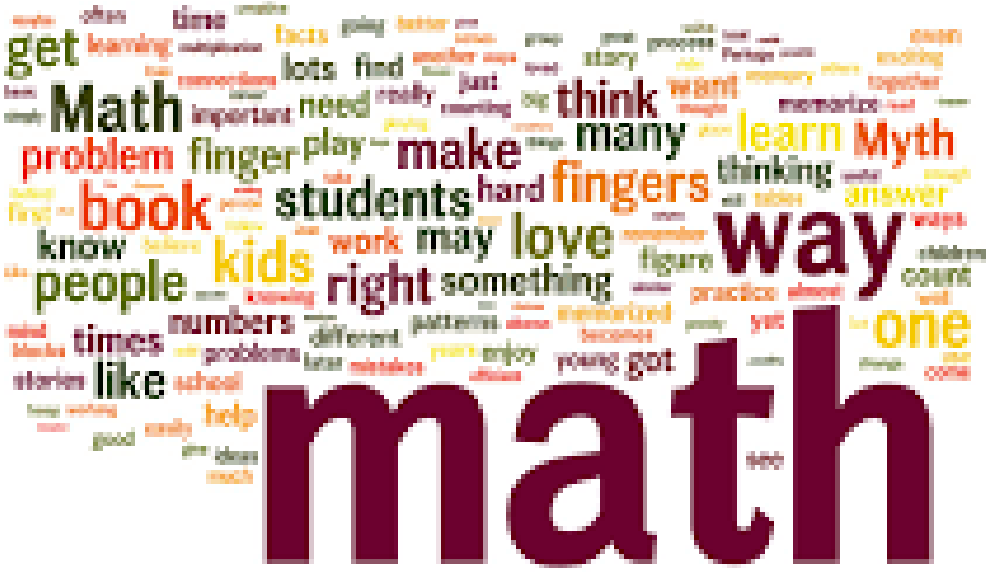
دانشگاه صنعتی اصفهان
دانشکده علوم ریاضی

جبر (دوره کارشناسی)

محمود بهبودی[1]



۲۲ شهریور ۱۳۹۷

[1] دانشیار دانشکده ریاضی دانشگاه صنعتی اصفهان

این نوشتار جهت استفاده دانشجویان کارشناسی ارشد 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

مباحثی در نظریه گروه‌ها

گروه‌ها یکی از مهم‌ترین ساختارهای جبری هستند که نقش اساسی در جبر مجرد دارند و در علوم مختلف مانند بلورشناسی و فیزیک کوانتم از اهمیت بالایی برخوردارند. همچنین گروه‌ها در شاخه‌های گوناگون ریاضیات چون هندسه جبری، توپولوژی جبری، نظریه جبری اعداد و ... استفاده می‌شود. از این‌رو مطالعه گروه‌ها حائز اهمیت است. در این فصل می‌خواهیم تا حدی مطالبی را که از گروه‌ها در درس مبانی جبر آموخته‌اید، تکمیل نماییم. بنابراین لازم است که اگر دانشجو برخی مفاهیم را از درس مبانی جبر از یاد برده، آن را مرور کند (مفاهیمی مانند گروه، زیرگروه، گروه دوری، زیرگروه نرمال، قضیه لاگرانژ، هم‌دسته، مرتبه گروه و عنصر، گروه خارج قسمت، قضیه‌های همریختی).

۱.۱ حاصل ضرب مستقیم گروه‌ها

در این بخش می‌خواهیم با کمک چند گروه یک گروه جدید بسازییم که اهمیت بالایی در ارائه قضایای ساختاری گروه دارد. با لم بدیهی زیر کار را آغاز می‌کنیم.

لم ۱.۱.۱. *فرض کنیم G_1، ...، G_n یک خانواده از گروه‌ها باشد. در این صورت حاصل ضرب دکارتی این گروه‌ها یعنی*

$$G_1 \times ... \times G_n = \{(g_1, ..., g_n) \mid g_i \in G_i\}$$

با عمل طبیعی

$$(g_1, ..., g_n).(g'_1, ..., g'_n) = (g_1 g'_1, ..., g_n g'_n)$$

یک گروه است.

اثبات. سر راست است. □

تعریف ۲.۱.۱. *فرض کنیم G_1، ...، G_n یک خانواده از گروه‌ها باشد. در این صورت به گروه $G_1 \times ... \times G_n$ که در لم ۱.۱.۱ معرفی شد، گروه حاصل ضرب مستقیم خارجی گروه‌های G_1، ...، G_n گوییم.*

ممکن این سوال مطرح شود که آیا ارتباطی بین ضرب خارجی زیرگروه‌های یک گروه و ضرب (عادی) زیرگروه وجود دارد؟ در قضیه مهم زیر به این سوال پاسخ می‌دهیم که چه زمانی یک گروه با حاصل ضرب مستقیم خانواده متناهی از زیرگروه‌هایش یکریخت است.

قضیه ۳.۱.۱. *فرض کنیم H_1، ...، H_n خانواده‌ای از زیرگروه‌های گروه G باشد و به علاوه $G = H_1H_2...H_n$. در این صورت شرایط زیر معادل هستند.*
(۱) همریختی طبیعی $\pi : H_1 \times ... \times H_n \longrightarrow G$ یکریختی است (یادآوری می‌کنیم که: $\pi((h_1, ..., h_n)) = h_1h_2...h_n$).
(۲) هر H_i یک زیرگروه نرمال از G است و هر عنصر $g \in G$ به صورت یکتا به شکل $g = h_1h_2...h_n$ نوشته می‌شود که $h_i \in H_i$.
(۳) هر H_i یک زیرگروه نرمال از G است و اگر $h_1h_2...h_n = e$ آنگاه برای هر i داریم $h_i = e$.
(۴) هر H_i یک زیرگروه نرمال از G است و برای هر i داریم

$$H_i \cap (H_1...H_{i-1}H_{i+1}...H_n) = \{e\}.$$

اثبات. (۱) $\Leftarrow$ (۲). قرار می‌دهیم

$$H'_i = \{(e, e, ..., h_i, e, ..., e) \mid h_i \in H_i\}.$$

بررسی سر راست نشان می‌دهد که H'_i در $H_1 \times ... \times H_n$ نرمال است. اما طبق فرض π یکریختی است پس $\pi(H'_i) = H_i$ باید در H نرمال باشد. که اثبات قسمت اول را تکمیل می‌کند. برای قسمت دوم، فرض کنیم

$$h_1...h_n = g = h'_1...h'_n$$

که $h_i, h'_i \in H_i$. لذا

$$\pi((h_1, ..., h_n)) = g = \pi((h'_1, ..., h'_n)).$$

در نتیجه چون π یک به یک است، برای هر i داریم که $h_i = h'_i$. پس g نمایش یکتا دارد.
(۲) $\Leftarrow$ (۳). طبق فرض هر H_i یک زیرگروه نرمال از G است. حال فرض کنیم $e = h_1h_2...h_n$. اما $e = ee...e$. طبق فرض یکتایی برای هر i داریم $h_i = e$.
(۳) $\Leftarrow$ (۴). طبق فرض هر H_i یک زیرگروه نرمال از G است. برای قسمت دوم، ابتدا نشان می‌دهیم که $H_i \cap H_j = \{e\}$ برای هر $i \neq j$. اگر $h_i \in H_i$ و $h_j \in H_j$ که $h_i = h_j$ آنگاه $e = h_ih_j^{-1}$. بنابراین طبق فرض $h_i = h_j = e$. حال نشان می‌دهیم که برای هر $x \in H_i$ و هر $y \in H_j$ که $i \neq j$ داریم $xy = yx$. طبق فرض داریم که H_i در G نرمال است پس $yxy^{-1} \in H_i$. اما H_i زیرگروه است در نتیجه $x^{-1} \in H_i$. پس $yxy^{-1}x^{-1} \in H_i$. حال

اما H_j زیرگروه است در نتیجه $y^{-۱} \in H_j$. طبق فرض داریم که H_j در G نرمال است پس $xy^{-۱}x^{-۱} \in H_j$ و در نتیجه $yxy^{-۱}x^{-۱} \in H_j$. اما نشان دادیم که $H_i \cap H_j = \{e\}$ در نتیجه $xy = yx$. حال می‌توانیم $H_i \cap (H_۱...H_{i-۱}H_{i+۱}...H_n) = \{e\}$ را نشان دهیم. فرض کنیم $x \in H_i \cap (H_۱...H_{i-۱}H_{i+۱}...H_n)$. پس

$$h_i = x = h_۱...h_{i-۱}h_{i+۱}...h_n$$

که $h_l \in H_l$. اما همه $h_l \in H_l$ جابجا می‌شوند پس $e = h_۱h_۲...h_{i-۱}h_i^{-۱}h_{i+۱}...h_n$. اکنون طبق فرض برای هر l داریم $h_l = e$. در نتیجه $x = e$ و حکم به دست می‌آید.
(۴) $\Leftarrow$ (۱). کافی است نشان دهیم که π یک به یک است (چرا؟). از طرفی مشابه با آنچه در حالت "(۳) $\Leftarrow$ (۴)" دیدیم، می‌توانیم نشان دهیم که برای هر $x \in H_i$ و هر $y \in H_j$ که $i \neq j$ داریم $xy = yx$. حال اگر $(h_۱, ..., h_n) \in Ker\pi$ آنگاه $h_۱h_۲...h_n = e$. در نتیجه $h_۱^{-۱} = h_۲...h_n$. اما طبق فرض $H_۱ \cap (H_۲...H_i...H_n) = \{e\}$. بنابراین $h_۱ = e$. به صورت مشابه و استقرایی (و این مطلب که همه $h_l \in H_l$ جابجا می‌شوند) می‌توان نشان داد که $h_۲ = ... = h_n = e$ و اثبات کامل است. □

تعریف ۴.۱.۱. *اگر گروه G در یکی از شرایط معادل قضیه ۱.۱.۳، صدق کند آنگاه گوییم G حاصل ضرب مستقیم داخلی زیرگروه‌های $H_۱$، ...، H_n است و به H_i ها جمعوند گوییم.*

تذکر ۵.۱.۱. *هر گاه زیرگروه‌های $H_۱$، ...، H_n از گروه G در یکی از شرایط معادل قضیه ۱.۱.۳، صدق کند آنگاه از گفتن کلمه داخلی و خارجی صرف نظر می‌کنیم. دقت شود که همیشه حاصل ضرب خارجی $H_۱$، ...، H_n وجود دارد (این همان صورت معادل اصل انتخاب است) اما حاصل ضرب داخلی موجود است اگر و تنها اگر یکی از شرایط معادل قضیه ۱.۱.۳، رخ دهد (تمرین‌های حل شده را ببینید). اگر گروه جمعی باشد حاصل ضرب داخلی $H_۱$، ...، H_n را به صورت $H_۱ \oplus ... \oplus H_n$ می‌نویسیم و به آن مجموع مستقیم می‌گوییم.*

مثال ۶.۱.۱. *گروه $(\mathbb{Z}_۶, +)$ را در نظر بگیرید. این گروه دو زیرگروه نرمال به صورت*

$$H = \{\bar{۰}, \bar{۳}\} \cong \mathbb{Z}_۲$$
$$K = \{\bar{۰}, \bar{۲}, \bar{۴}\} \cong \mathbb{Z}_۳$$

دارد. واضح است که $H \cap K = \bar{۰}$. پس طبق قضیه ۱.۱.۳، داریم

$$\mathbb{Z}_۶ = H \oplus K \cong H \times K \cong \mathbb{Z}_۲ \times \mathbb{Z}_۳.$$

برای این گروه هم حاصل ضرب خارجی و هم داخلی یکریختند. از این رو گاهی از آوردن واژه داخلی و خارجی صرف نظر می‌کنیم.

این بخش را با گزاره زیر به پایان می‌رسانیم.

گزاره ۷.۱.۱. *فرض کنیم G گروهی جمعی باشد و زیرگروه‌های $H_۱$، ...، H_n از گروه G در یکی از شرایط معادل قضیه ۱.۱.۳، صدق کند آنگاه $H_۱ \times ... \times H_n \cong H_۱ \oplus .. \oplus H_n$.*

اثبات. ابتدا دقت شود که هر عضو $H_1 \oplus ... \oplus H_n$ به صورت یکتا به شکل $h_1 + h_2 + ... + h_n$ است. حال رابطه

$$f : H_1 \oplus ... \oplus H_n \longrightarrow H_1 \times ... \times H_n, \quad f(h_1 + ... + h_n) = (h_1, ..., h_n)$$

با یک بررسی ساده یکریختی گروهی است. □

تمرین حل شده

تمرین ۸.۱.۱. *فرض کنیم G گروهی متناهی باشد که مرتبه هر عنصر غیر همانی برابر ۲ است. آنگاه G حاصل ضرب داخلی گروه‌های دوری از مرتبه ۲ است.*

اثبات. برای هر عنصر g در G چون مرتبه g برابر ۲ است پس $g = g^{-1}$. در نتیجه G گروهی آبلی است (چرا؟). فرض کنیم g_1 عنصر غیر همانی در G باشد. اگر $G =< g_1 >$ کار تمام است. پس فرض کنیم که $G \neq < g_1 >$. پس $g_2 \in G \setminus < g_1 >$ و $< g_2 >$ را در نظر بگیرید. چون G آبلی است تمام زیرگروه‌ها نرمال هستند. اگر $x \in < g_1 > \cap < g_2 >$ آنگاه چون مرتبه هر عضو دو است، پس باید $x = e$ باشد. حال اگر $G =< g_1 >< g_2 >$ آنگاه طبق قضیه ۳.۱.۱، قسمت (۴)، کار تمام است، در غیر این صورت روند بالا را تکرار می‌کنیم و چون G متناهی است پس باید $G =< g_1 >< g_2 > ... < g_n >$ و اثبات تمام است. □

تمرین ۹.۱.۱. *نشان دهید که گروه جمعی $\mathbb{Z}_{16}$ را نمی‌توان مجموع مستقیم دو تا از زیرگروه‌های نابدیهی نوشت.*

اثبات. می‌دانیم که زیرگروه‌های $\mathbb{Z}_{16}$ دو به دو قابل مقایسه هستند. پس زیرگروه‌های نابدیهی حتما اشتراک نابدیهی دارند. پس طبق قضیه ۳.۱.۱، قسمت (۴)، مسئله حل شده است. □

تمرین ۱۰.۱.۱. *نشان دهید که گروه جمعی $\mathbb{Z}_{10}$ جمع مستقیم دو تا از زیرگروه‌هایش است.*

اثبات. کافی است قرار دهیم

$$H_1 = \{\bar{0}, \bar{5}\}, \quad H_2 = \{\bar{0}, \bar{2}, ..., \bar{8}\}.$$

به وضوح $H_1 \cap H_2 = \{\bar{0}\}$ و $\mathbb{Z}_{10} = H_1 + H_2$. پس طبق قضیه ۳.۱.۱، قسمت (۴)، مسئله حل شده است. □

تمرین ۱۱.۱.۱. *فرض کنیم G یک گروه دوری از مرتبه mn باشد که $(m, n) = 1$. نشان دهید G حاصل ضرب مستقیم دو تا از زیرگروه‌های نابدیهی خودش است.*

اثبات. چون G دوری است یک و فقط یک زیرگروه از مرتبه m مانند H و یک و فقط یک زیرگروه از مرتبه n مانند K دارد (چرا؟). اما $H \cap K = \{e\}$ زیرا مرتبه $H \cap K$ هم m و هم n را می‌شمارد و چون $(m, n) = 1$ پس $H \cap K = \{e\}$. حال می‌دانیم

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

چون $HK \subseteq G$ پس $G = HK$. چون G آبلی است هر زیرگره آن نرمال است. اکنون طبق قضیه ۳.۱.۱، قسمت (۴)، $G \cong H \times K$. □

تمرین ۱۲.۱.۱. *نشان دهید گروه جمعی $\mathbb{Q}$ جمع مستقیم داخلی هیچ دو تا زیرگروه نابدیهی خودش نیست.*

اثبات. به برهان خلف، اگر $\mathbb{Q} = H_1 \oplus H_2$ باشد که H_1 و H_2 نابدیهی هستند آنگاه دو عنصر ناصفر $\frac{m}{n}$ و $\frac{p}{q}$ به ترتیب در H_1 و H_1 وجود دارند. حال داریم

$$np(\frac{m}{n}) = pm = qm\frac{p}{q} \in H_1 \cap H_2.$$

پس H_1 و H_1 اشتراک غیر صفر دارند که با قضیه ۳.۱.۱، قسمت (۴)، تناقض دارد. □

۲.۱ عمل یک گروه روی مجموعه

تعریف ۱.۲.۱. *فرض کنیم G یک گروه و S یک مجموعه ناتهی باشد. در این صورت گوییم G روی S عمل می‌کند هرگاه تابعی مانند $* : G \times S \longrightarrow S$ موجود باشد به طوری که برای هر $a, b \in G$ و $s \in S$ ویژگی‌های زیر برقرار باشند:*
(۱) $a * (b * s) = (ab) * s$
(۲) $e * s = s$ *که در آن e همانی گروه G است.*
تابع $*$ را عمل گروه G روی S می‌نامند و می‌گویند S یک Gـ مجموعه است.

مثال ۱.۲.۱. *فرض کنیم که G یک گروه و قرار می‌دهیم $S = G$. تعریف می‌کنیم*

$$* : G \times G \longrightarrow G, \quad g * g' = gg'.$$

بررسی سر راست زیر نشان می‌دهد که $*$ یک تابع است که در خواص (۱) و (۲) صدق می‌کند.
بررسی خاصیت (۱):

$$g * (g' * g'') = g * (g'g'') = gg'g'' = (gg') * g''.$$

بررسی خاصیت (۲):

$$e * g = eg = g.$$

پس G یک Gـ مجموعه است.

مثال ۱.۲.۱. *فرض کنیم که $G = (\mathbb{Q} \setminus \{0\}, .)$ گروه ضربی اعداد گویا، $S = \mathbb{R}$ و رابطه زیر را در نظر می‌گیریم*

$$q * r = qr.$$

یک بررسی سر راست نشان می‌دهد که $*$ یک تابع است که در خواص (۱) و (۲) صدق می‌کند.
بررسی خاصیت (۱):

$$q * (q' * r) = q * q'r = qq'r = (qq') * r.$$

بررسی خاصیت (۲):

$$1 * r = 1r = r.$$

یعنی S یک Gـ مجموعه است.

مثال ۱.۲.۱. *فرض کنیم $G = S_n$ گروه جایگشت‌ها روی مجموعه n عضوی باشد قرار می‌دهیم $S = \{1, 2, ..., n\}$. در این صورت رابطه زیر را در نظر می‌گیریم*

$$* : G \times S \longrightarrow S, \quad \sigma * i = \sigma(i).$$

به وضوح $*$ یک تابع است که در خواص (۱) و (۲) صدق می‌کند.
بررسی خاصیت (۱):

$$\sigma * (\sigma' * i) = \sigma * \sigma'(i) = \sigma(\sigma'(i)) = (\sigma\sigma') * i$$

بررسی خاصیت (۲):

$$id * i = id(i) = i$$

پس S یک Gـ مجموعه است.

مثال زیر منجر به یک تعریف می‌شود.

مثال ۱.۲.۵. *(عمل تزویج) فرض کنیم که G یک گروه و قرار می‌دهیم $S = G$. در این صورت رابطه زیر را در نظر می‌گیریم*

$$* : G \times G \longrightarrow G, \quad a * g = aga^{-1}.$$

یک بررسی سر راست نشان می‌دهد که $*$ یک تابع است که در خواص (۱) و (۲) صدق می‌کند.
بررسی خاصیت (۱):

$$a * (a' * g) = a * (a'ga'^{-1}) = aa'ga'^{-1}a^{-1} = (aa')g(aa')^{-1} = (aa') * g.$$

بررسی خاصیت (۲):

$$e * g = ege^{-1} = ege = g.$$

پس G یک Gـ مجموعه است. این عمل گروه G روی خودش را عمل تزویج می‌نامند.

در ادامه می‌خواهیم مدار را تعریف کنیم. برای این منظور نیاز به کمی مقدمات داریم.

تعریف ۱.۲.۶. *فرض کنیم G یک گروه باشد و روی مجموعه S عمل کند. تعریف می‌کنیم که $s_1, s_2 \in S$ در رابطه $\sim$ هستند (و با $s_1 \sim s_2$ نشان می‌دهیم) اگر و تنها اگر $g \in G$ چنان موجود باشد که $g * s_1 = s_2$.*

لم ۱.۲.۷. *فرض کنیم G یک گروه باشد و روی مجموعه S عمل کند. رابطه $\sim$ که در تعریف ۱.۲.۶، معرفی شد یک رابطه هم‌ارزی است. در نتیجه اعضای S به کلاس‌های هم‌ارزی افراز می‌شوند.*

اثبات. بررسی خاصیت انعکاسی: فرض کنیم $s \in S$ و e همانی گروه باشد

$$e * s = s \Rightarrow s \sim s.$$

بررسی خاصیت تقارنی: فرض کنیم که $s \sim s'$. پس $g \in G$ چنان و جود دارد که $g * s = s'$. چون G گروه است پس $g^{-1} \in G$ و در نتیجه $g^{-1} * s' = g^{-1} * (g * s)$ برقرار است. طبق خاصیت‌های عمل، تساوی زیر را داریم

$$g^{-1}s' = g^{-1} * (g * s) = (g^{-1}g) * s = e * s = s.$$

پس $s' \sim s$.
بررسی خاصیت تعدی: فرض کنیم $s_1 \sim s_2$ و $s_2 \sim s_3$. پس $g_1, g_2 \in G$ چنان وجود دارند که

$g_۱ * s_۱ = s_۲$ و $g_۲ * s_۲ = s_۳$. چون G گروه است پس $g = g_۲g_۱ \in G$ و از خاصیت (۱) عمل داریم

$$g * s_۱ = (g_۲g_۱) * s_۱ = g_۲ * (g_۱ * s_۱) = g_۲ * s_۲ = s_۳.$$

یعنی $s_۱ \sim s_۳$. □

اکنون لم بالا مجوز تعریف زیر را فراهم می‌کند و می‌توانیم به وعده خود عمل کنیم.

تعریف ۸.۲.۱. *فرض کنیم G یک گروه باشد و روی مجموعه S عمل کند. هر کلاس هم‌ارزی که از رابطه هم‌ارزی $\sim$ روی S به وجود می‌آید را یک مدار می‌نامیم. مدار $x \in S$ را با $\bar{x}$ نشان می‌دهیم و*

$$\bar{x} = \{s \in S \mid g * x = s, \ \ g \in G \text{ برای برخی}\} = \{g * x \mid g \in G\}.$$

تعریف ۹.۲.۱. *فرض کنیم G یک گروه باشد و روی مجموعه S عمل کند. منظور از پایدارساز $x \in S$ که با G_x نشان می‌دهیم مجموعه زیر است*

$$G_x = \{g \in G \mid g * x = x\}.$$

لم ۱۰.۲.۱. *فرض کنیم G یک گروه باشد و روی مجموعه S عمل کند. برای هر $x \in G$، G_x یک زیرگروه از G است.*

اثبات. عنصر دلخواه x و (از این لحظه ثابت) را در S در نظر می‌گیریم. چون $e \in G$ پس $e*x = x$ و این یعنی G_x ناتهی است. حال فرض می‌کنیم که $g, g' \in G_x$. پس طبق تعریف $g * x = x$ و $g' * x = x$. حال داریم

$$(g'g) * x = g' * (g * x) = g' * x = x.$$

یعنی $g'g \in G_x$. از طرفی دیگر چون $g * x = x$ پس

$$x = e * x = (g^{-۱}g) * x = g^{-۱} * (g * x) = g^{-۱} * x.$$

یعنی $g^{-۱} \in G_x$. بنابراین G_x زیرگروه است. □

نمادگذاری ۱۱.۲.۱. *تعداد اعضای مجموعه A (مدار $\bar{x}$) را با $|A|$ ($|\bar{x}|$) نشان می‌دهیم.*

تذکر ۱۲.۲.۱. *طبق لم ۱۰.۲.۱، عبارت $[G : G_x]$ (اندیس یا شاخص G_x در G) با معنی است.*

حال قضیه زیر تعداد اعضای یک مدار رانشان می‌دهد.

قضیه ۱۳.۲.۱. *اگر گروه G روی مجموعه S عمل کند و $x \in S$ آنگاه $|\bar{x}| = [G : G_x]$.*

اثبات. رابطه زیر را در نظر می‌گیریم

$$\begin{cases} \theta : \{gG_x \mid g \in G\} \longrightarrow \bar{x} = \{g * x \mid g \in G\} \\ \quad \theta(gG_x) = g * x \end{cases}$$

ابتدا نشان می‌دهیم که θ خوش‌تعریف (تابع) است.

$$gG_x = g'G_x \;\Rightarrow\; g^{-1}g'G_x \;\Rightarrow\; g^{-1}g' \in G_x$$

در نتیجه

$$(g^{-1}g')*x = x \;\Rightarrow\; g*[(g^{-1}g')*x] = g*x \;\Rightarrow\; (gg^{-1}g')*x = g*x \;\Rightarrow\; g'*x = g*x.$$

یعنی θ خوش‌تعریف است. عکس خوش‌تعریفی، یک به یک بودن θ را نشان می‌دهد. پوشایی θ نیز واضح است. بنابراین $|\bar{x}| = [G : G_x]$. □

نتیجه ۱.۲.۱۴. *اگر گروه G روی مجموعه متناهی S عمل کند آنگاه $|S| = \sum_{t\in S'}[G : G_t]$ که در آن S' زیرمجموعه‌ای از S که شامل دقیقا یک عنصر از هر مدار است.*

اثبات. طبق لم ۱.۲.۷، زیرمجموعه S' از S چنان وجود دارد که

$$S = \bigcup_{t\in S'} \bar{t} \qquad \text{(اجتماع مدارهای جدا)}$$

و چون S متناهی است پس

$$|S| = \sum_{t\in S'} |\bar{t}| = \sum_{t\in S'} [G : G_t]$$

و اثبات تمام است. □

در ادامه می خواهیم حالتی که G روی خودش با تزویج عمل می‌کند (مثال ۱.۲.۵) را بررسی کنیم. قضیه‌ای را بیان می‌کنیم که صورتی از قضیه ۱.۲.۱۳ و نتیجه ۱.۲.۱۴ است اما اثبات را مجدد تکرار خواهیم کرد چرا که ممکن است خواننده فقط به تزویج علاقمند باشد. در ابتدا یک تعریف و یک یادآوری را بیان می‌کنیم.

تعریف ۱.۲.۱۵. *فرض کنیم که G روی خودش با تزویج عمل می‌کند (مثال ۱.۲.۵). در این صورت مدار هر عنصر $g \in G$ را رده تزویجی نامیم و با $C(g)$ نشان می‌دهیم، یعنی*

$$C(g) = \{aga^{-1} \mid a \in G\}.$$

یادآوری ۱.۲.۱۶. *فرض کنیم G یک گروه باشد و $g \in G$. نرمال‌ساز g در G به صورت زیر تعریف می‌شود*

$$N(g) = \{a \in G \mid aga^{-1} = g\}.$$

قضیه ۱۷.۲.۱. *فرض کنیم G یک گروه باشد. در این صورت گزاره‌های زیر برقرارند:*
(الف) مجموعه رده‌های تزویجی G را افراز می‌کند.
(ب) $|C(g)| = [G : N(g)]$ که $g \in G$.
(ج) اگر G متناهی باشد آنگاه $|G| = \sum_{g\in T}[G : N(g)]$ که T زیرمجموعه‌ای از G شامل دقیقا یک عنصر از هر رده تزویجی است.

اثبات. (الف) طبق مثال ۵.۲.۱ و لم ۷.۲.۱، G افراز می‌شود و کلاس هم‌ارزی g در G مجموعه

$$\bar{g} = \{xgx^{-1} \mid x \in G\}$$

است که همان $C(g)$، رده تزویجی g است. پس $G = \bigcup C(g)$ یک اجتماع دو به دو مجزا از رده‌های تزویجی.
(ب) رابطه زیر را در نظر می‌گیریم

$$\begin{cases} \theta : C(g) \longrightarrow G/N(g) \\ \quad \theta(xgx^{-1}) = xN(g) \end{cases}$$

این که θ خوش‌تعریف، یک به یک و پوشا است سر راست است (اثبات قضیه ۱۳.۲.۱ را ببینید). پس $|C(g)| = |G/N(g)| = [G : N(g)]$.
(ج) طبق (الف) زیرمجموعه T از G چنان وجود دارد که

$$G = \bigcup_{g\in T} C(g) \qquad \text{(اجتماع رده‌های تزویجی جدا)}$$

و چون G متناهی است پس طبق (ب)

$$|G| = \sum_{g\in T} |C(g)| = \sum_{g\in T} [G : N(g)]$$

و اثبات تمام است. □

تذکر ۱۸.۲.۱. *به تساوی قسمت (ج) از قضیه ۱۷.۲.۱، معادله رده‌ای گویند.*

اکنون می‌خواهیم این بخش را با قضیه برنساید که کاربرد وسیعی در ترکیبیات دارد به پایان ببریم. برای این منظور نیاز به یک تعریف داریم.

تعریف ۱۹.۲.۱. *فرض کنیم G یک گروه باشد و روی مجموعه S عمل کند. در این صورت برای هر $g \in G$ تعریف کنید*

$$S_g = \{s \in S \mid g * s = s\}.$$

قضیه ۱.۲.۲۰. *(برنساید) اگر G گروهی متناهی و روی مجموعه ناتهی و متناهی S عمل کند و تعداد مدارهای S برابر m باشد، آنگاه*

$$m = \frac{۱}{|G|}\sum_{g\in G}|S_g|.$$

اثبات. فرض کنیم که $W = \{(g,s) \in G \times S \mid g * s = s\}$. حال $g' \in G$ را دلخواه ولی ثابت در نظر می‌گیریم. حال تعداد زوج‌های مرتب (g', s) در W دقیقا برابر است با $|S_{g'}|$. اکنون فرض کنیم $s' \in S$ دلخواه ولی ثابت باشد. در این صورت تعداد زوج‌های مرتب (g, s') در W دقیقا برابر است با $|G_{s'}|$. در نتیجه تساوی

$$\sum_{g\in G}|S_g| = |W| = \sum_{s\in S}|G_s|$$

برقرار است. اما طبق قضیه ۱۳.۲.۱، $|\bar{s}| = [G : G_s]$. از طرفی دیگر چون G متناهی است، پس $[G : G_s] = |G|/|G_s|$. لذا

$$|W| = \sum_{s\in S}|G_s| = \sum_{s\in S}\frac{|G|}{\bar{s}} = |G|\sum_{s\in S}\frac{۱}{\bar{s}}.$$

حال فرض کنیم که S' زیرمجموعه‌ای از S باشد که شامل دقیقا یک عنصر از هر مدار است. پس $|S'| = m$ و داریم

$$\sum_{s\in S}\frac{۱}{\bar{s}} = \sum_{t\in S'}\sum_{s\in\bar{t}}\frac{۱}{\bar{s}}.$$

حال برای هر $s \in \bar{t}$ داریم $|\bar{s}| = |\bar{t}|$ و در نتیجه

$$\sum_{s\in\bar{t}}\frac{۱}{\bar{s}} = ۱.$$

بنابراین $|W| = m|G|$ و این اثبات را تمام می‌کند. □

تمرین حل شده

تمرین ۱.۲.۲۱. *فرض کنیم که S مجموعه تمام اعداد مختلط مانند z با شرط $|z| = ۱$ باشد و $G = (\mathbb{R}, +)$ (اعداد حقیقی با جمع معمولی). در این صورت با رابطه*

$$* : G \times S \longrightarrow S, \quad r * z = e^{ir}z$$

که در آن عمل r دوران به اندازه r رادیان در خلاف جهت عقربه ساعت است. S یک Gـ مجموعه است.

اثبات. به وضوح $*$ یک تابع است که در خواص (۱) و (۲) صدق می‌کند.
بررسی خاصیت (۱):

$$r * (r' * z) = r * (e^{ir'}z) = e^{ir}e^{ir'}z = e^{i(r+r')}z = (r + r') * z$$

بررسی خاصیت (۲):

$$0 * z = e^{i0}z = e^{0}z = z$$

و اثبات تمام است. □

تمرین ۲۲.۲.۱. *فرض کنیم که G یک گروه متناهی باشد. در این صورت معادله رده‌ای را می توان به شکل زیر بازنویسی کرد*

$$|G| = |Z(G)| + \sum_{a \in W} [G : C(a)]$$

که W از هر رده تزویجی با بیش از یک عنصر، دقیقا یک نماینده دارد.

اثبات. قرار دهید $S = G$ و عمل را تزویج در نظر بگیرید. برای اثبات تساوی بالا ابتدا نشان می‌دهیم که

$$a \in Z(G) \Leftrightarrow C(a) = \{a\}.$$

فرض کنیم $a \in Z(G)$. پس

$$C(a) = \{xax^{-1} \mid x \in G\} = \{axx^{-1} \mid x \in G\} = \{a \mid x \in G\} = \{a\}.$$

حال فرض کنیم که $C(a) = \{a\}$. بنا به تعریف $C(a)$، برای هر $g \in G$ داریم که $gag^{-1} = a$.
پس $ga = ag$ یعنی $a \in Z(G)$.
اکنون طبق قسمت (الف) از قضیه ۱۷.۲.۱ و مطلبی که در بالا نشان داده‌ایم، G اجتماع جدا از هم $Z(G)$ و تمام رده‌های تزویجی با بیش از یک عنصر است. فرض کنیم W مجموعه‌ای شامل دقیقا یک عنصر از هر رده تزویجی با بیش از یک عنصر است. پس

$$|G| = |Z(G)| + \sum_{a \in W} [G : C(a)].$$

و اثبات کامل است. □

تمرین ۲۳.۲.۱. *فرض کنیم G یک گروه و S یک Gـ مجموعه باشد. گوییم G به صورت متعدی روی S عمل می‌کند هرگاه برای هر $s_1, s_2 \in S$ عنصر $g \in G$ موجود باشد که $g * s_1 = s_2$. در این صورت G به صورت متعدی روی S عمل می‌کند اگر و تنها اگر فقط یک مدار وجود داشته باشد.*

اثبات. فرض کنیم G به صورت متعدی روی S عمل می‌کند و $\bar{x}$ و $\bar{y}$ دو مدار هستند. چون $x, y \in S$ پس طبق فرض $g \in G$ چنان وجود دارد که $g * y = x$. حال فرض کنیم $t \in \bar{x}$. پس عنصر h چنان وجود دارد که $t = h * x$. بنابراین $t = h * (g * y) = (hg) * y$ و این یعنی $t \in \bar{y}$. پس

$\bar{x} \subseteq \bar{y}$. چون $g^{-۱} * x = y$ است پس می‌توان نتیجه گرفت که $\bar{y} \subseteq \bar{x}$ و اثبات تمام است. برعکس، فرض کنیم فقط یک مدار $\bar{x}$ وجود دارد. به علاوه فرض کنیم $u, w \in S$. طبق لم ۷.۲.۱ و فرض، باید $u, w \in \bar{x}$. پس $u = g * x$ و $w = h * x$ که $h, g \in G$. حال قرار دهید $g' = gh^{-۱}$ و داریم

$$g' * w = (gh^{-۱}) * (h * x) = (gh^{-۱}h) * x = g * x = u$$

و اثبات تمام است. □

تمرین ۲۴.۲.۱. *فرض کنیم G یک گروه متناهی و S یک Gـ مجموعه متناهی باشد. اگر G به صورت متعدی روی S عمل کند آنگاه $|G| = |S|$.*

اثبات. طبق تمرین ۲۳.۲.۱، فقط یک مدار $\bar{x}$ که $x \in S$ وجود دارد پس طبق نتیجه ۱۴.۲.۱، $|S| = [G : G_x]$. چون G متناهی است پس $[G : G_x] = |G|/|G_x|$. یعنی $|G| = |G_x||S|$ و اثبات تمام است. □

تمرین ۲۵.۲.۱. *فرض کنیم ۶ مروارید بی رنگ و ۲ اسپری رنگ آبی و قرمز در اختیار دارید. تمام گردن‌بندهای متفاوتی را که می‌توانیم بسازیم، محاسبه کنید.*

اثبات. برای محاسبه تعداد گردن‌بندهای متفاوت می‌خواهیم از قضیه برنساید کمک بگیریم. فرض کنیم $G = \mathbb{Z}_۶$ که گروهی از مرتبه ۶ است. همچنین فرض کنیم که S مجموعه کل گردن‌بندهای ممکن باشد و دقت کنید که تعداد کل گردن‌بندها برابر است با $|S| = ۲^۶ = ۶۴$ (چرا؟). پس اگر s عضوی از S باشد آنگاه s نمایشی به شکل

$$s = s_{i_۱} s_{i_۲} \dots s_{i_۶}$$

دارد. حال S را با عمل زیر به یک Gـ مجموعه تبدیل می‌کنیم

$$\bar{j} * s = s_{\overline{j+i_۱}} s_{\overline{j+i_۲}} \dots s_{\overline{j+i_۶}}$$

که در آن اندیس‌های جدید به پیمانه ۶ است. اکنون واضح است که هر عنصر دلخواه ولی ثابت $\bar{j}$ از گروه G وقتی روی گردن‌بندی عمل می‌کند فقط مرواریدها را به صورت دوری جابجا می‌کند پس تعداد گردن‌بندهای متفاوت برابر است با تعداد مدارها. اما طبق قضیه ۲۰.۲.۱، تعداد کل مدارها برابر است با

$$m = \frac{۱}{۶} \sum_{g \in \mathbb{Z}_۶} |S_g|.$$

پس باید $|S_g|$ها را حساب کنیم. در ادامه برای راحتی مرواریدها را با $s_۰$، ...، $s_۵$ نشان می‌دهیم. داریم که

$$S_{\bar{۰}} = \{s \in S \mid \bar{۰} * s = s\} = S.$$

در نتیجه $|S_{\bar{۰}}| = |S| = ۲^۶$. کار را ادامه می‌دهیم.

$$S_{\bar{۱}} = \{s \in S \mid \bar{۱} * s = s\}.$$

برای این که تساوی $\bar{۱} * s = s$ برقرار باشد باید همه مرواریدها یک رنگ باشند چرا که مثلا فرض کنیم مروارید s به صورت $s_۲s_۳s_۴s_۵s_۰s_۱s_۲$ باشد پس $\bar{۱} * s = s_۳s_۴s_۵s_۰s_۱s_۲$ و برای این که تساوی رخ دهد باید رنگ $s_۲$ همان $s_۳$ و رنگ $s_۳$ همان $s_۴$ و الی آخر باشد یعنی هم رنگی مرواریدها. پس $S_{\bar{۱}}$ شامل گردن‌بند فقط آبی یا فقط قرمز است یعنی $|S_{\bar{۱}}| = ۲$. کار را ادامه می‌دهیم.

$$S_{\bar{۲}} = \{s \in S \mid \bar{۲} * s = s\}.$$

فرض کنیم مروارید s به صورت $s_۰s_۱s_۲s_۳s_۴s_۵$ باشد پس $\bar{۲} * s = s_۲s_۳s_۴s_۵s_۰s_۱$ و برای این که تساوی رخ دهد باید رنگ $s_۲$، $s_۰$ و رنگ $s_۴$ یکی و رنگ بقیه نیز یکی باشد. پس تعداد انتخاب‌های ما ۴ تا است (چرا؟). یعنی $|S_{\bar{۲}}| = ۴$. به صورت مشابه $|S_{\bar{۳}}| = ۸$، $|S_{\bar{۴}}| = ۴$ و $|S_{\bar{۵}}| = ۲$ است. پس

$$m = \frac{۱}{۶}(۶۴ + ۲ + ۴ + ۸ + ۴ + ۲) = ۱۴.$$

پس ۱۴ گردن‌بند متفاوت می‌توان ساخت. □

۳.۱ قضایای سیلو

همانطور که در درس مبانی جبر با قضیه بسیار مهم لاگرانژ و کاربردهای آن برای گروه‌های متناهی آشنا شدید، مشاهده کردید که عکس این قضیه در حالت کلی صحیح نیست. اما این سوال طبیعی است که پرسیده شود عکس این قضیه در چه زمانی می‌تواند صحیح باشد. همین سوال به وجود آوردنده قضایای این بخش است که اولین بار توسط سیلو ریاضیدان نروژی مورد توجه قرار گرفت. و توسط ریاضیدانی به نام فروبنیوس تکمیل شد. البته اثبات‌های که ارائه خواهند شد مسلما با کارها و اثبات‌های قدیمی فرق دارد و به روز شده است. در ادامه با سه قضیه مهم که مشهور به قضایای سیلو هستند سر و کار داریم.

