲a}\left[-b+i\sqrt{۴ac-b^۲}\right],\quad \bar{u}=\frac{۱}{۲a}\left[-b-i\sqrt{۴ac-b^۲}\right].$$

عکس مطلب نیز درست است. اگر u عدد غیرحقیقی مختلط دلخواهی باشد، u، $\bar{u}$ ریشه‌های یک چندجمله‌ای حقیقی درجه‌ی ۲ هستند. در واقع ضرایب چندجمله‌ای درجه‌ی ۲ (تکین)

$$(x-u)(x-\bar{u})=x^۲-(u+\bar{u})-u\bar{u}$$

حقیقی است ($u\bar{u} = |u|^۲$ و $u + \bar{u} = ۲\mathrm{Re}(u)$، که در آن $\mathrm{Re}(u)$ قسمت حقیقی u است). بنابراین روی $\mathbb{R}$ تحویل‌ناپذیر است، چرا که ریشه‌های آن اعداد مختلط u و $\bar{u}$ هستند. فرض کنید $f(x) = a_۰ + a_۱x + a_۲x^۲ + \cdots + a_nx^n \in \mathbb{R}[x]$. برای هر عدد مختلط u داریم

$$\begin{aligned}\overline{f(u)} &= \overline{a_۰ + a_۱u + a_۲u^۲ + \cdots + a_nu^n} \\ &= \bar{a}_۰ + \bar{a}_۱\bar{u} + \bar{a}_۲\bar{u}^۲ + \cdots + \bar{a}_n\bar{u}^n \\ &= a_۰ + a_۱\bar{u} + a_۲\bar{u}^۲ + \cdots + a_n\bar{u}^n \\ &= f(\bar{u}).\end{aligned}$$

پس اگر u ریشه‌ای از $f(x)$ باشد، آن‌گاه

$$۰ = \bar{۰} = \overline{f(u)} = f(\bar{u}).$$

در نتیجه $\bar{u}$ نیز ریشه‌ای از $f(x)$ است. بنابراین ریشه‌های $f(x)$ دو بدو مزدوج مختلط هستند. به ویژه اگر درجه‌ی $f(x)$ فرد باشد، آن‌گاه $f(x)$ حداقل یک ریشه‌ی حقیقی دارد. بنا به قضیه‌ی ۸.۲.۱۱، $f(x)$ در $\mathbb{C}[x]$ به صورت زیر تجزیه می‌شود

$$a(x - r_۱)(x - r_۲)\cdots(x - r_m)(x - u_۱)(x - \bar{u}_۱)\cdots(x - u_k)(x - \bar{u}_k),$$

که در آن a ضریب پیشرو ی $f(x)$ است، $r_۱$، ...، r_m ریشه‌های حقیقی و $u_۱$، $\bar{u}_۱$، ...، u_k، $\bar{u}_k$، ریشه‌های غیرحقیقی $f(x)$ هستند. چندجمله‌ای

$$q_j(x) = (x - u_j)(x - \bar{u}_j) = x^۲ - (u_j + \bar{u}_j)x^۲ + u_j\bar{u}_j$$

یک چندجمله‌ای درجه‌ی دو حقیقی تحویل‌ناپذیر (روی $\mathbb{R}$) است. بنابراین

$$f(x) = a(x - r_۱)(x - r_۲)\cdots(x - r_m)q_۱(x)\cdots q_k(x).$$

پس ثابت کرده‌ایم:

قضیه ۹.۲.۱۱. اگر $f(x) \in \mathbb{R}[x]$ چندجمله‌ای غیرثابت باشد، آن‌گاه می‌توان نوشت

$$f(x) = a(x - r_۱)(x - r_۲)\cdots(x - r_m)q_۱(x)q_۲(x)\cdots q_k(x)$$

که در آن $r_۱$، $r_۲$، ...، r_m ریشه‌های حقیقی $f(x)$ (در صورت وجود) و $q_۱(x)$، $q_۲(x)$، ...، $q_k(x)$ چندجمله‌ای‌های تکین تحویل‌ناپذیر حقیقی درجه‌ی دو (ممکن است چنین عواملی وجود نداشته باشند) هستند و a ضریب پیشرو ی $f(x)$ است. □

نتیجه ۱۰.۲.۱۱. چندجمله‌ای‌های تحویل‌ناپذیر در $\mathbb{R}[x]$ یا خطی و یا درجه‌ی ۲ هستند. □

تا حالا چندجمله‌ای‌های تحویل‌ناپذیر روی $\mathbb{C}[x]$ و $\mathbb{R}[x]$ را کاملاً توصیف کرده‌ایم. اکنون چندجمله‌ای‌های روی $\mathbb{Q}[x]$ را در نظر می‌گیریم. اما وضعیت در $\mathbb{Q}[x]$ بسیار مشکل‌تر است. بسیاری از سوالات در مورد $\mathbb{Q}[x]$ به سوالاتی در $\mathbb{Z}[x]$ برمی‌گردد. در واقع اگر $f(x) \in \mathbb{Q}[x]$ و a کوچک‌ترین مضرب مشترک مخرج همه‌ی کسرهای ضرایب $f(x)$ باشد، آن‌گاه $af(x) \in \mathbb{Z}[x]$.
گاهی اوقات برای مشاهده‌ی تحویل‌ناپذیری $f(x) \in \mathbb{Z}[x]$ می‌توانیم چندجمله‌ای متناظر آن در $\mathbb{Z}_p[x]$ (به ازای یک عدد اول p) را در نظر بگیریم. به ازای هر عدد صحیح a فرض کنید $\bar{a}$ نشان دهنده‌ی رده‌ی مانده‌ای a در $\mathbb{Z}_p$ باشد. اگر

$$f(x) = a_۰ + a_۱x + a_۲x^۲ + \cdots + a_nx^n \in \mathbb{Z}[x]$$

چندجمله‌ای

$$\overline{f(x)} = \bar{a}_۰ + \bar{a}_۱x + \bar{a}_۲x^۲ + \cdots + \bar{a}_nx^n \in \mathbb{Z}_p[x]$$

را تحویل $f(x)$ به پیمانه‌ی p می‌نامیم. به سادگی می‌توان دید (نشان دهید) که نگاشت $\mathbb{Z}[x] \longrightarrow \mathbb{Z}_p[x]$ با ضابطه‌ی $f(x) \mapsto \overline{f(x)}$ یک همریختی حلقه‌ای پوشاست؛ یعنی

$$\overline{f(x) + g(x)} = \overline{f(x)} + \overline{g(x)} \quad \text{و} \quad \overline{f(x)g(x)} = \overline{f(x)}\ \overline{g(x)}.$$

قضیه ۱۱.۲.۱۱. (لم گاوس) فرض کنید در $\mathbb{Z}[x]$ داریم $f(x)=g(x)h(x)$. اگر عدد اول p همه‌ی ضرایب $f(x)$ را عدد کند، آنگاه p یا همه‌ی ضرایب $g(x)$ یا همه‌ی ضرایب $h(x)$ را عاد می‌کند.

اثبات. طبق فرض در $\mathbb{Z}_p[x]$، $\overline{f(x)}=۰$. در نتیجه $\overline{f(x)}=\overline{g(x)}\,\overline{h(x)}=۰$. چون $\mathbb{Z}_p[x]$ دامنه‌ی صحیح است پس $\overline{g(x)}=۰$ یا $\overline{h(x)}=۰$. اما $\overline{g(x)}=۰$ در $\mathbb{Z}_p[x]$، یعنی هر ضرایب آن در $\mathbb{Z}_p$ صفر است. بنابراین p هر ضرایب $g(x)$ را عاد می‌کند. □

قضیه ۱۲.۲.۱۱. فرض کنید $f(x)\in\mathbb{Z}[x]$ چندجمله‌ای غیر ثابت باشد.
(الف) اگر $f(x)=g(x)h(x)$، که در آن $g(x),h(x)\in\mathbb{Q}[x]$، آنگاه چندجمله‌ای‌های $g_۰(x),h_۰(x)\in\mathbb{Z}[x]$ وجود دارند که $f(x)=g_۰(x)h_۰(x)$. به علاوه داریم $\deg g_۰(x)=\deg g(x)$ و $\deg h_۰(x)=\deg h(x)$.
(ب) $f(x)$ در $\mathbb{Q}[x]$ تحویل‌ناپذیر است اگر و تنها اگر تجزیه‌ی سره‌ای در $\mathbb{Z}[x]$ نداشته باشد.

اثبات. (الف) فرض کنید a و b به ترتیب کوچک‌ترین مضرب مشترک مخرج کسرهای ضرایب $g(x)$ و $h(x)$ باشند. قرار دهید $g_۱(x)=ag(x)$ و $h_۱(x)=bh(x)$. آنگاه $g_۱(x),h_۱(x)\in\mathbb{Z}[x]$. پس

$$abf(x)=g_۱(x)h_۱(x)$$

معادله‌ای در $\mathbb{Z}[x]$ است. اگر p عدد اولی باشد که $p|ab$، آنگاه بنا به لم گاوس p یا همه‌ی ضرایب $g_۱(x)$ را عاد می‌کند و یا همه‌ی ضرایب $h_۱(x)$ را عاد می‌کند. بنابراین با حذف p معادله‌ی جدید دیگری در $\mathbb{Z}[x]$ به دست می‌آوریم

$$\frac{ab}{p}f(x)=g_۲(x)h_۲(x).$$

با انجام این عمل برای همه‌ی اعداد اول که ab را عاد می‌کنند درنهایت به تجزیه

$$f(x)=g_k(x)h_k(x)$$

در $\mathbb{Z}[x]$ خواهیم رسید. چون به ازای هر $۱\le i\le k$، $\deg g(x)=\deg g_i(x)$ و $\deg h(x)=\deg h_i(x)$، (الف) حاصل می‌شود.
(ب) اگر $f(x)$ در $\mathbb{Q}[x]$ تحویل‌ناپذیر باشد، آنگاه هیچ تجزیه‌ی سره‌ای در $\mathbb{Q}[x]$ و بنابراین در $\mathbb{Z}[x]$ ندارد. عکس مطلب از (الف) نتیجه می‌شود. □

اگر یک چندجمله‌ای در $\mathbb{Z}[x]$ تجزیه‌ی سره‌ای نداشته باشد، نمی‌گوییم در $\mathbb{Z}[x]$ تحویل‌ناپذیر است. دلیل این مطلب این است که چندجمله‌ای‌هایی مثل $۵x-۵=۵(x-۱)$ را با این که در $\mathbb{Z}[x]$ تجزیه‌ی سره‌ای ندارند تحویل‌ناپذیر نمی‌گوییم. مفهوم تحویل‌ناپذیری در یک دامنه‌ی صحیح را بعداً، در فصل ۱۲، به طور مفصل بررسی می‌کنیم.
فرض کنید $f(x)\in\mathbb{Q}[x]$. بنابراین اعداد صحیح $a\neq۰$ وجود دارد که $af(x)\in\mathbb{Z}[x]$ (a می‌تواند هر مضرب مشترک مخرج‌های کسرهای ضرایب $f(x)$ باشد). دیدیم $f(x)$ در $\mathbb{Q}[x]$ تحویل‌ناپذیر است اگر و تنها اگر $af(x)$ در $\mathbb{Q}[x]$ تحویل‌ناپذیر باشد. پس قضیه‌ی ۱۲.۲.۱۱، مساله‌ی نشان دادن تحویل‌ناپذیری $f(x)$ در $\mathbb{Q}[x]$ را به مساله‌ی نشان دادن این که $af(x)$ در $\mathbb{Z}[x]$ تجزیه‌ی سره‌ای ندارد تبدیل می‌کند.

مثال ۱۳.۲.۱۱. نشان دهید $f(x)=x^۵+۲x^۲+۱$ در $\mathbb{Q}[x]$ تحویل‌ناپذیر است.

حل بنا به قضیه‌ی ۱۲.۲.۱۱، کافی است نشان دهیم $f(x)$ در $\mathbb{Z}[x]$ تجزیه‌ی سره‌ای ندارد. طبق قضیه‌ی ۵.۲.۱۱، تنها کاندیداهای ریشه‌ی گویا برای $f(x)$ عبارت‌اند از ±۱، که خیچ‌کدام ریشه‌ی $f(x)$ نیستند، یعنی $f(x)$ هیچ ریشه‌ی گویایی ندارد. بنابراین اگر $f(x)$ در $\mathbb{Z}[x]$ به طور سره تجزیه شود، باید به یک چندجمله‌ای درجه‌ی ۲ و یک چندجمله‌ای درجه‌ی ۳ تجزیه شود. به علاوه چون $f(x)$ تکین است عوامل را می‌توان تکین در نظر گرفت:

$$f(x)=(x^۵+۲x^۲+۱)=(x^۲+ax+b)(x^۳+cx^۲+dx+e)$$

که در آن a، b، c، d و e اعداد صحیح‌اند. با ضرب عوامل سمت راست تساوی و متحد قرار دادن دو طرف تساوی داریم

$$a+c=۰,\quad d+ac+b=۰,\quad e+ad+bc=۲,\quad ae+bd=۰,\quad be=۱.$$

از آخرین معادله داریم $b = e = \pm ۱$. از این‌رو از معادله‌ی قبل از آن داریم $a + d = ۰$. چون $a + c = ۰$ معادله‌ی دوم نتیجه می‌دهد $-a - a^۲ + b = ۰$. پس a ریشه‌ی صحیح معادله‌ی $x^۲ + x - b = ۰$ است که در آن $b = \pm ۱$. اما تنها کاندیداهای ریشه‌ی گویا برای این معادله، ± ۱ است که هیچ‌کدام وقتی $b = ۱$ یا $b = -۱$ در آن صدق نمی‌کنند. بنابراین چنین تجزیه‌ای برای $f(x)$ وجود ندارد. پس $f(x)$ در $\mathbb{Q}[x]$ تحویل‌ناپذیر است. □

قضیه ۱۴.۲.۱۱. فرض کنید $f(x) \in \mathbb{Z}[x]$، عدد اول p وجود داشته باشد که
(الف) p ضریب پیشرو ی $f(x)$ را عدد نکند یعنی $\deg \overline{f(x)} = \deg f(x)$
(ب) $\overline{f(x)} \in \mathbb{Z}_p[x]$ روی $\mathbb{Z}_p$ تحویل‌ناپذیر باشد.
در این صورت $f(x)$ در $\mathbb{Q}[x]$ تحویل‌ناپذیر است.

اثبات. فرض کنید $f(x)$ روی $\mathbb{Q}[x]$ تحویل‌پذیر باشد. بنا به قضیه‌ی ۱۲.۲.۱۱، تجزیه‌ی سره‌ی $f(x) = g(x)h(x)$ در $Z[x]$ وجود دارد. بنابراین $\overline{f(x)} = \overline{g(x)h(x)}$ و داریم

$$\deg(\overline{g(x)}) \leq \deg g(x) < \deg f(x) = \deg \overline{f(x)}.$$

به همین نحو $\deg \overline{h(x)} < \deg \overline{f(x)}$، این یعنی $\overline{f(x)}$ روی $\mathbb{Z}_p[x]$ تحویل‌پذیر است که تناقض است. □

توجه کنید اگر $f(x)$ تکین باشد، شرط (الف) در قضیه‌ی ۱۴.۲.۱۱، همواره برقرار است.

مثال ۱۵.۲.۱۱. نشان دهید چندجمله‌ای $f(x) = \frac{۵}{۷}x^۳ - \frac{۱}{۲}x + ۱ \in \mathbb{Q}[x]$ روی $\mathbb{Q}$ تحویل‌ناپذیر است.

حل کوچک‌ترین مضرب مشترک مخرج کسرهای ضرایب $f(x)$ برابر ۱۴ است. پس قرار می‌دهیم $g(x) = ۱۰x^۳ - ۷x + ۱۴$. بنابراین $g(x) = ۱۴f(x)$. اکنون در $\mathbb{Z}_۳[x]$ داریم $\overline{g(x)} = \overline{۱۰}x^۳ - \overline{۷}x + \overline{۱۴} = x^۳ - x + \bar{۲}$، چون $\overline{g(\bar{۰})} = \bar{۲}$، $\overline{g(\bar{۱})} = \bar{۲}$ و $\overline{g(\bar{۲})} = \bar{۲}$، پس $\overline{g(x)}$ هیچ ریشه‌ای در $\mathbb{Z}_۳$ ندارد و بنابراین، بنا به قضیه‌ی ۲.۲.۱۱، روی $\mathbb{Z}_۳[x]$ تحویل‌ناپذیر است (زیرا $\deg \overline{g(x)} = ۳$). بنابراین $g(x)$ و در نتیجه $f(x)$ در $\mathbb{Q}[x]$ تحویل‌ناپذیر است. □

مثال ۱۶.۲.۱۱. نشان دهید چندجمله‌ای $f(x) = x^۴ + ۲x^۳ + ۲x^۲ - x + ۱$ روی $\mathbb{Q}$ تحویل‌ناپذیر است.

حل در $\mathbb{Z}_۲[x]$ داریم $\overline{f(x)} = x^۴ + x + ۱$. این چندجمله‌ای در $\mathbb{Z}_۲$ ریشه ای ندارد. بنابراین اگر $\overline{f(x)}$ تحویل‌پذیر باشد، باید به حاصل‌ضرب دو چندجمله‌ای درجه‌ی ۲ تجزیه شود. اما چندجمله‌ای‌های درجه‌ی دو روی $\mathbb{Z}_۲$ عبارت‌اند از

$$x^۲, \quad ۱ + x^۲, \quad x + x^۲, \quad ۱ + x + x^۲.$$

سه چندجمله‌ای اول در $\mathbb{Z}_۲$ ریشه دارند؛ پس $۱ + x + x^۲$ تنها چندجمله‌ای تحویل‌ناپذیر درجه‌ی دو روی $\mathbb{Z}_p$ است و

$$\overline{f(x)} = (x^۲ + x + ۱)^۲ = x^۴ + x^۲ + ۱ \neq \overline{f(x)},$$

که تناقض است. از این‌رو $\overline{f(x)}$ روی $\mathbb{Z}_۲[x]$ تحویل‌ناپذیر است. در نتیجه $f(x)$ روی $\mathbb{Q}[x]$ تحویل‌ناپذیر است. □

محک دیگر تحویل‌ناپذیری روی $\mathbb{Q}$ را آیزنشتاین، یکی از دانشجویان گاوس، اثبات کرد:

قضیه ۱۷.۲.۱۱. (محک آیزنشتاین) فرض کنید $f(x) = a_۰ + a_۱x + \cdots + a_nx^n$، $n \geq ۱$،یک چندجمله‌ای در $\mathbb{Z}[x]$ باشد. اگر p یک عدد اول باشد که
(الف) $p|a_i$، $i = ۰, ۱, \ldots, n - ۱$.
(ب) $p \nmid a_n$.
(ج) $p^۲ \nmid a_۰$.
در این صورت $f(x)$ روی $\mathbb{Q}[x]$ تحویل‌ناپذیر است.

اثبات. فرض کنید چنین نباشد و تجزیه‌ی سره‌ی $f(x)=g(x)h(x)$ از $f(x)$ را در $\mathbb{Z}[x]$ در نظر بگیرید. فرض کنید

$$g(x)=b_۰+b_۱x+\cdots+b_mx^m,\quad h(x)=c_۰+c_۱x+\cdots+c_tx^t.$$

بنابراین داریم

$$\begin{aligned}
a_۰ &= b_۰c_۰\\
a_۱ &= b_۰c_۱+b_۱c_۰\\
&\cdots\\
a_k &= b_kc_۰+b_{k-۱}c_۱+\cdots+b_۰c_k\\
&\cdots\\
a_n &= b_mc_t.
\end{aligned}$$

چون p، $a_۰=b_۰c_۰$ را عاد می‌کند و $p^۲$، $a_۰$ را عاد نمیکند پس p دقیقاً یکی از $b_۰$ یا $c_۰$ را عاد می‌کند. مثلاً فرض کند $p|b_۰$ و $p\not|c_۰$. اکنون چون p، $a_n=b_mc_t$ را عاد نمیکند، $p\not|b_m$. پس عدد k وجود دارد که $۰<k\leq m$، $p\not|b_k$ و $p|b_۰$، $p|b_۱$، ...، $p|b_{k-۱}$. یعنی b_k اولین عدد در فهرست $b_۰$، $b_۱$، ...، b_k است که $p\not|b_k$. چون $p|a_k$ (طبق (الف)) زیرا $k\leq m<n$ و بنا به انتخاب b_k، p را عاد می‌کند. از طرفی p، a_k را نیز عاد می‌کند. چون $a_k=b_kc_۰+b_{k-۱}c_۱+\cdots+b_۰c_k$، $p|b_kc_۰$. در نتیجه $p|b_k$ یا $p|c_۰$ که در هر دو صورت تناقض است. □

مثال ۱۸.۲.۱۱. بنا به محک آیزنشتاین ، با $p=۳$، چندجمله‌ای $۲x^۵+۲۷x^۳-۱۸x+۱۲$ روی $\mathbb{Q}[x]$ تحویل‌ناپذیر است. □

مثال ۱۹.۲.۱۱. نشان دهید ، به ازای هر $n\geq ۱$، چندجمله‌ای تحویل‌ناپذیر درجه‌ی n، روی $\mathbb{Q}$ وجود دارد.

حل بنا به محک آیزنشتاین ، با $p=۲$، چندجمله‌ای $x^n-۲$ در $\mathbb{Q}[x]$ تحویل‌ناپذیر است. □

مثال ۲۰.۲.۱۱. فرض کنید p عدد اول باشد. نشان دهید pامین چندجمله‌ای دایره‌بر

$$\Phi_p(x)=x^{p-۱}+x^{p-۲}+\cdots+x+۱$$

در $\mathbb{Q}[x]$ تحویل‌ناپذیر است.

حل چون $\Phi_p(x)=g(x)h(x)$ اگر و تنها اگر $\Phi_p(x+۱)=g(x+۱)h(x+۱)$. کافی است نشان دهیم $\Phi_p(x+۱)$ تحویل‌ناپذیر است. چون

$$(x-۱)\Phi_p(x)=(x-۱)(x^{p-۱}+x^{p-۲}+\cdots+x+۱)=x^p-۱,$$

با قرار دادن $x+۱$ به جای x داریم $x\Phi_p(x+۱)=(x+۱)^p-۱$. با استفاده قضیه‌ی دوجمله‌ای به دست می‌آوریم

$$\Phi_p(x+۱)=x^{p-۱}+\binom{p}{۱}x^{p-۲}+\cdots+\binom{p}{p-۲}x+p.$$

چون $p\Big|\binom{p}{p-k}$، $۱\leq k\leq p-۱$، بنا به محک آیزنشتاین $\Phi_p(x+۱)$ تحویل‌ناپذیر است. این حکم را ثابت می‌کند. □

۳.۱۱ یکتایی تجزیه

در قضیه‌های ۸.۲.۱۱ و ۹.۲.۱۱، دیدیم که هر چندجمله‌ای در $\mathbb{C}[x]$ و $\mathbb{R}[x]$ را می‌توان به حاصل‌ضرب عدد ثابت در چندجمله‌ای‌های تحویل‌ناپذیر تکین تجزیه کرد. نشان می‌دهیم این مطلب برای $F[x]$ درست است که در آن F میدان دلخواهی است، و این تجزیه یکتاست. نکته‌هایی در مورد یکتایی تجزیه بیان می‌کنیم. قضیه‌ی تجزیه‌ی اعداد اول در $\mathbb{Z}$ می‌گوید هر عدد صحیح $n \geq ۲$ به صورت یکتا به حاصل‌ضرب اعداد اول تجزیه می‌شود. اما این یکتایی به فرض مثبت بودن اعداد نیاز دارد. در نتیجه هر عدد صحیح بجز ۰، ۱ و -۱ به طور یکتا به ضرب ± ۱ در حاصل‌ضرب تعدادی عدد اول تجزیه می‌شود. تنها موارد استثنا، ۰ ، و یکه‌های ± ۱ در Z هستند. اگر F میدان باشد یکه‌های $F[x]$، عبارت‌اند از چندجمله‌ای‌های ثابت ناصفر و بنابراین مشابه قضیه‌ی تجزیه به عوامل اول برای $F[x]$ می‌شود: هر چندجمله‌ای غیرثابت در $F[x]$ به صورت ضرب عضو یکه‌ی u در حاصل‌ضرب چندجمله‌ای‌های تحویل‌ناپذیر تجزیه می‌شود. اما به خاطر تجزیه‌ی بدیهی $p(x) = a[a^{-۱}p(x)]$، برای یکتایی تجزیه به تکین بودن چندجمله‌ای‌های تحویل‌ناپذیر نیاز داریم (مشابه اعداد اول در $\mathbb{Z}$ که باید مثبت باشند.)دلیل این که این مطلب یکتایی را ثابت می‌کند قضیه‌ی زیر است:

قضیه ۱.۳.۱۱. فرض کنید F میدان و $f(x), g(x) \in F[x]$ ناصفر و تکین باشند. اگر $f(x)|g(x)$ و $g(x)|f(x)$، آنگاه $f(x) = g(x)$.

اثبات. بنا به فرض چندجمله‌ای‌های $p(x), q(x) \in F[x]$ وجود دارند که

$$f(x) = q(x)g(x) \quad و \quad g(x) = p(x)f(x).$$

در نتیجه $f(x) = q(x)p(x)f(x)$ و $q(x)p(x) = ۱$. پس $q(x) = u$ چندجمله‌ای ثابت است و $f(x) = ug(x)$. چون $f(x)$ و $g(x)$ تکین هستند ، با مقایسه‌ی ضرایب پیشروی تساوی اخیر داریم $u = ۱$. □

با داشتن قضیه‌ی ۱.۳.۱۱، اثبات قضیه‌ی تجزیه در $F[x]$ دقیقاً شبیه اثبات قضیه‌ی مشابه در $\mathbb{Z}$ است. بنابراین در قضیه‌ی زیر بسیاری از جزئیات را اثبات نمیکنیم.

قضیه ۲.۳.۱۱. اگر F میدان و $f(x), g(x) \in F[x]$ دو چندجمله‌ای ناصفر باشند، آنگاه چندجمله‌ای یکتای $d(x) \in F[x]$ وجود دارد که در شرایط زیر صدق نمی‌کند

(الف) $d(x)$ تکین است.

(ب) $d(x)|f(x)$ و $d(x)|g(x)$.

(ج) اگر $h(x)|f(x)$ و $h(x)|g(x)$، آنگاه $h(x)|d(x)$.

(د) $v(x), u(x) \in F[x]$ وجود دارند که $d(x) = u(x)f(x) + v(x)g(x)$.

اثبات. برای سادگی قرار می‌دهیم $f = f(x)$. همانند اثبات قضیه‌ی ۴.۱.۲، از صفحه‌ی ۳۶، قرار می‌دهیم $X = \{uf + vg \mid u, v \in F[x]\}$. چندجمله‌ای‌های f[۲]. پس X شامل چندجمله‌ای‌های تکین نیز هست. در بین همه‌ی چندجمله‌ای‌های تکین در X، عضوی چون $d = uf + vg$ با کمترین درجه را انتخاب می‌کنیم آنگاه (الف) و (د) برقرارند و (ج) نتیجه‌ی سرراستی از (د) است. پس (ب) را ثابت می‌کنیم. بنا به الگوریتم تقسیم چندجمله‌ای‌های $r, q \in F[x]$ وجود دارند که $f = qd + r$، که در آن $r = ۰$ یا $\deg r < \deg d$. آنگاه

$$r = f - qd = f - q(uf + vg) = (۱ - qu)f - (qv)g.$$

اگر $r \neq ۰$ ضریب پیشرو ی r برابر a باشد، عبارت اخیر نشان می‌دهد که $a^{-۱}r$ چندجمله‌ای تکین عضو X است و درجه‌ی آن از درجه‌ی d کمتر است. این متناقض انتخاب d است. پس $r = ۰$ و $d|f$. به طریق مشابه $d|g$ که (ب) را ثابت می‌کند. در نهایت اگر $d_۱$ چندجمله‌ای دیگری باشد که در (الف)، (ب) و (ج) صدق می‌کند، آنگاه $d|d_۱$ و $d_۱|d$. بنابراین بنا به قضیه‌ی ۱.۳.۱۱، $d = d_۱$. □

$d(x)$ در قضیه‌ی ۲.۳.۱۱، را بزرگ‌ترین مقسوم‌علیه مشترک $f(x)$، $g(x)$ در $F[x]$ گوییم و با $\gcd\{f(x), g(x)\}$ نشان می‌دهیم. اگر $d(x) = ۱$ گوییم $f(x)$ و $g(x)$ در $F[x]$ نسبت به هم اول‌اند.

مثال ۳.۳.۱۱. بزرگ‌ترین مقسوم‌علیه مشترک $x^۲-۱$ و $۲x+۱$ در $\mathbb{Q}[x]$ را بیابید.

حل چون $d(x)|(۲x+۱)$، $d(x)=۱$ یا $d(x)=x+\frac{۱}{۲}$. پس $d(x)=۱$، زیرا $\left(x+\frac{۱}{۲}\right)\nmid(x^۲-۱)$. به علاوه از الگوریتم تقسیم داریم

$$x^۲-۱=\left(\frac{۱}{۴}(۲x-۱)\right)(۲x+۱)-\frac{۳}{۴}.$$

از این‌رو $d(x)=۱=\frac{۱}{۳}(۲x-۱)(۲x+۱)-\frac{۴}{۳}(x^۲-۱)$ را به صورت ترکیب خطی $x^۲-۱$ و $۲x+۱$ به دست آوردیم. □

در حالت کلی اگر $d(x)=\gcd\{f(x),g(x)\}$، با استفاده از الگوریتمی شبیه الگوریتم اقلیدسی می‌توان $d(x)$ را به صورت ترکیب خطی $f(x)$ و $g(x)$ نوشت. مثال بعد نحوه‌ی کار را مشخص می‌کند.

مثال ۴.۳.۱۱. بزرگ‌ترین مقسوم‌علیه مشترک چند جمله‌ای‌های $f(x)=x^۴-x^۲+x-۱$ و $g(x)=x^۳-x^۲+x-۱$ را در $\mathbb{Q}[x]$ بیابید و آن را بر حسب ترکیب خطی $f(x)$ و $g(x)$ بنویسید.

حل با استفاده از چند بار تکرار الگوریتم تقسیم داریم

$$\begin{aligned} f(x) &= (x+۱)g(x)+(-x^۲+x)\\ g(x) &= (-x)(-x^۲+x)+(x-۱)\\ -x^۲+x &= (-x)(x-۱)+۰. \end{aligned}$$

مثل الگوریتم اقلیدسی در $\mathbb{Z}$، آخرین باقیمانده، $d(x)=x-۱$ بزرگ‌ترین مقسوم‌علیه مشترک است (در حالتی که آخرین باقیمانده تکین نباشد و a ضریب پیشرو ی آن باشد $d(x)$ را با ضرب $a^{-۱}$ در آن می‌یابیم). با حذف باقیمانده‌ها به دست می‌آوریم:

$$\begin{aligned} x-۱ &= g(x)+x(-x^۲+x)\\ &= g(x)+x[f(x)-(x+۱)g(x)]\\ &= xf(x)+(-x^۲-x+۱)g(x), \end{aligned}$$

که ترکیب خطی مورد نظر است. □

قضیه‌ی بعدی شبیه لم اقلیدس در اعداد صحیح برای چندجمله‌ای‌هاست.

قضیه ۵.۳.۱۱. فرض کنید F میدان باشد. اگر $p(x)$ یک چندجمله‌ای تحویل‌ناپذیر در $F[x]$ باشد طوری که $p(x)|f_۱(x)f_۲(x)\cdots f_n(x)$، که در آن $f_i(x)$ها چندجمله‌ای‌های ناصفر هستند ، آنگاه j وجود دارد که $p(x)|f_j(x)$.

اثبات. بنا به استقرا کافی است حالت $n=۲$ را در نظر بگیریم. برای راحتی کار چندجمله‌ای‌ها را به صورت $f=f(x)$ می‌نویسیم. اگر $p|fg$ قرار می‌دهیم $d=\gcd\{f,p\}$، آنگاه $d|p$. چون p تحویل‌ناپذیر است، یا $\deg d=۰$ (پس $d=۱$) یا $\deg d=\deg p$. اگر $d=۱$، بنا به قضیه‌ی ۲.۳.۱۱، $u,v\in F[x]$ وجود دارند که $۱=up+vf$. پس $g=upg+vfg$ و $p|g$ (زیرا $p|fg$). اگر $\deg d=\deg p$، آنگاه $a\in F$ وجود دارد که $p=ad$ و بنابراین $p|f$ (زیرا $d|f$). □

قضیه ۶.۳.۱۱. (قضیه‌ی یکتایی تجزیه) اگر F میدان و $f(x)\in F[x]$ چندجمله‌ای غیرثابت باشد، آنگاه
(الف) $a\in F$ و چندجمله‌ای‌های تکین تحویل‌ناپذیر $p_i(x)\in F[x]$، $i=۱,\dots,m$. وجود دارند که

$$f(x)=ap_۱(x)p_۲(x)\cdots p_m(x).$$

(ب) تجزیه در (الف) بجز در ترتیب عوامل یکتاست.

اثبات. برای سادگی چندجمله‌ای‌ها را به صورت $f = f(x)$ می‌نویسیم. کافی است نشان دهیم $f = q_1 q_2 \cdots q_m$، که در آن $q_i \in F[x]$ تحویل‌ناپذیر است (اگر a_i ضریب پیشرو ی q_i باشد، قرار می‌دهیم $p_i = a_i^{-1} q_i$ و $a = a_1 a_2 \cdots a_m$). به استقرا روی $n = \deg f$ عمل می‌کنیم. اگر $n = 1$، خود f تحویل‌ناپذیر است. فرض کنید $n > 1$ و قضیه برای همه‌ی چندجمله‌ای‌های با درجه‌ی کمتر از n برقرار باشد. اگر f تحویل‌ناپذیر باشد حکم ثابت است. بنابراین فرض کنید f تحویل‌پذیر باشد و $f = gh$، که در آن $0 < \deg g < n$ و $0 < \deg h < n$. در این حالت بنا به فرض استقرا، g و h برابر حاصل‌ضرب چندجمله‌ای‌های تحویل‌ناپذیرند. پس f نیز حاصل‌ضرب چندجمله‌ای‌های تحویل‌ناپذیر است.

(ب) اگر تجزیه یکتا نباشد، چندجمله‌ای غیر ثابت f با کوچک‌ترین درجه که دو تجزیه‌ی

$$f = a p_1 p_2 \cdots p_m = b q_1 q_2 \cdots q_k$$

داشته باشد را انتخاب می‌کنیم (p_iها و q_iها چندجمله‌ای‌های تکین تحویل‌ناپذیر و $a, b \in F$) آنگاه $a = b$ زیرا هر دو ضرایب پیشروی f هستند. اکنون بنا به قضیه‌ی ۵.۳.۱۱، j وجود دارد که $p_1 | q_j$. با تعویض ترتیب q_iها می‌توانیم فرض کنیم $p_1 | q_1$. چون $\deg p_1 \neq 0$ و q_1 تحویل‌ناپذیر است، داریم $\deg p_1 = \deg q_1$. پس $c \in F$ وجود دارد که $q_1 = c p_1$. اما چون p_1 و q_1 تکین هستند ، $c = 1$ و $p_1 = q_1$. با حذف این چندجمله‌ای‌ها، چندجمله‌ای $p_2 \cdots p_m = q_2 \cdots q_k$ با درجه‌ی کمتر از f با دو تجزیه به دست می‌آید. این خلاف انتخاب f است. □

مثال ۷.۳.۱۱. چندجمله‌ای $f(x) = x^3 - 1$ را در $\mathbb{C}[x]$، $\mathbb{R}[x]$، $\mathbb{Q}[x]$، $\mathbb{Z}_5[x]$ و $\mathbb{Z}_7[x]$ به صورت حاصل‌ضرب عوامل تحویل‌ناپذیر بنویسید.

حل روی هر میدان داریم $f(x) = (x-1)(x^2 + x + 1)$. اکنون $p(x) = x^2 + x + 1$ در $\mathbb{R}$، $\mathbb{Q}$، و یا $\mathbb{Z}_5$ ریشه ندارد. بنابراین در این حالت‌ها $f(x) = (x-1)p(x)$ تجزیه‌ی مورد نظر است. اما در $\mathbb{C}[x]$ داریم $p(x) = (x-u)(x-v)$ که در آن $u = \frac{1}{2}(-1 + i\sqrt{3})$ و $v = \frac{1}{2}(-1 - i\sqrt{3})$؛ و در $\mathbb{Z}_7[x]$ داریم $p(x) = (x-2)(x-4)$. پس $f(x)$ در دو حالت اخیر به عوامل خطی تجزیه می‌شود. □

تمرین‌ها

۱. فرض کنید R حلقه‌ی تعویض‌پذیر و یکدار و $\varphi_a : R[x] \longrightarrow R$ همریختی مقدارياب در $a \in R$ باشد.
(الف) نشان دهید به ازای هر $r \in R$، $\varphi_a(r) = r$.
(ب) اگر $\theta : R[x] \longrightarrow R$ یک همریختی حلقه‌ای باشد که به ازای هر $r \in R$، $\theta(r) = r$، آنگاه $a \in R$ وجود دارد که $\theta = \varphi_a$.
(ج) یک همریختی ناصفر $\varphi : \mathbb{C}[x] \longrightarrow \mathbb{C}$ بیابید که همریختی مقدارياب نباشد.

۲. نشان دهید چندجمله‌ای‌های زیر روی هر میدان دلخواهی تحویل‌ناپذیرند
(الف) $f(x) = x^3 - 2x^2 + 3x - 2$ (ب) $f(x) = x^3 + x^2 + 4$

۳. در کدام حالت چندجمله‌ای داده شده تحویل‌ناپذیر است.
(الف) $x^5 + 5 \in \mathbb{Z}_7[x]$ (ب) $x^2 - 2 \in \mathbb{R}[x]$ (ج) $x^2 + 11 \in \mathbb{C}[x]$
(د) $x^3 - 4 \in \mathbb{Q}[x]$ (هـ) $x^3 + x + 1 \in \mathbb{Z}_5[x]$ (و) $x^2 + x + 1 \in \mathbb{Z}_{11}[x]$.

۴. فرض کنید R یک دامنه‌ی صحیح و $f(x) \in R[x]$ یک چندجمله‌ای تکین باشد. اگر $f(x)$ در $R[x]$ تجزیه‌ی سره داشته باشد، نشان دهید دو چندجمله‌ای تکین $g(x)$ و $h(x)$ وجود دارند که $f(x) = g(x)h(x)$.

۵. همه‌ی چندجمله‌ای‌های درجه‌ی سوم تحویل‌ناپذیر روی $\mathbb{Z}_2[x]$ را بیابید.

۶. فرض کنید $p(x) \in \mathbb{Z}_2[x]$ چندجمله‌ای درجه‌ی ۴ باشد. نشان دهید $p(x)$ در $\mathbb{Z}_2[x]$ تحویل‌ناپذیر است اگر و تنها اگر $p(x)$ ریشه‌ای در $\mathbb{Z}_2$ نداشته باشد و $p(x) \neq x^4 + x^2 + 1$.

۷. فرض کنید $p(x) \in \mathbb{Z}_2[x]$ چندجمله‌ای درجه‌ی ۵ باشد. نشان دهید $p(x)$ در $\mathbb{Z}_2[x]$ تحویل‌ناپذیر است اگر و تنها اگر $p(x)$ ریشه‌ای در $\mathbb{Z}_2$ نداشته باشد و $p(x)$ برابر $x^5 + x^4 + 1$ و یا $x^5 + x + 1$ نباشد.

۸. همه‌ی چندجمله‌ای‌های تکین تحویل‌ناپذیر درجه‌ی ۴ در $\mathbb{Z}_۳[x]$ را بیابید.

۹. نشان دهید اگر $x^۲ + ۱$ روی $\mathbb{Z}_p$ تحویل‌ناپذیر باشد، آن‌گاه $p \equiv ۳ \mod ۴$.

۱۰. نشان دهید تعداد $\frac{۱}{۲}p(p-۱)$ چندجمله‌ای تکین تحویل‌ناپذیر درجه‌ی دو در $\mathbb{Z}_p[x]$ وجود دارد.

۱۱. در هر حالت چندجمله‌ای داده شده را به صورت حاصل‌ضرب چندجمله‌ای‌های تحویل‌ناپذیر در $F[x]$ بنویسید.

(الف) ۲ $f(x) = ۳x^۴ + ۲$، $F = \mathbb{Z}_۵$

(ب) ۲ $f(x) = ۳x^۲ + ۲$، $F = \mathbb{Z}_{۱۱}$

(ج) ۱ $f(x) = x^۳ + ۲x^۲ + ۲x + ۱$، $F = \mathbb{Z}_۷$

(د) ۱ $f(x) = x^۴ - x^۲ + x - ۱$، $F = \mathbb{Z}_{۱۷}$

(هـ) ۱ $f(x) = x^۵ + x + ۱$، $F = \mathbb{Z}_۲$

(و) ۱ $f(x) = x^۵ + x^۲ - x + ۱$، $F = \mathbb{Z}_۳$

۱۲. نشان دهید چندجمله‌ای‌های $f(x)$ داده شده روی $\mathbb{Q}[x]$ تحویل‌ناپذیرند.

(الف) ۲ $f(x) = ۳x^۳ + ۵x^۲ + x + ۲$

(ب) ۶ $f(x) = x^۳ + ۹x^۲ + x + ۶$

(ج) ۱۵ $f(x) = x^۵ + ۶x^۴ + ۱۲x + ۱۵$

(د) ۱۴ $f(x) = ۴x^۵ + ۲۸x^۴ + ۷x^۳ - ۲۸x^۲ + ۱۴$

(هـ) ۱ $f(x) = x^۴ + ۲x - ۱$

(و) ۱ $f(x) = x^۴ + ۴x + ۱$

(ز) ۳ $f(x) = x^۴ + ۴k - ۳$، که در آن k عدد صحیح است

(ح) ۵ $f(x) = x^۴ + ۴x^۳ + ۴x^۲ + ۴x + ۵$

(U) $f(x) = x^p + p^۲mx + (p-۱)$، ($p$ عدد اول و m عدد صحیح)

(i) $f(x) = ۱ - x + x^۲ - \cdots + x^{p-۱}$، ($p$ عدد اول فرد)

(k) ۱ $f(x) = x^۴ + ۴mx + ۱$، که در آن m عدد صحیح است

۱۳. آیا $x^۴ + ۱$ روی $\mathbb{R}$ تحویل‌ناپذیر است؟

۱۴. اگر F میدان باشد نشان دهید $x^۴ + ۱$ روی F تحویل‌ناپذیر است اگر و تنها اگر $x^۲ + ۱$، $x^۲ + ۲$ و $x^۲ - ۲$ در F ریشه نداشته باشند.

۱۵. فرض کنید $f_m(x) = x^۳ - ۴۲x^۲ + ۳۵x + m$، نشان دهید تعداد نامتناهی عدد صحیح m وجود دارند که $f_m(x)$ روی $\mathbb{Q}$ تحویل‌ناپذیر است.

۱۶. در هر حالت $f(x) \in \mathbb{Q}[x]$ را به حاصل‌ضرب چندجمله‌ای‌های تحویل‌ناپذیر روی $\mathbb{Q}$ تجزیه کنید.

(الف) ۱ $f(x) = x^۴ + ۳x^۳ + x^۲ + ۳x + ۱$

(ب) ۲ $f(x) = x^۴ + x^۳ - ۷x^۲ + ۳x - ۲$

(ج) ۲ $f(x) = x^۴ + ۲x^۳ - ۲x^۲ + ۷x - ۲$

(د) ۲ $f(x) = x^۴ - x^۳ + ۲x^۲ - ۳x + ۲$

(هـ) ۱ $f(x) = x^۵ + x + ۱$

(و) ۱ $f(x) = x^۵ + ۳x + ۱$

۱۷. نشان دهید $x^۵ + mx + ۱$ (m عدد صحیح) در $\mathbb{Q}[x]$ تحویل‌ناپذیر است اگر و تنها اگر $m \notin \{۰, -۲, ۱\}$.

۱۸. در حالت های زیر $d(x) = \gcd\{f(x), g(x)\}$ را بیابید و آن را در $F[x]$ بر حسب ترکیب خطی $f(x)$ و $g(x)$ بنویسید.

(الف) ۲ $f(x) = x^۲ + ۲$، $g(x) = x^۳ + ۴x^۲ + x + ۱$، $F = \mathbb{Z}_۵$

(ب) ۱ $f(x) = x^۲ + ۱$، $g(x) = x^۵ + x^۴ + x^۳ + x^۲ + x + ۱$، $F = \mathbb{Z}_۲$

(ج) ۲ $f(x) = x^۲ - x - ۲$، $g(x) = x^۵ - ۴x^۳ - ۲x^۲ + ۷x - ۶$، $F = \mathbb{Q}$

۴.۱۱ حلقه‌های چندجمله‌ای‌های خارج‌قسمتی روی یک میدان

قضیه ۱.۴.۱۱. اگر F یک میدان باشد، $F[x]$ یک PID (دامنه‌ی ایدآل اصلی) است.

اثبات. طبق قضیه‌ی ۳.۱.۱۱، $F[x]$ دامنه‌ی صحیح است. حال اگر I ایدآلی از $F[x]$ باشد، باید ثابت کنیم عضوی از $f(x) \in F[x]$ وجود دارد که $I = (f(x))$. توجه کنید

$$(f(x)) = f(x)F[x] = \{f(x)g(x) \mid g(x) \in F[x]\}.$$

اگر $I = \{0\}$ قرار می‌دهیم $f(x) = 0$. پس فرض کنید $I \neq \{0\}$. اگر $h(x) \in I$ چندجمله‌ای ناصفر با ضریب پیشروی a باشد، چون I ایدآل است $a^{-1}h(x) \in I$. بنابراین چندجمله‌ای تکین در I وجود دارد. از بین همه‌ی چندجمله‌ای‌های تکین در I چندجمله‌ای $f(x)$ با کوچک‌ترین درجه را انتخاب می‌کنیم. چون $f(x) \in I$ و I ایدآل است، $(f(x)) \subseteq I$. نشان می‌دهیم تساوی برقرار است. فرض کنید $g(x) \in I$. بنا به الگوریتم تقسیم $q(x), r(x) \in F[x]$ وجود دارند که $g(x) = q(x)f(x) + r(x)$، که در آن $r(x) = 0$ یا $\deg r(x) < \deg f(x)$. اگر $r(x) \neq 0$ و ضریب پیشروی آن a باشد، آنگاه $a^{-1}r(x)$ چندجمله‌ای تکین است و

$$a^{-1}r(x) = a^{-1}[g(x) - q(x)f(x)] = a^{-1}g(x) - a^{-1}q(x)f(x) \in I.$$

چون $\deg[a^{-1}r(x)] = \deg r(x) < \deg f(x)$، این نتیجه با انتخاب $f(x)$ متناقض است. پس $r(x) = 0$ و $g(x) = q(x)f(x) \in (f(x))$، که نتیجه می‌دهد $I = (f(x))$.
برای اثبات یکتایی، فرض کنید $I = (g(x))$، که در آن $g(x)$ چندجمله‌ای تکین است. چون $(f(x)) = (g(x))$، $f(x)$ و $g(x)$ یک‌دیگر را عدد می‌کنند. چون هر دو تکین هستند باید با هم مساوی باشند. □

قضیه ۲.۴.۱۱. اگر F میدان و $p(x) \in F[x]$ یک چندجمله‌ای غیرثابت تکین باشد، آنگاه $p(x)$ تحویل‌ناپذیر است اگر و تنها اگر $(p(x))$ ایدآل ماکسیمال باشد.

اثبات. ($\Longleftarrow$) فرض کنید ایدآل I از $F[x]$ وجود داشته باشد که $(p(x)) \subseteq I$. طبق قضیه‌ی ۱.۴.۱۱، $F[x]$ یک PID است. بنابراین چندجمله‌ای تکین $f(x) \in F[x]$ وجود دارد که $I = (f(x))$. چون $p(x) \in (p(x)) \subseteq (f(x))$، چندجمله‌ای $g(x) \in F[x]$ وجود دارد که $p(x) = f(x)g(x)$. چون $p(x)$ تکین و تحویل‌ناپذیر، و هم‌چنین $f(x)$ تکین است، $f(x) = 1$ یا $g(x) = 1$. در حالت اول داریم $I = F[x]$ و در حالت دوم داریم $p(x) = f(x)$، که نتیجه می‌دهد $I = (p(x))$. در نتیجه $(p(x))$ ماکسیمال است.
($\Longrightarrow$) فرض کنید $p(x) = f(x)g(x)$، که در آن $0 \leq \deg f(x) < \deg p(x)$. در این صورت $p(x) \in (f(x))$. پس

$$(p(x)) \subset (f(x)) \subset F[x],$$

که خلاف ماکسیمال بودن $p(x)$ است. بنابراین $p(x)$ تحویل‌ناپذیر است. □

چون در یک حلقه‌ی تعویض‌پذیر و یکدار R ایدآل M ماکسیمال است اگر و تنها اگر R/M میدان باشد، داریم :

نتیجه ۳.۴.۱۱. فرض کنید F میدان باشد. اگر $p(x) \in F[x]$ چندجمله‌ای غیرثابت تکین باشد، آنگاه $p(x)$ تحویل‌ناپذیر است اگر و تنها اگر $F[x]/(p(x))$ میدان باشد.

حال فرض کنید F یک میدان باشد و $I = (h(x))$ ایدآلی از $F[x]$، که در آن $h(x)$ یک چندجمله‌ای غیرثابت تکین با درجه‌ی m است. حلقه‌ی خارج‌قسمت

$$R = F[x]/I = \{f(x) + I \mid f(x) \in F[x]\}$$

را تشکیل می‌دهیم. هم مجموعه‌ی $f(x) + I$ را به صورت $\overline{f(x)} = f(x) + I$ نشان می‌دهیم. به ویژه برای هر $a \in F$، $\bar{a} = a + I$. هم‌چنین از نماد t به جای $x + I$ استفاده می‌کنیم:

$$t = \bar{x} = x + I.$$

اعمال جمع و ضرب در R به صورت زیر هستند

$$\overline{f(x)} + \overline{g(x)} = \overline{f(x) + g(x)}, \quad \overline{f(x)}\,\overline{g(x)} = \overline{f(x)g(x)}.$$

حال می‌خواهیم اعضای R را توصیف کنیم. یک عضو نوعی R به صورت $\overline{f(x)}$ است که در آن $f(x) \in F[x]$. بنا به الگوریتم تقسیم $q(x) \in F[x]$ و اعضای $a_i \in F$، $i = ۱, ۲, \ldots, m-۱$ وجود دارند که

$$f(x) = q(x)h(x) + a_۰ + a_۱x + \cdots + a_{m-۱}x^{m-۱}.$$

چون $h(x) \in I$ داریم $\overline{h(x)} = \bar{۰}$. از این‌رو

$$\overline{f(x)} = \overline{a_۰ + a_۱x + \cdots + a_{m-۱}x^{m-۱}} = \bar{a}_۰ + \bar{a}_۱t + \cdots + \bar{a}_{m-۱}t^{m-۱}.$$

بنابراین ثابت کرده‌ایم

$$R = \{\bar{a}_۰ + \bar{a}_۱t + \cdots + \bar{a}_{m-۱}t^{m-۱} \mid a_i \in F\}.$$

اکنون نشان می‌دهیم که F را می‌توان به عنوان زیرحلقه‌ای از R در نظر گرفت. در واقع تابع $\theta : F \to R$ را با ضابطه‌ی $\theta(a) = \bar{a}$، برای هر $a \in F$، تعریف می‌کنیم. θ همریختی است، زیرا به ازای هر $a, b \in F$ داریم ، $\overline{a+b} = \bar{a} + \bar{b}$ و $\overline{ab} = \bar{a}\bar{b}$. نشان می‌دهیم θ یک‌به‌یک است. فرض کنید $a \in \ker\theta$، یعنی $\bar{a} = \theta(a) = \bar{۰}$ و در نتیجه $a \in I$. اگر $a \neq ۰$، آن‌گاه چون a یکه است، $I = F[x]$. بنابراین $۱ \in I = (h(x))$ و $f(x) \in F[x]$ وجود دارد که $f(x)h(x) = ۱$. پس $\deg h(x) = ۰$ که تناقض است. بنابراین $a = ۰$. در نتیجه θ یک‌به‌یک است. در نتیجه $\operatorname{Im}\theta = \{\bar{a} \mid a \in F\}$ یک زیرحلقه‌ی R یکریخت با F است. بنابراین می‌توانیم F را با تصویر آن در R، با در نظر گرفتن $\bar{a} = a$ به ازای هر $a \in F$، یکی بگیریم. با این قرارداد داریم :

$$R = \{a_۰ + a_۱t + \cdots + a_{m-۱}t^{m-۱} \mid a_i \in F\}.$$

حال نشان می‌دهیم عناصر R به صورت یکتای بالا نمایش داده می‌شوند. اگر در R داشته باشیم،

$$a_۰ + a_۱t + \cdots + a_{m-۱}t^{m-۱} = b_۰ + b_۱t + \cdots + b_{m-۱}t^{m-۱}.$$

در نتیجه

$$(a_۰ - b_۰) + (a_۱ - b_۱)t + \cdots + (a_{m-۱} - b_{m-۱})t^{m-۱} = ۰.$$

پس کافی است نشان دهیم اگر $c_i \in F$ و $c_۰ + c_۱t + \cdots + c_{m-۱}t^{m-۱} = ۰$، آن‌گاه $c_i = ۰$، به ازای هر i. فرض کنید $k(x) = c_۰ + c_۱x + \cdots + c_{m-۱}x^{m-۱}$، در این صورت $k(x) \in F[x]$ و در R داریم

$$\overline{k(x)} = \bar{c}_۰ + \bar{c}_۱x + \cdots + \bar{c}_{m-۱}\bar{x}^{m-۱} = c_۱ + c_۱t + \cdots + c_{m-۱}t^{m-۱} = ۰.$$

از این‌رو $k(x) \in I$. بنابراین $q(x) \in F[x]$ وجود دارد که $k(x) = q(x)h(x)$. اگر $k(x) \neq ۰$ تناقض به دست می‌آید، زیرا

$$m - ۱ \geq \deg k(x) = \deg q(x) + \deg h(x) \geq \deg h(x) = m.$$

پس در $F[x]$، $k(x) = ۰$. بنابراین $c_i = ۰$، به ازای هر i.

قضیه ۴.۴.۱۱. با نمادهای این بخش داریم $h(t) = ۰$.

اثبات. فرض کنید $h(x) = c_۰ + c_۱x + \cdots + c_{m-۱}x^{m-۱} + x^m$.

یادآوری می‌کنیم $t = x + I$ و طبق قرار داد $a = \bar{a} = a + I$، به ازای هر $a \in F$. اکنون در حلقه‌ی R محاسبه می‌کنیم:

$$\begin{aligned} h(t) &= c_۰ + c_۱t + \cdots + c_{m-۱}t^{m-۱} + t^m \\ &= \bar{c}_۰ + \bar{c}_۱\bar{x} + \cdots + \bar{c}_{m-۱}\bar{x}^{m-۱} + \bar{x}^m \\ &= \overline{c_۰ + c_۱x + \cdots + c_{m-۱}x^{m-۱} + x^m} \\ &= \overline{h(x)} \\ &= \bar{۰}. \end{aligned}$$

پس در R، $h(t) = ۰$. □

مطالب بالا را جمع‌بندی می‌کنیم:

قضیه ۵.۴.۱۱. اگر F میدان و $h(x) \in F[x]$ یک چندجمله‌ای تکین با درجه‌ی $m \geq ۱$ باشد، آنگاه

$$\frac{F[x]}{(h(x))} = \{a_۰ + a_۱t + \cdots + a_{m-۱}t^{m-۱} \mid a_i \in F, \quad h(t) = ۰\}$$

که در آن $t = \bar{x} = x + I$ و برای هر $a \in F$، a را با $\bar{a} = a + I$ یکی گرفته‌ایم. به علاوه نمایش هر عضو $F[x]/(h(x))$ به مفهوم زیر یکتاست:

$$a_۰ + a_۱t + \cdots + a_{m-۱}t^{m-۱} = b_۰ + b_۱t + \cdots + b_{m-۱}t^{m-۱}$$

اگر و تنها اگر برای هر i، $a_i = b_i$ (یعنی مجموعه‌ی $\{۱, t, \ldots, t^{m-۱}\}$ روی F مستقل خطی است). □

مثال ۶.۴.۱۱. اگر F میدان باشد و $h(x) = x^۲ + ۱$، آنگاه

$$\frac{F[x]}{(x^۲ + ۱)} = \{a + bt \mid a, b \in F, \ \ t^۲ + ۱ = ۰\}.$$

جمع دو عضو به صورت $(a + bt) + (c + dt) = (a + c) + (b + d)t$ انجام می‌شود. هم‌چنین چون $t^۲ = -۱$، ضرب دو عضو به صورت

$$(a + bt)(c + dt) = ac + (ad + bc)t + bdt^۲ = (ac - bd) + (ad + bc)t.$$

در حالتی که $F = \mathbb{R}$ به جای t می‌نویسیم i و نتیجه‌ی کار حلقه‌ی اعداد مختلط $\mathbb{C}$ است. فرمول‌بندی قضیه‌ی بالا حلقه‌ی $F[x]/(h(x))$ را کاملاً توصیف می‌کند. هر عضو به صورت یکتای

$$a_۰ + a_۱t + \cdots + a_{m-۱}t^{m-۱}, \qquad (۱)$$

است، که در آن $a_i \in F$ و $m = \deg h(x)$. جمع و ضرب عبارت‌هایی به صورت بالا به طریق معمول و با استفاده از اعمال F انجام می‌شود. در حالت ضرب، ممکن است توان‌های t بیش از $m - ۱$ ظاهر شوند که برای تبدیل آن‌ها به عبارت‌هایی بر حسب توان‌های کمتر از m به $h(t) = ۰$ نیاز داریم. چون $h(x)$ تکین است، می‌توان t^m و بنابراین همه‌ی توان‌های بیشتر t را به صورت (۱) نوشت. □

مثال ۷.۴.۱۱. حلقه‌ی $\mathbb{Z}_۲[x]/(x^۲)$ را توصیف کنید.

حل طبق قضیه‌ی ۵.۴.۱۱، با $h(x) = x^۲$ و $m = ۲$، داریم

$$R = \frac{\mathbb{Z}_۲[x]}{(x^۲)} = \{a + bt \mid a, b \in \mathbb{Z}_۲, \quad t^۲ = ۰\} = \{۰, ۱, t, ۱ + t\}.$$

چون در $\mathbb{Z}_۲$، $۱+۱=۰$ و هم‌چنین چون $t^۲=۰$ جدول جمع و ضرب در R به صورت زیر هستند :

$+$	۰	۱	t	$۱+t$
۰	۰	۱	t	$۱+t$
۱	۱	۰	$۱+t$	t
t	t	$۱+t$	۰	۱
$۱+t$	$۱+t$	t	۱	۰

$\times$	۰	۱	t	$۱+t$
۰	۰	۰	۰	۰
۱	۰	۱	t	$۱+t$
t	۰	t	۰	t
$۱+t$	۰	$۱+t$	t	۱

از جدول ضرب بالا معلوم است که ۰، t تنها اعضای پوچ‌توان و ۱، $۱+t$ تنها اعضای وارون‌پذیر R هستند. □

مثال ۸.۴.۱۱. حلقه‌ی $\mathbb{Z}_۲[x]/(x^۳+۱)$ را توصیف کنید.

حل در این Ja $h(x)=x^۳+۱$. بنابراین با استفاده از قضیه‌ی ۵.۴.۱۱، با $m=۳$ و $t^۳+۱=۰$، داریم

$$R=\frac{\mathbb{Z}_۲[x]}{(x^۳+۱)}=\{a+bt+ct^۲ \mid a,b,c\in\mathbb{Z}_۲,\quad t^۳+۱=۰\}.$$

چون هر عضو R به صورت یکتای $a+bt+ct^۲$، $a,b,c\in\mathbb{Z}_۲$، قابل نمایش است، $|R|=۸$ و داریم

$$R=\{۰,۱,t,t^۲,۱+t,۱+t^۲,t+t^۲,۱+t+t^۲\}.$$

در $\mathbb{Z}_۲$ داریم $۱+۱=۰$. بنابراین در R داریم $۱+۱=۰$ و $t^۳=۱$. با استفاده از این روابط جمع و ضرب اعضای R را می‌توان انجام داد. مثلاً

$$(۱+t)(۱+t+t^۲)=۱+۲t+۲t^۲+t^۳=۱+۰+۰+۱=۰.$$

به همین صورت می‌توان هر دو عضو دلخواه R را با هم جمع و یا در هم ضرب کرد. □

مثال ۹.۴.۱۱. نشان دهید $f(x)=x^۴+x+۱\in\mathbb{Z}_۲[x]$ روی $\mathbb{Z}_۲$ تحویل‌ناپذیر است و با استفاده از آن میدانی از مرتبه‌ی ۱۶ بسازید.

حل فرض کنید $f(x)$ روی $\mathbb{Z}_۲$ تحویل‌پذیر باشد. پس چندجمله‌ای‌های $p(x)$ و $q(x)$ در $\mathbb{Z}_۲[x]$ وجود دارند که $f(x)=p(x)g(x)$. چون $f(x)$ در $\mathbb{Z}_۲$ ریشه ای ندارد ، $p(x)$ و $q(x)$ چندجمله‌ای‌های درجه‌ی دو هستند. اما $x^۲+x+۱$ تنها چندجمله‌ای تحویل‌ناپذیر روی $\mathbb{Z}_۲$ است؛ از این‌رو $p(x)=q(x)=۱+x+x^۲$ و

$$x^۴+x+۱=f(x)=p(x)q(x)=(۱+x+x^۲)^۲=۱+x^۲+x^۴,$$

که تناقض است. پس $f(x)$ روی $\mathbb{Z}_۲$ تحویل‌ناپذیر است. در نتیجه

$$\frac{\mathbb{Z}_۲[x]}{(f(x))}=\{a+bt+ct^۲+dt^۳ \mid a,b,c,d\in\mathbb{Z}_۲,\ \ t^۴=t+۱\}$$

یک میدان ۱۶ عضوی است. □

مثال ۱۰.۴.۱۱. اگر p عدد اول باشد که $p\equiv ۳ \mod ۴$ یک میدان با $p^۲$ عضو بسازید.

حل چندجمله‌ای $x^۲+۱\in\mathbb{Z}_p[x]$ را در نظر می‌گیریم. طبق فرض عدد صحیح $k\geq ۰$ وجود دارد که $p=۴k+۳$. محاسبه‌ها را در $\mathbb{Z}_p$ انجام می‌دهیم. ادعا می‌کنیم $x^۲+۱$ در $\mathbb{Z}_p$ ریشه‌ای ندارد ؛ و بنابراین در $\mathbb{Z}_p[x]$ تحویل‌ناپذیر است. اگر $a\in\mathbb{Z}_p$، $a\neq ۰$ و $a^۲+۱=۰$، آنگاه $a^۲=-۱$. اما طبق قضیه‌ی فرما، $a^{p-۱}=۱$. بنابراین

$$۱=a^{p-۱}=a^{۴k+۲}=(a^۲)^{۲k+۱}=(-۱)^{۲k+۱}=-۱,$$

که تناقض است، زیرا $p \neq ۲$. بنابراین $x^۲ + ۱$ در $\mathbb{Z}_p[x]$ تحویل‌ناپذیر است و

$$R = \frac{\mathbb{Z}_p[x]}{(x^۲ + ۱)} = \{a + bt \mid a, b \in \mathbb{Z}_p, \quad t^۲ + ۱ = ۰\}.$$

چون هر عضو R به صورت یکتای $a + bt$، $a, b \in \mathbb{Z}_p$ نوشته می‌شود، $|R| = p^۲$. پس R میدان $p^۲$ عضوی است. □

از مثال قبل واضح است که اگر $h(x)$ یک چندجمله‌ای درجه‌ی m تحویل‌ناپذیر در $\mathbb{Z}_p[x]$ باشد، آنگاه $\frac{\mathbb{Z}_p[x]}{(h(x))}$ یک میدان p^m عضوی است. به علاوه می‌توان ثابت کرد که چندجمله‌ای‌های تکین تحویل‌ناپذیر با درجه‌ی $m \geq ۱$، به ازای هر m، در $\mathbb{Z}_p[x]$ وجود دارد. پس به ازای هر عدد اول p و هر m می‌توان میدان p^m عضوی ساخت. در واقع می‌توان نشان داد که هر میدان متناهی را به چنین صورتی می‌توان ساخت (فصل ۱۴ را ببینید).

فرض کنید F میدان و $f(x)$ یک چندجمله‌ای غیرثابت در $F[x]$ باشد. در این صورت طبق قضیه‌ی یکتایی تجزیه، $f(x)$ یک عامل تکین و تحویل‌ناپذیر $p(x)$ دارد. بنابراین $q(x) \in F[x]$ وجود دارد که $f(x) = p(x)g(x)$. بنا به قضیه‌ی ۳.۴.۱۱، $E = F[x]/(p(x))$ میدان است. هم‌چنین می‌توان F را به عنوان زیرمیدان E در نظر گرفت (پس از یکی گرفتن هر $a \in F$ با هم مجموعه‌ی $\bar{a} = a + (p(x))$ در E). به علاوه E عضوی مثل t دارد که در E، $p(t) = ۰$. بنابراین در E، $f(t) = p(t)g(t) = ۰$ و بنابراین t ریشه‌ای از $f(x)$ در E است.

میدان E را توسیع میدان F گوییم هرگاه $F \subseteq E$. بنابراین قضیه‌ی مهم زیر را ثابت کرده‌ایم:

قضیه ۱۱.۴.۱۱. (قضیه‌ی کرونکر) اگر F میدان دلخواهی باشد و $f(x) \in F[x]$ چندجمله‌ای غیرثابت باشد، آنگاه توسیعی از F وجود دارد که $f(x)$ در آن ریشه دارد.

تمرین‌ها

در تمامی تمرین‌ها F یک میدان است.

۱. در هر حالت چندجمله‌ای تکین $h(x) \in F[x]$ را بیابید که $I = (h(x))$.
(الف) $I = \{f(x) \in F[x] \mid$ { جمله ثابت $f(x)$ برابر صفر است
(ب) $I = \{f(x) \in F[x] \mid$ { مجموع ضرایب $f(x)$ صفر است
(ج) $I = \{f(x) \in F[x] \mid f(۰) = f(۱) = ۰\}$
(د) $I = \{f(x) \in F[x] \mid f(۰) = f(۱) = f(۲) = ۰\}$، $F \neq \mathbb{Z}_۲$.

۲. در هر حالت $R = F[x]/(f(x))$ را توصیف کنید و جدول جمع و ضرب R را بنویسید (الف) $f(x) = x^۲ + ۱$، $F = \mathbb{Z}_۲$
(ب) $f(x) = x^۲ + x$، $F = \mathbb{Z}_۲$
(ج) $f(x) = x^۳ - ۱$، $F = \mathbb{Z}_۲$
(د) $f(x) = x - ۱$، $F = \mathbb{Z}_۳$
(هـ) $f(x) = x^۲ - x + ۱$، $F = \mathbb{Z}_۳$.

۳. (الف) میدانی از مرتبه‌ی ۸ بسازید و جدول ضرب آن را بنویسید.
(ب) میدانی از مرتبه‌ی ۹ بسازید و جدول ضرب آن را بنویسید.

۴. اعضای خودتوان، پوچ‌توان و یکه‌های حلقه‌ی $R = F[x]/(h(x))$، که در آن F میدان دلخواهی است، را بیابید.
(الف) $h(x) = x^۲ - x$ (ب) $h(x) = x^۲$.

۵. زیرحلقه‌ای از $\mathbb{R}$ بیابید که با $\mathbb{Q}[x]/(x^۳ - ۲)$ یکریخت است.

۶. فرض کنید $p(x)$ چندجمله‌ای تحویل‌ناپذیر روی F باشد و $R = F[x]/(p(x))$. در هر حالت $p(x)$ را به عوامل خطی روی $R[x]$ تجزیه کنید.
(الف) $p(x) = x^۳ - x + ۱$، $F = \mathbb{Z}_۲$

(ب) $F = \mathbb{Z}_۲$ ، $p(x) = x^۳ + x^۲ + ۱$
(ج) $F = \mathbb{Z}_۳$ ، $p(x) = x^۳ - x + ۱$
(د) $F = \mathbb{Z}_۳$ ، $p(x) = x^۳ - x^۲ + ۱$

۷. نشان دهید به ازای هر p میدانی از مرتبه‌ی $p^۲$ وجود دارد.

۸. چندجمله‌ای‌های $f_۱(x)$، $f_۲(x)$، ...، $f_m(x)$ در $F[x]$ را نسبت به هم اول گوییم هرگاه ۱ تنها چندجمله‌ای تکین در $F[x]$ باشد که هر $f_i(x)$ را عاد می‌کند. نشان دهید اگر $f_۱(x)$، $f_۲(x)$، ...، $f_m(x)$ نسبت به هم اول باشند، آنگاه چندجمله‌ای‌های $q_۱(x)$، $q_۲(x)$، ...، $q_m(x)$ در $F[x]$ وجود دارند که

$$۱ = q_۱(x)f_۱(x) + \cdots + q_m(x)f_m(x).$$

۹. فرض کنید $۰ \neq f(x) \in F[x]$ یک چندجمله‌ای تکین باشد. نشان دهید هر عضو $F[x]/(f(x))$ وارون پذیر یا پوچ‌توان است اگر و تنها اگر $n \geq ۱$ و چندجمله‌ای تکین تحویل‌ناپذیر $p(x)$ وجود داشته باشد $f(x) = p(x)^n$.

فصل ۱۲

تجزیه در دامنه‌های صحیح

دو قضیه‌ی یکتایی تجزیه را ثابت کرده‌ایم: (۱) هر عدد صحیح بزرگ‌تر از یک برابر حاصل‌ضرب تعدادی عدد اول یکتاست. (۲) اگر F یک میدان باشد، هر چندجمله‌ای با درجه‌ی مثبت را می‌توان به طور یکتا به حاصل‌ضرب عضوی از F در تعدادی چندجمله‌ای تکین تحویل‌ناپذیر نوشت. حال می‌خواهیم دامنه‌های صحیحی را در نظر بگیریم که قضیه‌ی مشابه در آنها برقرار است. (این دامنه‌ها را دامنه‌های تجزیه‌ی یکتا یا UFD می‌نامیم)

این نظریه تاریخچه قدیمی دارد و می‌توان آن را یکی از منابع اولیه‌ی جبر مجرد جدید دانست. در ابتدای قرن ۱۹ میلادی گاوس از این که حلقه‌ی $\mathbb{Z}[i]$ (که آن را حلقه‌ی اعداد صحیح گاوسی می‌نامیم) یک UFD است استفاده کرد و قانون تقابل درجه‌ی چهارم (روشی برای حل معادله‌ی $x^۴ \equiv b \mod n$ وقتی که جواب داشته باشد) را ثابت کرد. کومر، با الهام از این حقیقت که i ریشه‌ی (چهارم) واحد است، با در نظر گیری $\mathbb{Z}[w]$، که در آن w ریشه‌ی دلخواهی از واحد است، سعی کرد کار گاوس را تعمیم دهد. اما او دریافت که $\mathbb{Z}[w]$ ممکن است UFD نباشد. این مشاهده نتایج دیگری دربر داشت. لامه در سال ۱۸۴۷ اعلام کرد که یکی از مشهورترین مساله‌های نظریه‌ی اعداد، یعنی آخرین قضیه‌ی فرما را ثابت کرده است. این قضیه ادعا می‌کند که هیچ عدد صحیح x، y و z در معادله‌ی $x^n + y^n = z^n$، به ازای هر عدد صحیح $n \geq ۳$، صدق نمیکند. کافی است این ادعا برای وقتی که $n = p \geq ۳$ عدد اول است ثابت شود. اگر w یک ریشه‌ی pام واحد باشد، لامه عبارت $x^p + y^p$ را در $\mathbb{Z}[w]$ به صورت زیر تجزیه کرد

$$x^p + y^p = (x + y)(x + wy)(x + w^۲y) \cdots (x + w^{p-۱}y)$$

و سپس از یکتایی تجزیه در $\mathbb{Z}[w]$ (که لو فرض کرده بود) استفاده کرد.

کومر با اثبات این که یکتایی تجزیه در $\mathbb{Z}[w]$ برای چیز هایی که او آن‌ها را اعداد ایدآل نامیده برقرار نیست، پاسخ داد. این اثبات آخرین قضیه‌ی فرما را برای تعداد زیادی عدد اول حل کرد. (آخرین قضیه‌ی فرما تا سال ۱۹۹۷ حل نشده باقیمانده بود تا این که اندرو وایلز از دانشگاه پرینستون آن را حل کرد). اما ایده‌ی کومر تاثیر زیادی بر جبر مدرن گذاشت. زیرا اعداد ایدآلی او را اکنون ما ایدآل می‌نامیم. ددکیند با الهام از این ایده‌ها، دامنه‌های صحیحی را توصیف کرد که هر ایدآل ناصفر آن‌ها به حاصل‌ضرب یکتای ایدآل‌های اول است.

۱.۱۲ تجزیه و تحویل‌ناپذیرها

در این بخش می‌خواهیم ایده‌ی تجزیه، مقسوم‌علیه مشترک، الگوریتم تقسیم و ... را در حلقه‌های دلخواه تعویض‌پذیر در نظر بگیریم. فرض کنید R حلقه‌ی تعویض‌پذیر باشد و $a, b \in R$، $a \neq ۰$. یادآوری می‌کنیم اگر $c \in R$ وجود داشته باشد که $b = ac$، آن‌گاه گوییم a، b را عاد می‌کند و یا a یک مقسوم‌علیه b است و می‌نویسیم $a|b$. وقتی می‌نویسیم $a|b$، منظور این است که $a \neq ۰$ و a، b را عاد می‌کند. نماد $a \nmid b$ یعنی a، b را عاد نمی‌کند.

فرض کنید R حلقه‌ی تعویض‌پذیر و یکدار باشد. با استفاده از تعریف بلافاصله می‌توان ثابت کرد که به ازای هر $a, b, c \in R$:

(الف) $a|a$، $۱|a$، $a|۰$.

(ب) a یکه است اگر و تنها اگر $a|۱$.

(ج) اگر $a|b$ و $b|c$، آن‌گاه $a|c$.

تعریف ۱.۱.۱۲. فرض کنید R حلقه‌ی تعویض‌پذیر و یکدار باشد. عضو ناصفر $a \in R$ را هم‌مقسوم عضو ناصفر $b \in R$ گوییم، هرگاه عضو یکه‌ی $u \in R$ وجود داشته باشد که $a = bu$.

مثال ۲.۱.۱۲. (الف) یکه‌های $\mathbb{Z}$ عبارت‌اند از ± ۱. پس به ازای هر $a \in \mathbb{Z}$، a و $-a$ هم‌مقسوم هستند.
(ب) یکه‌های $\mathbb{Z}[i]$ عبارت‌اند از ± ۱ و $\pm i$. پس همه‌ی هم‌مقسوم‌های $i + ۱$ عبارت‌اند از $i + ۱$، $-i - ۱$، $-۱ + i$، $۱ - i$.
(ج) اگر F میدان باشد ، یکه‌های $F[x]$ اعضای ناصفر F هستند. بنابراین هم‌مقسوم‌های چندجمله‌ای غیرثابت $f(x)$ عبارت‌اند از $uf(x)$ که در آن $u \in F - \{۰\}$.

قضیه ۳.۱.۱۲. فرض کنید R حلقه‌ی تعویض‌پذیر و یکدار باشد و $a, b, c \in R$.
(الف) اگر a هم‌مقسوم b باشد، آن‌گاه b هم‌مقسوم a است.
(ب) اگر a هم‌مقسوم b و b هم‌مقسوم c باشند، آن‌گاه a هم‌مقسوم c است.
(ج) اگر R دامنه‌ی صحیح باشد، آن‌گاه a هم‌مقسوم b است اگر و تنها اگر $a|b$ و $b|a$.
(د) اگر R دامنه‌ی صحیح باشد، آن‌گاه a و b هم‌مقسوم هستند اگر و تنها اگر $(a) = (b)$.

اثبات. (الف) اگر a هم‌مقسوم b باشد، آن‌گاه عضو یکه‌ی $u \in R$ وجود دارد که $a = ub$. بنابراین $b = u^{-۱}a$ و b هم‌مقسوم a است.
(ب) طبق فرض اعضای یکه‌ی $u_۱, u_۲ \in R$ وجود دارند که $a = u_۱b$، $b = u_۲c$. بنابراین $a = u_۱b = u_۱u_۲c$. چون $u_۱u_۲$ یکه است، a هم‌مقسوم c است.
(ج) فرض کنید a هم‌مقسوم b باشد. پس عضو یکه‌ی $a \in R$ وجود دارد که $a = bu$. از این‌رو $b = au^{-۱}$. بنابراین $a|b$ و $b|a$. برعکس اگر $a|b$ و $b|a$، آن‌گاه $q_۱, q_۲ \in R$ وجود دارند که $a = q_۱b$ و $b = q_۲a$. پس $b = q_۲a = q_۲q_۱b$. بنابراین بنا به قانون حذف، $q_۲q_۱ = ۱$. از این‌رو $q_۱$ و $q_۲$ یکه هستند، یعنی a و b هم‌مقسوم‌اند.
(د) چون $a \in ()$ اگر و تنها اگر $b|a$، حکم از (ج) به دست می‌آید. □

اکنون مفهوم بزرگ‌ترین مقسوم‌علیه مشترک را در یک حلقه‌ی تعویض‌پذیر تعریف می‌کنیم:

تعریف ۴.۱.۱۲. فرض کنید R حلقه‌ی تعویض‌پذیر و $a_۱, \ldots, a_n \in R$ همگی ناصفر باشند. عضو ناصفر $d \in R$ را بزرگ‌ترین مقسوم‌علیه مشترک $a_۱$، ...، a_n گوییم هرگاه
(الف) d مقسوم‌علیه مشترک $a_۱$، ...، a_n باشد ؛ یعنی $d|a_i$، $i = ۱, ۲, \ldots, n$.
(ب) اگر $c \in R$ مقسوم‌علیه مشترک $a_۱$، ...، a_n باشد، آن‌گاه $c|d$.

در حالت کلی ممکن است بزرگ‌ترین مقسوم‌علیه مشترک دو عضو یکتا نباشد و یا حتی وجود نداشته باشد :

مثال ۵.۱.۱۲. در حلقه‌ی $\mathbb{Z}_{۱۰}$ داریم $\bar{۶} \times \bar{۴} = \bar{۴}$، یعنی $\bar{۴}|\bar{۶}$. پس $\bar{۶}$ یک مقسوم‌علیه مشترک $\bar{۴}$ و $\bar{۶}$ است. پس هم $\bar{۴}$ و هم $\bar{۶}$ باید بزرگ‌ترین مقسوم‌علیه مشترک $\bar{۴}$ و $\bar{۶}$ باشند. توجه کنید چون $\bar{۴} \times \bar{۹} = \bar{۶}$ و $\bar{۴}$ یکه است پس $\bar{۴}$ و $\bar{۶}$ هم‌مقسوم‌اند. □

مثال ۶.۱.۱۲. در حلقه‌ی $E = ۲\mathbb{Z}$. ۲ هیچ شمارنده‌ای ندارد. از این‌رو ۲ به همراه هر عدد صحیح زوج دیگر بزرگ‌ترین مقسوم‌علیه مشترک ندارد. □

مثال ۷.۱.۱۲. در یک میدان F به ازای هر دو عضو ناصفر $a, b \in F$، داریم $a|b$ و $b|a$ (چون مثلاً $a = (ab^{-۱})b$). پس هر عضو ناصفر بزرگ‌ترین مقسوم‌علیه مشترک هر زوج از اعضای F است. □

در قضیه‌ی بعد نشان می‌دهیم در حلقه‌ی ایدآل اصلی، هر دو عضو که یکی از آن‌ها صفر نباشد gcd دارند. یادآوری می‌کنیم حلقه‌ی ایدآل اصلی، حلقه‌ی تعویض‌پذیر و یکدار است که هر ایدآل آن اصلی باشد.

قضیه ۸.۱.۱۲. اگر R حلقه‌ی ایدآل اصلی باشد و دو عضو $a, b \in R$ هر دو با هم صفر نباشند، آن‌گاه بزرگ‌ترین مقسوم‌علیه مشترک d از a و b وجود دارد. برای هر بزرگ‌ترین مقسوم‌علیه مشترک d از a و b اعضای $t, s \in R$ وجود دارند که $d = sa + tb$.

اثبات. چون R حلقه‌ی ایدآل اصلی است، ایدآل تولید شده توسط a و b، یعنی (a,b)، اصلی است. بنابراین عضو $d \in R$ وجود دارد که $(a,b)=(d)$. چون $a,b \in (d)$، اعضای $u,v \in R$ وجود دارند که $a=ud$ و $b=vd$. در نتیجه d مقسوم‌علیه مشترک a و b است. چون $d \in (a,b)$، اعضای $s,t \in R$ وجود دارند که $d=sa+tb$. حال فرض کنید c یک مقسوم‌علیه مشترک دلخواه a و b باشد. پس $u_۱,v_۱ \in R$ وجود دارند که $a=u_۱c$ و $b=v_۱c$. در نتیجه $d=sa+tb=(su_۱+tv_۱)c$. پس $c|d$. بنابراین $d=\gcd\{a,b\}$. فرض کنید $d_۱$ بزرگ‌ترین مقسوم‌علیه مشترک دیگر i از a و b باشد، آنگاه $d_۱|d$ و $d|d_۱$. بنابراین $(d_۱)=(d)=(a,b)$. در نتیجه $t_۱ \in R$ و $s_۱$ وجود دارند که $d_۱=s_۱a+t_۱b$. □

اگر شرط اصلی بودن حلقه را در قضیه‌ی ۸.۱.۱۲، برداریم نتیجه درست نیست:

مثال ۹.۱.۱۲. $f(x),g(x) \in \mathbb{Z}[x]$ را طوری بیابید که $\gcd\{f(x),g(x)\}=۱$، اما هیچ ترکیب خطی از $f(x)$ و $g(x)$ در $\mathbb{Z}_۲[x]$ برابر ۱ نشود؛ یعنی $f_۱(x),g_۱(x) \in \mathbb{Z}_۲[x]$ وجود نداشته باشند که $f(x)f_۱(x)+g(x)g_۱(x)=۱$.

حل چندجمله‌ای‌های $x+۶$ و $x+۴$ در $\mathbb{Z}[x]$ را در نظر می‌گیریم. آنگاه به وضوح $\gcd\{x+۶,x+۴\}=۱$. اگر $f_۱(x) \in \mathbb{Z}[x]$ و $g_۱(x)$ وجود داشته باشند که

$$۱=(x+۶)f_۱(x)+(x+۴)g_۱(x),$$

آنگاه جمله‌ی ثابت راست معادله‌ی فوق عدد صحیح زوج است در حالتی که جمله‌ی ثابت سمت چپ ۱ است، که این تناقض است.

تمرین‌ها

۱. تمامی همدم‌های اعضای داده شده را بیابید.
(الف) $۲i-۳$ را در $\mathbb{Z}[i]$ (ب) $۱+i\sqrt{۵}$ را در $\mathbb{Z}[i\sqrt{۵}]$
(ج) $\bar{۶}$ را در $\mathbb{Z}_{۱۰}$ (د) $\bar{۴}$ را در $\mathbb{Z}_{۱۰}$
(هـ) $x+۲$ را در $\mathbb{Z}_۴[x]$ (و) $۲+x-۳x^۲$ را در $\mathbb{Z}[x]$
(ز) $۲+x^۲$ را در $\mathbb{Z}_۲[x]$ (ح) $۱+x^۲$ را در $\mathbb{Z}_۶[x]$.

۲. فرض کنید R دامنه‌ی صحیح و $a_۱$، $a_۲$، ...، a_n، $(n \geq ۲)$، عناصر ناصفر R باشند. اگر $d_۱$ و $d_۲$ دو بزرگ‌ترین مقسوم‌علیه مشترک $a_۱$، $a_۲$، ...، a_n باشد ثابت کنید $d_۱$ و $d_۲$ همدم‌اند.

۳. فرض کنید R یک PID باشد. ثابت کنید معادله‌ی هم‌نهشتی $ax \equiv b \mod c$، که در آن a، b، و c عناصر ناصفر R هستند، در R جواب دارد اگر و تنها اگر $\gcd\{a,c\}|b$. (معادله‌ی $ax \equiv b \mod c$، یعنی $c|(ax-b)$ در R.)

۴. فرض کنید R دامنه‌ی صحیح باشد. اگر $a,b,c \in R$ ناصفر باشند و $\gcd\{a,b\}$ و $\gcd\{ca,cb\}$ وجود داشته باشد، نشان دهید $\gcd\{ca,cb\}=c\gcd\{a,b\}$.

۵. فرض کنید R دامنه‌ی صحیح باشد. نشان دهید دو شرط زیر معادل‌اند
(الف) برای هر $a,b \in R$ ایدآل تولید شده توسط b، a، یعنی (a,b)، اصلی است.
(ب) اگر b، a اعضای ناصفر R باشند، آنگاه $d=\gcd\{a,b\}$ وجود دارد و $d=ra+sb$، که در آن $s \in R$.

۶. فرض کنید R دامنه‌ی صحیح باشد. اگر هر ایدآل متناهیاً تولید شده‌ی R ایدآل اصلی باشد، نشان دهید به ازای هر $a_۱,\ldots,a_n \in R$، $d=\gcd\{a_۱,\ldots,a_n\}$ وجود دارد و $(a_۱,\ldots,a_n)=(d)$.

۷. فرض کنید R، UFD باشد. نشان دهید R، PID است اگر و تنها اگر برای هر $a \neq ۰$ و $b \neq ۰$ در R اعضای $r,s \in R$ وجود داشته باشند که $\gcd\{a,b\}=ra+tb$.

۲.۱۲ عناصر اول و تحویل‌ناپذیر

در این بخش مفاهیم اول و تحویل‌ناپذیری در یک حلقه‌ی تعویض‌پذیر و یکدار را بررسی می‌کنیم و ثابت می‌کنیم در یک PID این مفاهیم یکی هستند. فرض کنید R حلقه‌ی تعویض‌پذیر و یکدار باشد. یادآوری می‌کنیم که عضو ناصفر و نایکه‌ی $p \in R$ را عضو اول نامیده می‌شود،

هرگاه از $p|ab$ $(a,b\in R)$ نتیجه شود $p|a$ یا $p|b$.
عضو ناصفر و نایکه‌ی $p\in R$ را تحویل‌ناپذیر گوییم هرگاه از $p=ab$، $(a,b\in R)$ نتیجه شود که یا a و یا b یکه است. عضو p را تحویل‌پذیر گوییم هرگاه تحویل‌ناپذیر نباشد.
$a,b\in R$ را نسبت به هم اول گوییم هرگاه همه‌ی مقسوم‌علیه‌های مشترک آن‌ها یکه باشند.
اگر $p\in\mathbb{Z}$ یک عدد اول باشد، آنگاه به مفهوم تعریف بالا p و $-p$ عناصر تحویل‌ناپذیر و اول هستند. از تعریف عضو تحویل‌ناپذیر نتیجه می‌شود که تنها شمارنده‌های یک عضو تحویل‌ناپذیر p، همدم‌های p و عناصر یکه‌ی R هستند :

قضیه ۱.۲.۱۲. فرض کنید R حلقه‌ی تعویض‌پذیر و $p\in R$ عضوی ناصفر و نایکه باشد. اگر p تحویل‌ناپذیر باشد، آنگاه تنها شمارنده‌های p، همدم‌های p و یکه‌های R هستند.

اثبات. فرض کنید $a\in R$ یکه نباشد و $a|p$. آنگاه $b\in R$ وجود دارد که $p=ab$. چون p تحویل‌ناپذیر است، یا a یکه است و یا b یکه است. چون a یکه نیست، b یکه است. پس a همدم p است. □

عکس قضیه‌ی ۱.۲.۱۲، در حالت کلی درست نیست. اما در حالتی که R دامنه‌ی صحیح باشد درست است:

قضیه ۲.۲.۱۲. فرض کنید R دامنه‌ی صحیح و $p\in R$ عضوی ناصفر و نایکه باشد. در این صورت p تحویل‌ناپذیر است اگر و تنها اگر تنها همدم‌های p، همدم‌های p و یکه‌های R باشند.

اثبات. فرض کنید $a,b\in R$ و $p=ab$. اگر a یکه نباشد، آنگاه چون $a|p$، طبق فرض a همدم p است. پس عضو یکه‌ی $u\in R$ وجود دارد که $a=pu$. اکنون داریم $p=ab=pub$. چون R دامنه‌ی صحیح است $ub=1$، یعنی b یکه است. از این‌رو p تحویل‌ناپذیر است. □

مثال ۳.۲.۱۲. یکه‌های حلقه‌ی تعویض‌پذیر و یکدار $\mathbb{Z}_6$ عبارت‌اند از $\bar{1}$، $\bar{5}$. چون $\bar{3}\times\bar{3}=\bar{3}$ و $\bar{3}$ یکه نیست، $\bar{3}$ تحویل‌پذیر است. اما $\bar{3}$ همدم $\bar{3}$ است، زیرا $\bar{5}\times\bar{3}=\bar{3}$. هم‌چنین می‌توان تحقیق کرد که تنها همدم‌های $\bar{3}$، همدم‌های $\bar{3}$ و یکه‌های $\mathbb{Z}_6$ هستند. اکنون نشان می‌دهیم $\bar{3}$ در $\mathbb{Z}_6$ اول است. فرض کنید $\bar{a},\bar{b}\in\mathbb{Z}_6$ و $\bar{3}|\bar{a}\bar{b}$. پس $\bar{c}\in\mathbb{Z}_6$ وجود دارد که $\bar{a}\bar{b}=\bar{3}\bar{c}$، یعنی $\overline{ab}=\overline{3c}$. در نتیجه $6|(ab-3c)$. چون $3|6$، $3|(ab-3c)$. اکنون چون $3|3c$، $3|ab$. چون 3 در $\mathbb{Z}$ اول است، $3|a$ یا $3|b$. بنابراین $\bar{3}|\bar{a}$ یا $\bar{3}|\bar{b}$. در نتیجه $\bar{3}$ عضو اول در $\mathbb{Z}_6$ است. □

اکنون از مفاهیم اول و تحویل‌ناپذیر چند مثال می‌آوریم.

مثال ۴.۲.۱۲. در حلقه‌ی $\mathbb{Z}[x,y]$، عناصر x و y تحویل‌ناپذیرند. $2x$ اول نیست، زیرا $2x|2x$ و $2\nmid x$ و $2x\nmid 2$. هم‌چنین $2x$ تحویل‌پذیر است. x^2 و y^2 نسبت به هم اول‌اند اما هیچ‌کدام تحویل‌ناپذیر و یا اول نیستند.

مثال ۵.۲.۱۲. در حلقه‌ی اعداد صحیح گاوسی $R=\mathbb{Z}[i]=\{m+ni\mid m,n\in\mathbb{Z}\}$ نشان دهید $p=1+i$ تحویل‌ناپذیر است.

حل فرض کنید $a,b\in R$ و $p=ab$. بنابراین $|p|^2=|a|^2|b|^2=2$. چون $|a|^2$ و $|b|^2$ اعداد صحیح هستند، $|a|^2=1$ یا $|b|^2=1$. فرض کنید $|a|^2=1$. اگر $a=m+ni$، که $m,n\in\mathbb{Z}$، آنگاه $m^2+n^2=|a|^2=1$. پس $a\in\{1,-1,i,-i\}$ و در نتیجه a در R یکه است. □

در حلقه‌ی $R=\mathbb{Z}[\sqrt{k}]$، که در آن k عدد صحیح است، تابع $N:\mathbb{Z}[\sqrt{k}]\longrightarrow\mathbb{Z}$ را با

$$N\left(n+m\sqrt{k}\right)=\left(m+m\sqrt{k}\right)\left(n-m\sqrt{k}\right)=n^2-km^2$$

تعریف می‌کنیم. واضح است که برای هر $a,b\in R$، $N(ab)=N(a)N(b)$. هم‌چنین توجه کنید اگر $k=-t<0$، آنگاه $R=\mathbb{Z}[i\sqrt{t}]$ و

$$N\left(n+mi\sqrt{t}\right)=\left(n+mi\sqrt{t}\right)\left(n-mi\sqrt{t}\right)=n^2+tm^2.$$

مثال ۶.۲.۱۲. نشان دهید $p=1+i\sqrt{5}$ در حلقه‌ی $R=\mathbb{Z}[i\sqrt{5}]$، تحویل‌ناپذیر است.

حل فرض کنید $a,b\in R$، $p=ab$. در نتیجه $۶=N(p)=N(ab)=N(a)N(b)$. به وضوح برای هر $c\in R$، $N(c)\neq ۲$، $N(c)\neq ۳$، که نتیجه می‌دهد $N(a)=۱$ یا $N(b)=۱$. بنابراین $a=\pm ۱$ یا $b=\pm ۱$. پس یا a یا b یکه است. □

قضیه ۷.۲.۱۲. اگر p عضوی اول از دامنه‌ی صحیح R باشد، آنگاه p تحویل‌ناپذیر است.

اثبات. فرض کنید $a,b\in R$ و $p=ab$، به ویژه $p|ab$ و چون p اول است، $p|a$ یا $p|b$. اگر $p|a$، آنگاه $q\in R$ وجود دارد که $a=pq$. بنابراین $p=ab=pqb$. چون R دامنه‌ی صحیح است و $p\neq ۰$، $qb=۱$. از این‌رو b یکه است. به همین نحو اگر $p|b$، آنگاه a یکه است. بنابراین p تحویل‌ناپذیر است. □

عکس قضیه‌ی ۷.۲.۱۲، درست نیست. مثال بعد این مطلب را نشان می‌دهد.

مثال ۸.۲.۱۲. نشان دهید ۳ در $R=\mathbb{Z}[i\sqrt{۵}]$ تحویل‌ناپذیر است اما اول نیست.

حل اگر $a,b\in R$ و $ab=۳$. آنگاه $۹=N(۳)=N(a)N(b)$. به وضوح به ازای هر $c\in R$، $N(c)\neq ۳$. پس $N(a)=۱$ یا $N(b)=۱$. از این‌رو $a=\pm ۱$ یا $b=\pm ۱$. بنابراین یا a و یا b در R یکه‌اند. در نتیجه $۳=۳+۰i\sqrt{۵}$ در R تحویل‌ناپذیر است. اکنون $۳|۶$ و $۳|(۱+i\sqrt{۵})(۱-i\sqrt{۵})=۶$. فرض کنید $۳|(۱+i\sqrt{۵})$. پس اعداد صحیح $m,n\in\mathbb{Z}$ وجود دارند که $۱+i\sqrt{۵}=۳(m+in\sqrt{۵})$. بنابراین $۳m=۱$، که تناقض است. از این‌رو $۳\nmid(۱+i\sqrt{۵})$ به طریق مشابه $۳\nmid(۱-i\sqrt{۵})$. پس ۳ اول نیست. □

در قضیه‌ی بعد نشان می‌دهیم عکس قضیه‌ی ۷.۲.۱۲، در حلقه‌های ایدآل اصلی برقرار است.

قضیه ۹.۲.۱۲. فرض کنید R یک حلقه‌ی ایدآل اصلی باشد و $p\in R$. اگر p تحویل‌ناپذیر باشد، آنگاه p اول است.

اثبات. فرض کنید $a,b\in R$ و $p|ab$. بنابراین عضو $r\in R$ وجود دارد که $ab=pr$. چون R حلقه‌ی ایدآل اصلی است، عضو d وجود دارد که $(p,b)=(d)$. پس $q\in R$ وجود دارد که $p=dq$. چون p تحویل‌ناپذیر است یا d و یا q یکه‌اند. اگر d یکه باشد، آنگاه $(p,b)=(d)=R$. از این‌رو $s,t\in R$ وجود دارند که $sp+tb=۱$. در نتیجه $a=asp+atb=asp+tpr=(as+tr)p$. از این‌رو $p|a$. از طرف دیگر اگر q یکه باشد، آنگاه $d=pq^{-۱}\in(p)$. بنابراین $(d)\subseteq(p)\subseteq(p,b)=(d)$ و $(p)=(p,b)$. در نتیجه $b\in(p)$ و $p|b$. □

نتیجه ۱۰.۲.۱۲. اگر R دامنه‌ی ایدآل اصلی باشد و $p\in R$، آنگاه p تحویل‌ناپذیر است اگر و تنها اگر اول باشد. □

قضیه ۱۱.۲.۱۲. فرض کنید R حلقه‌ی ایدآل اصلی باشد و $a,b\in R$. اگر a و b نسبت به هم اول باشند، آنگاه $s,t\in R$ وجود دارند که $sa+tb=۱$.

اثبات. چون مقسوم‌علیه‌های مشترک a، b، یکه هستند، ۱ بزرگ‌ترین مقسوم‌علیه مشترک a و b است. نتیجه از قضیه‌ی ۸.۱.۱۲، حاصل می‌شود. □

تمرین‌ها

۱. یکه‌های (الف) $\mathbb{Z}[i\sqrt{۵}]$ (ب) $\mathbb{Z}[i\sqrt{۳}]$ را بیابید.

۲. تعیین کنید کدام‌یک از عناصر ۱۱، $۲-i$، ۵ و $۷-i$ در $\mathbb{Z}[i]$ تحویل‌ناپذیرند.

۳. تعیین کنید کدام‌یک از عناصر $۲+i\sqrt{۵}$، ۶، ۷، ۲۹ و $۲-۳i\sqrt{۵}$ در $\mathbb{Z}[i\sqrt{۵}]$ تحویل‌ناپذیرند.

۴. کدام‌یک از عناصر $۲+i\sqrt{۵}$ و $۱+۲i\sqrt{۵}$ در $\mathbb{Z}[i\sqrt{۵}]$ تحویل‌ناپذیرند اما اول نیستند.

۵. کدام‌یک از عناصر $۳+۲i\sqrt{۳}$، $۲+۳i\sqrt{۳}$، ۵ و ۷ در $\mathbb{Z}[i\sqrt{۳}]$ اول‌اند.

۶. نشان دهید $۱+i\sqrt{۳}$ و $۱+۲i\sqrt{۳}$ در $\mathbb{Z}[i\sqrt{۳}]$ تحویل‌ناپذیرند اما اول نیستند.

۷. نشان دهید $۱+\sqrt{۵}$ در $\mathbb{Z}[\sqrt{۵}]$ تحویل‌ناپذیر است ولی اول نیست.

۸. فرض کنید $p\in\mathbb{Z}$ عدد اول باشد که $p\equiv ۳ \mod ۴$. نشان دهید p در $\mathbb{Z}[i]$ اول، و بنابراین تحویل‌ناپذیر است.

۹. فرض کنید $p \in \mathbb{Z}$ عدد اول باشد که $p \equiv ۱ \mod ۴$. نشان هید
(الف) $k \in \mathbb{Z}$ وجود دارد که $k^۲ + ۱ \equiv ۰ \mod p$.
(ب) p در $\mathbb{Z}[i]$ اول نیست.
(ج) $m, n \in \mathbb{Z}$ وجود دارند که $p = m^۲ + n^۲$.

۳.۱۲ دامنه‌های تجزیه‌ی یکتا

دامنه‌ی صحیح R را دامنه‌ی تجزیه (FD) می‌نامیم، هرگاه هر عضو ناصفر و نایکه‌ی آن را بتوان به صورت حاصل‌ضرب تعداد i از عناصر تحویل‌ناپذیر R نوشت. در بخش قبل دیدیم که در یک دامنه‌ی صحیح R، هر عضو ناصفر a را همدم‌های a و یکه‌های R عدد می‌کنند. این عناصر را شمارنده‌های بدیهی a گوییم و هر عامل دیگر (در صورت وجود) را عامل نابدیهی گوییم. برای مثال ± ۲ و ± ۳ در $\mathbb{Z}$ عوامل نابدیهی ۶ در $\mathbb{Z}$ هستند. $\mathbb{Z}$، هر میدان F و $F[x]$ مثالهایی از دامنه‌های تجزیه هستند.
در لم بعد نشان می‌دهیم اگر یک عضو ناصفر و نایکه را نتوان به صورت حاصل‌ضرب تحویل‌ناپذیرها نوشت، آنگاه می‌توان آن را به صورت حاصل‌ضرب هر تعداد دلخواه از عوامل نابدیهی نوشت.

لم ۱.۳.۱۲. فرض کنید R یک دامنه‌ی صحیح باشد. اگر عضو ناصفر و نایکه‌ی $a \in R$ هیچ تجزیه‌ای به عوامل تحویل‌ناپذیر نداشته باشد، آنگاه به ازای هر عدد صحیح n، اعضای ناصفر و نایکه‌ی $a_۱, a_۲, \ldots, a_n \in R$ وجود دارند که $a = a_۱ a_۲ \cdots a_n$.

اثبات. اگر a تحویل‌ناپذیر باشد، آنگاه خود a تجزیه‌ای برای a به عوامل تحویل‌ناپذیر است. پس a تحویل‌پذیر است و در نتیجه $a_۱, b_۱ \in R$ وجود دارند که $a = a_۱ b_۱$. هرگاه هم $a_۱$ و هم $b_۱$ را بتوان به عوامل تحویل‌ناپذیر تجزیه کرد، با قرار دادن این دو تجزیه کنار هم یک تجزیه به عوامل تحویل‌ناپذیر برای a حاصل می‌شود. بنابراین یا $a_۱$ و یا $b_۱$ را نمی‌توان به عوامل تحویل‌ناپذیر تجزیه کرد. فرض کنید مثلاً $a_۱$ را نتوان به عوامل تحویل‌ناپذیر تجزیه کرد. پس $a_۱$ عضو ناصفر و نایکه‌ی R است که تحویل‌پذیر است. در نتیجه $a_۲, b_۲ \in R$ وجود دارند که $a_۱ = a_۲ b_۲$. بنابراین $a = a_۲ b_۲ b_۱$. مثل قبل یکی از $a_۲$ و $b_۲$ را نمی‌توان به عوامل تحویل‌ناپذیر تجزیه کرد. اگر مثلاً $a_۲$ را نتوان به عوامل تحویل‌ناپذیر تجزیه کرد، همانند استدلال قبل با $a_۲$ عمل می‌کنیم. با ادامه روند فوق عوامل نابدیهی $a_۱, a_۲, \ldots, a_n \in R$ از a را می‌یابیم که $a = a_۱ a_۲ \cdots a_n$. □

قضیه ۲.۳.۱۲. فرض کنید R دامنه‌ی صحیح باشد و تابع $N : R - \{۰\} \longrightarrow \mathbb{N}$ وجود داشته باشد، طوری که به ازای هر $a, b \in R - \{۰\}$، $N(ab) \geq N(b)$، که در آن تساوی وقتی و فقط وقتی برقرار است که a یکه باشد. در این صورت R یک FD است.

اثبات. فرض کنید حکم درست نباشد. پس عضو ناصفر و نایکه‌ی $a \in R$ وجود دارد که به عوامل تحویل‌ناپذیر تجزیه نمیشود. اکنون $N(a) \in \mathbb{N}$. قرار می‌دهیم $n = N(a)$. بنا به لم ۱.۳.۱۲، a را می‌توان به صورت حاصل‌ضرب $n + ۲$ عامل نابدیهی $a_۱, a_۲, \ldots, a_{n+۲} \in R$ نوشت. بنابراین $a = a_۱ a_۲ \cdots a_{n+۲}$ و چون هیچ‌کدام از a_iها یکه نیستند، داریم

$$\begin{aligned} n &= N(a) \\ &= N(a_۱ a_۲ \cdots a_{n+۲}) > N(a_۲ \cdots a_{n+۲}) > \\ &\qquad N(a_۳ \cdots a_{n+۲}) > \cdots > N(a_{n+۲}). \end{aligned}$$

از این‌رو حداقل $n + ۱$ عدد صحیح نامنفی که اکیداً از n کمترند وجود دارند، که تناقض است. پس R یک FD است. □

مثال ۳.۳.۱۲. دامنه‌ی صحیح $\mathbb{Z}[i]$ را در نظر بگیرید. تابع $N : \mathbb{Z}[i] - \{۰\} \longrightarrow \mathbb{N}$ را با ضابطه‌ی $N(a) = |a|^۲$، به ازای هر $a \in \mathbb{Z}[i] - \{۰\}$ تعریف می‌کنیم. توجه کنید که اگر $a = n + mi$، آنگاه $N(a) = n^۲ + m^۲$. هم‌چنین چون

$$\begin{aligned} ab = ۱ &\iff N(ab) = ۱ \\ &\iff |ab|^۲ = ۱ \\ &\iff |a| = |b| = ۱, \end{aligned}$$

پس $a \in \mathbb{Z}[i]$ یکه است اگر و تنها اگر $N(a) = ۱$. حال اگر $a, b \in \mathbb{Z}[i]$ دو عضو ناصفر باشند، آنگاه

$$N(ab) = |ab|^۲ = |a|^۲|b|^۲ \geq |b|^۲ = N(b),$$

یعنی $N(ab) \geq N(b)$، و تساوی وقتی و فقط وقتی برقرار است که a یکه باشد (یعنی $N(a) = |a|^۲ = ۱$). بنابراین $\mathbb{Z}[i]$،یک FD است. □

تعریف ۴.۳.۱۲. گوییم دامنه‌ی صحیح R در شرط زنجیر صعودی ایدآل‌های اصلی یا ACCP صدق می‌کند هرگاه به ازای هر زنجیر

$$(a_۱) \subseteq (a_۲) \subseteq (a_۳) \subseteq \cdots$$

از ایدآل‌های R، عدد صحیح مثبت n (وابسته به زنجیر) وجود داشته باشد که به ازای هر $t \geq n$، $(a_n) = (a_t)$.

لم ۵.۳.۱۲. هر دامنه‌ی ایدآل اصلی R در ACCP صدق می‌کند.

اثبات. فرض کنید $(a_۱) \subseteq (a_۲) \subseteq (a_۳) \subseteq \cdots$ زنجیرi از ایدآل‌های اصلی در R باشد. به سادگی می‌توان دید $I = \bigcup_{m=۱}^{\infty}(a_m)$ ایدآلی از R است. چون R یک PID است پس عضو $a \in R$ وجود دارد که $I = (a)$. چون $a \in (a) = I = \bigcup_{m=۱}^{\infty}(a_m)$، عدد طبیعی n وجود دارد که $a \in (a_n)$. در نتیجه $I = (a) \subseteq (a_n) \subseteq I$ و بنابراین $I = (a_n)$. به ازای هر $t \geq n$، داریم $(a_t) \subseteq I = (a_n) \subseteq (a_t)$، یعنی $(a_n) = (a_t)$، به ازای هر $t \geq n$. □

قضیه ۶.۳.۱۲. هر دامنه‌ی صحیح R که در ACCP صدق کند، FD است.

اثبات. فرض کنید R، FD نباشد. پس عضو ناصفر و نایکه‌ی $a \in R$ وجود دارد که به عوامل تحویل‌ناپذیر تجزیه نمیشود. پس a تحویل‌پذیر است و اعضای $a_۱, a_۲ \in R$ وجود دارند که عوامل نابدیهی a هستند و $a = a_۱b_۱$. اگر هم $a_۱$ و هم $b_۱$ به حاصل‌ضرب عوامل تحویل‌ناپذیر تجزیه شوند با قرار دادن دو تجزیه کنار هم، تجزیه به عوامل تحویل‌ناپذیر برای a حاصل‌ضرب می‌شود. پس یا $a_۱$ و یا $b_۱$ به حاصل‌ضرب عوامل تحویل‌ناپذیر تجزیه نمی‌شوند. مثلاً فرض کنید $a_۱$ به عوامل تحویل‌ناپذیر تجزیه نمی‌شود. اکنون a و $a_۱$ همدم نیستند. پس $(a) \subset (a_۱)$. چون $a_۱$ به عوامل تحویل‌ناپذیر تجزیه نمی‌شود، عوامل نابدیهی $a_۲, b_۲ \in R$ وجود دارند که $a_۱ = a_۲b_۲$. مثل قبل حداقل یکی از $a_۲$ یا $b_۲$ به عوامل تحویل‌ناپذیر تجزیه نمیشوند، مثلاً $a_۲$، آنگاه $(a) \subset (a_۱) \subset (a_۲)$. اگر این روند را ادامه دهیم زنجیر صعودی اکید نامتناهی از ایدآل‌های اصلی R را می‌یابیم، که تناقض است. پس R یک FD است. □

نتیجه ۷.۳.۱۲. هر PID یک FD است. □

تعریف ۸.۳.۱۲. دامنه‌ی صحیح R را دامنه‌ی یکتایی تجزیه یا UFD گوییم هرگاه
(الف) هر عضو ناصفر و نایکه‌ی $a \in R$ را بتوان به صورت

$$a = p_۱p_۲ \cdots p_n$$

تجزیه کرد، که در آن $p_۱$، $p_۲$، . . .، p_n عناصر تحویل‌ناپذیر R هستند و
(ب) اگر $a = p_۱p_۲ \cdots p_n = q_۱q_۲ \cdots q_m$ دو تجزیه‌ی a به حاصل‌ضرب عناصر تحویل‌ناپذیر R باشد، آنگاه $m = n$ و پس از تعویض ترتیب q_iها (در صورت لزوم)، p_i و q_i، برای هر $i = ۱, ۲, \ldots, n$، همدم باشند.

بنابراین دامنه‌ی صحیح R،یک UFD است اگر و تنها اگر R، FD باشد و هر عضو ناصفر و نایکه‌ی R را بتوان به صورت یکتا (صرف نظر از عوامل یکه و ترتیب عومل) بر حسب حاصل‌ضرب تعداد متناهی عناصر تحویل‌ناپذیر نوشت.
ابتدا یک خاصیت جالب از UFD ثابت می‌کنیم. می‌دانیم در هر دامنه‌ی صحیح یک عضو اول یک عضو عضو تحویل‌ناپذیر است. ثابت می‌کنیم عکس مطلب در UFD درست است:

قضیه ۹.۳.۱۲. فرض کنید R یک UFD باشد و $p \in R$. اگر p تحویل‌ناپذیر باشد، آنگاه p اول است.

اثبات. فرض کنید $a,b\in R$ و $p|ab$. اگر $a=0$، آنگاه $p|a$ و اگر $b=0$، آنگاه $p|b$. اگر a یکه باشد، آنگاه $p|b$ و اگر b یکه باشد آنگاه $p|a$. پس می‌توانیم فرض کنیم a و b هر دو ناصفر و نایکه هستند. چون $p|ab$ عضو $c\in R$ وجود دارد که $ab=pc$. فرض کنید $d=pc=ab$. چون a و b یکه نیستند پس d یکه نیست. اگر c یکه باشد، آنگاه $d=pc$ تحویل‌ناپذیر است بنابراین یا a یا b یکه‌اند، که تناقض است، پس c یکه نیست. چون R یک UFD است، عناصر تحویل‌ناپذیر c_1، c_2، ...، c_n، a_1، a_2، ...، a_m، b_1، b_2، ...، b_r در R وجود دارند که $c=c_1c_2\cdots c_n$، $a=a_1a_2\cdots a_m$، و $b=b_1b_2\cdots b_r$. پس $d=pc_1c_2\cdots c_n=a_1a_2\cdots a_mb_1b_2\cdots b_r$ دو تجزیه‌ی d به حاصل‌ضرب عوامل تحویل‌ناپذیرند. چون R یک UFD است، p باید با یکی از عناصر تحویل‌ناپذیر a_1، a_2، ...، a_m، b_1، b_2، ...، b_r همدم باشد. اگر به ازای یک j، p و a_j همدم باشند، آنگاه $p|a$. و اگر به ازای یک i، p و b_i همدم باشند، آنگاه $p|b$. بنابراین p اول است. □

مثال ۱۰.۳.۱۲. دامنه‌ی صحیح $\mathbb{Z}[i\sqrt{5}]$، UFD نیست. زیرا $3+0i=3=3$ تحویل‌ناپذیر است ولی اول نیست (در مثال ۸.۲.۱۲ این مطلب نشان داده شده است). □

قضیه ۱۱.۳.۱۲. یک دامنه‌ی تجزیه‌ی R، UFD است اگر و تنها اگر هر عضو تحویل‌ناپذیر در R اول باشد.

اثبات. ($\Longleftarrow$) قضیه‌ی ۹.۳.۱۲.

($\Longrightarrow$) فرض کنید $a\in R$ و $a=p_1p_2\cdots p_n=q_1q_2\cdots q_m$ دو تجزیه‌ی a به عوامل تحویل‌ناپذیر باشد. به استقرا روی $\max\{n,m\}$ ثابت می‌کنیم $m=n$ و، پس از تعویض ترتیب اندیس‌ها، $p_i=q_i$. حالت $\max\{n,m\}=1$ بدیهی است؛ پس حالت $\max\{n,m\}>1$ را در نظر می‌گیریم و فرض می‌کنیم حکم برای تجزیه‌ی عناصر R به عوامل تحویل‌ناپذیر با تعداد عوامل کمتر از $\max\{n,m\}$ درست باشد. از این که $p_1p_2\cdots p_n=q_1(q_2\cdots q_m)$ نتیجه می‌گیریم که $q_1|p_1p_2\cdots p_n$. چون q_1 تحویل‌ناپذیر است، طبق فرض، اول است. بنابراین i وجود دارد که $q_1|p_i$. با تعویض ترتیب p_iها فرض می‌کنیم $i=1$، پس $q_1|p_1$. اکنون چون p_1 و q_1 هر دو تحویل‌ناپذیرند، عضو یکه‌ی $u_1\in R$ وجود دارد که $p_1=u_1q_1$. در نتیجه

$$u_1q_1p_2\cdots p_n=q_1q_2\cdots q_m.$$

چون R دامنه‌ی صحیح است با حذف q_1 از طرفین تساوی داریم $u_1p_2\cdots p_n=q_2\cdots q_m$. طبق فرض استقرا $n-1=m-1$ و با تعویض ترتیب p_jها، q_i با p_i، $i=1,\ldots,n$، همدم است. از این‌رو R یک UFD است. □

نتیجه ۱۲.۳.۱۲. هر PID یک UFD است. □

تمرین‌ها

۱. نشان دهید $\mathbb{Z}$ در ACCP صدق می‌کند.

۲. اگر دامنه‌ی صحیح R در ACCP صدق کند، نشان دهید $R[x]$ نیز در ACCP صدق می‌کند.

۳. ثابت کنید دامنه‌ی صحیح R، UFD است اگر و تنها اگر R در ACCP صدق کند و هر عضو تحویل‌ناپذیر، در R اول باشد.

۴. نشان دهید $\mathbb{Z}[i\sqrt{5}]$، $\mathbb{Z}[i\sqrt{7}]$، $\mathbb{Z}[i\sqrt{10}]$، FD هستند، اما UFD نیستند.

۵. نشان دهید در یک UFD بزرگ‌ترین مقسوم‌علیه مشترک دو عضو همواره وجود دارد.

۶. فرض کنید R یک UFD و $a,b\in R$ ناصفر باشند. اگر $\gcd\{a,b\}=1$ و $a|c$ و $b|c$، ثابت کنید $ab|c$، که در آن $c\in R$.

۷. اگر در یک UFD داشته باشیم $a|bc$ و $\gcd\{a,b\}=1$، نشان دهید $a|c$.

۸. نشان دهید در یک UFD، هر عضو تعداد متناهی شمارنده‌ی نابدیهی ناهمدم دارد.

۹. نشان دهید $R=\{a_0+a_1x+\cdots+a_nx^n\in\mathbb{Q}[x]\mid a_0\in\mathbb{Z},\ \ n\in\mathbb{N}\}$ یک UFD نیست.

۱۰. فرض کنید R دامنه‌ی صحیح باشد. نشان دهید R، PID است اگر و تنها در ACCP صدق کند و هر ایدآل ۲ مولدی آن اصلی باشد.

۴.۱۲ تجزیه‌ی چندجمله‌ای‌ها روی یک UFD

در این بخش نشان می‌دهیم که هر چندجمله‌ای غیرثابت روی یک حلقه‌ی UFD را می‌توان به طور یکتا بر حسب چندجمله‌ای‌های تحویل‌ناپذیر تجزیه کرد.

تعریف ۱.۴.۱۲. فرض کنید R یک UFD و $f(x)=a_۰+a_۱x+\cdots+a_nx^n$ چندجمله‌ای ناصفر در $R[x]$ باشد. در این صورت $\gcd\{a_۰,a_۱,\ldots,a_n\}$ را محتوای $f(x)$ گوییم و با $C(f(x))$ نشان می‌دهیم.

می‌دانیم که در یک UFD ، $\gcd\{a_۰,a_۱,\ldots,a_n\}$ عضوی یکتاست؛ به این معنی که اگر u و v دو بزرگ‌ترین مقسوم‌علیه مشترک $\{a_۰,a_۱,\ldots,a_n\}$ باشند، آن‌گاه u و v همدم هستند. بنابراین اگر $c_۱$ و $c_۲$ دو محتوای $f(x)$ باشند، آن‌گاه $c_۱$ و $c_۲$ همدم هستند و هر همدم $c_۱$ نیز محتوای $f(x)$ است. اگر $a,b\in R$ دو همدم باشند می‌نویسیم $a\sim b$.

تعریف ۲.۴.۱۲. فرض کنید R یک UFD باشد. چندجمله‌ای ناصفر $f(x)\in R[x]$ را چندجمله‌ای اولیه گوییم، هرگاه محتوای آن یکه باشد.

لم ۳.۴.۱۲. اگر R یک UFD و $g(x)$، $f(x)$ دو چندجمله‌ای اولیه در $R[x]$ باشند، آن‌گاه $f(x)g(x)$ نیز اولیه است.

اثبات. برای سادگی می‌نویسیم $f=f(x)$. فرض کنید $C(f)\sim a$ و $C(g)\sim b$. پس فرض کنید

$$f(x)=a_۰+a_۱x+\cdots+a_nx^n \quad و \quad g(x)=b_۰+b_۱x+\cdots+b_mx^m.$$

چون $f(x)$ و $g(x)$ اولیه‌اند، عناصر $C(f)$ و $C(g)$ در R یکه هستند. فرض کنید بر خلاف حکم $f(x)g(x)$ اولیه نباشد. قرار می‌دهیم $f(x)g(x)=c_۰+c_۱x+\cdots+c_{n+m}x^{n+m}$
که در آن

$$c_i=\sum_{j=۰}^{i}a_jb_{i-j},\quad i=۰,۱,\ldots,m+n,$$

که در آن $a_j=۰$، اگر $j>n$ و $b_{i-j}=۰$، اگر $i-j>m$. اکنون $C(f(x)g(x))$ یکه نیست. فرض کنید p عضو اولی در R باشد که $C(f(x)g(x))$ را عاد می‌کند. در این صورت به ازای هر $i=۰,۱,\ldots,n+m$،
$p|c_i$. چون $C(f)$ و $C(g)$ یکه هستند، p مقسوم‌علیه مشترک عناصر $a_۰$، $a_۱$، ...، a_n نیست. هم‌چنین p مقسوم‌علیه مشترک عناصر $b_۰$، $b_۱$، ...، b_m نیست. فرض کنید t کوچک‌ترین عدد صحیح نامنفی باشد که $p\nmid a_t$ و r کوچک‌ترین عدد صحیح نامنفی باشد که $p\nmid b_r$. پس برای $i=۰,۱,\ldots,t-۱$، $p|a_i$ و $p\nmid a_t$؛ و برای $j=۰,۱,\ldots,r-۱$، $p|b_j$ و $p\nmid b_r$. در نتیجه $p\nmid a_tb_r$. اکنون داریم

$$c_{t+r}=a_۰b_{t+r}+a_۱b_{t+r-۱}+\cdots+a_{t-۱}b_{r+۱}+a_tb_r+a_{t+۱}b_{r-۱}+\cdots+a_{t+r}b_۰$$

که در آن $b_i=۰$، اگر $i>m$ و $a_i=۰$، اگر $i>n$. چون $p|a_i$ برای هر $i=۰,۱,\ldots,t-۱$ و $p|b_j$ برای هر $j=۰,۱,\ldots,r-۱$ و $p|c_{t+r}$. پس $p|a_tb_r$، که تناقض است پس $C(f(x)g(x))$ یکه است، یعنی $f(x)g(x)$ اولیه است. □

مثال ۴.۴.۱۲. در $\mathbb{Z}[x]$ داریم $۶x^۲+۳x-۹=۳(۲x^۲+x-۳)$. پس $۶x^۲+۳x-۹$ اولیه نیست، اما $۲x^۲+x-۳$ چندجمله‌ای اولیه است. □

قضیه ۵.۴.۱۲. اگر R یک UFD و $f(x),g(x)\in R[x]$ چندجمله‌ای‌های ناصفر باشند، آن‌گاه $C(f(x)g(x))\sim C(f(x))C(g(x)))$، یعنی عضو یکه‌ی $u\in R$ وجود دارد که

$$C(f(x)g(x))=uC(f(x))C(g(x)).$$

اثبات. به خاطر سادگی در محاسبه‌ها، می‌نویسیم $f=f(x)$. فرض کنید $C(f)\sim a$ و $C(g)\sim b$. بنابراین چندجمله‌ای‌های اولیه‌ی $f_۱(x),g_۱(x)\in R[x]$ وجود دارند که $f(x)=af_۱(x)$ و $g(x)=bg_۱(x)$. اکنون چون $f(x)g(x)=abf_۱(x)g_۱(x)$، می‌توان نوشت

$$C(fg)\sim C(abf_۱g_۱)\sim abC(f_۱g_۱).$$

بنا به لم ۳.۴.۱۲، $C(f_۱g_۱)$ یکه است. از این‌رو رابطه فوق نتیجه می‌دهد

$$C(fg) \sim ab \sim aC(f_۱)bC(g_۱) \sim C(af_۱)C(bg_۱) \sim C(f)C(g)$$

و اثبات کامل است. □

فرض کنید R دامنه‌ی صحیح باشد، یادآوری می‌کنیم که $Q(R)$ میدان کسرهای R است.

لم ۶.۴.۱۲. فرض کنید R یک UFD باشد. اگر $f(x)$ یک چندجمله‌ای ناصفر در $Q(R)[x]$ باشد، آنگاه اعضای ناصفر $a, b \in R$ و چندجمله‌ای اولیه‌ی $f_۱(x) \in R[x]$ وجود دارند که $f(x) = ab^{-۱}f_۱(x)$، که در آن $b^{-۱}$ وارون b در $Q(R)[x]$ است.

اثبات. هر عضو $Q(R)$ به صورت $\frac{a}{b} = ab^{-۱}$ است که در آن $a, b \in R$ و $b \neq ۰$. بنابراین

$$f(x) = a_۰b_۰^{-۱} + a_۱b_۱^{-۱}x + \cdots + a_nb_n^{-۱}x^n$$

که در آن $a_i \in R$ و $b_i \neq ۰$، $i = ۰, ۱, \ldots, n$. اگر $b = b_۰b_۱ \cdots b_n$، آنگاه

$$bf(x) = a_۰b_۱b_۲ \cdots b_n + a_۱b_۰b_۲ \cdots b_nx + \cdots + a_nb_۰b_۱ \cdots b_{n-۱}x^n \in R[x].$$

به وضوح $bf(x)$ ناصفر است. فرض کنید $a \sim C(bf(x))$، در این صورت چندجمله‌ای اولیه‌ی $f_۱(x) \in R[x]$ وجود دارد که $bf(x) = af_۱(x)$. بنابراین $f(x) = b^{-۱}af_۱(x)$ و حکم ثابت است. □

لم ۷.۴.۱۲. فرض کنید R یک UFD و $f(x) \in R[x]$ یک چندجمله‌ای ناصفر باشد. اگر چندجمله‌ای‌های اولیه‌ی $f_۱(x), f_۲(x) \in R[x]$ و عناصر $d_۱, d_۲ \in Q(R)$ وجود داشته باشند که $f(x) = d_۱f_۱(x) = d_۲f_۲(x)$، در این صورت عضو یکه‌ی $u \in R$ وجود دارد که $d_۱ = ud_۲$.

اثبات. چون $d_۱, d_۲ \in Q(R)$، می‌نویسیم $d_۱ = ab^{-۱}$ و $d_۲ = cd^{-۱}$ که در آن $a, b, c, d \in R$. پس $f(x) = ab^{-۱}f_۱(x) = cd^{-۱}f_۲(x)$ و $adf_۱(x) = cbf_۲(x)$. چون $f_۱(x)$ و $f_۲(x)$ اولیه‌اند عضو یکه‌ی $u \in R$ وجود دارد که $ad = ucb$. بنابراین $d_۱ = ab^{-۱} = ucd^{-۱} = ud_۲$. □

قضیه ۸.۴.۱۲. اگر R یک UFD و $f(x) \in R[x]$ چندجمله‌ای اولیه‌ی ناصفر باشد، آنگاه $f(x)$ در $R[x]$ تحویل‌ناپذیر است اگر و تنها اگر $f(x)$ در $Q(R)[x]$ تحویل‌ناپذیر باشد.

اثبات. ($\Longleftarrow$) فرض کنید $f(x)$ در $Q(R)[x]$ تحویل‌پذیر باشد. پس چندجمله‌ای‌های $g(x)$ و $h(x)$ در $Q(R)[x]$ با $\deg h(x) \geq ۱$ و $\deg g(x) \geq ۱$ وجود دارند که $f(x) = h(x)g(x)$. بنا به لم ۶.۴.۱۲، اعضای $a, b, c, d \in R$ با $b \neq ۰$، $d \neq ۰$ و چندجمله‌ای‌های اولیه‌ی $h_۱(x), g_۱(x) \in R[x]$ وجود دارند که $h(x) = ab^{-۱}h_۱(x)$ و $g(x) = cd^{-۱}g_۱(x)$. پس $f(x) = ab^{-۱}cd^{-۱}h_۱(x)g_۱(x)$ و در نتیجه

$$bdf(x) = ach_۱(x)g_۱(x).$$

اکنون چون $f(x)$ و $h_۱(x)g_۱(x)$ اولیه‌اند، $bd \sim ac$. پس عضو یکه‌ی $w \in R$ وجود دارد که $bd = acw$ و در نتیجه $f(x) = wh_۱(x)g_۱(x)$. از این‌رو $f(x)$ در $R[x]$ تحویل‌پذیر است. این یک تناقض است. بنابراین $f(x)$ در $Q(R)[x]$ تحویل‌ناپذیر است.

($\Longrightarrow$) واضح است، زیرا $R[x] \subseteq Q(R)[x]$. □

مثال ۹.۴.۱۲. چندجمله‌ای $۴x + ۴ \in \mathbb{Q}[x]$ را در نظر بگیرید. چون $۴x + ۴ = ۴(x + ۱)$ و ۴ در $\mathbb{Q}[x]$ یکه و $x + ۱$ در $\mathbb{Q}[x]$ تحویل‌ناپذیر است، $۴x + ۴$ در $\mathbb{Q}[x]$ تحویل‌ناپذیر است. اما ۴ در $\mathbb{Z}[x]$ یکه نیست. در نتیجه $۴x + ۴$ در $\mathbb{Z}[x]$ تحویل‌ناپذیر نیست. هم‌چنین ۳ در $\mathbb{Z}[x]$ تحویل‌ناپذیر است، اما در $\mathbb{Q}[x]$ تحویل‌ناپذیر نیست. □

اکنون می‌خواهیم نتیجهی اصلی این بخش را ثابت کنیم. قبل از این‌که قضیه را ثابت کنیم، بعضی مطالبی که در مورد حلقه‌ی چندجمله‌ای‌های $R[x]$ ثابت شد را فهرست می‌کنیم تا به عمق قضیه‌ی اصلی این بخش پی ببریم: (الف) اگر R حلقه‌ی تعویض‌پذیر و یکدار باشد، آنگاه $R[x]$ نیز حلقه تعویض‌پذیر و یکدار است.
(ب) اگر R دامنه‌ی صحیح باشد، آنگاه $R[x]$ نیز دامنه‌ی صحیح است.
(ج) اگر R میدان باشد، آنگاه $R[x]$ میدان نیست.
(د) اگر R یک PID باشد، آنگاه $R[x]$ ممکن است PID نباشد.

قضیه ۱۰.۴.۱۲. اگر R یک UFD باشد، آنگاه $R[x]$ نیز UFD است.

اثبات. فرض کنید $f(x) \in R[x]$ چندجمله‌ای با درجه‌ی $n \geq 1$ باشد. چندجمله‌ای اولیه‌ی $f_1(x) \in R[x]$ وجود دارد که $f(x) = C(f(x))f_1(x)$. اکنون چون $Q(R)[x]$ یک UFD است و

$$f_1(x) \in R[x] \subseteq Q(R)[x],$$

چندجمله‌ای‌های تحویل‌ناپذیر $g_1(x)$، $g_2(x)$، ...، $g_r(x)$ در $Q(R)[x]$ وجود دارند که

$$f_1(x) = g_1(x)g_2(x)\cdots g_r(x).$$

بنا به لم ۶.۴.۱۲، اعضای $a_i, b_i \in R$، $b_i \neq 0$ و چندجمله‌ای‌های اولیه‌ی $h_i(x) \in R[x]$، $i = 1, 2, \ldots, r$، وجود دارند که $g_i(x) = a_i b_i^{-1} h_i(x)$. بنا به قضیه‌ی ۸.۴.۱۲، برای هر $i = 1, 2, \ldots, r$، $h_i(x)$ در $R[x]$ تحویل‌ناپذیر است. در نتیجه

$$f_1(x) = a_1 a_2 \cdots a_r b_1^{-1} b_2^{-1} \cdots b_r^{-1} h_1(x) \cdots h_r(x).$$

اگر $a = a_1 a_2 \cdots a_r$ و $b = b_1 b_2 \cdots b_r$، آنگاه

$$bf_1(x) = ah_1(x) \cdots h_r(x).$$

بنا به لم ۳.۴.۱۲، $h_r(x) \cdots h_1(x)$ اولیه است. از این‌رو عضو یکه $u \in R$ وجود دارد که $a = ub$. پس

$$f_1(x) = uh_1(x) \cdots h_r(x),$$

که نشان می‌دهد

$$f(x) = uC(f)h_1(x) \cdots h_r(x).$$

چون همدم یک چندجمله‌ای تحویل‌ناپذیر مجدداً تحویل‌ناپذیر است، $uh_1(x)$ تحویل‌ناپذیر است. پس برای هر چندجمله‌ای $f(x)$ با درجه‌ی $n \geq 1$، چندجمله‌ای‌های تحویل‌ناپذیر $g_1(x), \ldots, g_k(x) \in R[x]$ وجود دارند که

$$f(x) = C(f)g_1(x) \cdots g_k(x).$$

اگر $C(f)$ یکه نباشد اعضای تحویل‌ناپذیر $a_1, a_2, \ldots, a_t \in R$ وجود دارند که $C(f) = a_1 \cdots a_t$. پس

$$f(x) = a_1 a_2 \cdots a_t g_1(x) \cdots g_k(x).$$

حال فرض کنید

$$f(x) = a_1 a_2 \cdots a_t g_1(x) \cdots g_k(x) = b_1 b_2 \cdots b_s h_1(x) \cdots h_q(x)$$

که در آن a_i و b_j عناصر تحویل‌ناپذیر R، $i = 1, \ldots, t$، $j = 1, \ldots, s$ و

$$g_1(x), \ldots, g_k(x), h_1(x), \ldots, h_q(x)$$

عناصر تحویل‌ناپذیر $R[x]$ هستند. اکنون $g_1(x)$، ...، $g_k(x)$ و $h_1(x)$، ...، $h_q(x)$ چندجمله‌ای‌های تحویل‌ناپذیر در $R[x]$ هستند؛ پس در $R[x]$ اولیه‌اند. از این‌رو بنا به قضیه‌ی ۸.۴.۱۲، این چندجمله‌ای‌ها در $Q(R)[x]$ نیز تحویل‌ناپذیرند. چون $Q(R)[x]$ یک UFD است، $k = q$؛ و پس از تعویض جای $h_j(x)$ها در صورت لزوم، $g_i(x)$ و $h_i(x)$، $i = 1, \dots, k$، در $Q(R)[x]$ همدم‌اند و بنا به لم ۷.۴.۱۲، در $R[x]$ نیز همدم‌اند. از طرف دیگر $a_1 a_2 \cdots a_t$ و $b_1 b_2 \cdots b_s$ دو تجزیه‌ی $C(f)$ به عوامل تحویل‌ناپذیر در R هستند. پس عضو یکه‌ی $u \in R$ وجود دارد که

$$a_1 a_2 \cdots a_t = u b_1 b_2 \cdots b_s.$$

چون R یک UFD است، $t = s$ و پس از تعویض جای b_jها در صورت لزوم، a_i و b_i در R همدم‌اند. پس تجزیه‌ی $f(x)$ در $R[x]$ یکتاست و $R[x]$ یک UFD است. □

نتیجه ۱۱.۴.۱۲. اگر R یک UFD باشد، آنگاه $R[x_1, x_2, \dots, x_n]$ یک UFD است. □

تمرین‌ها

۱. مثالی از یک چندجمله‌ای اولیه بیاورید که در $\mathbb{Q}$ ریشه ای نداشته باشد.

۲. فرض کنید $f(x) \in \mathbb{Z}[x]$ تحویل‌ناپذیر باشد. ثابت کنید $f(x)$ اولیه است.

۳. فرض کنید $f(x) \in \mathbb{Z}[x]$ چندجمله‌ای اولیه‌ی غیرثابت باشد. ثابت کنید اگر $f(x)$ در $\mathbb{Q}[x]$ تحویل‌پذیر باشد، آنگاه $f(x)$ در $\mathbb{Z}[x]$ تحویل‌پذیر است.

۴. نشان دهید $\mathbb{Z}[x]$، UFD است اما PID نیست.

۵. نشان دهید $\mathbb{Q}[x, y]$، UFD است اما PID نیست.

۶. فرض کنید R یک UFD و $f(x) \in R[x]$ چندجمله‌ای اولیه باشد. نشان دهید هر شمارنده‌ی غیرثابت $f(x)$ نیز اولیه است.

۷. فرض کنید R یک UFD با میدان کسرهای $Q(R)$ و $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in R[x]$، $a_0 \neq 0$، $a_n \neq 0$، و $uv^{-1} \in Q(R)$ ریشه‌ای از $f(x)$ باشد، که در آن $u, v \in R$، $\gcd\{u, v\} = 1$. نشان دهید در R داریم $u | a_0$ و $v | a_n$.

۸. (محک آیزنشتاین) فرض کنید R یک UFD با میدان کسرهای $Q(R)$ و $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in R[x]$، $a_0 \neq 0$، $a_n \neq 0$، اگر p عضو اولی از R باشد طوری که
(الف) $p | a_i$، $i = 0, 1, \dots, n-1$.
(ب) $p \nmid a_n$.
(ج) $p^2 \nmid a_0$.
نشان دهید $f(x)$ در $Q(R)[x]$ تحویل‌ناپذیر است.

۵.۱۲ دامنه‌های اقلیدسی

دیدیم $\mathbb{Z}$ و $F[x]$، که در آن F میدان است، الگوریتم تقسیم دارند. حال این مفهوم را به طور کلی در نظر می‌گیریم.

تعریف ۱.۵.۱۲. دامنه‌ی صحیح R را دامنه‌ی اقلیدسی گوییم هرگاه تابع v از $R - \{0\}$ به $\mathbb{N}$ وجود داشته باشد که
(الف) به ازای هر $a, b \in R$ با $b \neq 0$، اعضای $q, r \in R$ وجود داشته باشند که $a = qb + r$ که در آن $r = 0$ یا $v(r) < v(b)$. و
(ب) به ازای هر $a, b \in R - \{0\}$، $v(a) \leq v(ab)$.

مثال ۲.۵.۱۲. حلقه‌ی اعداد صحیح $\mathbb{Z}$ به همراه تابع $v(a) = |a|$، به ازای هر $0 \neq a \in \mathbb{Z}$، دامنه‌ی اقلیدسی است. □

مثال ۳.۵.۱۲. اگر F میدان باشد، $F[x]$ به همراه تابع $v(f(x)) = \deg f(x)$، به ازای هر $0 \neq f(x) \in F[x]$، یک دامنه‌ی اقلیدسی است. □

مثال ۴.۵.۱۲. هر میدان همراه با تابع $v(a) = 1$، $a \neq 0$ یک دامنه‌ی اقلیدسی است. □

قضیه ۵.۵.۱۲. هر دامنه‌ی اقلیدسی PID است.

اثبات. فرض کنید I ایدآلی از دامنه‌ی اقلیدسی R باشد. اگر $I = \{۰\}$، آنگاه $I = (۰)$. پس فرض کنید $I \neq \{۰\}$. مجموعه‌ی $A = \{v(a) \mid ۰ \neq a \in I\}$ یک مجموعه‌ی ناتهی از اعداد طبیعی باشد. پس طبق اصل خوشترتیبی کوچک‌ترین عضو دارد. بنابراین عضو $۰ \neq a \in I$ وجود دارد که برای هر $۰ \neq b \in I$، $v(a) \leq v(b)$. نشان می‌دهیم $I = (a)$. چون $a \in I$ و I ایدآل است، $(a) \subseteq I$. حال فرض کنید $b \in I$؛ چون R دامنه‌ی اقلیدسی است، اعضای $q, r \in R$ وجود دارند که $b = aq + r$، که در آن $r = ۰$ یا $v(r) < v(a)$. اکنون $r = b - aq \in I$. اگر $r \neq ۰$، آنگاه $v(r) \in A$ و این متناقض با انتخاب a است. از این‌رو $r = ۰$ و $b = qa \in (a)$. در نتیجه $I \subseteq (a)$. بنابراین $I = (a)$. □

چون در هر PID بزرگ‌ترین مقسوم‌علیه مشترک دو عضو وجود دارد و ترکیب خطی آن‌ها است و هر دامنه‌ی اقلیدسی نیز PID است پس در یک دامنه‌ی اقلیدسی بزرگ‌ترین مقسوم‌علیه مشترک دو عضو وجود دارد و ترکیب خطی آن است.
اکنون با استفاده از الگوریتم اقلیدسی بزرگ‌ترین مقسوم‌علیه مشترک دو عضو a و b در یک دامنه‌ی اقلیدسی R را می‌یابیم.
مرحله اول : اعضای $q_۱ \in R$ و $r_۱$ را می‌یابیم که $a = q_۱b + r_۱$، که در آن $r_۱ = ۰$ یا $v(r_۱) < v(b)$. اگر $r_۱ = ۰$، آنگاه $b|a$ و $\gcd\{a, b\} = b$. اگر $r_۱ = ۰$، آنگاه $\gcd\{a, b\} = \gcd\{a, r_۱\}$. پس باید $\gcd\{a, r_۱\}$ را بیابیم.
مرحله دوم: اعضای $r_۲, q_۲ \in R$ را می‌یابیم که $b = q_۱r_۱ + r_۲$، که در آن $r_۲ = ۰$ یا $v(r_۲) < v(r_۱)$. اگر $r_۲ = ۰$، آنگاه $\gcd\{a, b\} = \gcd\{b, r_۱\} = r_۱$. اگر $r_۲ \neq ۰$، این روند را ادامه می‌دهیم. چون $v(b) > v(r_۱) > \cdots$ زنجیر نزولی از اعداد صحیح نامنفی است. این روند باید پس از تعداد متناهی مرحله توقف یابد. پس عدد صحیح m، یافت می‌شود که در nامین مرحله اعضای $q_n \in R$، r_n وجود دارند که $r_{n-۲} = q_n r_{n-۱} + r_n$، که در آن $r_n = ۰$. بنابراین

$$\begin{aligned}
\gcd\{a, b\} &= \gcd\{b, r_۱\} \quad (a = q_۱b + r_۱,\ \ v(r_۱) < v(b)) \\
&= \gcd\{r_۱, r_۲\} \quad (b = q_۲r_۱ + r_۲,\ \ v(r_۲) < v(r_۱)) \\
&= \gcd\{r_۲, r_۳\} \quad (r_۳ = q_۳r_۲ + r_۳,\ \ v(r_۳) < v(r_۲)) \\
&\ \ \vdots \quad \vdots \\
&= \gcd\{r_{n-۱}, r_n\} \quad (r_{n-۲} = q_n r_{n-۱} + r_n,\ \ r_n = ۰).
\end{aligned}$$

اکنون اعضای $r, s \in R$ را طوری که $\gcd\{a, b\} = ar + bs$ می‌یابیم:

$$\begin{aligned}
r_{n-۱} &= r_{n-۳} - q_{n-۲}r_{n-۲} \\
&= r_{n-۳} - q_{n-۱}(r_{n-۴} - q_{n-۲}r_{n-۳}) \\
&= r_{n-۳}(۱ + (-q_{n-۱})(-q_{n-۲})) + r_{n-۴}(-q_{n-۱}) \\
&\ \ \vdots \quad \vdots \\
&= ar + bs.
\end{aligned}$$

توجه کنید در اثبات قضیه‌ی ۵.۵.۱۲، و هم‌چنین در استفاده از الگوریتم اقلیدسی از خاصیت دوم دامنه‌ی اقلیدسی استفاده کرده‌ایم. این شرط اطلاعات بیشتری درباره‌ی دامنه‌ی اقلیدسی بر حسب تابع v به دست می‌دهد. در مثال بعدی یکه‌های دامنه‌ی اقلیدسی را بر حسب تابع v توصیف می‌کنیم.

مثال ۶.۵.۱۲. فرض کنید R دامنه‌ی اقلیدسی و $a \in R$ عضو ناصفری باشد. نشان دهید $v(۱) \leq v(a)$. به علاوه a یکه است اگر و تنها اگر $v(۱) = v(a)$.

حل بنا به خاصیت دوم دامنه‌ی اقلیدسی $v(۱) \leq v(۱a) = v(a)$. حال اگر a یکه باشد مجدداً بنا به خاصیت دوم $v(a) \leq v(aa^{-۱}) = v(۱)$ و $v(a) = v(۱)$. برعکس اگر $v(a) = v(۱)$. بنا به خاصیت اول، اعضای $q, r \in R$ وجود دارند که $۱ = qa + r$. که در آن $r = ۰$ یا $v(r) < v(a)$. اگر $r \neq ۰$ چون $v(a) = v(۱)$، رابطه‌ی $v(r) < v(a)$، بنا به قسمت اول اثبات، ممکن نیست. پس $r = ۰$. بنابراین $qa = ۱$ و a یکه است. □

۶.۱۲ برخی حلقه‌های اعداد صحیح مرتبه‌ی دوم

در این بخش نشان می‌دهیم حلقه‌ی اعداد صحیح گاوسی دامنه‌ی اقلیدسی است. روشی که به کار می‌بریم را می‌توان برای دامنه‌های صحیح دیگر که شبیه $\mathbb{Z}[i]$ هستند استفاده کرد. به عنوان مثال، قبلاً نشان دادیم که عضو $p = ۱ + i\sqrt{۵}$ در $\mathbb{Z} = [i\sqrt{۵}]$ تحویل‌ناپذیر است اما اول نیست. بنابراین $\mathbb{Z}[i\sqrt{۵}]$،یک UFD نیست. مطالعه‌ی چنین زیرحلقه‌هایی از $\mathbb{C}$ که منشاء ریاضیات مورد بحث این فصل بود، اکنون موضوعی مستقل است: نظریه‌ی جبری اعداد.
توجه کنید اعداد i، $i\sqrt{۵}$ ریشه‌های چندجمله درجه‌ی دوم $x^۲ + ۱$ و $x^۲ + ۵$ هستند. پس می‌توانیم زیرحلقه‌های $\mathbb{C}$ را که از الحاق ریشه‌های بعضی از چندجمله‌ای درجه‌ی دوم $x^۲ + m$، $(m \in \mathbb{Z})$ به $\mathbb{Z}$ به دست آمده‌اند را بررسی کنیم. فرض کنید w عدد مختلط باشد که $w \notin \mathbb{Q}$ و $w^۲ \in \mathbb{Z}$. حلقه‌ای که برای مطالعه انتخاب می‌کنیم عبارت است از

$$\mathbb{Z}[w] = \{m + nw \mid m, n \in \mathbb{Z}\}.$$

به وضوح $\mathbb{Z}[w]$ زیرحلقه‌ای از $\mathbb{C}$ و بنابراین دامنه‌ی صحیح است. به علاوه نمایش هر عضو $\mathbb{Z}[w]$ به مفهوم زیر یکتا است:

$$m + nw = m_۱ + n_۱w \Longleftrightarrow m = m_۱, n = n_۱.$$

در واقع اگر $m + nw = m_۱ + n_۱w$، آنگاه $m - m_۱ = (n_۱ - n)w$. اگر $n \neq n_۱$ آنگاه $w = \frac{m - m_۱}{n_۱ - n} \in \mathbb{Q}$ که خلاف فرض $w \notin \mathbb{Q}$ است. پس $n = n_۱$. بنابراین $m = m_۱$. اغلب مطالبی که در مورد $\mathbb{Z}[w]$ می‌خواهیم بررسی کنیم به دو مفهوم اساسی زیر بستگی دارند. اگر $a = m + nw \in \mathbb{Z}[w]$، مزدوج a را با a^* و نُرم a را با $N(a)$ نشان می‌دهیم و به صورت زیر تعریف می‌کنیم:

$$a^* = m - nw, \quad N(a) = aa^* = m^۲ - w^۲n^۲.$$

پس $a^* \in \mathbb{Z}[w]$. چون $w^۲ \in \mathbb{Z}$، داریم $N(a) \in \mathbb{Z}$.

مثال ۱.۶.۱۲. اگر در $a = m + ni \in \mathbb{Z}[i]$، آنگاه $a^* = m - ni$ همان مزدوج مختلط متعارف عدد a و $N(a) = m^۲ + n^۲ = |a|^۲$ مربع قدرمطلق متعارف a است. □

مثال ۲.۶.۱۲. اگر در $\mathbb{Z}[i\sqrt{۵}]$، $a = m + ni\sqrt{۵}$، آنگاه $a^* = m - ni\sqrt{۵}$ و $N(a) = m^۲ + ۵n^۲$. □

تعدادی از خواص مزدوج و نُرم را در قضیه‌ی زیر جمع‌آوری می‌کنیم:

قضیه ۳.۶.۱۲. اگر $w \in \mathbb{C}$ طوری باشد که $w^۲ \in \mathbb{Z}$ و $w \notin \mathbb{Q}$، آنگاه به ازای هر $a, b \in \mathbb{Z}[w]$ داریم
(الف) $aa^* = N(a) = N(a^*)$.
(ب) $(ab)^* = a^*b^*$ و $a^{**} = a$.
(ج) $N(ab) = N(a)N(b)$.
(د) a در $\mathbb{Z}[w]$ یکه است اگر و تنها اگر $N(a) = \pm ۱$، در این حالت $a^{-۱} = N(a)a^*$.
(هـ) $N(a) = ۰$ اگر و تنها اگر $a = ۰$.
(و) اگر $N(a)$ در $\mathbb{Z}$ اول باشد، آنگاه a در $\mathbb{Z}[w]$ تحویل‌ناپذیر است.

اثبات. (الف) و (ب) محاسبه های سرراست هستند.
(ج) بنا به (الف) و (ب) داریم

$$N(ab) = (ab)(ab)^* = aba^*b^* = aa^*bb^* = N(a)N(b)$$

(د) اگر a یکه باشد، آنگاه بنا به (ج)، $N(a)N(a^{-۱}) = N(aa^{-۱}) = N(۱) = ۱$. چون به ازای هر $c \in \mathbb{Z}$، $N(c) \in \mathbb{Z}$، داریم $N(a) = \pm ۱$. برعکس فرض کنید $N(a) = \pm ۱$. در نتیجه بنا به (الف) داریم $a[N(a)a^*] = N(a)aa^* = N(a)^۲ = ۱$ و بنابراین $a^{-۱} = N(a)a^*$.

(هـ) فرض کنید $a=m+nw$، در این صورت $N(a)=۰$، یعنی $m^۲-w^۲n^۲=۰$ و بنابراین $wn=\pm m$. اگر $n\neq ۰$، آنگاه $w=\pm\frac{m}{n}\in\mathbb{Q}$ که خلاف فرض است. از این‌رو $n=۰$ و $m=۰$. در نتیجه $a=۰$. عکس مطلب واضح است.
(و) فرض کنید $a=bc$، که در آن $b,c\in\mathbb{Z}[w]$، آنگاه، با اثر دادن تابع N بر این تساوی، در $\mathbb{Z}$ داریم $N(a)=N(bc)=N(b)N(c)$. چون $N(a)$ اول است، $N(b)=\pm ۱$ یا $N(c)=\pm ۱$. در نتیجه، بنا به (د)، b یا c در $\mathbb{Z}[w]$ یکه است. □

عکس (و) در قضیه‌ی ۳.۶.۱۲، درست نیست زیرا در $\mathbb{Z}[i\sqrt{۵}]$، $a=۱+i\sqrt{۵}$ تحویل‌ناپذیر است، اما $N(a)=۶=b$ اول نیست.
اکنون فرض کنید $a=m+ni\sqrt{۲}$ در $\mathbb{Z}[i\sqrt{۲}]$ یکه باشد، در این صورت طبق قضیه‌ی ۳.۶.۱۲، $m^۲+۲n^۲=N(a)=\pm ۱$. از این به سادگی نتیجه می‌شود ۱ و -۱ تنها یکه‌های $\mathbb{Z}[i\sqrt{۲}]$ هستند. از طرف دیگر $a=m+n\sqrt{۲}$ در $\mathbb{Z}[\sqrt{۲}]$ یکه است اگر و تنها اگر $N(a)=m^۲-۲n^۲=\pm ۱$. به ویژه $u=۱+\sqrt{۲}$ در $\mathbb{Z}[\sqrt{۲}]$ یکه است و $u^{-۱}=-۱+\sqrt{۲}$. پس به ازای هر $k\in\mathbb{Z}$، $\pm u^n$ در $\mathbb{Z}[\sqrt{۲}]$ یکه است. در واقع تمام یکه‌های $\mathbb{Z}[\sqrt{۲}]$ به این صورت هستند (چرا؟). به طور کلی، اگر $d>۰$ عدد صحیحی باشد که مربع عدد صحیحی نیست، آنگاه $m+n\sqrt{d}$ در $\mathbb{Z}[\sqrt{d}]$ اول است اگر و تنها اگر

$$m^۲-dn^۲=\pm ۱.$$

این رابطه را گاهی اوقات معادله‌ی پِل می‌نامند. همواره جوابی با $m\neq\pm ۱$ برای آن وجود دارد. پس $\mathbb{Z}[\sqrt{d}]$ یکه‌ای چون $u\neq\pm ۱$ دارد. با استفاده از توان‌های u بی‌نهایت جواب برای معادله‌ی پِل به دست می‌آید؛ کاری که اولین بار فرما انجام داد.

مثال ۴.۶.۱۲. اگر $d>۰$ عدد صحیحی باشد که مربع عدد صحیح نیست، آنگاه $\mathbb{Z}[\sqrt{d}]$ بی‌نهایت یکه دارد. □

اکنون به نظریه‌ی تجزیه در $\mathbb{Z}[w]$ برمی‌گردیم.

قضیه ۵.۶.۱۲. $\mathbb{Z}[w]$ یک FD است.

اثبات. با توجه به قضیه‌ی ۶.۳.۱۲، کافی است ثابت کنیم $\mathbb{Z}[w]$ در ACCP صدق می‌کند. فرض کنید

$$(a_۱)\subset(a_۲)\subset(a_۳)\subset\cdots$$

زنجیری اکیداً صعودی از ایدآل‌های اصلی $\mathbb{Z}[w]$ باشد. در این صورت به ازای هر n، $a_{n+۱}|a_n$، پس $b_n\in\mathbb{Z}[w]$ وجود دارد که $a_n=b_na_{n+۱}$. به علاوه b_n یکه نیست، زیرا $(a_n)\neq(a_{n+۱})$ و بنا به قضیه‌ی ۳.۶.۱۲، $|N(b_n)|>۱$. اما داریم $N(a_n)=N(b_n)N(a_{n+۱})$، که نتیجه می‌دهد $|N(a_n)|>|N(a_{n-۱})|$. پس

$$|N(a_۱)|>|N(a_۲)|>\cdots$$

یک زنجیر اکیداً نزولی از اعداد صحیح نامنفی است، که تناقض است. □

لم ۶.۶.۱۲. فرض کنید $w\in\mathbb{C}$ طوری باشد که $w^۲\in\mathbb{Z}$ و $w\notin\mathbb{Q}$. اگر به ازای هر $r,s\in\mathbb{Q}$ اعداد $m,n\in\mathbb{Z}$ وجود داشته باشند که

$$|(r-m)^۲-w^۲(s-n)^۲|<۱,$$

آنگاه $\mathbb{Z}[w]$ با تابع $v(a)=|N(a)|$ یک دامنه‌ی اقلیدسی است.

اثبات. خاصیت دوم دامنه‌ی اقلیدسی به وضوح برقرار است، زیرا به ازای $a,b\in\mathbb{Z}[w]$، داریم

$$v(ab)=|N(ab)|=|N(a)||N(b)|=v(a)v(b).$$

پس $b\neq ۰$ نتیجه می‌دهد $v(a)\leq v(ab)$. برای اثبات خاصیت اول، فرض کنید $a,b\in\mathbb{Z}[w]$ و $b\neq ۰$. در $\mathbb{C}$ داریم

$$\frac{a}{b}=\frac{ab^*}{bb^*}=\frac{ab^*}{N(b)}.$$

چون $N(b)$ عدد صحیح است، $ab^* \in \mathbb{Z}[w]$ پس اعداد $r, s \in \mathbb{Q}$ وجود دارند که $\frac{a}{b} = r + sw$، یعنی $a = (r + sw)b$. اعداد صحیح m و n را که در فرض مساله صدق می‌کند انتخاب می‌کنیم و قرار می‌دهیم $q = m + nw$. تعریف می‌کنیم

$$r = -qb + a = -qb + (r + sw)b = [(r - m) + (s - n)w]b,$$

آن‌گاه

$$v(r) = v[(r - m) + (s - n)w]v(b) = |(r - m)^۲ - w^۲(s - n)^۲|v(b) < v(b),$$

و خاصیت اول نیز ثابت شد. □

قضیه ۷.۶.۱۲. حلقه‌ی اعداد صحیح گاوسی $\mathbb{Z}[i]$ دامنه‌ی اقلیدسی است.

اثبات. فرض کنید r و s دو عدد گویا باشند. قرار می‌دهیم $m = [r]$ و $n = [s]$ ($[r]$ نزدیک‌ترین عدد صحیح بزرگ‌تر از r به r است) واضح است که $|r - m| \leq \frac{۱}{۲}$ و $|s - n| \leq \frac{۱}{۲}$. بنابراین

$$(r - m)^۲ - i^۲(s - n)^۲ = (r - m)^۲ + (s - n)^۲ \leq \frac{۱}{۴} + \frac{۱}{۴} = \frac{۱}{۲}.$$

پس بنا به لم ۶.۶.۱۲، $\mathbb{Z}[i]$ دامنه‌ی اقلیدسی است. □

فرض کنید $a, b \in \mathbb{Z}[i]$، $b \neq ۰$. با استفاده از روش لم ۶.۶.۱۲، می‌توانیم $q, r \in \mathbb{Z}[i]$ را طوری بیابیم که $a = qb + r$، که در آن $r = ۰$ یا $v(r) < v(b)$.

مثال ۸.۶.۱۲. اگر در $\mathbb{Z}[i]$، $a = ۷ + ۸i$ و $b = ۲ - i$. اعضای $q, r \in \mathbb{Z}[i]$ را طوری بیابید که $a = qb + r$ و $r = ۰$ یا $v(r) < v(b)$.

حل از روش اثبات لم ۶.۶.۱۲، استفاده می‌کنیم. در $\mathbb{C}$ محاسبه می‌کنیم

$$\frac{a}{b} = \frac{a\bar{b}}{b\bar{b}} = \frac{(۷ + ۸i)(۲ + i)}{۲^۲ + ۱^۲} = \frac{۶ + ۲۳i}{۵}.$$

نزدیک‌ترین اعداد صحیح به $\frac{۵}{۶}$ و $\frac{۲۳}{۵}$ به ترتیب ۱ و ۵ هستند. پس می‌نویسیم $\frac{۱}{۵} = ۱ + \frac{۱}{۵}$ و $\frac{۶}{۵} = ۵ - \frac{۲}{۵}$ و به دست می‌آوریم

$$\frac{a}{b} = (۱ + ۵i) + \left(\frac{۱}{۵} - \frac{۲}{۵}i\right).$$

پس

$$a = (۱ + ۵i)b + \left(\frac{۱}{۵} - \frac{۲}{۵}i\right) b = (۱ + ۵i)b + (۰ - i).$$

بنابراین $q = ۱ + ۵i$ و $r = -i$. توجه کنید $v(r) = ۱ < ۵ = v(b)$.

تمرین‌ها

۱. فرض کنید w همانند قضیه‌ی ۳.۶.۱۲، باشد و $w^۲ < ۰$. نشان دهید $\mathbb{Z}[w]$ تعداد متناهی عضو یکه دارد.

۲. (الف) نشان دهید $\mathbb{Z}[i\sqrt{۲}]$ همراه با تابع $v(a) = |N(a)|$ دامنه‌ی اقلیدسی است.
(ب) اگر $a = ۴ + ۳i\sqrt{۲}$ و $b = ۳ - i\sqrt{۲}$، بنویسید $a = qb + r$، که در آن $r = ۰$ یا $v(r) < v(b)$.

۳. (الف) نشان دهید $\mathbb{Z}[\sqrt{۳}]$ همراه با تابع $N(a) = |N(a)|$ دامنه اقلیدسی است.
(ب) اگر $a = ۴ + ۵\sqrt{۳}$ و $b = ۱ + \sqrt{۳}$ بنویسید $a = qb + r$، که در آن $r = ۰$ یا $v(r) < v(b)$.

۴. در $\mathbb{Z}[i]$، بزرگ‌ترین مقسوم‌علیه مشترک $۵i - ۹$ و $۱۳i + ۹-$ را بیابید.

۵. نشان دهید $\mathbb{Z}[i\sqrt{۳}]$ همراه با تابع $v(a) = |N(a)|$ دامنه‌ی اقلیدسی نیست.

۶. فرض کنید R دامنه‌ی اقلیدسی و $a, b \in R$ همدم باشند. نشان دهید $v(a) = v(b)$.

۷. اگر در یک دامنه‌ی اقلیدسی R، $a|b$ و $v(a) = v(b)$، نشان دهید a و b همدم‌اند.

۸. فرض کنید $p \in \mathbb{Z}$ عدد اول باشد، نشان دهید $\mathbb{Z}_{(p)}$ همراه با تابع $v(a) = k$، $a \neq ۰$، که در آن $(a) = (p^k)$ دامنه‌ی اقلیدسی است. در واقع نشان دهید به ازای هر $a \neq ۰$ و $b \neq ۰$ در $\mathbb{Z}_{(p)}$، $v(ab) = v(a) + v(b)$ و اگر $a + b \neq ۰$، آنگاه $v(a + b) \geq \min\{v(a), v(b)\}$.

۹. فرض کنید R دامنه‌ی اقلیدسی باشد و $b \neq ۰$. نشان دهید b نایکه است اگر و تنها اگر $a \in R$ $۰ \neq$ وجود داشته باشد که $v(ab) > v(a)$.

۱۰. فرض کنید R دامنه‌ی اقلیدسی باشد طوری که به ازای هر $b, a \in R$ که a، b و $a + b$ ناصفر باشند داشته باشیم $v(a + b) \leq \max\{v(a), v(b)\}$. نشان دهید a و $b \neq ۰$ اعضای r و q در الگوریتم تقسیم را به طور یکتا مشخص می‌کنند.

۱۱. فرض کنید R دامنه‌ی اقلیدسی و M مجموعه‌ی همه‌ی نایکه‌های R باشد
(الف) نشان دهید $M = \{۰\} \cup \{a \in R \mid a \neq ۰,\ \ v(a) > v(۱)\}$.
(ب) اگر برای اعضای ناصفر a، b و $a + b$ داشته باشیم

$$v(a + b) \geq \min\{v(a), v(b)\},$$

نشان دهید M ایدآل ماکسیمال یکتای R است.

۱۲. فرض کنید دامنه‌ی اقلیدسی R، ایدآل ماکسیمال یکتا مثل M داشته باشد. بنا به قضیه‌ی ۵.۵.۱۲، $M = (a)$.
(الف) نشان دهید M شامل همه‌ی نایکه‌ها است.
(ب) اگر $I \neq \{۰\}$ ایدآل R باشد، آنگاه $k \geq ۰$ وجود دارد که $I = (a^k)$.

فصل ۱۳

مدول‌ها و فضاهای برداری

در این فصل مفهوم مدول را به طور مختصر بررسی و مطالعه اساسی مورد نیاز فصل بعد را فراهم می‌کنیم.

۱.۱۳ مدول‌ها

مدول تعمیم مفهوم گروه آبلی است. اگر A یک گروه آبلی (جمعی) باشد، می‌دانیم به ازای هر $a, b \in A$ و هر $m, n \in \mathbb{Z}$، $(mn)a = m(na)$، $(m+n)a = ma + na$ و $m(a+b) = ma + mb$. حالت کلی‌تر این است که به جای $\mathbb{Z}$ یک حلقه‌ی دلخواه در نظر بگیریم:

تعریف ۱.۱.۱۳. فرض کنید R یک حلقه باشد. گروه آبلی $(A, +)$ را یک R- مدول چپ یا یک مدول چپ روی R گوییم هرگاه تابع $\cdot : R \times A \longrightarrow A$ وجود داشته باشد که به ازای هر $a, b \in A$، هر $r, s \in R$ داشته باشیم

(الف) $r \cdot (a + b) = r \cdot a + r \cdot b$

(ب) $r \cdot (s \cdot a) = (rs) \cdot a$

(ج) $(r + s) \cdot a = r \cdot a + s \cdot a$

اگر R یکدار باشد و به ازای هر $a \in A$، داشته باشیم $1 \cdot a = a$، آنگاه A را R- مدول چپ یکانی گوییم.

R- مدول‌های است نیز به طریق مشابه تعریف می‌شوند. اگر A یک R- مدول چپ باشد، اعضای R را اسکالر گوییم. ضرب $r \cdot a$ را ضرب اسکالری می‌نامیم و به جای $r \cdot a$ معمولاً می‌نویسیم ra، توجه کنید در تعریف فوق نمادهای یکسانی برای عمل جمع در گروه آبلی A و حلقه‌ی R به‌کار بردیم؛ هم‌چنین نمادهای یکسانی برای عمل ضرب در R و ضرب اسکالری استفاده شد.

مثال ۲.۱.۱۳. فرض کنید A یک گروه آبلی و R حلقه‌ای دلخواه باشد. به ازای هر $a \in A$ و هر $r \in R$، تعریف می‌کنیم $ra = 0$. در این صورت A یک R- مدول چپ است، که آن را مدول بدیهی گوییم. □

همه‌ی مطالبی که در مورد R- مدول‌های چپ بیان و ثابت می‌کنیم با تغییرات جزئی برای R- مدول‌های راست نیز درست هستند. پس مطالعه و قضیه‌ها را فقط برای R- مدول‌های چپ بیان ثابت می‌کنیم. از این پس منظور ما از R- مدول، R- مدول چپ است.
هرگاه R یک حلقه‌ی تقسیم باشد و A یک R- مدول یکانی، آنگاه A را یک فضای برداری روی R گوییم.

مثال ۳.۱.۱۳. فرض کنید I یک ایدآل چپ از حلقه‌ی R باشد، در این صورت I به همراه عمل جمع و ضرب در R،یک R- مدول چپ است. به ویژه R یک R- مدول چپ است. به همین نحو هر ایدآل راست R یک R- مدول راست است. □

مثال ۴.۱.۱۳. اگر A یک گروه آبلی باشد، می‌دانیم به ازای هر $a \in A$ و هر $m \in \mathbb{Z}$، $ma \in A$. تحت این عمل ضرب اسکالری A، یک $\mathbb{Z}$- مدول چپ یکانی است. □

مثال ۵.۱.۱۳. اگر I یک ایدآل چپ حلقه‌ی R باشد، گروه آبلی R/I تحت عمل جمع متعارف هم‌مجموعه‌ها و ضرب اسکالری $r(a + I) = ra + I$ یک R- مدول چپ است. توجه کنید R/I لزوماً حلقه نیست. □

۲.۱۳ زیرمدول

زیرمجموعه‌ی ناتهی B از R- مدول A را زیرمدول A گوییم هرگاه B زیرگروه جمعی A بوده و به ازای هر $b \in B$ و هر $r \in R$، $rb \in B$. زیرمدول یک فضای برداری روی یک حلقه‌ی تقسیم را زیرفضا گوییم. هر R- مدول دلخواه A دو زیرمدول بدیهی دارد A و $\{۰\}$. به علاوه هر زیرمدول یک R- مدول یکانی لزوماً یکانی است. اگر A یک R- مدول باشد، آنگاه به سادگی می‌توان دید به ازای هر $a \in A$ و $r \in R$، داریم $r۰ = ۰$، $۰a = ۰$، $r(-a) = -(ra) = (-r)a$ (تمرین ۱ را ببینید).

مثال ۱.۲.۱۳. فرض کنید I ایدآل چپ حلقه‌ی R باشد و $a \in A$، که در آن A یک R- مدول است. در این صورت $\{ra \mid r \in I\} =$ یک زیرمدول A است. □

متناظر هر ایدآل چپ I از حلقه‌ی R و هر زیرمجموعه‌ی ناتهی X از یک R- مدول می‌توان یک زیرمدول تعریف کرد:

قضیه ۲.۲.۱۳. اگر I ایدآل چپ حلقه‌ی R و X زیرمجموعه‌ی ناتهی از R- مدول A باشد، آنگاه

$$IX = \left\{ \sum_{i=۱}^{n} r_i x_i \,\middle|\, n \in \mathbb{N},\ \ r_i \in I,\ \ x_i \in X \right\}$$

یک زیرمدول A است. به ویژه RX یک زیرمدول A است. □

اثبات قضیه ساده است و به عنوان تمرین واگذار می‌شود. فرض کنید X زیرمجموعه‌ی ناتهی از R- مدول یکانی A باشد. در این صورت به ازای هر $x \in X$ داریم $x = ۱x \in RX$. بنابراین $X \subseteq RX$ و در حالتی که R یکدار باشد و A یک R- مدول یکانی، آنگاه RX یک زیر مدول A شامل X است. اما اگر A یکانی نباشد لزومی ندارد که RX شامل X باشد. می‌خواهیم زیرمدولی بیابیم که شامل X است. اگر M یک زیرمدول A باشد که شامل X است، آنگاه برای هر $x_۱, \ldots, x_k \in X$، داریم $x_۱, \ldots, x_k \in M$. پس به ازای هر $n_۱, \ldots, n_k \in \mathbb{Z}$ داریم $\sum_{i=۱}^{k} n_i x_i \in M$. با این ایده تعریف می‌کنیم

$$\mathbb{Z}X = \left\{ \sum_{i=۱}^{k} n_i x_i \,\middle|\, k \in \mathbb{N},\ \ n_i \in \mathbb{Z},\ \ x_i \in X \right\}.$$

اکنون برای هر زیرمجموعه‌ی ناتهی X از یک مدول، زیرمدولی که شامل X است را به دست می‌آوریم. اثبات قضیه‌ی بعد ساده است و به عنوان تمرین واگذار می‌شود.

قضیه ۳.۲.۱۳. اگر X زیرمجموعه‌ی ناتهی از R- مدول A باشد، آنگاه $RX + \mathbb{Z}X$ یک زیرمدول A شامل X است. □

فرض کنید X زیرمجموعه‌ی ناتهی R- مدول A باشد. اگر M یک زیرمدول A شامل X باشد، آنگاه به ازای هر $x_۱, \ldots, x_k \in X$ و به ازای هر $r_۱, \ldots, r_k \in R$ داریم $\sum_{i=۱}^{k} r_i x_i \in M$. بنابراین هر عضو RX در M قرار دارد و $RX \subseteq M$. هم‌چنین به ازای هر $n_۱, \ldots, n_k \in \mathbb{Z}$، داریم $\sum_{i=۱}^{k} n_i x_i \in M$. پس هر عضو $\mathbb{Z}X$ نیز در M قرار دارد و $\mathbb{Z}X \subseteq M$. در نتیجه $RX + \mathbb{Z}X \subseteq M$. بنابراین $RX + \mathbb{Z}X$ کوچک‌ترین زیرمدول A شامل X است.

تعریف ۴.۲.۱۳. فرض کنید X زیرمجموعه‌ی از R- مدول A باشد. زیرمدول تولید شده، توسط X را که با $\langle X \rangle$ یا $\mathrm{Span}(X)$ نشان می‌دهیم عبارت است از کوچک‌ترین زیرمدول A شامل X، یعنی

$$\langle X \rangle = \bigcap \{M \mid X \subseteq M,\ \ A \text{ زیرمدول } M\}.$$

X را مجموعه‌ی مولد $\langle X \rangle$ می‌نامیم. واضح است که اگر $X = \emptyset$، آنگاه $\langle X \rangle = \{۰\}$. اگر $X \neq \emptyset$ قضیه‌ی ۳.۲.۱۳، و بحث بالا نشان می‌دهند که $\langle X \rangle = RX + \mathbb{Z}X$. در حالتی که R یکدار و R- مدول A یکانی باشد داریم $\langle X \rangle = RX$. اگر $X = \{x_۱, \ldots, x_k\}$، زیرمدول تولید شده توسط X را با $\langle x_۱, \ldots, x_k \rangle$ نشان می‌دهیم و آن‌را زیرمدول متناهیاً تولید شده می‌نامیم. به ویژه اگر $X = \{x\}$، آنگاه $\langle x \rangle = Rx + \mathbb{Z}x$ و اگر A یکانی باشد، آنگاه $\langle x \rangle = Rx$. Rx را R-مدول دوری می‌نامیم.

فرض کنید M یک زیرمدول R- مدول A باشد. چون M به عنوان زیرگروه جمعی در A نرمال است، می‌توان گروه جمعی $A/M = \{a + M \mid a \in A\}$ را تشکیل داد، که در آن جمع هم‌مجموعه‌ها به صورت متعارف انجام می‌شود: به ازای هر $a, b \in A$،

$$(a + M) + (b + M) = (a + b) + M.$$

اگر $r \in R$ و $a + M \in A/M$ تعریف می‌کنیم:

$$r(a + M) = ra + M.$$

این ضرب اسکالر خوش تعریف است. زیرا اگر $a + M = b + M$، آنگاه $a - b \in M$. چون M زیرمدول است $r(a - b) \in M$، یعنی $ra + M = rb + M$. بنابراین A/M یک R- مدول است.

۳.۱۳ قضایای یکریختی

تعریف ۱.۳.۱۳. فرض کنید A و M دو R- مدول باشند. تابع $f : A \longrightarrow M$ را همریختی R- مدولی گوییم هرگاه به ازای هر $a, b \in A$ و هر $r \in R$ داشته باشیم

$$f(a + b) = f(a) + f(b), \quad f(ra) = rf(a).$$

به علاوه اگر f یک‌به‌یک و پوشا باشد f را یکریختی R- مدولی می‌نامیم و می‌گوییم A و M یکریخت‌اند و می‌نویسیم $A \cong M$.

هرگاه $f : A \longrightarrow M$ همریختی R- مدولی باشد، آنگاه f یک همریختی بین گروه‌های جمعی A و M است. پس به ازای هر $n \in \mathbb{Z}$ و هر $a \in A$ داریم $f(na) = nf(a)$. به ویژه $f(0) = 0$ و $f(-a) = -f(a)$. هم‌چنین هسته‌ی f، یعنی

$$\ker f = \{a \in A \mid f(a) = 0\},$$

یک زیرگروه جمعی A است. از طرف دیگر به ازای هر $a \in \ker f$ و هر $r \in R$ داریم $f(ra) = rf(a) = r0 = 0$. بنابراین $\ker f$ زیرمدول A است. یادآوری می‌کنیم $\ker f = \{0\}$ اگر و تنها اگر f یک‌به‌یک باشد.
فرض کنید M یک زیرمدول R- مدول A باشد. تابع $\pi : A \longrightarrow A/M$ با ضابطه‌ی $\pi(a) = a + M$ یک همریختی پوشای R- مدولی است، که همریختی طبیعی نامیده می‌شود. به وضوح $\ker \pi = M$. بنابراین M زیرمدول A است اگر و تنها اگر هسته‌ی یک همریختی از A به R- مدول دیگر باشد. قضیه‌ی زیر را به سادگی و با استفاده از قضیه‌ی مشابه در گروه‌ها می‌توان ثابت کرد.

قضیه ۲.۳.۱۳. (قضیه‌ی اول یکریختی) اگر $f : M \longrightarrow N$ همریختی R- مدولی باشد، آنگاه $M/\ker f \cong \operatorname{Im} f$.

اثبات. طبق قضیه‌ی اول یکریختی برای گروه‌ها می‌دانیم تابع $\bar{f} : M/\ker f \longrightarrow \operatorname{Im} f$ با ضابطه‌ی $\bar{f}(a + \ker f) = f(a)$ یک همریختی یک‌به‌یک و پوشای گروهی است. پس کافی است ثابت کنیم $\bar{f}$، عمل ضرب اسکالر را حفظ می‌کند. برای هر $r \in R$ و $a \in M$ داریم

$$\begin{aligned} \bar{f}(r(a + \ker f)) &= \bar{f}(ra + \ker f) \\ &= f(ra) \\ &= rf(a) \\ &= r\bar{f}(a + \ker f). \end{aligned}$$

بنابراین $\bar{f}$ همریختی R- مدولی نیز هست. □

قضیه ۳.۳.۱۳. (قضیه‌ی دوم یکریختی) اگر S و T زیرمدول‌های R- مدول M باشند، آنگاه $\dfrac{S}{S \cap T} \cong \dfrac{S + T}{T}$. □

قضیه ۴.۳.۱۳. (قضیه‌ی سوم یکریختی) اگر S و T زیرمدول‌های R- مدول M باشند و $S \subseteq T$، آنگاه داریم $\frac{M/S}{T/S} \cong M/T$.

قضیه ۵.۳.۱۳. اگر M یک زیر مدول R- مدول A باشد، آنگاه زیرمدول‌های R/M دقیقاً به صورت N/M هستند که در آن N یک زیرمدول A است و $M \subseteq N$. □

این بخش را با بررسی حاصل‌ضرب مدول‌ها ادامه می‌دهیم. برای استقلال این بحث از فصل ۴ همه‌ی مفاهیم مورد نیاز را می‌آوریم. فرض کنید I یک مجموعه‌ی اندیس و $\{A_i\}_{i\in I}$ خانواده‌ای از R- مدول‌ها باشد. یادآوری می‌کنیم حاصل‌ضرب دکارتی $\prod_{i\in I} A_i$ عبارت است از مجموعه‌ی همه‌ی دنباله‌های $(a_i)_{i\in I}$ که در آن $a_i \in A_i$ به ازای هر i:

$$\prod_{i\in I} A_i = \{(a_i)_{i\in I} \mid a_i \in A_i, \quad \forall i \in I\}.$$

$\prod_{i\in I} A_i$ تحت عمل جمع مولفه‌ای و ضرب اسکالر مولفه‌ای

$$(a_i)_{i\in I} + (b_i)_{i\in I} = (a_i + b_i)_{i\in I}$$
$$r(a_i)_{i\in I} = (ra_i)_{i\in I}$$

یک R- مدول است، عضو بی‌اثر جمع عبارت است از دنباله $(c_i)_{i\in I}$ است که به ازای هر $i \in I$، $c_i = 0$. قرینه‌ی دنباله $(a_i)_{i\in I}$ عبارت است از $(-a_i)_{i\in I}$. این مدول را با $\mathrm{Cr}_{i\in I} A_i$ نیز نشان می‌دهیم.
فرض کنید $u = (a_i)_{i\in I}$ دنباله دلخواهی در $\prod_{i\in I} A_i$ باشد. تکیه‌گاه u را که با $\mathrm{supp}(u)$ نشان می‌دهیم عبارت است از

$$\mathrm{supp}(u) = \{j \in I \mid a_j \neq 0\}.$$

اثبات قضیه‌ی زیر ساده است و به عنوان تمرین واگذار می‌شود.

