مبانی جبر

(برای رشته‌های ریاضیات و کاربردها و علوم کامپیوتر)

نوشته‌ی:

دکتر محمدمهدی ابراهیمی دکتر علیرضا سالمکار دکتر مژگان 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، بـی تردیـد **جبـر** ابـزاری دقیـق 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 کـرد. بسـیاری از سـاختارهایی که در شاخه‌های مختلف **علوم ریاضی** ظاهر می‌شوند، در مبحث **جبر** به صورت **مجرد** در مـی‌آینـد و مورد مطالعه قرار می‌گیرند که باعث پیشرفت بیشتر هر دو شاخه‌ی ریاضیات می‌شود.

مبحث **جبر**، مطالعه‌ی **دستگاه‌های جبری** است. **جبر کلاسیک** بـه همـت ریاضـی‌دانـانی چـون **وان‌در واردن** و **امی نوتر** با معرفی رسمی و اصل موضوعی دستگاهای جبری **گروه**، **حلقه**، **مـدول**، **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 گـروه**، **جبـر هیتینگ**، **مشبکه**، **جبر بول**، **اتوماتا**، **رسته**، **گروه و حلقه‌ی مرتب**، **جبرهای جامع مرتب**، **جبـر فازی**، و از این قبیل، نیز برای پاسخگویی به سؤال‌های جدید علـوم ریاضـی، علـوم کـامپیوتر، فیزیـک، 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 ابزارهـا در همه‌ی آن‌ها به اشتراک مطرح می‌شوند. از این رو، نیاز بـه یـک‌پارچـه کـردن دسـتگاه‌هـای جبـری 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 مثال‌هـایی از ایـن حالـت 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، کـه در دروس **علوم ریاضی و کاربردها** مطرح می‌شوند. مطالب جامع و کلی جالبی در این فصل مطرح می‌شوند که به نظـر مـا هـر دانشـجوی ریاضی، صرف نظر از اینکه با دستگاه‌های کلاسیک سروکار دارد یا روزی با دستگاه‌های جدیدتر سروکار خواهد داشت، باید آن‌ها را بدانـد! **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 طـور نیست؟** مطالب این فصل دانشجویان را برای مطالعه‌ی درس‌های دیگر ریاضی، به ویژه درس‌های جبـر، آماده می‌کند. به پیشنهاد برخی از همکاران که در کارگاه‌هـای معرفـی ایـن کتـاب در دانشـگاه شـهید

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، سالمکار، 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 $A \neq \varnothing$، آنگاه تابع f* **وارون چپ** *دارد، یعنی،*

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

م.۱.۳ بحث در کلاس

۱- پس از بحث روی صورت قضیه‌ی **م.۱.۲**، آن را در منزل اثبات کنید. **جالب است**!

۲- دوگان قضیه‌ی **م.۱.۲** 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.۱.۲** ، 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:

$$\begin{array}{ccc} A \times B \xrightarrow{p} A & , & A \times B \xrightarrow{q} B \\ (a,b) \mapsto a & , & (a,b) \mapsto b \end{array}$$

م.۱.۴ 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:

$$\begin{tikzcd} & X \arrow[dl, "g"'] \arrow[d, dotted, "h"] \arrow[dr, "f"] & \\ B & A \times B \arrow[l, "q"] \arrow[r, "p"'] & A \end{tikzcd}$$

م.۱.۵ 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.۱.۳** 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 $A \xrightarrow{f} X \xleftarrow{g} B$ 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.**)

$$\begin{tikzcd} & X & \\ B \arrow[ur, "g"] \arrow[r, "j"] & {[?]} \arrow[u, dotted, "h"] & A \arrow[ul, "f"'] \arrow[l, "i"'] \end{tikzcd}$$

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.۱.۶ 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 $x, y, z \in A$، "$(x \sim y \,\&\, y \sim z) \Rightarrow x \sim z$".

م۷.۱. **تعریف.** فرض کنیم $\sim$ رابطه‌ای هم‌ارزی روی A باشد. در این صورت، مجموعه‌ی همه‌ی رده‌های $\overline{x} = [x] = \{y \in X \mid y \sim x\}$، یعنی **افراز** $A/\sim = \{[x] \mid x \in A\}$ را **خارج قسمت** A بر $\sim$ می‌نامیم.

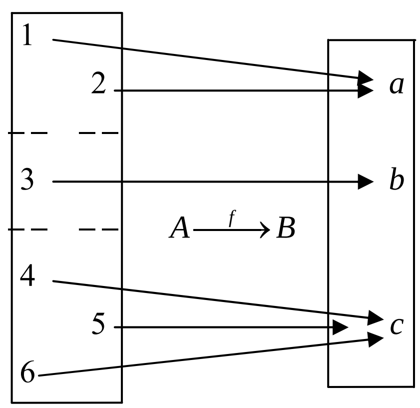
همتای خارج قسمت را نیز برای دستگاه‌های جبری خواهیم دید، که **بسیار با اهمیت** است. چند نکته‌ی بسیار مهم مرتبط با این مفهوم وجود دارند که همتاهایی در بسیاری از دستگاه‌های ریاضی، به ویژه جبری، دارند که سه بار در این کتاب و چندین بار در درس‌های دیگر مطرح خواهند شد.

م۸.۱. **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 **هسته‌ی** 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.

