فصل ۲

گروه‌ها

در **فصل ۱** مفاهیم دستگاه جبری (نه لزوماً با ویژگی) و P - جبر (با ویژگی P) را معرفی و برخی از مفاهیم، مانند **زیرجبر**، **ضرب**، **همضـرب**، **خـارج قسـمت**، و **همریختـی**، را کـه در همـه‌ی دستگاه‌های جبری مشترک هستند، بررسی کردیم. همان طور که در فصل **۱** نیز بیان شـد، تقریبـاً همه‌ی دستگاه‌های جبری‌ای که مطالعه خواهیم کرد P - جبری با یک یا چند **ویژگی** هسـتند. در بخش‌های **۲.۱** تا **۴.۱**، P - جبرهای نیم‌گروه، تکواره، حلقه، مشبکه، شبه‌گروه، و گروه را، به عنـوان نمونه‌هایی از دستگاه‌های جامع جبری با ویژگی، معرفی کردیم و قرار شـد دسـتگاه تـاریخی و پـر کاربرد گروه را در این فصل با جزییات بیشتری مورد مطالعه قرار دهیم.

از آنجا که هر بخش این فصل همتا و حالت خاص قسمتی یا تمام بخشی از **فصل ۱** اسـت، بـه شما خوبان **توصیه** می‌کنیم که شب قبل از کلاس چند دقیقـه‌ای حالـت کلـی موضـوع درس را از فصل **۱** مرور کنید تا درک بهتر و درست‌تری از هر دو حالت کلی و خاص به دست آورید. در ضمن، استاد درس نیز ممکن است برای صرفه جویی در وقت برخی از مطالب و فنون اثبات را تکرار نکنـد و به **فصل ۱** رجوع دهد!

مطابق معمول این کتاب و قولی که دادیم، در ارائه‌ی مطالب، بلافاصله سر اصـل مطلـب نمـی-رویم بلکه تا جایی که زمان اجازه دهد، شما خوانندگان را با **فوت و فن** کار آشنا می‌کنـیم و روش کار را آموزش می‌دهیم تا آمادگی بیش‌تری برای مطالعه‌ی فصل **۳** و درس‌های دیگر جبر به دست آورید. البته مجدداً سفارش می‌کنیم که

اندیشیدن بیاموزیم و اندیشه ورزی کنیم

۱.۲ قضیه‌های معادل تعریف گروه

در این بخش، ابتدا تعریف ۵.۴.۱ گروه و صورت معادل آن را از بند۲ بحث ۶.۴.۱ یادآوری می‌کنیم و آن‌ها را مورد بحث قرار می‌دهیم. سپس چند قضیه‌ی دیگر معادل با تعریف گروه ارائه می‌کنیم که هر یک سودمندی و کارایی ویژه‌ای دارد.

۱.۱.۲ تعریف. نیم‌گروه $(G;*)$ را **گروه** می‌نامیم اگر دارای عضو **همانی** باشد و هر عضو آن **وارون** داشته باشد. به عبارت دیگر، گروهواره‌ی $(G;*)$ را **گروه** می‌نامیم اگر دارای شرایط زیر باشد:

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

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

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

۲.۱.۲ بحث در کلاس

۱- با توجه به قضیه‌ی ۷.۳.۱، عضو همانی در هر گروه منحصر به فرد است و بنابر شرکت‌پذیر بودن عمل دوتایی گروه، هر عضو در گروه وارون یکتا دارد (قضیه‌ی ۳.۴.۱ را ببینید. البته توصیه می‌کنیم خودتان اثبات ساده‌ی آن را دوباره ارائه دهید). از این رو، در تعریف بالا نمادهای مشخصی به این عضوها اختصاص داده‌ایم.

۲- (اختیاری) تعریف گروه به همان صورت ۱.۱.۲ بین افرادی که با جبرهای سنتی سروکار دارند متداول‌تر است، ولی در فصل ۱ به دفعات گفتیم و دیدیم که اگر شرط‌های معرف یک دستگاه جبری را بتوان با **اتحاد**ها (بدون استفاده از سورهای وجودی) نیز بیان کرد، کار کردن با آن دستگاه، به ویژه با استفاده از برنامه‌های رایانه‌ای، آسان‌تر است. اگر چه شرط **(گ۱)** تعریف گروه به صورت اتحاد است ولی دو شرط دیگر **(گ۲)** و **(گ۳)** دارای سور وجودی هستند و از این رو اتحاد محسوب نمی‌شوند. سؤال بسیار مهم این است که، آیا می‌شود مفهوم گروه را به گونه‌ای معرفی کرد که اصول موضوع **(گ۲)** و **(گ۳)** تعریف ۱.۱.۲ گروه نیز اتحاد باشند؟ خوشبختانه پاسخ به این سوال مثبت است. مشابه تعریف ۱۱.۳.۱ برای تکواره و تعریف شبه‌گروه در بند ۴ بحث ۱۱.۴.۱، اگر عضو همانی منحصر به فرد گروه، یعنی e، را به عنوان عملی صفرتایی و وارون‌گیری منحصر به فرد را عملی یکانی چون

$$\cdot^{-1}:G\to G \qquad\qquad \{0\}\to G$$
$$x\mapsto x^{-1} \qquad\qquad 0\mapsto e$$

در نظر بگیریم، آنگاه تعریف زیر نشان می‌دهد که مفهوم گروه را می‌توانیم به جای دستگاه جبری $(G;*)$ از نوع $\tau=(2)$، به صورت دستگاهی جبری چون $(G;*,^{-1},e)$ از نوع $\tau=(2,1,0)$ معرفی کنیم، و سورهای وجودی در **(گ۲)** و **(گ۳)** را حذف و در نتیجه این دو اصل معرف گروه را نیز مانند **(گ۱)** به صورت دو **اتحاد** بیان کنیم.

۳.۱.۲ تعریف (صورت دوم). دستگاه جبری $(G;*,^{-1},e)$ از نوع $\tau=(2,1,0)$ **گروه** است اگر سه **معادله**‌ی زیر در آن برقرار (یعنی **اتحاد**) باشند:

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

(گ۲) (**اتحاد رابطه‌ی عمل صفرتایی e با $*$**) $(\forall x\in G)\quad x*e=x=e*x$

(گ۳) (**اتحاد رابطه‌ی عمل یکانی $^{-1}$ با e و $*$**) $(\forall x\in G)\quad x*x^{-1}=e=x^{-1}*x$

۴.۱.۲ بحث در کلاس

۱- یکی از ویژگی‌های مهم تعریف **۳.۱.۲** گروه این است که اصول معرف گروه‌ها، **اتحاد** هستند. از این رو، هر آنچه در فصل **۱** در باره‌ی خوبی‌های دستگاه‌های معادله‌ای گفتیم در باره‌ی گروه‌ها نیز برقرار هستند. به ویژه قضیه‌ی **۲.۹.۱** بیرخوف نتیجه می‌دهد که دسته‌ی گروه‌ها، نسبت به **زیرگروه**، **حاصل‌ضرب**، و**خارج قسمت** بسته است؛ یعنی، زیردستگاه جبری گروه‌ها، حاصل‌ضرب گروه‌ها، و خارج قسمت گروه‌ها، خود گروه هستند. **عالی است!** البته این مفاهیم را دوباره برای گروه‌ها مطالعه خواهیم کرد. توجه می‌کنیم که اگر $\mathcal{K}$ زیردسته‌ای از دسته‌ی گروه‌ها با یک (یا چند) ویژگی غیر اتحادی باشد، آنگاه این دسته لزومی ندارد نسبت به زیرگروه، حاصلضرب، وخارج قسمت بسته باشد. برعکس، اگر دسته‌ی $\mathcal{K}$ طوری انتخاب شده باشد که نسبت به زیرگروه، حاصل‌ضرب، یا خارج قسمت بسته نباشد، آنگاه این کلاس با دسته‌ای از اتحادها مشخص نمی‌شود (قضیه‌ی دو طرفه‌ی **۲.۹.۱** بیرخوف را ببینید). این مطالب را در درس‌های دیگر جبر نیز تجربه خواهید کرد.

۲- مفهوم گروه از چه زمانی و چطور وارد مباحث ریاضی شده است؟ چرا این دستگاه جبری ساده این اندازه با اهمیت است و پژوهش‌های بسیاری روی آن انجام شده است و می‌شود؟ تقریباً در هر گروه آموزشی ریاضی در دنیا، و البته در ایران، دست کم یک متخصص نظریه‌ی گروه‌ها وجود دارد.

نام ریاضی‌دانانی چون **لاگرانژ**، **آبل**، و به ویژه **گالوا** همواره با نظریه‌ی گروه‌ها آورده می‌شود. این افراد، به ویژه گالوا، در جستجوی پاسخی برای وجود یا عدم وجود فرمولی رادیکالی (مانند $(-b\pm\sqrt{b^2-4ac})/2a$ برای ریشه‌های ax^2+bx+c) برای پیدا کردن ریشه‌های چند

جمله‌ای‌های از درجه بیش‌تر از ۴، به دستگاهی جبری، حاصل از جایگشت‌های ریشه‌ها، دست یافتند که بعدها گروه نامیده شد. پاسخ به سؤال بالا در ویژگی‌های این گروه نهفته است. بررسی ویژگی‌های این گروه و چگونگی استفاده از آن در پاسخ به سؤال بالا، در درس نظریه‌ی گالوا مطالعه می‌شود.

۳- اجازه بدهید چند نمادگذاری را یادآوری کنیم که کار نوشتن را کوتاه‌تر و ساده‌تر می‌کنند. از این پس، اگر امکان اشتباه نباشد، بیشتر به جای $x*y$، **نمادگذاری ضربی** xy را به کار می‌بریم و حتی آن را **حاصل‌ضرب** می‌نامیم. البته اگر G آبلی باشد (یعنی، معادله‌ی $xy=yx$ برای هر $x,y\in G$ برقرار باشد)، گاهی از **نمادگذاری** جمعی $x+y$ نیز استفاده می‌کنیم و G را گروهی جمعی می‌نامیم. در این صورت، معمولاً وارون x را قرینه‌ی x می‌نامیم و با $-x$ نشان می‌دهیم و نماد صفر 0 را برای عضو همانی به کار می‌بریم و آن را **عضو خنثی** نیز می‌نامیم. همچنین، به دلیل شرکت‌پذیر بودن عمل دوتایی گروه، اغلب از نوشتن پرانتزها صرف نظر می‌کنیم و برای مثال می‌نویسیم xyz، $xyztu$ و از این قبیل. قبل از ادامه‌ی بحث، خوب است تکلیف نمادگذاری توانی x^n را در نمادگذاری ضربی و جمعی نیز روشن کنیم.

$$x^n=\begin{cases} xx\cdots x & (n>0)\\ e & (n=0)\\ x^{-1}\cdots x^{-1} & (n<0)\end{cases},\qquad nx=\begin{cases} x+\cdots+x & (n>0)\\ 0 & (n=0)\\ -x-x\cdots-x & (n<0)\end{cases}$$

که در آن $x-y=x+(-y)$. با استقرا می‌توانید نشان دهید که برای هر $m,n\in\mathbb{Z}$، در **نمادگذاری ضربی**، داریم $x^mx^n=x^{m+n}$ و $(x^m)^n=x^{mn}$ و در **نمادگذاری جمعی**، $(m+n)x=mx+nx$ و $n(mx)=(nm)x$.

۴- در تعریف گروه $(G;*)$، به طور صریح صحبت از ناتهی بودن مجموعه‌ی G نشده است، ولی شرط وجود عضو همانی e ایجاب می‌کند که G ناتهی باشد. عدد اصلی مجموعه‌ی G را **مرتبه‌ی** گروه $(G;*)$ می‌نامیم و با $|G|$ نشان می‌دهیم. هرگاه $|G|$ متناهی یا نامتناهی باشد، گروه $(G;*)$ را متناهی یا نامتناهی می‌گوییم.

۵- نمونه‌های دستگاه جبری گروه در سراسر علوم ریاضی و علوم دیگر، به ویژه فیزیک و شیمی، بسیارند و چند نمونه را در فصل ۱ دیدیم؛ از جمله، گروه‌های جمعی اعداد $(\mathbb{Z};+)$، $(\mathbb{Q};+)$، $(\mathbb{R};+)$، $(\mathbb{C};+)$، و گروه‌های ضربی اعداد $(\mathbb{Q}^*;\cdot)$، $(\mathbb{R}^*;\cdot)$، $(\mathbb{C}^*;\cdot)$. در زیر چند مثال دیگر می‌آوریم، و به مرور با مثال‌های بیشتری در این درس و درس‌های دیگر آشنا می‌شویم.

(الف) نشان دهید که هر یک از مجموعه‌های اعداد صحیح زوج $E=2\mathbb{Z}=\{2k\mid k\in\mathbb{Z}\}$ و مضارب صحیح عدد طبیعی n، $n\mathbb{Z}=\{nk\mid k\in\mathbb{Z}\}$، همراه با جمع معمولی اعداد، گروه تشکیل می‌دهد. همراه با ضرب اعداد **چطور؟**

(ب) مجموعه‌ی $G_n = \{z \in \mathbb{C} \mid z^n = 1\}$ همراه با عمل ضرب اعداد مختلط گروه است. توجه می‌کنیم که برای $z_1, z_2 \in G_n$ داریم $(z_1 z_2)^n = {z_1}^n {z_2}^n = 1 \cdot 1 = 1$ و در نتیجه G_n نسبت به ضرب اعداد مختلط بسته است. روشن است که عدد $e = 1$ عضو همانی G_n است و به آسانی **می‌توانید نشان دهید** که G_n نسبت به وارون‌ها نیز بسته است. به دلیل روشن، این گروه را **گروه ریشه‌های n-ام واحد** می‌نامیم.

(پ) روشن است که مجموعه‌ی $\mathbb{Q}^+ = \{a \in \mathbb{Q} \mid a > 0\}$ همراه با ضرب معمولی اعداد گویا گروه است. نشان دهید که $\mathbb{Q}^+$ همراه با عمل $*$ با تعریف $a * b = ab/2$ نیز گروه است. عضو همانی آن و وارون هر $a \in \mathbb{Q}^+$ را در این گروه بیابید.

(ت) نشان دهید که هر یک از مجموعه‌های زیر با عمل جمع اعداد مختلط، گروه تشکیل می‌دهد (این نوع گروه‌ها به ویژه در نظریه‌ی اعداد به کار می‌روند):

$$\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$$
$$\mathbb{Q}[i] = \{a + bi \mid a, b \in \mathbb{Q}\}$$

اگر عدد صفر را از $\mathbb{Q}[i]$ برداریم، آنگاه مجموعه‌ی حاصل همراه با ضرب اعداد مختلط گروه تشکیل می‌دهد. وارون هر عضو این گروه را بیابید.

(ث) در بند **(ت)** به جای عدد مختلط $i = \sqrt{-1}$، عددی گنگ، برای مثال، $\sqrt{2}$ یا π را قرار دهید و به همان سؤال پاسخ دهید.

(ج) آیا مجموعه‌ی $G = \{f : \mathbb{R} \to \mathbb{R} \mid (\forall x \in \mathbb{R}) \quad f(x) \neq 0\}$ همراه با ضرب توابع حقیقی، با تعریف $(fg)(x) = f(x)g(x)$، گروه تشکیل می‌دهد؟

(چ) برای هر مجموعه‌ی X، مجموعه‌ی همه‌ی توابع دوسویی روی X (از X به X) با نمادگذاری S_X همراه با ترکیب توابع، گروهی به نام **گروه جایگشت‌ها**، تشکیل می‌دهد. اگر $|X| = n$، گروه S_X را با S_n نشان می‌دهیم و آن را **گروه جایگشت‌های** روی n شیء می‌نامیم. این گروه را، که یکی از اولین مثال‌های گروه بوده است، در بخش **۶.۲** این فصل با جزییات بیش‌تر مطالعه می‌کنیم.

(ح) از مثال‌های مهم دیگر گروه، گروه‌های جمعی همنهشتی $(\mathbb{Z}_n; +_n)$ هستند. همچنین، با استفاده از واقعیت‌های

$$(a, n) = 1 = (b, n) \Rightarrow (ab, n) = 1$$
$$(a, n) = 1 \Rightarrow (\exists x, y \in \mathbb{Z}), \quad ax + ny = 1$$

می‌توانید نشان دهید که در $\{1,2,\cdots,n-1\}$ اعدادی که نسبت به n اول هستند نسبت به ضرب همنهشتی به پیمانه‌ی n گروه تشکیل می‌دهند، که آن را **گروه ضربی همنهشتی** به پیمانه‌ی n می‌نامیم و با C_n نشان می‌دهیم. این گروه‌ها به ویژه در نظریه‌ی اعداد و رمزنگاری کاربرد دارند.

قضیه‌های دیگری نیز معادل با تعریف دستگاه جبری گروه وجود دارند که هر یک سودمندی و کارایی ویژه‌ای دارد. یکی از این قضیه‌ها را در قضیه **۸.۴.۱** در فصل **۱** بدون اثبات آوردیم و کاربرد-هایی از آن را نیز ارائه دادیم. قبل از اثبات این قضیه، قضیه‌ی دیگری معادل با تعریف گروه می-آوریم که اثبات برخی از قضیه‌ها و مثال‌های گروه را اندکی آسان‌تر می‌کند. اثبات آن نیز آموزنده است.

۵.۱.۲ قضیه (تعریف راست). نیمگروه $(G;*)$ گروه است اگر و تنها اگر

(گ۲ر) (وجود عضو همانی راست) $(\exists e_r \in G)\ \ (\forall x \in G)\ \ xe_r = x$

(گ۳ر) (وجود وارون‌های راست) $(\forall x \in G)\ \ (\exists x_r \in G)\ \ xx_r = e_r$

اثبات. روشن است که اگر G گروه باشد، آنگاه نیم‌گروهی با شرایط **(گ۲ر)** و **(گ۳ر)** است. برای اثبات عکس قضیه، ابتدا نشان می‌دهیم که e_r همانی چپ نیز هست. فرض کنیم $x \in G$ دلخواه، $x_r \in G$ وارون راست x، و $x_{r_r} \in G$ وارون راست x_r باشد. در این صورت، داریم

$$\begin{aligned} xx_r = e_r = e_r e_r &= e_r(xx_r) \\ &= (e_r x)x_r \end{aligned}$$

دو طرف تساوی را از سمت راست در x_{r_r} ضرب (عمل گروه) کنید و نتیجه بگیرید که $x = e_r x$. پس $e = e_r$ همانی دوطرفه است.

حال فرض کنیم x_r وارون راست x و x_{r_r} وارون راست x_r باشد. به آسانی می‌توانید مراحل زیر را کامل کنید:

$$x_r x = (x_r x)e = (x_r x)(x_r x_{r_r}) = \cdots = e$$

در نتیجه، G گروه است.

۶.۱.۲ بحث در کلاس. قضیه‌ی بالا را **تعریف راست گروه** نیز می‌نامند. به همین صورت می‌توان **تعریف چپ گروه** را نیز ارائه داد. البته باید توجه داشته باشیم که اگر نیم‌گروه G دارای عضو همانی **راست** و هر عضو آن دارای وارون **چپ** باشد (یا دارای همانی **چپ** و هر عضو آن دارای وارون **راست** باشد) ، لزوماً گروه نیست. برای مثال، مجموعه‌ی $A = \{a,b,c\}$ یک‌بار همراه با عمل دوتایی $xy = x$ (برای مثال a را به عنوان عضو همانی راست در نظر بگیرید) و

بار دیگر با $xy = y$ که، به ترتیب، در جدول‌های زیر مشخص‌تر شده‌اند، ما را به نتیجه‌ی مورد نظر می‌رساند. **چطور؟**

	a	b	c
a	a	a	a
b	b	b	b
c	c	c	c

(الف)

	a	b	c
a	a	b	c
b	a	b	c
c	a	b	c

(ب)

حال قضیه‌ی جالب **۸.۴.۱** را اثبات می‌کنیم. قبلاً نیز گفتیم که اثبات برخی از قضیه‌ها سرراست، یعنی صرفاً بررسی حقایق هستند. ولی، اثبات برخی دیگر، مانند قضیه‌ی زیر، فنونی را به نمایش می‌گذارند که در اثبات‌های دیگر نیز به کار می‌آیند. اثبات‌ها را صرفاً از بر نکنید، بلکه به نکات آن نیز با دقت توجه کنید. وقت زیادی را از شما نمی‌گیرد! سعی کنید روش‌ها و فنون اثبات‌ها را بیاموزید تا لذت ببرید و همچنین

خودتان سازنده‌ی اثبات‌های دیگر باشید و به اصطلاح ماهی‌گیری بیاموزید!

۷.۱.۲ قضیه. *فرض کنیم* $(G;*)$ *نیمگروهی* ***ناتهی*** *باشد. در این صورت،* G *گروه است اگر و تنها اگر به ازای هر* $a,b \in G$*، هر یک از معادله‌های خطی* $ax = b$ *و* $ya = b$ *در* G ***حل‌پذیر*** *باشد.*

اثبات. یک طرف حکم به راحتی اثبات می‌شود. فرض کنیم G گروه است. به راحتی می‌توانید، با استفاده از هر سه ویژگی **(گ۱)** – **(گ۳)** تعریف گروه، با جایگذاری نشان دهید که $x = a^{-1}b$ جواب معادله‌ی اول است (**نشان دهید**). جواب معادله‌ی دوم چیست؟

برعکس، فرض کنیم برای هر $a,b \in G$، معادله‌های $ax = b$ و $ya = b$ در G حل‌پذیر باشند. چون G **ناتهی** است، عضوی چون $a \in G$ وجود دارد (فرض ناتهی بودن در اینجا استفاده شد.) حال، چون معادله‌ی $ax = a$ در G حل‌پذیر است، پس $e_r \in G$ وجود دارد به طوری که $ae_r = a$ (**هشدار:** برخی از دانشجویان به نادرست از همین مطلب نتیجه‌ای زودرس می‌گیرند که e_r عضو همانی راست G است). در حالی که این مطلب هنوز اثبات نمی‌کند که برای **هر عضو دلخواه** $g \in G$، داریم $ge_r = g$! ولی، فرض کنیم $g \in G$ دلخواه باشد. در این صورت، چون معادله‌ی $ya = g$ در G حل‌پذیر است، عضو $g' \in G$ وجود دارد به طوری که $g'a = g$. حال، با توجه به شرکت‌پذیری * و داشته‌هایمان، نتیجه می‌گیریم که

$$ge_r = (g'a)e_r = g'(ae_r) = g'a = g$$

یعنی e_r به واقع همانی راست در G است! تا اینجای اثبات **جالب بود، نبود؟!**

هنوز اثبات تمام نشده است! باید برای هر $g \in G$، وارونی راست در G بیابیم، و سپس از قضیه‌ی **۵.۱.۲** استفاده کنیم! این قسمت ساده‌تر است. از حل‌پذیری $gx = e$ ، عضو $g_r \in G$ به دست می‌آید به طوری‌که $gg_r = e$، یعنی g_r وارون راست g است. حال، قضیه‌ی **۵.۱.۲** را به کار ببرید.

۸.۱.۲ بحث در کلاس. یادآوری بندهایی از بحث **۹.۴.۱** از فصل **۱** مفید است.

۱- به راحتی می‌توانید نشان دهید که در گروه G، جواب هر یک از معادله‌های $ax = b$ و $ya = b$ **یکتا**ست.

