فصل دهم

مقدمه‌ای بر نظریه حلقه‌ها

در فصل‌های پیشین، دستگاههای ریاضی را با یک عمل دوتایی مورد مطالعه قرار دادیم. دستگاههای ریاضی زیادی با دو عمل دو تایی موسوم به حلقه وجود دارند. مفهوم یک حلقه حاصل از چنین دستگاههای ریاضی مانند اعداد صحیح، اعداد گویا، اعداد حقیقی، و اعداد مختلط است.

اگرچه دیوید هیلبرت نام «حلقه» را رواج داد، اما امیل نوتر بود که تحت تأثیر هیلبرت، اصولی را برای حلقه‌ها پایه‌ریزی کرد. در سال ۱۹۱۴، فرانکل تعریفی اولیه را از حلقه ارائه کرد. به هر حال، مدت مدیدی از کاربرد عمومی آن نمی‌گذرد.

همچنان که خواهید دید، حلقه ترکیبی خاص از یک گروه و یک نیم گروه می‌باشد. از این رو، مطالب قبلی در توصیف حلقه‌ها مفید واقع خواهند شد. به هر حال، ارائه مجموعه‌ای با دو عمل دوتایی مستقل کافی نمی‌باشد. به منظور به دست آوردن ساختار کامل اصل موضوعی، نیاز به وابستگی ما بین دو عمل - به ویژه قوانین پخشی است.

۱۰۰۱ خاصیت‌های مقدماتی

این بخش مشابه فصل ۲ است. ابتدا تعریفی از یک حلقه به دست می‌دهیم، سپس مثال‌ها و خواص مقدماتی آن را دنبال می‌کنیم. در ادامه چندین نماد و تعریف را معرفی می‌کنیم که در سر تا سر کتاب به کار می‌روند.

دو عمل دوتایی که روی مجموعه‌ای ناتهی در نظر گرفته می‌شوند معمولاً با + (جمع) و · (ضرب) نشان داده می‌شود.

یک حلقه، دستگاه ریاضی $(R, +, \cdot)$ است به طوری که $(R, +)$ گروهی تعویض پذیر، $(R, \cdot)$ یک نیم گروه می‌باشد، و قوانین پخشی برقرارند، یعنی به ازای هر $a, b, c \in R$ ،

$$a\cdot(b+c)=(a\cdot b)+(a\cdot c)\ ,$$
$$(b+c)\cdot a=(b\cdot a)+(c\cdot a)\ .$$

عنصر خنثای $(R,+)$ را با نماد ۰ نشان می‌دهیم. معکوس جمعی عنصر $a\in R$ با $-a$ نشان داده می‌شود.

حال تعریفی کامل از یک حلقه را ارائه می‌دهیم.

تعریف ۱۰.۱۰ یک حلقه عبارت است از سه تایی مرتب $(R,+,\cdot)$ به طوری که R مجموعه‌ای ناتهی است و $+$ و $\cdot$ دو عمل دوتایی روی R هستند که در شرایط زیر صدق می‌کنند.

(R۱) به ازای هر $a,b,c\in R$، $(a+b)+c=a+(b+c)$.

(R۲) به هر $a,b\in R$، $a+b=b+a$.

(R۳) عنصری مانند ۰ در R وجود دارد به طوری که به ازای هر $a\in R$، $a+0=a$.

(R۴) به ازای هر $a\in R$، عنصری مانند $-a\in R$ وجود دارد به طوری که $a+(-a)=0$.

(R۵) به ازای هر $a,b,c\in R$، $(a\cdot b)\cdot c=a\cdot(b\cdot c)$.

(R۶) به ازای هر $a,b,c\in R$، $a\cdot(b+c)=(a\cdot b)+(a\cdot c)$.

(R۷) به ازی هر $a,b,c\in R$، $(b+c)\cdot a=(b\cdot a)+(c\cdot a)$.

۰ را عنصر صفر حلقه $(R,+,\cdot)$ می‌نامیم.

در طی توسعهٔ نظریه حلقه‌ها، قراردادهای زیر را به کار خواهیم برد.

۱. اجرای ضرب بر عمل جمع مقدم انجام می‌شود.

۲. به جای $a\cdot b$ می‌نویسیم ab.

۳. به جای $a+(-b)$ می‌نویسیم $a-b$.

۴. $(R,+,\cdot)$ را به صورت حلقه R می‌نویسیم.

بنابراین، نماد $ab+c$ به جای $(a\cdot b)+c$، $ab+ac$ به جای $(a\cdot c)+(a\cdot c)$، $ab-ba$ به جای $(a\cdot b)+(-(a\cdot c))$ به کار می‌رود، که در آن $a,b,c\in R$.

مثال ۲۰.۱۰ مجموعهٔ اعداد صحیح $\mathbf{Z}$ را با عمل‌های جمع، $+$، و ضرب، $\cdot$، معمولی در نظر بگیرید. بنابراین مثال ۳.۱.۲، $(\mathbf{Z},+)$ یک گروه است. حال حاصلضرب دو عدد صحیح، عددی است صحیح و خاصیت شرکت‌پذیری برای $\cdot$ برقرار است. سرانجام، می‌دانیم که قوانین پخشی برای اعداد صحیح برقرارند. بنابراین، $(\mathbf{Z},+,\cdot)$ یک حلقه است.

مثال ۲۰.۱۰، حلقه اعداد صحیح نامیده می‌شود. این حلقه نقشی مهم در نظریه حلقه‌ها ایفا می‌کند. یکی از مسائل اساسی در نظریه حلقه‌ها، تعیین حلقه‌هایی است که خواصی مشابه

خواص حلقه اعداد صحیح دارند.

تعریف ۳۰۱۰۱۰ حلقه R تعویض پذیر نامیده می‌شود هرگاه به ازای هر $a,b\in R$، $ab=ba$. حلقه‌ای را که تعویض‌پذیر نباشد حلقه تعویض ناپذیر می‌نامند.

از تعریف فوق، نتیجه می‌شود که حلقه R تعویض پذیر است اگر و تنها اگر نیم گروه $(R,\cdot)$ تعویض‌پذیر باشد. حلقه اعداد صحیح، حلقه‌ای تعویض پذیر است.

برای یک حلقه $C(R)=\{a\in R\,|\,ab=ba\ ،b\in R$ به ازای هر$\}$، مرکز R نامیده می‌شود. نتیجه می‌شود که حلقه R تعویض پذیر است اگر و تنها اگر $C(R)=R$.

مثال ۴۰۱۰۱۰ فرض کنید $M_2(\mathbf{Z})$ مجموعه تمام ماتریس های 2×2 روی حلقه اعداد صحیح باشد. همچنین فرض کنید $+$ و $\cdot$ به ترتیب اعمال جمع و ضرب معمولی ماتریس را نشان دهند. چون جمع (ضرب) ماتریس 2×2 روی $\mathbf{Z}$ مجدداً یک ماتریس 2×2 روی $\mathbf{Z}$ است، لذا $+$ و اعمال دوتایی روی $M_2(\mathbf{Z})$ می‌باشند. حال به آسانی می‌توان نشان داد که $(M_2(\mathbf{Z}),+,\cdot)$ تشکیل یک حلقه می‌دهد. حال به ازای ماتریسهای $\begin{bmatrix}5&6\\7&8\end{bmatrix},\begin{bmatrix}1&2\\3&4\end{bmatrix}\in M_2(\mathbf{Z})$، ملاحظه می‌شود که

$$\begin{bmatrix}1&2\\3&4\end{bmatrix}\begin{bmatrix}5&6\\7&8\end{bmatrix}=\begin{bmatrix}19&22\\43&50\end{bmatrix}\neq\begin{bmatrix}23&34\\31&46\end{bmatrix}=\begin{bmatrix}5&6\\7&8\end{bmatrix}\begin{bmatrix}1&2\\3&4\end{bmatrix}.$$

بنابراین، $M_2(\mathbf{Z})$ یک حلقه تعویض پذیر نیست.

در حلقه R، عنصر $e\in R$ را عنصر همانی نامند هرگاه به ازای هر $a\in R$، $ea=a=ae$. عنصر همانی حلقه R (در صورت وجود)، عنصر همانی نیم گروه $(R,\cdot)$ است. بنابراین، یک حلقه نمی‌تواند شامل بیش از یک عنصر همانی باشد (قضیه ۱۱۰۶۰۱). عنصر همانی حلقه (در صورت وجود) با ۱ نشان داده می‌شود.

تعریف ۵۰۱۰۱۰ حلقه R را حلقه یکدار نامند هرگاه دارای عنصر همانی باشد.

مثال ۶۰۱۰۱۰ حلقه اعداد صحیح $\mathbf{Z}$ حلقه‌ای یکدار است. عدد صحیح ۱ عنصر همانی $\mathbf{Z}$ است.

مثال ۷۰۱۰۱۰ حلقه $M_2(\mathbf{Z})$ در مثال ۴۰۱۰۱۰ حلقه‌ای یکدار است. عنصر همانی $M_2(\mathbf{Z})$ برابر است با $\begin{bmatrix}1&0\\0&1\end{bmatrix}$.

مثال ۸۰۱۰۱۰ فرض کنید R مجموعه تمام توابع $f:\mathbf{R}\to\mathbf{R}$ باشد. به ازای هر $f,g\in R$ و هر $a\in R$، اعمال $+$ و $\cdot$ را روی R به صورت زیر تعریف کنید.

$$(f+g)(a)=f(a)+g(a),$$
$$(f\cdot g)(a)=f(a)\cdot g(a).$$

از تعریف + و ·، نتیجه می‌شود که + و · اعمال دوتایی روی R هستند. فرض کنید $f,g,h\in R$. در این صورت به ازای هر $a\in \mathbf{R}$، با استفاده از خاصیت شرکت پذیری روی $\mathbf{R}$ داریم:

$$\begin{aligned}((f+g)+h)(a) &= (f+g)(a)+h(a) = (f(a)+g(a))+h(a)\\ &= f(a)+(g(a)+h(a)) = f(a)+(g+h)(a)\\ &= (f+(g+h))(a)\end{aligned}$$

بنابراین، $(f+g)+h=f+(g+h)$. این نشان می‌دهد که + شرکت پذیر است. در روندی مشابه، می‌توان نشان داد که سایر خواص یک حلقه برای R برقرارند، با استفاده از این حقیقت که آنها برای $\mathbf{R}$ نیز برقرارند. بنابراین $(R,+,\cdot)$ تشکیل یک حلقه می‌دهد. توجه می‌کنیم که تابع $i_0:\mathbf{R}\to\mathbf{R}$ که در آن به ازای هر $a\in R$، $i_0(a)=0$، خنثای جمعی و عنصر $i_1\in R$ که در آن به ازای هر $a\in R$، $i_1(a)=a$ عنصر همانی R هستند. همچنین، به ازای هر $f,g\in R$، و هر $a\in \mathbf{R}$، $(f\cdot g)(a)=f(a)g(a)=g(a)f(a)=(g\cdot f)(a)$. بنابراین، به ازای هر $f,g\in R$، $f.g=g.f$. در نتیجه، $(R,+,\cdot)$ حلقه‌ای یکدار تعویض پذیر است.

جمع و ضرب روی R در مثال ۸۰۱۰۱۰ همان اعمالی هستند که دانش آموزان در حسابان می‌آموزند.

مثال ۹۰۱۰۱۰ فرض کنید $(G,*)$ گروهی تعویض‌پذیر و $Hom(G,G)$ مجموعهٔ تمام همریختی‌های از G به توی خودش باشد. حال ترکیب دو همریختی از G مجدداً یک همریختی از G می‌باشد و لذا o یک عمل دوتایی روی $Hom(G,G)$ است. همچنین، بنابر قضیه ۱۳.۵.۱، عمل o شرکت‌پذیر است و $i_G\in Hom(G,G)$ عنصر همانی است. بنابراین، $(Hom(G,G),o)$ تشکیل یک نیم گروه با عنصر همانی می‌دهد. حال به تعریف عمل + مناسبی روی $Hom(G,G)$ می‌پردازیم به طوری که $(Hom(G,G),o,+)$ حلقه‌ای یکدار شود. به ازای هر $f,g\in Hom(G,G)$، عمل + را روی $Hom(G,G)$ به صورت زیر تعریف کنید:

$$(f+g)(a)=f(a)*(g(a),$$

که در آن $a\in G$. فرض کنید $f,g\in Hom(G,G)$. از تعریف + نتیجه می‌شود که $f+g$ نگاشتی از G به توی G است. فرض کنید $a,b\in R$. در این صورت

$$\begin{aligned}(f+g)(ab) &= f(ab)*g(ab)\\ &= (f(a)*f(b))*(g(a)*g(b))\\ &= f(a)*g(a)*f(b)*g(b)\\ &= (f+g)(a)*(f+g)(b).\end{aligned}$$

این نشان می‌دهد که $f+g$ یک همریختی از G به توی G است. از بررسی شرکت پذیری $+$ صرفنظر می‌کنیم. عنصر همانی $(Hom(G,G),+)$ عبارت است از همریختی که هر عنصر G را به روی عنصر همانی G می‌نگارد. به ازای هر $f\in Hom(G,G)$، نگاشت $-f$ که به ازای هر $a\in G$ به صورت $(-f)(a)=f(a)^{-1}$ تعریف می‌شود، معکوس جمعی f است. بنابراین $(Hom(G,G),+)$ تشکیل یک گروه می‌دهد. حال نشان می‌دهیم که قوانین پخشی برقرارند. به ازای هر $a\in G$ و هر $f,g,h\in Hom(G,G)$،

$$[fo(g+h)](a)=f((g+h)(a))=f(g(a)*h(a))=f(g(a))*f(h(a))$$
$$=(fog)(a)*(foh)(a)=(fog+foh)(a).$$

از این رو، $fo(g+h)=(fog)+(foh)$. به طور مشابه قانون پخشی از راست برقرار است. در نتیجه $(Hom(G,G),+,o)$ تشکیل یک حلقه می‌دهد.

اکنون بعضی خواص مقدماتی حلقه‌ها را اثبات می‌کنیم.

قضیه ۱۰.۱.۱۰ فرض کنید R یک حلقه باشد و $a,b,c\in R$. در این صورت

(i) $a0=0a=0$،

(ii) $a(-b)=(-a)b=-(ab)$،

(iii) $(-a)(-b)=ab$،

(iv) $a(b-c)=ab-ac$ و $(b-c)a=ba-ca$.

اثبات. (i) واضح است که $a0=a(0+0)=a0+a0$. بنابراین، $(a0+a0)+(-(a0))=a0+(-(a0))$ و لذا $a0+(a0+(-(a0)))=0$. از این رو، $a0+0=0$ یا $a0=0$. به طور مشابه، $0a=0$.

(ii) $ab+a(-b)=a(b+(-b))=a0=0=0a=(-b+b)a=a(-b)+ab$.
چون معکوس جمعی یک عنصر یکتاست، لذا $a(-b)=-(ab)$. به طور مشابه، $(-a)b=-(ab)$.

(iii) با استفاده از (ii) داریم:

$$(-a)(-b)=-(a(-b))=-(-ab)=ab.$$

(iv) چون $b-c=b+(-c)$، لذا

$$a(b-c)=a(b+(-c))=ab+a(-c)=ab+(-ac)\ ((ii)\text{ بنابر})=ab-ac.$$

به طور مشابه، $(b-c)a=ba-ca$. ■

نتیجه ۱۱.۱.۱۰ فرض کنید R حلقه‌ای یکدار باشد. در این صورت $R\neq\{0\}$ اگر و تنها

اگر عناصر ۰ و ۱ متمایز باشند.

اثبات. فرض کنید $R \neq \{0\}$. همچنین فرض کنید که $a \in R$ به قسمی باشد که $a \neq 0$. فرض کنید $1 = 0$. در این صورت $a = a1 = a0 = 0$، که یک تناقض است. بنابراین $1 \neq 0$. عکس نتیجه برقرار است زیرا R دارای حداقل دو عنصر متمایز ۰ و ۱ است. ■

قرارداد: از این به بعد، فرض می‌کنیم که عنصر همانی ۱ (در صورت وجود) از عنصر صفر حلقه متفاوت است. از این قرارداد، نتیجه می‌شود که اگر R حلقه‌ای یکدار باشد، آنگاه R حداقل دو عنصر دارد.

فرض کنید R حلقه‌ای یکدار باشد. عنصر $u \in R$ را **یکه (یاعنصر وارون پذیر)** نامند هرگاه عنصر $v \in R$ وجودداشته باشدبه طوری که $uv = 1 = vu$. خواص زیررابرای عناصروارون‌پذیرداریم.

قضیه ۱۲۰۱۰۱۰ فرض کنید R حلقه‌ای یکدار و T مجموعه تمام یکه‌های R باشد. در این صورت

(i) $T \neq \varnothing$،

(ii) $0 \notin T$، و

(iii) به ازای هر $a, b \in T$، $ab \in T$.

اثبات. (i) چون $1 \cdot 1 = 1 = 1 \cdot 1$، لذا $1 \in T$. از این رو $T \neq \varnothing$.

(ii) فرض کنید $0 \in T$. در این صورت عنصر $v \in R$ وجود دارد به طوری که $0v = 1 = v0$. اما $0v = 0$ و لذا $1 = 0$، که یک تناقض است. بنابراین، $0 \notin T$.

(iii) فرض کنید $a, b \in T$. عناصر $c, d \in R$ وجود دارند به طوری که $ac = 1 = ca$ و $bd = 1 = db$. حال

$$(ab)(dc) = a(bd)c = a1c = ac = 1$$

و

$$(dc)(ab) = d(ca)b = d1b = db = 1.$$

از این رو، $(ab)(dc) = 1 = (dc)(ab)$. بنابراین، ab یکه است و لذا $ab \in T$. ■

تعریف ۱۳۰۱۰۱۰ (i) حلقه یکدار R را **حلقه تقسیم (میدان اریب)** نامند هرگاه هر عنصر ناصفر آن یکه باشد.

(ii) حلقه تقسیم تعویض پذیر R را **یک میدان** می‌نامند.

توجه کنید که حلقه R یک حلقه تقسیم (یا میدان اریب) است اگر و تنها اگر $(R \setminus \{0\}, \cdot)$ تشکیل یک گروه دهد. بنابراین، اگر R یک حلقه تقسیم باشد، آنگاه به ازای هر $a \in R$، $a \neq 0$، عنصر یکتای $a^{-1} \in R$ وجود دارد به طوری که $aa^{-1} = 1 = a^{-1}a$. عنصر a^{-1} را معکوس ضربی a می‌نامیم. به طور مشابه، حلقه R یک میدان است اگر و تنها اگر $(R \setminus \{0\}, \cdot)$ تشکیل یک گروه

تعویض پذیر دهد.

مثال ۱۴۰۱۰۱۰ (i) حلقه اعداد صحیح $\mathbf{Z}$ یک میدان نیست. در $\mathbf{Z}$، تنها عناصر وارون پذیر عبارتند از ۱ و ۱-.

(ii) از مثال ۳۰۱۰۲، نتیجه می‌شود که $(\mathbf{Q}, +, \cdot)$ یک میدان است، که درآن + و · به ترتیب جمع و ضرب معمولی هستند. $\mathbf{Q}$ را **میدان اعداد گویا** می‌نامند.

(iii) مثال ۳۰۱۰۲، نتیجه می‌دهد که $(\mathbf{R}, +, \cdot)$ یک میدان است، که درآن + و · به ترتیب جمع و ضرب معمولی هستند. $\mathbf{R}$ را **میدان اعداد حقیقی** می‌نامند.

(iv) از مثال ۳۰۱۰۲، نتیجه می‌شود که $(\mathbf{C}, +, \cdot)$ یک میدان است، که در آن + و · به ترتیب جمع و ضرب معمولی هستند. $\mathbf{C}$ را **میدان اعداد مختلط** می‌نامند.

مثال زیر به ویلیام روان هامیلتون William Rowan Hamilton منسوب است. در ارتباط با بحث فیزیکی، هاملیتون جبری را بنا کرد که قانون تعویض پذیری ضرب در آن برقرار نبود. در آن زمان، چنین ساختاری محال به نظر می‌رسید. کار وی و اچ.جی گراسمن H. G. Grassman روی دستگاههای اعداد ابر مختلط آغازی برای آزاد ساختن جبر بود. کار آنها دیگر ریاضیدانان را تشویق به ایجاد جبرهایی نمود، که باعث شکست سنت شد، به عنوان مثال، جبرهایی که درآنها $ab = 0$ در حالی که $a \neq 0$ و $b \neq 0$ و جبرهایی با $a^n = 0$، که $a \neq 0$ و n عددی صحیح و مثبت است.

مثال ۱۵۰۱۰۱۰ فرض کنید $\mathcal{Q}_{\mathbf{R}} = \{ (a_1, a_2, a_3, a_4) \mid a_i \in \mathbf{R}, i = 1, 2, 3, 4 \}$. روی $\mathcal{Q}_{\mathbf{R}}$ اعمال + و · را به صورت زیر تعریف کنید:

$$(a_1, a_2, a_3, a_4) + (b_1, b_2, b_3, b_4) = (a_1 + b_1, a_2 + b_2, a_3 + b_3, a_4 + b_4)$$

$$(a_1, a_2, a_3, a_4) \cdot (b_1, b_2, b_3, b_4) = (a_1 b_1 - a_2 b_2 - a_3 b_3 - a_4 b_4, a_1 b_2 + a_2 b_1 + a_3 b_4 - a_4 b_3, a_1 b_3 + a_3 b_1 + a_4 b_2 - a_2 b_4, a_1 b_4 + a_2 b_3 - a_3 b_2 + a_4 b_1).$$

از تعریف + و · نتیجه می‌شود که + و · اعمال دوتایی روی $\mathcal{Q}_{\mathbf{R}}$ هستند. حال + شرکت پذیر و تعویض پذیر است، زیرا + در $\mathbf{R}$ شرکت پذیر و تعویض پذیر است. همچنین توجه کنید که $(0, 0, 0, 0) \in \mathcal{Q}_{\mathbf{R}}$ عنصر خنثای جمعی است و اگر $(a_1, a_2, a_3, a_4) \in \mathcal{Q}_{\mathbf{R}}$، آنگاه

$$(-a_1, -a_2, -a_3, -a_4) \in \mathcal{Q}_{\mathbf{R}}$$

و

$$-(a_1, a_2, a_3, a_4) = (-a_1, -a_2, -a_3, -a_4).$$

از این رو، $(\mathcal{Q}_{\mathbf{R}}, +)$ تشکیل یک گروه تعویض پذیر می‌دهد. به طور مشابه، · شرکت‌پذیر است و $(1, 0, 0, 0) \in \mathcal{Q}_{\mathbf{R}}$ همانی ضربی است. فرض کنید $(a_1, a_2, a_3, a_4) \in \mathcal{Q}_{\mathbf{R}}$ عنصر ناصفر

باشد. در این صورت $N=a_1^2+a_2^2+a_3^2+a_4^2\neq 0$ و $N\in\mathbf{R}$. بنابراین،

$$\left(\frac{a_1}{N},\frac{-a_2}{N},\frac{-a_3}{N},\frac{-a_4}{N}\right)\in Q_{\mathbf{R}}\ .$$

از خواننده می‌خواهیم که تحقیق کند که عنصر

$$\left(\frac{a_1}{N},\frac{-a_2}{N},\frac{-a_3}{N},\frac{-a_4}{N}\right)$$

معکوس ضربی (a_1,a_2,a_3,a_4) است، بنابراین $Q_{\mathbf{R}}$ یک حلقه تقسیم است که آن را حلقه چهارگان‌های حقیقی می‌نامند. به هر حال، $Q_{\mathbf{R}}$ تعویض پذیر نیست، زیرا

$$(0,1,0,0)(0,0,1,0)=(0,0,0,1)\neq(0,0,0,-1)=(0,0,1,0)(0,1,0,0)\ .$$

بنابراین، $Q_{\mathbf{R}}$ نمی‌تواند یک میدان باشد.

عنصر ناصفر a در حلقه R را مقسوم علیه صفر نامند هر گاه عنصر $b\in R$ موجود باشد به طوری که $b\neq 0$ و یا $ab=0$ یا $ba=0$. عنصر ۰ را یک مقسوم علیه صفر نمی‌خوانیم. یک عنصر همزمان نمی‌تواند هم یکه و هم مقسوم علیه صفر باشد.(تمرین حل شده ۱، صفحه)

بنابراین، یک میدان دارای مقسوم علیه صفری نیست.

تعریف ۱۶۰۱۰۱۰ فرض کنید R حلقه‌ای تعویض پذیر و یکدار باشد. در این صورت $\mathbf{R}$ را **حوزه صحیح** نامند هرگاه R دارای هیچ مقسوم علیه صفری نباشد.

حلقه اعداد صحیح $\mathbf{Z}$ یک حوزه صحیح است. حلقه $M_2(\mathbf{Z})$ یک حوزه صحیح نیست، زیرا تعویض ناپذیر است. همچنین $M_2(\mathbf{Z})$ دارای مقسوم علیه‌های صفر است. به عنوان مثال

$$\begin{bmatrix}1&0\\0&0\end{bmatrix},\begin{bmatrix}0&1\\0&0\end{bmatrix}\in M_2(\mathbf{Z})\quad,\quad\begin{bmatrix}1&0\\0&0\end{bmatrix}\begin{bmatrix}0&1\\0&0\end{bmatrix}=\begin{bmatrix}0&0\\0&0\end{bmatrix}$$

توجه می‌کنیم که هر میدان F یک حوزه صحیح است، چون هر عنصر ناصفر F یکه است.

مثال ۱۷۰۱۰۱۰ $\mathbf{Z}[\sqrt{3}]=\{a+b\sqrt{3}\mid a,b\in\mathbf{Z}\}$ یک حوزه صحیح است، که در آن + و · عمل‌های معمولی جمع و ضرب هستند. $0+0\sqrt{3}$ خنثای جمع و $1+0\sqrt{3}$ همانی ضرب $\mathbf{Z}[\sqrt{3}]$ می‌باشند. فرض کنید $\sqrt{3}$ در $\mathbf{Z}[\sqrt{3}]$ یکه باشد. در این صورت به ازای $a,b\in\mathbf{Z}$ای، $(\sqrt{3})^{-1}=a+b\sqrt{3}$. اگر $a=0$، آنگاه $(\sqrt{3})^{-1}=b\sqrt{3}$ یا $1=3b$، که یک تناقض است، زیرا این معادله در $\mathbf{Z}$ دارای جواب نیست. بنابراین، $a\neq 0$ و لذا $1=a\sqrt{3}+3b$ یا $\sqrt{3}=\frac{1-3b}{a}\in\mathbf{Q}$، که یک تناقض است. از این رو، $\sqrt{3}$ یکه نیست. در نتیجه، $\mathbf{Z}[\sqrt{3}]$ یک میدان نخواهد بود.

با استدلال های مشابه استدلال به کار رفته در مثال ۱۷۰۱۰۱۰، می‌توان نشان داد که مجموعه‌های زیر تحت جمع و ضرب معمولی تشکیل یک حوزه صحیح می‌دهند.

$$\mathbf{Z}[\sqrt{n}] = \{a+b\sqrt{n} \mid a,b \in \mathbf{Z}\}$$
$$\mathbf{Z}[i\sqrt{n}] = \{a+bi\sqrt{n} \mid a,b \in \mathbf{Z}\}$$
$$\mathbf{Z}[i] = \{a+bi \mid a,b \in \mathbf{Z}\}$$
$$\mathbf{Q}[\sqrt{n}] = \{a+b\sqrt{n} / \mid a,b \in \mathbf{Q}\}$$
$$\mathbf{Q}[i\sqrt{n}] = \{a+bi\sqrt{n} \mid a,b \in \mathbf{Q}\}$$
$$\mathbf{Q}[i] = \{a+bi \mid a,b \in \mathbf{Q}\}$$

که در آن n عدد صحیح مثبت ثابتی است و $i^{۲} = -۱$. در واقع می‌توان نشان داد که $\mathbf{Q}[\sqrt{n}]$، $\mathbf{Q}[i\sqrt{n}]$، و $\mathbf{Q}[i]$ میدان هستند.

مثال ۱۸۰۱۰۱۰ حلقه اعداد صحیح زوج $\mathbf{E}$ حلقه‌ای تعویض پذیر، بدون یک و بدون مقسوم علیه صفر است.

حلقه ارائه شده در مثال زیر، گاهی اوقات در ساختن مثال‌های نقض مفید واقع می‌شود.

