مبانی جبر

(برای رشته‌های ریاضیات و کاربردها و علوم کامپیوتر)

نوشته‌ی:

دکتر محمدمهدی ابراهیمی دکتر علیرضا سالمکار دکتر مرتضی محمودی

گروه ریاضی

دانشگاه شهید بهشتی

۱۳۹۰

فهرست مطالب

فصل ۳ آشنایی با حلقه‌ها

منابع (کامل می‌شود)

فهرست راهنما (بعداً می‌آید)

سخنی با دانشجو و استاد

اگر **ریاضیات**، آنگونه که گفته می‌شود، **مادر همه‌ی دانش‌ها**ست، بی تردید **جبر** ابزاری دقیق و توانمند در دستان اوست!

در این مبحث از ریاضیات است که استدلال‌های منطقی به بهترین وجهی نمایان می‌شوند و سلول‌های خاکستری مغز را به کار می‌گیرند!

میزان مستدل بودن هر علمی بستگی به درجه‌ی تبدیل مسئله‌هایش به سؤال‌های ریاضیاتی دارد. نقش **جبر** را در ریاضیات شاید بتوان با همین نقش ریاضیات در علوم مقایسه کرد. بسیاری از ساختارهایی که در شاخه‌های مختلف **علوم ریاضی** ظاهر می‌شوند، در مبحث **جبر** به صورت **مجرد** در می‌آیند و مورد مطالعه قرار می‌گیرند که باعث پیشرفت بیشتر هر دو شاخه‌ی ریاضیات می‌شود.

مبحث **جبر**، مطالعه‌ی **دستگاه‌های جبری** است. **جبر کلاسیک** به همت ریاضی‌دانانی چون **وان‌در واردن** و **امی نوتر** با معرفی رسمی و اصل موضوعی دستگاهای جبری **گروه**، **حلقه**، **مدول**، و **فضای برداری** به وجود آمد و به موفقیت‌های بسزایی در حل مسئله‌های کلاسیک دست یافت. ولی

پاسخ به سؤال‌های نوین امروز، ابزاری نوین نیز می‌طلبند!

امروزه ناگزیریم از دستگاه‌های جدیدتری چون **نیمگروه**، **تکواره**، **سیستم‌ها**، **شبه گروه**، **جبر هیتینگ**، **مشبکه**، **جبر بول**، **اتوماتا**، **رسته**، **گروه و حلقه‌ی مرتب**، **جبرهای جامع مرتب**، **جبر فازی**، و از این قبیل، نیز برای پاسخگویی به سؤال‌های جدید علوم ریاضی، علوم کامپیوتر، فیزیک، شیمی، زیست شناسی، نانو، اقتصاد، محاسبات نرم، و از این قبیل، بهره بگیریم.

ریاضی‌دانان در مطالعه‌ی دستگاه‌های جبری کلاسیک متوجه شدند که برخی از مفاهیم و ابزارها در همه‌ی آن‌ها به اشتراک مطرح می‌شوند. از این رو، نیاز به یک‌پارچه کردن دستگاه‌های جبری احساس شد، و سرانجام **بیرخوف** ضمن معرفی چند دستگاه جبری جدیدتر، تعریف رسمی دستگاه‌های جامع جبری را به گونه‌ای معرفی کرد که **دستگاه‌های جبری کلاسیک مثال‌هایی از این حالت کلی شدند**، که ویژگی‌های بنیادی آن‌ها چیزی جز حالت خاص ویژگی‌های کلی نیستند!

از این رو، در فصل اول این کتاب، **مبانی ساختارهای جامع جبری** و مفاهیم کلی مربوط به آن‌ها را، با توجه به زمان محدودی که برای این قسمت تعیین شده است، به اختصار و به **زبانی ساده** مطالعه می‌کنیم و مثال‌هایی متنوع، کلاسیک و جدید، ارائه می‌دهیم، که در دروس **علوم ریاضی و کاربردها** مطرح می‌شوند. مطالب جامع و کلی جالبی در این فصل مطرح می‌شوند که به نظر ما هر دانشجوی ریاضی، صرف نظر از اینکه با دستگاه‌های کلاسیک سروکار دارد یا روزی با دستگاه‌های جدیدتر سروکار خواهد داشت، باید آن‌ها را بداند! **باید خواستگاه، بنیاد، منبع، سرچشمه، و علت معرفی مفاهیم را بدانیم** تا بهتر آن‌ها را به کار ببریم و خود، هنگام نیاز، **سازنده‌ی مفاهیم جدید باشیم**! **این طور نیست؟** مطالب این فصل دانشجویان را برای مطالعه‌ی درس‌های دیگر ریاضی، به ویژه درس‌های جبر، آماده می‌کند. به پیشنهاد برخی از همکاران که در کارگاه‌های معرفی این کتاب در دانشگاه شهید

بهشتی و دانشگاه‌های دیگر شرکت یا پیش نویس کتاب را مطالعه کردند، مطالبی را برای مطالعه‌ی اختیاری در پیوست کتاب آورده‌ایم.

سپس در دو فصل دیگر کتاب، مطالبی را که در فصل ۱ آموختیم برای دستگاه‌های جبری کلاسیک **گروه و حلقه**، که از اهمیت ویژه و تاریخی برخوردار هستند، با جزییات بیشتر مورد مطالعه و بررسی قرار می‌دهیم.

دانشجویان عزیز علوم ریاضی

با **خوش‌آمد** به رشته‌های علوم ریاضی و با سپاس از اینکه این کتاب را انتخاب کردید. قصد ما در کتاب درس **مبانی جبر** صرفاً آشنا کردن شما با مفاهیم مجرد این **مبحث زیبا** از ریاضییات **نیست**، بلکه می‌خواهیم در این خودآموز گپ‌گونه به کمک خود شما **فوت و فن** کار را طوری بیاموزید که ملکه‌ی ذهنتان و قسمتی از بصیرت‌تان شود. سعی شده است که زبان نگارش کتاب به گونه‌ای باشد که هنگام مطالعه‌ی آن، احساس تنهایی نکنید و **ما را نزدیک خود ببینید!**

هیچ مبحثی از ریاضیات، به ویژه مباحث مجرد، بلافاصله درک نمی‌شوند و در ذهن نمی-نشینند!

بنابراین، صبر و حوصله، پشتکار و امید شما را می‌طلبد. طولی نمی‌کشد که چنان با مفاهیم و روش-های جبری انس می‌گیرید که مجرد بودن آن‌ها را فراموش می‌کنید!

مسایل بخش کلیدی آموزش ریاضیات، به‌ویژه جبر، هستند.

کسب تبحر در این مبحث از علوم ریاضی و درک ظرافت‌هایش **جز با تلاش** برای حل‌کردن تمرین‌های آن (**چه به جواب نهایی برسد یا نرسد**) ممکن نیست! تجربه‌ی سال‌ها تحصیل و تدریس نویسندگان این کتاب نشان داده است که دانشجویان در نگاه نخستین به مسئله‌های مجرد، تصور می‌کنند که هیچ‌یک از آن‌ها را نمی‌توانند حل‌کنند (**ما نیز چنین بودیم**). ولی آن‌هایی که مصمم هستند، ترسی به دل راه نمی‌دهند و با خود می‌گویند که:

این مسئله‌ها برای آن‌ها طرح شده است و یقیناً با ابزاری که آموخته‌اند قابل حل هستند!

طولی نمی‌کشد که چنان تبحری در حل مسئله‌ها به دست می‌آورید و از زیبایی این بازی فکری لذت می‌برید و در لابلای کتاب‌های دیگر به دنبال مسئله‌های جدید و مبارز طلب می‌گردید و خود نیز تلاش می‌کنید مسئله طرح و حل کنید! آلبرت آینشتین گفته است که

هوشم نه چنان است تلاشم آنچنان است

به هر حال، وقت محدودی در اختیار استاد درس است و بدون کمک شما نمی‌تواند سرفصل درس را به خوبی آموزش دهد، **پس باید آستین‌ها را بالا زد و قسمتی از وظیفه را خود به عهده گرفت!**

همکار ارجمند درس مبانی جبر

از آنجا که این اولین باری است که دانشجویان (ریاضی و علوم کامپیوتر) با مبحث **شیرین جبر** آشنا می‌شوند، و در این درس مجرد است که با **اندیشه ورزی** می‌توانند استعدادهای خود را پرورش دهند، باید محطاط تر باشیم تا به هدفمان برسیم!

اکثر کتاب‌های سنتی و متداول با عنوان‌هایی چون "**جبر مجرد**" ، "**اساس جبر مجرد**"، و از این قبیل، در واقع تنها دو دستگاه جبری خاص **گروه** و **حلقه** را مورد مطالعه قرار می‌دهند، و صحبتی از **اساس** (**جبر**) به معنی عام آن نمی‌کنند، که انصاف نیست. برای مثال، خارج قسمت دستگاه‌های جبری به چه معنی است؟ چرا خارج قسمت گروه‌ها با استفاده از زیرگروه‌های نرمال یا خارج قسمت حلقه‌ها با استفاده ار ایده‌آل‌ها تعریف می‌شود؟ آیا این تنها راه ساختن خارج قسمت گروه‌ها و حلقه‌ها است؟ آیا این روش ساختن خارج قسمت برای همه‌ی دستگاه‌های جبری قابل اجرا است؟ این کتاب ابتدا به زبانی ساده به **مبانی جبر** می‌پردازد و به دانشجویان درس **مبانی جبر** می‌آموزد که **جبر چیست**، مثال‌های متنوع آن کدام‌اند، و چه مفاهیمی به گونه‌ی **جامع** در آن مطرح می‌شوند. سپس، در دو فصل دیگر، این مطالب جامع را برای دو دستگاه خاص و مهم گروه و حلقه با جزییات بیشتر بررسی می‌کنیم. مطالب جامع فصل **۱** ، منبع، سرچشمه، و علت معرفی مفاهیم را در این دستگاه‌های خاص و کلاسیک بیان و **درک آن‌ها را آسان‌تر می‌کند**. اگر چه زمان چندان زیادی به این درس اختصاص داده نشده است، نباید این مطالب را از **دانشجویان علوم ریاضی قرن بیست و یکم** دریغ کنیم! همچنین، باید در عین حال که مطالب مورد نظر را تدریس می‌کنیم، هر چقدر که زمان اجازه می‌دهد، دانشجویان را نیز در **برخی** از بندهای **بحث در کلاس** به فعالیت تشویق کنیم، تا اینکه خود **ماهی گیری بیاموزند**!

ما سعی کرده‌ایم که مطالب فصل‌های **۱** را برای **۹**، **۲** را برای **۱۳**، و **۳** را برای **۶** جلسه‌ی ۷۵ دقیقه‌ای تدوین کنیم. البته، چند جلسه نیز برای خطایمان باقی گذاشته‌ایم. اگر امکان **نمایش الکترونیکی** قسمت‌هایی از متن درس باشد، یقیناً فرصت بیشتری برای به بحث گذاشتن مطالب با دانشجویان خواهیم داشت.

با آرزوی موفقیت ما، شما، و دانشجویان عزیزمان

ابراهیمی، سالکار، محمودی

فصل م

مقدمه

خواهیم دید که جبر مطالعه‌ی **دستگاه‌های جبری** است، یعنی **مجموعه**هایی که از تعدادی معین از عضوهای آن می‌توان عضوی از آن را به دست آورد. برای مثال، **گروهواره** مجموعه‌ای همراه با دستورالعملی است که از هر **دو** عضو مجموعه می‌توان عضوی از آن مجموعه را به دست آورد. از این رو، اشیای اولیه‌ی سازنده‌ی دستگاه‌های جبری، **مجموعه**ها هستند.

در این مقدمه، مطالبی را در باره‌ی مجموعه‌ها، توابع و بخش‌پذیری اعداد، به اندازه‌ی نیاز این کتاب، به اختصار یادآوری می‌کنیم. **معمولاً استاد درس مرور اکثر قسمت‌های این فصل را به عهده‌ی شما عزیزان می‌گذارد.**

م.۱ مجموعه و تابع

در این بخش برخی از مطالب و نمادگذاری‌های مربوط به مجموعه‌ها و توابع را به اختصار یادآوری می‌کنیم. در صورت نیاز بیش‌تر، به **کتاب** زیر مراجعه نمایید:

مبانی علوم ریاضی، دکتر محمد مهدی ابراهیمی و دکتر مژگان محمودی، انتشارات دانشگاه شهید بهشتی، ۱۳۹۱

م.۱.۱ نمادگذاری. یادآوری می‌کنیم که $\mathbb{N}$، $\mathbb{Z}$، $\mathbb{Q}$، $\mathbb{R}$، $\mathbb{C}$، به ترتیب، مجموعه‌ی اعداد طبیعی، صحیح، گویا، حقیقی، و مختلط هستند. همچنین، برای مثال، $\mathbb{Z}^* = \{x \in \mathbb{Z} \mid x \neq 0\}$، $\mathbb{R}^+ = \{x \in \mathbb{R} \mid x > 0\}$ و $\mathbb{Z}_n = \{0, 1, 2, \cdots, n-1\}$.

م.۱.۲ قضیه. *احکام زیر برای تابع* $f : A \to B$ *معادل هستند:*

۱- *تابع* f **یک به یک** *است، یعنی،*

$$(\forall x, y \in A) \quad f(x) = f(y) \Rightarrow x = y$$

۲- *تابع* f از **چپ حذف** *می شود، یعنی،*

$$(\forall g, h : C \to A) \quad f \circ g = f \circ h \Rightarrow g = h$$

۳- *اگر* $A \neq \emptyset$، *آنگاه تابع* f **وارون چپ** *دارد، یعنی،*

$$(\exists g : B \to A) \quad g \circ f = id_A$$

م.۳.۱ بحث در کلاس

۱- پس از بحث روی صورت قضیه‌ی **م.۲.۱**، آن را در منزل اثبات کنید. **جالب است!**

۲- دوگان قضیه‌ی **م.۲.۱** را برای **تابع پوشا** بنویسید، و سپس آن را در منزل اثبات کنید.

۳- اثبات کنید که تابع $f : A \to B$ دوسویی (یعنی، یک به یک و پوشا) است اگر و تنها اگر **یک-ریختی** (یعنی، **وارون‌پذیر**) باشد. در این صورت، می‌گوییم که A با B **یک‌ریخت** (یا همتوان) است و می‌نویسیم $A \cong B$.

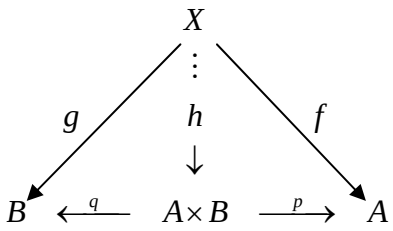
۴- **هشدار** می‌دهیم که قضیه‌ی **م.۲.۱**، و دوگان آن، برای **دستگاه‌های جبری** لزومی ندارد درست باشند (پیوست را ببینید).

۵- مهم‌ترین **ویژگی** حاصل‌ضرب دکارتی $A \times B = \{(a,b) \mid a \in A, b \in B\}$، قضیه‌ی جالب زیر است. این ویژگی در واقع **مشخص کننده‌ی** این شیء است. به این معنی که، هر مجموعه‌ای که دارای این ویژگی باشد، حتی اگر عضوهای آن برایمان معلوم نباشد، یقیناً با این مجموعه از زوج‌های مرتب **یک‌ریخت** است. حرف هایمان خیلی مجرد شد، و اگر در این لحظه متوجه‌ی منظورمان نشدید، نگران نباشید، به مرور با این چنین مطالب مجرد انس خواهید گرفت. فعلاً سعی کنید مطلب جالب و ساده‌ی زیر را درک کنید. ابتدا توابع تصویر را در زیر یادآوری می‌کنیم:

$$A \times B \xrightarrow{p} A \quad , \quad A \times B \xrightarrow{q} B$$
$$(a,b) \mapsto a \quad , \quad (a,b) \mapsto b$$

م.۴.۱ قضیه (ویژگی جهانی ضرب). *برای هر مجموعه چون X و هر دو تابع $f : X \to A$، $g : X \to B$، تابع منحصر به فرد $h : X \to A \times B$ وجود دارد به طوری که $p \circ h = f$ و $q \circ h = g$. (یعنی، مولفه‌ی اول $h(x)$ برابر با $f(x)$ و مولفه‌ی دوم آن $g(x)$ است. به این دلیل، گاهی نماد $f \times g$ یا (f,g) را برای h به کار می‌بریم).*

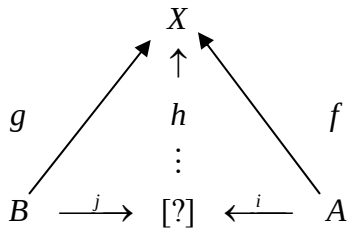
به زبان نموداری، می‌گوییم که **نمودار** زیر **تعویض‌پذیر** است. یعنی، تابع مرکب (مسیر) $X \xrightarrow{h} A \times B \xrightarrow{p} A$ همان تابع (مسیر) $X \xrightarrow{f} A$، و تابع مرکب (مسیر) $X \xrightarrow{h} A \times B \xrightarrow{q} B$ همان تابع (مسیر) $X \xrightarrow{g} B$ است:



م.۵.۱ بحث در کلاس. حال ببینیم که دوگان مفهوم ضرب مجموعه‌ها، که آن را **هم‌ضرب** می‌نامیم، چیست. حال بهتر متوجه می‌شویم که بند ۵ بحث م.۳.۱ چطور برای تعریف این مفهوم نا آشنا به یاریمان می‌آید! در این لحظه ممکن است ندانیم که عضوهای مجموعه‌ی **همضرب** مجموعه‌های A و B چه هستند، ولی می‌دانیم که با برعکس کردن پیکان‌ها، به دنبال مجموعه‌ای هستیم که توابعی از A و B به آن وجود دارند، یعنی

$$B \xrightarrow{j} \boxed{?} \xleftarrow{i} A$$

به طوری که برای هر مجموعه چون X و هر دو تابع چون $B \xrightarrow{g} X \xleftarrow{f} A$ به X، یک تابع **منحصر به فرد** چون $h:\boxed{?}\to X$ وجود دارد به طوری که مثلث‌های زیر تعویض‌پذیر باشند؟ (**به تغییر جهت پیکان‌ها نسبت به ویژگی جهانی ضرب توجه کنید.**)



اگر از درس **مبانی علوم ریاضی** به‌خاطر بیاورید، اجتماع مجزای

$$A \dot{\cup} B = (A \times \{1\}) \cup (B \times \{2\})$$

پاسخ به این سؤال است (**اثبات کنید، همتای این نوع مطالب را در درس‌های ریاضی بسیار خواهید دید**). دو مفهوم ضرب و همضرب مجموعه‌ها همتاهایی (نه لزوماً اجتماع مجزا) در مبحث جبر دارند که خواهیم دید.

مفهوم مهم دیگری را که بسیار ضروری است یادآوری کنیم، رابطه‌ی هم‌ارزی است. همان طور که در درس مبانی علوم ریاضی گفته شد، گاهی لازم است دو شئیی را که با هم یکی (مساوی) نیستند به دلایلی یکسان در نظر بگیریم. به تعریف مجرد زیر توجه کنید:

م.۶.۱ تعریف. رابطه‌ی $\sim$ روی A را **هم‌ارزی** می‌نامیم اگر

۱- **انعکاسی** باشد: برای هر $x \in A$، $x \sim x$.

۲- **متقارن** باشد: برای هر $x, y \in A$ ، "$x \sim y \Rightarrow y \sim x$".

۳- **متعدی** باشد: برای هر $x, y, z \in A$ ، "$(x \sim y \,\&\, y \sim z) \Rightarrow x \sim z$".

م.۷.۱ تعریف. فرض کنیم $\sim$ رابطه‌ای هم‌ارزی روی A باشد. در این صورت، مجموعه‌ی همه‌ی رده‌های $\{y \in X \mid y \sim x\}$ ، یعنی **افراز** $\bar{x} = [x] = \{y \in X \mid y \sim x\}$ را **خارج قسمت** A بر $\sim$ می‌نامیم.

همتای خارج قسمت را نیز برای دستگاه‌های جبری خواهیم دید، که **بسیار با اهمیت** است. چند نکته‌ی بسیار مهم مرتبط با این مفهوم وجود دارند که همتاهایی در بسیاری از دستگاه‌های ریاضی، به ویژه جبری، دارند که سه بار در این کتاب و چندین بار در درس‌های دیگر مطرح خواهند شد.

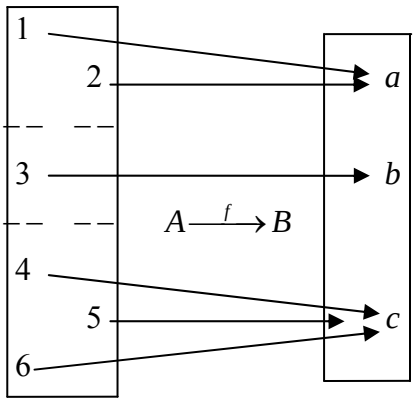
م.۸.۱ تعریف. فرض کنیم $f : A \to B$ تابع باشد. در این صورت، رابطه‌ی

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

را **هسته**‌ی f می‌نامیم. این رابطه را با نمادهایی چون $\sim_f$ ، $Kerf$ ، یا K_f نشان می‌دهیم.

بنابراین،

$$x \sim_f y \Leftrightarrow f(x) = f(y)$$



لم و قضیه‌ی زیر گویای اهمیت هسته‌ی توابع هستند.

م.۹.۱ لم. *فرض کنیم $f : A \to B$ تابع باشد. در این صورت،*

۱- *هسته‌ی f رابطه‌ای هم‌ارزی روی A است.*

۲- *و برعکس، هر رابطه‌ی هم‌ارزی $\sim$ روی A، هسته‌ی یک تابع است.* (یعنی، **تفاوتی اساسی بین دو مفهوم رابطه‌ی هم‌ارزی و هسته‌ی توابع وجود ندارد**).

۳- *تابع $f : A \to B$ یک به یک است اگر و تنها اگر $K_f = \Delta_A = \{(a,a) \mid a \in A\}$.*

اثبات

۱- نتیجه‌ی مستقیم تعریف رابطه‌ی هم‌ارزی K_f $\sim_f$ و خوش تعریفی تابع f است. **چطور؟**

۲- بر عکس، فرض کنیم $\sim$ رابطه‌ای هم‌ارزی روی A باشد. تابع طبیعی

$$\gamma : A \to A/\sim$$
$$a \mapsto [a]$$

را در نظر بگیرید. در زیر نشان می‌دهیم که رابطه‌ی هم‌ارزی $\sim$ برابر با هسته‌ی تابع γ است، یعنی $\sim = \sim_\gamma$. (مراحل زیر را توضیح دهید):

$$a \sim_f a' \Leftrightarrow \gamma(a) = \gamma(a') \Leftrightarrow [a]_\sim = [a]_\sim \Leftrightarrow a \sim a'$$

۳- کافی است توجه کنیم که $K_f = \Delta_A$ اگر و تنها اگر

$$\{(a,a') \mid f(a) = f(a')\} = \{(a,a) \mid a \in A\}$$

یعنی

$$f(a) = f(a') \Leftrightarrow a = a'$$

قضیه‌ی اساسی توابع بیان می‌کند که نگاره‌ی توابع (یا همان همدامنه‌ی توابع پوشا) چیزی جز خارج قسمت مجموعه‌ها نیست. همتای این قضیه و کاربردهای آن را در مطالعه‌ی همه‌ی دستگاه‌های جبری خواهیم دید. برخی ترجیح می‌دهند که این قضیه را تنها در دستگاه‌های جبری مطالعه کنند، ولی تصدیق خواهید کرد که بهتر است ابتدا آن را برای مجموعه‌ها اثبات کنیم، زیرا بیشتر قسمت‌های صورت و اثبات ساده‌ی آن در واقع مربوط به مبحث مبانی علوم ریاضی است!

م.۱۰.۱ قضیه‌ی اساسی توابع. *فرض کنیم $f : A \to B$ تابع و رابطه‌ی هم‌ارزی $\sim_f$ هسته‌ی آن باشد. در این صورت،*

$$A/\sim_f \cong f(A)$$

به ویژه، اگر f پوشا باشد، آنگاه $A/\sim_f \cong B$.

اثبات. اگر چه احتمالاً اثبات آن را از کتاب **مبانی علوم ریاضی** به خاطر می‌آورید، به دلیل اهمیت آن و اینکه دست‌کم سه بار دیگر آن را در همین کتاب خواهید دید، **توجه شما را به اثبات ساده‌ی آن جلب می‌کنیم.** تابع طبیعی

$$\begin{aligned} \overline{f} : A/\sim_f &\to f(A) \\ [a] &\mapsto f(a) \end{aligned}$$

را (که خود شما به آسانی می‌توانستید تعریف کنید) در نظر بگیرید. در درس مبانی علوم ریاضی آموختیم که هرگاه تابعی بر حسب نماینده‌های رده‌های یک رابطه‌ی هم‌ارزی تعریف شود، حتماً باید خوش‌تعریفی آن را بررسی کنیم، یعنی نشان دهیم که تعریف $\overline{f}$ به انتخاب a، یعنی نماینده‌ی رده‌ی $[a]$، بستگی ندارد. به اثبات ساده و طبیعی زیر توجه کنید:

$$\begin{aligned} [a]=[a'] &\Rightarrow a \sim_f a' \\ &\Rightarrow f(a)=f(a') \\ &\Rightarrow \overline{f}([a])=\overline{f}([a']) \end{aligned}$$

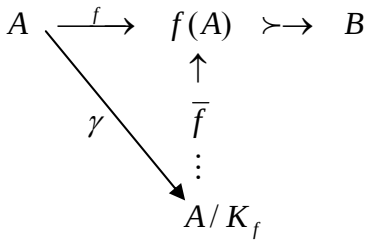
حال که خوش‌تعریف بودن $\overline{f}$ اثبات شد، نشان می‌دهیم که $\overline{f}$ یک به یک و پوشا است. پوشا بودن $\overline{f}$ روشن است، **این طور نیست؟** برای اثبات یک به یک بودن $\overline{f}$، باید نشان دهیم که

$$\overline{f}([a])=\overline{f}([a']) \Rightarrow [a]=[a']$$

با نگاهی به اثبات خوش‌تعریفی $\overline{f}$، متوجه می‌شویم که اگر مراحل آن را وارونه کنیم، به نتیجه می‌رسیم. این مطالب قضیه را اثبات می‌کنند. ■

م.۱۱.۱ بحث در کلاس

۱- نمودار تعویض‌پذیر زیر برای به خاطر سپردن صورت و اثبات قضیه‌ی اساسی توابع مفید است.



۲- رابطه‌ی همنهشتی به پیمانه‌ی n را روی $\mathbb{Z}$ به خاطر بیاورید:

$$x \equiv_n y \quad \Leftrightarrow \quad (\exists k \in \mathbb{Z}) \quad x - y = kn$$

گاهی به جای $x \equiv_n y$ می نویسیم $x \equiv y (\mathrm{mod}\, n)$ یا ($x \equiv y (n$ به پیمانه‌ی $)$. روشن است که

$$\mathbb{Z}/\equiv_n = \{[0],[1],\cdots,[n-1]\} \cong \mathbb{Z}_n = \{0,1,\cdots,n-1\}$$

ولی می‌خواهیم این مطلب را با استفاده از قضیه‌ی اساسی نیز نشان دهیم. برای این کار، تابع پوشای زیر را در نظر بگیرید:

$$\begin{aligned} f : \mathbb{Z} &\to \mathbb{Z}_n \\ x &\mapsto (\text{باقی‌مانده‌ی تقسیم } x \text{ بر } n) \end{aligned}$$

در این صورت، به آسانی می‌توانید نشان دهید که رابطه‌ی هم‌ارزی K_f برابر با $\equiv_n$ است (یعنی $x \equiv_n y$ اگر و تنها اگر باقی‌مانده‌ی تقسیم x بر n برابر با باقی‌مانده‌ی تقسیم y بر n باشد). حال، بنابر قضیه‌ی اساسی،

$$\mathbb{Z} / K_f = \mathbb{Z}/\equiv_n \cong \mathbb{Z}_n$$

به عنوان کاربرد دیگری از این قضیه، تمرین مهم ۸ این بخش را نیز ببینید.

همان طور که در سخنی با دانشجو گفتیم، تمرین‌ها قسمت بسیار مهمی از هر درس ریاضی هستند. در صورتی که بار اول موفق نشدید تمرینی را حل کنید، نا امید نشوید. تلاش برای حل کردن یک تمرین، حتی اگر به جواب کامل منتهی نشود، مفیدتر از مطالعه‌ی چند تمرین حل شده است.

موفق می‌شوید!

تمرین م۱.

۱- پاسخ به سؤال‌های بحث م۳.۱. را فراموش نکنید.

۲- با استفاده از قضیه‌ی م۴.۱. (ویژگی جهانی ضرب) نمودار

$$\begin{array}{ccccc} A & \xleftarrow{p} & A\times B & \xrightarrow{q} & B \\ \downarrow f & & \vdots & & \downarrow g \\ & & ? & & \\ & & \downarrow & & \\ A' & \xleftarrow{p'} & A'\times B' & \xrightarrow{q'} & B' \end{array}$$

را با تعریف تابع طبیعی زیر کامل کنید (توجه کنید که تابع f هر عضو متعلق به A را به عضوی متعلق به A' نظیر می‌کند. تابع g **چطور؟**) :

$$h: A\times B \to A'\times B'$$
$$(a,b) \mapsto (? \in A', ? \in B')$$

۳- با استفاده از بحث **م.۵.۱**، دوگان تمرین بالا را بیان و حل‌کنید. (ترسی به دل راه ندهید، **شما می‌توانید**).

۴- فرض کنیم که $\mathcal{P}_X$ و $\mathcal{E}_X$، به ترتیب، مجموعه‌ی همه‌ی افرازهای روی مجموعه‌ی X و مجموعه‌ی همه‌ی رابطه‌های هم‌ارزی روی X باشند. نشان دهید که تناظری دوسویی بین این دو مجموعه وجود دارد؛ یعنی، $\mathcal{P}_X \cong \mathcal{E}_X$. (برای هر افراز روی X یک رابطه‌ی هم‌ارزی روی X تعریف کنید، و برعکس).

۵- به دو روش تابع $A \xrightarrow{f} B$ را به صورت $f = h \circ g$ تجزیه کنید به طوری که g پوشا و h یک به یک باشد. یعنی به‌گونه‌ای که نمودار زیر تعویض‌پذیر باشد:

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ & {\scriptstyle g}\searrow \quad \nearrow{\scriptstyle h} & \\ & C & \end{array}$$

۶- فرض کنید $X = \mathbb{Z}\times\mathbb{Z}^* = \{(m,n) \mid m,n \in \mathbb{Z}, n \neq 0\}$. تابع

$$f: \mathbb{Z}\times\mathbb{Z}^* \to \mathbb{Q}$$
$$(m,n) \mapsto \frac{m}{n}$$

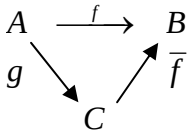
را در نظر بگیرید. ابتدا هسته‌ی f را مشخص کنید و سپس با استفاده از قضیه‌ی اساسی توابع، نتیجه بگیرید که $(\mathbb{Z}\times\mathbb{Z}^*)/\sim_f \cong \mathbb{Q}$.

۷- (**مهم**) تابع پوشای $f : X \to Y$ را در نظر بگیرید. فرض کنید $\mathcal{E}_Y$ مجموعه‌ی همه‌ی رابطه‌های هم‌ارزی روی Y و

$$\mathcal{T}_X = \{\sim \in \mathcal{E}_X \mid \sim_f \subseteq \sim\}$$

مجموعه‌ی همه‌ی رابطه‌های هم‌ارزی روی X باشد که شامل هسته‌ی f هستند. نشان دهید که تناظری دوسویی بین این دو مجموعه وجود دارد.

۸- (تمرینی مهم و جالب است) می‌گوییم که تابع $f : A \to B$ از طریق تابع $g : A \to C$ (تحت ترکیب) **تجزیه** می‌شود، و می نویسیم $g \mid f$، اگر تابع $\overline{f} : C \to B$ با ویژگی $f = \overline{f} \circ g$ وجود داشته باشد. به زبان نمودار،



تعویض‌پذیر است. برای مثال، قضیه‌ی اساسی توابع بیان می‌کند که $f \mid \gamma$. حال **تعمیم مهم قضیه‌ی اساسی توابع** را، که به صورت زیر است، اثبات کنید:

(الف) تابع f از طریق g تجزیه می‌شود اگر و تنها اگر $K_g \subseteq K_f$.

(ب) تابع $\overline{f}$، در صورت وجود، منحصر به فرد است.

(پ) تابع $\overline{f}$ یک به یک است اگر و تنها اگر $K_g = K_f$.

(ت) تابع $\overline{f}$ پوشا است اگر و تنها اگر f پوشا باشد.

(ث) قضیه‌ی اساسی توابع حالت خاص این قضیه است.

۲.م نظریه‌ی اعداد

در این بخش کوتاه مطالبی را از نظریه‌ی اعداد، به ویژه در مورد بخش‌پذیری، که در این کتاب مورد نیاز هستند، فهرست‌وار می‌آوریم.

۱.۲.م اصل خوش‌ترتیبی. هر زیرمجموعه‌ی ناتهی از اعداد طبیعی دارای کوچک‌ترین عضو است.

۲.۲.م اصل استقرا. فرض کنیم $p(n)$ گزاره‌نمایی روی اعداد طبیعی باشد به طوری که

(الف) $p(1)$ درست است.

(ب) گزاره‌ی "$p(n) \Rightarrow p(n+1)$" نیز درست است.

در این صورت، $p(n)$ برای هر $n \in \mathbb{N}$ درست است.

م.۲.۳ بخش‌پذیری. می‌گوییم که عدد طبیعی m عدد طبیعی n را **می‌شمارد**، و می‌نویسیم $m \mid n$، اگر عدد طبیعی q با ویژگی $n = mq$ وجود داشته باشد.

م.۲.۴ قضیه. احکام زیر در $\mathbb{N}$ برقرار هستند:

(الف) $a \mid a$

(ب) $a \mid b \Rightarrow a \mid bc$

(پ) $a \mid b, a \mid c \Rightarrow a \mid bx + cy$

(ت) $a \mid b, b \mid c \Rightarrow a \mid c$

(ث) $a \mid b, b \mid a \Rightarrow a = b$

(ج) $a \mid b \Rightarrow ka \mid kb$

م.۲.۵ الگوریتم تقسیم. فرض کنیم $m, n \in \mathbb{Z}$ و $n \neq 0$. در این صورت، اعداد صحیح یکتایی چون q و r وجود دارند به طوری که

$$m = nq + r \qquad 0 \leq r < |n|$$

م.۲.۶ می‌گوییم که عدد طبیعی d **بزرگ‌ترین مقسوم علیه مشترک** اعداد طبیعی m و n است، و می‌نویسیم $d = (m, n)$، اگر

(الف) $d \mid m, d \mid n$

(ب) $e \mid m, e \mid n \Rightarrow e \mid d$

م.۲.۷ می‌گوییم که عدد طبیعی k **کوچک‌ترین مضرب مشترک** اعداد طبیعی m و n است، و می‌نویسیم $k = [m, n]$، اگر

(الف) $m \mid k, n \mid k$

(ب) $m \mid l, n \mid l \Rightarrow k \mid l$

م.۲.۸ (عدد اول). عدد طبیعی $p > 1$ را **اول** می‌گوییم اگر تنها مقسوم علیه‌های آن 1 و p باشند. می‌توان نشان داد که این تعریف معادل است با "$p \mid b$ یا $p \mid a$ $\Rightarrow p \mid ab$". دو عدد m و n را **متباین** یا **نسبت به هم اول** می‌گوییم اگر $(m, n) = 1$، که معادل است با وجود $x, y \in \mathbb{Z}^*$ به طوری که $mx + ny = 1$.

م.۲.۹ قضیه. فرض کنیم $d = (m, n)$ و $k \in \mathbb{N}$. در این صورت،

۱- $\left(\frac{m}{d}, \frac{n}{d}\right) = 1$

۲- $m \mid nk, (m, n) = 1 \Rightarrow m \mid k$

۳- $m \mid nk \Rightarrow \frac{m}{d} \mid k$

م.۲.۱۰ قضیه‌ی اساسی حساب. فرض کنیم $m>1$. در این صورت،

۱- اعداد اول p_1، $\cdots$، p_r وجود دارند به طوری که $m=p_1p_2\cdots p_r$.

۲- این تجزیه به تعبیر زیر یکتا است:

$$m=p_1p_2\cdots p_r=q_1q_2\cdots q_s\Rightarrow r=s\ \&\ \{p_1,p_2,\cdots,p_r\}=\{q_1,q_2,\cdots,q_s\}$$

تمرین م.۲

یقین داریم که موفق می‌شوید

۱- نشان دهید که

$$(m,n)=1, d\mid mn\Rightarrow(\exists!d_1,d_2),\quad d=d_1d_2, d_1\mid m, d_2\mid n$$

۲- نشان دهید که $(m,n)[m,n]=mn$ و نتیجه بگیرید که

$$(m,n)=1\Rightarrow[m,n]=mn$$

۳- فرض کنید p عددی اول و k عددی طبیعی باشد. نشان دهید که $\varphi(p^k)=p^k-p^{k-1}$، که در آن φ تابع فی اویلر با تعریف $\varphi(n)=|\{0<k<n\mid(k,n)=1\}|$ است.

۴- فرض کنید اعداد طبیعی n_1، $\ldots$، n_k دو به دو نسبت به هم اول هستند. نشان دهید که

$$\varphi(n_1\cdots n_k)=\varphi(n_1)\cdots\varphi(n_k)$$

۵- فرض کنید دو عدد از سه عدد m، n، و a نسبت به هم اول باشند. نشان دهید که $(a,mn)=(a,m)(a,n)$. به ویژه، ثابت کنید که اگر $(a,m)=1=(a,n)$ آنگاه $(a,mn)=1$.

۶- فرض کنید k کوچکترین عدد صحیح و مثبت باشد به طوری که $m\mid k$ و $n\mid k$. ثابت کنید که $k=[m,n]$.

۷- فرض کنید $(a,b)=1$، $a\mid m$ و $b\mid m$. نشان دهید که $ab\mid m$.

فصل ۱

آشنایی با دستگاه‌های جبری

هدف و مزایای این فصل چیست؟ توجه می‌کنیم که، برای یک پزشک ممکن است تنها کافی باشد که چگونگی و اندازه‌ی استفاده از دارو را بداند، ولی **دانشمند علوم** مرتبط با پزشکی، نیازمند **شناخت عمیق‌تری** از این مواد است؛ همچنان که گیاه شناس لازم است اطلاعات بیشتری در باره‌ی گیاهان بداند تا گیاه فروش یا میوه فروش! به همین ترتیب، کاربر برنامه‌های کامپیوتری ممکن است نیاز چندانی به چگونگی تولید آن برنامه‌ها نداشته باشد، ولی برنامه‌نویسان هر چه از جزییات برنامه‌های خاص و زیربنای برنامه‌ها به طور عام اطلاع بیشتری داشته باشند، بهتر می‌توانند برنامه‌هایی کاراتر تهیه کنند. **این طور نیست؟!**

با این مقدمه، **روشن است که** **دانشجوی علوم ریاضی** (ریاضی، آمار، و علوم کامپیوتر)، و **دانشجوی علوم** به طور عام، لازم است، تا اندازه‌ای که به مقطع تحصیلی او مربوط می‌شود، **به طور دقیق** بداند که در هر مبحث از علم، به ویژه ریاضیات، با چه مفاهیمی مواجه است و ماهیت و نقش دقیق این مفاهیم چیست! باید خواستگاه، بنیاد، منبع، سرچشمه، و علت معرفی مفاهیم را بدانیم تا بهتر آن‌ها را به کار ببریم و خود، هنگام نیاز، سازنده‌ی مفاهیم جدید باشیم! **این طور نیست؟**

یکی از اهداف مبحث **جبر جامع**، تشخیص و کشف مفاهیم و ویژگی‌های **بنیادی مشترک** بین دستگاه‌های جبری شناخته شده‌ای چون نیم‌گروه، گروه، حلقه، فضای برداری، مدول، . . .، و مطالعه‌ی دقیق‌تر و کلی‌تر آن‌ها است. در این صورت، وقتی این مفاهیم یا ویژگی‌ها در دستگاه جبری ناآشنایی با ظاهری مبدل نمایان می‌شوند بهتر می‌توانیم آن‌ها را شناسایی کنیم و برخوردی فنی و اصولی با آن‌ها داشته باشیم.

خواهیم دید که مطالب این فصل، به ویژه در بخش‌های **۱** تا **۴**، به صورتی نسبتاً خودآموز بیش‌تر به توصیف مطالب و ارائه‌ی مثال می‌پردازد و وقت چندانی از کلاس درس را نمی‌گیرند تا اینکه زمان بیشتری برای بخش‌های اساسی‌تر بعدی این فصل باقی بماند.

۱.۱ عمل n– تایی

بنیادی‌ترین مفهوم در شناخت و معرفی دستگاه‌های جبری، مفهوم **عمل** است. از این رو گاهی می‌گویند که

جبر مطالعه‌ی عمل‌ها است

با عمل‌ها از همان دوران کودکی آشنا شدیم. پس از آشنایی با اعداد طبیعی ۱، ۲، ۳، . . .، رفته رفته در سالهای بعد، با انواع دیگر اعداد، مانند اعداد صحیح، گویا، اصم، حقیقی، و اعداد مختلط آشنا شدیم و **چهار عمل اصلی** جمع، تفریق، ضرب، و تقسیم اعداد را آموختیم. به مرور پی بردیم که اشیای دیگری چون توابع و بردارها را نیز می‌توانیم با هم جمع، در هم ضرب، یا با هم ترکیب کنیم. همچنین، دیدیم که برای محاسبه‌ی برخی از کمیت‌ها، مانند حجم اجسام، به بیش از دو کمیت نیاز است. برای نوشتن عبارت **مبانی جبر** به چند کلمه یا به چند حرف نیاز داریم؟

با نگاهی دقیق‌تر و ریاضی‌گونه به این عمل‌ها، متوجه می‌شویم که هر یک چیزی جز تابعی با یک یا **چند ورودی** و **یک خروجی** نیست. از این رو، تعریف مجرد و **جامع** زیر را داریم.

۱.۱.۱ تعریف. فرض کنیم A مجموعه و n عددی طبیعی یا صفر است. هر **تابع**

$$\lambda^A : A^n \to A$$

را یک **عمل** n– **تایی در** یا **روی** A می‌نامیم.

یادآوری می‌کنیم که A^n همان حاصلضرب دکارتی

$$A^1 = A, \quad A^2 = A \times A, \quad A^3 = A \times A \times A, \cdots$$

و مجموعه‌ی A^0 مجموعه‌ای تک عضوی است. **چطور؟**

۲.۱.۱ بحث در کلاس. گرچه تعریف بالا روشن است و نیازی به تفسیر ندارد، ولی از آنجا که در این درس **عمل‌های صفر**، **یک**، و **دوتایی** از اهمیت ویژه‌ای برخوردار هستند، خواندن مطالب زیر مفید است!

۱– گاهی در حاشیه‌ی همایش‌های ریاضی، برخی از دانشجویان، حتی دانشجویان دوره‌های تحصیلات تکمیلی، ابراز می‌کنند که با عمل **صفرتایی** مشکل دارند. این موضوع باعث تعجب نمی‌شود و از اعتبار دانش آن‌ها نیز کم نمی‌کند. البته، وقتی توضیح داده می‌شود، به بدیهی بودن آن پی‌می‌برند! به هر حال، **پرسیدن عیب نیست!**

به زبانی ساده، چون A^0 مجموعه‌ای تک عضوی مانند $\{\varnothing\}$، $\{0\}$، $\{*\}$، است (زیرا، برای هر عدد طبیعی n، مجموعه‌ی A^n با مجموعه‌ی توابع $A^{\{1,2,\cdots,n\}}$ (از $\{1,2,\cdots,n\}$ به A) یک‌ریخت است، پس طبیعی است که

$$A^0 \cong A^{\varnothing} = \{\varnothing : \varnothing \to A\}$$

مجموعه‌ای تک عضوی است، زیرا تنها یک تابع و آن تابع تهی از مجموعه‌ی $\varnothing$ به هر مجموعه‌ی A وجود دارد). آیا درست است که هر عمل صفرتایی چون

$$\lambda^A : A^0 = \{0\} \to A$$

عضوی از A را مشخص می‌کند؟ البته که درست است! از این رو، گاهی برای راحتی، عمل صفرتایی λ^A را با نگاره‌اش $\lambda^A(0) = a_0 \in A$ نشان می‌دهیم و می‌نویسیم

$$\begin{aligned} a_0 : \{0\} &\to A \\ 0 &\mapsto a_0 \end{aligned}$$

چند عمل صفرتایی در مجموعه‌ای پنج عضوی می‌توان تعریف کرد؟ در مجموعه‌ی $\mathbb{N}$ **چطور؟** در مجموعه‌ی تهی $\varnothing$ **چطور؟**

۲- با عمل ۱- تایی (که آن را عمل **یکانی** نیز می‌نامیم) و کاربردهای آن در سراسر علوم بسیار آشنا هستید، ولی ممکن است این نامگذاری را به کار نبرده باشید. در حقیقت، چون $A^1 = A$، هر عمل یکانی در A چیزی جز **تابعی** روی A، مانند $\lambda : A \to A$، نیست! چند عمل یکانی در مجموعه‌ی پنج عضوی می‌توان تعریف کرد؟ در $\varnothing$ چطور؟ تعدادی عمل یکانی در $\mathbb{Z}$ تعریف کنید. عمل‌های یکانی قرینه‌یابی و وارون‌گیری را بسیار به کار خواهیم برد:

$$\begin{aligned} -_{\cdot} : \mathbb{Z} &\to \mathbb{Z} & \qquad \cdot^{-1} : \mathbb{R}^* &\to \mathbb{R}^* \\ n &\mapsto -n & \qquad x &\mapsto x^{-1} \end{aligned}$$

۳- ممکن است تصور کنید که با عمل آشنای دوتایی $\lambda : A \times A \to A$ مشکلی ندارید! یقیناً چنین است. ولی از آنجا که در دروس ریاضی و کاربردهای آن، عمل دوتایی نقشی اساسی ایفا می‌کند، اجازه دهید چند دقیقه‌ای بیشتر به آن اختصاص دهیم. نخست اینکه، برای ساده نویسی حاصل عمل دوتایی، نمادگذاری‌های مجموع و حاصلضرب اعداد را الگو قرار می‌دهیم و به جای نمادگذاری طولانی $\lambda((x,y))$ می‌نویسیم $x\lambda y$، و حتی از این هم فراتر می‌رویم و نمادهایی چون $*$ را به‌جای λ به کار می‌بریم و می‌نویسیم $x * y$! یا حتی گاهی نمادهای متداول جمع و ضرب اعداد را به کار می‌بریم و می‌نویسیم $x + y$، $x \cdot y$، یا ساده تر از همه، xy، حتی اگر x و y اصلاً عدد نباشند (!) (یعنی،

صرفاً به عنوان نماد و علامت به کار می روند). ولی ما تا مدت‌ها، بـه ویـژه در ایـن فصـل، اغلـب همـان نمادگذاری $x*y$ را به کار می‌بریم تا اشتباه برانگیز نباشد.

چند عمل دوتایی در مجموعه‌ی سه عضـوی وجـود دارد؟ (آیـا $3^9=19683$ درسـت اسـت؟) در مجموعه‌ی یک عضوی یا در مجموعه‌ی تهی **چطور؟** ($\varnothing:\varnothing\times\varnothing\to\varnothing$). آیا دستورالعمل

$$\min:\mathbb{N}\times\mathbb{N}\to\mathbb{N}$$
$$(m,n)\mapsto\min\{m,n\}$$

عملی دوتایی در $\mathbb{N}$ است؟ (این عمل به ویژه در علوم کامپیوتر نظری با اهمیت است!) تعدادی عمل ۲ و ۳- تایی در $\mathbb{R}$ تعریف کنید. برای مثال،

$$\mathbb{R}\times\mathbb{R}\times\mathbb{R}\to\mathbb{R}$$
$$(x,y,z)\mapsto xy+xz+5$$

۴- احتمـالاً برایتـان جالـب اسـت کـه، بـرای مثـال، از هـر تـابع ۳- متغیـره‌ی $f:A\times B\times C\to D$ و هر $a\in A$، یک تابع با دو متغیر

$$f_a:B\times C\to D$$
$$(b,c)\mapsto f(a,b,c)$$

بـه دسـت مـی‌آیـد. بـه همـین صـورت سـاده، جالـب اسـت کـه از هـر عمـل دوتـایی $*:A\times A\to A$ و هر $a\in A$، دو عمل یکانی

$$r_a:A\to A,\qquad l_a:A\to A$$
$$x\mapsto x*a,\qquad x\mapsto a*x$$

به دست می‌آیند که r_a را **انتقال راست** و l_a را **انتقال چپ** به اندازه‌ی a می‌نامیم. از ایـن رو، از هـر عمل دوتایی، دو خانواده‌ی زیر از عمل‌های یکانی به دست می‌آیند:

$$(A\xrightarrow{r_a}A)_{a\in A}\quad,\quad(A\xrightarrow{l_a}A)_{a\in A}$$

و برعکس، هر یک از این دو خانواده عمل دوتایی $*$ را باز پس می‌دهند. **چطور؟**

۳.۱.۱ خوش‌تعریفی. توجه کنید که هر عمـل n- تـایی در A **تـابعی** چـون $\lambda:A^n\to A$ است، وبنابراین باید دارای دو شرط زیر باشد:

(ع۱) (**بسته بودن**) برای هر $a_1,a_2,\cdots,a_n\in A$، داریم $\lambda(a_1,a_2,\cdots,a_n)\in A$.

(ع۲) (**یکتایی**) هر عضو A^n تنها یک نگاره در A دارد. یعنی،

$$(a_1,\cdots,a_n)=(b_1,\cdots,b_n)\Rightarrow\lambda(a_1,\cdots,a_n)=\lambda(b_1,\cdots,b_n)$$

وقتی می‌گوییم که عمل دوتایی $*$ در A **خوش‌تعریف** است، منظور این است که $*: A\times A\to A$ به واقع تابع است، یعنی در شرایط بسته بودن و یکتایی بالا صدق می‌کند. این شرایط با نمادگذاری $x*y$ به صورت زیر نوشته می‌شوند:

(ع۱) (**بسته بودن**) برای هر $x,y\in A$ ، $x*y\in A$.

(ع۲) (**یکتایی**) $\begin{cases} a=a' \\ b=b' \end{cases} \Rightarrow a*b=a'*b'$

ممکن است در بررسی خوش‌تعریفی عمل‌ها مشکل داشته باشید. از این رو، با دقت بیشتری در بحث‌های زیر شرکت کنید!

۴.۱.۱ بحث در کلاس. اگر پاسخ به هر یک از سؤال‌های زیر منفی است، مشخص کنید که کدام شرط **بسته بودن** یا **یکتایی** برقرار نیست (و کدام برقرار است!)

۱- آیا جمع و ضرب معمولی اعداد در $\{1,2,\cdots,9\}$ خوش‌تعریف هستند؟

۲- آیا اجتماع و اشتراک در $\{\{a\},\{b\},\{a,b\}\}$ عمل‌هایی خوش‌تعریف هستند؟ در $\mathcal{P}(\{a,b\})$ چطور؟

ممکن است منتظر باشید بدانید که **دستگاه جامع جبری چیست؟** کمی دیگر باید صبر کنید تا خیال ما و استاد درس راحت شود که با عمل‌ها، به ویژه بررسی خوش‌تعریفی آن‌ها، در آینده مشکلی نخواهید داشت. در بحث زیر سطح سؤال‌ها را کمی بالاتر می‌بریم.

۵.۱.۱ بحث در کلاس

۱- فرض کنیم $\mathbb{Z}_n=\{0,1,\cdots,n-1\}$. روشن است که عمل‌های دوتایی زیر در $\mathbb{Z}_n$ خوش‌تعریف هستند:

$$a\oplus_n b=\text{(باقی‌مانده‌ی حاصل از تقسیم } a+b \text{ بر } n\text{)}$$
$$a\odot_n b=\text{(باقی‌مانده‌ی حاصل از تقسیم } ab \text{ بر } n\text{)}$$

۲- این سؤال بسیار مشابه با بند ۱ است، ولی تشابه آن مخفی است! حال مجموعه‌ی

$$\mathbb{Z}/\equiv_n=\{[0],[1],\cdots,[n-1]\}=\{\overline{0},\overline{1},\cdots,\overline{n-1}\}$$

متشکل از رده‌های هم‌ارزی نسبت به رابطه‌ی همنهشتی به پیمانه‌ی n را در نظر بگیرید. بررسی کنید که عمل‌های دوتایی زیر در این مجموعه خوش‌تعریف هستند:

$$[a]\bar{\oplus}_n[b]=[a+b] \qquad , \qquad [a]\bar{\odot}_n[b]=[ab]$$

توجه کنید که هر رده‌ی $[x]$ متعلق به $\mathbb{Z}/\equiv_n$ است. برای مثال، $[100]$ در $\mathbb{Z}/\equiv_3$ برابر با $[1]$ است. **چطور؟** همچنین، برای مثال، $\bar{\oplus}_n$ در شرط یکتایی صدق می‌کند، زیرا

$$\begin{cases}[a]=[a']\\ [b]=[b']\end{cases}\Rightarrow\begin{cases}a-a'=nk\\ b-b'=nl\end{cases}\Rightarrow (a+b)-(a'+b')=n(k+l)$$
$$\Rightarrow[a+b]=[a'+b']$$
$$\Rightarrow[a]\bar{\oplus}_n[b]=[a']\bar{\oplus}_n[b']$$

۳- روشن است که

$$[a]\bar{\oplus}_n[b]=[a+b]=[a\oplus_n b]$$
$$[a]\bar{\odot}_n[b]=[ab]=[a\odot_n b]$$

از این رو، اساساً تفاوتی نمی‌کند که عمل‌های $\oplus_n$ و $\odot_n$ را در $\mathbb{Z}_n=\{0,1,\cdots,n-1\}$ یا همتای‌های آن‌ها، $\bar{\oplus}_n$ و $\bar{\odot}_n$، را در $\mathbb{Z}/\equiv_n=\{[0],[1],\cdots,[n-1]\}$ در نظر بگیریم. بنابراین، اجازه بدهید، برای راحتی کار و اگر امکان اشتباه نباشد، گاهی آزادانه نماد جمعی $+_n$ را برای نمایش هر دو عمل $\oplus_n$ و $\bar{\oplus}_n$، و مجموعه‌ی $\mathbb{Z}_n$ را برای هر دو مجموعه‌ی $\mathbb{Z}_n$ و $\mathbb{Z}/\equiv_n$ به‌کار ببریم، و $+_n$ را **جمع همنهشتی به پیمانه‌ی** n بنامیم (البته، نوشته‌هایمان به خودی خود مشخص می‌کنند که این عمل‌ها را در $\{0,1,\ldots,n-1\}$ یا در $\{[0],[1],\ldots,[n-1]\}$ انجام می‌دهیم). به همین صورت، می‌توانیم نماد ضربی $\cdot_n$ را برای نمایش هر دو عمل $\odot_n$ و $\bar{\odot}_n$ به‌کار ببریم، و آن را **ضرب همنهشتی به پیمانه‌ی** n بنامیم.

۴- (اختیاری) ممکن است تصور کنیم که عمل‌هایی که با دستور یا فرمولی حق به جانب تعریف می‌شوند، یقینا خوش‌تعریف هستند! برای اینکه **هشدار** بدهیم که **لزومی ندارد که هر شئ با ظاهری حق به جانب درست هم کار کند، در بحث زیر شرکت کنید.**

۶.۱.۱ بحث در کلاس. دستورالعمل طبیعی توان

$$[a]*[b]=[a]^{[b]}=[a^b]$$

را در $\mathbb{Z}/\equiv_3$ در نظر بگیرید. برای مثال، داریم $[2]^{[2]}=[2^2]=[4]=[1]$ زیرا $4\equiv_3 1$.
ملاحظه می‌کنیم که دستور عمل بالا ظاهری حق به جانب و موجه دارد و حتی $\mathbb{Z}/\equiv_3$ نسبت به این، به ظاهر عمل دوتایی توان، **بسته** است. همچنین، با این دستور فریبنده حتی می‌توانید قضیه‌هایی را در باره‌ی قوانین توان اثبات کنید. برای مثال،

$$[a]^{[b]\bar{\oplus}_3[c]}=[a]^{[b+c]}=[a^{b+c}]=[a^b a^c]=[a^b]\bar{\odot}_3[a^c]=[a]^{[b]}\bar{\odot}_3[a]^{[c]} \qquad (!!)$$

ولی، همه‌ی این‌ها خوش خیالی است، زیرا * اصلاً **خوش‌تعریف نیست!** برای مثال، داریم $[2]=[5]$ و $[2]=[2]$، در حالی که

$$[2]^{[5]}=[2^5]=[2]\neq[1] \quad \text{و} \quad [2]^{[2]}=[2^2]=[4]=[1]$$

پس، شرط **یکتایی** خوش‌تعریفی عمل **نقض می‌شود!** چه نکته‌ای دستور به ظاهر موجه * را رسوا کرد؟ نکته‌ی باریک همان است که قبلا نیز **هشدار** دادیم: یک رده‌ی هم‌ارزی نماینده‌های متفاوت دارد! در واقع، هر عضو در یک رده‌ی هم‌ارزی نماینده‌ی آن رده است. از این رو، باید اطمینان حاصل می‌کردیم که نماینده‌های متفاوت اثری در حاصل دستور * ندارند، که متاسفانه در مورد بالا چنین نبود! خوشبختانه این اشکال در عمل‌های $+_n$ و $\cdot_n$ در $\mathbb{Z}/\equiv_n$ به وجود نمی‌آید.
حال که به اهمیت این موضوع پی بردید، در بحث زیر فعال‌تر شرکت کنید (مورد کلی‌تر این عمل-ها را در فصل **۳** خواهیم دید.)

۷.۱.۱ بحث در کلاس

۱- نشان دهید که جمع و ضرب معمولی اعداد گویا که به صورت زیر داده می‌شوند، خوش تعریف هستند (این مثال دبستانی **سهل و ممتنع** است):

$$\frac{m}{n}+\frac{r}{s}=\frac{ms+rn}{ns} \qquad , \qquad \frac{m}{n}\cdot\frac{r}{s}=\frac{mr}{ns}$$

باید درستی شرایط **(ع۱)** و **(ع۲)** خوش‌تعریفی را اثبات کنیم.
(ع۱) (**بسته بودن**): چون $n,s\neq 0$، پس در $\mathbb{Z}$ داریم $ns\neq 0$ و در نتیجه، حاصل دستور هر دو عمل، اعدادی گویا هستند.
(ع۲) (**یکتایی**) باید نشان دهیم که

$$\begin{cases} \frac{m}{n}=\frac{m'}{n'} \\ \frac{r}{s}=\frac{r'}{s'} \end{cases} \Rightarrow \frac{m}{n}+\frac{r}{s}=\frac{m'}{n'}+\frac{r'}{s'} \quad \& \quad \frac{m}{n}\cdot\frac{r}{s}=\frac{m'}{n'}\cdot\frac{r'}{s'}$$

از شما **خوبان** می‌خواهیم که اثبات این تساوی‌ها را در منزل انجام دهید. دقت کنید که تنها اعداد **ناصفر** را می‌توان از دو طرف یک تساوی در $\mathbb{Z}$ حذف کرد!

۲- (این مثال قدری مجردتر است) می‌دانیم که رابطه‌ی زیر روی $X=\mathbb{Z}\times\mathbb{Z}^*$ هم‌ارزی است:

$$(m,n)\sim(m',n')\Leftrightarrow mn'=nm'$$

حال تحقیق کنید که عمل‌های زیر در $X/\sim=\{[(m,n)]\,|\,m,n\in\mathbb{Z},n\neq 0\}$ خوش‌تعریف هستند (از نمادگذاری پیچیده‌ی کروشه-پرانتز ترسی نداشته باشید، این عمل‌ها همتای همان عمل‌های جمع و ضرب اعداد گویا هستند (!) این طور نیست؟) :

$$[(m,n)]*[(r,s)]=[(ms+nr,ns)]$$
$$[(m,n)]*'[(r,s)]=[(mr,ns)]$$

از آنجا که هر عمل دوتایی در A چیزی جز یک تابع از $A\times A$ به A نیست، مثال‌های بسیاری از این مفهوم می‌توان ارائه داد. سعی می‌کنیم مثال‌هایی را به مرور بیاوریم که در دروس جبر بیشتر مطرح می‌شوند. این بخش را با معرفی جدول کیلی به پایان می‌بریم.

۸.۱.۱ جدول کیلی. اگر $A=\{a_1,\cdots,a_n\}$، آنگاه با الگو قرار دادن جدول ضرب اعداد که در دوره‌ی دبستان دیدیم (**یاد آن دوران خوش بخیر!**)، حاصل هر عمل دوتایی * در A را با جدولی به صورت زیر نشان می‌دهیم (برای سادگی، نماد xy را به کار می‌بریم):

$*$	a_1	$\cdots$	a_j	$\cdots$	a_n
a_1	a_1a_1	$\cdots$	a_1a_j	$\cdots$	a_1a_n
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
a_i	a_ia_1	$\cdots$	a_ia_j	$\cdots$	a_ia_n
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
a_n	a_na_1	$\cdots$	a_na_j	$\cdots$	a_na_n

این جدول را به نام ریاضیدان انگلیسی، آرتور کیلی، **جدول کیلی** می‌نامند. برای مثال، در $\mathbb{Z}_3$ و $\mathbb{Z}/\equiv_3$، داریم

$\oplus_3$	$\circ$	1	2
$\circ$	$\circ$	1	2
1	1	2	$\circ$
2	2	$\circ$	1

$\odot_3$	$\circ$	1	2
$\circ$	$\circ$	$\circ$	$\circ$
1	$\circ$	1	2
2	$\circ$	2	1

$\overline{\oplus}_3$	$\overline{\circ}$	$\overline{1}$	$\overline{2}$
$\circ$	$\overline{\circ}$	$\overline{1}$	$\overline{2}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{\circ}$
$\overline{2}$	$\overline{2}$	$\overline{\circ}$	$\overline{1}$

$\overline{\odot}_3$	$\overline{\circ}$	$\overline{1}$	$\overline{2}$
$\overline{\circ}$	$\overline{\circ}$	$\overline{\circ}$	$\overline{\circ}$
$\overline{1}$	$\overline{\circ}$	$\overline{1}$	$\overline{2}$
$\overline{2}$	$\overline{\circ}$	$\overline{2}$	$\overline{1}$

به شباهت‌های بسیار زیاد جدول‌های $\oplus_3$ با $\overline{\oplus}_3$ و $\odot_3$ با $\overline{\odot}_3$ توجه کنید (بند ۳ بحث **۵.۱.۱** را نیز ببینید). بعداً بارها به چنین شباهت‌های جدول‌های کیلی اشاره خواهیم کرد.

تمرین ۱.۱

به توانایی‌های خود کم اهمیت ندهیم

۱- از ضابطه‌های زیر کدام‌ها عمل دوتایی روی مجموعه‌ی داده شده تعریف می‌کنند:

(الف) تفاضل روی $\mathbb{N}$؛ روی $\mathbb{Z}$؛ و روی $\mathbb{Q}^*$.

(ب) $m*n=m^n$ روی $\mathbb{N}$؛ روی $\mathbb{Z}$؛ و روی $\mathbb{R}$.

(پ) $A*B=A\setminus B$ روی $\mathcal{P}(X)$.

(ت) $a*b=a+b-ab$ روی $\mathbb{Z}$؛ و روی $\mathbb{R}$.

(ث) $a*b=(a+b)/3$ روی $\mathbb{Q}$؛ و روی $\mathbb{R}$.

(ج) $(a,b)*(a',b')=(a+a',ab'+a')$ روی $\mathbb{Z}^2=\mathbb{Z}\times\mathbb{Z}$؛ و روی $\mathbb{R}^2$.

(چ) $f*g=f\circ g$ روی $\mathbb{R}^{\mathbb{Z}}$ متشکل از توابع از $\mathbb{Z}$ به $\mathbb{R}$؛ و روی مجموعه‌ی توابع پیوسته از $\mathbb{R}$ به $\mathbb{R}$.

(ح) $f*g=f+g$ با تعریف $(f+g)(a)=f(a)+g(a)$، روی $\mathbb{R}^{\mathbb{Z}}$؛ و روی مجموعه‌ی توابع پیوسته از $\mathbb{R}$ به $\mathbb{R}$.

(خ) $a*b=a+b$ (برای اعداد زوج a و b دلخواه) و $a*b=ab$ (برای اعداد فرد a، و b دلخواه) روی $\mathbb{Z}$.

(د) $(a,b)*(c,d)=(ad+bc,bd)$ روی $\mathbb{Z}\times\mathbb{Z}^*$.

(ذ) $A*B=A^t$ که در آن A^t ترانهاده‌ی ماتریس A است، روی $M_2(\mathbb{Z})$.

۲- چند عمل صفرتایی، یکانی، یا دوتایی در هر یک از مجموعه‌های چهار عضوی یا $\varnothing$ وجود دارد؟

۳- بررسی کنید که عمل ضرب همنهشتی $\odot_n$ در $\mathbb{Z}_n$، که در بند ۱ بحث ۵.۱.۱ داده شد، خوش تعریف است.

۴- خوش تعریفی‌عمل‌های داده شده در بند ۱ بحث ۷.۱.۱ را اثبات کنید.

۵- (الف) نشان دهید که رابطه‌ی زیر روی $X=\mathbb{Z}\times\mathbb{Z}^*$ هم‌ارزی است:

$$(m,n)\sim(m',n')\Leftrightarrow mn'=nm'$$

(ب) تحقیق کنید که عمل‌های زیر در $X/\sim=\{[(m,n)]\,|\,m,n\in\mathbb{Z},n\neq 0\}$ خوش‌تعریف هستند:

$$[(m,n)]*[(r,s)]=[(ms+nr,ns)]$$
$$[(m,n)]*'[(r,s)]=[(mr,ns)]$$

۶- جدول کیلی عمل دوتایی * با تعریف زیر روی مجموعه‌ی $A=\{1,2,3\}$ را بنویسید:

*	(1,1)	(1,2)	(1,3)	(2,1)	(2,2)	(2,3)	(3,1)	(3,2)	(3,3)
	1	3	1	2	3	3	1	2	2

سپس مقدارهای زیر را محاسبه کنید:

$$(1*1)*2,\quad 2*(3*1),\quad ,(3*3)*(1*2),\quad (1*(2*1))*(1*2)$$

۲.۱ دستگاه‌های جبری و P - جبر

در بخش قبل، مفهوم کلی عمل n - تایی را معرفی، شاید یادآوری، کردیم و با مثال‌های متنوع آن آشنا شدیم. اشیای مورد مطالعه در مبحث جبر، مجموعه‌های مجهز به تعدادی عمل هستند که معمولاً از قوانین مشخصی پیروی می‌کنند.

جبر مطالعه‌ی دستگاه‌های جبری است

در پیش‌گفتار کتاب گفتیم که مبحث **جبر مجرد** و **اصل موضوعی** با معرفی رسمی دستگاه‌های جبری گروه، حلقه، مدول، و فضای برداری آغاز و سپس، با توجه به نیاز علوم جدید، دستگاه‌های جدیدتری معرفی شدند.

دستگاه جامع جبری چیست؟

یک دستگاه جبری می‌تواند متشکل از مجموعه‌ی $\mathbb{Z}$ و عمل دوتایی جمع، یا $\mathbb{Z}$ همراه با **عمل‌های** دوتایی جمع، ضرب، عمل یکانی قرینه‌یابی، و ده‌ها عمل دیگر باشد. به طور کلی و به بیان ساده، تعریف زیر را داریم.

۱.۲.۱ تعریف. یک **دستگاه (جامع) جبری**، که آن را **جبر جامع** یا به اختصار **جبر** نیز می‌نامیم، از یک **مجموعه‌ی زمینه** چون A و مجموعه‌ای چون $F=(\lambda^A)_{\lambda\in\Omega}$ از تعدادی عمل $n_\lambda-$تایی $\lambda^A:A^{n_\lambda}\to A$ تشکیل شده است. در این صورت، خانواده‌ی $\tau=(n_\lambda)_{\lambda\in\Omega}$ از اعداد را **نوع** یا **نشان** جبر A می‌نامیم. (توجه کنید که Ω مجموعه‌ای است که λها در آن تغییر می‌کنند).

۲.۲.۱ بحث در کلاس

۱- توجه می‌کنیم که مجموعه‌ی A ممکن است همراه با مجموعه‌هایی متفاوت از عمل‌ها، جبری جامع تشکیل دهد. از این رو، دستگاه‌های جبری را باید با جفت‌هایی به صورت $(A;F)$ نشان دهیم. برای مثال، $(\mathbb{Z};+),(\mathbb{Z};\cdot)$ جبرهایی از نوع $\tau=(2)$ و $(\mathbb{Z};\{+,\cdot\})$ جبری از نوع $\tau=(2,2)$ است. ولی، گاهی برای راحتی کار، البته اگر امکان اشتباه نباشد، به غلط متداول، می‌گوییم که A **جبری جامع** است، که یقیناً منظور این است که A همراه با مجموعه‌ای چون F از عمل‌های روی A، جبری جامع است.

۲- در علوم کامپیوتر نظری بیشتر واژه‌ی **نشان** به جای **نوع** به کار می‌رود. کلاس همه‌ی جبرهای از یک نوع (یا نشان) τ را با $\mathcal{A}\lg(\tau)$ نشان می‌دهیم. اگر مجموعه‌ی عمل‌های جبر جامع A متناهی باشد، برای مثال، $F=(\lambda_{n_1},\cdots,\lambda_{n_k})$، به طوری که $n_1\geq\cdots\geq n_k$، دستگاه جبری از نوع τ را می‌توان به صورت $(A;\lambda_{n_1},\cdots,\lambda_{n_k})$ نیز نشان داد. همچنین، گاهی λ^A را با λ_A نشان می‌دهیم، و اگر امکان اشتباه نباشد، نماد A را نیز حذف می‌کنیم.

۳- برخی از ریاضی‌دانان مجموعه‌ی زمینه، یعنی A، و مجموعه‌ی عمل‌ها یعنی F را ناتهی در نظر می‌گیرند، ولی ما چنین شرایطی را قایل نمی‌شویم!

۴- مثال‌های بسیاری از دستگاه‌های جبری می‌توانید ارائه دهید. اگر بخواهید جبری، برای مثال، از نوع $\tau=(3,2,2,1,1,0,0)$ ارائه دهید، کافی است برای مثال مجموعه‌ی $\mathbb{Z}$ یا حتی $A=\{a,b,c\}$ را در نظر بگیرید و یک عمل ۳- تایی λ_1، دو عمل ۲- تایی λ_2، λ_3، دو عمل یکانی λ_4، λ_5، و دو عضو ثابت $a_1,a_2\in A$ (به عنوان عمل‌های صفرتایی) را انتخاب کنید. در این صورت، $(A;\lambda_1,\lambda_2,\lambda_3,\lambda_4,\lambda_5,a_1,a_2)$ جبری از نوع مورد نظر است! **به همین سادگی!** از این رو، جبرهایی را مثال می‌زنیم که در مبحثی از علوم ریاضی و کاربردها مطرح می‌شوند. مثال‌ها را با دستگاه‌های جبری از ساده‌ترین **نوع** یا **نشان** آغاز می‌کنیم.

۳.۲.۱ مجموعه! تعجب نکنید، ساده‌ترین دستگاه جبری $(A;F)$ دستگاهی است که در آن $F=\varnothing$، که در این حالت، صرفاً صحبت از یک مجموعه است، که معمولا در درس **مبانی علوم ریاضی** و **نظریه‌ی مجموعه‌ها** مطالعه می‌شود نه در درس‌های جبر.

پس از مجموعه، که جبری با هیچ عمل است، جبر جامع از نوع $\tau=(0)$، یعنی تنها دارای یک عمل صفرتایی، ساده‌ترین است.

۴.۲.۱ تعریف. فرض کنیم $a_\circ$ عضوی ثابت از مجموعه‌ی A باشد. در این صورت، دستگاه جبری $(A;a_0)$ از نوع $\tau=(0)$ را **مجموعه‌ی نقطه‌ای** می‌نامیم.

تعداد عضوهای انتخاب شده در تعریف بالا ممکن است بیش از یکی باشد که در این صورت دستگاهی جبری از نوع $\tau=(0,0,0,\cdots)$ مطرح است. لازم است بگوییم که، اغلب حاصل عمل های صفرتایی را **ثابت‌ها**ی دستگاه جبری می‌نامند. دستگاه‌های جبری زیر جالب‌تر و پر کاربردتر هستند.

۵.۲.۱ تعریف

۱- جبر جامع $(A;F)$ را **جبر یکانی** می‌گوییم اگر F تنها از عمل‌های ۱- تایی (یکانی) تشکیل شده باشد. مجموعه‌ی A را **مجموعه‌ی وضعیت** و هر عمل $\lambda:A\to A$ را **تابع تغییر وضعیت** می‌نامیم.

۲- اگر $F=\{\lambda\}$ تنها از یک عمل یکانی λ تشکیل شده باشد، جبر جامع $(A;\lambda)$ را **جبر تک-یکانی** می‌نامیم.

توجه می‌کنیم که هر عمل یکانی $\lambda:A\to A$ وضعیت عضو $x\in A$ را (که ممکن است یک ذره‌ی فیزیکی یا قیمت کالایی باشد) به وضعیت $\lambda(x)$ تغییر می‌دهد. همچنین، این تغییر وضعیت ممکن است برگشت‌پذیر باشد (یعنی، λ وارون داشته باشد) یا چنین نباشد! برای مثال، ممکن است

عنصری شیمیایی به عنصر دیگری تبدیل شود گه برگشت‌پذیر نباشد، ولی ممکن است قیمت کالایی تغییر کند ولی به قیمت اول برگشت‌پذیر باشد!

جبرهای یکانی و حتی تک- یکانی مطالعه‌ی مستقلی را می‌طلبند و کتاب‌ها و مقاله‌های بسیاری در باره‌ی آن‌ها و کاربردهای آن‌ها نوشته شده است. این نوع دستگاه‌های جبری زیربنای جبری مباحث نسبتاً جدید **سیستم‌های دینامیکی و اتوماتا** (بحث زیر را ببینید) در ریاضیات نیز هستند که کاربردهای بسیاری، به ویژه در اقتصاد نظری، علوم کامپیوتر، فیزیک، . . . ، دارند. این نوع جبرهای یکانی، زیربنای جبری ابزاری چون کنترل از راه دور تلویزیون، و بسیاری دیگر، نیز هستند.

۶.۲.۱ بحث در کلاس

۱- آیا می‌توانید مثال‌هایی از جبر یکانی ارائه دهید؟ البته که می‌توانید! هر مجموعه‌ی A، برای مثال $\mathbb{Z}$، همراه با زیرمجموعه‌ای ناتهی مانند F از توابع از A به A، جبری یکانی است.

