فصل ۳

آشنایی با حلقه‌ها

مفهوم دستگاه جبری حلقه را در فصل **۱** معرفی کردیم و قرار شد جزییات بیش‌تری از آن را در این فصل کوتاه مطرح کنیم. البته این بررسی در درس‌های دیگر جبر ادامه خواهد یافت. بسیاری از ویژگی-های حلقه را که در این فصل می‌آوریم، همتای آن‌هایی هستند که در حالت کلی دستگاه‌های جبری فصل **۱** و در حالت خاص گروه‌ها در فصل **۲** بیان شدند. از این رو، از بیان جزییات برخی از مفاهیم تکراری صرف‌نظر می‌کنیم و بیش‌تر به مطالب جدید می‌پردازیم.

ولی فرصت خوبی برای شما است که مهارت‌های کسب شده‌ی خود را تمرین کنید!

۱.۳ حلقه و زیرحلقه

نیاز به معرفی ساختار جبری **حلقه** در قرن نوزدهم، به ویژه در بررسی ویژگی‌های جبری $\mathbb{Z}$ و چندجمله‌ای‌ها (در پاسخگویی به پرسش‌های نظریه اعداد، به ویژه در رابطه با آخرین قضیه‌ی فرما) مطرح شد و مفهوم مجرد حلقه در واقع در قرن بیستم حاصل شد. همان طور که گروه‌ها انواع متعددی، چون آبلی و دوری و از این قبیل، دارند، انواع خاص حلقه‌ها با مجرد سازی و تعمیم ویژگی‌های دستگاه‌های جبری اعداد، همراه با دو عمل دوتایی معمولی جمع و ضرب آن‌ها، به دست می‌آیند. ابتدا تعریف کلی و متداول حلقه را از فصل **۱** یادآوری می‌کنیم و به مرور در این فصل چند ویژگی دیگر حلقه‌ی اعداد را مجرد سازی و به تعریف حلقه می‌افزاییم و حلقه‌هایی خاص را معرفی می‌کنیم.

۱.۱.۳ تعریف. دستگاه جبری $(R;+,\cdot)$ از نوع $\tau=(2,2)$ را (همراه با دو عمل دوتایی،که معمولاً یکی را با **نماد جمع** و دیگری را با **نماد ضرب** نشان می‌دهیم) **حلقه** می‌گوییم اگر

(ح۱) دستگاه جبری $(R;+)$ **گروه آبلی** باشد،
(ح۲) دستگاه جبری $(R;\cdot)$ **نیم‌گروه** (گروهواره‌ی شرکت‌پذیر) باشد،
(ح۳) برای هر $x,y,z\in R$، اتحادهای **توزیع‌پذیری** (ضرب روی جمع) برقرار باشند:

$$x\cdot(y+z)=x\cdot y+x\cdot z \quad , \quad (y+z)\cdot x=y\cdot x+z\cdot x$$

۲.۱.۳ بحث در کلاس

۱- از این پس، برای راحتی کار، به جای $x.y$ می‌نویسیم xy. همچنین، مطابق آنچه در فصل ۲ بیان شد، عضو خنثی گروه آبلی $(R;+)$ را با 0 و قرینه‌ی هر $x\in R$ را با $-x$ نشان می‌دهیم.

۲- عمل‌های دوتایی حلقه را از این رو با نمادهای جمع و ضرب نشان داده‌ایم که مثال‌های اولیه‌ی حلقه، دستگاه‌های جبری اعداد $\mathbb{Z}$، $\mathbb{Q}$، $\mathbb{R}$، و $\mathbb{C}$ همراه با عمل‌های جمع و ضرب معمولی اعداد هستند.

۳- از مجموعه‌های اعداد بند ۲، مجموعه‌های دیگری از اعداد به وجود می‌آیند که مثال‌های خوبی از انواع حلقه‌ها را تشکیل می‌دهند. در این مثال‌ها، عضوها به صورت $a+b\alpha$ هستند که در آن α^2 عددی صحیح اول است. به عنوان نمونه:

$$\mathbb{Z}[\sqrt{2}]=\{m+n\sqrt{2}\mid m,n\in\mathbb{Z}\}$$
$$\mathbb{Q}[\sqrt{-5}]=\{a+b\sqrt{-5}\mid a,b\in\mathbb{Q}\}$$

همچنین، توجه می‌کنیم که $\mathbb{C}=\mathbb{R}[i]=\{a+bi\mid a,b\in\mathbb{R},i^2=-1\}$ حلقه‌ی اعداد مختلط و $\mathbb{Z}[i]=\{m+ni\mid m,n\in\mathbb{Z},i^2=-1\}$، که **حلقه‌ی اعداد صحیح گاوسی** نامیده می‌شود، به ویژه در نظریه‌ی اعداد کاربرد دارد.

۴- روشن است که مجموعه‌ی تک عضوی $R=\{0\}$ همراه با عمل‌های جمع و ضرب بدیهی $0+0=0$ و $00=0$ حلقه است. این حلقه را **حلقه‌ی صفر** می‌نامیم.

۵- به آسانی می‌توانید نشان دهید که **هر گروه آبلی** $(R;+)$، با عضو خنثی صفر، را می‌توان با تعریف عمل ضرب بدیهی زیر به حلقه تبدیل کرد.

$$(\forall a,b\in R)\quad ab=0$$

۳.۱.۳ بحث در کلاس. از آنجا که در حلقه‌ی $(R;+,\cdot)$، دستگاه جبری $(R;+)$ گروهی آبلی ولی $(R;\cdot)$ صرفاً یک نیمگروه است، بسیاری از ویژگی‌هایی که به تعریف حلقه می‌افزاییم به عمل ضرب حلقه مربوط می‌شود. برای مثال،

۱- اگر $(R;\cdot)$ نیم‌گروهی تعویض‌پذیر و با عضو همانی باشد، حلقه را **حلقه‌ی تعویض‌پذیر** و **یک‌دار** (یا **یکه**‌دار) می‌نامیم، زیرا معمولاً عضو همانی ضربی حلقه‌ی R را با نماد 1 یا 1_R نشان می‌دهیم. اگر $R=\{0\}$ آنگاه $1=0$ و در غیر این صورت $1\neq 0$ (سعی کنید این مطلب را اثبات کنید. اگر موفق نشدید، بند**۲** بحث **۴.۱.۳** را ببینید).

۲- روشن است که مجموعه‌های اعداد $\mathbb{Z}$، $\mathbb{Q}$، $\mathbb{R}$، $\mathbb{C}$ با جمع و ضرب معمولی، حلقه‌هایی تعویض-پذیر و یک‌دار هستند.

۳- مجموعه‌ی توانی $\mathcal{P}(X)$ همراه با عمل تفاضل متقارن Δ (برای نماد جمع)، و عمل اشتراک $\cap$ (برای نماد ضرب)، حلقه‌ای تعویض‌پذیر و یک‌دار است. ویژگی‌های شرکت‌پذیری و تعویض‌پذیری Δ و توزیع‌پذیری $\cap$ روی Δ را از درس مبانی علوم ریاضی به خاطر آورید. مجموعه‌ی $\varnothing$ همانی جمعی، و مجموعه‌ی $X\in\mathcal{P}(X)$ همانی ضربی این حلقه است. همچنین، قرینه‌ی هر عضو چون $A\in\mathcal{P}(X)$ در این حلقه (نسبت به عمل Δ) برابر با خودش است. **چطور؟**

۴- مجموعه‌ی توابع حقیقی مقدار $\mathbb{R}^R$، همراه با جمع و ضرب توابع، حلقه‌ای تعویض‌پذیر و یک‌دار است. به خاطر آورید که جمع و ضرب توابع حقیقی به صورت، به اصطلاح نقطه‌ای، زیر تعریف می‌شوند:

$$(f+g)(x)=f(x)+g(x),\qquad (fg)(x)=f(x)g(x)$$

همچنین، روشن است که تابع ثابت صفر نقش عضو همانی جمعی (عضو خنثی)، و تابع ثابت ۱ نقش همانی ضربی (یکه) را داراست. قرینه‌ی هر عضو نیز همان قرینه‌ی تابع است که در درس ریاضی عمومی دیدید:

$$(-f)(x)=-f(x)$$

۵- دستگاه‌های جبری $(\mathbb{Z}_n;+_n,\cdot_n)$ و $(\mathbb{Z}/\equiv_n;+_n,\cdot_n)$ حلقه‌هایی تعویض‌پذیر و یک‌دار هستند.

۶- مجموعه‌ی ماتریس‌های $n\times n$ با درایه‌های حقیقی، به نمایش $M_n(\mathbb{R})$، همراه با جمع و ضرب ماتریس‌ها، حلقه‌ای یک‌دار است که تعویض‌پذیر نیست. ماتریس صفر عضو خنثی، و ماتریس همانی، عضو یکه است. قرینه‌ی هر ماتریس نیز ماتریسی است که درایه‌های آن قرینه‌ی درایه‌های نظیر در ماتریس اولیه هستند.

۷- مجموعه‌ی ماتریس‌های به صورت زیر نیز، همراه با جمع و ضرب ماتریس‌ها، حلقه است، که یک‌دار یا تعویض‌پذیر نیست:

$$\begin{bmatrix} 0 & a \\ 0 & a \end{bmatrix}, \qquad a \in \mathbb{R}$$

۸- مجموعه‌ی همه‌ی چندجمله‌ای‌های $a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ با ضرایب صحیح (گویا یا حقیقی) همراه با جمع و ضرب معمولی چندجمله‌ای‌ها (که در دوره‌ی دبیرستان آموخته‌اید)، حلقه‌ای یک‌دار و تعویض‌پذیر است.

۹- برخی از ریاضی‌دانان فقط با حلقه‌های تعوض‌پذیر و یک‌دار سروکار دارند و از این رو حلقه‌ها را از همان ابتدا به صورت دستگاه جبری $(R;+,\cdot,1)$، با عمل صفرتایی 1، در نظر می‌گیرند. البته، برخی دیگر از ریاضی‌دانان این شرایط را قایل نمی‌شوند و با حلقه‌های کلی‌تر، نه لزوماً تعویض‌پذیر یا یک‌دار، سروکار دارند. **خوشبختانه هر دو نوع این ریاضی‌دانان در دانشگاه‌های ایران وجود دارند، و در جامعه‌ی جهانی نیز شناخته شده هستند.**

۴.۱.۳ بحث در کلاس

۱- اغلب ویژگی‌های معمولی حلقه‌ی $(R;+,\cdot)$ مربوط به گروه آبلی $(R;+)$ است. برخی از این ویژگی‌ها را، که برقراری آن‌ها طبیعی نیز به نظر می‌رسند، از فصل **۲** می‌آوریم:

(الف) $-(-a) = a$

(ب) $-(a+b) = (-a) + (-b)$

(پ) روشن است که قوانین حذف از چپ و راست برای جمع حلقه در گروه $(R;+)$ برقرار هستند.

(ت) معادله‌های $a + x = b$ و $y + a = b$ در گروه $(R;+)$ جواب منحصر به فرد $x = y = b - a = b + (-a)$ را دارند.

(ث) نماد مضرب $m \cdot x = x + x + \cdots + x$ را، برای عدد طبیعی m و تعمیم آن به عدد صحیح $m \in \mathbb{Z}$، از فصل گروه‌ها به خاطر آورید (به جای mx نماد $m \cdot x$ را به کار برده‌ایم تا با ضرب حلقه اشتباه نشود. البته اگر امکان اشتباه نباشد، از همان نماد ساده تر mx استفاده می‌کنیم). یادآوری می‌کنیم که، برای $m, n \in \mathbb{Z}$ داریم:

$$\begin{aligned}(m+n)\cdot a &= m\cdot a+n\cdot a\\ m\cdot(a+b) &= m\cdot a+m\cdot b\\ m\cdot(n\cdot a) &= (mn)\cdot a\end{aligned}$$

۲- اتحادهای زیر نیز در هر حلقه برقرار هستند:

(الف) اتحاد $a0=0=0a$. مراحل اثبات زیر را توضیح دهید (به توانایی اتحاد توزیع‌پذیری ضرب حلقه روی جمع آن توجه کنید):

$$a0=a(0+0)=a0+a0 \quad\Rightarrow\quad a0=0$$

(ب) اتحاد $a(-b)=(-a)b=-(ab)$. مراحل اثبات زیر را توضیح دهید:

$$0=a0=a(b+(-b))=ab+a(-b) \quad\Rightarrow\quad -(ab)=a(-b)$$

(پ) اتحاد $(-a)(-b)=ab$.

(ت) با قرارداد $a-b=a+(-b)$، اتحادهای زیر را داریم

$$a(b-c)=ab-ac, \qquad (a-b)c=ac-bc$$

(ث) در اینجا ارتباط **مضارب** $(m.a)$ در گروه آبلی حلقه، یعنی در $(R;+)$، را با **ضرب** حلقه می-بینیم.

$$m.(ab)=(m\cdot a)b=a(m\cdot b)$$

برای مثال، اگر m عددی طبیعی باشد، با استفاده از توزیع‌پذیری، داریم

$$\begin{aligned}m\cdot(ab) &= ab+ab+\cdots+ab\\ &=(a+a+\cdots+a)b=(m\cdot a)b\end{aligned}$$

۵.۱.۳ تعریف. فرض کنیم $(R;+,\cdot,1)$ حلقه‌ای یک‌دار باشد. اگر وارون ضربی عضو $a\in R$ وجود داشته باشد، عضو **وارون‌پذیر** a را در حلقه‌ها **یکال** نیز می‌نامیم. مجموعه‌ی یکال‌های حلقه‌ی R را با $U(R)$ نشان می‌دهیم.

۶.۱.۳ بحث در کلاس. فرض کنیم $(R;+,\cdot,1)$ حلقه‌ای یک‌دار است. در این صورت،

۱- وارون هر عضو یکال منحصر به فرد است (**چرا؟**) و مطابق معمول آن را با نماد a^{-1} نشان می‌دهیم.

۲- یادآوری می‌کنیم که اگر a و b در R وارون‌پذیر باشند، آنگاه a^{-1} و ab نیز وارون‌پذیر هستند و $(a^{-1})^{-1}=a$ و $(ab)^{-1}=b^{-1}a^{-1}$. از این رو، $U(R)$ تحت **عمل ضرب** حلقه یک گروه است.

۳- یکی از ویژگی‌های مهم عضوهای وارون‌پذیر (یکال‌های) حلقه این است که، مانند آنچه در مورد گروه‌ها دیدیم، این عضوها را می‌توان، به کمک شرکت‌پذیری عمل ضرب، از دو طرف یک تساوی حذف کرد. نشان دهید که

$$(\forall x,y\in R)\quad (u\in U(R))\quad ux=uy \quad\vee\quad xu=yu\Rightarrow x=y$$

۷.۱.۳ زیرحلقه. تاکنون اطلاعاتی کلی در فصل ۱ (و به ویژه در فصل **۲** گروه‌ها) در باره‌ی زیر-دستگاه‌ها و اهمیت آن‌ها به دست آوردیم. به ویژه، با مشبکه‌ی همه‌ی زیردستگاه‌های یک دستگاه جبری آشنا شدیم. در این بخش مطالبی را در باره‌ی زیرحلقه و مشبکه‌ی آن‌ها بیان می‌کنیم. توجه می‌کنیم که دستگاه جبری حلقه در واقع از دو عمل دوتایی، یک عمل یکانی قرینه یابی، و یک عمل صفرتایی 0 تشکیل شده است. پس، با توجه به تعریف کلی زیردستگاه جبری، زیرحلقه باید نسبت به همه‌ی این عمل‌ها بسته باشد. ولی، با الگو قرار دادن گروه‌ها ، زیرحلقه را (به بیان غلط مصطلح و بی ضرر) می‌توانیم به صورت ساده‌تر زیر تعریف کنیم.

۸.۱.۳ تعریف. زیرمجموعه‌ی S از حلقه‌ی $(R;+,\cdot)$ را **زیرحلقه** می‌گوییم، و می‌نویسیم $S\le R$، اگر S نسبت به اعمال (جمع و ضرب) R بسته باشد، و با همان اعمال تشکیل یک حلقه دهد.

بندهای **۲** و **۳** قضیه‌ی زیر همتای قضیه‌های **۶.۲.۲** و **۷.۲.۲** فصل گروه‌ها هستند.

۹.۱.۳ قضیه (محک‌های زیرحلقه). فرض کنیم $(R;+,\cdot)$ حلقه است و $S\subseteq R$. در این صورت هر یک از احکام زیر معادل با زیرحلقه بودن S از R است:

۱- S همراه با عمل جمع $+$ زیرگروه $(R;+)$ و همراه با عمل ضرب $\cdot$ زیرنیم‌گروه $(R;\cdot)$ باشد.

۲- $0\in S$ و برای هر $a,b\in S$، $-a,a+b,ab\in S$.

۳- $0\in S$ و برای هر $a,b\in S$، $a-b,ab\in S$.

اثبات. خلاصه‌ای از اثبات بسیار ساده‌ی این احکام را می‌آوریم تا اینکه شما با کامل کردن آن‌ها مهارت‌هایی را که تاکنون کسب کرده‌اید، تمرین کنید. روشن است که اگر S زیرحلقه‌ی R باشد آنگاه هر سه حکم **۱**، **۲**، و **۳** برقرار هستند. **این طور نیست؟** برعکس، اگر حکم **۱** برقرار باشد آنگاه شرایط

(ح۱) و (ح۲) تعریف حلقه برقرار هستند و **اتحاد** توزیع‌پذیری (ح۳) برای همه‌ی عضوهای R درست است، و در نتیجه برای عضوهای زیرمجموعه‌ی S از R نیز برقرار است. اگر حکم ۲ درست باشد، آنگاه از $0 \in S$ و $-a, a+b \in S$، بـه راحتـی مـی‌توانیـد (مشـابه قضـیه‌ی ۶.۲.۲) نشـان دهیـد کـه S زیرگروهی از گروه $(R;+)$ است، و $ab \in S$ نشان می‌دهد کـه $(S;\cdot)$ زیـرنیم‌گـروه $(R;\cdot)$ اسـت (شرکت‌پذیری ضرب چطور در S برقرار است؟). اثبات معادل بودن حکم ۳ با زیرحلقه بودن S را بـه عهده‌ی شما می‌گذاریم (قضیه‌ی ۷.۲.۲ را با نماد گذاری جمعی ببینید).

۱۰.۱.۳ بحث در کلاس

۱- در حالت کلی، اصراری نداریم که زیرحلقه‌ی یک حلقه‌ای یک‌دار، خـود حلقـه‌ای یـک‌دار باشـد، یـا حتی اگر یک‌دار است، یکه‌اش همان یکه‌ی حلقه‌ی مادر باشد! ولی، ریاضی‌دانانی که تنها با حلقـه‌هـای یک‌دار سروکار دارند یقیناً **اصرار دارند** که یکه‌ی حلقه‌ی مادر متعلق به زیرحلقه باشد. از این رو، برای مثال، $n\mathbb{Z}$ را برای $n \geq 2$ به عنوان زیرحلقه‌ی $\mathbb{Z}$ در نظر نمی‌گیرند! ولی تعریف ۸.۱.۳ چنین قیدی را قایل نمی‌شود.

درستی مثال‌های زیر را می‌توانید به کمک محک‌های ۹.۱.۳ زیرحلقه اثبات کنید.

۲- روشن است که $\mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R} \leq \mathbb{C}$.

۳- برای هر $n \in \mathbb{Z}$، $n\mathbb{Z} \leq \mathbb{Z}$. آیا می‌توانید همه‌ی زیرحلقه‌های $\mathbb{Z}$ را تعیین کنید؟ البته کـه مـی-توانید. از بند ۶ بحث ۹.۲.۲ می‌دانیم که هر زیرگروه $(\mathbb{Z};+)$ به صورت گروه دوری $n\mathbb{Z}$ است، و روشن است که این مجموعه‌ها نسبت به ضرب نیز بسته هستند. چه نتیجه‌ای می‌گیریم؟

۴- نشان دهید که همتای نتیجـه‌ی بنـد۳ بـرای حلقـه‌ی $(\mathbb{Z}_n;+_n,\cdot_n)$ نیـز درسـت اسـت. یعنـی، زیرحلقه‌های $\mathbb{Z}_n$ نیز به صورت $m\mathbb{Z}_n$ هستند، که البته $m \mid n$.

۵- هر مجموعه‌ی ناتهی چون $\mathcal{P}$ از زیرمجموعه‌های X که نسبت به اشتراک، اجتماع، و مـتمم بسـته باشد، زیر حلقه‌ای از حلقه‌ی $(\mathcal{P}(X);\Delta,\cap)$ است. توجه کنید که می‌توانیم بنویسیم

$$A\Delta B = (A \cap B') \cup (A' \cap B)$$

۶- مجموعه‌ی توابع حقیقی پیوسته $C(\mathbb{R},\mathbb{R})$ زیرحلقه‌ای از حلقه‌ی همه‌ی توابع حقیقی $\mathbb{R}^R$ است. زیرا تفاضل و حاصل‌ضرب توابع پیوسته، پیوسته هستند. ولی، برای مثال،

$$\{f \in \mathbb{R}^{\mathbb{R}} \mid f(0) = 1\}$$

زیرحلقه‌ی $\mathbb{R}^R$ نیست. **چرا؟**

۷- به راحتی می‌توانید نشان دهید که، **مرکز** (ضربی) حلقه‌ی R، یعنی

$$Z(R)=\{x\in R\,|\,(\forall r\in R)\quad xr=rx\}$$

زیرحلقه‌ی R است. گاهی $Z(R)$ را با $CentR$ نشان می‌دهیم.