مثال ۱۹۰۱۰۱۰ فرض کنید $(R, +)$ گروهی تعویض پذیر باشد. به ازای هر $a,b \in R$، عمل ضرب را روی R به صورت $ab = ۰$ تعریف کنید، که در آن ۰ عنصر خنثای گروه $(R, +)$ می‌باشد. در این صورت $(R, +, \cdot)$ حلقه صفر نامیده می‌شود. اگر R شامل بیش از یک عنصر باشد، آنگاه R حلقه‌ای تعویض پذیر بدون ۱ است و هر عنصر ناصفر آن یک مقسوم علیه صفر می‌باشد.

قضیه زیر رابطه‌ای را بین مقسوم علیه‌های صفر و خاصیت حذف یک حلقه برقراری می‌کند.

قضیه ۲۰۰۱۰۱۰ فرض کنید R یک حلقه باشد. اگر R هیچ مقسوم علیه صفری نداشته باشد، آنگاه قوانین حذف برقرارند، یعنی به ازای هر $a,b,c \in R$، $a \neq ۰$، $ab = ac$ ایجاب می‌کند که $b = c$. (قانون حذف از چپ) و $ba = ca$ ایجاب می‌کند $b = c$ (قانون حذف از راست). اگر یکی از قوانین حذف برقرار باشد، آنگاه R دارای مقسوم علیه صفر نمی‌باشد.

اثبات. فرض کنید R دارای هیچ مقسوم علیه صفر نباشد. همچنین فرض کنید $a,b,c \in R$ به گونه‌ای باشند که $ab = ac$ و $a \neq ۰$. در این صورت $ab - ac = ۰$ یا $a(b-c) = ۰$. چون R هیچ مقسوم علیه صفری ندارد و $a \neq ۰$، داریم $b - c = ۰$ یا $b = c$. از این رو، قانون حذف از چپ برقرار است. به طور مشابه، قانون حذف از راست نیز برقرار است. بعکس، فرض کنید یکی از قوانین حذف مثلاً چپ برقرار باشد، یعنی اگر $a,b,c \in R$، $a \neq ۰$، آنگاه $ab = ca$ ایجاب کند $b = c$. فرض کنید a عنصری ناصفر از R باشد و $b \in R$. همچنین فرض کنید $ab = ۰$. در این صورت $ab = a۰$. با حذف a، داریم $b = ۰$. حال فرض کنید $ba = ۰$ و $b \neq ۰$. در این صورت $ba = b۰$ و با حذف b به دست می‌آوریم $a = ۰$، که یک تناقض است. بنابراین $b = ۰$. از این رو، R دارای مقسوم علیه صفر

نمی‌باشد. به طور مشابه، قانون حذف از راست ایجاب می‌کند که R دارای هیچ مقسوم علیه صفر نیست. ■

تعریف ۲۱۰۱۰۱۰ حلقه R را یک حلقه متناهی نامند هر گاه R تنها دارای تعدادی متناهی عنصر باشد؛ در غیر این صورت R را با حلقه‌ای نامتناهی می‌نامند.

حلقه‌های $\mathbf{Z}$ و $M_2(\mathbf{Z})$ نامتناهی‌اند.

مثال ۲۲۰۱۰۱۰ $\mathbf{Z}_n$ را به همراه اعمال $+_n$ و $\cdot_n$ که در مثال ۵۰۱۰۲ تعریف شده‌اند، در نظر بگیرید. بنابر مثال ۵۰۱۰۲، $(\mathbf{Z}_n, +_n)$ گروهی تعویض پذیر و بنابر مثال ۶۰۱۰۲، عمل $\cdot_n$ شرکت پذیر و تعویض پذیر است، و [۱] همانی ضرب $(\mathbf{Z}_n, +_n, \cdot_n)$ می‌باشد. حال به ازای هر $[a],[b],[c]\in\mathbf{Z}_n$،

$$\begin{aligned}[a]\cdot_n([b]+_n[c]) &= [a]\cdot_n[b+c]\\ &= [a(b+c)] = [ab+ac] = [ab]+_n[ac]\\ &= [a]\cdot_n[b]+_n[a]\cdot_n[c]\end{aligned}$$

به طور مشابه، $([b]+_n[c])\cdot_n[a] = [b]\cdot_n[a]+_n[c]\cdot_n[a]$. از این رو، هر دو قانون پخشی، برقرارند. بنابراین، $(\mathbf{Z}_n, +, \cdot_n)$ حلقه‌ای تعویض پذیر و یکدار است که حلقه اعداد صحیح به پیمانه n نامیده می‌شود. از مثال ۶۰۱۰۲، نتیجه می‌شود که هر عنصر ناصفر از $\mathbf{Z}_n$ دارای معکوس نیست. برای مثال فرض کنید n اول نباشد، مثلاً $n=6$. در این صورت [۴] دارای معکوس ضربی در $\mathbf{Z}_6$ نیست. همچنین $\mathbf{Z}_6$ دارای مقسوم علیه صفر است، زیرا داریم $[2]\neq[0]\neq[3]$ و از طرفی چون $[2]\cdot_6[3]=[6]=[0]$، که نتیجه می‌شود [۳] و [۲] مقسوم علیه‌های صفرند. بنابراین $\mathbf{Z}_6$ نمی‌تواند یک حوزه صحیح و در نتیجه یک میدان باشد. همچنین نتیجه می‌گیریم [۲] و [۳] معکوس های ضربی ندارند، زیرا آنها مقسوم علیه صفر می‌باشند.

مثال فوق نشان می‌دهد که به ازای هر عدد صحیح مثبت n، حلقه تعویض پذیر یکدار R وجود دارد به طوری که تعداد عناصر آن برابر با n است.

در قضیه زیر، فرض می‌کنیم که R تعویض پذیر باشد. این فرض می‌تواند برداشته شود و نتیجه بگیریم که R همچنان میدان باقی بماند. به هر حال، چون نتایج مناسب را ارائه نداده‌ایم، نمی‌توان این مطلب را با حذف این فرض اثبات کنیم. البته درفصل ۲۴ قضیه را در حالت کلی‌تری اثبات می‌کنیم.

قضیه ۲۳۰۱۰۱۰ یک حلقه تعویض پذیر متناهی R با بیش از یک عنصر و بدون مقسوم علیه صفر یک میدان است.

اثبات. بایستی نشان دهیم که R دارای عنصر همانی است و هر عنصر ناصفر آن یکه است.

فرض‌کنید a_1، a_2، ...، a_n عناصری متمایز از R باشند. فرض کنید $a \in R$ و $a \neq 0$. حال به‌ازای هر i، $aa_i \in R$ ولذا $\{aa_1, aa_2, \ldots, aa_n\} \subseteq R$. اگر $aa_i = aa_j$، آنگاه بنابر قضیه ۲۰۰۱۰۱۰، $a_i = a_j$. بنابراین عناصر aa_1، aa_2، ...، aa_n بایستی متمایز باشند و لذا

$$R = \{aa_1, aa_2, \ldots, aa_n\}.$$

این ایجاب می‌کند که یکی از حاصلضرب‌ها برابر است با a، مثلاً $aa_i = a$. چون R تعویض پذیر است، همچنین داریم $a_i a = aa_i = a$. فرض کنید b عنصری دلخواه از R باشد. در این صورت $a_j \in R$ ای وجود دارد به طوری که $b = aa_j$. بنابراین

$$\begin{aligned} ba_i &= a_i b \quad (\text{زیرا } R \text{ تعویض پذیر است}) \\ &= a_i(aa_j) \quad (\text{جایگزینی } b \text{ به جای}) \\ &= (a_i a)a_j \\ &= aa_j \\ &= b. \end{aligned}$$

این ایجاب می‌کند که a_i عنصر همانی R باشد. همانی R را با ۱ نشان می‌دهیم. حال $1 \in R = \{aa_1, aa_2, \ldots, aa_n\}$ و لذا یکی از حاصلضرب‌ها مثلاً aa_j بایستی برابر با ۱ باشد. بنابر تعویض پذیری، $a_j a = aa_j = 1$. از این رو، هر عنصر ناصفر یکه است. در نتیجه R یک میدان است. ■

نتیجه زیر بلافاصله از قضیه فوق حاصل می‌شود.

نتیجه ۲۴۰۱۰۱۰ هر حوزه صحیح متناهی یک میدان است. ■

در مثال ۶۰۱۰۲، نشان داده‌ایم که هر عنصر ناصفر $[a]$ از $\mathbf{Z}_n$ دارای معکوس است اگر و تنها اگر $1 = \text{ب.م.م}(a, n)$. بنابراین نتیجه زیر بلافاصله از این حقیقت حاصل می‌شود. جزئیات را به عنوان تمرین واگذار می‌کنیم.

نتیجه ۲۵۰۱۰۱۰ فرض کنید n عددی صحیح و مثبت باشد. در این صورت $\mathbf{Z}_n$ میدان است اگر و تنها اگر n اول باشد. ■

فرض کنید R یک حلقه باشد و $a \in R$. در این صورت به ازای هر عدد صحیح n، na را به صورت زیر تعریف کنید:

$$0a = 0$$

$$na = a + (n-1)a \quad \text{اگر } n > 0،$$

$$na = (-n)(-a) \quad \text{اگر } n < 0،$$

تاکید می‌کنیم که na یک حاصلضرب مابین عناصر R نیست، زیرا R ممکن است شامل $\mathbf{Z}$ نباشد.

به ازای هر $a,b\in R$ و هر $m,n\in\mathbf{Z}$ خاصیت های زیر را داریم:

$$(m+n)a = ma+na,$$

$$m(a+b) = ma+mb,$$

$$(mn)a = m(na),$$

$$m(ab) = (ma)b = a(mb),$$

$$(ma)(nb) = mn(ab).$$

اثبات خاصیت های فوق می‌تواندبه روش استقراء و شرایط تعریف یک حلقه به دست آید.

تعریف ۲۶۰۱۰۱۰ اگر عدد صحیح و مثبتی مانند n موجود باشد به طوری که به ازای هر $a\in R$، $na=0$، آنگاه کوچکترین چنین عدد صحیح و مثبت را **مشخصه** R می‌نامند. اگر چنین عدد صحیح مثبتی موجود نباشد، آنگاه R را از **مشخصه صفر** نامند.

مثال ۲۷۰۱۰۱۰ حلقه های $\mathbf{Z}$، $\mathbf{Q}$، $\mathbf{R}$ و $\mathbf{C}$ دارای مشخصه ۰ می‌باشند. حلقه $\mathbf{Z}_n$ $(n=1,2,3,\ldots)$ دارای مشخصه n است. توجه کنید که در $\mathbf{Z}_6$، $3[2]=[6]=[0]$ و $2[3]=[6]=[0]$. به هر حال، ۶ کوچکترین عدد صحیح است که به ازای هر $[a]\in\mathbf{Z}_6$، $6[a]=[0]$. به ویژه، $[1]$ دارای مرتبه جمعی ۶ است.

مثال ۲۸۰۱۰۱۰ فرض کنید X مجموعه‌ای ناتهی و $P(X)$ مجموعه توانی X باشد. در این صورت $(P(X),\Delta,\cap)$ حلقه‌ای تعویض پذیر و یکدار است، که در آن Δ عمل تفاضل متقارن است. در این مثال Δ به عنوان $+$ و $\cap$ به عنوان $\cdot$ عمل می‌کنند. حال به ازای هر $A\in P(X)$، $2A=A\Delta A=(A\setminus A)\cup(A\setminus A)=\varnothing$. بنابراین $P(X)$ دارای مشخصه ۲ است.

قضیه ۲۹۰۱۰۱۰ فرض کنید R حلقه‌ای یکدار باشد. دراین صورت R دارای مشخصه $n>0$ است اگر و تنها اگر n کوچکترین عدد صحیح مثبتی باشد که $n1=0$.

اثبات. فرض کنید R دارای مشخصه $n>0$ باشد. در این صورت به ازای هر $a\in R$، $na=0$ و لذا به ویژه $n1=0$. اگر $m1=0$ و $0<m<n$، آنگاه به ازای هر $a\in R$، $ma=m(1a)=(m1)a=0a=0$. به هر حال، این متناقض با کمین بودن n است. از این رو، n کوچکترین عدد صحیح مثبتی است که $n1=0$. بعکس، فرض کنید n کوچکترین عدد صحیح مثبتی باشد که $n1=0$. در این صورت به ازای هر $a\in R$، $na=n(1a)=(n1)a=0a=0$. بنابر کمین بودن n برای ۱، عدد n بایستی مشخصه R باشد. ■

قضیه ۳۰۰۱۰۱۰ مشخصه یک حوزهٔ صحیح R یا صفر یا یک عدد اول است.

اثبات. اگر عدد صحیح مثبتی مانند n موجود نباشد به طوری که به ازای هر $a \in R$، $na = 0$، آنگاه R از مشخصه صفر است. فرض کنید عدد صحیح مثبت nای موجود باشد به طوری که به ازای هر $a \in R$، $na = 0$. همچنین فرض کنید m کوچکترین عدد صحیح مثبتی باشد که به‌ازای هر $a \in R$، $ma = 0$. در این صورت $m1 = 0$. اگر m اول نباشد، آنگاه اعداد صحیح m_1 و m_2 وجود دارند به طوری که $0 < m_1, m_2 < m$ و $m = m_1 m_2$. ازاین رو،

$$0 = (m_1 m_2)1 = (m_1 1)(m_2 1).$$

چون R دارای مقسوم علیه صفر نیست، یا $m_1 1 = 0$ یا $m_2 1 = 0$. اما این با کمین بودن m در تناقض است. بنابراین، m عددی است اول. ■

۱۰.۱.۱ تمرین های حل شده

تمرین ۱. فرض کنید R یک حلقه باشد. عنصر $a \in R$ را خود توان نامند هرگاه $a^2 = a$ و پوچ‌توان نامند هرگاه به ازای عدد صحیح مثبت nای، $a^n = 0$.

(i) فرض کنید $a \in R$ ناصفر و خود توان باشد. نشان دهید که a پوچ توان نیست.

(ii) فرض کنید R حلقه‌ای یکدار باشد و $a \in R$ به طوری که دارای معکوس است. نشان دهید که a نمی‌تواند یک مقسوم علیه صفر باشد.

(iii) فرض کنید R حلقه‌ای یکدار باشد که دارای هیچ مقسوم علیه صفری نمی‌باشد. نشان دهید که تنها عناصر خود توان در R عبارتند از ۰ و ۱.

حل: (i) از فرض داریم $a^2 = a$. بنابر استقراء، به ازای هر عدد صحیح مثبت n، $a^n = a$. فرض کنید a پوچ‌توان باشد. در این‌صورت به ازای عدد صحیح مثبت mای، $a^m = 0$ و لذا $a = a^m = 0$، که یک تناقض است. بنابراین a پوچ توان نیست.

(ii) $b \in R$ وجود دارد به طوری که $ab = 1 = ba$. فرض کنید که a یک مقسوم علیه صفر باشد. در این صورت $c \in R$ای وجود دارد به طوری که $c \neq 0$ و $ac = 0$. بنابراین، $0 = b0 = b(ac) = (ba)c = c$، که یک تناقض است. از این رو، a مقسوم علیه صفر نیست.

(iii) واضح است که ۰ و ۱ عناصر خود توان هستند. حال فرض کنید $e \in R$ نیز خود توان باشد. دراین صورت $e^2 = e$ و لذا $e(e-1) = 0$. چون R هیچ مقسوم علیه صفری ندارد، یا $e = 0$ یا $e - 1 = 0$، یعنی $e = 0$ یا $e = 1$. بنابراین، تنها عناصر خود توان R عبارتند از ۰ و ۱.

تمرین ۲. اعداد صحیح مثبت n را به گونه‌ای معین کنید که $\mathbb{Z}_n$ دارای هیچ عنصر پوچ توان نباشد.

حل: ادعا می‌کنیم که n عدد صحیح آزاد مربعی است، یعنی $n = p_1 p_2 \cdots p_k$، که در آن p_iها اعداد اول متمایز می‌باشند.

فرض کنید $n = p_1 p_2 \dots p_k$، که p_iها اعداد اول متمایزند. همچنین فرض کنید $[a] \in \mathbf{Z}_n$ پوچ توان باشد. در این صورت به ازای عدد صحیح mای، $[a]^m = [0]$. از این رو، n عدد a^m و لذا $p_1 p_2 \dots p_k$ عدد a^m را عاد می‌کند. در این صورت به ازای هر $i = 1, 2, \dots, k$، $p_i \mid a^m$. چون p_iها اول هستند، لذا به ازای هر $i = 1, 2, \dots, k$، $p_i \mid a$. چون p_1، p_2، ...، p_k اعداد اول متمایزی هستند، بایستی $p_1 p_2 \dots p_k \mid a$، یعنی $n \mid a$ و لذا $[a] = [0]$. این ایجاب می‌کند که $\mathbf{Z}_n$ دارای هیچ عنصر پوچ توانی نمی‌باشد. بعکس، فرض کنید $\mathbf{Z}_n$ دارای هیچ عنصر پوچ توانی نباشد. همچنین فرض کنید $n = p_1^{m_1} p_2^{m_2} \dots p_k^{m_k}$، که در آن p_iها اعداد اول متمایزند و $m_i \geq 1$. قرار دهید $m = max\{m_1, m_2, \dots, m_k\}$. حال $[p_1 p_2 \dots p_k]^m = [p_1^m p_2^m \dots p_k^m] = [0]$، زیرا $n \mid (p_1^m p_2^m \dots p_k^m)$. همچنین چون $\mathbf{Z}_n$ دارای هیچ عنصر پوچ توانی نیست، $[p_1 p_2 \dots p_k] = [0]$. از این رو، $n \mid (p_1 \dots p_k)$ و لذا $(p_1^{m_1} p_2^{m_2} \dots p_k^{m_k}) \mid (p_1 \dots p_k)$. بنابراین به ازای هر $i = 1, 2, \dots, k$، $m_i \leq 1$. از این رو، به ازای هر $i = 1, 2, \dots, k$، $m_i = 1$ و لذا n یک عدد صحیح آزاد مربعی است.

تمرین ۳. نشان‌دهید که تعداد عناصرخودتوان در $\mathbf{Z}_{mn}$ حداقل برابراست با ۴، که $m > 1$، $n > 1$ و m و n نسبت به هم اولند.

حل: واضح است که $[0]$ و $[1]$ عناصری خود توان می‌باشند. چون m و n نسبت به هم اولند، اعداد صحیح a و b وجود دارند به طوری که $am + bn = 1$. حال نشان می‌دهیم که n عدد a را و b عدد m را عاد نمی‌کند. فرض کنید $n \mid a$. در این صورت به ازای عدد صحیح rای، $a = nr$. بنابراین $n(rm + b) = nrm + nb = am + nb = 1$. این ایجاب می‌کند که $n = 1$، که یک تناقض است. بنابراین، n عدد a را عاد نمی‌کند. به طور مشابه m نمی‌تواند عدد b را عاد کند. حال $m^2 a = m(1 - nb)$. این ایجاب می‌کند که $[m^2 a] = [m]$. از این رو، $[ma]^2 = [ma]$. اگر $[ma] = [0]$، آنگاه $mn \mid ma$ و لذا $n \mid a$، که یک تناقض است. در نتیجه $[ma] \neq [0]$. اگر $[ma] = [1]$، آنگاه $mn \mid (ma - 1)$. از این رو به ازای عدد صحیح tای، $ma + mnt = 1$. بنابراین $m(a + nt) = 1$. این ایجاب می‌کند که $m = 1$، که یک تناقض است. از این رو $[ma] \neq [1]$. بنابراین $[ma]$ عنصری خود توان است که $[ma] \neq [0]$ و $[ma] \neq [1]$. به طور مشابه، $[nb]$ عنصر خود توانی است که $[nb] \neq [0]$ و $[nb] \neq [1]$. واضح است که $[ma] \neq [nb]$. بنابراین عناصر $[0]$، $[1]$، $[ma]$ و $[na]$ به دست می‌آیند که عناصری خود توان در $\mathbf{Z}_{mn}$ می‌باشند.

تمرین ۴. اعداد صحیح مثبت n را طوری تعیین کنید که $\mathbf{Z}_n$ دارای هیچ عنصر خود توانی به جز

$[0]$ و $[1]$ نباشد.

حل: نشان می‌دهیم که به ازای عدد اول p و عدد صحیح $r>0$ ای، $n=p^r$. ابتدا فرض کنید که به ازای عدد اول p و عدد صحیح مثبت r ای، $n=p^r$ و $[x]\in \mathbf{Z}_n$ خود توان باشد. در این صورت $[x]^2=[x]$. بنابراین $p^r|(x^2-x)$ یا $p^r|x(x-1)$. چون x و $x-1$ نسبت به هم اولند، لذا $p^r|x$ یا $p^r|(x-1)$. اگر $p^r|x$، آنگاه $[x]=[0]$ و اگر $p^r|(x-1)$، آنگاه $[x]=[1]$. بنابراین $[0]$ و $[1]$ تنها دو عنصر خود توان هستند. بعکس، فرض کنید $[0]$ و $[1]$ تنها دو عنصر خود توان باشند. همچنین فرض کنید $n=p_1^{m_1}p_2^{m_2}\dots p_k^{m_k}$، که در آن p_iها اعداد اول متمایزند، $m_i\geq 1$ و $k>1$. قرار دهید $t=p_1^{m_1}$ و $s=p_2^{m_2}\dots p_k^{m_k}$. در این صورت t و s نسبت به هم اولند و $n=ts$. بنابر تمرین حل شده ۳، $\mathbf{Z}_n=\mathbf{Z}_{ts}$ بایستی دارای حداقل چهار عنصر خود توان باشد، که یک تناقض است. بنابراین $k=1$. در نتیجه به ازای عدد اول p و عدد صحیح مثبت r ای، $n=p^r$.

تمرین ۵. فرض کنید R یک حلقه باشد. نشان دهید که شرایط زیر معادلند.

(i) R دارای هیچ عنصر پوچ توانی نیست.

(ii) به ازای هر $a\in R$، اگر $a^2=0$، آنگاه $a=0$.

حل: $(i)\Leftarrow(ii)$ فرض کنید $a\in R$ و $a^2=0$. اگر $a\neq 0$، آنگاه a عنصر پوچ توان ناصفری در R است، که یک تناقض می‌باشد. بنابراین $a=0$.

$(ii)\Leftarrow(i)$ فرض کنید $a\in R$ به گونه‌ای باشد که به ازای عدد صحیح مثبت n ای، $a^n=0$. فرض کنید $n\neq 0$ و n کوچکترین عدد صحیح مثبتی باشد که $a^n=0$. همچنین فرض کنید n زوج باشد، یعنی به ازای عدد صحیح مثبت m ای، $n=2m$. در این صورت $(a^m)^2=a^{2m}=0$ و لذا $a^m=0$، که تناقضی با کمین بودن n است. بنابراین $n>1$. فرض کنید $n=2m+1$. در این صورت $m+1<n$. بنابراین $a^{2m+2}=a^{2m+1}a=a^na=0$. این ایجاب می‌کند که $a^{m+1}=0$، که مجدداً در تناقض با کمین بودن n می‌باشد. از این رو R دارای هیچ عنصر پوچ توان ناصفری نیست.

تمرین ۶. عنصر e از حلقه R را همانی چپ (یاراست) نامند، هر گاه به ازای هر $a\in R$، $ea=a$ (یا $ae=a$). نشان دهید که اگر حلقه R دارای یک همانی چپ یکتای e باشد، آنگاه e همانی راست R نیز هست و از این رو عنصر همانی R می‌باشد.

حل: فرض کنید e همانی چپ یکتای R باشد. در این صورت به ازای هر $x\in R$، $ex=x$. فرض کنید $x\in R$. حال $(xe-x+e)x=xex-xx+ex=xx-xx+x=x$. این ایجاب می‌کند که $xe-x+e$ همانی چپ باشد. چون e همانی چپ یکتای R است، لذا $xe-x+e=e$ و لذا $xe=x$. بنابراین e همانی راست R است.

تمرین ۷. فرض کنید R حلقه‌ای تعویض پذیر و یکدار باشد و $a,b\in R$. همچنین فرض کنید که a وارون پذیر و b پوچ توان باشد. نشان دهید که $a+b$ وارون پذیر است. همچنین نشان دهید که اگر R تعویض پذیر نباشد، آنگاه نتیجه ممکن است برقرار نباشد.

حل: $c\in R$ ای وجود دارد به طوری که $ac=1$ و نیز عدد صحیح مثبت n ای وجود دارد به طوری که $b^n=0$. فرض کنید $d=c-c^2b+c^3b^2+\dots+(-1)^{n+1}c^nb^{n-1}$. حال

$$\begin{aligned}(a+b)d &= ac-ac^2b+ac^3b^2+\dots+(-1)^{n+1}ac^nb^{n-1}+\\ &\quad bc-bc^2b+bc^3b^2+\dots+(-1)^{n+1}bc^nb^{n-1}\\ &= 1-cb+c^2b^2+\dots+(-1)^{n+1}c^{n-1}b^{n-1}+bc-\\ &\quad c^2b^2+c^3b^3+\dots+(-1)^{n+1}c^nb^n\\ &= 1.\end{aligned}$$

به طور مشابه، $d(a+b)=0$. از این رو، $a+b$ وارون پذیر است.

حلقه $M_2(\mathbf{Z})$ را در نظر بگیرید. قرار دهید $a=\begin{bmatrix}0 & -1\\ -1 & 0\end{bmatrix}$ و $b=\begin{bmatrix}0 & 1\\ 0 & 0\end{bmatrix}$. در این صورت a وارون پذیر و b پوچ توان است. حال $a+b=\begin{bmatrix}0 & 0\\ -1 & 0\end{bmatrix}$ واضح است که $a+b$ عنصر پوچ توان ناصفری است. از این رو $a+b$ وارون پذیر نیست.

۱۰۰۱۰۲ تمرینها

۱. در حلقه های $\mathbf{Z}_8$ و $\mathbf{Z}_6$ عناصر زیر را بیابید:

(i) یکه ها، (ii) عناصر پوچ توان، و (iii) مقسوم علیه‌های صفر.

۲. فرض کنید R مجموعه تمام ماتریس های 2×2 روی میدان اعداد مختلط به صورت $\begin{bmatrix}z_1 & z_2\\ -\bar{z}_2 & \bar{z}_1\end{bmatrix}$ باشد، که در آن $\bar{z}$ مزدوج مختلط عدد مختلط z است. نشان دهید که $(R,+,\cdot)$ یک حلقه تقسیم است، که در آن $+$ و $\cdot$ به ترتیب جمع و ضرب معمولی ماتریس‌ها می‌باشند. آیا R میدان است؟

۳. فرض کنید R حلقه‌ای یکدار باشد. ثابت کنید

(i) $(-1)(-1)=1$ و $(-1)a=-a=a(-1)$،

(ii) اگر a در R یکه باشد، آنگاه $-a$ نیز یکه است و $(-a)^{-1}=-(a)^{-1}$.

۴. ثابت کنید که حلقه R تعویض پذیر است اگر و تنها اگر به ازای هر $a,b\in R$، $(a+b)^2=a^2+2ab+b^2$.

۵. ثابت کنید که حلقه R تعویض‌پذیر است اگر و تنها اگر به ازای هر $a,b\in R$، $a^2-b^2=(a-b)(a+b)$.

۶. فرض کنید R یک حلقه باشد. اگر به ازای هر $a\in R$، $a^3=a$، ثابت کنید که R تعویض پذیر است.

۷. فرض کنید R حلقه‌ای تعویض پذیر باشد و $a,b\in R$. ثابت کنید که به ازای هر $n\in \mathbf{N}$،

$$(a+b)^n=a^n+\binom{n}{1}a^{n-1}b+\dots+\binom{n}{r}a^{n-r}b^r+\dots+\binom{n}{n-1}ab^{n-1}+b^n.$$

۸. اگر a و b عنصرهایی از یک حلقه و m و n اعدادی صحیح باشند، ثابت کنید

(i) $(na)(mb)=(nm)(ab)$،

(ii) $n(ab)=(na)b=a(nb)$،

(iii) $n(-a)=(-n)a$.

۹. اگر R حوزه‌ای صحیح از مشخصه عدد اول p باشد، ثابت کنید که به ازای هر $a,b\in R$، $(a+b)^p=a^p+b^p$.

۱۰. فرض کنید R حلقه‌ای یکدار و بدون مقسوم علیه صفر باشد. ثابت کنید که به ازای هر $a,b\in R$، $ab=1$ ایجاب می‌کند که $ba=1$.