۲- اگر $\lambda : A \to A$ عملی یکانی باشد، آنگاه A همراه با مجموعه‌ی $F = \{\lambda^{\circ} = id, \lambda, \lambda \circ \lambda, \lambda \circ \lambda \circ \lambda, \cdots\}$ زیربنای جبری یک سیستم دینامیکی است. حال این مطلب را به صورت زیر تعمیم می‌دهیم. فرض کنیم M یک تکواره‌ی باشد. اگر دستگاه یکانی $(A;F)$ طوری باشد که $F = \{\lambda_m : A \to A \mid m \in M\}$ به طوری که $\lambda_m \circ \lambda_n = \lambda_{mn}$ و $\lambda_e = id_A$، آنگاه $(A;F)$ را یک **اتوماتون** می‌نامیم (واژه‌ی **اتوماتا** جمع اتوماتون است).

۳- برای هر $a \in \mathbb{N}$، عمل‌های یکانی زیر جالب هستند:

$$r_a : \mathbb{N} \to \mathbb{N} \quad , \quad r'_a : \mathbb{N} \to \mathbb{N}$$
$$n \mapsto n + a \qquad\qquad n \mapsto na$$

در این صورت $(\mathbb{N};(r_a)_{a\in\mathbb{N}})$ و $(\mathbb{N};(r'_a)_{a\in\mathbb{N}})$ از چه نوع τ هستند؟ در هر کدام چه تعداد عمل یکانی داده شده است؟

۴- شاید یکی از مهم‌ترین دستگاه‌های جبری تک- یکانی، جبر $(\mathbb{N};r_1)$ است، که در آن $r_1(n) = n+1$ **تالی** n است. این دستگاه جبری را، که زیربنای دستگاه اعداد طبیعی، و در نتیجه زیربنای دستگاه‌های همه‌ی اعداد، است به نام ریاضی‌دان ایتالیایی **جبر پئانو** می‌نامند.

۷.۲.۱ گروهواره. ساده‌ترین دستگاه جبری پس از جبرهای یکانی، دستگاه‌های جبری از نوع $\tau = (2)$، یعنی تنها شامل یک عمل دوتایی، هستند. این دستگاه‌های جبری را، که زیربنای اصلی

دستگاه‌های جبری مورد مطالعه در فصل‌های ۲ و ۳ این کتاب هستند، **گروهواره** یا **ماگما** می‌نامیم. مثال‌هایی از گروهواره را در بخش ۵.۱.۱ دیدیم، و بسیاری را نیز به مرور خواهیم دید.

۸.۲.۱ P - **جبر.** با نگاهی به تعریف ۱.۲.۱ متوجه می‌شویم که مفهوم دستگاه جبری بسیار کلی است و تنها دسته‌بندی‌ای که تاکنون از آن‌ها انجام دادیم، بر حسب **نوع** یا **نشان** آن‌ها است. ولی معمولاً دستگاه‌های جبری از یک نوع τ را نیز برحسب برخی از **ویژگی**‌هایی که به اشتراک دارند دسته‌بندی می‌کنیم. برای مثال، می‌توانیم همه‌ی آن دستگاه‌های جبری تک- یکانی را در یک دسته قرار دهیم که عمل یکانی آن‌ها وارون‌پذیر باشد؛ همه‌ی آن گروهواره‌هایی را در یک دسته قرار دهیم که در آن‌ها معادله‌ی $x^3 = x*(x*x) = x$ حل‌پذیر باشد یا مثلاً دقیقاً دارای سه جواب باشد؛ یا همه‌ی دستگاه‌های جبری A از نوع $\tau = (2,0)$ را در یک دسته قرار دهیم که دارای ویژگی‌های استلزامی و وجودی

$$(\forall x \in A)\ \ (x^2 = 0 \Rightarrow x = 0) \qquad \& \qquad (\exists a \in A)\ \ a^3 = a^2$$

باشند. یا همه‌ی آن دستگاه‌های جبری n عضوی از یک نوع τ را در یک دسته قرار دهیم. از این رو، تعریف جامع زیر را می‌آوریم.

۹.۲.۱ تعریف. فرض کنیم $\mathcal{A}\lg(\tau)$ دسته‌ی همه‌ی دستگاه‌های جبری از نوع τ باشد. فرض کنیم P مجموعه‌ای از **ویژگی**‌ها باشد (P حرف اول کلمه‌ی Property به معنی ویژگی است). در این صورت، می‌گوییم که $A \in \mathcal{A}\lg(\tau)$ یک P - **جبر** است اگر A دارای ویژگی‌های داده شده در P باشد.

۱۰.۲.۱ بحث در کلاس

۱- قبل از ادامه‌ی بحث، باید نکته‌ی مهمی را تذکر بدهیم که در سراسر درس‌های جبر مطرح می‌شود. تعریف ۱.۲.۱، دستگاه‌های جبری‌ای را معرفی می‌کند که ممکن است دارای هیچ ویژگی‌ای نباشند، ولی تقریباً همه‌ی دستگاه‌های جبری‌ای که با آن‌ها سروکار خواهیم داشت، از نوع P - جبر هستند. بنابراین، هر جا صحبت از ویژگی می‌شود، توجه بیش‌تر شما را می‌طلبد. البته، این تعریف نیز بسیار کلی است:

چه نوع ویژگی‌هایی در دستگاه‌های جبری بیش‌تر مورد نظر هستند و در کاربردها به‌کار می‌آیند؟

برای ایجاد انگیزه و کشف برخی از ویژگی‌های اساسی مربوط به انواعی از دستگاه‌های جبری، در بحث زیر شرکت کنید.

۲- می‌خواهیم به کمک یکدیگر چگونگی حل‌کردن معادله‌ی $2+x=5$ را در دستگاه جبری $(\mathbb{Z};+)$ بررسی کنیم. البته، روش حل‌کردن این معادله را به خوبی می‌دانید، قصد ما یادآوری و برجسته کردن حقایقی در باره‌ی عمل جمع در $\mathbb{Z}$ است. فرض کنیم $x\in\mathbb{Z}$ جوابی برای این معادله باشد. در این صورت،

(الف) $2+x=5 \Rightarrow -2+(2+x)=-2+5$

(ب) $\Rightarrow (-2+2)+x=3$

(پ) $\Rightarrow 0+x=3$

(ت) $\Rightarrow x=3$

حال ببینیم که در هر مرحله از کدام ویژگی عمل جمع در $\mathbb{Z}$ استفاده شده است؟

(الف) در این مرحله، عدد صحیح -2 با دو طرف تساوی جمع شده است. آیا می‌توانید بگویید که بنابر کدام ویژگی عمل $+$، تساوی برقرار است؟ روشن است، بنابر یکتایی مربوط به خوش‌تعریفی عمل جمع در $\mathbb{Z}$:

$$\begin{cases}-2=-2\\ 2+x=5\end{cases}\Rightarrow -2+(2+x)=-2+5$$

(ب) در این مرحله، از تساوی $-2+(2+x)=(-2+2)+x$ استفاده شده است. در حالت کلی می‌دانیم که

(ویژگی **شرکت‌پذیری** $+$) $(\forall a,b,c\in\mathbb{Z})\quad a+(b+c)=(a+b)+c$

(پ) تساوی $-2+2=0$ ویژگی دیگری از عمل $+$ در $\mathbb{Z}$ است:

(**وجود قرینه**) $(\forall a\in\mathbb{Z})\ (\exists -a\in\mathbb{Z})\quad a+(-a)=0=(-a)+a$

(ت) در اینجا از ویژگی عدد صفر در ارتباط با عمل جمع استفاده شده است:

(**وجود** و **ویژگی صفر**) $(\exists 0\in\mathbb{Z})\ (\forall a\in\mathbb{Z})\quad a+0=a=0+a$

یک روش دیگر حل‌کردن معادله‌ی بالا در $(\mathbb{Z};+)$ به صورت زیر است:

$$2+x=5 \Rightarrow 2+x=2+3$$

(حذف 2 از دو طرف) $\Rightarrow \quad x=3$

به طور کلی در دستگاه جبری $(\mathbb{Z};+)$ داریم:

(**قانون حذف** برای $+$) $(\forall a,b,c\in\mathbb{Z}) \quad a+b=a+c\Rightarrow b=c$

۳- آیا معادله‌ی $2+x=5$ در $\mathbb{N}$ نیز دارای جواب است؟ اگر چه پاسخ به این سؤال مثبت است و عدد طبیعی 3 جواب معادله است، ولی روش اول بالا برای یافتن $x=3$ به کار نمی‌آید! زیرا عمل جمع در $\mathbb{N}$ دارای همه‌ی ویژگی‌های عمل جمع در $\mathbb{Z}$ نیست. برای مثال، -2 و صفر در $\mathbb{N}$ وجود ندارند تا بتوانیم مراحل **(الف)** تا **(ت)** بالا را انجام دهیم (یقیناً برنامه‌ی کامپیوتری برای حل‌کردن این معادله در $\mathbb{N}$ به روش اول دچار مشکل می‌شود!). شاید بگویید که، ابتدا $\mathbb{N}$ را **درون** $\mathbb{Z}$ در نظر می‌گیریم. حال معادله‌ی $2+x=5$ را در $\mathbb{Z}$ به روش بالا حل می‌کنیم و سپس جواب(های) متعلق به $\mathbb{N}$ را جدا می‌کنیم! **بسیار عالی است!** این یکی از روش‌های جالبی است که در حالت‌های کلی‌تر، به ویژه در فصل **۳** و دروس دیگر جبر، مورد بحث قرار می‌گیرد. روش زیر این معادله را با استفاده از ویژگی‌های عمل $+$ در $\mathbb{N}$ حل می‌کند. از **ویژگی حذف** در $\mathbb{N}$ استفاده کنید:

$$(\forall a,b,c\in\mathbb{N}) \quad a+b=a+c\Rightarrow b=c$$

توجه می‌کنیم که با هیچ دسته‌ای از ویژگی‌های $+$ در $\mathbb{N}$ نمی‌توان معادله‌ی $2+x=1$ را در $\mathbb{N}$ حل کرد و جوابی به دست آورد! **آیا می‌توان؟** حتی اگر مشابه بالا $\mathbb{N}$ را **درون** $\mathbb{Z}$ قرار دهیم و معادله را در $\mathbb{Z}$ حل کنیم، جواب $x=-1$ به دست می‌آید که متعلق به $\mathbb{N}$ نیست.

۴- از آنجا که اتفاقاً عمل ضرب اعداد ناصفر گویا نیز دارای ویژگی‌هایی همتای **(الف)** تا **(ت)** بالا است، همتای ضربی $2+x=5$ یعنی $2x=5$ را نیز می‌توان به روش بالا در $\mathbb{Q}$ حل کرد! در اینجا $1/2$ نقش -2 و 1 نقش صفر را ایفا می‌کند. روشن است که معادله‌ی $2x=5$ را با هیچ دسته‌ای از ویژگی‌های ضرب در $\mathbb{Z}$ نمی‌توان حل‌کرد! **چرا؟** به روش قرار دادن $\mathbb{Z}$ درون $\mathbb{Q}$ **چطور؟**

۱۱.۲.۱ معادله. همان‌طور که دیدیم، مفهوم **ویژگی** مذکور در تعریف **۹.۲.۱** بسیار کلی است. دسته‌هایی از ویژگی‌ها که بیشتر مطرح می‌شوند، به گونه‌ای مربوط به معادله‌ها هستند. برای نمونه، در بین ویژگی‌های مطرح شده در بحث **۱۰.۲.۱**، شرکت‌پذیری مذکور در بند **(ب)** در $\mathbb{Z}$ برقراری معادله‌ی $x*(y*z)=(x*y)*z$ **برای هر** انتخاب از عضوهای $\mathbb{Z}$ به‌جای x، y، z است. در این صورت، می‌گوییم که $x*(y*z)=(x*y)*z$ در $\mathbb{Z}$ **اتحاد** است، (زیرا تنها با **سور عمومی** "**برای هر**" توصیف شده است)؛ **وجود** قرینه در بند **(پ)** مربوط به حل‌پذیری دسته‌ی معادله‌های $x+a=0=a+x$ و **وجود** صفر در بند **(ت)** مربوط به حل‌پذیری معادله‌های $x+a=a=a+x$ در $\mathbb{Z}$ است، که البته این دو ویژگی اتحاد نیستند. به دلایلی که خواهیم دید،

اتحادها در دستگاه‌های جبری از اهمیت ویژه‌ای برخوردار هستند. در زیر به اختصار و به اندازه‌ی نیاز این کتاب، این مفاهیم را با مثال توضیح می‌دهیم.

فرض کنیم $*_1$، $*_2$ نمادهایی برای عمل‌هایی دوتایی، λ نمادی برای عملی یکانی، و e_1، e_2 نمادهایی برای عمل‌هایی صفرتایی باشند. در این صورت هر یک از عبارت‌های صوری

$$x_1 * x_2 = x_2 * x_1 \quad , \quad x_1 * (x_2 * x_3) = (x_1 * x_2) * x_3 \quad , \quad x_1 * (\lambda(x_1) * x_1) = e_1$$
$$(x_1 * (x_2 * x_3)) * (e_1 * (x_4 * x_3)) = (e_2 * (x_2 * x_4)) \quad , \quad x_1 * \lambda(x_2) = e_2 \quad , \cdots$$

یک **معادله** حاصل از این عمل‌ها و متغیرهای x_1، x_2، x_3، x_4، و ثابت‌های e_1، e_2 است. برای مثال، $x_1 x_2 - x_1^{-1} + x_2 + 1 = 0$، $x_1 x_2^{-1} + (-x_1) + 1 = x_2$ معادله‌هایی حاصل از عمل‌های دوتایی جمع و ضرب، عمل‌های یکانی قرینه‌یابی و وارون‌گیری، و عمل‌های صفر- تایی (ثابت‌های) 0 و 1 و دو متغیر x_1 و x_2 در اعداد حقیقی هستند. هر عبارت در یک طرف تساوی‌های به صورت بالا را یک **جمله** می‌گوییم. به طور کلی‌تر، به زبان غیر رسمی، فرض کنیم $p(x_1,\cdots,x_n)$ و $q(x_1,\cdots,x_n)$ جمله‌هایی مانند مثال‌های بالا باشند که از عمل‌ها و مجموعه‌ی متغیرهای $X = \{x_1,\cdots,x_n\}$ ساخته شده‌اند. در این صورت،

(الف) هر تساوی صوری

$$p(x_1,\cdots,x_n) = q(x_1,\cdots,x_n)$$

را یک **معادله** از متغیرهای $X = \{x_1,\cdots,x_n\}$ می‌نامیم.

(ب) اگر برای دستگاهی جبری مانند A داشته باشیم

$$(\exists \ \ a_1,\cdots,a_n \in A) \quad p(a_1,\cdots,a_n) = q(a_1,\cdots,a_n)$$

که در آن $p(a_1,\ldots,a_n)$ از جایگذاری a_iها به جای x_iها در جمله‌ی $p(x_1,\ldots,x_n)$ به دست آمده است، می‌گوییم که معادله‌ی $p(x_1,\cdots,x_n) = q(x_1,\cdots,x_n)$ در A **حل‌پذیر** است.

(پ) اگر برای دستگاهی جبری مانند A داشته باشیم

$$(\forall \ \ a_1,\cdots,a_n \in A) \quad p(a_1,\cdots,a_n) = q(a_1,\cdots,a_n)$$

می‌گوییم که معادله‌ی $p(x_1,\cdots,x_n) = q(x_1,\cdots,x_n)$ در A برقرار، درست، یا **اتحاد** است، و می‌نویسیم $A \models (p = q)$ و در غیر این صورت، می‌نویسیم $A \not\models (p = q)$. اگر P مجموعه‌ای از معادله‌ها باشد به طوری که برای هر معادله‌ی $(p = q) \in P$، داشته باشیم $A \models (p = q)$، می‌نویسیم $A \models P$.

(ت) اگر $p_1 = q_1 ، \ldots ، p_k = q_k$ معادله باشند، آنگاه هر عبارت به صورت

$$(p_1 = q_1) \wedge \cdots \wedge (p_k = q_k) \Rightarrow (p = q) \quad \text{یا} \quad (p_1 = q_1) \Rightarrow (p = q)$$

را یک **گزاره نمای استلزامی** یا **شبه معادله** می‌نامیم. حال، اگر برای هر $a_1, \cdots, a_n \in A$،

$$(p_1(a_1, \cdots, a_n) = q_1(a_1, \cdots, a_n)) \wedge \cdots \wedge (p_k(a_1, \cdots, a_n) = q_k(a_1, \cdots, a_n))$$
$$\Rightarrow (p(a_1, \cdots, a_n) = q(a_1, \cdots, a_n))$$

می‌گوییم که شبه معادله‌ی $(p_1 = q_1) \wedge \cdots \wedge (p_k = q_k) \Rightarrow (p = q)$ در A برقرار یا **شبه اتحاد** است. مانند قانون حذف در بند (ت) بحث ۱۰.۲.۱ بالا.

تمرین ۲.۱

لذت حل کردن تمرین‌ها را از خودتان نگیرید

۱- فرض کنید O مجموعه‌ی اعداد صحیح فرد است. آیا $(O;+)$ گروهواره است؟ $(O;\cdot)$ چطور؟

۲- فرض کنید $X = \{1,2,3\}$. مجموعه‌ی A متشکل از توابع یک به یک روی X را در نظر بگیرید.د آیا A با عمل ترکیب توابع یک گروهواره است؟ جدول کیلی آن را بنویسید. آیا معادله‌های

$$(f \circ g) \circ h = f \circ (g \circ h) \quad \text{یا} \quad f \circ g = g \circ f$$

در این گروهواره اتحاد هستند؟ پاسخ مثبت یا منفی خود را اثبات کنید.

۳- درستی یا نادرستی معادله‌های زیر را برای عمل‌های حاصل از تمرین ۱ از بخش ۱.۱ بررسی کنید:

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

اگر این ویژگی‌ها را دارند، اثبات کنید و اگر ندارند، مثال نقض بیاورید.

۴- دستگاه‌های جبری $A = (\mathbb{N};\cdot,1)$ و $B = (\mathbb{R};\cdot,1)$، از نوع $\tau = (2,0)$، را در نظر بگیرید. با دلیل نشان دهید که هر دو شبه‌معادله‌ی

$$x^2 = x \Rightarrow x = 1 \quad , \quad x^2 = 2 \Rightarrow x = 1$$

در A برقرار (**شبه‌اتحاد**) هستند. آیا هر دو در $(\mathbb{R};\cdot,1)$ نیز برقرار هستند؟ در $(\mathbb{Z}_4;\cdot_4,1)$ چطور؟ همتای جمعی این معادله‌ها، یعنی

$$2x = x \Rightarrow x = 0 \quad , \quad 2x = 2 \Rightarrow x = 0$$

در $(\mathbb{Z};+,0)$، $(\mathbb{R}:+,0)$، یا $(\mathbb{Z}_4;+_4,0)$ **چطور؟**

۳.۱ نیم‌گروه و تکواره

در **۸.۲.۱** بیان شد که معمولاً دستگاه‌های جبری از یک نوع τ را برحسب برخی از ویژگی‌هایی که دارند، دسته‌بندی و نامگذاری می‌کنیم و در تعریف **۹.۲.۱** دستگاه‌های جبری‌ای را که در ویژگی‌هایی صدق می‌کنند، P - **جبر** نامیدیم. سپس دیدیم که برخی از این ویژگی‌ها بر حسب **اتحاد**، **شبه اتحاد**، یا **وجود** جواب **معادله‌ها** مطرح می‌شوند.

در تعریف **۱۱.۲.۱** دیدیم که معادله‌ها تساوی‌هایی هستند که جمله‌های دو طرف آن‌ها به کمک عمل‌ها و متغیرها ساخته می‌شوند. از آنجا که عمل‌های اغلب دستگاه‌های جبری‌ای که مطالعه خواهیم کرد، صفر، یک، و دوتایی هستند، برخی از متداول‌ترین این معادله‌ها و شبه‌معادله‌ها را به مرور در این فصل معرفی و برای مراجعه‌ی بعدی نامگذاری می‌کنیم. سپس برخی از P - جبرهای کلاسیک و همچنین تعدادی جدیدتر را نیز نامگذاری می‌کنیم، و **اندکی** مورد بحث و بررسی قرار می‌دهیم. مطالعه‌ی عمیق‌تر هر یک از این دستگاه‌های جبری در فصل‌های ۲ و ۳ یا درس‌های جداگانه‌ای انجام می‌شود. این P - جبرها صرفاً چند نمونه از دستگاه‌های جبری هستند که در دروس جبر بیشتر مطرح می‌شوند و در سراسر ریاضیات و کاربردهای آن، چون علوم کامپیوتر، فیزیک، شیمی، مهندسی، اقتصاد، علوم نانو، ریاضیات زیستی، و از این قبیل، به گونه‌ای صریح و ضمنی به کار می‌آیند.

۱.۳.۱ تعریف. برخی از معادله‌های متداول مربوط به عمل دوتایی $*$ همراه با نامگذاری آن‌ها، عبارت‌اند از

(**شرکت‌پذیری**) $x*(y*z) = (x*y)*z$.

(**تعویض‌پذیری**) $x*y = y*x$.

(**خودتوانی**) $x*x = x$.

بسیاری از عمل‌های دوتایی که می‌شناسیم، مانند جمع و ضرب اعداد و ماتریس‌ها و ترکیب توابع، در معادله‌ی شرکت‌پذیری صدق می‌کنند. البته بسیاری نیز، مانند **تفریق** روی اعداد صحیح و **تقسیم** در $\mathbb{R}^*$، چنین نیستند. از این رو، ابتدا تعریف زیر را می‌آوریم.

۲.۳.۱ تعریف. گروهواره‌ی $(A;*)$ را **نیم‌گروه** می‌نامیم اگر معادله‌ی شرکت‌پذیری در آن اتحاد، باشد. یعنی،

(**اتحاد شرکت پذیری**) $$(\forall a,b,c\in A)\quad a*(b*c)=(a*b)*c$$

توجه می‌کنیم که هر نیم‌گروه A، یک P - جبر از نوع $\tau=(2)$ است که در آن P اتحاد بودن $x*(y*z)=(x*y)*z$ است. اگر نیم‌گروه $(A;*)$ دارای ویژگی‌های دیگری نیز باشد، معمولاً آن ویژگی‌ها را به صورت پسوند واژه‌ی نیم‌گروه می‌آوریم و البته گاهی نامگذاری جدیدی نیز معرفی می‌کنیم. برای مثال، **نیم‌گروه متناهی** نیم‌گروهی چون $(A;*)$ است که در آن مجموعه‌ی A متناهی است. **نیم‌گروه تعویض‌پذیر** (یا **آبلی**) نیمگروهی چون $(A;*)$ است که در آن معادله‌ی تعویض‌پذیری نیز **اتحاد** باشد. یعنی، برای هر دو عضو $a,b\in A$، $a*b=b*a$. همچنین، **نیم-گروه خودتوان**، که آن را **باند** نیز می‌نامند، و **نیم‌گروه تعویض‌پذیر خودتوان**، که آن را **نیم‌مشبکه** نیز می‌نامند، به صورت مشابه تعریف می‌شوند. روشن است که می‌توانیم صفت‌های متناهی، تعویض‌پذیر و خودتوان را پسوند واژه‌ی گروهواره نیز قرار دهیم.

۳.۳.۱ بحث در کلاس

۱- روشن است که $(\mathbb{Z};+)$ و $(\mathbb{Z};\cdot)$ نیم‌گروه‌هایی تعویض‌پذیر هستند، ولی خودتوان نیستند. گروهواره‌های $(\mathbb{N};+)$ و $(\mathbb{N};\cdot)$ **چطور؟**

۲- نشان دهید که $\mathbb{N}$ همراه با عمل توان $m*n=m^n$ دارای هیچ‌یک از ویژگی‌های تعریف ۱.۳.۱ نیست. مجموعه‌ی $\mathbb{Z}$ همراه با عمل دوتایی تفریق **چطور؟**

۳- هردو گروهواره‌ی $(\wp(X);\cup)$ و $(\wp(X);\cap)$ نیم‌گروه تعویض‌پذیر و خودتوان (نیم‌مشبکه) هستند. گروهواره‌ی $(\wp(X);\Delta)$ **چطور؟** یادآوری می‌کنیم که عمل **تفاضل متقارن** Δ به صورت $A\Delta B=(A\cup B)\setminus(A\cap B)$ نیز تعریف می‌شود. جدول‌های زیر را برای $X=\{a,b\}$ کامل کنید:

$\cup$	$\varnothing$	$\{a\}$	$\{b\}$	X
$\varnothing$	?	$\{a\}$	$\{b\}$	?
$\{a\}$	?	?	X	?
$\{a\}$	$\{b\}$	$\{a\}$	X	?
X	X	?	X	?

$\cap$	$\varnothing$	$\{a\}$	$\{b\}$	X
$\varnothing$	$\varnothing$	?	?	?
$\{a\}$	?	$\{a\}$	$\varnothing$	?
$\{b\}$	?	$\varnothing$	?	?
X	?	$\{a\}$	$\{b\}$	?

Δ	$\varnothing$	$\{a\}$	$\{b\}$	X
$\varnothing$	?	$\{a\}$	?	X
$\{a\}$	?	?	?	$\{b\}$
$\{b\}$	?	?	$\varnothing$	?
X	?	$\{b\}$	?	?

۴- دستگاه‌های جبری $(\mathbb{Z}_n;+_n)$، $(\mathbb{Z}_n;\cdot_n)$، $(\mathbb{Z}/\equiv_n;+_n)$، $(\mathbb{Z}/\equiv_n;\cdot_n)$ نیم‌گروه تعویض‌پذیر هستند، ولی خودتوان نیستند.

۵- اگر عمل دوتایی $*$ در مجموعه‌ی متناهی A با جدول کیلی داده شده باشد، به راحتی می‌توان صدق یا عدم صدق تعویض‌پذیری و خودتوانی را با نگاه کردن به جدول معلوم کرد، ولی بررسی شرکت-پذیری چندان راحت نیست. برای مثال، عمل زیر را در $A=\{e,a,b\}$ درنظر بگیرید:

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

به راحتی مشاهده می‌کنید که تعویض‌پذیری برقرار است، زیرا عضوهای درون جدول (یعنی حاصل عمل $*$) نسبت به قطر (از گوشه‌ی چپ بالا به گوشه‌ی راست پایین) متقارن است، یعنی $x*y=y*x$ اتحاد است. در ضمن $*$ خودتوان نیز هست (**چطور؟**) حال ببینید آیا می‌توانید شرکت‌پذیر بودن یا نبودن این عمل را معلوم کنید؟ شاید بهتر باشد برنامه‌ای کامپیوتری بنویسید! البته گاهی روش‌های غیر مستقیم برای اثبات شرکت‌پذیری وجود دارد، که به مرور خواهیم دید. البته عمل $*$ در این مثال شرکت‌پذیر نیست، زیرا $(a*a)*b=a*b=e$ در حالی که $a*(a*b)=a*e=a\neq e$.

۶- نشان دهید که گروهواره‌ای که عمل آن با جدول

$*$	e	a
e	e	e
a	a	e

مشخص شده است در هیچ‌یک از ویژگی‌های تعریف ۱.۳.۱ صدق نمی‌کند. برای مثال، $a*(e*a)=a*e=a$ در حالی که $(a*e)*a=a*a=e$.

۷- دستگاه‌های جبری $(A;*)$ و $(A;*')$ را در نظر بگیرید، به طوری که، برای هر $x, y \in A$،

$$x * y = x \quad , \quad x *' y = y$$

به راحتی می‌توانید نشان دهید که این دو دستگاه جبری (ساده ولی مهم)، شرکت‌پذیر و خودتوان هستند ولی اگر $|A| > 1$، تعویض‌پذیر نیستند.

۴.۳.۱ تعریف. فرض کنیم $(A;*)$ گروهواره باشد. در این صورت، می‌گوییم که عضو $e_l \in A$ یک **همانی چپ** $(A;*)$ است اگر برای هر $a \in A$، $e_l * a = a$؛ عضو $e_r \in A$ یک **همانی راست** $(A;*)$ است اگر برای هر $a \in A$، $a * e_r = a$؛ و عضو $e \in A$ یک **همانی** (دوطرفه‌ی) $(A;*)$ است اگر برای هر $a \in A$، $e * a = a = a * e$.

۵.۳.۱ بحث در کلاس

۱- توجه می‌کنیم که، برای مثال، عضو همانی چپ e_l جواب مشترک دسته‌ی همه‌ی معادله‌های به صورت $x * a = a$ است، که در آن $a \in A$.

۲- گاهی به جای اینکه بگوییم e عضو همانی گروهواره‌ی $(A;*)$ است می‌گوییم که e همانی عمل $*$ است. روشن است که عدد صفر همانی $+$ در $\mathbb{Z}$ و عدد ۱ همانی ضرب در $\mathbb{Z}$ است. همچنین، اگر عمل $*$ تعویض‌پذیر باشد، سه مفهوم بالا یکسان هستند.

۳- آیا عمل توان $m * n = m^n$ در $\mathbb{N}$ دارای همانی چپ، راست، یا همانی (دوطرفه) است؟ عمل تفریق در $\mathbb{Z}$ چطور؟

۶.۳.۱ بحث در کلاس. در پاسخ به سؤال بند ۷ بحث ۳.۳.۱، مشاهده خواهید کرد که یک عمل دوتایی در یک مجموعه ممکن است بیش از یک عضو همانی راست داشته باشد، ولی حتی یک عضو همانی چپ نداشته باشد، و برعکس! همچنین، عمل $+$ در $\mathbb{N}$ هیچ یک از انواع عضوهای همانی را ندارد. اولین قضیه‌ای که در این فصل مطرح می‌کنیم، قضیه‌ی زیر است که اثباتی بسیار ساده دارد. توجه کنید که اثبات برخی از قضیه‌ها حاوی **فنونی** هستند که در اثبات برخی از قضیه‌های دیگر و حل تمرین‌ها به کار می‌روند. این فنون را بیاموزید تا به مرور در اثبات‌ها و حل تمرین‌ها به کار ببرید. ابتدا اثبات را به عهده‌ی شما می‌گذاریم، سپس کمی بعد آن را می‌آوریم.

۷.۳.۱ *قضیه.* *اگر عمل دوتایی $*$ در A دارای یک عضو همانی چپ e_l و یک عضو همانی راست e_r باشد، آنگاه $e_l = e_r$.*

۸.۳.۱ بحث در کلاس

۱- آیا عمل دوتایی * در A می‌تواند بیش از یک عضو همانی (دوطرفه) داشته باشد؟ (قضیه‌ی بالا را دوباره ببینید!)

۲- قبلاً نیز بیان شد که اگر عمل دوتایی * تعویض‌پذیر باشد، آنگاه روشن است که سه مفهوم همانی چپ، راست، و دو طرفه یکسان هستند. همچنین، اگر * تعویض‌پذیر باشد، معمولاً (نه لزوماً) آن را با نماد + و عضو همانی آن را، در صورت وجود، با نماد 0 نشان می‌دهیم و آن را **عضو خنثی** نیز می‌نامیم.

۳- اثبات ساده‌ی قضیه‌ی ۷.۳.۱ به صورت زیر است. دلیل هر مرحله را بیان کنید.

$$e_r = e_l * e_r = e_l$$

۴- با توجه به **یکتایی** عضو همانی (در صورت وجود) معمولاً آن را با نمادهایی چون 0، 1، یا e نشان می‌دهیم. البته در اینجا نمادهای 0 و 1 لزوماً **عدد** نیستند.

۹.۳.۱ تعریف. نیم‌گروه $(A;*)$ را **تکواره** می‌نامیم اگر دارای عضو همانی باشد. یعنی،

$$(\exists e \in A) \quad (\forall x \in A) \quad x*e = x = e*x$$

قبل از ارائه‌ی چند مثال، مطلب بسیار مهم زیر را می‌آوریم.

۱۰.۳.۱ بحث در کلاس. توجه می‌کنیم که ویژگی **شرکت‌پذیری** که با سور عمومی داده شده است، یک **اتحاد است**، ولی ویژگی **وجود عضو همانی** با سور **وجودی** داده شده است، و در نتیجه **اتحاد نیست!** به مرور خواهیم دید که ویژگی‌هایی که به صورت اتحادها داده می‌شوند از اهمیت بسیاری برخوردار هستند. از این رو، هر کجا امکان‌پذیر باشد، ویژگی‌ها را بر حسب صدق معادله‌ها (اتحادها) بیان می‌کنیم. خوشبختانه ویژگی وجود عضو همانی را می‌توان با تغییر **نوع** تکواره از $\tau = (2)$ به $\tau = (2,0)$ به صورت زیر، برطرف کرد.

۱۱.۳.۱ تعریف (صورت دوم). دستگاه جبری $(A;*,e)$ از نوع $\tau = (2,0)$ را همراه با عمل دوتایی * و عمل صفرتایی e **تکواره** می‌نامیم اگر **اتحادهای** زیر در آن برقرار باشند:

(**اتحاد** شرکت پذیری) $(\forall x,y,z \in A) \quad x*(y*z) = (x*y)*z$

(**اتحاد** ویژگی عضو همانی) $(\forall x \in A) \quad x*e = x = e*x$

در این تعریف تکواره (که خواهیم دید بیش‌تر مورد پسند است) وجود e به عنوان عملی صفرتایی در ساختار جبری A گنجانده شده است. توجه می‌کنیم که از هر یک از این دو تعریف می‌توان به دیگری رسید، و ما آزادانه هر دو را به کار خواهیم برد.

۱۲.۳.۱ بحث در کلاس. یقیناً، با مراجعه به بخش ۱ یا بحث‌های بالا، می‌توانید مثال‌هایی از تکواره ارائه دهید. حال چند مثال جدید می‌آوریم.

۱- روشن است که $(\mathbb{N};\times)$ تکواره است و نیم‌گروه $(\mathbb{N};+)$ تکواره نیست. **چرا؟**

۲- این مثال را برای آموزش و درک مفهومی مهم می‌آوریم. فرض کنیم $A=\{e,f\}$. در این صورت تعداد $2^4=16$ عمل دوتایی در این مجموعه می‌توان تعریف کرد. **چطور؟** مجموعه‌ی A همراه با چند تا از این عمل‌ها می‌تواند **تکواره شود؟** بدیهی است که یکی از دو عضو e یا f باید عضو همانی باشد. ابتدا فرض می‌کنیم که e عضو همانی است. در این صورت، جدول کیلی ناقص زیر را داریم:

$*_1$	e	f
e	e	f
f	f	?

دو انتخاب برای حاصل $f*f$ وجود دارد و در نتیجه جدول‌های زیر به دست می‌آیند:

$*_1$	e	f
e	e	f
f	f	e

,

$*_2$	e	f
e	e	f
f	f	f

همان طور که قبلاً نیز بیان کردیم، بررسی شرکت‌پذیری عملی دوتایی که با جدول کیلی داده شده است، چندان ساده نیست. در مورد این مثال ساده، با صرف کمی وقت و حوصله، می‌توانید با بررسی شرکت‌پذیری، نشان دهید که هر دو دستگاه جبری $(A;*_1,e)$ و $(A;*_2,e)$ تکواره هستند. روشن است که اگر حرف f را به جای e به عنوان عضو همانی انتخاب کنیم، جدول‌های زیر به دست می‌آیند:

$*_3$	f	e
f	f	e
e	e	f

,

$*_4$	f	e
f	f	e
e	e	e

در این صورت نیز $(A;*_3,f)$ و $(A;*_4,f)$ تکواره هستند.

یقیناً تشابهی بین جدول‌های $*_1$ با $*_3$ و $*_2$ با $*_4$ مشاهده می‌کنید. نکته‌ی جالب توجه این است که اگر در جدول $*_1$ به جای e حرف f را قرار دهیم، و بر عکس، همان جدول $*_3$ به دست می‌آید. یعنی، تابع تغییر نام حروف، φ:

x	e	f
$\varphi(x)$	f	e

جدول $*_1$ را به جدول $*_3$ تبدیل می‌کند. برای بیان این پدیده‌ی **جالب**، می‌گوییم که تکواره‌های $(A;*_1,e)$ و $(A;*_3,f)$ **اساساً یکسان** یا **یک‌ریخت** (یعنی دارای ریخت یکسان) هستند! با توجه به تشابه جدول‌های کیلی این تکواره‌ها، **یک‌ریخت** بودن واژه‌ی مناسبی برای بیان این مطلب است، **این طور نیست؟** به همین ترتیب، می‌توانید ببینید که $(A;*_2,e)$ و $(A;*_4,f)$ **یک‌ریخت** هستند. این طور نیست؟ ولی با هیچ تابع دوسویی نمی‌توانیم جدول $*_1$ را به جدول $*_2$ یا به جدول $*_4$ تبدیل کنیم (امتحان کنید!) به عبارت دیگر، تکواره‌های نظیر این جدول‌ها **یک‌ریخت نیستند!** مفهوم بسیار مهم **یک‌ریختی** را در بخش **۵.۱**، دقیق‌تر و ریاضی‌گونه، معرفی و بررسی می‌کنیم. فعلاً همین قدر که این واژه گویای مطلب است، کافی است.

۳- در ادامه‌ی بند **۲**، بیان این نکته نیز بسیار مفید است که تابع تغییر نام حروف به اعداد، ψ:

x	e	f
$\psi(x)$	0	1

جدول $*_1$ را به جدول تکواره‌ی $(\mathbb{Z}_2;\oplus_2)$، یعنی

$\oplus_2$	0	1
0	0	1
1	1	0

تبدیل می‌کند، که می‌دانیم شرکت‌پذیر است. پس $(A;*_1)$ نیز شرکت‌پذیر است. **چطور؟** به همین ترتیب می‌توانید جدول کیلی $(A;*_3)$ را به جدول $(\mathbb{Z}_2;+_2)$ و جدول‌های $(A;*_2)$ و $(A;*_4)$ را به جدول کیلی عمل همنهشتی ضرب به پیمانه‌ی ۲ در $(\mathbb{Z}_2;\cdot_2)$، یعنی

$\cdot_2$	0	1
0	0	0
1	0	1

تبدیل کنید و نتیجه بگیرید که $*_2$ و $*_4$ نیز شرکت‌پذیر هستند. **جالب بود، نبود!؟** البته، این مطالب همچنین نشان می‌دهند که این تکواره‌ها نیز **یک‌ریخت** هستند.

۴- این مثال نیز شامل نکته‌ای جالب توجه است. روشن است که $\mathbb{N}$ همراه با عمل دوتایی $m*n=\min\{m,n\}$ نیم‌گروه است، ولی تکواره نیست (**چطور؟**). نکته‌ی جالب این است که اگر **نمادی** مانند ∞ را به $\mathbb{N}$ بیفزاییم و $\mathbb{N}^{\infty}=\mathbb{N}\cup\{\infty\}$ را در نظر بگیریم، و تعریف کنیم که برای هر $n\in\mathbb{N}$، $n<\infty$، (و در نتیجه، $n*\infty=\min\{n,\infty\}=n$)، آنگاه $(\mathbb{N}^{\infty};\min)$ تکواره‌ای با همانی ∞ می‌شود! این تکواره در علوم کامپیوتر نظری کاربرد دارد.

۵- مشابه با بند۴، هر نیم‌گروه دلخواه بدون عضو همانی $(A;*)$ را می‌توان به یک تکواره، به اصطلاح، **گسترش** داد. به این صورت که، **نمادی** چون e خارج از A انتخاب می‌کنیم و آن را به A **الحاق** می‌کنیم، یعنی $A^{e}=A\cup\{e\}$ را تشکیل می‌دهیم. حال تعریف می‌کنیم که

$$(\forall x\in A^{e})\quad x*e=x=e*x$$

در این صورت، $(A^{e};*,e)$ تکواره است.

۶- در تعریف کلی جبر **یکانی** (تعریف **۵.۲.۱**) هیچ ارتباطی بین عمل‌ها قایل نشدیم، که البته کارایی کم‌تری به این نوع دستگاه می‌دهد. حال، با استفاده از یک نیم‌گروه یا تکواره، دستگاه جبری یکانی بسیار مفیدی را معرفی می‌کنیم که به گونه‌ای این نقص را برطرف می‌کند. (این دستگاه جبری، جامع‌تر از دستگاه‌های جبری **فضای برداری** و **مدول** است، که به تفصیل در درس‌های دیگر جبر و جبر خطی مطالعه خواهند شد. پیوست را ببینید). کاربردهای این دستگاه جبری در علوم انسانی، علوم ریاضی، علوم کامپیوتر، علوم تجربی، مهندسی، و در هر مسئله‌ای که حرکت و تغییری در آن مطرح باشد، **بسیار زیاد** است. خوشبختانه ریاضی‌دانانی در **دانشگاه‌های ایران** وجود دارند که این نوع دستگاه‌های جبری را مطالعه می‌کنند یا صرفاً به کار می‌برند.

فرض کنیم $(M;*,e)$ تکواره و A مجموعه باشد. اگر برای هر $x\in M$ یک عمل یکانی $l_x:A\to A$ وجود داشته باشد، آنگاه دستگاه یکانی $(A;(l_x)_{x\in M})$ به دست می‌آید. معمولاً، حاصل $l_x(a)$ را با نمادگذاری انتقال (یا **کنش**) چپ xa نشان می‌دهیم و تعریف زیر را می‌آوریم.

۱۳.۳.۱ تعریف. فرض کنیم $(M;*,e)$ یک تکواره با عضو همانی e و A مجموعه باشد. هر دستگاه یکانی $(A;(l_x)_{x\in M})$ را یک M - **مجموعه** (یا M - **دستگاه**، M - **اتوماتا**، M - **کنش**، M - **دستگاه انتقال**) **چپ** می‌نامیم اگر برای هر $x,y\in M$ و هر $a\in A$، دو اتحاد زیر برقرار باشند:

(الف) $(x*y)a=x(ya)$. [یعنی، $l_{x*y}(a)=l_x(l_y(a))$ یا $l_{x*y}=l_x\circ l_y$].

(ب) $ea=a$. [یعنی، $l_e(a)=a$ یا $l_e=id_A$].

۱۴.۳.۱ بحث در کلاس

۱- روشن است که هر تکواره‌ی $(M;*,e)$ خود یک M - مجموعه است. در اینجا، برای هر x در تکواره‌ی M و هر a در مجموعه‌ی M، xa همان حاصل $x*a$ در تکواره‌ی M است:

$$\begin{pmatrix} l_x : M \to M \\ \quad a \mapsto xa = x * a \end{pmatrix}_{x \in M}$$

۲- توجه می‌کنیم که خانواده‌ی عمل‌های یکانی $(l_x : A \to A)_{x \in M}$ تابعی به صورت

$$\begin{aligned} M \times A &\xrightarrow{\ l\ } A \\ (x, a) &\mapsto xa \quad (= l_x(a)) \end{aligned}$$

به دست می‌دهد، و برعکس (بند ۴ بحث ۲.۱.۱ را نیز ببینید). از این رو، اغلب ریاضی‌دانان برای تعریف M - مجموعه (و مشابه آن، برای تعریف فضای برداری یا مدول، که در درس‌های دیگر جبر خواهید دید)، از این نوع تابع استفاده می‌کنند. ولی ما چنین نکردیم، زیرا تابع l عمل‌های یکانی را به طور صریح نمایان نمی‌کند تا بتوانیم M - مجموعه (یا در درس‌های دیگر، فضای برداری و مدول) را به صورت **دستگاه جبری** از نوع تعریف ۱.۲.۱ ببینیم.

۳- با تعریف $r_x : A \to A$ به صورت $r_x(a) = ax$، و تغییر اتحادهای **(الف)** و **(ب)** به $a(x * y) = (ax)y$ و $ae = a$، M - مجموعه‌ی **راست** $(A; (r_x)_{x \in M})$ به دست می‌آید.

۴- تکواره‌ی $M = (\mathbb{Z}_2; +_2)$ را در نظر بگیرید و فرض کنید $A = \{a, b\}$. عمل‌های یکانی $l_0 : A \to A$ و $l_1 : A \to A$ را به صورت زیر تعریف می‌کنیم.

	a	b
l_0	a	b
l_1	b	a

یعنی، $0a = a$، $0b = b$، $1a = b$، $1b = a$. نشان دهید که $(A; l_0, l_1)$ یک M - مجموعه است. توجه کنید که $l_1 \circ l_1 = id$. اگر M را تکواره‌ی $(\mathbb{Z}_2; \cdot_2)$ در نظر بگیریم، آیا باز هم $A = \{a, b\}$ با همان عمل بالا M - مجموعه است؟

۵- تکواره‌ی $(\mathbb{Z}; +)$ را در نظر بگیرید. نشان دهید که مجموعه‌ی اعداد گویا یک $\mathbb{Z}$ - مجموعه است، که در آن عمل‌های یکانی $l_n : \mathbb{Q} \to \mathbb{Q}$ به صورت $l_n(q) = nq$ تعریف می‌شوند.

تمرین ۳.۱

هوشم نه چنان است تلاشم آنچنان است

۱- مثالی از یک تکواره بیاورید که تعویض‌پذیر و هر عضو آن خودتوان باشد.

۲- مثالی از یک تکواره بیاورید که در آن عضوهایی چون x و y وجود داشته باشند به طوری که $xy=1$ ولی $yx\neq 1$.

۳- مجموعه‌ی $R(X)$ متشکل از همه‌ی رابطه‌های روی مجموعه‌ی X را در نظر بگیرید و عمل ترکیب را به صورت

$$R\circ S=\{(x,y):\exists z,(x,z)\in S,(z,y)\in R\}$$

روی آن تعریف کنید. آیا $(R(X),\circ)$ نیم‌گروه است؟ تکواره چطور؟ اگر به جای مجموعه‌ی $R(X)$، مجموعه‌ی $E(X)$ متشکل از همه‌ی رابطه‌های هم‌ارزی روی مجموعه‌ی X را در نظر بگیریم، آیا $(E(X),\circ)$ گروهواره است؟

۴- نشان دهید که $\mathbb{N}$ همراه با عمل توان $m*n=m^n$ دارای هیچ‌یک از ویژگی‌های تعریف ۱.۳.۱ نیست. مجموعه‌ی $\mathbb{Z}$ همراه با عمل دوتایی تفریق چطور؟

۵- هردو گروهواره‌ی $(\wp(X);\cup)$ و $(\wp(X);\cap)$ نیم‌گروه تعویض‌پذیر و خودتوان (نیم‌مشبکه) هستند. گروهواره‌ی $(\wp(X);\Delta)$ **چطور؟** هر سه عمل $\cap$، $\cup$، Δ در $\wp(X)$ دارای همانی (دوطرفه) هستند. آن‌ها را مشخص کنید!

۶- دستگاه‌های جبری $(A;*)$ و $(A;*')$ را در نظر بگیرید، به طوری که، برای هر $x,y\in A$،

$$x*y=x \qquad , \qquad x*'y=y$$

آیا این دستگاه‌های جبری دارای همانی چپ، راست، یا دوطرفه هستند؟ پاسخ‌های جالبی به دست می‌آورید!

۶- آیا عمل توان $m*n=m^n$ در $\mathbb{N}$ دارای همانی چپ، راست، یا همانی (دوطرفه) است؟ عمل تفریق در $\mathbb{Z}$ چطور؟

۷- فرض کنید که $M=(\mathbb{Z}_2;+_2)$. نشان دهید که هر مجموعه چون A با یک عمل یکانی f که در شرط $f\circ f=id$ صدق می‌کند را می‌توان به صورت $(A;id,f)$ به یک $\mathbb{Z}_2$- مجموعه تبدیل کرد.

۸- تکواره‌ی $M=(\mathbb{N}\cup\{\infty\};\min,\infty)$ را در نظر بگیرید، که در آن $\min\{m,n\}$ همان کوچک‌ترین m و n است. نشان دهید که هر زیرمجموعه‌ی به صورت $\downarrow k=\{x\in\mathbb{N}:x\leq k\}=\{1,2,\ldots,k\}$ با همان عمل **min** یک M- مجموعه است.

۹- فرض کنید M یک تکواره باشد. نشان دهید که $\wp(M)$ همراه با عمل (موسوم به تقسیم) به صورت $X \cdot m = \{s \in M : sm \in X\}$ یک M - مجموعه است. با عمل $mX = \{mx \in M : x \in X\}$ چطور؟

۱۰- تکواره‌ی $M = (\mathbb{N} \cup \{0\}; +)$ را در نظر بگیرید. نشان دهید در هر M - مجموعه چون $(A; (l_x)_{x \in M})$ داریم $l_n = l_1^n$، که در آن l_1^n ترکیب l_1 با خودش به اندازه‌ی n بار است.

۴.۱ گروه، شبه‌گروه، حلقه، و مشبکه

در این بخش، برای نمونه، دو P - جبر مهم کلاسیک **گروه** و **حلقه** (یکی از نوع $\tau = (2)$ و دیگری از نوع $\tau = (2,2)$) و دو P - جبر مهم و مدرن‌تر **شبه‌گروه** و **مشبکه** (یکی از نوع $\tau = (2)$ و دیگری از نوع $\tau = (2,2)$) را معرفی می‌کنیم. دستگاه‌های جبری گروه و حلقه از قدیمی‌ترین دستگاه‌های جبری هستند و در فصل‌های ۲ و ۳ و در درس‌های دیگر جبر مورد مطالعه بیش‌تر و دقیق‌تر قرار می‌گیرند. دستگاه‌های جدیدتر شبه‌گروه و مشبکه نیز کاربردهای فراوانی در علوم مدرن از جمله در ترکیبیات، علوم کامپیوتر، هندسه، و آمار دارند. برای معرفی گروه، ابتدا مفهوم جامع زیر را می‌آوریم.

۱.۴.۱ تعریف. فرض کنیم عمل دوتایی $*$ در مجموعه‌ی A دارای عضو همانی e باشد. در این صورت، می‌گوییم که عضو $a \in A$ دارای **وارونی چپ** چون $a_l \in A$ است اگر $a_l * a = e$؛ دارای **وارونی راست** چون $a_r \in A$ است اگر $a * a_r = e$؛ و دارای **وارون** (دوطرفه) چون $a' \in A$ است اگر $a' * a = e = a * a'$.

۲.۴.۱ بحث در کلاس

۱- توجه کنید که واژه‌ی ساده‌ی **وارون** را برای وارون دوطرفه به کار برده‌ایم. همچنین، به زبان معادله‌ای، برای مثال، وارون راست a جواب معادله‌ی $a * x = e$ است. ابتدا وجود یا عدم وجود وارون‌ها را در برخی از مثال‌هایی که دیده‌ایم، بررسی، سپس از فرصت استفاده می‌کنیم و مثال‌هایی جدید نیز می‌آوریم.

۲- روشن است که عدد صفر عضو خنثی عمل جمع در $\mathbb{Z}$ است. همچنین، برای هر عدد صحیح n، عدد صحیح $-n$ وارون آن است، زیرا $-n + n = 0 = n + (-n)$. این نکته را نیز بیان می‌کنیم که اگر عمل $*$ را به صورت جمعی نشان دهیم، معمولاً واژه‌ی **قرینه** را به جای وارون به کار می‌بریم.

۳- روشن است که هر عضو در $\mathbb{Z}_4 = \{0,1,2,3\}$ نسبت به عمل جمع همنهشتی $+_4$ دارای قرینه است. برای مثال، عدد ۱ قرینه‌ی ۳ و ۲ قرینه‌ی خودش است. **چرا؟** ولی ۰ و ۲ نسبت به ضرب همنهشتی $\cdot_4$ وارون ندارند.

۴- آیا هر عضو $C_8 = \{1,3,5,7\}$ نسبت به ضرب همنهشتی به پیمانه‌ی ۸، یعنی $\cdot_8$، دارای وارون است؟ وارون هر عضوی را که وارون دارد، مشخص کنید. برای مثال، ۳ وارون خودش است، زیرا $3 \cdot_8 3 = 1$. جدول کیلی این عمل را بنویسید. حدس بزنید کدام عضوهای $\mathbb{Z}_n$ نسبت به ضرب همنهشتی $\cdot_n$ دارای وارون هستند!

۵- فرض کنید $F(X)$ مجموعه‌ی همه‌ی توابع روی X (از X به X) است. روشن است که عمل ترکیب توابع $\circ$ عملی دوتایی در $F(X)$ است. حال تعیین کنید که کدام نوع تابع در تکواره‌ی $(F(X);\circ)$ دارای وارون چپ، راست، یا دوطرفه است.

۶- جدول کیلی زیر را برای تعریف عمل $*$ در مجموعه‌ی $A = \{e,a,b,c,d\}$ در نظر بگیرید.

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

روشن است که e عضو همانی در $(A;*)$ است. حال چون $a*c=e$ ولی $c*a \neq e$، پس c یک وارون راست a است ولی وارون چپ آن نیست! مشاهده می‌کنیم که a و b، **هردو**، وارون (دوطرفه‌ی) a هستند! همچنین، d هیچ نوع وارونی ندارد.

۷- این مثال‌ها نشان می‌دهند که یک عضو نسبت به یک عمل دوتایی ممکن است **بیش از یک** وارون چپ، راست، یا **حتی دوطرفه**، داشته، یا اصلاً **هیچ** نوع وارونی نداشته، باشد!

۸- ممکن است با دیدن مثال بند ۶ بالا تعجب نکرده باشیم که وارون راست یا چپ یک عضو منحصر به فرد نیست (زیرا، برای مثال، در درس مبانی علوم ریاضی دیده بودیم که وارون چپ توابع یک به یک، یا وارون راست توابع پوشا، لزوماً منحصر به فرد نیستند) ولی قبل از این جدول **ندیده بودیم** که وارون دوطرفه منحصر به فرد نباشد! البته، گاهی ویژگی‌های دستگاه جبری $(A;*,e)$ ایجاب می‌کند که وارون (دوطرفه‌ی) هر عضو، در صورت وجود، منحصر به فرد نیز باشد. برای مثال، قضیه‌ی جالب زیر را ببینید که چطور **شرکت‌پذیری** عمل دوتایی $*$، یکتایی وارون را نتیجه می‌دهد (به **فن** اثبات نیز توجه کنید!).

۳.۴.۱ قضیه. *فرض کنیم* $(A;*,e)$ *تکواره (شرکت پذیر) باشد. در این صورت،*

۱- اگر $a\in A$ *دارای یک وارون چپ مانند* a_l *و یک وارون راست مانند* a_r *باشد، آنگاه* $a_l=a_r$.

۲- اگر $a\in A$ *دارای وارون (دوطرفه) باشد، آنگاه وارون آن منحصر به فرد است.*

اثبات

۱- به صورت زیر اثبات می‌شود. دلیل هر مرحله را بنویسید (به کاربرد شرکت‌پذیری توجه کنید):

$$a_l=a_l*e=a_l*(a*a_r)=(a_l*a)*a_r=e*a_r=a_r$$

۲- بلاواسطه از ۱ نتیجه می‌شود. **چطور؟** ■

۴.۴.۱ بحث در کلاس

۱- توجه کنید که در جدول بند ۶ بحث ۲.۴.۱، عضو c دارای یک وارون چپ چون a و یک وارون راست چون b است ولی $b\neq a$. همچنین، a بیش از یک وارون دوطرفه دارد. ولی این مطالب متناقض قضیه‌ی بالا نیستند، زیرا عمل * در آن جدول شرکت‌پذیر نیست: برای مثال،

$$a*(a*b)=a*e=a \quad \text{ولی} \quad (a*a)*b=e*b=b.$$

۲- گروهواره‌ی با همانی $(A;*,e)$ را که در بند ۵ بحث ۳.۳.۱ ارائه دادیم، و جدول کیلی آن به صورت زیر است، در نظر بگیرید:

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

همان طور که در بحث ۳.۳.۱ دیدیم، عمل دوتایی * شرکت‌پذیر نیست، ولی به راحتی می‌توانید نشان دهید که هر عضو A دارای وارون **منحصر به فرد** است! این مثال نشان می‌دهد که اگر چه، با توجه به قضیه‌ی ۳.۴.۱، شرط شرکت‌پذیری برای یکتایی عضو وارون کافی است، ولی لازم نیست.

۳- این مثال‌ها و تذکرها **هشدار** می‌دهند که همیشه باید در اثبات احکام (در درس‌های جبر یا در هر درس دیگر ریاضی و غیر ریاضی) دقت کنیم که از چه فرض‌هایی استفاده می‌کنیم و ببینیم که آیا با حذف یک یا چند فرض ، باز هم حکم برقرار است یا نیست.

۴- توجه کنید که در اثبات یکتایی عضو همانی در قضیه‌ی ۶.۳.۱ صرفاً از ویژگی خود عضو همانی استفاده شد و شرکت‌پذیر بودن یا نبودن * نقشی در آن نداشت.

۵- اگر عضوی وارون دوطرفه داشته باشد، می‌گوییم **وارون پذیر** است و اگر وارون a به هر دلیلی منحصر به فرد باشد، معمولاً وارون a را با a^{-1} نشان می‌دهیم (و اگر نماد عمل را با $+$ نشان داده باشیم، معمولاً وارون a را قرینه می‌نامیم و با $-a$ نشان می‌دهیم).

چند ویژگی دیگر عمل‌ها را به مرور مطرح خواهیم کرد. معادله‌ی $2x=5$ را به این دلیل نتوانستیم در تکواره‌ی $(\mathbb{Z};\cdot)$ حل کنیم که عضوی چون ۱/۲ در این دستگاه با معنی نبود! به همین دلیل لزوماً نمی‌توانیم هر معادله‌ی به صورت $a*x=b$ یا $y*a=b$ را در تکواره‌ی $(A;*)$ حل کنیم (مثالی بیاورید). در زیر، با الگو قرار دادن ویژگی‌های دستگاه جبری $(\mathbb{Z};+)$، دستگاه جبری مهم، تاریخی، و کلاسیکی را معرفی می‌کنیم که این معادله‌ها در آن حل می‌شوند!

۵.۴.۱ تعریف. نیم‌گروه $(G;*)$ را **گروه** می‌نامیم اگر دارای عضو **همانی** باشد و هر عضو آن **وارون** داشته باشد. به عبارت دیگر، گروهواره‌ای را که دارای سه ویژگی زیر باشد، **گروه** می نامیم:

(گ۱) (اتحاد شرکت‌پذیری) $(\forall x,y,z\in G)\quad x*(y*z)=(x*y)*z$

(گ۲) (وجود عضو همانی) $(\exists e\in G)\quad (\forall x\in G)\quad x*e=x=e*x$

(گ۳) (وجود وارون‌ها) $(\forall x\in G)\quad (\exists x^{-1}\in G)\quad x*x^{-1}=e=x^{-1}*x$

گروه‌ها شاید از اولین دستگاه‌های جبری بودند که به صورت اصل موضوعی تعریف و مطالعه شدند. گروه‌ها را به تفصیل در **فصل ۲** این کتاب و در درس‌های دیگر جبر مطالعه می‌کنیم. در اینجا صرفاً به چند مثال و تذکر اکتفا می‌کنیم.

۶.۴.۱ بحث در کلاس

۱- با توجه به قضیه‌ی ۷.۳.۱، عضو همانی در هر گروه منحصر به فرد است و بنابر شرکت‌پذیر بودن عمل دوتایی گروه، هر عضو در گروه وارون یکتا دارد (قضیه‌ی ۳.۴.۱ را ببینید).

۲- (اختیاری) مشابه تعریف ۱۱.۳.۱ تکواره، اگر عضو همانی را به عنوان عملی صفرتایی و وارون‌گیری را عملی یکانی چون

$$G\to G$$
$$x\mapsto x^{-1}$$

در نظر بگیریم (یکتایی وارون‌ها ایجاب می‌کند که این ضابطه تابعی خوش‌تعریف به دست دهد)، آنگاه گروه را می‌توانیم دستگاهی جبری چون $(G;*,^{-1},e)$ از نوع $\tau=(2,1,0)$ در نظر بگیریم، و سورهای وجودی در (گ۲) و (گ۳) را حذف کنیم و در نتیجه اصول معرف گروه را به صورت سه

اتحاد بیان کنیم. این نوع تعریف‌هایی که به کمک اتحادها داده می‌شوند طرفداران بیش‌تری، بـه ویـژه در علوم کامپیوتر نظری، دارند.

۳- به راحتی می‌توانید تشخیص دهید که از مثال‌هایی که تاکنون آوردیم کدام‌ها گروه هستند. اجـازه دهید مثال دیگری بیاوریم. فرض کنید F_X، M_X، و S_X، به ترتیب، مجموعه‌ی همـه‌ی توابـع، توابـع یک به یک، و توابع دوسویی روی X باشند. در این صورت، اگر چه F_X و M_X همراه با عمل دوتایی ترکیب توابع، تکواره هستند، ولی لزوماً گروه نیستند (**چرا؟**). نشان دهید که S_X تحـت ترکیـب توابـع گروه است.

۷.۴.۱ شبه‌گروه. حال می‌خواهیم دستگاه جبری **شبه‌گروه** را معرفی کنـیم. ایـن دسـتگاه جبـری کاربردهایی مفید، برای مثال در علوم کامپیوتر، ترکیبیات، هندسه، و طرح آزمایش‌هـا (در علـم آمـار)، دارد. ابتدا مطالبی را می‌آوریم که برای درک و دلیل معرفی اصول موضوع آن مفید هستند.

چون می‌خواهیم این دستگاه جبری را **شبه‌گروه** بنامیم، انتظار داریم به گونه‌ای **شبیه** بـه گـروه و با اصول موضوع آن در ارتباط، و در واقع تعمیم مفهوم گروه، باشد. ابتدا قضیه‌ی مفید زیر را، که معادلی برای تعریف گروه مطرح می‌کند، بیان می‌کنیم (البته اثبات جالب آن را در **فصل۲**، که تماماً مربوط بـه گروه است، می‌آوریم).

۸.۴.۱ قضیه. *فرض کنیم $(G;*)$ نیم‌گروهی **ناتهی** باشد. در این صـورت، G گـروه اسـت اگـر و تنها اگر برای هر $a,b\in G$، هر یک از معادله‌های خطی $a*x=b$ و $y*a=b$ در G حل‌پذیر* (دارای جواب) *باشد.*

۹.۴.۱ بحث در کلاس. نتیجه‌ی بسیار مفید و جالبی از قضیه‌ی بالا به دست می‌آید. ولی، قبل از پرداختن به آن،

۱- نشان دهید که در گروه $(G;*)$، جواب هر یک از معادلـه‌هـای $a*x=b$ و $y*a=b$ یکتـا است. یادآوری می‌کنیم که در این موارد فرض می‌کنیم کـه هـر دو عضـو c و d جـواب $a*x=b$ هستند، یعنی $a*c=b=a*d$، و سپس با استفاده از تعریف گـروه، **(گ۱)**-**(گ۳)**، نشـان مـی-دهیم که $c=d$ (**نشان دهید.**)

۲- حال نتیجه‌ی جالب و مفیدی را که از قضیه‌ی بالا به دست می‌آید، بیان می‌کنیم. فرض کنـیم a و b عضو گروه (متناهی) G باشند. در این صورت،

(الف) وجود و یکتایی جواب معادله‌ی $a*x=b$ ایجاب می‌کند که در جدول کیلـی گـروه G، هـر عضو $b\in G$ باید دقیقاً یک‌بار در سطر مربوط به a ظاهر شود!

(ب) به همین ترتیب، وجود و یکتایی جواب معادله‌ی $y*a=b$ نشان می‌دهد که هر عضو $b\in G$ دقیقاً یک‌بار در ستون مربوط به a ظاهر می‌شود! **چطور بود؟ جالب بود!**

چنین جدولی را مربع لاتین می‌نامیم.

۳- در بند ۲ بحث ۱۲.۳.۱ دیدیم که از تعداد ۱۶ عمل دوتایی در $A=\{e,f\}$، تنها از ۴ جدول زیر تکواره به دست می‌آید:

$*_1$	e	f
e	e	f
f	f	e

$*_2$	e	f
e	e	f
f	f	f

$*_3$	f	e
f	f	e
e	e	f

$*_4$	f	e
f	f	e
e	e	e

حال با استفاده از مطالب بالا، بگویید که کدام جدول‌ها، گروه به دست می‌دهند؟ درست حدس زدید، جدول‌های $*_1$ و $*_3$. در همان بحث ۱۲.۳.۱ دیدیم که تکواره‌های مربوط به این دو جدول **اساساً یکسان** (**یک‌ریخت**) هستند.

۴- اگر روش مذکور در بحث ۱۲.۳.۱ را با توجه به دو شرط **(الف)** و **(ب)** بند ۲ بالا روی جدول زیر اعمال کنید

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

مشاهده خواهید کرد که این جدول تنها به صورت زیر کامل می‌شود!

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

بنابراین (اگر، برای منحرف نشدن از نکته‌ی اصلی این بحث، فعلاً شرکت پذیر بودن این عمل را بپذیریم، تمرین ۳ این بخش را ببینید)، می‌توانیم بگوییم که

اساساً، یعنی تا حد یک‌ریختی، تنها یک گروه از هر یک از مرتبه‌های ۱ ، ۲، ۳ داریم!

این بحث را در فصل۲ ادامه می‌دهیم. حال آماده هستیم که مفهوم **شبه‌گروه** را تعریف کنیم. خواهیم دید که، با توجه به قضیه‌ی ۸.۴.۱، **شبه‌گروه** تعمیم مفهوم گروه است.

۱۰.۴.۱ تعریف. گروهواره‌ی (نه لزوماً شرکت‌پذیر و نه لزوماً دارای عضو همانی) $(Q;*)$ را **شبه گروه** می‌نامیم اگر برای هر $a,b\in Q$، هر یک از معادله‌های $a*x=b$ و $y*a=b$ در Q جواب **منحصر به فرد** داشته باشد. یعنی، برای هر $a,b\in A$،

(الف) $a*c=b \quad (\exists!c\in A)$ (ب) $d*a=b \quad (\exists!d\in A)$

۱۱.۴.۱ بحث در کلاس

۱- با توجه به بند **۲** بحث **۹.۴.۱**، تعریف شبه‌گروه (متناهی) $(Q;*)$ ایجاب می‌کند که جدول آن یک جدول لاتین باشد، و بر عکس هر جدول لاتین (متناهی) معرف یک شبه‌گروه (متناهی) است. ولی، اگر چه روشن است که جدول کیلی هر گروه متناهی نیز یک جدول لاتین است، آیا هر جدول لاتین معرف یک گروه است؟ جدول لاتین زیر پاسخی منفی به این سؤال است:

*	a	b	c
a	c	a	b
b	b	c	a
c	a	b	c

توجه می‌کنیم که عمل * نه همانی دارد و نه شرکت‌پذیر است. **چرا؟**

۲- با توجه به بند **۱**، مثال‌های شبه‌گروه فراوانند. چند مثال زیر را می‌آوریم.

(الف) روشن است که هر گروه یک شبه‌گروه است.

(ب) $(\mathbb{Z};-)$ همراه با عمل تفریق یک شبه‌گروه است.

(پ) هر یک ازگروهواره‌های $(\mathbb{Q}^*;\div)$ و $(\mathbb{R}^*;\div)$ نیز شبه گروه است ولی گروه نیست.

(ت) $\mathbb{R}$ همراه با عمل معدل‌گیری $x*y=(x+y)/2$ نیز **شبه‌گروه** است، ولی گروه نیست.

(ث) (طرح آزمایش‌ها) فرض کنیم هفت مدرس به شماره‌های ۱ تا ۷ می‌خواهند افراد شرکتی را در یک هفته (شنبه تا جمعه) تعلیم دهند. در هر روز هفته، گروهی سه نفره کار تعلیم را به عهده می‌گیرند به طوری که هر دو مدرس تنها در یک روز هفته به صورت زیر با هم ظاهر می‌شوند:

روز هفته	گروه سه نفره
شنبه	۶،۴،۲
یکشنبه	۵،۴،۱
دوشنبه	۷،۴،۳
سه‌شنبه	۱،۳،۲
چهارشنبه	۷،۵،۲
پنجشنبه	۷،۶،۱
جمعه	۶،۵،۳

این برنامه‌ریزی (طرح آزمایش) متناظر با شبه‌گروه $(Q;*)$ است، که در آن Q مجموعه‌ی مدرس‌ها است و $*$ به این صورت تعریف می‌شود که $x*x=x$ و $x*y=z$ هرگاه مدرس‌های x، y، z در یک روز تدریس کنند. جدول کیلی این شبه‌گروه به‌صورت زیر است:

$*$	1	2	3	4	5	6	7
1	1	3	2	5	4	7	6
2	3	2	1	6	7	4	5
3	2	1	3	7	6	5	4
4	5	6	7	4	1	2	3
5	4	7	6	1	5	3	2
6	7	4	5	2	3	6	1
7	6	5	4	3	2	1	7

توجه می‌کنیم که $*$ در این مثال تعویض‌پذیر و خودتوان است.

۴- (اختیاری) مشابه بند ۲ بحث ۶.۴.۱، اصول موضوع هر شبه‌گروه را نیز می‌توان با تغییر نوع دستگاه جبری از $\tau=(2)$ به $\tau=(2,2,2)$ به صورت **اتحاد** بیان کرد. فرض کنیم $(A;*)$ شبه‌گروه باشد. می‌دانیم که برای هر $a,b\in A$ معادله‌های $a*x=b$ و $y*a=b$ در A جواب منحصر به فرد دارند. معمولاً این جواب‌های یکتا را، به ترتیب، با **تقسیم چپ** $x=a\backslash b$ و **تقسیم راست** $y=a/b$ نشان می‌دهیم. بنابراین، عمل‌های دوتایی

$$\backslash : A\times A\to A \qquad / : A\times A\to A$$
$$(a,b)\mapsto a\backslash b \qquad (a,b)\mapsto b/a$$

را داریم. از این رو، هر شبه گروه را می‌توان به صورت دستگاه جبری $(A;*,\backslash,/)$ از نوع $\tau=(2,2,2)$ نیز در نظر گرفت. می‌توان نشان داد که اصول موضوع این دستگاه جبری اتحادهای زیر هستند:

$$a\backslash(a*b)=b \quad (1) \qquad a*(a\backslash b)=b \quad (2)$$
$$(a*b)/b=a \quad (3) \qquad (a/b)*b=a \quad (4)$$

برای مثال، بنا به تعریف عمل تقسیم چپ، عضو $a\backslash(a*b)$ جواب منحصر به فرد $a*x=a*b$ است. از طرفی b نیز جواب این معادله است. پس $a\backslash(a*b)=b$. به همین صورت، به راحتی می‌توانید اتحادهای (2) تا (4) را اثبات کنید. خوب است بدانیم که خوشبختانه به تازگی چند متخصص شبه‌گروه و کاربردهای آن در چند دانشگاه کشور مشغول فعالیت شده‌اند.

حلقه و مشبکه. حال دو P - جبر دیگر، هر دو از نوع $\tau=(2,2)$، را معرفی می‌کنیم که اولی، یعنی **حلقه**، یکی دیگر از قدیمی‌ترین دستگاه‌های جبری است (که با جزییات در **فصل ۳** و در درس‌های بعدی مطالعه خواهد شد) و دومی، یعنی **مشبکه**، یکی از اولین مثال‌های دستگاه‌های جامع مدرن‌تر جبری است.

۱۲.۴.۱ تعریف. دستگاه جبری $(R;+,\cdot)$ از نوع $\tau=(۲,۲)$ را **حلقه** می نامیم اگر

(ح۱) دستگاه جبری $(R;+)$ **گروه تعویض پذیر (آبلی)** باشد،

(ح۲) دستگاه جبری $(R;\cdot)$ **نیمگروه** باشد،

(ح۳) برای هر $x,y,z\in R$، اتحادهای **توزیع‌پذیری** زیر برقرار باشند:

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

۱۳.۴.۱ بحث در کلاس

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

۲- دستگاهی جبری که در ساختار آن بیش از یک عمل مطرح می‌شود، هنگامی منسجم‌تر و کارآمدتر است که ارتباطی بین عمل‌های آن وجود داشته باشد. برای مثال، به یاد بیاورید که در تکواره‌ی $(A;*,e)$، ارتباط بین عمل دوتایی $*$ و عمل صفرتایی e به صورت اتحادهای

$$(\forall x\in A)\quad x*e=x=e*x$$

داده شد یا وقتی گروه را به عنوان دستگاهی جبری از نوع $\tau=(2,1,0)$ در نظر گرفتیم، اتحادهای حاصل از **(گ۲)** و **(گ۳)** ارتباط بین عمل‌های گروه را نشان می‌دهند. اتحادهای توزیع‌پذیری در تعریف حلقه نیز ارتباط مهم بین دو عمل دوتایی حلقه را بیان می‌کنند.

۳- اگر در حلقه‌ی R، دستگاه جبری $(R;\cdot)$ نیم‌گروهی تعویض‌پذیر و با همانی باشد، حلقه را **حلقه‌ی تعویض‌پذیر** و **یک‌دار** می‌نامیم؛ زیرا معمولاً عضو همانی ضربی را با نماد **۱** نشان می‌دهیم. برخی از ریاضی‌دانان فقط با حلقه‌های تعوض‌پذیر و یک‌دار سر و کار دارند و از این رو حلقه‌ها را از همان ابتدا دارای عضو همانی ضربی ۱ و به صورت دستگاه جبری $(R;+,\cdot,1)$ از نوع $\tau=(2,2,0)$ (دو عمل دوتایی و یک عمل صفرتایی برای عضو همانی ضربی ۱) در نظر می‌گیرند. البته، برخی دیگر از ریاضی‌دانان این شرایط را قایل نمی‌شوند و با حلقه‌های کلی‌تر، نه لزوماً تعویض‌پذیر و یک‌دار، سروکار دارند. **خوشبختانه هر دو نوع این ریاضی‌دانان در دانشگاه‌های ایران وجود دارند**، و بسیار در کار پژوهشی فعال هستند.

۴- دستگاه جبری دیگری که به گونه‌ای تعمیم دستگاه‌های جبری حلقه و M - مجموعه است مدول نام دارد. این دستگاه جبری را در درس **نظریه‌ی حلقه و مدول** مورد مطالعه قرار می‌دهیم و کاربرد

های بسیاری در سراسر علوم ریاضی و علوم دیگر دارد. در اینجا صرفاً به معرفی آن می‌پردازیم. خوب است تعریف ۱۳.۳.۱ دستگاه جبری M - مجموعه را به خاطر بیاورید. این دستگاه جبری از یک **مجموعه** A و خانواده‌ی $(l_x)_{x\in M}$ به تعداد عضوهای یک **تکواره** M، از عمل‌های یکانی $l_x : A \to A$ تشکیل شده است به طوری که ، اگر نگاره‌ی عمل l_x روی عضو $a \in A$ را با $l_x(a) = xa$ نشان دهیم، اتحادهای $(x * y)a = x(ya)$ و $ea = a$ برقرار هستند. حال اگر به جای مجموعه‌ی A یک گروه آبلی $(A;+)$ و به جای تکواره‌ی M یک حلقه‌ی R در نظر بگیریم، مفهوم R - مدول به صورت زیر به دست می‌آید:

فرض کنیم $(R;+,\cdot)$ یک حلقه و $(A;+)$ گروهی آبلی باشد. فرض کنیم $(l_r)_{r\in R}$ خانواده‌ای از عمل‌های یکانی $l_r : A \to A$ روی A باشد. در این صورت می‌گوییم که A یک R - **مدول**، یا یک مدول روی R ، است اگر اتحاد های طبیعی زیر برقرار باشند:

(الف) $(r+s)a = ra + sa$ (ب) $(rs)a = r(sa)$

(پ) $r(a+b) = ra + rb$ (ت) $1_R a = a$ (اگر R یکدار باشد)

با توجه به بند ۲ بحث ۱۴.۳.۱، متداول است که خانواده‌ی $(l_r)_{r\in R}$ را به صورت تابع زیر در نظر بگیریم:

$$R \times A \to A$$
$$(r,a) \mapsto l_r(a) = ra$$

مثال‌های مدول بسیارند. برای نمونه، مشابه بند ۳ بحث ۱۴.۳.۱، هر حلقه‌ی R یک R - مدول است (**چطور؟**). همچنین، هرگروه آبلی $(A;+)$ به طور طبیعی یک $\mathbb{Z}$ - مدول است، که در آن

$$\mathbb{Z} \times A \to A$$
$$(m,a) \mapsto l_m(a) = ma = a + \cdots + a$$

از این رو، می‌توان گفت که مفهوم مدول تعمیم مفهوم گروه آبلی نیز هست. بیش از این مطلبی در باره‌ی مدول‌ها نمی‌آوریم تا دروس حلقه و مدول و جبر خطی برایتان تازگی داشته باشد.