تعریف ۱.۳.۱. *فرض کنیم G گروهی متناهی باشد و p عددی اول که $p^m \mid |G|$ ولی $p^{m+1} \nmid |G|$ که در آن $m \in \mathbb{N}$. در این صورت هر زیرگروه G از مرتبه p^m را یک pـ زیرگروه سیلوی G نامند.*

مثال ۲.۳.۱. *گروه $G = \mathbb{Z}_4 \times \mathbb{Z}_5$ از مرتبه ۲۰ را در نظر بگیرید. واضح است که $2^2 \mid 20$ ولی $2^3 \nmid 20$. از طرفی مرتبه زیرگروه $H = \mathbb{Z}_4 \times \{\bar{0}\}$ برابر ۴ است پس H یک ۲ـ زیرگروه سیلو است.*

برای ادامه به لم زیر نیاز داریم که به قضیه کشی برای گروه‌های متناهی معروف است. این لم برای گروه‌های آبلی متناهی اثبات می‌شود. در بخش کاربردهای قضایای سیلو صورت کلی این لم برای گروه دلخواه متناهی را خواهید دید.

لم ۳.۳.۱. *(قضیه کشی برای گروه‌های آبلی متناهی) فرض کنیم G گروهی آبلی و متناهی باشد و p یک عدد اول. اگر p مرتبه G را بشمارد آنگاه G عنصری از مرتبه p دارد. در نتیجه زیرگروهی از مرتبه p دارد.*

اثبات. فرض کنیم $n = |G|$. حکم را با استقرا به دست می‌آوریم. اگر $n = 1$ باشد چیزی برای اثبات نداریم. فرض کنیم حکم برای تمام گروه‌ها از مرتبه m که $m < n$ و $p|m$ برقرار باشد (فرض استقرا). اگر $|G| = p$ چیزی برای اثبات نداریم. حتی اگر G گروهی دوری باشد آنگاه زیرگروهی دوری از مرتبه p دارد (چرا؟) و باز هم در این حالت چیزی برای اثبات وجود ندارد. حال فرض کنیم $g \in G$، $g \neq e$ و $G \neq < g >$. اگر $p \mid | < g > |$ آنگاه $< g >$ زیرگروهی دوری از مرتبه p مانند H دارد (چرا؟) و همین H زیرگروه مرتبه p برای G است و حکم به دست می‌آید. پس فرض کنیم $p \nmid | < g > |$. در نتیجه $p \mid |G/ < g > |$. پس طبق فرض استقرا گروه $G/ < g >$ دارای عنصری مانند $\bar{a}$ است که $o(\bar{a}) = p$. فرض کنیم که $o(a) = t$ باشد. بنابراین $a^t = e$ که در نتیجه $\bar{a}^t = \bar{e}$. بنابراین $p|t$ (چرا؟). پس $t' \in \mathbb{Z}$ چنان وجود دارد که $t = pt'$. حال عنصر $a^{t'} \in G$ دارای مرتبه p است و اثبات کامل است. □

اکنون آمادگی لازم را داریم تا قضیه اول سیلو را بیان و اثبات کنیم.

قضیه ۴.۳.۱. *(قضیه اول سیلو) فرض کنیم G گروهی متناهی و p عددی اول باشد. اگر p^m، $|G|$ را بشمارد، آنگاه G دارای زیرگروهی از مرتبه p^m است.*

اثبات. فرض کنیم که $n = |G|$. حکم را با استقرا روی n اثبات می‌کنیم. اگر $n = ۱$ باشد چیزی برای اثبات نداریم. فرض کنیم حکم برای تمام گروه‌ها از مرتبه k که $k < n$ و $p^m|k$ برقرار باشد (فرض استقرا). فرض کنیم $p \mid |Z(G)|$. طبق لم ۳.۳.۱، $Z(G)$ دارای عنصری مانند a از مرتبه p است. قرار دهید $N =< a >$. N در G نرمال است (چرا؟) و مرتبه G/N برابر است با $\frac{n}{p}$. به وضوح $p^{m-۱} \mid \frac{n}{p}$. حال طبق فرض استقرا گروه G/N دارای زیرگروهی مانند H/N است که مرتبه آن برابر $p^{m-۱}$ است و بلافاصله نتیجه می‌شود که مرتبه H برابر p^m است (چرا؟) و در این حالت اثبات کامل است.
اکنون فرض کنیم $p \nmid |Z(G)|$. طبق تمرین ۲۲.۲.۱، معادله رده‌ای به شکل

$$n = |G| = |Z(G)| + \sum_{a \in W} [G : N(a)]$$

است که که W از هر رده تزویجی با بیش از یک عنصر، دقیقا یک نماینده دارد. اما $p|n$ ولی $p \nmid |Z(G)|$. پس برای دست کم یک $a \notin Z(G)$ داریم که $p \nmid [G : N(a)] = |G|/|N(a)|$ (چرا؟). پس باید $p^m \mid |N(a)|$ و $|N(a)| < |G|$. پس طبق فرض استقرا $N(a)$ زیرگروهی مانند H از مرتبه p^m دارد که H زیرگروه G نیز می‌باشد (چرا؟) و این اثبات را کامل می‌کند. □

نتیجه ۵.۳.۱. *فرض کنیم G یک گروه متناهی باشد. در این صورت G دارای دست کم یک pـ زیرگروه سیلو است.*

اثبات. اگر $|G| = ۱$ آنگاه $G = \{e\}$ یک pـزیرگروه سیلو است (چرا؟) و کار تمام است. اگر p مرتبه G را نشمارد آنگاه $\{e\}$ یک pـزیرگروه سیلو است (چرا؟) و باز کار تمام است. پس فرض کنیم مرتبه گروه G مخالف یک و به صورت $p^m r$ باشد که p عدد اول، r عدد طبیعی، $m > ۰$، p و r نسبت به هم اولند. با توجه به فرض $p^m \mid |G|$ و $p^{m+۱} \nmid |G|$. اکنون طبق قضیه اول سیلو، قضیه ۴.۳.۱، G یک زیرگروه از مرتبه p^m دارد که طبق تعریف pـزیرگروه سیلو نیز می‌باشد. □

قضیه اول سیلو بدون قضایای دیگر سیلو آن کارایی و کاربرد لازم را ندارد. این قضیه صرفا وجود یک زیرگروه از مرتبه خاص را معلوم می‌کند. همچنین این قضیه، قضیه کشی را که برای عناصر از مرتبه خاص گفته شده، برای زیرگروه بازسازی می‌کند. برای دیدن مثال‌های کاربردی از قضیه اول سیلو باید کمی صبر کنید.
برای بیان قضیه دوم سیلو نیاز به مقدمات زیر است.

تعریف ۶.۳.۱. *فرض کنیم G یک گروه و H زیرگروه‌ای از G باشد. اگر $x \in G$ در این صورت به*

$$x^{-۱}Hx = \{x^{-۱}hx \mid h \in H\}$$

مزدوج H گویند.

تعریف ۷.۳.۱. *فرض کنیم H و K زیرگروه‌های گروه G باشند. گوییم H مزدوج K است اگر $x \in G$ چنان موجود باشد که $H = xKx^{-۱}$.*

لم ۱.۳.۸. *فرض کنیم که G گروه از مرتبه p^n که p عددی اول است باشد. اگر S یک Gـ مجموعه متناهی باشد آنگاه $|S| \overset{p}{\equiv} |S_0|$ که در آن*

$$S_0 = \{s \in S \mid g * s = s,\ g \in G \text{ برای هر}\}.$$

اثبات. ابتدا دقت شود که $s \in S_0$ اگر و تنها اگر برای هر $g \in G$ داشته باشیم $g * s = s$ اگر و تنها اگر $\{s\} = \bar{s}$. از طرفی بنا بر نتیجه ۱۴.۲.۱ ، داریم که

$$|S| = \sum_{s \in S'} [G : G_s]$$

که در آن S' زیرمجموعه‌ای از S شامل دقیقا یک عنصر از هر مدار است. پس

$$|S| = |S_0| + \sum_{s \in S' \setminus S_0} [G : G_s] = |S_0| + \sum_{s \in S' \setminus S_0} |G|/|G_s|.$$

چون $p \mid |G|/|G_s|$ پس در پیمانه p داریم

$$|S| \overset{p}{\equiv} |S_0|$$

و اثبات تمام است. □

لم ۱.۳.۹. *فرض کنیم G یک گروه و H یک زیرگروه G و $a \in G$. در این صورت $|a^{-1}Ha| = |H|$.*

اثبات. رابطه زیر یک تابع یک به یک و پوشا است

$$\begin{cases} \theta : H \longrightarrow a^{-1}Ha \\ \theta(h) = a^{-1}ha \end{cases}$$

و اثبات کامل است. □

اکنون وقت بیان و اثبات قضیه دوم سیلو است.

قضیه ۱.۳.۱۰. *(قضیه دوم سیلو) فرض کنیم G گروهی متناهی و p عددی اول باشد. در این صورت تمام pـ زیرگروهای سیلوی G مزدوج هستند.*

اثبات. فرض کنیم H و K دو pـزیرگروه سیلوی دلخواه از G باشند. حال مجموعه S را همه هم‌دسته‌های چپ H در G در نظر می‌گیریم. طبق تعریف واضح است که $|S| = [G : H]$. اکنون می‌خواهیم S را به یک Kـمجموعه تبدیل کنیم. پس برای هر $k \in K$ و هر $aH \in S$ رابطه زیر را در نظر بگیرید

$$k * (aH) = (ka)H.$$

بررسی این مطلب سر راست است که رابطه بالا یک عمل است در نتیجه S را به یک Kـمجموعه تبدیل کرده‌ایم. حال داریم

$$S_\circ = \{aH \in S \mid k * (aH) = aH,\ k \in K \text{ برای هر}\}.$$

پس طبق لم ۸.۳.۱،

$$|S| \overset{p}{\equiv} |S_\circ|.$$

اگر $|S_\circ| = \circ$ باشد پس $p \mid |S|$ و این یعنی $p \mid [G : H] = \frac{|G|}{|H|}$. این در تناقض با pـزیرگروه سیلو بودن H است. بنابراین $|S_\circ| \neq \circ$. پس می‌توانیم عنصر aH را در $S_\circ$ در نظر بگیریم. پس برای هر $k \in K$ داریم که $k * (aH) = aH$. درنتیجه برای هر $k \in K$ داریم

$$(ka)H = aH \ \Rightarrow\ a^{-1}kaH = H.$$

و این یعنی این که برای هر $k \in K$ رابطه $a^{-1}ka \in H$ برقرار است. پس $a^{-1}Ka \subseteq H$. در نتیجه طبق لم ۹.۳.۱ داریم

$$|a^{-1}Ka| = |K| \leq |H|.$$

به همین صورت با تعویض H و K و لم ۹.۳.۱ می‌توانیم نشان دهیم که $|H| \leq |K|$. حال چون G متناهی پس H و K نیز متناهی هستند و چون روابط $|H| \leq |K|$ و $a^{-1}Ka \subseteq H$ برقرار است باید داشته باشیم $a^{-1}Ka = H$.این یعنی H و K مزدوج هستند. □

نتیجه ۱۱.۳.۱. *فرض کنیم G گروهی متناهی و H یک pـزیرگروه سیلو باشد. در این صورت G تنها یک pـزیرگروه سیلو H را دارد اگر و تنها اگر H زیرگروه نرمال باشد.*

اثبات. ($\Leftarrow$). فرض کنیم $x \in G$ دلخواه باشد. در این صورت $x^{-1}Hx$ زیرگروه G است (چرا؟). طبق لم ۹.۳.۱، $x^{-1}Hx$ یک pـزیرگروه سیلو است (چرا؟). حال از فرض باید داشته باشیم $x^{-1}Hx = H$ و این یعنی H نرمال است.
($\Rightarrow$). فرض کنیم K یک pـزیرگروه سیلو از G باشد. طبق قضیه دوم سیلو، قضیه ۱۰.۳.۱، عنصر $x \in G$ چنان وجود دراد که $x^{-1}Hx = K$. اما H نرمال است پس $H = K$ و اثبات کامل است. □

نتیجه ۱۲.۳.۱. *فرض کنیم G گروهی متناهی، K و H دو pـزیرگروه سیلو باشند. در این صورت H و K هم مرتبه هستند.*

اثبات. طبق قضیه دوم سیلو، قضیه ۱.۳.۱۰، عنصر $x \in G$ چنان وجود دراد که $x^{-1}Hx = K$.
اکنون از لم ۱.۳.۹، حکم به دست می‌آید. □

برای بیان قضیه سوم سیلو به لم زیر نیاز داریم.

لم ۱.۳.۱۳. *فرض کنیم که G گروه متناهی باشد و H یک pـ زیرگروه سیلو G باشد. اگر $H \leq K \leq G$ آنگاه H یک pـ زیرگروه سیلو K است.*

اثبات. برای اثبات فقط کافی است رابطه $|G| \mid |K| \mid |H|$ را در نظر بگیریم. □

یادآوری ۱.۳.۱۴. *فرض کنیم G یک گروه و W یک زیرمجموعه ناتهی از G باشد. نرمال‌ساز W در G عبارت است از مجموعه*

$$N_G(W) = N(W) = \{g \in G \mid gWg^{-1} = W\}.$$

$N(W)$ یک زیرگروه G است.

حال قضیه سوم سیلو را بیان و اثبات می‌کنیم. این قضیه تعداد pـ زیرگروه‌های سیلوی یک گروه متناهی را به دست می‌دهد.

قضیه ۱.۳.۱۵. *(قضیه سوم سیلو) فرض کنیم G گروه متناهی و n_p تعداد pـ زیرگروه‌های سیلو G باشد. در این صورت $n_p \mid |G|$ و عدد صحیح نامنفی k چنان وجود دارد که در آن $n_p = kp + 1$.*

اثبات. فرض کنیم S مجموعه همه pـ زیرگروه‌های سیلو G باشد. بنا به نتیجه ۱.۳.۵، S ناتهی است. عنصر H را در S دلخواه و از این لحظه ثابت در نظر بگیرید. می‌خواهیم S را به یک Hـ مجموعه تبدیل نماییم. برای این منظور به ازای هر $h \in H$ و هر $P \in S$ رابطه

$$h * P = hPh^{-1}$$

را تعریف می‌کنیم. با بررسی سر راست رابطه بالا یک عمل است. حال داریم

$$S_0 = \{P \in S \mid h*P = P,\ h \in H \text{ برای هر}\} = \{P \in S \mid hPh^{-1} = P,\ h \in H \text{ برای هر}\}.$$

پس طبق لم ۱.۳.۸،

$$|S| \overset{p}{\equiv} |S_0|.$$

واضح است که $H \in S_0$ پس $S_0 \neq \emptyset$ است. می‌خواهیم نشان دهیم که $|S_0| = 1$. فرض کنیم $Q \in S_0$. بنابراین برای هر $h \in H$ داریم که $hQh^{-1} = Q$. این نشان می‌دهد که $H \subseteq N(Q)$. طبق لم ۱.۳.۱۳، H یک pـ زیرگروه سیلو $N(Q)$ است. از طرفی $Q \subseteq N(Q)$ (چرا؟) و با استفاده دوباره از لم ۱.۳.۱۳، Q نیز pـ زیرگروه سیلو از $N(Q)$ است. حال طبق قضیه

دوم سیلو، قضیه ۱۰.۳.۱، H و Q در $N(Q)$ مزدوج هستند. پس $x \in N(Q)$ چنان وجود دارد که $Q = xQx^{-1} = H$. در نتیجه $S_0 = \{H\}$ و $|S_0| = 1$. بنابراین

$$|S| \overset{p}{\equiv} 1.$$

پس عدد صحیح نامنفی (چرا؟) مانند k وجود دارد که $|S| = n_p = pk + 1$.
حال نشان می‌دهیم که $n_p \mid |G|$. می‌خواهیم S را به یک Gـ مجموعه تبدیل نماییم. برای این منظور به ازای هر $g \in G$ و هر $P \in S$ رابطه

$$g * P = gPg^{-1}$$

را تعریف می‌کنیم. با بررسی سر راست رابطه بالا یک عمل است. حال برای عضو دلخواه $Q \in S$ مدار Q را محاسبه می‌کنیم. داریم که

$$\bar{Q} = \{g * Q \mid g \in G\} = \{gQg^{-1} \mid g \in G\} = N(Q).$$

اما طبق قضیه دوم سیلو، قضیه ۱۰.۳.۱، همه pـ زیرگروه‌های سیلو مزدوج هستند. بنابراین فقط یک مدار از S وجود دارد. حال طبق نتیجه ۱۴.۲.۱،

$$n_p = |S| = [G : G_y] = |G|/|G_y|$$

که y از تنها مدار موجود انتخاب شده است. پس $n_p \mid |G|$ و اثبات تمام است. □

تمرین حل شده

تمرین ۱۶.۳.۱. *فرض کنیم گروه G از مرتبه p^n باشد و از هر مرتبه p^i که $1 \leq i < n$ دقیقا یک زیرگروه داشته باشد. نشان دهید G دوری است.*

اثبات. فرض کنیم که H تنها زیرگروه مرتبه p^{n-1} از G باشد. طبق قضیه اول سیلو، قضیه ۴.۳.۱، H دارای زیرگروه‌های مرتبه p، ...، p^{n-2} است که اتفاقا همین زیرگروه‌ها برای G نیز می‌باشند (چرا؟) پس همه زیرگروه‌های G در H قرار می‌گیرند. حال فرض کنیم $x \in G \setminus H$. باید مرتبه زیرگروه $< x >$ برابر p^n باشد چون در غیر این صورت $< x >$ دارای مرتبه p^j که $1 \leq j < n$ است پس $< x > \subseteq H$ است و این تناقض است. پس مرتبه x برابر p^n است و این یعنی G دوری است. □

تمرین ۱۷.۳.۱. *فرض کنیم G گروهی از مرتبه $2p$ باشد که p عددی اول است. نشان دهید G زیرگروه نرمالی از مرتبه p دارد.*

اثبات. اگر $p = 2$ باشد آنگاه G گروهی از مرتبه ۴ است که تحت یکریختی دو حالت برای G امکان دارد یکی گروه چهارتایی کلاین و دیگری $\mathbb{Z}_4$ (چرا؟). در هر دو حالت چیزی برای اثبات نداریم (بررسی کنید). پس فرض کنیم p عدد اول فرد باشد. طبق قضیه اول سیلو، قضیه ۴.۳.۱، G زیرگروه مانند H دارد که مرتبه H برابر p است. اما $[G : H] = 2$ پس H زیرگروه نرمال است (چرا؟). □

تمرین ۱.۳.۱۸. *فرض کنیم G گروهی از مرتبه $p^m r$ باشد که p عددی اول و $(p,r)=۱$. اگر H زیرگروه مرتبه p^m باشد آنگاه نشان دهید که H تنها pـ زیرگروه سیلو از G است که $H \subseteq N(H)$.*

اثبات. چون H زیرگروه است پس $N(H)$ حاوی H است، پس H زیرگروه (نرمال) $N(H)$ نیز می‌باشد و باید $|N(H)|\,||H|$. در نتیجه $N(H)$ دارای مرتبه $p^m t$ است که $t \leq r$ و نسبت به p اول است. فرض کنیم H' یک pـزیرگروه سیلو از $N(H)$ باشد. طبق لم ۱.۳.۱۳، H نیز یک pـزیرگروه سیلو از $N(H)$ است. اکنون بنا به قضیه دوم سیلو، قضیه ۱.۳.۱۰، H و H' در $N(H)$ مزدوج هستند. پس $x \in N(H)$ وجود دارد که $H' = xHx^{-۱}$. اما H در $N(H)$ نرمال است (چرا؟) پس $H' = xHx^{-۱} = H$. □

تمرین ۱.۳.۱۹. *نشان دهید که گروه ۶۳ عضوی مانند G ساده نیست.*

اثبات. نشان می‌دهیم که G تنها یک ۷ـ زیرگروه سیلو دارد. طبق قضیه سوم سیلو، قضیه ۱.۳.۱۵، داریم $n_۷ | ۶۳$ و $n_۷ = ۷k + ۱$ که k عدد نامنفی مناسب است. طبق فرض $n_۷ | ۶۳$ برای $n_۷$ امکان‌های زیر وجود دارد

$$۱,\ ۳,\ ۷,\ ۹,\ ۲۱,\ ۶۳.$$

از بین اعداد بالا فقط ۱ در شرط $n_۷ = ۷k + ۱$ برای $k = ۰$ صدق می‌کند (بررسی کنید) یعنی $n_۷ = ۱$ است. در نتیجه تنها یک ۷ـ زیرگروه سیلو دارد. حال چون $۷ | ۶۳$ پس طبق قضیه اول سیلو، قضیه ۱.۳.۴، یک زیرگروه ۷ عضوی مانند H وجود دارد. از طرفی $۷^۲ \nmid ۶۳$ پس H همان تنها ۷ـ زیرگروه سیلو G است. حال طبق نتیجه ۱.۳.۱۱، G زیرگروه نرمال نابدیهی دارد پس ساده نیست. □

تمرین ۱.۳.۲۰. *فرض کنیم G گروهی از مرتبه ۶۸ باشد که حاوی یک زیرگروه نرمال ۴ عضوی است. نشان دهید G آبلی است.*

اثبات. فرض کنیم H همان زیرگروه ۴ عضوی باشد. پس H آبلی است (چرا؟). اما $۱۷ | ۶۸$ پس فرض کنیم $n_{۱۷}$ تعداد ۱۷ـ زیرگروه‌های سیلو G باشد. طبق قضیه سوم سیلو، قضیه ۱.۳.۱۵، داریم $n_{۱۷} = ۱۷k + ۱$ و $n_{۱۷} | ۶۸$. پس باید $n_{۱۷} = ۱$ باشد (بررسی کنید). در نتیجه تنها یک ۱۷ـ زیرگروه سیلو دارد. حال چون $۱۷ | ۶۸$ پس طبق قضیه اول سیلو، قضیه ۱.۳.۴، یک زیرگروه ۱۷ عضوی مانند K وجود دارد. از طرفی $۱۷^۲ \nmid ۶۸$ پس K همان تنها ۱۷ـ زیرگروه سیلو G است. حال طبق نتیجه ۱.۳.۱۱، K زیرگروه نرمال نابدیهی است. حال واضح است که $H \cap K = \{e\}$ زیرا $|H \cap K| = ۱$. اما

$$|HK| = |H|\,|K|/|H \cap K| = ۶۸.$$

چون $HK \subseteq G$ پس $G = HK$. حال نشان می‌دهیم که $G \cong H \times K$. ابتدا دقت کنید که $H \times K$ با عمل زیر یک گروه است

$$(h,k).(h',k') = (hh', kk').$$

رابطه

$$\begin{cases} f : H \times K \longrightarrow G = HK \\ \quad f((h,k)) = hk \end{cases}$$

یک همریختی پوشا است. برای اثبات همریختی تابع بالا، دقت کنید که برای هر $k \in K$ و هر $h \in H$ داریم $hk = kh$ (زیرا $hkh^{-1}k^{-1} \in H \cap K = \{e\}$). حال فرض کنیم $f((h,k)) = e$. پس $hk = e$ در نتیجه $h = k^{-1}$. پس $h \in H \cap K = \{e\}$. به صورت مشابه $k = e$ است و این یعنی f یک‌به‌یک است و یکریختی بالا اثبات می‌شود. اما H و K گروه‌های آبلی هستند (چرا؟). بنابراین باید G آبلی باشد. □

تمرین ۲۱.۳.۱. *فرض کنیم G گروهی متناهی باشد. اگر H و K دو pـ زیرگروه سیلو متمایز از G باشند آنگاه HK زیرگروه نیست.*

اثبات. چون H و K دو pـزیرگروه سیلو هستند پس طبق قضیه دوم سیلو، قضیه ۱۰.۳.۱ و لم ۹.۳.۱، داریم که $|H| = |K| = p^m$. اما H و K متمایزند در نتیجه $p^l = |H \cap K| \lneq p^m$. بنابراین

$$|HK| = |H||K|/|H \cap K| = p^{۲m-l} \gneq p^m.$$

حال اگر HK بخواهد زیرگروه باشد آنگاه طبق قضیه لاگرانژ باید $p^{۲m-l}||G|$ باشد و این pـ زیرگروه سیلو بودن H و K را نقض می‌کند. □

۴.۱ pـ گروه‌ها

در این بخش به مطالعه گروه‌های خاصی خواهیم پرداخت. در سرتاسر این بخش p نشان‌دهنده یک عدد اول است مگر خلافش را ذکر کنیم. مطالعه این بخش از این نظر اهمیت دارد که برای تعیین ساختار یک گروه متناهی با pـ زیرگروه سیلو سر و کار داریم. پس طبیعی است که کمی از pـ گروه‌ها اطلاعات فراهم کنیم.

تعریف ۱.۴.۱. *فرض کنیم p عددی اول باشد. گروه G را یک pـ گروه نامند هرگاه مرتبه هر عنصر G توانی از p باشد.*

مثال ۲.۴.۱. *گروه $\mathbb{Z}_p$ که p عددی اول است یک pـ گروه است.*

مثال ۳.۴.۱. *گروه چهار کلاین یک ۲ـ گروه است.*

تعریف ۴.۴.۱. *فرض کنیم p عددی اول باشد. زیرگروه H از گروه G را یک pـ زیرگروه نامند هرگاه مرتبه هر عنصر H توانی از p باشد.*

مثال ۵.۴.۱. *هر pـ زیرگروه سیلوی یک گروه G یک pـ زیرگروه است.*

مثال ۶.۴.۱. *هر زیرگروه تولید شده توسط یک دور به طول p در گروه S_n (که $p < n$) یک pـ زیرگروه است.*

قضیه زیر تکلیف مرتبه یک pـ گروه متناهی را مشخص می‌کند.

قضیه ۷.۴.۱. *گروه متناهی G یک pـ گروه است اگر و تنها اگر مرتبه‌اش توانی از p باشد.*

اثبات. ($\Leftarrow$). فرض کنیم مرتبه G توانی از p نباشد (فرض خلف). پس عدد اولی مانند q چنان وجود دارد که از p متمایز است و مرتبه G را می‌شمارد. حال طبق قضیه کشی، قضیه ۱.۷.۱، در G عنصری وجود دارد که مرتبه آن q است که این pـ گروه بودن را نقض می‌کند.
($\Rightarrow$). چون مرتبه هر عنصر (طبق نتایج قضیه لاگرانژ) مرتبه G را می‌شمارد و مرتبه G به صورت p^t است پس هر عنصر دارای مرتبه‌ای از توان p است یعنی G یک pـ گروه است. □

قضیه ۸.۴.۱. *فرض کنیم G یک pـ گروه با مرتبه بزرگتر از یک باشد. در این صورت $Z(G)$ نابدیهی است.*

اثبات. طبق تمرین ۲۲.۲.۱ داریم

$$|G| = |Z(G)| + \sum_{a \in W} [G : C(a)]$$

که W از هر رده تزویجی با بیش از یک عنصر، دقیقا یک نماینده دارد. حال اگر $G = Z(G)$ چیزی برای اثبات نداریم. پس فرض کنیم $Z(G) \neq G$. برای $x \in G \setminus Z(G)$، $C(x)$ زیرگروهی

سره از G است. طبق قضیه ۷.۴.۱، $|G| = p^k$ برای عدد طبیعی مناسب k. اما $p \mid |C(x)|$ و این ایجاب می‌کند که $p \mid [G : C(x)]$. پس برای هر $a \in W$ داریم که $p \mid [G : C(a)]$ و در نتیجه $p \mid \sum_{a \in W} [G : C(a)]$. چون $p \mid |G|$ پس $p \mid |Z(G)|$. بنابراین باید $|Z(G)| > 1$ باشد و این یعنی $Z(G)$ نابدیهی است. □

نتیجه ۹.۴.۱. *فرض کنیم G گروهی از مرتبه p^2 باشد. آنگاه G آبلی است.*

اثبات. طبق قضیه ۸.۴.۱، $Z(G)$ نابدیهی است و در نتیجه از قضیه لاگرانژ داریم که $|Z(G)| = p$ یا $|Z(G)| = p^2$. فرض کنیم $|Z(G)| = p$. پس $Z(G) \neq G$. برای $x \in G \setminus Z(G)$، $C(x)$ زیرگروهی سره از G است. حال واضح است که $Z(G) \subset C(x)$ (اثبات تمرین ۲۲.۲.۱ را ببینید). بنابراین $|C(x)| = p^2$ و در نتیجه باید $G = C(x)$ باشد و این یعنی $x \in Z(G)$ که تناقض است. بنابراین باید $|Z(G)| = p^2$ رخ دهد و این هم رابطه $G = Z(G)$ را نتیجه می‌دهد. □

گزاره ۱۰.۴.۱. *در هر گروه از مرتبه p^n که p عدد اول است، زیرگروه از مرتبه p^{n-1} نرمال است.*

اثبات. به استقرا حکم را ثابت می‌کنیم. اگر $n = 1$ باشد چیزی برای اثبات نداریم. فرض کنیم حکم برای هر گروه از مرتبه p^m که $m < n$ برقرار باشد (فرض استقرا). به علاوه فرض کنیم H زیرگروه مرتبه p^{n-1} باشد. اگر $H \neq N(H)$ باشد آنگاه باید $|N(H)| > p^{n-1}$ باشد. پس $|N(H)| = p^n$ و در نتیجه $G = N(H)$. بنابراین H نرمال است و کار تمام است. اگر $H = N(H)$ آنگاه $Z(G)$ زیرمجموعه H است (چرا؟). اما طبق قضیه ۸.۴.۱، $Z(G)$ نابدیهی است و یک pـزیرگروه است (چرا؟). حال طبق قضیه اول سیلو، ۴.۳.۱، زیرگروه K از $Z(G)$ وجود دارد که $|K| = p$ و K در G نرمال است (چرا؟). اکنون G/K از مرتبه p^{n-1} و H/K زیرگروهی از مرتبه p^{n-2} در G/K است. طبق فرض استقرا H/K در G/K نرمال است. در نتیجه H در G نرمال است (چرا؟). □

این بخش را با گزاره زیر به پایان می‌بریم.

گزاره ۱۱.۴.۱. *فرض کنیم H یک pـ زیرگروه از گروه متناهی G باشد. در این صورت داریم که $[G : H] \stackrel{p}{\equiv} [N(H) : H]$.*

اثبات. فرض کنیم S مجموعه همه هم‌دسته‌های چپ H در G باشد. پس $|S| = [G : H]$. حال برای هر $h \in H$ و هر $xH \in S$ عمل زیر

$$h * xH = hxH$$

S را یک Hـ مجموعه می‌کند. اما داریم

$$\begin{gathered} xH \in S_{\circ} \Leftrightarrow \\ h * xH = xH,\ h \in H \text{ برای هر } \Leftrightarrow \\ hxH = xH,\ h \in H \text{ برای هر } \Leftrightarrow \\ x^{-1}hxH = H,\ h \in H \text{ برای هر } \Leftrightarrow \\ x^{-1}hx \in H,\ h \in H \text{ برای هر } \Leftrightarrow \\ x^{-1}Hx = H \Leftrightarrow \\ xHx^{-1} = H \Leftrightarrow \\ x \in N(H) \end{gathered}$$

پس $|S_{\circ}|$ یعنی تعداد هم‌دسته‌های چپ به صورت xH که $x \in N(H)$. و این معادل است با $|S_{\circ}| = [N(H) : H]$. حال طبق لم ۸.۳.۱، $[N(H) : H] \overset{p}{\equiv} [G : H]$. □

تمرین حل شده

تمرین ۱۲.۴.۱. *نشان دهید که ۲ـ زیرگروه‌های گروه $(\mathbb{Z}_{۱۲}, +)$ دو تا است.*

اثبات. دقت کنید که زیرگروه‌های بدیهی در این تمرین ۲ـ زیرگروه نیستند. فرض کنیم H یک ۲ـ زیرگروه باشد. طبق قضیه ۷.۴.۱، $|H| = ۲^k$ که k عدد صحیح نامنفی مناسب است. اما $|H| \mid ۱۲$ پس k باید ۰، ۱ و ۲ باشد. اگر $k = ۲$ باشد آنگاه $|H| = ۴$ و تنها زیرگروه ۴ عضوی به صورت $\{\bar{۰}, \bar{۳}, \bar{۶}, \bar{۹}\}$ که ۲ـ زیرگروه است. یکی باقیمانده $\{\bar{۰}, \bar{۶}\}$ است. □

تمرین ۱۳.۴.۱. *هر گروه ناآبلی از مرتبه $p^۳$ دارای مرکز دوری است.*

اثبات. طبق قضیه ۸.۴.۱، $Z(G)$ نابدیهی است. پس $|Z(G)|$ فقط اعداد $p^۳$، $p^۲$ و p می‌تواند باشد. اگر $|Z(G)|$ برابر $p^۳$ باشد آنگاه $G = Z(G)$ و این تناقض است. اگر $|Z(G)|$ برابر $p^۲$ باشد آنگاه $|G/Z(G)| = p$ و در نتیجه $G/Z(G)$ دوری است که این هم نشان می‌دهد G آبلی است (چرا؟). پس $|Z(G)|$ برابر p است و کار تمام است. □

تمرین ۱۴.۴.۱. *فرض کنیم G گروهی است که فقط یک زیرگروه نابدیهی دارد. نشان دهید که G گروهی از مرتبه $p^۲$ که p عدد اول است و در نتیجه G آبلی است.*

اثبات. ابتدا نشان می‌دهیم G متناهی است. فرض کنیم $e \neq x \in G$ و $H = < x >$. اگر H نامتناهی باشد آنگاه H با $\mathbb{Z}$ یکریخت است (چرا؟) و در نتیجه بیشمار زیرگروه دارد که تناقض است. پس H متناهی است. فرض کنیم $|G| = n$. اگر در تجزیه n دو عدد اول متمایز مانند p و q ظاهر شود آنگاه طبق قضیه اول سیلو، قضیه ۴.۳.۱، G دارای دو زیرگروه متمایز از مرتبه‌های p و q است که تناقض است. پس باید مرتبه G به صورت p^m باشد. اگر $m \geq ۳$ آنگاه باز هم طبق قضیه اول سیلو، قضیه ۴.۳.۱، G دارای زیرگروه‌های متمایز از مرتبه‌های p، $p^۲$ است که تناقض است پس $m = ۲$ و در نتیجه $n = p^۲$ و طبق نتیجه ۹.۴.۱، G آبلی است. □

تمرین ۱۵.۴.۱. *فرض کنیم H یک pـ زیرگروه از گروه متناهی G باشد. اگر $p|[G : H]$ آنگاه $N(H) \neq H$.*

اثبات. طبق گزاره ۱۱.۴.۱، داریم

$$\circ \overset{p}{\equiv} [G : H] \overset{p}{\equiv} [N(H) : H].$$

پس باید $p|[N(H) : H]$. یعنی $[N(H) : H] > ۱$ و در نتیجه $N(H) \neq H$. □

۵.۱ گروه‌های حلپذیر

هدف این بخش آشنایی مقدماتی با مفهوم حلپذیری و بیان چند قضیه اولیه از مفهوم حلپذیری است. حلپذیری در نظریه گالوا از اهمیت بالایی برخوردار است.
برای تعریف گروه حلپذیر به مقدمات زیر نیاز داریم.