قضیه ۶.۳.۱۳. اگر $u = (a_i)_{i\in I}$ و $v = (b_i)_{i\in I}$ دنباله‌های دل‌خواهی در $\prod_{i\in I} A_i$ باشند و $0 \neq r \in R$، آنگاه
(الف) $\mathrm{supp}(u) = \mathrm{supp}(-u)$.
(ب) $\mathrm{supp}(u+v) \subseteq \mathrm{supp}(u) \cup \mathrm{supp}(v)$.
(ج) $\mathrm{supp}(ru) \subseteq \mathrm{supp}(u)$. □

مجموعه‌ی دنباله‌های در $\prod_{i\in I} A_i$ با تکیه‌گاه متناهی را با $\mathrm{Dr}_{i\in I} A_i$ یا $\oplus_{i\in I} A_i$ نشان می‌دهیم:

$$\oplus_{i\in I} A_i = \{(a_i)_{i\in I} \in \prod_{i\in I} A_i \mid |\mathrm{supp}((a_i)_{i\in I})| < \infty\}.$$

قضیه‌ی فوق نشان می‌دهد که $\oplus_{i\in I} A_i$ زیرمدول $\prod_{i\in I} A_i$ است. $\oplus_{i\in I} A_i$ را حاصل جمع مستقیم (خارجی) خانواده‌ی $\{A_i\}_{i\in I}$ گوییم. در حالتی که $I = \{1, 2, \ldots, n\}$ متناهی باشد $\prod_{i=1}^{n} A_i$ و $\oplus_{i=1}^{n} A_i$ با هم مساوی هستند و آن را با $A_1 \oplus \cdots \oplus A_n$ نشان می‌دهیم.
به ازای هر $j \in I$ تابع $\pi_j : \oplus_{i\in I} A_i \longrightarrow A_j$ با ضابطه‌ی $\pi_j((a_i)_{i\in I}) = a_j$ یک همریختی پوشا است که آن را همریختی تصویر روی مولفه‌ی jام گوییم. توجه کنید

$$\ker \pi_j = \{(a_i)_{i\in I} \in \oplus_{i\in I} A_i \mid a_j = 0\}.$$

به ازای هر $j \in I$، تابع $\iota_j : A_j \longrightarrow \oplus_{i\in I} A_i$ با ضابطه‌ی $\iota_j(a) = (a_i)_{i\in I}$، که در آن a در jامین مولفه است، یعنی $a_i = \begin{cases} 0 & i \neq j \\ a & i = j \end{cases}$، یک همریختی یک‌به‌یک است. ι_j را جادهی مولفه‌ی jام گوییم. چون ι_j یک‌به‌یک است $\iota_j(A_j)$ زیرمدولی از $\oplus_{i\in I} A_i$ و یکریخت با A_j است:

$$A_j \cong \iota_j(A_j) = \{(a_i)_{i\in I} \in \oplus_{i\in I} A_i \mid a_i = 0, \quad \forall i \neq j\}.$$

در حالتی که $I = \{۱, ۲, \dots, n\}$ داریم

$$A_j \cong \iota_j(A_j) = \{۰\} \oplus \cdots \oplus \{۰\} \oplus A_j \oplus \{۰\} \oplus \cdots \oplus \{۰\}.$$

هر عضو $\oplus_{i\in I} A_i$ به صورت یکتا بر حسب اعضای $\iota_j(A_j)$، $j \in I$، نوشته می‌شود. زیرا فرض کنید $(a_i)_{i\in I} \oplus_{i\in I} A_i$. در این صورت $j_۱, \dots, j_n \in I$ وجود دارند که اگر $i \notin \{j_۱, \dots, j_n\}$، آنگاه $a_i = ۰$. فرض کنید u_{j_k} دنباله‌ای باشد، که مولفه‌ی j_kام آن برابر a_{j_k} و همه‌ی مولفه‌های دیگر آن ۰ است، یعنی $u_{j_k} = (b_i)_{i\in I}$ و $b_i = \begin{cases} ۰ & i \neq j_k \\ a_{j_k} & i = j_k \end{cases}$. بنابراین داریم

$$(a_i)_{i\in I} = u_{j_۱} + u_{j_۲} + \cdots + u_{j_n}$$

و به وضوح این نحوه‌ی نوشتن $(a_i)_{i\in I}$ بر حسب اعضای $\iota_j(A_j)$، $i \in I$ یکتاست.
حال فرض کنید A یک R- مدول دلخواه و $\{M_i\}_{i\in I}$ خانواده‌ای از زیرمدول‌های A باشد، طوری که هر عضو $a \neq ۰$ به صورت یکتای $a = a_{j_۱} + a_{j_۲} + \cdots + a_{j_n}$ نوشته شود، که در آن $a_{j_k} \in M_{j_k}$، $a_{j_k} \neq ۰$، $k = ۱, \dots, n$. در این حالت گوییم A حاصل‌جمع مستقیم (داخلی) خانواده $\{M_i\}_{i\in I}$ است. در این حالت تابع $\varphi : \oplus_{i\in I} M_i \longrightarrow A$ با ضابطه‌ی $\varphi((a_i)_{i\in I}) = a_{j_۱} + \ldots + a_{j_n}$، که در آن برای هر $i \notin \{j_۱, \dots, j_n\}$، $a_i = ۰$، یک یکریختی است. پس $A \cong \oplus_{i\in I} M_i$. هرگاه A حاصل‌جمع مستقیم داخلی $\{M_i\}_{i\in I}$ باشد می‌نویسیم $A = \oplus_{i\in I} M_i$. توجه کنید که اگر A حاصل‌جمع مستقیم داخلی $\{M_i\}_{i\in I}$ باشد، آنگاه M_iها زیرمدول‌های A هستند. اما حاصل‌جمع خارجی $\oplus_{i\in I} M_i$ شامل هیچ‌کدام از M_iها نیست، بلکه که به ازای هر j، شامل یک کپی یکریخت با M_j، یعنی $\iota_j(M_j)$ است. به سادگی می‌توان ثابت کرد:

قضیه ۷.۳.۱۳. اگر $\{M_i\}_{i\in I}$ خانواده‌ای از زیرمدول‌های A باشند آنگاه $A = \oplus_{i\in I} M_i$ اگر و تنها اگر
(الف) $A = \langle \bigcup_{i\in I} M_i \rangle$.
(ب) به ازای هر $j \in I$، $M_j \cap \left\langle \bigcup_{\substack{i\in I \\ i\neq j}} M_i \right\rangle = \{۰\}$.

اثبات. ($\Longleftarrow$) فرض کنید $A = \oplus_{i\in I} M_i$. طبق تعریف حاصل‌جمع مستقیم داخلی، هر $a \in A$ به صورت (یکتای) $a = a_{j_۱} + \cdots + a_{j_n}$، که در آن $a_{j_k} \in M_{j_k}$، نوشته می‌شود، یعنی $A = \langle \bigcup_{i\in I} M_i \rangle$. اکنون فرض کنید $a \in M_j \cap \left\langle \bigcup_{\substack{i\in I \\ i\neq j}} M_i \right\rangle$. بنابراین می‌توان نوشت $a = a_{j_۱} + \cdots + a_{j_k}$، که در آن $a_{j_k} \in M_{j_k}$ و $j_k \neq j$. در نتیجه $-a + a_{j_۱} + \cdots + a_{j_k} = ۰$ و بنا به یکتایی تجزیه ۰ به صورت حاصل‌جمع اعضای $\{M_i\}_{i\in I}$، داریم $a = a_{j_۱} \cdots = a_{j_k} = ۰$. پس $M_j \cap \left\langle \bigcup_{\substack{i\in I \\ i\neq j}} M_i \right\rangle = \{۰\}$.
($\Longrightarrow$) چون به ازای هر $j \in I$، $M_j \cap \left\langle \bigcup_{\substack{i\in I \\ i\neq j}} M_i \right\rangle = \{۰\}$، به ویژه به ازای هر $i \neq j$ داریم $M_i \cap M_j = \{۰\}$. حال فرض کنید $a \in A$، $a \neq ۰$. بنا به (الف) اعضای $a_{j_k} \in M_{j_k}$، $a_{j_k} \neq ۰$، $k = ۱, \dots, n$ وجود دارند که $a = a_{j_۱} + \cdots + a_{j_n}$. باید ثابت کنیم این تجزیه یکتاست. فرض کنید $a = b_{i_۱} + b_{i_۲} + \cdots + b_{i_m}$، که در آن $b_{i_k} \in M_{i_k}$، $k = ۱, \dots, m$. به سادگی و به استقرا روی $\max\{m, n\}$ با استفاده از (ب) می‌توان ثابت کرد $m = n$ و پس از تعویض اندیس‌ها $b_{i_k} = a_{i_k}$. جزئیات اثبات را به خواننده واگذار می‌کنیم. □

۴.۱۳ مدول‌های آزاد متناهیاً تولید شده

فرض کنید R حلقه باشد. زیرمجموعه‌ی X از R- مدول A را مستقل خطی گوییم، هرگاه اگر $x_۱, \dots, x_n \in X$ اعضای متمایز باشند و $r_۱, \dots, r_n \in R$ داشته باشیم

$$r_۱x_۱ + r_۲x_۲ + \cdots + r_nx_n = ۰,$$

آنگاه نتیجه شود $r_i = ۰$، برای هر $۱ \leq i \leq n$. زیرمجموعه‌ی را که مستقل خطی نباشد وابسته‌ی خطی گوییم. اگر R یکدار و A یک مدول یکانی روی R باشد، آنگاه X مولد A است اگر و تنها اگر $A = RX$. بنابراین X مولد A است اگر و تنها اگر هر عضو A را بتوان به صورت $r_۱x_۱ + r_۲x_۲ + \cdots + r_nx_n$ نوشت که در آن $r_i \in R$ و $x_i \in X$.یک مجموعه‌ی مولد و مستقل خطی برای R- مدول

یکانی A را یک پایه گوییم. R- مدول یکانی A را مدول آزاد گوییم هرگاه پایه‌ای داشته باشد.
فضاهای برداری روی یک حلقه‌ی تقسیم R همواره دارای پایه‌اند و بنابراین R- مدول آزاد هستند. برای اثبات این مطلب به لم زیر نیاز داریم.

لم ۱.۴.۱۳. اگر X یک مجموعه‌ی مستقل خطی ماکسیمال در فضای برداری V روی حلقه‌ی تقسیم R باشد، آنگاه X یک پایه برای V است.

اثبات. باید ثابت کنیم X، V را تولید می‌کند، یعنی $\langle X\rangle = V$. فرض کنید چنین نباشد. پس عضو $v \in V - \langle X\rangle$ وجود دارد. ادعا می‌کنیم $X \cup \{v\}$ مجموعه‌ی مستقل خطی است، که این خلاف ماکسیمال بودن X است. اگر

$$rv + r_1x_1 + \cdots + r_nx_n = 0,$$

که در آن $r, r_i \in R$، $x_i \in X$، $1 \leq i \leq n$، و $r \neq 0$، آنگاه

$$v = -r^{-1}r_1x_1 - \cdots - r^{-1}r_nx_n \in \langle X\rangle,$$

که خلاف انتخاب v است. از این‌رو $X \cup \{v\}$ مستقل خطی است، و این متناقض با ماکسیمال بودن X است. □

قضیه ۲.۴.۱۳. اگر V یک فضای برداری روی حلقه‌ی تقسیم R باشد، آنگاه هر مجموعه‌ی مستقل خطی در V مشمول در یک پایه است.

اثبات. فرض کنید X یک زیرمجموعه‌ی مستقل خطی در V باشد. با استفاده از لم زُرن نشان می‌دهیم یک مجموعه‌ی مستقل خطی ماکسیمال شامل X وجود دارد. فرض کنید

$$\mathscr{A} = \{Y \subseteq V \mid X \subseteq Y \text{ مستقل خطی}\}.$$

چون $X \in \mathscr{A}$، $\mathscr{A} \neq \emptyset$. فرض کنید $\mathscr{B}$ یک زنجیر در $\mathscr{A}$ باشد. ادعا می‌کنیم $T = \bigcup_{Y\in\mathscr{B}} Y$ زیرمجموعه‌ی مستقل خطی در V است. اگر $r_1y_1 + \cdots + r_ny_n = 0$، که در آن $y_i \in T$ و $r_i \in R$، آنگاه اعضای $Y_i \in \mathscr{B}$ وجود دارند که $y_i \in Y_i$. چون $\mathscr{B}$ یک زنجیر است. j وجود دارد که $Y_1, \ldots, Y_n \subseteq Y_j$. بنابراین $y_1, \ldots, y_n \in Y_j$. چون Y_j مستقل خطی است باید داشته باشیم $y_i = 0$. بنابراین T یک مجموعه‌ی مستقل خطی در V شامل X است. پس هر زنجیر در $\mathscr{A}$ یک کران بالا در $\mathscr{A}$ دارد. بنا به لم زُرن $\mathscr{A}$ یک عضو ماکسیمال مثل Y دارد. چون Y یک زیرمجموعه‌ی مستقل خطی ماکسیمال است، بنا به لم ۱.۴.۱۳، یک پایه برای V است. □

نتیجه ۳.۴.۱۳. هر فضای برداری V روی حلقه‌ی تقسیم R یک پایه دارد و بنابراین R- مدول آزاد است.

اثبات. چون مجموعه‌ی $\emptyset$ مستقل خطی است، بنا به قضیه‌ی قبل یک پایه برای V وجود دارد. □

قضیه ۴.۴.۱۳. اگر V یک فضای برداری روی حلقه‌ی تقسیم R، و X یک مجموعه‌ی مولد برای V باشد، آنگاه X شامل پایه است.

اثبات. با استفاده از لم زُرن ثابت می‌کنیم که یک مجموعه‌ی مستقل خطی ماکسیمال از V مشمول در X وجود دارد. قرار می‌دهیم $\mathscr{A} = \{Y \mid Y \subseteq X$ مستقل خطی $\}$. مشابه اثبات قضیه‌ی ۲.۴.۱۳، بنا به لم زُرن $\mathscr{A}$ یک عضو ماکسیمال مثل Y دارد. پس Y یک مجموعه‌ی مستقل خطی ماکسیمال در V است و بنا به لم ۱.۴.۱۳،یک پایه برای V است. □

قضیه ۵.۴.۱۳. اگر $X = \{x_1, x_2, \ldots, x_n\}$ یک مجموعه‌ی مولد برای فضای برداری V روی حلقه‌ی تقسیم R باشد، آنگاه هر زیرمجموعه‌ی مستقل خطی V حداکثر n عضو دارد.

اثبات. فرض کنید $Y = \{y_1, y_2, \ldots, y_m\}$ یک زیرمجموعه‌ی مستقل خطی V باشد. باید ثابت کنیم $m \leq n$. به استقرا روی k ثابت می‌کنیم که پس از تعویض اندیس‌ها x_i، مجموعه‌ی $\{y_1, \ldots, y_k, x_{k+1}, \ldots, x_n\}$ یک مجموعه‌ی مولد برای V است. ابتدا حالت $k = 1$ را در نظر می‌گیریم. چون X مجموعه‌ی مولد برای V است، اعضای $r_1, \ldots, r_n \in R$ وجود دارند که $y_1 = r_1x_1 + r_2x_2 + \cdots + r_nx_n$. چون Y مستقل خطی است، $y_1 \neq 0$. بنابراین j وجود دارد که $r_j \neq 0$. با تعویض اندیس‌ها می‌توانیم فرض کنیم $j = 1$. پس $r_1 \neq 0$ و $x_1 = -r_1^{-1}r_2x_2 - \cdots - r_1^{-1}r_nx_n - r_1^{-1}y_1$.
بنابراین $x_1 \in \langle y_1, x_2, \ldots, x_n\rangle$.

از این‌رو $V = \langle y_1, x_2, \dots, x_n \rangle$. پس حالت $k = 1$ ثابت شد. اکنون فرض کنید $V = \langle y_1, \dots, y_{k-1}, x_k, \dots x_n \rangle$. بنابراین اعضای $s_1, \dots, s_n \in R$ وجود دارند که

$$y_k = s_1 y_1 + \cdots + s_{k-1} y_{k-1} + s_k x_k + \cdots + s_n x_n.$$

اگر $s_k = \cdots = s_n = 0$، آنگاه $y_k - s_1 y_1 + \cdots - s_{k-1} y_{k-1} = 0$، که خلاف مستقل خطی بودن Y است. پس $k \leq j \leq n$ وجود دارد که $s_j \neq 0$. با تعویض اندیس‌ها می‌توانیم فرض کنیم $j = k$. بنابراین $s_k \neq 0$ و داریم

$$x_k = -s_k^{-1}(s_1 y_1 + \cdots + s_{k-1} y_{k-1} + s_{k+1} x_{k+1} + \cdots + s_n x_n) + s_k^{-1} y_k,$$

یعنی $x_k \in \langle y_1, \dots, y_k, x_{k+1}, \dots, x_n \rangle$ و $V = \langle y_1, \dots, y_k, x_{k+1}, \dots, x_n \rangle$. اکنون فرض کنید بر خلاف حکم داشته باشیم $m > n$، در این صورت با انتخاب $k = n$ داریم $V = \langle y_1, y_2, \dots, y_n \rangle$. اما در این صورت $y_{n+1}, \dots, y_m \in V = \langle y_1, \dots, y_n \rangle$، که این خلاف استقلال خطی V است. □

نتیجه ۶.۴.۱۳. اگر X و Y دو پایه‌ی متناهی برای فضای برداری V روی حلقه‌ی تقسیم R باشند، آنگاه $|X| = |Y|$.

اثبات. چون X مجموعه‌ی مولد برای V و Y مستقل خطی است، طبق قضیه‌ی ۵.۴.۱۳، $|X| \leq |Y|$. به همین نحو $|Y| \leq |X|$. بنابراین $|X| = |Y|$. □

متذکر می‌شویم که اگر X و Y دو پایه (نه لزوماً متناهی) برای فضای برداری V روی حلقه‌ی تقسیم R باشند، آنگاه $|X| = |Y|$. اما در این‌جا این مطلب را ثابت نمی‌کنیم (صفحه‌ی ۳۸۱ از کتاب مرجع [۵] را ببینید).

تعریف ۷.۴.۱۳. فرض کنید V یک فضای برداری روی حلقه‌ی تقسیم R و X یک پایه برای V روی R باشد. $|X|$ را بعد V روی R گوییم و با $\dim_R V = |X|$ نشان می‌دهیم. V را فضای برداری با بعد متناهی گوییم هرگاه $|X|$ متناهی باشد.

اگر I یک مجموعه‌ی اندیس باشد و R یک حلقه‌ی یکدار و به ازای هر i، $A_i = R$، آنگاه $\oplus_{i \in I} R = \oplus_{i \in I} A_i$ یک R- مدول است. به ازای هر j، دنباله $e_j = (a_i)_{i \in I}$ را در نظر می‌گیریم که مولفه‌ی jام آن برابر ۱ و همه‌ی مولفه‌های دیگر آن برابر صفر باشد، یعنی $a_i = \begin{cases} 0 & i \neq j \\ 1 & i = j \end{cases}$. پس e_j عضوی از $\oplus_{i \in I} R$ است. فرض کنید $u = (b_i)_{i \in I}$ عضو دلخواهی از $\oplus_{i \in I} R$ باشد. بنابراین $j_1, \dots, j_n \in I$ وجود دارند که به ازای هر $i \in I$ که $i \in \{j_1, \dots, j_n\}$، $b_i = 0$. در نتیجه

$$u = (b_i)_{i \in I} = b_{j_1} e_{j_1} + \cdots + b_{j_n} e_{j_n}.$$

این یعنی $X = \{e_j \mid j \in I\}$ یک مجموعه‌ی مولد برای $\oplus_{i \in I} R$ است. علاوه بر این X مستقل خطی است زیرا اگر

$$b_{j_1} e_{j_1} + \cdots + b_{j_n} e_{j_n} = (0)_{i \in I},$$

آنگاه به ازای هر k، مولفه‌ی j_kام سمت چپ تساوی برای b_{j_k} و مولفه‌ی j_kام سمت راست تساوی برابر ۰ است. پس به ازای هر k، $b_{j_k} = 0$. بنابراین ثابت کرده‌ایم که $\oplus_{i \in I} R$ یک R- مدول آزاد با پایه‌ی $\{e_j \mid j \in I\}$ است.
حال فرض کنید X مجموعه‌ای دلخواه باشد. X را به عنوان مجموعه‌ی اندیس انتخاب می‌کنیم. پس R- مدول $\oplus_{x \in X} R$ یک R- مدول آزاد روی $Y = \{e_x \mid x \in X\}$ است. به وضوح $|X| = |Y|$. بنابراین به ازای هر مجموعه‌ی X یک R- مدول آزاد با پایه‌ای مثل Y وجود دارد که $|X| = |Y|$.

قضیه ۸.۴.۱۳. فرض کنید R حلقه‌ی یکدار و A یک R- مدول یکانی باشد. قضیه‌های زیر معادل‌اند
(الف) A یک پایه دارد.
(ب) A حاصل‌جمع مستقیم (داخلی) زیر مدول‌های یکریخت با R است.

اثبات. (الف) $\Longleftarrow$ (ب) فرض کنید X پایه‌ای برای A روی R و $a \in A$ عضو دلخواهی باشد. چون X مجموعه‌ی مولد A است، اعضای $x_1, \ldots, x_n \in X$ و $r_1, \ldots, r_n \in R$ وجود دارند که

$$a = r_1 x_1 + \cdots + r_n x_n.$$

به علاوه استقلال خطی X نتیجه می‌دهد که این طریقه‌ی نمایش a بر حسب ترکیب خطی عناصر X منحصر به فرد است. این یعنی A حاصل‌جمع مستقیم زیرمدول‌های $\{Rx\}_{x\in X}$ است: $A = \oplus_{x\in X} Rx$. اکنون ثابت می‌کنیم، به ازای هر $x \in X$، $R \cong Rx$. تابع $\varphi : R \longrightarrow Rx$ را با $\varphi(r) = rx$ تعریف می‌کنیم، φ همریختی R- مدولی است زیرا

$$\begin{aligned} \varphi(r+s) &= (r+s)x = rx + sx = \varphi(r) + \varphi(s), \\ \varphi(rs) &= (rs)x = r(sx) = r\varphi(s). \end{aligned}$$

به وضوح φ پوشاست و چون X مستقل خطی است، داریم

$$r \in \ker\varphi \Longleftrightarrow \varphi(r) = 0 \Longleftrightarrow rx = 0 \Longleftrightarrow r = 0,$$

که نتیجه می‌دهد φ یکریختی است و $R \cong Rx$.
(ب) $\Longleftarrow$ (الف) فرض کنید A حاصل‌جمع مستقیم (داخلی) زیرمدول‌های $\{A_i\}_{i\in I}$ باشد: $A = \oplus_{i\in I} A_i$، که در آن به ازای هر $i \in I$، $A_i \cong R$. پس $A \cong \oplus_{i\in I} R$. به سادگی می‌توان دید اگر یک R- مدول یکانی آزاد باشد هر R- مدول یکانی یکریخت با آن نیز آزاد است. چون $\oplus_{i\in I} R$ یک R- مدول یکانی آزاد و یکریخت با A است، A یک R- مدول آزاد است. □

نتیجه ۹.۴.۱۳. هر R- مدول یکانی آزاد با پایه‌ی n عضوی، به ویژه هر فضای برداری n بعدی روی حلقه‌ی تقسیم R، با $\underbrace{R \oplus \cdots \oplus R}_{n \text{ بار}}$ یکریخت است. □

برای تعریف همریختی از مدول آزاد یکانی به مدول دیگر کافی است آن‌را روی یک پایه‌ی آزاد تعریف کنیم. این مطلب محتوای قضیه‌ی بعد است.

قضیه ۱۰.۴.۱۳. فرض کنید A یک R- مدول یکانی آزاد با پایه‌ی X باشد. اگر M یک R- مدول یکانی دلخواه باشد، آنگاه هر تابع $g : X \longrightarrow M$ را می‌توان به یک همریختی یکتای $f : A \longrightarrow M$ توسعه داد، یعنی همریختی یکتای $f : A \longrightarrow M$ وجود دارد که $f|_X = g$، یعنی $f(x) = g(x)$ به ازای هر $x \in X$.

اثبات. چون X پایه‌ای برای A است، هر عضو $a \in A$ را می‌توان به صورت یکتای $a = r_1 x_1 + \cdots + r_n x_n$ نوشت که در آن $x_i \in X$ و $r_i \in R$. اگر تابع $f : A \longrightarrow M$ بخواهد همریختی باشد و به ازای هر $x \in X$، $f(x) = g(x)$، باید داشته باشیم

$$\begin{aligned} f(a) &= f(r_1 x_1 + \cdots + r_n x_n) \\ &= r_1 f(x_1) + \cdots + r_n f(x_n) \\ &= r_1 g(x_1) + \cdots + r_n g(x_n). \end{aligned}$$

پس تابع $f : A \longrightarrow M$ را با ضابطه‌ی

$$f(a) = r_1 g(x_1) + \cdots + r_n g(x_n)$$

تعریف می‌کنیم. f همریختی است، زیرا اگر $a = r_1 x_1 + r_2 x_2 + \cdots + r_n x_n$ و $b = s_1 x_1 + s_2 x_2 + \cdots + s_n x_n$ اعضایی از A

باشند و $r \in R$، که در آن $r_i, s_i \in R$ و $x_i, y_i \in X$، (با اضافه کردن $0x_i$ به a یا b، در صورت لزوم) داریم

$$\begin{aligned}
f(a+b) &= f(r_1x_1 + \cdots + r_nx_n + s_1x_1 + \cdots + s_nx_n) \\
&= f((r_1+s_1)x_1 + \cdots + (r_n+s_n)x_n) \\
&= (r_1+s_1)g(x_1) + \cdots + (r_n+s_n)g(x_n) \\
&= r_1g(x_1) + \cdots + r_ng(x_n) + s_1g(x_1) + \cdots + s_ng(x_n) \\
&= f(r_1x_1 + \cdots + r_nx_n) + f(s_1x_1 + \cdots + s_nx_n) \\
&= f(a) + f(b) \\
f(ra) &= f(r(r_1x_1 + \cdots + r_nx_n)) \\
&= f(rr_1x_1 + \cdots + rr_nx_n) \\
&= rr_1g(x_1) + \cdots + rr_ng(x_n) \\
&= r(r_1g(x_1) + \cdots + r_ng(x_n)) \\
&= rf(r_1x_1 + \cdots + r_nx_n) \\
&= rf(a).
\end{aligned}$$

به علاوه f یکتاست. زیرا اگر $h : A \longrightarrow M$ همریختی دیگری باشد که به ازای هر $x \in X$، $h(x) = g(x)$، آنگاه به ازای هر $a = r_1x_1 + \cdots + x_nx_n \in A$ داریم

$$\begin{aligned}
f(a) &= r_1g(x_1) + \cdots + r_ng(x_n) && (f \text{ طبق تعریف}) \\
&= r_1h(x_1) + \cdots + r_nh(x_n) && (g(x_i) = h(x_i) \text{ چون}) \\
&= h(r_1x_1 + \cdots + r_nx_n) && (h \text{ چون همریختی است}) \\
&= h(a)
\end{aligned}$$

بنابراین $f = h$. □

نتیجه ۱۱.۴.۱۳. هر R- مدول یکانی M تصویر همریخت یک R- مدول آزاد یکانی است.

اثبات. فرض کنید X یک مجموعه‌ی مولد برای M باشد (بزرگ‌ترین مجموعه‌ی مولد برای M خود M است). فرض کنید A یک R- مدول آزاد با پایه‌ای مثل Y باشد که $|X| = |Y|$. پس تابع یک‌به‌یک و پوشای $g : Y \longrightarrow X$ وجود دارد. بنا به قضیه‌ی قبل همریختی یکتای $f : A \longrightarrow M$ وجود دارد که به ازای هر $y \in Y$، $f(y) = g(y)$. چون $M = \langle X \rangle$ و g پوشاست، f پوشاست. بنابراین $A/\ker f \cong M$ و M تصویر همریخت R- مدول آزاد یکانی A است. □

تمرین‌ها

۱. فرض کنید A یک R- مدول باشد. ثابت کنید به ازای هر $a \in A$ و $r \in R$ داریم $r0 = 0$، $0a = 0$ و $-(ra) = (-r)a = r(-a)$.

۲. نشان دهید یک R- مدول متناهیاً تولید شده لزوماً گروه آبلی متناهیاً تولید شده نیست.

۳. فرض کنید $f : A \longrightarrow M$ یک همریختی R- مدولی باشد. نشان دهید
(الف) اگر B زیر مدول A باشد، آنگاه $f(b)$ زیر مدولی از M است.
(ب) اگر C زیر مدول M باشد، آنگاه $f^{-1}(C)$ زیر مدولی از A است.

۴. فرض کنید $f : A \longrightarrow A$ یک همریختی R- مدولی باشد و $f^2 = f$. نشان دهید $A = \operatorname{Im} f \oplus \ker f$.

۵. فرض کنید $f : A \longrightarrow M$ و $g : M \longrightarrow A$ همریختی‌های R- مدولی باشند، طوری که $g \circ f = \mathrm{id}_A$. نشان دهید $M = \operatorname{Im} f \oplus \ker g$.

۶. فرض کنید R حلقه‌ی یکدار باشد. ثابت کنید هر R- مدول یکانی دوری (با یک مولد) با R/I یکریخت است، که در آن I یک ایدآل چپ R است.

۷. فرض کنید V فضای برداری با بعد متناهی روی حلقه‌ی تقسیم R باشد. اگر U و W دو زیرفضای V باشند ثابت کنید
(الف) $U + W$ زیرفضایی از V است.
(ب) $\dim U + \dim W = \dim(U + W) + \dim(U \cap W)$.

۸. فرض کنید W زیرفضای فضای برداری V روی حلقه‌ی تقسیم R باشد. نشان دهید
(الف) $\dim W \leq \dim V$.
(ب) اگر $\dim V = \dim W$ و $\dim V$ متناهی باشد، آنگاه $W = V$.
(ج) $\dim V/W = \dim V - \dim W$.

۹. فرض کنید V و W فضاهای برداری روی حلقه‌ی تقسیم R باشند. اگر $f : V \longrightarrow W$ یک تبدیل خطی (یعنی همریختی R- مدولی) باشد، ثابت کنید پایه‌ای مثل X برای V وجود دارد که $X \cap \ker f$ پایه‌ای برای $\ker f$ و $\{f(x) \mid x \in X,\ \ f(x) \neq 0\}$ پایه‌ای برای $\operatorname{Im} f$ است؛ به ویژه

$$\dim_R V = \dim_R \ker f + \dim_R \operatorname{Im} f.$$

۱۰. فرض کنید A فضای برداری با بعد متناهی n روی حلقه‌ی تقسیم R باشد. نشان دهید ، به ازای هر m بعد $A^m = \underbrace{A \oplus \cdots \oplus A}_{m \text{ بار}}$ متناهی است و $\dim_R A^m = mn$.

۱۱. فرض کنید A و M دو R- مدول آزاد با پایه‌های X و Y هستند. نشان دهید اگر $|X| = |Y|$، آنگاه $A \cong M$.

۱۲. فرض کنید V یک فضای برداری روی حلقه‌ی تقسیم نامتناهی R باشد. اگر $W_1, \ldots, W_n$ زیرفضاهای ناصفر W باشند طوری که $V \subseteq \bigcup_{i=1}^{n} W_i$، نشان دهید $1 \leq j \leq n$ وجود دارد که $V \subseteq W_j$. نتیجه بگیرید که V را نمی‌توان به صورت اجتماع تعداد نامتناهی از زیرفضاهای نابدیهی نوشت.

۱۳. فرض کنید R یک دامنه‌ی ایدآل اصلی ، A یک R- مدول یکانی و $p \in R$ یک عضو اول (= تحویل ناپذیر) باشد. قرار می‌دهیم $pA = \{pa \mid a \in A\}$ و $A[p] = \{a \in A \mid pa = 0\}$. نشان دهید
(الف) pA و $A[p]$ زیرمدول‌های A هستند.
(ب) A/pA یک فضای برداری روی میدان $R/(p)$ است، که در آن ضرب اسکالر با $(r + (p))(a + pA) = ra + pA$ داده می‌شود.
(ج) $A[p]$ یک فضای برداری روی میدان $R/(p)$ است، که در آن ضرب اسکالر با $(r + (p))a = ra$ داده می‌شود.

۱۴. فرض کنید I و J ایدآل‌های راست [چپ] حلقه‌ی تعویض‌پذیر و یکدار R باشند. اگر R/I و R/J به عنوان R- مدول‌های راست [چپ] یکریخت باشند نشان دهید $I = J$. با ارئه‌ی مثالی نشان دهید که اگر شرط تعویض‌پذیر بودن R را حذف کنیم، ممکن است این حکم برقرار نباشد.

فصل ۱۴

میدان‌ها

در این فصل نوع خاصی از حلقه، یعنی میدان، را بررسی می‌کنیم. میدان‌ها کاربردهای زیادی در شاخه‌های مختلف ریاضیات، از جمله نظریه‌ی اعداد و نظریه‌ی معادله‌ها (که مرتبط با یافتن ریشه‌های چندجمله‌ای‌هاست)، و علوم دیگر دارند. در اینجا بیشتر روی نظریه‌ی معادله‌ها و ریشه‌ی چندجمله‌ای‌ها و هم‌چنین بررسی مقدماتی خواص اساسی میدان‌های متناهی تاکید می‌کنیم. از جمله نتایج این تاکید، ورود به نظریه‌ی گالوا و نظریه‌ی جبری کدگذاری است.

۱.۱۴ توسیع‌های جبری

فرض کنید F یک میدان باشد. می‌دانیم $\operatorname{char} F$ یا برابر صفر است و یا عدد اول p. به علاوه یادآوری می‌کنیم که اگر $\operatorname{char} F = 0$، آنگاه F زیرمیدانی یکریخت با $\mathbb{Q}$ دارد و اگر $\operatorname{char} F = p$، آنگاه F زیرمیدانی یکریخت با $\mathbb{Z}_p$ دارد (صفحه‌ی ۲۱۵ را ببینید).

تعریف ۱.۱.۱۴. میدان F را میدان اول گوییم، هرگاه زیرمیدان سره نداشته باشد.

مثال ۲.۱.۱۴. $\mathbb{Q}$ و $\mathbb{Z}_p$ میدان‌های اول هستند.

حل فرض کنید K زیرمیدانی از $\mathbb{Q}$ باشد. چون $K - \{0\}$ زیرگروه ضربی $\mathbb{Q} - \{0\}$ است، $1 \in K$. بنابراین، چون K زیرگروه جمعی $\mathbb{Q}$ است، $\mathbb{Z} \subseteq K$. در نتیجه $\mathbb{Q} \subseteq K$، پس $K = \mathbb{Q}$. هم‌چنین $\mathbb{Z}_p$ زیرمیدان سره ندارد. زیرا هر زیرمیدان، زیرگروه جمعی است و $\mathbb{Z}_p$ زیرگروه جمعی نابدیهی ندارد. □

قضیه ۳.۱.۱۴. اگر K زیرمیدان F باشد، آنگاه K زیرمیدان اول F است اگر و تنها اگر K برابر اشتراک همه‌ی زیرمیدان‌های F باشد.

اثبات. فرض کنید L اشتراک همه‌ی زیرمیدان‌های F باشد. چون K نیز زیرمیدانی از F است، $L \subseteq K$. اکنون اگر K زیرمیدان اول F باشد، چون زیرمیدان سره ندارد ، داریم $L = K$. برعکس اگر $L = K$، آنگاه K زیرمیدان سره ندارد. زیرا اگر E زیرمیدانی از K باشد، آنگاه E زیرمیدانی از F نیز هست و چون $L = K$ اشتراک زیرمیدان‌های F است، $K \subseteq E$. □

یادآوری می‌کنیم که اگر F میدان و K زیرمیدان F باشد، گوییم F توسیع K است. در این حالت می‌نویسیم $F : K$. اگر F و $A \subseteq F$، کوچک‌ترین زیرحلقه‌ی F که شامل اعضای K و A است را با $K[A]$ نشان می‌دهیم. به همین نحو کوچک‌ترین زیرمیدان F را که شامل اعضای K و A است را با $K(A)$ نشان می‌دهیم. بنابراین $K[A]$ برابر اشتراک همه‌ی زیرحلقه‌های F است که شامل $K \cup A$ هستند، و $K(A)$ برابر اشتراک همه‌ی زیرمیدان‌های F است که شامل $K \cup A$ هستند. $K[A]$ را زیرحلقه‌ی تولید شده توسط K و A گوییم. به همین نحو $K(A)$ را زیرمیدان تولید شده توسط K و A گوییم. اکنون می‌خواهیم شکل اعضای $K[A]$ و $K(A)$ را بیابیم. چون $K[A]$ زیرحلقه‌ی یک میدان است و به علاوه $1 \in K \subseteq K[A]$، $K[A]$ دامنه‌ی صحیح است. پس میدان کسرهای $K[A]$ وجود دارد و بنا به تمرین ۱ از صفحه‌ی ۲۲۱، کوچک‌ترین میدان شامل $K[A]$ است. این میدان کسرها چیزی جز $K(A)$ نیست، یعنی :

$$K(A) = \{rs^{-1} \mid r, s \in K[A], \quad s \neq 0\}.$$

اکنون $K[A]$ را توصیف می‌کنیم. اگر زیرحلقه‌ای از F شامل مجموعه‌ی A باشد، شامل همه‌ی حاصل‌ضرب‌های اعضای A نیز هست، یعنی شامل مجموعه‌ی

$$S = \{a_۱a_۲\cdots a_n \mid a_i \in A \cup \{۱\},\ \ n \in \mathbb{N}\}$$

است. اگر این زیرحلقه شامل K نیز باشد، شامل هر ترکیب خطی از حاصل‌ضرب عناصر K در عناصر مجموعه‌ی S است. پس این زیرحلقه شامل

$$\begin{aligned} T &= \{k_۱s_۱ + k_۲s_۲ + \cdots + k_ts_t \mid k_i \in K,\ \ s_i \in S,\ \ t \in \mathbb{N}\} \\ &= \{k_۱a_{۱۱}a_{۱۲}\cdots a_{۱n_۱} + \cdots + k_ta_{t_۱}a_{t_۲}\cdots a_{tn_t} \mid a_{ij} \in A \cup \{۱\}, \\ &\qquad\qquad k_j \in K,\ \ t, n_j \in \mathbb{N}\} \end{aligned}$$

است. بنابراین $T \subseteq K[A]$. اما به وضوح T زیرحلقه‌ای از F شامل $K \cup A$ است، پس $K[A] \subseteq T$. بنابراین $K[A] = T$. در حالتی که $A = \{a_۱, \ldots, a_n\}$، معمولاً به‌جای $K[A]$ می‌نویسیم $K[a_۱, a_۲, \ldots, a_n]$. به سادگی از تعریف می‌توان نتیجه گرفت $K[A][B] = K[A \cup B]$. پس $K[a_۱, a_۲, \ldots, a_n] = K[a_۱, a_۲, \ldots, a_{n-۱}][a_n]$ و به همین نحو $K(a_۱, \ldots, a_n) = K(a_۱, \ldots, a_{n-۱})(a_n)$.
توجه کنید

$$\begin{aligned} K[a_۱, \ldots, a_n] &= \{k_۱a_۱^{m_{۱۱}}a_۲^{m_{۱۲}}\cdots a_n^{m_{۱n}} + \cdots + k_ta_۱^{m_{t۱}}a_۲^{m_{t۲}}\cdots a_n^{m_{tn}} \mid \\ &\qquad\qquad k_j \in K, t \in \mathbb{N},\ \ m_{ij} \in \mathbb{N} \cup \{۰\}\} \\ &= \{f(a_۱, \ldots, a_n) \mid f(x_۱, \ldots, x_n) \in K[x_۱, \ldots, x_n]\} \end{aligned}$$

و

$$\begin{aligned} K(a_۱, \ldots, a_n) &= \{rs^{-۱} \mid r, s \in K[a_۱, \ldots, a_n],\ \ s \neq ۰\} \\ &= \{f(a_۱, \ldots, a_n)[g(a_۱, \ldots, a_n)]^{-۱} \mid g(a_۱, \ldots, a_n) \neq ۰\}. \end{aligned}$$

به ویژه داریم

$$\begin{aligned} K[a] &= \{k_۰ + k_۱a + \cdots + k_na^n \mid k_i \in K,\ \ n \in \mathbb{N}\} \\ &= \{f(a) \mid f(x) \in K[x]\} \end{aligned}$$

و

$$\begin{aligned} K(a) &= \{rs^{-۱} \mid r, s \in K[a],\ \ s \neq ۰\} \\ &= \{f(a)[g(a)]^{-۱} \mid g(a) \neq ۰\}. \end{aligned}$$

در بعضی حالت‌ها می‌توان توصیف ساده‌تری از $K(a)$ ارائه کرد. آن وقتی است که a روی K جبری باشد. ابتدا این مفهوم را تعریف می‌کنیم:

تعریف ۴.۱.۱۴. فرض کنید $F : K$ یک توسیع باشد. عضو $a \in F$ را روی K جبری گوییم هرگاه چندجمله‌ای ناصفر $f(x) \in K[x]$ وجود داشته باشد که $f(a) = ۰$. در غیر این صورت a را روی K متعالی گوییم.

بنابراین اگر $F : K$ توسیع باشد، $a \in F$ روی K جبری است اگر و تنها اگر ریشه‌ی یک چندجمله‌ای ناصفر با ضرایب در K باشد.

مثال ۵.۱.۱۴. $\sqrt{۲} \in \mathbb{R}$ روی $\mathbb{Q}$ جبری است، زیرا ریشه‌ی $x^۲ - ۲ \in \mathbb{Q}[x]$ است. $i \in \mathbb{C}$ روی $\mathbb{R}$ و هم‌چنین روی $\mathbb{Q}$ جبری است، زیرا ریشه‌ی $x^۲ + ۱ \in \mathbb{Q}[x]$ است. □

فرض کنید $F : K$ توسیع باشد و $a \in F$. نگاشت $\varphi_a : K[x] \longrightarrow F$ با ضابطه‌ی $\varphi_a(f(x)) = f(a)$،یک همریختی است، که آن‌را همریختی مقدارياب گوییم. داریم

$$\begin{aligned} \ker \varphi_a &= \{f(x) \in K[x] \mid \varphi_a(f(x)) = ۰\} \\ &= \{f(x) \in K[x] \mid f(a) = ۰\}. \end{aligned}$$

بنابراین a روی K جبری است اگر و تنها اگر همریختی مقدارياب φ_a یک‌به‌یک نباشد. توجه کنید $\operatorname{Im} \varphi_a = K[a]$.
اکنون فرض کنید a روی K جبری باشد. بنابراین $\ker \varphi_a$ ایدآل ناصفری از $K[x]$ است. بنا به قضیه‌ی ۱.۴.۱۱، $K[x]$ یک PID است، پس چندجمله‌ای ناصفر $m_a(x) \in K[x]$ وجود دارد که $\ker \varphi_a = (m_a(x)) = K[x]m_a(x)$. به علاوه چون یکه‌های $K[x]$ اعضای ناصفر K هستند ، می‌توان $m_a(x)$ را تکین اختیار کرد. $m_a(x)$ با این ویژگی‌ها را چندجمله‌ای می‌نیمال a روی K گوییم.
توجه کنید اگر $f(x) \in K[x]$ و $f(a) = ۰$، آنگاه $f(x) \in \ker \varphi_a = (m_a(x))$. پس چندجمله‌ای $g(x) \in K[x]$ وجود دارد که $f(x) = m_a(x)g(x)$. بنابراین $m_a(x)|f(x)$. برعکس اگر $f(x) = m_a(x)g(x)$، آنگاه $f(a) = m_a(a)g(a) = ۰$. بنابراین ثابت کرده‌ایم

قضیه ۶.۱.۱۴. فرض کنید $F : K$ توسیع و $a \in F$ روی K جبری با چندجمله‌ای می‌نیمال $m_a(x) \in K[x]$ باشد. اگر $f(x) \in K[x]$، آنگاه $f(a) = ۰$ اگر و تنها اگر $m_a(x)|f(x)$. □

مطلب مهم دیگر تحویل‌ناپذیری چندجمله‌ای می‌نیمال است:

قضیه ۷.۱.۱۴. اگر $F : K$ یک توسیع، $a \in F$ روی K جبری با چندجمله‌ای می‌نیمال $m_a(x) \in K[x]$ روی K باشد، آنگاه $m_a(x)$ روی $K[x]$ تحویل‌ناپذیر است.

اثبات. همریختی مقدارياب $\varphi_a : K[x] \longrightarrow F$ را در نظر می‌گیریم. آنگاه طبق تعریف، $\ker \varphi_a = (m_a(x))$. اگر $f(x), g(x) \in K[x]$ و $m_a(x) = f(x)g(x)$، آنگاه

$$۰ = m_a(a) = \varphi_a(m_a(x)) = \varphi_a(f(x))\varphi_a(g(x)) = f(a)g(a).$$

پس $f(a) = ۰$ یا $g(a) = ۰$. اگر $f(a) = ۰$، آنگاه $m_a(x)|f(x)$. از این‌رو چندجمله‌ای $h(x) \in K[x]$ وجود دارد که $f(x) = m_a(x)h(x)$. در نتیجه

$$m_a(x) = m_a(x)h(x)g(x),$$

و چون $K[x]$ دامنه‌ی صحیح است، $h(x)g(x) = ۱$. بنابراین $g(x)$ یکه است. به همین نحو اگر $g(a) = ۰$ آنگاه $f(x)$ یکه است. از این رو $m_a(x)$ در $K[x]$ تحویل‌ناپذیر است. □

نتیجه ۸.۱.۱۴. اگر $F : K$ توسیع باشد، آنگاه $a \in F$ روی K جبری است اگر و تنها اگر $K(a) = K[a]$.

اثبات. ابتدا توجه کنید همواره داریم $K[a] \subseteq K(a)$. فرض کنید a روی K جبری و $m_a(x)$ چندجمله‌ای می‌نیمال a روی K باشد. طبق قضیه‌ی ۷.۱.۱۴، $m_a(x)$ روی K تحویل‌ناپذیر است. پس ، بنا به قضیه ۲.۴.۱۱، $(m_a(x))$ یک ایدآل ماکسیمال $K[x]$ و بنا به قضیه‌ی ۳.۴.۱۱، $\dfrac{K[x]}{(m_a(x))}$ یک میدان است. از طرفی بنا به اولین قضیه‌ی یکریختی داریم

$$\frac{K[x]}{(m_a(x))} = \frac{K[x]}{\ker \varphi_a} \cong \operatorname{Im} \varphi_a = K[a],$$

که در آن $\varphi_a : K[x] \longrightarrow F$ همریختی مقدارياب است. بنابراین $K[a]$ زیرمیدان F است. چون $K(a)$ کوچک‌ترین زیرمیدان F شامل K و a است. $K(a) \subseteq K[a]$. در نتیجه $K(a) = K[a]$.
اکنون برعکس فرض کنید $K[a] = K(a)$. اگر $a = ۰$، آنگاه a ریشه‌ی چندجمله‌ای $x \in K[x]$ و بنابراین جبری است. پس فرض کنید $a \neq ۰$، آنگاه $a^{-۱} \in K(a) = K[a]$. بنابراین $f(x) \in K[x]$ وجود دارد که $a^{-۱} = f(a)$، یعنی $af(a) + ۱ = ۰$ و a ریشه‌ی چندجمله‌ای $xf(x) + ۱ \in K[x]$ است. از این‌رو a روی K جبری است. □

اکنون مفهوم‌های جبری و متعالی را از دید دیگری بررسی می‌کنیم. اگر $F : K$ توسیع باشد، آنگاه F را می‌توان به عنوان فضای برداری روی K در نظر گرفت. در واقع $(F, +)$ گروه آبلی است و به ازای هر $a, b \in F$ و $k, r \in K$، داریم $k(a + b) = ka + kb$، $(kr)a = k(ra)$ و $1a = a$. بُعد F به عنوان فضای برداری روی K را درجه‌ی F روی K یا درجه‌ی توسیع $F : K$ می‌نامیم و با $[F : K]$ نشان می‌دهیم:

$$\dim_K F = [F : K].$$

اگر درجه‌ی توسیع $F : K$ متناهی باشد، گوییم F توسیع متناهی K است.

قضیه ۹.۱.۱۴. اگر $F : K$ توسیع باشد، آنگاه $a \in F$ روی K جبری است اگر و تنها اگر $[K(a) : K]$ متناهی باشد. در این حالت اگر $\deg m_a(x) = n$، آنگاه $\{1, a, a^2, \ldots, a^{n-1}\}$ پایه‌ای برای $K(a)$ روی K است. بنابراین $[K(a) : K] = n$ و $K(a) = \{g(a) \mid g(x) \in K[x],\ \deg g(x) \leq n - 1\}$.

اثبات. ($\Longrightarrow$) فرض کنید $[K(a) : K] = n < \infty$. پس بُعد فضای برداری $K(a)$ روی K برابر n است. به ویژه، بنا به قضیه‌ی ۵.۴.۱۳، هر $n + 1$ بردار در $K(a)$ وابسته‌ی خطی‌اند. بنابراین اعضای 1، a، a^2، ...، a^n روی K وابسته‌ی خطی‌اند. یعنی عناصر k_0، k_1، ...، k_n از K، که حداقل یکی از آن‌ها ناصفر است، وجود دارند که

$$k_0 1 + k_1 a + k_2 a^2 + \cdots + k_n a^n = 0.$$

قرار می‌دهیم $f(x) = k_0 + k_1 x + \cdots + k_n x^n$. پس $f(x) \in K[x]$ چندجمله‌ای ناصفر است و $f(a) = 0$؛ یعنی a روی K جبری است.

($\Longleftarrow$) فرض کنید $m_a(x) \in K[x]$ چندجمله‌ای می‌نیمال a روی K باشد. بنابه نتیجه‌ی ۸.۱.۱۴، $K[a] = K(a)$. عضو دلخواه $g(a) \in K[a] = K(a)$ را در نظر می‌گیریم. بنابه الگوریتم تقسیم، چندجمله‌ای‌های $q(x), r(x) \in K[x]$ وجود دارند که $g(x) = q(x)m_a(x) + r(x)$، که در آن $r(x) = 0$ یا $\deg r(x) < \deg m_a(x)$. بنابراین $g(a) = q(a)m_a(a) + r(a) = r(a)$. در نتیجه $\{1, a, a^2, \ldots, a^{n-1}\}$ فضای $K(a)$ را تولید می‌کند.
اکنون فرض کنید

$$k_0 + k_1 a + k_2 a^2 + \cdots + k_{n-1} a^{n-1} = 0, \quad k_i \in K.$$

چندجمله‌ای $h(x) = k_0 + k_1 x + \cdots + k_{n-1} x^{n-1} \in K[x]$ را در نظر می‌گیریم. اگر برخی از k_i ها صفر نباشند، آنگاه a ریشه‌ی چندجمله‌ای ناصفر $h(x)$ است و $\deg h(x) < n$، که این امکان ندارد. پس به ازای هر i، $k_i = 0$ و $\{1, a, a^2, \ldots, a^{n-1}\}$ روی K مستقل خطی نیز هست. از این رو $\{1, a, a^2, \ldots, a^{n-1}\}$ پایه‌ای برای $K(a)$ روی K است. □

مثال ۱۰.۱.۱۴. $\sqrt{2} \in \mathbb{R}$ روی $\mathbb{Q}$ جبری با چندجمله‌ای می‌نیمال $m(x) = x^2 - 2$ است. بنابراین داریم $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$ و $\{1, \sqrt{2}\}$ پایه‌ای برای $\mathbb{Q}(\sqrt{2})$ روی $\mathbb{Q}$ است. از این‌رو $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$. □

مثال ۱۱.۱.۱۴. $i \in \mathbb{C}$ روی $\mathbb{R}$ جبری با چندجمله‌ای می‌نیمال $m(x) = x^2 + 1$ است. بنابراین $[\mathbb{R}(i) : \mathbb{R}] = 2$ و $\{1, i\}$ پایه‌ای برای $\mathbb{R}(i)$ روی $\mathbb{R}$ است و

$$\mathbb{R}(i) = \{a + bi \mid a, b \in \mathbb{R}\} = \mathbb{C}. \qquad \square$$

مثال ۱۲.۱.۱۴. $\mathbb{Q}(2 + \sqrt{3}i)$ را توصیف کنید.

حل فرض کنید $a = 2 + \sqrt{3}i$. در این صورت $(a - 2)^2 = -3$ یا $a^2 - 4a + 7 = 0$. بنابراین a ریشه‌ای از چندجمله‌ای $p(x) = x^2 - 4x + 7$ است. $p(x)$ روی $\mathbb{Q}$ تحویل‌ناپذیر است، زیرا روی $\mathbb{Q}$ ریشه‌ای ندارد و $\deg p(x) = 2$. پس $p(x)$ چندجمله‌ای می‌نیمال a روی $\mathbb{Q}$ است و بنا به قضیه‌ی ۹.۱.۱۴، $\mathbb{Q}(a) = \{r + sa \mid r, s \in \mathbb{Q}\}$. □

مثال ۱۳.۱.۱۴. اگر p عدد اول باشد، چندجمله‌ای $f(x) = 1 + x + \cdots + x^{p-1}$، بنا به مثال ۲۰.۲.۱۱ از صفحه‌ی ۲۴۴، روی $\mathbb{Q}[x]$ تحویل‌ناپذیر است. اگر $w = e^{\frac{2i\pi}{p}}$، آنگاه w ریشه‌ای از $x^p - 1 = 0$ است. چون $x^p - 1 = (x - 1)f(x)$ و $w \neq 1$، پس w ریشه‌ی $f(x)$ است. بنابراین $f(x)$ چندجمله‌ای می‌نیمال w روی $\mathbb{Q}$ است. از این‌رو $[\mathbb{Q}(w) : \mathbb{Q}] = p - 1$ و $\{1, w, w^2, \ldots, w^{p-2}\}$ پایه‌ای برای $\mathbb{Q}(w)$ روی $\mathbb{Q}$ است. □

توسیع $F : K$ را توسیع جبری گوییم هرگاه هر عضو F روی K جبری باشد. مثال‌های زیادی از توسیع‌های جبری وجود دارد و در واقع هر توسیع متناهی جبری است، این مطلب محتوای قضیه‌ی بعدی است.

قضیه ۱۴.۱.۱۴. اگر $F : K$ توسیع متناهی باشد، آنگاه $F : K$ توسیع جبری است.

اثبات. فرض کنید $[F : K] = n$ و عضو $a \in F$ را در نظر بگیرید. چون بُعد F روی K برابر n است، هر $n + ۱$ عضو F روی K وابسته خطی‌اند. به ویژه $۱, a, a^۲, \ldots, a^n$ وابسته‌ی خطی هستند. بنابراین $k_۰, k_۱, \ldots, k_n \in K$، که حداقل یکی از آن‌ها صفر نیست، وجود دارند که

$$k_۰ ۱ + k_۱ a + k_۲ a^۲ + \cdots + k_n a^n = ۰.$$

پس a ریشه‌ی چندجمله‌ای ناصفر $f(x) = k_۰ + k_۱ x + \cdots + k_n x^n \in K[x]$ است؛ یعنی a روی K جبری است. از این‌رو $F : K$ توسیع جبری است. □

این سوال مطرح می‌شود که آیا عکس قضیه‌ی ۱۴.۱.۱۴، درست است؟ یعنی آیا هر توسیع جبری، متناهی است. جواب منفی است؟ برای پاسخ به این سوال و اهداف دیگر ابتدا قضیه‌ای مهم موسوم به قانون برج را ثابت می‌کنیم. در صورتی که $L : K$ و $F : L$ توسیع باشند می‌نویسیم $F : L : K$ و می‌گوییم L میدان میانی است.

قضیه ۱۵.۱.۱۴. (قانون برج) اگر $L : K$ و $F : L$ توسیع‌های متناهی باشند، آنگاه $F : K$ نیز توسیع متناهی است و

$$[F : K] = [F : L][L : K].$$

اثبات. فرض کنید $[L : K] = n$ و $[F : L] = m$. فرض کنید $\mathscr{A} = \{x_۱, x_۲, \ldots, x_n\}$ پایه‌ای از L روی K و $\mathscr{B} = \{y_۱, y_۲, \ldots, y_m\}$ پایه‌ای از F روی L باشند. ادعا می‌کنیم $\mathscr{C} = \{x_i y_j \mid ۱ \le i \le n, \quad ۱ \le j \le m\}$ پایه‌ای برای F روی K است. عضو دلخواه $a \in F$ را در نظر می‌گیریم. چون $\mathscr{B}$، پایه‌ای از F روی L است، اسکالرهای $\ell_۱, \ell_۲, \ldots, \ell_m \in L$ وجود دارند که

$$a = \sum_{i=۱}^{m} \ell_i y_i.$$

اکنون چون $\ell_i \in L$ و $\mathscr{A}$ پایه‌ای برای L روی K است، اسکالرهای $k_{i_۱}, k_{i_۲}, \ldots, k_{i_n} \in K$ وجود دارند که

$$\ell_i = \sum_{j=۱}^{n} k_{ij} x_j.$$

بنابراین

$$a = \sum_{i=۱}^{m} \ell_i y_i = \sum_{i=۱}^{m} \sum_{j=۱}^{n} k_{ij} x_j y_i,$$

و چون $k_{ij} \in L$، $\mathscr{C}$ فضای F را روی K تولید می‌کند. حال فرض کنید

$$\sum_{i=۱}^{m} \sum_{j=۱}^{n} k_{ij} x_i y_j = ۰, \quad k_{ij} \in K.$$

بنابراین، چون $k_{ij} x_i \in L$ و $\mathscr{B}$ روی L مستقل خطی است، داریم

$$\sum_{j=۱}^{n} k_{ij} x_i = ۰, \quad i = ۱, ۲, \ldots, m.$$

اکنون چون $\mathscr{A}$ روی K مستقل خطی است، داریم

$$k_{ij} = ۰, \quad i = ۱, ۲, \ldots, m, \quad j = ۱, ۲, \ldots, n.$$

بنابراین $\mathscr{C}$ روی K مستقل خطی است. پس $\mathscr{C}$ یک پایه برای F روی K است و

$$[F : K] = |\mathscr{C}| = mn = [F : L][L : K]. \qquad \square$$

مثال ۱۶.۱.۱۴. درجه‌ی توسیع $[\mathbb{Q}(\sqrt{۲},\sqrt{۳}):\mathbb{Q}]$ و پایه‌ای از آن را بیابید.

حل $\sqrt{۲}$ روی $\mathbb{Q}$ جبری با چندجمله‌ای می‌نیمال $x^۲-۲$ است. پس $[\mathbb{Q}(\sqrt{۲}):\mathbb{Q}]=۲$ و $\{۱,\sqrt{۲}\}$ پایه‌ای برای $\mathbb{Q}(\sqrt{۲})$ روی $\mathbb{Q}$ است. اکنون ادعا می‌کنیم $x^۲-۳$ چندجمله‌ای می‌نیمال $\sqrt{۳}$ روی $\mathbb{Q}(\sqrt{۲})$ است. چون $\pm\sqrt{۳}$ ریشه‌های $x^۲-۳$ هستند ، کافی است ثابت کنیم $\pm\sqrt{۳}\notin\mathbb{Q}(\sqrt{۲})$. اگر چنین نباشد و $\sqrt{۳}=a+b\sqrt{۲}\in\mathbb{Q}(\sqrt{۲})$، که در آن $a,b\in\mathbb{Q}$. آنگاه $a\neq ۰$ و $b\neq ۰$، به علاوه با بتوان رساندن دو طرف تساوی داریم $۳=a^۲+۲ab\sqrt{۲}+۲b^۲\in\mathbb{Q}$؛ که نتیجه می‌دهد $\sqrt{۲}=\dfrac{۳-a^۲-۲b^۲}{۲ab}$. این تناقض است. بنابراین $\pm\sqrt{۳}\notin\mathbb{Q}(\sqrt{۲})$ و $x^۲-۳$ روی $\mathbb{Q}(\sqrt{۲})$ تحویل‌ناپذیر است. از این‌رو $[\mathbb{Q}(\sqrt{۲})(\sqrt{۳}):\mathbb{Q}(\sqrt{۲})]=۲$ و $\{۱,\sqrt{۳}\}$ پایه‌ای برای $\mathbb{Q}(\sqrt{۲},\sqrt{۳})$ روی $\mathbb{Q}(\sqrt{۲})$ است. پس بنا به قانون برج

$$[\mathbb{Q}(\sqrt{۲},\sqrt{۳}):\mathbb{Q}]=[\mathbb{Q}(\sqrt{۲},\sqrt{۳}):\mathbb{Q}(\sqrt{۲})][\mathbb{Q}(\sqrt{۲}):\mathbb{Q}]=۲\times۲=۴$$

و $\{۱,\sqrt{۲},\sqrt{۳},\sqrt{۶}\}$ پایه‌ای برای $\mathbb{Q}(\sqrt{۲},\sqrt{۳})$ روی $\mathbb{Q}$ است. □

مثال ۱۷.۱.۱۴. نشان دهید $[\mathbb{R}:\mathbb{Q}]=\infty$.

حل فرض کنید برخلاف حکم $[\mathbb{R}:\mathbb{Q}]=n<\infty$. عدد صحیح مثبت m را طوری در نظر می‌گیریم که $m>n$. بنا به محک آیزنشتاین (با $p=۲$) چندجمله‌ای $x^m-۲$ روی $\mathbb{Q}$ تحویل‌ناپذیر است. پس $x^m-۲$ چندجمله‌ای ماکسیمال $\sqrt[m]{۲}$ است و $[\mathbb{Q}(\sqrt[m]{۲}):\mathbb{Q}]=m$. اکنون بنا به قانون برج داریم

$$n=[\mathbb{R}:\mathbb{Q}]=[\mathbb{R}:\mathbb{Q}(\sqrt[m]{۲})][\mathbb{Q}(\sqrt[m]{۲}):\mathbb{Q}]=m[\mathbb{R}:\mathbb{Q}(\sqrt[m]{۲})]\geq m,$$

که تناقض است. بنابراین $[\mathbb{R}:\mathbb{Q}]=\infty$. □

اگر $a,b\in F$ روی K جبری باشند، آنگاه حاصل‌جمع و حاصل‌ضرب آن‌ها، در واقع هر عضو c حاصل‌ضرب از اعمال جبری روی a و b، روی K جبری است. نکته‌ی جالب توجه این است که اثبات این مطلب با استفاده از قانون برج انجام می‌شود بدون آن که مجبور باشیم چندجمله‌ای که c در آن صدق می‌کند را معرفی کنیم:

قضیه ۱۸.۱.۱۴. اگر $F:K$ توسیع باشد، آنگاه

$$L=\{a\in F\mid \text{ جبری } K \text{ روی } a\}$$

یک زیرمیدان F شامل K است.

اثبات. اگر $k\in K$، آنگاه k ریشه‌ی چندجمله‌ای $x-k\in K[x]$ است. بنابراین $K\subseteq L$. اکنون اگر $a,b\in L$، آنگاه a و b روی K جبری‌اند. پس بنا به قضیه‌ی ۹.۱.۱۴، $[K(a):K]=r<\infty$ و $[K(b):K]=s<\infty$. اگر $m_b(x)\in K[x]$ چندجمله‌ای می‌نیمال b روی K باشد، آنگاه چون $m_b(x)\in K[x]\subseteq K(a)[x]$، b روی $K(a)$ جبری است و

$$[K(a,b):K(a)]=[K(a)(b):K(a)]\leq \deg m_b(x)=s.$$

از این‌رو بنا به قانون برج (قضیه‌ی ۱۵.۱.۱۴)،

$$[K(a,b):K]=[K(a,b):K(a)][K(a):K]\leq rs<\infty.$$

بنابراین بنا به قضیه‌ی ۱۴.۱.۱۴، $K(a,b):K$ توسیع جبری است. اکنون $a-b$ و $ab^{-۱}$، $(b\neq ۰)$ به $K(a,b)$ تعلق دارند، بنابراین روی K جبری‌اند، یعنی $a-b\in L$ و $ab^{-۱}\in L$، $(b\neq ۰)$. پس L زیرمیدان F است. □

در مثال بعد نشان می‌دهیم که توسیع جبری نامتناهی وجود دارد ، پس عکس قضیه‌ی ۱۴.۱.۱۴، درست نیست.

مثال ۱۹.۱.۱۴. نشان دهید توسیع نامتناهی جبری وجود دارد.

حل توسیع $\mathbb{Q} : \mathbb{R}$ را در نظر می‌گیریم. فرض کنید

$$L = \{a \in \mathbb{R} \mid a \text{ روی } \mathbb{Q} \text{ جبری است}\}$$

زیرمیدان همه‌ی اعداد حقیقی باشد که روی $\mathbb{Q}$ جبری هستند. بنا به قضیه‌ی ۱۸.۱.۱۴، $L : \mathbb{Q}$ توسیع جبری است. ادعا می‌کنیم $[L : \mathbb{Q}] = \infty$. اگر چنین نباشد و $[L : \mathbb{Q}] = n < \infty$. عدد صحیح مثبت m را طوری در نظر می‌گیریم که $m > n$. بنا به محک آیزنشتاین (با $p = ۲$) چندجمله‌ای $x^m - ۲$ روی $\mathbb{Q}$ تحویل‌ناپذیر است. پس $x^m - ۲$ چندجمله‌ای ماکسیمال $\sqrt[m]{۲}$ است و $[\mathbb{Q}(\sqrt[m]{۲}) : \mathbb{Q}] = m$. اکنون بنا به قانون برج داریم

$$n = [L : \mathbb{Q}] = [L : \mathbb{Q}(\sqrt[m]{۲})][\mathbb{Q}(\sqrt[m]{۲}) : \mathbb{Q}] = m[L : \mathbb{Q}(\sqrt[m]{۲})] \geq m,$$

که تناقض است. بنابراین $[L : \mathbb{Q}] = \infty$. □

ثابت کردیم که اگر $F : K$ توسیع باشد، آنگاه a روی K جبری است اگر و تنها اگر $K(a) : K$ توسیع متناهی باشد. اکنون این مطلب را ، با استفاده از قانون برج، تعمیم می‌دهیم:

قضیه ۲۰.۱.۱۴. اگر $F : K$ توسیع باشد، آنگاه $a_۱, a_۲, \ldots, a_n \in F$ روی K جبری‌اند، اگر و تنها اگر $K(a_۱, a_۲, \ldots, a_n) : K$ توسیع متناهی باشد.

اثبات. ($\Longrightarrow$) فرض کنید $K(a_۱, a_۲, \ldots, a_n) : K$ توسیع متناهی باشد. بنا به قضیه‌ی ۱۴.۱.۱۴، هر توسیع متناهی، جبری است. بنابراین $K(a_۱, a_۲, \ldots, a_n) : K$ توسیع جبری است؛ به ویژه $a_۱$، $a_۲$، ...، a_n روی K جبری‌اند.
($\Longleftarrow$) قرار می‌دهیم $K_۰ = K$ و $K_i = K(a_۱, \ldots, a_i) = K_{i-۱}(a_i)$، به ازای هر $۱ \leq i \leq n$. بنابراین $K(a_۱, \ldots, a_n) = K_n$.
چون $a_i \in K_i$ روی K جبری است و $K \subseteq K_{i-۱}$، پس a_i روی $K_{i-۱}$ جبری است. در نتیجه بنا به قضیه‌ی ۹.۱.۱۴، $[K_i : K_{i-۱}] < \infty$. بنابراین با استفاده مکرر از قانون برج داریم

$$\begin{aligned}[K(a_۱, \ldots, a_n) : K] &= [K_n : K] \\ &= [K_n : K_{n-۱}][K_{n-۱} : K_{n-۲}] \cdots [K_۱ : K_۰] < \infty. \square\end{aligned}$$

قضیه ۲۱.۱.۱۴. اگر $F : L : K$، آنگاه $F : K$ توسیع جبری است اگر و تنها اگر $F : L$ و $L : K$ توسیع‌های جبری باشند.

اثبات. ($\Longleftarrow$) فرض کنید $F : K$ توسیع جبری باشد. عضو دلخواه $a \in F$ را در نظر می‌گیریم. چون $F : K$ جبری است. چندجمله‌ای ناصفر $f(x) \in K[x]$ وجود دارد که $f(a) = ۰$. چون $K \subseteq L$، داریم $f(x) \in K[x] \subseteq L[x]$. بنابراین a روی L جبری است. از این‌رو $L : F$ جبری است. از طرف دیگر چون هر عضو L به F تعلق دارد و F روی K جبری است، $L : K$ نیز جبری است.
($\Longrightarrow$) فرض کنید $F : L$ و $L : K$ جبری هستند. عضو دلخواه $a \in F$ را در نظر می‌گیریم. چون $F : L$ جبری است، چندجمله‌ای ناصفر $\ell_۰ + \ell_۱ x + \cdots + \ell_n x^n \in L[x]$ وجود دارد که a ریشه‌ی آن است. بنابراین a روی $K(\ell_۰, \ell_۱, \ldots, \ell_n)$ جبری است. پس

$$K(\ell_۰, \ell_۱, \ldots \ell_n)(a) : K(\ell_۰, \ell_۱, \ldots, \ell_n)$$

توسیع متناهی است. چون $\ell_۰$، $\ell_۱$، ...، ℓ_n روی K جبری هستند ، بنا به قضیه‌ی ۲۰.۱.۱۴، $K(\ell_۰, \ell_۱, \ldots, \ell_n) : K$ توسیع متناهی است. با استفاده از قانون برج داریم

$$\begin{aligned}[K(\ell_۰, \ell_۱, \ldots, \ell_n)(a) : K] &= [K(\ell_۰, \ell_۱, \ldots, \ell_n)(a) : K(\ell_۰, \ell_۱, \ldots, \ell_n)] \times \\ &\quad [K(\ell_۰, \ell_۱, \ldots, \ell_n) : K],\end{aligned}$$

که نتیجه می‌دهد $K(\ell_۰, \ell_۱, \ldots, \ell_n, a) : K$ توسیع متناهی است. بنابراین، بنا به قضیه‌ی ۱۴.۱.۱۴، a روی K جبری است. □

تمرین‌ها

۱. فرض کنید a, b دو عدد مختلط باشند. اگر a, b روی $\mathbb{Q}$ متعالی باشند، آیا می‌توان نتیجه گرفت که a^b روی $\mathbb{Q}$ متعالی است؟

۲. در هر حالت یک پایه برای F روی $\mathbb{Q}$ بیابید.
(الف) $F = \mathbb{Q}(\sqrt[3]{2})$ (ب) $F = \mathbb{Q}(1 + 2i)$
(ج) $F = \mathbb{Q}(\sqrt{3}, \sqrt{7})$ (د) $F = \mathbb{Q}(\sqrt[3]{3}, \sqrt{2})$

۳. در هر حالت درجه‌ی توسیع داده شده را بیابید.
(الف) $\mathbb{Q}(\sqrt{2}) : \mathbb{Q}(\sqrt{2} + \sqrt{3})$ (ب) $\mathbb{Q}(\sqrt{21}) : \mathbb{Q}(\sqrt{3}, \sqrt{7})$
(ج) $\mathbb{Q}(i) : \mathbb{Q}(\sqrt{2} + 3i)$ (د) $\mathbb{Q}(\sqrt{3}) : \mathbb{Q}(\sqrt[3]{2}, \sqrt{3})$

۴. فرض کنید $\theta = 2\frac{\pi}{7}$. چندجمله‌ای می‌نیمال $e^{i\theta}$ و $2\cos\theta$ روی $\mathbb{Q}$ را بیابید.

۵. فرض کنید $K : F$ یک توسیع با درجه‌ی عدد اول باشد. نشان دهید به ازای هر $a \in F - K$ داریم $F = K(a)$.

۶. فرض کنید $K : F$ توسیع باشد. اگر $a, b \in F$ روی K جبری به ترتیب با درجه‌های m و n باشند، نشان دهید
(الف) $[K(a, b) : K] \leq mn$.
(ب) اگر $\gcd\{m, n\} = 1$، آنگاه $[K(a, b) : K] = mn$.
(ج) عکس (ب) درست نیست.

۷. فرض کنید $K : F$ توسیع و $a \in F$ روی K جبری باشد. اگر $f(x) \in K[x]$، نشان دهید $f(a)$ روی K جبری است.

۸. فرض کنید $K : F$ توسیع، $0 \neq f(x) \in K[x]$، و a عضوی از F باشد. اگر $f(a)$ روی K جبری باشد، نشان دهید a روی K جبری است.

۹. فرض کنید $K : F$ توسیع باشد و $a, b \in F$. اگر $a + b$ روی K جبری باشد، نشان دهید b روی $K(a)$ جبری است.

۱۰. فرض کنید $K : K(a, b)$ یک توسیع باشد. اگر $a \notin K$، a روی K جبری و b روی K متعالی باشد، نشان دهید به ازای هر $c \in K(a, b)$، $K(a, b) \neq K(c)$.

۱۱. فرض کنید $K : F$ توسیع جبری است. اگر K شمارا باشد، نشان دهید F نیز شمارا است. نتیجه بگیرید عدد حقیقی متعالی روی $\mathbb{Q}$ وجود دارد.

۱۲. فرض کنید $p, q \in \mathbb{Q}$. اگر $\sqrt{p} \notin \mathbb{Q}$ و $\sqrt{q} \notin \mathbb{Q}(\sqrt{p})$.
(الف) نشان دهید $\mathbb{Q}(\sqrt{p}, \sqrt{q}) = \mathbb{Q}(\sqrt{p} + \sqrt{q})$.
(ب) پایه‌ای برای $\mathbb{Q}(\sqrt{p}, \sqrt{q})$ روی $\mathbb{Q}$ بیابید.
(ج) نشان دهید $x^4 - 2(p + q)x^2 + (p - q)^2$ چندجمله‌ای می‌نیمال $\sqrt{p} + \sqrt{q}$ روی $\mathbb{Q}$ است.

۱۳. میدان F را بسته‌ی جبری گوییم، هرگاه هر چندجمله‌ای با ضرایب در F روی F کاملاً تجزیه شود. نشان دهید هر میدان بسته‌ی جبری نامتناهی است.

۱۴. فرض کنید a روی میدان K متعالی است. اگر $f(x), g(x) \in K[x]$ دو چندجمله‌ای باشند که در $K[x]$ نسبت به هم اول‌اند، نشان دهید $f(x) - ag(x)$ در $K(a)[x]$ تحویل‌ناپذیر است. آیا شرط متعالی بودن a لازم است؟

۱۵. فرض کنید a روی میدان K متعالی باشد. اگر $b \in K(a) - K$، نشان دهید
(الف) b روی K متعالی است.
(ب) اگر $b = \frac{f(a)}{g(a)}$، که در آن $f(x), g(x) \in K[x]$ دو چندجمله‌ای هستند که در $K[x]$ نسبت به هم اول‌اند، آنگاه

$$[K(a) : K(b)] = \max\{\deg(f(x)), \deg(g(x))\}.$$

(ج) $K(a) : K(b)$ توسیع متناهی است.

۲.۱۴ توسیع‌های تجزیه

فرض کنید K یک میدان و $f(x) \in K[x]$ چندجمله‌ای ناصفر با درجه‌ی n باشد. می‌خواهیم توسیعی از K را بررسی کنیم که $f(x)$ روی آن به عوامل خطی تجزیه شود. یادآوری می‌کنیم بنا به قضیه‌ی کرونکر (قضیه‌ی ۱۱.۴.۱۱، صفحه‌ی ۲۵۳) توسیعی از K وجود دارد که $f(x)$ در آن دارای ریشه است. قضیه‌ی کرونکر را با نمادهای این فصل مرور می‌کنیم. ابتدا فرض کنید $f(x)$ روی $K[x]$ تحویل‌ناپذیر باشد. در این حالت $(f(x))$ ایدآل ماکسیمال $K[x]$ و $F = \frac{K[x]}{(f(x))}$ میدان است. پس از یکی گرفتن هر $k \in K$ با هم مجموعه‌ی $\bar{k} = k + (f(x))$ در F، می‌توان F را به عنوان توسیعی از K در نظر گرفت. به علاوه با فرض $a = \bar{x} = x + (f(x))$ داریم $f(a) = ۰$. بنابراین $a \in F$ ریشه‌ی چندجمله‌ای تحویل‌ناپذیر $f(x) \in K[x]$ است. از این‌رو ضرایب اسکالری از چندجمله‌ای می‌نیمال a روی K است. بنابراین

$$[F : K] = \deg f(x) = n.$$

توجه کنید $F = K(a)$. در حالت کلی دیدیم که $f(x)$ به صورت $f(x) = p(x)g(x)$ تجزیه می‌شود که در آن $p(x)$ چندجمله‌ای تکین و تحویل‌ناپذیر در $K[x]$ است. پس $p(x)$ و بنابراین $f(x)$ در توسیع $F = \frac{K[x]}{(p(x))}$ دارای ریشه است.

قضیه ۱.۲.۱۴. فرض کنید K میدان و $f(x) \in K[x]$ یک چندجمله‌ای غیرثابت با درجه‌ی n باشد. در این صورت توسیع $F : K$ وجود دارد که $f(x)$ روی F به عوامل خطی تجزیه می‌شود و درجه‌ی F روی K حداکثر $n!$ است.

اثبات. به استقرا روی $n = \deg f(x)$ عمل می‌کنیم. اگر $n = ۱$، آنگاه $f(x)$ روی $K[x]$ به عوامل خطی تجزیه می‌شود و $K : K$ توسیع تجزیه‌ی $f(x)$ است و $[K : K] = ۱$. اکنون فرض کنید $n > ۱$ و قضیه برای همه‌ی چندجمله‌ای‌های با درجه‌ی $n - ۱$ درست باشد. اگر $f(x)$ روی K به عوامل خطی تجزیه شود، چیزی برای اثبات نیست. پس فرض کنید $p(x)$ یک عامل تحویل‌ناپذیر و تکین از $f(x)$ باشد، که ریشه‌ای در K ندارد. بنا به قضیه‌ی کرونکر، توسیع $K_۱ : K$ و $a_۱ \in K_۱$ وجود دارد که $f(a_۱) = ۰$ و $[K_۱ : K] = \deg p(x) \leq n$. حال $f_۱(x) \in K_۱[x]$ وجود دارد که $\deg f_۱(x) = n - ۱$ و $f(x) = (x - a_۱)f_۱(x)$. اکنون بنا به فرض استقرا، توسیع $F : K_۱$ وجود دارد که $f_۱(x)$ روی آن به عوامل خطی تجزیه می‌شود و $[F : K_۱] \leq (n - ۱)!$. بنابراین $f(x)$ روی F به عوامل خطی تجزیه می‌شود و بنا به قانون برج

$$[F : K] = [F : K_۱][K_۱ : K] \leq (n - ۱)!n = n!. \qquad \square$$

اکنون یک سوال مطرح می‌شود: کوچک‌ترین میدانی که $f(x) \in K[x]$ روی آن به عوامل خطی تجزیه شود چیست؟ چنین میدانی را میدان تجزیه‌ی $f(x)$ گوییم:

تعریف ۲.۲.۱۴. فرض کنید K میدان باشد و $f(x) \in K[x]$. توسیع $F : K$ را توسیع تجزیه‌ی $f(x)$ گوییم، هرگاه
(الف) $f(x)$ روی F به عوامل خطی تجزیه شود.
(ب) $f(x)$ روی هیچ زیرمیدان سره F به عوامل خطی تجزیه نشود.

فرض کنید $f(x) \in K[x]$ چندجمله‌ای غیرثابت با درجه‌ی n باشد. بنا به قضیه‌ی ۱.۲.۱۴، توسیع $F : K$ وجود دارد که $f(x)$ روی F به عوامل خطی تجزیه می‌شود. بنابراین $a_۱, a_۲, \ldots, a_n \in F$ و $k \in K$ وجود دارند که

$$f(x) = k(x - a_۱)(x - a_۲) \cdots (x - a_n).$$

$f(x)$ روی $K(a_۱, a_۲, \ldots, a_n)$ تجزیه می‌شود. ثابت می‌کنیم $K(a_۱, a_۲, \ldots, a_n) : K$ توسیع تجزیه‌ی $f(x)$ است. فرض کنید $K \subseteq L \subseteq K(a_۱, \ldots, a_n)$ و $f(x)$ روی میدان L تجزیه شود. چون $K[x]$، UFD است، فقط یک تجزیه به عوامل خطی روی L برای $f(x)$ داریم. بنابراین $a_۱, \ldots, a_n \in L$. در نتیجه $K(a_۱, a_۲, \ldots, a_n) : K$ توسیع تجزیه‌ی $f(x)$ است.

مثال ۳.۲.۱۴. چون $\pm i$ ریشه‌های $x^۲ + ۱$ هستند، $\mathbb{Q}(-i, i) = \mathbb{Q}(i)$ میدان تجزیه برای $x^۲ + ۱$ روی $\mathbb{Q}$ است. به همین نحو $\mathbb{R}(-i, i) = \mathbb{R}(i) = \mathbb{C}$ میدان تجزیه برای $x^۲ + ۱$ روی $\mathbb{R}$ است. $\square$

مثال ۴.۲.۱۴. توسیع تجزیه‌ی $f(x)=x^۴+۱\in\mathbb{Q}[x]$ را روی $\mathbb{Q}$ بیابید و درجه‌ی آن‌را مشخص کنید.

حل چندجمله‌ای $f(x)$ را به صورت زیر تجزیه می‌کنیم

$$\begin{aligned} f(x) &= x^۴+۱ \\ &= x^۴+۲x^۲-۲x^۲+۱ \\ &= (x^۲+۱)^۲-۲x^۲ \\ &= (x^۲-\sqrt{۲}x+۱)(x^۲+\sqrt{۲}x+۱). \end{aligned}$$

بنابراین ریشه‌های $f(x)$ عبارت‌اند از

$$\frac{-\sqrt{۲}\pm i\sqrt{۲}}{۲},\quad \frac{\sqrt{۲}\pm i\sqrt{۲}}{۲}.$$

از این‌رو $F=\mathbb{Q}\left(\frac{-\sqrt{۲}\pm i\sqrt{۲}}{۲},\frac{\sqrt{۲}\pm i\sqrt{۲}}{۲}\right)$ میدان تجزیه برای $f(x)$ روی $\mathbb{Q}$ است. ادعا می‌کنیم $F=\mathbb{Q}(i,\sqrt{۲})$. چون

$$\sqrt{۲}=\frac{\sqrt{۲}+i\sqrt{۲}}{۲}+\frac{\sqrt{۲}-i\sqrt{۲}}{۲}\in F$$
$$\sqrt{۲}i=\frac{\sqrt{۲}+i\sqrt{۲}}{۲}-\frac{\sqrt{۲}-i\sqrt{۲}}{۲}\in F$$

و $i=\frac{i\sqrt{۲}}{\sqrt{۲}}\in F$، داریم $\mathbb{Q}(i,\sqrt{۲})\subseteq F$. از طرفی به وضوح $F\subseteq\mathbb{Q}(i,\sqrt{۲})$. پس $F=\mathbb{Q}(i,\sqrt{۲})$. اکنون $x^۲-۲$ چندجمله‌ای می‌نیمال $\sqrt{۲}$ روی $\mathbb{Q}$ است. از این‌رو $[\mathbb{Q}(\sqrt{۲}):\mathbb{Q}]=۲$. از طرف دیگر $x^۲+۱$ روی $\mathbb{Q}(\sqrt{۲})$ ریشه ای ندارد. پس روی $\mathbb{Q}(\sqrt{۲})$ تحویل‌ناپذیر است و $[\mathbb{Q}(\sqrt{۲})(i):\mathbb{Q}(\sqrt{۲})]=۲$. اکنون بنا به قانون برج داریم

$$[\mathbb{Q}(i,\sqrt{۲}):\mathbb{Q}]=[\mathbb{Q}(i,\sqrt{۲}):\mathbb{Q}(\sqrt{۲})][\mathbb{Q}(\sqrt{۲}):\mathbb{Q}]=۲\times۲=۴. \qquad \square$$

مثال ۵.۲.۱۴. فرض کنید p عدد اول و a عدد گویای مثبت باشد که $\sqrt[p]{a}\notin\mathbb{Q}$. توسیع تجزیه‌ی $f(x)=x^p-a\in\mathbb{Q}[x]$ را روی $\mathbb{Q}$ بیابید و درجه‌ی آن‌را مشخص کنید.

حل فرض کنید $\omega=e^{\frac{۲i\pi}{p}}$. در این صورت ۱، ω، $\omega^۲$، ...، $\omega^{p-۱}$ همه‌ی ریشه‌های $x^p-۱$ هستند. فرض کنید b ریشه‌ای از $f(x)$ باشد. داریم

$$b^p=a\Longrightarrow\left(\frac{b}{\sqrt[p]{a}}\right)^p=۱\Longrightarrow\frac{b}{\sqrt[p]{a}}=۱,\ \omega,\ \omega^۲,\ \ldots,\ \omega^{p-۱}.$$

پس همه‌ی ریشه‌های $f(x)$ عبارت‌اند از

$$\sqrt[p]{a},\ \omega\sqrt[p]{a},\ \omega^۲\sqrt[p]{a},\ \ldots,\ \omega^{p-۱}\sqrt[p]{a}.$$

از این‌رو میدان تجزیه‌ی $f(x)$ عبارت است از

$$\mathbb{Q}(\sqrt[p]{a},\omega\sqrt[p]{a},\omega^۲\sqrt[p]{a},\ldots,\omega^{p-۱}\sqrt[p]{a})=\mathbb{Q}(\omega,\sqrt[p]{a}).$$

بنا به قانون برج و مثال ۱۳.۱.۱۴، داریم

$$[\mathbb{Q}(\omega,\sqrt[p]{a}):\mathbb{Q}]=[\mathbb{Q}(\omega,\sqrt[p]{a}):\mathbb{Q}(\omega)][\mathbb{Q}(\omega):\mathbb{Q}]=p(p-۱).$$

پس تنها باید ثابت کنیم $[\mathbb{Q}(\omega,\sqrt[p]{a}):\mathbb{Q}(\omega)]=p$. برای این کار ثابت می‌کنیم $f(x)$ روی $\mathbb{Q}(\omega)$ تحویل‌ناپذیر است؛ بنابراین چند جمله‌ای می‌نیمال $\sqrt[p]{a}$ روی $\mathbb{Q}(\omega)$ است. فرض کنید چنین نباشد و $f(x)$ روی $\mathbb{Q}(\omega)$ تحویل‌پذیر باشد. پس $g(x),h(x)\in\mathbb{Q}(\omega)[x]$،

با $0 < \deg g(x) = m < p$، وجود دارند که $f(x) = g(x)h(x)$. فرض کنید $b = \sqrt[p]{a}$ و b، bu_1، bu_2، ...، bu_{m-1} ریشه‌های $g(x)$ باشند، که در آن $u_j \in \{\omega, \omega^2, \ldots, \omega^{p-1}\}$، $j = 1, \ldots, m-1$، و u_jها متمایزند. حاصل‌ضرب این ریشه‌ها عبارت است از

$$d = g(0) = (-1)^m b^m u_1 u_2 \cdots u_{m-1} = (-1)^m b^m v, \qquad v^p = 1.$$

چون $m < p$ داریم ، $\gcd\{m, p\} = 1$. پس اعداد صحیح r و s وجود دارند که $rm + sp = 1$. در نتیجه

$$ba^{-s} = b(b^p)^{-s} = b^{1-sp} = b^{rm} = \left((-1)^m dv^{-1}\right)^r$$

یا $b = (-1)^{rm} d^r v^{-r} a^s$. بنابراین

$$a = b^p = \left((-1)^{rm} d^r v^{-r} a^s\right)^p = \left((-1)^{rm} d^r a^s\right)^p,$$

و $(-1)^{rm} d^r a^s \in \mathbb{Q}(\omega)$ ریشه‌ای از $f(x) = x^p - a$ است. در نتیجه اگر $x^p - a$ روی $\mathbb{Q}(\omega)$ تحویل‌پذیر باشد، آنگاه ریشه‌ای در $\mathbb{Q}(\omega)$ دارد. این تناقض است زیرا ریشه‌های $x^p - a$ عبارت‌اند از $b\omega^j$، $j = 0, 1, \ldots, p-1$، که هیچ‌کدام در $\mathbb{Q}(\omega)$ نیستند. □

اکنون می‌خواهیم یکتایی توسیع‌های تجزیه را بررسی کنیم. برای این کار به قدری مقدمه نیاز داریم. یادآوری می‌کنیم که اگر K و L میدان باشند و $\alpha : K \longrightarrow L$ همریختی حلقه‌ای نابدیهی باشد (یعنی هر عضو را به صفر تصویر نکند)، آنگاه چون $\ker \alpha$، ایدآلی از K است و K ایدآل نابدیهی ندارد ، $\ker \alpha = \{0\}$ و بنابراین α یک‌به‌یک است. پس α یک همریختی یک‌به‌یک $K[x]$ به $L[x]$ القا می‌کند که آن‌را نیز با $\alpha : K[x] \longrightarrow L[x]$ نشان می‌دهیم: به ازای هر $f(x) = k_0 + k_1 x + \cdots + k_n x^n \in K[x]$ تعریف می‌کنیم

$$\alpha(f(x)) = \alpha(k_0) + \alpha(k_1)x + \cdots + \alpha(k_n)x^n \in L[x].$$

توجه کنید که اگر $a \in K$، آنگاه

$$\begin{aligned} \alpha(f(x))(\alpha(a)) &= \sum_{j=0}^{n} \alpha(k_j)(\alpha(a))^j \\ &= \sum_{j=0}^{n} \alpha(k_j)\alpha(a^j) \\ &= \alpha\left(\sum_{j=0}^{n} k_j a^j\right) \\ &= \alpha(f(a)). \end{aligned}$$

بنابراین a ریشه‌ای از $f(x)$ است اگر و تنها اگر $\alpha(a)$ ریشه‌ای از $\alpha(f(x))$ باشد. هم‌چنین واضح است که اگر $\alpha : K \longrightarrow L$ یکریختی باشد، آنگاه $\alpha : K[x] \longrightarrow L[x]$ نیز یکریختی است. در این حالت ، $p(x) \in K[x]$ روی $K[x]$ تحویل‌ناپذیر است اگر و تنها اگر $\alpha(p(x)) \in L[x]$ روی $L[x]$ تحویل‌ناپذیر باشد.

قضیه‌ی بعد یکی از قضیه‌های مهم و اساسی نظریه‌ی گالوا و در واقع نقطه‌ی شروع نظریه‌ی گالوا است. از این قضیه برای اثبات بسیاری از قضیه‌های دیگر استفاده می‌کنیم. یکی از این قضایا یکتایی توسیع‌های تجزیه است، که در ادامه آن را ثابت می‌کنیم.

قضیه ۶.۲.۱۴. فرض کنید $F : K$ توسیع و $a \in F$ روی K جبری با چندجمله‌ای می‌نیمال $p(x)$ باشد. اگر $E : L$ یک توسیع و $\alpha : K \longrightarrow L$ یکریختی و $b \in E$ ریشه‌ای از $\alpha(p(x))$ باشند، آنگاه یکریختی یکتای $\beta : K(a) \longrightarrow L(b)$ با $\beta(a) = b$ وجود دارد که $\beta|_K = \alpha$، یعنی برای هر $k \in K$، $\beta(k) = \alpha(k)$.

اثبات. چون $p(x)$ روی K تحویل‌ناپذیر و $\alpha : K \longrightarrow L$ یکریختی است، چندجمله‌ای $q(x) = \alpha(p(x))$ روی $L[x]$ تحویل‌ناپذیر و تکین است. از طرف دیگر b ریشه‌ی $q(x)$ است. پس $q(x)$ چندجمله‌ای می‌نیمال b روی $L[x]$ است. به علاوه چون a روی K جبری

است، $K(a) = K[a]$. فرض کنید $M = (p(x))$ و $N = (q(x))$. توجه کنید اگر $\varphi_a : K[x] \longrightarrow K(a)$ همریختی مقدارياب باشد، آنگاه بنا به قضیه‌ی اول یکریختی، تابع

$$\begin{aligned}&\bar{\varphi}_a : \frac{K[x]}{M} \longrightarrow K(a)\\ &\bar{\varphi}_a(f(x)+M) = \varphi_a(f(x)) = f(a),\end{aligned}$$

یکریختی است. اکنون نشان می‌دهیم که تابع

$$\begin{aligned}&\alpha^* : \frac{K[x]}{M} \longrightarrow \frac{L[x]}{N}\\ &\alpha^*(f(x)+M) = \alpha(f(x)) + N,\end{aligned}$$

یکریختی است. α^* خوش تعریف و یک‌به‌یک است، زیرا

$$\begin{aligned}f(x)+M = g(x)+M &\iff f(x)-g(x) \in M = (p(x))\\ &\iff \alpha(f(x)-g(x)) \in \alpha(M) = N\\ &\iff \alpha(f(x)) - \alpha(g(x)) \in N\\ &\iff \alpha(f(x)) + N = \alpha(g(x)) + N\\ &\iff \alpha^*(f(x)+M) = \alpha^*(g(x)+M).\end{aligned}$$

همریختی و پوشا بودن α^* به سادگی از این که α یکریختی است، ثابت می‌شود. اکنون قرار می‌دهیم $\beta = \bar{\varphi}_b \circ \alpha^* \circ \bar{\varphi}_a^{-1}$ در این صورت $\beta : K(a) \longrightarrow L(b)$ یکریختی است، زیرا ترکیب همریختی‌های یک‌به‌یک و پوشاست.

$$\begin{array}{ccc}\dfrac{K[x]}{M} & \xrightarrow{\quad\alpha^*\quad} & \dfrac{L[x]}{N}\\ \Big\downarrow{\scriptstyle \bar{\varphi}_a} & & \Big\downarrow{\scriptstyle \bar{\varphi}_b}\\ K(a) & \overset{\beta}{\dashrightarrow} & L(b)\end{array}$$

داریم

$$\begin{aligned}\beta(a) &= (\bar{\varphi}_b \circ \alpha^* \circ \bar{\varphi}_a^{-1})(a)\\ &= (\bar{\varphi}_b \circ \alpha^*)(x+M)\\ &= \bar{\varphi}_b(\alpha(x)+N)\\ &= \bar{\varphi}_b(x+N)\\ &= b.\end{aligned}$$

بنابراین یکریختی $\beta : K(a) \longrightarrow L(b)$ وجود دارد که $\beta(a) = b$. نشان می‌دهیم β یکتاست. فرض کنید $\beta' : K(a) \longrightarrow L(b)$ یکریختی باشد و $\beta'(a) = b$. قرار می‌دهیم $T = \{c \in K(a) \mid \beta(c) = \beta'(c)\}$. به سادگی می‌توان دید که T زیرمیدانی از $K(a)$ شامل K و a است، پس $T = K(a)$. بنابراین $\beta = \beta'$. □

قضیه ۷.۲.۱۴. فرض کنید $f(x) \in K[x]$ و $\alpha : K \longrightarrow L$ یکریختی باشد. اگر $F : K$ توسیع تجزیه‌ی $f(x)$ و $E : L$ توسیع تجزیه‌ی $\alpha(f(x))$ باشند، آنگاه یکریختی $\beta : F \longrightarrow E$ وجود دارد که $\beta|_K = \alpha$.

اثبات. به استقرا روی $n = \deg f(x)$ عمل می‌کنیم. اگر $n = ۱$، آنگاه $F = K$ و $\beta : F \longrightarrow E$ را با $\beta(k) = \alpha(k)$. تعریف می‌کنیم. اکنون فرض کنید قضیه برای همه‌ی چندجمله‌ای‌های با درجه‌ی کمتر از n برقرار باشد. فرض کنید $a_۱, a_۲, \ldots, a_n \in F$، ریشه‌های $f(x)$ باشند. چون $a_۱ \in F$ ریشه‌ای از $f(x)$ است، $a_۱$ روی K جبری است. فرض کنید $p(x)$ چندجمله‌ای می‌نیمال $a_۱$ روی K باشد. پس در $K[x]$، $p(x)|f(x)$. فرض کنید $b_۱$ ریشه‌ای از $\alpha(p(x))$ در E باشد. اکنون بنا به قضیه‌ی ۶.۲.۱۴، یکریختی یکتای $\beta_۱ : K(a_۱) \longrightarrow L(b_۱)$ وجود دارد که $\beta_۱(a_۱) = b_۱$ و $\beta_۱$ توسیع α است. چون $f(x) \in K[x] \subseteq K(a_۱)[x]$، چند جمله‌ای $h(x) \in K(a_۱)[x]$ وجود دارد که روی F تجزیه می‌شود و $f(x) = (x - a_۱)h(x)$. به علاوه چون $F = K(a_۱)(a_۲, \ldots, a_n)$، F توسیع تجزیه‌ی $h(x)$ روی $K(a_۱)$ است. از طرف دیگر داریم

$$\alpha(f(x)) = \beta_۱(f(x)) = (x - \beta_۱(a_۱))\beta_۱(h(x)) = (x - b_۱)\beta_۱(h(x)).$$

بنابراین E توسیع تجزیه‌ی $\beta_۱(h(x))$ روی $L(b_۱)$ است. پس بنا به فرض استقرا، یکریختی $\beta : F \longrightarrow E$ وجود دارد که توسیع $\beta_۱$ و بنابراین توسیع α است. □

نتیجه ۸.۲.۱۴. اگر $f(x) \in K[x]$، آنگاه هر دو توسیع تجزیه‌ی $f(x)$ یکریخت هستند.

اثبات. فرض کنید $F : K$ و $E : K$ دو توسیع تجزیه برای $f(x)$ باشند. اگر در قضیه‌ی ۷.۲.۱۴، قرار دهیم $\alpha = \mathrm{id}_K$، یکریختی، $\beta : F \longrightarrow E$ را به دست می‌آوریم، که حکم را ثابت می‌کند. □

این بخش را با اثبات یک محک برای تشخیص تکراری بودن ریشه‌های یک چندجمله‌ای به پایان می‌بریم؛ و آن استفاده از مفهوم مشتق است. فرض کنید K یک میدان باشد و $f(x) = k_۰ + k_۱x + \cdots + k_nx^n \in K[x]$. مشتق (صوری) $f(x)$ را به صورت زیر تعریف می‌کنیم:

$$f'(x) = k_۱ + \cdots + jk_jx^{j-۱} + \cdots + nk_nx^{n-۱} \in K[x].$$

به سادگی می‌توان دید

$$\begin{aligned} (f(x) + g(x))' &= f'(x) + g'(x) \\ (f(x)g(x))' &= f'(x)g(x) + f(x)g'(x). \end{aligned}$$

فرض کنید F میدان باشد و $f(x) \in F[x]$. اگر $a \in F$ ریشه‌ای از $f(x)$ باشد، a را ریشه‌ی تکراری $f(x)$ گوییم، هرگاه $m > ۱$ وجود داشته باشد که $(x - a)^m | f(x)$، در $F[x]$، یعنی $g(x) \in F[x]$ وجود داشته باشد که $f(x) = (x - a)^m g(x)$.

قضیه ۹.۲.۱۴. اگر F میدان و $f(x) \in F[x]$ چندجمله‌ای ناصفر باشد، آنگاه $a \in F$ ریشه‌ی تکراری $f(x)$ است اگر و تنها اگر $f(a) = f'(a) = ۰$ (یعنی $x - a$ هم $f(x)$ و هم $f'(x)$ را عاد کند).

اثبات. ($\Longleftarrow$) فرض کنید $m > ۱$ و $f(x) = (x - a)^m g(x)$، که در آن $g(x) \in F[x]$. بنابراین داریم

$$f'(x) = m(x - a)^{m-۱}g(x) + (x - a)^m g'(x),$$

و $f(a) = f'(a) = ۰$.

($\Longrightarrow$) چون $f(a) = ۰$، $h(x) \in F[x]$ وجود دارد که $f(x) = (x - a)h(x)$. پس ، با مشتق‌گیری از طرفین تساوی، داریم $f'(x) = h(x) + (x - a)h'(x)$. چون $f'(a) = ۰$ داریم $h(a) = ۰$. از این‌رو $g(x) \in F[x]$ وجود دارد که $h(x) = (x - a)g(x)$. بنابراین $f(x) = (x - a)^۲ g(x)$ و a ریشه‌ی تکراری $f(x)$ است. □

تمرین‌ها

۱. در هر یک از حالت‌های زیر توسیع تجزیه‌ی $f(x) \in \mathbb{Q}[x]$ روی $\mathbb{Q}$ را بیابید و درجه‌ی آن را مشخص کنید.
(الف) ۱ $f(x) = x^3 + 1$ (ب) ۱ $f(x) = x^6 + x^3 + 1$
(ج) ۱ $f(x) = x^4 + x^2 + 1$ (د) ۳ $f(x) = x^6 + 2x^3 - 3$
(هـ) ۱۰ $f(x) = x^4 - 7x^2 + 10$ (و) ۷ $f(x) = x^4 - 6x^2 - 7$
(ز) ۶ $f(x) = x^4 - 5x^2 + 6$ (ح) ۱ $f(x) = x^6 - 1$
(ط) ۱ $f(x) = x^6 + 1$ (ی) ۵ $f(x) = x^4 - 5$ (ک) ۴ $f(x) = x^4 + 4$

۲. در هر حالت توسیع تجزیه‌ی $f(x) \in K[x]$ را بیابید.
(الف) $f(x) = x^2 + x + 1 \in \mathbb{Z}_2[x]$ (ب) $f(x) = x^3 + 1 \in \mathbb{Z}_3[x]$
(ج) $f(x) = x^3 + x^2 + 1 \in \mathbb{Z}_2[x]$ (د) $f(x) = x^2 + x + 1 \in \mathbb{Z}_5[x]$

۳. فرض کنید K میدان، $a \in K$، و p عدد اول باشد. ثابت کنید $x^p - a \in K[x]$ روی K تحویل‌ناپذیر است اگر و تنها اگر در K ریشه‌ای نداشته باشد.

۴. فرض کنید $f(x), g(x) \in K[x]$. نشان دهید $f(x)$ و $g(x)$ در $K[x]$ نسبت به هم اول‌اند اگر و تنها اگر ریشه‌ی مشترکی در هیچ توسیع $F : K$ نداشته باشد.

۵. فرض کنید $f(x), g(x) \in K[x]$. نشان دهید توسیع تجزیه‌ی $f(x)g(x)$ شامل توسیع‌های تجزیه‌ی $f(x)$ و $g(x)$ است.

۶. فرض کنید K یک میدان با مشخصه‌ی عدد اول p باشد و $a \in K$. ثابت کنید $x^p - x - a$ روی K تحویل‌ناپذیر است اگر و تنها اگر در K ریشه نداشته باشد.

۷. فرض کنید $f(x) \in K[x]$ چندجمله‌ای غیر ثابت باشد. نشان دهید $f(x)$ در هیچ توسیع تجزیه، ریشه‌ی تکراری ندارد اگر و تنها اگر $f(x)$ و $f'(x)$ نسبت به هم در $K[x]$ اول باشند.

۸. فرض کنید $f(x) = x^n - x \in K[x]$، که در آن $n \geq 2$. اگر $\operatorname{char} K = 0$ یا $\operatorname{char} K = p$ و $p \nmid n$. نشان دهید $f(x)$ در هر توسیع تجزیه ریشه‌ی تکراری ندارد.

۹. فرض کنید $\operatorname{char} F = p$ و F شامل n ریشه‌ی متمایز nام واحد باشد (ریشه‌های چندجمله‌ای $x^n - 1 \in F[x]$ را ریشه‌های nام واحد می‌نامیم). نشان دهید $p \nmid n$.

۱۰. فرض کنید $\operatorname{char} K = p > 0$. اگر $f(x) = x^p - a \in K[x]$، نشان دهید یا $f(x)$ روی K تحویل‌ناپذیر است یا توانی از یک چندجمله‌ای خطی است.

۳.۱۴ میدان‌های متناهی

در این بخش به طور مختصر میدانهای متناهی و برخی از خواص اساسی آن‌ها را بررسی می‌کنیم. میدان‌های متناهی کاربردهای زیادی دارند که یکی از کاربرد آن‌ها را در نظریه‌ی جبری کد گذاری در فصل بعد ارائه می‌کنیم. فرض کنید F میدان متناهی است. چون F متناهی است، عدد اول p وجود دارد که $\operatorname{char} F = p$. بنابراین زیرمیدانی یکریخت با $\mathbb{Z}_p$ دارد. با یکی گرفتن این زیرمیدان با $\mathbb{Z}_p$ فرض می‌کنیم $\mathbb{Z}_p \subseteq F$. پس $\mathbb{Z}_p : F$ توسیع است. برای شروع کار نشان می‌دهیم مرتبه‌ی هر میدان متناهی توانی از یک عدد اول است:

قضیه ۱.۳.۱۴. اگر F میدان متناهی باشد، آنگاه عدد صحیح $n > 1$ وجود دارد که $|F| = p^n$، که در آن $\operatorname{char} F = p$.

اثبات. چون F متناهی است، $\mathbb{Z}_p : F$ توسیع متناهی است، مثلاً $n = [F : \mathbb{Z}_p]$، یعنی F یک فضای برداری با بُعد n روی $\mathbb{Z}_p$ است. بنابراین بنا به نتیجه ۹.۴.۱۳، داریم $F \cong \underbrace{\mathbb{Z}_p \oplus \cdots \oplus \mathbb{Z}_p}_{n \text{ بار}}$. به ویژه $|F| = |\mathbb{Z}_p|^n = p^n$. □

در قضیه‌ی ۱.۳.۱۴، دیدیم که اگر F میدان متناهی با $\operatorname{char} F = p$ باشد، آنگاه ، به ازای یک عدد صحیح مثبت n، $|F| = p^n$. حال

سوال این است که آیا به ازای هر عدد اول p، و هر عدد صحیح $n \geq ۱$، میدانی با p^n عضو وجود دارد؟ در ادامه ثابت می‌کنیم که به ازای هر عدد اول p، و هر عدد صحیح $n \geq ۱$، میدانی یکتا با p^n عضو وجود دارد. اگر $f(x) \in \mathbb{Z}_p[x]$ چندجمله‌ای تحویل‌ناپذیر روی $\mathbb{Z}_p$ باشد، آنگاه بنا به قضیه‌های ۲.۴.۱۱، ۳.۴.۱۱، و ۵.۴.۱۱، $\dfrac{\mathbb{Z}_p[x]}{(f(x))}$ میدانی با p^n عضو است. برای ساختن یک میدان p^n عضوی یافتن یک چندجمله‌ای تحویل‌ناپذیر با درجه‌ی n روی $\mathbb{Z}_p$ کار ساده‌ای نیست. بنابراین روش دیگری را باید در نظر بگیریم. در قضیه‌ی بعد ثابت می‌کنیم هر میدان p^n عضوی توسیع تجزیه‌ی چندجمله‌ای $x^{p^n} - x$ روی $\mathbb{Z}_p$ است.

قضیه ۲.۳.۱۴. فرض کنید F میدان و $|F| = p^n$، که در آن $\operatorname{char} F = p$، و $n \geq ۱$ عدد صحیح باشد. آنگاه هر عضو F ریشه‌ی چندجمله‌ای $f(x) = x^{p^n} - x \in \mathbb{Z}_p[x]$ است. به علاوه $F : \mathbb{Z}_p$ توسیع تجزیه‌ی $x^{p^n} - x$ روی $\mathbb{Z}_p$ است.

اثبات. چون $F^\times$ گروه ضربی با $p^n - ۱$ عضو است، بنا به قضیه‌ی لاگرانژ، به ازای هر $۰ \neq a \in F$، داریم $a^{p^n - ۱} = ۱$. بنابراین به ازای هر $a \in F$، داریم $a^{p^n} = a$. در نتیجه هر عضو F ریشه‌ای از چندجمله‌ای $f(x) = x^{p^n} - x \in \mathbb{Z}_p[x]$ است. چون $f'(x) = -۱ \neq ۰$، و $\deg f(x) = p^n$، دقیقاً p^n ریشه‌ی متمایز برای $f(x)$ داریم که همگی در F قرار دارند. پس $f(x)$ روی F تجزیه می‌شود و روی هیچ زیرمیدان سره F تجزیه نمی‌شود. بنابراین F توسیع تجزیه‌ی $f(x)$ روی $\mathbb{Z}_p$ است. □

چون هر دو توسیع تجزیه‌ی یک چندجمله‌ای یکریخت هستند ، میدان‌های متناهی با تعداد اعضای مساوی یکریخت هستند :

نتیجه ۳.۳.۱۴. هر دو میدان متناهی با p^n عضو یکریخت هستند ، که در آن p عدد اول ، و $n \geq ۱$ عدد صحیح است. □

اکنون با توجه به بحث کشاف بالا معلوم است که برای ساختن میدان p^n عضوی باید توسیع تجزیه‌ی $f(x) = x^{p^n} - x$ روی $\mathbb{Z}_p$ را در نظر بگیریم :

قضیه ۴.۳.۱۴. فرض کنید p عدد اول و $n \geq ۱$ عدد صحیح باشد. در این صورت توسیع تجزیه‌ی چندجمله‌ای $f(x) = x^{p^n} - x \in \mathbb{Z}_p[x]$ یک میدان p^n عضوی است.

اثبات. فرض کنید $F : \mathbb{Z}_p$ توسیع تجزیه‌ی $f(x) = x^{p^n} - x$ روی $\mathbb{Z}_p$ باشد. چون $f'(x) = -۱ \neq ۰$، بنا به قضیه‌ی ۹.۲.۱۴، ریشه‌های $f(x)$ متمایزند. چون $f(x)$ روی F تجزیه می‌شود و $\deg f(x) = p^n$، p^n ریشه‌ی متمایز در F برای $f(x)$ داریم. فرض کنید $T = \{a \in F \mid f(a) = ۰\}$ مجموعه‌ی همه‌ی ریشه‌های $f(x)$ در F باشد. پس $|T| = p^n$. نشان می‌دهیم T زیرمیدان F است. فرض کنید $a, b \in T$. بنابراین $a^{p^n} = a$ و $b^{p^n} = b$. چون $\operatorname{char} F = p$ و p، به ازای هر $j = ۱, ۲, \ldots, p^n - ۱$، عبارت $\binom{p^n}{j}$ را عاد می‌کند، داریم

$$\begin{aligned}(a+b)^{p^n} &= a^{p^n} + \binom{p^n}{۱} a^{p^n-۱}b + \cdots + \binom{p^n}{p^n-۱} ab^{p^n-۱} + b^{p^n} \\ &= a^{p^n} + b^{p^n} \\ &= a + b\end{aligned}$$

و $a + b \in T$. به علاوه $(-b)^{p^n} = (-۱)^{p^n} b^{p^n} = (-۱)^{p^n} b = -b$ (توجه کنید که اگر $p > ۲$، آنگاه $(-۱)^{p^n} b = -b$، و اگر $p = ۲$، آنگاه $-b = b = (-۱)^{p^n} b$). بنابراین $-b \in T$. اکنون اگر $b \neq ۰$، داریم

$$\left(ab^{-۱}\right)^{p^n} = a^{p^n} \left(b^{p^n}\right)^{-۱} = ab^{-۱}.$$

بنابراین $ab^{-۱} \in T$. از این‌رو T زیرمیدان F است. T زیرمیدانی از F شامل همه‌ی ریشه‌های $f(x)$ است. چون $F : \mathbb{Z}_p$ توسیع تجزیه‌ی $f(x)$ است، $F = T$. در نتیجه $|F| = |T| = p^n$. □

اگر p عدد اول و $n \geq ۱$ عدد صحیح باشد، میدان یکتای p^n عضوی را میدان گالوا از مرتبه‌ی p^n گوییم و با $\mathrm{GF}(p^n)$ نشان می‌دهیم. بنابراین $\mathrm{GF}(p) = \mathbb{Z}_p$. توجه کنید اگر زیرمیدان اول $\mathrm{GF}(p^n)$ را ، که با $\mathbb{Z}_p$ یکریخت است، با $\mathbb{Z}_p$ یکی در نظر بگیریم ، آنگاه $\mathrm{GF}(p^n) : \mathbb{Z}_p$ یک توسیع است. اگر $m = [\mathrm{GF}(p^n) : \mathbb{Z}_p]$، آنگاه چون $\mathrm{GF}(p^n)$ با m کپی از $\mathbb{Z}_p$ یکریخت است، داریم $p^n = p^m$. بنابراین $n = m$ و $[\mathrm{GF}(p^n) : \mathbb{Z}_p] = n$.

فرض کنید F میدان متناهی است. می‌دانیم $F^\times$ گروه دوری است (قضیه‌ی ۱۵.۱.۱۱ از صفحه‌ی ۲۳۶). هر مولد گروه ضربی $F^\times$ را یک عضو اولیه از F گوییم.
فرض کنید $F : K$ توسیع تجزیه‌ی چندجمله‌ای $f(x) = x^n - ۱ \in K[x]$ باشد. چون $F^\times$ یک گروه آبلی است، مجموعه‌ی متشکل از همه‌ی ریشه‌های $f(x)$ در F، یعنی

$$G = \{a \in F^\times \mid a^n = ۱\}$$

یک زیرگروه $F^\times$ است. چون $f(x) = x^n - ۱ \in K[x]$ حداکثر n ریشه در F دارد ، G گروه متناهی است. در نتیجه بنا به قضیه‌ی ۱۵.۱.۱۱، از صفحه‌ی ۲۳۶، G دوری است. هر عضو G را یک ریشه‌ی nام واحد و هر مولد G با مرتبه‌ی n را یک ریشه‌ی nام اولیه‌ی واحد روی K گوییم.

مثال ۵.۳.۱۴. عناصر $\mathrm{GF}(۹)$ را توصیف کنید.

حل ابتدا یک چندجمله‌ای تحویل‌ناپذیر دلخواه درجه‌ی ۲ روی $\mathbb{Z}_۳$ اختیار می‌کنیم، مثلاً $x^۲ + ۱$. فرض کنید a ریشه‌ای از این چندجمله‌ای باشد، پس در $\mathrm{GF}(۹)$ داریم ، $a^۲ + ۱ = ۰$. می‌توان نوشت $\mathrm{GF}(۹) = \{r + sa \mid r, s \in \mathbb{Z}_۳\}$. طریق دیگر توصیف عناصر $\mathrm{GF}(۹)$ این است که یک عضو اولیه‌ی دلخواه ξ روی آن در نظر بگیریم. در این صورت $\mathrm{GF}(۹) = \{۰, ۱, \xi, \xi^۲, \ldots, \xi^۷\}$ و ξ یک ریشه‌ی اولیه‌ی هشتم واحد روی $\mathbb{Z}_۳$ است. توجه کنید، با امتحان $r + sa$، می‌بینیم که $a + ۱$ عضو اولیه‌ای از $\mathrm{GF}(۹)$ است؛ پس قرار می‌دهیم $\xi = ۱ + a$. به سادگی می‌توان دید $\xi^۲ + \xi - ۱ = ۰$؛ بنابراین چندجمله‌ای می‌نیمال ξ روی $\mathbb{Z}_۳$ برابر $x^۲ + x - ۱$ است. عناصر ناصفر $\mathrm{GF}(۹)$ را می‌توان در جدول زیر

i	۰	۱	۲	۳	۴	۵	۶	۷
ξ^i	۱	$۱ + a$	$۲a$	$۱ + ۲a$	۲	$۲ + ۲a$	a	$۲ + a$

که به جدول لگاریتم گسسته موسوم است، نشان داد. □

به طور کلی اگر $\mathrm{GF}(q) = \{۰, ۱, \xi, \xi^۲, \ldots, \xi^{q-۲}\}$، و $a \in \mathrm{GF}(q)$ طوری باشد که، به ازای یک $۰ \le i \le q - ۲$، $a = \xi^i$، آنگاه i را لگاریتم گسسته‌ی a گوییم و با $i = \log_\xi(a)$ نشان می‌دهیم. لگاریتم گسسته خواص زیر را دارد :

$$\log_\xi(ab) \equiv \log_\xi(a) + \log_\xi(b) \mod q - ۱$$
$$\log_\xi(ab^{-۱}) \equiv \log_\xi(a) - \log_\xi(b) \mod q - ۱.$$

تابع وارون لگاریتم گسسته، ضد لگاریتم است و i را به ξ^i تصویر می‌کند.
زیرگروه‌های یک گروه دوری را در فصل ۳ کاملاً توصیف کرده‌ایم. در واقع اگر G گروه دوری مرتبه‌ی n باشد، آنگاه G زیرگروهی از مرتبه‌ی m دارد اگر و تنها اگر $m|n$، و در این حالت زیرگروه مرتبه‌ی m یکتاست. اما مساله‌ی توصیف همه‌ی زیرگروه‌های یک گروه، حتی اگر آبلی باشد، بسیار مشکل است. در مورد میدان‌های متناهی مساله راحت‌تر است و می‌توان همه‌ی زیرمیدان‌های یک میدان متناهی را توصیف کرد. این کار را در قضیه‌ی بعد انجام می‌دهیم.

قضیه ۶.۳.۱۴. فرض کنید p یک عدد اول و $n \ge ۱$ عدد صحیح باشد.
(الف) اگر K زیرمیدانی از $\mathrm{GF}(p^n)$ باشد، آنگاه عدد صحیح مثبت m وجود دارد که $m|n$ و $K \cong \mathrm{GF}(p^m)$.
(ب) اگر $m|n$، دقیقاً یک زیرمیدان $\mathrm{GF}(p^n)$ از مرتبه‌ی p^m وجود دارد. این زیرمیدان متشکل از همه‌ی ریشه‌های $x^{p^m} - x$ در $\mathrm{GF}(p^n)$ است.

اثبات. (الف) قرار می‌دهیم $F = \mathrm{GF}(p^n)$. چون K زیرمیدان F است، $\mathrm{char}\, K = p$. پس با توجه به قضیه‌ی ۴.۳.۱۴، به ازای یک $m \le n$، داریم $K \cong \mathrm{GF}(p^m)$. بنا به قانون برج داریم

$$n = [F : \mathbb{Z}_p] = [F : K][K : \mathbb{Z}_p] = [F : K]m.$$

بنابراین $m|n$.

(ب) چون $m|n$، عدد صحیح مثبت k وجود دارد که $n = mk$. بنابراین

$$p^n - ۱ = p^{mk} - ۱ = (p^m - ۱)(p^{mk-m} + p^{mk-۲m} + \cdots + p^k + ۱) = (p^m - ۱)r.$$

در نتیجه، با فرض $p^m - ۱ = t$ داریم

$$\begin{aligned} x^{p^n} - x &= x(x^{p^n - ۱} - ۱) \\ &= x(x^{tr} - ۱) \\ &= x(x^t - ۱)(x^{tr-t} + x^{tr-۲t} + \cdots + x^r + ۱) \\ &= x(x^{p^m - ۱} - ۱)g(x) \\ &= (x^{p^m} - x)g(x). \end{aligned}$$

بنابراین همه‌ی ریشه‌های چندجمله‌ای $x^{p^m} - x$ نیز در F قرار دارند. فرض کنید T زیرمجموعه‌ی F متشکل از همه‌ی ریشه‌های $x^{p^m} - x$ باشد ؛ بنا به اثبات قضیه‌ی ۴.۳.۱۴،یک زیرمیدان p^m عضوی F است. حال فرض کنید K زیرمیدان دلخواهی از F باشد و $|K| = p^m$. بنا به قضیه‌ی ۲.۳.۱۴، هر عضو K ریشه‌ی $x^{p^m} - x$ است. بنابراین $K \subseteq T$. چون $|K| = |T| = p^m$، داریم $K = T$. □

فرض کنید F یک میدان متناهی باشد. اگر $a \in F^\times$ عضو اولیه‌ای از F باشد، آنگاه $F = \mathbb{Z}_p(a)$، که در آن طبق معمول $\mathbb{Z}_p$ را با زیرمیدان یکریخت آن در F یکی گرفته‌ایم. بنابراین اگر a عضو اولیه‌ای از $\mathrm{GF}(p^n)$ باشد، آنگاه $\mathrm{GF}(p^n) = \mathbb{Z}_p(a)$. حال اگر $f(x)$ چندجمله‌ای می‌نیمال a روی $\mathbb{Z}_p$ باشد، آنگاه $f(x)$ روی $\mathbb{Z}_p$ تحویل‌ناپذیر است و

$$\deg f(x) = [\mathbb{Z}_p(a) : \mathbb{Z}_p] = [F : \mathbb{Z}_p] = n.$$

بنابراین به ازای هر عدد صحیح $n \geq ۱$ و هر عدد اول p چندجمله‌ای تحویل‌ناپذیر با درجه‌ی n روی $\mathbb{Z}_p$ وجود دارد.

فرض کنید K زیرمیدانی از $F = \mathrm{GF}(p^n)$ و a مولدی از گروه ضربی $F^\times$ باشد. پس $F^\times = \langle a \rangle$ و $O(a) = p^n - ۱$. چون $K^\times$ زیرگروه گروه دوری $F^\times$ است، دوری است و عدد صحیح مثبت d وجود دارد که $d|p^n - ۱$ و $K^\times = \langle a^d \rangle$. به علاوه $K^\times$ یکتا زیرگروه $F^\times$ از مرتبه‌ی $|K^\times|$ است. هم‌چنین چون $|K| = p^m$، که در آن $m|n$ (قضیه‌ی ۶.۳.۱۴)، داریم $p^m - ۱ = |K^\times| = \dfrac{|F^\times|}{d}$. پس $d = \dfrac{p^n - ۱}{p^m - ۱}$، $(m|n)$ و $K = \{۰\} \cup \langle a^d \rangle$. بنابراین زیرمیدان‌هایی F را برحسب شمارندهای m از n و عناصر اولیه‌ی a از F کاملاً توصیف کرده‌ایم.

از این جا تا آخر این بخش فرض می‌کنیم p یک عدد اول و q توانی از یک عدد اول است. فرض کنید $f(x)$ یک چندجمله‌ای تحویل‌ناپذیر با درجه‌ی k روی $F = \mathrm{GF}(q)$ باشد. اگر a ریشه‌ای از $f(x)$ در توسیعی از F باشد، آنگاه $[F(a) : F] = \deg f(x) = k$. از طرف دیگر $[GF(q^k) : F] = k$، پس $F(a) = \mathrm{GF}(q^k)$. بنابراین $a \in \mathrm{GF}(q^k)$، $a = a^{q^k}$، و a در چندجمله‌ای $g(x) = x^{q^k} - x$ صدق می‌کند. پس $f(x)|g(x)$ و ریشه‌های $f(x)$ همگی در $\mathrm{GF}(q^k)$ قرار دارند. از طرف دیگر چون $f(a^{q^j}) = f(a)^{q^j} = ۰$، اعضای a، a^q، $a^{q^۲}$، ...، $a^{q^{k-۱}}$، دقیقاً k ریشه‌ی $f(x)$ در $\mathrm{GF}(q^k)$ هستند ، و $\mathrm{GF}(q^k)$ توسیع تجزیه‌ی $f(x)$ روی $\mathrm{GF}(q)$ است. ریشه‌های a، a^q، $a^{q^۲}$، ...، $a^{q^{k-۱}}$، از $f(x)$ را مزدوجها a نسبت به $\mathrm{GF}(q)$ می‌نامیم. توجه کنید که این ریشه‌ها متمایزند؛ زیرا اگر $a^{q^n} = a^{q^m}$، که در آن $۰ \leq n < m \leq k - ۱$، آنگاه

$$a = a^{q^k} = (a^{q^n})^{q^{k-n}} = (a^{q^m})^{q^{k-n}} = a^{q^{k+m-n}}.$$

در نتیجه $a \in \mathrm{GF}(q^{k+m-n})$ و با استفاده از قانون برج نتیجه می‌شود که $k = [F(a) : F]$، $k + m - n = [\mathrm{GF}(q^{k+m-n}) : F]$ را عاد می‌کند، این تناقض است. بنابراین:

قضیه ۷.۳.۱۴. اگر $f(x)$ یک چندجمله‌ای تحویل‌ناپذیر با درجه‌ی k روی $\mathrm{GF}(q)$ باشد، آنگاه $\mathrm{GF}(q^k)$ توسیع تجزیه‌ی $f(x)$ روی $\mathrm{GF}(q)$ است و

$$f(x) = (x-a)(x-a^q)(x-a^{q^2})\cdots(x-a^{q^{k-1}}),$$

که در آن $a \in \mathrm{GF}(q^k)$ ریشه‌ی دلخواهی از $f(x)$ است. □

قضیه ۸.۳.۱۴. اگر $f(x)$ چندجمله‌ای تحویل‌ناپذیر روی $\mathrm{GF}(q)$ از درجه‌ی k باشد، آنگاه $f(x)|x^{q^n}-x$ اگر و تنها اگر $k|n$.

اثبات. ($\Longleftarrow$) چون $f(x)|x^{q^n}-x$، ریشه‌های $f(x)$ همگی در $\mathrm{GF}(q^n)$ قرار دارند. بنابراین میدان تجزیه‌ی آن ، یعنی $\mathrm{GF}(q^k)$، باید در $\mathrm{GF}(q^n)$ قرار داشته باشد. پس $k|n$ (بنا به قضیه‌ی ۶.۳.۱۴).
($\Longrightarrow$) چون $k|n$، $\mathrm{GF}(q^k)$ زیرمیدان $\mathrm{GF}(q^n)$ است. چون $f(x)$ و $x^{q^n}-x$ به عوامل خطی روی $\mathrm{GF}(q^n)$ تجزیه می‌شوند، و همه‌ی عناصر $\mathrm{GF}(q^n)$ ریشه‌های $x^{q^n}-x$ هستند ، $f(x)|x^{q^n}-x$. □

بنا به قضیه‌ی ۹.۲.۱۴، ریشه‌های $x^{q^n}-x \in \mathrm{GF}(q)[x]$ متمایزند (در واقع، بنا به قضیه‌ی ۲.۳.۱۴، q^n ریشه‌ی آن دقیقاً اعضای $\mathrm{GF}(q^n)$ هستند). بنا به قضیه‌ی ۸.۳.۱۴ (یا ۷.۳.۱۴) این مطلب برای هر چندجمله‌ای تحویل‌ناپذیر در $\mathrm{GF}(q)[x]$ برقرار است؛ یعنی ریشه‌های هر چندجمله‌ای تحویل‌ناپذیر روی $\mathrm{GF}(q)$ متمایزند. اکنون حالتی را در نظر می‌گیریم که $f(x)$ لزوماً تحویل‌ناپذیر نباشد :

قضیه ۹.۳.۱۴. فرض کنید $f(x) \in \mathrm{GF}(q)[x]$ و a ریشه‌ای از $f(x)$ با مرتبه‌ی ضربی n در یک توسیع $\mathrm{GF}(q)$ باشد، اگر r کوچک‌ترین عدد صحیح باشد که $q^r \equiv 1 \mod n$ (یعنی r مرتبه‌ی ضربی q به پیمانه‌ی n است)، آنگاه a، a^q، ...، $a^{q^{r-1}}$ ریشه‌های متمایزی از $f(x)$ هستند.

اثبات. چون $f(a^{q^i}) = f(a)^{q^i} = 0$، به ازای هر $i = 0, 1, 2, \ldots, r-1$، a^{q^i} ریشه‌ای از $f(x)$ است. اگر به ازای i، j، که $i<j$، $a^{q^i} = a^{q^j}$، آنگاه (چون مرتبه‌ی ضربی a برابر n است) $q^i \equiv q^j \mod n$، یعنی $q^{i-j} \equiv 1 \mod n$. اما $q^{i-j} \equiv 1 \mod n$ اگر و تنها اگر $i-j$ مضربی از r باشد. این نشان می‌دهد که a، a^q، ...، $a^{q^{r-1}}$ متمایزند. □

نتیجه ۱۰.۳.۱۴. چندجمله‌ای می‌نیمال $a \in \mathrm{GF}(q^n)$ روی $\mathrm{GF}(q)$ عبارت است از

$$m(x) = (x-a)(x-a^q)\cdots(x-a^{q^{r-1}}),$$

که در آن r کوچک‌ترین عدد صحیح مثبت است که $a^{q^r} = a$. □

قضیه ۱۱.۳.۱۴. اگر n عدد صحیح مثبت باشد، آنگاه داریم $x^{q^n}-x = \prod_i f_i(x)$، که در آن حاصل‌ضرب روی همه‌ی چندجمله‌ای‌های متمایز، تکین، و تحویل‌ناپذیر روی $\mathrm{GF}(q)$، با درجه‌ی k، $(k|n)$ انجام می‌شود.

اثبات. اگر درجه‌ی $f_i(x)$، برابر k_1 باشد و $k_1|n$، آنگاه بنا به قضیه‌ی ۸.۳.۱۴، داریم $f_i(x)|x^{q^n}-x$. اکنون اگر $f_j(x)$ چندجمله‌ای دیگری از درجه‌ی k_2 باشد و $k_2|n$ و $f_i(x)$ و $f_j(x)$ نسبت به هم اول باشند، آنگاه $f_i(x)f_j(x)|x^{q^n}-x$. بنابراین $\prod_i f_i(x)|x^{q^n}-x$ و حکم از قضیه‌ی ۸.۳.۱۴، و این که ریشه‌های $x^{q^n}-x$ متمایزند نتیجه می‌شود. □

قضیه‌ی ۱۱.۳.۱۴، بیان می‌کند هر عضو $a \in \mathrm{GF}(q^n)$ ریشه‌ای از یک چندجمله‌ای تحویل‌ناپذیر روی $\mathrm{GF}(q)$ با درجه‌ی کمتر یا مساوی n است. فرض کنید $m(x)$ چندجمله‌ای می‌نیمال a روی $\mathrm{GF}(q)$ با درجه‌ی k باشد که در آن $k|n$. در این صورت a، a^q، ...، $a^{q^{k-1}}$ ریشه‌های $m(x)$ هستند (قضیه‌ی ۷.۳.۱۴) و $m(x)$ چندجمله‌ای می‌نیمال هر کدام از این ریشه‌ها است. تجزیه‌ی داده شده در قضیه‌ی ۱۱.۳.۱۴، را می‌توان به عنوان حاصل‌ضرب چندجمله‌ای می‌نیمال عناصر $\mathrm{GF}(q^n)$ روی $\mathrm{GF}(q)$ در نظر گرفت. خواص چندجمله‌ای‌های می‌نیمال که تا حالا به دست آمده‌اند را در قضیه‌ی بعدی جمع‌بندی می‌کنیم.

قضیه ۱۲.۳.۱۴. فرض کنید $a \in \mathrm{GF}(q^n)$ با چندجمله‌ای می‌نیمال $m(x) \in \mathrm{GF}(q)[x]$ باشد، که در آن $\deg m(x) = d$. در این صورت
(الف) $m(x)$ روی $\mathrm{GF}(q)$ تحویل‌ناپذیر و $\deg m(x) = d$ شمارنده‌ای از n است.
(ب) اگر $f(x) \in \mathrm{GF}(q)[x]$، آنگاه $f(a) = 0$ اگر و تنها اگر $m(x)|f(x)$.

(ج) اگر a اولیه باشد، آن‌گاه $\deg m(x) = n$.
(د) ریشه‌های $m(x)$ عبارت‌اند از a، a^q، ...، $a^{q^{d-1}}$، و $m(x)$ چندجمله‌ای می‌نیمال همه‌ی این عناصر است.
(هـ) $m(x)$ شمارنده‌ای از $x^{q^n} - x$ و $x^{q^d} - x$ است. □

یک روش سر راست برای محاسبه‌ی چندجمله‌ای می‌نیمال یک عضو در میدان متناهی به صورت زیر است. عضو $a \in \mathrm{GF}(q^n)$ طوری در نظر می‌گیریم که $\{1, a, \ldots, a^{n-1}\}$ پایه‌ای برای $\mathrm{GF}(q^n)$ روی $\mathrm{GF}(q)$ باشد. اگر بخواهیم چندجمله‌ای می‌نیمال $b \in \mathrm{GF}(q^n)^\times$ روی $\mathrm{GF}(q)$ را بیابیم، b^0، b^1، ...، b^n را نسبت به عناصر این پایه می‌نویسیم:

$$b^{i-1} = \sum_{j=1}^{n} d_{ij} a^{j-1}, \qquad 1 \le i \le n+1.$$

فرض کنید $g(x) = c_0 + c_1 x + \cdots + c_n x^n$ چندجمله‌ای می‌نیمال b باشد. داریم

$$\begin{aligned} 0 = g(b) &= \sum_{i=1}^{n+1} c_{i-1} b^{i-1} \\ &= \sum_{i=1}^{n+1} c_{i-1} \sum_{j=1}^{n} d_{ij} a^{j-1} \\ &= \sum_{j=1}^{n} \left(\sum_{i=1}^{n+1} c_{i-1} d_{ij} \right) a^{j-1}. \end{aligned}$$

چون $\{1, a, \ldots, a^{n-1}\}$ مستقل خطی است، دستگاه

$$\sum_{i=1}^{n+1} c_{i-1} d_{ij} = 0, \quad 1 \le j \le n \tag{1}$$

با مجهولات c_0، ...، c_n را به دست می‌آوریم. فرض کنید D ماتریس ضرایب دستگاه فوق، یعنی D ماتریس $(n+1) \times n$ است که درایه‌های (i,j) آن d_{ij} است، و r رتبه‌ی D باشد. در این صورت بُعد فضای جواب دستگاه برابر $s = n + 1 - r$ است، و چون $1 \le r \le n$، داریم $1 \le s \le n$. بنابراین s تا از مجهول‌های c_1، ...، c_n را برابر مقدار از پیش تعیین شده در نظر می‌گیریم و باقی آن را به صورت یکتا می‌یابیم. اگر $s = 1$، قرار می‌دهیم $c_n = 1$ و اگر $s > 1$ قرار می‌دهیم $c_n = c_{n-1} = \cdots = c_{n-s+2} = 0$ و $c_{n-s+1} = 1$.

مثال ۱۳.۳.۱۴. چندجمله‌ای تحویل‌ناپذیر $x^6 + x + 1 \in \mathbb{Z}_2[x]$ و ریشه‌ی $a \in \mathrm{GF}(64)$ از آن را در نظر بگیرید. برای $b = a^3 + a^4$ داریم

$$\begin{aligned}
b^0 &= 1 \\
b^1 &= a^3 + a^4 \\
b^2 &= 1 + a + a^2 + a^3 \\
b^3 &= a + a^2 + a^3 \\
b^4 &= a + a^2 + a^4 \\
b^5 &= 1 + a^3 + a^4 \\
b^6 &= 1 + a + a^2 + a^4.
\end{aligned}$$

مثلاً

$$b^2 = (a^3 + a^4)^2 = a^6 + a^8 = a + 1 + a^8 = a + 1 + a^3 + a^2,$$

و به همین نحو می‌توان $b^۳$، ... را محاسبه کرد. بنابراین

$$D = \begin{bmatrix} ۱ & ۰ & ۰ & ۰ & ۰ & ۰ \\ ۰ & ۰ & ۰ & ۱ & ۱ & ۰ \\ ۱ & ۱ & ۱ & ۱ & ۰ & ۰ \\ ۰ & ۱ & ۱ & ۱ & ۰ & ۰ \\ ۰ & ۱ & ۱ & ۰ & ۱ & ۰ \\ ۱ & ۰ & ۰ & ۱ & ۱ & ۰ \\ ۱ & ۱ & ۱ & ۰ & ۱ & ۰ \end{bmatrix}.$$

به سادگی می‌توان دید که رتبه‌ی ماتریس D برابر $r = ۳$ است. بنابراین $s = n + ۱ - r = ۴$ و قرار می‌دهیم $c_۴ = c_۵ = c_۶ = ۰$ و $c_۳ = ۱$. ضرایب دیگر را از دستگاه (۱) به دست می‌آوریم: $c_۲ = ۱$، $c_۱ = ۰$، $c_۰ = ۱$. پس چندجمله‌ای می‌نیمال b روی $\mathbb{Z}_۲$ برابر $g(x) = ۱ + x^۲ + x^۳$ است. □

روش دیگری برای یافتن چندجمله‌ای می‌نیمال به صورت زیر است (نتیجه‌ی ۱۰.۳.۱۴). اگر بخواهیم چندجمله‌ای می‌نیمال $g(x)$ از $b \in \mathrm{GF}(q^n)$ روی $\mathrm{GF}(q)$ را بیابیم، ابتدا توان‌های b، b^q، $b^{q^۲}$، ... را می‌یابیم تا به کوچک‌ترین عدد صحیح d برسیم که $b^{q^d} = b$، یعنی مرتبه‌ی ضربی b را به دست می‌آوریم، که برابر $q^d - ۱$ است. عدد صحیح d درجه‌ی $g(x)$ است و

$$g(x) = (x - b)(x - b^q) \cdots (x - b^{q^{d-۱}}).$$

توجه کنید b، b^q، ...، $b^{q^{d-۱}}$ را مزدوج‌های b نسبت به $\mathrm{GF}(q)$ هستند؛ این عناصر متمایزند و $g(x)$ چندجمله‌ای می‌نیمال هر کدام از این عناصر روی $\mathrm{GF}(q)$ است.

مثال ۱۴.۳.۱۴. چندجمله‌ای می‌نیمال همه‌ی عناصر $\mathrm{GF}(۱۶)$ روی $\mathbb{Z}_۲$ را بیابید.

حل فرض کنید $a \in \mathrm{GF}(۱۶)$ ریشه‌ای از چندجمله‌ای تحویل‌ناپذیر $x^۴ + x + ۱$ روی $\mathbb{Z}_۲$ باشد. بنابراین a عضو اولیه‌ای از $\mathrm{GF}(۱۶)$ است و هر عضو ناصفر $\mathrm{GF}(۱۶)$ را می‌توان به صورت توانی از a نوشت. از طرف دیگر چون $\{۱, a, a^۲, a^۳\}$ پایه‌ای برای $\mathrm{GF}(۱۶)$ روی $\mathbb{Z}_۲$ است هر توان a را می‌توان به صورت ترکیب خطی از این عناصر نوشت. این کار را در جدول زیر انجام داده‌ایم (لازم است خواننده صحت آن را تحقیق کند).

i	۰	۱	۲	۳	۴
a^i	۱	a	$a^۲$	$a^۳$	$۱ + a$
i	۵	۶	۷	۸	۹
a^i	$a + a^۲$	$a^۲ + a^۳$	$۱ + a + a^۳$	$۱ + a^۲$	$a + a^۳$
i	۱۰	۱۱	۱۲	۱۳	۱۴
a^i	$۱ + a + a^۲$	$a + a^۲ + a^۳$	$۱ + a + a^۲ + a^۳$	$۱ + a^۲ + a^۳$	$۱ + a^۳$

اکنون با استفاده از جدول فوق چندجمله‌ای می‌نیمال اعضای $\mathrm{GF}(۱۶)$ روی $\mathbb{Z}_۲$ را می‌یابیم:

$b = ۰$: $g_۱(x) = x$.

$b = ۱$: $g_۲(x) = x - ۱$.

$b = a$: مزدوج‌های متمایز b نسبت به $\mathbb{Z}_۲$ عبارت‌اند از a، $a^۲$، $a^۴$، $a^۸$ و چندجمله‌ای می‌نیمال هر کدام از آن‌ها برابر است با

$$g_۳(x) = (x - a)(x - a^۲)(x - a^۴)(x - a^۸) = x^۴ + x + ۱.$$

$b = a^۳$: مزدوج‌های متمایز $a^۳$ نسبت به $\mathbb{Z}_۲$ عبارت‌اند از $a^۳$، $a^۶$، $a^{۱۲}$، $a^{۲۴} = a^۹$ و چندجمله‌ای می‌نیمال هر کدام از این عناصر برابر است با

$$\begin{aligned} g_۴(x) &= (x - a^۳)(x - a^۶)(x - a^{۱۲})(x - a^۹) \\ &= x^۴ + x^۳ + x^۲ + x + ۱. \end{aligned}$$

$b = a^{۵}$: مزدوج‌های متمایز $b^{۵}$ نسبت به $\mathbb{Z}_{۲}$ عبارت‌اند از $a^{۵}$ و $a^{۱۰}$ و چندجمله‌ای می‌نیمال هر کدام از این عناصر برابر است با

$$g_{۵}(x) = (x - a^{۵})(x - a^{۱۰}) = x^{۲} + x + ۱.$$

$b = a^{۷}$: مزدوج‌های متمایز $a^{۷}$ نسبت به $\mathbb{Z}_{۲}$ عبارت‌اند از $a^{۷}$، $a^{۱۴}$، $a^{۱۳} = a^{۲۸}$، $a^{۵۶} = a^{۱۱}$ و چندجمله‌ای می‌نیمال همه‌ی این عناصر برابر است با

$$g_{۶}(x) = (x - a^{۷})(x - a^{۱۴})(x - a^{۱۳})(x - a^{۱۱}) = x^{۴} + x^{۳} + ۱. \qquad \square$$

اکنون می‌خواهیم روشی که برای یافتن چندجمله‌ای‌های می‌نیمال در مثال ۱۴.۳.۱۴، بررسی شد را برای یافتن چندجمله‌ای‌های می‌نیمال اعضای $\mathrm{GF}(p^m)$ روی $\mathbb{Z}_p$، با استفاده از مجموعه‌هایی موسوم به هم مجموعه‌های دایره‌بر به کار ببریم. فرض کنید $a \in \mathrm{GF}(p^m)$ یک عضو اولیه‌ی دلخواه و b عضوی از $\mathrm{GF}(p^m)$ باشد طوری که به ازای یک $۰ \le s \le p^m - ۱$، $b = a^s$. اگر $b = a^s$، $b^p = a^{ps}$، ...، $b^{p^{r_s - ۱}} = a^{p^{r_s - ۱}s}$ همه‌ی مزدوج‌های b نسبت به $\mathbb{Z}_p$ باشند (بنابراین r_s کوچک‌ترین عدد صحیح است که $p^{r_s}s \equiv s \mod p^m - ۱$)، آنگاه $m(x) = (x - a^s)(x - a^{ps}) \cdots (x - a^{p^{r_s - ۱}s})$ چندجمله‌ای می‌نیمال $b = a^s$ است. هم مجموعه‌ی دایره‌بر شامل s را به صورت

$$C_s = \{s, ps, p^{۲}s, \cdots, p^{r_s - ۱}s\}$$

تعریف می‌کنیم، که در آن $p^i s$ به پیمانه‌ی $p^m - ۱$ محاسبه می‌شود؛ بنابراین داریم :

قضیه ۱۵.۳.۱۴. فرض کنید $m(x)$ چندجمله‌ای می‌نیمال $b \in \mathrm{GF}(p^m)$ و a عضو اولیه‌ی از $\mathrm{GF}(p^m)$ باشد و $b = a^i$، که در آن $۰ \le i \le p^m - ۱$. اگر s کوچک‌ترین عضو هم مجموعه‌ی دایره‌بر به پیمانه‌ی $p^m - ۱$ شامل i باشد، آنگاه

$$m(x) = \prod_{j \in C_s} (x - a^j). \qquad \square$$

اگر $\gcd\{s, p^m - ۱\} = ۱$، آنگاه $r_s = m$. اما اگر $\gcd\{s, p^m - ۱\} \neq ۱$، آنگاه r با تغییر s، تغییر می‌کند. هم مجموعه‌های دایره‌بر یک افراز $\mathbb{Z}_{p^m - ۱}$ را تشکیل می‌دهند. با استفاده از مثال ۱۴.۳.۱۴، هم مجموعه‌های دایره‌بر به پیمانه‌ی $۱۵ = ۱ - ۲^{۴}$ عبارت‌اند از :

$$C_{۰} = \{۰\}, \quad C_{۱} = \{۱, ۲, ۴, ۸\}, \quad C_{۳} = \{۳, ۶, ۱۲, ۹\},$$
$$C_{۵} = \{۵, ۱۰\}, \quad C_{۷} = \{۷, ۱۴, ۱۳, ۱۱\},$$

که یک افراز $\mathbb{Z}_{۲^۴ - ۱} = \mathbb{Z}_{۱۵}$ را تشکیل می‌دهند. هم مجموعه‌های دایره‌بر برای تجزیه‌ی چندجمله‌ای $x^n - ۱$ نیز مفید هستند. اگر $n = p^m - ۱$ می‌توانیم تعداد و درجه‌ی عوامل تحویل‌ناپذیر $x^{p^m - ۱} - ۱$ را با محاسبه‌ی هم‌مجموعه‌های دایره‌بر $p^m - ۱$ به دست آوردیم. در مثال قبل می‌توانیم بلافاصله از محاسبه‌ی $C_{۱}$، $C_{۳}$، $C_{۵}$، $C_{۷}$ نتیجه بگیریم که $x^{۱۵} - ۱$ سه عامل تحویل‌ناپذیر درجه‌ی ۴ و یک عامل تحویل‌ناپذیر درجه‌ی ۲ دارد.

مثال ۱۶.۳.۱۴. اگر $p^m - ۱ = ۶۳$، آنگاه هم‌مجموعه‌های دایره‌بر (به پیمانه‌ی ۶۳) عبارت‌اند از

$$C_{۰} = \{۰\}, \quad C_{۱} = \{۱, ۲, ۴, ۸, ۱۶, ۳۲\}, \quad C_{۳} = \{۳, ۶, ۱۲, ۲۴, ۴۸, ۳۳\},$$
$$C_{۵} = \{۵, ۱۰, ۲۰, ۴۰, ۱۷, ۳۴\}, \quad C_{۷} = \{۷, ۱۴, ۲۸, ۵۶, ۴۹, ۳۵\},$$
$$C_{۹} = \{۹, ۱۸, ۳۶\}, \quad C_{۱۱} = \{۱۱, ۲۲, ۴۴, ۲۵, ۵۰, ۳۷\},$$
$$C_{۱۳} = \{۱۳, ۲۶, ۵۲, ۴۱, ۱۹, ۳۸\}, \quad C_{۱۵} = \{۱۵, ۳۰, ۶۰, ۵۷, ۵۱, ۳۹\},$$
$$C_{۲۱} = \{۲۱, ۴۲\}, \quad C_{۲۳} = \{۲۳, ۴۶, ۲۹, ۵۸, ۵۳, ۴۳\},$$
$$C_{۲۷} = \{۲۷, ۵۴, ۴۵\}, \quad C_{۳۱} = \{۳۱, ۶۲, ۶۱, ۵۹, ۵۵, ۴۷\}.$$

بنابراین نتیجه می‌گیریم که $x^{۶۳} - ۱$، نه عامل تحویل‌ناپذیر درجه‌ی ۶، دو عامل تحویل‌ناپذیر درجه‌ی ۳ و یک عامل از درجه‌های ۱ و ۲ دارد. پیدا کردن عامل‌های درجه‌ی ۶ کار چندان ساده‌ای نیست. $\square$

برای یافتن عوامل تحویل‌ناپذیر $x^n - ۱$، $n = p^m - ۱$، ساده‌تر است که عوامل تحویل‌ناپذیر $x^{p^m} - x$ را بیابیم، زیرا چندجمله‌ای اخیر حاصل‌ضرب چندجمله‌ای‌های تحویل‌ناپذیر است که درجه‌شان m را می‌شمارد. اکنون حالت $n \neq p^m - ۱$ را در نظر می‌گیریم. فرض می‌کنیم $\gcd\{n, p\} = ۱$، بنابراین p به پیمانه‌ی n وارون دارد ، و مفهوم هم‌مجموعه‌ی دایره‌بر را به صورت زیر تعمیم می‌دهیم:

تعریف ۱۷.۳.۱۴. هم مجموعه‌ی دایره‌بر به پیمانه‌ی n شامل s را برابر

$$C_s = \{s, ps, p^۲s, \ldots, p^{r_s - ۱}s\},$$

تعریف می‌کنیم، که در آن $p^i s$ به پیمانه‌ی n محاسبه می‌شود. در این‌جا r_s کوچک‌ترین عدد صحیح است که $p^{r_s}s \equiv s \mod n$.

اگر اعداد n و p داده شده باشند، می‌دانیم کوچک‌ترین عدد صحیح m وجود دارد که n، $p^m - ۱$ را می‌شمارد. این رخ می‌دهد اگر و تنها اگر $x^n - ۱$، $x^{p^{m-۱}} - ۱$ را بشمارد. بنابراین $\mathrm{GF}(p^m)$ کوچک‌ترین میدان با مشخصه‌ی p شامل همه‌ی ریشه‌های $x^n - ۱$ است. ریشه‌های $x^n - ۱$ توان‌های یک ریشه‌ی اولیه‌ی واحد هستند. اکنون می‌توانیم قضیه‌ی ۱۵.۳.۱۴، را به سادگی تعمیم دهیم:

قضیه ۱۸.۳.۱۴. فرض کنید $b \in \mathrm{GF}(p^n)$ ریشه‌ای از $x^n - ۱$ و $m(x)$ چندجمله‌ای می‌نیمال آن باشد. فرض کنید a یک ریشه‌ی اولیه‌ی واحد در $\mathrm{GF}(p^m)$ باشد و $b = a^i$. اگر s کوچک‌ترین عضو هم مجموعه‌ی دایره‌بر به پیمانه‌ی n شامل i باشد، آن‌گاه

$$m(x) = \prod_{j \in C_s} (x - a^j). \qquad \square$$

چون $x^n - ۱ = \prod_{i=۰}^{n-۱}(x - a_i)$، که در آن $a_۰$، ...، $a_{n-۱}$ عناصر متمایز $\mathrm{GF}(p^m)$ هستند ، یعنی ریشه‌های nام متمایز واحد هستند ، هم‌چنین داریم $x^n - ۱ = \prod_{i=۰}^{n-۱}(x - a^i)$، که در آن a یک ریشه‌ی nام اولیه‌ی واحد است. اگر $m_s(x)$ چندجمله‌ای می‌نیمال a^s باشد، آن‌گاه بنا به قضیه‌ی ۱۸.۳.۱۴، داریم

$$x^n - ۱ = \prod_s m_s(x),$$

که در آن s در مجموعه‌ی نماینده‌های هم‌مجموعه‌های دایره‌بر به پیمانه‌ی n تغییر می‌کند. این فرمول تجزیه‌ی $x^n - ۱$ به عوامل تحویل‌ناپذیر روی $\mathrm{GF}(p^m)$ را به دست می‌دهد. نتایج مشابهی را می‌توان با در نظر گرفتن میدان متناهی دلخواه $\mathrm{GF}(q)$ به دست آورد.

مثال ۱۹.۳.۱۴. فرض کنید $x^۹ - ۱ \in \mathbb{Z}_۲[x]$. در این صورت $r = ۶$ کوچک‌ترین عدد طبیعی است که $۹ | ۲^r - ۱$. بنابراین $\mathrm{GF}(۱۶)$ توسیع تجزیه‌ی $x^۹ - ۱$ روی $\mathbb{Z}_۲$ است. هم مجموعه‌های دایره‌بر به پیمانه‌ی ۹ عبارت‌اند از $C_۰ = \{۰\}$، $C_۱ = \{۱, ۲, ۴, ۸, ۷, ۵\}$، $C_۳ = \{۳, ۶\}$. عضو $a \in \mathrm{GF}(۱۶)$ را طوری انتخاب می‌کنیم که $a^۶ + a^۳ + ۱ = ۰$. چندجمله‌ای‌های می‌نیمال که در قضیه‌ی قبل معرفی شد، عبارت‌اند از

$$m_۰(x) = x + ۱, \quad m_۱(x) = x^۶ + x^۳ + ۱, \quad m_۳(x) = x^۲ + x + ۱.$$

بنابراین $x^۹ - ۱ = m_۱(x)m_۲(x)m_۳(x)$. $\square$

مثال ۲۰.۳.۱۴. برای به دست آوردن برخی از اطلاعات تجزیه‌ی $x^{۲۳} - ۱$ روی $\mathbb{Z}_۲$ هم‌مجموعه‌های دایره‌بر به پیمانه‌ی ۲۳ را می‌یابیم:

$$C_۰ = \{۰\}, \quad C_۱ = \{۱, ۲, ۴, ۸, ۱۶, ۹, ۱۸, ۱۳, ۳, ۶, ۱۲\},$$
$$C_۵ = \{۵, ۱۰, ۲۰, ۱۷, ۱۱, ۲۲, ۲۱, ۱۹, ۱۵, ۷, ۱۴\}.$$

نتیجه می‌شود که $x^{۲۳} - ۱$ دو عامل تحویل‌ناپذیر درجه‌ی ۱۱ و یک عامل درجه‌ی اول ، یعنی $x - ۱$ دارد. هر کدام چندجمله‌ای می‌نیمال یک ریشه‌ی ۲۳ام اولیه‌ی واحد (که در $\mathrm{GF}(۲^{۱۱})$ قرار دارند) هستند ، زیرا $r = ۱۱$ کوچک‌ترین عدد صحیح است که $۲۳ | ۲^r - ۱$. $\square$

مثال ۲۱.۳.۱۴. همه‌ی هم مجموعه‌های دایره‌بر به پیمانه‌ی ۱۲ روی $\mathbb{Z}_۲$ را تعیین کنید و تجزیه‌ی $x^{۲۱} - ۱$ روی $\mathbb{Z}_۲$ را بیابید.

حل هم‌مجموعه‌های دایره‌بر به پیمانه‌ی ۱۲ روی $\mathbb{Z}_{۲}$ عبارت‌اند از

$$C_{۰}=\{۰\},\ \ C_{۱}=\{۱,۲,۴,۸,۱۱,۱۶\},\ \ C_{۳}=\{۳,۶,۱۲\}$$
$$C_{۵}=\{۵,۱۰,۱۲,۱۳,۱۴,۲۰\},\ \ C_{۷}=\{۷,۱۴\},\ \ C_{۹}=\{۹,۱۸,۱۵\}.$$

$x^{۲۱}-۱=m_{۰}(x)m_{۱}(x)m_{۳}(x)m_{۵}(x)m_{۷}(x)m_{۹}(x)$. اکنون ۶ کوچک‌ترین عدد صحیح است که $۲۱|۲^{۶}-۱$. $a\in \mathrm{GF}(۲^{۶})$ را با $a^{۶}+a^{۴}+a^{۲}+a+۱=۰$، انتخاب می‌کنیم و به دست می‌آوریم

$$m_{۰}(x)=۱+x,\quad m_{۱}(x)=۱+x+x^{۲}+x^{۴}+x^{۶},$$
$$m_{۳}(x)=۱+x^{۲}+x^{۳},\quad m_{۵}(x)=۱+x^{۲}+x^{۴}+x^{۵}+x^{۶},$$
$$m_{۷}(x)=۱+x+x^{۲},\quad m_{۹}(x)=۱+x+x^{۳}.$$

برای مثال $m_{۵}(x)$ را به تفصیل حساب می‌کنیم. فرض کنید $u=a^{۵}$، در این صورت با توجه به این که $a^{۶}+a^{۴}+a^{۲}+a+۱=۰$ داریم

$$u^{۰}=۱,\ \ u=a^{۵},\ \ u^{۲}=a^{۲}+a^{۳}+a^{۵},\ \ u^{۳}=۱+a^{۳},$$
$$u^{۴}=۱+a+a^{۳}+a^{۵},\ \ u^{۵}=a^{۴},\ \ u^{۶}=a+a^{۲}+a^{۴}.$$

با حل دستگاه

$$[c_{۰},c_{۱},c_{۲},c_{۳},c_{۴},c_{۵},c_{۶}]\begin{bmatrix}۱&۰&۰&۰&۰&۰\\ ۰&۰&۰&۰&۰&۱\\ ۰&۰&۱&۱&۰&۱\\ ۱&۰&۰&۱&۰&۰\\ ۱&۱&۰&۱&۰&۱\\ ۰&۰&۰&۰&۱&۰\\ ۰&۱&۱&۰&۱&۰\end{bmatrix}=\begin{bmatrix}۰\\ ۰\\ ۰\\ ۰\\ ۰\\ ۰\\ ۰\end{bmatrix},$$

خواهیم داشت : $c_{۱}=c_{۳}=۰$، $c_{۰}=c_{۲}=c_{۴}=c_{۵}=۱$، یعنی

$$m_{۵}(x)=۱+x^{۲}+x^{۴}+x^{۵}+x^{۶}.$$

چندجمله‌ای‌های می‌نیمال دیگر را می‌توان به طریق مشابه یا با محاسبه‌ی مستقیم و استفاده از $m_s(x)=\prod_{i\in C_s}(x-a^i)$ یافت. □

اکنون می‌خواهیم تعداد چندجمله‌ای‌های تکین و تحویل‌ناپذیر با درجه‌ی داده شده روی $\mathrm{GF}(q)$ را تعیین کنیم. برای این کار و اهداف دیگر تابع موبیوس و هم‌چنین فرمول وارون موبیوس را معرفی می‌کنیم:

تعریف ۲۲.۳.۱۴. نگاشت $\mu:\mathbb{N}\longrightarrow\{۰,-۱,۱\}$ را که با ضابطه‌ی

$$\begin{aligned}\mu(۱) &= ۱\\ \mu(p_{۱}\cdots p_{k}) &= (-۱)^{k},\quad p_i\text{ها اعداد اول متمایز}\\ \mu(n) &= ۰,\quad p^{۲}|n,\ p\text{ اگر به ازای یک عدد اول}\end{aligned}$$

را تابع موبیوس یا μ- تابع می‌نامیم.

تابع موبیوس خاصیت بسیار ساده و مفیدی دارد :

$$\sum_{d|n}\mu(d)=\begin{cases}۱ & n=۱\\ ۰ & n>۱.\end{cases}$$

حالت $n = ۱$ بدیهی است. برای اثبات این مطلب در حالت $n > ۱$ باید تنها شمارنده‌های d از n را در نظر بگیریم که $\mu(d) \neq ۰$، یعنی $d = ۱$ یا d حاصل‌ضرب اعداد اول متمایز باشد. بنابراین اگر $p_۱$، $p_۲$، . . .، p_k شمارنده‌های اول متمایز n باشد، داریم

$$\begin{aligned}\sum_{d|n}\mu(d) &= \mu(۱)+\sum_{i=۱}^{k}\mu(p_i)+\sum_{۱\le i_۱<i_۲\le k}\mu(p_{i_۱}p_{i_۲})+\cdots+\mu(p_۱\cdots p_k)\\ &= ۱+\binom{k}{۱}(-۱)+\binom{k}{۲}(-۱)^۲+\cdots+\binom{k}{k}(-۱)^k\\ &= (۱+(-۱))^k = ۰\end{aligned}$$

اکنون فرمول وارون موبیوس را ثابت می‌کنیم:

قضیه ۲۳.۳.۱۴. (فرمول وارون موبیوس، صورت جمعی) فرض کنید A یک گروه آبلی جمعی و $f : \mathbb{N} \longrightarrow A$، $g : \mathbb{N} \longrightarrow A$ دو تابع باشند. در این صورت

$$g(n) = \sum_{d|n} f(d) \iff f(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) g(d).$$

اثبات. فرض کنید $g(n) = \sum_{d|n} f(d)$. داریم

$$\begin{aligned}\sum_{d|n}\mu\left(\frac{n}{d}\right)g(d) &= \sum_{d|n}\mu(d)g\left(\frac{n}{d}\right)\\ &= \sum_{d|n}\mu(d)\sum_{c|\frac{n}{d}}f(c)\\ &= \sum_{c|n}\sum_{d|\frac{n}{c}}\mu(d)f(c)\\ &= \sum_{c|n}f(c)\sum_{d|\frac{n}{c}}\mu(d)\\ &= f(n).\end{aligned}$$

عکس مطلب با محاسبه‌ی مشابهی ثابت می‌شود. □

در حالتی که A گروه آبلی ضربی باشد مجموع به حاصل‌ضرب، و ضرایب به توان، مبدل می‌شود؛ بنابراین در این حالت فرمول وارون موبیوس به صورت زیر در می‌آید:

$$g(n) = \prod_{d|n} f(d) \iff f(n) = \prod_{d|n} g(d)^{\mu(n/d)}.$$

اکنون تعداد چندجمله‌ای‌های تکین و تحویل‌ناپذیر با درجه‌ی k روی $\mathrm{GF}(q)$ را تعیین می‌کنیم:

قضیه ۲۴.۳.۱۴. تعداد چندجمله‌ای‌های تکین و تحویل‌ناپذیر با درجه‌ی k روی $\mathrm{GF}(q)$ عبارت است از

$$I_q(k) = \frac{۱}{k}\sum_{d|k}\mu\left(\frac{k}{d}\right)q^d.$$

اثبات. بنا به قضیه‌ی ۱۱.۳.۱۴، درجه‌ی حاصل‌ضرب همه‌ی چندجمله‌ای‌های تکین و تحویل‌ناپذیر با درجه‌ی k روی $\mathrm{GF}(q)$ برابر $\sum_{d|k} I_q(d)d = q^k$ است. پس بنا به قضیه‌ی ۲۳.۳.۱۴ (صورت جمعی فرمول وارون موبیوس با $f(n) = I_q(n)n$ و $g(n) = q^n$) حکم ثابت است:

$$I_q(k)k = \sum_{d|k}\mu\left(\frac{k}{d}\right)q^d.$$ □

به عنوان مثال تعداد چندجمله‌ای‌های تحویل‌ناپذیر از درجه‌های $k = ۱, ۲, ۳, ۴, ۵$ روی $\mathbb{Z}_۲$ عبارت‌اند از

$$I_۱(۲) = ۲, \quad I_۲(۲) = ۱, \quad I_۳(۲) = ۲, \quad I_۴(۲) = ۳, \quad I_۵(۲) = ۶.$$

رابطه‌های جالبی بین چندجمله‌ای‌های می‌نیمال و عناصر اولیه در میدان متناهی وجود دارند. در ادامه این ارتباط را بررسی می‌کنیم. ابتدا باید مرتبه‌ی یک چندجمله‌ای ناصفر روی میدان متناهی را تعریف کنیم؛ برای این کار به لم زیر نیاز داریم.

لم ۲۵.۳.۱۴. اگر $f(x) \in \mathrm{GF}(q)[x]$ یک چندجمله‌ای با درجه‌ی $m \geq ۱$ باشد و $f(۰) \neq ۰$، آنگاه عدد صحیح مثبت $e \leq q^m - ۱$ وجود دارد که $f(x)|x^e - ۱$.

اثبات. حلقه‌ی خارج قسمتی $\mathrm{GF}(q)[x]/(f(x))$ را در نظر می‌گیریم. این حلقه q^m عضو دارد. چون $q^{m-۱}$ عضو ناصفر دارد. $x^j + (f(x))$، $۰ \leq j \leq q^m - ۱$، همگی ناصفرند، اعداد صحیح t و s وجود دارند که $۰ \leq s < t \leq q^m - ۱$ و $x^s + (f(x)) = x^t + (f(x))$، یعنی $f(x)|x^s - x^t$. اما چون $\gcd\{x, f(x)\} = ۱$، داریم $f(x)|x^{s-t} - ۱$. □

فرض کنید $f(x)$ یک چندجمله‌ای در $\mathrm{GF}(q)[x]$ باشد. اگر $f(۰) \neq ۰$ کوچک‌ترین عدد طبیعی e که، $f(x)|x^e - ۱$ را مرتبه‌ی $f(x)$ گوییم. در حالتی که $f(۰) = ۰$ و $f(x) = x^r g(x)$، که در آن $r \in \mathbb{N}$ و $g(x) \in \mathrm{GF}(q)[x]$ چندجمله‌ای یکتا باشد که $g(۰) \neq ۰$، مرتبه‌ی $f(x)$ را برابر مرتبه‌ی $g(x)$ تعریف می‌کنیم. مرتبه‌ی یک چندجمله‌ای تحویل‌ناپذیر را می‌توان با ریشه‌هایش توصیف کرد:

قضیه ۲۶.۳.۱۴. اگر $f(x) \in \mathrm{GF}(q)[x]$ چندجمله‌ای تحویل‌ناپذیر روی $\mathrm{GF}(q)$ با درجه‌ی m باشد و $f(۰) \neq ۰$، آنگاه مرتبه‌ی $f(x)$ برابر مرتبه‌ی ضربی هر ریشه‌ی دلخواه $f(x)$ در $\mathrm{GF}(q^n)^\times$ است.

اثبات. $\mathrm{GF}(q^m)$ میدان تجزیه‌ی $f(x)$ روی $\mathrm{GF}(q)$ است. مرتبه‌ی ضربی ریشه‌های $f(x)$ در $\mathrm{GF}(q^m)^\times$ یکسان است. فرض کنید $a \in \mathrm{GF}(q^m)^\times$ ریشه‌ی دلخواهی از $f(x)$ باشد، در این صورت $a^e = ۱$ اگر و تنها اگر $f(x)|x^e - ۱$. بنابراین حکم از تعریف مرتبه‌ی $f(x)$ و مرتبه‌ی a در گروه $\mathrm{GF}(q^m)^\times$ نتیجه می‌شود. □

نتیجه ۲۷.۳.۱۴. اگر $f(x) \in \mathrm{GF}(q)[x]$ روی $\mathrm{GF}(q)$ تحویل‌ناپذیر با درجه‌ی m باشد، آنگاه مرتبه‌ی $f(x)$، $q^m - ۱$ را عاد می‌کند.

اثبات. اگر $f(x) = cx$، که در آن $c \in \mathrm{GF}(q)^\times$، آنگاه مرتبه‌ی $f(x)$ برابر ۱ است. در غیر این صورت حکم از قضیه‌ی قبل و این که $|\mathrm{GF}(q^m)^\times| = q^m - ۱$ به دست می‌آید. □

قضیه ۲۸.۳.۱۴. تعداد چندجمله‌ای‌های تحویل‌ناپذیر با درجه‌ی m و مرتبه‌ی e روی $\mathrm{GF}(q)$ برابر $\varphi(e)/m$ است، که در آن φ تابع فی اویلر است.

اثبات. چون $\mathrm{GF}(q^m)$ کوچک‌ترین توسیع $\mathrm{GF}(q)$ است که مشتمل بر همه‌ی ریشه‌های هر چندجمله‌ای تحویل‌ناپذیر از درجه‌ی m است، داریم $e|(q^m - ۱)$ و $e \nmid (q^k - ۱)$، برای $k < m$. چون $(x^e - ۱)|(x^{q^m - ۱} - ۱)$، $\mathrm{GF}(q^m)$ شامل همه‌ی ریشه‌های eام واحد و بنابراین شامل همه‌ی $\varphi(e)$ تا ریشه‌ی eام اولیه‌ی واحد است. اگر a چنین ریشه‌ای باشد، آنگاه a، a^q، ...، $a^{q^{m-۱}}$ متمایزند و درجه‌ی چندجمله‌ای می‌نیمال ریشه‌ی eام اولیه‌ی واحد برابر m است (قضیه‌ی ۱۲.۳.۱۴ را ببینید). □

دیدیم که مرتبه‌ی یک چندجمله‌ای با درجه‌ی $m \geq ۱$ روی $\mathrm{GF}(q)$ حداکثر $q^m - ۱$ است. برای رده‌های مهمی از چندجمله‌ای‌ها این کران اختیار می‌شود. این چندجمله‌ای‌ها بر اساس عناصر اولیه‌ی میدان متناهی تعریف می‌شوند:

تعریف ۲۹.۳.۱۴. چندجمله‌ای تحویل‌ناپذیر از درجه‌ی m روی $\mathrm{GF}(q)$ را اولیه گوییم، هرگاه چندجمله‌ای می‌نیمال عضو اولیه‌ای از $\mathrm{GF}(q^m)$ باشد.

می‌خواهیم چندجمله‌ای‌های اولیه را توصیف کنیم. برای این کار به یک لم نیاز داریم. ابتدا توجه کنید که $x^m - ۱$ روی میدان دلخواه F، شمارنده‌ای از $x^n - ۱$ است اگر و تنها اگر $m|n$. برای اثبات این مطلب می‌نویسیم $n = km + r$، که در آن $۰ \leq r < m$، و توجه می‌کنیم که

$$x^n - ۱ = x^r(x^m + x^{۲m} + \cdots + x^{km})(x^m - ۱) + x^r - ۱,$$

بنابراین $x^m - ۱|x^n - ۱$ اگر و تنها اگر $x^r - ۱ = ۰$ اگر و تنها اگر $r = ۰$.

لم ۳۰.۳.۱۴. اگر $f(x) \in \mathrm{GF}(q)[x]$ و $f(۰) \neq ۰$، آنگاه $f(x)|x^m - ۱$ (m عدد صحیح مثبت) اگر و تنها اگر مرتبه‌ی $f(x)$ شمارنده‌ای از m باشد.

اثبات. فرض کنید مرتبه‌ی $f(x)$ برابر e باشد. اگر $e|m$، آنگاه $f(x)|x^e - ۱$ و بنابراین $x^e - ۱|x^m - ۱$. پس $f(x)|x^m - ۱$.
بر عکس، اگر $f(x)|x^m - ۱$، آنگاه $m \geq e$؛ بنابراین $m = ke + r$، که در آن $۰ \leq r < e$. چون $x^m - ۱ = x^r(x^{ke} - ۱) + x^r - ۱$، نتیجه می‌گیریم که $f(x)|x^r - ۱$. بنابراین $r = ۰$ و $e|m$. □

قضیه ۳۱.۳.۱۴. چندجمله‌ای $f(x) \in \mathrm{GF}(q)[x]$ از درجه‌ی m روی $\mathrm{GF}(q)$ اولیه است اگر و تنها اگر $f(x)$ تکین، $f(۰) \neq ۰$، و مرتبه‌ی $f(x)$ برابر $q^m - ۱$ باشد.

اثبات. ($\Longleftarrow$) اگر $f(x)$ اولیه باشد، به وضوح $f(x)$ تکین است و $f(۰) \neq ۰$. اکنون چون $f(x)$ تحویل‌ناپذیر و ریشه‌ی آن عضوی از $\mathrm{GF}(q^m)$ است، بنا به قضیه‌ی ۲۶.۳.۱۴، مرتبه‌ی $f(x)$ برابر $q^m - ۱$ است.
($\Longrightarrow$) تنها باید نشان دهیم $f(x)$ تحویل‌ناپذیر است. فرض کنید $f(x)$ تحویل‌پذیر باشد. دو حالت پیش می‌آید.
حالت اول : $f(x) = g_۱(x)g_۲(x)$، که در آن $g_۱$ و $g_۲$ دو چندجمله‌ای نسبت به هم اول هستند و $\deg g_۱(x) = k_۱ > ۰$، $\deg g_۲(x) = k_۲ > ۰$. فرض کنید $e_۱$ و $e_۲$ به ترتیب مرتبه‌ی $g_۱$ و $g_۲$ باشند. چون برای $i = ۱, ۲$ داریم $e_i|e_۱e_۲$، بنا به بحث قبل از قضیه، $x^{e_i} - ۱|x^{e_۱e_۲} - ۱$. بنابراین $g_i(x)$ شمارنده‌ای از $x^{e_۱e_۲} - ۱$ است. چون $g_۱(x)$ و $g_۲(x)$ نسبت به هم اول‌اند حاصل‌ضرب آن‌ها، یعنی $f(x)$ نیز $x^{e_۱e_۲} - ۱$ را می‌شمارد، یعنی مرتبه‌ی $f(x)$ کوچکتر یا مساوی $e_۱e_۲$ است. بنا به قضیه‌ی ۸.۳.۱۴، $g_i(x)|x^{qk_i - ۱} - ۱$، بنابراین $e_i \leq q^{k_i} - ۱$، $i = ۱, ۲$. در نتیجه

$$\text{مرتبه‌ی } f(x) \leq e_۱e_۲ \leq (q^{k_۱} - ۱)(q^{k_۲} - ۱) < q^{k_۱ + k_۲} - ۱ = q^m - ۱,$$

که تناقض است.
حالت دوم : $f(x) = g(x)^b$، که در آن $g(x) \in \mathrm{GF}(q)[x]$ تحویل‌ناپذیر است و $g(۰) \neq ۰$. فرض کنید مرتبه‌ی $g(x)$ برابر e باشد. بنا به قضیه‌ی ۸.۳.۱۴، و این که $g(x)|f(x)$ داریم $e|q^m - ۱$، بنابراین $p \nmid e$، که در آن p مشخصه‌ی $\mathrm{GF}(q)$ است. بنا به لم ۳۰.۳.۱۴، اگر $e|k$، آنگاه $g(x)|x^k - ۱$. بنابراین اگر $k = p^i j$، که در آن $p \nmid j$ داریم

$$x^k - ۱ = x^{p^i j} - ۱ = (x^j - ۱)^{p^i}.$$

چون $x^j - ۱$ ریشه‌ی تکراری ندارد ، هر عامل تحویل‌ناپذیر $x^k - ۱$، p^i بار تکرار می‌شود. فرض کنید t عدد صحیح مثبت یکتایی باشد که $p^{t-۱} < b \leq p^t$، در این صورت مرتبه‌ی $f(x)$ برابر ep^t است. اما $ep^t \leq (q^n - ۱)p^t$، که در آن $n = m/b$ درجه‌ی $g(x)$ است. به علاوه $ep^t \leq q^{n+t} - ۱$. پس $t \leq p^{t-۱} \leq b - ۱ \leq (b - ۱)n$. اکنون با استفاده از این نامساوی‌ها داریم

$$\text{مرتبه‌ی } f(x) < q^{n+۱} - ۱ \leq q^{bn} - ۱ = q^m - ۱,$$

که تناقض است. بنابراین $f(x)$ تحویل‌ناپذیر است و بنا به قضیه‌ی ۲۶.۳.۱۴، مرتبه‌ی ضربی همه‌ی ریشه‌های $f(x)$ برابر $q^m - ۱$ است، یعنی $f(x)$ اولیه است. □

با استفاده از نمادگذاری قضیه‌ی ۱۲.۳.۱۴، دو خاصیت دیگر چندجمله‌ای‌های می‌نیمال را فهرست می‌کنیم:
(و) اگر $a \neq ۰$، آنگاه مرتبه‌ی $m(x)$ برابر مرتبه‌ی a در $\mathrm{GF}(q)^\times$ است.
(ز) $m(x)$ روی $\mathrm{GF}(q)$ اولیه است اگر و تنها اگر مرتبه‌ی a در $\mathrm{GF}(q)^\times$ برابر $q^d - ۱$ باشد ($d = \deg m(x)$).
یکی از مسائل مهم تعیین چندجمله‌ای‌های اولیه است. یک روش مبتنی بر ساختن یک عنصر اولیه‌ی $\mathrm{GF}(q^m)$ و سپس تعیین چندجمله‌ای می‌نیمال این عضو روی $\mathrm{GF}(q)$ است؛ در مثال‌های ۱۳.۳.۱۴ و ۱۴.۳.۱۴، دو راه برای یافتن چندجمله‌ای می‌نیمال تشریح شد. روش دیگری که از خواص چندجمله‌ای‌های، موسوم به دایره‌بر، استفاده می‌کند را در صفحه‌ی ۳۲۳ شرح می‌دهیم. برای یافتن یک عضو اولیه‌ی $\mathrm{GF}(q^m)$، از $q^m - ۱$، یعنی مرتبه‌ی این عضو در $\mathrm{GF}(q^m)^\times$، شروع می‌کنیم و آن را به صورت $q^m - ۱ = n_۱ \cdots n_k$ تجزیه می‌کنیم، که در آن $n_۱$، ...، n_k اعداد صحیح نسبت به هم اول هستند. اگر به ازای یک i، $۱ \leq i \leq k$، عضو $a_i \in \mathrm{GF}(q^m)^\times$ با مرتبه‌ی n_i را بیابیم، آنگاه مرتبه‌ی $a_۱ \cdots a_k$ برابر $q^m - ۱$ و بنابراین عضو اولیه‌ای از $\mathrm{GF}(q^m)$ است.

توجه کنید که اگر $g(x)$ چندجمله‌ای می‌نیمال $a \in \mathrm{GF}(q^n)$ روی $\mathrm{GF}(q)$ با درجه‌ی d باشد، آنگاه $g(x)$ روی $\mathrm{GF}(q)$ اولیه است اگر و تنها اگر مرتبه‌ی a در $\mathrm{GF}(q^n)^\times$ برابر $q^d - ۱$ باشد. به علاوه اگر $a \neq ۰$، آنگاه مرتبه‌ی $g(x)$ برابر مرتبه‌ی a در $\mathrm{GF}(q^n)^\times$ است.
در قضیه‌ی بعدی فرمولی برای حاصل‌ضرب همه‌ی چندجمله‌ای‌های تکین و تحویل‌ناپذیر روی $\mathrm{GF}(q)$ به دست می‌آوریم:

قضیه ۳۲.۳.۱۴. اگر $I(n,q;x)$ حاصل‌ضرب همه‌ی چندجمله‌ای‌های تکین و تحویل‌ناپذیر با درجه‌ی n روی $\mathrm{GF}(q)$ باشد، آنگاه

$$I(n,q;x) = \prod_{d|n}(x^{q^d} - x)^{\mu(n/d)} = \prod_{d|n}(x^{q^{n/d}} - x)^{\mu(d)}.$$

اثبات. با استفاده از قضیه‌ی ۱۱.۳.۱۴، داریم $x^{q^n} - x = \prod_{d|n} I(d,q;x)$. با فرض $f(n) = I(n,q;x)$ و $g(n) = x^{q^n} - x$ در فرمول وارون موبیوس، قضیه‌ی ۲۳.۳.۱۴، حکم به دست می‌آید. □

مثال ۳۳.۳.۱۴. برای $n = ۴$ و $q = ۲$ داریم

$$I(۴,۲;x) = \frac{x^{۱۶} - x}{x^۴ - x} = x^{۱۲} + x^۹ + x^۶ + x^۳ + ۱$$

و

$$\begin{aligned} x^{۱۶} - x &= x^{۲^۴} - x \\ &= I(۱,۲;x)I(۲,۲;x)I(۴,۲;x) \\ &= x(x-۱)(x^۲ + x + ۱)(x^{۱۲} + x^۹ + x^۶ + x^۳ + ۱). \end{aligned}$$ □

تمرین‌ها

۱. جدول لگاریتم گسسته‌ی میدان ۲۷ عضوی را بیابید.
۲. اگر p عدد اول باشد زیرمیدان‌های $\mathrm{GF}(p^۸)$، $\mathrm{GF}(p^{۱۵})$، $\mathrm{GF}(p^{۳۲})$ را بیابید.
۳. فرض کنید K میدان باشد. اگر $K^\times$ دوری باشد، نشان دهید K متناهی است.
۴. اگر n عدد صحیح فرد باشد، نشان دهید $x^۲ + x + ۱$ روی $\mathrm{GF}(۲^n)$ تحویل‌ناپذیر است.
۵. نشان دهید $x^۴ + x + ۱$ روی $\mathbb{Z}_۲$ تحویل‌ناپذیر است و با استفاده از آن میدان $\mathrm{GF}(۱۶)$ را بسازید.
۶. اگر $m|n$، $[\mathrm{GF}(p^n) : \mathrm{GF}(p^m)]$ را بیابید.
۷. فرض کنید p عدد اول باشد. یک میدان نامتناهی بیابید که مرتبه‌ی ضربی هر عضو ناصفر آن متناهی باشد.
۸. فرض کنید K میدان باشد. اگر G و H زیرگروه‌های $K^\times$ از مرتبه‌ی متناهی n باشند، آنگاه $G = H$.
۹. فرض کنید p عدد اول است و $f(x) = x^p - x - ۱ \in \mathbb{Z}_p[x]$. اگر a ریشه‌ی دلخواهی از $f(x)$ باشد، نشان دهید $\mathbb{Z}_p(a) : \mathbb{Z}_p$ توسیع تجزیه‌ی $f(x)$ است.
۱۰. فرض کنید K میدان متناهی است. نشان دهید هر عضو K، مجموع دو مربع است.
۱۱. اگر m عدد صحیح مثبت دلخواهی باشد، نشان دهید

$$\sum_{a \in \mathrm{GF}(q)} a^m = \begin{cases} -۱ & (q-۱)|m \\ ۰ & \text{در غیر این صورت.} \end{cases}$$

به ویژه اگر $p \neq ۲$ عدد اول باشد، $\sum_{a \in \mathbb{Z}_p} a = ۰$.
۱۲. اگر $x^۳ + ax + b$ روی میدان متناهی F تحویل‌ناپذیر باشد، نشان دهید $-۴a^۳ - ۲۷b^۲$ مربع عضوی از F است.

۱۳. فرض کنید $a, b \in \mathrm{GF}(۲^n)$، که در آن n فرد است، نشان دهید $a^۲ + ab + b^۲ = ۰$ نتیجه می‌دهد $a = b = ۰$.

۱۴. فرض کنید a, b، عناصر ناصفر $\mathrm{GF}(q)$ باشند، نشان دهید $r, s \in \mathrm{GF}(q)$ وجود دارند که $۱ + r^۲a + s^۲b = ۰$.