آخرین نوع دستگاه جبری که معرفی می‌کنیم از اولین مثال‌های **دستگاه جامع جبری** هستند. این دستگاه جبری مدرن‌تر، علاوه بر کاربردهای طبیعی و فراوان آن در **سراسر علوم** (و زندگی روزانه)، زیربنای اصلی منطق، نظریه‌ی مجموعه‌ها، و علوم کامپیوتر است. خوشبختانه ریاضی‌دانانی در دانشگاه‌های ایران وجود دارند که این نوع دستگاه جبری را مطالعه می‌کنند.

۱۴.۴.۱ تعریف. دستگاه جبری $(L;\vee,\wedge)$ از نوع $\tau=(2,2)$ را **مشبکه** می‌نامیم اگر

۱- هر دو دستگاه جبری $(L;\vee)$ و $(L;\wedge)$ **نیم‌گروه تعویض‌پذیر** و **خودتوان** (یعنی نیم‌مشبکه) باشند.

۲- برای هر $x,y\in L$، **قوانین جذب** در L برقرار باشند:

$$x=x\wedge(x\vee y) \quad , \quad x=x\vee(x\wedge y)$$

۱۵.۴.۱ بحث در کلاس

۱- توجه کنید که نمادهای $\vee$ و $\wedge$ از این رو انتخاب شده‌اند که مثال‌های اولیه و اصلی **مشبکه**‌ها، ساختار منطق ($\vee$ برای "**یا**" و $\wedge$ برای "**و**") و مجموعه‌ها ($\vee$ به جای $\cup$ و $\wedge$ به جای $\cap$) هستند.

۲- توجه می‌کنیم که $(L;\vee,\wedge)$ **مشبکه** است اگر اتحادهای زیر برقرار باشند:

(**اتحاد**های شرکت‌پذیری) $x\wedge(y\wedge z)=(x\wedge y)\wedge z$ و $x\vee(y\vee z)=(x\vee y)\vee z$.

(**اتحاد**های تعویض‌پذیری) $x\wedge y=y\wedge x$ و $x\vee y=y\vee x$.

(**اتحاد**های خودتوانی) $x\wedge x=x$ و $x\vee x=x$.

(**اتحاد**های جذب) $x=x\wedge(x\vee y)$ و $x=x\vee(x\wedge y)$.

نکته‌ی قابل توجه این است که، ویژگی‌های عمل دوتایی $\vee$ همتای ویژگی‌های عمل دوتایی $\wedge$ هستند، و همگی برحسب اتحاد داده شده‌اند. همچنین، **قوانین جذب** ارتباط بین این دو عمل را بیان می‌کنند. از این رو، تعویض $\vee$ با $\wedge$ تغییری در این ساختار ایجاد نمی‌کند. یعنی، اگر $(L;\vee,\wedge)$ مشبکه باشد، آنگاه $(L;\wedge,\vee)$ نیز مشبکه است. آیا این مطلب برای دستگاه جبری حلقه نیز درست است؟

۳- مطالب بسیاری در باره‌ی دستگاه جبری مشبکه می‌توان بیان کرد (و کتاب‌ها و مقاله‌های بسیاری نیز نوشته شده‌اند) که خارج از بحث این کتاب هستند. در اینجا صرفاً به ارائه‌ی نکته‌ای مهم و سپس چند مثال اکتفا می‌کنیم. همان طور که بیان شد، استانده‌ترین مثال‌های مشبکه یکی $(\wp(X);\cup,\cap)$ و دیگری به صورت زیر است. فرض کنیم $\leq$ رابطه‌ای ترتیبی در مجموعه‌ی A باشد، به طوری که هر دو عضو $x,y\in A$ دارای سوپریمم (کوچک‌ترین کران بالا) و دارای اینفیمم (بزرگ‌ترین کران پایین) باشند، آنگاه با استفاده از نمادهای

$$x\vee y=sup\{x,y\} \quad , \quad x\wedge y=\inf\{x,y\}$$

دستگاه جبری $(A;\vee=\sup,\wedge=\inf)$ به دست می‌آید که به روشنی **مشبکه** است.

برعکس، اگر $(L;\vee,\wedge)$ **مشبکه** باشد، آنگاه می‌توان رابطه‌ی ترتیبی $\leq$ را در L به صورت زیر تعریف کرد

$$x \le y \quad \Leftrightarrow \quad x \vee y = y$$

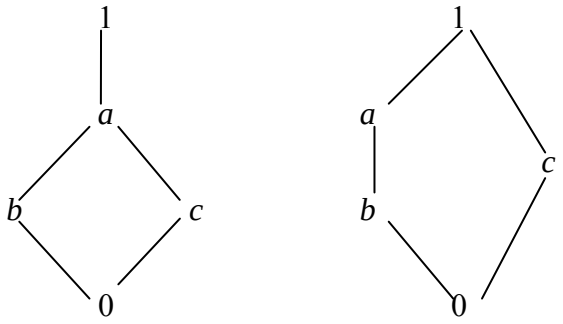
که می‌توانید با استفاده از قوانین جذب نشان دهید که معادل با $x \wedge y = x$ است:

$$x \vee y = y \Rightarrow x \wedge y = x \wedge (x \vee y) = x$$
$$x \wedge y = x \Rightarrow x \vee y = (x \wedge y) \vee y = y$$

حال نشان دهید که، نسبت به این رابطه‌ی ترتیبی، داریم $\sup\{x, y\} = x \vee y$ و $\inf\{x, y\} = x \wedge y$.

از این رو، مفهوم **مشبکه** را به دو صورت می‌توان تعریف کرد: یکی تعریف **جبری ۱۴.۴.۱** و دیگری به صورت مجموعه‌ی مرتب $(A; \le)$ که در آن هر دو عضو هم دارای سوپریمم و هم دارای اینفیمم باشند.

۵- همان‌طور که در درس مبانی علوم ریاضی دیدیم، هر مجموعه‌ی مرتب $(A; \le)$ را می‌توان با نمودارهایی به صورت تصویری زیر نشان داد. یادآوری می‌کنیم که در این نمودارها، اگر یک یا چند پاره‌خط، از پایین به بالا، حرف x را به حرف y وصل کند، به این معنی است که $x < y$ و در غیر این صورت، رابطه‌ای بین x و y وجود ندارد.



(ب) (الف)

روشن است که هر دو نمودار **(الف)** و **(ب)** معرف مشبکه هستند. برای مثال، در (الف)

$$a \vee b = a, \quad a \wedge b = b, \quad a \vee c = 1 = b \vee c, \quad a \wedge c = 0 = b \wedge c$$

و در **(ب)**، $b \vee c = a$.

دستگاه‌های جبری دیگری نیز در این یا آن مبحث از ریاضیات و کاربردها مطرح می‌شوند که متاسفانه، زمان اختصاص داده شده به این فصل از درس فرصت ارائه‌ی آن‌ها را نمی‌دهد!

برای مثال، علاوه بر دستگاه‌های جبری‌ای که در درس‌های دیگر جبر در دوره‌ی کارشناسی خواهیم دید، با اضافه یا کم کردن اصول موضوع دستگاه‌هایی که تاکنون دیدیم نیز دستگاه-های جبری جدیدی به دست می‌آیند.

تمرین ۴.۱

بدون تلاش برای حل کردن تمرین‌ها، نمی‌توانید متوجه شوید که چقدر از مطالب درس را آموخته‌اید.

۱- وجود یا عدم وجود عضو همانی را برای عمل‌های حاصل از تمرین ۱ از بخش۱.۱ بررسی کنید.

۲- بررسی کنید که آیا $(\mathbb{R}\setminus\{1\},*)$، که در آن $a*b=a+b-ab$، یک گروه است؟

۳- تابعی دوسویی از $A=\{a,b,c\}$ به $\mathbb{Z}_3=\{0,1,2\}$ چنان تعریف کنید که جدول کیلی عمل $*$ داده شده در بند ۴ بحث ۹.۴.۱ را به جدول کیلی جمع همنهشتی $+_3$ تبدیل کند:

$$f:\{e,a,b\}\to\{0,1,2\}$$

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

$\rightarrow$

$+_3$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

حال از شرکت‌پذیر بودن $+_3$ نتیجه بگیرید که $*$ نیز شرکت‌پذیر است.

۴- آیا در تعریف شبه‌گروه متناهی، وجود جواب معادله‌های یاد شده به خودی خود شرط منحصر به فردی را ایجاب می‌کند؟

۵- نشان دهید که اگر شبه گروه $(A;*)$ را مانند بحث ۱۱.۴.۱ به صورت دستگاه جبری $(A;*,/,\setminus)$ در نظر بگیریم، آنگاه اتحادهای زیر در آن برقرار هستند:

(1) $a\setminus(a*b)=b$ (3) $(a*b)/b=a$

(2) $a*(a\setminus b)=b$ (4) $(a/b)*b=a$

۶- فرض کنید X مجموعه است. ثابت کنید که علاوه بر $(\mathcal{P}(X);\subseteq)$ دستگاه دوگان آن، یعنی $(\mathcal{P}(X);\supseteq)$، که در آن $\supseteq$ رابطه‌ی عکس شمول $\subseteq$ است، نیز یک مشبکه است.

۷- ثابت کنید که مجموعه‌های مرتب $(\mathbb{N},\leq)$ و $(\mathbb{N},|)$ مشبکه هستند. تعریف اعمال $\vee$ و $\wedge$ را تعیین کنید.

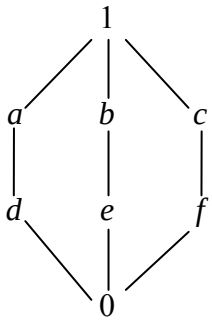
۸- ثابت کنید که مجموعه‌ی توابع حقیقی روی $[0,1]$ همراه با رابطه‌ی $\leq$، که به صورت نقطه‌ای تعریف می‌شود، یعنی

$$f \leq g \Leftrightarrow f(x) \leq g(x) \quad (\forall x)$$

یک مشبکه است. تعریف اعمال $\vee$ و $\wedge$ را تعیین کنید.

۹- نشان دهید که اتحاد خودتوانی در تعریف مشبکه را می‌توان از اتحادهای دیگر آن نتیجه گرفت. (اتحادهای جذب را امتحان کنید).

۱۰- در مشبکه‌ی زیر، عضوهای $a \wedge b$، $a \wedge c$، $d \wedge b$، $d \wedge e$، $d \vee f$، و $d \vee b$ را بیابید.



۵.۱ همریختی دستگاه‌های جبری

پس از معرفی مفهوم دستگاه جامع جبری و مثال‌هایی از آن، حال به مفاهیم **جدی‌تر** مرتبط با این مفهوم می‌پردازیم که توجه بیش‌تر و دقیق‌تر شما را می‌طلبد. در مطالعه‌ی مجموعه‌ها در درس **مبانی علوم ریاضی** دیدیم که توابع وسیله‌ی ارتباط بین مجموعه‌ها هستند. یکی از دلایل اهمیت توابع در این است که اغلب اطلاعات مفیدی در باره‌ی یک مجموعه از مجموعه‌ی دیگر به دست می‌دهند. در مطالعه‌ی هر دستگاه ریاضی، جبری یا غیر جبری، نیز توابع بین آن‌ها از اهمیت ویژه‌ای برخوردار هستند. البته توابع بین دستگاه‌های ریاضی باید ویژگی‌هایی داشته باشند که بتوانند اطلاعات مفید بیش‌تری را در باره‌ی یک دستگاه از دستگاه دیگر به دست دهند. برای مثال، در دروس آنالیز ریاضی، توابع پیوسته، مشتق‌پذیر، یا انتگرال‌پذیر مفیدتر هستند.

توابع بین دستگاه‌های جبری از چه نظر باید خاص باشند؟

اگر قرار است که اطلاعات جبری بین دو دستگاه جبری از نوع τ را منتقل کنند، باید ابتدا ارتباطی بین هر یک از عمل‌های یک دستگاه با همتای همان عمل در دستگاه دیگر برقرار کنند. برای روشن‌تر شدن مطلب، در بحث زیر شرکت کنید.

۱.۵.۱ بحث در کلاس

۱- ابتدا ببینیم که انتظارمان از رفتار توابع بین دو دستگاه جبری نسبت به **عمل صفرتایی** چه باید باشد؟ یادآوری می‌کنیم که هر عمل صفرتایی در A در واقع عضوی چون a_0 را در A مشخص می‌کند. فرض کنیم $(A;a_0)$ و $(B;b_0)$ دستگاه‌های جبری از نوع $\tau=(0)$ باشند. طبیعی است که توابعی از A به B مورد نظر باشند که a_0 را بر b_0 بنگارند. یعنی، $f:A\to B$ به طوری که $f(a_0)=b_0$؛ **این طور نیست؟**

۲- حال ببینیم که انتظارمان از رفتار توابع بین دو دستگاه جبری با **عمل ۱- تایی** (یکانی) چه باید باشد؟ فرض کنیم $\lambda^A:A\to A$ و $\lambda^B:B\to B$ اعمالی یکانی باشند. چه انتظاری از تابع $f:A\to B$ داریم؟ تابع f عضو $x\in A$ را بر $f(x)\in B$ می‌نگارد. از طرفی λ^A عضو x را در درون A به $\lambda^A(x)$، و λ^B عضو $f(x)$ را در درون B به $\lambda^B(f(x))$ تغییر می‌دهد. یقیناً شما نیز مانند ما انتظار دارید که f عضو $\lambda^A(x)$ از A را بر عضو $\lambda^B(f(x))$ در B بنگارد، یعنی

$$f(\lambda^A(x))=\lambda^B(f(x))$$

به عبارت دیگر، $f\circ\lambda^A=\lambda^B\circ f$ (می‌توان گفت که f باید از عمل λ^A عبور کند). از این رو، اگر در مثالی، حاصل عمل یکانی را به جای $\lambda(x)$ با نمادی ساده‌تر، برای مثال $\overline{x}$، نشان دهیم آنگاه $f(\overline{x})=\overline{f(x)}$. به زبان نمودار، یعنی باید مربع زیر تعویض‌پذیر باشد:

$$\begin{array}{ccccc}
x & - - - & - - - & - \text{---}\to & f(x) \\
| & A & \xrightarrow{f} & B & | \\
| & \lambda^A\downarrow & & \downarrow\ \lambda^B & | \\
\downarrow & A & \xrightarrow{f} & B & \downarrow \\
\lambda^A(x) & \cdots\cdots & \cdots\cdots & \cdots\cdots\to & f(\lambda^A(x))=\lambda^B(f(x))
\end{array}$$

۳- قبل از ارائه‌ی تعریف جامع توابع بین دستگاه‌های جبری، انتظارمان از رفتار توابع بین دو دستگاه جبری با **عمل ۲- تایی** را نیز مطرح می‌کنیم. فرض کنیم $*^A$ عملی دوتایی در A و $*^B$ عملی دوتایی در B باشد. چه انتظاری از تابع $f: A \to B$ داریم؟ با توجه به بحث **۱۲.۳.۱**، انتظار داریم که $x *^A y$ از (جدول کیلی) A بر $f(x) *^B f(y)$ از (جدول کیلی) B نگاشته شود. یعنی،

$$f(x *^A y) = f(x) *^B f(y)$$

(یعنی، f از عمل $*^A$ عبور می‌کند یا **حافظ** آن است). به زبان نمودار، یعنی باید مربع زیر تعویض‌پذیر باشد:

$$\begin{array}{ccccc}
(x,y) & - & - & \dashrightarrow & (f(x),f(y)) \\
| & A\times A & \xrightarrow{(f,f)} & B\times B & | \\
| & *^A\downarrow & & \downarrow *^B & | \\
\downarrow & A & \xrightarrow{f} & B & \downarrow \\
x *^A y & \cdots & \cdots & \to & f(x *^A y) = f(x) *^B f(y)
\end{array}$$

حال آماده‌ایم که موارد بالا را به همه‌ی دستگاه‌های جبری تعمیم دهیم.

۲.۵.۱ تعریف. فرض کنیم $(A;F)$ و $(B;F')$ دستگاه‌هایی جبری از نوع $\tau = (n_\lambda)_{\lambda\in\Omega}$ باشند. تابع $f: A \to B$ را **همریختی** یا **تابع جبری** می‌نامیم اگر برای هر عمل n- تایی $\lambda^A: A^n \to A$، تابع f، به اصطلاح، **حافظ عمل** λ^A باشد یا از آن عبور کند، به این معنی که برای هر $a_1,\cdots,a_n \in A$،

$$f(\lambda^A(a_1,\cdots,a_n)) = \lambda^B(f(a_1),\cdots,f(a_n))$$

یا $f\circ\lambda^A = \lambda^B\circ(f,\cdots,f)$. به زبان نمودار، یعنی برای هر λ^A، نمودار زیر تعویض‌پذیر باشد:

$$\begin{array}{ccccc}
(a_1,\cdots,a_n) & - & - - - & \dashrightarrow & (f(a_1),\cdots,f(a_n)) \\
| & A^n & \xrightarrow{(f,\cdots,f)} & B^n & | \\
\lambda^A & \downarrow & & \downarrow & \lambda^B \\
\downarrow & A & \xrightarrow{f} & B & \downarrow \\
\lambda^A(a_1,\cdots,a_n) & \cdots & \cdots\cdots\to & f(\lambda^A(a_1,\cdots,a_n)) & = \lambda^B(f(a_1),\cdots,f(a_n))
\end{array}$$

۳.۵.۱ بحث در کلاس. مثال‌های همریختی یا تابع جبری بسیارند. چند مثال را در زیر می‌آوریم، و مثال‌های بسیار دیگری را نیز به مرور در سراسر این کتاب خواهیم آورد. قصد ما در این فصل بیشتر بیان مطالب و هشدارهایی است که در سراسر دروس جبر با آن‌ها مواجه خواهید شد.

۱- چندان مشکل نیست که نشان دهید تابع زیر یک **همریختی** است:

$$f:(\mathbb{R};+,-,\circ)\to(\mathbb{R}^+;\cdot,\cdot^{-1},1)$$
$$f(x)=e^x$$

که در آن $\mathbb{R}^+=\{x\in\mathbb{R}\mid x>\circ\}$. توجه کنید که عمل‌های دو طرف، گرچه همنوع هستند، ولی متفاوت‌اند. داریم

$$f(x+y)=e^{x+y}=e^x\cdot e^y=f(x)\cdot f(y)$$ (حفظ عمل دوتایی)

$$f(-x)=e^{-x}=(e^x)^{-1}=f(x)^{-1}$$ (حفظ عمل یکانی)

$$f(\circ)=e^{\circ}=1$$ (حفظ عمل صفرتایی)

۲- نشان هید که تابع زیر همریختی **نیست**:

$$f:(\mathbb{Z};\cdot)\to(\mathbb{Z};\cdot)$$
$$n\mapsto 2n$$

حال چند نکته‌ای **بسیار مهم** را در باره‌ی همریختی‌ها بیان می‌کنیم که در سراسر دروس جبر به طور صریح یا ضمنی با آن‌ها مواجه خواهیم شد، پس خوب است دلایل آن‌ها را بدانیم.

۴.۵.۱ بحث در کلاس. (این نکته بسیار با اهمیت است که) در تعریف P - جبرها دیدیم که وقتی P - جبری بیش از یک عمل داشته باشد، معمولاً ارتباطی بین این عمل‌ها قایل می‌شویم. برای مثال، ویژگی توزیع‌پذیری ضرب روی جمع در حلقه‌ها، یا ویژگی جذب در مشبکه‌ها را یادآوری می‌کنیم. گاهی به دلیل ارتباط‌های بین عمل‌ها،

تابع بین دستگاه‌های جبری که چند عمل را حفظ کند، ممکن است به خودی خود چند عمل دیگر آن دستگاه را نیز حفظ کند!

برای مثال، در قضیه‌ی زیر خواهیم دید که اگر تابع f بین دو گروه، عمل دوتایی گروه را حفظ کند، آنگاه توانمندی تلفیق ویژگی‌های (گ۱) تا (گ۳) گروه‌ها ایجاب می‌کند که f عمل صفرتایی (یعنی، عضو همانی) و عمل یکانی (یعنی، وارون‌گیری) گروه را به خودی خود حفظ کند!

هشدار می‌دهیم که بسیاری از مطالبی که در مورد دستگاه‌های جبری کلاسیک گروه، حلقه، مدول، و فضای برداری رخ می‌دهند، لزومی ندارد در همه‌ی P - جبرها رخ دهند!

برای مثال، تابع بین تکواره‌ها که عمل دوتایی آن را حفظ کند، لزومی ندارد که عمل صفرتایی (یعنی عضو همانی) را نیز به خودی خود حفظ کند. به عنوان مثالی ساده، تابع ثابت صفر

$$f:(\mathbb{Z};+,\circ)\to(\mathbb{Z};\cdot,1)$$
$$x\mapsto\circ$$

بین این دو تکواره به روشنی عمل ۲- تایی را حفظ می‌کند. یعنی،

$$f(x+y)=\circ=\circ\cdot\circ=f(x)\cdot f(y)$$

ولی عضو همانی تکواره‌ی جمعی $(\mathbb{Z};+,\circ)$، یعنی عدد $\circ$، را به عضو همانی تکواره‌ی ضربی $(\mathbb{Z};\cdot,1)$، یعنی عدد ۱، نمی‌نگارد. از این رو، **برای توابع بین تکواره‌ها**، معمولاً **شرط حفظ عمل صفرتایی را نیز، علاوه بر حفظ عمل دوتایی، قایل می‌شویم.** حال قضیه‌ی جالب زیر را ببینید.

۵.۵.۱ قضیه. فرض کنیم $(A;*,(\cdot)^{-1},e)$ و $(B;*',(\cdot)^{-1},e')$ گروه باشند. اگر تابع $f:A\to B$ عمل دوتایی را حفظ کند، یعنی، برای هر $x,y\in A$، $f(x*y)=f(x)*'f(y)$، آنگاه f عمل‌های صفرتایی و ۱- تایی را نیز حفظ می‌کند، یعنی،

$$f(e)=f(e') \quad \text{و} \quad f(x^{-1})=f(x)^{-1}$$

اثبات. به فن اثبات توجه کنید! داریم

$$\begin{aligned} f(e) &= f(e*e) && \text{(زیرا . . .)}\\ &= f(e)*'f(e) && \text{(زیرا . . .)}\end{aligned}$$

حال، از این تساوی نتیجه می‌گیریم که

$$\begin{aligned} f(e)^{-1}*'f(e) &= f(e)^{-1}*'(f(e)*'f(e)) && \text{(چطور؟)}\\ \Rightarrow e' &= (f(e)^{-1}*'f(e))*'f(e) && \text{(چرا؟)}\\ &= e'*'f(e)=f(e)\end{aligned}$$

پس تابع f عضو همانی را بر عضو همانی می‌نگارد. توجه کنید که چطور از همه‌ی شرط‌های (گ۱)-(گ۳) گروه استفاده شد! برای اثبات اینکه تابع f وارون x را به وارون $f(x)$ می‌نگارد، باید نشان دهیم که $f(x^{-1}) = f(x)^{-1}$. دلیل هر مرحله‌ی زیر را بنویسید:

$$e' = f(e) = f(x * x^{-1}) = f(x) *' f(x^{-1})$$

به همین صورت، می‌توان نشان داد که $f(x^{-1}) *' f(x) = e'$ ، و در نتیجه $f(x^{-1})$ وارون $f(x)$ است، یعنی $f(x^{-1}) = f(x)^{-1}$. این مطالب حکم‌های قضیه را اثبات می‌کنند. ■

۶.۵.۱ بحث در کلاس. نکته‌هایی را که در اینجا بیان می‌کنیم شاید مهم‌تر از بحث ۴.۵.۱ باشند. فرض کنیم A و B دستگاه‌هایی جبری از نوع τ (نه لزوماً با ویژگی) باشند و تابع $f : A \to B$ همریختی، یعنی حافظ عمل‌ها، باشد. روشن است که $f(A)$ نیز دستگاهی جبری از نوع τ است، زیرا، به روشنی $f(A)$ نسبت به هر عمل n- تایی λ^B بسته است:

$$\lambda^B(f(a_1), \cdots, f(a_n)) = f(\lambda^A(a_1, \cdots, a_n)) \in f(A)$$

حال سؤال‌های زیر مطرح می‌شوند:

۱- آیا اگر A دارای ویژگی σ باشد، آنگاه $f(A)$ نیز دارای ویژگی σ است؟
۲- آیا اگر $f(A)$ دارای ویژگی σ باشد، آنگاه A نیز دارای ویژگی σ است؟

توجه کنید که تابع f کاری به عضوهای بیرون از نگاره‌اش ندارد و از این رو در بالا تنها صحبت از $f(A)$ کرده‌ایم نه تمام B. به همین دلیل، در سؤال‌های بالا، اغلب f را پوشا در نظر می‌گیریم که در آن صورت $B = f(A)$. به مرور خواهیم دید که **پاسخ** به هر دو سؤال در حالت کلی **منفی است!**

۷.۵.۱ تعریف. اگر پاسخ به **سؤال ۱** مثبت باشد (یعنی، $A \models \sigma \Rightarrow f(A) \models \sigma$) می‌گوییم که f ویژگی σ را **حفظ می‌کند**، و اگر پاسخ به **سؤال ۲** مثبت باشد (یعنی، $f(A) \models \sigma \Rightarrow A \models \sigma$) می‌گوییم که f ویژگی σ را **بازتاب** می‌دهد یا منعکس می‌کند.

قضیه‌ی زیر اهمیت ویژگی‌هایی را نشان می‌دهد که برحسب **اتحاد**ها بیان می‌شوند. **به مرور بیشتر به اهمیت اتحادها پی خواهیم برد.**

۸.۵.۱ قضیه. *فرض کنیم $A, B \in \mathcal{A}\lg(\tau)$ و $f : A \to B$ همریختی باشد. در این صورت،*
*۱- اگر معادله‌ی $p = q$ در A برقرار، یعنی **اتحاد**، باشد آنگاه در $f(A)$ نیز **اتحاد** است.*

۲- *اگر f یک به یک باشد آنگاه عکس حکم* **۱** *نیز برقرار است.*

اثبات

۱- فرض کنیم $f(a_1),\cdots,f(a_n)\in f(A)$ ، که در آن $a_1,\ldots,a_n\in A$. چون معادله‌ی $p=q$ در A اتحاد است، پس

$$p(a_1,\cdots,a_n)=q(a_1,\cdots,a_n)$$

چون در عبارت‌های دو طرف این تساوی، تنها عضوها و عمل‌های دستگاه جبری A به‌کار رفته‌اند (**۱۱.۲.۱** را ببینید) و f عمل‌ها را **حفظ** می‌کند، بدون ذکر جزییات، نتیجه می گیریم که f از p و q نیز عبور می کند، یعنی

$$f(p(a_1,\ldots,a_n))=p(f(a_1),\ldots,f(a_n))$$

و

$$f(q(a_1,\ldots,a_n))=q(f(a_1),\ldots,f(a_n))$$

از این رو، چون $f(p(a_1,\ldots,a_n))=f(q(a_1,\ldots,a_n))$ ، در نتیجه

$$p(f(a_1),\ldots,f(a_n))=p(f(a_1),\ldots,f(a_n))$$

و بنابراین، $f(A)\models(p=q)$.

۲- فرض کنیم معادله‌ی $p=q$ در $f(A)$ اتحاد باشد و $a_1,\cdots,a_n\in A$. در این صورت،

$$p(f(a_1),\cdots,f(a_n))=q(f(a_1),\cdots,f(a_n))$$

مشابه بند **۱**، نتیجه می‌گیریم که

$$f(p(a_1,\cdots,a_n))=f(q(a_1,\cdots,a_n))$$

حال چون f یک به یک است، داریم

$$p(a_1,\cdots,a_n)=q(a_1,\cdots,a_n)$$

و در نتیجه $p=q$ در A اتحاد است. ■

۹.۵.۱ بحث در کلاس. فرض کنیم $(A;*)$ و $(B;*')$ گروهواره باشند و $f:A\to B$ همریختی باشد (یعنی، برای هر $x,y\in A$، $f(x*y)=f(x)*'f(y)$). در این صورت، بنابر قضیه‌ی ۸.۵.۱، اگر $*$ شرکت‌پذیر، آبلی، یا خودتوان باشد، آنگاه $*'$ نیز در $f(A)$ دارای این ویژگی‌ها است، و اگر f یک به یک نیز باشد، همریختی f این ویژگی‌ها را منعکس نیز می‌کند. برای درک بهتر اثبات قضیه‌ی بالا، حفظ و بازتاب شرکت‌پذیری را بررسی می‌کنیم. فرض کنیم عمل $*$ در A شرکت‌پذیر باشد و $x'=f(x),y'=f(y),z'=f(z)\in f(A)$. در این صورت، چون $*$ شرکت‌پذیر است، داریم

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

حال، f را بر دو طرف این تساوی اثر می‌دهیم، و با استفاده از همریختی بودن f، نتیجه می‌گیریم که (دلیل هر مرحله را بیان کنید):

$$\begin{aligned}
& f(x*(y*z))=f((x*y)*z)\\
\Rightarrow\quad & f(x)*'f(y*z)=f(x*y)*'f(z)\\
\Rightarrow\quad & f(x)*'(f(y)*'f(z))=(f(x)*'f(y))*'f(z)\\
\Rightarrow\quad & x'*'(y'*'z')=(x'*'y')*'z'
\end{aligned}$$

پس، $*'$ در $f(A)$ نیز شرکت‌پذیر است.

برعکس، فرض کنیم همریختی f یک به یک نیز باشد و $*'$ در $f(A)$ شرکت‌پذیر باشد. در این صورت، چون f همریختی و یک به یک است، برای هر $x,y,z\in A$ داریم

$$\begin{aligned}
& (f(x)*'f(y))*'f(z)=f(x)*'(f(y)*'f(z))\\
\Rightarrow\ & f(x*y)*'f(z)=f(x)*'f(y*z)\\
\Rightarrow\ & f((x*y)*z)=f(x*(y*z))\\
\Rightarrow\ & (x*y)*z=x*(y*z)
\end{aligned}$$

حال، واژه‌ی **اساساً یکسان** یا **یک‌ریختی** را که قبلاً به کار بردیم، ریاضی‌گونه معرفی می‌کنیم.

۱۰.۵.۱ تعریف. می‌گوییم که دو دستگاه جبری از نوع τ چون A و B **یک‌ریخت** هستند، و می‌نویسیم $A\cong B$، اگر یک همریختی دوسویی چون f بین آن‌ها وجود داشته باشد. همریختی دوسویی f را **یک‌ریختی** می‌نامیم.

روشن است که اگر تابع f بین دو دستگاه جبری یک‌ریختی باشد، چون دوسویی است پس به عنوان تابع، وارون دارد. قضیه‌ی زیر نشان می‌دهد که خوشبختانه تابع وارون هر یک‌ریختی خود یک-

ریختی (حافظ عمل‌ها) است. **به فن اثبات توجه کنید** زیرا چند بار دیگر آن را، در این درس و درس-های دیگر جبری، به کار خواهید برد.

۱۱.۵.۱ قضیه. فرض کنیم $f : A \to B$ یک یک‌ریختی (همریختی **دوسویی**) بین دستگاه‌های جبری از نوع یکسان، باشد. در این صورت، تابع وارون آن نیز یک یک‌ریختی (همریختی دوسویی) است.

اثبات. باید نشان دهیم که برای هر عمل n - تایی و هر $b_1, \cdots, b_n \in B$،

$$f^{-1}(\lambda^B(b_1, \cdots, b_n)) = \lambda^A(f^{-1}(b_1), \cdots, f^{-1}(b_n)) \qquad (*)$$

به این منظور، توجه می‌کنیم که اثر همریختی f بر طرف چپ برابر است با $\lambda^B(b_1, \cdots, b_n)$ و همچنین بر طرف راست برابر است با

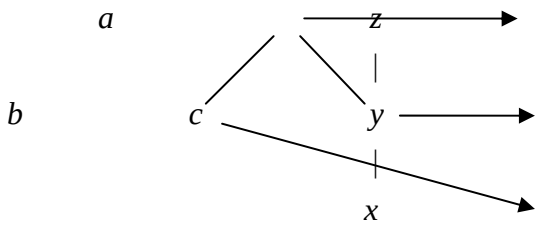
$$f(\lambda^A(f^{-1}(b_1), \cdots, f^{-1}(b_n))) = \lambda^B(ff^{-1}(b_1), \cdots, ff^{-1}(b_n))$$
$$= \lambda^B(b_1, \cdots, b_n)$$

حال می‌توان گفت که، چون حاصل تابع **یک به یک** f بر دو عضو یکسان شد، آن دو عضو، یعنی دو طرف $(*)$، یکسان هستند! **جالب بود؟** ■

۱۲.۵.۱ بحث در کلاس. (اختیاری) قضیه‌ی جالب بالا لزوماً برای دستگاه‌های غیر جبری **درست نیست**. برای مثال، اگر در مجموعه‌ی مرتب $A = \{a, b, c\}$ قرار دهیم $b, c < a$ و در $B = \{x, y, z\}$ قرار دهیم $x < y < z$، آنگاه تابع دوسویی

x	a	b	c
$f(x)$	z	x	y

از A به B حافظ ترتیب است (برای مثال، $b \le a$ و $f(b) = x \le z = f(a)$):



در حالی که تابع وارون آن ترتیب را **حفظ نمی‌کند** (برای مثال، $x \le y$ ولی $f^{-1}(x) = b \not\le c = f^{-1}(y)$). پس، قضیه‌ی بالا برای دستگاه‌های مرتب لزوماً برقرار نیست! از این رو، تابع دوسویی f بین دو مجموعه‌ی مرتب را وقتی یک‌ریختی می‌نامیم که هر دو تابع f و f^{-1} حافظ ترتیب باشند. در درس **توپولوژی** نیز خواهید دید که این تذکر در باره‌ی دستگاه‌های توپولوژیکی نیز صادق است. از این رو، اغلب ریاضی‌دانان ترجیح می‌دهند که **یک‌ریختی** را با شرط **وارون‌پذیری** (به جای دوسویی بودن) تعریف کنند، که البته، بنابر قضیه‌ی **۱۱.۵.۱**، برای دستگاه‌های جبری با تعریف **۱۰.۵.۱** معادل است.

۱۳.۵.۱ بحث در کلاس (اختیاری) در این بند به **نکته‌ی بسیار مهم** دیگری اشاره می‌کنیم. می دانیم که اگر همریختی f از دستگاه جبری A به دستگاه جبری B یک به یک (یا پوشا) باشد، آنگاه f **به عنوان تابع** دارای **وارون چپ** (یا **وارون راست**) از **مجموعه‌ی** B به **مجموعه‌ی** A است. نکته‌ی مهم این است که:

ممکن است هیچ‌یک از این وارون‌ها یک همریختی از دستگاه جبری B به دستگاه جبری A نباشد!

برای مثال، همریختی شمولی

$$i : (\{0,2\};\oplus_4) \rightarrowtail \mathbb{Z}_4 = (\{0,1,2,3\};\oplus_4)$$

را در نظر بگیرید. چهار تابع زیر وارون چپ برای تابع i هستند (**چطور؟**):

x	0	1	2	3
$f(x)$	0	0	2	2

x	0	1	2	3
$g(x)$	0	0	2	0

x	0	1	2	3
$k(x)$	0	2	2	2

x	0	1	2	3
$l(x)$	0	2	2	0

ولی هیچ‌یک از این توابع همریختی نیستند. برای مثال،

$$f(1\oplus_4 1)=f(2)=2 \quad \text{در حالی که} \quad f(1)\oplus_4 f(1)=0\oplus_4 0=0\neq 2$$
$$k(1\oplus_4 1)=k(2)=2 \quad \text{در حالی که} \quad k(1)\oplus_4 k(1)=2\oplus_4 2=0\neq 2$$

اینکه تحت چه شرایطی یکی از وارون‌های چپ یا راست **همریختی** باشد، قسمت زیادی از پژوهش‌های روی دستگاه‌های جبری (یا حتی غیر جبری) را به خود اختصاص داده است!

قضیه‌ی زیر نیز جالب توجه است. تکمیل اثبات ساده‌ی آن را به عهده‌ی **شما خوبان** می‌گذاریم!

۱۴.۵.۱ *قضیه.* *یک‌ریختی دستگاه‌های جبری رابطه‌ای هم‌ارزی است.*

اثبات. باید نشان دهیم که رابطه‌ی $\cong$ انعکاسی، تقارنی، و متعدی است. ابتدا توجه می‌کنیم که تابع همانی $id_A : A\to A$ روی دستگاه جبری A یک‌ریختی است، و در نتیجه $A\cong A$. حال اگر $f : A\to B$ یک یک‌ریختی بین دستگاه‌های جبری باشد آنگاه، بنابر قضیه‌ی ۱۱.۵.۱، $f^{-1} : B\to A$ نیز یک‌ریختی است. در پایان، فرض کنید توابع $A\xrightarrow{f} B\xrightarrow{g} C$ یک‌ریختی هستند و **نشان دهید** که $g\circ f : A\to C$ نیز یک‌ریختی (حافظ عمل‌ها) است.

۱۵.۵.۱ بحث در کلاس با توجه به قضیه‌ی ۱۴.۵.۱، دستگاه‌های جبری یک‌ریخت در یک رده قرار می‌گیرند و از این رو دستگاه‌های جبری یک‌ریخت را **اساساً یکسان** می‌نامیم. روشن است که تعداد عضوهای (عدد اصلی) دستگاه‌های جبری موجود در یک رده‌ی یک‌ریختی، یکسان هستند. حال، این سؤال بسیار مهم مطرح می‌شود که دستگاه‌های جبری با عدد اصلی α و از یک نوع معین τ و دارای ویژگی‌های مشخص P به چه دسته‌هایی، بر حسب یک‌ریختی، تقسیم می‌شوند؟ یعنی، آیا می‌توان نماینده‌ای آشنا و مشخص از هر رده‌ی هم‌ارزی (تحت یک‌ریختی) معرفی کرد؟ برای مثال، در بحث ۱۲.۳.۱ دیدیم که، برحسب یک‌ریختی، تکواره‌های دو عضوی تنها به دو دسته تقسیم می‌شوند و جدول‌های کیلی هر یک از این دو دسته به صورت زیر هستند:

$*_1$	e	f
e	e	f
f	f	e

$*_2$	e	f
e	e	f
f	f	f

توجه می‌کنیم که $(\mathbb{Z}_2;+_2)$، با جدول زیر، نماینده‌ی آشنایی برای رده‌ی مربوط به دستگاه‌های جبری با عمل $*_1$ و $(\mathbb{Z}_2;\cdot_2)$، با جدول زیر، نماینده‌ی آشنایی برای رده‌ی مربوط به دستگاه‌های جبری با عمل $*_2$ هستند:

$+_2$	0	1
0	0	1
1	1	0

$\cdot_2$	0	1
0	0	0
1	0	1

همچنین، توجه می‌کنیم که تکواره‌ای که با جدول $*_1$ مشخص شده است گروه است ولی دومی چنین نیست. از این رو، همه‌ی گروه‌های دو عضوی در یک رده‌ی یک‌ریختی قرار دارند.

به عنوان مثالی دیگر، با توجه به بند ۳ بحث ۹.۴.۱، تا حد یک‌ریختی، تنها یک دسته گروه سه عضوی وجود دارد که جدول کیلی عمل آن‌ها به صورت زیر است:

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

توجه می‌کنیم که گروه همنهشتی $(\mathbb{Z}_3;+_3)$ نماینده‌ی شناخته شده‌ای برای این دسته است. مشاهده می‌کنیم که تابع تغییر نام

x	e	a	b
$f(x)$	0	1	2

جدول بالا را به جدول گروه $\mathbb{Z}_3$ ، یعنی

$+_3$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

تبدیل می کند. پس، تابع دوسویی f حافظ عمل، یعنی یک یک‌ریختی، است.

ریاضی‌دانان بسیاری، که در ایران نیز وجود دارند، در موضوع یافتن نماینده‌هایی مشخص و آشنا برای رده‌های یک‌ریختی جبرها، به ویژه گروه‌ها، پژوهش می‌کنند. در فصل ۲ کمی بیشتر در این باره صحبت می‌کنیم.

تمرین ۵.۱

رفته رفته تبحر شما بیش‌تر می‌شود

۱- نشان دهید که گروه $(\mathbb{Z}_n;\oplus_n)$ با گروه $(\mathbb{Z}/\equiv_n;\overline{\oplus}_n)$ یک‌ریخت است.

۲- فرض کنید $f:A\to B$ همریختی است. نشان دهید که $f\times f:A\times A\to B\times B$ با تعریف $(f\times f)(a,a')=(f(a),f(a'))$ نیز همریختی است.

۳- نشان دهید که اگر تابع $f:(A;*,\backslash,/)\to(B;*,\backslash,/)$ بین شبه گروه‌ها عمل * را حفظ کند، آنگاه به خودی خود دو عمل دیگر را نیز حفظ می‌کند.

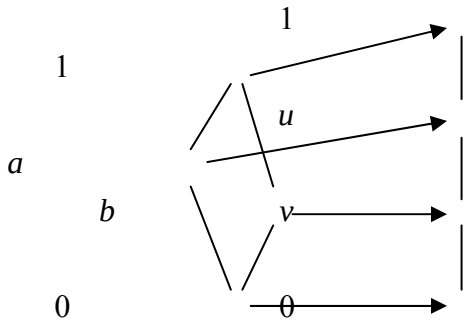
۴- فرض کنید که $Hom(A,B)$ مجموعه‌ی همه‌ی همریختی‌ها از گروهواره‌ی $(A,*_A)$ به گروهواره‌ی $(B,*_B)$ باشد. آیا عمل دوتایی * با تعریف

$$(f*g)(a)=f(a)*_B g(a)$$

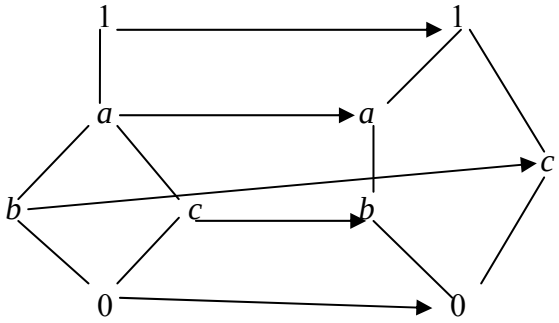
روی $Hom(A,B)$ خوش‌تعریف است؟ اگر A و B تعویض‌پذیر (آبلی) باشند، چطور؟ آیا اگر A و B گروه‌هایی آبلی باشند، آنگاه $Hom(A,B)$ نیز چنین است؟

۵- فرض کنید $(M,*)$ تکواره است. ساختار جبری A را با در نظر گرفتن $A=M$ به عنوان مجموعه‌ی زمینه و عمل‌های یکانی $\varphi_s:A\to A$ (برای هر $s\in M$) با تعریف $\varphi_s(x)=sx$، می‌سازیم. ثابت کنید که $(Hom(A,A),\circ)\cong(M,*)$ که در آن $Hom(A,A)$ مجموعه‌ی همریختی‌های از A به A است. (توجه کنید که، همریختی بودن $f\in Hom(A,A)$ به این معنی است که $f(\varphi_s(x))=\varphi_s(f(x))$ یا $f(sx)=sf(x)$.)

۶- نشان دهید که نه تنها تابع زیر یک یک‌ریختی مشبکه‌ای نیست بلکه هیچ یک‌ریختی بین این دو مشبکه وجود ندارد:



۷- ابتدا نشان دهید که تابع زیر یک یک‌ریختی مشبکه‌ای نیست. سپس حدس بزنید که آیا هیچ یک‌ریختی مشبکه‌ای می‌تواند بین این دو مشبکه وجود داشته باشد؟



۶.۱ زیردستگاه جبری و حاصل‌ضرب

همان‌طور که به کمک عمل‌های اجتماع، اشتراک، ضرب، افراز، و تشکیل زیرمجموعه، از مجموعه‌ها مجموعه‌های جدیدی می‌سازیم، روش‌های بسیاری برای تولید دستگاه‌های جبری جدید از دستگاه‌های داده شده وجود دارند، که به **مرور** در درس‌های جبر خواهیم دید. سه روش از مهم‌ترین و اساسی‌ترین این روش‌ها، تشکیل **زیردستگاه**، **انواع ضرب**، و **خارج قسمت** جبرها است، که سومی توجه ویژه‌ای را می‌طلبد. در این بخش، مفهوم زیردستگاه و ضرب را مطالعه می‌کنیم.

می‌دانیم که $\mathbb{N}\subseteq\mathbb{Z}$ و عمل جمع در $\mathbb{N}$ **اساساً** همان عمل جمع در $\mathbb{Z}$ است. پس، طبیعی است که گروهواره‌ی $(\mathbb{N};+)$ را **زیرگروهواره**‌ی $(\mathbb{Z};+)$ بدانیم. این پدیده را برای دستگاه‌های کلی جبری تعریف و مورد مطالعه قرار می‌دهیم. ابتدا مطلب زیر را می‌آوریم.

۱.۶.۱ تعریف. فرض کنیم $\lambda^A : A^n \to A$ عملی n- تایی است و $B\subseteq A$. می‌گوییم که مجموعه‌ی B تحت (یا نسبت به) عمل λ^A **بسته** است اگر برای هر $b_1,\cdots,b_n \in B$، حاصل عمل $\lambda^A(b_1,\cdots,b_n)$ متعلق به B باشد، یعنی $\lambda^A(b_1,\cdots,b_n)\in B$.

۲.۶.۱ بحث در کلاس. روشن است که اگر $B\subseteq A$ تحت λ^A بسته باشد، آنگاه λ^A تابعی از B^n به B، یعنی عملی n- تایی، در B به دست می‌دهد که آن را تحدید عمل λ^A بر B می‌نامیم و معمولاً آن را به‌جای $\lambda^A|_{B^n}$ با نماد λ^B، یا اغلب با همان نماد λ^A یا λ نشان می‌دهیم. برای مثال،

عمل جمع $+_{\mathbb{N}}$ در $\mathbb{N}$ تحدید عمل جمع $+_{\mathbb{Z}}$ در $\mathbb{Z}$ است، و همواره هر دو را با یک نماد $+$ نشان می‌دهیم. همچنین، چون $B=\{\circ,2\}$ تحت عمل جمع همنهشتی به پیمانه‌ی ۴ (یعنی، عمل $+_4$ در $\mathbb{Z}_4=\{\circ,1,2,3\}$) بسته است، پس عمل $+_4$ بر B تحدید می‌شود. ولی همین مجموعه‌ی $B=\{\circ,2\}$ تحت عمل $+_3$ در $\mathbb{Z}_3=\{0,1,2\}$ بسته نیست (**چرا؟**) همچنین، توجه کنید که عمل $+_3$ تحدید عمل $+_4$ نیست، زیرا، برای مثال، $2+_3 1=0$ در حالی که (به پیمانه‌ی 4) $2+_4 1=3\neq 0$. حال، **تعریف جامع** زیر را می‌آوریم.

۳.۶.۱ تعریف. فرض کنیم $A,B\in \mathcal{A}\mathrm{lg}(\tau)$ دو دستگاه جبری از نوع τ باشند. در این صورت، اگر $B\subseteq A$ و هر عمل λ^B تحدید عمل همتایش λ^A باشد (یعنی B نسبت به هر عمل λ^A بسته باشد)، آنگاه می‌گوییم که دستگاه جبری B **زیردستگاه** جبری A (یا جبر B **زیرجبر** A) است و، برای تاکید، به‌جای $B\subseteq A$ می نویسیم $B\leq A$.

۴.۶.۱ بحث در کلاس. مثال‌های **زیردستگاه** جبری بسیارند و شما خود می‌توانید تعدادی از آن‌ها را بیان کنید. ما سعی می‌کنیم **نکته‌ها** را بیاوریم.

۱- برخی شرط ناتهی بودن را برای دستگاه‌های جبری قایل می‌شوند، ولی ما ترجیح دادیم که این محدودیت را قایل نشویم. از این رو، مجموعه‌ی تهی به روشنی زیردستگاه جبری هر دستگاه جبری‌ای است که دارای عمل **صفرتایی نباشد**! برای مثال، مجموعه‌ی تهی می‌تواند زیرگروهواره و زیرنیم‌گروه باشد ولی نمی‌تواند زیرتکواره یا زیرگروه باشد.

۲- با وجودی که هر دو دستگاه جبری $(\mathbb{N};+)$ و $(\mathbb{Z};\cdot)$ از یک نوع $\tau=(2)$ هستند و $\mathbb{N}\subseteq\mathbb{Z}$، ولی عمل دوتایی $+$ در $\mathbb{N}$ تحدید عمل ضرب در $\mathbb{Z}$ نیست. پس، $(\mathbb{N};+)$ زیردستگاه جبری $(\mathbb{Z};\cdot)$ محسوب نمی‌شود!

۳- متداول است که برخی زیرجبر را به صورت زیر تعریف می‌کنند: "**مجموعه**‌ی (به جای دستگاه جبری) B را زیرجبر دستگاه جبری $(A;F)$ می‌گوییم اگر $B\subseteq A$ نسبت به هر عمل $\lambda^A\in F$ بسته باشد." منظور این است که، اگر $(A;F)$ دستگاهی جبری و B **زیرمجموعه**‌ی A باشد، به طوری که B تحت هر عمل λ^A بسته باشد، آنگاه روشن است که یک دستگاه جبری $(B;(\lambda^B)_{\lambda\in\Omega})$ از همان نوع τ به دست می‌آید، به طوری که هر عمل λ^B تحدید همتایش λ^A است، یعنی $\lambda^B=\lambda^A|_{B^n}:B^n\to B$. پس، **دستگاه** جبری (نه **مجموعه‌ی**) B **زیردستگاه** جبری A است. از این رو، اگر چه اصولاً نباید گفت که، برای مثال، **مجموعه‌ی** $\mathbb{N}$ **زیردستگاه جبری** $(\mathbb{Z};+,\cdot)$ است، ولی همه‌ی ما گاهی چنین واژه‌هایی را برای سادگی به کار می‌بریم. البته اغلب از فحوای کلام معلوم است که منظور همان است که در بالا گفتیم. برای مثال، در اینجا منظور این است که دستگاه جبری $(\mathbb{N};+,\cdot)$ زیردستگاه جبری $(\mathbb{Z};+,\cdot)$ است!

۴- (اختیاری) دو دستگاه جبری از نوع متفاوت $\tau \neq \tau'$ را اصولاً **نباید** با هم مقایسه کرد! برای مثال، اصولاً نباید دستگاه جبری $(B;*_1)$ از نوع $\tau=(2)$ را زیردستگاه جبری $(A;*_1,*_2)$ نامید! ولی ممکن است تمایل داشته باشید که، برای مثال، $(\mathbb{N};+)$ یا $(\mathbb{Z};\cdot)$ را نیز زیردستگاه جبری $(\mathbb{Z};+,\cdot)$ در نظر بگیرید! به شما حق می‌دهیم، ولی تعریف ۳.۶.۱ چنین اجازه‌ای نمی‌دهد، زیرا $(\mathbb{N};+)$ و $(\mathbb{Z};\cdot)$ از نوع $\tau=(۲)$ هستند، در حالی که $(\mathbb{Z};+,\cdot)$ از **نوع متفاوت** $\tau=(2,2)$ است. در صورت نیاز، این حالت را می‌توانیم با **واژه‌ی دیگری** به جای **زیردستگاه** تعریف کنیم: فرض کنیم که دستگاه‌های جبری $(A;F)$ و $(B;F')$ طوری باشند که $B\subseteq A$، $F'\subseteq F$، و $\lambda^B\in F'$ تحدید همتایش $\lambda^A\in F$ باشد. در این صورت، $(B;F')$ را **تحویل** $(A;F)$ می‌نامیم. برای مثال، $(\mathbb{N};+)$ و $(\mathbb{Z};\cdot)$ تحویل $(\mathbb{Z};+,\cdot)$ و دستگاه $(\mathbb{R};+)$ تحویل $(\mathbb{R};+,\cdot)$ است.

۵.۶.۱ بحث در کلاس. حال به موضوع **مهم** دیگری می‌پردازیم. توجه می‌کنیم که فرزندان جانداران، جاندارند و سنگ و چوب نیستند! همچنین، فرزند انسان، انسان است و پرنده نیست. البته، اگر چه فرزند یک انسان مشخص برخی از ویژگی‌های اساسی آن انسان را به ارث می‌برد، ولی ممکن است همه‌ی ویژگی‌های والدین را **به ارث نبرد**، و **برعکس**، فرزند ممکن است دارای ویژگی‌هایی باشد که والدین او ندارند! به عنوان مثالی در ریاضی، اگر چه گروهواره‌ی $(\mathbb{N};+)$ **زیرگروهواره**‌ی $(\mathbb{Z};+)$ است، ولی $(\mathbb{Z};+)$ ویژگی‌هایی دارد که $(\mathbb{N};+)$ ندارد! برای مثال، $(\mathbb{Z};+)$ گروه است در حالی که $(\mathbb{N};+)$ حتی تکواره نیست.

تعریف ۳.۶.۱ بسیار کلی است و هیچ صحبتی از به ارث بردن یا به ارث نبردن ویژگی‌ها نمی‌کند، و صرفاً **نوع** دستگاه‌ها را مد نظر قرار می‌دهد، در حالی که اغلب دستگاه‌های جبری مورد بحث در دروس ریاضی، P - جبر هستند. فرض کنیم P مجموعه‌ای از ویژگی‌ها (معادله‌ای یا غیر معادله‌ای) باشد.

۶.۶.۱ تعریف. فرض کنیم A یک P - جبر و B زیردستگاه جبری A باشد (یعنی، نسبت به عمل‌های روی A بسته باشد). اگر B نیز دارای همان ویژگی‌های P باشد، می‌گوییم که B یک P - **زیرجبر** A است.

۷.۶.۱ بحث در کلاس. اگرچه تعریف بالا نیازی به تفسیر و توضیح ندارد، و قبل از تعریف نیز مطالبی در باره‌ی آن بیان کردیم، ولی لازم است **نکته‌هایی** را بیاوریم.

۱- اگر واژه‌ی مشخصی چون نیم‌گروه، گروه، حلقه، مشبکه، و از این قبیل، برای یک P - جبر معرفی شده باشد، آنگاه از پیشوند **زیر**، مانند **زیرنیم‌گروه**، **زیرگروه**، **زیرحلقه**، **زیرمشبکه**، و از این قبیل، به‌جای P - **زیرجبر** استفاده می‌کنیم. بنابراین، $(\mathbb{N};+)$ زیرنیم‌گروه $(\mathbb{Z};+)$ است، و البته زیرگروه آن نیست.

۲- مراقب تفاوت بین دو مفهوم زیردستگاه جبری و P - زیرجبر باشید. همان طور که در بالا گفتیم، برای مثال $(\mathbb{N};+)$، با توجه به تعریف ۳.۶.۱، زیردستگاه جبری $(\mathbb{Z};+)$ است (زیرا $\mathbb{N}$ نسبت به جمع در $\mathbb{Z}$ بسته است) ولی زیرگروه یا حتی زیرتکواره‌ی آن نیست. البته، روشن است که اگر ویژگی-های متعلق به P صدق معادله‌ای با **سور عمومی**، یعنی **اتحاد**، (برای مثال، شرکت‌پذیری، تعویض-پذیری، یا خودتوانی درگروهواره‌ها) در A باشد و B زیردستگاه جبری A باشد، آنگاه چون $B \subseteq A$، این اتحادها به روشنی در دستگاه جبری کوچک‌تر B نیز برقرار هستند و در نتیجه B یک P - زیرجبر A نیز می‌شود. **در این موارد، تفاوتی بین زیردستگاه جبری و P - زیرجبر وجود ندارد.** در غیر این صورت، A ممکن است دارای ویژگی δ باشد ولی B آن ویژگی را نداشته باشد! مثالی بیاورید (بند ۱ را ببینید).

این مطالب اهمیت و مزیت ویژگی‌هایی را نشان می‌دهند که بر حسب اتحادها بیان می‌شوند!

۸.۶.۱ بحث در کلاس

۱- گاهی ممکن است ویژگی σ مبین **وجود** عضوی چون $a_\circ$ با ویژگی **خاص** در A باشد و زیردستگاه $B \leq A$ نیز دارای عضوی چون $b_\circ$ با همان ویژگی خاص باشد، ولی $b_\circ \neq a_\circ$. در این صورت، اگر چه B نیز دارای ویژگی σ است و شرط بیان شده در تعریف ۶.۶.۱ برآورده شده است، ولی ریاضی‌دانان اغلب ترجیح می‌دهند که $b_\circ = a_\circ$!

اجازه بدهید موضوع را با یک مثال ساده روشن‌تر کنیم. تکواره‌ی $A = \{e, f\}$ را با عمل دوتایی

$*$	e	f
e	e	f
f	f	f

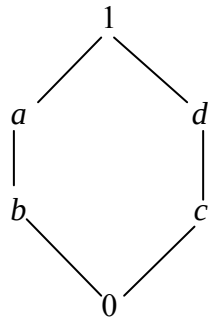
در نظر بگیرید. فرض کنید $B = \{f\}$. اگر تعریف تکواره را به صورت دستگاهی جبری از نوع $\tau = (2)$، تعریف ۱۰.۳.۱، در نظر بگیریم که دارای ویژگی (**وجود** عضو همانی)

$$\sigma := \ (\exists e \in A) \ \ (\forall x \in A) \qquad e * x = x = x * e$$

است، آنگاه $B = \{f\}$ تحت عمل $*$ بسته است (زیرا $f * f = f$) و دارای ویژگی σ است. (البته f نقش عضو همانی را بازی می‌کند). پس، با توجه به تعریف ۶.۶.۱، B **زیرتکواره‌ی** A است! **ولی** ریاضی‌دانان ترجیح می‌دهند که عضو همانی B همان عضو همانی A باشد و در نتیجه، علاوه بر بسته بودن B تحت عمل $*$، **شرط** $e \in B$ را نیز قایل می‌شوند. از این رو، $B = \{f\}$ را

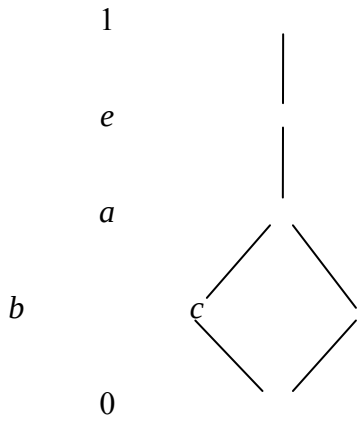
زیرتکواره‌ی A در نظر نمی‌گیرند، و لذا، در این مثال، تنها A و $\{e\}$ را زیرتکواره‌ی A در نظر می‌گیرند! البته، اگر تعریف تکواره را به صورت دستگاهی جبری از نوع $\tau=(2,0)$، تعریف **۱۱.۳.۱**، در نظر بگیریم، آنگاه تعریف زیردستگاه **۶.۶.۱** به خودی خود ایجاب می‌کند که B نه تنها باید تحت عمل دوتایی * بسته باشد بلکه **باید** نسبت به عمل **صفرتایی** آن نیز بسته باشد، که در این صورت عضو همانی A متعلق به B نیز **می‌شود**! از این رو، بسیاری از ریاضی‌دانان تعریف **۱۱.۳.۱** را برای تکواره بر تعریف **۱۰.۳.۱ ترجیح** می‌دهند!

۲- مثالی دیگر مشابه بند ۱ می‌آوریم. اگر تنها مشبکه‌های **کران‌دار** مورد نظر باشند (یعنی، دارای بزرگ‌ترین عضو، به نمایش 1، و کوچک‌ترین عضو، به نمایش 0 باشند)، آنگاه هر زیرمشبکه‌ی کران‌دار چون B از مشبکه‌ی کران‌دار $(A;\vee,\wedge,0,1)$ باید، علاوه بر بسته بودن نسبت به $\vee$ و $\wedge$، شامل 0 و 1 نیز باشد. برای مثال، مشبکه‌ی کران‌دار $A=\{0,a,b,c,d,1\}$ را با نمودار زیر در نظر بگیرید :

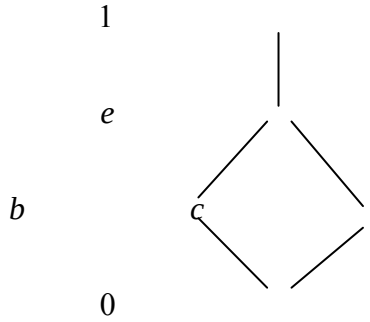


روشن است که $X=\{0,a,b\}$ زیرمشبکه‌ی A محسوب نمی‌شود، زیرا $1\notin X$ (اگر چه نسبت به $\vee$ و $\wedge$ بسته است و خود یک مشبکه‌ی کراندار است، که در آن b بزرگ‌ترین و 0 کوچک‌ترین عضو است). دلیل بیاورید که $C=\{0,b,c,1\}$ و $D=\{0,b,d,1\}$ زیرمشبکه‌ی A هستند.

۳- اجازه بدهید مثال دیگری بیاوریم تا اطمینان حاصل کنیم که متوجه مفهوم زیرمشبکه و نکته‌ی بالا شده‌اید. مشبکه‌ی کران‌دار A را با نمودار زیر در نظر بگیرید:



آیا $B=\{0,b,c,a\}$ زیرمشبکه‌ی کران‌دار A است؟ نشان دهید که مشبکه‌ی کران‌دار $C=\{0,b,c,e\}$ با نمودار



یک زیرمشبکه‌ی A نیست! (توجه کنید که در C، $b\vee c=e$ در حالی که در A داریم $b\vee c=a$)

۴- فرض کنیم دستگاه جبری $(A;*)$ با تعریف ۱۰.۴.۱ شبه‌گروه باشد، یعنی برای هر $a,a'\in A$، معادله‌های $a*x=a'$ و $y*a=a'$ دارای جواب **منحصر به فرد** در A باشند. در این صورت، با توجه به تعریف ۶.۶.۱، $B\subseteq A$ زیرشبه‌گروه A است اگر B نسبت به $*$ بسته باشد و برای هر $b,b'\in B$، معادله‌های $b*x=b'$ و $y*b=b'$ دارای جواب **منحصر به فرد** در B باشند. **سؤال** این است که آیا جواب این معادله‌ها در B با جوابشان در A برابر است؟ **پاسخ شما چیست** (یقیناً مثبت است؛ **چرا؟**).

۹.۶.۱ مشبکه‌ی زیردستگاه‌ها. با مفهوم مجموعه‌ی مرتب (جزئی) و مشبکه در درس مبانی علوم ریاضی و در بخش ۴.۱ این کتاب آشنا شدیم. فرض کنیم $Sub(A)$ مجموعه‌ی همه‌ی زیردستگاه‌های جبری دستگاه جبری A باشد. روشن است که $(Sub(A);\leq)$، که در آن $\leq$ رابطه‌ی ترتیبی شمولی $\subseteq$ است، مجموعه‌ای مرتب است (یعنی، برای هر $H,K,L\in Sub(A)$، داریم $H\subseteq H$؛ اگر $H\subseteq K$ و $K\subseteq H$، آنگاه $H=K$؛ اگر $H\subseteq K$ و $K\subseteq L$، آنگاه

$H \subseteq L$). خواهیم دید که این مجموعه‌ی مرتب یک مشبکه نیز هست (در واقع مشبکه‌ای کامل است). **برخی از پژوهشگران به کمک ویژگی‌های این مشبکه اطلاعات مفیدی در باره‌ی خود دستگاه جبری A به دست می‌آورند.**

برای اثبات مشبکه بودن مجموعه‌ی مرتب $(Sub(A);\leq)$ باید نشان دهیم که برای هر دو زیردستگاه $H,K \leq A$، $H \vee K = Sup\{H,K\}$ و $H \wedge K = Inf\{H,K\}$ وجود دارند. حتماً حدس زده‌اید که $H \wedge K = H \cap K$. حدس شما درست است. البته، ابتدا باید نشان دهیم که $H \cap K \in Sub(A)$. قضیه‌ی زیر بیش از این مطلب را اثبات می‌کند.

۱۰.۶.۱ لم. فرض کنیم A دستگاهی جبری است. در این صورت:

۱- برای هر $H,K \leq A$، $H \cap K$ نیز زیردستگاه جبری A است.

۲- برای هر خانواده‌ی $\{H_i\}_{i\in I}$ از زیردستگاه‌های جبری A، $H = \bigcap_{i\in I} H_i$ نیز زیردستگاه جبری A است.

اثبات. یقین داریم که این حکم‌ها را به راحتی می‌توانید اثبات کنید. برای مثال، فرض کنیم λ عملی n- تایی روی A است. چون H و K نسبت به λ بسته هستند، داریم

$$\begin{aligned} x_1,\cdots,x_n \in H \cap K &\Rightarrow x_1,\cdots,x_n \in H \;\&\; x_1,\cdots,x_n \in K \\ &\Rightarrow \lambda(x_1,\cdots,x_n) \in H \;\&\; \lambda(x_1,\cdots,x_n) \in K \\ &\Rightarrow \lambda(x_1,\cdots,x_n) \in H \cap K \end{aligned}$$

۱۱.۶.۱ بحث در کلاس

۱- همان‌طور که قبلاً نیز دیدیم، اگر A یک P- جبر باشد به طوری که P از **معادله‌هایی** تشکیل شده است که در A اتحاد هستند، آنگاه **تفاوتی** بین زیردستگاه جبری و P- زیرجبر **وجود ندارد**. در این صورت، در لم بالا اشتراک $H = \bigcap_{i\in I} H_i$ یک P- زیرجبر A می‌شود. در غیر این صورت، **ممکن** است این اشتراک یک Pـ زیرجبر A نباشد، **حتی** اگر هر H_i یک P- زیرجبر A باشد!

۲- حال ببینیم که برای زیردستگاه‌های جبری H و K از دستگاه جبری A، $H \vee K = Sup\{H,K\}$ و $\bigvee\{H_i\}_{i\in I} = Sup\{H_i\}_{i\in I}$ را چطور باید تعریف کنیم. روشن است که اگر $H \cup K$ زیردستگاه جبری A باشد، آنگاه سوپریمم H و K نیز خواهد بود، زیرا کوچک‌ترین زیردستگاه جبری شامل H و K است. ولی، به راحتی می‌توانید مثال‌هایی از زیردستگاه جبری $(\mathbb{Z};+)$ بیاورید به طوری که اجتماع آن‌ها نسبت به جمع بسته نباشد. برای تعریف سوپریمم زیردستگاه‌های جبری، ابتدا مفهوم کلی‌تر زیر را می‌آوریم.

۱۲.۶.۱ تعریف فرض کنیم $(A;F)$ دستگاهی جبری از نوع τ است و $X \subseteq A$. در این صورت،

۱- **کوچک‌ترین زیردستگاه** جبری A را که **شامل** X باشد **زیردستگاه تولید شده** از X می‌نامیم و آن را با $< X >$ نشان می‌دهیم.

۲- فرض کنیم A یک P ـ جبر باشد، که در آن P دسته‌ای از ویژگی‌ها (اتحاد یا غیر اتحاد) باشد. در این صورت، **کوچک‌ترین** P - **زیرجبر** A را که شامل X باشد، P - **زیرجبر تولید شده** از A می‌نامیم و آن را با $(X)^P$، (X)، یا اگر امکان اشتباه نباشد با همان $< X >$ نشان می‌دهیم.

۱۳.۶.۱ بحث در کلاس

۱- روشن است که $< \varnothing >$ متشکل از همه‌ی نگاره‌های عمل‌های صفرتایی روی A است (**چرا؟**) و اگر A دارای عمل صفرتایی نباشد، آنگاه $< \varnothing > = \varnothing$. برای مثال اگر $(A;*,e)$ تکواره یا گروه باشد، آنگاه $< \varnothing > = \{e\}$ و اگر $(A;*)$ صرفاً یک گروهواره باشد، آنگاه $< \varnothing > = \varnothing$. (شاید لازم باشد بند **۳** بحث **۲.۲.۱** را دوباره ببینید).

۲- اگر $X = \{x_1, x_2, \cdots, x_n\}$ زیرمجموعه‌ای متناهی از دستگاه جبری A باشد، آنگاه $H = < X > = < x_1, \cdots, x_n >$ را **زیردستگاه متناهی مولد** A می‌نامیم. اگر $A = < x_1, \cdots, x_n >$، آنگاه A را یک **دستگاه جبری متناهی مولد** می‌گوییم.

۳- به عنوان مثالی ساده، چطور، برای مثال، می‌توان زیردستگاه جبری تولید شده توسط $a \in A$ را در مجموعه‌ی نقطه‌ای $(A;a_0)$ یافت (**۴.۲.۱** را ببینید). دستگاه جبری $< a >$ باید کوچک‌ترین زیرمجموعه‌ی نقطه‌ای از $(A;a_0)$ باشد. یعنی، کوچک‌ترین زیرمجموعه‌ی A باشد که شامل a_0 است. پس $< a > = \{a\} \cup \{a_0\}$. به همین صورت، اگر $X \subseteq A$ آنگاه $< X > = X \cup \{a_0\}$.

۴- چطور، برای مثال، می‌توان زیردستگاه جبری تولید شده توسط ۲ را در دستگاه جبری $(\mathbb{Z};+)$ به دست آورد؟ اگر $(\mathbb{Z};+)$ را صرفاً یک گروهواره در نظر بگیریم، آنگاه $< 2 >$، به عنوان زیرگروهواره‌ی $(\mathbb{Z};+)$، تنها لازم است نسبت به عمل جمع بسته باشد و در نتیجه برابر است با $< 2 > = \{2, 2+2, 2+2+2, \cdots\} = \{2, 4, 6, \cdots\} = 2\mathbb{N}$. اگر $(\mathbb{Z};+,0)$ را به عنوان یک تکواره در نظر بگیریم، آنگاه $< 2 >$ به عنوان زیرتکواره‌ی $(\mathbb{Z};+,0)$ باید، علاوه بر بسته بودن نسبت به جمع، عضو همانی را نیز شامل شود، و در نتیجه برابر است با $< 2 > = \{0, 2, 4, 6, \cdots\}$. حال اگر $(\mathbb{Z};+,-,0)$ را گروه در نظر بگیریم، آنگاه $< 2 >$ به عنوان زیرگروه $(\mathbb{Z};+,-,0)$ باید نسبت به قرینه‌ها نیز بسته باشد و در نتیجه برابر است با

$$< 2 > = \{\cdots, -6, -4, -2, 0, 2, 4, 6, \cdots\} = 2\mathbb{Z}$$

۵- زیرگروهواره‌ی $<2>$ در گروهواره‌ی $(\mathbb{Z}_8;+_8)$ چیست؟ در این مثال نیز باید کم‌ترین تعداد عضو $\mathbb{Z}_8$ را به مجموعه‌ی $\{2\}$ بیفزاییم تا مجموعه‌ای بسته نسبت به عمل $+_8$ به دست آید! روشن است که

$$\begin{aligned}<2> &= \{2, 2+_8 2, 2+_8 2+_8 2, 2+_8 2+_8 2+_8 2, \cdots\} \\ &= \{2, 4, 6, 8 \equiv_8 0\}\end{aligned}$$

حتماً این **سؤال جالب** و **مهم** در ذهن شما نیز ایجاد شده است که، آیا اگر بخواهیم $<2>$ را به عنوان **زیرگروه** $(\mathbb{Z}_8;+_8)$ محاسبه کنیم باید، مانند بند ۴ بالا، صفر و قرینه‌ها را نیز به مجموعه‌ی بالا بیفزاییم؟ شما چه فکر می‌کنید؟ یقیناً می توانید با نگاهی دقیق تر به $\{2,4,6,0\}$ پاسخ سؤال را برای این مثال بیابید. ولی برای گروه‌های دیگر $(\mathbb{Z}_n;+_n)$ **چطور؟** برای اینکه لذت فکر کردن و یافتن پاسخ سؤال را از خودتان نگیرید، فعلاً به قضیه‌ی **۸.۲.۲** رجوع نکنید!

۶- حال شما $<3>$ را در گروهواره‌های $(\mathbb{Z}_8;+_8)$ و $(\mathbb{Z}_{15};+_{15})$ بیابید.

۷- زیرگروهواره‌ی $H =<2,3>$ در گروهواره‌ی $(\mathbb{Z}_8;+_8)$ کدام است؟ محاسبه‌ی این زیرگروهواره نیز راحت، ولی قدری پرزحمت‌تر، است! باید شامل عضوهای زیر باشد:

$$\begin{aligned}&0, 2, 4, 6 \\ &3, 3+_8 3 = 6, 3+_8 3+_8 3 = 1, 3+_8 3+_8 3+_8 3 = 4, \cdots \\ &2+_8 3 = 5, \cdots\end{aligned}$$

اگر کمی از عقل سلیم را به کار ببریم، اغلب این محاسبه‌ها را می‌توانیم کوتاه‌تر کنیم. برای مثال، چون $3 \oplus_8 3 \oplus_8 3 = 1 \in H$، پس $H = \mathbb{Z}_8$. **چرا؟**

۱۴.۶.۱ بحث در کلاس. یقیناً دو سؤال کلی زیر برایتان مطرح هستند. **(الف)** آیا کوچک‌ترین زیردستگاه A که شامل مجموعه‌ی X باشد، یعنی $<X>$، همیشه وجود دارد؟ **(ب)** کوچک‌ترین P - زیرجبر (مانند زیرنیم‌گروه، زیرگروه، زیرحلقه، زیرمشبکه، زیرشبه‌گروه، . . .) شامل مجموعه‌ی X، چطور؟ در قضیه‌ی زیر می‌بینیم که پاسخ به سؤال **(الف)** همیشه مثبت است. همچنین، اگر P از **اتحادها** تشکیل شده باشد، آنگاه پاسخ به سؤال **(ب)** نیز مثبت خواهد بود. این نکته‌های مهم را در فصل‌های **۲** و **۳** نیز مطرح خواهیم کرد.