۸- $\mathbb{Z}[i]\le\mathbb{Q}[i]\le\mathbb{R}[i]$.

۹- مجموعه‌ی ماتریس‌های به صورت

$$\begin{bmatrix} m & 0 \\ 0 & n \end{bmatrix}$$

که در آن $m,n\in\mathbb{Z}$، زیرحلقه‌ای از حلقه‌ی $M_2(\mathbb{Z})$، متشکل از ماتریس‌های 2×2 با درایه‌های عدد صحیح، است. این زیرحلقه، عضو همانی ضربی (ماتریس همانی) حلقه‌ی مادر را به ارث می‌برد ولی برخلاف حلقه‌ی مادر، تعویض‌پذیر است! همچنین، مجموعه‌ی ماتریس‌های به صورت

$$\begin{bmatrix} 0 & a \\ 0 & a \end{bmatrix},\qquad a\in\mathbb{Z}$$

یک زیرحلقه‌ی $M_2(\mathbb{Z})$ است که ماتریس همانی را از حلقه‌ی مادر به ارث نبرده است!

۱۰- روشن است که مجموعه‌ی $M_2(\mathbb{C})$ متشکل از ماتریس‌های 2×2 با درایه‌های مختلط همراه با جمع و ضرب ماتریس‌ها نیز یک حلقه است. حال، فرض کنیم

$$I=\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix},\qquad J=\begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix},\qquad K=\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix},\qquad L=JK=\begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}$$

در این صورت، به راحتی می‌توانید نشان دهید که

$$\begin{aligned} H&=\{aI+bJ+cK+dL\,|\,a,b,c,d\in\mathbb{R}\}\\ &=\left\{\begin{bmatrix} a+bi & c+di \\ -c+di & a-bi \end{bmatrix}\ \middle|\ a,b,c,d\in\mathbb{R}\right\} \end{aligned}$$

زیرحلقه‌ی $M_2(\mathbb{C})$ است. این حلقه را **حلقه‌ی چهارگان‌های همیلتن** می‌نامیم. می‌گویند که حدود ۱۰ تا ۱۵ سال طول کشید تا همیلتن، که به دنبال گسترش مشخصی از $\mathbb{C}=\{a+bi\,|\,a,b\in\mathbb{R}\}$ بود، به وجود این حلقه پی برد! حلقه‌ی چهارگان‌های همیلتن کاربردهایی خوب نیز در علم فیزیک دارد. توجه می‌کنیم که این حلقه تعویض‌پذیر نیست. زیرا، برای مثال $JK\ne KJ$.

۱۱.۱.۳ بحث در کلاس

با استفاده از محک زیرحلقه (قضیه‌ی ۹.۱.۳)، به راحتی می‌توانید نشان دهید که اشتراک زیرحلقه‌ها یک زیرحلقه است. ولی اجتماع زیرحلقه‌ها لزوماً زیرحلقه نیست. برای مثال، $2\mathbb{Z}\cup 3\mathbb{Z}$ زیرحلقه‌ی $\mathbb{Z}$ نیست. ولی مشابه آنچه در فصل‌های ۱ و ۲ دیدیم، مطالب زیر نشان می‌دهند که برای هر حلقه‌ی R، مجموعه‌ی مرتب $(Sub(R);\subseteq)$ متشکل از زیرحلقه‌های R مشبکه‌ای کامل است.

۱۲.۱.۳ تعریف. فرض کنیم $(R;+,\cdot)$ یک حلقه است و $X\subseteq R$. اشتراک همه‌ی زیرحلقه‌های شامل X را، که در واقع کوچکترین زیرحلقه‌ی شامل X است، زیرحلقه‌ی تولید شده از X می‌گوییم و آن را با $<X>$ نشان می‌دهیم.

۱۳.۱.۳ بحث در کلاس

۱- مجموعه‌ی مرتب $(Sub(R);\subseteq)$، با اعمال زیر، مشابه حالت گروه‌ها، تشکیل یک مشبکه کامل می‌دهد:

$$S\wedge T=S\cap T \qquad S\vee T=<S\cup T>$$
$$\bigwedge S_i=\bigcap S_i \qquad \bigvee S_i=<\bigcup S_i>$$

۲- از تعریف بالا روشن است که اگر X خود یک زیرحلقه‌ی R باشد، آنگاه $<X>=X$. همچنین، $<\varnothing>=<0>=\{0\}$.

۳- با توجه به نتیجه‌ی ۱۳.۴.۲، روشن است که $<n>=n\mathbb{Z}$، و

$$<m>\wedge<n>=<m>\cap<n>=(m,n)\mathbb{Z}$$
$$<m>\vee<n>=<m,n>=[m,n]\mathbb{Z}$$

۴- در حلقه‌ی $M_2(\mathbb{Z})$ از ماتریس‌ها، داریم (تمرین ۲۳ را ببینید).

$$<\begin{bmatrix}1&0\\0&0\end{bmatrix},\begin{bmatrix}0&0\\0&1\end{bmatrix}>=\left\{\begin{bmatrix}m&0\\0&n\end{bmatrix}|m,n\in\mathbb{Z}\right\}$$

حال ببینیم همتای قضیه‌ی ۹.۳.۲ و نتیجه های آن، برای حلقه‌ها به چه صورت هستند. با توجه به تجربه‌ای که در مورد گروه‌ها به دست آوردیم، حدس می‌زنید عضوهای حلقه‌ی $<X>$ به چه صورت باشند؟ احتمالاً درست حدس زده‌اید، مجموع و تفاضلی از حاصل‌ضرب‌های اعضای X. یعنی،

۱۴.۱.۳ قضیه. فرض کنیم $(R;+,\cdot)$ یک حلقه است و $\varnothing \neq X \subseteq R$. در این صورت،

$$< X > = \left\{ \sum_{i=1}^{n} m_i \cdot (x_{i1} \dots x_{ik_i}) : n, k_i \in \mathbb{N}, m_i \in \mathbb{Z}, x_{i1}, \dots, x_{ik_i} \in X \right\}$$

به ویژه، اگر $X = \{x\}$ آنگاه

$$< X > = < x > = \left\{ \sum_{i=1}^{n} m_i x^i \mid n \in \mathbb{N}, m_i \in \mathbb{Z} \right\}$$

اثبات. روش کار را در فصل های **۱** و **۲** آموختیم. کافی است که مجموعه‌ی طرف راست را با S نشان دهید، سپس ثابت کنید که S **زیرحلقه**ی R، **شامل** X، و **مشمول** در هر زیرحلقه‌ای است که X را شامل شود. ابتدا از ناتهی بودن X نتیجه بگیرید که $0 = 0 \cdot x \in S$. همچنین، برای هر $x \in X$، $x = 1 \cdot x \in S$، که در آن $1 \in \mathbb{Z}$. سپس توجه کنید که تفاضل هر دو عضو S عضوی از S است. در پایان، فرض کنید T نیز زیرحلقه‌ای از R باشد که X را شامل می‌شود. در این صورت، هر $x \in X$ و در نتیجه هر عبارت به صورت $\sum_{i=1}^{n} m_i \cdot (x_{i1} \dots x_{ik_i})$ نیز عضو T است. **چرا؟**

تمرین ۱.۳

هوشم نه چنان است   تلاشم آنچنان است

۱- با کدام زوج از عمل‌های دوتایی زیر ($*_1$ برای جمع و $*_2$ برای ضرب)، دستگاه جبری $(\mathbb{R}, *_1, *_2)$ حلقه است؟

(الف) $r *_1 s = 2(r+s)$، $r *_2 s = rs$.

(ب) $r *_1 s = 2rs$، $r *_2 s = rs$.

(پ) $r *_1 s = rs$، $r *_2 s = r^s$.

۲- فرض کنید $(A;+)$ گروهی **آبلی** و $EndA$ مجموعه‌ی همه‌ی درون‌ریختی‌های روی گروه A (همریختی‌های از A به A) باشد. **نشان دهید** که $(EndA:+,\circ)$، همراه با جمع و ترکیب توابع، یعنی

$$(f+g)(x) = f(x) + g(x)$$
$$(f \circ g)(x) = f(g(x))$$

حلقه‌ای یک‌دار است که در حالت کلی **تعویض‌پذیر نیست**.

۳- فرض کنید R حلقه‌ای یک‌دار است. ثابت کنید که به ازای هر $a \in R$، $(-1)a = -a$.

۴- اثبات قضیه‌ی **۱۴.۳.۱** را کامل کنید.

۵- نشان دهید که حلقه‌ی R تعویض‌پذیر است اگر و تنها اگر $CentR = R$.

۶- فرض کنید $(R,+,.)$ یک حلقه است. ثابت کنید $(R,+,*)$ ، که در آن $a * b = b.a$، نیز یک حلقه است. این حلقه‌ی را **حلقه‌ی دوگان** R می‌نامیم و با R^{op} (یا R^d) نشان می‌دهیم. روشن است که اگر R تعویض‌پذیر باشد، $R = R^{op}$.

۷- فرض کنید R حلقه است. ثابت کنید که R تعویض‌پذیر است اگر و تنها اگر برای هر $a,b \in R$،

$$(a+b)^2 = a^2 + 2ab + b^2$$

۸- فرض کنید R حلقه است. ثابت کنید که R تعویض‌پذیر است اگر و تنها اگر برای هر $a,b \in R$،

$$a^2 - b^2 = (a-b)(a+b)$$

توجه کنید که $(a-b)(a+b) = a^2 + ab - ba - b^2$.

۸- فرض کنید R حلقه‌ای **تعویض‌پذیر** است. ثابت کنید که به ازای هر $a,b \in R$، داریم

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

۹- فرض کنید R حلقه‌ای یک‌دار است. نشان دهید که اگر $a^2 = a$ آنگاه $(1-a)^2 = 1-a$.

۱۰- از مجموعه‌های زیر کدام(ها) زیرحلقه‌ی $M_2(\mathbb{Z})$ است؟

(الف) $S = \left\{ \begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix} | a,b \in \mathbb{Z} \right\}$.

(ب) $T = \left\{ \begin{bmatrix} 0 & 0 \\ a & b \end{bmatrix} | a,b \in \mathbb{Z} \right\}$.

۱۱- نشان دهید که $S=\{a+b\sqrt[3]{2}+c\sqrt[3]{4}:a,b\in\mathbb{Z}\}$ زیرحلقه‌ی $\mathbb{R}$ است. آیا عضوهای ناصفر این حلقه نسبت به ضرب وارون دارند؟

۱۲- فرض کنید R حلقه است و $a\in R$ خودتوان باشد (یعنی، $a^2=a$). نشان دهید که $aRa=\{ara:r\in R\}$ یک زیرحلقه‌ی R و a عضو همانی آن است. خودتوان بودن a در کجا استفاده می‌شود؟

۱۳- نشان دهید که مجموعه‌ی

$$S=\left\{\begin{bmatrix} a+bi & c+di \\ -c+di & a-bi\end{bmatrix}:a,b,c,d\in\mathbb{C}\right\}$$

زیرحلقه‌ی $M_2(\mathbb{C})$ است.

۱۴- فرض کنید R حلقه است و $a\in R$. نشان دهید که هر یک از مجموعه‌های

$$T=\{x\in r:xa=0\} \quad \text{و} \quad S=\{x\in R:ax=0\}$$

زیرحلقه‌ی R است.

۱۵- (الف) زیرحلقه‌ی $<3>$ را در حلقه‌ی $\mathbb{Z}$ مشخص کنید.

(ب) زیرحلقه‌ی $<1/2>$ را در حلقه‌ی $\mathbb{R}$ مشخص کنید.

دسته دوم

۱۶- فرض کنید R حلقه‌ای یک‌دار است. ثابت کنید که اگر به ازای هر $x,y\in R$ داشته باشیم $(xy)^2=x^2y^2$، آنگاه R تعویض‌پذیر است. با یک مثال نشان دهیدکه فرض یک‌دار بودن، ضروری است.

۱۷- فرض کنید R حلقه است. عضو $a\in R$ را **پوچتوان** می‌نامیم اگر عدد طبیعی n وجود داشته باشد به طوری که $a^n=0$.

(الف) عضوی پوچتوان در $M_2(\mathbb{Z})$ بیابید.

(ب) با استفاده از محک زیرحلقه نشان دهید که مجموعه‌ی عضوهای پوچتوان یک حلقه‌ی یک‌دار و تعویض‌پذیر، زیرحلقه‌ی آن است. (تمرین **۸** را ببینید).

۱۸- فرض کنید a عضوی پوچتوان در حلقه‌ی تعویض‌پذیر و یک‌دار R باشد. ثابت کنید که $1+a$ وارون پذیر (یکه) است و نتیجه بگیرید که مجموع یک عضو یکه و یک عضو پوچتوان عضوی یکه است.

۱۹- فرض کنید که حلقه‌ی R عضو پوچتوان ناصفر ندارد. ثابت کنید که هر عضو خودتوان در مرکز R قرار دارد.

۲۰- ثابت کنید که شرایط زیر در هر حلقه‌ی R معادل هستند:

(الف) R دارای هیچ عضو پوچتوان ناصفر نیست.

(ب) برای هر $r \in R$، اگر $r^2 = 0$ آنگاه $r = 0$.

۲۱- مثالی از حلقه‌ای یک‌دار بیابید که دارای زیرحلقه‌ای نا صفر یک‌دار باشد که یکه‌ی آن با یکه‌ی حلقه متفاوت است.

۲۲- فرض کنید R حلقه‌ای دلخواه باشد و $x \in R$. ثابت کنید که اگر **تنها یک** $a \in R$ وجود داشته باشد به طوری که $xa = a$، آنگاه $ax = x$ (به ویژه، اگر R تنها دارای یک عضو همانی راست باشد) آنگاه R حلقه‌ای یک‌دار است. (توجه می‌کنیم که $x(a + ax - x) = x$).

۲۳- فرض کنید R حلقه‌ای یک‌دار باشد و $x \in R$. ثابت کنید که اگر **تنها یک** $y \in R$ وجود داشته باشد به طوری که $xyx = x$، آنگاه x وارونپذیر است. (توجه کنید که اگر $xr = 0$ آنگاه $r = 0$ زیرا $x(y + r)x = x$. حال از یکتایی y و $x(yx - 1) = 0$ استفاده کنید).

۲۴- فرض کنید R حلقه‌ای یک‌دار و نامتناهی باشد. ثابت کنید که اگر $a \in R$ بیش از یک وارون راست داشته باشد، آنگاه دارای بی‌نهایت وارون راست است. (فرض کنید $a_0 \in A = \{a' \mid aa' = 1\}$ و سپس نشان دهید که تابع $f(a') = a'a - 1 + a_0$ روی A یک به یک است ولی پوشا نیست).

۲۵- فرض کنید $(R; +, \cdot, 1)$ دستگاهی جبری باشد که در تمام شرایط یک حلقه‌ی یک‌دار بجز احتمالاً شرط تعویض‌پذیری عمل جمع صدق کند. ثابت کنید که عمل جمع نیز باید تعویض پذیر باشد (باید ثابت کنید که شرط تعویض‌پذیری عمل جمع، از شرایط دیگر نتیجه می‌شود).

۲۶- فرض کنید R حلقه‌ای با این ویژگی باشد که به ازای هر $a \in R$، $a^2 + a$ در مرکز R واقع است. ثابت کنید که R تعویض‌پذیر است.

۲۷- حلقه‌ی یک‌دار R را **بولی** می‌گوییم اگر هر عضو آن خودتوان باشد، به این معنی که برای هر $x \in R$، $x^2 = x$. فرض کنید که حلقه‌ی R بولی است. نشان دهید که

(الف) برای هر $a \in R$، $a + a = 2.a = 0$ (یعنی، $a = -a$).

(ب) حلقه‌ی R تعویض‌پذیر است.

۲۸- فرض کنید $S = \{M_{a,b} \mid a, b \in R\}$ که در آن

$$M_{a,b} = \begin{bmatrix} a & b \\ -b & a \end{bmatrix}$$

(الف) نشان دهید که S زیرحلقه‌ی $M_2(\mathbb{R})$ است. (**راهنمایی:** نشان دهید که $M_{a,b} - M_{c,d} = M_{a-c,b-d}$ و $M_{a,b}M_{c,d} = M_{ac-bd,ad+bc}$).

(ب) نشان دهید که $T = \{M_{a,0} : a \in \mathbb{R}\}$ زیرحلقه‌ای از S است.

۲.۳ دامنه‌ی صحیح و میدان

برخی از انواع حلقه‌ها اهمیت ویژه‌ای دارند و در مباحث دیگر ریاضیات یا علوم دیگر بسیار به کار می‌روند. همان طور که گفتیم، برخی از انواع حلقه‌ها با مجرد سازی و تعمیم ویژگی‌های دستگاه‌های جبری اعداد (همراه با دو عمل دوتایی معمولی جمع و ضرب آن‌ها) به دست می‌آیند. دو نوع با اهمیت از این انواع، **دامنه‌ی صحیح** و **میدان** نام دارند. در این بخش این دو نوع حلقه را معرفی و به اختصار مطالعه می‌کنیم. مطالعه‌ی بیشتر این حلقه‌های مهم در درس‌های دیگر جبر انجام می‌شود.

۳.۲.۳ بحث در کلاس. با وجودی که $\mathbb{Z}$ یا حتی $\mathbb{Z}^* = \mathbb{Z} \setminus \{0\}$، همراه با ضرب معمولی اعداد، گروه نیست ولی قوانین حذف (چپ و راست) برقرار هستند. یعنی، برای هر $b,c \in \mathbb{Z}$، داریم

$$(\forall a \neq 0) \quad ab = ac \quad \vee \quad ba = ca \quad \Rightarrow \quad b = c$$

همچنین، حاصل ضرب هر دو عضو ناصفر در حلقه‌ی $\mathbb{Z}$ ناصفر است. یعنی،

$$a \neq 0 \quad \wedge \quad b \neq 0 \Rightarrow ab \neq 0$$

در حالی که، برای مثال، در حلقه‌ی $\mathbb{Z}_8$، $2 \odot_8 4 = 0$ و همچنین

$$2 \odot_8 4 = 2 \odot_8 0 \not\Rightarrow 4 = 0$$

حال می‌خواهیم حلقه‌های دلخواه با این ویژگی‌ها را نامگذاری و قدری مطالعه کنیم. قبل از این کار، به لم زیر توجه کنید.

۴.۲.۳ لم. احکام استلزامی زیر در هر حلقه‌ی R معادل هستند:

(الف) (**قوانین حذف**) $(\forall a \neq 0) \quad ab = ac$ یا $ba = ca \Rightarrow b = c$

(ب) $ab = 0 \Rightarrow a = 0$ یا $b = 0$.

(پ) مجموعه‌ی $R^* = R \setminus \{0\}$ نسبت به ضرب بسته است. یعنی،

$$a \neq 0, b \neq 0 \Rightarrow ab \neq 0$$

اثبات. گزاره‌های **(ب)** و **(پ)** عکس نقیض یکدیگرند و در نتیجه معادل هستند. پس کافی است معادل بودن **(الف)** را با یکی از این دو، اثبات کنیم.

(الف) $\Leftarrow$ **(ب)**: فرض کنیم قوانین حذف در R برقرار باشند. برای اثبات حکم (ب)، فرض می‌کنیم $ab=0$، و $a\neq 0$. حال از $ab=a0$ و **(الف)** نتیجه بگیرید که $b=0$. به همین صورت می‌توانید نشان دهید که اگر $b\neq 0$ آنگاه $a=0$.

(ب) $\Leftarrow$ **(الف)**: فرض کنیم $ab=ac$ و $a\neq 0$. در این صورت،

$$0=ab-ac=a(b-c)$$

پس بنابر **(ب)**، $b-c=0$ و در نتیجه $b=c$. به همین صورت می‌توانید نشان دهید که اگر $ba=ca$ و $a\neq 0$ آنگاه $b=c$.

حال مفهومی مرتبط با مفاهیم معادل بالا را تعریف می‌کنیم.

۵.۲.۳ تعریف. عضو ناصفر a را در حلقه‌ی R **مقسم**، یا **مقسوم‌علیه، صفر چپ** (یا **راست**) می‌نامیم اگر عضو ناصفر $b\in R$ با ویژگی $ab=0$ (یا $ba=0$) وجود داشته باشد. عضو $a\in R$ را **مقسوم‌علیه صفر** می‌نامیم اگر هم مقسوم‌علیه صفر چپ و هم مقسوم‌علیه صفر راست باشد.

روشن است که اگر R تعویض‌پذیر باشد، تفاوتی بین سه مفهوم بالا وجود ندارد. حال آماده‌ایم که حلقه‌های خاص مورد نظرمان را تعریف کنیم.

۶.۲.۳ تعریف. حلقه‌ی **ناصفر**، تعویض‌پذیر، و یک‌دار D را **دامنه** (**یا حوزه**) **صحیح** (به اختصار، **دامنه**) می‌گوییم اگر دارای مقسوم‌علیه صفر **نباشد**.

