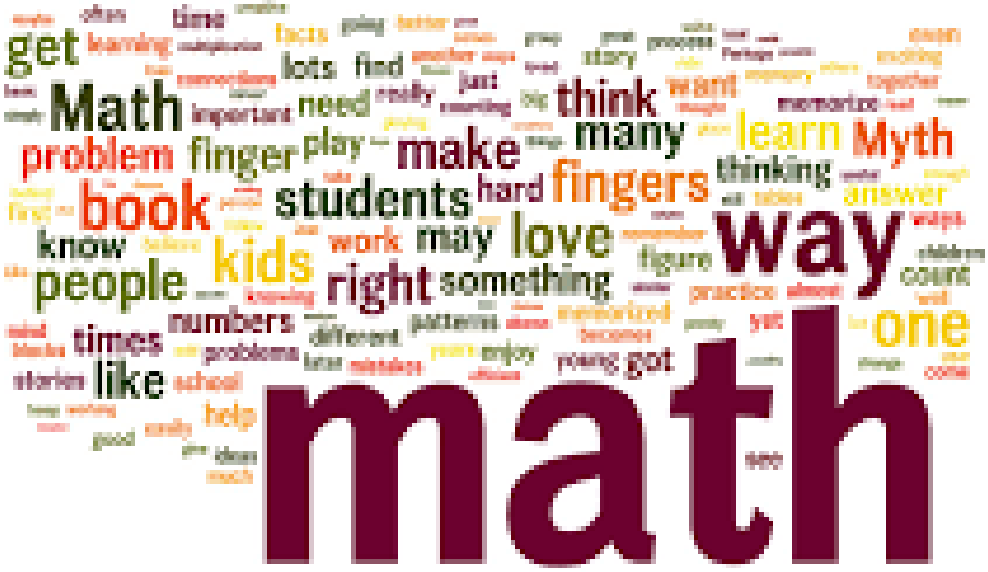
دانشگاه صنعتی اصفهان
دانشکده علوم ریاضی

مبانی جبر (دوره کارشناسی)

محمود بهبودی[1]



۳ بهمن ۱۳۹۷

[1] دانشیار دانشکده ریاضی دانشگاه صنعتی اصفهان

این نوشتار جهت استفاده دانشجویان کارشناسی دانشکده ریاضی دانشگاه صنعتی اصفهان آماده شده است و استفاده از آن برای دیگر موسسات آموزش عالی و دانشجویان بلامانع است.

باعث افتخار نویسنده است که نقدها، ایرادات و پیشنهادهای خود را به آدرس ایمیل زیر ارسال نمایید.

mbehbood@cc.iut.ac.ir

مقدمه

متن پیش‌رو حاصل چندین سال تجربه تدریس جبر اینجانب برای دانشجویان دوره کارشناسی دانشکده ریاضی دانشگاه صنعتی اصفهان است...

فهرست مطالب

فصل ۱

یادآوری برخی مفاهیم مقدماتی

در این فصل به صورت خلاصه مفاهیم پایه‌ای و از قبل دانسته شده را یادآوری خواهیم کرد. بیشتر حجم این بخش مربوط به درس مبانی ریاضی است. اگر دانشجویی احساس تسلط بر مبانی ریاضی دارد می‌تواند از این فصل چشم پوشی نماید و به صورت مستقیم وارد فصل دوم شود. باید این مطلب را ذکر کنیم که مطالب این فصل به صورت فهرست‌وار آمده‌اند و برای دیدن جزییات بیشتر و مثال‌ها به کتاب‌های مربوطه مراجعه نمایید.

۱.۱ مجموعه‌ها، رابطه‌ها، تابع‌ها، عدد اصلی یک مجموعه

از مفاهیم اساسی در ریاضیات مجموعه‌ها هستند. در این بخش ما وارد جزییات بعضا فلسفی نظریه مجموعه‌ها نمی‌شویم. همانطور که بارها گفته شده است مجموعه از مفاهیم تعریف ناپذیر است. این بخش را با تعریف زیر شروع می‌کنیم که بیان نادقیقی از مجموعه است.

تعریف ۱.۱.۱. *مجموعه دسته‌ای از اشیا است که این اشیا به صورت دقیق مشخص و تکراری نیستند. معمولا مجموعه‌ها با حروف انگلیسی بزرگ نمایش داده می‌شوند.*

نمادگذاری ۲.۱.۱. *اگر X یک مجموعه باشد و x عنصری از X باشد گوییم x متعلق به X است و با $x \in X$ نشان می‌دهیم. مجموعه که هیچ عضوی ندارد را مجموعه تهی گوییم و با $\emptyset$ نشان می‌دهیم. اگر x عضوی از X نباشد می‌نویسیم $x \notin X$.*

تعریف ۳.۱.۱. *فرض کنیم A و B دو مجموعه باشند. اگر هر عضو از A در B باشد آنگاه گوییم A زیرمجموعه B است و با $A \subseteq B$ نشان می‌دهیم. اگر $A \subseteq B$ و $B \subseteq A$ آنگاه گوییم A و B دو مجموعه یکسان هستند و با $A = B$ نشان می‌دهیم. اگر $A \subseteq B$ و B عضوی داشته باشد که در A نیست، آنگاه گوییم A زیرمجموعه سره B است و با $A \subsetneq B$ نمایش می‌دهیم.*

تعریف ۴.۱.۱. *فرض کنیم X و Y دو مجموعه باشند. مجموعه همه زوج‌های مرتب (x, y) را که $x \in X$ و $y \in Y$ است حاصل ضرب دکارتی دو مجموعه گوییم و با $A \times B$ نشان می‌دهیم. به عبارت دیگر*

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

تعریف ۵.۱.۱. *فرض کنیم A و B دو مجموعه باشند. به هر زیرمجموعه از $A \times B$ مانند R یک رابطه از A به B گوییم. مفهوم $(x, y) \in R$ را با xRy نشان می‌دهیم. اگر $A = B$ باشد آنگاه R را رابطه‌ایی روی A گوییم.*

تعریف ۶.۱.۱. *فرض کنیم X یک مجموعه و R رابطه‌ای روی X باشد. گوییم:*
(۱) R انعکاسی (بازتابی) است هرگاه برای هر $x \in X$ داشته باشیم xRx.
(۲) R متقارن است هرگاه برای هر $x, y \in X$ که xRy نتیجه شود yRx.
(۳) R پاد متقارن است هرگاه برای هر $x, y \in X$ که xRy و yRx نتیجه شود $x = y$.
(۴) R متعدی است هرگاه برای هر $x, y, z \in X$ که xRy و yRz نتیجه شود xRz.

تعریف ۷.۱.۱. *گوییم رابطه R روی X هم ارزی است هرگاه بازتابی، متقارن و متعدی باشد.*

تعریف ۸.۱.۱. *گوییم رابطه R روی X ترتیب جزیی است هرگاه بازتابی، پاد متقارن و متعدی باشد. به مجموعه X مرتب جزیی گوییم هرگاه رابطه R ترتیب جزیی باشد.*

تعریف ۹.۱.۱. *فرض کنیم رابطه R روی X ترتیب جزیی باشد. اگر برای هر $x, y \in X$ داشته باشیم xRy یا yRx آنگاه ترتیب جزیی را کلا مرتب یا زنجیر نامیم.*

تعریف ۱۰.۱.۱. *فرض کنیم R یک رابطه هم ارزی روی X باشد و $a \in X$. منظور از کلاس یا رده a تحت R که آن را با $[a]$ یا $\bar{a}$ نشان می‌دهیم، یعنی مجموعه زیر*

$$[a] = \bar{a} = \{x \in X \mid xRa\}.$$

زیرمجموعه A از X را یک کلاس یا رده هم ارزی R در X گوییم هرگاه $a \in X$ موجود باشد که $A = \bar{a}$. مجموعه همه کلاس‌های هم ارزی R در X را مجموعه خارج قسمتی نامیم و با X/R نشان می‌دهیم. به عبارت دیگر

$$X/R = \{A \subseteq X \mid A = \bar{a} \text{ که } a \text{ای در } X \text{باشد}\}.$$

تعریف ۱۱.۱.۱. *فرض کنیم X یک مجموعه باشد و $\mathcal{A}$ مجموعه‌ای باشد که عناصر آن زیرمجموعه‌های ناتهی از Xاند. اگر عنصرهای $\mathcal{A}$ دو به دو جدا از هم باشند و اجتماع آنها X باشد آنگاه به $\mathcal{A}$ یک افراز گوییم.*

قضیه ۱۲.۱.۱. *فرض کنیم R یک رابطه هم ارزی روی X باشد. در این صورت X/R یک افراز برای X است.*

قضیه ۱.۱.۱۳. *فرض کنیم $\mathcal{A}$ یک افراز برای X باشد. در این صورت رابطه هم ارزی R روی X چنان وجود دارد که $X/R = \mathcal{A}$.*

قضیه ۱.۱.۱۴. *فرض کنیم $\mathcal{A} = \{A_1, ..., A_n\}$ یک افراز برای X باشد. در این صورت $|X| = \sum_{i=1}^{n} |A_i|$.*

تعریف ۱.۱.۱۵. *فرض کنیم f یک رابطه از مجموعه A به مجموعه B باشد. گوییم رابطه f یک تابع است هرگاه برای هر $a \in A$ دقیقا یک $b \in B$ موجود باشد که xfy. اگر f تابعی از A به B باشد آنگاه می‌نویسیم $f : A \longrightarrow B$ یا $A \xrightarrow{f} B$. به A دامنه و به B برد گوییم. اگر xfy آنگاه می‌نویسیم $y = f(x)$ و به x پیش تصویر y و به y تصویر x گوییم.*

تعریف ۱.۱.۱۶. *به تابع $f : X \longrightarrow X$ که $f(x) = x$ تابع همانی گوییم و با id_X یا id نمایش می‌دهیم.*

تعریف ۱.۱.۱۷. *اگر $A \subseteq X$ باشد آنگاه به تابع $i : A \longrightarrow X$ که $i(a) = a$ تابع شمول گوییم.*

تعریف ۱.۱.۱۸. *فرض کنیم که $f : A \longrightarrow B$ یک تابع باشد. زیرمجموعه‌ای از B که تمام عناصر آن تصویری عنصر از A هستند تصویر f گویند و با $Im(f)$ نشان می‌دهند (دقت شود که برد تابع B است).*

نمادگذاری ۱.۱.۱۹. *منظور از نماد B^A یعنی مجموعه همه تابع‌ها از A به B.*

تذکر ۱.۱.۲۰. *اگر A مجموعه تهی باشد و B مجموعه دلخواه (حتی تهی) آنگاه فقط یک تابع از A به B وجود دارد. اما هیچ تابعی از B به A وجود ندارد (چرا؟).*

تعریف ۱.۱.۲۱. *تابع $f : A \longrightarrow B$ را یک‌به‌یک گوییم هرگاه برای هر $a, a' \in A$ که $f(a) = f(a')$ نتیجه شود که $a = a'$. گوییم f تابع پوشا است هرگاه برای هر $b \in B$ عنصر a در A وجود داشته باشد که $f(a) = b$. تابع f را تناظر گوییم هرگاه هم یک‌به‌یک و هم پوشا باشد. تناظرها را جایگشت نیز می‌نامیم.*

قضیه ۱.۱.۲۲. *فرض کنیم $f : X \longrightarrow Y$ یک تابع پوشا باشد. در این صورت*

$$f^{-1}(y) = \{x \in X \mid f(x) = y\}$$

یک افراز برای X است که در آن $y \in Y$.

قضیه ۱.۱.۲۳. *اگر X مجموعه متناهی و $f : X \longrightarrow X$ یک تابع یک‌به‌یک باشد آنگاه f تناظر است.*

تعریف ۱.۱.۲۴. *فرض کنیم $f : A \longrightarrow B$ و $g : B \longrightarrow C$ دو تابع باشند. در این صورت منظور از ترکیب f با g یعنی تابع $h : A \longrightarrow C$ که $h(x) = g(f(x))$. تابع h را با gof یا gf نیز نمایش می‌دهیم.*

قضیه ۱.۱.۲۵. *ترکیب تابع‌های (اگر مجاز باشد) شرکت پذیر است یعنی اگر $f : A \longrightarrow B$، $g : B \longrightarrow C$ و $h : C \longrightarrow D$ آنگاه $h(gf) = (hg)f$.*

قضیه ۱.۱.۲۶. *ترکیب توابع یک‌به‌یک (پوشا) یک تابع یک‌به‌یک (پوشا) است.*

تعریف ۱.۱.۲۷. *گوییم تابع $f : A \longrightarrow B$ دارای وارون است (وارونپذیر است) هرگاه تابع $g : B \longrightarrow A$ موجود باشد که $fg = id_B$ و $gf = id_A$. تابع g را با f^{-1} نشان می‌دهیم.*

قضیه ۱.۱.۲۸. *تابع f وارونپذیر است اگر و تنها اگر f تناظر باشد.*

تعریف ۱.۱.۲۹. *گوییم دو مجموعه X و Y همتوان هستند هرگاه یک تناظر بین X و Y موجود باشد. این مطلب را با $X \cong Y$ نشان می‌دهیم.*

تعریف ۱.۱.۳۰. *گوییم دو مجموعه X و Y دارای عدد اصلی یکسان (کاردینالیتی یکسان) هستند هرگاه همتوان باشند. عدد اصلی مجموعه X را با $|X|$ نشان می‌دهیم.*

نمادگذاری ۱.۱.۳۱. *عدد اصلی $\mathbb{N}$ را با $\aleph_0$ نمایش می‌دهیم (بخوانید "الف صفر").*

تعریف ۱.۱.۳۲. *گوییم مجموعه ناتهی X تعداد متناهی عضو دارد هرگاه عدد طبیعی n موجود باشد که یک تناظر بین X و $\{1, ..., n\}$ وجود داشته باشد. مجموعه‌ای که متناهی نباشد را نامتناهی گوییم. گوییم مجموعه X شمارا (شمارش پذیر) است هرگاه $|X| = \aleph_0$.*

قضیه ۱.۱.۳۳. *عدد اصلی $\mathbb{Z}$ و $\mathbb{Q}$ برابر $\aleph_0$ است.*

قضیه ۱.۱.۳۴. *هر زیرمجموعه یک مجموعه شمارا، متناهی یا شمارا است.*

قضیه ۱.۱.۳۵. *حاصل ضرب دکارتی و اجتماع مجموعه‌های شمارا، شمارا هستند.*

تعریف ۱.۱.۳۶. *مجموعه‌ای که شمارا نباشد را ناشمارا (شمارش ناپذیر) گوییم.*

قضیه ۱.۱.۳۷. *$\mathbb{R}$ ناشمارا است و $|\mathbb{R}| = 2^{\aleph_0}$.*

تعریف ۱.۱.۳۸. *فرض کنیم X و Y دو مجموعه باشند. گوییم $|X| \leq |Y|$ هرگاه یک تابع یک‌به‌یک از X به Y موجود باشد. اگر تابعی یک‌به‌یک از X به Y موجود باشد که پوشا نیست می‌نویسیم $|X| < |Y|$.*

قضیه ۱.۱.۳۹. *(شرودر- برنشتاین) اگر برای دو مجموعه X و Y داشته باشیم $|X| \leq |Y|$ و $|Y| \leq |X|$ آنگاه $|X| = |Y|$.*

قضیه ۱.۱.۴۰. *اگر $\mathbb{P}(X)$ نمایش مجموعه توانی مجموعه X باشد (مجموعه همه زیرمجموعه‌های X) آنگاه $|X| < |\mathbb{P}(X)|$.*

قضیه ۱.۱.۴۱. *عدد اصلی مجموعه B^A برابر است با $|B|^{|A|}$.*

در زیر تعریفی نادقیق از مفهوم خانواده را ارائه می‌کنیم.

تعریف ۱.۱.۴۲. *خانواده دسته‌ای از اشیا است که این اشیا به صورت دقیق مشخص هستند و یک شی می‌تواند تکرار شود.*

تعریف ۱.۱.۴۳. *فرض کنیم X یک مجموعه باشد. هر تابع $f : \mathbb{N} \longrightarrow X$ را یک دنباله از اعضای X گوییم. معمولا $f(n)$ را با f_n نشان می‌دهیم. یک دنباله را گاهی به صورت $(f_1, f_2, ...)$ یا $\{f_i\}_{i=1}^{\infty}$ نشان می‌دهیم.*

تعریف ۱.۱.۴۴. *فرض کنیم X و I دو مجموعه باشند. هر تابع $f : I \longrightarrow X$ را یک خانواده از عناصر X گوییم و با $(f_i)_{i\in I}$ یا $\{f_i \mid i \in I\}$ نشان می‌دهیم. به مجموعه I مجموعه اندیس گذار گوییم.*

تعریف ۱.۱.۴۵. *فرض کنیم $\{A_i\}_{i\in I}$ یک خانواده اندیس گذاری شده با I از مجموعه‌ها باشد. حاصل ضرب دکارتی $\{A_i\}_{i\in I}$ را این چنین تعریف می‌کنیم*

$$\prod_{i\in I} A_i = \{f : I \longrightarrow \bigcup_{i\in I} A_i \mid \forall i \in I,\ \ f(i) \in A_i\}.$$

در حالت خاص اگر برای هر $i \in I$، $A_i = A$ حاصل ضرب دکارتی $\prod_{i\in I} A_i$ همان A^I است. اگر I مجموعه متناهی باشد مانند $I = \{1, ..., n\}$ آنگاه داریم

$$\prod_{i\in I} A_i = \prod_{i=1}^{n} A_i = A_1 \times ... \times A_n = \{(a_1, ..., a_n) \mid a_i \in A_i\}.$$

اصل انتخاب را در قالب تعریف زیر بیان می‌کنیم. اصل انتخاب صورت‌های بسیار زیادی دارد که در زیر ساده‌ترین آن را مشاهده می‌کنید.

تعریف ۱.۱.۴۶. *(اصل انتخاب) حاصل ضرب دکارتی خانواده‌ای ناتهی از مجموعه‌های ناتهی، ناتهی است.*

تعریف ۴۷.۱.۱. *فرض کنیم X یک مجموعه مرتب جزیی با رابطه R و $A \subseteq X$ باشد.*
(الف) گوییم عنصر $y \in X$ کران بالا برای A است هرگاه برای هر $a \in A$ داشته باشیم aRy.
(ب) گوییم عنصر $y \in X$ کران پایین برای A است هرگاه برای هر $a \in A$ داشته باشیم yRa.
(ج) گوییم عنصر $y \in X$ ماکسیمال است هرگاه برای هر $x \in X$ که xRy نتیجه شود $x = y$.
(د) گوییم عنصر $y \in X$ مینیمال است هرگاه برای هر $x \in X$ که yRx نتیجه شود $x = y$.

تعریف ۴۸.۱.۱. *گوییم مجموعه کلا مرتب X خوشترتیب است هرگاه هر زیرمجموعه ناتهی از X عنصر مینیمال داشته باشد.*

قضیه ۴۹.۱.۱. *(لم زرن) اگر A (مجموعه ناتهی) یک مجموعه مرتب جزیی باشد، به طوری که هر زیرمجموعه کلا مرتب (زنجیر) آن، دارای کران بالا (در A) باشد، آنگاه A دارای عضو ماکسیمال است.*

قضیه ۵۰.۱.۱. *(اصل خوشترتیبی) هر مجموعه خوشترتیب شدنی است.*

۲.۱ اعداد طبیعی، صحیح، پیمانه‌ای، گویا، حقیقی و مختلط

در این بخش کمی راجع به اعداد صحبت خواهیم کرد و مشابه بخش قبل وارد جزییات نمی‌شویم. با تعریف اعداد طبیعی و صحیح در درس مبانی ریاضی آشنا شده‌اید و متوجه شده‌اید که چگونه با اصول پئانو اعداد طبیعی ساخته می‌شوند و با کمک رابطه هم ارزی اعداد صحیح ایجاد می‌شوند و سپس اعداد گویا از روی اعداد صحیح ساخته می‌شوند. در درس مبانی آنالیز یا مبانی ریاضی با نحوه ساخته شدن اعداد حقیقی آشنا شده‌اید. برای راحتی ما نمادهای را برای اعداد در زیر معرفی می‌کنیم و کمی قضیه‌های کاربردی و مورد استفاده خودمان را معرفی می‌کنیم.

نمادگذاری ۱.۲.۱. *مجموعه اعداد طبیعی، حسابی، صحیح، گویا و حقیقی را به ترتیب با* $\mathbb{N}$، $\mathbb{W}$، $\mathbb{Z}$، $\mathbb{Q}$ و $\mathbb{R}$ *نمایش می‌دهیم.*

قضیه ۲.۲.۱. *(استقرای ضعیف) فرض کنیم* S *زیرمجموعه* $\mathbb{N}$ *باشد که* $1 \in S$ *و اگر* $n \in S$ *آنگاه* $n+1 \in S$*. در این صورت* $S = \mathbb{N}$*.*

قضیه ۳.۲.۱. *(استقرای قوی) فرض کنیم* S *زیرمجموعه* $\mathbb{N}$ *که* $1 \in S$ *و اگر* $n \in S$ *آنگاه برای هر عدد صحیح مثبت* m *کمتر از* n*،* $m \in S$*. در این صورت* $S = \mathbb{N}$*.*

تعریف ۴.۲.۱. *گوییم عدد صحیح* b *یک مقسوم علیه عدد صحیح* a *است یا* a *مضربی از* b *است هرگاه عدد صحیح* c *موجود باشد که* $a = bc$*. گاهی این مفهوم را با* $b|a$ *نمایش می‌دهیم. اگر چنین* c*ای موجود نباشد آنگاه می‌نویسیم* $b \nmid a$*.*

تعریف ۵.۲.۱. *عدد صحیح* p *را اول گوییم هرگاه مخالف با* 1 *و* -1 *باشد و تنها مقسوم علیه‌های آن* 1*،* -1*،* p *و* $-p$ *باشند.*

قضیه ۶.۲.۱. *هر عدد صحیح مثبت یا* 1 *است یا می‌توان آن را به یک و تنها یک روش به صورت حاصل ضربی از اعداد اول مثبت نوشت.*

قضیه ۷.۲.۱. *(الگوریتم تقسیم) فرض کنیم* $a, b \in \mathbb{Z}$ *و* $b > 0$*. در این صورت اعداد صحیح یکتایی مانند* q *و* r *وجود دارند که* $a = bq + r$ *و* $0 \leq r < b$*. به* r *باقیمانده و به* q *را خارج قسمت نامیم.*

تعریف ۸.۲.۱. *گوییم عدد صحیح* d *بزرگترین مقسوم علیه مشترک دو عدد صحیح* a *و* b *است هرگاه* $d|a$ *و* $d|b$ *و اگر* $c|a$ *و* $c|b$ *آنگاه* $c|d$*. این مفهوم را با* $(a, b) = d$ *نشان می‌دهیم.*

تعریف ۹.۲.۱. *دو عدد صحیح* a *و* b *را نسبت به هم اول گوییم هرگاه* $(a, b) = 1$*.*

قضیه زیر به قضیه بزو[1] معروف است.

[1] Bezout

قضیه ۱.۲.۱۰. (بزو) برای هر دو عدد صحیح a و b با شرط $(a,b)=d$ اعداد صحیح r و s چنان وجود دارند که $ar+bs=d$.

قضیه ۱.۲.۱۱. اگر p عدد اول باشد که برای اعداد صحیح a و b داشته باشیم $p|ab$ آنگاه $p|a$ یا $p|b$.

تعریف ۱.۲.۱۲. مجموعه اعداد مختلط را مجموعه $\mathbb{R}\times\mathbb{R}$ با جمع و ضرب زیر تعریف می‌کنیم

$$(a,b)+(x,y)=(a+x,b+y) \qquad (a,b).(x,y)=(ax-by,ay+bx)$$

اعداد مختلط را با $\mathbb{C}$ نمایش می‌دهیم. به اعضای $\mathbb{C}$ اعداد مختلط گوییم

تذکر ۱.۲.۱۳. برای هر $(x,y)\in\mathbb{C}$ داریم که $(x,y).(۱,۰)=(x,y)$. یعنی $(۱,۰)$ مانند عدد حقیقی ۱ در اعداد حقیقی است. همچنین اگر فرض کنیم $i=(۰,۱)$ و $(a,۰)$ را با a یکی بگیریم آنگاه چون $b(۰,۱)+(۰,۱)=(a,b)$ به نمایش $a+ib$ برای عدد مختلط (a,b) خواهیم رسید. به علاوه $i^۲=i.i=(-۱,۰)$ و در نتیجه طبق قرار داد ما $i^۲=-۱$. عضو $(۰,۰)$ را با ۰ نشان می‌دهیم که مانند عدد حقیقی ۰ در اعداد حقیقی است.

تعریف ۱.۲.۱۴. در عدد مختلط $a+ib$ به a بخش حقیقی و به b بخش موهمی گوییم.

قضیه ۱.۲.۱۵. عدد مختلط ناصفر $z=a+ib$ دارای وارون ضربی $z^{-۱}=\frac{a}{a^۲+b^۲}+i(\frac{b}{a^۲+b^۲})$ است یعنی داریم $zz^{-۱}=z^{-۱}z=۱$.

تذکر ۱.۲.۱۶. همواره داریم

$$\mathbb{N}\subseteq\mathbb{W}\subseteq\mathbb{Z}\subseteq\mathbb{Q}\subseteq\mathbb{R}\subseteq\mathbb{C}.$$

تعریف ۱.۲.۱۷. به مجموعه اعداد مختلط که به صورت $a+ib$ هستند و $a,b\in\mathbb{Z}$ اعداد گوسی گوییم و با $\mathbb{Z}[i]$ نمایش می‌دهیم.

نمادگذاری ۱.۲.۱۸. برای اعداد صحیح k، t و زیرمجموعه X از اعداد مختلط، منظور از $kX+t$ یعنی مجموعه $\{kx+t\mid x\in X\}$.

تعریف ۱.۲.۱۹. *عدد طبیعی n را در نظر می‌گیریم. رابطه*

$$a, b \in \mathbb{Z}: \quad aRb \Leftrightarrow n|a-b$$

هم ارزی است. حال داریم

$$\bar{۰} = [۰] = \{a \in \mathbb{Z} \mid aR۰\} = \{a \in \mathbb{Z} \mid n|a\} = n\mathbb{Z}$$

یعنی کلاس ۰ همه مضرب‌های صحیح عدد n است یا به عبارتی تمام اعداد صحیح که به n باقیمانده ۰ دارند. اما

$$\bar{۱} = [۱] = \{a \in \mathbb{Z} \mid aR۱\} = \{a \in \mathbb{Z} \mid n|a-۱\} = n\mathbb{Z}+۱$$

یعنی کلاس ۱ تمام اعداد صحیح که به n باقیمانده ۱ دارند. با ادامه این روند تا $n-۱$ به n تا کلاس دست خواهیم یافت. یعنی مجموعه‌ای به شکل زیر

$$\{n\mathbb{Z}, n\mathbb{Z}+۱, n\mathbb{Z}+۲, ..., n\mathbb{Z}+(n-۱)\} = \{\bar{۰}, \bar{۱}, ..., \overline{n-۱}\}.$$

به مجموعه بالا اعداد پیمانه n گوییم و با $\mathbb{Z}_n$ نشان می‌دهیم.

تعریف ۲.۲.۱. *برای اعداد پیمانه‌ای جمع و ضرب به صورت زیر تعریف می‌شود.*

$$\bar{x}+\bar{y} = \overline{x+y} \qquad \bar{x}\cdot\bar{y} = \overline{xy}$$

نمادگذاری ۱.۲.۲۱. *فرض کنیم n عدد طبیعی و a، b اعداد صحیح باشند. گاهی به جای $n|a-b$ از نماد $a \overset{n}{\equiv} b$ استفاده می‌کنیم.*

قضیه ۱.۲.۲۲. *(قضیه ویلسون) برای هر عدد اول داریم $(p-۱)! \overset{p}{\equiv} -۱$.*

تعریف ۱.۲.۲۳. *تابع فی اویلر یا φ تابعی است که تعداد اعداد طبیعی کوچکتر از n که نسبت به n اول‌اند را می‌شمارد. اگر n یک عدد طبیعی مثبت باشد، آنگاه $\varphi(n)$ برابر است با تعداد اعداد طبیعی k در بازه ۱ تا n به طوری‌که $(k,n) = ۱$.*

قضیه ۱.۲.۲۴. *(قضیه اویلر- فرما) فرض کنیم n عدد صحیح مثبت و $\varphi(n)$ تابع اویلرباشد. در این صورت برای هر عدد صحیح a که $(a,n) = ۱$ داریم $a^{\varphi(n)} \overset{n}{\equiv} ۱$.*

قضیه ۱.۲.۲۵. *(قضیه کوچک فرما) برای هر $a, p \in \mathbb{Z}$ که p عددی اول است، داریم $a^p \overset{p}{\equiv} a$.*

۳.۱ ماتریس‌ها

در مقطع کارشناسی ماتریس‌ها بیشتر در درس جبر خطی مطالعه می‌شوند. اما ماتریس‌ها ابزار بسیار خوبی هستند تا بتوانیم مثال‌های متنوعی را در درس مبانی جبر فراهم کنیم. بنابراین مختصری در این بخش راجع به ماتریس‌ها خواهیم گفت.

تعریف ۱.۳.۱. *فرض کنیم m و n دو عدد طبیعی و X یک مجموعه باشد. هر تابع*

$$f : \{۱, ۲, ..., m\} \times \{۱, ۲, ..., n\} \longrightarrow X$$

را یک ماتریس $m \times n$ روی X گوییم. به $f((i,j))$ درایه گوییم که $i \in \{۱, ۲, ..., m\}$ و $j \in \{۱, ۲, ..., n\}$. برای راحتی آن را با f_{ij} نشان می‌دهیم. برای نمایشی بهتر از شکل زیر بهره می‌بریم.

$$\begin{pmatrix} f_{۱۱} & f_{۱۲} & \cdots & f_{۱n} \\ f_{۲۱} & f_{۲۲} & \cdots & f_{۲n} \\ & & \vdots & \\ f_{m۱} & f_{m۲} & \cdots & f_{mn} \end{pmatrix}_{m \times n}$$

همچنین یک ماتریس را گاهی با (f_{ij}) نمایش می‌دهیم.

تذکر ۲.۳.۱. *معمولا ماتریس‌ها را با حروف بزرگ انگلیسی نمایش می‌دهیم و مجموعه X را یکی از مجموعه‌های شناخته شده $\mathbb{N}$، $\mathbb{Z}$، $\mathbb{Q}$، $\mathbb{R}$ و یا $\mathbb{C}$ در نظر می‌گیریم.*

نمادگذاری ۳.۳.۱. *به ماتریس*

$$O = \begin{pmatrix} ۰ & ۰ & \cdots & ۰ \\ ۰ & ۰ & \cdots & ۰ \\ & & \vdots & \\ ۰ & ۰ & \cdots & ۰ \end{pmatrix}_{m \times n}$$

ماتریس صفر گوییم و اگر $m = n$ باشد آنگاه به ماتریس

$$I = \begin{pmatrix} ۱ & ۰ & \cdots & ۰ \\ ۰ & ۱ & \cdots & ۰ \\ & & \vdots & \\ ۰ & ۰ & \cdots & ۱ \end{pmatrix}_{n \times n}$$

ماتریس همانی گوییم که در آن $۰ \in \mathbb{C}$ و $۱ \in \mathbb{C}$.