۱۵. نشان دهید چندجمله‌ای $f(x) = \dfrac{x^e - ۱}{x - ۱} = x^{e-۱} + x^{e-۲} + \cdots + x + ۱$ روی $\mathrm{GF}(q)$ تحویل‌ناپذیر است اگر و تنها اگر e عدد اول باشد و q یک ریشه‌ی $(e - ۱)$ام اولیه‌ی واحد به پیمانه‌ی e باشد.

۱۶. نشان دهید تنها سه چندجمله‌ای درجه‌ی ۴، $x^۴ + x + ۱$، $x^۴ + x^۳ + ۱$، $x^۴ + x^۳ + x^۲ + x + ۱$، روی $\mathbb{Z}_۲$ تحویل‌ناپذیرند

۱۷. با استفاده از چندجمله‌ای اولیه‌ی $x^{۲۰} + x^۳ - ۱$ روی $\mathbb{Z}_۲$، میدان $\mathrm{GF}(۲^{۲۰})$ را بسازید. همه‌ی زیرمیدان‌های $\mathrm{GF}(۲^{۲۰})$ را بیابید.

۱۸. فرض کنید p عدد اول است و $a \in \mathbb{Z}_p$. نشان دهید $x^p - x + a$ شمارنده‌ای از $x^{p^n} - x + na$ است.

۱۹. چندجمله‌ای‌های اولیه‌ای با درجه‌های ۲۱، ۲۲، ۲۳، و ۲۴ روی $\mathbb{Z}_۲$ بیابید.

۲۰. فرض کنید $f_۱(x)$، ...، $f_k(x)$، چندجمله‌ای‌های ناصفر و نسبت به هم اول ، روی $\mathbb{Z}_p$ باشند و فرض کنید $f(x) = f_۱(x) \cdots f_k(x)$، که در آن نشان دهید مرتبه‌ی $f(x)$ برابر کوچک‌ترین مضرب مشترک مرتبه‌ی $f_۱(x)$، ...، $f_k(x)$ است.

۲۱. مرتبه‌ی چندجمله‌ای‌های زیر را روی $\mathbb{Z}_۲$ بیابید.
(الف) $x^۸ + x^۷ + x^۳ + x + ۱$.
(ب) $x^{۲۷} + x^۵ + x^۲ + x + ۱$.
(ج) $(x^۳ + x + ۱)^۳(x^۲ + x + ۱)$.

۲۲. $I(۳, ۴; x)$ و $I(۲, ۶; x)$ را محاسبه کنید.

۲۳. $x^۴ + x^۳ + x^۲ - x - ۱$ را روی $\mathrm{GF}(۹)$ تجزیه کنید و با استفاده از آن چندجمله‌ای‌های اولیه روی $\mathrm{GF}(۹)$ را بیابید.

۲۴. اولین عدد p را بیابید که چندجمله‌ای $\dfrac{x^{۱۹} - ۱}{x - ۱}$ روی $\mathbb{Z}_p$ تحویل‌ناپذیر باشد.

۲۵. چندجمله‌ای تحویل‌ناپذیر $f(x) = x^۴ + x^۳ + x^۲ + ۲x + ۲ \in \mathbb{Z}_۳[x]$ با مرتبه‌ی ۸۰ را در نظر بگیرید. نشان دهید $f(x)$ روی $\mathbb{Z}_۳$ اولیه است.

۲۶. آیا چندجمله‌ای $x^{۲۸} + x^۳ + ۱$ روی $\mathbb{Z}_۲$ اولیه است؟

۴.۱۴ توسیع‌های جداپذیر

فرض کنید K میدان باشد. چندجمله‌ای $f(x) \in K[x]$ را روی K جداپذیر گوییم، هرگاه ریشه‌های هر عامل تحویل‌ناپذیر آن در توسیع تجزیه‌اش متمایز باشد، در غیر این صورت آن را جداناپذیر گوییم. فرض کنید $K : F$ توسیع دلخواه و $a \in F$ روی K جبری باشد. a را روی K جداپذیر گوییم هرگاه چندجمله‌ای می‌نیمال آن روی K جداپذیر باشد، در غیر این صورت آن را جداناپذیر می‌نامیم. در نهایت توسیع جبری $K : F$ را جداپذیر گوییم هرگاه هر عضو F روی K جداپذیر باشد، در غیر این صورت آن را جداناپذیر می‌نامیم.

مثال ۱.۴.۱۴. عوامل تحویل‌ناپذیر $f(x) = (x^۲ + ۱)^۲(x^۳ - ۲)^۳ \in \mathbb{Q}[x]$ عبارت‌اند از $x^۲ + ۱$ و $x^۳ - ۲$، که ریشه‌های این عوامل، متمایز هستند. بنابراین $f(x)$ یک چندجمله‌ای جداپذیر روی $\mathbb{Q}$ است. □

قضیه ۲.۴.۱۴. فرض کنید K یک میدان و $f(x) \in K[x]$ چندجمله‌ای تحویل‌ناپذیر باشد. اگر $K : F$ توسیع تجزیه‌ی $f(x)$ باشد، آن‌گاه ریشه‌های $f(x)$ در F متمایزند (یعنی $f(x)$ روی K جداپذیر است) اگر و تنها اگر $f'(x) \neq ۰$.

اثبات. ($\Longleftarrow$) فرض کنید $a \in F$ ریشه‌ای از $f(x)$ باشد. اگر $f'(x) = ۰$، آن‌گاه $f(a) = f'(a) = ۰$. بنابراین طبق قضیه‌ی ۹.۲.۱۴، a ریشه‌ی تکراری $f(x)$ است، که متناقض با فرض است. پس $f'(x) \neq ۰$.
($\Longrightarrow$) فرض کنید $a \in F$ یک ریشه‌ی تکراری از $f(x)$ باشد، در این صورت بنا به قضیه‌ی ۹.۲.۱۴، داریم $f(a) = f'(a) = ۰$. چون $f(x)$ در $K[x]$ تحویل‌ناپذیر است و $f'(x)$ را در $K[x]$ عاد نمی‌کند (زیرا $f'(x) \neq ۰$ و $\deg f'(x) < \deg f(x)$)، پس $f(x)$ و

$f'(x)$ در $K[x]$ نسبت به هم اول‌اند. در این جا می‌توان از مساله‌ی ۷ صفحه‌ی ۲۹۶ استفاده کرد و تناقض به دست آورد؛ اما بدون توجه به آن مساله عمل می‌کنیم. چون $f(x)$ و $f'(x)$ در $K[x]$ نسبت به هم اول هستند، $h(x), g(x) \in K[x]$ وجود دارند که $g(x)f(x) + h(x)f'(x) = ۱$. اکنون داریم

$$۱ = g(a)f(a) + h(a)f'(a) = g(a) \times ۰ + h(a) \times ۰ = ۰,$$

که تناقض است. □

نتیجه ۳.۴.۱۴. فرض کنید K میدان و $f(x) \in K[x]$ چندجمله‌ای تحویل‌ناپذیر باشد. در این صورت
(الف) اگر $\operatorname{char} K = ۰$، آنگاه $f(x)$ روی K جداپذیر است.
(ب) اگر $\operatorname{char} K = p$، آنگاه $f(x)$ روی K جداپذیر است اگر و تنها اگر چندجمله‌ای $g(x) \in K[x]$ وجود نداشته باشد که $f(x) = g(x^p)$.

اثبات. ابتدا توجه کنید که اگر $f(x) = k_۰ + k_۱x + \cdots + k_nx^n$، آنگاه

$$f'(x) = k_۱ + ۲k_۲x + \cdots + nk_nx^{n-۱} = ۰$$

اگر و تنها اگر برای هر $j \geq ۱$، $jk_j = ۰$
(الف) چون $\operatorname{char} K = ۰$، پس $jk_j = ۰$ اگر و تنها اگر $k_j = ۰$، $j \geq ۱$. بنابراین $f(x) = k_۰$، که خلاف تحویل‌ناپذیری $f(x)$ است. پس $f'(x) \neq ۰$. بنابراین طبق قضیه‌ی ۲.۴.۱۴، $f(x)$ روی K جداپذیر است.
(ب) چون $\operatorname{char} K = p$، پس $jk_j = ۰$ اگر و تنها اگر $k_j = ۰$ یا $p|j$. از این‌رو $f'(x) = ۰$ اگر و تنها اگر

$$\begin{aligned} f(x) &= k_۰ + k_{i_۱}x^{pm_۱} + k_{i_۲}x^{pm_۲} + \cdots + k_{i_r}x^{pm_r} \\ &= g(x^p), \end{aligned}$$

که در آن $g(x) = k_۰ + k_{i_۱}x^{m_۱} + \cdots + k_{i_r}x^{m_r}$. □

نتیجه ۴.۴.۱۴. اگر $\operatorname{char} K = ۰$ تمام چندجمله‌ای‌های در $K[x]$ جداپذیرند. □

توسیع $F : K$ را توسیع ساده گوییم هرگاه $a \in F$ وجود داشته باشد که $F = K(a)$.

قضیه ۵.۴.۱۴. اگر K میدان نامتناهی باشد و $F = K(a, b)$، که در آن a روی K جبری و b روی K جداپذیر است، آنگاه F توسیع ساده K است، یعنی $c \in F$ وجود دارد که $F = K(c)$.

اثبات. فرض کنید $p(x)$ و $q(x)$ چندجمله‌ای‌های می‌نیمال a و b روی K با درجه‌های n و m باشند. فرض کنید $a = a_۱$، $a_۲$، ...، a_n ریشه‌های $p(x)$ و $b = b_۱$، $b_۲$، ...، b_m ریشه‌های $q(x)$ در توسیعی از K باشند. چون b جداپذیر است، b_iها متمایزند. به علاوه چون K نامتناهی است، $k \in K$ وجود دارد که به ازای هر $۱ \leq i \leq n$ و $۲ \leq j \leq m$، $a - kb \neq a_i - kb_j$، یعنی $k \neq \dfrac{a_i - a}{b_j - b}$.
فرض کنید $c = a + kb$. در این صورت به ازای هر $۱ \leq i \leq n$، و هر $۲ \leq j \leq m$، $c - kb_j \neq a_i$. ثابت می‌کنیم $K(c) = K(a, b)$. به وضوح داریم $K(c) \subseteq K(a, b)$. حال فرض کنید $f(x) = p(c - kx) \in K(c)[x]$. داریم

$$f(b) = p(c - kb) = p(a) = ۰,$$

و b ریشه‌ی $f(x)$ در میدان $K(a, b)$ است. چون به ازای هر $۲ \leq j \leq m$،

$$f(b_j) = p(c - kb_j) \neq ۰,$$

b تنها ریشه‌ی مشترک $q(x)$ و $f(x)$ است. فرض کنید $d(x) \in K(c)[x]$ بزرگ‌ترین مقسوم علیه مشترک $q(x)$ و $f(x)$ باشد. چون $d(x)$ ترکیب خطی $q(x)$ و $f(x)$ است، b ریشه‌ای از $d(x)$ نیز هست. از طرف دیگر چون $d(x)|q(x)$ و $d(x)|f(x)$، پس ریشه‌ی $d(x)$ نیز ریشه‌ای از $q(x)$ و $f(x)$ هست. چون $q(x)$ و $f(x)$ ریشه‌ی مشترکی جز b ندارند، درجه‌ی $d(x)$ برابر ۱ است و $d(x) = x - b$.
چون $d(x) \in K(c)[x]$، $b \in K(c)$. بنابراین $a = c + kb \in K(c)$ و $K(a, b) \subseteq K(c)$. در نتیجه $K(a, b) = K(c)$. □

نتیجه ۶.۴.۱۴. فرض کنید K میدان نامتناهی باشد و $F = K(a_۱, a_۲, \ldots, a_n)$، که در آن $a_۱$ روی K جبری و $a_۲$، $a_۳$، $\ldots$، a_n روی K جداپذیرند. در این صورت عضو $c \in F$ وجود دارد که $F = K(c)$. یعنی $K : K(a_۱, \ldots, a_n)$ توسیع ساده است.

اثبات. به استقرا روی n و با استفاده از قضیه‌ی ۵.۴.۱۴، حکم به سادگی به دست می‌آید. □

نتیجه ۷.۴.۱۴. فرض کنید $F : K$ توسیع باشد و $\operatorname{char} K = ۰$. اگر $a_۱$، $\ldots$، a_n روی K جبری باشند، آنگاه $K(a_۱, \ldots, a_n) : K$ توسیع ساده است. □

مثال ۸.۴.۱۴. توسیع $\mathbb{Q}(\sqrt{۲}, \sqrt{۳}) : \mathbb{Q}$ را در نظر بگیرید. قرار می‌دهیم $a = \sqrt{۲}$ و $b = \sqrt{۳}$. چندجمله‌ای‌های می‌نیمال a و b، به ترتیب، عبارت‌اند از $p(x) = x^۲ - ۲$ و $q(x) = x^۲ - ۳$. پس $a_۱ = \sqrt{۲}$، $a_۲ = -\sqrt{۲}$، و $b_۱ = \sqrt{۳}$، $b_۲ = -\sqrt{۳}$. عبارت $\dfrac{a_i - a}{b_j - b}$ در اثبات قضیه‌ی ۵.۴.۱۴، یا برابر ۰ است یا برابر $-\dfrac{\sqrt{۲}}{\sqrt{۳}}$. اگر قرار دهیم $k = ۱$، اثبات قضیه‌ی ۵.۴.۱۴، نشان می‌دهد $\mathbb{Q}(\sqrt{۲}, \sqrt{۳}) = \mathbb{Q}(\sqrt{۲} + \sqrt{۳})$. نشان دادن این مطلب به صورت مستقیم نیز ساده است. □

تمرین‌ها

۱. a را طوری بیابید که $F = \mathbb{Q}(a)$
(الف) $F = \mathbb{Q}(\sqrt{۳}, \sqrt{۷})$ (ب) $F = \mathbb{Q}(i, \sqrt{۵})$

۲. فرض کنید p و q اعداد صحیحی باشند که $\sqrt{p}, \sqrt{q} \notin \mathbb{Q}$. نشان دهید

$$\mathbb{Q}(\sqrt{p}, \sqrt{q}) = \mathbb{Q}(\sqrt{p} + \sqrt{q}).$$

۳. نشان دهید $\mathbb{Q}(\sqrt{p}, \sqrt{q}, \sqrt{r}) = \mathbb{Q}(\sqrt{p} + \sqrt{q} + \sqrt{r})$، که در آن p، q، و r اعداد اول متمایزند.

۴. فرض کنید $F = K(t)$، میدان کسرهای $K[t]$ باشد (t یک متغیر). نشان دهید $x^۲ - t$ روی F تحویل‌ناپذیر است، اما اگر $\operatorname{char} K = ۲$، جداپذیر نیست.

۵. فرض کنید $F : K$ توسیع متناهی باشد و $\operatorname{char} K = p$. اگر p، $[F : K]$ را عاد نکند. نشان دهید $F : K$ توسیع جداپذیر است.

۶. کدام چندجمله‌ای‌ها روی میدان داده شده جداپذیرند
(الف) $x^۲ - ۶x + ۱$ روی $\mathbb{Q}$ (ب) $x^۴ + x^۲ + ۱$ روی $\mathbb{Z}_۲$.

۵.۱۴ گروه گالوای توسیع

فرض کنید $F : K$ و $L : K$ توسیع هستند. همریختی $\alpha : F \longrightarrow L$ را K- همریختی گوییم، هرگاه هر عضو K را ثابت نگه دارد، یعنی به ازای هر $k \in K$، $\alpha(k) = k$. چون α همریختی ناصفر است، $\ker \alpha \neq F$. به علاوه چون $\{۰\}$ و F تنها ایدآل‌های میدان F است، $\ker \alpha = \{۰\}$ و α یک‌به‌یک است. بنابراین $\alpha : F \longrightarrow \operatorname{Im} \alpha$ یکریختی است. اگر $L = F = \operatorname{Im} \alpha$، گوییم α، K- خودریختی است. مجموعه‌ی K- خودریختی‌های F را با $\operatorname{Aut}_K F$ (یا $G(F : K)$ یا $\operatorname{Gal}(F : K)$) نشان می‌دهیم و آن را گروه گالوای توسیع $F : K$ گوییم. به سادگی می‌توان دید که $\operatorname{Aut}_K F$ زیرگروهی از $\operatorname{Aut} F$ است (تمرین ۱ را ببینید.) در صورتی که $F : K$ توسیع تجزیه برای چندجمله‌ای $f(x) \in K[x]$ باشد، گروه گالوای $F : K$ را گروه گالوای $f(x)$ می‌نامیم و گاهی اوقات با $\operatorname{Gal}_K(f)$ نشان می‌دهیم. اگر $\alpha, \beta \in \operatorname{Aut} F$، معمولاً به‌جای $\alpha \circ \beta$ می‌نویسیم $\alpha\beta$.

مثال ۱.۵.۱۴. به ازای هر میدان K داریم $\operatorname{Aut}_K K = \{\mathrm{id}_K\}$. □

اگر $f(x)=k_۰+k_۱x+k_۲x^۲+\cdots+k_nx^n\in K[x]$ و $a\in F$، آنگاه به ازای هر $\alpha\in \mathrm{Aut}_K F$ داریم

$$\begin{aligned} f(\alpha(a)) &= k_۰+k_۱\alpha(a)+k_۲\alpha(a)^۲+\cdots+k_n\alpha(a)^n \\ &= \alpha(k_۰)+\alpha(k_۱)\alpha(a)+\alpha(k_۲)\alpha(a)^۲+\cdots+\alpha(k_n)\alpha(a)^n \\ &= \alpha(k_۰+k_۱a+k_۲a^۲+\cdots+k_na^n) \\ &= \alpha(f(a)). \end{aligned}$$

به ویژه اگر a ریشه‌ای از $f(x)$ باشد، آنگاه $f(\alpha(a))=\alpha(f(a))=\alpha(۰)=۰$ و $\alpha(a)$ نیز ریشه‌ای از $f(x)$ است.

مثال ۲.۵.۱۴. فرض کنید $K(a):K$ توسیع ساده و a روی K جبری با چندجمله‌ای مینیمال $f(x)\in K[x]$ باشد. اگر $a_۱=a$، $a_۲$، ...، a_m ریشه‌های متمایز $f(x)$ باشند که در $K(a)$ قرار دارند، نشان دهید

$$\mathrm{Aut}_K K(a)=\{\alpha_۱,\alpha_۲,\ldots,\alpha_m\}$$

که در آن به ازای هر $۱\le j\le m$، α_j یکتا K- همریختی $\alpha_j:K(a)\longrightarrow K(a)$ است که $\alpha_j(a)=a_j$.

حل طبق فرض برای هر $۱\le j\le m$، داریم $a_j\in K(a)$؛ بنابراین $K(a_j)\subseteq K(a)$. چون $[K(a_j):K]=\deg f(x)=[K(a):K]$، $K(a_j)=K(a)$. برای هر $۱\le j\le m$ یکریختی همانی $\mathrm{id}_K:K\longrightarrow K$ را در نظر می‌گیریم. بنا به قضیه‌ی ۶.۲.۱۴ یکریختی یکتای $\alpha_j:K(a)\longrightarrow K(a_j)=K(a)$ وجود دارد که $\alpha_j(a)=a_j$ اکنون اگر $\gamma\in \mathrm{Aut}_K K(a)$، آنگاه $\gamma(a)$ ریشه‌ای از $f(x)$ است. پس $۱\le j\le m$ وجود دارد که $\gamma(a)=a_j=\alpha_j(a)$ و بنا به یکتایی α_j داریم $\gamma=\alpha_j$. از این‌رو $\mathrm{Aut}_K K(a)=\{\alpha_۱,\alpha_۲,\ldots,\alpha_m\}$. □

قضیه ۳.۵.۱۴. فرض کنید $F:K$ توسیع جبری باشد. اگر $\alpha:F\longrightarrow F$ یک K- همریختی باشد، آنگاه α خودریختی است.

اثبات. باید نشان دهیم α پوشاست. فرض کنید $a\in F$. چون a روی F جبری است. چندجمله‌ای $f(x)\in K[x]$ وجود دارد که $f(a)=۰$. فرض کنید $a=a_۱$، $a_۲$، ...، a_r ریشه‌های $f(x)$ هستند که در F قرار دارند. قرار می‌دهیم $L=K(a_۱,a_۲,\ldots,a_r)$. در این صورت، بنا به قضیه‌ی ۲۰.۱.۱۴، $L:K$ توسیع متناهی است. چون α هر ریشه‌ی $f(x)$ را به ریشه‌ای از $f(x)$ نظیر می‌کند، $\alpha(L)\subseteq L$ (تمرین ۲ را ببینید). بنا به قانون برج داریم

$$[L:K]=[L:\alpha(L)][\alpha(L):K].$$

چون $L\cong\alpha(L)$، $[L:K]=[\alpha(L):K]$ و $[L:\alpha(L)]=۱$؛ که نتیجه می‌دهد $L=\alpha(L)$. از این‌رو $a\in L=\alpha(L)\subseteq\alpha(F)$. بنابراین α پوشاست. □

قضیه ۴.۵.۱۴. فرض کنید $f(x)\in K[x]$ چندجمله‌ای جداپذیر روی K و $\alpha:K\longrightarrow L$ یکریختی باشد. اگر $F:K$ توسیع تجزیه‌ی $f(x)$ و $E:L$ توسیع تجزیه‌ی $\alpha(f(x))$ باشند، آنگاه دقیقاً $[F:K]$ یکریختی $\bar\alpha:F\longrightarrow E$ وجود دارند که توسیع α هستند.

اثبات. چون $f(x)$ روی $F[x]$ تجزیه می‌شود، اعضای $a_۱,a_۲,\ldots,a_m\in F$ و $k\in K$ وجود دارند که

$$f(x)=k(x-a_۱)\cdots(x-a_m).$$

به استقرا روی $n=[F:K]$ قضیه را ثابت می‌کنیم. اگر $n=۱$، آنگاه $F=K$. بنابراین $a_۱,a_۲,\ldots,a_m\in K$ و هم‌چنین $\alpha(f(x))=\alpha(k)(x-\alpha(a_۱))\cdots(x-\alpha(a_m))$. پس $\alpha(f(x))$ روی L تجزیه می‌شود و $L=E$. در این حالت تنها α توسیع α است.

حال فرض کنید $n>۱$ و قضیه برای همه‌ی توسیع‌های با درجه‌ی کمتر از n برقرار است. چون $K\subset F=K(a_۱,\ldots,a_m)$، $۱\le j\le m$ وجود دارد که $a_j\notin K$. با تعویض ترتیب اندیس‌ها فرض می‌کنیم $j=۱$؛ پس $a_۱\notin K$. فرض کنید $p(x)\in K[x]$ چندجمله‌ای مینیمال $a_۱$ روی K باشد، پس $\deg p(x)=t\ge ۲$. چون ریشه‌های $p(x)$ در F متمایزند، ریشه‌های $\alpha(p(x))$ نیز در E

متمایزند. بنابراین $\alpha(p(x))$ دقیقاً t ریشه‌ی $b_1, \dots, b_t \in E$ دارد. بنا به قضیه‌ی ۶.۲.۱۴، یکریختی یکتای $\beta_i : K(a_1) \longrightarrow L(b_i)$، به ازای هر $1 \leq i \leq t$، وجود دارد که توسیع α است و $\beta_i(a_1) = b_i$. توجه کنید β_1، ...، β_t تنها توسیع‌های متمایز α هستند زیرا اگر γ یک توسیع α باشد، آنگاه

$$\alpha(p(\gamma(a_1))) = \gamma(p(a_1)) = \gamma(0) = 0,$$

یعنی $\gamma(a_1)$ ریشه‌ای از $\alpha(p(x))$ است. پس $1 \leq i \leq t$ وجود دارد که

$$\gamma(a_1) = b_i = \beta_i(a_1).$$

از این‌رو بنا به یکتایی β_i، داریم $\gamma = \beta_i$.
اکنون می‌خواهیم فرض استقرا را برای توسیع $F : K(a_1)$ به کار ببریم. چون

$$n = [F : K] = [F : K(a_1)][K(a_1) : K],$$

داریم $[F : K(a_1)] < n$ و $t[F : K(a_1)] = [F : K]$. چون عوامل تحویل‌ناپذیر $f(x)$ در $K(a_1)[x]$، عوامل تحویل‌ناپذیر $f(x)$ در $K[x]$ را عدد می‌کنند، $f(x)$ روی $K(a_1)$ نیز جداپذیر است. بنابراین طبق فرض استقرا تعداد $[F : K(a_1)] = \dfrac{[F : K]}{t}$ یکریختی $\beta : F \longrightarrow E$ وجود دارند که توسیع β_1 هستند. به وضوح هر یک از این یکریختی‌ها توسیع α نیز هستند. چون تعداد β_iها برابر t است، پس تعداد یکریختی‌های $\beta : F \longrightarrow E$ که توسیع α هستند برابر $t[F : K(a_1)] = [F : K]$ است. □

نتیجه ۵.۵.۱۴. اگر $F : K$ توسیع تجزیه‌ی چندجمله‌ای جداپذیر $f(x) \in K[x]$ باشد، آنگاه داریم $|\mathrm{Aut}_K F| = [F : K]$. □

قضیه ۶.۵.۱۴. فرض کنید $f(x) \in K[x]$ یک چندجمله‌ای غیرثابت و $F : K$ توسیع تجزیه‌ی $f(x)$ روی K باشد. اگر $X = \{a \in F \mid f(a) = 0\}$، مجموعه‌ی ریشه‌های $f(x)$ در F باشد، آنگاه $\mathrm{Aut}_K F$ روی X با $\alpha \cdot a = \alpha(a)$ به صورت صادقانه عمل می‌کند؛ بنابراین $\mathrm{Aut}_K F$ با زیرگروهی از S_n یکریخت است، که در آن $n = |X|$. در حالتی که $f(x)$ تحویل‌ناپذیر باشد، عمل $\mathrm{Aut}_K F$ روی X ترایا است.

اثبات. ابتدا توجه کنید برای هر $\alpha \in \mathrm{Aut}_K F$ و $a \in X$، $\alpha(a) \in X$، یعنی $\alpha(a)$ ریشه‌ای از $f(x)$ است، زیرا $f(\alpha(a)) = \alpha(f(a)) = f(0) = 0$. اکنون اگر id_F، K- خودریختی همانی باشد، چون $\mathrm{id}_F(a) = a$، داریم $\mathrm{id}_F \cdot a = a$؛ به علاوه چون $(\alpha\beta)(a) = \alpha(\beta(a))$، داریم $(\alpha\beta) \cdot a = \alpha \cdot (\beta \cdot a)$. از این‌رو $\mathrm{Aut}_K F$ روی X عمل می‌کند.
حال اگر $\alpha \in \mathrm{Aut}_K F$ و به ازای هر $a \in X$، $\alpha \cdot a = a$، آنگاه به ازای هر $a \in X$، $\alpha(a) = a$. چون $F = K(X)$ و α، K را نیز ثابت نگه میدارد ، $\alpha = \mathrm{id}_F$ همانی است. بنابراین عمل $\mathrm{Aut}_K F$ روی X صادق است.
اکنون ثابت می‌کنیم وقتی که $f(x)$ تحویل‌ناپذیر باشد، این عمل ترایا است. فرض کنید a و b دو ریشه‌ی $f(x)$ باشند. یکریختی همانی $\mathrm{id}_K : K \longrightarrow K$ را در نظر می‌گیریم. طبق قضیه‌ی ۶.۲.۱۴، یکریختی یکتای $\alpha : K(a) \longrightarrow K(b)$ وجود دارد که توسیع id_K است و $\alpha(a) = b$. چون $F : K(a)$ توسیع تجزیه‌ی $f(x)$ روی $K(a)$ و $F : K(b)$ توسیع تجزیه‌ی $f(x)$ روی $K(b)$ است، بنا به قضیه‌ی ۷.۲.۱۴، یکریختی $\beta : F \longrightarrow F$ وجود دارد که توسیع α است. بنابراین $\beta \in \mathrm{Aut}_K F$ و $\beta(a) = b$. از این رو $\beta \cdot a = b$. پس عمل $\mathrm{Aut}_K F$ روی X ترایا است. □

مثال ۷.۵.۱۴. چندجمله‌ای می‌نیمال i روی $\mathbb{R}$ برابر $f(x) = x^2 + 1$ است، بنابراین $[\mathbb{R}(i) : \mathbb{R}] = 2$. اکنون چون مجموعه‌ی ریشه‌های $f(x)$ برابر $X = \{i, -i\}$ است، $\mathrm{Aut}_{\mathbb{R}}\mathbb{C} = \{\mathrm{id}_{\mathbb{C}}, \alpha\}$، که در آن $\alpha : \mathbb{C} \longrightarrow \mathbb{C}$، $\alpha(i) = -i$. به ازای هر $a, b \in \mathbb{R}$ داریم $\alpha(a + ib) = \alpha(a) + \alpha(i)\alpha(b) = a - ib$. □

مثال ۸.۵.۱۴. اگر p عدد اول باشد و $a = e^{\frac{2\pi i}{p}}$ ، آنگاه $\mathrm{Aut}_{\mathbb{Q}}\mathbb{Q}(a) \cong \mathbb{Z}_p^\times$.

حل چون a ریشه‌ی چندجمله‌ای $x^p - 1 = (x - 1)(x^{p-1} + x^{p-2} + \cdots + 1)$ است و $a \neq 1$، پس a ریشه‌ی چندجمله‌ای $f(x) = x^{p-1} + x^{p-2} + \cdots + 1$ است. طبق قضیه‌ی ۲۰.۲.۱۱ از صفحه‌ی ۲۴۴، $f(x)$ روی $\mathbb{Q}$ تحویل‌ناپذیر است. از این رو $|\mathrm{Aut}_{\mathbb{Q}}\mathbb{Q}(a)| = [\mathbb{Q}(a) : \mathbb{Q}] = p - 1$ (توجه کنید چون $\mathrm{char}\,\mathbb{Q} = 0$، ریشه‌های $f(x)$ متمایزند). فرض کنید $\overline{m}$ مولدی از گروه ضربی دوری $\mathbb{Z}_p^\times$ باشد. ادعا می‌کنیم $\alpha \in \mathrm{Aut}_{\mathbb{Q}}\mathbb{Q}(a)$ با $\alpha(a) = a^m$ مولد i از $\mathrm{Aut}_{\mathbb{Q}}\mathbb{Q}(a)$ است. فرض کنید $\beta \in \mathrm{Aut}_{\mathbb{Q}}\mathbb{Q}(a)$.

در این صورت $1 \leq t \leq p-1$ وجود دارد که $\beta(a) = a^t$. اکنون $1 \leq r \leq p-1$ وجود دارد که $\overline{m}^r = \overline{t}$. بنابراین $m^r \equiv t \mod p$ و

$$\alpha^r(a) = a^{m^r} = a^t = \beta(a).$$

در نتیجه $\beta = \alpha^r$. از این‌رو $\mathrm{Aut}_{\mathbb{Q}}\mathbb{Q}(a) = \langle \alpha \rangle \cong \mathbb{Z}_p^\times$. □

مثال ۹.۵.۱۴. اگر p عدد اول باشد و $F = \mathrm{GF}(p^n)$، نشان دهید $\mathrm{Aut}_{\mathbb{Z}_p} F \cong C_n$، که در آن طبق معمول $\mathbb{Z}_p$ را با زیرمیدان یکریخت آن در F یکی گرفته‌ایم.

حل چون $F^\times$ دوری است، عضو ناصفر $a \in F$ وجود دارد که $F^\times = \langle a \rangle$. از این‌رو $F = \mathbb{Z}_p(a)$. چون $F : \mathbb{Z}_p$ توسیع تجزیه‌ی $f(x) = x^{p^n} - x$ روی $\mathbb{Z}_p$ و $f(x)$ روی $\mathbb{Z}_p$ جداپذیر است، $|\mathrm{Aut}_{\mathbb{Z}_p} F| = [F : \mathbb{Z}_p] = n$. ثابت می‌کنیم خودریختی فروبنیوس $\alpha : F \longrightarrow F$ با $\alpha(a) = a^p$، مولد $\mathrm{Aut}_{\mathbb{Z}_p} F$ است. چون a^p ریشه‌ای از $f(x)$ است، $\alpha \in \mathrm{Aut}_{\mathbb{Z}_p} F$. به ازای هر $k \geq 1$ داریم $\alpha^k(a) = a^{p^k}$. پس اگر $\alpha^k = \mathrm{id}_F$، آنگاه هر عضو F ریشه‌ای از $x^{p^k} - x$ است. بنابراین $k \geq n$ و مرتبه‌ی α برابر n است و $\mathrm{Aut}_{\mathbb{Z}_p} F = \langle \alpha \rangle \cong C_n$. □

مثال ۱۰.۵.۱۴. گروه گالوای توسیع تجزیه‌ی $f(x) = (x^2 - 2)(x^2 - 3) \in \mathbb{Q}[x]$ را محاسبه کنید.

حل داریم

$$f(x) = (x - \sqrt{2})(x + \sqrt{2})(x - \sqrt{3})(x + \sqrt{3}).$$

بنابراین $f(x)$ روی $F = \mathbb{Q}(u, -u, v, -v) = \mathbb{Q}(u, v)$ تجزیه می‌شود و $F : \mathbb{Q}$ توسیع تجزیه‌ی $f(x)$ است، که در آن $u = \sqrt{2}$ و $v = \sqrt{3}$. چندجمله‌ای $x^2 - 2$، چندجمله‌ای می‌نیمال $u = \sqrt{2}$ روی $\mathbb{Q}$ است. بنابراین داریم $[\mathbb{Q} : \mathbb{Q}(u)] = 2$. از طرف دیگر ریشه‌های چندجمله‌ای $x^2 - 3$ عبارت‌اند از $\pm v$ که در $\mathbb{Q}(u)$ قرار ندارند. پس $x^2 - 3$ روی $\mathbb{Q}(u)$ تحویل‌ناپذیر است. بنابراین $[\mathbb{Q}(u)(v) : \mathbb{Q}(u)] = 2$ و بنا به قانون برج

$$[F : \mathbb{Q}] = [F : \mathbb{Q}(u)][\mathbb{Q}(u) : \mathbb{Q}] = 2 \times 2 = 4.$$

چون $F : \mathbb{Q}$ توسیع تجزیه‌ی چندجمله‌ای جداپذیر $f(x)$ است، بنا به نتیجه‌ی ۵.۵.۱۴، داریم $|\mathrm{Aut}_{\mathbb{Q}} F| = [F : \mathbb{Q}] = 4$. بنا به قضیه‌ی ۶.۵.۱۴، هر $\mathbb{Q}$ خودریختی F،یک جایگشت روی $X = \{u, -u, v, -v\}$ است، و ریشه‌های هر عامل تحویل‌ناپذیر $f(x)$ را به ریشه‌های همان عامل تحویل‌ناپذیر می‌برد؛ در واقع $\mathrm{Aut}_{\mathbb{Q}} F$ روی مجموعه‌ی ریشه‌های عوامل تحویل‌ناپذیر $f(x)$ به صورت ترایا عمل می‌کند. خودریختی‌های $\alpha, \beta \in \mathrm{Aut}_{\mathbb{Q}} F$ را با $\alpha(u) = -u$، $\alpha(v) = v$ و $\beta(u) = u$، $\beta(v) = -v$ را در نظر می‌گیریم. داریم

$$\alpha^2(u) = \alpha(-u) = u, \quad \alpha^2(v) = \alpha(v) = v$$

و

$$\beta^2(u) = \beta(u) = u, \quad \beta^2(-v) = \beta(-v) = v.$$

بنابراین $O(\beta) = O(\alpha) = 2$. به علاوه چون

$$\alpha\beta(u) = \alpha(u) = -u = -\beta(u) = \beta(-u) = \alpha(\beta(u))$$

و

$$\alpha\beta(v) = \alpha(-v) = -v = \beta(v) = \beta\alpha((v)),$$

داریم $\alpha\beta = \beta\alpha$. در نتیجه $\mathrm{Aut}_{\mathbb{Q}} F = \langle \alpha, \beta \rangle \cong C_2 \times C_2$. □

مثال ۱۱.۵.۱۴. گروه گالوای توسیع تجزیه‌ی $x^3 - 2 \in \mathbb{Q}[x]$ را بیابید.

حل فرض کنید F توسیع تجزیه‌ی چندجمله‌ای $x^۳-۲$ روی $\mathbb{Q}$ باشد، طوری که $F\subseteq\mathbb{C}$. فرض کنید $w=e^{۲\pi i/۳}$ یک ریشه‌ی اولیه‌ی واحد باشد. اگر a ریشه‌ای از $x^۳-۲$ و $u=\sqrt[۳]{۲}$، آنگاه

$$a^۳=۲\Longrightarrow\left(\frac{a}{\sqrt[۳]{۲}}\right)^۳=۱\Longrightarrow\frac{a}{u}=۱,\ \ w,\ \ w^۲\Longrightarrow a=u,\ \ uw,\ \ uw^۲.$$

بنابراین $F=\mathbb{Q}(u,uw,uw^۲)=\mathbb{Q}(u,w)$ میدان تجزیه‌ی برای $x^۳-۲$ است. چندجمله‌ای می‌نیمال w روی $\mathbb{Q}$ عبارت است از $x^۲+x+۱$. پس $[\mathbb{Q}(w):\mathbb{Q}]=۲$ و $\{۱,w\}$ پایه‌ای برای $\mathbb{Q}(w)$ روی $\mathbb{Q}$ است. چون ریشه‌های $x^۳-۲$ عبارت‌اند از u، uw و $uw^۲$ و هیچ‌کدام از ریشه‌ها در $\mathbb{Q}(w)$ قرار ندارند (ترکیب خطی از ۱ و w نیستند)، $x^۳-۲$ روی $\mathbb{Q}(w)$ ریشه‌ی ندارد ، و چون $\deg(x^۳-۲)=۳$، باید روی $\mathbb{Q}(w)$ تحویل‌ناپذیر باشد. بنابراین $[\mathbb{Q}(w)(\sqrt[۳]{۲}):\mathbb{Q}(w)]=۳$ و $\{۱,u,u^۲\}$ پایه‌ای برای $\mathbb{Q}(w)(u)$ روی $\mathbb{Q}(w)$ است. بنا به قانون برج

$$[F:\mathbb{Q}]=[F:\mathbb{Q}(w)][\mathbb{Q}(w):\mathbb{Q}]=۳\times۲=۶.$$

اعضای $\operatorname{Aut}_{\mathbb{Q}}F$ را می‌یابیم. بنا به قضیه‌ی ۶.۵.۱۴، هر $\mathbb{Q}$ خودریختی F،یک جایگشت روی $X=\{u,uw,uw^۲\}$ است، و ریشه‌های هر عامل تحویل‌ناپذیر $f(x)$ را به ریشه‌های همان عامل تحویل‌ناپذیر می‌برد؛ در واقع $\operatorname{Aut}_{\mathbb{Q}}F$ روی مجموعه‌ی ریشه‌های عوامل تحویل‌ناپذیر $f(x)$ به صورت ترایا عمل می‌کند. خودریختی‌های $\alpha,\beta\in\operatorname{Aut}_{\mathbb{Q}}F$ را با $\alpha(uw)=uw$، $\alpha(u)=uw^۲$ و $\beta(u)=uw$ و $\beta(uw)=uw^۲$ در نظر می‌گیریم. توجه کنید چون

$$uw=\alpha(uw)=\alpha(u)\alpha(w)=uw^۲\alpha(w),$$

داریم $\alpha(w)=w^۲$. هم‌چنین چون

$$uw^۲=\beta(uw)=\beta(u)\beta(w)=uw\beta(w),$$

داریم $\beta(w)=w$. چون

$$\alpha^۲(u)=\alpha(uw^۲)=uw^۲w^۴=u,\quad \alpha^۲(w)=\alpha(w^۲)=w^۴=w$$

و

$$\beta^۳(u)=\beta^۲(uw)=\beta(uw^۲)=uw^۳=u,\quad \beta^۳(w)=w,$$

داریم $O(\alpha)=۲$ و $O(\beta)=۳$. چون $F:\mathbb{Q}$ توسیع تجزیه برای چندجمله‌ای جداپذیر $x^۳-۲$ است، بنا به نتیجه‌ی ۵.۵.۱۴، $|\operatorname{Aut}_{\mathbb{Q}}F|=[F:\mathbb{Q}]=۶$. به علاوه چون $\operatorname{Aut}_{\mathbb{Q}}F=\langle\alpha,\beta\rangle\cong S_۳$ آبلی نیست، داریم $\operatorname{Aut}_{\mathbb{Q}}F$. □

برای تعیین گروه گالوای برخی از چندجمله‌ای‌هایی که درجه‌شان عدد اول است، به قضیه‌ی بعدی نیاز داریم.

قضیه ۱۲.۵.۱۴. فرض کنید p عدد اول باشد و $G\leq S_p$. اگر G شامل یک p- دور و یک ترانهش باشد، آنگاه $G=S_p$.

اثبات. فرض کنید $\alpha=(a_۱\ a_۲\ \cdots\ a_p)$، $\beta=(a_۱\ a_k)$ دورهای داده شده در G هستند. چون p عدد اول است، $\alpha^{k-۱}$ یک p- دور است و به علاوه $\alpha^{k-۱}(a_۱)=a_k$. بنابراین $\sigma=(b_۱\ b_۲\ \cdots\ b_p)$ و $\gamma=(b_۱\ b_۲)$ در G قرار دارند. به ازای هر j، $۰\leq j\leq p-۱$

$$\sigma^j\gamma\sigma^{-j}=(\sigma^j(b_۱)\ \sigma^j(b_۲))=(b_{j+۱}\ b_{j+۲})\in G.$$

اکنون به استقرا ثابت می‌کنیم به ازای هر $۲\leq j\leq p$، $(b_۱\ b_j)\in G$. برای $j=۲$، $(b_۱\ b_۲)=\gamma\in G$. اگر $(b_۱\ b_j)\in G$، آنگاه چون $(b_j\ b_{j+۱})\in G$،

$$(b_۱\ b_{j+۱})=(b_۱\ b_j)(b_j\ b_{j+۱})(b_۱\ b_j)\in G.$$

پس به ازای هر $۲\leq j\leq p$، $(b_۱\ b_j)\in G$. چون این ترانهش‌ها S_p را تولید می‌کنند، داریم $G=S_p$. □

قضیه ۱۳.۵.۱۴. فرض کنید p یک عدد اول و $f(x) \in \mathbb{Q}[x]$ یک چندجمله‌ای تحویل‌ناپذیر روی $\mathbb{Q}$ باشد که $\deg f(x) = p$. اگر $f(x)$ دقیقاً $p-2$ ریشه‌ی حقیقی و دو ریشه‌ی مختلط داشته باشد، آنگاه گروه گالوای $f(x)$ روی $\mathbb{Q}$ با S_p یکریخت است.

اثبات. فرض کنید $F \subseteq \mathbb{C}$، و $F : \mathbb{Q}$ توسیع تجزیه‌ی $f(x)$ و $G = \operatorname{Aut}_{\mathbb{Q}} F$ گروه گالوای این توسیع باشد. اکنون $|G| = [F : \mathbb{Q}]$ و $p|[F : \mathbb{Q}]$. چون اعضای G جایگشت‌های ریشه‌های $\{a_1, a_2, \ldots, a_p\}$ از $f(x)$ هستند و $p \mid |G|$، G عضوی از مرتبه‌ی p دارد ، که لزوماً یک p- دور است. فرض کنید $a_1 = a + ib$ و $a_2 = a - ib$ دو ریشه‌ی مختلط $f(x)$ باشند. فرض کنید $\alpha : \mathbb{C} \to \mathbb{C}$ خودریختی $\mathbb{C}$ باشد که هر عضو را به مزدوج خود تصویر می‌کند. در این صورت چون $F = \mathbb{Q}(a_1, a_2, \ldots, a_p)$ و $\alpha(a_1) = a_2$، $\alpha(a_2) = a_1$ و $\alpha(a_i) = a_i$، $3 \leq i \leq p$، داریم $\alpha(F) = F$. پس $\alpha|_F \in G$. چون α^2 خودریختی همانی است، پس G عضوی از مرتبه‌ی ۲ نیز دارد. از این‌رو بنا به قضیه‌ی ۱۲.۵.۱۴، $G \cong S_p$. □

در مثال بعدی از دو نتیجه استاندارد آنالیز مقدماتی یعنی قضیه‌ی مقدار میانی و قضیه‌ی استفاده می‌کنیم.

مثال ۱۴.۵.۱۴. نشان دهید گروه گالوای چندجمله‌ای $f(x) = 3x^5 - 15x - 5 \in \mathbb{Q}[x]$ روی $\mathbb{Q}$ برابر S_5 است.

حل بنا به محک آیزنشتاین با $p = 5$، $f(x)$ روی $\mathbb{Q}$ تحویل‌ناپذیر است. داریم

$$f(2) = 61 > 0, \quad f(0) = -5 < 0, \quad f(-1) = 7 > 0, \quad f(-2) = -86 < 0.$$

پس ، بنابه قضیه‌ی مقدار میانی، $f(x)$ حداقل سه ریشه‌ی حقیقی r_1، r_3، r_3 دارد که $-2 < r_1 < -1 < r_2 < 0 < r_3 < 2$. از طرف دیگر چون $f'(x) = 15(x^4 - 1)$ فقط دو ریشه‌ی حقیقی دارد ، بنا به قضیه‌ی $f(x)$ حداکثر سه ریشه‌ی حقیقی دارد. از این‌رو $f(x)$ دقیقاً سه ریشه‌ی حقیقی و دو ریشه‌ی مختلط دارد. پس بنا به قضیه‌ی ۱۳.۵.۱۴، گروه گالوای $f(x)$ برابر S_5 است. □

این بخش را با توصیف گروه گالوای توسیع تجزیه‌ی چندجمله‌ای‌های $x^n - 1$ و $x^n - a$ به پایان می‌بریم. ابتدا قدری مقدمه و یادآوری لازم است. فرض کنید $F : K$ توسیع تجزیه‌ی چندجمله‌ای $f(x) = x^n - 1 \in K[x]$ باشد. چون $F^\times$ یک گروه آبلی است، مجموعه‌ی متشکل از همه‌ی ریشه‌های $f(x)$ در F، یعنی

$$G = \{a \in F^\times \mid a^n = 1\}$$

یک زیرگروه $F^\times$ است. چون $f(x) = x^n - 1 \in K[x]$ حداکثر n ریشه در F دارد ، G گروه متناهی است. در نتیجه بنا به قضیه‌ی ۱۵.۱.۱۱، از صفحه‌ی ۲۳۶، G دوری است. هر عضو G را یک ریشه‌ی nام واحد و هر مولد G با مرتبه‌ی n را یک ریشه‌ی nام اولیه‌ی واحد روی K گوییم. اگر $\operatorname{char} F \nmid n$ (صفر، n را عاد نمی‌کند)، آنگاه $f'(x) = nx^{n-1} \neq 0$. بنابراین، بنا به قضیه‌ی ۲.۴.۱۴، $f(x)$، n ریشه‌ی متمایز دارد. بنابراین اگر $\operatorname{char} F \nmid n$، آنگاه $|G| = n$؛ در این حالت تعداد مولدهای G برابر $\varphi(n)$ است، که در آن φ تابع فی اویلر است؛ در نتیجه $\varphi(n)$ ریشه‌ی nام اولیه‌ی واحد وجود دارد. اگر a یک ریشه‌ی nام اولیه‌ی واحد باشد، آنگاه $G = \langle a \rangle$ و $F = K(a)$. قضیه‌ی بعد تعمیم مثال ۸.۵.۱۴ است.

قضیه ۱۵.۵.۱۴. فرض کنید K میدان باشد و $n \in \mathbb{N}$. در این صورت یک ریشه‌ی اولیه‌ی nام واحد w روی K وجود دارد اگر و تنها اگر $\operatorname{char} K \nmid n$. در این حالت

(الف) $K(w) : K$ توسیع تجزیه‌ی $x^n - 1$ است.

(ب) $\operatorname{Aut}_K K(w)$ با زیرگروهی از $\mathbb{Z}_n^\times$ یکریخت است.

اثبات. فرض کنید $\operatorname{char} K = p$. ابتدا فرض کنید w ریشه‌ی اولیه‌ی nام واحد روی K باشد. ثابت می‌کنیم $p \nmid n$. اگر $p|n$، آنگاه چون

$$x^n - 1 = x^{pd} - 1 = (x^d - 1)^p$$

داریم $(w^d - 1)^p = 0$ که نتیجه می‌دهد $w^d = 1$ و این تناقض است. پس $p \nmid n$. اکنون برعکس فرض کنید $p \nmid n$. اگر $f(x) = x^n - 1$، آنگاه $f'(x) = nx^{n-1} \neq 0$. بنابراین، بنا به قضیه‌ی ۲.۴.۱۴، $f(x)$ روی K جداپذیر است، یعنی $x^n - 1$ در توسیع تجزیه‌ی $F : K$، n ریشه‌ی متمایز دارد. این ریشه‌ها یک زیرگروه دوری مرتبه‌ی n از $F^\times$ را تشکیل می‌دهند. بنابراین مولد این زیرگروه یک ریشه‌ی اولیه‌ی nام واحد روی K است.

اکنون فرض کنید $p \nmid n$ (صفر n را عاد نمی‌کند) و w یک ریشه‌ی اولیه‌ی nام واحد روی K باشد. بنابراین ریشه‌های چندجمله‌ای

$x^n - ۱$ عبارت‌اند از ۱، w، $w^۲$، . . .، $w^{n-۱}$ که همگی متمایزند و در $K(w)$ قرار دارند. از این‌رو $K(w) : K$ توسیع تجزیه‌ی چندجمله‌ای جداپذیر $x^n - ۱$ است. در نهایت ثابت می‌کنیم $\operatorname{Aut}_K K(w)$ با زیرگروهی از $\mathbb{Z}_n^\times$ یکریخت است. فرض کنید $R = \langle w \rangle = \{۱, w, \dots, w^{n-۱}\}$.
اگر $\alpha \in \operatorname{Aut}_K K(w)$، آنگاه $\alpha|_R : R \longrightarrow R$ یک خودریختی R است. به سادگی می‌توان دید که نگاشت $\psi : \operatorname{Aut}_K K(w) \longrightarrow \operatorname{Aut} R$ با ضابطه‌ی $\psi(\alpha) = \alpha|_R$ یک همریختی یک‌به‌یک است. بنابراین داریم

$$\operatorname{Aut}_K K(w) \hookrightarrow \operatorname{Aut} R \cong \operatorname{Aut} \mathbb{Z}_n \cong \mathbb{Z}_n^\times. \qquad \square$$

قضیه ۱۶.۵.۱۴. فرض کنید K یک میدان و شامل یک ریشه‌ی nام اولیه‌ی واحد باشد $(n \in \mathbb{N})$ و $۰ \neq a \in K$. اگر $F : K$ توسیع تجزیه‌ی $f(x) = x^n - a \in K[x]$ و b ریشه‌ای از $f(x)$ باشد، آنگاه
(الف) $F = K(b)$.
(ب) $\operatorname{Aut}_K F$ آبلی است.

اثبات. فرض کنید $w \in K$ یک ریشه‌ی nام اولیه‌ی واحد باشد. اگر c ریشه‌ای از $f(x)$ باشد، آنگاه $c^n = a$ و

$$c^n = a \Longrightarrow c^n = b^n \Longrightarrow \left(\frac{c}{b}\right)^n = ۱ \Longrightarrow \frac{c}{b} = ۱,\ \ w,\ \ w^۲,\ \ \dots\ \ , w^{n-۱}.$$

بنابراین b، bw، $bw^۲$، . . .، $bw^{n-۱}$ همه‌ی ریشه‌های متمایز $f(x)$ در $K(b)$ هستند. پس $K(b) : K$ توسیع تجزیه‌ی چندجمله‌ای جداپذیر $x^n - a \in K[x]$ است. در نهایت اگر $\alpha, \beta \in \operatorname{Aut}_K F$، آنگاه $\alpha(b)$ و $\beta(b)$ ریشه‌هایی از $x^n - a$ هستند؛ مثلاً $\alpha(b) = bw^i$ و $\beta(b) = bw^j$. چون $\alpha(w) = w = \beta(w)$، داریم $\alpha\beta(b) = bw^{i+j} = \beta\alpha(b)$. بنابراین $\alpha\beta = \beta\alpha$ و $\operatorname{Aut}_K F$ آبلی است. $\square$

تمرین‌ها

۱. فرض کنید $F : K$ توسیع باشد. نشان دهید $\operatorname{Aut}_K F$ زیر گروهی از $\operatorname{Aut} F$ است.

۲. فرض کنید $F : K$ توسیع باشد، $A \subseteq F$، و $\alpha \in \operatorname{Aut} F$. نشان دهید $\alpha(K(A)) \subseteq \alpha(K)(\alpha(A))$؛ نتیجه بگیرید اگر $\alpha \in \operatorname{Aut}_K F$ و $\alpha(A) \subseteq A$، آنگاه $\alpha(K(A)) \subseteq K(A)$.

۳. فرض کنید F یک میدان متناهی با مشخصه‌ی p باشد. اگر $\varphi : F \longrightarrow F$، با ضابطه‌ی $\varphi(a) = a^p$، خودریختی فروبنیوس باشد، نشان دهید $\operatorname{Aut} F$ یک گروه دوری است و $\operatorname{Aut} F = \langle \varphi \rangle$.

۴. گروه گالوای $\operatorname{Aut}_{\mathbb{Q}} F$ را بیابید، هرگاه
(الف) $F = \mathbb{Q}(e^{۲i\pi/۸})$ (ب) $F = \mathbb{Q}(e^{۲i\pi/۶})$ (ج) $F = \mathbb{Q}(\sqrt{۲}, \sqrt{۵})$
(هـ) $F = \mathbb{Q}(i, \sqrt{۲})$ (د) $F = \mathbb{Q}(\sqrt[۳]{۲}, \sqrt{۲})$ (O) $F = \mathbb{Q}(\sqrt[۴]{۲})$

۵. فرض کنید $F : K$ توسیع باشد و $[F : K] = ۲$، نشان دهید $\operatorname{Aut}_K F \cong C_۲$. در حالتی که $[F : K] = p$، p عدد اول ، چه می‌توان گفت؟

۶. فرض کنید F توسیع تجزیه‌ی $f(x) = x^۶ + x^۳ - ۱$ روی $\mathbb{Z}_۳$ باشد. نشان دهید $F = \mathbb{Z}_۳(u)$، توسیع ساده است و $\operatorname{Aut}_{\mathbb{Z}_۳} F$ را بیابید.

۷. فرض کنید $F = \mathbb{Q}(\sqrt[۴]{۲}, i)$ نشان دهید $\operatorname{Aut}_{\mathbb{Q}} F \cong D_۸$.

۸. نشان دهید $\operatorname{Aut}_{\mathbb{Q}} \mathbb{R} = \{\mathrm{id}_{\mathbb{R}}\}$.

۹. گروه گالوای $f(x) = x^۳ - ۷$ را روی $\mathbb{Q}$ بیابید.

۱۰. گروه گالوای $f(x) = x^p - a$، p عدد اول و a عدد گویای مثبت، را روی $\mathbb{Q}$ بیابید.

۱۱. نشان دهید گروه گالوای چندجمله‌ای $(x^۲ - ۲)(x^۳ - ۳)$ روی $\mathbb{Q}$ با $S_۳ \times \mathbb{Z}_۲$ یکریخت است.

۱۲. مرتبه‌ی گروه گالوای $\mathbb{Q}(\sqrt{۲}, \sqrt{۵}, \sqrt{۷}) : \mathbb{Q}$ را بیابید.

۱۳. نشان دهید گروه گالوای $x^n - ۱ \in \mathbb{Q}[x]$ آبلی است.

۱۴. فرض کنید $f(x) \in K[x]$ یک چندجمله‌ای تکین جداپذیر با درجه‌ی n باشد. اگر $F : K$ توسیع تجزیه‌ی $f(x)$ باشد طوری که $\mathrm{Aut}_K F$ روی مجموعه‌ی ریشه‌های $f(x)$ به صورت ترایا عمل کند، نشان دهید $f(x)$ روی K تحویل‌ناپذیر است.

۶.۱۴ چندجمله‌ای‌های دایره‌بر و قضیه‌ی ودربُرن

در انتهای بخش قبل دیدیم که ریشه‌ی nام اولیه‌ی واحد روی میدان K وجود دارد اگر و تنها اگر مشخصه‌ی K عدد n را عاد نکند (طبق قرارداد ۰، n را عاد نمی‌کند). بنابراین ریشه‌های واحد روی هر میدان با مشخصه‌ی صفر همواره وجود دارند. اکنون مفهوم مهم چندجمله‌ای دایره‌بر را معرفی و خواص اساسی آن را بررسی می‌کنیم.

تعریف ۱.۶.۱۴. فرض کنید $n \geq ۱$ عدد صحیح مثبت باشد و K میدانی که مشخصه‌ی آن n را عاد نمی‌کند. فرض کنید $F : K$ توسیع تجزیه‌ی $x^n - ۱ \in K[x]$ و $a_۱$، $a_۲$، ...، a_m همه‌ی ریشه‌های nام اولیه‌ی واحد باشند. چندجمله‌ای

$$\Phi_n(x) = \prod_{j=۱}^{m} (x - a_j) \in F[x]$$

را nامین چندجمله‌ای دایره‌بر روی K گوییم. توسیع $F : K$ را nامین توسیع دایره‌بر گوییم.

به وضوح روی هر میدان دلخواه F داریم $\Phi_۱(x) = x - ۱$ و اگر $\mathrm{char}\, F \neq ۲$ داریم $\Phi_۲(x) = x + ۱$. هم‌چنین چون تعداد ریشه‌های nام اولیه‌ی واحد برابر تعداد مولدهای متمایز $G = \{a \in F^\times \mid a^n = ۱\}$ است، $\deg \Phi_n(x) = \varphi(n)$، که در آن φ تابع فی اویلر است.

مثال ۲.۶.۱۴. اگر F میدان باشد و $\mathrm{char}\, F \neq p$ (p عدد اول)، آن‌گاه

$$\Phi_p(x) = ۱ + x + x^۲ + \cdots + x^{p-۱}.$$

حل ریشه‌های pام اولیه‌ی متمایز واحد، ریشه‌های چندجمله‌ای $x^p - ۱$ هستند. چون p عدد اول است، هر ریشه‌ی این چندجمله‌ای به جز ۱، ریشه‌ی اولیه‌ی واحد است. چون $x^p - ۱ = (x - ۱)\Phi_p(x)$، حکم ثابت است. □

قضیه ۳.۶.۱۴. اگر $n \geq ۱$ عدد صحیح و K یک میدان باشد، که $\mathrm{char}\, K \nmid n$، آن‌گاه
(الف) $x^n - ۱ = \prod_{d|n, d>۰} \Phi_d(x)$.
(ب) اگر L زیرمیدان اول K باشد، آن‌گاه $\Phi_n(x) \in L[x]$.

اثبات. فرض کنید a یک ریشه‌ی nام اولیه‌ی واحد روی K باشد. در این صورت $K(a) : K$ توسیع تجزیه‌ی $x^n - ۱ \in K[x]$، و گروه ضربی G متشکل از همه‌ی ریشه‌های nام واحد گروه یک دوری مرتبه‌ی n است. فرض کنید d عدد صحیح مثبت باشد که $d|n$. قرار می‌دهیم $T_d = \{g \in G \mid O(g) = d\}$. پس $\{T_d \mid d > ۰,\ d|n\}$ یک افراز G است. به وضوح به ازای هر شمارنده مثبت d از n، G مشتمل بر همه‌ی ریشه‌های dام اولیه‌ی واحد و T_d متشکل از همه‌ی ریشه‌های dام اولیه‌ی واحد است، بنابراین

$$\begin{aligned} x^n - ۱ &= \prod_{g \in G} (x - g) \\ &= \prod_{d|n, d>۰} \prod_{g \in T_d} (x - g) \\ &= \prod_{d|n, d>۰} \Phi_d(x). \end{aligned}$$

(ب) به استقرا روی n حکم را ثابت می‌کنیم. اگر $n=۱$، آنگاه $\Phi(x)=x-۱\in L[x]$. اکنون فرض کنید حکم برای همه‌ی اعداد صحیح k که $۱\leq k<n$، درست است. در این صورت به ازای هر d که $۱\leq d<n$ و $d|n$ داریم ، $\Phi_d(x)\in L[x]$ و

$$f(x)=\prod_{d|n,۱\leq d<n}\Phi_d(x)\in L[x].$$

بنا به (الف) داریم

$$x^n-۱=\prod_{d|n,d>۰}\Phi_d(x)=f(x)\Phi_n(x)\in K(a)[x].$$

بنا به الگوریتم تقسیم برای چندجمله‌ای‌های $f(x)$، $x^n-۱$ در $L[x]$، چندجمله‌ای‌های $q(x),r(x)\in L[x]\subseteq K(a)[x]$ وجود دارند که

$$x^n-۱=q(x)f(x)+r(x),$$

که در آن $r(x)=۰$ یا $\deg r(x)<\deg f(x)$. از طرفی چون $x^n-۱=f(x)\Phi_n(x)$ و $q(x)$ و $\Phi_n(x)$ تکین هستند ، و بنا به یکتایی خارج قسمت و باقیمانده در $K(a)[x]$، داریم $r(x)=۰$ و $\Phi_n(x)=q(x)\in L[x]$، که حکم را ثابت می‌کند. □

بنا به قضیه‌ی ۳.۶.۱۴ (الف)، داریم $x^n-۱=(\prod_{d|n,۱\leq d<n}\Phi_d(x))\Phi_n(x)$. پس

$$\Phi_n(x)=\frac{x^n-۱}{\prod_{d|n,۱\leq d<n}\Phi_d(x)},$$

و اگر p عدد اول باشد،

$$\Phi_p(x)=\frac{x^p-۱}{\Phi_۱(x)}=\frac{x^p-۱}{x-۱}=۱+x+\cdots+x^{p-۱}.$$

هم‌چنین مثلاً

$$\begin{aligned}\Phi_۴(x)&=\frac{x^۴-۱}{\Phi_۱(x)\Phi_۲(x)}=\frac{x^۴-۱}{(x-۱)(x+۱)}=x^۲+۱\\ \Phi_۶(x)&=\frac{x^۶-۱}{\Phi_۱(x)\Phi_۲(x)\Phi_۳(x)}=\frac{x^۶-۱}{(x-۱)(x+۱)(x^۲+x+۱)}\\ &=x^۲-x+۱.\end{aligned}$$

محاسبات بالا نشان می‌دهد که همه‌ی ضرایب $\Phi_n(x)$ صحیح هستند. این مطلب روی $\mathbb{Q}$ در حالت کلی درست است:

قضیه ۴.۶.۱۴. اگر $\Phi_n(x)$، nامین چندجمله‌ای دایره‌بر روی $\mathbb{Q}$ باشد، آنگاه داریم $\Phi_n(x)\in\mathbb{Z}[x]$.

اثبات. به استقرا روی n حکم را ثابت می‌کنیم. اگر $n=۱$ داریم $\Phi_۱(x)=x-۱\in\mathbb{Z}[x]$. حال فرض کنید حکم برای هر d که $۱\leq d<n$ درست باشد. بنابراین به ازای هر d که $۱\leq d<n$ و $d|n$ داریم $\Phi_d(x)\in\mathbb{Z}[x]$. از این‌رو

$$f(x)=\prod_{d|n,۱\leq d<n}\Phi_d(x)\in\mathbb{Z}[x].$$

بنا به قضیه‌ی ۳.۶.۱۴،

$$x^n-۱=\prod_{d|n,d>۰}\Phi_d(x)=f(x)\Phi_n(x)\in\mathbb{Q}[x].$$

بنا به الگوریتم تقسیم برای چندجمله‌ای‌های $f(x)\in\mathbb{Z}[x]$، $x^n-۱$، چندجمله‌ای‌های $q(x),r(x)\in\mathbb{Z}[x]\subseteq\mathbb{Q}[x]$ وجود دارند که $x^n-۱=q(x)f(x)+r(x)$، که در آن $r(x)=۰$ یا $\deg r(x)<\deg f(x)$. از طرفی چون $x^n-۱=f(x)\Phi_n(x)$، $f(x)$ و $\Phi_n(x)$ تکین هستند ، بنا به یکتایی خارج قسمت و باقیمانده در $\mathbb{Q}[x]$ داریم $r(x)=۰$ و $\Phi_n(x)=q(x)\in\mathbb{Z}[x]$، که حکم را ثابت می‌کند. □

نتیجه ۵.۶.۱۴. اگر n عدد صحیح مثبت و $\Phi_n(x)$، nامین چندجمله‌ای دایره‌بر روی $\mathbb{Q}$ باشد، آنگاه به ازای هر شمارنده مثبت m از n داریم

(الف) $\dfrac{x^n-1}{x^m-1} \in \mathbb{Z}[x]$.

(ب) $\Phi_n(x)$ در $\mathbb{Z}[x]$، $\dfrac{x^n-1}{x^m-1}$ را عاد می‌کند.

اثبات. بنا به قضیه‌ی ۳.۶.۱۴، داریم

$$\begin{aligned} x^n-1 &= \prod_{d|n,d>0} \Phi_d(x) \\ &= \left(\prod_{d|m,d>0} \Phi_d(x)\right)\left(\prod_{d|n,d>0,d\nmid m} \Phi_d(x)\right) \\ &= (x^m-1)\left(\prod_{d|n,d>0,d\nmid m} \Phi_d(x)\right). \end{aligned}$$

بنابراین بنا به قضیه‌ی ۴.۶.۱۴، داریم

$$\frac{x^n-1}{x^m-1} = \prod_{d|n,d>0,d\nmid m} \Phi_d(x) \in \mathbb{Z}[x] \qquad (۲)$$

(ب) با استفاده از تساوی (۲) داریم

$$\frac{x^n-1}{x^m-1} = \Phi_n(x) \prod_{d|n,0<d<n,d\nmid m} \Phi_d(x). \qquad \square$$

اکنون قضیه‌ی معروف ودربُرن را ثابت می‌کنیم. قضیه‌ی ودربُرن می‌گوید هر حلقه تقسیم متناهی یک میدان است. می‌دانیم هر حلقه متناهی بدون مقسوم علیه صفر یک حلقه تقسیم است (قضیه‌ی ۲۰.۱.۱۰). بنابراین با استفاده از قضیه‌ی ودربُرن نتیجه می‌گیریم که هر حلقه متناهی بدون مقسوم علیه صفر میدان است. توجه کنید که اگر n، d و $q>1$ اعداد صحیح مثبت باشند و $(q^n-1) \mid (q^d-1)$، آنگاه $d|n$. زیرا بنا به الگوریتم تقسیم می‌توان نوشت $n=sd+r$، که در آن $0 \le r < d$. بنابراین، به پیمانه q^d-1 داریم $1 \equiv q^n \equiv q^{sd}q^r \equiv q^r$، که نتیجه می‌دهد $r=0$. از این نکته در اثبات قضیه‌ی ودربُرن استفاده می‌کنیم.

قضیه ۶.۶.۱۴. (قضیه‌ی ودربُرن) اگر R حلقه تقسیم متناهی باشد، آنگاه R میدان است.

اثبات. فرض کنید $\mathrm{Cent}(R)=\{a \in R \mid \forall b \in R,\ \ ab=ba\}$ مرکز R باشد. در این صورت $\mathrm{Cent}(R)$ یک میدان متناهی است، مثلاً $|\mathrm{Cent}(R)|=q$. اکنون R یک فضای برداری روی میدان $\mathrm{Cent}(R)$ است. اگر بُعد R روی $\mathrm{Cent}(R)$ برابر n باشد، آنگاه ، بنا به نتیجه‌ی ۹.۴.۱۳، $|R|=q^n$. توجه کنید $|R^\times|=q^n-1$ و $|\mathrm{Cent}(R^\times)|=q-1$. فرض کنید بر خلاف حکم R تعویض‌پذیر نباشد و $\mathrm{orb}(a_1)$، ...، $\mathrm{orb}(a_m)$، همه‌ی رده‌های مزدوجی متمایز و نابدیهی گروه ضربی $R^\times$ باشند. بنا به معادله‌ی رده‌ای داریم

$$|R^\times| = |\mathrm{Cent}(R^\times)| + \sum_{j=1}^{m} |R^\times : C_{R^\times}(a_j)|.$$

اکنون $C_R(a_j)=\{r \in R \mid ra_j=a_jr\}$ زیرحلقه تقسیم از حلقه R و شامل $\mathrm{Cent}(R)$ است. چون $C_R(a_j)$ نیز فضای برداری روی $\mathrm{Cent}(R)$ است، $|C_R(a_j)|=q^{d_j}$. به علاوه چون $C_{R^\times}(a_j)=C_R(a_j)^\times$، داریم $|C_{R^\times}(a_j)|=q^{d_j}-1$ که بنا به قضیه‌ی لاگرانژ، $|R^\times|=q^n-1$ را عاد می‌کند. بنابراین

$$q^n-1 = q-1+\sum_{j=1}^{m} \frac{q^n-1}{q^{d_j}-1}.$$

چون $(q^n-۱) \mid (q^{d_j}-۱)$، بنا به بحث قبل از قضیه، $d_j|n$. فرض کنید $\Phi_n(x)$، nامین چندجمله‌ای دایره‌بر روی $\mathbb{Q}$ باشد. بنا به نتیجه‌ی ۵.۶.۱۴، $\Phi_n(x)$، $\frac{x^n-۱}{x^{d_j}-۱} \in \mathbb{Z}[x]$ را عاد می‌کند. بنابراین $\Phi_n(q)$ عدد صحیحی است که $q^n-۱$ و به ازای هر j، $\frac{q^n-۱}{q^{d_j}-۱}$ را عاد می‌کند. پس باید $q-۱$ را عدد کند. اما اگر $u_۱$، ...، u_t همه‌ی ریشه‌های اولیه‌ی nام واحد باشند، چون $q \geq ۲$ داریم $|q-u_j| > q-۱ \geq ۱$. بنابراین

$$|\Phi_n(q)| = \left|\prod_j^t (q-u_j)\right| = \prod_j^t |q-u_j| > (q-۱)^t \geq q-۱,$$

اما این متناقض با $\Phi_n(q)|(q-۱)$ است. بنابراین R تعویض‌پذیر و در نتیجه میدان است. □

قضیه‌ی ودربُرن را می‌توان تعمیم داد. اگر R حلقه تقسیم متناهی باشد، مثلاً $|R| = n$، آنگاه بنا به قضیه‌ی لاگرانژ به ازای هر $۰ \neq a \in R$، $a^{n-۱} = ۱$. پس به ازای هر $a \in R$، $a^n = a$. به طور کلی حلقه دلخواه R را J- حلقه گوییم هرگاه به ازای هر $a \in R$ عدد صحیح مثبت n (وابسته به a) وجود داشته باشد که $a^n = a$. ژاکوبسون ثابت کرد که هر J- حلقه دلخواه تعویض‌پذیر است. پس قضیه‌ی ودربُرن حالت خاصی از قضیه‌ی ژاکوبسون است.

اکنون نشان می‌دهیم که چندجمله‌ای‌های دایره‌بر روی $\mathbb{Q}$ تحویل‌ناپذیر است:

قضیه ۷.۶.۱۴. اگر $\Phi_n(x)$، nامین چندجمله‌ای دایره‌بر روی $\mathbb{Q}$ باشد، آنگاه $\Phi_n(x)$ روی $\mathbb{Q}$ تحویل‌ناپذیر است.

اثبات. بنا به قضیه‌ی ۱۲.۲.۱۱، از صفحه‌ی ۲۴۲، کافی است ثابت کنیم $\Phi_n(x)$ روی $\mathbb{Z}[x]$ تجزیه‌ناپذیر است. فرض کنید $f(x) \in \mathbb{Z}[x]$ یک عامل تجزیه‌ناپذیر $\Phi_n(x)$ باشد. چندجمله‌ای $g(x) \in \mathbb{Z}[x]$ وجود دارد که $\Phi_n(x) = f(x)g(x)$. چون $\Phi_n(x)$ تکین است، می‌توان $f(x)$ و $g(x)$ را تکین گفت. فرض کنید $a \in \mathbb{C}$ ریشه‌ای از $f(x)$ باشد، در این صورت a ریشه‌ای از $\Phi_n(x)$ و بنابراین یک ریشه‌ی nام اولیه‌ی واحد است. فرض کنید p عدد اولی باشد که n را عاد نمی‌کند. بنابراین $\gcd\{p,n\} = ۱$ و a^p نیز یک ریشه‌ی nام اولیه‌ی واحد است. نشان می‌دهیم a^p نیز ریشه‌ای از $f(x)$ است.

فرض کنید a^p ریشه‌ی $f(x)$ نباشد. چون a^p ریشه‌ای از $\Phi_n(x)$ است، a^p ریشه‌ای از $g(x)$ نیز هست. بنابراین a ریشه‌ای از $g(x^p)$ است. پس در $\mathbb{Q}[x]$ داریم $f(x)|g(x^p)$. بنابراین $h(x) \in \mathbb{Q}[x]$ وجود دارد که $g(x^p) = f(x)h(x)$. چون $f(x), g(x^p) \in \mathbb{Z}[x]$، همانند اثبات قضیه‌ی ۴.۶.۱۴، با استفاده از الگوریتم تقسیم، می‌توان ثابت کرد $h(x) \in \mathbb{Z}[x]$. برای $t(x) \in \mathbb{Z}[x]$ فرض کنید $\overline{t(x)}$ چندجمله‌ای متناظر آن در $\mathbb{Z}_p[x]$ باشد، یعنی اگر $b \in \mathbb{Z}$ یکی از ضرایب $t(x)$ باشد، آنگاه $\bar{b} \in \mathbb{Z}_p$ ضرایب متناظر آن در $\overline{t(x)}$ است. چون $\operatorname{char} \mathbb{Z}_p = p$، داریم $\overline{g(x^p)} = \overline{g(x)}^p$ و

$$\overline{g(x)}^p = \overline{g(x^p)} = \overline{f(x)}\ \overline{h(x)}.$$

بنابراین $\overline{f(x)}$ و $\overline{g(x)}$ یک عامل تحویل‌ناپذیر مشترک دارند. اکنون $t(x) \in \mathbb{Z}[x]$ وجود دارد که $x^n-۱ = \Phi_n(x)t(x)$. پس در $\mathbb{Z}_p[x]$ داریم

$$\begin{aligned} x^n-۱ &= \overline{\Phi_n(x)}\ \overline{t(x)} \\ &= \overline{f(x)g(x)}\ \overline{t(x)} \\ &= \overline{f(x)}\ \overline{g(x)}\ \overline{t(x)}. \end{aligned}$$

بنابراین $x^n-۱ \in \mathbb{Z}_p[x]$ ریشه‌ی تکراری دارد ، که تناقض است، زیرا $p \nmid n$. این تناقض نشان می‌دهد a^p ریشه‌ای از $f(x)$ است. به استقرا می‌توان نشان داد به ازای هر عدد صحیح مثبت r، a^{p^r} نیز ریشه‌ای از $f(x)$ است. هم‌چنین به استقرا می‌توان نشان داد به ازای همه‌ی اعداد اول $p_۱$، ...، p_s، که n را عاد نمی‌کنند و به ازای همه‌ی اعداد صحیح مثبت $r_۱$، ...، r_s، $a^{p_۱^{r_۱}\cdots p_s^{r_s}}$ نیز ریشه‌ای از $f(x)$ است. در نتیجه به ازای هر $۱ \leq k < n$ که $\gcd\{k,n\} = ۱$، a^k ریشه‌ی $f(x)$ است. بنابراین همه‌ی ریشه‌های nام اولیه‌ی واحد ریشه‌های $f(x)$ نیز هستند. پس $\Phi_n(x) = f(x)$. بنابراین $\Phi_n(x)$ روی $\mathbb{Z}[x]$ تحویل‌ناپذیر است. □

نتیجه ۸.۶.۱۴. اگر $a \in \mathbb{C}$ یک ریشه‌ی nام اولیه‌ی واحد روی $\mathbb{Q}$ باشد، آنگاه $[\mathbb{Q}(a) : \mathbb{Q}] = \varphi(n)$، که در آن φ تابع فی اویلر است. به علاوه $\operatorname{Aut}_{\mathbb{Q}}\mathbb{Q}(a) \cong \mathbb{Z}_n^\times$.

اثبات. چون $\Phi_n(x) \in \mathbb{Q}[x]$ روی $\mathbb{Q}$ تحویل‌ناپذیر است و $\Phi_n(a) = ۰$، پس $\Phi_n(x)$ چندجمله‌ای می‌نیمال a روی $\mathbb{Q}$ است. از طرفی $\deg \Phi_n(x) = \varphi(n)$، که نتیجه می‌دهد

$$[\mathbb{Q}(a) : \mathbb{Q}] = \deg \Phi_n(x) = \varphi(n).$$

اکنون چون $\mathbb{Q}(a) : \mathbb{Q}$ توسیع تجزیه‌ی $\Phi_n(x)$ روی $\mathbb{Q}$ است، بنا به نتیجه‌ی ۵.۵.۱۴،

$$|\mathrm{Aut}_{\mathbb{Q}}\mathbb{Q}(a)| = [\mathbb{Q}(a) : \mathbb{Q}] = \varphi(n).$$

به ازای هر $\alpha \in \mathrm{Aut}_{\mathbb{Q}}\mathbb{Q}(a)$، $\alpha(a)$ یک ریشه‌ی nام اولیه‌ی واحد است. پس $۱ \leq d < n$، با $\gcd\{d, n\} = ۱$ وجود دارد که $\alpha(a) = a^d$. به علاوه اگر $\alpha(a)$ مشخص باشد، آن‌گاه α کاملاً معین می‌شود. این α را با α_d نشان می‌دهیم. نگاشت $\psi : \mathbb{Z}_n^\times \longrightarrow \mathrm{Aut}_{\mathbb{Q}}\mathbb{Q}(a)$ با ضابطه‌ی $\psi(\bar{d}) = \alpha_d$ را تعریف می‌کنیم. چون

$$\begin{aligned}
\bar{d} = \bar{r} &\iff \exists m \in \mathbb{Z},\ \ d - r = mn \\
&\iff a^{d-r} = ۱ \\
&\iff a^d = a^r \\
&\iff \alpha_d(a) = \alpha_r(a) \\
&\iff \alpha_d = \alpha_r
\end{aligned}$$

ψ، خوش تعریف و یک‌به‌یک است. پوشا بودن ψ واضح است. فرض کنید $\bar{c}, \bar{d} \in \mathbb{Z}_n^\times$. داریم

$$\alpha_{cd}(a) = a^{cd} = (a^d)^c = \alpha_c(\alpha_d(a)).$$

بنابراین $\alpha_{cd} = \alpha_c\alpha_d$، که نتیجه می‌دهد ψ همریختی نیز هست:

$$\psi(\bar{c}\bar{d}) = \psi(\overline{cd}) = \alpha_{cd} = \alpha_c\alpha_d = \psi(\bar{c})\psi(\bar{d}). \qquad \square$$

روشی برای تعیین چندجمله‌ای‌های اولیه مبتنی بر این حقیقت است که حاصل‌ضرب چندجمله‌ای‌های اولیه‌ی درجه‌ی m روی $\mathrm{GF}(q)$ برابر چندجمله‌ای دایره‌بر $\Phi_e(x)$ است، که در آن $e = q^m - ۱$. پس همه‌ی چندجمله‌ای‌های اولیه روی $\mathrm{GF}(q)$ از درجه‌ی m را می‌توان با به کار بردن یکی از الگوریتم‌های تجزیه، به چند جمله‌ای دایره‌بر $\Phi_e(x)$ به دست آورد.

مثال ۹.۶.۱۴. یک چندجمله‌ای اولیه روی $\mathbb{Z}_۳$ با درجه‌ی ۴ بیابید.

حل چون $۵ \times ۱۶ = ۳^۴ - ۱$، ابتدا دو عضو $\mathrm{GF}(۸۱)^\times$ با مرتبه‌های ۱۶ و ۵ به دست می‌آوریم. عناصر مرتبه‌ی ۱۶ ریشه‌های چندجمله‌ای دایره‌بر $\Phi_{۱۶}(x) = x^۸ + ۱ \in \mathbb{Z}_۳[x]$ هستند. چون مرتبه‌ی ضربی ۳ به پیمانه‌ی ۱۶ برابر ۴ است، $\Phi_{۱۶}(x)$ به دو چندجمله‌ای تحویل‌ناپذیر تکین در $\mathbb{Z}_۳[x]$ از درجه‌ی ۴ تجزیه می‌شود:

$$x^۸ + ۱ = (x^۴ - ۱)^۲ - x^۴ = (x^۴ - ۱ + x^۲)(x^۲ - ۱ - x^۲).$$

بنابراین $f(x) = x^۴ - x^۲ - ۱$ روی $\mathbb{Z}_۳[x]$ تحویل‌ناپذیر است. اگر a ریشه‌ای از $f(x)$ باشد، داریم $\mathrm{GF}(۸۱) = \mathbb{Z}_۳(a)$. به علاوه a، عضوی از مرتبه‌ی ۱۶ در $\mathrm{GF}(۸۱)^\times$ است. می‌توان دید مرتبه‌ی $b = a + a^۲$ برابر ۵ است. بنابراین

$$\xi = ab = a^۲ + a^۳$$

عضوی از مرتبه‌ی ۸۰ در $\mathrm{GF}(۸۱)$ است، یعنی ξ عضو اولیه‌ای از $\mathrm{GF}(۸۱)$ است. چندجمله‌ای می‌نیمال ξ روی $\mathbb{Z}_۳$ عبارت است از

$$\begin{aligned}
g(x) &= (x - \xi)(x - \xi^۳)(x - \xi^۹)(x - \xi^{۲۷}) \\
&= (x - a^۲ - a^۳)(x - ۱ + a + a^۲)(x - a^۲ + a^۳)(x - ۱ - a + a^۲) \\
&= x^۴ + x^۳ + x^۲ - x - ۱,
\end{aligned}$$

و بنابراین یک چندجمله‌ای اولیه‌ی $g(x)$ روی $\mathbb{Z}_۳$ با درجه‌ی ۴ به دست آوردیم. □

در حالت کلی تجزیه‌ی $x^n - ۱ = \prod_{d|n} \Phi_d(x)$، که آن را تجزیه‌ی دایره‌بر $x^n - ۱$ می‌نامیم، لزوماً تجزیه به عوامل تحویل‌ناپذیر نیست. با استفاده از فرمول وارون موبیوس، می‌توانیم فرمولی برای چندجمله‌ای‌های دایره‌بر بیابیم:

قضیه ۱۰.۶.۱۴. $\Phi_n(x) = \prod_{d|n}(x^d - ۱)^{\mu(n/d)} = \prod_{d|n}(x^{n/d} - ۱)^{\mu(d)}$.

اثبات. قرار می‌دهیم $g(n) = \Phi_n(x)$ و $f(n) = x^n - ۱$؛ آن‌گاه

$$f(n) = x^n - ۱ = \prod_{d|n} \Phi_d(x) = \prod_{d|n} g(d).$$

بنابراین با استفاده از صورت ضربی فرمول وارون موبیوس (قضیه‌ی ۲۳.۳.۱۴) داریم

$$\Phi_n(x) = g(n) = \prod_{d|n} f(d)^{\mu(n/d)} = \prod_{d|n}(x^d - ۱)^{\mu(n/d)}.$$

اثبات تساوی دیگر را به عنوان تمرین واگذار می‌کنیم. □

دیدیم ضرایب چندجمله‌ای‌های دایره‌بر روی $\mathbb{Q}$ صحیح هستند و روی $\mathbb{Q}$ تحویل‌ناپذیرند. این در حالی است که ضرایب چندجمله‌ای‌های دایره‌بر روی $\mathbb{Z}_p$ به پیمانه‌ی p محاسبه می‌شوند و لزوماً روی $\mathbb{Z}_p$ تحویل‌ناپذیر نیستند. مطلب جالب توجه این است که ضرایب اولین ۱۰۴ چندجمله‌ای دایره‌بر همگی ۰ یا ± ۱ هستند و در حالت $\Phi_{۱۰۵}(x)$ یکی از ضرایب برابر ۲ است. میدان دایره‌بر را می‌توان به صورت توسیع ساده‌ی $\mathbb{Z}_p$ و با استفاده از یک چندجمله‌ای $\Phi_n(x)$، که $x^n - ۱$ را عاد می‌کند، ساخت. میدان متناهی $\mathrm{GF}(p^n)$ میدان دایره‌بر $(p^n - ۱)$امین ریشه‌ی اولیه‌ی واحد است. در $\mathrm{GF}(p^n)$ داریم

$$x^{p^n - ۱} - ۱ = \prod_{d|p^n - ۱} \Phi_d(x).$$

در حالت کلی $\Phi_d(x)$ روی $\mathbb{Z}_p$ تحویل‌ناپذیر نیست، اما همه‌ی عناصر مرتبه‌ی d در $\mathrm{GF}(p^n)$ ریشه‌های آن هستند. درجه‌ی چندجمله‌ای می‌نیمال یک عضو مرتبه‌ی d در توسیعی از $\mathbb{Z}_p$ برابر k است، که در آن k کوچک‌ترین عدد صحیح است که $d|p^k - ۱$. چون $\varphi(d)$ عضو مرتبه‌ی d وجود دارند (φ تابع فی اویلر است)، $\varphi(d)/k$ چندجمله‌ای تحویل‌ناپذیر با درجه‌ی k روی $\mathbb{Z}_p$ با این خاصیت وجود دارند و حاصل‌ضرب این چندجمله‌ای‌ها برابر $\Phi_d(x)$ است.

مثال ۱۱.۶.۱۴. چندجمله‌ای $x^{۱۵} - ۱$ را روی $\mathbb{Z}_۲$ تجزیه کنید.

حل می‌نویسیم $x^{۱۵} - ۱ = \Phi_۱(x)\Phi_۳(x)\Phi_۵(x)\Phi_{۱۵}(x)$، که در آن

$$\Phi_۱(x) = x - ۱, \quad \Phi_۳(x) = x^۲ + x + ۱$$
$$\Phi_۵(x) = x^۴ + x^۳ + x^۲ + x + ۱,$$
$$\Phi_{۱۵}(x) = x^۸ - x^۷ + x^۵ - x^۴ + x^۳ - x + ۱.$$

$\Phi_۱(x)$، $\Phi_۳(x)$، $\Phi_۵(x)$، روی $\mathbb{Z}_۲$ تحویل‌ناپذیر هستند. چون $۱۵|۲^۴ - ۱$ و $\varphi(۱۵) = ۸$، نتیجه می‌گیریم $\Phi_{۱۵}(x)$ حاصل‌ضرب چندجمله‌ای‌های تحویل‌ناپذیر درجه‌ی ۴ روی $\mathbb{Z}_۲$ است:

$$\Phi_{۱۵}(x) = (x^۴ + x + ۱)(x^۴ + x^۳ + ۱).$$ □

تمرین‌ها

۱. چندجمله‌ای‌های دایره‌بر زیر را بیابید
(الف) $\Phi_{۸}(x)$ (ب) $\Phi_{۹}(x)$ (ج) $\Phi_{۱۰}(x)$
(د) $\Phi_{۳۶}(x)$ (H) $\Phi_{۱۰۵}(x)$ (و) $\Phi_{۱۲۰}(x)$.

۲. (الف) گروه گالوای چندجمله‌ای $f(x)=x^{۲}-x+۱$ را روی $\mathbb{Q}$ بیابید.
(ب) نشان دهید گروه گالوای چندجمله‌ای $x^{۴}-x+۱$ و $x^{۲}-x+۱$ روی $\mathbb{Q}$ یکریخت‌اند.

۳. نشان دهید اگر $n\geq ۳$ عدد اول فرد باشد، آنگاه $\Phi_{۲n}(x)=\Phi_n(-x)$.

۴. اگر $n\geq ۲$، نشان دهید $\Phi_n(x^{-۱})x^{\varphi(n)}=\Phi_n(x)$ (φ تابع فی اویلر است).

۵. (الف) فرض کنید $\gcd\{m,n\}=۱$. نشان دهید توسیع تجزیه‌ی چندجمله‌ای $x^{mn}-۱$ و $(x^m-۱)(x^n-۱)$ روی $\mathbb{Q}$ یکی هستند.
(ب) از (الف) نتیجه بگیرید $\varphi(mn)=\varphi(m)\varphi(n)$ (φ تابع فی اویلر است).

۶. فرض کنید n عدد صحیح مثبت، و p عدد اول است که $p\nmid n$، نشان دهید

$$\Phi_{p_n}(x)=\frac{\Phi_n(x^p)}{\Phi_n(x)}.$$

۷. فرض کنید p عدد اول باشد و $q=p^{n-۱}$. نشان دهید

$$\Phi_{p^n}(x)=۱+x^q+x^{۲q}+\cdots+x^{(p-۱)q}.$$

۸. با استفاده از اتحاد $q^n-۱=\prod_{d|n}\Phi_d(q)$ نشان دهید $n=\sum_{d|n}\varphi(d)$، که در آن φ تابع فی اویلر است.

۹. (الف) نشان دهید هر زیرحلقه متناهی یک حلقه تقسیم، حلقه تقسیم است.
(ب) اگر R حلقه تقسیم با مشخصه‌ی عدد اول p باشد. نشان دهید هر زیرگروه متناهی $R^\times$ دوری است. آیا اگر $\operatorname{char}R=۰$ مساله درست است؟

۱۰. فرض کنید $n=p_۱^{n_۱}p_۲^{n_۲}\cdots p_r^{n_r}$، که در آن p_iها اعداد اول متمایز هستند ، و $m=p_۱p_۲\cdots p_r$. نشان دهید $\Phi_n(x)=\Phi_m\left(x^{\frac{n}{m}}\right)$.

۱۱. با استفاده از روش چندجمله‌ای‌های دایره‌بر، چندجمله‌ای‌های اولیه با درجه‌ی **۲۱، ۲۲، ۲۳، ۲۴** را بیابید.

۱۲. نشان دهید به ازای هر e، که مرتبه‌ی $\Phi_e(x)\in\mathrm{GF}(q)[x]$ تعریف شده باشد، مرتبه‌ی $\Phi_e(x)$ برابر e است.

۱۳. فرض کنید $n>۱$، نشان دهید $I(n,q;x)=\prod_m\Phi_m(x)$، که در آن حاصل‌ضرب روی همه‌ی mهایی گرفته می‌شود که m شمارنده‌های $q^n-۱$ و n مرتبه‌ی ضربی q به پیمانه‌ی m است.

۱۴. $I(۲,۶;x)$ را با استفاده از تمرین قبل بیابید.

۷.۱۴ توسیع‌های نرمال

توسیع جبری $F:K$ را توسیع نرمال گوییم هرگاه هر چندجمله‌ای تحویل‌ناپذیر $f(x)\in K[x]$ که روی F ریشه‌ای داشته باشد، روی F کاملاً تجزیه شود.

مثال ۱.۷.۱۴. اگر $F:K$ توسیعی با درجه‌ی ۲ باشد، آنگاه $F:K$ توسیع نرمال است.

حل فرض کنید $f(x)\in K[x]$ روی K تحویل‌ناپذیر و $a\in F-K$ ریشه‌ای از $f(x)$ باشد. بنا به قانون برج داریم $۲=[F:K]=[F:K(a)][K(a):K]$. چون $[K(a):K]\neq ۱$، $[F:K(a)]=۱$ و $F=K(a)$. چون $f(a)=۰$،

چندجمله‌ای $h(x) \in F[x]$ وجود دارد که $f(x) = (x-a)h(x)$، اکنون $\deg h(x) = ۱$ و چون $f(x)$ و $x-a$ تکین هستند $h(x)$ نیز تکین است. پس $b \in F$ وجود دارد که $h(x) = x-b$. پس $f(x)$ روی F تجزیه می‌شود. بنابراین $F : K$ نرمال است. □

مثال ۲.۷.۱۴. نشان دهید $\mathbb{Q}(\sqrt{۲}) : \mathbb{Q}$ و $\mathbb{Q}(\sqrt[۴]{۲}) : \mathbb{Q}(\sqrt{۲})$ توسیع‌های نرمال هستند ، اما $\mathbb{Q}(\sqrt[۴]{۲}) : \mathbb{Q}$ توسیع نرمال نیست.

حل چون $[\mathbb{Q}(\sqrt{۲}) : \mathbb{Q}] = ۲$ و $[\mathbb{Q}(\sqrt[۴]{۲}) : \mathbb{Q}(\sqrt{۲})]$ این توسیع‌ها، بنا به مثال ۱.۷.۱۴، نرمال هستند. اما چند جمله‌ای می‌نیمال $\sqrt[۴]{۲}$ روی $\mathbb{Q}$ عبارت است از $x^۴ - ۲$. ریشه‌های این چندجمله‌ای عبارت‌اند از $\pm\sqrt[۴]{۲}$، $\pm i\sqrt[۴]{۲}$. چون $\pm i\sqrt[۴]{۲} \notin \mathbb{Q}(\sqrt[۴]{۲})$ توسیع $\mathbb{Q}(\sqrt[۴]{۲}) : \mathbb{Q}$ نرمال نیست. □

در قضیه‌ی بعد توسیع متناهی و نرمال را توصیف می‌کنیم.

قضیه ۳.۷.۱۴. اگر $F : K$ توسیع متناهی باشد، آنگاه شرایط زیر معادل‌اند.
(الف) $F : K$ توسیع نرمال است.
(ب) $F : K$ توسیع تجزیه‌ی یک چندجمله‌ای $f(x) \in K[x]$ است.
(ج) به ازای هر توسیع $F : E$، هر K- همریختی یک‌به‌یک $\alpha : F \longrightarrow E$ یک K- خودریختی F است.

اثبات. (الف) $\Longleftarrow$ (ب) چون $F : K$ توسیع متناهی است، $F : K$ جبری است و اعضای $a_۱$، $a_۲$، ...، a_n در F وجود دارند که $F = K(a_۱, \ldots, a_n)$. به ازای هر $۱ \leq j \leq n$ فرض کنید $f_j(x) \in K[x]$ چندجمله‌ای می‌نیمال a_j روی K است. چون $F : K$ توسیع نرمال است، هر $f_j(x)$ روی F تجزیه می‌شود. قرار می‌دهیم $f(x) = f_۱(x) \cdots f_n(x)$. بنابراین $f(x)$ روی F تجزیه می‌شود. چون هر میدان که $f(x)$ روی آن تجزیه شود باید شامل $a_۱$، ...، a_n و K باشد، پس $f(x)$ روی هیچ زیرمیدان سره $F = K(a_۱, \ldots, a_n)$ تجزیه نمی‌شود و در نتیجه $F : K$ توسیع تجزیه‌ی $f(x)$ است.
(ب) $\Longleftarrow$ (ج) فرض کنید $F : K$ توسیع تجزیه‌ی چندجمله‌ای $f(x) \in K[x]$ است. اگر $a_۱$، ...، a_n ریشه‌های $f(x)$ در F باشند، داریم $F = K(a_۱, \ldots, a_n)$. فرض کنید $E : F$ توسیع و $\alpha : F \longrightarrow E$ یک K- همریختی باشد. باید نشان دهیم $\alpha(F) = F$ چون α،یک K- همریختی است، به ازای هر $۱ \leq j \leq n$، داریم

$$f(\alpha(a_j)) = \alpha(f(a_j)) = \alpha(۰) = ۰.$$

پس $\alpha(a_j)$ نیز ریشه‌ای از $f(x)$ است. بنابراین $\alpha(\{a_۱, \ldots, a_n\}) = \{a_۱, \ldots, a_n\}$. در نتیجه، بنا به تمرین ۲ از صفحه‌ی ۳۱۸، $\alpha(F) \subseteq K(a_۱, \ldots, a_n) = F$. بنا به قانون برج $[F : K] = [F : \alpha(F)][\alpha(F) : K]$، و چون $\alpha(F) \cong F$، داریم $[\alpha(F) : K] = [F : K]$، که نتیجه می‌دهد $[F : \alpha(F)] = ۱$، یعنی $\alpha(F) = F$.
(ج) $\Longleftarrow$ (الف) عضو دلخواه $a \in F$ را با چندجمله‌ای می‌نیمال $f(x) \in K[x]$ در نظر می‌گیریم. فرض کنید $F = K(a_۱, \ldots, a_n)$ و $f_j(x) \in K[x]$ چندجمله‌ای می‌نیمال a_j روی K، به ازای هر $۱ \leq j \leq n$، باشد. چندجمله‌ای

$$g(x) = f(x)f_۱(x) \cdots f_n(x)$$

و توسیع تجزیه‌ی $F : E$ از $g(x)$ را در نظر می‌گیریم. اگر $r_۱$، $r_۲$، ...، r_n ریشه‌های $g(x)$ در E باشند، آنگاه $E = F(r_۱, r_۲, \ldots, r_m)$. چون $F = K(a_۱, \ldots, a_n)$ و هم‌چنین $a_۱, a_۲, \ldots, a_n \in \{r_۱, r_۲, \ldots, r_m\}$، توسیع $E : K$ توسیع تجزیه‌ی $g(x)$ روی K است. اکنون $f(x)$ روی E تجزیه می‌شود. باید ثابت کنیم $f(x)$ روی F تجزیه می‌شود. به ازای هر ریشه‌ی $b \in E$ از $f(x)$، بنا به قضیه‌ی ۶.۲.۱۴، K- یکریختی یکتای $\alpha : K(a) \longrightarrow K(b)$ وجود دارد که $\alpha(a) = b$. بنا به قضیه‌ی ۷.۲.۱۴، K- یکریختی $\beta : E \longrightarrow E$ وجود دارد که توسیع α است. اکنون $\beta|_F : F \longrightarrow E$ یک K- همریختی یک‌به‌یک است. پس طبق فرض، $\beta|_F$ یک K- خودریختی F است. به ویژه $\beta(F) = F$ و

$$b = \alpha(a) = \beta(a) \in \beta(F) = F.$$

بنابراین همه‌ی ریشه‌های $f(x)$ در F قرار دارند. □

فرض کنید K یک میدان باشد و $S \subseteq K[x]$. توسیع $F : K$ را توسیع تجزیهی S گوییم هرگاه هر $f(x) \in S$ روی F تجزیه شود و اگر L میدان باشد، $K \subseteq L \subseteq F$ و هر $f(x) \in S$ روی L تجزیه شود، آنگاه $L = F$. در قضیه‌ی بعد توسیع نرمال (نه لزوماً متناهی) را بر حسب این مفهوم توصیف می‌کنیم.

قضیه ۴.۷.۱۴. اگر $F : K$ توسیع باشد، آنگاه $F : K$ نرمال است اگر و تنها اگر $F : K$ توسیع تجزیه برای زیرمجموعه‌ای مثل S از $K[x]$ باشد.

اثبات. ($\Longleftarrow$) مجموعه‌ی S را برابر مجموعه‌ی همه‌ی چندجمله‌ای‌های می‌نیمال اعضای F روی K تعریف می‌کنیم. چون $F : K$ نرمال است، هر عضو S روی F تجزیه می‌شود. به وضوح هر زیر میدان F که همه‌ی اعضای S روی آن تجزیه شوند برابر F است. پس $F : K$ توسیع تجزیه‌ی S است.
($\Longrightarrow$) فرض کنید A مجموعه‌ی همه‌ی ریشه‌های چندجمله‌ای‌های در S باشد. چون $A \subseteq F$، داریم $K(A) \subseteq F$. از طرف دیگر هر چندجمله‌ای در S روی $K(A)$ تجزیه می‌شود. از این‌رو $F = K(A)$. فرض کنید $p(x) \in K[x]$ چندجمله‌ای تحویل‌ناپذیر و $a \in F$ ریشه‌ای از آن باشد. باید ثابت کنیم $p(x)$ روی F تجزیه می‌شود. چون $a \in F = K(A)$، اعضای $a_1, \ldots, a_n \in A$ وجود دارند که $a \in K(a_1, \ldots, a_n)$. چون a_1، ...، a_n روی K جبری هستند ، $K(a_1, \ldots, a_n)$ و در نتیجه a روی K جبری است. به ازای هر $1 \leq j \leq n$، $f_j(x) \in S$ وجود دارد که $f_j(a_j) = 0$. طبق فرض هر $f_j(x)$ روی F تجزیه می‌شود. فرض کنید R مجموعه‌ی همه‌ی ریشه‌های $f_1(x)$، ...، $f_n(x)$ باشد. قرار می‌دهیم $f(x) = f_1(x) \cdots f_n(x)$. به وضوح $K(R) : K$ توسیع تجزیه‌ی $f(x)$ است. داریم $p(x) \in K[x] \subseteq K(R)[x]$. توسیع تجزیه‌ی $E : K(R)$ برای $p(x)$ را در نظر می‌گیریم. فرض کنید b ریشه‌ی دیگر i از $p(x)$ در E باشد. نشان می‌دهیم $b \in K(R)$. بنا به قضیه‌ی ۶.۲.۱۴، یکریختی $\alpha : K(a) \longrightarrow K(b)$ وجود دارد که K را ثابت نگه می‌دارد و $\alpha(a) = b$. حال $K(R) : K(a)$ توسیع تجزیه برای $f(x)$ روی $K(a)$، و $K(R, b) : K(b)$ توسیع تجزیه برای $\alpha(f(x)) = f(x)$ روی $K(b)$ است. از این‌رو بنا به قضیه‌ی ۷.۲.۱۴، یکریختی $\beta : K(R) \longrightarrow K(R, b)$ وجود دارد که توسیع α است. بنابراین $[K(R) : K(a)] = [K(R, b) : K(b)]$. از طرف دیگر چون $p(x)$ روی K تحویل‌ناپذیر است، $[K(a) : K] = \deg p(x) = [K(b) : K]$. بنا به قانون برج داریم :

$$\begin{aligned} [K(R) : K] &= [K(R) : K(a)][K(a) : K] \\ &= [K(R, b) : K(b)][K(b) : K] \\ &= [K(R, b) : K]. \end{aligned}$$

اما چون $K(R) \subseteq K(R, b)$، داریم $K(R, b) = K(R)$، پس $b \in K(R)$. □

اگر $F : K$ توسیع نرمال و L یک میدان میانی باشد، آنگاه می‌توان دید $F : L$ توسیع نرمال است و توسیع $L : K$ لزوماً نرمال نیست (تمرین ۳ را ببینید). سوالی که مطرح می‌شود این است که چه موقع توسیع $L : K$ نرمال است؟ به این سوال در قضیه‌ی بعد پاسخ می‌دهیم.

قضیه ۵.۷.۱۴. اگر $F : K$ توسیع متناهی و نرمال و L یک میدان واسطه باشد، آنگاه $L : K$ توسیع نرمال است اگر و تنها اگر به ازای هر $\alpha \in \operatorname{Aut}_K F$ داشته باشیم $\alpha(L) = L$، یعنی $\alpha|_L \in \operatorname{Aut}_K L$.

اثبات. ($\Longleftarrow$) فرض کنید $L : K$ توسیع نرمال باشد و $\alpha \in \operatorname{Aut}_K F$. فرض کنید $a \in L$ و $p(x) \in K[x]$ چندجمله‌ای می‌نیمال a روی K باشد. چون α هر عضو K را ثابت نگه می‌دارد ، $p(\alpha(a)) = \alpha(p(a)) = \alpha(0) = 0$. بنابراین $\alpha(a)$ ریشه‌ای از $p(x)$ است. چون $p(x)$ روی L تجزیه می‌شود، $\alpha(a) \in L$. از این‌رو $\alpha(L) \subseteq L$. به همین نحو چون $\alpha^{-1} \in \operatorname{Aut}_K F$، $\alpha^{-1}(L) \subseteq L$؛ یعنی $L \subseteq \alpha(L)$. بنابراین $\alpha(L) = L$.
($\Longrightarrow$) چون $F : K$ توسیع نرمال است، توسیع تجزیه‌ی یک چندجمله‌ای $f(x) \in K[x]$ است. فرض کنید $a \in L$ و $p(x) \in K[x]$ چندجمله‌ای می‌نیمال a روی K باشد. چون $F : K$ نرمال است، $p(x)$ روی F تجزیه می‌شود. باید نشان دهیم $p(x)$ روی L تجزیه می‌شود. ریشه‌ی دلخواه b از $p(x)$ در F را در نظر می‌گیریم. بنا به قضیه‌ی ۶.۲.۱۴، یک یکریختی $\alpha : K(a) \longrightarrow K(b)$ وجود دارد که هر عضو K را ثابت نگه می‌دارد و $\alpha(a) = b$. چون α هر عضو K را ثابت نگه می‌دارد ، $\alpha(f(x)) = f(x)$. اکنون $F : K(a)$ و $F : K(b)$ توسیع‌های تجزیه برای $\alpha(f(x)) = f(x)$ هستند ، پس بنا به قضیه‌ی ۷.۲.۱۴، یکریختی $\beta : F \longrightarrow F$ وجود دارد که توسیع α است. چون β، K را ثابت می‌دارد ، طبق فرض داریم $\beta(L) = L$. به ویژه $b = \beta(a) \in \beta(L) = L$. بنابراین همه‌ی ریشه‌های $p(x)$ در L هستند. از این‌رو $L : K$ توسیع نرمال است. □

توسیع $F : K$ را توسیع گالوا گوییم، هرگاه متناهی، نرمال، و جداپذیر باشد. بنا به قضیه‌ی ۴.۷.۱۴، توسیع متناهی $F : K$ توسیع گالوا است اگر و تنها اگر توسیع تجزیه‌ی یک چندجمله‌ای جداپذیر روی K باشد. هم‌چنین، با توجه به نتیجه‌ی ۵.۵.۱۴، چون توسیع متناهی $F : K$ توسیع گالوا است اگر و تنها اگر $|\mathrm{Aut}_K F| = [F : K]$، خواهیم داشت :

نتیجه ۶.۷.۱۴. اگر $F : K$ توسیع گالوا و L یک میدان واسطه باشد، آن‌گاه داریم $|\mathrm{Aut}_K L| = [L : K]$ اگر و تنها اگر به ازای هر $\alpha \in \mathrm{Aut}_K F$، داشته باشیم $\alpha(L) = L$، یعنی $\alpha|_L \in \mathrm{Aut}_K L$. □

تمرین‌ها

۱. (الف) آیا $\mathbb{C}$ توسیع نرمال $\mathbb{R}$ است؟ (ب) آیا $\mathbb{R}$ توسیع نرمال $\mathbb{Q}$ است؟

۲. نشان دهید توسیع جبری $F : K$ نرمال است اگر و تنها اگر چندجمله‌ای می‌نیمال هر عضو $a \in F$ روی $K[x]$ کاملاً در F تجزیه شود.

۳. فرض کنید $F : K$ توسیع نرمال و L یک میدان میانی باشد
(الف) نشان دهید $F : L$ توسیع نرمال است.
(ب) نشان دهید $L : K$ لزوماً توسیع نرمال نیست.

۴. فرض کنید $\mathrm{char}\, K = ۰$ و $F : K$ توسیع نرمال متناهی باشد. فرض کنید $g(x) \in K[x]$ و E توسیع تجزیه‌ی $g(x)$ روی F باشد. نشان دهید $E : K$ توسیع نرمال است.

۸.۱۴ قضیه‌ی اساسی نظریه‌ی گالوا

در تمرین ۱ از صفحه‌ی ۳۱۸، دیدیم که اگر $F : K$ توسیع باشد، مجموعه‌ی K- خودریختی‌های F، یعنی $\mathrm{Aut}_K F$ (گروه خودریختی‌های F نسبت به K) زیرگروهی از $\mathrm{Aut}\, F$ است. اکنون فرض کنید G زیرمجموعه‌ی از $\mathrm{Aut}\, F$ باشد. می‌خواهیم یک زیرمیدان از F به G نظیر کنیم. تعریف می‌کنیم

$$F_G = \{a \in F \mid \forall \alpha \in G, \quad \alpha(a) = a\}.$$

چون به ازای هر $\alpha \in G$، $\alpha(۰) = ۰$ و $\alpha(۱) = ۱$، پس $۰, ۱ \in F_G$ و $F_G \neq \emptyset$. فرض کنید $a, b \in F_G$. به ازای هر $\alpha \in G$ داریم

$$\alpha(a - b) = \alpha(a) - \alpha(b) = a - b.$$

بنابراین $a - b \in F_G$. اگر $b \neq ۰$، آن‌گاه

$$\alpha(ab^{-۱}) = \alpha(a)\alpha(b)^{-۱} = ab^{-۱}$$

و $ab^{-۱} \in F_G$. از این‌رو F_G زیرمیدان F است. F_G را میدان ثابت F نسبت به G گوییم. بنابراین اگر $G \subseteq \mathrm{Aut}\, F$ آن‌گاه $F : F_G$ یک توسیع است.
هر مجموعه متشکل از خودریختی‌های میدان F مستقل خطی است. این مطلب محتوای قضیه‌ی بعد است:

قضیه ۱.۸.۱۴. فرض کنید F یک میدان و $\alpha_۱$، ...، α_n خودریختی‌های متمایز F باشند. در این صورت به ازای هر $a \in F$ و هر $a_۱, \ldots, a_n \in F$، اگر

$$a_۱\alpha_۱(a) + \cdots + a_n\alpha_n(a) = ۰,$$

آن‌گاه $a_۱ = \cdots = a_n = ۰$.

اثبات. به استقرا روی n، عمل می‌کنیم. اگر $n = ۱$ و به ازای هر $a \in F$، داشته باشیم $a_۱\alpha_۱(a) = ۰$، آن‌گاه $a_۱ = a_۱\alpha_۱(۱) = ۰$.
حال فرض کنید حکم برای هر m که $۱ \leq m < n$، درست باشد. فرض کنید اعضای $a_۱, \ldots, a_n \in F$ وجود دارند که همگی با هم صفر نیستند مثلاً $a_۱ \neq ۰$ و

$$a_۱\alpha_۱(a) + \cdots + a_n\alpha_n(a) = ۰, \quad \forall a \in F \tag{۳}$$

چون خودریختی‌های α_1، ...، α_n متمایزند، $b \in F$ وجود دارد که $\alpha_1(b) \neq \alpha_n(b)$. چون معادله‌ی (۳) به ازای هر $a \in F$ برقرار است، داریم

$$a_1\alpha_1(ab) + \cdots + a_n\alpha_n(ab) = 0$$

یا

$$a_1\alpha_1(a)\alpha_1(b) + \cdots + a_n\alpha_n(a)\alpha_n(b) = 0, \quad \forall a \in F \tag{۴}$$

اگر معادله‌ی (۳) را در $\alpha_n(b)$ ضرب کنیم و حاصل‌ضرب از معادله‌ی (۴) کم کنیم، به ازای هر $a \in F$، خواهیم داشت

$$a_1(\alpha_1(b) - \alpha_n(b))\alpha_1(a) + \cdots + a_{n-1}(\alpha_{n-1}(b) - \alpha_n(b))\alpha_{n-1}(a) = 0.$$

چون $\alpha_1(b) \neq \alpha_n(b)$، $\alpha_1(b) - \alpha_n(b) \neq 0$. این با فرض استقرا متناقض است. بنابراین $a_1 = \cdots = a_n = 0$. □

قضیه ۲.۸.۱۴. فرض کنید F یک میدان و A زیرمجموعه‌ی متناهی از $\mathrm{Aut}\, F$ باشد، در این صورت $|A| \leq [F : F_A]$.

اثبات. فرض کنید چنین نباشد و $|A| > [F : F_A]$. چون $|A|$ متناهی است، $[F : F_A]$ نیز متناهی است، مثلاً $[F : F_A] = n$. فرض کنید a_1، ...، a_n پایه‌ای برای F روی F_A است. چون $|A| > n$، پس $n+1$ خودریختی متمایز α_1، ...، α_{n+1} در $\mathrm{Aut}_{F_A} F$ وجود دارند، توجه کنید طبق تعریف، داریم $A \subseteq \mathrm{Aut}_{F_A} F$. دستگاه n معادله و $n+1$ مجهول زیر را در نظر بگیرید.

$$\begin{cases} \alpha_1(a_1)x_1 + \cdots + \alpha_{n+1}(a_1)x_{n+1} = 0 \\ \alpha_1(a_2)x_1 + \cdots + \alpha_{n+1}(a_2)x_{n+1} = 0 \\ \vdots \qquad\qquad\qquad\qquad \vdots \\ \alpha_1(a_n)x_1 + \cdots + \alpha_{n+1}(a_n)x_{n+1} = 0 \end{cases}$$

چون تعداد مجهولات از تعداد معادلات بیشتر است، این دستگاه در F جواب نابدیهی $x_1 = b_1$، ...، $x_{n+1} = b_{n+1}$ دارد. بنابراین

$$\alpha_1(a_i)b_1 + \cdots + \alpha_{n+1}(a_i)b_{n+1} = 0, \quad i = 1, 2, \ldots, n \tag{۵}$$

فرض کنید $a \in F$ عضو دلخواهی باشد. چون a_n، ...، a_1 پایه‌ای برای F روی F_A است، عناصر $k_1, \ldots, k_n \in F_A$ وجود دارند که $a = \sum_{i=1}^{n} k_i$. اگر در معادلات (۵) معادله‌ی iام را در k_i ضرب و همه‌ی معادلات حاصل‌ضرب را جمع کنیم، با توجه به این که هر α_i^n، k_1، ...، k_n را ثابت نگه می‌دارد ، خواهیم داشت

$$\begin{aligned} 0 &= \sum_{i=1}^{n} \left(k_i\alpha_1(a_i)b_1 + \cdots + k_i\alpha_{n+1}(a_i)b_{n+1} \right) \\ &= \sum_{i=1}^{n} \left(\alpha_1(k_i)b_1 + \cdots + \alpha_{n+1}(k_i)b_{n+1} \right) \\ &= \alpha_1\left(\sum_{i=1}^{n} k_i \right) b_1 + \cdots + \alpha_{n+1}\left(\sum_{i=1}^{n} k_i \right) b_{n+1} \\ &= b_1\alpha_1(a) + \cdots + b_{n+1}\alpha_{n+1}(a), \end{aligned}$$

که این متناقض با قضیه‌ی ۱.۸.۱۴، است. بنابراین $|A| \leq [F : F_A]$. □

در قضیه‌ی ۲.۸.۱۴، ثابت کردیم که تعداد اعضای هر زیرمجموعه از خودریختی‌های میدان F کمتر یا مساوی درجه‌ی F روی زیرمیدان ثابت آن زیرمجموعه است. حال ثابت می‌کنیم که در حالتی که زیرمجموعه، زیرگروه باشد تساوی برقرار است:

قضیه ۳.۸.۱۴. فرض کنید F یک میدان و G زیرگروهی متناهی از $\mathrm{Aut}\, F$ باشد، در این صورت $|G| = [F : F_G]$.

اثبات. طبق قضیه‌ی ۲.۸.۱۴، $|G| \leq [F : F_G]$. حال ثابت می‌کنیم $|G| \geq [F : F_G]$. فرض کنید چنین نباشد و $n = |G| < [F : F_G]$. بنابراین عناصر $a_1, a_2, \ldots, a_{n+1} \in F$ وجود دارند که روی F_G مستقل خطی‌اند. فرض کنید $G = \{\alpha_1, \alpha_2, \ldots, \alpha_n\}$. دستگاه n معادله و $n+1$ مجهول زیر را در نظر می‌گیریم

$$\begin{cases} x_1\alpha_1(a_1) + \cdots + x_{n+1}\alpha_1(a_{n+1}) = 0 \\ x_1\alpha_2(a_1) + \cdots + x_{n+1}\alpha_2(a_{n+1}) = 0 \\ \vdots \qquad\qquad\qquad\qquad \vdots \\ x_1\alpha_n(a_1) + \cdots + x_{n+1}\alpha_n(a_{n+1}) = 0. \end{cases}$$

چون تعداد مجهولات از تعداد معادلات بیشتر است، این دستگاه در F جواب نابدیهی $x_1 = b_1$، ...، $x_{n+1} = b_{n+1}$ دارد. پس

$$b_1\alpha_i(a_1) + \cdots + b_{n+1}\alpha_i(a_{n+1}) = 0, \quad i = 1, 2, \ldots, n \tag{۶}$$

از بین همه‌ی جوابهای نابدیهی دستگاه فوق، جوابی را انتخاب می‌کنیم که کم‌ترین عضو ناصفر، مثلاً m عضو، داشته باشد. در این صورت $m > 1$، زیرا اگر $m = 1$، $b_1\alpha_1(a_1) = 0$ که نتیجه می‌دهد $b_1 = 0$ یا $\alpha_1(a_1) = 0$. حالت اخیر امکان ندارد زیرا $a_1 \neq 0$ و α_1 یک‌به‌یک است. چون $m = 1$، حالت $b_1 = 0$ نیز امکان ندارد. با تعویض ترتیب b_i ها، فرض می‌کنیم $x_1 = b_1$، ...، $x_m = b_m$ مقادیر ناصفر جواب دستگاه باشند و به علاوه با ضرب معادله ها در b_m^{-1} فرض می‌کنیم $b_m = 1$. بنابراین معادلات (۶) به صورت زیر در می‌دهند:

$$b_1\alpha_i(a_1) + \cdots + b_{m-1}\alpha_i(a_{m-1}) + b_m\alpha_i(a_m) = 0, \quad i = 1, 2, \ldots, n \tag{۷}$$

فرض کنید α_1 نگاشت همانی باشد. پس در معادلات فوق با $i = 1$ داریم

$$b_1a_1 + \cdots + b_{m-1}a_{m-1} + b_ma_m = 0.$$

چون a_1، ...، a_m روی F_G مستقل خطی‌اند، حداقل یکی از b_1، ...، b_m در F_G نیست، مثلاً $b_1 \notin F_G$. بنابراین $2 \leq j \leq n$ وجود دارد که $\alpha_j(b_1) \neq b_1$. اگر α_j را بر معادلات (۷) اثر دهیم خواهیم داشت

$$\alpha_j(b_1(\alpha_i(a_1)) + \cdots + \alpha_j(b_m\alpha_i(a_m)) = 0, \quad i = 1, 2, \ldots, n$$

یا

$$\alpha_j(b_1)\alpha_j(\alpha_i(a_1)) + \cdots + \alpha_j(b_m)\alpha_j(\alpha_i(a_m)) = 0, \quad i = 1, 2, \ldots, n.$$

چون G گروه است، $\{\alpha_j\alpha_1, \alpha_j\alpha_2, \ldots, \alpha_j\alpha_n\} = G$.
پس با اندیس‌گذاری مجدد، معادله های فوق را به صورت

$$\alpha_j(b_1)\alpha_i(a_1) + \cdots + \alpha_j(b_m)\alpha_i(a_m) = 0, \quad i = 1, 2, \ldots, n$$

می‌نویسیم. اگر معادلات اخیر را از معادلات (۷) کم کنیم و توجه کنیم که $b_m = 1$، به ازای هر $i = 1, 2, \ldots, n$، خواهیم داشت

$$(b_1 - \alpha_j(b_1))\alpha_i(a_1) + \cdots + (b_{m-1} - \alpha_j(b_{m-1}))\alpha_i(a_{m-1}) = 0.$$

چون $b_1 - \alpha_j(b_1) \neq 0$، $b_1 - \alpha_j(b_1)$، $b_2 - \alpha_j(b_2)$، ...، $b_{m-1} - \alpha_j(b_{m-1})$، 0، 0، ...، 0 جواب نابدیهی از معادلات (۶) است که تعداد عناصر ناصفر آن از m کمتر است. این متناقض با انتخاب m است. پس فرض $|G| < [F : F_G]$ به تناقض منجر شد. در نتیجه $|G| \geq [F : F_G]$. بنابراین $|G| = [F : F_G]$. □

فرض کنید $F : K$ توسیع باشد. اگر L یک میدان میانی باشد، آنگاه به وضوح داریم $\mathrm{Aut}_L F \leq \mathrm{Aut}_K F$. برعکس اگر $G \leq \mathrm{Aut}_K F$، آنگاه F_G، میدان ثابت G، یک زیرمیدان F حاوی K است. قرار می‌دهیم $\mathscr{A} = \{L \mid K \subseteq L \subseteq F,$ میدان $L\}$ و $\mathscr{B} = \{G \mid G \leq \mathrm{Aut}_K F\}$. بنابراین توابع $\gamma : \mathscr{A} \longrightarrow \mathscr{B}$ و $\varphi : \mathscr{B} \longrightarrow \mathscr{A}$ با $\gamma(L) = \mathrm{Aut}_L F$ و $\varphi(G) = F_G$ را داریم. در ادامه از این نمادها استفاده می‌کنیم.

قضیه ۴.۸.۱۴. فرض کنید F یک میدان و G زیرگروه متناهی از $\operatorname{Aut} F$ باشد، در این صورت $G = \operatorname{Aut}_{F_G} F$، یعنی $\gamma\varphi(G) = G$.

اثبات. قرار می‌دهیم $H = \operatorname{Aut}_{F_G} F$. به وضوح $G \subseteq H$. زیرا اگر $\alpha \in G$، آنگاه به ازای هر $a \in F_G$، $\alpha(a) = a$ و $\alpha \in \operatorname{Aut}_{F_G} F = H$. با اثباتی مشابه اثبات قضیه‌ی ۲.۸.۱۴، می‌توان ثابت کرد H متناهی است. پس با توجه به قضیه‌ی ۳.۸.۱۴، $|H| = [F : F_H]$. اکنون توجه کنید $F_G = F_H$؛ زیرا ، بنا به تعریف H، $F_G \supseteq F_H$ و اگر $a \in F_G$، آنگاه به ازای هر $\alpha \in H$، $\alpha(a) = a$، یعنی $a \in F_H$. بنابراین

$$|G| = [F : F_G] = [F : F_H] = |H|.$$

چون $G \subseteq H$ و H متناهی است، $G = H$. □

قضیه ۵.۸.۱۴. فرض کنید $K : F$ توسیع باشد. فرض کنید L و M دو میدان میانی و H و T زیرگروه‌های $\operatorname{Aut}_K F$ باشند. در این صورت

(الف) اگر $L \subseteq M$، آنگاه $\gamma(L) \supseteq \gamma(M)$.

(ب) اگر $H \subseteq T$، آنگاه $\varphi(H) \supseteq \varphi(T)$.

(ج) $L \subseteq \varphi\gamma(L)$.

(د) $H \subseteq \gamma\varphi(H)$.

(هـ) $\varphi(H) = \varphi\gamma\varphi(H)$.

(و) $\gamma(L) = \gamma\varphi\gamma(L)$.

اثبات. (الف) داریم $\gamma(L) \supseteq \gamma(M)$، زیرا

$$\begin{aligned} \alpha \in \gamma(M) = \operatorname{Aut}_M F &\implies \forall a \in M, \quad \alpha(a) = a \\ &\implies \forall a \in L, \quad \alpha(a) = a \quad (L \subseteq M \text{ چون}) \\ &\implies \alpha \in \gamma(L). \end{aligned}$$

(ب) داریم

$$\begin{aligned} a \in \varphi(T) = F_T &\implies \forall \alpha \in T, \quad \alpha(a) = a \\ &\implies \forall \alpha \in H, \quad \alpha(a) = a \quad (H \subseteq T \text{ چون}) \\ &\implies a \in F_H = \varphi(H). \end{aligned}$$

بنابراین $\varphi(H) \supseteq \varphi(T)$.

(ج) طبق تعریف $\gamma(L)$ داریم

$$\begin{aligned} \ell \in L &\implies \forall \alpha \in \gamma(L), \quad \alpha(\ell) = \ell \\ &\implies \ell \in \varphi\gamma(L). \end{aligned}$$

بنابراین $L \subseteq \varphi\gamma(L)$.

(د) طبق تعریف $\varphi(H)$ داریم

$$\begin{aligned} \alpha \in H &\implies \forall a \in \varphi(H), \quad \alpha(a) = a \\ &\implies \alpha \in \gamma\varphi(H). \end{aligned}$$

بنابراین $H \subseteq \gamma\varphi(H)$.

(هـ) طبق (د) داریم $H \subseteq \gamma\varphi(H)$. بنابراین طبق (ب)، $\varphi(H) \supseteq \varphi\gamma\varphi(H)$. از طرف دیگر در (ج) به ازای $L = \varphi(H)$ داریم

$\varphi(H) \subseteq \varphi\gamma\varphi(H)$.
(و) طبق (ج) داریم $L \subseteq \varphi\gamma(L)$. بنابراین طبق (الف)، $\gamma(L) \supseteq \gamma\varphi\gamma(L)$. از طرف دیگر در (د) به ازای $H = \gamma(L)$ داریم $\gamma(L) \subseteq \gamma\varphi\gamma(L)$. □

قضیه ۶.۸.۱۴. فرض کنید $F : K$ توسیع باشد و $G = \mathrm{Aut}_K F$. شرایط زیر معادل‌اند
(الف) $\varphi(G) = K$.
(ب) $\varphi\gamma(K) = K$.
(ج) اگر $a \in F - K$، آنگاه $\alpha \in G$ وجود دارد که $\alpha(a) \neq a$.

اثبات. چون $\gamma(K) = \mathrm{Aut}_K F = G$، داریم $\varphi\gamma(K) = \varphi(G)$. پس (الف) و (ب) معادل‌اند. اکنون چون $\varphi(G) = F_G = \{a \in F \mid \forall \alpha \in G,\ \ \alpha(a) = a\}$، (الف) و (ج) نیز معادل‌اند. □

قضیه ۷.۸.۱۴. اگر $F : K$ توسیع متناهی باشد، آنگاه $F : K$ توسیع گالوا است اگر و تنها اگر $\varphi(G) = K$، یعنی $\varphi\gamma(K) = K$، که در آن $G = \mathrm{Aut}_K F$.

اثبات. فرض کنید $F : K$ توسیع گالوا باشد. بنا به نتیجه‌ی ۵.۵.۱۴، $|G| = [F : K]$. اما با توجه به قضیه‌ی ۳.۸.۱۴، $[F : F_G] = |G|$. اکنون چون $K \subseteq F_G \subset F$، بنا به قانون برج داریم

$$[F : K] = [F : F_G][F_G : K].$$

بنابراین $[F_G : K] = ۱$ و $\varphi(G) = F_G = K$. اثبات عکس مطلب را به عنوان تمرین واگذار می‌کنیم. □

قضیه ۸.۸.۱۴. (قضیه‌ی اساسی نظریه‌ی گالوا) فرض کنید $F : K$ توسیع گالوا باشد. اگر $\mathscr{A}$ مجموعه‌ی زیرمیدان‌های میانی و $\mathscr{B}$ مجموعه‌ی زیرگروه‌های $G = \mathrm{Aut}_K F$ باشند، آنگاه
(الف) نگاشت $\gamma : \mathscr{A} \longrightarrow \mathscr{B}$ با ضابطه‌ی $\gamma(L) = \mathrm{Aut}_L F$، به ازای هر $L \in \mathscr{A}$، نگاشت یک‌به‌یک و پوشاست. نگاشت $\varphi : \mathscr{B} \longrightarrow \mathscr{A}$ با ضابطه‌ی $\varphi(H) = F_H$، به ازای هر $H \in \mathscr{B}$ وارون γ است. به علاوه به ازای هر $L \in \mathscr{A}$، $[F : L] = |\mathrm{Aut}_L F|$ و $[L : K] = |\mathrm{Aut}_K F : \mathrm{Aut}_L F|$.
(ب) اگر $M \in \mathscr{A}$ و L، آنگاه $M \subseteq L$ اگر و تنها اگر $\gamma(M) \supseteq \gamma(L)$. در این حالت $[L : M] = |\gamma(M) : \gamma(L)|$.
(ج) اگر $H, T \in \mathscr{B}$، آنگاه $T \subseteq H$ اگر و تنها اگر $\varphi(T) \supseteq \varphi(H)$، در این حالت $|H : T| = [\varphi(T) : \varphi(H)]$.
(د) فرض کنید $L, M \in \mathscr{A}$. قرار می‌دهیم $\gamma(L) = H$ و $\gamma(M) = T$. اگر $\alpha \in G$، آنگاه $\alpha(L) = M$ اگر و تنها اگر $T = \alpha H \alpha^{-۱}$.
(هـ) اگر $L \in \mathscr{A}$، آنگاه $L : K$ توسیع نرمال است اگر و تنها اگر $H = \mathrm{Aut}_L F$ زیرگروه نرمالی از G باشد. در این حالت $G/H \cong \mathrm{Aut}_K L$.

اثبات. (الف) چون $F : K$ توسیع گالوا است، به ازای هر میدان میانی L، توسیع $F : L$ نیز گالوا است. پس بنا به قضیه‌ی ۷.۸.۱۴، $\varphi\gamma(L) = L$. از طرف دیگر چون $\mathrm{Aut}_K F$ متناهی است، زیرگروه H از $\mathrm{Aut}_K F$ نیز متناهی است. در نتیجه بنا به قضیه‌ی ۴.۸.۱۴، $\gamma\varphi(H) = H$. از این‌رو φ و γ، یک‌به‌یک ، پوشا و وارون یکدیگر هستند.
بنا به نتیجه ۵.۵.۱۴، $|\mathrm{Aut}_L F| = [F : L]$. اکنون بنا به قانون برج داریم

$$|\mathrm{Aut}_K F : \mathrm{Aut}_L F| = \frac{|\mathrm{Aut}_K F|}{|\mathrm{Aut}_L F|} = \frac{[F : K]}{[F : L]} = [L : K].$$

(ب) با توجه به قضیه‌ی ۵.۸.۱۴ و این که φ و γ وارون هم هستند ، واضح است که $M \subseteq L$ اگر و تنها اگر $\gamma(M) \supseteq \gamma(L)$. اکنون چون $F : M$ توسیع نرمال است، بنا به (الف)، که M را به جای K قرار داده‌ایم،

$$[\gamma(M) : \gamma(L)] = |\mathrm{Aut}_M F : \mathrm{Aut}_L F| = [L : M].$$

(ج) با توجه به قضیه‌ی ۵.۸.۱۴ و این که φ و γ وارون هم هستند ، واضح است که $T \subseteq H$ اگر و تنها اگر $\varphi(T) \supseteq \varphi(H)$. قرار می‌دهیم $\varphi(H) = M$ و $\varphi(T) = L$. پس $M \subseteq L$ و بنا به (الف) $\gamma(M) = \gamma\varphi(H) = H$ و $\gamma(L) = \gamma\varphi(T) = T$. بنابراین بنا به (ب)

$$|H : T| = |\gamma(M) : \gamma(L)| = [L : M] = [\varphi(T) : \varphi(H)].$$

(د) فرض کنید $\alpha(L) = M$. به ازای هر $b \in M$ عضو $a \in L$ وجود دارد که $\alpha(a) = b$. اکنون به ازای هر $\beta \in H = \gamma(L)$، $\beta(a) = a$. بنابراین

$$(\alpha\beta\alpha^{-1})(b) = \alpha(\beta(\alpha^{-1}(b))) = \alpha(\beta(a)) = \alpha(a) = b.$$

پس $\alpha\beta\alpha^{-1} \in \gamma(M) = T$. چون $\beta \in H$ دلخواه بود $\alpha H\alpha^{-1} \subseteq T$. از طرف دیگر

$$\begin{aligned} |T| &= |\gamma(M)| = [F : M] = [F : \alpha(L)] = [F : L] = |\gamma(L)| = |H| \\ &= |\alpha H\alpha^{-1}|. \end{aligned}$$

در نتیجه $\alpha H\alpha^{-1} = T$.

حال برعکس فرض کنید $\alpha H\alpha^{-1} = T$. به ازای هر $a \in L$ و هر $\beta \in H = \gamma(L)$ داریم

$$\alpha(\beta(\alpha^{-1}(\alpha(a)))) = \alpha(\beta(a)) = \alpha(a),$$

و $\alpha(a) \in \varphi(\alpha H\alpha^{-1}) = \varphi(T)$. اکنون داریم $\alpha(L) \subseteq \varphi(T) = \varphi\gamma(M) = M$

$$|H| = |\alpha H\alpha^{-1}| = |T| = |\gamma(M)|.$$

که نتیجه می‌دهد $[F : L] = [F : M]$ و بنابراین

$$[\alpha(L) : K] = [L : K] = \frac{[F : K]}{[F : L]} = \frac{[F : K]}{[F : M]} = [M : K].$$

اکنون چون $K \subseteq \alpha(L) \subseteq M$، بنا به قانون برج $[M : K] = [M : \alpha(L)][\alpha(L) : K]$. از این‌رو $[M : \alpha(L)] = ۱$ و $M = \alpha(L)$.

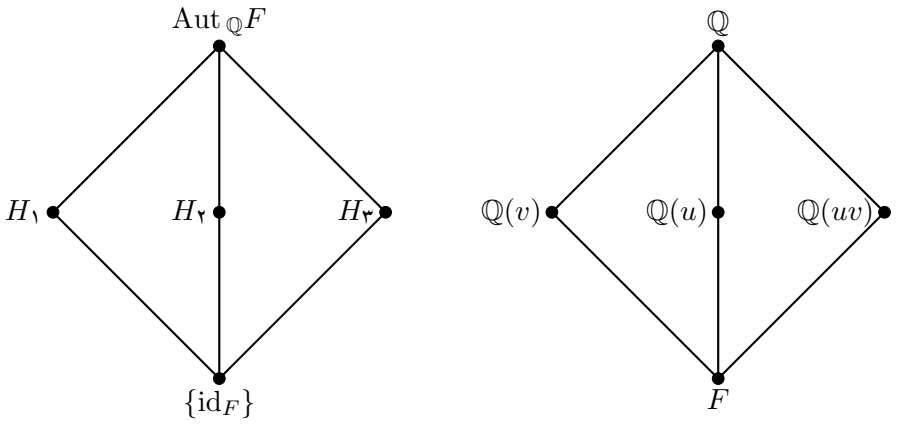
(هـ) H زیرگروه نرمالی از G است اگر و تنها اگر به ازای هر $\alpha \in G$، $H = \alpha H\alpha^{-1}$. بنا به (د) $\alpha H\alpha^{-1} = H$ اگر و تنها اگر $\alpha(L) = L$. اما بنا به قضیه‌ی ۵.۷.۱۴، $L : K$ نرمال است اگر و تنها اگر به ازای هر $\alpha \in G$، $\alpha(L) = L$. بنابراین $L : K$ توسیع نرمال است اگر و تنها اگر به ازای هر $\alpha \in G$، $H = \alpha H\alpha^{-1}$. اکنون چون به ازای هر $\alpha \in G$، $\alpha(L) = L$، تابع $\psi : G \longrightarrow \mathrm{Aut}_K L$ با ضابطه‌ی $\psi(\alpha) = \alpha|_L$ خوش تعریف است. این تابع به وضوح همریختی است. به علاوه ψ پوشاست؛ زیرا اگر $\sigma \in \mathrm{Aut}_K L$، آنگاه چون $F : L$ توسیع نرمال و بنابراین توسیع تجزیه‌ی یک چندجمله‌ای $f(x) \in L[x]$ است، بنا به قضیه‌ی ۷.۲.۱۴، یک K- خودریختی $\alpha : F \longrightarrow F$ وجود دارد که توسیع σ است. پس $\psi(\alpha) = \alpha|_L = \sigma$. در نهایت

$$\begin{aligned} \alpha \in \ker\psi &\iff \alpha|_L = \mathrm{id}_L \\ &\iff \forall a \in L, \quad \alpha(a) = a \\ &\iff \alpha \in \mathrm{Aut}_L F = H. \end{aligned}$$

بنابراین $\ker\psi = H$ و بنا به اولین قضیه‌ی یکریختی، $G/H \cong \mathrm{Im}\,\psi = \mathrm{Aut}_K L$. □

مثال ۹.۸.۱۴. فرض کنید $f(x) = (x^۲ - ۲)(x^۲ - ۳) \in \mathbb{Q}[x]$. قرار می‌دهیم $u = \sqrt{۲}$ و $v = \sqrt{۳}$ و $F = \mathbb{Q}(u, v)$. در مثال ۱۰.۵.۱۴، دیدیم که $F : \mathbb{Q}$ توسیع تجزیه‌ی $f(x)$ است و $\mathrm{Aut}_{\mathbb{Q}} F = \langle \alpha, \beta \rangle \cong C_۲ \times C_۲$. که در آن $\alpha(u) = -u$ و $\alpha(v) = v$ و $\beta(u) = u$ و $\beta(v) = -v$. زیرگروه‌های $\mathrm{Aut}_{\mathbb{Q}} F$ عبارت‌اند از $H_۰ = \{\mathrm{id}_F\}$، $H_۱ = \langle \alpha \rangle$، $H_۲ = \langle \beta \rangle$، $H_۳ = \langle \alpha\beta \rangle$، $H_۴ = \mathrm{Aut}_{\mathbb{Q}} F$. طبق قضیه‌ی اساسی نظریه‌ی گالوا زیرمیدان متناظر H عبارت است از

$$F_H = \{a \in F \mid \forall \alpha \in H, \quad \alpha(a) = a\}.$$



شکل ۱.۱۴: نمودار زیرمیدان‌های $F = \mathbb{Q}(u, v)$ و زیرگروه‌های $\mathrm{Aut}_{\mathbb{Q}}F$.

بنابراین زیرمیدان‌های میانی توسیع $F : \mathbb{Q}$ عبارت‌اند از

$$F_{H_0} = F, \quad F_{H_1} = \mathbb{Q}(v), \quad F_{H_2} = \mathbb{Q}(u), \quad F_{H_3} = \mathbb{Q}(uv), \quad F_{H_4} = \mathbb{Q}.$$

نمودار زیرمیدان‌های F و زیر گروه‌های $\mathrm{Aut}_{\mathbb{Q}}F$ در شکل ۱.۱۴ داده شده‌اند. چون $\mathrm{Aut}_{\mathbb{Q}}F$ آبلی است، هر زیرگروه آن نرمال است، و توسیع‌های $F_{H_i} : \mathbb{Q}$، $i = 0, 1, 2, 3, 4$ همگی توسیع‌های نرمال هستند. □

مثال ۱۰.۸.۱۴. فرض کنید $x^3 - 2 \in \mathbb{Q}[x]$. قرار می‌دهیم $w = e^{2\pi i/3}$ و $u = \sqrt[3]{2}$ و $F = \mathbb{Q}(u, w)$. در مثال ۱۱.۵.۱۴، دیدیم $F : \mathbb{Q}$ توسیع تجزیه برای $x^3 - 2$ است و $\mathrm{Aut}_{\mathbb{Q}}F = \langle \alpha, \beta \rangle \cong S_3$، که در آن $\alpha(u) = uw^2$، $\alpha(w) = w^2$، و $\beta(u) = uw$، $\beta(w) = w$. به علاوه $O(\alpha) = 2$ و $O(\beta) = 3$. زیرگروه‌های $\mathrm{Aut}_{\mathbb{Q}}F$ عبارت‌اند از $H_0 = \{\mathrm{id}_F\}$، $H_1 = \langle \alpha \rangle$، $H_2 = \langle \beta \rangle$، $H_3 = \langle \alpha\beta \rangle$، $H_4 = \langle \alpha\beta^2 \rangle$، و $H_5 = \mathrm{Aut}_{\mathbb{Q}}F$. طبق قضیه‌ی اساسی نظریه‌ی گالوا زیرمیدان متناظر H عبارت است از

$$F_H = \{a \in F \mid \forall \alpha \in H, \quad \alpha(a) = a\}.$$

بنابراین زیرمیدان‌های میانی توسیع $F : \mathbb{Q}$ عبارت‌اند از

$$F_{H_0} = F, \quad F_{H_1} = \mathbb{Q}(uw), \quad F_{H_2} = \mathbb{Q}(w),$$
$$F_{H_3} = \mathbb{Q}(uw^2), \quad F_{H_4} = \mathbb{Q}(u), \quad F_{H_5} = \mathbb{Q}.$$

بررسی نمودار زیرگروه‌های $\mathrm{Aut}_{\mathbb{Q}}F$ و زیرمیدان‌های متناظر آن‌ها در F را به عنوان تمرین واگذار می‌کنیم. زیرگروه‌های نرمال $\mathrm{Aut}_{\mathbb{Q}}F$ عبارت‌اند از H_0، H_2، H_5، پس توسیع‌های $F_{H_i} : \mathbb{Q}$، $i = 0, 2, 5$ توسیع‌های نرمال هستند. زیرگروه‌های H_1، H_3، H_4 در $\mathrm{Aut}_{\mathbb{Q}}F$ نرمال نیستند، در نتیجه توسیع‌های $F_{H_i} : \mathbb{Q}$، $i = 1, 3, 4$ توسیع‌های نرمال نیستند. □

این بخش را با اثبات قضیه‌ی معروف اساسی جبر به پایان می‌بریم:

قضیه ۱۱.۸.۱۴. (قضیه‌ی اساسی جبر) هر چندجمله‌ای $f(x) \in \mathbb{C}[x]$ با درجه‌ی $n \geq 1$ حداقل یک ریشه در $\mathbb{C}$ دارد.

اثبات. اثبات را به برهان خلف انجام می‌دهیم: فرض کنید، بر خلاف حکم ، $f(x)$ در $\mathbb{C}$ هیچ ریشه ای نداشته باشد. $\bar{f}(x)$ را مزدوج مختلط $f(x)$ در نظر می‌گیریم. بنابراین اگر $f(x) = \sum_{j=0}^{n} a_j x^j$، آنگاه $\bar{f}(x) = \sum_{j=0}^{n} \overline{a_j} x^j$. ادعا می‌کنیم ضرایب $f(x)\bar{f}(x)$ حقیقی‌اند. اگر c_k ضرایب x^k در $f(x)\bar{f}(x)$ باشد، داریم

$$c_k = a_0\overline{a_k} + a_1\overline{a_{k-1}} + \cdots + a_k\overline{a_0}.$$

بنابراین

$$\begin{aligned}\overline{c_k} &= \overline{a_۰\overline{a_k} + a_۱\overline{a_{k-۱}} + \cdots + a_k\overline{a_۰}} \\ &= \bar{a}_۰a_k + \overline{a_۱}a_{k-۱} + \cdots + \overline{a_k}a_۰ \\ &= c_k.\end{aligned}$$

از این‌رو $f(x)\bar{f}(x) \in \mathbb{R}[x]$. از طرف دیگر چون $\overline{f(a)} = \bar{f}(\bar{a})$، a ریشه‌ای از $f(x)$ است اگر و تنها اگر $\bar{a}$ ریشه‌ای از $\bar{f}(x)$ باشد. چون $f(x)$ ریشه‌ای در $\mathbb{C}$ ندارد، $\bar{f}(x)$ نیز در $\mathbb{C}$ ندارد. بنابراین $f(x)\bar{f}(x)$ نیز ریشه‌ای در $\mathbb{C}$ ندارد. فرض کنید $g(x) = f(x)\bar{f}(x)$، پس $\deg g(x)$ زوج است. فرض کنید $F : \mathbb{R}$ توسیع تجزیه‌ی $g(x)(x^۲ + ۱)$ باشد. چون i ریشه‌ای از $g(x)(x^۲ + ۱)$ است، $i \in F$. بنابراین $\mathbb{R} \subseteq \mathbb{C} \subseteq F$. به علاوه چون $\operatorname{char}\mathbb{R} = ۰$، توسیع $F : \mathbb{R}$ توسیع گالوا است. فرض کنید $G = \operatorname{Aut}_{\mathbb{R}}F$ گروه گالوای توسیع $F : \mathbb{R}$ باشد. اگر P یک ۲- زیرگروه سیلوی دلخواه از G با میدان ثابت $F_P = \{a \in F \mid \forall \alpha \in P,\ \ \alpha(a) = a\}$ باشد، آنگاه $[F : F_P] = |P|$. بنابراین با استفاده از قانون برج داریم

$$|G| = [F : \mathbb{R}] = [F : F_P][F_P : \mathbb{R}] = |P|[F_P : \mathbb{R}].$$

از این‌رو $[F_P : \mathbb{R}]$ فرد است. چون توسیع با درجه‌ی فرد بیش از یک از $\mathbb{R}$ وجود ندارد (تمرین ۱۰) داریم $[F_P : \mathbb{R}] = ۱$. پس $G = P$ و بنابراین $G = \operatorname{Aut}_{\mathbb{R}}F$ یک ۲- گروه است. چون $\operatorname{Aut}_{\mathbb{C}}F \leq G$، $|\operatorname{Aut}_{\mathbb{C}}F| = ۲^m$. بنابراین $\operatorname{Aut}_{\mathbb{C}}F$ یک زیرگروه H از مرتبه‌ی $۲^{m-۱}$، که لزوماً نرمال است، دارد. بنا به قضیه‌ی اساسی نظریه‌ی گالوا میدان میانی $\mathbb{C} \subseteq L \subseteq F$ وجود دارد که $H = \operatorname{Aut}_L F$. مجدداً بنا به قضیه‌ی اساسی نظریه‌ی گالوا

$$\frac{\operatorname{Aut}_{\mathbb{C}}F}{\operatorname{Aut}_L F} \cong \operatorname{Aut}_{\mathbb{C}}L,$$

به ویژه $[F : \mathbb{C}] = |\operatorname{Aut}_{\mathbb{C}}L| = ۲$. اما $\mathbb{C}$ هیچ توسیع درجه‌ی دومی ندارد (تمرین ۱۰). این یک تناقض است. □

تمرین‌ها

۱. فرض کنید $f(x) = x^۳ + bx + c$ چندجمله‌ای تحویل‌ناپذیر و جداپذیر روی میدان K باشد. اگر $F : K$ توسیع تجزیه‌ی $f(x)$ و G گروه گالوای $f(x)$ روی K باشند، نشان دهید $G \cong S_۳$، اگر و تنها اگر $D = -۴b^۳ - ۲۷c^۲$ در K مربع نباشد. اگر D در K مربع باشد نشان دهید، $[F : K] = ۳$.

۲. فرض کنید $f(x) = x^۳ + bx + c$ چندجمله‌ای تحویل‌ناپذیر و جداپذیر روی میدان K باشد. فرض کنید $F : K$ توسیع تجزیه‌ی $f(x)$ روی K باشد. اگر r ریشه‌ی دلخواهی از $f(x)$ باشد و $D = -۴b^۳ - ۲۷c^۲$، نشان دهید $F = K(\sqrt{D}, r)$.

۳. فرض کنید $f(x) = x^۳ - ۴x + ۲ \in \mathbb{Q}[x]$، نشان دهید گروه گالوای $f(x)$ با $S_۳$ یکریخت است و $\mathbb{Q}(\sqrt{۱۴۸}, r) : \mathbb{Q}$ توسیع تجزیه‌ی $f(x)$ است (r ریشه‌ی دلخواهی از $f(x)$ است).

۴. نشان دهید $f(x) = x^۳ - ۵$ گروه گالوای $f(x)$ روی $\mathbb{Q}$ با $S_۳$ یکریخت است.

۵. فرض کنید $u \neq ۱$ عدد مختلط و ریشه‌ی چندجمله‌ای $x^۵ - ۱ \in \mathbb{Q}[x]$ باشد. نشان دهید $\operatorname{Aut}_{\mathbb{Q}}\mathbb{Q}(u) \cong \mathbb{Z}_۴$. زیرمیدان‌های سره $\mathbb{Q}(u)$ را بیابید.

۶. گروه گالوای $f(x) = x^۴ - ۲ \in \mathbb{Q}[x]$ را بیابید و میدان‌های میانی $F : \mathbb{Q}$ را معین کنید، که در آن $F : \mathbb{Q}$ توسیع تجزیه‌ی $f(x)$ است.

۷. گروه گالوای توسیع $\mathbb{Q}(\sqrt[۳]{۵}, w) : \mathbb{Q}$ را بیابید، که در آن $w = \dfrac{-۱ + i\sqrt{۳}}{۲}$، و زیرمیدان‌های سره آن را مشخص کنید.

۸. گروه گالوای چندجمله‌ای‌های زیر را روی $\mathbb{Q}$ بیابید.
(الف) $(x^۲ - ۳x + ۱)^۲(x^۳ - ۲)$ (ب) $x^۴ + x^۲ + ۱$

۹. همه‌ی میدان‌های میانی $\mathbb{Q}(i, \sqrt{۵}) : \mathbb{Q}$ را بیابید.

۱۰. دو نکته که در اثبات قضیه‌ی اساسی جبر به عنوان تمرین واگذار شد را ثابت کنید:
(الف) توسیع با درجه‌ی فرد بیش از یک از $\mathbb{R}$ وجود ندارد.
(ب) توسیع با درجه‌ی زوج از $\mathbb{C}$ وجود ندارد.

۹.۱۴ حل‌پذیری چندجمله‌ای‌ها با رادیکال

یکی از فرمول‌های معروف در جبر فرمول ریشه‌های چندجمله‌ای درجه‌ی دوم $ax^۲ + bx + c = ۰$ است. با کامل کردن مربع، می‌نویسیم

$$\left(x + \frac{b}{۲}\right)^۲ = \frac{b^۲ - ۴ac}{۴a^۲}.$$

بنابراین ریشه‌های چندجمله‌ای را می‌یابیم

$$u_۱, u_۲ = \frac{-b \pm \sqrt{b^۲ - ۴ac}}{۲a}.$$

این فرمول در هر میدان K با مشخصه‌ی مخالف ۲ معتبر است و ریشه‌های این چندجمله‌ای‌ها را می‌توان با افزودن ریشه‌های دوم عناصر K به K یافت. عبارت $\Delta = b^۲ - ۴ac$ را دلتای چندجمله‌ای $ax^۲ + bx + c$ گوییم. تا قبل از قرن ۱۶ میلادی فرمولی مشابه برای چندجمله‌ای درجه‌ی ۳ پیدا نشده بود. فرض کنید چندجمله‌ای $f(y) = y^۳ + ry^۲ + sy + t$ داده شده باشد. با جای‌گذاری $y = x - \frac{۱}{۳}r$ به ازای b و c مناسب خواهیم داشت $y^۳ + ry^۲ + sy + t = x^۳ + bx + c$. بنابراین کافی است ریشه‌های چندجمله‌ای به صورت $x^۳ + bx + c$ را بیابیم. فرض کنید ریشه‌های این چندجمله‌ای $u_۱$، $u_۲$ و $u_۳$ هستند. بنابراین

$$x^۳ + bx + c = (x - u_۱)(x - u_۲)(x - u_۳).$$

با بسط عبارت سمت راست و متحد قرار دادن با سمت چپ تساوی داریم

$$\begin{aligned} u_۱ + u_۲ + u_۳ &= ۰ \\ u_۱u_۲ + u_۱u_۳ + u_۲u_۳ &= b \\ u_۱u_۲u_۳ &= -c. \end{aligned}$$

فرض کنید $w = e^{۲i\pi/۳}$ ریشه‌ی اولیه‌ای از واحد باشد. فرمول‌هایی برای ریشه‌های چندجمله‌ای $x^۳ + bx + c = ۰$ به صورت زیر می‌یابیم:

$$u_۱ = p + q, \quad u_۲ = wp + w^۲q, \quad u_۳ = w^۲p + wq \tag{۸}$$

که در آن p و q را باید تعیین کنیم. چون $۱ + w + w^۲ = ۰$ شرط $u_۱ + u_۲ + u_۳ = ۰$ برقرار است. دو شرط بعدی به صورت $pq = \frac{-b}{۳}$ و $p^۳ + q^۳ = -c$ در می‌دهند. دو معادله‌ی اخیر نتیجه می‌دهند که $p^۳$ و $q^۳$ هر دو در معادله‌ی درجه‌ی دوم $x^۲ + cx - \frac{b^۳}{۲۷} = ۰$ صدق می‌کنند. بنابراین

$$p = \sqrt[۳]{\frac{-c + \sqrt{c^۲ + \frac{۴b^۳}{۲۷}}}{۲}}, \quad q = \sqrt[۳]{\frac{-c - \sqrt{c^۲ + \frac{۴b^۳}{۲۷}}}{۲}}.$$

اگر ریشه‌های سوم را طوری اختیار کنیم که $pq = \frac{-b}{۳}$، آنگاه رابطه‌ی (۸) همه‌ی ریشه‌های $x^۳ + bx + c = ۰$ را به دست می‌دهد. این عبارت فرمول درجه‌ی سوم *نام* نام دارد و اسکینپون دل فِرو (۱۵۲۶–۱۶۴۵) اولین بار این فرمول‌ها را به دست آورد. عبارت

$\Delta = -۴b^۳ - ۲۷c^۲$ را دلتای $x^۳ + bx + c = ۰$ گوییم. بنابراین p و q به صورت $\sqrt[۳]{\frac{-c \pm \sqrt{\frac{-\Delta}{۲۷}}}{۲}}$ داده می‌شوند. این فرمول روی هر میدان K با مشخصه‌ی مخالف ۲ و ۳ معتبر است و ریشه‌های این چندجمله‌ای‌ها را می‌توان با الحاق ریشه‌های دوم و سوم عناصر K به K یافت. به طریق مشابه فرمولی برای ریشه‌های چندجمله‌ای درجه‌ی چهارم وجود دارد. این فرمول بر حسب ترکیب رادیکال‌ها و توابع گویا بر حسب ضرایب است. در فرن هفدهم میلادی بسیاری از جمله اویلر و لاگرانژ تلاش کردند که فرمولی برای ریشه‌های چندجمله‌ای‌های درجه‌ی پنج به دست بیاورند، که توفیقی نیافتند. آبل در سال ۴۲۸۱ نشان داد که چنین فرمولی برای چندجمله‌ای‌های معین درجه‌ی ۵ و بالاتر وجود ندارد. گالوا تعیین کرد که به ازای چه چندجمله‌ای‌هایی چنین فرمولی وجود دارد.

چندجمله‌ای درجه‌ی سوم $x^۳ + bx + c$ روی میدان K با مشخصه مخالف ۲ و ۳ را در نظر بگیرید. فرض کنید $u = \sqrt{c^۲ + \frac{۴b^۳}{۲۷}}$ و زنجیر میدان‌های

$$K \subseteq K(u) \subseteq K(u,p) \subseteq K(u,p,q) \subseteq K(u,p,q,w) = F$$

را در نظر بگیرید؛ در این صورت ریشه‌های چندجمله‌ای $x^۳ + ax + b$ در F قرار دارند. به علاوه $\pm u$ ریشه‌های چندجمله‌ای $x^۲ - u^۲$، $p = \sqrt[۳]{\frac{-c+u}{۲}}$ ریشه‌ی چندجمله‌ای $x^۳ - \left(\frac{-c+u}{۲}\right)$، $q = \sqrt[۳]{\frac{-c-u}{۲}}$ ریشه‌ی چندجمله‌ای $x^۳ - \left(\frac{-c-u}{۲}\right)$، و در نهایت w ریشه‌ی $x^۳ - ۱$ هستند. یعنی F شامل میدان تجزیه‌ی چندجمله‌ای $x^۳ + bx + c$ روی K است و F با الحاق متوالی ریشه‌های یک چندجمله‌ای به صورت $x^n - a$ حاصل‌ضرب شده به این مفهوم می‌گوییم چندجمله‌ای $x^۳ + bx + c$ با رادیکال‌ها حل‌پذیر است.

تعریف ۱.۹.۱۴. توسیع $F : K$ را توسیع رادیکالی گوییم هرگاه زنجیر متناهی

$$K = K_۰ \subseteq K_۱ \subseteq K_۲ \subseteq \cdots \subseteq K_m = F$$

از میدان‌های میانی وجود داشته باشد طوری که $K_j = K_{j-۱}(a_j)$، که در آن $a_j^{n_j} \in K_{j-۱}$، به ازای یک $n_j \in \mathbb{N}$، $(j = ۱, ۲, \ldots, m)$، یعنی a_j ریشه‌ای از چندجمله‌ای $x^{n_j} - k_{j-۱} \in K_{j-۱}[x]$ باشد. چندجمله‌ای $f(x) \in K[x]$، (یا معادله‌ی $f(x) = ۰$) را حل‌پذیر (با رادیکال‌ها) گوییم هرگاه توسیع تجزیه‌ی آن در یک توسیع رادیکالی از K قرار داشته باشد، یا به طور معادل همه‌ی ریشه‌های آن در یک توسیع رادیکالی K قرار داشته باشد.

چندجمله‌ای $f(x) \in K[x]$ حل‌پذیر است اگر و تنها اگر با استفاده از اعمال روی K و الحاق ریشه‌های nام بتوانیم ریشه‌های $f(x)$ را در یک میدان تجزیه بیابیم. به وضوح، با توجه به فرمول‌های یافته شده این اعمال همه‌ی ریشه‌های چندجمله‌ای‌های درجه‌ی دوم و سوم را به دست می‌دهند. بنابراین اگر $\operatorname{char} K \neq ۲, ۳$، همه‌ی چندجمله‌ای‌های درجه‌ی ۲ و ۳ حل‌پذیرند. می‌توان نشان داد که چندجمله‌ای‌های درجه‌ی ۴ نیز حل‌پذیرند (تمرین ۵ را ببینید). اما چندجمله‌ای‌های درجه‌ی ۵ وجود دارند که حل‌پذیر نیستند.

قضیه ۲.۹.۱۴. فرض کنید K یک میدان باشد و $\operatorname{char} K = ۰$. اگر $F : K$ توسیع نرمال و رادیکالی با زنجیر میدان‌های میانی

$$K = K_۰ \subseteq K_۱ \subseteq K_۲ \subseteq \cdots \subseteq K_m = F$$

باشد، طوری که $K_j = K_{j-۱}(a_j)$، که در آن $a_j^{n_j} \in K_{j-۱}$، به ازای یک $n_j \in \mathbb{N}$، $(j = ۱, ۲, \ldots, m)$. اگر به ازای هر j، $۱ \leq j \leq m$، $K_{j-۱}$ شامل همه‌ی ریشه‌های n_jام واحد باشد، آنگاه $\operatorname{Aut}_K F$ گروه حل‌پذیر است.

اثبات. فرض کنید $w_۱ = ۱$، $w_۲$، ...، w_{n_j} ریشه‌های n_jام واحد متمایز واحد در $K_{j-۱}$ باشند. در این صورت همه‌ی ریشه‌های متمایز چندجمله‌ای $x^{n_j} - k_{j-۱} \in K_{j-۱}[x]$ عبارتند از $a_j = a_j w_۱$، $a_j w_۲$، ...، $a_j w_{n_j}$. به وضوح همه‌ی این ریشه‌ها در $K_j = K_{j-۱}(a_j)$ قرار دارند. پس $K_j : K_{j-۱}$ توسیع تجزیه‌ی $x^{n_j} - k_{j-۱}$ روی $K_{j-۱}$ است. بنابراین بنا به قضیه‌ی ۱۶.۵.۱۴، $\operatorname{Aut}_{K_{j-۱}} K_j$ گروه آبلی است. قرار می‌دهیم $G_j = \operatorname{Aut}_{K_j} F$. توسیع $K_j : K_{j-۱}$ توسیع گالوا است. از طرف دیگر چون $F : K$ توسیع نرمال است، $F : K_j$ نیز توسیع نرمال است. پس بنا به قضیه‌ی اساسی نظریه‌ی گالوا $G_j = \operatorname{Aut}_{K_j} F$ زیرگروه نرمال $G_{j-۱} = \operatorname{Aut}_{K_{j-۱}} F$ است و

$$\frac{G_{j-۱}}{G_j} = \frac{\operatorname{Aut}_{K_{j-۱}} F}{\operatorname{Aut}_{K_j} F} \cong \operatorname{Aut}_{K_{j-۱}} K_j.$$

پس $\frac{G_{j-1}}{G_j}$، برای $j = ۱, ۲, \dots, m$، آبلی است. از این رو سری

$$G = G_۰ \supseteq G_۱ \supseteq \cdots \supseteq G_m = \{۱\}$$

یک سری آبلی برای $G = G_۰ = \operatorname{Aut}_K F$ است. بنابراین G یک گروه حل‌پذیر است. □

قضیه‌ی قبل در حالتی که همه‌ی ریشه‌های n_jام واحد در $K_{j-۱}$ باشند، نشان می‌دهد $\operatorname{Aut}_K F$ حل‌پذیر است. اکنون حالت کلی را ثابت می‌کنیم و آن وقتی است که ممکن است ریشه‌های n_jام واحد در $K_{j-۱}$ نباشند.

قضیه ۳.۹.۱۴. فرض کنید K یک میدان باشد و $\operatorname{char} K = ۰$. اگر $F : K$ توسیع نرمال و رادیکالی باشد، آنگاه $\operatorname{Aut}_K F$ گروه حل‌پذیر است.

اثبات. چون $F : K$ توسیع رادیکالی است، زنجیر متناهی

$$K = K_۰ \subseteq K_۱ \subseteq \cdots \subseteq K_m = F$$

از میدان‌های میانی وجود دارد که $K_j = K_{j-۱}(a_j)$، طوری که عدد $n_j \in \mathbb{N}$ وجود دارد ، $(j = ۱, ۲, \dots, m)$، که $a_j^{n_j} \in K_{j-۱}$. فرض کنید $n = n_۱ n_۲ \cdots n_m$، چون $\operatorname{char} K = ۰$، ریشه‌های اولیه‌ی nام واحد روی K وجود دارند. فرض کنید w یک ریشه‌ی اولیه‌ی nام واحد روی K باشد. قرار می‌دهیم $L_۰ = K$ و $L_j = K_j(w)$، $۱ \le j \le m$. چون $F : K$توسیع نرمال است، $F : K$ توسیع تجزیه‌ی یک چندجمله‌ای $f(x) \in K[x]$ است. بنابراین $L_m : K$ توسیع تجزیه‌ی چندجمله‌ای $(x^n - ۱)f(x)$ روی K است. بنابراین $L_m : K$ توسیع گالوا است (چون $\operatorname{char} K = ۰$). اکنون زنجیر متناهی

$$K = L_۰ \subseteq L_۱ \subseteq \cdots \subseteq L_m$$

را در نظر می‌گیریم. به ازای هر $۱ \le j \le m$ داریم

$$L_j = K_j(w) = K_{j-۱}(a_j, w) = L_{j-۱}(a_j)$$

و هم‌چنین $a_j^{n_j} \in K_{j-۱} \subseteq L_{j-۱}$. به علاوه $L_{j-۱}$ شامل یک ریشه‌ی n_jام اولیه‌ی واحد، یعنی w^{n/n_j}، است. بنابراین بنا به قضیه‌ی ۲.۹.۱۴، $\operatorname{Aut}_K L_m$ حل‌پذیر است.
از طرف دیگر چون $F : K$ توسیع نرمال است. بنا به قضیه‌ی اساسی نظریه‌ی گالوا $\operatorname{Aut}_F L_m$ زیرگروه نرمالی از $\operatorname{Aut}_K L_m$ است و

$$\operatorname{Aut}_K F \cong \operatorname{Aut}_K L_m / \operatorname{Aut}_F L_m.$$

چون $\operatorname{Aut}_K L_m$ حل‌پذیر است، پس $\operatorname{Aut}_K F$ نیز حل‌پذیر است. □

قضیه‌ی ۳.۹.۱۴، و مثال ۱۴.۵.۱۴، به سوال حل‌پذیری چندجمله‌ای‌های درجه‌ی ۵ جواب منفی می‌دهند. اما در مورد چندجمله‌ای‌های با درجه‌ی بالاتر چه می‌توان گفت. در واقع همان‌گونه که قبلاً ذکر شد آبل ثابت کرد که چندجمله‌ای‌های حل‌ناپذیر با هر درجه‌ی $n \ge ۵$ وجود دارند. برای به دست آوردن این مطلب به ازای هر $n > ۵$، چندجمله‌ای با درجه‌ی n می‌یابیم که گروه گالوای آن S_n است. چون S_n حل‌ناپذیر است بنا به قضیه‌ی ۳.۹.۱۴، این چندجمله‌ای نیز حل‌ناپذیر است. خودریختی در $\operatorname{Aut}_K F$ یک جایگشت روی ریشه‌های $f(x)$ است. به علاوه ضرایب $f(x)$ توابعی بر حسب ریشه‌ها هستند ، که با تعویض شدن ریشه‌ها بدون تغییر باقی می‌مانند. مثلاً اگر $a_۱$، $a_۲$ و $a_۳$ ریشه‌های $f(x)$ باشند، آنگاه

$$\begin{aligned} f(x) &= (x - a_۱)(x - a_۲)(x - a_۳) \\ &= x^۳ + (a_۱ + a_۲ + a_۳)x^۲ + (a_۱a_۲ + a_۱a_۳ + a_۲a_۳)x - a_۱a_۲a_۳ \end{aligned} \tag{۹}$$

این ایده را فرمول‌بندی می‌کنیم. فرض کنید F میدان باشد و حلقه‌ی چندجمله‌ای‌های n متغیره $K[x_۱, \dots, x_n]$ را در نظر بگیرید. چندجمله‌ای $f(x_۱, \dots, x_n) \in K[x_۱, \dots, x_n]$

را چندجمله‌ای متقارن گوییم هرگاه به ازای $\sigma \in S_n$،

$$f(x_{\sigma(1)}, \ldots, x_{\sigma(n)}) = f(x_1, \ldots, x_n).$$

به عنوان مثال چندجمله‌ای‌های $x_1^2 x_2^2 x_3^2$، $x_1 x_2 x_3^2 + x_1 x_2^2 x_3 + x_1^2 x_2 x_3$ همگی در $K[x_1, x_2, x_3]$ متقارن هستند. ضرایب چندجمله‌ای (۹) نیز چندجمله‌ای‌های متقارن بر حسب a_1، a_2 و a_3 هستند. چندجمله‌ای‌های مقدماتی متقارن در $K[x_1, \ldots, x_n]$ را به صورت زیر تعریف می‌کنیم

$$\begin{aligned} f_0 &= f_0(x_1, \ldots, x_n) = 1 \\ f_k &= f_k(x_1, \ldots, x_n) = \sum_{i_1 < i_2 < \cdots < i_k} x_{i_1} x_{i_2} \cdots x_{i_k}, \quad k = 1, 2, \ldots, n. \end{aligned}$$

بنابراین مثلاً وقتی $n = 3$ داریم

$$\begin{aligned} f_0 &= f_0(x_1, x_2, x_3) = 1 \\ f_1 &= f_1(x_1, x_2, x_3) = x_1 + x_2 + x_3 \\ f_2 &= f_2(x_1, x_2, x_3) = x_1 x_2 + x_1 x_3 + x_2 x_3 \\ f_3 &= f_3(x_1, x_2, x_3) = x_1 x_2 x_3. \end{aligned}$$

توجه کنید اگر $u_j = f_j(a_1, a_2, \ldots, a_n)$، که در آن a_1، ...، a_n ریشه‌های چندجمله‌ای $f(x)$ هستند ، آن‌گاه

$$\begin{aligned} f(x) &= (x - a_1)(x - a_2) \cdots (x - a_n) \\ &= x^n - u_1 x^{n-1} + u_2 x^{n-2} + \cdots + (-1)^{n-1} u_{n-1} x + (-1)^n u_n. \end{aligned}$$

میدان کسرهای حلقه‌ی چندجمله‌ای‌های n متغیره $K[x_1, \ldots, x_n]$، را در نظر بگیرید:

$$\begin{aligned} K(x_1, \ldots, x_n) = \{ & f(x_1, \ldots, x_n)/g(x_1, \ldots, x_n) \mid \\ & f(x_1, \ldots, x_n),\ g(x_1, \ldots, x_n) \in K[x_1, \ldots, x_n],\ g \neq 0\}. \end{aligned}$$

هر عضو $K(x_1, \ldots, x_n)$ را یک تابع گویا می‌نامیم. فرض کنید $\sigma \in S_n$ جایگشت دلخواهی باشد. نگاشتی که آن را با $\bar{\sigma}$ نشان می‌دهیم از $K(x_1, \ldots, x_n)$ به خودش تعریف می‌کنیم، به ازای هر تابع گویای $r(x_1, \ldots, x_n) \in K(x_1, \ldots, x_n)$ تعریف می‌کنیم

$$\bar{\sigma}(r(x_1, \ldots, x_n)) = r(x_{\sigma(1)}, \ldots, x_{\sigma(n)}).$$

به سادگی می‌توان دید که $\bar{\sigma} : K(x_1, \ldots, x_n) \longrightarrow K(x_1, \ldots, x_n)$
یک خودریختی است که هر عضو K را ثابت نگه می‌دارد (چرا؟)، پس $\bar{\sigma} \in \mathrm{Aut}_K K(x_1, \ldots, x_n)$.
به علاوه نگاشت $\sigma \longrightarrow \bar{\sigma}$ یک همریختی یک‌به‌یک از S_n به $\mathrm{Aut}_K K(x_1, \ldots, x_n)$ است. فرض کنید $\bar{S}_n = \{\bar{\sigma} \mid \sigma \in S_n\}$، تصویر S_n تحت همریختی یک‌به‌یک $\bar{\sigma}$ باشد. پس $S_n \cong \bar{S}_n \leq \mathrm{Aut}_K K(x_1, \ldots, x_n)$.
میدان ثابت $\bar{S}_n$ در $K(x_1, \ldots, x_n)$ عبارت است از

$$\begin{aligned} L = \{ & r(x_1, \ldots, x_n) \in K[x_1, \ldots, x_n] \mid \\ & r(x_1, \ldots x_n) = r(x_{\sigma(1)}, \ldots, x_{\sigma(n)}),\quad \forall \sigma \in S_n\}. \end{aligned}$$

عناصر L را توابع گویای متقارن روی K می‌نامیم.

قضیه ۴.۹.۱۴. فرض کنید K یک میدان با میدان توابع گویای $K(x_1,\dots,x_n)$ باشد. اگر $L \subseteq K(x_1,\dots,x_n)$ زیرمیدان همه‌ی توابع گویای متقارن روی K باشد، آنگاه
(الف) $K(x_1,\dots,x_n) : L$ توسیع گالوا است و $[K(x_1,\dots,x_n) : L] = n!$ و $\mathrm{Aut}_L K(x_1,\dots,x_n) \cong S_n$.
(ب) $L = K(f_0, f_1, \dots, f_n)$، که آن در f_iها چندجمله‌ای‌های مقدماتی متقارن در $K[x_1,\dots,x_n]$ هستند و هم‌چنین $K(x_1,\dots,x_n) : L$ توسیع تجزیه‌ی چندجمله‌ای $f(t) = t^n - f_1 t^{n-1} + \cdots + (-1)^n f_n \in L[t]$ است.

اثبات. از نمادهای قبل از قضیه استفاده می‌کنیم. چون $\bar{S}_n$ زیرگروه متناهی از گروه خودریختی‌های $K(x_1,\dots,x_n)$ است، طبق قضیه‌ی ۳.۸.۱۴،

$$[K(x_1,\dots,x_n) : L] = |\ \bar{S}_n\ | = n!.$$

چون f_0، f_1، ...، f_n چندجمله‌ای‌های مقدماتی متقارن در $K[x_1,\dots,x_n]$ هستند ، داریم

$$K(f_0, f_1, \dots, f_n) \subseteq L \subseteq K(x_1,\dots,x_n).$$

چندجمله‌ای $f(t)$ در $K(f_0, f_1, \dots, f_n)[t]$ را با

$$\begin{aligned} f(t) &= (t-x_1)(t-x_2)\cdots(t-x_n) \\ &= t^n - f_1 t^{n-1} + \cdots + (-1)^n f_n \end{aligned}$$

در نظر می‌گیریم. آنگاه $K(x_1,\dots,x_n) : K(f_0, f_1, \dots, f_n)$ توسیع تجزیه‌ی $f(t)$ است و چون $\deg f(t) = n$، بنا به قضیه‌ی ۱.۲.۱۴، داریم

$$[K(x_1,\dots,x_n) : K(f_0, f_1, \dots, f_n)] \leq n!.$$

بنا به قانون برج داریم

$$\begin{aligned} n! &\geq [K(x_1,\dots,x_n) : K(f_0,\dots,f_n)] \\ &= [K(x_1,\dots,x_n) : L][L : K(f_0, f, \dots, f_n)] = (n!)[L : K(f_0,\dots,f_n)]. \end{aligned}$$

بنابراین $[L : K(f_0,\dots,f_n)] = 1$ یا $L = K(f_0, f_1, \dots, f_n)$. اکنون چون چندجمله‌ای $f(t)$ روی $L = K(f_0, f_1, \dots, f_n)$ جداپذیر است، $K(x_1,\dots,x_n) : L$ توسیع گالوا است (بنا به قضیه‌ی ۴.۷.۱۴). بنابراین

$$|\mathrm{Aut}_L K(x_1,\dots,x_n)| = [K(x_1,\dots,x_n) : L] = n!.$$

چون مرتبه‌ی $\bar{S}_n$ نیز $n!$ است و $\bar{S}_n \leq \mathrm{Aut}_L K(x_1,\dots,x_n)$، داریم

$$S_n \cong \bar{S}_n = \mathrm{Aut}_L K(x_1,\dots,x_n). \qquad \square$$

نتیجه ۵.۹.۱۴. به ازای هر $n \geq 5$ چندجمله‌ای حل‌ناپذیر با درجه‌ی n وجود دارد.

اثبات. چندجمله $f(t) \in L[t]$ در قضیه‌ی ۴.۹.۱۴، حل‌ناپذیر است، زیرا گروه گالوای آن با S_n، $n \geq 5$، یکریخت است و S_n حل‌پذیر نیست. $\square$

تمرین‌ها

۱. گروه گالوای چندجمله‌ای $x^3 - 3x + 1$ روی $\mathbb{Q}$ را بیابید. معادله‌ی $x^3 - 3x + 1 = 0$ را با استفاده از رادیکال‌ها حل کنید.

۲. نشان دهید گروه گالوای چندجمله‌ای

$$f(x) = x^5 - 10x^4 + 2x^3 - 24x^2 + 2$$

روی $\mathbb{Q}$ برابر S_5 است. آیا معادله‌ی $f(x) = 0$ با رادیکال‌ها حل‌پذیر است؟

۳. توسیع رادیکالی $\mathbb{Q}$ را که شامل
(الف) $\sqrt{۳}(\sqrt[۳]{۵}-\sqrt[۵]{۷})$ (ب) $(\sqrt{۵}-۳)(۴-۳\sqrt[۵]{۶})$
است را بیابید.

۴. در هر حالت نشان دهید $f(x)\in\mathbb{Q}[x]$ با رادیکال‌ها حل‌پذیر نیست.
(الف) $f(x)=x^۵-۴x-۲$ (ب) $f(x)=x^۵-۶x^۲+۲$

۵. نشان دهید هر چندجمله‌ای درجه‌ی ۴ روی $\mathbb{Q}$ حل‌پذیر است.

۶. نشان دهید به ازای هر گروه متناهی G میدانی مثل K و چندجمله‌ای $f(x)\in K[x]$ وجود دارند طوری که گروه گالوای $f(x)$ روی K با G یکریخت است.

۱۰.۱۴ ساخت‌پذیری هندسی

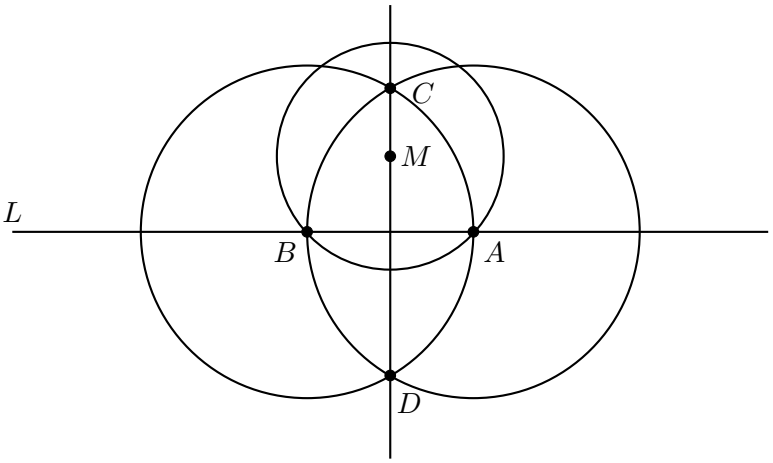
یونانیان قدیم در هندسه متبحر بودند. اما برخلاف هندسه تحلیلی جدید که زیربنای اصلی آن سیستم مختصات است، یونانیان ترجیح می‌دادند که از روش‌های ترکیبی نظیر رسم عمود بر یک خط از یک نقطه، برخورد خطوط و منحنی‌ها و ... استفاده کنند. به ویژه آنها علاقه داشتند که هندسه را فقط با استفاده از خطکش و پرگار انجام دهند. بنابراین آن ها فقط می‌خواستند برای ساختن هندسه از این روش استفاده کنند که: خطوط را با استفاده از دو نقطه‌ی داده شده رسم کنید، دایره‌هایی با مرکز و شعاع داده شده رسم کنند، و نقاط برخورد چنین خطوط و دایره‌هایی را بیابند. در این‌جا منظور از خطکش چوب لبه صاف و بدون نشان گذاری است. یونانیان قدیم نتوانستند به سوالات زیر پاسخ دهند:

(الف) تثلیث زاویه: آیا یک زاویه را می‌توان فقط با استفاده از خطکش و پرگار به سه قسمت مساوی تقسیم کرد؟

(ب) تضعیف مکعب: آیا یک مکعب را می‌توان فقط با استفاده از خطکش و پرگار دو برابر کرد؟ (یعنی مکعبی ساخت که حجم آن دو برابر حجم مکعب داده شده باشد؟)

این سوالات تا قرن ۱۹ میلادی و تا هنگامی که روش‌های جبری به‌کار گرفته شد، لاینحل باقی‌مانده بودند. جواب هر دو سوال منفی است. تا این قرن صدها نفر ادعا کرده‌اند که یکی از این دو مساله را حل کرده‌اند و برخی حتی به چاپ "حل‌های؟" خود اقدام کردند.
صفحه اقلیدسی را با $\mathbb{R}\times\mathbb{R}$ یکی در نظر می‌گیریم. فرض کنید یک واحد طول داریم و نقاط $(۰,۰)$ و $(۱,۰)$ را به ترتیب با O و X نشان گذاری کرده‌ایم. با استفاده از خطکش و پرگار سه عمل زیر را می‌توانیم در صفحه اقلیدسی انجام دیدیم:
(الف) خط گذرنده از دو نقطه‌ی داده شده را رسم کنیم.
(ب) دایره‌هایی به مرکز و شعاع داده شده را رسم کنیم.
(ج) نقاط محل برخورد منحنی‌های (الف) و (ب) را رسم کنیم.
با استفاده از سه عمل فوق می‌توانیم:
(د) خط موازی خط داده شده و گذرنده از نقطه‌ی داده شده را رسم کنیم.
(هـ) خط عمود بر یک خط داده شده و گذرنده از نقطه‌ی داده شده را رسم کنیم.