۷.۲.۳ بحث در کلاس

۱- روشن است که هر یک از سه شرط معادل لم ۴.۲.۳ برای حلقه‌های تعویض‌پذیر با شرط نداشتن مقسم صفر معادل است.

۲- در هر دامنه‌ی صحیح، داریم $1\neq 0$ (بند **۱** بحث **۳.۱.۳** را ببینید). از این رو، $(\mathbb{Z}_2;+_2,\cdot_2)$ کوچک‌ترین دامنه‌ی صحیح است.

۳- روشن است که $\mathbb{Z}$، $\mathbb{Q}$، $\mathbb{R}$، و $\mathbb{C}$ دامنه (صحیح) هستند. البته، حلقه‌ی ماتریس‌های حقیقی $n\times n$، برای $n\geq 2$ دامنه‌ی صحیح **نیست**. زیرا، برای مثال

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

۴- حلقه‌ی $n\mathbb{Z}$، برای $n \geq 2$، تنها به این دلیل دامنه نیست که همانی (ضربی) ۱ را ندارد.
۵- حلقه‌ی $\mathbb{Z}_n$، برای عدد غیر اول $n > 2$، دامنـه صـحیح نیسـت. زیـرا اگـر $n = rs$ و $r, s > 1$، آنگاه $r \cdot_n s = 0$. البته اگر p عددی اول باشد، آنگاه $\mathbb{Z}_p$ دامنه‌ی صحیح است. **چرا؟** در واقع، مـی-توانید نشان دهید که حلقه‌ی $\mathbb{Z}_n$ دامنه‌ی صحیح است اگر و تنها اگر $n = p$ عددی اول باشد. (بند ۶ زیر را نیز ببینید).
۶- عضو ناصفر m در حلقه‌ی $\mathbb{Z}_n$ مقسم صفر است اگر و تنها اگر $(m,n) \neq 1$. دلیل این امر ایـن است که اگر s عضوی ناصفر در حلقـه‌ی $\mathbb{Z}_n$ باشـد و $m \cdot_n s = 0$، آنگـاه $n \mid ms$. در نتیجـه، اگـر $(m,n) = 1$ آنگـــاه $n \mid s$ کـــه تنـــاقض اســـت. بـــرعکس، اگـــر $(m,n) = d > 1$ آنگـــاه $m(n/d) = (m/d)n$، و در نتیجـه $r \cdot_n (n/d) = 0$، یعنـی، m در حلقـه‌ی $\mathbb{Z}_n$ مقسـم صفر است. پس عضو ناصفر m در حلقه‌ی $\mathbb{Z}_n$ مقسم صفر نیست اگر و تنها اگـر $(m,n) = 1$ اگـر و تنها اگر m **وارون‌پذیر باشد** (بند ۵(ح) بحث ۴.۱.۲ را ببینید).
۷- به ازای هر مجموعه چون X که حداقل ۲ عضو دارد، حلقه‌ی $(\mathcal{P}(X); \Delta, \cap)$ دامنـه‌ی صـحیح نیست. زیرا X زیرمجموعه‌هایی ناتهی دارد که اشتراک تهی دارند!
۸- حلقه‌ی $\mathbb{R}^R$ دامنه‌ی صحیح نیست. زیرا، به سادگی می‌توان تابع‌هایی ناصـفر یافـت کـه ضربشـان صفر است. مثال بیاورید.
۹- حلقه‌ی چهارگان‌های همیلتون، دارای مقسم صفر نیست (تمرین ۶ این بخـش را ببینیـد)، ولـی بـه دلیل تعویض‌پذیر نبودن، دامنه‌ی صحیح نیست.

حال ویژگی دیگری از اعداد را مجرد سازی می‌کنیم که $\mathbb{Z}$ فاقـد آن اسـت ولـی $\mathbb{Q}$، $\mathbb{R}$، و $\mathbb{C}$ آن ویژگی را دارند: اگر چه $\mathbb{Z}^* = \mathbb{Z} \setminus \{0\}$ نسبت به عمل ضرب یک گروه نیست، ولی $\mathbb{Q}^*$، $\mathbb{R}^*$، و $\mathbb{C}^*$ گروه هستند. از این رو تعریف زیر را می‌آوریم.

۸.۲.۳ تعریف. حلقه‌ی $(F; +, \cdot)$ را **میدان** (یا **هیات**) می‌گوییم اگـر $F^* = F \setminus \{0\}$ همـراه بـا ضرب حلقه یک گروه **آبلی** باشد. اگر شرط آبلی بودن ضرب را در نظر نگیریم، حلقه‌ی حاصل را **حلقه-ی بخشی** (یا **حلقه‌ی تقسیم**) می‌گوییم.

۹.۲.۳ بحث در کلاس

۱- روشن است که حلقه‌های اعداد $\mathbb{Q}$، $\mathbb{R}$، و $\mathbb{C}$ میدان هستند.
۲- روشن است که هر میدان یک دامنه‌ی صحیح است. (بند ۳ بحث ۶.۱.۳ را ببینید). ولی عکس ایـن مطلب لزوماً برقرار نیست. مثالی نقض بیاورید.
۳- حلقه‌ی چهارگان‌های همیلتون نمونه‌ای مهم از حلقه‌ی بخشی است که میدان نیست.

۴- حلقه‌ی $\mathbb{Q}[\sqrt{2}]=\{a+b\sqrt{2}\mid a,b\in\mathbb{Q}\}$ میدان است. وارون ضربی عضو ناصفر $a+b\sqrt{2}$ را بیابید. ولی به روشنی $\mathbb{Z}[\sqrt{2}]$ میدان نیست. **چرا؟**

۵- حلقه‌ی $\mathbb{Z}_p$ که در آن p عددی اول است، یک میدان است. (چطور؟). توجه می‌کنیم که $\mathbb{Z}_2=\{0,1\}$ میدانی با کم‌ترین تعداد عضو است. در واقع، حلقه‌ی $\mathbb{Z}_n$ میدان است اگر و تنها اگر $n=p$ عددی اول باشد. **چرا؟**

۶- آیا میدان‌های متناهی بجز $\mathbb{Z}_p$ها وجود دارند؟ در واقع برای هر عدد اول p و هر عدد طبیعی n میدانی با p^n عضو وجود دارد. برای مثال، $F=\{0,1,a,b\}$ همراه با عمل‌های جمع و ضرب زیر، میدان است:

$+$	0	1	a	b
0	0	1	a	b
1	1	0	b	a
a	a	b	0	1
b	b	a	1	0

$\cdot$	0	1	a	b
0	0	0	0	0
1	0	1	a	b
a	0	a	b	1
b	0	b	1	a

توجه می‌کنیم که $(F;+)$ همان گروه کلاین است و $F\setminus\{0\}$ همراه با عمل ضرب، جدول سمت راست، اساساً همان گروه $\mathbb{Z}_3$ است. مثال‌های دیگر میدان‌های p^n عضوی و کاربردهای آن‌ها را در دروس دیگر جبر، به ویژه در نظریه‌ی گالوا و نظریه‌ی رمزنگاری، خواهیم دید.

قضیه‌ی زیر نیز بسیار جالب است. این قضیه در واقع همتای قضیه‌ی **۱۰.۱.۲** است.

۱۰.۲.۳ قضیه. هر دامنه‌ی صحیح **متناهی** D یک میدان است.

اثبات. یک روش اثبات این حکم را در فصل ۲ دیده‌اید. ارائه مجدد آن را به عهده‌ی شما می‌گذاریم. برای آموزش فنی دیگر، آن را به روش زیر اثبات می‌کنیم. نشان می‌دهیم که هر عضو ناصفر در دامنه‌ی صحیح و متناهی $D=\{0,1,a_1,\cdots,a_n\}$ وارون دارد. فرض کنیم $a\neq 0$ عضو D باشد. تابع $l_a:D\to D$ را با تعریف (انتقال چپ) $l_a(x)=ax$ در نظر می‌گیریم. چون D در قوانین حذف صدق می‌کند، l_a تابعی یک به یک است. ولی می‌دانیم که هر تابع یک به یک روی یک مجموعه‌ی متناهی، پوشا نیز هست. حال روشن است که پیش‌نگاره‌ی 1 تحت l_a وارون ضربی a است.

حال ویژگی جالبی را معرفی می‌کنیم که حلقه‌ها، به ویژه میدان‌ها، را از یکدیگر متمایز می‌سازد. این ویژگی برایتان نا آشنا نیست. تعریف زیر را ببینید.

۱۲.۲.۳ تعریف. فرض کنیم F میدان، دامنه‌ی صحیح، یـا حتـی حلقـه‌ای یـک‌دار اسـت. در ایـن صورت، مرتبه‌ی عضو ۱ در گروه جمعی $(F;+)$، یعنی کوچک‌ترین عدد طبیعی n را که

$$n \cdot 1 = 1 + 1 + \cdots + 1 = 0$$

مشخصه‌ی F می‌نامیم و می‌نویسیم $CharF = n$ یـا گـاهی $ChF = n$. اگـر ایـن عـدد وجـود نداشته باشد، می‌نویسیم $ChF = 0$.

۱۳.۲.۳ بحث در کلاس

۱- روشن است که اگر F یک میدان، دامنه‌ی صحیح، یا حلقه‌ای یک‌دار باشد و $CharF = n \neq 0$، آنگاه $n > 1$.

۲- مشخصه‌ی حلقه‌ی R را که ممکن است یک‌دار نباشد برابر با کوچک‌ترین عـدد طبیعـی n تعریـف می‌کنیم به طوری که **برای هر** $a \in R$،

$$n \cdot a = a + a + \cdots + a = 0$$

و اگر چنین عدد طبیعی وجود نداشته باشد، مانند بالا مـی‌نویسـیم $CharR = 0$. البتـه مـی‌توانیـد نشان دهید که تعریف **۱۲.۲.۳** برای حلقه‌های یک‌دار با این تعریف معـادل اسـت. بـرای اثبـات، از ایـن مطلب استفاده کنید که، بنابر اتحاد توزیع‌پذیری،

$$n \cdot a = a + \cdots + a = a1 + \cdots + a1 = a(1 + \cdots + 1) = a0 = 0$$

۳- روشن است که

$$Char\mathbb{Z} = Char\mathbb{Q} = Char\mathbb{R} = Char\mathbb{C} = 0, \qquad Char\mathbb{Z}_n = n$$

۴- این مطلب نیز جالب است که اگر F یک میدان یا دامنه‌ی صحیح باشد، آنگاه $CharF = 0$ یا عددی اول است. زیرا، اگر $CharF = n \neq 0$ اول نباشد، آنگاه $n = rs$، به طوری که $r, s < n$. حال، مراحل زیر را توضیح دهید:

$$0 = n\cdot 1 = rs\cdot 1 = \underbrace{(1+\cdots+1)}_{r}\underbrace{(1+\cdots+1)}_{s}$$
$$\Rightarrow \underbrace{(1+\cdots+1)}_{r} = 0 \quad \vee \quad \underbrace{(1+\cdots+1)}_{s} = 0$$

که تناقض است. **چرا؟**

تمرین ۲.۳

۱- مقسوم‌علیه‌های صفر حلقه‌های $\mathbb{Z}_{10}$ و $\mathbb{Z}_{25}$ را بیابید.

۲- نشان دهید که یک عضو که مقسم صفر (چپ یا راست) است، نمی‌تواند وارون‌پذیر باشد.

۳- ثابت کنید که حلقه‌ی دلخواه R دارای مقسوم‌علیه صفر چپ نیست اگر و تنها اگر دارای مقسوم‌علیه صفر راست نباشد.

۴- فرض کنید R حلقه‌ای تعویض‌پذیر باشد. نشان دهید که اگر $a \in R$ مقسوم‌علیه صفر باشد، آنگاه به ازای هر $r \in R$، ar نیز به شرطی که ناصفر باشد، مقسوم‌علیه صفر است.

۵- نشان دهید که هر عضو ناصفر و خود توان $a \neq 1$ در حلقه‌ی یک‌دار R مقسوم‌علیه صفر است.

۶- ثابت کنید که

(الف) حلقه‌ی چهارگان‌های همیلتون، دارای مقسم صفر نیست.

(ب) حلقه‌ی چهارگان‌های همیلتون، حلقه‌ی بخشی است.

۷- نشان دهید که معادله‌ی $x^2 = 1$ در یک دامنه‌ی صحیح تنها دارای جواب‌های ۱ و ۱- است. جواب های این معادله را در میدان $\mathbb{Z}_7$ و در نادامنه‌ی $\mathbb{Z}_8$ بیابید.

۸- نشان دهید که هر حلقه‌ی متناهی بدون مقسم صفر، یک حلقه‌ی بخشی است.

۹- قضیه‌ی **۱۰.۲.۳** را به روش مشابه قضیه‌ی **۱۰.۱.۲** در گروه‌ها اثبات کنید.

۱۰- نشان دهید که $\mathbb{Q}$ کوچک ترین میدان شامل $\mathbb{Z}$ و کوچکترین زیرمیدان $\mathbb{R}$ است.

۱۱- فرض کنید در حلقه‌ی ناصفر R، به ازای هر x، $x = -x$. مشخصه‌ی R چند است؟

۱۲- مثالی از یک حلقه‌ی با مشخصه‌ی ۳ بیابید که میدان نباشد.

دسته دوم

۱۳- با استفاده از میدان بودن $\mathbb{Z}_p$، برای عدد اول p، همنهشتی $x^{p-1} \equiv_p 1$ را برای اعداد صحیح x با ویژگی $p \nmid x$ اثبات کنید. این حکم در نظریه‌ی اعداد موسوم به **قضیه‌ی کوچک فرما** است.

(**راهنمایی:** این واقعیت را به کار ببرید که گروه ضربی $\mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{0\}$ دارای $p-1$ عضو است).

۱۴- فرض کنید R یک حلقه‌ی بخشی باشد. ثابت کنید که مرکز حلقه، یعنی $CentR$، تشکیل یک میدان می‌دهد.

۱۵- فرض کنید R حلقه‌ای با بیش از یک عضو باشد به طوری که معادله‌ی $ax=b$ برای هر عضو ناصفر $a\in R$ و هر $b\in R$ دارای جواب باشد. ثابت کنید R حلقه‌ای بخشی است.

۱۶- فرض کنید R حلقه‌ای با بیش از یک عضو باشد به طوری که برای هر عضو ناصفر $a\in R$، عضو منحصر به فرد $b\in R$ وجود داشته باشد به طوری که $aba=a$. ثابت کنید که

(الف) عضو صفر تنها مقسوم‌علیه صفر R است. **(ب)** $bab=b$.

(پ) R حلقه‌ای یک‌دار است. **(ت)** R حلقه‌ای بخشی است.

۱۷- ثابت کنید که هیچ دامنه‌ی صحیح از مرتبه‌ی ۶ وجود ندارد.

۱۸- فرض کنید a و b عضوهایی از حلقه‌ی R باشند به طوری که ab پوچتوان است. نشان دهید که ba نیز پوچتوان است.

۱۹- ثابت کنید که:

(الف) عضو خودتوان ناصفر در یک حلقه نمی‌تواند پوچتوان باشد.

(ب) تنها عضوهای خودتوان در یک دامنه‌ی صحیح، ۰ و ۱ هستند.

(پ) در یک دامنه‌ی صحیح، صفر تنها عضو پوچتوان است.

(ت) در یک حلقه‌ی یک‌دار، یک عضو پوچتوان، وارون‌پذیر نیست.

۲۰- فرض کنید R حلقه‌ای بدون عضو پوچتوان ناصفر باشد. ثابت کنید که هر عضو خودتوان در مرکز R قراردارد.

۲۱- فرض کنید که a عضوی پوچتوان از حلقه‌ی تعویض‌پذیر و یک‌دار R باشد. ثابت کنید که $1+a$ عضوی یکال در R است و نتیجه بگیرید که مجموع یک عضو یکال و یک عضو پوچتوان عضوی یکال است.

۲۲- فرض کنید R حلقه‌ای دلخواه باشد و $r\in R$، به طوری که $r-r^2$ پوچتوان باشد. ثابت کنید اگر r پوچتوان نباشد، آنگاه R دارای عضو خودتوان ناصفر است.

۲۳- ثابت کنید در هر حلقه‌ی دلخواه R، شرایط زیر معادل هستند.

(الف) R دارای هیچ عضو پوچتوان ناصفر نیست.

(ب) $r^2=0 \Rightarrow r=0$.

۲۴- فرض کنید R حلقه‌ای یک‌دار و تعویض‌پذیر با مشخصه‌ی عدد اول p باشد. ثابت کنید که به ازای هر $a,b\in R$ و هر عدد صحیح مثبت n، $(a+b)^{p^n}=a^{p^n}+b^{p^n}$.

۲۵- ثابت کنید که اگر F میدانی متناهی باشد، آنگاه مرتبه‌ی F توانی از عددی اول است.

۳.۳ حلقه‌ی خارج قسمتی و ایده‌آل

در فصل‌های ۱ و۲ آگاهی خوبی از چگونگی افراز یک دستگاه جبری A برای ساختن دستگاه جبری خارج قسمتی به دست آوردیم و دیدیم که در حالت کلی باید A را تحت یک رابطه‌ی همنهشتی $\sim$ افراز کنیم. ولی در فصل۲ دیدیم که مجموعه‌ی همه‌ی گروه‌های خارج قسمتی یک گروه و مجموعه‌ی همنهشتی‌های روی آن گروه در تناظر دوسویی با زیرگروه‌های خاصی هستند که آن‌ها را زیر گروه-های نرمال نامیدیم، و همچنین دیدیم که رده‌ی شامل عضو همانی به تعبیری سازنده‌ی همه‌ی رده‌ها است، و هشدار (جدی! با مثال) دادیم که همتای آن مطالب برای بسیاری از دستگاه‌های جبری برقرار نیست. پس این سؤال مطرح می‌شود که در مورد حلقه‌ها چطور؟ خوشبختانه، خواهیم دید که خارج قسمت و همنهشتی‌های حلقه‌ای نیز دارای همتای این ویژگی‌های مفید و خاص هستند و با نوعی از زیرحلقه‌ها که ایده‌آل نام دارند، در تناظر دوسویی هستند. در واقع خواهیم دید که، مشابه مورد گروه‌ها، سه مجموعه‌ی زیر در تناظر دوسویی با یکدیگر هستند:

$Q(R) = \{$ مجموعه‌ی همه‌ی حلقه‌های خارج قسمتی $R/\sim$ $\}$
$Con(R) = \{$ مجموعه‌ی همه‌ی رابطه‌های همنهشتی $\sim$ روی حلقه‌ی R $\}$
$Id(R) = \{$ مجموعه‌ی همه‌ی ایده‌آل‌های حلقه‌ی R $\}$

لزومی ندارد، و ما نیز قصد نداریم، که مطالب فصل ۱ و به ویژه فصل ۲ را خط به خط تکرار کنیم. ولی، روش کار اثبات هم‌توانی مجموعه‌های بالا را به اختصار در بحث زیر می‌گنجانیم.

۱.۳.۳ بحث در کلاس

۱- ابتدا تعریف جامع حلقه‌ی خارج قسمتی را می‌آوریم. با توجه به تعریف جامع رابطه‌ی همنهشتی ۱.۷.۱ و مطالب دیگر همان بخش ۷.۱، روشن است که

(الف) رابطه‌ی هم‌ارزی $\sim$ روی حلقه‌ی $(R;+,\cdot)$ همنهشتی است اگر و تنها اگر با هر دو عمل جمع و ضرب حلقه سازگار باشد (۱.۷.۱ را ببینید). یعنی،

$$\begin{cases} x \sim x' \\ y \sim y' \end{cases} \Rightarrow \quad x+y \sim x'+y' \quad \& \quad xy \sim x'y' \qquad (*)$$

(ب) رابطه‌ی هم‌ارزی $\sim$ روی حلقه‌ی $(R;+,\cdot)$ همنهشتی است اگر و تنها اگر هر دو عمل

$$[x]\bar{+}[y]=[x+y] \quad , \quad [x]\bar{\cdot}[y]=[x\cdot y]$$

روی افراز $R/\sim$ خوش‌تعریف باشند. (تمرین ۱ بخش ۷.۱).

(پ) اگر $\sim$ رابطه‌ای همنهشتی روی حلقه‌ی R باشد، به راحتی می‌توانید، با استفاده از حلقه بودن R، نشان دهید که افراز $R/\sim$ همراه با عمل‌های داده شده در بند (ب)، حلقه می‌شود. این حلقه را **حلقه‌ی خارج قسمتی** R بر $\sim$ می‌نامیم.

۲- حال که تعریف جامع حلقه‌ی خارج قسمتی را دیدیم، ببینیم که این تعریف در جبر کلاسیک معمولاً به چه صورتی داده می‌شود و چرا؟ مانند مورد گروه‌ها، در اغلب کتاب‌های کلاسیک جبر، نشان می‌دهند که هر **ایده‌آل** (که تعریف آن را ارائه خواهیم داد)، حلقه‌ای خارج قسمتی به دست می‌دهد و در نتیجه تابعی یک به یک از $Id(R)$ به $Q(R)$ و لذا به $Con(R)$ وجود دارد. ولی معمولاً بیان نمی‌شود که تصادفاً این توابع دوسویی نیز هستند. یعنی، هر خارج قسمت یک حلقه یا هر همنهشتی روی یک حلقه حاصل از یک ایده‌آل است. در زیر به اختصار به این مطالب می‌پردازیم. برای اینکه ببینیم **مفهوم مهم ایده‌آل چطور به وجود آمده است**، بحث زیر را می‌آوریم.