تعریف ۴.۳.۱. *اگر $m = n$ باشد آنگاه به ماتریس مربعی گوییم و n را مرتبه ماتریس نامیم.*

نمادگذاری ۱.۳.۵. *منظور از نماد $M_{m\times n}(X)$ یعنی مجموعه تمام ماتریس‌های $m\times n$ با درایه‌های از X. اگر $m=n$ باشد از نماد $M_n(X)$ استفاده می‌کنیم.*

تعریف ۱.۳.۶. *اگر $A=(a_{ij})\in M_{m\times n}(\mathbb{C})$ و $B=(b_{ij})\in M_{m\times n}(\mathbb{C})$ آنگاه جمع دو ماتریس به صورت زیر تعریف می‌شود*

$$A+B=(a_{ij}+b_{ij}).$$

تعریف ۱.۳.۷. *اگر $A=(a_{ij})\in M_{m\times n}(\mathbb{C})$ و $B=(b_{ij})\in M_{n\times l}(\mathbb{C})$ آنگاه ضرب دو ماتریس به صورت زیر تعریف می‌شود*

$$C=AB=\begin{pmatrix} c_{11} & c_{12} & \cdots & c_{1l} \\ c_{21} & c_{22} & \cdots & c_{2l} \\ & & \vdots & \\ c_{m1} & c_{m2} & \cdots & c_{ml} \end{pmatrix}$$

که در آن $c_{ij}=\sum_{k=1}^{n} a_{ik}b_{kj}$.

تعریف ۱.۳.۸. *فرض کنیم A یک ماتریس $m\times n$ باشد. منظور از سطر iام یعنی ماتریس $1\times n$ زیر*

$$\begin{pmatrix} a_{i1} & a_{i2} & \cdots & a_{in} \end{pmatrix}$$

و منظور از ستون jام یعنی ماتریس $j\times 1$ زیر

$$\begin{pmatrix} a_{1j} \\ a_{2j} \\ \vdots \\ a_{mj} \end{pmatrix}$$

تعریف ۱.۳.۹. *فرض کنیم A یک ماتریس $m\times n$ باشد. در این صورت به ماتریسی که از حذف سطر iام و ستون jام به دست می‌آید ماتریس کهاد یا خُرد گوییم و با $M_i^j(A)$ نمایش می‌دهیم. اگر بیم ابهام برای ماتریس A نباشد فقط از نماد M_i^j استفاده می‌کنیم.*

تعریف ۱.۳.۱۰. *دترمینان یک ماتریس مربعی از مرتبه ۲ با درایه‌های از $\mathbb{C}$ به صورت زیر است*

$$det \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} = a_{11}a_{22} - a_{12}a_{21}$$

و دترمینان یک ماتریس مربعی از مرتبه ۳ با درایه‌های از $\mathbb{C}$ به صورت زیر است

$$det \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} =$$
$$a_{11} det \begin{pmatrix} a_{22} & a_{23} \\ a_{32} & a_{33} \end{pmatrix} + a_{12} det \begin{pmatrix} a_{21} & a_{23} \\ a_{31} & a_{33} \end{pmatrix} + a_{13} det \begin{pmatrix} a_{21} & a_{22} \\ a_{31} & a_{32} \end{pmatrix} =$$
$$a_{11} det\ M_1^1 + a_{12} det\ M_1^2 + a_{13} det\ M_1^3$$

و با روند استقرایی دترمینان یک ماتریس مربعی از مرتبه n با درایه‌های از $\mathbb{C}$ به صورت زیر است

$$det \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ & & \vdots & \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix} = a_{11} det\ M_1^1 + a_{12} det\ M_1^2 + ... + a_{1n} det\ M_1^n$$

قضیه ۱.۳.۱۱. *برای هر دو ماتریس مربعی A و B داریم $det\ AB = det\ A\ det\ B$.*

تعریف ۱.۳.۱۲. *گوییم ماتریس مربعی A وارون پذیر است هرگاه ماتریس مربعی B موجود باشد که $AB = BA = I$. ماتریس مربعی B را با A^{-1} نمایش می‌دهیم.*

قضیه ۱.۳.۱۳. *ماتریس مربعی A وارون پذیر است اگر و تنها اگر $det\ A$ مخالف با عدد صفر باشد.*

تعریف ۱.۳.۱۴. *فرض کنیم A یک ماتریس $n \times m$ باشد. ترانهاده A ماتریسی است $m \times n$ مانند B که از قرار دادن درایه iام jام از A در مکان jام iام ماتریس B به دست می‌آید.*

فصل ۲

آشنایی با نظریه گروه‌ها

در جبر نوین نظریه گروه به مطالعه موجودات ریاضی می‌پردازد که به گروه‌ها معروف هستند. مفهوم گروه بخش مرکزی جبر نوین است و سایر موجودات جبر نوین مانند حلقه‌ها و فضاهای برداری بر پایه همین مفهوم گروه شکل گرفته‌اند. مطالعه گروه‌ها سایر شاخه‌های ریاضی را نیز تحت تاثیر قرار می‌دهد و کاربردهای آن در بسیار از بخش‌های ریاضی دیده می‌شود. به طور ویژه، گروه‌ها در جبر نوین جایگاه خاصی دارند که مهمترین آنها می‌توان به گروه‌های خطی و گروه لی[۱] اشاره کرد. در این فصل هدف ما آشنایی مختصر با نظریه گروه است و در درس جبر ۱ می‌توانید با مطالب تکمیلی از نظریه گروه آشنا شوید و در مقاطع بالاتر مطالب پیشرفته را بیاموزید.

۱.۲ عمل دوتایی

در این بخش شما را با مفهوم عمل دوتایی آشنا می‌کنیم و سپس منظور خود را از ساختار ریاضی بیان می‌کنیم. کار را با تعریف زیر آغاز می‌کنیم.

تعریف ۱.۱.۲. *فرض کنیم S یک مجموعه ناتهی باشد. هر تابع*

$$* : S \times S \longrightarrow S$$

را یک عمل دوتایی روی مجموعه S گوییم. در حقیقت عمل دوتایی روی زوج‌های مرتب از عنصرهای S دقیقا یک عنصر از S را نسبت می‌دهد. عمل دوتایی را به جای نماد متداول تابع مانند f، g و ... با $*$، $\cdot$ و یا o نمایش می‌دهیم.

مثال ۲.۱.۲. *فرض کنیم $S = \mathbb{Z}$ و $*$ را عمل جمع، $+$، در نظر می‌گیریم. واضح است که $+$ یک عمل دوتایی روی $\mathbb{Z}$ است. در واقع $+$ دو عدد صحیح را می‌گیرید و جمع عادی را روی آنها پیاده می‌کند.*

[۱] Lie

مثال ۳.۱.۲. *فرض کنیم $S = \mathbb{R}$ و $*$ را عمل ضرب، $\cdot$، در نظر می‌گیریم. واضح است که $\cdot$ یک عمل دوتایی روی $\mathbb{R}$ است. در واقع $\cdot$ دو عدد حقیقی را می‌گیرید و ضرب عادی را روی آنها پیاده می‌کند.*

مثال ۴.۱.۲. *فرض کنیم $S = M_n(\mathbb{R})$ و $*$ را عمل ضرب، $\cdot$، در نظر می‌گیریم. واضح است که $\cdot$ یک عمل دوتایی روی ماتریس‌ها است. در واقع $\cdot$ دو عدد ماتریس را می‌گیرید و ضرب عادی ماتریسی را روی آنها پیاده می‌کند.*

مثال ۵.۱.۲. *فرض کنیم S بازه $[-۱, ۰]$ باشد. در این صورت $* : S \times S \longrightarrow S$ با ضابطه $a * b = |a - b|$ عمل نیست. زیرا اگر قرار دهیم $a = ۰$ و $b = -۱$ آنگاه $a * b = ۱ \notin S$. پس $*$ تابع نیست.*

مثال ۶.۱.۲. *اگر X یک مجموعه باشد، $\mathbb{P}(X)$ را در نظر می‌گیریم. در این صورت اجتماع، اشتراک، تفاضل عمل‌های دوتایی روی $\mathbb{P}(X)$ هستند.*

مثال ۷.۱.۲. *مجموعه همه توابع روی مجموعه X را در نظر می‌گیریم یعنی مجموعه X^X. در این صورت ترکیب توابع یک عمل دوتایی روی X^X است.*

گزاره ۸.۱.۲. *اگر $|S| = n$ باشد آنگاه $n^{(n^۲)}$ عمل دوتایی روی S وجود دارد.*

اثبات. فرض کنیم $* : S \times S \longrightarrow S$ یک عمل دوتایی باشد. می‌دانیم که هر عمل دوتایی یک تابع است پس برای تعداد عمل‌هایی دوتایی در واقع می‌خواهیم تعداد توابع از $S \times S$ به S را به دست آوریم. اکنون واضح است که دامنه $*$، $n^۲ = n \times n$ عضو دارد و برد آن تعداد n عضو. حال طبق قضیه ۴۱.۱.۱، تعداد چنین $*$هایی برابر است با $n^{(n^۲)}$. □

تعریف ۹.۱.۲. *گوییم عمل دوتایی $* : S \times S \longrightarrow S$ روی مجموعه S:*
(الف) جابجایی است هرگاه برای هر $s, s' \in S$ داشته باشیم $s * s' = s' * s$.
(ب) شرکت پذیر است هرگاه برای هر $s, s', s'' \in S$ داشته باشیم $s*(s'*s'') = (s*s')*s''$.

مثال ۱۰.۱.۲. *عمل دوتایی $+$ روی $\mathbb{Z}$ یک عمل جابجایی و شرکت پذیر است.*

مثال ۱۱.۱.۲. *عمل دوتایی اجتماع روی $\mathbb{P}(X)$ یک عمل جابجایی و شرکت پذیر است.*

مثال ۱۲.۱.۲. *عمل ضرب ماتریسی روی $M_۲(\mathbb{R})$ جابجایی نیست. زیرا*

$$A = \begin{pmatrix} ۱ & ۰ \\ ۲ & ۳ \end{pmatrix}, \quad B = \begin{pmatrix} -۱ & ۰ \\ ۲ & -۱ \end{pmatrix} : \qquad A.B \neq B.A$$

مثال ۱۳.۱.۲. *فرض کنیم S برابر با بازه $[۰, ۴]$ باشد. در این صورت $* : S \times S \longrightarrow S$ با ضابطه $a * b = |a - b|$ یک عمل دوتایی است (چرا؟) که شرکت پذیر نیست. زیرا*

$$۱ * (۲ * ۳) = ۱ * (|۲ - ۳|) = ۱ * ۱ = ۰ \neq (۱ * ۲) * ۳ = (|۱ - ۲|) * ۳ = ۱ * ۳ = |۱ - ۳| = ۲.$$

تذکر ۱۴.۱.۲. *فرض کنیم $*$ عمل دوتایی شرکت پذیر روی S باشد. شرکت پذیری اجازه می‌دهد که در انجام عمل دوتایی روی سه عنصر از S قرار گرفتن پرانتز برای ما مهم نباشد و حاصل تغییری نکند. اما این سوال طبیعی است که اگر تعداد بیشتر از سه عنصر شود، باز هم می‌توان پرانتزها را هرگونه که بخواهیم قرار دهیم؟ مثلا برای ۴ عنصر a، b، c و d از S حالت‌های زیر را داریم*

$$a*((b*c)*d) \quad (a*b)*(c*d) \quad ((a*b)*c)*d \quad (a*(b*c))*d \quad (a*(b*(c*d))$$

در ادامه می‌خواهیم نشان دهیم که اگر $*$ شرکت پذیر باشد جایگاه پرانتز در حاصل نهایی تفاوتی ایجاد نمی‌کند. برای این کار از حالت‌های پرانتز گذاری یک حالت که راحتر در ذهن می‌نشیند را در نظر می‌گیریم (حالت ۳ مثال بالا) و به آن استانده می‌گوییم و سپس نشان می‌دهیم باقی حالت‌ها با همین حالت استانده یکی است.

تعریف ۱۵.۱.۲. *فرض کنیم $*$ یک عمل دوتایی روی S باشد و a_1، ...، a_n عناصری از S. عمل استانده a_iها را با استقرا چنین تعریف می‌کنیم*

$$\prod_{i=1}^{1} a_i = a, \quad \prod_{i=1}^{2} a_i = (a_1 * a_2), \quad \prod_{i=1}^{3} a_i = (\prod_{i=1}^{2} a_i) * a_3, ..., \prod_{i=1}^{n} a_i = (\prod_{i=1}^{n-1} a_i) * a_n.$$

مثال ۱۶.۱.۲. *عمل استانده ۵ عنصر a_1، a_2، a_3، a_4 و a_5 برابر است با*

$$\prod_{i=1}^{5} a_i = (((a_1 * a_2) * a_3) * a_4) * a_5.$$

اکنون قضیه زیر را داریم.

قضیه ۱۷.۱.۲. *اگر عمل دوتایی $*$ روی S شرکت پذیر باشد و a_1، ...، a_n عناصری از S آنگاه هر نوع انجام عمل دوتایی با معنی برای a_iها برابر با عمل استانده a_iها است.*

اثبات. حکم را با استقرای قوی روی n اثبات می‌کنیم. اگر $n = 1$ باشد که چیزی برای اثبات نداریم. فرض کنیم $n > 1$ و برای هر $m < n$ حکم صحیح باشد. می‌خواهیم حکم را برای n اثبات کنیم. فرض کنیم T نمایش عمل دوتایی با معنی باشد. اگر $T(a_1, ..., a_n)$ یک عمل دوتایی با معنی از a_iها باشد آنگاه $1 \leq k \leq n$ چنان وجود دارد که $T(a_1, ..., a_n) = T(a_1, ..., a_k) * T(a_{k+1}, ..., a_n)$. طبق فرض استقرار داریم

$$T(a_1, ..., a_n) = T(a_1, ..., a_k) * T(a_{k+1}, ..., a_n) = (\prod_{i=1}^{k} a_i) * (\prod_{j=k+1}^{n} a_j).$$

دو حالت ممکن است رخ دهد.
حالت اول. $k = n - 1$. پس

$$T(a_1, ..., a_n) = T(a_1, ..., a_{n-1}) * T(a_n) = (\prod_{i=1}^{n-1} a_i) * a_n = \prod_{i=1}^{n} a_i.$$

یعنی در این حالت اثبات کامل است.
حالت دوم. $k < n-1$. در این صورت با کمک شرکت پذیری و تعریف عمل استانده داریم

$$T(a_1,...,a_n) = T(a_1,...,a_k) * T(a_{k+1},...,a_n) = (\prod_{i=1}^{k} a_i) * (\prod_{j=k+1}^{n} a_j)$$

$$(\prod_{i=1}^{k} a_i) * ((\prod_{j=k+1}^{n-1} a_j) * a_n) = ((\prod_{i=1}^{k} a_i) * (\prod_{j=k+1}^{n-1} a_j)) * a_n$$

اما $(\prod_{i=1}^{k} a_i) * (\prod_{j=k+1}^{n-1} a_j)$ عمل دوتایی با معنی از $(n-1)$تا است یعنی $T(a_1,...,a_{n-1})$.
پس طبق فرض اسقرا داریم

$$(\prod_{i=1}^{k} a_i) * (\prod_{j=k+1}^{n-1} a_j) = \prod_{i=1}^{n-1} a_i.$$

با جایگذاری در بالا و استفاده از تعریف عمل استانده داریم

$$T(a_1,...,a_n) = (\prod_{i=1}^{n} a_i) * a_n = \prod_{i=1}^{n} a_i$$

در این حالت هم اثبات کامل است. □

تعریف ۱۸.۱.۲. *فرض کنیم S و $* : S \times S \longrightarrow S$ و $o : S \times S \longrightarrow S$ دو عمل دوتایی روی مجموعه S باشند. گوییم*
(الف) $*$ روی o توزیعپذیر از سمت چپ است هرگاه برای هر $x, y, z \in S$ داشته باشیم

$$x * (yoz) = (x * y)o(x * z).$$

(ب) $*$ روی o توزیعپذیر از سمت راست است هرگاه برای هر $x, y, z \in S$ داشته باشیم

$$(yoz) * x = (y * x)o(z * x).$$

(ج) $*$ روی o توزیعپذیر است هرگاه توزیعپذیر چپ و راست باشد.

مثال ۱۹.۱.۲. *روی $\mathbb{R}$ عمل دوتایی $*$ را جمع معولی و عمل دوتایی o را همان ضرب معمولی در نظر می‌گیریم. همان طوری که از دوران مدرسه تا کنون دیده‌اید جمع روی ضرب توزیعپذیر است.*

مثال ۲۰.۱.۲. *عمل دوتایی $*$ را اجتماع روی $\mathbb{P}(X)$ و عمل دوتایی o را اشتراک روی $\mathbb{P}(X)$ در نظر می‌گیریم. در این صورت $*$ روی o توزیعپذیر است. همچنین o روی $*$ توزیعپذیر است. زیرا از مبانی ریاضی دیده‌اید که*

$$A \cup (B \cap C) = (A \cap B) \cap (A \cup C)$$

بقیه حالت‌ها هم مشابه است.

مثال ۲.۱.۲۱. *روی اعداد حقیقی عمل $*$ را جمع و عمل o را قدرمطلق در نظر می‌گیریم. $*$ روی o توزیع‌پذیر (چپ- راست) نیست. زیرا*

$$۱ * (۲o۳) = ۱ * (|۲ - ۳|) = ۱ * ۱ = ۱ + ۱ = ۲$$

در حالی که

$$(۱ * ۲)o(۱ * ۳) = (۱ + ۲)o(۱ + ۳) = ۳o۴ = |۳ - ۴| = ۱.$$

تعریف ۲.۱.۲۲. *منظور از ساختار ریاضی یا دستگاه ریاضی یعنی مجموعه‌ای ناتهی مانند $*$ همراه با یک یا چند عمل دوتایی روی S مانند $*_۱$، ...، $*_n$ که معمولا با $(S, *_۱, ..., *_n)$ نمایش می‌دهیم.*

مثال ۲.۱.۲۳. $(\mathbb{Z}, +)$ *یک ساختار ریاضی است با یک عمل دوتایی است.*

مثال ۲.۱.۲۴. $(\mathbb{R}, +, \cdot)$ *یک ساختار ریاضی با دو عمل دوتایی است.*

تمرین‌های حل شده

تمرین ۲.۱.۲۵. *آیا $* : \mathbb{R} \times \mathbb{R} \longrightarrow \mathbb{R}$ با ضابطه $a * b = a^b$ یک عمل دوتایی است؟*

حل. $*$ یک عمل دوتایی نیست. زیرا اگر قرار دهیم $a = -۱$ و $b = \frac{۱}{۲}$ آنگاه $a^b = \sqrt{-۱}$ که همان $a * b$ است، معنی ندارد. یعنی $*$ یک تابع نیست.

تمرین ۲.۱.۲۶. *آیا $* : \mathbb{R} \times \mathbb{R} \longrightarrow \mathbb{R}$ با ضابطه $a * b = ۲^a \times ۳^b$ یک عمل دوتایی است؟*

حل. $*$ یک عمل دوتایی است. باید نشان دهیم $*$ تابع است. ابتدا دقت کنید باید نشان دهیم $a * b \in \mathbb{R}$. اگر a عددی گویا باشد یعنی $a = \frac{m}{n}$ آنگاه $۲^{\frac{m}{n}} = \sqrt[n]{۲^m}$ عددی حقیقی است. به صورت مشابه اگر b عدد گویا باشد باز هم ۳^b نیز عدد حقیقی است و حاصل ضرب دو عدد حقیقی باز هم عددی حقیقی است. بنابراین در این حالت $a * b \in \mathbb{R}$. اگر a عددی گویا نباشد آنگاه می‌دانیم که دنباله‌ای از اعداد گویا وجود دارد که به a میل می‌کند یعنی $a = \lim_{n\to\infty} x_n$ که x_nها گویا هستند. پس $۲^a = ۲^{\lim_{n\to\infty} x_n} = \lim_{n\to\infty}[۲^{x_n}]$. اما طبق حالت قبل ۲^{x_n} عددی حقیقی هستند که این نتیجه می‌دهد $۲^a \in \mathbb{R}$. پس در هر صورت، $a * b \in \mathbb{R}$. همچنین اگر $a = a'$ و $b = b'$ آنگاه $۲^a \times ۳^b = ۲^{a'} \times ۳^{b'}$. در نتیجه $*$ یک عمل دوتایی است.

تمرین ۲.۱.۲۷. *فرض کنیم $*$ عمل دوتایی شرکت پذیر روی مجموعه ناتهی S باشد و $a, b \in S$. اگر برای هر $x \in$ داشته باشیم $x * a = x$ و $b * x = x$ آنگاه نشان دهید که $a = b$.*

حل. طبق فرض می‌توانیم x را خود a یا b انتخاب کنیم. مثلا اگر $x = b$ در نظر بگیریم و در $x * a = x$ قرار دهیم آنگاه $b * a = b$ و به روش مشابه اگر $x = a$ را در $b * x = x$ قرار دهیم آنگاه $b * a = b$. پس $a = b$.

تمرین ۲.۱.۲۸. *فرض کنیم S یک مجموعه با عمل دوتایی شرکت پذیر $*$ باشد که برای $x, y, z \in S$ داریم $x * y = y * x$ و $x * z = z * x$. نشان دهید که x با $y * z$ جابجا می‌شود.*

حل. داریم

$$x * (y * z) = x * y * z = y * x * z = y * z * x = (y * z) * x.$$

۲.۲ تعریف گروه، مثال‌ها و قضیه‌های اولیه

با تعریف ساختارهای ریاضی در بخش قبل آشنا شدید. اما بعضی ساختارهای ریاضی عمل‌های دوتایی آن خواص بیشتری دارند و مورد توجه قرار می‌گیرند. در این بخش (حتی کل این فصل) روی ساختار ریاضی تمرکز می‌کنیم که فقط یک عمل دوتایی دارد و آن عمل ویژگی‌های خاصی را دارا است. با تعریف زیر آغاز می‌کنیم.

تعریف ۱.۲.۲. *فرض کنیم S یک مجموعه ناتهی و $*$ یک عمل دوتایی روی S باشد. گوییم $(S,*)$ یک نیم‌گروه است هرگاه $*$ شرکت پذیر باشد.*

مثال ۲.۲.۲. *$(\mathbb{Z},+)$ یک نیم‌گروه است. حتی $(\mathbb{R},\cdot)$ نیز یک نیم‌گروه است.*

مثال ۳.۲.۲. *فرض کنیم S برابر با بازه $[۰,۴]$ باشد. در این صورت $*: S\times S\longrightarrow S$ با ضابطه $a*b=|a-b|$ یک عمل دوتایی است (چرا؟) که شرکت پذیر نیست (چرا؟). بنابراین $(S,*)$ نیم‌گروه نیست.*

تعریف ۴.۲.۲. *فرض کنیم S یک مجموعه ناتهی و $*$ یک عمل دوتایی روی S باشد. گوییم:*
(الف) عنصر $e\in S$ عضو خنثی (همانی) چپ است هرگاه برای هر $s\in S$ داشته باشیم $e*s=s$.
(ب) عنصر $e\in S$ عضو خنثی (همانی) راست است هرگاه برای هر $s\in S$ داشته باشیم $s*e=s$.
(ج) عنصر $e\in S$ خنثی (همانی) است هرگاه هم خنثی چپ و هم خنثی راست باشد.

مثال ۵.۲.۲. *در $(\mathbb{Z},+)$ عنصر ۰ خنثی (چپ‌ـ راست) است. زیرا برای هر $x\in\mathbb{Z}$ داریم که $x+۰=۰+x=x$.*

مثال ۶.۲.۲. *فرض کنیم S برابر با بازه $[۰,۴]$ باشد. در این صورت $*: S\times S\longrightarrow S$ با ضابطه $a*b=|a-b|$ یک عمل دوتایی است. برای هر $s\in S$ داریم $s*۰=۰*s=s$. پس ۰ عنصر خنثی است.*

مثال ۷.۲.۲. *$(\mathbb{R},*)$ که در آن $a*b=۳$ عضو خنثی ندارد.*

مثال ۸.۲.۲. *فرض کنیم $S=\{۱,۲\}$ و برای هر $a,b\in S$ تعریف می‌کنیم $a*b=b$. در این صورت S عضو خنثی چپ دارد که یکتا هم نیست (چرا؟). در حالی که اصلا عضو خنثی راست ندارد!*

واضح است که اگر $*$ روی S جابجایی باشد و S عنصر خنثی چپ داشته باشد آنگاه این عنصر خنثی چپ، خنثی راست نیز می‌باشد. این مطلب و مثال قبل ما را به سمت گزاره زیر رهنمود می‌کند.

گزاره ۹.۲.۲. *فرض کنیم $*$ یک عمل دوتایی روی مجموعه S باشد. اگر $(S,*)$ دارای عضو خنثی چپ مانند e و عضو خنثی راست مانند f باشد آنگاه $e=f$. در نتیجه عضو خنثی یکتا است.*

اثبات. چون e عضو خنثی چپ است پس باید $e * f = f$ باشد. اما f عضو خنثی راست است پس $e * f = e$. بنابراین باید $e = f$. قسمت دوم بدیهی است چون هر عضو خنثی، خنثی چپ (راست) است. □

تعریف ۱۰.۲.۲. *فرض کنیم $(S, *)$ دارای عنصر خنثی مانند e باشد. گوییم*
(الف) عنصر $a \in S$ دارای وارون چپ است هرگاه عنصر $b \in S$ موجود باشد که $b * a = e$.
(ب) عنصر $a \in S$ دارای وارون راست است هرگاه عنصر $b \in S$ موجود باشد که $a * b = e$.
(ج) عنصر $a \in S$ وارون پذیر است هرگاه هم وارون چپ و هم وارون راست داشته باشد (وارون a را با a^{-1} نمایش می‌دهیم).

مثال ۱۱.۲.۲. *$(\mathbb{Z}, +)$ دارای عنصر خنثی ۰ نسبت به عمل دوتایی $+$ است و برای هر عدد صحیح x داریم که $x + (-x) = (-x) + x = 0$. پس هر عنصر در $\mathbb{Z}$ وارون پذیر است.*

مثال ۱۲.۲.۲. *$(\mathbb{Z}, \cdot)$ دارای عنصر خنثی ۱ نسبت به عمل دوتایی $\cdot$ است. هر عدد صحیح مخالف با ۱ و -1 وارون پذیر نیست. در حالی که -1 وارون پذیر است.*

مثال ۱۳.۲.۲. *$(\mathbb{R}, \cdot)$ عضو خنثی ۱ دارد. همه عناصر ناصفر وارون دارند در حالی که ۰ ندارد.*

مثال ۱۴.۲.۲. *$(\mathbb{N}, \cdot)$ یک نیم‌گروه است که عضو خنثی ۱ دارد. اما هیچ عنصر وارون پذیری ندارد.*

مثال ۱۵.۲.۲. *فرض کنیم S برابر با بازه $[0, 4]$ باشد. در این صورت $* : S \times S \longrightarrow S$ با ضابطه $a * b = |a - b|$ یک عمل دوتایی است. برای هر $s \in S$ داریم $0 * s = s * 0 = s$. پس ۰ عنصر خنثی است. جالب این که هر عنصر وارون خودش است!*

تذکر ۱۶.۲.۲. *فرض کنیم $(S, *)$ دارای عنصر خنثی مانند e باشد. واضح است که e وارون خودش است.*

مثال ۱۷.۲.۲. *فرض کنیم $S = \{1, 2\}$ و برای هر $a, b \in S$ تعریف می‌کنیم $a * b = b$. در این صورت ۱ عضو خنثی چپ است. همه عناصر وارون راست برابر با ۱ دارند. از طرفی ۲ نیز عضو خنثی چپ است و جالب این که همه عناصر وارون راست ۲ دارند. در حالی که اصلا عضو خنثی راست وجود ندارد! پس وارون چپ و راست بی معنی است!*

اگر عمل دوتایی $*$ جابجایی روی S باشد و S عنصر خنثی داشته باشد وارون چپ هر عنصر در صورت وجود وارون راست نیز می‌باشد. این مطلب و مثال بالا ما را به گزاره زیر رهنمود می‌کند.

گزاره ۱۸.۲.۲. *فرض کنیم نیم‌گروه $(S, *)$ دارای عنصر خنثی مانند e باشد. اگر x در S وارون چپ a و وارون راست b داشته باشد آنگاه $a = b$.*

اثبات. چون a وارون چپ x است پس $a * x = e$. به صورت مشابه $x * b = e$. اما با فرض نیم‌گروهی داریم

$$a = a * e = a * (x * b) = (a * x) * b = e * b = b.$$

اثبات کامل است. □

تذکر ۱۹.۲.۲. *بعضی مراجع و کتاب‌ها به یک نیم‌گروه با عنصر خنثی تکواره یا مونوئید گویند.*

مثال ۲۰.۲.۲. *مجموعه توابع پیوسته روی $\mathbb{R}$ را با $C(\mathbb{R})$ نشان می‌دهیم. $C(\mathbb{R})$ با عمل دوتایی ترکیب عادی توابع یک نیم‌گروه با عنصر خنثی $id_{\mathbb{R}}$ است (قضیه ۱.۱.۲۵ را ببینید). اما می‌دانیم که توابعی وارون پذیر هستند که یک‌به‌یک و پوشا باشند (قضیه ۱.۱.۲۸ را ببینید). در حالی که همه عناصر $C(\mathbb{R})$ یک‌به‌یک یا پوشا نیستند.*

اکنون آماده این مطلب هستیم که تعریف گروه را بیاوریم.

تعریف ۲۱.۲.۲. *فرض کنیم G مجموعه ناتهی و $*$ یک عمل دوتایی روی G باشد. گوییم $(G,*)$ یک گروه است هرگاه:*
(الف) $(G,*)$ نیم‌گروه باشد ($*$ شرکت پذیر باشد).
(ب) $(G,*)$ عضو خنثی داشته باشد.
(ج) هر عنصر G نسبت به عمل $*$ وارون داشته باشد.

مثال ۲۲.۲.۲. $(\mathbb{R},+)$ یک گروه است.

مثال ۲۳.۲.۲. $(\mathbb{R},\cdot)$ یک گروه نیست. زیرا 0 وارون ندارد.

مثال ۲۴.۲.۲. $(\mathbb{R}\setminus\{0\},\cdot)$ یک گروه است.