م۹.۱. **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.* (یعنــی، **تفاوتی اساسی بــین 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 $\sim_f = K_f$ و خوش تعریفی تابع f است. **چطور؟**

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

$$\begin{aligned} \gamma : A &\to A/\sim \\ a &\mapsto [a] \end{aligned}$$

را در نظر بگیرید. در زیر نشان می‌دهیم که رابطه‌ی هم‌ارزی $\sim$ برابر با هســته‌ی تــابع γ اســت، یعنــی $\sim = \sim_\gamma$. (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) چیــزی جــز خارج قسمت مجموعه‌ها نیست. همتای این قضیه و کاربردهای آن را در مطالعه‌ی همه‌ی دســتگاه‌هــای جبری خواهیم دید. برخی ترجیح می‌دهند که این قضیه را تنها در دستگاه‌های جبــری مطالعــه کننــد، ولی تصدیق خواهید کرد که بهتر است ابتدا آن را برای مجموعه‌ها اثبات کنیم، زیرا بیشتر قســمت‌هــای صورت و اثبات ساده‌ی آن در واقع مربوط به مبحث مبانی علوم ریاضی است!

۱۰.۱.م قضیه‌ی اساسی توابع. *فــرض کنــیم* $f: A \to B$ *تــابع و رابطــه‌ی هــم‌ارزی* $\sim_f$ *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

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

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 می-رسیم. این مطالب قضیه را اثبات می‌کنند. ■

۱۱.۱.م **بحث در کلاس**

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

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[dr, "\gamma"'] & f(A) \arrow[r, tail] & B \\ & A/K_f \arrow[u, dotted, "\overline{f}"'] & \end{tikzcd}$$

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 $x \equiv y(\operatorname{mod} n)$ یا $x \equiv y($به پیمانه‌ی $n)$. 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 $y \equiv_n x$ 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 م.۱

۱- پاسخ به سؤال‌های بحث م.۱.۳ را فراموش نکنید.

۲- با استفاده از قضیه‌ی م.۱.۴ (ویژگی جهانی ضرب) نمودار

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

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.۱.۵**، دوگان تمرین بالا را بیان و حل‌کنید. (ترسی به دل راه ندهید، **شما می-توانید**).

۴- فرض کنیم که $\mathcal{P}_X$ و $\mathcal{E}_X$، به ترتیب، مجموعه‌ی همه‌ی افرازهای روی مجموعه‌ی X و مجموعه-ی 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:

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

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،

$$\begin{tikzcd}
A \arrow[rr, "f"] \arrow[dr, "g"'] & & B \\
& C \arrow[ur, "\overline{f}"'] &
\end{tikzcd}$$

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.

م.۲ 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.

م.۲.۱ اصل خوش‌ترتیبی. هر زیرمجموعه‌ی ناتهی از اعداد طبیعی دارای کوچک‌ترین عضو است.

م.۲.۲ 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 $m|n$، اگر عدد طبیعی q با ویژگی $n=mq$ وجود داشته باشد.

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

(الف)	$a\|a$	(ب)	$a\|b \Rightarrow a\|bc$
(پ)	$a\|b, a\|c \Rightarrow a\|bx+cy$	(ت)	$a\|b, b\|c \Rightarrow a\|c$
(ث)	$a\|b, b\|a \Rightarrow a=b$	(ج)	$a\|b \Rightarrow ka\|kb$

م.۲.۵ الگوریتم تقسیم. فرض کنیم $m,n\in\mathbb{Z}$ و $n\neq 0$. در این صورت، اعداد صحیح یکتا-یی 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) $d|m, d|n$ (ب) $e|m, e|n \Rightarrow e|d$

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

(الف) $m|k, n|k$ (ب) $m|l, n|l \Rightarrow k|l$

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 "$p|ab \Rightarrow p|a$ یا $p|b$". 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- $(\frac{m}{d},\frac{n}{d})=1$

۲- $m|nk, (m,n)=1 \Rightarrow m|k$

۳- $m|nk \Rightarrow \frac{m}{d}|k$

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

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

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 $\varphi(n)=|\{0<k<n\,|\,(k,n)=1\}|$ است.

۴- فرض کنید اعداد طبیعی n_1، . . . ، 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 $m\,|\,k$ و $n\,|\,k$. ثابت کنید که $k=[m,n]$.

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

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:

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

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، به ویژه در این فصل، اغلب همان نمادگذاری $x*y$ را به کار می‌بریم تا اشتباه برانگیز نباشد.

چند عمل دوتایی در مجموعه‌ی سه عضوی وجود دارد؟ (آیا $3^9=19683$ درست است؟) 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- احتمالاً برایتان جالب است که، برای مثال، از هر تابع ۳- متغیره‌ی $f:A\times B\times C\to D$ و هر $a\in A$، یک تابع با دو متغیر

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

به دست می‌آید. به همین صورت ساده، جالب است که از هر عمل دوتایی $*:A\times A\to A$ 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 این رو، از هر 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 عمل n- تایی در A **تابعی** چون $\lambda:A^n\to A$ 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**) $\begin{cases} a=a' \\ b=b' \end{cases} \Rightarrow \quad a*b=a'*b'$

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

$a\oplus_n b =$ (باقی‌مانده‌ی حاصل از تقسیم $a+b$ بر n)

$a\odot_n b =$ (باقی‌مانده‌ی حاصل از تقسیم ab بر n)

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

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

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

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

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 $\{0,1,\ldots,n-1\}$ انجام می‌دهیم یا در $\{[0],[1],\ldots,[n-1]\}$). 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

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

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

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

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؟) :

$$\begin{aligned} &[(m,n)]*[(r,s)]=[(ms+nr,ns)] \\ &[(m,n)]*'[(r,s)]=[(mr,ns)] \end{aligned}$$

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):

$$\begin{array}{c|ccccc} * & a_1 & \cdots & a_j & \cdots & a_n \\ \hline a_1 & a_1a_1 & \cdots & a_1a_j & \cdots & a_1a_n \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ a_i & a_ia_1 & \cdots & a_ia_j & \cdots & a_ia_n \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ a_n & a_na_1 & \cdots & a_na_j & \cdots & a_na_n \end{array}$$

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

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

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

به شباهت‌های بسیار زیاد جدول‌های $\oplus_3$ با $\bar{\oplus}_3$ و $\odot_3$ با $\bar{\odot}_3$ 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 b، و a 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 $X/\sim=\{[(m,n)]\mid m,n\in\mathbb{Z}, n\neq 0\}$ 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 **ثابت‌های** 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 که 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:

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

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** می‌- نامند.