تعریف ۱.۵.۱. *فرض کنیم G یک گروه باشد. برای هر $x, y \in G$ عنصر $xyx^{-1}y^{-1}$ را یک جابجاگر نماییم. زیرگروه تولید شده توسط تمام جابجاگرها را گروه مشتق می‌نامیم و با G' نشان می‌دهیم.*

لم زیر برخی خواص مهم گروه مشتق را بیان می‌کند که بعدا نیاز داریم.

لم ۲.۵.۱. *برای گروه G موارد زیر برقرار است:*
(۱) $G' \trianglelefteq G$.
(۲) G/G' *آبلی است.*
(۳) *اگر $H \trianglelefteq G$ آنگاه G/H آبلی اگر و تنها اگر $G' \subseteq H$.*

اثبات. (۱) واضح است که اگر $a = xyx^{-1}y^{-1}$ جابجاگر دلخواهی در گروه G باشد آنگاه $a^{-1} = yxy^{-1}x^{-1}$ نیز جابجاگر است. حال برای هر $g \in G$ داریم

$$a^{-1} = (gxg^{-1})(gyg^{-1})(gx^{-1}g^{-1})(gy^{-1}g^{-1}) = (gxg^{-1})(gyg^{-1})(gxg^{-1})^{-1}(gyg^{-1})^{-1} \in G'.$$

از طرفی هر عنصر در گروه مشتق حاصل ضرب تعداد متناهی جابجاگر است (چرا؟) مثلا به صورت

$$b = a_1 a_2 ... a_n$$

که a_iها جابجاگر هستند. اکنون برای هر $g \in G$ داریم

$$gbg^{-1} = (ga_1g^{-1})...(ga_ng^{-1}) \in G'$$

که نشان می‌دهد G' نرمال است.
(۲) برای هر $x, y \in G$ داریم

$$(xG')(yG')(xG')^{-1}(yG')^{-1} = (xyx^{-1}y^{-1})G' = G'$$

و در نتیجه $(xG')(yG') = (yG')(xG')$. این نشان می‌دهد G/G' آبلی است.
(۳) ($\Leftarrow$). برای هر $x, y \in G$ داریم

$$(xyx^{-1}y^{-1})H = (xH)(yH)(xH)^{-1}(yH)^{-1} = (xH)(xH)^{-1}(yH)(yH)^{-1} = H$$

که در نتیجه $xyx^{-1}y^{-1} \in H$. پس همه جابجاگرها در H اند و بنابراین $G' \subseteq H$.
($\Rightarrow$). برای هر $x, y \in G$ داریم

$$(xH)(yH)(xH)^{-1}(yH)^{-1} = (xyx^{-1}y^{-1})H = H$$

که تساوی آخر به دلیل $G' \subseteq H$ است. در نتیجه $(xH)(yH) = (yH)(xH)$. بنابراین G/H آبلی است. □

تعریف ۳.۵.۱. *فرض کنیم n عدد صحیح نامنفی باشد. nامین گروه مشتق برای گروه G به صورت استقرایی زیر تعریف می‌شود*

$$G^{(0)} = G,\ G^{(1)} = G',\ G^{(2)} = (G^{(1)})',\ ..., G^{(n)} = (G^{(n-1)})'.$$

اکنون تعریف گروه حلپذیر را می‌توانیم بیان کنیم.

تعریف ۴.۵.۱. *گروه G را حلپذیر می‌نامیم اگر برای عدد نامنفی صحیحی مانند k داشته باشیم $G^{(k)} = \{e\}$.*

مثال ۵.۵.۱. *اگر G گروهی آبلی باشد آنگاه $G^{(1)} = G' = \{e\}$. پس هر گروه آبلی حلپذیر است. واضح است که اگر $G^{(1)} = G' = \{e\}$ آنگاه G آبلی است.*

تذکر ۶.۵.۱. *با تعریف و ابزارهای که تا کنون فراهم کرده‌ایم ساختن مثال ناآبلی حلپذیر کمی دشوار است و ما را درگیر محاسبات جابجاگرها خواهد کرد. برای ساختن مثالی ناآبلی تا بیان قضیه اصلی صبور باشید.*

گزاره ۷.۵.۱. *فرض کنیم G گروه باشد. اگر G حلپذیر باشد آنگاه هر زیرگروه G و هر تصویر همریخت G حلپذیر است. برعکس، اگر N زیرگروه نرمال باشد، N و G/N حلپذیر باشند آنگاه G حلپذیر است.*

اثبات. فرض کنیم G گروهی حلپذیر باشد. پس برای عدد صحیح نامنفی k داریم $G^{(k)} = \{e\}$.
اگر H زیرگروهی از G باشد آنگاه برای هر عدد صحیح نامنفی n داریم که $H^{(n)} \subseteq G^{(n)}$. پس باید $H^{(k)} = \{e\}$.
فرض کنیم T تصویر همریخت G باشد یعنی همریختی پوشا مانند $f : G \longrightarrow T$ موجود باشد. برای هر $x, y \in G$ داریم

$$f(xyx^{-1}y^{-1}) = f(x)f(y)f(x)^{-1}f(y)^{-1}$$

که این نتیجه می‌دهد $T^{(1)} = T' = f(G') = f(G^{(1)})$. حال برای هر عدد طبیعی n استقرایی می‌توان نشان داد که $T^{(n)} = f(G^{(n)})$. پس در نتیجه $T^{(k)} = f(G^{(k)}) = f(e) = \{e\}$. پس تصویر همریخت هر گروه حلپذیر، حلپذیر است.
اثبات برعکس، فرض کنیم N زیرگروه نرمال باشد، N و G/N حلپذیر باشند. پس برای اعداد

صحیح نامنفی k و l داریم $N^{(k)} = \{e\}$ و $(G/N)^{(l)} = \{\bar{e}\}$. اما تحت همریختی طبیعی $\pi : G \longrightarrow G/N$ دو گروه G و G/N تصویر همریخت هستند. پس برای هر عدد طبیعی n داریم

$$(G/N)^{(n)} = \pi(G^{(n)}) = G^{(n)}N/N.$$

چون $(G/N)^{(l)} = \{\bar{e}\}$ پس $G^{(l)} \subseteq N$. در نتیجه

$$G^{(k+l)} \subseteq N^{(k)} = \{e\}$$

و لذا G حلپذیر است و اثبات کامل است. □

برای بیان قضیه اصلی این بخش مقدمات زیر لازم است.

تعریف ۸.۵.۱. *دنباله $G_۰$، $G_۱$، ...، G_k از زیرگروه‌های گروه G را یک سری نرمال گوییم اگر داشته باشیم*

$$\{e\} = G_۰ \trianglelefteq G_۱ \trianglelefteq ... \trianglelefteq G_{k-۱} \trianglelefteq G_k = G.$$

به گروه خارج قسمتی $G_i/G_{i-۱}$ عامل سری گوییم. به عدد k طول سری نرمال گوییم.

مثال ۹.۵.۱. *در گروه $(\mathbb{Z}_{۱۲}, +)$ دو سری نرمال زیر را داریم*

$$G_۰ = \{\bar{۰}\} \trianglelefteq G_۱ = \{\bar{۰}, \bar{۶}\} \trianglelefteq G_۲ = \mathbb{Z}_{۱۲}$$
$$G_۰ = \{\bar{۰}\} \trianglelefteq G_۱ = \{\bar{۰}, \bar{۶}\} \trianglelefteq G_۲ = \{\bar{۰}, \bar{۳}, \bar{۶}, \bar{۹}\} \trianglelefteq G_۳ = \mathbb{Z}_{۱۲}$$

که در سری نرمال اول طول ۲ و در دومی طول ۳ است.

تعریف ۱۰.۵.۱. *سری نرمال مانند*

$$\{e\} = G_۰ \trianglelefteq G_۱ \trianglelefteq ... \trianglelefteq G_{k-۱} \trianglelefteq G_k = G$$

برای گروه G را سری ترکیبی گوییم هرگاه G_iها متمایز باشند و گروه خارج قسمتی $G_i/G_{i-۱}$ ساده باشند. سری نرمال را به صورت

$$\{e\} = G_۰ \lhd G_۱ \lhd ... \lhd G_{k-۱} \lhd G_k = G$$

نمایش می‌دهیم و به گروه خارج قسمتی $G_i/G_{i-۱}$ عامل سری ترکیبی گوییم. به عدد k طول سری ترکیبی گوییم.

مثال ۱۱.۵.۱. *در گروه $(\mathbb{Z}_{۱۲}, +)$ دو سری نرمال زیر را در نظر بگیرید*

$$G_۰ = \{\bar{۰}\} \trianglelefteq G_۱ = \{\bar{۰}, \bar{۶}\} \trianglelefteq G_۲ = \mathbb{Z}_{۱۲}$$
$$G_۰ = \{\bar{۰}\} \trianglelefteq G_۱ = \{\bar{۰}, \bar{۶}\} \trianglelefteq G_۲ = \{\bar{۰}, \bar{۳}, \bar{۶}, \bar{۹}\} \trianglelefteq G_۳ = \mathbb{Z}_{۱۲}$$

سری نرمال اول یک سری ترکیبی نیست چون $G_۲/G_۱$ ساده نیست (چرا؟) اما سری نرمال دومی ترکیبی است.

مثال ۱۲.۵.۱. *در گروه ساده G سری ترکیبی زیر را داریم*

$$G_۰ = \{e\} \lhd G_۱ = G.$$

اکنون وقت بیان قضیه اصلی این بخش است که یک مشخصه سازی برای گروه‌های حلپذیر ارائه می‌کند.

قضیه ۱۳.۵.۱. *گروه G حلپذیر است اگر و تنها اگر G سری نرمالی با عوامل آبلی داشته باشد.*

اثبات. ($\Leftarrow$). فرض کنیم G گروهی حلپذیر باشد. پس برای عدد صحیح نامنفی k داریم که $G^{(k)} = \{e\}$. برای هر عدد صحیح نامنفی n، طبق لم ۲.۵.۱، قسمت (۱)، داریم $G^{(n)} \trianglelefteq G^{(n-۱)}$. پس در نتیجه سری

$$\{e\} = G^{(k)} \trianglelefteq G^{(k-۱)} \trianglelefteq \ldots \trianglelefteq G^{(۱)} \trianglelefteq G^{(۰)} = G$$

یک سری نرمال است. چون برای صحیح نامنفی n، $G^{(n)} \subseteq G^{(n-۱)}$، پس طبق لم ۲.۵.۱، قسمت (۳)، داریم که $G^{(n)}/G^{(n-۱)}$ آبلی است و اثبات کامل است.
($\Rightarrow$). فرض کنیم سری

$$\{e\} = G_۰ \trianglelefteq G_۱ \trianglelefteq \ldots \trianglelefteq G_r = G$$

یک سری نرمال با عامل‌های آبلی است. چون $G_۱/G_۰$ آبلی است پس طبق لم ۲.۵.۱، قسمت (۳)، داریم $G'_۱ \subseteq G_۰$. حال چون $G_۲/G_۱$ آبلی است پس طبق لم ۲.۵.۱، قسمت (۳)، داریم $G'_۲ \subseteq G_۱$. پس

$$G^{(۲)}_۲ = (G'_۲)' \subseteq G'_۱ \subseteq G_۰.$$

در نتیجه $G^{(۲)}_۲ \subseteq G_۰$. استقرایی ادامه می‌دهیم پس باید $G^{(r)} \subseteq G_۰ = \{e\}$ باشد و این یعنی G حلپذیر است. □

با مثال زیر این بخش را به پایان می‌رسانیم. مثال زیر یک گروه ناآبلی حلپذیر ارائه می‌دهد.

مثال ۱۴.۵.۱. *گروه ناآبلی $S_۳$ حلپذیر است. چرا که $S_۳$ دارای سری نرمال با عامل‌های آبلی زیر است*

$$\{e\} \trianglelefteq A_۳ = \{e, (۱۲۳), (۳۲۱)\} \trianglelefteq S_۳.$$

دقت شود که $S_۳/A_۳$ گروهی دو عضوی و در نتیجه آبلی است. حال طبق قضیه ۱۳.۵.۱، $S_۳$ حلپذیر است.

تمرین حل شده

تمرین ۱۵.۵.۱. *اگر G گروهی ناآبلی و ساده باشد آنگاه $G^{(۱)} = G' = G$. در نتیجه چنین گروهی حلپذیر نیست.*

اثبات. چون G آبلی نیست پس $G^{(۱)} = G' \neq \{e\}$ و طبق لم ۲.۵.۱، قسمت (۱)، $G' \trianglelefteq G$ است و چون G ساده است پس $G^{(۱)} = G' = G$. قسمت دوم اکنون واضح است. □

تمرین ۱۶.۵.۱. *نشان دهید که برای گروه $S_۳$ یک سری ترکیبی وجود دارد.*

اثبات. سری زیر ترکیبی است

$$G_۰ = \{e\} \lhd G_۱ = A_۳ \lhd G_۳ = S_۳.$$

دقت کنیم که $G_۱/G_۰ \cong \mathbb{Z}_۳$ و $G_۲/G_۱ \cong \mathbb{Z}_۲$. □

تمرین ۱۷.۵.۱. *نشان دهید که برای گروه $(\mathbb{Z}_{۱۸}, +)$ یک سری ترکیبی وجود دارد.*

اثبات. سری زیر ترکیبی است

$$G_۰ = \{\bar{۰}\} \lhd G_۱ = \{\bar{۰}, \bar{۹}\} \lhd G_۲ = \{\bar{۰}, \bar{۳}, \bar{۶}, \bar{۹}, \bar{۱۲}, \bar{۱۵}\} \lhd G_۳ = \mathbb{Z}_{۱۸}.$$

دقت کنیم که $G_۳/G_۲$، $G_۲/G_۱$ و $G_۱/G_۰$ به ترتیب از مرتبه‌های ۳، ۳ و ۲ هستند در نتیجه آبلی می‌باشند. □

تمرین ۱۸.۵.۱. *اگر H زیرگروه نابدیهی از گروه حلپذیر G باشد آنگاه $H \neq H'$.*

اثبات. به برهان خلف، فرض کنیم که $H = H'$ است. پس برای هر عدد طبیعی n داریم که $H^{(n)} = H$. اما طبق گزاره ۷.۵.۱، H حلپذیر است پس عدد صحیح مثبت k چنان وجود دارد که $H^{(k)} = \{e\}$. در نتیجه H گروه بدیهی است که تناقض با فرض مسله دارد. □

تمرین ۱۹.۵.۱. *نشان دهید که هر گروه G از مرتبه pq که p و q عدد اولند، حلپذیر است.*

اثبات. فرض کنیم که $p = q$ پس $|G| = p^۲$. حال طبق قضیه اول سیلو، قضیه ۴.۳.۱، G دارای زیرگروهی از مرتبه p مانند H که آبلی است. از طرفی H به وضوح یک pـزیرگروه سیلو است. اما طبق قضیه سوم سیلو، ۱۵.۳.۱، داریم $n_p | p^۲$ و $n_p = pk + ۱$ که k عدد صحیح نامنفی است. در نتیجه $n_p = ۱$ است و طبق نتیجه ۱۱.۳.۱، H نرمال است. پس سری نرمال زیر را داریم

$$\{e\} \trianglelefteq H \trianglelefteq G.$$

چون G/H داری مرتبه p است پس آبلی است. حال طبق قضیه ۱۳.۵.۱، G حلپذیر است. اکنون فرض کنیم $p \neq q$ و بدون کم شدن از کلیت فرض کنیم که $p > q$. طبق قضیه اول سیلو، قضیه ۴.۳.۱، G دارای زیرگروهی آبلی از مرتبه p مانند H است. از طرفی H به وضوح یک pـزیرگروه سیلو است. اما طبق قضیه سوم سیلو، ۱۵.۳.۱، داریم $n_p | pq$ و $n_p = pk + ۱$ که k عدد صحیح نامنفی است. پس $n_p | q$. چون $p > q$ نتیجه می‌شود که $n_p = ۱$ و طبق نتیجه ۱۱.۳.۱، H نرمال است. پس سری نرمال زیر را داریم

$$\{e\} \trianglelefteq H \trianglelefteq G.$$

چون G/H داری مرتبه q است پس آبلی است. حال طبق قضیه ۱۳.۵.۱، G حلپذیر است. □

تمرین ۲۰.۵.۱. *اگر H و K زیرگروه‌های نرمال و حلپذیر از گروه G باشند. آنگاه نشان دهید که HK حلپذیر است.*

اثبات. واضح است که K زیرگروه نرمال از HK است. حال طبق قضیه دوم یکریختی داریم

$$HK/K \cong H/(H \cap K).$$

از طرفی $H/(H \cap K)$ تصویر همریخت گروه حلپذیر H است. بنابراین طبق گزاره ۷.۵.۱، گروه HK/K حلپذیر است. از طرفی چون K حلپذیر است با استفاده مجدد از گزاره ۷.۵.۱، گروه HK حلپذیر می‌شود. □

تمرین ۲۱.۵.۱. *نشان دهید گروه‌های H و K حلپذیرند اگر و تنها اگر گروه $H \times K$ حلپذیر باشد (مسئله با استقرا قابل تعمیم به تعداد متناهی بیشتر از دو تا نیز می‌باشد).*

اثبات. ($\Leftarrow$). واضح است که $H \cong H \times \{e_K\}$. از طرفی $H \times \{e_K\}$ زیرگروه نرمال از $H \times K$ است (چرا؟) پس داریم

$$K \cong (H \times K)/(H \times \{e_K\}).$$

پس $H \times \{e_K\}$ و $(H \times K)/(H \times \{e_K\})$ هر دو حلپذیرند. بنابراین طبق گزاره ۷.۵.۱، گروه $H \times K$ حلپذیر است.
($\Rightarrow$). با استفاده از گزاره ۷.۵.۱ و مطلب زیر

$$K \cong (H \times K)/(H \times \{e_K\}) \qquad H \cong (H \times K)/(\{e_H\} \times K)$$

حکم به دست می‌آید. □

۶.۱ گروه‌های پوچتوان

برای مشخصه سازی گروه‌ها یک مفهوم دیگر نیز در نظریه گروه به نام گروه پوچتوان معرفی شده است. البته گروه پوچتوان در نظریه گالوا و مشخصه سازی گروه لی نیز کاربرد دارد.
با تعریف زیر شروع می‌کنیم که کمی طولانی است.

تعریف ۱.۶.۱. *فرض کنیم G یک گروه باشد. قرار می‌دهیم*

$$Z_0(G) = \{e\}, \quad Z_1(G) = Z(G).$$

حال مرکز گروه خارج قسمتی $G/Z(G)$ یعنی $Z(G/Z(G))$ را در نظر می‌گیریم. چون $Z(G/Z(G))$ زیرگروه نرمالی از $G/Z(G)$ است طبق قضیه تناظر زیرگروه نرمال یکتای مانند $Z_2(G)$ از G وجود دارد که

$$Z(G/Z_1(G)) := Z_2(G)/Z_1(G).$$

روند را استقرایی ادامه می‌دهیم. برای هر عدد طبیعی $n > 1$، زیرگروه نرمالی از G مانند $Z_n(G)$ به دست می‌آوریم به طوری که

$$Z(G/Z_{n-1}(G)) = Z_n(G)/Z_{n-1}(G).$$

$Z_n(G)$ را nامین مرکز گروه G گویند.

تعریف ۲.۶.۱. *فرض کنیم G گروه باشد. گوییم G پوچتوان است هرگاه عددی مانند m چنان باشد که $Z_m(G) = G$. کوچکترین عدد m که $Z_m(G) = G$، رده پوچتوانی نامییم.*

مثال ۳.۶.۱. *چون در هر گروه آبلی $Z_1(G) = Z(G) = G$ است. پس هر گروه آبلی پوچتوان با رده پوچتوانی ۱ است.*

برای ساختن یک مثال ناآبلی قضیه زیر لازم است و باید کمی صبور باشیم. ابتدا لم زیر را داریم که عناصر nامین مرکز G را معلوم می‌کند.

لم ۴.۶.۱. *برای گروه G داریم*

$$Z_n(G) = \{x \in G \mid xyx^{-1}y^{-1} \in Z_{n-1}(G), \ y \in G \text{ برای هر}\}.$$

اثبات. برای هر $y \in G$ داریم

$$\begin{gathered} x \in Z_n(G) \Leftrightarrow \\ xZ_{n-1}(G) \in Z(G/Z_{n-1}(G)) \Leftrightarrow \\ (xZ_{n-1}(G))(yZ_{n-1}(G)) = (yZ_{n-1}(G))(xZ_{n-1}(G)) \Leftrightarrow \\ xyZ_{n-1}(G) = yxZ_{n-1}(G) \Leftrightarrow \\ x^{-1}y^{-1}xyZ_{n-1}(G) = Z_{n-1}(G) \Leftrightarrow \\ x^{-1}y^{-1}xy \in Z_{n-1}(G). \end{gathered}$$

اثبات کامل است. □

قضیه ۵.۶.۱. *گروه G پوچتوان است اگر و تنها اگر G دارای سری نرمال مانند*

$$G_0 = \{e\} \lhd G_1 \lhd ... \lhd G_m = G$$

موجود باشد به طوری که برای هر i داشته باشیم $G_i/G_{i-1} \lhd Z(G/G_{i-1})$.

اثبات. ($\Leftarrow$). فرض کنیم G دارای رده پوچتوانی m باشد. پس $Z_m(G) = G$. حال

$$G_0 = Z_0(G) = \{e\} \lhd G_1 = Z_1(G) \lhd ... \lhd G_m = Z_m(G) = G$$

یک سری نرمال است. چون برای هر i داریم

$$G_i/G_{i-1} = Z_i(G)/Z_{i-1}(G) = Z(G/Z_{i-1}(G))$$

در نتیجه سری نرمال بالا در شرط خواسته شده صدق می‌کند و کار تمام است.
($\Rightarrow$). فرض کنیم G دارای سری نرمالی مانند

$$G_0 = \{e\} \lhd G_1 \lhd ... \lhd G_m = G$$

باشد که برای هر i داشته باشیم $G_i/G_{i-1} \lhd Z(G/G_{i-1})$. بنابراین با فرض $i = 1$ رابطه $G_1 \subseteq Z_1(G) = Z(G)$ نتیجه می‌شود. برای $i = 2$ رابطه $G_2/G_1 \subseteq Z(G/G_1)$ نتیجه می‌شود. حال مشابه با اثبات لم ۴.۶.۱، برای هر $x \in G_2$ و هر $y \in G$ داریم

$$xyx^{-1}y^{-1} \in G_1 \subseteq Z_1(G).$$

طبق لم ۴.۶.۱، باید $x \in Z_2(G)$. یعنی $G_2 \subseteq Z_2(G)$. این روند را استقرایی ادامه می‌دهیم. بنابراین $G = G_m \subseteq Z_m(G)$ و این یعنی G پوچتوان است. □

حال مثال زیر که گروه ناآبلی است را بیان می‌کنیم که یک گروه پوچتوان به دست می‌دهد.

مثال ۶.۶.۱. *گروه کوترنیون: ماتریس‌های زیر را در میدان اعداد مختلط در نظر بگیرید*

$$e = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \ a = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \ b = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

آنگاه واضح است که $a^4 = e$، $a^2 = b^2$ و $a^3 = b^{-1}ab$. این ماتریس‌ها a و b یک گروه ۸ عضوی ناآبلی می‌سازند که به گروه کوترنیون معروف است و با Q_8 نشان می‌دهیم. حال سری نرمال زیر را داریم

$$G_0 = \{e\} \lhd G_1 = \{e, -e\} \lhd G_3 = Q_8.$$

چون G_1/G_0 و G_2/G_1 به ترتیب ۲ و ۴ عضوی هستند پس آبلی هستند در نتیجه داریم که $G_i/G_{i-1} \subseteq Z(Q_8/G_{i-1})$ و طبق قضیه ۵.۶.۱، Q_8 پوچتوان است.

نتیجه ۱.۶.۷. *هر گروه پوچتوان G حلپذیر است.*

اثبات. طبق قضیه ۱.۶.۵، G دارای سری نرمال مانند

$$G_0 = \{e\} \lhd G_1 \lhd ... \lhd G_m = G$$

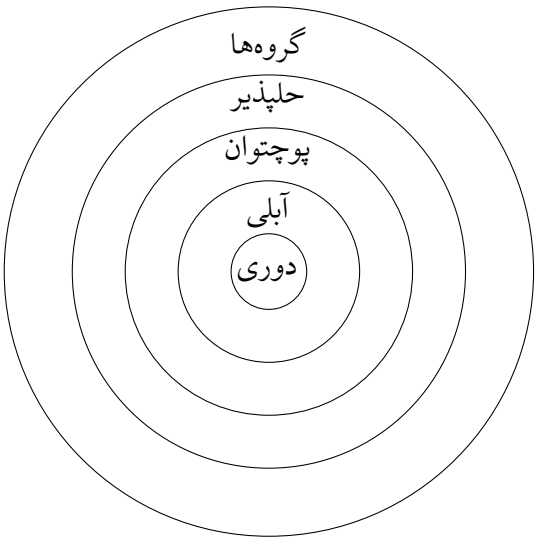
با عامل‌های آبلی است یعنی $G_i/G_{i-1} \subseteq Z(G/G_{i-1})$. حال طبق قضیه ۱.۵.۱۳، G حلپذیر است. □

تذکر ۱.۶.۸. *شاید این سوال به صورت طبیعی به ذهن برسد که آیا گروه حلپذیر نیز پوچتوان است؟ جواب این سوال منفی است. زیر طبق مثال ۱.۵.۱۴، گروه S_3 حلپذیر است. حال نشان می‌دهیم که S_3 پوچتوان نیست. داریم که $Z_0(S_3) = \{e\}$ و $Z_1(S_3) = Z(S_3) = \{e\}$. اما*

$$Z_2(S_3) \cong Z_2(S_3)/\{e\} = Z_2(S_3)/Z_1(S_3) = Z(S_3/Z_1(S_3)) = Z(S_3/\{e\}) \cong Z(S_3) = \{e\}.$$

با ادامه این روند به صورت استقرایی در می‌یابیم که برای هر عدد طبیعی m، $Z_m(S_3) = \{e\}$. بنابراین S_3 پوچتوان نیست.

نمودار زیر شهود خوبی برای شما تا اینجای نظریه گروه (که آموخته‌اید) ایجاد می‌کند.



این بخش را با گزاره زیر پایان می‌دهیم.

گزاره ۱.۶.۹. *فرض کنیم G گروهی پوچتوان باشد. در این صورت هر زیرگروه G و هر تصویر همریخت G پوچتوان هستند.*

اثبات. فرض کنیم G گروهی پوچتوان از رده m باشد یعنی $Z_m(G) = G$. اگر H زیرگروهی از G باشد آنگاه واضح است که $H \cap Z(G) \subseteq Z(H)$. برای هر $x \in Z_2(G)$ و هر $y \in G$ طبق لم ۴.۶.۱، $xyx^{-1}y^{-1} \in Z_1(G)$. پس برای هر $x \in H \cap Z_2(G)$ و هر $y \in H$ داریم $xyx^{-1}y^{-1} \in H \cap Z_1(G)$. در نتیجه $H \cap Z_2(G) \subseteq Z_2(H)$. با تکرار استقرایی این روند برای هر i داریم $H \cap Z_i(G) \subseteq Z_i(H)$. پس

$$H = H \cap G = H \cap Z_m(G) \subseteq Z_m(H).$$

بنابراین H پوچتوان است.
فرض کنیم $f : G \longrightarrow T$ همریختی پوشا باشد. در این صورت برای هر $x, y \in G$

$$f(xyx^{-1}y^{-1}) = f(x)f(y)f(x)^{-1}f(y)^{-1}.$$

پس $f(Z(G)) \subseteq Z(T)$ یا بطور معادل $f(Z_1(G)) \subseteq Z_1(T)$. فرض کنیم که $x \in Z_2(G)$. طبق لم ۴.۶.۱، پس برای هر $y \in G$ داریم $xyx^{-1}y^{-1} \in Z_1(G)$. پس

$$f(x)f(y)f(x)^{-1}f(y)^{-1} \in f(Z_1(G)) \subseteq Z_1(T).$$

چون f پوشا است باید $f(x) \in Z(T)$. بنابراین $f(Z_2(G)) \subseteq Z_2(T)$. با تکرار روند استقرایی می‌بینیم که برای هر i، $f(Z_i(G)) \subseteq Z_i(T)$. پس

$$T = f(G) = f(Z_m(G)) \subseteq Z_m(T).$$

بنابراین T پوچتوان است یعنی هر تصویر همریخت G پوچتوان است. □

تمرین حل شده

تمرین ۱۰.۶.۱. *فرض کیم H و K گروه باشند. نشان دهید که برای هر عدد صحیح نامنفی m داریم $Z_m(H \times K) = Z_m(H) \times Z_m(K)$ (مسئله با استقرا قابل تعمیم به تعداد متناهی بیشتر از دو تا نیز می‌باشد).*

اثبات. برای $m = 0$ چیزی برای اثبات نداریم. فرض کنیم حکم برای اعداد کمتر از m صحیح باشد (فرض استقرا). اگر $(h, k) \in Z_m(H \times K)$ آنگاه برای هر $(x, y) \in H \times K$ طبق لم ۴.۶.۱ و فرض استقرا داریم

$$(h, k)(x, y)(h, k)^{-1}(x, y)^{-1} \in Z_{m-1}(H \times K) = Z_{m-1}(H) \times Z_{m-1}(K).$$

در نتیجه داریم

$$(hxh^{-1}x^{-1}, kyk^{-1}y^{-1}) \in Z_{m-1}(H \times K) = Z_{m-1}(H) \times Z_{m-1}(K).$$

پس برای هر $x \in H$ (به روش مشابه $y \in K$) داریم $hxh^{-1}x^{-1} \in Z_{m-1}(H)$ (به روش مشابه $kyk^{-1}y^{-1} \in Z_{m-1}(K)$). پس $h \in Z_m(H)$ و $k \in Z_m(K)$. در نتیجه $(h,k) \in Z_m(H) \times Z_m(K)$. یعنی

$$Z_m(H \times K) \subseteq Z_m(H) \times Z_m(K).$$

چون مراحل بالا برگشت پذیر است عکس زیرمجموعه هم نتیجه می‌شود و اثبات کامل است. □

تمرین ۱.۶.۱۱. *فرض کنیم H و K گروه باشند. نشان دهید $H \times K$ پوچتوان است اگر و تنها اگر H و K پوچتوان باشند (مسئله با استقرا قابل تعمیم به تعداد متناهی بیشتر از دو تا نیز می‌باشد).*

اثبات. ($\Leftarrow$). چون $H \cong H \times \{e\}$ پس طبق گزاره ۹.۶.۱، H پوچتوان است. به صورت مشابه نیز K پوچتوان است.
($\Rightarrow$). فرض کنیم $Z_m(H) = H$ و $Z_r(K) = K$. عدد t را ماکسیمم m و r قرار می‌دهیم. طبق تمرین ۱۰.۶.۱، داریم

$$Z_t(H \times K) = Z_t(H) \times Z_t(K) = H \times K.$$

پس $H \times K$ پوچتوان است. □

تمرین ۱.۶.۱۲. *نشان دهید گروهی مانند G وجود دارد که زیرگروه نرمالی مانند H دارد که هر دوی H و G/H پوچتوانند اما G پوچتوان نیست.*

اثبات. قرار دهید $G = S_۳$ و $H = <(۱۲۳)>$. H و G/H هر دو آبلی هستند پس پوچتوانند در حالی که طبق تذکر ۸.۶.۱، $S_۳$ پوچتوان نیست. □

تمرین ۱.۶.۱۳. *فرض کنیم گروه $G = H \times K$ ناآبلی، H و K از مرتبه $p^۲$ و $p^۳$ برای عدد اول p باشند. نشان دهید که G پوچتوان است.*

اثبات. طبق تمرین ۱۰.۶.۱، داریم که

$$Z(G) = Z(H) \times Z(K).$$

طبق نتیجه ۹.۴.۱، $Z(H) = H$ است. پس $|Z(G)| = p^۲|Z(K)|$. چون G آبلی نیست پس باید $|Z(K)|$ یکی از اعداد ۱، p و $p^۲$ باشد. اما طبق قضیه ۸.۴.۱، مرتبه $Z(K)$ نمی‌تواند عدد ۱ باشد. اگر $|Z(K)| = p^۲$ آنگاه $K/Z(K)$ دارای مرتبه p و در نتیجه دوری است. پس K آبلی است (چرا؟). این نشان می‌دهد که G آبلی است که تناقض است. بنابراین مرتبه $Z(K)$ برابر p و در نتیجه $|Z(G)| = p^۳$ است. حال سری نرمال

$$G_۰ = \{e\} \lhd G_۱ = Z(G) \lhd G_۲ = G$$

را در نظر بگیرید. چون $G_۲/G_۱$ از مرتبه $p^۲$ است طبق نتیجه ۹.۴.۱، داریم

$$G_۲/G_۱ = G/Z(G) = Z(G/Z(G)) = Z(G_۲/G_۱).$$

همچنین

$$G_۱/G_۰ = Z(G)/\{e\} = Z(G) = Z(G/\{e\}) = Z(G_۱/G_۰).$$

پس طبق قضیه ۵.۶.۱، G پوچتوان است. □

۷.۱ کاربردهایی از قضایای سیلو و pـ گروه‌ها

در این بخش چند کاربرد از قضایای سیلو را خواهیم آورد. قضایای سیلو ابزاری قدرتمند در مطالعه ساختار گروه‌های ناآبلی متناهی فراهم می‌کند. در برخی موارد وجود یا عدم وجود گروه ساده از مرتبه‌ای معلوم را اثبات یا رد می‌کند.

اولین کاربرد قضایای سیلو قضیه کشی برای گروه متناهی دلخواه است و از شر واژه آبلی خلاص می‌شویم.

قضیه ۱.۷.۱. *(قضیه کشی برای گروه‌های متناهی) فرض کنیم G گروهی متناهی و p یک عدد اول باشد. اگر p مرتبه G را بشمارد آنگاه G عنصری از مرتبه p دارد. در نتیجه زیرگروهی از مرتبه p دارد.*

اثبات. در قضیه اول سیلو، قضیه ۴.۳.۱، قرار دهید $m = ۱$. □

گزاره ۲.۷.۱. *فرض کنیم گروه G مرتبه p^n دارد که $n > ۱$. در این صورت G ساده نیست.*

اثبات. طبق قضیه ۸.۴.۱، $Z(G)$ نابدیهی است. اگر $G = Z(G)$ باشد و G ساده باشد باید $n = ۱$ باشد که تناقض است. پس $Z(G) \neq G$. پس $Z(G)$ زیرگروه نابدیهی سره و به وضوح نرمال است و اثبات کامل است. □

گزاره ۳.۷.۱. *فرض کنیم گروه G مرتبه pq دارد. در این صورت G ساده نیست.*

اثبات. اگر $p = q$ آنگاه طبق گزاره ۲.۷.۱، G ساده نیست. پس فرض کنیم $p \neq q$. بدون کم شدن از کلیت مسله p را بزرگتر از q در نظر می‌گیریم. طبق قضیه سوم سیلو، قضیه ۱۵.۳.۱، داریم که $n_p = pk + ۱$ و $n_p | pq$. به وضوح باید $n_p | q$. در نتیجه $pk + ۱ \leq q$ است. اما $p > q$ پس باید $k = ۰$ باشد. بنابراین $n_p = ۱$ یعنی فقط یک pـزیرگروه سیلو در G وجود دارد. چون $p | pq$ و $p^۲ \nmid pq$، طبق قضیه اول سیلو، قضیه ۴.۳.۱، G باید pـزیرگروه سیلو نابدیهی مانند H داشته باشد. پس طبق نتیجه ۱۱.۳.۱، H نرمال است و این اثبات را تمام می‌کند. □

گزاره ۴.۷.۱. *هر گروه G از مرتبه $p^۲q$ که p و q اعداد اول متمایزند، حلپذیر است.*

اثبات. طبق قضیه اول سیلو، قضیه ۴.۳.۱، G دارای زیرگروهی مانند H از مرتبه $p^۲$ است که pـ زیرگروه سیلو نیز می‌باشد. طبق قضیه سوم سیلو، قضیه ۱۵.۳.۱، داریم $n_p | p^۲q$ و $n_p = pk + ۱$. پس $n_p | q$ و در نتیجه باید $k = ۰$ یا بطور معادل $n_p = ۱$ باشد. پس H تنها pـزیرگروه سیلو است. حال طبق نتیجه ۱۱.۳.۱، H باید نرمال باشد. حال سری نرمال

$$G_۰ = \{e\} \lhd G_۱ = H \lhd G_۲ = G$$

را داریم که چون مرتبه $G_۲/G_۱$ عدد اول q است، آبلی است. اما مرتبه $G_۱/G_۰$ برابر $p^۲$ است و طبق نتیجه ۹.۴.۱، آبلی است. یعنی یعنی در سری نرمال بالا عامل‌های سری آبلی هستند. پس طبق قضیه ۱۳.۵.۱، G حلپذیر است. □

گزاره زیر طیف وسیعی از مثال‌های گروه‌های پوچتوان فراهم می‌کند.