مثال ۲۵.۲.۲. *فرض کنیم S برابر با بازه $[0,4]$ باشد. در این صورت $*:S\times S\longrightarrow S$ با ضابطه $a*b=|a-b|$ یک عمل دوتایی است. برای هر $s\in S$ داریم $0*s=s*0=s$. پس 0 عنصر خنثی است. هر عنصر وارون خودش است. اما $*$ شرکت پذیر نیست. پس $(S,*)$ نیم‌گروه نیست و در نتیجه گروه نیست.*

مثال ۲۶.۲.۲. $(\mathbb{R},*)$ *که در آن $a*b=3$ عضو خنثی ندارد و در نتیجه گروه نیست.*

مثال ۲۷.۲.۲. $(M_n(\mathbb{R}),+)$ *یک گروه است ($+$ جمع عادی دو ماتریس). واضح است که ضرب ماتریس‌ها شرکت پذیر است و ماتریس O نقش عنصر خنثی را دارد. وارون هر ماتریس (a_{ij}) ماتریس $(-a_{ij})$ است.*

مثال ۲۸.۲.۲. $(M_n(\mathbb{R}),\cdot)$ *یک گروه نیست ($\cdot$ ضرب عادی دو ماتریس). زیرا همه ماتریس‌ها وارون ندارند (چرا؟). دقت شود که I عنصر خنثی است.*

مثال ۲۹.۲.۲. *فرض کنیم $GL_n(\mathbb{R})$ مجموعه همه ماتریس‌های مربعی وارون پذیر باشد (طبق قضیه ۱.۳.۱۳ ، همه ماتریس‌های که دترمینان ناصفر دارند). $(GL_n(\mathbb{R}),\cdot)$ یک گروه است (عمل $\cdot$ ضرب عادی دو ماتریس). دقت شود که I عنصر خنثی است. همچنین طبق قضیه ۱.۳.۱۱ ، اگر $A,B\in GL_n(\mathbb{R})$ آنگاه $A\cdot B\in GL_n(\mathbb{R})$. یعنی $\cdot$ روی $GL_n(\mathbb{R})$ تابع (عمل دوتایی) است. شرکت پذیری از $M_n(\mathbb{R})$ به $GL_n(\mathbb{R})$ ارث می‌رسد.*

مثال ۳۰.۲.۲. *فرض کنیم n یک عدد طبیعی باشد. در این صورت $(\mathbb{Z}_n,+)$ یک گروه است. برای تعریف اعداد پیمانه‌ای $\mathbb{Z}_n$ و عمل دوتایی جمع روی این مجموعه به فصل اول بخش دوم مراجعه نمایید. واضح است که $\bar{0}$ عضو خنثی است. وارون عنصر $\bar{x}$ به صورت $\overline{n-x}$ است. با یک محاسبه سر راست این عمل جمع شرکت پذیر است.*

مثال ۲.۲.۳۱. *فرض کنیم n یک عدد طبیعی باشد. در این صورت $(\mathbb{Z}_n, \cdot)$ یک گروه نیست. برای تعریف اعداد پیمانه‌ای $\mathbb{Z}_n$ و عمل دوتایی ضرب روی این مجموعه به فصل اول بخش دوم مراجعه نمایید. واضح است که $\bar{۱}$ عضو خنثی است. اما وارون عنصر $\bar{۰}$ وجود ندارد. با یک محاسبه سر راست این عمل ضرب شرکت پذیر است.*

مثال ۲.۲.۳۲. *$(\mathbb{Z}_۴ \setminus \{\bar{۰}\}, \cdot)$ یک گروه نیست. برای تعریف اعداد پیمانه‌ای $\mathbb{Z}_n$ و عمل دوتایی ضرب روی این مجموعه به فصل اول بخش دوم مراجعه نمایید. واضح است که $\bar{۱}$ عضو خنثی است. اما وارون عنصر $\bar{۲}$ وجود ندارد (چرا؟).*

مثال ۲.۲.۳۳. *فرض کنیم p یک عدد اول باشد. در این صورت $(\mathbb{Z}_p \setminus \{\bar{۰}\}, \cdot)$ یک گروه است. برای تعریف اعداد پیمانه‌ای $\mathbb{Z}_p$ و عمل دوتایی ضرب روی این مجموعه به فصل اول بخش دوم مراجعه نمایید. واضح است که $\bar{۱}$ عضو خنثی است. با یک محاسبه سر راست این عمل ضرب شرکت پذیر است. اکنون وارون یک عضو مانند $\bar{x}$ را ارئه می‌کنیم. چون $\bar{x}$ مخاف با $\bar{۰}$ است پس در $\mathbb{Z}$ داریم $(x, p) = ۱$. طبق قضیه بزو، قضیه ۱.۲.۱۰، اعداد صحیح r و s وجود دارند که $rx + sp = ۱$. در نتیجه $\overline{rx + sp} = \overline{rx} = \bar{۱}$. پس $\bar{r} \cdot \bar{x} = \bar{۱}$. یعنی $\bar{x}$ وارون پذیر است.*

مثال ۲.۲.۳۴. *مجموعه ریشه‌های nام واحد با ضرب معمولی اعداد مختلط یک گروه است، یعنی*

$$G = \{w \in \mathbb{C} \mid w^n = ۱\}.$$

اگر $w, w' \in G$ انگاه $(ww')^n = w^n w'^n = ۱$. پس $ww' \in G$ و به ضرب بسته است. شرکتپذیر از اعداد مختلط به ارث می‌رسد. عنصر خنثی برابر ۱ است و وارون هر عنصر w برابر $w^{n-۱}$ است.

تذکر ۲.۲.۳۵. *گاهی کشیدن یک جدول برای گروه کار را ساده‌تر می‌کند. فرض کنیم G یک گروه باشد که کاردینال آن متناهی است. مثلا فرض کنیم $G = \{e, a_۱, a_۲, ..., a_{n-۱}\}$ که e عنصر خنثی برای G است. می‌توانیم به G جدولی مانند زیر وابسته کنیم.*

	e	$a_۱$	$a_۲$	$\cdots$	$a_{n-۱}$
e	e	$a_۱$	$a_۲$	$\cdots$	$a_{n-۱}$
$a_۱$	$a_۱$	$a_۱a_۱$	$a_۱a_۲$	$\cdots$	$a_۱a_{n-۱}$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$a_{n-۱}$	$a_{n-۱}$	$a_{n-۱}a_۱$	$a_{n-۱}a_۲$	$\cdots$	$a_{n-۱}a_{n-۱}$

مثال ۲.۲.۳۶. *برای گروه $(\mathbb{Z}_۴, +)$ نمایش جدولی به صورت زیر است*

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

که بعد از محاسبه داریم

	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{0}$	$\bar{1}$	$\bar{2}$

نمادگذاری ۳۷.۲.۲. *در سرتاسر این فصل منظور از e_G یا e یعنی عنصر خنثی گروه G. مگر این که به صراحت خلاف این مطلب را ذکر کنیم. اگر در مبحثی چند گروه مطرح باشد از نماد e_G، e_H و ... استفاده می‌کنیم تا ابهامی ایجاد نشود.*

تعریف ۳۸.۲.۲. *گروه $(G,*)$ را آبلی گوییم هرگاه $*$ جابجایی باشد.*

مثال ۳۹.۲.۲. $(\mathbb{Z},+)$ *یک گروه آبلی است.*

مثال ۴۰.۲.۲. $(GL_n(\mathbb{R}),\cdot)$ *گروه آبلی نیست (ضرب ماترس‌ها (حتی وارون پذیرها) در حالت کلی جابجایی نیست).*

قضیه ۱۷.۱.۲ سبب می‌شود که پرانتز گذاری برای عمل دوتایی شرکت پذیر بی اهمیت شود که این منجر به تعریف زیر می‌شود.

تعریف ۴۱.۲.۲. *فرض کنیم $*$ عمل دوتایی شرکت پذیر روی S باشد (نیم‌گروه) و $n\in\mathbb{N}$. برای $a\in S$ توان a را به استقرا به صورت زیر تعریف می‌کنیم*

$$a^1=a,\ \ a^2=a*a,\ \ a^3=a^2*a,\ \ a^n=a^{n-1}*a.$$

به طور ویژه، اگر S گروه با عنصر خنثی e باشد و $k\in\mathbb{Z}$ آنگاه برای $g\in S$ تعریف می‌کنیم

$$g^k=\begin{cases}\underbrace{g*g*\ldots*g}_{k} & k>0\\ e & k=0\\ \underbrace{g^{-1}*g^{-1}*\ldots*g^{-1}}_{k} & k<0\end{cases}$$

مثال ۴۲.۲.۲. *عمل دوتایی $+$ روی $\mathbb{Z}$ شرکت پذیر است و برای $x\in\mathbb{Z}$ و هر عدد طبیعی n داریم*

$$\underbrace{x+x+\ldots+x}_{n}=nx.$$

مثال ۴۳.۲.۲. *عمل دوتایی $\cdot$ روی $\mathbb{R}$ شرکت پذیر است و برای $x\in\mathbb{R}$ و هر عدد طبیعی n داریم*

$$\underbrace{x\cdot x\cdot\ldots\cdot x}_{n}=x^n.$$

قضیه ۴۴.۲.۲. *فرض کنیم $(S,*)$ گروه باشد و $a \in S$. برای اعداد صحیح m و n داریم.*
(الف) $(a^m)^n = a^{mn}$
(ب) $a^m * a^n = a^{m+n}$

اثبات. سر راست است. □

در ادامه قضیه‌های را خواهیم آورد که نشان می‌دهد در چه زمانی یک نیم‌گروه یک گروه است.

قضیه ۴۵.۲.۲. *نیم‌گروه $(G,*)$ گروه است اگر و تنها اگر برای هر $a,b \in G$ معادلات $a*x=b$ و $y*a=b$ جواب داشته باشند.*

اثبات. $(\Leftarrow)$. چون G گروه است، قرار می‌دهیم $x = a^{-1} * b$. در این صورت $a * x = b$ دارای جواب است. برای معادله دوم از $y = b * a^{-1}$ استفاده می‌کنیم.
$(\Rightarrow)$. چون G نیم‌گروه است شرکت پذیر است. نشان می‌دهیم G عضو خنثی دارد. چون معالات برای هر a و b جواب دارند، a را با b مساوی می‌گیریم. پس معادله $a * x = a$ دارای جواب e است. حال برای c، نشان می‌دهیم $c * e = c$ یعنی e خنثی چپ است. معادله $y * a = c$ دارای جواب f است. یعنی $f * a = c$. پس

$$c * e = (f * a) * e = f * (a * e) f * a = c.$$

با روش مشابه وجود عضو خنثی راست اثبات می‌شود. طبق گزاره ۹.۲.۲، e عضو خنثی گروه است. اکنون فرض کنیم $c \in G$ دلخواه باشد. نشان می‌دهیم c وارون پذیر است. معادله $c * x = e$ دارای جواب c' است و معادله $y * c = e$ دارای جواب c'' است. c' و c'' به ترتیب وارون راست و چپ برای c هستند. طبق گزاره ۱۸.۲.۲، $c' = c''$ و c وارون پذیر است. □

تعریف ۴۶.۲.۲. *فرض کنیم $*$ یک عمل دوتایی روی S باشد. گوییم:*
(الف) قانون حذف از چپ در S برقرار است اگر $a,b,c \in S$ و $c*a = c*b$ آنگاه نتیجه شود $a = b$.
(ب) قانون حذف از راست در S برقرار است اگر $a,b,c \in S$ و $a*c = b*c$ آنگاه نتیجه شود $a = b$.
(ج) قانون حذف برقرار است هرگاه هم حذف چپ و هم حذف راست برقرار باشد.

مثال ۴۷.۲.۲. *در گروه $(\mathbb{Z},+)$ قانون حذف داریم. زیرا $(\mathbb{Z},+)$ یک گروه آبلی است و فقط کافی است حذف چپ را نشان دهیم. فرض کنیم $c+a=c+b$. با جمع طرفین تساوی با $-c$ داریم $a=b$.*

مثال ۴۸.۲.۲. *در نیم‌گروه $(\mathbb{N},*)$ که $*$ همان عمل دوتایی ضرب معمولی است، قانون حذف (چپ‌ـ راست) برقرار است.*

مثال ۴۹.۲.۲. $(\mathbb{R},*)$ *که در آن* $a * b = ۳$ *نه حذف چپ برقرار است نه حذف راست.*

مثال ۵۰.۲.۲. *فرض کنیم* $S = \{۱, ۲\}$ *و برای هر* $a, b \in S$ *تعریف می‌کنیم* $a * b = b$. *واضح است که اگر* $c * a = c * b$ *آنگاه* $a = b$. *پس حذف چپ برقرار است. یک بررسی ساده نشان می‌دهد حذف راست برقرار نیست.*

حال قضیه زیر را داریم.

قضیه ۵۱.۲.۲. *نیم‌گروه متناهی* $(G, *)$ *گروه است اگر و تنها اگر قانون حذف در* G *برقرار باشد.*

اثبات. ($\Leftarrow$). فرض کنیم برای $a, b, c \in G$ داشته باشیم $c * a = c * b$. چون G گروه است پس c در G وارون دارد. با انجام عمل دوتایی طرفین تساوی بالا از سمت چپ در $c^{-۱}$ داریم

$$c^{-۱} * c * a = c^{-۱} * c * b \;\Rightarrow\; e * a = e * b \;\Rightarrow\; a = b.$$

قانون حذف از راست مشابه بالا اثبات می‌شود و در نتیجه قانون حذف داریم.
($\Rightarrow$). فرض کنیم $G = \{a_۱, a_۲, ..., a_n\}$. طبق قضیه ۴۵.۲.۲، برای این که نشان دهیم G گروه است، کافی است نشان دهیم برای $a, b \in G$، معادلات $a * x = b$ و $y * a = b$ جواب دارند. مجموعه زیر را در نظر می‌گیریم

$$A = \{a * a_۱, a * a_۲, ..., a * a_n\}.$$

واضح است که $A \subseteq G$ (چرا؟). حال اگر $a * a_i = a * a_j$ که $۱ \leq i, j \leq n$، آنگاه بر طبق فرض قانون حذف از چپ بر قرار است و درنتیجه $a_i = a_j$. این نشان می‌دهد که اعضای A متمایز هستند و باید $|A| = n$ (چرا؟). یعنی داریم

$$A = \{a * a_۱, a * a_۲, ..., a * a_n\} = G = \{a_۱, a_۲, ..., a_n\}.$$

فرض کنیم $b = a_i$. پس a_j چنان وجو دارد که $a * a_j = a_i$ و این یعنی معادله $ax = b$ دارای جواب $x = a_j$ است. به روش مشابه و با در نظر گرفتن

$$B = \{a_۱ * a, a_۲ * a, ..., a_n * a\}$$

می‌توان نشان داد که $y * a = b$ جواب دارد. بنابراین بر طبق قضیه ۴۵.۲.۲ اثبات کامل است. □

اکنون این بخش را با قضیه زیر که منسوب به شخص هَیز[۲] است به پایان می‌رسانیم.

قضیه ۵۲.۲.۲. (هَیز) *نیم‌گروه* $(G, *)$ *گروه است اگر و تنها اگر برای هر عنصر* a *در* G، *عنصر یکتای* $a' \in G$ *وجود داشته باشد که* $aa'a = a$.

اثبات. ($\Leftarrow$). چون G گروه است کافی است a' را همان $a^{-۱}$ در نظر بگیریم و این یعنی دست کم یک a' وجود دارد که $a * a' * a = a$. حال اگر داشته باشیم $a * a'' * a = a$ که $a'' \in G$. پس $a * a'' * a = a * a' * a$. با دوبار استفاده از قضیه ۵۱.۲.۲، داریم $a' = a''$.

[۲] Hays

($\Rightarrow$). برای اثبات این قسمت ابتدا دو ادعای زیر را اثبات می‌کنیم:
ادعا ۱: عنصر b در G چنان وجود دارد که $b^2 = b$.
اثبات ادعا ۱: فرض کنیم $a \in G$. طبق فرض عنصر یکتای $a' \in G$ وجود دارد که $a * a' * a = a$.
قرار می‌دهیم $b = a * a'$ و داریم

$$b^2 = b * b = (a * a') * (a * a') = (a * a' * a) * a' = a * a' = b$$

پس ادعای ۱ اثبات شد.
ادعا ۲: فقط یک عنصر در $b \in G$ وجود دارد که $b^2 = b$.
اثبات ادعا ۲: فرض کنیم $c \in G$ و $c^2 = c$. واضح است که $b * c \in G$ (چرا؟) و در نتیجه طبق فرض $(b * c)'$ وجود دارد که

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

حال داریم

$$\begin{aligned}
&(b * c) * [(b * c)' * b] * (b * c) = (b * c) * (b * c)' * (b * b) * c = \\
&(b * c) * (b * c)' * b^2 * c = (b * c) * (b * c)' * b * c = \\
&(b * c) * (b * c)' * (b * c) = b * c.
\end{aligned}$$

چون فرض یکتایی را داریم پس باید $(b * c)' * b = (b * c)'$. به روش مشابه داریم

$$\begin{aligned}
&(b * c) * [c * (b * c)'] * (b * c) = b * (c * c) * (b * c)' * (b * c) = \\
&b * c^2 * (b * c)' * (b * c) = b * c * (b * c)' * (b * c) = \\
&(b * c) * (b * c)' * (b * c) = b * c.
\end{aligned}$$

چون فرض یکتایی را داریم پس باید $c * (b * c)' = (b * c)'$. از سوی دیگر داریم

$$\begin{aligned}
&(b * c) * [(b * c)' * (b * c) * (b * c)'] * (b * c) = \\
&[(b * c) * (b * c)' * (b * c)] * (b * c)' * (b * c) = \\
&(b * c) * (b * c)' * (b * c) = b * c.
\end{aligned}$$

چون فرض یکتایی را داریم پس باید

$$(b * c)' * (b * c) * (b * c)' = (b * c)' \qquad (I)$$

حال

$$\begin{aligned}
&((b * c)')^2 = (b * c)' * (b * c)' = \\
&[(b * c)' * b] * [c * (b * c)'] = (b * c)' * (b * c) * (b * c)' = (b * c)'
\end{aligned}$$

یعنی $((b*c)')^{۲} = (b*c)'$. بنابراین

$$(b*c)'*(b*c)'*(b*c)' = (b*c)' \qquad (II)$$

اما (I) و (II) همراه با فرض یکتایی نشان می‌دهند که $(b*c)' = b*c$. در نتیجه $(b*c)^{۲} = b*c$ (چرا؟). حال داریم

$$(b*c)*b*(b*c) = (b*c)*(b*b)*c = (b*c)*b^{۲}*c =$$
$$(b*c)*b*c = (b*c)*(b*c) = (b*c)^{۲} = b*c.$$

به روش مشابه $(b*c)*c*(b*c) = b*c$ (بررسی کنید). از فرض یکتایی باید $b = c$. اثبات ادعای ۲ کامل است.
اکنون نشان می‌دهیم G گروه است. طبق ادعا ۱، G دارای عنصری مانند e است که $e^{۲} = e$. طبق ادعا ۲، e یکتا است. حال فرض کنیم $g \in G$ دلخواه باشد. طبق فرض $g' \in G$ وجود دارد که $g*g'*g = g$. واضح است که $g*g' = (g*g')^{۲}$. چون e یکتا است پس $g*g' = e$. از طرفی دیگر $g'*g = (g'*g)^{۲}$. یکتایی e نتیجه می‌دهد که $g'*g = e$. بنابراین $e*g = g = g*e$. این یعنی e عنصر همانی است. چون $g*g' = e$ و $g'*g = e$ پس g وارون پذیر است. اثبات این که G گروه است. □

تمرین‌های حل شده

تمرین ۵۳.۲.۲. *عمل دوتایی $a*b = \frac{ab}{۱۳}$ را روی $\mathbb{Q}$ در نظر بگیرید. عضو خنثی و وارون هر عضو را معلوم کنید.*

حل. دقت شود که این عمل جابجایی است (چرا؟) پس صحبت از چپ و راست بی معنی است.
معرفی عضو خنثی: فرض کنیم $x \in \mathbb{Q}$ عضو خنثی این عمل دوتایی باشد. پس برای هر $a \in \mathbb{Q}$ داریم $a*x = a$. یعنی $\frac{ax}{۱۳} = a$. در نتیجه $x = ۱۳$ و این یعنی $e = ۱۳$ عنصر خنثی است.
معرفی وارون هر عضو: عنصر دلخواه $x \in \mathbb{Q}$ را درنظر می‌گیریم. وارون پذیری x معادل با این است که عنصر $a \in \mathbb{Q}$ موجود باشد که $a*x = e = ۱۳$. یعنی $\frac{ax}{۱۳} = ۱۳$. این نشان می‌دهد که اگر a ناصفر باشد آنگاه دارای وارون $a^{-۱} = \frac{۱۳^{۲}}{a}$ است.

تمرین ۵۴.۲.۲. *فرض کنیم*

$$S = \{\begin{pmatrix} a & b \\ ۰ & ۰ \end{pmatrix} \mid a, b \in \mathbb{Z}\}.$$

روی S عمل دوتایی $*$ را همان ضرب عادی ماتریسی بگیرید. آیا $*$ شرکت پذیر است؟ آیا $*$ عضو خنثی (چپ- راست) دارد؟

حل. ابتدا دقت شود که ضرب عادی ماتریسی از S خارج نمی‌شود. زیرا

$$\begin{pmatrix} a & b \\ ۰ & ۰ \end{pmatrix} \cdot \begin{pmatrix} a' & b' \\ ۰ & ۰ \end{pmatrix} = \begin{pmatrix} aa' & ab' \\ ۰ & ۰ \end{pmatrix} \in S.$$

چون ضرب عادی ماتریسی در حالت کلی شرکت پذیر است پس روی S نیز شرکت پذیری را داریم. برای هر عدد صحیح x عنصر

$$\begin{pmatrix} ۱ & x \\ ۰ & ۰ \end{pmatrix}$$

در S یک عنصر خنثی چپ است. زیرا

$$\begin{pmatrix} ۱ & x \\ ۰ & ۰ \end{pmatrix} \cdot \begin{pmatrix} a & b \\ ۰ & ۰ \end{pmatrix} = \begin{pmatrix} a & b \\ ۰ & ۰ \end{pmatrix}.$$

یعنی S نامتناهی خنثی چپ دارد. اما S نمی‌تواند خنثی راست داشته باشد. زیرا اگر S خنثی راست داشته باشد آنگاه طبق گزاره ۹.۲.۲، آنگاه نامتناهی عنصر خنثی راست داریم در حالی که طبق گزاره ۹.۲.۲، عنصر خنثی یکتا باید باشد.

تمرین ۵۵.۲.۲. *فرض کنیم نیم‌گروه $(S,*)$ دارای عضو خنثی e و دو عنصر a و b وارون پذیر (چپ‌ـ راست) باشند. آنگاه نشان دهید که $a*b$ وارون پذیر (چپ‌ـ راست) است. سپس وارون $a_۱ * a_۲ * ... * a_n$ را پیدا کنید.*

حل. فقط کافی است وارون چپ داشتن $a*b$ را اثبات کنیم، وارون راست مشابه است. فرض کنیم وارون چپ a، c باشد یعنی $c*a=e$ و وارون چپ b، d باشد یعنی $d*b=e$. ادعا می‌کنیم $a*b$ دارای وارون $d*c$ است. زیرا با فرض نیم‌گروه داریم

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

برای قسمت دوم، واضح است که با استقرای ضعیف، وارون عنصر $a_۱ * a_۲ * ... * a_n$ برابر است با $a_n^{-۱} * ... * a_۲^{-۱} * a_۱^{-۱}$.

تمرین ۵۶.۲.۲. *برای گروه $(G,*)$ نشان دهید که $(a^{-۱})^{-۱} = a$.*

حل. داریم که $a * a^{-۱} = e$. پس a وارون $a^{-۱}$ است و طبق تعریف وارون مسئله حل است.

تمرین ۵۷.۲.۲. *فرض کنیم $\mathbb{Q}[\sqrt{۲}] = \{a+b\sqrt{۲} \mid a,b \in \mathbb{Q}\}$. نشان دهید که $\mathbb{Q}[\sqrt{۲}]$ با عمل دوتایی زیر یک گروه است.*

$$(a+b\sqrt{۲}) + (a'+b'\sqrt{۲}) = (a+a') + (b+b')\sqrt{۲}$$

حل. ابتدا شرکت پذیری را بررسی می‌کنیم.

$$\begin{aligned}
&(a+b\sqrt{۲}) + [(a'+b'\sqrt{۲}) + (a''+b''\sqrt{۲})] = \\
&(a+b\sqrt{۲}) + [(a'+a'') + (b'+b'')\sqrt{۲}] = (a+a'+a'') + (b+b'+b'')\sqrt{۲} = \\
&[(a+b\sqrt{۲}) + (a'+b'\sqrt{۲})] + (a''+b''\sqrt{۲})
\end{aligned}$$

واضح است که $۰ + ۰\sqrt{۲}$ عنصر خنثی است. وارون $a+b\sqrt{۲}$ برابر است با $-a-b\sqrt{۲}$.

تمرین ۵۸.۲.۲. *نشان دهید که برای یک مجموعه X، $(\mathbb{P}(X), \cap)$ گروه نیست.*

حل. اگر $A, B \in \mathbb{P}(X)$ آنگاه واضح است که $A \cap B \in \mathbb{P}(X)$، یعنی اشتراک یک عمل دوتایی است. شرکت پذیری عمل دوتایی اشتراک واضح است. مجموعه X در نقش عنصر خنثی است. اگر $A \neq X$ آنگاه واضح است که برای هر زیرمجموعه Y از X همواره $A \cap Y \subsetneq X$، یعنی A وارون ندارد. پس $(\mathbb{P}(X), \cap)$ گروه نیست.

تمرین ۵۹.۲.۲. *فرض کنیم n یک عدد طبیعی باشد. عناصر وارون پذیر $\mathbb{Z}_n$ نسبت به عمل ضرب را با $U(\mathbb{Z}_n)$ نشان می‌دهیم. ثابت کنید که:*
(الف) $U(Z_n) = \{\bar{x} \mid (x, n) = ۱\}$.
(ب) $U(\mathbb{Z}_n)$ *با همان ضرب* $\mathbb{Z}_n$ *یک گروه است.*

حل. (الف) فرض کنیم $T = \{\bar{x} \mid (x, n) = ۱\}$ و $\bar{x} \in U(Z_n)$. پس عنصر $\bar{y}$ چنان وجود دارد که $\bar{x} \cdot \bar{y} = \bar{۱}$ یا معادلا $\overline{xy} = \bar{۱}$. این نتیجه می‌دهد که $n | xy - ۱$. پس $(n, xy) = ۱$ و در نتیجه $(n, x) = ۱$. پس $\bar{x} \in T$ و $U(Z_n) \subseteq T$.
فرض کنیم $\bar{x} \in T$. پس $(x, n) = ۱$ و در نتیجه از قضیه بزو، قضیه ۱۰.۲.۱، اعداد صحیح r و s وجود دارند که $rx + sn = ۱$. در نتیجه $\overline{rx + sn} = \overline{rx} = \bar{۱}$. پس $\bar{r} \cdot \bar{x} = \bar{۱}$. یعنی $\bar{x}$ وارون پذیر است. بنابراین $\bar{x} \in U(Z_n) \subseteq T$.
(ب) طبق تمرین ۵۵.۲.۲، حاصل ضرب دو عنصر وارون پذیر، وارون پذیر است، یعنی $\cdot$ روی $U(\mathbb{Z}_n)$ عمل دوتایی است. $\bar{۱}$ عضو خنثی است و شرکت پذیری هم از $\mathbb{Z}_n$ به ارث می‌رسد.

تمرین ۶۰.۲.۲. *اگر $(G, *)$ یک گروه متناهی بیشتر از ۲ عضو با عنصر خنثی e باشد آنگاه عنصر $e \neq g \in G$ وجود دارد که $g^۲ = g$ $(g^۲ = g * g)$.*

حل. فرض کنید $g \in G$. مجموعه $T = \{g^۲, g^۴, g^۸, ...\}$ را در نظر می‌گیریم. چون G نیم‌گروه است، برای هر عدد طبیعی k داریم که $g^k \in G$. در نتیجه $T \subseteq G$. اما G متناهی است، پس باید برای اعداد طبیعی متمایز i و j داشته باشیم $g^{۲^i} = g^{۲^j}$. بدون کم شدن از کلیت فرض کنیم $۱ \leq i < j$. پس طبق قضیه ۴۴.۲.۲ داریم

$$g^{۲^j} = (g^{۲^i})^{۲^{j-i}} = g^{۲^i}.$$

قرار می‌دهیم $k = ۲^{j-i}$ و $h = g^{۲^i}$. پس $h^k = h$. حال دو حالت رخ می‌دهد.
حالت اول. $k = ۲$ که کار تمام است و h همان مطلوب مسئله است.
حالت دوم. $k > ۲$ که با قضیه ۴۴.۲.۲ داریم

$$h^{k-۲} * h^k = h^{k-۲} * h \Rightarrow (h^{k-۱})^۲ = h^{k-۱}.$$

در این حالت $h^{k-۱}$ همان مطلوب مسئله است.

تمرین ۶۱.۲.۲. *فرض کنیم G گروهی باشد که برای هر عنصر $g \in G$ داریم $g^۲ = e$. نشان دهید G آبلی است.*

حل. برای هر $a \in G$، چون $a^۲ = e$ پس $a = a^{-۱}$. فرض کنیم $g, h \in G$. در نتیجه طبق فرض داریم $(g * h)^۲ = e$. پس

$$g * h * g * h = e \;\Rightarrow\; g^{-۱} * g * h * g * h = g^{-۱} \;\Rightarrow\; h * g * h = g^{-۱} = g.$$

حال طرفین تساوی آخر از سمت چپ در $h^{-۱}$ عمل دوتایی می‌کنیم

$$h * g * h = g \;\Rightarrow\; h^{-۱} * h * g * h = h^{-۱} * g = h * g \;\Rightarrow\; g * h = h * g.$$

تمرین ۶۲.۲.۲. *برای گروه $(G, *)$ و عدد طبیعی n نشان دهید که $a*b^n*a^{-۱} = (a*b*a^{-۱})^n$.*

حل. داریم

$$(a * b * a^{-۱})^n = \underbrace{a * b * a^{-۱} * a * b * a^{-۱} * \ldots * a * b * a^{-۱}}_{n\text{تا}}$$

چون $a^{-۱} * a = e$ و $b * e = b$ پس سمت راست تساوی با قضیه ۴۴.۲.۲، برابر است با $a * b^n * a^{-۱}$.

تمرین ۶۳.۲.۲. *نشان دهید هر گروه حداکثر ۵ عضو آبلی است.*

حل. برای گروه یک عضوی و دو عضوی چیزی برای اثبات نداریم. فرض کنیم G گروه سه عضوی باشد. یعنی $G = \{e, a, b\}$ که e عنصر همانی است. مشکل اساسی ما $a * b$ است! اگر $a * b = a$ باشد آنگاه داریم $a^{-۱} * a * b = a^{-۱} * a = e$ یعنی $b = e$ است که تناقض با سه عضوی بودن گروه است. مشابه اگر $a * b = b$ باشد آنگاه داریم $a * b * b^{-۱} * = b * b^{-۱} = e$ یعنی $a = e$ است که تناقض با سه عضوی بودن گروه است. اگر $a * b$ برابر e شود آنگاه a و b وارون هم هستند و لذا جابجا می‌شوند. حال فرض کنیم گروه چهار عضوی باشد. فرض کنیم e عنصر خنثی گروه باشد. دو عنصر متمایز از هم و متمایز از e مانند a و b انتخاب می‌کنیم. مشابه استدلال گروه سه عضوی، باید $a * b$ عنصر چهارم باشد. حال $b * a$ باید یکی از e، a، b و $a * b$ باشد. اگر $b * a = e$ آنگاه a و b وارون هم هستند و در نتیجه گروه سه عضوی می‌شود که تناقض است. اگر $b * a = a * b$ آنگاه چیزی برای اثبات نداریم. دو حالت دیگر هم رخ نمی‌دهد چون a و b مخالف e هستند. برای گروه پنج عضوی روند بالا را تکرار کنید.

تمرین ۶۴.۲.۲. *آیا در قضیه ۴۵. ۲. ۲، وجود جواب برای یک معادله مثلا $ax = b$ برای گروه شدن G کافی است؟*

حل. خیر کافی نیست و مثال نقض وجود دارد. فرض کنیم $G = \{۱, ۲\}$ و برای هر $a, b \in S$ تعریف می‌کنیم $a * b = b$. واضح است که G نیم‌گروه است و برای $a, b \in G$ همواره $ax = b$ دارای جواب $x = b$ است. اما G گروه نیست. زیرا عضو خنثی راست وجود ندارد.