مثلاً برای (هـ) را s پرگار را روی نقطه‌ی M مورد قرار داده و توک پرگار را روی نقطه‌ی دلخواهی از خط داده شده L قرار می‌دهیم. دایره‌ی رسم شده، خط را در دو نقطه‌ی A و B قطع می‌کند. اکنون دو دایره به مرکزهای A ، B و شعاع‌های یکسان $|AB|$ رسم می‌کنیم. این دو دایره یک‌دیگر را در نقطه‌های C و D قطع می‌کنند. خط CD، خطی است که از نقطه‌ی M می‌گذرد و بر L عمود است (شکل ۲.۱۴ را ببینید).
خط گذرنده از O و X را رسم می‌کنیم و آن را محور xها می‌نامیم. اکنون خطی عمود بر محور xها و گذرنده از O رسم می‌کنیم و آن‌را محور yها می‌نامیم. بنابراین می‌توانیم به نقاط در صفحه، مختصات نظیر کنیم. از این رو محور xها، محور yها و مبداء $O=(۰,۰)$ و نقطه‌ی $X=(۱,۰)$ را داریم. عدد حقیقی a را ساخت‌پذیر گوییم هرگاه پاره‌خطی به طول $|a|$ را بتوانیم با استفاده از واحد طول در تعداد متناهی مرحله با استفاده از خطکش و پرگار بسازیم. طبق تعریف، a ساخت‌پذیر است اگر و تنها اگر $-a$ ساخت‌پذیر باشد. در واقع می‌خواهیم ثابت کنیم مجموعه اعداد حقیقی ساخت‌پذیر یک زیرمیدان $\mathbb{R}$ است. ابتدا ثابت می‌کنیم:



شکل ۲.۱۴: رسم عمود بر یک خط گذرنده از نقطه‌ای خارج از آن

لم ۱.۱۰.۱۴. اگر $a \geq ۰$ و $b \geq ۰$ اعداد حقیقی ساخت‌پذیر باشند، آنگاه $a+b$، $a-b$، (اگر $a > b$)، ab، $\frac{b}{a}$ (اگر $a \neq ۰$) و $\sqrt{a}$ ساخت‌پذیر هستند.

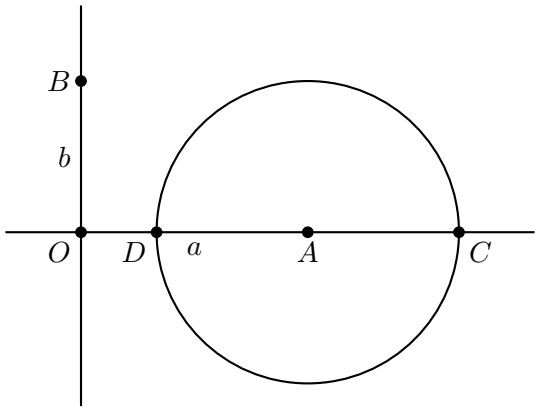
اثبات. فرض کنید OA و OB به ترتیب پاره‌خط‌ها به طول $|a|$ و $|b|$ باشند. با استفاده از پرگار یک دایره به مرکز A و شعاع $|OB|$ رسم می‌کنیم. دایره‌ی حاصل، خط گذرنده از OA را در نقطه‌های C و D قطع می‌کند. در این صورت

$$|OC| = |OA| + |OB| = a + b$$

و $a+b$ ساخت‌پذیر است. هم‌چنین چون

$$|OD| = |OA| - |AD| = a - b,$$

$a-b$ ساخت‌پذیر است (شکل ۳.۱۴ را ببینید).

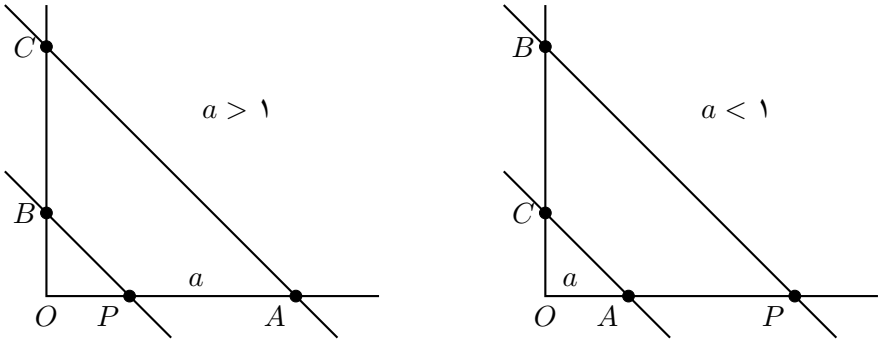


شکل ۳.۱۴: $a+b$ و $a-b$ ساخت‌پذیرند.

اکنون ثابت می‌کنیم ab ساخت‌پذیر است. اگر $a = ۱$ چیزی برای اثبات نیست، پس فرض کنید $a \neq ۱$. فرض کنید OP پاره‌خطی به طول ۱ باشد. ابتدا خط واصل P و B را رسم می‌کنیم. سپس از A خطی به موازات خط BP رسم می‌کنیم. دو مثلث ΔOBP و ΔOCA متشابهند. بنابراین

$$\frac{|OB|}{|OC|} = \frac{|OP|}{|OA|} \quad \text{یا} \quad \frac{b}{|OC|} = \frac{۱}{a},$$

و $|OC| = ab$ ساخت‌پذیر است (شکل ۴.۱۴ را ببینید).

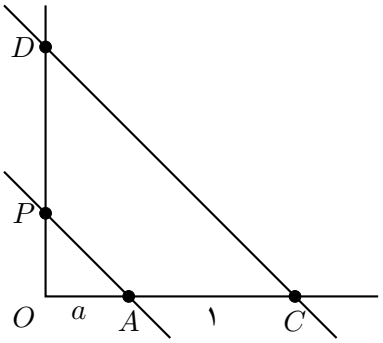


شکل ۴.۱۴: ab ساخت‌پذیر است.

اکنون اگر $a \neq ۰$ نشان می‌دهیم $a^{-۱}$ ساخت‌پذیر است. فرض کنید OP و AC پاره‌خط‌هایی به طول ۱ هستند. خطی از A به P رسم می‌کنیم. سپس خط گذرنده از C موازی خط AP را رسم می‌کنیم. مثلث‌های ΔOAP و ΔODC متشابه‌اند، پس

$$\frac{|OP|}{|OD|} = \frac{|OA|}{|AC|} \quad \text{یا} \quad \frac{۱}{|OD|} = \frac{a}{۱}$$

بنابراین $|OD| = a^{-۱}$ ساخت‌پذیر است (شکل ۵.۱۴ را ببینید). پس اگر a و b ساخت‌پذیر باشند و $a \neq ۰$، آنگاه $ba^{-۱} = \frac{b}{a}$



شکل ۵.۱۴: $\frac{۱}{a}$ ساخت‌پذیر است.

ساخت‌پذیر است.

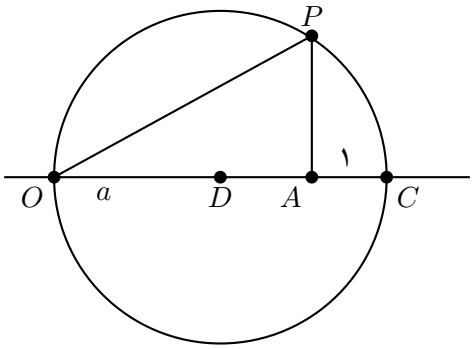
در نهایت ثابت می‌کنیم $\sqrt{a}$ ساخت‌پذیر است. فرض کنید AC پاره‌خطی به طول ۱ و OD پاره‌خطی به طول $\frac{|OC|}{۲}$ باشد. ابتدا دایره‌هایی به مرکز D و شعاع OD رسم می‌کنیم. سپس از A خطی عمود بر خط OC رسم می‌کنیم تا دایره را در نقطه‌ی P قطع کند. در این صورت مثلث‌های ΔAPC و ΔOAP متشابه‌اند. بنابراین

$$\frac{|AP|}{|AO|} = \frac{|AC|}{|AP|} \Longrightarrow \frac{|AP|}{a} = \frac{۱}{|AP|} \Longrightarrow (AP)^{۲} = a,$$

و $\sqrt{a} = |AP|$ ساخت‌پذیر است (شکل ۶.۱۴ را ببینید).

قضیه ۲.۱۰.۱۴. مجموعه همه‌ی اعداد حقیقی ساخت‌پذیر یک زیرمیدان $\mathbb{R}$ است.

اثبات. فرض کنید K مجموعه همه‌ی اعداد حقیقی ساخت‌پذیر باشد. چون ۱ و ۰، ساخت‌پذیرند $۱, ۰ \in K$. فرض کنید $a, b \in K$. چند حالت وجود دارد. اگر $a > ۰$ و $b > ۰$، طبق لم ۱.۱۰.۱۴، $a + b \in K$. اگر $a > ۰$ و $b < ۰$، آنگاه $a > ۰$ و $-b > ۰$. در این‌جا دو وضعیت پیش می‌آید یا $a > -b$ یا $a < -b$. اگر $a > -b$، با توجه به لم ۱.۱۰.۱۴، $a + b = a - (-b)$ ساخت‌پذیر است. اگر $a < -b$، آنگاه مجدداً طبق لم ۱.۱۰.۱۴، $-b - a = -(a + b)$ ساخت‌پذیر است. از این‌رو $a + b$ ساخت‌پذیر است. حالت های دیگر به طریق مشابه انجام می‌شود.



شکل ۶.۱۴: $\sqrt{a}$ ساخت‌پذیر است.

حال ثابت می‌کنیم $\frac{b}{a}$ ساخت‌پذیر است. اگر $a, b > ۰$ طبق لم ۱.۱۰.۱۴، حکم ثابت است، اگر مثلاً $a > ۰$ و $b < ۰$، آن‌گاه $a > ۰$ و $-b > ۰$. بنابراین طبق لم ۱.۱۰.۱۴، $\frac{-b}{a}$ ساخت‌پذیر است. پس $\frac{b}{a}$ ساخت‌پذیر است. □

فرض کنید K میدان اعداد حقیقی ساخت‌پذیر باشد. چون هر عدد گویا ساخت‌پذیر است، $\mathbb{Q} \subseteq K$. فرض کنید F یک زیرمیدان $\mathbb{R}$ باشد، مجموعه‌ی

$$P(F) = \{(x, y) \mid x, y \in F\}$$

را صفحه‌ی F می‌نامیم. فرض کنید $p_۱ = (x_۱, y_۱)$، $p_۲ = (x_۲, y_۲)$ دو نقطه در $P(F)$ باشند، یعنی $p_۱, p_۲ \in P(F)$، و L خط گذرنده از $p_۱$ و $p_۲$ باشد. اگر $x_۱ = x_۲$، آن‌گاه معادله‌ی L عبارت است از $x = x_۱$. اگر $x_۱ \neq x_۲$ معادله‌ی L عبارت است از

$$y - y_۱ = \frac{y_۲ - y_۱}{x_۲ - x_۱}(x - x_۱),$$

که می‌توان آن را به صورت $ax + by + c = ۰$، که در آن $a, b, c \in F$ نوشت. بنابراین معادله‌ی یک خط که دو نقطه‌ی آن در $P(F)$ قرار دارند به صورت

$$ax + by + c = ۰$$

است که در آن $a, b, c \in F$. چنین خطی را یک F- خط می‌نامیم. فرض کنید C یک دایره به مرکز $p_۱$ و گذرنده از $p_۲$ باشد. در این صورت معادله‌ی C عبارت است از

$$(x - x_۱)^۲ + (y - y_۱)^۲ = r^۲,$$

که در آن $r \in F$، شعاع C است. این معادله را می‌توان به صورت $x^۲ + y^۲ + ax + by + c = ۰$ نوشت، که در آن $a, b, c \in F$. بنابراین معادله‌ی یک دایره که مرکز آن و نقطه‌ای روی آن در $P(F)$ است، به صورت

$$x^۲ + y^۲ + ax + by + c = ۰$$

نوشته می‌شود، که در آن $a, b, c \in F$. چنین دایره‌هایی را یک F- دایره گوییم. اگر $x_۱, y_۱ \in F$، نقطه‌ی $p = (x_۱, y_۱)$ را یک F-نقطه گوییم. نقطه‌ی برخورد دو F- خط یک F- نقطه است. در واقع فرض کنید $a_۱x + b_۱y + c_۱ = ۰$ و $a_۲x + b_۲y + c_۲ = ۰$ دو F- خط باشند و یکدیگر را قطع می‌کنند. پس دترمینان دستگاه

$$\begin{cases} a_۱x + b_۱y = -c_۱ \\ a_۲x + b_۲y = -c_۲ \end{cases}$$

ناصفر است و

$$x = \frac{\begin{vmatrix} -c_۱ & b_۱ \\ -c_۲ & b_۲ \end{vmatrix}}{\begin{vmatrix} a_۱ & b_۱ \\ a_۲ & b_۲ \end{vmatrix}} = \frac{-c_۱b_۲ + c_۲b_۱}{a_۱b_۲ - a_۲b_۱} \in F,$$

$$y = \frac{\begin{vmatrix} a_۱ & -c_۱ \\ a_۲ & -c_۲ \end{vmatrix}}{\begin{vmatrix} a_۱ & b_۱ \\ a_۲ & b_۲ \end{vmatrix}} = \frac{-a_۱c_۲ + a_۲c_۱}{a_۱b_۲ - a_۲b_۱} \in F.$$

بنابراین نقطه‌ی برخورد دو F- خط یک F نقطه است.
نقطه‌ی برخورد یک F- خط و یک F- دایره لزوماً یک F- نقطه نیست. فرض کنید L یک F- خط و C یک F- دایره با معادله‌های

$$a_۱x + b_۱y + c_۱ = ۰ \qquad (۱۰)$$

و

$$x^۲ + y^۲ + a_۲x + b_۲y + c_۲ = ۰$$

باشند، که در آن $a_۱, a_۲, b_۱, b_۲, c_۱, c_۲ \in F$. با حذف y از دو معادله‌ی فوق به دست می‌آوریم

$$ax^۲ + bx + c = ۰,$$

که در آن $a, b, c \in F$. این معادله جواب حقیقی دارد ، پس $r = b^۲ - ۴ac \geq ۰$. بنابراین $r \in F$ و ریشه‌های معادله در $F(\sqrt{r})$ هستند. بنابراین $x \in F(\sqrt{r})$. از معادله‌ی (۱۰) نیز داریم $y \in F(\sqrt{r})$. پس (x, y) یک $F(\sqrt{r})$- نقطه است. با توجه به این که $x^۲ - r$ روی $F[x]$ تحویل‌ناپذیر باشد یا نه داریم :

$$[F(\sqrt{r}) : F] = ۲ \text{ یا } ۱.$$

حال فرض کنید $C_۱$ و $C_۲$ دو F- دایره با معادله‌های

$$x^۲ + y^۲ + a_۱x + b_۱y + c_۱ = ۰$$
$$x^۲ + y^۲ + a_۲x + b_۲y + c_۲ = ۰$$

باشند، که در آن $a_۱, a_۲, b_۱, b_۲, c_۱, c_۲ \in F$. با کم کردن معادله‌ی دوم از معادله‌ی اول داریم

$$(a_۱ - a_۲)x + (b_۱ - b_۲)y + (c_۱ - c_۲) = ۰.$$

پس نقاط برخورد $C_۱$ و $C_۲$ همان نقاط برخورد خط اخیر و هر یک از دایره‌های $C_۱$ و $C_۲$ است. بنابراین طبق بحث بالا این محل برخورد در $F(\sqrt{r})$ قرار دارد که در آن $r \in F$ و

$$[F(\sqrt{r}) : F] = ۲ \text{ یا } ۱.$$

توجه کنید اگر هر نقطه‌ی F ساخت‌پذیر باشد بنا به لم ۱.۱۰.۱۴، $\sqrt{r}$ ساخت‌پذیر است.

قضیه ۳.۱۰.۱۴. اگر a عدد حقیقی ساخت‌پذیر باشد، آن‌گاه عدد $k \geq ۰$ وجود دارد که $[\mathbb{Q}(a) : \mathbb{Q}] = ۲^k$. به ویژه درجه‌ی چندجمله‌ای می‌نیمال a روی $\mathbb{Q}$ برابر ۲^k است.

اثبات. فرض کنید K زیرمیدان اعداد حقیقی ساخت‌پذیر باشد. چون a ساخت‌پذیر است، $|a|$ فاصله‌ی بین دو $\mathbb{Q}$- نقطه‌ی A و B است و این نقاط را با استفاده از تعداد متناهی ساختن با خطکش و پرگار با شروع از $\mathbb{Q}$- نقطه می‌توان به دست آورد. چون هر عدد گویا ساخت‌پذیر است. $\mathbb{Q} \subseteq K$. فرض کنید با شروع از $\mathbb{Q}$- نقطه‌ها ، $m-1$ مرحله استفاده از خطکش و پرگار نیاز داریم تا نقاط A و B ساخته شوند. در اولین مرحله یکی از این سه کار انجام می‌شود یا نقطه‌ی برخورد دو $\mathbb{Q}$- خط یا نقطه‌ی برخورد یک $\mathbb{Q}$- دایره و یک $\mathbb{Q}$- خط و یا نقطه‌ی برخورد دو $\mathbb{Q}$- دایره به دست می‌آید. در هر حالت بنا به بحث قبل از قضیه، میدان F_1 وجود دارد که $\mathbb{Q} \subseteq F_1 \subseteq K$ و

$$[F_1 : \mathbb{Q}] = 1 \text{ یا } 2.$$

بنابراین با استفاده از $\mathbb{Q}$- نقطه‌ها میدان F_1 به صورت فوق حاصل می‌شود. به همین نحو در مرحله دوم با استفاده از F_1- نقطه‌ها میدان F_2 حاصل‌ضرب می‌شود که $\mathbb{Q} \subseteq F_1 \subseteq F_2 \subseteq K$ و

$$[F_2 : F_1] = 1 \text{ یا } 2.$$

با ادامه‌ی این روند میدان‌های $\mathbb{Q} = F_0 \subseteq F_1 \subseteq F_2 \subseteq \cdots \subseteq K$ به دست می‌آیند. چون $m-1$ مرحله برای ساخت A و B لازم است، A و B، F_{m-1}- نقطه هستند. چون a فاصله‌ی بین A و B است فرمول فاصله‌ی دو نقطه نشان می‌دهد $a \in F_{m-1}(\sqrt{b})$، که در آن $b \in F_{m-1}$ و $b > 0$. قرار می‌دهیم $F_m = F_{m-1}(\sqrt{b})$. پس

$$[F_m : F_{m-1}] = 1 \text{ یا } 2.$$

بنابراین زنجیر متناهی از میدان‌های

$$\mathbb{Q} = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_{m-1} \subseteq F_m$$

را داریم که در آن $a \in F_m$ و

$$[F_k : F_{k-1}] = 1 \text{ یا } 2, \quad \forall k, \quad 1 \leq k \leq m.$$

بنا به قانون برج داریم

$$[F_m : \mathbb{Q}] = [F_m : F_{m-1}] \cdots [F_2 : F_1][F_1 : F_0].$$

بنابراین $[F_m : \mathbb{Q}]$ توانی از ۲ است. چون $a \in F_m$ نتیجه می دهد $\mathbb{Q}(a) \subseteq F_m$، مجدداً از قانون برج $[\mathbb{Q}(a) : \mathbb{Q}]$ توانی از ۲ است. چون $[\mathbb{Q}(a) : \mathbb{Q}]$ درجه‌ی چندجمله‌ای می‌نیمال a روی $\mathbb{Q}$ است، حکم بعدی ثابت می‌شود. □

از قضیه‌ی ۱.۱۰.۱۴، نتیجه می‌شود هر عدد حقیقی ساخت‌پذیر روی $\mathbb{Q}$ جبری است. به علاوه نحوه‌ی اثبات قضیه‌ی ۳.۱۰.۱۴، توصیف کاملی از اعداد حقیقی ساخت‌پذیر را ارائه می‌کند:یک عدد حقیقی a ساخت‌پذیر است اگر و تنها اگر زنجیر

$$\mathbb{Q} = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_m$$

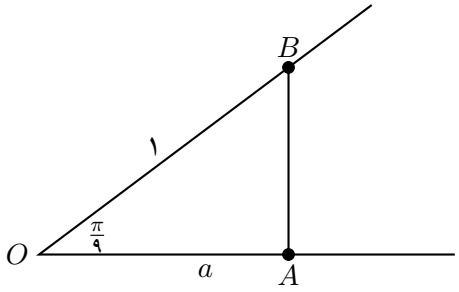
از زیرمیدان‌های $\mathbb{R}$ وجود داشته باشد طوری که $a \in F_m$ و $[F_j : F_{j-1}] = 1$ یا ۲، به ازای هر j، $1 \leq j \leq m$ (تمرین ۳ را ببینید).

نتیجه ۴.۱۰.۱۴. با استفاده از از خطکش و پرگار دو برابر کردن یک مکعب به طول ۱ امکان‌پذیر نیست.

اثبات. اگر چنین نباشد، آنگاه یک مکعب با حجم ۲ را می‌توان ساخت. یک طول این مکعب برابر $\sqrt[3]{2}$ است، که نتیجه می‌دهد $\sqrt[3]{2}$ ساخت‌پذیر است. اما $x^3 - 2$ روی $\mathbb{Q}$ (بنا به محک آیزنشتاین) تحویل‌ناپذیر است. بنابراین $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ و بنا به قضیه‌ی ۱.۱۰.۱۴، $\sqrt[3]{2}$ ساخت‌پذیر نیست، که تناقض است. □

نتیجه ۵.۱۰.۱۴. تقسیم $\frac{\pi}{3}$ با استفاده از خطکش و پرگار به سه قسمت مساوی امکان ندارد.

اثبات. فرض کنید $a = \cos\frac{\pi}{9}$. فرض کنید بتوان $\frac{\pi}{3}$ را به سه قسمت مساوی تقسیم کرد. در این صورت a ساخت‌پذیر است. زیرا از یک خط زاویه‌ی $\frac{\pi}{3}$، یک واحد جدا می‌کنیم و از آن نقطه یک عمود بر خط دیگر زاویه رسم می‌کنیم (شکل ۷.۱۴ را ببینید).



شکل ۷.۱۴: زاویه‌ی $\frac{\pi}{۹}$ ساخت‌پذیر نیست.

در این صورت یک مثلث قائم‌الزاویه‌ی OAB به دست می‌آید. پس

$$\cos\frac{\pi}{۹} = \frac{a}{۱} = a$$

ساخت‌پذیر است. می‌دانیم به ازای هر θ

$$\cos ۳\theta = ۴\cos^۳\theta - ۳\cos\theta.$$

بنابراین اگر قرار دهیم $\theta = \frac{\pi}{۹}$، به دست می‌آوریم $\frac{۱}{۲} = ۴a^۳ - ۳a$. از این‌رو a ریشه‌ی $p(x) = ۸x^۳ - ۶x - ۱$ است. $p(x)$ روی $\mathbb{Q}$ هیچ ریشه‌ای ندارد و چون $\deg p(x) = ۳$، $p(x)$ روی $\mathbb{Q}$ تحویل‌ناپذیر است و $[\mathbb{Q}(a) : \mathbb{Q}] = ۳$، که این متناقض با قضیه‌ی ۱.۱۰.۱۴، است. □

تمرین‌ها

۱. آیا زاویه‌ی $\frac{\pi}{۴}$ را می‌توان فقط با استفاده از خطکش و پرگار به سه قسمت مساوی تقسیم کرد.

۲. نشان دهید زاویه‌ی °۴۰ را نمی‌توان با استفاده از خطکش و پرگار ساخت.

۳. نشان دهید عدد حقیقی a ساخت‌پذیر است اگر و تنها اگر زنجیر

$$\mathbb{Q} = F_۰ \subseteq F_۱ \subseteq \cdots \subseteq F_m$$

از زیرمیدان‌های $\mathbb{R}$ وجود داشته باشد که $a \in F_m$ و $[F_j : F_{j-۱}] = ۱$ یا ۲، به ازای هر j.

۴. (الف) نشان دهید $\sin\theta$ ساخت‌پذیر است اگر و تنها اگر $\cos\theta$ ساخت‌پذیر باشد.
(ب) نشان دهید $\cos ۲\theta$ ساخت‌پذیر است اگر و تنها اگر $\cos\theta$ ساخت‌پذیر باشد.

۵. آیا می‌توان کره را به مکعب تبدیل کرد؟ یعنی آیا می‌توان مکعبی ساخت که حجم آن برابر حجم کره داده شده باشد؟

۶. آیا یک مکعب را می‌توان سه برابر کرد؟ یعنی آیا می‌توان مکعبی ساخت که حجم آن سه برابر حجم مکعب داده شده باشد؟

فصل ۱۵

کاربردی از جبر (کد گذاری)

تاکنون در این کتاب، جبر را صرفاً از نظری بررسی کرده‌ایم، بنابراین ممکن است دانشجویان هیچ گونه کاربردی از جبر را در زندگی بشری تصور نکنند. اما واقعیت امر چنین نیست و کاربردهای فراوانی از جبر در علوم مختلف می‌توان یافت. در این فصل نظریه‌ی کد گذاری را به طور کاملاً مختصر بررسی می‌کنیم. متذکر می‌شویم که جبر مجرد در رمزنگاری و مسائل ترکیبیاتی و علوم کامپیوتر نیز کار برد دارد، علاوه بر آن جبر مجرد در علومی مثل فیزیک و شیمی نیز کاربرهای وسیعی دارد و کتب فراوانی در این زمینه‌ها نوشته شده است.

۱.۱۵ کدهای خطی

در نظریه‌ی کد گذاری، مساله انتقال و دریافت سالم اطلاعات از یک کانال یا مخزن میانی، که ممکن است تحت تاثیر نوفه باشد، مطرح است. سیستم‌های مخابراتی مثل رادیو، تلویزیون، تلگراف، تلفن و یا سیستم‌های ذخیره‌ی اطلاعات مثل نوار، فیلم و غیره مثال‌هایی از این نوع هستند. در نظریه‌ی کد گذاری به صورت قابل ملاحظه‌ای از نظریه‌ی میدان‌های متناهی استفاده می‌شود. منشاء نظریه‌ی کد گذاری مقاله‌ی مشهور کلود شانون است که در سال ۱۹۴۸ چاپ شد. یکی دیگر از پیشگامان نظریه‌ی کد گذاری ریچارد همینگ است. او در سال ۱۹۵۰ کدهایی که یابنده‌ی خطا و تصحیح کننده‌ی خطا هستند را کشف کرد؛ این کدها به نام خود او معروفند. اما کد چیست؟ فرض کنید A مجموعه‌ای متناهی و n عدد صحیح مثبت باشد. زیرمجموعه‌ی C از $A^n = \underbrace{A \times \cdots \times A}_{n-\text{بار}}$ را یک کد به طول n گوییم. اعضای A را الفبا و اعضای A^n را واژه و هر عضو C را یک کد واژه می‌نامیم. یک واژه‌ی $u = (a_1, a_2, \ldots, a_n)$ را با $u = a_1 a_2 \cdots a_n$ نیز نشان می‌دهیم. کد C به طول n که شامل m کد واژه است را یک (n, m)- کد می‌نامیم. در حالت کلی مجموعه‌ای مثل $M \subseteq A^n$ متشکل از پیام‌ها داریم که با استفاده از یک تابع مناسب یک‌به‌یک ، آن را به یک کد C تبدیل می‌کنیم. این فرایند را کد گذاری می‌نامیم. سپس این کد از یک کانال که تحت تاثیر نوفه است، عبور می‌کند. بنابراین برخی از کد واژه‌های آن ممکن است تغییر کنند. کد پس از عبور از کانال به مکانی می‌رسد که دریافت کننده باید با استفاده از تابع کد گشایی به پیام‌های اولیه تبدیل کند. اما چون برخی از کد واژه‌ها تغییر کرده‌اند ابتدا باید خطاهای احتمالی کشف و تصحیح شوند.

از کدهای بسیار مهم که در این‌جا بررسی می‌کنیم کدهای خطی و به ویژه کدهای دوتایی هستند. یادآوری می‌کنیم که $\mathrm{GF}(q)$ میدان متناهی با q عضو است، که در آن q توانی از یک عدد اول است. به علاوه مرتبه‌ی هر میدان متناهی توانی از یک عدد اول است. در سرتاسر این فصل فرض می‌کنیم q توانی از یک عدد اول است.

تعریف ۱.۱.۱۵. زیرفضای C از فضای برداری $\mathrm{GF}(q)^n$ روی $\mathrm{GF}(q)$ را کد خطی به طول n روی $\mathrm{GF}(q)$ گوییم.

در حالتی که $q = 2$ کد خطی C را کد دوتایی می‌نامیم. بنابراین یک کد دوتایی زیرفضایی از فضای برداری $\mathbb{Z}_2^n = \mathrm{GF}(2)^n$ روی $\mathbb{Z}_2$ است. فرض کنید C یک کد خطی به طول n روی $\mathrm{GF}(q)$ باشد. اگر بُعد C روی $\mathrm{GF}(q)$ برابر k باشد گوییم C یک $[n, k]$- کد است. در این

حالت C شامل q^k کد واژه است. فرض کنید $u_1 = (a_{11}, \ldots, a_{1n})$، $\ldots$، $u_k = (a_{k1}, \ldots, a_{kn})$ پایه‌ای برای C روی $\mathrm{GF}(q)$ باشد. ماتریس $k \times n$، G که سطرهای آن به ترتیب u_1، $\ldots$، u_k باشد را یک ماتریس مولد برای C می‌نامیم:

$$G = \begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \vdots & \vdots \\ a_{k1} & \cdots & a_{kn} \end{bmatrix}.$$

بنابراین فضای تولید شده توسط سطرهای ماتریس G (فضای سطری G) همان C است. به ازای هر $u \in C$ اسکالرهای یکتای $c_1, \ldots, c_k \in \mathrm{GF}(q)$ وجود دارند که

$$\begin{aligned} u &= c_1 u_1 + \cdots + c_k u_k \\ &= (c_1 a_{11} + \cdots + c_k a_{k1}, \ldots, c_1 a_{1n} + \cdots + c_k a_{kn}) \\ &= [c_1, \ldots, c_k] \begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \vdots & \vdots \\ a_{k1} & \cdots & a_{kn} \end{bmatrix} \\ &= vG. \end{aligned}$$

بنابراین هر عضو $u \in C$ را می‌توان به صورت یکتای $u = vG$ نشان داد، که در آن $v \in \mathrm{GF}(q)^k$:

$$C = \{vG \mid v \in \mathrm{GF}(q)^k\}.$$

اگر G یک ماتریس مولد برای C باشد، آنگاه اعضای $\mathrm{GF}(q)^k$ را واژه‌های پیام گوییم. با انجام اعمال سطری مقدماتی (تعویض کردن جای سطرها، ضرب یک سطر در اسکالر ناصفر، و اضافه کردن مضربی از یک سطر به سطر دیگر) روی یک ماتریس، فضای سطری آن تغییر نمی‌کند. به علاوه چون رتبه‌ی ماتریس G برابر k است، پس از انجام اعمال سطری مقدماتی روی G صورت پلکانی آن عبارت است از

$$\begin{bmatrix} 1 & 0 & \cdots & 0 & b_{1,k+1} & \cdots & b_{1n} \\ 0 & 1 & \cdots & 0 & b_{2,k+1} & \cdots & b_{2n} \\ \vdots & \vdots & \ddots & & \vdots & & \vdots \\ 0 & 0 & \cdots & 1 & b_{k,k+1} & \cdots & b_{kn} \end{bmatrix} = [I_k \mid A]$$

که در آن I_k ماتریس همانی $k \times k$ است و

$$A = \begin{bmatrix} b_{1,k+1} & \cdots & b_{1n} \\ \vdots & & \vdots \\ b_{k,k+1} & \cdots & b_{kn} \end{bmatrix}$$

ماتریس G به صورت $G = [I_k \mid A]$ را ماتریس مولد استاندارد کد خطی C گوییم.

توجه کنید انجام یک عمل سطری مقدماتی روی ماتریس G به این معنی است که یک ماتریس مناسب $k \times k$ وارون‌پذیر E از سمت چپ در G ضرب شود. در واقع اگر E ماتریس حاصل از ماتریس همانی باشد که به جای سطر jام آن مجموع λ برابر سطر iام با سطر jام را قرار داده‌ایم، آنگاه EG همان ماتریس G است، جز این که به جای سطر iام آن مجموع λ برابر سطر jام با سطر iام G را قرار داده‌ایم. هم‌چنین اگر E ماتریس همانی باشد، جز این که به جای درایه‌های (i,i) آن λ قرار داده‌ایم، آنگاه ماتریس EG همان ماتریس G است، جز این که به جای سطر iام آن λ برابر سطر iام G را قرار داده‌ایم. در نهایت اگر E همان ماتریس همانی باشد، جز این که جای سطر iام و jام آن را تعویض کرده‌ایم، آنگاه ماتریس EG از تعویض جای سطر iام و jام G حاصل می‌شود.

حال اگر G یک ماتریس مولد $k \times n$ دلخواه برای $[n,k]$– کد خطی C، و M یک ماتریس وارون‌پذیر دلخواه $k \times k$ روی $\mathrm{GF}(q)$ باشند، آنگاه MG ماتریس $k \times n$ با رتبه‌ی k است و سطرهای آن ترکیب خطی از سطرهای G است. پس MG نیز یک ماتریس مولد برای کد

C است. به علاوه اگر M حاصل‌ضرب مناسبی از ماتریس‌های متناظر با اعمال سطری مقدماتی باشد، آنگاه $MG = [I_k \mid A]$ یک ماتریس مولد برای کد C است.

یک کد خطی را می‌توان به صورت دیگری، با استفاده از ماتریس امتحان توازن، توصیف کرد. فرض کنید C یک $[n,k]$- کدخطی روی $\mathrm{GF}(q)$ با ماتریس مولد استاندارد $G = [I_k \mid A]$ باشد. کد دوگان C یا مکمل متعامد C را که با $C^\perp$ نشان می‌دهیم عبارت است از

$$C^\perp = \{u \in \mathrm{GF}(q)^n \mid u \cdot v = ۰, \ \ \forall v \in C\},$$

که در آن $u \cdot v$ ضرب نقطه‌ای متعارف روی $\mathrm{GF}(q)^n$ است، یعنی اگر $u = (a_۱, \ldots, a_n)$ و $v = (b_۱, \ldots, b_n)$، آنگاه

$$u \cdot v = a_۱b_۱ + \cdots + a_nb_n.$$

اگر V یک فضای برداری روی میدان اعداد حقیقی با ضرب نقطه‌ای متعارف و W زیرفضای آن باشد به راحتی می‌توان دید که $V = W \oplus W^\perp$ و

$$\dim V = \dim W + \dim W^\perp.$$

اما اگر C یک کد خطی روی میدان متناهی $\mathrm{GF}(q)$ باشد، آنگاه ممکن است $\mathrm{GF}(q)^n$ به جمع مستقیم C و $C^\perp$ تجزیه نشود. حتی ممکن است $C = C^\perp$، که در این حالت C را خودمتعامد گوییم. اما همواره می‌توان ثابت کرد

$$\dim \mathrm{GF}(q)^n = \dim C + \dim C^\perp,$$

که نتیجه می‌دهد $\dim C^\perp = n - k$. فرض کنید H ماتریس $(n-k) \times n$ باشد که فضای سطری آن $C^\perp$ است. چون اعمال سطری مقدماتی روی H فضای سطری آن را تغییر نمی‌دهد، می‌توان فرض کرد $H = [B \mid I_{n-k}]$. توجه کنید چون بُعد $C^\perp$ برابر $n-k$ است، رتبه‌ی ماتریس H نیز برابر $n-k$ است. اکنون چون به ازای هر $u \in C^\perp$ و $v \in C$، $u \cdot v = ۰$، داریم $uG^\top = \mathbf{0}$، که در آن $G^\top$ ترانهاده‌ی ماتریس G است. از این‌رو $HG^\top = \mathbf{0}$ و

$$[B \mid I_{n-k}] \begin{bmatrix} I_k \\ A^\top \end{bmatrix} = \mathbf{0}$$

که نتیجه می‌دهد $B = -A^\top$. بنابراین $H = [-A^\top \mid I_{n-k}]$. چون $(C^\perp)^\perp = C$ داریم $GH^\top = \mathbf{0}$. ماتریس H را ماتریس امتحان توازن کد C گوییم. بنابراین اگر G ماتریس مولد و H ماتریس امتحان توازن کد C باشد، آنگاه H ماتریس مولد و G ماتریس امتحان توازن کد $C^\perp$ است. توجه کنید اگر C یک $[n,k]$- کد با ماتریس امتحان توازن H باشد، آنگاه $u \in C$ اگر و تنها اگر $Hu^\top = \mathbf{0}$. بنابراین C فضای جواب دستگاه معادلات همگن $Hu^\top = \mathbf{0}$ است. معادلات حاصل‌ضرب از دستگاه $Hu^\top = \mathbf{0}$ را معادلات امتحان گوییم.

اگر H یک ماتریس $(n-k) \times n$ دلخواه با درایه‌های در $\mathrm{GF}(q)$ و رتبه‌ی $n-k$ باشد، فضای جواب دستگاه $Hx^\top = \mathbf{0}$ یک کد خطی C به طول n و بعد k روی $\mathrm{GF}(q)$ است. ماتریس H را ماتریس امتحان توازن C گوییم.

مثال ۲.۱.۱۵. فرض کنید C یک $[۶,۳]$- کد دوتایی با ماتریس مولد استاندارد

$$G = \begin{bmatrix} ۱ & ۰ & ۰ & ۰ & ۱ & ۱ \\ ۰ & ۱ & ۰ & ۱ & ۰ & ۱ \\ ۰ & ۰ & ۱ & ۱ & ۱ & ۰ \end{bmatrix} = [I_۳ \mid A]$$

باشد. در این صورت چون $A = A^\top$، ماتریس امتحان توازن C عبارت است از

$$H = \begin{bmatrix} ۰ & ۱ & ۱ & ۱ & ۰ & ۰ \\ ۱ & ۰ & ۱ & ۰ & ۱ & ۰ \\ ۱ & ۱ & ۰ & ۰ & ۰ & ۱ \end{bmatrix} = [A \mid I_۳].$$

فرض کنید $u = (a_۱, a_۲, a_۳) \in \mathbb{Z}_۲^۳$ واژه دلخواهی باشد، در این صورت

$$uG = (a_۱, a_۲, a_۳, a_۲ + a_۳, a_۱ + a_۳, a_۱ + a_۲) \in C.$$

اگر قرار دهیم $x_۴ = a_۲ + a_۳$، $x_۵ = a_۱ + a_۳$ و $x_۶ = a_۱ + a_۲$، آنگاه پیام $u = a_۱a_۲a_۳$ به صورت $v = a_۱a_۲a_۳x_۴x_۵x_۶ \in C$ کد گذاری و انتقال داده شده است. از طرف دیگر اگر $v = (a_۱, a_۲, a_۳, a_۴, a_۵, a_۶) \in C$، آنگاه $Hv^\top = ۰$. پس

$$\begin{aligned} a_۲ + a_۳ + a_۴ &= ۰ \\ a_۱ + a_۳ + a_۵ &= ۰ \\ a_۱ + a_۲ + a_۶ &= ۰ \end{aligned}$$

و بنابراین $a_۴ = a_۲ + a_۳$، $a_۵ = a_۱ + a_۳$، $a_۶ = a_۱ + a_۲$. مثلاً اگر $u = ۰۱۱$ یک پیام باشد، کد واژه‌ی متناظر آن $v = ۰۱۱۰۱۱$ است. همه‌ی $۲^۳$ پیام‌ها و کد واژه‌ها عبارت‌اند از

پیام واژه	۰۰۰	۰۱۱	۱۱۰	۰۰۱
کد واژه	۰۰۰۰۰۰	۰۱۱۰۱۱	۱۱۰۱۱۰	۰۰۱۱۱۰
پیام واژه	۱۱۱	۰۱۰	۱۰۱	۱۰۰
کد واژه	۱۱۱۰۰۰	۰۱۰۱۰۱	۱۰۱۱۰۱	۱۰۰۰۱۱

در این‌جا در هر کد واژه سه حرف اول را پیام واژه و سه حرف بعد را حروف امتحان گوییم. به طور کلی فرض کنید C یک $[n, k]$-کد خطی روی $\mathrm{GF}(q)$ با ماتریس امتحان توازن $H = [B \mid I_{n-k}]$ باشد. اگر u یک کد واژه باشد k حرف اول در u را پیام واژه و $n - k$ حرف دیگر را حروف امتحان گوییم. □

مثال ۳.۱.۱۵. (کد تکرار) فرض کنید E ماتریس $۱ \times (n - ۱)$ باشد که همه‌ی درایه‌های آن برابر ۱ است. $[n, ۱]$- کد خطی دوتایی با ماتریس امتحان توازن $H = [E \mid I_{n-۱}]$ را کد تکرار گوییم. بنابراین

$$H = \begin{bmatrix} ۱ & ۱ & ۰ & \cdots & ۰ \\ ۱ & ۰ & ۱ & \cdots & ۰ \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ ۱ & ۰ & ۰ & \cdots & ۱ \end{bmatrix}.$$

در این جا هر کد واژه تنها یک حرف پیام $a_۱ \in \mathbb{Z}_۲$ و $n - ۱$ حرف امتحان $x_۲ = \cdots = x_n$ دارد که همگی با $a_۱$ برابرند (یعنی $a_۱$، n بار تکرار شده). در واقع در این کد تنها دو کد واژه‌ی ۰۰۰۰۰۰ و ۱۱۱۱۱۱ وجود دارند. ماتریس مولد استاندارد این کد ماتریس $G = [I_۱, T]$ است، که در آن T ماتریس $(n - ۱) \times ۱$ است که همه‌ی درایه‌های آن برابر ۱ است، بنابراین $G = [۱ \cdots ۱]$. □

مثال ۴.۱.۱۵. (کد امتحان توازن) این کد یک $[n, n - ۱]$- کد دوتایی با ماتریس امتحان توازن $H = [۱۱ \cdots ۱] = [B \mid I_۱]$ است، که در آن $B = [۱۱ \cdots ۱]$ ماتریس $(n - ۱) \times ۱$ است. اگر $v = (a_۱, a_۲, \ldots, a_n) \in C$، آنگاه $Hv^\top = ۰$. بنابراین

$$a_۱ + a_۲ + \cdots + a_n = ۰,$$

و $a_n = a_۱ + \cdots + a_{n-۱}$. پس پیام واژه‌ی $a_۱a_۲ \cdots a_{n-۱} \in \mathbb{Z}_۲^{n-۱}$ به صورت $a_۱a_۲ \cdots a_{n-۱}x_n$ کد گذاری می‌شود، که در آن $x_n = a_۱ + \cdots + a_{n-۱}$. توجه کنید ماتریس مولد استاندارد این کد عبارت است از

$$G = \begin{bmatrix} ۱ & ۰ & \cdots & ۰ & ۱ \\ ۰ & ۱ & \cdots & ۰ & ۱ \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ ۰ & ۰ & \cdots & ۱ & ۱ \end{bmatrix},$$

یعنی $G = [I_{n-۱} \mid B^\top]$. □

یکی از کدهای مهم کدهای همینگ هستند. کد دوتایی $\mathscr{H}(r, ۲)$ به طول $n = ۲^r - ۱$، $(r \geq ۲)$ که ستون‌های ماتریس امتحان توازن آن متشکل از همه‌ی بردارهای ناصفر $\mathbb{Z}_۲^r$ است را کد همینگ دوتایی گوییم. توجه کنید $\mathscr{H}(r, ۲)$ یک $[۲^r - ۱, ۲^r - ۱ - r]$- کد است. به عنوان مثال اگر $r = ۲$، آنگاه $\mathscr{H}(۲, ۲)$ یک $[۳, ۱]$- کد با ماتریس امتحان توازن، H، و ماتریس مولد، G،

$$H = \begin{bmatrix} ۱ & ۱ & ۰ \\ ۱ & ۰ & ۱ \end{bmatrix}, \quad G = [۱ \ ۱ \ ۱]$$

است. این کد همان $[۳, ۱]$- کد تکرار است.

مثال ۵.۱.۱۵. ماتریس امتحان توازن، H، و ماتریس مولد، G، $[۷, ۴]$- کد همینگ $\mathscr{H}(۳, ۲)$ عبارت‌اند از

$$H = \begin{bmatrix} ۱ & ۱ & ۱ & ۰ & ۱ & ۰ & ۰ \\ ۱ & ۱ & ۰ & ۱ & ۰ & ۱ & ۰ \\ ۱ & ۰ & ۱ & ۱ & ۰ & ۰ & ۱ \end{bmatrix}, \quad G = \begin{bmatrix} ۱ & ۰ & ۰ & ۰ & ۱ & ۱ & ۱ \\ ۰ & ۱ & ۰ & ۰ & ۱ & ۱ & ۰ \\ ۰ & ۰ & ۱ & ۰ & ۱ & ۰ & ۱ \\ ۰ & ۰ & ۰ & ۱ & ۰ & ۱ & ۱ \end{bmatrix}.$$

توجه کنید ستون‌های H بسط دودوئی اعداد ۱، ۲، ۳، . . .، ۷ هستند. با تعویض جای ستون‌های ماتریس H ماتریس کدهای معادل (که در ادامه تعریف می‌کنیم) با $\mathscr{H}(r, ۲)$ به دست می‌دهند. در این جا کدهای معادل را به پیمانه‌ی هم‌ارزی یکی می‌گیریم. اگر بنویسیم

$$H' = \begin{bmatrix} ۰ & ۰ & ۰ & ۱ & ۱ & ۱ & ۱ \\ ۰ & ۱ & ۱ & ۰ & ۰ & ۱ & ۱ \\ ۱ & ۰ & ۱ & ۰ & ۱ & ۰ & ۱ \end{bmatrix},$$

آنگاه H' یک ماتریس امتحان توازن برای $\mathscr{H}(۳, ۲)$ است. ستون‌های H' به ترتیب بسط دودوئی ۱، ۲، ۳، . . .، ۷ هستند. اگر بنویسیم

$$H'' = \begin{bmatrix} ۱ & ۱ & ۱ & ۰ & ۱ & ۰ & ۰ \\ ۰ & ۱ & ۱ & ۱ & ۰ & ۱ & ۰ \\ ۰ & ۰ & ۱ & ۱ & ۱ & ۰ & ۱ \end{bmatrix}$$

آنگاه H'' یک ماتریس امتحان توازن برای $\mathscr{H}(۳, ۲)$ است. در این جا می‌بینیم که این کد یک کد دوری است، یعنی شیفت دوری یک کد واژه مجدداً کد واژه است (شیفت دوری واژه‌ی $a_۱a_۲ \cdots a_n$ عبارت است از $a_na_۱ \cdots a_{n-۱}$). این خاصیت را در بخش کدهای دوری بررسی می‌کنیم. □

یکی از مفاهیم مهم مفهوم کدهای معادل است. برای تعریف این مفهوم ابتدا ماتریس‌های جایگشتی را معرفی می‌کنیم. ماتریس P را یک ماتریس جایگشتی گوییم، هرگاه از جابجا کردن ستون‌های ماتریس همانی به دست آمده باشد. در واقع اگر e_i، ستون iام ماتریس همانی باشد، آنگاه ستون iام ماتریس جایگشتی حاصل از جایگشت $\pi \in S_n$ برابر $e_{\pi(i)}$ است. به عنوان مثال ماتریس جایگشتی متناظر جایگشت $\pi = (۱ \ ۲ \ ۵)(۳ \ ۴) \in S_۶$ عبارت است از

$$P = \begin{bmatrix} ۰ & ۰ & ۰ & ۰ & ۱ & ۰ \\ ۱ & ۰ & ۰ & ۰ & ۰ & ۰ \\ ۰ & ۰ & ۰ & ۱ & ۰ & ۰ \\ ۰ & ۰ & ۱ & ۰ & ۰ & ۰ \\ ۰ & ۱ & ۰ & ۰ & ۰ & ۰ \\ ۰ & ۰ & ۰ & ۰ & ۰ & ۱ \end{bmatrix}.$$

اکنون توجه می‌کنیم که اگر $1 \leq j \leq n$، A_j، ستون jام ماتریس A باشد، آنگاه ستون jام ماتریس AP برابر $A_{\pi(j)}$ است. به عنوان مثال اگر P ماتریس جایگشتی متناظر $\pi = (۱\ ۲\ ۵)(۳\ ۴)$ باشد، که در بالا معرفی شد و

$$A = \begin{bmatrix} ۱ & ۲ & ۳ & ۴ & ۵ & ۶ \\ a & b & c & d & e & f \\ u & v & w & x & y & z \end{bmatrix}$$

آنگاه

$$AP = \begin{bmatrix} ۲ & ۵ & ۴ & ۳ & ۱ & ۶ \\ b & e & d & c & a & f \\ v & y & x & w & u & z \end{bmatrix}.$$

فرض کنید G ماتریس مولد $[n,k]$-کد دوتایی C باشد. اگر P یک ماتریس $n \times n$ دلخواه جایگشتی باشد، آنگاه GP یک ماتریس مولد برای کد k بُعدی $C_۱$ است. کدهای C و $C_۱$ را معادل گوییم. توجه کنید دو کد خطی دوتایی معادل هستند، هرگاه بتوان ماتریس مولد یکی را با ضرب یک ماتریس جایگشتی از راست در ماتریس مولد دیگری به دست آورد، یعنی اگر یکی از کدها را بتوان با استفاده از یک جایگشت بر روی مولفه‌های دیگری به دست آورد. به بیان دیگر دو کد معادل‌اند اگر کد واژه‌های آن‌ها تنها در ترتیب حروف متفاوت باشند. رابطه‌ی معادل بودن کدها یک رابطه‌ی هم‌ارزی است، بنابراین کدهای معادل را یکی در نظر می‌گیریم. اگر $u = u_۱u_۲\cdots u_n$ یک کدواژه در C باشد و $\sigma \in S_n$، تعریف می‌کنیم: $\sigma u = u_{\sigma(۱)}u_{\sigma(۲)}\cdots u_{\sigma(n)}$ و $\sigma C = \{\sigma u \mid u \in C\}$. بنابراین دو کد دوتایی C و $C_۱$ به طول n معادل‌اند اگر و تنها اگر جایگشت $\sigma \in S_n$ وجود داشته باشد که $\sigma C = C_۱$.

مثال ۶.۱.۱۵. کد خطی دوتایی $C_۱$ و $C_۲$ را با ماتریس‌های مولد $G_۱$ و $G_۲$ در نظر بگیرید که در آن

$$G_۱ = \begin{bmatrix} ۱ & ۰ & ۰ & ۰ & ۱ & ۱ \\ ۰ & ۱ & ۰ & ۱ & ۰ & ۱ \\ ۰ & ۰ & ۱ & ۱ & ۱ & ۰ \end{bmatrix}, \quad G_۲ = \begin{bmatrix} ۰ & ۱ & ۱ & ۱ & ۰ & ۰ \\ ۱ & ۰ & ۱ & ۰ & ۱ & ۰ \\ ۱ & ۱ & ۰ & ۰ & ۰ & ۱ \end{bmatrix}.$$

در این جا با تعویض ستون‌های اول و چهارم با یکدیگر ، تعویض ستون‌های دوم و پنجم با یکدیگر و تعویض ستون‌های سوم و ششم با یکدیگر در ماتریس $G_۱$، ماتریس $G_۲$ به دست می‌آید. یعنی با اعمال جایگشت $\pi = (۱\ ۴)(۲\ ۵)(۳\ ۶)$ بر مولفه‌های کد واژه‌های $C_۱$ کد واژه‌های $C_۲$ به دست می‌دهند. بنابراین با ضرب ماتریس $G_۱$ از راست در ماتریس جایگشتی

$$P = \begin{bmatrix} ۰ & ۰ & ۰ & ۱ & ۰ & ۰ \\ ۰ & ۰ & ۰ & ۰ & ۱ & ۰ \\ ۰ & ۰ & ۰ & ۰ & ۰ & ۱ \\ ۱ & ۰ & ۰ & ۰ & ۰ & ۰ \\ ۰ & ۱ & ۰ & ۰ & ۰ & ۰ \\ ۰ & ۰ & ۱ & ۰ & ۰ & ۰ \end{bmatrix}$$

ماتریس $G_۲$ به دست می‌آید: $G_۲ = G_۱P$. توجه کنید ماتریس P از ماتریس همانی با استفاده از جایگشت $(۱\ ۴)(۲\ ۵)(۳\ ۶)$ به دست آید، یعنی ستون اول و چهارم و ستون دوم و پنجم و ستون سوم و ششم در ماتریس I با یکدیگر تعویض شده‌اند. هم‌چنین با ضرب ماتریس $G_۲$ از راست در ماتریس

$$Q = \begin{bmatrix} ۰ & ۰ & ۰ & ۱ & ۰ & ۰ \\ ۰ & ۰ & ۰ & ۰ & ۱ & ۰ \\ ۰ & ۰ & ۰ & ۰ & ۰ & ۱ \\ ۱ & ۰ & ۰ & ۰ & ۰ & ۰ \\ ۰ & ۱ & ۰ & ۰ & ۰ & ۰ \\ ۰ & ۰ & ۱ & ۰ & ۰ & ۰ \end{bmatrix}$$

(که متناظر جایگشت $\pi = \pi^{-1}$ است) ماتریس G_1 به دست می‌آید: $G_1 = G_2 Q$. بنابراین $Q = P = Q^{-1}$. چون $C_1 = \{uG_1 \mid u \in \mathbb{Z}_2^3\}$ داریم

$$C_1 = \{000000, 100011, 010101, 001110, 110110, 101101, 011011, 111000\}$$

و چون $C_2 = \{uG_2 \mid u \in \mathbb{Z}_2^3\}$ داریم

$$C_2 = \{000000, 011100, 101010, 110001, 110110, 101101, 011101 1, 000100\}.$$

توجه کنید اگر جایگشت $\pi = (1\ 4)(2\ 5)(3\ 6)$ را بر هر کد واژه‌ی C_1 اثر دهیم، کد واژه‌های C_2 به دست می‌آیند. مثلاً اگر $100011 \in C_1$، آنگاه با اعمال π بر این عضو داریم $011100 \in C_2$. □

اکنون می‌خواهیم مفهوم کدهای معادل را به طور کلی تعریف کنیم. فرض کنید $\sigma \in S_n$ و $a_1, \ldots, a_n \in \mathrm{GF}(q)$ اعضای ناصفری باشند. تابع $\mu : \mathrm{GF}(q)^n \longrightarrow \mathrm{GF}(q)^n$ با ضابطه‌ی $\mu(u_1 \cdots u_n) = (a_1 u_{\sigma(1)}) \cdots (a_n u_{\sigma(n)})$ را یک تبدیل تک‌جمله‌ای گوییم.
$[n, k]$- کدهای خطی C و C_1 روی $\mathrm{GF}(q)$ را معادل گوییم، هرگاه تبدیل تک‌جمله‌ای μ وجود داشته باشد که $\mu C = C_1$، یعنی

$$\mu C = \{\mu(u_1 \cdots u_n) = (a_1 u_{\sigma(1)}) \cdots (a_n u_{\sigma(n)}) \mid u_1 \cdots u_n \in C\} = C_1.$$

در حالت $q = 2$ تعریف بالا همان تعریف آشنای قبلی برای کدهای دوتایی است. برای بیان ماتریسی این تعریف، ماتریس تک‌جمله‌ای را معرفی می‌کنیم. ماتریس M را تک‌جمله‌ای گوییم، هرگاه در هر سطر و ستون آن دقیقاً یک عضو ناصفر وجود داشته باشد. ماتریس تک‌جمله‌ای روی $\mathbb{Z}_2$ همان ماتریس جایگشتی است. ماتریس تک‌جمله‌ای روی یک میدان دلخواه برابر حاصل‌ضرب یک ماتریس جایگشتی در یک ماتریس قطری وارون‌پذیر است. فرض کنید C یک $[n, k]$- کد خطی روی $\mathrm{GF}(q)$ با ماتریس مولد G باشد. اگر μ یک تبدیل تک‌جمله‌ای متناظر با $a_1, \ldots, a_n \in \mathrm{GF}(q)$ و $\sigma \in S_n$ باشد، آنگاه ماتریس مولد $\mu C = C_1$ عبارت است از GM، که در آن M ماتریس تک‌جمله‌ای است که درایه‌های $(i, \sigma(i))$ آن a_i قرار دارد.
اگر C یک $[n, k]$- کد خطی روی $\mathrm{GF}(q)$ باشد، گروه خودریختی‌های C را که با $\mathrm{Aut}\, C$ نشان می‌دهیم، مجموعه‌ی همه‌ی تبدیل‌های تک‌جمله‌ای μ است که $\mu C \subseteq C$. در حالتی که $q = 2$ واضح است که $\mathrm{Aut}\, C = \{\sigma \in S_n \mid \sigma u \in C, \quad \forall u \in C\}$.

تمرین‌ها

در صورت لزوم برای انجام محاسبات از GAP استفاده کنید (صفحه‌ی ۳۶۸ را ببینید).

۱. نشان دهید کد C متشکل از واژه‌های داده شده خطی است، ماتریس مولد و ماتریس امتحان توازن استاندارد کد را بیابید. با استفاده از این ماتریس‌ها کدهای معادل آن‌ها را به دست آورید.
(الف) ۱۱۰۱۱۰، ۱۰۱۰۱۰، ۰۱۱۱۰۰، ۰۰۰۰۰۰.
(ب) ۰۰۰۰۰۰، ۰۰۰۰۱۱۱، ۰۱۱۱۰۰۱، ۰۱۱۱۱۱۰، ۱۰۱۰۰۱۱، ۱۰۱۰۱۰۰،
۱۱۰۱۰۱۰، ۱۱۰۱۱۰۱.
(ج) ۰۰۰۰۰۰، ۰۰۰۰۱۰، ۰۰۱۱۰۰، ۰۰۱۱۱۰، ۰۱۰۰۰۱، ۰۱۰۰۱۱، ۰۱۱۱۰۱، ۰۱۱۱۱۱،
۱۰۰۱۰۱، ۱۰۰۱۱۱، ۱۰۱۰۰۱، ۱۰۱۰۱۱، ۱۱۰۱۰۰، ۱۱۰۱۱۰، ۱۱۱۰۰۰، ۱۱۱۰۱۰.

۲. همه‌ی کد واژه‌های کد تولید شده توسط هر کدام از ماتریس‌های مولد زیر را بیابید. ماتریس امتحان توازن را بیابید.
(الف) $\begin{bmatrix} 1 & 0 & 2 & 0 \\ 0 & 1 & 1 & 2 \end{bmatrix}$ روی $\mathbb{Z}_3$.
(ب) $\begin{bmatrix} 1 & 0 & a & a & 1 & a^2 \\ 0 & 1 & a & 0 & 0 & 1 \end{bmatrix}$ روی $\mathrm{GF}(4)$، a عضو اولیه‌ای از $\mathrm{GF}(4)$.
(ج) $G = \begin{bmatrix} 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 \end{bmatrix}$ روی $\mathbb{Z}_2$.

(د) $\begin{bmatrix} ۱ & ۰ & ۰ & ۱ & ۱ & ۰ & ۱ \\ ۰ & ۱ & ۰ & ۰ & ۰ & ۱ & ۱ \\ ۰ & ۰ & ۱ & ۱ & ۰ & ۰ & ۱ \end{bmatrix}$ روی $\mathbb{Z}_۲$.

(هـ) $\begin{bmatrix} ۱ & ۰ & ۰ & ۱ & ۱ & ۰ \\ ۰ & ۱ & ۰ & ۰ & ۱ & ۱ \\ ۰ & ۰ & ۱ & ۱ & ۰ & ۱ \end{bmatrix}$ روی $\mathbb{Z}_۲$.

۳. همه‌ی کد واژه‌های کد تولید شده توسط هر کدام از ماتریس‌های امتحان توازن زیر را بیابید. ماتریس مولد استاندارد را مشخص کنید.

(الف) $\begin{bmatrix} ۱ & ۲ & ۱ & ۰ \\ ۰ & ۱ & ۰ & ۱ \end{bmatrix}$ روی $\mathbb{Z}_۳$.

(ب) $\begin{bmatrix} ۱ & ۱ & ۱ & ۱ & ۰ \\ ۰ & ۱ & ۰ & ۰ & ۱ \end{bmatrix}$ روی $\mathbb{Z}_۳$.

(ج) $\begin{bmatrix} ۱ & ۰ & ۱ & ۱ & ۰ & ۰ \\ ۰ & ۱ & ۱ & ۰ & ۱ & ۰ \\ ۱ & ۰ & ۰ & ۰ & ۰ & ۱ \end{bmatrix}$ روی $\mathbb{Z}_۲$.

(د) $\begin{bmatrix} ۱ & ۰ & ۱ & ۱ & ۰ & ۰ & ۰ \\ ۱ & ۱ & ۰ & ۰ & ۱ & ۰ & ۰ \\ ۰ & ۰ & ۱ & ۰ & ۰ & ۱ & ۰ \\ ۱ & ۱ & ۰ & ۰ & ۰ & ۰ & ۱ \end{bmatrix}$ روی $\mathbb{Z}_۲$.

۴. چه تعداد کد واژه در یک $[n, k]$- کد خطی روی $\mathrm{GF}(q)$ وجود دارد.

۵. ماتریس مولد برای یک $[۱۰, ۵]$- کد خطی دوتایی خود- دوگان C، یعنی $C = C^{\perp}$، را بیابید.

۶. با استفاده از تعریف، نشان دهید کدهای دوتایی با ماتریس‌های مولد زیر معادل هستند.

$$G_۱ = \begin{bmatrix} ۱ & ۱ & ۱ & ۰ \\ ۰ & ۱ & ۱ & ۰ \\ ۰ & ۰ & ۱ & ۱ \end{bmatrix}, \quad G_۲ = \begin{bmatrix} ۱ & ۰ & ۱ & ۱ \\ ۰ & ۱ & ۱ & ۱ \\ ۱ & ۰ & ۰ & ۱ \end{bmatrix}$$

۷. فرض کنید C یک $[۷, ۳]$- کد خطی دوتایی با ماتریس مولد زیر باشد:

$$G = \begin{bmatrix} ۰ & ۰ & ۰ & ۱ & ۱ & ۱ & ۱ \\ ۰ & ۱ & ۱ & ۰ & ۰ & ۱ & ۱ \\ ۱ & ۰ & ۱ & ۰ & ۱ & ۰ & ۱ \end{bmatrix}.$$

نشان دهید C یک کد خود- عمود (یعنی $C \subseteq C^{\perp}$) است. کد دوگان آن را بیابید.

۸. فرض کنید C یک $[۲k + ۱, k]$- کد خطی دوتایی باشد که $C \subseteq C^{\perp}$، یعنی C، خود عمود است. $C^{\perp} - C$ را توصیف کنید.

۹. فرض کنید p عدد اول باشد. آیا $[۸, ۴]$- کد خطی خود- دوگان C (یعنی $C = C^{\perp}$) روی $\mathbb{Z}_p$ وجود دارد؟

۲.۱۵ کدگشایی کدهای خطی

در این بخش نحوه‌ی کدگشایی کدهای خطی را بررسی می‌کنیم. فاصله‌ی همینگ دو واژه‌ی $u, v \in A^n$ را که با $d(u, v)$ نشان می‌دهیم عبارت است از تعداد مولفه‌های u و v که با یکدیگر متفاوت‌اند، یعنی

$$d(u, v) = |\{i \mid ۱ \leq i \leq n, a_i \neq b_i\}|$$

که در آن $u = (a_1, \ldots, a_n)$ و $v = (b_1, \ldots, b_n)$.

اگر $u \in \mathrm{GF}(q)^n$، وزن همینگ u را که با $\mathrm{wt}(u)$ نشان می‌دهیم عبارت است از تعداد مولفه‌های ناصفر u، یعنی $\mathrm{wt}(u) = d(u, \mathbf{0})$. اگر $u, v \in \mathrm{GF}(q)^n$، آنگاه داریم $d(u, v) = d(u - v, \mathbf{0}) = \mathrm{wt}(u - v)$. قضیه‌ی بعد که بیان می‌کند d یک متریک روی A^n و wt یک نُرم روی $\mathbb{Z}_4^n$ است را به عنوان تمرین واگذار می‌کنیم.

قضیه ۱.۲.۱۵. به ازای هر $u, v, w \in A^n$ داریم
(الف) $d(u, v) = d(v, u)$.
(ب) $d(u, v) = 0$ اگر و تنها اگر $u = v$.
(ج) $d(u, v) \leq d(u, w) + d(w, v)$، (نامساوی مثلث).
(د) اگر $u \in \mathbb{Z}_4^n$، آنگاه $u = \mathbf{0}$ اگر و تنها اگر $\mathrm{wt}(u) = 0$.

فاصله‌ی می‌نیمم کد C کوچک‌ترین فاصله‌ی ممکن بین کد واژه‌های متمایز آن است، یعنی

$$d_{\min} = \min\{d(u, v) \mid u, v \in C, u \neq v\}.$$

در حالتی که کد C خطی باشد، فاصله‌ی می‌نیمم آن عبارت است از کم‌ترین مقدار وزن همه‌ی کد واژه‌های ناصفر، این مطلب محتوای قضیه‌ی بعد است.

قضیه ۲.۲.۱۵. اگر C کد خطی به طول n روی $\mathrm{GF}(q)$ باشد، آنگاه

$$d_{\min} = \min\{\mathrm{wt}(u) \mid \mathbf{0} \neq u \in C\}.$$

اثبات. قرار می‌دهیم $d = \min\{\mathrm{wt}(u) \mid \mathbf{0} \neq u \in C\}$. فرض کنید $u, v \in C$ و $u \neq v$، چون C زیرفضای $\mathrm{GF}(q)^n$ است، $u - v \in C$. در نتیجه

$$d(u, v) = d(u - v, \mathbf{0}) = \mathrm{wt}(u - v) \in \{\mathrm{wt}(w) \mid \mathbf{0} \neq w \in C\}.$$

از این رو $d \leq d_{\min}$. حال اگر $\mathbf{0} \neq u \in C$ داریم

$$\mathrm{wt}(u) = d(u, \mathbf{0}) \in \{d(u, v) \mid u, v \in C,\ u \neq v\},$$

که نتیجه می‌دهد $d_{\min} \leq d$. □

مثال ۳.۲.۱۵. اگر C یک کد خطی به طول n روی $\mathrm{GF}(q)$ باشد، کد $\overline{C}$ به طول $n + 1$ روی $\mathrm{GF}(q)$ را به صورت

$$\overline{C} = \{(a_1, a_2, \ldots, a_n, a_{n+1}) \mid (a_1, a_2, \ldots, a_n) \in C,\ \sum_{i=1}^{n+1} a_i = 0\}$$

تعریف می‌کنیم. کد $\overline{C}$ را کد تعمیم یافته می‌نامیم. اگر G و H ماتریس مولد و امتحان توازن کد C باشند، به سادگی می‌توان دید که ماتریس مولد $\overline{G}$ از کد تعمیم یافته با اضافه کردن یک ستون به G حاصل می‌شود، طوری که مجموع عناصر روی سطرهای $\overline{G}$ برابر صفر باشد. به علاوه ماتریس امتحان توازن کد $\overline{C}$ برابر است با

$$\overline{H} = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ & & & 0 \\ & H & & \vdots \\ & & & 0 \end{bmatrix}.$$

اگر C کد دوتایی با فاصله‌ی می‌نیمم فرد باشد، فاصله‌ی می‌نیمم $\overline{C}$ برابر $d_{\min} \times 1 = d_{\min}$ است، زیرا همه‌ی وزن‌ها و همه‌ی فاصله‌های $\overline{C}$ زوج است. □

یک $[n,k]$- کد خطی با فاصله‌ی می‌نیمم d را $[n,k,d]$- کد گوییم. فرض کنید u یک کد واژه در کد C باشد که پس از انتقال از کانال v به جای آن دریافت شده است. اگر $u \neq v$، گوییم خطا رخ داده و $d(u,v)$ تعداد خطاهای انتقال u از کانال است. در حالتی که C خطی باشد $e = u - v$ را واژه‌ی خطا (یا بردار خطا) یا خطا گوییم. یک روش ساده‌ی کد گشایی، کد گشایی بردار v به نزدیک‌ترین کد واژه‌ی u نسبت به متریک همینگ است، یعنی انتخاب بردار خطا با وزن می‌نیمم. این روش کد گشایی را روش نزدیکترین همسایه گوییم و در آن v با همه‌ی q^k کد واژه مقایسه و نزدیک‌ترین آن‌ها به v انتخاب می‌شود. اگر احتمال p برای انتقال صحیح بزرگ‌تر از $\frac{۱}{۲}$ باشد، کد گشایی نزدیک‌ترین همسایه، کد گشایی با حداکثر امکان است. از این پس این مطلب را فرض می‌کنیم. به وضوح این روند برای مقادیر بزرگ k ممکن نیست، چرا که یکی از اهداف نظریه‌ی کد گذاری یافتن کدهایی با الگوریتم‌های کد گشایی سریع‌تر است. در حالتی که بیش از یک کاندیدا وجود داشته باشد یکی از آن‌ها را به دلخواه انتخاب می‌کنیم و یا (در صورت امکان) می‌خواهیم اطلاعات از نو منتقل شوند. فرض کنید $u \in A^n$ یک واژه باشد و $r \geq ۰$. مجموعه‌ی

$$S_r(u) = \{v \in A^n \mid d(u,v) \leq r\}$$

را کره به مرکز u و شعاع r یا یک r- کره حول u می‌نامیم. با استفاده از این مفهوم می‌توانیم در یک کد مثل C بفهمیم که این کد قادر به یافتن (یا تصحیح) t خطا هست یا نه؟ در کد گشایی بین کشف و تصحیح خطا تمایز قائل می‌شویم. هرگاه ساختار کد طوری باشد که بتوان حداکثر t خطا را که در انتقال یک واژه از کانال رخ داده است را کشف کرد، کد را t- یابنده‌ی خطا گوییم. در حالتی که بتوان حداکثر t خطا را کشف و تصحیح کرد، کد C را t- تصحیح کنندهی خطا می‌نامیم.
فرض کنید یک واژه‌ی $u \in C$ از کانال منتقل می‌شود و واژه‌ی v با t خطا $۱ \leq t \leq n$، دریافت می‌شود، در این صورت $t = d(u,v)$، یعنی تعداد خطاها برابر تعداد مولفه‌هایی از u و v است که با یکدیگر متفاوت‌اند. $S_t(u)$ منتقل بر همه‌ی واژه‌هایی است که حداکثر t خطا در آن ها رخ داده است. اگر مثلاً فرض کنیم هیچ کدام از کد واژه‌های C در t- کره‌ی واژه‌ی دیگر قرار نداشته باشند، یعنی $S_t(w) \cap S_t(w') = \emptyset$ به ازای هر $w' \in C$ و w، آنگاه از $v \in S_t(u)$ و $u \neq v$ نتیجه می‌شود v یک کد واژه در C نیست. بنابراین خطا کشف می‌شود. اگر همه‌ی t- کره‌های کد واژه‌های C دوبه‌دو مجزا باشند، آنگاه v تنها به یک کره‌ی یکتا $w \in C$ متعلق است. بنابراین خطا تصحیح می‌شود.

قضیه ۴.۲.۱۵. فرض کنید C یک کد به طول n با فاصله‌ی می‌نیمم d باشد و از روش کد گشایی نزدیک‌ترین همسایه استفاده کنیم.
(الف) اگر $t + ۱ \leq d$، آنگاه C، t- یابنده‌ی خطا است.
(ب) اگر $۲t + ۱ \leq d$، آنگاه C، t- تصحیح کننده‌ی خطا است.
در حالتی که C خطی باشد عکس (الف) و (ب) نیز برقرار است.

اثبات. (الف) فرض کنید $u \in C$. اگر $v \in C$ و $v \in S_t(u)$، آنگاه

$$d(u,v) \leq t \leq d - ۱,$$

که امکان ندارد ، زیرا d فاصله‌ی می‌نیمم C است. پس هیچ عضو C در $S_t(u)$ قرار ندارد. بنابراین از $v \in S_t(u)$ نتیجه می‌شود v عضو C نیست و از این رو C می‌تواند t خطا را بیابد.
(ب) فرض کنید $u \neq v$ دو کد واژه در C باشند. اگر $w \in S_t(u) \cap S_t(v)$، آنگاه بنا به نامساوی مثلث داریم

$$d(u,v) \leq d(u,w) + d(w,v) \leq t + t = ۲t \leq d - ۱,$$

که خلاف فرض است، زیرا d فاصله‌ی می‌نیمم C است. بنابراین به ازای هر $u, v \in C$ که $u \neq v$ داریم $S_t(u) \cap S_t(v) = \phi$. یعنی اگر واژه‌ی w دریافت شده و حاوی حداکثر t خطا باشد، آنگاه w به یک کره‌ی یکتا عضوی از C مثل u متعلق است. از این رو خطا تصحیح می‌شود. در واقع پیام فرستاده شده همان u است.
اثبات آخرین ادعای قضیه به عنوان تمرین واگذار می‌شود. □

مثال ۵.۲.۱۵. $[۶,۳]$- کد دوتایی مثال ۲.۱.۱۵ را در نظر بگیرید:

$$C = \{۰۰۰۰۰۰, ۰۱۱۰۱۱, ۱۱۰۱۱۰, ۰۰۱۱۱۰, ۱۰۰۰۱۱, ۰۱۰۱۰۱, ۱۰۱۱۰۱\}.$$

داریم

$$\mathrm{wt}(\text{۰۱۱۰۱۱}) = \text{۴}, \quad \mathrm{wt}(\text{۱۱۰۱۱۰}) = \text{۴}, \quad \mathrm{wt}(\text{۰۰۱۱۱۰}) = \text{۳}$$
$$d(\text{۰۱۱۰۱۱}, \text{۱۱۰۱۱۰}) = \text{۴}, \quad d(\text{۰۱۱۰۱۱}, \text{۰۰۱۱۱۰}) = \text{۳}.$$

فاصله‌ی می‌نیمم C که در این جا همان می‌نیمم وزن کد واژه‌های ناصفر C برابر با $d = \text{۳}$ است. چون $d - \text{۱} = \text{۲}$، بنا به قضیه‌ی ۴.۲.۱۵، C می‌تواند حداکثر ۲ خطا را بیابد، در واقع هیچ‌کدام از کد واژه‌های C در ۲- کره‌ی کد واژه‌ی دیگر قرار ندارد. اگر واژه‌ی ۰۰۱۰۰۱ دریافت شده باشد، مثلاً داریم $\text{۰۰۱۰۰۱} \in S_{\text{۲}}(\text{۰۱۱۰۱۱})$، که نتیجه می‌دهد ۰۰۱۰۰۱ کد واژه نیست. توجه کنید اگر $v = \text{۰۰۱۰۰۱}$، آنگاه به ازای هر $u \in C$، داریم $\mathrm{wt}(u - v) \leq \text{۲}$ که نتیجه می‌دهد $u - v \notin C$، زیرا می‌نیمم وزن C برابر $d = \text{۳}$ است، یعنی $v \notin C$. اکنون چون $\frac{d - \text{۱}}{\text{۲}} = \text{۱}$، بنا به قضیه‌ی ۴.۲.۱۵، C می‌تواند حداکثر یک خطا را تصحیح کند. در واقع همه‌ی ۱- کره‌های کد واژه‌های C دوبه‌دو مجزا هستند. اگر واژه ۰۰۱۰۱۱ دریافت شده باشد، آنگاه چون $\text{۰۰۱۰۱۱} \in S_{\text{۱}}(\text{۰۱۱۰۱۱})$، نتیجه می‌گیریم که یک خطا رخ داده و واژه‌ی ۰۰۱۰۱۱ را با ۰۱۱۰۱۱ کد گشایی می‌کنیم. توجه کنید اگر $v = \text{۰۰۱۰۱۱}$، آنگاه $\mathrm{wt}(\text{۰۱۱۰۱۱} - v) = \text{۱} \leq d$. پس یک خطا رخ داده و به صورت ۰۱۱۰۱۱ تصحیح می‌شود. در یک کد تصحیح کننده‌ی خطاهای تکی ستون‌های H باید ناصفر باشند، اگر ستون iام صفر باشد، نمی‌توان یک خطا را که در iامین مکان رخ داده تصحیح کرد؛ همه‌ی ستون‌ها باید متمایز باشند، در غیر این صورت نمی‌توان بین خطاها تمایز قائل شد. □

قضیه ۶.۲.۱۵. فرض کنید H ماتریس امتحان توازن یک $[n, k, d_{\min}]$- کد خطی C روی $\mathrm{GF}(q)$ باشد. در این صورت
(الف) $\dim C = n - \operatorname{rank} H$.
(ب) $d_{\min} = \operatorname{rank} H + \text{۱}$ اگر و تنها اگر هر $n - k$ ستون H مستقل خطی باشند.
(ج) $d_{\min} \geq \operatorname{rank} H + \text{۱}$
(د) d فاصله‌ی می‌نیمم C است، یعنی $d = d_{\min}$، اگر و تنها اگر هر s ستون $(s \leq d - \text{۱})$، H مستقل خطی باشند.

اثبات. (الف) واضح است.
(ب) فرض کنید G ماتریس مولد استاندارد C باشد. چون هر سطر G عضوی از C است و در هر سطر G حداقل $k - \text{۱}$ درایه صفر است، $d \leq n - (k - \text{۱})$. حال اگر $d \geq n - (k - \text{۱})$، آنگاه در هر سطر G دقیقاً $k - \text{۱}$ درایه صفر است. بنابراین هر k سطر دلخواه G مستقل خطی‌اند. از این رو هر $n - k$ ستون دلخواه H مستقل خطی‌اند.
(د) حال اگر $d = d_{\min}$، آنگاه $d = \operatorname{rank} H + \text{۱}$. پس هر $n - k = d - \text{۱}$ ستون H مستقل خطی‌اند. بنابراین به ازای هر $s \leq d - \text{۱}$، هر s ستون H مستقل خطی‌اند. حال اگر به ازای هر s که $s \leq d - \text{۱}$، هر s ستون H مستقل خطی باشند. به ویژه $d - \text{۱}$ ستون H مستقل خطی‌اند و

$$d_{\min} - \text{۱} = \operatorname{rank} H = d - \text{۱},$$

یعنی $d_{\min} = d$. □

در ماتریس امتحان توازن کد همینگ دوتایی $\mathscr{H}(r, \text{۲})$ همه‌ی ستون‌ها متمایز و ناصفرند، پس ستون‌ها دوبه‌دو مستقل خطی‌اند. بنابراین بنا به قسمت (د) قضیه‌ی ۶.۲.۱۵، فاصله‌ی می‌نیمم کد $\mathscr{H}(r, \text{۲})$ برابر ۳ است، یعنی $\mathscr{H}(r, \text{۲})$ یک $[\text{۲}^r - \text{۱}, \text{۲}^r - \text{۱} - r, \text{۳}]$- کد است. از این‌رو بنا به قضیه‌ی ۶.۲.۱۵، $\mathscr{H}(r, \text{۲})$ تصحیح کننده‌ی خطاهای تکی است.
اکنون کدهای همینگ را روی میدان دلخواه $\mathrm{GF}(q)$ تعمیم می‌دهیم.

تعریف ۷.۲.۱۵. فرض کنید $n = \frac{q^k - \text{۱}}{q - \text{۱}}$، که در آن q توانی از یک عدد اول است. $[n, n - k]$- کد همینگ $\mathscr{H}(k, q)$ روی $\mathrm{GF}(q)$ یک کد با ماتریس امتحان توازن H است، طوری که ستون‌های آن دوبه‌دو روی $\mathrm{GF}(q)$ مستقل خطی باشند، یعنی ستون‌ها مجموعه‌ی می‌نیمال متشکل از بردارهای دوبه‌دو مستقل خطی است.

بنا به قسمت (د) از قضیه‌ی ۶.۲.۱۵، فاصله‌ی می‌نیمم $\mathscr{H}(k, q)$ برابر ۳ است.

تعریف ۸.۲.۱۵. کد خطی C به طول n روی $\mathrm{GF}(q)$ با فاصله‌ی می‌نیمم $d = ۲t + ۱$ را کد کامل گوییم، هرگاه به ازای هر $u \in \mathrm{GF}(q)^n$ دقیقاً یک کد واژه‌ای $v \in C$ وجود داشته باشد که $d(u, v) \leq t$.

بنا به قضیه‌ی ۶.۲.۱۵، $[n, k, d]$- کد خطی C روی $\mathrm{GF}(q)$ کامل است اگر و تنها اگر تصحیح کننده‌ی حداقل $t = \frac{d-۱}{۲}$ خطا باشد. پس کدهای همینگ $\mathscr{H}(k, q)$ کامل هستند.

قضیه ۹.۲.۱۵. (کران همینگ) اگر C یک کد خطی t- تصحیح کننده‌ی خطا به طول روی $\mathrm{GF}(q)$ باشد، آنگاه

$$|C| \sum_{i=۰}^{t} \binom{n}{i} (q-۱)^i \leq q^n,$$

و تساوی برقرار است اگر و تنها اگر C کامل باشد.

اثبات. تعداد همه‌ی بردارها در $\mathrm{GF}(q)^n$ برابر q^n تا و تعداد بردارهای با وزن j در $\mathrm{GF}(q)^n$ برابر $\binom{n}{j}(q-۱)^j$ تا است. هم‌چنین کره‌های به مرکز کد واژه‌های در C و شعاع t مجزا هستند (چون C، تصحیح کننده‌ی t خطاست) و به علاوه هر کدام کره‌ها، که تعداد شان $|C|$ تا است، شامل $\sum_{i=۰}^{t} \binom{n}{i}(q-۱)^i$ بردار است. بنابراین

$$|C| \sum_{i=۰}^{t} \binom{n}{i} (q-۱)^i \leq q^n,$$

که حکم را ثابت می‌کند. □

در عمل یک $[n, k]$- کد خطی شامل تعداد زیادی واژه است. بنابراین به کارگیری روش کد گشایی نزدیک‌ترین همسایه با محاسبه‌ی فاصله‌ی بین واژه‌های دریافت شده و همه‌ی q^k واژه به صرفه نیست. اما روش‌هایی وجود دارد که محاسبات را به مقدار زیادی کاهش می‌دهد. یکی از این روشها، کد گشایی هم‌مجموعه است و اساس آن بر این است که گروه $\mathrm{GF}(q)^n$ به هم مجموعه‌های C افراز می‌شود. به ازای هر هم مجموعه‌ی C در $\mathrm{GF}(q)^n$ واژه‌ی e با وزن می‌نیمم را اختیار می‌کنیم، e را پیشروی هم‌مجموعه گوییم. توجه کنید ممکن است در یک هم‌مجموعه بیش از یک پیشرو وجود داشته باشد، که یکی از آن‌ها را انتخاب می‌کنیم. روند کد گشایی هم‌مجموعه به صورت زیر است: اگر واژه‌ی $b \in \mathrm{GF}(q)^n$ دریافت شده و e پیشرو هم‌مجموعه‌ی $v + C$ باشد، آنگاه u را به صورت $u - e$ کد گشایی می‌کنیم.

قضیه ۱۰.۲.۱۵. کد گشایی هم‌مجموعه همان کد گشایی نزدیک‌ترین همسایه است.

اثبات. فرض کنید C یک $[n, k]$- کد خطی باشد. اگر واژه‌ی v دریافت شده و e پیشرو هم‌مجموعه‌ی $v + C$ باشد، آنگاه $u = v - e$ یک کد واژه در C است، که از روش کد گشایی هم‌مجموعه برای کد گشایی v در نظر گرفته می‌شود. باید نشان دهیم u نزدیک‌ترین عضو به v نسبت به هر عضو دیگر w از C است. داریم $v - w \in v + C = e + C$، پس بنا به انتخاب e در C، $\mathrm{wt}(e) \leq \mathrm{wt}(v - w)$. از این رو

$$d(v, u) = \mathrm{wt}(v - u) = \mathrm{wt}(e) \leq \mathrm{wt}(v - w) = d(v, w),$$

و این همان چیزی است که می‌خواستیم. □

فرض کنید C یک $[n, k]$- کد خطی روی $\mathrm{GF}(q)$ باشد. پس C زیرفضای $\mathrm{GF}(q)$ است. فضای خارج قسمتی

$$\mathrm{GF}(q)^n / C = \{u + C \mid u \in \mathrm{GF}(q)^n\}$$

را در نظر می‌گیریم، که در آن $u + C = \{u + v \mid v \in C\}$ هم‌مجموعه‌ی C با نماینده‌ی $u \in \mathrm{GF}(q)^n$ است. چون هم مجموعه‌های C، $\mathrm{GF}(q)^n$ را افراز می‌کنند، داریم

$$\mathrm{GF}(q)^n = C \cup (u_۱ + C) \cup (u_۲ + C) \cup \cdots \cup (u_r + C), \quad r = q^{n-k} - ۱$$

فرض کنید $u_۱$، $u_۲$، ...، u_r پیشروهای هم‌مجموعه‌ها باشند. ابتدا یک جدول موسوم به جدول اسلپین به صورت زیر در نظر می‌گیریم

کد واژه‌های C	$v_1 = \mathbf{0}$	v_2	$\cdots$	v_{q^k}
هم‌مجموعه‌های دیگر	$u_1 + v_1$	$u_2 + v_2$	$\cdots$	$u_1 + v_{q^k}$
	$\vdots$	$\vdots$	$\vdots$	$\vdots$
	$u_r + v_1$	$u_r + v_2$	$\cdots$	$u_r + v_{q^k}$
	پیشروها			

اگر واژه‌ی v دریافت شده باشد، آنگاه v را در جدول اسلپین می‌یابیم. اگر مثلاً $v = u_i + v_i$، آنگاه خطای e همان پیشروی هم‌مجموعه‌های نظیر، یعنی u_i است. بنابراین v به صورت $u = v - e = v - u_i = v_i$ کد گشایی می‌شود. کد واژه‌ی u اولین عضو ستون مربوط به v است. هم مجموعه‌ی v را می‌توان با محاسبه‌ی سندرُم ، v که در زیر تعریف می‌کنیم، یافت.

تعریف ۱۱.۲.۱۵. فرض کنید H ماتریس امتحان توازن یک $[n, k]$- کد خطی C باشد. بردار $S(v) = Hv^\top$ را سندرُم v گوییم.

داریم $S(v) = \mathbf{0}$ اگر و تنها اگر $v \in C$. زیرا ، بنا به تعریف ماتریس امتحان توازن، داریم

$$S(v) = \mathbf{0} \iff Hv^\top = \mathbf{0} \iff v \in C.$$

هم‌چنین داریم $S(v) = S(u)$ اگر و تنها اگر $v + C = u + C$. زیرا

$$\begin{aligned} S(v) = S(u) &\iff Hv^\top = Hu^\top \\ &\iff H(v^\top - u^\top) = \mathbf{0} \\ &\iff v - u \in C \\ &\iff v + C = u + C. \end{aligned}$$

بنابراین می‌توان هم‌مجموعه‌ها را با استفاده از سندرُم تعریف کرد. فرض کنید $e = v - u$. که در آن $u \in C$ و $v \in \mathrm{GF}(q)^n$، آنگاه

$$S(v) = S(u + e) = S(u) + S(e) = S(e),$$

یعنی v و e در یک هم‌مجموعه هستند. اکنون می‌توانیم فرمول‌بندی دیگری از قضیه‌ی ۱۰.۲.۱۵، ارئه‌ی کنیم:

قضیه ۱۲.۲.۱۵. (الگوریتم کد گشایی) فرض کنید $v \in \mathrm{GF}(q)^n$ واژه‌ی دریافت شده باشد. $S(v)$ و پیشروی هم‌مجموعه‌ی e با سندرُم $S(v)$ را می‌یابیم. بیشترین امکان برای کد واژه‌ی منتقل شده از کانال عبارت است از $u = v - e$ (یعنی v به صورت $u = v - e$ کد گشایی می‌شود) و داریم $d(u, v) = \min\{d(w, v) \mid w \in C\}$. □

در کدهای خطی بزرگ، یافتن پیشروی هم‌مجموعه‌ها عملاً ممکن نیست. مثلاً یک $[۵۰, ۲۰]$- کد خطی روی $\mathbb{Z}_2$، تقریباً $۱۰^۹$ هم‌مجموعه دارد. بنابراین باید کدهایی ساخته شوند که بیشتر سیستماتیک باشند. در حالت کد دوتایی برای $v = u + e$، که در آن $u \in C$ و $v \in \mathrm{GF}(q)^n$، داریم $S(v) = He^\top$. بنابراین داریم:

قضیه ۱۳.۲.۱۵. در یک کد خطی دوتایی، سندرُم برابر مجموعه‌ی آن ستون‌های ماتریس امتحان توازن است که خطا رخ می‌دهد. □

مثال ۱۴.۲.۱۵. فرض کنید ماتریس امتحان توازن و مولد استاندارد $[۴, ۲]$- کد خطی دوتایی C عبارت باشند از

$$G = \begin{bmatrix} ۱ & ۰ & ۱ & ۱ \\ ۰ & ۱ & ۰ & ۱ \end{bmatrix}, \quad H = \begin{bmatrix} ۱ & ۰ & ۱ & ۰ \\ ۱ & ۱ & ۰ & ۱ \end{bmatrix}.$$

پیام‌ها	۰۰	۱۰	۰۱	۱۱	
کد واژه‌ها	۰۰۰۰	۱۰۱۱	۰۱۰۱	۱۱۱۰	$(۰۰)^\top$
هم‌مجموعه‌های دیگر	۱۰۰۰	۰۰۱۱	۱۱۰۱	۰۱۱۰	$(۱۱)^\top$
	۰۱۱۰	۱۱۱۱	۰۰۰۱	۱۰۱۰	$(۰۱)^\top$
	۰۰۱۰	۱۰۰۱	۰۱۱۱	۱۱۰۰	$(۱۰)^\top$
	پیشروها			سندرُم‌ها	

جدول هم‌مجموعه ها عبارت است از
به عنوان مثال اگر $v = ۱۱۱۱$ دریافت شده باشد، آنگاه $S(v) = Hv^\top = (۰۱)^\top$. بنابراین خطای $e = ۰۱۰۰$ و v به صورت $u = v - e = ۱۰۱۱$ کد گشایی می‌شود و پیام متناظر آن ۱۰ است. □

در ادامه‌ی این بخش چندجمله‌ای شمارش‌گر وزن یک کد و ارتباط آن با شمارش‌گر کد دوگان آن را بررسی می‌کنیم.

تعریف ۱۵.۲.۱۵. فرض کنید a_i، $۰ \le i \le n$، تعداد کد واژه‌های $[n,k]$- خطی C با وزن i باشد، یعنی $a_i = |\{u \in C \mid \mathrm{wt}(u) = i\}|$. چندجمله‌ای

$$W_C(x,y) = \sum_{i=۰}^{n} a_i x^i y^{n-i}$$

در $\mathbb{C}[x,y]$ را شمارش‌گر وزن C گوییم.

توجه کنید $W_C(۱,۰) = ۱$ و $W_C(۱,۱) = |C|$. یکی از قضیه‌ی مهم در نظریه‌ی کد گذاری قضیه‌ی مک‌ویلیامز است، که رابطه‌ی بین یک کد و دوگان آن را مشخص می‌کند. یکی از راه‌های اثبات این قضیه استفاده از سرشت گروه‌ها است. در این جا این قضیه را با استفاده از سرشت گروه‌ها ثابت می‌کنیم. یک همریختی χ از گروه جمعی $\mathrm{GF}(q)$ به گروه ضربی $\mathbb{C}^\times$ را یک سرشت $\mathrm{GF}(q)$ می‌نامیم و $\chi_۰ : \mathrm{GF}(q) \longrightarrow \mathbb{C}^\times$ با ضابطه‌ی $\chi_۰(a) = ۱$ را سرشت بدیهی گوییم.

لم ۱۶.۲.۱۵. (الف) اگر $\chi : \mathrm{GF}(q) \longrightarrow \mathbb{C}^\times$ یک سرشت نابدیهی $\mathrm{GF}(q)$ باشد، آنگاه $\sum_{a\in \mathrm{GF}(q)} \chi(a) = ۰$.
(ب) مجموعه‌ی سرشت‌های $\mathrm{GF}(q)$ تحت عمل ضرب،یک گروه یکریخت با گروه جمعی $\mathrm{GF}(q)$ تشکیل می‌دهند.
(ج) به ازای هر $a, b \in \mathrm{GF}(q)$، که $a \neq -b$ داریم $\sum \chi(a)\chi(b) = ۰$، که در آن χ در مجموعه‌ی همه‌ی سرشت‌های $\mathrm{GF}(q)$ تغییر می‌کند.

اثبات. (الف) چون χ نابدیهی است عضو $b \in \mathrm{GF}(q)$ وجود دارد که $\chi(b) \neq ۱$. آنگاه

$$\begin{aligned}
\chi(b) \sum_{a\in \mathrm{GF}(q)} \chi(a) &= \sum_{a\in \mathrm{GF}(q)} \chi(b)\chi(a) \\
&= \sum_{a\in \mathrm{GF}(q)} \chi(a+b) \\
&= \sum_{a\in \mathrm{GF}(q)} \chi(a).
\end{aligned}$$

بنابراین $\sum_{a\in \mathrm{GF}(q)} \chi(a) = ۰$ و چون $(\chi(b)-۱)\neq ۰$ حکم ثابت است.
(ب) فرض کنید ψ و χ دو سرشت $\mathrm{GF}(q)$ باشند. ضرب نقطه‌وار ψ و χ یک همریختی از $\mathrm{GF}(q)$ به $\mathbb{C}$ و بنابراین سرشت $\mathrm{GF}(q)$ است:

$$\forall a \in \mathrm{GF}(q) \quad (\chi\psi)(a) = \chi(a)\psi(a).$$

به وضوح مجموعه‌ی سرشت‌ها تحت این عمل یک گروه ضربی تشکیل می‌دهند. اگر $q = p^m$، آنگاه گروه جمعی $\mathrm{GF}(q)$ با $\mathbb{Z}_p^m$ یکریخت است. فرض کنید $\alpha : \mathbb{Z}_p^m \longrightarrow \mathrm{GF}(q)$ یکریختی باشد. قرار می‌دهیم $e_i = (۰,\ldots,۰,۱,۰,\ldots ۰) \in \mathbb{Z}_p^m$، که در آن ۱ در iامین مولفه است. سرشت دلخواه $\chi : \mathrm{GF}(q) \longrightarrow \mathbb{C}^\times$ را در نظر می‌گیریم و قرار می‌دهیم $\psi = \chi \circ \alpha$. در این صورت $\psi : \mathbb{Z}_p^m \longrightarrow \mathbb{C}^\times$ همریختی است، چون $\psi(e_i)^p = \psi(pe_i) = \psi(۰) = ۱$. نتیجه می‌گیریم $\psi(e_i)$ یک ریشه‌ی pام واحد است. از طرف دیگر به ازای هر $(a_۱,\ldots,a_n) \in \mathbb{Z}_p^m$ داریم

$$\begin{aligned}\psi(a_۱,\ldots,a_m) &= \psi(a_۱e_۱ + \cdots + a_me_m)\\ &= \psi(e_۱)^{a_۱}\cdots\psi(e_m)^{a_m}\end{aligned}$$

بنابراین اگر ξ یک ریشه‌ی pام اولیه‌ی واحد باشد، تابع $\overline{\psi} : \mathbb{Z}_p^m \longrightarrow \langle\xi\rangle \times \cdots \times \langle\xi\rangle \cong \mathbb{Z}_p^m$ با ضابطه‌ی $\overline{\psi}(a_۱,\ldots,a_m) = (\xi_۱^{a_۱},\ldots,\xi_m^{a_m})$ یک همریختی است، که در آن $\psi(e_i) = \xi_i \in \langle\xi\rangle$. به سادگی می‌توان دید که نگاشت $\chi \mapsto \overline{\psi}$ یک یکریختی از گروه سرشت‌های $\mathrm{GF}(q)$ به $\mathbb{Z}_p^m \cong \mathrm{GF}(q)$ است.
(ج) چون $a+b \neq ۰$، سرشت نابدیهی ψ وجود دارد طوری که

$$\psi(a)\psi(b) = \psi(a+b) \neq ۱.$$

بنابراین

$$\psi(a)\psi(b)\sum_{\chi}\chi(a)\chi(b) = \sum_{\chi}(\psi\chi)(a)(\psi\chi)(b) = \sum_{\chi}\chi(a)\chi(b),$$

و چون $\psi(a)\psi(b) \neq ۱$، حکم ثابت است. □

فرض کنید χ یک سرشت نابدیهی $\mathrm{GF}(q)$ و $u\cdot v$ نشان دهنده‌ی ضرب نقطه‌ای بردارهای $u,v \in \mathrm{GF}(q)^n$ باشد. اگر V فضای برداری روی $\mathbb{C}$ و $f : \mathrm{GF}(q)^n \longrightarrow V$ یک تابع باشد، تابع

$$\begin{aligned}&g_f : \mathrm{GF}(q)^n \longrightarrow V\\ &g_f(u) = \sum_{v\in\mathrm{GF}(q)^n}\chi(v\cdot u)f(v)\end{aligned}$$

را در نظر می‌گیریم و در لم و قضیه‌ی بعدی از آن استفاده می‌کنیم.

لم ۱۷.۲.۱۵. فرض کنید W یک زیرفضای $\mathrm{GF}(q)^n$ و $f : \mathrm{GF}(q)^n \longrightarrow V$ یک تابع باشد، که در آن V یک فضای برداری روی $\mathbb{C}$ است. اگر χ یک سرشت نابدیهی $\mathrm{GF}(q)$ باشد، آنگاه

$$\sum_{u\in W} g_f(u) = |W| \sum_{u\in W^\perp} f(u).$$

اثبات. داریم

$$\begin{aligned}\sum_{u\in W} g_f(u) &= \sum_{u\in W}\sum_{v\in\mathrm{GF}(q)^n}\chi(v\cdot u)f(v)\\ &= \sum_{v\in\mathrm{GF}(q)^n}\sum_{u\in W}\chi(v\cdot u)f(v)\\ &= |W|\sum_{v\in W^\perp} f(v) + \sum_{v\notin W^\perp}\sum_{a\in\mathrm{GF}(q)}\sum_{\substack{u\in W\\ v\cdot u=a}}\chi(a)f(v).\end{aligned}$$

بنا به لم ۱۶.۲.۱۵ (الف)، و این حقیقت که تعداد بردارهای $u \in W$ با $v \cdot u = a$، برای $v \notin W^\perp$، ثابت است داریم

$$\begin{aligned}\sum_{u\in W} g_f(u) &= |W| \sum_{v\in W^\perp} f(v) + \frac{|W|}{q} \sum_{v\notin W^\perp} f(v) \sum_{a\in \mathrm{GF}(q)} \chi(a) \\ &= |W| \sum_{v\in W^\perp} f(v),\end{aligned}$$

و این حکم را ثابت می‌کند. □

فرض کنید $V = \mathbb{C}[x,y]$ فضای برداری چندجمله‌ای‌های دو متغیره بر حسب دو متغیر x و y روی $\mathbb{C}$ باشد و تابع f را با $f(v) = x^{\mathrm{wt}(v)} y^{n-\mathrm{wt}(v)}$، که در آن $\mathrm{wt}(v)$ وزن بردار $v \in \mathrm{GF}(q)^n$ است.

قضیه ۱۸.۲.۱۵. (اتحاد مک ویلیامز) اگر C یک $[n,k]$- کد خطی روی $\mathrm{GF}(q)$ و $C^\perp$ کد دوگان آن باشد، آن‌گاه

$$W_{C^\perp}(x,y) = \frac{1}{q^k} W_C(y-x, y+(q-1)x).$$

اثبات. تابع $f : \mathrm{GF}(q)^n \longrightarrow \mathbb{C}[x,y]$ را به صورت بالا در نظر می‌گیریم. آن‌گاه

$$W_{C^\perp}(x,y) = \sum_{v\in C^\perp} f(v).$$

فرض کنید g_f همانند قبل باشد و برای $a \in \mathrm{GF}(q)$ قرار دهید $|a| = \begin{cases} 1 & a \neq 0 \\ 0 & a = 0 \end{cases}$. به ازای هر $u = (a_1, \ldots, a_n) \in \mathrm{GF}(q)^n$ داریم

$$\begin{aligned} g_f(u) &= \sum_{v\in \mathrm{GF}(q)^n} \chi(v\cdot u) x^{\mathrm{wt}(v)} y^{n-\mathrm{wt}(v)} \\ &= \sum_{b_1,\ldots,b_n \in \mathrm{GF}(q)} \chi(a_1 b_1 + \cdot + a_n b_n) x^{|b_1|+\cdots+|b_n|} y^{(1-|b_1|)+\cdots+(1-|b_n|)} \\ &= \sum_{b_1,\ldots,b_n \in \mathrm{GF}(q)} \prod_{i=1}^{n} \left(\chi(a_i b_i) x^{|b_i|} y^{1-|b_i|} \right) \\ &= \sum_{i=1}^{n} \sum_{b\in \mathrm{GF}(q)} \left(\chi(a_i b) x^{|b|} y^{1-|b|} \right). \end{aligned}$$

برای $a_i = 0$ داریم $\chi(a_i b) = \chi(a) = 1$ و بنابراین عامل متناظر آن $y + (q-1)x$ است. عامل متناظر $a_i \neq 0$ عبارت است از $y + x\sum_{b\in \mathrm{GF}(q)^n} \chi(b) = y - x$. بنابراین

$$g_f(u) = (y-x)^{\mathrm{wt}(u)} (y+(q-1)x)^{n-\mathrm{wt}(u)}$$

بنا به لم قبل داریم

$$\begin{aligned} |C| W_{C^\perp}(x,y) &= |C| \sum_{v\in C^\perp} f(v) \\ &= \sum_{u\in C} g_f(u) \\ &= W_C(y-x, y+(q-1)x). \end{aligned}$$

چون $|C| = q^k$ اتحاد مورد نظر ثابت است. □

اگر قرار دهیم $x = z$ و $y = ۱$ و $W_C(z) = W_C(z, ۱)$، می‌توان اتحاد مک ویلیامز را به صورت زیر نوشت

$$W_{C^\perp}(z) = \frac{۱}{q^k}(۱ + (q - ۱)z)^n W_C\left(\frac{۱ - z}{۱ + (q - ۱)z}\right).$$

مثال ۱۹.۲.۱۵. اگر $C = \{۰۰۰, ۰۱۱, ۱۰۱, ۱۱۰\}$، آنگاه C یک $[۳, ۲]$- کد خطی است و $C^\perp = \{۰۰۰, ۱۱۱\}$. به سادگی می‌توان توزیع وزن کد واژه‌ها را یافت، یعنی $a_۰ = ۱$، $a_۲ = ۳$، $a_۰^\perp = ۱$، $a_۳^\perp = ۱$، ($a_i^\perp$ها توزیع وزن $C^\perp$ هستند). بنابراین

$$W_C(x, y) = y^۳ + ۳x^۲y, \quad W_{C^\perp}(x, y) = y^۳ + x^۳.$$

در این حالت می‌توان اتحاد مک ویلیامز را تحقیق کرد:

$$\begin{aligned}\frac{۱}{q^k}W_C(y - x, y + (q - ۱)x) &= \frac{۱}{۴}((y + x)^۳ + ۳(y - x)^۲(y + x)) \\ &= y^۳ + x^۳ \\ &= W_{C^\perp}(x, y).\end{aligned}$$

مثال ۲۰.۲.۱۵. فرض کنید C، $[n, n - r]$- کد دو تایی همینگ $\mathscr{H}(r, ۲)$ باشد. ماتریس مولد کد $C^\perp$ همان ماتریس امتحان توازن H از کد C است. ستون‌های H مشتمل بر همه‌ی بردارهای ناصفر به طول r روی $\mathbb{Z}_۲$ است. $C^\perp$ مشتمل بر بردار صفر و $n = ۲^r - ۱$ بردار به وزن $۲^{r-۱}$ است. در نتیجه

$$W_{C^\perp}(x, y) = y^n + (۲^r - ۱)x^{۲^{r-۱}}y^{۲^{r-۱}} - ۱$$

بنابراین، بنا به اتحاد مک ویلیامز، شمارشگر وزن برای C عبارت است از (توجه کنید $۲^{r-۱} = \frac{n+۱}{۲}$)

$$\begin{aligned}W_C(x, y) &= \frac{۱}{۲^r}W_{C^\perp}(y - x, y + (۲ - ۱)x) \\ &= \frac{۱}{n + ۱}\left((y - x)^n + n(y - x)^{\frac{n+۱}{۲}}(y + x)^{\frac{n-۱}{۲}}\right).\end{aligned}$$

چون $W(x, ۱) = W(z) = \sum_{i=۰}^n a_i x^i$، به سادگی می‌توان دید $W(z)$ در معادله دیفرانسیل

$$(۱ - z)^۲W' + (۱ + nz)W = (۱ + z)^n \ , \ W(۰) = a_۰ = ۱$$

صدق می‌کند. با حل این معادله به روش سری‌ها می‌توان a_iها را یافت:

$$ia_i = \binom{n}{i - ۱} - a_{i-۱} - (n - i + ۲)a_{i-۲} \ , \ i = ۲, ۳, \ldots, n,$$

که در آن $a_۰ = ۱$ و $a_۱ = ۰$. بنابراین می‌توانیم a_iها را به صورت بازگشتی بیابیم. توجه کنید اتحاد مک ویلیامز را می‌توان به صورت زیر نیز بیان کرد:

$$\sum_{i=۰}^n \binom{n}{i}a_i = q^{k-s}\sum_{i=۰}^n \binom{-۱}{۰}^i \binom{n - i}{n - s}a_i^\perp, \quad ۰ \le s \le n. \qquad \square$$

تمرین‌ها

در صورت لزوم برای انجام محاسبات از GAP استفاده کنید (صفحه‌ی ۳۶۸ را ببینید).

۱. وزن همینگ هر کدام از واژه‌های داده شده را بیابید.
(الف) $\text{۰۱۲۰۱۰۰۱} \in \mathbb{Z}_{۳}^{۸}$ (ب) $\text{۱۰۱۰۰۱۱۰۰۱۱۱۰} \in \mathbb{Z}_{۳}^{۱۳}$
(ج) $\text{۰۱۱۱۱۱۰۰۱۱۰۱} \in \mathbb{Z}_{۲}^{۱۲}$ (د) $\text{۰۰۱۰۱۲۰۲۱۰۱} \in \mathbb{Z}_{۳}^{۱۱}$

۲. فاصله‌ی همینگ دو واژه‌ی داده شده را بیابید.
(الف) ۱۱۰۱۰۱۱۱۰۱۰۱، ۰۱۱۰۰۱۰۱۰۱۱۱
(ب) ۱۲۰۱۰۱۲۰۱۲۰۱، ۱۰۱۰۲۱۰۰۰۱۰۱
(ج) ۱۰۱۱۰۱۱۰۱۱۰۱۱، ۱۱۰۱۱۰۱۱۰۱۱۰۱
(د) ۱۰۱۱۱۰۱۱۱۰۱۱۱۰۱۱، ۰۱۱۰۰۰۱۱۱۰۱۰۰۱۱۰

۳. معین کنید کد خطی داده شده چند خطا را کشف و یا تصحیح می‌کند.
(الف) ۱۱۰۱۱۰، ۱۰۱۰۱۰، ۰۱۱۱۰۰، ۰۰۰۰۰۰.
(ب) ۰۰۰۰۰۰۰، ۰۰۰۰۱۱۱، ۰۱۱۱۰۰۱، ۰۱۱۱۱۱۰، ۱۰۱۰۰۱۱، ۱۰۱۰۱۰۰،
۱۱۰۱۰۱۰، ۱۱۰۱۱۰۱.
(ج) ۰۰۰۰۰۰، ۰۰۰۰۱۰، ۰۰۱۱۰۰، ۰۰۱۱۱۰، ۰۱۰۰۰۱، ۰۱۰۰۱۱، ۰۱۱۱۰۱، ۰۱۱۱۱۱،
۱۰۰۱۰۱، ۱۰۰۱۱۱، ۱۰۱۰۰۱، ۱۰۱۰۱۱، ۱۱۰۱۰۰، ۱۱۰۱۱۰، ۱۱۱۰۰۰، ۱۱۱۰۱۰.

۴. فرض کنید C یک $[n, k]$-کد خطی روی $\mathrm{GF}(q)$ با ماتریس مولد G باشد. اگر G ستونی که همه‌ی درایه‌هایش صفر باشد نداشته باشد، نشان دهید مجموع وزن همه‌ی کدواژه‌های C برابر $n(q-۱)q^{k-۱}$ است.

۵. همه‌ی سندرُم‌ها و پیشروی هم‌مجموعه‌های $[۲, ۵]$- کد دوتایی C که ماتریس مولد آن در تمرین ۲ (ج) از بخش قبل داده شده بیابید.

۶. فرض کنید

$$G = \begin{bmatrix} ۱ & ۰ & ۰ & ۱ & ۱ \\ ۰ & ۱ & ۰ & ۱ & a \\ ۰ & ۰ & ۱ & ۱ & ۱ \end{bmatrix}$$

ماتریس مولد $[۳, ۵]$- کد C روی $\mathrm{GF}(۴)$ باشد، (a عضو اولیه‌ای از $\mathrm{GF}(۴)$). همه‌ی کد واژه‌ها، ماتریس امتحان، و کد دوگان C را بیابید. ثابت کنید این کد ۱- تصحیح کننده‌ی خطا و کامل است.

۷. کد همینگ دوتایی $\mathscr{H}(۳, ۲)$ را در نظر بگیرید. نشان دهید این کد یک $[۴, ۷]$- کد خطی است و واژه‌های ۱۱۱۰۰۱۱، ۱۱۰۱۰۱۱، و ۱۰۰۱۰۱۰ را کد گشایی کنید.

۸. ماتریس امتحان توازن و ماتریس مولد کد همینگ دوتایی $\mathscr{H}(۴, ۲)$ را بنویسید، و واژه‌های ۱۱۱۰۱۱۱۰۰۰۰۰۰۰۰ و ۱۱۰۰۱۱۰۰۱۱۰۰۱۱۱ را کد گشایی کنید.

۹. آیا $[۱۲, ۷, ۵]$- کد خطی دوتایی وجود دارد ؟

۱۰. نشان دهید هر $[۲۳, ۱۲, ۷]$- کد خطی دوتایی، کامل است.

۱۱. نشان دهید هر $[۱۱, ۶, ۵]$- کد خطی روی $\mathbb{Z}_۳$، کامل است.

۱۲. فرض کنید C یک $[۵, ۳]$- کد خطی روی $\mathbb{Z}_۲$ با ماتریس مولد

$$G = \begin{bmatrix} ۱ & ۱ & ۱ & ۰ & ۰ \\ ۰ & ۰ & ۱ & ۱ & ۰ \\ ۱ & ۱ & ۱ & ۱ & ۱ \end{bmatrix}$$

باشد. کد دوگان C و شمارش‌گرهای وزن برای C و $C^{\perp}$ را بیابید.

۱۳. فرض کنید ماتریس کد خطی C به طول ۵ روی $\mathbb{Z}_۲$ برابر

$$G = \begin{bmatrix} ۰ & ۱ & ۰ & ۰ & ۱ \\ ۰ & ۰ & ۱ & ۰ & ۱ \\ ۱ & ۰ & ۱ & ۱ & ۱ \end{bmatrix}$$

باشد. فاصله‌ی می‌نیمم C، ماتریس امتحان توازن و همه‌ی کد واژه‌های C را بیابید. هم مجموعه‌های $C^{\perp}$ در $\mathbb{Z}_۲^۵$، پیشروی هم مجموعه‌ها، سندرُم‌ها را بیابید و واژه‌ی $u = ۰۱۰۰۱$ را کد گشایی کنید.

۱۴. فرض کنید C کد دوتایی کامل به طول n با فاصله‌ی می‌نیمم ۷ باشد. نشان دهید $n = ۷$ یا $n = ۲۳$.

۱۵. فرض کنید C کد دوتایی با ماتریس مولد

$$G = \begin{bmatrix} ۱ & ۰ & ۰ & ۰ & ۱ & ۰ & ۱ \\ ۰ & ۱ & ۰ & ۰ & ۱ & ۰ & ۱ \\ ۰ & ۰ & ۱ & ۰ & ۰ & ۱ & ۱ \\ ۰ & ۰ & ۰ & ۱ & ۰ & ۱ & ۱ \end{bmatrix}$$

باشد. واژه‌های ۱۱۰۱۰۱۱، ۰۱۱۰۱۱۱، و ۰۱۱۱۰۰۰ را کد گشایی کنید.

۱۶. اگر C یک $[n, k]$- کد خطی روی $\mathrm{GF}(q)$ با $d_{\min} \geq ۲s + ۱$ باشد. نشان دهید

$$|\{u \in \mathrm{GF}(q)^n \mid d(u, v) \leq s\}| \leq q^{n-k}.$$

۱۷. توزیع وزن $[۸, ۴]$- کد همینگ تعمیم یافته را بیابید.

۱۸. اتحاد مک ویلیامز را برای کدهای داده شده بررسی کنید.
(الف) کد خود- دوگان $\{۰۰, ۱۱\}$ (ب) $[۷, ۴]$-کد همینگ.

۱۹. واژه‌های ۰۱۱۰ و ۱۰۱۱ را با $[۷, ۴]$- کد همینگ $[۸, ۴]$-کد همینگ تعمیم یافته کد گذاری کنید. پیام ۱۱۰۰۱۰۱ را با $[۸, ۴]$-کد همینگ کد گشایی کنید.

۲۰. فرض کنید $A(z)$ شمارش‌گر وزن کد دوتایی C باشد. شمارش‌گر وزن کد تعمیم یافته $\overline{C}$ چیست؟

۲۱. شمارش‌گر وزن کد دوگان کد همینگ تعمیم یافته به طول ۲^k چیست؟

۲۲. شعاع پوششی برای یک کد C به طول n روی $\mathrm{GF}(q)$ عبارت است کوچک‌ترین عدد r که r- کره‌های به مرکز کد واژه‌های r همه‌ی فضای برداری $\mathrm{GF}(q)^n$ را بپوشاند. نشان دهید شعاع پوششی برابر وزن پیشروی هم‌مجموعه با بزرگ‌ترین وزن است.

۲۳. فرض کنید ماتریس مولد $[۱۰, ۵]$-کد دوتایی

$$G = \begin{bmatrix} ۱ & ۰ & ۰ & ۰ & ۰ & ۰ & ۰ & ۰ & ۱ & ۱ \\ ۰ & ۱ & ۰ & ۰ & ۰ & ۰ & ۱ & ۱ & ۰ & ۰ \\ ۰ & ۰ & ۱ & ۰ & ۰ & ۱ & ۰ & ۱ & ۰ & ۰ \\ ۰ & ۰ & ۰ & ۱ & ۰ & ۱ & ۱ & ۰ & ۰ & ۰ \\ ۰ & ۰ & ۰ & ۰ & ۱ & ۱ & ۱ & ۱ & ۰ & ۰ \end{bmatrix}$$

باشد. نشان دهید C کد گشاینده‌ی یکتاست، یعنی به ازای هر واژه‌ی دریافت شده‌ی u، کد یکتای v وجود دارد که $d(u, v)$ ماکسیمال است.

۲۴. ماتریس امتحان توازن و مولد کد همینگ روی $\mathbb{Z}_۳$ به طول ۳۱ را بیابید و واژه‌ی ۰۱۱۰۱۰۰۰۰۰۰۱۱ را کد گشایی کنید.

۳.۱۵ چند برنامه‌ی مفید به چند GAP

در این بخش چند برنامه به زبان GAP که برای انجام برخی محاسبات مفید هستند را ارائه می‌کنیم. یک برنامه‌ی مفید یافتن صورت استاندارد ماتریس مولد یک کد است. الگوریتم این برنامه همان روش حذفی گاوس است: فرض کنید G ماتریس $k \times n$، یک کد خطی باشد. به ازای هر $i = ۱, ۲, \ldots, k$ درایه‌ی (i, i) را در نظر می‌گیریم. اگر این درایه صفر باشد، جای سطر iام را با اولین سطر ناصفر پس از سطر iام عوض می‌کنیم (در صورتی که چنین سطری وجود نداشته باشد سطرهای ماتریس مستقل خطی نیستند و بنابراین صورت استاندارد وجود ندارد). اکنون مضرب مناسبی از سطر iام را به سطر jام، $j \neq i$ ، $۱ \leq j \leq k$، اضافه می‌کنیم تا درایه‌ی (j, i)ام صفر شود. برنامه‌ی $\mathrm{gs(G)}$ این الگوریتم را انجام می‌دهد:

```
gs:=function(G)
    local i,j,t,M,k,temp,zero;
    M:=G;  zero:=M[1][1]*0;  k:=Size(M);
    for i in [1..k] do
        if M[i][i]=zero then
            t:=i+1;
            while t<=k and M[t][i]=zero do
                t:=t+1;
            od;
            if t<=k then temp:=M[i];  M[i]:=M[t];  M[t]:=temp;
                    else return "has not standard form";
            fi;
        fi;
        M[i]:=M[i]/M[i][i];
        for j in [1..k] do
            if j <> i then
                M[j]:=-M[j][i]*M[i]+M[j];
            fi;
        od;
    od;
  return M;
end;;
```

مثلاً ماتریس مولد استاندارد کد خطی C روی $\mathbb{Z}_۲$ با ماتریس مولد G داده شده در زیر می‌یابیم:

```
gap>G:=[[0,1,0,0,1],[0,0,1,0,1],[1,0,1,1,1]];  Display(G);
 [ [ 0, 1, 0, 0, 1 ],
  [ 0, 0, 1, 0, 1 ],
  [ 1, 0, 1, 1, 1 ] ]
gap>G:=gs(G);
 [ [ 1, 0, 0, 1, 0 ], [ 0, 1, 0, 0, 1 ], [ 0, 0, 1, 0, 1 ] ]
gap>Display(G);
 [ [ 1, 0, 0, 1, 0 ],
  [ 0, 1, 0, 0, 1 ],
  [ 0, 0, 1, 0, 1 ] ]
```

به عنوان مثال دیگر ماتریس مولد استاندارد کد خطی C روی $\mathbb{Z}_۳$ با ماتریس مولد G داده شده در زیر می‌یابیم:

```
gap>G:=[[0,2,1,1,0,0],[1,1,2,0,2,0],[2,1,0,1,1,1]];
[ [ 0, 2, 1, 1, 0, 0 ], [ 1, 1, 2, 0, 2, 0 ], [ 2, 1, 0, 1, 1, 1 ] ]
gap>gs(G*Z(3));
[ [ Z(3)^0, 0*Z(3), 0*Z(3), Z(3)^0, Z(3), 0*Z(3) ],
  [ 0*Z(3), Z(3)^0, 0*Z(3), Z(3), 0*Z(3), Z(3)^0 ],
  [ 0*Z(3), 0*Z(3), Z(3)^0, 0*Z(3), 0*Z(3), Z(3)^0 ] ]
gap>Display(gs(G*Z(3)));
 1  .  .  1  2  .
 .  1  .  2  .  1
 .  .  1  .  .  1
```

یافتن ماتریس امتحان توازن یک کد با استفاده از ماتریس مولد استاندارد نیز مساله‌ای مهم است که برنامه‌ی $\mathrm{gen2par(G)}$ این کار را انجام می‌دهد:

```
gen2par:=function(G)
    local k,n,i,H,A,I,one,zero,s;
    s:=function(x)
        if x=one then return 1; fi;
        if x=zero then return 0; fi;
      return x;
    end;;
    k:=Size(G);  A:=[];  H:=[];
    one:=G[1][1]^0;  zero:=G[1][1]*0;  n:=Size(G[1]);
    for i in [1..k] do
        Append(A,[G[i][k+1..n]]);
    od;
    I:=IdentityMat(n-k)*one;  A:=-TransposedMat(A);
    for i in [1..n-k] do
        H[i]:=List(Flat([A[i],I[i]]),x->s(x));
    od;
  return H;
end;;
```

ماتریس امتحان توازن کد خطی C که در بالا تعریف شد عبارت است از

```
gap>H:=gen2par(G*Z(2));;  Display(H);
[ [ 1, 0, 0, 1, 0 ],
  [ 0, 1, 1, 0, 1 ] ]
```

با استفاده از برنامه‌ی $\mathrm{codewords}(G,F)$ می‌توان همه‌ی کدواژه‌های M وجود در کد خطی با ماتریس مولد G روی میدان F یافت:

```
codewords:=function(G,F)
    local u,k,res,s;
    s:=function(x)
        if x=One(F) then return 1; fi;
        if x=Zero(F) then return 0; fi;
      return x;
```

```
    end;;
    k:=Size(G);  res:=[];
    for u in F^k do
        Add(res,List(u*G,x-> s(x)));
    od;
  return res;
end;;
```

کد واژه‌های کد خطی C (که در بالا تعریف شده) عبارت‌اند از

```
gap> codewords(G*Z(2),GF(2));
[ [ 0, 0, 0, 0, 0 ], [ 0, 0, 1, 0, 1 ], [ 0, 1, 0, 0, 1 ], [ 0, 1, 1, 0, 0 ],
  [ 1, 0, 0, 1, 0 ], [ 1, 0, 1, 1, 1 ], [ 1, 1, 0, 1, 1 ], [ 1, 1, 1, 1, 0 ] ]
```

با استفاده از برنامه‌ی $\mathrm{cosets}(G,F)$ می‌توان همه‌ی هم‌مجموعه‌ها و پیشروهای هم‌مجموعه‌ها را یافت. ابتدا به برنامه‌ی $\mathrm{minwt}(L)$ نیاز داریم که از کد واژه‌های موجود در لیست L کد واژه‌ای با وزن می‌نیمم را به دست می‌دهد:

```
minwt:=function(L)
    local zero,a,i,m;  zero:=L[1][1]*0;  a:=[];
    for i in [1..Size(L)] do
        a[i]:=Number(L[i],x-> x<>zero);
    od;
    m:=Minimum(a);  i:=Position(a,m);
    return L[i];
end;;
```

برنامه‌ی $\mathrm{cosets}(G,F)$ ماتریس مولد G از کد خطی روی میدان F را گرفته و مجموعه‌ی هم مجموعه‌های کد را محاسبه می‌کند. توجه کنید اولین عضو یک هم‌مجموعه پیشروی آن است:

```
cosets:=function(G,F)
    local vecs,i,k,C,V,n,res,v,s,co,temp;
    s:=function(x)
        if x=One(F) then return 1; fi;
        if x=Zero(F) then return 0; fi;
      return x;
    end;;
    k:=Size(G);  vecs:=[];
    n:=Size(G[1]);  res:=[];
    for i in [1..k] do
        Add(vecs,G[i]);
    od;
    C:=VectorSpace(F,vecs);  V:=F^n;
    res:=List(V,x-> List(C,y-> List(y+x,t-> s(t))));
    res:=List(res,x-> Set(x));  res:=Set(res);
    for co in res do
        i:=Position(co,minwt(co));
        temp:=co[i];  co[i]:=co[1];  co[1]:=temp;
```

```
    od;
  return res;
end;;
```

هم‌مجموعه‌ها و پیشروهای کد خطی C عبارت‌اند از

```
gap>cosets(G*Z(2),GF(2));
[ [ [ 0, 0, 0, 0, 0 ], [ 0, 0, 1, 0, 1 ], [ 0, 1, 0, 0, 1 ], [ 0, 1, 1, 0, 0 ],
  [ 1, 0, 0, 1, 0 ], [ 1, 0, 1, 1, 1 ], [ 1, 1, 0, 1, 1 ], [ 1, 1, 1, 1, 0 ] ],
[ [ 0, 0, 0, 0, 1 ], [ 0, 0, 1, 0, 0 ], [ 0, 1, 0, 0, 0 ], [ 0, 1, 1, 0, 1 ],
[ 1, 0, 0, 1, 1 ], [ 1, 0, 1, 1, 0 ], [ 1, 1, 0, 1, 0 ], [ 1, 1, 1, 1, 1 ] ],
[ [ 0, 0, 0, 1, 0 ], [ 0, 0, 1, 1, 1 ], [ 0, 1, 0, 1, 1 ], [ 0, 1, 1, 1, 0 ],
[ 1, 0, 0, 0, 0 ], [ 1, 0, 1, 0, 1 ], [ 1, 1, 0, 0, 1 ], [ 1, 1, 1, 0, 0 ] ],
[ [ 0, 0, 0, 1, 1 ], [ 0, 0, 1, 1, 0 ], [ 0, 1, 0, 1, 0 ], [ 0, 1, 1, 1, 1 ],
[ 1, 0, 0, 0, 1 ], [ 1, 0, 1, 0, 0 ], [ 1, 1, 0, 0, 0 ], [ 1, 1, 1, 0, 1 ] ] ]
```

برنامه‌ی $\mathrm{synd}(G,F)$ همه‌ی سندرُم‌های کد خطی با ماتریس مولد G روی میدان F، را به دست می‌دهد:

```
synd:=function(G,F)
    local H,ccs,res,co,sy,s;
    s:=function(x)
        if x=One(F) then return 1; fi;
        if x=Zero(F) then return 0; fi;
      return x;
    end;;
    H:=gen2par(G);  res:=[];  ccs:=cosets(G,F);
    for co in ccs do
        sy:=H*co[1]*One(F);
        Add(res,List(sy,x-> s(x)));
    od;
  return res;
end;;
```

سندرُم کد خطی C متناظر با هم‌مجموعه‌هایی که در بالا به دست آمدند را می‌یابیم:

```
gap>synd(G*Z(2),GF(2));
[ [ 0, 0 ], [ 0, 1 ], [ 1, 0 ], [ 1, 1 ] ]
```

۴.۱۵ کدهای دوری

کدهای دوری از کدهای مهم هستند. این کدها الگوریتم‌های نسبتاً ساده‌ی کد گذاری و کد گشایی دارند و به سادگی قابل به کارگیری هستند. به علاوه، کدهای دوری خواص جبری مهمی دارند. بسیاری از کدهای خطی، دوری هستند. کد خطی C به طول n را دوری گوییم، هرگاه از $(a_0,a_1,\ldots,a_{n-1})\in C$ نتیجه شود $(a_{n-1},a_0,\ldots,a_{n-2})\in C$. شیفت دوری $(a_0,a_1,\ldots,a_{n-1})$ را برابر $(a_{n-1},a_0,\ldots,a_{n-2})$ تعریف می‌کنیم، بنابراین کد C دوری است، هرگاه شیفت دوری هر کد واژه مجدداً کد واژه باشد.

مثال ۱.۴.۱۵. کدهای $\{000\}$ و $\{111\}$ و $\{101, 011, 110, 000\}$ دوری هستند. □

مثال ۲.۴.۱۵. مجموعه‌ی همه‌ی واژه‌های در $\mathbb{Z}_2^n$ با توازن زوج (تعداد زوج ۱) یک کد دوری با مرتبه‌ی 2^{n-1} است. مثلاً برای $n=4$،

این کد برابر است با

$$C = \{۰۰۰۰, ۱۱۰۰, ۰۱۱۰, ۰۰۱۱, ۱۰۱۰, ۰۱۰۱, ۱۰۰۱, ۱۱۱۱\}. \qquad \square$$

یکی از ابزارهای بسیار مهم در توصیف کدهای دوری یکریختی بین $\mathrm{GF}(q)^n$ و حلقه‌ی خارج قسمتی $\mathrm{GF}(q)[x]/(x^n - ۱)$ است. یادآوری می‌کنیم که حلقه‌ی خارج قسمتی $V_n = \mathrm{GF}(q)[x]/(x^n - ۱)$ را می‌توان به صورت

$$V_n = \{a_۰ + a_۱t + \cdots + a_{n-۱}t^{n-۱} \mid a_i \in \mathrm{GF}(q), \quad t^n = ۱\}$$

توصیف کرد (بخش ۴ از فصل ۱۱ را ببینید). عمل جمع و ضرب در V_n شبیه چندجمله‌ای‌ها است جز این که $t^n = ۱$. در واقع نگاشت $\pi : \mathrm{GF}(q)[x] \longrightarrow V_n$ با ضابطه‌ی $\pi(f(x)) = f(t)$ یک همریختی حلقه‌ای پوشا با $\pi(x) = t$ و $\ker \pi = (x^n - ۱)$ است. به علاوه $\{۱, t, \ldots, t^{n-۱}\}$ پایه‌ای برای فضای برداری V_n روی میدان $\mathrm{GF}(q)$ است. بنابراین گروه‌های جمعی V_n و $\mathrm{GF}(q)^n$ تحت تناظر

$$a_۰ + a_۱t + \cdots + a_{n-۱}t^{n-۱} \longleftrightarrow a_۰a_۱ \cdots a_{n-۱}$$

یکریخت هستند. دو عبارت فوق را یکی می‌گیریم و غالباً به جای کد واژه‌ی u از $u(t)$ استفاده می‌کنیم. با این تعبیر یک کد خطی را به عنوان زیرمجموعه‌ی از V_n در نظر می‌گیریم. بنابراین کدهای خطی به طول n را به عنوان زیرمجموعه‌ی از $\mathrm{GF}(q)^n$ یا V_n در نظر می‌گیریم. نمایش یک واژه را در حالت اول صورت واژه‌ای و در حالت دوم صورت چندجمله‌ای گوییم. در برخی حالت‌ها استفاده از صورت چندجمله‌ای یک کد برای اثبات قضایا بهتر است. اکنون یک توصیف جالب از کدهای دوری ثابت می‌کنیم:

قضیه ۳.۴.۱۵. کد $C \subseteq V_n$ دوری است اگر و تنها اگر C یک ایدآل V_n باشد.

اثبات. فرض کنید $f(t) = a_۰ + a_۱t + \cdots + a_{n-۱}t^{n-۱}$ عضوی از C باشد. شیفت دوری $f(t)$ (با استفاده از عمل ضرب در V_n و این که $t^n = ۱$) عبارت است از

$$a_{n-۱} + a_۰t + a_۱t^۲ + \cdots + a_{n-۲}t^{n-۱} = tf(t).$$

بنابراین C دوری است اگر و تنها اگر $tC \subseteq C$، که در آن $tC = \{tf(t) \mid f(t) \in C\}$. حال اگر $tC \subseteq C$، آنگاه به ازای هر i، $t^iC \subseteq C$. چون C خطی است، به ازای هر $g(t) \in C$، $g(t)C \subseteq C$، پس C یک ایدآل V_n است.
برعکس اگر C ایدآل V_n باشد، آنگاه $tC \subseteq C$. بنابراین C دوری است. $\square$

چون ایدآل‌های V_n به راحتی توصیف می‌شوند، می‌توان همه‌ی کدهای دوری در V_n را یافت. بنابراین قضیه‌ی فوق از این حیث قضیه‌ای جالب است. اکنون ایدآل‌های V_n را توصیف می‌کنیم. فرض کنید C یک ایدآل V_n باشد. همریختی طبیعی $\pi : \mathrm{GF}(q)[x] \longrightarrow V_n$ با $\pi(f(x)) = f(t)$ را در نظر می‌گیریم. می‌دانیم $\ker \pi = (x^n - ۱)$. در این صورت

$$I = \pi^{-۱}(C) = \{f(x) \in \mathrm{GF}(q)[x] \mid f(t) \in C\}$$

یک ایدآل $\mathrm{GF}(q)[x]$ است و $\ker \pi \subseteq I$. چون $\mathrm{GF}(q)[x]$ دامنه‌ی ایدآل اصلی است، چندجمله‌ای تکین یکتای $g(x) \in \mathrm{GF}(q)[x]$ با کم‌ترین درجه وجود دارد که

$$I = (g(x)) = \{q(x)g(x) \mid q(x) \in \mathrm{GF}(q)[x]\}.$$

به علاوه $\ker \pi \subseteq I$، یعنی $(x^n - ۱) \subseteq (g(x))$. بنابراین $g(x)$ در $\mathrm{GF}(q)[x]$، $x^n - ۱$ را عاد می‌کند و

$$C = \pi(I) = (g(t)) = \{q(t)g(t) \mid q(t) \in V_n\},$$

که در آن $g(x) \in \mathrm{GF}(q)[x]$ چندجمله‌ای تکین با کوچک‌ترین درجه است که $g(t) \in C$. یکتا مولد تکین C با کوچک‌ترین درجه را مولد می‌نیمال C گوییم.

مثال ۴.۴.۱۵. فرض کنید عناصر $\mathbb{Z}_2^3$ مجموعه‌ی پیام‌ها باشند و $g(t) = 1 + t^3$ را چندجمله‌ای مولد کد دوری C در نظر بگیرید. توجه کنید $x^6 - 1 = (1 + x^3)^2$ و C یک $[6, 3]$- کد خطی دوتایی دوری است. در این صورت عناصر C، که عناصر ایدآل تولید شده توسط $1 + t^3$ در $\{t^6 = 1 \mid a_i \in \mathbb{Z}_2,\ V_6 = \{a_0 + a_1 t + \cdots + a_5 t^5$ هستند ، عبارت‌اند از: (یعنی، همه‌ی پیام‌ها به صورت زیر کد گذاری می‌شوند)

$$\begin{aligned}(1 + t^3) \ = \ \{&0, t^2 + t^5, t + t^4, t + t^2 + t^4 + t^5, 1 + t^3, 1 + t^2 + t^3 + t^5,\\ &1 + t + t^3 + t^4, 1 + t + t^2 + t^3 + t^4 + t^5\}.\end{aligned}$$

مثلاً چندجمله‌ای متناظر پیام ۰۱۱ عبارت است از $t + t^2$ و با ضرب آن در $1 + t^3$ داریم $(t + t^2)(1 + t^3) = t + t^2 + t^4 + t^5$، که کد واژه‌ای متناظر آن عبارت است از ۰۱۱۱۰۱۱. به همین صورت داریم

$$\begin{array}{llll} 000 \mapsto 00000 & 001 \mapsto 001001 & 010 \mapsto 010010 & 110 \mapsto 100100\\ 101 \mapsto 101101 & 110 \mapsto 110110 & 011 \mapsto 011011 & 111 \mapsto 111111. \end{array}$$

ماتریس مولد این کد عبارت است از

$$\begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 0\\ 0 & 1 & 0 & 0 & 1 & 0\\ 0 & 0 & 1 & 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} g(t)\\ tg(t)\\ t^2 g(t) \end{bmatrix}. \qquad \square$$

اکنون ثابت می‌کنیم کدهای همینگ دوتایی و برخی دیگر از کدهای همینگ (معادل با) کدهای دوری هستند.

قضیه ۵.۴.۱۵. فرض کنید $n = \dfrac{q^m - 1}{q - 1}$ و β یک ریشه‌ی اولیه‌ی nام واحد در $\mathrm{GF}(q^m)$ باشد. اگر $\gcd\{m, q - 1\} = 1$، آنگاه کد دوری C با مولد $g(x) = \prod_{j=0}^{m-1}(x - \beta^{q^j})$ (که چندجمله‌ای می‌نیمال β است) و $[n, n - m]$- کد همینگ $\mathscr{H}(m, q)$ روی $\mathrm{GF}(q)$ معادل هستند.

اثبات. چون

$$\begin{aligned} n \ &= \ q^{m-1} + q^{m-2} + \cdots + q + 1\\ &= \ (q - 1)\left(q^{m-2} + 2q^{m-3} + 3q^{m-2} + \cdots + (m - 2)q + m - 1\right) + m, \end{aligned}$$

داریم $\gcd\{n, q - 1\} = \gcd\{m, q - 1\} = 1$. بنابراین $\beta^{i(q-1)} \neq 1$، برای $i = 1, 2, \ldots, n - 1$، یعنی $\beta^i \notin \mathrm{GF}(q)$، برای $i = 1, 2, \ldots, n - 1$. از این رو ستون‌های ماتریس H که متشکل از نمایش 1، β، β^2، ...، β^{m-1} به عنوان بردارهای در $\mathrm{GF}(q)^m$ هستند، دوبه‌دو روی $\mathrm{GF}(q)$ مستقل خطی هستند. بنابراین H ماتریس امتحان توازن یک $[n, n - m]$- کد همینگ است. $\square$

قضیه ۶.۴.۱۵. فرض کنید C یک کد خطی دوری به طول n با مولد $g(t)$ باشد. اگر $\deg g(x) = m$ و $k = n - m$، آنگاه

$$X = \{g(t), tg(t), \ldots, t^{k-1} g(t)\}$$

پایه‌ای برای C روی $\mathrm{GF}(q)$ است، به ویژه $|C| = q^k$ و C یک $[n, k]$- کد است.

اثبات. چون $g(x)$ شمارنده‌ای از $x^n - 1$ است، چندجمله‌ای $h(x) \in \mathrm{GF}(q)[x]$ وجود دارد که $x^n - 1 = h(x)g(x)$. بنابراین $\deg h(x) = n - m = k$. عضو دلخواه $f(t)$ در $C = (g(t))$ را در نظر می‌گیریم، پس $f(t) = q(t)g(t)$، که در آن

$q(x) \in \mathrm{GF}(q)[x]$. بنا به الگوریتم تقسیم $p(x), r(x) \in \mathrm{GF}(q)[x]$ وجود دارند که $q(x) = p(x)h(x) + r(x)$، که در آن $r(x) = ۰$ یا $\deg r(x) < k$. بنابراین

$$\begin{aligned} f(t) &= q(t)g(t) \\ &= (p(t)h(t) + r(t))g(t) \\ &= p(t)h(t)g(t) + r(t)g(t) \\ &= p(t)(۱ - t^n) + r(t)g(t) \\ &= r(t)g(t). \end{aligned}$$

قرار می‌دهیم $r(x) = a_۰ + a_۱x + \cdots + a_{k-۱}x^{k-۱}$، بنابراین

$$f(t) = r(t)g(t) = a_۰g(t) + a_۱tg(t) + \cdots + a_{k-۱}t^{k-۱}g(t).$$

از این رو X فضای C را تولید می‌کند. حال نشان می‌دهیم X مستقل خطی است. فرض کنید $a_i \in \mathrm{GF}(q)$ و

$$a_۰g(t) + a_۱tg(t) + \cdots + a_{k-۱}t^{k-۱}g(t) = ۰.$$

قرار می‌دهیم $f(x) = a_۰ + a_۱x + \cdots + a_{k-۱}x^{k-۱}$. اگر $f(x) \neq ۰$، آن‌گاه داریم $f(t)g(t) = ۰$. بنابراین $f(x)g(x) \in (۱ - x^n)$ و $f(x)g(x) = q(x)(۱ - x^n)$. چون $۱ - x^n = h(x)g(x)$، نتیجه می‌گیریم $f(x) = q(x)h(x)$، که این تناقض است، زیرا $k = \deg h(x) \leq \deg f(x) \leq k - ۱$. پس $f(x) = ۰$ و $a_۰ = \cdots = a_{k-۱} = ۰$. از این رو X مستقل خطی نیز هست. □

فرض کنید $g(t) = a_۰ + a_۱t + \cdots + a_mt^m$ چندجمله‌ای مولد کد خطی دوری C به طول n باشد و $k = n - m$. طبق قضیه‌ی فوق $\{g(t), tg(t), \ldots, t^{k-۱}g(t)\}$ پایه‌ای برای C روی $\mathrm{GF}(q)$ است، بنابراین یک ماتریس مولد C عبارت است از

$$\begin{bmatrix} a_۰ & a_۱ & a_۲ & \cdots & a_m & ۰ & \cdots & ۰ \\ ۰ & a_۰ & a_۱ & \cdots & a_{m-۱} & a_m & \cdots & ۰ \\ \vdots & \vdots & \ddots & \ddots & \vdots & \vdots & \ddots & \vdots \\ ۰ & \cdots & ۰ & \cdots & a_۰ & \cdots & \cdots & a_m \end{bmatrix} = \begin{bmatrix} g(t) \\ tg(t) \\ \vdots \\ t^{k-۱}g(t) \end{bmatrix}.$$

اکنون فرض کنید $۱ - x^n = g(x)h(x)$ و $h(x) = b_۰ + b_۱x + \cdots + b_kx^k$. چندجمله‌ای $h(x)$ را چندجمله‌ای امتحان کد دوری $C \subseteq V_n$ گوییم. فرض کنید $f(t) \in C$، در این صورت $f(t) = q(t)g(t)$، که در آن $q(x) \in \mathrm{GF}(q)[x]$. داریم

$$f(t)h(t) = q(t)g(t)h(t) = q(t)(۱ - t^n) = ۰.$$

اکنون برعکس اگر چندجمله‌ای $f(x) \in \mathrm{GF}(q)[x]$ وجود داشته باشد که $f(t)h(t) = ۰$، نشان می‌دهیم $f(t) \in C$. چون $f(t)h(t) = ۰$ داریم $f(x)h(x) \in (۱ - x^n)$، و بنابراین $f(x)h(x) = q(x)(۱ - x^n)$. از این رو $f(x)h(x) = p(x)g(x)h(x)$ و $f(x) = p(x)g(x)$. پس $f(t) = p(t)g(t)$ و $f(t) \in C$. بنابراین ثابت کردیم

$$f(t) \in C \iff f(t)h(t) = ۰.$$

قرار می‌دهیم $f(x) = c_۰ + c_۱x + \cdots + c_{n-۱}x^{n-۱}$، آن‌گاه

$$\begin{aligned} &c_۰b_k + c_۱b_{k-۱} + \cdots + c_kb_۰ = ۰ \\ &c_۱b_k + c_۲b_{k-۱} + \cdots + c_{k+۱}b_۰ = ۰ \\ &\vdots \qquad\qquad\qquad \vdots \\ &c_{m-۱}b_k + c_mb_{k-۱} + \cdots + c_{n-۱}b_۰ = ۰ \end{aligned}$$

بنابراین ضرایب t^i در $f(t)h(t)$ عبارت است از

$$c_ib_k + c_{i+1}b_{k-1} + \cdots + c_{i+k}b_0 = 0, \quad i = 0, 1, \ldots, m-1,$$

که در آن اندیس‌ها به پیمانه‌ی n محاسبه می‌شوند (چون $t^n = 1$). بنابراین می‌بینیم که

$$f(t) \in C \iff Hf(t)^\top = 0.$$

که در آن

$$H = \begin{bmatrix} b_k & \cdots & b_0 & 0 & 0 & \cdots & 0 \\ 0 & b_k & \cdots & b_0 & 0 & 0 & 0 \\ 0 & 0 & b_k & \cdots & b_0 & 0 & \vdots \\ \vdots & \vdots & \ddots & \ddots & \cdots & \ddots & 0 \\ 0 & \cdots & 0 & 0 & b_k & \cdots & b_0 \end{bmatrix}.$$

پس H ماتریس امتحان توازن کد C با مولد $g(t)$ است. نشان می‌دهیم $C^\perp$ یک $[n, n-k]$- کد دوری با چندجمله‌ای مولد

$$h^\perp(t) = t^k h(t^{-1}) = b_0t^k + b_1t^{k-1} + \cdots + b_{k-1}t + b_k$$

است. اگر نشان دهیم $h^\perp(x)|x^n - 1$، آنگاه نتیجه می‌شود که $h^\perp(x)$ یک چندجمله‌ای مولد برای کد دوری $(h^\perp(t))$ با ماتریس مولد H است؛ بنابراین $(h^\perp(t)) = C^\perp$. داریم $h(x)g(x) = x^n - 1$. پس $h(x^{-1})g(x^{-1}) = x^{-n} - 1$ که نتیجه می‌دهد $x^k h(x^{-1})x^m g(x^{-1}) = 1 - x^n$، یعنی $h^\perp(x)|x^n - 1$. بنابراین $C^\perp = (h(t)^\perp)$. توجه کنید $C^\perp$ توسط $h(x)$ تولید نمی‌شود.

مثال ۷.۴.۱۵. تجزیه‌ی $x^7 - 1 = (x+1)(1+x^2+x^3)(1+x+x^3)$ به عوامل تحویل‌ناپذیر روی $\mathbb{Z}_2$ را در نظر بگیرید. قرار می‌دهیم $g(x) = 1 + x + x^3$ و $h(x) = \dfrac{x^7 - 1}{g(x)} = 1 + x + x^2 + x^4$. آنگاه ماتریس مولد کد دوری C تولید شده توسط $g(t)$ عبارت است از

$$G = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix} = \begin{bmatrix} g(t) \\ tg(t) \\ t^2g(t) \\ t^3g(t) \end{bmatrix}.$$

ماتریس امتحان این کد عبارت است از

$$K = \begin{bmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \end{bmatrix}.$$

که ماتریس مولد کد دوری تولید شده توسط $h(x) = 1 + x + x^2 + x^4$ است. اکنون ماتریس مولد کد دوگان را می‌یابیم. داریم $h^\perp(x) = x^4h(x^{-1}) = x^4 + x^3 + x^2 + 1$. بنابراین $h^\perp(x)$ چندجمله‌ای مولد کد $C^\perp$ با ماتریس مولد K است:

$$H = \begin{bmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix} \qquad \square$$

اگر a عضو اولیه‌ای از $\mathrm{GF}(q)$ باشد، آنگاه $\mathrm{GF}(q) = \{0, 1, a, a^2, \ldots, a^{q-1}\}$. به علاوه $\{1, a, a^2, \ldots, a^{q-1}\}$ پایه‌ای برای $\mathrm{GF}(q)$ روی $\mathbb{Z}_p$ است، که در آن $q = p^m$. بنابراین هر توان a را می‌توان بر حسب ترکیب خطی از اعضای این مجموعه نوشت. پس به ازای هر $0 \le i \le q-1$، می‌توان نوشت $a^i = a_0 + a_1a + a_2a^2 + \cdots + a_{q-1}a^{q-1}$، که در آن $0 \le a_i \le p-1$. به a^i واژه‌ی $a_0a_1a_2\cdots a_{q-1}$ را نظیر می‌کنیم.

مثال ۸.۴.۱۵. در $\mathrm{GF}(۴)$ عضو اولیه‌ی a را داریم که $a^۲ + a + ۱ = ۰$. بنابراین $a^۲ = ۱ + a$، $\mathrm{GF}(۴) = \{۰, ۱, a, a^۲\}$ و $\{۰, ۱, a, ۱ + a\}$،

$$۰ \longleftrightarrow ۰۰ \quad ۱ \longleftrightarrow ۱۰ \quad a \longleftrightarrow ۰۱ \quad a^۲ \longleftrightarrow ۱۱ \tag{۱}$$

کد دوری به طول ۲ روی $\mathbb{Z}_۲$ با چندجمله‌ای مولد $g(x) = ۱ + x + x^۲$ و چندجمله‌ای امتحان $h(x) = \dfrac{x^۳ - ۱}{g(x)} = x - ۱$ را در نظر بگیرید. a ریشه‌ی سوم اولیه‌ی واحد در $\mathrm{GF}(۴)$ است، بنابراین ماتریس امتحان توازن کد برابر $H = [۱ \;\; a \;\; a^۲]$ است. اگر از جدول (۱) استفاده کنیم، خواهیم داشت

$$H = \begin{bmatrix} ۱ & ۰ & ۱ \\ ۰ & ۱ & ۱ \end{bmatrix}.$$

برای $\mathrm{GF}(۲^۳)$ با عضو اولیه‌ی a، که $a^۳ + a + ۱ = ۰$، می‌توان جدول زیر را نوشت

عضو	۰	۱	a	$a^۲$	$a^۳$	$a^۴$	$a^۵$	$a^۶$
واژه	۰۰۰	۱۰۰	۰۱۰	۰۰۱	۱۱۰	۰۱۱	۱۱۱	۱۰۱

(۲)

مثلاً $a^۶ = ۱ + a^۲$، $a^۵ = ۱ + a + a^۲$، ... . کد دوری به طول ۳ روی $\mathbb{Z}_۲$ با چندجمله‌ای مولد $g(x) = ۱ + x + x^۳$ و چندجمله‌ای امتحان $h(x) = \dfrac{x^۷ - ۱}{g(x)}$ را در نظر بگیرید. a ریشه‌ی هفتم اولیه‌ی واحد در $\mathrm{GF}(۲^۳)$ است، بنابراین ماتریس امتحان توازن کد برابر $H = [۱ \;\; a \;\; a^۲ \;\; \cdots \;\; a^۶]$ است، که اگر از جدول (۲) استفاده کنیم، خواهیم داشت

$$H = \begin{bmatrix} ۱ & ۰ & ۰ & ۱ & ۰ & ۱ & ۱ \\ ۰ & ۱ & ۰ & ۱ & ۱ & ۱ & ۰ \\ ۰ & ۰ & ۱ & ۰ & ۱ & ۱ & ۱ \end{bmatrix}.$$

برای $\mathrm{GF}(۲^۳)$ عضو اولیه‌ی دیگر b، که $b^۳ + b^۲ + ۱ = ۰$، وجود دارد. برای این عضو می‌توان جدول زیر را نوشت

عضو	۰	۱	b	$b^۲$	$b^۳$	$b^۴$	$b^۵$	$b^۶$
واژه	۰۰۰	۱۰۰	۰۱۰	۰۰۱	۱۰۱	۱۱۱	۱۱۰	۰۱۱

(۳)

مثلاً $b^۶ = b + b^۲$، $b^۵ = ۱ + b$، ... . اکنون کد دوری به طول ۳ روی $\mathbb{Z}_۲$ با چندجمله‌ای مولد $g(x) = ۱ + x^۲ + x^۳$ و چندجمله‌ای امتحان $h(x) = \dfrac{x^۷ - ۱}{g(x)}$ را در نظر بگیرید. b ریشه‌ی هفتم اولیه‌ی واحد در $\mathrm{GF}(۲^۳)$ است، بنابراین ماتریس امتحان توازن کد برابر $H = [۱ \;\; b \;\; b^۲ \;\; \cdots \;\; b^۶]$ است، که اگر از جدول (۳) استفاده کنیم، خواهیم داشت

$$H = \begin{bmatrix} ۱ & ۰ & ۰ & ۱ & ۱ & ۱ & ۰ \\ ۰ & ۱ & ۰ & ۰ & ۱ & ۱ & ۱ \\ ۰ & ۰ & ۱ & ۱ & ۱ & ۰ & ۱ \end{bmatrix}. \qquad \square$$

مثال ۹.۴.۱۵. تجزیه‌ی $x^{۱۵} - ۱ = \Phi_۱(x)\Phi_۳(x)\Phi_۵(x)\Phi_{۱۵}(x)$ به چندجمله‌ای‌های دایره‌بر، روی $\mathbb{Z}_۲$، را در نظر بگیرید، که در آن

$$\begin{aligned} \Phi_۱(x) &= x - ۱ \\ \Phi_۳(x) &= x^۲ + x + ۱ \\ \Phi_۵(x) &= x^۴ + x^۳ + x^۲ + x + ۱ \\ \Phi_{۱۵}(x) &= x^۸ - x^۷ + x^۵ - x^۴ + x^۳ - x + ۱. \end{aligned}$$

چندجمله‌ای‌های $\Phi_1(x)$، $\Phi_3(x)$، و $\Phi_5(x)$ روی $\mathbb{Z}_2$ تحویل‌ناپذیرند. چون $15 \mid 2^4 - 1$ و $\varphi(5) = 8$، نتیجه می‌گیریم که $\Phi_{15}(x)$ حاصل‌ضرب دو چندجمله‌ای تحویل‌ناپذیر درجه‌ی ۴ روی $\mathbb{Z}_2$ است،

$$\Phi_{15}(x) = (x^4 + x + 1)(x^4 + x^3 + 1).$$

اکنون فرض کنید $g(x) = x^4 + x + 1$ و a ریشه‌ای از آن باشد. در این صورت α عضو اولیه‌ای از $\mathrm{GF}(2^4)$ و $g(x)$ یک چندجمله‌ای اولیه است (مثال ۱۴.۳.۱۴ از صفحه‌ی ۳۰۲، را ببینید). اگر از نماد برداری برای ۱۵ عضو $a^j \in \mathrm{GF}(2^4)^\times$، $j = 0, 1, \ldots, 14$، که بر حسب پایه $\{1, a, a^2, a^3\}$ بسط داده شده‌اند جدول زیر را به دست می‌آوریم:

(۴)

عضو	۰	۱	a	a^2	a^3	a^4	a^5	a^6
واژه	۰۰۰۰	۱۰۰۰	۰۱۰۰	۰۰۱۰	۰۰۰۱	۱۱۰۰	۰۱۱۰	۰۰۱۱
عضو	a^7	a^8	a^9	a^{10}	a^{11}	a^{12}	a^{13}	a^{14}
واژه	۱۱۰۱	۱۰۱۰	۰۱۰۱	۱۱۱۰	۰۱۱۱	۱۱۱۱	۱۰۱۱	۱۰۰۱

به عنوان مثال $a^{14} = 1 + a^3$، $a^{13} = 1 + a^2 + a^3$، ... کد دوری به طول ۴ روی $\mathbb{Z}_2$ با چندجمله‌ای مولد $g(x) = x^4 + x + 1$ و چندجمله‌ای امتحان $h(x) = \dfrac{x^{15} - 1}{g(x)}$ را در نظر بگیرید. a ریشه‌ی پانزدهم اولیه‌ی واحد در $\mathrm{GF}(2^4)$ است، بنابراین ماتریس امتحان توازن کد برابر $H = [1 \;\; a \;\; a^2 \;\; \cdots \;\; a^{14}]$ است، که اگر از جدول (۴) استفاده کنیم، نمایش دودوئی H، که یک ماتریس 15×4 است و ستون‌هایش این بردارها هستند ، به دست می‌آید:

$$H = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}.$$

این کد با $[15, 11]$- کد همینگ معادل است. یک پیام $u = (a_0, a_1, \ldots, a_{10}) = \sum a_i t^i$ را با $w(t) = u(t)(t^4 + t + 1)$ کد گذاری می‌کنیم. فرض کنید چندجمله‌ای دریافت شده شامل یک خطا باشد، یعنی اگر u فرستاده شده باشد $u + x^{e-1}$ دریافت شود. در این صورت سندرُم عبارت است از $u(\alpha) + \alpha^{e-1} = \beta^{e-1}$ و کد گشا درمی‌یابد که در eامین مکان خطا رخ داده است. □

فرض کنید C یک $[n, k]$- کد دوری با مولد $g(t)$، $(\deg g(x) = m)$ روی $\mathrm{GF}(q)$ باشد. می‌خواهیم ماتریس مولد استاندارد C را بیابیم. بنا به الگوریتم تقسیم چندجمله‌ای‌های $q_j(x)$ و $r_j(x)$ وجود دارند که $\deg r_j(x) < m$ و

$$x^j = q_j(x)g(x) + r_j(x), \quad j \in \mathbb{N}.$$

بنابراین $x^j - r_j(x) \in C$. اکنون $g_j(t) = t^k(t^j - r_j(t))$، $m \le j \le n - 1$، مستقل خطی‌اند. با استفاده از این واژه، ماتریس مولد استاندارد $G = [I_k \mid -A]$ برای C به دست می‌آید، که در آن A ماتریس $k \times m$ است و سطر iام آن بردار ضرایب $r_{n-k-1+i}(t)$ است.

مثال ۱۰.۴.۱۵. تجزیه‌ی $x^7 - 1 = (1 + x)(1 + x + x^3)(1 + x^2 + x^3)$ به عوامل تحویل‌ناپذیر روی $\mathbb{Z}_2$ را در نظر بگیرید. آنگاه چندجمله‌ای $g(x) = 1 + x^2 + x^3$ مولد یک $[7, 4]$- کد دوری با چندجمله‌ای امتحان $h(x) = 1 + x^2 + x^3 + x^4$ است. داریم

$$x^3 = 1g(x) + 1 + x^2, \quad x^4 = (1 + x)g(x) + 1 + x + x^2$$
$$x^5 = (1 + x + x^2)g(x) + 1 + x, \quad x^6 = (x + x^2 + x^3)g(x) + x + x^2$$

و بنابراین

$$\begin{aligned} g_3(t) &= t^4(t^3 - 1 - t^2) = 1 + t^4 + t^6 \\ g_4(t) &= t^4(t^4 - 1 - t - t^2) = t + t^4 + t^5 + t^6 \\ g_5(t) &= t^4(t^5 - 1 - t) = t^2 + t^4 + t^5 \\ g_6(t) &= t^4(t^6 - t - t^2) = t^3 + t^5 + t^6 \end{aligned}$$

از این‌رو ماتریس‌های

$$G=\begin{bmatrix}۱&۰&۰&۰&۱&۰&۱\\۰&۱&۰&۰&۱&۱&۱\\۰&۰&۱&۰&۱&۱&۰\\۰&۰&۰&۱&۰&۱&۱\end{bmatrix},\quad H=\begin{bmatrix}۱&۱&۱&۰&۱&۰&۰\\۰&۱&۱&۱&۰&۱&۰\\۱&۱&۰&۱&۰&۰&۱\end{bmatrix}$$

ماتریس‌های مولد استاندارد و امتحان توازن C هستند. □

در صورتی که ماتریس امتحان توازن کد دوری به صورت $H=[A\mid I_m]$ باشد، سندرُم واژه‌ها را می‌توان به راحتی محاسبه کرد:

قضیه ۱۱.۴.۱۵. اگر C کد دوری به طول n با مولد $g(t)$، $\deg g(x)=m$، و ماتریس امتحان توازن $H=[A\mid I_m]$ باشد، آنگاه سندرُم $S(u)$ از u برابر باقیمانده‌ی تقسیم $u(x)$ بر $g(x)$ است. □

فرض کنید $g(t)$ مولد $[n,k]$- کد دوری C باشد، $\deg g(x)=m$، همان طور که قبلاً دیده‌ایم برای کد گذاری پیام $u=a_۰a_۱\cdots a_{k-۱}\in \mathrm{GF}(q)^k$ صورت چندجمله‌ای آن را در نظر گرفته و آن را به صورت $u(t)g(t)\in C=(g(t))$ کد گذاری می‌کنیم. توجه کنید نگاشت $\varphi: V_k\longrightarrow V_n$ با ضابطه‌ی $\varphi(u(t))=u(t)g(t)$ خطی و یک‌به‌یک است. حال اگر واژه‌ی u دریافت شده باشد، $u(x)$ را بر $g(x)$ تقسیم می‌کنیم. اگر در این تقسیم باقیمانده وجود داشته باشد، آنگاه خطا رخ داده است و برای تصحیح خطا، ابتدا $e(t)=u(t)h(t)$ را محاسبه می‌کنیم، که در آن $h(x)$ چندجمله‌ای امتحان C است. در نهایت $u(t)$ را به صورت $w(t)=u(t)-e(t)$ کد گشایی می‌کنیم.

مثال ۱۲.۴.۱۵. فرض کنید $g(t)=۱+t^۲+t^۳$ مولد $[۷,۴]$- کد دوتایی C باشد. پیام $u=۱۰۱۰$ به صورت

$$u(t)g(t)=(۱+t^۲)(۱+t^۲+t^۳)=۱+t^۳+t^۴+t^۵$$

یعنی ۱۰۰۱۱۱ کد گذاری می‌شود. اکنون اگر واژه‌ی $u=۱۱۰۰۰۰۱$ دریافت شده باشد، آنگاه داریم

$$u(x)=(x+x^۲+x^۳)g(x)+۱+x^۲$$

بنابراین در انتقال واژه خطا رخ داده است و باقی‌مانده تقسیم $u(x)$ بر $g(x)$ خطا را مشخص می‌کند، یعنی $e=۱۰۱۰۰۰۰$. پس u به صورت $u-e=۰۱۱۰۰۰۱$ کد گشایی می‌شود. همین طور پیام اولیه‌ی $w(t)$ با تقسیم $u(t)-e(t)$ بر $g(t)$ به دست می‌آید، یعنی $w(t)=۰۱۱۱$. □

اکنون کدهای دوری را بر حسب ریشه‌های چندجمله‌ای مولد توصیف می‌کنیم:

قضیه ۱۳.۴.۱۵. فرض کنید C یک کد دوری با مولد $g(t)$ روی $\mathrm{GF}(q)$ باشد. اگر $\alpha_۱$، ...، α_m ریشه‌های $g(x)$ در یک توسیع $\mathrm{GF}(q)$ باشند، آنگاه

$$f(t)\in C\Longleftrightarrow f(\alpha_۱)=f(\alpha_۲)=\cdots=f(\alpha_m).$$

اثبات. ($\Longrightarrow$) اگر $f(t)\in C=(g(t))$، آنگاه داریم $f(t)=u(t)g(t)$. بنابراین $f(x)=u(x)g(x)+v(x)(x^n-۱)$، که در آن $v(x)\in \mathrm{GF}(q)[x]$، چون هر ریشه‌ی $g(x)$ ریشه‌ای از $x^n-۱$ نیز هست، پس هر ریشه‌ی $g(x)$ ریشه‌ای از $f(x)$ است.
($\Longleftarrow$) چون $f(\alpha_i)=۰$، پس $(x-\alpha_i)|f(x)$. بنابراین $g(x)|f(x)$ و $f(x)\in(g(x))$. در نتیجه $f(t)\in(g(t))=C$. □

فرض کنید a ریشه‌ی nام اولیه‌ی واحد روی $\mathrm{GF}(q)$ و K اجتماعی از هم مجموعه‌های دایره‌بر به پیمانه‌ی n باشد. در این صورت $g(x)=\prod_{i\in K}(x-a^i)$ مولد یک $[n,k]$- کد دوری روی $\mathrm{GF}(q)$ است و

$$u(t)\in C\Longleftrightarrow u(a^i)=۰,\quad \forall i\in K.$$

این مطلب حالت خاصی از قضیه‌ی قبل است. مشابه اثبات قضیه‌ی قبل می‌توان ثابت کرد:

قضیه ۱۴.۴.۱۵. اگر $g(x) = g_۱(x)\cdots g_s(x)$ چندجمله‌ای مولد کد دوری C روی $\mathrm{GF}(q)$ و α_i ریشه ای $g_i(x)$ در یک توسیع $\mathrm{GF}(q)$ باشد، آنگاه

$$f(t) \in C \Longleftrightarrow f(\alpha_۱) = f(\alpha_۲) = \cdots = f(\alpha_s) = ۰. \qquad \square$$

بنابراین کد دوری را می‌توان با تعیین این که کد واژه‌های ریشه‌های معین و از پیش تعیین شده‌ای داشته باشند، توصیف کرد. در واقع، کافی است از هر عامل تحویل‌ناپذیر $f_i(x)$ چندجمله‌ای مولد $g(x)$ یک ریشه‌ی β_i انتخاب کنیم و مقدر کنیم که همه‌ی کد واژه‌ها این ریشه‌ها را داشته باشند (در توسیع مناسبی از $\mathrm{GF}(q)$). اگر با $\alpha_۱$، $\alpha_۲$، ...، α_s شروع کنیم و کد C را با

$$f(t) \in C \Longleftrightarrow f(\alpha_i) = ۰ \ , \ \ i = ۱, ۲, \ldots, s$$

در نظر بگیریم ، آنگاه C دوری است و مولد آن کوچک‌ترین مضرب مشترک چندجمله‌ای‌های می‌نیمال $\alpha_۱$، $\alpha_۲$، ...، α_s است. فرض کنید همه‌ی ریشه‌ها در $\mathrm{GF}(q)^k$ قرار داشته باشند (که می‌توان آن‌را به عنوان فضای برداری $\mathrm{GF}(q)^k$ روی $\mathrm{GF}(q)$ در نظر گرفت). به ازای هر i ماتریس $sk \times n$ با ستون‌های ۱، $\alpha_۱$، $\alpha_۱^۲$، ...، $\alpha_s^{n-۱}$ (که آن‌ها را به صورت بردارهایی در $\mathrm{GF}(q)^k$ در نظر گرفته‌ایم، مانند مثال‌های ۸.۴.۱۵ و ۹.۴.۱۵، در نظر می‌گیریم) و با قرار دادن همه‌ی آن ها کنار هم، ماتریس $sk \times n$، H را که درایه‌های آن در $\mathrm{GF}(q)$ است را می‌سازیم. به وضوح $Hu^\top = ۰$، که در آن $u = (u_۰, u_۱, \ldots, u_{n-۱})$ و $u(a_i) = ۰$، $i = ۱, \ldots, s$. سطرهای H لزوماً مستقل خطی نیستند.

به ازای هر $u \in V_n$ چندجمله‌ای ماتسون-سولومون را به صورت زیر تعریف می‌کنیم

$$F_u(x) = \frac{۱}{n}\sum_{j=۱}^{n} u(a^j)x^{n-j}$$

با در نظر گیری نمادهای بالا فرض کنید $u = (u_۰, u_۱, \ldots, u_{n-۱}) \in C$. در این صورت به ازای هر $s = ۰, ۱, \ldots, n-۱$، داریم

$$\begin{aligned} F_u(a^s) &= \frac{۱}{n}\sum_{j=۱}^{n} u(a^j)a^{s(n-j)} \\ &= \frac{۱}{n}\sum_{j=۱}^{n}\left(\sum_{i=۰}^{n-۱} u_i a^{ji}\right)a^{-j} \\ &= \frac{۱}{n}\sum_{i=۰}^{n-۱} u_i \sum_{j=۱}^{n} a^{(i-s)j} \\ &= u_s \end{aligned}$$

(چون برای $i \neq s$ داریم $\sum_{j=۰}^{n-۱} a^{(i-s)j} = \frac{۱ - a^{(i-s)n}}{۱ - a^{i-s}} = ۰$). بنابراین کد دوری C را می‌توانیم به صورت

$$C = \{(F_u(a^۰), F_u(a_۱), \ldots, F_u(a^{n-۱})) \mid u \in C\}$$

نیز توصیف کنیم.

لم ۱۵.۴.۱۵. اگر $g(x) = \prod_{i\in K}(x - a^i)$ چندجمله‌ای مولد کد دوری C باشد و $\{۱, ۲, \ldots, d-۱\} \subseteq K$، که در آن K اجتماع هم مجموعه‌های دوری به پیمانه‌ی n باشد، آنگاه به ازای هر $u \in C$، $\deg F_u(x) \leq n - d$.

اثبات. چون $g(x)|u(x)$، به ازای هر $۱ \leq j \leq d-۱$ داریم $u(a^j) = ۰$. بنابراین حکم با استفاده از تعریف، حاصل می‌شود. $\square$

قضیه ۱۶.۴.۱۵. اگر دقیقاً r ریشه‌ی nام واحد ریشه‌های چندجمله‌ای ماتسون- سولومون $F_u(x)$ باشد، آنگاه وزن u برابر $n - r$ است.

اثبات. وزن u تعداد مولفه‌های ناصفر u است. پس حکم، بنا به بحث پیش از لم ۱۵.۴.۱۵، برقرار است. $\square$

قضیه ۱۷.۴.۱۵. اگر $C \subseteq V_k$ یک کد دوری با چندجمله‌ای مولد $g(t)$، و α_1، ...، α_{n-k} ریشه‌های $g(x)$ باشند، آنگاه $u \in V_n$ یک کد چندجمله‌ای است اگر و تنها اگر بردار ضرایب آن، $u = (a_0, \ldots, a_{n-1})$ در دستگاه $Hu^\top = 0$ صدق کند، که در آن

$$H = \begin{bmatrix} 1 & \alpha_1 & \alpha_1^2 & \cdots & \alpha_1^{n-1} \\ 1 & \alpha_2 & \alpha_2^2 & & \alpha_2^{n-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \alpha_{n-k} & \alpha_{n-k}^2 & \cdots & \alpha_{n-k}^{n-1} \end{bmatrix}.$$

اثبات. فرض کنید $u(x) = a_0 + a_1 x + a_2 x^2 \cdots + a_{n-1}x^{n-1}$، در این صورت $u(\alpha_i) = 0$، یعنی

$$(1, \alpha_i, \alpha_i^2 \ldots, \alpha_i^{n-1})(a_0, a_1, a_2, \ldots, a_{n-1})^\top = (0, 0, 0, \ldots, 0)$$

$1 \le i \le n-k$، اگر و تنها اگر $Hu^\top = 0$. □

فرض کنید α یک ریشه‌ی اولیه‌ی nام واحد در $\mathrm{GF}(q^m)$ با چندجمله‌ای می‌نیمال $g(x)$ روی $\mathrm{GF}(q)$ باشد. فرض کنید C کد دوری با مولد $g(t)$ باشد. می‌دانیم $u \in V_n$، $g(t)$ را عاد می‌کند اگر و تنها اگر $u(\alpha) = 0$. پس ماتریس امتحان توازن در قضیه‌ی فوق را می‌توان با $[1 \ \alpha \ \alpha^2 \cdots \alpha^{n-1}]$ جایگزین کرد. آنگاه $S(u) = Hu^\top$ و $S(u) = u(\alpha)$ هر دو سندرُم هستند ، زیرا $u = (a_0, \ldots, a_{n-1})$ را می‌توان به عنوان چندجمله‌ای با ضرایب a_i در نظر گرفت.
اکنون فرض کنید $g(x)$ یک عامل تحویل‌ناپذیر از $x^n - 1$ روی $\mathrm{GF}(q)$ باشد. پس ایدآل تولید شده توسط $g(x)$ در $\mathrm{GF}(q)[x]$ یک ایدآل ماکسیمال است. چون $(g(x))$ یک ایدآل ماکسیمال $\mathrm{GF}(q)[x]$ شامل $(x^n - 1)$ است، $(g(t))$ یک ایدآل ماکسیمال V_n است. بنابراین کد دوری تولید شده توسط $g(t)$ را کد ماکسیمال گوییم. از طرف دیگر $\hat{g}(x) = \dfrac{x^n - 1}{g(x)}$، آنگاه $(\hat{g}(x))$ یک ایدآل ماکسیمال $\mathrm{GF}(q)[x]$ شامل $(x^n - 1)$ است. زیرا اگر

$$(x^n - 1) \subseteq (u(x)) \subseteq (\hat{g}(x)),$$

آنگاه چندجمله‌ای $r(x)$ در $\mathrm{GF}(q)[x]$ وجود دارد که $u(x) = \dfrac{x^n - 1}{g(x)} r(x)$، در نتیجه $g(x)u(x) = (x^n - 1)r(x)$. بنابراین $g(x)u(x) = u(x)s(x)r(x)$ که نتیجه می‌دهد $g(x) = s(x)r(x)$. اما چون $g(x)$ تحویل‌ناپذیر است نتیجه می‌گیریم که $r(x) = 1$ یا $s(x) = 1$. در حالت اول داریم $u(x) = \hat{g}(x)$ و در حالت دوم داریم $u(x) = x^n - 1$. بنابراین $(\hat{g}(x))$ یک ایدآل ماکسیمال $\mathrm{GF}(q)[x]$ شامل $(x^n - 1)$ است. به همین دلیل کد دوری تولید شده توسط $\dfrac{x^n - 1}{g(x)}$ را کد ماکسیمال گوییم. فرض کنید $x^n - 1 = g_1(x) \cdots g_s(x)$، که در آن $g_i(x)$ روی $\mathrm{GF}(q)$ تحویل‌ناپذیر است. اگر β_i ریشه‌ای از $g_i(x)$ در توسیعی از $\mathrm{GF}(q)$ باشد، آنگاه کد M_i^+ با مولد $g_i(x)$ یک کد ماکسیمال است. به علاوه

$$M_i^+ = \{f(t) \mid f(\beta_i) = 0\}.$$

مثال ۱۸.۴.۱۵. $\mathrm{GF}(2^6)$ کوچک‌ترین توسیع $\mathbb{Z}_2$ که شامل یک ریشه‌ی ۹ام اولیه‌ی واحد است. فرض کنید α عضو اولیه‌ای از آن میدان باشد، پس $\alpha^{63} = 1$ و $\beta = \alpha^7$ یک ریشه‌ی اولیه‌ی ۹ام واحد است. ریشه‌های چندجمله‌ای می‌نیمال β عبارت‌اند از β، β^2، β^4، β^8، $\beta^{16} = \beta^7$، $\beta^{32} = \beta^5$. این چندجمله‌ای برابر $\dfrac{x^9 - 1}{x^3 - 1} = x^6 + x^3 + 1$ است. بنابراین

$$x^9 - 1 = (x - 1)(x^2 + x + 1)(x^6 + x^3 + 1) = g_1(x)g_2(x)g_3(x).$$

کد دوری ماکسیمال M_3^+ با مولد $g_3(t)$ را در نظر بگیرید. ستون‌های ماتریس امتحان توازن H از کد M_3^+ دوبه‌دو مستقل خطی‌اند، یعنی فاصله‌ی می‌نیمم کد، بزرگ‌تر یا مساوی ۳ است. چون به وضوح کد M_3^+ شامل کد واژه‌هایی به صورت

$$(a_0, a_1, a_2, a_0, a_1, a_2, a_0, a_1, a_2)$$

فوراً دیده می‌شود که فاصله‌ی می‌نیمم دقیقاً برابر ۳ است.
اکنون کد ماکسیمال $M_{۳}^{-}$ با چندجمله‌ای امتحان $x^{۶}+x^{۳}+۱$ را در نظر بگیرید. $M_{۳}^{-}$ یک $[۶,۹]$- کد است. چون $t^{۳}-۱$ یک کد واژه است، فاصله‌ی می‌نیمم برابر ۲ است.
اگر $\mathrm{GF}(۲^{۶})$ را با استفاده از چندجمله‌ای $x^{۶}+x+۱$ بسازیم، آنگاه ماتریس H ، ۹×۱۲ برای $M_{۳}^{-}$ به طریقی که در قضیه‌ی ۱۷.۴.۱۵، تشریح شده دارای ۶ سطر با درایه‌های صفر،یک سطر با درایه‌های ۱ و سطر (۱۱۰۱۱۰۱۱۰) و چهار سطر (۰۱۱۰۱۱۰۱۱) است. بنابراین یک ماتریس ۹×۳ امتحان توازن می‌یابیم. البته از $x^{۶}+x+۱$ می‌توانیم ماتریس امتحان توازن معادل با $[I,I,I]$ را بسازیم. □

در برخی کاربردها، استفاده از مولد خودتوان (عضو e که $e^{۲}=e$) برای یک کد دوری مزیت‌های زیادی دارد. اکنون ثابت می‌کنیم برای هر کد دوری به طول n روی $\mathrm{GF}(q)$، با فرض $\gcd\{n,q\}=۱$، مولد خودتوان وجود دارد و یکتاست:

قضیه ۱۹.۴.۱۵. اگر C یک کد دوری به طول n روی $\mathrm{GF}(q)$ باشد و $\gcd\{q,n\}=۱$، آنگاه عضو همانی $e(t)$ برای C وجود دارد. به ویژه $e(t)$ یکتا و خودتوان است. به علاوه داریم $C=(e(t))$.

اثبات. فرض کنید $g(x)$ چندجمله‌ای مولد و $h(x)$ چندجمله‌ای امتحان C باشد. در این صورت $g(x)h(x)=x^{n}-۱$. چون $x^{n}-۱$ ریشه‌ی تکراری ندارد، $g(x)$ و $h(x)$ نسبت به هم اول‌اند. پس چندجمله‌ای‌های $p(x)$ و $q(x)$ در $\mathrm{GF}(q)[x]$ وجود دارند که

$$p(x)g(x)+q(x)h(x)=۱.$$

قرار می‌دهیم

$$e(x)=p(x)g(x)=۱-q(x)h(x).$$

$e(t)$ یک کدواژه است، زیرا $e(t)=p(t)g(t)\in C$. به علاوه اگر $f(t)g(t)$ عضو دلخواهی از C باشد، آنگاه چون $h(t)g(t)=۰$ داریم

$$\begin{aligned} e(t)f(t)g(t) &= f(t)g(t)-f(t)g(t)q(t)h(t)\\ &= f(t)g(t). \end{aligned}$$

از این رو $e(t)$ عضو همانی C است. از طرف دیگر چون هر کد واژه‌ای $u(t)$ را می‌توان به صورت $u(t)=u(t)e(t)$ نوشت، نتیجه می‌شود که $e(t)$ یک مولد C است. □

لازم است تذکر دهیم که C ممکن است تعداد زیادی عضو خودتوان داشته باشد، اما تنها یکی از آن ها مولد خودتوان (همانی) است.
از این جا به بعد هرگاه در مورد مولد خودتوان یک کد دوری C به طول n روی $\mathrm{GF}(q)$ بحث می‌کنیم، فرض می‌کنیم $\gcd\{n,q\}=۱$.

قضیه ۲۰.۴.۱۵. فرض کنید $C_{۱}$ و $C_{۲}$ دو کد دوری با مولدهای خودتوان $e_{۱}(x)$ و $e_{۲}(x)$ باشند. در این صورت
(الف) $C_{۱}\cap C_{۲}$ کد دوری با مولد خودتوان $e_{۱}(x)e_{۲}(x)$ است.
(ب) $C_{۱}+C_{۲}$ کد دوری با مولد خودتوان $e_{۱}(x)+e_{۲}(x)-e_{۱}(x)e_{۲}(x)$ است.

اثبات. (الف) چون $e_{۱}(t)e_{۲}(t)$، هم مضرب $e_{۱}(t)$ و هم مضرب $e_{۲}(t)$ است، به $C_{۱}\cap C_{۲}$ تعلق دارد. هم‌چنین به ازای هر $u(t)\in C_{۱}\cap C_{۲}$، داریم $e_{۱}(t)u(t)=u(t)$ و $e_{۲}(t)u(t)=u(t)$، بنابراین $e_{۱}(t)e_{۲}(t)u(t)=u(t)$ و $e_{۱}(t)e_{۲}(t)$ عضو همانی $C_{۱}\cap C_{۲}$ است.
(ب) چون $-e_{۱}(t)e_{۲}(t)$ در $C_{۲}$ (هم‌چنین $C_{۱}$) قرار دارد ، داریم

$$e_{۱}(t)+(e_{۲}(t)-e_{۱}(t)e_{۲}(t))\in C_{۱}+C_{۲}.$$

به علاوه برای هر $u(t)\in C_{۱}$ و هر $v(t)\in C_{۲}$ داریم

$$\begin{aligned} &(e_{۱}(t)+e_{۲}(t)-e_{۱}(t)e_{۲}(t))(u(t)+v(t))=\\ &e_{۱}(t)u(t)+e_{۲}(t)v(t)-e_{۱}(t)e_{۲}(t)u(t)+e_{۱}(t)v(t)+e_{۲}(t)v(t)-e_{۱}(t)e_{۲}(t)v(t)=\\ &u(t)+e_{۲}(t)u(t)-e_{۲}(t)u(t)+e_{۱}(t)v(t)+v(t)-e_{۱}(t)v(t)=u(t)+v(t). \end{aligned}$$

پس $e_۱(t)+e_۲(t)-e_۲(t)e_۲(t)$ عضو همانی $C_۱+C_۲$ است. □

قضیه ۲۱.۴.۱۵. فرض کنید C کد دوری به طول n با چندجمله‌ای مولد $g(x)$ و مولد خودتوان $e(x)$ باشد. در این صورت $g(x)=\gcd\{e(x),x^n-۱\}$.