گزاره ۵.۷.۱. *هر pـ گروه G پوچتوان است.*

اثبات. طبق قضیه ۷.۴.۱، G گروهی از مرتبه p^n که p اول است، می‌باشد. طبق قضیه ۸.۴.۱، $Z_۱(G) = Z(G)$ نابدیهی است. اما $G/Z_۱(G)$ دارای مرتبه p^t که $t < n$ می‌باشد. دوباره طبق قضیه ۸.۴.۱، $G = Z_۱(G)$ دارای مرکز نابدیهی است پس باید $|Z_۱(G) < |Z_۲(G|$. این روند را ادامه می‌دهیم. چون G متناهی است پس برای یک m (که کوچکتر یا مساوی n) داریم $|Z_m(G)| = p^n$. پس باید $Z_m(G) = G$. □

تمرین حل شده

تمرین ۶.۷.۱. *فرض کنیم G گروهی از مرتبه ۲۱ باشد. نشان دهید G حلپذیر است.*

اثبات. طبق گزاره ۳.۷.۱، G ساده نیست زیر $۲۱ = ۳ \times ۷$. پس G دارای زیرگروه نرمال نابدیهی مانند N است که این زیرگروه نرمال دارای مرتبه ۳ یا ۷ است. حال سری نرمال

$$G_۰ = \{e\} \lhd G_۱ = N \lhd G_۲ = G$$

را داریم که چون مرتبه هر $G_i/G_{i-۱}$ عدد اول است، عامل‌های سری آبلی هستند. پس طبق قضیه ۱۳.۵.۱، G حلپذیر است. □

تمرین ۷.۷.۱. *فرض کنیم G گروهی باشد که $|G/Z(G)| = ۳۳$. نشان دهید که G زیرگروه نرمال متمایز از $Z(G)$ دارد.*

اثبات. چون $۳۳ = ۳ \times ۱۱$ پس طبق گزاره ۳.۷.۱، $G/Z(G)$ گروهی ساده نیست و دارای زیرگروه نرمال نابدیهی مانند $N/Z(G)$ است. حال طبق قضیه تناظر N زیرگروهی نرمال از G است که به وضوح از $Z(G)$ متمایز است. □

تمرین ۸.۷.۱. *فرض کنیم G گروهی از مرتبه ۱۰۰ باشد. نشان دهید که G زیرگروه نرمال از مرتبه ۵۰ دارد.*

اثبات. چون $۱۰۰ = ۲^۲ \times ۵^۲$ است پس طبق قضیه اول سیلو، قضیه ۴.۳.۱، G یک ۵ـ زیرگروه سیلو مانند K دارد. واضح است که مرتبه K برابر ۲۵ است. اما طبق قضیه سوم سیلو، قضیه ۱۵.۳.۱، داریم که $n_۵|۱۰۰$ و $n_۵ = ۵k + ۱$. در نتیجه $n_۵ = ۱$ است و طبق نتیجه ۱۱.۳.۱، H باید نرمال باشد. اما طبق قضیه کشی، قضیه ۱.۷.۱، چون $۲|۱۰۰$ پس زیرگروهی مانند H از

مرتبه ۲ در G وجود دارد. حال HK یک زیرگروه از G است (چرا؟). اما $(۲, ۲۵) = ۱$ است پس $H \cap K = \{e\}$ و در نتیجه

$$|HK| = |H||K|/|H \cap K| = ۲ \times ۲۵ = ۵۰.$$

پس داریم که $[G : HK] = ۲$. بنابراین طبق قضیه‌ای از مبانی جبر HK یک زیرگروه نرمال است. □

۸.۱ تاریخچه

پتر لودویگ میدل سیلو (به نروژی: Peter Ludwig Mejdell Sylow) (زاده:۱۲ دسامبر ۱۸۳۲ ـ درگذشته:۷ سپتامبر ۱۹۱۸) ریاضی دان نروژی بود. او دبیر ریاضی بود و مدتی در دانشگاه کریستیانا نیز نظریه گالوا را تدریس می‌کرد. از جمله تلاش‌های او در این زمینه مطالعه روی ساختار گروه‌های متناهی بود. قضایای سیلو در سال ۱۸۷۲ توسط او مطرح شد. که اطلاعاتی در مورد گروه‌های متناهی بدست می‌دهد. که در واقع بیان دیگری از عکس قضیه لاگرانژ است که در متن درس، بخش سوم از فصل اول، ادعا کردیم با شرایط خاصی برقرار است. جالب است که اولین بار قضیه سیلو توسط او برای گروه‌های جایگشت اثبات شده بود. بعد از او جورج فروبنیوس، قضیه را در حالت کلی برای گروه‌های متناهی اثبات کرد. او برای این کار از قضیه کیلی کمک گرفت. جالب است که بدانید امروزه شبیه قضایای سیلو برای گروه‌های نامتناهی توسط ریاضیدانان نیز بیان شده است. ولی امروزه این قضایا با نام سیلو خوانده می‌شود. او مدتی، همراه با سوفوس لی، به پژوهش در کارهای هموطنش نیلس هنریک آبل در ریاضیات پرداخت.

به دنبال دستاوردهای گالوا، نظریه گروه‌ها جای خود را در بسیاری از زمینه‌های ریاضی باز کرد. مثلاً، ریاضی‌دان آلمانی فلیکس کلاین سعی کرد که تمام هندسه‌های موجود را بر حسب گروه تبدیل‌هایی که تحت آن‌ها ویژگی‌های هندسه ناوردا بودند تدوین کند.

از جمله ریاضیدانانی که در قرن نوزدهم در زمینه نظریه گروه‌ها کار می‌کردند می‌توان برتراند، چارلز هرمیت، فروبنیوس و لئوپارد کرونکر و امیل ماتیو را نام برد. تا آن زمان اصول موضوع معینی برای تعریف گروه وجود نداشت. در سال ۱۸۵۴ کیلی اولین اصول موضوع را برای گروه‌ها ارائه داد اما تعریف وی خیلی زود فاقد ارزش شد. در سال ۱۸۷۰، کرونکر مجدداً اصول موضوعی را برای گروه‌ها پایه گذاشت. همچنین وبر در سال ۱۸۸۲، تعریفی برای گروه‌های متناهی و در سال ۱۸۸۳ تعریفی برای گروه‌های نامتناهی انجام داد. اما این والتر فون دایک بود که در سال ۱۸۸۲ اولین تعریف مدرن از گروه را ارائه داد.

در طی قرن بیستم پژوهش‌های بسیار زیادی برای تحلیل ساختار گروه‌های متناهی صورت گرفت. در دهه‌های اخیر، ریاضیدانان در جست و جوی همه گروه‌های ساده متناهی و توضیح نقش آن‌ها در ساختار تمام گروه‌های متناهی بوده‌اند. از جمله پیشگامان این تحقیقات، والترفیت، جان تامسن، دانیل گورنشتین و هال هستند. امروزه نظریه گروه‌ها به بنیادی‌ترین نظریه‌ها در جبر مجرد تبدیل شده است و منبع تحقیقات فراوانی برای ریاضیدانان است.

۹.۱ تمرین‌ها

تمرین ۱.۹.۱. *نشان دهید یک گروه غیر دوری از مرتبه ۴ حاصل ضرب خارجی دو گروه از مرتبه ۲ است.*

تمرین ۲.۹.۱. *برای گروه‌های G_1، ...، G_n نشان دهید که*

$$Z(G_1 \times ... \times G_n) = Z(G_1) \times ... \times Z(G_n).$$

تمرین ۳.۹.۱. *فرض کنیم G_1، ...، G_n گروه باشند که زیرگروه N_i در G_i نرمال باشد. نشان دهید که*

$$\frac{G_1 \times ... \times G_n}{N_1 \times ... \times N_n} \cong \frac{G_1}{N_1} \times ... \times \frac{G_n}{N_n}.$$

تمرین ۴.۹.۱. *فرض کنیم که G گروهی از مرتبه $n > 1$ باشد. در این صورت نشان دهید که $\mathbb{Z} \times G$ دوری نیست.*

تمرین ۵.۹.۱. *فرض کنیم G یک گروه و $S = \{xHx^{-1} \mid x \in G\}$ که در آن H یک زیرگروه G است. نشان دهید ضابطه زیر یک عمل است و S یک Gـ مجموعه است.*

$$g * (xHx^{-1}) = gxHx^{-1}.$$

تمرین ۶.۹.۱. *فرض کنیم که G گروه و $S(G)$ مجموعه همه زیرگروه‌های G باشد. رابطه مزدوج بودن (تعریف ۱.۳.۷) یک رابطه هم‌ارزی در $S(G)$ است.*

تمرین ۷.۹.۱. *فرض کنیم که G گروه و $S(G)$ مجموعه همه زیرگروه‌های G باشد. با رابطه*

$$H * g = gHg^{-1}$$

$S(G)$ یک Gـ مجموعه است و در نتیجه اگر $H, K \in S(G)$ آنگاه داریم:
(۱) پایدارساز یا نرمال‌ساز H:

$$G_H = \{x \in G \mid H * x = H\} = \{x \in G \mid xHx^{-1} = H\} = N(H).$$

(۲) پایدارساز یا نرمال‌ساز H در K:

$$N_K(H) = \{x \in K \mid H * x = H\} = \{x \in K \mid xHx^{-1} = H\}.$$

(۳) مدار یا مرکزساز H:

$$\bar{H} = \{H * x \mid x \in G\} = \{xHx^{-1} \mid x \in G\} = C(H).$$

(۴) مدار یا مرکزساز H در K:

$$C_K(H) = \{H * x \mid x \in G\} = \{xHx^{-1} \mid x \in G\}.$$

تمرین ۱.۹.۸. *فرض کنیم که G یک گروه باشد که دارای عنصری از مرتبه متناهی $n > ۱$ است و دقیقا دو رده تزویجی دارد. نشان دهید که $|G| = ۲$.*

تمرین ۱.۹.۹. *معادله رده‌ای را برای گروه متقارن $S_۳$ تحقیق کنید.*

تمرین ۱.۹.۱۰. *اگر G گروهی متناهی و N زیرگروه نرمال با $|N| = ۳$ باشد و $N \not\subset Z(G)$ آنگاه نشان دهید زیرگروهی مانند K چنان وجود دارد که $[G : K] = ۲$.*

تمرین ۱.۹.۱۱. (*) *فرض کنیم p مروارید بی رنگ و n اسپری رنگ در اختیار دارید. اگر p اول باشد نشان دهید تمام گردن‌بندهای متفاوتی را که می‌توانیم بسازیم، برابر است با*

$$\frac{۱}{p}(n^p + n(p - ۱)).$$

تمرین ۱.۹.۱۲. *نشان دهید گروهی از مرتبه ۵۶ ساده نیست.*

تمرین ۱.۹.۱۳. *نشان دهید گروهی از مرتبه ۳۶ ساده نیست.*

تمرین ۱.۹.۱۴. *فرض کنیم G گروهی متناهی و عدد اول p مرتبه G را بشمارد. اگر H در G نرمال باشد و $[G : H]$ نسبت به p اول باشد آنگاه نشان دهید که H شامل همه pـ زیرگروه‌های سیلو G است.*

تمرین ۱.۹.۱۵. *فرض کنیم G گروهی از مرتبه ۱۰۸ باشد. نشان دهید G زیرگروه نرمالی از مرتبه ۹ یا ۲۷ دارد.*

تمرین ۱.۹.۱۶. (*) *اگر هر زیرگروه سیلوی گروه متناهی G نرمال باشد آنگاه ثابت کنید که G حاصل ضرب مستقیم زیرگروه‌های سیلویش است.*

تمرین ۱.۹.۱۷. *نشان دهید که اگر H یک pـ زیرگروه سیلو از گروه متناهی G باشد در این صورت $N(N(H)) = N(H)$.*

تمرین ۱.۹.۱۸. (**) *نشان دهید تحت یکریختی فقط دو گروه ناآبلی از مرتبه ۸ وجود دارد.*

تمرین ۱.۹.۱۹. *نشان دهید که یک گروه از مرتبه ۲۰۰ حتما زیرگروه نرمال دارد.*

تمرین ۱.۹.۲۰. *فرض کنیم G گروهی متناهی و H یک pـ زیرگروه سیلو باشد. اگر $N = N(H)$ آنگاه هر زیرگروه G که شامل H باشد با نرمال‌ساز خودش برابر است.*

تمرین ۱.۹.۲۱. *نشان دهید که گروه متناوب $A_۵$ ساده است.*

تمرین ۱.۹.۲۲. *فرض کنیم H یک pـ زیرگروه سیلو G باشد. K را زیرگروهی از G بگیرید به طوری که $|H| = p^m$ و $m > ۰$. ثابت کنید که*

$$K \cap N(H) = K \cap H.$$

تمرین ۲۳.۹.۱. (*) فرض کنیم G یک گروه متناهی و H زیرگروه نرمال G باشد. اگر K یک pـ زیرگروه سیلو H باشد آنگاه $G = HN(K)$.

تمرین ۲۴.۹.۱. فرض کنیم G گروهی متناهی و $G = HK$ که H و K زیرگروه‌های سره از G اند. اگر T یک pـ زیرگروه سیلو از G باشد نشان دهید که برای یک $h \in H$، $h^{-1}Th \cap K$ یک pـ زیرگروه سیلو از K است.

تمرین ۲۵.۹.۱. فرض کنیم H زیرگروه نرمال گروه G باشد اگر H و G/H، pـ گروه باشند نشان دهید G یک p گروه است.

تمرین ۲۶.۹.۱. (*) فرض کنیم G گروه متناهی باشد به علاوه H یک pـ زیرگروه سیلو و $g \in G$ و $o(g) = p^t$ که $t \in \mathbb{N}$. اگر $gHg^{-1} = H$ آنگاه $g \in H$.

تمرین ۲۷.۹.۱. فرض کنیم G یک pـ گروه باشد. اگر H یک زیرگروه سره از G باشد نشان دهید $g \in G \setminus H$ وجود دارد که $gHg^{-1} = H$.

تمرین ۲۸.۹.۱. تمام ۳ـ زیرگروه‌های گروه $(\mathbb{Z}_{18}, +)$ را پیدا کنید.

تمرین ۲۹.۹.۱. نشان دهید که یک گروه از مرتبه ۸۱ دارای یک زیرگروه نرمال با بیش از ۳ عنصر است.

تمرین ۳۰.۹.۱. نشان دهید $(\mathbb{Q}, +)$ سری ترکیبی ندارد.

تمرین ۳۱.۹.۱. نشان دهید هر گروه متناهی سری ترکیبی دارد.

تمرین ۳۲.۹.۱. نشان دهید گروه آبلی G سری ترکیبی دارد اگر و تنها اگر متناهی باشد.

تمرین ۳۳.۹.۱. اگر G یک pـ گروه باشد نشان دهید هر عامل سری ترکیبی با $\mathbb{Z}_p$ یکریخت است.

تمرین ۳۴.۹.۱. گروه متناهی G حلپذیر است اگر و تنها اگر هر عامل سری ترکیبی با $\mathbb{Z}_p$ یکریخت باشد.

تمرین ۳۵.۹.۱. نشان دهید برای $n \geq 5$ گروه S_n حلپذیر نیست (راهنمایی: $S'_n = A_n$).

تمرین ۳۶.۹.۱. نشان دهید که اگر N زیرگروه نرمال گروه G با شرط $G \cap N = \{e\}$ باشد آنگاه $N \subseteq Z(G)$.

تمرین ۳۷.۹.۱. هر گروه از مرتبه p^2q^2 که p و q اعداد اولند حلپذیر است.

تمرین ۳۸.۹.۱. گروه متناهی G حلپذیر است اگر و تنها اگر برای هر زیرگروه $H \neq \{e\}$ داشته باشیم $H' \neq H$.

تمرین ۳۹.۹.۱. (*) فرض کنیم G گروه پوچتوان متناهی و p عدد اولی باشد که مرتبه G را می‌شمارد. نشان دهید p مرتبه $Z(G)$ را نیز می‌شمارد.

تمرین ۴۰.۹.۱. آیا گروه $S_3 \times S_3$ پوچتوان است؟

تمرین ۴۱.۹.۱. *فرض کنیم G گروهی پوچتوان و متناهی باشد. نشان دهید برای هر زیرگروه سره H داریم $H \subset N(H)$.*

تمرین ۴۲.۹.۱. (*) *فرض کنیم G گروهی پوچتوان و متناهی باشد. نشان دهید هر زیرگروه ماکسیمال G در G نرمال است.*

تمرین ۴۳.۹.۱. *فرض کنیم G گروهی پوچتوان و متناهی باشد. نشان دهید هر pـ زیرگروه سیلو G نرمال است.*

فصل ۲

مباحثی در نظریه حلقه‌ها

یکی از مهمترین ساختارهای جبری حلقه‌ها هستند. نظریه حلقه‌ها به مطالعه ساختار، مشخصه سازی حلقه، روابط بین عنصرهای حلقه و ایده‌آل‌ها می‌پردازد. مطالعه نظریه حلقه‌ها در شکل امروزی به دو دسته حلقه جابجایی و حلقه ناجابجایی تقسیم می‌شود. حلقه‌های جابجایی بهتر از حلقه‌های ناجابجایی فهمیده می‌شوند زیرا حلقه‌های ناجابجایی گاهی اوقات رفتار غیر معمول از خود نشان می‌دهند. نظریه حلقه‌های ناجابجایی در به دلیل پیچیدگی بیشتر در مقطع کارشناسی مطالعه نمی‌شود.

در این فصل ما قسمتی مقدماتی از نظریه حلقه‌های جابجایی را مطالعه خواهیم کرد. نظریه حلقه‌های جابجایی اهمیت فراوانی در هندسه جبری و نظریه اعداد دارد. انتظار این است که دانشجو با تعاریف و مفاهیم اولیه حلقه و برخی قضایا که در درس مبانی جبر آمده است، آشنا باشد. در صورت نیاز نگاهی به مطالبی که در مبانی جبر آموخته‌اید بیاندازید.

قرار داد: در ادامه هر جا صحبت از حلقه R می‌شود منظور حلقه‌ای جابجایی و یکدار است مگر این که به روشنی خلاف این قرار داد را بیان کنیم. علت فرض یکدار بودن حلقه را در بخش اول همین فصل خواهید دید.

۱.۲ حاصل ضرب مستقیم حلقه‌ها

در این بخش می‌خواهیم با کمک خانواده‌ای از حلقه‌ها حلقه جدیدی ارائه کنیم.

تعریف ۱.۱.۲. *فرض کنیم Γ یک مجموعه اندیس گذار ناتهی باشد. اگر $\{R_\alpha\}_{\alpha\in\Gamma}$ خانواده‌ای از حلقه‌ها باشد آنگاه منظور از حاصل ضرب مستقیم این خانواده یعنی مجموعه همه دنباله‌ها به صورت $(r_\alpha)_{\alpha\in\Gamma}$ که $r_\alpha \in R_\alpha$، به عبارت دیگر،*

$$\prod_{\alpha\in\Gamma} R_\alpha = \{(r_\alpha)_{\alpha\in\Gamma} \mid r_\alpha \in R_\alpha\}.$$

اگر این خانواده تهی باشد قرار می‌دهیم $\prod_{\alpha\in\Gamma} R_\alpha = 0$.

لم ۲.۱.۲. *اگر $\{R_\alpha\}_{\alpha\in\Gamma}$ خانواده‌ای از حلقه‌ها باشد آنگاه حاصل ضرب مستقیم این خانواده با عمل جمع و ضرب که به صورت زیر تعریف می‌شوند یک حلقه است.*

$$(r_\alpha)_{\alpha\in\Gamma}+(s_\alpha)_{\alpha\in\Gamma}=(r_\alpha+s_\alpha)_{\alpha\in\Gamma},\ \ (r_\alpha)_{\alpha\in\Gamma}\,.\,(s_\alpha)_{\alpha\in\Gamma}=(r_\alpha s_\alpha)_{\alpha\in\Gamma}$$

اثبات. اثبات سر راست است. دقت شود $(1_\alpha)_{\alpha\in\Gamma}$ که 1_α عنصر همانی حلقه R_α، همانی $\prod_{\alpha\in\Gamma}R_\alpha$ است. به علاوه چون هر R_α جابجایی است پس $\prod_{\alpha\in\Gamma}R_\alpha$ نیز جابجایی است. □

تعریف ۳.۱.۲. *فرض کنیم $\{R_\alpha\}_{\alpha\in\Gamma}$ خانواده‌ای از حلقه‌ها باشد. به مجموعه تمام دنباله‌های $(r_\alpha)_{\alpha\in\Gamma}$ در $\prod_{\alpha\in\Gamma}R_\alpha$ که به جز تعداد متناهی از عناصر دنباله بقیه صفر هستند، حاصل جمع مستقیم این خانواده گوییم و با $\bigoplus_{\alpha\in\Gamma}R_\alpha$ نمایش می‌دهیم، یعنی*

$$\bigoplus_{\alpha\in\Gamma}R_\alpha=\{(r_\alpha)_{\alpha\in\Gamma}\mid r_\alpha\in R_\alpha,\ \text{به جز تعداد متناهی از } r_\alpha\text{ها بقیه صفرند}\}.$$

واضح است که اگر این خانواده تهی باشد قرار می‌دهیم $\bigoplus_{\alpha\in\Gamma}R_\alpha=0$.

لم ۴.۱.۲. *اگر $\{R_\alpha\}_{\alpha\in\Gamma}$ خانواده‌ای از حلقه‌ها باشد آنگاه حاصل جمع مستقیم این خانواده با عمل جمع و ضرب القا شده از حلقه $\prod_{\alpha\in\Gamma}R_\alpha$ یک حلقه غیر یکدار است.*

اثبات. اثبات سر راست است. چون هر R_α جابجایی است پس $\bigoplus_{\alpha\in\Gamma}R_\alpha$ جابجایی است. دقت شود که اگر $\bigoplus_{\alpha\in\Gamma}R_\alpha$ بخواهد یکدار باشد آنگاه عنصر یک آن حتما باید به صورت $(1_\alpha)_{\alpha\in\Gamma}$ که 1_α عنصر همانی حلقه R_α است، باشد در حالی که چنین عنصری در $\bigoplus_{\alpha\in\Gamma}R_\alpha$ نیست (چرا؟). □

لم ۵.۱.۲. *اگر $\{R_\alpha\}_{\alpha\in\Gamma}$ خانواده‌ای از حلقه‌ها باشد آنگاه $\bigoplus_{\alpha\in\Gamma}R_\alpha$ ایده‌آلی از حلقه $\prod_{\alpha\in\Gamma}R_\alpha$ است.*

اثبات. اثبات سر راست است. □

لم ۶.۱.۲. *اگر $\{R_\alpha\}_{\alpha\in\Gamma}$ خانواده‌ای متناهی از حلقه‌ها باشد آنگاه $\bigoplus_{\alpha\in\Gamma}R_\alpha=\prod_{\alpha\in\Gamma}R_\alpha$.*

اثبات. اثبات سر راست است. □

گزاره زیر ساختار ایده‌آل‌های حاصل ضرب متناهی مستقیم را از روی ایده‌آل‌های اعضای خانواده به دست می‌دهد.

گزاره ۷.۱.۲. *اگر R_1، ...، R_n خانواده‌ای متناهی از حلقه‌ها باشد آنگاه $I=\prod_{i=1}^n I_i$ که I_i ایده‌آل R_i، یک ایده‌آل حلقه $\prod_{i=1}^n R_i$ است. به علاوه هر ایده‌آل I از حلقه $\prod_{i=1}^n R_i$ به صورت $I=\prod_{i=1}^n I_i$ است که I_i ایده‌آل R_i است.*

اثبات. اثبات قسمت اول سر راست است. برای قسمت دوم؛ فرض کنیم I یک ایده‌آل دلخواه از حلقه $\prod_{i=۱}^{n} R_i$ باشد. برای هر عدد طبیعی i همریختی حلقه‌ای (پوشا) طبیعی

$$\pi_i : \prod_{i=۱}^{n} R_i \longrightarrow R_i, \;\; \pi((r_۱, ..., r_i, ..., r_n)) = r_i$$

را در نظر می‌گیریم. حال قرار می‌دهیم $\pi_i(I) = I_i$. چون برای هر عدد طبیعی i، π_i یک همریختی است پس I_i یک ایده‌آل از R_i است. حال نشان می‌دهیم که $I = \prod_{i=۱}^{n} I_i$. فرض کنیم $x = (r_۱, ..., r_i, ..., r_n) \in I$. بوضوح $\pi_i(x) = r_i \in I_i$. در نتیجه $x \in \prod_{i=۱}^{n} I_i$ یعنی $I \subseteq \prod_{i=۱}^{n} I_i$. حال فرض کنیم $(s_۱, ..., s_i, ..., s_n) \in \prod_{i=۱}^{n} I_i$. پس $s_i \in I_i$ یعنی برای هر i، $x_i \in I$ چنان موجود است که $\pi_i(x_i) = s_i$. با توجه به ضابطه π_i حتما باید $x_i = (..., s_i, ...)$ باشد. چون I ایده‌آل است پس

$$e_i x_i = (۰, ..., ۰, \underset{i}{۱}, ۰, ..., ۰)x_i = (۰, ..., ۰, s_i, ۰, ..., ۰) \in I.$$

دوباره چون I ایده‌آل است پس

$$e_۱x_۱ + ... + e_i x_i + ... + e_n x_n = (s_۱, ..., s_i, ..., e_n) \in I.$$

در نتیجه $\prod_{i=۱}^{n} I_i \subseteq I$ و اثبات کامل است. □

وقت آن است که دلیل فرض یکدار بودن حلقه‌ها را در کتاب‌های مرجع جبر بیان کنیم. هر چند مطالعه حلقه‌های غیر یکدار خود به تنهایی مبحثی پیچیده و جالب است اما قضیه زیر بیان می‌دارد که چرا حلقه‌های یکدار بیشتر مورد توجه هستند. ابتدا تعریف زیر را داریم.

تعریف ۸.۱.۲. *گوییم حلقه R در حلقه S می‌نشیند یا نشانده می‌شود هرگاه همریختی حلقه‌ای یک به یک از R به S موجود باشد. این مفهوم را با $R \hookrightarrow S$ نشان می‌دهیم. گاهی اگر ابهامی ایجاد نشود بدون هیچ ترسی این مفهوم را با $R \subseteq S$ نشان می‌دهیم. این بدان معنی است که R با زیرحلقه‌ای از S یکریخت است و به همین جهت می‌توان خود R را زیرحلقه S در نظر گرفت.*

اکنون قضیه زیر را داریم.

قضیه ۹.۱.۲. *هر حلقه نه لزوما یکدار R در یک حلقه یکدار S نشانده می‌شود.*

اثبات. قرار می‌دهیم $S = R \times \mathbb{Z}$. مجموعه S را به جمع و ضرب زیر مجهز می‌کنیم

$$(r, n) + (r', n') = (r + r', n + n'), \;\; (r, n) \,.\, (r', n') = (rr' + nr' + rn', nn').$$

یک بررسی ساده نشان می‌دهد که S با جمع و ضرب بالا یک حلقه است. دقت شود که عنصر $(۰, ۱)$ همانی S است. به علاوه چون R جابجایی است S نیز جابجایی است. حال ضابطه

$$f : R \longrightarrow S, \;\; f(r) = (r, ۰)$$

یک همریختی حلقه‌ای یک به یک است یعنی $R \hookrightarrow S$. □

قضیه باقیمانده چینی قضیه‌ای در زمینه نظریه اعداد است که کاربرد وسیعی در نظریه اعداد دارد. این تذکر لازم است که پایه و اساس نظریه اعداد بر حلقه اعداد صحیح بنا نهاده شده است. در ادامه تعمیمی از باقیمانده چینی در حلقه جابجایی دلخواه بیان می‌شود.

یادآوری ۱۰.۱.۲. *(باقیمانده چینی در اعداد صحیح) فرض کنیم n_1، ...، n_k اعداد صحیحی باشند که دو به دو نسبت به هم اولند. برای هر سری اعداد صحیح a_1، ...، a_k عدد صحیح x وجود دارد به طوری که در دستگاه معادلات همنهشتی*

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv a_2 \pmod{n_2} \\ &\vdots \\ x &\equiv a_k \pmod{n_k} \end{aligned}$$

صدق کند. علاوه بر این تمام جواب‌های x به پیمانه $N = n_1 n_2 ... n_k$ همنهشتند.

قضیه ۱۱.۱.۲. *(باقیمانده چینی) فرض کنیم R یک حلقه باشد و I_1، ...، I_n ایده‌آل‌های R باشند که برای هر $i \neq j$ داشته باشیم $I_i + I_j = R$. اگر b_1، ...، b_n عنصرهای دلخواه در R باشند آنگاه عنصر b در R چنان موجود است که $b - b_i \in I_i$ (در واقع $b \overset{I_i}{\equiv} b_i$). به علاوه اگر c موجود باشد که خاصیت b را داشته باشد آنگاه $b - c \in \bigcap_{i=1}^{n} I_i$ (در واقع $b \overset{\cap_{i=1}^{n} I_i}{\equiv} c$).*

اثبات. با استقرا روی n نشان می‌دهیم که

$$I_1 + (I_2 \cap ... \cap I_n) = R.$$

اگر $n = 2$ باشد چیزی برای اثبات وجود ندارد. پس فرض کنیم (فرض استقرا) که

$$I_1 + (I_2 \cap ... \cap I_{n-1}) = R.$$

داریم که

$$\begin{gathered} R = R^2 = RR = (I_1 + I_n)(I_1 + (I_2 \cap ... \cap I_{n-1})) = \\ (I_1 + I_n)I_1 + (I_1 + I_n)(I_2 \cap ... \cap I_{n-1}) = \\ I_1 I_1 + I_n I_1 + I_1(I_2 \cap ... \cap I_{n-1}) + I_n(I_2 \cap ... \cap I_{n-1}) \subseteq \\ I_1 + (I_2 \cap ... \cap I_{n-1}) \end{gathered}$$

یعنی

$$I_1 + (I_2 \cap ... \cap I_n) = R.$$

به صورت کاملا مشابه بالا می‌توان برای هر j نشان داد که

$$I_j + (I_1 \cap ... \cap I_{j-1} \cap I_{j+1} \cap ... \cap I_n) = R.$$

چون b_iها در R هستند پس داریم که

$$\begin{aligned}
b_1 &= a_1 + r_1 \quad (a_1 \in I_1,\ r_1 \in I_2 \cap \ldots \cap I_n)\\
b_2 &= a_2 + r_2 \quad (a_2 \in I_2,\ r_2 \in I_1 \cap I_3 \cap I_4 \cap \ldots \cap I_n)\\
&\vdots\\
b_j &= a_j + r_j \quad (a_j \in I_j,\ r_j \in I_1 \cap \ldots \cap I_{j-1} \cap I_{j+1} \cap \ldots \cap I_n)\\
&\vdots\\
b_n &= a_n + r_n \quad (a_n \in I_n,\ r_n \in I_1 \cap \ldots \cap I_{n-1}).
\end{aligned}$$

حال عنصر b را برابر $r_1 + \ldots + r_n$ قرار می‌دهیم. این b خاصیت حکم را دارا است زیرا برای هر i داریم

$$b - b_i = r_1 + \ldots + r_n - a_i - r_i = r_1 + \ldots + r_{i-1} + r_{i+1} + \ldots + r_n - a_i \in I_i.$$

در واقع داریم $b \overset{I_i}{\equiv} b_i$. برای قسمت دوم؛ اگر c در خاصیت b صدق کند یعنی $c \overset{I_i}{\equiv} b_i$ آنگاه برای هر i داریم

$$(b - b_i) - (c - b_i) = b - c \in I_i.$$

در نتیجه برای هر i، $b \overset{I_i}{\equiv} c$. بنابراین $b \overset{\cap_{i=1}^n I_i}{\equiv} c$. □

حال نتیجه مهم زیر را داریم.

نتیجه ۱۲.۱.۲. *فرض کنیم R یک حلقه، I_1، ...، I_n ایده‌آل‌های R باشند و $I = \bigcap_{i=1}^n I_i$. در این صورت رابطه*

$$f : R/I \longrightarrow R/I_1 \times \ldots \times R/I_n, \quad f(r + I) = (r + I_1, \ldots, r + I_n)$$

یک همریختی حلقه‌ای است. به علاوه اگر برای هر $i \neq j$ داشته باشیم $I_i + I_j = R$ آنگاه f یکریختی است یعنی

$$R/I \cong R/I_1 \times \ldots \times R/I_n.$$

اثبات. این که f خوشتریف و همریختی حلقه‌ای یک به یک است یک بررسی ساده است. کافی است پوشایی f را نشان دهیم. فرض کنیم

$$(r_1 + I_1, \ldots, r_n + I_n) \in R/I_1 \times \ldots \times R/I_n.$$

حال طبق قضیه باقیمانده چینی، قضیه ۱۱.۱.۲، برای عنصرهای r_1، ...، r_n عنصر r چنان وجود دارد که $r - r_i \in I_i$. یعنی $r + I_i = r_i + I_i$. حال داریم

$$f(r) = (r + I_1, \ldots, r + I_n) = (r_1 + I_1, \ldots, r_n + I_n)$$

یعنی f پوشا است. □

تمرین حل شده

تمرین ۱۳.۱.۲. *نشان دهید که $R_1 \times R_2$ هرگز نمی‌تواند دامنه صحیح باشد.*

اثبات. بوضوح همواره داریم $(۰, ۱).(۱, ۰) = (۰, ۰)$. پس حاصل ضرب مستقیم حلقه‌ها هرگز نمی‌تواند دامنه صحیح باشد حتی اگر حاصل ضرب مستقیم توسط خانواده حلقه‌هایی باشد که دامنه صحیح‌اند. □

تمرین ۱۴.۱.۲. *اگر منظور از $U(R)$ مجموعه تمام عنصرهای یکال حلقه R باشد آنگاه نشان دهید که $U(R_1 \times ... \times R_n) = U(R_1) \times ... \times U(R_n)$.*

اثبات. فرض کنیم $x = (r_1, ..., r_n) \in U(R_1 \times ... \times R_n)$. پس عنصر $(s_1, ..., s_n)$ چنان وجود دارد که

$$(r_1, ..., r_n)(s_1, ..., s_n) = (1, ..., 1).$$

پس برای هر i، داریم $r_i s_i = 1$. یعنی $r_i \in U(R_i)$. پس $x \in U(R_1) \times ... \times U(R_n)$. حال برعکس؛ اگر $x = (r_1, ..., r_n) \in U(R_1) \times ... \times U(R_n)$ آنگاه برای هر i، عنصر s_i چنان موجود است که داریم $r_i s_i = 1$. پس

$$(r_1, ..., r_n)(s_1, ..., s_n) = (1, ..., 1).$$

یعنی $x = (r_1, ..., r_n) \in U(R_1 \times ... \times R_n)$ و اثبات کامل است. □

تمرین ۱۵.۱.۲. *نشان دهید $(r_1, ..., r_n) \in R_1 \times ... \times R_n$ پوچتوان است اگر و تنها اگر برای هر i، r_i پوچتوان باشد.*

اثبات. اگر $x = (r_1, ..., r_n)$ دارای مرتبه پوچتوانی k باشد آنگاه

$$(۰, ..., ۰) = (r_1, ..., r_n)^k = (r_1^k, ..., r_n^k).$$

یعنی برای i، $r_i^k = ۰$. حال برعکس؛ فرض کنیم برای هر i عدد صحیح و نامنفی k_i چنان باشد که $r_i^{k_i} = ۰$. قرار می‌دهیم $k = k_1 + ... + k_n$. بوضوح داریم

$$(۰, ..., ۰) = (r_1^k, ..., r_n^k) = (r_1, ..., r_n)^k$$

و اثبات کامل است. □

۲.۲ ایده‌آل‌های اول و ماکسیمال

اهمیت اعداد اول در نظریه اعداد بر کسی پوشیده نیست. در حقیقت اعداد اول در ساختار اعداد صحیح و اعداد گویا مشابه نقشی مانند اتم در در ساختار ملکول‌ها و مواد دارد. بنابراین بسیار بدیهی است که ریاضیدانان در حلقه‌های جابجایی دنبال تعمیمی از مفهوم اول باشند. اما $\mathbb{Z}$ یک دامنه ایده‌آل اصلی است (به بخش ۵ همین فصل مراجعه کنید) لذا هر ایده‌آل با یک عنصر تولید می‌شود پس در شناسایی خواص جبری $\mathbb{Z}$ تقریبا نقش عنصرها و ایده‌آل‌ها به نوعی یکسان است. اما وقتی یک حلقه جابجایی دلخواه در اختیار داریم ممکن است بررسی عناصر ساختار حلقه را به خوبی مشخص نکند و لذا گاهی مطالعه ایده‌آل‌ها مهم‌تر از مطالعه عناصر است. مطالعه حلقه با کمک ایده‌آل‌ها از یک نظر کاراتر است و آن این که یک مجموعه ممکن است با عمل‌های مختلفی تبدیل به حلقه‌های متفاوت شود که در این حالت عناصر تغییری نمی‌کنند اما ایده‌آل‌ها دچار تغییر می‌شوند. بنابراین برای تعمیم مفهوم عدد اول در حلقه اعداد صحیح به یک حلقه دلخواه از معادل ایده‌آلی استفاده می‌کنیم. برای این منظور توجه می‌کنیم که در $\mathbb{Z}$ عدد صحیح p اول است اگر و تنها اگر $p|ab$ آنگاه $p|a$ یا $p|b$. حال این مطلب به زبان ایده‌آلی به این شکل است که ایدهآل $I =< p >$ اول است اگر و تنها اگر $ab \in < p >$ آنگاه $a \in < p >$ یا $b \in < p >$. حال تعریف کلی زیر را داریم.