۳- مانند مطالب بخش ۸.۲، سازگاری $\sim$ با عمل $+$، یعنی همنهشتی بودن $\sim$ روی گروه $(R;+)$، ایجاب می‌کند که رده‌ی $I=[0]=\{x\in R \mid x\sim 0\}$ زیرگروه نرمال $(R;+)$ باشد (البته چون گروه جمعی $(R;+)$ آبلی است، هر زیر گروه آن به خودی خود نرمال است). سازگاری $\sim$ با عمل ضرب حلقه، یعنی همنهشتی بودن $\sim$ روی نیم‌گروه ضربی $(R;\cdot)$، چه ویژگی دیگری روی زیرگروه $I=[0]$ القا می‌کند؟ واقعیت زیر را ببینید:

$$\begin{cases} x\in I \\ r\in R \end{cases} \Rightarrow \begin{cases} x\sim 0 \\ r\sim r \end{cases} \Rightarrow \begin{cases} rx\sim r0 \\ xr\sim 0r \end{cases} \Rightarrow \begin{cases} rx\sim 0 \\ xr\sim 0 \end{cases}$$
$$\Rightarrow \begin{cases} rx\in [0]=I \\ xr\in [0]=I \end{cases}$$

با توجه به این ویژگی‌های $I=[0]$، تعریف زیر را می‌آوریم.

۲.۳.۳ تعریف. فرض کنیم R حلقه است و $I\subseteq R$. می‌گوییم که I **ایده‌آل** R است، و می نویسیم $I\trianglelefteq R$، اگر I زیرگروه $(R;+)$ باشد، و برای هر $x\in I$ و هر $r\in R$، $rx, xr\in I$.

۳.۳.۳ بحث در کلاس

۱- با توجه به مطالب بالا، هر رابطه‌ی همنهشتی $\sim$ روی حلقه‌ی R، ایده‌آل $I=[0]$ از R را به دست می‌دهد. حال عکس این مطلب را بررسی می‌کنیم و با الگو قرار دادن حالت گروه‌ها، نشان می‌دهیم که برای هر ایده‌آل دلخواه I از حلقه‌ی R، رابطه‌ی زیر یک رابطه‌ی همنهشتی روی R است:

$$a \sim_I b \Leftrightarrow a-b \in I \qquad (**)$$

اثبات راحت سازگاری $\sim_I$ با عمل جمع را (که تکرار قضیه‌ی **۸.۸.۲** در نمادگذاری جمعی است) به شما واگذار می‌کنیم. دلیل هر مرحله از اثبات سازگاری $\sim_I$ با عمل ضرب حلقه را در زیر توضیح دهید:

$$\begin{cases} a \sim_I b \\ x \sim_I y \end{cases} \Rightarrow \begin{cases} a-b \in I \\ x-y \in I \end{cases} \Rightarrow \begin{cases} (a-b)x \in I \\ b(x-y) \in I \end{cases}$$
$$\Rightarrow \begin{cases} ax-bx \in I \\ bx-by \in I \end{cases} \Rightarrow ax-bx+bx-by \in I$$
$$\Rightarrow ax-by \in I \Rightarrow ax \sim by$$

۲- از این رو، **حلقه‌ی خارج قسمتی** $R/\sim_I = \{[a]_{\sim_I} \mid a \in R\}$ را همراه با عمل‌های زیر داریم:

$$[x]_{\sim_I} \bar{+} [y]_{\sim_I} = [x+y]_{\sim_I} \qquad \& \qquad [x]_{\sim_I} \bar{\cdot} [y]_{\sim_I} = [xy]_{\sim_I}$$

با الگو قرار دادن گروه خارج قسمتی، معمولاً این حلقه را به صورت ساده تر R/I به جای $R/\sim_I$ نشان می‌دهیم.

۳- نکته‌ی **بسیار جالب** در باره‌ی این رابطه‌ی همنهشتی این است که، مشابه مورد گروه‌ها، (ولی در نمادگذاری جمعی)، هر رده‌ی آن به صورت **هم‌مجموعه**ی

$$[a]_{\sim_I} = a+I = \{a+x \mid x \in I\}$$

است، زیرا

$$\begin{aligned} [a]_{\sim_I} &= \{x \in R \mid x \sim_I a\} \\ &= \{x \in R \mid x-a \in I\} \\ &= \{x \in R \mid (\exists y \in I)\, x = a+y\} \\ &= \{a+y \mid y \in I\} \\ &= a+I \end{aligned}$$

توجه می‌کنیم که به ویژه $[0]_{\sim_I}=0+I=I$ عضو **صفر** حلقه‌ی R/I است.

۴- با جمع‌بندی مطالب و نمادگذاری‌های بالا، معمولاً، به طور سنتی و متداول، **حلقه‌ی خارج قسمتی** R بر ایده‌آل I (همان بر رابطه‌ی همنهشتی $\sim_I$) را برابر با مجموعه‌ی

$$R/I=\{a+I \mid a\in R\}$$

همراه با عمل‌های دوتایی زیر تعریف می‌کنیم:

$$\boxed{(a+I)+(b+I)=(a+b)+I \quad , \quad (a+I)(b+I)=ab+I}$$

۴.۳.۳ بحث در کلاس

۱- با توجه به ویژگی‌های هم‌مجموعه‌ها که در فصل **۲** بیان شد، ویژگی‌های زیر برای اعضای R/I (در نماد گذاری جمعی) برقرار هستند:

$$\boxed{(a+I)=I \Leftrightarrow a\in I,\ \ (a+I)=(b+I)\Leftrightarrow (a-b)\in I}$$

۲- اگر R حلقه‌ای یک‌دار و I ایده‌آل R باشد، آنگاه روشن است که $1+I$ یکه‌ی R/I است.

۳- در فصل **۱** دیدیم که اگر معادله‌ای در دستگاهی جبری برقرار (یعنی **اتحاد**) باشد، آن معادله در خارج قسمت آن جبر نیز برقرار (**اتحاد**) است. از این رو، اگر حلقه‌ی R تعویض‌پذیر و I ایده‌آلی از R باشد، آنگاه R/I نیز تعویض‌پذیر است. (البته این مطلب را به راحتی می‌توانید به طور مستقیم نیز اثبات کنید). ولی، برای مثال، حاصل‌ضرب هر دو عضو ناصفر در $\mathbb{Z}$ ناصفر است، در حالی که در حلقه‌ی خارج قسمتی $\mathbb{Z}/\equiv_n$، برای عدد غیر اول $n>2$، این ویژگی برقرار نیست. برای مثال، در حلقه‌ی خارج قسمتی $\mathbb{Z}/\equiv_4$ داریم $[2]\cdot_4[2]=[4]=[0]$. همچنین، هیچ عضو مخالف ۱ در $\mathbb{Z}$ وارون (ضربی) ندارد، در حالی که در $\mathbb{Z}/\equiv_p$ هر عضو ناصفر وارون (ضربی) دارد. در واقع، برای عضو $a+p\mathbb{Z}$ که $a\in\{1,\dots,p-1\}$، چون $(a,p)=1$ اعداد صحیح b و c وجود دارند به طوری که $ab+pc=1$. حال با محاسبه‌ای ساده می توانید نشان دهید که $b+p\mathbb{Z}$ وارون ضربی $a+p\mathbb{Z}$ است. در ضمن، داریم $\mathbb{Z}/\equiv_n=\mathbb{Z}/n\mathbb{Z}$. **چطور؟**

حال که به اهمیت ایده‌آل‌ها پی بردیم، نکاتی را در باره‌ی آن‌ها بیان می‌کنیم، که کار کردن با آن‌ها را آسان‌تر می‌کند. ابتدا، با توجه به محک‌های زیرگروه و زیرحلقه، محک ایده‌آل را به صورت زیر داریم.

۵.۳.۳ قضیه (محک ایدآل). زیرمجموعه‌ی I از حلقه‌ی R ایده‌آل است اگر و تنها اگر

(الف) $0 \in I$،

(ب) برای هر $a,b \in I$، $a-b \in I$،

(پ) برای هر $r \in R$، و هر $x \in I$، $xr \in I$ و $rx \in I$.

۶.۳.۳ بحث در کلاس

۱- روشن است که هر ایده‌آل یک حلقه، زیرحلقه‌ی آن نیز هست. **چطور** نسبت به ضرب بسته است؟

۲- برای هر حلقه‌ی R، زیرحلقه‌های $\{0\}$ و R ایده‌آل R هستند.

۲- ایده‌آل‌های $\mathbb{Z}$ و $\mathbb{Z}_n$ دقیقاً زیرگروه‌ها یا همان زیرحلقه‌های آن‌ها هستند. **چطور؟**

۳- دیدیم که $\mathbb{Z}$ زیرحلقه‌ی $\mathbb{Q}$ است. ولی روشن است که ایده‌آل $\mathbb{Q}$ نیست، زیرا برای مثال، داریم $1 \in \mathbb{Z}$ و $2/3 \in \mathbb{Q}$ ولی $(2/3).1 = 2/3 \notin \mathbb{Z}$. به همین روش، نشان دهید که اگر I هر ایده‌آل **ناصفر** $\mathbb{Q}$ باشد، آنگاه باید هر عدد گویای m/n متعلق به I باشد، و در نتیجه $I = \mathbb{Q}$.

۴- (تعمیم بند **۳**) بسیاری مواقع لازم است نشان دهیم که ایده‌آل I برابر با خود حلقه‌ی R است. فرض کنیم I ایده‌آلی از حلقه‌ی یکدار R است.

(الف) اگر $1 \in I$ آنگاه $I = R$، زیرا برای هر $r \in R$، $r = r.1 \in I$.

(ب) اگر I شامل عضوی یکال (وارون‌پذیر) چون u باشد، آنگاه $I = R$، زیرا تعریف ایده‌آل ایجاب می‌کند که $1 = uu^{-1} \in I$.

۵- با توجه به بند **۴** بالا، هر میدان F تنها دو ایده‌آل دارد، $\{0\}$ و F. چطور؟ برعکس، اگر R حلقه‌ای تعویض‌پذیر و یکدار باشد، که دارای تنها دو ایده‌آل است، آنگاه R میدان است. چطور؟ (راهنمایی: ایدآل اصلی تولید شده توسط a را در نظر بگیرید).

۶- زیرحلقه‌های $R = (\mathcal{P}(X); \Delta, \cap)$ نیز لزوماً ایده‌آل نیستند. برای مثال، اگر $X = \{1,2,3\}$ آنگاه $S = \{\phi, \{1\}, \{2,3\}, X\}$ زیرحلقه‌ی R است ولی ایده‌آل آن نیست، زیرا $\{2,3\} \in S$ و $\{2\} \in R$، ولی $\{2\} = \{2,3\} \cap \{2\} \notin S$. (یادآوری می‌کنیم که در این حلقه، عمل ضرب همان عمل اشتراک است).

۷- از آنجا که حاصل‌ضرب یک تابع حقیقی پیوسته در یک تابع حقیقی دلخواه لزوماً پیوسته نیست (مثال بیاورید)، پس اگرچه $C(\mathbb{R},\mathbb{R})$ زیرحلقه‌ی $\mathbb{R}^{\mathbb{R}}$ است ولی ایده‌آل آن نیست.

۸- هیچ یک از زیرحلقه‌های مثال‌های **۶-۹** بحث **۱۰.۱.۳**، ایده‌آل نیستند. **چطور؟**

۹- بندهای **۶-۸** را با استفاده از بند **۴** نیز حل کنید.

۱۰- (**قضیه‌ی تناظر** برای حلقه‌ها) فرض کنیم I ایده‌آل حلقه‌ی R باشد. در این صورت، مشابه گروه‌ها، به راحتی می‌توانید نشان دهید که:

(الف) زیرحلقه‌های R/I دقیقاً به صورت K/I هستندکه در آن $I \le K \le R$.

(ب) ایده‌آل‌های R/I دقیقاً به صورت K/I هستند که در آن $I \le K \trianglelefteq R$.

۷.۳.۳ مشبکه‌ی ایده‌آل‌ها. (همتای مطالب زیر را نیز برای دستگاه‌های کلی در فصل ۱ و برای گروه‌ها در فصل ۲ دیده‌ایم) اشتراک هر مجموعه از ایده‌آل‌های یک حلقه به روشنی ایده‌آل است. در واقع، چون اشتراک زیرگروه‌ها، زیرگروه است، کافی است تنها شرط (پ) محک ایده‌آل (قضیه‌ی ۵.۳.۳) را برای اشتراک بررسی کنیم، و این شرط به وضوح، برای اشتراک و حتی برای اجتماع ایده‌آل-ها نیز برقرار است. ولی اجتماع ایده‌آل‌ها لزوماً ایده‌آل نیست (برای مثال، $2\mathbb{Z} \cup 3\mathbb{Z}$ حتی زیرگروه $\mathbb{Z}$ نیست تا اینکه بتواند ایده‌آل آن باشد). خواهیم دید که مجموعه‌ی $Id(R)$ متشکل از ایده‌آل‌های حلقه‌ی R همراه با $\subseteq$ مشبکه‌ای است که در آن اشتراک نقش اینفیمم را دارد و برای شناخت سوپریمم در آن باید، مشابه مشبکه‌ی زیرگروه‌ها و زیرحلقه‌ها، مفهوم کوچک‌ترین ایده‌آل شامل اجتماع را در نظر بگیریم.

۸.۳.۳ تعریف. فرض کنیم R یک حلقه است و $X \subseteq R$. اشتراک همه‌ی ایده‌آل‌های شامل X را، که همان کوچک‌ترین ایده‌آل شامل X است، **ایده‌آل تولید شده از** X می‌گوییم و آن را با نماد (X) نشان می‌دهیم (تا با نماد زیرحلقه‌ی تولید شده $< X >$ اشتباه نشود). اگر $X = \{x_1, \cdots, x_n\}$، آنگاه ایده‌آل **متناهی مولد** (X) را با $(x_1, \cdots, x_n)$ نیز نشان می‌دهیم. ایده‌آل تک مولدی (x) را **ایده‌آل اصلی** می‌نامیم.

۹.۳.۳ قضیه. فرض کنیم R حلقه‌ای تعویض‌پذیر و یک‌دار است و $X \subseteq R$. در این صورت

$$(X) = \left\{ \sum_{i=1}^{n} r_i x_i \mid n \in \mathbb{N}, r_i \in R, x_i \in X \right\}$$

به ویژه،

$$(x) = \{rx \mid r \in R\} = Rx = xR$$

اثبات. با توجه به تعریف، مشابه موارد دیگری که در مورد زیردستگاه‌های (به ویژه زیرگروه‌های) تولید شده دیدیم، باید نشان دهیم که مجموعه‌ی طرف راست، یعنی

$$I = \left\{ \sum_{i=1}^{n} r_i x_i \mid n \in \mathbb{N}, r_i \in R, x_i \in X \right\}$$

کوچک‌ترین ایده‌آلی است که X را شامل می‌شود. ابتدا مشاهده می‌کنیم که چون هر $x \in X$ به صورت $x = 1x$ نوشته می‌شود، پس $X \subseteq I$ و همچنین، $0 = 0x \in I$. حال با استفاده از محک ایده‌آل، به راحتی می‌توانید نشان دهید که مجموعه‌ی I ایده‌آل R است. با توجه به تعویض‌پذیر بودن R، برای اثبات شرط (پ) محک ایده‌آل، کافی است توجه کنیم که برای هر $r \in R$،

$$r\left(\sum_{i=1}^{n} r_i x_i\right) = \sum_{i=1}^{n} r(r_i x_i) = \sum_{i=1}^{n} (rr_i)x_i \in I$$

در پایان، اگر J ایده‌آلی از R باشد به طوری که $X \subseteq J$، آنگاه همه‌ی عضوهای به صورت rx، که در آن $r \in R$ و $x \in X$، و لذا مجموع‌های آن‌ها، عضو J خواهند بود. چرا؟ در نتیجه، همان‌طور که می‌خواستیم، $I \subseteq J$.

۱۰.۳.۳ بحث در کلاس

۱- همان‌گونه که دیدیم اجتماع ایده‌آل‌های یک حلقه‌ی R لزوماً ایده‌آل آن نیست. ولی قضیه‌ی ۹.۳.۳ بالا نشان می‌دهد که ایده‌آل تولید شده از اجتماع هر خانواده از ایده‌آل‌های R یک ایده‌آل آن است.

۲- نکته‌ای جالب توجه این است که همتای (جمعی) تمرین ۹ بخش ۸.۲ برای ایده‌آل‌ها نیز برقرار است. یعنی، اگر I و J ایده‌آل حلقه‌ی R باشند، آنگاه مجموع آن‌ها

$$I + J =: \{a + b \mid a \in I, b \in J\}$$

نیز به روشنی یک ایده‌ال R است و می‌توانید نشان دهید که برابر با ایده‌آل تولید شده از اجتماع $I \cup J$ (یعنی، کوچک‌ترین ایده‌آل شامل I و J) است (تمرین ۴ این بخش را نیز ببینید).

۳- با دیدن ایده‌آل مجموع $I + J$، این سؤال مطرح می‌شود که آیا حاصل‌ضرب

$$IJ = \{ab \mid a \in I, b \in J\}$$

نیز یک ایده‌آل است؟ پاسخ در حالت کلی منفی است. برای مثال، $(3\mathbb{Z})(2\mathbb{Z})$ ایده‌آل $\mathbb{Z}$ نیست، زیرا $3 + 2 = 5 \notin (3\mathbb{Z})(2\mathbb{Z})$. متداول است که ایده‌آل تولید شده از مجموعه‌ی IJ را نیز با همان نماد IJ نشان دهیم و آن را حاصل‌ضرب I در J بنامیم. شاید تصور کنیم که ایده‌آل IJ مجموعه‌ای بزرگ و دست کم شامل I و J است! نشان دهید که، برعکس، $IJ \subseteq I, J$. مجدداً با فرض

اینکه R حلقه‌ای تعویض‌پذیر و یک‌دار باشد و با به کار بردن قضیه‌ی بالا، ایده‌آل تولید شده از IJ عبارت است از

$$\{\sum_{i=1}^{n} a_i b_i \mid a_i \in I, b_i \in J\}$$

(تمرین ۷ این بخش را ببینید).

در پایان این بخش، دو نوع ایده‌آل مهم را معرفی می‌کنیم، که همتای اولی را در گروه‌ها نیز دیدیم.

۱۱.۳.۳ تعریف

۱- ایده‌آل **سره‌ی** M از حلقه‌ی R را **ماکسیمال** می‌گوییم اگر هیچ ایده‌آل سره‌ای، آن را به طور سره شامل نشود. یعنی اگر J ایده‌آلی از R باشد به طوری که $M \subseteq J \subseteq R$ آنگاه $J = M$ یا $J = R$. (به عبارت دیگر، M در مجموعه‌ی مرتب جزئی $(Id(R), \subseteq)$ ماکسیمال است).

۲- ایده‌آل سره‌ی P از حلقه‌ی R را **اول** می‌گوییم اگر برای هر $a, b \in R$،

$$ab \in I \Rightarrow a \in I \text{ یا } b \in I$$

۱۲.۳.۳ بحث در کلاس

۱- در حلقه‌ی $\mathbb{Z}$، ایده‌آل‌های $p\mathbb{Z}$ ماکسیمال هستند، که در آن p عددی اول است، زیرا برای هر دو عدد صحیح m و n داریم:

$$m\mathbb{Z} \subseteq n\mathbb{Z} \Leftrightarrow n \mid m$$

ایده‌آل‌های اول $\mathbb{Z}$ نیز $\{0\}$ و $p\mathbb{Z}$ ها هستند، زیرا اگر $ab = 0$ آنگاه $a = 0$ یا $b = 0$، و

$$mn \in p\mathbb{Z} \Leftrightarrow p \mid mn \Leftrightarrow p \mid m \text{ یا } p \mid n \Leftrightarrow m \in p\mathbb{Z} \text{ یا } n \in p\mathbb{Z}$$

این مثال نشان می‌دهد که چطور تعریف ایده‌آل اول برگرفته از تعریف اعداد اول است.

۲- در هر دامنه‌ی صحیح، $\{0\}$ یک ایده‌آل اول است. **چرا؟**

۳- در درس‌های دیگر جبر خواهیم دید که ایده‌آل‌های ماکسیمال و **اول** کاربردهای بسیاری دارند. برای نمونه قضیه‌ی زیر را ببینید. به خاطر بیاورید که در فصل ۱دیدیم که اگر دستگاهی جبری چون A دارای ویژگی‌ای نباشد و بخواهیم از آن جبری بسازیم که آن ویژگی را داشته باشد، A را بر یک رابطه‌ی همنهشتی مناسب تقسیم می‌کنیم. این مطلب در مورد گروه‌ها معادل است با تقسیم کردن

گروه بر **زیرگروه نرمال مناسب**، و در مورد حلقه‌ها معادل است با تقسیم کردن حلقه بـر **ایـده‌آلـی مناسب**. قضیه‌ی مهم و پر کاربرد زیر، از یک حلقه یک میدان و یک دامنه‌ی صحیح می‌سازد، و همتای قضیه ی **۱۸.۹.۲** در گروه‌ها است.