۱۱. فرض کنید R حلقه‌ای یکدار باشد. اگر a عنصری پوچ توان از R باشد، ثابت کنید که $1-a$ و $1+a$ یکه‌اند.

۱۲. فرض کنید R حلقه‌ای تقسیم باشد و $a,b\in R$. نشان دهید که اگر $ab=0$، آنگاه یا $a=0$ یا $b=0$.

۱۳. فرض کنید $a\in R$ عنصری خود توان باشد. نشان دهید که به ازای هر $b\in R$، $(1-a)ba$ پوچ توان است.

۱۴. تمام عناصر خود توان حلقه $M_2(\mathbf{R})$ را بیابید.

۱۵. فرض کنید R حلقه‌ای یکدار باشد و $0\neq a\in R$. اگر دو عنصر متمایز b و c در R موجود باشند به طوری که $ab=ac=1$، نشان دهید که تعداد نامتناهی عنصر x در R وجود دارند به طوری که $ax=1$. (به ماهانه ریاضی آمریکا ۷۰ (۱۹۶۱) ۳۱۵ مراجعه شود).

۱۶. فرض کنید R حوزه‌ای صحیح باشد و $a,b\in R$. همچنین فرض کنید $m,n\in \mathbf{Z}$ متباین باشند. ثابت کنید که $a^m=b^m$ و $a^n=b^n$ ایجاب می‌کند که $a=b$.

۱۷. فرض کنید R و R' دو حلقه باشند. به ازای هر $(a,b),(c,d)\in R\times R'$، اعمال $+$ و $\cdot$ را روی $R\times R'$ به صورت زیر تعریف کنید:

$$(a,b)+(c,d)=(a+c,b+d)\,,\ (a,b)\cdot(c,d)=(a\cdot c,b\cdot d)\ .$$

(i) ثابت کنید که $(R\times R',+,\cdot)$ تشکیل یک حلقه می‌دهد. این حلقه را مجموع مستقیم R و R' می‌نامند و آن را با نماد $R\oplus R'$ نشان می‌دهند.

(ii) اگر R و R' تعویض پذیر و یکدار باشند، ثابت کنید که $R\oplus R'$ نیز تعویض‌پذیر و یکدار است.

۱۸. مفهوم حاصلجمع مستقیم تمرین ۱۷ را به هر تعداد متناهی حلقه تعمیم دهید.

۱۹. ثابت کنید که مشخصه یک حلقه متناهی R، مرتبه $|R|$ را عاد می‌کند.

۲۰. فرض کنید R حلقه‌ای یکدار باشد. ثابت کنید که مشخصه حلقه ماتریس $M_2(R)$ برابر است با مشخصه R.

۲۱. اگر p عددی صحیح اول باشد، ثابت کنید که $(p-1)!\equiv_p -1$.

۲۲. در تمرینهای زیر، در صورت درستی عبارت، اثباتی ارائه دهید؛ در غیر این صورت مثالی نقض ارائه کنید.

(i) در حلقه R، اگر a و b عناصری خود توان باشند، آنگاه $a+b$ عنصری خود توان است.

(ii) در حلقه R، اگر a و b عناصری پوچ توان باشند، آنگاه $a+b$ عنصری پوچ توان است.

(iii) هر حلقه متناهی یکدار یک حوزه صحیح است.

(iv) میدانی با هفت عنصر وجود دارد.

(v) مشخصه یک حلقه نامتناهی همیشه ۰ است.

(vi) عنصری از حلقه R که خود توان باشد، اما مقسوم علیه صفر نباشد، عنصر همانی R است.

(vii) اگر a و b دو مقسوم علیه صفر باشند، آنگاه $a+b$ نیز یک مقسوم علیه صفر در حلقه R است.

$(viii)$ در میدان متناهی F، به ازای هر $a,b\in F$، $a^2+b^2=0$ ایجاب می‌کند که $a=0$ و $b=0$.

(ix) در میدان F، به‌ازای هر دو عنصر ناصفر a,b که $a+b\neq 0$،

$$(a+b)^{-1}=a^{-1}+b^{-1}\ .$$

(x) میدانی با شش عنصر وجود دارد.

۱۰۰۲ بعضی حلقه‌های مهم

در این بخش به معرفی دو حلقه مهم پرداخته و خواص اساسی آنها را مطالعه می‌کنیم.

۱۰۰۲۰۱ حلقه‌های بولی

یادآور می‌شویم که در تمرین حل شده ۱ (صفحه ۳۵۳)، عنصر x در R خود توان نامیده می‌شود هرگاه $x^2=x$. عنصر صفر و عنصر همانی در یک حلقه عناصری خود توان هستند. در حلقه $\mathbf{Z}$، تنها عناصر خود توان ۰ و ۱ می‌باشند. برای مثال، در $M_2(\mathbf{Z})$، ماتریس $\begin{bmatrix} 1 & 0 \\ 2 & 0 \end{bmatrix}$ عنصری خود توان است.

تعریف ۱۰۲۰۱۰ حلقه یکدار R را یک حلقه بولی نامند اگر هر عنصر R خود توان باشد.

مثال ۲۰۲۰۱۰ (i) $\mathbf{Z}_2$ یک حلقه بولی است.

(ii) حلقه $P(X)$ از مثال ۲۸۰۱۰۱۰ یک حلقه بولی است، زیرا به ازای هر $A\in P(X)$، $A\cap A=A$.

قضیه ۳۰۲۰۱۰ فرض کنید R حلقه‌ای بولی باشد. در این صورت مشخصه R برابر است با ۲ و R تعویض پذیر است.

اثبات. ابتدا نشان می‌دهیم که R از مشخصه ۲ است. فرض کنید $x\in R$. حال

$$x+x=(x+x)^2=(x+x)(x+x)=x(x+x)+x(x+x)$$
$$=x^2+x^2+x^2+x^2=x+x+x+x\ .$$

این ایجاب می‌کند که $2x=4x$ و لذا $2x=0$. از این رو، $2\cdot 1=0$، زیرا x عنصری دلخواه است. در نتیجه بنابر قضیه ۲۹۰۱۰۱۰، مشخصه R برابر است با ۲. برای نشان دادن تعویض‌پذیری R، فرض کنید $x,y\in R$. در این صورت

$$(x+y)=(x+y)^2=(x+y)(x+y)=x^2+xy+yx+y^2=x+xy+yx+y\ .$$

این ایجاب می‌کند که $xy+yx=0$. از این رو، $xy=xy+0=xy+xy+yx=2xy+yx=yx$، زیرا $2xy=0$. بنابراین R تعویض پذیر است. ■

۱۰۰۲۰۲ حلقه‌های منظم

عنصر x از حلقه R را یک عنصر منظم نامند هرگاه $y\in R$ ای موجود باشد به طوری که $x=xyx$.

تعریف ۴۰۲۰۱۰ حلقه R را یک حلقه منظم نامند هرگاه هر عنصر آن منظم باشد.

در حلقه $\mathbf{Z}$، تنها عناصر منظم ۰، ۱ و ۱- هستند. بنابراین $\mathbf{Z}$ حلقه‌ای منظم نیست.

مثال ۵۰۲۰۱۰ فرض کنید R حلقه‌ای تقسیم باشد و $x\in R$. اگر $x=0$، آنگاه $x=xxx$ فرض کنید $x\neq 0$. در این صورت $xx^{-1}=1$ و لذا $x=xx^{-1}x$. بنابراین R حلقه‌ای منظم نیست.

از تعریف یک حلقه بولی نتیجه می‌شود که هر حلقه بولی یک حلقه منظم است. میدان $\mathbf{R}$ حلقه‌ای منظم است اما حلقه‌ای بولی نمی‌باشد.

مثال ۶۰۲۰۱۰ میدان اعداد حقیقی $\mathbf{R}$ را در نظر بگیرید و

$$\mathbf{R}\times\mathbf{R}\{(x,y)\mid x,y\in\mathbf{R}\}.$$

به ازای هر $x,y,z,w\in\mathbf{R}$، $+$ و $\cdot$ را روی $\mathbf{R}\times\mathbf{R}$ به صورت زیر تعریف کنید:

$$(x,y)+(z,w)=(x+z,y+w)$$
$$(x,y)\cdot(z,w)=(xz,yw)$$

در این صورت $\mathbf{R}\times\mathbf{R}$ حلقه‌ای تعویض پذیر با عنصر همانی است. حال $(1,0),(0,1)\in\mathbf{R}\times\mathbf{R}$ و $(1,0)(0,1)=(0,0)$. این نشان می‌دهد که $\mathbf{R}\times\mathbf{R}$ شامل مقسوم علیه صفر است و لذا میدان نیست. ادعا می‌کنیم که $\mathbf{R}\times\mathbf{R}$ منظم است. فرض کنید $(x,y)\in\mathbf{R}\times\mathbf{R}$. اگر $x=0=y$، آنگاه $(x,y)=(x,y)(x,y)(x,y)$. اگر $x\neq 0$ و $y\neq 0$، آنگاه

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

اگر $x=0$، اما $y\neq 0$، آنگاه $(x,y)=(x,y)(x,y^{-1})(x,y)$. به طور مشابه، اگر $x\neq 0$ و $y=0$، آنگاه $(x,y)=(x,y)(x^{-1},y)(x,y)$. بنابراین در هر حالت (x,y) عنصری منظم است. از این رو، $\mathbf{R}\times\mathbf{R}$ حلقه‌ای منظم است.

مثال ۷۰۲۰۱۰ فرض کنید $M_2(\mathbf{R})$ مجموعه ماتریس‌های 2×2 روی $\mathbf{R}$ باشد. حال $M_2(\mathbf{R})$ یک حلقه تعویض ناپذیر و یکدار است، که در آن $+$ و $\cdot$ به ترتیب جمع و ضرب معمولی ماتریسهای می‌باشند. نشان دهیم که $M_2(\mathbf{R})$ حلقه‌ای منظم است. فرض کنید

$$A=\begin{bmatrix} x & y\\ z & w\end{bmatrix}\in M_2(\mathbf{R}).$$

حالت ۱: $xw-zy\neq 0$. در این صورت

$$B=\begin{bmatrix} \dfrac{w}{xw-zy} & \dfrac{-y}{xw-zy}\\ \dfrac{-z}{xw-zy} & \dfrac{x}{xw-zy}\end{bmatrix}\in M_2(\mathbf{R}),\ A=ABA$$

حالت ۲: $xw-zy=0$.

زیر حالت (آ۲): x، y، z و w همگی صفرند. در این حالت $A=\begin{bmatrix} 0 & 0\\ 0 & 0\end{bmatrix}$ و لذا به ازای هر

$$A = ABA \text{ ، } B \in M_2(\mathbf{R}) .$$

زیر حالت (ب۲) : x، y، z و w همگی صفر نیستند. فرض کنید $x \neq 0$ و قرار دهید

$$B = \begin{bmatrix} \frac{1}{x} & 0 \\ 0 & 0 \end{bmatrix}$$

در این صورت

$$ABA = \begin{bmatrix} x & y \\ z & w \end{bmatrix} \begin{bmatrix} \frac{1}{x} & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} x & y \\ z & w \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 0 \\ \frac{z}{x} & 0 \end{bmatrix} \begin{bmatrix} x & y \\ z & w \end{bmatrix}$$

$$= \begin{bmatrix} x & y \\ z & \frac{zy}{x} \end{bmatrix} = \begin{bmatrix} x & y \\ z & w \end{bmatrix}.$$

چون $xw - zy = 0$ و $x \neq 0$ نتیجه می‌دهد $w = \frac{zy}{x}$. اگر $y \neq 0$، آنگاه فرض کنید $B = \begin{bmatrix} 0 & 0 \\ \frac{1}{y} & 0 \end{bmatrix}$،

در این صورت

$$ABA = \begin{bmatrix} x & y \\ z & w \end{bmatrix} \begin{bmatrix} 0 & 0 \\ \frac{1}{y} & 0 \end{bmatrix} \begin{bmatrix} x & y \\ z & w \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 0 \\ \frac{w}{y} & 0 \end{bmatrix} \begin{bmatrix} x & y \\ z & w \end{bmatrix}$$

$$= \begin{bmatrix} x & y \\ \frac{wx}{y} & w \end{bmatrix} = \begin{bmatrix} x & y \\ z & w \end{bmatrix}.$$

به طور مشابه، اگر $z \neq 0$ یا $w \neq 0$، آنگاه می‌توانیم ماتریس B را به گونه‌ای بیابیم که $A = ABA$.

بنابراین، $M_2(\mathbf{R})$ یک حلقه منظم است.

چون $M_2(\mathbf{R})$ یک حلقه تقسیم نیست، نتیجه می‌شود که یک حلقه منظم لزوماً یک حلقه تقسیم نیست. به هر حال، یک حلقه تقسیم یک حلقه منظم است که این مطلب در مثال ۵۰۲۰۱۰ نشان داده شده است. در قضیه بعد، نشان می‌دهیم که یک حلقه منظم تحت شرط خاصی یک حلقه تقسیم می‌شود.

قضیه ۸.۲.۱۰ فرض کنید R حلقه‌ای منظم بابیش از یک عنصر باشد. همچنین فرض کنید به ازای هر $x\in R$، عنصر یکتای $y\in R$ موجود باشد به طوری که $x=xyx$. در این صورت

(i) R دارای مقسوم علیه صفر نیست،

(ii) اگر $x\neq 0$ و $x=xyx$، آنگاه به ازای هر $x,y\in R$، $y=yxy$،

(iii) R دارای عنصر همانی است،

(iv) R یک حلقه تقسیم است.

اثبات. (i) فرض کنید x عنصری ناصفر از R باشد و به ازای $z\in R$ای، $xz=0$. حال بنابر فرض، عنصر یکتای $y\in R$ وجود دارد به طوری که $x=xyx$. بنابراین $x(y-z)x=xyx-xzx=xyx$. از این رو، بنابر یکتایی y، $y-z=y$ و لذا $z=0$. این ثابت می‌کند که R دارای مقسوم علیه صفر نمی‌باشد.

(ii) فرض کنید $x\neq 0$ و $x=xyx$. در این صورت $x(y-yxy)=xy-xyxy=xy-xy=0$. چون R دارای مقسوم علیه صفر نیست و $x=0$، لذا $y-yxy=0$ و لذا $yxy=y$.

(iii) فرض کنید $0\neq x\in R$. در این صورت عنصر یکتای $y\in R$ وجود دارد به طوری که $x=xyx$. قرار دهید $e=yx$. اگر $e=0$، آنگاه $x=xyx=0$، که یک تناقض است. بنابراین $e\neq 0$. همچنین $e^2=yxyx=y(xyx)=yx=e$. فرض کنید $z\in R$، در این صورت $(ze-z)e=ze^2-ze=ze-ze=0$. بنابراین، بنابر (i)، یا $ze-z=0$ یا $ze=z$. به طور مشابه، $e(ez-z)=0$ ایجاب می‌کند که $ez=z$. از این رو، e عنصر همانی R است.

(iv) بنابر (iii)، R شامل عنصر همانی e است. برای نشان دادن این که R یک حلقه تقسیم است، باقی می‌ماند نشان دهیم که هر عنصر ناصفر R دارای معکوس در R می‌باشد. فرض کنید x عنصری ناصفر در R باشد. در این صورت عنصر یکتای $y\in R$ وجود دارد به طوری که $x=xyx$. بنابراین، $xyx=xe$، یعنی $x(yx-e)=0$. چون R دارای مقسوم علیه صفر نیست و $x\neq 0$، لذا $yx-e=0$ و بنابراین $yx=e$. به طور مشابه $xyx=ex$ ایجاب می‌کند که $xy=e$. بنابراین $xy=e=yx$. از این رو، R یک حلقه تقسیم است. ■

۱۰.۲.۳ تمرینها

۱. ثابت کنید که یک حلقه بولی یک میدان است اگر و تنها اگر R تنها شامل ۰ و ۱ باشد.

۲. ثابت کنید که یک حلقه یکدار، حلقه‌ای بولی است اگر و تنها اگر به ازای هر $a,b\in R$، $(a+b)ab=0$.

۳. فرض کنید R حلقه‌ای بولی با بیش از دو عنصر باشد. تمام مقسوم علیه‌های صفر R را بیابید.

CamScanner

۴. فرض کنید $T=\{f\mid f:\mathbf{R}\to\mathbf{Z}_2\}$. به ازای هر $f,g\in T$ و هر $x\in R$ اعمال + و · را روی T به صورت $(f+g)(x)=f(x)+g(x)$ و $(f\cdot g)(x)=f(x)g(x)$ تعریف کنید. نشان دهید که $(T,+,\cdot)$ یک حلقه بولی است.

۵. ثابت کنید که یک عنصر ناصفر از یک حلقه یکدار منظم یا یکه یا مقسوم علیه صفر است.

۶. ثابت کنید که مرکز یک حلقه منظم، منظم است.

۷. فرض کنید R حلقه‌ای باشد که هر عنصر آن خود توان است. قرار دهید $\bar{R}=R\times\mathbf{Z}_2$. به ازای هر $(a,[n]),(b,[m])\in\bar{R}$ اعمال + و · را روی $\bar{R}$ به صورت زیر تعریف کنید:

$$(a,[n])+(b,[m])=(a+b,[n+m])$$

$$(a,[n])\cdot(b,[m])=(na+mb+ab,[nm])$$

نشان دهید که + و · روی $\bar{R}$ خوش تعریف می‌باشند و $\bar{R}$ یک حلقه بولی است.

۸. فرض کنید R حلقه‌ای یکدار و منظم باشد.

(i) ثابت کنید که به ازای هر $a\in R$، عنصر خود توان $e\in R$ وجود دارد به طوری که $Ra=Re$.

(ii) ثابت کنید که به ازای هر دو عنصر خود توان $e,f\in R$، عنصر خود توان $g\in R$ وجود دارد به طوری که $Re+Rf=Rg$.

ویـلیام روان هـامیلتون Willam Rowan Hamilton (۱۸۰۵-۱۸۶۵) در روز ۴ اوت ۱۸۰۵ در دابلین ایـرلند مـتولد شـد. او چـهارمین فـرزند از خـانواده‌ای نـه فرزندی بود. تحصیلات زودرس وی از سـه سالگی توسط عمویش آغـاز شـد.در سـن ۵ سالگی ، او در زبانهای لاتین، یونانی، و عبری ماهر شده بود.

هامیلتون هنگامی که حدود ۱۵ ساله بود شروع به خواندن اصول نیوتن کرد و به نجوم علاقمند شد. در سال ۱۸۲۲، اشتباهی در مکـانیک سماوی لاپلاس کشف کرد که از طریق یک دوست به جان برینکلی John Brinkley رسید. بعدها برینکلی در به دست آوردن پستی به عـنوان جـایگزین خـود در رصـدخانهٔ دانسـینک Dunsink Observatory به هامیلتون کمک کرد.

در ۲۳ آوریل ۱۸۲۷ هنگامی که هنوز یک دانشـجوی لیسـانس در کـالج تـرینیتی Trinity College دانشگاه آکسفورد بود، هاملیتون اولین مقالهٔ خود را تحت عـنوان، "نـظریهٔ دسـتگاههای پرتوها" به آکادمی سلطنتی ایرلند ارائه کرد. این مقاله اساس کشف زمینه فیزیک نور ریاضی شد. هامیلتون تابع مشخصه را، که اولین کشف وی بود، معرفی کرد. در ۱۰ ژوئن ۱۸۲۷، گر چه هنوز هیچ درجهٔ تحصیلی نداشت به عنوان اختر شـناس سـلطنتی در رصـدخانهٔ دانسـینک مـنصوب و پروفسور نجوم در کالج ترینیتی آکسفورد شد.

سهم اصلی هامیلتون در جبر چهارگان‌ها، فیزیک نور، و دینامیک بوده است. وی مثالهای کمی برای توضیح مفاهیم خود ارائه می‌کرد و در نتیجه خواندن مقالاتش مشکل بود. او بیشتر عمر خود را صرف مطالعهٔ چهارگان‌ها کرد .

هامیلتون به اعداد مختلط سه - بعدی علاقمند بود، که آنها را "سه تایی" نامید. او در این زمینه موفقیت کمی به دست آورد. گر چه به این بخش از ریاضی مطالبی اضافه کرد، ولی نتوانست قاعدهٔ ضرب مناسبی پیدا کند. سپس او به اصطلاح چهارگان‌ها را مورد بررسی قرار داد. هامیلتون در روز ۱۶ اکتبر ۱۸۴۳، هنگامی که در طول کانال سلطنتی قدم می‌زد، کشف چهارگان‌ها به ذهنش خطور کرد، و او بلافاصله فرمول ضرب را برای چهارگان‌ها بر روی سنگ پـلی روی کـانال نـوشت. وی دریافت که می‌تواند از قانون تعویض‌پذیری صرفنظر کند، و با وجود این باز هم یک دستگاه جبری با معنی داشته باشد. زمانی که هامیلتون و کیلی به طور مستقل نشان دادند اعمال چهارگان‌ها، بردارها

را حول محوری مفروض دوران می‌دهد، جذابیت هندسی چهارگان‌ها تشخیص داده شد. در سال ۱۸۳۷، هامیلتون اثبات آبل از ناممکن بودن حل معادلات عمومی درجهٔ ۵ را اصلاح کرد.

نام هامیلتون با مفاهیمی مانند توابع هامیلتون، معادلات دیفرانسیل هامیلتون - ژاکوبی، میسر هامیلتون در نظریهٔ گراف، و قضیهٔ کیلی - هامیلتون در جبر خطی همراه است. وی اصطلاحات "بردار"، "اسکالر" و "تانسور" را ابداع کرد. سرانجام هامیلتون در روز ۲ سپتامبر ۱۸۶۵ درگذشت.

فصل یازدهم

حلقه‌ها، ایده‌آل‌ها، و همریختی‌ها

مهمترین زیرساختار یک حلقه، زیر مجموعه خاصی است که "ایده‌آل" نامیده می‌شود. کلمه ایده‌آل توسط ددکیند Dedekind در به افتخار کارکومر Kummer بر روی تعداد ایده‌آلها رایج شد. این مفهوم کومر و ددکیند برای استخراج خواص تجزیه یکتا به کار رفته بود. کومر ایدهٔ عدد ایده‌آل را هنگام کارش روی آخرین قضیه فرما معرفی کرد. نوتر Noether بعضی نتایج مهم را روی نظریه ایده‌آل ها استنتاج کرد. برخی از ایده‌های نوتر، نه تنها برخاسته از کار ددکیند بلکه از کارهای کرونکر Kroneker و لاسکر Lasker بوده است.

۱۱۰۱ زیرحلقه‌ها و زیرمیدان ها

در این بخش، مفهوم زیرحلقه از یک حلقه را معرفی می‌کنیم. این مفهوم به مفهوم زیرگروه یک گروه شباهت دارد.

تعریف ۱۰۱۰۱۱ فرض کنید $(R,+,\cdot)$ یک حلقه و R' زیر مجموعه‌ای از R باشد. در این صورت $(R',+,\cdot)$ یک زیرحلقه $(R,+,\cdot)$ نامیده می‌شود هرگاه $(R',+)$ زیرگروهی از $(R,+)$ باشد و به ازای هر $x,y\in R'$، $x\cdot y\in R'$.

فرض کنید $(R',+\cdot)$ زیرحلقه‌ای از حلقه $(R,+,\cdot)$ باشد. چون $R'\subseteq R$ و نیز چون شرکت پذیری برای $\cdot$ و قوانین پخشی برقرارند، لذا $(R',+,\cdot)$ خود تشکیل یک حلقه می‌دهد. معمولاً اعمال $+$ و $\cdot$ را نمی‌نویسیم و R' را زیرحلقه R می‌نامیم. هنگامی که R' و R میدان هستند، R' زیرمیدان R نامیده می‌شود.

قضیه زیر شرطی لازم و کافی را برای زیرحلقه بودن یک زیر مجموعه به دست می‌دهد. با این شرایط، به سادگی تحقیق می‌شود که آیا زیر مجموعه‌ای ناتهی از یک حلقه R یک زیرحلقه هست یا

خیر.

قضیه ۲۰۱۰۱۱ فرض کنید R یک حلقه باشد. زیر مجموعه ناتهی R' از R یک زیرحلقه R است اگر و تنها اگر به ازای هر $x,y\in R'$، $x-y\in R'$ و $xy\in R'$.

اثبات. ابتدا فرض کنید که R' زیرحلقه‌ای از R باشد. در این صورت R' یک حلقه است و لذا به ازای هر $x,y\in R'$، $x-y,xy\in R'$. بعکس، فرض‌کنید به ازای هر $x,y\in R'$، $x-y\in R'$ و $xy\in R'$. چون به ازای هر $x,y\in R'$، $x-y\in R'$، لذا بنابر قضیه ۳۰۱۰۴، $(R',+)$ زیرگروهی از $(R,+)$ است. بنابر فرض، به ازای هر $x,y\in R'$، $xy\in R'$. از این رو R' زیرحلقه‌ای از R است. ■

مثال ۳۰۱۰۱۱ (i) حلقه اعداد صحیح زوج $\mathbf{E}$ یک زیرحلقه از $\mathbf{Z}$ است. $\mathbf{E}$ بدون ۱ می‌باشد.

(ii) زیر مجموعه $\mathbf{E}_8=\{[0],[2],[4],[6]\}$ از $\mathbf{Z}_8$ را در نظر بگیرید. در این صورت $\mathbf{E}_8$ زیرحلقه‌ای از $\mathbf{Z}_8$ است. از این رو، $\mathbf{E}_8$ تعویض‌پذیر است. به هر حال، $\mathbf{E}_8$ عنصر همانی ندارد و دارای مقسوم علیه‌های صفر $[2]$، $[4]$ و $[6]$ است.

مثال ۴۰۱۰۱۱ فرض کنید $Q_{\mathbf{Z}}=\{(a_1,a_2,a_3,a_4)\mid a_i\in\mathbf{Z}, i=1,2,3,4\}$. اعمال $+$ و $\cdot$ را روی $Q_{\mathbf{Z}}$ همانند مثال ۱۵۰۱۰۱۰ تعریف کنید. چون تفاضل و حاصلضرب اعداد صحیح، عددی صحیح است، به ازای هر $(a_1,a_2,a_3,a_4),(b_1,b_2,b_3,b_4)\in Q_{\mathbf{Z}}$ داریم:

$$(a_1,a_2,a_3,a_4)-(b_1,b_2,b_3,b_4)\in Q_{\mathbf{Z}}$$

و

$$(a_1,a_2,a_3,a_4)\cdot(b_1,b_2,b_3,b_4)\in Q_{\mathbf{Z}}$$

ازاین رو، $Q_{\mathbf{Z}}$ زیرحلقه‌ای از $Q_{\mathbf{R}}$ است. توجه می‌کنیم که $Q_{\mathbf{Z}}$ تعویض ناپذیر، دارای عنصر همانی، و فاقد مقسوم علیه صفر است. حال $(0,2,0,0)\in Q_{\mathbf{Z}}$ و $(0,2,0,0)^{-1}=(0,-\frac{1}{2},0,0)\notin Q_{\mathbf{Z}}$. بنابراین $Q_{\mathbf{Z}}$ یک حلقه تقسیم نمی‌باشد.

مثال ۵۰۱۰۱۱ قرار دهید $Q_{\mathbf{E}}=\{(a_1,a_2,a_3,a_4)\mid a_i\in\mathbf{E}, i=1,2,3,4\}$. اعمال $+$ و $\cdot$ را روی $Q_{\mathbf{E}}$ همانند مثال ۱۵۰۱۰۱۰ تعریف کنید. چون تفاضل و حاصلضرب اعداد صحیح زوج، عددی صحیح زوج است، لذا $Q_{\mathbf{E}}$ زیرحلقه‌ای از $Q_{\mathbf{Z}}$ می‌باشد. در واقع، $Q_{\mathbf{E}}$ حلقه‌ای تعویض ناپذیر، فاقد عنصر همانی و مقسوم علیه صفر است.

مثال ۶۰۱۰۱۱ حلقه $M_2(\mathbf{Z})$ از مثال ۴۰۱۰۱۰ را در نظر بگیرید. فرض کنید $M_2(\mathbf{E})$ مجموعه تمام ماتریس های 2×2 با درایه‌هایی از $\mathbf{E}$ باشد. چون مجموع، تفاضل و حاصلضرب اعداد صحیح زوج، عددی صحیح زوج است، نتیجه می‌شود که $M_2(\mathbf{E})$ زیرحلقه‌ای از $M_2(\mathbf{Z})$ است. همچنین، $M_2(\mathbf{E})$ حلقه‌ای تعویض ناپذیر، فاقد عنصر همانی و مقسوم علیه صفر است.