۲- فرض کنیم a و b عضو گروه (متناهی) G باشند. در این صورت، وجود و یکتایی جواب معادله‌ی $ax = b$ ایجاب می‌کند که در جدول کیلی گروه G، هر عضو $b \in G$ دقیقاً یک‌بار در سطر مربوط به a ظاهر شود! به همین ترتیب، وجود و یکتایی جواب معادله‌ی $ya = b$ نشان می‌دهد که هر عضو $b \in G$ دقیقاً یک‌بار در ستون مربوط به a ظاهر می‌شود! در انتهای بحث **۹.۴.۱** گفتیم که **اساساً** (یعنی، تا حد یک‌ریختی) تنها یک دسته گروه از هر مرتبه‌ی ۱، ۲، و ۳ عضوی وجود دارد، که $\mathbb{Z}_1 = \{0\}$، $\mathbb{Z}_2 = \{0,1\}$، $\mathbb{Z}_3 = \{0,1,2\}$ با جدول‌های زیر نماینده‌های آن دسته‌ها هستند:

$+_1$	0
0	0

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

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

۳- حال ببینیم در حالت گروه ۴ عضوی چه اتفاق می‌افتد. فرض کنیم $G = \{e, a, b, c\}$. اگر e را به عنوان عضو همانی در نظر بگیریم، ابتدا جدول ناقص زیر را داریم:

	e	a	b	c
e	e	a	b	c
a	a	?	–	–
b	b	–	–	–
c	c	–	–	–

با توجه به مطالب بند ۲ بالا حدس می‌زنید چه عضوهایی باید در محل علامت سؤال بنویسیم؟ درست است، در سطر درونی جدول عضو a آمده است، پس هر یک از سه عضو دیگر G یعنی، e، b، و c را می‌توان انتخاب کرد. از این رو، جدول بالا را می‌توان به هر یک از سه جدول زیر گسترش داد (توضیح دهید که همین سطر و ستون را در این جدول‌ها چطور کامل کردیم):

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	–	–
c	c	b	–	–

(۳)

	e	a	b	c
e	e	a	b	c
a	a	c	e	b
b	b	e	–	–
c	c	b	–	–

(۲)

	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	–	–
c	c	a	–	–

(۱)

روشن است که جدول‌های (۱) و (۲) تنها به یک صورت ولی جدول (۳) به دو صورت (۳) و (۴) زیر کامل می‌شوند. **چطور؟**

(2)

	e	a	b	c
e	e	a	b	c
a	a	c	e	b
b	b	e	c	a
c	c	b	a	e

(1)

	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

(4)

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	a	e
c	c	b	e	a

(3)

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

۴- آیا بند ۳ بالا به این معنی است که اساساً (تا حد یک‌ریختی) چهار نوع گروه چهار عضوی وجود دارند؟ همان طور که در فصل ۱ نیز بیان شد، بررسی شرکت‌پذیری عمل‌هایی که با جدول کیلی داده می‌شوند کار پر زحمتی است. گاهی می‌توانیم با تبدیل جدول کیلی داده شده به جدول عملی که شرکت پذیری آن را می‌دانیم به این مقصود دست یابیم. برای مثال، اگر روش بند ۲ بحث ۱۲.۳.۱ را به کار ببریم به نتایج زیر می‌رسیم. تابع دوسویی تغییر نام h با تعریف

x	e	a	b	c
$h(x)$	$\circ$	1	2	3

جدول (۱) بالا را به جدول گروه $(\mathbb{Z}_4;+_4)$ که در زیر آمده است، تبدیل می‌کند:

$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

این مطلب نه تنها نشان می‌دهد که جدول کیلی (۱) شرکت پذیر است (زیرا جدول عمل همنهشتی به پیمانه‌ی n شرکت‌پذیر است) بلکه نشان می‌دهد که گروه چهار عضوی $\{e,a,b,c\}$ همراه با عملی که با جدول کیلی (۱) داده شده است با گروه همنهشتی $(\mathbb{Z}_4;+_4)$ اساساً یکسان (یعنی **یک‌ریخت**) است. به همین صورت، می‌توانید جدول‌های (۲) و (۴) را نیز به جدول $\mathbb{Z}_4$ تبدیل کنید! در نتیجه، جدول‌های (۱)، (۲)، و (۴) اساساً معرف گروه $\mathbb{Z}_4$ هستند. توجه می‌کنیم که با هیچ یک از ۲۴ = !۴ تابع دوسویی از مجموعه‌ی $\{e,a,b,c\}$ به $\{0,1,2,3\}$ نمی‌توان جدول(۳) را به جدول گروه $\mathbb{Z}_4$ تبدیل کرد. گروه متناظر با جدول (۳) را **چهار-گروه کلاین** (یا **گروه چارینه‌ی کلاین**) می‌نامیم و آن را با V **یا** K_4 نشان می‌دهیم. این گروه در هندسه نیز کاربرد دارد. یک‌بار دیگر جدول آن را مرور کنید زیرا چند بار دیگر به آن رجوع خواهیم داد. مشاهده می‌کنیم که $a^2=b^2=c^2=e^2=e$. همچنین، $ab=c=ba$ ،$bc=a=cb$ ،$ca=b=ac$.

۹.۱.۲ قوانین حذف. قبل از پایان دادن به این بخش، قضیه‌ی معادل دیگری را صرفاً برای تعریف گروه **متناهی** می‌آوریم. به آسانی می‌توانید، با استفاده از وجود وارون، شرکت‌پذیری، و ویژگی عضو همانی، نشان دهید که **قوانین حذف** (چپ و راست) در هر گروه برقرار هستند. یعنی، نشان دهید که شبه‌معادله‌ی (**استلزامی**) زیر در هر گروه برقرار است:

$$ax=ay \quad \vee \quad xa=ya \quad \Rightarrow x=y$$

آیا اگر در نیم‌گروهی ناتهی یا در تکواره‌ی $(M;*,e)$ قوانین حذف برقرار باشند، M باید گروه باشد؟ مثالی بیاورید که پاسخی منفی به این سوال می‌دهد. قضیه‌ی زیر برای نیم‌گروه‌های متناهی بسیار جالب است. روش اثبات فنی و نه چندان سرراست آن را به خاطر بسپارید؛ همتای این روش اثبات را در فصل ۳ نیز خواهیم دید.

۱۰.۱.۲ قضیه. هر نیم‌گروه **متناهی** و ناتهی که قوانین حذف در آن برقرار باشند، لزوماً گروه است.

اثبات. فرض کنیم $G=\{a_1,\cdots,a_n\}$. عضوهای زیر را در نظر بگیرید:

$$a_1a_1, a_2a_1, \cdots, a_na_1 \in G$$

ادعا می‌کنیم که این عضوها متمایز هستند؛ زیرا، بنابر قانون حذف راست در G، داریم

$$a_ia_1 = a_ja_1 \Rightarrow a_i = a_j$$

از این رو، تعداد این عضوها برابر با $|G|=n$ است و بنابراین،

$$G=\{a_1a_1, a_2a_1, \cdots, a_na_1\}$$

چون $a_1 \in G=\{a_1a_1, a_2a_1, \cdots, a_na_1\}$، پس عضو $a_k \in G$ وجود دارد به طوری که $a_1=a_ka_1$. (توجه کنید که این مطلب هنوز نشان نمی‌دهد که a_k همانی چپ G است). حال فرض کنیم $a_i \in G$ دلخواه باشد. در این صورت،

$$a_ia_1 = a_i(a_ka_1) = (a_ia_k)a_1$$

و در نتیجه، بنابر قانون حذف راست، $a_i=a_ia_k$. یعنی، $a_k=e_r$ همانی راست G است.

حال، فرض کنیم $a_i \in G$ عضوی دلخواه باشد. به روشی مشابه بالا و با استفاده از قانون حذف راست، نشان دهید که

$$G=\{a_ia_1, a_ia_2\cdots, a_ia_n\}$$

چون $e_r \in G=\{a_ia_1, a_ia_2\cdots, a_ia_n\}$، عضوی مانند $a_j \in G$ وجود دارد به طوری که $e_r=a_ia_j$. یعنی، a_i وارون راست دارد. از این رو، بنابر قضیه‌ی **۵.۱.۲**، G گروه است. **جالب بود؟**

۱۱.۱.۲ بحث در کلاس. اگر چه تعریف‌های معادل **۱.۱.۲**، **۵.۱.۲**، **۷.۱.۲** برای گروه برحسب برقراری معادله‌ها یعنی اتحادها داده نشده است، و تعریف مذکور در قضیه‌ی **۱۰.۱.۲** برای گروه متناهی برحسب شبه‌اتحاد (گزاره‌ی استلزامی) داده شده است، تعریف جالب **۳.۱.۲** کاملاً بر حسب **اتحادها** است. این مطلب نشان می‌دهد که کلاس گروه‌ها، با توجه به مطالب بخش **۹.۱**، دارای همه‌ی مزایای کلاس‌های معادله‌ای است.

تمرین ۱.۲

هوشم نه چنان است تلاشم آنچنان است

دسته‌ی اول

۱- با استقرا، اثبات کنید که برای هر $m,n\in\mathbb{Z}$، اتحادهای $x^m x^n = x^{m+n}$ $(x^m)^n = x^{mn}$ در هر گروه برقرار هستند.

۲- نشان دهید که عضو همانی گروه $(\mathbb{Q}^+;*)$ که در آن $a*b = ab/2$ عدد گویای ۲، و وارون هر $a\in\mathbb{Q}^+$ برابر با $4/a$ است.

۳- وارون $a+bi\neq 0$ را در گروه ضربی $\mathbb{Q}^*[i]=\mathbb{Q}[i]\setminus\{0\}$ به‌دست آورید؟

۴- نشان دهید که جدول‌های زیر نمی‌توانند جدول کیلی عمل یک گروه روی مجموعه‌ی داده شده باشند:

	a	b
a	a	a
b	a	a

	a	b
a	a	b
b	b	b

	a	b	c
a	a	b	c
b	b	b	c
c	c	b	c

۵- جدول کیلی گروه ضربی $(C_7;\cdot_7)$ را بنویسید.

۶- بزرگ‌ترین زیرمجموعه‌ای از $\mathbb{Z}_8$ را بیابید که همراه با ضرب همنهشتی $\cdot_8$ گروه تشکیل دهد. جدول کیلی عمل آن را بنویسید.

۷- **(الف)** چطور با نگاهی به جدول‌های کیلی گروه‌های $\mathbb{Z}_4$ و K_4، متوجه می‌شویم که هر دو آبلی هستند؟

(ب) همچنین، نشان دهید که معادله‌ی **درجه‌ی دوم** $x^2=e$ در K_4 دارای **چهار** جواب است در حالی که $\mathbb{Z}_4$ دارای این ویژگی نیست. (تفاوت جبری دیگر این دو گروه را بعداً خواهیم دید.)

۸- **(الف)** نشان دهید که برای هر x و هر y در گروه G، داریم

$$xy = yx \Leftrightarrow (xy)^2 = x^2y^2$$

(**هشدار** می‌دهیم که مبتدیان گاهی به اشتباه اتحاد $(xy)^2 = x^2y^2$ را در هر گروه، آبلی یا غیر آبلی، به کار می‌برند. شاید به این دلیل باشد که هنوز با گروه‌های ناآبلی سروکار نداشته‌اند).

(ب) نشان دهید که برای هر x و هر y در گروه G، داریم

$$xy = yx \Leftrightarrow (xy)^{-1} = x^{-1}y^{-1}$$

۹- نشان دهید که مجموعه‌ی $G = \mathbb{R} \times \mathbb{R}$ همراه با عمل مولفه‌ای زیر، گروه است:

$$(a,b) * (c,d) = (a+c, b+d)$$

۱۰- (یک تعمیم تمرین بالا) نشان دهید که $G \times G$ همراه با عمل زیر، گروه است:

$$(a,b) *' (c,d) = (a * c, b * d)$$

۱۱- تمرین **۱۰** را به دو گروه دلخواه $(G_1; *_1)$ و $(G_2; *_2)$ تعمیم دهید. یعنی، نشان دهید که $G = G_1 \times G_2$ همراه با عمل دوتایی زیر، گروه است:

$$(a,b) * (c,d) = (a *_1 c, b *_2 d)$$

۱۲- با استفاده از قوانین حذف، نشان دهید که تنها عضو خودتوان (یعنی عضوی چون x که $x^2 = xx = x$) در هر گروه، عضو همانی آن است.

دسته‌ی دوم

۱۳- (الف) نشان دهید که اگر هر عضو گروه G وارون خودش باشد، یعنی،

$$(\forall x \in G) \quad x^2 = e$$

آنگاه G آبلی است ($(ab)^2$ را محاسبه کنید) . آیا عکس این مطلب درست است؟

(ب) فرض کنید که دو عدد طبیعی متباین m و n وجود دارند به طوری که برای هر a و b در گروه G داریم

$$a^m b^m = b^m a^m \quad , \quad a^n b^n = b^n a^n$$

نشان دهید که G آبلی است.

(پ) فرض کنید که در گروه G، برای سه عدد متوالی k داریم

$$(\forall a,b \in G) \quad (ab)^k = a^k b^k$$

ثابت کنید که گروه G آبلی است.

۱۴- فرض کنید G گروه است. نشان دهید که هر یک از **انتقال**های راست و چپ

$$r_a : G \to G \qquad l_a : G \to G$$
$$x \mapsto xa \qquad x \mapsto ax$$

دوسویی هستند.

۱۵- (بعداً این تمرین را به کار خواهیم برد) فرض کنید G گروه است. نشان دهید که هر دو مجموعه‌ی زیر همراه با ترکیب توابع گروه تشکیل می‌دهند:

$$G_r = \{r_a \mid a \in G\} \quad , \quad G_l = \{l_a \mid a \in G\}$$

۱۶- جدول‌های کیلی گروه‌های G_r و G_l را برای گروه $G = \mathbb{Z}_4$ بنویسید و آن‌ها را با جدول گروه $\mathbb{Z}_4$ مقایسه کنید.

۱۷- نشان دهید که هر نیم‌گروه ناتهی **متناهی** دارای عضوی خودتوان است.

۱۸- فرض کنید که G تکواره‌ای **متناهی** است. نشان دهید که G گروه است اگر و تنها اگر دارای یک عضو خودتوان منحصر به فرد باشد.

۱۹- ثابت کنید که مجموعه‌ی $G = \mathbb{R} \times \mathbb{R}^* = \{(a,b) \mid a,b \in \mathbb{R}, a \neq 0\}$ همراه با عمل $(a,b)*(c,d) = (ac, bc+d)$ گروهی ناآبلی است.

۲۰- فرض کنید G گروهی با عضو همانی e باشد که در آن برای هر عدد صحیح n و هر $a,b \in G$، $(ab)^n = a^n b^n$. ثابت کنید که برای هر $a,b \in G$،

$$(aba^{-1}b^{-1})^{n(n-1)} = e$$

۲.۲ زیرگروه

در بخش **۶.۱** مفهوم کلی زیردستگاه جبری و P - زیرجبر را معرفی کردیم. در این بخش، این مفاهیم را برای گروه‌ها با جزییات بیشتری مورد بررسی قرار می‌دهیم. تعریف **۳.۶.۱** را یادآوری می‌کنیم، که بیان می‌کند دستگاه جبری B زیردستگاه جبری A، هر دو از نوع τ (بدون در نظر

گرفتن ویژگی‌های آن‌ها)، است اگر $B \subseteq A$ و هر عمل B تحدید عمل همتایش در A باشد. حال تعریف زیر را می‌آوریم.

۱.۲.۲ تعریف. می‌گوییم که گروهواره‌ی $(B;*^B)$ زیرگروهواره‌ای از گروهواره‌ی $(A;*^A)$ است اگر دو شرط زیر برقرار باشند:

۱- $B \subseteq A$، و

۲- عمل دوتایی $*^B$ تحدید عمل دوتایی $*^A$ باشد. یعنی،

$$(\forall x, y \in B) \quad x *^B y = x *^A y$$

۲.۲.۲ بحث در کلاس

۱- اگر چه نباید مجموعه را با دستگاه جبری مقایسه کرد، ولی غلطی متداول (و بی ضرر) است که اغلب می‌گوییم که"زیر**مجموعه**ی B از گروهواره‌ی $(A;*)$ زیرگروهواره‌ی $(A;*)$ است اگر B نسبت به عمل $*$ بسته باشد". منظور این است که اگر مجموعه‌ی B نسبت به عمل $*$ بسته باشد، آنگاه B همراه با تحدید تابع $*$ بر آن، گروهواره‌ای تشکیل می‌دهد که آن را زیرگروهواره‌ی A می‌نامیم!

همچنین، وقتی گروهواره‌ی $(B;*^B)$ زیرگروهواره‌ی $(A;*^A)$ است، متداول است که هر دو عمل را با نماد ساده‌ی $*$ نشان دهیم، و البته بنابر قرارداد قبلی، اگر امکان اشتباه نباشد، به جای $x * y$ به طور ساده می‌نویسیم xy.

۲- آیا گروهواره‌ی $H = (\{0,1,2\}, +_3)$ زیرگروهواره‌ی $\mathbb{Z}_4 = (\{0,1,2,3\}, +_4)$ است؟ برای پاسخ **منفی** خود دلیل بیاورید!

۳- آیا گروهواره‌ی $H = (\{0,2\}; +_4)$ زیرگروهواره‌ی $\mathbb{Z}_4 = (\{0,1,2,3\}, +_4)$ است؟ برای پاسخ **مثبت** خود دلیل بیاورید!

۴- یادآوری می‌کنیم که دستگاه جبری گروهواره لزوماً دارای هیچ ویژگی‌ای بجز وجود عمل دوتایی‌اش نیست. ولی، دستگاه جبری مورد نظر ما در این فصل، یعنی **گروه**، با سه ویژگی شرکت-پذیری، وجود عضو همانی، و وجود وارون‌ها مشخص می‌شود. پس باید تعریف **۶.۶.۱**، یعنی P-زیرجبر، را برای مفهوم زیرگروه تعبیر کنیم. پیشنهاد می‌کنیم که بحث‌های **۷.۶.۱** و **۸.۶.۱** را مرور کنید.

۳.۲.۲ تعریف. فرض کنیم گروهواره‌ی $(G;*_G)$ گروه باشد (یعنی در شرط‌های **(گ۱)**، **(گ۲)**، و **(گ۳)** تعریف **۱.۱.۲** صدق کند.) می‌گوییم که گروهواره‌ی $(H;*_H)$ **زیرگروه** $(G;*_G)$ است، و می‌نویسیم $H \leq G$، اگر شرایط زیر برقرار باشند:

۱- H زیرگروهواره‌ی G باشد. یعنی، $H \subseteq G$ و $*_H$ تحدید عمل $*_G$ باشد.

۲- این زیرگروهواره، خودش گروه باشد. یعنی، H همراه با عمل $*_H$ (که تحدید $*_G$ بر H است) دارای شرط‌های **(گ۱)** - **(گ۳)** تعریف **۱.۱.۲** باشد.

۴.۲.۲ بحث در کلاس. نکته‌هایی در این تعریف پنهان است که مبتدیان ممکن است به آن توجه نکنند. بیان این موارد برای مطالعه‌ی دستگاه‌های جبری دیگر نیز مفید است. می‌دانیم که بنابر شرط **(گ۲)**، گروه G دارای عضو همانی، به نمایش e_G، است و همچنین، بنابر **(گ۳)**، هر عضو $x \in G$ وارونی، مثلاً به نمایش x_G^{-1}، در G دارد. و شرط **۲** بالا بیان می‌کند که H نیز دارای شرایط **(گ۲)** و **(گ۳)** است و در نتیجه باید **برای خودش** دارای عضو همانی، به نمایش e_H، باشد و هر عضو $h \in H$ وارونی، مثلاً به نمایش h_H^{-1}، در H داشته باشد! حال حتماً این سؤال‌ها برایتان مطرح می‌شود که **(الف)** آیا به خودی خود $e_H = e_G$ و $h_H^{-1} = h_G^{-1}$، یا باید این شرایط را نیز در تعریف زیرگروه می‌گنجاندیم؟ اگر چه پاسخ‌های به این سؤال‌ها در همه‌ی دستگاه‌های جبری لزوماً مثبت نیستند (برای مثال، بند **۱** بحث **۸.۶.۱** را در مورد تکواره ببینید)، ولی در قضیه‌ی **۵.۲.۲** خواهیم دید که تلفیق شرط‌های **(گ۱)**- **(گ۳)** گروه بسیار توانمند است و خوشبختانه پاسخ به هر دو سؤال برای **گروه‌ها** مثبت است.

۵.۲.۲ قضیه. فرض کنیم گروهواره‌ی $(H;*_H)$ زیرگروهی از گروه $(G;*_G)$ باشد. در این صورت،

(الف) $e_H = e_G$؛

(ب) برای هر $h \in H$، $h_H^{-1} = h_G^{-1}$.

اثبات (الف). در گروه H داریم $e_H e_H = e_H$. از طرفی، در گروه G داریم $e_H e_H = e_H = e_H e_G$. حال، قانون حذف چپ **(۹.۱.۲)** را در گروه G به کار ببرید و نتیجه بگیرید که $e_H = e_G$.

(ب) چون $xx_H^{-1} = x_H^{-1}x = e_H = e_G$، پس x_H^{-1} وارون x در G است. به دلیل یکتایی وارون در گروه‌ها، $x_H^{-1} = x_G^{-1}$.

اثبات قضیه‌ی زیر نیز راحت است.

۶.۲.۲ قضیه (محک زیرگروه). فرض کنیم G گروه و H زیرمجموعه‌ی G باشد به طوری که:

(الف) H نسبت به عمل گروه G بسته باشد؛

(ب) $e \in H$؛

(پ) برای هر $h \in H$، $h^{-1} \in H$.

در این صورت، H همراه با (تحدید) عمل G بر آن (حاصل از بند (**الف**)) زیرگروهی از G تشکیل می‌دهد.

قضیه‌ی زیر کار بررسی زیرگروه بودن را اندکی (فقط اندکی) کوتاه‌تر از محک بالا می‌کند.

۷.۲.۲ قضیه. زیرمجموعه‌ی **ناتهی** H از گروه G (همراه با تحدید عمل G بر آن) زیرگروه G است اگر و تنها اگر برای هر $x, y \in H$، $xy^{-1} \in H$. (و در نمادگذاری جمعی، $x - y = x + (-y) \in H$)

اثبات. یک طرف حکم به راحتی اثبات می‌شود. فرض کنیم H زیرگروه G باشد. برای هر $x, y \in H$، چون $y^{-1} \in H$ و H نسبت به عمل گروه G بسته است، پس $xy^{-1} \in H$.

برای اثبات عکس حکم قضیه، فرض می‌کنیم $a, b \in H$ دلخواه باشند. کافی است $x = a$ و $y = b^{-1}$ را در $xy^{-1} \in H$ قرار دهیم و نتیجه بگیریم که $a(b^{-1})^{-1} = ab \in H$. برای اثبات $e \in H$، فرض کنید $h \in H \neq \varnothing$ و در $xy^{-1} \in H$ قرار دهید $x = y = h$، و سرانجام، با قرار دادن $x = e$ و $y = h$ در $xy^{-1} \in H$ نتیجه بگیرید که $h^{-1} \in H$.

بسیاری مواقع لازم است که زیرگروه بودن زیرمجموعه‌ی **متناهی** H از گروه G را بررسی کنیم. در این موارد قضیه‌ی ساده‌تر و جالب زیر بسیار مفید است. برای اثبات آن، قضیه‌ی **۱۰.۱.۲** را به کار ببرید.

۸.۲.۲ قضیه. فرض کنیم H زیرمجموعه‌ای **متناهی** و ناتهی از گروه G باشد. در این صورت، H (همراه با تحدید عمل G بر آن) زیرگروه G است اگر و تنها اگر H نسبت به عمل دوتایی G بسته (یعنی، صرفاً زیرگروهواره) باشد.

۹.۲.۲ بحث در کلاس. چندان ساده نیست که همه‌ی زیرگروه‌های یک گروه را بیابیم. به مرور مطالب مفیدی را با استفاده از قضیه‌های بالا در این رابطه می‌آوریم که این کار را ساده‌تر می‌کند.