تمرین ۶۵.۲.۲. *آیا در قضیه ۵۱. ۲. ۲ شرط متناهی بودن لازم است؟*

حل. نیم‌گروه نامتناهی $(\mathbb{N}, \cdot)$ را در نظر می‌گیریم. در این نیم‌گروه قانون حذف برقرار است در حالی که گروه نیست (چرا؟).

تمرین ۶۶.۲.۲. *فرض کنیم $(G, *)$ یک گروه با عضو خنثی e باشد و $a, b \in G$. اگر $a^۴ = e$ و $a^۲ * b = b * a$ آنگاه نشان دهید که $a = e$.*

حل. چون G گره است پس اعضا وارون دارند و با عمل دوتایی طرفین تساوی $a^۲ * b = b * a$ از چپ با $b^{-۱}$ داریم $b^{-۱} * a^۲ * b = a$. طبق تمرین ۶۲.۲.۲، داریم

$$a^۲ = (b^{-۱} * a^۲ * b)^۲ = b^{-۱} * a^۴ * b.$$

چون $a^۴ = e$ در نتیجه باید $a^۲ = e$ باشد. اما فرض $a^۲ * b = b * a$ ایجاب می‌کند که $b * a = b$. با عمل دوتایی طرفین تساوی آخر از سمت چپ در $b^{-۱}$ داریم $a = e$.

تمرین ۶۷.۲.۲. *فرض کنیم $(G, *)$ یک گروه متناهی باشد که $|G|$ عدد زوج است. نشان دهید $e \neq a \in G$ وجود دارد که $a^۲ = e$ (e عضو خنثی گروه است).*

حل. مجموعه

$$A = \{g \in G \mid g \neq g^{-۱}\}$$

را در نظر می‌گیریم. واضح است که اگر $g \in A$ آنگاه $g^{-۱} \in A$ (چرا؟). از طرفی چون $A \subseteq G$ و G متناهی پس $|A|$ باید عدد زوج باشد (چرا؟). اکنون مجموعه $B = \{e\} \cup A$ یک مجموعه متناهی است و کاردینال آن عدد فرد است. این نشان می‌دهد که $B \subsetneq G$. پس عنصر $a \in G \setminus B$ وجود دارد که $a = a^{-۱}$ و این یعنی $a^۲ = e$.

تمرین ۶۸.۲.۲. *فرض کنیم $(G, *)$ یک گروه با عنصر خنثی e باشد که برای $a, b \in G$ داریم $a * b = b * a^{-۱}$ و $b * a = a * b^{-۱}$. نشان دهید که $a^۴ = b^۴ = e$.*

حل. از فرض نتیجه می‌شود که $a = b * a^{-۱} * b^{-۱}$. و در نتیجه

$$b * a = a * b^{-۱} = b * a^{-۱} * b^{-۱} * b^{-۱} = b * a^{-۱} * b^{-۲}.$$

با انجام عمل دوتایی طرفین تساوی بالا از سمت چپ با $b^{-۱}$ داریم

$$a = a^{-۱} * b^{-۲}.$$

تساوی آخر نشان می‌۲دهد که $a^۲ = b^{-۲}$. بنابراین

$$a^۴ = a^۲ * a^۲ = a^۲ * b^{-۲} = a * (a * b^{-۱}) * b^{-۱} = a * (b * a) * b^{-۱} =$$
$$(a * b) * a * b^{-۱} = (b * a^{-۱}) * a * b^{-۱} = b * a^{-۱} * a * b^{-۱} = e$$

با روندی مشابه اثبات می‌شود که $b^۴ = e$.

تمرین ۶۹.۲.۲. *نشان دهید که اگر در گروه $(G,*)$، برای سه عدد صحیح متوالی مانند n داشته باشیم $(a*b)^n = a^n * b^n$ آنگاه G آبلی است.*

حل. فرض کنیم

$$(a*b)^n = a^n * b^n \qquad (a*b)^{n+1} = a^{n+1} * b^{n+1} \qquad (a*b)^{n+2} = a^{n+2} * b^{n+2}$$

پس

$$a^{n+1} * b^{n+1} = (a*b)^{n+1} = (a*b) * (a*b)^n = a*b*a^n*b^n.$$

با انجام عمل دوتایی مناسب در طرفین تساوی داریم $a^n * b = b * a^n$ (چگونه؟). از طرفی دیگر

$$a^{n+2} * b^{n+2} = a^{n+1} * b^{n+1} = (a*b) * (a*b)^{n+1} = a*b*a^{n+1}*b^{n+1}.$$

با انجام عمل دوتایی مناسب در طرفین تساوی داریم $a^{n+1} * b = b * a^{n+1}$ (چگونه؟). بنابراین

$$b * a^{n+1} = a^{n+1} * b = a * a^n * b = a*b*a^n.$$

با انجام عمل دوتایی مناسب در طرفین تساوی داریم $a*b = b*a$. یعنی G آبلی است.

۳.۲ چند مثال خاص از گروه‌ها

در این قسمت چند مثال ویژه از گروه‌ها را به دست می‌دهیم. این مثال‌ها بسیار با اهمیت هستند و لازم است که دانشجو روی آن ها مسلط شود. در بخش‌های آینده برای ساختن مثال‌ها مناسب از مفاهیم جدید تسلط دانشجو بر مثال‌های زیر بسیار کمک کننده است. از این رو این مثال‌ها را در یک بخش جمع آوری کرده‌ایم.

همین قدر از اهمیت این مثال‌ها بدانید که در آرم شرکت‌های معروف مانند مرسدس بنز (گروه D_3)، تا ملکول‌های مواد مانند NH_3 (گروه D_3)، تا زیبایی خانه‌های لوکس (گروه D_5)، تا لوگوی معروف کرایسلر[3] (گروه D_5)، تا دانه‌های برف و کریستال و شن و ماسه، تا موجودات زنده مانند ستاره دریایی یا حتی غشای بیرونی ویروس HIV و ... گروه‌های متقارن ظاهر می‌شوند!

تعریف ۱.۳.۲. *هر تابع یک‌به‌یک و پوشا روی یک مجموعه مانند X را یک جایگشت نامیم. مجموعه همه جایگشت‌ها روی X را با S_X نمایش می‌دهیم. اگر $X = \{۱, ۲, ..., n\}$ باشد آنگاه از نماد S_n به جای S_X استفاده می‌کنیم.*

قضیه ۲.۳.۲. *اگر X یک مجموعه ناتهی باشد آنگاه S_X با عمل ترکیب یک گروه است.*

اثبات. ابتدا دقت کنید طبق قضیه ۲۶.۱.۱ به واقع ترکیب توابع یک عمل است و طبق قضیه ۲۵.۱.۱ این عمل شرکت پذیر است. واضح است که تابع همانی، id_X، عضو خنثی است و طبق قضیه ۲۸.۱.۱، هر عنصر در S_X وارونپذیر است. □

تعریف ۳.۳.۲. *به گروه S_n، گروه متقارن روی n حرف یا گروه متقارن از درجه n گوییم. اعضای این گروه را معمولا با حروف σ، τ و ... نشان می‌دهیم.*

نمادگذاری ۴.۳.۲. *فرض کنیم $\sigma \in S_n$، یعنی σ یک تناظر روی $\{۱, ۲, ..., n\}$ است. همچنین می‌دانیم که σ عنصر i از S_n را به $\sigma(i)$ نظیر می‌کند یعنی $i \mapsto \sigma(i)$. این مطلب سبب می‌شود که بتوانیم اعضای S_n را به شکل جالبی نمایش دهیم و بتوانیم با این اعضا به صورت راحتتر مواجه شویم*

$$\sigma = \begin{pmatrix} ۱ & ۲ & ... & n \\ \sigma(۱) & \sigma(۲) & ... & \sigma(n) \end{pmatrix}.$$

اگر

$$\tau = \begin{pmatrix} ۱ & ۲ & ... & n \\ \tau(۱) & \tau(۲) & ... & \tau(n) \end{pmatrix}$$

جایگشت دیگری باشد آنگاه مثلا عنصر ۳ توسط σ به $j = \sigma(۳)$ نگاشته می‌شود و τ عنصر j را به $\tau(j)$ می‌نگارد. پس ترکیب به شکل زیر اعمل می‌شود

$$\sigma\tau = \begin{pmatrix} ۱ & ۲ & ... & n \\ \tau\sigma(۱) & \tau\sigma(۲) & ... & \tau\sigma(n) \end{pmatrix}.$$

[3] Chrysler

مثال ۵.۳.۲. *اگر* $X = \{۱\}$ *باشد آنگاه* $S_۱$ *فقط عنصر* $\sigma = \begin{pmatrix} ۱ \\ ۱ \end{pmatrix}$ *را دارد که همان عنصر خنثی است.*

مثال ۶.۳.۲. *اگر* $X = \{۱, ۲\}$ *باشد آنگاه* $S_۲$ *فقط دو عنصر*

$$\sigma_۱ = \begin{pmatrix} ۱ & ۲ \\ ۱ & ۲ \end{pmatrix} \qquad \sigma_۲ = \begin{pmatrix} ۱ & ۲ \\ ۲ & ۱ \end{pmatrix}$$

را دارد که $\sigma_۱$ *همان عنصر خنثی است. وارون عنصر* $\sigma_۲$ *خودش است.*

مثال ۷.۳.۲. *اگر* $X = \{۱, ۲, ۳\}$ *باشد آنگاه* $S_۳$ *شش عنصر*

$$\sigma_۱ = \begin{pmatrix} ۱ & ۲ & ۳ \\ ۱ & ۲ & ۳ \end{pmatrix} \qquad \sigma_۲ = \begin{pmatrix} ۱ & ۲ & ۳ \\ ۲ & ۳ & ۱ \end{pmatrix} \qquad \sigma_۳ = \begin{pmatrix} ۱ & ۲ & ۳ \\ ۳ & ۱ & ۲ \end{pmatrix}$$
$$\sigma_۴ = \begin{pmatrix} ۱ & ۲ & ۳ \\ ۱ & ۳ & ۲ \end{pmatrix} \qquad \sigma_۵ = \begin{pmatrix} ۱ & ۲ & ۳ \\ ۳ & ۲ & ۱ \end{pmatrix} \qquad \sigma_۶ = \begin{pmatrix} ۱ & ۲ & ۳ \\ ۲ & ۱ & ۳ \end{pmatrix}$$

را دارد که $\sigma_۱$ *همان عنصر خنثی است. وارون عنصر* $\sigma_۲$ *عنصر* $\sigma_۳$ *است. همچنین*

$$\sigma_۳\sigma_۵ = \begin{pmatrix} ۱ & ۲ & ۳ \\ ۲ & ۱ & ۳ \end{pmatrix} = \sigma_۶.$$

قضیه ۸.۳.۲. *برای هر عدد طبیعی* n*، همواره داریم* $|S_n| = n!$ *.*

اثبات. برای عنصر ۱ تعداد n حالت انتخاب ممکن است و برای عنصر ۲ تعداد حالت $(n - ۱)$ انتخاب ممکن است. دقت شود که قرار است تناظر باشد! روند را ادامه می‌دهیم و طبق اصل ضرب داریم

$$|S_n| = n \times (n - ۱) \times (n - ۲) \times ... \times ۳ \times ۲ \times ۱ = n!$$

و اثبات کامل است. □

قضیه ۹.۳.۲. *وارون عنصر*

$$\begin{pmatrix} ۱ & ۲ & ... & n \\ \sigma(۱) & \sigma(۲) & ... & \sigma(n) \end{pmatrix}$$

برابر

$$\begin{pmatrix} \sigma(۱) & \sigma(۲) & ... & \sigma(n) \\ ۱ & ۲ & ... & n \end{pmatrix}$$

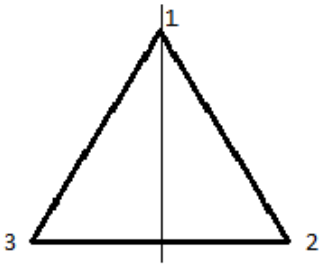
است.

اثبات. سر راست است. □

تذکر ۱۰.۳.۲. *در قسمت تمرینات حل شده بخش دوم از فصل دوم مشاهده کردید که گروه‌های حداکثر پنج عضوی آبلی هستند اما S_3 یک گروه* **۶** *عضوی است که غیر آبلی است زیرا $\sigma_2\sigma_4 \neq \sigma_4\sigma_2$.*

به مثال زیر توجه کنید.

مثال ۱۱.۳.۲. *یک مثلث متساوی الاضلاع را در نظر بگیرید که رئوس آن را با $X = \{1, 2, 3\}$ شماره گذاری کرده‌ایم خطوط تقارن از راس‌ها رسم می‌کنیم یعنی*



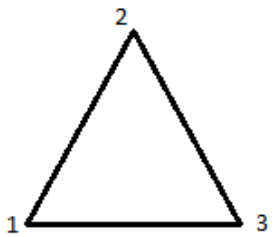
می‌توان به شکل بالا با کمک انعکاس جایگشت

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

را نظیر کرد. اگر بقیه خطوط تقارن را رسم کنیم به جایگشت‌های

$$\sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \qquad \sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

می‌رسیم. حال فرض کنید رئوس مثلث را به اندازه ۱۲۰ درجه در جهت خلاف عقربه ساعت دوران دهیم، یعنی



می‌توان به شکل بالا جایگشت

$$\tau_1 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

را نظیر کرد. با دوران ۲۴۰ درجه و ۳۶۰ درجه داریم

$$\tau_۲ = \begin{pmatrix} ۱ & ۲ & ۳ \\ ۲ & ۳ & ۱ \end{pmatrix} \qquad \tau_۳ = \begin{pmatrix} ۱ & ۲ & ۳ \\ ۱ & ۲ & ۳ \end{pmatrix}$$

می‌رسیم. حال یک بررسی ساده نشان می‌دهد که

$$D_۳ = \{\sigma_۱, \sigma_۲, \sigma_۳, \tau_۱, \tau_۲, \tau_۳\}$$

یک گروه است با عنصر همانی $\tau_۳$.

تعریف ۱۲.۳.۲. یک nـ ضلعی منتظم در نظر بگیرید. گروه متشکل از nتا انعکاس نسبت به محور تقارن و nتا دوران نسبت به مرکز چند ضلعی منتظم با زاویه $\frac{۲k\pi}{n}$ که $k \in \{۱, ..., n\}$ را گروه دو وجهی مرتبه n گوییم. این گروه را با D_n نشان می‌دهیم.

مثال ۱۳.۳.۲. گروه دو وجهی یک برف ریزه

گروه $D_۶$ است.

قضیه ۱۴.۳.۲. تعداد اعضای D_n برابر $۲n$ است.

اثبات. با توجه به ساختن D_n، nتا انعکاس و nتا دوران داریم پس $|D_n| = n + n = ۲n$. □

تعریف ۱۵.۳.۲. گروه چهارتایی کلاین دارای چهار عضو a، b، c و e است که e عضو همانی است. ضرب اعضای آن به صورت زیر تعریف می‌شود

$$ea = ae = a \quad eb = be = b \quad ec = ce = c \quad ee = e$$
$$a^۲ = b^۲ = c^۲ = e \quad ab = ba = c \quad ac = ca = b \quad bc = cb = a$$

و این گروه را با $\mathbb{K}_۴$ نمایش می‌دهیم.

مثال ۱۶.۳.۲. *جدول گروه $\mathbb{K}_4$ به شکل زیر است و این گروه آبلی است.*

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

تعریف ۱۷.۳.۲. *گروه کوترنیون‌ها دارای هشت عضو به صورت*

$$\{۱, -۱, i, -i, j, -j, k, -k\}$$

است و ضرب اعضای آن به صورت زیر تعریف می‌شود

$$i^۲ = j^۲ = k^۲ = -۱ \qquad ij = k \qquad jk = i$$
$$ki = j \qquad ik = -j \qquad ji = -k \qquad kj = -i$$

و این گروه را با $\mathbb{Q}_8$ نمایش می‌دهیم. عنصر خنثی ۱ است.

مثال ۱۸.۳.۲. *گروه $\mathbb{Q}_8$ غیر آبلی است. زیرا داریم $ij = k \neq ji = -k$.*

مثال ۱۹.۳.۲. *در گروه $\mathbb{Q}_8$ وارون عنصر j برابر $-j$ است. زیرا داریم*

$$j(-j) = jik = (ji)k = -kk = (-۱)kk = (-۱)k^۲ = (-۱)(-۱) = ۱.$$

مواردی که در زیر می‌آید دست ما را برای داشتن گروه‌های متنوع باز می‌گذارد. هر چند این موارد را آنچنان که شایسته است گسترش نمی‌دهیم و فقط جهت آشنایی می‌آوریم.

تعریف ۲۰.۳.۲. *فرض کنیم $\{G_i\}_{i\in I}$ خانواده‌ای ازگروه‌ها باشد. تمام دنباله‌ها به صورت $(x_i)_{i\in I}$ که برای هر $i \in I$، $x_i \in G_i$ را در نظر می‌گیریم. عمل دوتایی را به صورت*

$$(x_i)_{i\in I} * (y_i)_{i\in I} = (x_i y_i)_{i\in I}$$

تعریف می‌کنیم و این دنباله‌ها را به یک گروه تبدیل می‌کنیم. در واقع، در مکان i ام عمل دوتایی گروه G_i پیاده می‌شود. گروه جدید را حاصل ضرب مستقیم یا حاصل ضرب دکارتی G_i ها گوییم و با $\prod_{i\in I} G_i$ نشان می‌دهیم. اگر I متناهی باشد از نماد $G_۱ \times ... \times G_k$ نیز استفاده می‌کنیم که $k = |I|$. اگر I تهی باشد تعریف می‌کنیم $\prod_{i\in I} G_i = ۰$.

تعریف ۲.۳.۲۱. *فرض کنیم $\{G_i\}_{i\in I}$ خانواده‌ای از گروه‌ها باشد. تمام دنباله‌ها به صورت $(x_i)_{i\in I}$ از $\prod_{i\in I} G_i$ را در نظر می‌گیریم که به جز تعداد متناهی اندیس بقیه مولفه‌ها عناصر خنثی هستند. با همان عمل دوتایی $\prod_{i\in I} G_i$ این دنباله‌ها گروه تشکیل می‌دهند. گروه جدید (در واقع زیرگروه $\prod_{i\in I} G_i$) را حاصل جمع مستقیم G_i ها گوییم و با $\bigoplus_{i\in I} G_i$ نشان می‌دهیم. اگر I متناهی باشد از نماد $G_1 \oplus ... \oplus G_k$ نیز استفاده می‌کنیم که $k = |I|$. اگر I تهی باشد تعریف می‌کنیم $\bigoplus_{i\in I} G_i = 0$.*

مثال ۲.۳.۲۲. *عنصر همانی گروه $\prod_{i\in I} G_i$ به صورت $(e_i)_{i\in I}$ است که e_i عنصر خنثی گروه G_i است.*

مثال ۲.۳.۲۳. *وارون عنصر $(x_i)_{i\in I}$ از گروه $\prod_{i\in I} G_i$ به صورت $(x_i^{-1})_{i\in I}$ است.*

مثال ۲.۳.۲۴. *فرض کنیم $G = S_3$ و $H = \mathbb{Z}_4$. دراین صورت*

$$G \times H = \{(\sigma, \bar{i}) \mid \sigma \in G,\ \bar{i} \in H\}$$

با عمل زیر

$$(\sigma, \bar{i}) * (\tau, \bar{j}) = (\sigma\tau, \bar{i} + \bar{j})$$

یک گروه است.

مثال ۲.۳.۲۵. *فرض کنیم $H = G = \mathbb{Z}_2$. دراین صورت*

$$G \times H = \{(\bar{i}, \bar{j}) \mid \bar{i}, \bar{j} \in H\}$$

با عمل زیر

$$(\bar{i}, \bar{j}) * (\bar{i}', \bar{j}') = (\overline{ii'}, \overline{jj'})$$

یک گروه است.

تمرین‌های حل شده

تمرین ۲.۳.۲۶. *آیا در گروه S_3 عنصری مانند σ وجود دارد که $\sigma\sigma$ همانی شود؟*

حل. با توجه به متن درس که اعضای S_3 را به دست آورده‌ایم، قرار می‌دهیم

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}.$$

حال داریم

$$\sigma\sigma = \sigma^2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}.$$

تمرین ۲.۳.۲۷. *آیا در گروه S_3 عنصری مانند σ وجود دارد که $\sigma\sigma\sigma$ همانی شود؟*

حل. با توجه به متن درس که اعضای S_3 را به دست آورده‌ایم، قرار می‌دهیم

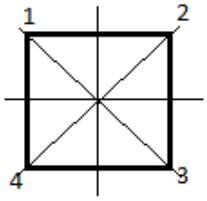
$$\sigma = \begin{pmatrix} ۱ & ۲ & ۳ \\ ۲ & ۳ & ۱ \end{pmatrix}.$$

حال داریم

$$\sigma\sigma\sigma = \sigma^۳ = \begin{pmatrix} ۱ & ۲ & ۳ \\ ۱ & ۲ & ۳ \end{pmatrix}.$$

تمرین ۲.۳.۲۸. *اعضای گروه D_4 را بنویسید.*

حل. یک مربع را در نظر بگیرید که رئوس آن را با $X = \{۱, ۲, ۳, ۴\}$ شماره گذاری کرده‌ایم. خطوط تقارن مربع چهارتا است، یعنی



حال می‌توان به شکل بالا با کمک انعکاس جایگشت‌های

$$\sigma_۱ = \begin{pmatrix} ۱ & ۲ & ۳ & ۴ \\ ۱ & ۴ & ۳ & ۲ \end{pmatrix} \qquad \sigma_۲ = \begin{pmatrix} ۱ & ۲ & ۳ & ۴ \\ ۳ & ۲ & ۱ & ۴ \end{pmatrix}$$
$$\sigma_۳ = \begin{pmatrix} ۱ & ۲ & ۳ & ۴ \\ ۲ & ۱ & ۴ & ۳ \end{pmatrix} \qquad \sigma_۴ = \begin{pmatrix} ۱ & ۲ & ۳ & ۴ \\ ۴ & ۳ & ۴ & ۱ \end{pmatrix}$$

را نظیر کرد. حال فرض کنید رئوس مربع را به اندازه۹۰، ۱۸۰، ۲۷۰ و ۳۶۰ درجه در جهت خلاف عقربه ساعت دوران دهیم، جایگشت‌های

$$\tau_۱ = \begin{pmatrix} ۱ & ۲ & ۳ & ۴ \\ ۴ & ۱ & ۲ & ۳ \end{pmatrix} \qquad \tau_۲ = \begin{pmatrix} ۱ & ۲ & ۳ & ۴ \\ ۳ & ۲ & ۱ & ۴ \end{pmatrix}$$
$$\tau_۳ = \begin{pmatrix} ۱ & ۲ & ۳ & ۴ \\ ۲ & ۳ & ۴ & ۱ \end{pmatrix} \qquad \tau_۴ = \begin{pmatrix} ۱ & ۲ & ۳ & ۴ \\ ۱ & ۲ & ۳ & ۴ \end{pmatrix}$$

حال داریم

$$D_۴ = \{\sigma_۱, \sigma_۲, \sigma_۳, \sigma_۴, \tau_۱, \tau_۲, \tau_۳, \tau_۴\}$$

که یک گروه هشت عضوی است با عنصر همانی $\tau_۴$.

تمرین ۲۹.۳.۲. *برای $\mathbb{K}_4$ یک نمایش ماتریسی به دست آورید.*

حل. اعضای

$$E = \begin{pmatrix} ۱ & ۰ \\ ۰ & ۱ \end{pmatrix} \qquad A = \begin{pmatrix} ۱ & ۰ \\ ۰ & -۱ \end{pmatrix} \qquad B = \begin{pmatrix} -۱ & ۰ \\ ۰ & ۱ \end{pmatrix} \qquad C = \begin{pmatrix} -۱ & ۰ \\ ۰ & -۱ \end{pmatrix}$$

از $M_۲(\mathbb{R})$ را در نظر می‌گیرم. با فرض $A = a$، $B = b$، $C = c$ و $E = e$ و ضرب ماتریسی عادی همان گروه $\mathbb{K}_4$ حاصل می‌شود.

تمرین ۳۰.۳.۲. *برای $\mathbb{Q}_8$ یک نمایش ماتریسی به دست آورید.*

حل. اعضای

$$A = \begin{pmatrix} ۱ & ۰ \\ ۰ & ۱ \end{pmatrix} \qquad B = \begin{pmatrix} i & ۰ \\ ۰ & -i \end{pmatrix} \qquad C = \begin{pmatrix} ۰ & ۱ \\ -۱ & ۰ \end{pmatrix} \qquad D = \begin{pmatrix} ۰ & i \\ i & ۰ \end{pmatrix}$$

از $M_۲(\mathbb{C})$ را در نظر می‌گیرم. با فرض $A = ۱$، $B = i$، $C = j$ و $D = k$ و ضرب ماتریسی عادی همان گروه $\mathbb{Q}_8$ حاصل می‌شود.

۴.۲ زیرگروه

در این بخش بررسی می‌کنیم چه زمانی یک زیرمجموعه ناتهی از یک گروه، خود یک گروه است.

تعریف ۱.۴.۲. *فرض کنیم G با عمل $*$ یک گروه باشد و $H \subseteq G$. گوییم H زیرگروه G است و با $H \leq G$ نمایش می‌دهیم هرگاه H با عمل $*$ که از G الحاق می‌شود، به گروه تبدیل شود.*

مثال ۲.۴.۲. *می‌دانیم که $(\mathbb{R}, +)$ یک گروه است. زیرمجموعه‌های $\mathbb{Z}$ و $\mathbb{Q}$ با عمل جمع الحاق شده از $\mathbb{R}$ گروه هستند. زیرا جمع الحاق شده روی $\mathbb{Z}$ بسته و شرکتپذیری است و همچنین عضو خنثی و وارون پذیری در $\mathbb{Z}$ و $\mathbb{Q}$ برقرار است و لذا $\mathbb{Z} \leq \mathbb{R}$ و $\mathbb{Q} \leq \mathbb{R}$.*

مثال ۳.۴.۲. *اگر e عنصر خنثی گروه G باشد آنگاه $\{e\}$ یک زیرگروه است. همچنین به وضوح G زیرگروه G است. به این دو زیرگروه که در هرگروه وجود دارد، زیرگروه‌های بدیهی گوییم.*

مثال ۴.۴.۲. *زیرمجموعه $۲\mathbb{Z} = \{۲k \mid k \in \mathbb{Z}\}$ یک زیرگروه از $(\mathbb{Z}, +)$ است. واضح است که برای هر $k, k' \in \mathbb{Z}$ داریم $۲k + ۲k' = ۲(k + k') \in ۲\mathbb{Z}$. پس $۲\mathbb{Z}$ نسبت به عمل دوتایی $+$ بسته است. صفر عنصر از $۲\mathbb{Z}$ است و به وضوح عضو خنثی است. شرکتپذیری و وارونپذیری نیز واضح است.*

بررسی زیرگروه بودن با کمک تعریف بالا شاید خسته کننده باشد. قضیه زیر یک محک ساده در اختیار ما قرار می‌دهد.

قضیه ۵.۴.۲. *فرض کنیم G گروه باشد. در این صورت موارد زیر معادل هستند.*
(۱) زیرمجموعه ناتهی H از G زیرگروه است.
(۲) برای هر $a, b \in H$ داشته باشیم $ab \in H$ و $a^{-۱} \in H$.
(۳) برای هر $a, b \in H$ داشته باشیم $ab^{-۱} \in H$.

اثبات. (۱) $\Leftarrow$ (۲). فرض کنیم $a, b \in H$. چون H زیرگروه است پس $a^{-۱}$ در H قرار دارد. چون H زیرگروه است نسبت به عمل القایی بسته است و لذا $ab \in H$.
(۲) $\Leftarrow$ (۳). فرض کنیم $x, y \in H$. طبق فرض $y^{-۱}$ در H قرار دارد (در حقیقت $a = y$ فرض کرده ایم). دوباره طبق فرض باید $xy^{-۱}$ در H باشد (در حقیقت $a = x$ و $b = y^{-۱}$ فرض کرده‌ایم).
(۳) $\Leftarrow$ (۱). ابتدا دقت شود که H ناتهی است. فرض کنیم $x \in H$. طبق فرض $xx^{-۱} \in H$، در حقیقت فرض کرده‌ایم $a = b = x$. اما در گروه G داریم $xx^{-۱} = e$. لذا $e \in H$. حال برای هر $a \in H$ داریم $a = ae = ea$ و در نتیجه H عنصر خنثی e را دارد.
حال فرض کنیم $x \in H$. اکنون قرار می‌دهیم که $a = e$ و $b = x$. بنابراین بر طبق فرض $ab^{-۱} = ex^{-۱} = x^{-۱} \in H$. یعنی وارون هر عضو از H در خود H قرار دارد.
فرض کنیم $x, y \in H$. طبق قسمت بالا $y^{-۱} \in H$ و لذا طبق فرض باید $xy = x(y^{-۱})^{-۱} \in H$ باشد. در حقیقت فرض کرده‌ایم $a = x$ و $b = y^{-۱}$ (دقت شود که طبق تمرین ۵۶.۲.۲ داریم $y = (y^{-۱})^{-۱}$). پس H نسبت به عمل الحاقی بسته است.

چون H زیرمجموعه G است شرکتپذیری از G به H ارث می‌رسد و لذا طبق تعریف H زیرگروه است. □

مثال ۶.۴.۲. *گروه $(\mathbb{R} \setminus \{0\}, .)$ را در نظر بگیرید. در این صورت $\mathbb{R}^+$، مجموعه اعداد حقیقی مثبت، یک زیرگروه است. فرض کنیم $a, b \in \mathbb{R}^+$. در این صورت $b^{-1} = \frac{1}{b}$ عضوی از $\mathbb{R}^+$ است و به وضوح $ab^{-1} = \frac{a}{b} \in \mathbb{R}^+$. حال طبق قضیه ۵.۴.۲ باید $\mathbb{R}^+$ زیرگروه باشد.*

مثال ۷.۴.۲. *گروه $(\mathbb{R} \setminus \{0\}, .)$ را در نظر بگیرید. در این صورت $A = \{a \in \mathbb{R} \mid |a| \in \mathbb{N}\}$ یک زیرگروه نیست. واضح است که $2 \in A$. اما $2^{-1} = \frac{1}{2} \notin A$ عضوی از A نیست. زیرا داریم $|2^{-1}| = \frac{1}{2}$. حال طبق قضیه ۵.۴.۲، A زیرگروه نیست. این در حالی است که اگر قرار دهیم $B = \{a \in \mathbb{R} \mid |a| \in \mathbb{Q}\}$ آنگاه B زیرگروه است.*

مثال ۸.۴.۲. *می‌خواهیم تمام زیرگروه‌های $(\mathbb{Z}, +)$ را شناسایی کنیم. ادعا می‌کنیم تمام زیرگروه‌های $\mathbb{Z}$ با عمل دوتایی جمع به صورت*

$$n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}$$

است که در آن $n \in \mathbb{Z}$. واضح است که $0 \in n\mathbb{Z}$ و لذا $n\mathbb{Z}$ ناتهی است. حال فرض کنیم $nk, nk' \in \mathbb{Z}$. در گروه $\mathbb{Z}$ عنصر nk' دارای وارون $-nk'$ است و داریم

$$nk + (-nk') = nk - nk' = n(k - k') = nk''.$$

واضح است که $nk'' \in n\mathbb{Z}$. حال طبق قضیه ۵.۴.۲، $n\mathbb{Z}$ زیرگروه است. اکنون فرض کنیم H یک زیرگروه دلخواه از $\mathbb{Z}$ باشد. اگر $H = \{0\}$ باشد چیزی برای اثبات نداریم! فرض کنیم $H \neq \{0\}$. پس x ناصفری در H قرار دارد. H حتما شامل یک عنصر مثبت است. زیرا اگر x مثبت نبود آنگاه چون H عنصر خنثی 0 را دارد (چرا؟)، پس طبق قضیه ۵.۴.۲، $0 - x = -x$ که مثبت است در H قرار دارد. بنابراین فرض کنیم n کوچکترین عدد صحیح مثبت در H باشد (چرا چنین فرضی معتبر است؟). نشان می‌دهیم $H = n\mathbb{Z}$. چون $n \in H$ مشابه استدلال بالا داریم $-n \in H$ و لذا طبق قضیه ۵.۴.۲، $n - (-n) = n + n = 2n$ در H قرار دارد. این روند را تکرار کنید! پس هر مضربی از n در H قرار دارد و این یعنی $n\mathbb{Z} \subseteq H$. حال فرض کنیم $t \in H$ دلخواه باشد. طبق قضیه الگوریتم تقسیم، قضیه ۷.۲.۱، $t = nq + r$ که $0 \leq r < n$. طبق مطلبی که بالا نشان دادیم $nq \in H$. پس طبق قضیه ۵.۴.۲، $r = t - nq \in H$ و این کوچکترین بودن n را نقض می‌کند مگر این که $r = 0$. پس $t \in n\mathbb{Z}$ و $H \subseteq n\mathbb{Z}$.