تعریف ۱.۲.۲. *ایده‌آل سره P از حلقه (جابجایی) R را اول گوییم هرگاه $ab \in P$ که $a, b \in R$ ایجاب کند $a \in P$ یا $b \in P$.*

مثال ۲.۲.۲. *به وضوح ایده‌آل صفر در حلقه اعداد صحیح اول است. اما ایده‌آل صفر در حلقه $\mathbb{Z}_۴$ اول نیست. زیرا $\bar{۲} \times \bar{۲} = \bar{۰} \in < \bar{۰} >$ اما $\bar{۲} \notin < \bar{۰} >$.*

حال در چند قضیه زیر مشخصه سازی‌های برای ایده‌آل اول در اختیار قرار می‌دهیم.

قضیه ۳.۲.۲. *ایده‌آل سره P از حلقه R اول است اگر و تنها اگر $IJ \subseteq P$ که I و J ایده‌آل‌های حلقه R هستند، ایجاب کند $I \subseteq P$ یا $J \subseteq P$.*

اثبات. ($\Leftarrow$). فرض کنیم که I و J دو ایده‌آل از R باشند و $IJ \subseteq P$ ولی $I \nsubseteq P$. می‌خواهیم نشان دهیم که $J \subseteq P$. چون $I \nsubseteq P$ پس می‌توانیم عنصری مانند $x \in I \setminus P$ انتخاب کنیم. پس $xJ \subseteq P$ و بنابراین برای هر $y \in J$ داریم که $xy \in P$. اما طبق فرض P اول است و چون $x \notin P$ در نتیجه $y \in P$. و این نشان می‌دهد که $J \subseteq P$.
($\Rightarrow$). طبق فرض P سره است پس کافی است نشان دهیم که اگر $ab \in P$ که $a, b \in R$ آنگاه $a \in P$ یا $b \in P$. چون $ab \in P$ پس $Rab \subseteq P$. اما R حلقه جابجایی است در نتیجه $RaRb \subseteq P$. حال طبق فرض باید $Ra \subseteq P$ یا $Rb \subseteq P$. یعنی نشان داده‌ایم که $a \in P$ یا $b \in P$. □

قضیه ۴.۲.۲. *ایده‌آل سره P از حلقه R اول است اگر و تنها اگر حلقه خارج قسمتی R/P دامنه صحیح باشد.*

اثبات. ($\Leftarrow$). فرض کنیم که $(a+P)(b+P)=\bar{0}$. بوضوح باید $ab\in P$. چون P اول است پس $a\in P$ یا $b\in P$ و این معادل این است که $a+P=\bar{0}$ یا $b+P=\bar{0}$. بنابراین حلقه خارج قسمتی R/P دامنه است.
($\Rightarrow$). طبق فرض P سره است پس کافی است نشان دهیم که اگر $ab\in P$ که $a,b\in R$ آنگاه $a\in P$ یا $b\in P$. چون $ab\in P$ پس $ab+P=\bar{0}$. در نتیجه $(a+P)(b+P)=\bar{0}$. چون R/P دامنه است پس $a+P=\bar{0}$ یا $b+P=\bar{0}$ این معادل این است که $a\in P$ یا $b\in P$. □

تعریف ۵.۲.۲. *گوییم ایده‌آل سره M از حلقه R ماکسیمال است هرگاه برای هر ایده‌آل N که $M\subseteq N$ داشته باشیم $N=M$ یا $N=R$.*

مثال ۶.۲.۲. *به وضوح ایده‌آل صفر در حلقه اعداد صحیح $\mathbb{Z}$ ماکسیمال نیست ولی $۲\mathbb{Z}$ در $\mathbb{Z}$ ماکسیمال است. همچنین ایده‌آل $۲\mathbb{Z}_۴$ با یک بررسی سر راست در حلقه $\mathbb{Z}_۴$ ماکسیمال است.*

حال قضیه زیر را داریم.

قضیه ۷.۲.۲. *برای حلقه R و ایده‌آل سره M احکام زیر معادل هستند.*
(۱) *M ماکسیمال است.*
(۲) *R/M میدان است.*
(۳) *برای هر عنصر $x\in R\setminus M$ داریم $M+Rx=R$.*

اثبات. (۱) $\Leftarrow$ (۲). طبق قضیه تناظر، هر ایده‌آل حلقه R/M به صورت N/M است که N ایده‌آلی از R شامل M است. پس $N=M$ یا $N=R$. یعنی R/M ایده‌آل نابدیهی ندارد. اکنون فرض کنیم $\bar{x}=x+M$ عنصر ناصفر در $\bar{R}=R/M$ باشد. پس باید $\bar{R}\bar{x}=\bar{R}$. پس عنصر $\bar{y}$ چنان موجود است که $\bar{x}\bar{y}=\bar{۱}$. یعنی $\bar{R}$ میدان است.
(۲) $\Leftarrow$ (۳). ایده‌آل $M+Rx$ ایده‌آلی از R است که به صورت سره شامل M است. این یعنی ایده‌آل $(M+Rx)/M$ یک ایده‌آل ناصفر در R/M است. چون میدان فقط دو ایده‌آل دارد پس باید $M+Rx=R$ باشد.
(۳) $\Leftarrow$ (۱). فرض کنیم $M\subseteq N$ باشد و $x\in N\setminus M$. طبق فرض داریم $M+Rx=R$. این نشان می‌دهد که $R\subseteq N$. بنابراین $N=R$ و در نتیجه M ماکسیمال است.
□

مثال قبلی مطلبی مهم را نشان می‌دهد که لزومی ندارد یک ایده‌آل اول ماکسیمال باشد. پس سوال طبیعی ممکن است پیش آید و آن این است که آیا هر ماکسیمالی اول است؟ گزاره زیر پاسخ این مطلب را می‌دهد.

گزاره ۸.۲.۲. *هر ایده‌آل ماکسیمال M اول است.*

اثبات. فرض کنیم $IJ\subseteq M$ باشد. به برهان خلف، اگر $I\not\subseteq M$ و $J\not\subseteq M$ آنگاه طبق قضیه ۷.۲.۲، $I+M=R$ و $J+M=R$ است. داریم

$$R=R^۲=(I+M)(J+M)=IJ+IM+MJ+M^۲\subseteq M+M+M+M=M.$$

یعنی $R = M$ است که تناقض با اول بودن M است. □

این بخش را با قضیه زیر به پایان می‌رسانیم. بر خود لازم می‌دانیم که یکبار دیگر قرار داد مهم این فصل را تکرار کنیم که حلقه‌ها یکدار هستند و قضیه زیر برای حلقه‌های یکدار اعتبار دارد.

قضیه ۹.۲.۲. *هر حلقه R دارای ایده‌آل ماکسیمال است.*

اثبات. قضیه را با کمک لم زرن اثبات می‌کنیم. قرار می‌دهیم

$$\mathcal{A} = \{I \mid I \text{ یک ایده‌آل سره از } R \text{ است}\}.$$

چون ایده‌آل صفر در $\mathcal{A}$ است پس $\mathcal{A}$ ناتهی است. می‌دانیم که با رابطه شمول می‌توان $\mathcal{A}$ را به یک مجموعه جزئا مرتب تبدیل کنیم. حال زنجیر ناتهی دلخواه $\{I_\alpha\}_{\alpha\in\Gamma}$ را در $\mathcal{A}$ در نظر می‌گیریم. قرار می‌دهیم $I = \bigcup_{\alpha\in\Gamma} I_\alpha$. با یک بررسی سر راست I یک ایده‌آل I است. اگر $I + R$ باشد آنگاه $1 \in I$. پس اندیس α چنان وجود دارد که $1 \in I_\alpha$. این در تناقض آشکار با اعضای زنجیر است که در $\mathcal{A}$ قرار دارند. پس $R \neq I$ و در نتیجه $I \in \mathcal{A}$. به وضوح I یک کران بالا برای زنجیر است. یعنی تا اینجا نشان داده‌ایم که هر زنجیر ناتهی از $\mathcal{A}$ کران بالایی در $\mathcal{A}$ دارد و در نتیجه طبق لم زرن $\mathcal{A}$ داری عضو ماکسیمال مانند M است. چون $M \in \mathcal{A}$ پس M ایده‌آل است و باید نشان دهیم که M ایده‌آل ماکسیمال است تا اثبات کامل شود. فرض کنیم که ماکسیمال نباشد پس ایده‌آل N چنان وجود دارد که $M \subset N \subset R$. بنابراین $N \in \mathcal{A}$ و این یعنی M عضو ماکسیمال $\mathcal{A}$ نیست که تناقض است. □

نتیجه ۱۰.۲.۲. *هر ایده‌آل سره I از حلقه R در داخل یک ایده‌آل ماکسیمال قرار می‌گیرد.*

اثبات. حلقه R/I را در نظر می‌گیریم. حال طبق قضیه ۹.۲.۲، حلقه R/I دارای ایده‌ال ماکسیمال است. طبق قضیه تناظر این ایده‌آل ماکسیمال به صورت M/I که M ایده‌آلی از R شامل I است. دوباره با کمک قضیه تناظر باید M در R ایده‌آل ماکسیمال باشد و اثبات کامل است. □

تمرین حل شده

تمرین ۱۱.۲.۲. *نشان دهید که تعداد ایده‌آل‌های اول حلقه $\mathbb{Z}_8$ فقط یکی است.*

اثبات. می‌دانیم تمام ایده‌آل‌های $\mathbb{Z}_8$ به صورت زیر است.

$$I_1 = \{\bar{0}\}$$
$$I_2 = \{\bar{0}, \bar{4}\}$$
$$I_3 = \{\bar{0}, \bar{2}, \bar{4}, \bar{6}\}$$
$$I_4 = \mathbb{Z}_8$$

ایده‌آل $I_۴$ که به وضوح اول نیست. اما چون $\bar۰ = \bar۲\bar۴ \in I_۱$ ولی $\bar۲ \notin I_۱$ و $\bar۴ \notin I_۱$ پس $I_۱$ هم اول نیست. از طرفی $\bar۴ = \bar۲\bar۲ \in I_۲$ اما $\bar۲ \notin I_۲$ پس $I_۲$ هم اول نیست. چوا ایده‌آل‌های $\mathbb{Z}_۸$ یک زنجیر هستند بوضوح $I_۳$ ایده‌آل ماکسیمال است و طبق گزاره ۸.۲.۲، $I_۳$تنها ایده‌آل اول است. □

تمرین ۱۲.۲.۲. *اگر هر ایده‌آل حلقه R اول باشد آنگاه R یک میدان است.*

اثبات. فرض کنیم $xy = ۰$ که $x, y \in R$. پس $xy \in < ۰ > = \{۰\}$ و طبق فرض $< ۰ >$ اول است. در نتیجه باید $x = ۰$ یا $y = ۰$. بنابراین R دامنه صحیح است. حال برای هر عنصر ناصفر $x \in R$ داریم که $Rx^۲ \subseteq Rx$. اما طبق فرض $Rx^۲$ اول است و چون $x^۲ \in Rx^۲$ پس $x \in Rx^۲$ و لذا $Rx \subseteq Rx^۲$، یعنی $Rx = Rx^۲$. در نتیجه عنصر $r \in R$ چنان موجود است که $x = rx^۲$ یا معادلا $x(۱ - rx) = ۰$. چون R دامنه صحیح و x ناصفر است باید $rx = ۱$. یعنی x وارون‌پذیر است و درنتیجه R میدان است. □

تمرین ۱۳.۲.۲. *فرض کنیم R حلقه باشد که هر عنصر آن خودتوان است (حلقه بولی، $x^۲ = x$ برای هر $x \in R$). نشان دهید هر ایده‌آل اول P از R ماکسیمال است.*

اثبات. چون P اول است پس طبق قضیه ۴.۲.۲، R/P دامنه صحیح است. اما برای هر $x \in R$ داریم

$$(x + P)(x + P) = x^۲ + P = x + P.$$

یعنی حلقه R/P نیز بولی است. این نتیجه می‌دهد که $R/P = \{\bar۰\}$ یا $R/P = \{\bar۰, \bar۱\}$. اگر $R/P = \{\bar۰\}$ آنگاه $R = P$ که با فرض اول بودن P در تناقض است. پس $R/P = \{\bar۰, \bar۱\}$. در نتیجه R/P یک میدان است و طبق قضیه ۷.۲.۲، P ایده‌آل ماکسیمال است و حل کامل است. □

۳.۲ آشنایی با حلقه چندجمله‌ای‌ها

حلقه چندجمله‌ای‌ها جایگاه ویژه‌ای در جبر و حتی سایر رشته‌های ریاضی دارد. مطالعه این حلقه‌ها برای نظریه میدان از اهمیت بالایی برخوردار است. در این بخش شما را تا حدی با این حلقه‌های مهم آشنا می‌کنیم.

تعریف ۱.۳.۲. *فرض کنیم R یک حلقه باشد. مجموعه چندجمله‌ای‌های با ضرایب روی R و یک متغیر x به صورت زیر تعریف می‌شود*

$$R[x] = \{r_n x^n + r_{n-1} x^{n-1} + ... + r_1 x + r_0 \mid n \in \mathbb{N},\ r_i \in R\}.$$

به هر عضو $R[x]$ یک چندجمله‌ای گوییم.

مثال ۲.۳.۲. *$f(x) = x^2 + x + 3$ یک چندجمله‌ای در $\mathbb{Z}[x]$ است.*

تعریف ۳.۳.۲. *فرض کنیم $f(x) = r_n x^n + ... + r_1 x + r_0 \in R[x]$. اگر $r_n \neq 0$ آنگاه به n درجه چندجمله‌ای و به r_0 ثابت $f(x)$ گوییم. به هر $r_i x^i$ جمله $f(x)$ گوییم. به r_n ضریب پیشرو و جمله $r_n x^n$ را جمله پیشرو نامیم.*

مثال ۴.۳.۲. *$f(x) = 2x^3 + x + 3$ یک چندجمله‌ای از درجه ۳ و ثابت ۳ در $\mathbb{Z}[x]$ است که سه جمله دارد. ۲ ضریب پیشرو و $2x^3$ جمله پیشرو است.*

تذکر ۵.۳.۲. *دو چندجمله‌ای مساویند اگر درجه‌های آنها مساوی و ضرایب جمله‌های هم درجه مساوی باشند.*

تذکر ۶.۳.۲. *گاهی لازم است دو عضو از $R[x]$ را در تعداد جملات یکسان کنیم. برای این کار از $0 \in R$ کمک می‌گیریم. به این صورت عمل می‌کنیم که اگر درجه $f(x)$ برابر n و درجه $g(x)$ برابر m و $m < n$ آنگاه به تعداد $m - n$ تا جمله به $g(x)$ اضافه می‌کنیم یعنی*

$$g(x) = 0x^n + 0x^{n-1} + ... + 0x^{m+1} + g_m x^m + ... + g_1 x + g_0.$$

اکنون می‌خواهیم $R[x]$ را به حلقه تبدیل کنیم. برای تبدیل $R[x]$ به یک حلقه یکدار نیاز به تعریف جمع و ضرب داریم. قبل از تعریف جمع و ضرب نیاز است که قرار داد زیر را بیان کنیم.

قرار داد ۷.۳.۲. *همواره فرض بر این است که عناصر حلقه R با x جابجا می‌شوند یعنی $rx = xr$ برای هر $r \in R$. به علاوه $x^i x^j = x^{i+j}$.*

تعریف ۸.۳.۲. *فرض کنیم*

$$f(x) = \sum_{i=1}^{n} r_i x^i \qquad g(x) = \sum_{i=1}^{m} s_i x^i$$

دو عضو دلخواه از $R[x]$ باشند. اگر نیاز باشد تعداد جملات $f(x)$ و $g(x)$ را طبق تذکر ۲.۳.۶، یکسان می‌کنیم (یعنی زمانی که مثلا $m < n$) پس می‌توانیم فرض کنیم

$$f(x) = \sum_{i=۱}^{n} r_i x^i = r_n x^n + ... + r_۰ \qquad g(x) = \sum_{i=۱}^{n} s_i x^i = s_n x^n + ... + s_۰$$

حال جمع را به صورت زیر تعریف می‌کنیم

$$f(x) + g(x) = \sum_{i=۱}^{n} r_i x^i + \sum_{i=۱}^{m} s_i x^i = \\ (r_n + s_n)x^n + ... + (r_۱ + s_۱)x + (r_۰ + s_۰).$$

ضرب به شکل زیر تعریف می‌شود (نیاز به یکسان سازی تعداد جملات نیست)

$$f(x)g(x) = (r_n x^n + ... + r_۰)(s_m x^m + ... + s_۰) = \\ (r_n s_m)x^{n+m} + ... + (r_۱ s_۰ + s_۱ r_۰)x + r_۰ s_۰.$$

یا گاهی خلاصه تر

$$f(x)g(x) = (\sum_{i=۱}^{n} r_i x^i)(\sum_{j=۱}^{m} s_j x^j) = \sum_{k=۰}^{n+m} c_k x^k$$

که در آن $c_k = \sum_{t=۰}^{k} r_t s_{k-t}$.

مثال ۹.۳.۲. *فرض کنیم*

$$f(x) = \bar{۲}x^۲ + \bar{۲} \qquad g(x) = \bar{۲}x + \bar{۳}$$

دو عنصر در $\mathbb{Z}_۴[x]$ باشند. داریم

$$f(x) + g(x) = \bar{۲}x^۲ + \bar{۲}x + \bar{۱}$$

و

$$f(x)g(x) = \bar{۰}x^۳ + \bar{۲}x^۲ + \bar{۰}x + \bar{۲} = \bar{۲}x^۲ + \bar{۲}.$$

حال لم زیر نشان می‌دهد که $R[x]$ یک حلقه جابجایی یکدار است.

لم ۱۰.۳.۲. *با جمع و ضرب داده شده در تعریف ۸.۳.۲، $R[x]$ یک حلقه جابجایی و یکدار است.*

اثبات. بررسی سر راست نشان می‌دهد که $(R[x], +)$ یک گروه آبلی است. البته این تذکر لازم است که چون $۰ \in R$ چندجمله‌ای

$$o(x) = ۰x^n + ۰x^{n-۱} + ... + ۰x + ۰$$

عضو خنثی جمعی است. همچنین $(R[x],.)$ یک نیم‌گروه است. البته این تذکر لازم است که چون $1 \in R$ چندجمله‌ای

$$i(x) = 0x^n + 0x^{n-1} + ... + 1x + 0$$

عضو خنثی جمعی است. به علاوه ضرب روی جمع توزیع‌پذیر از هر دو طرف است یعنی $R[x]$ یک حلقه یکدار است. از طرفی R جابجایی است پس طبق قرار داد ۷.۳.۲، $R[x]$ جابجایی است. □

نمادگذاری ۱۱.۳.۲. *برای راحتی کار صفر و یک حلقه $R[x]$ را با 0 و 1 نشان می‌دهیم. فرض کنیم $f(x) \in R[x]$ در این صورت منظور از $deg(f(x))$ همان درجه $f(x)$ است. گاهی اوقات برای راحتی نمایش عناصر حلقه $R[x]$ از x در $f(x)$ صرف نظر می‌کنیم.*

قرار داد ۱۲.۳.۲. *درجه چندجمله‌ای صفر را برابر $-\infty$ در نظر می‌گیریم.*

لم ۱۳.۳.۲. *برای هر $f, g \in R[x]$ داریم*

$$deg(f(x) + g(x)) \leq max\{deg(f(x)), deg(g(x))\}$$
$$deg(f(x)g(x)) \leq deg(f(x)) + deg(g(x))$$

اثبات. سر راست است. □

مثال ۱۴.۳.۲. *مثال ۹.۳.۲، نشان می‌دهد که در $deg(f(x)g(x)) \leq deg(f(x)) + deg(g(x))$ ممکن است تساوی رخ ندهد. چون $\mathbb{Z}_4$ مقسوم علیه صفر دارد.*

تعریف ۱۵.۳.۲. *گوییم $f(x) \in R[x]$ تکین است هرگاه ضریب پیشرو $f(x)$ برابر 1_R باشد.*

حال می‌خواهیم نشان دهیم که در $R[x]$ مانند حلقه اعداد صحیح الگوریتم تقسیم داریم.

قضیه ۱۶.۳.۲. *(الگوریتم تقسیم) فرض کنیم R حلقه باشد و $f(x), g(x) \in R[x]$. اگر ضریب پیشرو $g(x)$ یکال باشد آنگاه چندجمله‌ای‌های یکتای مانند $q(x)$ و $r(x)$ چنان وجود دارند که $f(x) = q(x)g(x) + r(x)$ و $deg(r(x)) < deg(g(x))$.*

اثبات. ابتدا دقت می‌کنیم که اگر درجه $f(x)$ از درجه $g(x)$ کمتر باشد کافی است $q(x)$ را صفر و $r(x)$ را خود $f(x)$ در نظر بگیریم. حال فرض کنیم

$$f(x) = \sum_{i=1}^{n} f_i x^i = f_n x^n + ... + f_0 \qquad g(x) = \sum_{i=1}^{m} g_i x^i = g_m x^m + ... + g_0$$

که $m \leq n$ و g_m نیز یکال است. حکم را به استقرا روی درجه $f(x)$ یعنی n اثبات می‌کنیم. فرض کنیم $n = 0$ پس در نتیجه $m = 0$. یعنی $g = g_0$ و طبق فرض باید g_0 یکال باشد. حال قرار

می‌دهیم $r = ۰$ و $q = f_۰ g_۰^{-۱}$ پس به وضوح داریم

$$f_۰ = f(x) = q(x)g(x) + r(x) =$$
$$(f_۰ g_۰^{-۱})g_۰ + ۰, \quad -\infty = deg(۰) = deg(r(x)) < deg(g(x)) = ۰.$$

اکنون فرض کنیم حکم برای هر عدد کمتر از n صحیح باشد (فرض استقرا). داریم

$$h(x) = f(x) - f_n g_m^{-۱} x^{n-m} g(x) =$$
$$(f_n x^n + ... + f_۰) - (f_n x^n + f_n g_m^{-۱} g_{m-۱} x^{n-۱} + \cdots + f_n g_m^{-۱} g_۰) =$$
$$(f_{n-۱} - f_n g_m^{-۱} g_{m-۱}) x^{n-۱} + \cdots .$$

چون $h(x)$ از درجه کمتر از n است پس طبق فرض استقرا $q'(x)$ و $r(x)$ چنان وجود دارند که

$$h(x) = q'(x)g(x) + r(x),\ deg(r(x)) < deg(g(x)).$$

پس

$$f(x) = h(x) + f_n g_m^{-۱} x^{n-m} g(x) = q'(x)g(x) + r(x) + f_n g_m^{-۱} x^{n-m} g(x) =$$
$$(q'(x) + f_n g_m^{-۱} x^{n-m}) g(x) + r(x).$$

در واقع $q(x) = q'(x) + f_n g_m^{-۱} x^{n-m}$. یعنی نشان داده‌ایم $f(x) = q(x)g(x) + r(x)$ و $deg(r(x)) < deg(g(x))$. حال یکتایی، فرض کنیم

$$q_۱(x)g(x) + r_۱(x) = f(x) = q_۲(x)g(x) + r_۲(x) \ \Rightarrow$$
$$(q_۱(x) - q_۲(x))g(x) = r_۲(x) - r_۱(x).$$

چون ضریب پیشرو $g(x)$ یکال است در لم ۱۳.۳.۲، برای حالت ضرب تساوی رخ می‌دهد (چرا؟) پس داریم

$$deg(r_۲(x) - r_۱(x)) = deg((q_۱(x) - q_۲(x))g(x)) =$$
$$deg(q_۱(x) - q_۲(x)) + deg(g(x)).$$

حال به برهان خلف فرض کنیم $q_۱(x) - q_۲(x) \neq ۰$. آنگاه $deg(q_۱(x) - q_۲(x)) \geq ۰$. بنابراین باید $deg(r_۲(x) - r_۱(x)) \geq deg(g(x))$. اما طبق لم ۱۳.۳.۲، داریم

$$deg(r_۲(x) - r_۱(x)) \leq max\{deg(r_۲(x)), deg(r_۱(x))\} < deg(g(x)).$$

این تناقض است و در نتیجه باید $q_۱(x) = q_۲(x)$. چون $(q_۱(x) - q_۲(x))g = r_۲(x) - r_۱(x)$ بلافاصله داریم $r_۱(x) = r_۲(x)$ و اثبات تمام است. □

مثال ۱۷.۳.۲. *خارج قسمت و باقیمانده* (q و r) *حاصل تقسیم* $\bar{۱} + x + x^۲$ *بر* $\bar{۱}x + \bar{۲}$ *در حلقه* $\bar{Z}_۵[x]$ *به ترتیب برابر است با* $\bar{۲} + \bar{۳}x$ *و* $\bar{۴}$.

قضیه ۱۸.۳.۲. *فرض کنیم R حلقه یکدار و $f(x) \in R[x]$. در این صورت به ازای هر $c \in R$ چندجمله‌ای یکتای $q(x)$ موجود است که*

$$f(x) = (x-c)q(x) + f(c).$$

اثبات. فرض کنیم $g(x) = x - c$. حال طبق قضیه ۱۶.۳.۲ ، چندجمله‌ای یکتای $q(x)$ چنان وجود دارد که داریم

$$f(x) = q(x)g(x) + r(x),\ deg(r) < ۱.$$

اکنون فرض کنیم که

$$q(x) = \sum_{i=۰}^{n} q_i x^i$$

در نتیجه داریم

$$f(x) = (\sum_{i=۰}^{n} q_i x^i)(x-c) + r(x) = \sum_{i=۰}^{n} q_i x^{i+۱} - \sum_{i=۰}^{n} q_i c x^i + r(x).$$

با محاسبه $f(c)$ داریم

$$f(c) = \sum_{i=۰}^{n} q_i c^{i+۱} - \sum_{i=۰}^{n} q_i c c^i + r(c) = \sum_{i=۰}^{n} q_i c^{i+۱} - \sum_{i=۰}^{n} q_i c^{i+۱} + r(c) = r(c)$$

و اثبات تمام است. □

تعریف ۱۹.۳.۲. *گوییم $r \in R$ ریشه چند جمله‌ای $f(x) \in R[x]$ است هرگاه $f(r) = ۰$.*

نتیجه ۲۰.۳.۲. *فرض کنیم $f(x) \in R[x]$. در این صورت $c \in R$ ریشه $f(x)$ است اگر و تنها اگر $q(x) \in R[x]$ موجود باشد که $f = (x-c)q(x)$.*

اثبات. ($\Leftarrow$). با استفاده از قضیه ۱۸.۳.۲ ، برای c چندجمله‌ای یکتای $q(x)$ وجود دارد که

$$f(x) = (x-c)q(x) + f(c).$$

اما طبق فرض c ریشه است یعنی $f(c) = ۰$. پس $f(x) = (x-c)q(x)$.
($\Rightarrow$). چون $f(x) = (x-c)q(x)$ پس به وضوح داریم

$$f(c) = q(c)(c-c) = ۰$$

یعنی c ریشه است. □

اکنون قضیه زیر را داریم.

قضیه ۲۱.۳.۲. *فرض کنیم D و E دو دامنه صحیح باشند که $D \subseteq E$ و $۰ \neq f(x) \in D[x]$ از درجه n باشد. در این صورت $f(x)$ در E حداکثر n ریشه دارد.*

اثبات. فرض کنیم T نشان دهنده مجموعه همه ریشه‌های $f(x)$ در E باشد. می‌خواهیم ثابت کنیم که $|T| \leq n$. به برهان خلف فرض کنیم که $|T| > n$. حال زیرمجموعه $\{c_۱, c_۲, ..., c_{n+۱}\}$ از T را در نظر می‌گیریم. چون $f(c_۱) = ۰$ پس طبق نتیجه ۲۰.۳.۲، چندجمله‌ای $q_۱(x)$ چنان در $E[x]$ وجود دارد که

$$f(x) = q_۱(x)(x - c_۱).$$

پس در نتیجه داریم

$$۰ = f(c_۲) = q_۱(c_۲)(c_۲ - c_۱).$$

اما $c_۲ - c_۱ \neq ۰$ و E دامنه صحیح است پس باید $q_۱(c_۲) = ۰$. با استفاده دوباره از نتیجه ۲۰.۳.۲، چندجمله‌ای $q_۲(x)$ چنان در $E[x]$ وجود دارد که

$$q_۱(x) = q_۲(x)(x - c_۲).$$

پس داریم

$$f(x) = q_۲(x)(x - c_۲)(x - c_۱).$$

این روند را nبار تکرار می‌کنیم در نتیجه خواهیم داشت

$$f(x) = q_n(x)(x - c_n)(x - c_{n-۱})...(x - c_۱).$$

اما درجه f برابر n است پس باید $q_n(x)$ چندجمله‌ای ثابت باشد یعنی $q_n(x) = b \in E$. پس

$$f(x) = b(x - c_n)(x - c_{n-۱})...(x - c_۱).$$

از طرفی داریم

$$۰ = f(c_{n+۱}) = b(c_{n+۱} - c_n)(c_{n+۱} - c_{n-۱})...(c_{n+۱} - c_۱).$$

اما برای هر i داریم $c_{n+۱} - c_i \neq ۰$ و E دامنه صحیح است پس باید $b = ۰$ باشد. در نتیجه $f = ۰$ که این تناقض است. بنابراین $|T| \leq n$. □

این بخش را با یک تعریف و یک گزاره به پایان می‌رسانیم.

تعریف ۲۲.۳.۲. *فرض کنیم R یک حلقه است. قرار می‌دهیم $S = R[x]$. حال حلقه چندجمله‌ای $S[y]$ (روی S و متغییر y) را حلقه چندجمله‌ای با دو متغییر گوییم و با $R[x, y]$ نشان می‌دهیم. این کار را می‌توان استقرایی به تعداد n متغییر گسترش داد. حلقه چندجمله‌ای با n متغییر را با $R[x_۱, ..., x_n]$ نشان می‌دهیم.*

تذکر ۲۳.۳.۲. *یک عنصر در حلقه $R[x, y]$ دارای نمایشی به شکل*

$$\sum_{i=۰}^{n} \sum_{j=۰}^{m} r_{ij} x^i y^j$$

است که در آن $r_{ij} \in R$.

گزاره ۲۴.۳.۲. *همواره برای حلقه R داریم $R[x, y] = R[y, x]$.*

اثبات. بدیهی است. □

تمرین حل شده

تمرین ۲۵.۳.۲. *فرض کنیم که $R[x]$ مقسوم علیه صفر دارد. نشان دهید که R نیز مقسوم علیه صفر دارد.*

اثبات. فرض کنیم که $f(x)$ و $g(x)$ دو عنصر ناصفر در $R[x]$ باشند که $f(x)g(x) = ۰$. چون $f(x)$ ناصفر است پس می‌توانیم جمله r_ix^i را در $f(x)$ چنان انتخاب کنیم که مینیمم درجه در جملات $f(x)$ باشد و r_i نیز ناصفر باشد. به همین صورت فرض کنیم s_jx^j مینیمم درجه در جملات $g(x)$ باشد و s_j نیز ناصفر باشد. حال واضح است که $r_is_jx^{i+j}$ مینیمم درجه در چندجمله‌ای $f(x)g(x)$ است. اما $f(x)g(x) = ۰$ پس باید $r_is_j = ۰$ و این یعنی R مقسوم علیه صفر دارد. □

تمرین ۲۶.۳.۲. *نشان دهید $f(x) \in R[x]$ یک مقسوم علیه صفر است اگر و تنها اگر $۰ \neq b \in R$ چنان موجود باشد که $bf(x) = ۰$.*

اثبات. ($\Leftarrow$). اگر $f(x) = f_۰ \in R[x]$ باشد آنگاه چون $f(x)$ مقسوم علیه صفر است پس چندجمله‌ای ناصفر $h(x)$ چنان وجود دارد که $h(x)f(x) = ۰$. چون $h(x)$ ناصفر است پس یک ضریب ناصفر مثل h_i در جملات h وجود دارد. حال داریم

$$\begin{gathered} h(x)f(x) = ۰ \ \Rightarrow \\ (h_mx^m + ... + h_۰)r_۰ = ۰ \ \Rightarrow \\ h_ir_۰ = ۰. \end{gathered}$$

در این حالت مسله اثبات می‌شود. اکنون فرض کنیم درجه $f(x)$ مثبت باشد یعنی

$$f(x) = r_nx^n + ... + r_۰$$

که $r_n \neq ۰$. قرار می‌دهیم

$$T = \{g(x) \in R[x] \mid g(x)f(x) = ۰\}.$$

به وضوح T یک ایده‌آل ناصفر از $R[x]$ است (چرا؟). باید نشان دهیم که $T \cap R \neq ۰$. به برهان خلف، فرض کنیم $T \cap R = ۰$. حال فرض کنیم $g(x)$ از کمترین درجه در T باشد

$$g(x) = s_tx^t + ... + s_۰.$$

دقت شود که $s_t \neq ۰$ و $t > ۰$. حال باید $s_tf(x) \neq ۰$ (زیرا فرض کرده‌ایم $T \cap R = ۰$). در نتیجه i چنان وجود دارد که $r_ig(x) \neq ۰$. اکنون فرض کنیم l بزرگترین عدد صحیح و مثبتی باشد که $r_lg(x) \neq ۰$. پس

$$r_{l+۱}g(x) = r_{l+۲}g(x) = ... = r_ng(x) = ۰.$$

در نتیجه داریم

$$۰ = f(x)g(x) = (r_۰ + ... + r_lx^l)g(x).$$

پس $r_۱g_m = ۰$. این نشان می‌دهد که درجه $r_۱g(x)$ کمتر از m است. از طرفی به وضوح $(r_۱g(x))f(x) = ۰$. پس $r_۱g(x) \in T$. اما $r_۱g(x)$ درجه کمتر از m دارد و تناقض با انتخاب ما از $g(x)$ دارد. پس $T \cap R \neq ۰$. لذا $b \in R$ چنان موجود است که $bf = ۰$.
($\Leftarrow$). واضح است. □

تمرین ۲.۳.۲۷. *فرض کنیم R یک دامنه صحیح باشد که میدان نیست. نشان دهید که $R[x]$ یک ایده‌آل دارد که اصلی نیست.*

اثبات. چون R میدان نیست پس عنصر ناصفر $r \in R$ چنان وجود دارد که وارونپذیر نیست. به برهان خلف، فرض کنیم که در $R[x]$ هر ایده‌آل، اصلی است. پس ایده‌آل $< x > + < r >$ باید اصلی باشد یعنی $f(x) \in R[x]$ چنان وجود دارد که $< x > + < r >=< f(x) >$. چون $r \in < f(x) >$ پس $g(x) \in R[x]$ چنان موجود است که $r = g(x)f(x)$. با کمک درجه می‌توان نشان داد که باید $g(x) = g_۰ \in R$ و $f(x) = f_۰ \in R$. از طرفی دیگر $x \in < f(x) >$ پس $h(x) \in R[x]$ چنان موجود است که $x = h(x)f(x) = h(x)f_۰$. حال با کمک درجه ثابت می‌شود که اگر $h(x) = h_m x^m + ... + h_۱x + h_۰$ آنگاه $f_۰h_۱ = ۱$. یعنی $f_۰$ وارونپذیر است پس $R[x] =< f(x) >=< f_۰ >$. یعنی نشان داده‌ایم که $< x > + < r >= R[x]$. چون $۱ \in R[x]$ پس چندجمله‌ای های $u(x), v(x) \in R[x]$ چنان وجود دارند که $u(x)x + v(x)r = ۱$. با کمک درجه می‌توان نشان داد که $u(x) = ۰$ و $v(x) = v_۰ \in R$. یعنی $v_۰r = ۱$ و لذا r وارونپذیر می‌شود که تناقض است. □

تمرین ۲.۳.۲۸. *با یک مثال نشان دهید که شرط دامنه صحیح بودن در قضیه ۲.۳.۲۱ ، قابل حذف نیست.*

اثبات. مطابق با علایم قضیه ۲.۳.۲۱، قرار می‌دهیم $D = E = \mathbb{Z} \times \mathbb{Z}$. می‌دانیم که D دامنه صحیح نیست (چرا؟). چندجمله‌ای $f(x) = (۱, ۰)x$ از درجه یک است که به ازای هر $n \in \mathbb{Z}$ یک ریشه به صورت $x = (۰, n)$ دارد. در نتیجه بیشمار ریشه دارد. □

تمرین ۲.۳.۲۹. *نشان دهید که $۱ + rx$ در $R[x]$ یکال است اگر و تنها اگر $r^m = ۰$ برای $m \in \mathbb{N}$.*

اثبات. ($\Leftarrow$). طبق فرض داریم

$$(۱ + rx)(f_۰ + ... + f_n x^n) = ۱$$

که در نتیجه

$$f_۰ + (f_۱ + rf_۰)x + ... + (f_n + rf_{n-۱})x^n + rf_n x^{n+۱} = ۱.$$

پس $f_۰ = ۱$، $f_۱ = -r$، $f_۲ = r^۲$، $f_۳ = -r^۳$، ...، $f_n = (-۱)^n r^n$ و $rf_n = ۰$. بنابراین $r^{(n+۱)} = ۰$ یعنی $m = n + ۱$.
($\Rightarrow$). قرار دهیم

$$f(x) = ۱ - rx + r^۲x^۲ - r^۳x^۳ + ... + (-۱)^{m-۱}r^{m-۱}x^{m-۱}.$$

بررسی سر راست نشان می‌دهد که $f(x)(۱ + rx) = ۱$. □

تمرین ۳۰.۳.۲. *با یک مثال نشان دهید شرط یکال بودن ضریب پیشرو $g(x)$ در قضیه ۱۶.۳.۲ ، حذف شدنی نیست.*

اثبات. حلقه $\mathbb{Z}_۴[x]$ را در نظر می‌گیریم. قرار دهید $f(x) = x^۲$ و $g(x) = \bar{۲}x$. به وضوح $\bar{۲}$ در $\mathbb{Z}_۴$ یکال نیست. اکنون اگر قضیه ۱۶.۳.۲ ، برای این حلقه بر قرار باشد آنگاه باید داشته باشیم

$$x^۲ = q(x)(\bar{۲}x) + r(x),\ deg(r(x)) < ۱.$$

شرط درجه در بالا ایجاب می‌کند که $r(x) = \bar{r}_۰ \in \mathbb{Z}_۴$. اما شرط $x^۲ = q(x)(\bar{۲}x) + r(x)$ ایجاب می‌کند که

$$\bar{۲}x^۲ = \bar{۲}r(x) = \bar{۲}r_۰.$$

طرف راست تساوی بالا در $\mathbb{Z}_۴$ است اما سمت چپ خیر. این تناقض است. □

تمرین ۳۱.۳.۲. *اگر R یک دامنه صحیح باشد. نشان دهید یکال‌های $R[x]$ در R قرار می‌گیرند.*

اثبات. فرض کنیم $f(x)g(x) = ۱$ و قرار دهیم

$$f(x) = r_۰ + r_۱x + ... + r_nx^n,\ g(x) = s_۰ + s_۱x + ... + s_mx^m.$$

واضح است که $r_ns_m = ۰$. اما ضریب $x^{m+n-۱}$ در $f(x)g(x)$ برابر است با

$$r_{n-۱}s_m + r_ns_{m-۱} = ۰.$$

با ضرب طرفین این تساوی در r_n داریم که $r_n^۲s_{m-۱} = ۰$. اما ضریب $x^{m+n-۲}$ در $f(x)g(x)$ برابر است با $r_{n-۲}s_m + r_{n-۱}s_{m-۱} + r_ns_{m-۲} = ۰$. با ضرب طرفین این تساوی در $r_n^۲$ داریم که $r_n^۳s_{m-۲} = ۰$. روند را استقرایی ادامه دهید. پس $r_n^{m+۱}s_۰ = ۰$. اما $r_۰s_۰ = ۱$ پس $r_n^{m+۱} = ۰$ و چون R دامنه است پس $r_n = ۰$. همین روند نشان می‌دهد که $r_{n-۱}$، ...، $r_۱$ همگی صفر هستند و فقط $r_۰ = f(x)$ که به وضوح یکال و در R است.