اثبات. اگر $h(x)$ چندجمله‌ای امتحان C باشد، آنگاه $g(x)h(x)=x^n-۱$. از طرف دیگر بنا به اثبات قضیه‌ی ۱۹.۴.۱۵ داریم $e(x)=p(x)g(x)$. بنابراین

$$\begin{aligned}\gcd\{e(x),x^n-۱\} &= \gcd\{p(x)g(x),h(x)g(x)\}\\ &= g(x) \quad (\text{چون } \gcd\{p(x),h(x)\}=۱).\end{aligned}$$ □

قضیه ۲۲.۴.۱۵. فرض کنید C کد دوری به طول n با مولد خودتوان $e(x)$ و چندجمله‌ای مولد $g(t)$ و چندجمله‌ای امتحان $h(x)$ باشد، که در آن $\deg g(x)=m$، $\deg h(x)=l$. در این صورت مولد خود توان کد دوری تولید شده توسط $h(x)$ برابر $۱-e(x)$ و مولد خودتوان $C^\perp=(g^\perp(x))$ برابر $۱-e(x^{n-۱})$ است.

اثبات. چون $g(x)h(x)=x^n-۱$ داریم $g(t)h(t)=۰$. از طرف دیگر طبق اثبات قضیه‌ی ۱۹.۴.۱۵، $e(x)=f(x)g(x)$. پس

$$h(t)(۱-e(t))=h(t)(۱-f(t)g(t))=h(t).$$

بنابراین $۱-e(t)$ عضو همانی $C=(h(t))$ است.
به طریق مشابه چون $g^\perp(x)=x^kh(x^{-۱})$، داریم

$$\begin{aligned}g^\perp(t)(۱-e(t^{n-۱})) &= g^\perp(t)-t^kh(t^{n-۱})e(t^{n-۱})\\ &= g^\perp(t)-t^kh(t^{n-۱})f(t^{n-۱})g(t^{n-۱})\\ &= g^\perp(t)\end{aligned}$$

بنابراین $۱-e(t^{n-۱})$ عضو همانی $C^\perp=(g^\perp(t))$ است. □

فرض کنید $x^n-۱=g_۱(x)\cdots g_s(x)$ تجزیه‌ی $x^n-۱$ به عوامل تحویل‌ناپذیر روی $\mathrm{GF}(q)$ باشد، که در آن $\gcd\{n,q\}=۱$. یادآوری می‌کنیم کد دوری تولید شده توسط $g_i(x)$ را با M_i^+ نشان می‌دهیم، که یک ایدآل ماکسیمال V_n است و آن را کد ماکسیمال گوییم. هم‌چنین کد دوری تولید شده توسط $h_i(x)=\dfrac{x^n-۱}{g_i(x)}$ را با M_i^- نشان می‌دهیم که یک ایدآل ماکسیمال V_n است و آن را کد ماکسیمال گوییم. فرض کنید $\deg g_i(x)=d_i$. چون $g_i(x)$ و $h_i(x)$ نسبت به هم اول هستند. چندجمله‌ای‌های $p_i(x)$ و $q_i(x)$ در $\mathrm{GF}(q)[x]$ وجود دارند که $p_i(x)g_i(x)+q_i(x)h_i(x)=۱$. پس اگر $u(t)$ واژه‌ی دلخواهی در V_n باشد، آنگاه

$$u(t)=p_i(t)g_i(t)u(t)+q_i(t)h_i(t)u(t)\in M_i^++M_i^-$$

بنابراین $V_n=M_i^++M_i^-$. از طرف دیگر به وضوح $M_i^+\cap M_i^-=\{۰\}$، بنابراین $V_n=M_i^+\oplus M_i^-$. به ویژه

$$n=\dim V_n=\dim M_i^++\dim M_i^-=n-d_i+\dim M_i^-.$$

چون M_i^- هیچ ایدآل نابدیهی ندارد ،یک میدان است. بنابراین

$$M_i^-\cong \mathrm{GF}(q)^{d_i}\cong \mathrm{GF}(q^{d_i}).$$

چندجمله‌ای مولد خودتوان M_i^- را خودتوان اولیه می‌نامیم و با $\theta_i(x)$ نشان می‌دهیم.

قضیه ۲۳.۴.۱۵. اگر $\theta_1(x)$، ...، $\theta_s(x)$ خودتوان‌های اولیه‌ی V_n باشند، آنگاه
(الف) $\theta_i(t)\theta_j(t) = 0$، $i \neq j$.
(ب) $\theta_1(t) + \cdots + \theta_s(t) = 1$.
(ج) چندجمله‌ای مولد خودتوان کد دوری $(g_{i_1}(t) \cdots g_{i_k}(t))$ برابر $1 - \theta_{i_1}(t) \cdots - \theta_{i_k}(t)$ است.

اثبات. (الف) فرض کنید $i \neq j$. $M_i^- \cap M_j$ هم ایدآل M_i^- و هم ایدآل M_j^- است. چون M_i^- و M_j^- ایدآل نابدیهی ندارند، $M_i^- \cap M_j^- = \{0\}$. از طرف دیگر بنا به قضیه‌ی ۲۰.۴.۱۵، $\theta_i(t)\theta_j(t)$ مولد خودتوان $M_i^- \cap M_j^-$ است. پس $\theta_i(t)\theta_j(t) = 0$.
(ب) از قضیه‌ی ۲۰.۴.۱۵ و قسمت (الف) نتیجه می‌شود که

$$M_1^- + M_2^- + \cdots + M_s^- = (\theta_1(t) + \cdots + \theta_s(t)).$$

از طرف دیگر بنا به تمرین ۱۶ داریم $M_1^- + M_2^- + \cdots + M_s^- = (f(t))$، که در آن $f(x) = \gcd\{h_1(x), \ldots, h_s(x)\} = 1$.
بنابراین $f(t) = 1$ و

$$(\theta_1(t) + \cdots + \theta_s(t)) = (1) = V_n$$

بنا به یکتایی عضو همانی، $\theta_1(t) + \cdots + \theta_s(t) = 1$.

(ج) فرض کنید

$$g_{j_1 j_2 \cdots j_r}(x) = \frac{x^n - 1}{g_{j_1}(x) g_{j_2}(x) \cdots g_{j_r}(x)}.$$

در این صورت چون

$$g_{j_1 j_2 \cdots j_r}(x) = \gcd\{g_{j_1}(x), g_{j_2}(x), \cdots, g_{j_r}(x)\}$$

از تمرین ۱۶، قضیه‌ی ۲۰.۴.۱۵ و قسمت (الف) نتیجه می‌شود

$$(g_{j_1 j_2 \cdots j_r}(t)) = M_{j_1}^- + M_{j_2}^- + \cdots + M_{j_r}^- = (\theta_{j_1}(t) + \theta_{j_2}(t) + \cdots + \theta_{j_r}(t)).$$

اگر $\{i_1, \ldots, i_k\} = \{1, \ldots, s\} - \{j_1, \ldots, j_r\}$، آنگاه قسمت (ب) نتیجه می‌دهد که

$$(g_{i_1}(t) g_{i_2}(t) \cdots g_{i_k}(t)) = (1 - \theta_{i_1}(t) - \theta_{i_2}(t) - \cdots - \theta_{i_k}(t)). \qquad \square$$

توجه کنید از قسمت‌های (الف) و (ب) قضیه‌ی قبل نتیجه می‌شود

$$\begin{aligned} V_n &= M_1^- \oplus M_2^- \oplus \cdots \oplus M_s^- \\ &\cong \mathrm{GF}(q^{d_1}) \oplus \mathrm{GF}(q^{d_2}) \oplus \cdots \oplus \mathrm{GF}(q^{d_s}). \end{aligned}$$

در حالتی که $q = 2$ می‌توان مولد خودتوان را به سادگی یافت: چون در $\mathbb{Z}_2[x]$ داریم $f^2(x) = f(x^2)$، چندجمله‌ای $e(x) = e_0 + e_1 x + \cdots + e_{n-1}x^{n-1}$ در V_n خودتوان است اگر و تنها اگر $e(t) = e(t^2)$، یعنی

$$e_0 + e_1 t^2 + \cdots + e_{n-1} t^{2n-2} = e_0 + e_1 t + \cdots + e_{n-1} t^{n-1},$$

و این رابطه وقتی و فقط وقتی برقرار است که هرگاه $e_i \neq 0$، آنگاه $e_{2i} \neq 0$، که در آن $2i$ به پیمانه‌ی n محاسبه می‌شود. بنابراین $e(x)$ باید به صورت

$$x^i + x^{2i} + \cdots + x^{2^{d-1}i}$$

باشد، که در آن توان‌های x یک هم مجموعه‌ی دایره‌بر برای ۲ به پیمانه‌ی n تشکیل می‌دهند. برای مثال اگر $n = ۹$، همه مجموعه‌های دایره‌بر برای ۲ به پیمانه‌ی ۹ عبارت‌اند از $C_۰ = \{۰\}$، $C_۱ = \{۱, ۲, ۴, ۸, ۷, ۵\}$، و $C_۳ = \{۳, ۶\}$. بنابراین $۲^۳ = ۸$ عضو خودتوان وجود دارند:

$$\begin{aligned}
e_۱(x) &= ۰ \\
e_۲(x) &= x^۰ = ۱ \\
e_۳(x) &= x + x^۲ + x^۴ + x^۵ + x^۷ + x^۸ \\
e_۴(x) &= x^۳ + x^۶ \\
e_۵(x) &= e_۲(x) + e_۳(x) \\
e_۶(x) &= e_۲(x) + e_۴(x) \\
e_۷(x) &= e_۳(x) + e_۴(x) \\
e_۸(x) &= e_۲(x) + e_۳(x) + e_۴(x).
\end{aligned}$$

چندجمله‌ای مولد متناظر را می‌توان با استفاده از فرمول $g(x) = \gcd\{e(x), x^۹ - ۱\}$ یافت (قضیه‌ی ۲۱.۴.۱۵)؛ مثلاً

$$g_۳(x) = \gcd\{e_۳(x), x^۹ - ۱\} = x + ۱$$

اکنون می‌خواهیم روشی برای یافتن خودتوان‌های اولیه ارائه‌ی کنیم. ابتدا به دو لم نیاز داریم:

لم ۲۴.۴.۱۵. فرض کنید a یک ریشه‌ی n ام اولیه‌ی واحد روی $\mathrm{GF}(q)$ باشد. در این صورت

$$\sum_{i=۰}^{n-۱} a^i = \begin{cases} ۰ & a \neq ۱ \\ n & a = ۱. \end{cases}$$

اثبات. اگر $a = ۱$ حکم واضح است. فرض کنید $a \neq ۱$، در این صورت

$$\sum_{i=۰}^{n-۱} a^i = \frac{۱ - a^n}{۱ - a} = ۰. \qquad \square$$

در لم بعد نشان می‌دهیم که چگونه می‌توان ضرایب یک چندجمله‌ای با درجه‌ی کمتر یا مساوی $n - ۱$ را با استفاده از مقادیرش روی یک ریشه‌ی اولیه‌ی واحد یافت:

لم ۲۵.۴.۱۵. فرض کنید $f(x) = a_۰ + a_۱x + \cdots + a_{n-۱}x^{n-۱}$ یک چندجمله‌ای روی $\mathrm{GF}(q)$ و α یک ریشه‌ی n ام اولیه‌ی واحد روی $\mathrm{GF}(q)$ باشد. در این صورت

$$a_j = \frac{۱}{n} \sum_{j=۰}^{n-۱} f(\alpha^j)\alpha^{-ij}$$

که در آن محاسبات سمت راست در میدان تجزیه‌ی $x^n - ۱$ روی $\mathrm{GF}(q)$ انجام می‌شود.

اثبات. با فرض $\delta_{ki} = \begin{cases} ۱ & k=i \\ ۰ & k\neq i \end{cases}$ داریم

$$\begin{aligned}\sum_{j=۰}^{n-۱} f(\alpha^j)\alpha^{-ij} &= \sum_{j=۰}^{n-۱}\sum_{k=۰}^{n-۱} a_k\alpha^{jk}\alpha^{-ij} \\ &= \sum_{k=۰}^{n-۱} a_k \sum_{j=۰}^{n-۱} \alpha^{j(k-i)} \\ &= \sum_{k=۰}^{n-۱} a_k n\delta_{ki} \\ &= na_i \quad \text{بنابه لم قبل.}\end{aligned}$$ □

اکنون فرض کنید $\gcd\{n,q\} = ۱$ و $x^n - ۱ = g_۱(x)\cdots g_s(x)$ تجزیه‌ی $x^n-۱$ به عوامل تحویل‌ناپذیر روی $\mathrm{GF}(q)$ باشد، که در آن

$$g_i(x) = \prod_{j\in C_i}(x-a^j)$$

و $C_i = \{i, qi, \ldots, q^{d_i-۱}i\}$ هم‌مجموعه‌ی دایره‌بر شامل i، به پیمانه‌ی n است. فرض کنید $\theta_i(x)\in \mathrm{GF}(q)[x]$ خودتوان اولیه‌ی کد ماکسیمال $M_i^- = (h_i(x))$ در V_n باشد. چون $\theta_i(x)$ خودتوان است، $\theta_i^۲(t) = \theta_i(t)$ و بنابراین $f(x)\in \mathrm{GF}(q)[x]$ وجود دارد که

$$\theta_i^۲(x) = \theta_i(x) + f(x)(x^n - ۱).$$

پس $\theta_i^۲(a^j) = \theta_i(a^j)$ و $\theta_i(a_j)$ یا برابر ۰ یا برابر ۱ است. اما چون ریشه‌های nام اولیه‌ی واحد $\theta_i(x)$ و $h_i(x)$ یکی هستند (قضیه‌ی ۲۱.۴.۱۵)، داریم

$$\theta_i(a^j) = \begin{cases} ۰ & j\in C_i \\ ۱ & j\notin C_i. \end{cases}$$

اگر $\theta_i(x) = \sum_{j=۰}^{n-۱}\xi_j x^j$، بنا به لم فوق داریم

$$\xi_j = \frac{۱}{n}\sum_{j=۰}^{n-۱}\theta_i(a^j)a^{-ij} = \frac{۱}{n}\sum_{j\in C_i} a^{-ij}.$$

پس ثابت کرده‌ایم:

قضیه ۲۶.۴.۱۵. اگر $M_i^- = (h_i(t))$ کد ماکسیمال دوری در V_n باشد و

$$g_i(x) = \prod_{j\in C_i}(x-a^j)$$

که در آن C_i یک هم مجموعه‌ی دایره‌بر به پیمانه‌ی n است، آنگاه عضو خودتوان اولیه‌ی M_i^- عبارت است از

$$\theta_i(x) = \frac{۱}{n}\sum_{k=۰}^{n-۱}\left(\sum_{j\in C_i} a^{-kj}\right)x^k.$$ □

توجه کنید محاسبات داخل مجموع برای $\theta_i(x)$، اگر چه در میدان تجزیه‌ی $x^n-۱$ روی $\mathrm{GF}(q)$ انجام می‌شود، نتیجه باید در $\mathrm{GF}(q)$ باشد.

مثال ۲۷.۴.۱۵. فرض کنید a یک ریشه‌ی ۱۹ام واحد روی $\mathbb{Z}_2$ باشد. چون هم مجموعه‌های دایره‌بر برای ۲ به پیمانه‌ی ۹ عبارت‌اند از $C_0 = \{0\}$، $C_1 = \{1, 2, 4, 8, 7, 5\}$، و $C_3 = \{3, 6\}$. داریم

$$\begin{aligned}
\theta_0(x) &= 1 + x + \cdots + x^8 \\
\theta_1(x) &= \sum_{i=0}^{8} (a^{-i} + a^{-2i} + a^{-4i} + a^{-5i} + a^{-7i} + a^{-8i}) x^i \\
\theta_3(x) &= \sum_{i=0}^{8} (a^{-3i} + a^{-6i}) x^i
\end{aligned}$$

چون ۶ کوچک‌ترین عددی است که $19 | 2^6 - 1$، پس $\mathrm{GF}(2^6)$ میدان تجزیه‌ی $x^9 - 1$ روی $\mathbb{Z}_2$ است. به علاوه اگر α یک عضو اولیه‌ی $\mathrm{GF}(64)$ و ریشه‌ی چندجمله‌ای تحویل‌ناپذیر $x^6 + x + 1 \in \mathbb{Z}_2[x]$ باشد، قرار می‌دهیم $a = \alpha^7$. در این صورت a یک ریشه‌ی ۱۹ام اولیه‌ی واحد است. $\theta_3(x)$ را می‌یابیم:

$$\begin{aligned}
\text{ضریب } x^0 &: 1 + 1 = 0 \\
\text{ضریب } x^1 &: a^{-3} + a^{-6} = a^6 + a^3 = \alpha^{42} + \alpha^{21} = 1 \\
\text{ضریب } x^2 &: a^{-6} + a^{-12} = a^3 + a^6 = 1 \\
\text{ضریب } x^3 &: a^{-9} + a^{-18} = 1 + 1 = 0 \\
\text{ضریب } x^4 &: a^{-12} + a^{-24} = a^6 + a^3 = 1 \\
\text{ضریب } x^5 &: a^{-15} + a^{-30} = a^3 + a^6 = 1 \\
\text{ضریب } x^6 &: a^{-18} + a^{-36} = 1 + 1 = 0 \\
\text{ضریب } x^7 &: a^{-21} + a^{-42} = a^6 + a^3 = 1 \\
\text{ضریب } x^8 &: a^{-24} + a^{-48} = a^3 + a^6 = 1.
\end{aligned}$$

پس

$$\theta_3(x) = x + x^2 + x^4 + x^5 + x^7 + x^8. \qquad \square$$

این بخش را با مختصری در باره‌ی گروه خودریختی‌های کد به پایان می‌بریم. گروه خودریختی‌های یک کد در تعیین ساختار کد، محاسبه‌ی توزیع وزن، توصیف کدها و کدگشایی مفید است. در صفحه‌ی ۳۵۵ مفهوم هم‌ارزی کدها را با استفاده از جایگشت‌ها و هم‌چنین گروه خودریختی‌های یک کد را تعریف کردیم. در این جا گروه خودریختی‌ها را برای کدهای دوتایی بررسی می‌کنیم. یادآوری می‌کنیم اگر C یک کد خطی دوتایی به طول n باشد و $\sigma \in S_n$، آنگاه کد

$$C_1 = \{u_{\sigma(1)} \cdots u_{\sigma(n)} \mid u_1 \cdots u_n \in C\}$$

یک کد معادل با C است. اگر $G = [A_1, \ldots, A_n]$، آنگاه ماتریس مولد C با ستون‌های A_1، ...، A_n باشد، ماتریس مولد C_1 ماتریس $G_1 = [A_{\sigma(1)}, \ldots, A_{\sigma(n)}]$ است. جایگشت $\sigma \in S_n$ را یک خودریختی C گوییم، هرگاه برای $u = u_1 u_2 \cdots u_n \in C$ واژه $\sigma u = u_{\sigma(1)} \cdots u_{\sigma(n)}$ در C باشد، یا به طور معادل اگر σ روی ستون‌های ماتریس مولد C اثر کند، مجدداً یک ماتریس مولد برای C حاصل‌ضرب شود:

$$\operatorname{Aut} C = \{\sigma \in S_n \mid \forall u_1 \cdots u_n \in C, \quad u_{\sigma(1)} \cdots u_{\sigma(n)} \in C\}$$

چون

$$\begin{aligned}
\pi\sigma(u_1 u_2 \cdots u_n) &= u_{\pi\sigma(1)} u_{\pi\sigma(2)} \cdots u_{\pi\sigma(n)} \\
&= \pi(u_{\sigma(1)} u_{\sigma(2)} \cdots u_{\sigma(n)}) \\
&= \pi(\sigma(u_1 \cdots u_n)),
\end{aligned}$$

به سادگی می‌توان دید $\operatorname{Aut} C$ یک زیرگروه S_n است.
مثلاً، اگر C کد تکرار دوتایی به طول n باشد، آنگاه $\operatorname{Aut} C = S_n$ هم‌چنین اگر $C = \mathrm{GF}(q)^n$، آنگاه $\operatorname{Aut} C = S_n$.
اگر C یک کد دوری به طول n روی $\mathrm{GF}(q)$ باشد، آنگاه چون $u_۰u_۱\cdots u_{n-۱} \in C$ اگر و تنها اگر $u_{n-۱}u_۰u_۱\cdots u_{n-۲} \in C$، داریم $\sigma \in \operatorname{Aut} C$ که در آن $\sigma = (۱\ ۲\ \cdots\ n)$. پس $\langle\sigma\rangle \le \operatorname{Aut} C$. از طرف دیگر اگر $u(t) \in C$، آنگاه $u(t^q) = u(t)^q \in C$. بنابراین جایگشت $\pi \in S_n$ که به صورت $\pi(i) = qi \mod n$ تعریف می‌شود، (یعنی $\pi : x \to x^q$) نیز کد دوری C را به خودش تصویر می‌کند. از این‌رو $\langle\sigma,\pi\rangle \le \operatorname{Aut} C$. توجه کنید اگر مرتبه‌ی ضربی q به پیمانه‌ی n برابر m باشد، آنگاه $O(\pi) = m$ و به علاوه $\langle\sigma,\pi\rangle$ یک زیرگروه مرتبه‌ی mn از $\operatorname{Aut} C$ است:

قضیه ۲۸.۴.۱۵. فرض کنید $\sigma = (۱\ ۲\ \cdots\ n)$ و $\pi(i) = iq \mod n$ و مرتبه‌ی ضربی q به پیمانه‌ی n برابر m باشد. در این صورت $\pi\sigma\pi^{-۱} = \sigma^q$ و $\pi^{-۱}\sigma\pi = \sigma^{q^{m-۱}}$. بنابراین $|\langle\sigma,\pi\rangle| = mn$.

اثبات. داریم $\pi^{-۱}(i) = q^{m-۱}i$. بنابراین

$$\begin{aligned}
(\pi\sigma\pi^{-۱})(i) &= \pi\sigma(q^{m-۱}i)\\
&= \pi(q^{m-۱}i + ۱)\\
&= q(q^{m-۱}i + ۱)\\
&= i + q \mod n\\
&= \sigma^q(i),\\
\pi^{-۱}\sigma\pi(i) &= \pi^{-۱}\sigma(iq)\\
&= \pi^{-۱}(iq + ۱) \mod n\\
&= q^{m-۱}(iq + ۱)\\
&= i + q^{m-۱}\\
&= \sigma^{q^{m-۱}}(i).
\end{aligned}$$

بنابراین $\pi\sigma\pi^{-۱} = \sigma^q$ و $\pi^{-۱}\sigma\pi = \sigma^{q^{m-۱}}$.
در نتیجه $\pi\sigma^i\pi^{-۱} = \sigma^{iq}$ و $\pi^{-۱}\sigma^i\pi = \sigma^{iq^{m-۱}}$ و $\pi^{-k}\sigma^i\pi^k = \sigma^{iq^{k(m-۱)}}$. بنابراین $\sigma^i\pi^k = \pi^k\sigma^{iq^{(m-۱)}}$. و هر عضو $\langle\sigma,\pi\rangle$ به صورت یکتای $\pi^i\sigma^j$، $۱ \le i \le m$، $۱ \le j \le n$، نوشته می‌شود. بنابراین $|\langle\sigma,\pi\rangle| = mn$. □

اگر a و n دو عدد طبیعی باشند، جایگشت $\mu_a \in S_n$ را با $\mu_a(i) = ai \mod n$ تعریف می‌کنیم. اگر $\gcd\{a,n\} = ۱$، μ_a هر کد دوری را به یک کد دوری تصویر می‌کند حال نشان می‌دهیم ضرب چندجمله‌ای‌ها را نیز حفظ می‌کند:

قضیه ۲۹.۴.۱۵. فرض کنید $\gcd\{a,n\} = ۱$. جایگشت μ_a که به صورت

$$\mu_a(i) = ai \mod n$$

تعریف می‌شود، ضرب چندجمله‌ای‌ها در V_n را حفظ می‌کند.

اثبات. فرض کنید $u(x) = \sum_{j=۰}^{n-۱} b_jx^j$ و $v(x) = \sum_{j=۰}^{n-۱} c_jx^j$. در این صورت $u(x)v(x) = \sum_{j=۰}^{n-۱}\sum_{k=۰}^{j} b_kc_{n-۱-k}x^j$ بنابراین

$$\begin{aligned}
\mu_a(u(x))\mu_a(v(x)) &= \left(\sum_{j=۰}^{n-۱} b_jx^{aj}\right)\left(\sum_{j=۰}^{n-۱} c_jx^{aj}\right)\\
&= \sum_{j=۰}^{n-۱}\sum_{k=۰}^{j} b_kc_{n-۱-k}(x^a)^j\\
&= \mu_a(u(x)v(x)).
\end{aligned}$$

□

نتیجه ۳۰.۴.۱۵. اگر μ_a کد دوری C با عضو خودتوان مولد $e(x)$ را به یک کد C_1 تصویر کند، آنگاه C_1 دوری با عضو خودتوان $\mu_a(e(x))$ است. □

تمرین‌ها

در هر جا لازم باشد می‌توانید برای انجام محاسبات از GAP استفاده کنید.

۱. فرض کنید G ماتریس $[۵, ۳]$- کد خطی روی $\mathbb{Z}_۳$ باشد:

$$G = \begin{bmatrix} ۲ & ۱ & ۱ & ۰ & ۰ \\ ۱ & ۱ & ۰ & ۲ & ۰ \\ ۰ & ۰ & ۲ & ۱ & ۱ \end{bmatrix}$$

ماتریس امتحان توازن کد را بیابید. آیا این کد دوری است؟

۲. چه تعداد $[۸, k]$- کد دوتایی دوری برای $k = ۱, ۲, \ldots, ۷$ وجود دارد؟ چه تعداد $[۱۰, k]$- کد دوری روی $\mathbb{Z}_۳$ وجود دارد؟

۳. نشان دهید $[۴, ۲, ۳]$- کد همینگ روی $\mathbb{Z}_۳$ دوری نیست.

۴. چندجمله‌ای مولد $[۱۷, ۹, ۵]$- کد همینگ دوتایی را بیابید.

۵. چندجمله‌ای مولد $[۹, ۷]$- کد همینگ روی $\mathrm{GF}(۸)$ را بیابید.

۶. نشان دهید $[۲۱, ۱۸]$- کد همینگ روی $\mathrm{GF}(۴)$ دوری نیست.

۷. نشان دهید کدهای همینگ به طول $n = \dfrac{q^m - ۱}{q - ۱}$ روی $\mathrm{GF}(۹)$ دوری هستند اگر و تنها اگر $\gcd\{m, q - ۱\} = ۱$.

۸. فرض کنید $n = \dfrac{q^m - ۱}{q - ۱}$ و a یک ریشه‌ی nام اولیه‌ی واحد در $\mathrm{GF}(q^m)$ باشد، $m \geq ۲$، و

$$H = \begin{bmatrix} ۱ & a & a^۲ & \cdots & a^{n-۱} \end{bmatrix}.$$

نشان دهید مجموعه‌ی جواب دستگاه $Hu^\top = ۰$ یک کد دوری روی $\mathrm{GF}(q)$ با فاصله‌ی می‌نیمم ۳ است اگر و تنها اگر $\gcd\{m, q - ۱\} = ۱$.

۹. همه‌ی کد واژه‌های یک کد دوری با مولد $g(x) = ۱ + x + x^۳$ روی $\mathbb{Z}_۲$ را بیابید. اگر طول واژه‌های پیام برابر ۴ باشد، خطای کدام یک از واژه‌های دریافت شده‌ی ۱۰۰۰۱۱، ۰۱۱۰۰۱۱، و ۱۰۰۰۰۱۱ قابل کشف است.

۱۰. ماتریس امتحان توازن و مولد کد دوری تولید شده توسط $g(t) = ۱ + t + t^۴$ روی $\mathbb{Z}_۲$ را بیابید.

۱۱. جدول پیشروی هم‌مجموعه‌ها و سندرُم‌های $[۳, ۱]$- کد دوتایی تولید شده توسط $g(t) = ۱ + t + t^۲$ را بیابید.

۱۲. جدول پیشروی هم‌مجموعه‌ها و سندرُم‌های $[۷, ۳]$- کد دوتایی تولید شده توسط $g(t) = ۱ + t^۲ + t^۳ + t^۴$ را بیابید.

۱۳. فرض کنید $f(x) = b_۰ + b_۱x + \cdots + b_{k-۱}x^{k-۱} \in \mathbb{Z}_۲[x]$ طوری باشد که $f(x)|(x^n - ۱)$. نشان دهید

$$C = \left\{ (a, a_۱, \ldots, a_{n-۱}) \;\middle|\; \sum_{j=۰}^{k} a_{i+k-j} b_j = ۰,\ i = ۰, ۱, \ldots, n - k + ۱ \right\}$$

یک $[n, k]$- کد خطی دوری روی $\mathbb{Z}_۲$ است.

۱۴. نشان دهید کد دوری تولید شده توسط $g(t) = ۱ + t + t^۲ + t^۴$ با $[۸, ۴]$- کد همینگ تعمیم یافته معادل است. $d_{\min}$ را بیابید.

۱۵. فرض کنید C یک کد خطی دوتایی باشد که $C \subseteq C^\perp$. نشان دهید وزن هر کد واژه زوج است. به علاوه اگر ۴ وزن هر سطر ماتریس مولد را عاد کند، آنگاه وزن هر کد واژه را نیز عاد می‌کند.

۱۶. اگر C_1 و C_2 دو کد دوری با مولدهای $g_1(x)$ و $g_2(x)$ باشند، نشان دهید
(الف) $C_1 \cap C_2$ کد دوری با مولد $\{\text{lcm}\{g_1(x), g_2(x)\}$ است.
(ب) $C_1 + C_2$ کد دوری با مولد $\{\gcd\{g_1(x), g_2(x)\}$ است.
(ج) C_1C_2 کد دوری با مولد $\{\gcd\{g_1(x)g_2(x), x^n - 1\}$ است.

۵.۱۵ کدهای BCH

رده‌ی مهمی از کدهای دوری را باوس و چادوری در سال ۱۹۶۰ و مستقل از این دو هاکوئنگوم در سال ۱۹۵۹ کشف کردند. این کد هم اکنون BCH نامیده می‌شود.

تعریف ۱.۵.۱۵. کد دوری به طول n روی $\text{GF}(q)$ را کد BCH با فاصله‌ی طرح δ گوییم هرگاه مولد آن برابر کوچک‌ترین مضرب مشترک چندجمله‌ای‌های می‌نیمال a^ℓ، $a^{\ell+1}$، ...، $a^{\ell+\delta-2}$ باشد، که در آن ℓ یک عدد ثابت و $a \in \text{GF}(q^m)$ یک ریشه‌ی nام اولیه‌ی واحد است. در صورتی که $n = q^m - 1$، یعنی a عضو اولیه‌ای از $\text{GF}(q^m)$ باشد، کد BCH را اولیه گوییم.

فرض کنید a عضو اولیه‌ای از $\text{GF}(q^m)$ و ریشه‌ی nام اولیه‌ی واحد باشد، که در آن $n = q^m - 1$. فرض کنید به ازای هر $\ell \le i \le \ell + \delta - 2$، $f_i(x) \in \text{GF}(q)[x]$ چندجمله‌ای می‌نیمال a^i و $g(x)$ کوچک‌ترین مضرب مشترک آن‌ها باشد. کد BCH C با چندجمله‌ای مولد $g(x)$ را در نظر می‌گیریم. در این صورت

$$C = \{u \in V_n \mid u(a^i) = 0 \ , \ \ell \le i \le \ell + \delta - 2\}.$$

برعکس اگر C به صورت فوق باشد، آنگاه C یک کد BCH است.
اکنون ماتریس

$$H = \begin{bmatrix} 1 & a^\ell & a^{2\ell} & \cdots & a^{(n-1)\ell} \\ 1 & a^{\ell+1} & a^{2(\ell+1)} & \cdots & a^{(n-1)(\ell+1)} \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ 1 & a^{\ell+\delta-2} & a^{2(\ell+\delta-2)} & \cdots & a^{(n-1)(\ell+\delta-2)} \end{bmatrix}$$

را در نظر می‌گیریم. فرض کنید $u = (u_0, u_1, \ldots, u_{n-1})$، در این صورت

$$\begin{aligned} Hu^\top = 0 &\iff \sum_{i=0}^{n-1} a^{ij} u_i = 0, \quad j = \ell, \ell+1, \ldots, \ell+\delta-2 \\ &\iff u(a^j) = 0, \quad j = \ell, \ell+1, \ldots, \ell+\delta-2. \end{aligned}$$

بنابراین C یک کد BCH است اگر و تنها اگر ماتریس امتحان توازن آن ماتریس H به صورت بالا باشد.

قضیه ۲.۵.۱۵. فاصله‌ی می‌نیمم کد BCH با فاصله‌ی طرح δ، حداقل δ است.

اثبات. بدون کم شدن از کلیت فرض می‌کنیم $\ell = 1$. بنا به لم ۱۵.۴.۱۵، درجه‌ی چندجمله‌ای ماتسون- سولومون هر کد واژه‌ی u حداکثر $n - \delta$ است. بنابراین در قضیه‌ی ۱۷.۴.۱۵، داریم $r \le n - \delta$ یعنی $\text{wt}(u) \ge \delta$. □

قضیه‌ی فوق به کران BCH معروف است. اثبات دیگری از قضیه‌ی فوق را می‌توان به صورت زیر ارائه کرد: باید نشان دهیم هر $\delta - 1$ ستون H مستقل خطی‌اند. $\delta - 1$ ستون دلخواه H را انتخاب کرده و فرض می‌کنیم اولین عضو هر ستون به ترتیب $a^{\ell_{i_1}}, a^{\ell_{i_2}}, \ldots, a^{\ell_{i_{\delta-1}}}$ باشند. پس دترمینان ماتریس $(\delta - 1) \times (\delta - 1)$ حاصلضرب را در نظر می‌گیریم. می‌توانیم از $a^{\ell_{i_k}}$، $k = 1, 2, \ldots, \delta - 1$، فاکتور

بگیریم و به دست بیاوریم

$$a^{\ell(i_۱+\cdots+i_{\delta-۱})}\begin{vmatrix} ۱ & ۱ & \cdots & ۱ \\ a^{i_۱} & a^{i_۲} & \cdots & a^{i_{\delta-۱}} \\ \vdots & & & \\ a^{(\delta-۲)i_۱} & a^{(\delta-۲)i_۲} & \cdots & a^{(\delta-۲)i_{\delta-۱}} \end{vmatrix} = a^{\ell(i_۱+\cdots+i_{\delta-۱})}\prod_{۱\le k<j\le \delta-۱}(a^{i_j}-a^{i_k}) \neq ۰.$$

دترمینان فوق به دترمینان واندرموند معروف است و به استقرا می‌توان ثابت کرد که مقدار آن برابر مقدار داده شده در بالا است (تمرین ۱۰ را ببینید)، و بنابراین ناصفر است. پس $\delta - ۱$ ستون انتخاب شده مستقل خطی‌اند و فاصله‌ی می‌نیمم حداقل δ است. پیدا کردن فاصله‌ی می‌نیمم یک کد BCH در حالت کلی دشوار است. اما در برخی حالت‌ها مثلاً کدهای BCH اولیه‌ی دوتایی می‌توانیم فاصله‌ی می‌نیمم را بیابیم. ابتدا یک لم ثابت می‌کنیم. در زیر $\mathrm{GF}(۲^k)$ را با فضای برداری $\mathbb{Z}_۲^k$ یکی در نظر می‌گیریم.

لم ۳.۵.۱۵. فرض کنید U زیرفضایی از $\mathbb{Z}_۲^k$ با بُعد ℓ باشد. اگر کمتر از ℓ تا ۱ در بسط دودوئی i وجود داشته باشد، آنگاه $\sum_{a\in U} a^i = ۰$.

اثبات. به استقرا روی ℓ عمل می‌کنیم. حالت $\ell = ۱$ بدیهی است. فرض کنید ادعا برای ℓ درست باشد و V را یک زیرفضای $\mathbb{Z}_۲^k$ با بُعد $\ell + ۱$ در نظر بگیرید. در این صورت $V = U \cap (U + b)$ که در آن U یک زیرفضای ℓ بُعدی است. داریم

$$\begin{aligned}\sum_{a\in V} a^i &= \sum_{a\in V} a^i + \sum_{a\in U}(a+b)^i \\ &= \sum_{a\in U}\sum_{j=۰}^{i}\binom{i}{j}a^j b^{i-j} \\ &= \left(\sum_{a\in U} a^j\right)\left(\sum_{j=۰}^{i-۱} b^{i-j}\right).\end{aligned}$$

اگر دو بسط دودویی i حداکثر ℓ تا ۱ وجود داشته باشد، بنا به تذکر زیر ضرایب دوجمله‌ای $\binom{i}{j}$ برای $j < i$، برابر صفر است، مگر آن که بسط دودویی j کمتر از ℓ تا ۱ داشته باشد، که در آن حالت بنا به فرض استقرا $\sum_{a\in U} a^j = ۰$. □

برای اثبات قضیه بعدی ابتدا نکته‌ای را ثابت می‌کنیم. فرض کنید p عدد اول و

$$n = \sum_{i=۰}^{\ell} n_i p^i, \quad k = \sum_{i=۰}^{\ell} k_i p^i$$

بسط n و k در پایه p باشد (یعنی $p \le n_i \le p - ۱$، $۰ \le k_i \le p - ۱$). در این صورت

$$\binom{n}{k} = \prod_{i=۰}^{\ell}\binom{n_i}{k_i} \mod p$$

برای اثبات این مطلب، از رابطه‌ی $(۱ + x)^p \equiv ۱ + x^p \mod p$ استفاده می‌کنیم. اگر $۰ \le r \le p$، آنگاه

$$(۱ + x)^{ap+r} \equiv (۱ + x^p)^a(۱ + x)^r \mod p$$

با مقایسه ضرایب x^{bp+s} (که $۰ \le s < p$) از دو طرف تساوی به دست می‌آید

$$\binom{ap+r}{bp+s} \equiv \binom{a}{b}\binom{r}{s} \mod p$$

و بنابراین نتیجه به استقرا ثابت می‌شود. □

قضیه ۴.۵.۱۵. اگر C یک کد اولیه BCH به طول $n = ۲^m - ۱$ و فاصله‌ی طرح $\delta = ۲^\ell - ۱$ باشد، آنگاه فاصله‌ی می‌نیمم C برابر δ است.

اثبات. فرض کنید U یک زیرفضای ℓ بُعدی $\mathbb{Z}_۲^m$ باشد. بردار u را در نظر بگیرید که آن دقیقاً در مکان‌های متناظر عناصر ناصفر U باشند، یعنی

$$u(t) = \sum_{j;\alpha^j \in U - \{۰\}} t^j.$$

فرض کنید $۱ \le i \le ۲^\ell - ۱$، در این صورت بسط دودویی i کمتر از ℓ تا ۱ دارد. به علاوه $u(a^i) = \sum_{a \in U} a^i$. بنابراین بنا به بحث قبل از قضیه، $u(a^i) = ۰$، $۱ \le i \le ۲^{\ell-\delta} - ۱$. یعنی $u(t)$ یک کد واژه در C است. □

نتیجه ۵.۵.۱۵. فاصله‌ی می‌نیمم یک کد BCH با فاصله‌ی طرح δ کوچکتر یا مساوی $۲\delta - ۱$ است.

اثبات. در قضیه‌ی قبل فرض کنید ℓ طوری باشد که $۲^{\ell-۱} \le \delta \le ۲^\ell - ۱$. کد قضیه‌ی قبل یک زیرکد (زیرفضا) با فاصله‌ی طرح δ است. □

رده خاصی از کدهای BCH کدهای RS هستند.

تعریف ۶.۵.۱۵. یک کد رید- سولومون (یا کد RS) یک کد BCH با فاصله‌ی طرح δ و طول $n = q - ۱$ روی $\mathrm{GF}(q)$ است.

اگر در تعریف کد BCH قرار دهیم $\ell = m = ۱$، چندجمله‌ای مولد کد RS به دست می‌آید، که در آن a عضو اولیه‌ای از $\mathrm{GF}(q)$ است:

قضیه ۷.۵.۱۵. فاصله‌ی می‌نیمم یک کد RS با چندجمله‌ای مولد

$$g(x) = \prod_{i=۱}^{\delta-۱} (x - a^i),$$

برابر δ است.

اثبات. بنا به قضیه‌ی ۲.۵.۱۵، $d_{\min} \ge \delta$. اگر یک کد خطی به طول n و بُعد k را در نظر بگیریم و مجموعه‌ی همه‌ی کد واژه‌های با $k - ۱$ ریشه یک زیر کد با بُعد حداقل ۱ و فاصله‌ی می‌نیمم حداکثر $n - k + ۱$ است. به ویژه این مطلب برای کد RS داده شده درست است که بُعد آن برابر $k = n + ۱ - d$ است. □

مثال ۸.۵.۱۵. فرض کنید $\ell = ۱$، $\delta = ۳$، و $n = ۲^m - ۱$. اگر $a \in \mathrm{GF}(۲^m)$ یک عضو اولیه با چندجمله‌ای مولد $g(x) \in \mathbb{Z}_۲[x]$ باشد و $\deg g(x) = m$، آنگاه $C = (g(t))$ یک کد BCH با فاصله‌ی طرح $\delta = ۳$ به طول n، و به علاوه یک کد همینگ دوتایی با m حرف امتحان است. □

مثال ۹.۵.۱۵. فرض کنید $q = ۲$، $n = ۱۵$، $\delta = ۵$ و $\ell = ۱$. کد BCH، C به طول ۱۵ روی $\mathbb{Z}_۲$ با فاصله‌ی طرح $\delta = ۵$ را می‌سازیم. فرض کنید $a \in \mathrm{GF}(۱۶) \cong \mathbb{Z}_۲^۴$ یک ریشه‌ی اولیه‌ی واحد باشد، آنگاه a، $a^۲$، و $a^۴$ ریشه‌های چندجمله‌ای اولیه‌ی $x^۴ + x + ۱$ روی $\mathbb{Z}_۲$ هستند. هم‌چنین $x^۴ + x^۳ + x^۲ + x + ۱$ چندجمله‌ای می‌نیمال $a^۳$ روی $\mathbb{Z}_۲$ است. بنابراین چندجمله‌ای

$$\begin{aligned} g(x) &= (x^۴ + x + ۱)(x^۴ + x^۳ + x^۲ + x + ۱) \\ &= ۱ + x^۴ + x^۶ + x^۷ + x^۸ \end{aligned}$$

چندجمله‌ای مولد کد BCH با فاصله‌ی طرح $\delta = ۵$ است؛ زیرا $\ell - \delta - ۲ = ۴$، و $g(x)$ کوچک‌ترین مضرب مشترک چندجمله‌ای‌های می‌نیمال اعضای a^i، $۴ \le i \le ۱$، است. بُعد کد C برابر $k = ۱۵ - \deg g(x) = ۷$ و ماتریس امتحان توازن کد C برابر است با

$$H = \begin{bmatrix} ۱ & a & a^۲ & \cdots & a^{۱۳} & a^{۱۴} \\ ۱ & a^۳ & a^۶ & \cdots & a^{۳۹} & a^{۴۲} \end{bmatrix}$$

بنابراین C یک $[۱۵, ۷]$- کد با چندجمله‌ای امتحان توازن

$$h(x) = \frac{x^{۱۵} - ۱}{g(x)} = ۱ + x^{۴} + x^{۶} + x^{۷}$$

است. توجه کنید سندرُم واژه‌ی $u(t) = a_{۰} + a_{۱}t + \cdots + a_{n-۱}t^{n-۱}$ برابر

$$\begin{aligned} S(u) &= Hu^{\top} \\ &= \begin{bmatrix} ۱ & a & a^{۲} & \cdots & a^{۱۳} & a^{۱۴} \\ ۱ & a^{۳} & a^{۶} & \cdots & a^{۳۹} & a^{۴۲} \end{bmatrix} [a_{۰}\ a_{۱}\ \cdots\ a_{n-۱}]^{\top} \\ &= [u(a)\ u(a^{۳})] \end{aligned}$$

است. اگر با استفاده از رابطه‌ی $a^{۴} + a + ۱ = ۰$، توان‌های a را بر حسب ترکیب خطی از $a^{۳}$، $a^{۲}$، a، ۱ بنویسیم، بردارهای دودویی به طول ۴ به دست خواهند آمد، که در جدول ۴ در مثال ۹.۴.۱۵، نشان داده شده است. توجه کنید چون $a^{۱۵} = ۱$، با استفاده از جدول ۴، توان‌های دیگر مثل

$$a^{۱۸} = a^{۳}, a^{۲۱} = a^{۶}, a^{۲۴} = a^{۹}, \ldots$$

را می‌توان یافت. بنابراین نمایش ماتریس H به صورت دودوئی به دست می‌آید:

$$H = \begin{bmatrix} ۱ & ۰ & ۰ & ۰ & ۱ & ۰ & ۰ & ۱ & ۱ & ۰ & ۱ & ۰ & ۱ & ۱ & ۱ \\ ۰ & ۱ & ۰ & ۰ & ۱ & ۱ & ۰ & ۱ & ۰ & ۱ & ۱ & ۱ & ۱ & ۰ & ۰ \\ ۰ & ۰ & ۱ & ۰ & ۰ & ۱ & ۱ & ۰ & ۱ & ۰ & ۱ & ۱ & ۱ & ۱ & ۰ \\ ۰ & ۰ & ۰ & ۱ & ۰ & ۰ & ۱ & ۱ & ۰ & ۱ & ۰ & ۱ & ۱ & ۱ & ۱ \\ ۱ & ۰ & ۰ & ۰ & ۱ & ۱ & ۰ & ۰ & ۰ & ۱ & ۱ & ۰ & ۰ & ۰ & ۱ \\ ۰ & ۰ & ۰ & ۱ & ۱ & ۰ & ۰ & ۰ & ۱ & ۱ & ۰ & ۰ & ۰ & ۱ & ۱ \\ ۰ & ۰ & ۱ & ۰ & ۱ & ۰ & ۰ & ۱ & ۰ & ۱ & ۰ & ۰ & ۱ & ۰ & ۱ \\ ۰ & ۱ & ۱ & ۱ & ۱ & ۰ & ۱ & ۱ & ۱ & ۱ & ۰ & ۱ & ۱ & ۱ & ۱ \end{bmatrix}$$

ماتریس مولد C که سطرهای آن متناظر $g(t)$، $tg(t)$، ...، $t^{۶}g(t)$ است عبارت است از

$$G = \begin{bmatrix} ۱ & ۰ & ۰ & ۰ & ۱ & ۰ & ۱ & ۱ & ۱ & ۰ & ۰ & ۰ & ۰ & ۰ & ۰ \\ ۰ & ۱ & ۰ & ۰ & ۰ & ۱ & ۰ & ۱ & ۱ & ۱ & ۰ & ۰ & ۰ & ۰ & ۰ \\ ۰ & ۰ & ۱ & ۰ & ۰ & ۰ & ۱ & ۰ & ۱ & ۱ & ۱ & ۰ & ۰ & ۰ & ۰ \\ ۰ & ۰ & ۰ & ۱ & ۰ & ۰ & ۰ & ۱ & ۰ & ۱ & ۱ & ۱ & ۰ & ۰ & ۰ \\ ۰ & ۰ & ۰ & ۰ & ۱ & ۰ & ۰ & ۰ & ۱ & ۰ & ۱ & ۱ & ۱ & ۰ & ۰ \\ ۰ & ۰ & ۰ & ۰ & ۰ & ۱ & ۰ & ۰ & ۰ & ۱ & ۰ & ۱ & ۱ & ۱ & ۰ \\ ۰ & ۰ & ۰ & ۰ & ۰ & ۰ & ۱ & ۰ & ۰ & ۰ & ۱ & ۰ & ۱ & ۱ & ۱ \end{bmatrix}$$

بنا به قضیه‌ی ۲.۵.۱۵ داریم

$$d_{\min} \geq \delta = ۵ = ۲ \times ۲ + ۱,$$

در نتیجه بنا به قضیه‌ی ۴.۲.۱۵، کد C تصحیح کننده‌ی ۲ خطاست. □

مثال ۱۰.۵.۱۵. فرض کنید $n = ۵$ و a عضو اولیه‌ای از $\mathrm{GF}(۹)$ با چندجمله‌ای می‌نیمال $x^{۲} - x - ۱$ روی $\mathbb{Z}_{۳}$ باشد. در این صورت چندجمله‌ای می‌نیمال $a^{۲}$ برابر $x^{۲} + ۱$ و چندجمله‌ای می‌نیمال $a^{۳}$ برابر $x^{۲} - x - ۱$ است. چندجمله‌ای می‌نیمال یک کد BCH با فاصله‌ی طرح $\delta = ۴$ به طول ۸ و بُعد ۴ روی $\mathbb{Z}_{۳}$ عبارت است از

$$g(x) = (x^{۲} - x - ۱)(x^{۲} + ۱) = x^{۴} - x^{۳} - x - ۱.$$ □

مثال ۱۱.۵.۱۵. فرض کنید $q = ۲$، $n = ۲۳$، $\delta = ۵$. اگر قرار دهیم

$$f_۰(x) = x^{۱۱} + x^۹ + x^۷ + x^۶ + x^۵ + x^۴ + x + ۱, \quad f_۱(x) = x^{۱۱} + x^{۱۰} + x^۶ + x^۵ + x^۲ + ۱,$$

آنگاه $x^{۲۳} - ۱ = (x-۱)f_۰(x)f_۱(x)$ تجزیه‌ای به عوامل تحویل‌ناپذیر روی $\mathbb{Z}_۲$ است. ریشه‌های این چندجمله‌ای‌ها در $\mathrm{GF}(۲^{۱۱})$ قرار دارند و همگی ریشه‌های ۲۳ام اولیه‌ی واحد روی $\mathbb{Z}_۲$ هستند ، زیرا $۸۹ \times ۲۳ = ۲^{۲۳} - ۱$. اگر a یکی از این ریشه‌ها باشد، آنگاه مزدوج‌های آن عبارت‌اند از a^j، $j = ۱, ۲, ۴, ۸, ۱۶, ۹, ۱۸, ۱۳, ۳, ۶, ۱۲$. هر دو کد دوری در $\mathbb{Z}_۲^{۲۳}$ که توسط چندجمله‌ای‌های تحویل‌ناپذیر $f_۰(x)$، $f_۱(x)$ تولید می‌شوند، کدهای BCH با بُعد ۱۲ و فاصله‌ی طرح $\delta = ۵$ هستند. این کدها را کدهای گولای دوتایی می‌نامیم. □

اکنون کد گشایی کدهای BCH را بررسی می‌کنیم. فرض کنید C یک کد BCH با مولد $g(t)$ روی $\mathrm{GF}(q)^n$ و فاصله‌ی طرح $\delta = ۲s+۱$ باشد. فرض کنید a یک ریشه‌ی nام اولیه‌ی واحد روی $\mathrm{GF}(q^m)$، و $g(x)$ برابر کوچک‌ترین مضرب مشترک چندجمله‌ای‌های مینیمال a، $a^۲$، ...، $a^{۲s} = a^{\delta-۱}$، باشد (در این‌جا $\ell = ۱$)، در این صورت

$$v(t) \in C \iff u(a^i) = ۰, \quad \ell \le j \le \ell + \delta - ۲.$$

اگر واژه‌ی $v(t)$ فرستاده شده و واژه‌ی

$$u(t) = a_۰ + a_۱t + \cdots + a_{n-۱}t^{m-۱}$$

دریافت شده باشد، قرار می‌دهیم

$$e(t) = u(t) - v(t) = e_۰ + e_۱t + \cdots + e_{n-۱}t^{n-۱}$$

هدف ما یافتن $e(t)$ و در نتیجه $v(t)$ است. تعریف می‌کنیم

$M = \{i \mid e_i \neq ۰\}$	مکان‌هایی که خطا رخ داده
$E = \lvert M \rvert$	تعداد خطاها
$\sigma(z) = \prod_{i \in M}(۱ - a^i z)$	چندجمله‌ای مکان نمای خطا

$$w(z) = \sum_{i \in M} e_i a^i z \prod_{j \in M - \{i\}} (۱ - a^i z) = \sum_{i \in M} e_i a^i z \frac{\sigma(z)}{۱ - a^i z}$$

توجه کنید که خطا در مکان rام رخ داده اگر و تنها اگر $r \in M$ اگر و تنها اگر $\sigma(a^{-r}) = ۰$. در این حالت

$$e_r = \frac{-w(a^{-r})a^r}{\sigma'(a^{-r})},$$

زیرا

$$\frac{\sigma'(z)}{\sigma(z)} = -\sum_{i \in M} \frac{a^i}{۱ - a^i z} \ , \ \sigma'(z) = -\sum_{i \in M} a^i \frac{\sigma(z)}{۱ - a^i z},$$

که نتیجه می‌دهد

$$\begin{aligned} e_r\sigma(a^{-r}) &= -e_r \sum_{i \in M} a^i \frac{\sigma(a^{-r})}{۱ - a^i a^{-r}} \\ &= -e_r a^r \prod_{j \in M - \{r\}} (۱ - a^i a^{-r}) \\ &= -w(a^{-r})a^r. \end{aligned}$$

بنابراین اگر $\sigma(z)$ و $w(z)$ را بیابیم می‌توانیم خطاها را کشف و تصحیح کنیم. از حالا به بعد فرض می‌کنیم $E \leq s$ (در غیر این صورت انتظار نمی‌رود که بتوانیم خطاها را تصحیح کنیم) ملاحظه می‌کنیم که

$$\begin{aligned}\frac{w(z)}{\sigma(z)} &= \sum_{i\in M} \frac{e^i z}{1 - a^i z} \\ &= \sum_{i\in M} e_i \sum_{j=1}^{\infty} (a^i z)^j \\ &= \sum_{j=1}^{\infty} z^j \sum_{i\in M} e_i a^{ij} \\ &= \sum_{j=1}^{\infty} z^j e(a^j),\end{aligned}$$

که در آن همه‌ی محاسبه‌ها در $\mathrm{GF}(q^m)$ انجام می‌شود. به ازای $1 \leq j \leq 2s$، چون $v(t) \in C$، داریم

$$u(a^j) - e(a^j) = v(a^j) = 0 \qquad (۵)$$

بنابراین $u(a^j) = e(a^j)$، $1 \leq j \leq 2s$. یعنی دریافت کننده‌ی پیام اولین $2s$ ضرایب را از سمت راست می‌داند. پس $w(z)/\sigma(z)$ به پیمانه‌ای z^{2s+1} معلوم است. ادعا می‌کنیم که دریافت کننده باید چندجمله‌ای‌های $\sigma(z)$، $w(z)$ را طوری تعیین کند که $\deg w(z) \leq \deg \sigma(z)$ و $\deg \sigma(z)$ کوچک‌ترین مقدار ممکن نسبت به شرط

$$\frac{w(z)}{\sigma(z)} = \sum_{j=1}^{2s} z^j u(a^j) \mod z^{2s+1}$$

را داشته باشد. فرض کنید $S_j = u(a^j)$، به ازای هر $j = 1, 2, \ldots, 2s$، و قرار دهید $\sigma(z) = \sum_{i=0}^{E} \sigma_i z^i$. در این صورت داریم

$$\begin{aligned}w(z) &= \left(\sum_{j=1}^{2s} S_j z^j\right)\left(\sum_{i=0}^{E} \sigma_i z^i\right) \\ &\equiv \sum_k \left(\sum_{i+j=k} S_j \sigma_i\right) z^k \mod z^{2s+1}\end{aligned}$$

چون $\deg w(z) \leq E$ داریم

$$\sum_{i+j=k} S_j \sigma_i = 0, \quad E+1 \leq k \leq 2s \qquad (۶)$$

دستگاه اخیر یک دستگاه معادله متشکل از $2s - E$ معادله‌ی خطی با E مجهول σ_1، ...، σ_E است (می‌دانیم $\sigma_0 = 1$). فرض کنید $\hat{\sigma}(z) = \sum_{i=0}^{E} \hat{\sigma}_i z^i$ (که در آن $\hat{\sigma}_0 = 1$) چندجمله‌ای با کوچک‌ترین درجه باشد که از حل دستگاه فوق حاصل می‌شود (می‌دانیم حداقل یک جواب $\sigma(z)$ وجود دارد). برای $E+1 \leq k \leq 2s$ داریم

$$\begin{aligned}0 &= \sum_j S_{k-1} \hat{\sigma}_j \\ &= \sum_{i\in M} \sum_j e_i a^{(k-j)i} \hat{\sigma}_j \\ &= \sum_{i\in M} e_i a^{ik} \hat{\sigma}(\hat{a}^i).\end{aligned}$$

می‌توانیم طرف راست معادلات فوق را به عنوان یک دستگاه معادله‌ی خطی با مجهولات $e_i\hat{\sigma}(a^{-i})$ و ضرایب a^{ik} تصور کنیم. اگر $M=\{i_۱,\dots i_r\}$، دترمینان ماتریس ضرایب عبارت است از

$$\begin{vmatrix} a^{i_۱} & a^{i_۲} & \cdots & a^{i_r} & \\ a^{۲i_۱} & a^{۲i_۲} & \cdots & a^{۲i_r} & \\ \vdots & \vdots & \cdots & \vdots & \vdots \\ a^{۲si_۱} & a^{۲si_۲} & \cdots & a^{۲si_r} & \end{vmatrix},$$

و با فاکتورگیری از a^{ij} از ستون jام یک دترمینان واندرموند به دست می‌آید، که ناصفر است. پس به ازای هر $i\in M$، $e_i\hat{\sigma}(a^{-i})=۰$. چون برای $i\in M$، $e_i\neq ۰$، می‌بینیم که $\hat{\sigma}(a^{-i})=۰$. بنابراین $\sigma(z)|\hat{\sigma}(z)$. پس $\sigma(z)=\hat{\sigma}(z)$. بنابراین دو واقع، جواب $\hat{\sigma}(z)$ از کوچک‌ترین درجه مساله‌ی ما را حل می‌کند و هم‌چنین که دیدیم یافتن آن به حل یک دستگاه معادلات خطی بستگی دارد. مزیت این روش این است که کد گشا یک الگوریتم که به E بستگی ندارد در اختیار دارد. البته در عمل حتی بسیار مهم‌تر است که یک الگوریتم سریع بیابیم که مطالبی که با دیدگاه نظری در نظر گرفتیم عملاً انجام دهد. چنین الگوریتمی (همراه با پیاده سازی) در کتاب مرجع [۱] مطرح شده است و غالباً آن‌را کد گشایی برلکمپ می‌نامند.

مثال ۱۲.۵.۱۵. BCH کد دوتایی C به طول ۵۱ با $\ell=۱$ و فاصله‌ی طرح $\delta=۵$ را که تصحیح کننده‌ی دو خطا است و در مثال ۹.۵.۱۵، ساخته شد را در نظر بگیرید. فرض کنید واژه‌ی $u=۱۰۰۱۰۰۱۱۰۰۰۱۰۰$ دریافت شده باشد. u را به صورت چندجمله‌ای می‌نویسیم

$$u(t)=۱+t^{۳}+t^{۶}+t^{۷}+t^{۱۲}.$$

بنا به قضیه‌ی ۲.۵.۱۵، $d_{\min}\geq\delta=۵=۲\times۲+۱$، در نتیجه بنا به قضیه‌ی ۴.۲.۱۵، C تصحیح کننده‌ی ۲ خطاست. مطابق بحث قبل قرار می‌دهیم (بنا به معادلات ۵، برای $۱\leq i\leq ۲s=۴$، داریم $u(a^i)=e(a^i)$)

$$\begin{aligned} S_۱ &= e(a)=u(a)=۱,\\ S_۲ &= e(a^{۲})=u(a^{۲})=۱+a^{۳}+a^{۶}+a^{۱۴}+a^{۲۴}=۱\\ S_۳ &= e(a^{۳})=u(a^{۳})=a\\ S_۴ &= e(a^{۴})=u(a^{۴})=۱ \end{aligned}$$

باید دستگاه زیر (دستگاه معادلات ۶) را حل کنیم

$$\begin{cases} S_۳\sigma_۰+S_۲\sigma_۱+S_۱\sigma_۲=۰\\ S_۴\sigma_۰+S_۳\sigma_۱+S_۲\sigma_۲=۰ \end{cases}$$

چون $S_۱=S_۲=S_۴=۱$ و $S_۳=a$ دستگاه اخیر به صورت زیر می‌آید

$$\begin{cases} \sigma_۱+\sigma_۲=a^{۴}\\ a^{۴}\sigma_۱+\sigma_۲=۱ \end{cases}$$

چون این دو معادله مستقل خطی‌اند، دو خطا رخ داده است، یعنی $E=۲$. با حل این دستگاه داریم $\sigma_۱=۱$ و $\sigma_۲=a$. با قرار دادن این مقادیر در $\sigma(z)$، و توجه به این که $\sigma_۰=۱$، به دست می‌آید $\sigma(z)=۱+z+az^{۲}$. ریشه‌های $\sigma(z)$، در $\mathrm{GF}(۱۶)$، که با سعی و خطا به دست می‌دهند، عبارت‌اند از $a^{۶}$ و $a^{۸}$. چون $a^{-۶}=a^{۹}$، پس خطا در مولفه‌های هشتم و دهم رخ داده است. یعنی $e(t)=t^{۷}+t^{۹}$. بنابراین واژه‌ی u را به صورت

$$\begin{aligned} w(t)=u(t)-e(t) &= (۱+t^{۳}+t^{۶}+t^{۷}+t^{۱۲})-(t^{۷}-t^{۹})\\ &= ۱+t^{۳}+t^{۶}+t^{۹}+t^{۱۲} \end{aligned}$$

کد گشایی می‌کنیم و کد واژه‌ی متناظر ۱۰۰۱۰۰۱۰۰۱۰۰۱۰۰ $= w$ است. پیام اولیه که با تقسیم چندجمله‌ای تصحیح شده $w(x)$ بر $g(x)$ به دست می‌آید عبارت است از

$$\frac{v(t)}{g(t)} = ۱ + t^۳ + t^۴,$$

که پیام واژه‌ی نظیر آن ۱۰۰۱۱۰۰ است. □

۶.۱۵ کدهای مانده‌ای درجه‌ی دوم

فرض کنید یک p عدد اول فرد باشد. مربعهای ناصفر به پیمانه‌ی p، یعنی اعداد $۱^۲$، $۲^۲$، $۳^۲$، ...، که به پیمانه‌ی p در نظر گرفته می‌شوند را ماندههای درجه‌ی دوم به پیمانه‌ی p یا مانده‌ها به پیمانه‌ی p می‌نامیم. برای یافتن مانده‌ها به پیمانه‌ی p کافی است که مربع اعداد از ۱ تا $\frac{p-۱}{۲}$ را در نظر بگیریم. در واقع چون

$$(p-a)^۲ \equiv (-a)^۲ \equiv a^۲ \mod p,$$

کافی است

$$۱^۲, ۲^۲, ۳^۲, \ldots, \left(\frac{p-۱}{۲}\right)^۲,$$

را به پیمانه‌ی p در نظر بگیریم. همه‌ی این عناصر متمایزند، زیرا اگر $i^۲ \equiv j^۲$، که در آن $۱ \le i, j \le \frac{۱}{۲}(p-۱)$، آنگاه $p|(i-j)(i+j)$، که تنها وقتی امکانپذیر است که $i = j$. بنابراین $\frac{۱}{۲}(p-۱)$ مانده‌ی درجه‌ی دوم به پیمانه‌ی p وجود دارد و $\frac{۱}{۲}(p-۱)$ اعداد دیگر به پیمانه‌ی p را نامانده گوییم. صفر نه مانده است و نه نامانده. مثلاً اگر $p = ۱۱$، آنگاه مانده‌ها به پیمانه‌ی ۱۱ عبارت‌اند از

$$۱^۲ = ۱, \quad ۲^۲ = ۴, \quad ۳^۲ = ۹, \quad ۴^۲ = ۱۶ \equiv ۵, \quad ۵^۲ = ۲۵ \equiv ۳.$$

نامانده‌ها ۲، ۶، ۷، ۸، و ۱۰ هستند.

به وضوح مجموعه‌ی مانده‌ها به پیمانه‌ی p تحت عمل ضرب یک زیرگروه $\mathbb{Z}_p^\times$ است؛ و حاصل‌ضرب دو مانده‌ی درجه‌ی دوم و یا دو نامانده، یک مانده‌ی درجه‌ی دوم است، هم‌چنین حاصل‌ضرب یک مانده‌ی درجه‌ی دوم در یک نامانده، یک نامانده است. به علاوه اگر $p = ۴k+۱$، آنگاه -۱ یک مانده‌ی درجه‌ی دوم به پیمانه‌ی p و اگر $p = ۴k+۳$، آنگاه -۱ یک نامانده به پیمانه‌ی p است (مثال ۱۰.۴.۱۱ از صفحه‌ی ۲۵۲ و تمرین ۹ از صفحه‌ی ۲۴۸ را ببینید).

اکنون تابع χ را که نماد لژاندر می‌نامیم به صورت زیر تعریف می‌کنیم

$$\chi(i) = \begin{cases} ۰ & i \text{ مضرب } p \\ ۱ & \text{باقیمانده‌ی تقسیم بر } p \text{ مانده باشد} \\ -۱ & \text{باقیمانده‌ی تقسیم بر } p \text{ نامانده باشد}. \end{cases}$$

قضیه ۱.۶.۱۵. به ازای هر c که $p \nmid c$ داریم

$$\sum_{j=۰}^{p-۱} \chi(j)\chi(j+c) = -۱.$$

اثبات. بنا به بحث قبل از قضیه داریم

$$\chi(ab) = \chi(a)\chi(b), \quad ۰ \le a, b \le p-۱.$$

جمله‌i متناظر $j = ۰$ برابر صفر است. اکنون فرض کنید $j \neq ۰$ و $b \equiv \frac{j+c}{j} \mod p$. به ازای هر j عدد صحیح یکتای b که $۰ \le b \le p-۱$ وجود دارد. چون j بین ۱ تا $p-۱$ تغییر می‌کند b مقادیر ۰، ۲، ...، $p-۱$ را اختیار می‌کند ولی ۱ را اختیار نمی‌کند.

بنابراین

$$\begin{aligned}\sum_{j=0}^{p-1}\chi(j)\chi(j+c) &= \sum_{j=0}^{p-1}\chi(j)\chi(jb)\\ &= \sum_{j=0}^{p-1}\chi(j)^2\chi(b)\\ &= \sum_{b=0,b\neq 1}^{p-1}\chi(b)\\ &= 0-\chi(1)=-1,\end{aligned}$$

که حکم را ثابت می‌کند. □

لم ۲.۶.۱۵. فرض کنید p عدد اول فرد باشد. در این صورت به ازای هر عدد صحیح a داریم ،

$$\chi(a)\equiv a^{\frac{1}{2}(p-1)} \mod p.$$

اثبات. اگر a مضربی از p باشد، حکم واضح است؛ پس فرض کنید $p\nmid a$. فرض کنید ξ یک عضو اولیه‌ی $\mathbb{Z}_p$ باشد ؛ پس $\xi^{\frac{1}{2}(p-1)}\equiv -1 \mod p$. اکنون به ازای یک i، $a\equiv \xi^i \mod p$ و بنابراین $a^{\frac{1}{2}(p-1)}\equiv (-1)^i \mod p$. چون a نامانده‌ی درجه‌ی دوم است اگر و تنها اگر i زوج باشد حکم واضح است. □

لم ۳.۶.۱۵. اگر p یک عدد اول فرد و μ تعداد عضوهای مجموعه‌ی اعداد a، $2a$، ...، $\frac{1}{2}(p-1)a$، باشد که کوچک‌ترین باقی‌مانده آن ها به پیمانه‌ی p منفی است. (مثلاً اگر $p=7$ و $a=2$، آنگاه مجموعه‌ی ۲، ۴، ۶، می‌شود ۲، ۳−، ۱؛ و $\mu=2$.) انگاه $\chi(a)=(-1)^\mu$.

اثبات. فرض کنید r_1، r_2، ...، $-r'_1$، $-r'_2$، ... مقادیر کوچک‌ترین با باقیمانده a، $2a$، ...، $\frac{1}{2}(p-1)a$. اگر $i\neq j$، آنگاه $r_i\neq r_j$، $r'_i\neq r'_j$، و $r_i\neq r'_j$؛ زیرا اگر $m_1a\equiv r_i \mod p$ و $m_2a\equiv -r'_i \mod p$، آنگاه $r_i=r'_j$ نتیجه می‌دهد $(m_1+m_2)a\equiv 0 \mod p$، یعنی $p|(m_1+m_2)$. این امکان ندارد ، زیرا $m_1+m_2\leq p-1$. پس $\frac{1}{2}(p-1)$ عدد r_i، r'_j اعداد صحیح متمایز بین ۱ و $\frac{1}{2}(p-1)$ هستند؛ یعنی دقیقاً همان اعداد ۱ ، ۲، ...، $\frac{1}{2}(p-1)$ هستند (با ترتیبی دیگر). پس

$$a\cdot 2a\cdots\frac{1}{2}(p-1)a\equiv(-1)^\mu\left(\frac{p-1}{2}\right)! \mod p,$$

یعنی

$$a^{\frac{1}{2}(p-1)}\equiv(-1)^\mu \mod p.$$

اکنون حکم از لم قبل نتیجه می‌شود. □

قضیه ۴.۶.۱۵. اگر $p=8k\pm 1$، آنگاه ۲ یک مانده‌ی درجه‌ی دوم به پیمانه‌ی p؛ و اگر $p=8k\pm 3$، آنگاه ۲ نامانده است.

اثبات. در لم قبل $a=2$ قرار می‌دهیم. μ تعداد اعداد صحیح $2m$، $1\leq m\leq\frac{1}{2}(p-1)$، است که $2m>\frac{1}{2}p$، یا $m>\frac{1}{4}p$. بنابراین $\mu=\frac{1}{2}(p-1)-\left[\frac{p}{4}\right]$. چهار حالت مورد نظر عبارت‌اند از

p	μ
$8k-3$	$4k-2-(2k-1)=2k-1$
$8k-1$	$4k-1-(2k-1)=2k$
$8k+1$	$4k-2k=2k$
$8k+3$	$4k+1-2k=2k+1$,

پس حکم از لم قبل به دست می‌آید. □

نتایج کاملاً مشابهی برای وقتی که به جای p، p^m و به جای عناصر $\mathbb{Z}_p$، عناصر میدان $\mathrm{GF}(p^m)$ را در نظر بگیریم درست است. بنابراین در تعمیم مطالب فوق ماندهای درجه‌ی دوم در $\mathrm{GF}(p^m)$ را مربع عناصر ناصفر این میدان تعریف می‌کنیم. خودریختی فروبنیوس $\varphi : \mathrm{GF}(P^m) \longrightarrow \mathrm{GF}(p^m)$، $\varphi(a) = a^p$، را در نظر می‌گیریم. بنا به تمرین ۳ از صفحه‌ی ۳۱۸، داریم $\mathrm{Aut}\,\mathrm{GF}(p^m) = \langle\varphi\rangle$. بنابراین به ازای هر $1 \le j \le p^m - 1$ هر عضو $\mathrm{GF}(p^m)$ ریشه‌ی p^jام یکتا دارد. توجه کنید که ریشه‌ی درجه‌ی دوم یکتای هر عضو $b \in \mathrm{GF}(2^m)$ برابر $b^{2^{m-1}}$ است. اگر $p \neq 2$، آنگاه دقیقاً نصف عناصر ناصفر $\mathrm{GF}(p^m)$ ریشه‌ی دوم دارند، که آن‌ها را ماندهای درجه‌ی دوم $\mathrm{GF}(p^m)$ نامیده‌ایم. هرگاه a عضو اولیه‌ای از $\mathrm{GF}(p^m)$ باشد، ماندهای درجه‌ی دوم در این میدان عبارت‌اند از a^{2i}، پس مجموعه‌ی ماندهای درجه‌ی دوم در $\mathrm{GF}(p^m)$ یک زیرگروه از گروه ضربی $\mathrm{GF}(p^m)$ است، و حاصل‌ضرب دو مانده و یا حاصل‌ضرب دو نامانده، یک مانده؛ هم‌چنین حاصل‌ضرب یک مانده در یک ناماندہ، یک ناماندہ است.

قضیه ۵.۶.۱۵. فرض کنید p عدد اول باشد. $p^m = 4k + 1$، آنگاه -1 یک ماندهٔ درجه‌ی دوم و اگر $p^m = 4k - 1$، آنگاه -1 یک ناماندہ در $\mathrm{GF}(p^m)$ است.

اثبات. اگر a عضو اولیه‌ای از $\mathrm{GF}(p^m)$ باشد، آنگاه $a^{\frac{1}{2}(p^m-1)}$. اکنون اگر $p^m = 4k + 1$، آنگاه $\frac{1}{2}(p^m - 1) = 2k$ و -1 توان زوجی از a و اگر $p^m = 4k - 1$، آنگاه $\frac{1}{2}(p^m - 1) = 2k - 1$ و -1 توان فردی از a است. □

اکنون می‌خواهیم کدهای ماندهای درجه‌ی دوم (QR-کدهای) به طول عدد اول فرد p روی $\mathrm{GF}(\ell)$، که در آن ℓ یک مانده درجه‌ی دوم به پیمانه‌ی p و توانی از یک عدد اول است، تعریف کنیم. در حالت مهم کدهای ماندهای درجه‌ی دوم دوتایی (حالت $\ell = 2$) دیدیم (قضیه‌ی ۴.۶.۱۵) که p باید به صورت $p = 8k \pm 1$ باشد.

فرض کنید p عدد اول فرد باشد و ℓ توانی از یک عدد اول طوری که $\gcd\{p, \ell\} = 1$ و به علاوه ℓ یک مانده‌ی درجه‌ی دوم به پیمانه‌ی p باشد. فرض کنید Q مجموعه‌ی همه‌ی ماندهها به پیمانه‌ی p و N مجموعه‌ی همه‌ی ناماندهها باشد. اگر b عضو اولیه‌ای از $\mathbb{Z}_p$ باشد، آنگاه $b^e \in Q$ اگر و تنها اگر e زوج باشد؛ در حالی که $b^e \in N$ اگر و تنها اگر e فرد باشد. بنابراین Q یک گروه دوری با مولد b^2 است. چون $\ell \in Q$، مجموعه‌ی Q تحت ضرب در ℓ بسته است. بنابراین Q اجتماع مجزایی از هم مجموعه‌های دایره‌بر به پیمانه‌ی p است. بنابراین ضرایب چندجمله‌ای‌های

$$g_0(x) = \prod_{j \in Q}(x - a^j), \quad g_1(x) = \prod_{j \in N}(x - a^j)$$

در $\mathrm{GF}(\ell)$ قرار دارند، که در آن a یک ریشه‌ی pام اولیه‌ی واحد در یک توسیع $\mathrm{GF}(\ell)$ است ($a \in \mathrm{GF}(\ell^t)$، که در آن $t = \frac{p-1}{2}$ مرتبه‌ی b^2 در $\mathbb{Z}_p^\times$ است). توجه کنید که داریم $x^p - 1 = (x - 1)g_0(x)g_1(x)$. کدهای دوری تولید شده توسط چندجمله‌ای‌های $g_0(x)$، $(x - 1)g_0(x)$، $g_1(x)$، و $(x - 1)g_1(x)$ را به ترتیب با C_0^+، C_0، C_1^+، و C_1 نشان می‌دهیم و آن‌ها را کدهای ماندهای درجه‌ی دوم یا QR می‌نامیم. واضح است که $C_0 \subseteq C_0^+$ و $C_1 \subseteq C_1^+$. به سادگی می‌توان دید کدهای C_0 و C_1 (و هم‌چنین C_0^+ و C_1^+) معادل هستند. در واقع اگر m یک ناماندههای ثابت باشد، جایگشت روی V_n که $x \mapsto x^m$، کدهای C_0^+ و C_1^+ را به هم و کدهای C_0 و C_1 را به هم تصویر می‌کند. بُعد C_0^+ و C_1^+ برابر $\frac{1}{2}(p + 1)$ و بُعد C_0 و C_1 برابر $\frac{1}{2}(p - 1)$ است. به علاوه اگر $p = 4k - 1$، آنگاه $C_0^+ = C_0^\perp$، $C_1^+ = C_1^\perp$ و اگر $p = 4k + 1$، آنگاه $C_0^+ = C_1^\perp$، $C_1^+ = C_0^\perp$.

مثال ۶.۶.۱۵. فرض کنید $\ell = 2$ و $p = 7$. ماندههای درجه‌ی دوم به پیمانه‌ی ۷ عبارت‌اند از ۱، ۲، ۴؛ و ناماندهها ۳، ۵، ۶ هستند. بنابراین (مثال ۸.۴.۱۵ را ببینید)

$$g_0(x) = (x - a)(x - a^2)(x - a^4) = x^3 + x + 1$$
$$g_1(x) = (x - a^3)(x - a^5)(x - a^6) = x^3 + x^2 + 1$$

که در آن a عضو اولیه‌ای از $\mathrm{GF}(2^3)$ ریشه‌ی ۷ام اولیه‌ی واحد، و به علاوه ریشه‌ای از چندجمله‌ای $x^3 + x + 1$ است. (توجه کنید در اینجا $t = \frac{7-1}{2} = 3$). C_0^+ همان $[7, 4, 3]$- کد همینگ است. هم‌چنین C_0 یک کد با چندجمله‌ای مولد $(x + 1)(x^3 + x + 1)$

است. چون $۷ \equiv -۱ \mod ۴$، کدهای $C_۰^+$ و $C_۱^+$ معادل هستند؛ بنابراین $C_۱^+$ نیز با $[۷, ۴, ۳]$- کد همینگ معادل است. توجه کنید که با تغییر انتخاب a کدهای $C_۰$ و $C_۱$ نیز تغییر می‌کنند. □

اگر $\ell = ۲$ و $p = ۲۳$. کد گولای $\mathscr{G}_{۲۳}$ (مثال ۱۱.۵.۱۵ را ببینید) عبارت است از کد مانده‌ای درجه‌ی دوم $C_۰^+$ (یا $C_۱^+$). اگر $\ell = ۳$ و $p = ۱۱$. کد گولای $\mathscr{G}_{۱۱}$ عبارت است از کد مانده‌ای درجه‌ی دوم $C_۰^+$ (یا $C_۱^+$). این کدها به ترتیب دارای پارامترهای $[۲۳, ۱۴, ۷]$ و $[۱۱, ۶, ۵]$ هستند. روی $\mathbb{Z}_۲$ داریم $x^{۲۳} - ۱ = (x-۱)g_۰(x)g_۱(x)$، که در آن

$$g_۰(x) = x^{۱۱} + x^{۱۰} + x^۶ + x^۵ + x^۴ + x^۲ + x + ۱$$
$$g_۱(x) = x^{۱۱} + x^۹ + x^۷ + x^۶ + x^۵ + x + ۱.$$

پس چندجمله‌ای مولد $\mathscr{G}_{۲۳}$ را می‌توان برابر $g_۰(x)$ یا $g_۱(x)$ گرفت.
روی $\mathbb{Z}_۳$ داریم $x^{۱۱} - ۱ = (x-۱)g_۰(x)g_۱(x)$، که در آن

$$g_۰(x) = x^۵ + x^۴ - x^۳ + x^۲ - ۱$$
$$g_۱(x) = x^۵ - x^۳ + x^۲ + x^۶ - x - ۱.$$

پس چندجمله‌ای مولد $\mathscr{G}_{۱۱}$ را می‌توان برابر $g_۰(x)$ یا $g_۱(x)$ گرفت.

قضیه ۷.۶.۱۵. اگر d فاصله‌ی می‌نیمم $C_۰^+$ یا $C_۱^+$ باشد، آنگاه $d^۲ \geq p$. به علاوه اگر $p = ۴k - ۱$، آنگاه $d^۲ - d + ۱ \geq p$.

اثبات. فرض کنید $f(x)$ یک کدواژه در $C_۰^+$ با وزن می‌نیم باشد. اگر n یک نامانده باشد، آنگاه $f(x^n)$ یک کدواژه با فاصله‌ی می‌نیم در $C_۱^+$ است. اکنون $f(x^n)f(x)$ باید در $C_۰^+ \cap C_۱^+$ باشد، یعنی مضربی از

$$\prod_{j\in Q}(x-a^j)\prod_{j\in N}(x-a^j) = \prod_{j=۱}^{p-۱}(x-a^j) = \sum_{j=۰}^{p-۱}x^j$$

باشد. پس وزن $f(x^n)f(x)$ برابر p است، و چون وزن $f(x)$ برابر d است، حداکثر تعداد ضرایب ناصفر $f(x^n)f(x)$ برابر $d^۲$ است. پس $d^۲ \geq p$.
اگر $p = ۴k - ۱$، آنگاه $n = -۱$ یک نامانده است و بنا به بحث فوق در $f(x^{-۱})f(x)$ تعداد d جمله برابر ۱ است. پس حداکثر وزن این حاصل‌ضرب برابر $d^۲ - d + ۱$ است. □

مثال ۸.۶.۱۵. در $[۷, ۴, d]$- کد مانده‌ای درجه‌ی دوم روی $\mathrm{GF}(\ell)$ داریم $d \geq ۳$ (و اگر $\ell = ۲$ داریم $d = ۳$). □

حال می‌خواهیم خودتوان‌های کدهای مانده‌ای درجه‌ی دوم را در حالت $\ell = ۲$ بررسی کنیم.

لم ۹.۶.۱۵. اگر $\ell = ۲$، آنگاه $e(x)$ خودتوان است اگر و تنها اگر

$$e(\alpha^i) = ۰ \text{ یا } ۱ \qquad i = ۰, ۱, \ldots, n-۱,$$

که در آن α یک ریشه‌ی nام اولیه‌ی واحد است (n فرد).

اثبات. ($\Longleftarrow$) داریم $e(a^i)^۲ = e(\alpha^i)$. بنابراین $e(\alpha^i)$ یا برابر ۰ است یا برابر ۱.
($\Longrightarrow$) فرض کنید $e(x) = \sum_{i=۰}^{n-۱}\xi_i x^i$. چون $e(\alpha^i)$ یا برابر است ۰ یا برابر ۱، داریم $e(\alpha^{۲j}) = e(\alpha^j)^۲ = e(\alpha^j)$. بنا به لم ۲۵.۴.۱۵،

$$\xi_i = \sum_{j=۰}^{n-۱}e(\alpha^j)\alpha^{-ij} = \sum_s\sum_{j\in C_s}\alpha^{-ij},$$

که در آن s در یک زیرمجموعه از هم مجموعه‌های دایره‌بر تغییر می‌کند. بنابراین $\xi_i = \xi_{۲i}$ و $e(x)$ خودتوان است. □

نتیجه ۱۰.۶.۱۵. اگر C کد دوری دوتایی به طول فرد n با مولد $g(x)$ و همانی $e(x)$ باشد، آنگاه بُعد C برابر است با
(الف) تعداد α^iهایی که $g(\alpha^i) \neq 0$.
(ب) تعداد α^iهایی که $e(\alpha^i) = 1$. □

قضیه ۱۱.۶.۱۵. اگر $\ell = 2$ و $p = 4k - 1$، آنگاه می‌توان α را طوری اختیار کرد که مولدهای خودتوان C_0^+، C_0، C_1^+، C_1، به ترتیب برابر $e_Q(x) = \sum_{i\in Q} x^i$، $f_Q(x) = 1 + \sum_{i\in N} x^i$، $e_N(x) = \sum_{i\in N} x^i$، و $f_N(x) = 1 + \sum_{i\in Q} x^i$ باشد.

اثبات. چون ۲ یک مانده‌ی درجه‌ی دوم به پیمانه‌ی p است (قضیه‌ی ۴.۶.۱۵)، داریم $e_Q(t)^2 = e_Q(t)$ و به همین نحو ثابت می‌شود که سایر چندجمله‌ای‌ها خودتوان هستند.
بنا به لم قبل، $e_Q(\alpha^i)$ یا برابر ۰ است یا برابر ۱. به ازای هر مانده‌ی درجه‌ی دوم s

$$e_Q(\alpha^s) = \sum_{i\in Q} \alpha^{is} = \sum_{j\in Q} \alpha^j = e_Q(\alpha),$$

مستقل از s است. به طریق مشابه برای هر نامانده‌های t داریم

$$e_Q(\alpha^t) = \sum_{i\in Q} \alpha^{it} = \sum_{i\in Q} \alpha^{-i} = e_Q(\alpha^{-1}).$$

چون $e_Q(\alpha) + e_Q(\alpha^{-1}) = 1$، بسته به انتخاب α دو حالت پیش می‌آید:
یا $e_Q(\alpha^s) = 0$ و $e_Q(\alpha^t) = 1$، به ازای هر $s \in Q$ و $t \in N$.
یا $e_Q(\alpha^s) = 1$ و $e_Q(\alpha^t) = 0$، به ازای هر $s \in Q$ و $t \in N$.
فرض کنید α را طوری اختیار کرده‌ایم که حالت اول برقرار باشد، در این صورت $e_Q(x)$ عضو خودتوان C_0^+ است. به علاوه برای $t \in N$

$$e_N(\alpha^t) = \sum_{i\in N} \alpha^{it} = \sum_{i\in Q} \alpha^i$$

و برای هر $s \in Q$، $e_N(\alpha^s) = 1$. بنابراین $e_N(x)$ عضو خودتوان C_1^+ است.
در نهایت برای هر $s \in Q$ داریم $f_Q(\alpha^s) = 0$ و $f_Q(1) = 0$. از این‌رو $f_Q(x)$ عضو خودتوان C_0 است. □

توجه کنید که اگر $\ell = 2$ و $p = 4k + 1$ خودتوان‌های C_0^+، C_0، C_1^+ و C_1 به ترتیب برابر $\sum_{i\in N} x^i$، $1 + \sum_{i\in Q} x^i$ و $\sum_{i\in Q} x^i$ هستند.

مثال ۱۲.۶.۱۵. اگر $\ell = 2$ و $p = 23$، آنگاه

$$Q = \{1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18\}$$

و خودتوان‌های C_0^+ و C_1^+ عبارت‌اند از $\sum_{i\in Q} x^i$ و $\sum_{i\in Q} x^{-i}$. هر دو چندجمله‌ای یک کد معادل کد گولای $\mathscr{G}_{23}$ تولید می‌کنند. □

فرض کنید C یک کد دوری به طول n روی $\mathrm{GF}(q)$ با چندجمله‌ای مولد $g(x)$ و چندجمله‌ای امتحان $h(x)$ باشد. در این صورت $g(x)h(x) = x^n - 1$. به علاوه داریم $g(x) = \prod_{i\in K}(x - a^i)$، که در آن K اجتماعی از هم مجموعه‌های دایره‌بر به پیمانه‌ی n است ($i \in K \longrightarrow qi \mod n \in K$). عناصر مجموعه‌ی $\{\alpha^i \mid i \in K\}$ را ، که متشکل از ریشه‌های nام واحد است، صفرهای کد C می‌نامیم. در قضیه‌ی بعد کدهای دوگان QR-کدهای دوتایی را می‌یابیم.

قضیه ۱۳.۶.۱۵. فرض کنید $\ell = 2$، اگر $p = 4k - 1$، آنگاه $C_0^\perp = C_0^+$ و $C_1^\perp = C_1^+$. اگر $p = 4k - 1$، آنگاه $C_1 = C_0^+$ و $C_0^\perp = C_1^+$. در هر حالت C_0 و $(1, 1, \ldots, 1)$، C_0^+ را تولید می‌کنند و C_1 و $(1, 1, \ldots, 1)$، C_1^+ را تولید می‌کنند.

اثبات. فرض کنید $p = ۴k - ۱$. صفرهای $C_۰^+$ عبارت‌اند از α^j، که در آن $j \in Q$. چون چندجمله‌ای مولد کد دوری $(g(t))$ عبارت است از $h(x) = \dfrac{x^n - ۱}{g(x)}$، که در آن $h^\top(x) = x^{\deg h} h(x^{-۱})$، صفرهای $(C_۰^+)^\perp$ عبارت‌اند از α^{-j}، که در آن $j \in N$. اما $-j \in Q$، پس $C_۰^\perp = C_۰^+$ و گزاره‌ی اول ثابت شد.
بنا به قضیه‌ی ۱۱.۶.۱۵،

$$e_Q(x) = f_Q(x) + \frac{۱}{p}\sum_{i=۰}^{p-۱} x^i,$$

که سومین گزاره را ثابت می‌کند. به طریق مشابه می‌توان سایر گزاره‌ها را ثابت کرد. □

اکنون ماتریس مولد برای QR-کدهای دوتایی را می‌یابیم. فرض کنید

$$f_Q(x) = \sum_{i=۰}^{p-۱} a_i x^i$$

مولد خودتوان $C_۰$ باشد، که در قضیه‌ی ۱۱.۶.۱۵ داده شده است. در این صورت ماتریس مولد $C_۰$ ماتریس $p \times p$

$$G_۰ = \begin{bmatrix} a_۰ & a_۱ & \cdots & a_{p-۱} \\ a_{p-۱} & a_۰ & \cdots & a_{p-۲} \\ \vdots & \vdots & \vdots & \vdots \\ a_۱ & a_۲ & \cdots & a_۰ \end{bmatrix} = [g_{ij}] \qquad g_{ij} = a_{j-i}, \quad ۱ \le i, j \le p-۱$$

است، که در آن اندیسهای $g_{ij} = a_{j-i}$ به پیمانه‌ی p محاسبه می‌شوند. یک ماتریس مولد برای $C_۰^+$ عبارت است از

$$\left[\begin{array}{ccccc} & & G_۰ & & \\ & & & & \\ \hline ۱ & ۱ & \cdots & ۱ & \end{array}\right] \tag{۷}$$

برای کدهای $C_۱$ و $C_۱^+$ می‌توان به طریق مشابه عمل کرد. توجه کنید که رتبه‌ی ماتریس $G_۰$ برابر $\frac{۱}{۲}(p-۱)$ است.

مثال ۱۴.۶.۱۵. اگر $\ell = ۲$ و $p = ۷$،یک ماتریس مولد برای $[۷, ۴, ۳]$- کد همینگ $C_۰^+$ عبارت است از

$$\left[\begin{array}{ccccccc} ۱ & ۰ & ۰ & ۱ & ۰ & ۱ & ۱ \\ ۱ & ۱ & ۰ & ۰ & ۱ & ۰ & ۱ \\ ۱ & ۱ & ۱ & ۰ & ۰ & ۱ & ۰ \\ ۰ & ۱ & ۱ & ۱ & ۰ & ۰ & ۱ \\ ۱ & ۰ & ۱ & ۱ & ۱ & ۰ & ۰ \\ ۰ & ۱ & ۰ & ۱ & ۱ & ۱ & ۰ \\ ۰ & ۰ & ۱ & ۰ & ۱ & ۱ & ۱ \\ \hline ۱ & ۱ & ۱ & ۱ & ۱ & ۱ & ۱ \end{array}\right].$$

□

اکنون QR-کدهای تعمیم یافته‌ی دوتایی را در نظر می‌گیریم : مثلاً

$$\overline{C_۰^+} = \left\{ u_۰u_۱\cdots u_{p-۱}u_p \mid u_۰u_۱\cdots u_{p-۱} \in C_۰^+, \quad u_p = \sum_{i=۰}^{p-۱} u_i \right\}.$$

توجه کنید $\overline{C_۰^+}$ و $\overline{C_۱^+}$، $\left[p+۱, \dfrac{p+۱}{۲}\right]$ - کد هستند.

قضیه ۱۵.۶.۱۵. اگر $p = ۴k - ۱$، کدهای QR تعمیم یافته‌ی دوتایی $\overline{C_۰^+}$ و $\overline{C_۱^+}$ خود دوگان هستند.

اثبات. ماتریس مولد $\overline{C_۰^+}$ با اضافه کردن یک ستون به ۷ به دست می‌آید و به صورت

$$\bar{G} = \left[\begin{array}{ccccc|c} & & G_۰ & & & ۰ \\ & & & & & \vdots \\ \hline ۱ & ۱ & \cdots & ۱ & \vdots & ۰ \end{array}\right]$$

است. چون $C_۰ \subseteq C_۰^{\perp}$، هر سطر $G_۰$ بر خودش و بر هر سطر دیگر عمود است. پس هر سطر $\overline{G}$ بر همه‌ی سطرهای $\overline{G}$ عمود است و $\overline{C_۰^+} \subseteq (\overline{C_۰^+})^{\perp}$. اما رتبه‌ی $\overline{G}$ برابر $\frac{۱}{۲}(p+۱)$ است. پس $\overline{C_۰^+} = (\overline{C_۰^+})^{\perp}$. □

بنابراین کدهای گولای $\overline{\mathscr{G}_{۲۳}} = \mathscr{G}_{۲۴}$ و $\overline{\mathscr{G}_{۱۱}} = \mathscr{G}_{۱۲}$ خود دوگان هستند.
توجه کنید که اگر $p = ۴k + ۱$، می‌توان QR-کدهای تعمیم یافته‌ی دوتایی را طوری تعریف کرد که $C_۱^+ = (\overline{C_۰^+})^{\perp}$.

قضیه ۱۶.۶.۱۵. اگر $\ell = ۲$ و $p = ۴k - ۱$، آنگاه ۴ وزن هر کد واژه در $\overline{C_۰^+}$ را عاد می‌کند و وزن هر کد واژه در $C_۰^+$ با ۰ یا ۳ به پیمانه‌ی ۴ هم‌نهشت است.

اثبات. اگر ۲ یک مانده‌ی درجه‌ی دوم به پیمانه‌ی p باشد، آنگاه بنا به قضیه‌ی ۴.۶.۱۵ $p = ۸m \pm ۱$. پس می‌توان فرض کرد $p = ۸m - ۱$. تعداد مانده‌ها، که مساوی تعداد نامانده‌ها است، برابر $۴m - ۱$ است. بنابراین وزن هر سطر $\overline{G}$ مضربی از ۴ است. پس حکم از تمرین ۱۵ صفحه‌ی ۳۸۸ ثابت است. □

اگر $\ell = ۲$ و $p = ۴k + ۱$ می‌توان نشان داد که وزن کد واژه‌های $\overline{C_۰^+}$ زوج است.
از قضیه‌ی ۷.۶.۱۵ و قضیه‌ی قبل نتیجه می‌گیریم که فاصله‌ی می‌نیمم کد گولای $\mathscr{G}_{۲۳}$ و $\mathscr{G}_{۱۱}$ به ترتیب برابر ۷ و ۵ است. بنابراین $\mathscr{G}_{۲۴}$ تنها کد واژه‌هایی به وزن ۰، ۸، ۱۲، ۱۶ و ۲۴ دارد و $\mathscr{G}_{۱۲}$ تنها کد واژه‌هایی به وزن ۰، ۶، ۹ و ۱۲ دارد.

تمرین‌ها

در هر جا لازم باشد می‌توانید برای انجام محاسبات از GAP استفاده کنید.

۱. بُعد یک کد BCH روی $\mathbb{Z}_۳$ به طول ۸۰ که ۵- تصحیح کننده‌ی خطاست را بیابید.

۲. چندجمله‌ای مولد $[۷, ۳]$- کد RS روی $\mathrm{GF}(۸)$ را بیابید.

۳. یک کد BCH دوتایی به طول ۳۱ کد ۲- تصحیح کننده‌ی خطاست با ریشه‌ی a از $۱ + x^۲ + x^۵ \in \mathbb{Z}_۲[x]$ تعریف می‌شود. اگر سندرُم واژه‌ی دریافت شده $(۱۱۱۰۰۱۱۱۰۱)^{\top}$ باشد، خطا را بیابید.

۴. چندجمله‌ای مولد کد BCH به طول ۱۵ که ۳- تصحیح کننده‌ی خطاست را با استفاده از عضو اولیه‌ی a از $\mathrm{GF}(۲^۴)$ بیابید، که در آن $a^۴ = a^۳ + ۱$.

۵. چندجمله‌ای مولد که BCH به طول ۳۱ با فاصله‌ی می‌نیمم ۹ را بیابید.

۶. همه‌ی کدهای دوتایی BCH با $\ell = ۱$ به طول ۵۱ را بیابید.

۷. فرض کنید a عضو اولیه‌ای از $\mathrm{GF}(۲^۴)$ با $a^۴ + a + ۱ = ۰$ و چندجمله‌ای مولد $g(x) = ۱ + x + x^۲ + x^۴ + x^۵ + x^۸ + x^{۱۰}$ یک $[۱۵, ۵]$- کد BCH باشد. فرض کنید واژه‌ی $u = ۱۱۰۰۰۱۰۰۱۱۰۱۰۰۰$ دریافت شده باشد. واژه‌ی تصحیح شده را تعیین و آن را کد گشایی کنید.

۸. چندجمله‌ای مولد کد BCH به طول ۸ با $\ell = ۱$، روی $\mathbb{Z}_۳$ که ۲- تصحیح کننده‌ی خطاست را بیابید ($a \in \mathrm{GF}(۳^۲)$، که در آن $a^۲ + a + ۲ = ۰$ صدق می‌کند، اولیه است) $u = ۲۲۰۰۱۰۰۱$ را کد گشایی کنید.

۹. فرض کنید $n = ad$، نشان دهید که برای کد BCH دوتایی به طول n و فاصله‌ی طرح d داریم $d_{\min} = d$.

۱۰. دترمینان واندرموند را که در صفحه‌ی ۳۹۰ معرفی شد را به استقرا محاسبه کنید.

۱۱. چندجمله‌ای $g(x) = x^۶ + ۳x^۵ + x^۳ + ۲x^۲ + ۲x + ۱$ مولد یک $[۱۵, ۹]$- کد روی $\mathrm{GF}(۴)$ است. $t^۸ + ۲t_t^۲ + ۱$ را کد گشایی کنید. چندجمله‌ای امتحان کد را بیابید. آیا $t^{۱۱} + ۳t^۲ + ۲t + ۱$ یک کد واژه است؟ سندرُم $t^{۱۰} + ۳t^۲ + t + ۲$ را بیابید.

۱۲. به ازای هر عدد صحیح مثبت m و $t \leq ۲^{m-۱} - ۱$، نشان دهید یک BCH- کد دوتایی به طول $n = ۲^m - ۱$ وجود دارد که t- تصحیح کننده‌ی خطا است و بُعد آن بزرگ‌تر یا مساوی $n - mt$ است.

۱۳. یک کد BCH به طول ۲۶ با فاصله‌ی طرح $\delta = ۵$ روی $\mathbb{Z}_۳$ بسازید.

۱۴. فرض کنید a عضو اولیه‌ای از $\mathrm{GF}(۲^۵)$ باشد که در $a^۵ = a^۲ + ۱$ صدق می‌کند. کد BCH به طول ۳۱ و فاصله‌ی طرح $\delta = ۵$ با $\ell = ۱$ را در نظر بگیرید و واژه‌ی ۱۱۱ ۰۱۱۱ ۰۱۰۲ ۱۱۰۱ ۰۰۰۰ ۱۱۱۱ ۰۱۱۰ ۱۰۰۱ کد گشایی کنید.

۱۵. $[۱۵, ۱۳]$- کد RS روی $\mathrm{GF}(۱۶)$ را با تعیین چندجمله‌ای مولد و تعداد خطاهایی که می‌تواند تصحیح کند، توصیف کنید.

۱۶. (الف) آیا دوگان یک BCH- کد مجدداً BCH- کد است؟
(ب) آیا دوگان یک RS- کد مجدداً RS- کد است؟

۱۷. یک چندجمله‌ای مولد برای RS- کد به طول ۴ روی $\mathbb{Z}_۵$ با فاصله‌ی طرح ۳ بیابید.

۱۸. فرض کنید C، $[n = q^m - ۱, k]$- کد RS با فاصله‌ی می‌نیمم d باشد. نشان دهید کد تعمیم یافته‌ی آن یک $[q^m, k]$- کد با فاصله‌ی می‌نیمم $d + ۱$ است.

۱۹. فرض کنید A_i تعداد کد واژه‌های $[۲۳, ۱۲]$- کد گولای به وزن i باشد. نشان دهید به ازای هر $۰ \leq i \leq ۲۳$، $A_i = A_{۲۳-i}$.

۲۰. به ازای هر کد مانده‌ای درجه‌ی دوم به طول عدد اول p، نشان دهید $d_{\min} \geq \sqrt{p}$.

۲۱. نشان دهید $[۲۳, ۱۲]$- کد گولای هیچ کد واژه‌ی ناصفری با وزن ۴ یا کمتر ندارد.

۲۲. ماتریس مولد $[۱۲, ۶]$- کد گولای عبارت است از $G = [I \mid A]$، که در آن

$$A = \begin{bmatrix} ۰ & ۱ & ۱ & ۱ & ۱ & ۱ \\ ۱ & ۰ & ۱ & -۱ & -۱ & ۱ \\ ۱ & ۱ & ۰ & ۱ & -۱ & -۱ \\ ۱ & -۱ & ۱ & ۰ & ۱ & -۱ \\ ۱ & -۱ & -۱ & ۱ & ۰ & ۱ \\ ۱ & ۱ & -۱ & -۱ & ۱ & ۰ \end{bmatrix}.$$

نشان دهید این کد خود- عمود است. تحقیق کنید فاصله‌ی می‌نیمم آن برابر ۶ است.

۲۳. نشان دهید QR-کدهای $C_۰^+$ و $C_۱^+$ معادل هستند.

۲۴. نشان دهید وزن همه‌ی کدواژه‌های $[۱۱, ۶, ۵]$- کد گولای روی $\mathbb{Z}_۳$ با ۱ به پیمانه‌ی ۳ هم‌نهشت نیست.

۲۵. نشان دهید کد گولای روی $\mathbb{Z}_۳$ کامل، و فاصله‌ی می‌نیمم آن برابر ۵ است.

فصل ۱۶

آزمایشگاه‌های GAP

۱.۱۶ آشنایی با GAP، آزمایشگاه اول

GAP یک زبان برنامه نویسی برای انجام محاسبات در ریاضیات شاخه‌ی جبر است. علاوه بر قابلیت‌های مناسب برای برنامه نویسی، ابزاری پرقدرت برای انجام محاسبات در شاخه‌های مختلف جبر است. GAP مخفف

Groups، Algorithms and Programming

است. در ابتدا این نرم‌افزار برای انجام محاسبه در نظریه‌ی گروه‌ها طراحی شد و سپس به تدریج سایر شاخ‌های جبر را نیز در برگرفت. دسترسی به این نرم‌افزار برای همه آزاد و بدون پرداخت وجه است و بدون قصد تجارت می‌توان آن را کپی و توزیع کرد. آدرس یکی از سایت‌هایی اینترنتی که می‌توان نسخه‌های به روز شده‌ی GAP را از آن دریافت کرد عبارت است از

$$\text{http} : //\text{www} - \text{gap.dcs.st} - \text{and.ac.uk/} \sim \text{gap}$$

همان طور که می‌دانید زبان‌های برنامه نویسی دو گونه‌اند، مفسر یا محاوره‌ای (interpneter)، و مترجم (compiler). در حالت محاوره‌ای، نرم‌افزار پس از دریافت هر دستور بلافاصله پردازش آن را شروع می‌کند. در حالت مترجم، پس از ذخیره‌ی همه‌ی برنامه و ترجمه‌ی (compile) آن به زبان ماشین طی مراحلی انجام می‌شود. پس از خواست استفاده کننده می‌توان برنامه را که به زبان ماشین تبدیل شده اجرا کرد. از محاسن نرم‌افزارهای محاوره‌ای پردازش بلافاصله و بدون هیچ مرحله‌ی واسطه‌ای است و شخص می‌تواند از نتیجه‌ی برنامه فوراً (در صورتی که جوابی فوری داشته باشد) آگاه شود. اما از معایب آن، به خصوص برای برنامه‌های بزرگ، این است که مفسر برای اجرای برنامه، هر خط برنامه را از نظر دستور زبان نرم‌افزار بررسی می‌کند و این کار ممکن است بارها و بارها انجام شود. در صورتی که یک بار بررسی صحت برنامه از نظر دستوری کافی است. اما در حالت مترجم این مساله پیش نمیآید و صحت برنامه از نظر دستور زبان نرم‌افزار یک بار بررسی شده و برنامه به زبان ماشین تبدیل می‌شود که برنامه با سرعت بالاتری اجرا می‌شود. به هر ترتیب GAP امکان استفاده از هر دو مورد، مفسر و مترجم را فراهم می‌کند. برای شروع کار از امکان مفسر آن استفاده می‌کنیم. پس از احضار برنامه‌ی GAP چند لحظه طول می‌کشد تا GAP، با بارکردن کتاب‌خانه‌ی خود، آماده‌ی انجام دستورات شود. علامت آمادگی GAP،

gap>

است. برای خارج شدن از برنامه کافی است تایپ کنیم:

gap>quit;

در انتهای هر دستور باید علامت ”؛“ تایپ و سپس دکمه‌ی enter فشار داده شود. استفاده از کمک (help) در GAP به صورت مستقیم امکان‌پذیر است. کافی است دستوری را که می‌خواهیم اطلاعاتی در مورد آن کسب کنیم با علامت ? و یا ?? تایپ کنیم

gap>??integers

Help: several entries match this topic - type ?2 to get match [2]

[1] Reference: Integers

[2] Reference: Integers

[3] Reference: Elementary Operations for Integers

[4] Reference: Prime Integers and Factorization
[5] Reference: Roots Modulo Integers
[6] Reference: Normal Forms over the Integers
[7] Reference: mod!Integers
[8] Reference: IsMonomial!for positive integers
[9] Reference: PositiveIntegers
[10] Reference: NonnegativeIntegers
[11] Reference: IsIntegers
[12] Reference: IsPositiveIntegers
[13] Reference: IsNonnegativeIntegers
[14] Reference: Random!for integers
[15] Reference: GaussianIntegers
[16] Reference: IsGaussianIntegers

اگر مثلاً بخواهیم در مورد بخش ۱۱ از خروجی بالا اطلاعی بیابیم، می‌نویسیم 11?

```
gap>?11
Integers ————————————————————- reference
[...]
> IsIntegers(<obj> )                                    C
> IsPositiveIntegers(<obj> )                            C
> IsNonnegativeIntegers(<obj> )                         C
are the defining categories for the domains ‘Integers’,
‘PositiveIntegers’, and ‘NonnegativeIntegers’.
‘Integers’ is a subset of ‘Rationals’, which is a subset of
‘Cyclotomics’. See Chapter “Cyclotomic Numbers” for arithmetic
operations and comparison of integers.
```

دستور IsInteger را امتحان می‌کنیم

```
gap>IsIntegers(Integers);
true
gap>IsIntegers(Rationals);
false
gap>IsIntegers(7);
false
```

راهنمای GAP به زبان‌های TEX و HTML نوشته شده و به علاوه فایل پست‌اسکریپت راهنمای آن در دایرکتوری GAP وجود دارد و استفاده کننده می‌تواند از هر کدام از آن‌ها که بخواهد برای یادگیری بهتر زبان GAP بهره گیرد.
برای نوشتن توضیح بین خطوط و دستورات، طوری که GAP آن را پردازش نکند، از علامت # استفاده می‌کنیم. پس از # هر عبارتی که بیابد GAP آن را توضیح برنامه‌نویس تلقی کرده و پردازش نمی‌کند.
اعمال جمع و تفریق، ضرب و تقسیم و توان را می‌توان به راحتی انجام داد:

مثال ۱.۱.۱۶. عبارت $\frac{(۸-۵)(۶+۴)^۳}{۵}$ را محاسبه کنید.

حل کافی است عبارت مورد نظر را تایپ کنیم، جواب آن بلافاصله دیده می‌شود:

gap>(8-5)*(6+4)^3/5; **# a simple expresion**
600

هر دو شیء قابل مقایسه را می‌توان با علامت‌های =، <>، >، <، =>، و =< با یکدیگر مقایسه کرد، که تساوی، نامساوی، کوچک‌تر، بزرگ‌تر، کوچک‌تر یا مساوی، و بزرگ‌تر یا مساوی را برای دو شیء آزمایش می‌کند و نتیجه‌ی آن true (درست) یا false (نادرست) است.

مثال ۲.۱.۱۶. (الف) کدام عبارت بزرگ‌تر است: $\left(\frac{۲۵}{۲۷}\right)^{۳}$، $\left(\frac{۴۶}{۴۷}\right)^{۴}$.

(ب) چند عبارت بولی بنویسید

حل (الف)

gap>(25/27)^3 > (46/47)^4;
true

(ب) مقادیر بولی true و false و عبارت‌هایی را که حاصل‌ضرب آن ها مقادیر بولی باشد می‌توان با عملگرهای منطقی پردازش کرد، مثلاً:

gap>true and false; true or false;
false
true

gap>not (true and (false or true));
false

مثال ۳.۱.۱۶. عدد $a = \frac{(۶+۳)(۲۹-۳/۲)^{۲}}{۷}$ را در نظر بگیرید و مقدار $a(a+۱)^{۴}$ را بیابید.

حل مقادیر را می‌توان به متغیر ها منتسب کرد. استفاده از متغیر امکان می‌دهد که با دادن یک نام به یک مقدار رجوع کنیم. برای انتساب مقدار به متغیر از =: استفاده می‌کنیم

gap>a:=(6+3)*(29-3/2)^2/7;
27225/28

gap>a*(a+1)^4;
150184513930169785052225/17210368

مثال ۴.۱.۱۶. عدد $b = \left(\frac{۲۵}{۷}\right)^{۴}$ را در نظر بگیرید و مقدار $b^{۲}+۳$ و $b(b+۱)$ را بیابید.

حل در صورتی که جمله درست نباشد، GAP با دادن پیغام خطا آن‌را اجرا نمی‌کند. یا اگر به متغیری که مقداری به آن منتسب نکرده‌ایم رجوع کنیم GAP پیغام خطا می‌دهد. اگر پس از دستور، به جای ";" از ";;" استفاده کنیم، محاسبه توسط GAP انجام می‌شود اما نتیجه بر صفحه‌ی کامپیوتر ظاهر نمی‌شود

gap>b:=(25/7)^4;; **b^2+3;**
152605185028/5764801

gap>b(b+1);
<func> must be a function (not a rational)

gap>b*(b+1);
153525781250/5764801

gap>u+1;
Variable: ‘u’ must have a value

با استفاده از کلمات last ، last۲ ،. .. می‌توان به آخرین مقدارهای خروجی GAP دسترسی یافت، مثلاً

gap>a:=390628;
390628

gap>last;

```
 390628
gap>last2;
 390628
gap>last4;
 Variable: ‘last4’ must have a value
```

یک برنامه را که به زبان GAP نوشته شده باشد تابع گوییم. اغلب توابع در GAP مثل توابع ریاضی‌اند. آن ها بر تعدادی شیء موسوم به متغیر (یا آرگومان) تابع اثر کرده و پس از انجام پردازش روی آن‌ها، شیء یا اشیای جدیدی را به برنامه برمی‌گرداند.

مثال ۵.۱.۱۶. (الف) !۵ و !۷ را بیابید. (ب) بزرگ‌ترین مقسوم‌علیه مشترک ۴۵ و ۲۵ را بیابید. (ج) آیا ۱۹۹۷ و ۱۹۹۱ اول هستند.

حل (الف) تابع Factorial یکی از توابع GAP است که فاکتوریل یک عدد صحیح مثبت را حساب می‌کند

```
gap>Factorial(5);        Factorial(7);
 120
 5040
```

(ب) Gcd یکی دیگر از توابع GAP است که بزرگ‌ترین مقسوم‌علیه مشترک هر تعداد عدد را به دست می‌آورد.

```
gap>Gcd(25,45);
 5
```

(ج) دستور IsPrime اول بودن یا اول نبودن عدد داده شده را بررسی می‌کند. نام توابع مورد استفاده‌ی GAP با حرف بزرگ شروع می‌شوند

```
gap>IsPrime(1999);        IsPrime(1997);
 true
 true
```

در صورتی که یک نام مرکب باشد، شروع هر کلمه‌ی جدید با حرف بزرگ است، مثلاً IsPrime یک تابع با نام مرکب است که در مثال بالا استفاده شد.

مثال ۶.۱.۱۶. تابعی تعریف کنید که خروجی آن مکعب عدد داده شده باشد.

حل یک طریق تعریف تابع به صورت زیر است: تابع cub را که مکعب عدد داده شده را به دست می‌آورد در زیر تعریف می‌کنیم و به عنوان مثال مکعب اعداد ۳ و ۷ را می‌یابیم

```
gap>cub:=u->u^3;
 function( u ). .. end
gap>cub(3);    cub(7);
 27
 343
```

نحوه‌ی دیگر تعریف تابع به صورت زیر است. مثلاً تابع cub2 را که همانند cub عمل کند به صورت زیر تعریف می‌کنیم

```
gap>cub2:=function(u)
>        return u^3;
> end;
 function( u ) ... end
gap>cub2(3);    cub2(7);
 27
 343
```

تمرین‌ها (با استفاده از GAP)

۱. با استفاده از help در GAP دستوراتی را که در ارتباط با اعداد صحیح (Integers) و اعداد گویا (Rationals) تعریف شده‌اند بررسی کنید.
۲. تعدادی عمل جبری نظیر جمع، ضرب، تقسیم، و توان را در GAP انجام دهید.
۳. تعدادی جمله حاوی عبارت بولی در GAP بنویسید.
۴. تابعی بنویسید که دو عدد را گرفته و دو برابر عدد کوچکتر را با توان دوم عدد بزرگ‌تر جمع کند. این تابع را برای تعدادی عدد امتحان کنید.

۲.۱۶ لیست‌ها در GAP، آزمایشگاه دوم

در این آزمایشگاه لیست‌ها در GAP و برخی اعمال روی آن‌ها را بررسی می‌کنیم. در GAP یک لیست گردایه‌ای از اشیاء است که با کاما ''، '' از یکدیگر جدا شده‌اند و اعضای این گردایه بین دو کروشه قرار گرفته‌اند. در مثال بعد چند عمل ساده روی لیست‌ها را بررسی می‌کنیم.

مثال ۱.۲.۱۶. اعداد ۲، ۴، ۶، ۷، ۲، ۷ را در لیست a قرار دهید و اعمال زیر را روی آن انجام دهید.
(الف) سه عدد ۶، ۸ و ۱۱ را به انتهای لیست اضافه کنید.
(ب) عدد ۳ را به انتهای لیست اضافه کنید.
(ج) عضو سوم و هفتم آن را خارج کنید.
(د) مکان عضو ۶ و عضو ۱۱ را در لیست بیابید.
(هـ) معین کنید آیا ۵ و یا ۴ در لیست قرار دارند یا نه.
(و) مجموع مربعات، مربع و دو برابر همه‌ی اعضای لیست a را بیابید.
(ز) مجموع و حاصل‌ضرب اعضای لیست a را بیابید.
(ح) مجموع مکعب اعضای سوم تا هفتم لیست a را بیابید.
(ط) حاصل‌ضرب اعضای سوم تا پنجم a را که با عدد پنج جمع شده‌اند بیابید.
(ی) لیست a را معکوس کنید.
(ک) تعداد تکرارهای هر عضو a را بیابید.
(ل) تعداد اعداد فرد و اول را در لیست a بیابید.
(م) اعداد بزرگ‌تر یا مساوی ۵ را از لیست بیابید.

حل ابتدا a را تعریف می‌کنیم

```
gap>a:=[2,4,6,7,2,7];
[ 2, 4, 6, 7, 2, 7 ]
```

(الف) دستور $\mathrm{Append}(L,m)$ به انتهای لیست L اعضای لیست m را اضافه می‌کند

```
gap>Append(a,[6,8,11]);          a;
[ 2, 4, 6, 7, 2, 7, 6, 8, 11 ]
```

(ب) دستور $\mathrm{Add}(L,x)$ عضو x را به انتهای لیست L اضافه می‌کند

```
gap>Add(a,3);     a;
[ 2, 4, 6, 7, 2, 7, 6, 8, 11, 3 ]
```

(ج) با دستور $L[i]$ به عضو iام لیست L دسترسی پیدا می‌کنیم

```
gap>a[3];    a[7];
6
6
```

(د) دستور Position(L, x) اولین مکان x را که در لیست L ظاهر شده به دست می‌دهد

```
gap>Position(a,6);    Position(a,11);
 3
 9
```

(هـ)

```
gap>5 in a;    4 in a;
 false
 true
```

(و) ابتدا دو برابر و مجموع مربعات اعضای a را می‌یابیم

```
gap>2*a;    a^2;
[ 4, 8, 12, 14, 4, 14, 12, 16, 22, 6 ]
388
```

دستور List(L, f) لیست متشکل از اعضای لیست L را که تابع f بر آن‌ها اعمال شده به دست می‌دهد

```
gap>List(a,x->x^2);    List(a,x->2*x);
[ 4, 16, 36, 49, 4, 49, 36, 64, 121, 9 ]
[ 4, 8, 12, 14, 4, 14, 12, 16, 22, 6 ]
```

(ز) با دستورهای Sum(L)، (Product(L)) می‌توان اعضای داخل لیست L را با هم جمع و در هم ضرب کرد

```
gap>Sum(a);    Product(a);
 56
 7451136
```

(ح) و (ط) دستورهای Sum(L, f)، (Product(L, f)) پس از اعمال تابع f بر اعضای L آن‌ها را جمع (ضرب) می‌کنند

```
gap>Sum(a[3..7],x->x^3);        Product(a[3..5],x->x+5);
 1126
 924
```

(ی) دستور Reversed(L) لیست L را معکوس می‌کند

```
gap>Reversed(a);
[ 3, 11, 8, 6, 7, 2, 7, 6, 4, 2 ]
```

(ک) دستور Collected(L) تعداد تکرارهای هر عضو را به دست می‌دهد

```
gap>Collected(a);
[ [ 2, 2 ], [ 3, 1 ], [ 4, 1 ], [ 6, 2 ], [ 7, 2 ], [ 8, 1 ], [ 11, 1 ] ]
```

(ل) دستور Number(L) تعداد اعضای لیست L را به دست می‌دهد، همان‌گونه که تابع Length(L) این کار را انجام می‌دهد. اگر f یک تابع بولی باشد دستور Number(L, f) تعداد اعضای L را که مقدار تابع f به ازای آن‌ها، ture است به دست می‌دهد

```
gap>Number(a);    Length(a);
 10
 10
gap>Number(a,x-> x>2 and IsPrime(x));
 4
```

(م) دستور Filtered(L, f) اعضای لیست L را که مقدار تابع بولی f به ازای آن ها درست است، می‌یابد

```
gap>Filtered(a,IsPrime);
 [ 2, 7, 2, 7, 11, 3 ]
gap>Filtered(a,x-> x>=5 and IsPrime(x));
```

[7, 7, 11]

تمرین‌ها (با استفاده از GAP)

۱. اعداد اول بین ۱ و ۱۰۰۰ را بیابید.

۲. دستوری بنویسید که تعداد یک عضو داده شده را در یک لیست بیابید. این دستور را برای عضو ۱ در لیست $a = [۲, ۱, ۳, ۱, ۱, ۴, ۱]$ امتحان کنید.

۳. اعداد بین ۱ تا ۱۰۰ را با هم جمع کنید.

۴. با یک دستور برای $i = ۱, ۲, \ldots, ۱۰۰$ اعداد iام بین ۱ تا ۱۰۰ را در عدد iام بین ۱۰۰ تا ۲۰۰ ضرب کنید.

۵. دستوری بنویسید که لیست داده شده را به ترتیب صعودی مرتب کند.

۶. دستوری بنویسید که لیست داده شده را به ترتیب نزولی مرتب کند.

۳.۱۶ توابع در GAP، آزمایشگاه سوم

در این آزمایشگاه تعدادی تابع در GAP را معرفی می‌کنیم. هم‌چنین نحوه‌ی تعریف توابع، برنامه نویسی با GAP، استفاده از جملات شرطی، حلقه‌های for و while را بررسی می‌کنیم.

مثال ۱.۳.۱۶. تابعی به نام fac بنویسید که شمارنده‌های اول عدد داده شده‌ی n را بیابید و آن را برای اعداد ۱۹۶۲، ۱۹۹۸، ۱۹۹۹ امتحان کنید.

حل در GAP تابعی به نام Factors وجود دارد که این کار را انجام می‌دهد.

```
gap>Factors(1962);    Factors(1999);    Factors(1998);
[ 2, 3, 3, 109 ]
[ 1999 ]
[ 2, 3, 3, 3, 37 ]
```

اما می‌خواهیم این تابع را خودمان بنویسیم. ابتدا با استفاده از یک ویرایشگر مثلاً notepad ، دستورات زیر را در یک فایل مثلاً به نام fc.txt قرار می‌دهیم. توجه کنید هر تابع تعدادی متغیر محلی دارد که حتماً باید در ابتدای تعریف تابع با دستور local معرفی شوند. در برنامه زیر i و res متغیر های محلی هستند. در بین اعداد ۲ تا $\frac{n}{۲}$ اعداد اولی را می‌یابیم که n بر آن‌ها بخشپذیر است. در صورتی که i اول باشد باید تعداد تکرارهای i به عنوان شمارنده‌ی n معلوم شود. این کار با حلقه while انجام می‌شود. ساختار یک حلقه while به صورت

while شرط do بدنه od;

است، که در آن "شرط" یک عبارت بولی است و تا وقتی که حاصل شرط true باشد، "بدنه" که حاوی دستورات مورد نیاز است، اجرا می‌شود. ساختار یک حلقه for به صورت

for var in L do بدنه od;

است، که در آن var یک متغیر و L یک لیست است و به ازای همه‌ی اعضای لیست L "بدنه" که حاوی دستورات مورد نیاز است اجرا می‌شود. ساختار عبارت شرطی به صورت

if شرط بدنه۲ else بدنه۱ fi;

است، که در آن "شرط" یک عبارت بولی است که اگر حاصل آن true باشد، دستورات که در "بدنه۱" قرار دارند و اگر حاصل آن false باشد، دستورات که در "بدنه۲" قرار دارند، اجرا می‌شوند. البته می‌توان در عبارت شرطی، else را به کار نبرد. هم‌چنین در عبارتهای شرطی می‌توان عبارتهای شرطی دیگر و حلقه‌های while و for را به کار برد.

```
fac:=function(n)
        local i,res;    res:=[];
        for i in [2..Int(n/2)] do
                        if IsPrime(i) then
                                while n mod i =0 do
                                        Add(res,i);    n:=n/i;
                                od;
                        fi;
        od;
        if res=[] then return [n];   else return res;
        fi;
 end;
```

اکنون برنامه‌ای را که در فایل fc.txt قرار داده‌ایم با استفاده از دستورر عدد در داخل GAP می‌خوانیم. اگر مثلاً fc.txt در درایو D و در دایرکتوری gp قرار داشته باشد می‌نویسیم

```
gap>Read("D:/gp/fc.txt");
 function( n ) ... end
```

و سپس تابع fac را برای اعداد داده شده اجرا می‌کنیم. در صورتی که برنامه نوشته شده در فایل fc.txt ایراد داشته باشد GAP خطوط اشکال‌دار را مشخص می‌کند. ابتدا باید اشکال برنامه را رفع کرد و سپس دوباره فایل را به داخل GAP خواند.

```
gap>fac(1962);
 [ 2, 3, 3, 109 ]
gap>fac(1999);     fac(1998);
 [ 1999 ]
 [ 2, 3, 3, 3, 37 ]
```

در GAP امکان نوشتن برنامه به صورت بازگشتی وجود دارد. در مثال بعد برنامه‌ای به صورت بازگشتی می‌نویسیم.

مثال ۲.۳.۱۶. برنامه‌ای به نام fib بنویسید که دنباله‌ی فیبوناچی $f(۱)=f(۲)=۱$، $f(n)=f(n-۱)+f(n-۲)$ را محاسبه کند. سپس $fib(۱۵)$ را بیابید.

حل در GAP تابعی به نام Fibonacci وجود دارد که nامین جمله‌ی دنباله‌ی فیبوناچی را محاسبه می‌کند.

```
gap>Fibonacci(5);     Fibonacci(15);
 5
 610
```

اما می‌خواهیم خودمان برنامه‌ای بنویسیم که این کار را انجام دهد. این کار را به صورت یک برنامه‌ی بازگشتی انجام می‌دهیم

```
gap>fib:=function(n)
>       if n in [1,2] then
>                       return 1;
>                       else return fib(n-1)+fib(n-2);
>       fi;
> end;
 function( n ) ... end
```

این برنامه را برای دو عدد ۵ و ۵۱ امتحان می‌کنیم

```
gap>fib(5);     fib(15);
 5
 610
```

تمرین‌ها (با استفاده از GAP)

۱. تابعی بنویسید که همه‌ی مکان‌های عضو داده شده را در یک لیست بیابید.

۲. برنامه‌ای بنویسید که یک ماتریس $n \times n$ را گرفته و قرینه‌ی آینه‌ای آن را نسبت به قطر اصلی بیابید.

۳. مساله‌ی قبل را با فطر فرعی حل کنید.

۴. برنامه‌ای بنویسید که یک ماتریس $m \times n$ و یک ماتریس $n \times ۱$ را گرفته و ماتریس افزوده را تشکیل دهد.

۵. برنامه‌ای بنویسید که ماتریس $m \times n$ را گرفته و آن را به اندازه‌ی ۹۰° در جهت خلاف عقربه‌های ساعت بچرخاند.

۶. برنامه‌ای بنویسید که nامین جمله‌ی دنباله‌ی $a_n = a_{n-۱} + ۲a_{n-۲} - ۳a_{n-۳}^۲$، $a_۰ = ۱$، $a_۱ = ۲$، و $a_۲ = ۳$ را بیابید.

۷. برنامه‌ای بنویسید که ماتریس $m \times n$ و عدد r را گرفته و اعضای ماتریس را به اندازه‌ی r عدد به سمت راست شیفت دهد. مثلاً اگر $r = ۲$ و $a = \begin{bmatrix} ۰ & ۱ & ۲ \\ ۳ & ۴ & ۵ \\ ۶ & ۷ & ۸ \end{bmatrix}$ خروجی برنامه $a = \begin{bmatrix} ۷ & ۸ & ۰ \\ ۱ & ۲ & ۳ \\ ۴ & ۵ & ۶ \end{bmatrix}$ است.

۴.۱۶ مجموعه، رابطه، و تابع در GAP، آزمایشگاه چهارم

در GAP برای نشان دادن مجموعه‌ها از لیست‌ها استفاده می‌شود. بنابراین GAP فقط با مجموعه‌های متناهی سر و کار دارد. برخلاف لیست یک مجموعه عضو تکراری ندارد و هم‌چنین هیچ گونه ترتیبی روی عناصر آن نیست (یعنی نمی‌توان گفت چه عضوی در چه مکانی است). چون یک شیء به یک مجموعه تعلق دارد یا ندارد و چون ترتیب برای مجموعه تعریف نشده، می‌توان عناصر مجموعه را به هر صورت دلخواه کنار هم قرار داد، در GAP به طور قراردادی عناصر مجموعه به ترتیب صعودی قرار می‌گیرند.

مثال ۱.۴.۱۶. لیست [۳, ۲, ۱۱, ۷, ۲, ۵, ۲] را به مجموعه تبدیل کنید.

حل با استفاده از دستور Set می‌توان یک لیست را به مجموعه تبدیل کرد. تابع IsSet برای تشخیص این که یک شیء مجموعه است یا نه به کار می‌رود

```
gap>a:=[3,2,11,7,2,5,2];   b:=Set(a);
 [3, 2, 11, 7, 2, 5, 2]
 [2, 3, 5, 7, 11]
gap>IsSet(a);   IsSet(b);
 false
 true
```

مثال ۲.۴.۱۶. لیست‌های

$$[\text{"۲"}, \text{"۱"}, ۱, \text{"apple"}, \text{"ange"}] \qquad \text{و} \qquad [\text{"ange"}, ۱, \text{"۲"}, ۳, ۸]$$

را به مجموعه تبدیل کنید (به نام‌های a و b) و کمیت‌های زیر را بیابید.
(الف) $a \cup b$، $a \cap b$، $a - b$، و $b - a$.
(ب) عضو ۱ را از مجموعه‌ی a حذف و عضو ۳ را به آن اضافه کنید.

حل ابتدا لیست‌های مورد نظر را به مجموعه تبدیل می‌کنیم

```
gap>a:=Set([“2”,“1”,1,“apple”,“ange”]);
 [ 1, “1”, “2”, “ange”, “apple” ]
gap>b:=Set([“ange”,1,“2”,3,8]);
 [ 1, 3, 8, “2”, “ange” ]
```

(الف) با استفاده از دستورهای Union، Intersection، و Difference می‌توان اجتماع، اشتراک و تفاضل مجموعه‌ها را یافت

```
gap> Union(a,b);          Intersection(a,b);
 [ 1, 3, 8, “1”, “2”, “ange”, “apple” ]
 [ 1, “2”, “ange” ]
gap>Difference(a,b);
 [ “1”, “apple” ]
gap>Difference(b,a);
 [ 3, 8 ]
```

(ب) با استفاده از دستور AddSet و RemoveSet می‌توان یک عضو را به یک مجموعه اضافه و یا یک عضو را از یک مجموعه حذف کرد

```
gap> RemoveSet(a,1); a;
 [ “1”, “2”, “ange”, “apple” ]
gap>AddSet(a,3); a;
 [ 3, “1”, “2”, “ange”, “apple” ]
```

مثال ۳.۴.۱۶. مجموعه‌ی $a = \{۱, ۲, ۳\}$ و رابطه‌های $S = \{(۱, ۱), (۲, ۳), (۳, ۱)\}$ و $R = \{(۱, ۱), (۲, ۳), (۳, ۳), (۱, ۲), (۲, ۱)\}$ روی آن را تعریف کنید.

(الف) معین کنید آیا R و S تابع‌اند؟

(ب) برد R و S را بیابید.

(ج) تصویر ۱ و $\{۱, ۲\}$ را تحت R و S بیابید.

(د) تصویر معکوس $\{۲, ۳\}$ را تحت R و S بیابید.

(هـ) ترکیب S و R و $S \circ R$ را بیابید. آیا $S \circ R$ و $R \circ S$ تابع‌اند؟

حل Domain نامی است که GAP برای مجموعه‌های ساخت‌یافته مجموعه‌ی ساخت‌یافته (ساختارهای جبری) به کار می‌برد. در وهله‌ی اول دامنه (Domain) مجموعه است. هم‌چنین در GAP با استفاده از دستور $\text{GeneralMappingByElements}(a, b, elms)$ یک رابطه روی مجموعه‌ی X، که یک نگاشت کلی از X به خودش است، ساخته می‌شود، که در آن a و b دو دامنه (Domain) هستند و elms لیستی از دوتایی‌های درایه‌های از a، b است و این دوتایی‌ها با استفاده از دستور $\text{Tuple}([x, y])$ به دست می‌دهند، که در آن $x \in a$، $y \in b$

```
gap>a:=Domain([1,2,3]);
 <object>
gap>Elements(a);
 [ 1, 2, 3 ]
gap>IsSet(a);     IsDomain(a);
 false
 true
gap>r1:=[Tuple([1,1]),Tuple([2,2]),Tuple([3,3]),Tuple([1,2]),Tuple([2,1])];
 [ Tuple( [ 1, 1 ] ), Tuple( [ 2, 2 ] ), Tuple( [ 3, 3 ] ), Tuple( [ 1, 2 ] ),
  Tuple( [ 1, 2 ] ), Tuple( [ 2, 1 ] ) ]
```

```
gap>s1:=[Tuple([1,1]),Tuple([1,2]),Tuple([2,1]),Tuple([3,1]) ];;
gap>R:=GeneralMappingByElements(a,a,r1);
 <general mapping: <object> -> <object> >
gap>S:=GeneralMappingByElements(a,a,s1);
 <general mapping: <object> -> <object> >
gap>IsBinaryRelation(R);     IsBinaryRelation(S);
 true
 true
```

(الف)

```
gap>IsMapping(R);     IsMapping(S);
 false
 false
```

(ب)، (ج) با استفاده از دستور $\mathrm{Image}(f)$ برد f به دست می‌آید. هم‌چنین با استفاده از دستور $\mathrm{Images}(f,x)$، یا $\mathrm{Image}(f,x)$، تصویر f روی عضو (یا مجموعه) x به دست می‌آید

```
gap>Image(R);     Image(S);
 [ 1, 2, 3 ]
 [ 1, 2 ]
gap>Images(R,1);
 [ 1, 2 ]
```

(د) با استفاده از دستور $\mathrm{PreImage}(f)$ پیش تصویر f به دست می‌آید. هم‌چنین با استفاده از دستور $\mathrm{PreImage}(f,x)$ پیش تصویر عضو (یا مجموعه) x تحت f به دست می‌آید

```
gap>PreImage(R,[2,3]);     PreImages(R,2);
 [ 1, 2, 3 ]
 [ 1, 2 ]
```

(هـ) اگر R یک رابطه (یا یک تابع) باشد، برای نشان دادن تصویر آن روی یک عضو یا یک مجموعه‌ی x دو روش استفاده می‌شود. یکی نماد $R(x)$ و دیگری نماد $(x)R$. روش استاندارد در نظریه‌ی گروه‌ها استفاده از نماد دوم است. در GAP نیز از روش دوم استفاده می‌شود. بنابراین در روش دوم برای ترکیب روابط (یا توابع) وقتی $R \circ S$ می‌نویسیم که دامنه‌ی R در برد S قرار داشته باشد. در این حالت تصویر x تحت $R \circ S$ عبارت است از $((x)R)S$. با استفاده از دستور $\mathrm{CompositionMapping}(f,g)$ می‌توان ترکیب f و g را یافت. دستوری به نام SetName نیز در GAP وجود دارد که با استفاده از آن می‌توان یک متغیر را نامگذاری کرد به طوری که در خروجی GAP آن نام به جای متغیر ظاهر شود

```
gap>k:=CompositionMapping(R,S);
 CompositionMapping(<general mapping: < object >- >
   <object> > <general mapping: <object> -> <object> > )
gap>Images(k,1);
 [1, 3]
gap>SetName(S,"S");;     SetName(R,"R");;
gap>u:=CompositionMapping(S,R);
 CompositionMapping( S, R )
gap>IsMapping(k);
 false
gap>IsMapping(u);
```

false

مثال ۴.۴.۱۶. تابع f با دامنه‌ی $\{i \mid -۵ \leq i \leq ۲۰\}$ و ضابطه‌ی $f(x) = x^۲ + ۳x - ۲$ تعریف کنید
(الف) برد f را بیابید.
(ب) تصویر f را روی مجموعه‌ی $\{۲, ۳, ۷\}$ و پیش تصویر f را روی $\{-۱, -۲, ۳\}$ بیابید.
(ج) آیا f یک‌به‌یک است؟

حل اگر m و n اعداد صحیح باشند، $[m..n]$ همه‌ی اعداد صحیح بین m و n را به دست می‌دهد. برای تعریف یک تابع با دامنه، هم دامنه (مجموعه‌ای که مقادیر تابع در آن قرار می‌گیرند) و ضابطه‌ی مشخص از دستور $\text{MappingByFunction}(a, b, func)$ استفاده می‌کنیم، که در آن a دامنه، b هم‌دامنه، و $func$ ضابطه‌ی تابع است. در این جا هم‌دامنه تابع را مجموعه‌ی اعداد صحیح می‌گیریم

```
gap>f:=MappingByFunction([-5..20],Integers, x->x^2+3*x-2);
 MappingByFunction( [ -5 .. 20 ], Integers, function( x ) ... end )
```

(الف) با استفاده از دستور (Image(f برد تابع f را می‌یابیم

```
gap>im:=Image(f);
[-4,-2,2,8,16,26,38,52,68,86,106,128,152,178,206,236,268, 302,338,376,416,458]
```

اکنون تابع g را تابعی با دامنه‌ی f، هم‌دامنه‌ی برد f، و با همان ضابطه‌ی f تعریف می‌کنیم. بنابراین تنها فرق f و g در هم دامنه آن‌ها است.
با استفاده از دستور $\text{Range}(f)$ هم‌دامنه f به دست می‌آید

```
gap>g:=MappingByFunction([-5..20],im, x->x^2+3*x-2);;
gap>Range(f);
 Integers
gap>Range(g);
 [ -4, -2, 2, 8, 16, 26, 38, 52, 68, 86, 106, 128, 152,
  178, 206, 236, 268, 302, 338, 376, 416, 458 ]
```

(ب) با استفاده از دستور $\text{Image}(f, x)$ تصویر f روی یک مجموعه‌ی x به دست می‌آید. با استفاده از دستور $\text{PreImage}(f, y)$ پیش تصویر f روی یک مجموعه‌ی y به دست می‌آید.

```
gap>Image(f,[2,3,7]);        PreImage(f,[-1,-2,3]);
 [ 8, 16, 68 ]
 [ -3, 0 ]
```

(ج) با استفاده از دستور $\text{IsInjective}(f)$ یا $\text{IsSurjective}(f)$ یک‌به‌یک یا پوشا بودن f معین می‌شود

```
gap>IsInjective(f);          IsSurjective(f);
 false
 false
gap>IsInjective(g);          IsSurjective(g);
 false
 true
```

تمرین‌ها (با استفاده از GAP)

۱. رابطه‌های زیر را تعریف کنید:

$$R = \{(x^۲, x) \mid x \in \{-۵, -۴, \ldots, ۰, ۱, \ldots, ۱۰\}\}$$
$$S = \{(x^۳, x^۲ - ۱) \mid x \in \{-۳, -۲, \ldots, ۰, ۱, \ldots, ۷\}\}$$

(الف) $k = R \circ S$ و $t = S \circ R$ را بیابید.
(ب) آیا k و t تابع‌اند؟
(ج) تصویر k و t را روی $\{-۵, ۳\}$ و پیش تصویر k و t را روی $\{۰, ۱\}$ بیابید.

۲. مجموعه‌ی $a = \{-۱, ۰, \ldots, ۱, ۲, \ldots, ۱۰۰\}$ را در نظر بگیرید و تابع f را با دامنه‌ی a و با ضابطه‌ی $f(x) = x^۳ - x$ تعریف کنید.
(الف) برد f را بیابید.
(ب) بزرگ‌ترین زیرمجموعه‌ی b از a را ، که f روی آن یک‌به‌یک باشد، و $f|_b$ را بیابید.

۵.۱۶ اعمال بیشتر روی مجموعه‌ها و لیست‌ها در GAP، آزمایشگاه پنجم

در این آزمایشگاه دستورات دیگری را برای پردازش لیست‌ها و مجموعه‌ها بررسی می‌کنیم.

مثال ۱.۵.۱۶. مجموعه‌ی $a = \{۱, ۲, ۳, ۴\}$ را تعریف کنید و
(الف) همه‌ی **۳-** تایی‌های حاصل از عناصر a را بیابید.
(ب) همه‌ی **۳-** تایی‌های از عناصر a را بیابید که عناصر این سه تایی‌ها به صورت صعودی مرتب شده باشند.
(ج) همه‌ی زیرمجموعه‌ها همه‌ی زیرمجموعه‌های **۳-** عضوی a را بیابید.
(د) همه‌ی جایگشت‌های حاصل از عناصر a را بیابید.
(هـ) همه‌ی اختلال‌های اعضای a را بیابید؛ یعنی همه‌ی مجموعه‌هایی را بیابید که اعضای‌شان همان اعضای a باشند اما مکان هیچ عضو از مجموعه با مکان آن در a یکی نباشد.

حل (الف) دستور $\text{Tuples}(L, n)$ همه‌ی n- تایی‌های عناصر لیست L را به دست می‌دهد و دستور $\text{NrTuples}(L, n)$ تعداد n- تایی‌های عناصر لیست L را مشخص می‌کند

```
gap>a:=[1,2,3,4];;
gap>Tuples(a,3);     NrTuples(a,3);
 [[1,1,1],[1,1,2],[1,1,3],[1,1,4],[1,2,1], [1,2,2],[1,2,3],[1,2,4],[1,3,1],[1,3,2],
 [1,3,3],[1,3,4],[1,4,1],[1,4,2],[1,4,3], [1,4,4],[2,1,1],[2,1,2],[2,1,3],[2,1,4],
 [2,2,1],[2,2,2],[2,2,3],[2,2,4],[2,3,1], [2,3,2],[2,3,3],[2,3,4],[2,4,1],[2,4,2],
 [2,4,3],[2,4,4],[3,1,1],[3,1,2],[3,1,3], [3,1,4],[3,2,1],[3,2,2],[3,2,3],[3,2,4],
 [3,3,1],[3,3,2],[3,3,3],[3,3,4],[3,4,1], [3,4,2],[3,4,3],[3,4,4],[4,1,1],[4,1,2],
 [4,1,3],[4,1,4],[4,2,1],[4,2,2],[4,2,3], [4,2,4],[4,3,1],[4,3,2],[4,3,3],[4,3,4],
 [4,4,1],[4,4,2],[4,4,3],[4,4,4]]
 64
```

(ب) یک k- تایی نامرتب از عناصر یک لیست L انتخاب k عضو از عناصر L است، که تکرار عناصر L نیز در آن مجاز است. در k -تایی نامرتب ترتیب قرار گرفتن عناصر مهم نیست. با استفاده از دستور $\text{UnorderedTuples}(L, k)$ همه‌ی k- تایی بدون ترتیب از عناصر لیست L به دست می‌آید که عناصر هر k- تایی به صورت صعودی مرتب شده‌اند

```
gap>UnorderedTuples(a,3);     NrUnorderedTuples(a,3);
 [[1,1,1],[1,1,2],[1,1,3],[1,1,4],[1,2,2], [1,2,3],[1,2,4],[1,3,3],[1,3,4],[1,4,4],
 [2,2,2],[2,2,3],[2,2,4],[2,3,3],[2,3,4], [2,4,4],[3,3,3],[3,3,4],[3,4,4],[4,4,4]]
 20
```

(ج) با استفاده از دستور $\text{Combination}(L)$ همه‌ی ترکیبات عناصر لیست L به دست می‌آید. بنابراین در حالتی L مجموعه باشد این دستور همه‌ی زیرمجموعه‌های L را محاسبه می‌کند. دستور $\text{Combination}(L, k)$ همه‌ی ترکیبات k عضوی از عناصر لیست L را می‌یابد. بنابراین در حالتی L مجموعه باشد این دستور همه‌ی زیرمجموعه‌های k عضوی L را می‌یابد

gap>Combinations(a); NrCombinations(a);
[[ ],[1],[1,2],[1,2,3],[1,2,3,4],[1,2,4], [1,3],[1,3,4], [1,4],[2],[2,3],[2,3,4],
[2,4],[3],[3,4],[4]]
16
gap>Combinations(a,3); NrCombinations(a,3);
[[1,2,3],[1,2,4],[1,3,4],[2,3,4]]
4

(د) با استفاده از دستور PermutationsList(L) همه جایگشت‌های عناصر لیست L به دست می‌آید

gap>PermutationsList(a); NrPermutationsList(a);
[[1,2,3,4],[1,2,4,3],[1,3,2,4],[1,3,4,2], [1,4,2,3],[1,4,3,2],[2,1,3,4],[2,1,4,3],
[2,3,1,4],[2,3,4,1],[2,4,1,3],[2,4,3,1], [3,1,2,4],[3,1,4,2],[3,2,1,4],[3,2,4,1],
[3,4,1,2],[3,4,2,1],[4,1,2,3],[4,1,3,2], [4,2,1,3],[4,2,3,1],[4,3,1,2],[4,3,2,1]]
24

(هـ) دستور Derangements(L) همه‌ی اختلال‌های لیست L را به دست می‌دهد

gap>Derangements(a); NrDerangements(a);
[[2,1,4,3],[2,3,4,1],[2,4,1,3], [3,1,4,2],[3,4,1,2],[3,4,2,1],[4,1,2,3],
[4,3,1,2],[4,3,2,1]]
9

(و) با استفاده از دستورهای PartitionsSet(L) و PartitionsSet(L,k)، به ترتیب همه‌ی افرازهای مجموعه‌ی L و همه‌ی افرازهای k عضوی مجموعه‌ی L را به دست می‌دهند

gap>PartitionsSet(a); NrPartitionsSet(a);
[[[1],[2],[3],[4]],[[1],[2],[3,4]], [[1],[2,3],[4]],[[1],[2,3,4]],[[1],[2,4],[3]],
[[1,2],[3],[4]],[[1,2],[3,4]],[[1,2,3],[4]], [[1,2,3,4]],[[1,2,4],[3]], [[1,3],[2],[4]],
[[1,3],[2,4]],[[1,3,4],[2]],[[1,4],[2],[3]], [[1,4],[2,3]]]
15
gap>PartitionsSet(a,3);
[[[1],[2],[3,4]],[[1],[2,3],[4]],[[1],[2,4],[3]],
[[1,2],[3],[4]],[[1,3],[2],[4]],[[1,4],[2],[3]]]

تمرین‌ها (با استفاده از GAP)

۱. بدون استفاده از دستور Combination و دستورات مشابه برنامه‌ای بنویسید که همه‌ی زیرمجموعه‌های یک مجموعه را، که شامل اعضای خاصی از مجموعه باشند، بیابید.

۲. دستور یا دستوراتی بنویسید که از همه‌ی k- تایی‌های متشکل از دو شیء داده شده را بسازد که دو عضو اول هر k- تایی متفاوت باشد.

۳. دستور یا دستوراتی بنویسید که همه‌ی زیرمجموعه‌های k عضوی شامل یک مجموعه داده شده از یک مجموعه را بیابد و با استفاده از آن همه‌ی زیرمجموعه‌های ۳ عضوی از مجموعه‌ی $\{۱, ۲, ۳, ۴, ۵\}$ را که شامل $\{۱, ۳\}$ هستند بیابید.

۴. دستور یا دستوراتی بنویسید که همه‌ی افرازهای k عضوی شامل یک مجموعه‌ی داده شده از یک مجموعه را بیابد و با استفاده از آن همه‌ی افرازهای ۳ عضوی از مجموعه‌ی $\{۱, ۲, ۳, ۴, ۵\}$ را که شامل $\{۱, ۳\}$ هستند را بیابید.

۶.۱۶ جایگشت‌ها در GAP، آزمایشگاه ششم

GAP ابزار بسیار قوی برای تعریف و انجام اعمال بسیار متنوع بر گروه‌های جایگشتی است. در این جا تعدادی از دستورهای ساده را در پردازش گروه‌های جایگشتی بررسی می‌کنیم. همان طور که قبلاً اشاره شد در ترکیب توابع در GAP از چپ به راست انجام می‌شود. بنابراین تصویر نقطه x تحت تابع مرکب $f \circ g$ عبارت است از $((x)f)g$. به خصوص به این نکته در ضرب جایگشت‌ها دقت کنید.

مثال ۱.۶.۱۶. جایگشت‌های $a = (۱\ ۲\ ۴)(۲\ ۴)$ و $b = (۲\ ۳)(۳\ ۴\ ۵)$ را تعریف، و عبارت‌های زیر محاسبه کنید.
(الف) ab، $aba^{-۱}$، $bab^{-۱}$، $a^{-۱}ba$، $b^{-۱}ab$.
(ب) مقدار جایگشت $a^۲b^۲$ در ۱ و ۲.
(ج) مرتبه‌ی a، b، $a^۲b$. (مرتبه‌ی یک جایگشت α کوچک‌ترین عدد طبیعی n است که $\alpha^n = (۱)$.)
(د) کوچک‌ترین زیرگروه‌هایی که به ترتیب شامل جایگشت‌های a و b و شامل جایگشت b باشند.

حل در GAP برای تعریف یک جایگشت باید آن را به صورت حاصل‌ضرب دورهای مجزا نوشت و حروف را با استفاده از کاما از یکدیگر جدا کرد. در این جا جایگشت‌های a و b مجزا نیستند. اگر بخواهیم به صورت داده شده آن ها را تعریف کنیم با پیغام خطای GAP مواجه خواهیم شد:

```
gap>a:=(1,2,4,3)(4,2);   b:=(2,3)(3,4,5);
 Permutation: cycles must be disjoint and duplicate-free
 Permutation: cycles must be disjoint and duplicate-free
```

برای این که خودمان تجزیه دوری جایگشت‌های a و b را به دست نیاوریم آن‌ها را به عنوان حاصل‌ضرب جایگشت‌های تجزیه داده شده می‌نویسیم. دو جایگشت را با علامت $*$ با یکدیگر ترکیب می‌کنیم. در این حالت GAP حاصل‌ضرب ترکیب را به صورت دورهای مجزا می‌یابد

```
gap>a:=(1,2,4,3)*(4,2);   b:=(2,3)*(3,4,5);
 (1,4,3)
 (2,4,5,3)
```

(الف) برای ضرب عناصر گروه‌ها از $*$ استفاده می‌کنیم. هم‌چنین می‌توانیم عبارت $a^{-۱}ba$ (مزدوج b توسط a) را با b^a نشان دهیم

```
gap>a*b^2;      a*b*a^-1;
 (1,3)(2,5)
 (1,5,4,2)
gap>b^(a^-1);      b^2*a;
 (1,5,4,2)
 (1,4)(2,5)
gap>b^-1*a*b;      a^b;
 (1,5,2)
 (1,5,2)
```

(ب) برای یافتن مقدار جایگشت a در نقطه‌ی x می‌نویسیم x^a

```
gap>1^(a^2*b^3);
 5
gap>2^(a^2*b^3);
 3
```

(ج) مرتبه‌ی عضو a در یک گروه با استفاده از دستور $\mathrm{Order}(a)$ به دست می‌آید

```
gap>Order(a);   Order(b);
 3
 4
```

```
gap>Order(a^2*b);
 6
```

(د) اگر a، b، c، ... اعضای یک گروه G باشند دستور $\mathrm{Group}(a,b,c,\ldots)$ کوچک‌ترین گروهی (واقع در G) که شامل a، b، c، ... است را محاسبه می‌کند، که آن را زیرگروه تولید شده توسط a، b، c، ... گوییم. بنابراین اگر H گروهی مشمول در G (زیرگروه G) باشد که شامل a، b، c، ...، آن‌گاه شامل زیرگروه تولید شده توسط a، b، c، ... نیز هست. با استفاده از دستورهای $\mathrm{Size}(G)$ و $\mathrm{Elements}(G)$ به ترتیب، تعداد اعضا و همه‌ی اعضای گروه G را می‌یابیم

```
gap>G:=Group(a,b);    Size(G);
 Group([ (1,4,3), (2,4,5,3) ])
 120
gap>H:=Group(b);    Size(H);
 Group([ (2,4,5,3) ])
 4
gap>Elements(H);
 [ (), (2,3,5,4), (2,4,5,3), (2,5)(3,4) ]
```

بنابراین گروه تولید شده توسط جایگشت‌های a و b برابر S_5 است و تعداد اعضای گروه تولید شده توسط جایگشت b برابر ۴ است.

مثال ۲.۶.۱۶. گروه‌های S_4 و A_4 را تعریف کنید و
(الف) تعداد اعضای آن ها را بیابید و عناصر آن‌ها را فهرست کنید.
(ب) عناصر هم‌مرتبه را کنار هم قرار دهید.
(ج) دو عضو x, y را در یک گروه مزدوج نامیم هرگاه عضو g از گروه وجود داشته باشد که $y = g^{-1}xg$. رابطه‌ی مزدوجی روی یک گروه رابطه‌ای هم‌ارزی است. مزدوج‌های (۱, ۲, ۳) را در S_4 و در A_4 بیابید.
(د) رده‌های مزدوجی S_4 و A_4 را بیابید. از هر رده‌ی مزدوجی یک نماینده انتخاب کنید.

حل گروه‌های متناوب و متقارن روی n حرف را به سادگی و با دستورات $\mathrm{Alt}(n)$ و $\mathrm{Sym}(n)$ می‌توان یافت. در زیر S_4 را در متغیر s و A_4 را در متغیر a قرار می‌دهیم

```
gap>a:=AlternatingGroup(4);  s:=SymmetricGroup(4);
 Alt( [ 1 .. 4 ] )
 Sym( [ 1 .. 4 ] )
```

(الف) برای یافتن تعداد اعضا و فهرست کردن اعضای گروه‌ها از دستورهای $\mathrm{Size}(G)$ و $\mathrm{Elements}(G)$ استفاده می‌کنیم. عناصر $a = A_4$ را در متغیر ea و عناصر $s = S_4$ را در متغیر es قرار می‌دهیم

```
gap>Size(a);
 12
gap>Size(s);
 24
gap>ea:=Elements(a);
 [(),(2,3,4),(2,4,3),(1,2)(3,4),(1,2,3),(1,2,4),(1,3,2),
 (1,3,4),(1,3)(2,4),(1,4,2),(1,4,3),(1,4)(2,3)]
gap>es:=Elements(s);
 [(),(3,4),(2,3),(2,3,4),(2,4,3),(2,4), (1,2),(1,2)(3,4),(1,2,3),(1,2,3,4),
 (1,2,4,3),(1,2,4),(1,3,2),(1,3,4,2), (1,3),(1,3,4),(1,3)(2,4),(1,3,2,4),
 (1,4,3,2),(1,4,2),(1,4,3),(1,4),(1,4,2,3),(1,4)(2,3)]
```

(ب) الگوریتمی که برای قرار دادن اعضای هم مرتبه اختیار می‌کنیم به صورت زیر است. ابتدا مرتبه‌ی همه‌ی عناصر گروه داده شده را می‌یابیم.

سپس به ازای هر عدد که مرتبه‌ی یک از اعضای گروه باشد همه‌ی اعضای دیگر با آن مرتبه را می‌یابیم و در کنار یک‌دیگر قرار می‌دهیم. این الگوریتم را می‌توان برای $a = a_4$ با عناصر ea با برنامه زیر به زبان GAP نوشت و آن را اجرا کرد

```
gap>sameorder:=function(G)
>               local eG,r,t,i;  r:=[];   eG:=Elements(G);
>               t:=Set(eG,x->Order(x));
>               for i in t do
>                   Add(r,[i,Filtered(eG,x->Order(x)=i)]);
>               od;
>          return r;
>      end;
 function( G ) ... end
gap>sameorder(ea);
 [[1,[()]],[2,[(1,2)(3,4),(1,3)(2,4),(1,4)(2,3)]],
 [3,[(2,3,4),(2,4,3),(1,2,3),(1,2,4),(1,3,2), (1,3,4),(1,4,2),(1,4,3)]]]
```

اگر برنامه را برای $s = S_4$ اجرا کنیم خواهیم داشت

```
gap>sameorder(es);
 [[1,[()]],[2,[(3,4),(2,3),(2,4),(1,2),(1,2)(3,4),(1,3),(1,3)(2,4),(1,4),(1,4)(2,3)]],
 [3,[(2,3,4),(2,4,3),(1,2,3),(1,2,4), (1,3,2),(1,3,4),(1,4,2),(1,4,3)]],
 [4,[(1,2,3,4),(1,2,4,3),(1,3,4,2),(1,3,2,4), (1,4,3,2),(1,4,2,3)]]]
```

(ج) دستور ConjugacyClass(G, x) رده‌ی مزدوجی عضو x در گروه G را محاسبه می‌کند. سپس با استفاده از دستور Elements می‌توان همه اعضای آن را یافت

```
gap>ConjugacyClass(a,(1,2,3));
 (1,2,3)^G
gap>Elements(last);
 [(2,4,3),(1,2,3),(1,3,4),(1,4,2)]
gap>cs:=ConjugacyClass(s,(1,2,3));
 (1,2,3)^G
gap>Elements(cs);
 [(2,3,4),(2,4,3),(1,2,3),(1,2,4),(1,3,2), (1,3,4),(1,4,2),(1,4,3)]
```

(د) دستور ConjugacyClasses(G) همه‌ی رده‌های مزدوجی گروه G را به دست می‌دهد

```
gap>ca:=ConjugacyClasses(a);
 ()^G,(1,2)(3,4)^G,(1,2,3)^G, (1,2,4)^G]
gap>List(ca,x->Elements(x));
 [[()],[(1,2)(3,4),(1,3)(2,4),(1,4)(2,3)], [(2,4,3),(1,2,3),(1,3,4),(1,4,2)],
 [(2,3,4),(1,2,4), (1,3,2),(1,4,3)]]
gap>List(ConjugacyClasses(s), x->Elements(x));
 [[()],[(3,4),(2,3),(2,4),(1,2),(1,3),(1,4)],[(1,2)(3,4),(1,3)(2,4),(1,4)(2,3)],
 [(2,3,4),(2,4,3),(1,2,3),(1,2,4),(1,3,2),(1,3,4), (1,4,2),(1,4,3)],
 [(1,2,3,4),(1,2,4,3),(1,3,4,2),(1,3,2,4),(1,4,3,2),(1,4,2,3)]]
```

مثال ۳.۶.۱۶. توابع $f, g : S_3 \longrightarrow S_3$ را با ضابطه‌های $f(x) = x * (1\ 2)$ و $g(x) = x^2$ را تعریف کنید.
(الف) یک‌به‌یک و پوشا بودن آن ها را بررسی کنید.

(ب) تصویر این توابع را روی چند عضو S_3 بیابید.

حل ابتدا S_3 را تعریف و سپس با استفاده از دستور MappingByFunction توابع مورد نظر را تعریف می‌کنیم

```
gap>s3:=SymmetricGroup(3);;  SetName(s3,"S3");
gap>f:=MappingByFunction(s3,s3,x->x*(1,2));
 MappingByFunction( S3, S3 ), function( x ) ... end )
gap>g:=MappingByFunction(s3,s3,x->x^2);
 MappingByFunction( S3, S3 ), function( x ) ... end )
```

(الف) یک‌به‌یک و پوشا بودن f و g را بررسی می‌کنیم و برد g را می‌یابیم

```
gap>IsInjective(f);  IsInjective(g);
 true
 false
gap>IsSurjective(f);  IsSurjective(g);
 true
 false
gap>Image(g);
 [ (), (1,2,3), (1,3,2) ]
```

(ج) تصویر f و g را روی تعدادی از اعضای S_3 می‌یابیم

```
gap>(1,2)^f; (1,2,3)^g;
 ()
 (1,3,2)
gap>(2,3)^f; (1,3,2)^g;
 (1,2,3)
 (1,2,3)
```

مثال ۴.۶.۱۶. فرض کنید $n \geq 2$ عدد صحیح باشد. عضوهای x_1، x_2، ...، x_n از یک گروه را n- جایگشت‌پذیر گوییم هرگاه جایگشت غیرهمانی $\sigma \in S_n$ وجود داشته باشد که

$$x_1 x_2 \cdots x_n = x_{\sigma(1)} x_{\sigma(2)} \cdots x_{\sigma(n)}.$$

زیرمجموعه‌ی L از یک گروه را n- جایگشت‌پذیر نامیم هرگاه هر n عضو آن n- جایگشت‌پذیر باشد. برنامه‌ای بنویسید که تعیین کند زیرمجموعه‌ی داده شده از یک گروه n- جایگشت‌پذیر هست یا نه.

حل تابعی به نام nper می‌نویسیم که زیرمجموعه‌ی SG از یک گروه و عدد طبیعی n را گرفته و تعیین کند که آیا SG ، n- جایگشت‌پذیر است؟ الگوریتم برنامه را به صورت زیر در نظر می‌گیریم :

مرحله‌ی اول : عناصر گروه متقارن S_n را به دست آورده و جایگشت همانی را از آن حذف می‌کنیم.

مرحله‌ی دوم: مجموعه‌ی همه‌ی n- تایی‌های متمایز از عناصر SG را تشکیل می‌دهیم.

مرحله‌ی سوم: به ازای هر n- تایی $[x_1, \ldots, x_n]$ از عناصر SG جایگشت غیرهمانی a را در نظر می‌گیریم. اگر $x_1 x_2 \cdots x_n = x_{a(1)} x_{a(2)} \cdots x_{a(n)}$، آنگاه n- تایی $[x_1, \ldots, x_n]$، n- جایگشت‌پذیر است. در این حالت n- تایی دیگری انتخاب می‌کنیم و این مرحله را تکرار می‌کنیم تا جایی که همه‌ی n- تایی‌ها تمام شوند. در این صورت SG ، n- جایگشت‌پذیر است. اگر $x_1 x_2 \cdots x_n \neq x_{a(1)} x_{a(2)} \cdots x_{a(n)}$، آنگاه جایگشت بعدی را امتحان می‌کنیم. اگر برای همه‌ی جایگشت‌ها تساوی برقرار نشود، آنگاه این n- تایی و در نتیجه SG جایگشت‌پذیر نیست. در غیر این صورت این n- تایی جایگشت‌پذیر است و n- تایی دیگری را انتخاب می‌کنیم و این مرحله را تکرار می‌کنیم.

این تابع را مثلاً در مسیر D:/gp/f۲.txt قرار می‌دهیم. در این برنامه برای یافتن همه‌ی جایگشت‌های یک لیست از تابع $\text{Permuted}(L, a)$ استفاده می‌کنیم. در این دستور اگر L برابر لیست $[x_1, x_2, \ldots, x_n]$ و a یک جایگشت

در S_n باشد، دستور $\text{Permuted}(L,a)$ لیست $[x_{a(1)}, x_{a(2)} \ldots, x_{a(n)}]$ را به دست می‌دهد. این تابع عبارت است از

```
nper:=function(SG,n)
  local a,sn,ntup,i,tag;
  sn:=Set(Elements(SymmetricGroup(n)));
  RemoveSet(sn,());
  ntup:=Filtered(UnorderedTuples(SG,n),u->Length( Set(u) )=Length(u) );
   for i in [1..Length(ntup)] do
     tag:=0;
     for a in sn do
      if Product(ntup[i])=Product(Permuted(ntup[i],a)) then
        tag:=1; break;
      fi;
     od;
     if tag=0 then
      return [“is not ”, n,“-permutable”, ntup[i]];
     fi;
   od;
    return [“is ”, n, “-permutable”];
 end;;
```

اکنون برنامه‌ی نوشته شده را به داخل GAP فرامی‌خوانیم و برای گروه S_3 اجرا می‌کنیم

```
gap>Read(“D:/gp/f2.txt”);
gap>s3:=Set(Elements(SymmetricGroup(3)));;
RemoveSet(s3,());   s3;
[ (2,3), (1,2), (1,2,3), (1,3,2), (1,3) ]
gap>nper(s3,2);
[ “is not ”, 2, “-permutable”, [ (2,3), (1,2) ] ]
gap>nper(s3,3);
[ “is not ”, 3, “-permutable”, [ (2,3), (1,2,3), (1,3) ] ]
gap>nper(s3,4);
[ “is ”, 4, “-permutable” ]
```

بنابراین S_3 ، ۴-جایگشت‌پذیر است اما برای هر $n < 4$، n- جایگشت‌پذیر نیست. حال برنامه را برای S_4 اجرا می‌کنیم

```
gap>s4:=Set(Elements(SymmetricGroup(4)));;
gap>RemoveSet(s4,());
gap>nper(s4,2);
[ “is not ”, 2, “-permutable”, [ (3,4), (2,3) ] ]
gap>nper(s4,3);
[ “is not ”, 3, “-permutable”, [ (3,4), (2,3), (1,2) ] ]
gap>nper(s4,4);
[ “is not ”, 4, “-permutable”, [ (3,4), (2,3), (1,2), (1,2,4,3) ] ]
gap>nper(s4,5);
[ “is not ”, 5, “-permutable”,
```

[(2,3), (1,2,4), (1,3,4,2), (1,3,2,4), (1,4,2)]]

gap>nper(s4,6);

[“is ”, 6, “-permutable”]

بنابراین $S_۴$، ۶-جایگشت‌پذیر است اما برای هر $n < ۶$، n- جایگشت‌پذیر نیست.

تمرین‌ها (با استفاده از GAP)

۱. فرض کنید $n \geq ۲$ عدد صحیح باشد. عضوهای $x_۱$، $x_۲$، ...، x_n از یک گروه را n- بازنویس‌پذیر گوییم هرگاه دو جایگشت متمایز $\tau, \sigma \in S_n$ وجود داشته باشند که

$$x_{\tau(۱)}x_{\tau(۲)}\cdots x_{\tau(n)} = x_{\sigma(۱)}x_{\sigma(۲)}\cdots x_{\sigma(n)}.$$

زیرمجموعه‌ی L از یک گروه را n- بازنویس‌پذیر نامیم هرگاه هر n عضو آن n- بازنویس‌پذیر باشد. برنامه‌ای بنویسید که تعیین کند که زیرمجموعه‌ی داده شده از یک گروه n- بازنویس‌پذیر هست یا نه.

۲. گروه G را (m, n)- جایگشت‌پذیر تحدیدی گوییم هرگاه برای هر n زیرمجموعه‌ی m عضوی $X_۱$، ...، X_n از G جایگشت نابدیهی $\sigma \in S_n$ وجود داشته باشد که

$$X_۱X_۲\cdots X_n \cap X_{\sigma(۱)}X_{\sigma(۲)}\cdots X_{\sigma(n)} \neq \emptyset.$$

برنامه‌ای بنویسید که تعیین کند گروه G، (m, n) جایگشت‌پذیر تحدیدی است یا نه.

۳. جایگشت‌های

$$\alpha = (۱\ ۴\ ۳\ ۷\ ۵)(۶\ ۲)(۳\ ۷\ ۴\ ۶)(۲\ ۵\ ۴),$$
$$\beta = (۳\ ۴\ ۲\ ۶\ ۵)(۱\ ۵)(۴\ ۲\ ۳\ ۷),$$
$$\gamma = (۳\ ۴\ ۱\ ۶\ ۵\ ۸)(۷\ ۱)(۵\ ۴\ ۸)(۱\ ۶\ ۳)(۳\ ۸\ ۷)$$

را به دورهای مجزا تجزیه و عبارت‌های زیر را محاسبه کنید

(الف) $\alpha\beta$ (ب) $\beta\alpha$ (ج) $\alpha\beta\sigma^{-۱}$

(د) $\sigma\alpha^{۲}$ (هـ) $\beta\alpha\beta^{-۱}$ (و) $\beta^{۲}\sigma^{-۲}$

۴. ساختار دوری، مرتبه‌ی اعضا، و توازن (زوج یا فرد بودن) اعضای $S_۶$ را مشخص کنید.

۵. مرتبه و زوج یا فرد بودن جایگشت‌های زیر را مشخص کنید.

(الف) $(۲\ ۶)(۲\ ۳\ ۴)(۱\ ۲\ ۵)$ (ب) $(۳\ ۶\ ۷\ ۱)(۲\ ۳)(۱\ ۲\ ۵)$.

۶. دستوری بنویسید که تعداد نقاط ثابت یک جایگشت را بیابید.

۷. فرض کنید G یک گروه و S زیرمجموعه‌ی از G باشد که شامل عضو همانی نیست. گراف جهت‌دار (دی‌گراف) $\mathrm{Cay}(G, S)$ را به صورت زیر تعریف می‌کنیم: رئوس گراف $\mathrm{Cay}(G, S)$ همان عناصر G هستند. کمانی از عضو $a \in G$ به عضو $b \in G$ وجود دارد هرگاه $ab^{-۱} \in S$. این گراف را دی‌گراف کیلی گوییم.

(الف) برنامه‌ای بنویسید که دی‌گراف کیلی $\mathrm{Cay}(G, S)$ را بیابد.

(ب) برنامه‌ای بنویسید که مشخص کند بین دو عضو یک گروه مسیری در دی‌گراف کیلی $\mathrm{Cay}(G, S)$ وجود دارد یا نه.

۷.۱۶ اعداد صحیح در GAP، آزمایشگاه هفتم

در این آزمایشگاه تعدادی تابع دیگر در GAP را معرفی می‌کنیم. هم‌چنین نحوه‌ی تعریف توابع، برنامه‌نویسی با GAP، استفاده از جملات شرطی، حلقه‌های for و while را به طور کامل‌تر بررسی می‌کنیم.

مثال ۱.۷.۱۶. برنامه‌ای به نام gcd بنویسید که بزرگ‌ترین مقسوم‌علیه مشترک دو عدد را بیابید.

حل در GAP تابعی به نام Gcd وجود دارد که بزرگ‌ترین مقسوم‌علیه مشترک هر تعداد عدد صحیح را می‌یابد. هم‌چنین تابع Gcdex، علاوه بر یافتن بزرگ‌ترین مقسوم‌علیه مشترک m و n اعداد ، اعداد t و s را می‌یابد که $d = tm + sn$

```
gap> Gcd(60,63);
 3
gap> Gcdex(15,20);
 rec( gcd := 5, coeff1 := -1, coeff2 := 1, coeff3 := 4, coeff4 := -3 )
```

بنابراین $۵ = (-۱) \times ۱۵ + (۱) \times ۲۰$.

```
gap> Gcdex(125,66);
 rec( gcd := 1, coeff1 := -19, coeff2 := 36, coeff3 := 66, coeff4 := -125 )
```

بنابراین $۱ = (-۱۹) \times ۱۲۵ + (۳۶) \times ۶۶$. اما می‌خواهیم برنامه را خودمان بنویسیم

```
gap> gcd:=function(a,b)
>               local c;
>               while b<>0 do
>                       c:=b;
>                       b:=a mod b;
>                       a:=c;
>               od;
>           return c;
>       end;
 function( a, b ) ... end
gap> gcd(60,63);
 3
```

مثال ۲.۷.۱۶. تابعی به نام nparts بنویسید که تعداد افرازهای عدد طبیعی n را محاسبه کند.

حل مجموعه‌ی همه‌ی افرازهای عدد طبیعی n را می‌توان به دو زیرمجموعه نسبت به بزرگ‌ترین عضو تقسیم کرد. بنابراین تعداد افرازهای n برابر است با مجموع افرازهای $n-i$ با عناصر کمتر از i، به ازای هر i به طور کلی‌تر تعداد افرازهای n با عناصر کمتر از m برابر مجموع تعداد افرازهای $n-i$ با عناصر کمتر از i، برای هر i کمتر از m و n است. این توصیف به تابع زیر منجر می‌شود. در تابع زیر از یک تابع دیگر که در متن تابع تعریف شده و در واقع متغیر محلی است استفاده می‌کند. هم‌چنین از تابع Minimum استفاده کرده‌ایم که می‌نیمم اعداد داده شده را می‌یابد

```
gap> nparts:=function(n)
>       local np;
>       np:=function(n,m)
>               local i,res;
>               if n=0 then return 1;
>               fi;
>               res:=0;
>               for i in [1..Minimum(m,n)] do
>                       res:=res+np(n-i,i);
>               od;
>               return res;
```

```
>                end;
>          return np(n,n);
>     end;
 function( n ) ... end
gap> nparts(3);       nparts(7);
 3
 15
```

در GAP تابعی به نام $\text{Partitions}(n)$ وجود دارد که مجموعه‌ی افرازهای عدد طبیعی n را می‌یابد. $\text{Partitions}(n,k)$ مجموعه‌ی افرازهای n را که k جمع‌وند دارند را می‌یابد. در صورتی که از تابع NrPartitions استفاده کنیم تعداد افرازها به دست می‌آید. به مثال‌های زیر توجه کنید

```
gap>NrPartitions(3)      NrPartitions(7);
 3
 15
gap>Partitions(3);
 [ [ 1, 1, 1 ], [ 2, 1 ], [ 3 ] ]
gap>Partitions(7);
 [ [ 1, 1, 1, 1, 1, 1, 1 ], [ 2, 1, 1, 1, 1, 1 ], [ 2, 2, 1, 1, 1 ], [ 2, 2, 2, 1 ],
 [ 3, 1, 1, 1, 1 ], [ 3, 2, 1, 1 ], [ 3, 2, 2 ], [ 3, 3, 1 ], [ 4, 1, 1, 1 ],
 [ 4, 2, 1 ], [ 4, 3 ], [ 5, 1, 1 ], [ 5, 2 ], [ 6, 1 ], [ 7 ] ]
gap> Partitions(7,3);
 [ [ 3, 2, 2 ], [ 3, 3, 1 ], [ 4, 2, 1 ], [ 5, 1, 1 ] ]
gap> NrPartitions(100);
 190569292
gap> OrderedPartitions(5);
 [ [ 1, 1, 1, 1, 1 ], [ 1, 1, 1, 2 ], [ 1, 1, 2, 1 ], [ 1, 1, 3 ],
 [ 1, 2, 1, 1 ], [ 1, 2, 2 ], [ 1, 3, 1 ], [ 1, 4 ], [ 2, 1, 1, 1 ],
 [ 2, 1, 2 ], [ 2, 2, 1 ], [ 2, 3 ], [ 3, 1, 1 ], [ 3, 2 ], [ 4, 1 ], [ 5 ] ]
gap> OrderedPartitions(5,3);
 [ [ 1, 1, 3 ], [ 1, 2, 2 ], [ 1, 3, 1 ], [ 2, 1, 2 ], [ 2, 2, 1 ], [ 3, 1, 1 ] ]
gap> NrOrderedPartitions(100);
 6338253001141147007483516026 88
```

مثال ۳.۷.۱۶. اعضای $\mathbb{Z}_{۱۰}$ را در مجموعه‌ی z10 و اعضای $\mathbb{Z}_۸$ را در مجموعه‌ی z8 قرار دهید.

(الف) اعضای وارون پذیر $\mathbb{Z}_{۱۰}$ و $\mathbb{Z}_۸$ یعنی $\mathbb{Z}_{۱۰}^{\times}$ و $\mathbb{Z}_۸^{\times}$ را بیابید.

(ب) در $\mathbb{Z}_{۱۰}$، ۳×۸، ۹×۹ و در $\mathbb{Z}_۸$، ۳×۸، ۳×۶ و ۷×۷ را بیابید.

(ج) توابع $f : \mathbb{Z}_{۱۰} \to \mathbb{Z}_{۱۰}$، $g : \mathbb{Z}_۸ \to \mathbb{Z}_۸$، $g \circ h : \mathbb{Z}_{۱۰} \to \mathbb{Z}_۸$ با ضابطه‌های $f(x) = x^۲$، $g(x) = ۳x$، $h(\bar{x}) = \bar{x}$ را تعریف کنید.

(د) تصویر ۱، ۵ و ۷ را تحت f و g بیابید.

(هـ) یک‌به‌یک و پوشا بودن f، g و h را بررسی کنید.

(و) تصویر مجموعه‌ی $\{۱, ۳, ۴\}$ را تحت f، تصویر معکوس $\{۲, ۳, ۴\}$ تحت g؛ و تصویر معکوس مجموعه‌های $\{۱\}$، $\{۲, ۳\}$، و $\{۴\}$ را تحت f بیابید.

(ز) برد f، g و h را بیابید.

(ح) $f \circ h$، $h \circ g$ را بیابید. یک‌به‌یک و پوشا بودن آن ها را بررسی کنید.

حل اگر m و n اعداد صحیح باشند و $m < n$، دستور [m..n] همه‌ی اعداد صحیح بین m و n را به دست می‌دهد

```
gap>z10:=[0..9];          z8:=[0..7];
[ 0 .. 9 ]
[ 0 .. 7 ]
```

(الف) با استفاده از دستور $\mathrm{PrimeResidues}(n)$ اعداد کوچک‌تر از n که نسبت به n اول‌اند به دست می‌دهند

```
gap>PrimeResidues(10);          PrimeResidues(8);
[ 1, 3, 7, 9 ]
[ 1, 3, 5, 7 ]
```

(ب) با دستور mod به سادگی می‌توان اعمال جمع و ضرب به پیمانه n را انجام داد

```
gap>8*3 mod 10;    9^2 mod 10;
 4
 1
gap>8*3 mod 8;     7^2 mod 8;
 0
 1
gap>6*3 mod 8;     7^2 mod 8;
 2
 1
```

(ج) تعریف توابع با استفاده از دستور $\mathrm{GeneralMappingByFunction}(a, b, func)$ انجام می‌شود، که در آن a دامنه تابع، b برد تابع، و $func$ تابعی است که به زبان GAP نوشته شده و برای تصویر اعضای a به اعضای b به‌کار می‌رود

```
gap> f:=MappingByFunction(z10,z10,x->x^2 mod 10);
 MappingByFunction( [ 0 .. 9 ], [ 0 .. 9 ], function( x ) ... end )
gap> g:=MappingByFunction(z8,z8,x->3*x mod 8);;
gap> h:=MappingByFunction(z10,z8,x->x mod 8);;
```

(د) تصویر یک عضو x از دامنه تابع f را می‌توان به سادگی و به دو صورت $x\hat{}f$ یا $\mathrm{Image}(f, x)$ یافت

```
gap>Image(f,1);   5^f;    7^f;
 1
 5
 9
gap>Image(g,1);   Image(g,5);    7^g;
 3
 7
 5
```

(هـ) با استفاده از دستورات $\mathrm{IsInjective}(f)$، $\mathrm{IsSurective}(f)$ و $\mathrm{IsBijective}(f)$ می‌توان به ترتیب یک‌به‌یک ، پوشا، و دوسویی بودن تابع f را معین کرد

```
gap>IsInjective(f);      IsInjective(g);      IsInjective(h);
 false
 true
 false
gap>IsSurjective(f);     IsSurjective(g);     IsSurjective(h);
```

```
false
true
true
```

(و) و (ز) با استفاده از دستور Image می‌توان برد تابع f و یا تصویر هر زیر مجموعه دلخواهی از برد تابع را تحت f یافت

```
gap>Image(f);  Image(g);  Image(h);
[ 0, 1, 4, 5, 6, 9 ]
[ 0, 1, 2, 3, 4, 5, 6, 7 ]
[ 0, 1, 2, 3, 4, 5, 6, 7 ]
gap>Image(f,[1,3,4]);  Image(f,[2,3,4]);
[ 1, 6, 9 ]
[ 4, 6, 9 ]
gap>PreImage(f,[1]);  PreImage(f,[2,3]);
[ 1, 9 ]
[ ]
gap>PreImage(f,[4]);  PreImage(g,[2,3,4]);
[ 2, 8 ]
[ 1, 4, 6 ]
```

(ج) با استفاده از دستور $\mathrm{CompositionMapping}(h, f)$ ترکیب دو تابع h و f، یعنی $h \circ f$، به دست می‌آید

```
gap>k:=CompositionMapping(h,f);;
gap>a:=CompositionMapping(g,h);;
gap>Image(k);  Image(a);
[ 0, 1, 4, 5, 6 ]
[ 0, 1, 2, 3, 4, 5, 6, 7 ]
gap>IsInjective(k);  IsInjective(h);  IsInjective(a);
false
false
false
gap>IsSurjective(k);  IsSurjective(a);
false
true
```

تمرین‌ها (با استفاده از GAP)

۱. تابعی بنویسید که gcd و lcm اعداد داده شده را با تجزیه به عوامل اول بیابید.

۲. برنامه‌ای به صورت بازگشتی بنویسید که بزرگ‌ترین مقسوم‌علیه مشترک دو عدد صحیح را بیابید.

۳. برنامه‌ای بنویسید که برای اعداد داده شده m و b، $d = \gcd\{m, n\}$ و اعداد t و s را که $d = sn + tm$ بیابید. برنامه را برای n عدد تعمیم دهید. (بدون استفاده از دستور Gcdex).

۴. برنامه‌ای به نام digits بنویسید که ارقام عدد صحیح داده شده را در یک لیست قرار دهد.