۱- روشن است که اگر e عضو همانی گروه G باشد، آنگاه $\{e\}$ و G زیرگروه G هستند. این زیرگروه‌ها را **زیرگروه‌های بدیهی** می‌نامیم. البته، شاید بهتر باشد $\{e\}$ را زیرگروه بدیهی و G را زیرگروه ناسره بنامیم.

۲- اگر $\mathbb{Z}_2 = (\{0,1\};+_2)$ آنگاه $\{0\}$ و $\mathbb{Z}_2$ تنها زیرگروه‌های $\mathbb{Z}_2$ هستند.

۳- اگر $\mathbb{Z}_3 = (\{0,1,2\};+_3)$ آنگاه در این مورد نیز $\{0\}$ و $\mathbb{Z}_3$ تنها زیرگروه‌های $\mathbb{Z}_3$ هستند! زیرا هر زیرگروه H از G باید شامل عضو همانی (خنثی) 0 باشد. حال اگر $1 \in H$ آنگاه، بنابر قضیه‌ی ۸.۲.۲، H باید شامل $1+_3 1 = 2$ نیز باشد، که در این صورت $H = G$. اگر $2 \in H$، آنگاه $2 +_3 2 = 1 \in H$.

۴- آیا گروه $\mathbb{Z}_4 = (\{0,1,2,3\};+_4)$ زیرگروهی چون H متفاوت با $\{0\}$ و $\mathbb{Z}_4$ دارد؟ مشابه بند۳، فرض می‌کنیم $1 \in H$. در این صورت، $1+_4 1 = 2, 1+_4 2 = 3 \in H$ و در نتیجه $H = G$. هنوز کار تمام نشده است! فرض کنیم $0,2 \in H$. چون $2+_4 2 = 0$، پس $H = \{0,2\}$ نسبت به عمل $+_4$ بسته است. حال، بنابر قضیه‌ی ۸.۲.۲، $H = \{0,2\}$ زیرگروه $\mathbb{Z}_4$ است. به همین روش‌ها نشان دهید که $\mathbb{Z}_4$ زیرگروه دیگری بجز $\{0\}$، $H = \{0,2\}$ و $\mathbb{Z}_4$ ندارد.

۵- حال گروه کلاین K_4 را با جدول عمل

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

در نظر بگیرید. آیا علاوه بر $\{e\}$ و K_4، زیرگروه دیگری وجود دارد؟ با توجه به قضیه‌ی ۸.۲.۲، $\{e,a\}$، $\{e,b\}$، و $\{e,c\}$ نیز زیرگروه هستند و هیچ زیرگروه دیگری وجود ندارد. زیرا، برای مثال $\{e,a,b\}$ نسبت به عمل K_4 بسته نیست.

۶- حال ببینیم آیا با اطلاعاتی که تاکنون داریم می‌توانیم زیرگروه‌های گروه نامتناهی $(\mathbb{Z};+)$ را تعیین کنیم؟ این گروه هیچ زیرگروه **متناهی** بجز $\{0\}$ ندارد! زیرا اگر H زیرگروه آن باشد و $0 \neq n \in H$ آنگاه، چون H باید نسبت به جمع بسته باشد، پس برای هر k، باید $kn = n+n+\cdots+n \in H$. این مطلب نشان می‌دهد که H نامتناهی است. به آسانی می-

توانید با بررسی شرایط قضیه‌ی ۶.۲.۲ نشان دهید که برای هر عدد صحیح n، مجموعه‌ی مضارب صحیح n، یعنی

$$n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\} = \{\cdots, -2n, -n, \circ, n, 2n, \cdots\}$$

زیرگروه $(\mathbb{Z}; +)$ است. توجه می‌کنیم که، $0\mathbb{Z} = \{0\}$، $1\mathbb{Z} = \mathbb{Z}$، و $-n\mathbb{Z} = n\mathbb{Z}$. خواهیم دید که $\mathbb{Z}$ زیرگروه دیگری ندارد! البته، اثبات این مطلب قدری فنی است که بعداً (در نتیجه ۱۳.۴.۲) ارائه خواهیم کرد.

۱۰.۲.۲ قضیه‌ی لاگرانژ. قضیه‌ای بسیار مهم، به نام قضیه‌ی لاگرانژ، بیان می‌کند که اگر H زیرگروهی از یک گروه **متناهی** G باشد، آنگاه مرتبه‌ی H، یعنی $|H|$، باید مرتبه‌ی G، یعنی $|G|$، را بشمارد. برای مثال، $\mathbb{Z}_4$ و K_4 زیرگروهی با ۳ عضو نمی‌توانند داشته باشند، $\mathbb{Z}_{15}$ تنها **ممکن** است زیرگروه‌هایی ۱، ۳، ۵، و ۱۵ عضوی داشته باشد! اثبات این **قضیه‌ی مهم**، بسیار راحت ولی فنی و جالب است، و ابزار لازم برای اثبات آن کاربردهای دیگری نیز در بخش ۸.۲، مربوط به خارج قسمت گروه‌ها، دارد. حال روش کار را با هم می‌بینیم. رابطه‌ای هم‌ارزی روی مجموعه‌ی G تعریف می‌کنیم به طوری که افراز حاصل از آن نه تنها قضیه‌ی لاگرانژ را اثبات می‌کند، بلکه در بخش مهم ۸.۲ نیز به کار می‌رود. فرض کنیم H زیرگروه G باشد.

۱- به آسانی می‌توانید نشان دهید که رابطه‌ی $\sim_H$ با تعریف

$$a \sim_H b \iff (\exists h \in H)\, a = bh \iff b^{-1}a \in H$$

رابطه‌ای هم‌ارزی است. برای مثال، مراحل زیر را برای اثبات متعدی بودن $\sim_H$ توضیح دهید:

$$a \sim_H b \sim_H c \Rightarrow (\exists h_1, h_2 \in H)\ \ a = bh_1 \,\&\, b = ch_2$$
$$\Rightarrow a = bh_1 = ch_2h_1 \Rightarrow a \sim_H c$$

۲- رده‌های این رابطه‌ی هم‌ارزی ویژگی‌های **بسیار بسیار** جالب توجهی به صورت زیر دارند، که برای دستگاه‌های جبری دیگر (برای مثال، نیم‌گروه و تکواره) لزوماً درست نیستند.

(الف) ابتدا توجه می‌کنیم که، به اصطلاح، H سازنده‌ی همه‌ی رده‌هاست. به این معنی که

$$\begin{aligned}[a] &= \{x \in G \mid x \sim_H a\} \\ &= \{x \in G \mid (\exists h \in H)\ \ x = ah\} \\ &= \{ah \mid h \in H\} \\ &= aH\end{aligned}$$

نمایش $\{ah \mid h \in H\}$ با نماد aH طبیعی است، **این طور نیست؟** توجه می‌کنیم که زیرگروه H از گروه G نیز یکی از رده‌ها است، زیرا $[e] = eH = H$، و البته هیچ رده‌ی دیگری زیرگروه نیست. **چرا؟**

(ب) از آنجا که، مانند هر رابطه‌ی هم‌ارزی، $[a] = [b]$ اگر و تنها اگر $a \sim_H b$، به روشنی داریم

$$aH = bH \Leftrightarrow a \sim_H b \Leftrightarrow (\exists h \in H)\, a = bh \Leftrightarrow b^{-1}a \in H$$

(پ) هر مجموعه‌ی $aH = \{ah \mid h \in H\}$ (یا در نمادگذاری جمعی $a + H = \{a + h \mid h \in H\}$) را، که انتقال چپ اعضای H به اندازه‌ی a است، یک **هم‌مجموعه (یا هم‌رده)ی چپ** H می‌گوییم. بنابراین، افراز $G / \sim_H$، که **برای سادگی** آن را با L_H نشان می‌دهیم، عبارت است از $L_H = \{aH \mid a \in G\}$.

(ت) ویژگی بسیار مهم هم‌مجموعه‌های چپ این است که (چه متناهی باشند یا نامتناهی) تعداد عضوهای یکسان دارند. در واقع، برای هر $a \in G$، $|aH| = |H|$. زیرا، به آسانی **می‌توانید** نشان دهید که تابع زیر دوسویی (یک به یک و پوشا) است:

$$\begin{aligned} f : H &\to aH \\ h &\mapsto ah \end{aligned}$$

حال آماده‌ایم که قضیه‌ی لاگرانژ را به راحتی اثبات کنیم.

۱۱.۲.۲ قضیه(ی لاگرانژ). فرض کنیم H زیرگروهی از گروه متناهی G باشد. در این صورت، مرتبه‌ی H مرتبه‌ی G را می‌شمارد، یعنی $|G| = k\,|H|$.

اثبات. دیدیم که مجموعه‌ی $L_H = \{aH \mid a \in G\}$ مجموعه‌ی G را افراز می‌کند. از این رو، اجتماع مجزای $G = \bigcup_{a \in G} aH$ را داریم. بنابراین، چون گروه G **متناهی** است، و در نتیجه L_H مجموعه‌ای متناهی، برای مثال k عضوی است. فرض می‌کنیم $L_H = \{a_1H, \cdots, a_kH\}$. پس

$$\begin{aligned} |G| &= |a_1H| + \cdots + |a_kH| = |H| + \cdots + |H| \\ &= k\,|H| \end{aligned}$$

بنابراین قضیه‌ی مهم لاگرانژ به صورتی جالب اثبات شد.

۱۲.۲.۲ بحث در کلاس

۱- به آسانی می‌توانید نشان دهید که رابطه‌ی $\sim_H$ با تعریف

$$a \sim_H b \quad \Leftrightarrow \quad (\exists h \in H)\, a = hb \quad \Leftrightarrow \quad ab^{-1} \in H$$

نیز رابطه‌ای هم‌ارزی است و $[a] = Ha$، $[e] = He = H$، $|Ha| = |H|$، و

$$Ha = Hb \Leftrightarrow a \sim_H b \Leftrightarrow (\exists h \in H) \quad a = hb \Leftrightarrow ab^{-1} \in H$$

۲- هر Ha را یک **هم‌مجموعه‌ی راست** H در G می‌نامیم. اگر $R_H = \{Hb \mid b \in G\}$ آنگاه، به راحتی می‌توان نشان داد که تابع زیر دوسویی است :

$$f : L_H \to R_H$$
$$aH \mapsto Ha^{-1}$$

خوش‌تعریفی و یک به یک بودن f به صورت زیر اثبات می‌شود (مراحل آن را توضیح دهید):

$$\begin{aligned} aH = bH &\Leftrightarrow b^{-1}a \in H \Leftrightarrow (b^{-1}a)^{-1} \in H \\ &\Leftrightarrow a^{-1}b \in H \Leftrightarrow (a^{-1})(b^{-1})^{-1} \in H \\ &\Leftrightarrow Ha^{-1} = Hb^{-1} \end{aligned}$$

پوشا بودن f روشن است (این طور نیست؟) در نتیجه، $|L_H| = |R_H|$.

۳- توجه می‌کنیم که تساوی‌های $|aH| = |H| = |Ha|$ و $|L_H| = |R_H|$ به متناهی یا نامتناهی بودن این عددها بستگی ندارند. عدد $|L_H| = |R_H|$ را، چه متناهی باشد یا نامتناهی، **اندیس** H در G می‌نامیم و آن را با نماد $[G:H]$ یا $(G:H)$ نشان می‌دهیم. البته، با توجه به اثبات قضیه‌ی لاگرانژ، برای گروه‌های متناهی داریم $[G:H] = |G| / |H|$.

۱۳.۲.۲ قضیه. فرض کنیم G گروهی دلخواه (متناهی یا نامتناهی) باشد و $H, K \leq G$ به طوری که $H \subseteq K$. در این صورت، اگر $[G:K]$ و $[K:H]$ متناهی باشند آنگاه

$$[G:H] = [G:K][K:H]$$

اثبات فرض کنیم $L_1 = \{a_1K, \cdots, a_mK\}$ و $L_2 = \{b_1H, \cdots, b_nH\}$ به ترتیب مجموعه‌ی هم‌مجموعه‌های (چپ) متمایز K در G و H در K باشند. حال کافی است نشان دهیم که $L_3 = \{a_ib_jH \mid i = 1, \cdots, m,\ j = 1, \cdots, n\}$ مجموعه‌ی هم‌مجموعه‌های (چپ)

متمایز H در G اسـت(چـرا؟؟؟؟؟؟؟؟ //؟؟؟) ، و در نتیجـه $|L_3| = mn = |L_1||L_2|$.
ابتدا توجه کنید که در L_3 داریم

$$\begin{aligned} a_r b_s H = a_p b_q H &\Rightarrow (a_p b_q)^{-1}(a_r b_s) \in H \subseteq K \\ &\Rightarrow (a_p b_q)^{-1}(a_r b_s) \in K \\ &\Rightarrow a_r b_s K = a_p b_q K \\ &\Rightarrow a_r K = a_p K \\ &\Rightarrow a_r = a_p \\ &\Rightarrow b_s H = b_q H \\ &\Rightarrow b_s = b_q \\ &\Rightarrow a_r b_s = a_p b_q \end{aligned}$$

(مراحل اثبات بالا را توضیح دهید) بنابراین، اعضای L_3 متمایز هستند. حال نشان مـی‌دهـیم کـه L_3 در واقع برابر با مجموعه‌ی همه‌ی هم‌مجموعه‌های چپ H در G است. کـافی اسـت نشـان دهیم که بـرای هـر $x \in G$، $xH \in L_3$. چـون $xK \in L_1$، پـس $xK = a_r K$ و در نتیجـه $x = a_r k$ گه در آن $k \in K$. حال از $kH = b_s H \in L_2$ نتیجه مـی گیـریم کـه $k = b_s h$ که در آن $h \in H$. بنابراین،

$$xH = a_r kH = a_r b_s hH = a_r b_s H \in L_3$$

در پایان، $[G:H] = [G:K][K:H] = mn$.

تمرین ۲.۲

به توانایی‌های خود کم اهمیت ندهید

دسته‌ی اول

۱– در هر مورد زیر، با دلیل تعیین کنید که آیا H زیرگروه G هست یا نیست.

(الف) $G = (\mathbb{Z}; +)$ و $H = \mathbb{Z}^+ = \{n \in \mathbb{Z} \mid n \geq 0\}$.

(ب) $G=(\mathbb{Z}_8;+_8)$ و $H=\{\circ,2,4\}$.

(پ) $G=(\mathbb{R};+)$ و $H=\pi\mathbb{Q}=\{\pi x \mid x\in\mathbb{Q}\}$.

(ت) $G=(\mathbb{R};+)$ و $H=\pi\mathbb{Z}=\{\pi n \mid n\in\mathbb{Z}\}$.

(ث) $G=GL(n,\mathbb{R})$ و $H=SL(n,\mathbb{R})$ (**گروه خطی خاص** متشکل از ماتریس‌های حقیقی $n\times n$ با دترمینان ۱).

(ج) گروه (ضربی) G دلخواه و برای $a\in G$، $H=\{a^n \mid n\in\mathbb{Z}\}$.

۲- فرض کنید گروه (ضربی) G آبلی است و $n\in\mathbb{N}$. نشان دهید که مجموعه‌ی جواب‌های معادله‌ی $x^n=e$ در G، یعنی $H=\{x\in G \mid x^n=e\}$ یک زیرگروه G است.

۳- فرض کنید G گروه است.

(الف) نشان دهید که برای هر $a\in G$، مجموعه‌ی همه‌ی عضوهای G که با a تعویض پذیر باشند، یعنی $C_G(a)=\{x\in G \mid ax=xa\}$، زیرگروه G است.

(ب) (تعمیم **(الف)**) فرض کنید $S\subseteq G$. نشان دهید که مجموعه‌ی همه‌ی عضوهای G که با همه‌ی عضوهای S تعویض‌پذیر هستند، یعنی

$$C_G(S)=\{x\in G \mid (\forall s\in S)\quad xs=sx\}$$

زیرگروه G است. این زیرگروه را **مرکزساز** S در G می‌نامیم. اگر $S=\{a_1,\cdots,a_n\}$، می‌نویسیم $C_G(S)=C_G(a_1,\cdots,a_n)$.

(پ) (حالت خاص **(ب)**) نشان دهید که **مرکز گروه** G، یعنی

$$Z(G)=C_G(G)=\{x\in G \mid (\forall g\in G)\quad xg=gx\}$$

زیرگروه G است.

(ت) نشان دهید که $Z(G)=\bigcap_{a\in G} C_G(a)$.

(ث) ثابت کنید که G آبلی است اگر و تنها اگر $Z(G)=G$.

(ج) نشان دهید که مرکز گروه $GL(2,\mathbb{R})$ برابر است با

$$\left\{ \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix} \mid a \in \mathbb{R},\ \ a \neq 0 \right\}$$

(توجه کنید که هر عضو مرکز باید دست کم با $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ و $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ تعویض‌پذیر باشد.)

۴ـ فرض کنید H و K زیرگروه G باشند. مجموعه‌ی به نمایش طبیعی

$$HK = \{hk \mid h \in H, k \in K\}$$

را در نظر بگیرید.

(الف) نشان دهید که اگر هر عضو H با هر عضو K تعویض‌پذیر باشد، یعنی

$$(\forall h \in H)(\forall k \in K)\quad hk = kh$$

آنگاه $T = HK$ زیرگروه G است.

(ب) نشان دهید که $T = HK$ زیرگروه G است اگر و تنها اگر $HK = KH$. (به تفاوت بین $HK = KH$ و شرط قوی‌تر بند **(الف)** توجه کنید).

دسته‌ی دوم

۵- فرض کنید که G گروه و H زیرگروه آن باشد. برای هر $a \in G$، تعریف می‌کنیم

$$aHa^{-1} = \{aha^{-1} \mid h \in H\}$$

(الف) نشان دهید که aHa^{-1} زیرگروه G است. عضو aha^{-1} را **مزدوج** h تحت a، و aHa^{-1} را **مزدوج** H تحت a می‌نامیم. گاهی aha^{-1} را با h^a و aHa^{-1} را با H^a نیز نشان می‌دهند.

(ب) نشان دهید که $|H| = |aHa^{-1}|$.

(پ) نشان دهید که $N_G(H) = \{a \in G \mid aHa^{-1} = H\}$ زیرگروه G است. این زیرگروه را **نرمال‌ساز** H در G می‌نامیم. اگر $N_G(H) = G$، یعنی

$$(\forall a \in G)\quad aHa^{-1} = H$$

آنگاه می‌گوییم که H **خودمزدوج** است. در بخش **۸.۲** خواهیم دید که این زیرگروه‌ها بسیار با اهمیت هستند.

۶- مثالی از گروه G با زیرگروه نا بدیهی H ارائه دهید که $[G:H]$ نامتناهی باشد.

۷- فرض کنید G یک گروه و $H,K \leq G$. نشان دهید که $H \cap K$ زیرگروه G است.

۸- فرض کنید G یک گروه و زیرگروه‌های $H,K \leq G$ متناهی باشند. نشان دهید که اگر $(|H|,|K|)=1$ آنگاه $H \cap K = \{e\}$.

۹- فرض کنید H و K زیرگروه‌هایی از گروه متناهی G باشند به طوری که $|H|=p$ عددی اول باشد و $H \cap K \neq \{e\}$. ثابت کنید که $H \subseteq K$.

۱۰- فرض کنید که H و K زیرگروه‌هایی متمایز از گروه G باشند به طوری که $|H|=|K|=p$ عددی اول است. ثابت کنید که $|H \cup K| = 2p-1$.

۱۱- فرض کنید که H و K زیرگروه‌هایی از گروه G باشند به طوری که اندیس آن‌ها در G متناهی است. نشان دهید که.

(الف) اندیس $H \cap K$ در G متناهی است و

$$[G:H \cap K] \leq [G:H][G:K]$$

(ب) اندیس $H \cap K$ در K متناهی است و $[K:H \cap K] \leq [G:H]$.

(پ) تساوی در **(ب)** برقرار است اگر و تنها اگر $G=HK$.

(ت) اگر اندیس‌های H و K در G متناهی و متباین باشند، آنگاه $G=HK$ و

$$[G:H \cap K] = [G:H][G:K]$$

۱۲- فرض کنید که H و K زیرگروه‌هایی متناهی از گروه دلخواه G باشند. ثابت کنید که

$$|HK| = \frac{|H||K|}{|H \cap K|}$$

۱۳- فرض کنید G گروهی از مرتبه ی ۲۰ و $H,K \leq G$، با $|H|=4$ و $|K|=5$. ثابت کنید که $G=HK$.

۱۴- فرض کنید که H و K زیرگروه‌هایی از گروه متناهی G باشند به طوری که $|H|,|K| \geq \sqrt{|G|}$. ثابت کنید که $H \cap K \neq \{e\}$.

۱۵- فرض کنید G گروهی از مرتبه‌ی pq باشد که در آن p و q دو عدد اول هستند و $p > q$. ثابت کنید که گروه G حداکثر دارای یک زیرگروه از مرتبه‌ی p است.

۳.۲ مشبکه‌ی زیرگروه‌ها

مشبکه‌ی زیردستگاه‌های کلی جبری را در فصل ۱، بندهای ۹.۶.۱ - ۱۹.۶.۱ معرفی و اندکی مطالعه کردیم. در این بخش تعبیر این مطالب کلی را برای گروه‌ها مطالعه می‌کنیم. بسیاری از مطالب این بخش تکرار مطالب بخش ۶.۱ به زبان گروه‌ها است. فرض کنیم $Sub(G)$ مجموعه‌ی همه‌ی زیرگروه‌های گروه G باشد. در زیر خواهیم دید که مجموعه‌ی مرتب $(Sub(G);\leq)$، که در آن $\leq$ رابطه‌ی ترتیبی $\subseteq$ است، نیز یک مشبکه (در واقع مشبکه‌ای کامل) است. برخی از پژوهشگران به کمک ویژگی‌های این مشبکه اطلاعات مفیدی در باره‌ی خود گروه G به دست می‌آورند. این مشبکه در پژوهش‌های علوم شیمی و فیزیک نیز کاربردهای خوبی دارد.

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

۱.۳.۲ قضیه. فرض کنیم G گروه است. در این صورت:

۱- برای هر $H, K \leq G$، $H \cap K$ نیز زیرگروه G است.

۲- برای هر خانواده‌ی $\{H_i\}_{i\in I}$ از زیرگروه‌های G، $H = \bigcap_{i\in I} H_i$ نیز زیرگروه G است.

اثبات. یقین داریم که این قضیه را به راحتی می‌توانید اثبات کنید. محک ۶.۲.۲ یا ۷.۲.۲ را به کار ببرید. (آیا لم ۱۰.۶.۱ این قضیه را اثبات می‌کند؟ بند ۱ بحث ۱۱.۶.۱ همراه با تعریف ۳.۱.۲ چطور؟).

حـال ببینـیم کـه $H \vee K = Sup\{H, K\}$ و $\bigvee\{H_i\}_{i\in I} = Sup\{H_i\}_{i\in I}$ کـدام زیرگروه‌های G هستند. روشن است که اگر اجتماع $H \cup K$ زیرگروه G باشد، آنگاه سـوپریمم نیز خواهد بود، زیرا کوچک‌ترین زیرگروه شامل H و K است. ولی، همان طور کـه در بخـش ۶.۱ نیز دیدیم، اجتماع دو زیردستگاه جبری لزوماً یک زیردستگاه نیست! (مثالی از زیرگروه‌های کلایـن یا $\mathbb{Z}$ بیاورید به طوری که اجتماع آن‌ها نسبت به عمل گروه بسته نباشد). برای حل کردن مساله، ابتدا تعبیر بند ۲ تعریف کلی ۱۲.۶.۱ را برای زیرگروه‌ها می‌آوریم.

۲.۳.۲ تعریف. فرض کنیم X زیرمجموعه‌ی گروه G باشد. در این صـورت، **کوچـک‌تـرین زیرگروه** G را که **شامل** X باشـد **زیرگـروه تولیـد شـده توسـط** X مـی‌نـامیم و آن را بـا $< X >$ نشان می‌دهیم. اگر $G = < X >$، می‌گوییم که گروه G توسـط X تولیـد شـده یـا X **مولد** G است.