۱۳.۳.۳ قضیه. اگر R حلقه‌ای **تعویض‌پذیر و یک‌دار** و M ایده‌آلی از R باشد، آنگاه ۱- حلقه‌ی R/M میدان است اگر و تنها اگر ایده‌آل M ماکسیمال باشد. ۲- حلقه‌ی R/P دامنه‌ی صحیح است اگر و تنها اگر ایده‌آل P اول باشد.

اثبات

۱- فرض کنیم حلقه‌ی R/M میدان است. در این صورت، با توجه به تعریف میدان، که ناصفر است، $M \neq R$. حال فرض کنیم J ایده‌آلی از R باشد بـه طـوری کـه $M \subseteq J \subseteq R$. در ایـن صـورت J/M ایده‌آلی از میدان R/M است (بند ۱۰ بحث ۶.۳.۳ را ببینید). از آنجا که $\{0\}$ و F تنهـا ایده‌آل‌های هر میدان F هستند، پس $J/M = \{M\}$ یا $J/M = R/M$. یعنی، $J = M$ یـا $J = R$.

برعکس، فرض کنیم ایده‌آل M ماکسیمال است. در این صورت، حلقـه‌ی R/M ناصـفر اسـت. چرا؟ چون R تعویض‌پذیر و یک‌دار است، R/M نیز چنین است. حال، نشان می‌دهیم که هـر عضـو ناصفر آن دارای وارون ضربی است. فرض کنیم $a+M \in R/M$ ناصفر است. پس $a+M \neq M$ و در نتیجه $a \notin M$. چون ایده‌آل مجموع $M+(a)$ ایده‌آل M را به طور سـره شـامل مـی‌شـود، بنابر ماکسیمال بودن M باید $M+(a)=R$. پس عضوهای $x \in M$ و $r \in R$ وجـود دارنـد بـه طوری که $1_R = x + ra$. حال، بنابر تعریف جمع و ضرب در R/M، داریم

$$\begin{aligned}1_R + M &= (x+ra)+M = (x+M)+(ra+M)\\ &= ra+M = (r+M)(a+M)\end{aligned}$$

زیـرا، بـه دلیـل $x \in M$، $x+M = M$ صـفر R/M اسـت. بنـابراین، $r+M$ وارون ضـربی $a+M$ است، و در نتیجه R/M میدان است.

۲- ابتدا توجه می‌کنیم که مانند بند ۱، سره بودن P معادل با ناصفر بودن R/P است. حال توجه می‌کنیم که در حالت کلی،

$$(a+P)(b+P) = 0+P = P \Leftrightarrow ab+P = P \Leftrightarrow ab \in P$$

و در حالتی که ایده‌آل P اول است گزاره‌های بالا معادل هستند با

$$(a+P)(b+P) \Leftrightarrow ab \in P \Leftrightarrow a \in P \quad \vee \quad b \in P$$
$$\Leftrightarrow a+P=P \quad \vee \quad b+P=P$$

که همان مقسم صفر نداشتن R/P است (توجه کنید که از این واقعیت بسیار استفاده می‌کنیم که هم‌رده‌ی $P=0+P$ صفر حلقه‌ی R/P است). پس حکم اثبات شده است.

۱۴.۳.۳ بحث در کلاس

۱- در حلقه‌های تعویض‌پذیر و یک‌دار، هر ایده‌آل ماکسیمال اول است. این حکم، در واقع نتیجه‌ای از قضیه‌ی ۱۳.۳.۳ و این مطلب است که هر میدان، دامنه‌ی صحیح است .

۲- ایده‌آل‌های اول لزوماً ماکسیمال نیستند. برای مثال، ایده‌آل $\{0\}$ در $\mathbb{Z}$ اول است ولی ماکسیمال نیست! البته، ایده‌ال $\{0\}$ در هر $\mathbb{Z}_p$، و در هر میدان دلخواه، هم ماکسیمال است هم اول، **این طور نیست؟**

۳- ایده‌آل‌های ماکسیمال و اول حلقه‌های $\mathbb{Z}_4$ و $\mathbb{Z}_{12}$ را بیابید.

تمرین ۳.۳

۱- فرض کنید که $\sim$ رابطه‌ای همنهشتی روی حلقه‌ی R باشد. با استفاده از حلقه بودن R، نشان دهید که افراز $R/\sim$ همراه با عمل‌های طبیعی تعریف شده در بحث ۱.۳.۳، حلقه است.

۲- اگر I ایده‌آلی از حلقه‌ی R باشد، به طور مستقیم ثابت کنید که عمل‌های جمع و ضرب تعریف شده در بند ۴ بحث ۳.۳.۳ روی مجموعه‌ی هم‌مجموعه‌ها، یعنی روی $\{a+I \mid a \in R\}$، خوش-تعریف هستند.

۳- فرض کنید R حلقه‌ای دلخواه (نه لزوماً تعویض‌پذیر یا یک‌دار) است و $x \in R$. نشان دهید که

(الف) اعضای ایده‌آل تولید شده توسط x به صورت

$$rx + xs + nx + \sum_{i=1}^{m} r_i x s_i$$

هستند که در آن $r, s, r_i, s_i \in R$، $n \in \mathbb{Z}$، $m \in \mathbb{N}$.

(ب) اگر R یک‌دار باشد (و لزوماً تعویض‌پذیر نباشد)، اعضای ایده‌آل تولید شده توسط x به صورت $\sum_{i=1}^{m} r_i x s_i$ هستند که در آن $r_i, s_i \in R$، $m \in \mathbb{N}$.

۴- فرض کنید R حلقه‌ای دلخواه است، و I و J ایده‌آل هستند. به صورت مستقیم (با استفاده از تعریف)، تساوی $(I \cup J) = I + J$ را ثابت کنید.

۵- فرض کنید R حلقه‌ای تعویض‌پذیر و یک‌دار است، و I و J ایده‌آل آن هستند. با استفاده از قضیه‌ی **۹.۳.۳**، تساوی $(I \cup J) = I + J$ را اثبات کنید.

۶- دامنه‌ی صحیح R را یک **دامنه‌ی ایده‌آل اصلی** (PID) می‌گوییم، اگر هر ایده‌آل آن اصلی باشد. (برای مثال حلقه‌ی $\mathbb{Z}$ و حلقه‌های $\mathbb{Z}_n$، PID هستند). نشان دهید که هر میدان یک دامنه‌ی ایده‌آل اصلی است.

۷- فرض کنید R حلقه‌ای دلخواه است، و I و J ایده‌آل هستند. به صورت مستقیم (با استفاده از تعریف **۸.۳.۳**) ثابت کنید که

$$IJ = \left\{ \sum_{i=1}^{n} a_i b_i \mid n \in \mathbb{N}, a_i \in I, b_i \in J \right\}$$

۸- فرض کنید R حلقه‌ای دلخواه است، و I و J ایده‌آل هستند. ثابت کنید که $I \cup J$ ایده‌آل است اگر و تنها اگر $I \subseteq J$ یا $J \subseteq I$.

۹- فرض کنید R حلقه‌ای دلخواه است و I، J، و K ایده‌آل باشند. تساوی $I(J+K) = IJ + IK$ را اثبات یا رد کنید.

۱۰- حلقه‌ی ناصفر R را **ساده** می‌گویند اگر ایده‌آلی بجز صفر و خودش نداشته باشد. ثابت کنید که هر حلقه‌ی تعویض‌پذیر و یک‌دار ساده است اگر و تنها اگر میدان باشد.

۱۱- فرض کنید R حلقه‌ای تعویض‌پذیر، و I و J ایده‌آل R است. نشان دهید که

$$(I : J) = \{a \in R \mid aJ \subseteq I\}$$

ایده‌آل R است. این ایده‌آل را **حاصل تقسیم** I بر J می‌نامیم. به ویژه

$$(0 : I) = \{a \in R \mid aI = 0\}$$

را پوچساز I می‌نامیم و معمولاً آن را با $Ann_R I$ نشان می‌دهیم.

۱۲- فرض کنید R حلقه‌ای تعویض‌پذیر و یک‌دار، $I, J, K \trianglelefteq R$، و $\{I_n\}_{n \in \mathbb{N}}$ خانواده‌ای از ایده‌آل‌های R باشد. ثابت کنید که

الف) $I \subseteq (I : J)$.

ب) $((I : J) : K) = (I : JK) = ((I : K) : J)$.

پ) $(\bigcap_{n \in \mathbb{N}} I_n : J) = \bigcap_{n \in \mathbb{N}} (I_n : J$.

ت) $(I : J) = R$ اگر و تنها اگر $J \subseteq I$.

۱۳- (**جالب است**) فرض کنید R حلقه و I ایده‌آل R است. نشان دهید که حلقه‌ی R/I تعویض‌پذیر است اگر و تنها اگر به ازای هر $x, y \in R$، $xy - yx \in I$. (عبارت $xy - yx$ را با $[x, y]$ نشان می‌دهیم و آن را یک **تعویض‌گر** R می‌نامیم. ایده‌آل تولید شده توسط تعویض‌گرهای R را **ایده‌آل تعویض‌گر** R می‌نامیم و با $[R, R]$ نشان می‌دهیم).

دسته‌ی دوم

۱۴- حلقه‌ی R را یک **حلقه‌ی نوتری (آرتینی)** می‌نامیم اگر هر زنجیر صعودی (نزولی) به صورت

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \dots$$
$$(I_1 \supseteq I_2 \supseteq I_3 \supseteq \dots)$$

از ایده‌آل‌های R خاتمه‌پذیر باشد، یعنی، عدد طبیعی n موجود باشد به طوری که برای هر $j \geq n$ داشته باشیم $I_j = I_n$. ثابت کنید

(الف) حلقه‌های $\mathbb{Z}$ و $\mathbb{Z}_n$ نوتری هستند. البته، حلقه‌ی $\mathbb{Z}$ آرتینی نیست (**چرا؟**) و هر حلقه‌ی متناهی نوتری و آرتینی است. **چرا؟**

(ب) هر میدان هم نوتری و هم آرتینی است.

(پ) ثابت کنید که هر دامنه‌ی ایده‌آل اصلی نوتری است. (**راهنمایی**: فرض کنید

$$< a_1 > \subseteq < a_2 > \subseteq < a_3 > \subseteq \ \cdots$$

حال نشان دهید که $\bigcup < a_i >$ ایده‌آلی برابر با یکی از $< a_i >$ها است.)

۱۵- حلقه‌ی تعویض‌پذیر و یک‌دار R را **حلقه‌ی موضعی** می‌گوییم اگر تنها یک ایده‌آل ماکسیمال داشته باشد. ثابت کنید که هر میدان، و هر $\mathbb{Z}_{p^n}$ (p عدد اول) موضعی است.

۱۶- فرض کنید R حلقه‌ای یک‌دار و تعویض‌پذیر است. نشان دهید که ایده‌آل P از R اول است اگر و تنها اگر برای هر دو ایده‌آل I و J از R،

$$I \cap J \subseteq P \Rightarrow I \subseteq P \text{ یا } J \subseteq P$$

۱۷- فرض کنید R حلقه‌ای تعویض‌پذیر است. نشان دهید که ایده‌آل سره‌ی I از حلقه‌ی R اول است اگر و تنها اگر برای هر دو ایده‌آل J و K،

$$JK \subseteq I \Rightarrow J \subseteq I \text{ یا } K \subseteq I$$

۱۸- فرض کنید R حلقه‌ای یک‌دار و تعویض‌پذیر است. نشان دهید که اگر هر ایده‌آل سره‌ی R اول باشد، آنگاه R میدان است.

۱۹- فرض کنید R حلقه‌ای یک‌دار و تعویض‌پذیر و I ایده‌آل R است. نشان دهید که **رادیکال** I با تعریف

$$\sqrt{I} = \{x \in R \mid \exists n \in \mathbb{N}, x^n \in I\}$$

ایده‌آل R است. ایده‌آل $\sqrt{0} = \{x \in R \mid \exists n \in \mathbb{N}, x^n = 0\}$ را **ایده‌آل پوچ** R می‌نامیم. همچنین، نشان دهید که

(الف) $I \subseteq \sqrt{I}$

(ب) $\sqrt{\sqrt{I}} = \sqrt{I}$.

(پ) $\sqrt{\sqrt{I} + \sqrt{J}} = \sqrt{I + J}$.

(ت) $\sqrt{IJ} = \sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$.

(ث) اگر ایده‌آل I اول باشد، آنگاه $\sqrt{I} = I$.

۲۰- فرض کنید M ایده‌آل سره‌ای از حلقه‌ی تعویض‌پذیر و یک‌دار R باشد. ثابت کنید که M ماکسیمال است اگر و تنها اگر برای هر $a \notin M$، $M + (a) = R$، اگر و تنها اگر برای هر $a \notin M$، عضو $b \in R$ وجود داشته باشد به طوری که $1 - ab \in M$، اگر و تنها اگر برای هر ایده‌آل I از R، داشته باشیم $I \subseteq M$ یا $M + I = R$.

۲۰- نشان دهید که اگر M_1 و M_2 دو ایده‌آل ماکسیمال و متمایز از حلقه‌ی تعویض‌پذیر و یک‌دار R باشند، آنگاه

$$M_1 M_2 = M_1 \cap M_2$$

۲۱- فرض کنید R حلقه‌ای تعویض‌پذیر و یک‌دار است. ثابت کنید که هر ایده‌آل سره‌ی R در یک ایده‌آل ماکسیمال قرار دارد. (**راهنمایی**: لم زورن را به کار ببرید.)

۲۲- فرض کنید R حلقه‌ای تعویض‌پذیر و یک‌دار باشد. نشان دهید که $r \in R$ وارون‌ناپذیر است اگر و تنها اگر r عضو ایده‌آلی ماکسیمال باشد.

۲۳- فرض کنید که R حلقه‌ای تعویض‌پذیر و یک‌دار است. ثابت کنید که

(الف) اگر P_1 و P_2 دو ایده‌آل اول R باشند به طوری که $P_1 \not\subseteq P_2$ و $P_2 \not\subseteq P_1$، آنگاه $P = P_1 \cap P_2$ اول نیست.

(ب) اگر $\{P_i\}_{i \in I}$ زنجیری از ایده‌آل‌های اول R باشد، آنگاه $\bigcap P_i$ و $\bigcup P_i$ ایده‌آل‌هایی اول هستند.

۲۴- ثابت کنید که در هر حلقه‌ی تعویض‌پذیر و یک‌دار متناهی، هر ایده‌آل اول یک ایده‌آل ماکسیمال است.

۲۵-با ارائه مثال، نشان دهید که خاصیت تعدی برای ایده‌آل‌ها برقرار نیست. یعنی،

$$I \trianglelefteq J \trianglelefteq R \not\Rightarrow I \trianglelefteq R$$

۲۶- فرض کنید R حلقه‌ای تعویض‌پذیر و یک‌دار است. فرض کنید که I یک ایده‌آل R و P یک ایده‌آل اول I باشد. نشان دهید که P ایده‌آل R است.

۲۷-فرض کنید R حلقه‌ای یک‌دار است. ثابت کنید که R هیچ ایده‌آل راست (یا چپ) سره ندارد اگر و تنها اگر R یک حلقه‌ی بخشی باشد. زیرگروه I از $(R;+)$ را یک **ایده‌آل راست** (یا **چپ**) می‌گوییم اگر برای هر $x \in I$ و هر $r \in R$، $xr \in I$ (یا $rx \in I$).

۴.۳ همریختی و قضیه‌های یک‌ریختی حلقه‌ها

در این بخش، قضیه‌ی اساسی همریختی‌ها و قضیه‌های یکریختی را، که برای همه‌ی دستگاه‌های جبری در فصل ۱ و برای گروه‌ها در فصل۲ دیدیم، یک بار دیگر برای حلقه‌ها به اختصار مطالعه می‌کنیم.

با توجه به تعریف کلی همریختی بین دستگاه‌های جبری، همریختی بین دو دستگاه جبری تابعی است که همه‌ی عمل‌های ساختار جبری دامنه را **حفظ** می‌کند. از این رو، تعریف همریختی حلقه‌ها به صورت زیر است.

۱.۴.۳ تعریف. فرض کنیم $(R;+,\cdot)$ و $(S;+,\cdot)$ حلقه باشند. تابع $f: R \to S$ را **همریختی حلقه‌ای** می‌گوییم اگر برای هر $a,b \in R$،

$$f(a+b) = f(a) + f(b) \qquad , \qquad f(ab) = f(a)f(b)$$

مطابق معمول، همریختی دوسویی را **یک‌ریختی**، همریختی یک به یک را **تک‌ریختی**، و همریختی پوشا را **بروریختی** نیز می‌نامیم.

۲.۴.۳ بحث در کلاس

۱- با توجه به ویژگی‌های همریختی گروه‌ها که در فصل۲ بیان شد، از ویژگی حفظ عمل جمع در تعریف همریختی حلقه‌ها، نتیجه می‌گیریم که اگر f یک همریختی حلقه‌ای باشد، آنگاه یک همریختی از گروه جمعی $(R;+)$ به گروه جمعی $(S;+)$ است و در نتیجه داریم

$$f(0)=0,$$
$$f(-a)=-f(a)$$
$$f(a-b)=f(a)-f(b)$$

ولی اگر حلقه‌های R و S یک‌دار باشند، لزومی ندارد که f به خودی خود حافظ ۱ باشد. (همریختی صفر را در نظر بگیرید). البته اگر $f:R\to S$ یک همریختی **پوشا** بین حلقه‌های یک‌دار باشد، آنگاه $f(1_R)=1_S$ (**چطور؟**). این نکته را نیز متذکر می‌شویم که ریاضی‌دانانی که تنها با حلقه‌های یک‌دار سروکار دارند، شرط $f(1_R)=1_S$ را نیز به تعریف همریختی بین حلقه‌ها می‌افزایند.

۲- فرض کنیم $f:R\to S$ یک همریختی حلقه‌ای باشد. به راحتی می‌توانید نشان دهید که

(الف) برای هر $a\in R$ و $n\in\mathbb{Z}$، $f(n\cdot a)=n\cdot f(a)$. برای مثال، اگر $n>0$ آنگاه

$$f(n\cdot a)=f(a+\cdots+a)=f(a)+\cdots+f(a)=n\cdot f(a)$$

(ب) برای هر $a\in R$ و $n\in\mathbb{N}$، $f(a^n)=(f(a))^n$.

۳- فرض کنیم R و S حلقه باشند و $S\subseteq R$. در این صورت تابع **شمولی** $i:S\to R$ همریختی است اگر و تنها اگر S **زیرحلقه‌ی** R باشد. این مطلب از محک زیر حلقه.

۴- فرض کنیم $(R;+,.)$ و $(R';+,.)$ حلقه باشند. تابع ثابت صفر $f:R\to R'$ با تعریف $f(x)=0$ یک همریختی حلقه‌ای است.

۵- در تعریف همریختی، اگر فرض کنیم حلقه‌ها یک‌دار هستند، و شرط $f(1)=1$ را اضافه کنیم، آنگاه برای هر عضو یکال $u\in R$، $f(u^{-1})=(f(u))^{-1}$. در واقع، برای هر $n\in\mathbb{Z}$، $f(u^n)=(f(u))^n$.

۶- تابع $f:\mathbb{Z}\to\mathbb{Z}_n$ با تعریف (باقی‌مانده‌ی x بر n) $f(x)=$ یک همریختی حلقه‌ای است.

۷- فرض کنیم $(R;+,\cdot)$ حلقه‌ای یک‌دار باشد. تابع $f:\mathbb{Z}\to R$ با تعریف $f(k)=k\cdot 1=1+\cdots+1$ یک همریختی حلقه‌ای است. **چطور؟** آیا این همریختی برای هر حلقه‌ی یک‌دار R، یک به یک است؟ (حلقه‌ی $\mathbb{Z}_n$ را در نظر بگیرید!)

۸- تابع $f:M_n(\mathbb{R})\to\mathbb{R}$ با تعریف $f(A)=\det A$ حافظ ضرب است، ولی جمع را حفظ نمی‌کند. پس همریختی نیم‌گروهی است ولی همریختی حلقه‌ای نیست.

۹- توجه می‌کنیم که، اگرچه تابع $f:\mathbb{Z}\to\mathbb{Z}$ با تعریف، برای مثال، $f(n)=2n$ عمل جمع را حفظ می‌کند، و در نتیجه همریختی گروهی است، ولی ضرب را حفظ نمی‌کند، و بنابراین همریختی حلقه‌ای نیست! حال نشان دهید که تنها همریختی‌های حلقه‌ای $f:\mathbb{Z}\to\mathbb{Z}$، همریختی ثابت صفر و

همریختی همانی هستند! (توجه کنید که اگر، برای مثال، $f(m)\neq 0$ ، آنگاه از $f(m)=f(m1)=f(m)f(1)$ نتیجه می شود که $f(1)=1$).

قضیه‌ی زیر همتای قضیه‌های ۳.۵.۲ و ۱.۹.۲ در گروه‌ها است.

۳.۴.۳ قضیه. فرض کنیم تابع $f:R\to R'$ یک همریختی حلقه‌ای باشد. در این صورت:

۱- اگر S زیرحلقه‌ی R باشد، آنگاه $f(S)$ زیرحلقه‌ی R' است.