۵. برنامه‌ای به نام $\mathrm{bas}(m, i)$ بیابید که عدد m را در پایه‌ی i بیابد و ارقام آن را در یک لیست قرار دهد.

۶. برنامه‌ای بنویسید که همه شمارنده‌های یک عدد صحیح مثبت را محاسبه کند.

۷. عدد طبیعی n را کامل گوییم، هرگاه برابر مجموع مقسوم‌علیه‌های خودش باشد (مقسوم‌علیه‌های کوچکتر از n). برنامه‌ای با خروجی true یا false بنویسید که کامل بودن عدد طبیعی n را مشخص کند.

۸. با استفاده از تمرین قبل، برنامه‌ای بنویسید که همه‌ی اعداد کامل بین ۱ و عدد داده شده را محاسبه کند.

۸.۱۶ مقدمه‌ای بر گروه‌ها در GAP، آزمایشگاه هشتم

در این آزمایشگاه نحوه‌ی تعریف گروه‌های دوری، گروه‌های ماتریسی، و گروه کواترنیونی و هم‌چنین پردازش آن‌ها را بررسی می‌کنیم.

مثال ۱.۸.۱۶. گروه دوری مرتبه‌ی ۷ و ۱۲ را تعریف کنید.

حل با استفاده از دستور $\mathrm{CyclicGroup}(n)$ گروه دوری مرتبه‌ی n به دست می‌آید. همان طور که ملاحظه می‌کنید در خروجی این دستور نام pc –گروه به آن اطلاق شده است. این رده‌ی گروه‌ها به گروه‌های چند دوری معروف‌اند. این رده را در فصل ۷ بخش ۵ توصیف می‌کنیم. هم‌چنین تعداد مولدهای این گروه ذکر شده است. یک مجموعه‌ی مولد برای یک گروه مجموعه‌ای از اعضای گروه است طوری که هر عضو گروه را بتوان بر حسب (حاصل‌ضرب) توان‌های اعضای این مجموعه نوشت

```
gap>C7:=CyclicGroup(7);    Elements(C7);
 <pc group of size 7 with 1 generators>
 [ <identity> of ..., f1, f1^2, f1^3, f1^4, f1^5, f1^6 ]
```

دستور $\mathrm{CyclicGroup}(\mathrm{IsPermGroup}, n)$ را می‌توان به صورت های دیگری نیز استفاده کرد. یکی از این صورت ها است که در آن گروه دوری مرتبه‌ی n به صورت یک گروه جایگشتی به دست می‌آید. گروه دوری مرتبه‌ی ۷ را به صورت گروه جایگشتی می‌یابیم

```
gap>c7:=CyclicGroup(IsPermGroup,7);
 Group([ (1,2,3,4,5,6,7) ])
gap>Elements(c7);
 [(),(1,2,3,4,5,6,7),(1,3,5,7,2,4,6),(1,4,7,3,6,2,5), (1,5,2,6,3,7,4),
 (1,6,4,2,7,5,3),(1,7,6,5,4,3,2)]
```

با استفاده از دستور $\mathrm{GeneratorsOfGroup}(G)$ مجموعه‌ای از مولدهای گروه G به دست می‌آید. البته این مجموعه‌ی مولد ممکن است از نظر تعداد اعضا می‌نیمال نباشد. با استفاده از دستور $\mathrm{MinimalGeneratingSet}(G)$ یک مجموعه‌ی مولد می‌نیمال حاصل می‌شود

```
gap>GeneratorsOfGroup(C7);   GeneratorsOfGroup(c7);
 [ f1 ]
 [ (1,2,3,4,5,6,7) ]
gap>MinimalGeneratingSet(C7);
 [ f1 ]
gap>MinimalGeneratingSet(C7);
 [ (1,2,3,4,5,6,7) ]
```

اکنون گروه دوری مرتبه‌ی ۱۲ را به صورت pc –گروه و گروه جایگشتی می‌یابیم

```
gap>C12:=CyclicGroup(12);
 <pc group of size 12 with 3 generators>
gap>c12:=CyclicGroup(IsPermGroup,12);
 Group([ (1,2,3,4,5,6,7,8,9,10,11,12) ])
```

حال عناصر C۱۲، گروه دوری مرتبه‌ی ۱۲ را به صورت pc –گروه، و c۱۲، گروه دوری مرتبه‌ی ۱۲ را به صورت گروه جایگشتی فهرست می‌کنیم

```
gap>Elements(C12);
 [ <identity> of ..., f1, f2, f3, f1*f2, f1*f3, f2*f3, f3^2,
```

```
 f1*f2*f3, f1*f3^2, f2*f3^2, f1*f2*f3^2 ]
gap>Elements(c12);
 [(),(1,2,3,4,5,6,7,8,9,10,11,12),(1,3,5,7,9,11)(2,4,6,8,10,12),
 (1,4,7,10)(2,5,8,11)(3,6,9,12), (1,5,9)(2,6,10)(3,7,11)(4,8,12),
 (1,6,11,4,9,2,7,12,5,10,3,8), (1,7)(2,8)(3,9)(4,10)(5,11)(6,12),
 (1,8,3,10,5,12,7,2,9,4,11,6), (1,9,5)(2,10,6)(3,11,7)(4,12,8),
 (1,10,7,4)(2,11,8,5)(3,12,9,6), (1,11,9,7,5,3)(2,12,10,8,6,4),
 (1,12,11,10,9,8,7,6,5,4,3,2)]
```

اکنون مولدهای C۱۲، گروه دوری مرتبه‌ی ۱۲ را به صورت pc -گروه و c۱۲، گروه دوری مرتبه‌ی ۱۲ را به صورت گروه جایگشتی فهرست می‌کنیم

```
gap>GeneratorsOfGroup(C12);
 [ f1, f2, f3 ]
gap>GeneratorsOfGroup(c12);
 [(1,2,3,4,5,6,7,8,9,10,11,12)]
gap>List(GeneratorsOfGroup(C12),x-> Order(x));
 [ 12, 6, 3 ]
```

با استفاده از دستور MinimalGeneratingSet مجموعه‌ی مولد می‌نیمال آن ها را می‌یابیم

```
gap>MinimalGeneratingSet(C12);
 [ f1 ]
gap> MinimalGeneratingSet(c12);
 [ (1,2,3,4,5,6,7,8,9,10,11,12) ]
```

در مثال‌های بعد از تابع sameorder که عناصر هم مرتبه‌ی یک گروه را می‌یابد و آن را در آزمایشگاه ششم تعریف کردیم استفاده می‌کنیم

```
gap>sameorder:=function(G)
>        local eG,r,t,i;   r:=[];  eG:=Elements(G);
>        t:=Set(eG,x-> Order(x));
>        for i in t do
>            Add(r,[i,Filtered(eG,x-> Order(x)=i)]);
>        od;
>     return r;
>     end;;
```

مثال ۲.۸.۱۶. میدانهای متناهی با ۷ و ۱۶ عضو تعریف کنید. عناصر آن‌ها را فهرست کنید. مرتبه‌ی ضربی اعضای میدانها را بیابید.

حل با استفاده از دستور $\mathrm{GF}(m)$ یا $\mathrm{GaliosField}(m)$ میدان متناهی از مرتبه‌ی m به دست می‌آید. اگر F یک میدان متناهی باشد نشان داده می‌شود که: اولاً $|F| = p^r$، که در آن p عدد اول است و $r \in \mathbb{N}$. ثانیاً $F^\times = F - \{0\}$ یک گروه دوری است، یعنی عضوی در $F^\times$ وجود دارد که از توان‌های آن همه اعضای $F^\times$ حاصل می‌شوند. این عضو در GAP با $Z(m)$ نشان داده می‌شود. بنابراین اگر F یک میدان متناهی با $m = p^r$ عضو باشد، آنگاه $F^\times = \{Z(m)^0, Z(m)^1, \ldots, Z(m)^{m-1}\}$.

ابتدا میدان ۷ عضوی F۷ را تعریف می‌کنیم و مرتبه‌ی ضربی عناصر $\mathrm{F7} - \{0\}$ را می‌یابیم

```
gap>F7:=GF(7);   Elements(F7);
 GF(7)
 [ 0*Z(7), Z(7)^0, Z(7), Z(7)^2, Z(7)^3, Z(7)^4, Z(7)^5 ]
gap>G:=Group(Z(7));   Elements(G);
```

```
 <group with 1 generators>
 [ Z(7)^0, Z(7), Z(7)^2, Z(7)^3, Z(7)^4, Z(7)^5 ]
gap>sameorder(G);
 [[0,[0*Z(7)]],[1,[Z(7)^0]],[2,[Z(7)^3]], [3,[Z(7)^2,Z(7)^4]], [6,[Z(7),Z(7)^5]]]
gap>Z(7)^-1;
 Z(7)^5
gap>Z(7)*Z(7)-3;
 Z(7)^3
```

همان طور که ذکر شد مرتبه‌ی هر میدان متناهی توانی از یک عدد اول است. در صورتی که در تعریف میدان متناهی این نکته رعایت نشود با پیغام خطا مواجه خواهیم شد

```
gap>GF(12);
 Error <subfield> must be a prime or a finite field at
 Error( "<subfield> must be a prime or a finite field" );
 <function> ( <arguments> ) called from read-eval-loop
 Entering break read-eval-print loop, you can 'quit;'
 to quit to outer loop, or you can return to continue
 brk>
```

اکنون میدان ۱۶ عضوی F16 را تعریف کرده و مرتبه‌ی ضربی عناصر $\text{F16} - \{0\}$ را می‌یابیم

```
gap>F16:=GF(16);   Elements(F16);
 GF(2^4)
 [0*Z(2),Z(2)^0,Z(2^2),Z(2^2)^2,Z(2^4),Z(2^4)^2,Z(2^4)^3, Z(2^4)^4,Z(2^4)^6,
  Z(2^4)^7,Z(2^4)^8,Z(2^4)^9,Z(2^4)^11,Z(2^4)^12,Z(2^4)^13,Z(2^4)^14]
gap>sameorder(Group(Z(16));
 [[1,<aGF2vectoroflength1> ],
 [3,[Z(2^2),Z(2^2)^2]], [5,[Z(2^4)^3,Z(2^4)^6,Z(2^4)^9,Z(2^4)^12]],
 [15,[Z(2^4),Z(2^4)^2,Z(2^4)^4,Z(2^4)^7,Z(2^4)^8,Z(2^4)^11,
              Z(2^4)^13,Z(2^4)^14]]]
```

مثال ۳.۸.۱۶. گروه‌ها $\mathrm{GL}_۲(F_۳)$ و $\mathrm{SL}_۲(F_۳)$ را تعریف کنید ($F_۳$ میدان ۳ عضوی است). تعداد اعضای آن ها را بیابید. چند عمل جبری روی برخی از اعضای آن ها انجام دهید. از هر رده‌ی مزدوجی عضوی را انتخاب کنید.

حل با استفاده از دستور $\mathrm{GL}(n,m)$ گروه ماتریس‌های وارون‌پذیر با درایه‌های در $\mathrm{GF}(m)$ به دست می‌آید

```
gap>G:=GL(2,3);   Size(G);
 GL(2,3)
 48
gap>eG:=Elements(G);;
gap>eG[1]; eG[2]; eG[2]^-1; eG[2]*eG[4];
 [[0*Z(3),Z(3)^0],[Z(3)^0,0*Z(3)]]
 [[0*Z(3),Z(3)^0],[Z(3)^0,Z(3)^0]]
 [[Z(3),Z(3)^0],[Z(3)^0,0*Z(3)]]
  [[Z(3),0*Z(3)],[Z(3),Z(3)^0]]
```

دستور $\mathrm{Display}(a)$ سطرهای ماتریس a را به طریق معمول نشان می‌دهد

```
gap>Display(eG[2]*eG[4]);
 2 .
 2 1
gap>Display(eG[1]);
 . 1
 1 .
gap>Display(eG[2]^-1);
 2 1
 1 .
```

اکنون از هر رده‌ی مزدوجی $\mathrm{GL}_2(F_3)$ عضوی را انتخاب می‌کنیم

```
gap>List(ConjugacyClasses(G),Representative);
[[[Z(3)^0,0*Z(3)],[0*Z(3),Z(3)^0]], [[0*Z(3),Z(3)^0],[Z(3)^0,0*Z(3)]],
[[0*Z(3),Z(3)^0],[Z(3)^0,Z(3)^0] ], [[0*Z(3),Z(3)^0],[Z(3)^0,Z(3)]],
[[0*Z(3),Z(3)^0],[Z(3),0*Z(3)]], [[0*Z(3),Z(3)^0],[Z(3),Z(3)^0]],
 [[0*Z(3),Z(3)^0],[Z(3),Z(3)]], [[Z(3),0*Z(3)],[0*Z(3),Z(3)]]]
```

با استفاده از دستور $\mathrm{SL}(n,m)$ گروه ماتریس‌های با دترمینان واحد با درایه‌های در $\mathrm{GF}(m)$ به دست می‌آید

```
gap>SG:=SL(2,3);
SL(2,3)
gap>Size(SG);
24
gap>List(ConjugacyClasses(SG),Representative);
[[[Z(3)^0,0*Z(3)],[0*Z(3),Z(3)^0]], [[0*Z(3),Z(3)^0],[Z(3),0*Z(3)]],
 [[0*Z(3),Z(3)^0],[Z(3),Z(3)^0]], [[0*Z(3),Z(3)^0],[Z(3),Z(3)]],
 [[0*Z(3),Z(3)],[Z(3)^0,Z(3)^0]], [[0*Z(3),Z(3)],[Z(3)^0,Z(3)]],
[[Z(3),0*Z(3)],[0*Z(3),Z(3)]]]
```

مثال ۴.۸.۱۶. گروه کواترنیونی Q_8 را تعریف کنید و مرتبه‌ی عناصر آن‌ها را بیابید. رده‌ی مزدوجی عناصر گروه را به دست آورید.

حل عناصر ۱، i، j، k از گروه کواترنیونی پایه یک ساختار جبری موسوم به جبر کواترنیونی هستند. اعضای این ساختار ترکیب خطی از عناصر پایه‌اند، که در آن ضرایب ترکیب خطی از میدان مشخصی مثلاً میدان اعداد گویا هستند. این ساختار یک فضای برداری است. در این ساختار جمع و ضرب عناصر به طور متعارف، با استفاده از عمل جمع و ضرب در میدان داده شده و اعمال ضرب عناصر i، j، k انجام می‌شود. با استفاده از دستور $\mathrm{QuaternionAlgebra}(F)$ جبر کواترنیونی با ضرایب در میدان F به دست می‌آید. دستور $\mathrm{Basis}(V)$ یک پایه از فضای برداری V را به دست می‌دهد

```
gap>q:=QuaternionAlgebra(Rationals);
<algebra-with-one of dimension 4 over Rationals>
gap>Elements(Basis(q));
[ k, j, i, e ]
gap>i:=Elements(Basis(q))[3];;
gap>j:=Elements(Basis(q))[2];;
gap>k:=Elements(Basis(q))[1];;
gap>i*j;
k
```

هر عضو Q_8 حاصل‌ضربی از عناصر i، j است. پس $\{i,j\}$ یک مجموعه‌ی مولد برای Q_8 است. دستور $\mathrm{Group}(gens)$ گروه حاصل از تمام حاصل‌ضرب توان‌های عناصر لیست $gens$ را به دست می‌اورد. این گروه که کوچک‌ترین گروه شامل عناصر $gens$ است را گروه تولید شده توسط $gens$ گوییم

```
gap>q8:=Group(i,j);
 # I default 'IsGeneratorsOfMagmaWithInverses' method returns 'true' for [ i, j ]
 <group with 2 generators>
gap>Elements(q8);
 [ (-1)*e, (-1)*i, (-1)*j, (-1)*k, k, j, i, e ]
gap>sameorder(q8);
 [ [ 1, [ e ] ], [ 2, [ (-1)*e ] ], [ 4, [ (-1)*i, (-1)*j, (-1)*k, k, j, i ] ] ]
gap>List(ConjugacyClasses(q8),x-> Elements(x));
 [ [ e ], [ (-1)*e ], [ (-1)*i, i ], [ (-1)*j, j ], [ (-1)*k, k ] ]
```

تمرین‌ها (با استفاده از GAP)

۱. گروه‌های D_{16} و C_{16} را هم به صورت pc -گروه‌ها و هم به صورت گروه‌های جایگشتی تعریف کنید. رده‌ی مزدوجی عناصر آن‌ها را بیابید.

۲. گروه‌های ماتریسی $\mathrm{GL}_2(F_{27})$ و $\mathrm{SL}_2(F_{27})$ (F_{27} میدان ۲۷ عضوی است) را تعریف کرده و رده‌ی مزدوجی آن ها را بیابید.

۳. مرتبه‌ی هر عضو و هم‌چنین مولدهای گروه‌های C_{12}، C_{15}، C_{17}، C_{38} را بیابید.

۴. مرتبه‌ی هر عضو و هم‌چنین مولدهای گروه‌های $\mathbb{Z}_{12}$، $\mathbb{Z}_{15}$، $\mathbb{Z}_{17}$، $\mathbb{Z}_{38}$ را بیابید.

۵. مرتبه‌ی هر عضو گروه‌های $\mathbb{Z}_{12}^{\times}$، $\mathbb{Z}_{15}^{\times}$، $\mathbb{Z}_{17}^{\times}$، $\mathbb{Z}_{38}^{\times}$ را بیابید.

۶. ماتریس‌های $a=\begin{bmatrix}1 & 1\\ 0 & -1\end{bmatrix}$ و $b=\begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}$ در $\mathrm{GL}_2(\mathbb{R})$ را در نظر بگیرید. ثابت کنید $O(a)=O(b)=2$ و $O(ab)=\infty$.

۷. ماتریس‌های $a=\begin{bmatrix}0 & -1\\ 1 & 1\end{bmatrix}$ و $b=\begin{bmatrix}0 & 1\\ -1 & -1\end{bmatrix}$ در $\mathrm{GL}_2(\mathbb{R})$ را در نظر بگیرید. ثابت کنید $O(a)=4$، $O(b)=3$ و $O(ab)=\infty$.

۸. اعضای $\mathrm{GL}_2(\mathbb{Z}_2)$ را مشخص کرد و مرتبه‌ی آن‌ها را بیابید.

۹. مرتبه‌ی اعضای Q_8 را بیابید.

۹.۱۶ تعدادی گروه دیگر در GAP، آزمایشگاه نهم

در این آزمایشگاه نحوه‌ی تعریف تعداد دیگری از گروه‌ها را بررسی می‌کنیم. گروه‌های دووجهی و دیگر گروه‌ها را به صورت pc -گروه‌ها و گروه‌های جایگشتی تعریف می‌کنیم. هم‌چنین گروه‌های آزاد و نحوه‌ی تعریف گروه‌ها از گروه‌های آزاد را بررسی می‌کنیم.

مثال ۱.۹.۱۶. ۴-گروه کلاین را تعریف کنید و مرتبه‌ی عناصر آن را بیابید. آیا این گروه آبلی است؟ آیا دوری است؟

حل از تابع sameorder که عناصر هم مرتبه‌ی یک گروه را می‌یابد و آن را در آزمایشگاه ششم و هشتم تعریف کردیم استفاده می‌کنیم. ۴-گروه کلاین همان گروه دووجهی مرتبه‌ی ۴ است. با استفاده از دستور $\mathrm{DihedralGroup}(m)$ گروه دووجهی D_m را می‌یابیم

```
gap>D4:=DihedralGroup(4);
 <pc group of size 4 with 2 generators>
```

همان طور که ملاحظه می‌کنید در خروجی این دستور نام pc گروه به آن اطلاق شده است. همان طور که در آزمایشگاه قبل گفته شد این رده‌ی گروه‌ها به گروه‌های چند دوری معروف‌اند، و آن‌ها را در فصل ۷ بخش ۵ بررسی می‌کنیم. هم‌چنین تعداد مولدهای این گروه ذکر شده است. یک مجموعه‌ی مولد برای یک گروه مجموعه‌ای از اعضای گروه است طوری که هر عضو گروه را بتوان بر حسب (حاصل‌ضرب) توان‌های اعضای این مجموعه نوشت

```
gap>Elements(D4);
 [ <identity> of ..., f1, f2, f1*f2 ]
gap>sameorder(D4);
 [ [ 1, [ <identity> of ... ] ], [ 2, [ f1, f2, f1*f2 ] ] ]
```

با استفاده از دستور $\mathrm{IsAbelian}(G)$ آبلی و یا ناآبلی بودن گروه G مشخص می‌شود. هرگاه یک مجموعه‌ی مولد یک عضوی برای گروه وجود داشته باشد، گروه را دوری گوییم. با استفاده از دستور $\mathrm{IsCyclic}(G)$ دوری یا دوری نبودن گروه G معلوم می‌شود

```
gap>IsAbelian(D4);
 true
gap>IsCyclic(D4);
 false
```

دستور DihedralGroup را می‌توان به صورت های دیگری نیز استفاده کرد. یکی از این صورت ها که در آن گروه دووجهی به صورت یک گروه جایگشتی به دست می‌آید عبارت است از $\mathrm{DihedralGroup}(\mathrm{IsPermGroup}, m)$

```
gap>d4:=DihedralGroup(IsPermGroup,4);
 Group([ (1,2), (3,4) ])
gap>Elements(d4);
 [ (), (3,4), (1,2), (1,2)(3,4) ]
gap>sameorder(d4);
 [ [ 1, [ () ] ], [ 2, [ (3,4), (1,2), (1,2)(3,4) ] ] ]
gap>IsAbelian(d4);
 true
gap>IsCyclic(d4);
 false
```

مثال ۲.۹.۱۶. گروه‌های دووجهی مرتبه‌ی ۶ و ۸ را تعریف کنید و مرتبه‌ی عناصر آن‌ها را بیابید. رده‌های مزدوجی این گروه‌ها را به دست آورید.

حل ابتدا گروه‌ها را تعریف می‌کنیم و عناصر هم مرتبه را می‌یابیم

```
gap>D6:=DihedralGroup(6);;
gap>D8:=DihedralGroup(8);;
gap>sameorder(D6);
 [ [ 1, [ <identity> of ... ] ], [ 2, [ f1, f1*f2, f1*f2^2 ] ], [ 3, [ f2, f2^2 ] ] ]
gap>sameorder(D8);
 [ [ 1, [ <identity> of ... ] ], [ 2, [ f1, f3, f1*f2, f1*f3, f1*f2*f3 ] ],
  [ 4, [ f2, f2*f3 ] ] ]
```

اکنون با استفاده از دستور ConjugacyClasses رده‌های مزدوجی D_8 را به دست می‌آوریم

```
gap>List(ConjugacyClasses(D8),x-> Elements(x));
 [ [ <identity> of ... ], [ f1, f1*f3 ], [ f2, f2*f3 ], [ f3 ], [ f1*f2, f1*f2*f3 ] ]
gap>Size(last);
```

5

با استفاده از دستور GeneratorsOfGroup(G) یک مجموعه‌ی مولد برای گروه G به دست می‌آید. توجه کنید مجموعه‌ی مولد یافته شده لزوماً یک مجموعه‌ی مولد با کم‌ترین عضو نیست. هم‌چنین برای پردازش اعضای گروهی که با این مولدها توصیف شده بایستی این مولد ها را نامگذاری کرد. اگر به خود این متغیر ها رجوع کنیم با پیغام خطا مواجه خواهیم شد

```
gap>gens:=GeneratorsOfGroup(D8);
 [ f1, f2, f3 ]
gap>f1;
 Variable: 'f1' must have a value
gap>a:=gens[1];;  b:=gens[2];;  c:=gens[3];;
gap>[Order(a), Order(b), Order(c)];
 [ 2, 4, 2 ]
gap>a*b;   a^2;
 f1*f2
 <identity> of ...
gap>a*c;   a*b*c^2;
 f1*f3
 f1*f2
gap>a*b^2*c;
 f1
```

برخی از اعمال فوق را با استفاده از صورت جایگشتی D_8 انجام می‌دهیم

```
gap>d8:=DihedralGroup(IsPermGroup,8);;
gap>sameorder(d8);
 [ [ 1, [ () ] ], [ 2, [ (2,4), (1,2)(3,4), (1,3), (1,3)(2,4), (1,4)(2,3) ] ],
   [ 4, [ (1,2,3,4), (1,4,3,2) ] ] ]
gap>List(ConjugacyClasses(d8),x-> Elements(x));
 [ [ () ], [ (2,4), (1,3) ], [ (1,2)(3,4), (1,4)(2,3) ],
   [ (1,2,3,4), (1,4,3,2) ], [ (1,3)(2,4) ] ]
gap>gen:=GeneratorsOfGroup(d8);
 [ (1,2,3,4), (2,4) ]
```

راه دیگری برای تعریف گروه‌ها استفاده از مولدهای گروه و روابطی است که بین مولدها وجود دارد. مثلاً ρ و ε مولدهای گروه دووجهی D_{2n} هستند. هم‌چنین با استفاده از رابطه‌های $\rho^n = 1$، $\varepsilon^2 = 1$، $\rho\varepsilon = \varepsilon\rho^{-1}$ همه‌ی اعضای گروه D_{2n} توصیف می‌شوند. می‌خواهیم ببینیم تعریف چنین زیرگروه‌هایی در GAP به چه صورت است. ابتدا حالتی را در نظر بگیرید که گروه مورد نظر یک مجموعه‌ی مولد مثل X دارد، اما هیچ گونه رابطه‌ای روی مولدها وجود ندارد. چنین گروهی را گروه آزاد روی مجموعه‌ی X گوییم. در این حالت $|X|$ رتبه‌ی گروه آزاد نامیده می‌شود. تعریف گروه آزاد در GAP با دستور FreeGroup انجام می‌شود. دستور FreeGroup(n) گروه آزاد با رتبه‌ی n را به دست می‌دهد. در صورتی که مثلاً اگر متغیر F یک گروه آزاد باشد دستور F.t مولد tام آن را مشخص می‌کند. دستور FreeGroup("a","b",...) گروه آزاد روی a، b، ... را به دست می‌دهد. البته در این حالت نیز برای دسترسی به مولدها باید از دستور $F.t$ استفاده کرد.

گروه آزاد روی دو حرف را تعریف، و متغیر ها با r و s نامگذاری می‌کنیم

```
gap>U:=FreeGroup("r","s");
 <free group on the generators [ r, s ]>
gap>r:=U.1;  s:=U.2;
```

r
s
gap>SetName(U.1,"r"); SetName(U.2,"s");

اگر F یک گروه آزاد روی مجموعه‌ی متناهی X باشد و R مجموعه‌ای متناهی از روابط روی اعضای X، دستور F/R گروهی را مشخص می‌کند که مولدهای آن اعضای X هستند و در روابط R صدق می‌کنند. این گروه را یک گروه با نمایش متناهی گوییم (در GAP با علامت اختصاری .(fp مثلاً برای تعریف ۴-گروه کلاین می‌توان به صورت زیر عمل کرد

gap>D4:=U/[r^2,s^2,r^-1*s^-1*r*s];
<fp group on the generators [r, s]>
gap>Elements(D4);
[<identity ...> , r, s, r*s]
gap>IsAbelian(D4);
true
gap>IsCyclic(D4);
false

در زیر گروه‌های دووجهی D_6 و D_8 را با استفاده از مولدها و رابطه‌ها تعریف می‌کنیم و عناصر آن‌ها را می‌یابیم

gap>D6:=U/[r^3,s^2,(r*s)^2];
<fp group on the generators [r, s]>
gap>Elements(D6);
[<identity ...> , s, r^2*s, r, r^2, r*s]
gap>List(ConjugacyClasses(D6),x-> Elements(x));
[[<identity ...>], [s, r^-2*s*r^2, r^-1*s*r], [r, s^-1*r*s]]
gap>sameorder(D6);
[[1, [<identity ...>]], [2, [s, r^2*s, r*s]], [3, [r, r^2]]]
gap>D8:=F/[r^4,s^2,(r*s)^2];
<fp group on the generators [r, s]>
gap>Elements(D8);
[<identity ...> , s, r^3*s, r, r^2*s, r^2, r^3, r*s]
gap>List(ConjugacyClasses(D8),Representative);
[<identity ...> , s, r^3*s, r, r^2]

اکنون گروه‌های دوری مرتبه‌ی ۷ و ۱۲ را با استفاده از مولدها و رابطه‌ها تعریف می‌کنیم و عناصر آن‌ها را می‌یابیم

gap>S:=FreeGroup("a");;
gap>a:=S.1
gap>SetName(S.1,"a");
gap>C7:=S/[a^7];
<fp group on the generators [a]>
gap>Elements(C7);
[<identity ...> , a, a^2, a^3, a^4, a^5, a^6]
gap>IsCyclic(C7);
true
gap>C12:=S/[a^12];
<fp group on the generators [a]>

gap>Elements(C12);
[<identity ...> , a, a^2, a^3, a^4, a^5, a^6, a^7, a^8, a^9, a^10, a^11]

تمرین‌ها (با استفاده از GAP)

۱. فرض کنید G گروه باشد و $a, b \in G$. اگر $ab = ba^{-1}$ و $ba = ab^{-1}$، نشان دهید $a^2 = b^2 = 1$.
۲. فرض کنید G گروه باشد و $a, b \in G$. اگر $b^{-1}a^2b = a^3$ و $a^{-1}b^2a = b^3$، نشان دهید $a = b = 1$.
۳. فرض کنید G گروه باشد و $a, b \in G$. اگر $a^4 = 1$ و $a^2b = ba$، نشان دهید $a = 1$.
۴. اگر $a^6 = 1$ و $ab = ba^3$، در یک گروه، نشان دهید $a^2 = 1$ و $ab = ba$.
۵. اگر $a^6 = 1$ و $ab = ba^2$، در یک گروه، نشان دهید $a^3 = 1$ و $aba = b$.
۶. فرض کنید a, b دو عضو یک گروه متناهی باشند. اگر $a^{-1}ba = b^2$ و $O(a) = 3$، $O(b)$ را بیابید.

۱۰.۱۶ همریختی در GAP، آزمایشگاه دهم

در این آزمایشگاه نحوه‌ی تعریف همریختی بین گروه‌ها و هم‌چنین یافتن خودریختی‌های یک گروه را بررسی می‌کنیم.

مثال ۱.۱۰.۱۶. (الف) تابع $f : C_7 \longrightarrow C_7$ با ضابطه‌ی $f(x) = x^3$ را تعریف کنید. آیا این تابع دوسویی است. آیا یکریختی است؟ (ب) گروه خودریختی‌های C_7 را بیابید. عناصر آن را فهرست کنید.

حل (الف) با استفاده از دستور MappingByFunction تابع f را تعریف می‌کنیم. و سپس با دستورات مناسب به صورت زیر یک‌به‌یک ، پوشا، دوسویی، و همریختی بودن f را بررسی می‌کنیم

gap>C7:=CyclicGroup(7);; SetName(C7,"C7");
gap>f:=MappingByFunction(C7,C7,x-> x^3);;
gap>IsInjective(f); IsSurjective(f); IsBijective(f);
true
true
true
gap>IsGroupHomomorphism(f);
true

f یکریختی است، زیرا یک‌به‌یک ، پوشا، و همریختی است.
(ب) دستور AutomorphismGroup(G) گروه خودریختی‌های گروه G را محاسبه می‌کند

gap>aut7:=AutomorphismGroup(C7);
<group with 1 generators>
gap>e7:=Elements(aut7);
[IdentityMapping(C7), Pcgs([f1]) -> [f1^2], [f1] -> [f1^3],
Pcgs([f1]) -> [f1^4], Pcgs([f1]) -> [f1^5], Pcgs([f1]) -> [f1^6]]
gap>g:=e7[2]; IsBijective(g);
Pcgs([f1]) -> [f1^2]
true
gap>IsGroupHomomorphism(g);
true

مثال ۲.۱۰.۱۶. (الف) تابع $f : C_{۱۲} \longrightarrow C_{۱۲}$ با ضابطه‌ی $f(x) = x^{۳}$ را تعریف کنید. آیا این تابع دوسویی است. آیا یکریختی است؟ (ب) گروه خودریختی‌های $C_{۱۲}$ را بیابید. عناصر آن را فهرست کنید.

حل (الف)

```
gap>C12:=CyclicGroup(IsPermGroup,12);;
gap>SetName(C12,"C12");
gap>h:=MappingByFunction(C12,C12,x-> x^3);
 MappingByFunction( C12, C12, function( x ) ... end )
gap>IsGroupHomomorphism(h);
 true
gap>IsInjective(h); IsSurjective(h);
 false
 false
gap>Image(h);
 Group([ ( 1, 4, 7, 10)( 2, 5, 8, 11)( 3, 6, 9, 12) ])
gap>Elements(Image(h));
 [ (), ( 1, 4, 7, 10)( 2, 5, 8, 11)( 3, 6, 9, 12), ( 1, 7)( 2, 8)( 3, 9)( 4,10)( 5,11)( 6,12),
  ( 1,10, 7, 4)( 2,11, 8, 5)( 3,12, 9, 6) ]
```

پس h همریختی هست، یک‌به‌یک و پوشا نیست.

(ب)

```
gap>aut12:=AutomorphismGroup(C12);;
gap>e12:=Elements(aut12);
  [ IdentityMapping( C12 ),
 [(1,4,7,10)(2,5,8,11)(3,6,9,12), (1,5,9)(2,6,10)(3,7,11)(4,8,12)]->
 [(1,4,7,10)(2,5,8,11)(3,6,9,12), (1,9,5)(2,10,6)(3,11,7)(4,12,8)],
  [(1,5,9)(2,6,10)(3,7,11)(4,8,12), (1,4,7,10)(2,5,8,11)(3,6,9,12)]->
 [(1,5,9)(2,6,10)(3,7,11)(4,8,12), (1,10,7,4)(2,11,8,5)(3,12,9,6)],
 [(1,4,7,10)(2,5,8,11)(3,6,9,12), (1,5,9)(2,6,10)(3,7,11)(4,8,12)]->
 [(1,10,7,4)(2,11,8,5)(3,12,9,6), (1,9,5)(2,10,6)(3,11,7)(4,12,8)]]
gap>k:=e12[2];;  eg12:=GeneratorsOfGroup(C12);
 [ ( 1, 2, 3, 4, 5, 6, 7, 8, 9,10,11,12) ]
gap>eg:=eg12[1];;  Image(k,eg);  Image(k,eg^3);
 ( 1, 6,11, 4, 9, 2, 7,12, 5,10, 3, 8)
 ( 1, 4, 7,10)( 2, 5, 8,11)( 3, 6, 9,12)
```

مثال ۳.۱۰.۱۶. (الف) تابع $f : D_{۱۲} \longrightarrow D_{۱۲}$ با ضابطه‌ی $f(x) = x^{۲}$ را تعریف کنید. آیا این تابع دوسویی است. آیا یکریختی است؟ (ب) گروه خودریختی‌های $C_{۱۲}$ را بیابید. عناصر آن را فهرست کنید.

حل (الف)

```
gap>D12:=DihedralGroup(12); SetName(D12,"D12");
 <pc group of size 12 with 3 generators>
gap>f:=MappingByFunction(D12,D12,x-> x^2);
 MappingByFunction( D12, D12, function( x ) ... end )
```

```
gap>IsBijective(f); IsInjective(f); IsSurjective(f);
 false
 false
 false
gap>Image(f);   IsGroupHomomorphism(f);
 [ <identity> of ..., f3, f3^2 ]
 false
```

(ب)

```
gap>Aut12:=AutomorphismGroup(D12);;
gap>E12:=Elements(Aut12);
  [ Pcgs([ f1, f2, f3 ]) -> [ f1*f2*f3, f2*f3^2, f3^2 ],
  Pcgs([ f1, f2*f3, f3 ]) -> [ f1*f2*f3, f2*f3, f3 ],
  Pcgs([ f1, f2, f3 ]) -> [ f1*f3^2, f2, f3 ],
 Pcgs([ f1, f2, f3 ]) -> [ f1*f3^2, f2*f3^2, f3^2 ],
  Pcgs([ f1, f2, f3 ]) -> [ f1*f2*f3^2, f2, f3 ],
  Pcgs([ f1, f2, f3 ]) -> [ f1*f2*f3^2, f2*f3^2, f3^2 ],
 IdentityMapping( D12 ), Pcgs([ f1, f2*f3, f3 ]) -> [ f1, f2*f3, f3^2 ],
  Pcgs([ f1, f2, f3 ]) -> [ f1*f2, f2, f3 ],
 Pcgs([ f1, f2, f3 ]) -> [ f1*f2, f2*f3^2, f3^2 ],
  Pcgs([ f1, f2, f3 ]) -> [ f1*f3, f2*f3^2, f3^2 ],
  Pcgs([ f1, f2*f3, f3 ]) -> [ f1*f3, f2*f3, f3 ] ]
gap>g:=E12[2];; Image(g,D12.1);
 f1*f2*f3
gap> Image(g,D12.2); Image(g,D12.3);
 f2
 f3
```

مثال ۴.۱۰.۱۶. نشان دهید $\mathrm{Aut}\, S_3 \cong S_3$.

حل ابتدا گروه متقارن S_3 را تعریف می‌کنیم و سپس گروه خودریختی‌های آن‌را می‌یابیم

```
gap>s3:=SymmetricGroup(3);; SetName(s3,"s3");
gap>as3:=AutomorphismGroup(s3);;
gap>e3:=Elements(as3);
  [ IdentityMapping( s3 ), ^(2,3), ^(1,3), ^(1,3,2), ^(1,2,3), ^(1,2) ]
```

با استفاده از دستور GroupHomomorphismByImages یک همریختی (در صورت وجود) از S_3 به $\mathrm{Aut}\, S_3$ می‌سازیم. اگر L یک مجموعه‌ی مولد برای گروه G و S یک مجموعه‌ی مولد برای گروه H باشد دستور $\mathrm{GroupHomomorphismByImages}(G,H,L,S)$ یک همریختی (در صورت وجود) از گروه G به گروه H که عضو iام L را به عضو iام S نظیر می‌کند را به دست می‌دهد. در صورتی که چنین همریختی وجود نداشته باشد خروجی این دستور fail خواهد بود. اکنون مولدهای S_3 و $\mathrm{Aut}\, S_3$ را به دست می‌آوریم. سپس با استفاده از دستور GroupHomomorphismByImages همریختی مورد نظر را تعریف می‌کنیم

```
gap>genas3:=GeneratorsOfGroup(as3);
 [ ^(1,2,3), ^(1,2) ]
gap> gens3:=GeneratorsOfGroup(s3);
```

```
[ (1,2,3), (1,2) ]
gap>f:=GroupHomomorphismByImages(s3,as3,gens3,genas3);
[ (1,2,3), (1,2) ] -> [ ConjugatorAutomorphism( s3, (1,2,3) ),
  ConjugatorAutomorphism( s3, (1,2) ) ]
gap>IsBijective(f);
 true
gap>g:=GroupHomomorphismByImages(s3,as3,> [(1,2),(1,2,3)],genas3);
 fail
```

مثال ۵.۱۰.۱۶. نشان دهید $S_3 \cong \mathrm{GL}_2(\mathbb{Z}_2)$.

حل در زیر با به دست آوردن یک مجموعه‌ی مولد برای $\mathrm{GL}_2(\mathbb{Z}_2)$ یک همریختی یک‌به‌یک و پوشا به طور مناسب از S_3 به $\mathrm{GL}_2(\mathbb{Z}_2)$ تعریف می‌کنیم. بررسی جزئیات کار را به خواننده واگذار می‌کنیم

```
gap>G:=GL(2,2);    Size(G);
 GL(2,2)
 6
gap>Ggens:=GeneratorsOfGroup(G);
 <an immutable 2x2 matrix over GF2> , <an immutable 2x2 matrix over GF2> ]
gap>Display(Ggens[1]);
  1 1
  . 1
gap>Display(Ggens[2]);
  . 1
  1 .
gap>Order(Ggens[1]);    Order(Ggens[2]);
 2
 2
gap>z:=Z(2);;   gens:=[ [[z,z],[0*z,z]], [[0*z,z],[z,0*z]] ];
  [ [ <a GF2 vector of length 2> , <a GF2 vector of length 2> ],
  [ <a GF2 vector of length 2> , <a GF2 vector of length 2> ] ]
gap>G=Group(gens);
 true
gap>h:=GroupHomomorphismByImages(s3,G, [(1,2),(1,3)],gens);
[(1,2),(1,3)]-> [ [[Z(2)^0,Z(2)^0], [0*Z(2),Z(2)^0]],
        [[0*Z(2),Z(2)^0],[Z(2)^0,0*Z(2)]] ]
gap>IsBijective(h);
 true
```

تمرین‌ها (با استفاده از GAP)

۱. نشان دهید $S_3 \cong \langle x, y \mid x^2 = y^3 = (xy)^2 \rangle$.

۲. نشان دهید $S_4 \cong \langle x, y \mid x^4 = y^4 = (xy)^3 \rangle$.

۳. نشان دهید $A_4 \cong \langle x, y \mid x^2 = y^3 = (xy)^3 \rangle$.

۴. اگر V_4، ۴-گروه کلاین باشد، نشان دهید $\mathrm{Aut}\, V_4 \cong S_3$.

۵. نشان دهید $\mathrm{Aut}\, D_8 \cong D_8$.

۶. نشان دهید $\mathrm{Aut}\, A_5 \cong S_5$.

۷. نشان دهید $\mathrm{Aut}\, \mathbb{Z} \cong \mathbb{Z}^\times$ و به ازای تعدادی n (مثلاً $n = 3, 4, 5, 6$) تحقیق کنید $\mathrm{Aut}\, \mathbb{Z}_n \cong \mathbb{Z}_n^\times$.

۸. فرض کنید G گروهی با مولدهای a، b باشد طوری که $ba = a^3b = a^{-1}b$، $a^2 = b^2$، و به علاوه $O(a) = O(b) = 4$. نشان دهید $G \cong Q_8$.

۹. ثابت کنید $\mathrm{Aut}\,(\mathbb{Z}_2 \times \mathbb{Z}_4) \cong D_8$.

۱۱.۱۶ زیر گروه‌ها در GAP، آزمایشگاه یازدهم

مثال ۱.۱۱.۱۶. (الف) گروه‌های S_5 و A_5 را تعریف کنید. آیا $A_5 \leq S_5$؟
(ب) مرکز S_5 را بیابید.
(ج) نرمال‌ساز A_5 در S_5 و مرکزساز جایگشت $(1\ 2)$ را در S_5 بیابید.
(د) زیرگروه مشتق S_5 و A_5 را محاسبه کنید. آیا A_5 و S_5 حل‌پذیرند؟

حل (الف) دستور $\mathrm{IsSubgroup}(G, H)$ معین می‌کند که آیا H زیرگروه G است یا نه؟

```
gap>S5:=SymmetricGroup(5);; SetName(S5,"S5");
gap>A5:=AlternatingGroup(5);; SetName(A5,"A5");
gap>IsSubgroup(S5,A5);
 true
```

(ب) با استفاده از دستور $\mathrm{Center}(G)$ مرکز گروه G به دست می‌آید

```
gap>Center(S5); Elements(Center(S5));
 Group(())
 [ () ]
```

(ج) دستور $\mathrm{Normalizer}(G, H)$ نرمال‌ساز زیرگروه H در گروه G را محاسبه می‌کند. به همین نحو دستور $\mathrm{Centralizer}(G, L)$ مرکزساز زیرمجموعه‌ی L (یا عضو L) در G را محاسبه می‌کند

```
gap>nor:=Normalizer(S5,A5); Size(nor); nor=S5;
 Group([ (1,5,4,3,2), (2,4,3), (2,3) ])
 120
 true
gap>cen:=Centralizer(S5,(1,2));
 Group([ (4,5), (3,4), (1,2) ])
gap>Size(cen);
 12
```

(د) با استفاده از دستور $\mathrm{DerivedSubgroup}(G)$ زیرگروه مشتق G به دست می‌آید. دستور $\mathrm{IsSolvable}(G)$ تعیین می‌کند که آیا Gحل‌پذیر است یا نه؟

```
gap>ds5:=DerivedSubgroup(S5); A5=ds5;
 Group([ (1,3,2), (2,4,3), (2,5,3) ])
 true
gap>da5:=DerivedSubgroup(A5);
```

Group([(1,4,3), (2,3,5)])
gap>A5=da5; IsSolvable(A5);
true
false

مثال ۲.۱۱.۱۶. (الف) گروه‌های S_4 و A_4 را تعریف کنید. آیا $A_4 \leq S_4$؟
(ب) زیرگروه مشتق A_4 را محاسبه کنید. آیا A_4حل‌پذیر است؟
(ج) نرمال‌ساز ۴-گروه کلاین را در A_4 محاسبه کنید.
(د) مشتق‌های مرتبه‌ی بالاتر A_4 و S_4 را بیابید. عناصر این مشتقها و تعداد اعضای آن ها را مشخص کنید.

حل (الف)

gap>S4:=SymmetricGroup(4);; SetName(S4,"S4");
gap>A4:=AlternatingGroup(4);; SetName(A4,"A4");
gap>IsSubgroup(A5,A4);
true

(ب)

gap>V:=DerivedSubgroup(A4);
Group([(1,4)(2,3), (1,2)(3,4)])
gap>Size(last);
4
gap>IsSolvable(A4);
true

(ج) ۴-گروه کلاین همان زیرگروه مشتق A_4 است. پس

gap>norm:=Normalizer(A4,V); A4=norm;
Group([(1,4)(2,3), (1,2)(3,4), (2,3,4)])
true

(د) دستور DerivedSeries(G) سری زیرگروه‌های مشتقهای گروه G را به دست می‌دهد. ابتدا سری مشتق A_4 و عناصر و مرتبه‌ی این زیرگروه‌ها را می‌یابیم

gap>d:=DerivedSeries(A4);
[Group([(2,4,3), (1,3)(2,4), (1,2)(3,4)]),
Group([(1,3)(2,4), (1,2)(3,4)]), Group(())]
gap>List(d,x-> Elements(x));
[[(), (2,3,4), (2,4,3), (1,2)(3,4), (1,2,3), (1,2,4), (1,3,2), (1,3,4),
(1,3)(2,4), (1,4,2), (1,4,3), (1,4)(2,3)],
[(), (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)], [()]]
gap>List(d,x-> Size(x));
[12, 4, 1]

اکنون سری مشتق S_4 و عناصر و مرتبه‌ی این زیرگروه‌ها را می‌یابیم

gap>dd:=DerivedSeries(S4);
[Group([(3,4), (2,4,3), (1,4)(2,3), (1,2)(3,4)]),
Group([(2,4,3), (1,4)(2,3), (1,2)(3,4)]),
Group([(1,4)(2,3), (1,2)(3,4)]), Group(())]

```
gap>List(dd,x-> Elements(x));
[ (), (3,4), (2,3), (2,3,4), (2,4,3), (2,4), (1,2), (1,2)(3,4), (1,2,3),
(1,2,3,4), (1,2,4,3), (1,2,4), (1,3,2), (1,3,4,2), (1,3), (1,3,4),(1,3)(2,4),
(1,3,2,4), (1,4,3,2), (1,4,2), (1,4,3), (1,4), (1,4,2,3), (1,4)(2,3) ],
[ (), (2,3,4), (2,4,3), (1,2)(3,4), (1,2,3), (1,2,4), (1,3,2),
(1,3,4), (1,3)(2,4), (1,4,2), (1,4,3), (1,4)(2,3) ],
 [ (), (1,2)(3,4), (1,3)(2,4), (1,4)(2,3) ], [ () ] ]
gap>List(dd,x-> Size(x));
[ 24, 12, 4, 1 ]
```

مثال ۳.۱۱.۱۶. گروه D_{18} را تعریف کرده و سری مشتق آن را بیابید.

حل مشابه مثال‌های قبل عمل می‌کنیم. بررسی جزئیات را به خواننده واگذار می‌کنیم

```
gap>D18:=DihedralGroup(18);; IsSolvable(D18);
 true
gap>t:=DerivedSeries(D18);
[ <pc group of size 18 with 3 generators> , Group([ f2, f3 ]), Group([ ]) ]
gap>List(t,x-> Size(x));
[ 18, 9, 1 ]
gap>List(t,x-> Elements(x));
[ [ <identity> of ..., f1, f2, f3, f1*f2, f1*f3, f2^2, f2*f3,
  f3^2, f1*f2^2, f1*f2*f3, f1*f3^2, f2^2*f3, f2*f3^2,
  f1*f2^2*f3, f1*f2*f3^2, f2^2*f3^2, f1*f2^2*f3^2 ],
[ <identity> of ..., f2, f3, f2^2, f2*f3, f3^2, f2^2*f3,
```

تمرین‌ها (با استفاده از GAP)

۱. برنامه‌ای بنویسید که تعداد مرکزسازهای یک گروه متناهی را بیابید.

۲. $\mathrm{GL}_۲(F_۲)$ و $\mathrm{GL}_۲(F_۳)$ را تعریف کرده و نشان دهید حل‌پذیر هستند.

۳. نشان دهید همه‌ی زیرگروه‌های $Q_۸$ دوری هستند و در $Q_۸$ نرمال‌اند.

۴. مرکزساز $(۴\ ۳\ ۱)(۲\ ۱)$ را در $S_۸$ بیابید.

۵. سری مشتق برای گروه $\mathrm{GL}_۲(F_۸)$ را بیابید.

۶. ماتریس‌های $a = \begin{bmatrix} ۱ & ۰ \\ ۰ & -۱ \end{bmatrix}$ و $b = \begin{bmatrix} ۱ & ۱ \\ ۰ & -۱ \end{bmatrix}$ در $\mathrm{GL}_۲(\mathbb{R})$ را در نظر بگیرید. ثابت کنید $\langle a, b\rangle \cong D_\infty$.

۷. مجموعه‌ی ماتریس‌های بالا مثلثی وارون‌پذیر ۳×۳ با درایه‌های در $F_۸$ را تعریف کنید و نشان دهید زیرگروه $\mathrm{GL}_۳(F_۸)$ است.

۸. همه‌ی عناصر با مرتبه‌ی ۲ را در $\mathrm{GL}_۲(F_۴)$ را بیابید.

۹. اگر H و K دو زیرگروه یک گروه G باشند، برنامه‌ای بنویسید که HK را تشکیل دهد و معین کند که آیا گروه است.

۱۰. برنامه‌ای بنویسید که یک زیرگروه ماکسیمال شامل زیرمجموعه‌ی A از گروه G متناهی را بیابید.

۱۲.۱۶ هم‌مجموعه‌ها و گروه‌های خارج قسمتی در GAP، آزمایشگاه دوازدهم

در این آزمایشگاه نحوه‌ی تشکیل هم مجموعه‌های یک زیر گروه، گروه‌های خارج‌قسمتی و اعمال روی آن‌ها را بررسی می‌کنیم.

مثال ۱.۱۲.۱۶. معادله‌ی رده‌ای را برای گروه دووجهی $D_{۲۰}$ بررسی کنید.

حل ابتدا گروه دووجهی مرتبه ۲۰ را تعریف می‌کنیم. مجموع تعداد عناصر رده‌های مزدوجی $D_{۲۰}$ باید برابر تعداد عناصر $D_{۲۰}$ باشد

```
gap>D20:=DihedralGroup(20);;
gap>Size(D20)=Sum(List(ConjugacyClasses(D20),Size));
 true
```

در دستور بعد تعداد اعضای $D_{۲۰}$ را با مجموع تعداد اعضای مرکز $D_{۲۰}$ و تعداد اعضای رده‌های مزدوجی نابدیهی (با بیش از یک عضو) مقایسه می‌کنیم

```
gap>L:=List(Filtered(ConjugacyClasses(D20),x-> Size(x)> 1),Size);
 [ 5, 2, 2, 5, 2, 2 ]
gap>Size(D20)=Size(Center(D20))+Sum(L);
 true
```

مثال ۲.۱۲.۱۶. فرض کنید H گروه تولید شده توسط جایگشت‌های زیر باشد

$$(۱\ ۲)(۳\ ۴)(۵\ ۶)(۷\ ۸), \quad (۱\ ۳)(۲\ ۴)(۵\ ۷)(۶\ ۸), \quad (۱\ ۵)(۲\ ۶)(۳\ ۷)(۴\ ۸).$$

(الف) نشان دهید H زیرگروه $A_۸$ است. مرتبه‌ی H و شاخص H در $A_۸$ را بیابید.
(ب) تعداد مزدوج‌های H را در $A_۸$ بیابید.
(ج) گروه خارج‌قسمتی $N_{A_۸}(H)/H$ را بیابید. تعداد اعضای آن‌را مشخص کنید. آیا این گروه ساده است؟
(د) همریختی طبیعی از $N_{A_۸}(H)$ به $N_{A_۸}(H)/H$ را تعریف کنید. پیش تصویر یک عضو که به صورت تصادفی اختیار شده است را بیابید.

حل (الف) ابتدا گروه H و گروه متناوب $A_۸$ را تعریف می‌کنیم. سپس بررسی می‌کنیم که آیا H زیرگروه $A_۸$ هست؟ درنهایت با استفاده از دستور $\mathrm{Index}(G,H)$، که شاخص زیرگروه H در گروه G را می‌دهد، شاخص H در $A_۸$ را می‌یابیم

```
gap>a8:=AlternatingGroup(8);;
gap>H:=Group((1,2)(3,4)(5,6)(7,8),(1,3)(2,4)(5,7)(6,8), (1,5)(2,6)(3,7)(4,8));;
gap>Size(H); SetName(H,"H");
 8
gap>IsSubgroup(a8,H);
 true
gap>Index(a8,H);
 2520
```

(ب) با استفاده از دستور $\mathrm{Normalizer}(G,H)$ نرمال‌ساز H در G به دست می‌آید. هم‌چنین می‌دانیم تعداد مزدوج‌های زیرگروه H در گروه G برابر شاخص $N_G(H)$ در G است. پس

```
gap>N:=Normalizer(a8,H);
  Group([ (1,5)(2,6)(3,7)(4,8), (1,3)(2,4)(5,7)(6,8), (1,2)(3,4)(5,6)(7,8),
  (5,6)(7,8), (5,7)(6,8), (3,4)(7,8), (3,5)(4,6), (2,3)(6,7) ])
gap>Size(N);
 1344
```

```
gap>Index(a8,N);
 15
```

(ج) چون H در $N_G(H)$ نرمال است، می‌توان $N_G(H)/H$ را تشکیل داد. با استفاده از دستور $\mathrm{IsNormal}(G,J)$ نرمال بودن H در گروه G بررسی می‌شود. اگر H در G نرمال باشد با استفاده از دستور $\mathrm{FactorGroup}(G,H)$ یا به طور ساده با G/H می‌توان گروه خارج‌قسمتی G/H را ساخت. البته با این کار گروه جایگشتی یکریخت با G/H حاصل می‌شود

```
gap>IsNormal(N,H);
 true
gap>IsNormal(a8,N);
 false
gap>fac:=N/H;
 Group([ (), (), (), (3,4)(5,6), (3,5)(4,6), (1,2)(5,6), 1,3)(2,4), (1,7)(4,5) ])
```

داریم

```
gap>Size(fac);
 168
gap>IsSimple(fac);
 true
```

پس $N_G(H)/H$ یک گروه ساده از مرتبه‌ی ۱۶۸ است.

(د) با استفاده از دستور $\mathrm{NaturalHomomorphismByNormalSubgroup}(G,H)$ می‌توان همریختی طبیعی $G \longrightarrow G/H$ را به دست آورد. دستور $\mathrm{Kernel}(f)$ هسته‌ی همریختی f را محاسبه می‌کند. هم‌چنین با استفاده از دستور $\mathrm{Random}(L)$ یک عضو به صورت تصادفی از L به دست می‌آید

```
gap>hom:=NaturalHomomorphismByNormalSubgroup(N,H);
 <action homomorphism>
gap>Kernel(hom)=H;
 true
gap>x:=Random(N);
 (2,4,8)(3,5,7)
gap> x^hom;
 (1,3,5)(2,6,7)
gap>im:=Image(hom,x);
 (1,3,5)(2,6,7)
gap>coset:=PreImages(hom,im);
 RightCoset(H,(2,4,8)(3,5,7))
```

مثال ۳.۱۲.۱۶. فرض کنید K برابر گروه تولید توسط (۲ ۱) در S_3 باشد. هم مجموعه‌های K در S_3 را بیابید. یک پیمایش راست K در S_3 را مشخص کنید. آیا K در S_3 نرمال است؟

حل با استفاده از دستور $\mathrm{RightCosets}(G,H)$ مجموعه‌ی هم مجموعه‌های راست H در G به دست می‌آید

```
gap>s3:=SymmetricGroup(3);;
gap>K:=Group((1,2));; SetName(K,"K");
gap>R:=RightCosets(s3,K);
 [ RightCoset(K,()), RightCoset(K,(1,3,2)), RightCoset(K,(1,2,3)) ]
gap>List(R,Representative);
```

[(), (1,3,2), (1,2,3)]
gap>IsNormal(s3,K);
false

تمرین‌ها (با استفاده از GAP)

۱. نشان دهید $D_{۳۶}/Z(D_{۳۶}) \cong D_{۱۸}$.

۲. اگر G گروه متناهی باشد احتمال تعویض شدن دو عضو در G عبارت است از

$$\mathrm{pr}G = \frac{|\{(x,y) \mid xy = yx\}|}{|G|^۲}.$$

برنامه‌ای بنویسید که $\mathrm{pr}G$ را بیابید. این برنامه را برای گروه‌های $S_۳$، $D_۸$، $Q_۸$، و $S_۵$ امتحان کنید.

۳. می‌توان نشان داد $\mathrm{pr}G = \frac{k}{|G|}$، که در آن k تعداد رده‌های مزدوجی G است. برنامه‌ای بنویسید که $\mathrm{pr}G$ را به این روش محاسبه کند. این برنامه را در مورد گروه‌های $S_۳$، $D_۸$، $Q_۸$، و $S_۵$ امتحان کنید.

۴. فرض کنید H، مرکزساز $(۶\ ۳\ ۲)(۲\ ۱)$ در $S_۷$ باشد.
(الف) تعداد مزدوج‌های H در $S_۷$ را بیابید.
(ب) نرمال‌ساز H در $S_۷$ را محاسبه کنید.
(ج) گروه خارج‌قسمتی $K = N_{S_۷}(H)/H$ را تشکیل دهید.
(د) آیا K گروهی ساده است؟
(هـ) یک پیمایش راست H در $S_۷$ و یک پیمایش راست H را در $N_{S_۷}(H)$ بیابید.

۱۳.۱۶ حاصل‌ضرب مستقیم و نیم‌مستقیم در GAP، آزمایشگاه سیزدهم

در این آزمایشگاه نحوه‌ی تعریف و پردازش حاصل‌ضرب مستقیم و نیم‌مستقیم گروه‌ها را بررسی می‌کنیم.

مثال ۱.۱۳.۱۶. فرض کنید $G = S_۳ \times \mathbb{Z}_۴ \times \mathbb{Z}_۴ \times D_۶$.
(الف) مولدهای G را بیابید.
(ب) همریختی‌های تصویر روی مولفه‌های اول ، دوم ، و چهارم را بیابید. می‌دانیم که اگر $G = G_۱ \times \cdots \times G_n$، آنگاه تصویر روی مولفه‌ی iام، $\pi_i : G \longrightarrow G_i$ با $\pi_i(g_۱, \ldots, g_n) = g_i$،یک همریختی پوشا با هسته‌ی $G_۱ \times \cdots \times \widehat{G_i} \times \cdots \times G_n$ است. صحت مطالب فوق را برای این همریختی‌ها تحقیق کنید.
(ج) جادهی مولفه‌های اول و چهارم را بیابید.

حل (الف) با استفاده از دستور $\mathrm{DirectProduct}(G_۱, G_۲, \ldots)$ حاصل‌ضرب مستقیم $G_۱ \times G_۲ \times \cdots$ به دست می‌آید

gap>s3:=SymmetricGroup(3);; z4:=CyclicGroup(4);;
gap>D6:=DihedralGroup(6);;
gap>G:=DirectProduct(s3,z4,z4,D6);
<group of size 576 with 8 generators>
gap>GeneratorsOfGroup(G);
[Tuple([(1,2,3),<identity> of ..., <identity> of ..., <identity> of ...]),
Tuple([(1,2),<identity> of ..., <identity> of ..., <identity> of ...]),
Tuple([(), f1, <identity> of ..., <identity> of ...]),
Tuple([(), f2, <identity> of ..., <identity> of ...]),

```
 Tuple( [ (), <identity> of ..., f1, <identity> of ... ] ),
 Tuple( [ (), <identity> of ..., f2, <identity> of ... ] ),
 Tuple( [ (), <identity> of ..., <identity> of ..., f1 ] ),
 Tuple( [ (), <identity> of ..., <identity> of ..., f2 ] ) ]
```

(ب) اگر G حاصل‌ضرب مستقیم تعدادی گروه باشد، با استفاده از دستور $\mathrm{Projection}(G,i)$ همریختی تصویر روی مولفه‌ی iام حاصل‌ضرب می‌شود

```
gap>p1:=Projection(G,1);;    p2:=Projection(G,2);;
gap>p4:=Projection(G,4);;
gap>Image(p1); Image(p2); Image(p4);
 Sym( [ 1 .. 3 ] )
 <pc group of size 4 with 2 generators>
 <pc group of size 6 with 2 generators>
gap>s3=Image(p1); z4=Image(p2); D6=Image(p4);
 true
 true
 true
gap>Image(p2,Tuple([(1,2,3),z4.1,z4.1,D6.1]));
 f1
gap>Image(p1,Tuple([(1,2,3),z4.1,z4.2,D6.1]));
 (1,2,3)
gap>Kernel(p1)=DirectProduct(Group(()),z4,z4,D6);
 true
gap>Kernel(p2)=DirectProduct(s3,Group(z4.1^0),z4,D6);
 true
gap>Kernel(p4)=DirectProduct(s3,z4,z4,Group(D6.1^0));
 true
gap>IsAbelian(G); IsAbelian(Image(p2));
 false
 true
```

(ج) اگر G حاصل‌ضرب مستقیم تعدادی گروه باشد، با استفاده از دستور $\mathrm{Embeding}(G,i)$ همریختی جادهی مولفه‌ی iام حاصل‌ضرب می‌شود

```
gap>e1:=Embing(G,1);; e4:=Embing(G,4);;
gap>Image(e1); Size(Image(e1));
 <group with 2 generators>
 6
gap>Range(e1);
 <group of size 576 with 8 generators>
gap>Image(e4); Range(e4);
 <group with 2 generators>
 <group of size 576 with 8 generators>
gap>Order(Tuple([(1,2),z4.1,z4.1,D6.1]));
```

4

مثال ۲.۱۳.۱۶. فرض کنید H و N گروه‌های دوری مرتبه‌ی **۲۵** باشند. نشان دهید یک همریختی $g : H \longrightarrow \mathrm{Aut}\, N$ وجود دارد و حاصل‌ضرب نیم‌مستقیم H توسط N را نسبت به g تشکیل دهید. مرتبه‌ی مرکز و تعداد مرکزسازهای این حاصل‌ضرب نیم‌مستقیم را بیابید.

حل گروه‌های H و N را تعریف کرده و گروه خودریختی‌های N را متغیر an عناصر آن را در متغیر anel قرار می‌دهیم. در نهایت مولدهای H را در متغیر hgen قرار می‌دهیم

```
gap>H:=CyclicGroup(25);; N:=CyclicGroup(25);;
gap>an:=AutomorphismGroup(N);;
gap>anel:=Elements(an);;
gap>hgen:=GeneratorsOfGroup(H);
[ f1, f2 ]
```

اکنون سعی می‌کنیم که همریختی g را از H به $\mathrm{Aut}\, N$ تعریف کنیم طوری که اولین و دومین مولد H را به ترتیب به اولین و دومین عضو از گروه خودریختی‌های N تصویر کند. چون خروجی این دستور fail نیست، همریختی مورد نظر وجود دارد. سپس با استفاده از دستور $\mathrm{SemidirectProduct}(H, g, N)$ حاصل‌ضرب نیم‌مستقیم H توسط N را نسبت به همریختی g می‌یابیم

```
gap>g:=GroupHomomorphismByImages(H,an,hgen,[anel[1],anel[3]]);
[ f1, f2 ] -> [ Pcgs([ f1, f2 ]) -> [ f1*f2^4, f2 ],
  IdentityMapping( Group( [ f1, f2 ] ) ) ]
gap>G:=SemidirectProduct(H,g,N);
<pc group of size 625 with 4 generators>
gap>Size(Center(G));
25
```

اکنون برنامه‌ای به‌نام $\mathrm{numbcent}(G)$ می‌نویسیم که تعداد مرکزسازهای گروه متناهی G را محاسبه کند

```
gap>numbcent:=function(G)
>               local eG;
>                eG:=Elements(G);
>         return Size( Set( eG,x->Centralizer( G,x ) ) );
>       end;;
```

تعداد مرکزسازهای G، حاصل‌ضرب نیم‌مستقیم H توسط N را نسبت به g، عبارت است از

```
gap>numbcent(G);
7
```

مثال ۳.۱۳.۱۶. نشان دهید یک همریختی $g : S_3 \longrightarrow \mathrm{Aut}\, D_8$ وجود دارد و حاصل‌ضرب نیم‌مستقیم S_3 توسط D_8 را نسبت به g تشکیل دهید. مرتبه‌ی مرکز آن‌را بیابید.

حل گروه‌های S_3 و D_8 را تعریف می‌کنیم. گروه خودریختی‌های D_8 را می‌یابیم و عناصر آن را در متغیر $e8$ قرار می‌دهیم. عناصر S_3 را در متغیر $e3$ قرار می‌دهیم. مرتبه‌ی عناصر $\mathrm{Aut}\, D_8$ و S_3 را فهرست می‌کنیم

```
gap>s3:=SymmetricGroup(IsPcGroup,3);;
gap>D8:=DihedralGroup(8);;
gap>aut8:=AutomorphismGroup(D8);
<group of size 8 with 3 generators>
gap>e8:=Elements(aut8);;
gap>e3:=Elements(s3);;
gap>List(e8,Order); List(e3,Order);
```

```
[ 2, 4, 2, 2, 4, 2, 2, 1 ]
[ 1, 2, 3, 2, 3, 2 ]
```

اکنون در جهت تعریف همریختی g۱ از S_3 به $\mathrm{Aut}\, D_8$ تلاش می‌کنیم. چون مرتبه‌ی تصویر یک عضو تحت همریختی، مرتبه‌ی آن عضو را عاد می‌کند، سعی می‌کنیم با رعایت این نکته همریختی را تعریف کنیم. اولین تلاش ما موفق نیست. اما دومین تلاش منجر به تعریف همریختی مورد نظر می‌شود. که با استفاده از آن حاصل‌ضرب نیم‌مستقیم را تشکیل می‌دهیم

```
gap>g1:=GroupHomomorphismByImages(s3,aut8,
>    [e3[2],e3[4]],[e8[1],e8[3]]);
 fail
gap>g1:=GroupHomomorphismByImages(s3,aut8,
>     [e3[2],e3[4]],[e8[1],e8[1]]);
[ f1, f1*f2 ] -> [ Pcgs([ f1, f2, f3 ]) -> [ f1*f2*f3, f2*f3, f3 ],
  Pcgs([ f1, f2, f3 ]) -> [ f1*f2*f3, f2*f3, f3 ] ]
gap>W1:=SemidirectProduct(s3,g1,D8);
 <pc group of size 48 with 5 generators>
gap>Center(W1);    Size(Center(W1));
 Group([ f5 ])
 2
```

در زیر نیز سعی برای تعریف همریختی g۲ از S_3 به $\mathrm{Aut}\, D_8$ نشان داده شده است

```
gap>g2:=GroupHomomorphismByImages(s3,aut8,
>    [e3[2],e3[4]],[e8[1],e8[7]]);
 fail
gap>g2:=GroupHomomorphismByImages(s3,aut8,
>     [e3[2],e3[4]],[e8[7],e8[7]]);
[ f1, f1*f2 ] -> [ Pcgs([ f1, f2, f3 ]) -> [ f1*f3, f2*f3, f3 ],
  Pcgs([ f1, f2, f3 ]) -> [ f1*f3, f2*f3, f3 ] ]
gap>W2:=SemidirectProduct(s3,g2,D8);  Size(Center(W2));
 <pc group of size 48 with 5 generators>
 2
gap>g3:=GroupHomomorphismByImages(s3,aut8,
>     [e3[2],e3[4]],[e8[2],e8[4]]);
 fail
```

تمرین‌ها (با استفاده از GAP)

۱. $D_8 \times S_3$ را تشکیل دهید و
(الف) مرتبه‌ی عناصر آن را بیابید.
(ب) رده مزدوجی عناصر آن را بیابید.

۲. $Q_8 \times S_3$ را تشکیل دهید و
(الف) مرتبه‌ی عناصر آن را بیابید.
(ب) رده مزدوجی عناصر آن را بیابید.

۳. $\mathrm{Hol}C_3$ را بیابید.

۴. $\mathrm{Hol}S_۳$ را بیابید.

۵. نشان دهید $\mathrm{Hol}(C_۲ \times C_۲) \cong S_۳$ را بیابید.

۶. نشان دهید یک همریختی $g : \mathbb{Z}_۴ \longrightarrow \mathrm{Aut}\,\mathbb{Z}_۳$ وجود دارد و حاصل‌ضرب نیم‌مستقیم $\mathbb{Z}_۳$ توسط $\mathbb{Z}_۴$ نسبت به g را تشکیل دهید. رده مزدوجی عناصر آن را بیابید.

۱۴.۱۶ عمل گروه در GAP، آزمایشگاه چهاردهم

در این آزمایشگاه نحوه‌ی تعریف و پردازش عمل گروه بر مجموعه را بررسی می‌کنیم. همان‌گونه که قبلاً ذکر شد عمل ترکیب توابع در GAP از چپ به راست انجام می‌شود. بنابراین اگر f و g دو تابع باشند تصویر x تحت تابع مرکب $f \circ g$ عبارت است از $g(f((x))$. یکی از مواردی که در این تعریف باید دقت شود هنگام عمل یک گروه بر یک مجموعه است. در این جا اگر گروه G روی مجموعه‌ی X عمل کند، برای نشان دادن عمل $g \in G$ روی $x \in X$ می‌نویسیم $x \cdot g$ و می‌گوییم G از راست روی X عمل می‌کند. به ازای هر $g \in G$، تابع $\varphi_g : X \longrightarrow X$ با ضابطه‌ی $(x)\varphi_g = x \cdot g$ یک جایگشت روی X است. از طرفی به ازای هر $g_۱, g_۲ \in G$ و به ازای هر $x \in X$ داریم

$$(x)\varphi_{g_۱g_۲} = x \cdot (g_۱g_۲) = (x \cdot g_۱) \cdot g_۲ = ((x)\varphi_{g_۱})\varphi_{g_۲}.$$

پس تابع $\varphi : G \longrightarrow S_X$ یک همریختی است. در واقع شرط لازم و کافی برای این که G از راست روی X عمل کند این است که همریختی $\varphi : G \longrightarrow S_X$ وجود داشته باشد.
بنابراین در این جا گروه G با ضرب از راست ، با ضرب وارون از چپ، و به صورت مزدوجی $x \cdot g = g^{-۱}xg$، روی خودش عمل می‌کند.

مثال ۱.۱۴.۱۶. عمل طبیعی $S_۳$ را روی مجموعه‌ی $\{۱, ۲, ۳\}$ تعریف کنید. مدار ۱ و ۲ و ثابت‌سازهای آن‌ها را بیابید.

حل در GAP عمل طبیعی گروه‌های جایگشتی روی مجموعه‌ی $\{۱, ۲, \ldots, n\}$ به طور پیش‌فرض در نظر گرفته می‌شود. این عمل طبیعی در GAP با OnPoints تعریف می‌شود. با استفاده از دستور $\mathrm{Orbit}(G, x, action)$ مدار x تحت عمل داده شده‌ی $action$ به دست می‌آید. همانطور که گفته شد در صورتی که نام عمل $action$ ذکر نشود، GAP آن‌را OnPoints در نظر خواهد گرفت. با استفاده از دستور $\mathrm{Stabilizer}(G, x, action)$ ثابت‌ساز x تحت عمل داده شده‌ی $action$ به دست می‌آید

```
gap>s3:=SymmetricGroup(3);;
gap>Orbit(s3,1,OnPoints);
[ 1, 2, 3 ]
gap>Orbit(s3,2,OnPoints);
[ 2, 3, 1 ]
gap>Stabilizer(s3,1);
 Group([ (2,3) ])
gap>Stabilizer(s3,2,OnPoints);
 Group([ (1,3) ])
```

مثال ۲.۱۴.۱۶. عمل $S_۳$ روی خودش را با ضرب از راست در نظر بگیرید. مدار $(۱, ۲)$ و $(۱, ۳, ۲)$ و ثابت‌سازهای آن‌ها را بیابید. همریختی متناظر این عمل را تعریف کنید؛ تصویر $(۱, ۲)$ و $(۱, ۳)$ را بیابید.

حل با استفاده از دستور $\mathrm{Orbit}(G, x, OnRight)$ مدار x تحت عمل گروه G با ضرب از راست روی خودش به دست می‌آید. به همین نحو ثابت ساز x تحت عمل گروه G با ضرب از راست روی خودش با استفاده از دستور $\mathrm{Stabilizer}(G, x, OnRight)$ به دست می‌آید

```
gap>s3:=SymmetricGroup(3);;
gap>Orbit(s3,(1,2),OnRight);
[ (), (2,3), (1,2), (1,2,3), (1,3,2), (1,3) ]
gap>Orbit(s3,(1,3,2),OnRight);
```

```
 [ (), (2,3), (1,2), (1,2,3), (1,3,2), (1,3) ]
gap>Stabilizer(s3,(1,2),OnRight);
 Group(())
gap>Stabilizer(s3,(1,3,2),OnRight);
 Group(())
```

اگر گروه G روی مجموعه‌ی x عمل کند، یک همریختی از G به S_X وجود دارد. دستور $\mathrm{Action}(G, X, act)$ گروه جایگشتی متناظر با S_X را به دست می‌دهد. هم‌چنین دستور $\mathrm{ActionHomomorphism}(G, X, act)$ همریختی متناظر عمل G روی x را می‌یابد

```
gap>sxr:=Action(s3,AsList(s3),OnRight);
 Group([ (1,4,5)(2,3,6), (1,3)(2,4)(5,6) ])
gap>h1:=ActionHomomorphism(s3,AsList(s3),OnRight);
 <action homomorphism>
gap>Image(h1);  Size(Range(h1));  Size(Image(h1));
 Group([ (1,4,5)(2,3,6), (1,3)(2,4)(5,6) ])
 720
 6
gap>Image(h1,(1,2));  Image(h1,(1,3));
 (1,3)(2,4)(5,6)
 (1,6)(2,5)(3,4)
```

مثال ۳.۱۴.۱۶. عمل S_3 را روی خودv، با ضرب وارون از چپ، در نظر بگیرید. مدار $(۲ ,۱)$ و $(۲ ,۳ ,۱)$ و ثابت‌سازهای آن‌ها را بیابید. همریختی متناظر این عمل را تعریف کنید؛ تصویر $(۲ ,۱)$ و $(۳ ,۱)$ را بیابید.

حل همانند مثال قبل عمل می‌کنیم. اما در این جا عمل مورد نظر LeftInverse است. بررسی جزئیات کار را به خواننده واگذار می‌کنیم

```
gap>s3:=SymmetricGroup(3);;
gap>Orbit(s3,(1,2),OnLeftInverse);  Orbit(s3,(1,3,2),OnLeftInverse);
 [ (), (2,3), (1,2), (1,2,3), (1,3,2), (1,3) ]
 [ (), (2,3), (1,2), (1,2,3), (1,3,2), (1,3) ]
gap>Stabilizer(s3,(1,2),OnLeftInverse);
 Group(())
gap>Stabilizer(s3,(1,3,2),OnLeftInverse);
 Group(())
gap>h2:=ActionHomomorphism(s3,AsList(s3),OnLeftInverse);
 <action homomorphism>
gap>Image(h2);
 Group([ (1,5,4)(2,3,6), (1,3)(2,5)(4,6) ])
gap>Size(Range(h2));  Size(Image(h2));
 720
 6
gap>Image(h2,(1,2));  Image(h2,(1,3));
 (1,3)(2,5)(4,6)
 (1,6)(2,4)(3,5)
```

مثال ۴.۱۴.۱۶. فرض کنید $X_n = \{۱, ۲, \ldots, n\}$. در این صورت S_n روی مجموعه‌ی $X_n^m = \underbrace{X_n \times \cdots \times X_n}_{m \text{ بار}}$ به طور طبیعی با

$$[x_۱, \ldots, x_m] \cdot \alpha = [x_۱\alpha, \ldots, x_m\alpha]$$

عمل می‌کند. عمل $S_۳$ روی $X_۳ \times X_۳$ در نظر بگیرید. مدار $[۱, ۲]$ و $[۲, ۳]$ و ثابت‌سازهای آن‌ها را بیابید. همریختی متناظر این عمل را تعریف کنید؛ تصویر $(۱, ۲)$ و $(۲, ۳)$ را بیابید.

حل در این جا عمل $S_۳$ روی دوتایی‌های متشکل از عناصر $X_۳$ مورد نظر است. در GAP این عمل با OnPairs مشخص می‌شود. همانند مثال قبل عمل می‌کنیم. اما در این جا عمل مورد نظر OnPairs است. بررسی جزئیات کار را به خواننده واگذار می‌کنیم

```
gap>s3:=SymmetricGroup(3);;
gap>Orbit(s3,[1,2],OnPairs);    Orbit(s3,[2,3],OnPairs);
[ [ 1, 2 ], [ 1, 3 ], [ 2, 1 ], [ 2, 3 ], [ 3, 1 ], [ 3, 2 ] ]
[ [ 1, 2 ], [ 1, 3 ], [ 2, 1 ], [ 2, 3 ], [ 3, 1 ], [ 3, 2 ] ]
gap>Stabilizer(s3,[1,2],OnPairs);
Group(())
gap>Stabilizer(s3,[2,3],OnPairs);
Group(())
gap>h3:=ActionHomomorphism(s3,Tuples([1..3],2),OnPairs);
<action homomorphism>
gap>Size(Range(h3));  Size(Image(h3));
362880
6
gap>Image(h3,(1,2));  Image(h3,(2,3));
(1,5)(2,4)(3,6)(7,8)
(2,3)(4,7)(5,9)(6,8)
```

مثال ۵.۱۴.۱۶. فرض کنید H گروه تولید شده توسط جایگشت‌های $(۲, ۳)$، $(۱, ۲)(۳, ۴)$ باشد. عمل $S_۴$ روی مجموعه‌ی هم مجموعه‌های راست H در $S_۴$ با ضرب از راست را در نظر بگیرید. همریختی متناظر این عمل را تعریف کنید. تصویر جایگشت‌های $(۱, ۲, ۳, ۴)$، $(۳, ۴)$، و $(۱, ۴, ۲, ۳)$ را بیابید.

حل ابتدا گروه $S_۴$ و H را تعریف می‌کنیم. سپس هم مجموعه‌های راست H در $S_۴$ را در متغیر x قرار می‌دهیم. باقی مراحل همانند مثال‌های قبل است. در این جا عمل مورد نظر OnRight است. بررسی جزئیات را به خواننده واگذار می‌کنیم

```
gap>s4:=SymmetricGroup(4);;
gap>H:=Group((1,2)(3,4),(2,3));; SetName(H,"H");
gap>Size(H);
8
gap>x:=RightCosets(s4,H);
[ RightCoset(H,()), RightCoset(H,(3,4)), RightCoset(H,(2,3,4)) ]
gap>a:=Action(s4,x,OnRight);
Group([ (1,3), (1,2) ])
gap>h5:=ActionHomomorphism(s4,x,OnRight);
<action homomorphism>
gap>Kernel(h5);  Image(h5);
```

```
 Group([ (1,2)(3,4), (1,3)(2,4) ])
 Group([ (1,3), (1,2) ])
gap>Size(Range(h5));  Size(Image(h5));
 6
 6
gap>Image(h5,(1,2,3,4));  Image(h5,(3,4));
 (1,3)
 (1,2)
gap>Image(h5,(1,4,2,3));
 (1,2)
```

مثال ۶.۱۴.۱۶. عمل S_4 روی A_4 را به صورت مزدوجی در نظر بگیرید. مدارهای این عمل را به دست آورید. مدار عناصر $(۱, ۲, ۳)$ و $(۱, ۳, ۴, ۲)$ را پیدا کنید. همریختی متناظر این عمل را تعریف کنید.

حل ابتدا گروه S_4 را تعریف می‌کنیم. سپس عناصر گروه A_4 را در مجموعه‌ی $a4$ قرار می‌دهیم. چون عمل مزدوجی در GAP تعریف نشده تابعی به‌نام $\mathrm{onconj}(x, g)$ می‌نویسیم که مزدوج x تحت G را به دست دهد. باقی مراحل همانند مثال‌های قبل است. اما در این جا عمل مورد نظر onconj است. بررسی جزئیات کار را به خواننده واگذار می‌کنیم

```
gap>s4:=SymmetricGroup(4);;
gap>a4:=AsList(AlternatingGroup(4));;
gap>onconj:=function(x,g)
>     return x^g;
> end;;
gap>Orbits(s4,a4,onconj);
 [[()],[(2,3,4),(2,4,3),(1,2,3),(1,2,4),(1,3,2), (1,3,4),(1,4,2),(1,4,3)],
 [(1,2)(3,4),(1,3)(2,4),(1,4)(2,3)]]
gap>Orbit(s4,(1,2,3),onconj);
 [(2,3,4),(2,4,3),(1,2,3),(1,2,4),(1,3,2),(1,3,4),(1,4,2),(1,4,3) ]
gap>Orbit(s4,(1,3,4,2),onconj);
 [(1,2,3,4),(1,2,4,3),(1,3,4,2),(1,3,2,4),(1,4,3,2),(1,4,2,3) ]
gap>sx4:=Action(s4,a4,onconj); Size(sx4);
 Group([(2,8,6,5)( 3,11,10,7)(4,12),(2,8)(3,11)(5,7)(6,10)(9,12)])
 24
gap>h4:=ActionHomomorphism(s4,a4,onconj);
 <action homomorphism>
gap>Image(h4);
 Group([(2,8,6,5)(3,11,10,7)(4,12), (2,8)(3,11)(5,7)(6,10)(9,12)])
gap>Size(Range(h4));   Size(Image(h4));
 479001600
 24
gap>Kernel(h4);
 Group(())
```

تمرین‌ها (با استفاده از GAP)

۱. نمایش جایگشتی راست منظم گروه D_8 را بیابید.

۲. نمایش جایگشتی راست منظم گروه $\mathrm{GL}_2(\mathbb{Z}_3)$ را بیابید.

۳. عمل طبیعی S_5 را روی $X_5 \times X_5 \times X_5$ در نظر بگیرید و مدار $[1,2,3]$ و ثابت‌ساز آن را بیابید. این عمل چند مدار دارد.

۴. معادله‌ی $|X| = |X_f| + \sum |G : \mathrm{stab}(x_i)|$ را برای عمل A_5 روی هم‌مجموعه‌های راست $H = \langle (1\ 2)(1\ 3\ 4) \rangle$ تحقیق کنید.

۵. عمل $A_4 \times S_3$ روی S_4 را با $(h,k) \cdot x = h^{-1}xk$ در نظر بگیرید و مدارهای عمل را بیابید.

۱۵.۱۶ زیرگروه‌های سیلو در GAP، آزمایشگاه پانزدهم

در این آزمایشگاه نحوه‌ی یافتن زیرگروه‌های سیلوی گروه را تشریح می‌کنیم.

مثال ۱.۱۵.۱۶. فرض کنید p عدد اول باشد. برنامه‌ای بنویسید که همه‌ی p- زیرگروه‌های سیلوی گروه داده شده را بیابید. با استفاده از این برنامه همه‌ی زیرگروه‌های سیلوی A_5 را بیابید.

حل با استفاده از دستور $\mathrm{SylowSubgroup}(G,p)$ یک p- زیرگروه سیلو از گروه G به‌دست می‌آید. چون p- زیرگروه‌های سیلوی G در G مزدوج‌اند، با پیدا کردن همه‌ی مزدوج‌ها یک p- زیرگروه سیلو می‌توان همه‌ی p- زیرگروه‌های سیلوی G را یافت. با توجه به این مطلب برنامه $sylp(g,p)$ را می‌نویسیم که همه‌ی p- زیرگروه‌های سیلوی گروه g را محاسبه می‌کند

```
gap>sylp:=function(g,p)
>    return ConjugateSubgroups(g,SylowSubgroup(g,p));
>end;;
```

همه‌ی شمارنده‌های اول $|A_5|$ را می‌یابیم

```
gap>a5:=AlternatingGroup(5);; Set(Factors(Size(a5)));
 [2,3,5]
```

اکنون با استفاده از تابع sylp که در بالا تعریف شد زیرگروه‌های سیلوی A_5 را می‌یابیم. ۲- زیرگروه‌های سیلوی A_5 عبارت‌اند از

```
gap>s2:=sylp(a5,2);
 [Group([(1,2)(3,4),(1,3)(2,4)]), Group([(1,5)(2,3),(1,3)(2,5)]),
 Group([(1,2)(4,5),(1,4)(2,5)]), Group([(1,5)(3,4),(1,4)(3,5)]),
 Group([(2,3)(4,5),(2,4)(3,5)])]
gap>List(s2,x->Elements(x));
 [[(),(1,2)(3,4),(1,3)(2,4),(1,4)(2,3)], [(),(1,2)(3,5),(1,3)(2,5),(1,5)(2,3)],
 [(),(1,2)(4,5),(1,4)(2,5),(1,5)(2,4)], [(),(1,3)(4,5),(1,4)(3,5),(1,5)(3,4)],
 [(),(2,3)(4,5),(2,4)(3,5),(2,5)(3,4)]]
```

۳- زیرگروه‌های سیلوی A_5 عبارت‌اند از

```
gap>s3:=sylp(a5,3);
 [Group([(1,2,3)]),Group([(1,2,4)]),Group([(1,2,5)]), Group([(1,3,4)]),
 Group([(1,3,5)]),Group([(1,4,5)]),Group([(2,3,4)]), Group([(2,3,5)]),
 Group([(2,4,5)]),Group([(3,4,5)])]
gap>List(s3,x->Elements(x));
 [[(),(1,2,3),(1,3,2)],[(),(1,2,4),(1,4,2)], [(),(1,2,5),(1,5,2)],
```

[(),(1,3,4),(1,4,3)],[(),(1,3,5),(1,5,3)],[(),(1,4,5),(1,5,4)],
[(),(2,3,4),(2,4,3)],[(),(2,3,5),(2,5,3)],[(),(2,4,5),(2,5,4)],[(),(3,4,5),(3,5,4)]]

۵- زیرگروه‌های سیلوی A_5 عبارت‌اند از

```
gap>s5:=sylp(a5,5);
[Group([(1,2,3,4,5)]),Group([(1,2,4,5,3)]), Group([(1,2,5,3,4)]),
Group([(1,3,2,5,4)]), Group([(1,3,4,2,5)]),Group([(1,4,2,3,5)])]
gap>List(s5,x->Elements(x));
[[(),(1,2,3,4,5),(1,3,5,2,4),(1,4,2,5,3),(1,5,4,3,2)],
[(),(1,2,4,5,3),(1,3,5,4,2),(1,4,3,2,5),(1,5,2,3,4)],
[(),(1,2,5,3,4),(1,3,2,4,5),(1,4,3,5,2),(1,5,4,2,3)],
[(),(1,2,4,3,5),(1,3,2,5,4),(1,4,5,2,3),(1,5,3,4,2)],
[(),(1,2,3,5,4),(1,3,4,2,5),(1,4,5,3,2),(1,5,2,4,3)],
[(),(1,2,5,4,3),(1,3,4,5,2),(1,4,2,3,5),(1,5,3,2,4)]]
```

تمرین‌ها (با استفاده از GAP)

۱. فرض کنید P، p- زیرگروه سیلوی دلخواهی از گروه متناهی G باشد ؛ داریم $N_G(N_G(P)) = N_G(P)$. این مطلب را برای همه‌ی زیر گروه‌های سیلوی A_4، S_5، D_{32} تحقیق کنید.

۲. با استفاده از فرمول $n_p = |G : N_G(P)|$، تعداد p- زیرگروه‌های سیلوی $GL_3(F_8)$ و S_7 را بیابید.

۳. فرض کنید X مجموعه ۲- زیرگروه‌های سیلوی A_6 باشد. عمل A_6 را روی X به صورت مزدوجی و $P \in X$ را دلخواه در نظر بگیرید. $\mathrm{stab}(P)$ را بیابید. برقراری معادله‌ی $|X| = |X_f| + \sum |A_6 : \mathrm{stab}(P_i)|$ را تحقیق کنید.

۴. یک p- زیرگروه سیلوی دلخواه P از A_6 را در نظر بگیرید. عمل A_6 روی هم مجموعه‌های چپ P در A_6 را تشکیل داده و برقراری معادله‌ی زیر را تحقیق کنید:

$$|X| = |X_f| + \sum |A_6 : \mathrm{stab}(Px_i)|.$$

۱۶.۱۶ سری زیر گروه‌ها در GAP، آزمایشگاه شانزدهم

قبل از هر چیز از آزمایشگاه ششم یادآور می‌شویم یک طریقه‌ی نمایش برخی گروه‌ها در GAP به صورت pc -گروه (گروه‌های چند دوری) است. اگر G یک گروه چند دوری با سری دوری

$$G = G_0 \rhd G_1 \rhd \cdots \rhd G_n = \{1\}$$

باشد، آنگاه به ازای هر $i = 0, 1, 2, \ldots, n-1$،

$$G_i/G_{i+1} = \langle x_i G_{i+1} \rangle ;$$

و بنابراین $G = \langle x_0, x_1, \ldots, x_{n-1} \rangle$. در GAP برای نمایش یک گروه چند دوری با استفاده از مولدها، یک سری دوری برای گروه اختیار می‌شود و مانند بالا مولدهای گروه به دست می‌دهند. واضح است به این ترتیب ممکن است مجموعه‌ی مولد ماکسیمال برای گروه به دست نیاید.

در این آزمایشگاه سری‌های متناظر یک گروه از قبیل سری‌های ترکیبی، مرکزی پایینی، مرکزی بالایی، ... را بررسی می‌کنیم. قبل از هر چیز چند مفهوم دیگر را تعریف می‌کنیم. اگر G یک گروه باشد و $H \leq G$. سری

$$H = H_0 \trianglelefteq H_1 \trianglelefteq \cdots \trianglelefteq H_n = G$$

از زیر گروه‌های G را یک سری زیرنرمال از H به G نامیم. توجه کنید به ازای هر i، $H_i \trianglelefteq H_{i+1}$؛ اما لزومی ندارد که جملات سری در G نرمال باشند. سری زیرنرمال از $\{1\}$ به G را به‌طور ساده یک سری گوییم. بنابراین یک سری ترکیبی برای G یک سری (زیرنرمال از $\{1\}$ به G) است که تظریف سره ندارد.
یادآوری می‌کنیم یک سری نرمال برای G یک سری به صورت

$$\{1\} = G_0 \leq G_1 \leq \cdots \leq G_n = G \qquad (1)$$

است طوری که به ازای هر i، $G_i \trianglelefteq G$.یک سری نرمال که تظریف سره به سری زیرنرمال نداشته باشد را سری اساسی (یا چیف سری) نامیم. عوامل سری اساسی را عوامل اساسی گوییم. می‌دانیم (قضیه‌ی ۱۷.۴.۷ را ببینید) سری (۱) سری اساسی است اگر و تنها هر عامل G_{i+1}/G_i از آن ، زیرگروه نرمال ماکسیمال G/G_i باشد.

مثال ۱.۱۶.۱۶. گروه متقارن S_4 را تعریف کنید و
(الف) یک سری ترکیبی برای S_4 را بیابید. اندازه هر جمله و نوع هر عامل سری را بیابید.
(ب) یک سری اساسی برای S_4 بیابید.
(ج) یک سری زیرنرمال از $H = \langle (1\ 2)(3\ 4), (1\ 2) \rangle$ به S_4 بیابید.
(د) سری‌های مرکزی پائینی و بالایی برای S_4 را بیابید.
(هـ) آیا S_4حل‌پذیر است؟ آیا S_4 پوچ‌توان است؟
(و) می‌توان نشان داد هر عامل اساسی یک گروه حل‌پذیر متناهی، آبلی مقدماتی است. یک سری اساسی با عوامل آبلی مقدماتی برای S_4 بیابید.

حل (الف) ابتدا S_4 را تعریف می‌کنیم. با استفاده از دستور $\mathrm{CompositionSeries}(G)$ سری ترکیبی برای یک گروه G را به دست می‌آوریم

```
gap>s4:=SymmetricGroup(4);;
gap>co:=CompositionSeries(s4);
 [Group([(3,4),(2,4,3),(1,4)(2,3),(1,2)(3,4)]),Group([(2,4,3),(1,4)(2,3),(1,2)(3,4)]),
 Group([(1,4)(2,3),(1,2)(3,4)]),Group([(1,2)(3,4)]), Group(())]
gap>List(co,Size);
 [ 24, 12, 4, 2, 1 ]
```

دستور $\mathrm{DisplayCompositionSeries}(G)$ سری ترکیبی برای گروه G را به صورت جالبی نمایش می‌دهد. در این دستور تعداد مولدهای هر جمله، اندازه‌ی هر جمله، و نوع هر عامل ترکیبی به دست می‌آید

```
gap>DisplayCompositionSeries(s4);
 G (4 gens, size 24)
 | Z(2)
 S (3 gens, size 12)
 | Z(3)
 S (2 gens, size 4)
 | Z(2)
 S (1 gens, size 2)
 | Z(2)
 1 (0 gens, size 1)
```

(ب) با استفاده از دستور $\mathrm{ChiefSeries}(G)$ یک سری اساسی برای گروه G به دست می‌آید

```
gap>ch:=ChiefSeries(s4);
 [Sym([ 1 .. 4 ]),Group([(2,4,3),(1,4)(2,3),(1,2)(3,4)]),
```

```
 Group([(1,4)(2,3),(1,2)(3,4)]),Group(())]
gap>List(ch,Size);
 [ 24, 12, 4, 1 ]
```

(ج) با استفاده از دستور SubnormalSeries(G,H) سری زیرنرمال از H به گروه G به دست می‌آید

```
gap>su:=SubnormalSeries(s4,Group((1,2)(3,4)));
 [Sym([ 1 .. 4 ]),Group([(1,2)(3,4),(1,3)(2,4)]),Group([(1,2)(3,4)]) ]
gap>List(su,Size);
 [ 24, 4, 2 ]
```

(د) با استفاده از دستورهای LowerCentralSeries(G) و UpperCentralSeries(G)، به ترتیب سری مرکزی پائینی و سری مرکزی بالایی برای گروه G حاصل می‌شود

```
gap>lo:=LowerCentralSeries(s4);
 [Sym([ 1 .. 4 ]),Group([(1,3,2),(1,4,3)])]
gap>List(lo,Size);
 [ 24, 12 ]
gap>up:=UpperCentralSeries(s4);
 [ Group(())]
```

(هـ) هر چند که از سری مشتق و سری‌های مرکزی می‌توان دریافت که S_4حل‌پذیر است، اما پوچ‌توان نیست. با استفاده از دستورهای IsSolvable(G) و IsNilpotent(G) بررسی این مطالعه مستقیماً نیز امکانپذیر است

```
gap>IsSolvable(s4);
 true
gap>IsNilpotent(s4);
 false
```

(و) با استفاده از دستور ElementaryAbelianSeries(G) سری اساسی با عوامل آبلی مقدماتی به دست می‌آید

```
gap>e:=ElementaryAbelianSeries(s4);
 [Group([(3,4),(2,4,3),(1,4)(2,3),(1,3)(2,4)]),Group([(2,4,3),(1,4)(2,3),(1,3)(2,4)]),
 Group([(1,4)(2,3),(1,3)(2,4)]),Group(())]
gap>List(e,Size);
 [ 24, 12, 4, 1 ]
```

در صورتی که گروه G حل‌پذیر نباشد دستور ElementaryAbelianSeries(G) منجر به پیغام خطا می‌شود

```
gap>ElementaryAbelianSeries(AlternatingGroup(5));
 Error <G> must be solvable at Error( "<G> must be solvable" );
 <function>( <arguments> ) called from read-eval-loop
 Entering break read-eval-print loop, you can 'quit;'
 to quit to outer loop, or you can return to continue
 brk>
```

مثال ۲.۱۶.۱۶. یک ۲-زیرگروه سیلوی S_6 را بیابید؛ آن را syl2 نام‌گذاری کنید و

(الف) یک سری ترکیبی برای syl2 را بیابید. اندازه‌ی هر جمله و نوع هر عامل سری را بیابید.

(ب) یک سری اساسی برای syl2 بیابید.

(د) سری‌های مرکزی پائینی و بالایی برای syl2 را بیابید.

(هـ) یک سری اساسی با عوامل آبلی مقدماتی برای syl2 بیابید.

حل ابتدا syl2 را با استفاده از دستور SylowSubgroup(G,p) می‌یابیم

```
gap>s6:=SymmetricGroup(6);;
gap>Factors(Size(s6));
 [ 2, 2, 2, 2, 3, 3, 5 ]
gap>syl2:=SylowSubgroup(s6,2);
 Group([(1,2),(3,4),(1,3)(2,4),(5,6)])
gap>Size(syl2);
 16
```

(الف) با استفاده از دستور CompositionSeries(syl2) یک سری ترکیبی برای syl2 را به دست می‌آوریم

```
gap>co:=CompositionSeries(syl2);
 [Group([(5,6),(1,3)(2,4),(3,4),(1,2)]), Group([(1,3)(2,4),(3,4),(1,2)]),
 Group([(3,4),(1,2)]),Group([(1,2)]),Group(())]
gap>List(co,Size);
 [ 16, 8, 4, 2, 1 ]
```

و با استفاده از دستور DisplayCompositionSeries(syl2) خصوصیات سری ترکیبی syl2 را ملاحظه می‌کنیم

```
gap>DisplayCompositionSeries(syl2);
 G (4 gens, size 16)
  | Z(2)
 S (3 gens, size 8)
  | Z(2)
 S (2 gens, size 4)
  | Z(2)
 S (1 gens, size 2)
  | Z(2)
 1 (0 gens, size 1)
```

(ب) با استفاده از دستور ChiefSeries(syl2) یک سری اساسی برای syl2 به دست می‌آوریم

```
gap>ch:=ChiefSeries(syl2);
 [Group([(1,2),(3,4),(1,3)(2,4),(5,6)]), Group([(1,3)(2,4),(3,4),(1,2)]),
 Group([(3,4),(1,2)]),Group([(1,2)(3,4)]),Group(())]
gap>List(ch,Size);
 [ 16, 8, 4, 2, 1 ]
```

(ج) با استفاده از دستور LowerCentralSeries($syl۲$) سری مرکزی پائینی و با استفاده از دستور UpperCentralSeries(syl2) سری مرکزی بالایی گروه syl2 را می‌یابیم

```
gap>IsNilpotent(syl2);
 true
gap>lo:=LowerCentralSeries(syl2);
 [Group([(5,6),(1,3)(2,4),(3,4),(1,2)(3,4)]),Group([(1,2)(3,4)]),Group(())]
gap>List(lo,Size);
 [ 16, 2, 1 ]
gap>up:=UpperCentralSeries(syl2);
 [ Group([(1,2)(3,4),(5,6),(1,3)(2,4),(3,4)]),Group([(1,2)(3,4),(5,6)]),Group(())]
```

```
gap>List(up,Size);
[ 16, 4, 1 ]
```

(د) با استفاده از دستور ElementaryAbelianSeries(syl2) سری اساسی syl2 با عوامل مقدماتی را می‌یابیم

```
gap>e:=ElementaryAbelianSeries(syl2);
[Group([(5,6),(1,3)(2,4),(3,4),(1,2)]), Group([(1,3)(2,4),(3,4),(1,2)]),
 Group([(3,4),(1,2)]),Group(())]
gap>List(e,Size);
[ 16, 8, 4, 1 ]
```

تمرین‌ها (با استفاده از GAP)

۱. در هر مورد پوچ‌توان بودن یا نبودن گروه داده شده را بررسی کنید.
(الف) گروه ماتریس‌های ۲×۲ بالا مثلثی وارون پذیر با درایه‌های در میدان $\mathbb{Z}_۵$.
(ب) گروه ماتریس‌های ۳×۳ پایین مثلثی وارون پذیر با درایه‌های در میدان $\mathbb{Z}_۳$.
(ج) $D_{۱۸}$، $D_{۳۲}$، $D_{۶۴}$.

۲. سری‌های مرکزی پایینی، بالایی، و سری ترکیبی گروه‌های تمرین قبل را بیابید.

۳. با استفاده از دستور MaximalSubgroup زیرگروه‌های ماکسیمال گروه‌های داده شده را بیابید و زیرگروه فراتینی آن‌ها را تعیین کنید.
(الف) $D_۸$ (ب) $D_{۱۲}$ (ج) $S_۵$
(د) $D_{۳۸}$ (هـ) $\mathrm{GL}_۲(\mathbb{Z}_۳)$ (و) $\mathrm{GL}_۳(\mathbb{Z}_۵)$

۴. در حالت زیر طول ترکیبی و عوامل ترکیبی گروه داده شده را بیابید.
(الف) $C_۸$ (ب) $C_{۱۲}$ (ج) $D_۸$ (د) $A_۴$ (هـ) $Q_۸$

۵. همه‌ی سری‌های ترکیبی گروه‌های زیر را بیابید
(الف) $\mathbb{Z}_{۲۰}$ (ب) $C_{۲۴}$ (ج) $C_{۳۰}$ (د) $S_۳$ (هـ) $S_۴$
(و) $\mathbb{Z}_۲ \times \mathbb{Z}_۲$ (ز) $C_۸ \times C_۴$

۱۷.۱۶ حلقه‌ها در GAP، آزمایشگاه هفدهم

در این آزمایشگاه چگونگی تعریف و پردازش حلقه‌های متنوع را بررسی می‌کنیم.

مثال ۱.۱۷.۱۶. (الف) حلقه‌ی رده‌های مانده‌ای به پیمانه‌ی ۸، $\mathbb{Z}_۸$، را تعریف کنید و
(الف) یکه‌های آن را بیابید.
(ب) زیرحلقه‌ی تولید شده توسط عضو $\bar{۲}$ در $\mathbb{Z}_۸$ (یعنی کوچک‌ترین زیرحلقه‌ی $\mathbb{Z}_۸$ که شامل $\bar{۲}$ است) را بیابید.
(ج) ایدآل تولید شده توسط $\bar{۲}$ در $\mathbb{Z}_۸$ (یعنی کوچک‌ترین ایدآل $\mathbb{Z}_۸$ که شامل $\bar{۲}$) را بیابید.

حل با استفاده از دستور ZmodnZ(n) یا معادل آن n mod Integers حلقه‌ی اعداد صحیح به پیمانه‌ی n به دست می‌دهند. در این حلقه برای نشان دادن $\bar{a}$ از ZmodnZObj(a, n) استفاده می‌شود

```
gap>Z8:=Integers mod 8;
(Integers mod 8)
gap>e8:=Elements(Z8);
[ZmodnZObj(0,8),ZmodnZObj(1,8),ZmodnZObj(2,8),
 ZmodnZObj(3,8),ZmodnZObj(4,8),ZmodnZObj(5,8),
```

ZmodnZObj(6,8),ZmodnZObj(7,8)]

(الف) یکه‌های حلقه‌ی یکدار R با استفاده از دستور $\mathrm{Units}(R)$ به دست می‌دهند

gap>G:=Units(Z8);

<group of size 4 with 2 generators>

gap>E8:=Elements(G);

[ZmodnZObj(1,8),ZmodnZObj(3,8),ZmodnZObj(5,8),ZmodnZObj(7,8)]

(ب) با استفاده از دستور $\mathrm{Subring}(R,X)$ زیرحلقه‌ی تولید شده توسط زیرمجموعه‌ی X در حلقه‌ی R حاصل می‌شود

gap>S:=Subring(Z8,[e8[3]]);

<ring with 1 generators>

gap>Elements(S);

[ZmodnZObj(0,8),ZmodnZObj(2,8),ZmodnZObj(4,8),ZmodnZObj(6,8)]

(ج) با استفاده از دستور $\mathrm{Ideal}(R,X)$ یا به طور معادل $\mathrm{TwoSidedIdeal}(R,X)$ ایدآل تولید شده توسط زیرمجموعه‌ی X در حلقه‌ی R حاصل می‌شود

gap>I:=Ideal(Z8,[e8[3]]);

<two-sided ideal in (Integers mod 8), (1 generators)>

gap>Elements(I);

[ZmodnZObj(0,8),ZmodnZObj(2,8),ZmodnZObj(4,8),ZmodnZObj(6,8)]

gap>S=I;

true

همانطور که ملاحظه شد در حلقه‌ی $\mathbb{Z}_8$ زیرحلقه‌ی تولید شده توسط $\bar{2}$ با ایدآل تولید شده توسط $\bar{2}$ برابر است.

مثال ۲.۱۷.۱۶. کوچک‌ترین حلقه‌ی شامل ۲ و i را بیابید.

حل با استفاده از دستور $\mathrm{Ring}(z,w,\ldots)$ کوچک‌ترین حلقه‌ای که شامل اعضای $z,w,\ldots$ است حاصل می‌شود. در GAP عدد $e^{\frac{2\pi i}{n}}$، که یک ریشه‌ی اولیه‌ی واحد است، با E(n) نشان داده می‌شود. در این‌جا داریم $E(4)=e^{\frac{2\pi i}{4}}=i$. یادآوری می‌کنیم یک ریشه‌ی اولیه‌ی واحد عددی مثل ω است که گروه ضربی $C_n=\{z\in\mathbb{C}\mid z^n=1\}$، متشکل از همه‌ی ریشه‌های nام واحد را تولید کند

gap>R1:=Ring(2,E(4));

<ring with 2 generators>

gap>Order(2+E(4));

infinity

gap>Order(E(4));

4

مثال ۳.۱۷.۱۶. (الف) حلقه‌ی اعداد صحیح گاوسی $\mathbb{Z}[i]=\{m+in\mid m,n\in\mathbb{Z}\}$ را تعریف کنید و مجموعه‌ی مولد (یعنی زیرمجموعه‌ی X که زیرحلقه‌ی تولید شده توسط آن برابر $\mathbb{Z}[i]$ باشد) آن را بیابید.

(ب) زیرحلقه‌ی و ایدآل تولید شده توسط $2+i$ را بیابید.

(ج) یکه‌های $\mathbb{Z}[i]$ را به دست آورید.

حل با استفاده از دستور GaussianIntegers حلقه‌ی اعداد صحیح گاوسی به دست می‌آید. مجموعه‌ی مولد یک حلقه‌ی R با استفاده از دستور $\mathrm{GeneratorsOfRing}(R)$ حاصل می‌شود

gap>R2:=GaussianIntegers;

GaussianIntegers

gap>Size(R2);

infinity

```
gap>2+E(4) in R2;
 true
gap>GeneratorsOfRing(R2);
 [ E(4) ]
```

(ب)

```
gap>S1:=Subring(R2,[2+E(4)]);
 <ring with 1 generators>
gap>I1:=Ideal(R2,[2+E(4)]);
 <two-sided ideal in GaussianIntegers, (1 generators)>
```

(ج) یکه‌های $\mathbb{Z}[i]$ عبارت‌اند از

```
gap>Units(R2);
 [ -1, 1, -E(4), E(4) ]
```

مثال ۴.۱۷.۱۶. (الف) حلقه‌ی ماتریس‌های ۲ × ۲ با درایه‌های در $\mathbb{Z}_8$ (با نام M) را تعریف کنید.
(ب) حلقه‌ی ماتریس‌های ۲ × ۲ با درایه‌های در $\mathbb{Z}_2$ (با نام T) را تعریف کنید.
(ج) تعداد اعضای M، و T را بیابید.
(د) یکه‌های T را بیابید.

حل (الف) استفاده از هر کدام از دستورهای $\mathrm{FullMatrixAlgebra}(R,n)$ یا $\mathrm{MatAlgebra}(R,n)$، یا $R[n,n]$، منجر به تعریف جبر ماتریس‌های $n \times n$ روی حلقه‌ی R حاصل می‌شود. اگر R حلقه‌ی تعویض‌پذیر و یکدار باشد حلقه‌ی M را یک R- جبر گوییم هرگاه $(M,+)$ یک R- مدول یکانی باشد (یعنی بتوان هر عضو R، که آن‌ها را اسکالر می‌نامیم، در هر عضو M ضرب کرد و عضوی از M به دست آورد طوری که برای هر $r,s \in R$ و $a,b \in M$، داشته باشیم $r(a+b) = ra+rb$، $r(sa) = (rs)a$، $(r+s)a = ra+sa$، $1a = a$) و به علاوه به ازای هر $r \in R$، و $a,b \in M$، $r(ab) = (ra)b = a(rb)$. مدول‌ها را در فصل ۱۳ مطالعه خواهیم کرد. البته ما در این‌جا به ساختار حلقه‌ای M توجه داریم

```
gap>Z8:=Integers mod 8;;
gap>M:=FullMatrixAlgebra(Z8,2);
 ( (Integers mod 8)^[2,2] )
gap>IsRing(M);
 true
```

با استفاده از دستور $\mathrm{LeftActingDomain}(M)$ حلقه‌ی R حاصل می‌شود که M یک R- جبر باشد

```
gap>LeftActingDomain(M);
 (Integers mod 8)
```

(ب) با استفاده از دستور $\mathrm{MatAlgebra}(GF(۲),۲)$ جبر ماتریس‌های ۲ × ۲ با درایه‌های در $\mathbb{Z}_2$ را می‌یابیم

```
gap>T:=MatAlgebra(GF(2),2);
 ( GF(2)^[2,2] )
gap>LeftActingDomain(T);
 GF(2)
```

(ج) تعداد اعضای M و T عبارت‌اند از

```
gap>Size(M);     Size(T);
 256
 16
```

(د) یکه‌های T و تعداد آن‌ها عبارت‌اند از

```
gap>Units(T);      Size(Units(T));
 SL(2,2)
 6
```

مثال ۵.۱۷.۱۶. (الف) حلقه‌ی ماتریس‌های ۲ × ۲ با درایه‌های در حلقه‌ی $\mathbb{Z}_5$ (با نام M) را تعریف کنید.
(ب) اندازه و یکه‌های M را بیابید.
(ج) زیرحلقه‌ی

$$S = \begin{bmatrix} \mathbb{Z}_5 & \mathbb{Z}_5 \\ 0 & \mathbb{Z}_5 \end{bmatrix} = \left\{ \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \middle| \, a, b, c \in \mathbb{Z}_5 \right\}$$

از M را تعریف کنید. آیا این زیرحلقه‌ی ایدآل M است؟
(د) ایدآل‌های چپ، راست ، و دوطرفی تولید شده توسط ماتریس‌های زیر را بیابید.

$$m_1 = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \; m_2 = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}, \; m_3 = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$$

(هـ) اعضای خودتوان و مرکز n را بیابید.

حل (الف) با استفاده از دستور GF(5)^[2،2] جبر ماتریس‌های ۲ × ۲ با درایه‌های در $\mathbb{Z}_5$ را می‌یابیم.

```
gap>M:=GF(5)^[2,2];     Size(M);
 ( GF(5) ^[2,2] )
 625
```

(ب) یکه‌های M و تعداد آن‌ها عبارت‌اند از

```
gap>Units(M);     Size(Units(M));
 GL(2,5)
 480
```

(ج) ابتدا ماتریس‌های m۱، m۲ و m۳ را تعریف می‌کنیم. توجه کنید زیرحلقه‌ی تولید شده توسط این ماتریس‌ها برابر S است. سپس با استفاده دستور Subring$(M, [m1, m2, m3])$ زیرحلقه‌ی تولید شده توسط این ماتریس‌ها را می‌یابیم. در نهایت با دستور IsIdeal(M, S) ایدآل بودن S در M را بررسی می‌کنیم

```
gap>o:=0*Z(5);  l:=Z(5)^0;
 0*Z(5)
 Z(5)^0
gap>m1:=[[l,o],[o,o]];
 [ [ Z(5)^0, 0*Z(5) ], [ 0*Z(5), 0*Z(5) ] ]
gap>m2:=[[o,l],[o,o]];
 [ [ 0*Z(5), Z(5)^0 ], [ 0*Z(5), 0*Z(5) ] ]
gap>m3:=[[o,o],[o,l]];
 [ [ 0*Z(5), 0*Z(5) ], [ 0*Z(5), Z(5)^0 ] ]
gap>S:=Subring(M,[m1,m2,m3]);
 <algebra over GF(5), with 3 generators>
gap>Size(S);   IsIdeal(M,S);
 125
 false
```

(د) با استفاده از دستور Ideal$(M, [m1, m2, m3])$ ایدآل دوطرفی تولید شده توسط ماتریس‌های m_1، m_2، m_3 را می‌یابیم. به همین

نحو ایدآل چپ تولید شده توسط ماتریس‌های m_1، m_2، m_3 را با استفاده از دستور $\mathrm{LeftIdeal}(M,[m۱,m۲,m۳])$ و ایدآل راست تولید شده توسط ماتریس‌های m_1، m_2، m_3 را با استفاده از دستور $\mathrm{RightIdeal}(M,[m۱,m۲,m۳])$ می‌یابیم. ملاحظه کنید این ایدآل‌ها دقیقاً برابر M هستند. می‌دانیم $M_n(D)$ ایدآل (چپ، راست ، یا دوطرفی) نابدیهی ندارد

```
gap>I:=Ideal(M,[m1,m2,m3]);
 <two-sided ideal in <algebra-with-one of dimension 4 over GF(5)>,
   (3 generators)>
gap>Size(I);
 625
gap>IL:=LeftIdeal(M,[m1,m2,m3]);
 <left ideal in <algebra-with-one of dimension 4 over GF(5)>, (3 generators)>
gap>Size(IL);
 625
gap>IR:=RightIdeal(M,[m1,m2,m3]);
 <right ideal in<algebra-with-one of dimension 4 over GF(5)>, (3 generators)>
gap>Size(IR);
 625
```

(هـ) مجموعه‌ی اعضای خودتوان M و تعداد آن‌ها را می‌یابیم

```
gap>Idem:=Filtered(Elements(M),x-> x=x^2);;
gap>Size(Idem);
 32
```

اکنون مرکز M را به دست می‌آوریم

```
gap>C:=Center(M);
 <algebra of dimension 1 over GF(5)>
gap>Size(C);
 5
```

مثال ۶.۱۷.۱۶. کوچک‌ترین حلقه‌ای که شامل همه اعداد صحیح است و $\sqrt{۵}$ و i را در بر دارد بیابید.

حل با استفاده از دستور $\mathrm{ClosureRing}(R,llis)$ کوچک‌ترین حلقه‌ای که شامل حلقه‌ی R و لیست lis است به دست می‌آید

```
gap>R1:=ClosureRing(Integers,[Sqrt(2),E(4)]);
 <ring-with-one, with 3 generators>
```

مثال ۷.۱۷.۱۶. حلقه‌ی ماتریس‌های ۲×۲ با درایه‌های در $\mathbb{Z}_۵$ را تعریف کنید (به نام M) و
(الف) زیرحلقه‌ی تولید شده توسط ماتریس همانی را بیابید. آیا این زیرحلقه یک ایدآل است؟
(ب) نشان دهید زیرحلقه‌ی $S۲ = \begin{bmatrix} \mathbb{Z}_۵ & ۰ \\ \mathbb{Z}_۵ & ۰ \end{bmatrix}$ ایدآل چپ است و ایدآل راست نیست.
(ج) نشان دهید زیرحلقه‌ی $S۳ = \begin{bmatrix} ۰ & ۰ \\ \mathbb{Z}_۵ & \mathbb{Z}_۵ \end{bmatrix}$ ایدآل راست است و ایدآل چپ نیست.

حل $M_۲(\mathbb{Z}_۵)$ را تعریف می‌کنیم

```
gap>M:=GF(5)^[2,2];
 (GF(5)^[2,2])
```

(الف) با استفاده از دستور $\mathrm{One}(R)$ عضو همانی حلقه‌ی R به دست می‌آید. پس زیرحلقه‌ی تولید شده توسط ماتریس همانی را می‌توان به صورت زیر یافت

```
gap>S1:=Subring(M,[One(M)]);
 <algebra over GF(5), with 1 generators>
```

این زیرحلقه ایدآل نیست، زیرا

```
gap>IsIdeal(M,S1);
 false
```

(ب) زیرحلقه‌ی $S_۲$ را می‌توان به صورت زیر یافت و تحقیق کرد که ایدآل چپ است اما ایدآل راست نیست

```
gap>S2:=Subring(M,[One(GF(5))*[[1,0],[0,0]],One(GF(5))*[[0,0],[1,0]]]);
 <algebra over GF(5), with 2 generators>
gap>IsIdeal(M,S2);
 false
gap>IsLeftIdeal(M,S2);
 true
gap>IsRightIdeal(M,S2);
 false
```

(ج) زیرحلقه‌ی $S_۳$ را به صورت زیر می‌یابیم و تحقیق می‌کنیم که ایدآل راست است، اما ایدآل چپ نیست

```
gap>S3:=Subring(M,[One(GF(5))*[[0,0],[1,0]] , One(GF(5))*[[0,0],[0,1]] ]);
 <algebra over GF(5), with 2 generators>
gap>IsIdeal(M,S3);
 false
gap>IsLeftIdeal(M,S3);
 false
gap>IsRightIdeal(M,S3);
 true
```

تمرین‌ها (با استفاده از GAP)

۱. اعضای خودتوان، پوچ‌توان، و یکه حلقه‌های داده شده را بیابید.
(الف) $\mathbb{Z}_{۳۸}$ (ب) $\mathbb{Z}_{۱۴۶}$ (ج) $\mathbb{Z}_{۶۲۴}$
(د) $M_۲(\mathbb{Z}_۴)$ (هـ) $M_۳(\mathbb{Z}_۲)$ (و) $M_۳(\mathbb{Z}_۳)$

۲. مجموعه‌ی

$$R=\begin{bmatrix}\mathbb{Z}_۷ & \mathbb{Z}_۵\\ ۰ & \mathbb{Z}_۷\end{bmatrix}=\left\{\begin{bmatrix}n & a\\ ۰ & m\end{bmatrix}\middle| \, n,m\in\mathbb{Z}_۷,\ \ a\in\mathbb{Z}_۵\right\}$$

تحت عمل جمع و ضرب متعارف ماتریس‌ها، حلقه است. یکه‌ها پوچ‌توان‌ها و خودتوان‌های R را بیابید.

۳. در حلقه‌ی ماتریس‌های ۲×۲ با درایه‌های در $\mathbb{Z}_۶$ ایدآل و زیرحلقه‌ی تولید شده توسط

$$m_۱=\begin{bmatrix}۱ & ۰\\ ۰ & ۰\end{bmatrix},\ \ m_۲=\begin{bmatrix}۰ & ۱\\ ۰ & ۰\end{bmatrix},\ \ m_۳=\begin{bmatrix}۰ & ۰\\ ۱ & ۰\end{bmatrix}$$

را بیابید. آیا این دو با هم برابرند.

۴. در حلقه‌ی اعداد صحیح گاوسی ایدآل و زیرحلقه‌ی تولید شده توسط $۲i-۳$ را بیابید و آن‌ها را مقایسه کنید.

۵. کوچک‌ترین حلقه‌ی یکدار R که شامل $\sqrt{۲}$ و i است را بیابید. ایدآل و زیرحلقه‌ی تولید شده توسط $۲i-۳\sqrt{۲}$ را مقایسه کنید.

۶. کوچک‌ترین حلقه‌ی یکدار R که شامل $\sqrt{۲}$ و i است را بیابید با استفاده از دستور (RingWithOne). ایدآل و زیرحلقه‌ی تولید شد توسط $۲i - ۳\sqrt{۲}$ را مقایسه کنید.

۱۸.۱۶ حلقه‌ی چندجمله‌ای‌ها در GAP، آزمایشگاه هجدهم

در این آزمایشگاه نحوه‌ی تعریف و پردازش چندجمله‌ای‌ها روی یک حلقه‌ی دلخواه در GAP را بررسی می‌کنیم.

مثال ۱.۱۸.۱۶. (الف) چندجمله‌ای‌های $f(x) = x^۳ - ۴x + ۵$ و $g(x) = ۲x + ۱$ را در $\mathbb{Q}[x]$ تعریف کنید و
(ب) حاصل‌جمع و حاصل‌ضرب $f(x)$ و $g(x)$ را بیابید.
(ج) خارج‌قسمت و باقیمانده تقسیم $f(x)$ بر $g(x)$ را بیابید.
(د) $d(x) = \gcd\{f(x), g(x)\}$ را بیابید. چندجمله‌ای‌های $p(x)$ و $q(x)$ را طوری بیابید که $d(x) = p(x)f(x) + q(x)g(x)$.
(هـ) چندجمله‌ای $h(x) = ۴x^۴ + ۴x + ۳x^۲ - x - ۱ \in \mathbb{Q}[x]$ را تعریف کنید و ریشه‌ها و عوامل تحویل‌ناپذیر $h(x)$ را بیابید. هم‌چنین خارج‌قسمت و باقیمانده تقسیم $h(x)$ بر $f(x)$ را بیابید. به علاوه $d(x) = \gcd\{f(x), h(x)\}$ را بیابید و چندجمله‌ای‌های $p(x)$ و $q(x)$ را طوری بیابید که $d(x) = p(x)f(x) + q(x)h(x)$.

حل (الف) استفاده از دستور Indeterminate$(R, "ind")$ منجر به تعریف یک متغیر به نام ind برای چندجمله‌ای‌های با ضرایب در حلقه‌ی R می‌شود

```
gap>x:=Indeterminate(Rationals,"x");;
gap>f:=x^3-4*x+5;
 5-4*x+x^3
gap>g:=2*x+1;
 1+2*x
```

(ب) جمع و ضرب $f(x)$ و $g(x)$ را به صورت زیر می‌یابیم

```
gap>f*g;
 5+6*x-8*x^2+x^3+2*x^4
gap>f+g;
 6-2*x+x^3
```

(ج) با استفاده از دستور EuclideanQuotient(f, g) خارج‌قسمت تقسیم $f(x)$ بر $g(x)$ به دست می‌آید. با استفاده از دستور EuclideanRemainder(f, g) باقیمانده تقسیم $f(x)$ بر $g(x)$ حاصل‌ضرب می‌شود. در نهایت دستور QuotientRemainder(f, g) خارج‌قسمت و باقیمانده تقسیم $f(x)$ بر $g(x)$ را به دست می‌دهد

```
gap>EuclideanQuotient(f,g);
 -15/8-1/4*x+1/2*x^2
gap>EuclideanRemainder(f,g);
 55/8
gap>QuotientRemainder(f,g);
 [ -15/8-1/4*x+1/2*x^2, 55/8 ]
gap>QuotientRemainder(g,f);
 [ 0, 1+2*x ]
```

(د) با استفاده از دستور Gcd بزرگ‌ترین مقسوم‌علیه مشترک $f(x)$ و $g(x)$ را می‌یابیم. هم‌چنین دستور GcdRepresentation(f, g) چندجمله‌ای‌های $p(x)$ و $q(x)$ را به دست می‌دهد که $\gcd\{f, g\} = pf + qg$

```
gap>Gcd(f,g);
 1
```

```
gap>t:=GcdRepresentation(f,g);
[ 8/55, 3/11+2/55*x-4/55*x^2 ]
gap>t[1]*f+t[2]*g;
1
```

(هـ) با استفاده از دستور RootsOfUPol(f) ریشه‌های چندجمله‌ای یک متغیره $f(x)$ به دست می‌آید

```
gap>h:=4*x^4+4*x^3+3*x^2-x-1;
-1-x+3*x^2+4*x^3+4*x^4
```

هم‌چنین دستور Factor(a) عوامل تحویل‌ناپذیر a را به دست می‌دهد

```
gap>RootsOfUPol(h);
[ 1/2, -1/2 ]
gap>Factors(h);
[ -2+4*x, 1/2+x, 1+x+x^2 ]
```

اکنون خارج‌قسمت و باقی‌مانده تقسیم h بر $f(x)$ را می‌یابیم

```
gap>QuotientRemainder(h,f);
[ 4+4*x, -21-5*x+19*x^2 ]
```

با استفاده از دستور Gcd(f,g)، $d(x) = \gcd\{f(x), h(x)\}$ را تعیین می‌کنیم. در نهایت با استفاده از دستور GcdRepresentation(f,g) چندجمله‌ای‌های $p(x)$ و $q(x)$ را می‌یابیم که $d(x) = p(x)f(x) + q(x)h(x)$

```
gap>Gcd(f,h);
1
gap>GcdRepresentation(f,h);
[ 2139/10450+861/5225*x+586/5225*x^2+204/5225*x^3,
  49/2090-191/10450*x-51/5225*x^2 ]
```

مثال ۲.۱۸.۱۶. چندجمله‌ای‌های

$$f(x) = x^۴ + ۳x^۳ + x^۲ + ۳x + ۱$$
$$g(x) = x^۴ + x^۳ - ۷x^۲ + ۳x - ۲$$
$$h(x) = x^۴ + ۲x^۳ - ۲x^۲ + ۷x - ۲$$

را در $\mathbb{Q}[x]$ تعریف کنید. ریشه‌ها و عوامل تحویل‌ناپذیر آن‌ها روی $\mathbb{Q}$ بیابید.

حل با استفاده از دستور Indeterminate($Rationals$,"x") متغیر x را برای تعریف چندجمله‌ای‌های با ضرایب در حلقه‌ی $\mathbb{Q}$ تعریف می‌کنیم

```
gap>x:=Indeterminate(Rationals,"x");
x
```

اکنون چندجمله‌ای‌ها را تعریف می‌کنیم

```
gap>f:=x^4+3*x^3+x^2+3*x+1; g:=x^4+x^3-7*x^2+3*x-2;
1+3*x+x^2+3*x^3+x^4
-2+3*x-7*x^2+x^3+x^4
gap>h:=x^4+2*x^3-2*x^2+7*x-2;
-2+7*x-2*x^2+2*x^3+x^4
```

با استفاده از دستور RootsOfUPol(f) ریشه‌های چندجمله‌ای‌ها را می‌یابیم. هم‌چنین با اعمال دستور Factors(f) عوامل تحویل‌ناپذیر آن‌ها را به دست می‌آوریم

```
gap>RootsOfUPol(f); RootsOfUPol(g); RootsOfUPol(h);
[ ]
[2]
[ ]
gap>Factors(f); Factors(g); Factors(h);
[ 1+3*x+x^2+3*x^3+x^4 ]
[ -2+x, 1-x+3*x^2+x^3 ]
[ 2-x+x^2, -1+3*x+x^2 ]
```

مثال ۳.۱۸.۱۶. چندجمله‌ای $f(y) = y^5 + y^2 - y + 1 \in \mathbb{Z}_3[y]$ را تعریف کنید و ریشه‌ها و عوامل تحویل‌ناپذیر آن را روی $\mathbb{Z}_3$ بیابید.

حل با استفاده از دستور $\text{Indeterminate}(GF(3),"y")$ متغیر y را تعریف می‌کنیم. سپس با تعریف $f(x)$ عوامل تحویل‌ناپذیر و ریشه‌های $f(x)$ را می‌یابیم

```
gap>y:=Indeterminate(GF(3),"y");
y
gap>f:=y^5+y^2-y+1;
Z(3)^0-y+y^2+y^5
gap>Factors(f); RootsOfUPol(f);
[ Z(3)^0+y^2, Z(3)^0-y+y^3 ]
[ ]
```

مثال ۴.۱۸.۱۶. چندجمله‌ای‌های $f(z) = z^2 + 2$ و $g(z) = z^3 + 4z^2 + z + 1$ را در $\mathbb{Z}_5[z]$ تعریف کنید و

(الف) $f(z)g(z)$ را بیابید.

(ب) $d(z) = \gcd\{f(z), g(z)\}$ را به دست آورید. به علاوه چندجمله‌ای‌های $p(z)$ و $q(z)$ در $\mathbb{Z}_5[x]$ را طوری بیابید که $d(z) = p(z)f(z) + q(z)g(z)$.

حل ابتدا چندجمله‌ای‌های $f(x)$ و $g(x)$ را تعریف می‌کنیم

```
gap>z:=Indeterminate(GF(5),"z");
z
gap>f:=z^2+2;
Z(5)^0+z^2
gap>g:=z^3+4z^2+z+1;
Z(5)^0+z-z^2+z^3
```

(الف) $f(z)g(z)$ را به صورت زیر می‌یابیم

```
gap>f*g;
Z(5)^0+Z(5)^0*z-z^2+Z(5)^3*z^3-z^9-z^5
```

(ب) با استفاده از دستور Gcd بزرگ‌ترین مقسوم‌علیه مشترک $f(x)$ و $g(x)$ را می‌یابیم و با اعمال دستور $\text{GcdRepresentation}(f,g)$ چندجمله‌ای‌های $p(z)$ و $q(z)$ را می‌یابیم که $\gcd\{f,g\} = pf + qg$

```
gap>Gcd(f,g);
Z(5)^0
gap>GcdRepresentation(f,g);
[ -Z(5)^0+Z(5)^3*z-z^2, Z(5)^3+z ]
```

مثال ۵.۱۸.۱۶. چندجمله‌ای‌های

$$f(w) = w^۲ + ۱$$
$$g(w) = w^۵ + w^۴ + w^۳ + w^۲ + w + ۱$$

را در $\mathbb{Z}_۲[w]$ تعریف کنید. جمع، ضرب، بزرگ‌ترین مقسوم‌علیه مشترک ، عوامل تحویل‌ناپذیر ، و ریشه‌های $f(w)$ و $g(w)$ را بیابید.

حل چندجمله‌ای‌های $f(w)$ و $g(w)$ را تعریف می‌کنیم و همانند مثال‌های پیش عمل می‌کنیم

```
gap>w:=Indeterminate(GF(2),"w");
 w
gap>f:=w^2+1; g:=w^5+w^4+w^3+w^2+w+1;
 Z(2)^0+w^2
 Z(2)^0+w+w^2+w^3+w^4+w^5
gap>Gcd(f,g); GcdRepresentation(f,g);
 Z(2)^0+w
 [ w^2+w^3, Z(2)^0 ]
gap>f*g; f+g;
 Z(2)^0+w+w^6+w^7
 w+w^3+w^4+w^5
gap>Factors(f); Factors(g);
 [ Z(2)^0+w, Z(2)^0+w ]
 [ Z(2)^0+w, Z(2)^0+w+w^2, Z(2)^0+w+w^2 ]
```

تمرین‌ها (با استفاده از GAP)

۱. $f(x) + g(x)$ و $f(x)g(x)$ را در هر حالت محاسبه کنید.

(الف) در $\mathbb{Z}_۵[x]$، $f(x) = ۳ + ۲x + x^۲ + ۴x^۳$، $g(x) = ۱ + x^۲ + x^۳$

(ب) در $\mathbb{Z}_۷[x]$، $f(x) = ۵ + ۲x + x^۲ + x^۳$، $g(x) = ۲ + x + x^۲$

۲. در هر حالت چندجمله‌ای‌های $q(x)$ و $r(x)$ را در $R[x]$ چنان بیابید که $g(x) = q(x)f(x) + r(x)$ که در آن $r(x) = ۰$ یا $\deg r(x) < \deg f(x)$.

(الف) $g(x) = x^۵ + ۲x^۴ + x^۲ + x + ۴$، $f(x) = x^۲ + x + ۲$، $R = \mathbb{Z}_۷$.

(ب) $g(x) = ۳x^۳ + ۲x^۲ - x + ۱$، $f(x) = x^۲ + ۲$، $R = \mathbb{Z}_{۱۱}$.

(ج) $g(x) = ۳x^۳ + ۲x^۲ - x + ۱$، $f(x) = x^۲ + ۲$، $R = \mathbb{Z}_۸$.

(د) $g(x) = x^۵ + ۴x^۴ + x^۳ + ۵x^۲ + x + ۲$، $f(x) = x^۲ + x + ۱$، $R = \mathbb{Z}_۶$.

۳. ریشه‌ها و عوامل تحویل‌ناپذیر $f(x)$ را روی $\mathbb{Q}$، $\mathbb{Z}_۵$، $\mathbb{Z}_۷$، و $\mathbb{Z}_{۱۱}$ را بیابید.

(الف) $f(x) = ۴x^۴ + x^۳ - ۳x^۲ + ۴x - ۳$

(ب) $f(x) = ۴x^۴ + ۴x^۳ + ۳x^۲ - x - ۱$

(ج) $f(x) = x^۴ - x^۳ - x^۲ - x - ۲$

(د) $f(x) = x^۵ - x^۴ + x^۳ - x^۲ + x - ۱$

(هـ) $f(x) = x^۴ - \frac{۵}{۲}x^۳ + \frac{۵}{۲}x^۲ - \frac{۵}{۲}x + \frac{۳}{۲}$

۴. در کدام حالت چندجمله‌ای داده شده تحویل‌ناپذیر است.

(الف) $x^۵ + ۵ \in \mathbb{Z}_۷[x]$ (ب) $x^۲ - ۲ \in \mathbb{R}[x]$ (ج) $x^۲ + ۱۱ \in \mathbb{C}[x]$

(د) $x^۳ - ۴ \in \mathbb{Z}[x]$ (هـ) $x^۳ + x + ۱ \in \mathbb{Z}_۵[x]$ (و) $x^۲ + x + ۱ \in \mathbb{Z}_{۱۱}[x]$.

۵. در هر حالت چندجمله‌ای داده شده را به صورت حاصل‌ضرب چندجمله‌ای‌های تحویل‌ناپذیر در $F[x]$ بنویسید.
(الف) $f(x) = ۳x^۴ + ۲$، $F = \mathbb{Z}_۵$
(ب) $f(x) = ۳x^۲ + ۲$، $F = \mathbb{Z}_{۱۱}$
(ج) $f(x) = x^۳ + ۲x^۲ + ۲x + ۱$، $F = \mathbb{Z}_۷$
(د) $f(x) = x^۴ - x^۲ + x - ۱$، $F = \mathbb{Z}_{۱۷}$
(هـ) $f(x) = x^۵ + x + ۱$، $F = \mathbb{Z}_۲$
(و) $x^۵ + x^۲ - x + ۱$، $F = \mathbb{Z}_۳$

۶. در هر حالت چندجمله‌ای داده شده را به صورت حاصل‌ضرب چندجمله‌ای‌های تحویل‌ناپذیر در $\mathbb{Q}[x]$، $\mathbb{Z}_۵[x]$، و $\mathbb{Z}_۳[x]$ بنویسید.
(الف) $۳x^۲ + ۵x^۲ + x + ۲$.
(ب) $x^۳ + ۹x^۲ + x + ۰$.
(ج) $x^۵ + ۶x^۴ + ۱۲x + ۱۵$.
(د) $۴x^۵ + ۲۸x^۴ - ۲۸x^۲ + ۱۴$.
(هـ) $x^۴ + ۲x - ۱$.
(و) $x^۴ + ۴x + ۱$.
(ز) $x^۴ + m$، که در آن $m = ۴k - ۳$، k عدد صحیح (برای چند k امتحان کنید).
(ح) $x^۴ + ۴x^۳ + ۴x^۲ + ۴x + ۵$.

۷. در هر حالت $f(x)$ را به حاصل‌ضرب چندجمله‌ای‌های تحویل‌ناپذیر روی $\mathbb{Q}[x]$، $\mathbb{Z}_۷[x]$، و $\mathbb{Z}_{۱۱}[x]$ تجزیه کنید.
(الف) $f(x) = x^۴ + ۳x^۳ + x^۲ + ۳x + ۱$.
(ب) $f(x) = x^۴ + x^۳ - ۷x^۲ + ۳x - ۲$.
(ج) $f(x) = x^۴ + ۲x^۳ - ۲x^۲ + ۷x - ۲$.
(د) $f(x) = x^۴ - x^۳ + ۲x^۲ - ۳x + ۲$.
(هـ) $f(x) = x^۵ + x + ۱$.
(و) $f(x) = x^۵ + ۳x + ۱$

۸. در حالت های زیر $d(x) = \gcd\{f(x), g(x)\}$ را بیابید و آن را در $\mathbb{Q}[x]$، $\mathbb{Z}_۳[x]$، و $\mathbb{Z}_۵[x]$ بر حسب ترکیب خطی $f(x)$ و $g(x)$ بنویسید.
(الف) $f(x) = x^۲ + ۲$، $g(x) = x^۳ + ۴x^۲ + x + ۱$
(ب) $f(x) = x^۲ + ۱$، $g(x) = x^۵ + x^۴ + x^۳ + x^۲ + x + ۱$
(ج) $f(x) = x^۲ - x - ۲$، $g(x) = x^۵ - ۴x^۳ - ۲x^۲ + ۷x - ۶$

۱۹.۱۶ مدول‌ها و فضاهای برداری در GAP، آزمایشگاه نوزدهم

در این آزمایشگاه نحوه‌ی تعریف مدول‌ها و همریختی‌های مدولی را بررسی می‌کنیم.

مثال ۱.۱۹.۱۶. ماتریس $m = \begin{bmatrix} ۱ & ۲ & -۳ \\ ۰ & ۲ & ۴ \\ ۱ & ۱ & -۲ \end{bmatrix}$ را تعریف کنید و
(الف) m را به صورت متعارف و با درایه‌های در $\mathrm{GF}(۵)$ نشان دهید.
(ب) در $\mathrm{GF}(۹)$، ماتریس $a^۲m^۲ + am^۳$ را محاسبه کنید، که در آن $a = Z(۹)$ مولد گروه دوری $\mathrm{GF}(۹)^\times$ است.
(ج) صورت پلکانی ماتریس m را با درایه‌های در $\mathbb{Z}$، $\mathrm{GF}(۵)$، و $\mathrm{GF}(۲)$ بیابید.
(د) مرتبه‌ی (ضربی) ماتریس m را روی $\mathbb{Q}$، $\mathrm{GF}(۵)$، و $\mathrm{GF}(۲)$ بیابید.
(هـ) وارون ماتریس m (در صورت وجود) را با درایه‌های در $\mathbb{Q}$، و $\mathrm{GF}(۲)$ بیابید. هم‌چنین وارون ماتریس m (در صورت وجود) به

پیمانه‌های ۳ و ۵ (روی $\mathbb{Z}_3$ و $\mathbb{Z}_5$) بیابید.
(و) چندجمله‌ای می‌نیمال و عوامل تحویل‌ناپذیر آن را روی $\mathbb{Q}$، $GF(5)$، و $GF(2)$ بیابید.

حل (الف) ماتریس m را تعریف می‌کنیم و با استفاده از دستور Display آن‌را با درایه‌های در $GF(5)$ نمایش می‌دهیم

```
gap>m:=[[1,2,-3],[0,2,4],[1,1,-2]];
[ [ 1, 2, -3 ], [ 0, 2, 4 ], [ 1, 1, -2 ] ]
gap>Display(One(GF(5))*m);
 1  2  2
 .  2  4
 1  1  3
```

(ب)

```
gap>Display(m^2*Z(9)^2+m^3*Z(9));
 z = Z(9)
 z^2  z^1  z^7
 z^3  z^6  z^5
  2   2   2
```

(ج) دستور $\mathrm{BaseMat}(m)$ صورت پلکانی ماتریس m را به دست می‌دهد

```
gap>IsMatrix(m);   BaseMat(m);
 true
[ [ 1, 0, 0 ], [ 0, 1, 0 ], [ 0, 0, 1 ] ]
gap>BaseMat(m*Z(5)^0);
[[Z(5)^0,0*Z(5),0*Z(5)],[0*Z(5),Z(5)^0,0*Z(5)],[[0*Z(5),0*Z(5),Z(5)^0]]
gap>BaseMat(m*Z(2)^0);
[[Z(2)^0,0*Z(2),Z(2)^0],[0*Z(2),Z(2)^0,Z(2)^0]]
```

(د)

```
gap>Order(m);
 infinity
gap>Order(m*Z(5)^0);   Order(m*Z(2)^0);
 31
 3
```

(هـ) وارون یک ماتریس m به سادگی و به صورت m^-۱ می‌توان به دست آورد. در صورتی که ماتریس وارون‌پذیر نباشد خروجی دستور fail خواهد بود

```
gap>m^-1;
[ [ -4/3, 1/6, 7/3 ], [ 2/3, 1/6, -2/3 ], [ -1/3, 1/6, 1/3 ] ]
gap>(m*Z(5)^0)^-1;
[[Z(5),Z(5)^0,Z(5)^2],[Z(5)^2, Z(5)^0,Z(5)^0], [Z(5)^3,Z(5)^0,Z(5)]]
gap>(m*Z(2)^0)^-1;
 fail
```

با استفاده از دستور $\mathrm{InverseMatMod}(m,n)$ وارون ماتریس m به پیمانه‌ی n (روی $\mathbb{Z}_n$) به دست می‌آید. در صورتی که ماتریس وارون‌پذیر نباشد خروجی دستور fail خواهد بود

```
gap>InverseMatMod(m,3);
 fail
```

gap>InverseMatMod(m,5);
[[2, 1, 4], [4, 1, 1], [3, 1, 2]]

(و) با استفاده از دستور MinimalPolynomial(K, m) چندجمله‌ای می‌نیمال ماتریس m با درایه‌های در میدان K به دست می‌آید. چندجمله‌ای می‌نیمال m و عوامل تحویل‌ناپذیر آن روی $\mathbb{Q}$ عبارت است از

gap>f:=MinimalPolynomial(Rationals,m); Factors(f);
-6-5*x_1-x_1^2+x_1^3
[-6-5*x_1-x_1^2+x_1^3]

چندجمله‌ای می‌نیمال m و عوامل تحویل‌ناپذیر آن روی GF(۵) عبارت است از

gap>g:=MinimalPolynomial(GF(5),m*Z(5)^0);
-Z(5)^0-x_1^2+x_1^3
gap>Factors(g);
[-Z(5)^0-x_1^2+x_1^3]

چندجمله‌ای می‌نیمال m و عوامل تحویل‌ناپذیر آن روی GF(۲) عبارت است از

gap>h:=MinimalPolynomial(GF(2),m*Z(2)^0);
x_1+x_1^2+x_1^3
gap>Factors(h);
[x_1, Z(2)^0+x_1+x_1^2]

مثال ۲.۱۹.۱۶. فضای برداری V تولید شده توسط بردارهای

$$(۱, ۱, ۱),\ \ (۱, ۰, ۳),\ \ (-۱, ۲, ۱),\ \ (۳, ۴, -۳)$$

روی میدان اعداد گویا را تعریف کنید و
(الف) بعد V و پایه‌ای برای V بیابید. آیا بردار $(۳, ۱, ۲)$ در V قرار دارد.
(ب) ضرایب بردارهای $(۵, ۰, ۱)$ و $(۵, -۳, ۹)$ را نسبت به پایه‌ی پیدا شده در (الف) بیابید.
(ج) زیرفضای W از V را که توسط بردارهای $(۳, ۲, ۱)$ و $(۴, ۳, -۱)$ تولید می‌شود را بیابید. بعد W را تعیین کنید.
(د) فضای خارج‌قسمتی V/W را و همریختی طبیعی $f : V \longrightarrow V/W$، $f(v) = v + W$، را تشکیل دهید. تصویر بردارهای $(۳, ۲, ۱)$ و $(۳, ۰, -۱)$ را تحت f بیابید.

حل با استفاده از دستور VectorSpace(K, lis) فضای برداری V تولید شده توسط بردارهای در lis روی حلقه‌ی تقسیم K حاصل می‌شود

gap>V:=VectorSpace(Rationals,[[1,1,1],[1,0,3],[-1,2,1],[3,4,-3]]);
<vector space over Rationals, with 4 generators>

(الف) دستورهای Dimension(V) و با Basis(V) بعد و پایه‌ی فضای برداری V را می‌یابیم

gap>Dimension(V);
3
gap>b:=Basis(V);
SemiEchelonBasis(<vector space of dimension 3 over Rationals>,
[[1, 1, 1], [0, 1, -2], [0, 0, 1]])
gap>[2,1,3] in V;
true

(ب) دستور Coefficients(B, v) ضرایب بردار v نسبت به پایه‌ی B را به دست می‌دهد

gap>Coefficients(b,[1,0,5]);
[1, -1, 2]

gap>Coefficients(b,[9,3,-5]);
[9, -6, -26]

بنابراین

$$(۱,۰,۵) = (۱,۱,۱) - (۰,۱,-۲) + ۲(۰,۰,۱),$$
$$(۹,۳,-۵) = ۹(۱,۱,۱) - ۶(۰,۱,-۲) - ۲۶(۰,۰,۱).$$

(ج) دستور $\mathrm{Subspace}(V, lis)$ زیرفضای تولید شده در V توسط بردارهای در lis را به دست می‌دهد

gap>W:=Subspace(V,[[1,2,3],[-1,3,4]]);
<vector space over Rationals, with 2 generators>
gap>Dimension(W);
2

(د) فضای خارج‌قسمتی V/W را به راحتی می‌توان به دست آورد. در این حالت GAP یک فضای یکریخت با V/W را به دست می‌آورد

gap>fac:=V/W;
(Rationals^1)

با استفاده از دستور $\mathrm{NaturalHomomorphismBySubspace}(V,W)$ می‌توان همریختی طبیعی $V \longrightarrow V/W$ را به دست آورد

gap>f:=NaturalHomomorphismBySubspace(V,W);
<linear mapping by matrix, VectorSpace(Rationals,
[[1, 1, 1], [1, 0, 3], [-1, 2, 1], [3, 4, -3]]) -> (Rationals^1)>
gap>Image(f,[1,2,3]);
[0]
gap>Image(f,[-1,0,3]);
[-16/3]

مثال ۳.۱۹.۱۶. فضای برداری $V = \mathbb{Q}^۳$، متشکل از ۳ تایی‌های مرتب با درایه‌های در $\mathbb{Q}$ را تشکیل دهید و
(الف) زیرفضای W تولید شده توسط بردارهای $(۲,-۱,۱)$ و $(۱,۰,۱)$ را تعریف کنید.
(ب) آیا تابعی خطی از V به W وجود دارد که بردار $(۱,۰,۰)$ را به $(۲,-۱,۱)$ و $(۰,۱,۰)$ را به $(۱,۰,۱)$ تصویر کند؟
(ج) آیا تابعی خطی از W به V وجود دارد که بردار $(۲,-۱,۱)$ را به $(۱,۰,۱)$ و $(۱,۰,۱)$ را به $(۱,۳,-۱)$ تصویر کند؟
(د) همریختی $\mathbb{Q}$- مدولی (نگاشت خطی) از V به W (در صورت وجود) طوری تعریف کنید که بردار $(۱,۰,۰)$ را به $(۲,-۱,۱)$ و $(۳,۲,۱)$ را به $(۱,۰,۱)$ تصویر کند.
(هـ) همریختی $\mathbb{Q}$- مدولی (نگاشت خطی) از W به V (در صورت وجود) طوری تعریف کنید که بردار $(۲,-۱,۱)$ را به $(۱,۰,۱)$ و $(۱,۰,۱)$ را به $(۱,۳,-۱)$ تصویر کند.

حل با استفاده از دستور $\mathrm{FullRowSpace}(K,n)$ یا nK فضای برداری K^n روی حلقه‌ی تقسیم K به دست می‌آید

gap>V:=FullRowSpace(Rationals,3); V=Rationals^3;
(Rationals^3)
true

(الف) زیرفضای W عبارت است از

gap>W:=SubSpace(Rationals,[[1,-1,2],[1,0,1]]);
<vector space over Rationals, with 2 generators>

(ب) با استفاده از دستور $\mathrm{LeftModuleGeneralMappingByImages}(V,W,s۱,s۲)$ نگاشت کلی از فضای V به فضای W که بردارهای در لیست $s۱$ را به بردارهای در لیست $s۲$، به ترتیب، نظیر کند به دست می‌آید. توجه کنید طول لیست‌ها باید برابر باشند

```
gap>f:=LeftModuleGeneralMappingByImages(V,W,
> [[1,0,0],[0,1,0]], [[1,-1,2],[1,0,1]]);
[ [ 1, 0, 0 ], [ 0, 1, 0 ] ] -> [ [ 1, -1, 2 ], [ 1, 0, 1 ] ]
```

با استفاده از دستور IsMapping(f) تابع تک‌مقداری بودن نگاشت کلی f را تعیین می‌کنیم. ملاحظه کنید f تابع نیست

```
gap>IsMapping(f);
 false
```

(ج)

```
gap>g:=LeftModuleGeneralMappingByImages(W,V,
> [[1,-1,2],[1,0,1]], [[1,0,0],[-1,3,1]]);
[ [ 1, -1, 2 ], [ 1, 0, 1 ] ] -> [ [ 1, 0, 0 ], [ -1, 3, 1 ] ]
gap>IsMapping(g);
 true
gap>Image(g,[2,-1,3]);
 [ 0, 3, 1 ]
```

(د) و (هـ) دستور LeftModuleHomomorphismByImages($V, W, s۱, s۲$) یک همریختی مدولی از فضای V به فضای W که بردارهای در لیست $s۱$ را به بردارهای در لیست $s۲$، به ترتیب، نظیر کند به دست می‌دهد. توجه کنید طول لیست‌ها باید برابر باشند. در حالتی که چنین همریختی وجود نداشته باشد خروجی دستور fail خواهد بود

```
gap>f:=LeftModuleHomomorphismByImages(V,W,
> [[1,0,0],[1,2,3]], [[1,-1,2],[1,0,1]]);
 fail
gap>h:=LeftModuleHomomorphismByImages(W,V,
> [[1,-1,2],[1,0,1]], [[1,0,0],[-1,3,1]]);
[ [ 1, -1, 2 ], [ 1, 0, 1 ] ] -> [ [ 1, 0, 0 ], [ -1, 3, 1 ] ]
gap>IsInjective(h);
 true
gap>IsSurjective(h);
 false
gap>Kernel(h);
 <vector space over Rationals, with 0 generators>
```

تمرین‌ها (با استفاده از GAP)

۱. ماتریس $m = \begin{bmatrix} ۴ & -۵ & ۳ & ۲ \\ ۱ & ۵ & ۶ & -۵ \\ ۰ & ۳ & -۴ & ۰ \end{bmatrix}$ را تعریف کنید و

(الف) m را به صورت متعارف و با درایه‌های در GF(۵) و GF(۷) نشان دهید.

(ب) در GF(۲۷)، ماتریس $a^۲m^۲ + am^۳$ را محاسبه کنید، که در آن $a = Z(۲۷)$ مولد گروه دوری $\mathrm{GF}(۲۷)^\times$ است.

(ج) صورت پلکانی ماتریس m را با درایه‌های در $\mathbb{Z}$، GF(۲۵)، و GF(۹) بیابید.

(د) مرتبه‌ی (ضربی) ماتریس m را روی $\mathbb{Q}$، GF(۷)، و GF(۹) بیابید.

(هـ) وارون ماتریس m (در صورت وجود) را با درایه‌های در $\mathbb{Q}$، و GF(۸) بیابید. هم‌چنین وارون ماتریس m (در صورت وجود) به پیمانه‌های ۴ و ۷ بیابید.

(و) عوامل تحویل‌ناپذیر چندجمله‌ای می‌نیمال آن را روی $\mathbb{Q}$، GF(۸) و GF(۲۷) محاسبه کنید.

۲. فرض کنید $V = \mathbb{Q}^۶$ و W زیرفضای تولیدشده توسط بردارهای زیر است:

$$(۱,۱,۰,۰,۱,۰),\quad (-۱,۴,۳,۱,۱,-۱),\quad (۴,-۷,۰,۱,-۱,۰,۱).$$

(الف) پایه و بعد W را بیابید.
(ب) همریختی طبیعی $V \longrightarrow V/W$ را تعریف کنید و تصویر $(۳,-۳,۳,۲,۱,۰)$ و $(۰,-۱,۲,۴,-۱,۶)$ تحت آن را بیابید.
(د) برقراری رابطه $\dim V/W = \dim V - \dim W$ را بررسی کنید.

۳. فرض کنید $V = \mathbb{Z}_۵^۵$ و W زیرفضای تولیدشده توسط بردارهای $(-۳,۴,۱,۱,۳)$، $(۰,۴,۳,۲,۰)$، و $(۱,۳,۰,۱,۰)$ است.
(الف) پایه و بعد W را بیابید.
(ب) همریختی طبیعی $V \longrightarrow V/W$ را تعریف کنید و تصویر $(۴,-۳,۲,۱,۰)$ و $(۲-,۳,۲,-۱,۱)$ تحت آن را بیابید.
(د) برقراری رابطه $\dim V/W = \dim V - \dim W$ را بررسی کنید.

۴. برای زیرفضاهای داده شده از $V = \mathbb{Q}^۵$، $V = \mathbb{Z}_۵^۵$، $V = \mathbb{Z}_۳^۵$ برقراری رابطه‌های

$$\dim V/W = \dim V - \dim W$$

و

$$\dim U + \dim W = \dim(U+W) - \dim(U \cap W)$$

را تحقیق کنید.
(الف) U زیرفضای تولید شده توسط بردارهای $(۰,-۳,۱,۰,۶)$ و $(۱,۴,۱,۰,۳)$؛ و W زیرفضای تولید شده توسط بردارهای $(-۱,۲,۱,۰,۳)$، $(۰,۱,-۲,۴,۳)$، و $(۰,۰,۱,۱,۰)$.
(ب) U زیرفضای تولید شده توسط بردارهای $(۱,۷,۵,۴,۳)$ و $(-۱,۴,۲,-۱)$؛ و W زیرفضای تولید شده توسط بردارهای $(۱,۰,۰,۱,۲)$، $(۰,۳,-۲,۱,۴)$، و $(۱,۰,۰,۱,۱)$.

۲۰.۱۶ میدان‌ها در GAP، آزمایشگاه بیستم

در GAP می‌توان میدان‌های متناهی، میدان‌های دایره‌بر، که از الحاق ریشه‌های واحد به $\mathbb{Q}$ حاصل‌ضرب می‌شوند، و زیر میدان‌های میدان‌های دایره‌بر را پردازش کرد. بنابراین مثلاً $\mathbb{Q}(\sqrt{۵})$ را که زیرمیدان میدان دایره‌بر $\mathbb{Q}(e^{\frac{۲\pi i}{۵}})$ است را می‌توان به دست آورد. این میدانها را به خاطر اختصار میدان‌های عددی گوییم. فعلاً در GAP نمی‌توان میدان‌های جبری دلخواه را به دست آورد. در واقع، فعلاً، توسیع‌های جبر در GAP را می‌توان تعریف کرد که گروه گالوای آن‌ها آبلی است.

مثال ۱.۲۰.۱۶. میدان ۱۶ عضوی، به نام $K = \mathrm{GF}(۱۶)$ را تعریف کنید و
(الف) عضو همانی و صفر K، و هم‌چنین مشخصه‌ی K را بیابید.
(ب) زیرمیدان‌های K را به دست آورید.
(ج) درجه‌ی K را روی زیرمیدان اولش، $\mathbb{Z}_۲ = \mathrm{GF}(۲)$، بیابید. پایه‌ای برای K روی $\mathrm{GF}(۲)$ به دست آورید.
(د) درجه‌ی K را روی زیرمیدان $L = \mathrm{GF}(۴)$، و پایه‌ای برای K روی $\mathrm{GF}(۴)$ بیابید.
(هـ) گروه گالوای توسیع $L : K$ را بیابید.

حل با استفاده از دستور GF(۱۶) میدان ۱۶ عضوی K را تعریف می‌کنیم

```
gap>K:=GF(16);
GF(2^4)
```

(الف) با دستورهای One(K) و Zero(K) به عضو همانی و صفر K دسترسی پیدا می‌کنیم. در نهایت مشخصه‌ی K را با استفاده از دستور $\mathrm{Characteristic}(K)$ می‌یابیم

```
gap>One(K);  Zero(K);
Z(2)^0
```

```
0*Z(2)
gap>Characteristic(K);
2
```

(ب) دستور $\mathrm{Subfields}(K)$ همه زیرمیدان‌های میدان K را به دست می‌دهد

```
gap>Subfields(K);
[ GF(2), GF(2^2), GF(2^4) ]
```

(ج) در GAP به صورت پیش‌فرض هر میدان به عنوان توسیعی از زیرمیدان اولش در نظر گرفته می‌شود. با استفاده از دستور $\mathrm{LeftActingDomain}(K)$ می‌توان دریافت که میدان K توسیعی از چه میدانی است. با استفاده از دستور $\mathrm{Dimension}(K)$ بُعد فضای برداری K روی میدانی که با $\mathrm{LeftActingDomain}(K)$ مشخص شده به دست می‌آید (درجه‌ی توسیع). دستور $\mathrm{Basis}(K)$ پایه فضای برداری K را به دست می‌دهد

```
gap>LeftActingDomain(K);
GF(2)
gap>Dimension(K);
4
gap>b:=Basis(K);  Elements(b);
CanonicalBasis( GF(2^4) )
[ Z(2)^0, Z(2^4), Z(2^4)^2, Z(2^4)^3 ]
```

(د) با استفاده از دستور $\mathrm{AsField}(L,K)$ می‌توان K را به عنوان توسیعی از L در نظر گرفت. پس از این کار استفاده از دستورات $\mathrm{Dimension}(K)$ و $\mathrm{Basis}(K)$ منجر به یافتن بُعد و پایه برای فضای برداری K روی L خواهد شد

```
gap>K:=AsField(GF(4),K);
AsField( GF(2^2), GF(2^4) )
gap>LeftActingDomain(K);
GF(2^2)
gap>Dimension(K);
2
gap>b:=Basis(K);  Elements(b);
CanonicalBasis( AsField( GF(2^2), GF(2^4) ) )
[ Z(2)^0, Z(2^4) ]
```

(هـ) با استفاده از دستور $\mathrm{GaloisGroup}(K)$ گروه گالوای توسیع $L : K$ حاصل می‌شود که در آن L میدانی است که با $\mathrm{LeftActingDomain}(K)$ مشخص شده

```
gap>G:=GaloisGroup(K);  Size(G);
<group with 1 generators>
2
```

مثال ۲.۲۰.۱۶. میدان $۵^۶$ عضوی، به نام $F=\mathrm{GF}(۵^۶)$ را تعریف کنید و
(الف) گروه گالوای توسیع $F : \mathrm{GF}(۵)$ را بیابید. آیا این گروه آبلی است؟ آیا دوری است؟ مولدهای آن را بیابید.
(ب) اگر a مولد گروه دوری (ضربی) $\mathrm{GF}(۵)^\times$ باشد، چندجمله‌ای می‌نیمال a، $a^۳$، $a^۲+۱$، $a^۲+۲a$ را بیابید.
(ج) اگر b مولد گروه ضربی $\mathrm{GF}(۵^۲)^\times$ و c مولد گروه ضربی $\mathrm{GF}(۵^۳)^\times$ باشند، چندجمله‌ای می‌نیمال $b^۲+۲b$ و $c^۲+۲b$ را بیابید.

حل (الف) با استفاده از دستور $\mathrm{GF}(۱۶)$ میدان ۱۶ عضوی K را تعریف می‌کنیم

```
gap>F:=GF(5^6);;
gap>H:=GaloisGroup(F);
```

<group with 1 generators>
gap>Size(H);
6
gap>IsAbelian(H);
true
gap>IsCyclic(H);
true
gap>GeneratorsOfGroup(H);
[FrobeniusAutomorphism(GF(5^6))]

(ب) در GAP مولد گروه ضربی $\mathrm{GF}(p^n)^\times$ با $Z(p^n)$ نشان داده می‌شود. با استفاده از $\mathrm{MinimalPolynomial}(F,a)$ چندجمله‌ای می‌نیمال $a \in F$ روی زیرمیدان L از F حاصل می‌شود (زیر میدان L که با $\mathrm{LeftActingDomain}(F)$ مشخص شده است)

gap>MinimalPolynomial(F,Z(5));
Z(5)^3+z
gap>MinimalPolynomial(F,Z(5)^3);
Z(5)+z
gap>MinimalPolynomial(F,Z(5)^2+1);
z
gap>MinimalPolynomial(F,Z(5)^2+2*Z(5));
Z(5)+z

(ج)

gap>MinimalPolynomial(F,Z(5)^2+2*Z(25));
Z(5^2)^9+z
gap>MinimalPolynomial(F,Z(5^3)^2+2*Z(25));
Z(5^6)^2962+z

مثال ۳.۲۰.۱۶. با استفاده از دستور NumberField، یا NF، می‌توان میدان‌های عددی (زیرمیدان‌های میدان دایره‌بر) را به‌دست آورد. در واقع دستور $\mathrm{NumberField}(n,lis)$ یا $\mathrm{NF}(n,lis)$ میدان ثابت گروه ضربی تولید شده توسط مانده‌های اول موجود در لیست lis را در میدان دایره‌بر $\mathbb{Q}(e^{\frac{۲\pi i}{n}})$ به دست می‌دهد. (نامانده‌های اول عدد m عبارت‌اند از اعدادی که بین ۱ تا $m-1$ واقع‌اند و نسبت به m اول هستند.) برای تشریح مطلب فرض کنید lis=[۲] و $n=۵$. در گروه ضربی $\mathbb{Z}_۵^\times$ گروه تولید شده توسط ۲ عبارت است از $\{۱,۲,۴\}$. سه خودریختی $\alpha_۱$، $\alpha_۲$، و $\alpha_۴$ از $\mathbb{Q}(e^{\frac{۲\pi i}{n}})$ وجود دارند که $\alpha_i(w)=w^i$، $i=۱,۲,۴$. در این صورت خروجی دستور $\mathrm{NF}(۵,[۲])$ عبارت است از

$$\{a \in \mathbb{Q}(e^{\frac{۲\pi i}{۵}}) \mid \alpha_i(a)=a,\ \ i=۱,۲,۴\}.$$

در زیر تعداد i از زیرمیدان‌های $\mathbb{Q}(e^{\frac{۲\pi i}{۵}})$ را با استفاده از دستور NF به دست آورده‌ایم

gap>NF(5,[2,3]);
Rationals
gap>NF(5,[1]);
CF(5)
gap>NF(5,[1,2]);
Rationals
gap>NF(5,[1,2,4]);
Rationals

```
gap>NF(5,[4]);
 NF(5,[1,4])
```

مثال ۴.۲۰.۱۶. اگر $w = e^{\frac{۲\pi i}{n}}$ یک ریشه‌ی اولیه‌ی واحد باشد. میدان دایره‌بر $K = \mathbb{Q}(w)$ را ، که در آن $w = e^{\frac{۲\pi i}{۷}}$ یک ریشه‌ی اولیه‌ی ۷ام واحد است، را تعریف کنید و
(الف) زیرمیدان‌های K را به دست آورید.
(ب) درجه‌ی K را روی زیرمیدان اول $\mathbb{Q}$ Xv، بیابید. پایه‌ای برای K روی $\mathbb{Q}$ به دست آورید.
(ج) گروه گالوای توسیع $K : \mathbb{Q}$ را بیابید. نشان دهید این گروه دوری است و تصویرهای $w^۲$، $\{w, w + w^۳\}$، و پایه K روی $\mathbb{Q}$، را تحت مولد آن بیابید.
(د) چند جمله‌ای می‌نیمال $w + ۱$، $w^۳ + ۱$، $w^۳ + ۲$، و $w + ۳w^۲$ را بیابید.

حل در GAP با استفاده از دستور $\mathrm{CyclotomicField}(n)$ یا به طور معادل $CF(n)$، میدان دایره‌بر $\mathbb{Q}(w)$، که در آن $w = e^{\frac{۲\pi i}{n}}$، ساخته می‌شود

```
gap>K:=CF(7);
 CF(7)
```

(الف) با استفاده از دستور $\mathrm{Subfield}(K)$ زیرمیدان‌های K را می‌یابیم

```
gap>Subfields(K);
 [Rationals, CF(7), NF(7,[ 1, 2, 4 ]), NF(7,[ 1, 6 ]) ]
```

(ب) زیر میدان اول K میدان $\mathbb{Q}$ است. با استفاده از دستورهای KDimension) و با sis بُعد و پایه K روی $\mathbb{Q}$ را می‌یابیم

```
gap>LeftActingDomain(K);
 Rationals
gap>Dimension(K);
 6
gap>b:=Basis(K);   Elements(b);
 CanonicalBasis( CF(7) )
 [ E(7)^6, E(7)^5, E(7)^4, E(7)^3, E(7)^2, E(7) ]
```

(ج) گروه گالوای توسیع $K : \mathbb{Q}$ عبارت است از

```
gap>G:=GaloisGroup(K);
 <group of size 6 with 1 generators>
gap>Size(G);
 6
gap>IsCyclic(G);
 true
```

گروه گالوای توسیع $K : \mathbb{Q}$ یک گروه دوری مرتبه‌ی ۶ است. مولد آن را با استفاده از دستور $\mathrm{GeneratorsOfGroup}(G)$ و تصویر نقاط و مجموعه‌های داده شده را تحت آن می‌یابیم

```
gap>a:=GeneratorsOfGroup(G);
 [ ANFAutomorphism( CF(7), 3 ) ]
```

توجه کنید مولد G عبارت است از خودریختی $\mathrm{ANFAutomorphism}(CF(۷)), ۳)$. فرض کنید F یک میدان عدد i و n کوچک‌ترین عددی باشد که همه‌ی عناصر F در nامین میدان دایره‌بر قرار دارند. n را هادی F نامیده می‌شود و در GAP با دستور استفاده از $\mathrm{Conductor}(F)$ به دست می‌آید. اگر k عددی باشد که نسبت به n اول است دستور $\mathrm{ANFAutomorphism}(F, k)$ خودریختی F را ، که توسیع خطی نگاشتی است که هر ریشه‌ی nام واحد را به توان kام آن ریشه نظیر می‌کند، به دست می‌دهد. برای اطلاعات بیشتر به راهنمای GAP مراجعه کنید.

اکنون تصویرهای مورد نظر را می‌یابیم. توجه کنید در GAP برای نشان دادن $w = e^{\frac{2\pi i}{n}}$ از E(n) استفاده می‌شود

```
gap>Image(a[1],E(7)^2);
 E(7)^6
gap>Image(a[1],[E(7),E(7)+E(7)^3]);
 [ E(7)^3, E(7)^2+E(7)^3 ]
gap>Image(a[1],Basis(K));
 [ E(7)^6, E(7)^5, E(7)^4, E(7)^3, E(7)^2, E(7) ]
```

(د) با استفاده از دستور MinimalPolynomial(K, a) چندجمله‌ای می‌نیمال عضوهای داده شده در K را روی $\mathbb{Q}$ می‌یابیم

```
gap>MinimalPolynomial(K,E(7)+1);
 E(7)^2+E(7)^3+E(7)^4+E(7)^5+ E(7)^6+x
gap>MinimalPolynomial(K,E(7)^3+1);
 E(7)+E(7)^2+E(7)^4+E(7)^5+E(7)^6+x
gap>MinimalPolynomial(K,E(7)^3+2);
 2*E(7)+2*E(7)^2+E(7)^3+2*E(7)^4+ 2*E(7)^5+2*E(7)^6+x
gap>MinimalPolynomial(K,E(7)+3*E(7)^2);
 -E(7)-3*E(7)^2+x
```

مثال ۵.۲۰.۱۶. میدان دایره‌بر $K = \mathbb{Q}(e^{\frac{2\pi i}{7}})$ را تعریف کنید و
(الف) درجه‌ی K را روی زیرمیدان $L = NF(7, [1, 2, 4])$، بیابید. بُعد K روی L و پایه‌ای برای K روی L به دست آورید.
(ب) گروه گالوای توسیع $K : L$ را بیابید.

حل مشابه مثالهای قبل عمل می‌کنیم. بررسی جزئیات را به خواننده واگذار می‌کنیم.
(الف)

```
gap>K:=CF(7);;  K1:=AsField(NF(7,[1,2,4]),K);
 AsField( NF(7,[ 1, 2, 4 ]), CF(7) )
gap>LeftActingDomain(K1);
 NF(7,[ 1, 2, 4 ])
gap>Dimension(K1);
 3
gap>b:=Basis(K1);  Elements(b);
 CanonicalBasis( AsField( NF(7,[ 1, 2, 4 ]), CF(7) ) )
 [ -E(7)-E(7)^5, -E(7)^2-E(7)^3, -E(7)^4-E(7)^6 ]
```

(ب)

```
gap>G1:=GaloisGroup(K1);
 <group with 1 generators>
gap>Size(G1);
 3
gap>GeneratorsOfGroup(G1);
 [ ANFAutomorphism( AsField( NF(7,[ 1, 2, 4 ]), CF(7) ), 2 ) ]
```

مثال ۶.۲۰.۱۶. کوچک‌ترین میدان شامل $\sqrt{2}$، یعنی $F = \mathbb{Q}(\sqrt{2})$ را بیابید و
(الف) درجه‌ی توسیع $F : \mathbb{Q}$ را بیابید.

(ب) پایه‌ای برای F روی $\mathbb{Q}$ به دست آورید.
(ج) مولد و همه زیرمیدان‌های F را بیابید.

حل (الف) با استفاده از دستور $\text{Field}((Sqrt(۲))$ کوچک‌ترین میدانی که شامل $\sqrt{۲}$ است را به دست می‌آوریم

```
gap>F:=Field(Sqrt(2));
 NF(8,[ 1, 7 ])
```

(ب) بُعد F روی $\mathbb{Q}$ را می‌یابیم و پایه‌ای برای F روی $\mathbb{Q}$ به دست می‌آوریم

```
gap>LeftActingDomain(F);
 Rationals
gap>Dimension(F);
 2
gap>b:=Basis(F);  Elements(b);
 CanonicalBasis( NF(8,[ 1, 7 ]) )
 [ 1, E(8)-E(8)^3 ]
```

(ج) با استفاده از دستور $\text{GeneratorsOfField}(F)$ مولدهای میدان F را روی زیرمیدانی که با LeftActingDomain مشخص می‌شود به دست می‌آید

```
gap>GeneratorsOfField(F);
 [ E(8)-E(8)^3 ]
```

در این‌جا F روی $\mathbb{Q}$ یک مولد دارد : $a = e^{\frac{۲\pi i}{۸}} - e^{\frac{۶\pi i}{۸}}$. پس $F = \mathbb{Q}(\sqrt{۲}) = \mathbb{Q}(a)$. اکنون با استفاده از دستور $\text{Subfield}(F)$ زیرمیدان‌های F را می‌یابیم

```
gap>Subfields(F);
 [Rationals, NF(8,[ 1, 7 ]) ]
```

مثال ۷.۲۰.۱۶. $K = \mathbb{Q}(\sqrt{۲})$ و $F = \mathbb{Q}(\sqrt{۲} + \sqrt{۳})$ را بیابید و
(الف) درجه‌ی توسیع $K : F$ و پایه‌ای برای F روی K به دست آورید.
(ب) مولد F روی K را بیابید.
(ج) درجه‌ی توسیع $\mathbb{Q} : F$ و پایه‌ای برای F روی $\mathbb{Q}$ به دست آورید.
(د) مولد F روی $\mathbb{Q}$ را بیابید.

حل با استفاده از دستور Field میدان‌های مورد نظر را می‌یابیم

```
gap>F:=Field(Sqrt(2)+Sqrt(3));
 NF(24,[ 1, 23 ])
gap>K:=Field(Sqrt(2));
 NF(8,[ 1, 7 ])
```

(الف) چون در GAP هر میدان به طور پیش‌فرض توسیعی از زیرمیدان اولش در نظر گرفته می‌شود، با دستور $\text{AsFiled}(K, F)$ میدان F را به عنوان توسیعی از K در نظر می‌گیریم

```
gap>LeftActingDomain(F);
 Rationals
gap>LeftActingDomain(K);
 Rationals
gap>F:=AsField(K,F);
 AsField( NF(8,[ 1, 7 ]), NF(24,[ 1, 23 ]) )
```

```
gap>LeftActingDomain(F);
 NF(8,[ 1, 7 ])
```

بُعد و پایه $F : K$ را می‌یابیم

```
gap>Dimension(F);
 2
gap>b:=Basis(F);   Elements(b);
 CanonicalBasis( AsField( NF(8,[ 1, 7 ]), NF(24,[ 1, 23 ]) ) )
 [-1/6*E(24)-1/2*E(24)^8+1/6*E(24)^11-1/6*E(24)^14-
 1/2*E(24)^16+1/6*E(24)^17-1/6*E(24)^19 +1/6*E(24)^22,
 1/6*E(24)-1/2*E(24)^8-1/6*E(24)^11+ 1/6*E(24)^14-
 1/2*E(24)^16-1/6*E(24)^17+1/6*E(24)^19-1/6*E(24)^22 ]
```

(ب) مولد F روی K عبارت است از

```
gap>GeneratorsOfField(F);
 [ E(24)-E(24)^11 ]
```

(ج) با استفاده از دستور $\mathrm{AsFiled}(K, F)$ مجدداً میدان F را به عنوان توسیعی از $\mathbb{Q}$ در نظر می‌گیریم. بُعد و پایه $\mathbb{Q} : F$ را می‌یابیم

```
gap>F:=AsField(Rationals,F);
 NF(24,[ 1, 23 ])
gap>Dimension(F);
 4
gap>b:=Basis(F);   Elements(b);
 CanonicalBasis( NF(24,[ 1, 23 ]) )
 [ -1, E(12)^7-E(12)^11, E(24)^17-E(24)^19, E(24)-E(24)^11 ]
```

(د) مولد F روی $\mathbb{Q}$ عبارت است از

```
gap>GeneratorsOfField(F);
 [ E(24)-E(24)^11 ]
```

مثال ۸.۲۰.۱۶. توسیع تجزیه‌ی چندجمله‌ای‌های زیر را روی $\mathbb{Q}$ بیابید و درجه‌ی آن‌ها را مشخص کنید.
(الف) x^2+x+1 (ب) x^2+x-1 (ج) x^6+x^3+1.

حل ابتدا متغیر x را که بتوان با استفاده از آن چندجمله‌ای‌های با ضرایب گویا تعریف کرد را معرفی می‌کنیم

```
gap>x:=Indeterminate(Rationals,"x");
 x
```

(الف) با استفاده از دستور FieldExtension(K،f) توسیع تجزیه‌ی چندجمله‌ای تحویل‌ناپذیر f روی میدان K حاصل می‌شود

```
gap>F:=FieldExtension(Rationals,x^2+x+1);
 CF(3)
gap>LeftActingDomain(F);
 Rationals
gap>Dimension(F);
 2
```

(ب)

```
gap>K:=FieldExtension(Rationals,x^2+x-1);
 NF(5,[ 1, 4 ])
```

```
gap>LeftActingDomain(K);
 Rationals
gap>Dimension(K);
 2
```

(ج)

```
gap>L:=FieldExtension(Rationals,x^6+x^3+1);
 <field in characteristic 0>
gap>LeftActingDomain(L);
 Rationals
gap>Dimension(L);
 6
```

چون درجه‌ی توسیع تجزیه‌ی چندجمله‌ای $x^۶ + x^۳ + ۱$ برابر ۶ است، باید روی $\mathbb{Q}$ تحویل‌ناپذیر باشد. این مطلب را تحقیق می‌کنیم

```
gap>Factors(x^6+x^3+1);
[ 1+x^3+x^6 ]
```

مثال ۹.۲۰.۱۶. توسیع تجزیه‌ی چندجمله‌ای $f(y) = y^۳ + y^۲ + ۱ \in \mathbb{Z}_۳[x]$ را بیابید و درجه‌ی آن را مشخص کنید.

حل ابتدا متغیر y را که بتوان با استفاده از آن چندجمله‌ای‌های با ضرایب در $\mathrm{GF}(۳)$ تعریف کرد معرفی می‌کنیم

```
gap>y:=Indeterminate(GF(3),"y");
 y
```

اکنون عوامل تحویل‌ناپذیر $f(y)$ را می‌یابیم

```
gap>Factors(Z(3)^0*(y^3+y^2+1));
[ -Z(3)^0+y, -Z(3)^0-y+y^2 ]
```

بنابراین $y - ۱$ و $y^۲ - y - ۱$ عوامل تحویل‌ناپذیر $f(y)$ هستند. چون ریشه‌ی اولین چندجمله‌ای در $\mathrm{GF}(۳)$ قرار دارد توسیع تجزیه‌ی $f(y)$ همان توسیع تجزیه‌ی $y^۲ - y - ۱$ است

```
gap> F:=FieldExtension(GF(3),-Z(3)^0-y+y^2);
 GF(3^2)
gap>b:=Basis(F);   Elements(b);
 CanonicalBasis( GF(3^2) )
 [ Z(3)^0, Z(3^2) ]
```

مثال ۱۰.۲۰.۱۶. اگر a عضو اولیه‌ای از $F = \mathrm{GF}(p^n)$ باشد و F را به عنوان فضای برداری روی $K = \mathrm{GF}(p^m)$ در نظر بگیریم ، آنگاه $\{۱, a, a^۲, \ldots, a^s\}$ پایه‌ای برای F روی K است و هر توان a به صورت ترکیب خطی از اعضای این مجموعه نوشته می‌شود. برنامه‌ای به نام $\mathrm{tabeloffield}(F, K)$ که a^i، $۰ \leq i \leq p^n$، را بر حسب ترکیب خطی اعضای این مجموعه می‌یابد را در زیر آورده‌ایم

```
tabeloffield:=function(F,K)
    local i,b,res,z,s;
     res:=[];
    s:=function(x)
        if x=One(F) then return 1; fi;
        if x=Zero(F) then return 0; fi;
      return x;
    end;;
    F:=AsField(K,F);
```

```
    b:=Basis(F);
    z=PrimitiveRoot(F);
    for i in [0..Size(F)-2] do
        Add(res,[z^i, List(Coefficients(b,z^i),x>s(x))]);
    od;
  return res;
end;;
```

مثلاً جدول نمایش عضو اولیه‌ی $\mathrm{GF}(۱۶)$ را روی $\mathbb{Z}_۲$ می‌یابیم

```
gap>tabeloffield(GF(16),GF(2));
[ [ Z(2)^0, [ 1, 0, 0, 0 ] ], [ Z(2^4), [ 0, 1, 0, 0 ] ],
  [ Z(2^4)^2, [ 0, 0, 1, 0 ] ], [ Z(2^4)^3, [ 0, 0, 0, 1 ] ],
  [ Z(2^4)^4, [ 1, 1, 0, 0 ] ], [ Z(2^2), [ 0, 1, 1, 0 ] ],
  [ Z(2^4)^6, [ 0, 0, 1, 1 ] ], [ Z(2^4)^7, [ 1, 1, 0, 1 ] ],
  [ Z(2^4)^8, [ 1, 0, 1, 0 ] ], [ Z(2^4)^9, [ 0, 1, 0, 1 ] ],
  [ Z(2^2)^2, [ 1, 1, 1, 0 ] ], [ Z(2^4)^11, [ 0, 1, 1, 1 ] ],
  [ Z(2^4)^12, [ 1, 1, 1, 1 ] ], [ Z(2^4)^13, [ 1, 0, 1, 1 ] ],
  [ Z(2^4)^14, [ 1, 0, 0, 1 ] ] ]
```

بنابراین اگر $a = Z(۲^۴)$، آنگاه $a^{۱۱} = a + a^۲ + a^۳$ و $a^{۱۴} = ۱ + a^۳$، ....