حدس می‌زنیم که سلول‌های خاکستری شما می‌گویند که با توجه به مفهوم سوپریمم، زیردستگاه تولید شده از X همان کوچک‌ترین عضو مجموعه‌ی

$$S = \{B \leq A \mid X \subseteq B\}$$

است! درست است! ولی این کوچک‌ترین عضو چیست؟ با کمی دقت متوجه می‌شویم که اشتراک این مجموعه نامزد خوبی است. قضیه‌ی زیر این مطالب را اثبات می‌کند.

۱۵.۶.۱ قضیه. فرض کنیم که $(A;F)$ دستگاهی جبری از نوع τ است و $X \subseteq A$. در این صورت، اگر $S = \{B \leq A \mid X \subseteq B\}$، آنگاه $< X > = \bigcap_{B \in S} B = \bigcap \{B \leq A \mid X \subseteq B\}$

اثبات. با توجه به تعریف $< X >$، که با دو ویژگی **زیردستگاه** A و **شامل** X **کوچک‌ترین** است، باید نشان دهیم که $K = \bigcap_{B \in S} B$ دارای این ویژگی‌ها است. لم **۱۰.۶.۱** نشان می‌دهد که $K = \bigcap_{B \in S} B$ زیردستگاه A است. چون هر عضو $B \in S$ شامل X است، پس $K = \bigcap_{B \in S} B$ نیز شامل X است. تا اینجا اثبات شد که K زیردستگاهی از A و شامل X است. برای اثبات اینکه K با این دو ویژگی کوچک‌ترین است، فرض می‌کنیم که L نیز زیردستگاهی از A و شامل X باشد. پس $L \in S$. حال، روشن است که $K = \bigcap_{B \in S} B \subseteq L$ و اثبات تمام است!

۱۶.۶.۱ بحث در کلاس

۱- دوباره باید موضوعی را تکرار کنیم. با توجه به قضیه‌ی بالا و بند **۱** بحث **۱۱.۶.۱**، اگر P از معادله‌ها تشکیل شده باشد، آنگاه زیردستگاه تولید شده توسط X همان P- زیرجبر تولید شده توسط X است، یعنی $(X) = < X > = \bigcap \{B \leq A \mid X \subseteq B\}$.

۲- تعمیم بندهای **۴-۷** بحث **۱۳.۶.۱** بالا به صورت زیر است. فرض کنیم $(A;*)$ نیمگروه باشد. در این صورت، با استفاده از تعریف **۱۲.۶.۱** و مشابه اثبات قضیه‌ی بالا، می‌توانید نشان دهید که

(الف) برای هر $x \in A$، زیرنیم‌گروه تولید شده توسط x برابر است با $< x > = \{x^n \mid n \in \mathbb{N}\}$، که در آن ($n$ مرتبه) $x^n = x * x * \cdots * x$ (یعنی، نشان دهید که $B = \{x^n \mid n \in \mathbb{N}\}$ **زیرنیم-گروه** A و **شامل** x است، و اگر C نیز زیرنیم‌گروه A و شامل x باشد، آنگاه $B \subseteq C$).

(ب) در حالت کلی، برای $X \subseteq A$، $< X > = \{x_1 * x_2 * \cdots * x_n \mid n \in \mathbb{N}, x_i \in X\}$. (یعنی، نشان دهید که $B = \{x_1 * x_2 * \cdots * x_n \mid n \in \mathbb{N}, x_i \in X\}$ **زیرنیم‌گروه** A و **شامل** X است، و اگر C نیز زیرنیم‌گروه A و شامل X باشد، آنگاه $B \subseteq C$).

۱۷.۶.۱ نتیجه. فرض کنیم که A دستگاهی جبری و H و K زیردستگاه آن باشند. در این صورت، $H \vee K = Sup\{H, K\} = < H \cup K >$

۱۸.۶.۱ نتیجه. مجموعه‌ی مرتب $(Sub(A);\subseteq)$ یک مشبکه (و در واقع، مشبکه‌ای کامل) است.

$$.\left(\bigvee\{H_i\}_{i\in I} = Sup\{H_i\}_{i\in I} = <\bigcup_{i\in I} H_i>\right)$$

۱۹.۶.۱ تعریف. نمودار مشبکه‌ی $(Sub(A);\subseteq)$ را **نمودار مشبکه‌ی زیردستگاه‌های** A می‌نامیم.

۲۰.۶.۱ بحث در کلاس

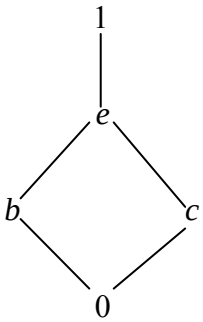
۱- تکواره $M = (\{e, f\};*)$ داده شده در بند ۱ بحث ۸.۶.۱ را به خاطر آورید:

	e	f
e	e	f
f	f	f

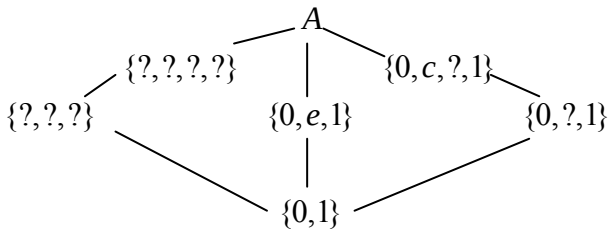
نمودار مشبکه‌ی زیرتکواره‌های آن به صورت زیر است:

مشبکه‌ی زیرگروهواره‌های آن قدری متفاوت است. آن را تعیین کنید.

۲- مشبکه‌ی A را به صورت زیر در نظر بگیرید:



مشبکه‌ی زیرمشبکه‌های کراندار این مشبکه را که در زیر به صورت ناقص داده‌ایم، کامل کنید:



بحث بالا را در فصل‌های ۲ و ۳ ادامه می‌دهیم. در زیر دو روش کلی دیگر ساختن دستگاه‌های جبری جدید از دستگاه‌های داده شده را معرفی می‌کنیم.

۲۱.۶.۱ ضرب و همضرب در اینجا روش‌های اساسی دیگری را برای ساختن دستگاه‌های جبری جدید از دستگاه‌های داده شده مطالعه می‌کنیم. روش کار، به ویژه در مورد ضرب، بسیار ساده است، ولی از این نظر اهمیت دارد که می‌توان دستگاه‌های جبری همنوع ولی با عمل‌های متفاوت را با هم در آمیخت و دستگاهی از همان نوع ولی (اغلب) بزرگ‌تر از آن‌ها به دست آورد!

۲۲.۶.۱ تعریف. فرض کنیم $(A;F)$ و $(B;F')$ دو دستگاه جبری از نوع τ باشند. در این صورت، مجموعه‌ی $A\times B$ همراه با عمل‌های (مؤلفه‌ای)

$$\lambda^{A\times B}((a_1,b_1),\cdots,(a_n,b_n))=(\lambda^A(a_1,\cdots,a_n),\lambda^B(b_1,\cdots,b_n))$$

دستگاهی جبری از نوع τ است که آن را **حاصل‌ضرب** (**دکارتی**) A در B می‌نامیم.

۲۳.۶.۱ بحث در کلاس

۱- برای مثال، اگر $(A;*_A)$ و $(B;*_B)$ گروهواره باشند، آنگاه

$$A\times B=\{(a,b)\,|\,a\in A,b\in B\}$$

همرا با عمل

$$(a,b)*_{A\times B}(a',b')=(a*_A a',b*_B b')$$

گروهواره است. البته، اگر اشتباه برانگیز نباشد، که معمولاً نیست، می‌نویسیم

$$(a,b)(a',b')=(aa',bb')$$

۲- به‌راحتی می‌توانید همتای قضیه‌ی **م.۴.۱** را برای دستگاه جبری $A\times B$ اثبات کنید. باید نشان دهید که توابع تصویری $B \xleftarrow{q} A\times B \xrightarrow{p} A$ **همریختی** هستند، و برای هر دستگاه جبری C از نوع τ و هر جفت **همریختی** $B \xleftarrow{g} C \xrightarrow{f} A$، **همریختی** منحصر به فرد $h: C \to A\times B$ که در واقع همان تابع $h(c)=(f(c),g(c))$ است) وجود دارد به طوری که $p\circ h = f$ و $q\circ h = g$. توجه می‌کنیم که صرفاً واژه‌های **مجموعه** و **تابع** در قضیه‌ی **م.۴.۱**، به ترتیب ، به **دستگاه جبری** و **همریختی** تبدیل شده‌اند.

۳- ممکن است A و B دارای ویژگی σ باشند ولی $A\times B$ آن ویژگی را **به ارث نبرد!** برای مثال، حاصل‌ضرب هر دو عضو ناصفر در گروهواره‌ی ضربی $(\mathbb{Z};\cdot)$ ناصفر است، در حالی که در $\mathbb{Z}\times\mathbb{Z}$، داریم $(1,0)(0,1)=(0,0)$.

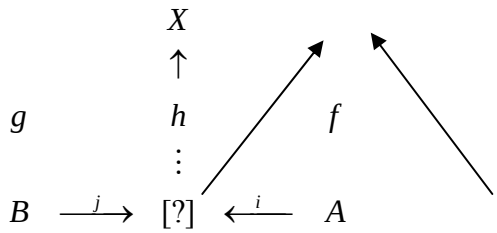
به عنوان مثالی دیگر، هر عضو ناصفر در $\mathbb{R}$ نسبت به عمل ضرب (معمولی) وارون دارد، در حالی که، برای مثال، عضو ناصفر $(۱,۰)$ در $\mathbb{R}\times\mathbb{R}$ وارون (ضربی) ندارد! ولی، اگر **معادله‌ی** σ در A و در B **اتحاد** باشد، آنگاه σ در $A\times B$ نیز **اتحاد** است. حالت کلی این مطلب را در اینجا اثبات نمی‌کنیم، ولی مثالی می‌آوریم. برای مثال، اگر عمل‌های دوتایی $*^A$ و $*^B$ آبلی باشند، آنگاه عمل دوتایی مؤلفه‌ای $*^{A\times B}$ در $A\times B$ نیز آبلی است:

$$\begin{aligned}(a,b)*^{A\times B}(a',b') &= (a*^A a', b*^B b') = (a'*^A a, b'*^B b)\\ &= (a',b')*^{A\times B}(a,b)\end{aligned}$$

همضرب. همان طور که در بحث **م.۵.۱** بیان شد، همضرب دوگان مفهوم ضرب است، به این معنی که دارای ویژگی جهانی دوگان ضرب است. پس، برای تعریف همضرب دستگاه جبری A با دستگاه جبری B، هر دو از نوع τ، کافی است در بحث **م.۵.۱** به جای هر مجموعه یک دستگاه جبری و به جای هر تابع یک همریختی قرار دهیم. یعنی، **همضرب** A با B دستگاهی جبری است که همریختی‌هایی از A و B به آن وجود داشته باشند

$$B \xrightarrow{j} \boxed{?} \xleftarrow{i} A$$

به طوری که برای هر دستگاه جبری X و هر دو همریختی $B \xrightarrow{g} X \xleftarrow{f} A$، یک همریختی منحصر به فرد چون $h: \boxed{?} \to X$ وجود داشته باشد به طوری که مثلث‌های زیر تعویض‌پذیر باشند؟ (**به تغییر جهت پیکان‌ها نسبت به ویژگی جهانی ضرب توجه کنید.**)



اگرچه همضرب دو مجموعه، اجتماع مجزای

$$A \dot{\cup} B = (A \times \{1\}) \cup (B \times \{2\})$$

است (بحث م.۵.۱ را ببینید) ولی برای دستگاه‌های جبری گاهی چنین است و گاهی نیست. یافتن همضرب دو دستگاه جبری اغلب پیچیده است، و لزوماً به سادگی یافتن حاصل‌ضرب نیست. . بخش ۷.۲ را برای مورد گروه‌های آبلی و بحث زیر را برای M - مجموعه‌ها ببینید.

۲۴.۶.۱ بحث در کلاس

همضرب در M - مجموعه‌ها مشابه با مجموعه‌ها تعریف می‌شود. در واقع، اگر M - مجموعه‌های A و B را در نظر بگیریم، آنگاه **همضرب** A با B همان مجموعه‌ی

$$A \dot{\cup} B = (A \times \{1\}) \cup (B \times \{2\})$$

با تعریف عمل M روی آن به صورت

$$s(a,1) = (sa,1), \qquad s(b,2) = (sb,2)$$

است، که در آن sa همان عمل M روی A و sb عمل M روی B است.

تمرین ۶.۱

تمرین‌ها مهم‌ترین قسمت هر درس هستند

۱- نشان دهید که اگر $X \subseteq Y$ زیرمجموعه‌هایی از دستگاهی جبری باشند، آنگاه $< X > \subseteq < Y >$. همچنین، با ارائه مثال نشان دهید که ممکن است $X \neq Y$ ولی $< X > = < Y >$.

۲- نمودار مشبکه‌ی زیردستگاه‌های جبری مجموعه‌ی نقطه‌ای $(\{a,b,c\};a)$ با عمل صفرتایی a را نشان دهید.

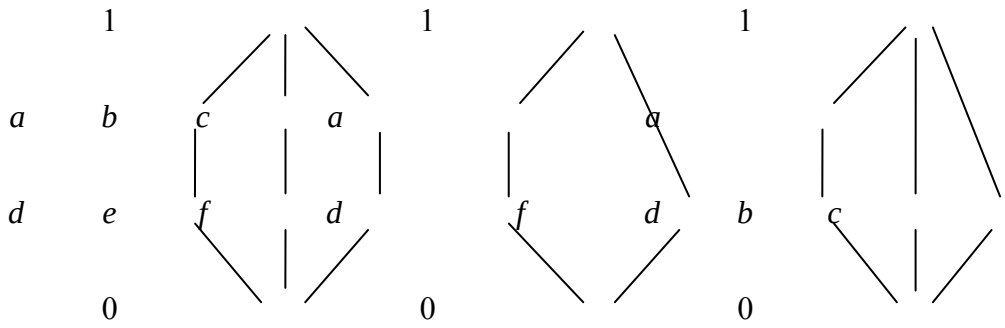
۳- نمودار مشبکه‌ی زیرگروهواره‌های گروهواره‌ی $(\{0,1,2,3\};+_4,0)$ را نشان دهید.

۴- نمودار مشبکه‌ی زیرگروهواره‌های گروهواره‌ی $(\{0,1,2,3\};\cdot_4,0)$ را نشان دهید.

۵- فرض کنید $f,g:A\to B$ همریختی بین دو دستگاه جبری باشند. نشان دهید که $E=\{a\in A \mid f(a)=g(a)\}$ زیرجبر A است.

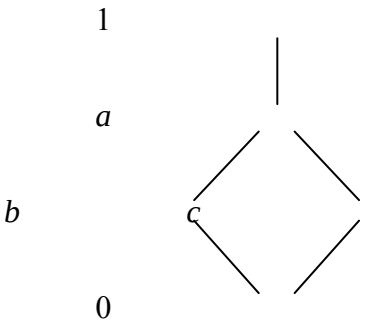
۶- فرض کنید $f:A\to A$ همریختی روی دستگاه جبری A باشد. نشان دهید که $E=\{(a,b)\in A\times A \mid f(a)=f(b)\}$ زیرجبر $A\times A$ است.

۷- مشبکه‌ی کران‌دار (الف) را در نظر بگیرید. آیا مشبکه‌های کراندار (ب) و (پ) زیرمشبکه‌هایی از مشبکه‌ی (الف) هستند؟



(الف) (ب) (پ)

۸- مشبکه‌ی کران‌دار زیر را در نظر بگیرید. دو زیرمشبکه‌ی سه عضوی و یک زیرمشبکه‌ی چهار عضوی کران‌دار (شامل 0 و 1) از این مشبکه ارائه دهید.



۹- فرض کنید A ، B و C ساختارهای جبری از یک نوع هستند. نشان دهید که

(الف) $A\times\{1\}\cong A$

(ب) $A\times B\cong B\times A$

(پ) $(A\times B)\times C\cong A\times(B\times C)$.

۱۰- فرض کنید A، B، Cو Dساختارهای جبری از یک نوع هستند، و C زیرجبر A و D زیرجبر C است. نشان دهید که $C\times D$ زیرجبر $A\times B$ است. با مثال نشان دهید که زیرجبرهای $A\times B$ لزوماً به صورت بالا نیستند.

۱۱- فرض کنید A ، B ساختارهای جبری از یک نوع هستند، و یک عمل دوتایی $*$روی A با تعریف $x*y=x$ ، و یک عمل دوتایی $*'$روی B با تعریف $x*y=y$، وجود دارد. ثابت کنید که در این صورت زیرجبرهای $A\times B$به صورت $C\times D$هستند که Cزیرجبر A و D زیرجبر C است.

۱۲- با استفاده از تمرین بالا نشان دهید که اگر A و B گروههایی متناهی به ترتیب با m و n عضو باشند و $(m,n)=1$، آنگاه زیرگروههای $A\times B$به صورت $C\times D$هستند که Cزیرگروه A و D زیرگروه C است.

۷.۱ همنهشتی و خارج قسمت

در بخش ۶.۱ سه روش مهم ساختن دستگاه‌های جبری جدید از دستگاه‌های جبری داده شده ارائه دادیم. در این بخش، روش **بسیار مهم** دیگری را معرفی می‌کنیم. می‌توانیم بدون هیچ توضیح و مقدمه‌ای، وارد بحث شویم و تعریف ۱.۷.۱ را بیاوریم و کارمان را ادامه دهیم! ولی، چون قصد ما تنها ارائه‌ی مطالب نیست، بلکه می‌خواهیم، در صورت امکان، **فوت و فن** رسیدن به تعریف‌ها و قضیه‌ها را نیز قدری شرح دهیم، مطالب زیر را می‌آوریم.

واژه‌ی **خارج قسمت** دستگاه جبری A به این معنی است که A را به دسته‌های جدا از هم تقسیم، یعنی **افراز**، کنیم. ولی، همان طور که در مورد مفاهیم زیردستگاه و حاصل‌ضرب دیدیم، انتظار داریم که خارج قسمت هر دستگاه جبری از **نوع** τ دستگاهی جبری ازهمان **نوع** τ باشد! از این رو، باید **عمل‌هایی** در افراز $\mathcal{P}$ تعریف کنیم که از آن یک دستگاه جبری از نوع τ بسازد. همچنین، مانند موردهای زیردستگاه جبری و حاصل‌ضرب، این عمل‌ها نیز باید به‌گونه‌ای حاصل از عمل‌های دستگاه داده شده‌ی A باشند. برای اینکه مشاهده کنیم که رسیدن به این هدف **کار چندان مشکلی نیست**، ابتدا حالت ساده‌ی گروهواره را در نظر می‌گیریم که تنها دارای یک عمل دوتایی است.

فرض کنیم $(A;*)$ گروهواره و $\mathcal{P}$ افرازی از A باشد و می‌خواهیم عملی دوتایی چون $\overline{*}$ در $\mathcal{P}$ تعریف کنیم. فرض کنیم $X,Y\in\mathcal{P}$. **حدس** می‌زنید که

$$X\overline{*}Y=\{?\}$$

را **چطور** تعریف کنیم؟ عقل سلیم می‌گوید که طبیعی است که اعضای X را یکی یکی در اعضای Y، $*$ کنیم. یعنی،

$$X\overline{*}Y=\{x*y\,|\,x\in X,y\in Y\}$$

ولی آیا **تضمینی** وجود دارد که $X\overline{*}Y$ متعلق به $\mathcal{P}$ باشد؟ یعنی آیا $\mathcal{P}$ نسبت به عمل $\overline{*}$ **بسته است**؟ به مثال زیر توجه کنید. گروهواره‌ی $(\mathbb{Z}_4;\oplus_4)$ و افراز زیر را در نظر بگیرید.

$$\mathcal{P}=\{\{0,1\},\{2\},\{3\}\}$$

مشاهده می‌کنیم که

$$\{2\}\,\overline{\oplus}_4\,\{0,1\}=\{2\oplus_4 0,2\oplus_4 1\}=\{2,3\}\notin\mathcal{P}$$

در این لحظه ممکن است عقل سلیم و سلول‌های خاکستری نتوانند بیشتر از این یاریمان دهند! اجازه بدهید موضوع را از زاویه‌ی دیگری بررسی کنیم. قضیه‌ی بسیار مهم و زیبایی در درس **مبانی علوم ریاضی** دیدیم (تمرین **۴** از بخش **م.۱** را ببینید) که می‌تواند دریچه‌ی دیگری به روی سلول‌های خاکستری بگشاید. این قضیه در واقع بیان می‌کند که هر افراز $\mathcal{P}$ از مجموعه‌ی A حاصل از رابطه‌ای هم‌ارزی روی A است، و برعکس. از این رو، فرض می‌کنیم که $\sim$ رابطه‌ای هم‌ارزی روی A و $\mathcal{P}=A/\sim$ افراز حاصل از آن باشد. حال، عقل سلیم در باره‌ی حاصل $[x]\overline{*}[y]$ **چه پیشنهاد می‌کند؟** یقین داریم که می‌گویید $[x]\overline{*}[y]=[x*y]$. ولی با وجودی که به روشنی $\mathcal{P}$ نسبت به این عمل بسته است، **آیا** این دستور عمل زیبا **خوش‌تعریف** است؟ یعنی، آیا

$$\begin{cases}[x]=[x']\\ [y]=[y']\end{cases}\Rightarrow[x]\overline{*}[y]=[x']\overline{*}[y']\quad(\Leftrightarrow[x*y]=[x'*y'])$$

به عبارت دیگر، آیا

$$\begin{cases} x \sim x' \\ y \sim y' \end{cases} \overset{?}{\Rightarrow} x * y \sim x' * y' \qquad (*)$$

دوباره مثال بالا را در نظر می‌گیریم. فرض کنیم $\sim$ رابطه‌ی هم‌ارزی متناظر با افراز $\mathcal{P}$ باشد. مشاهده می‌کنیم که

$$\begin{cases} 2 \sim 2 \\ 0 \sim 1 \end{cases} \not\Rightarrow 2 \oplus_4 0 \sim 2 \oplus 1$$

این مطالب و مثال‌ها نشان می‌دهند که **نباید** A را به دلخواه افراز کنیم، یا اینکه **لزومی ندارد** که هر رابطه‌ی هم‌ارزی دلخواه روی A ما را به نتیجه‌ی مطلوب برساند! بحث بالا ایجاب می‌کند که باید شرط $(*)$ بالا را برای رابطه‌ی هم‌ارزی قایل شویم، زیرا عمل $\overline{*}$ در افراز $\mathcal{P}$ **خوش‌تعریف** است اگر و تنها اگر **شرط** $(*)$ **برای رابطه‌ی هم‌ارزی متناظر با** $\mathcal{P}$ **برقرار باشد** (تمرین **۱.۷.۱** را ببینید)! **موفق شدیم!** در تعریف زیر، حالت کلی را برای عمل‌های n- تایی در نظر می‌گیریم.

۱.۷.۱ تعریف. فرض کنیم A دستگاهی جبری از نوع τ و $\sim$ رابطه‌ای هم ارزی روی A باشد. می‌گوییم که $\sim$ **رابطه‌ای همنهشتی** روی A است اگر برای هر عمل n- تایی λ^A و $a_i, b_i \in A$، $1 \le i \le n$، **شرط سازگاری** زیر برقرار باشد:

$$(\forall i, a_i \sim b_i) \Rightarrow \lambda^A(a_1, \cdots, a_n) \sim \lambda^A(b_1, \cdots, b_n)$$

۲.۷.۱ بحث در کلاس

۱- به آسانی می‌توانید نشان دهید که رابطه‌ی $\sim$ همنهشتی است اگر و تنها اگر $\sim = \{(x,y) \mid x \sim y\}$ (به عنوان زیرمجموعه‌ی $A \times A$) یک زیردستگاه جبری دستگاه جبری $A \times A$ باشد، یعنی $\sim$ نسبت به هر عمل $\lambda^{A \times A}$ بسته باشد. برای مثال، اگر رابطه‌ی $\sim$ روی گروهواره‌ی $(A;*)$ همنهشتی باشد، آنگاه $\sim$ نسبت به عمل $*^{A \times A}$ در $A \times A$ بسته است. زیرا

$$\begin{aligned} (x,x'),(y,y') \in \sim \;&\Rightarrow\; \begin{cases} x \sim x' \\ y \sim y' \end{cases} \Rightarrow\; x * y \sim x' * y' \\ &\Rightarrow\; (x * y \sim x' * y') \in \sim \end{aligned}$$

عکس این مطلب را نیز می‌توانید نشان دهید.

۲- به آسانی می‌توانیم اثبات کنیم که، برای هر عدد طبیعی n، رابطه‌ی آشنای **همنهشتی به پیمانه‌ی** n (بند ۲ بحث م.۱.۱۱ را ببینید) در شرط سازگاری بالا (نسبت به عمل جمع) صدق می‌کند. یعنی،

$$\begin{cases} a \equiv_n b \\ c \equiv_n d \end{cases} \Rightarrow \quad a+c \equiv_n b+d$$

با توجه به این مثال کلاسیک تاریخی، هر رابطه‌ی هم‌ارزی‌ای را که در شرط سازگاری صدق کند، **همنهشتی** نامیدیم.

۳- توجه می‌کنیم که رابطه‌های **هم‌ارزی** بسیاری روی مجموعه‌ی $\mathbb{Z}$ می‌توانیم تعریف کنیم. یعنی، $\mathbb{Z}$ را به گونه‌های بسیاری می‌توانیم افراز کنیم. ولی آیا همه‌ی آن‌ها در شرط سازگاری تعریف بالا، برای مثال، نسبت به عمل جمع صدق می‌کنند؟ برای مثال، در افراز $\mathbb{Z} = \{0,1,2,\cdots\} \cup \{-1,-2,\cdots\}$ داریم

$$\begin{cases} 2 \sim 2 \\ -1 \sim -4 \end{cases} \not\Rightarrow 2+(-1) \sim 2+(-4)$$

سؤال: آیا هیچ همنهشتی دیگری (با تعریف ۱.۷.۱) بجز همنهشتی‌های به پیمانه‌ی n روی گروه $(\mathbb{Z};+)$ وجود دارد؟ شاید تعجب کنیم که پاسخ به این سؤال منفی است! فرض کنیم $\sim$ یک رابطه‌ی همنهشتی نابدیهی روی گروه $(\mathbb{Z};+)$ باشد. بنابر اصل خوش‌ترتیبی، کوچک‌ترین عدد طبیعی n در رده‌ی $[0]_{\sim}$ وجود دارد. در تمرین ۲.۷.۱ نشان دهید که

$$x \sim y \Leftrightarrow x \equiv_n y$$

۴- حال، با الگو قرار دادن تعریف عمل دوتایی

$$\overline{*}([a_1],[a_2]) = [a_1] \overline{*} [a_2] = [a_1 * a_2] = [*(a_1,a_2)]$$

تعریف **جامع** زیر را داریم: متناظر با هر عمل n- تایی λ^A و برای هر $[a_1],\cdots,[a_n] \in A/\sim$، تعریف می‌کنیم

$$\lambda^{A/\sim}([a_1],\cdots,[a_n]) = [\lambda^A(a_1,\cdots,a_n)]$$

۳.۷.۱ تعریف. فرض کنیم $(A;(\lambda^A)_{\lambda\in\Omega})$ دستگاهی جبری از نوع τ و $\sim$ رابطه‌ای همنهشتی روی A باشد. در این صورت، دستگاه جبری $(A/\sim;(\lambda^{A/\sim})_{\lambda\in\Omega})$ را **خارج قسمت** دستگاه جبری A بر رابطه‌ی همنهشتی $\sim$ می‌نامیم.

۴.۷.۱ بحث در کلاس. (اختیاری) در زیر دو نکته جالب را در باره‌ی رابطه‌های همنهشتی برای علاقه‌مندان بیان می‌کنیم.

۱- مشابه با بند ۳ بحث ۲.۷.۱، در برخی از دستگاه‌های جبری کلاسیک مانند گروه‌ها، رابطه‌های همنهشتی در تناظر دوسویی با زیردستگاه‌هایی بسیار خاص قرار دارند، و رده‌های خارج قسمت، به‌گونه‌ای جالب تنها توسط یک رده‌ی خاص تعیین می‌شوند. برای مثال، در گروه‌ها، رده‌های خارج قسمت توسط رده‌ی همانی، یعنی $N=[e]$، مشخص می‌شوند. به این معنی که اگر به صورت نمادی بنویسیم

$$aN=\{a*y\mid y\in N\}$$

آنگاه $aN=[a]$! بنابراین، اگر فقط رده‌ی $N=[e]$ معلوم باشد، هر رده‌ی $[a]$ نیز مشخص می‌شود! **جالب است، نیست؟** این مطالب را در فصل‌های ۲ و ۳ برای گروه‌ها و حلقه‌ها به تفصیل مطالعه خواهیم کرد. البته، لازم است **هشدار** بدهیم که این اتفاق‌های بسیار جالب، **بسیار نادر هستند**، و از آنجا که در دستگاه‌های جبری کلاسیک مانند گروه، حلقه، مدول، و فضای برداری رخ می‌دهند، این **تصور نادرست** را در دانشجویان کارشناسی و حتی بالاتر ایجاد می‌کند که برای تمام دستگاه‌های جبری درست هستند، در حالی که حتی برای تکواره‌ها لزوماً **درست نیستند**! برای مثال، به‌آسانی می‌توانید نشان دهید که هم‌ارزی متناظر با افراز $\{\{1\},\{0,2,3\}\}$ روی **تکواره‌ی** ضربی $(\mathbb{Z}_4;\cdot_4)$ همنهشتی است، ولی $\{0,2,3\}$ برابر با هیچ یک از مجموعه‌های $\{1\}*\{0\}$، $\{1\}*\{2\}$، یا $\{1\}*\{3\}$ **نیست**. یعنی، رده‌ی $[1]=\{1\}$ تعیین کننده‌ی $\{0,1,2\}$ نیست.

۲- در اینجا **نکته‌ی بسیار مهم** دیگری را بسیار مختصر مطرح می‌کنیم که در درس‌های دیگر جبر مورد مطالعه‌ی جامع‌تر قرار می‌گیرد، و پژوهش‌های بسیاری را به خود اختصاص داده است.

گاهی به این دلیل یک دستگاه جبری A را با رابطه‌ی همنهشتی $\sim$ به دسته‌هایی افراز می‌کنیم زیرا به دلایلی می‌خواهیم تفاوتی بین عضوهای متعلق به یک دسته قایل نشویم و در واقع هر رده‌ی $[a]$ را یک **واحد** در نظر بگیریم.

گاهی لازم است جبر خارج قسمتی $A/\sim$ دارای ویژگی‌ای چون σ باشد که احتمالاً A فاقد آن است. برای مثال، در $(\mathbb{Z};\cdot)$ هیچ عضو متفاوت با ۱ و ۱- وارون (ضربی) ندارد، در حالی که برای عدد اول p، در $(\mathbb{Z}/\equiv_p;\cdot_p)$ هر عضو بجز صفر وارون دارد.

معمولاً این کار اخیر را به گونه‌ای انجام می‌دهیم که کم‌ترین تعداد عضوها را با هم یکسان در نظر بگیریم، و در نتیجه بیش‌ترین تعداد دسته‌ها را داشته باشیم. پس باید $\sim$ را کوچک‌ترین رابطه‌ی همنهشتی در نظر بگیریم که ما را به مقصود برساند.

برای مثال اگر بخواهیم گروه $(\mathbb{Z}_4;+_4)$ را با یک رابطه‌ی همنهشتی چون $\sim$ افراز کنیم به طوری که در گروه خارج قسمتی $\mathbb{Z}_4/\sim$ هر عضو قرینه‌ی خودش باشد، یعنی $[x]=[-x]$ اتحاد باشد، یا برای هر $x\in\mathbb{Z}_4$، $x\sim -x$، آنگاه $\sim$ باید شامل مجموعه‌ی

$$\{(0,0),(1,-1),(2,-2),(3,-3)\}=\{(0,0),(1,3),(2,2),(3,1)\}$$

باشد. حال می‌توانید با افزودن کم‌ترین تعداد جفت مرتب به این مجموعه، رابطه‌ی همنهشتی زیر را روی $\mathbb{Z}_4$ به دست آورید:

$$\sim=\{(0,0),(1,1),(2,2),(3,3),(1,3),(3,1),(2,0),(0,2)\}$$

توجه می‌کنیم که، چون $3\sim 3$ و $1\sim 3$ و $\sim$ همنهشتی است، پس $3\oplus_4 3\sim 3\oplus_4 1$ یا $0\sim 2$. بنابراین،

$$[0]=\{x\in\mathbb{Z}_4\mid x\sim 0\}=\{0,2\}=[2]$$
$$[1]=\{x\in\mathbb{Z}_4\mid x\sim 1\}=\{1,3\}=[3]$$

و در نتیجه $\mathbb{Z}_4/\sim=\{[0],[1]\}$ دارای ویژگی مورد نظر است.

به عنوان مثالی دیگر، فرض کنیم $(A;*)$ گروهواره است. اگر بخواهیم گروهواره‌ی خارج قسمتی $(A/\sim;\overline{*})$ آبلی باشد، یعنی برای هر $x,y\in A$، عبارت‌های معادل زیر برقرار باشند:

$$[x]\overline{*}[y]=[y]\overline{*}[x]\Leftrightarrow[x*y]=[y*x]\Leftrightarrow x*y\sim y*x\Leftrightarrow(x*y,y*x)\in\sim$$

کافی است که $\sim$ را کوچک‌ترین رابطه‌ی همنهشتی در نظر بگیریم به طوری که برای هر $x,y\in A$، $x*y\sim y*x$ یا $(x*y,y*x)\in\sim$.

محاسبه‌ی کامل چنین رابطه‌های همنهشتی در حالت کلی کار ساده‌ای نیست و کتاب‌ها و مقاله‌های بسیاری در این باره نوشته شده است. مثال اخیر را در فصل ۲ در باره‌ی گروه‌ها حل می‌کنیم. توجه می‌کنیم که اگر A گروه باشد، $x*y\sim y*x$ به $(x*y)*(y*x)^{-1}\sim e$ یا $x*y*x^{-1}*y^{-1}\sim e$ تبدیل می‌شود (چطور؟) که کار کردن با آن ساده‌تر است.

۵.۷.۱ قضیه‌ی اساسی همریختی‌ها. در قسمتی از کتاب مبانی علوم ریاضی، که آن را در فصل مقدمه یادآوری کردیم، دیدیم که متناظر با هر تابع $f:A\to B$ رابطه‌ای هم‌ارزی به نمایش

$K_f = \sim_f$ و به نام **هسته‌ی** f روی A وجود دارد که بسیار با اهمیت است. دیدیم که ویژگی‌هایی که این رابطه‌ی هم‌ارزی را با اهمیت می‌کند یکی این است که مقیاسی برای **سنجش** درجه‌ی **یک به یک بودن یا نبودن** تابع f به دست می‌دهد (لم **م.۹.۱** را ببینید)، و شاید از آن **مهم‌تر** این است که هر رابطه‌ی هم‌ارزی روی A از این نوع است، یعنی **هسته‌ی تابعی** است. همچنین، **قضیه‌ی اساسی م.۱۰.۱** بیان می‌کند که **نگاره‌ی** هر تابع f اساساً **خارج قسمتی** از A است، یعنی $f(A) \cong A/\sim_f$.

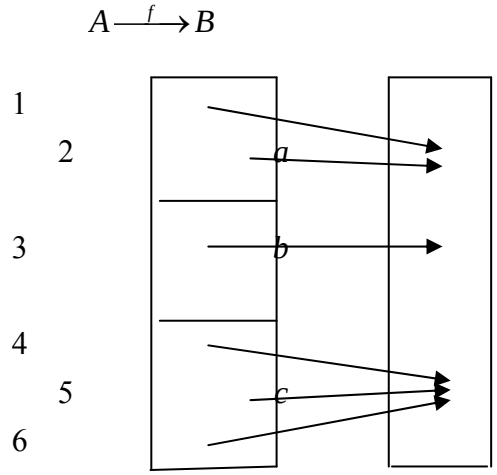
در اینجا خواهیم دید که همتای همه‌ی این مطالب برای هر **همریختی** $f : A \to B$ بین دستگاه‌های کلی جبری (ازجمله، گروه، حلقه، مشبکه، . . .) نیز **برقرار است**! از این رو، بسیاری از مطالب مهمی را که در زیر می‌آوریم، تقریباً **تکرار** مطالبی است که در مقدمه آوردیم (که دو بار دیگر در فصل‌های **۲** و **۳** نیز تکرار می‌شوند). کافی است واژه‌های **دستگاه جبری** را به جای **مجموعه** و **همریختی** را به جای **تابع** به کار ببریم. ابتدا، همتای تعریف **م.۸.۱** را می‌آوریم.

۶.۷.۱ تعریف. فرض کنیم $f : A \to B$ یک همریختی بین دستگاه‌های جبری باشد. در این صورت، رابطه‌ی

$$\{(a, a') \in A \times A \mid f(a) = f(a')\}$$

را **هسته‌ی** f می‌نامیم. این رابطه را با $Kerf$، K_f، یا $\sim_f$ نشان می‌دهیم. بنابراین،

$$a \sim_f b \Leftrightarrow a K_f a' \Leftrightarrow f(a) = f(a')$$



۷.۷.۱ لم. *فرض کنیم* $f : A \to B$ *همریختی بین دستگاه‌های جبری باشد. در این صورت،*

۱- *هسته‌ی* f *رابطه‌ای همنهشتی روی دستگاه جبری* A *است،*

۲- *بر عکس، هر رابطه‌ی همنهشتی* $\sim$ *روی* A *هسته‌ی یک همریختی است.*

۳- *همریختی* f *یک به یک است اگر و تنها اگر*

$$K_f = \Delta_A = \{(a,a) \mid a \in A\}$$

اثبات

۱- در اثبات لم **۹.۱.م** دیدیم که $\sim_f$ رابطه‌ای هم‌ارزی روی A است. برای اثبات **سازگاری** $\sim_f$ با هر عمل n- تایی λ^A، فرض می‌کنیم که $a_1,\cdots,a_n,a'_1,\cdots,a'_n \in A$ به طوری که برای هر i، $a_i \sim_f a'_i$، یعنی $f(a_i) = f(a'_i)$. در این صورت، چون f همریختی است، داریم

$$\begin{aligned} f(\lambda^A(a_1,\cdots,a_n)) &= \lambda^B(f(a_1),\cdots,f(a_n)) \\ &= \lambda^B(f(a'_1),\cdots,f(a'_n)) \\ &= f(\lambda^A(a'_1,\cdots,a'_n)) \end{aligned}$$

در نتیجه $\lambda^A(a_1,\cdots,a_n) \sim_f \lambda^A(a'_1,\cdots,a'_n)$. بنابراین، $\sim_f$ رابطه‌ای همنهشتی روی A است.

۲- ابتدا به راحتی می‌توانید نشان دهید که تابع طبیعی و پوشای

$$\gamma : A \to A/\sim, \qquad \gamma(a) = [a]_\sim$$

همریختی است. در واقع، برای هر عمل n- تایی λ^A روی A و $a_1,\cdots,a_n \in A$، داریم

$$\begin{aligned} \gamma(\lambda^A(a_1,\cdots,a_n)) &= [\lambda^A(a_1,\cdots,a_n)]_\sim = \lambda^{A/\sim}([a_1]_\sim,\cdots,[a_n]_\sim) \\ &= \lambda^{A/\sim}(\gamma(a_1),\cdots,\gamma(a_n)) \end{aligned}$$

حال، فرض کنیم $\sim$ رابطه‌ای همنهشتی روی A باشد. نشان می‌دهیم که $\sim$ هسته‌ی همریختی γ است. داریم

$$a \sim_\gamma a' \;\Leftrightarrow\; \gamma(a)=\gamma(a') \;\Leftrightarrow\; [a]_\sim = [a']_\sim$$
$$\Leftrightarrow\; a \sim a'$$

۳- این حکم در لم **م.۹.۱** اثبات شد. ■

قضیه‌ی زیر همتای قضیه‌ی اساسی **م.۱۰.۱** است.

۸.۷.۱ قضیه‌ی اساسی همریختی‌ها. *فرض کنیم* $f : A \to B$ *همریختی بین دستگاه‌های جبری است. در این صورت،*

$$A/\sim_f = A/K_f \cong f(A)$$

به ویژه، اگر f *پوشا باشد آنگاه* $A/\sim_f \cong B$.

اثبات. در اثبات قضیه‌ی **م.۱۰.۱** دیدیم که تابع

$$\overline{f} : A/K_f \to f(A)$$
$$[a] \mapsto f(a)$$

خوش‌تعریف، **یک به یک**، و **پوشا** است. پس، کافی است ثابت کنیم که $\overline{f}$ همریختی نیز هست، که آن نیز به‌راحتی اثبات می‌شود. فرض کنیم $[a_1],\cdots,[a_n] \in A/\sim$ و λ^{A/K_f} عمل n-تایی متناظر با λ^A در A/K_f باشد. در این صورت، بنابر تعریف این عمل و همریختی بودن f، داریم (دلیل هر مرحله را بیان کنید)

$$\begin{aligned}\overline{f}(\lambda^{A/K_f}([a_1],\cdots,[a_n])) &= \overline{f}[\lambda^A(a_1,\cdots,a_n)]\\ &= f(\lambda^A(a_1,\cdots,a_n))\\ &= \lambda^B(f(a_1),\cdots,f(a_n))\\ &= \lambda^B(\overline{f}[a_1],\cdots.\overline{f}[a_n])\end{aligned}$$

بنابراین، $\overline{f}$ همریختی (و دوسویی) است و در نتیجه $A/K_f \cong f(A)$. حکم آخر قضیه روشن است. ■

قضیه‌ی بالا را قضیه‌ی اول یکریختی نیز می‌نامند. **قضیه‌های دوم و سوم یکریختی** نیز برای دستگاه‌های کلی جبری وجود دارند که ترجیح می‌دهیم آن‌ها را صرفاً برای گروه‌ها و حلقه‌ها در فصل-های ۲ و ۳ بیان و اثبات کنیم.

۱۱.۷.۱ بحث در کلاس

۱-در تمرین ۵.۱ (۱) دیدیم که گروه $(\mathbb{Z}_n;\oplus_n)$ با گروه $(\mathbb{Z}/\equiv_n;\overline{\oplus}_n)$ یکریخت است. در اینجا، برای به نمایش گذاشتن نحوه‌ی استفاده از **قضیه‌ی اساسی همریختی‌ها**، یک بار دیگر آن را اثبات می‌کنیم. به‌راحتی می‌توانید نشان دهید که تابع

$$f:\mathbb{Z}\to\mathbb{Z}_n$$
$$f(a)=(\text{باقی‌مانده‌ی تقسیم } a \text{ بر } n)$$

یک همریختی پوشا است. یعنی:

$$f(a+b)=(\text{باقی‌مانده‌ی تقسیم } a \text{ بر } n)\oplus_n(\text{باقی‌مانده‌ی تقسیم } b \text{ بر } n)$$

حال، هسته‌ی f را محاسبه می‌کنیم. داریم

$$\begin{aligned} aK_f b &\Leftrightarrow f(a)=f(b)\\ &\Leftrightarrow (\text{باقی‌مانده‌ی تقسیم } a \text{ بر } n)=(\text{باقی‌مانده‌ی تقسیم } b \text{ بر } n)\\ &\Leftrightarrow a\equiv_n b \end{aligned}$$

در نتیجه، K_f همان $\equiv_n$ است. حال، بنا بر **قضیه‌ی اساسی همریختی‌ها**، داریم

$$\mathbb{Z}/\equiv_n=\mathbb{Z}/K_f\cong\mathbb{Z}_n$$

۱۲.۷.۱ بحث در کلاس. قبلاً نیز بیان شد که برخی از مفاهیم برای دستگاه‌های جبری کلاسیک گروه، حلقه، مدول، و فضای برداری می‌توانند به زبانی دیگر نیز مطرح شوند و نباید این **تصور نادرست** ایجاد شود که آن زبان را می‌توان برای همه‌ی دستگاه‌های جبری به‌کار برد! **هسته‌ی همریختی** نیز یکی از این موارد است. در مطالعه‌ی گروه‌ها در فصل ۲ خواهیم دید که هسته‌ی همریختی $f:A\to B$ بین گروه‌ها به صورت

$$f^{-1}(e_B) = \overleftarrow{f}(e_B) = \{a \in A \mid f(a) = e_B\}$$

تعریف می شود ولی در همان فصل ۲ خواهیم دید که این دو تعریف معادل یکدیگر هستند، به این معنی که از هر یک به دیگری دست می‌یابیم.

تمرین ۷.۱

تلاش برای حل کردن تمرین‌ها لذت بخش است

۱- فرض کنید A دستگاهی جبری و $\sim$ رابطه‌ای هم‌ارزی روی A است. نشان دهید که عمل $\lambda^{A/\sim}$ روی $A/\sim$ خوش‌تعریف است اگر و تنها اگر $\sim$ همنهشتی باشد.

۲- فرض کنید $\sim$ یک رابطه‌ی همنهشتی نابدیهی (با تعریف ۱.۷.۱) روی گروه $(\mathbb{Z};+)$ و n کوچک‌ترین عدد طبیعی در رده‌ی $[0]_\sim$ باشد. نشان دهید که

$$x \sim y \Leftrightarrow x \equiv_n y$$

۳- فرض کنید A ساختارجبری یکانی باشد، یعنی همه‌ی اعمال آن یکانی باشند. فرض کنید B زیرجبر A است. رابطه‌ی θ را به صورت زیر در نظر بگیرید:

$$a\theta b \Leftrightarrow a = b \text{ یا } \{a,b\} \subseteq B$$

نشان دهید که θ یک رابطه‌ی همنهشتی روی A است. رده‌های θ را مشخص کنید.

۴- فرض کنید $f : A \to B$ همریختی و θ یک رابطه‌ی همنهشتی روی A باشد. نشان دهید که $(f \times f)^{-1}(\theta)$ یک رابطه‌ی همنهشتی روی B است.

۵- دستگاه جبری A را **ساده** می نامیم اگر تنها دارای دو همنهشتی (Δ و ∇) باشد. نشان دهید که اگر θ یک رابطه‌ی همنهشتی روی دستگاه جبری دلخواه A باشد، آنگاه A/θ ساده است اگر وتنها اگر θ یک رابطه‌ی همنهشتی ماکسیمال روی A باشد. (یعنی، $\theta \neq \Delta$ و برای هر رابطه‌ی همنهشتی $\sim$ روی A، داریم $\sim = \Delta$ یا $\sim = \nabla$.

۶- فرض کنید $\{\theta_i \mid i \in I\}$ خانواده‌ای از همنهشتی‌های روی A باشد، و $\gamma_i : A \to A/\theta_i$ همریختی‌های طبیعی باشند. نشان دهید که

(الف) $\prod \gamma_i : A \to \prod A/\theta_i$ با تعریف $\prod \gamma_i(a) = (\gamma_i(a))_{i\in I}$ همریختی است.

(ب) ثابت کنید که $Ker(\prod \gamma_i) = \bigcap \theta_i$.

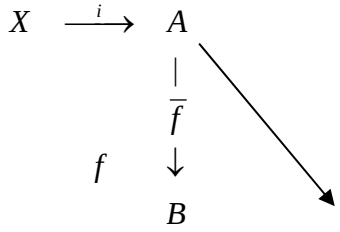
۷- همتای تمرین م. ۸.۱ (تعمیم قضیه‌ی اساسی همریختی‌ها) را بیان و اثبات کنید.

۸.۱ دستگاه جبری آزاد و کدگذاری

برخی از دستگاه‌های جبری، به تعبیر و دلیلی که خواهیم دید، **آزاد** نامیده می‌شوند. این دستگاه‌های جبری اهمیت ویژه‌ای در مبحث جبر دارند. دست‌کم به این دلیل که **هر دستگاه جبری خارج قسمت یک دستگاه جبری آزاد است**. در این بخش ابتدا این مفهوم را در حالت کلی تعریف می‌کنیم و سپس، به عنوان نمونه، نیم‌گروه، تکواره، و گروه **آزاد** را، که کاربردهای بسیاری از جمله در علوم کامپیوتر، ترکیبیات، و کدگذاری دارند، تا اندازه‌ای که به این درس مقدماتی مربوط می‌شود، مطالعه خواهیم کرد. در پایان این بخش مختصری در باره‌ی **کدگذاری** نیز صحبت خواهیم کرد.

اگر چه هدف اصلی این بخش تعریف نیم‌گروه و تکواره‌ی آزاد است (که در علوم کامپیوتر، علم نانو، و بسیاری از علوم دیگر کاربرد دارند)، ابتدا تعریف (نسبتاً) کلی زیر را می آوریم که مزیت‌های مفیدی دارد. این تعریف ممکن است **واژه‌ی آزاد** را توجیه نکند، ولی بعداً واژه‌ی آزاد را نیز توجیه خواهیم کرد. در این بخش، به دلیل کمبود وقت، به جای ارائه‌ی اثبات‌های دقیق، روش آن‌ها را با مثال روشن می‌کنیم.

۱.۸.۱ تعریف. فرض کنیم $\mathcal{K}$ دسته‌ای از دستگاه‌های جبری از نوع τ باشد، $A \in \mathcal{K}$ و $X \subseteq A$. در این صورت، می‌گوییم که دستگاه جبری A **روی** مجموعه‌ی X **در دسته‌ی** $\mathcal{K}$ **آزاد** است اگر **شرط جهانی** زیر برقرار باشد: برای هر $B \in \mathcal{K}$ و هر **تابع** $f : X \to B$، **همریختی** منحصر به فرد $\overline{f} : A \to B$ وجود داشته باشد به طوری که $\overline{f}\,|_X = f$، یعنی، برای هر $x \in X$، $\overline{f}(x) = f(x)$. یعنی، نمودار زیر تعویض‌پذیر باشد:



در این صورت، X را **پایه‌ی** دستگاه جبری آزاد A می‌نامیم و معمولاً می‌نویسیم $A = F(X)$ (که در آن F حرف اول Free به معنی آزاد است).

۲.۸.۱ بحث در کلاس. قبل از بررسی حالت‌های نیم‌گروه، تکواره، و گروه آزاد، چند نکته‌ی کلی را بیان می‌کنیم.

۱- با توجه به تعریف بالا، آزاد بودن A به دو عامل **مجموعه‌ی** X **و دسته‌ی** $\mathcal{K}$ بستگی دارد. یعنی، اگر هر یک از این دو عامل را تغییر دهیم، ممکن است دیگر A **نسبت به حالت جدید آزاد نباشد**! مثال‌هایی ارائه خواهیم داد که این موضوع را اثبات می‌کنند.

۲- یک ویژگی **بسیار مهم** و اساسی جبر $F(X)$ که با پایه‌ی X در $\mathcal{K}$ **آزاد** است، این است که برای تعریف هر همریختی g با دامنه‌ی جبر آزاد $F(X)$، تنها کافی است $g(x)$ را برای هر $x \in X$ مشخص کنیم! و در این صورت وجود همریختی g تضمین می‌شود! برای مثال، اگر $X = \{x_1, \cdots, x_n\}$، آنگاه برای تعریف همریختی g کافی است تنها چند نگاره‌ی $g(x_1)$، $\cdots$، $g(x_n)$ را مشخص کنیم، در این صورت، شرط جهانی داده شده در تعریف **۱.۸.۱ وجود** همریختی **یکتای** g را تضمین می‌کند! **جالب است! این طور نیست؟** (این مطلب به ویژه یکی از قضیه‌های مهم و پر کاربرد در دروس جبر و جبر خطی است).

۳- ویژگی مهم و جالب دیگر دستگاه جبری آزاد $F(X)$ که در یکتایی مذکور در بند **۲** مستتر است، این است که اگر دو **همریختی** با دامنه‌ی $F(X)$ روی عضوهای X یکسان عمل کنند، آنگاه آن دو همریختی **برابر** هستند!

۴- بررسی و مطالعه‌ی وجود یا عدم وجود دستگاه‌های جبری آزاد در یک دسته‌ی داده شده‌ی دلخواه، خارج از بحث این کتاب است. همچنین، نشان نمی‌دهیم که X دستگاه جبری آزاد $F(X)$ را، در صورت وجود، به تعبیر تعریف **۱۲.۶.۱** تولید می‌کند، یعنی $< X > = F(X)$.

۳.۸.۱ نیم‌گروه‌های آزاد. توجه می‌کنیم که تعریف **۱.۸.۱** نه تنها صحبتی از **وجود** جبرهای آزاد در $\mathcal{K}$ نمی‌کند، بلکه ارتباطی بین عضوهای $F(X)$ و عضوهای X ارائه نمی‌دهد! در ادامه‌ی این بخش خواهیم دید که وقتی $\mathcal{K}$ کلاس نیم‌گروه‌ها، تکواره‌ها، یا گروه‌ها باشد، نه تنها این نوع جبرهای آزاد **وجود دارند**، بلکه **الگوریتمی** برای ساختن عضوهای $F(X)$ بر حسب عضوهای X نیز وجود دارد. ابتدا، برای درک بهتر تعریف **۱.۸.۱**، و چگونگی به کار بردن آن، چند مثال می‌آوریم.

۴.۸.۱ بحث در کلاس (اختیاری) **ترفندهای زیر را بیاموزید**، زیرا در بسیاری از درس‌های ریاضی، به ویژه در جبر و جبر خطی، به کار می‌آیند.

۱- نیم‌گروه جمعی $(\mathbb{N}; +)$ با پایه‌ی تک عضوی $X = \{1\}$ در کلاس نیم‌گروه‌ها آزاد است. زیرا، فرض کنیم $(B; *)$ نیم‌گروهی دلخواه و $f : \{1\} \to B$ تابعی دلخواه باشد. در این صورت، به راحتی می‌توانید نشان دهید که $\overline{f} : \mathbb{N} \to B$ با تعریف

$$\overline{f}(n) = f(1) * \cdots * f(1) \qquad (n \text{ مرتبه})$$

همریختی مورد نظر در تعریف **۱.۸.۱** است. **چطور؟**

۲- حال، کلاس $\mathcal{K}$ را تغییر می‌دهیم. **آیا** $(\mathbb{N}; +)$ روی همان $X = \{1\}$ در کلاس بزرگ‌تر **همه‌ی گروهواره‌ها**، به جای **نیم‌گروه‌ها**، آزاد است؟ **پاسخ منفی است**. زیرا، فرض کنیم $(B; *)$ گروهواره‌ی $\mathbb{Z}$ همراه با عمل دوتایی **تفریق** باشد (که البته شرکت‌پذیر نیست) و تابع $f : \{1\} \to \mathbb{Z}$ با شرط $f(1) = k \neq 0$ داده شده باشد. در این صورت، بر **خلاف ادعا**، فرض

کنیم همریختی $\overline{f}:\mathbb{N}\to\mathbb{Z}$ مذکور در تعریف ۱.۸.۱ وجود داشته باشد. حال، اگر $\overline{f}(3)$ را به دو صورت

$$\overline{f}(3)=\overline{f}((1+1)+1) \quad \text{و} \quad \overline{f}(3)=\overline{f}(1+(1+1))$$

محاسبه کنیم، دو جواب متفاوت k و $-k$ را به دست می‌آوریم، که **تناقض** است! توجه کنید که، چون $\overline{f}$ همریختی است و اینکه عمل گروهواره‌ی $B=\mathbb{Z}$ را تفریق در نظر گرفته‌ایم، داریم

$$\begin{aligned}\overline{f}(1+(1+1))&=\overline{f}(1)-(\overline{f}(1+1))=\overline{f}(1)-(\overline{f}(1))-\overline{f}(1))\\&=k-(k-k)=k-k+k=k\end{aligned}$$

$$\begin{aligned}\overline{f}((1+1)+1)&=\overline{f}(1+1)-\overline{f}(1)=(\overline{f}(1)-\overline{f}(1))-\overline{f}(1)\\&=k-k-k=-k\end{aligned}$$

۳- مثال‌های بالا درستی ادعای بند ۱ بحث ۲.۸.۱ را نیز نشان می‌دهند.

قضیه‌ی جالب زیر یکی دیگر از **مزیت‌های** نیم‌گروه‌های آزاد را بر نیم‌گروه‌های غیر آزاد نشان می‌دهد. این قضیه بیان می‌کند که با داشتن مجموعه‌ی X ، همه‌ی عضوهای $A=F(X)$ را می‌توان به گونه‌ای **منحصر به فرد** تولید کرد. برخی (به ویژه در علوم کامپیوتر) این قضیه را **به عنوان تعریف** نیم‌گروه آزاد ارائه می‌دهند.

۵.۸.۱ قضیه. نیم‌گروه $(A;*)$ با پایه‌ی $X\subseteq A$ آزاد است اگر و تنها اگر

(الف) هر عضو $a\in A$ را بتوان به صورت $a=x_1*\cdots*x_n$ نوشت، که در آن هر x_i در X است (یعنی، باتوجه به بند ۲ بحث ۱۶.۶.۱، X دستگاه جبری A را تولید می‌کند)، و

(ب) این عبارت برای هر $a\in A$ منحصر به فرد باشد. یعنی، برای $x_i,y_i\in X$،

$$a=x_1*\cdots*x_n=y_1*\cdots*y_m\Leftrightarrow m=n\,\&\,(\forall i)x_i=y_i$$

۶.۸.۱ بحث در کلاس. برای به نمایش گذاشتن چگونگی استفاده از این قضیه، مثال نیم‌گروه آزاد $(\mathbb{N};+)$ را دوباره می‌آوریم. نیم‌گروه جمعی $(\mathbb{N};+)$ با پایه‌ی تک عضوی $X=\{1\}$ در دسته‌ی نیم‌گروه‌ها آزاد است، زیرا هر عدد طبیعی n را می‌توان به‌گونه‌ی منحصر به فرد (n مرتبه) $n=1+\cdots+1$ نوشت.

توجه می‌کنیم که اگر چه هر عدد طبیعی را می‌توان به صورت مجموعی از عضوهای $\{1,2\}$ نیز نوشت (**چطور؟**) ولی، برای مثال، تساوی‌های

$$۵ = ۱+۱+۲+۱ = ۱+۱+۱+۲ = ۱+۲+۲$$

نشان می‌دهند که شرط **(ب)** منحصر به فرد بودن در قضیه‌ی بالا **برقرار نیست!** یعنی، نیم‌گروه $(\mathbb{N};+)$ **با پایه‌ی** $\{1,2\}$ **آزاد نیست!**

در مثال‌های بالا، نیم‌گروه A همراه با عمل دوتایی $*$ داده شده بود و می‌خواستیم ببینیم که آیا زیرمجموعه‌ای چون X از A وجود دارد که پایه‌ای برای A باشد؟ حال، می‌خواهیم **عکس** این سؤال را بررسی کنیم. به عبارت دیگر، فرض می‌کنیم مجموعه‌ای چون X داده شده است. **آیا** نیم-گروه آزاد $F(X)$ وجود دارد که X پایه‌ای برای آن باشد؟

فرض کنیم X مجموعه‌ای دلخواه باشد. ساختن نیم‌گروهی آزاد با پایه‌ی X، کار چندان پیچیده و سختی نیست. کافی است دست کم یک نیم‌گروه صوری (به طور مصنوعی) بسازیم که دارای **شرایط (الف)** و **(ب)** قضیه‌ی **۵.۸.۱** باشد. با الگو قرار دادن ساختن کلمه و جمله از حروف الفبای زبان‌های محاوره‌ای، تعریف صوری زیر را می‌آوریم.

۷.۸.۱ تعریف. عضوهای X را **الفبا** می‌نامیم و هر دنباله‌ی متناهی (و ناتهی) چون $(x_1,\cdots,x_n)$ از عضوهای X را با عبارت صوری $x_1\cdots x_n$ نمایش می‌دهیم و آن را یک **کلمه‌ی آزاد** یا، به طور ساده، یک **کلمه** روی X می‌نامیم.

برای مثال، اگر X مجموعه‌ی حروف الفبای فارسی باشد، آنگاه ق، ل، م، ق ل م، م ب ا ن ی، ج ب ر، ب ج ر، ر ب ج، . . .، مثال‌هایی از کلمه (ی **آزاد**) روی X هستند.

حال، فرض کنیم X^* مجموعه‌ی همه‌ی کلمه‌های آزاد (ناتهی) روی X باشد. در این صورت، به روشنی

$$x_1\ldots x_m * y_1\ldots y_n = x_1\ldots x_m\, y_1\ldots y_n$$

که صرفاً از **کنار هم** گذاشتن صوری دو کلمه به دست می‌آید، عملی دوتایی در X^* تعریف می‌کند. در این صورت، به راحتی می‌توانید نشان دهید که

۸.۸.۱ قضیه. *نیم‌گروه $(X^*;*)$ نیم‌گروهی آزاد با پایه‌ی X است.* ■

توجه می‌کنیم که چون هر کلمه یک دنباله است، تساوی دنباله‌ها به روشنی در شرط (ب) قضیه‌ی ۵.۸.۱ صدق می‌کند. همچنین، عضوهای X^* **آزادانه** و بدون هیچ قیدی از کنار هم گذاشتن الفبا، یعنی عضوهای X ، ساخته شدند. این مطلب توجیهی برای انتخاب واژه‌ی **آزاد** است!

۹.۸.۱ بحث در کلاس

۱- برای هر $X \neq \varnothing$ ، نیم‌گروه آزاد X^* نامتناهی است. **چطور؟**

۲- فرض کنیم $X = \{x\}$ تک عضوی باشد. در این صورت، نیمگروه X^* **به خودی خود آبلی** (تعویض‌پذیر) است (**چطور؟**) نشان دهید که اگر X دست کم دارای دو عضو متفاوت x و y باشد، آنگاه نیم‌گروه آزاد X^* **آبلی نیست!**

۳- همان طور که گفتیم، هیچ قیدی برای ساختن عضوهای نیم‌گروه آزاد وجود ندارد. ولی ممکن است خودمان از قبل بخواهیم **قیدهایی** برای ساختن کلمه‌ها قایل شویم. برای مثال، در زبان محاوره‌ای، معمولاً کلمه‌هایی از حروف الفبا می‌سازیم که در آن زبان با معنی باشند. روشن است که مجموعه‌ی این نوع کلمه‌ها زیرمجموعه‌ی X^* است، ولی لزوماً زیرنیم‌گروه آن **نیست.**

چطور نیم‌گروه **آبلی** آزاد، **تکواره‌ی** آزاد، یا **گروه** آزاد بسازیم؟

۱۰.۸.۱ نیمگروه آبلی آزاد. برای تعریف نیم‌گروه **آبلی** آزاد، کافی است در **تعریف ۱.۸.۱**، $\mathcal{K}$ را **دسته‌ی نیمگروه‌های آبلی** در نظر بگیریم. ولی، صورت قضیه‌ی ۵.۸.۱ و عضوهای X^* چه تغییری می‌کنند؟ بند (الف) قضیه‌ی ۵.۸.۱ را می‌توان تغییر نداد، ولی بند (ب) **چطور؟** یقیناً باید عضو $x*y$ با عضو $y*x$ برابر باشد. پس، بند (ب) را باید به صورت زیر اصلاح کرد:

$$x_1 *\cdots* x_m = y_1 *\cdots* y_n \quad \Leftrightarrow m = n$$

و در صورت لزوم، با **تغییر ترتیب** x_i ها، برای هر i ، $x_i = y_i$ ، یعنی، $\{x_1,\cdots,x_n\} = \{y_1,\cdots,y_n\}$. (همین ایده‌ی تغییر ترتیب بیان می‌کند که بند (الف) را می‌توان به صورت زیر تغییر داد: هر عضو $a \in A$ را می‌توان به صورت $a = x_1^{k_1} *\cdots* x_n^{k_n}$ نیز نوشت، که در آن $k_i \in \mathbb{N}$ و برای هر $k \in \mathbb{N}$ ، $x^k = x*\cdots*x$. **چطور؟**).

۱۱.۸.۱ بحث در کلاس. آیا نیم‌گروه ضربی $\mathbb{N}\setminus\{1\}$ در دسته‌ی نیمگروه‌ها آزاد است؟ به عبارت دیگر، **آیا** زیرمجموعه‌ی $X \subseteq \mathbb{N}\setminus\{1\}$ وجود دارد به طوری که هر عدد طبیعی $n \neq 1$ حاصلضرب منحصر به فرد عضوهای X باشد؟ با قدری تامل متوجه می‌شویم که مجموعه‌ی **اعداد اول** نامزد خوبی است. ولی دارای ویژگی بند (ب) قضیه‌ی ۵.۸.۱ نیست! برای مثال،

$$۴۵ = ۳ \times ۵ \times ۳ = ۵ \times ۳ \times ۳$$

ولی از آنجا که ترتیب در ضرب اعداد مهم نیست، این نقص بر طرف می‌شود و نیم‌گروه ضربی **آبلی** $\mathbb{N}\setminus\{1\}$ با پایه‌ی $X = \{$اعداد اول$\}$ در **دسته‌ی همه‌ی نیمگروه‌های آبلی**، آزاد است، که البته در دسته‌ی بزرگ‌تر همه‌ی نیم‌گروه‌ها (آبلی و غیر آبلی) **آزاد نیست. چرا؟**

۱۲.۸.۱ تکواره‌ی آزاد. برای تعریف **تکواره‌ی** آزاد نیز کافی است در **تعریف ۱.۸.۱**، $\mathcal{K}$ را **دسته‌ی تکواره‌ها** در نظر بگیریم. ارائه‌ی همتای قضیه‌ی **۵.۸.۱** نیز راحت است. بند **(الف)** آن نیازی به تغییر ندارد. بند **(ب) چطور؟** برای مثال، اگر e عضو همانی تکواره‌ی آزاد $(A;*,e)$ باشد، عبارت‌های

$$e*x*y*e = x*y$$

در شرط **(ب)** آن قضیه صدق نمی‌کنند. این **نقص** را چگونه **برطرف** می‌کنید؟ **آیا** تکواره‌ی ضربی $(\mathbb{N};\cdot)$ در دسته‌ی تکواره‌ها آزاد است؟

حدس می‌زنید که **چطور** می‌توان تکواره‌ی آزاد با پایه‌ی X **ساخت؟** یعنی، همتای X^* **چیست؟** یقیناً پیشنهاد می‌کنید که X^* را همان نیم‌گروه کلمه‌های (آزاد) روی X در نظر بگیریم و سپس مانند بند **۵** بحث **۱۲.۳.۱** تکواره‌ی $(X^{*e};*,e)$ را تشکیل دهیم، که در آن $e \notin X^*$ و $X^{*e} = X^* \cup \{e\}$! **درست است.** به‌راحتی می‌توانید درستی تعریف **۱.۸.۱** را بررسی کنید.

خوب است این نکته را نیز بیان کنیم که در تعریف **۷.۸.۱** همه‌ی دنباله‌های **ناتهی** را در نظر گرفتیم. حال، اگر دنباله‌ی **تهی** را نیز در نظر بگیریم و آن را e بنامیم، مجدداً مسئله را حل کرده‌ایم!

۱۳.۸.۱ گروه آزاد. (اختیاری) با توجه به تجربه‌ای که تاکنون در یافتن و بررسی نیم‌گروه، تکواره، و، به ویژه نیم‌گروه آبلی آزاد به دست آوردید، می‌توانیم **قدمی جلوتر** برویم و **گروه آزاد** را مطالعه کنیم. مجدداً، برای تعریف آن بر اساس **۱.۸.۱ مشکلی نداریم**. کافی است در آن تعریف، $\mathcal{K}$ را **دسته‌ی گروه‌ها** در نظر بگیریم. همتای قضیه‌ی **۵.۸.۱، به ویژه** بند **(ب)** آن، **چه می‌شود؟** همتای X^* **چیست؟**

۱۴.۸.۱ بحث در کلاس. اگر $X = \{1\}$ را زیرمجموعه‌ی $\mathbb{Z}$ در نظر بگیریم و **مقید** باشیم که تنها از عمل دوتایی جمع استفاده کنیم، بند **(الف)** قضیه‌ی **۵.۸.۱** تنها عضوهای $\mathbb{N}$ را به صورت زیر به دست می دهد:

$$۱\ ,\ ۱+۱\ ,\ ۱+۱+۱\ ,\cdots$$

ولی، اگر عمل یکانی **قرینه‌یابی** را نیز به کار ببریم، یقیناً **همه**ی عضوهای $\mathbb{Z}$ به دست می‌آیند:

$$۰=۱+(-۱),\ -۱,\ (-۱)+(-۱),\ (-۱)+(-۱)+(-۱),\ \cdots$$

شرط **۲** را نیز باید تغییر دهیم! زیرا، برای مثال

$$۱+(-۱)+۱+۰+۱ = ۱+۱ \quad \text{یا} \quad ۰+۰ = ۰+۰+۰ = ۱+(-۱)$$

منحصر به فردی مذکور در بند **(ب)** قضیه‌ی **۵.۸.۱** را **نقض** می‌کند! **چطور** این نقض را برطرف کنیم؟ **درست حدس زدید**، هر عبارت را با **حذف** صفرهای اضافی و **حذف** عبارت‌های $1+(-1)$ و $(-1)+1$ به **ساده‌ترین صورت** می‌نویسیم! حال، همتای قضیه‌ی **۵.۸.۱** به صورت زیر بیان می‌شود:

۱۵.۸.۱ قضیه. گروه $(A;*,\cdot^{-1},e)$ یا $(A;*)$ با پایه‌ی X آزاد است اگر و تنها اگر

۱- هر عضو $a\in A$ را بتوان به‌صورت $a=x_1*\cdots*x_n$ نوشت، که در آن هر x_i یا وارون آن در X است، و

۲- این عبارت برای a با شرط **حذف** e های اضافی و **حذف** عبارت‌های به صورت $x*x^{-1}$ و $x^{-1}*x$ منحصر به فرد باشد.

۱۶.۸.۱ بحث در کلاس. بحث **۱۴.۸.۱** بالا راهنمایمان برای پیدا کردن همتای گروه آزاد X^* است. فرض کنیم مجموعه‌ی X داده شده است و می‌خواهیم گروه آزاد $(F(X);*)$ را به صورت صوری روی X بسازیم. اگر همه‌ی کلمه‌های (تهی و ناتهی) روی X را در نظر بگیریم، تنها به یک تکواره دست خواهیم یافت. **چه کار کنیم؟** شاید ساده‌ترین روش، به زبانی نه چندان دقیق، این باشد که متناظر با هر $x\in X$ ، عنصری (نمادی) به نمایش صوری، **تنها به نمایش**، x^{-1} **خارج از** X انتخاب کنیم و مجموعه‌ی این نمادهای جدید را با X^{-1} نشان دهیم، سپس فرض کنیم $Y=X\cup X^{-1}$. توجه می‌کنیم که $X\cap X^{-1}=\varnothing$ و $|X|=|X^{-1}|$. حال، مجموعه‌ی همه‌ی کلمه‌های (تهی و ناتهی) روی Y را، که در آن‌ها عبارت‌های $x*x^{-1}$ و $x^{-1}*x$ وجود ندارند، Y^* می‌نامیم. عمل $*$ را در Y^* همان "**کنار هم گذاری**" کلمه‌ها در نظر می‌گیریم، با این شرط که با حذف عبارت‌های $x*x^{-1}$ و $x^{-1}*x$ آن کلمه را به کلمه‌ای متعلق به Y^* تبدیل می‌کنیم. برای مثال،

$$xy^{-1}z*z^{-1}yu=xy^{-1}zz^{-1}yu=xy^{-1}yu=xu$$

در این صورت، $(Y^*;*)$ گروهی خواهد شد که در آن عضو همانی e همان کلمه‌ی تهی و وارون هر عبارت صوری $y_1y_2\cdots y_n$ برابر با عبارت صوری $y_n^{-1}y_{n-1}^{-1}\cdots y_1^{-1}$ است. با بررسی تعریف **۱.۸.۱** می‌توانید نشان دهید که $(Y^*;*,^{-1},e)$ در دسته‌ی گروه‌ها روی X **آزاد** است.

۱۷.۸.۱ کدگذاری یکی از کاربردهای نیم‌گروه و تکواره‌ی آزاد در کدگذاری است. در این قسمت مطالبی بسیار به اختصار در باره‌ی مفهوم **کد** به زبان جبری می‌آوریم و مطالعه‌ی دقیق آن را به دروس مستقل دیگری، به ویژه در کهادهای کدگذاری و علوم کامپیوتر، واگذار می‌کنیم. برای توجیه تعریف زیر، فرض کنیم هر حرف الفبا را با رشته‌ای از نمادهای "**نقطه** – **خط**" **مورس کدگذاری** کنیم. در این صورت، هر حرف، کلمه، و جمله متناظر با رشته‌ای **منحصر به فرد** از نمادهای مورس است. منحصر به فردی باعث می‌شود که بتوانیم آن کلمه یا جمله را از رشته‌ی متناظرش باز نویسی کنیم.

به عنوان مثالی دیگر، هر رقم صفر تا ۹ و در نتیجه هر عدد در مبنای ۱۰، رشته‌ای **منحصر به فرد** از نمادهای 0 و 1 در مبنای ۲ دارد تا بتوان عدد نوشته شده در مبنای ۱۰را از رشته‌ی متناظرش در مبنای ۲ بازنویسی کرد. **به زبان جبری**، تعریف زیر را داریم.

۱۸.۸.۱ تعریف. هر زیرمجموعه‌ی ناتهی چون C از نیم‌گروه آزاد X^* را یک **کد** (یا **رمز**) روی X می‌نامیم، اگر در **شرط یکتایی** زیر صدق کند. برای هر $c_1,\cdots,c_m,d_1,\cdots,d_n\in C$ ،

$$c_1c_2\cdots c_m=d_1d_2\cdots d_n\Leftrightarrow m=n\,\&\,(\forall i)\quad c_i=d_i$$

۱۹.۸.۱ بحث در کلاس

۱- آیا شرط بالا همان شرط (ب) قضیه‌ی **۵.۸.۱** نیست؟

۲- با توجه به این تعریف، $C=\{0,01,10\}$ یک **کد** روی $X=\{0,1\}$ **نیست**. زیرا، برای مثال، به ازای $c_1=10$ ، $c_2=0$ ، $c_3=10$ ، $d_1=10$ ، $d_2=01$ ، $d_3=0$ ، داریم

$$c_1c_2c_3=10010=d_1d_2d_3$$

درحالی که $c_2\neq d_2$ و همچنین $c_3\neq d_3$!

۳- به عنوان مثالی دیگر، فرض کنیم $X=\{a\}$ در این صورت، $C=\{a\}$ **تنها کد** روی X است. برای مثال، $C=\{aa\}$ یک کد روی X **نیست**. زیرا، اگر قرار دهیم $c_1=aa$

و $d_1 = d_2 = d_3 = d_4 = a$ ، آنگاه $c_1c_1 = aaaa = d_1d_2d_3d_4$ یکتایی مذکور در تعریف کد را نقض می‌کند. نشان دهید که $C = \{a, aa\}$ نیز یک کد روی $X = \{a\}$ **نیست**.