همانند روند قضیه ۲۰۱۰۱۱، می‌توان قضیه بعدی را اثبات کرد، که اثبات آن را به عنوان تمرین واگذار می‌کنیم.

قضیه ۷۰۱۰۱۱ فرض کنید F یک میدان باشد. زیر مجموعه ناتهی S از F یک زیرمیدان از F است اگر و تنها اگر

(i) S شامل بیش از یک عنصر باشد،

(ii) به ازای هر $x,y\in S$، $x-y,xy\in S$، و

(iii) به ازای هر $x\in S$، $x\neq 0$ و $x^{-1}\in S$. ■

مثال ۸۰۱۰۱۱ $\mathbf{Q}$ و $\mathbf{Q}[\sqrt{2}]=\{a+b\sqrt{2}\mid a,b\in\mathbf{Q}\}$ زیرمیدان‌هایی از $\mathbf{R}$ می‌باشند (تمرین حل شده ۴ زیر را ببینید).

قضیه ۹۰۱۰۱۱ فرض کنید R یک حلقه (یا میدان) و $\{R_i\mid i\in\Lambda\}$ خانواده‌ای ناتهی از زیرحلقه‌های (یا زیرمیدان های) R باشد. در این صورت $\cap_{i\in\Lambda}R_i$ زیرحلقه‌ای (یا زیرمیدانی) از R است.

اثبات. چون به ازای هر $i\in\Lambda$، $0\in R_i$، لذا $0\in\cap_{i\in\Lambda}R_i$ و بنابراین $\cap_{i\in\Lambda}R_i\neq\varnothing$. فرض کنید $x,y\in\cap_{i\in\Lambda}R_i$. در این صورت به ازای هر $i\in\Lambda$، $x,y\in R_i$. چون هر R_i یک زیرحلقه می‌باشد، لذا به ازای هر $i\in\Lambda$، $x-y,xy\in R_i$. از این رو، $x-y,xy\in\cap_{i\in\Lambda}R_i$. بنابراین $\cap_{i\in\Lambda}R_i$ تشکیل زیرحلقه‌ای از R می‌دهد. ■

جالب است توجه کنید که اشتراک تمام زیرمیدان های $\mathbf{R}$ برابر است با $\mathbf{Q}$.

۱۱۰۱۰۱ تمرین های حل شده

تمرین ۱. فرض کنید X مجموعه‌ای نامتناهی باشد. در این صورت $(P(X),\Delta,\cap)$ حلقه‌ای یکدار است. قرار دهید

$$R=\{A\in P(X)\mid A \text{ متناهی است}\}.$$

گزاره‌های زیر را اثبات کنید.

(i) R زیرحلقه‌ای از $P(X)$ است.

(ii) R بدون همانی است.

(iii) به ازای هر $A\in R$، $A\neq\varnothing$، A یک مقسوم علیه صفر در R است.

(iv) به ازای هر $A\in P(X)$، $A\neq X$، $A\neq\varnothing$، A یک مقسوم علیه صفر در $P(X)$ است.

حل: (i) چون $\varnothing$ متناهی است، لذا $\varnothing\in R$ و لذا R ناتهی است. فرض کنید $A,B\in R$. در این صورت A و B متناهی‌اند و لذا $A\cap B$ متناهی می‌باشد. حال $A\Delta B=(A\cup B)\setminus(A\cap B)$ و لذا $A\Delta B$

متناهی است. بنابراین، $A\Delta B, A\cap B\in R$. لذا R تحت اعمال Δ و $\cap$ بسته است. حال به آسانی می‌توان تحقیق کرد که $(R,\Delta,\cap)$ یک زیرحلقه است.

(ii) فرض کنید R دارای عنصری همانی مانند E باشد. در این صورت E متناهی است. چون X نامتناهی است، $a\in X$ ای وجود دارد به طوری که $a\notin E$. حال $\{a\}\in R$. بنابراین $\{a\}=E\cap\{a\}=\varnothing$، که یک تناقض است. از این رو، R هیچ عنصر همانی ندارد.

(iii) فرض کنید $A\in R$ و $A\neq\varnothing$. چون A متناهی و X نامتناهی است، $x\in X$ ای وجود دارد به طوری که $x\notin A$. حال $\{x\}\in R$. چون $A\cap\{x\}=\varnothing$، لذا A یک مقسوم علیه صفر است.

(iv) فرض کنید $A\in P(X)$ به قسمی باشد که $A\neq X$ و $A\neq\varnothing$. در این صورت $x\in X$ ای وجود دارد به طوری که $x\notin A$. از این رو، $A\cap\{x\}=\varnothing$ و لذا A یک مقسوم علیه صفر است.

تمرین ۲. فرض کنید R حلقه‌ای باشد که به ازای هر $a\in R$، $a^2+a\in C(R)$. نشان دهید که R تعویض پذیر است.

حل: فرض کنید $x,y\in R$. در این صورت $(x+y)^2+(x+y)\in C(R)$، یعنی $x^2+xy+yx+x+y\in C(R)$. چون $x^2+x, y^2+y\in C(R)$ و $C(R)$ یک زیرحلقه است (تمرین ۱۴، صفحه ۳۷۱)، لذا $xy+yx\in C(R)$. بنابراین $x(xy+yx)=(xy+yx)x$ و لذا $x^2y+xyx=xyx+yx^2$. بنابراین، $x^2y=yx^2$. حال $x^2+x\in C(R)$ و لذا $y(x^2+x)=(x^2+x)y$. از این رو، $yx^2+yx=x^2y+xy$ و لذا $xy=yx$. این ثابت می‌کند که R تعویض پذیر است.

تمرین ۳. تمام زیرحلقه‌های حلقه اعداد صحیح $\mathbf{Z}$ را پیدا کنید. زیرحلقه‌هایی را بیابید که شامل عنصر همانی نیستند.

حل: فرض کنید n عددی صحیح نامنفی باشد و $T_n=n\mathbf{Z}=\{nt\mid t\in\mathbf{Z}\}$. چون $0\in T_n$، لذا $T_n\neq\varnothing$. فرض کنید $a=nt$ و $b=ns$ دو عنصر در T_n باشند. در این صورت

$$a-b=nt-ns=n(t-s)\in T_n\ ,\ \ ab=(nt)(ns)=n(t(ns))\in T_n$$

از این رو، T_n زیرحلقه‌ای از $\mathbf{Z}$ است. حال نشان می‌دهیم که اگر A زیرحلقه‌ای دلخواه از $\mathbf{Z}$ باشد، آنگاه به ازای عدد صحیح نامنفی n ای، $A=T_n$.

فرض کنید A زیرجلقه‌ای از $\mathbf{Z}$ باشد. اگر $A=\{0\}$، آنگاه $A=0\mathbf{Z}$. فرض کنید $A\neq\{0\}$. در این صورت $m\in A$ ای وجود دارد به طوری که $m\neq 0$. حال $-m\in A$ و لذا A شامل عدد صحیح مثبتی است. بنابر اصل خوش ترتیبی، A شامل عضو ابتداست. فرض کنید n عضو ابتدای A باشد. در این صورت $n\mathbf{Z}\subseteq A$. فرض کنید $m\in A$. بنابر الگوریتم تقسیم، اعداد صحیح r و q موجودند به طوری که $m=nq+r$، که $0\leq r<n$. چون $n\in A$، $nq\in A$. از این رو، $r=m-nq\in A$. کمین

بودن n ایجاب می‌کند که $r=0$ و لذا $m=nq\in nZ$. بنابراین، $A=nZ$. اگر $n\neq 1$، آنگاه nZ شامل عنصر همانی نیست.

تمرین ۴. نشان دهید که $Q[\sqrt{2}]=\{a+b\sqrt{2}\mid a,b\in Q\}$ زیرمیدانی از میدان R است.

حل: چون $0+0\sqrt{2}\in Q[\sqrt{2}]$ ، $0=0$ ، لذا $Q[\sqrt{2}]\neq\varnothing$. فرض کنید $a+b\sqrt{2}$, $c+d\sqrt{2}\in Q[\sqrt{2}]$. در این صورت

$$(a+b\sqrt{2})-(c+d\sqrt{2})=(a-c)+(b-d)\sqrt{2}\in Q[\sqrt{2}]$$

و

$$(a+b\sqrt{2})(c+d\sqrt{2})=(ac+2bd)+(ad+bc)\sqrt{2}\in Q[\sqrt{2}]$$

حال $0+0\sqrt{2}$ و $1+0\sqrt{2}$ عناصر متمایزی در $Q[\sqrt{2}]$ می‌باشند. بنابراین $Q[\sqrt{2}]$ بیش از یک عنصر دارد. فرض کنید $a+b\sqrt{2}$ عنصری ناصفر از $Q[\sqrt{2}]$ باشد. در این صورت a و b هر دو با هم صفر نیستند. نشان می‌دهیم که $a-b\sqrt{2}\neq 0$. فرض کنید $a-b\sqrt{2}=0$. دراین صورت $a=b\sqrt{2}$. اگر $b=0$، آنگاه $a=0$. بنابراین a و b هر دو صفرند، که یک تناقض است. اگر $b\neq 0$، آنگاه $\sqrt{2}=\frac{a}{b}\in Q$، که یک تناقض است. از این رو، $a-b\sqrt{2}\neq 0$. به طور مشابه $a+b\sqrt{2}\neq 0$. بنابراین $a^2-2b^2=(a+b\sqrt{2})(a-b\sqrt{2})\neq 0$. حال

$$\frac{1}{a+b\sqrt{2}}=\frac{a-b\sqrt{2}}{a^2-2b^2}=\frac{a}{a^2-2b^2}-\frac{b}{a^2-2b^2}\sqrt{2}\in Q[\sqrt{2}]\ .$$

چون $(a+b\sqrt{2})(\frac{1}{a+b\sqrt{2}})=1$ ، لذا $(a+b\sqrt{2})^{-1}$ در $Q[\sqrt{2}]$ وجود دارد . در نتیجه، بنابر قضیه ۷۰۱۰۱۱ ، $Q[\sqrt{2}]$ زیرمیدانی از R خواهد بود.

۱۱۰۱۰۲ تمرینها

۱. گزاره های زیر را اثبات کنید.

(i) $T_1=\left\{\begin{bmatrix} a & b \\ 0 & c\end{bmatrix}\mid a,b,c\in Z\right\}$ زیرحلقه‌ای از $M_2(Z)$ است.

(ii) $T_2=\left\{\begin{bmatrix} a & b \\ -b & a\end{bmatrix}\mid a,b\in Z\right\}$ زیرحلقه‌ای از $M_2(Z)$ است.

(iii) $T_3=\left\{\begin{bmatrix} a & 0 \\ 0 & a\end{bmatrix}\mid a\in Z\right\}$ زیرحلقه‌ای از $M_2(Z)$ است.

(iv) $T_4=\left\{\begin{bmatrix} a & b \\ 0 & a\end{bmatrix}\mid a,b\in Z\right\}$ زیرحلقه‌ای از T_1 است.

۲. در حلقه اعداد صحیح Z ، تعیین کنید کدامیک از زیر مجموعه‌های مفروض زیرحلقه‌اند:

(i) مجموعه اعداد صحیح به صورت $4k+2$، که $k\in\mathbf{Z}$.

(ii) مجموعه اعداد صحیح به صورت $4k+1$، که $k\in\mathbf{Z}$.

(iii) مجموعه اعداد صحیح به صورت $4k$، که $k\in\mathbf{Z}$.

۳. نشان دهید که $T=\{[0],[5]\}$ زیرحلقه‌ای از حلقه $\mathbf{Z}_{10}$ است.

۴. فرض‌کنید R حلقه‌ای یکدار باشد. نشان دهید که زیرمجموعه $T=\{n1\mid n\in\mathbf{Z}\}$ زیرحلقه‌ای از R است.

۵. فرض کنید R یک حلقه و n عددی صحیح مثبت باشد. نشان دهید که مجموعه $\{a\in R\mid na=0\}$ زیرحلقه ای از R است.

۶. نشان دهید که $T=\left\{\begin{bmatrix} a & b\sqrt{3} \\ -b\sqrt{3} & a\end{bmatrix}\mid a,b\in\mathbf{R}\right\}$ زیرحلقه ای از $M_2(\mathbf{R})$ است.

۷. نشان دهید که $\mathbf{Q}[\sqrt{3}]$ و $\mathbf{Q}[\sqrt{5}]$ زیرمیدان‌هایی از میدان $\mathbf{R}$ هستند، اما $\mathbf{Z}[\sqrt{2}]=\{a+b\sqrt{2}\mid a,b\in\mathbf{Z}\}$ زیرمیدانی از $\mathbf{R}$ نیست.

۸. نشان دهید که $\mathbf{Q}[i]=\{a+bi\mid a,b\in\mathbf{Q}\}$ زیرمیدانی از $\mathbf{C}$ است، که در آن $i^2=-1$.

۹. نشان دهید که $F=\left\{\begin{bmatrix} a & -b \\ b & a\end{bmatrix}\mid a,b\in\mathbf{Z}_5\right\}$ زیرحلقه‌ای از $M_2(\mathbf{Z}_5)$ است. آیا F یک میدان است؟

۱۰. فرض کنید w یک ریشهٔ $x^2+x+1=0$ باشد. ثابت کنید که $T=\{a+bw\mid a,b\in\mathbf{Q}\}$ زیرمیدانی از میدان اعداد مختلط است.

۱۱. فرض کنید F میدانی با مشخصه $p>0$ باشد. نشان دهید $T=\{a\in F\mid a^p=a\}$ زیرمیدانی از F است.

۱۲. ثابت کنید که $T=\left\{\begin{bmatrix} x+y & y \\ -y & x\end{bmatrix}\mid x,y\in\mathbf{Z}\right\}$ زیرحلقه‌ای از $M_2(\mathbf{Z})$ است. همچنین نشان دهید که هر عنصر ناصفر T در $M_2(\mathbf{R})$ یکه است.

۱۳. فرض کنید R حلقه‌ای تعویض پذیر باشد. نشان دهید که مجموعه $T=\{r\in R\mid r^n=0$، به ازای عدد صحیح n ای$\}$ زیرحلقه‌ای از R است.

۱۴. ثابت کنید که $C(R)$ زیرحلقه‌ای از R است که تعویض پذیر نیز می‌باشد.

۱۵. فرض کنید e عنصری خود توان در R باشد. ثابت کنید که مجموعه $eRe=\{ere\mid r\in R\}$ زیرحلقه‌ای از R است که e همان عنصر همانی می‌باشد.

۱۶. مرکز حلقه $M_2(\mathbf{R})$ را تعیین کنید.

۱۷. ثابت کنید که مشخصه یک زیرمیدان همان مشخصه میدان می‌باشد.

۱۸. تمام زیرحلقه‌های یکدار را از حلقه $\mathbf{Z}_{16}$ به دست آورید.

۱۹. تمام زیرمیدان‌های $\mathbf{Z}_p$ را بیابید، که در آن p عددی صحیح اول است.

۲۰. فرض کنید R حلقه‌ای بدون هیچ عنصر ناصفر پوچ توان باشد. نشان دهید که به ازای هر $r\in R$ و هر عنصر خود توان $a\in R$، $(ara-ra)^2=0$. از این رو، نشان دهید که $C(R)$ شامل تمام عناصر خود توان است.

۲۱. فرض کنید $C=\{f:\mathbf{R}\to\mathbf{R}\mid f$ روی $\mathbf{R}$ پیوسته‌است$\}$. به‌ازای‌هر $f,g\in C$ و هر $x\in\mathbf{R}$، اعمال $+$ و $\cdot$ را روی C به صورت زیر تعریف کنید:

$$(f+g)(x)=f(x)+g(x),$$

$$(f\cdot g)(x)=f(x)g(x).$$

(i) نشان دهید که C تشکیل یک حلقه می‌دهد.

(ii) فرض کنید $D=\{f\in C\mid f$ روی $\mathbf{R}$ مشتق پذیر است$\}$. نشان دهید که D زیرحلقه‌ای از C است.

۲۲. فرض کنید R یک حلقه و به ازای هر $a,b\in R$، تابع $f:R\to[0,1]$ به قسمی باشد که

$$f(a-b)\geq min\{f(a),f(b)\},$$

$$f(ab)\geq min\{f(a),f(b)\}.$$

ثابت کنید که به ازای هر $t\in I(f)$، $R_t=\{x\in R\mid f(x)\geq t\}$ زیرحلقه‌ای از R است.

۲۳. در تمرین های زیر، اگر گزاره درست است، اثباتی بنویسید؛ در غیر این صورت مثال نقضی ارائه دهید.

(i) اجتماع دو زیرحلقه یک زیرحلقه می‌باشد.

(ii) عنصر همانی یک زیرحلقه همیشه عنصر همانی حلقه است.

(iii) $\mathbf{Q}$ تنها زیرمیدان $\mathbf{R}$ است.

(iv) $\mathbf{Q}[\sqrt{3}]=\{a+b\sqrt{3}\mid a,b\in\mathbf{Q}\}$ برابر است با اشتراک تمام زیرمیدان‌های $\mathbf{R}$ که شامل $\sqrt{3}$ هستند.

(v) مجموعه اعداد صحیح $\mathbf{Z}$، زیرحلقه‌ای از میدان اعداد حقیقی است.

(vi) هر زیرگروه جمعی $\mathbf{Z}$، زیرحلقه‌ای از $\mathbf{Z}$ است.

۱۱.۲ ایده‌آل ها و حلقه‌های خارج قسمت

در این بخش به معرفی مفاهیم ایده‌آل و حلقه‌های خارج قسمت می‌پردازیم. این مفاهیم به مفاهیم زیرگروه‌های نرمال و گروههای خارج قسمت شباهت دارد.

مسأله بسیار معروفی به نام "قضیهٔ آخر فرما" باعث تحقیق در مورد ایده‌آل‌ها می‌شود. فرما (۱۶۰۱-۱۶۶۵) بسیاری از نتایج‌اش را در حاشیه کتاب محاسبات دیافونتوس با عجله نوشت. در مورد این قضیه خاص، فرما نوشت که وی قضیهٔ بسیار جالبی را کشف کرده است که به دلیل طولانی بودن اثباتش نمی‌توان آن را در حاشیه نوشت. قضیه بدین صورت آمده است: اگر n عددی صحیح بزرگتر از ۲ باشد، آنگاه هیچ اعداد صحیح مثبت x, y, zای وجود ندارند به طوری که $x^n+y^n=z^n$. به هر حال، هیچ شخصی تا قرن‌ها قادر به اثبات این نتیجه نبود؛ در سال ۱۹۹۴، آندرو واینر بعد از سال‌ها کار اثباتی برای آن به دست داد.

در سال ۱۸۴۳، کومر (۱۸۱۰-۱۸۹۳) گمان کرد که اثباتی برای قضیه آخر فرما به دست آورده است. به هر حال، کومر به طور نادرستی یکتایی تجزیه اعداد مختلط به صورت $x+\lambda y$را، که در آن به ازای عدد اول فرد pای، $\lambda^p=1$ فرض گرفته بود. دیرکله Dirichlet (۱۸۰۵-۱۸۵۹) فرض نادرستی درباره یکتایی اعداد انجام داده بود. کومر تلاش خود را برای حل قضیه آخر فرما ادامه داد. وی به وسیله معرفی مفهوم "عدد ایده‌آل" موفقیتی نسبی به دست آورد. ددکیند (۱۸۳۱-۱۹۱۶) ایده‌های کومر را برای کشف مفهوم یک ایده‌آل به کار برد. همچنین کرونکر (۱۸۳۱-۱۹۱۶) نقش مهمی در توسعه نظریه حلقه‌ها ایفا نمود.

تعریف ۱۰۲.۱۱ فرض کنید R یک حلقه باشد. زیر مجموعه ناتهی I از R یک ایده‌آل چپ (راست) R نامیده می‌شود هر گاه به ازای هر $a,b\in I$ و هر $r\in R$، $a-b\in I$ و $ra\in I$ ($ar\in I$ و $a-b\in I$).

زیر مجموعه ناتهی I از حلقه R را یک ایده‌آل (دو طرفه) R می‌نامند هر گاه I یک ایده‌آل چپ و راست R باشد.

از تعریف ایده‌آل چپ (یا راست)، نتیجه می‌شود که اگر I یک ایده‌آل چپ (یا راست) R باشد، آنگاه I زیرحلقه‌ای از R است. همچنین اگر R حلقه‌ای تعویض پذیر باشد، آنگاه هر ایده‌آل چپ یک ایده‌آل راست و هر ایده‌آل راست یک ایده‌آل چپ نیز می‌باشد. بنابراین، برای حلقه‌های تعویض‌پذیر هر ایده‌آل چپ یا راست، یک ایده‌آل می‌باشد.

بنابر قضیه ۲۰۱.۱۱، واضح است که یک زیرمجموعه ناتهی I از حلقه R یک ایده‌آل است اگر و تنها اگر $(I,+)$ زیرگروهی از $(R,+)$ باشد و به ازای هر $a\in I$ و هر $r\in R$، $ar, ra\in I$.

مثال ۲۰۲۰۱۱ فرض کنید R یک حلقه باشد. زیر مجموعه‌های $\{0\}$ و R از R ایده‌آل‌های (چپ ، و راست) R می‌باشند. این ایده‌آل ها را **ایده‌آل‌های بدیهی** می‌نامند. تمام ایده‌آل های (راست،و چپ) دیگر نابدیهی نامیده می‌شوند.

ایده‌آل I از یک حلقه R را ایده آل سره نامند هرگاه $I\neq R$.

مثال ۳۰۲۰۱۱ فرض کنید $n\in\mathbf{Z}$ و $I=\{nk\,|\,k\in\mathbf{Z}\}$. بنابر تمرین حل شده ۳ (صفحه)، I یک زیرحلقه است. همچنین به ازای هر $r\in\mathbf{Z}$، $(nk)r=n(kr)\in I$ و $r(nk)=n(rk)\in I$. از این رو، I ایده‌آلی از $\mathbf{Z}$ است.

اینک مثالی از یک حلقه ارائه می‌دهیم که دارای یک ایده‌آل چپ می‌باشد ولی ایده‌آل راست نیست و یک ایده‌آل راست دارد که ایده‌آل چپ نمی‌باشد و نیز زیرحلقه‌ای دارد که ایده‌آل چپ (یاراست) نیست .

مثال ۴۰۲۰۱۱ حلقه $M_2(\mathbf{Z})$ را در نظر بگیرید. قرار دهید

$$I_1=\left\{\begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix}\,\middle|\,a,b\in\mathbf{Z}\right\},$$

$$I_2=\left\{\begin{bmatrix} 0 & a \\ 0 & b \end{bmatrix}\,\middle|\,a,b\in\mathbf{Z}\right\},$$

$$I_3=\left\{\begin{bmatrix} a & c \\ b & d \end{bmatrix}\,\middle|\,\text{اعداد صحیح زوجند } a\text{ ، } b\text{ ، } c\text{ ، } d\right\}$$

و

$$I_4=\left\{\begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix}\,\middle|\,a\in\mathbf{Z}\right\}.$$

چون $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}\in I_1$، $I_1\neq\varnothing$. فرض کنید $\begin{bmatrix} c & 0 \\ d & 0 \end{bmatrix}, \begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix}\in I_1$ و $\begin{bmatrix} x & y \\ z & w \end{bmatrix}\in M_2(\mathbf{Z})$. در این صورت

$$\begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix}-\begin{bmatrix} c & 0 \\ d & 0 \end{bmatrix}=\begin{bmatrix} a-c & 0 \\ b-d & 0 \end{bmatrix}\in I_1$$

و

$$\begin{bmatrix} x & y \\ z & w \end{bmatrix}\begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix}=\begin{bmatrix} xa+yb & 0 \\ za+wb & 0 \end{bmatrix}\in I_1,$$

این نشان می‌دهد که I_1 یک ایده‌آل چپ $M_2(\mathbf{Z})$ است. حال $\begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix} \in I_1$ و $\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \in M_2(\mathbf{Z})$،

اما

$$\begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix} \notin I_1$$

.

از این رو، I_1 یک ایده‌آل راست $M_2(\mathbf{Z})$ نیست. به طور مشابه، I_2 یک ایده‌آل راست $M_2(\mathbf{Z})$ است، اما یک ایده‌آل چپ نمی‌باشد، I_3 یک ایده‌آل از $M_2(\mathbf{Z})$ است، و I_4 یک زیرحلقه است، اما یک ایده‌آل از $M_2(\mathbf{Z})$ نمی‌باشد.

خاطر نشان می‌کنیم که خواننده به شباهت چند نتیجه بعدی با نتایج متناظر آن در جبر خطی و نظریه گروهها توجه نماید.

قضیه ۵.۲.۱۱ فرض کنید R یک حلقه و $\{I_\alpha \mid \alpha \in \Lambda\}$ خانواده‌ای ناتهی از ایده‌آل های چپ (یا راست) R باشد. در این صورت $\cap_{\alpha\in\Lambda} I_\alpha$ یک ایده‌آل چپ (یا راست) R است.

اثبات. فرض کنید $\{I_\alpha \mid \alpha \in \Lambda\}$ خانواده‌ای ناتهی از ایده‌آل های چپ R باشد. چون به ازای هر α، $0 \in I_\alpha$، بنابراین $0 \in \cap_{\alpha\in\Lambda} I_\alpha$ و لذ $\cap_\alpha I_\alpha \neq \varnothing$. فرض کنید $a, b \in \cap_\alpha I_\alpha$، در این صورت به‌ازای هر α، $a, b \in I_\alpha$. چون‌هر I_α یک ایده‌آل چپ است، لذابه ازای هر α، $a-b \in I_\alpha$. از این رو، $a-b \in \cap_\alpha I_\alpha$. فرض کنید $r \in R$. چون هر I_α یک ایده‌آل چپ R است، لذا به ازای هر α، $ra \in I_\alpha$ و بنابراین $ra \in \cap_\alpha I_\alpha$. در نتیجه $\cap_\alpha I_\alpha$ یک ایده‌آل چپ R است. به طور مشابه، اگر $\{I_\alpha \mid \alpha \in \Lambda\}$ خانواده‌ای ناتهی از ایده‌آل‌های راست R باشد، آنگاه $\cap_\alpha I_\alpha$ یک ایده‌آل راست R است. ■

فرض کنید $a_1, a_2, \ldots, a_n \in R$، در این صورت مجموع $a_1+a_2+\ldots+a_m$ را با نماد $\Sigma_{i=1}^{n} a_i$ نشان می‌دهیم.

تعریف ۶.۲.۱۱ فرض کنید S زیر مجموعه‌ای ناتهی از حلقه R باشد. $<S>_l$ را اشتراک تمام ایده‌آل‌های چپ R تعریف کنید که شامل S می‌باشند. در این صورت ایده‌آل چپ $<S>_l$، ایده‌آل چپ تولید شده توسط S نامیده می‌شود. به طور مشابه، می‌توان $<S>_r$، ایده‌آل راست تولید شده توسط S، و $<S>$، ایده‌آل تولید شده توسط S را تعریف کرد.

توجه کنید که $<S>_l$ کوچکترین ایده‌آل چپ R شامل S است.