قضیه زیر برای گروه‌های متناهی و زیرگروه بودن یک زیرمجموعه آن محک ساده‌تری ارائه می‌کند.

قضیه ۹.۴.۲. *فرض کنیم G گروه متناهی باشد. زیرمجموعه ناتهی H از G زیرگروه است اگر و تنها اگر برای هر $a, b \in H$ داشته باشیم $ab \in H$.*

اثبات. ($\Leftarrow$). فرض کنیم $a, b \in H$. چون H زیرگروه است نسبت به عمل القایی بسته است و لذا $ab \in H$.

($\Rightarrow$). ابتدا دقت شود که H ناتهی است. فرض کنیم $x, y \in H$. طبق فرض باید $xy \in H$ باشد.

پس H نسبت به عمل الحاقی بسته است. چون H زیرمجموعه G است شرکتپذیری از G به H ارث می‌رسد و لذا طبق تعریف H نیم‌گروه متناهی است. اگر $a, x, y \in H$ و $ax = ay$ آنگاه چون G گروه است داریم $a^{-1}ax = a^{-1}ay$ یعنی $x = y$. لذا حذف از چپ برقرار است. به صورت مشابه حذف از راست نیز برقرار است. حال طبق قضیه ۵۱.۲.۲ باید H با عمل الحاقی گروه باشد و این یعنی H زیرگروه G است. □

تذکر ۱۰.۴.۲. *متناهی بودن در قضیه قبل شرط اساسی است. زیرا برای هر $a, b \in \mathbb{N}$ داریم $ab \in \mathbb{N}$. اما می‌دانیم که $\mathbb{N}$ با عمل دوتایی ضرب معمولی یک گروه نیست.*

مثال ۱۱.۴.۲. *گروه $(\mathbb{Z}_m, +)$ را در نظر بگیرید. فرض کنیم $k \in \mathbb{N}$. در این صورت*

$$k\mathbb{Z}_m = \{\bar{k}\bar{i} \mid \bar{i} \in \mathbb{Z}_m\}$$

یک زیرگروه است. فرض کنیم $\bar{x}, \bar{y} \in k\mathbb{Z}_m$. پس $\bar{x} = \bar{k}\bar{i}$ و $\bar{y} = \bar{k}\bar{j}$. حال داریم

$$\bar{x} + \bar{y} = \bar{k}\bar{i} + \bar{k}\bar{j} = \bar{k}(\bar{i} + \bar{j}) = \overline{\bar{k}\overline{i+j}}$$

و لذا طبق قضیه ۹.۴.۲ زیرگروه بودن حاصل می‌شود.

اکنون گزاره زیر را داریم.

گزاره ۱۲.۴.۲. *فرض کنیم G یک گروه و $\{H_i\}_{i\in I}$ خانواده‌ای از زیرگروه‌های G باشد. در این صورت $H = \bigcap_{i\in I} H_i$ یک زیرگروه است.*

اثبات. می‌دانیم که برای هر $i \in I$، عنصر خنثی e عضوی از H_i است (چرا؟). لذا $e \in \bigcap_{i\in I} H_i$ و در نتیجه $e \in H$ و H ناتهی است. حال فرض کنیم که $a, b \in H$. پس برای هر $i \in I$ داریم $a, b \in H_i$. چون برای هر $i \in I$، H_i زیرگروه است باید $b^{-1} \in H_i$ (چرا؟). لذا برای هر $i \in I$ طبق قضیه ۵.۴.۲ داریم $ab^{-1} \in H_i$. این یعنی $ab^{-1} \in H$ و طبق قضیه ۵.۴.۲ باید $H \leq G$. □

تذکر ۱۳.۴.۲. *جالب است که اجتماع زیرگروه‌های لازم نیست که زیرگروه باشد. مثلا در گروه $(\mathbb{Z}, +)$ زیرگروه‌های $۲\mathbb{Z}$ و $۳\mathbb{Z}$ را در نظر بگیرید. در این صورت $۲, ۳ \in ۲\mathbb{Z} \cup ۳\mathbb{Z}$. اما داریم $۲ + ۳ = ۵ \notin ۲\mathbb{Z} \cup ۳\mathbb{Z}$.*

برای اجتماع زیرگروه‌های گزاره زیر را داریم.

گزاره ۱۴.۴.۲. *فرض کنیم G یک گروه و $H, K \leq G$. در این صورت $H \cup K$ زیرگروه است اگر و تنها اگر $H \subseteq K$ یا $K \subseteq H$.*

اثبات. ($\Leftarrow$). به برهان خلف فرض کنیم $K \not\subseteq H$ و $H \not\subseteq K$. حال عناصر $h \in H \setminus K$ و $k \in K \setminus H$ را در نظر می‌گیریم. اما واضح است که $h \in H \cup K$ و $k \in H \cup K$. لذا $hk \in H \cup K$ (چرا؟). اکنون باید $hk \in H$ یا $hk \in K$. اگر $hk \in H$ باشد آنگاه چون H

زیرگروه است داریم $h^{-1} \in H$ و لذا $h^{-1}hk = k \in H$ و این تناقض است. اگر $hk \in K$ باشد آنگاه چون K زیرگروه است داریم $k^{-1} \in K$ و لذا $hkk^{-1} = h \in K$ و این نیز تناقض است.
$(\Rightarrow)$. طبق فرض $H \cup K = H$ یا $H \cup K = K$ و چیزی برای اثبات نداریم. □

مثال ۱۵.۴.۲. *گروه چهارتایی کلاین $\mathbb{K}_4$ را به یاد آورید! قرار می‌دهیم*

$$A = \{e, a\} \qquad B = \{e, b\} \qquad C = \{e, c\}$$

در این صورت A، B و C با یک بررسی ساده زیرگروه‌های سره از $\mathbb{K}_4$ هستند و $\mathbb{K}_4 = A \cup B \cup C$.

سوال ۱۶.۴.۲. *آیا می‌توانیم گزاره قبل را برای اجتماع سه زیرگروه یا تعداد دلخواه زیرگروه تعمیم دهیم؟*

سوال ۱۷.۴.۲. *به نظر شما گروهی که اجتماع دو زیرگروه سره خود است، چگونه است؟ گروهی که اجتماع سه زیرگروه سره خود است، چطور؟*

در ادامه می‌خواهیم دو زیرگروه بسیار مهم از یک گروه را برای شما معرفی کنیم. با تعریف زیر شروع می‌کنیم.

تعریف ۱۸.۴.۲. *فرض کنیم G یک گروه باشد. به مجموعه*

$$Z(G) = \{x \in G \mid xa = ax \qquad \forall a \in G\}$$

مرکز گروه G گوییم.

مثال ۱۹.۴.۲. *اگر G یک گروه آبلی باشد آنگاه بسیار واضح است که $Z(G) = G$.*

مثال ۲۰.۴.۲. *اگر $G = S_3$ باشد آنگاه در بخش قبل دیده‌اید که S_3 یک گروه غیر آبلی است و با توجه به این که عناصر S_3 را می‌شناسیم می‌توان دید که اگر e عضو خنثی گروه S_3 باشد آنگاه $Z(S_3) = \{e\}$.*

مثال ۲۱.۴.۲. *اگر $G = \mathbb{Q}_8$ باشد آنگاه در بخش قبل دیده‌اید که $\mathbb{Q}_8$ یک گروه غیر آبلی است و با توجه به این که عناصر ان را می‌شناسیم می‌توان دید که $Z(\mathbb{Q}_8) = \{1, -1\}$.*

گزاره ۲۲.۴.۲. *برای هر گروه G داریم $Z(G) \leq G$.*

اثبات. واضح است که $e \in Z(G)$ و لذا $Z(G)$ ناتهی است. حال فرض کنیم $x, y \in Z(G)$. لذا برای هر $a \in G$ داریم $xa = ax$ و $ay = ya$. بنابراین برای هر $a \in G$

$$a(xy) = (ax)y = (xa)y = xay = x(ay) = x(ya) = xya = (xy)a.$$

درنتیجه $xy \in Z(G)$. چون برای هر $a \in G$ داریم $xa = ax$ پس با ضرب طرفین از راست در x^{-1} داریم $xax^{-1} = a$ و با ضرب طرفین تساوی آخر از سمت چپ در x^{-1} داریم $x^{-1}a = ax^{-1}$.
لذا $x^{-1} \in Z(G)$. حال طبق قضیه ۵.۴.۲ باید $Z(G) \leq G$. □

تعریف ۲.۴.۲۳. *فرض کنیم G یک گروه و A زیرمجموعه ناتهی از G باشد. به مجموعه*

$$C_G(A) = \{x \in G \mid xa = ax \qquad \forall a \in A\}$$

مرکزساز A در گروه G گوییم. اگر $A = \{a\}$ آنگاه به مجموعه

$$C_G(a) = \{x \in G \mid xa = ax\}$$

مرکزساز عنصر a در گروه G گوییم. اگر بیم ابهام نباشد از نمادهای $C(A)$ و $C(a)$ نیز استفاده می‌کنیم.

مثال ۲.۴.۲۴. *اگر G یک گروه با عنصر خنثی e باشد آنگاه بسیار واضح است که $C_G(e) = G$.*

مثال ۲.۴.۲۵. *اگر $G = S_۳$ باشد و*

$$\sigma = \begin{pmatrix} ۱ & ۲ & ۳ \\ ۱ & ۳ & ۲ \end{pmatrix}$$

آنگاه می‌خواهیم $C_{S_۳}(\sigma) = C(\sigma)$ را به دست آوریم. فرض کنیم

$$\tau = \begin{pmatrix} ۱ & ۲ & ۳ \\ a & b & c \end{pmatrix}$$

عنصری در $C(\sigma)$ باشد. پس داریم $\tau\sigma = \sigma\tau$. لذا

$$\tau\sigma = \begin{pmatrix} ۱ & ۲ & ۳ \\ a & c & b \end{pmatrix}.$$

حال اگر a برابر ۲ یا ۳ باشد با یک بررسی ساده تساوی $\tau\sigma = \sigma\tau$ نقض می‌شود و لذا باید $a = ۱$. اگر $b = ۲$ باشد انگاه $c = ۳$ است و لذا τ همان عنصر خنثی e از $S_۳$ است. اگر $b = ۳$ باشد آنگاه $c = ۲$ است یعنی $\sigma = \tau$ و تساوی $\sigma\tau = \sigma\tau$ حفظ می‌شود. لذا $C(\sigma) = \{e, \sigma\}$.

گزاره ۲.۴.۲۶. *برای هر گروه G و $\emptyset \neq A \subseteq G$ داریم $C_G(A) \leq G$.*

اثبات. واضح است که $e \in C_G(A)$ و لذا $C_G(A)$ ناتهی است. حال فرض کنیم $x, y \in C_G(A)$. لذا برای هر $a \in A$ داریم $xa = ax$ و $ay = ya$. بنابراین برای هر $a \in A$ نتیجه می‌شود که

$$a(xy) = (ax)y = (xa)y = xay = x(ay) = x(ya) = xya = (xy)a.$$

درنتیجه $xy \in C_G(A)$. اما برای هر $a \in A$ داریم $xa = ax$، پس با ضرب طرفین از راست در $x^{-۱}$ نتیجه می‌شود که $xax^{-۱} = a$ و با ضرب طرفین تساوی آخر از سمت چپ در $x^{-۱}$ داریم $ax^{-۱} = x^{-۱}a$. لذا $x^{-۱} \in C_G(A)$. حال طبق قضیه ۵.۴.۲ باید $C_G(a) \leq G$. □

تعریف ۲.۴.۲۷. *فرض کنیم G یک گروه باشد و $H, K \leq G$. منظور از HK یعنی*

$$\{hk \mid h \in H, \ \ k \in K\}.$$

مثال زیر نشان می‌دهد که لزومی ندارد HK زیرگروه باشد.

مثال ۲.۴.۲۸. *فرض کنیم $G = Gl_2(\mathbb{R})$ (عمل دوتایی ضرب عادی ماتریس است). دو زیرگروه G به صورت*

$$H = \{\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \mid x \in \mathbb{R}\} \qquad K = \{\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \ \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\}$$

را در نظر می‌گیریم. حال داریم

$$HK = \{\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}, \ \begin{pmatrix} x & 1 \\ 1 & 0 \end{pmatrix} \mid x \in \mathbb{R}\}.$$

اکنون

$$A = \{\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \qquad B = \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix}$$

اعضای HK هستند. اما BA عضوی از HK نیست. زیرا اعضای HK یک درایه صفر دارند اما BA اصلا درایه صفر ندارد. لذا HK زیرگروه G نیست!

حال گزاره زیر را داریم.

گزاره ۲.۴.۲۹. *فرض کنیم G یک گروه باشد و $H, K \leq G$. در این صورت HK زیرگروه است اگر و تنها اگر $HK = KH$.*

اثبات. ($\Leftarrow$). نشان می‌دهیم $KH \subseteq HK$. فرض کنیم $x \in KH$. لذا $x = kh$ که $k \in K$ و $h \in H$. اکنون طبق تمرین ۵۵.۲.۲ داریم $x^{-1} = h^{-1}k^{-1}$ و در نتیجه $x^{-1} \in HK$. اما طبق فرض HK زیرگروه است پس $x \in HK$ و این یعنی $KH \subseteq HK$. اکنون فرض کنیم $x \in HK$. چون HK زیرگروه است پس $x^{-1} \in HK$. فرض کنیم $x^{-1} = hk$ که $h \in H$ و $k \in K$. طبق تمرین ۵۶.۲.۲ و تمرین ۵۵.۲.۲ داریم که $x = (x^{-1})^{-1} = k^{-1}h^{-1} \in KH$. بنابراین $HK \subseteq KH$.

($\Rightarrow$). چون H و K زیرگروه هستند دارای عنصر خنثی e هستند و در نتیجه $e = ee \in HK$ و لذا HK ناتهی است. فرض کنیم $x, y \in HK$. بنابراین $x = ab$ و $y = uv$ که $u, a \in H$ و $b, v \in K$. می‌خواهیم قضیه ۵.۴.۲ را به کار ببریم. طبق تمرین ۵۵.۲.۲ داریم $xy^{-1} = abv^{-1}u^{-1}$. اما $bv^{-1} \in K$ پس $bv^{-1}u^{-1} \in KH$. لذا از فرض $bv^{-1}u^{-1} \in HK$. پس فرض کنیم $bv^{-1}u^{-1} = hk$ که $h \in H$ و $k \in K$. حال داریم

$$xy^{-1} = abv^{-1}u^{-1} = ahk = (ah)k = h'k \in HK.$$

اکنون طبق قضیه ۵.۴.۲ داریم $HK \leq G$. □

سوال ۳۰.۴.۲. *اگر H و K زیرگروه‌های گروه G باشند آنگاه می‌توان از $hk \in HK$ نتیجه گرفت که $h \in H$ و $k \in K$؟*

این بخش را با قضیه کاربردی و مهم زیر به پایان می‌رسانیم.

قضیه ۳۱.۴.۲. *فرض کنیم G گروه متناهی باشد و $H, K \leq G$. در این صورت همواره داریم $|HK| = \frac{|H|\,|K|}{|H \cap K|}$. این قضیه برای زیرگروه‌های متناهی از یک گروه نه لزوما متناهی نیز صادق است.*

اثبات. قرار می‌دهیم

$$f : H \times K \longrightarrow HK, \quad f((h,k)) = hk.$$

f یک تابع است (برسی کنید). اگر $x \in HK$ انگاه $x = hk$ که $h \in H$ و $k \in K$. در نتیجه $f((h,k)) = hk = x$. یعنی f یک تابع پوشا است. حال طبق قضیه ۲۲.۱.۱ داریم که $f^{-1}(x)$ ها که $x \in HK$ یک افراز است. لذا $H \times K = \bigcup_{x \in HK} f^{-1}(x)$. اکنون برای هر $x \in HK$ ادعا می‌کنیم $|f^{-1}(x)| = |H \cap K|$. فرض کنیم $x = hk \in HK$. اگر $y \in H \cap K$ آنگاه

$$f((hy, y^{-1}k)) = hyy^{-1}k = hk = x.$$

لذا $(hy, y^{-1}k) \in f^{-1}(x)$. در نتیجه

$$T = \{(hy, y^{-1}k) \mid y \in H \cap K\} \subseteq f^{-1}(x).$$

اکنون فرض کنیم $(a,b) \in f^{-1}(x)$. پس

$$ab = f((a,b)) = x = hk = f((h,k)).$$

لذا با ضرب‌های مناسب از سمت چپ و راست داریم $h^{-1}a = kb^{-1}$. واضح است که $h^{-1}a \in H$ و $kb^{-1} \in K$. پس باید $h^{-1}a = kb^{-1} = y \in H \cap K$. بنابراین از $h^{-1}a = y$ نتیجه می‌شود $a = hy$ و از $kb^{-1} = y$ نتیجه می‌شود $b = y^{-1}k$. یعنی $(a,b) = (hy, y^{-1}k)$ و لذا $f^{-1}(x) \subseteq T$. بنابراین $f^{-1}(x) = T$. اما واضح است که $|T| = |H \cap K|$. پس ادعا اثبات می‌شود. حال چون H و K متناهی هستند، داریم $|H \times K| = |H|\,|K|$. بنابراین طبق قضیه ۱۴.۱.۱ داریم

$$|H|\,|K| = |H \times K| = \sum_{x \in HK} |f^{-1}(x)| =$$
$$\sum_{x \in HK} |H \cap K| = |HK|\,|H \cap K|$$

و اثبات کامل است. □

مثال ۳۲.۴.۲. *فرض کنیم G یک گروه متناهی باشد و $|G|= n$. اگر H و K دو زیرگروه G باشند که تعداد اعضای آنها از $\sqrt{n}$ بیشتر باشد آنگاه حتما H و K اشتراک غیر بدیهی دارند یعنی $H \cap K \neq \{e\}$. زیرا طبق قضیه ۳۱.۴.۲ داریم*

$$n \geq |HK|= \frac{|H|\,|K|}{|H \cap K|} > \frac{n}{|H \cap K|}$$

و لذا باید $H \cap K \neq \{e\}$.

تمرین‌های حل شده

تمرین ۳۳.۴.۲. *زیرگروه‌های $(\mathbb{Z}_۶, +)$ را بنویسید.*

حل. واضح است که $\{\bar{۰}\}$ و $\mathbb{Z}_۶$ دو زیرگروه بدیهی هستند. دو مجموعه

$$۲\bar{Z}_۶ = \{\bar{۰}, \bar{۲}, \bar{۴}\} \qquad ۳\bar{Z}_۶ = \{\bar{۰}, \bar{۳}\}$$

نیز با یک بررسی ساده زیرگروه هستند. حال فرض کنیم H زیرگروه متمایز از زیرگروه‌های باشد که شناسایی کرده‌ایم. پس H باید شامل $\bar{۱}$ یا $\bar{۵}$ باشد. اگر شامل $bar۱$ باشد آنگاه H برابر $\mathbb{Z}_۶$ است. زیرا H زیرگروه است پس $\bar{۲} = \bar{۱} + \bar{۱}$ در H قرار دارد. همینطور $\bar{۳} = \bar{۱} + \bar{۲}$ در H قرار دارد. با ادامه این روند H باید خود گروه باشد و این تناقض است. اگر H شامل $\bar{۵}$ باشد آنگاه $\bar{۴} = \bar{۵} + \bar{۵}$ عضو H است. همینطور $\bar{۳} = \bar{۴} + \bar{۵}$ در H قرار دارد. با تکرار این روند باید H خود گروه باشد که باز تناقض است. پس تمام زیرگروه‌ها شناسایی شد!

تمرین ۳۴.۴.۲. *فرض کنیم G یک گروه متناهی باشد و H زیرمجموعه ناتهی باشد. اگر $HH = H$ آنگاه نشان دهید که $H \leq G$.*

حل. فرض کنیم $a, b \in H$. واضح است که $ab \in HH$ و لذا طبق فرض $ab \in H$. حال طبق قضیه ۹.۴.۲ باید $H \leq G$.

تمرین ۳۵.۴.۲. *فرض کنیم G یک گروه باشد و $H \leq G$. نشان دهید که برای $x \in G$،*

$$T = xHx^{-۱} = \{xhx^{-۱} \mid h \in H\}$$

زیرگروه G است و $|H|= |xHx^{-۱}|$.

حل. فرض کنیم $a, b \in T$. پس $a = xhx^{-۱}$ و $b = xh'x^{-۱}$ که $h, h' \in H$. طبق تمرین ۵۵.۲.۲ و تمرین ۵۶.۲.۲ داریم که $b^{-۱} = (x^{-۱})^{-۱}h'^{-۱}x^{-۱} = xh'^{-۱}x^{-۱}$. پس

$$ab^{-۱} = xhx^{-۱}xh'^{-۱}x^{-۱} = xhh'^{-۱}x^{-۱} = xh''x^{-۱} \in T$$

و لذا طبق قضیه ۵.۴.۲ زیرگروه بودن T حاصل می‌شود. برای قسمت دوم، تعریف می‌کنیم

$$f : H \longrightarrow T, \quad f(h) = xhx^{-1}.$$

بررسی کنید که f یک تابع خوشتعریف است. اگر $x = xhx^{-1} \in T$ آنگاه $f(h) = x$ و این یعنی f پوشا است. اگر $f(h) = f(h')$ آنگاه $xhx^{-1} = xh'x^{-1}$. با ضرب طرفین تساوی آخر از سمت چپ در x^{-1} و از سمت راست در x به دست می‌آید که $h = h'$. یعنی f یک‌به‌یک است. لذا $|H| = |xHx^{-1}|$.

تمرین ۳۶.۴.۲. *فرض کنیم H زیرگروهی از گروه G باشد. نشان دهید که برای $a \in G$، $Ha = H$ اگر و تنها اگر $a \in H$.*

حل. فرض کنیم $Ha = H$. چون H زیرگروه است دارای عنصر خنثی e است. لذا طبق فرض $ea \in H$ و درنتیجه $a \in H$.
اکنون فرض کنیم $a \in H$. اگر $h \in H$ آنگاه چون H زیرگروه است داریم $ha \in H$. بنابراین به وضوح $Ha \subseteq H$. اما a^{-1} و ha^{-1} عضو H هستند، به این دلیل که H زیرگروه است. پس برای هر $h \in H$ داریم $h = he = ha^{-1}a = (ha^{-1})a \in Ha$. لذا $H \subseteq Ha$ و اثبات کامل است.

تمرین ۳۷.۴.۲. *برای گروه G نشان دهید که $Z(G) = \bigcap_{a \in G} C_G(a)$.*

حل. فرض کنیم $x \in \bigcap_{a \in G} C_G(a)$. پس برای هر $a \in G$ داریم $x \in C_G(a)$. پس برای هر $a \in G$ داریم $xa = ax$. لذا $x \in Z(G)$ و در نتیجه $\bigcap_{a \in G} C_G(a) \subseteq Z(G)$.
فرض کنیم $x \in Z(G)$. پس برای هر $a \in G$ داریم $xa = ax$. چون x با a جابجا می‌شود داریم $x \in C_G(a)$ و در نتیجه $Z(G) \subseteq \bigcap_{a \in G} C_G(a)$ و اثبات کامل است.

تمرین ۳۸.۴.۲. *مرکز گروه S_n را به دست آورید.*

حل. طبق تمرین ۶۳.۲.۲، اگر $n \leq ۲$ باشد آنگاه S_n آبلی است و لذا $Z(S_n) = S_n$.
فرض کنیم $n \geq ۳$ و $e \neq \sigma \in S_n$. چون σ عنصر خنثی نیست، پس عناصر متمایز i و j در $\{۱, ۲, ..., n\}$ چنان وجود دارند که $\sigma(i) = j$. حال چون $n \geq ۳$ است می‌توانیم $l \neq j$ را در $\{۱, ۲, ..., n\}$ و عنصر $\tau \in S_n$ را چنان انتخاب کنیم که $\tau(j) = l$ و $\tau(i) = i$. اکنون داریم

$$l = \tau(j) = \tau(\sigma(i)) = \tau\sigma(i) = \sigma\tau(i) = \sigma(\tau(i)) = \sigma(i) = j$$

که تناقض آشکار است. پس σ عنصر خنثی است و $Z(S_n) = \{e\}$.

تمرین ۳۹.۴.۲. *فرض کنیم G یک گروه ۱۲ عضوی باشد و $H, K \leq G$. اگر $H \cap K = \{e\}$، $|H| = ۲$ و $|K| = ۶$ باشد آنگاه نشان دهید که $G = HK$.*

حل. طبق قضیه ۳۱.۴.۲ داریم

$$|HK| = \frac{|H|\,|K|}{|H \cap K|} = ۱۲$$

و چون $HK \subseteq G$، لذا باید $G = HK$.

تمرین ۴۰.۴.۲. *فرض کنیم G یک گروه آبلی باشد و $H, K \leq G$. اگر $H \cup K = HK$ آنگاه نشان دهید که $H \subseteq K$ یا $K \subseteq H$.*

حل. فرض کنیم $hk \in HK$. چون G آبلی است پس باید $hk = kh$ باشد. لذا $HK \subseteq KH$ و $KH \subseteq HK$. یعنی $KH = HK$ و طبق گزاره ۲۹.۴.۲ باید HK زیرگروه باشد. چون $H \cup K = HK$ است پس طبق گزاره ۱۴.۴.۲ باید $H \subseteq K$ یا $K \subseteq H$.

تمرین ۴۱.۴.۲. *فرض کنیم G یک گروه، H و K زیرگروه‌های متناهی از G باشند. نشان دهید که $H \cap K = \{e\}$ اگر و تنها اگر $|HK| = |H|\,|K|$.*

حل. فرض کنیم $H \cap K = \{e\}$. بنابراین $|H \cap K| = ۱$ و لذا طبق قضیه ۳۱.۴.۲ داریم $|HK| = |H|\,|K|$.
برای برعکس، به برهان خلف، فرض کنیم $H \cap K \neq \{e\}$. لذا $|H \cap K| > ۱$. در نتیجه طبق قضیه ۳۱.۴.۲ داریم

$$|H|\,|K| = |HK| = \frac{|H|\,|K|}{|H \cap K|}$$

و این تناقض آشکار است.

۵.۲ مولد یک گروه و گروه‌های دوری

در این بخش می‌خواهیم ببینیم که آیا می‌شود با داشتن تعداد منتخبی از عناصر یک گروه، تمام گروه را تولید کرد. اگر چنین اتفاقی رخ دهد مطالعه گروه کمی ساده می‌شود.

تعریف ۱.۵.۲. *فرض کنیم G یک گروه باشد و X یک زیرمجموعه از G باشد. در این صورت اشتراک همه زیرگروه‌های G که شامل X هستند را با $< X >$ نمایش می‌دهیم، یعنی*

$$< X >= \bigcap_{X \subseteq H \leq G} H.$$

دو نکته مهم را باید مد نظر قرار دهیم. اول اینکه اشتراک بالا بامعنی است. زیرا دست کم خود G شامل X است. دوم اینکه طبق گزاره ۱۲.۴.۲، $< X >$ یک زیرگروه از G است. از این رو به $< X >$ زیرگروه تولید شده توسط X گوییم. اگر $X = \emptyset$ آنگاه قرار می‌دهیم $< X >= \{e\}$.

مثال ۲.۵.۲. *گروه $G = (\mathbb{Z}, +)$ را در نظر بگیرید. فرض کنیم $X = \{۲\}$. با توجه به مثال ۸.۴.۲ می‌دانیم تمام زیرگروه‌های G به صورت $n\mathbb{Z}$ است. لذا تنها زیرگروه G که شامل X باشد به صورت $۲\mathbb{Z}$ است. پس $< X >= ۲\mathbb{Z}$.*

مثال ۳.۵.۲. *گروه $G = (\mathbb{Z}, +)$ را در نظر بگیرید. فرض کنیم $X = \{۲, ۴\}$. با توجه به مثال ۸.۴.۲ می‌دانیم تمام زیرگروه‌های G به صورت $n\mathbb{Z}$ است. لذا زیرگروه‌های G که شامل X باشد به صورت $۲\mathbb{Z}$ یا $۴\mathbb{Z}$ است. پس $< X >= ۴\mathbb{Z}$.*

مثال‌های بالا این تصور را به وجود می‌آورد که شناسایی $< X >$ کار ساده‌ای نیست و باید تسلط روی تمام زیرگروه‌های یک گروه داشت. اما این تصور اشتباه است! در ادامه نتایجی را خواهیم آورد که شناسایی $< X >$ آسانتر شود.

لم ۴.۵.۲. *فرض کنیم G یک گروه باشد و $X \subseteq G$. در این صورت $< X >$ (نسبت به رابطه $\subseteq$) کوچکترین زیرگروه G است که شامل X است.*

اثبات. فرض کنیم K زیرگروهی از G باشد که $X \subseteq K$. پس K حتما در اشتراک $\bigcap_{X \subseteq H \leq G} H$ ظاهر شده است. لذا $< X > \subseteq K$ و این یعنی $< X >$ کوچکترین زیرگروه G است که شامل X است. □

قضیه زیر برای محاسبه $< x >$ کمک کننده است.