□

تمرین ۳۲.۳.۲. *نشان دهید که در حلقه $\mathbb{Z}[x]$ ایده‌آل زیر اول است در حالی که ایده‌آل ماکسیمال نیست.*

$$I = \{f(x) \in \mathbb{Z}[x] \mid f(-۲) = ۰\}.$$

اثبات. با یک بررسی ساده می‌توان نشان داد که رابطه

$$\theta : \mathbb{Z}[x] \longrightarrow \mathbb{Z},\ \theta(f(x)) = f(-۲)$$

یک همریختی حلقه‌ای است. حال داریم. حال اگر $f(-۲) = ۰$ انگاه طبق نتیجه ۲۰.۳.۲ ، داریم که $x + ۲ | f(x)$. این نتیجه می‌دهد که $Ker\theta = I =< x + ۲ >$. همچنین اگر $n \in \mathbb{Z}$ دلخواه باشد آنگاه داریم

$$\theta(x + ۲ + n) = -۲ + ۲ + n = n$$

یعنی θ یک همریختی پوشا است. اکنون طبق قضیه اول یکریختی داریم $\mathbb{Z}[x]/I \cong \mathbb{Z}$. اما $\mathbb{Z}$ دامنه صحیح است پس طبق قضیه ۴.۲.۲ ، I ایده‌آل اول است. برای قسمت دوم؛ اگر I ماکسیمال باشد آنگاه طبق قضیه ۷.۲.۲ ، باید $\mathbb{Z}$ میدان باشد که این تناقضی آشکار است. □

۴.۲ دامنه اقلیدسی

یک کلاس از حلقه‌های مهم در جابجایی دامنه اقلدیسی است. چرا که در این حلقه‌ها مجاز به استفاده ار الگوریتم تقسیم هستیم.

تعریف ۱.۴.۲. *فرض کنیم R یک دامنه صحیح باشد. گوییم R یک دامنه اقلیدسی است هرگاه تابعی مانند $v : R \setminus \{۰\} \longrightarrow \mathbb{N} \cup \{۰\}$ موجود باشد که در شرایط زیر صدق کند.*
(۱) برای هر $a, b \in R \setminus \{۰\}$ داشته باشیم $v(a) \leq v(ab)$.
(۲) برای هر $a, b \in R$ که $b \neq ۰$ عنصرهای q و r از R چنان موجود باشند که $a = bq + r$ و $v(r) < v(b)$ یا $r = ۰$.
به تابع v، تابع ارزیاب اقلیدسی گوییم.

مثال ۲.۴.۲. *حلقه اعداد صحیح، $\mathbb{Z}$، با تابع*

$$v : \mathbb{Z} \setminus \{۰\} \longrightarrow \mathbb{N} \cup \{۰\},\ v(t) = |t|$$

یک دامنه اقلیدسی است.
بررسی خاصیت (۱): فرض کنیم $a, b \in \mathbb{Z} \setminus \{۰\}$. داریم

$$v(a) = |a| \leq |a||b| = |ab| = v(ab).$$

بررسی خاصیت (۲): فرض کنیم $a, b \in \mathbb{Z}$ که $b \neq ۰$. طبق تقسیم معمولی که در $\mathbb{Z}$ وجود دارد عنصرهای q و r از R چنان موجود هستند که $a = bq + r$. اگر $r = ۰$ که چیزی برای اثبات نداریم. اگر $r \neq ۰$ آنگاه واضح است که داریم $r = |r| = v(r) < v(b) = |b| = b$.

مثال ۳.۴.۲. *هر میدان F با تابع*

$$v : F \setminus \{۰\} \longrightarrow \mathbb{N} \cup \{۰\},\ v(a) = ۱$$

یک دامنه اقلیدسی است.
بررسی خاصیت (۱): فرض کنیم $a, b \in F \setminus \{۰\}$. داریم

$$v(a) = ۱ = v(ab).$$

بررسی خاصیت (۲): فرض کنیم $a, b \in F$ که $b \neq ۰$. به وضوح داریم $a = (ab^{-۱})b + ۰$ یعنی $q = ab^{-۱}$ و $r = ۰$ پس $a = bq + r$.

در ادامه می‌خواهیم یک دسته مثال نابدیهی از دامنه اقلیدسی ارائه کنیم. لم زیر را نیاز داریم.

لم ۴.۴.۲. *اگر R دامنه صحیح باشد آنگاه $R[x]$ نیز دامنه صحیح است.*

اثبات. فرض کنیم $R[x]$ دارای مقسوم علیه صفر ناصفر مانند $f(x) = r_n x^n + ... + r_۰$ باشد. طبق تمرین ۲۶.۳.۲، عنصر $۰ \neq b \in R$ چنان وجود دارد که $bf(x) = ۰$. چون $f(x)$ ناصفر است پس باید i چنان موجود باشد که $r_i \neq ۰$. اما $bf(x) = ۰$ پس $br_i = ۰$ یعنی R مقسوم علیه صفر ناصفر دارد و این تناقض است. □

قضیه زیر یک دسته مثال نابدیهی از دامنه اقلیدسی به دست می‌دهد.

قضیه ۵.۴.۲. *فرض کنیم F یک میدان باشد. در این صورت $F[x]$ دامنه اقلیدسی است.*

اثبات. دقت شود که طبق لم ۴.۴.۲، $R = F[x]$ دامنه صحیح است. اکنون تعریف می‌کنیم

$$v : R \setminus \{۰\} \longrightarrow \mathbb{N} \cup \{۰\},\ v(f(x)) = deg(f(x)).$$

به وضوح v یک تابع است. نشان می‌دهیم R یک دامنه اقلیدسی است.
بررسی خاصیت (۱): فرض کنیم $f(x), g(x) \in R \setminus \{۰\}$. قرار می‌دهیم

$$f = r_۰ + ... + r_n x^n \qquad g = s_۰ + ... + s_m x^m$$

که r_n و s_m ناصفرند. در نتیجه ضریب x^{n+m} یعنی $r_n s_m$ در $f(x)g(x)$ ناصفر است. پس داریم $def(f(x)g(x)) = m + n$. بنابراین

$$v(f(x)) = deg(f(x)) = n \leq m + n = deg(f(x)g(x)) = v(f(x)g(x)).$$

بررسی خاصیت (۲): فرض کنیم $f(x), g(x) \in R$ که $g(x) \neq ۰$. طبق قضیه ۱۶.۳.۲، $q(x)$ و $r(x)$ چنان وجود دارند که $f(x) = q(x)g(x) + r(x)$ و در آن $r(x) = ۰$ یا این که داریم $v(r(x)) = deg(r(x)) < deg(g(x)) = v(g)$. □

این بخش را با گزاره زیر به پایان می‌بریم.

گزاره ۶.۴.۲. *فرض کنیم R دامنه اقلیدسی باشد. در این صورت $x \in R$ یکال است اگر و تنها اگر $v(x) = v(۱)$.*

اثبات. ($\Leftarrow$). فرض کنیم $xs = ۱$ برای $s \in R$. چون x یکال است پس s و x هر دو ناصفرند. حال طبق خاصیت (۱) داریم $v(x) \leq v(xs) = v(۱)$. از طرفی دوباره طبق خاصیت (۱) داریم

$$v(۱) = v(xs) \leq v((xs)x) = v(xsx) = v(x).$$

پس $v(x) = v(۱)$.
($\Rightarrow$). طبق خاصیت (۲)، q و r چنان وجود دارند به طوری که $xq + r = ۱$ به علاوه $r = ۰$ یا $v(r) < v(x)$. حال نشان می‌دهیم که $r = ۰$. به برهان خلف، اگر $r \neq ۰$ آنگاه با کمک فرض و خاصیت (۱) داریم

$$v(r) < v(x) = v(۱) \leq v(۱r) = v(r).$$

این تناقض است پس $r = ۰$ و در نتیجه $xq = ۱$ یعنی x یکال است. □

تمرین حل شده

تمرین ۷.۴.۲. *فرض کنیم* $R = \mathbb{Z}[i] = \{a + ib \mid a, b \in \mathbb{Z}\}$ *. نشان دهید* R *با رابطه*

$$v : R \setminus \{۰\} \longrightarrow \mathbb{N} \cup \{۰\},\ v(a + ib) = a^۲ + b^۲$$

یک دامنه اقلیدسی است.

اثبات. به وضوح v تابع است.
بررسی خاصیت (۱): فرض کنیم $a + ib, c + id \in R \setminus \{۰\}$. داریم

$$\begin{gathered} v((a + ib)(c + id)) = \\ v(ac - bd + i(bc + ad)) = \\ (ac - bd)^۲ + (bc + ad)^۲ = \\ (a^۲ + b^۲)(c^۲ + d^۲) = \\ v(a + ib)v(c + id). \end{gathered}$$

حال چون $c + id$ ناصفر است پس به وضوح $v(c + id)$ عدد ناصفر مثبت است پس طبق رابطه بالا داریم

$$v(a + ib) \leq v(a + ib)v(c + id) = v((a + ib)(c + id)).$$

بررسی خاصیت (۲): فرض کنیم $a + ib, c + id \in R$ که $c + id \neq ۰$. می‌توان اعداد گویایی مانند x و y چنان یافت که

$$(a + ib)(c + id)^{-۱} = x + iy.$$

از طرفی می‌توان اعداد صحیحی مانند n و m به گونه‌ای یافت که

$$|x - n| \leq \frac{۱}{۲},\ |y - m| \leq \frac{۱}{۲}.$$

حال داریم

$$\begin{gathered} a + ib = (c + id)(x + iy) = \\ (c + id)[(x - n) + n + i(y - m) + im] = \\ (c + id)(n + im) + (c + id)(x - n) + (c + id)i(y - m). \end{gathered}$$

با توجه به بالا کافی است که قرار دهیم

$$q = n + im,\ \ r = (c + id)(x - n) + (c + id)i(y - m).$$

دقت شود که q و r در R هستند (چرا؟). فقط مانده نشان دهیم $v(r) < v(c + id)$. داریم

$$\begin{gathered} v(r) = v((c + id)(x - n) + (c + id)i(y - m)) = \\ v((c + id)[(x - n) + i(y - m)]) = \\ v(c + id)v((x - n) + i(y - m)) = \\ v(c + id)[(x - n)^۲ + (y - m)^۲] \leq \\ v(c + id)[\tfrac{۱}{۴} + \tfrac{۱}{۴}] = \\ \tfrac{۱}{۲}v(c + id) < v(c + id) \end{gathered}$$

و اثبات تمام است. □

تمرین ۸.۴.۲. *فرض کنیم R دامنه اقلیدسی باشد. اگر $0 \neq b \in R$ وارونپذیر باشد و $x = by$ آنگاه $v(x) = v(y)$.*

اثبات. طبق خاصیت (۱) داریم که

$$v(y) \leq v(by) = v(x).$$

از طرفی $y = b^{-1}x$ پس به طریق مشابه $v(x) \leq v(y)$. اثبات کامل است. □

تمرین ۹.۴.۲. *فرض کنیم R دامنه اقلیدسی باشد. اگر $0 \neq a \in R$ و برای یک $u \in R$ داشته باشیم $a = bu$ و $v(a) = v(b)$ آنگاه عنصر u یکال است.*

اثبات. دقت شود که چون R دامنه است و a صفر نیست، $a = bu$ نتیجه می‌دهد که $b \neq 0$. حال طبق خاصیت (۲) داریم $b = aq + r$ که $r = 0$ یا $v(r) < v(a)$. می‌خواهیم نشان دهیم $r = 0$. به برهان خلف اگر $r \neq 0$ آنگاه باید $v(r) < v(a)$ رخ دهد. اما $a = bu$ پس

$$b = aq + r = buq + r \;\Rightarrow\; (1 - uq)b = r$$

و طبق خاصیت (۱) و فرض داریم که

$$v(b) \leq v((1 - uq)b) = v(r) < v(a) = v(b)$$

که یک تناقض است پس $r = 0$ است. یعنی $b = aq$. پس $b = buq$ یعنی $b(1 - uq) = 0$. اما R دامنه و b ناصفر است پس $uq = 1$ یعنی u یکال است و اثبات کامل است. □

تمرین ۱۰.۴.۲. *فرض کنیم R دامنه اقلیدسی با تابع ارزیاب اقلیدسی v باشد. به علاوه فرض کنیم n یک عدد صحیح باشد که $v(1) + n \geq 0$. نشان دهید رابطه زیر نیز یک تابع ارزیاب اقلیدسی دیگر برای R است*

$$v_n : R \setminus \{0\} \longrightarrow \mathbb{N} \cup \{0\},\ v_n(x) = v(x) + n.$$

اثبات. اول باید نشان دهیم v_n خوشتعریف است. فرض کنیم $x \in R$ ناصفر باشد. چون v تابع ارزیاب اقلیدسی است طبق خاصیت (۱) برای v و فرض داریم

$$v_n(x) = v(x) + n = v(1x) + n \geq v(1) + n \geq 0.$$

پس $v_n(x) \in \mathbb{N} \cup \{0\}$.
اگر $x = y$ پس به وضوح $v(x) = v(y)$ در نتیجه $v(x)+n = v(y)+n$ یعنی $v_n(x) = v_n(y)$.
پس v_n خوشتعریف است.
بررسی خاصیت (۱): فرض کنیم $x, y \in R \setminus \{0\}$. با خاصیت (۱) برای v داریم

$$v_n(xy) = v(xy) + n \geq v(x) + n = v_n(x).$$

بررسی خاصیت (۲): فرض کنیم $x, y \in R$ که $y \neq 0$. طبق قضیه خاصیت (۲) برای v، داریم q و r چنان وجود دارند که $x = qy + r$ که در آن $r = 0$ یا $v(r) < v(y)$. اگر $r = 0$ چیزی برای ادامه وجود ندارد. اگر $v(r) < v(y)$ آنگاه $v(r) + n < v(y) + n$ یعنی $v_n(r) < v_n(y)$ و اثبات کامل است. □

۵.۲ دامنه ایده‌آل اصلی

دسته مهم دیگری از حلقه‌های جابجایی دامنه‌های ایده‌آل اصلی هستند که نقش مهمی در نظریه مدول و نظریه اعداد ایفا می‌کنند.

تعریف ۱.۵.۲. *اگر هر ایده‌آل حلقه R اصلی باشد به R حلقه ایده‌آل اصلی گوییم. اگر R دامنه باشد و هر ایده‌آل آن اصلی باشد به R دامنه ایده‌آل اصلی گوییم.*

مثال ۲.۵.۲. *$\mathbb{Z}$ یک دامنه ایده‌آل اصلی است. $\mathbb{Z}_4$ یک حلقه ایده‌آل اصلی است که دامنه نیست.*

قضیه زیر یک دسته مثال غیر بدیهی برای دامنه ایده‌آل اصلی ارائه می‌کند.

قضیه ۳.۵.۲. *هر دامنه اقلیدسی R یک دامنه ایده‌آل اصلی است.*

اثبات. فرض کنیم I ایده‌آل R باشد. اگر I صفر باشد به وضوح ایده‌آل اصلی است. پس فرض کنیم I ناصفر باشد. قرار دهیم

$$T = \{v(x) \mid x \in I\}.$$

دقت شود که T ناتهی است زیرا I ناصفر است. از طرفی T زیرمجموعه اعداد صحیح مثبت است پس طبق اصل خوشترتیبی عضو مینیمم مانند $v(y)$ دارد که y عضو I و ناصفر است. ادعا می‌کنیم $I = Ry$. چون I ایده‌آل است و $y \in I$ پس به وضوح $Ry \subseteq I$. حال فرض کنیم $u \in I$. پس q و r در R چنان وجود دارد که $u = qy + r$ و در آن $r = 0$ یا $v(r) < v(y)$. نشان می‌دهیم $r = 0$ است. به برهان خلف اگر $r \neq 0$ آنگاه باید $v(r) < v(y)$ رخ دهد. اما $r = u - qy$ پس $r \in I$ پس $v(r) \in T$. اما $v(r) < v(y)$ که مینیمم بودن $v(y)$ را نقض می‌کند. در نتیجه $r = 0$ و $u = qy$. بنابراین $u \in Ry$ که این اثبات را کامل می‌کند. □

تذکر ۴.۵.۲. *قضیه ۳.۵.۲، این سوال طبیعی را به ذهن می‌رساند که آیا هر دامنه ایده‌آل اصلی نیز یک دامنه اقلیدسی است؟ جواب این سوال منفی است! اما برای اطلاع خواننده باید ذکر کنیم با محاسبات طولانی در سال ۱۹۷۳ ویلسون در مقاله‌ای نشان داد که حلقه*

$$\mathbb{Z}[\sqrt{-19}] = \{a + b\sqrt{-19} \mid a, b \in \mathbb{Z}, \text{ هر دو زوج یا هر دو فرد } a \text{ و } b\}$$

یک دامنه ایده‌آل اصلی است که دامنه اقلیدسی نیست.

در ادامه برای دسته خاصی از حلقه‌ها نشان می‌دهیم که دامنه ایده‌آل اصلی بودن با دامنه اقلیدسی بودن یکی است. این قضیه جواب مثبت تحت شرایطی خاص به تذکر ۴.۵.۲، می‌دهد.

قضیه ۵.۵.۲. *موارد زیر برای حلقه R معادل است.*
(۱) *R میدان است.*
(۲) *$R[x]$ دامنه اقلیدسی است.*
(۳) *$R[x]$ یک دامنه ایده‌آل اصلی است.*

اثبات. (۱) $\Leftarrow$ (۲). این همان قضیه ۵.۴.۲ است.
(۲) $\Leftarrow$ (۳). این همان قضیه ۳.۵.۲ است.
(۳) $\Leftarrow$ (۱). طبق فرض $R[x]$ دامنه است پس به وضوح R دامنه است. حال به برهان خلف فرض کنیم R میدان نیست. پس طبق تمرین ۲۷.۳.۲، $R[x]$ دامنه ایده‌آل اصلی نیست و این تناقض است. □

نتیجه ۶.۵.۲. *حلقه $\mathbb{Z}[x]$ دامنه ایده‌آل اصلی نیست.*

اثبات. از قضیه ۵.۵.۲ بدیهی است. □

تمرین حل شده

تمرین ۷.۵.۲. *فرض کنیم I یک ایده‌آل سره در دامنه ایده‌آل اصلی R باشد که $I^۲ = I$. آنگاه I برابر صفر است.*

اثبات. چون R دامنه ایده‌آل اصلی است پس $x \in I$ چنان وجود دارد که $I = Rx =< x >$. حال فرض کنیم $y \in I^۲$. پس $y = \sum_{j=۱}^{t} u_j v_j$ که برای هر j، $u_j, v_j \in I$. حال برای هر j عناصر r_j و s_j چنان وجود دارد که $u_j = r_j x$ و $v_j = s_j x$. پس $y = \sum_{j=۱}^{t} r_j s_j x^۲ = (\sum_{j=۱}^{t} r_j s_j)x^۲$. یعنی نشان داده‌ایم $I^۲ = Rx^۲ =< x^۲ >$. پس عنصر $r \in R$ چنان وجود دارد که $x = rx^۲$. پس $x(۱ - rx) = ۰$. چون R دامنه است پس $x = ۰$ یا $rx = ۱$. اگر $rx = ۱$ باشد آنگاه x وارونپذیر است و $I = R$ که تناقض است. در نتیجه $x = ۰$ و بنابراین $I = ۰$ است. □

تمرین ۸.۵.۲. *فرض کنیم R یک دامنه ایده‌آل اصلی باشد. اگر P و Q دو ایده‌آل اول باشد که در شرط $P \subset Q$ صدق کنند آنگاه $P = ۰$ و Q ایده‌آل ماکسیمال است.*

اثبات. می‌دانیم که p و q چنان وجود دارند که $P = Rp$ و $Q = Rq$. حال فرض کنیم Q ماکسیمال نباشد (برهان خلف) پس ایده‌آل Rx چنان وجود دارد که $Rp \subset Rq \subset Rx \subset R$. اما t چنان وجود دارد که $tx = q$. پس $tx \in Q$ و چون $x \notin Q$ نتیجه می‌شود که $t \in Q$. بنابراین s چنان وجود دارد که $sq = t$. لذا $sxq = q$. یعنی $q(sx - ۱) = ۰$. چون R دامنه است پس $q = ۰$ یا $sx = ۱$. اگر $q = ۰$ آنگاه $P = Q = ۰$ که تناقض است. پس $sx = ۱$ و این یعنی x یکال است. لذا $Rx = R$ که تناقض است. پس باید Q ماکسیمال باشد.
حال فرض کنیم $P \neq ۰$ (برهان خلف). پس $۰ \subset Rp \subset Rq$. اما t چنان وجود دارد که $tq = p$. پس $tq \in P$ و چون $q \notin P$ نتیجه می‌شود که $t \in P$. بنابراین s چنان وجود دارد که $sp = t$. لذا $spq = p$. یعنی $p(sq - ۱) = ۰$. چون R دامنه است پس $p = ۰$ یا $sx = ۱$. اگر $p = ۰$ آنگاه $P = ۰$ که تناقض است. پس $sq = ۱$ و این یعنی q یکال است. لذا $Rq = Q = R$ که تناقض است. □

تمرین ۹.۵.۲. *فرض کنیم R یک دامنه باشد به طوری که تعداد متناهی ایده‌آل قابل مقایسه با رابطه شمول دارد. نشان دهید R دامنه ایده‌آل اصلی است.*

اثبات. فرض کنیم I یک ایده‌آل سره R باشد. کافی است نشان دهیم I اصلی است. اگر I صفر باشد چیزی برای اثبات نداریم. فرض کنیم I ناصفر باشد. پس عنصر ناصفر x_1 در I وجود دارد. اگر $I =< x_1 >$ که کار تمام است. پس باید $< x_1 > \subset I$. حال $x_2 \in I \setminus < x_1 >$ را در نظر بگرید. اگر $I =< x_2 >$ که کار تمام است. پس باید $< x_2 > \subset I$. اما طبق فرض $< x_1 >$ و $< x_2 >$ قابل مقایسه هستند پس $< x_2 > \subseteq < x_1 >$ یا $< x_1 > \subseteq < x_2 >$. واضح است که $< x_1 > \subseteq < x_2>$ رخ نمی‌دهد. پس $< x_2 > \subset < x_1 >$. حال این روند را ادامه می‌دهیم چون تعداد ایده‌آل‌های R متناهی است پس باید روند متوقف شود و این روند زمانی ایستا است که عنصر x_n موجود باشد که $I = Rx_n =< x_n >$. پس هر ایده‌آل R اصلی است و چون R دامنه است پس R یک دامنه ایده‌آل اصلی است. □

۶.۲ دامنه تجزیه یکتا

این بخش تعمیمی از مفهوم تجزیه به اعداد اول در حلقه $\mathbb{Z}$ و قضیه اساسی حساب است. این بخش اهمیت ویژه‌ای در نظریه اعداد دارد. در ابتدا مفاهیم مقسوم، مقسوم علیه، اول، شریک و ... را تعریف می‌کنیم که ایده اصلی آن در همان حلقه $\mathbb{Z}$ است.

تعریف ۱.۶.۲. *فرض کنیم a و b عناصری از حلقه R باشند که $b \neq 0$. گوییم b یک مقسوم علیه a است (یا b، a را می‌شمارد یا a مضربی از b است یا b، a را عاد می‌کند) هرگاه عنصر c از R موجود باشد که $a = bc$. این مفهوم را با $b|a$ نشان می‌دهیم.*

مثال ۲.۶.۲. *در هر حلقه R برای هر عنصر ناصفر $a \in R$ همواره داریم $0|a$.*

مثال ۳.۶.۲. *در حلقه $\mathbb{Z}_4$ چون $\bar{3}\bar{3} = \bar{2}$ پس $\bar{3}|\bar{2}$. اما واضح است که $\bar{3} \nmid \bar{2}$.*

مثال ۴.۶.۲. *اگر u عنصری یکال در حلقه R باشد آنگاه چون برای هر $a \in R$ رابطه $a = u(u^{-1}a)$ برقرار است پس $u|a$.*

گزاره ۵.۶.۲. *در حلقه R عنصر ناصفر x یکال است اگر و تنها اگر x یک مقسوم علیه ۱ باشد.*

اثبات. ($\Leftarrow$). چون x یکال است پس $xy = 1$ که $y \in R$. پس طبق تعریف $1|x$.
($\Rightarrow$). فرض کنیم $1|x$. پس $y \in R$ چنان وجود دارد که $xy = 1$. یعنی x یکال است. □

تعریف ۶.۶.۲. *دو عنصر a و b را در حلقه R شریک گوییم هرگاه عنصر یکالی مانند u در R موجود باشد که $a = bu$.*

مثال ۷.۶.۲. *در حلقه $\mathbb{Z}_6$ داریم که $\bar{2}\bar{5} = \bar{4}$. پس $\bar{2}$ و $\bar{4}$ شریک هستند.*

گزاره ۸.۶.۲. *در دامنه صحیح R دو عنصر ناصفر x و y شریک هستند اگر و تنها اگر $x|y$ و $y|x$.*

اثبات. ($\Leftarrow$). طبق فرض عنصر یکال u وجود دارد که $x = yu$ در نتیجه $y|x$. اما داریم $y = xu^{-1}$ پس $x|y$.
($\Rightarrow$). طبق فرض عناصر u و v چنان وجود دارد که $x = yu$ و $y = xv$. پس $x = xvu$. در نتیجه $x(1 - vu) = 0$. چون R دامنه صحیح است و x ناصفر است پس $vu = 1$. یعنی u و v یکال هستند پس x و y شریک هستند. □

تعریف ۹.۶.۲. *عنصر ناصفر a در حلقه R را تحویل ناپذیر گوییم هرگاه شرایط زیر برقرار باشد.*
(۱) a یکال نباشد.
(۲) اگر $a = bc$ که $b, c \in R$ آنگاه b یا c یکال باشند.

مثال ۱۰.۶.۲. *در حلقه $\mathbb{R}[x]$ عنصر $x^۲+۱$ تحویل ناپذیر است. زیرا واضح است که این عنصر وارونپذیر نیست و اگر $x^۲+۱=f(x)g(x)$ با کمک درجه $f(x)$ یا $g(x)$ باید یکال باشند.*

تعریف ۱۱.۶.۲. *عنصر ناصفر p در حلقه R را اول گوییم هرگاه شرایط زیر بر قرار باشد.*
(۱) *p یکال نباشد.*
(۲) *به ازای هر a و b اگر $p|ab$ آنگاه $p|a$ یا $p|b$.*

مثال ۱۲.۶.۲. *در حلقه $\mathbb{Z}_۶$ عنصر $\bar۲$ اول است زیر واضح است که این عنصر یکال نیست و اگر $\bar۲|\bar{a}\bar{b}$ آنگاه عنصر $\bar{x}$ چنان وجود دارد که $\bar{a}\bar{b}=\bar۲\bar{x}$. پس این تساوی در حلقه $\mathbb{Z}$ به صورت $ab=۲x+۶k$ است. یعنی $۲|ab$ پس $۲|a$ یا $۲|b$ در نتیجه $\bar۲|\bar{a}$ یا $\bar۲|\bar{b}$.*

حال لم زیر را داریم.

لم ۱۳.۶.۲. *هر عنصر اول p در دامنه صحیح R تحویل ناپذیر است.*

اثبات. شرط اول بر قرار است و p یکال نیست. فرض کنیم $p=ab$ در نتیجه $p|a$ یا $p|b$. اگر $p|a$ آنگاه عنصر x چنان وجود دارد که $a=px$. در نتیجه $p=ab=pxb$. پس $p(۱-xb)=۰$. چون R دامنه است و p ناصفر پس $xb=۱$ یعنی b یکال است. □

تذکر ۱۴.۶.۲. *در لم ۱۳.۶.۲، شرط دامنه لازم است. در حلقه $\mathbb{Z}_۶$ عنصر $\bar۲$ اول است (مثال ۱۲.۶.۲ را ببینید) در حالی که $\bar۴\bar۲=\bar۲$ که نه $\bar۲$ و نه $\bar۴$ یکال نیستند.*

تذکر ۱۵.۶.۲. *لم ۱۳.۶.۲، این سوال طبیعی را به ذهن می‌رساند که آیا هر تحویل ناپذیری در دامنه صحیح اول است؟ جواب به این سوال منفی است (تمرین ۲۳.۱۰.۲). اما قضیه زیر پاسخ مثبت تحت شرایط خاصی به سوال بالا می‌دهد.*

قضیه ۱۶.۶.۲. *در هر حلقه ایده‌آل اصلی R، هر عنصر تحویل ناپذیر اول است.*

اثبات. فرض کنیم $p\in R$ عنصر تحویل ناپذیر باشد و $p|ab$. بدون کم شدن از کلیت می‌توان فرض کرد که $p\nmid a$. طبق فرض عنصر $c\in R$ چنان وجود دارد که $Rp+Ra=Rc$. پس $p\in Rc$ و در نتیجه $d\in R$ چنان وجود دارد که $p=dc$. بنابراین d یا c باید یکال باشد. اگر d یکال باشد آنگاه $c=d^{-۱}p$ و در نتیجه $c\in Rp$. بنابراین $Rc=Rp$. پس $a\in Rp$ و این یعنی عنصر x چنان وجود دارد که $a=xp$ و لذا $p|a$ که تناقض است. بنابراین باید c یکال باشد و $Rc=R$. در نتیجه $Rp+Ra=R$. پس عناصر x و y چنان وجود دارد که $xp+ya=۱$. لذا $xbp+yba=b$. چون $p|ab$ و $p|xbp$ پس $p|b$ و اثبات کامل است. □

نتیجه ۱۷.۶.۲. *در هر دامنه ایده‌آل اصلی R، $p\in R$ اول است اگر و تنها اگر تحویل ناپذیر باشد.*

اثبات. قضیه ۱۶.۶.۲ و لم ۱۳.۶.۲ را به کار ببندید. □

اکنون آمادگی لازم را داریم تا تعریف اصلی این بخش را بیان کنیم.

تعریف ۱۸.۶.۲. *فرض کنیم R یک دامنه صحیح باشد. گوییم R یک دامنه تجزیه یکتا است هرگاه شرایط زیر بر قرار باشد.*
(۱) هر عنصر ناصفر و ناوارون از R حاصل ضرب متناهی از تحویل ناپذیرها باشد.
(۲) هر عنصر تحویل ناپذیر اول باشد.

مثال ۱۹.۶.۲. *حلقه $\mathbb{Z}$ یک دامنه تجزیه یکتا است. زیرا طبق نتیجه ۱۷.۶.۲، هر عنصر تحویل ناپذیر اول است. و طبق قضیه اساسی حساب هر عنصر ناصفر و ناوارون حاصل ضربی از اول‌ها است. دقت شود که طبق لم ۱۳.۶.۲، هر اول تحویل ناپذیر است.*

قضیه بعدی یک دسته مثال در اختیار ما قرار می‌دهد. ولی برای بیان قضیه لم زیر نیاز است.

لم ۲۰.۶.۲. *در دامنه ایده‌آل اصلی R زنجیر نامتناهی و سره از ایده‌آل‌های افزایشی وجود ندارد.*

اثبات. ابتدا دقت کنید که همه ایده‌آل‌ها اصلی هستند. حال زنجیر افزایشی و سره ایده‌آل‌ها در R را در نظر بگیرید

$$Rx_1 \subset Rx_2 \subset Rx_3 \cdots .$$

اکنون قرار می‌دهیم $I = \cup_{i=1}^{\infty} Rx_i$. بررسی سر راست نشان می‌دهد که I ایده‌آل R است. پس عنصر x چنان وجود دارد که $I = Rx$. چون $x \in I$ پس اندیس k چنان وجود دارد که $x \in Rx_k$. پس $I = Rx \subseteq Rx_k \subseteq I$. پس $I = Rx = Rx_k$ و در نتیجه

$$Rx_k = Rx_{k+1} = R_{k+2} = \cdots .$$

یعنی زنجیر نامتناهی و سره از ایده‌آل‌های افزایشی در R وجود ندارد. □

اکنون به وعده خود عمل می‌کنیم.

قضیه ۲۱.۶.۲. *هر دامنه ایده‌آل اصلی R یک دامنه تجزیه یکتا است.*

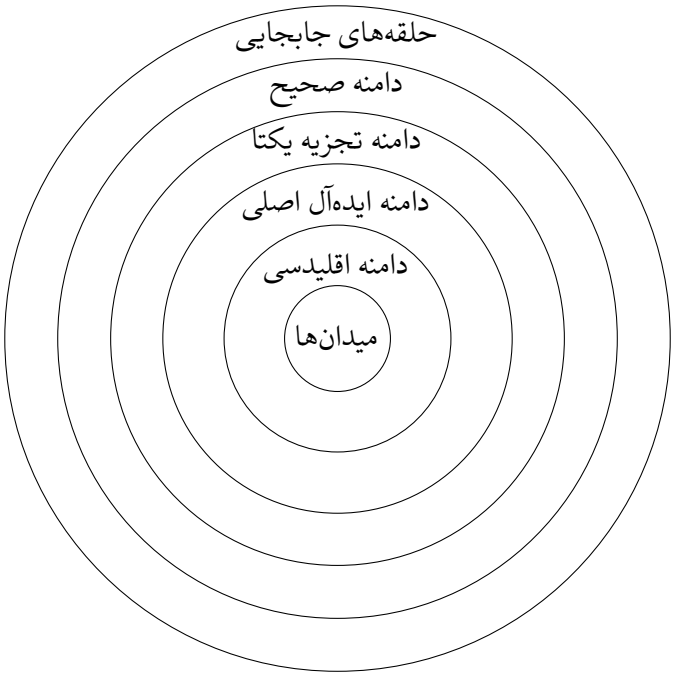
اثبات. ابتدا دقت کنید که طبق نتیجه ۱۷.۶.۲، خاصیت (۲) بر قرار است. حال فرض کنیم $x \in R$. اگر x تحویل ناپذیر باشد کار تمام است. پس فرض کنیم x تحویل ناپذیر نباشد. پس $x = ab$ که $a, b \in R$ و هر دو ناوارون هستند. اگر a و b هر دو حاصل ضرب تعداد متناهی عنصر تحویل ناپذیر باشند آنگاه کار تمام است. پس بدون کم شدن از کلیت فرض کنیم که b حاصل ضرب تعداد متناهی عنصر تحویل ناپذیر نباشند. پس خود b هم تحویل ناپذیر نیست و این یعنی $b = cd$ که $c, d \in R$ و هر دو ناوارون هستند. بدون کم شدن از کلیت فرض کنیم که d حاصل ضرب تعداد متناهی عنصر تحویل ناپذیر نباشند. فرآیند بالا را همین طور استقرایی ادامه می‌دهیم پس می‌توانیم زنجیر نامتناهی و سره از ایده‌آل‌های افزایشی

$$(x) \subset (b) \subset (d) \cdots$$

در R بسازییم که این با لم ۲۰.۶.۲، در تناقض است. بنابراین x حاصل ضربی متناهی از عناصر تحویل ناپذیر است. □

تذکر ۲.۶.۲۲. *قضیه ۲.۶.۲۱ ، این سوال طبیعی را به ذهن می‌رساند که آیا هر دامنه تجزیه یکتا یک دامنه ایده‌آل اصلی است؟ جواب این سوال منفی است. چرا که طبق قضیه‌ای که بعدا خواهیم گفت (قضیه ۲.۶.۳۴) حلقه $\mathbb{Z}[x]$ یک دامنه تجزیه یکتا است در حالی که طبق نتیجه ۲.۶.۵، $\mathbb{Z}[x]$ دامنه ایده‌آل اصلی نیست.*

برای شهود بهتر و دیدن مطالبی که تا اینجا از نظریه حلقه جابجایی آموخته‌اید نمودار زیر کار ساز است.