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** یـا **ماگما** مـی‌نـامیم. 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 دسـتگاه جبـری بسـیار کلـی است و تنها دسته‌بندی‌ای که تاکنون از آن‌ها انجام دادیم، بر حسب **نوع** یـا **نشـان** آن‌هـا اسـت. ولـی معمولاً دستگاه‌های جبری از یک نوع τ را نیز برحسب برخـی از **ویژگی**‌هـایی کـه بـه اشـتراک دارنـد دسته‌بندی می‌کنیم. برای مثال، می‌توانیم همه‌ی آن دستگاه‌های جبری تک- یکـانی را در یـک دسـته 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 مـثلاً دقیقـاً دارای سـه جـواب باشـد؛ یـا همه‌ی دستگاه‌های جبری A از نوع $\tau = (2,0)$ را در یک دسته قرار دهـیم کـه دارای ویژگـی‌هـای استلزامی و وجودی

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

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

۹.۲.۱ تعریف. فرض کنیم $\mathcal{A}\lg(\tau)$ دسته‌ی همه‌ی دستگاه‌های جبـری از نـوع τ باشـد. فـرض کنیم P مجموعه‌ای از **ویژگی**‌ها باشد (P حرف اول کلمه‌ی Property به معنی ویژگـی اسـت). در این صورت، می‌گوییم که $A \in \mathcal{A}\lg(\tau)$ یک P - **جبر** است اگر A دارای ویژگی‌های داده شـده 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 می‌شـود. 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 بحـث 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** +) $$(\forall a,b,c \in \mathbb{Z}) \qquad a+(b+c)=(a+b)+c$$

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

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

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

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

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 بـه انـدازه‌ی نیـاز این کتاب، این مفاهیم را با مثال توضیح می‌دهیم.

فرض کنیم $*_1$، $*_2$ نمادهایی برای عمل‌هایی دوتایی، λ نمـادی بـرای عملـی یکـانی، 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. بـرای مثـال، $x_1x_2^{-1} + (-x_1) + 1 = x_2$ ،$x_1x_2 - x_1^{-1} + x_2 + 1 = 0$ معادله‌هایی حاصل از عمل‌هـای دوتـایی جمع و ضرب، عمل‌های یکانی قرینه‌یابی و وارون‌گیری، و عمل‌های صفر- تایی (ثابت‌هـای) 0 و 1 و دو متغیر x_1 و x_2 در اعداد حقیقی هستند. هر عبارت در یک طرف تساوی‌هـای بـه صـورت بـالا را یـک **جمله** می‌گوییم. به طور کلی‌تر، به زبان غیر رسمی، فرض کنـیم $p(x_1,\cdots,x_n)$ و $q(x_1,\cdots,x_n)$ جمله‌هایی مانند مثال‌های بالا باشـند کـه از عمـل‌هـا و مجموعـه‌ی متغیـرهـای $X = \{x_1,\cdots,x_n\}$ 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

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

که در آن $p(a_1,...,a_n)$ از جایگذاری a_iها به جـای x_i هـا در جملـه‌ی $p(x_1,...,x_n)$ بـه دسـت 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

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

می‌گوییم که معادله‌ی $p(x_1,\cdots,x_n) = q(x_1,\cdots,x_n)$ در A برقرار، درست، یـا **اتحـاد** اسـت، و می‌نویسیم $A \models (p = q)$ و در غیر این صورت، می‌نویسیم $A \not\models (p = q)$. اگر P مجموعـه‌ای از معادله‌ها باشد به طوری که برای هر معادله‌ی $(p = q) \in P$، داشته باشیم $A \models (p = q)$، مـی-نویسیم $A \models P$.

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

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

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

$$\begin{aligned}(p_1(a_1,\cdots,a_n) = q_1(a_1,\cdots,a_n)) \wedge \cdots \wedge (p_k(a_1,\cdots,a_n) = q_k(a_1,\cdots,a_n)) \\ \Rightarrow (p(a_1,\cdots,a_n) = q(a_1,\cdots,a_n))\end{aligned}$$

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

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

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:

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

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

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

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،

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

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، **نیم‌گروه 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:

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

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

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 $x,y\in A$،

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

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:
>
> $$(\forall x, y, z \in A) \quad x * (y * z) = (x * y) * z$$ (**اتحاد** شرکت پذیری)
>
> $$(\forall x \in A) \quad x * e = x = e * x$$ (**اتحاد** ویژگی عضو همانی)

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:

$$\begin{array}{c|cc} *_1 & e & f \\ \hline e & e & f \\ f & f & ? \end{array}$$

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

$$\begin{array}{c|cc} *_1 & e & f \\ \hline e & e & f \\ f & f & e \end{array} \quad , \quad \begin{array}{c|cc} *_2 & e & f \\ \hline e & e & f \\ f & f & f \end{array}$$