مثال ۱۱.۲۰.۱۶. برنامه‌ای بنویسید که مرتبه‌ی یک چندجمله‌ای را روی یک میدان متناهی محاسبه کند. مرتبه‌ی چندجمله‌ای $(x^۳ + x + ۱)^۳(x^۲ + x + ۱)$ را روی $\mathbb{Z}_۲$ بیابید.

حل تابعی به نام $exofpol(f, x, F)$ می‌نویسیم، که چندجمله‌ای f با متغیر x روی میدان F را گرفته و مرتبه‌ی f را محاسبه کند. می‌دانیم که اگر $|F| = q$ و $\deg f(x) = m$، آنگاه مرتبه‌ی f کوچکتر یا مساوی $q^m - ۱$ است؛ از این نکته در نوشتن برنامه استفاده می‌کنیم. $x^e - ۱$ را برای $۱ \le e \le q^m - ۱$ در نظر گرفته و باقی‌مانده تقسیم آن را بر $f(x)$ می‌یابیم؛ اولین e که باقی‌مانده تقسیم ۰ باشد مرتبه‌ی $f(x)$ است

```
expofpol:=function(f,x,F)
    local e,q,m,g; g:=f;
    while EuclideanRemainder(g,x)=Zero(F)*x do
        g:=EuclideanQuotient(g,x);
    od;
    q:=Size(F); m:=DegreeIndeterminate(g,x);
    for e in [1..q^m-1] do
        if EuclideanRemainder(x^e-1,g)=Zero(F)*x then
            return e;
        fi;
    od;
end;;
```

اکنون برنامه را برای چندجمله‌ای داده شده امتحان می‌کنیم

```
gap>x:=Indeterminate(GF(2),"x");;
gap>f:=(x^2+x+1)^3*(x^3+x+1);
Z(2)^0+x^2+x^5+x^6+ x^7+x^8+x^9
```

```
gap>expofpol(f,x,GF(2));
84
```

تمرین‌ها (با استفاده از GAP)

۱. در هر حالت درجه‌ی توسیع داده شده را بیابید.
(الف) $\mathbb{Q}(\sqrt{۲}+\sqrt{۳}):\mathbb{Q}(\sqrt{۲})$ (ب) $\mathbb{Q}(\sqrt{۳},\sqrt{۷}):\mathbb{Q}(\sqrt{۲۱})$
(ج) $\mathbb{Q}(\sqrt{۲}+۳i):\mathbb{Q}(i)$ (د) $\mathbb{Q}(\sqrt[۳]{۲},\sqrt{۳}):\mathbb{Q}(\sqrt{۳})$

۲. در هر یک از حالت زیر توسیع تجزیه‌ی $f(x)\in\mathbb{Q}[x]$ روی $\mathbb{Q}$، $\mathbb{Z}_۳$، $\mathbb{Z}_۵$ را بیابید و درجه‌ی آن را مشخص کنید.
(الف) $f(x)=x^۳+۱$ (ب) $f(x)=x^۶+x^۳+۱$
(ج) $f(x)=x^۴+x^۲+۱$ (د) $f(x)=x^۶+۲x^۳-۳$
(هـ) $f(x)=x^۴-۷x^۲+۱۰$ (و) $f(x)=x^۴-۶x^۲-۷$
(ز) $f(x)=x^۲+x+۱$ (ح) $f(x)=x^۳+x^۲+۱$

۳. چندجمله‌ای‌های دایره‌بر زیر را بیابید
(الف) $\Phi_۸(x)$ (ب) $\Phi_۹(x)$ (ج) $\Phi_۴(x)$

۴. (الف) گروه گالوای چندجمله‌ای $f(x)=x^۲-x+۱$ را روی $\mathbb{Q}$ بیابید.
(ب) نشان دهید گروه گالوای چندجمله‌ای $x^۴-x+۱$ و $x^۲-x+۱$ روی $\mathbb{Q}$ یکریخت‌اند.

۵. فرض کنید $f(x)=x^۳-۴x+۲\in\mathbb{Q}[x]$. نشان دهید گروه گالوای $f(x)$ با $S_۳$ یکریخت است و $\mathbb{Q}(\sqrt{۱۴۸},r):\mathbb{Q}$ توسیع تجزیه‌ی $f(x)$ است (r ریشه‌ی دلخواهی از f است)

۶. نشان دهید گروه گالوای $f(x)=x^۳-۵$ روی $\mathbb{Q}$ با $S_۳$ یکریخت است.

۷. فرض کنید $u\neq ۱$ عدد مختلط و ریشه‌ی چندجمله‌ای $x^۵-۱\in\mathbb{Q}[x]$ است. نشان دهید $\mathrm{Aut}_{\mathbb{Q}}\mathbb{Q}(u)\cong\mathbb{Z}_۴$. زیرمیدان‌های سره $\mathbb{Q}(u)$ را بیابید.

۸. گروه گالوای $x^۴-۲\in\mathbb{Q}[x]$ را بیابید و زیرمیدان‌های سره $F:\mathbb{Q}$ را مشخص کنید، که در آن $F:\mathbb{Q}$ توسیع تجزیه‌ی $x^۴-۲$ است.

۹. گروه گالوای توسیع $\mathbb{Q}(\sqrt[۳]{۵},w)$ را بیابید که در آن $w=\dfrac{-۱+i\sqrt{۳}}{۲}$.

۱۰. گروه گالوای چندجمله‌ای‌های زیر را روی $\mathbb{Q}$ بیابید.
(الف) $(x^۲-۳x+۱)^۲(x^۳-۲)$ (ب) $x^۴+x^۲+۱$

۱۱. همه میدان‌های میانی $\mathbb{Q}(i,\sqrt{۵}):\mathbb{Q}$ را بیابید.

کتاب‌نامه

[1] E. R. Berlekamp, *Algebraic coding theory,* New York: McGraw-Hill, (1968).

[2] H. Enderton, *Elements of set theory,* Academic Press INC, (1977).

[3] J. A. Gallian, *Contemporary abstract algebra,* Houghton Miffilin, (1998).

[4] I. N. Herstein, *Topics in algebra,* 2nd ed. Wiley (1975).

[5] T. W. Hungerford, *Algebra,* 2nd ed. Springer-Veralg (1974).

[6] D. S. Malik, J. M. Mordeson, and M. K. Sem, *Fundementals of abstract algebra,* McGraw-Hill, (1997).

[7] F. J. Macwilliams, and N. J. A. Sloane, *The theory of error correcting codes,* Amesterdam-New York-Oxford: North Holland, (1979).

[8] W. K. Nicholson, *Introduction to abstract algebra,* Wiley, (1999).

[9] R. Lidl, G. Pilz, *Applied abstract algebra,* Springer-Verlag, (1984).

[10] J. H. Van Lint, *Introduction to coding theory,* Springer-Verlag, (1982).

[11] V. Pless, *Introduction to error-correcting codes,* Wiley, (1990).

[12] D. J. S. Robinson, *A course in the theory of groups,* 2nd ed. Springer-Verlag, (1996).

[13] J. S. Rose, *A course on group theory,* Cambridge University Press, (1978).

[14] J. Rotman, *Galios Theory,* Springer-Verlag, (1990).

[15] M. Schörnet et al, *Groups, Algorithms, and Programming,* Lehrsthul D für Mathematik, Reinisch-Westflische Thehnisch Hochschule, 6th ed, (1999).

راهنمایی برای حل برخی از تمرین‌ها

تمرین‌های ۱.۱، مجموعه، صفحه‌ی ۴

۱. $A \cap B = \{y\}$ ، $A - B = \{x, z\}$ ، $B - A = \{w\}$ ، $A \times B = \{(x, y), (x, w), (y, y), (y, w), (z, y), (z, w)\}$ ،
$A \cup B = \{x, y, z, w\}$ ،
$P(A) = \{\emptyset, \{x\}, \{y\}, \{z\}, \{x, y\}, \{x, z\}, \{y, z\}, \{x, y, z\}\}$.

۳. (الف) فرض کنید $A \subseteq B$. اگر $x \in A$، آن‌گاه $x \in B$. پس $x \in A \cap B$. بنابراین $A \subseteq A \cap B$. از طرف دیگر طبق تعریف، $A \cap B \subseteq A$. پس $A \cap B = A$. برعکس اگر $A = A \cap B$، چون $A \cap B \subseteq B$، داریم $A \subseteq B$.

۴. اگر $a \in A$، باید ثابت کنیم $a \in B$. چون $A \subseteq A \cup X = B \cup X$ داریم $a \in B \cup X$. پس $a \in B$ یا $a \in X$. اگر $a \in B$ حکم ثابت است. اگر $a \in X$، آن‌گاه $a \in A \cap X = B \cap X$. بنابراین $a \in B$ و $A \subseteq B$. به همین نحو $B \subseteq A$.

۷. (الف)

$$\begin{aligned}
(a, b) \in A \times (B \cap C) &\iff a \in A, \quad b \in B \cap C \\
&\iff a \in A, \quad b \in B, \quad b \in C \\
&\iff a \in A, \quad b \in B, \quad a \in A, \quad b \in C \\
&\iff (a, b) \in A \times B, \quad (a, b) \in A \times C \\
&\iff (a, b) \in (A \times B) \cap (A \times C).
\end{aligned}$$

تمرین‌های ۲.۱، رابطه، صفحه‌ی ۸

۱. (الف) و (ج) رابطه‌های هم‌ارزی‌اند.

۳. همه‌ی رابطه‌های هم‌ارزی روی A عبارت‌اند از

$$\begin{aligned}
R_۱ &= \{(a, a), (b, b), (c, c)\}, \\
R_۲ &= \{(a, a), (b, b), (c, c), (a, b), (b, a)\} \\
R_۳ &= \{(a, a), (b, b), (c, c), (a, c), (c, a)\}, \\
R_۴ &= \{(a, a), (b, b), (c, c), (b, c), (c, b)\} \\
R_۵ &= \{(a, a), (b, b), (c, c), (a, b), (b, a), (a, c), (c, a), (b, c), (c, b)\}
\end{aligned}$$

۴. همه‌ی افرازهای مجموعه‌ی A عبارت‌اند از

$$
\begin{aligned}
P_۱ &= \{\{۱\},\{۲\},\{۳\},\{۴\}\}, \quad P_۲ = \{\{۱,۲\},\{۳\},\{۴\}\},\\
P_۳ &= \{\{۱\},\{۲\},\{۳,۴\}\}, \quad P_۴ = \{\{۱,۲\},\{۳,۴\}\},\\
P_۵ &= \{\{۱,۳\},\{۲,۴\}\}, \quad P_۶ = \{\{۱,۴\},\{۲,۳\}\},\\
P_۷ &= \{\{۱,۳\},\{۲\},\{۴\}\}, \quad P_۸ = \{\{۱,۴\},\{۲\},\{۳\}\},\\
P_۹ &= \{\{۲,۳\},\{۱\},\{۴\}\}, \quad P_{۱۰} = \{\{۲,۴\},\{۱\},\{۳\}\},\\
P_{۱۱} &= \{\{۱,۲,۳\},\{۴\}\}, \quad P_{۱۲} = \{\{۱,۲,۴\},\{۳\}\},\\
P_{۱۳} &= \{\{۱,۳,۴\},\{۲\}\}, \quad P_{۱۵} = \{\{۲,۳,۴\},\{۱\}\},\\
P_{۱۵} &= \{\{۱,۲,۳,۴\}\}
\end{aligned}
$$

۶. ($\Longleftarrow$) داریم $R_۱ \circ R_۲ = R_۲ \circ R_۱$ زیرا

$$
\begin{aligned}
x(R_۱ \circ R_۲)y &\iff y(R_۱ \circ R_۲)x \quad (\text{چون } R_۱ \circ R_۲ \text{ متقارن است})\\
&\iff \exists z \in A, \quad yR_۲z, \ zR_۱x \quad (\text{طبق تعریف})\\
&\iff \exists z \in A, \quad zR_۲y, \ xR_۱z \quad (\text{چون } R_۲, R_۱ \text{ متقارن‌اند})\\
&\iff x(R_۲ \circ R_۱)y.
\end{aligned}
$$

($\Longrightarrow$) $R_۱ \circ R_۲$ متقارن است، زیرا

$$
\begin{aligned}
x(R_۱ \circ R_۲)y &\implies x(R_۲ \circ R_۱)y \qquad (R_۱ \circ R_۲ = R_۲ \circ R_۱ \text{ چون})\\
&\implies \exists z \in A, \quad xR_۱z, \ zR_۲y\\
&\implies \exists z \in A, \quad zR_۱x, \ yR_۲z\\
&\implies y(R_۱ \circ R_۲)x.
\end{aligned}
$$

تمرین‌های ۳.۱، مجموعه‌های جزئاً مرتب، صفحه‌ی ۱۱

۳. اگر a و b دو عضو متمایز و ناصفر $\mathbb{R}$ باشند، آنگاه چون $a = b(b^{-۱}a)$ و $b = a(a^{-۱}b)$، طبق تعریف $\leq$، داریم $a \leq b$ و $b \leq a$. اما $a \neq b$. بنابراین $\leq$ روی $\mathbb{R}$ پاد متقارن نیست.

۴. بله. چون رابطه‌های $\leq_۱$ و $\leq_۲$ بازتابی هستند، به ازای هر $a \in A$، داریم $(a,a) \in \leq_۱$، $(a,a) \in \leq_۲$. بنابراین $(a,a) \in \leq_۱ \cap \leq_۲$ و $\leq_۲ \cap \leq_۱$ بازتابی هستند. اگر $(a,b),(b,a) \in \leq_۱ \cap \leq_۲$، آنگاه $(a,b),(b,a) \in \leq_۱$ و $(a,b),(b,a) \in \leq_۲$. چون $\leq_۱$ و $\leq_۲$ پاد متقارن هستند ، $a = b$. بنابراین $\leq_۲ \cap \leq_۱$ پاد متقارن است. در نهایت اگر $(a,b),(b,c) \in \leq_۱ \cap \leq_۲$، آنگاه $(a,b),(b,c) \in \leq_۱$ و $(a,b),(b,c) \in \leq_۲$. چون $\leq_۱$ و $\leq_۲$ ترایا هستند ، داریم $(a,c) \in \leq_۱$ و $(a,c) \in \leq_۲$. پس $(a,c) \in \leq_۱ \cap \leq_۲$ و $\leq_۲ \cap \leq_۱$ ترایا است.

تمرین‌های ۴.۱، استقرا، صفحه‌ی ۱۳

۱. (ب) فرض کنید $S(n)$ گزاره‌ی زیر باشد :

$$
S(n): \quad ۱^۲ + ۲^۲ + \cdots + n^۲ = \frac{n(n+۱)(۲n+۱)}{۶}, \qquad n \geq ۱.
$$

به وضوح $S(۱)$ درست است. فرض کنید $n \in \mathbb{N}$ و $S(n)$ درست باشد، نشان می‌دهیم $S(n+۱)$ درست است. بنا به فرض استقرا داریم

$$\begin{aligned} ۱^۲ + ۲^۲ + \cdots + n^۲ + (n+۱)^۲ &= \frac{n(n+۱)(۲n+۱)}{۶} + (n+۱)^۲ \\ &= \frac{n(n+۱)(۲n+۱) + ۶(n+۱)}{۶} \\ &= \frac{(n+۱)(۲n^۲ + ۷n + ۶)}{۶} \\ &= \frac{(n+۱)(n+۲)(۲n+۳)}{۶} \end{aligned}$$

بنابراین $S(n+۱)$ درست است.

۳. (ج) به استقرا روی n عمل می‌کنیم. به وضوح حکم به ازای $n = ۱$ برقرار است. اکنون فرض کنید حکم برای $n \geq ۱$ برقرار باشد، بنا به فرض استقرا، داریم

$$\begin{aligned} (a+b)^{n+۱} &= (a+b)\sum_{k=۰}^{n} \binom{n}{k} a^{n-k} b^k \\ &= \sum_{k=۰}^{n} \binom{n}{k} a^{n-k+۱} b^k + \sum_{k=۰}^{n} \binom{n}{k} a^{n-k} b^{k+۱} \\ &= a^{n+۱} + \sum_{k=۱}^{n} \binom{n}{k} a^{n-k+۱} b^k + \sum_{k=۰}^{n-۱} \binom{n}{k} a^{n-k} b^{k+۱} + b^{n+۱} \end{aligned}$$

با تبدیل k به $k-۱$ در مجموع دوم و با استفاده از (ب) داریم

$$\begin{aligned} (a+b)^{n+۱} &= a^{n+۱} + \sum_{k=۱}^{n} \binom{n}{k} a^{n-k+۱} b^k + \sum_{k=۱}^{n} \binom{n}{k-۱} a^{n-k+۱} b^k + b^{n+۱} \\ &= a^{n+۱} + \sum_{k=۱}^{n} \left[\binom{n}{k} + \binom{n}{k-۱} \right] a^{n-k+۱} b^k + b^{n+۱} \\ &= \sum_{k=۰}^{n+۱} \binom{n+۱}{k} a^{n+۱-k} b^k. \end{aligned}$$

تمرین‌های ۵.۱، توابع، صفحه‌ی ۲۱

۱. (ب) و (د) خوش تعریف هستند ، (الف) و (ج) خوش تعریف نیستند.

۲. (ج) f یک‌به‌یک نیست، پس معکوس چپ ندارد. f پوشاست و $g(x) = ۲x$ یک معکوس راست برای f است.

(د) f یک‌به‌یک است و $g(x) = \begin{cases} x & \text{زوج } x \\ k & \text{فرد } k = \frac{x-۱}{۲} \\ ۲ & \text{زوج } \frac{x-۱}{۲} \end{cases}$ یک معکوس چپ برای f است. f پوشا نیست، پس معکوس راست ندارد.

۴. به ازای هر $a \in A$، داریم $f(a) = f(a)$، یعنی aRa. پس R بازتابی است. اگر $a, b \in A$ و aRb، آنگاه $f(a) = f(b)$؛ پس bRa، یعنی R متقارن است. درنهایت اگر $a, b, c \in R$ و aRb و bRc، آنگاه $f(a) = f(b)$ و $f(b) = f(c)$. پس $f(a) = f(c)$، یعنی aRc. از این‌رو R ترایا است. بنابراین R رابطه‌ی هم‌ارزی است.

۶. (الف) داریم $f(A\cup B)\subseteq f(A)\cup f(B)$ زیرا

$$\begin{aligned} y\in f(A\cup B) &\implies \exists x\in A\cup B,\ \ y=f(x)\\ &\implies x\in A \text{ یا } x\in B,\ \ y=f(x)\\ &\implies y\in f(A) \text{ یا } y\in f(B)\\ &\implies y\in f(A)\cup f(B). \end{aligned}$$

هم‌چنین داریم $f(A)\cup f(B)\subseteq f(A\cup B)$، زیرا

$$\begin{aligned} y\in f(A)\cup f(B) &\implies y\in f(A) \text{ یا } y\in f(B)\\ &\implies \exists a\in A,\ \ y=f(a) \ \text{ یا } \ \exists b\in B,\ \ y=f(b)\\ &\implies a\in A\cup B,\ \ y=f(a)\\ &\implies y\in f(A\cup B). \end{aligned}$$

(ب) داریم $f(A\cap B)\subseteq f(A)\cap f(B)$، زیرا

$$\begin{aligned} x\in f(A\cap B) &\implies \exists c\in A\cap B,\ \ x=f(c)\\ &\implies c\in A,\ \ c\in B,\ \ x=f(c)\\ &\implies x\in f(A),\ \ x\in f(B)\\ &\implies x\in f(A)\cap f(B) \end{aligned}$$

(ج) داریم $f(A-B)\subseteq f(A)-f(B)$، زیرا

$$\begin{aligned} y\in f(A-B) &\implies \exists a\in A-B,\ \ y=f(a)\\ &\implies a\in A,\ \ a\notin B,\ \ y=f(a)\\ &\implies y\in f(A)-f(B)\ (a\notin B, \text{ چون } f \text{ یک‌به‌یک است}) \end{aligned}$$

۷. ($\Longleftarrow$) داریم $f(A)\cap f(B)\subseteq f(A\cap B)$، زیرا

$$\begin{aligned} y\in f(A)\cap f(B) &\implies y\in f(A),\ \ y\in f(B)\\ &\implies \exists a\in A,\ \ y=f(a),\ \ \exists b\in B,\ \ y=f(b)\\ &\implies y=f(a)=f(b),\ \ a\in A,\ \ b\in B\\ &\implies a=b,\ \ y=f(a) \qquad (f \text{ یک‌به‌یک است})\\ &\implies y\in f(A\cap B). \end{aligned}$$

از طرف دیگر با استفاده از قسمت (ب) تمرین قبل داریم $f(A\cap B)\subseteq f(A)\cap f(B)$. بنابراین $f(A\cap B)=f(A)\cap f(B)$.
($\Longleftarrow$) فرض کنید $f(x_1)=f(x_2)$. قرار می‌دهیم $A=\{x_1\}$ و $B=\{x_2\}$. پس طبق فرض داریم $f(A\cap B)=\{f(x_1)\}$. اگر $x_1\neq x_2$، آنگاه داریم $f(A)\cap f(B)=\{f(x_1)\}\cap\{f(x_2)\}=\{f(x_1)\}$، که تناقض است. در نتیجه $x_1=x_2$.

۹. بنا به فرض توابع یک‌به‌یک $f:A\longrightarrow B$ و $g:B\longrightarrow A$ وجود دارند. قرار می‌دهیم $C_0=A-\operatorname{ran} g$. اگر $C_0=\emptyset$، آنگاه g پوشاست، بنابراین $B\approx A$. فرض کنید $C_0\neq\emptyset$. به طور استقرایی به ازای هر n قرار می‌دهیم $C_{n+1}=g(f(C_n))$. فرض کنید $C=\bigcup_{n=0}^{\infty}C_n$. ادعا می‌کنیم تابع $h:A\longrightarrow B$ با ضابطه‌ی

$$h(a)=\begin{cases} f(a) & a\in C\\ b & g(b)=a,\ \ a\notin C \end{cases}$$

یک‌به‌یک و پوشاست. ابتدا ثابت می‌کنیم h یک‌به‌یک است. فرض کنید $a_۱, a_۲ \in A$ دو عضو متمایز هستند چون f و g یک‌به‌یک هستند تنها باید حالتی را در نظر بگیریم که $a_۱ \in C$ و $a_۲ \notin C$. پس به ازای mای، $a_۱ \in C_m$ و به ازای هر n، $a_۲ \notin C_n$. در این حالت $h(a_۱) = f(a_۱) \in f(C_m)$ و حال آن‌که $h(a_۲) = b \notin f(C_m)$، که در آن $g(b) = a_۲$، زیرا اگر $b \in f(C_m)$ داریم $a_۲ = g(b) \in g(f(C_m)) = C_{m+۱}$. بنابراین $h(a_۱) \neq h(a_۲)$ و h یک‌به‌یک است. حال فرض کنید $b \in B$. اگر به ازای nای $b \in f(C_n)$، آن‌گاه $a \in C_n$ وجود دارد که $b = f(a)$. بنابراین طبق تعریف، $h(a) = f(a) = b$. پس فرض کنید به ازای هر n، $b \notin f(C_n)$. کافی است نشان دهیم به ازای هر n، $g(b) \notin C_n$. در این صورت طبق تعریف h داریم ، $h(g(b)) = b$، که نشان می‌دهد h پوشاست. چون $C_۰ = A - \operatorname{ran} g$، $g(b) \notin C$. هم‌چنین اگر $g(b) = C_{n+۱} = g(f(C_n))$ آن‌گاه $b_۱ \in f(C_n)$ وجود دارد که $g(b) = g(b_۱)$. چون g یک‌به‌یک است $b = b_۱ \in f(C_n)$ که تناقض است.

۱۱. (ج) تابع شمولی $i : \mathbb{Z} \longrightarrow \mathbb{Q}$، $i(x) = x$ یک‌به‌یک است. به علاوه تابع $f : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$ با ضابطه‌ی $f(m, n) = ۲^m(۲n + ۱) - ۱$ یک‌به‌یک و پوشا است. پس $\mathbb{Q} \approx \mathbb{N} \times \mathbb{N} \approx \mathbb{N}$ و بنا به قضیه شرودر- برنشتاین $\mathbb{Q} \approx \mathbb{Z}$.
(و) تابع $f : A \longrightarrow B$ با ضابطه‌ی $f(x) = ۳x + ۶$ یک‌به‌یک و پوشاست.

۱۳. فرض کنید $f : \mathbb{N} \longrightarrow \mathbb{R}$. به ازای هر $n \in \mathbb{N}$، عدد حقیقی $f(n)$ را با بسط اعشاری نامتناهی نشان می‌دهیم. عدد حقیقی $a \in \mathbb{R}$ را چنین می‌سازیم. قسمت صحیح a را برابر صفر می‌گیریم و nامین رقم اعشاری آن را برابر ۵ می‌گیریم اگر n امین رقم اعشاری $f(n)$ برابر ۱ نباشد و برابر صفر می‌گیریم هرگاه n امین رقم اعشاری $f(n)$ برابر ۵ باشد. چون به ازای هر n، a در nامین رقم اعشاری با $f(n)$ متفاوت است. پس $a \notin \operatorname{ran} f$ و f پوشا نیست.

۱۴. فرض کنید $f : X \longrightarrow \mathscr{P}(X)$. قرار می‌دهیم $B = \{x \in X \mid x \notin f(x)\}$. بنابراین $B \subseteq X$. اگر به ازای یک $x \in X$، $f(x) = B$. دو حالت پیش می‌آید: اگر $x \in B$، آن‌گاه طبق تعریف B، $x \notin f(x) = B$ که تناقض است. اگر $x \notin B$ آن‌گاه طبق تعریف B، $x \in f(x) = B$، که مجدداً تناقض است. پس به ازای هر $x \in X$، $f(x) \neq B$. بنابراین f پوشا نیست.

۱۷. (الف) در هر قرص یک عدد گویا انتخاب کنید.
(ب) خیر.

۱۸. مجموع طول فاصله‌ها را محدود کنید.

۱۹. از قضیه‌ی ۱۶.۵.۱ استفاده کنید.

تمرین‌های ۷.۱، جایگشت‌ها، صفحه‌ی ۳۳

۱. $\alpha = (۱\ ۲)(۳\ ۴)$، $\beta = (۱\ ۳)(۲\ ۴\ ۵)$، $\sigma = (۱\ ۳\ ۲\ ۵\ ۴)$.
(الف) $\alpha\beta = (۱\ ۴\ ۵)(۳\ ۲)$ (ب) $\beta\alpha = (۱\ ۴)(۲\ ۳\ ۵)$
(ج) $\alpha\beta\sigma^{-۱} = (۱\ ۵\ ۳\ ۴)$ (د) $\sigma\alpha^۲ = (۱\ ۳\ ۲\ ۵\ ۴)$
(هـ) $\beta\alpha\beta^{-۱} = (۳\ ۴)(۱\ ۵)$ (و) $\beta^۲\sigma^{-۲} = (۱\ ۵\ ۲\ ۳\ ۴)$.

۲. (الف) $(۱\ ۴\ ۸\ ۳\ ۹\ ۲\ ۷\ ۶)$ (ب) $(۱\ ۳\ ۹\ ۷\ ۶)(۲\ ۸\ ۴\ ۵)$
(ج) $(۱۶)(۲\ ۴\ ۹)(۳\ ۸\ ۵)$ (د) $(۱\ ۷\ ۲\ ۳\ ۴\ ۵\ ۶)$

۳.

نوع تجزیه اعضای $S_۶$	تعداد		
$(\times)$	۱	$=$	زوج ۱
$(\times\times)$	$\frac{۶\times۵}{۲}$	$=$	فرد ۱۵
$(\times\times\times)$	$\frac{۶\times۵\times۴}{۳}$	$=$	زوج ۴۰
$(\times\times\times\times)$	$\frac{۶\times۵\times۴\times۳}{۴}$	$=$	فرد ۹۰
$(\times\times\times\times\times)$	$\frac{۶\times۵\times۴\times۳\times۲}{۵}$	$=$	زوج ۱۴۴
$(\times\times\times\times\times\times)$	$\frac{۶!}{۶}$	$=$	فرد ۱۲۰
$(\times\times)(\times\times)$	$\frac{۱}{۲}\left[\frac{۶\times۵}{۲}\times\frac{۴\times۳}{۲}\right]$	$=$	زوج ۴۵
$(\times\times\times)(\times\times)$	$\frac{۶\times۵\times۴}{۳}\times\frac{۳\times۲}{۲}$	$=$	فرد ۱۲۰
$(\times\times\times)(\times\times\times)$	$\frac{۱}{۲}\left[\frac{۶\times۵\times۴}{۳}\times\frac{۳\times۲\times۱}{۳}\right]$	$=$	زوج ۴۰
$(\times\times)(\times\times\times\times)$	$\frac{۶\times۵}{۲}\times\frac{۴\times۳\times۲\times۱}{۴}$	$=$	زوج ۹۰
$(\times\times)(\times\times)(\times\times)$	$\frac{۱}{۳!}\left[\frac{۶\times۵}{۲}\times\frac{۴\times۳}{۲}\times\frac{۲\times۱}{۲}\right]$	$=$	فرد ۱۵
		$=$	۷۲۰

۴. (الف) $(۵\ ۴\ ۳\ ۶\ ۲\ ۱)$، فرد (ب) $(۲\ ۳)(۵\ ۳\ ۶\ ۷\ ۱)$، زوج

۶. چون $|A|=|B|$ داریم $|A-B|=|B-A|$. بنابراین تابع دوسویی ψ از $A-B$ به $B-A$ وجود دارد. جایگشت $\tau\in S_X$ را به صورت زیر تعریف می‌کنیم:

$$\tau(x)=\begin{cases} b_i & x=a_i,\ \ i=۱,۲,\dots,m \\ \psi(x) & x\in B-A \\ x & x\in X-(A\cup B). \end{cases}$$

۷. چون τ یک‌به‌یک است، $(\tau(a_۱)\ \tau(a_۲)\ \cdots\ \tau(a_m))$ یک m-دور است. کافی است ثابت کنیم

$$\tau(a_۱\ a_۲\ \cdots\ a_m)=(\tau(a_۱)\ \tau(a_۲)\ \cdots\ \tau(a_m))\tau.$$

اگر $i=۱,\dots,m-۱$ هر دو طرف رابطه‌ی فوق a_i را به $\tau(a_{i+۱})$ می‌برند. هم‌چنین هر دو طرف a_m را به $\tau(a_۱)$ می‌برند. در نهایت اگر $a\neq a_i$، $i=۱,\dots,m$، هر دو طرف a را به $\tau(a)$ می‌برند. پس دو طرف با هم مساوی‌اند.

۸. (الف) اگر دو دور α و β مزدوج باشند، طبق مساله‌i قبل، طول آن ها یکسان است. برعکس اگر $\alpha=(b_۱,\dots,b_m)$ و $\beta=(a_۱,\dots,a_m)$، آنگاه α و β مزدوج‌اند، زیرا اگر جایگشت τ را با $\tau(a_i)=b_i$ تعریف کنیم (مساله‌ی ۶ را ببینید)، طبق مساله‌ی قبل داریم

$$\tau\beta\tau^{-۱}=(\tau(a_۱)\cdots\tau(a_m))=(b_۱\cdots b_m)=\alpha,$$

تمرین‌های ۱.۲، تجزیه در اعداد صحیح، صفحه‌ی ۴۱

۹. (الف) $۶=۳m-۵n$ (ب) $۱=۱۱m-۱۸n$ (ج) $۳=m-۶n$
(د) $۱=۱۱m-۱۲۴n$ (هـ) $۳=-۱۳m-۲n$ (و) $۱۱=-۱۷m-۷n$

۱۲. (الف) $\gcd\{۷۳۵, ۱۱۰\} = ۵$، $\operatorname{lcm}\{۷۳۵, ۱۱۰\} = ۱۶۱۷۶$
(ب) $\gcd\{۱۱۳, ۱۰۱\} = ۱$، $\operatorname{lcm}\{۱۱۳, ۱۰۱\} = ۱۱۴۱۳$
(ج) $\gcd\{۲۷۸, ۱۳۹\} = ۱۳۹$، $\operatorname{lcm}\{۲۷۸, ۱۳۹\} = ۲۷۸$

۱۳. از قضیه‌ی اساسی حساب استفاده کنید.

۱۴. اگر $x, y \geq ۰$ اعداد صحیح باشند که $۰ \leq c \leq x + y$، نشان دهید دهید c را می‌توان به صورت $c = x_۱ + y_۱$ نوشت که در آن $۰ \leq x_۱ \leq x$ و $۰ \leq y_۱ \leq y$. سپس از قضیه‌ی ۱۶.۱.۲ استفاده کنید.

۱۶. اگر $m^۲ | n^۲$ با استفاده از قضیه‌ی اساسی حساب، نشان دهید $m|n$.

۱۸. d را با استفاده از الگوریتم اقلیدس بیابید و از (الف) استفاده کنید.

تمرین‌های ۲.۲، اعداد صحیح به پیمانه‌ی n، $\mathbb{Z}_n$، صفحه‌ی ۴۶

۲. (الف) ۵ (ب) ۰۲ (ج) ۹ (د) ۵

۵. (الف) $x = \bar{۳۳}$ (ب) $x = \bar{۱۶}$ (ج) $x = \bar{۱۶}$ (د) $x = \bar{۱۴}$

۸. (الف) $x = \bar{۲}$، $y = \bar{۴}$ (ب) $x = \bar{۸}$، $y = \bar{۵}$ (ج) جواب ندارد
(د) جواب ندارد (هـ) $x = \bar{۲}$، $y = \bar{۰}$ (و) $x = \bar{۱}$، $y = \bar{۶}$

۹. (الف) $x = \bar{۳}, \bar{۶}$ (ب) $x = \bar{۲}, \bar{۴}$ (ج) $x = \bar{۲}, \bar{۴}$ (د) $x = \bar{۴}, \bar{۸}$

۱۰. با استفاده از قضیه‌ی فرما نشان دهید تابع $f : \mathbb{Z}_p \longrightarrow \mathbb{Z}_p$، با ضابطه‌ی $f(\bar{a}) = \bar{a}^{p-۲}$ یک‌به‌یک است.

۱۱. (ب) با توجه (الف) می‌توانیم فرض کنیم $p \geq ۳$. بنا به قضیه‌ی فرما به ازای هر $\bar{a} \in \mathbb{Z}_p$، $a^{-p} = \bar{a}$. پس به ازای هر $\bar{a} \neq \bar{۰} \in \mathbb{Z}_p$ داریم $a^{-p-۱} = \bar{۱}$. از این‌رو $\bar{۱}$، $\bar{۲}$، ...، $\overline{p-۱}$ همگی در معادله‌ی $x^{p-۱} = \bar{۱}$ در $\mathbb{Z}_p$ صدق می‌کنند. بنابراین $(x - \bar{۱})(x - \bar{۲}) \cdots (x - \overline{(p-۱)}) = x^{p-۱} - \bar{۱}$. با فرض $x = \bar{۰}$ داریم $(\overline{-۱})(\overline{-۲}) \cdots (\overline{-p-۱}) = (-\bar{۱})^{p-۱}(\overline{p-۱})! = -\bar{۱}$ و $(\overline{p-۱})! \equiv -۱ \mod p$. چون p فرد است داریم $-\bar{۱}$.

۱۲. (الف) چون $p - ۱ = ۴n$ تعداد جملات حاصل‌ضرب

$$x = \frac{p-۱}{۲}! = ۱ \times ۲ \times \cdots \times \frac{p-۱}{۲}$$

زوج است، پس $x = (-۱) \times (-۲) \times \cdots \times \left(-\frac{p-۱}{۲}\right)$. اما چون در $\mathbb{Z}_p$ داریم $p - k \equiv -k$ می‌توان نوشت $x \equiv (p-۱)(p-۲) \cdots \left(\frac{p+۱}{۲}\right)$. در نتیجه

$$x^۲ \equiv \left(\frac{p-۱}{۲}\right)! \frac{p+۱}{۲} \cdots (p-۲)(p-۱) \equiv (p-۱)!$$

که با استفاده از قضیه‌ی ویلسون حکم ثابت است.

تمرین‌های ۱.۳، خواص مقدماتی گروه‌ها، صفحه‌ی ۵۷

۱. داریم

$$\begin{aligned} aa^{-۱} &= a\left(ea^{-۱}\right) && (ea^{-۱} = a^{-۱} \text{ چون}) \\ &= a\left(a^{-۱}a\right)a^{-۱} && (a^{-۱}a = e \text{ چون}) \\ &= \left(aa^{-۱}\right)\left(aa^{-۱}\right). \end{aligned}$$

چون aa^{-1} وارون چپ $(aa^{-1})^{-1}$ دارد. با ضرب آن در طرفین تساوی فوق داریم $e = aa^{-1}$. بنابراین a^{-1} وارون راست a نیز هست. از طرف دیگر

$$ae = a\left(a^{-1}a\right) = \left(aa^{-1}\right)a = ea = a.$$

پس e همانی راست نیز هست.

۲. مجموعه‌ی اعداد گویا، $\mathbb{Q}$، را با عمل $a * b = |a|b$ $(a, b \in \mathbb{Q})$ در نظر بگیرید.

۳. فرض کنید $b \in G$ عضو ثابتی باشد ؛ ثابت می‌کنیم e_b عضو بی‌اثر G است. برای هر $a \in G$ داریم $ab = (ae_a)b$ و $ab = a(e_b b)$. پس $ae_b b = ae_a b$ و بنا به قانون حذف، $e_b = e_a$. از این‌رو e_b عضو بی‌اثر G است.

۴. فرض کنید G نیم‌گروه متناهی باشد که قوانین حذف در آن برقرار است. فرض کنید $a \in G$ عضو دلخواهی باشد. مجموعه‌ی $Ga = \{ga \mid g \in G\}$ را در نظر بگیرید. ثابت کنید $|Ga| = |G|$ و $Ga = G$. چون $a \in G = Ga$، $e_a \in G$ وجود دارد که $e_a a = a$. بنابراین $ae_a a = aa$ و طبق قانون حذف از راست، داریم $ae_a = a$. پس G عضو همانی e دارد. اکنون با استفاده از $e \in G = Ga$ و قانون حذف از راست ، عضو $b \in G$ را بیابید که $e = ab = ba$.

۷.

$$\begin{aligned} xy = yx &\iff (yx)^{-1}xy = (yx)^{-1}yx \\ &\iff x^{-1}y^{-1}xy = 1 \\ &\iff x\left(x^{-1}y^{-1}xy\right) = x^{-1} \\ &\iff y^{-1}xy = x^{-1} \end{aligned}$$

۸. برای $n \in \mathbb{N}$ به استقرا روی n عمل می‌کنیم. به وضوح حکم برای $n = 1$ برقرار است. فرض کنید مساله برای n درست باشد و حالت $n + 1$ را در نظر می‌گیریم

$$\begin{aligned} (ab)^{n+1} &= (ab)(ab)^n \\ &= aba^n b^n && \text{(فرض استقرا)} \\ &= aa^n bb^n && (ab = ba) \\ &= a^{n+1}b^{n+1}. \end{aligned}$$

برای $n = 0$ نیز مساله درست زیرا $(ab)^0 = 1 = a^0 b^0$. مساله برای اعداد صحیح منفی نیز درست است، زیرا اگر $n \in \mathbb{N}$ داریم

$$\begin{aligned} (ab)^{-n} &= \left(ab^{-1}\right)^n \\ &= \left(b^{-1}a^{-1}\right)^n \\ &= \left(a^{-1}b^{-1}\right)^n && (ab = ba) \\ &= \left(a^{-1}\right)^n \left(b^{-1}\right)^n && (n > 0) \\ &= a^{-n}b^{-n}. \end{aligned}$$

۹. (الف) برای حالت $n > 0$ مساله را به استقرا روی n حل می‌کنیم. حالت $n = 1$ واضح است. فرض کنید مساله برای n درست باشد و حالت $n + 1$ را در نظر می‌گیریم

$$\begin{aligned} a^m a^{n+1} &= a^m(a^n a) \\ &= (a^m a^n)a \\ &= a^{m+n}a && \text{(فرض استقرا)} \\ &= a^{m+n+1} && \text{(طبق تعریف)} \end{aligned}$$

بنابراین مساله برای هر $n > ۰$ درست است. برای $n = ۰$ نیز داریم $a^m a^۰ = a^m ۱ = a^{m+۰}$ و مساله در این حالت نیز برقرار است. مشابه استدلال فوق برای هر $m > ۰$ نیز داریم $a^m a^n = a^{m+n}$. حال اگر $m, n \in \mathbb{N}$

$$\begin{aligned} a^{-m}a^{-n} &= \left(a^{-۱}\right)^m \left(a^{-۱}\right)^n \\ &= \left(a^{-۱}\right)^{m+n} && \text{طبق مراحل قبل} \\ &= a^{-(m+n)}. \end{aligned}$$

پس مساله برای هر m و n درست است.

(ب) برای $n > ۰$ به استقرا روی n عمل می‌کنیم. برای $n = ۱$ حکم واضح است. حال اگر مساله برای n درست باشد، داریم

$$\begin{aligned} (a^m)^{n+۱} &= (a^m)^n a^m && \text{(طبق تعریف)} \\ &= a^{mn}a^m && \text{(فرض استقرا)} \\ &= a^{mn+m} && \text{(قسمت الف)} \\ &= a^{m(n+۱)}. \end{aligned}$$

پس مساله برای هر $n > ۰$ درست است. برای $n = ۰$ نیز درست، زیرا $(a^m)^۰ = ۱ = a^{m۰}$. حال اگر $n \in \mathbb{N}$ داریم

$$\begin{aligned} (a^m)^{-n} &= \left[(a^m)^{-۱}\right]^n = \left(a^{-m}\right)^n \\ &= a^{(-m)n} && \text{(مرحله‌ی قبل)} \\ &= a^{m(-n)}. \end{aligned}$$

بنابراین مساله برای هر $n \in \mathbb{Z}$ درست است.

۱۰. (الف) به استقرا روی n عمل می‌کنیم. برای $n = ۱$ مساله واضح است. حال اگر مساله برای n درست باشد برای $n + ۱$ نیز درست است:

$$\begin{aligned} \left(a^{-۱}ba\right)^{n+۱} &= \left(a^{-۱}ba\right)^n \left(a^{-۱}ba\right) \\ &= \left(a^{-۱}b^n a\right) \left(a^{-۱}ba\right) && \text{(فرض استقرا)} \\ &= a^{-۱}b^n aa^{-۱}ba \\ &= a^{-۱}b^n ۱ba \\ &= a^{-۱}b^{n+۱}a \end{aligned}$$

(ب) برای $n = ۱$ مساله واضح است. اگر مساله برای n درست باشد داریم

$$\begin{aligned} a^{-(n+۱)}ba^{n+۱} &= a^{-n}(a^{-۱}ba)a^n \\ &= a^{-n}b^r a^n && \text{(طبق فرض)} \\ &= \left(a^{-n}ba^n\right)^r && \text{(طبق الف)} \\ &= \left(b^{r^n}\right)^r && \text{(فرض استقرا)} \\ &= b^{r^{n+۱}} \end{aligned}$$

و مساله برای هر $n > ۰$ درست است.

۱۱. فرض کنید $a, b \in G$. داریم $(ab)^۲ = e$ و $a^۲ = e$ و $b^۲ = e$. بنابراین $a^۲b^۲ = (ab)^۲$. پس $a^۲b^۲ = abab$ و طبق قانون حذف $ab = ba$.

۱۲. اگر $g \in G$، نشان دهید $i, j \in \mathbb{N}$ وجود دارند که $i < j$ و $g^i = g^j$. نتیجه بگیرید برای هر $g \in G$ عدد طبیعی n_g وجود دارد که $g^{n_g} = ۱$. m را کوچک‌ترین مضرب مشترک n_gها بگیرید و نشان دهید به ازای هر $a \in G$، $a^m = ۱$.

۱۶. اگر $n > m$، نشان دهید به ازای هر $k \geq ۰$ و $j \geq m$، $a^{j+k(n-m)} = a^j$. نتیجه بگیرید $a^{m(n-m)}$ خودتوان است.

۱۷. a، $a^۲$، $a^۳$، ... را در نظر بگیرید.

۲۱. با قرار دادن $b = a^{-۲}ba^۳$ در رابطه‌ی $a^{-۱}b^۲a = b^۳$ نتیجه بگیرید $(ba)^۲ = (ab)^۳$. به طریق مشابه نشان دهید $(ab)^۲ = (ba)^۳$. از دو رابطه‌ی اخیر نتیجه بگیرید $a^۲ = b^{-۲}$. در نهایت با استفاده از این رابطه و رابطه‌ی $a^{-۱}b^۲a = b^۳$ نشان دهید $b^۲ = b^۳$ و $b = ۱$. به همین نحو $a = ۱$.

۲۴. ($\Longleftarrow$) فرض کنید S گروه باشد. اگر $a \in S$، آنگاه چون $aa^{-۱}a = a$، $b = a^{-۱}$ وجود دارد که $aba = a$. حال اگر $c \in S$ نیز وجود داشته باشد که $aca = a$. بنابراین $aba = aca$ و بنا به قانون حذف $b = c$. پس b یکتا است.

($\Longrightarrow$) فرض کنید $a \in S$. طبق فرض عضو یکتای $b \in S$ وجود دارد که $aba = a$. پس $abab = ab$ و $(ab)^۲ = ab$. پس S یک عضو خودتوان دارد. چون یک گروه تنها یک عضو خودتوان دارد، ابتدا نشان می‌دهیم S تنها یک عضو خودتوان دارد. فرض کنید c و d اعضای خودتوان در S باشند. چون $cd \in S$ پس عضو یکتای $g \in S$ وجود دارد که $cdgcd = cd$ اکنون داریم $(cd)(gc)(cd) = cdgc^۲d = cdgcd$. چون g یکتاست، $gc = g$. به طریق مشابه $(cd)(dg)(cd) = cd^۲gcd = cdgcd$. چون g یکتاست، $dg = g$. هم‌چنین چون $(cd)(gcdg)(cd) = (cdgcd)gcd = cdgcd$، مجدداً بنا به یکتایی g، $gcdg = g$. در نتیجه $g = g^۲ = gg = (gc)(dg) = g(cd)g = g$. پس g نیز خودتوان است. اکنون $ggg = g$، $g(cd)g = g$ و بنا به یکتایی $g = cd$. بنابراین cd خودتوان است. حال $(cd)d(cd) = cd^۲cd = cdcd = cd$ و $(cd)c(cd) = cdc^۲d = cdcd = cd$. بنابراین بنا به یکتایی $c = d$. پس S تنها یک عضو خودتوان دارد.

فرض کنید $e \in S$ عضو خودتوان یکتای S باشد. اگر $a \in S$ عضو یکتای $b \in S$ وجود دارد که $aba = b$ که از آن نتیجه می‌شود $(ab)^۲ = ab$. بنابراین $ab = e$، به علاوه چون $aba = a$ داریم $(ba)^۲ = ba$ و ba خودتوان است. پس $ba = e$. اکنون $aba = a$ و $ab = e = ba$ نتیجه می‌دهد $ea = a = ae$ و e عضو بی‌اثر است. چون $ab = e = ba$، b وارون a است. پس S گروه است.

تمرین‌های ۲.۳، مرتبه، گروه‌های دوری، صفحه‌ی ۶۱

۱. $O(\pm i) = O(\pm j) = O(\pm k) = ۴, \quad O(-۱) = ۲$.

۲. مولدهای $C_{۱۲}$ عبارت‌اند از $w = e^{\frac{۲\pi i}{۱۲}}$، $w^۵$، $w^۷$، $w^{۱۱}$. هم‌چنین $O(w^۲) = ۶$، $O(w^۳) = ۴$، $O(w^۴) = ۳$، $O(w^۶) = ۲$، $O(w^۸) = ۳$، $O(w^۹) = ۴$، $O(w^{۱۰}) = ۶$، $O(w) = O(w^۵) = O(w^۷) = O(w^{۱۱}) = ۱۲$.

۳. مولدهای $\mathbb{Z}_{۱۲}$ عبارت‌اند از $\bar{۱}$، $\bar{۵}$، $\bar{۷}$، $\bar{۱۱}$. داریم $O(\bar{۲}) = ۶$، $O(\bar{۳}) = O(\bar{۹}) = ۴$، $O(\bar{۶}) = ۲$، $O(\bar{۸}) = ۳$ و $O(\bar{۱}) = O(\bar{۵}) = O(\bar{۷}) = O(\bar{۱۱}) = ۱۲$.

۴. داریم $\mathbb{Z}_{۱۲}^{\times} = \{\bar{۱}, \bar{۵}, \bar{۷}, \bar{۱۱}\}$، $O(\bar{۱}) = ۱$، $O(\bar{۵}) = O(\bar{۷}) = O(\bar{۱۱}) = ۲$.

۵. داریم $a^{-۳}ba^۳ = b^{۲۳}$. چون $O(a) = ۲$، داریم $b = b^۸$. پس یا $b = ۱$ یا $b^۷ = ۱$ و $O(b) = ۷$.

۶. اگر $O(a) = m$، $O(b) = n$، آنگاه چون $ab = ba$، داریم

$$(ab)^{mn} = a^{mn}b^{mn} = (a^m)^n (b^n)^m = e^n e^m = e.$$

۷. چون $ab = \begin{bmatrix} ۱ & -۱ \\ ۰ & ۱ \end{bmatrix}$ به ازای هر $n \in \mathbb{N}$ داریم $(ab)^n = \begin{bmatrix} ۱ & -n \\ ۰ & ۱ \end{bmatrix} \neq I$. پس $O(ab) = \infty$.

۱۰. از جبر خطی می‌دانیم ماتریس $n \times n$، A وارون پذیر است اگر و تنها اگر ستون‌های آن مستقل خطی باشند. پس باید n بردار $۱ \times n$ مستقل خطی با درایه‌های در F بیابیم. چون F، q عضو دارد و هر بردار ناصفر مستقل خطی است، برای اولین بردار $q^n - ۱$ انتخاب داریم. بردار بعدی نبایستی ضریبی از بردار اول باشد پس برای بردار دوم $q^n - q$ انتخاب داریم. بردار بعدی نبایستی ترکیب خطی از

دو بردار اول و دوم باشد، پس برای بردار سوم $q^n - q^2$ انتخاب داریم. به همین نحو برای بردار nام $q^n - q^{n-1}$ انتخاب داریم. از این‌رو کل انتخابها عبارت است از $(q^n - 1)(q^n - q)\cdots(q^n - q^{n-1})$.

۱۱. (الف) چون $x^n = 1$ اگر و تنها اگر $(x^{-1})^n = 1$، داریم $O(x) = O(x^{-1})$.
(ب) چون $(y^{-1}xy)^n = y^{-1}x^n y$، داریم $x^n = 1$ اگر و تنها اگر $(y^{-1}xy)^n = 1$. در نتیجه داریم $O(x) = O(y^{-1}xy)$.
(ج) بنا به (ب) داریم $O(yx) = O(y^{-1}(yx)y) = O(xy)$.

۱۲. چون $\gcd\{n_1, n_2\} = 1$، اعداد صحیح c_1 و c_2 وجود دارند که $c_1 n_1 + c_2 n_2 = 1$. قرار می‌دهیم $a_1 = a^{c_2 n_2}$ و $a_2 = a^{c_1 n_1}$. نشان دهید $a = a_1 a_2 = a_2 a_1$. و با استفاده از این که $\gcd\{n_2, c_1\} = 1$، نشان دهید $O(a_1) = n_1$ و $O(a_2) = n_2$. حال اگر $b_1, b_2 \in G$، و $a = b_1 b_2 = b_2 b_1$، $O(b_1) = n_1$ و $O(b_2) = n_2$. نشان دهید $a_2^{n_1} = b_2^{n_1}$ و نتیجه بگیرید $a_2^{n_1 c_1} = b_2^{n_1 c_1}$ و $a_2^{1-n_2 c_2} = b_2^{1-n_2 c_2}$. چون $a_2^{n_2} = 1 = b_2^{n_2}$ داریم $a_2 = b_2$ و به همین نحو $a_1 = b_1$.

۱۵. (و) چون $(۵\ ۴\ ۳\ ۶\ ۲\ ۱) = (۲\ ۶)(۲\ ۳\ ۴)(۱\ ۲\ ۵) = \alpha$، داریم $O(\alpha) = ۶$.
(ز) چون $(۲\ ۳)(۵\ ۶\ ۷\ ۱) = (۳\ ۶\ ۷\ ۱)(۲\ ۳)(۱\ ۲\ ۵) = \alpha$، داریم $O(\alpha) = ۴$.

۱۶. بنابه الگوریتم تقسیم q و k وجود دارند که $1 \le k \le r$ و $i + j = qr + k$. توجه کنید چون $1 \le i \le r$ و $1 \le j \le r$، داریم $q = ۰, ۱$. پس

$$\alpha^i(x_j) = \alpha^{k+qr-j}(x_j) = \alpha^k \alpha^{qr-j}(x_j) = \alpha^k(x_r) = x_k.$$

۱۹. ابتدا نشان دهید $(ab)^k = 1$. پس اگر $O(ab) = t$، داریم $t|k$. نشان دهید $a^t = b^{-t} \in \langle a\rangle \cap \langle b\rangle = \{1\}$ و نتیجه بگیرید $n|t$ و $m|t$. بنابراین $k = \operatorname{lcm}\{m, n\}|t$ و در نتیجه $k = t$.

۲۱. ابتدا حالت $\gcd\{m, n\} = 1$ را در نظر بگیرید. برای حالت $\gcd\{m, n\} = d > 1$ فرض کنید $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}$ و $n = p_1^{\beta_1} p_2^{\beta_2} \cdots p_s^{\beta_s}$ تجزیه‌ی m و n به عوامل اول باشند (ممکن است بعضی α_iها و β_iها صفر باشند) طوری که

$$p_s^{\alpha_s} \ge p_s^{\beta_s},\ \ \ldots,\ \ p_{r+1}^{\alpha_{r+1}} \ge p_{r+1}^{\beta_{r+1}},\quad p_r^{\alpha_r} < p_r^{\beta_r},\ \ \ldots,\ \ p_1^{\alpha_1} < p_1^{\beta_1}.$$

نتیجه بگیرید $\operatorname{lcm}\{m, n\} = p_1^{\beta_1} \cdots p_r^{\beta_r} p_{r+1}^{\alpha_{r+1}} \cdots p_s^{\beta_s}$. فرض کنید

$$m_1 = p_1^{\beta_1} \cdots p_r^{\beta_r} \quad \text{و} \quad n_1 = p_{r+1}^{\alpha_{r+1}} \cdots p_s^{\alpha_s},$$

و از حالت اول ثابت استفاده کنید.

۲۴. تمرین ۲۲ را تعمیم دهید.

تمرین‌های ۳.۳، همریختی، صفحه‌ی ۶۵

۱. (الف) اگر $O(a) = m$، آنگاه $f(a)^n = f(a^n) = f(1) = 1$ و $O(f(a))|n$.
(ب) اگر $O(f(a)) = m$، آنگاه $f(a)^m = f(a^m) = 1$. چون $f(1) = 1$ و f یک‌به‌یک است، $a^m = 1$. بنابراین $O(a)|m$، که به همراه (الف) نتیجه می‌دهد $O(f(a)) = O(a)$.

۳. (الف) $i \notin \mathbb{C}^\times$ عضوی با مرتبه‌ی ۴ است در صورتی که $\mathbb{R}^\times$ عضو مرتبه‌ی ۴ ندارد. پس بنا به مساله‌ی ۱، $\mathbb{R}^\times \ncong \mathbb{C}^\times$.
(ب) اگر $f : \mathbb{Z} \longrightarrow \mathbb{Q}$ یکریختی باشد. ثابت کنید $\langle f(1)\rangle = \mathbb{Q}$، که تناقض است؛ چون $\mathbb{Q}$ دوری نیست. (ج) $-1 \in \mathbb{Q}^\times$ عضوی از مرتبه‌ی ۲ است در صورتی که $\mathbb{Q}$ عضو مرتبه‌ی ۲ ندارد، پس $\mathbb{Q} \ncong \mathbb{Q}^\times$.
(د)) $-1 \in \mathbb{R}^\times$عضو مرتبه‌ی ۲ است و $\mathbb{R}$ عضو مرتبه‌ی ۲ ندارد.
(هـ) چون $\mathbb{Q}$ شمارا و $\mathbb{R}$ ناشمارا است پس تابع یک‌به‌یک و پوشا از $\mathbb{R}$ به $\mathbb{Q}$ وجود ندارد. راه دیگر این که اگر $f : \mathbb{Q} \longrightarrow \mathbb{R}$ یکریختی باشد، آنگاه برای هر $n \in \mathbb{Z}$ داریم $f(n) = nf(1)$، و نتیجه بگیرید برای هر $m, n \in \mathbb{Z}$، $f\left(\frac{m}{n}\right) = mf\left(\frac{1}{n}\right) = \frac{m}{n}f(1)$. پس برای $x \in \mathbb{Q}$، $f(x) = xf(1)$. چون f پوشاست، این یعنی هر عدد حقیقی مضربی گویا از عدد ثابت $a = f(1)$ است، این تناقض

است.

(و) به تعداد اعضای مرتبه‌ی ۲ یا ۴ نگاه کنید.

۴. چون $|X| = |Y|$، تابع دوسویی $\psi : X \longrightarrow Y$ وجود دارد. تابع $f : S_X \longrightarrow S_Y$ را با $f(\sigma) = \psi\sigma\psi^{-1}$ تعریف کنید. نشان دهید f یکریختی است.

۵. اگر $f, g \in \operatorname{Aut} G$، آنگاه $f \circ g$ یک‌به‌یک و پوشاست. $f \circ g$ همریختی نیز هست، زیرا

$$\begin{aligned}(f \circ g)(ab) &= f(g(ab)) \\ &= f(g(a)g(b)) \\ &= f(g(a))f(g(b)) \\ &= (f \circ g)(a)(f \circ g)(b).\end{aligned}$$

پس $f \circ g \in \operatorname{Aut} G$. از طرفی ترکیب توابع شرکت‌پذیر و هم‌چنین تابع همانی $\mathrm{id}_G : G \longrightarrow G$ یکریختی است. اکنون ثابت می‌کنیم $f^{-1} \in \operatorname{Aut} G$. برای این کار باید ثابت کنیم f^{-1} همریختی است. فرض کنید $a, b \in G$ و $a_1 = f^{-1}(a)$ و $b_1 = f^{-1}(b)$. پس $a = f(a_1)$ و $b = f(b_1)$. از این‌رو $ab = f(a_1)f(b_1) = f(a_1b_1)$ که نتیجه می‌دهد f^{-1} همریختی است: $f^{-1}(ab) = a_1b_1 = f^{-1}(a)f^{-1}(b)$.

۸. اگر به ازای یک $a \in G$، $\tau_a \neq \mathrm{id}_G$، آنگاه τ_a یک خودریختی نابدیهی از G است. در غیر این صورت G آبلی است و $f : G \longrightarrow G$، $f(a) = a^{-1}$ را در نظر بگیرید.

۹. فرض کنید $T = \{a^{-1}f(a) \mid a \in G\}$ و ثابت کنید تابع $\psi : G \longrightarrow T$ با ضابطه‌ی $\psi(a) = a^{-1}f(a)$ یک‌به‌یک است.

۱۰. با استفاده از تمرین قبل ثابت کنید $f(x) = x^{-1}$.

۱۲. به ازای هر یکریختی $\psi : G \longrightarrow H$، تابع $\theta : \operatorname{Aut} G \longrightarrow \operatorname{Aut} H$ را با ضابطه‌ی $\theta(f) = \psi f \psi^{-1}$ تعریف کنید. برای عکس مساله توجه کنید که $\mathbb{Z} \ncong \mathbb{Z}_3$ اما $\operatorname{Aut}\mathbb{Z} \cong \mathbb{Z}^\times \cong \mathbb{Z}_3^\times \cong \operatorname{Aut}\mathbb{Z}_3$.

۱۴. فرض کنید H آبلی باشد و $a, b \in G$، در این صورت

$$f(ab) = f(a)f(b) = f(b)f(a) = f(ba)$$

و چون f یک‌به‌یک است، $ab = ba$. اکنون فرض کنید $H = \langle h \rangle$. اگر $G = \{1\}$ چیزی برای اثبات نیست در غیر این صورت نشان دهید توان مثبتی از h در $\operatorname{Im} f$ قرار دارد و کوچک‌ترین عضو مجموعه‌ی $T = \{n \in \mathbb{N} \mid h^n \in \operatorname{Im} f\}$ را در نظر بگیرید، مثلاً m. پس عضو $b \in G$ وجود دارد که $f(b) = h^m$ و m کوچک‌ترین توان مثبت h است که در $\operatorname{Im} f$ قرار دارد. نشان دهید $G = \langle b \rangle$؛ برای اثبات این که هر عضو $a \in G$ در $\langle b \rangle$ قرار دارد ؛ نشان دهید به ازای nای، $f(a) = h^n$ و با استفاده از الگوریتم تقسیم، اعداد صحیح q و r را بیابید که $0 \leq r < m$ و $n = mq + r$. سپس از خاصیت m استفاده کنید.

۱۶. فرض کنید $X = \{v_1, \ldots, v_n\}$ پایه‌ای دلخواه برای V روی $\mathbb{Z}_p$ باشد و $f \in \operatorname{Aut} V$. فرض کنید $A = [\bar{a}_{ij}]$ ماتریس f در پایه‌ی X باشد. پس $f(v_j) = \sum_{i=1}^{n} \bar{a}_{ij}v_i$، $j = 1, \ldots, n$، که در آن $\bar{a}_{ij} \in \mathbb{Z}_p$. چون X پایه است، A وارون‌پذیر است. بنابراین تابع $\theta : \operatorname{Aut} V \longrightarrow \mathrm{GL}_n(\mathbb{Z}_p)$، که هر تبدیل خطی را با ماتریس آن در پایه‌ی X نظیر می‌کند، خوش تعریف است. به راحتی می‌توان دید θ همریختی یک‌به‌یک و پوشاست.

۱۷. فرض کنید V مجموعه‌ی اعضای G باشد. عمل جمع روی V را همان عمل ضرب در گروه G در نظر می‌گیریم $v + w = v \cdot w$ برای هر $v, w \in r = G$. پس $(V, +)$ یک گروه آبلی است. اگر $\bar{r} \in \mathbb{Z}_p$ و $v \in V$ تعریف می‌کنیم $\bar{r}v = v^r$. که در آن v^r با استفاده از عمل

ضرب G محاسبه می‌شود. نشان دهید ضرب اسکالر فوق خوش تعریف است. چون

$$\begin{aligned}(\bar{r}+\bar{s})v &= (\overline{r+s})v = v^{r+s} = v^r \cdot v^s = \bar{r}v + \bar{s}v\\ (\bar{r}+\bar{s})v &= (\overline{rs})v = v^{rs} = (v^r)^s = \bar{s}(\bar{r}v)\\ \bar{r}(v+w) &= (vw)^r = v^r w^r = \bar{r}v + \bar{r}w\\ \bar{1}v &= v^1 = v,\end{aligned}$$

V فضای برداری روی $\mathbb{Z}_p$ است. نشان دهید تابع $f : G \longrightarrow V$ را با ضابطه‌ی $f(a) = a$، یکریختی است، و $G \cong V$. به ویژه اگر G متناهی باشد، آنگاه V متناهی و در نتیجه $\dim_{\mathbb{Z}_p} V = n$ متناهی است. پس $V \cong \mathbb{Z}_p^n$ و $|G| = |V| = |\mathbb{Z}_p^n| = p^n$.

۱۹. از برهان خلف استفاده کنید: اگر $\psi : F^\times \longrightarrow F$ یکریختی باشد، آنگاه $\psi(1) = 0$. حال اگر $\psi(-1) = a$، نشان دهید $a + a = 0$. اگر $a \neq -1$، چون ψ یک‌به‌یک است، $\psi(-1) = a \neq 0 = \psi(1)$. پس برای هر $b \in F$ نتیجه بگیرید $b + b = 0$، به ویژه $1 + 1 = 0$، یعنی $-1 = 1$ که تناقض است. پس $-1 = 1$ و برای هر $b \in F$ داریم $b = -b$. نتیجه بگیرید $\psi(b^{-1}) = \psi(b)$ و بنابراین $b = b^{-1}$ و $b^2 = 1$. حال اگر $x \in F$ و $x \neq 0, 1$، داریم

$$1 = (1+x)^2 = 1 + 2x + x^2 = 1 + 0 + 1,$$

که نتیجه می‌دهد $1 = 0$، این تناقض است. از این‌رو $F = \{0, 1\}$ و $F^\times = \{1\}$ که مجدداً تناقض است.

۲۰. اگر به ازای یک $a \in G$، $a^2 \neq 1$، بنابه مساله‌ی ۸، حکم ثابت است. پس فرض کنید برای هر $a \in G$، $a^2 = 1$. پس G آبلی است و $G \cong V$ که در آن V فضای برداری روی $\mathbb{Z}_2$ است. اگر X پایه‌ای برای V روی $\mathbb{Z}_2$ باشد. $v \neq w \in X$ تبدیل خطی یکتای ψ وجود دارد که $\psi(v) = w$ و $\psi(w) = v$ و $\psi(x) = x$ برای هر $x \neq v, w$. تبدیل خطی ψ یک خودریختی G است.

تمرین‌های ۴.۳، زیرگروه، صفحه‌ی ۶۹

۱. $\{1, a\} = \langle a\rangle$، $\{1, b\} = \langle b\rangle$، $\{1, c\} = \langle c\rangle$، $\{1\}$، زیرگروه‌های سره‌ی V_4 هستند.

۲. فرض کنید $H, K \leq \mathbb{Q} \neq \{0\}$. اگر $\frac{m_1}{n_1} \in K \neq 0$ و $\frac{m_2}{n_2} \in H \neq 0$، نشان دهید $m_1 m_2 \in H \cap K \neq 0$.

۳. اگر $H, K \leq G$ و $H \cup K \leq G$، نشان دهید $H \subseteq K$ یا $K \subseteq H$. اگر $H \not\subseteq K$ و $K \not\subseteq H$، آنگاه اعضای $h \in H - K$ و $k \in K - H$ وجود دارند. سپس hk را در نظر بگیرید. Q_8 اجتماع سه زیرگروه سره‌ی $\{\pm 1, \pm i\}$، $\{\pm 1, \pm j\}$ و $\{\pm 1, \pm k\}$ است.

۶. از این که اعداد صحیح c_2 و c_1 وجود دارند که $c_1 m + c_2 n = 1$ استفاده کنید.

۷. چون $K \leq G$، $1 \in K$. چون f همریختی است $1 = f(1) \in f(K)$ و $f(K) \neq \emptyset$. حال اگر $f(b), f(a) \in f(K)$، که در آن $a, b \in K$، داریم

$$\begin{aligned} f(a)f(b) = f(ab) &\in f(K) \qquad (a, b \in K \text{ چون})\\ f\left(a^{-1}\right) = f(a)^{-1} &\in f(K) \qquad (a^{-1} \in K \text{ چون})\end{aligned}$$

۸. اگر $x = \begin{bmatrix} a & b \\ 0 & c \end{bmatrix}$ عضوی از مرتبه‌ی ۲ در G باشد. داریم

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = x^2 = \begin{bmatrix} a & b \\ 0 & c \end{bmatrix}\begin{bmatrix} a & b \\ 0 & c \end{bmatrix} = \begin{bmatrix} a^2 & ab+bc \\ 0 & c^2 \end{bmatrix}.$$

پس $a^2 = 1$، $c^2 = 1$، و $ab + bc = 0$؛ و

$$\begin{cases} a = 1 \\ c = 1 \\ b = 0 \end{cases} \quad \begin{cases} a = 1 \\ c = -1 \\ b \text{ دلخواه} \end{cases} \quad \begin{cases} a = -1 \\ c = 1 \\ b \text{ دلخواه} \end{cases} \quad \begin{cases} a = -1 \\ c = -1 \\ b = 0 \end{cases}$$

و اعضای مرتبه‌ی ۲ در G عبارت‌اند از

$$\begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}, \quad \begin{bmatrix} 1 & b \\ 0 & -1 \end{bmatrix}, \quad \begin{bmatrix} -1 & b \\ 0 & 1 \end{bmatrix}.$$

۹. در گروه دووجهی D_8، زیرگروه‌های $H = \{1, \varepsilon\}$ و $K = \{1, \varepsilon\rho\}$ را در نظر می‌گیریم. در این صورت $HK = \{1, \varepsilon, \varepsilon\rho, \rho^{-1}\}$، که زیرگروه D_8 نیست.

۱۰. فرض کنید $HK \leq G$. ثابت می‌کنیم $HK = KH$. اگر $hk \in HK$ که در آن $h \in H$ و $k \in K$، آنگاه چون $HK \leq G$، داریم $k^{-1}h^{-1} = (hk)^{-1} \in HK$. پس اعضای $h_1 \in H$ و $k_1 \in K$ وجود دارند که $k^{-1}h^{-1} = h_1k_1$. بنابراین $hk = k_1^{-1}h_1^{-1} \in KH$. پس $HK \subseteq KH$. حال اگر $kh \in KH$، آنگاه $(kh)^{-1} = h^{-1}k^{-1} \in HK$. چون HK زیرگروه است، داریم $((kh)^{-1})^{-1} \in HK$. پس $kh \in HK$ و در نتیجه $KH \subseteq HK$.
اکنون فرض کنید $HK = KH$. ثابت می‌کنیم $HK \leq G$. چون $1 \in H$ و $1 \in K$، داریم $1 \in HK$. حال اگر $h_1k_1, h_2k_2 \in HK$، که در آن $h_i \in H$ و $k_i \in K$، داریم

$$\begin{aligned} (h_1k_1)(h_2k_2) &= h_1(k_1h_2)k_2 \\ &= h_1(h_3k_3)k_2 \quad (HK = KH \text{ چون}, \ h_3 \in H, k_3 \in K) \\ &= (h_1h_3)(k_3k_2) \in HK. \end{aligned}$$

هم‌چنین $(h_1k_1)^{-1} = k_1^{-1}h_1^{-1} \in KH = HK$. پس $HK \leq G$.

۱۱. فرض کنید $k \in K$. پس $k \in K \subseteq KN = HN$. پس $h \in H$ و $a \in N$ وجود دارند که $k = ha$. بنابراین $a = h^{-1}k \in K \cap N = H \cap N$. از این‌رو $h^{-1}k \in H$ و $k \in H$. در نتیجه $K \subseteq H$ و $K = H$.

۱۲. توجه کنید که اگر Ka یک زیرگروه G باشد، چون $1 \in Ka$ داریم $a^{-1} \in K$ و بنابراین $a \in K$. اکنون چون $H = Kyx^{-1}$ داریم $yx^{-1} \in K$. پس $H = Kyx^{-1} = K$.

۱۵. داریم $C_p \subset C_{p^2} \subset C_{p^3} \subset \cdots$ و $C_{p^\infty} = \bigcup_{i=1}^{\infty} C_{p^i}$. توجه کنید که اگر $p^{n_1} < p^{n_2} < \cdots$ دنباله‌ای نامتناهی از توان‌های p باشد، آنگاه $C_{p^\infty} = \bigcup_{k=1}^{\infty} C_{p^{n_k}}$. حال اگر $\{1\} \neq H < C_{p^\infty}$، ثابت کنید به ازای nای، $H = C_{p^n}$. اگر H متناهی باشد، اعضای ناهمانی H را بر حسب مرتبه مرتب کنید و اعداد طبیعی n_1، ...، n_r با $p^{n_1} < p^{n_2} < \cdots < p^{n_r}$ بیابید طوری که $H = \{1, h_1, \ldots, h_r\}$ و $O(h_i) = p^{n_i}$. بنابراین $C_{p^{n_1}} \subset C_{p^{n_2}} \subset \cdots \subset C_{p^{n_r}} \subseteq H$ و $H = C_{p^{n_r}}$. پس فرض کنید H نامتناهی باشد. قرار می‌دهیم $T_1 = \{O(h) \mid h \in G - \{1\}\}$. پس T_1 مجموعه‌ی ناتهی از اعداد طبیعی است که توانی از p هستند. بنا به اصل خوشترتیبی کوچک‌ترین عضو p^{n_1} دارد. پس $h_1 \in H$ وجود دارد که $O(h_1) = p^{n_1}$ و h_1 عضوی با کوچک‌ترین مرتبه در $H - \{1\}$ است. به استقرا اعداد طبیعی n_1، ...، n_k، ... و اعضای h_1، ...، h_k، ... از H را با $p_1^{n_1} < \cdots < p_k^{n_k}$ و $O(h_i) = p^{n_i}$ را بیابید و توجه کنید $C_{p^{n_i}} = \langle h_i \rangle$. در نتیجه $C_{p^\infty} = \bigcup_{k=1}^{\infty} C_{p^{n_k}} \subseteq H$. پس $H = C_{p^\infty}$، که متناقض با سره بودن H در C_{p^∞} است.

۱۶. فرض کنید $a \in G$. باید ثابت کنیم $O(a) < \infty$. اگر چنین نباشد و $O(a) = \infty$، قرار دهید $H = \langle a \rangle$ و $K = \langle a^2 \rangle$. پس $H \cong K$، که این خلاف فرض است. بنابراین $O(a) < \infty$. مثالی از چنین گروهی C_{p^∞} است.

۱۹. چون $K \subseteq L$، داریم $(H \cap L)K \subseteq HK \cap L$. فرض کنید $a \in HK \cap L$، پس اعضای $h \in H$ و $k \in K$ وجود دارند که $a = hk$. چون $K \subseteq L$ داریم $ak^{-1} = h \in H \cap L$ و بنابراین $a \in (H \cap L)K$. در نتیجه $HK \cap L \subseteq (H \cap L)K$

۲۰. اگر $g \in H$ که در این صورت $g^{-1}Hg = H$ و $H = (g^{-1}Hg) = H \subset G$. پس فرض کنید $g \notin H$. اگر $H(g^{-1}Hg) = G$ در این صورت چون $g \in G$، اعضای $b, a \in H$ وجود دارند که $g = a(g^{-1}bg)$. بنابراین $ag^{-1}b = 1$ و در نتیجه $g^{-1} = a^{-1}b^{-1}$ و $g = ba \in H$ که تناقض است. پس $H(g^{-1}Hg) \subset G$.

۲۱. فرض کنید $a \in G$ ، $a \neq 1$، نشان دهید $G = \langle a \rangle$. و $\langle a^2 \rangle$ را در نظر بگیرید و نتیجه بگیرید $O(a) = m < \infty$. حال اگر $m_1 | m$، داریم $\langle a^{m_1} \rangle \leq \langle a \rangle$. بنابراین $\langle a^{m_1} \rangle = \langle a \rangle$، که در این حالت $m_1 = 1$ (چون $m_1 | m$) و اگر $\langle a^{m_1} \rangle = \{1\}$، داریم $m_1 = m$. بنابراین m عدد اول است.

۲۲. فرض کنید G گروه نامتناهی باشد. اگر $a \in G$ و $O(a) = \infty$، آنگاه $\langle a \rangle$، $\langle a^2 \rangle$، $\langle a^3 \rangle$ و ... تعداد نامتناهی زیرگروه متمایز از G است. بنابراین فرض کنید برای هر $a \in G$، $O(a) < \infty$. اگر تعداد زیرگروه‌های G متناهی باشد، آنگاه تعداد زیرگروه‌های دوری G متناهی است. فرض کنید $H_i = \langle a_i \rangle$، $i = 1, \dots n$، همه‌ی زیرگروه‌های دوری G باشند. در این صورت $a \in G \setminus \bigcup_{i=1}^{n} H_i$ وجود دارد. اکنون j وجود دارد که $\langle a \rangle = H_j$، اما این خلاف $a \notin H_i$، $i = 1, \dots, n$، است.

۲۳. فرض کنید G گروه نابدیهی باشد. اگر $G = \langle a \rangle$ دوری نامتناهی باشد، آنگاه $G \cong \mathbb{Z}$. از طرفی هر زیرگروه نابدیهی H از G به صورت $H = \langle a^m \rangle$. پس H دوری نامتناهی است. بنابراین $H \cong \mathbb{Z}$ و $G \cong H$.
برعکس فرض کنید G گروه نابدیهی باشد که با زیرگروه‌های نابدیهی‌اش یکریخت است. عضو $1 \neq a \in G$ را انتخاب می‌کنیم. اگر $\langle a \rangle$ زیرگروه سره‌ی G باشد، آنگاه طبق فرض $G \cong \langle a \rangle$، پس G دوری است. اگر $\langle a \rangle$ زیرگروه سره‌ی G نباشد، چون $1 \neq a$، داریم $G = \langle a \rangle$. در هر صورت G دوری است. از طرفی G نامتناهی است، زیرا هیچ تابع دوسویی بین یک مجموعه‌ی متناهی و زیرمجموعه‌ی سره‌اش وجود ندارد.

۲۴. فرض کنید H زیرگروه سره‌ای از گروه متناهی G باشد. اگر H ماکسیمال باشد، حکم ثابت است. پس فرض کنید H ماکسیمال نباشد. بنابراین زیرگروه سره‌ی H_1 از G وجود دارد که $H < H_1 < G$. فرض کنید به صورت استقرایی زیرگروه‌های سره‌ی

$$H < H_1 < H_2 < \cdots < H_n < G$$

را به دست آورده باشیم. اگر H_n ماکسیمال باشد حکم ثابت است؛ در غیر این صورت زیرگروه H_{n+1} وجود دارد که $H_n < H_{n+1} < G$. چون G متناهی است این روند متوقف می‌شود. پس H در یک زیرگروه ماکسیمال قرار می‌گیرد.

تمرین‌های ۶.۳، تولید گروه‌ها، گروه‌های متناهیاً تولید شده، صفحه ۷۳

۱.

$$\begin{aligned} u \in f(\langle X \rangle) &\iff \exists v \in \langle X \rangle, \quad u = f(v) \\ &\iff v = x_1^{n_1} \cdots x_s^{n_s}, \quad n_i \in \mathbb{Z}, \quad x_i \in X, \quad u = f(v) \\ &\iff u = f(x_1^{n_1} \cdots x_s^{n_s}) \\ &\iff u = f(x_1)^{n_1} \cdots f(x_s)^{n_s} \\ &\iff u \in \langle f(X) \rangle . \end{aligned}$$

۲. از این که $\langle X \rangle$ کوچک‌ترین زیرگروه G شامل X است، استفاده کنید.

۳. چون $H < G$، عضو $x \in G - H$ وجود دارد. فرض کنید $a \in G$. باید ثابت کنیم $a \in \langle G - H \rangle$. اگر $a \in H$، آنگاه می‌توان نوشت $a = (ax)x^{-1}$ که در آن $ax, x^{-1} \in G - H$. پس $a \in \langle G - H \rangle$.

۴. فرض کنید $H = \left\langle \frac{r_1}{s_1}, \dots, \frac{r_k}{s_k} \right\rangle$ یک زیرگروه متناهیاً تولید شده‌ی $\mathbb{Q}$ باشد. نشان دهید H زیرگروه گروه دوری $\left\langle \frac{1}{s_1 s_2 \cdots s_k} \right\rangle$ است.

۵. فرض کنید $p_1 < p_2 < p_3 < \cdots$ دنباله همه‌ی اعداد اول فرد باشد و قرار دهید $H = \left\langle \frac{1}{p_1}, \frac{1}{p_2}, \dots \right\rangle$. نشان دهید H دوری نیست. برای این کار قرار دهید $H = \left\langle \frac{a}{b} \right\rangle$، که در آن $a, b \in \mathbb{Z}$ و $b \geq 0$. عدد اول p را طوری اختیار کنید که $p > b$ و از این که $\frac{1}{p} \in H = \left\langle \frac{a}{b} \right\rangle$ استفاده کنید.

۶. فرض کنید $\mathbb{Q}_{pos}^{\times} = \left\langle \frac{r_1}{s_1}, \dots, \frac{r_k}{s_k} \right\rangle$ متناهیاً تولید شده باشد ($s_i \neq 0, r_i > s_i \in \mathbb{Z}$). عدد اول p را طوری انتخاب می‌کنیم که از همه‌ی اعداد اول در تجزیه‌ی r_iها و s_iها بزرگ‌تر باشد. اعداد صحیح $n_1, \dots, n_k$ وجود دارند که $p = (\frac{r_1}{s_1})^{n_1} \cdots \left(\frac{r_k}{s_k}\right)^{n_k}$. فرض

کنید $n_{i_1},\dots,n_{i_r}$ نامنفی و $n_{j_t},\dots,n_{j_1}$ منفی باشند، پس

$$ps_{i_1}^{n_{i_1}}\cdots s_{i_r}^{n_{i_r}}r_{j_1}^{-n_{j_1}}\cdots r_{j_t}^{-n_{j_t}}=r_{i_1}^{n_{i_1}}\cdots r_{i_r}^{n_{i_r}}s_{j_1}^{-n_{j_1}}\cdots s_{j_t}^{-n_{j_t}}.$$

در تساوی فوق همه‌ی اعداد صحیح‌اند. چون p سمت چپ تساوی را عاد می‌کند سمت راست را نیز عاد می‌کند و بنابراین یکی از r_iها یا s_jها را عاد می‌کند که متناقض انتخاب p است.

۷. فرض کنید $H=\langle z_1,\dots,z_k\rangle$ زیرگروهی متناهیاً تولید شده از C_{p^∞} است و $O(z_i)=p^{n_i}$. بدون کم شدن از کلیت مساله می‌توان فرض کرد z_iها بر حسب مرتبه مرتب شده‌اند. در این صورت $z_1,\dots,z_k\in\langle z_k\rangle=C_{p^{n_k}}$. پس $H\subseteq C_{p^{n_k}}$ و چون $C_{p^{n_k}}=\langle z_k\rangle\subseteq H$، داریم $H=C_{p^{n_k}}$.

۸. فرض کنید $G=\langle a_1,\dots,a_n\rangle$ گروهی متناهیاً تولید شده باشد و $H<G$. نشان می‌دهیم زیرگروهی ماکسیمال از G شامل H وجود دارد. قرار می‌دهیم $T=\{K\mid H<K<G\}$. با استفاده از لم زُرن نشان می‌دهیم T عضو ماکسیمال M دارد و این یعنی M زیرگروه ماکسیمال G شامل K است. فرض کنید $\mathscr{C}=\{K_i\}_{i\in I}$ یک زنجیر در T باشد. قرار می‌دهیم $K=\bigcup_{i\in I}K_i$. ثابت می‌کنیم $K\in T$. ابتدا ثابت می‌کنیم $K\leq G$. چون $K_i<G$، داریم $1\in K_i$. پس $1\in K$، و در نتیجه $K\neq\emptyset$. حال اگر $x,y\in K$، آنگاه $i,j\in I$ وجود دارند که $x\in K_i$ و $y\in K_j$. چون $\mathscr{C}$ یک زنجیر است $K_i\subseteq K_j$ یا $K_j\subseteq K_i$. فرض کنید مثلاً $K_i\subseteq K_j$. پس $x,y\in K_j$ و $xy\in K_j$ و $x^{-1}\in K_j$. در نتیجه $xy\in K$ و x^{-1}. پس $K\leq G$. چون $H<K_i$، داریم $H<\bigcup_{i\in I}K_i=K$. حال تنها باید ثابت کنیم $K<G$. فرض کنید چنین نباشد و $K=G$. چون $a_1,\dots,a_n\in G=K$، آنگاه همه‌ی $i_1,\dots,i_n\in I$ وجود دارند. $s=1,\dots,n$، $a_s\in K_{i_s}$. چون $\mathscr{C}$ زنجیر است، یک K_{i_m} وجود دارد $a_1,\dots,a_n\in K_{i_m}$، و این متناقض با سره بودن K_{i_m} در G است. پس $K<G$. بنابراین K عضوی از T است. چون برای هر $i\in I$، $K_i\subseteq K$ پس K کران بالا برای $\mathscr{C}$ است. از این‌رو بنا به لم زُرن T عضو ماکسیمال دارد.

۹. با توجه به رابطه‌ی $bab^{-1}=a^2$، نشان دهید برای هر $n\in\mathbb{Z}$ و $m\in\mathbb{N}$، داریم $(b^mab^{-m})^n=(a^{2^m})^n$. بنابراین $b^ma^nb^{-m}=a^{2^mn}$ و

$$\begin{cases}a^nb^{-m}=b^{-m}a^{2^mn}\\ a^nb^m=b^{-m}a^{2^mn}b^{2^m}.\end{cases}$$

چون هر عضو $\langle a,b\rangle$ به صورت $u=a^{n_1}b^{m_1}a^{n_2}b^{m_2}\cdots a^{n_k}b^{m_k}$ نوشته می‌شود که در آن $n_i,m_i\in\mathbb{Z}$، با توجه به دو رابطه‌ی اخیر و قدری محاسبه می‌توان نوشت $u=b^\alpha a^\beta b^\gamma$ که در آن $\alpha,\beta,\gamma\in\mathbb{Z}$.

۱۰. داریم $c=ab=\begin{bmatrix}1&0\\0&-1\end{bmatrix}\begin{bmatrix}1&1\\0&-1\end{bmatrix}=\begin{bmatrix}1&1\\0&1\end{bmatrix}$. در این صورت $O(a)=2$ و $O(c)=\infty$ و $\langle a,b\rangle=\langle a,c\rangle$. هم‌چنین داریم

$$cac=\begin{bmatrix}1&1\\0&1\end{bmatrix}\begin{bmatrix}1&0\\0&-1\end{bmatrix}\begin{bmatrix}1&1\\0&1\end{bmatrix}=\begin{bmatrix}1&-1\\0&-1\end{bmatrix}\begin{bmatrix}1&1\\0&1\end{bmatrix}=a.$$

پس $ac=c^{-1}a$ و $\langle a,c\rangle=\{c^na^m\mid n\in\mathbb{Z},m=0,1\}$.
از طرفی چون

$$D_\infty=\langle\tau,\varepsilon\rangle=\{\tau^n\varepsilon^m\mid n\in\mathbb{Z},\ \ m=0,1\}$$

به راحتی می‌توان دید تابع $f:\langle a,c\rangle\longrightarrow D_\infty$ با ضابطه‌ی $f(c^na^m)=\tau^n\varepsilon^m$ یک یکریختی است.

تمرین‌های ۶.۳، چند زیرگروه مهم، صفحه‌ی ۷۶

۱. داریم $[\rho^i,\rho^j]=[\varepsilon,\varepsilon]=1$ و چون $\rho\varepsilon=\varepsilon\rho^{-1}$، داریم $[\rho^i\varepsilon,\rho^j\varepsilon]=\rho^{2(i-j)}$، $[\rho^i\varepsilon,\rho^j]=\rho^{2j}$، $[\rho^j,\rho^i\varepsilon]=\rho^{-2j}$، پس

$$D'_{2n}=\left\langle[\rho^i\varepsilon^j,\rho^r\varepsilon^s]\mid 1\leq i,r\leq n-1,\ \ 0\leq j,s\leq 1\right\rangle=\left\langle\rho^2\right\rangle.$$

به همین صورت چون $\tau\varepsilon = \varepsilon\tau^{-1}$، داریم $D'_\infty = \langle\tau^2\rangle$. چون $D'_{2n} = \langle\rho^2\rangle$ و $\langle\rho^2\rangle$ آبلی است، داریم $D''_{2n} = \langle\rho^2\rangle' = \{1\}$. پس D_{2n} حل‌پذیر است. به همین صورت $D''_\infty = \langle\tau^2\rangle' = \{1\}$.

۲. داریم $ab = ba$ اگر و تنها اگر $[a,b] = 1$. چون $[\tau^i\varepsilon, \tau^j\varepsilon] = \tau^{2(i-j)} \neq 1$ پس $\tau^i\varepsilon \notin Z(D_\infty)$، $i = 0, 1, 2, \ldots$. از طرف دیگر چون $\tau\varepsilon = \varepsilon\tau^{-1}$ و $\tau \neq \tau^{-1}$، داریم $\tau \notin Z(D_\infty)$ و $\varepsilon \notin Z(D_a)$. پس $Z(D_\infty) = \{1\}$.

۳. داریم $[\rho^i\varepsilon, \rho^j] = \rho^{2j}$. پس $[\rho^i\varepsilon, \rho^j] = 1$ اگر و تنها اگر $\rho^{2j} = 1$. به علاوه ρ^j با ε تعویض می‌شود اگر و تنها اگر با $\rho^i\varepsilon$ تعویض شود (چون ρ^j و ρ^i تعویض می‌شوند). پس ρ^j، $(0 < j < n)$، در $Z(D_{2n})$ قرار دارد اگر و تنها اگر $\rho^{2j} = 1$ اگر و تنها اگر $n|2j$ (چون $O(\rho) = n$). بنابراین اگر n فرد باشد، آن‌گاه $n|j$ که تناقض است، زیرا $0 < j < n$. پس n زوج است. بنابراین $\frac{n}{2}|j$. در نتیجه $j = \frac{n}{2}$. در نتیجه اگر n فرد باشد داریم ، $Z(D_{2n}) = \{1\}$ و اگر n زوج باشد، داریم $Z(D_{2n}) = \left\{1, \rho^{\frac{n}{2}}\right\}$.

۴. ماتریس $A = [a_{ij}] \in \mathrm{GL}_n(F)$ در $Z = Z(\mathrm{GL}_n(F))$ قرار دارد اگر و تنها اگر برای هر $1 \leq i, j \leq n$، $E_{ij}A = AE_{ij}$. توجه کنید AE_{ij} ماتریسی است که همه‌ی ستون‌های آن صفرند، جز ستون jام، که در آن ستون iام A قرار دارد. هم‌چنین $E_{ij}A$ ماتریسی است که همه‌ی سطرهای آن صفرند جز سطر iام که در آن سطر jام A قرار دارد :

$$\begin{aligned} AE_{ij} &= a_{1i}E_{ij} + a_{2i}E_{2j} + \cdots + a_{ni}E_{nj} \\ E_{ij}A &= a_{j1}E_{i1} + a_{j2}E_{i2} + \cdots + a_{jn}E_{in} \end{aligned}$$

تساوی $AE_{ij} = E_{ij}A$ وقتی برقرار است که برای $i \neq j$، $a_{ij} = 0$. پس همه‌ی درایه‌های غیرقطری A صفرند. اکنون $AE_{1j} = a_{11}E_{ij}$ و $E_{1j}A = a_{jj}E_{1j}$. پس $a_{11} = a_{jj}$ برای هر $1 \leq j \leq n$. پس $A \in Z$ اگر و تنها اگر A ماتریس قطری باشد که عناصر روی قطر برابرند یعنی A ضرایب ماتریس همانی است.

۸. فرض کنید $x \in G$. تابع $f : \mathrm{orb}(x) \longrightarrow G'$ را با $f(a^{-1}xa) = x^{-1}a^{-1}xa$ تعریف کنید و نشان دهید f تابع یک‌به‌یک است.

۹. توجه کنید که اگر $A = [a_{ij}]_{n\times n}$، که در آن $a_{ij} = 0$، برای $i > j$. آن‌گاه $A^{-1} = [d_{ij}]$، که در آن $d_{ii} = a_{ii}^{-1}$ و $d_{ij} = 0$، برای $i > j$. به ازای هر $A, B \in H$ (H گروه ماتریس‌های بالا مثلثی وارون‌پذیر است) ماتریس $A^{-1}B^{-1}AB = [c_{ij}]$ یک ماتریس بالا مثلثی است که روی قطر آن برابر ۱ است، یعنی $c_{ii} = 1$ و $c_{ij} = 0$، برای $i > j$. نتیجه بگیرید زیرگروه مشتق H مجموعه‌ی ماتریس‌های بالا مثلثی است که روی قطرشان ۱ است. حال اگر $A = [a_{ij}]$ و $B = [b_{ij}]$ دو ماتریس بالا مثلثی باشند که روی قطرشان ۱ است، توجه کنید $A^{-1} = [d_{ij}]$ که در آن $d_{ii} = 1$، $d_{i,i+1} = -a_{i,i+1}$، یعنی A^{-1} ماتریس بالا مثلثی که روی قطرش ۱ است و درایه‌های بالای قطر آن صفر است، یعنی $c_{ii} = 1$، $c_{i,i+1} = 0$. نتیجه بگیرید مشتق دوم H متشکل از ماتریس‌های بالا مثلثی است که روی قطرشان ۱ و یک درایه‌های بالای قطرشان صفر است. این روند را ادامه دهید.

۱۰. نشان دهید $C_G(a^{-1}xa) = a^{-1}C_G(x)a$.

۱۱. فرض کنید $x, y \in G$. زیرمجموعه‌های نامتناهی $xZ(G)$ و $yZ(G)$ را در نظر بگیرید.

۱۲. فرض کنید $T = \{a \in G \mid a^n \neq 1\}$ در این صورت T متناهی است. عضو $g \in T$ و مجموعه‌ی مزدوج‌های g، یعنی $X = \{x^{-1}gx \mid x \in G\}$ را در نظر بگیرید. نشان دهید هر دو حالت X متناهی و نامتناهی به تناقض می‌انجامد؛ بنابراین $T = \emptyset$. در حالت $|X| < \infty$، نشان دهید $C_G(g)$ نامتناهی است و فرض مساله را برای مجموعه‌ی نامتناهی gS، که در آن $S = \{x \in C_G(g) \mid x^n = 1\}$، به کار ببرید.

۱۳. به برهان خلف عمل کنید: یعنی فرض کنید هر زیرگروه آبلی شامل g، متناهی باشد. در این صورت $O(g) < \infty$، زیرا $\langle g\rangle$ آبلی است. اکنون چون G نامتناهی است، طبق فرض $G_1 = C_G(g)$ نامتناهی است. بنابراین عضو $g_1 \in G_1 - \langle g\rangle$ وجود دارد. قرار می‌دهیم $H_1 = \langle g, g_1\rangle$. چون $gg_1 = g_1g$، H_1 آبلی است؛ پس $|H_1| < \infty$. چون G_1 نامتناهی است طبق فرض $G_2 = C_{G_1}(g_1)$ نامتناهی است و بنابراین عضو $g_2 \in G_2 - H_1$ وجود دارد. توجه کنید چون g و g_1 و g_2 دوبه‌دو با هم تعویض می‌شوند، $H_2 = \langle g, g_1, g_2\rangle$ آبلی است. به استقرا اعضای g_1، g_2، ...، g_n و زیرگروه‌های G_1، G_2، ...، G_n را طوری بیابید که $H_i = \langle g, g_1, \ldots, g_i\rangle$، $(i = 1, \ldots, n)$، زیرگروه‌های آبلی، و $G_{i+1} = C_{G_i}(g_i)$ زیرگروه‌های نامتناهی از G باشند، $i = 1, 2, \ldots, n-1$ و $g_i \in G_i - H_{i-1}$، $i = 2, 3, \ldots, n$. چون H_n آبلی است، $|H_n| < \infty$. قرار می‌دهیم $A = \bigcup_{n=1}^{\infty} H_n$. در این صورت A گروه آبلی نامتناهی و شامل g است، که تناقض است.

تمرین‌های ۷.۳، زیرگروه‌های مشخصه و نرمال، صفحه‌ی ۸۲

۲. در گروه دووجهی D_8 فرض کنید $H=\{1,\varepsilon,\rho^2,\varepsilon\rho^2\}$ و $K=\{1,\varepsilon\}$ در این صورت $K\trianglelefteq H\trianglelefteq D_8$، اما $K\not\trianglelefteq Q_8$.

۴. چون $1\in H$ و $1\in K$، داریم $HK\neq\emptyset$. حال اگر $h_1k_1\in HK$ و h_2K_2 که در آن $h_i\in H$ و $k_i\in K$. داریم

$$\begin{aligned}(h_1k_1)(h_2k_2) &= h_1(k_1h_2k_1^{-1})k_1k_2\\ &= h_1h_3k_1k_2\in HK \quad (h_3=k_1h_2k_1^{-1}\in H,\ H\lhd G \text{ چون})\end{aligned}$$

و

$$(h_1k_1)^{-1}=k_1^{-1}h_1^{-1}=(k_1^{-1}h_1^{-1}k_1)k_1^{-1}=h_4k_1^{-1}\in HK.$$

بنابراین $HK\trianglelefteq G$. به همین نحو ثابت می‌شود که اگر $K\trianglelefteq G$ آنگاه $HK\leq G$.

۵. از نرمال بودن H و K استفاده کنید و نشان دهید $k^{-1}h^{-1}kh=1$.

۱۳. اگر $[h,k]$ مولدی از $[H,K]$ باشد برای هر مولد $h_1\in H$ یا $k_1\in K$ از $\langle H,K\rangle$ می‌توان نوشت

$$h_1^{-1}[h,k]h_1=[h_1^{-1}hh_1,h_1^{-1}kh_1]$$

۱۴. فرض کنید $H\trianglelefteq G$. چون برای هر $h\in H$ و هر $a^{-1}\in G$، داریم $a^{-1}ha\in H$، برای هر $h\in H$، $\mathrm{orb}(h)\subseteq H$. پس $\bigcup_{h\in H}\mathrm{orb}(h)\subseteq H$. برعکس چون برای هر $h\in H$، داریم $h\in\mathrm{orb}(h)$. پس $H\subseteq\bigcup_{h\in H}\mathrm{orb}(h)$. در نتیجه $H=\bigcup_{h\in H}\mathrm{orb}(h)$. یعنی H اجتماعی از رده‌های مزدوجی G است. اکنون اگر $H=\bigcup_{i\in I}\mathrm{orb}(a_i)$، که در آن $a_i\in G$. ثابت می‌کنیم $H\trianglelefteq G$. فرض کنید $h\in H$، پس $i\in I$ وجود دارد که $h\in\mathrm{orb}(a_i)$. بنابراین به ازای یک $b\in G$ داریم $h=b^{-1}a_ib$. حال برای هر $a\in G$ داریم

$$a^{-1}ha=a^{-1}(b^{-1}a_ib)a=(ba)^{-1}a_i(ba)\in\mathrm{orb}(a_i)\subseteq H.$$

پس $a^{-1}ha\in H$ و $H\trianglelefteq G$.

۱۷. فرض کنید $x\in G$، داریم

$$\begin{aligned}x^{-1}H_Gx &= x^{-1}\left(\bigcap_{a\in G}a^{-1}Ha\right)x\\ &= \bigcap_{a\in G}x^{-1}a^{-1}Hax\\ &= \bigcap_{a\in G}(ax)^{-1}Hax\\ &= \bigcap_{y\in G}y^{-1}Hy\\ &= H_G.\end{aligned}$$

پس $H_G\trianglelefteq G$. چون $1\in H$، داریم $H=1H1^{-1}\supseteq\bigcap_{a\in G}a^{-1}Ha=H_G$. حال اگر $K\trianglelefteq G$ و $K\subseteq H$، آنگاه به ازای هر $a\in G$، $a^{-1}Ka=K$ و بنابراین $K=a^{-1}Ka\subseteq a^{-1}Ha$. پس $K\subseteq\bigcap_{a\in G}a^{-1}Ha=H_G$.

۱۸. (ب) فرض کنید $K=\langle a^{-1}ha\mid a\in G,\ h\in H\rangle$. اگر $x\in G$ و $a^{-1}ha$ مولدی از K باشد، داریم $x^{-1}(a^{-1}ha)x=(ax)^{-1}h(ax)\in k$. پس $K\trianglelefteq G$. از طرفی واضح است که $H\subseteq K$. بنابراین طبق تعریف H^G، $H^G\subseteq K$. برعکس فرض کنید $H\subseteq N\trianglelefteq G$. پس برای هر $h\in H$ داریم $h\in N$. از این‌رو برای هر $a\in G$، $a^{-1}ha\in N$. پس هر مولد K

در N قرار دارد. بنابراین $K \subseteq N$ و $K \subseteq \bigcap\{N \mid H \subseteq N \trianglelefteq G\} = H^G$.
(ج) طبق (ب) $H^G = \langle a^{-1}ha \mid a \in G, \ \ h \in H\rangle$. حال اگر $a^{-1}ha$ مولدی از H^G باشد می‌توان نوشت

$$a^{-1}ha = hh^{-1}a^{-1}ha = h[h,a] \in H[H,G].$$

پس $H^G \subseteq H[H,G]$. برای عکس مطلب، می‌دانیم $H \subseteq H^G$، و اگر $[h,a]$ مولدی از $[H,G]$ باشد، داریم $[h,a] = h^{-1}a^{-1}ha = h^{-1}(a^{-1}ha) \in H^G$. بنابراین $H[H,G] \subseteq H^G$.

تمرین‌های ۸.۳، هم‌مجموعه‌ها و قضیه‌ی لاگرانژ، صفحه‌ی ۹۰

۱. از قضیه‌ی لاگرانژ استفاده کنید.

۲. نشان دهید در گروه $\mathbb{Z}^{\times}_{m^n-1}$، مرتبه‌ی $\bar{m}$ برابر n است و از قضیه‌ی لاگرانژ استفاده کنید.

۳. (الف) از $HK \subseteq \langle H,K\rangle$ نتیجه بگیرید $\frac{|HK|}{|K|} \leq \frac{|\langle H,K\rangle|}{|K|}$. بنابراین $\frac{|H|}{|H\cap K|} \leq |\langle H,K\rangle : K|$ و $|H : H\cap K| \leq |\langle H,K\rangle : K|$.
(ب) طبق فرض و (الف) داریم $\frac{1}{2}|G : K| < |H : H\cap K| < |\langle H,K\rangle : K|$. نتیجه بگیرید $\frac{1}{2}|G| < |\langle H,K\rangle|$ و $|G : \langle H,K\rangle| < 2$. پس $|G : \langle H,K\rangle| = 1$ و $G = \langle H,K\rangle$.

۴. (الف) فرض کنید $X = \{x(H\cap K) \mid x \in H\}$ و $Y = \{yK \mid y \in G\}$، به ترتیب، مجموعه‌ی چپ هم‌مجموعه‌های $H\cap K$ در H و مجموعه‌ی هم مجموعه‌های چپ K در G هستند. نشان دهید تابع $f : X \longrightarrow Y$ با ضابطه‌ی $f(x(H\cap K)) = xK$، خوشتعریف و یک‌به‌یک است. پس $|H : H\cap K| = |X| \leq |Y| = |G : K|$.
(ب) اگر $G = HK$ تابع f در (الف) پوشا نیز هست، بنابراین $|H : H\cap K| = |G : K|$.

۵. از لم پوانکاره استفاده کنید و نشان دهید $|G : H\cap K| = |G : H||G : K|$. سپس از این که G متناهی است استفاده کنید.

۶. اگر $M \leq K \leq G$، از این که $p = |G : M| = |G : K||K : M|$ استفاده کنید.

۸. فرض کنید $\mathrm{orb}(X) = \{g^{-1}Xg \mid g \in G\}$ مجموعه‌ی مزدوج‌های X در G و $T = \{N_G(X)g \mid g \in G\}$ مجموعه‌ی هم مجموعه‌های چپ $N_G(X)$ در G باشد، تابع $f : T \longrightarrow \mathrm{orb}(X)$ را با ضابطه‌ی $f(N_G(X)g) = g^{-1}Xg$ تعریف کنید و نشان دهید f خوش‌تعریف، یک‌به‌یک و پوشا است.

۱۰. فرض کنید $|G| = n$ و $G = \{x_1, x_2 \ldots, x_m, \ldots, x_n\}$، که در آن $m > \frac{3}{4}|G|$ و ازای هر $1 \leq i \leq m$، $f(x_i) = x_i^{-1}$. داریم $x_1G = G$. ابتدا نشان می‌دهیم G آبلی است. قرار می‌دهیم

$$A = \{x_1x_j \mid 1 \leq j \leq n, \quad f(x_1x_j) = (x_1x_j)^{-1}\}.$$

بنابراین داریم

$$\begin{aligned} |A| \ &\geq \ (1 \leq j \leq m \text{ که } x_1x_j \text{ها} \text{ تعداد }) - \\ &\quad \text{(حداکثر تعداد اعضای } G \text{ که ممکن است تحت } f \text{ به معکوس‌هایشان نروند)} \\ &\geq \ m - (n-m) = 2m - n > 2 \times \frac{3}{4}n - n = \frac{n}{2}. \end{aligned}$$

بنابراین $|A| > |G|/2$. حال اگر $x_1x_j \in A$، $1 \leq j \leq m$، داریم $f(x_j) = x_j^{-1}$ و $f(x_1) = x_1^{-1}$. پس

$$f(x_1x_j) = f(x_1)f(x_j) = x_1^{-1}x_j^{-1} = (x_jx_1)^{-1}.$$

از طرفی چون $x_1x_j \in A$، خواهیم داشت $f(x_1x_j) = (x_1x_j)^{-1}$، که به همراه رابطه‌ی فوق نتیجه می‌دهد $(x_jx_1)^{-1} = (x_1x_j)^{-1}$. یعنی $x_ix_1 = x_1x_j$ و $x_j \in C_G(x_1)$. پس $|C_G(x_1)| \geq |A| > |G|/2$ و در نتیجه $|C_G(x_1)| = |G|$. بنابراین $G = C_G(x_1)$،

یعنی $x_1 \in Z(G)$. به همین نحو برای هر x_i که $1 \leq i \leq m$، نتیجه می‌شود $x_i \in Z(G)$. پس $|Z(G)| \geq \frac{3}{4}n$. بنابراین $G = Z(G)$ و G آبلی است. اکنون مجموعه‌ی $K = \{a \in G \mid f(a) = a^{-1}\}$ را در نظر می‌گیریم. ثابت کنید $K \leq G$. چون طبق فرض $|K| > \frac{3}{4}|G|$، داریم $K = G$ و حکم ثابت است. برای مثال خواسته شده تابع $f : D_8 \longrightarrow D_8$ را با $f(\rho) = \rho^3$ و $f(\varepsilon) = \varepsilon$ را در نظر بگیرید: $f(\rho^i\varepsilon^j) = \rho^{3i}\varepsilon^j$.

۱۱. (الف) فرض کنید $a \in G$، $O(a) = s$. در این صورت $H = \langle a \rangle$ یکتا زیرگروه G از مرتبه‌ی s است. از طرف دیگر برای هر $h \in H$ داریم $h^s = 1$. پس $H \subseteq G_s$. ثابت کنید G_s زیرگروه G است و نتیجه بگیرید G_s یکتا زیرگروه G، و لاجرم یکتا زیرگروه H از مرتبه‌ی t است، $t = s$ و $G_s = H$.

(ب) فرض کنید $s|n$، پس زیرگروه یکتای $G_s = \langle g \rangle = \{x \in G \mid x^s = 1\}$ وجود دارد که $|G_s| = s$. اکنون چون

$$\begin{aligned} \langle g \rangle = \left\langle g^k \right\rangle &\iff \exists m \in \mathbb{Z}, \quad g = g^{mk} \\ &\iff s|(mk-1) \\ &\iff \gcd\{s,k\} = 1, \end{aligned}$$

عناصر مرتبه‌ی s در G دقیقاً برابر $\varphi(s)$ است. پس تعداد عناصر G برابر مجموع $\varphi(s)$ است، وقتی $s|n$. یعنی $n = \sum_{s|n} \varphi(s)$.

(ج) فرض کنید G عضو مرتبه‌ی n ندارد. اگر $g \in G$ و $O(g) = s$، آنگاه $|\langle g \rangle| = s$. بنابراین $\langle g \rangle$ یکتا زیرگروه G از مرتبه‌ی s است (بنا به فرض). پس عناصر مرتبه‌ی s در $\langle g \rangle$ قرار دارند و تعداد $\varphi(s)$ عضو مرتبه‌ی s در G وجود دارد. بنابراین $n = \sum_{s|n} s < n$ و این متناقض با (ب) است.

۱۲. فرض کنید X یک مجموعه‌ی مولد برای G باشد. به ازای هر $x \in X$، با اضافه کردن x^{-1} به X، می‌توان فرض کرد که X تحت وارون بسته است. فرض کنید T یک پیمایش راست برای H در G باشد طوری که $1 \in T$. پس به ازای هر $x \in X$ و $t \in T$، عضو $t' \in T$ وجود دارد که $tx \in Ht'$. قرار می‌دهیم $h_{x,t} = txt'^{-1} \in H$ و $S = \{h_{x,t} \mid x \in X, \ t \in T\}$، آنگاه $|S| < \infty$. نشان می‌دهیم $H = \langle S \rangle$. عضو دلخواه $h = x_1x_2\cdots x_n \in H$ را در نظر می‌گیریم، که در آن $x_i \in X$. به ازای هر $i \leq n$، عناصر $t_i \in T$ را چنین تعریف می‌کنیم: $t_1 = 1$ و $t_ix_i \in Ht_{i+1}$. پس $Ht_ix = Ht_{i+1}$. از این رو $Ht_{n+1} = Ht_nx_n = Ht_{n-1}x_{n-1}x_n = \cdots = Hx_1\cdots x_n = Hh = H$. بنابراین $t_{n+1} = 1$ و داریم

$$\begin{aligned} h &= t_1x_1(t_2^{-1}t_2)x_2(t_3^{-1}t_3)\cdots(t_n^{-1}t_n)x_nt_n^{-1} \\ &= (t_1x_1t_2^{-1})(t_2x_2t_3^{-1})\cdots(t_nx_nt_{n+1}^{-1}) \in \langle S \rangle \end{aligned}$$

۱۳. چون $G = \langle g_1, g_2 \ldots, g_n \rangle$ داریم $Z(G) = \bigcap_{i=1}^n C_G(g_i)$. اکنون از این که $|G : C_G(g_i)| \leq m$ و لم پوانکاره استفاده کنید.

۱۴. (الف) طبق مساله‌ی ۸ تعداد مزدوج‌های H در G عبارت است از $|G : N_G(H)|$ و چون $H \leq N_G(H)$ داریم $|G : N_G(H)| \leq |G : H|$. هم چنین چون ۱ در تمامی مزدوج‌های H قرار دارد خواهیم داشت

$$\left|\bigcup_{g\in G} g^{-1}Hg\right| \leq 1 + (|H|-1)|G : N_G(H)| \leq |H|(|H|-1)|G : H|.$$

(ب) طبق (الف) اگر $H < G$ داریم $\bigcup_{g\in G} g^{-1}Hg \subset G$. پس $x \in G - \bigcup_{g\in G} g^{-1}Hg$ وجود دارد. بنابراین برای هر $g \in G$، $x \notin g^{-1}Hg$. پس برای هر $g \in G$، $gxg^{-1} \notin H$ و این یعنی $\mathrm{orb}(x) \cap H = \emptyset$ که خلاف فرض است. پس $H = G$.

۱۵. چون $\mathrm{orb}(1) = \{1\}$، داریم $1 \in FC(G)$. حال اگر $x, y \in FC(G)$، آنگاه $|\mathrm{orb}(x)| < \infty$ و $|\mathrm{orb}(y)| < \infty$. نشان دهید توابع

$$\begin{aligned} &f : \mathrm{orb}(xy) \to \mathrm{orb}(x) \times \mathrm{orb}(y) \\ &f\left(a^{-1}(xy)a\right) = \left(a^{-1}xa, a^{-1}ya\right) \end{aligned}$$

$x \in FC(G)$ و $\alpha \in \operatorname{Aut} G$ اگر $g : \operatorname{orb}(x^{-1}) \longrightarrow \operatorname{orb}(x)$ با $f(a^{-1}x^{-1}a) = a^{-1}xa$ یک‌به‌یک و پوشا هستند. اکنون $\alpha(\operatorname{orb}(x))$ متناهی است، چون $\operatorname{orb}(x)$ متناهی و α یک‌به‌یک است. نشان دهید $\alpha(\operatorname{orb}(x)) = \operatorname{orb}(\alpha(x))$ و نتیجه بگیرید $\alpha(x) \in FC(G)$. پس $FC(G)$ زیرگروه مشخصه‌ی G است.

۱۶. اگر G یک FC- گروه G باشد، و $H \leq$. اگر $h \in H$، چون

$$\{a^{-1}ha \mid a \in H\} \subseteq \{a^{-1}ha \mid a \in G\}$$

نتیجه می‌گیریم که $|\{a^{-1}ha \mid a \in H\}| \leq |\{a^{-1}ha \mid a \in G\}| < \infty$. پس H یک FC- گروه است.

۱۷. فرض کنید $G = \langle g_1, \ldots, g_n \rangle$، بنابراین داریم $Z(G) = \bigcap_{i=1}^{n} C_G(g_i)$ و با استفاده از لم پوانکاره و این که $|G_i : C_G(g_i)| < \infty$، نشان دهید $|G : Z(G)| < \infty$.

۱۸. اگر $a \in G$، نشان دهید $|G : Z(G)| = |G : C_G(a)||C_G(a) : Z(G)|$ و از $|G : Z(G)| < \infty$ نتیجه بگیرید $|G : C_G(a)| < \infty$.

۱۹. فرض کنید $Z(G) = 1$ و x_1، ...، x_{k-1} همه‌ی نماینده‌های رده‌های مزدوجی بیش از دو عضوی باشند. بنا به معادله‌ی رده‌ای داریم $|G| = 1 + \sum_{i=1}^{k-1} |G : C_G(x_i)|$. چون p کوچک‌ترین عدد اول شمارنده‌ی $|G|$ است و $|G| \mid |G : C_G(x_i)|$، داریم $|G : C_G(x_i)| \geq p$. پس $|G| \geq 1 + (k-1)p > (k-1)p$. از طرفی طبق فرض داریم $k > \dfrac{|G|}{p}$ که نتیجه می‌دهد $k > \dfrac{|G|}{p} > k - 1$ و این تناقض است، زیرا $|G|/p$ عددی صحیح است.

تمرین‌های ۹.۳، گروه‌های خارج‌قسمتی، صفحه‌ی ۹۴

۱. فرض کنید $X = \{aH \mid a \in G\}$ تحت عمل $(aH)(bH) = abH$ یک گروه تشکیل دهد. فرض کنید $a \in G$ و $h \in H$ در این صورت چون $hH = H$ و H عضو بی‌اثر X است داریم $(aH)H = H(aH) = (hH)(aH)$ بنابراین طبق تعریف عمل ضرب در X، $aH = haH$ و طبق تساوی هم‌مجموعه‌ها $a^{-1}ha \in H$. بنابراین $H \trianglelefteq G$.

۳. از این که اعداد صحیح c_2 و c_1 وجود دارند که $c_1m + c_2n = 1$، هم چنین از این که $g^n \in H$، استفاده کنید.

۴. (الف) چون $O(x) = n$، داریم $x^n = 1$ و $(xK)^n = x^nK = K$. اگر $t = O(xK)$، آنگاه $t|n$. حال چون $K = (xK)^t = x^tK$، داریم $x^t \in K$؛ و چون $|K| = m$، داریم $(x^t)^m = 1$. بنابراین $n|mt$. چون $\gcd\{m, n\} = 1$، داریم $n|t$. پس $n = t$ و حکم ثابت است.
(ب) از این که اعداد صحیح c_2 و c_1 وجود دارند که $c_1m + c_2n = 1$، و این که $x^n \in K$ استفاده کنید. قرار دهید $y = x^{c_1m}$.

۶. فرض کنید $G/Z(G) = \langle aZ(G) \rangle$. اگر $x \in G$، آنگاه $xZ(G) \in Z/Z(G)$. پس $n \in \mathbb{Z}$ وجود دارد که $xZ(G) = (aZ(G))^n$. بنابراین $z = a^{-n}x \in Z(G)$. اکنون اگر $x, y \in G$، آنگاه اعضای $z_1, z_2 \in Z(G)$ و $n_1, n_2 \in \mathbb{Z}$ وجود دارند که $x = a^{n_1}z_1$ و $y = a^{n_2}z_2$. نشان دهید $xy = yx$.
اگر $|G| = p^2$، از این که $Z(G) \neq 1$ استفاده کنید.

۱۰. اگر $aH, bH \in G/H$، داریم

$$[aH, bH] = (aH)^{-1}(bH)^{-1}aHbH = a^{-1}b^{-1}abH = [a, b]H.$$

پس هر مولد $(G/H)' = [G/H, G/H]$ در $\dfrac{G'H}{H}$ قرار دارد. برعکس هر مولد $\dfrac{G'H}{H}$ نیز در $[G/H, G/H]$ قرار دارد. از این‌رو $(G/H)' = \dfrac{G'H}{H}$. بنابراین به طور استقرایی به دست می‌آوریم $(G/H)^{(n)} = \dfrac{G^{(n)}H}{H}$. حال اگر Gحل‌پذیر باشد، آنگاه به ازای nای، $G^{(n)} = \{1\}$. بنابراین $(G/H)^{(n)} = \dfrac{H}{H} = \{H\}$ و G/Hحل‌پذیر است.

۱۱. اگر Gحل‌پذیر باشد و $H \lhd G$، آنگاه H، G/H حل‌پذیرند. برعکس اگر H و G/Hحل‌پذیر باشند، آنگاه n و m وجود دارند که $H^{(n)} = \{۱\}$ و $(G/H)^{(n)} = \{H\}$. طبق حل تمرین قبل داریم $(G/H)^{(m)} = \dfrac{G^{(m)}H}{H}$، پس $G^{(m)} \subseteq G^{(m)}H \subseteq H$. در نتیجه $G^{(m+n)} \subseteq H^{(n)} = \{۱\}$ و Gحل‌پذیر است.

۱۳. (الف) فرض کنید $a, b \in G$، آنگاه

$$\begin{aligned}(aG')(bG') = (bG')(aG') &\iff abG' = baG' \\ &\iff (ba)^{-۱}ab \in G' \\ &\iff a^{-۱}b^{-۱}ab \in G'.\end{aligned}$$

(ب) فرض کنید H مجموعه‌ی اعضای با مرتبه‌ی متناهی در G باشد. اگر $a, b \in H$، آنگاه $m, n \in \mathbb{N}$ وجود دارند که $a^n = ۱$، $b^m = ۱$. از این که G/G' آبلی است نتیجه بگیرید $(ab)^{mn} \in G'$. چون G' تاب‌دار است، $O((ab)^{mn})$ متناهی است و بنابراین $O(ab) < \infty$.

۱۴. اگر $n = ۱$، $G = \{۱\}$ سری مورد نظر است. فرض کنید حکم برای n برقرار باشد و حالت $n+۱$ را در نظر می‌گیریم. فرض کنید $|G| = p^{n+۱}$. چون $Z(G) \neq \{۱\}$، بنا به قضیه‌ی کُشی عضو $a \in Z(G)$ وجود دارد که $o(a) = p$. قرار می‌دهیم $G_n = \langle a\rangle$، در این صورت $G_n \trianglelefteq G$ و $|G/G_n| = p^n$. پس بنا به فرض استقرا سری

$$\frac{G}{G_n} \supset \frac{G_۱}{G_n} \supset \frac{G_۲}{G_n} \supset \cdots \supset \frac{G_{n-۱}}{G_n} = \{G_n\}$$

از زیرگروه‌های نرمال G/G_n وجود دارد که $|G_i/G_{i+۱}| = \left|\dfrac{G_i/G_n}{G_{i+۱}/G_n}\right| = p$. بنابراین $G_i \trianglelefteq G$ و سری

$$G = G_۰ \supset G_۱ \supset G_۲ \supset \cdots G_{n-۱} \supset G_n \supset G_{n+۱} = \{۱\}$$

همه‌ی خواص مورد نظر را دارد.

۱۵. با استفاده از معادله‌ی رده‌ای، داریم $|G| = |Z(G)| + \sum_{i=۱}^{k} |G : C_G(x_i)|$، که در آن $x_۱$، ...، x_k نماینده‌های رده‌های مزدوجی‌اند که بیش از دو عضو دارند. اگر $|G| = ۱$، حکم به انتفای مقدم ثابت است. پس فرض کنید حکم برای همه‌ی گروه‌های با مرتبه‌ی کمتر از $|G|$ درست باشد. اگر به ازای هر $۱ \leq i \leq n$، $p \mid |G : C_G(x_i)|$، آنگاه $p \mid \sum_{i=۱}^{n} |G : C_G(x_i)|$ و $p \mid (|G| - \sum_{i=۱}^{k} |G : C_G(x_i)|)$. بنابراین $p \mid |Z(G)|$ و بنا به قضیه‌ی کُشی برای گروه‌های آبلی، $Z(G)$ عضوی چون a از مرتبه‌ی p دارد. قرار می‌دهیم $N = \langle a\rangle$. چون $N \leq Z(G)$، داریم $N \trianglelefteq G$. پس $|G/N| = \dfrac{|G|}{|N|} = p^{n-۱}m$ و بنا به فرض استقرا، G/N زیرگروهی چون P/N از مرتبه‌ی $p^{n-۱}$ دارد. پس $|P| = |P/N||N| = p^{n-۱}mp = p^n m$ و P یک زیرگروه مرتبه‌ی p^n از G است. بنابراین فرض کنید به ازای یک $۱ \leq j \leq m$، $p \nmid |G : C_G(x_j)|$. چون $|G| = |G : C_G(x_j)||C_G(x_j)|$، داریم $|C_G(x_i)| = p^n k$، که در آن $p \nmid k$. پس بنا به فرض استقرا $C_G(x_i)$ و لاجرم G زیرگروهی از مرتبه‌ی p^n دارد.

۱۶. (الف) اگر $|\mathbb{Q}/H| = n$، آنگاه به ازای هر $a \in \mathbb{Q}$ داریم $n(a+H) = H$ و $na \in H$. حال اگر $\dfrac{r}{s} \in \mathbb{Q}$ عدد گویای دلخواهی باشد، آنگاه $\dfrac{r}{ns} \in \mathbb{Q}$ و $\dfrac{r}{s} = n\dfrac{r}{ns} \in H$؛ یعنی $H = \mathbb{Q}$، که متناقض با سره بودن H در $\mathbb{Q}$ است.

۱۷. فرض کنید $M < \mathbb{Q}$ یک زیرگروه ماکسیمال $\mathbb{Q}$ باشد. آنگاه $a \in \mathbb{Q} - M$ وجود دارد. بنابراین داریم $M < M + \langle a\rangle \leq \mathbb{Q}$. چون M ماکسیمال است و $a \notin M$، داریم $\mathbb{Q} = M + \langle a\rangle$. برای $x \in \mathbb{Q}$ عضو $y \in M$ و $n \in \mathbb{Z}$ وجود دارد که $x = y + na$. پس

$$x + M = (y + na) + M = (y + M) + (na + M) = n(a + M),$$

و $\mathbb{Q}/M \leq \langle a + M\rangle$. بنابراین $\mathbb{Q}/M$ دوری است که متناقض با تمرین ۱۶ است.

۱۹. چون G ناآبلی است، $Z(G) < G$. اگر $|Z(G)| = p^۲$، آنگاه $|G/Z(G)| = p$. پس G دوری و در نتیجه آبلی است؛ که تناقض است. پس $|Z(G)| = p$. از این‌رو معادله‌ی رده‌ای $|G| = |Z(G)| + \sum_{i=۱}^{k} |G : C_G(x_i)|$، که در آن $x_۱$، ...، x_k نماینده‌های

رده‌های مزدوجی‌اند که بیش از دو عضو دارند، به صورت $p^۳ = p + \sum_{i=۱}^{k} |G : C_G(x_i)|$ در می‌آید. چون $|G : C_G(x_i)| > ۱$، داریم $Z(G) \subset C_G(x_i) \subset G$. بنابراین $|C_G(x_i)| = p^۲$ و $|G : C_G(x_i)| = p$. پس $p^۳ = p + kp$، یعنی $k = p^۲ - ۱$ و

$$k(G) = |Z(G)| + k = p + p^۲ - ۱.$$

۲۰. (الف) چون $H \trianglelefteq G$، H اجتماعی از رده‌های مزدوجی G است، مثلاً فرض کنید $H = \bigcup_{i=۱}^{n} \operatorname{orb}(t_i)$. اگر $\operatorname{orb}(x_kH)$، ...، $\operatorname{orb}(x_۱H)$ رده‌های مزدوجی متمایز G/H باشند، که در آن $x_۱ = ۱$، آنگاه $\operatorname{orb}(t_۱)$، ...، $\operatorname{orb}(t_n)$، $\operatorname{orb}(x_۱)$، ...، $\operatorname{orb}(x_k)$، $k + j - ۱$ رده‌های مزدوجی متمایز G هستند. بنابراین $k + j - ۱ \leq k(G)$.
(ب) چون $G/Z(G)$ آبلی است، هر رده‌ی مزدوجی $G/Z(G)$ یک عضوی است. در نتیجه تعداد رده‌های مزدوجی دقیقاً برابر تعداد اعضا است: $k(G/Z(G)) = |Z(G/Z(G))|$. بنابراین بنا به (الف) داریم

$$|G/Z(G)| = k(G/Z(G))| \leq k(G) - k(Z(G)) + ۱.$$

۲۲. چون برای هر $a \in G$، $x^{-۱}a^{-۱}xa \in G'$، داریم $a^{-۱}xa \in xG'$. در نتیجه $\operatorname{orb}(x) \subseteq xG'$. پس $|G : C_G(x)| = |\operatorname{orb}(x)| \leq |xG'| = |G'|$. بنابراین $\frac{|G|}{|C_G(x)|} \leq |G'|$ و $|C_G(x)| \leq \frac{|G|}{|G'|}$. و چون $G' \lhd G$ داریم $|G/G'| \leq |C_G(x)|$

۲۳. فرض کنید $x \in G$. آنگاه $|G : C_G(x)| < \infty$. اگر $T = \{t_۱, \ldots, t_k\}$ یک پیمایش راست $C_G(x)$ در G باشد، آنگاه $G = C_G(x)T$. قرار می‌دهیم $H = \bigcap_{i=۱}^{k} C_G(t_i)$. چون G یک FC- گروه است، با استفاده از لم پوانکاره نشان دهید $|G : H| < \infty$ و نتیجه بگیرید $|G : H_G| = m < \infty$. پس $x^m \in H_G \subseteq H = \bigcap_{i=۱}^{k} C_G(t_i)$ و x^m با همه‌ی t_iها تعویض می‌شود. چون x^m با عناصر $C_G(x)$ نیز تعویض می‌شود و $G = C_G(x)T$، داریم $x^m \in Z(G)$. پس $(xZ(G))^m = Z(G)$. بنابراین $G/Z(G)$ تاب‌دار است.

۲۵. ابتدا ثابت کنید G، FC- گروه است. سپس نشان دهید G، بی‌تاب است. با استفاده از مساله‌های **۲۳** و **۲۴** ثابت کنید G آبلی است. اکنون عضو دلخواه $a \in G \neq ۱$ را در نظر بگیرید که $\langle a \rangle < G$. پس طبق فرض $|G : \langle a \rangle| = n < \infty$. بنابراین به ازای هر $x \in G$، $x^n \in \langle a \rangle$. پس $G^n = \langle x^n \mid x \in G \rangle \subseteq \langle a \rangle$. نشان دهید تابع $f : G \longrightarrow G$ با ضابطه‌ی $f(x) = x^n$ همریختی یک‌به‌یک است و نتیجه بگیرید G با زیرگروهی از گروه دوری نامتناهی $\langle a \rangle$ یکریخت است. پس G دوری نامتناهی است.

تمرین‌های ۱۰.۳، قضیه‌ی یکریختی، صفحه‌ی ۹۷

۱. اگر $\operatorname{Aut} G$ دوری باشد، آنگاه $\operatorname{Inn} G$ نیز دوری است. اما $\operatorname{Inn} G \cong G/Z(G)$. بنابراین $G/Z(G)$ دوری و G آبلی است.

۲. فرض کنید $\operatorname{Aut} G$ دوری با مرتبه‌ی فرد بیش از یک باشد. در این صورت طبق تمرین قبل G آبلی است. اگر به ازای یک $x \in G$، $x^۲ \neq ۱$، آنگاه تابع $f : G \longrightarrow G$ با ضابطه‌ی $f(a) = a^{-۱}$ یک خودریختی نابدیهی است و $O(f) = ۲$. پس $۲ \mid |\operatorname{Aut} G|$، که تناقض است. پس فرض کنید به ازای هر $x \in G$، $x^۲ = ۱$. در این صورت $G \cong (V, +)$، که در آن V یک فضای برداری روی $\mathbb{Z}_۲$ است. از این‌رو به ازای یک $n \in \mathbb{N}$، $|G| = ۲^n$ و $\operatorname{Aut} G \cong \operatorname{Aut} V \cong \mathrm{GL}_n(\mathbb{Z}_۲)$. پس $\operatorname{Aut} G$ حتی آبلی نیست، که تناقض است.

۳. تابع $f : N_G(H) \longrightarrow \operatorname{Aut} H$ را با ضابطه‌ی $f(a) = \tau_a|_H$ تعریف کنید. نشان دهید f خوش تعریف یک‌به‌یک و همریختی است؛ و $\ker f = C_G(H)$. سپس از اولین قضیه‌ی یکریختی استفاده کنید.

۴. از تمرین قبل استفاده کنید و نشان دهید

$$G/C_G(K) = N_G(K)/C_G(K) \hookrightarrow \operatorname{Aut} K \cong \operatorname{Aut} Z_p \cong \mathbb{Z}_p^{\times}$$

نتیجه بگیرید $|G/C_G(K)| \mid (p - ۱)$ و $G = C_G(K)$، یعنی $K \leq Z(G)$.

۵. فرض کنید $H \neq \{۱\}$ زیرگروه نرمال و متناهی از G باشد. از تمرین **۳** استفاده کرده و نشان دهید $G/C_G(H)$ متناهی است. اما چون طبق فرض G هیچ گروه خارج قسمتی متناهی نابدیهی ندارد ، نتیجه بگیرید $G = C_G(H)$ و $H \leq Z(G)$.

تمرین‌های ۱.۴، حاصل‌ضرب مستقیم گروه‌ها، صفحه‌ی ۱۰۴

۲. تابع f با ضابطه‌ی $f(a)=\left(|a|,\frac{a}{|a|}\right)$ را در نظر بگیرید.

۶. تابع f با ضابطه‌ی $f(A)=\left(\det A,\frac{۱}{(\det A)^n}A\right)$ را در نظر بگیرید.

۷. تابع f با ضابطه‌ی $f(A)=(a_{۱۱},a_{۲۲},\dots,a_{nn})$ را در نظر بگیرید، $A=[a_{ij}]$، $a_{ij}=۰$، $i\neq j$.

۸. اگر Gحل‌پذیر باشد، هر زیرگروه آن نیز حل‌پذیر است. برعکس اگر زیرگروه‌های H و Kحل‌پذیر باشند، چون $H\cong\frac{H}{H\cap K}=\frac{HK}{K}$ و $\frac{G}{K}$ حل‌پذیرند، Gحل‌پذیر است.

۹. (الف) تابع f با ضابطه‌ی $f(\alpha,\beta)=f_{\alpha,\beta}$ را در نظر بگیرید که در آن $f_{\alpha,\beta}:G\longrightarrow G$ تابعی با ضابطه‌ی $f_{\alpha,\beta}(hk)=\alpha(h)\beta(k)$ است.
(ب) فرض کنید $\gamma\in\operatorname{Aut}G$، آنگاه طبق فرض داریم $\alpha=\gamma|_H\in\operatorname{Aut}(H)$ و $\beta=\gamma|_K\in\operatorname{Aut}(K)$. بنابراین $f_{\alpha,\beta}=\gamma$ و تابع f پوشاست.

۱۰. (الف) از تمرین ۳ استفاده کنید.
(ب) از تمرین ۷ (الف) استفاده کنید.

۱۱. اگر $|G|=p_۱^{n_۱}p_۲^{n_۲}\cdots p_k^{n_k}$ قرار دهید $H_i=\{g\in G\mid g^{p^{n_i}}=۱\}$. اگر $m_i=\frac{p_۱^{n_۱}\cdots p_k^{n_k}}{p_i^{n_i}}$، آنگاه $\gcd\{m_۱,\dots,m_k\}=۱$. پس اعداد صحیح $c_۱$، $\dots$، c_k وجود دارند که $c_۱m_۱+\cdots+c_km_k=۱$. نتیجه بگیرید به ازای هر $g\in G$، $g=h_۱h_۲\cdots h_k$، که در آن $h_i\in H_i$. به علاوه با استفاده از این که مرتبه‌ی H_iها نسبت به هم اول‌اند، نتیجه بگیرید $H_j\cap H_i\cdots H_{j-۱}H_{j+۱}\cdots H_k=\{۱\}$.

تمرین‌های ۲.۴، حاصل‌ضرب نیم‌مستقیم، صفحه‌ی ۱۰۸

۱. هر دو زیرگروه نابدیهی $Q_۸$ اشتراک نابدیهی دارند.

۳. (الف) اگر $\alpha,\beta\in\operatorname{Aut}H$ و $a,b\in H$، آنگاه

$$(a\alpha)(b\beta)=a\varepsilon_\alpha(b)\alpha\beta=(a\alpha(b))\alpha\beta.$$

(ب) همواره داریم $H\trianglelefteq H\rtimes K$، پس $H\trianglelefteq\operatorname{Hol}H$.
(ج) اگر $H=\langle a\rangle$ گروه دوری مرتبه‌ی ۳ باشد، آنگاه $\operatorname{Aut}H\cong\mathbb{Z}_۳^\times\cong\mathbb{Z}_۲$. بنابراین $|\operatorname{Hol}H|=|H||\operatorname{Aut}H|=۶$. داریم $\operatorname{Aut}H=\{\mathrm{id}_H,\alpha\}$، که در آن $\alpha(a)=a^۲$. بنابراین $\operatorname{Hol}H=\{۱,a,a^۲,\alpha,a\alpha,a^۲\alpha\}$. تابع f را با ضابطه‌ی $f(a)=(۱\ ۲\ ۳)$، $f(\alpha)=(۱\ ۲)$ تعریف کنید.

۴. اگر $A=\langle a\rangle\cong C_n$، تابع $f:D_{۲n}\longrightarrow\operatorname{Dih}A$ با $f(\rho^i\varepsilon^j)=a^i\eta^j$ را در نظر بگیرید. اگر $A=\langle a\rangle\cong\mathbb{Z}$، تابع $f:D_\infty\longrightarrow\operatorname{Dih}A$ با $f(\tau^n\varepsilon^m)=a^n\varepsilon^m$ را در نظر بگیرید.

۵. (الف) خودریختی $\eta:A\longrightarrow A$ با $\eta(a)=a^{-۱}$ را در نظر می‌گیریم در این صورت $D=\operatorname{Dih}A=A\rtimes\langle\eta\rangle$. داریم

$$(a\eta)^۲=a\eta a\eta=a\varphi_\eta(a)\eta\eta=a\eta(a)=aa^{-۱}=۱$$

(ب) اگر $a\in A$، آنگاه

$$a\eta=\eta a\iff a\eta=\eta(a)\eta\iff a^۲=۱$$

چون $D = A\langle\eta\rangle$ و A آبلی است. پس $T = \{a \in A \mid a^۲ = ۱\} \subseteq Z(D)$. از طرفی چون عضوی مثل b در A وجود دارد که $b^۲ \neq ۱$، $b\eta \neq \eta b$. پس $\eta \notin Z(D)$. اگر $a\eta \in Z(D)$ نتیجه بگیرید $a^۲ = ۱$، و $a^۲ \in Z(D)$؛ بنابراین $\eta \in Z(D)$ که تناقض است. در نتیجه $a\eta \notin Z(D)$ و $A \subseteq Z(D)$. بنابراین $T = Z(D)$.

(ج) فرض کنید $\alpha \in \operatorname{Aut} D$ و $a \in A$ باید ثابت کنیم $\alpha(a) \in A$. اگر $\alpha(a) = c\eta$، که در آن $c \in A$ آنگاه از (الف) نتیجه بگیرید $a^۲ = ۱$ و از (ب) نتیجه بگیرید $a \in Z(D)$. در نهایت چون مرکز یک گروه مشخصه است. $\alpha(a) \in Z(D)$ که متناقض با (ب) است.

(د) تابع $f : \operatorname{Hol} A \longrightarrow \operatorname{Aut} D$ را با ضابطه‌ی $f(a\beta) = \beta_a$ تعریف کنید که در آن $\beta_a : D \longrightarrow D$، $\beta_a(b) = \beta(b)$، $\beta_a(\eta) = a\eta$.

۸. بله: $S_n = A_n \rtimes \langle(۱\ ۲)\rangle$.

تمرین‌های ۱.۵، ۲.۵، ۳.۵، عمل گروه روی مجموعه، صفحه‌ی ۱۱۷

۱. برای هر $a, b \in \mathbb{R}$ و $z \in \mathbb{C}$ داریم

$$a \cdot (b \cdot z) = a \cdot (e^{ib}z) = e^{ia}(e^{ib}z) = e^{i(a+b)}z = (a+b) \cdot z,$$
$$۰ \cdot z = e^{۰i}z = z$$

اگر $z = re^{i\theta}$، داریم

$$\operatorname{orb}_{\mathbb{R}}(z) = \{re^{i(a+\theta)} \mid a \in \mathbb{R}\}$$
$$\operatorname{stab}_{\mathbb{R}}(z) = \{a \in \mathbb{R} \mid e^{ia} = ۱\} = \{۲\pi k \mid k \in \mathbb{Z}\}.$$

۲. عمل G/K روی X به صورت زیر است:

$$\forall gK \in G/K, \quad x \in X, \quad (gK) \cdot x = g \cdot x.$$

۳. G روی $X = \{xH \mid x \in G\}$، مجموعه‌ی هم‌مجموعه‌های چپ H در G، عمل می‌کند: $g \cdot (xH) = gxH$ و $\operatorname{stab}_G(۱H) = H$.

۴. داریم

$$\begin{aligned} a \in \operatorname{stab}_G(g \cdot x) &\iff a \cdot (g \cdot x) = g \cdot x \\ &\iff (ag) \cdot x = g \cdot x \\ &\iff g^{-۱}ag \in \operatorname{stab}_G(x). \end{aligned}$$

۵. چون $H \trianglelefteq G$، برای هر $g \in G$ و $x \in H$، $gxg^{-۱} \in H$. پس رابطه‌ی $g \cdot x = gxg^{-۱}$ یک عمل G روی H را مشخص می‌کند. ثابت ساز و مدار $x \in H$ عبارتند از

$$\operatorname{stab}_G(x) = C_G(x), \qquad \operatorname{orb}(x) = \{gxg^{-۱} \mid g \in G\}.$$

مدار $x \in H$ تک عضوی است اگر و تنها اگر برای هر $g \in G$، $g \cdot x = x$ اگر و تنها اگر برای هر $g \in G$، $gxg^{-۱} = x$ اگر و تنها اگر $x \in Z(G) \cap H$. حال اگر $\operatorname{orb}(x_۱)$، ...، $\operatorname{orb}(x_k)$، $\operatorname{orb}(y_۱)$، ...، $\operatorname{orb}(y_r)$ همه‌ی مدارهای متمایز عمل G روی H باشند طوری که $|\operatorname{orb}(x_i)| = ۱$ و $|\operatorname{orb}(y_i)| > ۱$، آنگاه H اجتماع مجزایی این مدارها است و

$$|H| = \sum_{i=۱}^{k} |\operatorname{orb}(x_i)| + \sum_{i=۱}^{r} |\operatorname{orb}(y_i)| = |Z(G) \cap H| + \sum_{i=۱}^{r} |G : C_G(y_i)|.$$

نتیجه بگیرید $p \mid |Z(G) \cap H|$ و $Z(G) \cap H \neq \{۱\}$.

۱۰. بنا به به لم پوانکاره، داریم $|G : H \cap K| \leq |G : H||G : K| < \infty$. پس زیرگروه نرمال M از G مشمول در $H \cap K$ وجود دارد طوری که G/M متناهی است. اکنون K/M و H/M زیرگروه‌های از گروه متناهی G/M هستند که

$$\gcd\left\{\left|\frac{G}{M} : \frac{H}{M}\right|, \left|\frac{G}{M} : \frac{K}{M}\right|\right\} = ۱$$

و بنا به لم پوانکاره داریم $\frac{G}{M} = \frac{H}{M}\frac{K}{M}$، که نتیجه می‌دهد، $G = HK$. از طرف دیگر داریم

$$\left|\frac{G}{M} : \frac{H \cap K}{M}\right| = \left|\frac{G}{M} : \frac{H}{M}\right| = \left|\frac{G}{M} : \frac{K}{M}\right|.$$

پس $|G : H \cap K| = |G : H||G : K|$.

۱۲. عمل G روی مجموعه‌ی زیرگروه‌های خود را با مزدوجی در نظر بگیرید.

۱۳. عمل G روی مجموعه‌ی X متشکل از همه‌ی زیرگروه‌های مرتبه‌های p^kی G را با مزدوجی در نظر بگیرید.

۱۴. اگر $H_۱$، $H_۲$، ...، H_m همه‌ی زیرگروه‌های با شاخص p در G باشند، آنگاه

$$p = |G : H_i| = |G : N_G(H_i)||N_G(H_i) : H_i|.$$

طبق قضایا داریم $H_i < N_G(H_i)$. بنابراین $G = N_G(H_i)$ و $H_i \trianglelefteq G$. در نتیجه G/H_i یک گروه آبلی با مرتبه‌ی p است. اکنون چون $H_i \trianglelefteq G$، به ازای هر i، داریم $K = \bigcap_{i=۱}^{m} H_i \trianglelefteq G$. هم چنین

$$G/K = G/\bigcap_{i=۱}^{m} H_i \hookrightarrow G/H_۱ \times \cdots \times G/H_m.$$

چون مرتبه‌ی هر عضو ناهمانی G/H_i برابر p است، مرتبه‌ی هر عضو ناهمانی نیز G/K برابر p است.

۱۵. فرض کنید $X = \{hkh^{-۱} \mid h \in H\}$، آنگاه H روی X با مزدوجی عمل می‌کند. این عمل ترایا است، زیرا $\mathrm{orb}_H(k) = \{hkh^{-۱} \mid h \in H\} = X$. از دیگر $\mathrm{stab}_H(k) = H \cap N_G(H)$. در نتیجه

$$|H : K \cap N_G(H)| = |H : \mathrm{stab}_H(k)| = |\mathrm{orb}_H(k)| = |X|.$$

۱۶. اگر $a, b \in H \cap K$، $(h, k) \in H \times K$ داریم

$$\begin{aligned}(ab) \cdot (h, k) &= (h(ab)^{-۱}, (ab)k) \\ &= (hb^{-۱}a^{-۱}, abk) \\ &= a \cdot (hb^{-۱}, ak) \\ &= a \cdot (b \cdot (h, k))\end{aligned}$$

و

$$۱ \cdot (h, k) = (h^{-۱}۱, ۱k) = (h, k).$$

پس $H \cap K$ روی $H \times K$ عمل می‌کند. ثابت ساز (h, k) عبارت است از

$$\mathrm{stab}_{H\cap K}(h, k) = \{a \in H \cap K \mid (ha^{-۱}, ak) = (h, k)\} = \{۱\}.$$

از این‌رو

$$|H \cap K| = |H \cap K : \mathrm{stab}_{H\cap K}(h, k)| = |\mathrm{orb}_{H\cap K}(h, k)|$$

و تعداد عناصر هر مدار برابر $|H \cap K|$ است. نشان دهید تابع $hk \mapsto \mathrm{orb}(h,k)$ از HK به مجموعه‌ی مدارها، خوش‌تعریف، یک‌به‌یک و پوشا است، پس تعداد مدارها برابر $|HK|$ است. چون $H \times K$ اجتماع مجزایی مدارهای متمایز است، هم چنین چون طول هر مدار برابر $|H \cap K|$ است، داریم $|H||K| = |H \times K| = |HK||H \cap K|$.

۱۷. اگر $(h_1,k_1) \in H \times K$ و (h_2,k_2) و $x \in G$، آن‌گاه

$$\begin{aligned}((h_1,k_1)(h_2,k_2)) \cdot x &= (h_1h_2, k_1k_2) \cdot x = h_1h_2, x(k_1k_2)^{-1} \\ &= h_1h_2, xk_2^{-1}k_1^{-1} = (h_1,k_1) \cdot (h_2xk_2^{-1}) \\ &= (h_1,k_1) \cdot [(h_2,k_2) \cdot x]\end{aligned}$$

و $x = 1x1^{-1} = (1,1) \cdot x$. پس $H \times K$ روی G عمل می‌کند. مدار $x \in G$ عبارت است از

$$\begin{aligned}\mathrm{orb}_{H\times K}(x) &= \{(h,k) \cdot x \mid (h,k) \in H \times K\} \\ &= \{hxk^{-1} \mid h \in H, \quad k \in K\} \\ &= \{hxt \mid h \in H, \quad k \in K\} \\ &= HxK.\end{aligned}$$

(b) داریم

$$|HxK| = |HxKx^{-1}| = \frac{|H||xKx^{-1}|}{|H \cap xKx^{-1}|} = \frac{|H||K|}{|H \cap xKx^{-1}|}$$

و به همین نحو

$$|HxK| = |x^{-1}HxK| = \frac{|H||K|}{|x^{-1}Hx \cap K|}.$$

از طرفی چون $|H \times K : \mathrm{stab}_{H\times K}(x)| = |\mathrm{orb}_{H\times K}(x)| = |HxK|$، داریم

$$|\mathrm{stab}_{H\times K}(x)| = \frac{|H \times K|}{|HxK|} = \frac{|H||K|}{|HxK|} = \frac{|H||K|}{\frac{|H||K|}{|H\cap xKx^{-1}|}} = |H \cap xHx^{-1}|$$

به همین صورت رابطه‌ی دیگر ثابت می‌شود.

(ج) چون G اجتماع مجزایی مدارهای متمایز است، با استفاده از (ب) داریم

$$|G| = \sum_{i=1}^{n} |Hx_iK| = \sum_{i=1}^{n} \frac{|H||K|}{|x_i^{-1}Hx_i \cap K|}.$$

۱۹. فرض کنید $\rho(g) = \rho_g$. اگر $x \in G$ داریم

$$\rho_g(x) = xg, \quad \rho_g(xg) = xg^2, \ldots, \rho_g(xg^{n-2}) = xg^{n-1}, \quad \rho_g(xg^{n-1}) = x.$$

پس در تجزیه‌ی ρ_g به دورهای مجزا n- دور $\alpha_x = (x \ xg \ xg^2 \ \cdots \ xg^{n-1})$ ظاهر می‌شود. اگر $y \in G$ طوری باشد که $y \neq xg^i$، آن‌گاه $\alpha_y = (y \ yg \ yg^2 \ \cdots \ yg^{n-1})$، یک دور دیگر به طول n در تجزیه‌ی ρ_g و مجزایی از α_x است. چون $|G| = mn$، این کار دقیقاً m بار قابل انجام است. بنابراین ρ_g به m دور مجزا به‌طول n تجزیه می‌شوند.

۲۰. (الف) فرض کنید $y \in X$. چون G روی X به صورت ترایا عمل می‌کند، $g \in G$ وجود دارد که $y = g \cdot x$. بنابراین

$$\mathrm{stab}_G(y) = \mathrm{stab}_G(g \cdot x) = g\mathrm{stab}_G(x)g^{-1} = g1g^{-1} = 1.$$

(ب) فرض کنید $x, y \in X$. چون G به صورت ترایا روی X عمل می‌کند، $g \in G$ وجود دارد که $y = g \cdot x$. از طرفی G آبلی است؛ پس

$$\mathrm{stab}_G(y) = \mathrm{stab}_G(g \cdot x) = g\mathrm{stab}_G(x)g^{-1} = \mathrm{stab}_G(x).$$

اکنون چون عمل صادق است، داریم $\bigcap_{x\in X} \mathrm{stab}_G(x) = \{1\}$. بنابراین بنا به رابطه‌ی فوق برای هر $x \in X$، $\mathrm{stab}_G(x) = \{1\}$.

۲۱. چون عمل G روی X ترایا است، $x \in X$ وجود دارد که $\mathrm{orb}_G(x) = X$. پس

$$|X| = |\mathrm{orb}_G(x)| = |G : \mathrm{stab}_G(x)| = \frac{|G|}{|\mathrm{stab}_G(x)|},$$

یعنی $|G| = |\mathrm{stab}_G(x)||X|$. اکنون اگر عمل G روی X معلوم باشد، آنگاه داریم $\mathrm{stab}_G(x) = \{1\}$. پس $|G| = |X|$. برعکس اگر داشته باشیم $|G| = |X|$، آنگاه $\mathrm{stab}_G(x) = \{1\}$. بنابراین بنا به تمرین قبل، عمل G روی X منظم است.

تمرین‌های ۴.۵، قضایای سیلو، صفحه‌ی ۱۲۴

۲. فرض کنید $|G| = ۱۷۵ = ۵^۲ \times ۷$. داریم $n_۵ | ۷$ و $n_۵ = ۱ + ۵k$ $(k \geq ۰)$. پس $n_۵ = ۱$ و دقیقاً یک ۵- زیرگروه سلوی P از G وجود دارد. از این‌رو $P \trianglelefteq G$. به طریق مشابه $n_۷ = ۱$ و ۷- زیرگروه سیلوی Q از G نیز در G نرمال است. چون مرتبه‌ی P و مرتبه‌ی Q نسبت به هم اول‌اند، $P \cap Q = \{1\}$. بنابراین $|PQ| = |P||Q| = |G|$ و $G = PQ$. پس $G = P \times Q$. چون P و Q آبلی‌اند، G نیز آبلی است.

۳. (الف) فرض کنید $|G| = ۵۶ = ۸ \times ۷$. آنگاه $n_۷ | ۸$. پس $n_۷$ برابر ۱ یا ۸ است. اگر $n_۷ = ۱$، آنگاه ۷- زیرگروه سیلوی G در G نرمال است پس فرض کنید $n_۷ = ۸$. چون اشتراک ۷- زیرگروه‌های سیلوی متمایز بدیهی است پس تعداد اعضای مرتبه‌ی ۷ برابر $n_۷(۷ - ۱) = ۸ \times ۶ = ۴۸$ است. اعضای باقی مانده $۵۶ - ۴۸ = ۸$ تا هستند، که ۲- زیرگروه سیلوی یکتای G را به دست می‌دهند. پس ۲- زیرگروه سیلوی G نرمال است.

(ب) فرض کنید $|G| = ۷۲ = ۸ \times ۹$. آنگاه $n_۳ | ۸$ و $n_۳ = ۱ + ۳k$. پس $n_۳ = ۱$ یا $n_۳ = ۴$. فرض کنید $P \in \mathrm{Syl}_۳(G)$. اگر $n_۳ = ۱$، آنگاه $P \trianglelefteq G$ و مساله حل است. اگر $n_۳ = ۴$، آنگاه بنا به قضیه‌ی سیلو $|G : N_G(P)| = ۴$. در نتیجه همریختی $\rho : G \longrightarrow S_۴$ وجود دارد. داریم $\ker \rho \neq \{1\}$، زیرا $|G| = ۷۲$ و $|S_۴| = ۲۴$. بنابراین $\ker \rho \trianglelefteq G$ $\neq \{1\}$.

(هـ) نشان دهید $n_{۱۱} = ۱$.

(و) نشان دهید $n_۵ = ۱$.

(ز) فرض کنید $|G| = ۱۵۰ = ۲ \times ۳ \times ۵^۲$. دو حالت وجود دارد: $n_۵ = ۱$ یا $n_۵ = ۶$. در حالت $n_۵ = ۶$ از این که $۶ \nmid ۱۵!$ استفاده کنید.

(ح) فرض کنید $|G| = ۶۵۴۵ = ۵ \times ۷ \times ۱۱ \times ۱۷$. چون $n_۵ | ۷ \times ۱۱ \times ۱۷$ دو حالت داریم: $n_۵ = ۱$ یا $n_۵ = ۱۱$. در حالت $n_۵ = ۱۱$ از این که $۱۱ \nmid ۶۵۴۵!$ استفاده کنید.

۴. داریم $|G| = ۳۸۵ = ۵ \times ۷ \times ۱۱$. چون $n_{۱۱} | ۵ \times ۷$ و $n_{۱۱} = ۱ + ۱۱k$، داریم $n_{۱۱} = ۱$؛ یعنی ۱۱- زیرگروه سیلوی G نرمال است. اکنون چون $n_۷ | ۵ \times ۱۱$ و $n_۷ = ۱ + ۷r$، داریم $n_۷ = ۱$. پس ۷- زیرگروه سیلوی P از G نرمال است. بنابراین داریم

$$G/C_G(P) = N_G(P)/C_G(P) \hookrightarrow \mathrm{Aut}\, P.$$

چون $\mathrm{Aut}\, P \cong \mathrm{Aut}\, \mathbb{Z}_۷ \cong \mathbb{Z}_۷^\times$. پس $|G/C_G(P)| | ۶$. چون $۳۸۵ \nmid |G/C_G(P)|$ و $۵۸۳ \nmid |G/C_G(P)|$، $|G/C_G(P)| = ۱$. از این‌رو $G = C_G(P)$ و $P \leq Z(G)$.

۶. داریم $|G| = ۴۵۵ = ۵ \times ۷ \times ۱۳$. فرض کنید $P \in \mathrm{Syl}_{۱۳}(G)$ و نشان دهید $P \trianglelefteq G$. چون $G/C_G(P) = N_G(P)/C_G(P) \hookrightarrow \mathrm{Aut}\, P$ و $\mathrm{Aut}\, P = \mathrm{Aut}\, \mathbb{Z}_{۱۳} \cong \mathbb{Z}_{۱۳}^\times$. پس $|G/C_G(P)| | ۱۲$. چون $۴۵۵ \nmid |G/C_G(P)|$ و $۲۱ \nmid |G/C_G(P)|$ و ۵۵۴ نسبت به هم اول‌اند، $|G/C_G(P)| = ۱$. از این‌رو $G = C_G(P)$ و $P \leq Z(G)$. بنابراین $|Z(G)|$ برابر یکی از اعداد ۱۳، ۶۵، ۹۱ و یا ۴۵۵ است. در نتیجه $|G/Z(G)|$ برابر یک از اعداد ۳۵، ۷، ۵ یا ۱ است. در هر حالت $G/Z(G)$ دوری و G آبلی است.

در نتیجه همه‌ی زیرگروه‌های G نرمال‌اند. به وضوح اگر $P \in \mathrm{Syl}_{۱۳}(G)$ و $Q \in \mathrm{Syl}_{۵}(G)$، $R \in \mathrm{Syl}_{۷}(G)$. آنگاه $P, Q, R \trianglelefteq G$. به وضوح $G = P \times Q \times R$ چون P و Q و R دوری و با مرتبه‌های نسبت به هم اول‌اند، G دوری است.

۷. داریم $n_p | q$ و $n_p \equiv ۱ \mod p$، پس $n_p = q$ یا $n_p = ۱$. اگر $n_p = q$، آنگاه $q \equiv ۱ \mod p$ که خلاف فرض است. پس $n_p = ۱$ و p- زیرگروه سیلوی G نرمال است. داریم $n_q | p^۲$ و $n_q \equiv ۱ \mod q$، پس $n_p = p^۲$ یا $n_q = p$ یا $n_q = ۱$. اگر $n_q = p^۲$، آنگاه $p^۲ \equiv ۱ \mod q$، که خلاف فرض است. اگر $n_q = p$، آنگاه $p \equiv ۱ \mod q$ و بنابراین $p^۲ \equiv ۱ \mod q$، که تناقض است.

۸. فرض کنید $P \in \mathrm{Syl}_p(G)$. پس $|P| = p^m$ و $|G : P| = r$. بنابراین همریختی $\rho : G \longrightarrow S_r$ وجود دارد. چون G ساده است، $\ker \rho = ۱$. بنابراین G با زیرگروهی از S_r یکریخت است؛ به وضوح $p^m r | r!$ و $p^m | (r-۱)!$.

۹. اگر $|G| = ۲^m \times ۵$، آنگاه چون ۲^m برای $m \geq ۴$، $۲۴ = ۵! = (۱-۵)!$ را عاد نمی‌کند، طبق تمرین قبل G ساده نیست.

۱۱. فرض کنید $g \in G$. چون $H \trianglelefteq G$، داریم $gPg^{-۱} \leq gHg^{-۱} = P$. پس $gPg^{-۱}$ نیز p- زیرگروه سیلوی از H است. بنا به قضایای سیلو $h \in H$ وجود دارد که $gPg^{-۱} = hPh^{-۱}$. بنابراین $h^{-۱}gPg^{-۱}h = P$. پس $h^{-۱}g \in N_G(P)$ و در نتیجه $g = h(h^{-۱}g) \in HN_G(P)$. بنابراین $G = HN_G(P)$.

۱۲. داریم $N_G(P) \leq K \leq G$. چون $P \leq N_G(P) \leq K$، پس P یک p- زیرگروه سیلوی K است. فرض کنید $L = N_G(K)$. در این صورت $K \trianglelefteq L$ و $P \in \mathrm{Syl}_P(K)$. پس طبق تمرین قبل $L = KN_L(P)$. چون $N_L(P) \leq N_G(P) \leq K$، داریم $L = K$.

۱۳. چون P و Q در G مزدوج‌اند عضو $g \in G$ وجود دارد که $Q = gPg^{-۱}$. بنابراین

$$N_G(Q) = N_G(gPg^{-۱}) = gN_G(P)g^{-۱} = gPg^{-۱} = Q.$$

۱۶. فرض کنید $p \neq q$ دو شمارنده‌ی اول $\frac{G}{G'}$ باشند. چون $\frac{G}{G'}$ آبلی است، زیرگروه نرمال H/G' با شاخص q در G/G' وجود دارد (تمرین ۱۱ از صفحه‌ی ۱۰۴). پس $H \lhd G$ و $q = \left|\frac{G/G'}{H/G'}\right| = |G/H|$. اگر $Q \in \mathrm{Syl}_p(H)$ طبق بحث فراتینی $G = HN_G(Q)$. هم‌چنین طبق تمرین قبل $N_G(Q) = Q$. بنابراین $G = HQ$ و

$$\frac{G}{H} = \frac{HQ}{H} \cong \frac{Q}{H \cap Q},$$

که تناقض است زیرا $|G/H| = q$ و $\left|\frac{Q}{H \cap Q}\right|$ توانی از p است.

۱۹. فرض کنید H هسته‌ی عمل G روی $\mathrm{Syl}_p(G)$ با مزدوجی باشد. در این صورت $H = \bigcap_{P \in \mathrm{Syl}_p(G)} N_G(P)$. فرض کنید $P_۰$ یک p-زیرگروه سیلوی دلخواه G باشد. نشان دهید $H \cap P_۰$ یکتا p-زیرگروه سیلوی H است و نتیجه بگیرید $H \cap P_۰ = \bigcap_{P \in \mathrm{Syl}_p(G)} P$. پس $p^{n-۱} \mid |H|$ و $p^n \nmid |H|$. از این‌رو $|\bigcap_{P \in \mathrm{Syl}_p(G)} P| = p^{n-۱}$.

تمرین‌های ۱.۶ و ۲.۶، گروه‌های آبلی متناهیاً تولید شده، صفحه‌ی ۱۳۵

۴. (الف)

مولفه‌ها :	$\mathbb{Z}_{۱۳}$	$\mathbb{Z}_۵$	$\mathbb{Z}_۹ \oplus \mathbb{Z}_۳$	$\mathbb{Z}_۴$
نوع :	(۱)	(۱)	$(۲, ۱)$	(۲)
شمارنده‌های مقدماتی :	۱۳	۵	$(۳^۲, ۳)$	$۲^۲$

(ب)

مولفه‌ها :	$\mathbb{Z}_۵ \oplus \mathbb{Z}_۵ \oplus \mathbb{Z}_۵$	$\mathbb{Z}_۳ \oplus \mathbb{Z}_۳$	$\mathbb{Z}_۸ \oplus \mathbb{Z}_۲ \oplus \mathbb{Z}_۲$
نوع :	$(۱, ۱, ۱)$	$(۱, ۱)$	$(۳, ۱, ۱)$
شمارنده‌های مقدماتی :	$(۵, ۵, ۵)$	$(۳, ۳)$	$(۲^۳, ۲, ۲)$

۵. از لم ددکیند استفاده کنید: $G = G_1 \cap (H + K) = H + (G_1 \cap K)$.

۶. از این که هر گروه آبلی متناهی، حاصل‌ضرب مستقیم مولفه‌های اولیه‌اش است استفاده کنید.

۷. هر گروه آبلی مرتبه‌ی ۸ با یکی از گروه‌های $\mathbb{Z}_8$، $\mathbb{Z}_2 \oplus \mathbb{Z}_4$، $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$، یکریخت است و دو گروه $\mathbb{Z}_4 \oplus \mathbb{Z}_2$ و $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$ بیش از یک زیرگروه مرتبه‌ی ۲ دارند.

۸. از تمرین ۶ استفاده کنید.

۹. اگر $|G| = m$، آنگاه به ازای یک $k \in \mathbb{N}$ داریم $m = nk$. اکنون یک زیرگروه H با مرتبه‌ی k از G اختیار کنید.

۱۰. (الف) تابع $\varphi : G \longrightarrow G$ با $\varphi(a) = p^k a$ یک همریختی با $\ker f = G[p^k]$ و $\operatorname{Im} f = p^k G$ است. اگر $G = \langle a \rangle$، آنگاه $p^k G = \varphi(\langle a \rangle) = \langle \varphi(a) \rangle = \langle p^k a \rangle$. هم چنین توجه کنید که اگر $k < n$، داریم $O(a^k) = p^{n-k}$.
(b) اگر $g = g_1 + \cdots + g_r$، آنگاه $p^k g = p^k g_1 + \cdots + p^k g_r \in p^k G_1 + \cdots p^n G_r$. پس $p^k G \subseteq p^k G_1 + \cdots + p^k G_r$. به طریق مشابه $p^k G_1 + \cdots + p^k G_r \subseteq p^k G$. مجموع $p^k G_1 + \cdots + p^k G_r$ مستقیم است زیرا O $p^k G_i \subseteq G_i$ $G = G_1 \oplus \cdots \oplus G_r$.
(ج) از (الف) و (ب) استفاده کنید.

۱۲. از مثال ۱۳.۱.۶ و تمرین قبل استفاده کنید.

۱۳. ابتدا برای p- گروه‌ها ثابت کنید.

۱۴. ابتدا برای گروه‌های دوری و سپس برای p- گروه‌ها ثابت کنید.

تمرین‌های ۱.۷، گروه‌های حل‌پذیر، صفحه‌ی ۱۴۰

۱. توجه کنید که $|\mathrm{GL}_2(\mathbb{Z}_3)| = ۲۴$.

۶. (الف) از این که هر گروه مرتبه‌ی pqr ساده نیست استفاده کنید.
(ب) از این که هر گروه مرتبه‌ی $p^2 q$ ساده نیست استفاده کنید.

۷. نشان دهید هر گروه با مرتبه‌ی کمتر یا مساوی ۱۰۰ و نایکریخت با A_5، حل‌پذیر است: فرض کنید حکم درست نباشد؛ پس مجموعه‌ی

$$T = \{|G| \mid G \ncong A_5, \ \ G \text{ گروه حل‌ناپذیر } \ |G| \leq ۱۰۰\}$$

مجموعه‌ای ناتهی از اعداد طبیعی است و کوچک‌ترین عضو دارد، یعنی گروه G حل‌ناپذیر با مرتبه‌ی می‌نیمم وجود دارد که $|G| \leq ۱۰۰$ و $G \ncong A_5$. چون G حل‌ناپذیر با مرتبه‌ی می‌نیمم است، نشان دهید G ساده است، که این خلاف تمرین ۵ از صفحه ۸۹۱ است.

۹. A_5، $A_5 \times \mathbb{Z}_2$، S_5، $\mathrm{GL}_3(\mathbb{Z}_3)$ (مثال ۷-۱-۵)، $A_5 \times \mathbb{Z}_3$.

۱۲. از این که $\dfrac{G}{\bigcap_{i=1}^{n} K_i}$ با زیرگروهی از $G/K_1 \times \cdots \times G/K_n$ یکریخت است، استفاده کنید و توجه کنید $G/K_1 \times \cdots \times G/K_n$ حل‌پذیر است.

۱۳. $\dfrac{K}{H \cap K}$ و $\dfrac{HK}{H}$ را در نظر بگیرید.

۱۴. (ب) $\Longleftarrow$ (الف) چون G غیرهمانی است، طبق فرض زیرگروه نرمال سره‌ی H از G وجود دارد، که G/H آبلی است. حال به استقرا روی $|G|$ عمل کنید.
(ج) $\Longleftarrow$ (الف) چون $G/\{1\}$ غیرهمانی است، طبق فرض زیرگروه آبلی $G_1 \neq \{1\}$ از G وجود دارد. به استقرا روی $|G|$ سری آبلی برای G_1 و بنابراین برای G وجود دارد.

تمرین‌های ۲.۷، گروه‌های پوچ‌توان، صفحه‌ی ۱۴۶

۱. هر زیرگروه یک گروه پوچ‌توان، پوچ‌توان است. S_3 را در نظر بگیرید.

۲. خیر

۳. می‌دانیم $\Gamma_۲(D_{۲n}) = D'_{۲n} = \langle \rho^۲ \rangle$. به استقرا نشان دهید $\Gamma_{j+۱}(D_{۲n}) = \left\langle \rho^{۲^j} \right\rangle$.

۴. $k \geq ۰$ را طوری بیابید که $H \cap \Gamma_{k+۱}(G) = \{۱\}$، اما $H \cap \Gamma_k(G) \neq \{۱\}$.

۵. به استقرا روی i عمل کنید. توجه کنید که اگر H زیرگروه نرمال G باشد هر خودریختی $\alpha \in \operatorname{Aut} G$ یک خودریختی $\bar{\alpha} \in \operatorname{Aut} \frac{G}{H}$ القا می‌کند.

۶. $K \cap Z(G)$ را در نظر بگیرید.

۷. نشان دهید $Z(H) \trianglelefteq G$.

۹. $K \cap L$ زیرگروه نرمال G مشمول در L و K است، پس $K \cap L = \{۱\}$.

۱۰. از این که یک گروه متناهی، پوچ‌توان است اگر و تنها اگر حاصل‌ضرب مستقیم زیرگروه‌های سیلوی خودش باشد، استفاده کنید.

۱۲. فرض کنید $xZ_۱(G) \in \frac{Z_۲(G)}{Z_۱(G)}$ طوری باشد که $(xZ_۱(G))^m = Z_۱(G)$، آنگاه داریم $x^m \in Z_۱(G)$. بنابراین به ازای هر $g \in G$، چون $[x,g] \in Z_۱(G)$، داریم $[x,g]^m = [x^m, g] = ۱$. سپس به استقرا عمل کنید.

۱۳. فرض کنید $Z(G) \neq G$. عضو $x \in Z_۲(G)$ و $g \in G$ را در نظر بگیرید. آنگاه $[x,g] \in Z(G)$ و $[x,g]^e = [x^e, g] = ۱$. پس $x^e \in Z_۱(G)$. بنابراین نمای $\frac{Z_۲(G)}{Z_۱(G)}$ متناهی است و e را عاد می‌کند. سپس به استقرا رده‌ی پوچ‌توانی G عمل کنید.

تمرین‌های ۳.۷، زیرگروه فراتینی، صفحه‌ی ۱۴۹

۱. (الف) $\Phi(D_۸) = \langle \rho^۲ \rangle$ (ب) $\Phi(D_۸) = \langle \rho^۳ \rangle$.

۲. از این که اگر $G/Z(G)$ دوری باشد آنگاه G آبلی است نشان دهید $|Z(G)| = p$. و از این که هر گروه مرتبه‌ی $p^۲$ آبلی است نتیجه بگیرید $G/Z(G)$ آبلی است و $\{۱\} \neq G' \leq Z(G)$ پس $G' = Z(G)$. چون G پوچ‌توان است $G' \leq \Phi(G)$. از طرف دیگر از این که $\Phi(G)$ مجموعه‌ی نامولدهای G است نتیجه بگیرید $|\Phi(G)| \neq p^۲$.

۳. زیرگروه‌های ماکسیمال $\langle a \rangle$ عبارتند از $M_i = \langle a^{p_i} \rangle$، $i = ۱, ۲, \ldots, r$.

۴. از این که $\Phi(G)$ مجموعه‌ی نامولدهای G است، استفاده کنید.

۵. از این که $\Phi(G)$ مجموعه‌ی نامولدهای G است، استفاده کنید.

۶. ($\Longrightarrow$) از این که هر گروه آبلی مقدماتی، مشخصاً ساده است، استفاده کنید.
($\Longleftarrow$) نشان دهید هر زیرگروه ماکسیمال M، نرمال است و $|G/M| = p$.

۷. اگر M زیرگروه ماکسیمال G باشد و $\Phi(H) \not\subseteq M$، چون M ماکسیمال است، $G = \Phi(H)M$. پس بنا به لم ددکیند و تمرین ۵

$$H = H \cap G = H \cap \Phi(H)M = \Phi(H)(H \cap M) = H \cap M.$$

از این‌رو $\Phi(H) \leq H \leq M$، که تناقض است.

۸. (الف) ابتدا گوییم که اگر L زیرگروه ماکسیمال K باشد، آنگاه $H \times L$ یک زیرگروه ماکسیمال $H \times K$ است. زیرا اگر $H \times L \leq J \leq H \times K$، آنگاه بنا به لم ددکیند

$$J = J \cap HK = H(J \cap K) = H \times (J \cap K).$$

پس $L \leq J \cap K \leq K$، و چون L ماکسیمال است داریم $J \cap K = L$ یا $J \cap K = K$. از این‌رو $J = H \times L$ یا $J = H \times K$.
حال اگر J یک زیرگروه ماکسیمال $H \times K$ شامل H باشد، ثابت کنید $J \cap K$ در K ماکسیمال است و $J = H \times (J \cap K)$.

(ج) طبق (ب) اشتراک همه‌ی زیرگروه‌های ماکسیمال G، شامل H، برابر $H \times \Phi(K)$ و اشتراک همه‌ی زیرگروه‌های ماکسیمال G، شامل K، برابر $\Phi(H) \times K$ است. پس

$$\Phi(G) \leq (\Phi(H) \times K) \cap (H \times \Phi(K)) = \Phi(H) \times \Phi(K)$$

از طرفی چون $H \trianglelefteq G$ و $K \trianglelefteq G$، با توجه به تمرین ۷، داریم $\Phi(H) \leq \Phi(G)$ و $\Phi(K) \leq \Phi(G)$. پس $\Phi(H) \times \Phi(K) \leq \Phi(G)$.

۹. از این که $\Phi(G)$ مجموعه‌ی نامولدهای G است، استفاده کنید.

۱۱. (الف) ابتدا نشان دهید هر زیرگروه ماکسیمال G/K دقیقاً به صورت M/K است که در آن M زیرگروه ماکسیمال G شامل K است.

۱۲. نشان دهید هر زیرگروه ماکسیمال M، نرمال است و $|G/M| = p$ نتیجه بگیرید $G'G^p \leq \Phi(G)$. از طرف دیگر از این که $\dfrac{G}{G'G^p}$ یک گروه آبلی مقدماتی است، و تمرین‌های ۶ و ۱۱ (الف) استفاده کنید.

تمرین‌های ۴.۷، سری ترکیبی، صفحه‌ی ۱۵۵

۱. (الف)، (ج)، (هـ) $\ell(Q_8) = \ell(D_8) = \ell(C_8) = 3$، عوامل ترکیبی: $\{C_2, C_2, C_2\}$ (ب)، (د) $\ell(A_4) = \ell(C_{12}) = 3$، عوامل ترکیبی: $\{C_3, C_2, C_2\}$.

۲. چون $G = C_{p^n}$ دوری است، هر زیرگروه آن و هر گروه خارج قسمتی آن دوری است. به علاوه اگر $H \leq G$، آنگاه G/H ساده است اگر و تنها اگر $|G/H| = p$. اگر $n = 1$، آنگاه $G = C_p$ ساده است و تنها سری ترکیبی آن $G \supset \{1\}$ است. فرض کنید $n > 1$ و G_1 زیرگروه یکتایی G از مرتبه‌ی p^{n-1} است. در این صورت G/G_1 ساده است. به علاوه تنها زیرگروه H از G که G/H ساده است، همان G_1 است. حال با در نظر گرفتن G_1، و به طوور استقرایی می‌توان عمل کرد.

۳. (الف) $\mathbb{Z}_{20} \supset \langle\bar{5}\rangle \supset \langle\bar{10}\rangle \supset \langle\bar{2}\rangle \supset \{\bar{1}\}$، $\mathbb{Z}_{20} \supset \langle\bar{10}\rangle \supset \{\bar{1}\}$
$\mathbb{Z}_{20} \supset \langle\bar{2}\rangle \supset \langle\bar{4}\rangle \supset \{\bar{1}\}$
(ب) اگر $C_{24} = \langle w\rangle$، آنگاه

$$\langle w\rangle \supset \langle w^2\rangle \supset \langle w^6\rangle \supset \langle w^2\rangle \supset \{1\},$$
$$\langle w\rangle \supset \langle w^2\rangle \supset \langle w^4\rangle \supset \langle w^8\rangle \supset \{1\},$$
$$\langle w\rangle \supset \langle w^2\rangle \supset \langle w^6\rangle \supset \langle w^2\rangle \supset \{1\},$$
$$\langle w\rangle \supset \langle w^2\rangle \supset \langle w^4\rangle \supset \langle w^2\rangle \supset \{1\}$$

(ج) اگر $C_{30} = \langle w\rangle$، آنگاه

$$\langle w\rangle \supset \langle w^3\rangle \supset \langle w^{15}\rangle \supset \{1\}, \quad \langle w\rangle \supset \langle w^3\rangle \supset \langle w^6\rangle \supset \{1\}$$
$$\langle w\rangle \supset \langle w^2\rangle \supset \langle w^6\rangle \supset \{1\}, \quad \langle w\rangle \supset \langle w^2\rangle \supset \langle w^{10}\rangle \supset \{1\}$$
$$\langle w\rangle \supset \langle w^5\rangle \supset \langle w^{10}\rangle \supset \{1\}$$

(د) $S_3 \supset A_3 \supset \langle(123)\rangle \supset \{1\}$، $S_3 \supset A_3 \supset \langle(12)\rangle \supset \{1\}$.
(هـ) $S_4 \supset A_4 \supset V_4 \supset \langle(12)(34)\rangle \supset \{1\}$،
$S_4 \supset A_4 \supset V_4 \supset \langle(13)(24)\rangle \supset \{1\}$،
$S_4 \supset A_4 \supset V_4 \supset \langle(14)(23)\rangle \supset \{1\}$.
(و) $\mathbb{Z}_2 \times \mathbb{Z}_2 \supset \langle(\bar{0}, \bar{1})\rangle \supset \{(\bar{0}, \bar{0})\}$، $\mathbb{Z}_2 \times \mathbb{Z}_2 \supset \langle(\bar{1}, \bar{0})\rangle \supset \{(\bar{0}, \bar{0})\}$،
$\mathbb{Z}_2 \times \mathbb{Z}_2 \supset \langle(\bar{1}, \bar{1})\rangle \supset \{(\bar{0}, \bar{0})\}$.

۴. C_8 و D_8.

۵. (الف) تابع $\alpha : K \cap G_i \longrightarrow G_i/G_{i+1}$ را با $\alpha(x) = xG_{i+1}$ تعریف می‌کنیم. به وضوح α یک همریختی است و $\ker\alpha = \{x \in K \cap G_i \mid x \in G_{i+1}\} = K \cap G_{i+1}$. بنابراین $K \cap G_{i+1} \trianglelefteq K \cap G_i$. اکنون تنها باید ثابت کنیم $\alpha(K \cap G_i) \trianglelefteq G_i/G_{i+1}$. اگر $x \in K \cap G_i$ و $y \in G_i$، آن‌گاه

$$(yG_{i+1})\alpha(x)(yG_{i+1})^{-1} = (yxy)^{-1}G_{i+1} = \alpha(yxy^{-1}) \in \alpha(K \cap G_i),$$

زیرا $yxy^{-1} \in (yKy^{-1}) \cap G_i = K \cap G_i$.

(ب) بنا به قضیه‌ی سوم یکریختی، $\frac{G_{i+1}K}{K} \trianglelefteq \frac{G_iK}{K}$ و $\frac{(G_iK)/K}{(G_{i+1}K)/K} \cong \frac{KG_i}{KG_{i+1}}$. پس تنها باید ثابت کنیم $G_iK/G_{i+1}K$ یک تصویر همریخت G_i/G_{i+1} است. برای این کار نشان دهید تابع $\alpha : \frac{G_i}{G_{i+1}} \longrightarrow \frac{G_iK}{G_{i+1}K}$ با ضابطه‌ی $\alpha(xG_{i+1}) = xG_{i+1}K$ خوش‌تعریف و پوشا است.

۶. فرض کنید G سری ترکیبی داشته باشد و $G = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_n = \{1\}$ یک سری ترکیبی برای G باشد. بنا به تمرین ۵، سره‌های متناظر K و G/K نیز سری‌های ترکیبی‌اند. در واقع در هر دو حالت عوامل آن‌ها یا با زیرگروه نرمال و یا تصویر همریخت گروه‌های ساده G_i/G_{i+1} یکریخت هستند؛ پس یا ساده‌اند و یا برابر $\{1\}$ هستند. بنابراین پسا از حذف عوامل مساوی به سری ترکیبی برای K و G/K خواهیم رسید.
بر عکس فرض کنید

$$K = K_0 \supset K_1 \supset \cdots \supset K_m = \{1\}$$
$$\frac{G}{K} = \frac{G_0}{K} \supset \frac{G_1}{K} \supset \cdots \supset \frac{G_r}{K} = \{K\}$$

سری‌های ترکیبی برای K و G/K باشند. چون $\frac{G_i}{G_{i+1}} \cong \frac{G_i/K}{G_{i+1}/K}$، به ازای هر i، سری

$$G = G_0 \supset G_1 \supset \cdots \supset G_r = K = K_0 \supset K_1 \supset \cdots \supset K_m = \{1\}$$

یک سری ترکیبی برای G است. اکنون هر سه حالت (الف)، (ب) و (ج) بدیهی هستند.