قضیه ۵.۵.۲. *اگر G یک گروه باشد و $\emptyset \neq X \subseteq G$ آنگاه*

$$< X >= \{x_۱^{\epsilon_۱} x_۲^{\epsilon_۲} ... x_n^{\epsilon_n} \mid x_i \in X,\ \epsilon_i \in \{-۱, ۱\},\ n \in \mathbb{N}\}.$$

اثبات. برای راحتی فرض کنیم

$$T = \{x_۱^{\epsilon_۱} x_۲^{\epsilon_۲} ... x_n^{\epsilon_n} \mid x_i \in X,\ \epsilon_i \in \{-۱, ۱\},\ n \in \mathbb{N}\}.$$

باید نشان دهیم $T =< X >$. نشان می‌دهیم که $T \leq G$. واضح است که $X \subseteq T$. زیرا قرار می‌دهیم $n = ۱$ و $\epsilon_۱ = ۱$. لذا T ناتهی است. حال فرض کنیم $a, b \in T$. پس

$$a = x_۱^{\epsilon_۱} x_۲^{\epsilon_۲} ... x_n^{\epsilon_n} \qquad b = y_۱^{\epsilon'_۱} y_۲^{\epsilon'_۲} ... y_n^{\epsilon'_m}$$

حال واضح است که طبق تمرین ۵۵.۲.۲ داریم

$$b^{-۱} = y_m^{-\epsilon'_m} ... y_۲^{-\epsilon'_۲} y_۱^{-\epsilon'_m}.$$

چون $-\epsilon_j \in \{-۱, ۱\}$ لذا

$$ab^{-۱} = x_۱^{\epsilon_۱} x_۲^{\epsilon_۲} ... x_n^{\epsilon_n} y_m^{-\epsilon'_m} ... y_۲^{-\epsilon'_۲} y_۱^{-\epsilon'_m}$$

نیز به شکل اعضای T است یعنی $ab^{-۱} \in T$. بنابراین طبق قضیه ۵.۴.۲، T یک زیرگروه شامل X است. لذا طبق لم ۴.۵.۲ باید $< X > \subseteq T$.
حال فرض کنیم

$$a = x_۱^{\epsilon_۱} x_۲^{\epsilon_۲} ... x_n^{\epsilon_n} \in T.$$

چون $X \subseteq < X >$ پس برای هر j که $\epsilon_j = ۱$ باشد، داریم $x_j^{\epsilon_j} \in X \subseteq < X >$. اگر $\epsilon_j = -۱$ آنگاه $x_j^{-\epsilon_j} \in X \subseteq < X >$. چون $< X >$ زیرگروه است پس $x_j^{\epsilon_j} \in < X >$. دوباره چون $< X >$ زیرگروه است پس نسبت به عمل دوتایی بسته است لذا $a \in < X >$ و $T \subseteq < X >$. اثبات کامل است. □

مثال ۶.۵.۲. *گروه $G = (\mathbb{Z}, +)$ را در نظر بگیرید. فرض کنیم $X = \{۱\}$. حال طبق قضیه ۵.۵.۲ و این مطلب که گروه جمعی است، داریم*

$$< X >= \{\epsilon_۱ x_۱ + \epsilon_۲ x_۲ + ... + \epsilon_n x_n \mid x_i \in X,\ \epsilon_i \in \{-۱, ۱\},\ n \in \mathbb{N}\} =$$
$$\{\underbrace{\pm ۱ \pm ۱ \pm ... \pm ۱}_{\text{تا } n} \mid n \in \mathbb{N}\} = \{m \mid m \in \mathbb{Z}\} = \mathbb{Z}.$$

مثال ۷.۵.۲. *گروه $G = (\mathbb{Z}, +)$ را در نظر بگیرید. فرض کنیم $X = \{۲\}$. حال طبق قضیه ۵.۵.۲ و این مطلب که گروه جمعی است، داریم*

$$< X >= \{\epsilon_۱ x_۱ + \epsilon_۲ x_۲ + ... + \epsilon_n x_n \mid x_i \in X,\ \epsilon_i \in \{-۱, ۱\},\ n \in \mathbb{N}\} =$$
$$\{\underbrace{\pm ۲ \pm ۲ \pm ... \pm ۲}_{\text{تا } n} \mid n \in \mathbb{N}\} = \{۲m \mid m \in \mathbb{Z}\} = ۲\mathbb{Z}.$$

مثال ۸.۵.۲. *گروه* $G = (GL_۲(\mathbb{R}), .)$ *را در نظر بگیرید. فرض کنیم* $X = \{\begin{pmatrix} ۲ & ۰ \\ ۰ & ۱ \end{pmatrix}\}$. *حال طبق قضیه* ۵.۵.۲ *و این مطلب که گروه ضربی است، داریم*

$$< X >= \{x_۱^{\epsilon_۱} x_۲^{\epsilon_۲} ... x_n^{\epsilon_n} \mid x_i \in X,\ \epsilon_i \in \{-۱, ۱\},\ n \in \mathbb{N}\} =$$

$$\{\underbrace{\begin{pmatrix} ۲ & ۰ \\ ۰ & ۱ \end{pmatrix}^{\pm ۱} \begin{pmatrix} ۲ & ۰ \\ ۰ & ۱ \end{pmatrix}^{\pm ۱} ... \begin{pmatrix} ۲ & ۰ \\ ۰ & ۱ \end{pmatrix}^{\pm ۱}}_{\text{ن}n} \mid n \in \mathbb{N}\} =$$

$$\{\begin{pmatrix} ۲ & ۰ \\ ۰ & ۱ \end{pmatrix}^{m} \mid m \in \mathbb{Z}\} = \{\begin{pmatrix} ۲^m & ۰ \\ ۰ & ۱ \end{pmatrix} \mid m \in \mathbb{Z}\}.$$

نمادگذاری ۹.۵.۲. *اگر* $X = \{x_۱, ..., x_n\}$ *باشد آنگاه* $< X >$ *را با* $< x_۱, ..., x_n >$ *نمایش می‌دهیم.*

حال نتیجه زیر را داریم.

نتیجه ۱۰.۵.۲. *فرض کنیم* G *یک گروه باشد و* $\emptyset \neq X \subseteq G$.
(۱) *اگر* G *یک گروه آبلی باشد آنگاه*

$$< X >= \{x_۱^{k_۱} x_۲^{k_۲} ... x_n^{k_n} \mid x_i \in X,\ x_i \neq x_j,\ k_i \in \mathbb{Z},\ n \in \mathbb{N}\}.$$

(۲) *اگر* $X = \{x_۱, x_۲, ..., x_n\}$ *و* G *آبلی باشد آنگاه برای گروه ضربی داریم*

$$< x_۱, x_۲, ..., x_n >= \{x_۱^{k_۱} x_۲^{k_۲} ... x_n^{k_n} \mid k \in \mathbb{Z}\}$$

و برای گروه جمعی داریم

$$< x_۱, x_۲, ..., x_n >= \{k_۱x_۱ + k_۲x_۲ + ... + k_nx_n \mid k \in \mathbb{Z}\}.$$

(۳) *اگر* $X = \{x\}$ *و* G *آبلی باشد آنگاه برای گروه ضربی داریم*

$$< x >= \{x^k \mid k \in \mathbb{Z}\}$$

و برای گروه جمعی داریم

$$< x >= \{kx \mid k \in \mathbb{Z}\}.$$

اثبات. (۱) چون گروه آبلی است آنقدر اعضا را جابجا می‌کنیم تا مشابه‌ها کنار هم قرار بگیرند و دیگر مشابه‌ای در مکان دیگری نباشد. حال طبق قضیه ۴۴.۲.۲ توان‌ها جمع می‌شوند و عددی صحیح خواهند بود.
(۲) نتیجه مستقیم (۱) است.
(۳) نتیجه مستقیم (۲) است. □

اکنون مثال‌های زیر را دنبال کنید.

مثال ۱۱.۵.۲. *گروه $G = (\mathbb{Z}, +)$ را در نظر بگیرید. فرض کنیم $X = \{۲, ۳\}$. واضح است که G آبلی طبق نتیجه ۱۰.۵.۲ داریم*

$$< ۲, ۳ >= \{۲k + ۳k' \mid k, k' \in \mathbb{Z}\} = \mathbb{Z}.$$

مثال ۱۲.۵.۲. *گروه $G = (\mathbb{Z}, +)$ را در نظر بگیرید. فرض کنیم $X = \{۲, ۴, ۶\}$. واضح است که G آبلی طبق نتیجه ۱۰.۵.۲ داریم*

$$< ۲, ۴, ۶ >= \{۲k + ۴k' + ۶k'' \mid k, k', k'' \in \mathbb{Z}\} =$$
$$\{۲(k + ۲k' + ۳k'') \mid k, k', k'' \in \mathbb{Z}\} = ۲\mathbb{Z}.$$

مثال ۱۳.۵.۲. *گروه $G = \mathbb{Q}_۸$ را در نظر بگیرید. فرض کنیم $X = \{i\}$. این گروه غیر آبلی است و چون $i^{۲} = i^{-۲} = -۱$ پس $i^{۴} = i^{-۴} = ۱$ و $i^{۳} = i^{-۳} = -i$. بنابراین*

$$< X >= \{x^k \mid k \in \mathbb{Z}\} = \{i^k \mid k \in \mathbb{Z}\} = \{۱, -۱, i, -i\}.$$

گزاره ۱۴.۵.۲. *برای هر گروه G و $x \in G$ همواره $< x >$ آبلی است.*

اثبات. فرض کنیم $a, b \in < x >$. پس طبق نتیجه ۱۰.۵.۲ اعداد صحیح k و k' وجود دارند که $a = x^k$ و $b = x^{k'}$. لذا داریم

$$ab = x^k x^{k'} = x^{k+k'} = x^{k'+k} = x^{k'} x^k = ba$$

و اثبات تمام است. □

تعریف ۱۵.۵.۲. *فرض کنیم G یک گروه باشد و $X \subseteq G$. گوییم X مجموعه مولد برای G هرگاه $G =< X >$. همچنین*
(الف) اگر $|X| = ۱$ باشد آنگاه به $< x >$ زیرگروه دوری گوییم.
(ب) اگر $|X| < \infty$ باشد آنگاه به $< X >$ زیرگروه متناهیا تولید شده گوییم.
(ج) اگر $|X| = ۱$ باشد و $G =< x >$ آنگاه به G گروه دوری گوییم.
(د) اگر $|X| < \infty$ باشد و $G =< X >$ آنگاه به G گروه متناهیا تولید شده گوییم.

مثال ۱۶.۵.۲. *گروه $(\mathbb{Z}, +)$ دوری است. زیرا $\mathbb{Z} =< ۱ >$.*

مثال ۱۷.۵.۲. *گروه $(\mathbb{Z}_۴, +)$ دوری است. زیرا $\mathbb{Z}_۴ =< \bar{۱} >$.*

مثال ۱۸.۵.۲. *گروه جمعی $G = \mathbb{Z} \times \mathbb{Z}$ دوری نیست. به برهان خلف، فرض کنیم که داشته باشیم $G =< (a,b) >$. پس طبق نتیجه ۱۰.۵.۲ داریم*

$$< (a,b) >= \{k(a,b) \mid k \in \mathbb{Z}\} = \{(ka,kb) \mid k \in \mathbb{Z}\}.$$

اما واضح است که $(۱,۰) \in G$. پس عدد صحیح k چنان وجود دارد که $(ka,kb) = (۱,۰)$. پس $kb = ۰$ و لذا باید $b = ۰$. اما واضح است که $(۰,۱) \in G$. پس عدد صحیح k چنان وجود دارد که $(ka,kb) = (۰,۱)$. پس $ka = ۰$ و لذا باید $a = ۰$. بنابراین $\mathbb{Z} \times \mathbb{Z} =< (۰,۰) >$ این تناقض آشکار است.

مثال ۱۹.۵.۲. *گروه جمعی $G = \mathbb{Z} \times \mathbb{Z}$ متناهیا تولید شده است. زیرا این گروه آبلی است و طبق نتیجه ۱۰.۵.۲ داریم*

$$< (۱,۰),(۰,۱) >= \{k_۱(۱,۰) + k_۲(۰,۱) \mid k_۱,k_۲ \in \mathbb{Z}\} =$$
$$\{(k_۱,۰) + (۰,k_۲) \mid k_i \in \mathbb{Z}\} = \{(k_۱,k_۲) \mid k_۱,k_۲ \in \mathbb{Z}\} = \mathbb{Z} \times \mathbb{Z}.$$

مثال ۲۰.۵.۲. *گروه آبلی جمعی $G = \mathbb{Q}$ متناهیا تولید شده نیست. به برهان خلف فرض کنیم که $G =< \frac{m_۱}{n_۱}, ..., \frac{m_t}{n_t} >$. چون اعداد اول نامتناهی هستند، می‌توانیم عدد اول p را چنان انتخاب کنیم که $p \nmid n_i$. اما $\frac{۱}{p} \in G$ و لذا طبق نتیجه ۱۰.۵.۲ داریم $\frac{۱}{p} = k_۱\frac{m_۱}{n_۱} + ... + k_t\frac{m_t}{n_t}$ که $k_i \in \mathbb{Z}$.*

$$\frac{۱}{p} = k_۱\frac{m_۱}{n_۱} + ... + k_t\frac{m_t}{n_t} = \frac{k_۱m_۱n_۲...n_t + ... + k_tm_tn_۱...n_{t-۱}}{n_۱...n_t} = \frac{s}{n_۱...n_t}$$

لذا $n_۱...n_t = ps$ و اندیس i چنان وجود دارد که $p|n_i$ و این تناقض است.

تذکر ۲۱.۵.۲. *واضح است که برای هر گروه G داریم $G =< G >$. لذا هر گروه مجموعه مولد دارد، دست کم خودش!*

حال این بخش را با قضیه مهم زیر را پایان می‌بریم.

قضیه ۲۲.۵.۲. *هر زیرگروه از یک گروه دوری G، دوری است.*

اثبات. فرض کنیم $G =< x >$ که $x \in G$ و $H \leq G$. اگر H زیرگروه بدیهی باشد انگاه چیزی برای اثبات نداریم. فرض کنیم H زیرگروه سره باشد. چون H زیرگروه است پس ناتهی است. از طرفی $H \subseteq G$ پس طبق نتیجه ۱۰.۵.۲، H دارای عضوی به شکل x^i است که $i \in \mathbb{Z}$. چون H زیرگروه است پس x^{-i} هم در H قرار دارد. در نتیجه می‌توانیم فرض کنیم کوچکترین عدد صحیح مثبت k وجود دارد که $x^k \in H$ (چگونه؟). ادعا می‌کنیم $H =< x^k >$. طبق لم ۴.۵.۲ واضح است که $H \supseteq < x^k >$. فرض کنیم $y \in H$. لذا $y = x^j$ چرا که $H \subseteq G$. طبق الگوریتم تقسیم، قضیه ۷.۲.۱، داریم $j = kq + r$ که $۰ \leq r < k$. اما داریم

$$x^r = x^{j-kq} = x^jx^{-kq} = x^j(x^q)^{-k}.$$

سمت راست تساوی بالا در H قرار دارد (چرا؟). در نتیجه $x^r \in H$. این تناقض با انتخاب ما از k دارد و لذا باید $r = 0$. بنابراین $y = x^j = x^{kq} = (x^k)^q \in < x >$ و $H \subseteq < x^k >$. اثبات کامل است. □

شاید برای شما این سوال ایجاد شود که آیا زیرگروه یک گروه متناهیا تولید شده، متناهیا تولید شده است؟ در پاسخ به این سوال باید همین قدر اشاره کنیم که خیر اینگونه نیست! ساختن چنین مثالی نیاز به داشتن اطلاعاتی بیشتر در مورد گروه‌ها دارد! خواننده علاقمند می‌تواند با دیدن گروه‌های آزاد در مراجع انتهای جزوه یا اینترنت به راحتی چنین مثالی را ارائه کند. هر چند در بخش تمرینات حل شده این بخش با پذیرفتن یک مطلب از نظریه گروه مثالی را ارائه کرده‌ایم.

تمرین‌های حل شده

تمرین ۲۳.۵.۲. *نشان دهید که زیرگروه‌های متناهیا تولید شده $\mathbb{Q}$ دوری هستند.*

حل. فرض کنیم $H =< \frac{n_1}{m_1}, ..., \frac{n_t}{m_t} >$ زیرگروه $\mathbb{Q}$ باشد. قرار می‌دهیم که $x = m_1 m_2 ... m_t$. ادعا می‌کنیم که $H \leq < \frac{1}{x} >$. داریم

$$\frac{n_i}{m_i} = n_i m_1 m_2 ... m_{i-1} m_{i+1} ... m_t \ \frac{1}{x}.$$

پس هر مولد H در $< \frac{1}{x} >$ قرار دارد پس $H \leq < \frac{1}{x} >$. اما طبق قضیه ۲۲.۵.۲ باید H دوری باشد.

تمرین ۲۴.۵.۲. *برای دو عدد صحیح k و m نشان دهید که گروه $G = m\mathbb{Z} + k\mathbb{Z}$ با m و $k + 7m$ تولید می‌شود.*

حل. واضح است که $m \in m\mathbb{Z} \subseteq m\mathbb{Z} + k\mathbb{Z}$. همچنین $7m + k \in m\mathbb{Z} + k\mathbb{Z}$. لذا $< m, k + 7m > \subseteq G$. فرض کنیم $ma + kb \in G$. داریم

$$ma + kb = (a - 7b)m + b(k + 7m).$$

لذا $ma + kb \in < m, k + 7m >$. بنابراین $G =< m, k + 7m >$.

تمرین ۲۵.۵.۲. *فرض کنیم G گروهی باشد که اصلا زیرگروه سره نابدیهی ندارد. نشان دهید که G دوری است. یک مثال از چنین گروهی را ارائه نمایید.*

حل. اگر $G = \{e\}$ چیزی برای اثبات نداریم. فرض کنیم $G \neq \{e\}$ و $x \in G$ یک عنصر مخالف عنصر خنثی باشد. حال واضح است که $< x >$ زیرگروه G است و $< x > \neq \{e\}$. طبق فرض باید $G =< x >$. برای قسمت دوم، کافی است گروه $G = (\mathbb{Z}_2, +)$ در نظر بگیریم (حتی برای هر عدد اول p، $G = (\mathbb{Z}_p, +)$).

تمرین ۲۶.۵.۲. *فرض کنیم H زیرگروهی از گروه G باشد که توسط دو عنصر x و y تولید شده است. نشان دهید که اگر $xy = yx$ آنگاه H آبلی است.*

حل. طبق فرض داریم که $H =< x, y >$. فرض کنیم $a, b \in H$. طبق قضیه ۵.۵.۲ داریم

$$a = x^{\epsilon_1} y^{\epsilon_2} ... x^{\epsilon_{n-1}} y^{\epsilon_n} \qquad (\epsilon_i \in \{-1, 1\},\ n \in \mathbb{N})$$
$$b = x^{\epsilon'_1} y^{\epsilon'_2} ... x^{\epsilon'_{n-1}} y^{\epsilon'_n} \qquad (\epsilon'_i \in \{-1, 1\},\ n \in \mathbb{N})$$

چون $xy = yx$ پس با تعدادی جابجایی مناسب داریم

$$a = x^s y^l \qquad b = x^{s'} y^{l'} \qquad (s, l, s', l' \in \mathbb{Z})$$

لذا دوباره با کمک $xy = yx$ و تعداد جابجایی مناسب داریم

$$ab = x^s y^l x^{s'} y^{l'} = x^s x^{s'} y^l y^{l'} = x^{s+s'} y^{l+l'} = x^{s'} x^s y^{l'} y^l = x^{s'} y^{l'} x^s y^l = ba.$$

تمرین ۲۷.۵.۲. *برای زیرگروه سره H از گروه G نشان دهید که $G =< G \setminus H >$.*

حل. واضح است که $G = H \cup < G \setminus H >$. بنابراین طبق گزاره ۱۴.۴.۲ داریم که $H \subseteq < G \setminus H >$ یا $< G \setminus H > \subseteq H$. اگر $< G \setminus H > \subseteq H$ آنگاه $G = H$ و این تناقض با فرض است. پس $H \subseteq < G \setminus H >$ و لذا $G =< G \setminus H >$.
پس

تمرین ۲۸.۵.۲. *با دانسته فرض کردن مطلب زیر یک گروه متناهیا تولید شده چنان ارائه کنید که یک زیرگروه آن متناهیا تولید شده نباشد.*
"گروه G متناهیا تولید شده است اگر و تنها اگر برای هر زنجیر از زیرگروه‌های G به شکل

$$H_0 \leq H_1 \leq H_2 \leq H_3 \leq ...$$

عدد طبیعی n موجود باشد که $H_n = H_{n+1} = ...$، یعنی زنجیر متوقف شود."

حل. در گروه ضربی $GL_2(\mathbb{R})$ دو ماتریس زیر را در نظر می‌گیریم

$$A = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \qquad B = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

و قرار می‌دهیم $G =< A, B >$ که گروهی متناهیا تولید شده است. حال فرض کنیم H مجموعه همه آن اعضا از G باشد که روی قطر اصلی آنها درایه ۱ قرار دارد. H ناتهی است. زیرا ماتریس همانی را دارد و یک بررسی ساده با کمک قضیه ۵.۴.۲ نشان می‌دهد که H زیرگروه است. همچنین برای هر $n \in \mathbb{W}$، $A^n B A^{-n} = A^n B (A^{-1})^n$ یک عضو از H است (بررسی کنید). دقت کنید که A وارونپذیر است. اما داریم

$$A^{n+1} B A^{-(n+1)} = A^{n+1} B A^{-n-1} = A(A^n B A^{-n}) A^{-1}.$$

این نشان می‌دهد که $< A^{n+1} B A^{-(n+1)} > \leq < A^n B A^{-n} >$. حال قرار می‌دهیم $H_i =< A^i B A^{-i} >$. حال زنجیر زیر از زیرگروه‌های H به شکل

$$H_0 \leq H_1 \leq H_2 \leq H_3 \leq ...$$

متوقف نمی‌شود. پس H متناهیا تولید شده نیست.

۶.۲ مرتبه گروه و عناصر گروه

در این بخش ابزاری را معرفی می‌کنیم تا به کمک آن بتوانیم خواص بیشتری از گروه‌ها را کشف کنیم. با تعریف زیر کار را آغاز می‌کنیم. تمرینات حل شده این بخش را با دقت مطالعه نمایید.

تعریف ۱.۶.۲. *فرض کنیم G یک گروه باشد. عدد اصلی مجموعه G را مرتبه گروه نامیم و آن را با $|G|$ یا $o(G)$ نمایش می‌دهیم. واضح است که اگر $o(G)$ متناهی باشد آنگاه به گروه G یک گروه متناهی و در غیر این صورت به G یک گروه نامتناهی گوییم.*

مثال ۲.۶.۲. *گروه $G = (\mathbb{Z}_m, +)$ از مرتبه m است یعنی $o(G) = m$. واضح است که این گروه متناهی است.*

مثال ۳.۶.۲. *گروه $G = (\mathbb{Z}, +)$ از مرتبه نامتناهی است یعنی $o(G) = \infty$.*

مثال ۴.۶.۲. *برای هر عدد طبیعی $n \geq ۲$، گروه $G_n = (\mathbb{Z}_n, +)$ از مرتبه متناهی است. اما $\prod_{n=۲}^{\infty} G_n$ گروهی نامتناهی است.*

مثال ۵.۶.۲. *گروه $G = S_n$ از مرتبه $n!$ است، یعنی $o(G) = n!$. واضح است که این گروه متناهی است.*

مثال ۶.۶.۲. *گروه $G = (\mathbb{Z}_p, .)$ که p عددی اول، از مرتبه p است یعنی $o(G) = p$. واضح است که این گروه متناهی است.*

مثال ۷.۶.۲. *با توجه به تمرین ۵۹. ۲. ۲، گروه $U(\mathbb{Z}_n)$ از مرتبه $\varphi(n)$ است یعنی $o(G) = \varphi(n)$ (φ تابع اویلر است، فصل اول را ببینید). واضح است که این گروه متناهی است.*

تعریف ۸.۶.۲. *فرض کنیم G یک گروه با عنصر خنثی e باشد و $x \in G$. اگر کوچکترین عدد طبیعی n موجود باشد که $x^n = e$ آنگاه n را مرتبه x نامیم و با $o(x)$ نمایش می‌دهیم. اگر چنین عدد طبیعی موجود نباشد آنگاه گوییم x از مرتبه نامتناهی است و می‌نویسیم $o(x) = \infty$.*

مثال ۹.۶.۲. *عنصر $\bar{۲}$ در گروه $(\mathbb{Z}_۶, +)$ دارای مرتبه سه است. زیرا $\bar{۲} + \bar{۲} + \bar{۲} = \bar{۰}$. بنابراین $o(\bar{۲}) = ۳$.*

مثال ۱۰.۶.۲. *عنصر $\bar{۳}$ در گروه $(\mathbb{Z}_۴, +)$ دارای مرتبه چهار است. زیرا $\bar{۱۲} = \bar{۰}$. $۴\bar{۳} = \bar{۱۲}$. بنابراین $o(\bar{۳}) = ۴$.*

مثال ۱۱.۶.۲. *در گروه $\mathbb{K}_۴$ مرتبه هر عنصر به جز عنصر خنثی e، برابر دو است. زیرا در این گروه داریم $a^۲ = b^۲ = c^۲ = e$. در نتیجه $o(a) = o(b) = o(c) = ۲$.*

مثال ۱۲.۶.۲. *عنصر i در گروه $\mathbb{Q}_۸$ دارای مرتبه چهار است. زیرا $i^۴ = ۱$. بنابراین $o(i) = ۴$.*

مثال ۱۳.۶.۲. *عنصر ۳ در گروه $(\mathbb{Z}, +)$ دارای مرتبه نامتناهی است. بنابراین $o(۳) = \infty$.*

آیا ارتباطی بین مرتبه گروه و مرتبه عناصر آن وجود دارد؟ گزاره زیر به همین مطلب پاسخ می دهد.

گزاره ۱۴.۶.۲. *فرض کنیم G گروهی از مرتبه متناهی n باشد. در این صورت هر عنصر G مرتبه متناهی کمتر یا دارد.*

اثبات. فرض کنیم $x \in G$. مجموعه زیر را در نظر می‌گیریم

$$T = \{x, x^۲, x^۳, ...\}.$$

واضح است که T زیرمجموعه G است و چون G متناهی است باید T متناهی باشد. پس اعداد طبیعی i و j چنان وجود دارند که $x^i = x^j$. بدون کم شدن از کلیت فرض کنیم $i > j$. چون $x^j \in G$ و G گروه است، x^j دارای وارون x^{-j} در G است (چرا؟). پس با ضرب طرفین در x^{-j} داریم $x^{i-j} = x^۰ = e$. □

مرتبه متناهی بودن همه عناصر گروه نمی‌تواند به گروه اجبار کند که متناهی باشد! مثال زیر را به دقت مطالعه کنید.

مثال ۱۵.۶.۲. *فرض کنیم $G = \mathbb{P}(\mathbb{N})$. عمل دوتایی روی G را همان تفاضل متقارن مجموعه‌ها در نظر می‌گیریم. یعنی برای هر $A, B \in G$*

$$A * B = (A \cup B) \setminus (A \cap B).$$

یک بررسی ساده نشان می‌دهد که $(G, *)$ یک گروه آبلی است که $\emptyset$ عنصر خنثی آن است. اما برای هر $A \in G$ داریم

$$A^۲ = A * A = (A \cup A) \setminus (A \cap A) = \emptyset.$$

این یعنی $o(A) = ۲$. دقت شود که G یک گروه نامتناهی است ولی هر عنصر آن مرتبه متناهی دارد!

به عنوان مثالی دیگر، مثال زیر را ببینید.

مثال ۱۶.۶.۲. *فرض کنیم برای هر عدد طبیعی i، قرار می‌دهیم $G_i = (\mathbb{Z}_۲, +)$. مرتبه هر عنصر گروه $\prod_{i=۱}^{\infty} G_i$ متناهی است و دقیقا برابر ۲ است. اما این گروه نامتناهی است.*

حال گزاره زیر را داریم.

گزاره ۱۷.۶.۲. *فرض کنیم G یک گروه با عنصر خنثی e باشد و $x \in G$.*
(۱) اگر برای عدد صحیحی مانند m داشته باشیم $x^m = e$ آنگاه $o(x)$ متناهی است و $o(x)|m$.
(۲) اگر $o(x) = n$ آنگاه به ازای هر عدد صحیح مثبت k، $x^k = x^r$ که در آن $r \overset{n}{\equiv} k$.

اثبات. (۱) چون $x^m = e$ پس $x^{-m} = e$. در نتیجه کوچکترین عدد طبیعی n وجود دارد که $x^n = e$ (چرا؟) یعنی $o(x) = n$. طبق الگوریتم تقسیم، قضیه ۷.۲.۱ داریم $m = nq + r$ که $0 \leq r < n$. بنابراین $e = x^m = x^{nq+r} = x^{nq}x^r = (x^n)^q x^r = x^r$ که این در تناقض با انتخاب ما از n است. لذا $r = 0$ و $n|m$.
(۲) طبق الگوریتم تقسیم، قضیه ۷.۲.۱ داریم $k = nq + r$ که $0 \leq r < n$. بنابراین $x^k = x^{nq+r} = (x^n)^q x^r = x^r$ بدیهی است که $k \overset{n}{\equiv} r$. □

اکنون قضیه مهم زیر را داریم.

قضیه ۱۸.۶.۲. *فرض کنیم G یک گروه باشد و $x \in G$. در این صورت $< x >$ مرتبه n است اگر و تنها اگر $o(x) = n$.*

اثبات. فرض کنیم $H =< x >$ از مرتبه متناهی n باشد، یعنی $|H| = n$. طبق گزاره ۱۴.۶.۲ باید مرتبه x متناهی باشد. فرض کنیم $o(x) = m$. طبق نتیجه ۱۰.۵.۲ و گزاره ۱۷.۶.۲ قسمت (۲) داریم

$$< x >= \{x^k \mid k \in \mathbb{Z}\} = \{x^k = x^r \mid k \overset{m}{\equiv} r\} = \{x^r \mid r = 0, 1, 2, ..., m-1\} = \{e, x, x^2, ..., x^{m-1}\}$$

پس H دارای عدد اصلی m است و این تناقض است مگر این که $m = n$.
برعکس، فرض کنیم $o(x) = n$. در این صورت باید عناصر e، x، ...، x^{n-1} متمایز باشند. زیرا اگر برای $0 \leq i < j \leq n-1$ داشته باشیم $x^i = x^j$ آنگاه $x^{j-i} = e$ و طبق گزاره ۱۷.۶.۲ قسمت (۱)، باید $n|j-i$ که $o(x) = n$ که تناقض آشکار است. طبق نتیجه ۱۰.۵.۲ و گزاره ۱۷.۶.۲ قسمت (۲) داریم

$$< x >= \{x^k \mid k \in \mathbb{Z}\} = \{x^k = x^r \mid k \overset{n}{\equiv} r\} = \{x^r \mid r = 0, 1, 2, ..., n-1\} = \{e, x, x^2, ..., x^{n-1}\}$$

و لذا $|< x >| = n$. □

نتیجه ۱۹.۶.۲. *اگر G یک گروه متناهی و $e \in G$ عنصر خنثی باشد آنگاه عدد طبیعی k چنان وجود دارد که برای $x \in G$ داریم $x^k = e$.*

اثبات. چون G متناهی است پس زیرگروه $H =< x >$ نیز متناهی است که $x \in G$. اگر $|H| = n_x$ باشد آنگاه طبق قضیه ۱۸.۶.۲ داریم $o(x) = n_x$. اکنون قرار می‌دهیم $k = \prod_{x \in G} n_x$.
واضح است که برای $x \in G$ داریم $x^k = e$. □

این بخش را با قضیه زیر به پایان می‌رسانیم.