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:

$$\begin{array}{c|cc} *_3 & f & e \\ \hline f & f & e \\ e & e & f \end{array} \quad , \quad \begin{array}{c|cc} *_4 & f & e \\ \hline f & f & e \\ e & e & e \end{array}$$

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:

$$\begin{array}{c|cc} x & e & f \\ \hline \varphi(x) & f & e \end{array}$$

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:

$$\begin{array}{c|cc} x & e & f \\ \hline \psi(x) & 0 & 1 \end{array}$$

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

$$\begin{array}{c|cc} \oplus_2 & 0 & 1 \\ \hline 0 & 0 & 1 \\ 1 & 1 & 0 \end{array}$$

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

$$\begin{array}{c|cc} \cdot_2 & 0 & 1 \\ \hline 0 & 0 & 0 \\ 1 & 0 & 1 \end{array}$$

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 بند**۴**، 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، جامع-تر 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

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

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 $\mathbf{min}\{m,n\}$ 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 $\mathbf{min}$ یک M- مجموعه است.

۹- فرض کنید M یک تکواره باشد. نشان دهید که $\wp(M)$ همراه با عمل (موسوم به تقسیم) به صورت $m\cdot X=\{s\in M: sm\in X\}$ 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 $-n+n=\circ=n+(-n)$. 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 $\mathbb{Z}_4 = \{\circ,1,2,3\}$ 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 بزنیدکدام 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،

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

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 $۲x=۵$ 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 **فصل۲** 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

$$\begin{aligned}G&\to G\\ x&\mapsto x^{-1}\end{aligned}$$

در نظر بگیریم (یکتایی وارون‌ها ایجاب می‌کند که این ضابطه تابعی خوش‌تعریف به دست دهد)، آنگاه گروه را می‌توانیم دستگاهی جبری چون $(G;*,\cdot^{-1},e)$ 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، به ویژه در علوم کامپیوتر نظری، دارند.

۳- به راحتی می‌توانید تشخیص دهید که از مثال‌هایی که تاکنون آوردیم کدام‌ها گروه هستند. اجازه دهید مثال دیگری بیاوریم. فرض کنید F_X، M_X، و S_X، به ترتیب، مجموعه‌ی همه‌ی توابع، توابع 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 تحت ترکیب توابع گروه است.

۷.۴.۱ شبه‌گروه. حال می‌خواهیم دستگاه جبری **شبه‌گروه** را معرفی کنیم. این دستگاه جبری کاربردهایی مفید، برای مثال در علوم کامپیوتر، ترکیبیات، هندسه، و طرح آزمایش‌ها (در علم آمار)، 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** به گروه 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 به گروه است، می‌آوریم).

۸.۴.۱ قضیه. *فرض کنیم* $(G;*)$ *نیم‌گروهی* ***ناتهی*** *باشد. در این صورت،* G *گروه است اگر 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 معادله‌های $a*x=b$ و $y*a=b$ یکتا است. یادآوری می‌کنیم که در این موارد فرض می‌کنیم که هر دو عضو c و d جواب $a*x=b$ هستند، یعنی $a*c=b=a*d$، و سپس با استفاده از تعریف گروه، **(گ۱)-(گ۳)**، نشان می‌دهیم که $c=d$ (**نشان دهید.**)

۲- حال نتیجه‌ی جالب و مفیدی را که از قضیه‌ی بالا به دست می‌آید، بیان می‌کنیم. فرض کنیم 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 کیلی گروه G، هر 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 فصل **۲** 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:

$$\begin{array}{c|ccc} * & a & b & c \\ \hline a & c & a & b \\ b & b & c & a \\ c & a & b & c \end{array}$$

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** $x=a\setminus b$ و **تقسیم راست** $y=a/b$ نشان می‌دهیم. بنابراین، عمل‌های دوتایی

$$\begin{aligned}\setminus : A\times A &\to A \\ (a,b) &\mapsto a\setminus b\end{aligned} \qquad \begin{aligned}/ : A\times A &\to A \\ (a,b) &\mapsto b/a\end{aligned}$$

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

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

برای مثال، بنا به تعریف عمل تقسیم چپ، عضو $a\setminus(a*b)$ جواب منحصر به فرد $a*x=a*b$ است. از طرفی b نیز جواب این معادله است. پس $a\setminus(a*b)=b$. 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:

$$\begin{aligned} &R \times A \to A \\ &(r,a) \mapsto l_r(a) = ra \end{aligned}$$

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

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

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 $\le$ 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 $\le$ را در L به صورت زیر تعریف کرد

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

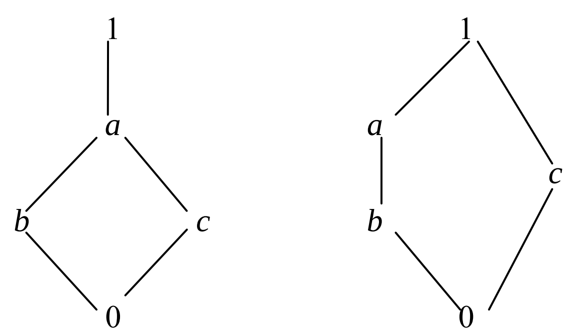
که می‌توانید با استفاده از قوانین جذب نشان دهید که معادل با $x \wedge y = x$ است:

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

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 $(A;*,/,\backslash)$ در نظر بگیریم، آنگاه اتحادهای زیر در آن برقرار هستند:

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

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.