قضیه ۷.۲.۱۱ فرض کنید R یک حلقه و S زیر مجموعه‌ای ناتهی از R باشد. در این صورت

$$<S>_l = \{\Sigma_{i=1}^{k} r_i s_i + \Sigma_{j=1}^{l} n_j s'_j \mid r_i \in R,\ n_j \in \mathbf{Z},\ s_i,\ s'_j \in S,\ 1 \le i \le k,\ 1 \le j \le l,\ k, l \in \mathbf{N}\}. \quad (i)$$

$$<S>_r=\{\Sigma_{i=1}^{k} s_i r_i+\Sigma_{j=1}^{l} n_j s_j' \mid r_i\in R, n_j\in \mathbf{Z}, s_i, s_j'\in S, \quad (ii)$$
$$1\le i\le k, 1\le j\le l, k,l\in N\}.$$

اثبات. (i) فرض کنید

$$A=\{\Sigma_{i=1}^{k} r_i s_i+\Sigma_{j=1}^{l} n_i s_j' \mid r_i\in R, n_j\in \mathbf{Z}, s_i, s_j'\in S, \quad (i)$$
$$1\le i\le k, 1\le j\le l, k,l\in \mathbf{N}\}.$$

چون $<S>_l$ اشتراک تمام ایده‌آل‌های چپ R است که شامل S می‌باشند، داریم $<S>_l\supseteq S$. همچنین چون $<S>_l$ تحت عمل جمع بسته است و نیز از چپ تحت ضرب به وسیله عناصر R بسته می‌باشد، داریم $A\subseteq <S>_l$. حال نشان می‌دهیم که A یک ایده‌آل چپ از R است، به طوری که $A\supseteq S$. در این‌صورت $A\supseteq <S>_l$، زیرا $<S>_l$ کوچکترین ایده‌آل چپ R شامل S می‌باشد. فرض‌کنید $s\in S$. در این صورت $s=0\cdot s+1s\in A$ و لذا $S\subseteq A$. فرض کنید

$$\Sigma_{i=1}^{k} r_i s_i+\Sigma_{j=1}^{l} n_j s_j', \Sigma_{i=1}^{t} \bar{r}_i \bar{s}_i+\Sigma_{j=1}^{m} \bar{n}_j \bar{s}_j'\in A.$$

در این صورت

$$(\Sigma_{i=1}^{k} r_i s_i+\Sigma_{j=1}^{l} n_j s_j')-(\Sigma_{i=1}^{t} \bar{r}_i \bar{s}_i+\Sigma_{j=1}^{m} \bar{n}_j \bar{s}_j')$$
$$=(\Sigma_{i=1}^{k} r_i s_i+\Sigma_{i=1}^{t}(-\bar{r}_i)\bar{s}_i)+(\Sigma_{j=1}^{l} n_j s_j'+\Sigma_{j=1}^{m}(-\bar{n}_j)\bar{s}_j')\in A.$$

فرض کنید $r\in R$، در این صورت

$$r(\Sigma_{i=1}^{k} r_i s_i+\Sigma_{j=1}^{l} n_j s_j')=\Sigma_{i=1}^{k}(rr_i)s_i+\Sigma_{j=1}^{l}(n_j r)s_j'\in A.$$

از این رو، A یک ایده‌آل چپ R است.

(ii) اثبات مشابه (i) است. ■

نتیجه ۸۰۲۰۱۱ فرض کنید R یک حلقه و S زیر مجموعه‌ای ناتهی از آن باشد. اگر R یکدار باشد، آنگاه

$$<S>_l=\{\sum_{i=1}^{k} r_i s_i \mid r_i\in R, s_i\in S, 1\le i\le k\}. \quad (i)$$

$$<S>_r=\{\sum_{i=1}^{k} s_i r_i \mid r_i\in R, s_i\in S, 1\le i\le k\}. \quad (ii)$$

اثبات. (i) واضح است که $<S>_l\supseteq\{\Sigma_{i=1}^{k} r_i s_i \mid r_i\in R, s_i\in S\}$. فرض کنید

$$\Sigma_{i=1}^{t} r_i s_i+\Sigma_{j=1}^{l} n_j s_j'\in <S>_l.$$

چون R یکدار است، لذا $n_j s_j'=(n_j 1)s_j'$ و $n_j 1\in R$. بنابراین،

$$\Sigma_{i=1}^{t} r_i s_i+\Sigma_{j=1}^{l} n_j s_j'=\Sigma_{i=1}^{t} r_i s_i+\Sigma_{j=1}^{l}(n_j 1)s_j'\in\{\Sigma_{i=1}^{k} r_i s_i \mid r_i\in R, s_i\in S, 1\le i\le k\}.$$

از این رو، $<S>_l\subseteq\{\Sigma_{i=1}^{k} r_i s_i \mid r_i\in R, s_i\in S, 1\le i\le k\}$.

(ii) اثبات مشابه (i) است. ■

اگر $S=\{a_1,a_2,\dots,a_n\}$، آنگاه ایده‌آل چپ $<S>_l$ تولید شده توسط S را با نماد $<a_1,a_2,\dots,a_n>$ نشان می‌دهند. در این حالت، $<S>_l$ را یک ایده‌آل چپ متناهیاً تولید شده می‌نامیم. اصطلاح مشابه‌ای برای $<S>_r$ و $<S>$ به کار می‌رود. اگر $S=\{a\}$، آنگاه $<a>_l$ را ایده‌آل اصلی چپ تولید شده توسط a می‌نامند. $<a>_r$ ایده‌آل اصلی راست تولید شده توسط a و $<a>$ ایده‌آل اصلی تولید شده توسط a نامیده می‌شوند.

نتیجه ۹۰۲۰۱۱ فرض کنید R یک حلقه باشد و $a\in R$.

(i) در این صورت

$$<a>_l=\{ra+na \mid r\in R, n\in \mathbf{Z}\}.$$

(ii) اگر R حلقه‌ای یکدار باشد، آنگاه

$$<a>_l=\{ra \mid r\in R\}.$$

اثبات. (i) این ادعا از تساوی زیر حاصل می‌شود

$$\sum_{i=1}^{k} r_i a+\sum_{j=1}^{m} n_j a=(\sum_{i=1}^{k} r_i)a+(\sum_{j=1}^{m} n_j)a.$$

(ii) این قسمت از (i) و نتیجه ۸۰۲۰۱۱ به دست می‌آید. ■

به طور مشابه، می‌توان ثابت کرد که $<a_r>=\{ar+na \mid r\in R, n\in \mathbf{N}\}$ و

$$<a>=\{ra+as+na+\Sigma_{i=1}^{k} r_i a_i s_i \mid r,s,r_i,s_i\in R, n\in \mathbf{Z}, 1\le i\le k, k\in \mathbf{N}\}.$$

زیرمجموعه‌های $Ra=\{ra \mid r\in R\}$ و $aR=\{ar \mid r\in R\}$ را از R در نظر بگیرید. اگر R فاقد عنصر همانی باشد، آنگاه Ra (aR) یک ایده‌آل چپ (راست) R خواهد بود (تمرین ۴، صفحه ۳۸۶). در مثال بعدی توضیح داده شده است که شرط $a\in Ra$ $(a\in aR)$ الزامی نیست.

مثال ۱۰۰۲۰۱۱ حلقه اعداد صحیح زوج $\mathbf{E}$ را در نظر بگیرید. $\mathbf{E}$ عنصر همانی ندارد. حال

$$<2>=\{r2+n2 \mid r\in \mathbf{E}, n\in \mathbf{Z}\}=\{0,\pm 2,\pm 4,\dots\},\ 2\in <2>$$

به هر حال $\{r2 \mid r\in \mathbf{E}\}=\{0,\pm 4,\pm 8,\dots\}$ که شامل ۲ نیست.

قضیه ۱۱۰۲۰۱۱ فرض کنید R حلقه‌ای یکدار باشد. در این صورت R یک حلقه تقسیم است اگر و تنها اگر R دارای هیچ ایده‌آل چپ نابدیهی نباشد.

اثبات. فرض کنید R یک حلقه تقسیم باشد. همچنین فرض کنید که I یک ایده‌آل چپ R باشد به طوری که $I\supset\{0\}$. در این صورت $a\in I$ ای وجود دارد به طوری که $a\neq 0$ و چون I یک ایده‌آل چپ است، $1=a^{-1}a\in I$. از این رو، به ازای هر $r\in R$، $r=r1\in I$، یعنی $I=R$.

بعکس، فرض کنید R دارای ایده‌آل چپ نابدیهی نباشد، $a\in R$ و $a\neq 0$. در این صورت

$<a>_l = R$ و لذا $1 \in <a>_l$. حال $<a>_l = \{ra \mid r \in R\}$. بنابراین $r \in R$ ای وجود دارد به طوری که $ra = 1$. این ایجاب می‌کند که $r \neq 0$. همانند حالت عنصر ناصفر a، به ازای $t \in R$ ای داریم که $tr = 1$. بنابراین $t = t1 = t(ra) = (tr)a = 1a = a$. پس $ra = 1 = ar$ و لذا a یکه است. در نتیجه هر عنصر ناصفر R یکه است. از این رو، R یک حلقه تقسیم می‌باشد. ■

در امتداد روند قضیه فوق، می‌توان ثابت کرد که حلقه یکدار R یک حلقه تقسیم است اگر و تنها اگر R دارای ایده‌آل راست نابدیهی نباشد.

نتیجه زیر بلافاصله از قضیه فوق حاصل می‌شود.

نتیجه ۱۲۰۲۰۱۱ فرض کنید R یک حلقه تعویض‌پذیر یکدار باشد. در این صورت R یک میدان است اگر و تنها اگر R دارای ایده‌آل نابدیهی نباشد.

تعریف ۱۳۰۲۰۱۱ حلقه R را ساده نامند هرگاه $R \neq \{0\}$ و $\{0\}$ و R تنها ایده‌آل‌های R باشند.

مثال ۱۴۰۲۰۱۱ هر حلقه تقسیم یک حلقه ساده است.

مثال ۱۵۰۲۰۱۱ در این مثال نشان می‌دهیم که $M_2(\mathbf{R})$ حلقه‌ای ساده است. فرض کنید A یک ایده‌آل ناصفر $M_2(\mathbf{R})$ باشد. در این صورت عنصر ناصفر $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in A$ وجود دارد. حال حداقل یکی از عناصر a، b، c، d ناصفرند. چون A ایده‌آل است و $\begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \in M_2(\mathbf{R})$، داریم

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} b & 0 \\ d & 0 \end{bmatrix} \in A,$$

$$\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} c & d \\ 0 & 0 \end{bmatrix} \in A,$$

و

$$\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} d & 0 \\ 0 & 0 \end{bmatrix} \in A.$$

بنابراین، A شامل ماتریسی مانند $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ است به طوری که $a \neq 0$. حال $a^{-1} \in \mathbf{R}$ و

$$\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} a^{-1} & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ ca^{-1} & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \in A.$$

بنابراین،

$$\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \in A.$$

سرانجام،

$$\begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} \in A.$$

از این رو،

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} \in A.$$

این ایجاب می‌کند که $A = M_2(\mathbf{R})$.

مثال فوق نشان می‌دهد که حلقه‌های ساده‌ای وجود دارند که حلقه تقسیم نیستند.

به ازای $a \in R$، aRa مجموعه $\{ara \mid r \in R\}$ را نشان می‌دهد.

حال **مجموع** و **حاصلضرب** ایده‌آل‌های چپ (راست) را در نظر می‌گیریم.

فرض کنید A و B دو زیرمجموعه ناتهی از حلقه R باشند. **مجموع** و **حاصلضرب** A و B را به صورت زیر تعریف کنید:

$$A + B = \{a + b \mid a \in A, b \in B\}$$

$$AB = \{a_1b_1 + a_2b_2 + \dots + a_nb_n \mid a_i \in A, b_i \in B, i = 1, 2, \dots, n, n \in \mathbf{N}\}$$

بنابراین، AB مجموعه تمام حاصلجمع‌های متناهی Σa_ib_i را نشان می‌دهد، که $a_i \in A$ و $b_i \in B$.

فرض کنید $n \in \mathbf{N}$. به طور استقرایی، تعریف می‌کنیم

$$A^1 = A,$$

$$A^n = AA^{n-1}, \text{ اگر } n > 1$$

اینک بعضی خواص جالب این اعمال را فهرست می‌کنیم.

قضیه ۱۶.۲.۱۱ فرض کنید A، B و C ایده‌آل‌های چپ (یا راست) حلقه R باشند. در این صورت گزاره‌های زیر برقرارند.

(i) $A+B=B+A$ یک ایده‌آل چپ (یا راست) R است.

(ii) $A+A=A$.

(iii) $(A+B)+C=A+(B+C)$.

(iv) AB یک ایده‌آل چپ (یا راست) R است.

(v) $(AB)C=A(BC)$.

(vi) اگر A، B و C ایده‌آل باشند، آنگاه $A(B+C)=AB+AC$، $(B+C)A=BA+CA$.

(vii) اگر A یک ایده‌آل راست و B یک ایده‌آل چپ باشد، آنگاه $AB \subseteq A \cap B$.

(viii) R منظم است اگر و تنها اگر به ازای هر ایده‌آل راست A و هر ایده‌آل چپ B،

$AB=A\cap B$.

(ix) مجموعه $I(R)$ از تمام ایده‌آل‌های R با رابطه شمولیت مجموعه‌ها به عنوان یک مجموعه مرتب جزئی تشکیل یک مشبکه مدولی می‌دهد.

اثبات. فقط قسمت‌های $(viii)$ و (ix) را اثبات کرده، دیگر خواص را به عنوان تمرین واگذار می‌کنیم.

$(viii)$ فرض کنید R حلقه‌ای منظم باشد و $a\in A\cap B$. در این صورت $b\in R$ای وجود دارد به طوری که $a=aba$. چون B یک ایده‌آل چپ است و $a\in B$، $ba\in B$. بنابراین، $a=a(ba)\in AB$. از این رو $A\cap B\subseteq AB$. بنابر (vii)، $AB\subseteq A\cap B$. در نتیجه $AB=A\cap B$، بعکس، فرض کنید که به ازای هرایده‌آل راست A و ایده‌آل چپ B از R، $AB=A\cap B$. همچنین فرض کنید $a\in R$ و ایده‌آل راست تولید شده توسط a یعنی $<a>_r$ را در نظر بگیرید. چون $<a>_r$ یک ایده‌آل راست است، $<a>_rR\subseteq <a>_r$. همچنین، بنابر فرض $<a>_r\cap R=<a>_rR$. از این رو،

$$a\in <a>_r\cap R=<a>_rR .$$

بنابراین، به ازای $a_i\in <a>_r$، $b_i\in R$ که $i=1,2,\dots,n$، $a=\Sigma_{i=1}^{n}a_ib_i$. از گزاره‌های نتیجه ۹۰۲۰۱۱ نتیجه می‌شود که به ازای $t_i\in R$، $n_i\in \mathbf{Z}$، $i=1,2,\dots,n$، $a_i=at_i+n_ia$. بنابراین،

$$a=\Sigma_{i=1}^{n}a_ib_i=\Sigma_{i=1}^{n}(at_i+n_ia)b_i=a(\Sigma_{i=1}^{n}(t_ib_i+n_ib_i))\in aR .$$

این ایجاب می‌کندکه $<a>_r\subseteq aR$. چون $aR\subseteq <a>_r$، $<a>_r=aR$. به طور مشابه، $<a>_l=Ra$. حال نتیجه می‌شود که $a\in aR\cap Ra=(aR)(Ra)\subseteq aRa$. از این رو، $b\in R$ای وجود دارد به طوری که $a=aba$، یعنی a منظم است و در نتیجه، R منظم است.

(ix) با استدلالی مشابه اثبات قضیه ۱۶۰۱۰۴، می‌توان نشان داد که $(I(R),\subseteq)$ یک مجموعه مرتب جزئی است. برای نشان دادن این که $(I(R),\subseteq)$ یک مشبکه است، فرض کنید $A,B\in I(R)$. حال $A\cap B, A+B\in I(R)$. همچنین، $A,B\subseteq A+B$. فرض کنید $C\in I(R)$ به قسمی باشد که $A,B\subseteq C$. چون C یک ایده‌آل است، $A+B\subseteq C$. از این رو، $A+B=A\vee B$، کوچکترین کران بالای $\{A,B\}$. به طور مشابه، $A\cap B=A\wedge B$، بزرگترین کران پائین $\{A,B\}$ است. بنابراین، $I(R)$ یک مشبکه‌است. برای نشان دادن این که $(I(R),\subseteq)$ یک مشبکه مدولی است، فرض کنید A، B و C سه عنصر در $I(R)$ باشند به طوری که $A\subseteq C$. توجه کنید که $A\vee(B\wedge C)=A+(B\cap C)$ و $(A\vee B)\wedge C=(A+B)\cap C$. حال $A+(B\cap C)\subseteq(A+B)\cap C$ ولذا $A\vee(B\wedge C)\subseteq(A\vee B)\wedge C$. فرض کنید $x\in(A+B)\cap C$. در این صورت $x\in C$ و $x\in A+B$. بنابراین به ازای $a\in A\subseteq C$ای و $b\in B$ای، $x=a+b$. این ایجاب می‌کند که $b=x-a\in C$ و لذا $b\in B\cap C$، که نشان می‌دهد

$x \in A+(B\cap C)$. از این رو، $(A+B)\cap C \subseteq A+(B\cap C)$، یعنی، $(A\vee B)\wedge C \subseteq A\vee(B\wedge C)$. بنابراین، $A\vee(B\wedge C)\subseteq(A\vee B)\wedge C$. در نتیجه، $I(R)$ یک مشبکه مدولی است. ■

حال همانند گروههای خارج قسمت برای حلقه‌ها عمل می‌کنیم. فرض کنید R یک حلقه و I ایده‌آلی از آن باشد. در این صورت $(I,+)$ زیرگروهی نرمال از $(R,+)$ است، زیرا گروه دوم، تعویض‌پذیر است. از این رو، اگر R/I به ازای هر $r\in R$، مجموعه تمام همرده‌های $r+I=\{r+a \mid a\in I\}$ را نشان دهد، آنگاه $(R/I,+)$ گروهی تعویض‌پذیر است، که در آن به ازای هر $r+I, r'+I\in R/I$،

$$(r+I)+(r'+I)=(r+r')+I$$

حال به ازای هر $r+I, r'+I\in R/I$، ضربی را روی R/I به صورت $(r+I)\cdot(r'+I)=rr'+I$ تعریف‌کنید. در این صورت $(R/I,+,\cdot)$ تشکیل یک حلقه می‌دهد. جزئیات را به عنوان تمرین واگذار می‌کنیم.

تعریف ۱۷۰۲۰۱۱ اگر R یک حلقه و I ایده‌آلی از آن باشد، آنگاه حلقه $(R/I,+,\cdot)$ حلقه خارج قسمت R به وسیله I نامیده می‌شود.

قضیه ۱۸۰۲۰۱۱ فرض کنید $n\in\mathbf{Z}$ عددی صحیح مثبت ثابت باشد. در این صورت شرایط زیر معادلند.

(i) n اول است.

(ii) $\mathbf{Z}/<n>$ یک حوزه صحیح است.

(iii) $\mathbf{Z}/<n>$ یک میدان است.

اثبات. $(i)\Leftarrow(ii)$: فرض کنید $a+<n>, b+<n>\in\mathbf{Z}/<n>$ و

$$(a+<n>)(b+<n>)=0+<n>.$$

در این صورت $ab+<n>=0+<n>$ و لذا $ab\in<n>$. بنابراین $r\in\mathbf{Z}$ای وجود دارد به طوری که $ab=rn$. این ایجاب می‌کند که $n\mid ab$. چون n عددی اول است، $n\mid a$ یا $n\mid b$، یعنی $a\in<n>$ یا $b\in<n>$ و از این رو $a+<n>=0+<n>$ یا $b+<n>=0+<n>$. این ایجاب می‌کند که $\mathbf{Z}/<n>$ دارای مقسوم علیه صفر نیست. این نشان می‌دهد که $\mathbf{Z}/<n>$ یک حوزه صحیح است.

$(ii)\Leftarrow(iii)$: چون $\mathbf{Z}/<n>$ یک حوزه صحیح متناهی است، نتیجه از قضیه ۲۳۰۱۰۱۰ حاصل می‌شود.

$(iii)\Leftarrow(i)$: فرض کنید n اول نباشد. در این صورت به ازای $1<n_1<n$ و $1<n_2<n$، $n=n_1n_2$. حال $n_1+<n>$ و $n_2+<n>$ عناصری ناصفر از $\mathbf{Z}/<n>$ می‌باشند و

$$(n_1+<n>)(n_2+<n>)=n_1n_2+<n>=n+<n>=0+<n>\ .$$

چون $\mathbf{Z}/<n>$ یک میدان است، لذا دارای مقسوم علیه صفر نیست. بنابراین $n_1+<n>=0+<n>$ یا $n_2+<n>=0+<n>$، که یک تناقض است. در نتیجه n عددی اول است. ■

تعریف ۱۹۰۲۰۱۱ فرض کنید I ایده‌آلی از حلقه R باشد.

(i) I یک ایده‌آل پوچ نامیده می‌شود هرگاه هر عنصر آن عنصری پوچ توان باشد.

(ii) I یک ایده‌آل پوچ‌توان نامیده می‌شود هرگاه به ازای عدد صحیح مثبت nای، $I^n=\{0\}$.

مثال ۲۰۰۲۰۱۱ در حلقه $\mathbf{Z}_8$، ایده‌آل $I=\{[0],[4]\}$ یک ایده‌آل پوچ و نیز پوچ‌توان است. $I^2=\{\Sigma_{i=1}^{k}[a_i][b_i]\,|\,[a_i][b_i]\in I, k\in\mathbf{N}\}$، زیرا $16\,|\,a_ib_i$.

از تعریف نتیجه می‌شود که هر ایده‌آل پوچ‌توان یک ایده‌آل پوچ است. مثال زیر نشان می‌دهد که عکس این مطلب نادرست است. در این مثال، حلقه R را به وسیله حلقه‌های $\mathbf{Z}_{p^n}$ می‌سازیم، که در آن $n=1,2,\ldots$، یعنی به وسیله حلقه‌های $\mathbf{Z}_p$، $\mathbf{Z}_{p^2}$، $\mathbf{Z}_{p^3}$، ...، که در آن p عددی اول است.

مثال ۲۱۰۲۰۱۱ فرض کنید p عددی اول ثابت و R گردایه تمام دنباله‌های $\{a_n\}$ باشد به طوری که $a_n\in\mathbf{Z}_{p^n}$ $(n\geq 1)$ و عدد صحیح مثبت mای (وابسته به $\{a_n\}$) موجود باشد به طوری که به ازای هر $n\geq m$، $a_n=[0]$. به ازای هر $\{a_n\},\{b_n\}\in R$، اعمال جمع و ضرب را روی R به صورت زیر تعریف کنید:

$$\{a_n\}+\{b_n\}=\{a_n+b_n\},$$
$$\{a_n\}\{b_n\}=\{a_nb_n\}\ .$$

از خواننده می‌خواهیم که تحقیق کند R تحت این دو عمل تشکیل یک حلقه تعویض‌پذیر می‌دهد، که در آن عنصر صفر عبارت است از دنباله $\{a_n\}$ به طوری که به ازای هر n، $a_n=[0]$ و معکوس جمعی دنباله $\{a_n\}$ برابر است با دنباله $\{-a_n\}$. حال در $\mathbf{Z}_{p^n}$، $[p]$ عنصری پوچ توان است، زیرا $[p]^n=[p^n]=[0]$. بنابراین به ازای هر $[r]\in\mathbf{Z}_{p^n}$، $[p][r]=[pr]$ عنصری پوچ توان است. لذا هر عنصر $[p]\mathbf{Z}_{p^n}$ عنصری پوچ توان است. قرار دهید

$$I=\{\{[p]a_1,[p]a_2,\ldots,[p]a_n,[0],[0],\ldots\}\in R\,|\,n\in\mathbf{N}, a_i\in\mathbf{Z}_{p^i}\ ,i=1,2,\ldots,n\}.$$

در این صورت I یک ایده‌آل از R است. همچنین هر عنصر I پوچ توان است. حال نشان می‌دهیم که I پوچ توان نیست. فرض کنید I پوچ توان باشد. در این صورت عدد مثبت mای وجود دارد به طوری که $I^m=\{0\}$. حال دنباله $\{a_n\}$ که به ازای هر $n=1,2,\ldots,m+1$، $a_n=[p]$ و به‌ازای هر $n\geq m+2$، $a_n=0$، عنصری پوچ توان از I است. در این صورت

$$\{a_n\}^m=\{[0],[0],\ldots,[0],[p^m],[0],[0],\ldots\}\ ,$$

که جمله $(m+1)$ ام این دنباله $[p^m]$ و دیگر جملات برابر با صفرند. چون $[p^m]$ در $\mathbf{Z}_{p^{m+1}}$ صفر نیست، می‌یابیم که $\{a_n\}^m \neq 0$ و $\{a_n\}^m \in I^m = \{0\}$، که یک تناقض است. این ایجاب می‌کند که I پوچ‌توان نباشد.

قضیه ۲۲۰۲۰۱۱ فرض کنید R حلقه‌ای تعویض‌پذیر و یکدار و I مجموعه تمام عناصر پوچ توان R باشد. در این صورت

(i) I یک ایده‌آل پوچ از R است،

(ii) حلقه خارج قسمت R/I دارای هیچ عنصر پوچ توان ناصفر نیست.

اثبات. (i) چون $0 \in I$، $I \neq \varnothing$. فرض کنید $a, b \in I$، در این صورت اعداد صحیح مثبت m و nای وجود دارند به طوری که $a^n = 0$ و $b^m = 0$. چون R تعویض‌پذیر است، می‌توان نوشت

$$(a-b)^{n+m} = a^{n+m} + \ldots + (-1)^r \binom{n+m}{r} a^{n+m-r} b^r + \ldots + (-1)^{n+m} b^{n+m}$$

جمله عمومی عبارت فوق برابر است با $(-1)^r \binom{n+m}{r} a^{n+m-r} b^r$، که در آن $0 \leq r \leq m+n$. اگر $r \leq m$، آنگاه $n+m-r \geq n$ و از این رو $a^{n+m-r} = a^n a^{m-r} = 0$. مجدداً اگر $r > m$، آنگاه $b^r = b^{m+(r-m)} = b^m b^{r-m} = 0$. بنابراین $(-1)^r \binom{n+m}{r} a^{n+m-r} b^r = 0$، که $r = 0, 1, \ldots, n+m$. این ایجاب می‌کند که $(a-b)^{n+m} = 0$، یعنی $a-b$ پوچ توان است و لذا $a-b \in I$. فرض کنید $r \in R$. دراین صورت $(ra)^n = r^n a^n = r^n 0 = 0$. چون R تعویض‌پذیر است، لذا $(ar)^n = (ra)^n = 0$. بنابراین، $ar, ra \in I$. در نتیجه، I یک ایده‌آل از R است. چون هر عنصر I پوچ‌توان است، لذا I پوچ است.

(ii) فرض کنید $a+I$ عنصری پوچ توان از R/I باشد در این صورت به ازای عددی صحیح مثبت، $(a+I)^n = I$. اما $a^n + I = (a+I)^n$. بنابراین، $a^n + I = I$، که ایجاب می‌کند $a^n \in I$. چون هر عنصر I پوچ‌توان است، عدد صحیح مثبت mای وجود دارد به طوری که $(a^n)^m = 0$، یعنی $a^{nm} = 0$، که نشان می‌دهد a پوچ توان است و لذا $a \in I$. این ایجاب می‌کند که $a+I = I$. از این رو، R/I هیچ عنصر پوچ توان ناصفری ندارد. ■

قضیه ۲۳۰۲۰۱۱ فرض کنید A و B دو ایده‌آل پوچ از حلقه تعویض‌پذیر یکدار R باشند. در این صورت $A+B$ یک ایده‌آل پوچ است.

اثبات. بنابر قضیه ۱۶۰۲۰۱۱، می‌دانیم که $A+B$ یک ایده‌آل R است. فرض کنید I مجموعه تمام عناصر پوچ توان R باشد. در این صورت $A \subseteq I$، $B \subseteq I$ و بنابر قضیه ۲۲۰۲۰۱۱، I یک ایده‌آل است. از این رو، $A+B \subseteq I$. چون I ایده‌آل پوچ است، $A+B$ نیز پوچ است. ■

۱۱۰۲۰۱ تمرین‌های حل شده

تمرین ۱. تمام ایده‌آل‌های $\mathbf{Z}$ را بیابید.

حل: از تمرین حل شده ۳ (صفحه ۳۶۹)، می‌دانیم که زیرحلقه‌های $\mathbf{Z}$ عبارتند از زیر مجموعه‌های $n\mathbf{Z}$، که $n = 0, 1, 2, \ldots$. حال نشان می‌دهیم که این زیرحلقه‌ها دقیقاً ایده‌آل‌های $\mathbf{Z}$ هستند. اگر ایده‌آلی از $\mathbf{Z}$ باشد، آنگاه I زیرحلقه‌ای از $\mathbf{Z}$ است و لذا به ازای عدد صحیح نامنفی nای، $I=n\mathbf{Z}$. حال قرار دهید $I=n\mathbf{Z}$ (n عدد صحیح نامنفی است). در این صورت I یک زیرحلقه است. اگر $r\in\mathbf{Z}$، آنگاه $rI=r(n\mathbf{Z})=n(r\mathbf{Z})\subseteq n\mathbf{Z}=I$. به طور مشابه، $Ir\subseteq I$. ازاین‌رو، I یک ایده‌آل $\mathbf{Z}$ است.