۲- اگر I ایدآل R باشد، آنگاه $f(I)$ ایده‌آل $\operatorname{Im} f$ است.

۳- اگر S' زیرحلقه‌ی R' باشد، آنگاه $\overleftarrow{f}(S')=f^{-1}(S')$ زیرحلقه‌ی R است.

۴- اگر J ایده‌آل R' باشد، آنگاه $\overleftarrow{f}(J)=f^{-1}(J)$ ایده‌آل R است.

۵- هسته‌ی f ، یعنی $f^{-1}(0)=\{x\in R\mid f(x)=0\}$ ، ایده‌آل R است.

اثبات. احکام بالا با استفاده از تعریف زیرحلقه و ایده‌آل به سادگی اثبات می‌شوند. برای نمونه، ۲ و ۴ را اثبات می‌کنیم.

۲- ابتدا داریم $0=f(0)\in f(I)$، زیرا $0\in I$. همچنین اگر $f(a),f(b)\in f(I)$ که در آن $a,b\in I$ آنگاه $a-b\in I$ و در نتیجه $f(a)-f(b)=f(a-b)\in f(I)$. در پایان، برای $f(a)\in f(I)$ که در آن $a\in I$ و $f(b)\in \operatorname{Im} f$ داریم $f(a)f(b)=f(ab)\in f(I)$ زیرا $ab\in I$. چرا؟ به همین ترتیب، $f(b)f(a)\in f(I)$.

۴- ابتدا داریم $0\in f^{-1}(J)$، زیرا $f(0)=0\in J$. همچنین اگر $a,b\in f^{-1}(J)$ آنگاه $f(a),f(b)\in J$ و در نتیجه $f(a-b)=f(a)-f(b)\in J$ ، پس $a-b\in f^{-1}(J)$. در پایان، اگر $a\in f^{-1}(J)$ و $r\in R$ آنگاه $f(a)\in J$ و در نتیجه $f(ra)=f(r)f(a)\in J$. پس $ra\in f^{-1}(J)$. به همین صورت، $ar\in f^{-1}(J)$.

قبل از اینکه به قضیه‌های یکریختی بپردازیم، حاصل‌ضرب حلقه‌ها و همریختی‌های تصویری و تزریقی را می‌آوریم. روشن است که ضرب دکارتی حلقه‌ها مانند ضرب گروه‌ها و دستگاه‌های کلی جبری به صورت زیر تعریف می‌شود.

۴.۴.۳ قضیه و تعریف. فرض کنیم R_1 و R_2 حلقه باشند. در این صورت حاصل‌ضرب دکارتی $R_1\times R_2$ همراه با اعمال مؤلفه‌ای جمع و ضرب به صورت

$$(a,b)+(c,d)=(a+c,b+d)$$
$$(a,b)(c,d)=(ac,bd)$$

تشکیل یک حلقه می‌دهد که آن را **حاصل ضرب** R_1 در R_2 می‌نامیم.

۵.۴.۳ بحث در کلاس

(الف) با توجه به تعریف عمل ضرب روی حلقه‌ی حاصل‌ضرب، روشن است که اگر حلقه‌های R_1 و R_2 یک‌دار باشند، آنگاه $R_1 \times R_2$ نیز یک‌دار است. در واقع، $(1_{R_1}, 1_{R_2})$ همانی (یکه‌ی) $R_1 \times R_2$ است.

ب) با توجه به تعریف عمل ضرب روی حلقه‌ی حاصل‌ضرب، روشن است که اگر حلقه‌های R_1 و R_2 تعویض‌پذیر باشند، آنگاه حلقه‌ی $R_1 \times R_2$ نیز تعویض‌پذیر است. برعکس، اگر حلقه‌های R_1 و R_2 یکدار باشند و $R_1 \times R_2$ تعویض‌پذیر باشد، آنگاه حلقه‌های R_1 و R_2 تعویض‌پذیرند.

پ) فرض کنیم R_1 و R_2 حلقه باشند. در این صورت توابع تصویر

$$R_1 \xleftarrow{p_1} R_1 \times R_2 \xrightarrow{p_2} R_2$$

که در آن $p_1(x,y)=x$ و $p_2(x,y)=y$، و توابع تزریق

$$R_1 \xrightarrow{i_1} R_1 \times R_2 \xleftarrow{i_2} R_2$$

که در آن $i_1(x)=(x,0)$ و $i_2(y)=(0,y)$، همریختی حلقه‌ای هستند. **چرا؟**. به علاوه، ویژگی جهانی ضرب برای ضرب دکارتی حلقه‌ها برقرار است (تمرین ۲ را ببینید.).

۶.۴.۳ بحث در کلاس دیدیم که اگرچه حلقه‌ی $\mathbb{Z}$ دامنه‌ی صحیح است، زیرحلقه‌ی آن $2\mathbb{Z}$ دامنه نیست (شامل ۱ نیست)؛ حاصل‌ضرب $\mathbb{Z}\times\mathbb{Z}$ دامنه نیست، زیرا $(1,0)(0,1)=(0,0)$؛ خارج قسمت $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$، برای عدد غیر اول $n>2$، دامنه‌ی صحیح نیست. هر یک از این سه دلیل به تنهایی بیان می‌کند که دسته‌ی دامنه‌های صحیح یک **واریته نیست** (**قضیه‌ی بیرخوف** را ببینید)، و در نتیجه این دسته را نمی‌توان با دسته‌ای از **اتحادها** مشخص کرد. این مطلب در مورد دسته‌ی میدان‌ها نیز درست است. چطور؟

حال قضیه‌های یک‌ریختی را به اختصار می‌آوریم. ابتدا یادآوری می‌کنیم که با توجه به بند ۵ قضیه‌ی ۳.۴.۳، هسته‌ی هر همریختی چون f ایده‌آلی از دامنه‌ی همریختی است. مشابه گروه‌ها، از نماد $Kerf$ یا K_f برای نمایش هسته‌ی f استفاده می‌کنیم.

۷.۴.۳ قضیه(اساسی همریختی). اگر $f: R \to R'$ همریختی حلقه‌ای باشد و $K = Kerf$، آنگاه $R/K \cong f(R)$، و اگر f پوشا باشد، $R/K \cong R'$.

اثبات. مشابه اثبات قضیه‌ی اساسی توابع در فصل مقدمه و اثبات قضیه‌ی اساسی همریختی در گروه‌ها، ضابطه‌ی $[x] \mapsto f(x)$، یا در نمادگذاری متداول با هم‌مجموعه‌ها، $\bar{f}(x+K) = f(x)$، قضیه را اثبات می‌کند. اگرچه روش کار را آموخته‌اید و نیازی به ارائه‌ی مجدد آن نیست، ولی اثبات را بدون توضیح می‌آوریم (مراحل اثبات زیر را توضیح دهید):

خوش‌تعریفی و یک به یک بودن $\bar{f}$:

$$\begin{aligned}(x+K)=(y+K) &\Leftrightarrow x-y \in K \Leftrightarrow f(x-y)=0\\ &\Leftrightarrow f(x)-f(y)=0 \Leftrightarrow f(x)=f(y)\\ &\Leftrightarrow \bar{f}(x+K)=\bar{f}(y+K)\end{aligned}$$

حفظ عمل‌های جمع و ضرب:

$$\begin{aligned}\bar{f}[(x+K)+(y+K)] &= \bar{f}[(x+y)+K] = f(x+y)\\ &= f(x)+f(y) = \bar{f}(x+K)+\bar{f}(y+K)\end{aligned}$$

$$\begin{aligned}\bar{f}[(x+K)(y+K)] &= \bar{f}(xy+K) = f(xy)\\ &= f(x)f(y) = \bar{f}(x+K)\bar{f}(y+K)\end{aligned}$$

۸.۴.۳ بحث در کلاس. قضیه‌ی اساسی همریختی را برای همریختی $f: \mathbb{Z} \to \mathbb{Z}_n$ با تعریف $f(k) =$ (باقی مانده‌ی تقسیم k بر n) به کار ببرید و نتیجه بگیرید که، به عنوان دو حلقه نیز، $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$.

۹.۴.۳ قضیه(ی دوم یکریختی) فرض کنیم I و J ایده‌آل‌هایی از حلقه‌ی R باشند. در این صورت، $\dfrac{I+J}{J} \cong \dfrac{I}{I \cap J}$

اثبات. این قضیه را می‌توانید، مشابه قضیه‌ی دوم یک‌ریختی گروه‌ها، به روش زیر اثبات کنید. ابتدا نشان دهید که ضابطه‌ی

$$f: I+J \to \frac{I}{I\cap J}$$
$$x+y \mapsto x+(I\cap J)$$

تابعی خوش‌تعریف، پوشا، و همریختی است. توجه کنید که خوش‌تعریفی به صورت زیر اثبات می‌شود (مراحل اثبات را توضیح دهید):

$$\begin{aligned} x+y=x'+y' &\Rightarrow x-x'=y'-y \\ &\Rightarrow x-x' \in I\cap J \\ &\Rightarrow x+(I\cap J)=x'+(I\cap J) \\ &\Rightarrow f(x+y)=f(x'+y') \end{aligned}$$

سپس توجه کنید که $Kerf = J$:

$$\begin{aligned} Kerf &= \{x+y \mid x\in I, y\in J, f(x+y)=0_{I/I\cap J}\} \\ &= \{x+y \mid x+I\cap J = I\cap J\} \\ &= \{x+y \mid x\in I\cap J\} = J \end{aligned}$$

تساوی آخر را اثبات کنید. حال قضیه‌ی اساسی ۷.۴.۳ را به کار ببرید.

۱۰.۴.۳ قضیه(سوم یکریختی). فرض کنیم I و J ایده‌آل‌هایی از حلقه‌ی R باشند به طوری که $I \subseteq J$. در این صورت،

$$\frac{R/I}{J/I} \cong R/J$$

اثبات. ابتدا توجه می‌کنیم که، بنابر قضیه‌ی **تناظر**، J/I ایده‌آل R/I است. حال قضیه را می‌-توانید، برای مثال، مشابه‌ی اثبات قضیه‌ی سوم یک‌ریختی گروه ها و با در نظر گرفتن تابع زیر، اثبات کنید:

$$\begin{aligned} f : R/I &\to R/J \\ x+I &\mapsto x+J \end{aligned}$$

توجه کنید که خوش‌تعریفی f به صورت زیر اثبات می‌شود:

$$\begin{aligned} x+I = y+I &\Rightarrow x-y \in I \subseteq J \Rightarrow x-y \in J \\ &\Rightarrow x+J = y+J \Rightarrow f(x+I) = f(y+I) \end{aligned}$$

سپس نشان دهید که $Kerf = J/I$ و قضیه‌ی اساسی **۷.۴.۳** را به کار ببرید.

۱۱.۴.۳ میدان کسرها. این بخش را با معرفی مفهوم مهم دیگری به پایان می‌بریم. در بخش ۷.۱ و در **۱۳.۸.۲** گفتیم که گاهی لازم است برای به دست آوردن بزرگ‌ترین دستگاه جبری، با ویژگی‌ای خاص، از دستگاه جبری داده شده‌ی A، دستگاه جبری A را بر کوچک‌ترین رابطه‌ی همنهشتی $\sim$ که ما را به مقصود می‌رساند، تقسیم (یعنی افراز) کنیم. در این صورت، همریختی پوشای $\gamma : A \twoheadrightarrow A/\sim$ را داریم. گاهی نیز لازم است دستگاه جبری A را درون کوچک‌ترین دستگاهی جبری چون $\hat{A}$ با ویژگی‌ای خاص قرار دهیم. در این صورت، همریختی یک به یک $A \rightarrowtail \hat{A}$ را داریم. (شاید تشبیه دقیقی نباشد که بگوییم مانند این است که مثلث را برون دایره‌ی محاطی‌اش، یا مثلث را درون دایره‌ی محیطی‌اش، قرار دهیم!). اجازه بدهید، برای ایجاد انگیزه‌ی بیش‌تر، فرض کنیم، برای مثال، می‌خواهیم جواب‌های معادله‌ی $2x^2 - 3x - 2 = 0$ را در دامنه‌ی صحیح $\mathbb{Z}$ به دست آوریم. ممکن است ابزار لازم در $\mathbb{Z}$ وجود نداشته باشد یا اینکه ابزار موجود در میدان‌های $\mathbb{Q}$ یا $\mathbb{R}$، که شامل $\mathbb{Z}$ هستند، مناسب تر باشد. برای مثال، داریم

$$x = \frac{3 \pm \sqrt{9+16}}{4} = 2 \quad \text{یا} \quad -\frac{1}{2}$$

پس، جواب این معادله در $\mathbb{Z}$ برابر با ۲ است. در تمرین **۱۰** بخش **۲.۳** دیدیم که $\mathbb{Q}$ کوچک‌ترین میدان شامل دامنه‌ی صحیح $\mathbb{Z}$ است. در زیر می‌خواهیم این واقعیت را برای هر دامنه‌ی صحیح دلخواه D تعمیم دهیم. یعنی، می‌خواهیم **کوچک‌ترین میدان شامل** D (در واقع شامل نسخه‌ای یک‌ریخت با D) بسازیم.

اثبات ساده‌ی بند **۲** قضیه‌ی زیر دقیقاً همتای بند **۱** و به ویژه بند **۲** بحث **۷.۱.۱** است. (تمرین **م.۱-(۶)** را نیز ببینید).

۱۲.۴.۳ قضیه فرض کنیم که D دامنه‌ی صحیح است و

$$\mathcal{D} = D \times D^* = \{(a,b) \mid a,b \in D, b \neq 0\}$$

در این صورت،

۱- رابطه‌ی زیر روی $\mathcal{D}$ هم‌ارزی است:

$$(a,b) \sim (c,d) \Leftrightarrow ad = bc$$

۲- عمل‌های زیر روی مجموعه‌ی

$$F_D = \mathcal{D}/\sim = (D \times D^*)/\sim = \{[(a,b)] \mid (a,b) \in D \times D^*\}$$

خوش تعریف هستند:

$$[(a,b)] + [(c,d)] = [(ad + bc, bd)]$$
$$[(a,b)][(c,d)] = [(ac, bd)]$$

۳- مجموعه‌ی F_D همراه با عمل‌های بند ۲ میدان است.

۴- $D_1 = \{[a,1] \mid a \in D\}$ نسخه‌ی D در میدان F_D است، یعنی $D \cong D_1$.

۵- F_D کوچک‌ترین میدان با ویژگی بند ۴ است. به این معنی که اگر E میدانی شامل (نسخه‌ای یک‌ریخت با) دامنه‌ی صحیح D باشد، آنگاه E شامل (نسخه‌ای یک‌ریخت با) میدان F_D است.

اثبات اثبات همه‌ی بندهای این قضیه بسیار ساده و سرراست است. کافی است ترسی از نمایش **کروشه - پرانتز** $[(a,b)]$ برای عضوهای F_D نداشته باشیم و آن را در ذهن خود همتای کسر a/b در اعداد گویای $\mathbb{Q}$ در نظر بگیریم.

۱- ابتدا توجه کنید که تعریف رابطه‌ی هم‌ارزی بالا مشابه تعریف تساوی دو عدد کسری (گویا) یعنی

$$\frac{a}{b} = \frac{c}{d} \Leftrightarrow ad = bc$$

است (**این طور نیست؟**). اثبات هم‌ارزی بودن $\sim$ نیز ساده است (بندهای ۱ و به ویژه ۲ بحث ۷.۱.۱ را نیز ببینید). مراحل اثبات متعدی بودن $\sim$ را توضیح دهید:

$$\begin{aligned}(a,b)\sim(c,d)\sim(e,f) &\Rightarrow ad=bc \,\&\, cf=de\\ &\Rightarrow adf=bcf=bde\\ &\Rightarrow af=be\\ &\Rightarrow (a,b)\sim(e,f)\end{aligned}$$

۲- عمل جمع در F_D همتای عمل جمع اعداد کسری، یعنی

$$\frac{a}{b}+\frac{c}{d}=\frac{ad+bc}{bd}$$

است. و اثبات خوش‌تعریفی آن (با نماد کروشه-پرانتز) نیز سر راست است. ابتدا توجه می‌کنیم که این عمل بسته است. زیرا

$$b,d\neq 0\Rightarrow bd\neq 0$$

حال باید نشان دهیم که

$$\begin{cases}[(a,b)]=[(a',b')]\\ [(c,d)]=[(c',d')]\end{cases}\Rightarrow\quad [(a,b)]+[(c,d)]=[(a',b')]+[(c',d')]$$

$$\begin{aligned}&(\Leftrightarrow\quad [(ad+bc,bd)]=[(a'd'+b'c',b'd')]\\ &\Leftrightarrow (ad+bc)b'd'=(bd)(a'd'+b'c'))\end{aligned}$$

مرحله آخر زیر را توضیح دهید:

$$\begin{cases}[(a,b)]=[(a',b')]\\ [(c,d)]=[(c',d')]\end{cases}\Rightarrow\quad\begin{cases}(a,b)\sim(a',b')\\ (c,d)\sim(c',d')\end{cases}$$

$$\Rightarrow\quad\begin{cases}ab'=ba'\\ cd'=dc'\end{cases}$$

$$\Rightarrow ?\quad (ad+bc)b'd'=(bd)(a'd'+b'c')$$

لذت اثبات ساده‌ی خوش‌تعریفی عمل ضرب را از شما خوبان نمی‌گیریم!

۳- اثبات میدان بودن F_D سر راست ولی پر زحمت است. برخی از شرایط را اثبات می‌کنیم و لذت انجام برخی دیگر را از شما نمی‌گیریم. شرکت‌پذیری هر دو عمل جمع وضرب، از ویژگی‌های جمع و ضرب در دامنه‌ی D حاصل می‌شود (**چطور؟**). عضو $[(0,1)]$ نقش عضو خنثی را نسبت به عمل جمع ایفا می‌کند:

$$[(a,b)]+[(0,1)]=[(a\cdot 1+b\cdot 0,b\cdot 1)]=[(a,b)]$$

قرینه‌ی هر عضو دلخواه $[(a,b)]$ برابر با $[(-a,b)]=[(a,-b)]$ است:

$$[(a,b)]+[(-a,b)]=[(ab+b(-a),b^2)]=[(0,b^2)]=[(0,1)]$$

تساوی آخر از این مطلب حاصل می شود که، برای هر $x\neq 0$ داریم

$$[(0,1)]=[(0,x)]\Leftrightarrow (0,1)\sim(0,x)\Leftrightarrow 0\cdot x=1\cdot 0\Leftrightarrow 0=0$$

تعویض‌پذیری جمع و توزیع‌پذیری ضرب روی جمع نیز به راحتی از برقراری ویژگی‌های نظیر در دامنه‌ی D حاصل می‌شود (جالب است، **اثبات کنید**). در پایان، کافی است به روشنی ببینیم که $[(1,1)]$ عضو همانی F_D نسبت به عمل ضرب است، و هر عضو ناصفر چون $[(a,b)]$ دارای وارون ضربی $[(b,a)]$ است. برای نمونه، داریم

$$[(a,b)][(b,a)]=[(aa,bb)]=[(1,1)]$$

توجه کنید که، برای هر $x\neq 0$، داریم $[(x,x)]=\{(1,1)\}$.

۴- برای اثبات این بند، نشان می‌دهیم که تابع

$$\begin{aligned} i:D &\rightarrowtail F_D \\ a &\mapsto [(a,1)] \end{aligned}$$

(که همتای $i:\mathbb{Z}\to\mathbb{Q}$ با تعریف $i(m)=m=\frac{m}{1}$ است) یک همریختی یک به یک با نگاره‌ی D_1 است (مراحل زیر را توضیح دهید):

$$\begin{aligned} i(ab)&=[(ab,1)]=[(a,1)][(b,1)]=i(a)i(b) \\ i(a+b)&=[(a+b,1)]=[(a,1)]+[(b,1)]=i(a)+i(b) \end{aligned}$$

۵- این بند **خیلی جالب** است. حکم **۵** به این معنی است که برای هر میدان E که شامل D باشد، یک همریختی یک به یک $\bar{j}:F_D\rightarrowtail E$ وجود دارد. تعریف $\bar{j}$ که در زیر می‌آید، بسیار طبیعی است. **این طور نیست؟** در واقع همان تصور نمایش کروشه – پرانتز به صورت طبیعی کسر است:

$$\bar{j}([(a,b)])=ab^{-1}\qquad (\equiv\frac{a}{b})$$

حال باید نشان دهیم که $\bar{j}$ همریختی یک به یک است، که آن نیز در واقع به این معنی است که عمل‌های جمع و ضرب با نمایش کروشه – پرانتز اساساً همان عمل‌های جمع و ضرب با نمایش کسری است. برای نمونه داریم

$$\begin{aligned}\bar{j}([(a,b)]+[(c,d)]) &= \bar{j}([(ad+bc,bd)] \\ &= (ad+bc)(bd)^{-1} \qquad (\equiv \frac{ad+bc}{bd} \\ &= add^{-1}b^{-1}+bcd^{-1}b^{-1} \qquad (\equiv \frac{ad}{bd}+\frac{bc}{bd}) \\ &= ab^{-1}+cd^{-1} \qquad (\equiv \frac{a}{b}+\frac{c}{d}) \\ &\bar{j}([(a,b)])+\bar{j}([(c,d)])\end{aligned}$$

اثبات ساده‌ی حفظ عمل ضرب و یک به یک بودن $\bar{j}$ را به عهده‌ی شما می‌گذاریم!