۴- فرض کنیم $C \subseteq X^*$ دلخواه و

$$< C > = \{c_1c_2 \cdots c_n \mid n \in \mathbb{N}, c_i \in C\}$$

زیرنیم‌گروه X^* باشد که توسط C تولید شده است. در این صورت، اگر چه هر عضو $< C >$ به صورت کلمه‌ی $c_1c_2 \cdots c_n$ نوشته می‌شود، ولی این عبارت لزوماً منحصر به فرد نیست! شرط مذکور در تعریف **کد** بیان می‌کند که اگر C یک کد باشد، آنگاه این عبارت، به گونه‌ای که در تعریف بالا بیان شد، باید منحصر به فرد باشد. به عبارت دیگر، زیرنیم‌گروه $< C >$ از نیم‌گروه آزاد X^* خود روی مجموعه‌ی C آزاد است. همان طور که قبل از تعریف کد بیان شد، اگر این منحصر به فرد بودن وجود نداشته باشد؛ کد متناظر با یک جمله را نمی‌توان دقیقاً به همان جمله باز گرداند. این مطالب را به **زبان جبری** می‌توان به یکی از صورت‌های معادل زیر بیان کرد:

۱- زیرمجموعه‌ی C یک کد روی X است.

۲- برای تابع شمولی $f : C \rightarrowtail < C >$ ، همریختی منحصر به فرد $\overline{f} : C^* \rightarrow < C >$ مذکور در تعریف ۱.۸.۱ دوسویی است.

۳- مجموعه‌ی B و همریختی یک به یک نیم‌گروه‌ها چون $k : B^* \rightarrow X^*$ وجود دارد به طوری که $k(B) = C$.

همریختی یک به یک k در بند ۳ قضیه‌ی بالا را **همریختی کدگذار** و وارون آن $k^{-1} : < C > \rightarrow B^*$ را **همریختی کد گشا** می‌نامیم.

تمرین ۸.۱

هوشم نه چنان است تلاشم آنچنان است
موفق باشید

۱- اثبات قضیه‌ی ۵.۸.۱ را با توجه به تعریف ۱.۸.۱ بنویسید.

۲- تکواره‌ی آزاد روی $\{x\}$ را تعیین کنید. این تکواره با چه تکواره‌ی شناخته شده‌ای یکریخت است؟

۳- فرض کنید A و B ساختارهای جبری آزاد روی یک مجموعه‌ی X **در** $\mathcal{K}$ باشند. نشان دهید که A و B یک‌ریختند.

۴- فرض کنید A دستگاه جبری است که روی هر دو مجموعه‌ی X **و** Y **در دسته‌ی** $\mathcal{K}$ آزاد است. نشان دهید که مجموعه‌های X و Y همتوان هستند.

۵- فرض کنید A ساختار جبری آزاد روی مجموعه‌ی X **در** $\mathcal{K}$ باشد و $Y \subseteq X$. نشان دهید که $B = <Y>$ روی مجموعه‌ی Y **در** $\mathcal{K}$ آزاد است.

۹.۱ واریته و قضیه‌ی بیرخوف

در این بخش بسیار کوتاه صرفاً می‌خواهیم **قضیه‌ی بسیار مهمی** را بدون اثبات بیان کنیم. استادان درس ممکن است به دلیل کمبود وقت این بخش را تدریس ننمایند.

فرض کنیم $\mathcal{K} \subseteq \mathcal{A}\lg(\tau)$ دسته‌ای از دستگاه‌های جبری از نوع τ باشد. در این صورت، $\mathcal{K}$ ممکن است دارای برخی از ویژگی‌های زیر باشد:

I: دسته‌ی $\mathcal{K}$ **نسبت به یک‌ریختی بسته باشد**: یعنی، هر جبری از نوع τ که با عضوی از $\mathcal{K}$ یکریخت است، متعلق به $\mathcal{K}$ باشد.

$$\{A \in \mathcal{A}\lg(\tau) \mid (\exists B \in \mathcal{K}), A \cong B\} = \mathcal{K}$$

S: دسته‌ی $\mathcal{K}$ **نسبت به زیرجبر بسته باشد**: یعنی، هر جبری از نوع τ که زیرجبر عضوی از $\mathcal{K}$ است، متعلق به $\mathcal{K}$ باشد. $\{A \in \mathcal{A}\lg(\tau) \mid (\exists B \in \mathcal{K}), A \leq B\} = \mathcal{K}$.

P_r: دسته‌ی $\mathcal{K}$ **نسبت به ضرب بسته باشد**: یعنی، هر جبری از نوع τ که حاصلضرب عضوهایی از $\mathcal{K}$ است، متعلق به $\mathcal{K}$ باشد.

$$\{A \in \mathcal{A}\lg(\tau) \mid (\exists \{B_i\}_{i\in I} \subseteq \mathcal{K}), A = \prod_{i\in I} B_i\} = \mathcal{K}$$

H: دسته‌ی $\mathcal{K}$ **نسبت به خارج قسمت بسته باشد**: یعنی، هر جبری از نوع τ که خارج قسمت عضوی از $\mathcal{K}$ است، متعلق به $\mathcal{K}$ باشد.

$$\{A \in \mathcal{A}\lg(\tau) \mid (\exists B \in \mathcal{K}), A = B/\sim\} = \mathcal{K}$$

۱.۹.۱ تعریف. فرض کنیم $\mathcal{K} \subseteq \mathcal{A}lg(\tau)$ دسته‌ای از دستگاه‌های جبری از نوع τ باشد.

۱- دسته‌ی $\mathcal{K}$ را **واریته** (یا **چند گونا**) می‌نامیم اگر $\mathcal{K}$ دارای ویژگی‌های I، S، P_r، و H باشد.

۲- دسته‌ی $\mathcal{K}$ را **معادله‌ای** (یا اتحادی) می‌نامیم اگر مجموعه‌ای چون P از معادله‌ها وجود داشته باشد به‌طوری که $\mathcal{K}$ متشکل از همه‌ی جبرهای از نوع τ باشد به طوری که هر معادله‌ی متعلق به P در هر عضو $\mathcal{K}$ اتحاد باشد. یعنی،

$$\mathcal{K} = \{A \in \mathcal{A}lg(\tau) \mid A \models P\}$$

شاید مهم‌ترین قضیه در مبحث جبر، قضیه‌ی بسار جالب و مفید بیرخوف باشد که بیان می‌کند:

۲.۹.۱ قضیه (**بیرخوف**). دسته‌ی $\mathcal{K} \subseteq \mathcal{A}lg(\tau)$ **واریته** است اگر و تنها اگر دسته‌ای **معادله‌ای** باشد.

۳.۹.۱ بحث در کلاس. شاید خوب باشد قضیه‌ی بیرخوف را کمی بیش‌تر تفسیر کنیم.

۱- با توجه به قضیه‌ی اساسی همریختی‌ها، بسته بودن نسبت به خارج قسمت با بسته بودن نسبت به نگاره‌ی همریختی‌ها معادل است. همچنین، روشن است که بسته بودن نسبت به همریختی‌ها، بسته بودن نسبت به یک‌ریختی‌ها را ایجاب می‌کند.

۲- یک طرف قضیه‌ی بیرخوف بیان می‌کند که اگر $\mathcal{K}$ دارای ویژگی‌های H، S، P_r، باشد، حتماً دسته‌ای از معادله‌ها مانند P وجود دارد به طوری که در هر عضو $\mathcal{K}$ برقرار (**اتحاد**) هستند و هر جبری (از نوع τ) که در این معادله‌ها صدق کند متعلق به $\mathcal{K}$ است. این ویژگی $\mathcal{K}$ باعث می‌شود که برنامه‌های کامپیوتری نیز برای مطالعه‌ی جبرهای متعلق به $\mathcal{K}$ به کار بیایند. البته پیدا کردن این دسته از معادله‌ها همیشه کار راحتی نیست. برخی از ریاضی‌دانان، که در دانشگاه‌های ایران نیز وجود دارند، در کارهای پژوهشی خود (به ویژه در نظریه‌ی گروه‌ها) به دنبال روش‌هایی برای پیدا کردن P می‌گردند.

۳- طرف دیگر قضیه بیان می‌کند که اگر $\mathcal{K} = \{A \in \mathcal{A}lg(\tau) \mid A \models P\}$ با دسته‌ای از معادله‌ها مشخص شود (برای مثال، نیم‌گروه‌ها دسته‌ای از گروهواره‌ها، جبرهای از نوع $\tau = (2)$، هستند که در معادله‌ی شرکت‌پذیری صدق می‌کنند) آنگاه $\mathcal{K}$ یقیناً دارای ویژگی‌های H، S، P_r است.

۴- فرض کنیم $\mathcal{K}$ دسته‌ی همه‌ی تکواره‌هایی مانند $(A;*,e)$ باشد به طوری که حاصل ضرب هر دو عضو ناهمانی در A ناهمانی باشد. در بند ۳ بحث ۲۲.۶.۱ دیدیم که اگر چه $(\mathbb{Z};+,0)$ عضو دسته‌ی $\mathcal{K}$ است، ولی حاصل ضرب $\mathbb{Z}\times\mathbb{Z}$ متعلق به $\mathcal{K}$ نیست (زیرا $(1,0)(0,1) = (0,0)$). پس، غیر ممکن است بتوان مجموعه‌ای از معادله‌ها یافت که مشخص کننده‌ی دسته‌ی $\mathcal{K}$ باشد!

۵- حال بهتر متوجه می‌شویم که چرا این قدر به P- جبرهایی اهمیت می‌دهیم که در آن P مجموعه‌ای از **معادله**‌ها باشد. همچنین، قضیه‌ی بالا مطالعه‌ی **زیردستگاه**، **همریختی**، **ضرب دکارتی**، و **خارج قسمت** را در هر دسته‌ای از جبرها توجیه می‌کند.

تمرین ۹.۱

۱- یک طرف قضیه‌ی بیرخوف (**۲.۹.۱**) با استفاده از قضیه‌های این فصل اثبات می‌شود. آن قضیه‌ها را مشخص کنید.

فصل ۲

گروه‌ها

در **فصل ۱** مفاهیم دستگاه جبری (نه لزوماً با ویژگی) و P - جبر (با ویژگی P) را معرفی و برخی از مفاهیم، مانند **زیرجبر**، **ضرب**، **همضرب**، **خارج قسمت**، و **همریختی**، را که در همه‌ی دستگاه‌های جبری مشترک هستند، بررسی کردیم. همان طور که در فصل **۱** نیز بیان شد، تقریباً همه‌ی دستگاه‌های جبری‌ای که مطالعه خواهیم کرد P - جبری با یک یا چند **ویژگی** هستند. در بخش‌های **۲.۱** تا **۴.۱**، P - جبرهای نیم‌گروه، تکواره، حلقه، مشبکه، شبه‌گروه، و گروه را، به عنوان نمونه‌هایی از دستگاه‌های جامع جبری با ویژگی، معرفی کردیم و قرار شد دستگاه تاریخی و پر کاربرد گروه را در این فصل با جزییات بیشتری مورد مطالعه قرار دهیم.

از آنجا که هر بخش این فصل همتا و حالت خاص قسمتی یا تمام بخشی از **فصل ۱** است، به شما خوبان **توصیه** می‌کنیم که شب قبل از کلاس چند دقیقه‌ای حالت کلی موضوع درس را از فصل **۱** مرور کنید تا درک بهتر و درست‌تری از هر دو حالت کلی و خاص به دست آورید. در ضمن، استاد درس نیز ممکن است برای صرفه جویی در وقت برخی از مطالب و فنون اثبات را تکرار نکند و به **فصل ۱** رجوع دهد!

مطابق معمول این کتاب و قولی که دادیم، در ارائه‌ی مطالب، بلافاصله سر اصل مطلب نمی‌رویم بلکه تا جایی که زمان اجازه دهد، شما خوانندگان را با **فوت و فن** کار آشنا می‌کنیم و روش کار را آموزش می‌دهیم تا آمادگی بیش‌تری برای مطالعه‌ی فصل **۳** و درس‌های دیگر جبر به دست آورید. البته مجدداً سفارش می‌کنیم که

اندیشیدن بیاموزیم و اندیشه ورزی کنیم

۱.۲ قضیه‌های معادل تعریف گروه

در این بخش، ابتدا تعریف ۵.۴.۱ گروه و صورت معادل آن را از بند۲ بحث ۶.۴.۱ یادآوری می‌کنیم و آن‌ها را مورد بحث قرار می‌دهیم. سپس چند قضیه‌ی دیگر معادل با تعریف گروه ارائه می‌کنیم که هر یک سودمندی و کارایی ویژه‌ای دارد.

۱.۱.۲ تعریف. نیم‌گروه $(G;*)$ را **گروه** می‌نامیم اگر دارای عضو **همانی** باشد و هر عضو آن **وارون** داشته باشد. به عبارت دیگر، گروهواره‌ی $(G;*)$ را **گروه** می‌نامیم اگر دارای شرایط زیر باشد:

(گ۱) (**اتحاد شرکت‌پذیری**) $(\forall x,y,z\in G)\quad x*(y*z)=(x*y)*z$

(گ۲) (**وجود عضو همانی**) $(\exists e\in G)\quad (\forall x\in G)\quad x*e=x=e*x$

(گ۳) (**وجود وارون‌ها**) $(\forall x\in G)\quad (\exists x^{-1}\in G)\quad x*x^{-1}=e=x^{-1}*x$

۲.۱.۲ بحث در کلاس

۱- با توجه به قضیه‌ی ۷.۳.۱، عضو همانی در هر گروه منحصر به فرد است و بنابر شرکت‌پذیر بودن عمل دوتایی گروه، هر عضو در گروه وارون یکتا دارد (قضیه‌ی ۳.۴.۱ را ببینید. البته توصیه می‌کنیم خودتان اثبات ساده‌ی آن را دوباره ارائه دهید). از این رو، در تعریف بالا نمادهای مشخصی به این عضوها اختصاص داده‌ایم.

۲- (اختیاری) تعریف گروه به همان صورت ۱.۱.۲ بین افرادی که با جبرهای سنتی سروکار دارند متداول‌تر است، ولی در فصل ۱ به دفعات گفتیم و دیدیم که اگر شرط‌های معرف یک دستگاه جبری را بتوان با **اتحاد**ها (بدون استفاده از سورهای وجودی) نیز بیان کرد، کار کردن با آن دستگاه، به ویژه با استفاده از برنامه‌های رایانه‌ای، آسان‌تر است. اگر چه شرط (گ۱) تعریف گروه به صورت اتحاد است ولی دو شرط دیگر (گ۲) و (گ۳) دارای سور وجودی هستند و از این رو اتحاد محسوب نمی‌شوند. سؤال بسیار مهم این است که، آیا می‌شود مفهوم گروه را به گونه‌ای معرفی کرد که اصول موضوع (گ۲) و (گ۳) تعریف ۱.۱.۲ گروه نیز اتحاد باشند؟ خوشبختانه پاسخ به این سوال مثبت است. مشابه تعریف ۱۱.۳.۱ برای تکواره و تعریف شبه‌گروه در بند ۴ بحث ۱۱.۴.۱، اگر عضو همانی منحصر به فرد گروه، یعنی e، را به عنوان عملی صفرتایی و وارون‌گیری منحصر به فرد را عملی یکانی چون

$$\cdot^{-1}:G\to G \qquad\qquad \{0\}\to G$$
$$x\mapsto x^{-1} \qquad\qquad 0\mapsto e$$

در نظر بگیریم، آنگاه تعریف زیر نشان می‌دهد که مفهوم گروه را می‌توانیم به جای دستگاه جبری $(G;*)$ از نوع $\tau=(2)$، به صورت دستگاهی جبری چون $(G;*,^{-1},e)$ از نوع $\tau=(2,1,0)$ معرفی کنیم، و سورهای وجودی در (گ۲) و (گ۳) را حذف و در نتیجه این دو اصل معرف گروه را نیز مانند (گ۱) به صورت دو **اتحاد** بیان کنیم.

۳.۱.۲ تعریف (صورت دوم). دستگاه جبری $(G;*,^{-1},e)$ از نوع $\tau=(2,1,0)$ **گروه** است اگر سه **معادله**‌ی زیر در آن برقرار (یعنی **اتحاد**) باشند:

(گ۱) (**اتحاد شرکت‌پذیری**) $(\forall x,y,z\in G)\quad x*(y*z)=(x*y)*z$

(گ۲) (**اتحاد رابطه‌ی عمل صفرتایی e با $*$**) $(\forall x\in G)\quad x*e=x=e*x$

(گ۳) (**اتحاد رابطه‌ی عمل یکانی $^{-1}$ با e و $*$**) $(\forall x\in G)\quad x*x^{-1}=e=x^{-1}*x$

۴.۱.۲ بحث در کلاس

۱- یکی از ویژگی‌های مهم تعریف ۳.۱.۲ گروه این است که اصول معرف گروه‌ها، **اتحاد** هستند. از این رو، هر آنچه در فصل ۱ در باره‌ی خوبی‌های دستگاه‌های معادله‌ای گفتیم در باره‌ی گروه‌ها نیز برقرار هستند. به ویژه قضیه‌ی ۲.۹.۱ بیرخوف نتیجه می‌دهد که دسته‌ی گروه‌ها، نسبت به **زیرگروه**، **حاصل‌ضرب**، و**خارج قسمت** بسته است؛ یعنی، زیردستگاه جبری گروه‌ها، حاصل‌ضرب گروه‌ها، و خارج قسمت گروه‌ها، خود گروه هستند. **عالی است!** البته این مفاهیم را دوباره برای گروه‌ها مطالعه خواهیم کرد. توجه می‌کنیم که اگر $\mathcal{K}$ زیردسته‌ای از دسته‌ی گروه‌ها با یک (یا چند) ویژگی غیر اتحادی باشد، آنگاه این دسته لزومی ندارد نسبت به زیرگروه، حاصلضرب، وخارج قسمت بسته باشد. برعکس، اگر دسته‌ی $\mathcal{K}$ طوری انتخاب شده باشد که نسبت به زیرگروه، حاصل‌ضرب، یا خارج قسمت بسته نباشد، آنگاه این کلاس با دسته‌ای از اتحادها مشخص نمی‌شود (قضیه‌ی دو طرفه‌ی ۲.۹.۱ بیرخوف را ببینید). این مطالب را در درس‌های دیگر جبر نیز تجربه خواهید کرد.

۲- مفهوم گروه از چه زمانی و چطور وارد مباحث ریاضی شده است؟ چرا این دستگاه جبری ساده این اندازه با اهمیت است و پژوهش‌های بسیاری روی آن انجام شده است و می‌شود؟ تقریباً در هر گروه آموزشی ریاضی در دنیا، و البته در ایران، دست کم یک متخصص نظریه‌ی گروه‌ها وجود دارد.

نام ریاضی‌دانانی چون **لاگرانژ**، **آبل**، و به ویژه **گالوا** همواره با نظریه‌ی گروه‌ها آورده می‌شود. این افراد، به ویژه گالوا، در جستجوی پاسخی برای وجود یا عدم وجود فرمولی رادیکالی (مانند $(-b\pm\sqrt{b^2-4ac})/2a$ برای ریشه‌های ax^2+bx+c) برای پیدا کردن ریشه‌های چند

جمله‌ای‌های از درجه بیش‌تر از ۴، به دستگاهی جبری، حاصل از جایگشت‌های ریشه‌ها، دست یافتند که بعدها گروه نامیده شد. پاسخ به سؤال بالا در ویژگی‌های این گروه نهفته است. بررسی ویژگی‌های این گروه و چگونگی استفاده از آن در پاسخ به سؤال بالا، در درس نظریه‌ی گالوا مطالعه می‌شود.

۳- اجازه بدهید چند نمادگذاری را یادآوری کنیم که کار نوشتن را کوتاه‌تر و ساده‌تر می‌کنند. از این پس، اگر امکان اشتباه نباشد، بیشتر به جای $x*y$، **نمادگذاری ضربی** xy را به کار می‌بریم و حتی آن را **حاصل‌ضرب** می‌نامیم. البته اگر G آبلی باشد (یعنی، معادله‌ی $xy=yx$ برای هر $x,y\in G$ برقرار باشد)، گاهی از **نمادگذاری** جمعی $x+y$ نیز استفاده می‌کنیم و G را گروهی جمعی می‌نامیم. در این صورت، معمولاً وارون x را قرینه‌ی x می‌نامیم و با $-x$ نشان می‌دهیم و نماد صفر 0 را برای عضو همانی به کار می‌بریم و آن را **عضو خنثی** نیز می‌نامیم. همچنین، به دلیل شرکت‌پذیر بودن عمل دوتایی گروه، اغلب از نوشتن پرانتزها صرف نظر می‌کنیم و برای مثال می‌نویسیم xyz، $xyztu$ و از این قبیل. قبل از ادامه‌ی بحث، خوب است تکلیف نمادگذاری توانی x^n را در نمادگذاری ضربی و جمعی نیز روشن کنیم.

$$x^n=\begin{cases} xx\cdots x & (n>0)\\ e & (n=0)\\ x^{-1}\cdots x^{-1} & (n<0)\end{cases},\qquad nx=\begin{cases} x+\cdots+x & (n>0)\\ 0 & (n=0)\\ -x-x\cdots-x & (n<0)\end{cases}$$

که در آن $x-y=x+(-y)$. با استقرا می‌توانید نشان دهید که برای هر $m,n\in\mathbb{Z}$، در **نمادگذاری ضربی**، داریم $x^mx^n=x^{m+n}$ و $(x^m)^n=x^{mn}$ و در **نمادگذاری جمعی**، $(m+n)x=mx+nx$ و $n(mx)=(nm)x$.

۴- در تعریف گروه $(G;*)$، به طور صریح صحبت از ناتهی بودن مجموعه‌ی G نشده است، ولی شرط وجود عضو همانی e ایجاب می‌کند که G ناتهی باشد. عدد اصلی مجموعه‌ی G را **مرتبه‌ی** گروه $(G;*)$ می‌نامیم و با $|G|$ نشان می‌دهیم. هرگاه $|G|$ متناهی یا نامتناهی باشد، گروه $(G;*)$ را متناهی یا نامتناهی می‌گوییم.

۵- نمونه‌های دستگاه جبری گروه در سراسر علوم ریاضی و علوم دیگر، به ویژه فیزیک و شیمی، بسیارند و چند نمونه را در فصل ۱ دیدیم؛ از جمله، گروه‌های جمعی اعداد $(\mathbb{Z};+)$، $(\mathbb{Q};+)$، $(\mathbb{R};+)$، $(\mathbb{C};+)$، و گروه‌های ضربی اعداد $(\mathbb{Q}^*;\cdot)$، $(\mathbb{R}^*;\cdot)$، $(\mathbb{C}^*;\cdot)$. در زیر چند مثال دیگر می‌آوریم، و به مرور با مثال‌های بیشتری در این درس و درس‌های دیگر آشنا می‌شویم.

(الف) نشان دهید که هر یک از مجموعه‌های اعداد صحیح زوج $E=2\mathbb{Z}=\{2k\mid k\in\mathbb{Z}\}$ و مضارب صحیح عدد طبیعی n، $n\mathbb{Z}=\{nk\mid k\in\mathbb{Z}\}$، همراه با جمع معمولی اعداد، گروه تشکیل می‌دهد. همراه با ضرب اعداد **چطور؟**

(ب) مجموعه‌ی $G_n = \{z \in \mathbb{C} \mid z^n = 1\}$ همراه با عمل ضرب اعداد مختلط گروه است. توجه می‌کنیم که برای $z_1, z_2 \in G_n$ داریم $(z_1 z_2)^n = {z_1}^n {z_2}^n = 1 \cdot 1 = 1$ و در نتیجه G_n نسبت به ضرب اعداد مختلط بسته است. روشن است که عدد $e = 1$ عضو همانی G_n است و به آسانی **می‌توانید نشان دهید** که G_n نسبت به وارون‌ها نیز بسته است. به دلیل روشن، این گروه را **گروه ریشه‌های n-ام واحد** می‌نامیم.

(پ) روشن است که مجموعه‌ی $\mathbb{Q}^+ = \{a \in \mathbb{Q} \mid a > 0\}$ همراه با ضرب معمولی اعداد گویا گروه است. نشان دهید که $\mathbb{Q}^+$ همراه با عمل $*$ با تعریف $a * b = ab/2$ نیز گروه است. عضو همانی آن و وارون هر $a \in \mathbb{Q}^+$ را در این گروه بیابید.

(ت) نشان دهید که هر یک از مجموعه‌های زیر با عمل جمع اعداد مختلط، گروه تشکیل می‌دهد (این نوع گروه‌ها به ویژه در نظریه‌ی اعداد به کار می‌روند):

$$\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$$
$$\mathbb{Q}[i] = \{a + bi \mid a, b \in \mathbb{Q}\}$$

اگر عدد صفر را از $\mathbb{Q}[i]$ برداریم، آنگاه مجموعه‌ی حاصل همراه با ضرب اعداد مختلط گروه تشکیل می‌دهد. وارون هر عضو این گروه را بیابید.

(ث) در بند **(ت)** به جای عدد مختلط $i = \sqrt{-1}$، عددی گنگ، برای مثال، $\sqrt{2}$ یا π را قرار دهید و به همان سؤال پاسخ دهید.

(ج) آیا مجموعه‌ی $G = \{f : \mathbb{R} \to \mathbb{R} \mid (\forall x \in \mathbb{R}) \quad f(x) \neq 0\}$ همراه با ضرب توابع حقیقی، با تعریف $(fg)(x) = f(x)g(x)$، گروه تشکیل می‌دهد؟

(چ) برای هر مجموعه‌ی X، مجموعه‌ی همه‌ی توابع دوسویی روی X (از X به X) با نمادگذاری S_X همراه با ترکیب توابع، گروهی به نام **گروه جایگشت‌ها**، تشکیل می‌دهد. اگر $|X| = n$، گروه S_X را با S_n نشان می‌دهیم و آن را **گروه جایگشت‌های** روی n شیء می‌نامیم. این گروه را، که یکی از اولین مثال‌های گروه بوده است، در بخش **۶.۲** این فصل با جزییات بیش‌تر مطالعه می‌کنیم.

(ح) از مثال‌های مهم دیگر گروه، گروه‌های جمعی همنهشتی $(\mathbb{Z}_n; +_n)$ هستند. همچنین، با استفاده از واقعیت‌های

$$(a, n) = 1 = (b, n) \Rightarrow (ab, n) = 1$$
$$(a, n) = 1 \Rightarrow (\exists x, y \in \mathbb{Z}), \quad ax + ny = 1$$

می‌توانید نشان دهید که در $\{1,2,\cdots,n-1\}$ اعدادی که نسبت به n اول هستند نسبت به ضرب همنهشتی به پیمانه‌ی n گروه تشکیل می‌دهند، که آن را **گروه ضربی همنهشتی** به پیمانه‌ی n می‌نامیم و با C_n نشان می‌دهیم. این گروه‌ها به ویژه در نظریه‌ی اعداد و رمزنگاری کاربرد دارند.

قضیه‌های دیگری نیز معادل با تعریف دستگاه جبری گروه وجود دارند که هر یک سودمندی و کارایی ویژه‌ای دارد. یکی از این قضیه‌ها را در قضیه ۸.۴.۱ در فصل ۱ بدون اثبات آوردیم و کاربرد-هایی از آن را نیز ارائه دادیم. قبل از اثبات این قضیه، قضیه‌ی دیگری معادل با تعریف گروه می-آوریم که اثبات برخی از قضیه‌ها و مثال‌های گروه را اندکی آسان‌تر می‌کند. اثبات آن نیز آموزنده است.

۵.۱.۲ قضیه (تعریف راست). نیمگروه $(G;*)$ گروه است اگر و تنها اگر

(گ۲ر) (وجود عضو همانی راست) $(\exists e_r \in G)\ (\forall x \in G)\ \ xe_r = x$

(گ۳ر) (وجود وارون‌های راست) $(\forall x \in G)\ (\exists x_r \in G)\ \ xx_r = e_r$

اثبات. روشن است که اگر G گروه باشد، آنگاه نیم‌گروهی با شرایط (گ۲ر) و (گ۳ر) است. برای اثبات عکس قضیه، ابتدا نشان می‌دهیم که e_r همانی چپ نیز هست. فرض کنیم $x \in G$ دلخواه، $x_r \in G$ وارون راست x، و $x_{r_r} \in G$ وارون راست x_r باشد. در این صورت، داریم

$$\begin{aligned} xx_r = e_r = e_r e_r &= e_r(xx_r) \\ &= (e_r x)x_r \end{aligned}$$

دو طرف تساوی را از سمت راست در x_{r_r} ضرب (عمل گروه) کنید و نتیجه بگیرید که $x = e_r x$. پس $e = e_r$ همانی دوطرفه است.

حال فرض کنیم x_r وارون راست x و x_{r_r} وارون راست x_r باشد. به آسانی می‌توانید مراحل زیر را کامل کنید:

$$x_r x = (x_r x)e = (x_r x)(x_r x_{r_r}) = \cdots = e$$

در نتیجه، G گروه است.

۶.۱.۲ بحث در کلاس. قضیه‌ی بالا را **تعریف راست گروه** نیز می‌نامند. به همین صورت می‌توان **تعریف چپ گروه** را نیز ارائه داد. البته باید توجه داشته باشیم که اگر نیم‌گروه G دارای عضو همانی **راست** و هر عضو آن دارای وارون **چپ** باشد (یا دارای همانی **چپ** و هر عضو آن دارای وارون **راست** باشد)، لزوماً گروه نیست. برای مثال، مجموعه‌ی $A = \{a,b,c\}$ یکبار همراه با عمل دوتایی $xy = x$ (برای مثال a را به عنوان عضو همانی راست در نظر بگیرید) و

بار دیگر با $xy = y$ که، به ترتیب، در جدول‌های زیر مشخص‌تر شده‌اند، ما را به نتیجه‌ی مورد نظر می‌رساند. **چطور؟**

	a	b	c
a	a	a	a
b	b	b	b
c	c	c	c

(الف)

	a	b	c
a	a	b	c
b	a	b	c
c	a	b	c

(ب)

حال قضیه‌ی جالب **۸.۴.۱** را اثبات می‌کنیم. قبلاً نیز گفتیم که اثبات برخی از قضیه‌ها سرراست، یعنی صرفاً بررسی حقایق هستند. ولی، اثبات برخی دیگر، مانند قضیه‌ی زیر، فنونی را به نمایش می‌گذارند که در اثبات‌های دیگر نیز به کار می‌آیند. اثبات‌ها را صرفاً از بر نکنید، بلکه به نکات آن نیز با دقت توجه کنید. وقت زیادی را از شما نمی‌گیرد! سعی کنید روش‌ها و فنون اثبات‌ها را بیاموزید تا لذت ببرید و همچنین

خودتان سازنده‌ی اثبات‌های دیگر باشید و به اصطلاح ماهی‌گیری بیاموزید!

۷.۱.۲ قضیه. *فرض کنیم* $(G;*)$ *نیمگروهی* ***ناتهی*** *باشد. در این صورت،* G *گروه است اگر و تنها اگر به ازای هر* $a,b \in G$*، هر یک از معادله‌های خطی* $ax = b$ *و* $ya = b$ *در* G ***حل‌پذیر*** *باشد.*

اثبات. یک طرف حکم به راحتی اثبات می‌شود. فرض کنیم G گروه است. به راحتی می‌توانید، با استفاده از هر سه ویژگی **(گ۱)** – **(گ۳)** تعریف گروه، با جایگذاری نشان دهید که $x = a^{-1}b$ جواب معادله‌ی اول است (**نشان دهید**). جواب معادله‌ی دوم چیست؟

برعکس، فرض کنیم برای هر $a,b \in G$، معادله‌های $ax = b$ و $ya = b$ در G حل‌پذیر باشند. چون G **ناتهی** است، عضوی چون $a \in G$ وجود دارد (فرض ناتهی بودن در اینجا استفاده شد.) حال، چون معادله‌ی $ax = a$ در G حل‌پذیر است، پس $e_r \in G$ وجود دارد به طوری که $ae_r = a$ (**هشدار:** برخی از دانشجویان به نادرست از همین مطلب نتیجه‌ای زودرس می‌گیرند که e_r عضو همانی راست G است). در حالی که این مطلب هنوز اثبات نمی‌کند که برای **هر عضو دلخواه** $g \in G$، داریم $ge_r = g$! ولی، فرض کنیم $g \in G$ دلخواه باشد. در این صورت، چون معادله‌ی $ya = g$ در G حل‌پذیر است، عضو $g' \in G$ وجود دارد به طوری که $g'a = g$. حال، با توجه به شرکت‌پذیری * و داشته‌هایمان، نتیجه می‌گیریم که

$$ge_r = (g'a)e_r = g'(ae_r) = g'a = g$$

یعنی e_r به واقع همانی راست در G است! تا اینجای اثبات **جالب بود، نبود؟!**

هنوز اثبات تمام نشده است! باید برای هر $g \in G$، وارونی راست در G بیابیم، و سپس از قضیه‌ی ۵.۱.۲ استفاده کنیم! این قسمت ساده‌تر است. از حل‌پذیری $gx = e$ ، عضو $g_r \in G$ به دست می‌آید به طوری‌که $gg_r = e$، یعنی g_r وارون راست g است. حال، قضیه‌ی ۵.۱.۲ را به کار ببرید.

۸.۱.۲ بحث در کلاس. یادآوری بندهایی از بحث ۹.۴.۱ از فصل ۱ مفید است.

۱- به راحتی می‌توانید نشان دهید که در گروه G، جواب هر یک از معادله‌های $ax = b$ و $ya = b$ یکتاست.

۲- فرض کنیم a و b عضو گروه (متناهی) G باشند. در این صورت، وجود و یکتایی جواب معادله‌ی $ax = b$ ایجاب می‌کند که در جدول کیلی گروه G، هر عضو $b \in G$ دقیقاً یک‌بار در سطر مربوط به a ظاهر شود! به همین ترتیب، وجود و یکتایی جواب معادله‌ی $ya = b$ نشان می‌دهد که هر عضو $b \in G$ دقیقاً یک‌بار در ستون مربوط به a ظاهر می‌شود! در انتهای بحث ۹.۴.۱ گفتیم که **اساساً** (یعنی، تا حد یک‌ریختی) تنها یک دسته گروه از هر مرتبه‌ی ۱، ۲، و ۳ عضوی وجود دارد، که $\mathbb{Z}_1 = \{0\}$، $\mathbb{Z}_2 = \{0,1\}$، $\mathbb{Z}_3 = \{0,1,2\}$ با جدول‌های زیر نماینده‌های آن دسته‌ها هستند:

$+_1$	0
0	0

$+_2$	0	1
0	0	1
1	1	0

$+_3$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

۳- حال ببینیم در حالت گروه ۴ عضوی چه اتفاق می‌افتد. فرض کنیم $G = \{e, a, b, c\}$. اگر e را به عنوان عضو همانی در نظر بگیریم، ابتدا جدول ناقص زیر را داریم:

	e	a	b	c
e	e	a	b	c
a	a	?	–	–
b	b	–	–	–
c	c	–	–	–

با توجه به مطالب بند ۲ بالا حدس می‌زنید چه عضوهایی باید در محل علامت سؤال بنویسیم؟ درست است، در سطر درونی جدول عضو a آمده است، پس هر یک از سه عضو دیگر G یعنی، e، b، و c را می‌توان انتخاب کرد. از این رو، جدول بالا را می‌توان به هر یک از سه جدول زیر گسترش داد (توضیح دهید که همین سطر و ستون را در این جدول‌ها چطور کامل کردیم):

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

(۳)

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

(۲)

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

(۱)

روشن است که جدول‌های (۱) و (۲) تنها به یک صورت ولی جدول (۳) به دو صورت (۳) و (۴) زیر کامل می‌شوند. **چطور؟**

(2)

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

(1)

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

(4)

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

(3)

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

۴- آیا بند ۳ بالا به این معنی است که اساساً (تا حد یک‌ریختی) چهار نوع گروه چهار عضوی وجود دارند؟ همان طور که در فصل ۱ نیز بیان شد، بررسی شرکت‌پذیری عمل‌هایی که با جدول کیلی داده می‌شوند کار پر زحمتی است. گاهی می‌توانیم با تبدیل جدول کیلی داده شده به جدول عملی که شرکت پذیری آن را می‌دانیم به این مقصود دست یابیم. برای مثال، اگر روش بند ۲ بحث ۱۲.۳.۱ را به کار ببریم به نتایج زیر می‌رسیم. تابع دوسویی تغییر نام h با تعریف

x	e	a	b	c
$h(x)$	$\circ$	1	2	3

جدول (۱) بالا را به جدول گروه $(\mathbb{Z}_4;+_4)$ که در زیر آمده است، تبدیل می‌کند:

$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

این مطلب نه تنها نشان می‌دهد که جدول کیلی (۱) شرکت پذیر است (زیرا جدول عمل همنهشتی به پیمانه‌ی n شرکت‌پذیر است) بلکه نشان می‌دهد که گروه چهار عضوی $\{e,a,b,c\}$ همراه با عملی که با جدول کیلی (۱) داده شده است با گروه همنهشتی $(\mathbb{Z}_4;+_4)$ اساساً یکسان (یعنی **یک‌ریخت**) است. به همین صورت، می‌توانید جدول‌های (۲) و (۴) را نیز به جدول $\mathbb{Z}_4$ تبدیل کنید! در نتیجه، جدول‌های (۱)، (۲)، و (۴) اساساً معرف گروه $\mathbb{Z}_4$ هستند. توجه می‌کنیم که با هیچ یک از ۲۴ = !۴ تابع دوسویی از مجموعه‌ی $\{e,a,b,c\}$ به $\{0,1,2,3\}$ نمی‌توان جدول(۳) را به جدول گروه $\mathbb{Z}_4$ تبدیل کرد. گروه متناظر با جدول (۳) را **چهار-گروه کلاین** (یا **گروه چارینه‌ی کلاین**) می‌نامیم و آن را با V **یا** K_4 نشان می‌دهیم. این گروه در هندسه نیز کاربرد دارد. یک‌بار دیگر جدول آن را مرور کنید زیرا چند بار دیگر به آن رجوع خواهیم داد. مشاهده می‌کنیم که $a^2=b^2=c^2=e^2=e$. همچنین، $ab=c=ba$ ،$bc=a=cb$ ،$ca=b=ac$.

۹.۱.۲ قوانین حذف. قبل از پایان دادن به این بخش، قضیه‌ی معادل دیگری را صرفاً برای تعریف گروه **متناهی** می‌آوریم. به آسانی می‌توانید، با استفاده از وجود وارون، شرکت‌پذیری، و ویژگی عضو همانی، نشان دهید که **قوانین حذف** (چپ و راست) در هر گروه برقرار هستند. یعنی، نشان دهید که شبه‌معادله‌ی (**استلزامی**) زیر در هر گروه برقرار است:

$$ax=ay \quad \vee \quad xa=ya \quad \Rightarrow x=y$$

آیا اگر در نیم‌گروهی ناتهی یا در تکواره‌ی $(M;*,e)$ قوانین حذف برقرار باشند، M باید گروه باشد؟ مثالی بیاورید که پاسخی منفی به این سوال می‌دهد. قضیه‌ی زیر برای نیم‌گروه‌های متناهی بسیار جالب است. روش اثبات فنی و نه چندان سرراست آن را به خاطر بسپارید؛ همتای این روش اثبات را در فصل ۳ نیز خواهیم دید.

۱۰.۱.۲ قضیه. هر نیم‌گروه **متناهی** و ناتهی که قوانین حذف در آن برقرار باشند، لزوماً گروه است.

اثبات. فرض کنیم $G=\{a_1,\cdots,a_n\}$. عضوهای زیر را در نظر بگیرید:

$$a_1a_1, a_2a_1,\cdots,a_na_1\in G$$

ادعا می‌کنیم که این عضوها متمایز هستند؛ زیرا، بنابر قانون حذف راست در G، داریم

$$a_ia_1=a_ja_1\Rightarrow a_i=a_j$$

از این رو، تعداد این عضوها برابر با $|G|=n$ است و بنابراین،

$$G=\{a_1a_1, a_2a_1,\cdots,a_na_1\}$$

چون $a_1\in G=\{a_1a_1, a_2a_1,\cdots,a_na_1\}$، پس عضو $a_k\in G$ وجود دارد به طوری که $a_1=a_ka_1$. (توجه کنید که این مطلب هنوز نشان نمی‌دهد که a_k همانی چپ G است). حال فرض کنیم $a_i\in G$ دلخواه باشد. در این صورت،

$$a_ia_1=a_i(a_ka_1)=(a_ia_k)a_1$$

و در نتیجه، بنابر قانون حذف راست، $a_i=a_ia_k$. یعنی، $a_k=e_r$ همانی راست G است.

حال، فرض کنیم $a_i\in G$ عضوی دلخواه باشد. به روشی مشابه بالا و با استفاده از قانون حذف راست، نشان دهید که

$$G=\{a_ia_1, a_ia_2\cdots,a_ia_n\}$$

چون $e_r\in G=\{a_ia_1, a_ia_2\cdots,a_ia_n\}$، عضوی مانند $a_j\in G$ وجود دارد به طوری که $e_r=a_ia_j$. یعنی، a_i وارون راست دارد. از این رو، بنابر قضیه‌ی **۵.۱.۲**، G گروه است. **جالب بود؟**

۱۱.۱.۲ بحث در کلاس. اگر چه تعریف‌های معادل **۱.۱.۲**، **۵.۱.۲**، **۷.۱.۲** برای گروه برحسب برقراری معادله‌ها یعنی اتحادها داده نشده است، و تعریف مذکور در قضیه‌ی **۱۰.۱.۲** برای گروه متناهی برحسب شبه‌اتحاد (گزاره‌ی استلزامی) داده شده است، تعریف جالب **۳.۱.۲** کاملاً بر حسب **اتحادها** است. این مطلب نشان می‌دهد که کلاس گروه‌ها، با توجه به مطالب بخش **۹.۱**، دارای همه‌ی مزایای کلاس‌های معادله‌ای است.

تمرین ۱.۲

هوشم نه چنان است تلاشم آنچنان است

دسته‌ی اول

۱- با استقرا، اثبات کنید که برای هر $m,n\in\mathbb{Z}$، اتحادهای $x^m x^n = x^{m+n}$ $(x^m)^n = x^{mn}$ در هر گروه برقرار هستند.

۲- نشان دهید که عضو همانی گروه $(\mathbb{Q}^+;*)$ که در آن $a*b = ab/2$ عدد گویای ۲، و وارون هر $a\in\mathbb{Q}^+$ برابر با $4/a$ است.

۳- وارون $a+bi\neq 0$ را در گروه ضربی $\mathbb{Q}^*[i]=\mathbb{Q}[i]\setminus\{0\}$ به‌دست آورید؟

۴- نشان دهید که جدول‌های زیر نمی‌توانند جدول کیلی عمل یک گروه روی مجموعه‌ی داده شده باشند:

	a	b
a	a	a
b	a	a

	a	b
a	a	b
b	b	b

	a	b	c
a	a	b	c
b	b	b	c
c	c	b	c

۵- جدول کیلی گروه ضربی $(C_7;\cdot_7)$ را بنویسید.

۶- بزرگ‌ترین زیرمجموعه‌ای از $\mathbb{Z}_8$ را بیابید که همراه با ضرب همنهشتی $\cdot_8$ گروه تشکیل دهد. جدول کیلی عمل آن را بنویسید.

۷- **(الف)** چطور با نگاهی به جدول‌های کیلی گروه‌های $\mathbb{Z}_4$ و K_4، متوجه می‌شویم که هر دو آبلی هستند؟

(ب) همچنین، نشان دهید که معادله‌ی **درجه‌ی دوم** $x^2=e$ در K_4 دارای **چهار** جواب است در حالی که $\mathbb{Z}_4$ دارای این ویژگی نیست. (تفاوت جبری دیگر این دو گروه را بعداً خواهیم دید.)

۸- **(الف)** نشان دهید که برای هر x و هر y در گروه G، داریم

$$xy = yx \Leftrightarrow (xy)^2 = x^2y^2$$

(**هشدار** می‌دهیم که مبتدیان گاهی به اشتباه اتحاد $(xy)^2=x^2y^2$ را در هر گروه، آبلی یا غیر آبلی، به کار می‌برند. شاید به این دلیل باشد که هنوز با گروه‌های ناآبلی سروکار نداشته‌اند).

(ب) نشان دهید که برای هر x و هر y در گروه G، داریم

$$xy = yx \Leftrightarrow (xy)^{-1} = x^{-1}y^{-1}$$

۹- نشان دهید که مجموعه‌ی $G = \mathbb{R} \times \mathbb{R}$ همراه با عمل مولفه‌ای زیر، گروه است:

$$(a,b)*(c,d) = (a+c, b+d)$$

۱۰- (یک تعمیم تمرین بالا) نشان دهید که $G \times G$ همراه با عمل زیر، گروه است:

$$(a,b)*'(c,d) = (a*c, b*d)$$

۱۱- تمرین ۱۰ را به دو گروه دلخواه $(G_1;*_1)$ و $(G_2;*_2)$ تعمیم دهید. یعنی، نشان دهید که $G = G_1 \times G_2$ همراه با عمل دوتایی زیر، گروه است:

$$(a,b)*(c,d) = (a*_1 c, b*_2 d)$$

۱۲- با استفاده از قوانین حذف، نشان دهید که تنها عضو خودتوان (یعنی عضوی چون x که $x^2 = xx = x$) در هر گروه، عضو همانی آن است.

دسته‌ی دوم

۱۳- (الف) نشان دهید که اگر هر عضو گروه G وارون خودش باشد، یعنی،

$$(\forall x \in G) \quad x^2 = e$$

آنگاه G آبلی است ($(ab)^2$ را محاسبه کنید) . آیا عکس این مطلب درست است؟

(ب) فرض کنید که دو عدد طبیعی متباین m و n وجود دارند به طوری که برای هر a و b در گروه G داریم

$$a^m b^m = b^m a^m \quad , \quad a^n b^n = b^n a^n$$

نشان دهید که G آبلی است.

(پ) فرض کنید که در گروه G، برای سه عدد متوالی k داریم

$$(\forall a,b \in G) \quad (ab)^k = a^k b^k$$

ثابت کنید که گروه G آبلی است.

۱۴- فرض کنید G گروه است. نشان دهید که هر یک از **انتقال**های راست و چپ

$$r_a : G \to G \qquad l_a : G \to G$$
$$x \mapsto xa \qquad x \mapsto ax$$

دوسویی هستند.

۱۵- (بعداً این تمرین را به کار خواهیم برد) فرض کنید G گروه است. نشان دهید که هر دو مجموعه‌ی زیر همراه با ترکیب توابع گروه تشکیل می‌دهند:

$$G_r = \{r_a \mid a \in G\} \quad , \quad G_l = \{l_a \mid a \in G\}$$

۱۶- جدول‌های کیلی گروه‌های G_r و G_l را برای گروه $G = \mathbb{Z}_4$ بنویسید و آن‌ها را با جدول گروه $\mathbb{Z}_4$ مقایسه کنید.

۱۷- نشان دهید که هر نیم‌گروه ناتهی **متناهی** دارای عضوی خودتوان است.

۱۸- فرض کنید که G تکواره‌ای **متناهی** است. نشان دهید که G گروه است اگر و تنها اگر دارای یک عضو خودتوان منحصر به فرد باشد.

۱۹- ثابت کنید که مجموعه‌ی $G = \mathbb{R} \times \mathbb{R}^* = \{(a,b) \mid a,b \in \mathbb{R}, a \neq 0\}$ همراه با عمل $(a,b)*(c,d) = (ac, bc+d)$ گروهی ناآبلی است.

۲۰- فرض کنید G گروهی با عضو همانی e باشد که در آن برای هر عدد صحیح n و هر $a,b \in G$، $(ab)^n = a^n b^n$. ثابت کنید که برای هر $a,b \in G$،

$$(aba^{-1}b^{-1})^{n(n-1)} = e$$

۲.۲ زیرگروه

در بخش ۶.۱ مفهوم کلی زیردستگاه جبری و P - زیرجبر را معرفی کردیم. در این بخش، این مفاهیم را برای گروه‌ها با جزییات بیشتری مورد بررسی قرار می‌دهیم. تعریف ۳.۶.۱ را یادآوری می‌کنیم، که بیان می‌کند دستگاه جبری B زیردستگاه جبری A، هر دو از نوع τ (بدون در نظر

گرفتن ویژگی‌های آن‌ها)، است اگر $B \subseteq A$ و هر عمل B تحدید عمل همتایش در A باشد. حال تعریف زیر را می‌آوریم.

۱.۲.۲ تعریف. می‌گوییم که گروهواره‌ی $(B;*^B)$ زیرگروهواره‌ای از گروهواره‌ی $(A;*^A)$ است اگر دو شرط زیر برقرار باشند:

۱- $B \subseteq A$، و

۲- عمل دوتایی $*^B$ تحدید عمل دوتایی $*^A$ باشد. یعنی،

$$(\forall x, y \in B) \quad x *^B y = x *^A y$$

۲.۲.۲ بحث در کلاس

۱- اگر چه نباید مجموعه را با دستگاه جبری مقایسه کرد، ولی غلطی متداول (و بی ضرر) است که اغلب می‌گوییم که "زیرمجموعه‌ی B از گروهواره‌ی $(A;*)$ زیرگروهواره‌ی $(A;*)$ است اگر B نسبت به عمل $*$ بسته باشد". منظور این است که اگر مجموعه‌ی B نسبت به عمل $*$ بسته باشد، آنگاه B همراه با تحدید تابع $*$ بر آن، گروهواره‌ای تشکیل می‌دهد که آن را زیرگروهواره‌ی A می‌نامیم!

همچنین، وقتی گروهواره‌ی $(B;*^B)$ زیرگروهواره‌ی $(A;*^A)$ است، متداول است که هر دو عمل را با نماد ساده‌ی $*$ نشان دهیم، و البته بنابر قرارداد قبلی، اگر امکان اشتباه نباشد، به جای $x * y$ به طور ساده می‌نویسیم xy.

۲- آیا گروهواره‌ی $H = (\{0,1,2\}, +_3)$ زیرگروهواره‌ی $\mathbb{Z}_4 = (\{0,1,2,3\}, +_4)$ است؟ برای پاسخ منفی خود دلیل بیاورید!

۳- آیا گروهواره‌ی $H = (\{0,2\}; +_4)$ زیرگروهواره‌ی $\mathbb{Z}_4 = (\{0,1,2,3\}, +_4)$ است؟ برای پاسخ مثبت خود دلیل بیاورید!

۴- یادآوری می‌کنیم که دستگاه جبری گروهواره لزوماً دارای هیچ ویژگی‌ای بجز وجود عمل دوتایی‌اش نیست. ولی، دستگاه جبری مورد نظر ما در این فصل، یعنی گروه، با سه ویژگی شرکت-پذیری، وجود عضو همانی، و وجود وارون‌ها مشخص می‌شود. پس باید تعریف ۶.۶.۱ ، یعنی P - زیرجبر، را برای مفهوم زیرگروه تعبیر کنیم. پیشنهاد می‌کنیم که بحث‌های ۷.۶.۱ و ۸.۶.۱ را مرور کنید.

۳.۲.۲ تعریف. فرض کنیم گروهواره‌ی $(G;*_G)$ گروه باشد (یعنی در شرط‌های (گ۱)، (گ۲)، و (گ۳) تعریف ۱.۱.۲ صدق کند.) می‌گوییم که گروهواره‌ی $(H;*_H)$ **زیرگروه** $(G;*_G)$ است، و می‌نویسیم $H \leq G$، اگر شرایط زیر برقرار باشند:

۱- H زیرگروهواره‌ی G باشد. یعنی، $H \subseteq G$ و $*_H$ تحدید عمل $*_G$ باشد.

۲- این زیرگروهواره، خودش گروه باشد. یعنی، H همراه با عمل $*_H$ (که تحدید $*_G$ بر H است) دارای شرط‌های (گ۱)- (گ۳) تعریف ۱.۱.۲ باشد.

۴.۲.۲ بحث در کلاس. نکته‌هایی در این تعریف پنهان است که مبتدیان ممکن است به آن توجه نکنند. بیان این موارد برای مطالعه‌ی دستگاه‌های جبری دیگر نیز مفید است. می‌دانیم که بنابر شرط (گ۲)، گروه G دارای عضو همانی، به نمایش e_G، است و همچنین، بنابر (گ۳)، هر عضو $x \in G$ وارونی، مثلاً به نمایش x_G^{-1}، در G دارد. و شرط ۲ بالا بیان می‌کند که H نیز دارای شرایط (گ۲) و (گ۳) است و در نتیجه باید **برای خودش** دارای عضو همانی، به نمایش e_H، باشد و هر عضو $h \in H$ وارونی، مثلاً به نمایش h_H^{-1}، در H داشته باشد! حال حتماً این سؤال‌ها برایتان مطرح می‌شود که (الف) آیا به خودی خود $e_H = e_G$ و $h_H^{-1} = h_G^{-1}$، یا باید این شرایط را نیز در تعریف زیرگروه می‌گنجاندیم؟ اگر چه پاسخ‌های به این سؤال‌ها در همه‌ی دستگاه‌های جبری لزوماً مثبت نیستند (برای مثال، بند ۱ بحث ۸.۶.۱ را در مورد تکواره ببینید)، ولی در قضیه‌ی ۵.۲.۲ خواهیم دید که تلفیق شرط‌های (گ۱)- (گ۳) گروه بسیار توانمند است و خوشبختانه پاسخ به هر دو سؤال برای **گروه‌ها** مثبت است.

۵.۲.۲ قضیه. فرض کنیم گروهواره‌ی $(H;*_H)$ زیرگروهی از گروه $(G;*_G)$ باشد. در این صورت،

(الف) $e_H = e_G$؛

(ب) برای هر $h \in H$، $h_H^{-1} = h_G^{-1}$.

اثبات (الف). در گروه H داریم $e_H e_H = e_H$. از طرفی، در گروه G داریم $e_H e_H = e_H = e_H e_G$. حال، قانون حذف چپ (۹.۱.۲) را در گروه G به کار ببرید و نتیجه بگیرید که $e_H = e_G$.

(ب) چون $xx_H^{-1} = x_H^{-1}x = e_H = e_G$، پس x_H^{-1} وارون x در G است. به دلیل یکتایی وارون در گروه‌ها، $x_H^{-1} = x_G^{-1}$.

اثبات قضیه‌ی زیر نیز راحت است.

۶.۲.۲ قضیه (محک زیرگروه). فرض کنیم G گروه و H زیرمجموعه‌ی G باشد به طوری که:

(الف) H نسبت به عمل گروه G بسته باشد؛

(ب) $e \in H$؛

(پ) برای هر $h \in H$، $h^{-1} \in H$.

در این صورت، H همراه با (تحدید) عمل G بر آن (حاصل از بند (**الف**)) زیرگروهی از G تشکیل می‌دهد.

قضیه‌ی زیر کار بررسی زیرگروه بودن را اندکی (فقط اندکی) کوتاه‌تر از محک بالا می‌کند.

۷.۲.۲ قضیه. زیرمجموعه‌ی **ناتهی** H از گروه G (همراه با تحدید عمل G بر آن) زیرگروه G است اگر و تنها اگر برای هر $x, y \in H$، $xy^{-1} \in H$. (و در نمادگذاری جمعی، $x - y = x + (-y) \in H$)

اثبات. یک طرف حکم به راحتی اثبات می‌شود. فرض کنیم H زیرگروه G باشد. برای هر $x, y \in H$، چون $y^{-1} \in H$ و H نسبت به عمل گروه G بسته است، پس $xy^{-1} \in H$.

برای اثبات عکس حکم قضیه، فرض می‌کنیم $a, b \in H$ دلخواه باشند. کافی است $x = a$ و $y = b^{-1}$ را در $xy^{-1} \in H$ قرار دهیم و نتیجه بگیریم که $a(b^{-1})^{-1} = ab \in H$. برای اثبات $e \in H$، فرض کنید $h \in H \neq \varnothing$ و در $xy^{-1} \in H$ قرار دهید $x = y = h$، و سرانجام، با قرار دادن $x = e$ و $y = h$ در $xy^{-1} \in H$ نتیجه بگیرید که $h^{-1} \in H$.

بسیاری مواقع لازم است که زیرگروه بودن زیرمجموعه‌ی **متناهی** H از گروه G را بررسی کنیم. در این موارد قضیه‌ی ساده‌تر و جالب زیر بسیار مفید است. برای اثبات آن، قضیه‌ی **۱۰.۱.۲** را به کار ببرید.

۸.۲.۲ قضیه. فرض کنیم H زیرمجموعه‌ای **متناهی** و ناتهی از گروه G باشد. در این صورت، H (همراه با تحدید عمل G بر آن) زیرگروه G است اگر و تنها اگر H نسبت به عمل دوتایی G بسته (یعنی، صرفاً زیرگروهواره) باشد.

۹.۲.۲ بحث در کلاس. چندان ساده نیست که همه‌ی زیرگروه‌های یک گروه را بیابیم. به مرور مطالب مفیدی را با استفاده از قضیه‌های بالا در این رابطه می‌آوریم که این کار را ساده‌تر می‌کند.

۱- روشن است که اگر e عضو همانی گروه G باشد، آنگاه $\{e\}$ و G زیرگروه G هستند. این زیرگروه‌ها را **زیرگروه‌های بدیهی** می‌نامیم. البته، شاید بهتر باشد $\{e\}$ را زیرگروه بدیهی و G را زیرگروه ناسره بنامیم.

۲- اگر $\mathbb{Z}_2 = (\{0,1\};+_2)$ آنگاه $\{0\}$ و $\mathbb{Z}_2$ تنها زیرگروه‌های $\mathbb{Z}_2$ هستند.

۳- اگر $\mathbb{Z}_3 = (\{0,1,2\};+_3)$ آنگاه در این مورد نیز $\{0\}$ و $\mathbb{Z}_3$ تنها زیرگروه‌های $\mathbb{Z}_3$ هستند! زیرا هر زیرگروه H از G باید شامل عضو همانی (خنثی) 0 باشد. حال اگر $1 \in H$ آنگاه، بنابر قضیه‌ی ۸.۲.۲، H باید شامل $1+_3 1 = 2$ نیز باشد، که در این صورت $H = G$. اگر $2 \in H$، آنگاه $2 +_3 2 = 1 \in H$.

۴- آیا گروه $\mathbb{Z}_4 = (\{0,1,2,3\};+_4)$ زیرگروهی چون H متفاوت با $\{0\}$ و $\mathbb{Z}_4$ دارد؟ مشابه بند۳، فرض می‌کنیم $1 \in H$. در این صورت، $1+_4 1 = 2, 1+_4 2 = 3 \in H$ و در نتیجه $H = G$. هنوز کار تمام نشده است! فرض کنیم $0,2 \in H$. چون $2+_4 2 = 0$، پس $H = \{0,2\}$ نسبت به عمل $+_4$ بسته است. حال، بنابر قضیه‌ی ۸.۲.۲، $H = \{0,2\}$ زیرگروه $\mathbb{Z}_4$ است. به همین روش‌ها نشان دهید که $\mathbb{Z}_4$ زیرگروه دیگری بجز $\{0\}$، $H = \{0,2\}$ و $\mathbb{Z}_4$ ندارد.

۵- حال گروه کلاین K_4 را با جدول عمل

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

در نظر بگیرید. آیا علاوه بر $\{e\}$ و K_4، زیرگروه دیگری وجود دارد؟ با توجه به قضیه‌ی ۸.۲.۲، $\{e,a\}$، $\{e,b\}$، و $\{e,c\}$ نیز زیرگروه هستند و هیچ زیرگروه دیگری وجود ندارد. زیرا، برای مثال $\{e,a,b\}$ نسبت به عمل K_4 بسته نیست.

۶- حال ببینیم آیا با اطلاعاتی که تاکنون داریم می‌توانیم زیرگروه‌های گروه نامتناهی $(\mathbb{Z};+)$ را تعیین کنیم؟ این گروه هیچ زیرگروه **متناهی** بجز $\{0\}$ ندارد! زیرا اگر H زیرگروه آن باشد و $0 \neq n \in H$ آنگاه، چون H باید نسبت به جمع بسته باشد، پس برای هر k، باید $kn = n+n+\cdots+n \in H$. این مطلب نشان می‌دهد که H نامتناهی است. به آسانی می-

توانید با بررسی شرایط قضیه‌ی ۶.۲.۲ نشان دهید که برای هر عدد صحیح n، مجموعه‌ی مضارب صحیح n، یعنی

$$n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\} = \{\cdots, -2n, -n, \circ, n, 2n, \cdots\}$$

زیرگروه $(\mathbb{Z}; +)$ است. توجه می‌کنیم که، $0\mathbb{Z} = \{0\}$، $1\mathbb{Z} = \mathbb{Z}$، و $-n\mathbb{Z} = n\mathbb{Z}$. خواهیم دید که $\mathbb{Z}$ زیرگروه دیگری ندارد! البته، اثبات این مطلب قدری فنی است که بعداً (در نتیجه ۱۳.۴.۲) ارائه خواهیم کرد.

۱۰.۲.۲ قضیه‌ی لاگرانژ. قضیه‌ای بسیار مهم، به نام قضیه‌ی لاگرانژ، بیان می‌کند که اگر H زیرگروهی از یک گروه **متناهی** G باشد، آنگاه مرتبه‌ی H، یعنی $|H|$، باید مرتبه‌ی G، یعنی $|G|$، را بشمارد. برای مثال، $\mathbb{Z}_4$ و K_4 زیرگروهی با ۳ عضو نمی‌توانند داشته باشند، $\mathbb{Z}_{15}$ تنها **ممکن** است زیرگروه‌هایی ۱، ۳، ۵، و ۱۵ عضوی داشته باشد! اثبات این **قضیه‌ی مهم**، بسیار راحت ولی فنی و جالب است، و ابزار لازم برای اثبات آن کاربردهای دیگری نیز در بخش ۸.۲، مربوط به خارج قسمت گروه‌ها، دارد. حال روش کار را با هم می‌بینیم. رابطه‌ای هم‌ارزی روی مجموعه‌ی G تعریف می‌کنیم به طوری که افراز حاصل از آن نه تنها قضیه‌ی لاگرانژ را اثبات می‌کند، بلکه در بخش مهم ۸.۲ نیز به کار می‌رود. فرض کنیم H زیرگروه G باشد.

۱- به آسانی می‌توانید نشان دهید که رابطه‌ی $\sim_H$ با تعریف

$$a \sim_H b \iff (\exists h \in H)\ a = bh \iff b^{-1}a \in H$$

رابطه‌ای هم‌ارزی است. برای مثال، مراحل زیر را برای اثبات متعدی بودن $\sim_H$ توضیح دهید:

$$a \sim_H b \sim_H c \Rightarrow (\exists h_1, h_2 \in H)\ \ a = bh_1 \ \&\ b = ch_2$$
$$\Rightarrow a = bh_1 = ch_2h_1 \Rightarrow a \sim_H c$$

۲- رده‌های این رابطه‌ی هم‌ارزی ویژگی‌های **بسیار بسیار** جالب توجهی به صورت زیر دارند، که برای دستگاه‌های جبری دیگر (برای مثال، نیم‌گروه و تکواره) لزوماً درست نیستند.

(الف) ابتدا توجه می‌کنیم که، به اصطلاح، H سازنده‌ی همه‌ی رده‌هاست. به این معنی که

$$\begin{aligned}[a] &= \{x \in G \mid x \sim_H a\} \\ &= \{x \in G \mid (\exists h \in H)\ \ x = ah\} \\ &= \{ah \mid h \in H\} \\ &= aH\end{aligned}$$

نمایش $\{ah \mid h \in H\}$ با نماد aH طبیعی است، **این طور نیست؟** توجه می‌کنیم که زیرگروه H از گروه G نیز یکی از رده‌ها است، زیرا $[e] = eH = H$، و البته هیچ رده‌ی دیگری زیرگروه نیست. **چرا؟**

(ب) از آنجا که، مانند هر رابطه‌ی هم‌ارزی، $[a] = [b]$ اگر و تنها اگر $a \sim_H b$، به روشنی داریم

$$aH = bH \Leftrightarrow a \sim_H b \Leftrightarrow (\exists h \in H)\, a = bh \Leftrightarrow b^{-1}a \in H$$

(پ) هر مجموعه‌ی $aH = \{ah \mid h \in H\}$ (یا در نمادگذاری جمعی $a + H = \{a + h \mid h \in H\}$) را، که انتقال چپ اعضای H به اندازه‌ی a است، یک **هم‌مجموعه (یا هم‌رده)ی چپ** H می‌گوییم. بنابراین، افراز $G / \sim_H$، که **برای سادگی** آن را با L_H نشان می‌دهیم، عبارت است از $L_H = \{aH \mid a \in G\}$.

(ت) ویژگی بسیار مهم هم‌مجموعه‌های چپ این است که (چه متناهی باشند یا نامتناهی) تعداد عضوهای یکسان دارند. در واقع، برای هر $a \in G$، $|aH| = |H|$. زیرا، به آسانی **می‌توانید** نشان دهید که تابع زیر دوسویی (یک به یک و پوشا) است:

$$f : H \to aH$$
$$h \mapsto ah$$

حال آماده‌ایم که قضیه‌ی لاگرانژ را به راحتی اثبات کنیم.

۱۱.۲.۲ قضیه(ی لاگرانژ). فرض کنیم H زیرگروهی از گروه متناهی G باشد. در این صورت، مرتبه‌ی H مرتبه‌ی G را می‌شمارد، یعنی $|G| = k|H|$.

اثبات. دیدیم که مجموعه‌ی $L_H = \{aH \mid a \in G\}$ مجموعه‌ی G را افراز می‌کند. از این رو، اجتماع مجزای $G = \bigcup_{a \in G} aH$ را داریم. بنابراین، چون گروه G **متناهی** است، و در نتیجه L_H مجموعه‌ای متناهی، برای مثال k عضوی است. فرض می‌کنیم $L_H = \{a_1H, \cdots, a_kH\}$. پس

$$|G| = |a_1H| + \cdots + |a_kH| = |H| + \cdots + |H|$$
$$= k|H|$$

بنابراین قضیه‌ی مهم لاگرانژ به صورتی جالب اثبات شد.

۱۲.۲.۲ بحث در کلاس

۱- به آسانی می‌توانید نشان دهید که رابطه‌ی $\sim_H$ با تعریف

$$a \sim_H b \quad \Leftrightarrow \quad (\exists h \in H)\, a = hb \quad \Leftrightarrow \quad ab^{-1} \in H$$

نیز رابطه‌ای هم‌ارزی است و $[a] = Ha$، $[e] = He = H$، $|Ha| = |H|$، و

$$Ha = Hb \Leftrightarrow a \sim_H b \Leftrightarrow (\exists h \in H) \quad a = hb \Leftrightarrow ab^{-1} \in H$$

۲- هر Ha را یک **هم‌مجموعه‌ی راست** H در G می‌نامیم. اگر $R_H = \{Hb \mid b \in G\}$ آنگاه، به راحتی می‌توان نشان داد که تابع زیر دوسویی است :

$$f : L_H \to R_H$$
$$aH \mapsto Ha^{-1}$$

خوش‌تعریفی و یک به یک بودن f به صورت زیر اثبات می‌شود (مراحل آن را توضیح دهید):

$$\begin{aligned} aH = bH &\Leftrightarrow b^{-1}a \in H \Leftrightarrow (b^{-1}a)^{-1} \in H \\ &\Leftrightarrow a^{-1}b \in H \Leftrightarrow (a^{-1})(b^{-1})^{-1} \in H \\ &\Leftrightarrow Ha^{-1} = Hb^{-1} \end{aligned}$$

پوشا بودن f روشن است (این طور نیست؟) در نتیجه، $|L_H| = |R_H|$.

۳- توجه می‌کنیم که تساوی‌های $|aH| = |H| = |Ha|$ و $|L_H| = |R_H|$ به متناهی یا نامتناهی بودن این عددها بستگی ندارند. عدد $|L_H| = |R_H|$ را، چه متناهی باشد یا نامتناهی، **اندیس** H در G می‌نامیم و آن را با نماد $[G:H]$ یا $(G:H)$ نشان می‌دهیم. البته، با توجه به اثبات قضیه‌ی لاگرانژ، برای گروه‌های متناهی داریم $[G:H] = |G| / |H|$.

۱۳.۲.۲ قضیه. فرض کنیم G گروهی دلخواه (متناهی یا نامتناهی) باشد و $H, K \leq G$ به طوری که $H \subseteq K$. در این صورت، اگر $[G:K]$ و $[K:H]$ متناهی باشند آنگاه

$$[G:H] = [G:K][K:H]$$

اثبات فرض کنیم $L_1 = \{a_1K, \cdots, a_mK\}$ و $L_2 = \{b_1H, \cdots, b_nH\}$ به ترتیب مجموعه‌ی هم‌مجموعه‌های (چپ) متمایز K در G و H در K باشند. حال کافی است نشان دهیم که $L_3 = \{a_ib_jH \mid i = 1, \cdots, m,\ j = 1, \cdots, n\}$ مجموعه‌ی هم‌مجموعه‌های (چپ)

متمایز H در G است(چـرا؟؟؟؟؟؟؟؟ //؟؟؟) ، و در نتیجـه $|L_3| = mn = |L_1||L_2|$.
ابتدا توجه کنید که در L_3 داریم

$$\begin{aligned} a_r b_s H = a_p b_q H &\Rightarrow (a_p b_q)^{-1}(a_r b_s) \in H \subseteq K \\ &\Rightarrow (a_p b_q)^{-1}(a_r b_s) \in K \\ &\Rightarrow a_r b_s K = a_p b_q K \\ &\Rightarrow a_r K = a_p K \\ &\Rightarrow a_r = a_p \\ &\Rightarrow b_s H = b_q H \\ &\Rightarrow b_s = b_q \\ &\Rightarrow a_r b_s = a_p b_q \end{aligned}$$

(مراحل اثبات بالا را توضیح دهید) بنابراین، اعضای L_3 متمایز هستند. حال نشان مـی‌دهـیم کـه L_3 در واقع برابر با مجموعه‌ی همه‌ی هم‌مجموعه‌های چپ H در G است. کـافی اسـت نشـان دهیم که بـرای هـر $x \in G$، $xH \in L_3$. چـون $xK \in L_1$، پـس $xK = a_r K$ و در نتیجـه $x = a_r k$ گه در آن $k \in K$. حال از $kH = b_s H \in L_2$ نتیجه مـی گیـریم کـه $k = b_s h$ که در آن $h \in H$. بنابراین،

$$xH = a_r kH = a_r b_s hH = a_r b_s H \in L_3$$

در پایان، $[G:H] = [G:K][K:H] = mn$.

تمرین ۲.۲

به توانایی‌های خود کم اهمیت ندهید

دسته‌ی اول

۱- در هر مورد زیر، با دلیل تعیین کنید که آیا H زیرگروه G هست یا نیست.

(الف) $G = (\mathbb{Z}; +)$ و $H = \mathbb{Z}^+ = \{n \in \mathbb{Z} \mid n \geq 0\}$.

(ب) $G=(\mathbb{Z}_8;+_8)$ و $H=\{0,2,4\}$.

(پ) $G=(\mathbb{R};+)$ و $H=\pi\mathbb{Q}=\{\pi x \mid x\in\mathbb{Q}\}$.

(ت) $G=(\mathbb{R};+)$ و $H=\pi\mathbb{Z}=\{\pi n \mid n\in\mathbb{Z}\}$.

(ث) $G=GL(n,\mathbb{R})$ و $H=SL(n,\mathbb{R})$ (**گروه خطی خاص** متشکل از ماتریس‌های حقیقی $n\times n$ با دترمینان ۱).

(ج) گروه (ضربی) G دلخواه و برای $a\in G$، $H=\{a^n \mid n\in\mathbb{Z}\}$.

۲- فرض کنید گروه (ضربی) G آبلی است و $n\in\mathbb{N}$. نشان دهید که مجموعه‌ی جواب‌های معادله‌ی $x^n=e$ در G، یعنی $H=\{x\in G \mid x^n=e\}$ یک زیرگروه G است.

۳- فرض کنید G گروه است.

(الف) نشان دهید که برای هر $a\in G$، مجموعه‌ی همه‌ی عضوهای G که با a تعویض پذیر باشند، یعنی $C_G(a)=\{x\in G \mid ax=xa\}$، زیرگروه G است.

(ب) (تعمیم (الف)) فرض کنید $S\subseteq G$. نشان دهید که مجموعه‌ی همه‌ی عضوهای G که با همه‌ی عضوهای S تعویض‌پذیر هستند، یعنی

$$C_G(S)=\{x\in G \mid (\forall s\in S)\quad xs=sx\}$$

زیرگروه G است. این زیرگروه را **مرکزساز** S در G می‌نامیم. اگر $S=\{a_1,\cdots,a_n\}$، می‌نویسیم $C_G(S)=C_G(a_1,\cdots,a_n)$.

(پ) (حالت خاص (ب)) نشان دهید که **مرکز گروه** G، یعنی

$$Z(G)=C_G(G)=\{x\in G \mid (\forall g\in G)\quad xg=gx\}$$

زیرگروه G است.

(ت) نشان دهید که $Z(G)=\bigcap_{a\in G} C_G(a)$.

(ث) ثابت کنید که G آبلی است اگر و تنها اگر $Z(G)=G$.

(ج) نشان دهید که مرکز گروه $GL(2,\mathbb{R})$ برابر است با

$$\left\{ \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix} \mid a \in \mathbb{R},\ \ a \neq 0 \right\}$$

(توجه کنید که هر عضو مرکز باید دست کم با $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ و $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ تعویض‌پذیر باشد.)

۴ـ فرض کنید H و K زیرگروه G باشند. مجموعه‌ی به نمایش طبیعی

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

را در نظر بگیرید.

(الف) نشان دهید که اگر هر عضو H با هر عضو K تعویض‌پذیر باشد، یعنی

$$(\forall h \in H)(\forall k \in K) \quad hk = kh$$

آنگاه $T = HK$ زیرگروه G است.

(ب) نشان دهید که $T = HK$ زیرگروه G است اگر و تنها اگر $HK = KH$. (به تفاوت بین $HK = KH$ و شرط قوی‌تر بند **(الف)** توجه کنید).

دسته‌ی دوم

۵- فرض کنید که G گروه و H زیرگروه آن باشد. برای هر $a \in G$، تعریف می‌کنیم

$$aHa^{-1} = \{aha^{-1} \mid h \in H\}$$

(الف) نشان دهید که aHa^{-1} زیرگروه G است. عضو aha^{-1} را **مزدوج** h تحت a، و aHa^{-1} را **مزدوج** H تحت a می‌نامیم. گاهی aha^{-1} را با h^a و aHa^{-1} را با H^a نیز نشان می‌دهند.

(ب) نشان دهید که $|H| = |aHa^{-1}|$.

(پ) نشان دهید که $N_G(H) = \{a \in G \mid aHa^{-1} = H\}$ زیرگروه G است. این زیرگروه را **نرمال‌ساز** H در G می‌نامیم. اگر $N_G(H) = G$، یعنی

$$(\forall a \in G) \quad aHa^{-1} = H$$

آنگاه می‌گوییم که H **خودمزدوج** است. در بخش **۸.۲** خواهیم دید که این زیرگروه‌ها بسیار با اهمیت هستند.

۶- مثالی از گروه G با زیرگروه نا بدیهی H ارائه دهید که $[G:H]$ نامتناهی باشد.

۷- فرض کنید G یک گروه و $H,K\leq G$. نشان دهید که $H\cap K$ زیرگروه G است.

۸- فرض کنید G یک گروه و زیرگروه‌های $H,K\leq G$ متناهی باشند. نشان دهید که اگر $(|H|,|K|)=1$ آنگاه $H\cap K=\{e\}$.