تمرین ۲. فرض کنید R حلقه‌ای باشد که دارای هیچ مقسوم علیه صفر نیست. نشان دهید که اگر هر زیرحلقه‌ای از R یک ایده‌آل R باشد، آنگاه R تعویض‌پذیر است.

حل: فرض کنید $0\neq a\in R$، در این صورت $C(a)=\{x\in R \mid xa=ax\}$ زیرحلقه‌ای از R است و از این رو یک ایده‌آل R است. بنابراین، به ازای هر $r\in R$، $ra\in C(a)$. فرض کنید $r\in R$. حال $ara=ra^2$ و لذا $ar=ra$. از این رو، a در مرکز R قرار دارد. چون a دلخواه است، لذا R تعویض‌پذیر است.

تمرین ۳. مثالی از یک حلقه R و ایده‌آل‌های A_i، $i\in I$، ارائه کنید به طوری که اگر $i\neq j$، $A_i\cap A_j=\{0\}$، اما $A_i\cap(\Sigma_{j\neq i} A_j)$.

حل: فرض کنید $R=\{0,a,b,c\}$. به ازای هر $x,y\in R$، اعمال $+$ و $\cdot$ را روی R به صورت زیر تعریف کنید:

$$2a=2b=2c=0, xy=0,$$
$$a+b=b+a=c, a+c=c+a=b,$$
$$b+c=c+b=a.$$

در این‌صورت $(R,+,\cdot)$ یک حلقه است. قراردهید $A_1=\{0,a\}$، $A_2=\{0,b\}$، و $A_3=\{0,c\}$. در این صورت $A_1+A_2=A_1+A_3=A_2+A_3=R$ و $A_1\cap A_2=A_1\cap A_3=A_2\cap A_3$.

تمرین ۴. مثالی از یک حلقه R و ایده‌آل‌های A و B ارائه دهید به طوری که $AB\subset A\cap B$.

حل: فرض کنید R حلقه تمرین حل شده ۳ باشد. فرض کنید $A=B=\{0,a\}$. در این صورت $AB=\{0\}\subset\{0,a\}=A\cap B$.

تمرین ۵. تمام حلقه‌های تعویض‌پذیر R را مشخص کنید به طوری که تنها دارای دو ایده‌آل R و $\{0\}$ باشند.

حل: فرض کنید R حلقه‌ای تعویض‌پذیر باشد به طوری که تنها ایده‌آل‌های آن R و $\{0\}$

باشند. حال R^2 یک ایده‌آل R است. بنابراین $R^2=\{0\}$ یا $R^2=R$.

حالت ۱. $R^2=\{0\}$. در این صورت به ازای هر $a,b\in R$، $ab=0$. در این حالت، هر زیرگروه $(R,+)$ یک ایده‌آل است. از این رو، $(R,+)$ دارای هیچ زیرگروه سره نیست و لذا بنابر تمرین ۲۱ (صفحه ۱۸۶)، $(R,+)$ گروهی دوری از مرتبه عدد اول است.

حالت ۲. $R^2=R$. فرض کنید $0\neq a\in R$. در این صورت aR یک ایده‌آل R است. از این رو، $aR=\{0\}$ یا $aR=R$. فرض کنید $aR=\{0\}$. قراردهید $T=\langle a\rangle$. در این صورت T یک ایده‌آل R است و $a\in T$. بنابراین $T=R$. حال $aR=\{0\}$ ایجاب می‌کند که $TR=\{0\}$ و از این رو $R^2=\{0\}$، که یک تناقض است. بنابراین، $aR=R$. در نتیجه، به ازای هر $0\neq a\in R$، $aR=R$. حال نشان می‌دهیم که R دارای مقسوم علیه صفر نیست. فرض کنید a و b دو عنصر ناصفر از R باشند به طوری که $ab=0$. قرار دهید $T=\{c\in R\mid ac=0\}$. به آسانی ملاحظه می‌شود که T ایده‌آلی ناصفر از R است. از این رو، بنابر فرض $T=R$. این ایجاب می‌کند که $R=aR=aT=\{0\}$، که یک تناقض با $R=R^2=\{0\}$ است. در نتیجه، R دارای مقسوم علیه صفر نیست. حال، به ازای $0\neq a\in R$، $aR=R$ و لذا به ازای $e\in R$ ای، $ae=a$. چون $a\neq 0$، بایستی $e\neq 0$. همچنین، چون R دارای هیچ مقسوم علیه صفر نیست، $a(e^2-e)=0$ ایجاب می‌کند که $e^2=e$. حال به ازای هر $b\in R$، $eb=e^2b$ ایجاب می‌کند که $e(b-eb)=0$ و از این رو $b=eb=be$. این نشان می‌دهد که e عنصر همانی R است. همچنین، $aR=R$ ایجاب می‌کند که به ازای $b\in R$ ای، $e=ab$. از این رو، a^{-1} در R وجود دارد. در نتیجه R یک میدان است.

لذا از دو حالت فوق نتیجه می‌گیریم که R حلقهٔ صفر با تعداد اولی از عناصر است یا R یک میدان است.

۱۱.۲.۲ تمرینها

۱. فرض کنید $T_2(\mathbf{Z})=\left\{\begin{bmatrix} a & b\\ 0 & c\end{bmatrix}\mid a,b,c\in\mathbf{Z}\right\}$ حلقه تمام ماتریس‌های بالا مثلثی روی $\mathbf{Z}$ باشد.

(i) ثابت کنید که $I=\left\{\begin{bmatrix} 0 & b\\ 0 & c\end{bmatrix}\mid b,c\in\mathbf{Z}\right\}$ ایده‌آلی از $T_2(\mathbf{Z})$ است. حلقه خارج قسمت $T_2(\mathbf{Z})/I$ را بیابید.

(ii) ثابت کنید که $I=\left\{\begin{bmatrix} 0 & a\\ 0 & 0\end{bmatrix}\mid a\in\mathbf{Z}\right\}$ ایده‌آلی از $T_2(\mathbf{Z})$ است. حلقه خارج قسمت $T_2/(\mathbf{Z})I$ را به دست آورید.

۲. در حلقه $\mathbf{Z}_{24}$، نشان دهید که $I=\{[0],[8],[16]\}$ یک ایده‌آل است. تمام عناصر حلقه خارج قسمت $\mathbf{Z}_{24}/I$ را بیابید.

۳. نشان دهید که مجموعه $\{a-b$ زوج است و $a,b\in\mathbf{Z}\}$ $I=\{a+bi\sqrt{5}\,|\,a,b\in\mathbf{Z}$ یک ایده‌آل حلقه $\mathbf{Z}[i\sqrt{5}]$ است.

۴. فرض کنید R یک حلقه باشد و $a\in R$. نشان دهید که aR ایده‌آل راست R و Ra ایده‌آل چپ R است.

۵. فرض کنید R یک حلقه باشد. همچنین فرض کنید A یک ایده‌آل چپ A و B یک ایده‌آل راست R باشد. نشان دهید که AB یک ایده‌آل R است و $BA\subseteq A\cap B$.

۶. فرض کنید R یک حلقه باشد به طوری که $R^2\neq\{0\}$. ثابت کنید که R یک حلقه تقسیم است اگر و تنها اگر R هیچ ایده‌آل چپ نابدیهی نداشته باشد.

۷. فرض کنید R حلقه‌ای یکدار باشد. ثابت کنید که R دارای هیچ ایده‌آل چپ نابدیهی نیست اگر و تنها اگر R هیچ ایده‌آل راست نابدیهی نداشته باشد.

۸. فرض کنید I_1 و I_2 ایده‌آل‌هایی از حلقه R باشند. ثابت کنید $I_1\cup I_2$ ایده‌آلی از R است اگر و تنها اگر $I_1\subseteq I_2$ یا $I_2\subseteq I_1$.

۹. فرض کنید I و J ایده‌آل‌هایی از حلقه R باشند. ثابت کنید که $I+J$ ایده‌آلی از R است و $I+J=\langle I\cup J\rangle$، ایده‌آل تولید شده توسط $I\cup J$ است.

۱۰. فرض کنید I یک ایده‌آل از حلقه تعویض‌پذیر R باشد و $a\in R$. ثابت کنید که

$$\langle I\cup\{a\}\rangle=\{i+ra+na\,|\,i\in I,r\in R,n\in\mathbf{Z}\}.$$

۱۱. فرض کنید m و n اعداد صحیح مثبتی در $\mathbf{Z}$ باشند. ثابت کنید که

(i) $\langle m,n\rangle=\langle m\rangle+\langle n\rangle=\langle d\rangle$، که در آن d بزرگترین مقسوم علیه مشترک m و n است،

(ii) $\langle m\rangle\cap\langle n\rangle=\langle q\rangle$، که در آن q کوچکترین مضرب مشترک m و n است.

۱۲. تمام ایده‌آل‌های حاصلضرب دکارتی $F_1\times F_2$ از دو میدان F_1 و F_2 را بیابید.

۱۳. حاصلضرب دکارتی حلقه $R_1\times R_2$ از حلقه‌های R_1 و R_2 را در نظر بگیرید.

(i) اگر I_1 یک ایده‌آل از R_1 و I_2 یک ایده‌آل از R_2 باشد، ثابت کنید $I_1\times I_2$ ایده‌آلی از $R_1\times R_2$ است.

(ii) فرض کنید R_1 و R_2 یکدار باشند و I ایده‌آلی از $R_1\times R_2$ باشد. آیا ایده‌آل‌های I_1 از R_1 و I_2 از R_2 وجود دارند به طوری که $I=I_1\times I_2$؟

۱۴. فرض کنید I یک ایده‌آل از حلقه R باشد. ثابت کنید که حلقه خارج قسمت R/I حلقه‌ای تعویض‌پذیر است اگر و تنها اگر به ازای هر $a,b\in R$، $ab-ba\in I$.

۱۵. فرض کنید $T=\{\frac{a}{b} \mid \frac{a}{b}\in \mathbf{Q}$, a و b متباین‌اند و ۵ عدد b را عاد نمی‌کند$\}$. نشان دهید که T تحت جمع و ضرب معمولی تشکیل یک حلقه می‌دهد. همچنین ثابت کنید که

$$I=\{\frac{a}{b}\in T \mid \text{۵ عدد } a \text{ را عاد می‌کند}\}$$

ایده‌آلی از T است و حلقه خارج قسمت T/I یک میدان است.

۱۶. فرض کنید I ایده‌آلی از حلقه R باشد. ثابت کنید که اگر R حلقه‌ای تعویض‌پذیر با عنصر همانی باشد، آنگاه R/I حلقه‌ای تعویض‌پذیر با عنصر همانی است. اگر F دارای هیچ مقسوم علیه صفر نباشد، آیا همین مطلب لزوماً برای R/I درست است؟

۱۷. فرض کنید I ایده‌آلی از حلقه تعویض‌پذیر R باشد. پوچساز I را مجموعه زیر تعریف کنید:

$$annI=\{r\in R \mid ra=0 \text{ ، به ازای هر } a\in I\}.$$

ثابت کنید که $annI$ ایده‌آلی از R است.

۱۸. در حلقه $\mathbf{Z}_{20}$، ثابت کنید که $I=\{[n] \mid n \text{ زوج است}\}$ یک ایده‌آل است. $annI$ را بیابید.

۱۹. در حلقه $\mathbf{Z}[i]$، نشان دهید که $I=\{a+bi \mid a,b\in \mathbf{Z}$, a و b زوج اند$\}$ یک ایده‌آل است. $annI$ را بیابید.

۲۰. در حلقه تعویض‌پذیر منظم یکدار R، ثابت کنید که هر ایده‌آل اصلی I توسط یک عنصر خود توان تولید می‌شود و به ازای هر ایده‌آل اصلی I، ایده‌آل اصلی J وجود دارد به طوری که $R=I+J$ و $I\cap J=\{0\}$.

۲۱. ثابت کنید که هر ایده‌آل از یک حلقه منظم، منظم است.

۲۲. ثابت کنید که حلقه R منظم است اگر و تنها اگر هر ایده‌آل اصلی چپ R به وسیلهٔ عنصری خود توان تولید شده باشد.

۲۳. ثابت کنید که در یک حلقه منظم تعویض‌پذیر یکدار، هر ایده‌آل متناهیاً تولید شده، یک ایده‌آل اصلی است.

۲۴. در حلقه R، ثابت کنید که $\{0\}$ تنها ایده‌آل پوچ توان است اگر و تنها اگر به ازای هر ایده‌آل A و B از R، $AB=\{0\}$ ایجاب می‌کند که $A\cap B=\{0\}$.

۲۵. فرض کنید R یک حلقه و $f:R\to[0,1]$ به قسمی باشد که به ازای هر $a,b,r\in R$،

$$f(a-b)\geq min\{f(a),f(b)\} \quad , \quad f(rb)\geq f(b)$$

ثابت کنید:

(i) به ازای هر $a\in R$، $f(0)\geq f(a)$،

(ii) به ازای هر $a\in R$، $f(a)=f(-a)$،

(iii) به ازای هر $t \in I(f)$، $R_t=\{x \in R \mid f(x) \geq t\}$ یک ایده‌آل چپ R است،

(iv) $R_0=\{a \in R \mid f(a)=f(0)\}$ یک ایده‌آل چپ R است.

۲۶. فرض کنید R یک حلقه باشد. رابطه ρ را روی R یک رابطه همنهشتی روی حلقه R نامند هرگاه ρ رابطه‌ای هم‌ارزی روی R باشد و به‌ازای هر $a,b,c \in R$، $a\rho b$ ایجاب می‌کند که $ac\rho bc$، $ca\rho cb$، و $(a+c)\rho(b+c)$. فرض کنید I ایده‌آلی از R و ρ رابطه‌ای باشد که روی R به صورت زیر تعریف شده باشد:

$a\rho b$ اگر و تنها اگر $a-b \in I$

نشان دهید که ρ یک رابطه همنهشتی روی R است.

۲۷. در هر یک از تمرین‌های زیر، در صورت درستی اثبات آن را بنویسید؛ در غیر این صورت مثال نقضی ارائه دهید.

(i) اگر $\{I_i \mid i \in \mathbf{N}\}$ گردایه تمام ایده‌آل‌های R باشد، آنگاه $\cup_{i \in \mathbf{N}} I_i$ ایده‌آلی از R است.

(ii) $\mathbf{Z}$ زیرحلقه‌ای از $\mathbf{R}$ است، اما ایده‌آلی از آن نیست.

(iii) اگر I ایده‌آلی نابدیهی از حوزه صحیح R باشد، آنگاه حلقه خارج قسمت R/I یک حوزه صحیح است.

۱۱۰۳ همریختی‌ها و یکریختی‌ها

در این بخش، همریختی و یکریختی‌ها را معرفی می‌کنیم. این مفاهیم مشابه همریختی‌ها و یکریختی‌ها برای گروهها می‌باشند.

تعریف ۱۰۳۰۱۱ فرض کنید $(R,+,\cdot)$ و $(R',+,\cdot)$ دو حلقه و f تابعی از R به توی R' باشد. در این صورت f را یک همریختی از R به توی R' نامند هرگاه به ازای هر $a,b \in R$،

$$f(a+b)=f(a)+'f(b) \ , \ f(a.b)=f(a)\cdot' f(b)$$

همریختی f از حلقه R به توی حلقه R' را

(i) تکریختی نامند هرگاه f یک به یک باشد،

(ii) برورریختی نامند هرگاه f پوشا باشد، و

(iii) یکریختی نامند هرگاه f یک به یک و پوشا باشد.

اگر f یک یکریختی از حلقه R به روی حلقه R' باشد، آنگاه f^{-1} نیز یک یکریختی از R' به روی R است.

یک یکریختی از حلقه R به روی حلقه R را یک خود ریختی می‌نامند.

تعریف ۲۰۳۰۱۱ دو حلقه را R' و R یکریخت نامند هرگاه یک یکریختی از R به روی R' موجود باشد. وقتی R و R' یک یکریخت باشند، می‌نویسیم $R \cong R'$.

زمانی که از دو حلقه R و R' صحبت می‌کنیم، معمولاً اعمال + و · را برای هر دو حلقه به کار می‌بریم. فرض کنید $f: R \to R'$ یک همریختی حلقه‌ها باشد. چون f عمل + را حفظ می‌کند، لذا f یک همریختی گروههای $(R, +)$ و $(R', +)$ نیز می‌باشد. از این رو، بلافاصله می‌توانیم قضیه ۲۰۱۰۵ را به کاربرده و نتیجه بگیریم که f عنصر ۰ را به $0'$ می‌نگارد. یعنی $f(0) = 0'$، و به ازای هر $a \in R$، $-f(a) = f(-a)$. بعضی از خواص همریختی‌ها در قضیه زیر فهرست شده‌اند. اثبات آنها همانند قضیه ۲۰۱۰۵ است و لذا آنها را به عنوان تمرین به خواننده واگذار می‌کنیم.

قضیه ۳۰۳۰۱۱ فرض کنید f یک همریختی از حلقه R به توی حلقه R' باشد. در این صورت گزاره‌های زیر برقرارند.

(i) $f(0) = 0'$، که در آن $0'$ عنصر صفر R' است.

(ii) به ازای هر $a \in R$، $f(-a) = -f(a)$.

(iii) $f(R) = \{f(a) \mid a \in R\}$ زیرحلقه‌ای از R' است.

(iv) اگر R تعویض‌پذیر باشد، آنگاه $f(R)$ تعویض‌پذیر است.

(v) فرض کنید R دارای همانی باشد و $f(R) = R'$. در این صورت R' دارای عنصر همانی $f(1)$ است.

(vi) اگر $a \in R$ یکه باشد، آنگاه $f(a)$ در R' نیز یکه است و $f(a)^{-1} = f(a^{-1})$. ■

تاکید می‌کنیم که در قسمت (v) قضیه ۳۰۳۰۱۱، اگر f پوشا نباشد، آنگاه R' ممکن است دارای عنصر همانی باشد یا نباشد. حتی اگر R' دارای عنصر همانی باشد، عنصر همانی R لزوماً به همانی R' نگاشته نمی‌شود. توضیح این نکته را در مثال ۷۰۳۰۱۱ می‌آوریم.

تعریف ۴۰۳۰۱۱ فرض کنید f یک همریختی از حلقه R به توی حلقه R' باشد. در این صورت هسته f را که با نماد $Ker\ f$ نشان می‌دهند با مجموعه زیر تعریف می‌شود:

$$Ker\ f = \{a \in R \mid f(a) = 0'\}.$$

از قضیه ۳۰۳۰۱۱، می‌دانیم که $0 \in Ker\ f$.

مثال ۵۰۳۰۱۱ نگاشت همانی از یک حلقه R یک همریختی می‌باشد (در واقع، یک یکریختی). هسته آن برابر است با $\{0\}$. فرض کنید R و R' دو حلقه باشند و به ازای هر $a \in R$، نگاشت $f: R \to R'$ با ضابطه $f(a) = 0'$ تعریف شده باشد. در این صورت f یک همریختی از R به توی R' می‌باشد و $Ker\ f = R$.

مثال ۶۰۳۰۱۱ فرض کنید f نگاشتی از $\mathbf{Z}$ به روی $\mathbf{Z}_n$ باشد که به ازای هر $a\in\mathbf{Z}$ با ضابطه $f(a)=[a]$ تعریف شود. از مثال ۴۰۱۰۵، به ازای هر $a,b\in\mathbf{Z}$، $f(a+b)=f(a)+_n f(b)$. همچنین به ازای هر $a,b\in\mathbf{Z}$، $f(a\cdot b)=[ab]=[a]\cdot_n[b]=f(a)\cdot_n f(b)$. بنابراین f یک همریختی از $\mathbf{Z}$ به روی $\mathbf{Z}_n$ است. با توجه در مثال ۴۰۱۰۵، $Ker\ f=\{qn\,|\,q\in\mathbf{Z}\}$.

در مثال زیر، نشان می‌دهیم که اگر f یک همریختی ناپوشا از حلقه یکدار R به توی حلقه یکدار R' باشد، آنگاه همانی R لزوماً به روی همانی R' نگاشته نمی‌شود.

مثال ۷۰۳۰۱۱ حاصلجمع مستقیم $\mathbf{Z}\oplus\mathbf{Z}$ را در نظر بگیرید (تمرین ۱۷، صفحه ۳۵۷ را ببینید). به ازای هر $a\in\mathbf{Z}$، تابع $f:\mathbf{Z}\to\mathbf{Z}\oplus\mathbf{Z}$ را با ضابطه $f(a)=(a,0)$ تعریف کنید. از تعریف f نتیجه می‌شود که f خوش تعریف است. حال به ازای هر $a,b\in\mathbf{Z}$،

$$f(a+b)=(a+b,0)=(a,0)+(b,0)=f(a)+f(b)\,,$$

$$f(ab)=(ab,0)=(a,0)(b,0)=f(a)f(b)\,.$$

بنابراین f یک همریختی است. همچنین $Ker\ f=\{0\}$. حال $f(1)=(1,0)$، در حالی که $(1,1)$ همانی $\mathbf{Z}\oplus\mathbf{Z}$ است. بنابراین همانی $\mathbf{Z}$ به روی همانی $\mathbf{Z}\oplus\mathbf{Z}$ نگاشته نمی‌شود.

حلقه‌های $\mathbf{Z}$ و $\mathbf{Q}$ را در نظر بگیرید. فرض کنید $\mathbf{Z}\cong\mathbf{Q}$، در این صورت گروههای $(\mathbf{Z},+)$ و $(\mathbf{Q},+)$ یکریختند. به هر حال این ممکن نیست، زیرا $(\mathbf{Z},+)$ گروهی دوری و $(\mathbf{Q},+)$ دوری نیست. در مثال زیر، استدلال دیگری ارائه می‌دهیم که نشان می‌دهد $\mathbf{Z}$ با $\mathbf{Q}$ یکریخت نیست.

مثال ۸۰۳۰۱۱ فرض کنید $\mathbf{Z}\cong\mathbf{Q}$ و $f:\mathbf{Z}\to\mathbf{Q}$ یک یکریختی باشد. در این صورت $f(1)=1$ و $f(0)=0$. فرض کنید n عددی صحیح مثبت باشد. در این صورت

$$f(n)=f(\underbrace{1+1+\dots+1}_{n\text{-مرتبه}})=f(1)+f(1)+\dots+f(1)=nf(1)=n1=n\,.$$

حال فرض کنید که n عددی صحیح منفی باشد. قرار دهید $n=-m$، که در آن m عددی مثبت است. در این صورت

$$f(n)=f(-m)=f(-1-1-\dots-1)=-f(1)-\dots-f(1)=m(-f(1))=-mf(1)=-m1=-m=n\,.$$

از این رو، به ازای هر $n\in\mathbf{Z}$، $f(n)=n$. فرض کنید $0\neq\frac{a}{b}\in\mathbf{Q}|\mathbf{Z}$. چون f پوشاست، $n\in\mathbf{Z}$ای وجود دارد به طوری که $\frac{a}{b}=f(n)=n$، که یک تناقض است. از این رو، $\mathbf{Q}$ یکریخت با $\mathbf{Z}$ نیست.

در مثال زیر، دو حلقه‌ای را در نظر می‌گیریم که به نظر مشابه می‌رسند ولی یکریخت نیستند.

مثال ۹۰۳۰۱۱ در این مثال، نشان می‌دهیم حلقه‌های $\mathbf{Z}[\sqrt{3}]=\{a+b\sqrt{3}\,|\,a,b\in\mathbf{Z}\}$ و $\mathbf{Z}[\sqrt{5}]=\{a+b\sqrt{5}\,|\,a,b\in\mathbf{Z}\}$ یکریخت نیستند. فرض کنید یکریختی $f:\mathbf{Z}[\sqrt{3}]\to\mathbf{Z}[\sqrt{5}]$ موجود باشد. حال $3=(0+\sqrt{3})^2$. بنابراین، $f(3)=f((\sqrt{3})^2)=(f(\sqrt{3}))^2$. چون f یک

یکریختی است، داریم $f(1)=1$. این ایجاب می‌کند که $f(3)=3$. از این رو، $3=(f(\sqrt{3}))^2$. چون $f(\sqrt{3})\in \mathbf{Z}[\sqrt{5}]$ ، لذا بـه ازای $a+b\sqrt{5}\in \mathbf{Z}[\sqrt{5}]$ ، ای $f(\sqrt{3})=a+b\sqrt{5}$. بنابراین $3=(a+b\sqrt{5})^2$ و لذا $3=a^2+5b^2+2ab\sqrt{5}$. اگر $ab=0$ ، آنگاه $3=a^2+5b^2$. اما هیچ عـددصحیح a و b ای وجـودندارد کـه $ab=0$ و $3=a^2+5b^2$. اگـر $ab\neq 0$ ، آنگـاه $\sqrt{5}=\frac{3-a^2-5b^2}{2ab}\in \mathbf{Q}$ ، که یک تناقض است. از این رو، $\mathbf{Z}[\sqrt{3}]$ و $\mathbf{Z}[\sqrt{5}]$ یکریخت نیستند.

در مثال بعد نشان می‌دهیم که حلقه‌های $\mathbf{Z}_n$ و $\mathbf{Z}/<n>$ یکریختند.

مثال ۱۰۰۳۰۱۱ ایده‌آل تولید شده توسط عدد صحیح مثبت ثابت n یعنی $<n>$ را در نظر بگیرید. بنابر نتیجه ۹۰۲۰۱۱ ، $<n>=\{qn \mid q\in \mathbf{Z}\}$. همرده های $<n>$ در $\mathbf{Z}$ عبارتند از $a+<n>=\{a+qn \mid q\in \mathbf{Z}\}$. حال

$$\mathbf{Z}/<n>=\{a+<n> \mid a\in \mathbf{Z}\} .$$

به ازای هر $[a]\in \mathbf{Z}_n$ ، $f:\mathbf{Z}_n\to \mathbf{Z}$ را با ضابطه $f([a])=a+<n>$ تعریف کنید. یادآور می‌شویم که f یک یکریختی از $(\mathbf{Z}_n, +_n)$ به روی $(\mathbf{Z}/<n>, +)$ است (مثال ۱۵۰۱۰۵) حال

$$f([a]\cdot_n[b])=f([ab])=ab+<n>=(a+<n>)(b+<n>)=f([a])f([b]) .$$

بنابراین f یک یکریختی از $\mathbf{Z}_n$ به روی $\mathbf{Z}/<n>$ است.

قضیه ۱۱۰۳۰۱۱ فرض کنید f یک همریختی از حلقه R به توی حلقه R' باشد. در این صورت $Ker\ f$ یک ایده‌آل R است.

اثبات. چـون $0\in Ker\ f$ ، $Ker\ f\neq\varnothing$. فـرض کـنید $a,b\in Ker\ f$ ، در این صـورت $f(a-b)=f(a)-f(b)=0'-0'=0'$ و لذا $a-b\in Ker\ f$. فـرض کـنید $r\in R$ ، در ایـن صـورت $f(ra)=f(r)\cdot f(a)=f(r)\cdot 0'=0'$ و لذا $ra\in R$. به طور مشابه ، $ar\in Ker\ f$. از این رو، $Ker\ f$ یک ایده‌آل R است . ■

در باقیمانده این بخش، قضیه‌های یکریختی را در نظر می‌گیریم که در امتداد قضیه‌های مربوط به گروهها می‌باشند(بخش ۲۰۵).

قضیه ۱۲۰۳۰۱۱ فرض کنید R یک حلقه و I ایده‌آلی از آن باشد. به ازای هـر $a\in R$ ، نگاشت $g:R\to R/I$ را با ضابطه $g(a)=a+I$ تعریف کنید. در این صورت g یک همریختی است، که آن را همریختی طبیعی از R به روی R/I می‌نامند . بعلاوه ، $Ker\ g=I$.

اثبات. به ازای هر از $a,b\in R$ ، $g(a+b)=(a+b)+I=(a+I)+(b+I)=g(a)+g(b)$ و $g(ab)=ab+I=(a+I)(b+I)=g(a)g(b)$. بـرقراری تساوی $Ker\ g=I$ قـضیه ۱۲۰۱۰۵ در نظریه گروهها نتیجه می‌شود . ■

قضیه ۱۳۰۳۰۱۱ فرض کنید R یک همریختی از حلقه R به روی حلقه R' و I ایده‌آلی از R شمول در $Ker\ f$ باشد. همچنین فرض کنید g همریختی طبیعی از R به روی R/I باشد. در این صورت همریختی یکتای h از R/I به روی R' وجود دارد به طوری که $f=h\circ g$. بعلاوه، h یک به یک است اگر و تنها اگر $I=Ker\ f$.