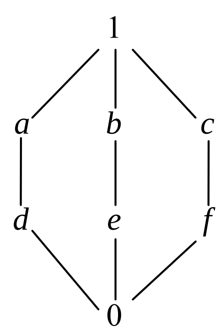
۸- ثابت کنید که مجموعه‌ی توابع حقیقی روی $[0,1]$ همراه با رابطه‌ی $\leq$، که به صورت نقطه‌ای تعریف می‌شود، یعنی

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

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 $a \wedge b$، $a \wedge c$، $d \wedge b$، $d \vee e$، $d \vee f$، 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 $a_\circ$ را در A مشخص می‌کند. فرض کنیم $(A;a_\circ)$ و $(B;b_\circ)$ دستگاه‌های جبری از نوع $\tau=(0)$ باشند. طبیعی است که توابعی از A به B مورد نظر باشند که $a_\circ$ را بر $b_\circ$ 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:

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

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:

$$\begin{tikzcd}
(x,y) \arrow[rrr, dashed] \arrow[ddd, dashed] & & & (f(x),f(y)) \arrow[ddd, dashed] \\
& A\times A \arrow[r, "(f,f)"] \arrow[d, "*^A"'] & B\times B \arrow[d, "*^B"] & \\
& A \arrow[r, "f"] & B & \\
x*^A y \arrow[rrr, dotted] & & & f(x*^A y)=f(x)*^B f(y)
\end{tikzcd}$$

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:

$$\begin{tikzcd}
(a_1,\cdots,a_n) \arrow[rrr, dashed] \arrow[ddd, dashed, "\lambda^A"'] & & & (f(a_1),\cdots,f(a_n)) \arrow[ddd, dashed, "\lambda^B"] \\
& A^n \arrow[r, "(f,\cdots,f)"] \arrow[d] & B^n \arrow[d] & \\
& A \arrow[r, "f"] & B & \\
\lambda^A(a_1,\cdots,a_n) \arrow[rrr, dotted] & & & f(\lambda^A(a_1,\cdots,a_n))=\lambda^B(f(a_1),\cdots,f(a_n))
\end{tikzcd}$$

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:

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

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

$$f(x+y)=e^{x+y}=e^x\cdot e^y=f(x)\cdot f(y) \quad \text{(حفظ عمل دوتایی)}$$
$$f(-x)=e^{-x}=(e^x)^{-1}=f(x)^{-1} \quad \text{(حفظ عمل یکانی)}$$
$$f(\circ)=e^\circ=1 \quad \text{(حفظ عمل صفرتایی)}$$

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

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

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 ۰، 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،

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

اثبات. به فن اثبات توجه کنید! داریم

$$f(e)=f(e*e) \qquad (\text{زیرا} \;...)$$
$$=f(e)*'f(e) \qquad (\text{زیرا} \;...)$$

حال، از این تساوی نتیجه می‌گیریم که

$$f(e)^{-1}*'f(e)=f(e)^{-1}*'(f(e)*'f(e)) \qquad (\text{چطور؟})$$
$$\Rightarrow e'=(f(e)^{-1}*'f(e))*'f(e) \qquad (\text{چرا؟})$$
$$=e'*'f(e)=f(e)$$

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

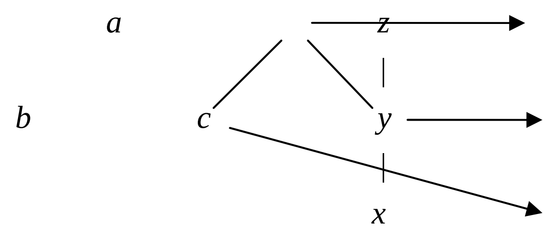
$$\begin{aligned} f(\lambda^A(f^{-1}(b_1),\cdots,f^{-1}(b_n))) &= \lambda^B(ff^{-1}(b_1),\cdots,ff^{-1}(b_n)) \\ &= \lambda^B(b_1,\cdots,b_n) \end{aligned}$$

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 $A \xrightarrow{f} B \xrightarrow{g} C$ یک-ریختی 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.

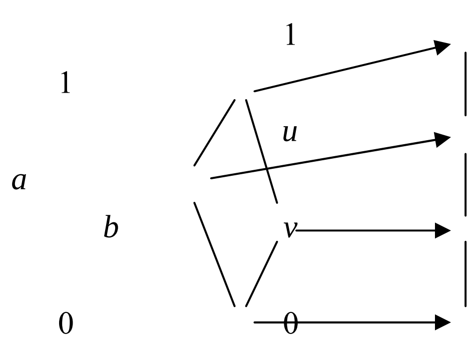
۴- فرض کنید که $Hom(A,B)$ مجموعه‌ی همه‌ی همریختی‌ها از گروهواره‌ی $(A,*_A)$ به گروهواره‌ی $(B,*_B)$ باشد. آیا عمل دوتایی * با تعریف

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

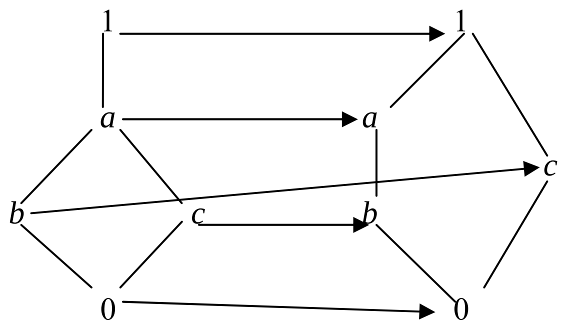
روی $Hom(A,B)$ خوش‌تعریف است؟ اگر A و B تعویض‌پذیر (آبلی) باشند، **چطور؟**
آیا اگر A و B گروه‌هایی آبلی باشند، آنگاه $Hom(A,B)$ نیز چنین است؟

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 $B=\{0,2\}$ تحت عمل جمع همنهشتی به پیمانه‌ی ۴ (یعنی، عمل $+_4$ در $\mathbb{Z}_4=\{0,1,2,3\}$) بسته است، پس عمل $+_4$ بر B تحدید می‌شود. ولی همین مجموعه‌ی $B=\{0,2\}$ 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 $2+_4 1=3\neq 0$ (4. حال، **تعریف جامع** زیر را می‌آوریم.