در قضیه زیر یک تعریف معادل برای دامنه تجزیه یکتا اثبات می‌کنیم که در پاره‌ای از مواقع این تعریف معادل برای تعریف دامنه تجزیه یکتا در نظر گرفته می‌شود و تعریف قدیمی تحت قضیه‌ای اثبات می‌گردد.

قضیه ۲.۶.۲۳. *فرض کنیم R یک دامنه صحیح باشد. در این صورت R دامنه تجزیه یکتا است اگر و تنها اگر هر عنصر ناصفر x حاصل ضرب متناهی از یک عنصر یکال u و عناصر تحویل ناپذیر $p_1, \dots, p_n$ که $n \geq 0$ باشد (یعنی $x = up_1p_2 \dots p_n$) و به علاوه این نمایش به معنی زیر منحصر به فرد است؛ اگر x دارای نمایشی دیگر مانند $wq_1q_2 \dots q_m$ که w یکال و q_iها تحویل ناپذیرند، باشد آنگاه $m = n$ و هر p_i با یک q_j شریک است (این منحصر به فردی، با تقریب شریک بودن منحصر به فرد نیز نامیده می‌شود).*

اثبات. ($\Leftarrow$). فرض کنیم x یک عنصر ناصفر باشد. اگر x یکال باشد چیزی برای اثبات نداریم در واقع $n = 0$. پس فرض کنیم x نایکال باشد. طبق تعریف دامنه تجزیه یکتا، خاصیت (۱)، x حاصل ضربی متناهی از عناصر تحویل ناپذیر است یعنی $x = p_1p_2 \dots p_n$ که در آن $u = 1$.

حال نشان می‌دهیم که این نمایش با تقریب شریک بودن منحصر به فرد است. پس فرض کنیم $wq_1q_2...q_m = x = up_1p_2...p_n$ که u و w یکال و p_iها، q_jها تحویل ناپذیرند. نشان می‌دهیم $m = n$. فرض کنیم $m > n$ باشد (دو عدد صحیح که مساوی نیستند بلاخره یکی از آن دیگری کمتر است). طبق تعریف دامنه تجزیه یکتا، خاصیت (۲)، p_iها اول هستند. اما داریم

$$p_1|up_1p_2...p_n = wq_1q_2...q_m \Rightarrow p_1|wq_1q_2...q_m.$$

پس باید اندیس j چنان باشد که $p_1|q_j$ (چرا؟). بدون کم شدن کلیت می‌توان فرض کرد $j = 1$ زیرا اگر لازم باشد اندیس‌ها را تغییر می‌دهیم. یعنی $p_1|q_1$. پس y_1 چنان وجود دارد که $q_1 = p_1y_1$. چون q_1 تحویل ناپذیر است پس باید y_1 یکال باشد (چرا؟). حال داریم

$$up_1p_2...p_n = wp_1y_1q_2...q_m.$$

پس $p_1[(up_2...p_n) - (wy_1q_2...q_m)] = 0$. چون R دامنه صحیح و p_1 ناصفر است باید $up_2...p_n = wy_1q_2...q_m$.
اما داریم

$$p_2|up_2p_3...p_n = wy_1q_2...q_m \Rightarrow p_2|wy_1q_2...q_m.$$

پس باید اندیس j چنان باشد که $p_2|q_j$ (چرا؟). بدون کم شدن کلیت می‌توان فرض کرد $j = 2$ زیرا اگر لازم باشد اندیس‌ها را تغییر می‌دهیم. یعنی $p_2|q_2$. پس y_2 چنان وجود دارد که $q_2 = p_2y_2$. چون q_2 تحویل ناپذیر است پس باید y_2 یکال باشد (چرا؟). حال داریم

$$up_2p_3...p_n = wy_1p_2y_2q_3...q_m.$$

پس $p_2[(up_3...p_n) - (wy_1y_2q_3...q_m)] = 0$. چون R دامنه صحیح و p_2 ناصفر است باید $up_3...p_n = wy_1y_2q_3...q_m$. این روند را ادامه می‌دهیم پس بعد از n مرحله داریم

$$u = wy_1y_2...y_nq_{n+1}...q_m.$$

چون u یکال است باید q_{n+1}، ...، q_m یکال باشند (چرا؟) و این تناقض با تحویل ناپذیر بودن q_iها است پس $n = m$. یعنی نشان داده‌ایم

$$wq_1q_2...q_n = x = up_1p_2...p_n.$$

حال نشان می‌دهیم که p_i با یک q_j شریک است. چون $p_i|wq_1q_2...q_n$ پس پس باید اندیس j چنان باشد که $p_i|q_j$ (چرا؟). پس y_i چنان وجود دارد که $q_j = p_iy_i$. چون q_j تحویل ناپذیر است پس باید y_j یکال باشد (چرا؟) و این یعنی p_i و q_j شریک هستند.
($\Rightarrow$). واضح است که خاصیت (۱) تعریف دامنه تجزیه یکتا بر قرار است و فقط باید خاصیت (۲)، هر تحویل ناپذیری اول است، را نشان دهیم. فرض کنیم p عنصر تحویل ناپذیر باشد و $p|xy$. پس عنصر a چنان موجود است که $xy = pa$. طبق فرض x، y و a دارای تجزیه زیر هستند

$$x = u_1p_1...p_n,\ y = u_2q_1...q_m,\ a = u_3r_1...r_t$$

که در آن p_iها، q_jها و r_lها تحویل ناپذیر و $u_۱$، $u_۲$ و $u_۳$ یکال هستند. پس داریم

$$u_۱p_۱...p_nu_۲q_۱...q_m = pu_۳r_۱...r_t.$$

بنا به فرض p باید شریک یکی از p_i ها یا q_j ها باشد. اگر p شریک p_i باشد آنگاه عنصر یکال v_i چنان موجود است که $pv_i = p_i$. یعنی $p|p_i|x$. لذا $p|x$. به صورت مشابه اگر p با یک q_j شریک باشد آنگاه $p|y$. بنابراین p اول است. □

برای بیان دو قضیه اساسی دیگر نیاز به مقدمات زیر است. قضیه اول بیان می‌کند که در هر دامنه تجزیه یکتا بزرگترین مقسوم علیه مشترک وجود دارد و قضیه دوم این مطلب را نشان می‌دهد که اگر R یک دامنه تجزیه یکتا باشد آنگاه $R[x]$ نیز یک دامنه تجزیه یکتا است.

تعریف ۲.۶.۲۴. *فرض کنیم $a_۱$، ...، a_n عناصر در حلقه R باشند که همگی صفر نیستند. عنصر ناصفر d را مقسوم علیه مشترک گوییم هرگاه برای هر i، $d|a_i$.*
به مقسوم علیه مشترک d، بزرگترین مقسوم علیه مشترک گوییم هرگاه برای هر i و عنصر ناصفر c داشته باشیم $c|a_i$ نتیجه شود $c|d$.
اگر $d = ۱$ باشد آنگاه عناصر $a_۱$، ...، a_n را نسبت به هم اول گوییم.

مثال ۲.۶.۲۵. *حلقه $\mathbb{Z}_{۱۰}$ را در نظر بگیرید. داریم که $\bar{۶}\bar{۴} = \bar{۴}$ و $\bar{۴}\bar{۴} = \bar{۶}$. پس برای $\bar{۴}$ و $\bar{۶}$ عنصر $\bar{۴}$ یک مقسوم علیه مشترک است. واضح است که $\bar{۶}$ هم یک مقسوم علیه مشترک است. اما داریم $\bar{۹}\bar{۴} = \bar{۶}$ و $\bar{۹}$ یکال است پس برای $\bar{۴}$ و $\bar{۶}$ عنصر $\bar{۴}$ و $\bar{۶}$ هر دو بزرگترین مقسوم علیه مشترک هستند. این مثال نشان می‌دهد که بزرگترین مقسوم علیه مشترک ممکن است یکتا نباشد.*

تذکر ۲.۶.۲۶. *بزرگترین مقسوم علیه مشترک گاهی اصلا وجود ندارد! برای مثال تمرین ۲.۶.۳۹ را ببینید.*

قضیه زیر تضمین می‌کند در دامنه تجزیه یکتا همیشه بزرگترین مقسوم علیه مشترک وجود دارد.

قضیه ۲.۶.۲۷. *فرض کنیم R یک دامنه تجزیه یکتا باشد. در این صورت بزرگترین مقسوم علیه مشترک عناصر ناصفر a و b وجود دارد. به علاوه بزرگترین مقسوم علیه مشترک تحت شریک بودن منحصر به فرد است.*

اثبات. طبق قضیه ۲.۶.۲۳، می‌توانیم a و b را به شکل زیر بنویسیم (چرا؟)

$$a = p_۱^{e_۱}...p_n^{e_n},\ b = p_۱^{f_۱}...p_n^{f_n}.$$

دقت شود p_i ها تحویل ناپذیر و e_i و f_i اعداد صحیح نامنفی هستند و منظور از $p_i^۰$ یک یکال است. قرار می‌دهیم $g_i = min\{e_i, f_i\}$ و $d = p_۱^{g_۱}...p_n^{g_n}$. واضح است که $d|a$ و $d|b$. اگر c چنان باشد که $c|a$ و $c|b$ آنگاه $c = p_۱^{h_۱}...p_n^{h_n}$ که h_i ها اعداد صحیح نامنفی هستند. چون $c|a$ و $c|b$ پس باید $h_i \le e_i$ و $h_i \le f_i$. در نتیجه $h_i \le g_i$ و این یعنی $c|d$. پس d بزرگترین مقسوم علیه مشترک است. اگر d و d' دو بزرگترین مقسوم علیه مشترک a و b باشند آنگاه $d|d'$ و $d'|d$. حال طبق گزاره ۲.۶.۸، d و d' شریک هستند. □

اکنون هدف ما این است که نشان دهیم حلقه چندجمله‌ها روی یک دامنه تجزیه یکتا، یک دامنه تجزیه یکتا است.

تعریف ۲.۶.۲۸. *فرض کنیم $f(x) \in R[x]$. گوییم $f(x)$ چندجمله‌ای اولیه یا به اختصار اولیه است هرگاه بزرگترین مقسوم علیه مشترک ضرایب $f(x)$ موجود و یکال باشد.*

تذکر ۲.۶.۲۹. *فرض کنیم R یک دامنه تجزیه یکتا باشد و $f(x) \in R[x]$. مشاهده می‌شود که اگر $f(x)$ ناصفر باشد آنگاه $c \in R$ که $f(x) = cf_1(x)$ بزرگترین مقسوم علیه ضرایب و $f_1(x)$ اولیه است. دقت شود که طبق قضیه ۲.۶.۲۷، برای ضرایب $f(x)$ بزرگترین مقسوم علیه مشترک وجود دارد. از طرفی فرض کنیم که $c \in R$ چنان باشد که $f(x) = cf_1(x)$ و $f_1(x)$ اولیه باشد. در این صورت حتما c بزرگترین مقسوم علیه مشترک است. پس طبق قضیه ۲.۶.۲۷، c تحت شریک بودن منحصر به فرد است. این منحصر به فرد بودن c تعریف زیر را نتیجه می‌دهد.*

تعریف ۲.۶.۳۰. *فرض کنیم R یک دامنه تجزیه یکتا باشد و $f(x) \in R[x]$. عنصر c در تذکر ۲.۶.۲۹ محتوای $f(x)$ نامیده می‌شود و با $c(f(x))$ نمایش می‌دهیم.*

مثال ۲.۶.۳۱. *چندجمله‌ای $6x + 3x^2$ در $\mathbb{Z}[x]$ اولیه نیست. زیرا $(6, 3) = 3$ در $\mathbb{Z}$ یکال نیست. اما $1 + x^2$ اولیه است. دقت شود که $c(3x^2 + 6x) = 3$.*

لم ۲.۶.۳۲. *فرض کنیم R یک دامنه تجزیه یکتا باشد و $f(x) \in R[x]$. در این صورت $c(f(x))$ یکال است اگر و تنها اگر $f(x)$ اولیه باشد.*

اثبات. ($\Leftarrow$). فرض کنیم بزرگترین مقسوم علیه مشترک ضرایب $f(x)$ برابر d باشد. از طرفی $c(f(x))$ نیز بزرگترین مقسوم علیه مشترک است. پس طبق قضیه ۲.۶.۲۷، $c(f(x))$ و d شریک هستند یعنی عنصر یکال u وجود دارد که $d = uc(f(x))$ پس d یکال است و در نتیجه $f(x)$ اولیه است.

($\Rightarrow$). مشابه بالا اثبات می‌شود. □

لم ۲.۶.۳۳. *(لم گاوس) فرض کنیم R یک دامنه تجزیه یکتا باشد و $f(x), g(x) \in R[x]$. در این صورت $c(f(x)g(x)) = c(f(x))c(g(x))$. به ویژه ضرب دو اولیه دوباره اولیه است.*

اثبات. فرض کنیم $c = c(f(x))$ و $c' = c(g(x))$ داریم $f(x) = cf_1(x)$ و $g(x) = c'g_1(x)$ که $f_1(x)$ و $g_1(x)$ اولیه هستند. از طرفی $f(x)g(x) = cc'f_1(x)g_1(x)$. پس کافی است نشان دهیم $f_1(x)g_1(x)$ اولیه است (یعنی حاصل ضرب دو اولیه، اولیه است). به برهان خلف فرض کنیم $f_1(x)g_1(x)$ اولیه نباشد. پس می‌توانیم عنصر تحویل ناپذیری مانند $p \in R$ را در نظر بگیریم که همه ضرایب $f_1(x)g_1(x)$ را می‌شمارد. همچنین فرض کنیم

$$f_1 = a_0 + \ldots + a_n x^n, \; g_1 = b_0 + \ldots + b_m x^m.$$

چون $f_1(x)$ و $g_1(x)$ اولیه هستند پس $p \nmid c$ و $p \nmid c'$ (چرا؟). پس می‌توانیم (اولین) ضرایب مانند a_i و b_j را در $f_1(x)$ و $g_1(x)$ چنان انتخاب کنیم که $p \nmid a_i$ و $p \nmid b_j$. اما ضریب x^{i+j} در

ضرب $f_۱(x)g_۱(x)$، عبارت a_ib_j ظاهر می‌شود. پس $p|a_ib_j$. اما طبق تعریف دامنه تجزیه یکتا هر تحویل ناپذیر اول است،خاصیت (۲)، پس $p|a_i$ یا $p|b_j$ که تناقض است. پس باید $f_۱(x)g_۱(x)$ اولیه باشد. □

قضیه زیر که هدف نهایی این بخش است را بدون اثبات می‌پذیریم.

قضیه ۳۴.۶.۲. *اگر R دامنه تجزیه یکتا باشد آنگاه $R[x_۱,...,x_n]$ نیز دامنه تجزیه یکتا است.*

تمرین حل شده

تمرین ۳۵.۶.۲. *نشان دهید شریک یک عنصر اول، اول است.*

اثبات. فرض کنیم x عنصر اول باشد که با y شریک است. پس عنصر یکالی مانند u وجود دارد که $y = xu$. اگر y یکال باشد آنگاه x یکال می‌شود که تناقض است. پس y یکال نیست. حال فرض کنیم $y|ab$. پس c چنان وجود دارد که $ab = yc$. در نتیجه $ab = xuc$. پس $x|a$ یا $x|b$. اگر $x|a$ پس c' چنان وجود دارد که $a = xc'$. در نتیجه $a = yu^{-۱}c'$. بنابراین $y|a$. مشابه نتیجه می‌شود که اگر $x|b$ آنگاه $y|b$. پس y اول است. □

تمرین ۳۶.۶.۲. *در حلقه R عنصر ناصفر p اول است اگر و تنها اگر ایده‌آل Rp اول باشد.*

اثبات. ($\Leftarrow$). فرض کنیم $ab \in Rp$. پس t چنان وجود دارد که $ab = pt$. یعنی $p|a$ یا $p|b$. اگر $p|a$ آنگاه u چنان وجود دارد که $a = pu$. یعنی $a \in Rp$. به صورت مشابه اگر $p|b$ آنگاه $b \in Rp$. پس Rp اول است.
($\Rightarrow$). چون Rp اول است p یکال نیست (چرا؟). فرض کنیم $p|ab$. پس t چنان وجود دارد که $ab = tp$. یعنی $ab \in Rp$. چون Rp اول است پس $a \in Rp$ یا $b \in Rp$. اگر $a \in Rp$ آنگاه u چنان وجود دارد که $a = pu$. یعنی $p|a$. به صورت مشابه اگر $b \in Rp$ آنگاه $p|b$. پس p عنصر اول است. □

تمرین ۳۷.۶.۲. *نشان دهید که اگر $(a,b) = ۱$ و $b|ac$ آنگاه $b|c$.*

اثبات. طبق فرض t چنان وجود دارد که $ac = bt$. حال داریم که

$$c = c(a,b) = (ca,cb) = (bt,bc) = b(t,c).$$

در نتیجه $b|c$. □

تمرین ۳۸.۶.۲. *فرض کنیم که $R = \{f_۰ + ... + f_nx^n \in \mathbb{R}[x] \mid f_۰ \in \mathbb{Z}\}$. نشان دهید که R یک دامنه تجزیه یکتا نیست.*

اثبات. به برهان خلف، فرض کنیم R دامنه تجزیه یکتا است. واضح است که $R \subset \mathbb{R}[x]$. حال طبق قضیه ۵.۵.۲، $\mathbb{R}[x]$ دامنه ایده‌آل اصلی است پس R دامنه است. دقت شود که R حاوی ۱ است. حال طبق تمرین ۳۱.۳.۲، یکال‌های $\mathbb{R}[x]$ برابر عناصر ناصفر $\mathbb{R}$ است. اما هر عنصر یکال

R عنصر یکال $\mathbb{R}[x]$ است. اما $R\cap\mathbb{Q}=\mathbb{Z}$ در نتیجه تنها ۱ و -۱ در R یکال هستند. حال دنباله به صورت $a_n=۲n$ را در نظر بگیرید. حال واضح است که برای هر n، $f_n=\frac{۱}{a_n}x$ عنصری از R است و برای هر $n\neq n'$، f_n و $f_{n'}$ شریک نیستند (چرا؟). اما برای هر n داریم $x=a_nf_n$. پس برای هر n داریم $a_n|x$. پس x بیشمار مقسوم علیه دارد یعنی بزرگترین مقسوم علیه مشترک وجود ندارد. این با قضیه ۲۷.۶.۲، در تناقض است. □

تمرین ۳۹.۶.۲. *نشان دهید در حلقه $\mathbb{Z}[\sqrt{-۵}]$ دو عنصر ۶ و $۲+۲\sqrt{-۵}$ بزرگترین مقسوم علیه مشترک ندارند.*

اثبات. برای اثبات حکم نیاز به تابع ارزیاب (نرم) داریم. یادآوری می‌کنیم که

$$v:\mathbb{Z}[\sqrt{-۵}]\setminus\{۰\}\longrightarrow\mathbb{N}\cup\{۰\},\ v(a+b\sqrt{-۵})=a^۲+۵b^۲$$

یک نرم است. با محاسبات سر راست خاصیت $(*)$ زیر برای نرم به دست می‌آید.
$(*)$ $v(xy)=v(x)v(y)$ برای هر $x,y\in\mathbb{Z}[\sqrt{-۵}]$. در نتیجه اگر $x|y$ آنگاه $v(x)|v(y)$.
حال به برهان خلف فرض کنیم که دو عنصر ۶ و $۲+۲\sqrt{-۵}$ بزرگترین مقسوم علیه مشترک دارند. پس دو عنصر ۳ و $۱+\sqrt{-۵}$ نیز بزرگترین مقسوم علیه مشترک مانند $d=e+f\sqrt{-۵}$ دارند. چون $d|۳$ و $d|۱+\sqrt{-۵}$ پس طبق $(*)$، داریم $v(d)|۹$ و $v(d)|۶$. یعنی $v(d)$ برابر با ۱ یا ۳ است. اگر $v(d)=۳$ باشد آنگاه $e^۲+۵f^۲=۳$ که چنین معادله‌ای در $\mathbb{Z}$ جواب ندارد (چرا؟) و در نتیجه $v(d)=۱$. پس $e^۲+۵f^۲=۱$. چنین معادله‌ای در $\mathbb{Z}$ جواب $f=۰$ و $e=۱$ دارد پس $d=۱$. این یعنی دو عنصر ۶ و $۲+۲\sqrt{-۵}$ بزرگترین مقسوم علیه مشترک برابر با ۲ دارند.
اکنون واضح است که $(۱+\sqrt{-۵})(۱-\sqrt{-۵})=۶$ و $۲(۱+\sqrt{-۵})=۲+۲\sqrt{-۵}$. پس $۱+\sqrt{-۵}$ یک مقسوم علیه مشترک است در نتیجه $۲|۱+\sqrt{-۵}$. طبق $(*)$، $v(۱+\sqrt{-۵})|v(۲)$ یعنی $۶|۲$ که تناقض است. □

تمرین ۴۰.۶.۲. *در حلقه ایده‌آل اصلی R نشان دهید که هر دو عنصر ناصفر a و b دارای بزرگترین مقسوم علیه مشترک d هستند. به علاوه عناصر r و s چنان وجود دارند که $d=ra+sb$.*

اثبات. ایده‌آل $Ra+Rb$ طبق فرض اصلی است پس $d\in R$ چنان وجود دارد که $Ra+Rb=Rd$.
به علاوه واضح است که عناصر r و s چنان وجود دارند که $d=ra+sb$. ادعا می‌کنیم d همان مطلوب مسئله است. چون $a,b\in Rd$ پس u و v موجود هستند که $a=du$ و $b=dv$. پس $d|a$ و $d|b$. حال فرض کنیم c یک مقسوم علیه مشترک دیگر باشد یعنی $c|a$ و $c|b$. لذا $a=cu'$ و $b=cv'$. در نتیجه $d=rcu'+scv'=(ru'+sv')c$ و این یعنی $c|d$. □

تمرین ۴۱.۶.۲. *نشان دهید که اگر F میدان باشد آنگاه $F[x,y]$ یک دامنه تجزیه یکتا است که دامنه ایده‌آل اصلی نیست.*

اثبات. می‌دانیم که $F[x,y]=F[x][y]$. چون F میدان است پس طبق قضیه ۵.۵.۲، $F[x]$ یک دامنه ایده‌آل اصلی است. پس طبق قضیه ۲۱.۶.۲، $F[x]$ یک دامنه تجزیه یکتا است پس باید $F[x][y]$ طبق قضیه ۳۴.۶.۲، دامنه تجزیه یکتا باشد یعنی $F[x,y]$ دامنه تجزیه یکتا است. اما طبق تمرین ۳۱.۳.۲، x در $F[x]$ وارونپذیر نیست پس $F[x]$ یک میدان نیست و در نتیجه طبق قضیه ۵.۵.۲، $F[x][y]$ یک دامنه ایده‌آل اصلی نیست. □

۷.۲ تحویل‌ناپذیری چندجمله‌ای‌ها

در این بخش می‌خواهیم چند محک معرفی کنیم تا در حلقه $R[x_1,...,x_n]$ بتوانیم عنصر (چندجمله‌ای) تحویل ناپذیر را تشخیص دهیم. چندجمله‌ای تحویل ناپذیر کاربرد فراوانی در ساختن میدان متناهی، هندسه جبری، نظریه کد و رمز، نظریه گالوا و گسترش میدان‌ها دارد. در سرتاسر این بخش F و E نمایش میدان است مگر به صراحت خلافش را ذکر کنیم.

تعریف ۱.۷.۲. *فرض کنیم F و E دو میدان باشند که $F \subseteq E$. گوییم $a \in E$ یک ریشه یا صفر $f(x) \in F[x]$ است هرگاه $f(a) = 0$.*

تعریف ۲.۷.۲. *گوییم $f(x) \in F[x]$ تحویل پذیر است هرگاه تحویل ناپذیر نباشد.*

گزاره ۳.۷.۲. *فرض کنیم $f(x) \in F[x]$ که $deg(f(x)) > 1$. اگر برای یک $a \in F$، $f(a) = 0$ آنگاه $f(x)$ تحویل پذیر است.*

اثبات. چون F میدان است پس همه ضرایب یکال هستند از جمله ضریب پیشرو. حال طبق قضیه ۱۶.۳.۲، داریم

$$f(x) = (x-a)q(x) + r(x),\ deg(r) < deg(x-a).$$

واضح است که $r(x) \in F$. اما $f(a) = 0$ پس باید $r = 0$ باشد یعنی $f(x) = (x-a)q(x)$. چون $deg(f(x)) > 1$ پس باید $deg(q(x)) \geq 1$. حال طبق تمرین ۳۱.۳.۲، نه $x-a$ و نه $q(x)$ یکال نیست. پس f تحویل ناپذیر نیست. □

تذکر ۴.۷.۲. *دقت شود که به سادگی با کمک درجه و این مطلب که F میدان است می‌توان نشان داد $ax+b$ که $a \neq 0$ در حلقه $F[x]$ تحویل ناپذیر است. اما این مطلب ممکن است در حلقه $R[x]$ که R دامنه تجزیه یکتا است صحیح نباشد به عنوان مثال $f(x) = 2x+2 = 2(x+1)$ در $\mathbb{Z}[x]$ تحویل ناپذیر نیست.*

تذکر ۵.۷.۲. *عکس گزاره ۳.۷.۲، در حالت کلی صحیح نیست. مثلا $f(x) = (x^2+1)(x^2+5)$ در $\mathbb{R}[x]$ تحویل پذیر است زیرا طبق تمرین ۳۱.۳.۲، نه x^2+1 و نه x^2+5 یکال نیست. در حالی که نه x^2+1 و نه x^2+5 در $\mathbb{R}$ ریشه ندارند. در قضیه بعدی تحت شرایط خاصی نشان می‌دهیم عکس گزاره ۳.۷.۲، نیز بر قرار است.*

قضیه ۶.۷.۲. *فرض کنیم $f(x) \in F[x]$ از درجه ۲ یا ۳ باشد. در این صورت $f(x)$ تحویل پذیر است اگر و تنها اگر $f(x)$ ریشه داشته باشد.*

اثبات. ($\Leftarrow$). چون $f(x)$ تحویل پذیر است پس $f(x) = g(x)h(x)$ که $h(x)$ و $g(x)$ چندجمله‌ای ثابت نیستند زیرا یکال نیستند (تمرین ۳۱.۳.۲ را ببینید). چون درجه $f(x)$ حداکثر ۳ است پس $h(x)$ یا $g(x)$ باید از درجه ۱ باشد. بدون کم شدن از کلیت فرض کنیم که $h(x)$ از درجه ۱ باشد. پس $h(x) = ax+b$ که $a,b \in F$. حال واضح است که $h(-ba^{-1}) = 0$. بنابراین $-ba^{-1}$ ریشه $f(x)$ است.

($\Rightarrow$). گزاره ۳.۷.۲ را ببینید. □

مثال ۲.۷.۷. چندجمله‌ای $x^۲ + x + \bar{۲}$ در حلقه $\mathbb{Z}_۳[x]$ تحویل ناپذیر است. زیرا $f(\bar{۰}) \neq \bar{۰}$، $f(\bar{۱}) \neq \bar{۰}$ و $f(\bar{۲}) \neq \bar{۰}$ پس طبق قضیه ۲.۷.۶، $f(x)$ تحویل ناپذیر است.

در ادامه روی دو حلقه خاص $\mathbb{Z}[x]$ و $\mathbb{Q}[x]$ تمرکز می‌کنیم و محکی جهت شناسایی چندجمله‌ای تحویل ناپذیر در این دو حلقه خاص ارائه می‌دهیم. باید خاطر نشان کنیم که از این بابت این دو حلقه برای ما خاص و با اهمیت هستند که شناختن تحویل ناپذیرها در این دو حلقه کاربرد زیادی در هندسه جبری دارد و همچنین $\mathbb{Q}$ میدان کسر $\mathbb{Z}$ است (با تعریف میدان کسر در این دوره آشنا نمی‌شوید).

تعریف ۲.۷.۸. گوییم $f(x) \in F[x]$ تکین است هرگاه ضریب پیشرو آن ۱ باشد.

لم ۲.۷.۹. *در حلقه $\mathbb{Z}[x]$ برای عنصر $f(x) = r_n x^n + ... + r_۰$ موارد زیر بر قرار است.*
(۱) اگر $f(x)$ تکین باشد آنگاه اولیه است.
(۲) اگر $f(x)$ تحویل ناپذیر و غیر ثابت باشد آنگاه اولیه است.

اثبات. (۱) طبق فرض $r_n = ۱$. پس $(۱, r_{n-۱}, ..., r_۰) = ۱$. چون ۱ در $\mathbb{Z}$ یکال است $f(x)$ اولیه است.
(۲) فرض کنیم $d = (r_n, ..., r_۰)$. پس $f(x) = dg(x)$. اگر d برابر با ۱ نباشد (تنها یکال‌های $\mathbb{Z}$ برابر با ۱ و -۱ است) آنگاه چون $f(x)$ تحویل ناپذیر است پس $g(x)$ یکال است. در نتیجه طبق تمرین ۲.۳.۳۱، $g(x)$ برابر با ۱ یا -۱ است. در نتیجه $f(x)$ ثابت است که تناقض است. پس $d = ۱$ و $f(x)$ اولیه است. □

دو نتیجه که در زیر می‌آید منسوب به گاوس است.

گزاره ۲.۷.۱۰. *اگر $f(x) \in \mathbb{Z}[x]$ روی $\mathbb{Q}$ تحویل پذیر باشد آنگاه $f(x)$ روی $\mathbb{Z}$ نیز تحویل پذیر است.*

اثبات. چون $f(x)$ روی $\mathbb{Q}$ تحویل پذیر است پس $f(x) = g(x)h(x)$ که $h(x), g(x) \in \mathbb{Q}[x]$. چون $h(x)$ و $g(x)$ یکال نیستند پس طبق تمرین ۲.۳.۳۱، $h(x) \notin \mathbb{Q}$ و $g(x) \notin \mathbb{Q}$. فرض کنیم $m \in \mathbb{Z}$ کوچکترین مضرب مشترک مخرج همه ضرایب $g(x)$ و $n \in \mathbb{Z}$ کوچکترین مضرب مشترک مخرج همه ضرایب $h(x)$ باشد. واضح است که $g'(x) = mg(x) \in \mathbb{Z}[x]$ و $h'(x) = nh(x)$. حال داریم

$$mnf(x) = g'(x)h'(x).$$

حال c را کوچکترین عدد صحیح در نظر بگیرید که $cf(x) = g'(x)h'(x)$. ادعا می‌کنیم $c = ۱$. به برهان خلف، فرض کنیم $c > ۱$. پس عدد اول p چنان وجود دارد که $p|c$. حال ضرایب $g'(x)$ و $h'(x)$ را به پیمانه p می‌بریم و چند جمله‌ای‌های جدید را با $\overline{g'(x)}$ و $\overline{h'(x)}$ نمایش می‌دهیم یعنی $\overline{g'(x)}, \overline{h'(x)} \in \mathbb{Z}_p[x]$. حال داریم

$$۰ \overset{p}{\equiv} cf(x) \overset{p}{\equiv} g'(x)h'(x) \overset{p}{\equiv} \overline{g'(x)}\,\overline{h'(x)}.$$

اما $\mathbb{Z}_p$ یک دامنه صحیح (میدان) است پس طبق تمرین ۲۶.۳.۲، $\mathbb{Z}_p[x]$ دامنه صحیح است. پس $\overline{g'(x)} \overset{p}{\equiv} ۰$ یا $\overline{h'(x)} \overset{p}{\equiv} ۰$. بدون کم شدن از کلیت فرض کنیم که $\overline{g'(x)} \overset{p}{\equiv} ۰$. پس همه ضرایب $g'(x)$، بر p قابل قسمت هستند. حال قرار می‌دهیم $g''(x) = \frac{g'(x)}{p}$ و $c' = \frac{c}{p}$. پس $c'f(x) = g''(x)h'(x)$. اما به وضوح $c' < c$ و این با انتخاب ما از c در تناقض است. پس $c = ۱$. در نتیجه $f(x) = g'(x)h'(x)$ که $g(x), h(x) \in \mathbb{Z}[x]$. اما با توجه به نوع ساختن $g'(x)$ و $h'(x)$ داریم که

$$deg(g(x)) = deg(g'(x)),\ deg(h(x)) = deg(h'(x)).$$

اما $h(x) \notin \mathbb{Q}$ و $g(x) \notin \mathbb{Q}$ پس $g'(x)$ و $h'(x)$ یکال نیستند (تمرین ۳۱.۳.۲ را ببینید). و این یعنی $f(x)$ در $\mathbb{Z}[x]$ تحویل ناپذیر نیست و اثبات کامل است. □

تذکر ۱۱.۷.۲. *عکس گزاره ۱۰.۷.۲، در حالت کلی صحیح نیست. واضح است که x در $\mathbb{Z}[x]$ ۲ تحویل پذیر است (چرا؟) اما x در $\mathbb{Q}[x]$ ۲ تحویل ناپذیر است زیرا در $\mathbb{Q}$ ۲ یکال است. در قضیه بعدی در حالتی خاص عکس گزاره را نیز نشان می‌دهیم.*

قضیه ۱۲.۷.۲. *(گاوس) فرض کنیم $f(x) \in \mathbb{Z}[x]$ اولیه باشد. در این صورت $f(x)$ روی $\mathbb{Q}$ تحویل پذیر است اگر و تنها اگر $f(x)$ روی $\mathbb{Z}$ تحویل پذیر است.*

اثبات. ($\Leftarrow$). گزاره ۱۰.۷.۲ را ببینید.
($\Rightarrow$). چون $f(x)$ روی $\mathbb{Z}$ تحویل پذیر است پس $f(x) = g(x)h(x)$. اما اگر یکی از $g(x)$ یا $h(x)$ ثابت باشد مثلا $h(x)$ ثابت باشد یعنی فرض کنیم $f(x) = ng(x)$ باشد که $n \in \mathbb{Z}$ آنگاه طبق لم گاوس، لم ۳۳.۶.۲، داریم $c(f(x)) = nc(g(x))$. اما طبق فرض $f(x)$ روی $\mathbb{Z}$ اولیه است پس $c(f(x))$ یکال است و در نتیجه n در $\mathbb{Z}$ یکال است (یعنی n برابر با ۱ یا ۱−). پس $f(x)$ حتما تجزیه به صورت $f(x) = g(x)h(x)$ دارد که حتما درجه $g(x)$ و $h(x)$ بزرگتر مساوی ۱ است. حال طبق تمرین ۳۱.۳.۲، نه $h(x)$ و نه $g(x)$ در $\mathbb{Q}[x]$ یکال نیستند یعنی $f(x) = g(x)h(x)$ تحویل ناپذیر نیست و اثبات کامل است. □

بر طبق گزاره ۳.۷.۲ هر چندجمله‌ای از درجه بیشتر مساوی ۱ در $F[x]$ که ریشه داشته باشد تحویل پذیر است. قضیه زیر نشان می‌دهد که اگر یک چندجمله‌ای در $\mathbb{Z}[x]$ ریشه $\alpha \in \mathbb{Q}$ داشته باشد (یعنی بر طبق گزاره ۳.۷.۲ تحویل پذیر باشد) آنگاه α در $\mathbb{Z}$ قرار دارد. در واقع به نوعی حدود ریشه را تعیین می‌کند.

قضیه ۱۳.۷.۲. *فرض کنیم $f(x) = r_۰ + ... + r_t x^t \in \mathbb{Z}[x]$ یک چندجمله‌ای تکین باشد که $r_۰ \neq ۰$. اگر $f(x)$ ریشه $\alpha \in \mathbb{Q}$ داشته باشد آنگاه $\alpha \in \mathbb{Z}$ و $\alpha | f_۰$.*

اثبات. فرض کنیم $\alpha = \frac{m}{n}$ و $(m, n) = ۱$. پس

$$۰ = r_۰ + r_۱(\frac{m}{n}) + ... + r_t(\frac{m}{n})^t.$$

حال طرفین را در n^{t-1} ضرب می‌کنیم

$$0 = r_0 n^{t-1} + r_1 m n^{t-2} + ... + r_{t-1} m^{t-1} + r_t \frac{m^t}{n}.$$

در نتیجه

$$r_0 n^{t-1} + r_1 m n^{t-2} + ... + r_{t-1} m^{t-1} = -r_t \frac{m^t}{n}.$$

سمت چپ تساوی فوق به وضوح در $\mathbb{Z}$ است پس باید $-r_t \frac{m^t}{n} \in \mathbb{Z}$. یعنی باید $n|m^t$. اما $(m,n) = 1$ در نتیجه n برابر با ۱ یا -1 است. این نشان می‌دهد که $\alpha = \pm m \in \mathbb{Z}$. اما در سمت راست آخرین تساوی بالا $\alpha = \pm m$ را می‌شمارد پس باید همه جملات سمت چپ آخرین تساوی بالا $\alpha = \pm m$ را بشمارد از جمله r_0. این یعنی $\alpha = \pm m | r_0$. □

در ادامه این بخش دو محک جالب که تحویل ناپذیر بودن یک چندجمله‌ای روی $\mathbb{Q}$ را نشان می‌دهد، ارائه می‌کنیم.