۷. همریختی تصویر روی مولفه‌ی اول را در نظر می‌گیریم: $\pi_1 : G \times H \longrightarrow H$، که در آن $\pi_1(g,h) = h$، به ازای هر $(g,h) \in G \times H$. همریختی π_1 پوشا است و $\ker\pi_1 = \{(g,1) \mid g \in G\} \cong G$. اگر $K = \ker\pi_1$، آن‌گاه $K \cong G$ و $H \cong \frac{G \times H}{K}$ سری ترکیبی دارند، پس بنا به تمرین ۶،

$$\ell(G \times H) = \ell(K) + \ell\left(\frac{G \times H}{K}\right) = \ell(K) + \ell(H).$$

۸. به استقرا روی $|G|$ عمل می‌کنیم. اگر $|G| = 1$ حکم واضح است. در حالت کلی فرض کنید K یک زیرگروه ماکسیمال (نرمال) G است. آن‌گاه $|G/K|$ یک عدد اول شمارنده‌ی $|G|$ است، مثلاً $|G/K| = p_1$. بنابراین $|K| = p_1^{n_1-1}p_2^{n_2}\cdots p_r^{n_r}$. پس بنا به فرض استقرا و تمرین ۶

$$\begin{aligned}\ell(G) = \ell(K) + \ell(G/K) &= [(n_1 - 1) + n_2 + \cdots + n_r] + 1 \\ &= n_1 + n_2 + \cdots + n_r.\end{aligned}$$

۹. ابتدا ثابت می‌کنیم $G = HK$. داریم $H \subseteq HK \trianglelefteq G$ و $K \subseteq HK \trianglelefteq G$. پس اگر $G \neq HK$، آن‌گاه چون H و K زیرگروه‌های نرمال ماکسیمال هستند، باید داشته باشیم $K = HK = H$، که خلاف فرض است. پس $G = HK$. اکنون بنا به قضیه‌ی دوم یکریختی داریم $\frac{G}{K} = \frac{HK}{K} \cong \frac{H}{H \cap K}$. چون G/K ساده است، $H \cap K$ زیرگروه ماکسیمال H است، حالت دیگر مشابه است.

۱۰. فرض کنید

$$G = G_0 \supset G_1 \supset G_2 \supset \cdots \supset G_n = \{1\} \tag{1}$$

یک سری ترکیبی برای G است، به استقرا روی n نشان می‌دهیم که هر سری ترکیبی

$$G = H_0 \supset H_1 \supset H_2 \supset \cdots \supset H_m = \{1\} \tag{2}$$

با سری (۱) معادل است. اگر $n = 1$، آنگاه G ساده است. بنابراین $G_1 = \{1\} = H_1$ و حکم ثابت است. فرض کنید $n \geq 2$ و حکم برای همه‌ی گروه‌های با یک سری ترکیبی با طول کمتر از n برقرار باشد. به ویژه G_1، سری ترکیبی $G_1 \supset G_2 \supset \cdots \supset G_n = \{1\}$ به طول $n-1$ دارد. اگر $H_1 = G_1$، آنگاه $G_1 \supset H_2 \supset \cdots \supset H_m = \{1\}$ سری ترکیبی دیگری برای G_1 است. پس بنا به فرض استقرا با سری $G_1 \supset G_2 \supset \cdots \supset G_n = \{1\}$ معادل است و بنابراین حکم ثابت است. پس فرض کنید $H_1 \neq G_1$ و $H_1 \cap G_1 = G_0 \supset L_1 \supset \cdots \supset L_s = \{1\}$ یک سری ترکیبی برای $H_1 \cap G_1$ باشد. اکنون سری‌های زیر برای G را در نظر بگیرید

$$G \supset G_1 \supset (H_1 \cap G_1) \supset L_1 \supset \cdots \supset L_s = \{1\} \tag{3}$$

$$G \supset H_1 \supset (H_1 \cap G_1) \supset L_1 \supset \cdots \supset L_s = \{1\} \tag{4}$$

چون $H_1 \neq G_1$، بنا به تمرین ۹، $H_1 \cap G_1$ زیرگروه ماکسیمال و نرمال در هم H_1 و هم G_1 است، پس (۳) و (۴) هر دو سری‌های ترکیبی برای G هستند. به علاوه بنا به تمرین ۹ $G/G_1 \cong H_1/(H_1 \cap G_1)$ و $G/H_1 \cong G_1/(H_1 \cap G_1)$ و (۳) و (۴) معادل‌اند. توجه کنید این معادل بودن حالتی برای $S = 0$ برقرار است، یعنی اگر $H_1 \cap G_1 = \{1\}$. اکنون $G_1 \supset G_2 \supset \cdots \supset G_n = \{1\}$ و $G_1 \supset (H_1 \cap G_1) \supset L_1 \supset \cdots \supset L_s = \{1\}$ سری‌های ترکیبی برای G_1 است و بنا به فرض استقرا معادل‌اند. از این رو (۳) $\iff$ (۱) و هم چنین داریم $s + 1 = n - 1$. اما در این صورت طول سری ترکیبی $H_1 \supset (H_1 \cap G_1) \supset L_1 \supset \cdots \supset L_s = \{1\}$ برابر $n-1$ است و مجدداً بنا به فرض استقرا، با سری $H_1 \supset H_2 \supset \cdots \supset H_m = \{1\}$ معادل است. از این رو (۴) $\iff$ (۲). در نتیجه (۲) $\iff$ (۴) $\iff$ (۳) $\iff$ (۱) و حکم ثابت است.

۱۱. (الف) اگر $C_n = \langle w \rangle$ و H زیرگروهی ماکسیمال از C_n باشد، آنگاه $|C_n/H|$ یک عدد اول شمارنده‌ی $|C_n|$ است، پس دقیقاً r انتخاب برای H داریم.
(ب) به استقرا روی m عمل کنید.

تمرین‌های ۵.۷، گروه‌های چند دوری و ابرحل‌پذیر، صفحه‌ی ۱۵۹

۱. اگر $G = \langle g_1, \ldots, g_n \rangle$، آنگاه $\{1\} \leq \langle g_1 \rangle \leq \langle g_1, g_2 \rangle \leq \cdots \leq G$ یک سری دوری برای G است. سپس بنا به اثبات قضیه‌ی ۷-۵-۲ هر زیرگروه G، n مولدی است.

۲. کافی است ثابت کنیم مرتبه‌ی هر زیرگروه می‌نیمال نرمال N از G عددی اول است. سری نرمال و دوری

$$\{1\} = G_0 < G_1 < \cdots < G_n = G$$

را در نظر می‌گیریم. چون $N \cap G_0 = \{1\}$ و $N \cap G_n \neq \{1\}$، عدد i وجود دارد که $1 \leq i \leq n$ و $N \cap G_i \neq \{1\}$ و $N \cap G_{i-1} = \{1\}$. نتیجه بگیرید $N \leq G_i$ و

$$N \cong \frac{NG_{i-1}}{G_{i-1}} \leq \frac{G_i}{G_{i-1}}$$

دوری با مرتبه‌ی عدد اول است. برعکس اگر مرتبه‌ی هر عامل اصلی G عددی اول باشد، پس سری اصلی برای G یک سری دوری است.

۳. از تمرین ۲ استفاده کنید. S_3 ابر حل‌پذیر است، اما پوچ‌توان نیست.

۴. هر تظریف یک سری دوری برای G، مجدداً یک سری دوری، با همان تعداد عوامل دوری نامتناهی، است. در واقع اگر H/K یک عامل دوری نامتناهی باشد و

$$K \leq K_1 \leq H_1 \leq H,$$

آنگاه چون شاخص هر زیرگروه دوری نامتناهی، متناهی است داریم

$$|H : K_1| = |H/K : K_1/K| < \infty.$$

نتیجه بگیرید $H : H_1$ و $K_1 : K$ متناهی هستند. چون هر دو سری دوری تظریف‌های معادل دارند، پس تعداد عوامل دوری نامتناهی عددی پایا است.

تمرین‌های ۱۶۵، گروه آزاد، صفحه‌ی ۱۶۵

۱. اگر $a = x_1^{\varepsilon_1} \cdots x_n^{\varepsilon_n}$ ($x_i \in X$ و $\varepsilon_i = \pm 1$)، طوری باشد که $a^m = 1$، آنگاه

$$a^m = x_1^{\varepsilon_1} \cdots x_n^{\varepsilon_n} \cdots x_1^{\varepsilon_1} \cdots x_n^{\varepsilon_n} = 1$$

نتیجه بگیرید a^m یک واژه‌ی کاهشی است که با واژه‌ی تهی ۱ برابر شد و این امکان ندارد مگر این که $m = 0$.

۲. اگر F گروه آزاد روی $X = \{x\}$ باشد، هر واژه‌ی کاهشی در F به صورت x^n است که در آن $n \in \mathbb{Z}$.

۳. هر عضو G به صورت واژه‌ی کاهشی است.

۴. اگر a عضو مرکز یک گروه آزاد با رتبه‌ی بیش از یک باشد، آنگاه $ax = xa$ منجر به یک رابطه‌ی $a^{-1}x^{-1}ax = 1$ خواهد شد. اما در گروه آزاد هیچ گونه رابطه‌ی نابدیهی بین اعضا وجود ندارد.

۷. چون شاخص H در F متناهی است، زیرگروه نرمال مشمول در H با شاخص متناهی در F وجود دارد. این زیرگروه در واقع همان $N = N_G$ است. فرض کنید K زیرگروه نابدیهی دلخواهی از F است، از این که داریم

$$|K : N \cap K| = |NK : N| \leq |F : N| < \infty,$$

نتیجه بگیرید $N \cap K \neq \{1\}$.

تمرین‌های ۱.۱۰، خواص مقدماتی حلقه‌ها، صفحه‌ی ۲۰۴

۴. می‌توان از مساله‌ی ۲۴ صفحه‌ی ۵۸ استفاده کرد؛ اما راهی ساده که از عمل جمع نیز استفاده کند به صورت زیر است:
(الف) اگر $ac = 0$، آنگاه $a(b + c)a$ را در نظر بگیرید.
(ب) با در نظر گرفتن $a(ab - ba)a$، ابتدا نشان دهید $ab = ba$. پس نشان دهید ab عضو بی‌اثر ضرب R است.

۶. (الف) $\text{lcm}\{m, n\}$. (ب) m. (ج) ۰.

۷. چندجمله‌ای $g(x) = b_0 + b_1x + \cdots + b_mx^m$ را با درجه‌ی می‌نیمم طوری انتخاب کنید که $f(x)g(x) = 0$. با متحد قرار دادن دو طرف تساوی و استقرا روی i، ثابت کنید $a_{n-i}g(x) = 0$، $i = 0, 1, \ldots, n$. بنابراین $a_{n-i}b_0 = 0$، $i = 0, 1, \ldots, n$، که نتیجه می‌دهد $b_0f(x) = 0$.

۱۳. از قضیه‌ی لاگرانژ استفاده کنید.

۱۴. $O(1)$ در گروه $(F, +)$ را در نظر بگیرید.

تمرین‌های ۲.۱۰، زیرحلقه، صفحه‌ی ۲۰۷

۴. فرض کنید $n = p_۱^{m_۱} \cdots p_r^{m_r}$، که در آن p_iها اعداد اول متمایزند. اگر $\bar{۱}, \bar{۰} \neq \bar{a} \in \mathbb{Z}_p$ خودتوان باشد، آنگاه $n|a(a-۱)$. چون p نسبت به a یا $a-۱$ اول است، p^{m_j} یا a یا $a-۱$ را عاد می‌کند. نتیجه بگیرید $\bar{۱}, \bar{۰} \neq \bar{a}$ خودتوان است اگر و تنها اگر به ازای هر $۱ \leq j \leq r$، p^{m_j} عاملی از a یا $-a$ باشد.

۵. اگر $e \in R$ عضو خودتوان R باشد به ازای هر $x \in R$، اعضای $(exe - ex)^۲$ و $(exe - xe)^۲$ را در نظر بگیرید.

۷. $a+۱$ را به جای a قرار دهید.

۹. (الف) اگر $n > m$ نشان دهید، به ازای هر $k \geq ۰$ و $j \geq m$، $a^{j+k(n-m)} = a^j$. نتیجه بگیرید $a^{m(n-m)}$ خودتوان است.
(ب) اگر $a \in R$، دنباله a، $a^۲$، $a^۳$، ... را در نظر بگیرید.

۱۳. $-a$ را در نظر بگیرید.

۱۸. برای هر $a, x \in R$ با در نظر گرفتن این که $(a+x)^۲ + (a+x)$ با x تولید می‌شود، ابتدا نشان دهید $ax^۲ = x^۲a$.

۱۹. ابتدا نشان دهید $a^۲$ خودتوان است و سپس نشان دهید R عضو پوچ‌توان ناصفر ندارد. از تمرین ۵ نتیجه بگیرید $a^۲$ در مرکز R قرار دارد. در نهایت از تمرین ۱۸ استفاده کنید.

۲۲. ابتدا حالت‌های $n = ۲, ۳$ را در نظر بگیرید.

۲۳. (الف) ($\Longrightarrow$) از مثال ۸.۲.۱۰ نتیجه بگیرید $a_۱x + \cdots + a_nx^n$ پوچ‌توان است و از تمرین ۲ استفاده کنید.
($\Longleftarrow$) اگر $g(x) = b_۰ + b_۱x + \cdots + b_mx^m$ وارون $f(x)$ باشد. با متحد قرار دادن دو طرف تساوی $f(x)g(x) = ۱$ و استقرا روی i نشان دهید $a_n^{i+۱}b_{m-i} = ۰$، $i = ۰, ۱, \ldots, m$. به ویژه برای $i = m$ داریم $a_n^{m+۱}b_۰ = ۰$. چون $b_۰$ وارون‌پذیر است. $a_n^{m+۱} = ۰$. پس a_n پوچ‌توان است. اکنون $f(x) - a_nx^n$ وارون‌پذیر است می‌توان به استقرا روی n عمل کرد.

۲۴. اگر $a_k = \frac{m}{n}$، که در آن $m^۲ - ۲n^۲ = \pm ۱$، نشان دهید همین تساوی برای $a_{k+۱}$ برقرار است. با $a_۰ = \frac{۳}{۲}$ شروع کنید.

تمرین‌های ۳.۱۰، همریختی، صفحه‌ی ۲۱۱

۵. خیر

۷. همریختی $f : \mathbb{Z} \longrightarrow \mathbb{Z}_۲$ با ضابطه‌ی $f(n) = \bar{n}$ را در نظر بگیرید.

۹. همریختی $f : \mathbb{Z} \longrightarrow \mathbb{Z}_۴$ با ضابطه‌ی $f(n) = \bar{n}$ را در نظر بگیرید.

۱۱.

$$\begin{aligned} f\left(\frac{۱}{n}\right) &= f\left(\frac{۱}{n}\right) f(۱) = f\left(\frac{۱}{n}\right) g(۱) = f\left(\frac{۱}{n}\right) g(n) g\left(\frac{۱}{n}\right) \\ &= f\left(\frac{۱}{n}\right) f(n) g\left(\frac{۱}{n}\right) = f(۱) g\left(\frac{۱}{n}\right) \\ &= g\left(\frac{۱}{n}\right) \end{aligned}$$

تمرین‌های ۴.۱۰، ایدآل حلقه‌ی خارج‌قسمتی، صفحه‌ی ۲۱۷

۵. اگر T ایدآلی از $M_n(R)$ باشد. قرار دهید

$$I_{ij} = \{a \in R \mid \text{درایه‌ی } (i,j) \text{ عضوی از } T \text{ است } a\}.$$

به ازای هر $1 \leq i, j \leq n$، نشان دهید I_{ij} ایدآلی از R است. حال اگر $1 \leq i, j, t, k \leq n$ و $a \in I_{ij}$ درایه i, j ماتریس $A \in T$ باشد، آنگاه

$$(E_{ti}A)E_{jk} = (a_{i1}E_{t1} + \cdots + a_{in}E_{tn})E_{jk} = a_{ij}E_{tk} \in T.$$

بنابراین $a = a_{ij} \in I_{tk}$ و $I_{ij} \subseteq I_{tk}$. به همین نحو $J = I_{tk} \subseteq I_{ij}$. پس $T = M_n(J)$.

۶. تمرین قبل را ببینید.

۷. اگر $0 \neq A \in L_j$، آنگاه $A = \alpha_1 E_{1j} + \alpha_2 E_{2j} + \cdots + \alpha_n E_{nj}$، که در آن $a_s \neq 0$. سپس نشان دهید $E_{ij} = (\alpha_s^{-1}E_{is})A \in L_j$ و نتیجه بگیرید $M_n(R)E_{ij} \subseteq L_j$.

۸. برای هر $x \in R$، $C_R(x)$، مرکز ساز x در R را در نظر بگیرید.

۱۲. اگر $\varphi : \mathbb{R} \longrightarrow \mathbb{R}$ همریختی یک‌به‌یک و پوشا باشد. ابتدا نشان دهید به ازای هر $m, n \in \mathbb{Z}$، $f\left(\frac{m}{n}\right) = \frac{m}{n}$. اگر $x \in \mathbb{R}$ عدد مثبت باشد، آنگاه $\varphi(x) = \varphi(\sqrt{x})^2 > 0$، نتیجه بگیرید اگر $x < y$، آنگاه $\varphi(x) < \varphi(y)$. حال اگر $x \in \mathbb{R}$ و $\varphi(x) \neq x$، عدد گویایی بین x و $\varphi(x)$ انتخاب کنید و با استفاده از صعودی بودن φ به تناقض برسید.

۲۰. طبق تمرین‌های ۱۲ و ۱۳ از صفحه‌ی ۲۱۱، حلقه‌ی یکدار S وجود دارد که $R \subseteq S$. قرار دهید $I = \{a \in S \mid ar = 0, \ \forall r \in R\}$. نشان دهید $R \cap I = \{0\}$ و $R \hookrightarrow S/I$.

۲۱. به استقرا روی n عمل کنید. اگر مساله برای n درست باشد و $A \subseteq \bigcup_{i=1}^{n+1} A_i$، آنگاه $x \in A - \bigcup_{i=1}^{n} A_i$ و $y \in A - A_{n+1}$ وجود دارند. سپس $n+2$ متمایز $r_1, r_2, \ldots, r_{n+2} \in F$ را در نظر بگیرید و نتیجه بگیرید $x + r_j y \in \bigcup_{i=1}^{n+1} A_i$، $j = 1, 2, \ldots, n+2$. از با استفاده از اصل لانه کبوتری i، t، s را بیابید که $x + r_s y, x + r_t y \in A_i$ و نشان دهید $y \in A_i$، هم چنین $i \neq n+1$. در نهایت از فرض استقرا استفاده کنید.

تمرین‌های ۵.۱۰، میدان کسرهای یک دامنه‌ی صحیح، صفحه‌ی ۲۲۱

۱. قرار دهید $K = \{rs^{-1} \mid r, s \in R, \ \ s \neq 0\}$.

۲. $\mathbb{Z}[\sqrt{m}]$ زیرحلقه‌ی $\mathbb{C}$ است، پس دامنه‌ی صحیح است. میدان کسرهای $\mathbb{Z}[\sqrt{m}]$ در حالت $m > 0$ عبارت است از $\{a + \sqrt{m} \mid a, b \in \mathbb{Z}\}$ و در حالت $m < 0$ عبارت است از $\{a + bi + c\sqrt{-m} + di\sqrt{-m} \mid a, b, c, d \in \mathbb{Z}\}$.

۳. به ازای هر $\frac{r}{s} \in Q$ تعریف کنید $\bar{\alpha}\left(\frac{r}{s}\right) = \frac{\alpha(r)}{\alpha(s)}$. نشان دهید $\bar{\alpha}$ خوش‌تعریف، همریختی، یک‌به‌یک و پوشا است.

تمرین‌های ۶.۱۰، تولید ایدآل‌ها، صفحه‌ی ۲۲۴

۱. از $(1 + 2i)(1 - i) = 3 + i$ و $(1 + 3i)(1 - 3i) = 10$ استفاده کنید.
(الف) $R/I = \{0 + I\}$ (j) $R/I = \{0 + I, 1 + I, 2 + I, 3 + I, 4 + I\}$

۴. R^2 یک ایدآل R است، پس طبق فرض $R^2 = \{0\}$ یا $R^2 = R$. اگر $R^2 = \{0\}$ نشان دهید R حلقه‌ی بدیهی است و هر زیرگروه جمعی R ایدآل R نیز هست، و R زیرگروه جمعی نابدیهی ندارد. نتیجه بگیرید گروه جمعی R دوری با مرتبه‌ی عدد اول است. در حالت $R^2 = R$ به صورت زیر نشان دهید R میدان است: چون R توزیع‌پذیر است، به ازای هر $a \in R$، aR ایدآل R است. اگر $aR = \{0\}$ با در نظر گرفتن (a) نشان دهید $R^2 = \{0\}$، پس $aR = R$. سپس با نشان دادن این که $T = \{c \in R \mid ac = 0\}$ یک ایدآل است، نشان دهید R مقسوم‌علیه صفر ندارد. در نهایت با استفاده از $aR = R$ ثابت کنید R یکدار است و هر عضو ناصفر آن وارون ضربی دارد.

۵. از تمرین ۴ و این که یک حلقه‌ی یکدار حلقه‌ی تقسیم است اگر و تنها اگر ایدآل چپ [راست] نابدیهی نداشته باشد استفاده کنید.

۶. چون f پوشا است، به ازای هر $n \in \mathbb{N}$، f^n پوشا است. قرار دهید $\ker f^n = (a_n)$. بنابراین $(a_1) \subseteq (a_2) \subseteq \cdots$. با در نظر گرفتن $\bigcup_{n=1}^{\infty}(a_n)$ نشان دهید nای وجود دارد که، به ازای هر $j \geq 1$، $\ker f^n = \ker f^{n+j}$. نتیجه بگیرید $\ker f = \{0\}$.

تمرین‌های ۷.۱۰، ایدآل‌های اول و ماکسیمال، صفحه‌ی ۲۲۹

۲. اگر P ایدآل اول و I یک ایدآل حلقه‌ی بولی R باشند که $P \subset I \subseteq R$. عضو $a \in I - P$ را اختیار کنید و ثابت کنید $I = R$. اگر $x \in R - P$، نشان دهید $a(ax - x) \in P$، $ax - x \in P$. به علاوه $x(xa - a) \in P$ و $xa - a \in P$. چون R توزیع‌پذیر است نتیجه بگیرید $a - x \in P \subseteq I$ و بنابراین $x \in I$.

۳. اگر P ایدآل اول R باشد، نشان دهید R/P میدان است.

۵. فرض کنید a در هر ایدآل اول قرار داشته باشد و a پوچ‌توان نباشد. با استفاده از لم زُرن نشان دهید که مجموعه‌ی $\{I \mid I \cap A = \emptyset\}$ و ایدآل $R\}$، که در آن $A = \{a^n \mid n \in \mathbb{N}\}$، یک عضو ماکسیمال M دارد که لزوماً ایدآل اول است. پس $a \notin M$ که خلاف فرض است.

۶. نشان دهید R دامنه‌ی صحیح است و برای هر $0 \neq a \in R$ ایدآل (a^2) را در نظر بگیرید.

۱۱. هر زیرگروه $\mathbb{Z}_n$ به صورت $\bar{k}\mathbb{Z}_n$ است که در آن $0 \leq k \leq n-1$، و در واقع هر ایدآل $\mathbb{Z}_n$ به این صورت است. در نتیجه هر ایدآل ماکسیمال $\mathbb{Z}_n$ به صورت $\bar{k}\mathbb{Z}_n = (\bar{k})$ است که در آن $\left|\frac{\mathbb{Z}_n}{\bar{k}\mathbb{Z}_n}\right|$ عدد اول است، اگر $n = p_1^{n_1} \cdots p_r^{n_r}$ نشان دهید ایدال‌های ماکسیمال $\mathbb{Z}_n$ عبارتند از $\bar{p}_i\mathbb{Z}_n$، $1 \leq i \leq r$. نتیجه بگیرید $J(\mathbb{Z}_n) = \bigcap_{i=1}^{r} \bar{p}_i\mathbb{Z}_n$.

۱۳. به استقرا روی n عمل کنید. اگر $I \subseteq \bigcup_{i=1}^{n+1} P_i$ و $I \not\subseteq P_j$، $1 \leq j \leq n+1$ عضو $a_j \in I - \bigcup_{\substack{i=1 \\ i \neq j}}^{n+1} P_j$ وجود دارد (طبق فرض استقرا). در این صورت $a_j \notin P_j$، $1 \leq j \leq n+1$. سپس عضو $a = a_1 + a_2a_3 \cdots a_{n+1}$ را در نظر بگیرید و نشان دهید a در I هست ولی در $\bigcup_{i=1}^{n+1} P_i$ نیست.

۱۶. از لم زُرن استفاده کنید.

۱۸. از تمرین ۷۱ استفاده کنید.

۱۹. اگر حکم درست نباشد، به ازای هر $f \in M$ عدد $0 \leq \alpha \leq 1$، وجود دارد که $f(\alpha) \neq 0$. چون f پیوسته است، همسایگی U_α وجود دارد که f روی آن ناصفر است. پوشش $\{U_\alpha \mid 0 \leq \alpha \leq 1\}$ برای $[0, 1]$ را در نظر بگیرید در این صورت α_n، ...، α_1 وجود دارند که $[0, 1] \subseteq \bigcup_{i=1}^{n} U_{\alpha_i}$. به ازای هر $1 \leq i \leq n$، تابع $f_i \in U_{\alpha_i}$ را اختیار کنید و تعریف کنید $f(x) = f_1(x)^2 + \cdots + f_n(x)^2$. نتیجه بگیرید $f \notin M$.

تمرین‌های ۱.۱۱، خواص مقدماتی چندجمله‌ای‌های، صفحه‌ی ۲۳۷

۲. از قضیه‌ی دوجمله‌ای استفاده کنید.

۳. $m^n(m-1)$ چندجمله‌ای درجه‌ی n در $\mathbb{Z}_m[x]$ وجود دارد که m^n تایی آن‌ها تکین است.

۴. (الف) ریشه‌های در $\mathbb{Z}_3$ عبارتند از ۱، ۲. ریشه در $\mathbb{Z}_6$ عبارتند از ۱، ۲، ۴، ۵

۵. $q(x) = -\frac{15}{8} - \frac{1}{4}x + \frac{1}{2}x^2$، $r(x) = \frac{55}{8}$.

۶. (ب) $q(x) = x^3 + x^2 + 4x + 2$، $r(x) = 5x$.

۱۴. (الف) $f(x) = (x^3 + x^2 + 1)(4x - 3)$

(ب) $f(x) = \left(x - \frac{1}{2}\right)\left(x + \frac{1}{2}\right)(x^2 + x + 1)$

(ج) $f(x) = (x + 1)(x - 2)(x^2 + 1)$

(د) $f(x) = (x - 1)(x^2 + x + 1)(x^2 - x + 1)$

(هـ) $f(x) = (x - 1)\left(x - \frac{3}{2}\right)(x^2 + 1)$

۱۵. $f(x) - g(x)$ را در نظر بگیرید.

۱۷. میدان کسرهای $\mathbb{Z}_p[x]$ را در نظر بگیرید.

۱۸. همریختی $\varphi : R[x] \longrightarrow R/I$ را با $\varphi(f(x)) = f(۰) + I$ در نظر بگیرید.

۱۹. همریختی $\varphi : R[x] \longrightarrow R$ با ضابطه‌ی $\varphi(f(x)) = f(۰)$ در نظر بگیرید.

تمرین‌های ۲.۱۱ و ۳.۱۱، تجزیه‌ی چندجمله‌ای‌ها روی یک میدان، یکتایی تجزیه، صفحه‌ی ۲۴۷

۱. (ج) همریختی $\varphi : \mathbb{C}[x] \longrightarrow \mathbb{C}$ با ضابطه‌های $\varphi(f(x)) = \overline{f(۰)}$ را در نظر بگیرید، که در آن $\bar{a}$ مزدوج مختلط a است.

۹. هر عدد اول فرد به صورت $۴k+۱$ یا $۴k+۳$ است (چرا). اکنون به برهان خلف عمل کنید، یعنی فرض کنید $p \not\equiv ۳ \mod ۴$، پس $p = ۴k+۱$. قرار دهید

$$x = ۱ \times ۲ \times ۳ \times \cdots \times \frac{p-۱}{۲}.$$

چون $p - ۱ = ۴k$، داریم $x = (-۱)(-۲)(-۳) \times \cdots \times \left(-\frac{p-۱}{۲}\right)$. اما در $\mathbb{Z}_p$ داریم $p - m = -m$، پس $x = (p-۱)(p-۲)\cdots\frac{p+۱}{۲}$. نتیجه بگیرید $x^۲ \equiv (p-۱)!$ و از قضیه‌ی ویلسون استفاده کنید.

۱۰. نشان دهید تعداد چندجمله‌ای‌های تکین درجه‌ی دو که روی $\mathbb{Z}_p[x]$ تحویل‌پذیر هستند (یعنی روی $\mathbb{Z}_p$ تجزیه می‌شوند) برابر $\frac{p(p-۱)}{۲} + p = \frac{p(p+۱)}{۲}$ است.

۱۱. (الف) $f(x) = ۳(x+۲)(x+۳)(x-۱)(x+۱)$

(ب) $f(x) = (x+۶)(۳x+۴)$

(ج) $f(x) = (x+۵)(x+۳)(x+۱)$

(د) $f(x) = (x+۳)(x-۱)(x+۴)(x^۲+۱۵x)$

(هـ) $f(x) = (x^۳+x^۲+۱)^۲$

(و) $f(x) = (x^۳-x+۱)(x^۲+۱)$

۱۱. (هـ)، (و)، (ز)، (ح)، (ط)، (ک) از روش مثال ۲۰.۲.۱۱ استفاده کنید.

۱۳. خیر

۱۶. (الف) $f(x)$ تحویل‌ناپذیر است.

(ب) $f(x) = (x-۲)(x^۳+x^۲+۳x-x+۱)$

(ج) $f(x) = (x^۲-x+۲)(x^۲+۳x-۱)$

(د) $f(x)$ تحویل‌ناپذیر است.

(هـ) $f(x) = (x^۲+x+۱)(x^۳-x^۲+۱)$

(و) $f(x)$ تحویل‌ناپذیر است.

۱۸. (الف) $d(x) = ۱$، $۱ = (-x^۲+۳x-۱)f(x) + (x+۳)g(x)$

(ب) $d(x) = x+۱$، $x+۱ = (x^۳+x^۲)f(x) + g(x)$

(ج) $d(x) = x-۲$، $x-۲ = -\frac{۱}{۴}(x^۳+x^۲-x-۱)f(x) + \frac{۱}{۴}g(x)$

تمرین‌های ۴.۱۱، حلقه‌های خارج‌قسمتی چندجمله‌ای‌ها روی یک میدان، صفحه‌ی ۲۵۳

۱. (الف) $h(x) = x$ (ب) $h(x) = x-۱$

(ج) $h(x) = x(x-۱)$ (د) $h(x) = x(x-۱)(x-۲)$.

۲. (الف) $R = \{۰, ۱, t, ۱+t\}$

$+$	۰	۱	t	$۱+t$
۰	۰	۱	t	$۱+t$
۱	۱	۰	$۱+t$	t
t	t	$۱+t$	۰	۱
$۱+t$	$۱+t$	t	۱	۰

$\times$	۰	۱	t	$۱+t$
۰	۰	۰	۰	۰
۱	۰	۱	t	$۱+t$
t	۰	t	۱	۰
$۱+t$	۰	$۱+t$	$۱+t$	۰

(ب) $R = \{۰, ۱, t, ۱+t\}$

$+$	۰	۱	t	$۱+t$
۰	۰	۱	t	$۱+t$
۱	۱	۰	$۱+t$	t
t	t	$۱+t$	۰	۱
$۱+t$	$۱+t$	t	۱	۰

$\times$	۰	۱	t	$۱+t$
۰	۰	۰	۰	۰
۱	۰	۱	t	$۱+t$
t	۰	t	t	۰
$۱+t$	۰	$۱+t$	۰	$۱+t$

۳. (الف) $R = \dfrac{\mathbb{Z}_۲[x]}{(x^۳+x+۱)}$ (ب) $R = \dfrac{\mathbb{Z}_۳[x]}{(x^۲+۱)}$

۴. (الف) خودنوان‌ها ۰، ۱، t، $t-۱$. عضو پوچ‌توان ۰. یکه‌ها: $a+bt$، که $a \neq -b$ و $a \neq ۰$.

۵. $\{a+b\sqrt[۳]{۲} \mid a,b,c \in \mathbb{Q}\}$

تمرین‌های ۱.۱۲، تجزیه و تحویل‌ناپذیرها، صفحه‌ی ۲۵۷

۱. (الف) $\pm(۳-۲i)$، $\pm(۲+۳i)$ (ب) $\pm(۱+i\sqrt{۵})$
(ج) $\bar{۶}$، $\bar{۸}$، $\bar{۲}$، $\bar{۴}$ (و) $\pm(۲+x-۳x^۲)$

۳. فرض کنید $d = \gcd\{a,c\}$. اگر $c|(ax-b)$، آنگاه $r \in R$ وجود دارد که $ax-b = rc$. پس $b = ax - rc \in (a,c) = (d)$ و $d|b$. برعکس اگر $d|b$ آنگاه $b \in (d) = (a,c)$. از این‌رو $b = ra+sc$ و $c|(ra-b)$.

۵. (b) $\Longleftarrow$ (الف) فرض کنید $d = \gcd\{a,b\}$، آنگاه طبق فرض $d = ra+sb$. پس $d \in (a,b)$ و $(d) \subseteq (a,b)$. از طرف دیگر $d|a$ و $d|b$. پس $(a,b) \in (d)$ و $(a,b) \subseteq (d)$.

تمرین‌های ۲.۱۲، عناصر اول و تحویل‌ناپذیر، صفحه‌ی ۲۵۹

۱. (الف) و (ب) ± ۱.

۲. ۱۱ و $۲-i$ در $\mathbb{Z}[i]$ تحویل‌ناپذیر، ۵ و $۷-i$ تحویل‌پذیر.

۳. $۵+i\sqrt{۵}$، ۶، ۷، $۲-۳i\sqrt{۵}$ در $\mathbb{Z}[i\sqrt{۵}]$ تحویل‌ناپذیرند و ۲۹ تحویل‌پذیر.

۴. هر دو عضو تحویل‌ناپذیرند و اول نیستند.

۸. اگر $p = ab$، آنگاه $p^۲ = N(p) = N(a)N(b)$. اگر $N(a) = p$ و $a = m+in$، آنگاه $m^۲+n^۲ = p$. چون p فرد است، پس m زوج و n فرد است یا m فرد و n زوج است. در هر صورت به دست می‌آید $p = m^۲+n^۲ \equiv ۱ \mod ۴$، که خلاف $p \equiv ۳ \mod ۴$ است. پس $N(a) = ۱$ یا $N(b) = ۱$. بنابراین یا a یکه است یا b یکه است.

۹. (ب) بنا به (الف) عدد k وجود دارد که $k^۲ \equiv -۱ \mod p$. می‌توان فرض کرد $۰ \leq k \leq p-۱$، زیرا فقط باقیمانده‌ی تقسیم k به p مورد نیاز است. در واقع می‌توانیم فرض کنیم $۰ \leq k \leq \frac{p}{۲}$، زیرا اگر $k > \frac{p}{۲}$، آنگاه $r = p-k$ در $r^۲ \equiv -۱ \mod p$ صدق می‌کند

و $0 \leq r \leq \frac{p}{2}$. اکنون عدد c وجود دارد که $k^2 + 1 = cp$. اگر p در $\mathbb{Z}[i]$ اول باشد چون $cp = k^2 + 1 = (k-i)(k+i)$ باید داشته باشیم $p|k+i$ Ia $p|k-i$. اگر $p|k+i$ عضو $a+ib+\mathbb{Z}[i]$ وجود دارد که $k+i = p(a+ib)$. سپس $k = pa$ و $pb = 1$، که نتیجه می‌دهد $p = \pm 1$ و این تناقض است. به همین نحو حالت $p|k-i$ رد می‌شود.

(j) چون p در $\mathbb{Z}[i]$ اول نیست، اعضای نایکه‌ی $c+id$ و $a+ib$ در $\mathbb{Z}[i]$ وجود دارند که $p = (a+ib)(c+id)$. پس $p = (a-ib)(c-id)$. نتیجه بگیرید $p^2 = (a^2+b^2)(c^2+d^2)$ و چون $a^2+b^2 \neq 1$ و $c^2+d^2 \neq 1$ داریم $p = a^2+b^2 = c^2+d^2$.

تمرین‌های ۳.۱۲، دامنه‌های تجزیه‌ی یکتا، صفحه‌ی ۲۶۲

۲. اگر

$$(f_1(x)) \subseteq (f_2(x)) \subseteq \cdots$$

زنجیر صعودی از ایدآل‌های اصلی $R[x]$ باشد، آنگاه $\cdots \geq \deg f_2(x) \geq \deg f_1(x)$ و عدد n وجود دارد که $\deg f_n(x) = \deg f_{n+i}(x)$. بنابراین $b_{n+i} \in R$ وجود دارد که $f_n(x) = b_{n+i} f_{n+i}(x)$. کافی است ثابت کنیم b_{m+i}، به ازای یک m، یکه است. فرض کنید $a_j \in R$ ضریب پیشرو $f_j(x)$ باشد. پس $a_n = a_{n+i} b_{n+i}$ و زنجیر صعودی

$$(a_n) \subseteq (a_{n+1}) \subseteq \cdots$$

را داریم. پس عدد $m \geq n$ وجود دارد که $(a_m) = (a_{m+i})$. بنابراین a_m و a_{m+i} همدم هستند. از این رو b_{m+i} یکه است

۴. ۳ در $\mathbb{Z}[i\sqrt{5}]$، و $\mathbb{Z}[i\sqrt{7}]$ تحویل‌ناپذیر است ولی اول نیست. ۱۱ در $\mathbb{Z}[i\sqrt{10}]$ تحویل‌ناپذیر است ولی اول نیست.

تمرین‌های ۴.۱۲، تجزیه‌ی چندجمله‌ای‌ها روی یک UFD، صفحه‌ی ۲۶۶

۴. چون $\mathbb{Z}$ یک UFD است، $\mathbb{Z}[x]$ نیز UFD است. از طرف دیگر $(2, x)$ ایدآل اصلی نیست (چرا؟)، پس $\mathbb{Z}[x]$ یک PID نیست

تمرین‌های ۵.۱۲ و ۶.۱۲، دامنه‌های اقلیدسی، برخی حلقه‌های اعداد صحیح، صفحه‌ی ۲۷۰

۲. (ب) $b + (-1 + i\sqrt{2})$ و $a = (1 + i\sqrt{2})$.

۳. (ب) $b + (0 - \sqrt{3})$ و $a = (-2 + \sqrt{3})$

۵. $a = 2$ و $b = 1 + i\sqrt{3}$ را در نظر بگیرید.

۶. عضو یکه $u \in R$ وجود دارد که $a = bu$. طبق خاصیت (ب) دامنه‌های اقلیدسی $v(a) = v(bu) \geq v(b)$. به همین نحو چون $b = au^{-1}$، $v(b) \geq v(a)$.

۹. فرض کنید b یکه است، به ازای هر عضو ناصفر $a \in R$ داریم $v(ab) \geq v(a)$. از طرف دیگر با توجه به این که $v(a) = v(abb^{-1}) \geq v(ab)$، داریم $v(a) = v(ab)$. برعکس اگر به ازای هر $0 \neq a \in R$، $v(ab) = v(a)$، یا فرض $a = 1$ داریم $v(b) = v(1)$. پس b یکه است.

تمرین‌های فصل ۲۸۱، مدول‌ها، صفحه‌ی ۲۸۱

۲. $\mathbb{Q}$ را در نظر بگیرید.

۴. نشان دهید $\operatorname{Im} f \cap \ker f = \{0\}$ و به ازای هر $a \in A$،

$$a = f(a) + (a - f(a)) \in \operatorname{Im} f + \ker f$$

۵. نشان دهید $\operatorname{Im} f \cap \ker g = \{۰\}$ و به ازای هر $x \in M$،

$$x = f(g(x)) + (x - f(g(x))) \in \operatorname{Im} f + \ker g$$

۶. برای R- مدول دوری Ra تابع $\varphi : R \longrightarrow Ra$ با $\varphi(a) = ra$ را در نظر بگیرید.

۱۲. به استقرا روی n عمل کنید. اگر $V \subseteq \bigcup_{i=۱}^{n+۱} W_i$، بنا به فرض استقرا، می‌توان فرض کرد $V \nsubseteq \bigcup_{i=۱}^{n} W_i$ و $V \nsubseteq W_{n+۱}$. پس $x \in V - \bigcup_{i=۱}^{i=۱} W_i$ و $y \in V - W_{n+۱}$ وجود دارند. $n+۲$ اسکالر $r_۱$، $r_۲$، ...، $r_{n+۲}$ و اعضای $x + r_۱y$، $x + r_۲y$، ...، $x + r_{n+۲}y$ در V را در نظر بگیرید. بنا به اصل لانه کبوتری $۱ \leq j \leq n+۱$ و $۱ \leq k \leq t \leq n+۲$ وجود دارند که $k \neq t$ و $x + r_ky$ و $x + r_ty \in W_j$. از این که $x \notin \bigcup_{i=۱}^{n} W_i$ و $y \notin W_{n+۱}$ و میدان بدون R استفاده کنید.

۱۴. فرض کنید $f : \frac{R}{I} \longrightarrow \frac{R}{J}$ همریختی R- مدولی چپ است. در این صورت $f(۱ + I) = r + J$، که در آن $r \in R$. عضو دلخواه، $a \in J$ را در نظر بگیرید. از این که f همریختی R- مدولی چپ و R تحویل‌پذیر است نتیجه بگیرید $f(a + I) = J$. پس $a + I \in \ker f = \{I\}$ و $a \in I$. برای مثال حلقه‌ی ماتریس‌های ۲×۲ و I و J مجموعه‌ی ماتریس‌هایی که به ترتیب ستون اول و ستون دوم آن‌ها صفر است در نظر بگیرید.

تمرین‌های ۱.۱۴، توسیع‌های جبری، صفحه‌ی ۲۹۰

۲. (الف) $\{۱, \sqrt[۳]{۲}, \sqrt[۳]{۴}\}$ (ب) $\{۱, i\}$
(ج) $\{۱, \sqrt{۳}, \sqrt{۷}, \sqrt{۲۱}\}$ (د) $\{۱, \sqrt{۲}, \sqrt[۳]{۳}, \sqrt[۳]{۹}, \sqrt{۲}\sqrt[۳]{۹}, \sqrt{۲}\sqrt[۳]{۳}\}$.

۳. درجه‌ی توسیع‌های (الف)، (ب) و (ج) برابر ۲ و درجه‌ی توسیع (د) برابر ۳ است.

۴. چندجمله‌ای می‌نیمال $e^{i\theta}$ عبارت است از $x^۶ + x^۵ + \cdots + x + ۱$.

۵. از قانون برج استفاده کنید.

۶. (الف) با توجه به $[K(a,b) : K(b)] \leq \deg m_a(x) = m$ از قانون برج استفاده کنید.
(ب) با استفاده از قانون برج نشان دهید m و n هر دو $[K(a,b) : K]$ را عاد می‌کند.
(ج) $\mathbb{Q}(\sqrt{۲}, \sqrt{۳}) : \mathbb{Q}$ را در نظر بگیرید.

۸. توجه کنید که $K(f(a)) \subseteq K(a)$.

۱۱. نشان دهید $K[x]$ شمارا است و نتیجه بگیرید مجموعه‌ی T متشکل از چندجمله‌ای‌های ماکسیمال اعضای F نیز شمارا است. اگر R_m مجموعه‌ی همه‌ی ریشه‌های $m(x) \in T$ در F باشد، آنگاه R_m متناهی است، و نتیجه بگیرید $F = \bigcup_{m(x) \in T} R_m$ شمارا است.

۱۳. اگر K میدان بسته‌ی جبری باشد و $|K| < \infty$، آنگاه n عدد اول $p_۱$، $p_۲$، ...، p_n را طوری اختیار کنید که $n > |K|$. چندجمله‌ای‌های $x^{p_j} - ۱$، $۱ \leq j \leq n$ را در نظر گرفته و نتیجه بگیرید $۱ \neq a \in K$ و $i \neq j$ وجود دارند که $a^{p_i} = ۱$ و $a^{p_j} = ۱$. در نهایت نتیجه بگیرید $a = ۱$ که تناقض است.

۱۴. توجه کنید $K(y)$ میدان کسرهای $K[y]$ است. حال کافی است ثابت کنیم $f - yg$ روی $K[y][x] = K[x,y]$ تحویل‌ناپذیر است. اگر $h(x,y), r(x,y) \in K[x,y]$ وجود داشته باشند که $f(x) - yg(x) = h(x,y)r(x,y)$، آنگاه با مقایسه‌ی درجه‌های دو طرف تساوی نشان دهید $h(x,y) = t(x+y)s(x)$ و $r(x,y) = p(x)$ و نتیجه بگیرید $p(x)$ هم $f(x)$ و $g(x)$ را در $K[x]$ عاد می‌کند که این خلاف متباین بودن f و g است.
برای مثال نقض قرار دهید $K = \mathbb{Q}$، $f = x^۲ - ۱$، $g = ۲x$ و $y = i$.

۱۵. (الف) چون a روی K متعالی است و $b \in K(a)$، پس $f(x), g(x) \in K[x]$ وجود دارند که $b = \frac{f(a)}{g(a)}$. چون $s = g(a)$ متعالی است. $s^{-۱}$ نیز متعالی است. با استفاده از قانون برج روی $K \subset K(rs^{-۱}) \subseteq K(r, s^{-۱})$، که در آن $r = f(a)$، نشان دهید $b = \frac{f(a)}{g(a)}$ روی K متعالی است.

(ب) بنا به تمرین ۵۱، $h(x) = f(x) - bg(x)$ روی $K(b)$ متعالی است. نشان دهید $h(x)$ چندجمله‌ای می‌نیمال a روی $K(b)$ است، و اکنون از این که $K(a,b) = K(a)$ استفاده کنید.

تمرین‌های ۲.۱۴، توسیع‌های تجزیه، صفحه‌ی ۲۹۶

۱. (الف) اگر $w = e^{۲\frac{i\pi}{۳}}$، آنگاه ریشه‌های f عبارت‌اند از

$$-۱, \quad -w = -\frac{-۱ + i\sqrt{۳}}{۲}, \quad -w^۲ = -e^{۴i\frac{\pi}{۳}} = -\frac{-۱ - i\sqrt{۳}}{۲}$$

داریم $\mathbb{Q}(-۱, -w, -w^۲) = \mathbb{Q}(w) = \mathbb{Q}(i\sqrt{۳})$. بنابراین $\mathbb{Q}(w) : \mathbb{Q}$ توسیع تجزیه‌ی $f(x)$ است. چون چندجمله‌ای می‌نیمال w روی $\mathbb{Q}$ عبارت است از $۱ + x + x^۲$، درجه‌ی توسیع برابر ۲ است.
(ب) اگر $u = e^{۲\frac{i\pi}{۹}}$، آنگاه $\mathbb{Q}(u) : \mathbb{Q}$ توسیع تجزیه‌ی $f(x)$، و درجه‌ی آن ۶ است.
(هـ) $\mathbb{Q}(\sqrt{۲}, \sqrt{۵}) : \mathbb{Q}$ توسیع تجزیه‌ی $f(x)$، و درجه‌ی آن ۴ است.
(و) $\mathbb{Q}(i, \sqrt{۷}) : \mathbb{Q}$ توسیع تجزیه‌ی $f(x)$، و درجه‌ی آن ۴ است.

۲. (الف) $f(x)$ در $\mathbb{Z}_۲$ ریشه ای ندارد. چون $\deg f(x) = ۲$، پس $f(x)$ روی $\mathbb{Z}_۲$ تحویل‌ناپذیر است. بنا به قضیه‌ی کرونکر توسیع $\mathbb{Z}_۲ : \mathbb{Z}_۲(a)$ وجود دارد که a ریشه‌ای از $f(x)$ است. داریم $\mathbb{Z}_۲(a) = \{۰, ۱, a, ۱ + a\}$. با امتحان اعضای $\mathbb{Z}_۲(a)$ می‌بینیم که $a + ۱$ ریشه‌ای از $f(x)$ است، زیرا

$$f(a+۱) = (a+۱)^۲ + (a+۱) + ۱ = a^۲ + ۱ + a + ۱ + ۱ = a^۲ + a + ۱ = f(a) = ۰.$$

پس $\mathbb{Z}_۲(a) : \mathbb{Z}_۲$ توسیع تجزیه‌ی $f(x)$ و درجه‌ی آن ۲ است.
(ب) در $\mathbb{Z}_۳[x]$ داریم $x^۳ + ۱ = (x+۱)(x^۲ + ۲x + ۱)$. چون $x^۲ + ۲x + ۱$ در $\mathbb{Z}_۳$ ریشه ندارد ، روی $\mathbb{Z}_۳$ تحویل‌ناپذیر است. بنا به قضیه‌ی کرونکر توسیع $\mathbb{Z}_۳(a) : \mathbb{Z}_۳$ وجود دارد که $a^۲ + ۲a + ۱ = ۰$. داریم

$$\mathbb{Z}_۳(a) = \{۰, ۱, ۲, a, ۲a, ۱ + a, ۲ + a, ۱ + ۲a, ۲ + ۲a\}.$$

$x^۲ + ۲x + ۱$ روی $\mathbb{Z}_۳(a)$ تجزیه می‌شود، زیرا $x - a$ در $\mathbb{Z}_۳(a)[x]$ آن را عاد می‌کند. در واقع اگر b ریشه‌ای از آن باشد،

$$x^۲ + ۲x + ۱ = (x-a)(x-b) = x^۲ - (a+b)x + ab$$

که نتیجه می‌دهد $b = ۲a + ۲$. پس $\mathbb{Z}_۳(a) : \mathbb{Z}_۳$ توسیع تجزیه‌ی $f(x)$ با درجه‌ی ۲ است.

۳. فرض کنید در $K[x]$، $f(x) = g(x)h(x)$، که در آن $۰ < \deg g(x) = m < p$ و $h(x)$ و $g(x)$ تکین هستند. داریم $g(۰) = d \in K$. اکنون b را ریشه‌ای از $f(x)$ در توسیعی از K در نظر بگیرید. دو حالت را بررسی کنید: در حالت $\operatorname{char} K = p$، نشان دهید همه‌ی ریشه‌های $f(x)$ با b برابرند و نتیجه بگیرید $b^m = d$ و $b = d^s a^t \in K$، که در آن $sm + tp = ۱$. در حالت $\operatorname{char} R \neq p$، نشان دهید هر ریشه‌ی دلخواه c از $f(x)$ به صورت $c = bu$ است که در آن $u^p = ۱$ و مثل استدلال مثال ۵.۲.۱۴ عمل کنید.

۹. فرض کنید a یک ریشه‌ی چندجمله‌ای $f(x) = x^n - ۱$. اگر $p|n$، آنگاه داریم $f(a) = f'(a) = ۰$. پس a ریشه‌ی تکراری $f(x)$ است که خلاف فرض است.

۱۰. از تمرین ۳ استفاده کنید. اگر $f(x)$ روی K تحویل‌پذیر باشد، آنگاه ریشه ای مثل b در K دارد. پس $f(x) = x^p - a = x^p - b^p = (x-b)^p$.

تمرین‌های ۳.۱۴، میدان‌های متناهی، صفحه‌ی ۳۰۹

۲. زیرمیدان‌های $\mathrm{GF}(p^۸)$ عبارت‌اند از $\mathrm{GF}(p)$، $\mathrm{GF}(p^۲)$، $\mathrm{GF}(p^۴)$.

۳. اگر $K^\times = \langle a\rangle$ و L زیرمیدان اول K باشد، نشان دهید $K = L(a)$ و نتیجه بگیرید a روی K جبری است و $L \cong \mathbb{Z}_p$.

۴. اگر a ریشه‌ای از $x^۲ + x + ۱$ باشد نشان دهید به ازای هر $k \geq ۱$، $a^{۲^k}$ نیز ریشه است.

۹. $f(a+u)$ را برای $u \in \mathbb{Z}_p$ حساب کنید.

۱۰. به ازای هر $a \in K$، نشان دهید که مجموعه‌های $X = \{u^۲ \mid u \in K\}$ و $Y = \{a - u^۲ \mid u \in K\}$ بیش از $\frac{۱}{۲}|K|$ عضو دارند

۱۱. اگر $m|(q-۱)$، آنگاه $n \in \mathbb{N}$ وجود دارد که $m = n(q-۱)$. به ازای هر $a \in \mathrm{GF}(q)^\times$ داریم $a^m = a^{n(q-۱)} = ۱$. پس $(a^{q-۱})^n = ۱$.

$$\sum_{a\in \mathrm{GF}(q)} a^m = \sum_{a\in \mathrm{GF}(q)^\times} a^m = \sum_{a\in \mathrm{GF}(q)^\times} ۱ = q - ۱ = ۱.$$

اکنون فرض کنید $m \nmid (q-۱)$. داریم $GF(q)^\times = \langle b\rangle$. بنابراین $b^m - ۱ \neq ۰$ و

$$\begin{aligned}\sum_{a\in \mathrm{GF}(q)} a^m &= \sum_{j=۰}^{q-۲} (b^j)^m \\ &= (b^m - ۱)^{-۱}\left((b^m)^{q-۱} - ۱\right) \\ &= (b^m - ۱)^{-۱}\, ۰ \\ &= ۰.\end{aligned}$$

۱۴. اگر $q = ۲^n$، آنگاه $\mathrm{GF}(q)$، ۲^n عضو دارد و هر عضو آن مربع است. پس عضو $a \in \mathrm{GF}(q)$ وجود دارد که $a^{-۱} = a^۲$. پس $۱ + aa^{-۱} = ۰$. اگر $q = p^n$ و $p \neq ۲$، قرار دهید $M_a = \{۱ + ax^۲ \mid x \in \mathrm{GF}(q)\}$ و $M_b = \{-bx^۲ \mid x \in \mathrm{GF}(q)\}$، آنگاه $|M_a| = |M_b| = \frac{q+۱}{۲}$. پس عضو $c \in M_a \cap M_b$ وجود دارد ، یعنی $c = ۱ + ar^۲$ و $c = -bs^۲$. پس $۱ + ar^۲ = -bs^۲$.

۱۵. اگر $f(x)$ تحویل‌ناپذیر باشد، آنگاه تنها یک چندجمله‌ای تحویل‌ناپذیر با مرتبه‌ی e وجود دارد. بنابراین $\frac{\varphi(e)}{e-۱} = ۱$، یعنی e عدد اول است. به علاوه چون $\mathrm{GF}(q^{e-۱})$ میدان تجزیه برای $f(x)$ روی $\mathrm{GF}(q)$ است، داریم $e|(q^{e-۱} - ۱)$ و به ازای هر $k < e - ۱$، $e \nmid (q^k - ۱)$. پس q یک ریشه‌ی اولیه‌ی eام واحد (به پیمانه‌ی e) است.
بر عکس اگر e عدد اول و q ریشه‌ی اولیه‌ی $(e-۱)$ام واحد باشد، آنگاه $f(x)$ تحویل‌ناپذیر است، زیرا درجه‌ی چندجمله‌ای می‌نیمال یک ریشه‌ی $f(x)$ باید برابر $e-۱$ باشد.

۱۶. به سادگی می‌توان دید چندجمله‌ای‌های داده شده روی $\mathbb{Z}_۲$ تحویل‌ناپذیرند. از طرف دیگر بنا به قضیه‌ی ۲۴.۳.۱۴ تعداد چندجمله‌ای‌های تکین تحویل‌ناپذیر روی $\mathbb{Z}_۲$ عبارت است از

$$I_۲(۴) = \frac{۱}{۴}\sum_{d|۴} \mu\left(\frac{۴}{d}\right) ۲^d = ۳.$$

۲۰. فرض کنید مرتبه‌ی $f(x)$ برابر e و مرتبه‌ی $f_i(x)$ برابر e_i، $i = ۱, ۲, \ldots, k$، باشد و $m = \gcd\{e_۱, \ldots, e_k\}$؛ در این صورت $f_i(x)|x^{e_i} - ۱$ و $f_i(x)|x^m - ۱$. چون $f_۱(x)$، ...، $f_k(x)$ نسبت به هم اول هستند ، $f(x)|x^m - ۱$. پس بنا به لم ۳۰.۳.۱۴ داریم $e|m$. چون $f(x)|x^e - ۱$، بنا به همان لم داریم $f_i(x)|x^e - ۱$. پس $e = m$.

۲۴. $f(x)$ روی $\mathbb{Z}_p$ تحویل‌ناپذیر است اگر و تنها اگر p یک ریشه‌ی اولیه‌ی ۱۸ام واحد باشد. اکنون ۱۹ شمارنده‌ای از $۲^{۱۸} - ۱ = ۲۶۲۱۴۳$ است و مستقیماً می‌توان نشان داد برای $k < ۱۸$، $۱۹ \nmid ۲^k - ۱$. پس $f(x)$ روی $\mathbb{Z}_۲$ تحویل‌ناپذیر است.

۲۵. از قضیه‌ی ۳۱.۳.۱۴ استفاده کنید.

تمرین‌های ۴.۱۴، توسیع‌های جداپذیر ، صفحه‌ی ۳۱۲

۱. (الف) $F = \mathbb{Q}(\sqrt{۳} + \sqrt{۷})$

۴. اگر $\frac{f(t)}{g(t)} \in F$ و $\left(\frac{f(t)}{g(t)}\right)^{۲} - t = ۰$، آنگاه $(f(t))^{۲} = t(g(t))^{۲}$. با مقایسه‌ی درجه‌ی دو طرف تساوی به تناقض برسید.

۵. $F : K$ توسیع جبری است. اگر $a \in F$ با چندجمله‌ای می‌نیمال $m(x)$ از درجه‌ی n باشد، آنگاه $[K(a) : K] = n$ و $n|[F : K]$. چون $p \nmid n$، $m'(x) \neq ۰$. پس ریشه‌های $m(x)$ متمایزند.

تمرین‌های ۵.۱۴، گروه گالوای توسیع، صفحه‌ی ۳۱۸

۴. (الف) $w = e^{۲\frac{\pi i}{۸}}$ ریشه‌ی چندجمله‌ای تحویل‌ناپذیر $f(x) = x^{۴} + ۱$ و $[F : \mathbb{Q}] = ۴$. $F : \mathbb{Q}$ توسیع تجزیه‌ی $f(x)$ است و ریشه‌های $f(x)$ عبارت‌اند از $w, w^{۳}, w^{۵}, w^{۷}$. به علاوه $\operatorname{Aut}_{\mathbb{Q}}F = \{\mathrm{id}_F, \alpha_۳, \alpha_۵, \alpha_۷\} \cong V_۴$، که در آن $\alpha_j : F \longrightarrow F$، $\alpha_j(w) = w^j$.
(ب) $F : \mathbb{Q}$ توسیع تجزیه‌ی $f(x) = x^{۳} + ۱$ است و $[F : \mathbb{Q}] = ۳$. چون $f(x)$ جداپذیر و $F : \mathbb{Q}$ توسیع تجزیه‌ی $f(x)$ است، داریم $|\operatorname{Aut}_{\mathbb{Q}}F| = ۳$. پس $\operatorname{Aut}_{\mathbb{Q}}F \cong C_۳$.
(ج) $F : \mathbb{Q}$ توسیع تجزیه‌ی $(x^{۲} - ۲)(x^{۲} - ۵)$ است، $|\operatorname{Aut}_{\mathbb{Q}}F| = [F : \mathbb{Q}] = ۴$، $\operatorname{Aut}_{\mathbb{Q}}F = \{\mathrm{id}_F, \beta_۱, \beta_۲, \beta_۳\}$، که در آن $a = \sqrt{۲}$ و $b = \sqrt{۵}$) $\beta_۱(a) = -a$، $\beta_۱(b) = b$، $\beta_۲(a) = -a$، $\beta_۲(b) = -b$، $\beta_۳(a) = a$، $\beta_۳(-b) = -b$.
(هـ) $\operatorname{Aut}_{\mathbb{Q}}F \cong V_۴$
(و) $\operatorname{Aut}_{\mathbb{Q}}F = \{\mathrm{id}_F\}$
(د) $\operatorname{Aut}_{\mathbb{Q}}F \cong C_۲$

۶. اگر $f(x) = x^{۶} + x^{۳} - ۱ = (x^{۲} + x - ۱)^{۳}$ و $u \in F$ ریشه‌ای از $f(x)$ باشد، آنگاه $f(۲u + ۲) = ۰$. چون $f(x)$ تنها دو ریشه‌ی متمایز دارد ، $F = \mathbb{Z}_۳(u)$ توسیع تجزیه‌ی $f(x)$ روی $\mathbb{Z}_۳$ است و $\operatorname{Aut}_{\mathbb{Z}_۳}F \cong C_۲$.

۷. $F = \mathbb{Q}(\sqrt[۴]{۲}, i)$ توسیع تجزیه‌ی $f(x) = x^{۴} - ۲$ روی $\mathbb{Q}$ است. ریشه‌های $f(x)$ عبارت‌اند از $\pm a$، $\pm$، که در آن $a = \sqrt[۴]{۲}$. می‌توان دید $[F : \mathbb{Q}] = ۸$ و چون ریشه‌های $f(x)$ متمایزند، $|\operatorname{Aut}_{\mathbb{Q}}F| = ۸$. چون $f(x)$ روی $\mathbb{Q}$ تحویل‌ناپذیر است $\operatorname{Aut}_{\mathbb{Q}}F$ روی مجموعه‌ی ریشه‌های به صورت ترایا عمل می‌کند. پس $\alpha, \beta \in \operatorname{Aut}_{\mathbb{Q}}F$ وجود دارند که $\alpha(a) =$ ، $\alpha() = -a$ و $\beta(a) = a$، $\beta() = -$. پس $\alpha(i) = i$ و چون $\beta(i) = -i$. به سادگی می‌توان دید $O(\alpha) = ۴$ و $O(\beta) = ۲$ و $\alpha\beta\alpha = \beta$. که از آن جا نتیجه می‌شود $\operatorname{Aut}_{\mathbb{Q}}F = \langle \alpha, \beta \rangle \cong D_۸$.

۹. فرض کنید $a = \sqrt[۳]{۷}$ و $w = e^{۲\frac{\pi i}{۳}}$، در این صورت $F = \mathbb{Q}(a, w)$ توسیع تجزیه‌ی $f(x)$ روی $\mathbb{Q}$ است و $\operatorname{Aut}_{\mathbb{Q}}F \cong S_۳$.

تمرین‌های ۶.۱۴، چندجمله‌ای‌های دایره‌بر و قضیه‌ی ودربرن، صفحه‌ی ۳۲۵

۱. (الف) $\Phi_۸(x) = x^{۴} + ۱$ (ب) $\Phi_۹(x) = x^{۶} + x^{۳} + ۱$
(ج) $\Phi_{۱۰}(x) = x^{۴} - x^{۳} + x^{۲} - ۱$

۲. (الف) اگر $F : \mathbb{Q}$ توسیع تجزیه‌ی $f(x)$ باشد، $\operatorname{Aut}_{\mathbb{Q}}F \cong \mathbb{Z}_۶^{\times} \cong \mathbb{Z}_۲$.
(ب) هر دو با $\mathbb{Z}_۲$ یکریخت‌اند.

۳. از فرمول $\Phi_n(x) = \Pi_{d|n, d>۰}\Phi_d(x)$، و در صورت نیاز از $\Phi_۲(x) = -\Phi_۱(-x)$، استفاده کنید.

۶. اگر a یک ریشه‌ی اولیه‌ی pnام واحد باشد، آنگاه a^p یک ریشه‌ی اولیه‌ی nام واحد است، پس $\Phi_n(x^p)|\Phi_{pn}(x)$ و چندجمله‌ای $f(x)$ وجود دارد که $\Phi_n(x^p) = f(x)\Phi_{pn}(x)$. توجه کنید که $\deg f(x) = \varphi(x)$ زیرا $\gcd\{p, n\} = ۱$ و

$$p\varphi(n) = \deg f(x) + \varphi(pn).$$

حال اگر b یک ریشه‌ی nام اولیه‌ی واحد باشد آنگاه b^p نیز چنین است. پس b ریشه‌ای از $\Phi_n(x^p)$ است. بنابراین b ریشه‌ای از $f(x)$ است و $\Phi_n(x)|f(x)$. چون $f(x)$ تکین با درجه‌ی $\varphi(n)$ است، $f(x) = \Phi_n(x)$.

۷. به طریق زیر نشان دهید $\Phi_{p^n}(x) = \Phi_p(x^{p^{n-1}})$. هر ریشه‌ی $\Phi_{p^n}(x)$ ریشه‌ای از $\Phi_p(x^{p^{n-1}})$ است، پس $\Phi_{p^n}(x)|\Phi_p(x^{p^{n-1}})$ و

$$\varphi(p^n) = \deg \Phi_{p^n}(x) = \deg \Phi_p(x^{p^{n-1}}) = p^{n-1}\varphi(p)$$

۹. $\mathbb{Z}_p \subseteq R$ در نظر بگیرید و اگر $G = \{g_1, \ldots, g_n\}$، $R_0 = \{\sum r_i g_i \mid r_i \in \mathbb{Z}_p\}$ را در نظر بگیرید.

۱۳. فرض کنید A مجموعه‌ی اعضایی از $\mathrm{GF}(q^n)$ باشد که درجه‌ی آن‌ها روی $\mathrm{GF}(q)$ برابر $n > 1$ است. درجه‌ی چندجمله‌ای می‌نیمال هر $a \in A$ روی $\mathrm{GF}(q)$ برابر n است، پس چنین aی ریشه‌ای از $I(n,q;x)$ است. اگر b ریشه‌ای از $I(n,q;x)$ باشد، آنگاه b ریشه‌ای از یک چندجمله‌ای تکین تحویل‌ناپذیر از درجه‌ی n روی $\mathrm{GF}(q)$ است. پس $b \in A$ و $I(n,q;x) = \prod_{a\in A}(x-a)$. به وضوح به ازای هر $a \in A$ مرتبه‌ی a شمارنده‌ای از $q^n - 1$ است. به سادگی می‌توان نشان داد که اگر مرتبه‌ی $a \in A$ برابر m باشد، آنگاه n مرتبه‌ی ضربی q به پیمانه‌ی m است، یعنی $q^n \equiv 1 \mod n$. فرض کنید A_m مجموعه‌ی همه‌ی اعضای A با مرتبه‌ی m باشد. در این صورت A اجتماع مجزای A_mها است؛ پس $I(n,q;x) = \prod_m \prod_{a\in A_m}(x-a)$. مجموعه‌ی A_m شامل همه‌ی عناصر $\mathrm{GF}(q^n)^\times$ با مرتبه‌ی m است، پس برابر مجموعه‌ی ریشه‌های اولیه‌ی mام واحد روی $GF(q)$ است. از این‌رو بنا به تعریف چندجمله‌ای‌های دایره‌بر $\prod_{a\in A_m}(x-a) = \Phi_m(x)$.

۱۴. $\dfrac{(x^{64}-x)(x^2-x)}{(x^8-x)(x^4-x)}$.

تمرین‌های ۸.۱۴، قضیه‌ی اساسی گالوا، صفحه‌ی ۳۳۵

۱. چون $f(x)$ روی K تحویل‌ناپذیر است و $\deg f(x) = 3$، روی K ریشه ای ندارد. چون $f(x)$ جداپذیر است، ریشه‌های آن متمایزند. اگر a_1، a_2، a_3 ریشه‌های $f(x)$ در توسیع تجزیه‌ی $F : K$ باشند، آنگاه $f(x) = (x-a_1)(x-a_2)(x-a_3)$. پس

$$\begin{aligned} a_1 + a_2 + a_3 &= 0 \\ a_1a_2 + a_1a_3 + a_2a_3 &= b \\ -a_1a_2a_3 &= c \end{aligned}$$

داریم

$$\begin{aligned} D &= -4b^3 - 27c^2 \\ &= -4(a_1a_2 + a_1a_3 + a_2a_3)^3 - 27(-a_1a_2a_3)^2 \\ &= [(a_2-a_1)(a_3-a_1)(a_3-a_2)]^2. \end{aligned}$$

قرار می‌دهیم $d = (a_2-a_1)(a_3-a_1)(a_3-a_2)$، آنگاه هر K- خودریختی α از $F = K(a_1,a_2,a_3)$، D را ثابت نگه می‌دارد. چون $\alpha(d)$ برابر d یا $-d$ است. اکنون بنا به بحث فوق $D \in K$. فرض کنید $d \in K$، آنگاه به ازای هر $\alpha \in \mathrm{Aut}_K F$، $\alpha(d) = d$. بنابراین، هر α عضو گروه متناوب A_3 است. برعکس اگر $\alpha \in A_3$، آنگاه $\alpha(d) = d$. چون $\mathrm{Aut}_K F \neq \{\mathrm{id}_F\}$، بحث بالا نشان می‌دهد $\mathrm{Aut}_K F = A_3$ اگر و تنها اگر $d \in K$. در نتیجه $\mathrm{Aut}_K F = S_3$ اگر و تنها اگر $d \notin K$. هرگاه $d \in K$، آنگاه $\mathrm{Aut}_K F = A_3$ و در نتیجه $[F : K] = 3$.

۲. داریم $[K(r) : K] = 3$. اگر $F = K(r)$، آنگاه $F = K(\sqrt{D}, r)$. فرض کنید $K(r) \subset F$. آنگاه $[F : K] = 6$ و $[F : K(r)] = 2$، داریم $\mathrm{Aut}_K F = S_3$. پس $d \notin K$. چون d ریشه‌ای از $x^2 - D$ است (d در تمرین قبل تعریف شده)، $x^2 - D$ روی k تحویل‌ناپذیر است. چون ۲ و ۳ نسبت به هم اول‌اند، $x^2 - D$ روی $K(r)$ تحویل‌ناپذیر است. بنابراین $F = K(\sqrt{D}, r)$.

۴. از تمرین ۱ استفاده کنید $b = 0$، $c = -5$، $D = (-27)(25)$ مربع نیست.

۵. چون u ریشه‌ی اولیه‌ی پنجم واحد است $\mathbb{Q}(u) : \mathbb{Q}$ توسیع تجزیه‌ی $x^5 - 1$ است و $\mathrm{Aut}_{\mathbb{Q}}\mathbb{Q}(u) \cong \mathbb{Z}_5^\times \cong \mathbb{Z}_4$. داریم $\mathrm{Aut}_{\mathbb{Q}}\mathbb{Q}(u) = \{\alpha_1, \alpha_2, \alpha_3, \alpha_4\}$ که در آن $\alpha_j(u) = u^j$. $\mathrm{Aut}_{\mathbb{Q}}\mathbb{Q}(u)$ تنها یک زیرگروه سره $H = \{\alpha_1, \alpha_4\}$ دارد و زیرمیدان متناظر آن عبارت است از

$$\mathbb{Q}(u)_H = \{a \in \mathbb{Q}(u) \mid \alpha_4(a) = a\} = \mathbb{Q}((u^2 - u^3)^2).$$

۶. اگر $a = \sqrt[4]{2}$، آنگاه $F = \mathbb{Q}(a, i)$ میدان تجزیه برای $f(x)$ است و $[F : \mathbb{Q}] = 8$ و $\mathrm{Aut}_{\mathbb{Q}}F = \langle \alpha, \beta \rangle \cong D_8$، که در آن $\alpha(a) = ia$، $\alpha(i) = i$، $\beta(a) = a$، $\beta(i) = -i$. داریم $O(\alpha) = 4$، $O(\beta) = 2$، $\alpha\beta\alpha = \beta$. زیرگروه‌های سره‌ی $\mathrm{Aut}_{\mathbb{Q}}F$ و میدان‌های میانی متناظر آن‌ها عبارت‌اند از

$$\begin{aligned}
&H_1 = \langle \alpha \rangle = \{\mathrm{id}_F, \alpha, \alpha^2, \alpha^3\}, \quad H_2 = \langle \alpha^2, \beta \rangle = \{\mathrm{id}_F, \alpha^2, \beta, \alpha^2\beta\},\\
&H_3 = \langle \alpha^2, \alpha\beta \rangle = \{id_F, \alpha^2, \alpha\beta, \alpha^3\beta\}, \quad H_4 = \langle \alpha^2 \rangle = \{\mathrm{id}_F, \alpha^2\},\\
&H_5 = \langle \beta \rangle = \{\mathrm{id}_F, \beta\}, \quad H_6 = \langle \alpha\beta \rangle = \{\mathrm{id}_F, \alpha\beta\},\\
&H_7 = \langle \alpha^2\beta \rangle = \{\mathrm{id}_F, \alpha^2\beta\}, \quad H_8 = \langle \alpha^3\beta \rangle = \{\mathrm{id}_F, \alpha^3\beta\}\\
&F_{H_1} = \mathbb{Q}(i), \quad F_{H_2} = \mathbb{Q}(a^2), \quad F_{H_3} = \mathbb{Q}(a^{2,2}), \quad F_{H_4} = \mathbb{Q}(a^2)\\
&F_{H_5} = \mathbb{Q}(a), \quad F_{H_6} = \mathbb{Q}(^2), \quad F_{H_7} = \mathbb{Q}(a^2), \quad F_{H_8} = \mathbb{Q}(a^2)
\end{aligned}$$

۹. میدان‌های میانی سره عبارت‌اند از $\mathbb{Q}(i)$، $\mathbb{Q}(\sqrt{5})$، $\mathbb{Q}(i\sqrt{5})$.

تمرین‌های ۹.۱۴، حل‌پذیری چندجمله‌ای‌ها با رادیکال، صفحه‌ی ۳۴۰

۱. $G = A_3$.

۲. از قضیه‌ی ۱۳.۵.۱۴ استفاده کنید، $f(x)$ با رادیکال‌ها حل‌پذیر نیست.

۴. از قضیه‌ی ۱۳.۵.۱۴ استفاده کنید.

تمرین‌های ۱۰.۱۴، ساخت‌پذیری هندسی، صفحه‌ی ۳۴۷

۱. خیر

۳. اگر a، b، c ساخته شدنی باشند، آنگاه ریشه‌های معادله‌ی $ax^2 + bx + c = 0$ که به صورت $\frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$ هستند نیز ساخته شوند. اکنون به استقرا روی i نشان دهید هر عضو F_i ساخته شدنی است. اگر $i > 0$ و هر عضو F_i ساخته شدنی باشد، عضو $b \in F_{i+1}$ را در نظر می‌گیریم. اگر $b \in F_i$ بنا به فرض استقرا حکم ثابت است. اگر $b \notin F_i$ نشان دهید $F_{i+1} = F_i(b)$. پس $[F_i(b) : F_i] = 2$، یعنی b در یک چندجمله‌ای درجه‌ی ۲ با ضرایب در F_i صدق می‌کند و بنابراین ساخته شدنی است.

تمرین‌های ۱.۱۵، کدهای خطی، صفحه‌ی ۳۵۵

۶. فرض کنید C_1 و C_2 کدهایی با ماتریس‌های مولد G_1 و G_2 باشند. در این صورت

$$\begin{aligned}
C_1 &= \{a(1,1,1,0) + b(0,1,1,0) + c(0,0,1,1) \mid a, b, c \in \mathbb{Z}_2\}\\
&= \{(0,0,0,0), (1,1,1,0), (0,1,1,0), (0,0,1,1),\\
&\qquad (1,0,0,0), (1,1,0,1), (0,1,0,1), (1,0,1,1)\}\\
C_2 &= \{a(1,0,1,1) + b(0,1,1,1) + c(1,0,0,1) \mid a, b, c \in \mathbb{Z}_2\}\\
&= \{(0,0,0,0), (1,0,1,1), (0,1,1,1), (1,0,0,1),\\
&\qquad (1,1,0,0), (0,0,1,0), (1,1,1,0), (0,1,0,1)\}
\end{aligned}$$

با مقایسه‌ی $C_۱$ و $C_۲$ می‌بینیم که اگر هر یک از مولفه‌های کد واژه‌های $C_۱$ را به راست حرکت دیدیم، $C_۲$ به دست می‌آید.

۷. هر ستون G بر خودش عمود است. زیرا وزن هر سطر زوج است. حال اگر v و u دو واژه در C باشند، چون ترکیب خطی از سطرهای G هستند، $u \cdot v = ۰$. کد دوگان C یک $[۷, ۴]$- کد است که توسط C و بردار $(۱, ۱, \dots, ۱)$ تولید می‌شود.

۸. چون $C \subseteq C^{\perp}$ به ازای هر $a \in C$، داریم $u \cdot u = ۰$، یعنی $\mathrm{wt}(u)$ زوج است و بنابراین $u = (۱, \dots, ۱) = ۰$. اما چون طول واژه فرد است داریم

$$(۱, \dots, ۱) \cdot (۱, \dots, ۱) = ۱.$$

بنابراین $C^{\perp} - C$ با اضافه کردن $(۱, \dots, ۱)$ به همه‌ی واژه‌های C به دست می‌آید.

۹. **حالت اول :** اگر $p \equiv ۱ \mod ۴$، آنگاه $\alpha \in \mathbb{Z}_p$ وجود دارد که $\alpha^۲ = -۱$ و $G = [I_۴ \mid \alpha I_۴]$ یک ماتریس مولد برای کد خواسته شده است.

حالت دوم : اگر $p \equiv ۳ \mod ۴$، آنگاه $\beta, \alpha \in \mathbb{Z}_p$ وجود دارند که $\beta^۲ + \gamma^۲ = -۱$ و

$$G = \begin{bmatrix} ۱ & ۰ & ۰ & ۰ & \beta & \gamma & ۰ & ۰ \\ ۰ & ۱ & ۰ & ۰ & -\gamma & \beta & ۰ & ۰ \\ ۰ & ۰ & ۱ & ۰ & ۰ & ۰ & \beta & \gamma \\ ۰ & ۰ & ۰ & ۱ & ۰ & ۰ & -\gamma & \beta \end{bmatrix}$$

ماتریس مولد کد خواسته شده است.

حالت سوم: اگر $p = ۲$، $[۷, ۴]$- کد همینگ دوتایی را در نظر بگیرید.

تمرین‌های ۲.۱۵، کد گشایی کدهای خطی، صفحه‌ی ۳۶۵

۱. (الف) ۴ (ب) ۷ (ج) ۸ (د) ۶

۲. (الف) ۵ (ب) ۷ (ج) ۸ (د) ۸

۴. بنا به جبر خطی، به ازای هر i، می‌توان پایه‌ای برای C انتخاب کرد که مکان i ام هر $k - ۱$ بردار، ۰ باشد و در سایر مکان‌ها ۱. پس دقیقاً $q^{k-۱}$ کد واژه در iامین مولفه ۰ دارند.

۷. ماتریس امتحان توازن عبارت است از

$$H = \begin{bmatrix} ۱ & ۰ & ۰ & ۱ & ۱ & ۰ & ۱ \\ ۰ & ۱ & ۰ & ۱ & ۰ & ۱ & ۱ \\ ۰ & ۰ & ۱ & ۰ & ۱ & ۱ & ۱ \end{bmatrix}.$$

اگر $u = ۱۱۱۰۰۱۱$، آنگاه $S(u) = Hu^{\top} = (۰۱۱)^{\top}$ برابر ستون ششم H است. بنابراین (احتمالاً) در ستون ششم خطا رخ داده و کدواژه‌ی ارسال شده ۱۱۱۰۰۰۱ است.

۱۳. چون اعمال سطری مقدماتی فضای سطری G را تغییر نمی‌دهد می‌توانیم G را به صورت زیر در نظر بگیریم :

$$G = \begin{bmatrix} ۱ & ۰ & ۰ & ۱ & ۱ \\ ۰ & ۱ & ۰ & ۰ & ۱ \\ ۰ & ۰ & ۱ & ۰ & ۱ \end{bmatrix}.$$

$۸ = ۲^۳$ کد واژه عبارت‌اند از $a_i R_i$، که در آن R_i سطر iام G است و $a_i \in \mathbb{Z}_۲$:

$$۱۰۰۱۱, \quad ۰۱۰۰۱, \quad ۰۰۱۰۱, \quad ۱۱۰۱۰,$$
$$۱۰۱۱۰, \quad ۰۱۱۰۰, \quad ۰۰۰۰۰, \quad ۱۱۱۱۱$$

با نوشتن $G = [I_۳ \mid -A^\top]$ داریم

$$H = [A \mid I_۲] = \begin{bmatrix} ۱ & ۰ & ۰ & ۱ & ۰ \\ ۱ & ۱ & ۱ & ۰ & ۱ \end{bmatrix}.$$

فاصله‌ی می‌نیمم برابر با

$$d_{\min} = \min_{۰ \neq c \in C} \mathrm{wt}(c) = ۲$$

و رتبه‌ی G برابر ۳ است.
اکنون داریم ماتریس مولد کد $C^\perp$ عبارت است از

$$H = \begin{bmatrix} ۱ & ۰ & ۰ & ۱ & ۰ \\ ۱ & ۱ & ۱ & ۰ & ۱ \end{bmatrix}$$

که یک $[۵, ۲]$- کد دوتایی است. $۲^۴$ کد واژه در این کد هستند. هم‌چنین $۸ = ۲^۵/۲^۴$ هم‌مجموعه وجود دارند:

سندرُم $= Gu^\top$	هم‌مجموعه			پیشروی هم‌مجموعه
$[۰۰۰]^\top$	۰۱۱۱۱	۱۱۱۰۱	۱۰۰۱۰	۰۰۰۰۰
$[۰۰۱]^\top$	۱۱۱۱۱	۰۱۱۰۱	۰۰۰۱۰	۱۰۰۰۰
$[۱۰۰]^\top$	۰۰۱۱۱	۱۰۱۰۱	۱۱۰۱۰	۰۱۰۰۰
$[۰۱۰]^\top$	۰۱۰۱۱	۱۱۰۰۱	۱۰۱۱۰	۰۰۱۰۰
$[۱۱۱]^\top$	۰۱۱۱۰	۱۱۱۰۰	۱۰۰۱۱	۰۰۰۰۱
$[۱۰۱]^\top$	۱۰۱۱۱	۰۰۱۰۱	۰۱۰۱۰	۱۱۰۰۰
$[۱۱۰]^\top$	۰۰۰۱۱	۱۰۰۰۱	۱۱۱۱۰	۰۱۱۰۰
$[۰۱۱]^\top$	۰۱۰۰۱	۱۱۰۱۱	۱۰۰۱۰	۰۰۱۱۰

اگر $u = ۰۱۰۰۱$، آن‌گاه

$$S(u) = Gu^\top = \begin{bmatrix} ۱ \\ ۰ \\ ۱ \end{bmatrix} = S(۱۱۰۰۰).$$

پس خطا عبارت است از ۱۱۰۰۰، و u را به صورت

$$v = u - e = ۰۱۰۰۱ - ۱۱۰۰۰ = ۱۰۰۰۱$$

کد گشایی می‌کنیم.

۱۴. می‌دانیم که اگر C یک $[n, k]$- کد خطی کامل t- تصحیح کننده‌ی خطا باشد، آن‌گاه $|C| \sum_{i=۰}^{t} \binom{n}{i}(q-۱)^i = q^n$. پس به ازای یک ℓ داریم ، $\sum_{i=۰}^{۳} \binom{n}{i} = ۲^\ell$. از این معادله نتیجه می‌شود، $(n+۱)(n^۲ - n + ۶) = ۳ \times ۲^\ell + ۱$، یعنی

$$(n+۱)[(n+۱)^۲ - ۳(n+۱) + ۸] = ۳ \times ۲^\ell + ۱$$

اگر $۱۶ | n+۱$، آن‌گاه ۸ عامل دوم در سمت چپ را می‌شمارد ولی ۱۶ آن را نمی‌شمارد. یعنی برابر ۸ یا ۲۴ است، که تناقض است. پس $۲۴ | n+۱$. چون $n \geq ۷$، پس n برابر ۷، ۱۱، یا ۲۳ است. اما $n = ۱۱$ در معادله صدق نمی‌کند. برای $n = ۷$ کد، $C = \{(۰, \ldots, ۰), (۱, \ldots, ۱)\}$ کامل است و برای $n = ۲۳$ کدهای گولای کامل هستند (بخش ۴ را ببینید).

۱۵. از ماتریس مولد به ازای هر $u \in C$ با $u = a_۰a_۱ \cdots a_۷$ به دست می‌آوریم:

$$a_۱ + a_۲ + a_۵ = a_۳ + a_۴ + a_۶ = a_۱ + a_۲ + a_۳ + a_۴ + a_۷ = ۰.$$

پس سندرُم‌ها عبارت‌اند از

$$(s_۱, s_۲, s_۳) = (e_۱ + e_۲ + e_۵, e_۳ + e_۴ + e_۶, e_۱ + e_۲ + e_۳ + e_۴ + e_۷)$$

و سه کد واژه‌ی دریافت شده به ترتیب عبارت‌اند از ۰۰۰، ۰۰۱، ۱۰۱. بنابراین، بنا به روش کدگشایی نزدیک‌ترین همسایه، اولین واژه، کد واژه است، دومین واژه در مکان هفتم و سومین واژه در مکان اول و سوم خطا دارند.

۱۷. $A_۰ = A_۸ = ۱$، $A_۴ = ۱۴$، و $A_i = ۰$، برای i های دیگر.

۱۸. (ب) توجه کنید $A_۰ = A_۷ = ۱$، $A_۳ = A_۴ = ۷$، و $A_i = ۰$ برای i های دیگر.

۱۹. ماتریس امتحان توازن $[۷, ۴]$- کد همینگ عبارت است از

$$H = \begin{bmatrix} ۰ & ۱ & ۱ & ۱ & ۱ & ۰ & ۰ \\ ۱ & ۰ & ۱ & ۱ & ۰ & ۱ & ۰ \\ ۱ & ۱ & ۰ & ۱ & ۰ & ۰ & ۱ \end{bmatrix}.$$

پس $G = [I, -A^\top]$. ماتریس مولد و امتحان $[۸, ۴]$- کد همینگ تعمیم یافته عبارت‌اند از

$$\overline{G} = \begin{bmatrix} & ۱ \\ G & ۱ \\ & ۱ \\ & ۰ \end{bmatrix}, \quad \overline{H} = \begin{bmatrix} ۱ & ۱ & \cdots & ۱ \\ & & & ۰ \\ & H & & \vdots \\ & & & ۰ \end{bmatrix}.$$

برای کد گذاری داریم

$$۰۱۱۰G = ۰۱۱۰۰۱۱, \quad ۱۰۱۱G = ۱۰۱۱۰۱۰,$$
$$۰۱۱۰\overline{G} = ۰۱۱۰۰۱۱۰, \quad ۱۰۱۱\overline{G} = ۱۰۱۱۰۱۰۰.$$

برای کد گشایی فرض کنید $u = ۱۱۰۰۱۱۰۱$، داریم $S(u) = (۱۰۰۰)^\top$، پس در مولفه‌ی آخر u خطا رخ داده. کد واژه و پیام به ترتیب ۱۱۰۰۱۱۰۰ و ۱۱۰۰ بوده‌اند.

۲۰. فرض کنید $(\overline{A}_۰, \overline{A}_۱, \ldots, \overline{A}_n, \overline{A}_{n+۱})$ توزیع وزن $\overline{C}$ باشد، در این صورت $\overline{A}_{۲k-۱} = ۰$ و $\overline{A}_{۲k} = A_{۲k-۱} + A_{۲k}$. اکنون چون

$$\sum A_{۲k-۱} z^{۲k-۱} = \frac{۱}{۲}[A(z) - A(-z)] \quad \text{و} \quad \sum A_{۲k} z^{۲k} = \frac{۱}{۲}[A(z) + A(-z)]$$

داریم

$$\overline{A}(z) = \frac{۱}{۲}[(۱ + z)A(z) + (۱ - z)A(-z)].$$

۲۱. بنا به تمرین قبل و رابطه‌ی

$$A(z) = \frac{۱}{n+۱}(۱ + z)^n + \frac{n}{n+۱}(۱ + z)^{\frac{n-۲}{۲}}(۱ - z)^{\frac{n+۱}{۲}}$$

شمارش‌گر وزن کد همینگ تعمیم یافته به طول $n + ۱ = ۲^k$ را می‌یابیم:

$$\frac{۱}{۲}\left[\frac{(۱ + z)^{n+۱} + (۱ - z)^{n+۱}}{n+۱}\right] + \frac{n}{n+۱}(۱ - z^۲)^{\frac{n+۱}{۲}}.$$

اکنون اگر از قضیه‌ی شمارش‌گر وزن کد دوگان استفاده کنیم، شمارش‌گر کد دوگان را به دست می‌آوریم: $۱ + ۲nz^{\frac{n+۱}{۲}} + z^{n+۱}$؛ یعنی وزن همه‌ی واژه‌ها این کد به جز $(۰, \ldots, ۰)$ و $(۱, \ldots, ۱)$ برابر $۲^{k-۱}$ است.

۲۲. فرض کنید u یک پیشروی هم‌مجموعه با وزن بزرگ‌تر از r باشد. در این صورت به ازای هر $v \in C$، داریم $d(u,v) = \mathrm{wt}(u-v) > r$. پس $u \in S_r(v)$. بر عکس فرض کنید k وزن پیشروی هم‌مجموعه با وزن ماکسیمم باشد. نشان می‌دهیم کره‌های $S_k(c)$، $c \in C$ نیز Fyda را می‌پوشانند. فرض کنید بر خلاف حکم که v در یک هم‌مجموعه با پیشروی u باشد و $d(u,v) > k$. پس به ازای یک $c \in C$ داریم $v = u + c$. اما

$$d(v,c) = d(u+c,c) = \mathrm{wt}(u) < k,$$

که تناقض است.

۲۳. زیرکد (زیرفضای یک کد را زیرکد می‌نامیم) حاصل‌ضرب از ستون‌های ۱، ۹ و ۱۰ کد تکرار، که یک کد کامل و ۲- تصحیح کننده‌ی خطا است. زیرکد حاصل‌ضرب از هفت مکان باقی‌مانده $[۴, ۷]$- کد همینگ، که یک کد کامل و ۱- تصحیح کننده‌ی خطا است. پس به طریق یکتا می‌توانیم یک خطا را روی هر کدام از زیرکدها تصحیح کنیم. فاصله‌ی می‌نیمم C برابر ۳ و شعاع پوششی (تمرین قبل را ببینید) ۲ است.

۲۴. داریم

$$H = \begin{bmatrix} ۰ & ۰ & ۰ & ۰ & ۱ & ۱ & ۱ & ۱ & ۱ & ۱ & ۱ & ۱ & ۱ \\ ۰ & ۱ & ۱ & ۱ & ۰ & ۰ & ۰ & ۱ & ۱ & ۱ & ۲ & ۲ & ۲ \\ ۱ & ۰ & ۱ & ۲ & ۰ & ۱ & ۲ & ۰ & ۱ & ۲ & ۰ & ۱ & ۲ \end{bmatrix}.$$

با تعویض کردن ستون‌های $(۱, ۳)$، $(۲, ۱۲)$، $(۵, ۱۱)$ به دست می‌آید:

$$H^* = \begin{bmatrix} ۱ & ۱ & ۰ & ۰ & ۱ & ۱ & ۱ & ۱ & ۱ & ۱ & ۱ & ۰ & ۰ \\ ۲ & ۲ & ۱ & ۱ & ۲ & ۰ & ۰ & ۱ & ۱ & ۱ & ۰ & ۱ & ۰ \\ ۲ & ۱ & ۱ & ۲ & ۰ & ۱ & ۲ & ۰ & ۱ & ۲ & ۰ & ۰ & ۱ \end{bmatrix}.$$

بنابراین

$$G^* = \begin{bmatrix} & ۲ & ۱ & ۱ \\ & ۲ & ۱ & ۲ \\ I_q & ۰ & ۲ & ۲ \\ & ۰ & ۲ & ۱ \\ & ۲ & ۱ & ۰ \\ & ۲ & ۰ & ۲ \\ & ۲ & ۰ & ۱ \\ & ۲ & ۲ & ۰ \\ & ۲ & ۲ & ۲ \\ & ۲ & ۲ & ۱ \end{bmatrix}$$

با عکس کردن تعویض ستون‌ها، یعنی $(۱, ۱۳)$، $(۲, ۱۲)$، $(۱۱, ۵)$ به دست می‌آوریم

$$G = \begin{bmatrix} ۱ & ۱ & ۰ & ۰ & ۲ & ۰ & ۰ & ۰ & ۰ & ۰ & ۰ & ۰ & ۱ \\ ۲ & ۱ & ۰ & ۰ & ۲ & ۰ & ۰ & ۰ & ۰ & ۰ & ۰ & ۱ & ۰ \\ ۲ & ۲ & ۱ & ۰ & ۰ & ۰ & ۰ & ۰ & ۰ & ۰ & ۰ & ۰ & ۰ \\ ۱ & ۲ & ۰ & ۱ & ۰ & ۰ & ۰ & ۰ & ۰ & ۰ & ۰ & ۰ & ۰ \\ ۰ & ۱ & ۰ & ۰ & ۲ & ۰ & ۰ & ۰ & ۰ & ۰ & ۱ & ۰ & ۰ \\ ۲ & ۰ & ۰ & ۰ & ۲ & ۱ & ۰ & ۰ & ۰ & ۰ & ۰ & ۰ & ۰ \\ ۱ & ۰ & ۰ & ۰ & ۲ & ۰ & ۱ & ۰ & ۰ & ۰ & ۰ & ۰ & ۰ \\ ۰ & ۲ & ۰ & ۰ & ۲ & ۰ & ۰ & ۱ & ۰ & ۰ & ۰ & ۰ & ۰ \\ ۲ & ۲ & ۰ & ۰ & ۲ & ۰ & ۰ & ۰ & ۱ & ۰ & ۰ & ۰ & ۰ \\ ۱ & ۲ & ۰ & ۰ & ۲ & ۰ & ۰ & ۰ & ۰ & ۱ & ۰ & ۰ & ۰ \end{bmatrix}$$

اکنون چون $S(۰۱۱۰۱۰۰۰۰۰۰۱۱)(۰۰۱)^\top =$، برابر اولین ستون H است، داریم $u = ۲۱۱۰۱۰۰۰۰۰۱۱$ که به ۱۱۱۰۰۰۰۰۰۰ کد گشایی می‌شود.

تمرین‌های ۴.۱۵، کدهای دوری، صفحه‌ی ۳۸۸

۳. داریم $H = \begin{bmatrix} ۱ & ۱ & ۱ & ۰ \\ ۱ & ۲ & ۰ & ۱ \end{bmatrix}$. اکنون $۱۱۱۰ \in C$، اما شیفت دوری آن یعنی ۰۱۱۱ در C نیست، زیرا

$$H[۰۱۱۱]^\top = [۲۰]^\top \neq [۰۰] \mod ۲.$$

پس C دوری نیست.

۹. داریم

$$G = \begin{bmatrix} ۱ & ۱ & ۰ & ۱ & ۰ & ۰ & ۰ \\ ۰ & ۱ & ۱ & ۰ & ۱ & ۰ & ۰ \\ ۰ & ۰ & ۱ & ۱ & ۰ & ۱ & ۰ \\ ۰ & ۰ & ۰ & ۱ & ۱ & ۰ & ۱ \end{bmatrix}.$$

کد واژه‌ها عبارت‌اند از uG، به ازای هر $u \in \mathbb{Z}_۲^۴$، یعنی

۱۱۰۱۰۰۰، ۰۱۱۰۱۰۰، ۰۰۱۱۰۱۰، ۰۰۱۱۰۱، ۱۰۱۱۱۰۰،
۰۱۰۱۱۱۰، ۰۰۱۰۱۱۱، ۰۰۰۰۰۰۰، ۱۱۱۰۰۱۰، ۰۱۱۱۰۰۱،
۱۱۰۰۱۰۱، ۰۱۰۰۰۱۱، ۱۰۰۰۱۱۰، ۱۱۱۱۱۱۱، ۱۰۱۱۰۰۱، ۱۰۰۱۰۱۱

نمایش چندجمله‌ای ۱۰۰۰۱۱۱، یعنی $f(t) = ۱ + t^۴ + t^۵ + t^۶$ را در نظر می‌گیریم، داریم

$$f(t) = g(t)(t^۳ + t^۲) + t^۲ + ۱.$$

چون $g(t) \nmid f(t)$، ۱۰۰۰۱۱۱ یک کد واژه نیست و بنابراین خطا رخ داده ، برای ۰۱۱۰۰۱۱، چندجمله‌ای $f(t) = t + t^۲ + t^۵ + t^۶$، را در نظر می‌گیریم، داریم

$$f(t) = g(t)(t^۳ + t^۲ + t) + t^۲$$

چون $g(t) | f(t)$، خطا رخ داده است. آخرین واژه، یعنی ۰۱۰۰۰۱۱، کد واژه است زیرا $g(t) | (t + t^۵ + t^۶)$.

۱۱. داریم $g(x) = ۱ + x + x^۲$، $h(x) = \dfrac{x^۳ + ۱}{g(x)} = x + ۱$ و $H = \begin{bmatrix} ۰ & ۱ & ۱ \\ ۱ & ۱ & ۰ \end{bmatrix}$. پس

سندرُم	۰۰	۰۱	۱۰	۱۱
پیشروی هم‌مجموعه	۰۰۰	۱۰۰	۰۰۱	۰۱۰

۱۲. داریم $g(x) = ۱ + x^۲ + x^۳ + x^۴$ و $h(x) = \dfrac{۱ + x^۷}{g(x)} = ۱ + x^۲ + x^۳$. پس $[۷, ۳]$- کد دوتایی با مولد $g(x)$ و توازن H را دارد

$$H = \begin{bmatrix} ۰ & ۰ & ۰ & ۱ & ۱ & ۰ & ۱ \\ ۰ & ۰ & ۱ & ۱ & ۰ & ۱ & ۰ \\ ۰ & ۱ & ۱ & ۰ & ۱ & ۰ & ۰ \\ ۱ & ۱ & ۰ & ۱ & ۰ & ۰ & ۰ \end{bmatrix}$$

سندرُم	۰۰۰۰	۰۰۰۱	۰۰۱۰	۰۱۰۰
پیشرو	۰۰۰۰۰۰۰	۱۰۰۰۰۰۰	۱۱۰۰۰۰۰	۰۰۰۰۰۱۰
سندرُم	۱۰۰۰	۰۰۱۱	۰۱۱۰	۱۱۰۰
پیشرو	۰۰۰۰۰۰۱	۱۰۰۰۰۰۰	۰۰۱۰۰۰۰	۰۰۰۰۰۱۱
سندرُم	۰۱۰۱	۱۰۰۱	۱۰۱۰	۰۱۱۱
پیشرو	۱۰۰۰۰۱۰	۱۰۰۰۰۱۰	۰۰۰۰۰۱۰	۱۰۱۰۰۰۰
سندرُم	۱۱۱۰	۱۰۱۱	۱۱۰۱	۱۱۱۱
پیشرو	۰۰۰۰۱۱۰	۰۱۰۰۰۰۱	۰۰۰۱۰۰۰	۰۱۰۰۰۱۱

۱۴. داریم $g(x) = (۱ + x)(۱ + x^۲ + x^۳)$. چندجمله‌ای $۱ + x^۲ + x^۳$ اولیه است، پس اگر ξ یک ریشه‌ی هفتم اولیه‌ی واحد باشد که $۱ + \xi^۲ + \xi^۳ = ۰$، آن‌گاه

$$f(t) \in C \iff f(۱) = f(\xi) = ۰.$$

اگر $f(t) = a_i t^i$، آن‌گاه $f(۱) = \sum_{i=۱}^{n} a_i = ۰$ و $f(\xi) = \sum_{i=۱}^{n} a_i \xi^i = ۰$. در نتیجه ماتریس امتحان توازن عبارت است از

$$H = \begin{bmatrix} \xi^۶ & \xi^۵ & \xi^۴ & \xi^۳ & \xi^۲ & \xi & ۱ \\ ۱ & ۱ & ۱ & ۱ & ۱ & ۱ & ۱ \end{bmatrix}$$

که، با نمایش دادن ξ^i در بسط دوتایی، همان ماتریس امتحان توازن کد همینگ تعمیم یافته است. به سادگی می‌توان دید فاصله‌ی می‌نیمم برای کد دوری تولید شده توسط $۱ + t^۲ + t^۳$ برابر ۳ است. چون C با انتخاب کد واژه‌های C به دست می‌آید داریم $d_{\min} = ۴$.

تمرین‌های ۵.۱۵ و ۶.۱۵، کدهای BCH و QR، صفحه‌ی ۴۰۲

۱. کد BCH که در زیر می‌سازیم به طول ۸۰ روی $\mathbb{Z}_۳$ با فاصله‌ی طرح $\delta = ۱۱$، تصحیح کننده‌ی حداقل ۵ خطاست. به برخی از هم مجموعه‌های دایره‌بر (به پیمانه‌ی ۸۰) نیاز داریم:

$$C_۱ = \{۱, ۳, ۹, ۲۷\}, \quad C_۲ = \{۲, ۶, ۱۸, ۵۴\}, \quad C_۴ = \{۴, ۱۲, ۳۶, ۲۸\}$$
$$C_۵ = \{۵, ۱۵, ۴۵, ۵۵\}, \quad C_۷ = \{۷, ۲۱, ۶۳, ۲۹\}, \quad C_{۱۰} = \{۱۰, ۳۰\}$$

فرض کنید $g(x)$، کوچک‌ترین مضرب مشترک $f_i(x)$، $i = ۱, ۲, ۴, ۵, ۷, ۱۰$، باشد که در آن $f_i(x)$ چندجمله‌ای می‌نیمال a^i است و a، ریشه‌ی ۸۰ام اولیه‌ی واحد است. درجه‌ی $g(x)$ برابر ۲۲ است و $\dim C = ۸۰ - ۲۲ = ۵۸$.

۳. $S(v) = (۱۱۱۰۰۱۱۱۰۱)^\top \neq ۰$، پس حداقل یک خطا رخ داده است. فرض کنید $S_۱ = (۱۱۱۰۰)^\top$ و $S_۳ = (۱۱۱۰۱)^\top$ و

$$\begin{aligned}\sigma(z) &= ۱ + S_۱ z + \left(\frac{S_۳}{S_۱} + S_۱^۲\right) z^۲ \\ &= ۱ + a^{۱۱} z + a^۶ z^۲.\end{aligned}$$

با سعی و خطا ریشه‌های σ را می‌یابیم: $a^{۳۰}$ و $a^{۲۶}$. بنابراین $a^{-۳۰} = a$ و $a^{-۲۶} = a^۵$ و نتیجه می‌گیریم که خطا در دومین و ششمین مکان رخ داده است.

۴. برای تصحیح سه خطا باید فاصله‌ی طرح $\delta = ۷$ را در نظر بگیریم. چندجمله‌ای مولد مناسب $g(x)$ عبارت است از کوچک‌ترین مضرب مشترک $f_i(x)$، $i = ۰, ۱, ۳, ۵, ۷$. هم مجموعه‌های دایره‌بر (به پیمانه‌ی ۱۵) را داریم:

$$\begin{aligned}&C_۰ = \{۰\},\ \ C_۱ = \{۱, ۲, ۴, ۸\},\ \ C_۳ = \{۳, ۶, ۱۲, ۹\},\\ &C_۵ = \{۵, ۱۰\},\ \ C_۷ = \{۷, ۱۴, ۱۳, ۱۱\}.\end{aligned}$$

بنابراین $f_۱(x) = f_۲(x) = f_۴(x)$ و $f_۳(x) = f_۶(x)$ و

$$\begin{aligned}g(x) &= f_۱(x) f_۲(x) f_۳(x) \\ &= (x^۴ + x^۳ + ۱)(x^۴ + x^۳ + x^۲ + x + ۱)(x^۲ + x + ۱) \\ &= ۱ + x^۲ + x^۵ + x^۶ + x^۷ + x^۹ + x^{۱۰}.\end{aligned}$$

۵. کد BCH دوتایی به طول ۳۱ را در زیر می‌سازیم. فرض کنید a ریشه‌ی ۳۱ام اولیه‌ی واحد (و $a^۵ + a^۲ + ۱ = ۰$) و $g(x)$ کوچک‌ترین مضرب مشترک $i = ۱, \ldots, ۸$ باشد، که در آن $f_i(x)$ چندجمله‌ای می‌نیمال a^i است. اما

$$\begin{aligned}&C_۱ = \{۱, ۲, ۴, ۸, ۱۶\},\ \ C_۳ = \{۳, ۶, ۱۲, ۲۴, ۲۷\},\\ &C_۵ = \{۵, ۱۰, ۲۰, ۹, ۱۸\},\ \ C_۷ = \{۷, ۱۴, ۲۸, ۲۵, ۱۹\}.\end{aligned}$$

بنابراین $f_۱(x) = f_۲(x) = f_۴(x) = f_۸(x)$ و $f_۳(x) = f_۶(x)$ و

$$\begin{aligned}g(x) &= f_۱(x) f_۳(x) f_۵(x) f_۸(x) \\ &= (x^۵ + x^۲ + ۱)(x^۵ + x^۴ + x^۳ + x^۲ + ۱) \times \\ &\qquad (۱ + x + x^۲ + x^۴ + x^۵)(۱ + x + x^۲ + x^۳ + x^۵).\end{aligned}$$

$g(x)$ یک مولد کد دوتایی BCH به طول ۳۱ با فاصله‌ی طرح ۹ است. (به سادگی می‌توان دید $d_{\min} \geq ۱$).

۶. می‌دانیم که اگر ξ یک ریشه‌ی ۱۵ام اولیه‌ی واحد باشد که در $\xi^۴ + \xi + ۱ = ۰$ صدق کند، آن‌گاه

$$\begin{aligned}x^{۱۵} - ۱ &= f_۰(x) f_۱(x) f_۳(x) f_۵(x) f_۷(x) \\ &= (x + ۱)(x^۴ + x + ۱)(x^۴ + x^۳ + x^۲ + x + ۱) \times \\ &\qquad (x^۲ + x + ۱)(x^۴ + x^۳ + ۱).\end{aligned}$$

اگر قرار دهیم $g(x) = ۱$ به یک $[n, n, ۱]$- کد به دست می‌آوریم. اگر قرار دهیم $g(x) = f_۱(x)$، آن‌گاه ξ، $\xi^۲$، $\xi^۴$، $\xi^۸$ ریشه‌های $g(x)$ هستند. پس فاصله‌ی طرح کد حاصل‌ضرب برابر $\delta = ۳$ است و داریم $k = n - \deg g(x) = ۱۱$. $۱ + t + t^۴$ یک کد واژه با وزن ۳ است، پس $d_{\min} = \delta = ۳$. اگر قرار دهیم $g(x) = f_۱(x) f_۳(x)$، آن‌گاه ξ، $\xi^۲$، $\xi^۳$، $\xi^۴$، $\xi^۶$، $\xi^۸$، $\xi^۹$، $\xi^{۱۲}$ ریشه‌های $g(x)$ هستند. پس فاصله‌ی طرح کد حاصل‌ضرب برابر $\delta = ۵$ است و داریم $k = n - \deg g(x) = ۷$. $۱ + t^۴ + t^۶ + t^۷ + t^۸$ یک کد واژه با وزن ۵ است، پس $d_{\min} = \delta = ۵$. اگر $g(x) = f_۱(x) f_۳(x) f_۵(x)$، آن‌گاه ξ، $\xi^۲$،

$\xi^{۳}$، $\xi^{۴}$، $\xi^{۵}$، $\xi^{۶}$، $\xi^{۸}$، $\xi^{۹}$، $\xi^{۱۰}$، $\xi^{۱۲}$ ریشه‌های $g(x)$ هستند. پس فاصله‌ی طرح کد حاصل‌ضرب برابر $\delta = ۷$ است و داریم $k = n - \deg g(x) = ۵$. $d_{\min} = \delta = ۷$. در نهایت اگر $g(x) = f_۱(x)f_۳(x)f_۵(x)f_۷(x)$، آنگاه ξ، $\xi^{۲}$، ...، $\xi^{۱۴}$ ریشه‌های $g(x)$ هستند. پس $\delta = ۱۵$ است و $k = ۱$ و به وضوح $d_{\min} = ۱۵$. پس $g(x)$ یک $[۱۵, ۱, ۱۵]$- کد تولید می‌کند.

۷. داریم $g(x) = (۱ + x + x^{۲})(۱ + x + x^{۳} + x^{۴})(۱ + x + x^{۴})$. فرض کنید

$$H = \begin{bmatrix} ۱ & a^{۱} & a^{۳} & \cdots & a^{۱۴} \\ ۱ & a^{۳} & a^{۹} & \cdots & a^{۴۲} \\ ۱ & a^{۵} & a^{۱۵} & \cdots & a^{۷۰} \end{bmatrix}.$$

داریم

$$S(v) = Hv^{\top} = \begin{bmatrix} ۱ + a + a^{۵} + a^{۸} + a^{۹} + a^{۱۱} \\ ۱ + a^{۳} + a^{۱۵} + a^{۲۴} + a^{۲۷} + a^{۳۳} \\ ۱ + a^{۵} + a^{۲۵} + a^{۴۰} + a^{۴۵} + a^{۵۵} \end{bmatrix} = \begin{bmatrix} S_۱ \\ S_۲ \\ S_۳ \end{bmatrix}$$

چون $a^{۱۵} = ۱$، می‌توان دید

$$S(v) = \begin{bmatrix} S_۱ \\ S_۲ \\ S_۳ \end{bmatrix} = \begin{bmatrix} a^{۲} \\ ۱ + a^{۲} \\ ۱ \end{bmatrix} \neq ۰,$$

پس حداقل یک خطا رخ داده است. فرض کنید دو یا سه خطا رخ داده است و تابع $\sigma(z) = \sum_{i=۰}^{۳} \sigma_z^i$ با $\sigma_۰ = ۱$ و

$$\begin{bmatrix} ۱ & ۰ & ۰ \\ S_۱ & S_۲ & ۱ \\ S_۴ & S_۳ & S_۲ \end{bmatrix} \begin{bmatrix} \sigma_۱ \\ \sigma_۲ \\ \sigma_۳ \end{bmatrix} = \begin{bmatrix} S_۱ \\ S_۳ \\ S_۵ \end{bmatrix}$$

که دارای جواب $\sigma_۱ = S_۱ = a^{۲}$، $\sigma_۲ = a^{۱۲}$ و $\sigma_۳ = ۰$ است. با سعی و خطا ریشه‌های σ به دست می‌آید: a، $a^{۲}$. بنابراین $a^{۱۴} = a^{-۱}$ و $a^{۱۳} = a^{-۲}$ و خطا در مکان ۱۴ و مکان ۱۵ رخ داده است. پس کد واژه‌ی فرستاده شده، ۱۱۰۰۰۱۰۰۱۱۰۱۰۱۱ بوده است. کدگشایی با استفاده از الگوریتم تقسیم انجام می‌شود:

$$\frac{۱ + x + x^{۵} + x^{۸} + x^{۹} + x^{۱۱} + x^{۱۳} + x^{۱۴}}{۱ + x + x^{۲} + x^{۴} + x^{۵} + x^{۸} + x^{۱۰}} = ۱ + x^{۲} + x^{۳} + x^{۴}.$$

پس پیام فرستاده شده عبارت است از ۱۱۱۰۱.

۸. با استفاده از $a^{۲} + a + ۲ = ۰$ در $\mathrm{GF}(۳^{۲})$ داریم

$$a^{۲} = ۲a + ۱,\ \ a^{۳} = ۲a + ۲,\ \ a^{۴} = ۲,\ \ a^{۵} = ۲a,\ \ a^{۶} = ۲ + a,\ \ a^{۷} = ۱ + a.$$

هم مجموعه‌های دایره‌بر به پیمانه‌ی ۸ عبارت‌اند از $C_۰ = \{۰\}$، $C_۱ = \{۱, ۳\}$، $C_۲ = \{۲, ۶\}$، $C_۴ = \{۴\}$، $C_۵ = \{۵, ۷\}$. برای ساختن یک کد ۲- تصحیح کننده‌ی خطا قرار می‌دهیم $\sigma = ۵$، $g(x) = f_۱(x)f_۲(x)f_۴(x)$، که در آن

$$f_۱(x) = ۲ + x + x^{۲},\ \ f_۲(x) = (x - a^{۲})(x - x^{۶}) = ۱ + x^{۲}$$
$$f_۴(x) = x - a^{۴} = x - ۲,$$

پس $g(x) = x^{۵} - x^{۴} + x^{۳} + x^{۲} - ۱$. توجه کنید $g(t)$۱ یک کد واژه به طول ۵ است. بنابراین $d_{\min} = \delta = ۵$ و $k = ۸ - ۵ = ۳$. داریم

$$H = \begin{bmatrix} ۱ & a & a^{۲} & a^{۳} & a^{۴} & a^{۵} & a^{۶} & a^{۷} \\ ۱ & a^{۲} & a^{۴} & a^{۶} & a^{۸} & a^{۱۰} & a^{۱۲} & a^{۱۴} \\ ۱ & a^{۴} & a^{۸} & a^{۱۲} & a^{۱۶} & a^{۲۰} & a^{۲۴} & a^{۲۸} \end{bmatrix}$$

و

$$S(v) = Hv^\top = \begin{bmatrix} a^۷ + a^۴ - a - ۱ \\ a^{۱۴} + a^۸ - a^۲ - ۱ \\ a^{۲۸} + a^{۱۶} - a^۴ - ۱ \end{bmatrix} = \begin{bmatrix} -۱ \\ ۱ - a \\ ۰ \end{bmatrix} = \begin{bmatrix} S_۱ \\ S_۲ \\ S_۳ \end{bmatrix}.$$

فرض کنید دو خطا رخ داده ، می‌نویسیم: $\sigma(z) = \sum_{k=۰}^{۲} \sigma_k z^k = ۱ + \sigma_۱ z + \sigma_۲ z^۲$، که در آن $\sigma_۰ = ۱$. داریم

$$\begin{bmatrix} S_۳ & S_۲ & S_۱ \\ S_۴ & S_۳ & S_۲ \end{bmatrix} \begin{bmatrix} ۱ \\ \sigma_۱ \\ \sigma_۲ \end{bmatrix} = \begin{bmatrix} ۰ \\ ۰ \\ ۰ \end{bmatrix}$$

و $s_۳ = s_۱^۳ = -۱$. پس

$$\begin{bmatrix} -۱ & ۱ - a & -۱ \\ ۰ & -۱ & ۱ - a \end{bmatrix} \begin{bmatrix} ۱ \\ \sigma_۱ \\ \sigma_۲ \end{bmatrix} = \begin{bmatrix} ۰ \\ ۰ \\ ۰ \end{bmatrix}$$

و با حل دستگاه اخیر داریم $\sigma_۱ = ۱ - a$ و $\sigma_۲ = ۱$. بنابراین $\sigma = ۱ + (۱ - a)z + z^۲$. با سعی و خطا ریشه‌های σ را می‌یابیم: $a^۳$ و $a^۵$. بنابراین $a^{-۳} = a^۵$ و $a^{-۵} = a^۳$ و خطا در چهارمین و ششمین مکان رخ داده است. برای تعیین خطا محاسبه می‌کنیم:

$$-۱ = S_۱ = e_۳ a^۳ + e_۵ a^۵, \quad -۱ = S_۳ = e_۳ a^۹ + e_۵ a^{۱۵}$$
$$۱ - a = S_۲ = e_۳ a^۶ + e_s a^{۱۰}, \quad ۰ = S_۴ = e_۳ a^{۱۲} + e_۵ a^{۲۰}.$$

پس $e_۳ = ۱$ و $e_۵ = -۱$ و واژه‌ی ارسال شده $v - e = ۱۰۱۱۰ - ۱۰ - ۱ - ۱$، یعنی $t^۷ + t^۶ + t^۴ - t^۳ - t - ۱$ است. با تقسیم بر $g(t)$، به دست می‌آید که این چندجمله‌ای برابر $g(t)(t^۲ + t + ۱)$ است. پس پیام ارسال شده ۱۱۱ است.

۹. می‌دانیم $d_{\min} \geq d$. فرض کنید ξ یک ریشه‌ی nام اولیه‌ی واحد باشد، در این صورت برای هر $i < a$ داریم $\xi^{id} \neq ۱$. داریم

$$x^n - ۱ = x^{ad} - ۱ = (x^a - ۱)(۱ + x^a + x^{۲a} + \cdots + x^{(d-۱)a}).$$

چون ξ، $\xi^۲$، $\xi^۳$، ...، $\xi^{d-۱}$ ریشه‌های $x^a - ۱$ هستند، ریشه‌هایی از چندجمله‌ای $f(x) = ۱ + x^a + x^{۲a} + \cdots + x^{(d-۱)a}$ نیز هستند. از این‌رو $f(t)$ یک کد واژه به وزن d است.

۱۰. فرض کنید مقدار دترمینان واندرموند برابر D_n باشد. اگر در دترمینان واندرموند، به ازای هر $۱ \leq i \leq n - ۱$، $-\alpha_i$ برابر سطر iام را با سطر $i + ۱$ام جمع کنیم و حاصل‌ضرب را در سطر iام قرار دهیم، مقدار دترمینان تغییر نمی‌کند:

$$D_n = \begin{vmatrix} ۱ & ۱ & \cdots & ۱ \\ \alpha_۱ & \alpha_۲ & \cdots & \alpha_n \\ \alpha_۱^۲ & \alpha_۲^۲ & \cdots & \alpha_n^۲ \\ \alpha_۱^۳ & \alpha_۲^۳ & \cdots & \alpha_n^۳ \\ \vdots & \vdots & \vdots & \vdots \\ \alpha_۱^{n-۱} & \alpha_۲^{n-۱} & \cdots & \alpha_n^۲ \end{vmatrix}$$

$$= \begin{vmatrix} ۱ & ۱ & \cdots & ۱ \\ ۰ & \alpha_۲ - \alpha_۱ & \cdots & \alpha_n - \alpha_۱ \\ ۰ & \alpha_۲^۲ - \alpha_۱\alpha_۲ & \cdots & \alpha_n^۲ - \alpha_۱\alpha_n \\ ۰ & \alpha_۲^۳ - \alpha_۱\alpha_۲^۲ & \cdots & \alpha_n^۳ - \alpha_۱\alpha_n^۲ \\ \vdots & \vdots & \vdots & \vdots \\ ۰ & \alpha_۲^{n-۱} - \alpha_۱\alpha_۲^{n-۲} & \cdots & \alpha_n^۲ - \alpha_۱\alpha_n \end{vmatrix}$$

$$\begin{aligned}
&= \begin{vmatrix} \alpha_2-\alpha_1 & \cdots & \alpha_n-\alpha_1 \\ \alpha_2^2-\alpha_1\alpha_2 & \cdots & \alpha_n^2-\alpha_1\alpha_n \\ \alpha_2^3-\alpha_1\alpha_2^2 & \cdots & \alpha_n^3-\alpha_1\alpha_n^2 \\ \vdots & \vdots & \vdots \\ \alpha_2^{n-1}-\alpha_1\alpha_2^{n-2} & \cdots & \alpha_n^2-\alpha_1\alpha_n \end{vmatrix} \\
&= (\alpha_2-\alpha_1)(\alpha_3-\alpha_1)\cdots(\alpha_n-\alpha_1)D_{n-1} \\
&= \prod_{i<j}(\alpha_i-\alpha_j)
\end{aligned}$$

۱۲. فرض کنید ξ عضو اولیه‌ای از $\mathrm{GF}(2^m)$ و C کد دوری با ریشه‌های ξ، ξ^2، ...، ξ^{2t-1} باشد. اگر $f_i(x)$ چندجمله‌ای می‌نیمال ξ^i باشد، آنگاه $C=(g(t))$، که در آن $g(x)=\mathrm{lcm}\{f_i(x) \mid i=1,2,\ldots,2t-1\}$. C یک کد دوتایی است، پس هر توان زوج ξ ریشه‌ای از یک چندجمله‌ای می‌نیمال توان فردی از ξ است؛ مثلاً اگر $f_1(x)$ چندجمله‌ای می‌نیمال ξ باشد، آنگاه ξ^2، ξ^4، ...، همگی ریشه‌های $f_1(x)$ هستند. پس کافی است تنها توان‌های فرد i را در نظر بگیریم. در این‌جا $\deg f_i(x)\le m$ و t چندجمله‌ای می‌نیمال برای iهای فرد وجود دارد، پس $\dim C \ge n-mt$.

۱۳. $\mathbb{Z}_3^3$ را با استفاده از x^3+2x+1 تولید کنید. اگر a عضو اولیه‌ای باشد، چندجمله‌ای x^3+2x+1 ریشه‌ای از آن است. نشان دهید چندجمله‌ای می‌نیمال a^2 عبارت است از $(x-a^2)(x-a^6)(x-a^{18})=x^3+x^2+2$ و چندجمله‌ای می‌نیمال a^4 عبارت است از x^3+2x^2+2. عناصر a، a^2، a^3، a^4 ریشه‌هایی از حاصل‌ضرب این چندجمله‌ای‌ها هستند. پس این حاصل‌ضرب کد مورد نظر را تولید می‌کند:

$$1+x+x^2+x^3+2x^4+x^6+2x^7+x^9.$$

بعد این کد برابر ۱۷ است.

۱۴. ابتدا جدول ضرب $\mathrm{GF}(2^5)$ را بسازید. با جایگذاری درمی‌یابیم که برای $i=1,2,3,4$، $e(\xi^i)=u(\xi^i)$. این‌ها به ترتیب ξ^{28}، ξ^{25}، ۱، ξ^{19} هستند. باید $\sigma(z)=1+S_1z+S_2z^2$ را از معادلات $S_1\xi^{25}+S_2\xi^{28}+1=0$ و $\xi^{19}+S_1+S_2\xi^{25}=0$ به دست بیاوریم. داریم $S_1=\xi^{28}$، $S_2=\xi^{10}$؛ یعنی

$$\sigma(z)=(1-\xi^{14}z)(1-\xi^{27}z).$$

پس کد واژه برابر ۱۰۰۱۰۱۱۰۱۱۱۱۰۰۱۰۱۱۰۱۰۱۰۱۰۱۱۰۱۱۱ بوده است. چندجمله‌ای مولد کد برابر $(1+x^2+x^5)(1+x^2+x^3+x^4+x^5)$ است، یعنی

$$g(x)=1+x^3+x^5+x^6+x^8+x^9+x^{10}.$$

کد واژه عبارت است از $g(x)(1+x^{11}+x^{20})$.

۱۶. (الف) خیر (ب) بله

۱۷. $g(x)=(x-a)(x-a^2)=x^2+4x+3$، که در آن $a=2$ عضو اولیه‌ای از $\mathbb{Z}_5$ است.

۱۷. فرض $c=c_0c_1\cdots c_{n-1}$ یک کد واژه به وزن d باشد، در این صورت اگر $c_i\neq 0$ $c(1)=-c_n=\sum_{i=0}^{n-1}c_i$، آنگاه وزن می‌نیم به $d+1$ افزایش می‌یابد. اکنون به ازای یک a داریم $c(t)=a(t)g(t)$، پس $c(1)=a(1)g(1)$. تحقیق کنید $a(1)\neq 0$ و $g(1)\neq 0$ و از قضیه‌ی ۲.۵.۱۵ برای تکمیل اثبات استفاده کنید.

۲۳. فرض کنید $\{0,1,\ldots,p-1\}$ عناصر $\mathbb{Z}_p$ باشند. اگر k یک نامانده‌ی درجه‌ی دوم به پیمانه‌ی p باشد، آنگاه نگاشت $i\mapsto ik \mod p$ یک جایگشت روی $\mathbb{Z}_p$ است طوری که $kQ=N$، $kN=Q$. بنابراین

$$g_1(x)=\prod_{j\in N}(x-a^j)=\prod_{j\in Q}(x-a^j).$$

اگر σ نشان دهنده‌ی جایگشتی باشد که روی مولفه‌های $c = (c_۰, \dots, c_{p-۱}) \in \mathbb{Z}_p^p$ القا می‌شود، آن‌گاه داریم

$$\sum_{i=۰}^{p-۱} c^{ij} = \sum_{i=۰}^{p-۱} c_\sigma(i)(a^{kj})^i.$$

بنابراین a^j، به ازای هر $j \in Q$، ریشه‌ای از $c = \sum_{i=۰}^{p-۱} c_i x^i$ است اگر و تنها اگر a^{kj}، به ازای هر $kj \in N$، ریشه‌ای از $c = \sum_{i=۰}^{p-۱} c_{\sigma(i)} x^i$ باشد ؛ یعنی

$$c \in (g_۰(t)) \iff c_\sigma \in (g_۱(t)).$$

۲۴. فرض کنید $a \in \mathbb{Z}_۳^۶$، و G ماتریس مولد، و $c = aG$ عضوی از [۱۱, ۶, ۵]- کد گولای باشد، آن‌گاه $\mathrm{wt}(c) = c \cdot c^\top$. در $\mathbb{Z}_۳$ داریم

$$aGG^\top a^\top = -\left(\sum_{i=۲}^{۶} a_i\right)^۲ \not\equiv ۱ \mod ۳,$$

زیرا -۱ یک نامانده در $\mathbb{Z}_۳$ است.

۲۵. بعد کد برابر ۶ است، زیرا ماتریس مولد G از آن متقارن است. وزن هر سطر G بزرگ‌تر یا مساوی ۵، و وزن هر ترکیب خطی از دو سطر G بزرگ‌تر یا مساوی ۴، و بنا به تمرین قبل بزرگ‌تر یا مساوی ۵ است. به طریق مشابه، برای ترکیب هر سه یا چهار سطر G این مطلب برقرار است. فاصله‌ی می‌نیمم برابر ۵ است، یعنی کره‌های با شعاع ۲ هر دو کد واژه مجزا هستند. اما این کره‌ها $\mathbb{Z}_۳^{۱۱}$ را می‌پوشاند، زیرا

$$۳^۶\left(۱ + ۲\binom{۱۱}{۱} + ۲^۲\binom{۱۱}{۲}\right) = ۳^{۱۱}.$$

بنابراین کد، کامل است.

واژه‌نامه فارسی–انگلیسی

آ	
آبلی	abelian
حل‌پذیر	supper soluble
اجتماع	union
آزاد	free
اسکالر	scalar
اشتراک	intersection
اصل لانه کبوتری	piegonhole principle
اصل خوشترتیبی	well ordering principle
اصل موضوع انتخاب	axiom of choice
افراز	partition
الگوریتم اقلیدسی	Euclidian algorithm
الگوریتم تقسیم	division algorithm
انتزاعی	abstraction
اندیس	index
اندیس‌دار	indexed
اولیه	primitive
ایدآل	ideal
ایدآل اصلی	principal ideal
ایدآل اول	prime ideal
ایدآل ماکسیمال	maximal ideal
ب	
بازتابی	reflexive
بازنویس‌پذیر پذیر	rewritable
باقی‌مانده	remandier
بدیهی	trivial
برد	range
برووریختی	epimorphism
بستار نرمال	normal closuer
بعد	dimension
بی‌تاب	torsion free

پ

پایه	basis
پوشا	surjective
پوچ	nil
پوچ‌توان	nilpotent
تصویر تصویر	pre image
پیمانه	modulo
پیمایش	transversal

ت

تاب‌دار	tersion
تابع	function
تثلیث زاویه	angel trisection
تجزیه	decomposition
تجزیه‌ی اولیه	primary decomposition
تحدید	restricition
تحویل‌پذیر	reducible
تحویل‌ناپذیر	irreducible
ترانهش	transpostion
ترایا	transitive
ترتیب جزئی	partial order
ترکیب	composition
ترکیب خطی	linear combination
تزویج	conjugacy
تصویر	image
تصویر همریختی	epimorphic image
تضعیف مکعب	cube duplication
تظریف	refinement
تعویض‌پذیر	commutative
تعویض‌گر	commutator
تفاضل	difference
تک‌جمله‌ای	monomial
تک مقداری	single valued
تکیه‌گاه	support
تناظر	correspodence
توان	power
توسیع	extension
توسیع جبری	algebraic extension
توسیع جداپذیر	seperable extension
توسیع تجزیه	splitting extension
توسیع گالوا	Galios extension

توسیع متناهی	finite extension
تهی	empty

ث

ثابت‌ساز	stabilizer

ج

جادهی	injection
جایگشت	permutation
جایگشتپذیری	permutable
جبر	algebra
جبری	algebraic
جداپذیری	seperable
جدا ناپذیر	inseperable
جدول ضرب	multiplication table
جمع‌وند	summand

چ

چند دوری	polycyclic
چندجمله‌ای	polynomial

ح

حاصل‌ضرب	product
حساب	arithmatic
حلقه	ring
حل‌پذیر	soluble

خ

خارج‌قسمت	qoutient
خاصیت جهانی	universal property
خودتوان	idempotent
خودریختی	automorphism
خوش ترتیبی	well ordering
خوش تعریف	well defined

د

داخلی	inner
دامنه	domain
دامنه‌ی صحیح	integral domain
دایره‌بر	cyclotomic
درجه	degree

درون‌ریختی	endomorphism
درون نرمال	normal interior
دوجمله‌ای	binomial
دنباله	sequence
دور	cycle
دوری	cyclic
دو طرفی	two sided
دووجهی	dihedral

ر

رابطه	relation
رده	class
رده‌ی مزدوجی	conjugacy class
رتبه	rank
ریشه	root
ریشه‌ی اولیه‌ی واحد	primitive root of unity
ریشه‌ی واحد	root of unity

ز

زنجیر	chain
زوج مرتب	orderel pair
زیرحلقه	subring
زیرفضا	subspace
زیرگروه	subgroup
زیرمجموعه	subset
زیرمدول	submodule
زیرمیدان	subfield
زیرمیدان اول	prime subfield

س

ساختار جبری	algebraic structure
ساخت‌پذیر	constractible
ساده	simple
سرشت	character
سری	series
سری ترکیبی	composition series
سری مرکزی	central series
سری مرکزی بالایی	upper central series
سری مرکزی پایینی	lower central series
سری مشتق	derived series
سری نرمال	normal series

سره	proper
ش	
شاخص	index
شرکت‌پذیر	associative
شمارا	denumerable
شمارنده مقدماتی	elementary divisior
ص	
صادق	faithful
ض	
ضرایب	coefficient
ضرب	multiplication
ط	
طبیعی	natural
ع	
عدد اصلی	cardinal number
عدد اول	prime number
عدد حقیقی	real number
عدد صحیح	integer
عدد طبیعی	natural number
عدد گویا	rational number
عدد مختلط	complex number
عضو	element
عمل	action
عمل دوتایی	binary operation
ف	
فرا آبلی	metabelian
فضای برداری	vector space
ق	
قانون برج	tower law
قانون حذف	cancellation law
قرینه	negative
قضیه	theorem
ک	

کاملاً پایا	fully invariant
کسر	fraction

گ

گروه	group
گروه آزاد	free group
گروه خطی عمومی	general linear group
گروه خطی خاص	sperial linear group
گروه ساده	simple group
گروه متقارن	symmetric group
گروه متناوب	alternating group

م

ماکسیمال	maximal
متقارن	symemetric
متناهیاً تولید شده	finitely generated
مجزا	disjoint
مجموع	sum
مجموعه	set
مجموعه‌ی توانی	powerset
مجموعه‌ی مولد	generating set
محتوای	content
محک	ceriterion
مدار	orbit
مدول	module
مرتبه	order
مرکز	center
مرکزی	central
مرکزساز	centralizer
مزدوج	conjugate
مزدوج مختلط	complex conjugate
مستقل خطی	linearly independent
مستقیم	direct
مشخصه	charactristic
مشخصاً ساده	charactristically simple
معادله	equation
معادله‌ی رده‌ای	class equation
معکوس	inverse
مقسوم علیه	divisor
مقسوم علیه صفر	zero divisor
مقداریاب	evaluation

مولد	generator
میدان	field

ن

نابدیهی	nontrivial
ناشمارا	nondenumarable
نامتناهی	infinite
نامولد	non generator
نایکه	non unit
نرمال	normal
نرمال‌ساز	normalizer
نظریه	theory
نقطه‌وار	pointwise
نگاشت	function
نما	exponent
نمایش	representation
نوع	type
نیم‌گروه	semigroup

و

وابسته‌ی خطی	linearly dependent
واحد	unity
واژه	word
واژه‌ی تهی	empty word
واژه‌ی کاهشی	redued word
وارون	inverse
وارون‌پذیر	invertible

هـ

هم‌ارزی	equivalence
همانی	ideutity
هم‌توان	equinumerous
همدم	associate
همریختی	homomorphism
همریختی تصویر	projection homorphism
هم‌عدد	equinumerous
هم‌مجموعه	coset
هم‌مجموعه‌ی مضاعف	double coset
هم‌نهشت	congeruent
هولومورف	holomorph

ی

یکانی	unitary
یک‌به‌یک	one to one
یکریخت	isomorphic
یکریختی	isomorphism
یکه	unit
یکتایی تجزیه	unique factorization

فهرست اسامی خاص

Abel, Neils Henrick, ۱۸۰۲ – ۱۸۲۹, ۲۵, ۴۹, ۳۳۷
Aschbacher, Michael, ۱۹۴۴ – ..., ۸۲
Berlekamp, Elwyn, , ۳۹۵
Bernstein, Felix, ۱۸۷۸ – ۱۹۵۶, ۲۲
Bool, Georg, ۱۸۱۵ – ۱۸۶۴, ۲۰۷
Bose, Raj Chandra, ۱۹۰۱ – ۱۹۸۷, ۳۸۹
Brauer, Richard Dagobert, ۱۹۰۱ – ۱۹۷۷, ۸۱, ۸۲
Burnside, William, ۱۸۵۲ – ۱۹۲۷, ۸۲
Cantor, Georg Ferdinand Ludwig Philipp, ۱۸۴۵ – ۱۹۱۸, ۱۸
Chevally Claud, ۱۹۰۹ – ۱۹۸۴, ۸۲
Clairant, Alexis Claude, ۱۷۱۳ – ۱۷۶۵, ۱۴
Conway, John Horton, ۱۹۳۷ – ۲۰۲۰, ۸۲
Cauchy, Augustin Louis, ۱۷۸۹ – ۱۸۵۷, ۲۵, ۲۶, ۹۲
Cayley, Arthur, ۱۸۲۱ – ۱۸۹۵, ۴۹
Cole, Frank Nelson, ۱۸۶۱ – ۱۹۲۶, ۸۱, ۸۲
Chaudhuri, Dwijendra Kumar Ray, ۱۹۳۳ – ..., ۳۸۹
Dedekind, Richard, ۱۸۳۱ – ۱۹۱۶, ۷۰, ۲۵۵
Dieudonnè, Jean Alexandre Engenè, ۱۹۰۶ – ۱۹۹۲, ۸۲
Dickson, Leonard, ۱۸۷۴ – ۱۹۵۴, ۸۲
De Morgan, Augustus, ۱۸۰۶ – ۱۸۷۱, ۵
Dirichlet, Johann Peter Gustav Lejeune, ۱۸۰۵ – ۱۸۵۹, ۱۴
Eisenstien, Ferdinand Gotthold Max, ۱۸۳۲ – ۱۸۵۲, ۲۴۳
Euclid of Alexandria, $B.C$۳۲۵ – $B.C.$۲۶۵, ۳۷, ۳۸, ۳۹
Euler, Lenohard, ۱۷۰۷ – ۱۷۸۳, ۱۴, ۳۳۷
Feit, Walter, ۱۹۳۲ – ۲۰۰۴, ۸۲
Frege, Fredrich Ludwig Gotlop, ۱۸۴۸ – ۱۹۲۵, ۴
Fermat, Pierre De, ۱۶۰۱ – ۱۶۶۵, ۴۶, ۲۵۵
Ferro, Scipione del, ۱۴۶۵ – ۱۹۲۶, ۳۳۶
Frattini, Giovanni, ۱۸۵۲ – ۱۹۲۵, ۱۴۷
Fischer, Brend, ۱۹۳۶ – ۲۰۲۰, ۸۲, ۸۲
Frobenius, Ferdinand Georg, ۱۸۴۹ – ۱۹۱۷, ۱۲۷
Galios, Evariste, ۱۸۱۱ – ۱۸۳۲, ۴۹, ۸۱, ۲۹۳, ۳۳۷
Gauss, Johann Carl Friedrich, ۱۷۷۷ – ۱۸۵۵, ۲۴۰, ۲۴۰, ۲۴۳

Gorenstein, Daniel, ۱۹۲۳ – ۱۹۹۲, ۸۲, ۸۲
Griess, Robert Louis, ۱۹۴۵ – ..., ۸۲
Golay, Marcel Jules Edouard, ۱۹۰۲ – ۱۹۸۹, ۳۹۳, ۴۰۰
Hamming, Richard Wesely, ۱۹۱۵ – ۱۹۹۸, ۳۴۹
Hirsch, Kurt August, ۱۹۰۶ – ۱۹۸۶, ۱۵۹
Hölder, Otto Ludwig, ۱۸۵۹ – ۱۹۳۷, ۱۵۴, ۸۱
Hocquenghem, Alexis, ۱۹۰۸ – ۱۹۹۰, ۳۸۹
Jacobson, Nathan, ۱۹۱۰ – ۱۹۹۹, ۲۲۸, ۳۲۲
Janko, Zvonimir, ۱۹۳۲ – ۲۰۲۲, ۸۲
Jordan, Ennemond Camille, ۱۸۳۸ – ۱۹۲۲, ۸۱, ۸۱, ۹۱
Kuratowski, Kazimierz, ۱۸۶۰ – ۱۹۸۰, ۱۱
Klien, Felix, ۱۸۹۴ – ۱۹۲۵, ۸۱
Kronecker, Leopold, ۱۸۲۳ – ۱۹۸۱, ۲۵۳
Kummer, Ernest, ۱۸۱۰ – ۱۸۹۳, ۲۵۵
Lammè, Gabriel, ۱۷۹۵ – ۱۸۷۰, ۲۵۵
Lagrange, Joseph Louis, ۱۷۳۶ – ۱۸۱۳, ۲۵, ۸۳, ۳۳۷
MacWilliams, Florence Jessie Collinson, ۱۹۱۷ – ۱۹۹۰, ۳۶۲
Mathieu, Emil Lèonard, ۱۸۳۵ – ۱۸۹۰, ۸۱
Mattson, , ۳۷۹
Miller, Geoerg Abram, ۱۸۳۶ – ۱۹۵۱, ۸۱
Möbius, August Ferdinand, ۱۷۹۰ – ۱۸۶۸, ۳۰۵
Newton, Sir Issac, ۱۶۴۳ – ۱۷۲۷, ۲۰۸
Pascal, Blaise, ۱۶۲۳ – ۱۶۶۲, ۱۳, ۲۰۱
Pell, John, ۱۶۱۱ – ۱۶۸۵, ۲۶۹
Poincarè, Jules Henri, ۱۸۵۴ – ۱۹۱۲, ۸۸
Reed, Irving Stoy, ۱۹۲۳ – ۲۰۱۲, ۳۹۱
Rolle, Michel, ۱۶۵۲ – ۱۷۱۹, ۷۶۵
Ruffini, Paolo, ۱۷۶۵ – ۱۸۲۲, ۲۵
Russel, Bertrand Arthur William, ۱۸۷۲ – ۱۹۷۰, ۴, ۲۱
Shannon, Claud Elwood, ۱۹۱۶ – ۲۰۰۱, ۳۴۹
Schröder, Fredrich Wilhem Karl Ernest, ۱۸۴۱ – ۱۹۰۲, ۲۲
Schreier, Otto, ۱۹۰۱ – ۱۹۲۹, ۱۵۴
Slepian, David, ۱۹۲۳ – ۲۰۰۷, ۳۶۰
Solomon, Gustave, ۱۹۳۰ – ۱۹۹۶, ۳۷۹, ۳۹۱
Stickelberger, ۱۸۵۰ – ۱۹۳۶, ۱۲۷
Sylow, Peter Ludwig Mejdell, ۱۸۲۳ – ۱۹۱۸, ۹۲, ۱۱۹
Thompson, John Griggs, ۱۹۳۲ – ..., ۸۱
Vandermond, Alexandre Théophile, ۱۷۳۵ – ۱۷۹۰, ۳۹۰
Von Dyck, Walther Franz, ۱۸۵۶ – ۱۹۳۴, ۱۶۵
Wedderburn, Joseh Henry Malcagen, ۱۸۸۲ – ۱۹۴۸, ۳۲۱
Wiles, Andrew, ۱۹۵۳ – ..., ۲۵۵

Wilson, John, ۱۷۴۱ – ۱۷۹۳, ۴۷
Zassenhaus, Hans, ۱۹۱۲ – ۱۹۹۱, ۱۵۳
Zermelo, Ernest Friedrich Ferdinand, ۱۸۷۱ – ۱۹۵۳, ۴
Zorn, Max, ۱۹۰۶ – ۱۹۹۳, ۱۱

فهرست نمادها

عدد داده شده اولین صفحه‌ی معرفی نماد را مشخص می‌کند.

$\in$	تعلق داشتن عضو به مجموعه، ۱
$\notin$	تعلق نداشتن عضو به مجموعه، ۱
$\subseteq$	زیرمجموعه بودن، ۱
$\emptyset$	مجموعه‌ی تهی، ۱
$\mathbb{N}$	مجموعه‌ی اعداد طبیعی، ۱
$\mathbb{Z}$	مجموعه‌ی اعداد صحیح، ۱
$\mathbb{Q}$	مجموعه‌ی اعداد گویا، ۱
$\mathbb{R}$	مجموعه‌ی اعداد حقیقی، ۱
$\mathbb{C}$	مجموعه‌ی اعداد مختلط، ۱
$A \cup B$	اجتماع دو مجموعه، ۲
$A \cap B$	اشتراک دو مجموعه، ۲
$\exists$	وجود دارد، ۲
$\forall$	به ازای هر، ۲
$\bigcup_{\alpha \in I} A_\alpha$	اجتماع خانواده‌ای از مجموعه‌ها، ۲
$\bigcup \mathcal{A}$	اجتماع خانواده‌ای از مجموعه‌ها، ۲
$\bigcap_{\alpha \in I} A_\alpha$	اشتراک خانواده‌ای از مجموعه‌ها، ۲
$\bigcap \mathcal{A}$	اشتراک خانواده‌ای از مجموعه‌ها، ۲
$A - B$	تفاضل دو مجموعه، ۳
$\mathcal{P}(X)$	مجموعه‌ی همه‌ی زیر مجموعه‌های یک مجموعه، ۳
(x, y)	زوج مرتب، ۳
$A \times B$	حاصل‌ضرب دکارتی دو مجموعه، ۳
$\iff$	اگر و تنها اگر، ۳
$\impliedby$	تنها اگر، ۵
$\implies$	اگر، ۵
$\operatorname{dom} R$	دامنه یک رابطه، ۵
xRy	زوج مرتب (x, y) در R است، ۵
$\operatorname{ran} R$	برد یک رابطه، ۵
A/R	مجموعه‌ی رده‌های هم‌ارزی، ۷
$S \circ R$	ترکیب دو رابطه، ۷
R^n	توان‌های یک رابطه، ۷
R^{-1}	معکوس یک رابطه، ۷

$a \mid b$	a، b را عاد می‌کند، ۹
$f : A \longrightarrow B$	f تابعی از A به B است، ۱۴
$f(x)$	تصویر x تحت تابع f، ۱۴
f^{-1}	وارون تابع f، ۱۴
id_A	تابع همانی روی مجموعه‌ی A، ۱۴
$f\|_X$	تحدید تابع f به X، ۱۵
$A \approx B$	A با B هم‌توان است، ۱۶
$\mathbb{N}_k$	مجموعه‌ی اولین k عدد طبیعی، ۱۶
$\aleph_0$	عدد اصلی مجموعه‌ی اعداد طبیعی، ۱۸
$\prod_{\alpha\in I} A_\alpha$	حاصل‌ضرب دکارتی خانواده‌ای از مجموعه‌ها، ۲۰
	گروه‌ها، حلقه‌ها، مدول‌ها، ۲۰
$A_1 \times \cdots \times A_n$	حاصل‌ضرب دکارتی n مجموعه، گروه، حلقه، مدول، ۲۰
$(x_1, \ldots, x_n)$	n-تایی مرتب، ۲۰
$\mathbb{Q}_{pos}$	مجموعه‌ی اعداد گویای مثبت، ۲۱
$f(X)$	تصویر مجموعه‌ی X تحت تابع f، ۲۲
$f^{-1}(X)$	تصویر معکوس مجموعه‌ی X تحت تابع f، ۲۲
$k\mathbb{Z}$	مجموعه‌ی اعداد صحیح مضرب k، ۲۲
S_X	مجموعه‌ی جایگشت‌های روی مجموعه‌ی X، ۲۵
$\mathrm{Sym}(X)$	مجموعه‌ی جایگشت‌های روی مجموعه‌ی X، ۲۵
S_n	مجموعه‌ی جایگشت‌های روی $\{1, 2, \ldots, n\}$ ، ۲۵
$\mathrm{Sym}(n)$	مجموعه‌ی جایگشت‌های روی $\{1, 2, \ldots, n\}$ ، ۲۵
$\mathrm{orb}_\alpha(x)$	مدار جایگشت α شامل عضو x ، ۲۹
A_n	گروه جایگشت‌های زوج روی $\{1, 2, \ldots, n\}$ ، ۳۳
$\gcd\{a, b\}$	بزرگ‌ترین مقسوم‌علیه مشترک a و b ، ۳۶
$\mathrm{lcm}\{a, b\}$	کوچک‌ترین مضرب مشترک a و b، ۳۹
$\varphi(n)$	تعداد اعداد طبیعی کمتر از n و متباین با n، ۴۰
$a \equiv b \mod n$	n، $b - a$ را عاد می‌کند، ۴۲
$\mathbb{Z}_n$	مجموعه‌ی اعداد صحیح به پیمانه n، ۴۲
$\bar{a}$	رده هم‌نهشتی a، ۴۲
$\mathbb{Z}_n^\times$	مجموعه‌ی اعضای وارون‌پذیر در $\mathbb{Z}_n$، ۴۴
$\mathbb{R}^\times$	$\mathbb{R} - \{0\}$، ۵۰
$\mathbb{Q}^\times$	$\mathbb{Q} - \{0\}$، ۵۰
$\mathbb{C}^\times$	$\mathbb{C} - \{0\}$، ۵۰
$\mathbb{Z}^\times$	$\{-1, 1\}$، ۵۰
$\mathrm{Map}(X, X)$	مجموعه‌ی توابع از X به X، ۵۰
V_4	۴-گروه کلاین، ۵۳
Q_8	گروه چهارگان، ۵۳
C_n	گروه ضربی ریشه‌های nام واحد، ۵۳
C_{p^∞}	گروه شبه دوری، ۵۳
D_{2n}	گروه دووجهی از مرتبه‌ی $2n$، ۵۴
$\mathrm{GL}_n(F)$	گروه ضربی ماتریس‌های وارون‌پذیر با درایه‌های در میدان F، ۵۵

$\mathrm{SL}_n(F)$	گروه ضربی ماتریس‌های با دترمینان ۱ با درایه‌های در میدان F، ۵۵
$\mathrm{GL}(V)$	گروه ضربی تبدیل‌های خطی وارون‌پذیر روی فضای برداری V، ۵۵
$G_1 \times \cdots \times G_n$	حاصل‌ضرب مستقیم گروه‌ها، ۵۷
$g^{-1}xg$	مزدوج x تحت g، ۵۸
$\mathrm{orb}(x)$	رده مزدوجی x، ۵۸
$O(x)$	مرتبه‌ی یک عضو در یک گروه، ۵۸
$\exp(G)$	نمای یک گروه، ۵۹
$\langle a \rangle$	گروه دوری تولید شده توسط a، ۶۰
$G \cong H$	یکریختی دو گروه، ۶۳
$\mathrm{Aut}\, G$	گروه خودریختی‌های یک گروه، ۶۴
$\mathrm{End} G$	مونوئید درون‌ریختی‌های یک گروه، ۶۴
$H \leq G$	H زیرگروه G است، ۶۶
$H < G$	H زیرگروه سره G است، ۶۶
$\ker f$	هسته یک همریختی، ۶۷
$\mathrm{Inn}\, G$	گروه خودریختی‌های داخلی یک گروه، ۶۷
$G \hookrightarrow H$	همریختی یک‌به‌یک از G به H وجود دارد ، ۶۷
XY	حاصل‌ضرب دو زیرمجموعه از یک گروه، ۶۹
$\langle X \rangle$	گروه تولید شده توسط مجموعه‌ی X، ۷۰
D_∞	گروه دووجهی نامتناهی، ۷۱
$C_G(x)$	مرکزساز x در G، ۷۴
$C_G(X)$	مرکزساز مجموعه‌ی X در G، ۷۴
$Z(G)$	مرکز یک گروه، ۷۴
$N_G(X)$	نرمال‌ساز X در G، ۷۴
$[x, y]$	تعویض‌گر x و y، ۷۵
G'	زیرگروه مشتق G، ۷۵
$[H, K]$	تعویض‌گر دو زیرگروه، ۷۶
G''	مشتق مرتبه‌ی دوم ، ۷۶
G'''	مشتق مرتبه‌ی سوم، ۷۶
$G^{(n)}$	مشتق مرتبه‌ی nام، ۷۶
H char G	H در G مشخصه است، ۷۷
$H \trianglelefteq G$	H زیرگروه نرمال G است، ۷۷
$H \lhd G$	H زیرگروه نرمال و سره G است، ۷۷
H_G	درون نرمال یا هسته H در G، ۸۳
H^G	بستار نرمال H در G، ۸۳
aH	هم‌مجموعه‌ی چپ H، ۸۴
$\lvert G : H \rvert$	شاخص H در G، ۸۴
Ha	هم‌مجموعه‌ی راست H، ۸۵
$k(G)$	تعداد رده‌های مزدوجی G، ۹۰
$\mathrm{FC}(G)$	FC-مرکز G، ۹۱
G/H	گروه خارج قسمتی، ۹۲
$H \times K$	حاصل‌ضرب مستقیم دو گروه، ۹۹

$H \oplus K$ حاصل‌ضرب مستقیم دو گروه جمعی ، ۹۹

$\prod_{i \in I} G_i$ حاصل‌ضرب دکارتی خانواده‌ای از گروه‌ها، ۱۰۲

$\mathrm{Cr}_{i \in I} G_i$ حاصل‌ضرب دکارتی خانواده‌ای از گروه‌ها، ۱۰۲

$\mathrm{Dr}_{i \in I} G_i$ حاصل‌ضرب مستقیم خانواده‌ای از گروه‌ها، ۱۰۲

$\oplus_{i \in I} G_i$ حاصل‌جمع مستقیم خانواده‌ای از گروه‌های جمعی ، ۱۰۲

$H \rtimes K$ حاصل‌ضرب نیم‌مستقیم H توسط K، ۱۰۵

$H \rtimes_{\varphi} K$ حاصل‌ضرب نیم‌مستقیم H توسط K نسبت به همریختی φ، ۱۰۶

$\mathrm{Hol}\, H$ هولومورف H، حاصل‌ضرب نیم‌مستقیم H توسط $\mathrm{Aut}\, H$، ۱۰۸

نسبت به همریختی شمولی، ۱۰۸

$\mathrm{Dih}\, A$ هولومورف نسبی گروه آبلی A، ۱۰۸

$g \cdot x$ عمل g روی x، ۱۰۹

$\mathrm{stab}_G(x)$ ثابت‌ساز x در G، ۱۱۱

$\mathrm{orb}_G(x)$ رده هم‌ارزی شامل x نسبت به عمل گروه، ۱۱۱

G_x ثابت‌ساز x در G، ۱۱۱

X_f مجموعه‌ی اعضای X که مدارشان یک عضوی است، ۱۱۲

$\mathrm{Syl}_p(G)$ مجموعه‌ی p- زیرگروه‌های سیلوی G، ۱۲۰

$G(p)$ مجموعه‌ی اعضایی از G که مرتبه‌شان توانی از p است، ۱۲۵

$T(G)$ مجموعه‌ی عناصر با مرتبه‌ی متناهی در G، ۱۳۴

$G[n]$ مجموعه‌ی اعضایی از G که مرتبه‌شان n را عاد می‌کند، ۱۳۵

nG مجموعه‌ی مضارب اعضای گروه آبلی G، ۱۳۵

$\Gamma_1(G)$ اولین جمله سری مرکزی پایینی، ۱۴۱

$\Gamma_2(G)$ دومین جمله سری مرکزی پایینی، ۱۴۱

$\Gamma_n(G)$ nامین جمله سری مرکزی پایینی، ۱۴۱

$Z_0(G)$ اولین جمله سری مرکزی بالایی، ۱۴۳

$Z_1(G)$ دومین جمله سری مرکزی بالایی، ۱۴۳

$Z_{n+1}(G)$ nامین جمله سری مرکزی بالایی، ۱۴۳

$\Phi(G)$ زیرگروه فراتینی، ۱۴۷

$\ell(G)$ طول ترکیبی G، ۱۵۴

$\langle X \mid R \rangle$ گروه تولید شده توسط X که در روابط R صدق می‌کند، ۱۶۱

$F(X)$ گروه آزاد روی مجموعهX، ۱۶۲

$\sigma(G)$ عدد n است که G را می‌توان به صورت اجتماع n زیرگروه سره‌اش نوشت، اما نه کمتر، ۱۷۳

$\#\mathrm{cent}(G)$ تعداد مرکزسازهای یک گروه، ۱۷۸

$\mathrm{pr}(G)$ احتمال تعویض شدن دو عضو در یک گروه، ۱۸۲

$\#\mathrm{prcyc}(G)$ احتمال دوری بودن گروه تولید شده توسط دو عضو در یک گروه، ۱۸۵

$M_n(R)$ حلقه‌ی ماتریس‌های $n \times n$ با درایه‌های در حلقه‌ی R، ۱۹۸

$R[x]$ حلقه‌ی چندجمله‌ای‌ها با درایه‌های در حلقه‌ی R، ۱۹۹

Q_R حلقه‌ی کواترنیونی با ضرایب در R، ۱۹۹

$\mathrm{char}\, R$ مشخصه‌ی حلقه‌ی R، ۲۰۰

$\mathrm{Cent}(R)$ مرکز حلقه‌ی R، ۲۰۵

$(X)_\ell$ ایدآل چپ تولید شده توسط X، ۲۲۲

$(X)_r$	ایدآل راست تولید شده توسط X، ۲۲۲
(X)	ایدآل تولید شده توسط X، ۲۲۲
IJ	حاصل‌ضرب دو ایدآل، ۲۲۳
$J(R)$	رادیکال ژاکوبسون حلقه‌ی R، ۲۲۸
$\deg f(x)$	درجه‌ی چندجمله‌ای $f(x)$، ۲۳۲
$\Phi_n(x)$	nامین چندجمله‌ای دایره‌بر، ۲۴۴
$C(f)$	محتوای چندجمله‌ای $f(x)$، ۲۶۳
$\langle X \rangle$	مدول تولید شده توسط X، ۲۷۴
$\operatorname{Span} X$	مدول تولید شده توسط X، ۲۷۴
$\dim_R V$	بعد فضای برداری V روی حلقه‌ی تقسیم R، ۲۷۹
$\dim V$	بعد فضای برداری V روی حلقه‌ی تقسیم R، ۲۷۹
$K(A)$	کوچک‌ترین میدان که شامل میدان K و مجموعه‌ی A است، ۲۸۳
$K[A]$	کوچک‌ترین حلقه‌ی که شامل K و A است، ۲۸۳
$F : K$	F یک میدان شامل میدان K است، ۲۸۳
$K[a_1, \ldots, a_n]$	کوچک‌ترین حلقه‌ای که شامل K و a_1، ...، a_n است ، ۲۸۳
$K(a_1, \ldots, a_n)$	کوچک‌ترین میدانی که شامل K و a_1، ...، a_n است ، ۲۸۳
$[F : K]$	درجه‌ی توسیع، ۲۸۶
$\mathrm{GF}(p^n)$	میدان متناهی با مرتبه‌ی p^n، ۲۸۶
$\operatorname{Aut}_K F$	گروه گالوای F روی K، ۲۹۷
$\mathrm{G}(F : K)$	گروه گالوای F روی K، ۳۱۲
$\mathrm{Gal}(F : K)$	گروه گالوای F روی K، ۳۱۲
$\mathrm{Gal}(f(x))$	گروه گالوای چندجمله‌ای $f(x)$، ۳۱۲
F_G	میدان ثابت G، ۳۲۸
$C^\perp$	دوگان کد C، ۳۵۱
$A^\top$	ترانهاده‌ی ماتریس A، ۳۵۱
$\mathrm{wt}(u)$	وزن واژه‌ی u، ۳۵۷
$d(u, v)$	فاصله‌ی دو واژه‌ی u و v ، ۳۵۷
$d_{\min}$	فاصله‌ی می‌نیمم یک کد، ۳۵۷
$S_r(u)$	کره به مرکز u و شعاع r، ۳۵۸
$\mathcal{H}(k, q)$	$[n, n-k]$- کد همینگ $(n = \frac{q^k - 1}{q - 1})$، ۳۵۹
$W_C(x, y)$	چندجمله‌ای شمارش‌گر وزن کد C، ۳۶۲

نمایه

آبل، ۴۶۰
آبلی، ۳۴، ۶۸
آبلی مقدماتی، ۱۰۹
آیزنشتاین، ۳۳۲
ابرحل‌پذیر، ۲۱۴
اتحاد مک ویلیامز، ۴۹۷
اتحاد پاسکال، ۱۸، ۲۷۳
اجتماع، ۲
احتمال تعویض شدن، ۲۴۹
استقرا، ۱۶
استیکلبرگر، ۱۷۴
اسکالر، ۳۷۱
اشباخه، ۱۱۲
اشتراک، ۲
اصل استقرای ریاضی، ۱۶
اصل خوش‌ترتیبی، ۱۵
اصل لانه کبوتری، ۲۲
اصل موضوع انتخاب، ۲۷
اعداد ، ۴۹
افراز، ۹، ۱۱۵
اقلیدس، ۵۵
الفبا، ۴۷۷
الگوریتم اقلیدسی، ۵۲، ۳۳۶
الگوریتم تقسیم، ۴۹، ۳۱۸
الگوریتم کد گشایی، ۴۹۴
اندیس‌دار، ۳
اولیه، ۳۵۸
اویلر، ۱۹، ۴۶۰
ایدآل، ۲۸۸
ایدآل اول، ۳۰۶
ایدآل سره، ۲۸۹
ایدآل ماکسیمال، ۳۰۸، ۳۴۰
ایدآل پوچ، ۳۰۴
ایدآل پوچ‌توان، ۳۰۴
ایدآل چپ تولید شده، ۳۰۲
ایدآل‌های بدیهی، ۲۸۹
بازتابی، ۸
بازنویس‌پذیر، ۲۶۲
باقیمانده، ۵۰، ۳۱۹
باوس، ۵۳۰
براوئر، ۱۱۱
برن ساید، ۱۱۱
برنشتاین، ۳۱
بروریختی، ۸۵
بزرگ‌ترین مقسوم‌علیه مشترک، ۵۱، ۳۳۵، ۳۴۹، ۳۶۴
بستار نرمال، ۱۱۳، ۲۲۴
بسته‌ی جبری، ۳۹۵
بی‌تاب، ۸۰
تابع، ۱۸
تابع موبیوس، ۴۱۶
تاب‌دار، ۸۰
تامپسون، ۱۱۱
تبدیل تک‌جمله‌ای، ۴۸۵
تبدیل خطی کسری، ۲۲۵
تثلیث زاویه، ۴۶۶
تحدید، ۲۰
تحویل‌ناپذیر، ۳۲۵، ۳۴۰، ۳۵۱
ترانهش، ۳۸
ترایا، ۸
ترتیب جزیی، ۱۲
ترکیب، ۱۰، ۲۰
تزویج، ۷۹
تصحیح خطا، ۴۸۹
تصحیح کننده، ۴۸۹
تصویر، ۱۹، ۱۴۰، ۲۹۴
تصویر همریخت، ۲۲۴
تضعیف مکعب، ۴۶۷
تظریف، ۲۰۷
تظریف سره، ۲۰۷
تعمیم قانون شرکت‌پذیری، ۷۰

تعویض‌ناپذیر، ۲۶۸
تعویض‌پذیر، ۳۲، ۳۴، ۶۸، ۲۶۸
تعویض‌گر، ۱۰۲، ۱۸۷
تفاضل، ۴
تقارن، ۷۴
تهی، ۱
توابع گویای متقارن، ۴۶۴
توازن، ۴۶
توان، ۷۱
توزیع‌پذیری، ۷۴، ۲۶۷
توسیع، ۳۸۶
توسیع تجزیه، ۳۹۷، ۴۴۶
توسیع جبری، ۳۹۰
توسیع رادیکالی، ۴۶۱
توسیع ساده، ۴۲۴
توسیع متناهی، ۳۸۹
توسیع میدان، ۳۴۵
توسیع نرمال، ۴۴۵
تولید متناهی، ۳۰۳
تکریختی، ۸۵
تکیه‌گاه، ۱۳۹، ۲۹۳، ۳۷۵
تک‌مقداری، ۱۹
ثابت ساز، ۱۵۱
جادهی، ۱۴۰، ۲۹۴
جایگشت، ۳۴
جایگشت‌پذیر، ۲۵۵
جبری، ۳۸۷
جداناپذیر، ۴۲۳
جداپذیر ، ۴۲۳
جدول اسلیپن، ۴۹۳
حاصل‌جمع مستقیم، ۱۳۶، ۱۷۸، ۲۹۵، ۳۷۷
حاصل‌ضرب دکارتی، ۵، ۲۷، ۷۷، ۱۳۵، ۱۳۷، ۲۷۱
حاصل‌ضرب مستقیم، ۷۷، ۱۳۶، ۱۴۰، ۲۹۴
حاصل‌ضرب نیم‌مستقیم، ۱۴۳، ۱۴۶
حلقه، ۲۶۷
حلقه تقسیم متناهی، ۴۳۹
حلقه‌ی اعداد صحیح گاوسی، ۳۴۷، ۳۵۲، ۳۶۵
حلقه‌ی ایدآل اصلی، ۳۴۹
حلقه‌ی بولی، ۲۸۱، ۳۱۲
حلقه‌ی تقسیم ، ۲۶۸
حلقه‌ی خارج‌قسمتی، ۲۸۸
حلقه‌ی صفر، ۲۷۴، ۳۰۵
حلقه‌ی ماتریس‌ها، ۲۶۹
حلقه‌ی ماتریس‌های بالا مثلثی، ۲۷۹
حلقه‌ی موضعی، ۲۹۷، ۳۱۳
حلقه‌ی چندجمله‌ای‌ها، ۳۱۵
حلقه‌ی کواترنیونی، ۲۷۱
حلقه‌ی یکدار، ۲۶۸
حل‌پذیر، ۱۰۳، ۱۸۷، ۴۶۱
خارج قسمت، ۵۰، ۳۱۹
خاصیت جهانی، ۲۲۱
خودتوان، ۷۹، ۲۷۹
خودریختی، ۸۷، ۲۸۳، ۴۲۶
خودریختی داخلی، ۸۸، ۹۱
خودریختی فروبنیوس، ۲۹۰، ۴۳۰، ۴۳۵، ۵۴۲
خوش‌تعریف، ۱۹
دامنه‌ی اقلیدسی، ۳۶۳
دامنه‌ی ایدآل اصلی، ۳۴۰
دامنه‌ی تجزیه، ۳۵۴
دامنه‌ی صحیح، ۲۷۴
دامنه‌ی یکتایی تجزیه، ۳۵۶
دایره‌بر، ۳۳۴
دترمینان واندرموند، ۵۳۱
ددکیند، ۹۵
درجه‌ی توسیع، ۳۸۹
درجه‌ی چندجمله‌ای، ۳۱۶
درون نرمال، ۱۱۳
درون‌ریختی، ۸۷
درون‌ریختی فروبنیوس، ۲۹۰
دو متغیره، ۳۲۳
دور، ۳۸
دوری، ۸۲
دیریکله، ۱۹
دیودونه، ۱۱۲
دیکسون، ۱۱۱
رابطه‌ی دوتایی، ۷
رابطه‌ی هم‌ارزی، ۸
رادیکال پوچ، ۲۸۰
راسل، ۵
رتبه، ۱۸۰
رده، ۶
رده‌ی سره، ۶

رده‌ی مزدوجی، ۱۱۸
روابط، ۲۲۴
روش انتزاعی، ۲
روش حذفی گاوس، ۵۰۲
ریشه‌ی اولیه‌ی واحد، ۴۰۶، ۴۳۳
زرملو، ۵
زنجیر، ۱۳
زوج، ۴۵
زوج مرتب، ۴
زیرحلقه، ۲۷۸
زیرحلقه‌ی تولید شده، ۳۸۶
زیرمجموعه، ۱
زیرمدول، ۳۷۲
زیرمدول تولید شده، ۳۷۳
زیرمیدان، ۲۷۸
زیرمیدان تولید شده، ۳۸۶
زیرکد، ۵۳۳
زیرگروه، ۹۰
زیرگروه فراتینی، ۲۰۱
زیرگروه ماکسیمال ، ۱۹۸
زیرگروه مشتق، ۱۰۲، ۱۸۷
زیرگروه‌های بدیهی، ۹۰
ساختار جبری، ۳۲
ساختار دوری، ۴۳
ساخت‌پذیر، ۴۶۸
سرشت، ۴۹۵
سرشت بدیهی، ۴۹۵
سرشت گروه‌ها، ۴۹۵
سری اصلی، ۲۱۲
سری ترکیبی، ۲۰۵، ۲۱۱
سری سره، ۲۰۵
سری مرکزی، ۱۹۶
سری مرکزی بالایی، ۱۹۶
سری مرکزی پائینی، ۱۹۳
سری مشتق، ۱۰۳، ۱۸۸
سری نرمال، ۱۹۱، ۲۰۵، ۲۱۲
سندرُم ، ۴۹۳
شانون، ۴۷۷
شرایر، ۲۱۰
شرط زنجیر صعودی، ۳۵۵
شرودر، ۳۱
شرکت‌پذیر، ۳۲
شرکت‌پذیر ، ۲۱، ۳۴
شعاع پوششی، ۵۰۱
شمارش‌گر وزن، ۴۹۴
شمارنده‌ها، ۵۱
شمارنده‌های مقدماتی، ۱۷۵
شیفت دوری، ۵۰۷
صادق، ۱۵۱
ضریب پیشرو، ۳۱۶
طول حل‌پذیری، ۱۰۳، ۱۸۸
عاد، ۵۱
عدد اصلی، ۲۴
عدد اول، ۵۳
عضو اول، ۳۰۷، ۳۵۱، ۳۵۶
عضو اولیه، ۴۰۵
عضو بی‌اثر، ۳۲، ۳۴، ۶۸
عضو تحویل‌ناپذیر، ۳۵۶
عضو همانی، ۳۲، ۳۴، ۶۸
عمل، ۱۴۹
عمل بدیهی، ۱۵۱
عمل دوتایی، ۳۲
عمل صادق، ۱۵۲
عمل منظم، ۱۵۲
عمل چپ منظم، ۱۵۴
عوامل اصلی، ۲۱۲
عوامل دوری، ۲۱۴
فاصله‌ی طرح، ۵۳۰
فاصله‌ی می‌نیمم، ۴۸۸
فاصله‌ی همینگ، ۴۸۷
فراآبلی، ۱۰۳
فرد، ۴۵
فرما، ۳۴۷
فرمول وارون موبیوس، ۴۱۶، ۴۱۷
فروبنیوس، ۱۷۴
فرگه، ۵
فضای برداری، ۳۷۲
فلوئر، ۱۱۲
فیت، ۱۱۱
قانون برج، ۳۹۰
قرینه، ۷۱
قضایای سیلو، ۱۶۲

قضیه‌ی اساسی جبر، ۳۲۷، ۴۵۷
قضیه‌ی اساسی حساب، ۵۴
قضیه‌ی اساسی نظریه‌ی گالوا، ۴۵۴
قضیه‌ی اول سیلو، ۱۶۳
قضیه‌ی اول یکریختی، ۱۳۰، ۲۹۱، ۳۷۴
قضیه‌ی باقیمانده چینی، ۸۵، ۲۹۷
قضیه‌ی تجزیه‌ی اولیه، ۱۷۱
قضیه‌ی دوجمله‌ای، ۱۸، ۲۷۲
قضیه‌ی دوم سیلو، ۱۶۳
قضیه‌ی دوم یکریختی، ۱۳۱، ۲۹۱، ۳۷۵
قضیه‌ی سوم سیلو، ۱۶۵
قضیه‌ی سوم یکریختی، ۱۳۲، ۲۹۱، ۳۷۵
قضیه‌ی فرما، ۶۴، ۳۴۷
قضیه‌ی لاگرانژ، ۱۱۵
قضیه‌ی ودربُرن، ۴۳۹
قضیه‌ی ویلسون، ۶۵
قضیه‌ی ژاکوبسون، ۴۴۰
قضیه‌ی کرونکر، ۳۴۵، ۳۹۶
قضیه‌ی کُشی، ۱۲۶، ۱۲۷
قضیه‌ی کیلی، ۱۵۴
قوانین حذف، ۶۹
قوانین دمورگان، ۶
لامه، ۳۴۷
لاگرانژ، ۱۱۴، ۴۶۰
لم اقلیدس، ۵۳، ۳۳۶
لم زُرن، ۱۴، ۳۱۰
لم پروانه‌ای زاسنهاوس، ۲۰۹
لم پوانکاره، ۱۲۰
لم گاوس، ۳۳۰
لژاندر، ۵۴۰
لگاریتم گسسته، ۴۰۶
ماتریس امتحان توازن، ۴۷۹
ماتریس تک‌جمله‌ای، ۴۸۵
ماتریس جایگشتی، ۴۸۳
ماتریس مولد، ۴۷۸
ماتیو، ۱۱۱
مانده، ۵۳۹
ماکسیمال، ۱۳، ۹۵، ۲۰۱
ماکسیمال نرمال، ۱۰۹
ماکسیمم، ۱۳
مترجم، ۵۵۱
متریک، ۴۸۸
متعالی، ۳۸۷
متقارن، ۸
متناهی، ۲۲، ۶۸
متناهیاً تولید شده، ۹۶، ۳۷۳
مجزا، ۳، ۳۷
مجموعه، ۱
مجموعه‌ی اندیس‌دار، ۳
مجموعه‌ی توانی، ۴
مجموعه‌ی خارج قسمتی، ۱۰
مجموعه‌ی رده‌های مانده‌ای، ۵۹، ۶۸
مجموعه‌ی ساخت‌یافته، ۵۶۳
مجموعه‌ی مولد، ۹۶، ۲۲۰
مجموعه‌ی نقاط ثابت، ۱۵۲
محاوره‌ای، ۵۵۱
محتوای، ۳۵۸
محک آیزنشتاین، ۳۳۳
مدار، ۴۰، ۱۵۱
مدول آزاد، ۳۷۸
مدول دوری، ۳۷۳
مدول چپ، ۳۷۱
مرتب خطی، ۱۳
مرتبه، ۳۴، ۶۸، ۷۹، ۴۱۸
مرتبه‌ی یک چندجمله‌ای، ۴۱۸
مرکز، ۱۰۱، ۲۷۸
مرکز دوم ، ۱۹۵
مرکزساز، ۱۰۰، ۱۰۱، ۱۱۸، ۲۴۳
مزدوج، ۷۸، ۱۰۲، ۴۰۸
مزدوجی، ۱۵۸
مستقل خطی، ۱۷۷، ۳۷۷
مشخصاً ساده، ۱۰۸
مشخصه، ۱۰۴، ۲۷۶
مشخصه‌ی مثبت، ۲۷۷
مضرب مشترک، ۵۵
معادلات امتحان، ۴۸۰
معادله‌ی رده‌ای، ۱۱۸، ۱۵۹، ۲۵۰، ۴۳۹
معادله‌ی پِل، ۳۶۷
معکوس، ۶۸
مفسر، ۵۵۱
مقسوم‌علیه صفر، ۲۷۳
مقسوم‌علیه مشترک، ۵۱، ۳۴۸

موبیوس، ۴۱۷
موضعاً دوری ، ۱۰۰
موضعی سازی، ۳۱۳
مولد، ۸۲، ۹۲، ۲۲۴
مولفه، ۴
مولفه‌ی اولیه، ۱۷۱
مونوئید، ۶۸
مکمل، ۴
مکمل متعامد، ۴۷۹
مک‌ویلیامز، ۴۹۵
میدان، ۷۴، ۲۶۸
میدان اول، ۲۹۲، ۳۸۵
میدان تجزیه، ۳۹۶
میدان ثابت، ۴۴۹
میدان متناهی، ۳۴۵، ۴۰۴، ۴۰۵، ۴۰۷، ۴۳۹
میدان میانی، ۳۹۰
میدان کسرها، ۳۰۰، ۳۸۶
میدان گالوا، ۴۰۵
میلر، ۱۱۱
می‌نیمال، ۱۳
می‌نیمم، ۱۳
ناآبلی، ۳۵
نامانده، ۵۴۰
نامتناهی، ۲۲، ۶۸
نامساوی مثلث، ۴۸۸
نامولد، ۲۰۲
نرمال، ۱۰۴
نرمال‌ساز، ۱۰۱
نزدیکترین همسایه، ۴۸۹
نسبت به هم اول، ۵۳
نشانده شده، ۹۱
نما، ۸۰
نماد دو سطری، ۳۵
نماد لژاندر، ۵۴۰
نمایش جایگشتی، ۱۴۹
نمایش جایگشتی چپ منظم، ۱۵۴
نمایش گروه، ۲۲۴
نوع، ۱۷۵
نوفه، ۴۷۷
نُرم، ۳۶۵
نگاشت، ۱۸
نگاشت مقداریاب، ۳۲۱
نیم‌گروه ، ۶۸
هاکوئنگوم، ۵۳۰
هسته، ۹۱، ۱۱۳، ۲۸۳
هسته‌ی عمل، ۱۵۱
همدم، ۳۴۸، ۳۵۸
همریختی، ۸۵، ۳۷۴، ۴۲۶
همریختی (حلقه‌ای)، ۲۸۳
همریختی تصویر، ۸۶
همریختی جادهی، ۸۶
همریختی طبیعی، ۱۲۷، ۲۹۱، ۳۷۴
همریختی مقداریاب، ۳۲۱، ۳۸۷
همینگ، ۴۷۷
هم‌توان، ۲۲
هم‌مجموعه‌ی راست، ۱۱۷
هم‌مجموعه‌ی چپ، ۱۱۵
هولدر، ۱۱۰
وابسته‌ی خطی، ۱۷۷، ۳۷۸
وارون، ۱۰، ۳۴، ۶۱، ۶۸
وارون راست، ۲۵
وارون چپ، ۲۵
وارون‌پذیر، ۲۵، ۲۶۸
واژه، ۲۲۰
واژه‌ی تهی، ۲۲۰
واژه‌ی خطا، ۴۸۹
واژه‌ی کاهشی، ۲۲۰
ودربرن، ۲۷۵
وزن همینگ، ۴۸۷
ون دایک، ۲۲۴
پاد متقارن، ۱۲
پارادکس راسل، ۵
پاسکال، ۲۷۳
پایه، ۱۷۷، ۳۷۸
پراکنده، ۱۱۱
پوشا، ۱۹
پوچ‌توان، ۱۹۳، ۱۹۸، ۲۰۳، ۲۸۰
پِل، ۳۶۷
پیش تصویر، ۱۹
پیشروی هم‌مجموعه، ۴۹۲
پیمایش چپ، ۱۱۵

چادوری، ۵۳۰

چند دوری، ۲۱۴
چندجمله‌ای، ۳۱۵
چندجمله‌ای امتحان، ۵۱۰
چندجمله‌ای اولیه، ۳۵۸
چندجمله‌ای تحویل‌ناپذیر ، ۳۲۵
چندجمله‌ای تکین، ۳۱۶
چندجمله‌ای دایره‌بر، ۴۳۶
چندجمله‌ای ماتسون–سولومون، ۵۱۷
چندجمله‌ای متقارن، ۴۶۳
چندجمله‌ای مولد کد، ۵۰۸
چندجمله‌ای می‌نیمال، ۳۸۷
چولی، ۱۱۲
ژردان، ۱۱۰
ژردان–هولدر، ۲۱۱
کاملاً پایا، ۱۰۴
کانتور، ۲۵
کانوی، ۱۱۲
کد، ۴۷۷
کد BCH، ۵۳۰
کد امتحان توازن، ۴۸۲
کد تعمیم یافته، ۴۸۸
کد تکرار، ۴۸۱
کد خطی، ۴۷۸
کد خود– دوگان، ۴۸۷
کد خود– عمود، ۴۸۷
کد دوتایی، ۴۷۸
کد دوگان، ۴۷۹
کد ماکسیمال، ۵۱۸، ۵۱۹
کد همینگ، ۴۸۲
کد واژه، ۴۷۷
کد کامل، ۴۹۲
کد گذاری، ۴۷۷
کد گشایی، ۴۷۷
کد گشایی برلکمپ، ۵۳۸
کدهای دوری، ۵۰۷
کدهای معادل، ۴۸۴
کران BCH، ۵۳۱
کران همینگ، ۴۹۲
کسر، ۲۹۸
کلاس، ۶
کلاین، ۱۱۰
کلرو، ۱۹
کواترنیونی، ۷۲
کوراتوفسکی، ۱۴
کول، ۱۱۱
کومر، ۳۴۷
کوچک‌ترین زیرگروه، ۹۲، ۹۶
کُر، ۱۱۳
گالوا، ۱۱۰، ۴۶۰
گاوس، ۳۲۷، ۳۳۲، ۳۴۷
گروه، ۳۴، ۶۱
گروه آبلی آزاد، ۱۷۸
گروه آبلی متناهی، ۱۷۱
گروه آزاد، ۲۲۰، ۲۲۱
گروه خارج‌قسمتی، ۱۲۶
گروه خطی عمومی، ۷۵
گروه دوری، ۸۲، ۹۲
گروه دووجهی، ۷۴، ۹۷
گروه دووجهی نامتناهی، ۹۷
گروه ساده، ۱۰۷
گروه شبه دوری، ۷۳
گروه متقارن، ۳۵
گروه چهارگان، ۷۲
گروه کلاین، ۷۲
گروه‌های آبلی متناهیاً تولید شده، ۱۷۷
گورنشتاین، ۱۱۲
گولای، ۵۳۵، ۵۴۴

یابنده‌ی خطا، ۴۸۹
یکدار، ۲۶۸
یکریختی، ۸۵
یکه، ۲۶۸
یک‌به‌یک، ۱۹

Elmenents of asbract algebra

(with computer laboratories)

By

Bijan Taeri

Departmets of mathemaical sciences
Isfahan university of thechnology