۳.۳.۲ بحث در کلاس. یقیناً دو سؤال زیر برایتان مطرح هسـتند: **(الف)** آیـا کوچـک‌تـرین زیرگروه G شامل مجموعه‌ی X، یعنی $< X >$، همیشه وجود دارد؟ **(ب)** اگـر X داده شـود، چطور می‌توانیم کوچک‌ترین زیرگروه شامل مجموعه‌ی X، یعنی $< X >$ را (به ویـژه بـه کمـک برنامه‌ی رایانه‌ای) پیدا کنیم؟ در قضیه‌ی ۱۵.۶.۱ دیـدیم کـه $< X >$ بـه عنـوان زیرگروهـواره‌ی $(G;*)$ همیشه وجود دارد، ولی آیا زیر گروه است؟ در بحث ۱۴.۶.۱ گفتیم که اگر P از معادله‌ها تشکیل شده باشد، $< X >$ یک P - زیرجبر می‌شود. خوشبختانه بند ۱ قضیه‌ی ۱.۳.۲ نیـز نویـد می‌دهد که $< X >$ زیرگروه است. شگرد اثبات قضیه‌ی زیر را در اثبات قضیه‌ی ۱۵.۶.۱ آموختیم. از آنجا که این روش اثبات را در بسیاری از دروس دیگر جبر و جبر خطی به کـار مـی‌بـریم، اثبـات ساده‌ی آن را برای گروه‌ها دو باره می‌آوریم. اثبـات قضـیه‌ی ۹.۳.۲ و نتیجـه‌هـای پـس از آن نیـز تمرین خوبی هستند.

۴.۳.۲ قضیه. فرض کنیم G گـروه اسـت، $X \subseteq G$، و $S = \{H \leq G \mid X \subseteq H\}$ در این صورت،

$$< X > = \bigcap S = \bigcap_{H\in S} H = \bigcap\{H \leq G \mid X \subseteq H\}$$

اثبات. با توجه به تعریف $< X >$ که با دو ویژگی **زیرگروه** G **شـامل** X **کوچـک‌تـرین** است، ابتدا باید نشان دهیم که $K = \bigcap_{H\in S} H$ دارای این دو ویژگـی اسـت. قضـیه‌ی ۱.۳.۲ نشـان می‌دهد که $K = \bigcap_{H\in S} H$ زیرگروه G است. چون هـر عضـو $H \in S$ شـامل X اسـت، پـس

$K = \bigcap_{H \in S} H$ نیز شامل X است. تا اینجا اثبات شد که K زیرگروهی از G و شامل X است. برای اثبات اینکه K با این دو ویژگی کوچک‌ترین است، فرض می‌کنیم کـه L نیـز زیرگروهـی از G و شامل X باشد. پس $L \in S$. حال، روشن است کـه $K = \bigcap_{H \in S} H \subseteq L$ و اثبـات تمـام است!

۵.۳.۲ نتیجه. فرض کنیم که G گروه و H و K زیرگروه آن باشند. در این صورت،

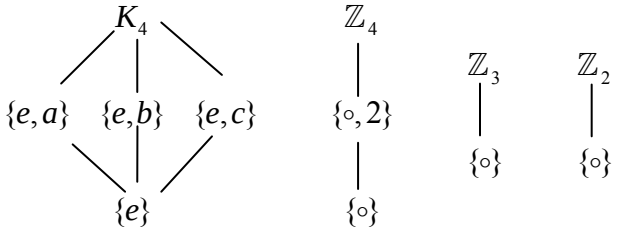
$$H \vee K = Sup\{H, K\} = <H \cup K>$$

۶.۳.۲ نتیجه. مجموعه‌ی مرتب $(Sub(G); \subseteq)$ متشکل از زیرگروه‌های گروه G مشبکه (و در واقع، مشبکه‌ای کامل) است $\left(\bigvee\{H_i\}_{i \in I} = Sup\{H_i\}_{i \in I} = <\bigcup_{i \in I} H_i>\right)$.

۷.۳.۲ تعریف. نمودار مشبکه‌ی $(Sub(G); \subseteq)$ را **نمودار مشبکه‌ی زیرگـروه‌هـای** G می‌نامیم.

۸.۳.۲ بحث در کلاس

۱- با توجه به بحث ۹.۲.۲، نمودارهای مشبکه‌ی زیرگروه‌های چند گروه را در زیر می‌آوریم:



۲- با توجه به بند ۱، $<2>$ را در $\mathbb{Z}_3$ و در $\mathbb{Z}_4$ و $<a>$، $<a,b>$ را در K_4 بیابید.

۳- روشن است که اگر X خود یک زیرگروه G باشد، آنگاه $<X> = X$. **چطور؟** همچنین، کوچـک‌تـرین زیرگـروه G شـامل مجموعـه‌ی تهـی برابـر بـا $\{e\}$ اسـت. یعنـی، $<\varnothing> = \{e\} = <e>$.

۴- (جالب است) فرض کنیم G گروه و H و K زیرگـروه آن باشـند. نشـان دهیـد کـه، اجتمـاع $H \cup K$ زیرگروه G است اگر و تنها اگر $H \subseteq K$ یا $K \subseteq H$.

۵- ممکن است $X \neq Y$ ولی $<X>=<Y>$. برای مثال، فرض کنید $G=(\mathbb{Z}_4;+_4)$. در این صورت، $<1,2>=<1>$. چطور؟

۶- با استفاده از قضیه‌ی ۴.۳.۲، نشان دهید که اگر $X \subseteq Y$ زیرمجموعه‌های گروه G باشند آنگاه $<X> \subseteq <Y>$.

۷- علت اینکه فعلاً توانایی چندانی در محاسبه‌ی $<X>$ نداریم و حتی نمی‌توانیم برنامه‌ای رایانه‌ای برای محاسبه‌ی آن بنویسیم، این است که تعریف ۲.۳.۲ و قضیه‌ی ۴.۳.۲ مطلبی در باره‌ی عضوهای $<X>$ بر حسب عضوهای X بیان نمی‌کنند!

۸- این مثال‌ها را در بخش ۶.۱ نیز دیده‌ایم. چطور، برای مثال، می‌توان $<2>$ را در گروه $(\mathbb{Z}_8;+_8)$ محاسبه کرد؟ چون $\mathbb{Z}_8$ متناهی است، قضیه‌ی ۸.۲.۲ به کار می‌آید. یعنی باید کم‌ترین تعداد عضو $\mathbb{Z}_8$ را به مجموعه‌ی $\{0,2\}$ بیفزاییم تا مجموعه‌ای بسته نسبت به عمل جمع همنهشتی $+_8$ به دست آید! روشن است که

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

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

۱۰- زیرگروه $H=<2,3>$ در گروه $\mathbb{Z}_{15}$ کدام است؟ محاسبه‌ی این زیرگروه نیز راحت، ولی قدری پرزحمت‌تر، است! باید شامل عضوهای زیر باشد:

$$\begin{aligned}&0,2,4,6,8,\cdots \\ &3, 3+_{15} 3=6, 9, \cdots \\ &2+_{15} 3=5, \cdots\end{aligned}$$

اگر کمی از عقل سلیم را به کار ببریم، اغلب این محاسبه‌ها را می‌توانیم کوتاه‌تر کنیم. برای مثال، چون $1 \in H$ $(8+_{15} 8=16 \equiv_{15} 1)$، پس $H=\mathbb{Z}_{15}$. چرا؟

۱۱- آیا برای محاسبه‌ی زیرگروه $<1>$ در گروه $(\mathbb{Z};+)$ می‌توان قضیه‌ی ۸.۲.۲ را به کار برد؟ بنابر بند ۶ بحث ۹.۲.۲، هر زیرگروه نابدیهی $(\mathbb{Z};+)$ نامتناهی است. پس قضیه‌ی ۸.۲.۲ به کار نمی‌آید! ولی می‌توانید قضیه‌ی ۶.۲.۲ را به کار ببرید و نتیجه بگیرید که $<1>=\mathbb{Z}$. به همین ترتیب، می‌توانید نشان دهید که، برای مثال،

$$<2>=2\mathbb{Z}=\{2k \mid k \in \mathbb{Z}\} \quad ,\cdots, \quad <n>=n\mathbb{Z}$$

۱۲- با توجه به نمونه‌های بالا و با الگو (صرفاً الگو) قرار دادن حالت بسیار کلی و صوری ساختن گروه آزاد در بحث **۱۶.۸.۱**، حدس بزنید که در حالت کلی، چطور عضوهای $< X >$ را در گروه دلخواه G تعیین کنیم؟ چون $< \varnothing > = \{e\}$، فرض می‌کنیم $X \neq \varnothing$. احتمالاً درست حدس زده‌اید. به زبان غیر رسمی، ابتدا عضوهای X را در سبدی می‌ریزیم. سپس وارون‌های این عضوها را به سبد اضافه می‌کنیم و مجموعه‌ی زیر را به دست می‌آوریم:

$$T_1 = X \cup X^{-1}$$

که در آن $X^{-1} = \{x^{-1} \mid x \in X\}$ مجموعه‌ی همه‌ی وارون‌های عضوهای X است. هنوز کارمان تمام نشده است، زیرا ممکن است این سبد نسبت به عمل گروه بسته نباشد. پس حاصل-ضرب‌های هر تعداد متناهی از عضوهای سبد را نیز به آن اضافه می‌کنیم و مجموعه‌ی زیر را به دست می‌آوریم:

$$T_2 = \{x \in G \mid x \text{ حاصل‌ضرب تعدادی متناهی از عضوهای } T_1 \text{ است}\}$$

آیا به هدفمان رسیدیم؟ حتماً می‌گویید که پس وارون‌ها و حاصل‌ضرب‌های عضوهای مجموعه‌ی T_2 **چطور؟** فرض کنیم این عضوها را نیز در سبدمان انداختیم؛ وارون‌ها و حاصل-ضرب‌های این مجموعه‌ی اخیر **چطور؟** به نظر می‌رسد که باید این روند را تا بینهایت ادامه دهیم و هرگز سبدمان به یک زیرگروه تبدیل نشود! ولی، قضیه‌ی زیر نشان می‌دهد که در همان مرحله‌ی رسیدن به T_2 کارمان تمام است! یقیناً نخواهید گفت که این همه تلاش ما برای چیست!؟ مطابق معمول این کتاب، هدف ما آموزش **فوت و فن** کارها است و هدف شما نیز آموختن این فوت و فن‌ها و روش‌های تفکر و به کار بردن این شگردها در موارد مشابه است. همتای بسیاری از مفاهیم این کتاب، به ویژه قضیه‌ی زیر، را در مباحث دیگر ریاضی، به ویژه در درس‌های جبر و جبرخطی (و البته، در کاربردهای آن‌ها در فیزیک، شیمی، کامپیوتر نظری، و علوم دیگر) خواهید دید.

۹.۳.۲ قضیه. اگر $X \neq \varnothing$ زیرمجموعه‌ی گروه G باشد، آنگاه $< X >$ (در نمادگذاری ضربی) متشکل از همه‌ی حاصل‌ضرب‌های متناهی به صورت $x_1 x_2 \cdots x_n$ است که در آن، برای هر i، $x_i \in X$ یا $x_i \in X^{-1}$. یعنی،

$$< X > = \{x_1 x_2 \cdots x_n \mid n \in \mathbb{N}, x_i \in X \cup X^{-1}\}$$

اثبات. قرار می‌دهیم $H = \{x_1 x_2 \cdots x_n \mid n \in \mathbb{N}, x_i \in X \cup X^{-1}\}$ و نشان می دهیم که **(الف)** $H \leq G$، **(ب)** $X \subseteq H$، **(پ)** اگر K نیز زیرگروه G باشد و $X \subseteq K$، آنگاه $H \subseteq K$.

بـرای اثبـات **(الــف)**، توجـه مـی‌کنـیم کـه عضـوی چـون $x \in X$ وجـود دارد. پـس $e = xx^{-1} \in H$. حال اگر، برای $x_i, y_j \in X \cup X^{-1}$،

$$x = x_1 \cdots x_n, \quad y = y_1 \cdots y_m \in H$$

آنگاه (درستی واقعیت زیر را توضیح دهید):

$$xy^{-1} = x_1 \cdots x_n (y_1 \cdots y_n)^{-1} = x_1 \cdots x_n y_n^{-1} \cdots y_1^{-1} \in H$$

درستی شرط **(ب)** روشن است. اثبات درستی شرط **(پ)** نیز راحت است. چون $X \subseteq K$ و K نسبت به وارون‌ها بسته است، پس $X \cup X^{-1} \subseteq K$. حال، چون K نسبت بـه عمـل گروه بسته اسـت و هـر عضـو H بـه صـورت $x = x_1 \cdots x_n$ اسـت، کـه در آن هـر x_i در $X \cup X^{-1}$ است، پس $H \subseteq K$.

نتیجه‌های زیر را به راحتی می‌توانید اثبات کنید.

۱۰.۳.۲ نتیجه. اگر $X \neq \emptyset$ زیرمجموعه‌ی گروه G باشد، آنگاه (در نمادگذاری ضربی)

$$< X > = \{x_1^{n_1} x_2^{n_2} \cdots x_k^{n_k} \mid x_i \in X, n_i \in \mathbb{Z}\}$$

۱۱.۳.۲ نتیجه. اگر $X = \{x_1, \cdots, x_k\}$ زیرمجموعه‌ای متناهی از گروه G باشد، به طوری که

$$(\forall i, j = 1, \cdots, k) \quad x_i x_j = x_j x_i$$

آنگاه $< x_1, \cdots, x_n > = < \{x_1, \cdots, x_k\} > = \{x_1^{n_1} \cdots x_k^{n_k} \mid n_1, \cdots, n_k \in \mathbb{Z}\}$

۱۲.۳.۲ نتیجه. اگر $X = \{x\}$ زیرمجموعه‌ای تک عضوی از گروه G باشد، آنگاه

$$< x > = \{x^n \mid n \in \mathbb{Z}\}$$

و در نمادگذاری جمعی، $< x > = \{nx \mid n \in \mathbb{Z}\}$.

۱۳.۳.۲ تعریف

۱- اگـر $X = \{x_1, x_2, \cdots, x_n\}$ زیرمجموعـه‌ای متنـاهی از گـروه G باشـد، آنگـاه $H = < X > = < x_1, \cdots, x_n >$ را **زیرگروه متناهی مولد** G می‌نامیم.

۲- اگر $X=\{x\}$، آنگاه $H=<x>$ را **زیرگروه دوری** با مولد x می‌نامیم.

۳- اگر $G=<x_1,\cdots,x_n>$، آنگاه G را **گروهی متناهی مولد** و اگر $G=<x>$، آن را **گروهی دوری** با مولد x می‌نامیم.

۱۴.۳.۲ بحث در کلاس

۱- به دلیل اهمیت گروه‌های دوری، آن‌ها را در بخش۴.۲ به تفصیل مطالعه خواهیم کرد. توجه می‌کنیم که یک تفاوت دیگر گروه‌های $\mathbb{Z}_4$ و K_4 این است که $\mathbb{Z}_4=<1>=<3>$ دوری است، در حالی که K_4 چنین نیست. **چرا؟**

۲- با استفاده از نتیجه‌ی۱۲.۳.۲، نشان دهید که هر گروه دوری، آبلی است.

۳- با استفاده از قضیه‌ی۹.۳.۲ و نتیجه‌ی۱۰.۳.۲ ، برنامه‌ای کامپیوتری بنویسید به طوری که $<X>$ را در گروه دلخواه G تعیین کند.

۴- با دیدن نمونه‌های

$$
\begin{aligned}
&<e>=\{e\},\quad <G>=G\\
&\mathbb{Z}=<1>=<2,3>=\cdots\\
&2\mathbb{Z}=<2>=<-2>=<2,4,16>=\cdots\\
&n\mathbb{Z}=<n>=<-n>=\cdots\\
&\mathbb{Z}_4=<\mathbb{Z}_4>=<1>=<1,2>=<3>=<2,3>\\
&\mathbb{Z}_n=<1>=<k>,\quad (k,n)=1\\
&K_4=<a,b>=<a,c>=\cdots\\
&K_4\neq<e>\neq<a>\neq<b>\neq<c>,\{e\}=<e>,\\
&\{e,a\}=<a>,\quad \{e,b\}=<b>,\quad \{e,c\}=<c>
\end{aligned}
$$

متوجه چه نکته‌هایی در مورد تعریف بالا می‌شویم؟ درست است: $X=G$ مولد خود گروه G است؛ مجموعه‌های متفاوت ممکن است مولد یک گروه باشند؛ یک گروه یا زیرگروه آن ممکن است با مجموعه‌ای نامتناهی تولید شود و در عین حال با مجموعه‌ای متناهی یا حتی تک عضوی نیز تولید شود، یعنی متناهی مولد یا حتی دوری باشد؛ گروه‌های $(\mathbb{Z};+)$، $2\mathbb{Z}$، $(\mathbb{Z}_n;+_n)$ دوری هستند؛ اگر مولد گروه‌های دوری $\mathbb{Z}$ و $\mathbb{Z}_n$، یعنی عدد ۱، عضو زیرگروهی از $\mathbb{Z}$ یا $\mathbb{Z}_n$ باشد، آن زیرگروه برابر با خود گروه است؛ با وجودی که K_4 دوری نیست، ولی هر زیرگروه دیگر آن دوری است!

تمرین ۳.۲

تمرین‌ها مهم‌ترین قسمت هر درس هستند

دسته‌ی اول

۱- نشان دهید که $\mathbb{Z}_{12} = <2,3>$. سپس نشان دهید که، برای $n \geq 3$، $\mathbb{Z}_n = <2,3>$.

۲- فرض کنیم G گروه و H و K زیرگروه آن باشند. نشان دهید که، اجتماع $H \cup K$ زیرگروه G است اگر و تنها اگر $H \subseteq K$ یا $K \subseteq H$. همچنین، نتیجه بگیرید که هیچ گروهی را نمی‌توان به صورت اجتماع دو زیرگروه سره‌اش نوشت.

۳- بدون استفاده‌ی مستقیم از قضیه‌ی **۹.۳.۲**، ولی مشابه با اثبات آن، نشان دهید که اگر $X \neq \varnothing$ زیرمجموعه‌ی گروه G باشد، آنگاه

(الف) $$< X > = \{x_1^{n_1} x_2^{n_2} \cdots x_k^{n_k} \mid x_i \in X, n_i \in \mathbb{Z}\}$$

(ب) اگر $X = \{x\}$ زیرمجموعه‌ای تک عضوی از گروه G باشد، آنگاه

$$< x > = \{x^n \mid n \in \mathbb{Z}\}$$

دسته‌ی دوم

۴- فرض کنید H، K، و T زیرگروه‌هایی از گروه G باشند به طوری که $H \subseteq K$، $H \cap K = K \cap T$، و $HT = KT$. ثابت کنید که $H = K$.

۵- فرض کنید که A و B زیرگروه‌هایی آبلی از گروه G باشند و $G = AB$. ثابت کنید که

$$Z(G) = (A \cap Z(G))(B \cap Z(G))$$

۶- فرض کنید A، B، C زیرگروه‌هایی از گروه G باشند به طوری که $A \subseteq C$. ثابت کنید که

$$(AB) \cap C = A(B \cap C)$$

۴.۲ گروه‌های دوری

گروه‌های دوری دسته‌ای ساده و در عین حال بسیار با اهمیت از گروه‌ها هستند. از این رو یک بخش کامل را به مطالعه‌ی آن‌ها اختصاص داده‌ایم. همان طور که اعداد اول سازنده‌ی همه‌ی اعداد طبیعی هستند، در دروس بعدی جبر خواهیم دید که گروه‌های **دوری** نیز به تعبیری **سازنده‌ی** همه‌ی گروه‌های **آبلی** متناهی مولد هستند. برای طولانی نشدن این بخش، در بخش بعد دسته-بندی کاملی از گروه‌های دوری به دست خواهیم آورد. در واقع، خواهیم دید که همه‌ی گروه‌های دوری نامتناهی با گروه دوری $(\mathbb{Z};+)$ و هر گروه دوری متناهی n عضوی با گروه دوری $(\mathbb{Z}_n;+_n)$ یک‌ریخت است! بنابراین، تا حد یک‌ریختی، تنها یک دسته گروه دوری نامتناهی داریم و، برای هر عدد طبیعی $n \in \mathbb{N}$، تنها یک دسته گروه دوری n عضوی وجود دارد. از این رو، برای مطالعه‌ی گروه‌های دوری، و لذا گروه‌های آبلی متناهی مولد، تنها کافی است گروه‌های دوری $(\mathbb{Z};+)$ و $(\mathbb{Z}_n;+_n)$ را مطالعه کنیم! **جالب است، این طور نیست؟**

ابتدا مفهوم زیر را می‌آوریم که نه تنها در مطالعه‌ی گروه‌های دوری مفید و اساسی است، بلکه در بررسی همه‌ی گروه‌ها مفید است. داستان از این قرار است که در برخی از گروه‌ها، مانند گروه-های جمعی $(\mathbb{Z};+)$، $(\mathbb{Q};+)$، $(\mathbb{R};+)$، $(\mathbb{C};+)$، هیچ عدد ناصفر، به ویژه عدد ۱، را نمی-توان به تعدادی متناهی با خودش جمع کرد و عدد صفر را به دست آورد. یا در گروه‌های ضربی $(\mathbb{Q}^*;\cdot)$، $(\mathbb{R}^*;\cdot)$، هیچ عدد متفاوت با ۱ و ۱- را نمی‌توان به تعدادی متناهی در خودش ضرب کرد و عدد ۱ را به دست آورد! البته در گروه ضربی $(\mathbb{C}^*;\cdot)$ داریم $(\sqrt{-1})^4 = 1$، ولی بسیاری از اعداد مختلط دیگر این ویژگی را ندارند! از این‌ها جالب‌تر اینکه، در گروه همنهشتی $(\mathbb{Z}_n;+_n)$، هر عضو را می‌توان، برای مثال، به تعداد n یا $2n$ بار، با خودش جمع (همنهشتی) کرد وعضو خنثی 0 را به دست آورد! **این طور نیست؟** همچنین، در K_4 داریم $a^2 = b^2 = c^2 = e$. حدس می‌زنید تابع دوسویی $\sigma \in S_n$ را چند بار با خودش ترکیب کنیم، تابع همانی به دست می‌آید؟ حال تعریف کلی زیر را ببینید.

۱.۴.۲ تعریف. فرض کنیم G گروهی با عضو همانی e باشد و $a \in G$. در این صورت،

۱- می‌گوییم که **مرتبه‌ی** a (در G) **متناهی** است اگر عدد طبیعی m وجود داشته باشد به طوری که $a^m = e$.

۲- کوچک‌ترین عدد طبیعی n با ویژگی $a^n = e$ را **مرتبه‌ی** a (در G) می‌نامیم و می‌نویسیم $O_G(a)$، یا $O(a)$ اگر امکان اشتباه نباشد.

۳- اگر عدد طبیعی m با ویژگی $a^m = e$ وجود نداشته باشد، می‌گوییم که **مرتبه‌ی** a (در G) **نامتناهی** است، و می‌نویسیم $O_G(a) = \infty$.

۲.۴.۲ بحث در کلاس

۱- یادآوری می‌کنیم که در نمادگذاری جمعی، عبارت $a^n = e$ به $na = 0$ تبدیل می‌شود، که در آن $na = a + a + \cdots + a$. در هر گروه G، $O(e) = 1$.