۳.۶.۱ تعریف. فرض کنیم $A,B\in\mathcal{A}\lg(\tau)$ 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، **مجموعه**ی $\mathbb{N}$ **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

$$\begin{array}{c|cc} * & e & f \\ \hline e & e & f \\ f & f & f \end{array}$$

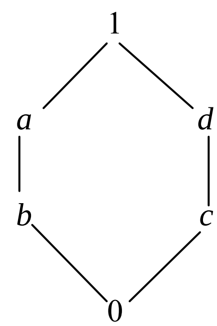
در نظر بگیرید. فرض کنید $B = \{f\}$. اگر تعریف تکواره را به صورت دستگاهی جبری از نوع $\tau = (2)$، تعریف **۱۰.۳.۱**، در نظر بگیریم که دارای ویژگی (**وجود** عضو همانی)

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

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

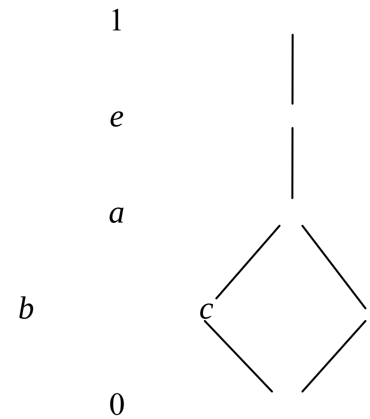
زیرتکوارهی A در نظر نمی‌گیرند، و لذا، در این مثال، تنها A و $\{e\}$ را زیرتکوارهی A در نظر می-گیرند! البته، اگر تعریف تکواره را به صورت دستگاهی جبری از نوع $\tau=(2,0)$، تعریف **۱۱.۳.۱**، در نظر بگیریم، آنگاه تعریف زیردستگاه **۶.۶.۱** به خودی خود ایجاب می‌کند که B نه تنها باید تحت عمل دوتایی * بسته باشد 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 :

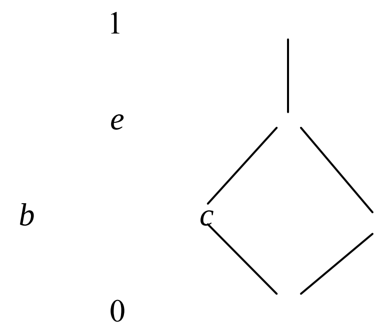


روشن است که $X=\{0,a,b\}$ زیرمشبکه‌ی A محسوب نمی‌شود، زیرا $1\notin X$ (اگر چه نسبت به $\vee$ و $\wedge$ بسته است و خود یک مشبکه‌ی کرانداراست، که در آن b بزرگ‌ترین و 0 کوچک‌ترین عضو است). دلیل بیاورید که $C=\{0,b,c,1\}$ و $D=\{0,b,d,1\}$ زیرمشبکه‌ی A هستند.

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

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

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 $S=\{B \le A \mid X \subseteq B\}$، آنگاه $<X> = \bigcap_{B\in S} B = \bigcap\{B \le A \mid X \subseteq B\}$

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 $(X) = <X> = \bigcap\{B \le A \mid X \subseteq B\}$.

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 $x^n = x*x*\cdots*x$ (n مرتبه) (یعنی، نشان دهید که $B=\{x^n \mid n\in\mathbb{N}\}$ زیرنیم‌گروه 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.

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

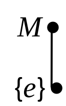
۱۹.۶.۱ تعریف. نمودار مشبکه‌ی $(Sub(A);\subseteq)$ را **نمودار مشبکه‌ی زیردستگاه‌های** A می‌نامیم.

۲۰.۶.۱ بحث در کلاس

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

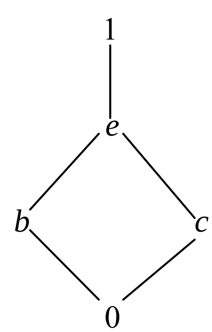
	e	f
e	e	f
f	f	f

نمودار مشبکه‌ی زیرتکواره‌های آن به صورت زیر است:

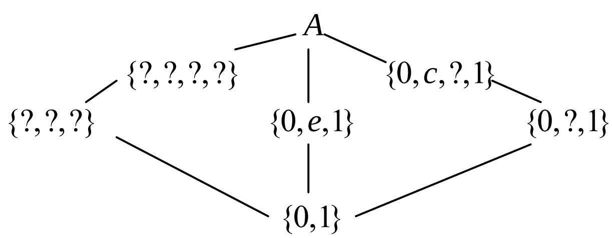


مشبکه‌ی زیرگروهواره‌های آن قدری متفاوت است. آن را تعیین کنید.