۹- فرض کنید H و K زیرگروه‌هایی از گروه متناهی G باشند به طوری که $|H|=p$ عددی اول باشد و $H\cap K\neq\{e\}$. ثابت کنید که $H\subseteq K$.

۱۰- فرض کنید که H و K زیرگروه‌هایی متمایز از گروه G باشند به طوری که $|H|=|K|=p$ عددی اول است. ثابت کنید که $|H\cup K|=2p-1$.

۱۱- فرض کنید که H و K زیرگروه‌هایی از گروه G باشند به طوری که اندیس آن‌ها در G متناهی است. نشان دهید که.

(الف) اندیس $H\cap K$ در G متناهی است و

$$[G:H\cap K]\leq[G:H][G:K]$$

(ب) اندیس $H\cap K$ در K متناهی است و $[K:H\cap K]\leq[G:H]$.

(پ) تساوی در **(ب)** برقرار است اگر و تنها اگر $G=HK$.

(ت) اگر اندیس‌های H و K در G متناهی و متباین باشند، آنگاه $G=HK$ و

$$[G:H\cap K]=[G:H][G:K]$$

۱۲- فرض کنید که H و K زیرگروه‌هایی متناهی از گروه دلخواه G باشند. ثابت کنید که

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

۱۳- فرض کنید G گروهی از مرتبه ی ۲۰ و $H,K\leq G$، با $|H|=4$ و $|K|=5$. ثابت کنید که $G=HK$.

۱۴- فرض کنید که H و K زیرگروه‌هایی از گروه متناهی G باشند به طوری که $|H|,|K| \geq \sqrt{|G|}$. ثابت کنید که $H \cap K \neq \{e\}$.

۱۵- فرض کنید G گروهی از مرتبه‌ی pq باشد که در آن p و q دو عدد اول هستند و $p > q$. ثابت کنید که گروه G حداکثر دارای یک زیرگروه از مرتبه‌ی p است.

۳.۲ مشبکه‌ی زیرگروه‌ها

مشبکه‌ی زیردستگاه‌های کلی جبری را در فصل ۱، بندهای ۹.۶.۱ - ۱۹.۶.۱ معرفی و اندکی مطالعه کردیم. در این بخش تعبیر این مطالب کلی را برای گروه‌ها مطالعه می‌کنیم. بسیاری از مطالب این بخش تکرار مطالب بخش ۶.۱ به زبان گروه‌ها است. فرض کنیم $Sub(G)$ مجموعه‌ی همه‌ی زیرگروه‌های گروه G باشد. در زیر خواهیم دید که مجموعه‌ی مرتب $(Sub(G);\leq)$، که در آن $\leq$ رابطه‌ی ترتیبی $\subseteq$ است، نیز یک مشبکه (در واقع مشبکه‌ای کامل) است. برخی از پژوهشگران به کمک ویژگی‌های این مشبکه اطلاعات مفیدی در باره‌ی خود گروه G به دست می‌آورند. این مشبکه در پژوهش‌های علوم شیمی و فیزیک نیز کاربردهای خوبی دارد.

برای اثبات مشبکه بودن $(Sub(G);\leq)$، باید نشان دهیم که برای هر دو زیرگروه $H, K \leq G$، $H \vee K = Sup\{H,K\}$ و $H \wedge K = Inf\{H,K\}$ وجود دارند. حتماً حدس زده‌اید که $H \wedge K = H \cap K$. حدس شما درست است. البته، ابتدا باید نشان دهیم که $H \cap K \in Sub(G)$. قضیه‌ی زیر بیش از این مطلب را اثبات می‌کند.

۱.۳.۲ قضیه. فرض کنیم G گروه است. در این صورت:

۱- برای هر $H, K \leq G$، $H \cap K$ نیز زیرگروه G است.

۲- برای هر خانواده‌ی $\{H_i\}_{i\in I}$ از زیرگروه‌های G، $H = \bigcap_{i\in I} H_i$ نیز زیرگروه G است.

اثبات. یقین داریم که این قضیه را به راحتی می‌توانید اثبات کنید. محک ۶.۲.۲ یا ۷.۲.۲ را به کار ببرید. (آیا لم ۱۰.۶.۱ این قضیه را اثبات می‌کند؟ بند ۱ بحث ۱۱.۶.۱ همراه با تعریف ۳.۱.۲ چطور؟).

حـال ببینـیم کـه $H \vee K = Sup\{H,K\}$ و $\bigvee\{H_i\}_{i\in I} = Sup\{H_i\}_{i\in I}$ کـدام زیرگروه‌های G هستند. روشن است که اگر اجتماع $H \cup K$ زیرگروه G باشد، آنگاه سـوپریمم نیز خواهد بود، زیرا کوچک‌ترین زیرگروه شامل H و K است. ولی، همان طور کـه در بخـش ۶.۱ نیز دیدیم، اجتماع دو زیردستگاه جبری لزوماً یک زیردستگاه نیست! (مثالی از زیرگروه‌های کلایـن یا $\mathbb{Z}$ بیاورید به طوری که اجتماع آن‌ها نسبت به عمل گروه بسته نباشد). برای حل کردن مساله، ابتدا تعبیر بند ۲ تعریف کلی ۱۲.۶.۱ را برای زیرگروه‌ها می‌آوریم.

۲.۳.۲ تعریف. فرض کنیم X زیرمجموعه‌ی گروه G باشد. در این صـورت، **کوچـک‌تـرین زیرگروه** G را که **شامل** X باشـد **زیرگـروه تولیـد شـده توسـط** X مـی‌نـامیم و آن را بـا $< X >$ نشان می‌دهیم. اگر $G = < X >$، می‌گوییم که گروه G توسـط X تولیـد شـده یـا X **مولد** G است.

۳.۳.۲ بحث در کلاس. یقیناً دو سؤال زیر برایتان مطرح هسـتند: **(الف)** آیـا کوچـک‌تـرین زیرگروه G شامل مجموعه‌ی X، یعنی $< X >$، همیشه وجود دارد؟ **(ب)** اگـر X داده شـود، چطور می‌توانیم کوچک‌ترین زیرگروه شامل مجموعه‌ی X، یعنی $< X >$ را (به ویـژه بـه کمـک برنامه‌ی رایانه‌ای) پیدا کنیم؟ در قضیه‌ی ۱۵.۶.۱ دیـدیم کـه $< X >$ بـه عنـوان زیرگروهـواره‌ی $(G;*)$ همیشه وجود دارد، ولی آیا زیر گروه است؟ در بحث ۱۴.۶.۱ گفتیم که اگر P از معادله‌ها تشکیل شده باشد، $< X >$ یک P - زیرجبر می‌شود. خوشبختانه بند ۱ قضیه‌ی ۱.۳.۲ نیـز نویـد می‌دهد که $< X >$ زیرگروه است. شگرد اثبات قضیه‌ی زیر را در اثبات قضیه‌ی ۱۵.۶.۱ آموختیم. از آنجا که این روش اثبات را در بسیاری از دروس دیگر جبر و جبر خطی به کـار مـی‌بـریم، اثبـات ساده‌ی آن را برای گروه‌ها دو باره می‌آوریم. اثبـات قضـیه‌ی ۹.۳.۲ و نتیجـه‌هـای پـس از آن نیـز تمرین خوبی هستند.

۴.۳.۲ قضیه. فرض کنیم G گـروه اسـت، $X \subseteq G$، و $S = \{H \leq G \mid X \subseteq H\}$ در این صورت،

$$< X > = \bigcap S = \bigcap_{H\in S} H = \bigcap\{H \leq G \mid X \subseteq H\}$$

اثبات. با توجه به تعریف $< X >$ که با دو ویژگی **زیرگروه** G **شـامل** X **کوچـک‌تـرین** است، ابتدا باید نشان دهیم که $K = \bigcap_{H\in S} H$ دارای این دو ویژگـی اسـت. قضـیه‌ی ۱.۳.۲ نشـان می‌دهد که $K = \bigcap_{H\in S} H$ زیرگروه G است. چون هـر عضـو $H \in S$ شـامل X اسـت، پـس

$K = \bigcap_{H \in S} H$ نیز شامل X است. تا اینجا اثبات شد که K زیرگروهی از G و شامل X است. برای اثبات اینکه K با این دو ویژگی کوچک‌ترین است، فرض می‌کنیم کـه L نیـز زیرگروهـی از G و شامل X باشد. پس $L \in S$. حال، روشن است کـه $K = \bigcap_{H \in S} H \subseteq L$ و اثبـات تمـام است!

۵.۳.۲ نتیجه. فرض کنیم که G گروه و H و K زیرگروه آن باشند. در این صورت،

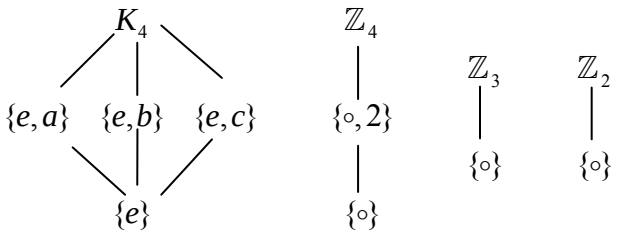
$$H \vee K = Sup\{H, K\} = < H \cup K >$$

۶.۳.۲ نتیجه. مجموعه‌ی مرتب $(Sub(G); \subseteq)$ متشکل از زیرگروه‌های گروه G مشبکه (و در واقع، مشبکه‌ای کامل) است $\left(\bigvee\{H_i\}_{i \in I} = Sup\{H_i\}_{i \in I} = < \bigcup_{i \in I} H_i >\right)$.

۷.۳.۲ تعریف. نمودار مشبکه‌ی $(Sub(G); \subseteq)$ را **نمودار مشبکه‌ی زیرگـروه‌هـای** G می‌نامیم.

۸.۳.۲ بحث در کلاس

۱- با توجه به بحث ۹.۲.۲، نمودارهای مشبکه‌ی زیرگروه‌های چند گروه را در زیر می‌آوریم:



۲- با توجه به بند ۱، $< 2 >$ را در $\mathbb{Z}_3$ و در $\mathbb{Z}_4$ و $< a >$، $< a,b >$ را در K_4 بیابید.

۳- روشن است که اگر X خود یک زیرگروه G باشد، آنگاه $< X > = X$. **چطور؟** همچنین، کوچـک‌تـرین زیرگـروه G شـامل مجموعـه‌ی تهـی برابـر بـا $\{e\}$ اسـت. یعنـی، $< \varnothing > = \{e\} = < e >$.

۴- (جالب است) فرض کنیم G گروه و H و K زیرگـروه آن باشـند. نشـان دهیـد کـه، اجتمـاع $H \cup K$ زیرگروه G است اگر و تنها اگر $H \subseteq K$ یا $K \subseteq H$.

۵- ممکن است $X \neq Y$ ولی $<X>=<Y>$. برای مثال، فرض کنید $G=(\mathbb{Z}_4;+_4)$. در این صورت، $<1,2>=<1>$. چطور؟

۶- با استفاده از قضیه‌ی ۴.۳.۲، نشان دهید که اگر $X \subseteq Y$ زیرمجموعه‌های گروه G باشند آنگاه $<X> \subseteq <Y>$.

۷- علت اینکه فعلاً توانایی چندانی در محاسبه‌ی $<X>$ نداریم و حتی نمی‌توانیم برنامه‌ای رایانه‌ای برای محاسبه‌ی آن بنویسیم، این است که تعریف ۲.۳.۲ و قضیه‌ی ۴.۳.۲ مطلبی در باره‌ی عضوهای $<X>$ بر حسب عضوهای X بیان نمی‌کنند!

۸- این مثال‌ها را در بخش ۶.۱ نیز دیده‌ایم. چطور، برای مثال، می‌توان $<2>$ را در گروه $(\mathbb{Z}_8;+_8)$ محاسبه کرد؟ چون $\mathbb{Z}_8$ متناهی است، قضیه‌ی ۸.۲.۲ به کار می‌آید. یعنی باید کم‌ترین تعداد عضو $\mathbb{Z}_8$ را به مجموعه‌ی $\{0,2\}$ بیفزاییم تا مجموعه‌ای بسته نسبت به عمل جمع همنهشتی $+_8$ به دست آید! روشن است که

$$\begin{aligned}<2> &= \{0, 2, 2+_8 2=4, 2+_8 2+_8 2=6\} \\ &= \{0,2,4,6\}\end{aligned}$$

۹- حال شما $<3>$ را در گروه $(\mathbb{Z}_8;+_8)$ و در گروه $(\mathbb{Z}_{15};+_{15})$ بیابید.

۱۰- زیرگروه $H=<2,3>$ در گروه $\mathbb{Z}_{15}$ کدام است؟ محاسبه‌ی این زیرگروه نیز راحت، ولی قدری پرزحمت‌تر، است! باید شامل عضوهای زیر باشد:

$$\begin{aligned}&0,2,4,6,8,\cdots \\ &3, 3+_{15} 3=6, 9, \cdots \\ &2+_{15} 3=5, \cdots\end{aligned}$$

اگر کمی از عقل سلیم را به کار ببریم، اغلب این محاسبه‌ها را می‌توانیم کوتاه‌تر کنیم. برای مثال، چون $1 \in H$ $(8+_{15} 8=16 \equiv_{15} 1)$، پس $H=\mathbb{Z}_{15}$. چرا؟

۱۱- آیا برای محاسبه‌ی زیرگروه $<1>$ در گروه $(\mathbb{Z};+)$ می‌توان قضیه‌ی ۸.۲.۲ را به کار برد؟ بنابر بند ۶ بحث ۹.۲.۲، هر زیرگروه نابدیهی $(\mathbb{Z};+)$ نامتناهی است. پس قضیه‌ی ۸.۲.۲ به کار نمی‌آید! ولی می‌توانید قضیه‌ی ۶.۲.۲ را به کار ببرید و نتیجه بگیرید که $<1>=\mathbb{Z}$. به همین ترتیب، می‌توانید نشان دهید که، برای مثال،

$$<2>=2\mathbb{Z}=\{2k \mid k \in \mathbb{Z}\} \quad ,\cdots, \quad <n>=n\mathbb{Z}$$

۱۲- با توجه به نمونه‌های بالا و با الگو (صرفاً الگو) قرار دادن حالت بسیار کلی و صوری ساختن گروه آزاد در بحث **۱۶.۸.۱**، حدس بزنید که در حالت کلی، چطور عضوهای $< X >$ را در گروه دلخواه G تعیین کنیم؟ چون $< \varnothing > = \{e\}$، فرض می‌کنیم $X \neq \varnothing$. احتمالاً درست حدس زده‌اید. به زبان غیر رسمی، ابتدا عضوهای X را در سبدی می‌ریزیم. سپس وارون‌های این عضوها را به سبد اضافه می‌کنیم و مجموعه‌ی زیر را به دست می‌آوریم:

$$T_1 = X \cup X^{-1}$$

که در آن $X^{-1} = \{x^{-1} \mid x \in X\}$ مجموعه‌ی همه‌ی وارون‌های عضوهای X است. هنوز کارمان تمام نشده است، زیرا ممکن است این سبد نسبت به عمل گروه بسته نباشد. پس حاصل-ضرب‌های هر تعداد متناهی از عضوهای سبد را نیز به آن اضافه می‌کنیم و مجموعه‌ی زیر را به دست می‌آوریم:

$$T_2 = \{x \in G \mid x \text{ حاصل‌ضرب تعدادی متناهی از عضوهای } T_1 \text{ است}\}$$

آیا به هدفمان رسیدیم؟ حتماً می‌گویید که پس وارون‌ها و حاصل‌ضرب‌های عضوهای مجموعه‌ی T_2 **چطور؟** فرض کنیم این عضوها را نیز در سبدمان انداختیم؛ وارون‌ها و حاصل-ضرب‌های این مجموعه‌ی اخیر **چطور؟** به نظر می‌رسد که باید این روند را تا بینهایت ادامه دهیم و هرگز سبدمان به یک زیرگروه تبدیل نشود! ولی، قضیه‌ی زیر نشان می‌دهد که در همان مرحله‌ی رسیدن به T_2 کارمان تمام است! یقیناً نخواهید گفت که این همه تلاش ما برای چیست!؟ مطابق معمول این کتاب، هدف ما آموزش **فوت و فن** کارها است و هدف شما نیز آموختن این فوت و فن‌ها و روش‌های تفکر و به کار بردن این شگردها در موارد مشابه است. همتای بسیاری از مفاهیم این کتاب، به ویژه قضیه‌ی زیر، را در مباحث دیگر ریاضی، به ویژه در درس‌های جبر و جبرخطی (و البته، در کاربردهای آن‌ها در فیزیک، شیمی، کامپیوتر نظری، و علوم دیگر) خواهید دید.

۹.۳.۲ قضیه. اگر $X \neq \varnothing$ زیرمجموعه‌ی گروه G باشد، آنگاه $< X >$ (در نمادگذاری ضربی) متشکل از همه‌ی حاصل‌ضرب‌های متناهی به صورت $x_1 x_2 \cdots x_n$ است که در آن، برای هر i، $x_i \in X$ یا $x_i \in X^{-1}$. یعنی،

$$< X > = \{x_1 x_2 \cdots x_n \mid n \in \mathbb{N}, x_i \in X \cup X^{-1}\}$$

اثبات. قرار می‌دهیم $H = \{x_1 x_2 \cdots x_n \mid n \in \mathbb{N}, x_i \in X \cup X^{-1}\}$ و نشان می‌دهیم که **(الف)** $H \leq G$، **(ب)** $X \subseteq H$، **(پ)** اگر K نیز زیرگروه G باشد و $X \subseteq K$، آنگاه $H \subseteq K$.

برای اثبات **(الف)**، توجه می‌کنیم که عضوی چون $x \in X$ وجود دارد. پس $e = xx^{-1} \in H$. حال اگر، برای $x_i, y_j \in X \cup X^{-1}$،

$$x = x_1 \cdots x_n, \quad y = y_1 \cdots y_m \in H$$

آنگاه (درستی واقعیت زیر را توضیح دهید):

$$xy^{-1} = x_1 \cdots x_n (y_1 \cdots y_n)^{-1} = x_1 \cdots x_n y_n^{-1} \cdots y_1^{-1} \in H$$

درستی شرط **(ب)** روشن است. اثبات درستی شرط **(پ)** نیز راحت است. چون $X \subseteq K$ و K نسبت به وارون‌ها بسته است، پس $X \cup X^{-1} \subseteq K$. حال، چون K نسبت به عمل گروه بسته است و هر عضو H به صورت $x = x_1 \cdots x_n$ است، که در آن هر x_i در $X \cup X^{-1}$ است، پس $H \subseteq K$.

نتیجه‌های زیر را به راحتی می‌توانید اثبات کنید.

۱۰.۳.۲ نتیجه. اگر $X \neq \emptyset$ زیرمجموعه‌ی گروه G باشد، آنگاه (در نمادگذاری ضربی)

$$< X > = \{x_1^{n_1} x_2^{n_2} \cdots x_k^{n_k} \mid x_i \in X, n_i \in \mathbb{Z}\}$$

۱۱.۳.۲ نتیجه. اگر $X = \{x_1, \cdots, x_k\}$ زیرمجموعه‌ای متناهی از گروه G باشد، به طوری که

$$(\forall i, j = 1, \cdots, k) \quad x_i x_j = x_j x_i$$

آنگاه $< x_1, \cdots, x_n > = < \{x_1, \cdots, x_k\} > = \{x_1^{n_1} \cdots x_k^{n_k} \mid n_1, \cdots, n_k \in \mathbb{Z}\}$

۱۲.۳.۲ نتیجه. اگر $X = \{x\}$ زیرمجموعه‌ای تک عضوی از گروه G باشد، آنگاه

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

و در نمادگذاری جمعی، $< x > = \{nx \mid n \in \mathbb{Z}\}$.

۱۳.۳.۲ تعریف

۱- اگر $X = \{x_1, x_2, \cdots, x_n\}$ زیرمجموعه‌ای متناهی از گروه G باشد، آنگاه $H = < X > = < x_1, \cdots, x_n >$ را **زیرگروه متناهی مولد** G می‌نامیم.

۲- اگر $X=\{x\}$، آنگاه $H=<x>$ را **زیرگروه دوری** با مولد x می‌نامیم.

۳- اگر $G=<x_1,\cdots,x_n>$، آنگاه G را **گروهی متناهی مولد** و اگر $G=<x>$، آن را **گروهی دوری** با مولد x می‌نامیم.

۱۴.۳.۲ بحث در کلاس

۱- به دلیل اهمیت گروه‌های دوری، آن‌ها را در بخش ۴.۲ به تفصیل مطالعه خواهیم کرد. توجه می‌کنیم که یک تفاوت دیگر گروه‌های $\mathbb{Z}_4$ و K_4 این است که $\mathbb{Z}_4=<1>=<3>$ دوری است، در حالی که K_4 چنین نیست. **چرا؟**

۲- با استفاده از نتیجه‌ی ۱۲.۳.۲، نشان دهید که هر گروه دوری، آبلی است.

۳- با استفاده از قضیه‌ی ۹.۳.۲ و نتیجه‌ی ۱۰.۳.۲ ، برنامه‌ای کامپیوتری بنویسید به طوری که $<X>$ را در گروه دلخواه G تعیین کند.

۴- با دیدن نمونه‌های

$$
\begin{aligned}
&<e>=\{e\},\quad <G>=G\\
&\mathbb{Z}=<1>=<2,3>=\cdots\\
&2\mathbb{Z}=<2>=<-2>=<2,4,16>=\cdots\\
&n\mathbb{Z}=<n>=<-n>=\cdots\\
&\mathbb{Z}_4=<\mathbb{Z}_4>=<1>=<1,2>=<3>=<2,3>\\
&\mathbb{Z}_n=<1>=<k>,\quad (k,n)=1\\
&K_4=<a,b>=<a,c>=\cdots\\
&K_4\neq <e>\neq <a>\neq <b>\neq <c>,\{e\}=<e>,\\
&\{e,a\}=<a>,\quad \{e,b\}=<b>,\quad \{e,c\}=<c>
\end{aligned}
$$

متوجه چه نکته‌هایی در مورد تعریف بالا می‌شویم؟ درست است: $X=G$ مولد خود گروه G است؛ مجموعه‌های متفاوت ممکن است مولد یک گروه باشند؛ یک گروه یا زیرگروه آن ممکن است با مجموعه‌ای نامتناهی تولید شود و در عین حال با مجموعه‌ای متناهی یا حتی تک عضوی نیز تولید شود، یعنی متناهی مولد یا حتی دوری باشد؛ گروه‌های $(\mathbb{Z};+)$، $2\mathbb{Z}$، $(\mathbb{Z}_n;+_n)$ دوری هستند؛ اگر مولد گروه‌های دوری $\mathbb{Z}$ و $\mathbb{Z}_n$، یعنی عدد ۱، عضو زیرگروهی از $\mathbb{Z}$ یا $\mathbb{Z}_n$ باشد، آن زیرگروه برابر با خود گروه است؛ با وجودی که K_4 دوری نیست، ولی هر زیرگروه دیگر آن دوری است!

تمرین ۳.۲

تمرین‌ها مهم‌ترین قسمت هر درس هستند

دسته‌ی اول

۱- نشان دهید که $\mathbb{Z}_{12} = <2,3>$. سپس نشان دهید که، برای $n \geq 3$، $\mathbb{Z}_n = <2,3>$.

۲- فرض کنیم G گروه و H و K زیرگروه آن باشند. نشان دهید که، اجتماع $H \cup K$ زیرگروه G است اگر و تنها اگر $H \subseteq K$ یا $K \subseteq H$. همچنین، نتیجه بگیرید که هیچ گروهی را نمی‌توان به صورت اجتماع دو زیرگروه سره‌اش نوشت.

۳- بدون استفاده‌ی مستقیم از قضیه‌ی ۹.۳.۲، ولی مشابه با اثبات آن، نشان دهید که اگر $X \neq \emptyset$ زیرمجموعه‌ی گروه G باشد، آنگاه

(الف) $$< X > = \{x_1^{n_1} x_2^{n_2} \cdots x_k^{n_k} \mid x_i \in X, n_i \in \mathbb{Z}\}$$

(ب) اگر $X = \{x\}$ زیرمجموعه‌ای تک عضوی از گروه G باشد، آنگاه

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

دسته‌ی دوم

۴- فرض کنید H، K، و T زیرگروه‌هایی از گروه G باشند به طوری که $H \subseteq K$، $H \cap K = K \cap T$، و $HT = KT$. ثابت کنید که $H = K$.

۵- فرض کنید که A و B زیرگروه‌هایی آبلی از گروه G باشند و $G = AB$. ثابت کنید که

$$Z(G) = (A \cap Z(G))(B \cap Z(G))$$

۶- فرض کنید A، B، C زیرگروه‌هایی از گروه G باشند به طوری که $A \subseteq C$. ثابت کنید که

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

۴.۲ گروه‌های دوری

گروه‌های دوری دسته‌ای ساده و در عین حال بسیار با اهمیت از گروه‌ها هستند. از این رو یک بخش کامل را به مطالعه‌ی آن‌ها اختصاص داده‌ایم. همان طور که اعداد اول سازنده‌ی همه‌ی اعداد طبیعی هستند، در دروس بعدی جبر خواهیم دید که گروه‌های **دوری** نیز به تعبیری **سازنده‌ی** همه‌ی گروه‌های **آبلی** متناهی مولد هستند. برای طولانی نشدن این بخش، در بخش بعد دسته-بندی کاملی از گروه‌های دوری به دست خواهیم آورد. در واقع، خواهیم دید که همه‌ی گروه‌های دوری نامتناهی با گروه دوری $(\mathbb{Z};+)$ و هر گروه دوری متناهی n عضوی با گروه دوری $(\mathbb{Z}_n;+_n)$ یک‌ریخت است! بنابراین، تا حد یک‌ریختی، تنها یک دسته گروه دوری نامتناهی داریم و، برای هر عدد طبیعی $n \in \mathbb{N}$، تنها یک دسته گروه دوری n عضوی وجود دارد. از این رو، برای مطالعه‌ی گروه‌های دوری، و لذا گروه‌های آبلی متناهی مولد، تنها کافی است گروه‌های دوری $(\mathbb{Z};+)$ و $(\mathbb{Z}_n;+_n)$ را مطالعه کنیم! **جالب است، این طور نیست؟**

ابتدا مفهوم زیر را می‌آوریم که نه تنها در مطالعه‌ی گروه‌های دوری مفید و اساسی است، بلکه در بررسی همه‌ی گروه‌ها مفید است. داستان از این قرار است که در برخی از گروه‌ها، مانند گروه-های جمعی $(\mathbb{Z};+)$، $(\mathbb{Q};+)$، $(\mathbb{R};+)$، $(\mathbb{C};+)$، هیچ عدد ناصفر، به ویژه عدد ۱، را نمی-توان به تعدادی متناهی با خودش جمع کرد و عدد صفر را به دست آورد. یا در گروه‌های ضربی $(\mathbb{Q}^*;\cdot)$، $(\mathbb{R}^*;\cdot)$، هیچ عدد متفاوت با ۱ و ۱- را نمی‌توان به تعدادی متناهی در خودش ضرب کرد و عدد ۱ را به دست آورد! البته در گروه ضربی $(\mathbb{C}^*;\cdot)$ داریم $(\sqrt{-1})^4 = 1$، ولی بسیاری از اعداد مختلط دیگر این ویژگی را ندارند! از این‌ها جالب‌تر اینکه، در گروه همنهشتی $(\mathbb{Z}_n;+_n)$، هر عضو را می‌توان، برای مثال، به تعداد n یا $2n$ بار، با خودش جمع (همنهشتی) کرد وعضو خنثی 0 را به دست آورد! **این طور نیست؟** همچنین، در K_4 داریم $a^2 = b^2 = c^2 = e$. حدس می‌زنید تابع دوسویی $\sigma \in S_n$ را چند بار با خودش ترکیب کنیم، تابع همانی به دست می‌آید؟ حال تعریف کلی زیر را ببینید.

۱.۴.۲ تعریف. فرض کنیم G گروهی با عضو همانی e باشد و $a \in G$. در این صورت،

۱- می‌گوییم که **مرتبه‌ی** a (در G) **متناهی** است اگر عدد طبیعی m وجود داشته باشد به طوری که $a^m = e$.

۲- کوچک‌ترین عدد طبیعی n با ویژگی $a^n = e$ را **مرتبه‌ی** a (در G) می‌نامیم و می‌نویسیم $O_G(a)$، یا $O(a)$ اگر امکان اشتباه نباشد.

۳- اگر عدد طبیعی m با ویژگی $a^m = e$ وجود نداشته باشد، می‌گوییم که **مرتبه‌ی** a (در G) **نامتناهی** است، و می‌نویسیم $O_G(a) = \infty$.

۲.۴.۲ بحث در کلاس

۱- یادآوری می‌کنیم که در نمادگذاری جمعی، عبارت $a^n = e$ به $na = 0$ تبدیل می‌شود، که در آن $na = a + a + \cdots + a$. در هر گروه G، $O(e) = 1$.

۲- یک عضو ممکن است متعلق به چند گروه باشد و مرتبه‌ی آن در هر گروه متفاوت باشد. برای مثال، $O_{\mathbb{Z}_4}(1) = 4$ در حالی که $O_{\mathbb{Z}_7}(1) = 7$ و $O_{\mathbb{Z}}(1) = \infty$. به عنوان نمونه‌هایی دیگر، $O_{\mathbb{Z}_4}(2) = 2$، در حالی که $O_{\mathbb{Z}_{16}}(2) = 8$.

۳- نشان دهید که $O_G(a) = \infty$ اگر و تنها اگر همه‌ی توان‌های a متمایز باشند! راهنمایی: از این مطالب استفاده کنید که **(الف)** اگر برای دو عدد صحیح $r > s$، داشته باشیم $a^r = a^s$، آنگاه، به دلیل وجود وارون‌ها در گروه G، $a^{r-s} = e$ که در آن $r - s \in \mathbb{N}$، و **(ب)** اگر $a^m = e$ آنگاه $a^{2m} = e = a^m$.

۴- با استفاده از بند۳، نشان دهید که مرتبه‌ی هر عضو در گروهی متناهی، یقیناً متناهی است!

۵- آیا مرتبه‌ی عضوی نا همانی در گروهی نامتناهی می‌تواند متناهی باشد؟ توجه می‌کنیم که، اگر چه در گروه جمعی اعداد مختلط $(\mathbb{C};+)$ مرتبه‌ی هر عضو ناصفر نامتناهی است، ولی در گروه ضربی و نامتناهی $(\mathbb{C}^*;\cdot)$ داریم $O(i) = O(\sqrt{-1}) = 4$.

۶- در گروه K_4، $O(a) = O(b) = O(c) = 2$.

۷- در گروه خطی عام نامتناهی $GL(2,\mathbb{R})$، $O\left(\begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}\right) = 2$ (چرا؟)

۸- در مطالعه‌ی گروه‌های دوری، حساب اعداد طبیعی (بخش‌پذیری، الگوریتم تقسیم، و از این قبیل، که در مقدمه آوردیم) نقش مهمی دارد. قضیه‌ی زیر کار محاسبه‌ی مرتبه را اغلب ساده‌تر می‌کند.

۳.۴.۲ لم. فرض کنیم که مرتبه‌ی عضو $a \in G$ متناهی باشد. در این صورت $O(a) = n$ اگر و تنها اگر دو شرط زیر برقرار باشند:

۱- $a^n = e$؛

۲- اگر برای عدد طبیعی m، $a^m = e$ آنگاه $n \mid m$. (در حالی که در تعریف مرتبه تنها شرط $n \leq m$ آمده است.)

اثبات. روشن است که اگر شرایط (الف) و (ب) برقرار باشند، آنگاه $O(a) = n$. برعکس، فرض کنیم $O(a) = n$. روشن است که $a^n = e$. حال فرض کنیم $a^m = e$. برای اثبات بخشپذیری $n \mid m$، بنابر الگوریتم تقسیم، می‌نویسیم

$$m = nq + r, \qquad 0 \leq r < n \qquad (*)$$

حال داریم (به فن اثبات توجه کنید)

$$e = a^m = a^{nq+r} = a^{nq}a^r = (a^n)^q a^r$$
$$= e^q a^r = a^r$$

بنابراین، چون $r < n$، باید $r = 0$ (چرا؟) و در نتیجه $m = nq$، که حکم قضیه را اثبات می‌کند.

قبل از به کار بردن مفهوم مرتبه در مطالعه‌ی گروه‌های دوری، حکم‌های زیر را نیز می‌آوریم.

۴.۴.۲ **لم.** حکم‌های زیر برای عضوهای گروه G برقرار هستند.

۱- $O(a) = O(b) \Leftrightarrow (\forall m \in \mathbb{N})(a^m = e \Leftrightarrow b^m = e)$.

۲- $O(a) = O(a^{-1})$.

۳- $O(a) = O(xax^{-1})$.

۴- $O(ab) = O(ba)$.

۵- اگر $O(a) = n$ و $k \mid n$، آنگاه $O(a^k) = n/k$.

۶- فرض کنیم $O(a) = n$ و $d = (m,n)$. در این صورت،

$$O(a^m) = \frac{O(a)}{(m,n)} = \frac{n}{d}$$

اثبات. حکم ۶ را اثبات می‌کنیم. بقیه را به آسانی می‌توانید، با استفاده از لم ۳.۴.۲ و بند ۱ این لم، اثبات کنید.

۶- بنـا بـه فـرض، داریـم $m = dm_1$ و $n = dn_1$ کـه در آن $(m_1, n_1) = 1$. بـرای اثبـات $O(a^m) = n/d$، توجه می‌کنیم که

$$(a^m)^{\frac{n}{d}} = a^{\frac{mn}{d}} = a^{\frac{dm_1 n}{d}} = a^{m_1 n} = (a^n)^{m_1} = e^{m_1} = e$$

حال، اگر $(a^m)^l = e$، آنگاه $n \mid ml$، یعنی $dn_1 \mid dm_1 l$ و در نتیجه، $n_1 \mid m_1 l$. ولی $(n_1, m_1) = 1$ ایجاب می‌کند که $(n/d) = n_1 \mid l$ و حکم اثبات شده است.

حال برخی از ویژگی‌های گروه‌های دوری را بررسـی مـی‌کنـیم. ابتـدا یـادآوری مـی‌کنـیم کـه $< a > = \{a^n \mid n \in \mathbb{Z}\}$ و در نمادگذاری جمعی، $< a > = \{na \mid n \in \mathbb{Z}\}$. قضـیه‌ی زیـر و اثبات آن بسیار با اهمیت است. یادآوری می‌کنیم که $|G|$ عدد اصلی یا **مرتبه**‌ی گروه G اسـت. قضیه‌ی زیر توجیه می‌کند که چرا واژه‌ی **مرتبه** را برای تعداد عضوهای گروه نیز به کار بردیم.

۵.۴.۲ قضیه. فـرض کنـیم a عضـو گـروه G باشـد. در ایـن صـورت، مرتبـه‌ی گـروه دوری $< a >$ برابر با مرتبه‌ی هر مولد آن است. یعنی، $O(a) = |< a >|$.

اثبات ابتدا فرض می‌کنیم که $O(a) = n < \infty$ متناهی باشـد. ادعـا مـی‌کنـیم کـه عضـوهای $\{e, a, a^2, \cdots, a^{n-1}\}$ متمایز هستند و $< a > = \{e, a, a^2, \cdots, a^{n-1}\}$. روشـن اسـت کـه $\{e, a, a^2, \cdots, a^{n-1}\} \subseteq < a >$. برعکس، فرض کنـیم $x = a^m \in < a >$. بنـابر الگـوریتم تقسیم، داریم

$$m = nq + r \qquad 0 \le r < n$$

حـال، بـا محاسـبه‌ی $a^m = a^{nq+r}$، نشـان دهیـد کـه $a^m = a^r$ و نتیجـه بگیریـد کـه $x = a^m \in \{e, a, a^2, \cdots, a^{n-1}\}$. برای کامل کردن اثبـات، بایـد نشـان دهـیم کـه عضـوهای $\{e, a, a^2, \cdots, a^{n-1}\}$ متمایز هستند. داریم

$$a^r = a^s \quad (r > s, 0 \le r, s < n-1) \quad \Rightarrow a^{r-s} = e$$

که متناقض با $O(a) = n$ است، زیرا $0 < r - s < n$. این مطلب حکـم را در حالـت متنـاهی بودن مرتبه اثبات می‌کند. **چطور؟**

حال فرض کنید $O(a) = \infty$. کافی است نشان دهید که همه‌ی عضوهای

$$e, a, a^2, \cdots, a^k, \cdots$$

متمایز هستند (فن کار را آموخته‌اید. بند ۳ بحث ۲.۴.۲ را نیز ببینید).

۶.۴.۲ نتیجه. فرض کنیم گروه G دارای n عضو باشد. در این صورت، G دوری است اگر و تنها اگر دارای عضوی چون $a \in G$ با مرتبه‌ی n باشد.

اثبات. کافی است با دقت بیشتری به اثبات قضیه‌ی بالا توجه کنید.

نتیجه‌های جالبی بلاواسطه از تلفیق قضیه‌های لاگرانژ و ۵.۴.۲ به دست می‌آیند که بسیار به کار خواهیم برد.

۷.۴.۲ نتیجه. مرتبه‌ی هر عضو a از گروه متناهی G مرتبه‌ی گروه G را می‌شمارد، یعنی $O_G(a) \mid\mid G$.

۸.۴.۲ نتیجه. اگر G گروهی با n عضو باشد، آنگاه

$$(\forall a \in G) \quad a^n = e$$

۹.۴.۲ نتیجه. هر گروه از مرتبه‌ی عددی اول، دوری است و هر عضو $a \neq e$ مولد آن است.

۱۰.۴.۲ بحث در کلاس

۱- با استفاده از نتیجه‌ی ۶.۴.۲، یک بار دیگر نشان دهید که گروه K_4 دوری نیست.

۲- توجه می‌کنیم که چون $\mathbb{Z} = <1> = <-1>$ و برای هر عدد صحیح دیگر n، $\mathbb{Z} \neq <n>$، این گروه دوری تنها دارای دو مولد است. ولی گروه‌های دوری متناهی ممکن است یک، دو یا بیش از دو مولد داشته باشند. همه‌ی مولدهای گروه‌های دوری $\mathbb{Z}_4$، $\mathbb{Z}_6$، و $\mathbb{Z}_5$، را بیابید.

۳- در بخش ۹ از فصل ۱، دسته‌های دستگاه‌های جبری را مطرح کردیم که ممکن است نسبت به اعمالی چون زیردستگاه، حاصل ضرب، و خارج قسمت بسته باشند. اگر $\mathcal{K}$ دسته‌ی همه‌ی گروه‌های دوری باشد، خواهیم دید که $\mathcal{K}$ نسبت به زیرگروه و خارج قسمت بسته است ولی نسبت به حاصل‌ضرب بسته نیست! از این مطلب آخر و قضیه‌ی بیرخوف، در بخش ۹.۱، چه نتیجه‌ای در باره‌ی دسته‌ی گروه‌های دوری به دست می‌آید؟ **روش اثبات** قضیه‌ی بسیار مهم زیر را یکی دو بار دیگر به کار خواهیم برد.

۱۱.۴.۲ قضیه. زیرگروه هر گروه دوری، گروهی دوری است.

اثبات. فرض کنیم $G=<a>$ گروهی دوری و H زیرگروه آن باشد. حالت $H=\{e\}=<e>$ روشن است. فرض کنیم $H\neq\{e\}$ و $h\neq e$ در H باشد. چون $h\in H\subseteq G=<a>$، پس $h=a^k$ که در آن $k\in\mathbb{Z}^*$. از طرفی، $h^{-1}=a^{-k}\in H$ و در نتیجه مجموعه‌ی

$$S=\{m\in\mathbb{N}\mid a^m\in H\}\subseteq\mathbb{N}$$

ناتهی است. **چرا؟** حال، بنابر **اصل خوش‌ترتیبی** در $\mathbb{N}$، مجموعه‌ی S دارای **کوچک‌ترین** عدد طبیعی مانند n است. ادعا می‌کنیم که $H=<a^n>$. روشن است که $a^n\in H$ و در نتیجه $<a^n>\subseteq H$. **چرا؟** برای اثبات $H\subseteq<a^n>$، فرض می‌کنیم $h\in H$ دلخواه باشد. داریم $h=a^m$ که در آن $m\in\mathbb{Z}$. **چرا؟** حال، بنابر الگوریتم تقسیم، داریم

$$m=nq+r\qquad(0\leq r<n)$$

و در نتیجه $a^m=a^{nq+r}=(a^n)^q a^r$. بنابراین، $a^r=a^m(a^n)^{-q}\in H$. **چرا؟** حال، چون n کوچک‌ترین عدد طبیعی با شرط $a^n\in H$ است و $0\leq r<n$، باید $r=0$. در نتیجه، $m=nq$ و $a^m=(a^n)^q\in<a^n>$. این مطلب اثبات می‌کند که $H=<a^n>$.

۱۲.۴.۲ نتیجه. اگر $H\neq\{e\}$ زیرگروهی از گروه دوری $G=<a>$ باشد، آنگاه $H=<a^n>$، که در آن n کوچک‌ترین عدد طبیعی با ویژگی $a^n\in H$ است.

اثبات. کافی است به اثبات قضیه‌ی بالا توجه کنید.

در بند ۶ بحث **۹.۲.۲** قول دادیم که همه‌ی زیرگروه‌های $(\mathbb{Z};+)$ را مشخص خواهیم کرد. نتیجه‌ی مهم زیر در این باره است.

۱۳.۴.۲ نتیجه

۱- هر زیر گروه $(\mathbb{Z};+)$ دوری و به صورت $H=n\mathbb{Z}=\{nk\mid k\in\mathbb{Z}\}$ است، که در آن $n\in\mathbb{N}\cup\{0\}$.

۲- رابطه‌ی ترتیبی در $Sub(\mathbb{Z})$ به صورت زیر است:

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

۳- سوپریمم و اینفیمم در مشبکه‌ی $Sub(\mathbb{Z})$ به صورت زیر هستند:

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

که در آن، $[m,n]$ کوچک‌ترین مضرب مشترک m و n و (m,n) بزرگ‌ترین مقسوم‌علیه آن‌ها است.

اثبات. بلاواسطه از قضیه‌ی ۱۱.۴.۲ نتیجه می‌شود. در ضمن، توجه می‌کنیم که اگر $H \neq \{0\}$ زیرگروه $\mathbb{Z}$ باشد، آنگاه n کوچک‌ترین عدد طبیعی متعلق به H است به طوری که $H = n\mathbb{Z}$.

۱۴.۴.۲ بحث در کلاس. قضیه‌ی مهم ۱۱.۲.۲ لاگرانژ را به خاطر بیاورید که بیان می‌کند اگر H زیرگروهی از یک گروه متناهی G باشد، آنگاه مرتبه‌ی H، یعنی $|H|$، مرتبه‌ی G، یعنی $|G|$، را می‌شمارد. حال، سؤال این است که آیا عکس قضیه‌ی لاگرانژ درست است؟ یعنی، اگر m مرتبه‌ی گروه متناهی G را بشمارد، آیا G لزوماً باید زیرگروهی m عضوی داشته باشد؟ پاسخ به این سؤال در حالت کلی منفی است، و قضیه‌های سیلو در درس‌های دیگر جبر مشخص می‌کنند که عکس قضیه‌ی لاگرانژ برای کدام نوع از گروه‌ها و از چه مرتبه‌ای درست است. ولی با اطلاعاتی که تاکنون به دست آورده‌ایم، پاسخ سؤال بالا را می‌توانیم در قضیه‌ی زیر برای گروه‌های دوری متناهی اثبات کنیم.

۱۵.۴.۲ قضیه. فرض کنیم $G = < a >$ گروهی دوری با n عضو باشد. در این صورت،

۱- برای هر عدد طبیعی m، G زیرگروهی m عضوی دارد اگر و تنها اگر $m \mid n$.

۲- اگر $m \mid n$، آنگاه G زیرگروهی منحصر به فرد با m عضو دارد.

۳- $< a^r > = < a^s >$ اگر و تنها اگر $(r,n) = (s,n)$.

اثبات

۱- فرض کنیم $m \mid n$. در این صورت $H = < a^{n/m} >$ زیر گروه مورد نظر است، زیرا (مراحل اثبات را توضیح دهید):

$$|H| = O(a^{n/m}) = \frac{n}{(n/m,n)} = \frac{n}{n/m} = m$$

برعکس، اگر $H \leq G$ و $|H| = m$، آنگاه، بنابر قضیه‌ی لاگرانژ، داریم $m \mid n$. یا چون H دوری است و، برای مثال، $H = < a^k >$. در این صورت (مراحل اثبات را توضیح دهید)

$$m = |H| = O(a^k) = \frac{n}{(k,n)} \Rightarrow n = m \cdot (k,n) \Rightarrow m \mid n$$

۲- فرض کنیم $m \mid n$. با توجه به اثبات بند ۱، $H = < a^{n/m} >$ از مرتبه‌ی m است. حال اگر $K = < a^k >$ نیز از مرتبه‌ی m باشد، آنگاه (مراحل زیر را توضیح دهید):

$$\begin{aligned} O(a^k) = m \Rightarrow a^{km} = e \Rightarrow n \mid km \\ \Rightarrow km = nl \Rightarrow k = l(n/m) \\ \Rightarrow a^k \in < a^{n/m} > = H \\ \Rightarrow K \subseteq H \end{aligned}$$

چون $|H| = |K|$ متناهی است، نتیجه بگیرید که $H = K$.

۳- مراحل اثبات زیر را توضیح دهید:

$$\begin{aligned} < a^r > = < a^s > \Leftrightarrow |< a^r >| = |< a^s >| \\ \Leftrightarrow O(a^r) = O(a^s) \\ \Leftrightarrow \frac{n}{(r,n)} = \frac{n}{(s,n)} \\ \Leftrightarrow (r,n) = (s,n) \end{aligned}$$

۱۶.۴.۲ بحث در کلاس

۱- بند ۱ قضیه‌ی بالا برای گروه‌های آبلی متناهی نیز برقرار است، ولی یکتایی بیان شده در بند ۲ چنین نیست. برای مثال گروه آبلی ولی غیر دوری K_4 دارای سه زیرگروه دو عضوی است.

۲- بندهای ۱ و ۲ بیان می‌کنند که تعداد زیرگروه‌های یک گروه دوری n عضوی دقیقاً برابر با تعداد مقسوم‌علیه‌های n، یعنی $d(n)$، است. برای مثال، تعداد زیرگروه‌های $\mathbb{Z}_4$ برابر با ۳، تعداد زیرگروه‌های $\mathbb{Z}_5$ (یا $\mathbb{Z}_p$) برابر با ۲، و تعداد زیرگروه‌های $\mathbb{Z}_{12}$ برابر با ۶ است.

۳- آیا همتای نتیجه‌ی ۱۳.۴.۲ برای گروه‌های دوری $(\mathbb{Z}_n; +_n)$ نیز برقرار است؟ یعنی، آیا می‌توانیم همه‌ی زیرگروه‌های هر گروه دوری $\mathbb{Z}_n$ را دقیقاً مشخص کنیم؟ بحث بعد از نتیجه‌ی زیر پاسخ مثبت به این سؤال است.

۱۷.۴.۲ نتیجـــه. فـــرض کنـــیم کـــه $G=<a>$ گروهـــی دوری از مرتبـــه‌ی n، و $\{k_1,k_2,\cdots,k_t\}$ مجموعه‌ی مقسوم‌علیه‌های n باشد. در این صورت،

۱- $Sub(G)=\{<a^{k_1}>,<a^{k_2}>,\cdots,<a^{k_t}>\}$ مجموعه‌ی همه‌ی زیرگروه‌های G است.

۲- رابطه‌ی ترتیبی در $Sub(G)$ به صورت زیر است:

$$<a^{k_i}>\subseteq<a^{k_j}> \quad \Leftrightarrow \quad k_j \mid k_i$$

۲- سوپریمم و اینفیمم در مشبکه‌ی $Sub(G)$ به صورت زیر هستند:

$$<a^{k_i}>\wedge<a^{k_j}>=<a^{k_i}>\cap<a^{k_j}>=<a^{[i,j]}>$$
$$<a^{k_i}>\vee<a^{k_j}>=<a^{(i,j)}>$$

اثبات. قضیه‌ها و فنون بالا را به کار ببرید.

۱۸.۴.۲ بحث در کلاس. حال ببینیم که چطور با استفاده از این نتیجـه مـی‌تـوانیم همـه‌ی زیرگروه‌های $\mathbb{Z}_n$ را بیابیم. ابتدا بند ۱ صورت نتیجه را برای $\mathbb{Z}_n$ می‌نویسیم.

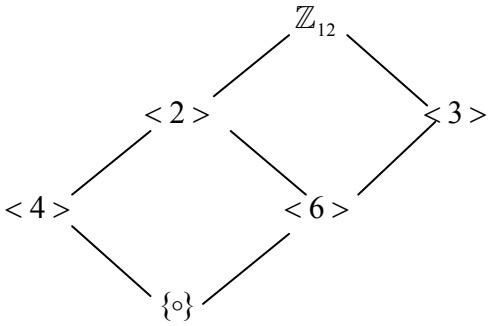
۱- روشن است که $a=1$ یکی از مولدهای گروه $\mathbb{Z}_n$ است. با قرار دادن $a=1$ در بند ۱ نتیجـه، داریم

$$Sub(G)=\{<k_1>,<k_2>,\cdots,<k_t>\}$$

۲- برای مثال، چون مقسوم‌علیه‌های ۱۲ عبارت‌اند از ۱، ۲، ۳، ۴، ۶، و ۱۲، پس زیرگروه‌های $\mathbb{Z}_{12}$ عبارت‌اند از

$$<1>=\mathbb{Z}_{12}, \qquad <2>=\{0,2,4,6,8,10\}$$
$$<3>=\{0,3,6,9\}, \qquad <4>=\{0,4,8\}$$
$$<6>=\{0,6\}, \qquad <12>=\{0\}=<0>$$

۳- با توجه با بندهای ۲ و ۳ نتیجه، نمودار مشبکه‌ی $Sub(\mathbb{Z}_{12})$ به صورت زیر است:



نتیجه‌ی جالب دیگری که می‌توان از قضیه‌های ۵.۴.۲ و ۱۵.۴.۲ به دست آورد، به صورت زیر است.

۱۹.۴.۲ نتیجه. اگر $G=<a>$ گروهی دوری با $|G|=n$ عضو و با مولد a باشد، آنگاه مولدهای دیگر آن به صورت a^r (یا در نماد جمعی ra) هستند که در آن $0<r<n$ و $(r,n)=1$. پس، تعداد مولدهای G برابر است با $\varphi(n)=|\{0<r<n\,|\,(r,n)=1\}|$ (که در آن φ، با همین تعریف، تابع فی اویلر نامیده می‌شود).

اثبات. این نیز روشن است (مراحل زیر را توضیح دهید):

$$\begin{aligned} G=<a^r> &\Leftrightarrow |<a^r>|=n \\ &\Leftrightarrow \frac{n}{(r,n)}=n \\ &\Leftrightarrow (r,n)=1 \end{aligned}$$

۲۰.۴.۲ بحث در کلاس. برای استفاده از نتیجه‌ی بالا در مورد $\mathbb{Z}_n$، مجدداً توجه می‌کنیم که $a=1$ یک مولد $\mathbb{Z}_n$ است. از این رو، برای پیدا کردن همه‌ی مولدهای گروه $\mathbb{Z}_{12}$، ابتدا توجه می‌کنیم که $(r,12)=1$ اگر و تنها اگر $r=1,5,7,11$. حال با قرار دادن $a=1$ و این اعداد در همتای جمعی عبارت $a^r=aa\cdots a$، یعنی $ra=a+a+\cdots+a$، همه‌ی مولدهای $\mathbb{Z}_{12}$ عبارت هستند از: $r1=1,5,7,11$.

شاید این مثال بدیهی چندان روش کار را نشان نداده باشد، مثال نابدیهی‌تری می‌آوریم. زیرگروه $H=<2>=\{0,2,4,6,\ldots,28\}$ از گروه $\mathbb{Z}_{30}=\{0,1,2,\cdots,29\}$ را در نظر می‌گیریم که در آن $a=2$. ابتدا باید $|H|$ را بیابیم. البته روشن است که در این مثال

$|H|=15$، ولی می‌خواهیم روش کلی کار را نشان دهیم. با توجه به مطالبی که در باره‌ی گروه‌های دوری می‌دانیم (دلایل هر مرحله از محاسبات زیر را توضیح دهید)، داریم

$$|H|=|<2>|=O_{\mathbb{Z}_{30}}(2)=\frac{30}{(2,30)}=\frac{30}{2}=15$$

حال $(r,15)=1$ اگر و تنها اگر $r=1,2,4,7,8,11,13,14$ و در نتیجه همه‌ی مولدهای H عبارت‌اند از $r.2=2,4,8,14,16,22,26,28$. برای مثال،

$$\begin{aligned}<16>&=\{1.16,2.16,3.16,\cdots,\\&=\{16,2,18,4,20,6,22,8,24,10,26,12,28,14,0\}\\&=H\end{aligned}$$

تمرین ۴.۲

تنها تماشاچی نباشید!

دسته‌ی اول

۱- فرض کنید که گروه دوری G تنها دارای یک مولد است. نشان دهید که $|G|\leq 2$.

۲- ثابت کنید که هر گروه G با $|G|\leq 5$ آبلی است. اگر $|G|=6$ چطور؟

۳- تعداد مولدهای گروه‌های دوری از مرتبه‌های ۱۷، ۶۰ و ۸۱ را بیابید.

۴- تعداد مولدهای هر یک از زیرگروه‌های دوری زیر را بیابید:

(الف) زیرگروه دوری $H=<25>$ از گروه $\mathbb{Z}_{30}$.

(ب) زیرگروه دوری $H=<a^{25}>$ از گروه دوری ۱۶۰ عضوی $G=<a>$.

(پ) زیرگروه دوری $H=<\frac{i+1}{\sqrt{2}}>$ از گروه ضربی $\mathbb{C}^*$.

۵- گروهی مثال بزنید که مرتبه‌ی هر عضو آن توانی از ۲ باشد.

۶- گروهی مثال بزنید که مرتبه‌ی هر عضو آن توانی از عدد اول p باشد.

۷- مثال‌هایی ارائه دهید که گزاره‌های زیر را نقض کنند:

(الف) اگر مرتبه‌ی هر عضو گروه G عدد طبیعی n را بشمارد، آنگاه $|G|$ عدد n را می شمارد.

(ب) اگر گروه G متناهی و هر زیرگروه اکید آن دوری باشد، آنگاه G دوری است.

(پ) اگر n مرتبه‌ی گروه متناهی G را بشمارد، آنگاه G دارای عضوی از مرتبه‌ی n است.

(ت) اگر گروه G شامل زیرمجموعه‌ی C باشد به طوری که $C^2 = C$ و $e \in C$، آنگاه C زیرگروه G است. یادآوری می‌کنیم که $C^2 = \{xy \mid x, y \in C\}$.

(ث) اگر هر زیرگروه اکید از گروه G متناهی باشد، آنگاه G نیز متناهی است.

۸- فرض کنید $G = \left\{ \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix} \mid n \in \mathbb{Z} \right\}$. نشان دهید که مجموعه‌ی G با عمل ضرب ماتریس‌ها گروهی آبلی است. همچنین، نشان دهید که G دارای عضوی ناهمانی از مرتبه‌ی متناهی نیست.

۹- فرض کنید گروه آبلی G از مرتبه‌ی pq باشد که در آن $(p,q) = 1$. ثابت کنید که اگر G دارای عضوهای a و b، به ترتیب از مرتبه‌های p و q، باشد آنگاه G دوری است.

دسته‌ی دوم

۱۰- گروهی نامتناهی مثال بزنید که مرتبه‌ی هر عضو آن متناهی باشد.

۱۱- فرض کنید که a تنها عضو گروه G باشد که $O(a) = n$. نشان دهید که $a \in Z(G)$.

۱۲- فرض کنید G گروهی از مرتبه‌ی n و m عددی طبیعی باشد به طوری که $(m,n) = 1$. ثابت کنید که برای هر $g \in G$، عضوی مانند $x \in G$ وجود دارد به طوری که $g = x^m$.

۱۳- فرض کنید G گروه است.

(الف) نشان دهید که اگر $a \in G$ و $O(a) = mn$، که در آن $(m,n) = 1$، آنگاه عضوهای $b, c \in G$ وجود دارند به طوری که $O(b) = m$، $O(c) = n$، و $a = bc = cb$.

(ب) تعمیم بند **(الف)** را با $O(a) = m_1 \cdots m_k$ بیان و آن را اثبات کنید.

۱۴- فرض کنید G گروهی از مرتبه‌ی n و m عددی طبیعی باشد به طوری که $(m,n) = 1$. در این صورت،

(الف) ثابت کنید که برای هر $a, b \in G$، اگر $a^m = b^m$ آنگاه $a = b$.

(ب) با ارائه‌ی مثالی نقض، نشان دهید که فرض $(m,n) = 1$ در بند **(الف)** ضروری است.

۱۵- فرض کنید که G گروهی از مرتبه‌ی فرد باشد. ثابت کنید که برای هر $a \in G$، معادله‌ی $x^2 = a$ دقیقاً دارای یک جواب در G است.

۱۶- فرض کنید که گروه آبلی G دارای عضوهایی از مرتبه‌های m و n باشد. نشان دهید که G دارای عضوی از مرتبه‌ی $[m,n]$ است.

۱۷- فرض کنید G گروهی آبلی و H، K دو زیرگروه دوری G باشند به طوری که $|H| = m$ و $|K| = n$. در این صورت،

(الف) نشان دهید که اگر $(m,n) = 1$، آنگاه G زیرگروهی دوری با mn عضو دارد.

(ب) همتای حکم **(الف)** را بدون شرط $(m,n) = 1$ بیان و آن را اثبات کنید.

۱۸- فرض کنید G گروه باشد، $x, y \in G$ و $xy = yx$. نشان دهید که اگر $O(x)$ و $O(y)$ متناهی باشند، آنگاه $O(xy)$ عدد $O(x)O(y)$ را می‌شمارد.

۱۹- فرض کنید G گروه باشد، $x, y \in G$ و $xy = yx$. نشان دهید که اگر $(O(x), O(y)) = 1$ آنگاه $O(xy) = O(x)O(y)$.

۲۰- فرض کنید که $\{e\}$ و G تنها زیرگروه‌های گروه G باشند. نشان دهید که $G = \{e\}$ یا G گروهی دوری از مرتبه‌ی عددی اول است.

۲۱- نشان دهید که اگر تعداد زیرگروه‌های گروه G متناهی باشد، آنگاه G متناهی است.

۲۲- فرض کنید که گروه دوری $G = < a >$ دارای n عضو است. نشان دهید که برای هر عدد طبیعی m، معادله ی $x^m = e$ در G دارای m جواب است اگر و تنها اگر $m \mid n$.

۲۳- فرض کنید G گروهی آبلی و متناهی باشد به طوری که برای هر عدد طبیعی n ، تعداد جواب های معادله‌ی $x^n = e$ حداکثر برابر با n است. ثابت کنید که G دوری است.

۲۴- فرض کنید مرتبه‌ی a در گروه G برابر با ۵ باشد. ثابت کنید که $C_G(a) = C_G(a^2)$.

۲۵- فرض کنید G گروهی متناهی و آبلی است. آیا مجموعه‌ی متشکل از عضو همانی و همه‌ی عضوهای گروه G که از مرتبه‌ی نامتناهی هستند یک زیرگروه از G تشکیل می‌دهد؟

۵.۲ همریختی و یک‌ریختی گروه‌ها

همریختی و یک‌ریختی دستگاه‌های جامع جبری را در بخش ۵.۱ معرفی و ویژگی‌های جامع آن‌ها را بررسی کردیم. دیدیم که، در حالت کلی، همریختی‌ها بین دستگاه‌های جبری توابعی هستند که عمل‌ها را حفظ می‌کنند. از این رو، تعریف زیر را برای مورد خاص گروه‌ها داریم.

۱.۵.۲ تعریف. فرض کنیم که $(G_1;*_{G_1})$ و $(G_2;*_{G_2})$ گروه باشند. در این صورت، تابع $\varphi: G_1 \to G_2$ همریختی گروهی است اگر حافظ عمل باشد، یعنی برای هر $x, y \in G_1$،

$$\varphi(x *_{G_1} y) = \varphi(x) *_{G_2} \varphi(y)$$

همریختی از گروه G به G را **درون‌ریختی**، همریختی یک به یک را **تکریختی**، همریختی پوشا را **بروریختی**، و همریختی دوسویی را **خودریختی** می‌نامیم.

۲.۵.۲ بحث در کلاس

۱- مطابق قراردادهایمان، معمولاً $*$ها را در عبارت بالا حذف می‌کنیم و به صورت ساده‌ی زیر می‌نویسیم و اشتباهی نیز پیش نمی‌آید:

$$\varphi(xy) = \varphi(x)\varphi(y)$$

۲- فرض کنیم که تعریف گروه ۳.۱.۲ را در نظر بگیریم، که در آن گروه را به صورت دستگاه جبری $(G;*,^{-1},e)$ از نوع $\tau = (2,1,0)$ معرفی می‌کند. توجه می‌کنیم که تعریف ۱.۵.۲ صرفاً حفظ عمل دوتایی $*$ را شرط همریختی بودن φ بیان می‌کند. حال این سؤال مطرح می‌شود که چرا حفظ دو عمل دیگر یکانی و صفرتایی را شرط همریختی بودن بین گروه‌ها قرار نداده‌ایم؟ قضیه‌ی ۵.۵.۱ پاسخ به این سؤال است: اتحادهای (گ۱) – (گ۳) به کمک هم آنقدر توانمند هستند که همریختی $\varphi: G_1 \to G_2$ به خودی خود حافظ عضو همانی و وارون‌ها نیز می‌شود! یعنی، $\varphi(e_1) = e_2$ و $\varphi(x^{-1}) = \varphi(x)^{-1}$ (اثبات ساده‌ی آن را یک بار دیگر ارایه دهید). از این رو، می‌توانید نشان دهید که برای هر توان x^k، که در آن k عددی صحیح (مثبت، صفر، یا منفی) است، داریم $\varphi(x^k) = \varphi(x)^k$. این مطلب را بسیار به کار خواهیم برد.

۳- قضیه‌ی مهم ۱۱.۵.۱ و اثبات جالب آن را یادآوری می‌کنیم که برای همه‌ی دستگاه‌های جبری، به ویژه گروه‌ها، بیان می‌کند که برای هر همریختی دوسویی (یعنی یک‌ریختی) $\varphi: G_1 \to G_2$، تابع وارون آن $\varphi^{-1}: G_2 \to G_1$ نیز یک همریختی است. (اثبات ساده ولی جالب آن را یک بار دیگر ارائه دهید.)

۴- روشن است که اگر تابع دوسویی $\varphi : G_1 \to G_2$ بین گروه‌ها، جدول کیلی G_1 را به جدول کیلی G_2 تبدیل کند، آنگاه φ حافظ عمل، و در نتیجه یک‌ریختی است. این مطلب گواه بر درستی بند **۲** بحث **۱۲.۳.۱** است.

۵- مثال‌های همریختی دستگاه‌های جامع جبری را در بخش **۵.۱** دیدیم. در زیر چند مثال مربوط به گروه‌ها را می‌آوریم. مثال‌های بسیاری را به مرور و در حین آموزش نکته‌های جدید، خواهیم آورد.

(الف) به آسانی می‌توانید نشان دهید که تابع ثابت $\varphi : G_1 \to G_2$ بین گروه‌ها با تعریف $\varphi(x) = e_2$، برای هر $x \in G_1$، همریختی است. ولی هیچ تابع ثابت دیگر $G_1 \to G_2$ همریختی گروهی نیست. **چرا؟**

(ب) می‌خواهیم ببینیم که چه همریختی‌هایی از گروه جمعی $(\mathbb{Q};+)$ به گروه جمعی $(\mathbb{Z};+)$ وجود دارند؟ روشن است که تابع ثابت صفر، یعنی $\varphi : \mathbb{Q} \to \mathbb{Z}$ با تعریف $\varphi(x) = 0$، همریختی است (زیرا، $\varphi(x+y) = 0 = 0+0 = \varphi(x)+\varphi(y)$). ادعا می‌کنیم که **هیچ همریختی دیگری وجود ندارد!** فرض کنیم $\psi : \mathbb{Q} \to \mathbb{Z}$ یک همریختی باشد. ابتدا نشان می‌دهیم که اگر $\psi(1) = 0$ آنگاه $\psi = 0$. زیرا، اگر $\psi(1) = 0$، آنگاه، چون ψ عمل $+$ در $\mathbb{Q}$ را حفظ می‌کند، برای هر $n \in \mathbb{N}$ داریم

$$0 = \psi(1) = \psi(\frac{n}{n}) = \psi(\frac{1}{n} + \cdots + \frac{1}{n}) = \psi(\frac{1}{n}) + \cdots + \psi(\frac{1}{n})$$

و در نتیجه $\psi(\frac{1}{n}) = 0$ (**چرا؟**). حال برای هر $m, n \in \mathbb{N}$،

$$\psi(\frac{m}{n}) = \psi(\frac{1}{n} + \cdots \frac{1}{n}) = \psi(\frac{1}{n}) + \cdots + \psi(\frac{1}{n}) = 0$$

حال، به آسانی می‌توانید نشان دهید که $\psi = 0$.

بنابراین، اگر همریختی دلخواه ψ ناصفر باشد، آنگاه $\psi(1) = k \neq 0$ و در نتیجه، برای هر عدد طبیعی $n \in \mathbb{N}$،

$$k = \psi(1) = \psi(\frac{n}{n}) = \psi(\frac{1}{n}) + \cdots + \psi(\frac{1}{n}) = n \cdot \psi(\frac{1}{n})$$

یعنی، هر عدد طبیعی n عدد طبیعی k را می‌شمارد، که تناقض است (**چرا؟**) در نتیجه، تنها همریختی از گروه $(\mathbb{Q};+)$ به گروه $(\mathbb{Z};+)$ همریختی بدیهی صفر است! **جالب بود؟!** روشن است که گروه $(\mathbb{Q};+)$ نمی‌تواند با گروه $(\mathbb{Z};+)$ یک‌ریخت باشد، در حالی که در درس مبانی علوم ریاضی دیدیم که **مجموعه**ی $\mathbb{Q}$ با **مجموعه**ی $\mathbb{Z}$ یک‌ریخت (همتوان) است.

(پ) تابع دترمینان از گروه جمعی ماتریس‌های حقیقی $n\times n$ به گروه جمعی $(\mathbb{R};+)$ همریختی نیست، زیرا ماتریس‌های $n\times n$، A و B وجود دارند به طوری که $\det(A+B)\neq \det(A)+\det(B)$.

(ت) تابع دترمینان از گروه ضربی **خطی عام** $GL(n,\mathbb{R})$ (یعنی، ماتریس‌های حقیقی $n\times n$ وارون‌پذیر) به گروه ضربی اعداد حقیقی $(\mathbb{R}^*;\cdot)$، همریختی است. **چرا؟**

حال ببینیم که تاثیر همریختی‌ها بر زیرگروه‌ها چگونه است. بحث **۶.۵.۱** و قضیه‌ی **۸.۵.۱** را مرور کنید.

۳.۵.۲ قضیه. فرض کنیم $\varphi: G_1 \to G_2$ همریختی گروهی باشد. در این صورت،

۱- همریختی φ زیرگروه‌ها را حفظ می‌کند. یعنی،

$$H \leq G_1 \Rightarrow \varphi(H) \leq G_2$$

به ویژه، $\varphi(G_1) \leq G_2$.

۲- همریختی φ زیرگروه‌ها را بازتاب می‌دهد. یعنی،

$$K \leq G_2 \Rightarrow \varphi^{-1}(K) = \bar{\varphi}(K) \leq G_1$$

به ویژه، $\varphi^{-1}(\{e_{G_2}\}) = \bar{\varphi}(e_{G_2}) = \{x \in G_1 \mid \varphi(x) = e_{G_2}\} \leq G_1$.

اثبات. مبتدیان گاهی با نگاره‌ی معکوس اندکی مشکل دارند. از این رو، قسمت اول حکم **۲** را اثبات و بقیه‌ی احکام (به ویژه اثبات مستقیم قسمت دوم حکم **۲**) را به عهده‌ی شما خوبان می‌گذاریم. (توجه کنید که، از آنجا که عضوهای $x \in \varphi(H)$ به صورت $x = \varphi(h)$ هستند، که در آن $h \in H$، مبتدیان عضوهای $x \in \varphi^{-1}(K)$ را نیز به اشتباه به صورت $x = \varphi^{-1}(k)$ می‌نویسند، در حالی که باید از این مطلب استفاده کنند که $x \in \varphi^{-1}(K)$ اگر و تنها اگر $\varphi(x) \in K$.)

۲- برای اثبات بسته بودن $\tilde{\varphi}(K)$ نسبت به عمل G_1، فرض می‌کنیم $x, y \in \tilde{\varphi}(K)$، یعنی $\varphi(x), \varphi(y) \in K$. چون φ همریختی است و K نسبت به عمل G_2 بسته است، پس داریم $\varphi(xy) = \varphi(x)\varphi(y) \in K$. در نتیجه، بنابر تعریف $\tilde{\varphi}(K)$، $xy \in \tilde{\varphi}(K)$. برای اثبات $e_{G_1} \in \tilde{\varphi}(K)$، توجه می‌کنیم که $\varphi(e_{G_1}) = e_{G_2} \in K$. در مورد وارون‌ها، فرض می‌کنیم که $x \in \tilde{\varphi}(K)$، یعنی $\varphi(x) \in K$. حال، چون $\varphi(x^{-1}) = \varphi(x)^{-1} \in K$، پس $x^{-1} \in \varphi^{-1}(K)$ و حکم اثبات شده است.

در قسمت پایانی این بخش، دسته‌بندی گروه‌های دوری را که قول داده بودیم انجام می‌دهیم. در اثبات قضیه‌ی زیر و بحث پس از آن فنونی می‌آموزیم که در درس جبرخطی نیز به کار می‌آیند. این فنون را در بخش ۸ از فصل ۱ نیز دیدیم.

۴.۵.۲ قضیه

۱- فرض کنیم $G_1 = < a >$ گروهی دوری و $\varphi : G_1 \to G_2$ همریختی گروهی باشد. در این صورت، $\varphi(G_1)$ نیز گروهی دوری و با مولد $b = \varphi(a)$ است. البته اگر φ پوشا باشد، آنگاه $G_2 = < b >$ نیز دوری است.

۲- فرض کنیم که $G_1 = < a >$ و $\varphi_1, \varphi_2 : G_1 \to G_2$ همریختی باشند به طوری که $\varphi_1(a) = \varphi_2(a)$. در این صورت، $\varphi_1 = \varphi_2$.

اثبات

۱- فرض کنیم $\varphi(x) \in \varphi(G_1)$، که در آن $x \in G_1$. چون $x \in G_1 = < a >$، پس $x = a^n$، که در آن $n \in \mathbb{Z}$. چون φ همریختی است، و در نتیجه عمل دوتایی گروه، عضو همانی، و وارون‌ها را حفظ می‌کند، داریم $\varphi(x) = \varphi(a^n) = \varphi(a)^n = b^n$، و در نتیجه $\varphi(G_1) = < \varphi(a) >$.

۲- روشن است (مراحل زیر را توضیح دهید):

$$\begin{aligned} x \in G_1 = < a > \Rightarrow (\exists k \in \mathbb{Z}) \quad & x = a^k \\ \Rightarrow \varphi_1(x) &= \varphi_1(a^k) = (\varphi_1(a))^k \\ = (\varphi_2(a))^k &= \varphi_2(a^k) = \varphi_2(x) \end{aligned}$$

۵.۵.۲ بحث در کلاس. نتایج زیر حاصل از قضیه‌ی بالا هستند.

۱- هیچ همریختی پوشا از یک گروه دوری به یک گروه غیر دوری وجود ندارد!

۲- همریختی $\varphi: G \to H$ بین گروه‌های دوری پوشا است اگر و تنها اگر φ **هر** مولد گروه دوری G را بر مولدی از گروه دوری H بنگارد. **چطور؟**

۳- (**جالب است**) همریختی $\varphi: G \to H$ بین گروه‌های دوری پوشا است اگر و تنها اگر φ **دست کم یک** مولد گروه دوری G را بر مولدی از گروه دوری H بنگارد. **چطور؟**

۴- فرض کنیم $|G|=|H|$. در این صورت، هر همریختی پوشای $\varphi: G \to H$ بین گروه‌های دوری دوسویی است.

۵- تنها دو همریختی پوشا از گروه دوری $\mathbb{Z}$ به گروه دوری $\mathbb{Z}$ وجود دارند! **چطور؟** آن دو همریختی را تعریف می‌کنید. (بند **۱** قضیه‌ی بالا و بند **۲** این بحث را ببینید.)

۶- چند همریختی پوشا (و لذا یک‌ریختی) از $\mathbb{Z}_n$ به خودش وجود دارد؟

کیک این بخش را با بیان قضیه‌ی زیر که در ابتدای بخش قول دادیم می‌خوریم. اثبات ساده آن را به عهده‌ی شما می‌گذاریم.

۶.۵.۲ قضیه

۱- اگر گروه دوری $G = < a >$ نامتناهی باشد، آنگاه $G \cong \mathbb{Z}$.

۲- اگر گروه دوری $G = < a >$ متناهی با n عضو باشد، آنگاه $G \cong \mathbb{Z}_n$.

اثبات. تابع با ضابطه‌ی $\varphi(a) = a^n$ را به کار ببرید. اثبات قضیه‌ی **۵.۴.۲** را نیز ببینید.

۷.۵.۲ بحث در کلاس

۱- نشان دهید که گروه‌های $\mathbb{R}$، $\mathbb{R}^*$، $\mathbb{C}$، $\mathbb{C}^*$ دوری نیستند.

۲- گروه‌های دوری جمعی $< \pi > = \{n\pi \mid n \in Z\}$ و ضربی $\{\pi^n \mid n \in Z\}$ با کدام گروه دوری یک‌ریخت هستند؟

۸.۵.۲ بحث در کلاس. این بخش را با مطالب مهم زیر به پایان می‌بریم. **چگونه نشان دهیم که دو گروه یک‌ریخت هستند یا نیستند؟** روشن است که اگر تابعی چون φ از گروه

G_1 به گروه G_2 داده شده باشد و بخواهیم نشان دهیم که φ یک‌ریختی است باید نشان دهیم که دوسویی و همریختی است؛ یعنی، برای هر $x, y \in G_1$

$$\varphi(xy) = \varphi(x)\varphi(y)$$

ولی اگر φ داده نشده باشد چطور آن را پیدا کنیم ؟ این کار اغلب بسیار مشکل است!