۲- یک عضو ممکن است متعلق به چند گروه باشد و مرتبه‌ی آن در هر گروه متفاوت باشد. برای مثال، $O_{\mathbb{Z}_4}(1) = 4$ در حالی که $O_{\mathbb{Z}_7}(1) = 7$ و $O_{\mathbb{Z}}(1) = \infty$. به عنوان نمونه‌هایی دیگر، $O_{\mathbb{Z}_4}(2) = 2$، در حالی که $O_{\mathbb{Z}_{16}}(2) = 8$.

۳- نشان دهید که $O_G(a) = \infty$ اگر و تنها اگر همه‌ی توان‌های a متمایز باشند! راهنمایی: از این مطالب استفاده کنید که **(الف)** اگر برای دو عدد صحیح $r > s$، داشته باشیم $a^r = a^s$، آنگاه، به دلیل وجود وارون‌ها در گروه G، $a^{r-s} = e$ که در آن $r - s \in \mathbb{N}$، و **(ب)** اگر $a^m = e$ آنگاه $a^{2m} = e = a^m$.

۴- با استفاده از بند۳، نشان دهید که مرتبه‌ی هر عضو در گروهی متناهی، یقیناً متناهی است!

۵- آیا مرتبه‌ی عضوی نا همانی در گروهی نامتناهی می‌تواند متناهی باشد؟ توجه می‌کنیم که، اگر چه در گروه جمعی اعداد مختلط $(\mathbb{C};+)$ مرتبه‌ی هر عضو ناصفر نامتناهی است، ولی در گروه ضربی و نامتناهی $(\mathbb{C}^*;\cdot)$ داریم $O(i) = O(\sqrt{-1}) = 4$.

۶- در گروه K_4، $O(a) = O(b) = O(c) = 2$.

۷- در گروه خطی عام نامتناهی $GL(2,\mathbb{R})$، $O\left(\begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}\right) = 2$ (چرا؟)

۸- در مطالعه‌ی گروه‌های دوری، حساب اعداد طبیعی (بخش‌پذیری، الگوریتم تقسیم، و از این قبیل، که در مقدمه آوردیم) نقش مهمی دارد. قضیه‌ی زیر کار محاسبه‌ی مرتبه را اغلب ساده‌تر می‌کند.

۳.۴.۲ لم. فرض کنیم که مرتبه‌ی عضو $a \in G$ متناهی باشد. در این صورت $O(a) = n$ اگر و تنها اگر دو شرط زیر برقرار باشند:

۱- $a^n = e$؛

۲- اگر برای عدد طبیعی m، $a^m = e$ آنگاه $n \mid m$. (در حالی که در تعریف مرتبه تنها شرط $n \leq m$ آمده است.)

اثبات. روشن است که اگر شرایط (الف) و (ب) برقرار باشند، آنگاه $O(a) = n$. برعکس، فرض کنیم $O(a) = n$. روشن است که $a^n = e$. حال فرض کنیم $a^m = e$. برای اثبات بخشپذیری $n \mid m$، بنابر الگوریتم تقسیم، می‌نویسیم

$$m = nq + r, \qquad 0 \leq r < n \qquad (*)$$

حال داریم (به فن اثبات توجه کنید)

$$e = a^m = a^{nq+r} = a^{nq}a^r = (a^n)^q a^r$$
$$= e^q a^r = a^r$$

بنابراین، چون $r < n$، باید $r = 0$ (چرا؟) و در نتیجه $m = nq$، که حکم قضیه را اثبات می‌کند.

قبل از به کار بردن مفهوم مرتبه در مطالعه‌ی گروه‌های دوری، حکم‌های زیر را نیز می‌آوریم.

۴.۴.۲ **لم.** حکم‌های زیر برای عضوهای گروه G برقرار هستند.

۱- $O(a) = O(b) \Leftrightarrow (\forall m \in \mathbb{N})(a^m = e \Leftrightarrow b^m = e)$.

۲- $O(a) = O(a^{-1})$.

۳- $O(a) = O(xax^{-1})$.

۴- $O(ab) = O(ba)$.

۵- اگر $O(a) = n$ و $k \mid n$، آنگاه $O(a^k) = n/k$.

۶- فرض کنیم $O(a) = n$ و $d = (m,n)$. در این صورت،

$$O(a^m) = \frac{O(a)}{(m,n)} = \frac{n}{d}$$

اثبات. حکم ۶ را اثبات می‌کنیم. بقیه را به آسانی می‌توانید، با استفاده از لم ۳.۴.۲ و بند ۱ این لم، اثبات کنید.

۶- بنـا بـه فـرض، داریـم $m = dm_1$ و $n = dn_1$ کـه در آن $(m_1, n_1) = 1$. بـرای اثبـات $O(a^m) = n/d$، توجه می‌کنیم که

$$(a^m)^{\frac{n}{d}} = a^{\frac{mn}{d}} = a^{\frac{dm_1 n}{d}} = a^{m_1 n} = (a^n)^{m_1} = e^{m_1} = e$$

حال، اگر $(a^m)^l = e$، آنگاه $n \mid ml$، یعنی $dn_1 \mid dm_1 l$ و در نتیجه، $n_1 \mid m_1 l$. ولی $(n_1, m_1) = 1$ ایجاب می‌کند که $(n/d) = n_1 \mid l$ و حکم اثبات شده است.

حال برخی از ویژگی‌های گروه‌های دوری را بررسـی مـی‌کنـیم. ابتـدا یـادآوری مـی‌کنـیم کـه $< a > = \{a^n \mid n \in \mathbb{Z}\}$ و در نمادگذاری جمعی، $< a > = \{na \mid n \in \mathbb{Z}\}$. قضـیه‌ی زیـر و اثبات آن بسیار با اهمیت است. یادآوری می‌کنیم که $|G|$ عدد اصلی یا **مرتبه**‌ی گروه G اسـت. قضیه‌ی زیر توجیه می‌کند که چرا واژه‌ی **مرتبه** را برای تعداد عضوهای گروه نیز به کار بردیم.

۵.۴.۲ قضیه. فـرض کنـیم a عضـو گـروه G باشـد. در ایـن صـورت، مرتبـه‌ی گـروه دوری $< a >$ برابر با مرتبه‌ی هر مولد آن است. یعنی، $O(a) = |< a >|$.

اثبات ابتدا فرض می‌کنیم که $O(a) = n < \infty$ متناهی باشـد. ادعـا مـی‌کنـیم کـه عضـوهای $\{e, a, a^2, \cdots, a^{n-1}\}$ متمایز هستند و $< a > = \{e, a, a^2, \cdots, a^{n-1}\}$. روشـن اسـت کـه $\{e, a, a^2, \cdots, a^{n-1}\} \subseteq < a >$. برعکس، فرض کنـیم $x = a^m \in < a >$. بنـابر الگـوریتم تقسیم، داریم

$$m = nq + r \qquad 0 \le r < n$$

حـال، بـا محاسـبه‌ی $a^m = a^{nq+r}$، نشـان دهیـد کـه $a^m = a^r$ و نتیجـه بگیریـد کـه $x = a^m \in \{e, a, a^2, \cdots, a^{n-1}\}$. برای کامل کردن اثبـات، بایـد نشـان دهـیم کـه عضـوهای $\{e, a, a^2, \cdots, a^{n-1}\}$ متمایز هستند. داریم

$$a^r = a^s \quad (r > s, 0 \le r, s < n-1) \quad \Rightarrow a^{r-s} = e$$

که متناقض با $O(a) = n$ است، زیرا $0 < r - s < n$. این مطلب حکـم را در حالـت متنـاهی بودن مرتبه اثبات می‌کند. **چطور؟**

حال فرض کنید $O(a) = \infty$. کافی است نشان دهید که همه‌ی عضوهای

$$e, a, a^2, \cdots, a^k, \cdots$$

متمایز هستند (فن کار را آموخته‌اید. بند ۳ بحث ۲.۴.۲ را نیز ببینید).

۶.۴.۲ نتیجه. فرض کنیم گروه G دارای n عضو باشد. در این صورت، G دوری است اگر و تنها اگر دارای عضوی چون $a \in G$ با مرتبه‌ی n باشد.

اثبات. کافی است با دقت بیشتری به اثبات قضیه‌ی بالا توجه کنید.

نتیجه‌های جالبی بلاواسطه از تلفیق قضیه‌های لاگرانژ و ۵.۴.۲ به دست می‌آیند که بسیار به کار خواهیم برد.

۷.۴.۲ نتیجه. مرتبه‌ی هر عضو a از گروه متناهی G مرتبه‌ی گروه G را می‌شمارد، یعنی $O_G(a) \mid\mid G \mid$.

۸.۴.۲ نتیجه. اگر G گروهی با n عضو باشد، آنگاه

$$(\forall a \in G) \quad a^n = e$$

۹.۴.۲ نتیجه. هر گروه از مرتبه‌ی عددی اول، دوری است و هر عضو $a \neq e$ مولد آن است.

۱۰.۴.۲ بحث در کلاس

۱- با استفاده از نتیجه‌ی ۶.۴.۲، یک بار دیگر نشان دهید که گروه K_4 دوری نیست.

۲- توجه می‌کنیم که چون $\mathbb{Z} = <1> = <-1>$ و برای هر عدد صحیح دیگر n، $\mathbb{Z} \neq <n>$، این گروه دوری تنها دارای دو مولد است. ولی گروه‌های دوری متناهی ممکن است یک، دو یا بیش از دو مولد داشته باشند. همه‌ی مولدهای گروه‌های دوری $\mathbb{Z}_4$، $\mathbb{Z}_6$، و $\mathbb{Z}_5$، را بیابید.

۳- در بخش ۹ از فصل ۱، دسته‌های دستگاه‌های جبری را مطرح کردیم که ممکن است نسبت به اعمالی چون زیردستگاه، حاصل ضرب، و خارج قسمت بسته باشند. اگر $\mathcal{K}$ دسته‌ی همه‌ی گروه-های دوری باشد، خواهیم دید که $\mathcal{K}$ نسبت به زیرگروه و خارج قسمت بسته است ولی نسبت به حاصل‌ضرب بسته نیست! از این مطلب آخر و قضیه‌ی بیرخوف، در بخش ۹.۱، چه نتیجه‌ای در باره‌ی دسته‌ی گروه‌های دوری به دست می‌آید؟ **روش اثبات** قضیه‌ی بسیار مهم زیر را یکی دو بار دیگر به کار خواهیم برد.

۱۱.۴.۲ قضیه. زیرگروه هر گروه دوری، گروهی دوری است.

اثبات. فرض کنیم $G=<a>$ گروهی دوری و H زیرگروه آن باشد. حالت $H=\{e\}=<e>$ روشن است. فرض کنیم $H\neq\{e\}$ و $h\neq e$ در H باشد. چون $h\in H\subseteq G=<a>$، پس $h=a^k$ که در آن $k\in\mathbb{Z}^*$. از طرفی، $h^{-1}=a^{-k}\in H$ و در نتیجه مجموعه‌ی

$$S=\{m\in\mathbb{N}\mid a^m\in H\}\subseteq\mathbb{N}$$

ناتهی است. **چرا؟** حال، بنابر **اصل خوش‌ترتیبی** در $\mathbb{N}$، مجموعه‌ی S دارای **کوچک‌ترین** عدد طبیعی مانند n است. ادعا می‌کنیم که $H=<a^n>$. روشن است که $a^n\in H$ و در نتیجه $<a^n>\subseteq H$. **چرا؟** برای اثبات $H\subseteq<a^n>$، فرض می‌کنیم $h\in H$ دلخواه باشد. داریم $h=a^m$ که در آن $m\in\mathbb{Z}$. **چرا؟** حال، بنابر الگوریتم تقسیم، داریم

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

و در نتیجه $a^m=a^{nq+r}=(a^n)^q a^r$. بنابراین، $a^r=a^m(a^n)^{-q}\in H$. **چرا؟** حال، چون n کوچک‌ترین عدد طبیعی با شرط $a^n\in H$ است و $0\leq r<n$، باید $r=0$. در نتیجه، $m=nq$ و $a^m=(a^n)^q\in<a^n>$. این مطلب اثبات می‌کند که $H=<a^n>$.

۱۲.۴.۲ نتیجه. اگر $H\neq\{e\}$ زیرگروهی از گروه دوری $G=<a>$ باشد، آنگاه $H=<a^n>$، که در آن n کوچک‌ترین عدد طبیعی با ویژگی $a^n\in H$ است.

اثبات. کافی است به اثبات قضیه‌ی بالا توجه کنید.

در بند ۶ بحث **۹.۲.۲** قول دادیم که همه‌ی زیرگروه‌های $(\mathbb{Z};+)$ را مشخص خواهیم کرد. نتیجه‌ی مهم زیر در این باره است.

۱۳.۴.۲ نتیجه

۱- هر زیر گروه $(\mathbb{Z};+)$ دوری و به صورت $H=n\mathbb{Z}=\{nk\mid k\in\mathbb{Z}\}$ است، که در آن $n\in\mathbb{N}\cup\{0\}$.

۲- رابطه‌ی ترتیبی در $Sub(\mathbb{Z})$ به صورت زیر است:

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

۳- سوپریمم و اینفیمم در مشبکه‌ی $Sub(\mathbb{Z})$ به صورت زیر هستند:

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

که در آن، $[m,n]$ کوچک‌ترین مضرب مشترک m و n و (m,n) بزرگ‌ترین مقسوم‌علیه آن‌ها است.

اثبات. بلاواسطه از قضیه‌ی ۱۱.۴.۲ نتیجه می‌شود. در ضمن، توجه می‌کنیم که اگر $H \neq \{0\}$ زیرگروه $\mathbb{Z}$ باشد، آنگاه n کوچک‌ترین عدد طبیعی متعلق به H است به طوری که $H = n\mathbb{Z}$.

۱۴.۴.۲ بحث در کلاس. قضیه‌ی مهم ۱۱.۲.۲ لاگرانژ را به خاطر بیاورید که بیان می‌کند اگر H زیرگروهی از یک گروه متناهی G باشد، آنگاه مرتبه‌ی H، یعنی $|H|$، مرتبه‌ی G، یعنی $|G|$، را می‌شمارد. حال، سؤال این است که آیا عکس قضیه‌ی لاگرانژ درست است؟ یعنی، اگر m مرتبه‌ی گروه متناهی G را بشمارد، آیا G لزوماً باید زیرگروهی m عضوی داشته باشد؟ پاسخ به این سؤال در حالت کلی منفی است، و قضیه‌های سیلو در درس‌های دیگر جبر مشخص می‌کنند که عکس قضیه‌ی لاگرانژ برای کدام نوع از گروه‌ها و از چه مرتبه‌ای درست است. ولی با اطلاعاتی که تاکنون به دست آورده‌ایم، پاسخ سؤال بالا را می‌توانیم در قضیه‌ی زیر برای گروه‌های دوری متناهی اثبات کنیم.

۱۵.۴.۲ قضیه. فرض کنیم $G = < a >$ گروهی دوری با n عضو باشد. در این صورت،

۱- برای هر عدد طبیعی m، G زیرگروهی m عضوی دارد اگر و تنها اگر $m \mid n$.

۲- اگر $m \mid n$، آنگاه G زیرگروهی منحصر به فرد با m عضو دارد.

۳- $< a^r > = < a^s >$ اگر و تنها اگر $(r,n) = (s,n)$.

اثبات

۱- فرض کنیم $m \mid n$. در این صورت $H = < a^{n/m} >$ زیر گروه مورد نظر است، زیرا (مراحل اثبات را توضیح دهید):

$$|H| = O(a^{n/m}) = \frac{n}{(n/m,n)} = \frac{n}{n/m} = m$$

برعکس، اگر $H \leq G$ و $|H| = m$، آنگاه، بنابر قضیه‌ی لاگرانژ، داریم $m \mid n$. یا چون H دوری است و، برای مثال، $H = < a^k >$. در این صورت (مراحل اثبات را توضیح دهید)

$$m = |H| = O(a^k) = \frac{n}{(k,n)} \Rightarrow n = m \cdot (k,n) \Rightarrow m \mid n$$

۲- فرض کنیم $m \mid n$. با توجه به اثبات بند ۱، $H = < a^{n/m} >$ از مرتبه‌ی m است. حال اگر $K = < a^k >$ نیز از مرتبه‌ی m باشد، آنگاه (مراحل زیر را توضیح دهید):

$$\begin{aligned} O(a^k) = m \Rightarrow a^{km} = e \Rightarrow n \mid km \\ \Rightarrow km = nl \Rightarrow k = l(n/m) \\ \Rightarrow a^k \in < a^{n/m} > = H \\ \Rightarrow K \subseteq H \end{aligned}$$

چون $|H| = |K|$ متناهی است، نتیجه بگیرید که $H = K$.

۳- مراحل اثبات زیر را توضیح دهید:

$$\begin{aligned} < a^r > = < a^s > \Leftrightarrow |< a^r >| = |< a^s >| \\ \Leftrightarrow O(a^r) = O(a^s) \\ \Leftrightarrow \frac{n}{(r,n)} = \frac{n}{(s,n)} \\ \Leftrightarrow (r,n) = (s,n) \end{aligned}$$

۱۶.۴.۲ بحث در کلاس

۱- بند ۱ قضیه‌ی بالا برای گروه‌های آبلی متناهی نیز برقرار است، ولی یکتایی بیان شده در بند ۲ چنین نیست. برای مثال گروه آبلی ولی غیر دوری K_4 دارای سه زیرگروه دو عضوی است.

۲- بندهای ۱ و ۲ بیان می‌کنند که تعداد زیرگروه‌های یک گروه دوری n عضوی دقیقاً برابر با تعداد مقسوم‌علیه‌های n، یعنی $d(n)$، است. برای مثال، تعداد زیرگروه‌های $\mathbb{Z}_4$ برابر با ۳، تعداد زیرگروه‌های $\mathbb{Z}_5$ (یا $\mathbb{Z}_p$) برابر با ۲، و تعداد زیرگروه‌های $\mathbb{Z}_{12}$ برابر با ۶ است.

۳- آیا همتای نتیجه‌ی ۱۳.۴.۲ برای گروه‌های دوری $(\mathbb{Z}_n; +_n)$ نیز برقرار است؟ یعنی، آیا می‌توانیم همه‌ی زیرگروه‌های هر گروه دوری $\mathbb{Z}_n$ را دقیقاً مشخص کنیم؟ بحث بعد از نتیجه‌ی زیر پاسخ مثبت به این سؤال است.

۱۷.۴.۲ نتیجـــه. فـــرض کنـــیم کـــه $G=<a>$ گروهـــی دوری از مرتبـــه‌ی n، و $\{k_1,k_2,\cdots,k_t\}$ مجموعه‌ی مقسوم‌علیه‌های n باشد. در این صورت،

۱- $Sub(G)=\{<a^{k_1}>,<a^{k_2}>,\cdots,<a^{k_t}>\}$ مجموعه‌ی همه‌ی زیرگروه‌های G است.

۲- رابطه‌ی ترتیبی در $Sub(G)$ به صورت زیر است:

$$<a^{k_i}>\subseteq<a^{k_j}> \quad \Leftrightarrow \quad k_j \mid k_i$$

۲- سوپریمم و اینفیمم در مشبکه‌ی $Sub(G)$ به صورت زیر هستند:

$$<a^{k_i}>\wedge<a^{k_j}>=<a^{k_i}>\cap<a^{k_j}>=<a^{[i,j]}>$$
$$<a^{k_i}>\vee<a^{k_j}>=<a^{(i,j)}>$$

اثبات. قضیه‌ها و فنون بالا را به کار ببرید.

۱۸.۴.۲ بحث در کلاس. حال ببینیم که چطور با استفاده از این نتیجـه مـی‌تـوانیم همـه‌ی زیرگروه‌های $\mathbb{Z}_n$ را بیابیم. ابتدا بند ۱ صورت نتیجه را برای $\mathbb{Z}_n$ می‌نویسیم.

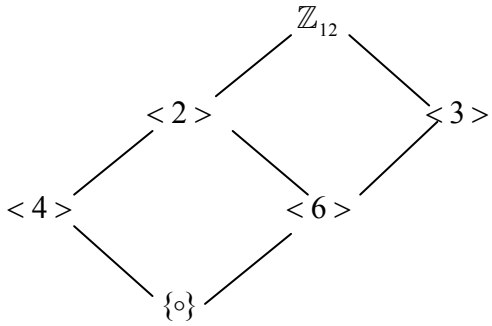
۱- روشن است که $a=1$ یکی از مولدهای گروه $\mathbb{Z}_n$ است. با قرار دادن $a=1$ در بند ۱ نتیجـه، داریم

$$Sub(G)=\{<k_1>,<k_2>,\cdots,<k_t>\}$$

۲- برای مثال، چون مقسوم‌علیه‌های ۱۲ عبارت‌اند از ۱، ۲، ۳، ۴، ۶، و ۱۲، پس زیرگروه‌های $\mathbb{Z}_{12}$ عبارت‌اند از

$$<1>=\mathbb{Z}_{12}, \qquad <2>=\{0,2,4,6,8,10\}$$
$$<3>=\{0,3,6,9\}, \qquad <4>=\{0,4,8\}$$
$$<6>=\{0,6\}, \qquad <12>=\{0\}=<0>$$

۳- با توجه با بندهای ۲ و ۳ نتیجه، نمودار مشبکه‌ی $Sub(\mathbb{Z}_{12})$ به صورت زیر است:



نتیجه‌ی جالب دیگری که می‌توان از قضیه‌های **۵.۴.۲** و **۱۵.۴.۲** به دست آورد، به صورت زیر است.

۱۹.۴.۲ نتیجه. اگر $G=<a>$ گروهی دوری با $|G|=n$ عضو و با مولد a باشد، آنگاه مولدهای دیگر آن به صورت a^r (یا در نماد جمعی ra) هستند که در آن $0<r<n$ و $(r,n)=1$. پس، تعداد مولدهای G برابر است با $\varphi(n)=|\{0<r<n\,|\,(r,n)=1\}|$ (که در آن φ، با همین تعریف، تابع فی اویلر نامیده می‌شود).

اثبات. این نیز روشن است (مراحل زیر را توضیح دهید):

$$\begin{aligned} G=<a^r> &\Leftrightarrow |<a^r>|=n \\ &\Leftrightarrow \frac{n}{(r,n)}=n \\ &\Leftrightarrow (r,n)=1 \end{aligned}$$

۲۰.۴.۲ بحث در کلاس. برای استفاده از نتیجه‌ی بالا در مورد $\mathbb{Z}_n$، مجدداً توجه می‌کنیم که $a=1$ یک مولد $\mathbb{Z}_n$ است. از این رو، برای پیدا کردن همه‌ی مولدهای گروه $\mathbb{Z}_{12}$، ابتدا توجه می‌کنیم که $(r,12)=1$ اگر و تنها اگر $r=1,5,7,11$. حال با قرار دادن $a=1$ و این اعداد در همتای جمعی عبارت $a^r=aa\cdots a$، یعنی $ra=a+a+\cdots+a$، همه‌ی مولدهای $\mathbb{Z}_{12}$ عبارت هستند از: $r1=1,5,7,11$.

شاید این مثال بدیهی چندان روش کار را نشان نداده باشد، مثال نابدیهی‌تری می‌آوریم. زیرگروه $H=<2>=\{0,2,4,6,...,28\}$ از گروه $\mathbb{Z}_{30}=\{0,1,2,\cdots,29\}$ را در نظر می‌گیریم که در آن $a=2$. ابتدا باید $|H|$ را بیابیم. البته روشن است که در این مثال

$|H|=15$، ولی می‌خواهیم روش کلی کار را نشان دهیم. با توجه به مطالبی که در باره‌ی گروه-های دوری می‌دانیم (دلایل هر مرحله از محاسبات زیر را توضیح دهید)، داریم

$$|H|=|<2>|=O_{\mathbb{Z}_{30}}(2)=\frac{30}{(2,30)}=\frac{30}{2}=15$$

حال $(r,15)=1$ اگر و تنها اگر $r=1,2,4,7,8,11,13,14$ و در نتیجه همه‌ی مولدهای H عبارت‌اند از $r.2=2,4,8,14,16,22,26,28$. برای مثال،

$$\begin{aligned}<16>&=\{1.16,2.16,3.16,\cdots,\\&=\{16,2,18,4,20,6,22,8,24,10,26,12,28,14,0\}\\&=H\end{aligned}$$

تمرین ۴.۲

تنها تماشاچی نباشید!