۱۳.۴.۳ بحث در کلاس. فرض کنیم D یک دامنه‌ی صحیح باشد.

۱- اگر در هر میدان بنویسیم $ab^{-1}=a/b$ و به دلیل یکریخت بودن D با D_1، و برای سادگی، $[(a,1)]$ را با $a/1=a$ نمایش دهیم، آنگاه داریم

$$[(a,b)]=[(a,1)][(1,b)]=[(a,1)][(b,1)]^{-1}=\frac{[(a,1)]}{[(b,1)]}=\frac{a}{b}$$

یعنی (مشابه ارتباط $\mathbb{Q}$ با $\mathbb{Z}$) هر عضو F_D به صورت **کسری** از عضوهای D **نمایش** داده می‌شود. از این رو، F_D را **میدان کسرهای** D می‌نامیم و آن را با $Q(D)$ نیز نشان می‌دهیم (که در آن Q حرف اول *Quotient* به معنی **کسر** است).

۲- حالت کلی‌تر حکم **۵** این است که برای هر میدان E و هر همریختی یک به یک $j:D\rightarrowtail E$ ، یک همریختی یک به یک $\bar{j}:F_D\rightarrowtail E$ وجود دارد به طوری که $\bar{j}\circ i=j$ ، یعنی مثلث زیر تعویض‌پذیر است:

$$\begin{tikzcd} D \arrow[r, tail, "i"] \arrow[dr, "j"'] & F_D \arrow[d, "\bar{j}"] \\ & E \end{tikzcd}$$

در این حالت $\bar{j}$ به صورت $\bar{j}([(a,b)])=i(a)i(b)^{-1}$ تعریف می‌شود، که از نظر نمادگذاری قدری پیچیده‌تر از $\bar{j}([(a,b)])=ab^{-1}$ است، و اثبات‌ها نیز از لحاظ نمادگذاری پیچیده‌تر می‌شوند. از این رو، در بالا حالت ساده‌تری را آوردیم که در آن همریختی یک به یک j همریختی شمولی باشد. به هر حال، تفاوت تابع یک به یک با تابع شمولی اساساً چیزی جز در نمادگذاری نگاره‌ها نیست، **هست؟**

تمرین ۴.۳

۱- فرض کنید R حلقه‌ای یک‌دار است.

(الف) ثابت کنید که مشخصه‌ی R صفر است اگر و تنها اگر تابع $f:\mathbb{Z}\to R$ با تعریف $f(k)=k\cdot 1$ تک‌ریختی باشد.

(ب) ثابت کنید که مشخصه‌ی R برابر با n است اگر و تنها اگر تابع $f:\mathbb{Z}_n\to R$ با تعریف $f(k)=k\cdot \bar{1}$ تک‌ریختی باشد.

۲- فرض کنید I و J ایده‌آل‌هایی از حلقه‌ی R باشند. با استفاده از قضیه‌های یک‌ریختی حلقه‌ها، نشان دهید که اگر R/I و R/J متناهی باشند، آنگاه $R/I\cap J$ نیز متناهی است.

۳- ثابت کنید که حلقه‌های $2\mathbb{Z}$ و $3\mathbb{Z}$ یک‌ریخت نیستند.

۴- فرض کنید R حلقه‌ای دلخواه و $a\in R$ وارون‌پذیر باشد. ، ثابت کنید که تابع $\rho_a:R\to R$ با تعریف $\rho_a(x)=a^{-1}xa$ یک یک‌ریختی حلقه‌ای است.

۵- فرض کنید R حلقه‌ای یک‌دار و D دامنه‌ی صحیح باشد. فرض کنید که 1_R و 1_D، به ترتیب، همانی ضربی R و D باشند. ثابت کنید برای هر همریختی ناصفر $f:R\to D$ ، داریم $f(1_R)=1_D$.

۶- فرض کنید $f:R\to R'$ یک همریختی حلقه‌ای باشد. ثابت کنید که

(الف) $f(Z(R))\subseteq Z(f(R))$.

(ب) اگر $CharR=m\neq 0$، آنگاه $Char\ f(R)\leq m$.

۷- فرض کنید F یک میدان است. نشان دهید که هر همریختی حلقه‌ای **ناصفر** با دامنه‌ی F یک به یک است. نتیجه بگیرید که هر همریختی ناصفر $F\to F$ یک‌ریختی است.

۸- فرض کنید $f:R\to S$ یک همریختی حلقه‌ای پوشا باشد. اگر I و J ایده‌آل‌هایی از حلقه‌ی R و U و V ایده‌آل‌هایی از حلقه‌ی S باشند. ثابت کنید که

(الف) $f(I+J)=f(I)+f(J)$.

ب) $f(IJ)=f(I)f(J)$.

پ) $f^{-1}(U+V)=f^{-1}(U)+f^{-1}(V)$.

ت) $f^{-1}(UV)\supseteq f^{-1}(U)f^{-1}(V)$ و مثالی بیابید که تساوی برقرار نباشد.

۹- دامنه‌ی صحیح بودن یا نبودن $\mathbb{Z}_2\times\mathbb{Z}_3$ و $\mathbb{Z}\times\mathbb{Z}_4$ را تعیین کنید.

۱۰- نشان دهید که حلقه‌های $\mathbb{Z}$ و $\mathbb{Z}\times\mathbb{Z}$ یک‌ریخت نیستند.

۱۱- ایده‌آل‌های حلقه‌ی $\mathbb{Z}\times\mathbb{Z}$ را تعیین کنید.

۱۲- نشان دهید که دسته‌ی میدان‌ها یک واریته نیست.

۱۳- ثابت کنید که $\mathbb{Q}$ میدان کسرهای $\mathbb{Z}$ است. میدان کسرهای $\mathbb{Q}$ چیست؟

۱۴- ثابت کنید که $\mathbb{Q}[\sqrt{2}]$ میدان کسرهای $\mathbb{Z}[\sqrt{2}]$ است.

۱۵- نشان دهید که رابطه‌ی $\sim$ مذکور در قضیه‌ی **۱۲.۴.۳**، برای حلقه‌ی $D=\mathbb{Z}_4$، که دامنه‌ی اصلی نیست، هم‌ارزی نیست.

۱۶- نشان دهید که هر میدان با مشخصه‌ی صفر، دارای زیرمیدانی یک‌ریخت با $\mathbb{Q}$ است.

۱۷- ثابت کنید که هر دامنه‌ی صحیح و میدان کسرهای نظیرش دارای یک مشخصه هستند.

دسته‌ی دوم

۱۹- نشان دهید که ویژگی جهانی ضرب برای ضرب دکارتی حلقه‌ها برقرار است.

۲۰- نشان دهید که زیرحلقه‌ی S از $M_2(\mathbb{R})$ که در تمرین **۲۵** بخش **۱.۳** معرفی شده، با حلقه‌ی $\mathbb{C}$ یک‌ریخت است. همچنین، زیرحلقه‌ی T از S (در همان تمرین) با $\mathbb{R}$ یک‌ریخت است.

۲۱- فرض کنید R حلقه‌ای یک‌دار و تعویض‌پذیر با مشخصه‌ی عدد اول p است. ثابت کنید که تابع $\varphi:R\to R$ با تعریف $\varphi(x)=x^p$ همریختی حلقه‌ای است.

۲۲- فرض کنید R حلقه‌ای یک‌دار است. ثابت کنید که R با زیرحلقه‌ای از حلقه‌ی $End(R,+)$ متشکل از خودریختی‌های روی گروه جمعی $(R,+)$ یک‌ریخت است. (اثبات قضیه‌ی کیلی را در گروه ها به خاطر بیاورید).

۲۳- فرض کنید I ایده‌آلی از حلقه‌ی R باشد. با استفاده از قضیه‌ی **۳.۴.۳**، ثابت کنید که

(الف) زیرحلقه‌های R/I دقیقاً به صورت S/I هستند، که S زیرحلقه‌ای از R است و $I\subseteq S$.

(ب) ایده‌آل‌های R/I دقیقاً به صورت J/I هستند، که J ایده‌آلی از R است و $I\subseteq J$.

۲۴- فرض کنید I و J ایده آل هایی از حلقه ی تعویض پذیر R باشند به طوری که $I+J=R$. ثابت کنید که

(الف) نشان دهید که هر عضو R/I به صورت $b+I$ است که در آن $b\in J$.

(ب) $\dfrac{R}{I\cap J}\cong\dfrac{R}{I}\times\dfrac{R}{J}$.

۲۵- فرض کنید R_1 و R_2 حلقه‌هایی یک‌دار باشند، $R = R_1 \times R_2$، و $I \subseteq R$. ثابت کنید که I ایده‌آل R است اگر و تنها اگر $I = I_1 \times I_2$، که در آن $I_1 \trianglelefteq R_1$ و $I_2 \trianglelefteq R_2$.

۲۶- فرض کنید F یک میدان و $f : \mathbb{Z} \to F$ یک همریختی حلقه‌ای پوشا باشد. ثابت کنید که F میدانی از مرتبه‌ی عددی اول است.

۲۷- فرض کنید $R \to S$ یک بروریختی حلقه‌ها باشد. ثابت کنید که

(الف) اگر M ایده‌آل ماکسیمالی از R باشد به طوری که $Ker(f) \subseteq M$، آنگاه $f\left(M\right)$ ایده‌آل ماکسیمال S است.

(ب) اگر M' ایدآل ماکسیمال S باشد، آنگاه $f^{-1}\left(M'\right)$ ایده‌آل ماکسیمال R است.

(پ) ضابطه‌ی $M \mapsto f\left(M\right)$ یک تناظر یک به یک بین مجموعه‌ی ایده‌آل‌های ماکسیمال R که شامل $Ker\left(f\right)$ هستند و مجموعه‌ی ایده‌آل‌های ماکسیمال S تعریف می‌کند.

۲۸- فرض کنید $f : R \to S$ یک همریختی حلقه‌ای پوشا باشد. ثابت کنید که

(الف) (تمرین ۱۳ از بخش ۳.۳ را ببینید) S تعویض‌پذیر است اگر و تنها اگر $[R,R] \subseteq Kerf$، که در آن

$$[R,R] = \{xy - yx \mid x, y \in R\}$$

(ب) اگر $Kerf \subseteq [R,R]$ آنگاه $R/[R,R] \cong S/[S,S]$.

۲۹- حلقه‌ی $R = (\mathcal{P}(X); \Delta, \cap)$ را در نظر می‌گیریم و فرض می‌کنیم $Y \subseteq X$. تابع مشخصه‌ی $f_Y : X \to \mathbb{Z}_2$ با تعریف

$$f_Y(x) = \begin{cases} 1, & x \in Y \\ 0, & x \notin Y \end{cases}$$

را در نظر بگیرید. نشان دهید که $S = \{ f_Y : X \to \mathbb{Z}_2 \mid Y \subseteq X \}$ با جمع و ضرب معمولی توابع، حلقه است. به علاوه، حلقه‌ی S با حلقه‌ی R یک‌ریخت است. (**راهنمایی**: تابع $g : R \to S$ با تعریف $f(Y) = f_Y$ یک‌ریختی مورد نظر است.)

۳۰- فرض کنید m و n اعداد صحیح مثبت و متمایز باشند.

(الف) آیا حلقه‌ای یک‌دار وجود دارد که زیرحلقه‌هایی یک‌ریخت با $\mathbb{Z}_m$ و $\mathbb{Z}_n$ داشته باشد؟

(ب) سؤال قسمت **(الف)** را برای حالت دامنه‌ی صحیح پاسخ دهید.

۳۱- فرض کنید دامنه‌های صحیح D و D' یک‌ریخت باشند، نشان دهید که $Q(D) \cong Q(D')$.

۳۲- با یک مثال، نشان دهید که دامنه‌های صحیح D و D' وجود دارند به طوری که $D \subset D'$ ولی $Q(D) = Q(D')$.

۳۳- فرض کنید $D = \{a/2k \mid a,k \in \mathbb{Z}, k \geq 0\}$. نشان دهید که

(الف) D یک دامنه‌ی صحیح است.

(ب) میدان کسرهای D با $\mathbb{Q}$ یک‌ریخت است.

۳۴- فرض کنید R یک حلقه‌ی تعویض‌پذیر باشد. زیرمجموعه‌ی M از R را **ضربی بسته می‌نامیم** اگر $0 \notin M$ و برای $a,b \in M$ داشته باشیم $ab \in M$. نشان دهید که اگر R یک دامنه‌ی صحیح باشد، آنگاه $R^* = R - \{0\}$ ضربی بسته است.

۳۵- فرض کنید R یک حلقه‌ی تعویض‌پذیر و یک‌دار و M زیرمجموعه‌ای ضربی بسته از R باشد که شامل ۱ است. رابطه‌ی $\sim$ را روی مجموعه‌ی $R \times M$ به صورت

$$(a,b) \sim (c,d) \Leftrightarrow \exists s \in M, \quad s(ad - bc) = 0$$

تعریف کنید. نشان دهید که

(الف) رابطه‌ی $\sim$ هم ارزی است.

(ب) نشان دهید که $R_S = R \times M / \sim$ با اعمالی مشابه اعمال مذکور در قضیه‌ی **۱۲.۴.۳**، حلقه‌ای تعویض‌پذیر و یک‌دار است. این حلقه را **حلقه‌ی موضعی سازی** R در M می‌نامیم.

(پ) ثابت کنید $\varphi : R \to R_S$ با تعریف $a \mapsto [(a,1)]$ یک تکریختی است.

(ت) نشان دهید در حالتی که R یک دامنه‌ی صحیح باشد، و $M = R - \{0\}$، داریم $R_S = F_R$.

۵.۳ حلقه‌ی چندجمله‌ای‌ها

یکی از انواع حلقه که مطالعه روی آن پیشینه‌ای کهن، و در حل معادلات، جبر خطی، نظریـه گـالوا، تـا مطالعات امروز، نقش دارد، **حلقه‌ی چندجمله‌ای‌ها** است. با اعضا و اعمال جمع، ضرب، و تقسـیم روی چندجمله‌ای‌های با ضرایب اعداد حقیقی در دوره‌ی دبیرستان آشنا شدیم. حال، بـا مجـرد سـازی ایـن مفهوم، حلقه‌ی چندجمله‌ای‌های با ضرایب متعلق به حلقه‌ای دلخواه را معرفی و به اختصار مطالعه می-کنیم. مطالعه‌ی بیشتر این حلقه را در درس‌های دیگر جبر ادامه می‌دهیم. به زبان ساده

۱.۵.۳ تعریف. فرض کنیم R حلقه‌ای یک‌دار باشد. هر عبارت صوری به شکل

$$f = f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$$

را که در آن a_0، a_1، ...، a_n عضو R هستند، یک **چندجمله‌ای** (با ضرایب متعلق بـه R، یـا **روی** R) می‌نامیم . در این عبارت صوری، نماد x را **مجهول**، a_i را **ضریب iام**، a_0 را **جمله‌ی ثابت**، a_n را با شرط ناصفر بودن، **ضریب پیشرو**، و n را **درجه**ی چندجمله‌ای می‌نامیم، و می‌نویسیم $\deg f = n$. (برای چندجمله‌ای صفر درجه‌ای قایل نمی‌شویم). دو چندجمله‌ای را **مساوی** مـی‌گـوییم اگـر ضـرایب نظیرشان برابر باشند. مجموعه‌ی همه‌ی چندجمله‌ای‌های با ضرایب متعلـق بـه حلقـه‌ی R را بـا نمـاد $R[x]$ نشان می‌دهیم.

۲.۵.۳ بحث در کلاس. معمولاً از نمادگذاری فشرده‌ی مجموع

$$f = \sum_{i=0}^{n} a_ix^i = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$$

برای نمایش چندجمله‌ای‌ها استفاده می‌کنیم. همچنین، گاهی به جای $f(x)$ نماد ساده‌تر f را به کار می بریم. برای هر حلقه‌ی یک‌دار R، مجموعه‌ی $R[x]$، با اعمال معمولی زیر، یک حلقه است:

$$\sum\nolimits_{i=0}^{n} a_ix^i + \sum\nolimits_{i=0}^{m} b_ix^i = \sum\nolimits_{i=0}^{\max\{m,n\}} (a_i + b_i)x^i$$
$$(\sum\nolimits_{i=0}^{n} a_ix^i)(\sum\nolimits_{i=0}^{m} b_ix^i) = \sum_{k=0}^{m+n} (\sum\nolimits_{i=0}^{k} a_ib_{k-i})x^k$$

حاصل‌ضرب، در نمادگذاری فشرده، پیچیده **به نظر** می‌رسد، ولی به همان صورت **ساده‌ای** انجـام مـی-شود که در دبیرستان دیدیم. برای مثال، در $\mathbb{R}[x]$ داریم

$$\begin{aligned}(2x^2-5x+4)(-x^3+2x) &= -2x^2x^3+4x^2x+5xx^3-10xx-4x^3+8x\\ &= -2x^5+4x^3+5x^4-10x^2-4x^3+8x\\ &= -2x^5+5x^4-10x^2+8x\end{aligned}$$

که در آن از تساوی $x^i x^j = x^{i+j}$ استفاده شده است. بررسی شرط‌های حلقه برای $R[x]$ سرراست و راحت است (ولی قدری پیچیده **به نظر** می‌رسد). برای نمونه، شرکت‌پذیری ضرب را اثبات و بقیه را به شما واگذار می‌کنیم. فرض کنیم

$$f=\sum_{i=0}^{n} a_i x^i,\;\; g=\sum_{i=0}^{m} b_i x^i,\;\; h=\sum_{i=0}^{t} c_i x^i$$

نشان می‌دهیم که برای هر k، ضریب kام $(fg)h$ و $f(gh)$ برابرند. بنابر تعریف، ضریب kام $(fg)h$ برابر است با

$$\sum_{i=0}^{k} d_i c_{k-i} = \sum_{i=0}^{k} (\sum_{j=0}^{i} a_j b_{i-j}) c_{k-i}$$

و ضریب kام $f(gh)$ برابر است با

$$\sum_{i=0}^{k} a_i e_{k-i} = \sum_{i=0}^{k} a_i (\sum_{j=0}^{i} b_j c_{i-j})$$

که با توجه به توزیع‌پذیری ضرب روی جمع در حلقه‌ی R، هر دو ضریب برابر هستند با

$$\sum_{i+j+l=k} a_i b_j c_l$$

برخی از ویژگی‌های حلقه‌ی R به حلقه‌ی $R[x]$ منتقل می‌شوند. برای آگاهی از برخی از آن‌ها، در بحث زیر شرکت کنید.

۳.۵.۳ بحث در کلاس

۱- به عنوان نمونه‌ای دیگر، اعمال جمع و ضرب زیر را در حلقه‌ی $\mathbb{Z}_4[x]$ انجام می‌دهیم:

$$\begin{aligned}(x^6+3x^3+x+3)+(3x^6+2x+1) \\ &= (1+_4 3)x^6+3x^3+(1+_4 2)x+(3+_4 1) \\ &= 0x^6+3x^3+3x+0 \\ &= 3x^3+3x\end{aligned}$$

$$\begin{aligned}(2x^6+3x^3+3)(2x^2+1) \\ &= (2\cdot_4 2)x^6x^2+2x^6+(3\cdot_4 2)x^3x^2+3x^3+(3\cdot_4 2)x^2+3 \\ &= 0x^8+2x^6+2x^5+3x^3+2x^2+3 \\ &= 2x^6+2x^5+3x^3+2x^2+3\end{aligned}$$

۲- روشن است که اگر حلقه‌ی R یک‌دار باشد، آنگاه $R[x]$ نیز یک‌دار است. اگر R تعویض‌پذیر باشد، آنگاه $R[x]$ نیز چنین است.

۳- اگر حلقه‌ی R دامنه‌ی صحیح باشد، آنگاه حلقه‌ی $R[x]$ نیز چنین است. با توجه به بند**۲**، کافی است نشان دهیم که $R[x]\setminus\{0\}$ نسبت به ضرب بسته است. فرض کنیم

$$f=\sum_{i=0}^{n}a_ix^i,\quad g=\sum_{i=0}^{m}b_ix^i,$$

ناصفر باشند (روشن است که $fg\neq 0$ ، ولی اثبات آن را می آوریم). در این صورت، حداقل یک ضریب از هر یک از ضریب‌های f و g ناصفر است. با توجه به متناهی بودن تعداد ضرایب، بزرگترین $s,t\geq 0$ وجود دارند به طوری که $a_s\neq 0$ و $b_t\neq 0$. یعنی، به ازای $i>s$ داریم $a_i=0$ و به ازای $j>t$ داریم $b_j=0$. در نتیجه، ضریب $(s+t)$ام fg برابر است با

$$a_0b_{s+t}+a_1b_{s+t-1}+\cdots+a_sb_t+a_{s+1}b_{t-1}+\cdots a_{s+t}b_0=a_sb_t$$

که چون R دامنه است، a_sb_t عضوی ناصفر از R است. بنابراین، $fg\neq 0$.