فرض کنیم تابع φ داده شده است و می‌خواهیم نشان دهیم که یک‌ریختی بین گروه‌ها نیست. کافی است ثابت کنیم که دارای یکی از شرط‌های یک به یک، پوشا، یا همریختی نیست. گاهی این کار نیز چندان ساده نیست! برای مثال، چطور دو عضو متفاوت $a, b \in G_1$ بیابیم به طوری که $\varphi(a) = \varphi(b)$؟ یا چطور عضوی چون $a \in G_1$ بیابیم که با هیچ عضو متعلق به G_2 توسط φ پوشیده نشود؟ شاید از این هر دو مشکل‌تر این باشد که دو عضو $a, b \in G_1$ بیابیم به طوری که $\varphi(ab) \neq \varphi(a)\varphi(b)$! مشاهده می‌کنیم که حتی اگر تابع φ داده شده باشد، گاهی کار چندان ساده‌ای نیست که نشان دهیم این تابع یک‌ریختی نیست! اغلب رجوع به بحث‌ها و قضیه‌هایی که در بالا آوردیم، یا بعدها در این درس و درس‌های دیگر خواهند آمد، ساده‌تر است. برای مثال، شاید باید ابتدا ببینیم که آیا φ عضو همانی گروه G_1 را به عضو همانی گروه G_2 می‌نگارد یا نه؟

حال فرض کنیم که بخواهیم نشان دهیم که دو گروه G_1 و G_2 یک‌ریخت نیستند. این کار گاهی بسیار مشکل‌تر از حالت‌های بالا است! اگر به گونه‌ای بدانیم که هیچ تابع دوسویی بین دو مجموعه‌ی زمینه‌ی این دو گروه وجود ندارد (مانند وقتی که $|G_1| \neq |G_2|$ ، برای مثال وقتی که G_1 و G_2 متناهی هستند ولی تعداد عضوهای آن‌ها یکسان نیست، یا یکی شمارا و دیگری ناشمارا است) مساله حل است. ولی اگر توابع دوسویی بین دو گروه وجود داشته باشند چطور؟ برای مثال، آیا همه‌ی گروه‌های متناهی n عضوی یک‌ریخت هستند؟ یا آیا گروه‌های جمعی و شمارای $\mathbb{Z}$ و $\mathbb{Q}$ یک‌ریخت هستند؟ گاهی ممکن است، مانند بند **۵(ب)** بحث **۲.۵.۲**، بتوانیم اثبات کنیم که، اگر چه توابع دوسویی بین دو گروه وجود دارند (در این مثال، بین $\mathbb{Z}$ و $\mathbb{Q}$)، ولی هیچ کدام نمی‌تواند **همریختی** باشد!

در این موارد، یک ابزار دیگر این است که به دنبال یک **ویژگی جبری** باشیم که یکی از گروه‌ها داشته باشد ولی دیگری فاقد آن است. نمونه‌هایی از این نوع ویژگی‌ها را در بحث‌ها و قضیه‌های بالا آوردیم و تعدادی را نیز در تمرین‌های زیر، مطالب بخش‌های دیگر، و در درس‌های دیگر می‌آوریم. برای مثال، چون گروه $\mathbb{Z}_4$ دوری است ولی گروه کلاین K_4 دوری نیست، بنابر تمرین **۱** زیر، این دو گروه نمی‌توانند یک‌ریخت باشند. البته، دو گروه ممکن است در یک یا چند ویژگی گروهی شریک باشند، ولی یک‌ریخت نباشند. به هر حال، روشن است که هر چه تعداد بیش‌تری از این نوع ویژگی‌ها در دسترس باشند، در این مورد و موارد دیگر موفق‌تر هستیم.

تمرین ۵.۲

دسته‌ی اول

۱- فرض کنید که دو گروه G_1 و G_2 یک‌ریخت هستند. نشان دهید که **(الف)** G_1 آبلی است اگر و تنها اگر G_2 آبلی باشد. **(ب)** G_1 دوری است اگر و تنها اگر G_2 دوری باشد. **(پ)** هر عضو G_1 وارون خودش است اگر و تنها اگر هر عضو G_2 وارون خودش باشد.

۲- با استفاده از بند **(الف)** تمرین **۱** نشان دهید که دو گروه $\mathbb{Z}_6$ و S_6 یک‌ریخت نیستند.

۳- با استفاده از بند **(ب)** تمرین **۱** نشان دهید که دو گروه $\mathbb{Z}_4$ و K_4 یک‌ریخت نیستند.

۴- تحقیق کنید که از توابع زیر کدام‌ها همریختی روی گروه $(\mathbb{Z};+)$ هستند:

$$f(n)=2n, \qquad g(n)=n+1, \qquad h(n)=n^2$$

۵- نشان دهید که تابع زیر روی گروه G لزوماً همریختی نیست. حدس بزنید که تحت چه شرط لازم و کافی همریختی است:

$$(\forall x\in G)\quad f(x)=x^{-1}$$

۶- فرض کنید $\varphi: G_1 \to G_2$ همریختی گروهی باشد. نشان دهید که،

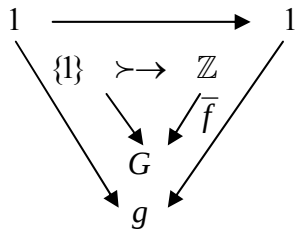
(الف) برای هر $x\in G_1$، اگر $O_{G_1}(x)=n<\infty$، آنگاه $O_{G_2}(\varphi(x)) \mid n$.

(ب) اگر φ یکریختی باشد، آنگاه $O_{G_1}(x)=O_{G_2}(\varphi(x))$.

۷- برای هر عدد صحیح n، تابع $f_n:\mathbb{Z}\to\mathbb{Z}$ را با ضابطه‌ی $f_n(x)=n+x$ در نظر بگیرید. نشان دهید که مجموعه‌ی $\{f_n \mid n\in\mathbb{Z}\}$ همراه با عمل ترکیب توابع یک گروه است و با گروه $(\mathbb{Z};+)$ یک‌ریخت است.

دسته‌ی دوم

۸- ($\mathbb{Z}$ در کلاس گروه‌ها **آزاد** است) فرض کنید G گروهی دلخواه باشد. نشان دهید که برای هر $g\in G$ یک همریختی منحصر به فرد چون $\overline{f}:\mathbb{Z}\to G$ با ویژگی $\overline{f}(1)=g$ وجود دارد. نمودار زیر را ببینید:



نشان دهید که گروه $\mathbb{Z}_n$ در کلاس گروه‌ها آزاد نیست. آیا هیچ گروه متناهی می‌تواند آزاد باشد. بحث **۹.۸.۱** را نیز ببینید.

۹- (تعمیم قضیه‌ی **۴.۵.۲**) فرض کنید که $\varphi : G \to H$ همریختی گروهی باشد و $G = < X >$. نشان دهید که

(الف) $\varphi(G) = < \varphi(X) >$.

(ب) اگر $\varphi_1, \varphi_2 : G \to H$ همریختی باشند به طوری که برای هر $x \in X$، $\varphi_1(x) = \varphi_2(x)$. نشان دهید که $\varphi_1 = \varphi_2$.

۱۰- فرض کنید a عضوی در گروه G است. نشان دهید که تابع زیر خودریختی است (توجه می‌کنیم که، $axya^{-1} = (axa^{-1})(aya^{-1})$):

$$\rho_a : G \to G$$
$$x \mapsto axa^{-1}$$

گاهی می‌نویسیم $x^a = axa^{-1}$. این نوع خودریختی‌ها را **خودریختی درونی** می‌نامیم.

۱۱- فرض کنید $Aut(G)$ و $Inn(G)$، به ترتیب، مجموعه‌ی خودریختی‌ها و مجموعه‌ی خودریختی‌های درونی G باشند. نشان دهید که این دو مجموعه، همراه با ترکیب توابع، گروه تشکیل می‌دهند.

۱۲- فرض کنید G گروهی متناهی و $\varphi : G \to H$ همریختی پوشا باشد. ثابت کنید که مرتبه‌ی H مرتبه‌ی G را می‌شمارد.

۱۳- فرض کنید G گروهی آبلی از مرتبه‌ی عددی فرد و $\psi : G \to G$ یک خودریختی از مرتبه‌ی۲ باشد (یعنی، $\psi \circ \psi = id_G$). ثابت کنید که هر عضو $g \in G$ را می‌توان به طور یکتا به صورت $g = xy$ نوشت، که در آن $\psi(x) = x$ و $\psi(y) = y^{-1}$.

۱۴- فرض کنید G گروهی دلخواه باشد. ثابت کنید که برای هر $\psi_a, \psi_b \in Inn(G)$، که در آن $a,b \in G$، تساوی $\psi_a = \psi_b$ برقرار است اگر و تنها اگر $ab^{-1} \in Z(G)$.

۱۵- فرض کنید که $(G;*_G)$ گروهی دلخواه و $(A;*_A)$ گروهی آبلی است. مجموعه‌ی همه‌ی همریختی‌های از G به A را با $Hom(G,A)$ نشان می‌دهیم. ثابت کنید که $Hom(G,A)$ همراه با عمل

$$(fg)(x) = f(x) *_A g(x)$$

برای $f, g \in Hom(G,A)$، گروهی آبلی است و $Hom(\mathbb{Z}, A) \cong A$.

۱۶- فرض کنید $G = \{x \in \mathbb{R} \mid x^2 < 1\}$. نشان دهید که مجموعه‌ی G همراه با عمل

$$x * y = \frac{x+y}{1+xy}$$

گروهی آبلی، و با گروه جمعی $(\mathbb{R};+)$ یک‌ریخت، است. (از تابع $f : G \to \mathbb{R}$ با ضابطه‌ی $f(x) = Ln\left(\frac{1+x}{1-x}\right)$ استفاده کنید).

۱۷- فرض کنید S مجموعه‌ی ماتریس‌های 2×2 حقیقی مانند X باشد به طوری که $X + I$ وارون‌پذیر است (که در آن I ماتریس همانی است) نشان دهید که S همراه با عمل

$$A * B = A + B + AB \qquad (A, B \in S)$$

گروه تشکیل می‌دهد. سپس، ثابت کنید که گروه S با گروه ضربی همه‌ی ماتریس‌های حقیقی 2×2 وارون‌پذیر یک‌ریخت است.

۱۸- فرض کنید که دو گروه G و H یک‌ریخت هستند. ثابت کنید که $Aut(G) \cong Aut(H)$. آیا عکس این مطلب درست است؟ **چرا؟**

۱۹- فرض کنید G گروهی با مرکز بدیهی است. ثابت کنید که $C_{Aut(G)}(Inn(G)) = \{id_G\}$. نتیجه بگیرید که $Z(Aut(G)) = \{id_G\}$.

۶.۲ گروه جایگشت‌ها

همان طور که در بحث ۴.۱.۲(چ) دیدیم، روشن است که مجموعه‌ی S_X متشکل از همه‌ی توابع دوسویی روی X همراه با عمل ترکیب توابع، گروه تشکیل می‌دهد. این گروه و هر زیرگروه آن را گروهی از جایگشت‌های روی X نامیدیم. همچنین، اگر $X=\{1,2,\cdots,n\}$، آنگاه S_X را با S_n نشان دادیم و آن را **گروه جایگشت‌های** روی n شیء یا **گروه متقارن** درجه‌ی n نامیدیم. این گروه‌ها حتی قبل از معرفی مفهوم مجرد گروه به کار می‌رفتند. ریاضی‌دانانی از جمله لاگرانژ، کشی، آبل، و از همه مهم‌تر، گالوا در جستجوی جواب‌های معادله‌های چندجمله‌ای، جایگشت‌ها را به کمک گرفتند و به نتایج مفیدی دست پیدا کردند. مطالعه‌ی عمیق این مطالب، نظریه‌ی گالوا را به وجود آورد که خود کتاب‌های مفصل دیگری را می‌طلبد.

این تلاش‌ها منجر به معرفی و پرورش نظریه‌ی مجرد گروه‌ها شد. ریاضی‌دان انگلیسی، آرتور کیلی، جنبه‌ی دیگری از اهمیت گروه‌های جایگشت‌ها را به نمایش می‌گذارد و نشان می‌دهد که هر گروه مجرد G (متناهی یا نامتناهی) با گروهی از جایگشت‌ها یکریخت است! **خیلی جالب است، نیست؟** این قضیه را در این بخش اثبات می‌کنیم. با توجه به این سابقه‌ی تاریخی و به دلیل کاربردهای بسیارگروه جایگشت‌ها (برای مثال، در ترکیبیات) به حق است که یک بخش هر چند کوتاه را به مطالعه‌ی آن‌ها اختصاص دهیم. البته به دلیل کمبود وقت، برخی از قضیه‌ها را اثبات نمی‌کنیم.

۱.۶.۲ بحث در کلاس

۱- ابتدا، برای راحتی کار محاسبات، نمادگذاری زیر را به کار می‌بریم. هر جایگشت $\sigma \in S_n$ را می‌توانیم با نماد دوخطی زیر نشان دهیم:

$$\sigma=\begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \cdots & \sigma(n) \end{pmatrix}$$

جایگشت همانی را به طور ساده با $\rho_\circ=(1)$ نشان می‌دهیم. پس

$$id_X=\rho_\circ=(1)=\begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ 1 & 2 & 3 & \cdots & n \end{pmatrix}$$

توجه می‌کنیم که، چون هر جایگشت σ دوسویی است، پس هر عضو $\{1,2,\cdots,n\}$ در سطر دوم نمایش دوخطی σ نیز یک و تنها یک بار رخ می‌دهد.

۲- برای محاسبه‌ی σ^{-1} کافی است ابتدا جای دو سطر σ را با هم عوض کنیم و سپس ستون‌ها را طوری مرتب کنیم که سطر اول به صورت متعارف از ۱ تا n نوشته شود. برای مثال،

$$\begin{pmatrix}1&2&3&4&5\\2&4&5&1&3\end{pmatrix}^{-1}=\begin{pmatrix}2&4&5&1&3\\1&2&3&4&5\end{pmatrix}$$
$$=\begin{pmatrix}1&2&3&4&5\\4&1&5&2&3\end{pmatrix}$$

۳- روشن است که حاصل‌ضرب (یعنی ترکیب) دو جایگشت $\sigma,\delta\in S_n$ در نمادگذاری متداول ترکیب توابع به صورت $(\sigma\circ\delta)(x)=\sigma(\delta(x))$ تعریف می‌شود، یعنی ابتدا تابع سمت راست یعنی δ بر x اثر و سپس σ بر حاصل $\delta(x)$ اثر می‌کند. برای مثال، داریم

$$\sigma\circ\delta=\begin{pmatrix}1&2&3&4&5\\2&4&5&1&3\end{pmatrix}\begin{pmatrix}1&2&3&4&5\\3&5&1&2&4\end{pmatrix}$$
$$=\begin{pmatrix}1&2&3&4&5\\\downarrow&\downarrow&\downarrow&\downarrow&\downarrow\\3&5&1&2&4\\\downarrow&\downarrow&\downarrow&\downarrow&\downarrow\\5&3&2&4&1\end{pmatrix}=\begin{pmatrix}1&2&3&4&5\\5&3&2&4&1\end{pmatrix}$$

زیرا، برای مثال، داریم $(\sigma\circ\delta)(1)=\sigma(\delta(1))=\sigma(3)=5$ و $(\sigma\circ\delta)(2)=\sigma(\delta(2))=\sigma(5)=3$. توجه می‌کنیم که در این نمادگذاری، پرانتزها را از پرانتز سمت راست به پرانتز سمت چپ به کار می‌بریم. برخی از ریاضی‌دانان نمادگذاری $x(\sigma\circ\delta)=(x\sigma)\delta$ را به کار می‌برند، که در این صورت در نمادگذاری حاصل‌ضرب جایگشت‌ها، پرانتزها، به ترتیب طبیعی‌تر، از چپ به راست به کار می‌روند.

۴- روشن است که $|S_n|=n!$. شش عضو گروه S_3 عبارت هستند از

$$\rho_\circ=\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix},\quad \rho_1=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix},\quad \rho_2=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$$

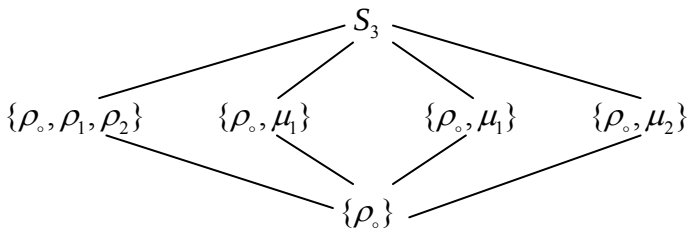
$$\mu_1=\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix},\quad \mu_2=\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix},\quad \mu_3=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}$$

با محاسبه می‌توانید نشان دهید که جدول گروه S_3 به صورت زیر است:

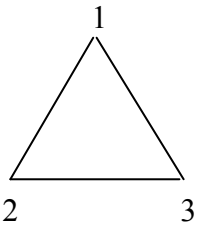
$\circ$	ρ_0	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_0	ρ_0	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_1	ρ_1	ρ_2	ρ_0	μ_3	μ_1	μ_2
ρ_2	ρ_2	ρ_0	ρ_1	μ_2	μ_3	μ_1
μ_1	μ_1	μ_2	μ_3	ρ_0	ρ_1	ρ_2
μ_2	μ_2	μ_3	μ_1	ρ_2	ρ_0	ρ_1
μ_3	μ_3	μ_1	μ_2	ρ_1	ρ_2	ρ_0

۵- نشان دهید که اگر $n \geq 3$، آنگاه برای هر $\sigma \in S_n$ دست کم یک $\delta \in S_n$ وجود دارد به طوری که $\sigma\delta \neq \delta\sigma$. به عبارت دیگر، نه تنها برای $n \geq 3$، S_n آبلی نیست، بلکه مرکز آن بسیار کوچک و در واقع برابر است با $Z(S_n) = \{\rho_0\}$ و در نتیجه فاصله‌ی زیادی با آبلی بودن دارد. یادآوری می‌کنیم که گروه G آبلی است اگر و تنها اگر $Z(G) = G$.

۶- با توجه به قضیه‌ی لاگرانژ، S_3 تنها می‌تواند زیرگروه‌هایی ۱، ۲، ۳، و ۶ عضوی داشته باشد، که اتفاقاً دارد. با مراجعه به جدول کیلی گروه S_3، و البته با کمی محاسبه، می‌توانید مشبکه‌ی زیرگروه‌های آن را به صورت زیر به دست آورید:



۷- چرا گروه جایگشت‌ها را گروه تقارن‌ها یا گروه متقارن نیز می‌نامند؟ مثلث سه ضلع مساوی زیر را در نظر بگیرید:



روشن است که این مثلث را می‌توان با سه دوران (نسبت به مرکز مثلث) و سه انعکاس نسبت به سه نیمساز زاویه‌ها (همان عمود منصف‌های اضلاع) بر خودش منطبق کرد. این شش دوران و

انعکاس را تقارن‌های مثلث می‌نامند. با شماره‌گذاری ۱، ۲، ۳ راس‌ها، سه دوران را می‌توان با ρ_0، ρ_1، ρ_2 و سه انعکاس را با μ_1، μ_2، و μ_3 نشان داد. همچنین، می‌توان نشان داد که این تقارن‌ها، نسبت به ترکیب، گروه S_3 را تشکیل می‌دهند.

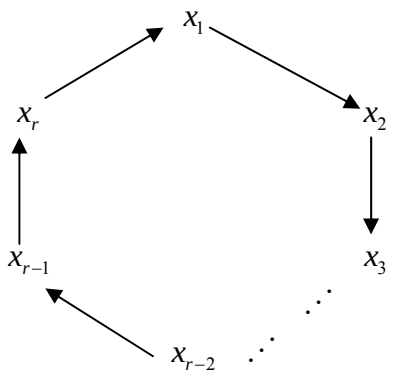
۷- حال گروه تقارن‌های مربع را محاسبه می‌کنیم. توجه می‌کنیم که مربع را می‌توان با چهار دوران (نسبت به مرکز مربع) و دو انعکاس نسبت به دو نیمساز زاویه‌ها و دو انعکاس نسبت به دو عمود منصف اضلاع بر خودش منطبق کرد. مانند مورد مثلث، با شماره‌گذاری ۱، ۲، ۳، ۴ راس‌های مربع، گروه تقارن‌های مربع را می‌توان زیرگروهی $4+4=2\times 4=8$ از گروه S_4 در نظر گرفت.

به طور کلی، هر n- ضلعی منتظم دارای $2n$ تقارن است (n دوران، و n انعکاس نسبت به عمود منصف‌ها و نسبت به نیمسازها) که، تحت ترکیب، زیرگروهی از S_n تشکیل می‌دهند. این گروه $2n$ عضوی را با D_n نشان می‌دهیم و آن را **گروه دو وجهی** مرتبه‌ی $2n$ (یا nامین گروه دو وجهی) می‌نامیم.

۲.۶.۲ تعریف. جایگشت σ روی مجموعه‌ی X را **جایگشت دوری** به طول r، یا یک r-**دور**، می‌نامیم اگر $x_1,\cdots,x_r\in X$ وجود داشته باشند به طوری که

$$\sigma(x_1)=x_2,\quad \sigma(x_2)=x_3,\quad \cdots,\quad \sigma(x_{r-1})=x_r,\quad \sigma(x_r)=x_1$$

و هر $x\notin\{x_1,\cdots,x_r\}$ تحت σ ثابت بماند، یعنی $\sigma(x)=x$:



معمولاً جایگشت دوری را به صورت ساده‌ی یک خطی $\sigma=(x_1,x_2,\cdots,x_r)$ نشان می‌دهیم. برای مثال، روشن است که

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

برای مثال،

$$\begin{pmatrix}1 & 2 & 3 & 4 & 5\\ 1 & 4 & 3 & 5 & 2\end{pmatrix} = (2,4,5) = (4,5,2) = (5,2,4)$$

۳.۶.۲ بحث در کلاس

۱- توجه می‌کنیم که اعدادی که در نمادگذاری یک خطی جایگشت دوری $\sigma \in S_n$ ظاهر نمی‌شوند، تحت σ ثابت می‌مانند. برای مثال $\rho_\circ = (1) = (2) = \cdots = (n)$، و در S_5،

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

یک جایگشت دوری به طول ۳ یعنی یک ۳- دور است که در آن ۲ و ۵ ثابت هستند. هر ۲- دور (a,b) را یک **ترانهش** می‌نامیم.

۲- مطلبی بسیار مهم (مشابه نوشتن اعداد طبیعی $n \geq 2$ به صورت حاصلضرب اعداد اول)، که می‌خواهیم به مرور در بندهای زیر نشان دهیم، این است که برای $n \geq 2$، **هر جایگشت $\sigma \in S_n$ را می‌توان به صورت حاصلضرب ترانهش‌ها نوشت.** ابتدا هر جایگشت

$$\sigma = \begin{pmatrix}1 & 2 & \cdots & n\\ \sigma(1) & \sigma(2) & \cdots & \sigma(n)\end{pmatrix}$$

را در مرحله‌های زیر به صورت حاصلضرب دورها می‌نویسیم.

(الف) جایگشت دوری $\delta_1 = (1, \sigma(1), \sigma(\sigma(1)), \cdots, 1)$ را تشکیل می‌دهیم.

(ب) کوچکترین عدد x را با شرط

$$x \in \{1,2,\cdots,n\} \setminus \{1, \sigma(1), \sigma(\sigma(1)), \cdots\}$$

در نظر بگیرید و جایگشت دوری $\delta_2 = (x, \sigma(x), \sigma(\sigma(x)), \cdots)$ را تشکیل دهید.

(پ) کوچکترین عدد y را با شرط

$$y \in \{1,2,\cdots,n\} \setminus \{1,\sigma(1),\sigma(\sigma(1)),\cdots,x,\sigma(x),\sigma(\sigma(x)),\cdots\}$$

در نظر بگیرید و با ادامه‌ی این روند، به نتیجه‌ی مطلوب $\sigma = \delta_k \cdots \delta_2 \delta_1$ می‌رسیم. برای مثال،

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 3 & 2 & 1 & 4 & 8 & 7 & 6 \end{pmatrix} = \begin{pmatrix} . & 2 & 3 & . & . & 6 & 7 & 8 \\ . & 3 & 2 & . & . & 8 & 7 & 6 \end{pmatrix} (1,5,4)$$
$$= \begin{pmatrix} . & . & . & . & . & 6 & 7 & 8 \\ . & . & . & . & . & 8 & 7 & 6 \end{pmatrix} (2,3)(1,5,4)$$
$$= \begin{pmatrix} . & . & . & . & . & . & 7 & . \\ & & & & & & & \\ . & . & . & . & . & . & 7 & . \end{pmatrix} (6,8)(2,3)(1,5,4)$$
$$= (7)\,(6,8)(2,3)(1,5,4)$$
$$= (6,8)(2,3)(1,5,4)$$

۳- هر r- دور با $r \geq 2$ را می‌توان به حاصل‌ضرب ترانهش‌ها نوشت. زیرا، به آسانی می‌توانید با محاسبه‌ی مستقیم ترکیب جایگشت‌ها (ضرب از راست به چپ پرانتزها) نشان دهید که

$$(x_1, x_2, \cdots, x_r) = (x_1, x_r)(x_1, x_{r-1}) \cdots (x_1, x_2)$$

برای مثال، $\rho_\circ = (1,2)(2,1) = (5,6)(6,5) = \cdots$. به طور کلی $\rho_\circ = (a,b)(b,a)$. به عنوان مثالی دیگر، در S_4 داریم

$$(1,2,3) = (1,3)(1,2) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix}$$
$$= \begin{pmatrix} 1 & 2 & 3 & 4 \\ \downarrow & \downarrow & \downarrow & \downarrow \\ 2 & 1 & 3 & 4 \\ \downarrow & \downarrow & \downarrow & \downarrow \\ 2 & 3 & 1 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix} = (1,2,3)$$

۴- با توجه به بندهای ۳ و ۴، برای $n \geq 2$، **هر جایگشت** $\sigma \in S_n$ **را می‌توان به صورت حاصل‌ضرب ترانهش‌ها نوشت.** برای مثال،

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 3 & 2 & 1 & 4 & 8 & 7 & 6 \end{pmatrix} = (7)(6,8)(2,3)(1,5,4)$$
$$= (6,8)(2,3)(1,5,4)$$
$$= (6,8)(2,3)(1,4)(1,5)$$

۵- همان طور که گفتیم و در مثال $\rho_\circ = (1,2)(2,1) = (5,6)(6,5) = \cdots$ نیز دیدیم، تجزیه‌ی جایگشت‌ها به حاصل‌ضرب ترانهش‌ها یکتا نیست. برای مثالی دیگر، می‌توانید به روش بالا نشان دهید که در S_4،

$$(1,2,3) = (1,3)(1,2) = (2,1)(2,3) = (2,1)(2,3)(1,2)(2,1) = \cdots$$

نکته‌ی جالب این است که به هر صورتی که جایگشتی را به ترانهش‌ها تجزیه کنیم، تعداد ترانهش‌ها **همواره زوج یا همواره فرد است** (اثبات رسمی این مطلب را نمی‌آوریم). از این رو، تعریف زیر را داریم.

۴.۶.۲ تعریف. اگر $\sigma \in S_n$ به حاصل‌ضرب تعدادی زوج ترانهش نوشته شود، آن را **زوج** و در غیر این صورت **فرد** می‌نامیم.

۵.۶.۲ بحث در کلاس

۱- چون $(x_1, x_2, \cdots, x_r) = (x_1, x_r)(x_1, x_{r-1}) \cdots (x_1, x_2)$، روشن است که هر r - دور زوج است اگر و تنها اگر r فرد باشد.

۲- جایگشت همانی زوج است، زیرا اگر $n = 1$ آنگاه $\rho_\circ$ به تعداد صفر ترانهش دارد و اگر $n \geq 2$ آنگاه $\rho_\circ = (1,2)(2,1)$. همچنین، به راحتی می‌توانید نشان دهید که حاصل‌ضرب دو جایگشت، فرد است اگر و تنها اگر دقیقاً یکی از آن‌ها فرد باشد، وارون هر ترانهش $\tau = (a,b)$ برابر با خودش است، وارون هر جایگشت σ زوج است اگر و تنها اگر σ زوج باشد. زیرا اگر $\sigma = \tau_k \cdots \tau_2 \tau_1$ حاصل ضرب تعدادی ترانهش باشد، آنگاه

$$\sigma^{-1} = (\tau_k \cdots \tau_2 \tau_1)^{-1} = \tau_1^{-1} \tau_2^{-1} \cdots \tau_k^{-1} = \tau_1 \tau_2 \cdots \tau_k$$

حال اگر A_n مجموعه‌ی جایگشت‌های زوج و B_n مجموعه‌ی جایگشت‌های فرد در S_n باشند، آنگاه B_n زیرگروه S_n نیست در حالی که A_n زیرگروه S_n است. حال قضیه‌ی زیر را ببینید.

۶.۶.۲ قضیه. برای $n \geq 2$، $|A_n| = |B_n|$.

اثبات. کافی است تابعی دوسویی چون $\varphi : A_n \to B_n$ تعریف کنیم. چون $n \geq 2$، ترانهش τ وجود دارد. حال φ را به صورت زیر تعریف می‌کنیم:

$$\begin{aligned} \varphi : A_n &\to B_n \\ \sigma &\mapsto \sigma\tau \end{aligned}$$

توجه می‌کنیم که، چون σ زوج است، $\sigma\tau$ فرد است. همچنین،

$$\begin{aligned} \varphi(\sigma_1) = \varphi(\sigma_2) &\Leftrightarrow \sigma_1\tau = \sigma_2\tau \\ &\Leftrightarrow \sigma_1\tau\tau^{-1} = \sigma_2\tau\tau^{-1} \\ &\Leftrightarrow \sigma_1 = \sigma_2 \end{aligned}$$

پس، φ خوش تعریف و یک به یک است. اثبات ساده و جالب پوشا بودن φ را به عهده‌ی شما می‌گذاریم.

۷.۶.۲ بحث در کلاس

۱- با توجه به قضیه‌ی بالا، $|A_n| = \frac{1}{2}n!$.

۲-گروه مهم A_n را **گروه متناوب** درجه‌ی n می‌نامیم.

۳- روشن است که $A_3 = \{\rho_0, \rho_1, \rho_2\}$.

بیش از این به ویژگی‌های جایگشت‌ها در این درس نمی‌پردازیم. ولی، در پاراگراف دوم مقدمه‌ی این بخش، قول دادیم که قضیه‌ی کیلی را اثبات کنیم. روشن است که نمایش یک شیء ریاضی با شیء ریاضی دیگری که کار کردن با آن ساده‌تر باشد یا برنامه‌های رایانه‌ای را نیز بتوان برای آن به کار برد، بسیار مفید است. قضیه‌ی کیلی، هر گروه را با گروهی از جایگشت‌ها **نمایش** می‌دهد که در کاربردها بسیار مفید است.

۸.۶.۲ قضیه هر گروه (متناهی یا نامتناهی) G با گروهی از جایگشت‌ها یکریخت است.

اثبات. یقیناً از این قضیه تعجب نخواهید کرد، زیرا در هر سطر جدول کیلی گروه G، هر عضو یک و تنها یک بار رخ می‌دهد. یعنی، هر سطر چیزی جز جایگشتی از عضوهای G نیست. حال خلاصه‌ای از اثبات را می‌آوریم. برای هر $a \in G$، تابع انتقال چپ

$$l_a : G \to G$$
$$x \mapsto ax$$

را در نظر می‌گیریم. همان طور که در تمرین‌های ۱۴ و ۱۵ از بخش ۱.۲ دیدیم، به راحتی می‌توانید نشان دهید که هر l_a یک جایگشت (دوسویی) است و $G_l = \{l_a \mid a \in G\}$ همراه با ترکیب توابع گروه است. توجه می‌کنیم که l_e عضو همانی این گروه است، و $l_a \circ l_b = l_{ab}$. زیرا

$$(l_a \circ l_b)(x) = l_a(l_b(x)) = l_a(bx) = a(bx) = (ab)x = l_{ab}(x)$$

و $(l_a)^{-1} = l_{a^{-1}}$. حال نشان می‌دهیم که تابع

$$\varphi : G \to G_l$$
$$a \mapsto l_a$$

یک‌ریختی گروهی است. اثبات زیر را برای یک به یک بودن φ توضیح دهید:

$$\varphi(a) = \varphi(b) \Rightarrow l_a = l_b \Rightarrow (\forall x \in G)\, l_a(x) = l_b(x)$$
$$\Rightarrow l_a(e) = l_b(e) \Rightarrow ae = be \Rightarrow a = b$$

پوشا بودن روشن است. **چطور؟** حال اثبات همریختی بودن را توضیح دهید:

$$\varphi(ab) = l_{ab} = l_a \circ l_b = \varphi(a) \circ \varphi(b)$$

۹.۶.۲ بحث در کلاس

۱- به روشی مشابه اثبات قضیه‌ی کیلی، می‌توان نشان داد که گروه G با گروه انتقال‌های راست $G_r = \{r_a \mid a \in G\}$ نیز یک‌ریخت است. (اثبات کنید، جالب است). گروه‌های G_r و G_l را، به ترتیب، **نمایش منظم راست** و **چپ** گروه G می‌نامیم. روشن است که اگر G آبلی باشد، $G_r = G_l$.

۲- هر گروه از مرتبه‌ی n با زیرگروهی از S_n یک‌ریخت است.

۳- برای نمونه، جایگشت‌های نمایش منظم گروه $\mathbb{Z}_4$ را بیابید. برای مثال، تابع انتقال راست r_2 هر عضو گروه $\mathbb{Z}_4$ را به اندازه‌ی ۲ انتقال می‌دهد:

$$\varphi(2)=r_2=\begin{pmatrix}\circ & 1 & 2 & 3\\ 2 & 3 & \circ & 1\end{pmatrix}$$

۴- با توجه به بند ۲ و متناهی بودن تعداد زیرگروه‌های S_n، برای هر عدد طبیعی n تنها تعدادی متناهی رده‌ی یک‌ریختی از گروه‌های n عضوی وجود دارند.

تمرین ۶.۲

رفته رفته تبحر شما بیش‌تر می‌شود

دسته‌ی اول

۱- با یک مثال نشان دهید که حاصل‌ضرب دو جایگشت دوری لزوماً دوری نیست.

۲- دو جایگشت دوری $\sigma=(x_1,\cdots,x_r)$ و $\delta=(y_1,\cdots,y_s)$ را **مجزا** می‌گوییم اگر $\{x_1,\cdots,x_r\}\cap\{y_1,\cdots,y_s\}=\varnothing$. برای مثال، در S_6، $(1,2)$ و $(3,4,5)$ مجزا هستند. نشان دهید که عمل ترکیب (ضرب) روی جایگشت‌های دوری مجزا تعویض‌پذیر است.

۳- فرض کنید که $\sigma,\delta\in S_n$ دو جایگشت دوری مجزا باشند. نشان دهید که

(الف) مرتبه‌ی هر جایگشت دوری برابر با طول آن است.

(ب) نشان دهیدکه $O(\sigma\delta)=[O(\sigma),O(\delta)]$.

(پ) ابتدا جایگشت زیر را به حاصل‌ضرب دورهای مجزا بنویسید و سپس، با استفاده از بندهای **(الف)** و **(ب)**، مرتبه‌ی آن را بیابید:

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

(ت) جایگشت‌های σ^{60} و σ^{62} را مشخص کنید.

۴- فرض کنید که

$$\sigma=\begin{pmatrix}1&2&3&4&5&6\\5&4&3&2&1&6\end{pmatrix}\quad,\quad \delta=\begin{pmatrix}1&2&3&4&5&6\\5&4&3&2&1&6\end{pmatrix}$$

حاصل ضرب‌های $\sigma\delta$، $\delta\sigma$، σ^{-1}، $\sigma^{-1}\delta^{-1}$، $\sigma^{100}\delta^{-61}$ را بیابید.

۵- جایگشت‌های σ و δ تمرین ۴ را به جایگشت‌های دوری و به ترانهش‌ها تجزیه و سپس زوج یا فرد بودن آن‌ها را مشخص کنید.

۶- فرض کنید که $Y\subseteq X$ و $y\in Y$ ثابت باشد. تعیین کنید که از مجموعه‌های زیر کدام(ها) زیرگروه S_X هستند:

(الف) $A=\{\sigma\in S_X\mid \sigma(y)=y\}$ (ب) $B=\{\sigma\in S_X\mid \sigma(y)\in Y\}$

(پ) $C=\{\sigma\in S_X\mid \sigma(Y)\subseteq Y\}$ (ت) $D=\{\sigma\in S_X\mid \sigma(Y)=Y\}$

دسته‌ی دوم

۷- ثابت کنید که $Aut(S_3)\cong Inn(S_3)\cong S_3$.

۸- فرض کنید $\sigma=(k_1,\cdots,k_r)$ جایگشتی دوری در گروه S_n باشد. ثابت کنید که برای هر $\delta\in S_n$، $\delta^{-1}\sigma\delta=(\delta(k_1),\ldots,\delta(k_r))$.

۹- فرض کنید $H\le S_n$. نشان دهید که همه یا دقیقاً نیمی از جایگشت‌های متعلق به H زوج هستند.

۱۰- ثابت کنید که برای $n>3$، هر عضو A_n را می توان به صورت حاصلضرب دورهای به طول ۳ نوشت. (توجه کنید که $(ab)(cd)=(cbc)(cdc)$).

۱۱- فرض کنید که جایگشت σ یک دور از مرتبه‌ی فرد است. ثابت کنید که σ^2 نیز یک دور است.

۱۲- فرض کنید H و K دو زیرگروه از مرتبه‌ی ۱۵ در گروه متقارن S_8 باشند به طوری که $H\cap K=\{e\}$. نشان دهید که $HK\neq KH$.

۱۳- فرض کنید که برای $n > 2$، گروه S_n دارای زیرگروه نابدیهی H باشد. ثابت کنید که $H \cap A_n \neq \{e\}$.

۷.۲ ضرب و همضرب گروه‌ها

در فصل ۱ چند روش ساختن دستگاه‌های جبری جدید را از دستگاه‌های جبری داده شده معرفی کردیم. یکی از این روش‌ها به گونه‌ای متصل کردن دستگاه‌ها به یکدیگر است. به صورت‌های متعدد می‌توان این کار را انجام داد، که یکی از آن‌ها ساختن حاصل‌ضرب دکارتی است که در بخش ۶.۱ معرفی شد. در این بخش این مفهوم و مفهوم هم‌ضرب را برای گروه‌ها با جزییات بیشتری مطالعه می‌کنیم.

علاوه بر ساختن گروه‌های جدید، مفهوم ضرب را می‌توان برای کسب اطلاعات در باره‌ی یک گروه نیز به کار برد. همان طور که تجزیه‌ی اعداد به اعداد اول، یا تجزیه‌ی جایگشت‌ها به جایگشت‌های ساده‌تر دوری یا ترانهش‌ها اطلاعات خوبی به دست می‌دهد، نوشتن یک گروه به حاصل‌ضرب گروه‌های کوچک‌تر، و به تعبیری ساده‌تر، اطلاعات مفیدی در باره‌ی خود گروه به دست می‌دهد.

حال تعریف ضرب داده شده در بخش ۶.۱ را برای گروه‌ها یادآوری می‌کنیم.

۱.۷.۲ قضیه و تعریف. فرض کنیم G_1 و G_2 گروه باشند. در این صورت $G_1 \times G_2$ همراه با عمل دوتایی **مولفه‌ای**

$$(g_1, g_2)(g_1', g_2') = (g_1 g_1', g_2 g_2')$$

یک گروه تشکیل می‌دهد. این گروه را **حاصل‌ضرب** (**دکارتی**) G_1 در G_2 می‌نامیم.

۲.۷.۲ بحث در کلاس

۱- تعمیم تعریف بالا به هر تعداد متناهی و نامتناهی گروه روشن است. معمولاً نمادهای زیر به کار می‌روند:

$$\prod_{i=1}^{n} G_i = G_1 \times G_2 \times \cdots G_n$$
$$\prod_{i\in I} G_i = \{f : I \to \bigcup_{i\in I} G_i \mid (\forall i \in I)\ f(i) \in G_i\}$$
$$\cong \{(g_i)_{i\in I} \mid (\forall i \in I) \quad g_i \in G_i\}$$

۲- توجه می‌کنیم که در تعریف ۱.۷.۲ بالا، عمل‌های گروه‌ها را، که ممکن است با هم متفاوت باشند، ننوشته‌ایم و معمولاً اشتباهی رخ نمی‌دهد. البته در مثال‌های مشخص، عمل‌ها را همان طور که داده شده‌اند می‌نویسیم و اجرا می‌کنیم. برای مثال، در $\mathbb{Z}_2 \times \mathbb{Z}_3$ می‌نویسیم

$$(g_1, g_2)(g_1', g_2') = (g_1 +_2 g_1', g_2 +_3 g_2')$$
$$(1,1)(1,1) = (1 +_2 1, 1 +_3 1) = (0,2)$$

۳- دلیل استفاده از پسوند **دکارتی**، یکی تعریف حاصل‌ضرب دکارتی مجموعه‌ای

$$G_1 \times G_2 = \{(g_1, g_2) \mid g_1 \in G_1, g_2 \in G_2\}$$

و دیگری این است که گروه $G_1 \times G_2$ در ویژگی جهانی ضرب، قضیه‌ی م. ۴.۱ صدق می‌کند. البته گاهی واژه‌ی **حاصل‌ضرب مستقیم برونی** یا **خارجی** را نیز به کار می‌برند، زیرا G_iها زیرگروه حاصل‌ضرب نیستند، و نسبت به آن **خارجی**‌اند. در این مورد بعداً بیش‌تر صحبت می‌کنیم.

۴- همان طور که در بند ۳ بحث ۲۳.۶.۱ دیدیم، گروه $G_1 \times G_2$ ممکن است برخی از ویژگی‌های مولفه‌هایش G_1 و G_2 را به ارث نبرد! در همان بحث گفتیم که اگر G_1 و G_2 دارای ویژگی معادله‌ای (**اتحاد**) σ باشند، آنگاه $G_1 \times G_2$ نیز در آن ویژگی صدق می‌کند. برای مثال، $G_1 \times G_2$ ویژگی آبلی بودن را از مولفه‌هایش به ارث می‌برد.

۵- آیا $G_1 \times G_2$ ویژگی دوری بودن را از مولفه‌هایش به ارث می‌برد؟ (نشان دهید که گروه $\mathbb{Z}_2 \times \mathbb{Z}_2$ دارای عضوی با رتبه‌ی ۴ نیست و قضیه‌ی ۵.۴.۲ را به کار ببرید).

۶- یادآوری می‌کنیم که، تا حد یک‌ریختی، تنها دو (دسته) گروه چهار عضوی وجود دارند، یکی با نماینده‌ی $\mathbb{Z}_4$ و دیگری با نماینده‌ی K_4. حال که، با توجه به بند ۵، $\mathbb{Z}_2 \times \mathbb{Z}_2$ دوری نیست، بگویید با کدام گروه چهار عضوی یک‌ریخت است. روشن است، نیست؟ جدول کیلی گروه $\mathbb{Z}_2 \times \mathbb{Z}_2$ را در زیر کامل و آن را با جدول گروه کلاین K_4 مقایسه کنید:

K_4	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

$+$	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
$(0,0)$	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
$(0,1)$	$(0,1)$	?	?	$(1,0)$
$(1,0)$	$(1,0)$	$(1,1)$	$(0,0)$	?
$(1,1)$	$(1,1)$	?	$(0,1)$	$(0,0)$

۷- دوباره می‌پرسیم که، حال که دسته‌ی گروه‌های دوری **نسبت به ضرب بسته نیست**، از قضیه‌ی ۲.۹.۱ بیرخوف چه نتیجه‌ای می‌گیرید؟ درست است، دسته‌ی گروه‌های دوری را نمی‌توان با مجموعه‌ای از معادله‌ها مشخص کرد!

۸- البته حاصل‌ضرب برخی از گروه‌های دوری، دوری است. برای مثال، چون مرتبه‌ی 1 در گروه $\mathbb{Z}_2$ برابر با ۲ و در گروه $\mathbb{Z}_3$ برابر با ۳ است، به آسانی می‌توانید نشان دهید که مرتبه‌ی $(1,1)$ در گروه $\mathbb{Z}_2\times\mathbb{Z}_3$ برابر است با $|\mathbb{Z}_2\times\mathbb{Z}_3|=6$ و در نتیجه، بنابر قضیه‌ی ۵.۴.۲، $\mathbb{Z}_2\times\mathbb{Z}_3=<(1,1)>$ دوری است.

۹- حدس می‌زنید که چه عاملی باعث می‌شود که $\mathbb{Z}_2\times\mathbb{Z}_3$ و $\mathbb{Z}_3\times\mathbb{Z}_4$ دوری باشند ولی $\mathbb{Z}_2\times\mathbb{Z}_2$، $\mathbb{Z}_4\times\mathbb{Z}_6$، یا $\mathbb{Z}_3\times\mathbb{Z}_6\times\mathbb{Z}_5$ دوری نباشند؟ به احتمال زیاد درست حدس زده‌اید. برای اثبات درستی حدس خود، ابتدا مسأله‌ی زیر را با استفاده از لم ۳.۴.۲ حل کنید.

۱۰- فرض کنید $g=(g_1,\cdots,g_n)\in G=G_1\times\cdots\times G_n$ و $O_{G_i}(g_i)=m_i$. نشان دهید که $O_G(g)=m=[m_1,\cdots,m_n]$ (لم ۳.۴.۲ را به کار ببرید).

۳.۷.۲ قضیه. گروه $G=\mathbb{Z}_{m_1}\times\cdots\times\mathbb{Z}_{m_n}$ دوری است اگر و تنها اگر برای هر $i\neq j$، $(m_i,m_j)=1$.

اثبات. با استفاده از بند ۱۰ بحث ۲.۷.۲ بالا، نشان دهید که

$$O_G(1,1,\cdots,1)=m_1m_2\cdots m_n=|G|$$

و قضیه‌ی ۵.۴.۲ را به کار ببرید.

۴.۷.۲ بحث در کلاس

۱- اگر گروه G برابر، یا یک‌ریخت، با حاصل‌ضرب دو گروه نابدیهی (مخالف $\{e\}$) باشد، می‌گوییم که G **تجزیه‌پذیر** است. برای مثال، K_4 تجزیه پذیر است ولی $\mathbb{Z}_4$ تجزیه پذیر نیست. **چطور؟** با توجه به قضیه‌ی بالا، تعیین کنید که $\mathbb{Z}_n$ برای کدام عدد طبیعی n تجزیه‌پذیر است؟

۲- نشان دهید که گروه $\mathbb{Z}\times\mathbb{Z}$ دوری نیست. ابتدا نشان دهید که $(1,1)$ نمی‌تواند مولد $\mathbb{Z}\times\mathbb{Z}$ باشد. حال فرض کنید که $(m,n)\neq(1,1)$ و نشان دهید که $(1,1)$ مضرب (m,n) نیست.

۳- نشان دهید که برای $n\geq 2$، گروه $\mathbb{Z}\times\mathbb{Z}_n$ دوری نیست.

۴- نشان دهید که اگر $G_1\times G_2$ با مولد (g_1,g_2) دوری باشد آنگاه G_1 با مولد g_1 و G_2 با مولد g_2 دوری هستند.

۵- با استفاده از مطالب بالا، نشان دهید که $\mathbb{Z}$ تجزیه‌ناپذیر است.

بحث بالا تکلیف تجزیه‌پذیری یا تجزیه‌ناپذیری گروه‌های دوری را کاملاً روشن می‌کند. ولی در حالت کلی، کدام گروه‌ها تجزیه‌پذیر یا تجزیه‌ناپذیر هستند؟ این سؤال را در قضیه‌ی ۷.۷.۲ پاسخ می دهیم. ابتدا لم زیر را می‌آوریم.

۵.۷.۲ لم. فرض کنیم $G=H\times K$ حاصل‌ضرب گروه‌های H و K باشند. در این صورت،

۱- $\hat{H}=H\times\{e_K\}=\{(h,e_k)\,|\,h\in H\}$ و $\hat{K}=\{e_h\}\times K$ زیر گروه $G=H\times K$ هستند، به طوری که $H\cong\hat{H}$، $K\cong\hat{K}$، و $G=H\times K\cong\hat{H}\times\hat{K}$.

۲- $\hat{H}\cap\hat{K}=\{(e_H,e_K)\}$.

۳- برای هر $\hat{h}\in\hat{H}$ و $\hat{k}\in\hat{K}$ داریم $\hat{h}\hat{k}=\hat{k}\hat{h}$.

۴- $G=H\times K=\hat{H}\hat{K}$

اثبات. اثبات این مطالب سرراست هستند. خلاصه‌ای از آن را می‌آوریم.

۱- روشن است که $\hat{e}=(e_H,e_K)$ عضو همانی $\widehat{H}$ و $\widehat{K}$ است. همچنین،

$$(h_1,e_K)(h_2,e_K)=(h_1h_2,e_K)\in\widehat{H}$$
$$(h,e_K)^{-1}=(h^{-1},e_K)\in\widehat{H}$$

از این رو، $\widehat{H}\leq H\times K=G$. به همین صورت، $\widehat{K}\leq H\times K=G$. به آسانی می‌توانید نشان دهید که توابع زیر یک‌ریختی هستند:

$$\varphi : H \to \widehat{H}, \qquad \psi : K \to \widehat{K}$$
$$h \mapsto \hat{h} = (h, e_K) \qquad k \mapsto \hat{k} = (e_H, k)$$

$$\Phi : H \times K \to \widehat{H} \times \widehat{K}$$
$$(h,k) \mapsto (\hat{h}, \hat{k}) = ((h, e_k), (e_K, k))$$

۲- توجه می‌کنیم که $(h, e_K) = (e_H, k)$ اگر و تنها اگر $h = e_H$ و $k = e_K$. که بند ۲ را اثبات می‌کند.

۳- برای هر $\hat{h} \in \widehat{H}$ و $\hat{k} \in \widehat{K}$، داریم

$$\hat{h}\hat{k} = (h, e_K)(e_H, k) = (he_H, e_K k) = (h, k)$$
$$\hat{k}\hat{h} = (e_H, k)(h, e_K) = (e_H h, k e_K) = (h, k)$$

۴- سرانجام توجه می‌کنیم که

$$\begin{aligned} \hat{H}\hat{K} &= \{(h, e_K) \mid h \in H\}\,\{(e_K, k) \mid k \in K\} \\ &= \{(h, e_K)(e_K, k) = (h, k) \mid h \in H, k \in K\} \\ &= H \times K = G \end{aligned}$$

۶.۷.۲ **بحث در کلاس.** قضیه‌ی بالا نشان می‌دهد که مولفه‌های حاصل‌ضرب $H \times K$، یعنی H و K با زیرگروه‌هایی چون $\widehat{H}$ و $\widehat{K}$ از گروه $H \times K$ یک‌ریخت هستند که این زیرگروه‌ها دارای ویژگی‌های ۲، ۳، ۴ هستند. حال عکس این روند را بررسی می‌کنیم. ادعا می‌کنیم که اگر گروهی دلخواه چون G دارای زیرگروه‌هایی چون H و K با ویژگی‌های همتای ۲، ۳، ۴، باشند آنگاه $G \cong H \times K$.

۷.۷.۲ **قضیه.** فرض کنیم H و K زیرگروه‌هایی از گروه دلخواه G با ویژگی‌های زیر باشند:

(الف) برای هر $h \in H$ و $k \in K$، داشته باشیم $hk = kh$؛

(ب) $H \cap K = \{e\}$؛

(پ) $G = HK$.

در این صورت، $G \cong H \times K$.

اثبات. نشان می‌دهیم که

$$\varphi : H \times K \to G$$
$$(h,k) \mapsto hk$$

یک‌ریختی مورد نظر است. روشن است که φ خوش‌تعریف و بنابر (پ) پوشا است. اثبات یک به یک بودن φ جالب است! توجه می‌کنیم که

$$\varphi(h_1,k_1)=\varphi(h_2,k_2) \Rightarrow h_1k_1 = h_2k_2$$
$$\Rightarrow h_2^{-1}h_1 = k_2k_1^{-1} \in H \cap K = \{e\}$$

(درستی سطر دوم را توضیح دهید). پس، $h_2^{-1}h_1 = e$ و $k_1k_2^{-1} = e$، و در نتیجه $h_1 = h_2$، $k_1 = k_2$، یعنی φ یک به یک است. در پایان، به آسانی می‌توان نشان داد که φ همریختی است (درستی مراحل زیر را توضیح دهید):

$$\varphi[(h_1,k_1)(h_2,k_2)] \Rightarrow \varphi(h_1h_2,k_1k_2) = (h_1h_2)(k_1k_2)$$
$$\Rightarrow (h_1k_1)(h_2k_2)$$
$$\Rightarrow \varphi(h_1,k_1)\varphi(h_2,k_2)$$

بنابراین، قضیه اثبات شده است. **راحت بود، نبود؟**

۸.۷.۲ بحث در کلاس

۱- قضیه‌های بالا **شرایط لازم و کافی برای تجزیه‌پذیری گروه** دلخواه G را ارائه می‌دهد. نمونه‌های زیر را ببینید.

۲- نشان می‌دهیم که K_4 تجزیه پذیر است. البته، قبلاً دیدیم که $K_4 \cong \mathbb{Z}_2 \times \mathbb{Z}_2$، ولی می‌خواهیم روش استفاده از قضیه‌ی بالا را نشان دهیم. به آسانی می‌توانید نشان دهید که زیرگروه‌های $H = \{e,a\}$ و $K = \{e,b\}$ از K_4 در شرایط قضیه صدق می‌کنند. توجه کنید که $c = ab$. در نتیجه، $K_4 \cong H \times K$. همچنین، چون $H \cong \mathbb{Z}_2$ و $K \cong \mathbb{Z}_2$، پس $K_4 \cong H \times K \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

۳- آیا $\mathbb{Z}_4$ تجزیه‌پذیر است؟ پاسخ منفی است، زیرا $H = K = \{0,2\}$ تنها زیرگروه نابدیهی $\mathbb{Z}_4$ است ولی در شرط‌های (ب) و (پ) قضیه صدق نمی‌کند.

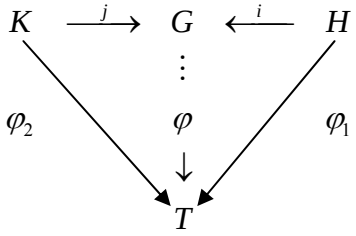
۴- به راحتی می‌توانید به دو روش، یکی با استفاده از قضیه‌ی ۱۵.۴.۲ و دیگری با استفاده از قضیه‌ی بالا، نشان دهید که $\mathbb{Z}_p$ و S_3 تجزیه ناپذیر هستند و $\mathbb{Z}_6$ تجزیه‌پذیر است.

۹.۷.۲ تعریف. فرض کنیم G گروه و H و K **زیرگروه** آن باشند به طوری که در شرط‌های قضیه‌ی ۷.۷.۲ صدق کنند، و در نتیجه $G \cong H \times K$. در این صورت، می‌گوییم که G **حاصل‌ضرب مستقیم درونی** H و K است.

۱۰.۷.۲ بحث در کلاس. قضیه‌ی ۵.۷.۲ نشان می‌دهد که اگر $G = H \times K$ حاصل ضرب **برونی** H و K باشد، آنگاه $\widehat{H}$ و $\widehat{K}$ در شرط‌های قضیه‌ی ۷.۷.۲ صدق می‌کنند و در نتیجه $G \cong \widehat{H} \times \widehat{K}$ حاصل‌ضرب **درونی** است. از این رو اساساً تفاوتی بین دو مفهوم حاصل‌ضرب برونی و حاصل ضرب درونی دو گروه وجود ندارد. از این رو، تنها وقتی از پسوندهای برونی و درونی استفاده می‌کنیم که بخواهیم بر زیرگروه بودن یا نبودن مؤلفه‌ها تاکید کنیم.

۱۱.۷.۲ همضرب گروه‌های آبلی. مفهوم همضرب را در م.۵.۱ و بخش ۶ از فصل ۱ معرفی کردیم. اثبات وجود همضرب گروه‌های **غیر آبلی قدری پیچیده** است و در درس‌های دیگر مطرح می‌شود. در اینجا می‌خواهیم وجود همضرب را برای گروه‌های **آبلی** به اختصار بیاوریم.

فرض کنیم H و K گروه‌هایی **آبلی** باشند (که عمل‌های هر دو را با $+$ نشان می‌دهیم). به دنبال گروهی **آبلی** چون G همراه با دو همریختی $K \xrightarrow{i_2} G \xleftarrow{i_1} H$ با **ویژگی جهانی** زیر هستیم: برای هر گروه **آبلی** $(T;+)$ و هر جفت همریختی گروهی $K \xrightarrow{\varphi_2} T \xleftarrow{\varphi_1} H$، همریختی منحصر به فرد $\varphi : G \to T$ وجود داشته باشد به طوری که نمودار زیر تعویض‌پذیر باشد:



ادعا می‌کنیم که همان گروه $G = H \times K$ ولی همراه با همریختی‌های درون‌بری

$$K \xrightarrow{i_2} G = H \times K \xleftarrow{i_1} H$$
$$k \mapsto (\circ_H, k) \qquad (h, \circ_K) \leftarrow h$$

به جای همریختی‌های تصویری، گروه مورد نظر است. کافی است در نمودار بالا تعریف کنیم

$$\varphi : H \times K \to T$$
$$(h,k) \mapsto \varphi_1(h) + \varphi_2(k)$$

به آسانی می‌توانید نشان دهید که تابع φ نمودار بالا را تعویض‌پذیر می‌کند و با این ویژگی منحصر به فرد است. پس کافی است اثبات کنید که φ همریختی است. در اثبات آسان و سرراست این مطلب، **آبلی بودن** T را به کار خواهید برد.

چون گروه‌های بالا آبلی هستند، نمادهای جمعی را به کار برده‌ایم. از این رو، معمولاً ضرب گروه‌های آبلی H و K را با $G = H \oplus K$ نشان می‌دهیم و آن را **مجموع مستقیم** نیز می‌نامیم.

تمرین ۷.۲

آستین ها را بالا بزنید

دسته‌ی اول

۱- نشان دهید که گروه $G = \mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_n}$ با گروه $\mathbb{Z}_{m_1 \cdots m_n}$ یک‌ریخت است اگر و تنها اگر برای هر $i \neq j$، $(m_i, m_j) = 1$.

۲- در زیر، مرتبه‌ی هر عضو را در گروه داده شده بیابید:

(الف) $(4,9) \in \mathbb{Z}_{18} \times \mathbb{Z}_{18}$.

(ب) $(4,9) \in \mathbb{Z}_8 \times \mathbb{Z}_{12}$.

(پ) $(4,5,3) \in \mathbb{Z}_{18} \times \mathbb{Z}_{18} \times \mathbb{Z}_6$.

(ت) $(\rho_1, 4) \in S_3 \times \mathbb{Z}_6$.

۳- دو گروه نا آبلی، یکی از مرتبه‌ی ۱۸ و دیگری از مرتبه‌ی ۳۲ مثال بزنید.

۴- یک گروه G از مرتبه‌ی ۱۲۵ مثال بزنید که مرتبه‌ی هر عضو ناهمانی آن ۵ باشد.

نشان دهید که $Z(G_1 \times G_2) = Z(G_1) \times Z(G_2)$.

۵- فرض کنید که $H_1 \leq G_1$ و $H_2 \leq G_2$. نشان دهید که $H_1 \times H_2 \leq G_1 \times G_2$.

۶- فرض کنید $G_1 \cong G_1'$ و $G_2 \cong G_2'$. نشان دهید که $G_1 \times G_2 \cong G_1' \times G_2'$.

۷- زیرگروه‌های $6\mathbb{Z} \cap 9\mathbb{Z}$ و $6\mathbb{Z} + 9\mathbb{Z}$ از گروه $\mathbb{Z}$ را مشخص کنید.

۸- زیرگروه‌های $H=<4>$ و $K=<6>$ از گروه $\mathbb{Z}_{12}$ را در نظر بگیرید و $H+K$ را مشخص کنید.

۹- گروه $\mathbb{Z}_{26}\times\mathbb{Z}_{15}$ دارای چند عضو از مرتبه‌ی ۵ و چند عضو از مرتبه‌ی ۱۵ است؟

دسته‌ی دوم

۱۰- ثابت کنید که گروه ضربی $(\mathbb{R}^*;\cdot)$ تجزیه‌پذیر است. تابع زیر را به کار ببرید:

$$f:\mathbb{R}^*\to\mathbb{R}^+\times\{1,-1\}$$
$$f(x)=\begin{cases}(x,1) & x>0\\(-x,-1) & x<0\end{cases}$$

۱۱- ابتدا با یک مثال نشان دهید که زیرگروه‌های گروه $G_1\times G_2$ لزوماً به صورت $H_1\times H_2$ نیستند. سپس ثابت کنید که اگر همه‌ی زیرگروه‌های گروه $G_1\times G_2$ به صورت $H_1\times H_2$ باشند، آنگاه $G_1\times G_2$ دوری است. آیا عکس این مطلب نیز درست است.

۱۲- (**تمرین جالب**) فرض کنید که $H,K\le G$. نشان دهید که G حاصل‌ضرب (مستقیم درونی) H و K است اگر و تنها اگر دو شرط زیر برقرار باشند:

(الف) برای هر $h\in H$ و $k\in K$، $hk=kh$؛

(ب) هر عضو $g\in G$ تجزیه‌ای یکتا به صورت $g=hk$ داشته باشد که در آن $h\in H$ و $k\in K$.

۱۳- فرض کنید که $H,K\le G$. نشان دهید که G حاصل‌ضرب مستقیم درونی H و K است اگر و تنها اگر تابع زیر یک یک‌ریختی گروهی باشد:

$$\varphi:H\times K\to G$$
$$(h,k)\mapsto hk$$

۱۴- فرض کنید $G=G_1\times\cdots\times G_n$ حاصل‌ضرب (برونی) گروه‌ها باشد. در این صورت، زیرگروه‌های $\hat{G}_i\le G$ وجود دارند به طوری که

(الف) برای هر i، $G_i\cong\hat{G}_i$.

(ب) برای هر $i\neq j$، $x\in\hat{G}_i$ و $y\in\hat{G}_j$، داریم $xy=yx$.

(پ) برای هر i، $\hat{G}_i \cap (\hat{G}_1 \cdots \hat{G}_{i-1}\hat{G}_{i+1} \cdots \hat{G}_n) = \{e_G\}$.

(ت) $G = \hat{G}_1\hat{G}_2 \cdots \hat{G}_n$.

(ث) $G \cong \hat{G}_1 \times \cdots \times \hat{G}_n$.

۱۵- مثال هایی از گروه‌های H_i و K_i $(i = 1,2)$ ارائه دهید به طوری که $H_1 \times H_2 \cong K_1 \times K_2$ در حالی که هیچ یک از H_i با K_j ها یکریخت نباشد.

۸.۲ گروه خارج قسمتی

یکی دیگر از روش‌های **بسیار مهم** ساختن دستگاه‌های ریاضی جدید (جبری یا غیر جبری) از یک دستگاه ریاضی داده شده، تشکیل خارج قسمت آن دستگاه است. در بخش ۷ از فصل ۱، این روش را برای دستگاه‌های جبری کلی معرفی و ویژگی‌های جامع آن را بررسی کردیم. در این بخش می‌خواهیم مطالب بخش ۷.۱ را برای گروه‌ها با جزییات بیشتری بررسی کنیم.

۱.۸.۲ بحث در کلاس

۱- مطالب جالبی در فصل ۱، به ویژه در بخش ۷.۱ ، مطرح شد که به نظر ما هر دانشجوی ریاضی، صرف نظر از اینکه با دستگاه‌های کلاسیک سروکار دارد یا روزی با دستگاه‌هایی جدید سروکار خواهد داشت، باید آن‌ها را بداند! باید خواستگاه، بنیاد، منبع، سرچشمه، و علت معرفی مفاهیم را بدانیم تا بهتر آن‌ها را به کار ببریم و خود، هنگام نیاز، سازنده‌ی مفاهیم جدید باشیم! **این طور نیست؟** در همان بخش ۷.۱ **هشدار** دادیم که برای برخی از دستگاه‌های کلاسیک (از جمله، گروه‌ها و حلقه‌ها)، روش ساختن خارج قسمت به صورتی بسیار خاص انجام می‌شود که لزوماً در بسیاری از دستگاه‌های جبری، از جمله، نیم‌گروه‌ها، تکواره‌ها، مشبکه‌ها، ... به کار نمی‌آید!

۲- در اغلب کتاب‌های کلاسیک جبر، برای تعریف گروه خارج قسمتی گروه G، کار را با زیرگروه خاصی چون N به نام **زیرگروه نرمال** آغاز می‌کنند و از مجموعه‌ی هم‌مجموعه‌های چپ $L_N = \{aN \mid a \in G\}$ یا راست $R_N = \{Na \mid a \in G\}$، همراه با عمل طبیعی $(aN)(bN) = abN$ یا $(Na)(Nb) = Nab$، گروهی خارج قسمتی می‌سازند. در این روند نه تنها علت کار مشخص نمی‌شود، بلکه روشن نمی‌شود که آیا این تنها روش ساختن گروه خارج قسمتی است یا نیست؟ به عبارت دیگر، آیا تنها برای هر زیرگروه نرمال می‌توانیم خارج قسمتی از یک گروه بسازیم، یا به گونه‌ای دیگر نیز می‌توان یک گروه را تقسیم‌بندی (**افراز**) کرد و گروهی خارج قسمتی ساخت؟ متاسفانه در بسیاری از کتاب‌های کلاسیک پاسخی صریح به این سؤال‌ها داده نمی‌شود و مدرسانی که پاسخ را می‌دانند نیز، احتمالاً به دلیل کمبود وقت یا عدم نیاز برای

دستگاه‌های جبری مورد نظر آن‌ها، یعنی گروه‌ها و حلقه‌ها، از کنار آن می‌گذرند! ما نیز می‌توانیم همین روش کوتاه‌تر، ولی بسیار خاص، را به کار ببریم،

ولی قول دادیم که فوت و فن کار را نیز از شما پنهان نکنیم!

۳- در این فصل، هر دو روش کلاسیک یا متداول (که تنها برای معدودی از دستگاه‌های جبری به کار می‌آید) و روش جامع را (که برای همه‌ی دستگاه‌های جبری به کار می‌رود) برای ساختن گروه-های خارج قسمتی می‌آوریم. سپس نشان می‌دهیم که روش کلاسیک برای گروه‌ها (و در فصل ۳ برای حلقه‌ها) تصادفاً معادل با روش جامع است! در بحث زیر، که یادآوری مطالبی از بخش ۷ فصل ۱ است، شرکت کنید.

هشدار می‌دهیم که در این فصل با مجموعه‌هایی متشکل از مجموعه‌ها سر و کار داریم و عمل‌ها نیز روی این نوع مجموعه‌ها (ی نا بسیط) تعریف می‌شوند! از این رو باید بیشتر دقت کنیم.

۲.۸.۲ بحث در کلاس

در بخش ۷.۱ دیدیم که هر **خارج قسمت** دستگاه جبری A ، از نوع τ ، چیزی جز **افراز** خاصی از A نیست. همچنین دیدیم که این افراز باید به گونه‌ای خاص باشد که همراه با عمل‌هایی که حاصل از عمل‌های خود A است، دستگاهی جبری از نوع τ به دست دهد. برای رسیدن به این هدف در مورد گروه‌ها، در بخش ۷.۱ دیدیم که تنها باید آن رابطه‌های هم‌ارزی $\sim$ را روی گروه G در نظر بگیریم که عمل $[x]\overline{*}[y]=[x*y]$ روی افراز آن $G/\sim$ خوش تعریف باشد، یعنی

$$\begin{cases}[x]=[x']\\ [y]=[y']\end{cases}\Rightarrow [x]\overline{*}[y]=[x']\overline{*}[y'] \quad (\Leftrightarrow [x*y]=[x'*y'])$$

که معادل است با اینکه

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

یعنی $\sim$ رابطه‌ای **همنهشتی** باشد (تعریف ۱.۷.۱ را ببینید.) این مطلب را برای گروه‌ها دوباره در زیر اثبات می‌کنیم.

۳.۸.۲ قضیه

۱- رابطه‌ی هم‌ارزی $\sim$ روی گروه G رابطه‌ای همنهشتی است اگر و تنها اگر عمل $[x]\overline{*}[y]=[x*y]$ روی $G/\sim$ خوش‌تعریف باشد.

۲- اگر $\sim$ رابطه‌ای همنهشتی روی گروه G باشد، آنگاه افراز $G/\sim$ همراه با عمل $[x]\overline{*}[y]=[x*y]$ گروه است.

اثبات

۱- فرض کنیم $\sim$ رابطه‌ای همنهشتی باشد. در این صورت، داریم

$$\begin{cases}[x]=[x']\\ [y]=[y']\end{cases}\Rightarrow\begin{cases}x\sim x'\\ y\sim y'\end{cases}\Rightarrow x*y\sim x'*y'$$
$$\Rightarrow[x*y]=[x'*y']$$
$$\Rightarrow[x]\overline{*}[y]=[x']\overline{*}[y']$$

پس $\overline{*}$ خوش‌تعریف است. برعکس، فرض کنیم $\overline{*}$ خوش‌تعریف باشد. در این صورت، رابطه‌ی $\sim$ همنهشتی است، زیرا

$$\begin{cases}x\sim x'\\ y\sim y'\end{cases}\Rightarrow\begin{cases}[x]=[x']\\ [y]=[y']\end{cases}\Rightarrow[x]\overline{*}[y]=[x']\overline{*}[y']$$
$$\Rightarrow[x*y]=[x'*y']$$
$$\Rightarrow x*y\sim x'*y'$$

۲- اثبات شرکت‌پذیری $\overline{*}$ در $G/\sim$ به راحتی از شرکت‌پذیری $*$ در G نتیجه می‌شود. روشن است که $[e]$ عضو همانی $G/\sim$ است. زیرا

$$[x]\overline{*}[e]=[x*e]=[x]\quad\&\quad[e]\overline{*}[x]=[e*x]=[x]$$

در پایان، به راحتی می‌توانید نشان دهید که وارون $[x]$، یعنی $[x]^{-1}$، برابر با $[x^{-1}]$ است.

آسان بود، نبود؟

۴.۸.۲ تعریف. فرض کنیم $\sim$ رابطه‌ای همنهشتی روی گروه G باشد. گروه $(G/\sim;\overline{*})$ را **گروه خارج قسمتی** G بر $\sim$ می‌نامیم.

۵.۸.۲ بحث در کلاس در بالا روش کلی ساختن گروه‌های خارج قسمتی را آوردیم. قبل از آوردن روش کلاسیک، مثال‌ها و نکته‌هایی را در باره‌ی روش بالا ارائه می‌کنیم.

۱- آیا افراز

$$\mathcal{P}_1 = \{\{0,1\},\{2\},\{3\}\} \quad = \quad \begin{array}{|c|c|}\hline 0 & 2 \\ \hline 1 & 3 \\ \hline \end{array}$$

گروهی خارج قسمتی از گروه $\mathbb{Z}_4$ به دست می‌دهد؟ چطور به چنین سؤالی پاسخ دهیم؟ با توجه به قضیه‌ی ۳.۸.۲ باید نشان دهیم که رابطه‌ی هم‌ارزی $\sim$ متناظر با این افراز یک رابطه‌ی همنهشتی است، یعنی در شرط $(*)$ بالا صدق می‌کند. ولی، چون

$$\begin{cases} 0 \sim 1 \\ 2 \sim 2 \end{cases} \not\Rightarrow \quad 0 +_4 2 \sim 1 +_4 2$$

پس پاسخ به سؤال بالا منفی است.

۱- افراز $\mathcal{P}_2 = \{\{0,1\},\{2,3\}\}$ **چطور؟** اگر چه در این حالت داریم

$$\begin{cases} 0 \sim 1 \\ 2 \sim 2 \end{cases} \Rightarrow \quad 0 +_4 2 \sim 1 +_4 2$$

ولی مطلب زیر نشان می‌دهد که این افراز نیز منجر به گروهی خارج قسمتی حاصل از گروه $\mathbb{Z}_4$ نمی‌شود!

$$\begin{cases} 0 \sim 1 \\ 3 \sim 3 \end{cases} \not\Rightarrow \quad 0 +_3 3 \sim 1 +_3 3$$

۲- نشان دهید که هر یک از سه افراز

$$\mathcal{P}_3 = \{\{0,2\},\{1,3\}\}, \mathcal{P}_4 = \{\{0\},\{1\},\{2\},\{3\}\}, \mathcal{P}_5 = \{\{0,1,2,3\}\}$$

(و تنها این سه افراز) گروهی خارج قسمتی از $\mathbb{Z}_4$ به دست می‌دهند.

۳- نشان دهید که هر یک از افرازهای $\mathcal{P}_a = \{\{e,a\},\{b,c\}\}$ و $\mathcal{P}_b = \{\{e,b\},\{a,c\}\}$ گروهی خارج قسمتی از گروه کلاین K_4 به دست می‌دهد. سه افراز دیگر نیز چنین هستند، آن‌ها را مشخص کنید.

۶.۸.۲ **بحث در کلاس.** برای آگاهی از **فوت و فن** روش کلاسیک و متداول ساختن گروه‌های خارج قسمتی، ابتدا مطالبی از بحث ۱۲.۲.۲ را، که به اثبات قضیه‌ی مهم لاگرانژ انجامید، مرور می‌کنیم.

۱- فرض کنیم N **زیرگروه** $(G;*)$ است. برای هر عضو $a \in G$، مجموعه‌ی $aN = \{an \mid n \in N\}$ (یا در نمادگذاری جمعی $a+N = \{a+n \mid n \in N\}$)، را یک **هم-مجموعه‌ی چپ** N نامیدیم. دیدیم که این هم‌مجموعه‌ها، رده‌های **رابطه‌ی هم‌ارزی** $a \sim_N b$ با تعریف

$$a \sim_N b \Leftrightarrow (\exists n \in N) \quad a = bn \Leftrightarrow b^{-1}a = n \in N \qquad (**)$$

هستند؛ زیرا

$$\begin{aligned}[a] &= \{x \in G \mid x \sim_N a\} \\ &= \{x \in G \mid (\exists n \in N)\, x = an\} \\ &= \{an \mid n \in N\} \\ &= aN\end{aligned}$$

بنابراین، با توجه به اینکه $[a]=[b]$ اگر و تنها اگر $a \sim_N b$، داریم

$$\begin{aligned}aN = bN &\Leftrightarrow a \sim_N b \Leftrightarrow (\exists n \in N) \quad a = bn \\ &\Leftrightarrow b^{-1}a = n \in N\end{aligned}$$

ویژگی‌های دیگر هم‌مجموعه‌های چپ و راست $Na = \{na \mid n \in N\}$ عبارت هستند از $|aN| = |N| = |Na|$ و $|L_N| = |R_N|$، که در آن $R_N = \{Na \mid a \in G\}$ مجموعه‌ی هم‌مجموعه‌های راست N در G است.

۲- بنابر قضیه‌ی لاگرانژ، برای گروه متناهی G، داریم $|R_N| = |L_N| = \dfrac{|G|}{|N|}$، و این عدد را **اندیس** N در G نامیدیم و با $[G:H]$ نشان دادیم.

تا اینجای کار نیازی به ویژگی دیگری از زیرگروه N نشدا! ولی، آیا رابطه‌ی هم‌ارزی متناظر با این افراز که در بند ۱ با $(**)$ داده شد همیشه **همنهشتی** است؟ مثال زیر پاسخی منفی به این سؤال است.