دسته‌ی اول

۱- فرض کنید که گروه دوری G تنها دارای یک مولد است. نشان دهید که $|G|\leq 2$.

۲- ثابت کنید که هر گروه G با $|G|\leq 5$ آبلی است. اگر $|G|=6$ چطور؟

۳- تعداد مولدهای گروه‌های دوری از مرتبه‌های ۱۷، ۶۰ و ۸۱ را بیابید.

۴- تعداد مولدهای هر یک از زیرگروه‌های دوری زیر را بیابید:

(الف) زیرگروه دوری $H=<25>$ از گروه $\mathbb{Z}_{30}$.

(ب) زیرگروه دوری $H=<a^{25}>$ از گروه دوری ۱۶۰ عضوی $G=<a>$.

(پ) زیرگروه دوری $H=<\frac{i+1}{\sqrt{2}}>$ از گروه ضربی $\mathbb{C}^*$.

۵- گروهی مثال بزنید که مرتبه‌ی هر عضو آن توانی از ۲ باشد.

۶- گروهی مثال بزنید که مرتبه‌ی هر عضو آن توانی از عدد اول p باشد.

۷-مثال‌هایی ارائه دهید که گزاره‌های زیر را نقض کنند:

(الف) اگر مرتبه‌ی هر عضو گروه G عدد طبیعی n را بشمارد، آنگاه $|G|$ عدد n را می شمارد.

(ب) اگر گروه G متناهی و هر زیرگروه اکید آن دوری باشد، آنگاه G دوری است.

(پ) اگر n مرتبه‌ی گروه متناهی G را بشمارد، آنگاه G دارای عضوی از مرتبه‌ی n است.

(ت) اگر گروه G شامل زیرمجموعه‌ی C باشد به طوری که $C^2 = C$ و $e \in C$، آنگاه C زیرگروه G است. یادآوری می‌کنیم که $C^2 = \{xy \mid x, y \in C\}$.

(ث) اگر هر زیرگروه اکید از گروه G متناهی باشد، آنگاه G نیز متناهی است.

۸- فرض کنید $G = \left\{ \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix} \mid n \in \mathbb{Z} \right\}$. نشان دهید که مجموعه‌ی G با عمل ضرب ماتریس‌ها گروهی آبلی است. همچنین، نشان دهید که G دارای عضوی ناهمانی از مرتبه‌ی متناهی نیست.

۹- فرض کنید گروه آبلی G از مرتبه‌ی pq باشد که در آن $(p,q) = 1$. ثابت کنید که اگر G دارای عضوهای a و b، به ترتیب از مرتبه‌های p و q، باشد آنگاه G دوری است.

دسته‌ی دوم

۱۰- گروهی نامتناهی مثال بزنید که مرتبه‌ی هر عضو آن متناهی باشد.

۱۱- فرض کنید که a تنها عضو گروه G باشد که $O(a) = n$. نشان دهید که $a \in Z(G)$.

۱۲- فرض کنید G گروهی از مرتبه‌ی n و m عددی طبیعی باشد به طوری که $(m,n) = 1$. ثابت کنید که برای هر $g \in G$، عضوی مانند $x \in G$ وجود دارد به طوری که $g = x^m$.

۱۳- فرض کنید G گروه است.

(الف) نشان دهید که اگر $a \in G$ و $O(a) = mn$، که در آن $(m,n) = 1$، آنگاه عضوهای $b, c \in G$ وجود دارند به طوری که $O(b) = m$، $O(c) = n$، و $a = bc = cb$.

(ب) تعمیم بند **(الف)** را با $O(a) = m_1 \cdots m_k$ بیان و آن را اثبات کنید.

۱۴- فرض کنید G گروهی از مرتبه‌ی n و m عددی طبیعی باشد به طوری که $(m,n) = 1$. در این صورت،

(الف) ثابت کنید که برای هر $a, b \in G$، اگر $a^m = b^m$ آنگاه $a = b$.

(ب) با ارائه‌ی مثالی نقض، نشان دهید که فرض $(m,n) = 1$ در بند **(الف)** ضروری است.

۱۵- فرض کنید که G گروهی از مرتبه‌ی فرد باشد. ثابت کنید که برای هر $a \in G$، معادله‌ی $x^2 = a$ دقیقاً دارای یک جواب در G است.

۱۶- فرض کنید که گروه آبلی G دارای عضوهایی از مرتبه‌های m و n باشد. نشان دهید که G دارای عضوی از مرتبه‌ی $[m,n]$ است.

۱۷- فرض کنید G گروهی آبلی و H، K دو زیرگروه دوری G باشند به طوری که $|H| = m$ و $|K| = n$. در این صورت،

(الف) نشان دهید که اگر $(m,n) = 1$، آنگاه G زیرگروهی دوری با mn عضو دارد.

(ب) همتای حکم **(الف)** را بدون شرط $(m,n) = 1$ بیان و آن را اثبات کنید.

۱۸- فرض کنید G گروه باشد، $x, y \in G$ و $xy = yx$. نشان دهید که اگر $O(x)$ و $O(y)$ متناهی باشند، آنگاه $O(xy)$ عدد $O(x)O(y)$ را می‌شمارد.

۱۹- فرض کنید G گروه باشد، $x, y \in G$ و $xy = yx$. نشان دهید که اگر $(O(x), O(y)) = 1$ آنگاه $O(xy) = O(x)O(y)$.

۲۰- فرض کنید که $\{e\}$ و G تنها زیرگروه‌های گروه G باشند. نشان دهید که $G = \{e\}$ یا G گروهی دوری از مرتبه‌ی عددی اول است.

۲۱- نشان دهید که اگر تعداد زیرگروه‌های گروه G متناهی باشد، آنگاه G متناهی است.

۲۲- فرض کنید که گروه دوری $G = < a >$ دارای n عضو است. نشان دهید که برای هر عدد طبیعی m، معادله ی $x^m = e$ در G دارای m جواب است اگر و تنها اگر $m \mid n$.

۲۳- فرض کنید G گروهی آبلی و متناهی باشد به طوری که برای هر عدد طبیعی n ، تعداد جواب های معادله‌ی $x^n = e$ حداکثر برابر با n است. ثابت کنید که G دوری است.

۲۴- فرض کنید مرتبه‌ی a در گروه G برابر با ۵ باشد. ثابت کنید که $C_G(a) = C_G(a^2)$.

۲۵- فرض کنید G گروهی متناهی و آبلی است. آیا مجموعه‌ی متشکل از عضو همانی و همه‌ی عضوهای گروه G که از مرتبه‌ی نامتناهی هستند یک زیرگروه از G تشکیل می‌دهد؟

۵.۲ همریختی و یک‌ریختی گروه‌ها

همریختی و یک‌ریختی دستگاه‌های جامع جبری را در بخش ۵.۱ معرفی و ویژگی‌های جامع آن‌ها را بررسی کردیم. دیدیم که، در حالت کلی، همریختی‌ها بین دستگاه‌های جبری توابعی هستند که عمل‌ها را حفظ می‌کنند. از این رو، تعریف زیر را برای مورد خاص گروه‌ها داریم.

۱.۵.۲ تعریف. فرض کنیم که $(G_1;*_{G_1})$ و $(G_2;*_{G_2})$ گروه باشند. در این صورت، تابع $\varphi: G_1 \to G_2$ همریختی گروهی است اگر حافظ عمل باشد، یعنی برای هر $x, y \in G_1$،

$$\varphi(x *_{G_1} y) = \varphi(x) *_{G_2} \varphi(y)$$

همریختی از گروه G به G را **درون‌ریختی**، همریختی یک به یک را **تکریختی**، همریختی پوشا را **بروریختی**، و همریختی دوسویی را **خودریختی** می‌نامیم.

۲.۵.۲ بحث در کلاس

۱- مطابق قراردادهایمان، معمولاً $*$ها را در عبارت بالا حذف می‌کنیم و به صورت ساده‌ی زیر می‌نویسیم و اشتباهی نیز پیش نمی‌آید:

$$\varphi(xy) = \varphi(x)\varphi(y)$$

۲- فرض کنیم که تعریف گروه ۳.۱.۲ را در نظر بگیریم، که در آن گروه را به صورت دستگاه جبری $(G;*,^{-1},e)$ از نوع $\tau = (2,1,0)$ معرفی می‌کند. توجه می‌کنیم که تعریف ۱.۵.۲ صرفاً حفظ عمل دوتایی $*$ را شرط همریختی بودن φ بیان می‌کند. حال این سؤال مطرح می‌شود که چرا حفظ دو عمل دیگر یکانی و صفرتایی را شرط همریختی بودن بین گروه‌ها قرار نداده‌ایم؟ قضیه‌ی ۵.۵.۱ پاسخ به این سؤال است: اتحادهای (گ۱) – (گ۳) به کمک هم آنقدر توانمند هستند که همریختی $\varphi: G_1 \to G_2$ به خودی خود حافظ عضو همانی و وارون‌ها نیز می‌شود! یعنی، $\varphi(e_1) = e_2$ و $\varphi(x^{-1}) = \varphi(x)^{-1}$ (اثبات ساده‌ی آن را یک بار دیگر ارایه دهید). از این رو، می‌توانید نشان دهید که برای هر توان x^k، که در آن k عددی صحیح (مثبت، صفر، یا منفی) است، داریم $\varphi(x^k) = \varphi(x)^k$. این مطلب را بسیار به کار خواهیم برد.

۳- قضیه‌ی مهم ۱۱.۵.۱ و اثبات جالب آن را یادآوری می‌کنیم که برای همه‌ی دستگاه‌های جبری، به ویژه گروه‌ها، بیان می‌کند که برای هر همریختی دوسویی (یعنی یک‌ریختی) $\varphi: G_1 \to G_2$، تابع وارون آن $\varphi^{-1}: G_2 \to G_1$ نیز یک همریختی است. (اثبات ساده ولی جالب آن را یک بار دیگر ارائه دهید.)

۴- روشن است که اگر تابع دوسویی $\varphi : G_1 \to G_2$ بین گروه‌ها، جدول کیلی G_1 را به جدول کیلی G_2 تبدیل کند، آنگاه φ حافظ عمل، و در نتیجه یک‌ریختی است. این مطلب گواه بر درستی بند **۲** بحث **۱۲.۳.۱** است.

۵- مثال‌های همریختی دستگاه‌های جامع جبری را در بخش **۵.۱** دیدیم. در زیر چند مثال مربوط به گروه‌ها را می‌آوریم. مثال‌های بسیاری را به مرور و در حین آموزش نکته‌هایی جدید، خواهیم آورد.

(الف) به آسانی می‌توانید نشان دهید که تابع ثابت $\varphi : G_1 \to G_2$ بین گروه‌ها با تعریف $\varphi(x) = e_2$، برای هر $x \in G_1$، همریختی است. ولی هیچ تابع ثابت دیگر $G_1 \to G_2$ همریختی گروهی نیست. **چرا؟**

(ب) می‌خواهیم ببینیم که چه همریختی‌هایی از گروه جمعی $(\mathbb{Q};+)$ به گروه جمعی $(\mathbb{Z};+)$ وجود دارند؟ روشن است که تابع ثابت صفر، یعنی $\varphi : \mathbb{Q} \to \mathbb{Z}$ با تعریف $\varphi(x) = 0$، همریختی است (زیرا، $\varphi(x+y) = 0 = 0+0 = \varphi(x)+\varphi(y)$). ادعا می‌کنیم که **هیچ همریختی دیگری وجود ندارد!** فرض کنیم $\psi : \mathbb{Q} \to \mathbb{Z}$ یک همریختی باشد. ابتدا نشان می‌دهیم که اگر $\psi(1) = 0$ آنگاه $\psi = 0$. زیرا، اگر $\psi(1) = 0$، آنگاه، چون ψ عمل $+$ در $\mathbb{Q}$ را حفظ می‌کند، برای هر $n \in \mathbb{N}$ داریم

$$0 = \psi(1) = \psi(\frac{n}{n}) = \psi(\frac{1}{n} + \cdots + \frac{1}{n}) = \psi(\frac{1}{n}) + \cdots + \psi(\frac{1}{n})$$

و در نتیجه $\psi(\frac{1}{n}) = 0$ (**چرا؟**). حال برای هر $m, n \in \mathbb{N}$،

$$\psi(\frac{m}{n}) = \psi(\frac{1}{n} + \cdots \frac{1}{n}) = \psi(\frac{1}{n}) + \cdots + \psi(\frac{1}{n}) = 0$$

حال، به آسانی می‌توانید نشان دهید که $\psi = 0$.

بنابراین، اگر همریختی دلخواه ψ ناصفر باشد، آنگاه $\psi(1) = k \neq 0$ و در نتیجه، برای هر عدد طبیعی $n \in \mathbb{N}$،

$$k = \psi(1) = \psi(\frac{n}{n}) = \psi(\frac{1}{n}) + \cdots + \psi(\frac{1}{n}) = n \cdot \psi(\frac{1}{n})$$

یعنی، هر عدد طبیعی n عدد طبیعی k را می‌شمارد، که تناقض است (**چرا؟**) در نتیجه، تنها همریختی از گروه $(\mathbb{Q};+)$ به گروه $(\mathbb{Z};+)$ همریختی بدیهی صفر است! **جالب بود؟!** روشن است که گروه $(\mathbb{Q};+)$ نمی‌تواند با گروه $(\mathbb{Z};+)$ یک‌ریخت باشد، در حالی که در درس مبانی علوم ریاضی دیدیم که **مجموعه**ی $\mathbb{Q}$ با **مجموعه**ی $\mathbb{Z}$ یک‌ریخت (همتوان) است.

(پ) تابع دترمینان از گروه جمعی ماتریس‌های حقیقی $n\times n$ به گروه جمعی $(\mathbb{R};+)$ همریختی نیست، زیرا ماتریس‌های $n\times n$، A و B وجود دارند به طوری که $\det(A+B)\neq \det(A)+\det(B)$.

(ت) تابع دترمینان از گروه ضربی **خطی عام** $GL(n,\mathbb{R})$ (یعنی، ماتریس‌های حقیقی $n\times n$ وارون‌پذیر) به گروه ضربی اعداد حقیقی $(\mathbb{R}^*;\cdot)$، همریختی است. **چرا؟**

حال ببینیم که تاثیر همریختی‌ها بر زیرگروه‌ها چگونه است. بحث **۶.۵.۱** و قضیه‌ی **۸.۵.۱** را مرور کنید.

۳.۵.۲ قضیه. فرض کنیم $\varphi: G_1 \to G_2$ همریختی گروهی باشد. در این صورت،

۱- همریختی φ زیرگروه‌ها را حفظ می‌کند. یعنی،

$$H \leq G_1 \Rightarrow \varphi(H) \leq G_2$$

به ویژه، $\varphi(G_1) \leq G_2$.

۲- همریختی φ زیرگروه‌ها را بازتاب می‌دهد. یعنی،

$$K \leq G_2 \Rightarrow \varphi^{-1}(K) = \tilde{\varphi}(K) \leq G_1$$

به ویژه، $\varphi^{-1}(\{e_{G_2}\}) = \tilde{\varphi}(e_{G_2}) = \{x \in G_1 \mid \varphi(x) = e_{G_2}\} \leq G_1$.

اثبات. مبتدیان گاهی با نگاره‌ی معکوس اندکی مشکل دارند. از این رو، قسمت اول حکم **۲** را اثبات و بقیه‌ی احکام (به ویژه اثبات مستقیم قسمت دوم حکم **۲**) را به عهده‌ی شما خوبان می‌گذاریم. (توجه کنید که، از آنجا که عضوهای $x \in \varphi(H)$ به صورت $x = \varphi(h)$ هستند، که در آن $h \in H$، مبتدیان عضوهای $x \in \varphi^{-1}(K)$ را نیز به اشتباه به صورت $x = \varphi^{-1}(k)$ می‌نویسند، در حالی که باید از این مطلب استفاده کنند که $x \in \varphi^{-1}(K)$ اگر و تنها اگر $\varphi(x) \in K$.)

۲- برای اثبات بسته بودن $\tilde{\varphi}(K)$ نسبت به عمل G_1، فرض می‌کنیم $x, y \in \tilde{\varphi}(K)$، یعنی $\varphi(x), \varphi(y) \in K$. چون φ همریختی است و K نسبت به عمل G_2 بسته است، پس داریم $\varphi(xy) = \varphi(x)\varphi(y) \in K$. در نتیجه، بنابر تعریف $\tilde{\varphi}(K)$، $xy \in \tilde{\varphi}(K)$. برای اثبات $e_{G_1} \in \tilde{\varphi}(K)$، توجه می‌کنیم که $\varphi(e_{G_1}) = e_{G_2} \in K$. در مورد وارون‌ها، فرض می‌کنیم که $x \in \tilde{\varphi}(K)$، یعنی $\varphi(x) \in K$. حال، چون $\varphi(x^{-1}) = \varphi(x)^{-1} \in K$، پس $x^{-1} \in \varphi^{-1}(K)$ و حکم اثبات شده است.

در قسمت پایانی این بخش، دسته‌بندی گروه‌های دوری را که قول داده بودیم انجام می‌دهیم. در اثبات قضیه‌ی زیر و بحث پس از آن فنونی می‌آموزیم که در درس جبرخطی نیز به کار می‌آیند. این فنون را در بخش ۸ از فصل ۱ نیز دیدیم.

۴.۵.۲ قضیه

۱- فرض کنیم $G_1 = < a >$ گروهی دوری و $\varphi : G_1 \to G_2$ همریختی گروهی باشد. در این صورت، $\varphi(G_1)$ نیز گروهی دوری و با مولد $b = \varphi(a)$ است. البته اگر φ پوشا باشد، آنگاه $G_2 = < b >$ نیز دوری است.

۲- فرض کنیم که $G_1 = < a >$ و $\varphi_1, \varphi_2 : G_1 \to G_2$ همریختی باشند به طوری که $\varphi_1(a) = \varphi_2(a)$. در این صورت، $\varphi_1 = \varphi_2$.

اثبات

۱- فرض کنیم $\varphi(x) \in \varphi(G_1)$، که در آن $x \in G_1$. چون $x \in G_1 = < a >$، پس $x = a^n$، که در آن $n \in \mathbb{Z}$. چون φ همریختی است، و در نتیجه عمل دوتایی گروه، عضو همانی، و وارون‌ها را حفظ می‌کند، داریم $\varphi(x) = \varphi(a^n) = \varphi(a)^n = b^n$، و در نتیجه $\varphi(G_1) = < \varphi(a) >$.

۲- روشن است (مراحل زیر را توضیح دهید):

$$\begin{aligned} x \in G_1 = < a > \Rightarrow (\exists k \in \mathbb{Z}) \quad & x = a^k \\ \Rightarrow \varphi_1(x) &= \varphi_1(a^k) = (\varphi_1(a))^k \\ = (\varphi_2(a))^k &= \varphi_2(a^k) = \varphi_2(x) \end{aligned}$$

۵.۵.۲ بحث در کلاس.

نتایج زیر حاصل از قضیه‌ی بالا هستند.

۱- هیچ همریختی پوشا از یک گروه دوری به یک گروه غیر دوری وجود ندارد!

۲- همریختی $\varphi: G \to H$ بین گروه‌های دوری پوشا است اگر و تنها اگر φ **هر** مولد گروه دوری G را بر مولدی از گروه دوری H بنگارد. **چطور؟**

۳- (**جالب است**) همریختی $\varphi: G \to H$ بین گروه‌های دوری پوشا است اگر و تنها اگر φ **دست کم یک** مولد گروه دوری G را بر مولدی از گروه دوری H بنگارد. **چطور؟**

۴- فرض کنیم $|G|=|H|$. در این صورت، هر همریختی پوشای $\varphi: G \to H$ بین گروه‌های دوری دوسویی است.

۵- تنها دو همریختی پوشا از گروه دوری $\mathbb{Z}$ به گروه دوری $\mathbb{Z}$ وجود دارند! **چطور؟** آن دو همریختی را تعریف می‌کنید. (بند **۱** قضیه‌ی بالا و بند **۲** این بحث را ببینید.)

۶- چند همریختی پوشا (و لذا یک‌ریختی) از $\mathbb{Z}_n$ به خودش وجود دارد؟

کیک این بخش را با بیان قضیه‌ی زیر که در ابتدای بخش قول دادیم می‌خوریم. اثبات ساده آن را به عهده‌ی شما می‌گذاریم.

۶.۵.۲ قضیه

۱- اگر گروه دوری $G = < a >$ نامتناهی باشد، آنگاه $G \cong \mathbb{Z}$.

۲- اگر گروه دوری $G = < a >$ متناهی با n عضو باشد، آنگاه $G \cong \mathbb{Z}_n$.

اثبات. تابع با ضابطه‌ی $\varphi(a) = a^n$ را به کار ببرید. اثبات قضیه‌ی **۵.۴.۲** را نیز ببینید.

۷.۵.۲ بحث در کلاس

۱- نشان دهید که گروه‌های $\mathbb{R}$، $\mathbb{R}^*$، $\mathbb{C}$، $\mathbb{C}^*$ دوری نیستند.

۲- گروه‌های دوری جمعی $< \pi > = \{n\pi \mid n \in Z\}$ و ضربی $\{\pi^n \mid n \in Z\}$ با کدام گروه دوری یک‌ریخت هستند؟

۸.۵.۲ بحث در کلاس. این بخش را با مطالب مهم زیر به پایان می‌بریم. **چگونه نشان دهیم که دو گروه یک‌ریخت هستند یا نیستند؟** روشن است که اگر تابعی چون φ از گروه

G_1 به گروه G_2 داده شده باشد و بخواهیم نشان دهیم که φ یک‌ریختی است باید نشان دهیم که دوسویی و همریختی است؛ یعنی، برای هر $x, y \in G_1$

$$\varphi(xy) = \varphi(x)\varphi(y)$$

ولی اگر φ داده نشده باشد چطور آن را پیدا کنیم ؟ این کار اغلب بسیار مشکل است!

فرض کنیم تابع φ داده شده است و می‌خواهیم نشان دهیم که یک‌ریختی بین گروه‌ها نیست. کافی است ثابت کنیم که دارای یکی از شرط‌های یک به یک، پوشا، یا همریختی نیست. گاهی این کار نیز چندان ساده نیست! برای مثال، چطور دو عضو متفاوت $a, b \in G_1$ بیابیم به طوری که $\varphi(a) = \varphi(b)$؟ یا چطور عضوی چون $a \in G_1$ بیابیم که با هیچ عضو متعلق به G_2 توسط φ پوشیده نشود؟ شاید از این هر دو مشکل‌تر این باشد که دو عضو $a, b \in G_1$ بیابیم به طوری که $\varphi(ab) \neq \varphi(a)\varphi(b)$! مشاهده می‌کنیم که حتی اگر تابع φ داده شده باشد، گاهی کار چندان ساده‌ای نیست که نشان دهیم این تابع یک‌ریختی نیست! اغلب رجوع به بحث‌ها و قضیه‌هایی که در بالا آوردیم، یا بعدها در این درس و درس‌های دیگر خواهند آمد، ساده‌تر است. برای مثال، شاید باید ابتدا ببینیم که آیا φ عضو همانی گروه G_1 را به عضو همانی گروه G_2 می‌نگارد یا نه؟

حال فرض کنیم که بخواهیم نشان دهیم که دو گروه G_1 و G_2 یک‌ریخت نیستند. این کار گاهی بسیار مشکل‌تر از حالت‌های بالا است! اگر به گونه‌ای بدانیم که هیچ تابع دوسویی بین دو مجموعه‌ی زمینه‌ی این دو گروه وجود ندارد (مانند وقتی که $|G_1| \neq |G_2|$ ، برای مثال وقتی که G_1 و G_2 متناهی هستند ولی تعداد عضوهای آن‌ها یکسان نیست، یا یکی شمارا و دیگری ناشمارا است) مساله حل است. ولی اگر توابع دوسویی بین دو گروه وجود داشته باشند چطور؟ برای مثال، آیا همه‌ی گروه‌های متناهی n عضوی یک‌ریخت هستند؟ یا آیا گروه‌های جمعی و شمارای $\mathbb{Z}$ و $\mathbb{Q}$ یک‌ریخت هستند؟ گاهی ممکن است، مانند بند **۵(ب)** بحث **۲.۵.۲**، بتوانیم اثبات کنیم که، اگر چه توابع دوسویی بین دو گروه وجود دارند (در این مثال، بین $\mathbb{Z}$ و $\mathbb{Q}$)، ولی هیچ کدام نمی‌تواند **همریختی** باشد!