قضیه ۲۰.۶.۲. *فرض کنیم G یک گروه دوری متناهی مرتبه n باشد و $d|n$. در این صورت G دقیقا یک زیرگروه مانند H دارد که $|H| = d$.*

اثبات. فرض کنیم $G =< x >$ که $x \in G$. پس طبق قضیه ۱۸.۶.۲ داریم $o(x) = n$. اگر $d = n$ و یا $d = ۱$ آنگاه به ترتیب $H = \{e\}$ و یا $H = G$، لذا چیزی برای اثبات نداریم. فرض کنیم $۱ < d < n$. طبق فرض، عدد صحیح m چنان وجود دارد که $n = dm$. عنصر $y = x^m$ از G را در نظر می‌گیریم و نشان می‌دهیم که $o(y) = d$. واضح است که $y^d = x^{md} = x^n = e$. لذا طبق قسمت (۱) از گزاره ۱۴.۶.۲ داریم $o(y)|d$. لذا $o(y) \leq d$. اگر $o(y) = t < d$ آنگاه $e = y^t = x^{mt}$. حال طبق گزاره ۱۴.۶.۲ قسمت (۱) باید $n|mt$. بنابراین $n = md < mt$ و لذا $d < t$ که تناقض آشکار است. در نتیجه $o(y) = d$ و طبق قضیه ۱۸.۶.۲ $H =< y >$ از مرتبه d است. فقط مانده این مطلب که یکتایی H را نشان دهیم. فرض کنیم زیرگروه H' از G موجود باشد که $|H'| = d$. چون G دوری است لذا طبق قضیه ۲۲.۵.۲ باید H' نیز دوری باشد. بنابراین می‌توانیم فرض کنیم $H' =< x^t >$. طبق قضیه ۱۸.۶.۲ داریم $o(x^t) = d$. لذا $(x^t)^d = x^{td} = e$ و از گزاره ۱۴.۶.۲ قسمت (۱) باید $o(x) = n = md|td$. این نشان می‌دهد که $m|t$. فرض کنیم $t = lm$. در این صورت $x^t = x^{lm} = (x^m)^l$. بنابراین $H' \subseteq H$. اما دو مجموعه متناهی H و H' عدد اصلی d دارند و یکی زیرمجموعه دیگری است لذا باید $H = H'$. اثبات کامل است. □

مثال ۲۱.۶.۲. *می‌دانیم که گروه $G = (\mathbb{Z}_{۱۲}, +)$ یک گروه دوری متناهی است. دقت شود که $G =< \bar{۱} >$. از طرفی عدد ۳ مرتبه گروه یعنی عدد ۱۲ را می‌شمارد. لذا طبق قضیه ۲۰.۶.۲ در G فقط یک زیرگروه H مرتبه ۳ وجود دارد. چون G دوری است لذا طبق قضیه ۲۲.۵.۲ باید H نیز دوری باشد. فرض کنیم $H =< \bar{x} >$. پس طبق قضیه ۱۸.۶.۲ داریم $o(\bar{x}) = ۳$. اما در G عنصر $\bar{۴}$ مرتبه ۳ دارد. بنابراین*

$$H =< \bar{۴} >= \{\bar{۰}, \bar{۴}, \bar{۸}\}.$$

تمرین‌های حل شده

تمرین ۲۲.۶.۲. *فرض کنیم G گروهی از مرتبه زوج باشد. نشان دهید که دقیقا تعداد فردی عنصر در G وجود دارد که از مرتبه ۲ هستند.*

حل. می‌دانیم که $x^۲ \neq e$ اگر و تنها اگر $x \neq x^{-۱}$. مجموعه زیر را در نظر می‌گیرم

$$T = \{(x, x^{-۱}) \mid x \in G, \ \ x \neq x^{-۱}\}.$$

به وضوح $|T|$ عدد زوج است. در نتیجه تعداد زوج عنصر مانند x هست که $x^۲ \neq e$. چون مرتبه گروه زوج است، تعداد زوجی عنصر مانند y در G هستند که $y^۲ = e$. چون e یکی از عناصری هست که $e^۲ = e$، پس تعداد فردی عنصر در G مانند y وجود دارد که $y^۲ = e$.

تمرین ۲۳.۶.۲. *فرض کنیم G یک گروه مرتبه متناهی باشد و برای دو زیرمجموعه ناتهی A و B از G داشته باشیم $|G| < |A| + |B|$. نشان دهید که $G = AB$.*

حل. واضح است که $AB \subseteq G$. قرار می‌دهیم

$$A^* = \{a^{-۱} \mid a \in A\}.$$

فرض کنیم $g \in G$. یک بررسی ساده نشان می‌دهد که رابطه

$$f : A \longrightarrow A^*g, \quad f(a) = a^{-1}g$$

یک تابع خوشتعریف یک‌به‌یک و پوشا است. لذا $|A| = |A^*g|$. اما داریم

$$|A|+|B| > |G| \geq |A^*g \cup B| = |A^*g|+|B|-|A^* \cap B| = |A|+|B|-|A^*g \cap B|.$$

لذا باید $|A^*g \cap B| \geq 1$. یعنی $A^*g \cap B$ ناتهی است. فرض کنیم $b \in A^*g \cap B$. پس عنصر $a^{-1} \in A^*$ وجود دارد که $b = a^{-1}g$. لذا $g = ab \in AB$ و $G \subseteq AB$.

تمرین ۲۴.۶.۲. *نشان دهید که برای هر عضو x از گروه G داریم $o(x) = o(x^{-1})$.*

حل. فرض کنیم $o(x) = t$ و $o(x^{-1}) = k$. پس $(x^{-1})^t = (x^t)^{-1} = e$ و لذا طبق گزاره ۱۷.۶.۲ داریم $k|t$. اما $e = (x^{-1})^k = (x^k)^{-1}$ و لذا باید $x^k = e$. حال طبق گزاره ۱۷.۶.۲ داریم $t|k$. در نتیجه $k = t$.

تمرین ۲۵.۶.۲. *اگر x و y عناصری دلخواه در گروه G باشند آنگاه نشان دهید که $o(xy) = o(yx)$.*

حل. فرض کنیم $o(xy) = t$ و $o(yx) = k$. حال داریم

$$(yx)^t = \underbrace{yxyx...yx}_{\text{تا } t} = y\underbrace{xyxy...xy}_{\text{تا } (t-1)}x = y(xy)^{t-1}x.$$

از سمت چپ تساوی بالا را در y ضرب می‌کنیم

$$(yx)^t y = y(xy)^{t-1}xy = y(xy)^t = y.$$

حال طرفین را در y^{-1} از سمت چپ ضرب می‌کنیم $(yx)^t = e$. حال طبق گزاره ۱۷.۶.۲ داریم $k|t$. با روش مشابه $t|k$ و لذا $t = k$.

تمرین ۲۶.۶.۲. *اگر x و y عناصری در گروه G باشند آنگاه نشان دهید که $o(y) = o(x^{-1}yx)$.*

حل. حتما قبل از دیدن حل، تمرین ۶۲.۲.۲ را یکبار دیگر مطالعه نمایید. اکنون فرض کنیم $o(x^{-1}yx) = t$ و $o(y) = k$. پس داریم

$$(x^{-1}yx)^k = \underbrace{x^{-1}yx\ x^{-1}yx\ x^{-1}yx...x^{-1}yx}_{\text{تا } k} = x^{-1}y^kx = x^{-1}x = e.$$

حال طبق گزاره ۱۷.۶.۲ داریم $t|k$. حال داریم

$$y^t = xx^{-1}y^txx^{-1} = x(x^{-1}yx)^tx^{-1} = xx^{-1} = e.$$

پس $t|k$ و لذا $t = k$.

تمرین ۲۷.۶.۲. *فرض کنیم G گروهی باشد که دقیقا یک عنصر از مرتبه n مانند x دارد. نشان دهید که $x \in Z(G)$ و $n = ۲$.*

حل. طبق تمرین حل شده قبل، می‌دانیم که برای هر $y \in G$ داریم $o(x) = o(y^{-۱}xy)$. چون فقط یک عنصر از مرتبه n وجود دارد پس باید $x = y^{-۱}xy$ و لذا $yx = xy$. این نشان می‌دهد که $x \in Z(G)$. از طرفی $o(x) = o(x^{-۱})$ (چرا؟)، پس باید $x = x^{-۱}$ و این یعنی $x^۲ = e$. یعنی $n = ۲$.

تمرین ۲۸.۶.۲. *فرض کنیم در گروه G برای $x \in G$ داشته باشیم $o(x) = n$. اگر برای عدد صحیح m رابطه $(m, n) = ۱$ برقرار باشد آنگاه $o(x^m) = n$.*

حل. فرض کنیم $o(x^m) = k$. پس $e = (x^m)^k = x^{mk}$. طبق گزاره ۱۷.۶.۲، داریم $n|mk$. چون $(m, n) = ۱$ پس $n|k$. اما $(x^m)^n = x^{mn} = (x^n)^m = e$. دوباره طبق گزاره ۱۷.۶.۲، داریم $k|n$ و لذا $k = n$.

تمرین ۲۹.۶.۲. *فرض کنیم که G یک گروه و $x \in G$. اگر $o(x) = n$ و برای عدد صحیح m داشته باشیم $(m, n) = d$ آنگاه نشان دهید که $o(x^m) = \frac{n}{d}$.*

حل. فرض کنیم $o(x^m) = k$. پس $e = (x^m)^k = x^{mk}$. طبق گزاره ۱۷.۶.۲، داریم $n|mk$ و در نتیجه $\frac{n}{d}|\frac{m}{d}k$. چون $(m, n) = d$ پس $(\frac{m}{d}, \frac{n}{d}) = ۱$ و لذا $\frac{n}{d}|k$. از طرفی دیگر داریم $e = (x^n)^{\frac{m}{d}} = x^{\frac{nm}{d}} = (x^m)^{\frac{n}{d}}$. دوباره طبق گزاره ۱۷.۶.۲، داریم $k|\frac{n}{d}$ و لذا $k = \frac{n}{d}$.

تمرین ۳۰.۶.۲. *نشان دهید هر گروه دوری از مرتبه نامتناهی فقط دو مولد دارد.*

حل. فرض کنیم $G =< x >$ یک گروه دوری نامتناهی باشد. واضح است که $G =< x^{-۱} >$. زیرا $x^n = (x^{-۱})^{-n}$. پس دو مولد را پیدا کرده‌ایم یکی x و دیگری $x^{-۱}$. حال فرض کنیم $G =< y >$. عدد صحیح n چنان وجود دارد که $y = x^n$ (چرا؟). همچنین عدد صحیح m چنان وجود دارد که $x = y^m$ (چرا؟). لذا

$$x = y^m = (x^n)^m = x^{mn}.$$

با ضرب طرفین تساوی در $x^{-۱}$ داریم $x^{mn-۱} = e$، یعنی $o(x)$ متناهی است. حال طبق قضیه ۱۸.۶.۲ باید $G =< x >$ متناهی باشد. این تناقض آشکار است، مگر این که $mn = ۱$. این معادل است با $m = n = ۱$ و یا $m = n = -۱$. پس $y = x$ یا $y = x^{-۱}$.

تمرین ۳۱.۶.۲. *فرض کنیم G یک گروه باشد و $G =< x, y >$ به طوری که $o(x) = ۲$، $o(y) = ۳$ و $o(xy) = ۲$. نشان دهید که $o(G) = ۶$.*

حل. چون $x^۲ = e$ پس $x = x^{-۱}$. چون $y^۳ = e$ و $y^{-۱} = y^۲$. اما $(xy)^۲ = xyxy = e$ و لذا $xy = y^{-۱}x^{-۱} = y^۲x$. یعنی $xy = y^۲x$. با توجه به قضیه ۵.۵.۲ و رابطه $xy = y^۲x$ داریم

$$G =< x, y >= \{x^m y^n \mid m \in \{۰, ۱\}, \ n \in \{۰, ۱, ۲\}\}.$$

حال داریم $|G|= o(G) \leq ۶$. اکنون فرض می‌کنیم $H =< x >$ و $K =< y >$. طبق قضیه ۱۸.۶.۲ داریم $|H|= ۲$ و $|K|= ۳$. اما همه اعضای H مرتبه ۲ هستند و همه اعضای K مرتبه ۳ (بررسی کنید)، بنابراین باید $H \cap K = \{e\}$. لذا طبق قضیه ۳۱.۴.۲ نتیجه می‌شود که

$$|G|\geq |HK|= \frac{|H|\,|K|}{|H \cap K|} = |H|\,|K|= ۶.$$

در نتیجه $|G|= o(G) = ۶$.

تمرین ۳۲.۶.۲. *برای گروه D_n یک مجموعه مولد دو عضوی مانند $\{\sigma, \tau\}$ پیدا کنید یعنی نشان دهید*

$$D_n =< \{\sigma, \tau \mid \sigma^n = \tau^۲ = (\tau\sigma)^۲ = e\} > .$$

حل. فرض کنیم

$$\sigma = \begin{pmatrix} ۱ & ۲ & ... & n \\ ۲ & ۳ & ... & ۱ \end{pmatrix}$$

که دوران به اندازه $\frac{۲\pi}{n}$ و

$$\tau = \begin{pmatrix} ۱ & ۲ & ... & n \\ ۱ & n & ... & ۲ \end{pmatrix}$$

که انعکاس نسبت به راس ۱ است. یک بررسی ساده نشان می‌دهد که $o(\sigma) = n$ و $o(\tau) = ۲$. همچنین $o(\tau\sigma) = ۲$. رابطه آخر و این که $\tau = \tau^{-۱}$ روابط

$$\tau\sigma = \sigma^{-۱}\tau^{-۱} = \sigma^{-۱}\tau \qquad \tau\sigma^k\tau = \sigma^{-k}$$

را می‌دهد. پس

$$\begin{aligned} H =& < \{\sigma, \tau \mid \sigma^n = \tau^۲ = (\tau\sigma)^۲ = e\} >= \\ & \{\sigma^i, \sigma^i\tau \mid ۰ \leq i \leq n - ۱\} = \\ & \{\sigma, \sigma^۲, ..., \sigma^{n-۱}, \sigma\tau, \sigma^۲\tau, ..., \sigma^{n-۱}\tau\}. \end{aligned}$$

اما $H \subseteq D_n$ و $|H|= ۲n$ پس طبق قضیه ۱۴.۳.۲ باید $H = D_n$.

تمرین ۳۳.۶.۲. *فرض کنیم $G =< x >$ و $H =< y >$ دو گروه دوری به ترتیب از مرتبه m و n باشند که $(m, n) = ۱$. نشان دهید که $G \times H$ دوری و از مرتبه mn است.*

حل. فرض کنیم $o((x, y)) = k$. حال داریم

$$(x, y)^{mn} = (x^{mn}, y^{mn}) = (e_G, e_H).$$

یعنی $k|mn$ (چرا؟). اما

$$(e_G, e_H) = (x, y)^k = (x^k, y^k).$$

پس باید $x^k = e_G$ و $y^k = e_H$. لذا $m|d$ و $n|d$، در نتیجه $mn|d$. بنابراین $k = mn$. طبق قضیه ۱۸.۶.۲، $|< (x, y) >|= mn$. اما $|G \times H|= mn$ و $< (x, y) > \subseteq G \times H$، پس باید $< (x, y) >= G \times H$.

۷.۲ هم‌دسته‌ها و قضیه لاگرانژ

برای مطالعه گروه‌ها در این یک ابزار قدرتمند دیگر معرفی می‌کنیم.

تعریف ۱.۷.۲. *فرض کنیم G یک گروه، $H \leq G$ و $a \in G$.*
(الف) به مجموعه

$$aH = \{ah \mid h \in H\}$$

هم دسته چپ H در G گوییم.
(ب) به مجموعه

$$Ha = \{ha \mid h \in H\}$$

هم دسته راست H در G گوییم.
(ج) عنصر a را نماینده هم دسته چپ aH یا هم دسته راست Ha نامیم.

مثال ۲.۷.۲. *گروه $G = (\mathbb{Z}, +)$ و زیرگروه $H = ۳\mathbb{Z}$ را در نظر می‌گیرم. فرض کنیم $a \in \mathbb{Z}$. طبق الگوریتم تقسیم، قضیه ۱.۲.۷ نتیجه می‌شود که $a = ۳q + r$ که $۰ \leq r < ۳$. لذا چون گروه جمعی است داریم*

$$a + H = \{k + h \mid h \in H\} = \{a + ۳k \mid ۳k \in H\} =$$
$$\{۳q + r + ۳k \mid ۳k \in H,\ \ ۰ \leq r < ۳\} = \{r + ۳k' \mid ۳k' \in H,\ ۰ \leq r < ۳\}.$$

پس هم دسته‌های چپ H در G به صورت $۳\mathbb{Z}$، $۳\mathbb{Z} + ۱$ و $۳\mathbb{Z} + ۲$ هستند. اگر a مضربی از عدد ۳ باشد، هم دسته $H = ۳\mathbb{Z}$ حاصل می‌شود. اگر a بر عدد ۳ باقیمانده ۱ داشته باشد هم دسته $۳\mathbb{Z} + ۱$ حاصل می‌شود. اگر a بر عدد ۳ باقیمانده ۲ داشته باشد هم دسته $۳\mathbb{Z} + ۲$ حاصل می‌شود. برای زیرگروه دلخواه $n\mathbb{Z}$ به صورت مشابه، هم دسته‌های چپ $n\mathbb{Z}$، $n\mathbb{Z} + ۱$، ...، $n\mathbb{Z} + (n - ۱)$ هستند.

تذکر ۳.۷.۲. *اگر G گروهی آبلی باشد آنگاه هم دسته چپ و راست یکی هستند، یعنی $aH = Ha$. هم دسته‌های چپ یا راست زیرمجموعه گروه هستند ولی لزوما زیرگروه نیستند! مثلا هم دسته $۳\mathbb{Z} + ۱$ زیرگروه نیست.*

مثال ۴.۷.۲. *فرض کنیم*

$$G = \{\begin{pmatrix} a & b \\ ۰ & a \end{pmatrix} \mid a, b \in \mathbb{Z}_۳,\ \ a \neq \bar{۰}\}.$$

G با ضرب عادی ماتریسی یک گروه است. قرار می‌دهیم

$$H = \{\begin{pmatrix} \bar{۱} & c \\ ۰ & \bar{۱} \end{pmatrix} \mid c \in \mathbb{Z}_۳\}.$$

واضح است که $H \leq G$. برای هر

$$\begin{pmatrix} a & b \\ ۰ & a \end{pmatrix} \in G$$

داریم

$$\begin{pmatrix} a & b \\ ۰ & a \end{pmatrix} = \begin{pmatrix} a & ۰ \\ ۰ & a \end{pmatrix} \begin{pmatrix} ۱ & a^{-۱}b \\ ۰ & ۱ \end{pmatrix}.$$

عنصر دوم از ضرب سمت راست تساوی بالا عضوی از H است. حال نوشتن هم دسته‌های چپ بسیار ساده است زیرا طبق تساوی بالا شکل aH ظاهر شده است. چون $a \neq ۰$، هم دسته‌های چپ با انتخاب $a = ۱$ و $a = ۲$ حاصل می‌شوند. یعنی

$$\begin{pmatrix} ۱ & ۰ \\ ۰ & ۱ \end{pmatrix} H = H$$
$$\begin{pmatrix} ۲ & ۰ \\ ۰ & ۲ \end{pmatrix} H = \{\begin{pmatrix} ۲ & ۲c \\ ۰ & ۲ \end{pmatrix} \mid c \in \mathbb{Z}_۳\}$$

هم دسته‌های چپ هستند.

مثال ۵.۷.۲. فرض کنیم

$$G = \{\begin{pmatrix} a & b \\ ۰ & a \end{pmatrix} \mid a, b \in \mathbb{Z}_۳, \ a \neq ۰\}.$$

G با ضرب عادی ماتریسی یک گروه است. قرار می‌دهیم

$$H = \{\begin{pmatrix} ۱ & c \\ ۰ & ۱ \end{pmatrix} \mid c \in \mathbb{Z}_۳\}.$$

واضح است که $H \leq G$. برای هر

$$\begin{pmatrix} a & b \\ ۰ & a \end{pmatrix} \in G$$

داریم

$$\begin{pmatrix} a & b \\ ۰ & a \end{pmatrix} = \begin{pmatrix} ۱ & ba^{-۱} \\ ۰ & ۱ \end{pmatrix} \begin{pmatrix} a & ۰ \\ ۰ & a \end{pmatrix}.$$

عنصر اول از ضرب سمت راست تساوی بالا عضوی از H است. حال نوشتن هم دسته‌های راست بسیار ساده است زیرا طبق تساوی بالا شکل Ha ظاهر شده است. چون $a \neq ۰$، هم دسته‌های راست با انتخاب $a = ۱$ و $a = ۲$ حاصل می‌شوند. یعنی

$$H \begin{pmatrix} ۱ & ۰ \\ ۰ & ۱ \end{pmatrix} = H$$
$$H \begin{pmatrix} ۲ & ۰ \\ ۰ & ۲ \end{pmatrix} = \{\begin{pmatrix} ۲ & ۲c \\ ۰ & ۲ \end{pmatrix} \mid c \in \mathbb{Z}_۳\}$$

هم دسته‌های راست هستند.

در مثال‌های بالا هم دسته‌های چپ با هم دسته‌های راست مساوی شدند! زیرا زیرگروه H یک زیرگروه خاص است که در بخش بعد مطالعه خواهیم کرد. اکنون مثال زیر را ببینید.

مثال ۶.۷.۲. *گروه $G = S_3$ را در نظر می‌گیریم. طبق نمادهای مثال ۷.۳.۲ قرار می‌دهیم*

$$\sigma_6 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \qquad H =< \sigma_6 >= \{\sigma_1, \sigma_6\}.$$

اگر حوصله کنید و با دقت محاسبات را انجام دهید آنگاه هم دسته‌ها چپ

$$\sigma_1 H = H = \sigma_6 H$$
$$\sigma_2 H = \{\sigma_2, \sigma_5\} = \sigma_5 H$$
$$\sigma_3 H = \{\sigma_3, \sigma_4\} = \sigma_4 H$$

هستند و هم دسته‌های راست

$$H\sigma_1 = H = H\sigma_6$$
$$H\sigma_2 = \{\sigma_2, \sigma_4\} = H\sigma_4$$
$$H\sigma_3 = \{\sigma_3, \sigma_5\} = H\sigma_5$$

هستند! هم دسته‌های چپ با هم دسته‌های راست یکی نیست، یعنی

$$\{H, \sigma_2 H, \sigma_3 H\} \neq \{H, H\sigma_2, H\sigma_3\}.$$

مثال‌های بالا در سه مطلب مشترک هستند. یکی این که عدد اصلی هم دسته چپ aH و راست Ha یکسان است. دوم این که عدد اصلی مجموعه همه هم دسته‌های چپ و راست یکسان است و آخر آن که اجتماع آن ها برابر خود گروه می‌شود! در ادامه این بخش همین نکات مشترک به شدت مورد توجه ما است.
کار را با گزاره زیر شروع می‌کنیم.

گزاره ۷.۷.۲. *موارد زیر برای گروه G، $H \leq G$ و $a \in G$ برقرار است.*
(۱) *اگر $a \in H$ آنگاه $aH = Ha = H$.*
(۲) *همواره داریم $|aH| = |Ha| = |H|$.*

اثبات. (۱) چون H زیرگروه است پس برای هر $h \in H$ داریم $ah \in H$ و $ha \in H$. زیرا $a \in H$. بنابراین بدیهی است که $aH = Ha = H$.
(۲) رابطه

$$f : H \longrightarrow aH, \quad f(h) = ah$$

یک تابع خوشتعریف یک‌به‌یک و پوشا است (بررسی کنید). پس $|aH| = |H|$. رابطه

$$g : H \longrightarrow Ha, \quad f(h) = ha$$

یک تابع خوشتعریف یک‌به‌یک و پوشا است (بررسی کنید). پس $|Ha| = |H|$. اثبات کامل است. □

حال قضیه مهم زیر را داریم.

قضیه ۸.۷.۲. *فرض کنیم G یک گروه و $H \leq G$. برای هر $u, v \in G$، تعریف می‌کنیم*

$$u \doteq v \iff u^{-1}v \in H.$$

در این صورت موارد زیر بر قرار است.
(۱) *$\doteq$ رابطه هم ارزی روی G است.*
(۲) *کلاس هم ارزی $a \in G$ برابر است با aH یعنی $[a] = aH$.*
(۳) *هم دسته‌های چپ برای G یک افراز هستند.*
(۴) *داریم $G/\doteq = \{aH \mid a \in G\}$.*

اثبات. (۱) برای هر $u \in G$ داریم $u^{-1}u = e \in H$ و لذا $u \doteq u$، یعنی $\doteq$ انعکاسی است. فرض کنیم $u \doteq v$. پس $u^{-1}v \in H$. اما H زیرگروه است، لذا طبق تمرین ۵۵.۲.۲ و تمرین ۵۶.۲.۲ داریم $v^{-1}u = (u^{-1}v)^{-1} \in H$. این یعنی $v \doteq u$ و $\doteq$ تقارنی است. اکنون فرض کنیم $u \doteq v$ و $v \doteq w$. پس $u^{-1}v \in H$ و $v^{-1}w \in H$. چون H زیرگروه است، باید $u^{-1}vv^{-1}w = u^{-1}w \in H$. یعنی $u \doteq w$ و لذا $\doteq$ تعدی و در نتیجه هم ارزی است.
(۲) طبق تعریف کلاس هم ارزی داریم

$$[a] = \{g \in G \mid g \doteq a\} = \{g \in G \mid a \doteq g\} =$$
$$\{g \in G \mid a^{-1}g \in H\} \overset{a^{-1}g=h}{=} \{ah \mid h \in H\} = aH.$$

(۳) طبق قضیه ۱۲.۱.۱، $G/\doteq$ یک افراز برای G است.
(۴) طبق تعریف داریم (صفحه دوم از فصل اول را ببینید)

$$G/\doteq = \{A \subseteq G \mid A = [a] \text{ باشد که } a \text{ ای در } G\} =$$
$$\{A \subseteq G \mid A = aH \text{ باشد که } a \text{ ای در } G\} =$$
$$\{aH \mid a \in G\}$$

و اثبات کامل است. □

قضیه بالا ما را به سمت تعریف زیر سوق می‌دهد.

تعریف ۹.۷.۲. *مجموعه هم دسته‌های چپ زیرگروه H در گروه G را با نماد $(G/H)_l$ نشان می‌دهیم. یعنی*

$$(G/H)_l = G/\doteq = \{aH \mid a \in G\}.$$

مثال ۱۰.۷.۲. *به ترتیب در اولین، دومین وچهارمین مثال این بخش داریم*

$$(\mathbb{Z}/3\mathbb{Z})_l = \{3\mathbb{Z}, 3\mathbb{Z}+1, 3\mathbb{Z}+2\} \qquad \mathbb{Z} = 3\mathbb{Z} \cup (3\mathbb{Z}+1) \cup (3\mathbb{Z}+2)$$
$$(G/H)_l = \{\begin{pmatrix} \bar{1} & \bar{0} \\ \bar{0} & \bar{1} \end{pmatrix} H, \begin{pmatrix} \bar{2} & \bar{0} \\ \bar{0} & \bar{2} \end{pmatrix} H\} \qquad G = \begin{pmatrix} \bar{1} & \bar{0} \\ \bar{0} & \bar{1} \end{pmatrix} H \cup \begin{pmatrix} \bar{2} & \bar{0} \\ \bar{0} & \bar{2} \end{pmatrix} H$$
$$(S_3/H)_l = \{H, \sigma_1 H, \sigma_2 H\} \qquad S_3 = H \cup \sigma_1 H \cup \sigma_2 H$$

حال قضیه زیر را داریم.

قضیه ۱۱.۷.۲. *فرض کنیم G یک گروه و $H \leq G$. برای هر $u, v \in G$، تعریف می‌کنیم*

$$u \mathrel{\dot{\sim}} v \iff uv^{-1} \in H.$$

در این صورت موارد زیر بر قرار است.
(۱) *$\dot{\sim}$ رابطه هم ارزی روی G است.*
(۲) *کلاس هم ارزی $a \in G$ برابر است با aH یعنی $[a] = aH$.*
(۳) *هم دسته‌های راست برای G یک افراز هستند.*
(۴) *داریم $G/\dot{\sim} = \{Ha \mid a \in G\}$.*

اثبات. مشابه قضیه قبل است. □

قضیه بالا ما را به سمت تعریف زیر سوق می‌دهد.

تعریف ۱۲.۷.۲. *مجموعه هم دسته‌های راست زیرگروه H در گروه G را با نماد $(G/H)_r$ نشان می‌دهیم. یعنی*

$$(G/H)_r = G/\dot{\sim} = \{Ha \mid a \in G\}.$$

مثال ۱۳.۷.۲. *به ترتیب در اولین، دومین و چهارمین مثال این بخش داریم*

$$(\mathbb{Z}/\mathbb{3}\mathbb{Z})_r = \{\mathbb{3}\mathbb{Z}, \mathbb{3}\mathbb{Z}+\mathbb{1}, \mathbb{3}\mathbb{Z}+\mathbb{2}\} \qquad \mathbb{Z} = \mathbb{3}\mathbb{Z} \cup (\mathbb{3}\mathbb{Z}+\mathbb{1}) \cup (\mathbb{3}\mathbb{Z}+\mathbb{2})$$

$$(G/H)_r = \{H\begin{pmatrix} \bar{1} & \bar{0} \\ \bar{0} & \bar{1} \end{pmatrix}, H\begin{pmatrix} \bar{2} & \bar{0} \\ \bar{0} & \bar{2} \end{pmatrix}\} \qquad G = H\begin{pmatrix} \bar{1} & \bar{0} \\ \bar{0} & \bar{1} \end{pmatrix} \cup H\begin{pmatrix} \bar{2} & \bar{0} \\ \bar{0} & \bar{2} \end{pmatrix} H$$

$$(S_3/H)_r = \{H, H\sigma_1, H\sigma_2\} \qquad S_3 = H \cup H\sigma_1 \cup H\sigma_2$$

نتیجه ۱۴.۷.۲. *اگر هم دو هم دسته چپ (راست) دست کم در یک عنصر مشترک باشند آنگاه با هم مساوی هستند*

اثبات. طبق قضیه‌های بالا هم دسته‌های چپ و راست افراز برای گروه می‌باشند و افرازها اشتراک ندارند مگر این که مساوی باشند. □

لم ۱۵.۷.۲. *فرض کنیم G یک گروه و $H \leq G$. برای هر $a, b \in G$ موارد زیر معادل هستند.*
(۱) $aH = bH$.
(۲) $Ha^{-1} = Hb^{-1}$.
(۳) $aH \subseteq bH$.
(۴) $a \in bH$.
(۵) $a^{-1}b \in H$.

اثبات. (۱) $\Leftarrow$ (۲). فرض کنیم $x \in Ha^{-1}$. پس عنصر $h \in H$ وجود دارد که $x = ha^{-1}$. طبق تمرین ۵۶.۲.۲ و تمرین ۵۵.۲.۲ داریم که $x^{-1} = ah^{-1} \in aH = bH$. لذا $x^{-1} = bh'$ که $h' \in H$. دوباره طبق تمرین ۵۶.۲.۲ و تمرین ۵۵.۲.۲ داریم $x = (x^{-1})^{-1} = h'^{-1}b^{-1}$. حال واضح است که $x \in Hb^{-1}$ و لذا $Ha^{-1} \subseteq Hb^{-1}$. برعکس، $Hb^{-1} \subseteq Ha^{-1}$، مشابه است. پس $Ha^{-1} = Hb^{-1}$.