قضیه ۱۴.۷.۲. (محک آیزنشتاین) *فرض کنیم* $f(x) = f_0 + ... + f_n x^n \in \mathbb{Z}[x]$ و $n \geq 1$. *اگر* p *عددی اول با ویژگی‌های*
(۱) $p \nmid f_n$
(۲) $p^2 \nmid f_0$
(۳) $p|f_0$، $p|f_1$، ...، $p|f_{n-1}$
باشد آنگاه $f(x)$ *روی* $\mathbb{Q}$ *تحویل ناپذیر است.*

اثبات. ادعا می‌کنیم که $f(x)$ روی $\mathbb{Z}$ تحویل ناپذیر است. فرض کنیم ادعای ما اثبات شده است. حال اگر $f(x)$ روی $\mathbb{Q}$ تحویل پذیر باشد آنگاه بر طبق گزاره ۱۰.۷.۲، $f(x)$ روی $\mathbb{Z}$ تحویل پذیر است که این ادعای اثبات شده ما را نقض می‌کند پس $f(x)$ روی $\mathbb{Q}$ تحویل ناپذیر است.
حال اثبات ادعا؛ به برهان خلف فرض کنیم $f(x)$ روی $\mathbb{Z}$ تحویل پذیر باشد پس

$$f(x) = (g_0 + ... + g_r x^r)(h_0 + ... + h_t x^t)$$

که در آن $g_r \neq 0$، $h_t \neq 0$ و $g_i, h_i \in \mathbb{Z}$. واضح است که $r < n$ و $t < n$. اما $p|f_0 = g_0 h_0$ پس $p|g_0$ یا $p|h_0$. از طرفی $p^2 \nmid f_0 = g_0 h_0$. در نتیجه دو حالت زیر رخ می‌دهد
(الف) $p|g_0$ و $p \nmid h_0$
(ب) $p|h_0$ و $p \nmid g_0$.
ما نشان می‌دهیم که حالت (ب) به تناقض می‌رسد به صورت مشابه حالت (الف) نیز به تناقض منجر می‌شود. پس فرض کنیم که $p|h_0$ و $p \nmid g_0$. طبق فرض $p \nmid f_n = g_r h_t$. در نتیجه $p \nmid g_r$ و $p \nmid h_t$. بنابراین می‌توانیم فرض کنیم که h_m اولین ضریب در $h_0 + ... + h_t x^t$ باشد که $p \nmid h_m$. اما می‌دانیم که ضریب x^m در $f(x)$ یعنی f_m برابر

$$g_0 h_m + g_1 h_{m-1} + ... + g_m h_0$$

است. حال چون $p \nmid h_m$ و $p \nmid g_0$ پس $p \nmid f_m$. این فرض (۳) را نقض می‌کند مگر این که $m = n$ باشد. اما در این صورت $m = n \leq s < n$ که تناقض است. پس $f(x)$ روی $\mathbb{Z}$ تحویل ناپذیر است و ادعا اثبات شد. اثبات کامل است. □

قضیه ۱۵.۷.۲. *فرض کنیم $f(x) = f_0 + f_1 x + ... + f_n x^n \in \mathbb{Z}[x]$ و $n > 1$. اگر عدد اول p چنان موجود باشد که*

$$\overline{f(x)} = \bar{f}_0 + \bar{f}_1 x + ... + \bar{f}_n x^n$$

درشرایط
(۱) $\overline{f(x)}$ در $\mathbb{Z}_p[x]$ تحویل ناپذیر
(۲) $deg(\overline{f(x)}) = n$
صدق کند آنگاه $f(x)$ در $\mathbb{Q}[x]$ تحویل ناپذیر است.

اثبات. به برهان خلف، فرض کنیم $f(x)$ در $\mathbb{Q}[x]$ تحویل پذیر است. حال طبق گزاره ۱۰.۷.۲، $f(x)$ در $\mathbb{Z}[x]$ تحویل پذیر است. در نتیجه

$$f(x) = (g_0 + ... + g_m x^m)(h_0 + ... + h_k x^k)$$

که در آن $h_i, g_i \in \mathbb{Z}$، $0 < m < n$ و $0 < k < n$. بنابراین

$$\overline{f(x)} = \overline{g(x)h(x)} = (\bar{g}_0 + ... + \bar{g}_m x^m)(\bar{h}_0 + ... + \bar{h}_k x^k).$$

حال طبق شرط (۲) باید داشته باشیم $n = k + m$ و این یعنی $\bar{g}_m \times \bar{h}_k \neq \bar{0}$. اما $\mathbb{Z}_p$ دامنه صحیح (میدان) است پس $\bar{g}_m \neq 0$ و $\bar{h}_k \neq 0$. در نتیجه دو چندجمله‌ای $\overline{g(x)}$ و $\overline{h(x)}$ در $\mathbb{Z}_p[x]$ ثابت نیستند. اکنون طبق تمرین ۳۱.۳.۲، $\overline{g(x)}$ و $\overline{h(x)}$ یکال نیستند. در نتیجه $\overline{f(x)}$ در در $\mathbb{Z}_p[x]$ تحویل ناپذیر نیست. این تناقض آشکار با شرط (۱) است. از این رو باید $f(x)$ در $\mathbb{Q}[x]$ تحویل ناپذیر باشد. □

این بخش را با دو مثال مربوط به محک‌های بالا که نحوه استفاده از دو محک را نشان می‌دهد به پایان می‌رسانیم.

مثال ۱۶.۷.۲. *چندجمله‌ای $x^2 - 2$ روی $\mathbb{Q}$ تحویل ناپذیر است. زیرا اگر فرض کنیم $p = 2$ است آنگاه $f_n = 1$، $2 \nmid f_0$، $2^2 \nmid f_0 = -2$ و $p | f_1 = 0$. حال طبق محک آیزنشتاین، قضیه ۱۴.۷.۲، حکم به دست می‌آید.*

مثال ۱۷.۷.۲. *چندجمله‌ای $f(x) = x^3 + \frac{1}{2}x^2 - \frac{1}{2}$ روی $\mathbb{Q}$ تحویل ناپذیر است. زیرا واضح است که $g(x) = 2f(x) = 2x^3 + x^2 - 1$ عنصری از $\mathbb{Z}[x]$ است و اگر فرض کنیم $p = 3$ آنگاه $deg(f(x)) = deg(\overline{g(x)}) = 3$ که $\overline{g(x)} \in \mathbb{Z}_3[x]$. حال واضح است که هیچ عنصری از $\mathbb{Z}_3[x]$ ریشه $\overline{g(x)}$ نیست پس طبق قضیه ۶.۷.۲، $\overline{g(x)} \in \mathbb{Z}_3[x]$ تحویل ناپذیر است. اکنون طبق قضیه ۱۵.۷.۲، $f(x)$ روی $\mathbb{Q}$ تحویل ناپذیر است.*

تمرین حل شده

تمرین ۲.۷.۱۸. *فرض کنیم $f(x)$ یک چندجمله‌ای ناصفر در $\mathbb{Q}[x]$ باشد. آنگاه عناصر ناصفر m و n در $\mathbb{Z}$ و چندجمله‌ای اولیه $f_1(x)$ در $\mathbb{Z}[x]$ وجود دارند که $f(x) = \frac{m}{n} f_1(x)$.*

اثبات. فرض کنیم

$$f(x) = \frac{m_0}{n_0} + ... + \frac{m_t}{n_t} x^t.$$

قرار دهید $n = n_0 n_1 ... n_t$. واضح است که $n \in \mathbb{Z}$. حال داریم

$$nf(x) = m_0 n_1 ... n_t + ... + m_t n_0 ... n_{t-1} x^t.$$

واضح است که $nf(x) \in \mathbb{Z}[x]$ و $nf(x) \neq 0$. پس چندجمله‌ای اولیه $f_1(x) \in \mathbb{Z}[x]$ چنان وجود دارد که $nf(x) = c(nf(x)) f_1(x)$. حال قرار دهید $m = c(nf(x))$. واضح است که $m \in \mathbb{Z}$. در نتیجه $f(x) = \frac{m}{n} f_1(x)$. □

تمرین ۲.۷.۱۹. *فرض کنیم $f(x)$ یک چندجمله‌ای ناصفر در $\mathbb{Z}[x]$ باشد. اگر*

$$\frac{m'}{n'} f_2(x) = f(x) = \frac{m}{n} f_1(x)$$

که چندجمله‌ای‌های $f_1(x)$ و $f_2(x)$ در $\mathbb{Z}[x]$ اولیه باشند و $\frac{m}{n}, \frac{m'}{n'} \in \mathbb{Q}$. آنگاه عنصر یکال $u \in \mathbb{Z}$ (1 یا -1) وجود دارد که $\frac{m}{n} = u\frac{m'}{n'}$.

اثبات. طبق فرض داریم $nm' f_2(x) = n'm f_1(x)$. اما $f_1(x)$ و $f_2(x)$ در $\mathbb{Z}[x]$ اولیه هستند پس

$$nm' = c(nm' f_2(x)) = c(n'm f_1(x)) = n'm.$$

حال طبق تذکر ۲۹.۶.۲، $n'm$ و nm' شریک هستند. در نتیجه عنصر یکال $u \in \mathbb{Z}$ چنان وجود دارد که $unm' = n'm$. پس $\frac{m}{n} = u\frac{m'}{n'}$. □

تمرین ۲.۷.۲۰. *$f(x)$ در $F[x]$ تحویل ناپذیر است اگر و تنها اگر $f(x+1)$ در $F[x]$ تحویل ناپذیر باشد.*

اثبات. فرض کنیم $f(x)$ تحویل ناپذیر باشد. به برهان خلف فرض کنیم $f(x+1)$ تحویل پذیر باشد. پس $f(x+1) = g(x)h(x)$. حال جای x را با $x-1$ عوض کنید. در نتیجه $f(x) = g(x-1)h(x-1)$. این تناقض است. برعکس نیز مشابه است. □

تمرین ۲.۷.۲۱. *نشان دهید که تنها چندجمله‌ای تحویل ناپذیر از درجه ۲ روی Z_2 برابر است با $x^2 + x + \bar{1}$.*

اثبات. صورت کلی چندجمله‌ای درجه به شکل زیر است

$$f(x) = \bar{a}x^2 + \bar{b}x + \bar{c}.$$

چون درجه چندجمله‌ای ۲ است پس $\bar{a} = \bar{1}$. پس تمام چندجمله‌ای‌ها برای $\bar{b}$ و $\bar{c}$ متفاوت به شکل زیر است

$$x^2 + \bar{1},\ x^2 + x,\ x^2 + x + \bar{1},\ x^2.$$

اما داریم

$$x^2 + \bar{1} = (x + \bar{1})(x + \bar{1}),\ x^2 + x = x(x + \bar{1}), x^2 = xx.$$

حال واضح است که هر سه تا چندجمله‌ای بالا تحویل پذیرند و مسئله اثبات می‌شود. □

۸.۲ کاربردهایی از نظریه چندجمله‌ای‌ها

یکی از کاربردهای نظریه حلقه‌ها ساختن میدان‌های متناهی است. میدان‌های متناهی علاوه بر این که برای جبردان‌ها جذاب و پر اهمیت هستند در نظریه اطلاعات، نظریه کد، رمزنگاری و نظریه اعداد نیز ظاهر می‌شوند. در این بخش شما را تا حدی با نظریه میدان متناهی آشنا می‌کنیم. شاید لازم باشد که جهت یادآوری کمی درس جبر خطی و قضیه‌های مربوط به پایه و بعد را مطالعه نمایید.

تعریف ۱.۸.۲. *میدان F را اول گوییم که زیر میدان سره‌ای نداشته باشد.*

مثال ۲.۸.۲. *واضح است که $\mathbb{Q}$ و $\mathbb{Z}_p$ که p عددی اول است، میدان اولند.*

لم ۳.۸.۲. *هر میدان F شامل یک زیر میدان اول است.*

اثبات. کافی است اشتراک خانواده تمام زیر میدان‌های F را در نظر بگیریم. دقت شود که این خانواده دست کم شامل F است پس ناتهی است و اشتراک زیر میدان‌ها بوضوح یک میدان است. □

در گزاره بعدی نشان می‌دهیم که تحت یکریختی فقط دو تا میدان اول وجود دارد.

گزاره ۴.۸.۲. *میدان اول هر میدان چون F یا با $\mathbb{Q}$ یا با $\mathbb{Z}_p$ که p عددی اول است، یکریخت است.*

اثبات. فرض کنیم ۱ همانی F باشد. قرار می‌دهیم

$$f : \mathbb{Z} \longrightarrow F, \quad f(n) = n۱.$$

بوضوح f یک همریختی حلقه‌ای است. اکنون دو حالت رخ می‌دهد.
حالت ۱: اگر f یک به یک باشد یا معادلا $Kerf =< ۰ >$ یا معادلا $CharF = ۰$. در این صورت f یک نشاننده است. با تعریف زیر f را به یک نشاننده روی $\mathbb{Q}$ گسترش می‌دهیم

$$\bar{f} : \mathbb{Q} \longrightarrow F, \quad \bar{f}(\frac{m}{n}) = \frac{m۱}{n۱}.$$

پس $\mathbb{Q}$ در F نشانده می‌شود پس میدان اول F با $\mathbb{Q}$ یکریخت است.
حالت ۲: اگر f یک به یک نباشد یا معادلا $Kerf \neq< ۰ >$ یا معادلا $CharF \neq ۰$. حال چون F دامنه صحیح است در نتیجه از قضیه‌ای در مبانی جبر باید $CharF = p$ که p عددی اول است. اما $\mathbb{Z}$ یک دامنه صحیح اصلی است در نتیجه $Kerf =< p >$. حال طبق قضیه اول یکریختی داریم $F \cong \mathbb{Z}/ < p > \cong \mathbb{Z}_p$. پس $\mathbb{Z}_p$ در F نشانده می‌شود. بنابراین میدان اول F با $\mathbb{Z}_p$ یکریخت است. □

اکنون می‌توانیم اولین قضیه مهم این بخش را بیان کنیم.

قضیه ۵.۸.۲. *هر میدان متناهی F دارای مشخصه عدد اول p است. به علاوه عدد صحیح n چنان وجود دارد که F دارای تعداد p^n عنصر است.*

اثبات. قسمت اول، چون F دامنه صحیح متناهی است در نتیجه (بنابر قضیه‌ای در مبانی جبر) $CharF = p$ که p عددی اول است. اکنون طبق گزاره ۴.۸.۲، میدان اول F با $\mathbb{Z}_p$ یکریخت است. حال F را می‌توانیم یک $\mathbb{Z}_p$ـ فضای برداری در نظر بگیریم. چون F متناهی است پس حتما برای این فضای برداری پایه‌ای مانند $\{f_1, ..., f_n\}$ وجود دارد. حال برای هر عنصر دلخواه $f \in F$ نمایش یکتا

$$f = \bar{a}_1 f_1 + ... + \bar{a}_n f_n$$

وجود دارد که $\bar{a}_i \in \mathbb{Z}_p$. چون انتخاب ما برای هر $\bar{a}_i \in \mathbb{Z}_p$ برابر p است پس تعداد عناصر F برابر p^n می‌باشد و اثبات کامل است.

□

لم زیر را صرفا برای با معنی بودن فرض قضیه ۷.۸.۲، آورده‌ایم. برای اثبات این لم به اطلاعاتی بیشتر از نظریه میدان نیاز داریم که مربوط به این درس نیست بنابراین این لم را بدون اثبات می‌پذیریم.

لم ۶.۸.۲. *فرض کنیم n یک عدد طبیعی باشد. در این صورت همواره یک چندجمله‌ای تحویل ناپذیر تکین از درجه n در $\mathbb{Z}_p[x]$ وجود دارد.*

این بخش را با قضیه مهم زیر به پایان می‌بریم. قضیه زیر نشان می‌دهد که چگونه برای هر عدد صحیح n و هر عدد اول p یک میدان متناهی با p^n عضو بسازییم.

قضیه ۷.۸.۲. *فرض کنیم n عدد طبیعی و $P(x)$ چندجمله‌ای تکین تحویل ناپذیر از درجه n در $\mathbb{Z}_p[x]$ باشد. در این صورت حلقه $\mathbb{Z}_p[x]/ < P(x) >$ یک میدان از مرتبه p^n است.*

اثبات. چون $\mathbb{Z}_p$ میدان است طبق قضیه ۵.۵.۲، یک دامنه ایده‌آل اصلی است. حال نشان می‌دهیم که $< P(x) >$ ایده‌آل ماکسیمال است. فرض کنیم که $< P(x) > \subseteq N$. چون $\mathbb{Z}_p[x]$ دامنه ایده‌آل اصلی است پس $N =< Q(x) >$. در نتیجه $P(x) = F(x)Q(x)$ که $F(x) \in \mathbb{Z}_p[x]$. چون $P(x)$ تحویل ناپذیر است پس $F(x)$ یا $Q(x)$ یکال است. اگر $F(x)$ یکال باشد آنگاه $N =< Q(x) >$. اگر $Q(x)$ یکال باشد آنگاه $N = \mathbb{Z}_p[x]$. یعنی $< P(x) >$ ایده‌آل ماکسیمال است. حال طبق قضیه ۷.۲.۲، $\mathbb{Z}_p[x]/ < P(x) >$ میدان است. اما عناصر میدان $\mathbb{Z}_p[x]/ < P(x) >$ طبق قضیه الگوریتم تقسیم، ۱۶.۳.۲، به شکل

$$\bar{a}_0 + \bar{a}_1 x + ... + \bar{a}_{n-1} x^{n-1}$$

است که $\bar{a}_i \in \mathbb{Z}_p$ و چون انتخاب ما برای هر $\bar{a}_i \in \mathbb{Z}_p$ برابر p است پس تعداد عناصر F برابر p^n می‌باشد و اثبات کامل است. □

تمرین حل شده

تمرین ۸.۸.۲. *فرض کنیم F یک میدان متناهی از مرتبه p^n باشد نشان دهید که*

$$f(x) = x^{p^n} - x = \prod_{a \in F} (x - a).$$

اثبات. طبق قضیه کوچک فرما، برای هر $a \in F$ داریم $a^{p^n} = a$ (تساوی را در حلقه $\mathbb{Z}_p$ نوشته‌ایم که میدان اول F است). پس هر $a \in F$ ریشه چندجمله‌ای $f(x)$ است. حال طبق نتیجه ۲۰.۳.۲، هر $a \in F$ داریم $x - a | f(x)$. چون تعداد عناصر F با درجه $f(x)$ برابر است رابطه

$$f(x) = x^{p^n} - x = \prod_{a \in F} (x - a)$$

نتیجه می‌شود. □

تمرین ۹.۸.۲. *یک میدان ۴ عضوی بسازیید و تمام عناصر آن را مشخص نمایید.*

اثبات. چند جمله‌ای $f(x) = x^۲ + x + ۱$ بوضوح تکین از درجه ۲ است و چون در $\mathbb{Z}_۲$ ریشه ندارد، طبق قضیه ۶.۷.۲، تحویل ناپذیرند. اکنون طبق قضیه ۷.۸.۲، $F = \mathbb{Z}_۲[x]/ < f(x) >$ میدان از مرتبه $۲^۲$ است. طبق اثبات قضیه ۷.۸.۲،

$$F = \{\bar{a}_۰ + \bar{a}_۱ x \mid \bar{a}_i \in \mathbb{Z}_۲\} = \{\bar{۰}, \bar{۱}, x, \bar{۱} + x\}$$

عناصر این میدان هستند. □

تمرین ۱۰.۸.۲. *نشان دهید که در یک میدان F با مشخصه p برای هر دو عنصر x و y در F همواره داریم $(x+y)^p = x^p + y^p$ و $(xy)^p = x^p y^p$.*

اثبات. می‌دانیم که بسط دو جمله‌ای در یک حلقه جابجایی بر قرار است. حال مشخصه p است یعنی برای هر عنصر $f \in F$ داریم $pf = ۰$. پس

$$(x+y)^p = x^p + px^{p-۱}y + \ldots + pxy^{p-۱} + y^p = x^p + y^p.$$

قسمت دوم از این که هر میدان جابجایی است به راحتی به دست می‌آید. □

تمرین ۱۱.۸.۲. *فرض کنیم F میدان متناهی با مشخصه p باشد. نشان دهید که هر عنصر a در F دارای ریشه pام یکتا در F است که آن را با $\sqrt[p]{a}$ نشان می‌دهیم.*

اثبات. رابطه

$$f : F \longrightarrow F, \quad f(x) = x^p$$

طبق تمرین ۱۰.۸.۲، یک همریختی حلقه‌ای ناصفر است. چون میدان دو ایده‌آل بیشتر ندارد و f ناصفر است باید $Ker f =< ۰ >$ باشد. یعنی f یک به یک است. از طرفی F متناهی است پس f پوشا نیز می‌باشد. حال برای هر عنصر a در F عنصر $b \in F$ چنان وجود دارد که $b^p = f(b) = a$. چون f یک به یک است این b یکتا است که آن را با $\sqrt[p]{a}$ نشان می‌دهیم و اثبات کامل است. □

تمرین ۱۲.۸.۲. *در حلقه $\mathbb{Z}_۲[x]$ دو چند جمله‌ای تحویل ناپذیر تکین درجه ۳ بیابید و سپس دو میدان ۸ عضوی بسیازید.*

اثبات. دو چند جمله‌ای

$$f(x) = x^۳ + x + ۱, \quad g(x) = x^۳ + x^۲ + ۱$$

بوضوح تکین از درجه ۳ هستند و چون در $\mathbb{Z}_۲$ ریشه ندارند، طبق قضیه ۶.۷.۲، تحویل ناپذیرند. اکنون طبق قضیه ۷.۸.۲، $\mathbb{Z}_۲[x]/ < f(x) >$ و $\mathbb{Z}_۲[x]/ < g(x) >$ دو میدان از مرتبه $۲^۳$ هستند و مسئله حل است. □

تمرین ۱۳.۸.۲. *برای هر عدد اول p نشان دهید که* $p|[(p-۱)! + ۱]$.

اثبات. اگر $p = ۲$ آنگاه چیزی برای اثبات نداریم. فرض کنیم $p \neq ۲$ و $f(x) = x^p - x$ باشد یا به طور معادل در تمرین ۸.۸.۲، قرار داده‌ایم $n = ۱$ و $F = \mathbb{Z}_p$. طبق همان تمرین ۸.۸.۲، داریم

$$f(x) = x^p - x = \prod_{a \in \mathbb{Z}_p} (x - a) = (x - \bar{۰})(x - \bar{۱})...(x - \overline{p-۱}).$$

با متحد قرار دادن هم درجه‌ها داریم

$$-x = [-\bar{۱} \times -\bar{۲} \times ... \times -\overline{p-۱}]x.$$

پس

$$-\bar{۱} = -\bar{۱} \times -\bar{۲} \times ... \times -\overline{p-۱}.$$

یعنی

$$(p-۱)! + ۱ \overset{p}{\equiv} ۰$$

و اثبات کامل است. □

۹.۲ تاریخچه

نظریه حلقه از نظر تاریخی، پیشینه‌ایی طولانی دارد. شاید اولین حلقه از نظر تاریخی که کشف شد همان حلقه اعداد صحیح باشد. معادله سیاله یا معادلهٔ دیوفانتی در ریاضیات معادله‌ای چند جمله‌ای با متغیرهای صحیح است که در آن بیش از یک متغیر (مجهول) داشته باشیم. حل این معادلات در زمان‌های قدیم در حلقه اعداد صحیح مورد توجه بوده است.

مطالعه به شکل امروزی نظریه حلقه با کارهای عمیق ریاضیدانانی چون گالوا در اوایل قرن نوزدهم شروع شد و سبب پیدایش نظریه‌ی میدان شد. گالوا کارهای عمیقی در نظریه میدان انجام داده است و دو شاخه مهم جبر را به هم مربوط کرده است. قضیه اساسی گالوا ارتباطی بین نظریه گروه و نظریه میدان به دست می‌دهد. اما در حدود همان سال‌های حیات گالوا مطالعه حلقه‌های جبری اعداد توسط ریاضیدانانی شاخص چون گاوس، کومر و ددکیند نیز آغاز شد. نظریه همنهشتی یا حساب پیمانه‌ای سیستمی برای محاسبه با اعداد صحیح است که به وسیله گاوس در کتاب رساله حساب در سال ۱۸۰۱ معرفی شد.

بخش دیگری از مطالعات روی نظریه حلقه‌ها، به ماتریس برمی‌گردد. پیشگامان مطالعه روی حلقه‌ی ماتریس‌ها ریاضیدانانی مانند کیلی، فروبنیوس و هامیلتون بودند. هامیلتون اولین شخصی است که توانست یک حلقه تقسیم (میدانی که شرط جابجایی ندارد) را بسازد و این باور را که حلقه ناجابجایی که نزدیک به میدان باشد وجود ندارد را نقض نمود. این کار هامیلتون سبب پیدایش شاخه جدیدی در نظریه حلقه شد. اما باور دیگری نیز وجود داشت که تنها حلقه‌های ناجابجایی حلقه ماتریس‌ها است. حتی حلقه ناجابجایی هامیلتون نیز به نوعی زیر حلقه‌ای از حلقه ماتریس‌ها روی میدان اعداد مختلط بود. این باور نیز توسط جبردان‌ها نقض شد. جبردان‌های مثل نوتر و ویل در کارهای عمیقی توانستند حلقه‌های ناجابجایی غیر از حلقه مانریس‌ها بسازند. این حلقه‌ها که حلقه‌های چندجمله با روابط خیلی خاص بودن مورد توجه ریاضیدان‌ها قرار گرفتند.

پژوهش روی نظریه حلقه هنوز ادامه دارد و مسایل حل نشده بسیاری در این شاخه مطرح است که برخی از آنها حتی ارتباط بسیاری نزدیکی با شاخه‌های دیگر مثل نظریه اعداد دارند. پژوهش‌های جدید خیلی تخصصی‌تر شده‌اند و بدون گذراندن درس‌های تخصصی این رشته مطالعه مقالات مرتبط دشوار است. اکنون دو شاخه مهم در نظریه حلقه وجود دارد که به حلقه‌های جابجایی و حلقه‌های ناجابجایی نامگذاری شده‌اند. گاهی مرز این دو زیر شاخه به شدت به هم نزدیک می‌شود و گاهی بسیار از هم فاصله می‌گیرند. نظریه‌های جدیدی نیز برای مطالعه حلقه‌ها ایجاد شده است که به شناسایی حلقه‌ها کمک می‌کند مانند نظریه مدول.

۱۰.۲ تمرین‌ها

تمرین ۱.۱۰.۲. *فرض کنیم $R_۱$ ، ...، R_n حلقه باشند. صورت تمام ایده‌آل‌های اول و ماکسیمال حلقه $R_۱ \times ... \times R_n$ را به دست آورید.*

تمرین ۲.۱۰.۲. *نشان دهید که برای حلقه‌های R و S، ایده‌آل‌های I و J به ترتیب از R و S، همواره داریم*

$$\frac{R \times S}{I \times J} \cong \frac{R}{I} \times \frac{S}{J}.$$

تمرین ۳.۱۰.۲. *نشان دهید که هر عنصر پوچتوان در حلقه R عضوی از اشتراک تمام ایده‌ال‌های اول R است.*

تمرین ۴.۱۰.۲. *برای دو ایده‌آل ماکسیمال مجزا از هم M و N از حلقه R نشان دهید که همواره داریم $MN = M \cap N$.*

تمرین ۵.۱۰.۲. *نشان دهید که همواره برای حلقه R یک میدان F چنان موجود است که یک همریختی حلقه‌ای پوشا از R به F وجود دارد.*

تمرین ۶.۱۰.۲. (**) *تمام ایده‌آل‌های ماکسیمال حلقه تمام توابع پیوسته حقیقی مقدار بر بازه واحد بسته $[۰, ۱]$ را شناسایی کنید.*

تمرین ۷.۱۰.۲. *فرض کنیم R دامنه صحیح باشد نشان دهید برای هر $f(x), g(x) \in R[x]$ داریم که $deg(f(x)g(x)) = deg(f(x)) + deg(g(x))$.*

تمرین ۸.۱۰.۲. *فرض کنیم R یک میدان باشد. آیا $R[x]$ یک میدان است؟ برای پاسخ خود دلیل بیاورید.*

تمرین ۹.۱۰.۲. *فرض کنیم I یک ایده‌آل R باشد. نشان دهید $I[x]$ ایده‌آل $R[x]$ است. با یک مثال نشان دهید که اگر J ایده‌آلی از $R[x]$ باشد لزومی ندارد که ایده‌آل I از R موجود باشد به طوری که $J = I[x]$.*

تمرین ۱۰.۱۰.۲. (*) *نشان دهید که $f(x) = r_n x^n + ... + r_۰$ در $R[x]$ یکال است اگر و تنها اگر $r_۰$ در R یکال و $r_۱$، ...، r_n در R پوچتوانند. سپس یکال‌های $\mathbb{Z}[x]$ و $\mathbb{Z}_۴[x]$ را معلوم کنید.*

تمرین ۱۱.۱۰.۲. *فرض کنیم I یک ایده‌آل از R باشد. نشان دهید که $R[x]/I[x] \cong (R/I)[x]$.*

تمرین ۱۲.۱۰.۲. *فرض کنیم R دامنه صحیح باشد و $f(x), g(x) \in R[x]$. اگر $g(x) \neq ۰$، $deg(f(x)) = n$، $deg(g(x)) = m$، s_m ضریب پیشرو $g(x)$ و*

$$k = min\{n - m + ۱, ۰\}$$

باشد آنگاه چندجمله‌ای‌های یکتای مانند $q(x)$ و $r(x)$ چنان وجود دارند که

$$s_m^k f(x) = q(x)g(x) + r(x), \;\; deg(r(x)) < deg(g(x)).$$

این تمرین را با قضیه الگوریتم تقسیم، قضیه ۱۶.۳.۲ ، مقایسه کنید.

تمرین ۲.۱۰.۱۳. *نشان دهید که اگر حلقه R میدان نباشد آنگاه برای هر ایده‌آل سره I از R هرگز ایده‌آل $I[x]$ از حلقه $R[x]$ ایده‌آل ماکسیمال نیست.*

تمرین ۲.۱۰.۱۴. *یکال‌های حلقه $\mathbb{Z}[i]$ را معلوم کنید.*

تمرین ۲.۱۰.۱۵. *نشان دهید هر ایده‌آل اول در حلقه دامنه اقلیدسی ماکسیمال است.*

تمرین ۲.۱۰.۱۶. *در هر حلقه دامنه اقلیدسی R نشان دهید که برای عنصر ناصفر x داریم $v(x) = v(-x)$.*

تمرین ۲.۱۰.۱۷. *نشان دهید که $\mathbb{Z}[\sqrt{۲}] = \{a + b\sqrt{۲} \mid a, b \in \mathbb{Z}\}$ یک دامنه اقلیدسی است.*

تمرین ۲.۱۰.۱۸. *یک دامنه صحیح مثال بزنید که دامنه اقلیدسی نباشد.*

تمرین ۲.۱۰.۱۹. *نشان دهید شریک یک عنصر تحویل ناپذیر، تحویل ناپذیر است.*

تمرین ۲.۱۰.۲۰. *نشان دهید ۳ در حلقه $\mathbb{Z}[i\sqrt{۵}]$ اول نیست.*

تمرین ۲.۱۰.۲۱. *نشان دهید که $۱ + i$ در حلقه $\mathbb{Z}[i]$ تحویل ناپذیر است*

تمرین ۲.۱۰.۲۲. *نشان دهید که $۲ + i\sqrt{۵}$ در حلقه $\mathbb{Z}[i\sqrt{۵}]$ تحویل ناپذیر است.*

تمرین ۲.۱۰.۲۳. *نشان دهید که $۲ + \sqrt{-۵}$ در حلقه $\mathbb{Z}[\sqrt{-۵}]$ تحویل ناپذیر است اما اول نیست.*

تمرین ۲.۱۰.۲۴. *در دامنه ایده‌آل اصلی R موارد زیر معادل هستند.*
(۱) عنصر ناصفر a اول است.
(۲) عنصر ناصفر a تحویل ناپذیر است.
(۳) Ra اول است.
(۴) Ra ماکسیمال است.

تمرین ۲.۱۰.۲۵. *نشان دهید در هر دامنه ایده‌آل اصلی هر ایده‌آل حاصل ضرب متناهی از ایده‌آل‌های اول است.*

تمرین ۲.۱۰.۲۶. *نشان دهید که همواره در حلقه R عنصر $c(a, b)$ و (ca, cb) شریک هستند.*

تمرین ۲.۱۰.۲۷. *نشان دهید در حلقه $\mathbb{Z}[\sqrt{-۳}]$ داریم*

$$(۱ + \sqrt{-۳}, ۱ - \sqrt{-۳}) = ۱.$$

تمرین ۲.۱۰.۲۸. *در حلقه $\mathbb{Z}[i]$ بزرگترین مقسوم علیه مشترک $۱۱i + ۱۰$ و $۸ + i$ را بیابید.*

تمرین ۲.۱۰.۲۹. *نشان دهید $\mathbb{Z}[i\sqrt{۶}]$ دامنه تجزیه یکتا نیست.*

تمرین ۲.۱۰.۳۰. *(*) نشان دهید در حلقه $\mathbb{Z}[\sqrt{۲}]$ هیچ عنصر یکالی بین ۱ و $\sqrt{۲} + ۱$ نیست.*

تمرین ۳۱.۱۰.۲. *فرض کنیم $f(x) \in \mathbb{Z}[x]$ از درجه $n > 1$ باشد. اگر عدد اول p چنان موجود باشد که $\overline{f}(x) \in \mathbb{Z}_p[x]$ تحویل ناپذیر باشد و به علاوه $deg(f(x)) = deg(\overline{f(x)})$ آنگاه $f(x)$ روی $\mathbb{Q}[x]$ تحویل ناپذیر است.*

تمرین ۳۲.۱۰.۲. *اگر p عددی اول باشد نشان دهید که $f_p(x) = x^{p-1} + ... + x + 1$ روی $\mathbb{Q}$ تحویل ناپذیر است.*

تمرین ۳۳.۱۰.۲. *تمام چندجمله‌ای‌های تحویل ناپذیر از درجه ۳ را روی $\mathbb{Z}_2$ مشخص کنید.*

تمرین ۳۴.۱۰.۲. *تمام چندجمله‌ای‌های تحویل ناپذیر از درجه ۴ را روی $\mathbb{Z}_2$ مشخص کنید.*

تمرین ۳۵.۱۰.۲. *نشان دهید $x^4 + 8$ روی $\mathbb{Q}$ تحویل ناپذیر است.*

تمرین ۳۶.۱۰.۲. *نشان دهید که $x^3 + \bar{3}x + \bar{2} \in \mathbb{Z}_7[x]$ روی $\mathbb{Z}_7$ تحویل ناپذیر است.*

تمرین ۳۷.۱۰.۲. *تمام چندجمله‌ای‌های تحویل ناپذیر درجه ۲ که تکین هستند را روی $\mathbb{Z}_p$ معلوم کنید.*

تمرین ۳۸.۱۰.۲. *روی $\mathbb{Z}_3$ یک چندجمله‌ای درجه ۲ تحویل ناپذیر بیابید.*

تمرین ۳۹.۱۰.۲. *نشان دهید که $x^n + 2$ برای $n > 1$ روی $\mathbb{Z}[x]$ تحویل ناپذیر است.*

تمرین ۴۰.۱۰.۲. *نشان دهید که چندجمله‌ای $x^2 + \frac{1}{3}x - \frac{2}{5}$ روی $\mathbb{Q}[x]$ تحویل ناپذیر است.*

تمرین ۴۱.۱۰.۲. *یک چندجمله‌ای تحویل ناپذیر مانند $f(x)$ روی $\mathbb{Z}[x]$ مثال بزنید که $\overline{f(x)}$ در $\mathbb{Z}_2[x]$ تحویل پذیر باشد.*

تمرین ۴۲.۱۰.۲. *برای عدد طبیعی m نشان دهید که اگر $f(x) \in \mathbb{Z}_p[x]$ در این صورت داریم $f(x^{p^m}) = (f(x))^{p^m}$.*

تمرین ۴۳.۱۰.۲. *یک میدان با ۹ عضو بسازید. تمام اعضای میدان را بنویسید.*

تمرین ۴۴.۱۰.۲. *آیا یک میدان ۳۴۳ عضوی وجود دارد؟ پاسخ خود به صورت کامل شرح دهید.*

تمرین ۴۵.۱۰.۲. *(*) گروه ضربی عناصر ناصفر یک میدان متناهی دوری است.*

تمرین ۴۶.۱۰.۲. *نشان دهید که هر دو میدان متناهی با تعداد عنصرهای یکسان با هم یکریخت هستند.*

کتاب‌نامه

[1] Bhattacharya, P. B.; Jain, S. K.; Nagpaul, S. R. Basic abstract algebra. Second edition. Cambridge University Press, Cambridge, 1994.

[2] Herstein, I. N. Abstract algebra. Third edition. With a preface by Barbara Cortzen and David J. Winter. Prentice Hall, Inc., Upper Saddle River, NJ, 1996.

[3] Hungerford, Thomas W. Algebra. Reprint of the 1974 original. Graduate Texts in Mathematics, 73. Springer-Verlag, New York-Berlin, 1980.

[4] Malik, D.S.; Mordeson, J.N.; Sen, M.K. Fundamentals of abstract algebra. McGraw-Hill, 1997.