در این موارد، یک ابزار دیگر این است که به دنبال یک **ویژگی جبری** باشیم که یکی از گروه‌ها داشته باشد ولی دیگری فاقد آن است. نمونه‌هایی از این نوع ویژگی‌ها را در بحث‌ها و قضیه‌های بالا آوردیم و تعدادی را نیز در تمرین‌های زیر، مطالب بخش‌های دیگر، و در درس‌های دیگر می‌آوریم. برای مثال، چون گروه $\mathbb{Z}_4$ دوری است ولی گروه کلاین K_4 دوری نیست، بنابر تمرین **۱** زیر، این دو گروه نمی‌توانند یک‌ریخت باشند. البته، دو گروه ممکن است در یک یا چند ویژگی گروهی شریک باشند، ولی یک‌ریخت نباشند. به هر حال، روشن است که هر چه تعداد بیش‌تری از این نوع ویژگی‌ها در دسترس باشند، در این مورد و موارد دیگر موفق‌تر هستیم.

تمرین ۵.۲

دسته‌ی اول

۱- فرض کنید که دو گروه G_1 و G_2 یک‌ریخت هستند. نشان دهید که **(الف)** G_1 آبلی است اگر و تنها اگر G_2 آبلی باشد. **(ب)** G_1 دوری است اگر و تنها اگر G_2 دوری باشد. **(پ)** هر عضو G_1 وارون خودش است اگر و تنها اگر هر عضو G_2 وارون خودش باشد.

۲- با استفاده از بند **(الف)** تمرین **۱** نشان دهید که دو گروه $\mathbb{Z}_6$ و S_6 یک‌ریخت نیستند.

۳- با استفاده از بند **(ب)** تمرین **۱** نشان دهید که دو گروه $\mathbb{Z}_4$ و K_4 یک‌ریخت نیستند.

۴- تحقیق کنید که از توابع زیر کدام‌ها همریختی روی گروه $(\mathbb{Z};+)$ هستند:

$$f(n)=2n, \qquad g(n)=n+1, \qquad h(n)=n^2$$

۵- نشان دهید که تابع زیر روی گروه G لزوماً همریختی نیست. حدس بزنید که تحت چه شرط لازم و کافی همریختی است:

$$(\forall x\in G)\quad f(x)=x^{-1}$$

۶- فرض کنید $\varphi: G_1 \to G_2$ همریختی گروهی باشد. نشان دهید که،

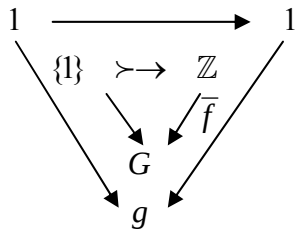
(الف) برای هر $x\in G_1$، اگر $O_{G_1}(x)=n<\infty$، آنگاه $O_{G_2}(\varphi(x)) \mid n$.

(ب) اگر φ یکریختی باشد، آنگاه $O_{G_1}(x)=O_{G_2}(\varphi(x))$.

۷- برای هر عدد صحیح n، تابع $f_n:\mathbb{Z}\to\mathbb{Z}$ را با ضابطه‌ی $f_n(x)=n+x$ در نظر بگیرید. نشان دهید که مجموعه‌ی $\{f_n \mid n\in\mathbb{Z}\}$ همراه با عمل ترکیب توابع یک گروه است و با گروه $(\mathbb{Z};+)$ یک‌ریخت است.

دسته‌ی دوم

۸- ($\mathbb{Z}$ در کلاس گروه‌ها **آزاد** است) فرض کنید G گروهی دلخواه باشد. نشان دهید که برای هر $g\in G$ یک همریختی منحصر به فرد چون $\overline{f}:\mathbb{Z}\to G$ با ویژگی $\overline{f}(1)=g$ وجود دارد. نمودار زیر را ببینید:



نشان دهید که گروه $\mathbb{Z}_n$ در کلاس گروه‌ها آزاد نیست. آیا هیچ گروه متناهی می‌تواند آزاد باشد. بحث **۹.۸.۱** را نیز ببینید.

۹- (تعمیم قضیه‌ی **۴.۵.۲**) فرض کنید که $\varphi : G \to H$ همریختی گروهی باشد و $G = < X >$. نشان دهید که

(الف) $\varphi(G) = < \varphi(X) >$.

(ب) اگر $\varphi_1, \varphi_2 : G \to H$ همریختی باشند به طوری که برای هر $x \in X$، $\varphi_1(x) = \varphi_2(x)$. نشان دهید که $\varphi_1 = \varphi_2$.

۱۰- فرض کنید a عضوی در گروه G است. نشان دهید که تابع زیر خودریختی است (توجه می‌کنیم که، $axya^{-1} = (axa^{-1})(aya^{-1})$):

$$\rho_a : G \to G$$
$$x \mapsto axa^{-1}$$

گاهی می‌نویسیم $x^a = axa^{-1}$. این نوع خودریختی‌ها را **خودریختی درونی** می‌نامیم.

۱۱- فرض کنید $Aut(G)$ و $Inn(G)$، به ترتیب، مجموعه‌ی خودریختی‌ها و مجموعه‌ی خودریختی‌های درونی G باشند. نشان دهید که این دو مجموعه، همراه با ترکیب توابع، گروه تشکیل می‌دهند.

۱۲- فرض کنید G گروهی متناهی و $\varphi : G \to H$ همریختی پوشا باشد. ثابت کنید که مرتبه‌ی H مرتبه‌ی G را می‌شمارد.

۱۳- فرض کنید G گروهی آبلی از مرتبه‌ی عددی فرد و $\psi : G \to G$ یک خودریختی از مرتبه‌ی۲ باشد (یعنی، $\psi \circ \psi = id_G$). ثابت کنید که هر عضو $g \in G$ را می‌توان به طور یکتا به صورت $g = xy$ نوشت، که در آن $\psi(x) = x$ و $\psi(y) = y^{-1}$.

۱۴- فرض کنید G گروهی دلخواه باشد. ثابت کنید که برای هر $\psi_a, \psi_b \in Inn(G)$، که در آن $a, b \in G$، تساوی $\psi_a = \psi_b$ برقرار است اگر و تنها اگر $ab^{-1} \in Z(G)$.

۱۵- فرض کنید که $(G;*_G)$ گروهی دلخواه و $(A;*_A)$ گروهی آبلی است. مجموعه‌ی همه‌ی همریختی‌های از G به A را با $Hom(G,A)$ نشان می‌دهیم. ثابت کنید که $Hom(G,A)$ همراه با عمل

$$(fg)(x) = f(x) *_A g(x)$$

برای $f, g \in Hom(G,A)$، گروهی آبلی است و $Hom(\mathbb{Z}, A) \cong A$.

۱۶- فرض کنید $G = \{x \in \mathbb{R} \mid x^2 < 1\}$. نشان دهید که مجموعه‌ی G همراه با عمل

$$x * y = \frac{x+y}{1+xy}$$

گروهی آبلی، و با گروه جمعی $(\mathbb{R};+)$ یک‌ریخت، است. (از تابع $f : G \to \mathbb{R}$ با ضابطه‌ی $f(x) = Ln\left(\frac{1+x}{1-x}\right)$ استفاده کنید).

۱۷- فرض کنید S مجموعه‌ی ماتریس‌های 2×2 حقیقی مانند X باشد به طوری که $X + I$ وارون‌پذیر است (که در آن I ماتریس همانی است) نشان دهید که S همراه با عمل

$$A * B = A + B + AB \qquad (A, B \in S)$$

گروه تشکیل می‌دهد. سپس، ثابت کنید که گروه S با گروه ضربی همه‌ی ماتریس‌های حقیقی 2×2 وارون‌پذیر یک‌ریخت است.

۱۸- فرض کنید که دو گروه G و H یک‌ریخت هستند. ثابت کنید که $Aut(G) \cong Aut(H)$. آیا عکس این مطلب درست است؟ **چرا؟**

۱۹- فرض کنید G گروهی با مرکز بدیهی است. ثابت کنید که $C_{Aut(G)}(Inn(G)) = \{id_G\}$. نتیجه بگیرید که $Z(Aut(G)) = \{id_G\}$.

۶.۲ گروه جایگشت‌ها

همان طور که در بحث ۴.۱.۲(چ) دیدیم، روشن است که مجموعه‌ی S_X متشکل از همه‌ی توابع دوسویی روی X همراه با عمل ترکیب توابع، گروه تشکیل می‌دهد. این گروه و هر زیرگروه آن را گروهی از جایگشت‌های روی X نامیدیم. همچنین، اگر $X=\{1,2,\cdots,n\}$، آنگاه S_X را با S_n نشان دادیم و آن را **گروه جایگشت‌های** روی n شیء یا **گروه متقارن** درجه‌ی n نامیدیم. این گروه‌ها حتی قبل از معرفی مفهوم مجرد گروه به کار می‌رفتند. ریاضی‌دانانی از جمله لاگرانژ، کشی، آبل، و از همه مهم‌تر، گالوا در جستجوی جواب‌های معادله‌های چندجمله‌ای، جایگشت‌ها را به کمک گرفتند و به نتایج مفیدی دست پیدا کردند. مطالعه‌ی عمیق این مطالب، نظریه‌ی گالوا را به وجود آورد که خود کتاب‌های مفصل دیگری را می‌طلبد.

این تلاش‌ها منجر به معرفی و پرورش نظریه‌ی مجرد گروه‌ها شد. ریاضی‌دان انگلیسی، آرتور کیلی، جنبه‌ی دیگری از اهمیت گروه‌های جایگشت‌ها را به نمایش می‌گذارد و نشان می‌دهد که هر گروه مجرد G (متناهی یا نامتناهی) با گروهی از جایگشت‌ها یکریخت است! **خیلی جالب است، نیست؟** این قضیه را در این بخش اثبات می‌کنیم. با توجه به این سابقه‌ی تاریخی و به دلیل کاربردهای بسیارگروه جایگشت‌ها (برای مثال، در ترکیبیات) به حق است که یک بخش هر چند کوتاه را به مطالعه‌ی آن‌ها اختصاص دهیم. البته به دلیل کمبود وقت، برخی از قضیه‌ها را اثبات نمی‌کنیم.

۱.۶.۲ بحث در کلاس

۱- ابتدا، برای راحتی کار محاسبات، نمادگذاری زیر را به کار می‌بریم. هر جایگشت $\sigma \in S_n$ را می‌توانیم با نماد دوخطی زیر نشان دهیم:

$$\sigma=\begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \cdots & \sigma(n) \end{pmatrix}$$

جایگشت همانی را به طور ساده با $\rho_\circ=(1)$ نشان می‌دهیم. پس

$$id_X=\rho_\circ=(1)=\begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ 1 & 2 & 3 & \cdots & n \end{pmatrix}$$

توجه می‌کنیم که، چون هر جایگشت σ دوسویی است، پس هر عضو $\{1,2,\cdots,n\}$ در سطر دوم نمایش دوخطی σ نیز یک و تنها یک بار رخ می‌دهد.

۲- برای محاسبه‌ی σ^{-1} کافی است ابتدا جای دو سطر σ را با هم عوض کنیم و سپس ستون‌ها را طوری مرتب کنیم که سطر اول به صورت متعارف از ۱ تا n نوشته شود. برای مثال،

$$\begin{pmatrix}1&2&3&4&5\\2&4&5&1&3\end{pmatrix}^{-1}=\begin{pmatrix}2&4&5&1&3\\1&2&3&4&5\end{pmatrix}$$
$$=\begin{pmatrix}1&2&3&4&5\\4&1&5&2&3\end{pmatrix}$$

۳- روشن است که حاصل‌ضرب (یعنی ترکیب) دو جایگشت $\sigma,\delta\in S_n$ در نمادگذاری متداول ترکیب توابع به صورت $(\sigma\circ\delta)(x)=\sigma(\delta(x))$ تعریف می‌شود، یعنی ابتدا تابع سمت راست یعنی δ بر x اثر و سپس σ بر حاصل $\delta(x)$ اثر می‌کند. برای مثال، داریم

$$\sigma\circ\delta=\begin{pmatrix}1&2&3&4&5\\2&4&5&1&3\end{pmatrix}\begin{pmatrix}1&2&3&4&5\\3&5&1&2&4\end{pmatrix}$$
$$=\begin{pmatrix}1&2&3&4&5\\\downarrow&\downarrow&\downarrow&\downarrow&\downarrow\\3&5&1&2&4\\\downarrow&\downarrow&\downarrow&\downarrow&\downarrow\\5&3&2&4&1\end{pmatrix}=\begin{pmatrix}1&2&3&4&5\\5&3&2&4&1\end{pmatrix}$$

زیرا، برای مثال، داریم $(\sigma\circ\delta)(1)=\sigma(\delta(1))=\sigma(3)=5$ و $(\sigma\circ\delta)(2)=\sigma(\delta(2))=\sigma(5)=3$. توجه می‌کنیم که در این نمادگذاری، پرانتزها را از پرانتز سمت راست به پرانتز سمت چپ به کار می‌بریم. برخی از ریاضی‌دانان نمادگذاری $x(\sigma\circ\delta)=(x\sigma)\delta$ را به کار می‌برند، که در این صورت در نمادگذاری حاصل‌ضرب جایگشت‌ها، پرانتزها، به ترتیب طبیعی‌تر، از چپ به راست به کار می‌روند.

۴- روشن است که $|S_n|=n!$. شش عضو گروه S_3 عبارت هستند از

$$\rho_\circ=\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix},\quad \rho_1=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix},\quad \rho_2=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$$

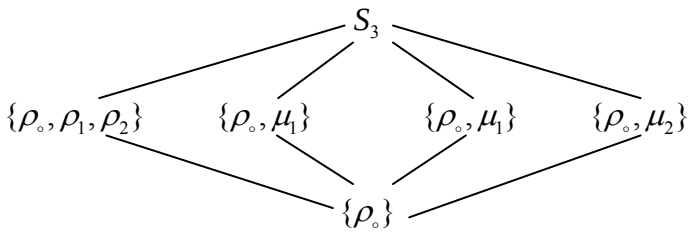
$$\mu_1=\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix},\quad \mu_2=\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix},\quad \mu_3=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}$$

با محاسبه می‌توانید نشان دهید که جدول گروه S_3 به صورت زیر است:

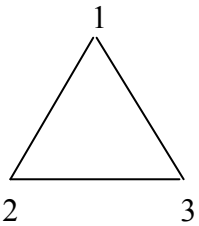
$\circ$	$\rho_\circ$	ρ_1	ρ_2	μ_1	μ_2	μ_3
$\rho_\circ$	$\rho_\circ$	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_1	ρ_1	ρ_2	$\rho_\circ$	μ_3	μ_1	μ_2
ρ_2	ρ_2	$\rho_\circ$	ρ_1	μ_2	μ_3	μ_1
μ_1	μ_1	μ_2	μ_3	$\rho_\circ$	ρ_1	ρ_2
μ_2	μ_2	μ_3	μ_1	ρ_2	$\rho_\circ$	ρ_1
μ_3	μ_3	μ_1	μ_2	ρ_1	ρ_2	$\rho_\circ$

۵- نشان دهید که اگر $n \geq 3$، آنگاه برای هر $\sigma \in S_n$ دست کم یک $\delta \in S_n$ وجود دارد به طوری که $\sigma\delta \neq \delta\sigma$. به عبارت دیگر، نه تنها برای $n \geq 3$، S_n آبلی نیست، بلکه مرکز آن بسیار کوچک و در واقع برابر است با $Z(S_n) = \{\rho_\circ\}$ و در نتیجه فاصله‌ی زیادی با آبلی بودن دارد. یادآوری می‌کنیم که گروه G آبلی است اگر و تنها اگر $Z(G) = G$.

۶- با توجه به قضیه‌ی لاگرانژ، S_3 تنها می‌تواند زیرگروه‌هایی ۱، ۲، ۳، و ۶ عضوی داشته باشد، که اتفاقاً دارد. با مراجعه به جدول کیلی گروه S_3، و البته با کمی محاسبه، می‌توانید مشبکه‌ی زیرگروه‌های آن را به صورت زیر به دست آورید:



۷- چرا گروه جایگشت‌ها را گروه تقارن‌ها یا گروه متقارن نیز می‌نامند؟ مثلث سه ضلع مساوی زیر را در نظر بگیرید:



روشن است که این مثلث را می‌توان با سه دوران (نسبت به مرکز مثلث) و سه انعکاس نسبت به سه نیمساز زاویه‌ها (همان عمود منصف‌های اضلاع) بر خودش منطبق کرد. این شش دوران و

انعکاس را تقارن‌های مثلث می‌نامند. با شماره‌گذاری ۱، ۲، ۳ راس‌ها، سه دوران را می‌توان با ρ_0، ρ_1، ρ_2 و سه انعکاس را با μ_1، μ_2، و μ_3 نشان داد. همچنین، می‌توان نشان داد که این تقارن‌ها، نسبت به ترکیب، گروه S_3 را تشکیل می‌دهند.

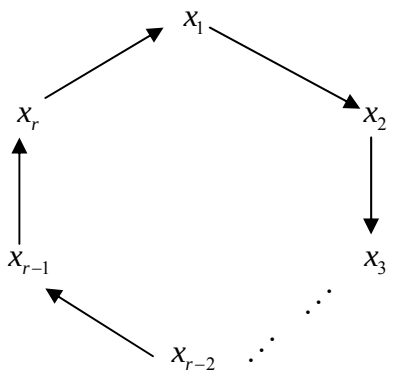
۷- حال گروه تقارن‌های مربع را محاسبه می‌کنیم. توجه می‌کنیم که مربع را می‌توان با چهار دوران (نسبت به مرکز مربع) و دو انعکاس نسبت به دو نیمساز زاویه‌ها و دو انعکاس نسبت به دو عمود منصف اضلاع بر خودش منطبق کرد. مانند مورد مثلث، با شماره‌گذاری ۱، ۲، ۳، ۴ راس‌های مربع، گروه تقارن‌های مربع را می‌توان زیرگروهی $4+4=2\times 4=8$ از گروه S_4 در نظر گرفت.

به طور کلی، هر n- ضلعی منتظم دارای $2n$ تقارن است (n دوران، و n انعکاس نسبت به عمود منصف‌ها و نسبت به نیمسازها) که، تحت ترکیب، زیرگروهی از S_n تشکیل می‌دهند. این گروه $2n$ عضوی را با D_n نشان می‌دهیم و آن را **گروه دو وجهی** مرتبه‌ی $2n$ (یا nامین گروه دو وجهی) می‌نامیم.

۲.۶.۲ تعریف. جایگشت σ روی مجموعه‌ی X را **جایگشت دوری** به طول r، یا یک r-**دور**، می‌نامیم اگر $x_1,\cdots,x_r\in X$ وجود داشته باشند به طوری که

$$\sigma(x_1)=x_2,\quad \sigma(x_2)=x_3,\quad \cdots\quad ,\quad \sigma(x_{r-1})=x_r,\quad \sigma(x_r)=x_1$$

و هر $x\notin\{x_1,\cdots,x_r\}$ تحت σ ثابت بماند، یعنی $\sigma(x)=x$:



معمولاً جایگشت دوری را به صورت ساده‌ی یک خطی $\sigma=(x_1,x_2,\cdots,x_r)$ نشان می‌دهیم. برای مثال، روشن است که

$$\begin{aligned}(x_1, x_2, \cdots, x_r) &= (x_2, x_3, x_4, \cdots, x_1)\\ &= (x_3, x_4, \cdots, x_1, x_2)\\ &= \cdots\\ &= (x_r, x_1, x_2, \cdots, x_{r-1})\end{aligned}$$

برای مثال،

$$\begin{pmatrix}1 & 2 & 3 & 4 & 5\\ 1 & 4 & 3 & 5 & 2\end{pmatrix} = (2,4,5) = (4,5,2) = (5,2,4)$$

۳.۶.۲ بحث در کلاس

۱- توجه می‌کنیم که اعدادی که در نمادگذاری یک خطی جایگشت دوری $\sigma \in S_n$ ظاهر نمی‌شوند، تحت σ ثابت می‌مانند. برای مثال $\rho_\circ = (1) = (2) = \cdots = (n)$، و در S_5،

$$\sigma = (1,3,4) = \begin{pmatrix}1 & 2 & 3 & 4 & 5\\ 3 & 2 & 4 & 3 & 5\end{pmatrix}$$

یک جایگشت دوری به طول ۳ یعنی یک ۳- دور است که در آن ۲ و ۵ ثابت هستند. هر ۲- دور (a,b) را یک **ترانهش** می‌نامیم.

۲- مطلبی بسیار مهم (مشابه نوشتن اعداد طبیعی $n \geq 2$ به صورت حاصلضرب اعداد اول)، که می‌خواهیم به مرور در بندهای زیر نشان دهیم، این است که برای $n \geq 2$، **هر جایگشت $\sigma \in S_n$ را می‌توان به صورت حاصلضرب ترانهش‌ها نوشت.** ابتدا هر جایگشت

$$\sigma = \begin{pmatrix}1 & 2 & \cdots & n\\ \sigma(1) & \sigma(2) & \cdots & \sigma(n)\end{pmatrix}$$

را در مرحله‌های زیر به صورت حاصلضرب دورها می‌نویسیم.

(الف) جایگشت دوری $\delta_1 = (1, \sigma(1), \sigma(\sigma(1)), \cdots, 1)$ را تشکیل می‌دهیم.

(ب) کوچکترین عدد x را با شرط

$$x \in \{1,2,\cdots,n\} \setminus \{1, \sigma(1), \sigma(\sigma(1)), \cdots\}$$

در نظر بگیرید و جایگشت دوری $\delta_2 = (x, \sigma(x), \sigma(\sigma(x)), \cdots)$ را تشکیل دهید.