۳- زیرگروه $H = \{\rho_0, \mu_1\}$ را از گروه S_3 در نظر بگیرید. با استفاده از جدول گروه S_3 که در بند ۴ بحث ۱.۶.۲ داده شد، به آسانی می‌توانید نشان دهید که $\mu_2 \sim_H \rho_2$ زیرا

$$\rho_2^{-1}\mu_2 = \rho_1\mu_2 = \mu_1 \in H$$

از طرفی، $\mu_1 \ {}_H\sim \rho_0$. در حالی که، $\mu_1\mu_2 = \rho_1$ با $\rho_0\rho_2 = \rho_2$ در رابطه نیست، زیرا $\rho_2^{-1}\rho_1 = \rho_1\rho_1 = \rho_2 \notin H$. در نتیجه،

$$\begin{cases}\mu_1 \ {}_H\sim \rho_0\\ \mu_2 \ {}_H\sim \rho_2\end{cases} \not\Rightarrow \mu_1\mu_2 \sim \rho_0\rho_2$$

۴- (به این بند **مهم** بیش‌تر توجه کنید) **تحت چه شرطی** روی زیر گروه N از گروه G رابطه‌ی $(**)$ یک همنهشتی می‌شود؟ توجه می‌کنیم که برای هر $n \in N$ و هر $x \in G$، شرط $x^{-1}nx \in N$ یک **شرط لازم** است. زیرا،

$$\begin{cases}n \sim e\\ x \sim x\end{cases} \Rightarrow \begin{cases}nx \sim ex = x\\ x^{-1} \sim x^{-1}\end{cases} \Rightarrow x^{-1}nx \sim x^{-1}x = e \Rightarrow x^{-1}nx \in N$$

آیا این شرط **کافی** نیز هست؟ **پاسخ مثبت است!** (دلیل هر مرحله‌ی زیر را توضیح دهید):

$$\begin{cases}a \ {}_N\sim b\\ x \ {}_N\sim y\end{cases} \Rightarrow \begin{cases}b^{-1}a \in N\\ y^{-1}x \in N\end{cases} \Rightarrow \begin{cases}y^{-1}(b^{-1}a)y \in N\\ y^{-1}x \in N\end{cases}$$
$$\Rightarrow y^{-1}(b^{-1}a)y(y^{-1}x) \in N$$
$$\Rightarrow (y^{-1}b^{-1})(ax) \in N$$
$$\Rightarrow (by)^{-1}(ax) \in N$$
$$\Rightarrow ax \ {}_N\sim by$$

موفق شدیم! حال چه واژه‌ای به چنین زیرگروه **خوبی** اختصاص دهیم. تعریف زیر را ببینید.

۷.۸.۲ تعریف. زیرگروه N از گروه G را **نرمال** می‌گوییم، و می‌نویسیم $N \trianglelefteq G$ اگر

$$(\forall x \in G) \quad (\forall n \in N) \qquad x^{-1}nx \in N$$

۸.۸.۲ قضیه. حکم‌های زیر برای زیرگروه N از گروه G معادل هستند:

(الف) زیرگروه N از گروه G نرمال است (تعریف **۷.۸.۲**).

(ب) رابطه‌ی $a \ {}_N\sim b \Leftrightarrow b^{-1}a \in N$ همنهشتی است.

(پ) عمل دوتایی $(aN)(bN)=abN$، که همان $[a]_{N\sim}[b]_{N\sim}=[ab]_{N\sim}$ است، در $G/_{N}\sim=\{aN \mid a\in G\}$ خوش‌تعریف است.

اثبات. از بند۴ بحث ۶.۸.۲ و قضیه‌ی ۳.۸.۲، و اینکه، با توجه به بند ۱ از بحث ۶.۸.۲، $[a]_{\sim_N}=aN=\{ax \mid x\in N\}$، نتیجه می‌شود.

۹.۸.۲ قضیه و تعریف. فرض کنیم N زیرگروهی نرمال از گروه G باشد. در این صورت، $G/_{N}\sim=\{aN \mid a\in G\}$ همراه با عمل $(aN)(bN)=abN$ گروه است.

معمولاً گروه $G/_{N}\sim$ را برای سادگی با G/N نشان می‌دهیم و آن را گروه خارج قسمت G بر N (به جای بر $\sim_N$) می‌نامیم.

۱۰.۸.۲ جمع بندی. قضیه‌ی ۹.۸.۲ روش کلاسیک ساختن گروه‌های خارج قسمتی را به سرانجام می‌رساند. حال، مجموعه‌های زیر را در رابطه با گروه G درنظر بگیرید:

$Q(G)=\{$مجموعه‌ی همه‌ی گروه‌های خارج قسمتی $(G/\sim;\overline{*})\}$
$Con(G)=\{$مجموعه‌ی همه‌ی رابطه‌های همنهشتی $\sim$ روی گروه $G\}$
$Nor(G)=\{$مجموعه‌ی همه‌ی زیرگروه‌های نرمال $G\}$

۱- قضیه‌ی ۳.۸.۲ نتیجه می‌دهد که تناظری دوسویی بین $Q(G)$ و $Con(G)$ وجود دارد. توجه می‌کنیم که، $(G/\sim;\overline{*})$ گروه است اگر و تنها اگر $\sim$ همنهشتی باشد.

۲- قضیه‌های ۸.۸.۲ و ۹.۸.۲ بیان می‌کنند که دو تابع یک به یک از $Nor(G)$ به $Con(G)$ و از $Nor(G)$ به $Q(G)$ وجود دارند؛ برای هر زیر گروه نرمال $N\leq G$، رابطه‌ی $\sim_N$ رابطه‌ای همنهشتی و $G/N=G/_{N}\sim$ گروهی خارج قسمتی است.

۳- بند ۲ بیان نمی‌کند که این توابع یک به یک، دوسویی نیز هستند. یعنی، بیان نمی‌کند که برای هر گروه خارج قسمتی $(G/\sim;\overline{*})$ زیر گروهی نرمال مانند N وجود دارد به طوری که $G/\sim=G/N$، و برای هر رابطه‌ی همنهشتی $\sim$ روی G، زیرگروهی نرمال مانند N وجود دارد به طوری که $\sim=\sim_N$! ولی، آیا امیدی به دوسویی بودن این توابع وجود دارد؟ خوشبختانه قضیه‌ی زیر پاسخ مثبت به این سؤال را دربر دارد!

۱۱.۸.۲ قضیه. فرض کنیم $\sim$ رابطه‌ای همنهشتی روی گروه G باشد. در این صورت، رده‌ی $N=[e]$ زیرگروه نرمال G است، و $G/\sim = G/[e] = G/N$.

اثبات. (الف) ابتدا نشان می‌دهیم که $N=[e]$ زیرگروه G است. برای اثبات این مطلب، کافی است نشان دهیم که $N=[e]$ نسبت به عمل $*$ **بسته** است، $e\in N$، و برای هر $a\in N$ داریم $a^{-1}\in N$. روشن است که چون $e\sim e$ (انعکاسی بودن $\sim$) پس $e\in N$. حال، اگر $x,y\in N=[e]$، آنگاه $x\sim e$ و $y\sim e$. در نتیجه، بنا بر **شرط سازگاری** $\sim$، داریم $x*y\sim e*e=e$ و در نتیجه $x*y\in[e]=N$. حال، نشان می‌دهیم که برای هر $a\in N$ داریم $a^{-1}\in N$. چون $a\in N=[e]$، پس $a\sim e$. از طرفی، بنابر انعکاسی بودن $\sim$، داریم $a^{-1}\sim a^{-1}$. حال، **شرط سازگاری** $\sim$ ایجاب می‌کند که $a^{-1}*a\sim a^{-1}*e$، یعنی $e\sim a^{-1}$، و در نتیجه $a^{-1}\in N=[e]$. پس، $N=[e]$ زیرگروه G است.

(ب) برای اثبات نرمال بودن، فرض می‌کنیم $x\in G$ و $n\in N=[e]$ دلخواه باشند. باید نشان دهیم که $x^{-1}nx\in N=[e]$. مراحل زیر را توضیح دهید.

$$\begin{cases} n\sim e \\ x\sim x \end{cases} \Rightarrow \begin{cases} nx\sim x \\ x^{-1}\sim x^{-1} \end{cases}$$
$$\Rightarrow x^{-1}nx\sim x^{-1}x=e$$
$$\Rightarrow x^{-1}nx\in[e]=N$$
$$\Rightarrow N\leq|\, G$$

(پ) اثبات زیر را، که نشان می‌دهد $G/\sim = G/N$، توضیح دهید:

$$y\in[x]_{\sim}\Leftrightarrow y\sim x\Leftrightarrow x^{-1}y\sim x^{-1}x=e\Leftrightarrow x^{-1}y\in[e]=N$$
$$\Leftrightarrow xN=yN\Leftrightarrow y\in xN$$

تساوی $[x]=xN=x[e]$ به این معنی است که رده‌ی $N=[e]$ **سازنده‌ی همه‌ی رده‌ها است!** ولی، همان طور که بارها در این فصل و فصل ۱ گفتیم، احکام بسیار جالب قضیه‌ی بالا، **بسیار نادر هستند**، و از آنجا که در دستگاه‌های جبری کلاسیک مانند گروه، حلقه، مدول، و فضای برداری رخ می‌دهند، این **تصور نادرست** را در دانشجویان کارشناسی و حتی بالاتر ایجاد می‌کند که برای تمام دستگاه‌های جبری درست هستند، در حالی که حتی برای نیمگروه و تکواره هم لزوماً **درست نیستند!** (بند ۱ بحث ۴.۷.۱ را ببینید).

۱۲.۸.۲ بحث در کلاس. حال که به اهمیت زیرگروه‌های نرمال پی بردیم، چند شرط دیگر معادل با تعریف نرمال بودن را، علاوه بر آن‌هایی که در قضیه‌ی **۸.۸.۲** آمد، می‌آوریم که در اثبات قضیه‌ها و حل تمرین‌ها به کار خواهند رفت. این احکام را به عنوان تمرین اثبات کنید. فرض کنیم G گروه است.

۱- زیرگروه N از G نرمال است اگر و تنها اگر

$$(\forall x \in G)\ \ (\forall n \in N) \qquad xnx^{-1} \in N$$

۲- زیرگروه N از G نرمال است اگر و تنها اگر برای هر $x \in G$، $xN = Nx$. توجه می‌کنیم که $xN = Nx$ به معنی این شرط قوی که برای هر $n \in N$، $xn = nx$ نیست (**به چه معنی است؟**) توجه می‌کنیم که

$$nx = x(x^{-1}nx) \in xN \qquad \& \qquad xn = (xnx^{-1})x \in Nx$$

۳- (ضعیف تر از بند **۲**) زیرگروه N از G نرمال است اگر و تنها اگر

$$(\forall x \in G)(\exists y \in G)\ \ xN = Ny$$

به عبارت دیگر، هر هم‌مجموعه‌ی چپ یک هم‌مجموعه‌ی راست است و بر عکس، یعنی $L_N = R_N$ که در آن

$$L_N = \{xN \mid x \in G\}, \qquad R_N = \{Ny \mid y \in G\}$$

۴- احکام زیر بلاواسطه از تعریف **۷.۸.۲** زیرگروه نرمال و بند **۱** بالا به دست می‌آیند:

$$\begin{aligned} N \trianglelefteq G \ &\Leftrightarrow (\forall x \in G)\ \ x^{-1}Nx \subseteq N \\ &\Leftrightarrow (\forall x \in G)\ \ xNx^{-1} \subseteq N \end{aligned}$$

۵- احکام زیر را با استفاده از بند **۳** اثبات کنید (به سور عمومی توجه کنید):

$$\begin{aligned} N \trianglelefteq G \ &\Leftrightarrow (\forall x \in G)\ \ x^{-1}Nx = N \\ &\Leftrightarrow (\forall x \in G)\ \ xNx^{-1} = N \end{aligned}$$

۶- روشن است که برای هرگروه G، زیرگروه‌های $\{e\}$ و G نرمال هستند.

۷- روشن است که **اگر گروه G آبلی** باشد، آنگاه **هر زیرگروه آن نرمال** است.

۸- بـرای هـر گـروه G، مرکـز آن $Z(G)=\{g\in G\mid(\forall x\in G)\quad xg=gx\}$، و هـر زیرگروه مرکز، در G نرمال است.

۹- نشان دهید که گروه خطی خاص $SL(n,\mathbb{R})$ در گروه خطی عام $GL(n,\mathbb{R})$ نرمال اسـت. باید نشان دهید که برای هر ماتریس $n\times n$ وارون‌پذیر چون A و هر ماتریس $n\times n$ چون B با دترمینان ۱، داریم $\det(A^{-1}BA)=1$.

۱۰- نشان دهید که A_3 در S_3، و به طور کلی A_n (متشکل از جایگشت‌های زوج)، در S_n نرمـال است. (به نظر شما اگر $\delta\in A_n$ زوج باشد، $\sigma^{-1}\delta\sigma$ زوج است یا فرد؟)

۱۱- فرض کنید که $N\le G$ به طوری کـه $[G:N]=2$ (یعنـی، $L_N=\{N,aN\}$). نشـان دهید که $N\trianglelefteq G$. (حال سؤال بند ۱۰ را با استفاده از این مطلب نیز پاسخ دهید).

۱۳.۸.۲ مشتق گروه. همان طور که (در بنـد ۲ بحـث ۴.۷.۱) قـول دادیـم، و بـه بهانـه‌ی معرفی یک زیرگروه نرمال مهم (به نام زیرگروه مشتق)، در اینجا **فوت و فنی** را که در بند ۲ بحث ۴.۷.۱ معرفی کردیم برای گروه‌ها به نمایش می‌گذاریم.

فرض کنیم G گروه است و می‌خواهیم کوچک‌ترین رابطه‌ی همنهشتی $\sim$ را بیابیم بـه طـوری که گروه خارج قسمتی $G/\sim$ آبلی باشد، یعنی برای هر $x,y\in G$، عبارت‌های معادل زیر برقـرار باشند:

$$[x][y]=[y][x]\Leftrightarrow[xy]=[yx]\Leftrightarrow xy\sim yx$$

از این رو، کافی است که $\sim$ را کوچک‌ترین رابطه‌ی همنهشتی روی گـروه G در نظـر بگیـریم بـه طـوری کـه بـرای هـر $x,y\in G$، $xy\sim yx$. از ایـن عبـارت نتیجـه مـی‌گیـریم کـه $xyx^{-1}y^{-1}\sim e$ (چطـور؟) یعنـی $xyx^{-1}y^{-1}\in[e]$. ازطرفـی، مـی‌دانـیم کـه $N=[e]$ زیرگروه نرمال G است. بنابراین، باید به دنبال کوچک‌ترین زیرگروهی نرمال چـون N باشـیم بـه طوری که

$$(\forall x,y)\quad xyx^{-1}y^{-1}\in N$$

به دلیل اهمیت این عبارت، نمادگذاری $[x,y]=xyx^{-1}y^{-1}$ را برای آن به کار مـی‌بـریم و آن را (با توجه به قضیه‌ی ۱۴.۸.۲) یک **جا به جا گر** یا **تعویض‌گر** می‌نامیم.

برای رسیدن به مقصود، مراحل زیر را انجـام مـی‌دهـیم. ابتـدا بـا اسـتفاده از قضـیه‌ی ۹.۳.۲، زیرگروه تولید شده توسط مجموعه‌ی تعویض‌گرها، یعنی

$$< X = \{[x,y] = xyx^{-1}y^{-1} \mid x,y \in G\} >$$
$$= \{[x_1,y_1][x_2,y_2]\cdots[x_n,y_n] \mid n \in \mathbb{N}, [x_i,y_i] \in X \cup X^{-1}\}$$

را به دست می‌آوریم. ولی، چون تصادفاً داریم

$$[x,y]^{-1} = (xyx^{-1}y^{-1})^{-1} = yxy^{-1}x^{-1} = [y,x] \in X$$

یعنی، $X = X^{-1}$ و $X \cup X^{-1} = X$، عبارت بالا قدری ساده‌تر نوشته می‌شود:

$$< X > = \{[x_1,y_1][x_2,y_2]\cdots[x_n,y_n] \mid n \in \mathbb{N}, x_i, y_i \in G\}$$

حال باید کوچک‌ترین زیرگروه **نرمال** G را بیابیم که شامل $< X >$ باشد. خوشبختانه، ولی تصادفاً، $< X >$ به خودی خود نرمال نیز می‌شود. این زیرگروه نرمال G را معمولاً با G' یا $[G,G]$ نشان می‌دهیم و آن را **زیرگروه تعویض‌گر** یا **مشتق** G می‌نامیم. قضیه‌ی زیر نشان می‌دهد که به مقصود رسیده‌ایم و G' همان **کوچک‌ترین زیرگروه نرمال** G است به طوری که G/G' **آبلی** است.

۱۴.۸.۲ قضیه. فرض کنیم G گروه است. در این صورت،

۱- اگر $G' \subseteq H \leq G$، آنگاه H در G نرمال است. به ویژه، $G' \leq G$.

۲- اگر $N \leq G$ آنگاه G/N آبلی است اگر و تنها اگر $G' \subseteq N$. به ویژه G/G' آبلی است.

اثبات

۱- فرض کنیم $h \in H$ و $g \in G$. نشان می‌دهیم که $ghg^{-1} \in H$. بنابر تعریف G'، داریم $[g,h] = ghg^{-1}h^{-1} \in G'$ و چون $G' \subseteq H$، $[g,h] = ghg^{-1}h^{-1} \in H$ و در نتیجه $ghg^{-1} = ghg^{-1}h^{-1}h \in H$.

۲- توجه می‌کنیم که برای هر $x,y \in G$، داریم

$$
\begin{aligned}
(xN)(yN) = (yN)(xN) &\Leftrightarrow xyN = yxN \\
&\Leftrightarrow (yx)^{-1}(xy) \in N \\
&\Leftrightarrow x^{-1}y^{-1}xy \in N \\
&\Leftrightarrow [x,y] \in N \\
&\Leftrightarrow G' \subseteq N
\end{aligned}
$$

(مرحله‌ی آخر را توضیح دهید. **جالب است**). در نتیجه، گروه G/N آبلی است اگر و تنها اگر $G' \subseteq N$.

۱۵.۸.۲ بحث در کلاس

۱- ابتدا توجه می‌کنیم که گروه G آبلی است اگر و تنها اگر $G' = \{e\}$. **چطور؟** پس، برای مثال $\mathbb{Z}' = \{0\} = \mathbb{Z}'_n$، ولی برای $n \geq 3$، $S'_n \neq \{\rho_0\}$.

۲- می‌خواهیم، به عنوان نمونه، زیرگروه مشتق گروه متقارن S_3 را بیابیم. محاسبه‌ی مستقیم G' معمولاً طولانی است و بهتر است برنامه‌ای کامپیوتری بنویسید یا به روش‌های نظری دیگر به نتیجه برسید. برای نمونه، این مثال را به دو روش حل می‌کنیم. روشن است که برای هر $x, y \in S_3$، تعویض‌گر $[x,y] = xyx^{-1}y^{-1}$ جایگشتی زوج است. **چرا؟** پس $\{\rho_0\} \leq S'_3 \leq A_3$. ولی، چون S_3 آبلی نیست، پس $S'_3 \neq \{\rho_0\}$، از طرفی A_3 زیرگروه نابدیهی ندارد. پس $S'_3 = A_3$. برای تمرین، ρ_1 را به صورت کروشه‌ی تعویض‌گر $[-,-]$ بنویسید.

روش دیگر این است که، بنابر بند **۱** قضیه‌ی **۱۴.۸.۲**، S'_3 در S_3 نرمال است. همچنین، $S_3 / A_3 \cong \mathbb{Z}_2$ آبلی است. پس، بنابر بند **۲** همان قضیه، $\{\rho_0\} \leq S'_3 \leq A_3$. از این رو، مانند بالا، $S'_3 = A_3$.

تمرین ۸.۲

بدون تلاش برای حل کردن تمرین‌ها، مطالب درس را خوب نیاموخته‌اید

دسته اول

۱- اعضای گروه‌های خارج قسمتی $\mathbb{Z}_8 / \{0,4\}$ و $\mathbb{Z}_{12} / <3>$ را بیابید و جدول‌های کیلی آن‌ها را تعیین کنید.

۲- نشان دهید که خارج قسمت هر گروه آبلی گروهی آبلی است. با یک مثال نشان دهید که عکس این مطلب در حالت کلی درست نیست؟

۳- نشان دهید که خارج قسمت هر گروه دوری، گروهی دوری است. با یک مثال نشان دهید که عکس این مطلب در حالت کلی درست نیست؟

۴- در زیر، مرتبه‌ی هر یک از عضوهای داده شده را در گروه مورد نظر بیابید:

(الف) $12+<6>, 14+<6>, 7+<6> \in \mathbb{Z}_{24}/<6>$.

(ب) $12+<6>, 14+<6>, 7+<6> \in \mathbb{Z}_{18}/<6>$.

۵- مرتبه‌ی هر یک از گروه‌های زیر را تعیین کنید:

$$\mathbb{Z}_{24}/<6>, \mathbb{Z}_{24}/<8>, \mathbb{Z}_4 \times \mathbb{Z}_6/<(0,2)>, \mathbb{Z}_4 \times \mathbb{Z}_6/<2> \times <3>$$

۶- فرض کنید که $H \leq G$. نشان دهید که $N_G(H) = N(H) = \{g \in G \mid g^{-1}Hg = H\}$ بزرگ‌ترین زیرگروه G است به طوری که $H \trianglelefteq N(H)$. این زیرگروه را **نرمالساز** H در G می‌نامیم. نتیجه بگیرید که $H \trianglelefteq G$ اگر و تنها اگر $N(H) = G$.

۷- فرض کنید که $N \leq G$ و برای هر $a \in G$، $a^2 \in N$. نشان دهید که $N \trianglelefteq G$ و گروه G/N آبلی است.

۸- فرض کنید H تنها زیرگروه n عضوی گروه G باشد. نشان دهید که H در G نرمال است.

۹- فرض کنید G گروه است، و $H, K \leq G$، $H \cap K = \{e\}$. نشان دهید که برای هر $h \in H$ و $k \in K$، $hk = kh$. فرض کنید G گروه، $N \trianglelefteq G$، و $H \leq G$. ثابت کنید که:

(الف) $HN \leq G$ (ب) $H \cap N \trianglelefteq H$

(پ) $N \trianglelefteq HN$ (ت) اگر $H \trianglelefteq G$، آنگاه $HN \trianglelefteq G$

۱۰- فرض کنید که $N \leq G$ و $[G:N] = 2$. (بند ۱۱ بحث ۱۲.۸.۲ را ببینید). نشان دهید که برای هر $a \in G$، $a^2 \in N$. با استفاده از این مطلب نشان دهید که، اگر چه $6 \mid 12$ ولی گروه متناوب ۱۲ عضوی A_4 زیرگروه ۶ عضوی ندارد.

۱۲- فرض کنید G گروهی متناهی است، و $N \trianglelefteq G$، و $(|N|, [G:N]) = 1$. ثابت کنید که، برای هر $x \in G$، اگر $x^{|N|} = e$ آنگاه $x \in N$.

۱۳- فرض کنید G گروهی دلخواه، $N \trianglelefteq G$، و $[G:N]$ متناهی باشد. ثابت کنید که اگر $H \leq G$ زیرگروهی متناهی باشد به طوری که $(|H|,[G:N])=1$، آنگاه $H \subseteq N$.

۱۴- فرض کنید G گروهی دلخواه، $N \trianglelefteq G$، و $|N|$ متناهی باشد. ثابت کنید که اگر $H \leq G$ زیرگروهی با اندیس متناهی باشد به طوری که $(|N|,[G:H])=1$، آنگاه $N \subseteq H$.

۱۵- فرض کنید N زیرگروهی دوری و نرمال در G است. ثابت کنید که هر زیرگروه N در G نرمال است.

۱۶- با یک مثال نشان دهید که نرمال بودن زیرگروه‌ها خاصیت تعدی ندارد. یعنی، گروهی با زیرگروه‌های $H, N \leq G$ بیابید به طوری که H در N و N در G نرمال هستند، ولی H در G نرمال نیست.

۱۷- فرض کنید که هر زیرگروه دوری در گروه G نرمال است. نشان دهید که همه‌ی زیرگروه‌های G در آن نرمال هستند.

۱۸- ثابت کنید که اگر N زیرگروهی نرمال از گروه متناهی G باشد و $(|N|,[G:N])=1$، آنگاه N تنها زیرگروه G با مرتبه‌ی $|N|$ است.

۱۹- فرض کنید که عضو a از گروه G دقیقاً دارای دو مزدوج $b^{-1}ab$ و $c^{-1}ac$ است. ثابت کنید که G زیرگروهی سره و نابدیهی نرمال دارد.

۲۰- فرض کنید $H=\{e,a\}$ زیرگروهی از گروه G است. ثابت کنید که $N_G(H)=C_G(H)$ و نتیجه بگیرید که اگر $N_G(H)=G$، آنگاه $H \subseteq Z(G)$.

۲۱- فرض کنید G گروهی متناهی، $N \trianglelefteq G$ از مرتبه‌ی p باشد به طوری که p کوچک‌ترین عدد اولی باشد که $|G|$ را می‌شمارد. ثابت کنید که $N \subseteq Z(G)$.

۲۲- فرض کنید G گروهی متناهی و p کوچک‌ترین عدد اولی باشد که $|G|$ را می‌شمارد. نشان دهید که هر زیرگروه $H \leq G$ با اندیس p در G نرمال است.

۲۳- فرض کنید N زیرگروهی نرمال از گروه G باشد به طوری که $N \cap G' = \{e\}$. ثابت کنید که $N \subseteq Z(G)$ و نتیجه بگیرید که $Z(\frac{G}{N}) = \frac{Z(G)}{N}$.

۲۴- فرض کنید که G گروه، N زیرگروه نرمال G، و $M_1, M_2 \leq G$ شامل N باشند به طوری که $\frac{M_1}{N} = \frac{M_2}{N}$. ثابت کنید که $M_1 = M_2$.

۲۵- مثالی از یک گروه ناآبلی ارایه دهید که همه‌ی زیرگروه‌های آن نرمال باشند.

۲۶- فرض کنید N زیرگروهی نرمال در گروه G باشد و $a \in G$. نشان دهید که مرتبه‌ی aN (به عنوان عضوی از گروه G/N) مرتبه‌ی a را می‌شمارد.

(الف) فرض کنید که $G = < a >$ گروهی دوری از مرتبه‌ی n باشد، و $d \mid n$، و $H = < a^d >$. همه‌ی زیرگروه‌های گروه خارج قسمت G / H را تعیین کنید.

(ب) حکم بند **(الف)** را برای $\mathbb{Z}_{36}$ و $H = < 6 >$ بررسی کنید.

۲۷- فرض کنید G گروه، $H, K \leq G$، و K متناهی باشد. ثابت کنید که $[H,K] = \{[h,k] \mid h \in H, k \in K\}$ زیرگروه K است اگر و تنها اگر $H \subseteq N_G(K)$.

۲۸- فرض کنید G گروه، $H, K \leq G$، و $H \subseteq K$. ثابت کنید که $[K,G] \leq H$ اگر و تنها اگر $\frac{K}{H} \subseteq Z(G / H)$.

۲۹- فرض کنید G گروه و $[G, Z(G)] = n$. نشان دهید که G دارای حداکثر n^2 تعویض‌گر متمایز است.

۳۰- فرض کنید G گروه و G' زیرگروه مشتق G از مرتبه‌ی متناهی m باشد. نشان دهید که هر عضو G دارای حداکثر m مزدوج متمایز در G است.

۳۱- فرض کنید G گروهی دلخواه و A گروهی آبلی باشد. ثابت کنید که

(الف) اگر $\varphi : G \to A$ همریختی باشد آنگاه $G' \subseteq Ker\,\varphi$.

(ب) $Hom(G, A) \cong Hom(G / G', A)$.

۳۲- فرض کنید p و q اعدادی اول و G گروهی ناآبلی از مرتبه‌ی pq است. نشان دهید که مرکز G بدیهی است.

۳۳- فرض کنید G گروه است و $H \leq G$. نشان دهید که هسته‌ی H در G، یعنی

$$Cor_G(H) = \bigcap_{g \in G} gHg^{-1}$$

بزرگ‌ترین زیرگروه نرمال در G مشمول در H است.

۹.۲ قضیه‌های اساسی همریختی‌ها

با همریختی‌ها و یک‌ریختی‌های دستگاه‌های جامع جبری در بخش ۵.۱ آشنا شدیم و برخی از ویژگی‌های آن‌ها را در رابطه با گروه‌ها در این فصل دیدیم. یکی از هدف‌های این بخش ارائه‌ی اثبات قضیه‌ی اساسی همریختی‌ها به زبان متداول گروه‌ها است، که حالت کلی آن در قضیه‌ی ۸.۷.۱ برای دستگاه‌های جامع جبری داده شد، و همچنین اثبات قضیه‌های دوم و سوم یک‌ریختی که قول آن را در بخش ۷.۱ دادیم. این قضیه‌های بسیار جالب و مهم در مورد ارتباط بین سه مفهوم زیرگروه نرمال (که در تناظر با همنهشتی‌ها هستند)، گروه خارج قسمتی، و همریختی هستند. از این رو، ابتدا قضیه‌ی زیر را در باره‌ی حفظ و انعکاس زیرگروه‌های نرمال تحت همریختی‌ها می‌آوریم.

۱.۹.۲ قضیه. فرض کنیم $\varphi : G_1 \to G_2$ همریختی گروه‌ها باشد. در این صورت،

۱- همریختی φ زیرگروه‌های نرمال را تا نگاره حفظ می‌کند. یعنی،

$$N \trianglelefteq G_1 \quad \Rightarrow \quad \varphi(N) \trianglelefteq Im\varphi = \varphi(G)$$

۲- همریختی φ زیرگروه‌های نرمال را منعکس می‌کند. یعنی،

$$K \trianglelefteq G_2 \quad \Rightarrow \quad \varphi^{-1}(K) = \tilde{\varphi}(K) \trianglelefteq G_1$$

اثبات

۱- دانشجویان معمولاً در اثبات این بند مشکلی ندارند. دلیل هر مرحله‌ی زیر را بیان کنید:

$$\begin{aligned}\varphi(g)^{-1}\varphi(n)\varphi(g) &= \varphi(g^{-1})\varphi(n)\varphi(g)\\ &= \varphi(g^{-1}ng) \in \varphi(N)\end{aligned}$$

۲- همان طور که در اثبات زیرگروه بودن $\varphi^{-1}(K)$ در قضیه‌ی ۳.۵.۲ نیز گفتیم، مبتدیان گاهی با نگاره‌ی معکوس اندکی مشکل دارند (البته یقیناً تا بحال ای مشکل احتمالی حل شده است). برای اثبات نرمال بودن، باید نشان دهیم که

$$(\forall g \in G_1) \quad (\forall a \in \tilde{\varphi}(K)) \quad \Rightarrow \quad g^{-1}ag \in \tilde{\varphi}(K)$$

یعنی، بنابر تعریف نگاره‌ی معکوس، باید نشان دهیم که $\varphi(g^{-1}ag) \in K$. ولی، چون K در G_2 نرمال است و $\varphi(a) \in K$ (چرا؟) داریم (دلیل هر مرحله‌ی زیر را توضیح دهید)،

$$\varphi(g^{-1}ag)=\varphi(g^{-1})\varphi(a)\varphi(g)=\varphi(g)^{-1}\varphi(a)\varphi(g)\in K$$

بنابراین $\varphi^{-1}(K)=\tilde{\varphi}(K)\leq|G_1$.

برای ادامه‌ی کار، نیاز به معرفی مفهوم **هسته‌ی همریختی**‌های بین گروه‌ها داریم. این مفهوم را برای همریختی‌های $f:A\to B$ بین دستگاه‌های کلی جبری در **۶.۷.۱ به صورت** $\sim_f=K_f=\{(a,a')\in A\times A\mid f(a)=f(a')\}$، یعنی

$$a\sim_f a'\Leftrightarrow f(a)=f(a')$$

تعریف کردیم و دربحث **۱۲.۷.۱** بدون اثبات بیان کردیم که این تعریف در مورد گروه‌ها معادل با تعریف زیر است.

۲.۹.۲ تعریف. فرض کنیم $f:A\to B$ همریختی گروه‌ها و e_B عضو همانی گروه B باشد. در این صورت، نگاره‌ی معکوس e_B تحت f، یعنی،

$$f^{-1}(e_B)=\bar{f}(e_B)=\{a\in A\mid f(a)=e_B\}$$

را (فعلاً) **پوچ‌خانه‌ی** f (و کمی بعد، **هسته‌ی** f) می‌نامیم.

چطور دو مفهوم به ظاهر متفاوت **پوچ‌خانه**‌ی همریختی گروه‌ها (همچنین برای حلقه‌ها، مدول‌ها، و فضاهای برداری) و **هسته**‌ی f معادل هستند؟ لم زیر را ببینید.

۳.۹.۲ لم. *فرض کنیم $f:A\to B$ همریختی گروه‌ها باشد. در این صورت، هسته‌ی f و **پوچ خانه**‌ی f یکدیگر را کاملاً مشخص می‌کنند. به این معنی که،*

۱- رده‌ی شامل عضو همانی e_A، تحت رابطه‌ی هم‌ارزی هسته $\sim_f=K_f$، برابر با پوچ‌خانه‌ی f است:

$$f^{-1}(e_B)=\bar{f}(e_B)=[e_A]_{\sim_f}$$

۲- پوچ‌خانه‌ی f هسته‌ی f را کاملاً مشخص می‌کند. یعنی

$$a\sim_f a'\Leftrightarrow a*a'^{-1}\in f^{-1}(e_B)$$

اثبات. با کمی دقت به اثبات لم، متوجه می‌شویم که این احکام برای چه دستگاه‌های جبری می‌توانند برقرار باشند.

۱- چون f عضو همانی را حفظ می‌کند، یعنی، $f(e_A)=e_B$ (چرا؟)، داریم

$$\begin{aligned} a\in f^{-1}(e_B) &\Leftrightarrow f(a)=e_B \\ &\Leftrightarrow f(a)=f(e_A) \\ &\Leftrightarrow a\sim_f e_A \\ &\Leftrightarrow a\in[e_A]_{\sim_f} \end{aligned}$$

۲- **(به این قسمت بیش‌تر توجه کنید)** چون هر عضو گروه دارای وارون است و همریختی f - وارون‌ها را حفظ می‌کند، داریم

$$\begin{aligned} aK_f a' &\Leftrightarrow f(a)=f(a') \\ &\Leftrightarrow f(a)*f(a')^{-1}=e_B \\ &\Leftrightarrow f(a)*f(a'^{-1})=e_B \\ &\Leftrightarrow f(a*a'^{-1})=e_B \\ &\Leftrightarrow a*a'^{-1}\in f^{-1}(e_B) \end{aligned}$$

با توجه به قضیه‌ی بالا، ریاضی‌دانان اغلب واژه‌ی **هسته** را برای **پوچ‌خانه**‌ی همریختی گروه‌ها (حلقه‌ها، و مدول‌ها) به کار می‌برند، و ما **موقتاً** از واژه‌ی **پوچ‌خانه** استفاده کردیم! همچنین، از این پس نماد **رابطه**‌ی همنهشتی K_f (یا $Kerf$) را برای **زیرگروه** نرمال هسته یا پوچ خانه‌ی همریختی f بین گروه‌ها (و حلقه‌ها در فصل ۳) نیز به کار می‌بریم، و اشتباهی نیز پیش نمی‌آید. قضیه‌ی مهم و طبیعی زیر را بسیار به کار خواهیم برد.

۴.۹.۲ قضیه. فرض کنیم $N\trianglelefteq G$. در این صورت، تابع طبیعی زیر همریختی پوشای گروه‌ها است:

$$\begin{aligned} \gamma : G &\to G/N \\ x &\mapsto xN \end{aligned}$$

اثبات. نکته‌ی جالب این است که عمل دوتایی روی G/N طوری تعریف شده است که این تابع طبیعی همریختی شود. توجه کنید که

$$\gamma(ab)=abN=(aN)(bN)=\gamma(a)\gamma(b)$$

پوشا بودن γ روشن است.

لم زیر همتای لم های م.۹.۱ و ۷.۷.۱ است.

۵.۹.۲ لم. *فرض کنیم* $\varphi: G_1 \to G_2$ *همریختی گروهی باشد. در این صورت،*

۱- *هسته‌ی* φ *در* G_1 *نرمال است.*

۲- *بر عکس، هر زیرگروه نرمال* G_1 *هسته‌ی یک همریختی با دامنه‌ی* G_1 *است.*

۳- *همریختی* φ *یک به یک است اگر و تنها اگر* $K_\varphi = \{e_1\}$.

اثبات

۱- توجه می‌کنیم که $K_\varphi = \tilde{\varphi}(e_2)$ و $\{e_2\}$ در G_2 نرمال هستند. حال، بند ۲ قضیه‌ی ۱.۹.۲ را به کار ببرید. (تمرین خوبی است که حکم را به طور مستقیم، بدون استفاده از قضیه‌ی ۱.۹.۲، نیز اثبات کنید).

۲- فرض کنیم $N \trianglelefteq G$. ادعا می‌کنیم که N هسته‌ی همریختی طبیعی $\gamma: G \to G/N$ است (مراحل اثبات زیر را توضیح دهید):

$$x \in K_\gamma \Leftrightarrow \gamma(x) = e_{G/N} \Leftrightarrow xN = N \Leftrightarrow x \in N$$

۳- فرض کنیم $K_\varphi = \{e_1\}$. مراحل اثبات یک به یک بودن φ را در زیر توضیح دهید:

$$\begin{aligned}
\varphi(a) = \varphi(b) &\Rightarrow \varphi(a)\varphi(b)^{-1} = e_2 \\
&\Rightarrow \varphi(a)\varphi(b^{-1}) = e_2 \\
&\Rightarrow \varphi(ab^{-1}) = e_2 \\
&\Rightarrow ab^{-1} \in K_\varphi = \{e_1\} \\
&\Rightarrow ab^{-1} = e_1 \\
&\Rightarrow a = b
\end{aligned}$$

بر عکس، فرض کنیم φ یک به یک باشد. حال، مراحل اثبات $K_\varphi = \{e_1\}$ را در زیر توضیح دهید:

$$\begin{aligned}
x \in K_\varphi &\Rightarrow \varphi(x) = e_2 \\
&\Rightarrow \varphi(x) = \varphi(e_1) \\
&\Rightarrow x = e_1
\end{aligned}$$

با توجه به بندهای ۱ و ۲ لم بالا، می‌گوییم که **دو مفهوم زیرگروه نرمال و هسته‌ی همریختی‌ها اساساً یکسان هستند!** قضیه‌ی اساسی همریختی‌های گروه‌ها نیز بیان می‌کند که

تفاوتی اساسی بین گروه‌های خارج قسمتی و همریختی‌های پوشا وجود ندارد! این قضیه همتای قضیه‌ی اساسی **۶.۷.۱** است.

۶.۹.۲ قضیه(ی اساسی همریختی‌گروه‌ها). *فرض کنیم* $\varphi : G_1 \to G_2$ *همریختی گروهی و* K_φ *هسته‌ی آن باشد. در این صورت،*

$$G_1 / K_\varphi \cong \varphi(G_1)$$

به ویژه، اگر φ *پوشا باشد آنگاه* $G_1 / K_\varphi \cong G_2$.

اثبات. در اثبات قضیه‌ی **م.۱۰.۱** دیدیم که تابع

$$\begin{aligned} \overline{\varphi} : G_1 / K_\varphi &\to \varphi(G_1) \\ xK_\varphi &\mapsto \varphi(x) \end{aligned}$$

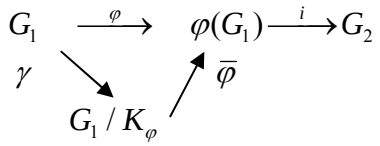
خوش‌تعریف، **یک به یک**، و **پوشا** است (**اثبات را در اینجا بنویسید**). کافی است ثابت کنیم که $\overline{\varphi}$ همریختی گروهی است، که آن نیز مانند حالت کلی **۸.۷.۱** به راحتی انجام می‌شود. مراحل اثبات زیر را توضیح دهید:

$$\begin{aligned} \overline{\varphi}[(aK_\varphi)(bK_\varphi)] &= \overline{\varphi}(abK_\varphi) \\ &= \varphi(ab) = \varphi(a)\varphi(b) \\ &= \overline{\varphi}(aK_\varphi)\overline{\varphi}(bK_\varphi) \end{aligned}$$

بنابراین، $G_1 / K_\varphi \cong \varphi(G_1)$. حکم آخر قضیه روشن است.

۷.۹.۲ بحث در کلاس

۱- اثبات قضیه‌ی اساسی نشان می‌دهد که نمودار زیر تعویض‌پذیر است، یعنی $\overline{\varphi} \circ \gamma = \varphi$:



۲- توجه می‌کنیم که چون γ پوشا و در نتیجه از راست حذف‌پذیر است، $\overline{\varphi}$ با ویژگی $\overline{\varphi} \circ \gamma = \varphi$ منحصر به فرد است. **چطور؟**

۳- اگر φ پوشا باشد آنگاه، چون دامنه‌های φ و γ برابر و نگاره‌های آن‌ها یک‌ریخت هستند، می‌گوییم که هر همریختی پوشا φ اساساً با یک همریختی طبیعی پوشا γ یکسان است، و این مطلب اهمیت همریختی‌های طبیعی γ را نشان می‌دهد!

۴- مثال‌های داده شده در بحث ۱۱.۷.۱ را یک‌بار دیگر ببینید.

۵- در بند ۵(ت) بحث ۲.۵.۲ دیدیم که تابع دترمینان از گروه ضربی **خطی عام** $GL(n,\mathbb{R})$ به گروه ضربی اعداد حقیقی $(\mathbb{R}^*;\cdot)$ همریختی است. این همریختی پوشا است. **چطور؟** همچنین هسته‌ی آن برابر است با

$$\begin{aligned} K_{\det} &= \{A \in GL(n,\mathbb{R}) \mid \det A = 1\} \\ &= SL(n,\mathbb{R}) \end{aligned}$$

در نتیجه، بنابر قضیه‌ی اساسی همریختی گروه‌ها،

$$GL(n,\mathbb{R}) / SL(n,\mathbb{R}) \cong \mathbb{R}^* .$$

دو قضیه‌ی مهم دیگر که مشابه با قضیه‌ی اساسی هستند پایان بخش این فصل است. برخی قضیه‌ی اساسی را اولین قضیه‌ی یک‌ریختی می‌نامند. از این رو دو قضیه‌ای را که می‌آوریم، دومین و سومین می‌نامیم. برای بیان هر یک نیاز به آوردن لم‌هایی است که مربوط به آن قضیه نیز هستند. تکرار می‌کنیم که در اینجا اغلب با مجموعه‌ای متشکل از مجموعه‌ها سر و کار داریم و نیاز به توجه بیشتری است.

۸.۹.۲ لم. فرض کنیم G گروه و H، N زیرگروه آن باشند به طوری که $N \trianglelefteq G$. در این صورت،

۱- اشتراک $H \cap N$ درگروه G و در نتیجه در H نیز نرمال است.

۲- HN زیرگروه G است و $N \trianglelefteq HN$.

۳- اگر H نیز در G نرمال باشد، آنگاه $HN \trianglelefteq G$.

اثبات. تمرین ۹ بخش ۸.۲ را ببینید.

۹.۹.۲ بحث در کلاس. با توجه به بند ۲ لم بالا، گروه خارج قسمتی HN / N وجود دارد. دومین قضیه‌ی یک‌ریختی بیان می‌کند که این گروه با چه گروهی یک‌ریخت است. شاید بگویید، با حذف N از صورت و مخرج، با H یک‌ریخت است!

۱۰.۹.۲ قضیه(ی دوم یکریختی). فرض کنیم H و N زیرگروه G باشند و $N \trianglelefteq G$. در این صورت،

$$\frac{HN}{N} \cong \frac{H}{H \cap N}$$

اثبات. اثبات این قضیه برایتان چندان مشکل نیست. خلاصه‌ای را از دو روش اثبات برای این قضیه می‌آوریم. روش اول فنی‌تر است و قضیه‌ی اساسی را به کار می‌برد.

روش اول: ابتدا به آسانی می‌توانید نشان دهید که تابع زیر همریختی پوشا است:

$$\begin{aligned} \Phi : H &\to \frac{HN}{N} \\ h &\mapsto heN = hN \end{aligned}$$

حال هسته‌ی آن را محاسبه می‌کنیم (یادآوری می‌کنیم که N عضو همانی گروه HN/N است. مراحل زیر را توضیح دهید):

$$\begin{aligned} K_\Phi &= \{h \in H \mid \Phi(h) = e_{HN/N}\} \\ &= \{h \in H \mid hN = N\} \\ &= \{h \in H \mid h \in N\} = H \cap N \end{aligned}$$

سرانجام می‌گوییم که بنابر قضیه‌ی اساسی، $H/K_\Phi \cong HN/N$، یعنی

$$\frac{H}{H \cap N} \cong \frac{HN}{N}$$

روش دوم: (اختیاری) نشان دهید که تابع زیر خوش‌تعریف، همریختی، و دوسویی است:

$$\begin{aligned} \Psi : \frac{H}{H \cap N} &\to \frac{HN}{N} \\ h(H \cap N) &\mapsto heN = hN \end{aligned}$$

مراحل اثبات خوش‌تعریفی را، که در زیر می‌آوریم، توضیح دهید: برای $h_1, h_2 \in H$، داریم

$$\begin{aligned} h_1(H \cap N) = h_2(H \cap N) &\Rightarrow h_2^{-1}h_1 \in H \cap N \\ &\Rightarrow h_2^{-1}h_1 \in N \\ &\Rightarrow h_1N = h_2N \end{aligned}$$

بقیه‌ی اثبات را به عنوان تمرین به عهده‌ی شما **عزیزان** می‌گذاریم.

۱۱.۹.۲ بحث در کلاس. بنابر قضیه‌ی دوم یک‌ریختی، داریم

$$\frac{4\mathbb{Z}}{4\mathbb{Z}\cap 6\mathbb{Z}} \cong \frac{4\mathbb{Z}+6\mathbb{Z}}{6\mathbb{Z}}$$

یعنی، $2\mathbb{Z}/6\mathbb{Z} \cong 4\mathbb{Z}/12\mathbb{Z}$.

قضیه‌ی سوم یک‌ریختی در باره‌ی خارج قسمت گروه خارج قسمتی G/N است. ابتدا قضیه‌ی مهم زیر را ببینید که شکل زیرگروه‌ها و زیرگروه‌های نرمال G/N را مشخص می‌کند. این قضیه را **قضیه‌ی تناظر** یا **قضیه‌ی چهارم یک‌ریختی** نیز می‌نامند. این قضیه نشان می‌دهد که **تناظری دوسویی** بین مجموعه‌ی زیرگروه‌های گروه خارج قسمتی G/N، یعنی $Sub(G/N)$، و زیرگروه‌های G که شامل N هستند، یعنی $\{H \leq G \mid N \subseteq H\}$، وجود دارد. به همین صورت، **تناظری دوسویی** بین مجموعه‌ی زیرگروه‌های **نرمال** گروه خارج قسمتی G/N، یعنی $Nor(G/N)$، و زیرگروه‌های **نرمال** G که شامل N هستند، یعنی $\{H \trianglelefteq G \mid N \subseteq H\}$، وجود دارد.

۱۲.۹.۲ قضیه (**قضیه‌ی تناظر**). فرض کنیم G گروه و N زیرگروه نرمال G باشد. در این صورت،

۱- $\mathcal{T}$ زیرگروه G/N است اگر و تنها اگر $\mathcal{T} = H/N$ که در آن $N \leq H \leq G$.

۲- $\mathcal{T}$ زیرگروه نرمال G/N است اگر و تنها اگر $\mathcal{T} = H/N$ که در آن $N \trianglelefteq H \trianglelefteq G$.

اثبات. اگر چه اثبات این قضیه چندان مشکل نیست، جزییات قسمت‌هایی از آن را برای آموزش می‌آوریم.

۱-**(الف)** ابتدا فرض می‌کنیم $N \leq H \leq G$ و نشان می‌دهیم که H/N زیرگروه G/N است. روشن است که عضو همانی گروه G/N، یعنی $eN = N$، متعلق به H/N است، زیرا $e \in H$. حال، فرض کنیم $xN, yN \in H/N$، که در آن $x, y \in H$. چون $xy^{-1} \in H$، پس

$$(xN)(yN)^{-1} = (xN)(y^{-1}N) = xy^{-1}N \in H/N$$

(ب) برعکس، فرض کنیم $\mathcal{T}$ زیرگروه G/N باشد. (توجه می‌کنیم که $\mathcal{T}$ مجموعه‌ای از مجموعه‌های به صورت aN است). ادعا می‌کنیم که زیرگروه H از گروه G وجود دارد که شامل

N است و $\mathcal{T} = H/N = \{hN \mid h \in H\}$. حدس می زنید که چون $\mathcal{T} = \{aN, bN, \ldots\}$، H کدام زیرمجموعه‌ی G ممکن است باشد؟ درست حدس زده‌اید، اجتماع عضوهای $\mathcal{T}$:

$$H = \{a \in G \mid aN \in \mathcal{T}\}$$
$$= \bigcup \mathcal{T} = \bigcup_{aN \in \mathcal{T}} aN$$

حال به راحتی می توانید ادعای بالا را اثبات کنید. (توجه کنید که، پس از اثبات زیرگروه بودن H در G و $N \subseteq H$، روشن است که چون N در G نرمال است، پس در جای کوچک‌تر H نیز نرمال است).

۲- اثبات این حکم مشابه حکم ۱ است. در قسمت (الف) باید نشان دهیم که اگر H در G نرمال باشد، آنگاه H/N در G/N نرمال است. برای اثبات این مطلب، توجه کنید که برای هر $x \in G$ و هر $h \in H$، داریم $xhx^{-1} \in H$ و در نتیجه

$$(xN)(hN)(xN)^{-1} = (xN)(hN)(x^{-1}N) = (xhx^{-1})N \in H/N$$

برعکس، در قسمت (ب) باید اثبات کنیم که اگر $\mathcal{T}$ زیرگروه نرمال G/N باشد، آنگاه

$$H = \{a \in G \mid aN \in \mathcal{T}\}$$

در G نرمال است. برای اثبات این مطلب، فرض می‌کنیم $x \in G$ و $a \in H$، و در نتیجه $aN \in \mathcal{T}$. در این صورت، بنابر نرمال بودن $\mathcal{T}$ در G/N، داریم

$$(xN)(aN)(xN)^{-1} \in \mathcal{T} \Rightarrow (xax^{-1})N \in \mathcal{T} \Rightarrow xax^{-1} \in H$$

و بنابراین قضیه اثبات شده است.

۱۳.۹.۲ قضیه (سوم یکریختی). فرض کنیم H و N زیرگروه‌هایی نرمال از G باشند به طوری که $N \subseteq H$. در این صورت،

$$\frac{G/N}{H/N} \cong G/H$$

اثبات. ابتدا، با توجه به نرمال بودن H و N در G، گروه‌های خارج قسمتی G/H و G/N با معنی هستند. همچنین، با توجه به قضیه‌ی تناظر ۱۲.۹.۲، H/N در G/N

نرمال، و در نتیجه گروه خارج قسمتی $\frac{G/N}{H/N}$ نیز با معنی، والبته هر عضو آن به صورت $(gN)(H/N)$ است.

حال، مشابه اثبات قضیه‌ی دوم یک‌ریختی، قضیه را به دو صورت زیر می‌توان اثبات کرد.

روش اول: ابتدا نشان دهید که تابع

$$\begin{aligned}\varphi : G/N &\to G/H \\ gN &\mapsto gH\end{aligned}$$

خوش‌تعریف، همریختی، و پوشا است. حال توضیح دهید که

$$\begin{aligned}Ker\varphi &= \{gN \in G/N \mid \varphi(gN) = gH = 0_{G/H} = H\} \\ &= \{gN \mid g \in H\} = H/N\end{aligned}$$

در پایان، قضیه‌ی اساسی همریختی‌ها را به کار ببرید.

روش دوم: نشان دهید که تابع زیر یک همریختی دوسویی است:

$$\begin{aligned}\psi : \frac{G/N}{H/N} &\to G/H \\ (gN)(H/N) &\mapsto gH\end{aligned}$$

اثبات خوش‌تعریفی ψ را در زیر توضیح و بقیه اثبات را ارائه دهید:

$$\begin{aligned}(g_1N)(H/N) = (g_2N)(H/N) &\Rightarrow (g_1N)(g_2N)^{-1} \in H/N \\ &\Rightarrow (g_1 g_2^{-1})N \in H/N \\ &\Rightarrow g_1 g_2^{-1} \in H \\ &\Rightarrow g_1 H = g_2 H\end{aligned}$$

۱۴.۹.۲ گروه‌های ساده. (اختیاری) یادآوری می‌کنیم که هر عدد اول p مقسوم علیهی بجز ۱ و p ندارد. از دو تعبیر این واقعیت به زبان گروه‌ها، یکی این است که هیچ زیرگروه (نرمال) $\mathbb{Z}$ بجز $\mathbb{Z}$ و $p\mathbb{Z}$ گروه $p\mathbb{Z}$ را شامل نمی‌شود، و دیگری اینکه گروه $\mathbb{Z}_p$ (که با $\mathbb{Z}/p\mathbb{Z}$ یک‌ریخت است) زیرگروهی (نرمال) بجز $\{0\}$ و خودش ندارد. قبل از بیان همتای این مفاهیم برای گروه‌های دلخواه، حالت کلی آن‌ها را برای دستگاه‌های جامع جبری از فصل ۱ یادآوری تا زیربنای این مفاهیم را بیاموزید و خودتان هنگام نیاز سازنده باشید.

۱۵.۹.۲ تعریف. فرض کنیم θ رابطه‌ای همنهشتی روی دستگاه جبری A باشد. در این صورت،

۱- رابطه‌ی θ را رابطه‌ی همنهشتی **ماکسیمال** روی A می‌گوییم اگر $\theta \neq \nabla (= A\times A)$ و هیچ رابطه‌ی همنهشتی بجز ∇ و θ رابطه‌ی θ را شامل نشود. یعنی، برای هر رابطه‌ی همنهشتی $\sim$ روی A،

$$\theta \subseteq \sim \subseteq \nabla \quad \Rightarrow \theta = \sim \quad \vee \quad \sim = \nabla$$

۲- دستگاه جبری نابدیهی A را **ساده** می‌گوییم اگر Δ و ∇ تنها رابطه‌های همنهشتی روی A باشند؛ یعنی، $Con(A) = \{\Delta, \nabla\}$.

با توجه به اینکه در گروه‌ها، زیرگروه‌های نرمال همتای رابطه‌های همنهشتی هستند، به راحتی می‌توانید تعبیر این مفاهیم را برای گروه‌ها به صورت زیر بیان کنید.

۱۶.۹.۲ تعریف. فرض کنید M زیرگروه نرمال گروه G است. در این صورت،

۱- M را زیرگروه نرمال **ماکسیمال** G می‌گوییم اگر $M \neq G$ و هیچ زیرگروه نرمالی از G، بجز G و M آن را شامل نشود. یعنی، برای هر زیرگروه نرمال H از G،

$$M \subseteq H \subseteq G \quad \Rightarrow \quad M = H \quad \vee \quad H = G$$

۲- گروه نابدیهی G را **ساده** می‌گوییم اگر G و $\{e\}$ تنها زیرگروه‌های نرمال آن باشند. یعنی، $Nor(G) = \{\{e\}, G\}$.

۱۷.۹.۲ بحث در کلاس

۱- زیرگروه متناوب A_3 در S_3 نرمال ماکسیمال است. توجه کنید که هر سه گروه $\{\rho_0, \mu_1\}$، $\{\rho_0, \mu_2\}$، $\{\rho_0, \mu_3\}$ در S_3 ماکسیمال هستند ولی **نرمال** ماکسیمال نیستند. **چطور؟** هر سه گروه $\{e, a\}$، $\{e, b\}$، و $\{e, c\}$ زیرگروه نرمال ماکسیمال گروه کلاین K_4 هستند (یادآوری می‌کنیم که هر زیرگروه از یک گروه آبلی، نرمال نیز هست). برای هر عدد اول p، زیرگروه $p\mathbb{Z}$ در گروه $\mathbb{Z}$ نرمال ماکسیمال است. زیرگروه $\{0\}$ در هر $\mathbb{Z}_p$ نرمال ماکسیمال است. گروه $(\mathbb{Q}; +)$ زیرگروه نرمال ماکسیمال ندارد. **چرا؟**

۲- مثال‌های بند ۱ نشان می‌دهند که یک گروه ممکن است هیچ زیرگروه نرمال ماکسیمال نداشته باشد یا بیش از یکی داشته باشد. ولی، هر گروه متناهی نابدیهی G دست کم دارای یک زیرگروه نرمال ماکسیمال است. (راهنمایی: روند زیر را ادامه دهید و از متناهی بودن G به نتیجه‌ی

مطلوب برسید. اگر $N_1 = \{e\}$ در G نرمال ماکسیمال نباشد، زیرگروه نرمال N_2 از G وجود دارد به طوری که $N_1 \subset N_2 \subset G$).

۳- بنابر قضیه‌ی لاگرانژ،گروه $\mathbb{Z}_n$ ساده است اگر و تنها اگر n اول باشد (چرا؟). روشن است که گروه $\mathbb{Z}$ ساده نیست؛ زیرا، برای هر عدد طبیعی $n \neq 1$، $n\mathbb{Z}$ یک زیرگروه نرمال $\mathbb{Z}$ است. در واقع، گروه آبلی نابدیهی G ساده است اگر و تنها اگر دوری و یکریخت با $\mathbb{Z}_p$ باشد. زیرا، چون G ساده است، برای هر $g \neq 0$ در G، $G = < g >$ (چرا؟) و در نتیجه، G دوری است. حال، چون $G \ncong \mathbb{Z}$ (چرا؟)، پس $G \cong \mathbb{Z}_p$. چرا؟

۴- این مطلب را اثبات نمی‌کنیم که برای هر $n \geq 5$، گروه متناوب (ناآبلی) A_n ساده است. این گروه‌ها از اولین مثال‌های گروه‌های ساده بودند که گالوا برای اثبات قضیه‌ی بسیار مهم خود از آن‌ها استفاده کرد. قضیه‌ی جالب گالوا را در درس بعدی جبر یا در درس نظریه‌ی گالوا خواهید دید. این قضیه بیان می‌کند که ریشه‌های چندجمله‌ای‌های از درجه‌ی ۵ و بیشتر را لزوماً نمی‌توان با فرمولی رادیکالی به دست آورد (مانند $x = -b \pm \sqrt{b^2 - 4ac}\ /2a$ برای ریشه‌های معادله‌ی درجه‌ی دوم $ax^2 + bx + c = 0$!)

۵- دیدیم که گروه خارج قسمتی $\mathbb{Z} / n\mathbb{Z} \cong \mathbb{Z}_n$ ساده است اگر و تنها اگر n اول باشد. قضیه‌ی پایانی این بخش این مطلب را در حالت کلی اثبات می‌کند. (مطالعه‌ی بیش‌تر و جامع‌تر گروه‌های ساده خارج از بحث این کتاب و درس مبانی جبر است).

۱۸.۹.۲ قضیه. فرض کنیم M زیرگروه نرمال گروه G است. در این صورت، گروه G / M ساده است اگر و تنها اگر M زیرگروه نرمال ماکسیمال G باشد.

اثبات. بنابر قضیه‌ی تناظر ۱۲.۹.۲،

$$Nor(G / M) \cong \{N \in Nor(G) \mid M \subseteq N\}$$

از طرفی، G / M ساده است اگر و تنها اگر $Nor(G / M) = \{\{M\}, G / M\}$ و $\{N \in Nor(G) \mid M \subseteq N\} = \{M, G\}$ زیرگروه نرمال ماکسیمال G است اگر و تنها اگر . این مطالب قضیه را اثبات می‌کند. چطور؟ تمرین خوبی است که قضیه را به طور مستقیم نیز اثبات کنید.

تمرین ۹.۲

تلاش برای حل کردن تمرین‌ها نه تنها آموزنده است، لذت بخش نیز هست

دسته اول

۱- زیرگروه‌هایی چون H و K از گروه $G=\mathbb{Z}_2\times\mathbb{Z}_4$ بیابید به طوری که $H\cong K$ ولی $G/H\ncong G/K$.

۲- زیرگروه‌هایی چون H و K از گروه $G=\mathbb{Z}_2\times\mathbb{Z}_4$ بیابید به طوری که $H\ncong K$ ولی $G/H\cong G/K$.

۳- نشان دهید که $Inn(G)\cong G/Z(G)$.

۴- نشان دهید که زیرگروه N در گروه G نرمال است اگر و تنها اگر تحت هر خودریختی درونی $\psi_a\in Inn(G)$ پایا (ناوردا) باشد. یعنی، $\psi_a(N)\subseteq N$.

۵- فرض کنید که G گروه و $G=HK$، که در آن $H,K\leq G$. ثابت کنید که $\frac{G}{H\cap K}\cong\frac{G}{H}\times\frac{G}{K}$.

۶- فرض کنید G گروهی متناهی و $f:G\to H$ همریختی باشد. ثابت کنید که $|f(G)|\,|\,|G|$.

دسته دوم

۷- می‌گوییم که زیرگروه H در G **ویژه** یا **مشخصه** است، و می‌نویسیم $H\overset{c}{\leq}G$، اگر تحت **هر** خودریختی دلخواه $\varphi:G\to G$ پایا (ناوردا) باشد؛ یعنی، $\varphi(H)\subseteq H$. روشن است که هر زیرگروه مشخصه در G نرمال است (**چرا؟**). نشان دهید که عکس این مطلب لزوماً درست نیست.

۸- نشان دهید که $Z(G)$ و G' در گروه G مشخصه هستند.

۹- فرض کنید G گروه، $N\overset{c}{\leq}G$، و $H\overset{c}{\leq}N$. ثابت کنید که $H\overset{c}{\leq}G$.

۱۰- فرض کنید G گروه، $N\leq G$ و $H\overset{c}{\leq}N$. ثابت کنید که $H\leq G$.

۱۱- فرض کنید G گروهی متناهی باشد و $H\leq G$. نشان دهید که اگر $([G:H],|H|)=1$، آنگاه $H\overset{c}{\leq}G$.

۱۲- فرض کنید G گروه، $H,K\overset{c}{\leq}G$، و $G=H\times K$. ثابت کنید که

$$Aut(G)\cong Aut(H)\times Aut(K)$$

۱۳- فرض کنید G گروه و $f:G\to G$ همریختی است به طوری که $f^2=f$ و $G\cong \operatorname{Im} f\times Kerf$. ثابت کنید که $\operatorname{Im} f\leq |G$.

۱۴- فرض کنید S_n گروه متقارن و H زیرگروه تولید شده توسط ترانهش‌های $(i,i+1)$ باشد که در آن $1\leq i\leq n-1$. تعیین کنید که HA_n/A_n با کدام گروه شناخته شده‌ای یکریخت است.

۱۵- فرض کنید G یک گروه و $G'\subseteq Z(G)$. ثابت کنید که برای هر $a\in G$، $C_G(a)\leq |G$ و $G/C_G(a)$ با زیرگروهی از G' یکریخت است.

۱۶- گروه G را **شبه آبلی** می‌گوییم اگر دارای یک زیرگروه آبلی نرمال N باشد به طوری که G/N نیز آبلی است.

(الف) مثالی از یک گروه شبه آبلی ارائه دهید که آبلی نباشد.

(ب) فرض کنید $\varphi:G\to K$ یک همریختی پوشا و G شبه آبلی باشد. نشان دهید که K نیز شبه آبلی است.

۱۷- فرض کنید $f:G_1\to G_2$ یک همریختی بین گروه‌ها است و $H\leq |G_1$. نشان دهید که اگر $f|_H:H\to G_2$ یکریختی باشد آنگاه $G_1\cong H\times Kerf$.

۱۸- (**تعمیم قضیه‌ی اساسی همریختی**) فرض کنید $f:A\to B$ و $g:A\to C$ همریختی بین گروه‌ها باشند به طوری که g پوشا است. نشان دهید که

(الف) همریختی f از طریق g تجزیه می‌شود (یعنی، همریختی $\overline{f}:C\to B$ با ویژگی $f=\overline{f}\circ g$ وجود دارد) اگر و تنها اگر $K_g\subseteq K_f$.

(ب) همریختی $\overline{f}$، در صورت وجود، منحصر به فرد است.

(پ) همریختی $\overline{f}$ یک به یک است اگر و تنها اگر $K_g=K_f$.

(ت) همریختی $\overline{f}$ پوشا است اگر و تنها اگر f پوشا باشد.

(ث) قضیه‌ی اساسی همریختی گروه‌ها حالت خاص این قضیه است.

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 **یکه‌دار**) 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، بند۲ 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 تعویض‌پذیر 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:

$$(m+n)\cdot a = m\cdot a + n\cdot a$$
$$m\cdot(a+b) = m\cdot a + m\cdot b$$
$$m\cdot(n\cdot a) = (mn)\cdot a$$

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 می‌بینیم.

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

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

$$m\cdot(ab) = ab + ab + \cdots + ab$$
$$= (a + a + \cdots + a)b = (m\cdot a)b$$

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 $-a, a+b \in S$، به راحتی می‌توانید (مشابه قضیه‌ی ۶.۲.۲) نشان دهید که S زیرگروهی از گروه $(R;+)$ است، و $ab \in S$ نشان می‌دهد که $(S;\cdot)$ زیرنیم‌گروه $(R;\cdot)$ است (شرکت‌پذیری ضرب چطور در S برقرار است؟). اثبات معادل بودن حکم ۳ با زیرحلقه بودن S را به 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، خود حلقه‌ای یک‌دار باشد، یا حتی اگر یک‌دار است، یکه‌اش همان یکه‌ی حلقه‌ی مادر باشد! ولی، ریاضی‌دانانی که تنها با حلقه‌های 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 که می‌توانید. 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 نتیجه‌ی بند ۳ برای حلقه‌ی $(\mathbb{Z}_n;+_n,\cdot_n)$ نیز درست است. یعنی، 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 متمم بسته 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

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

در این صورت، به راحتی می‌توانید نشان دهید که

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

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 $JK\neq KJ$.

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).

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

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،

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

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 $\sum_{i=1}^{n} m_i \cdot (x_{i1}...x_{ik_i})$ 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

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

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

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

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

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

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

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

(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 $n > 2$، دامنه صحیح نیست. زیرا اگر $n = rs$ 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، می‌توانید 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 این است که اگر s عضوی ناصفر در حلقه‌ی $\mathbb{Z}_n$ باشد و $m \cdot_n s = 0$، آنگاه $n \mid ms$. در نتیجه، اگر $(m,n) = 1$ آنگاه $n \mid s$ که تناقض است. برعکس، اگر $(m,n) = d > 1$ آنگاه $m(n/d) = (m/d)n$، و در نتیجه $r \cdot_n (n/d) = 0$، یعنی، m در حلقه‌ی $\mathbb{Z}_n$ مقسم صفر است. پس عضو ناصفر m در حلقه‌ی $\mathbb{Z}_n$ مقسم صفر نیست اگر و تنها اگر $(m,n) = 1$ 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 $(\mathcal{P}(X); \Delta, \cap)$ دامنه‌ی صحیح نیست. زیرا X زیرمجموعه‌هایی ناتهی دارد که اشتراک تهی دارند!

۸- حلقه‌ی $\mathbb{R}^R$ دامنه‌ی صحیح نیست. زیرا، به سادگی می‌توان تابع‌هایی ناصفر یافت که ضربشان صفر است. مثال بیاورید.

۹- حلقه‌ی چهارگان‌های همیلتون، دارای مقسم صفر نیست (تمرین ۶ این بخش را ببینید)، ولی به دلیل تعویض‌پذیر نبودن، دامنه‌ی صحیح نیست.

حال ویژگی دیگری از اعداد را مجرد سازی می‌کنیم که $\mathbb{Z}$ فاقد آن است ولی $\mathbb{Q}$، $\mathbb{R}$، 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 اگر $F^* = F \setminus \{0\}$ همراه با ضرب حلقه یک گروه **آبلی** باشد. اگر شرط آبلی بودن ضرب را در نظر نگیریم، حلقه‌ی حاصل را **حلقه‌ی 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 این 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، یا حتی حلقه‌ای یک‌دار است. در این 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 $CharF = n$ یا گاهی $ChF = n$. اگر این عدد وجود 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 عدد طبیعی n تعریف 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 می‌نویسیم $CharR = 0$. البته می‌توانید نشان دهید که تعریف ۱۲.۲.۳ برای حلقه‌های یک‌دار با این تعریف معادل است. برای اثبات، از این 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:

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

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،

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

(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 بخش۸.۲، 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 می‌نویسیم $I\trianglelefteq R$، 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 **هم‌مجموعه‌ی**

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

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:

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

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:

$$(a+I)=I \Leftrightarrow a \in I, \quad (a+I)=(b+I) \Leftrightarrow (a-b) \in I$$

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 $a \in \{1,\ldots,p-1\}$، 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.

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

۴- 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 $I = \mathbb{Q}$.

۵- (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 $1 = uu^{-1} \in I$.

۶- 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).

۷- 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 $\{2\} \cap \{2,3\} = \{2\} \notin S$. (یادآوری می‌کنیم که در این حلقه، عمل ضرب همان عمل اشتراک است).

۸- 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.

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

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

۱۱- (**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 $I \le K \le R$.

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 **سره**‌ی 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 اسـت، $M \neq R$. 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

$$1_R + M = (x+ra)+M = (x+M)+(ra+M)$$
$$= ra+M = (r+M)(a+M)$$

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، $I, J, K \leq R$، 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

$$M_1 M_2 = M_1 \bigcap M_2$$

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،

$$I \trianglelefteq J \trianglelefteq R \Rightarrow I \trianglelefteq R$$

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 فصل ۲ 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 $a,b \in R$،

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

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

۲.۴.۳ بحث در کلاس

۱- با توجه به ویژگی‌های همریختی گروه‌ها که در فصل ۲ 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 $\bar{f}(S')=f^{-1}(S')$ زیرحلقه‌ی R است.

۴- اگر J ایده‌آل R' باشد، آنگاه $\bar{f}(J)=f^{-1}(J)$ 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، $\overline{f}(x+K) = f(x)$ ، 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 $\overline{f}$:

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

حفظ عمل‌های جمع و ضرب:

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

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

۸.۴.۳ بحث در کلاس. قضیه‌ی اساسی همریختی را برای همریختی $f : \mathbb{Z} \to \mathbb{Z}_n$ با تعریف $f(k) = (n$ بر k باقی مانده‌ی تقسیم) 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 می‌توانید، برای مثال، مشابه‌ی اثبات قضیه‌ی سوم یک‌ریختی گروه ها و با در نظر گرفتن تابع زیر، اثبات کنید:

$$f : R/I \to R/J$$
$$x+I \mapsto x+J$$

توجه کنید که خوش‌تعریفی f به صورت زیر اثبات می‌شود:

$$x+I = y+I \Rightarrow x-y \in I \subseteq J \Rightarrow x-y \in J$$
$$\Rightarrow x+J = y+J \Rightarrow f(x+I) = f(y+I)$$

سپس نشان دهید که $Ker f = J/I$ 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:

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

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

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

مرحله آخر زیر را توضیح دهید:

$$\begin{cases}[(a,b)]=[(a',b')]\\ [(c,d)]=[(c',d')]\end{cases}\Rightarrow\begin{cases}(a,b)\sim(a',b')\\ (c,d)\sim(c',d')\end{cases}$$
$$\Rightarrow\begin{cases}ab'=ba'\\ cd'=dc'\end{cases}$$
$$\Rightarrow ?\ \ (ad+bc)b'd'=(bd)(a'd'+b'c')$$

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!

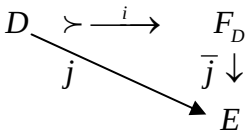
۱۳.۴.۳ بحث در کلاس. فرض کنیم D یک دامنه‌ی صحیح باشد.

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:



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 $f(k)=k\cdot\overline{1}$ 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 $Char\ f(R)\le m$.

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 برووریختی حلقه‌ها باشد. ثابت کنید که

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

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

(پ) ضابطه‌ی $M \mapsto f(M)$ یک تناظر یک به یک بین مجموعه‌ی ایده‌آل‌های ماکسیمال R که شامل $Ker(f)$ 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 $g(Y) = f_Y$ 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، نظریه گالوا، تا مطالعات امروز، نقش دارد، **حلقه‌ی چندجمله‌ای‌ها** است. با اعضا و اعمال جمع، ضرب، و تقسیم روی چندجمله‌ای‌های با ضرایب اعداد حقیقی در دوره‌ی دبیرستان آشنا شدیم. حال، با مجرد سازی این مفهوم، حلقه‌ی چندجمله‌ای‌های با ضرایب متعلق به حلقه‌ای دلخواه را معرفی و به اختصار مطالعه می‌کنیم. 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 به R، یا **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** می‌گوییم اگر ضرایب نظیرشان برابر باشند. مجموعه‌ی همه‌ی چندجمله‌ای‌های با ضرایب متعلق به حلقه‌ی R را با نماد $R[x]$ 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:

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

$$\left(\sum_{i=0}^{n} a_ix^i\right)\left(\sum_{i=0}^{m} b_ix^i\right) = \sum_{k=0}^{m+n} \left(\sum_{i=0}^{k} a_ib_{k-i}\right)x^k$$

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

$$(2x^2-5x+4)(-x^3+2x) = -2x^2x^3+4x^2x+5xx^3-10xx-4x^3+8x$$
$$= -2x^5+4x^3+5x^4-10x^2-4x^3+8x$$
$$= -2x^5+5x^4-10x^2+8x$$

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 $f=\sum_{i=0}^{n}a_ix^i\neq 0$ دارای وارونی چون $f^{-1}=\sum_{i=0}^{m}b_ix^i\neq 0$ باشد، آنگاه $f\cdot f^{-1}=1$، یعنی

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

از طرف دیگر، با استدلالی مشابه‌ی بند۳، بزرگترین $s,t\geq 0$ وجود دارند به طوری که $a_s\neq 0$ و $b_t\neq 0$، و در نتیجه ضریب $(s+t)$ام چندجمله‌ای ff^{-1} برابر با a_sb_t است، که با توجه به میدان (و در نتیجه دامنه) بودن R، عضوی ناصفر است و در نتیجه با تساوی (*) در تناقض است، مگر اینکه $s+t=0$، 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

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

البته اگر ضرایب چندجمله‌ای‌های f و g متعلق به یک میدان یا دامنه‌ی صحیح باشند، یا حتی اگر 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 $h:R\to R[x]$ وجود دارد که به 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 صورت زیر تعریف می‌شود:

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

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 بند۲ قضیه‌ی بالا، در واقع یکی از دسته همریختی‌هایی است که **ارزیاب** یا **مقدارياب** 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

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

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 وارونه‌پذیر 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

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

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 **ریشه‌ی** 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 صورت 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 درجه‌ی 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 شـهید بهشـتی، ۱۳۷۷