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.۱.۴** 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** $A\xleftarrow{f} C \xrightarrow{g} B$، **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.۱.۴**، 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.۱.۵** 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.۱.۵** 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 $A\xrightarrow{f}X\xleftarrow{g}B$، 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.**)

$$\begin{tikzcd} & X & \\ B \arrow[ur, "g"] \arrow[r, "j"] & {[?]} \arrow[u, dotted, "h"] & A \arrow[ul, "f"'] \arrow[l, "i"'] \end{tikzcd}$$

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.

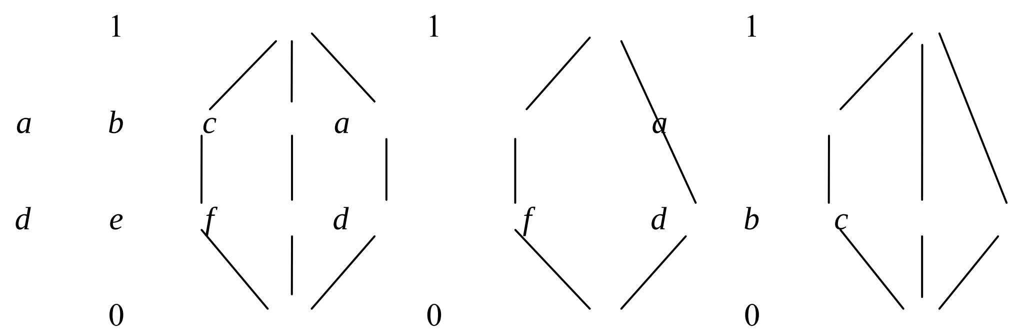
۳- نمودار مشبکه‌ی زیرگروهواره‌های گروهواره‌ی $(\{0,1,2,3\};+_4,0)$ را نشان دهید.

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.

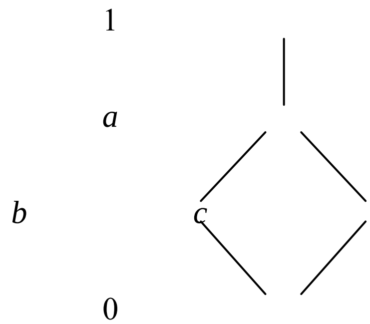
۶- فرض کنید $f : A \to A$ همریختی روی دستگاه جبری A باشد. نشان دهید که $E = \{(a,b) \in A \times A \mid f(a) = f(b)\}$ زیرجبر $A \times A$ است.

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، C و D ساختارهای 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 C زیرجبر 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 C زیرگروه 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 کـه A را بـه دسـته‌هـای جـدا از هـم تقسیم، یعنی **افراز**، کنیم. ولی، همان طور که در مورد مفاهیم زیردستگاه و حاصل‌ضرب دیدیم، انتظـار داریم که خارج قسمت هر دستگاه جبری از **نوع** τ دستگاهی جبری ازهمان **نوع** τ باشـد! از ایـن رو، باید **عمل‌هایی** در افراز $\mathcal{P}$ تعریف کنیم که از آن یک دستگاه جبری از نوع τ بسازد. همچنین، ماننـد موردهای زیردستگاه جبری و حاصل‌ضرب، این عمل‌ها نیز باید به‌گونه‌ای حاصل از عمـل‌هـای دسـتگاه 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 چـون $\bar{*}$ در $\mathcal{P}$ تعریف کنیم. فرض کنیم $X,Y\in\mathcal{P}$. **حدس** می‌زنید که

$$X\,\bar{*}\,Y=\{?\}$$

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

$$X\,\bar{*}\,Y=\{x*y\mid x\in X,\,y\in Y\}$$

ولی آیا **تضمینی** وجود دارد که $X\,\bar{*}\,Y$ متعلق به $\mathcal{P}$ باشد؟ یعنی آیا $\mathcal{P}$ نسبت بـه عمـل $\bar{*}$ **بسـته 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

$$\{2\}\,\bar{\oplus}_4\,\{0,1\}=\{2\oplus_4 0,2\oplus_4 1\}=\{2,3\}\notin\mathcal{P}$$

در این لحظه ممکن است عقل سلیم و سلول‌های خاکستری نتوانند بیشتر از ایـن یاریمـان دهنـد! اجازه بدهید موضوع را از زاویه‌ی دیگری بررسی کنیم. قضیه‌ی بسـیار مهـم و زیبـایی در درس **مبـانی علوم ریاضی** دیدیم (تمرین **۴** از بخش **م.۱** را ببینید) که می‌تواند دریچه‌ی دیگری به روی سلول‌هـای خاکستری بگشاید. این قضیه در واقع بیان می‌کند که هر افراز $\mathcal{P}$ از مجموعه‌ی A حاصـل از رابطـه‌ای هم‌ارزی روی A است، و بـرعکس. از ایـن رو، فـرض مـی‌کنـیم کـه $\sim$ رابطـه‌ای هـم‌ارزی روی A و $\mathcal{P}=A/\sim$ افراز حاصل از آن باشد. حال، عقل سلیم در باره‌ی حاصل $[x]\,\bar{*}\,[y]$ **چـه پیشـنهاد می‌کند**؟ یقین داریم که می‌گویید $[x]\,\bar{*}\,[y]=[x*y]$. ولی با وجودی که به روشنی $\mathcal{P}$ نسبت به این عمل بسته است، **آیا** این دستور عمل زیبا **خوش‌تعریف** است؟ یعنی، آیا

$$\begin{cases}[x]=[x'] \\ [y]=[y']\end{cases}\Rightarrow [x]\,\bar{*}\,[y]=[x']\,\bar{*}\,[y'] \quad (\Leftrightarrow [x*y]=[x'*y'])$$