(۲) $\Leftarrow$ (۳). فرض کنیم $x \in aH$. پس عنصر $h \in H$ وجود دارد که $x = ah$. طبق تمرین ۵۶.۲.۲ و تمرین ۵۵.۲.۲ داریم که $x^{-1} = h^{-1}a^{-1} \in Ha^{-1} = Hb^{-1}$. لذا $x^{-1} = h'b^{-1}$ که $h' \in H$. دوباره طبق تمرین ۵۶.۲.۲ و تمرین ۵۵.۲.۲ داریم $x = (x^{-1})^{-1} = bh'^{-1}$. حال واضح است که $x \in bH$ و لذا $aH \subseteq bH$.

(۳) $\Leftarrow$ (۴). چون $e \in H$ پس داریم $a = ae \in aH \subseteq bH$.

(۴) $\Leftarrow$ (۵). طبق قضیه ۸.۷.۲ داریم که $bH = [b]$. پس $a \simeq b$ و لذا $a^{-1}b \in H$.

(۵) $\Leftarrow$ (۱). طبق قضیه ۸.۷.۲ داریم که $a^{-1}b \in H$ اگر و تنها اگر $a \simeq b$. طبق تعریف کلاس هم ارزی بدیهی است که $aH = [a] = bH = [b]$. □

لم ۱۶.۷.۲. *فرض کنیم G یک گروه و $H \leq G$. برای هر $a, b \in G$ موارد زیر معادل هستند.*

(۱) $Ha = Hb$.

(۲) $a^{-1}H = b^{-1}H$.

(۳) $Ha \subseteq Hb$.

(۴) $a \in Hb$.

(۵) $ab^{-1} \in H$.

اثبات. مشابه لم ۱۵.۷.۲ اثبات می‌شود. □

اکنون قضیه مهم زیر را داریم.

قضیه ۱۷.۷.۲. *برای هر گروه G و $H \leq G$ داریم*

$$|(G/H)_l| = |(G/H)_r|.$$

اثبات. ضابطه

$$f : (G/H)_l \longrightarrow (G/H)_r, \quad f(aH) = Ha^{-1}$$

را در نظر می‌گیریم. ابتدا خوشتعریفی را بررسی می‌کنیم. اگر $aH = bH$ باشد آنگاه طبق لم ۱۵.۷.۲ داریم $Ha^{-1} = Hb^{-1}$ و این یعنی $f(aH) = f(bH)$.
یک‌به‌یک بودن هم مشابه خوشتعریفی نتیجه مستقیم لم ۱۵.۷.۲ است. پوشایی هم واضح است. بنابراین حکم به دست می‌آید. دقت کنید که اگر رابطه

$$f : (G/H)_r \longrightarrow (G/H)_l, \quad f(Ha) = a^{-1}H$$

را در نظر می‌گرفتیم، لم ۱۶.۷.۲ کارساز بود. □

قضیه بالا ما را به تعریف زیر رهنمود می‌کند.

تعریف ۱۸.۷.۲. *طبق قضیه ۱۷.۷.۲ به عدد اصلی و یکتای $|(G/H)_l|=|(G/H)_r|$ اندیس زیرگروه H در G گوییم و با $[G:H]$ نمایش می‌دهیم.*

مثال ۱۹.۷.۲. *طبق مثال اول این بخش داریم* $[\mathbb{Z}:۳\mathbb{Z}]=۳$.

مثال ۲۰.۷.۲. *طبق مثال دوم این بخش داریم* $[G:H]=۲$.

مثال ۲۱.۷.۲. *طبق مثال چهارم این بخش داریم* $[S_۳:H]=۳$.

برای دیدن یک مثال از یک گروه و زیرگروه آن که اندیس نامتناهی دارد، مثال زیر را دنبال کنید.

مثال ۲۲.۷.۲. *فرض کنیم $G=(\mathbb{Q},+)$ و $H=\mathbb{Z}$. همچنین فرض کنیم $\{p_i\}_{i=۱}^{\infty}$ مجموعه اعداد اول باشد. چون گروه آبلی و جمعی است، برای هر i، یک هم دسته چپ یا راست به صورت*

$$\frac{۱}{p_i}+H=\{\frac{۱}{p_i}+k \mid k\in\mathbb{Z}\}$$

خواهیم داشت. حال اگر برای $i\neq j$ داشته باشیم $x\in(\frac{۱}{p_i}+\mathbb{Z})\cap(\frac{۱}{p_j}+\mathbb{Z})$ آنگاه

$$\frac{۱}{p_i}+k=x=\frac{۱}{p_i}+k'$$

که $k,k'\in\mathbb{Z}$. پس $\frac{۱}{p_i}-\frac{۱}{p_j}=k'-k\in\mathbb{Z}$ و لذا باید $p_ip_j|p_j-p_i$. چون $p_i|p_ip_j$ پس $p_i|p_j-p_i$. لذا باید $p_i|p_j$ که تناقض آشکار است. پس هم دسته‌ها هیچ اشتراکی ندارند و تعداد آنها نامتناهی است. یعنی $[\mathbb{Q}:\mathbb{Z}]=\infty$.

اکنون وقت آن است که شما را با یکی از مهمترین و پرکاربردترین قضایای جبر و نظریه گروه آشنا کنیم. افسوس (از این جهت که در برخی مسایل تحقیقاتی اگر عکس قضیه لاگرانژ صحیح باشد بسیار کار راحت می‌شود) که عکس قضیه لاگرانژ صحیح نیست! برای دیدن مثال نقض باید تا بخش آخر این فصل صبر کنید! اما برای گروه‌های خاص مانند گروه دوری متناهی، طبق قضیه ۲۰.۶.۲ عکس قضیه لاگرانژ صحیح است. هر چند همین صحیح نبودن عکس قضیه لاگرانژ سبب پیدایش قضایای کلیدی در نظریه گروه شده است، از جمله قضایای سیلو[۴]!

قضیه ۲۳.۷.۲. *(قضیه لاگرانژ) فرض کنیم G یک گروه متناهی باشد و $H\leq G$. در این صورت $|H|\mid|G|$ یا به عبارتی $[G:H]=\frac{|G|}{|H|}$.*

[۴] Sylow

اثبات. می‌دانیم که طبق قضیه ۸.۷.۲ هم دسته‌های چپ گروه G را افراز می‌کنند. و چون G متناهی است می‌توانیم فرض کنیم $G = \bigcup_{i=1}^{t} a_iH$. پس $[G : H] = t$. اما طبق گزاره ۷.۷.۲ داریم $|a_iH| = |H|$. بنابراین

$$|G| = \sum_{i=1}^{t} |a_iH| = \sum_{i=1}^{t} |H| = t|H| = [G : H]\,|H|$$

و این یعنی $|H| \mid |G|$ یا به عبارتی $[G : H] = \frac{|G|}{|H|}$. □

چند نتیجه بدیهی از قضیه لاگرانژ را در ادامه ببینید.

نتیجه ۲۴.۷.۲. *فرض کنیم G گروهی متناهی از مرتبه n باشد. در این صورت برای هر $x \in G$ داریم $o(x) \mid |G|$.*

اثبات. قرار می‌دهیم $H = \langle x \rangle$. طبق قضیه ۱۸.۶.۲ داریم $|H| = o(x)$ و لذا طبق قضیه لاگرانژ، قضیه ۲۳.۷.۲ باید $|G| = n$ $o(x) \mid |G|$. □

نتیجه ۲۵.۷.۲. *هر گروه متناهی G با مرتبه عدد اول دوری و در نتیجه آبلی است.*

اثبات. فرض کنیم $|G| = p$ که p عددی اول است. همچنین فرض کنیم $e \neq x \in G$. طبق نتیجه قبل باید $o(x) \mid p$. در نتیجه $o(x) = 1$ یا $o(x) = p$. چون x عنصر خنثی نیست باید $o(x) = p$. طبق قضیه ۱۸.۶.۲ داریم $|\langle x \rangle| = p$ و لذا باید $G = \langle x \rangle$. زیرا $\langle x \rangle \subseteq G$. طبق گزاره ۱۴.۵.۲ باید G آبلی باشد. □

نتیجه ۲۶.۷.۲. *در گروه متناهی G، برای زیرگروه‌های H و K که $(o(H), o(K)) = 1$، داریم $H \cap K = \{e\}$.*

اثبات. طبق قضیه لاگرانژ، قضیه ۲۳.۷.۲، داریم $|H \cap K| \mid |H|$ و $|H \cap K| \mid |K|$. بنابراین باید $|H \cap K| \mid (|H|, |K|) = 1$. یعنی $H \cap K = \{e\}$. □

مثال ۲۷.۷.۲. *قضیه اویلر- فرما، قضیه ۲۴.۲.۱، می‌گوید که اگر عدد صحیح n نسبت به عدد صحیح m اول باشد آنگاه $n^{\varphi(m)} \overset{m}{\equiv} 1$ که φ تابع اویلر است. این مطلب اکنون اثبات ساده‌ای دارد. کافی است گروه $G = U(\mathbb{Z}_m)$ را در نظر بگیریم. طبق تمرین ۵۹.۲.۲ داریم که $\bar{n}$ در G قرار دارد و باید $|G| = \varphi(m)$ باشد. طبق قضیه لاگرانژ، قضیه ۲۳.۷.۲، $\bar{n}^{\varphi(m)} = \bar{1}$. پس در $\mathbb{Z}$ داریم $n^{\varphi(m)} \overset{m}{\equiv} 1$.*

مثال ۲۸.۷.۲. *می‌دانیم که ضریب جملات در بسط دو جمله‌ای به صورت $\binom{n}{k} = \frac{n!}{k!(n-k)!}$ است. می‌خواهیم نشان دهیم که این حاصل یک عدد صحیح است! اگر $m = n$ و یا $k = 0$ باشد چیزی برای اثبات نداریم. حال گروه S_n را در نظر می‌گیریم. طبق قضیه ۸.۳.۲ داریم $|S_n| = n!$. فرض*

کنیم H مجموعه‌ای از اعضای S_n باشد که
روی مجموعه $\{۱, ۲, ..., k\}$ جایگشت و روی $\{k + ۱, k + ۲, ..., n\}$ ثابت عمل کند،
روی مجموعه $\{۱, ۲, ..., k\}$ ثابت و روی $\{k + ۱, k + ۲, ..., n\}$ جایگشت عمل کند.
یک بررسی نشان می‌دهد که $H \leq S_n$. طبق قضیه لاگرانژ، قضیه ۲۳.۷.۲ داریم $|H| \mid n!$. اما به طبق اصل ضرب $|H| = k!\,(n-k)!$ است.

مثال ۲۹.۷.۲. برای اعداد طبیعی m و n، آیا $\frac{(mn)!}{(m!)^n}$ یک عدد صحیح است؟ پاسخ مثبت است.
اعداد ۱ تا mn را به شکل

$$۱, ۲, ..., m;\ m + ۱, m + ۲, ..., ۲m;\ ۲m + ۱, ۲m + ۲, ..., ۳m;\ ...;$$
$$(n - ۱)m + ۱, (n - ۱)m + ۲, ..., nm$$

می‌نویسیم. n تا m عدد توسط نقطه ویرگول‌ها جدا شده‌اند! حال گروه S_{mn} را در نظر می‌گیریم.
طبق قضیه ۸.۳.۲ داریم $|S_{mn}| = (mn)!$. فرض کنیم H مجموعه‌ای از اعضای S_{mn} باشد که
روی مجموعه $\{۱, ۲, ..., m\}$ جایگشت و روی بقیه اعداد بین نقطه ویرگول ثابت عمل کند،
روی مجموعه $\{m + ۱, , ..., ۲m\}$ جایگشت و روی بقیه اعداد بین نقطه ویرگول ثابت عمل کند،
روی مجموعه $\{۲m + ۱, , ..., ۳m\}$ جایگشت و روی بقیه اعداد بین نقطه ویرگول ثابت عمل کند، ...
روی مجموعه $\{(n - ۱)m, ..., nm\}$ جایگشت و روی بقیه اعداد بین ویرگول ثابت عمل کند.
یک بررسی نشان می‌دهد که $H \leq S_n$. طبق قضیه لاگرانژ، قضیه ۲۳.۷.۲ داریم $|H| \mid n!$. اما به طبق اصل ضرب $|H| = m!\ m!\ ...m! = (m!)^n$ است.

این بخش را با سه قضیه به پایان می‌بریم. قبل از آوردن این قضیه‌ها مقدماتی برای اثبات آنها لازم داریم. ابتدا مفهوم تراگشتی[۵] را معرفی می‌کنیم.

تعریف ۳۰.۷.۲. فرض کنیم G یک گروه باشد و $H \leq G$. گوییم $T \subseteq G$
(الف) تراگشتی چپ برای H در G است اگر هر هم دسته چپ دقیقا حاوی یک عنصر از T باشد.
(ب) تراگشتی راست برای H در G است اگر هر هم دسته چپ دقیقا حاوی یک عنصر از T باشد.
(ج) تراگشتی برای H در G است اگر تراگشتی چپ و تراگشتی راست باشد.

مثال ۳۱.۷.۲. اولین مثال این بخش را به یاد بیاورید! زیرمجموعه $T = \{۰, ۱, ۲\}$ یک تراگشتی برای $۳\mathbb{Z}$ در $\mathbb{Z}$ است.

مثال ۳۲.۷.۲. چهارمین مثال این بخش را به یاد بیاورید! زیرمجموعه $T = \{\sigma_۱, \sigma_۲, \sigma_۳\}$ یک تراگشتی برای H در $S_۳$ است. زیرمجموعه $T = \{\sigma_۱, \sigma_۴, \sigma_۵\}$ یک تراگشتی دیگر برای H در $S_۳$ است.

[۵] transversal

تذکر ۳۳.۷.۲. *وجود مجموعه تراگشتی چپ (راست) با کمک اصل انتخاب تضمین شده است! زیرا کافی است از هم دسته‌های چپ دقیقا یک عنصر انتخاب کنیم. دقت کنید که همه دسته‌های چپ از هم مجزا هستند چون برای گروه افراز هستند. لذا بسیار بدیهی است که اگر T یک تراگشتی چپ (راست) برای زیرگروه H از G باشد آنگاه $|T|=[G:H]$.*

تذکر ۳۴.۷.۲. *یک تراگشتی چپ برای یک زیرگروه لزوما یک تراگشتی راست نیست. در مثال‌های بالا تراگشتی‌های چپ، راست هم بودند! علت این مطلب زیرگروه نرمال است که در بخش بعد مطالعه می‌کنیم. در واقع اثبات می‌شود (ما بدون اثبات می‌پذیریم) که یک تراگشتی چپ یک تراگشتی راست برای زیرگروه H از گروه G است اگر و تنها اگر H زیرگروه نرمال باشد.*

لم ۳۵.۷.۲. *فرض کنیم G یک گروه باشد و $H \leq G$. اگر T یک تراگشتی چپ برای H در G باشد آنگاه $G = \bigcup_{t\in T} tH$ و هر عنصر G به صورت یکتا به شکل th است که $t \in T$ و $h \in H$.*

اثبات. طبق قضیه ۸.۷.۲ هم دسته‌های چپ H در G گروه G را افراز می‌کنند، یعنی می‌توانیم فرض کنیم مجموعه I چنان وجود دارد که $|I|=|T|=[G:H]$ و $G=\bigcup_{i\in I} a_iH$. حال از هم دسته چپ a_iH نماینده t_i در T قرار دارد. پس اکنون هم دسته چپ a_iH و t_iH در عنصر t_i مشترک هستند و لذا طبق نتیجه ۱۴.۷.۲ باید $a_iH = t_iH$. این نشان می‌دهد که

$$G = \bigcup_{i\in I} a_iH = \bigcup_{t\in T} tH.$$

فرض کنیم $g \in G$ به صورت $g = th = t'h'$ نوشته شود که $t,t' \in T$ و $h,h' \in H$. پس $th \in t'H$ و این یعنی دو هم دسته tH و $t'H$ عنصر مشترک دارند. لذا طبق نتیجه ۱۴.۷.۲ باید $tH = t'H$. چون T تراگشتی چپ است باید $t = t'$ و لذا $th = th'$ و باید $h = h'$ باشد. □

قضیه ۳۶.۷.۲. *فرض کنیم G یک گروه باشد و $K \leq H \leq G$. در این صورت*

$$[G:K] = [G:H]\,[H:K].$$

اثبات. می‌دانیم (تذکر اول بالا) که تراگشتی‌های چپ $T \subseteq G$ و $S \subseteq H$ چنان وجود دارند که $|T| = [G:H]$ و $|S| = [H:K]$. طبق قضیه ۸.۷.۲ داریم

$$G = \bigcup_{t\in T} tH \qquad\qquad H = \bigcup_{s\in S} sK$$

و لذا

$$G = \bigcup_{t\in t} t(\bigcup_{s\in S} sK) = \bigcup_{t\in T}\bigcup_{s\in S} tsK = \bigcup_{(t,s)\in T\times S} tsK.$$

اگر نشان دهیم که هم‌دسته‌های چپ tsK مجزا هستند آنگاه باید

$$[G:K] = |T\times S| = |T|\,|S| = [G:H]\,[H:K].$$

پس فرض کنیم $tsK = t's'K$. لذا $ts \in t's'K$ و این یعنی $ts = t's'k$ که $k \in K$. چون $s \in K \leq H$ پس $tsH = t(sH) = tH$. بنابراین با روشی کاملا مشابه خواهیم داشت $tsH = t's'kH = t'(s'k'H) = t'H$. پس $tH = t'H$. اما T تراگشتی چپ برای H در G است لذا باید $t = t'$. بلافاصله داریم $s = s'k$. یعنی $sK = s'kK = s'(kK) = s'K$. اما S تراگشتی چپ برای K در H است لذا باید $s = s'$. □

مثال ۳۷.۷.۲. *می‌خواهیم اندیس زیرگروه $15\mathbb{Z}$ در گروه $G = (3\mathbb{Z}, +)$ را پیدا کنیم. طبق اولین مثال این بخش داریم $[\mathbb{Z} : 3\mathbb{Z}] = 3$ و $[\mathbb{Z} : 15\mathbb{Z}] = 15$. طبق قضیه ۳۶.۷.۲ داریم*

$$[3\mathbb{Z} : 15\mathbb{Z}] = \frac{[\mathbb{Z} : 15\mathbb{Z}]}{[\mathbb{Z} : 3\mathbb{Z}]} = 5.$$

قضیه ۳۸.۷.۲. *فرض کنیم G یک گروه باشد و $H, K \leq G$. در این صورت*

$$[G : H \cap K] \leq [G : K].$$

همچنین وقتی $[G : K] < \infty$، در بالا تساوی رخ می‌دهد اگر و تنها اگر $G = KH$.

اثبات. ابتدا دقت کنید که $H \cap K$ زیرگروه H و K است. حال ضابطه

$$f : (H/(H \cap K))_l \longrightarrow (G/K)_l, \quad f(h(H \cap K)) = hK$$

یک تابع خوشتعریف است. زیرا اگر فرض کنیم $h(H \cap K) = h'(H \cap K)$ آنگاه از لم ۱۵.۷.۲ باید $h^{-1}h' \in H \cap K \leq K$. دوباره طبق لم ۱۵.۷.۲ باید $hK = h'K$ یعنی $f(h(H \cap K)) = f(h'(H \cap K))$.
حال اگر برای $h, h' \in H$ داشته باشیم $hK = h'K$ آنگاه از لم ۱۵.۷.۲ $h^{-1}h' \in K$. اما $h^{-1}h \in H$ پس $h^{-1}h' \in H \cap K$ و طبق لم ۱۵.۷.۲ باید $h(H \cap K) = h'(H \cap K)$. یعنی f یک‌به‌یک است. پس

$$[G : H \cap K] = |(H/(H \cap K))_l| \leq |(G/K)_l| = [G : K].$$

برای قسمت دوم، فرض کنیم $[G : H \cap K] = [G : K]$. این یعنی f پوشا است. زیرا f یک‌به‌یک و $|(G/K)_l| = [G : K] < \infty$ است. حال فرض کنیم $g \in G$. هم دسته چپ gK را درنظر می‌گیریم. چون f پوشا است، عنصر $h \in H$ چنان وجود دارد که

$$hK = (fh(H \cap K)) = gK.$$

طبق لم ۱۵.۷.۲ داریم $h^{-1}g \in K$. پس $g = hh^{-1}g = h(h^{-1}g) \in HK$ و لذا $G \subseteq HK$. واضح است که $HK \subseteq G$. پس $G = HK$ و طبق گزاره ۲۹.۴.۲ باید $G = KH$.
اکنون فرض کنیم $G = KH$. طبق گزاره ۲۹.۴.۲ باید $G = HK$. هم دسته چپ gK را در نظر می‌گیریم. پس $g = hk$ که $h \in H$ و $k \in K$. حال داریم

$$f(h(H \cap K)) = hK = hkk^{-1}K = (hk)k^{-1}K = hkK = gK$$

یعنی f پوشا است و اثبات کامل است. □

قضیه ۳۹.۷.۲. *(قضیه پوانکاره) فرض کنیم H و K زیرگروه‌های با اندیس متناهی در گروه G باشند. در این صورت داریم که $[G : H \cap K] < \infty$ و*

$$[G : H \cap K] \leq [G : H][G : K].$$

همچنین در بالا تساوی رخ می‌دهد اگر و تنها اگر $G = KH$.

اثبات. می‌دانیم که $(H \cap K) \leq H \leq G$. طبق قضیه ۳۶.۷.۲ و طبق قضیه ۳۸.۷.۲ داریم که

$$[G : (H \cap K)] = [G : H]\,[H : (H \cap K)] \leq [G : H]\,[G : K] < \infty.$$

برای قسمت دوم، طبق قضیه ۳۸.۷.۲ در بالا (آخرین کوچکتر یا مساوی منظور ما است) تساوی رخ می‌دهد اگر و تنها اگر $[H : (H \cap K)] = [G : K]$ اگر و تنها اگر $G = HK$. □

تمرین‌های حل شده

تمرین ۴۰.۷.۲. *برای زیرگروه $H = \{۱, -۱, j, -j\}$ از گروه $\mathbb{Q}_۸$ هم دسته‌های چپ را بنویسید.*

حل. یکی از هم دسته‌ها خود H است. حال داریم

$$\begin{aligned} iH &= \{i, -i, ij, i(-j)\} = \{i, -i, k, -k\} = (-i)H \\ jH &= \{j, -j, j^۲, -j^۲\} = \{j, -j, -۱, ۱\} = H = (-j)H \\ kH &= \{k, -k, kj, k(-j)\} = \{k, -k, -i, i\} = (-k)H \end{aligned}$$

پس دو هم دسته چپ داریم یکی H و دیگری $\{i, -i, k, -k\}$.

تمرین ۴۱.۷.۲. *فرض کنیم $G = (\mathbb{R}, +)$ باشد. برای گروه $G \times G$ و زیرگروه*

$$H = \{(x, ۰) \in G \times G \mid\ x \in \mathbb{R}\}$$

هم دسته‌های چپ را معلوم کنید ($G \times G$ همان صفحه مختصات است و H محور xها).

حل. برای عنصر دلخواه ولی ثابت $(u, v) \in G \times G$، چون گروه جمعی است داریم

$$\begin{aligned} &(u, v) + H = \{(u, v) + (x, ۰) \mid\ (x, ۰) \in H\} = \\ &\{(u + x, v) \mid\ x, u, v \in \mathbb{R}\} \end{aligned}$$

و این یعنی همه نقاط در صفحه مختصات که همواره عرض v دارند. یعنی خطوط موازی محور xها! پس بیشمار هم دسته چپ داریم.

تمرین ۴۲.۷.۲. *برای گروه $G = (\mathbb{R}, +)$ و زیرگروه $\mathbb{Z}$ هم دسته‌های چپ را معلوم کنید.*

حل. هر عدد حقیقی r به صورت $n+\epsilon$ است که n عدد صحیح و $0 \leq \epsilon < 1$. چون گروه جمعی است داریم

$$r+\mathbb{Z} = \{r+x \mid x \in \mathbb{Z}\} = \{n+\epsilon+x \mid x \in \mathbb{Z}\} = \\ \{m+\epsilon \mid m \in \mathbb{Z}\} =$$

و این یعنی هم دسته‌های چپ به صورت $\epsilon+\mathbb{Z}$ هستند که $0 \leq \epsilon < 1$. پس بیشمار هم دسته چپ داریم.

تمرین ۴۳.۷.۲. *فرض کنیم G یک گروه دوری باشد و H یک زیرگروه مخالف با $\{e\}$. نشان دهید $[G:H]$ متناهی است.*

حل. فرض کنیم $G =< x >$. طبق قضیه ۲۲.۵.۲ داریم $H =< x^k >$ که $k \in \mathbb{N}$ (چرا؟). حال برای عنصر دلخواه و ثابت $x^i \in G$ داریم

$$x^iH = \{x^ih \mid h \in H\} = \{x^i(x^k)^j \mid j \in \mathbb{Z}\} = \\ \{x^ix^{jk} \mid j \in \mathbb{Z}\} = \{x^{i+jk} \mid j \in \mathbb{Z}\}.$$

برای این که هم دسته چپ تکراری حاصل نشود باید i از مجموعه $\{0, 1, 2, ..., k-1\}$ انتخاب شود. یعنی $[G:H] = k$.

تمرین ۴۴.۷.۲. *فرض کنیم G یک گروه و $H \leq G$. در این صورت $G \setminus H$ متناهی است اگر و تنها اگر $G = H$ یا G متناهی باشد.*

حل. فرض کنیم $G \setminus H$ متناهی است و $G \neq H$. نشان می‌دهیم G متناهی است. طبق قضیه ۸.۷.۲ هم دسته‌های چپ گروه G را افراز می‌کنند. یکی از این هم دسته‌های چپ خود H است. پس می‌توانیم بنویسیم

$$G = H \cup (\bigcup_{e \neq a \in G} aH)$$

که در آن $\bigcup_{e \neq a \in G} aH$ حتما ناتهی است، زیرا $G \neq H$. به روشنی $\bigcup_{e \neq a \in G} aH \subseteq (G \setminus H)$. یعنی $\bigcup_{e \neq a \in G} aH$ متناهی است. این نشان می‌دهد که H نیز باید متناهی باشد. زیرا اگر H نامتناهی باشد آنگاه در H نامتناهی عنصر متمایز مانند h_1، h_2، h_3 و ... وجود دارد. چون $\bigcup_{e \neq a \in G} aH$ متناهی است، پس aH متناهی است و لذا باید $ah_i = ah_j$. این نشان می‌دهد که $h_i = h_j$ (چگونه؟) که تناقض آشکار است. حال H متناهی و $\bigcup_{e \neq a \in G} aH$ متناهی پس باید G متناهی باشد.
برعکس، بسیار بدیهی است.

تمرین ۴۵.۷.۲. *برای اعداد اول p و q نشان دهید که هر زیرگروه سره از یک گروه pq عضوی دوری است.*

حل. برای زیرگروه سره که فقط شامل عنصر خنثی است، چیزی برای اثبات نداریم. فرض کنیم H یک زیرگروه سره نابدیهی از G باشد. طبق قضیه لاگرانژ، قضیه ۲۳.۷.۲، باید $|H| \mid pq$. پس $|H|$ برابر با p و یا q است. در هر صورت طبق نتیجه ۲۵.۷.۲ کار تمام است.

تمرین ۴۶.۷.۲. *فرض کنیم G گروهی از مرتبه عدد اول باشد. نشان دهید G زیرگروه سره نابدیهی ندارد.*

حل. فرض کنیم H زیرگروه سره نابدیهی از G باشد. طبق قضیه لاگرانژ، قضیه ۲۳.۷.۲، $|H|$ باید مرتبه گروه را بشمارد. اما این یعنی عدد اول شمارنده غیر ۱ و خودش دارد که تناقض آشکار است.

تمرین ۴۷.۷.۲. *فرض کنیم G گروهی متناهی و $d(G)$ کمترین تعداد اعضای از G باشد که G را تولید می‌کند. نشان دهید که $|G|\geq ۲^{d(G)}$.*

حل. برای راحتی فرض می‌کنیم $d(G)=k$. همچنین فرض کنیم $G=<g_۱,g_۲,...,g_k>$. قرار می‌دهیم $H=<g_۱,...,g_{k-۱}>$. ادعا می‌کنیم $d(H)=k-۱$. فرض کنیم $d(H)=t<k-۱$. پس $H=<h_۱,...,h_t>$ و لذا با یک بررسی داریم

$$G=<g_۱,...,g_k>=<H,g_k>=<<h_۱,...,h_t>,g_k>=<h_۱,...,h_t,g_k>.$$

این یعنی G با تعداد کمتر از k عنصر تولید می‌شود که در تناقض با انتخاب ما از k است. پس $d(H)=k-۱$. حال حکم را با اسقرا اثبات می‌کنیم. اگر $k=۰$ آنگاه $G=<\emptyset>=\{e\}$ و به وضوح حکم برقرار است. حال فرض کنیم حکم برای هر گروه H' که $d(H')<k$ درست باشد، یعنی $|H'|\geq ۲^{d(H')}$. چون $d(H)<k$ داریم $|H|\leq ۲^{k-۱}$. اما طبق قضیه لاگرانژ، قضیه ۲۳.۷.۲، داریم $|G|=l\,|H|$ که $l\in\mathbb{N}$. اگر $l=۱$ باشد آنگاه $H=G$ و این یعنی G با تعداد کمتر از k عنصر تولید می‌شود که در تناقض با انتخاب ما از k است. پس $l\geq ۲$. لذا داریم

$$|G|=l\,|H|\geq ۲\;۲^{k-۱}=۲^k.$$

تمرین ۴۸.۷.۲. *فرض کنیم G یک گروه متناهی باشد و $H,K\leq G$. قرار دهید $[G:H]=m$ و $[G:K]=n$. نشان دهید $c\leq[G:(H\cap K)]\leq mn$ که در آن c کوچکترین مضرب مشترک m و n است. در نتیجه اگر m و n نسبت به هم اول باشند تساوی رخ می‌دهد.*

حل. می‌دانیم که $(H\cap K)\leq H\leq G$ و $(H\cap K)\leq K\leq G$. پس طبق قضیه ۳۶.۷.۲ داریم

$$[G:(H\cap K)]=[G:H]\,[H:(H\cap K)]=m[H:(H\cap K)]$$
$$[G:(H\cap K)]=[G:K]\,[K:(H\cap K)]=n[K:(H\cap K)].$$

پس $m|[G:(H\cap K)]$ و $n|[G:(H\cap K)]$ و لذا $c|[G:(H\cap K)]$. اما طبق قضیه پوانکاره، قضیه ۳۹.۷.۲، داریم

$$[G:(H\cap K)]\leq[G:H]\,[G:K]=mn.$$

برای قسمت دوم، چون $c=mn$ است چیزی برای اثبات نداریم.

تمرین ۴۹.۷.۲. *فرض کنیم H و K زیرگروه‌هایی از گروه متناهی G باشند به طوری که داشته باشیم $([G:H],[G:K])=۱$. نشان دهید که $G=HK$ و در نتیجه $HK=KH$.*

حل. طبق نتیجه ۲۶.۷.۲ داریم $H \cap K = \{e\}$. پس طبق تمرین قبلی داریم

$$|G| = [G : \{e\}] = [G : (H \cap K)] = [G : H]\,[G : K].$$

اما طبق قضیه لاگرانژ، قضیه ۲۳.۷.۲ داریم $|G| = |H|\,[G : H]$ و $|G| = |K|\,[G : K]$. این ایجاب می‌کند که $|G| = |H|\,|K| = [G : H][G : K]$. اکنون طبق قضیه ۳۱.۴.۲ باید $|HK| = |H|\,|K| = |G|$. چون $HK \subseteq G$ نتیجه می‌شود که $G = HK$. قسمت دوم نتیجه بدیهی از گزاره ۲۹.۴.۲ است.