اثبات. یکبار دیگر، روش انجام شده برای گروهها را به کار می‌بریم. به ازای هر $a\in R$، تابع $h:R/I\to R'$ را با ضابطه $h(a+I)=f(a)$ تعریف کنید. هنگامی که تحقیق کنیم h عمل ضرب را حفظ می‌کند، بنابر قضیه ۱۰۲۰۵ نتایج مورد نظر را داریم. حال

$$h((a+I)(b+I))=h(ab+I)=f(ab)=f(a)f(b)=h(a+I)h(a+b).\blacksquare$$

اثبات قضیه زیر مشابه قضیه اول یکریختی برای گروههاست و لذا از اثبات آن صرفنظر می‌کنیم. این قضیه نیز به عنوان قضیه اساسی همریختی هابرای حلقه‌ها شناخته می‌شود.

قضیه ۱۴۰۳۰۱۱ (قضیه اول یکریختی) فرض کنید f یک همریختی از حلقهٔ R به توی حلقهٔ R' باشد. در این صورت $f(R)$ یک ایده‌آل R' است و

$$R/Ker\ f\cong f(R).\blacksquare$$

قضیه زیر را بدون اثبات بیان می‌کنیم. اثباتش ترجمهٔ مستقیمی از اثبات قضیهٔ تناظر گروههاست.

قضیه ۱۵۰۳۰۱۱ (قضیه تناظر) فرض کنید f یک همریختی از حلقهٔ R به روی حلقهٔ R' باشد. در این صورت f تناظری یک به یک حافظ شمولیت را بین ایده‌آل‌های R شامل $Ker\ f$ و ایده‌آل‌های R' القا می‌کند به طریقی که اگر I ایده‌آلی از R شامل $Ker\ f$ باشد، آنگاه $f(I)$ ایده‌آل متناظر در R' است، و چنانچه I' ایده‌آلی از R' باشد، آنگاه $f^{-1}(I')$ ایده‌آل متناظر R است.$\blacksquare$

مثالی همانند مثال ۱۳۰۲۰۵ می‌تواند برای توضیح قضیه ۱۵۰۳۰۱۱ گسترش داده شود.

دو قضیه یکریختی بعد برای حلقه‌ها به ترتیب با قضیه‌های ۸۰۲۰۵ و ۶۰۲۰۵ متناظراند.

قضیه ۱۶۰۳۰۱۱ فرض کنید f یک همریختی از حلقهٔ R به روی حلقهٔ R' و I ایده‌آلی از R باشد به طوری که $I\supseteq Ker\ f$. همچنین فرض کنید g و g' به ترتیب همریختی های طبیعی از R به روی R/I و از R' به روی $R'/f(I)$ باشد. دراین صورت یکریختی یکتای h از R/I به روی $R'/f(I)$ وجود دارد به طوری که $g'\circ f=h\circ g$.$\blacksquare$

نتیجه ۱۷۰۳۰۱۱ فرض کنید I_1 و I_2 ایده‌آل‌هایی از حلقه R باشند به طوری که $I_1\subseteq I_2$. در این صورت

$$(R/I_1)/(I_2/I_1)\cong R/I_2.\blacksquare$$

قضیه ۱۸۰۳۰۱۱ اگر I و J ایده‌آل‌هایی از حلقه R باشند، آنگاه

$$I/(I\cap J)\cong(I+J)/J.\blacksquare$$

۱۱.۳.۱ تمرین های حل شده

تمرین ۱. نشان دهید تابع $f:\mathbf{Z}_6\to\mathbf{Z}_{10}$ که به ازای هر $[a]\in\mathbf{Z}_6$ به صورت $f([a])=5[a]$ تعریف شده است، یک همریختی حلقه‌ها از $\mathbf{Z}_6$ به توی $\mathbf{Z}_{10}$ است.

حل: ابتدا نشان می‌دهیم که f خوش تعریف است. فرض کنید در $\mathbf{Z}_6$، $[a]=[b]$. در این صورت $a-b$ بر ۶ بخش پذیر است. بنابراین به ازای $k\in\mathbf{Z}$ای، $a=6k+b$. حال $5a=30k+5b$ نشان‌می‌دهد که‌در $\mathbf{Z}_{10}$، $5[a]=[5a]=[30k+5b]=[30k]+_{10}[5b]=[0]+_{10}5[b]=5[b]$، پس $f([a])=f([b])$. بنابراین f خوش تعریف است. فرض کنید $[a],[b]\in\mathbf{Z}_6$. در این صورت $f([a])+_6[b])=f([a+b])=5[a+b]=5([a]+_{10}[b])=5[a]+_{10}5[b]=f(a)+_{10}f(b)$ و

$$f([a]\cdot_6[b])=f([ab])=5[ab]=25[ab]\quad(\text{زیرا } \mathbf{Z}_{10} \text{ از مشخصه } 10 \text{ است})$$
$$=(5[a]\cdot_{10}5[b])=f(a)\cdot_{10}f(b).$$

از این رو f یک همریختی است.

تمرین ۲. فرض کنید $\mathbf{R}$ میدان اعداد حقیقی و α یک خود ریختی از $\mathbf{R}$ باشد. نشان دهید که به ازای هر $x\in\mathbf{R}$، $\alpha(x)=x$.

حل: چون α یک خودریختی از $\mathbf{R}$ است، $\alpha(0)=0$ و $\alpha(1)=1$. فرض کنید $n\in\mathbf{N}$. دراین صورت $\alpha(n)=\alpha(1+1+\ldots+1)=\alpha(1)+\alpha(1)+\ldots+\alpha(1)=1+1+\ldots+1=n$. حال فرض کنید $m\in\mathbf{Z}$ و $m<0$. قراردهید $n=-m>0$. دراین صورت $\alpha(m)=\alpha(-n)=-\alpha(n)=-n=m$. این نشان می‌دهد که به ازای هر $x\in\mathbf{Z}$، $\alpha(x)=x$. فرض کنید $\frac{p}{q}\in\mathbf{Q}$. در این صورت

$$\alpha(\frac{p}{q})=\alpha(pq^{-1})=\alpha(p)\alpha(q^{-1})=p\alpha(q)^{-1}=pq^{-1}=\frac{p}{q}.$$

این نشان می‌دهد که به ازای هر $x\in\mathbf{Q}$، $\alpha(x)=x$. فرض کنید $x\in\mathbf{R}$ به قسمی باشد که $x\geq 0$. در این صورت به ازای $y\in\mathbf{R}$ای، $x=y^2$. بنابراین $\alpha(x)=\alpha(y^2)=\alpha(yy)=\alpha(y)\alpha(y)=\alpha(y)^2\geq 0$. حال فرض کنید $a,b\in\mathbf{R}$ به قسمی باشند که $a\geq b$. در این صورت $a-b\geq 0$. از این رو، $\alpha(a-b)\geq 0$ و لذا $\alpha(a)-\alpha(b)\geq 0$، یعنی $\alpha(a)\geq\alpha(b)$. بنابراین α حافظ ترتیب است. حال نشان می‌دهیم که α پیوسته است. فرض کنید $\varepsilon\in\mathbf{R}$ و $\varepsilon>0$. چون α پوشاست، $\delta>0$ای وجود دارد به طوری که $\alpha(\delta)=\varepsilon$. حال فرض کنید $x,y\in\mathbf{R}$ به قسمی باشند که $|x-y|<\delta$. بنابراین

$$-\delta<x-y<\delta.$$

چون α حافظ ترتیب است،

$$\alpha(-\delta)<\alpha(x-y)<(\alpha(\delta).$$

بنابراین،

$$-\varepsilon<\alpha(x-y)<\varepsilon$$

و لذا

$$-\varepsilon<\alpha(x)-\alpha(y)<\varepsilon\ .$$

این ایجاب می‌کند که

$$|\alpha(x)-\alpha(y)|<\varepsilon$$

از این رو α پیوسته است. حال فرض کنید $x\in\mathbf{R}$. چون $\mathbf{Q}$ در $\mathbf{R}$ چگال است، لذا دنباله $\{a_n\}$ از اعداد گویا وجود دارد به طوری که

$$\lim_{n\to\infty} a_n=x\ .$$

چون α پیوسته است،

$$\alpha(x)=\alpha(\lim_{n\to\infty} a_n)=\lim_{n\to\infty}\alpha(a_n)=\lim_{n\to\infty} a_n=x$$

که این حکم را اثبات می‌کند.

تمرین ۳. فرض کنید R حلقه‌ای یکدار با مشخصه ۰ باشد. نشان دهید که R شامل زیرحلقه‌ای یکریخت با $\mathbf{Z}$ است.

حل: فرض کنید $T=\{n1\,|\,n\in\mathbf{Z}\}$. چون $0=01\in T$، $T\neq\varnothing$. فرض کنید $a=n1$ و $b=m1$ دو عنصر دلخواه از T باشند. در این صورت $a-b=n1-m1=(n-m)1$ و $(n1)(m1)=(nm)1$. از این رو، $a-b\,,ab\in T$. بنابراین T زیرحلقه‌ای از R است. فرض کنید n و m اعدادی صحیح باشند به طوری که $n1=m1$. اگر $n>m$، آنگاه $(n-m)1=0$. این با فرض این که R از مشخصه ۰ است در تناقض می‌باشد. به طور مشابه، $m>n$ نیز به یک تناقض منجر می‌شود. از این رو، $n=m$. بنابراین، به ازای هر $a\in T$، عدد صحیح یکتای n ای وجود دارد به طوری که $a=n1$. از این رو، نگاشت $f:\mathbf{Z}\to T$ که با ضابطه $f(n)=n1$ تعریف شده یکریختی است.

تمرین ۴. فرض کنید p عددی صحیح اول باشد. نشان دهید که تنها دو حلقه نایکریخت با p عنصر وجود دارد.

حل: می‌دانیم که $(\mathbf{Z}_p,+_p)$ تنها گروهی از مرتبه p (تا حد یکریختی) است. به ازای هر $[a],[b]\in\mathbf{Z}_p$، اعمال $\odot_1$ و $\odot_2$ را روی $\mathbf{Z}_p$ به صورت $[a]\odot_1[b]=[0]$ و $[a]\odot_2[b]=[ab]$ تعریف کنید. حال $\odot_1$ و $\odot_2$ خوش تعریف‌اند و $(\mathbf{Z}_p,+_p,\odot_1)$ و $(\mathbf{Z}_p,+_p,\odot_2)$ حلقه می‌باشند. فرض کنید R حلقه‌ای با p عنصر باشد. دراین صورت $(R,+)\cong(\mathbf{Z}_p,+_p)$. اگر $R\cong(\mathbf{Z}_p,+_p,\odot_1)$، آنگاه ضرب R برابر با $\odot_1$ نیست. فرض کنید $[a]$ یک مولد $(\mathbf{Z}_p,+_p)$ باشد. حال به ازای عدد

صحیح نامنفی n ای، $[a]^2=n[a]$. عدد صحیح m وجود دارد به قسمی که $mn\equiv_p 1$. فرض کنید $[b]=m[a]$، در این صورت $[b]^2=m^2[a^2]=m^2n[a]=m[a]=[b]$. فرض کنید g یک یکریختی از $(\mathbf{Z}_p,+_p)$ به روی $(R,+)$ باشد. نگاشت $f:\mathbf{Z}_p\to R$ را به ازای هر $[u]\in\mathbf{Z}_p$ با ضابطه $f([u])=ug([b])$ تعریف کنید. در این صورت

$$f([u]+_p[v])=f([u+v])=(u+v)g([b])=ug([b])+vg([b])=f([u])+f([v]).$$

و

$$f([u]\odot_2[v])=f([uv])=(uv)g([b])=uvg([b]^2)=uvg([b])g([b])$$
$$=ug([b])vg([b])=f([u])f([v]).$$

از این رو، f یک همریختی حلقه‌هاست. فرض کنید $c\in R$، در این صورت $[u]\in\mathbf{Z}_p$ ای وجود دارد به طوری که $g([u])=c$. حال به ازای $t\in\mathbf{Z}$ ای، $[u]=t[a]$. بنابراین

$$f([tn])=tng([b])=tng(m[a])=tg(mn[a])=tg([a])=g(t[a])=g([u])=c.$$

از این رو f پوشاست. چون $|\mathbf{Z}_p|=|R|$ ، نتیجه می‌شود که f یک به یک است. بنابراین f یکریختی است.

۱۱۰۳۰۲ تمرینها

۱. فرض کنید R مجموعه تمام ماتریسهای 2×2 به صورت $\begin{bmatrix} a & b \\ -b & a \end{bmatrix}$ باشد، که در آن a و b اعداد حقیقی هستند. ثابت کنید که R یک حلقه است و تابع $a+bi\to\begin{bmatrix} a & b \\ -b & a \end{bmatrix}$ یک یکریختی از $\mathbf{C}$ به روی $\mathbf{R}$ است.

۲. به ازای هر $a,b\in\mathbf{Z}$، اعمال دوتایی $\oplus$ و $\odot$ را روی $\mathbf{Z}$ به ترتیب با $a\oplus b=a+b-1$ و $a\odot b=a+b-ab$ تعریف کنید. نشان دهید که $(\mathbf{Z},\oplus,\odot)$ با حلقه $(\mathbf{Z},+,\cdot)$ یکریخت است.

۳. (i) نشان دهید که حلقه‌های $\mathbf{R}$ و $\mathbf{Q}$ یکریخت نیستند.

(ii) نشان دهید که حلقه‌های $\mathbf{R}$ و $\mathbf{C}$ یکریخت نیستند.

(iii) آیا حلقه‌های $\mathbf{Z}_6$ و $\mathbf{Z}_3\times\mathbf{Z}_2$ یکریختند؟

۴. فرض کنید $T_2(\mathbf{Z})=\left\{\begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \middle| a,b,c\in\mathbf{Z}\right\}$ حلقه تمام ماتریس‌های بالا مثلثی روی $\mathbf{Z}$ باشند. به ازای هر $\begin{bmatrix} a & b \\ 0 & c \end{bmatrix}\in T_2(\mathbf{Z})$ ، تابع $f:T_2(\mathbf{Z})\to\mathbf{Z}$ را به صورت زیر تعریف کنید:

$$f\left(\begin{bmatrix} a & b \\ 0 & c \end{bmatrix}\right)=a.$$

(*i*) نشان دهید که f یک همریختی است.

(*ii*) آیا f بر وریختی است؟

(*iii*) آیا f یکریختی است؟

(*iv*) $Ker\ f$ را بیابید.

۵. آیا یک برویختی از حلقه $\mathbf{Z}_{۲۴}$ به روی حلقه $\mathbf{Z}_{۷}$ وجود دارد؟

۶. نشان دهید که یک تکریختی از حلقه $\mathbf{Z}_{۶}$ به روی حلقه $\mathbf{Z}_{۱۱}$ وجود ندارد.

۷. نشان دهید که حلقه $۲\mathbf{Z}$ با حلقه $۳\mathbf{Z}$ یکریخت نیست.

۸. فرض کنید R یک حلقه‌بولی باشد. اگر $\{۰\}$ و R تنهاایده‌آل‌های R باشند، ثابت کنید که $R\cong\mathbf{Z}_{۲}$.

۹. نشان دهید که حلقه $\mathbf{Z}$ با هیچ زیرحلقه سرهٔ خود یکریخت نیست.

۱۰. آیا حلقه $\mathbf{Q}[\sqrt{۲}]$ با حلقه $\mathbf{Q}[\sqrt{۳}]$ یکریخت است؟

۱۱. فرض کنید $f:R\to S$ یک همریختی نابدیهی از میدان R به روی حلقه S باشد. ثابت کنید که S میدان است.

۱۲. فرض کنید R حلقه‌ای یکدار باشد. اگر مشخصه R برابر با $n>۰$ باشد، نشان دهید که R شامل زیرحلقه‌ای است که با حلقه $\mathbf{Z}_n$ یکریخت می‌باشد.

۱۳. نشان دهید که تنها دو همریختی از $\mathbf{R}$ به توی $\mathbf{R}$ وجود دارد.

۱۴. ثابت کنید که هر حلقه R با زیرحلقه‌ای از $M_n(R)$، حلقه ماتریس‌های $n\times n$ روی R، یکریخت است.

۱۵. فرض کنید f یک همریختی از حلقه R به روی حلقه R' باشد. ثابت کنید که

(*i*) اگر I ایده‌آلی از R باشد، آنگاه $f(I)$ یک ایده‌آل R' است،

(*ii*) اگر I' ایده‌آلی از R' باشد، آنگاه $f^{-۱}(I')$ یک ایده‌آل R است و $f^{-۱}(I')\supseteq Ker\ f$،

(*iii*) اگر R تعویض‌پذیر و I,J دو ایده‌آل R باشند، آنگاه $f(I+J)=f(I)+f(J)$ و $f(IJ)=f(I)f(J)$.

۱۶. در هر یک از تمرین‌های زیر، در صورت درستی اثبات بنویسید؛ در غیر این صورت مثالی نقض ارائه کنید.

(*i*) تنها دو همریختی از حلقه اعداد به توی خودش وجود دارد.

(*ii*) نگاشت $f:\mathbf{Z}\to\mathbf{Z}$ که به صورت $f(n)=۳n$ تعریف شده یک همریختی گروههاست، اما یک همریختی حلقه‌ها نیست.

(*iii*) تنها یکریختی از حلقه R به روی خودش، نگاشت همانی R است.

(iv) فرض کنید R حلقه‌ای یکدار باشد. همچنین فرض کنید $f:R\to S$ یک همریختی حلقه‌ها باشد. در این صورت $f(1)$ عنصر همانی S است.

(v) یک همریختی ناصفر از یک میدان به توی حلقه‌ای با بیش از یک عنصر یک تکریختی است.

(vi) هر تصویر همریخت نابدیهی از یک حوزه صحیح یک حوزه صحیح است.

فصل چهاردهم

حلقه‌های چند جمله‌ای

مطالعه چندجمله‌ای‌ها به ۱۶۵۰ قبل از میلاد بر می‌گردد، زمانی که مصریان معادلات چندجمله‌ای خطی معین را حل کرده بودند. در سال‌های ۶۰۰ قبل از میلاد هندیها، چگونگی حل معادلات درجه دوم را آموخته بودند. به هر حال، چندجمله‌ای هایی که امروزه می‌شناسیم، یعنی چندجمله‌ای هایی که در نمادگذاری‌هانوشته‌می‌شوندتقریباًتاسال‌های ۱۷۰۰ بعدازمیلادوجودنداشتند.

در حدود ۴۰۰ بعد از میلاد کاربرد جبر نمادی در هند و عربستان آغاز به ظهور نمود. بعضی افراد کاربرد نمادها در جبر را به عنوان اولین گام تجرید در ریاضیات می‌دانند.

۱۴۰۱ حلقه‌های چند جمله‌ای

ردهٔ مهمی از حلقه‌ها به نام رده حلقه‌های چندجمله‌ای موسوم است. همه ما با چندجمله‌ای‌ها آشنایی داریم. ممکن‌است یک چندجمله‌ای را به عنوان عبارتی به صورت $a_0+a_1x+\dots+a_nx^n$ در نظر بگیریم، که در آن x یک نماد و a_i ها احتمالاً اعداد حقیقی هستند، یا به عنوان یک تابع $f(x)=a_0+a_1x+\dots+a_nx^n$. به هر حال، کسی واقعاً می‌داند که یک چندجمله‌ای چیست؟ در واقع نماد x چیست؟ چرا دو چندجمله‌ای $a_0+a_1x+\dots+a_nx^n$ و $b_0+b_1x+\dots+b_mx^m$ برابرند اگر و تنها اگر $n=m$ و $a_i=b_i$، که $i=1,2,\dots,n$؟ در این بخش، به این پرسش‌ها پاسخ داده و بعضی خواص اساسی چندجمله‌ای‌ها را ارائه می‌دهیم.

تعریف ۱۰۱۰۱۴ به ازای هر حلقه R، فرض کنید $R[x]$ مجموعه تمام دنباله‌های نامتناهی $(a_0,a_1,a_2,\dots)$ باشد، که در آن $a_i\in R$، $i=0,1,2,\dots$ و عدد صحیح نامنفی n ای (وابسته به $(a_0,a_1,a_2,\dots)$) وجود دارد به طوری که به ازای تمام اعداد صحیح $k\geq n$، $a_k=0$. عناصر $R[x]$ را چند جمله‌ای‌های روی R می‌نامند.

حال جمع و ضرب را روی $R[x]$ به صورت زیر تعریف می‌کنیم:

$$(a_0,a_1,a_2,\dots)+(b_0,b_1,b_2,\dots)=(a_0+b_0,a_1+b_1,a_2+b_2,\dots)$$
$$(a_0,a_1,a_2,\dots)\cdot(b_0,b_1,b_2,\dots)=(c_0,c_1,c_2,\dots),$$

که در آن

$$c_j=\sum_{i=0}^{j}a_ib_{j-i}\quad,\quad j=0,1,2,\dots$$

به خواننده واگذار می‌کنیم که تحقیق کند که $(R[x],+,\cdot)$ تشکیل یک حلقه می‌دهد. توجه می‌کنیم که $(0,0,\dots)$ عنصر همانی جمعی $R[x]$ است و معکوس جمعی $(a_0,a_1,\dots)$ برابر است با $(-a_0,-a_1,\dots)$. حلقه $R[x]$ را یک حلقهٔ چند جمله‌ایها یا حلقه چند جمله‌ای روی R می‌نامند. واضح است که $R[x]$ تعویض‌پذیر است وقتی R تعویض‌پذیر باشد. همچنین، اگر R یکدار باشد، آنگاه $R[x]$ دارای عنصر همانی به صورت $(1,0,0,0,\dots)$ است.

نگاشت $a\to(a,0,0,\dots)$ یک تکریختی از R به توی $R[x]$ است. بنابراین R در $R[x]$ نشانده می‌شود. لذا می‌توان R را به عنوان زیرحلقه‌ای از $R[x]$ در نظر گرفت و تفاوت چندانی مابین a و $(a,0,0,\dots)$ قائل نشد.

حال نمادهای چندجمله‌ای‌ها را به نمادهایی که بیشتر برای خواننده آشناست، تبدیل می‌کنیم.

فرض کنید

$ax^0=a$ نشان دهنده $(a,0,0,\dots)$

$ax^1=ax$ نشان دهنده $(0,a,0,\dots)$

ax^2 نشان دهنده $(0,0,a,0,\dots)$

$\vdots$

در این صورت

$$(a_0,a_1,a_2,\dots,a_n,0,\dots)=(a_0,0,0,\dots)+(0,a_1,0,0,\dots)$$
$$+\dots+(0,\dots,0,a_n,0,\dots)=a_0+a_1x+a_2x^2+\dots+a_nx^n$$

نماد x را یک مجهول روی R و عناصر a_0، a_1، ...، a_n از R را ضرایب چندجمله‌ای $a_0+a_1x+a_2x^2+\dots+a_nx^n$ می‌نامند.

دلیل این که دو چندجمله‌ای $a_0+a_1x+\dots+a_nx^n$ و $b_0+b_1x+\dots+b_mx^m$ برابرند اگر و تنها اگر $n=m$ و $a_i=b_i$، $i=0,1,\dots,n$ این است که دو دنباله $(a_0,a_1,\dots)$ و $(b_0,b_1,\dots)$ برابرند اگر و تنها اگر $a_i=b_i$، $i=0,1,\dots$ (باید یاد آور شویم که دنباله نامتناهی از عناصر R عبارت است از تابعی از مجموعه اعداد صحیح نامنفی به توی R. در نتیجه، مجدداً مفهوم جفت مرتب جهت

ارائه تعریفی دیگر از یک مفهوم ریاضی به کار می‌رود.)

اگر حلقه R دارای عنصر همانی ۱ باشد، آنگاه می‌توان x را به عنوان عنصری از $R[x]$ در نظر گرفت. بنابراین $1x$ را با x یکی در نظر می‌گیریم، یعنی $(0,1,0,\dots)$ را x می‌نامیم.

خواننده می‌تواند بررسی کند که تعاریف جمع و ضرب دو چندجمله‌ای همان تعاریف آشنا هستند. بنابراین وقتی R دارای عنصر همانی است،

$$ax=(a,0,0,\dots)(0,1,0,\dots)=(0,a,0,\dots)=(0,1,0,\dots)(a,0,0,\dots)=xa.$$

قضیه ۲۰۱۰۱۴ (i) اگر R حلقه‌ای تعویض‌پذیر یکدار باشد، آنگاه $R[x]$ نیز حلقه‌ای تعویض‌پذیر یکدار است.

(ii) اگر R یک حوزه صحیح باشد، آنگاه $R[x]$ نیز یک حوزه صحیح است.

اثبات. (i) فرض کنید $f(x)=a_0+a_1x+\dots+a_nx^n$ و $g(x)=b_0+b_1x+\dots+b_mx^m$ دو عنصر در $R[x]$ باشند. همچنین فرض کنید $f(x)g(x)=c_0+c_1x+\dots+c_tx^t$ و $g(x)f(x)=d_0+d_1x+\dots+d_sx^s$. داریم $c_j=\Sigma_{i=0}^{j}a_ib_{j-i}$ و $d_j=\Sigma_{i=0}^{j}b_ia_{j-i}$. چون R تعویض‌پذیر است، به ازای هر $j=0,1,2,\dots$،

$$c_j=a_0b_j+a_1b_{j-1}+\dots+a_jb_0=b_0a_j+b_1a_{j-1}+\dots+b_ja_0=d_j.$$

بنابراین $R[x]$ حلقه‌ای تعویض‌پذیر است. چون $1\in R$، لذا $1\in R[x]$ و به ازای هر $f(x)\in R[x]$، $1f(x)=f(x)1=f(x)$. از این رو، $R[x]$ حلقه‌ای تعویض‌پذیر و یکدار است.

(ii) فرض کنید R یک حوزه صحیح باشد. در این صورت بنابر (i)، $R[x]$ حلقه‌ای تعویض‌پذیر و یکدار است. فرض کنید $f(x)=a_0+a_1x+\dots+a_nx^n$ و $g(x)=b_0+b_1x+\dots+b_mx^m$ دو چندجمله‌ای ناصفر در $R[x]$ باشند. در این صورت عناصر a_i و b_j ای وجود دارند به طوری که $a_i\neq 0$، $b_j\neq 0$، و به ازای هر $t\geq 1$، $a_{i+t}=0$، و $b_{j+t}=0$. چندجمله‌ای $f(x)g(x)=c_0+c_1x+\dots+c_{n+m}x^{n+m}$ را در نظر بگیرید. حال $c_{i+j}=a_0b_{i+j}+a_1b_{i+j-1}+\dots+a_ib_j+\dots+a_{i+j}b=a_ib_j\neq 0$، زیرا R یک حوزه صحیح است. این ایجاب می‌کند که $f(x)g(x)\neq 0$. بنابراین $R[x]$ یک حوزه صحیح می‌باشد. ■

تعریف ۳۰۱۰۱۴ فرض کنید R یک حلقه باشد. اگر $f(x)=a_0+a_1x+\dots+a_nx^n$، که $a_n\neq 0$، یک چندجمله‌ای در $R[x]$ باشد، آنگاه n را درجه $f(x)$ نامیده و آن را با $\deg f(x)$ نشان می‌دهند، همچنین a_n را ضریب پیشرو $f(x)$ می‌نامند. اگر R یکدار باشد و $a_n=1$، آنگاه $f(x)$ یک چند جمله‌ای تکین نامیده می‌شود.

چندجمله‌ای‌هایی از درجه ۰ در $R[x]$ دقیقاً عناصر $R\setminus\{0\}$ می‌باشند. چندجمله‌ای $0\in R[x]$

دارای درجه نمی‌باشد. عناصر R را اسکالر یا چند جلمه‌ای‌های ثابت می‌نامیم.

قضیه ۴۰۱۰۱۴ فرض کنید $R[x]$ یک حلقه چندجمله‌ای، $f(x)$ و $g(x)$ دو چندجمله‌ای ناصفر در $R[x]$ باشند.

(i) اگر $f(x)g(x)\neq 0$، آنگاه $deg\, f(x)g(x)\leq deg\, f(x)+deg\, g(x)$.