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 $\bar{*}$ 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

$$(x,x'),(y,y') \in \sim \;\Rightarrow\; \begin{cases} x \sim x' \\ y \sim y' \end{cases} \;\Rightarrow\; x * y \sim x' * y'$$
$$\Rightarrow\; (x * y \sim x' * y') \in \sim$$

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 $[a]=aN$! 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 **تکواره**‌ی ضربی $(\mathbb{Z}_4;\cdot_4)$ همنهشتی است، ولی $\{0,2,3\}$ برابر با هیچ یک از مجموعه‌های $0*\{1\}$، $2*\{1\}$، یا $3*\{1\}$ **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 $3\sim 1$ و $\sim$ همنهشتی است، پس $3\oplus_4 3\sim 1\oplus_4 3$ یا $2\sim 0$. 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 مقاله‌ها-ی بسیاری در این باره نوشته شده است. مثال اخیر را در فصل۲ در باره‌ی گروه‌ها حل می‌کنیم. توجه می کنیم 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.۱.۹** 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.۱.۱۰** بیان می‌کند که **نگاره‌ی** هر تابع f اساساً **خارج قسمتی** از A است، یعنی $f(A) \cong A/\sim_f$.

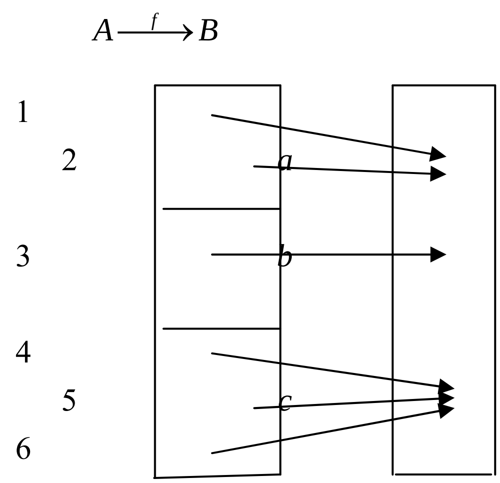
در اینجا خواهیم دید که همتای همه‌ی این مطالب برای هر **همریختی** $f: A \to B$ بین دستگاه‌های کلی جبری (ازجمله، گروه، حلقه، مشبکه، . . .) نیز **برقرار است**! از این رو، بسیاری از مطالب مهمی را که در زیر می‌آوریم، تقریباً **تکرار** مطالبی است که در مقدمه آوردیم (که دو بار دیگر در فصل‌های **۲** و **۳** 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.۱.۸** 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 $Ker f$، K_f ، یا $\sim_f$ نشان می‌دهیم. بنابراین،

$$a \sim_f b \Leftrightarrow a\, K_f\, a' \quad \Leftrightarrow \quad f(a) = f(a')$$



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- *برعکس، 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 **م.۹.۱** 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

$$
\begin{aligned}
a \sim_{\gamma} a' \quad \Leftrightarrow \quad \gamma(a)=\gamma(a') \quad &\Leftrightarrow \quad [a]_{\sim}=[a']_{\sim} \\
&\Leftrightarrow \quad a \sim a'
\end{aligned}
$$

۳- این حکم در لم **م.۱.۹** اثبات شد. ■

قضیه‌ی زیر همتای قضیه‌ی اساسی **م.۱.۱۰** 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.۱.۱۰** دیدیم که تابع

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

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 فصل‌های **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

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

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 $\theta \subseteq \sim \subseteq \Delta \Rightarrow \theta = \sim$ یا $\sim = \Delta$.)

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 $\overline{f}|_X = f|_X$، یعنی، برای هر $x \in X$، $\overline{f}(x) = f(x)$. یعنی، نمودار زیر تعویض‌پذیر باشد:

$$\begin{tikzcd} X \arrow[r, "i"] \arrow[dr, "f"'] & A \arrow[d, "\overline{f}"] \\ & B \end{tikzcd}$$

در این صورت، X را **پایه**‌ی 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 بـه 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، کـه **تناقض** اسـت! توجـه کنیـد کـه، 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، کـه در آن هـر 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 کـه 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 محاوره-ای، معمولاً کلمه‌هایی از حروف الفبا می‌سازیم که در آن زبان با معنی باشند. روشن است که مجموعه-ی 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 کـه مجموعـه‌ی **اعـداد اول** نـامزد 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:

$$\cdots,\ (-۱)+(-۱)+(-۱),\ \ (-۱)+(-۱),\ \ -۱,\ \ ۰=۱+(-۱)$$

شرط **۲** را نیز باید تغییر دهیم! زیرا، برای مثال

$$۱+(-۱)=۰+۰+۰=۰+۰ \quad \text{یا} \quad ۱+۱=۱+۰+۱+(-۱)+۱$$

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 $\varnothing=X\cap X^{-1}$ 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 **1.8.1** می‌توانید نشان دهید که $(Y^*;*,{\cdot}^{-1},e)$ 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:

<table><tr><td>

۱- زیرمجموعه‌ی C یک کد روی X است.

۲- برای تابع شمولی $f : C \rightarrowtail < C >$ ، همریختی منحصر به فرد $\overline{f} : C^* \to < C >$ مذکور در تعریف **۱.۸.۱** دوسویی است.

۳- مجموعه‌ی B و همریختی یک به یک نیم‌گروه‌ها چون $k : B^* \to X^*$ وجود دارد به طوری که $k(B) = C$.

</td></tr></table>

همریختی یک به یک k در بند **۳** قضیه‌ی بالا را **همریختی کدگذار** و وارون آن $k^{-1} : < C > \to B^*$ 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.