۴- اگر R میدان باشد، لزومی ندارد که $R[x]$ میدان باشد. در واقع، تنها عضوهای وارون‌پذیر $R[x]$ **چندجمله‌ای‌های ثابت** ناصفر

$$f=a_0+0x+0x^2+\cdots=a_0$$

هستند. در واقع، اگر $0 \neq f = \sum_{i=0}^{n} a_i x^i$ دارای وارونی چون $0 \neq f^{-1} = \sum_{i=0}^{m} b_i x^i$ باشد، آنگاه $f \cdot f^{-1} = 1$ ، یعنی

$$\sum_{k=0}^{m+n} (\sum_{i=0}^{k} a_i b_{k-i}) x^k = 1 + 0x + 0x^2 + \cdots \qquad (*)$$

از طرف دیگر، با استدلالی مشابهی بند۳، بزرگترین $s,t \geq 0$ وجود دارند بـه طـوری کـه $a_s \neq 0$ و $b_t \neq 0$، و در نتیجه ضریب $(s+t)$ام چندجمله‌ای ff^{-1} برابر با $a_s b_t$ است، که با توجه به میـدان (و در نتیجه دامنه) بودن R، عضوی ناصفر است و در نتیجه با تساوی (*) در تناقض است، مگر اینکـه $s+t=0$، یعنی $s=t=0$. پس $a_0 \neq 0$ ولی برای $i>0$، $a_i = 0$. بنابراین، f چندجمله‌ای ثابت ناصفر است.

۵- در حالت کلی اگر $f \neq 0$، $g \neq 0$، $f+g \neq 0$ ، و $fg \neq 0$ ، آنگاه

$$\deg fg \leq \deg f + \deg g \quad \text{و} \quad \deg(f+g) \leq \max\{\deg f + \deg g)$$

البته اگر ضرایب چندجمله‌ای‌های f و g متعلق به یک میدان یا دامنه‌ی صحیح باشند، یا حتـی اگـر ضریب پیشرو یکی از آن‌ها مقسم صفر نباشد، آنگاه $\deg fg = \deg f + \deg g$.

در قضیه‌ی زیر، که به راحتی اثبات می‌شود، دو همریختی ساده بین حلقه‌ی R و حلقه‌ی $R[x]$ را معرفی می‌کنیم.

۴.۵.۳ قضیه

۱- برای هر حلقه چون R، یک همریختی حلقه‌ای یک به یک $h: R \to R[x]$ وجـود دارد کـه بـه صورت زیر تعریف می‌شود:

$$h(a) = a + 0x + 0x^2 + \cdots = a$$

۲- برای هر حلقه چون R، یک همریختی حلقه‌ای پوشا $k: R[x] \to R$ وجود دارد که به صـورت زیر تعریف می‌شود:

$$k(\sum_{i=0}^{n} a_i x^i) = a_0$$

۵.۵.۳ بحث در کلاس

۱- تک‌ریختی داده شده در بند **۱** قضیه‌ی بالا، عضوهای حلقه‌ی R را به عنوان چندجمله‌ای‌های ثابت در $R[x]$ معرفی می‌کند، و در نتیجه R زیرحلقه‌ی $R[x]$ **محسوب** می‌شود.

۲- همریختی تعریف شده در بند**۲** قضیه‌ی بالا، در واقع یکی از دسته همریختی‌هایی است که **ارزیاب** یا **مقداریاب** نام دارند (که در زیر تعریف می‌کنیم) و با جایگذاری عضوی از حلقه‌ی R به جای x در چندجمله‌ای‌ها حاصل می‌شوند. در آن بند، تابع k از جایگذاری عضو 0 به جای x در چندجمله‌ای به دست آمده است. اگر قضیه‌ی اساسی همریختی را در مورد همریختی k به کار ببریم، این نتیجه حاصل می‌شود که

$$R[x]/Kerk \cong R$$

که در آن

$$\begin{aligned} Ker\,k &= \left\{ \sum_{i=0}^{n} a_i\, x^i \mid a_0 = 0, n \in \mathbb{N} \right\} \\ &= \{a_1 x + a_2 x^2 + \cdots + a_n x^n \mid n \in \mathbb{N}\} \\ &= \{x(a_1 + a_2 x^2 + \cdots + a_n x^{n-1}) \mid, n \in \mathbb{N}\} \end{aligned}$$

این مجموعه، در صورتی که فرض یک‌دار بودن حلقه‌ی R را اضافه کنیم، همان ایده‌آل تولید شده توسط عضو x، یعنی (x)، در حلقه‌ی $R[x]$ است. پس، بنابر قضیه‌ی اساسی همریختی‌ها، $R[x]/(x) \cong R$. حال، تعریف کلی زیر را می‌آوریم.

۶.۵.۳ تعریف. فرض کنیم S حلقه و R زیرحلقه‌ی آن باشد. فرض کنیم $\alpha \in S$. در این صورت همریختی $\varphi_\alpha : R[x] \to S$ با تعریف

$$\varphi_\alpha(\textstyle\sum_{i=0}^{n} a_i x^i) = \displaystyle\sum_{i=0}^{n} a_i \alpha^i$$

را، به دلیلی روشن، **همریختی ارزیاب** یا **مقدار یاب در** α می‌نامیم. زیرا، $\varphi_\alpha(f(x)) = f(\alpha)$.

توجه کنید که φ_α واقعاً همریختی است. این واقعیت از تعریف جمع و ضرب چندجمله‌ای‌ها و ویژگی‌های اعمال حلقه نتیجه می‌شود. برای مثال، حفظ عمل جمع به صورت زیر است:

$$\varphi_\alpha(\sum_{i=0}^{n} a_i x^i + \sum_{i=0}^{m} b_i x^i) = \varphi_\alpha(\sum_{i=0}^{\max\{m,n\}} (a_i + b_i) x^i)$$
$$= \sum_{i=0}^{\max\{m,n\}} (a_i + b_i)\alpha^i$$
$$= \sum_{i=0}^{n} a_i \alpha^i + \sum_{i=0}^{m} b_i \alpha^i$$

که تساوی آخر با استفاده از توزیع‌پذیری ضرب روی جمع در حلقه‌ی S و تعویض‌پذیری جمع S به دست آمده است. همچنین روشن است که در قضیه‌ی بالا، $k = \varphi_0$.

تقسیم چندجمله‌ای‌های با ضرایب عددی را در دبیرستان دیده‌ایم. در زیر، الگوریتم تقسیم چندجمله‌ای‌های روی یک حلقه دلخواه (به ویژه روی میدان) را می‌بینیم.

۷.۵.۳ قضیه (الگوریتم تقسیم). فرض کنیم R حلقه‌ای یک‌دار باشد و $f, g \in R[x]$ که در آن $g \neq 0$ و ضریب پیشرو آن وارون‌پذیر است (به ویژه اگر R میدان باشد). در این صورت، چندجمله‌ای‌های منحصر به فرد $q, r \in R[x]$ وجود دارند به طوری که

$$f = qg + r$$

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

اثبات. فرض کنیم $f = \sum_{i=0}^{n} a_i x^i$ و $g = \sum_{i=0}^{m} b_i x^i$. ابتدا مشاهده می‌کنیم که اگر $f = 0$ یا اگر $\deg f < \deg g$ آنگاه با قرار دادن $q = 0$ و $r = f$ حکم حاصل می‌شود. حال فرض کنیم $f \neq 0$ و $\deg f \geq \deg g$. حکم را با استقرا روی $\deg f$ اثبات می‌کنیم. ملاحظه می‌کنیم که اگر $\deg f = 0$ آنگاه با قرار دادن $q = b_0^{-1} a_0$ و $r = 0$ حکم ثابت می‌شود. فرض می‌کنیم $\deg f \neq 0$ و حکم برای همه‌ی چندجمله‌ای‌های ناصفر از درجه‌ی کمتر از $n = \deg f$ برقرار باشد. قرار می‌دهیم

$$h = f - b_m^{-1} a_n x^{n-m} g =$$
$$= (a_0 + a_1 x + \cdots + a_n x^n)$$
$$-(b_0 b_m^{-1} a_n x^{n-m} + b_1 b_m^{-1} a_n x^{n-m+1} + \cdots + b_m b_m^{-1} x^{n-m+m})$$
$$= a_0 + a_1 x + \cdots + (a_{n-m} - b_0 b_m^{-1} a_n) x^{n-m}$$
$$+(a_{n-m+1} - b_1 b_m^{-1} a_n) x^{n-m+1} + \cdots + (a_{n-1} - b_{m-1} b_m^{-1}) x^{n-1}$$

حال، یا $h = 0$ و در نتیجه

$$f = b_m^{-1} a_n x^{n-m} g + 0$$

که حکم ثابت شده است، یا $h \neq 0$ که در این صورت، با به کار بردن فرض استقرا برای h، چندجمله‌ای‌های $s, r \in R[x]$ وجود دارند به طوری که

$$h = sg + r$$

و $r = 0$ یا $\deg r < \deg g$. در این حالت داریم

$$\begin{aligned} f &= b_m^{-1} a_n x^{n-m} g + h \\ &= b_m^{-1} a_n x^{n-m} g + sg + r \\ &= (s + b_m^{-1} a_n x^{n-m}) g + r \end{aligned}$$

که باز هم حکم ثابت شده است. در پایان برای اثبات منحصر به فرد بودن q و r، فرض می‌کنیم

$$f = qg + r = q'g + r'$$

که در آن $r = 0$ یا $\deg r < \deg g$ و $r' = 0$ یا $\deg r' < \deg g$. پس

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

حال، اگر $q \neq q'$، آنگاه $q - q' \neq 0$ و در نتیجه (چون ضریب پیشرو g وارون‌پذیر است)

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

که تناقض با ویژگی‌های فرض در مورد r و r' دارد. پس باید $q = q'$ و در نتیجه $r = r'$.

۸.۵.۳ تعریف. چندجمله‌ای‌های q و r قضیه‌ی بالا را به ترتیب **خارج قسمت** و **باقی‌مانده‌ی** تقسیم f بر g می‌نامیم.

۹.۵.۳ بحث در کلاس. تقسیم چندجمله‌ای‌های با ضرایب عددی را در دبیرستان دیده‌اید. حال آن تجربه را برای چندجمله‌ای‌های با ضرایب در حلقه‌ی $\mathbb{Z}_n$ مرور می‌کنیم. خارج قسمت و باقی‌مانده‌ی تقسیم $f = 2x^4 - 3x^3 + 2x^2 + 3x - 1$ بر $g = x^2 - 3x + 2$ را در $\mathbb{Z}_5[x]$ به دست

می آوریم. توجه کنید که حاصل‌ضرب، مجموع، و قرینه ضرایب را در همنهشتی به پیمانه‌ی ۵ انجام می‌دهیم. (برای آموزش، مراحل تقسیم را یکی یکی نشان داده‌ایم، ولی شما می‌توانید این کار را ساده‌تر انجام دهید). ابتدا توجه می‌کنیم که روی میدان $\mathbb{Z}_5$ داریم $f = 2x^4 + 2x^3 + 2x^2 + 3x + 4$. حال، داریم

$$2x^4 + 2x^3 + 2x^2 + 3x + 4 = (x^2 - 3x + 2)(2x^2 - 2x - 3) + 3x$$

زیرا

$$\begin{array}{ll}
2x^4 - 3x^3 + 2x^2 + 3x - 1 & \underline{|x^2 - 3x + 2} \\
2x^4 - (6 \equiv_5)1x^3 + 4x^2 & \quad 2x^2 \\
------------- & \\
(2-2)x^4 + (-3-(-1))x^3 + (2-4)x^2 + 3x - 1 & \\
= -2x^3 - 2x^2 + 3x - 1 & \underline{|x^2 - 3x + 2} \\
-2x^3 + (6 \equiv_5)1x^2 - 4x & \quad -2x \\
---------------- & \\
(-2+2)x^3 + (-2-1)x^2 + (3-(-4))x - 1 & \\
= -3x^2 + (7 \equiv_5)2x - 1 & \underline{|x^2 - 3x + 2} \\
-3x^2 + (9 \equiv_5)4x - (6 \equiv_5)1 & \quad -3 \\
--------------- & \\
(-3+3)x^2 + (2-4)x + (-1+1) & \\
= -2x &
\end{array}$$

بنابراین، خارج قسمت و باقی‌مانده برابر هستند با

$$q = 2x^2 - 2x - 3 = 2x^2 + 3x + 2$$
$$r = -2x = 3x$$

که در آن، تساوی‌های آخر از محاسبه‌ی قرینه‌ها در $\mathbb{Z}_5$ حاصل شده است. البته، در هر مرحله‌ی تقسیم می‌توانیم اعداد منفی را با اعدادی مثبت در میدان $\{0,1,2,3,4\}$ جایگذاری کنیم.

۱۰.۵.۳ تعریف. فرض کنیم R و S حلقه باشند، $R \leq S$ و $f \in R[x]$. عضو $\alpha \in S$ را یک **ریشه**‌ی f در S می‌گوییم، اگر $f(\alpha) = 0$.

۱۱.۵.۳ قضیه. فرض کنیم R حلقه‌ای یکدار باشد و $f \in R[x]$ و $a \in R$. در این صورت،

۱- باقی‌مانده‌ی تقسیم f بر $x-a$ برابر با $f(a)$ است.

۲- عضو a یک ریشه‌ی f در R است اگر و تنها اگر باقی‌مانده‌ی تقسیم f بر $x-a$ برابر با 0 باشد.

اثبات

۱- بنابر الگوریتم تقسیم، چندجمله‌ای‌های منحصر به فرد $q,r \in R[x]$ وجود دارند به طوری که

$$f = q(x-a)+r$$

در نتیجه، $f(a)=q(a)(a-a)+r(a)=r(a)$. از طرف دیگر، $r=0$ یا $\deg r < \deg(x-a)$. اگر $r=0$ آنگاه $0=r=r(a)=f(a)$، پس، در این صودت نیز $r=f(a)$. اگر $\deg r < \deg(x-a)=1$ آنگاه $\deg r = 0$، پس r چندجمله‌ای ثابت است، و در نتیجه، $r=r(a)=f(a)$.

۲- به راحتی از بند ۱ نتیجه می‌شود.

۱۲.۵.۳ بحث در کلاس. مثال‌های زیر نشان می‌دهند که در حالت کلی قانونی برای تعداد ریشه‌های یک چندجمله‌ای $f \in R[x]$ در R وجود ندارد.

۱- تنها ریشه‌ی چندجمله‌ای درجه‌ی دو $f = 1+x+x^2$ در $\mathbb{Z}_3$ برابر با ۱ است، زیرا $f(1)=0$ ولی $f(0)=1=f(2)$.

۲- ریشه‌های $f = x+x^2$ در $\mathbb{Z}_6$ برابرند با 0، 2، 3 و 5.

۳- چندجمله‌ای $f = 1+x+x^2$ در $\mathbb{Z}_5$ ریشه ندارد.

ولی قضیه‌ی زیر نشان می‌دهد که برای چندجمله‌های روی یک دامنه صحیح، تعداد ریشه‌های موجود در آن دامنه‌ی صحیح، حداکثر برابر با درجه‌ی چندجمله‌ای است. همچنین ثابت شده است که روی برخی از میدان‌ها، (مانند $\mathbb{C}$) تعداد ریشه‌های یک چندجمله‌ای در آن میدان، دقیقاً برابر با درجه-ی چندجمله‌ای است.

۱۳.۵.۳ قضیه. فرض کنیم D یک دامنه‌ی صحیح است و $f \in D[x]$. در این صورت تعداد ریشه‌های f در D حداکثر برابر با $\deg f$ است.

اثبات. فرض می‌کنیم $\deg f = n$ و حکم را با استقرا روی n اثبات می‌کنیم. اگر $n = 0$ حکم واضح است. اگر $n = 1$ و $f = ax + b$ که در آن $a \neq 0$. در این صورت، f حداکثر یک ریشه دارد. زیرا، اگر α, β ریشه‌های f باشند، آنگاه $a\alpha + b = 0 = a\beta + b$ و درنتیجه، $a\alpha = a\beta$ و با توجه به برقرای قوانین حذف در دامنه‌ی D، $\alpha = \beta$.

حال فرض کنیم قضیه برای هر چندجمله‌های از درجه‌ی $n-1$ برقرار باشد. اگر f در D ریشه نداشته باشد، حکم ثابت شده است. فرض کنیم $a \in D$ ریشه‌ی f باشد. در این صورت، چندجمله‌ای منحصر به فرد $q \in D[x]$ وجود دارد به طوری که $f = (x-a)q$ و در نتیجه درجه‌ی چندجمله‌ای q، برابر با $n-1$ است. پس بنابر فرض استقرا، تعداد ریشه‌های q حداکثر $n-1$ است. حال چون $x - a$ تنها یک ریشه دارد، بنابراین، تعداد ریشه‌های f حداکثر n است.

تعریف دامنه‌ی ایدآل اصلی را از تمرین ۶ بخش ۳.۳ به خاطر آورید.

۱۴.۵.۳ قضیه. اگر F یک میدان باشد، آنگاه $F[x]$ یک دامنه‌ی ایده‌آل اصلی است.

اثبات. فرض کنیم F یک میدان و I یک ایدآل $F[x]$ است. باید نشان دهیم که I یک ایدآل اصلی است. اگر $I = \{0\}$، آنگاه I ایده‌آل اصلی است. فرض کنیم $I \neq \{0\}$ و

$$P = \{\deg f : 0 \neq f \in I\}$$

در این صورت، P زیرمجموعه‌ای ناتهی از $\mathbb{N}_0$ است. پس بنابر اصل خوش‌ترتیبی، P دارای کوچک‌ترین عضوی چون n است. فرض کنیم $g \in I$ از درجه‌ی n است. نشان می‌دهیم $I = gF[x]$. از آنجا که I ایده‌آل $F[x]$ است، پس $gF[x] \subseteq I$. برعکس، فرض کنیم $f \in I$. بنابر الگوریتم تقسیم، چندجمله‌ای‌های منحصر به فرد $q, r \in F[x]$ وجود دارند به طوری که

$$f = gq + r$$

و $r = 0$ یا $\deg r < \deg g$. در نتیجه،

$$r = f - gq \in I$$

پس با توجه به انتخاب g، $\deg r < \deg g$ ناممکن است. بنابراین، $r = 0$ و

$$f = gq \in gF[x].$$

در قضیه‌ی ۱۴.۵.۳ اگر F میدان نباشد، $F[x]$ لزوماً دامنه‌ی ایده‌آل اصلی نیست. زیرا برای مثال، $\mathbb{Z}[x]$ دامنه‌ای است که ایده‌آل‌های آن لزوماً اصلی نیستند، به عنوان مثال، $(x)+(2)$ ایده‌آل اصلی نیست. راهنمایی بیشتر.

از خوبی‌های برخی از دامنه‌های ایده‌آل اصلی یکی دیگر این است که ، مشابه تجزیه‌ی اعداد صحیح به اعداد اول، هرعضو در آن دارای تجزیه‌ای به عضوهای ساده‌تر است. این ویژگی و مطالعه‌ی بیشتر حلقه‌ی چندجمله‌ای‌ها را در درس‌های بعدی جبر پی می‌گیریم.

تمرین ۵.۳

دسته اول

۱- فرض کنید R دامنه‌ی صحیح و $R[x]$ دامنه‌ی ایدآل اصلی باشد. ثابت کنید

الف) هر ایدآل اول ناصفر $R[x]$ ماکسیمال است.

ب) R میدان است.

۲- فرض کنید R حلقه‌ای یک‌دار باشد. نشان دهید که $R[x]/(x) \cong R$.

۳- فرض کنید R حلقه‌ای یک‌دار باشد. ثابت کنید که

$$R[x]/(x^2) = \{(a_0 + a_1x) + (x^2) \mid a_0, a_1 \in R\}$$

و نتیجه بگیرید که اگر R دارای n عضو باشد، آنگاه $R[x]/(x^2)$ دارای n^2 عضو است.

۴- فرض کنید R حلقه‌ای یک‌دار و I ایدآلی از R باشد. ثابت کنید که $I[x]$ ایدآل $R[x]$ است و $R[x]/I[x] \cong (R/I)[x]$.

۵- با استفاده از همریختی ارزیاب φ_0، نشان دهید که $\mathbb{Z}[x]/(x) \cong \mathbb{Z}$. آیا (x) ایدآل ماکسیمالی از $\mathbb{Z}[x]$ است؟

۶- همریختی ارزیاب $\varphi_i : \mathbb{Q}[x] \to \mathbb{C}$ را که در آن $i = \sqrt{-1}$ در نظر بگیرید. نشان دهید که $Ker\varphi_i = \{(1+x^2)f \mid f \in \mathbb{Q}[x]\}$.

مراجع

1. S. Burris, H.P. Sankappanavar, A Course in Universal Algebra, Springer-Verlag, 1981.

2. K. Denecke, S.L. Wismath, Universal Algebra and Applications in Theoretical Computer Science, 2002.

3. G. Gratzer, Universal Algebra, Springer, 20083.

4. J.D.H Smith, A.B. Romanowska, Post-Modern Algebra, John Wiley, 1999.

5. E.G. Wagner, Universal Algebra for Computer Science, Wagner, Mathematics, 2006.

6. W. Wechler, Universal Algebra for Computer Scientists, Springer, 1992.

حلقه و تجزیه ، دیوید شارپ، ترجمه‌ی دکتر محمد مهدی ابراهیمی، انتشارات دانشگاه شهید بهشتی، ۱۳۷۷