(ii) اگر $f(x)+g(x)\neq 0$، آنگاه

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

اثبات. (i) اگر $f(x)=a_0+a_1x+\ldots+a_nx^n$ و $g(x)=b_0+b_1x+\ldots+b_mx^m$، آنگاه $f(x)g(x)=a_0b_0+(a_0b_1+a_1b_0)x+\ldots+a_nb_mx^{n+m}$. اگر $f(x)g(x)\neq 0$، آنگاه حداقل یکی از ضرایب $f(x)g(x)$ ناصفر است. فرض کنید $a_nb_m\neq 0$، در این صورت

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

اگر $a_nb_m=0$ (که می‌تواند چنین باشد اگر R دارای مقسوم صفر باشد)، آنگاه

$$deg(f(x)g(x))<deg\, f(x)+deg\, g(x).$$

(ii) اگر $deg\, f(x)>deg\, g(x)$، آنگاه $deg\,(f(x)+g(x))=max\{deg\, f(x), deg\, g(x)\}$.

اگر $deg\, f(x)=deg\, g(x)$، آنگاه ممکن است که $f(x)+g(x)=0$ یا

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

جزئیات را به عنوان تمرین واگذار می‌کنیم. ■

از اثبات ۴۰۱۰۱۴ (i)، بلافاصله نتیجه می‌شود که اگر R یک حوزه صحیح باشد، آنگاه در (i) تساوی برقرار است.

مثال ۵۰۱۰۱۴ حلقه چندجمله‌ای $\mathbb{Z}_4[x]$ را در نظر بگیرید. فرض کنید $f(x)=[1]+[2]x^2$ و $g(x)=[1]+[3]x$. در این صورت

$$f(x)g(x)=[1]+[3]x+[2]x^2.$$

از این رو، $deg(f(x)g(x))=2<3=deg\, f(x)+deg\, g(x)$. فرض کنید $h(x)=[5]+[4]x^2$، در این صورت $f(x)+g(x)=[6]+[6]x^2=[0]$ و لذا $deg(f(x)+g(x))$ تعریف نشده است.

قضیه ۶۰۱۰۱۴ (الگوریتم تقسیم) فرض کنید R حلقه‌ای تعویض‌پذیر یکدار و $f(x)$ و $g(x)$ چندجمله‌ای هایی در $R[x]$ باشند به طوری که ضریب پیشروی $g(x)$ در R یکه باشد. در این صورت چندجمله‌ای‌های یکتای $q(x), r(x)\in R[x]$ موجودند به طوری که

$$f(x)=q(x)g(x)+r(x),$$

که در آن $r(x)=0$ یا $\deg r(x)<\deg g(x)$.

اثبات. اگر $f(x)=0$ یا $\deg f(x)<\deg g(x)$، آنگاه قرار می‌دهیم $q(x)=0$ و $r(x)=f(x)$. حال فرض می‌کنیم که $\deg f(x)\geq\deg g(x)$ و حکم را به روش استقراء روی $\deg f(x)=n$ اثبات می‌کنیم. اگر $\deg f(x)=\deg g(x)=0$، آنگاه داریم $q(x)=f(x)g(x)^{-1}$ و $r(x)=0$. فرض استقراء را چنین بیان می‌کنیم که قضیه به ازای تمام چندجمله‌ای‌ها با درجه کمتر از n درست باشد. فرض کنید $f(x)=a_0+a_1x+\ldots+a_nx^n$ دارای درجه n و $g(x)=b_0+b_1x+\ldots+b_mx^m$ دارای درجه m باشد، که در آن $n\geq m$. چندجمله‌ای

$$f_1(x)=f(x)-(a_nb_m^{-1})x^{n-m}g(x). \qquad (۱۴۰۱)$$

دارای درجه کمتر از n است، زیرا ضریب x^n برابر است با $a_n-(a_nb_m^{-1})b_m=0$ است. از این رو، بنابر فرض استقراء، چندجمله‌ای‌های $q_1(x),r_1(x)\in R[x]$ موجودند به طوری که

$$f_1(x)=q_1(x)g(x)+r_1(x), \qquad (۱۴۰۲)$$

که در آن $r_1(x)=0$ یا $\deg r_1(x)<\deg g(x)$. با جایگزینی $f_1(x)$ از معادله (۱۴۰۲) در معادله (۱۴۰۱) و حل آن بر حسب $f(x)$، به دست می‌آوریم.

$$f(x)=(q_1(x)+a_nb_m^{-1}x^{n-m})g(x)+r_1(x)=q(x)g(x)+r(x),$$

که در آن $q(x)=q_1(x)+a_nb_m^{-1}a^{n-m}$ و $r(x)=r_1(x)$، نمایش مورد نظر برای $f(x)$ از درجه n است.

لازم است نشان دهیم که $q(x)$ و $r(x)$ یکتا هستند. فرض کنید چندجمله‌ای‌های $q'(x),r'(x)\in R[x]$ موجود باشند به طوری که

$$f(x)=q(x)g(x)+r(x)=q'(x)g(x)+r'(x),$$

که در آن $r(x)=0$ یا $\deg r(x)<\deg g(x)$، $r'(x)=0$ و $\deg r'(x)<\deg g(x)$. در این صورت

$$r(x)-r'(x)=(q'(x)-q(x))g(x).$$

فرض کنید $r(x)-r'(x)\neq 0$. چون ضریب پیشروی $g(x)$ یکه است، لذا

$$\deg((q'(x)-q(x))g(x))=\deg(q'(x)-q(x))+\deg g(x)\geq\deg g(x).$$

این ایجاب می‌کند که

$$\deg(r(x)-r'(x))\geq\deg g(x),$$

که ناممکن است، زیرا $\deg r(x),\deg r'(x)<\deg g(x)$. لذا

$$r(x)-r'(x)=0 \text{ یا } r(x)=r'(x).$$

بنابراین،

$$0=(q'(x)-q(x))g(x)\ . \qquad (۱۴۰۳)$$

چون b_m یکه است، $deg((q'(x)-q(x))g(x))\geq 0$ اگر نه $q'(x)-q(x)=0$. بنابراین از معادله (۱۴۰۳)، ملاحظه می‌کنیم که $q'(x)-q(x)=0$ بایستی حالت مطلوب باشد. ■

چندجمله‌ای‌های $q(x)$ و $r(x)$ در قضیه ۶۰۱۰۱۴ را به ترتیب **خارج قسمت** و **باقیمانده** تقسیم $f(x)$ بر $g(x)$ می‌نامند.

تعریف ۷۰۱۰۱۴ فرض کنید R حلقه‌ای تعویض‌پذیر یکدار باشد و $f(x)=a_0+a_1x+...+a_nx^n\in R[x]$. به ازای هر $r\in R$، تعریف کنید

$$f(r)=a_0+a_1r+...+a_nr^n\ .$$

وقتی $f(r)=0$، r را یک ریشه یا صفر $f(x)$ می‌نامند.

در تعریف ۷۰۱۰۱۴، چنین تصور می‌کنیم که r را به جای x در $f(x)$ جایگزین کرده‌ایم. دانشجویان عادت به انجام چنین کاری دارند. به هر حال، مشکلات معین هنگامی بروز می‌کنند که R تعویض‌پذیر نباشد. به عنوان مثال، فرض کنید $f(x)=a-x$ و $g(x)=b-x$. قرار دهید $h(x)=f(x)g(x)$. دراین صورت $h(x)=(a-x)(b-x)=ab-(a+b)x+x^2$. به ازای $c\in R$، $h(c)=ab-(a+b)c+c^2=ab-ac-bc+c^2$ درحالی که

$$f(c)g(c)=(a-c)(b-c)=ab-cb-ac+c^2\ .$$

از این رو نمی‌توان نتیجه گرفت که $h(c)=f(c)g(c)$. به هر حال، اگر R تعویض‌پذیر (یکدار) باشد، آنگاه می‌توان نتیجه گرفت که $h(c)=f(c)g(c)$. واضح است که اگر $k(x)=f(x)+g(x)$، آنگاه $k(c)=f(c)+g(c)$.

تعریف ۸۰۱۰۱۴ فرض کنید R حلقه‌ای تعویض‌پذیر یکدار باشد و $f(x),g(x)\in R[x]$ به قسمی باشند که $g(x)\neq 0$. گوئیم که $g(x)$ چندجمله‌ای $f(x)$ را عاد می‌کند یا $g(x)$ یک عامل $f(x)$ است و می‌نویسیم $g(x)\mid f(x)$ هرگاه $q(x)\in R[x]$ ای موجود باشد به طوری که $f(x)=q(x)g(x)$.

قضیه ۹۰۱۰۱۴ (قضیه باقیمانده) فرض کنید R حلقه‌ای تعویض‌پذیر یکدار باشد. به ازای $f(x)\in R[x]$ و $a\in R$، چندجمله‌ای $q(x)\in R[x]$ وجود دارد به طوری که

$$f(x)=(x-a)q(x)+f(a)\ .$$

اثبات. با به کار بردن الگوریتم تقسیم با انتخاب $g(x)=x-a$، چندجمله‌ای‌های یکتای $q(x),r(x)\in R[x]$ موجودند به طوری که $f(x)=(x-a)q(x)+r(x)$، که در آن $r(x)=0$ یا

$deg\ r(x)<1$. از این رو، $r(x)$ یک چندجمله‌ای ثابت است. فرض کنید $r(x)=d$. با جایگزینی a به جای x حاصل می‌شود $f(a)=(a-a)q(a)+d$، که نتیجه مورد نظر به دست می‌آید. ■

نتیجه ۱۰.۱.۱۴ (قضیه تجزیه) فرض کنید R حلقه‌ای تعویض‌پذیر یکدار باشد. به ازای $f(x)\in R[x]$ و $a\in R$، عامل $x-a$ چندجمله‌ای $f(x)$ را عاد می‌کند اگر و تنها اگر a یک ریشه $f(x)$ باشد.

اثبات. فرض کنید $(x-a)\,|\,f(x)$، در این صورت چندجمله‌ای $q(x)\in R[x]$ وجود دارد به طوری که $f(x)=(x-a)q(x)$. از این رو، $f(a)=(a-a)q(a)=0$ و لذا a یک ریشه $f(x)$ است. بعکس، فرض کنید a یک ریشه $f(x)$ باشد. در این صورت بنابر قضیه باقیمانده (قضیه ۹.۱.۱۴) و این حقیقت که $f(a)=0$، داریم $f(x)=(x-a)q(x)$. در نتیجه، $(x-a)\,|\,f(x)$. ■

قضیه ۱۱.۱.۱۴ فرض کنید R حوزه‌ای صحیح و $f(x)$ چندجمله‌ای ناصفر در $R[x]$ از درجه n باشد. در این صورت $f(x)$ حداکثر دارای n ریشه در R است.

اثبات. اگر $deg\ f(x)=0$، آنگاه $f(x)$ یک چندجمله‌ای ثابت مانند $f(x)=c\neq 0$ است. واضح است که c ریشه‌ای در R ندارد. فرض کنید قضیه به ازای تمام چندجمله‌ای‌های از درجه کمتر از n برقرار باشد، که در آن $n>0$ (فرض استقراء). همچنین فرض کنید $deg\ f(x)=n$. اگر $f(x)$ دارای ریشه‌ای در R نباشد، آنگاه حکم برقرار است. فرض کنید $r\in R$ یک ریشه $f(x)$ باشد. در این صورت بنابر نتیجه ۱۰.۱.۱۴، $f(x)=(x-r)q(x)$، که در آن $deg\ q(x)=n-1$. اگر ریشه دلخواه دیگر مانند $r'\in R$ از $f(x)$ موجود باشد، آنگاه $0=f(r')=(r'-r)q(r')$. چون $r'\neq r$ و R یک حوزه صحیح است، لذا $q(r')=0$ و لذا r' یک ریشه $q(x)$ است. بنابراین، هر ریشه دلخواه دیگری $f(x)$ یک ریشه $q(x)$ نیز می‌باشد. چون $f(x)=(x-r)q(x)$، هر ریشه $q(x)$ یک ریشه $f(x)$ نیز است. بنابر فرض استقراء و این حقیقت که $deg\ q(x)=n-1$، حداکثر $n-1$ از این ریشه‌های دیگر r' وجود دارد. از این رو، $f(x)$ حداکثر n ریشه در R دارد. ■

حال حلقه چندجمله‌ای را از یک مجهول به چندین مجهول گسترش می‌دهیم.

تعریف ۱۲.۱.۱۴ به ازای هر حلقه R، به طور بازگشتی تعریف می‌کنیم

$$R[x_1,x_2,\dots,x_n]=R[x_1,x_2,\dots,x_{n-1}][x_n],$$

که در آن x_1 یک مجهول روی R و x_n یک مجهول روی $R[x_1,x_2,\dots,x_{n-1}]$ است. $R[x_1,x_2,\dots,x_n]$ را حلقه چند جمله‌ای n مجهولی می‌نامند.

قبل از توصیف حلقه $R[x_1,x_2,\dots,x_n]$ بعضی نمادها را معرفی می‌کنیم. به جای $\sum_{i_1=0}^{k_1}\cdots\sum_{i_n=0}^{k_n} r_{i_1\dots i_n}x_1^{i_1}\dots x_n^{i_n}$ می‌نویسیم $\sum_{i_1,\dots,i_n} r_{i_1\dots i_n}x_1^{i_1}\dots x_n^{i_n}$، که در آن هر $r_{i_1\dots i_n}\in R$

و هر $k_1, \ldots, k_n$ اعداد صحیح نامنفی هستند.

حلقهٔ مورد نظر بدین صورت نوشته می‌شود:

$$R[x_1, x_2, \ldots, x_n] = \{ \sum_{i_n, \ldots, i_1} r_{i_1 \ldots i_n} x_1^{i_1} \ldots x_n^{i_n} \mid r_{i_1 \ldots i_n} \in R \}$$

به ازای $n = 2$ داریم

$$R[x_1, x_2] = R[x_1][x_2] = \{ \sum_{i_2} s_{i_2} x_2^{i_2} \mid s_{i_2} \in R[x_1] \}.$$

حال هر s_{i_2} به صورت $\sum_{i_1} r_{i_1 i_2} x_1^{i_1}$ می‌باشد. بنابراین

$$R[x_1, x_2] = \{ \sum_{i_2} (\sum_{i_1} r_{i_1 i_2} x_1^{i_1}) x_2^{i_2} \mid r_{i_1 i_2} \in R \}$$

$$= \{ \sum_{i_2} \sum_{i_1} r_{i_1 i_2} x_1^{i_1} x_2^{i_2} \mid r_{i_1 i_2} \in R \}$$

$$= \{ \sum_{i_2 i_2, i_1} r_{i_1 i_2} x_1^{i_1} x_2^{i_2} \mid r_{i_1 i_2} \in R \}$$

تعریف ۱۳۰۱۰۱۴ فرض کنید S زیرحلقه‌ای از حلقه S و $c_1, c_2, \ldots, c_n$ عناصری از S باشند. تعریف کنید $R[c_1] = \{ \sum_i r_i c_1^i \mid r_i \in R \}$ و

$$R[c_1, c_2, \ldots, c_n] = R[c_1, c_2, \ldots, c_{n-1}][c_n].$$

گوئیم که $c_1, c_2, \ldots, c_n$ روی R مستقل جبری هستند هرگاه

$$\sum_{i_n, \ldots, i_1} r_{i_1 \ldots i_n} c_1^{i_1} \ldots c_n^{i_n} = 0$$

که تنها وقتی می‌تواند رخ دهد که هر $r_{i_1 \ldots i_n} = 0$، که در آن $r_{i_1 \ldots i_n} \in R$.

$R[c_1, c_2, \ldots, c_n]$ زیرحلقه‌ای از S است و برابر مجموعه تمام مجموع‌های متناهی به صورت زیر می‌باشد.

$$\sum_{i_n, \ldots, i_1} r_{i_1 \ldots i_n} c_1^{i_1} \ldots c_n^{i_n},$$

که در آن $r_{i_1 \ldots i_n} \in R$.

قضیه ۱۴۰۱۰۱۴ فرض کنید R زیرحلقه‌ای از حلقه تعویض‌پذیر S باشد به طوری که R و S دارای عناصر همانی یکسانی باشند. همچنین فرض کنید $c \in S$. در این صورت همریختی یکتای α از $R[x]$ به روی $R[c]$ وجود دارد به طوری که $\alpha(x) = c$ و به ازای هر $a \in R$، $\alpha(a) = a$.

اثبات. به ازای هر $\sum a_i x^i \in R[x]$ تابع $\alpha : R[x] \to R[c]$ را با ضابطهٔ $\alpha(\sum a_i x^i) = \sum a_i c^i$ تعریف کنید. حال $a_0 + a_1 x + \ldots + a_n x^n = b_0 + b_1 x + \ldots + b_m x^m$ ایجاب می‌کند که $n = m$ و به‌ازای هر $i = 1, 2, \ldots, n$، $a_i = b_i$. بنابراین $a_0 + a_1 c + \ldots + a_n c^n = b_0 + b_1 c + \ldots + b_n c^n$ و لذا α خوش تعریف است. بنابر تعریف ۱۳۰۱۰۱۴، واضح است که α حلقه $R[x]$ را به روی

$R[c]$ می‌نگارد. چون به ازای هر دو چندجمله‌ای $f(x),g(x)\in R[x]$، $k(x)=f(x)+g(x)$ ایجاب می‌کند $k(c)=f(c)+g(c)$ و نیز $h(x)=f(x)g(x)$ ایجاب می‌کند که $h(c)=f(c)g(c)$، نتیجه می‌شود که α اعمال + و · را حفظ می‌کند. بنابراین α یک همریختی از $R[x]$ به روی $R[c]$ است. واضح است که $\alpha(x)=c$ و به ازای هر $a\in R$، $\alpha(a)=a$. فرض کنید β همریختی از $R[x]$ به روی $R[c]$ باشد به طوری که $\beta(x)=c$ و به ازای هر $a\in R$، $\beta(a)=a$. در این صورت

$$\beta(\Sigma a_i x^i)=\Sigma\beta(a_i)\beta(x)^i=\Sigma a_i c^i=\alpha(\Sigma a_i x^i)\ .$$

بنابراین، $\beta=\alpha$ و لذا α یکتاست. ■

تاکید می‌کنیم که همریختی α در قضیه ۱۴۰۱۰۱۴ خوش تعریف است، زیرا x روی R مستقل جبری است. در مثال زیر این مطلب را توضیح می‌دهیم.

مثال ۱۵۰۱۰۱۴ اگر $\alpha:Q[\sqrt{2}]\to Q[x]$ را با ضابطه $\alpha(\Sigma a_i\sqrt{2})=\Sigma a_i x^i$ تعریف می‌کنیم، آنگاه α یک تابع نمی‌باشد، زیرا $\alpha(2)=2$ و $\alpha(2)=\alpha((\sqrt{2})^2)=x^2$ و $2\neq x^2$.

۱۴۰۱۰۱ تمرین‌های حل شده

تمرین ۱. فرض کنید R حلقه‌ای یکدار باشد. نشان دهید که

$$R[x]/\langle x\rangle\cong R\ .$$

حل: به ازای هر $a_0+a_1x+a_2x^2+\dots+a_nx^n\in R[x]$ نگاشت $f:R[x]\to R$ را با ضابطه زیر تعریف کنید:

$$f(a_0+a_1x+a_2x^2+\dots+a_nx^n)=a_0\ .$$

فرض کنید $a_0+a_1x+a_2x^2+\dots+a_nx^n=b_0+b_1x+b_2x^2+\dots+b_mx^m$، دراین‌صورت $a_0=b_0$ و لذا $f(a_0+a_1x+a_2x^2+\dots+a_nx^n)=f(b_0+b_1x+b_2x^2+\dots+b_mx^m)$. بنابراین f خوش تعریف است. واضح است که f یک بروریختی است. حال

$$a_0+a_1x+a_2x^2+a_nx^n\in Ker\,f$$

اگر و تنها اگر $f(a_0+a_1x+a_2x^2+\dots+a_nx^n)=0$ اگر و تنها اگر $a_0=0$ اگر و تنها اگر $a_0+a_1x+a_2x^2+\dots+a_nx^n\in\langle x\rangle$. بنابراین $Ker\,f=\langle x\rangle$. لذا

$$R[x]/\langle x\rangle\cong R\ .$$

تمرین ۲. فرض کنید F یک میدان و $\alpha:F[x]\to F[x]$ یک خود ریختی باشد به طوری که به ازای هر $a\in F$، $\alpha(a)=a$. نشان دهید که $a,b\in F$ ای وجود دارند به طوری که $\alpha(x)=ax+b$.

حل: بنابرالگوریتم تقسیم، به ازای $g(x)\in F[x]$ ای و $b\in F$ ای، $\alpha(x)=g(x)x+b$.

چون α پوشاست، چندجمله‌ای‌های $h(x), p(x) \in F[x]$ موجودند به طوری که $g(x)=\alpha(h(x))$ و $x=\alpha(p(x))$. بنابراین

$$\alpha(x)=g(x)x+b=\alpha(h(x))\alpha(p(x))+\alpha(b)=\alpha(h(x)p(x)+b).$$

لذا $x=h(x)p(x)+b$، زیرا α یک به یک است. حال $\deg g(x)=\deg(h(x)p(x)+b)$ ایجاب می‌کند که $\deg(h(x)p(x))=1$. از این رو، یا $\deg h(x)=1$ و $\deg p(x)=0$ یا $\deg h(x)=0$ و $\deg p(x)=1$. فرض کنید $\deg p(x)=0$، در این صورت به ازای $c\in F$ای، $p(x)=c$. این ایجاب می‌کند که $x=\alpha(p(x))=\alpha(c)=c$، که یک تناقض است. بنابراین $\deg h(x)=0$ و $\deg p(x)=1$. فرض کنید به ازای $a\in F$ای، $h(x)=a$. در این صورت $\alpha(x)=\alpha(h(x))x+b=\alpha(a)x+b=ax+b$.

تمرین ۳. فرض کنید R حلقه‌ای تعویض‌پذیر یکدار باشد و

$$f(x)=a_0+a_1x+a_2x^2+\dots+a_nx^n\in R[x].$$

اگر a_0 یکه و a_1 و a_2 ... a_n عناصری پوچ توان باشند، ثابت کنید که $f(x)$ معکوس‌پذیر است.

حل: حکم را به روش استقراء روی $n=\deg f(x)$ اثبات می‌کنیم. اگر $n=0$، آنگاه $f(x)=a_0$. از این رو، $f(x)$ معکوس‌پذیر است. فرض کنید که حکم به ازای تمام چندجمله‌ای‌های به صورت فوق و از درجه کوچکتر از n برقرار باشد. حال فرض کنید که

$$f(x)=a_0+a_1x+a_2x^2+\dots+a_nx^n\in R[x]$$

به قسمی باشد که a_0 یکه و a_1، a_2، ...، a_n عناصری پوچ توان باشند و $\deg f(x)=n$. قرار دهید $g(x)=a_0+a_1x+a_2x^2+\dots+a_{n-1}x^{x-1}$. توجه کنید که $\deg g(x)<n$. از این رو، بنابر فرض استقراء، $g(x)$ معکوس‌پذیر است. چون a_n پوچ توان است، لذا عدد صحیح مثبت mای وجود دارد به طوری که $a_n^m=0$. در این صورت

$$(g(x)+a_nx^n)(g(x)^{-1}-a_ng(x)^{-2}x^n+a_n^2g(x)^{-3}x^{2n}-\dots+$$
$$(-1)^{m-1}a_n^{m-1}g(x)^{-(m-1)}x^{(m-1)n})=1.$$

این نتیجه می‌دهد که $f(x)$ معکوس‌پذیر است.

۱۴۰۱۰۲ تمرینها

۱. اگر I ایده‌آلی از حلقه R باشد، ثابت کنید که $I[x]$ نیز ایده‌آلی از حلقه چندجمله‌ای $R[x]$ است.

۲. فرض کنید R حوزه‌ای صحیح باشد. ثابت کنید که R و $R[x]$ دارای مشخصهٔ یکسانند.

۳. فرض کنید R حلقه‌ای تعویض‌پذیر یکدار باشد. ایده‌آل $<x>$ از $R[x]$ را که با x تولید شده، توصیف کنید.

۴. (i) فرض کنید $g(x)=x^2+2x+1\in\mathbf{Q}[x]$ و $f(x)=x^4+3x^3+2x^2+2$.
چندجمله‌ای‌های یکتای $q(x),r(x)\in\mathbf{Q}[x]$ را به گونه‌ای بیابید که $f(x)=q(x)g(x)+r(x)$،
که در آن $r(x)=0$ یا $0<deg\ r(x)<deg\ g(x)$.

۵. فرض کنید $g(x)=x^4+x^3+[3]x^2+[2]x\in\mathbf{Z}_5[x]$, $f(x)=x^5+x^4+x^3+x+[3]$.
چندجمله‌ای‌های $q(x),r(x)\in\mathbf{Z}_5[x]$ را به گونه‌ای بیابید که $f(x)=q(x)g(x)+r(x)$، که در
آن $r(x)=0$ یا $0<deg\ r(x)<deg\ g(x)$.

۶. فرض کنید $R=\mathbf{Z}\oplus\mathbf{Z}$. نشان دهید که چندجمله‌ای $x(1,0)$ در $R[x]$ دارای تعداد نامتناهی ریشه در R است.

۷. نشان دهید که حلقه چندجمله‌ای $\mathbf{Z}_4[x]$ روی حلقه $\mathbf{Z}_4$ نامتناهی است، اما $\mathbf{Z}_4[x]$ از مشخصه متناهی است.

۸. در حلقه $\mathbf{Z}_8[x]$ نشان دهید که $[1]+[2]x$ یکه است.

۹. فرض کنید R حلقه‌ای تعویض‌پذیر و یکدار باشد و $f(x)=a_0+a_1x+\ldots+a_nx^n\in R[x]$.
اگر $f(x)$ در $R[x]$ یکه باشد، ثابت کنید که a_0 در R یکه و به ازای هر $i=1,2,\ldots,n$، a_i پوچ توان است.

۱۰. از نتیجه تمرین ۹ جهت نشان دادن این که $5x+1$ در $\mathbf{Z}[x]$ یکه نیست، استفاده کنید.

۱۱. تمام یکه‌های $\mathbf{Z}[x]$ را بیابید.

۱۲. تمام یکه‌های $\mathbf{Z}_6[x]$ را بیابید.

۱۳. فرض کنید R حوزه‌ای صحیح باشد. ثابت کنید که یکه‌های $R[x]$ در R قرار دارند.

۱۴. در $\mathbf{Z}_8[x]$ ثابت کنید

(i) $[4]x^2+[2]x+[4]$ یک مقسوم علیه صفر است.

(ii) $[2]x$ پوچ توان است.

(iii) $[4]x+1$ و $[4]x+[3]$ یکه‌اند.

۱۵. فرض کنید R زیرحلقه‌ای از حلقه تعویض‌پذیر S باشد به طوری که R دارای عنصر همانی است.

(i) در حلقه چندجمله‌ای $R[x_1,x_2,\ldots,x_n]$ ثابت کنید که x_1، x_2، ...، x_n روی R مستقل جبری هستند.

(ii) ثابت کنید که نگاشت

$$\alpha:R[x_1,x_2,\ldots,x_n]\to R[c_1,c_2,\ldots,c_n]$$

که با ضابطهٔ $\alpha(\sum_{i_n\ldots i_1} r_{i_1\ldots i_n}x_1^{i_1}\ldots x_n^{i_n})=\sum_{i_n\ldots i_1} r_{i_1\ldots i_n}c_1^{i_1}\ldots c_n^{i_n}$ تعریف شده، یک همریختی از

$R[x_1, x_2, \ldots, x_n]$ به روی $R[c_1, c_2, \ldots, c_n]$ است، که در آن $c_1, \ldots, c_n \in S$.

(iii) ثابت کنید که همریختی α در قسمت (ii) یکریختی است اگر و تنها اگر c_1، c_2، ...، c_n روی R مستقل جبری باشند.

۱۶. فرض کنید $f(x)$ یک چندجمله‌ای از درجه $n > 0$ در حلقه چندجمله‌ای $K[x]$ روی میدان K باشد. ثابت کنید که هر عنصر حلقه خارج قسمت $K[x]/\langle f(x)\rangle$ به صورت $g(x) + \langle f(x)\rangle$ است، که در آن $g(x)$ یک چندجمله‌ای از درجه حداکثر $n-1$ باشد.

۱۷. برای عبارات زیر، در صورت درستی اثباتی بیاورید، در غیر این صورت مثال نقضی را ارائه دهید.

(i) اگر حلقه چندجمله‌ای $R[x]$ دارای مقسوم علیه صفر باشد، آنگاه R نیز چنین است.

(ii) اگر R یک میدان باشد، $R[x]$ نیز یک میدان است.

(iii) در $\mathbf{Z}_7[x]$، $(x+[1])^7 = x^7 + [1]$.