(پ) کوچکترین عدد y را با شرط

$$y \in \{1,2,\cdots,n\} \setminus \{1,\sigma(1),\sigma(\sigma(1)),\cdots,x,\sigma(x),\sigma(\sigma(x)),\cdots\}$$

در نظر بگیرید و با ادامه‌ی این روند، به نتیجه‌ی مطلوب $\sigma = \delta_k \cdots \delta_2 \delta_1$ می‌رسیم. برای مثال،

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 3 & 2 & 1 & 4 & 8 & 7 & 6 \end{pmatrix} = \begin{pmatrix} . & 2 & 3 & . & . & 6 & 7 & 8 \\ . & 3 & 2 & . & . & 8 & 7 & 6 \end{pmatrix}(1,5,4)$$
$$= \begin{pmatrix} . & . & . & . & . & 6 & 7 & 8 \\ . & . & . & . & . & 8 & 7 & 6 \end{pmatrix}(2,3)(1,5,4)$$
$$= \begin{pmatrix} . & . & . & . & . & . & 7 & . \\ & & & & & & & \\ . & . & . & . & . & . & 7 & . \end{pmatrix}(6,8)(2,3)(1,5,4)$$
$$= (7)\,(6,8)(2,3)(1,5,4)$$
$$= (6,8)(2,3)(1,5,4)$$

۳- هر r- دور با $r \geq 2$ را می‌توان به حاصل‌ضرب ترانهش‌ها نوشت. زیرا، به آسانی می‌توانید با محاسبه‌ی مستقیم ترکیب جایگشت‌ها (ضرب از راست به چپ پرانتزها) نشان دهید که

$$(x_1, x_2, \cdots, x_r) = (x_1, x_r)(x_1, x_{r-1}) \cdots (x_1, x_2)$$

برای مثال، $\rho_\circ = (1,2)(2,1) = (5,6)(6,5) = \cdots$. به طور کلی $\rho_\circ = (a,b)(b,a)$. به عنوان مثالی دیگر، در S_4 داریم

$$(1,2,3) = (1,3)(1,2) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix}$$
$$= \begin{pmatrix} 1 & 2 & 3 & 4 \\ \downarrow & \downarrow & \downarrow & \downarrow \\ 2 & 1 & 3 & 4 \\ \downarrow & \downarrow & \downarrow & \downarrow \\ 2 & 3 & 1 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix} = (1,2,3)$$

۴- با توجه به بندهای ۳ و ۴، برای $n \geq 2$، **هر جایگشت** $\sigma \in S_n$ **را می‌توان به صورت حاصل‌ضرب ترانهش‌ها نوشت.** برای مثال،

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 3 & 2 & 1 & 4 & 8 & 7 & 6 \end{pmatrix} = (7)(6,8)(2,3)(1,5,4)$$
$$= (6,8)(2,3)(1,5,4)$$
$$= (6,8)(2,3)(1,4)(1,5)$$

۵- همان طور که گفتیم و در مثال $\rho_\circ = (1,2)(2,1) = (5,6)(6,5) = \cdots$ نیز دیدیم، تجزیه‌ی جایگشت‌ها به حاصل‌ضرب ترانهش‌ها یکتا نیست. برای مثالی دیگر، می‌توانید به روش بالا نشان دهید که در S_4،

$$(1,2,3) = (1,3)(1,2) = (2,1)(2,3) = (2,1)(2,3)(1,2)(2,1) = \cdots$$

نکته‌ی جالب این است که به هر صورتی که جایگشتی را به ترانهش‌ها تجزیه کنیم، تعداد ترانهش‌ها **همواره زوج یا همواره فرد است** (اثبات رسمی این مطلب را نمی‌آوریم). از این رو، تعریف زیر را داریم.

۴.۶.۲ تعریف. اگر $\sigma \in S_n$ به حاصل‌ضرب تعدادی زوج ترانهش نوشته شود، آن را **زوج** و در غیر این صورت **فرد** می‌نامیم.

۵.۶.۲ بحث در کلاس

۱- چون $(x_1, x_2, \cdots, x_r) = (x_1, x_r)(x_1, x_{r-1}) \cdots (x_1, x_2)$، روشن است که هر r - دور زوج است اگر و تنها اگر r فرد باشد.

۲- جایگشت همانی زوج است، زیرا اگر $n = 1$ آنگاه $\rho_\circ$ به تعداد صفر ترانهش دارد و اگر $n \geq 2$ آنگاه $\rho_\circ = (1,2)(2,1)$. همچنین، به راحتی می‌توانید نشان دهید که حاصل‌ضرب دو جایگشت، فرد است اگر و تنها اگر دقیقاً یکی از آن‌ها فرد باشد، وارون هر ترانهش $\tau = (a,b)$ برابر با خودش است، وارون هر جایگشت σ زوج است اگر و تنها اگر σ زوج باشد. زیرا اگر $\sigma = \tau_k \cdots \tau_2 \tau_1$ حاصل ضرب تعدادی ترانهش باشد، آنگاه

$$\sigma^{-1} = (\tau_k \cdots \tau_2 \tau_1)^{-1} = \tau_1^{-1} \tau_2^{-1} \cdots \tau_k^{-1} = \tau_1 \tau_2 \cdots \tau_k$$

حال اگر A_n مجموعه‌ی جایگشت‌های زوج و B_n مجموعه‌ی جایگشت‌های فرد در S_n باشند، آنگاه B_n زیرگروه S_n نیست در حالی که A_n زیرگروه S_n است. حال قضیه‌ی زیر را ببینید.

۶.۶.۲ قضیه. برای $n \geq 2$، $|A_n| = |B_n|$.

اثبات. کافی است تابعی دوسویی چون $\varphi : A_n \to B_n$ تعریف کنیم. چون $n \geq 2$، ترانهش τ وجود دارد. حال φ را به صورت زیر تعریف می‌کنیم:

$$\begin{aligned} \varphi : A_n &\to B_n \\ \sigma &\mapsto \sigma\tau \end{aligned}$$

توجه می‌کنیم که، چون σ زوج است، $\sigma\tau$ فرد است. همچنین،

$$\begin{aligned} \varphi(\sigma_1) = \varphi(\sigma_2) &\Leftrightarrow \sigma_1\tau = \sigma_2\tau \\ &\Leftrightarrow \sigma_1\tau\tau^{-1} = \sigma_2\tau\tau^{-1} \\ &\Leftrightarrow \sigma_1 = \sigma_2 \end{aligned}$$

پس، φ خوش تعریف و یک به یک است. اثبات ساده و جالب پوشا بودن φ را به عهده‌ی شما می‌گذاریم.

۷.۶.۲ بحث در کلاس

۱- با توجه به قضیه‌ی بالا، $|A_n| = \frac{1}{2}n!$.

۲-گروه مهم A_n را **گروه متناوب** درجه‌ی n می‌نامیم.

۳- روشن است که $A_3 = \{\rho_0, \rho_1, \rho_2\}$.

بیش از این به ویژگی‌های جایگشت‌ها در این درس نمی‌پردازیم. ولی، در پاراگراف دوم مقدمه‌ی این بخش، قول دادیم که قضیه‌ی کیلی را اثبات کنیم. روشن است که نمایش یک شیء ریاضی با شیء ریاضی دیگری که کار کردن با آن ساده‌تر باشد یا برنامه‌های رایانه‌ای را نیز بتوان برای آن به کار برد، بسیار مفید است. قضیه‌ی کیلی، هر گروه را با گروهی از جایگشت‌ها **نمایش** می‌دهد که در کاربردها بسیار مفید است.

۸.۶.۲ قضیه هر گروه (متناهی یا نامتناهی) G با گروهی از جایگشت‌ها یکریخت است.

اثبات. یقیناً از این قضیه تعجب نخواهید کرد، زیرا در هر سطر جدول کیلی گروه G، هر عضو یک و تنها یک بار رخ می‌دهد. یعنی، هر سطر چیزی جز جایگشتی از عضوهای G نیست. حال خلاصه‌ای از اثبات را می‌آوریم. برای هر $a \in G$، تابع انتقال چپ

$$\begin{aligned} l_a : G &\to G \\ x &\mapsto ax \end{aligned}$$

را در نظر می‌گیریم. همان طور که در تمرین‌های **۱۴** و **۱۵** از بخش **۱.۲** دیدیم، به راحتی می‌توانید نشان دهید که هر l_a یک جایگشت (دوسویی) است و $G_l = \{l_a \mid a \in G\}$ همراه با ترکیب توابع گروه است. توجه می‌کنیم که l_e عضو همانی این گروه است، و $l_a \circ l_b = l_{ab}$. زیرا

$$(l_a \circ l_b)(x) = l_a(l_b(x)) = l_a(bx) = a(bx) = (ab)x = l_{ab}(x)$$

و $(l_a)^{-1} = l_{a^{-1}}$. حال نشان می‌دهیم که تابع

$$\begin{aligned} \varphi : G &\to G_l \\ a &\mapsto l_a \end{aligned}$$

یک‌ریختی گروهی است. اثبات زیر را برای یک به یک بودن φ توضیح دهید:

$$\begin{aligned} \varphi(a) = \varphi(b) \Rightarrow l_a = l_b &\Rightarrow (\forall x \in G)\, l_a(x) = l_b(x) \\ &\Rightarrow l_a(e) = l_b(e) \Rightarrow ae = be \Rightarrow a = b \end{aligned}$$

پوشا بودن روشن است. **چطور؟** حال اثبات همریختی بودن را توضیح دهید:

$$\varphi(ab) = l_{ab} = l_a \circ l_b = \varphi(a) \circ \varphi(b)$$

۹.۶.۲ بحث در کلاس

۱- به روشی مشابه اثبات قضیه‌ی کیلی، می‌توان نشان داد که گروه G با گروه انتقال‌های راست $G_r = \{r_a \mid a \in G\}$ نیز یک‌ریخت است. (اثبات کنید، جالب است). گروه‌های G_r و G_l را، به ترتیب، **نمایش منظم راست** و **چپ** گروه G می‌نامیم. روشن است که اگر G آبلی باشد، $G_r = G_l$.

۲- هر گروه از مرتبه‌ی n با زیرگروهی از S_n یک‌ریخت است.

۳- برای نمونه، جایگشت‌های نمایش منظم گروه $\mathbb{Z}_4$ را بیابید. برای مثال، تابع انتقال راست r_2 هر عضو گروه $\mathbb{Z}_4$ را به اندازه‌ی ۲ انتقال می‌دهد:

$$\varphi(2) = r_2 = \begin{pmatrix} \circ & 1 & 2 & 3 \\ 2 & 3 & \circ & 1 \end{pmatrix}$$

۴- با توجه به بند **۲** و متناهی بودن تعداد زیرگروه‌های S_n، برای هر عدد طبیعی n تنها تعدادی متناهی رده‌ی یک‌ریختی از گروه‌های n عضوی وجود دارند.

تمرین ۶.۲

رفته رفته تبحر شما بیش‌تر می‌شود

دسته‌ی اول

۱- با یک مثال نشان دهید که حاصل‌ضرب دو جایگشت دوری لزوماً دوری نیست.

۲- دو جایگشت دوری $\sigma = (x_1, \cdots, x_r)$ و $\delta = (y_1, \cdots, y_s)$ را **مجزا** می‌گوییم اگر $\{x_1, \cdots, x_r\} \cap \{y_1, \cdots, y_s\} = \varnothing$. برای مثال، در S_6، $(1,2)$ و $(3,4,5)$ مجزا هستند. نشان دهید که عمل ترکیب (ضرب) روی جایگشت‌های دوری مجزا تعویض‌پذیر است.

۳- فرض کنید که $\sigma, \delta \in S_n$ دو جایگشت دوری مجزا باشند. نشان دهید که

(الف) مرتبه‌ی هر جایگشت دوری برابر با طول آن است.

(ب) نشان دهیدکه $O(\sigma\delta) = [O(\sigma), O(\delta)]$.

(پ) ابتدا جایگشت زیر را به حاصل‌ضرب دورهای مجزا بنویسید و سپس، با استفاده از بندهای **(الف)** و **(ب)**، مرتبه‌ی آن را بیابید:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 4 & 1 & 6 & 7 & 5 & 8 & 2 \end{pmatrix}$$

(ت) جایگشت‌های σ^{60} و σ^{62} را مشخص کنید.

۴- فرض کنید که

$$\sigma=\begin{pmatrix}1&2&3&4&5&6\\5&4&3&2&1&6\end{pmatrix}\quad,\quad \delta=\begin{pmatrix}1&2&3&4&5&6\\5&4&3&2&1&6\end{pmatrix}$$

حاصل ضرب‌های $\sigma\delta$، $\delta\sigma$، σ^{-1}، $\sigma^{-1}\delta^{-1}$، $\sigma^{100}\delta^{-61}$ را بیابید.

۵- جایگشت‌های σ و δ تمرین ۴ را به جایگشت‌های دوری و به ترانهش‌ها تجزیه و سپس زوج یا فرد بودن آن‌ها را مشخص کنید.

۶- فرض کنید که $Y\subseteq X$ و $y\in Y$ ثابت باشد. تعیین کنید که از مجموعه‌های زیر کدام(ها) زیرگروه S_X هستند:

(الف) $A=\{\sigma\in S_X\mid \sigma(y)=y\}$ (ب) $B=\{\sigma\in S_X\mid \sigma(y)\in Y\}$

(پ) $C=\{\sigma\in S_X\mid \sigma(Y)\subseteq Y\}$ (ت) $D=\{\sigma\in S_X\mid \sigma(Y)=Y\}$

دسته‌ی دوم

۷- ثابت کنید که $Aut(S_3)\cong Inn(S_3)\cong S_3$.

۸- فرض کنید $\sigma=(k_1,\cdots,k_r)$ جایگشتی دوری در گروه S_n باشد. ثابت کنید که برای هر $\delta\in S_n$، $\delta^{-1}\sigma\delta=(\delta(k_1),\ldots,\delta(k_r))$.

۹- فرض کنید $H\le S_n$. نشان دهید که همه یا دقیقاً نیمی از جایگشت‌های متعلق به H زوج هستند.

۱۰- ثابت کنید که برای $n>3$، هر عضو A_n را می توان به صورت حاصل‌ضرب دورهای به طول ۳ نوشت. (توجه کنید که $(ab)(cd)=(cbc)(cdc)$).

۱۱- فرض کنید که جایگشت σ یک دور از مرتبه‌ی فرد است. ثابت کنید که σ^2 نیز یک دور است.

۱۲- فرض کنید H و K دو زیرگروه از مرتبه‌ی ۱۵ در گروه متقارن S_8 باشند به طوری که $H\cap K=\{e\}$. نشان دهید که $HK\neq KH$.

۱۳- فرض کنید که برای $n > 2$، گروه S_n دارای زیرگروه نابدیهی H باشد. ثابت کنید که $H \cap A_n \neq \{e\}$.

۷.۲ ضرب و همضرب گروه‌ها

در فصل ۱ چند روش ساختن دستگاه‌های جبری جدید را از دستگاه‌های جبری داده شده معرفی کردیم. یکی از این روش‌ها به گونه‌ای متصل کردن دستگاه‌ها به یکدیگر است. به صورت‌های متعدد می‌توان این کار را انجام داد، که یکی از آن‌ها ساختن حاصل‌ضرب دکارتی است که در بخش ۶.۱ معرفی شد. در این بخش این مفهوم و مفهوم هم‌ضرب را برای گروه‌ها با جزییات بیشتری مطالعه می‌کنیم.

علاوه بر ساختن گروه‌های جدید، مفهوم ضرب را می‌توان برای کسب اطلاعات در باره‌ی یک گروه نیز به کار برد. همان طور که تجزیه‌ی اعداد به اعداد اول، یا تجزیه‌ی جایگشت‌ها به جایگشت‌های ساده‌تر دوری یا ترانهش‌ها اطلاعات خوبی به دست می‌دهد، نوشتن یک گروه به حاصل‌ضرب گروه‌های کوچک‌تر، و به تعبیری ساده‌تر، اطلاعات مفیدی در باره‌ی خود گروه به دست می‌دهد.

حال تعریف ضرب داده شده در بخش ۶.۱ را برای گروه‌ها یادآوری می‌کنیم.

۱.۷.۲ قضیه و تعریف. فرض کنیم G_1 و G_2 گروه باشند. در این صورت $G_1 \times G_2$ همراه با عمل دوتایی **مولفه‌ای**

$$(g_1, g_2)(g_1', g_2') = (g_1 g_1', g_2 g_2')$$

یک گروه تشکیل می‌دهد. این گروه را **حاصل‌ضرب (دکارتی)** G_1 در G_2 می‌نامیم.

۲.۷.۲ بحث در کلاس

۱- تعمیم تعریف بالا به هر تعداد متناهی و نامتناهی گروه روشن است. معمولاً نمادهای زیر به کار می‌روند:

$$\prod_{i=1}^{n} G_i = G_1 \times G_2 \times \cdots G_n$$
$$\prod_{i\in I} G_i = \{f : I \to \bigcup_{i\in I} G_i \mid (\forall i \in I)\ f(i) \in G_i\}$$
$$\cong \{(g_i)_{i\in I} \mid (\forall i \in I) \quad g_i \in G_i\}$$

۲- توجه می‌کنیم که در تعریف **۱.۷.۲** بالا، عمل‌های گروه‌ها را، که ممکن است با هم متفاوت باشند، ننوشته‌ایم و معمولاً اشتباهی رخ نمی‌دهد. البته در مثال‌های مشخص، عمل‌ها را همان طور که داده شده‌اند می‌نویسیم و اجرا می‌کنیم. برای مثال، در $\mathbb{Z}_2 \times \mathbb{Z}_3$ می‌نویسیم

$$(g_1, g_2)(g_1', g_2') = (g_1 +_2 g_1', g_2 +_3 g_2')$$
$$(1,1)(1,1) = (1 +_2 1, 1 +_3 1) = (0,2)$$

۳- دلیل استفاده از پسوند **دکارتی**، یکی تعریف حاصل‌ضرب دکارتی مجموعه‌ای

$$G_1 \times G_2 = \{(g_1, g_2) \mid g_1 \in G_1, g_2 \in G_2\}$$

و دیگری این است که گروه $G_1 \times G_2$ در ویژگی جهانی ضرب، قضیه‌ی **م. ۴.۱** صدق می‌کند. البته گاهی واژه‌ی **حاصل‌ضرب مستقیم برونی** یا **خارجی** را نیز به کار می‌برند، زیرا G_iها زیرگروه حاصل‌ضرب نیستند، و نسبت به آن **خارجی**‌اند. در این مورد بعداً بیش‌تر صحبت می‌کنیم.

۴- همان طور که در بند ۳ بحث **۲۳.۶.۱** دیدیم، گروه $G_1 \times G_2$ ممکن است برخی از ویژگی‌های مولفه‌هایش G_1 و G_2 را به ارث نبرد! در همان بحث گفتیم که اگر G_1 و G_2 دارای ویژگی معادله‌ای (**اتحاد**) σ باشند، آنگاه $G_1 \times G_2$ نیز در آن ویژگی صدق می‌کند. برای مثال، $G_1 \times G_2$ ویژگی آبلی بودن را از مولفه‌هایش به ارث می‌برد.

۵- آیا $G_1 \times G_2$ ویژگی دوری بودن را از مولفه‌هایش به ارث می‌برد؟ (نشان دهید که گروه $\mathbb{Z}_2 \times \mathbb{Z}_2$ دارای عضوی با رتبه‌ی ۴ نیست و قضیه‌ی **۵.۴.۲** را به کار ببرید).

۶- یادآوری می‌کنیم که، تا حد یک‌ریختی، تنها دو (دسته) گروه چهار عضوی وجود دارند، یکی با نماینده‌ی $\mathbb{Z}_4$ و دیگری با نماینده‌ی K_4. حال که، با توجه به بند **۵**، $\mathbb{Z}_2 \times \mathbb{Z}_2$ دوری نیست، بگویید با کدام گروه چهار عضوی یک‌ریخت است. روشن است، نیست؟ جدول کیلی گروه $\mathbb{Z}_2 \times \mathbb{Z}_2$ را در زیر کامل و آن را با جدول گروه کلاین K_4 مقایسه کنید:

K_4	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

$+$	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
$(0,0)$	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
$(0,1)$	$(0,1)$	?	?	$(1,0)$
$(1,0)$	$(1,0)$	$(1,1)$	$(0,0)$	?
$(1,1)$	$(1,1)$	?	$(0,1)$	$(0,0)$

۷- دوباره می‌پرسیم که، حال که دسته‌ی گروه‌های دوری **نسبت به ضرب بسته نیست**، از قضیه‌ی ۲.۹.۱ بیرخوف چه نتیجه‌ای می‌گیرید؟ درست است، دسته‌ی گروه‌های دوری را نمی‌توان با مجموعه‌ای از معادله‌ها مشخص کرد!

۸- البته حاصل‌ضرب برخی از گروه‌های دوری، دوری است. برای مثال، چون مرتبه‌ی 1 در گروه $\mathbb{Z}_2$ برابر با ۲ و در گروه $\mathbb{Z}_3$ برابر با ۳ است، به آسانی می‌توانید نشان دهید که مرتبه‌ی $(1,1)$ در گروه $\mathbb{Z}_2\times\mathbb{Z}_3$ برابر است با $|\mathbb{Z}_2\times\mathbb{Z}_3|=6$ و در نتیجه، بنابر قضیه‌ی ۵.۴.۲، $\mathbb{Z}_2\times\mathbb{Z}_3=<(1,1)>$ دوری است.

۹- حدس می‌زنید که چه عاملی باعث می‌شود که $\mathbb{Z}_2\times\mathbb{Z}_3$ و $\mathbb{Z}_3\times\mathbb{Z}_4$ دوری باشند ولی $\mathbb{Z}_2\times\mathbb{Z}_2$، $\mathbb{Z}_4\times\mathbb{Z}_6$، یا $\mathbb{Z}_3\times\mathbb{Z}_6\times\mathbb{Z}_5$ دوری نباشند؟ به احتمال زیاد درست حدس زده‌اید. برای اثبات درستی حدس خود، ابتدا مسأله‌ی زیر را با استفاده از لم ۳.۴.۲ حل کنید.

۱۰- فرض کنید $g=(g_1,\cdots,g_n)\in G=G_1\times\cdots\times G_n$ و $O_{G_i}(g_i)=m_i$. نشان دهید که $O_G(g)=m=[m_1,\cdots,m_n]$ (لم ۳.۴.۲ را به کار ببرید).

۳.۷.۲ قضیه. گروه $G=\mathbb{Z}_{m_1}\times\cdots\times\mathbb{Z}_{m_n}$ دوری است اگر و تنها اگر برای هر $i\neq j$، $(m_i,m_j)=1$.

اثبات. با استفاده از بند ۱۰ بحث ۲.۷.۲ بالا، نشان دهید که

$$O_G(1,1,\cdots,1)=m_1m_2\cdots m_n=|G|$$

و قضیه‌ی ۵.۴.۲ را به کار ببرید.

۴.۷.۲ بحث در کلاس

۱- اگر گروه G برابر، یا یک‌ریخت، با حاصل‌ضرب دو گروه نابدیهی (مخالف $\{e\}$) باشد، می‌گوییم که G **تجزیه‌پذیر** است. برای مثال، K_4 تجزیه پذیر است ولی $\mathbb{Z}_4$ تجزیه پذیر نیست. **چطور؟** با توجه به قضیه‌ی بالا، تعیین کنید که $\mathbb{Z}_n$ برای کدام عدد طبیعی n تجزیه‌پذیر است؟

۲- نشان دهید که گروه $\mathbb{Z}\times\mathbb{Z}$ دوری نیست. ابتدا نشان دهید که $(1,1)$ نمی‌تواند مولد $\mathbb{Z}\times\mathbb{Z}$ باشد. حال فرض کنید که $(m,n)\neq(1,1)$ و نشان دهید که $(1,1)$ مضرب (m,n) نیست.

۳- نشان دهید که برای $n\geq 2$، گروه $\mathbb{Z}\times\mathbb{Z}_n$ دوری نیست.

۴- نشان دهید که اگر $G_1\times G_2$ با مولد (g_1,g_2) دوری باشد آنگاه G_1 با مولد g_1 و G_2 با مولد g_2 دوری هستند.

۵- با استفاده از مطالب بالا، نشان دهید که $\mathbb{Z}$ تجزیه‌ناپذیر است.

بحث بالا تکلیف تجزیه‌پذیری یا تجزیه‌ناپذیری گروه‌های دوری را کاملاً روشن می‌کند. ولی در حالت کلی، کدام گروه‌ها تجزیه‌پذیر یا تجزیه‌ناپذیر هستند؟ این سؤال را در قضیه‌ی ۷.۷.۲ پاسخ می دهیم. ابتدا لم زیر را می‌آوریم.

۵.۷.۲ لم. فرض کنیم $G=H\times K$ حاصل‌ضرب گروه‌های H و K باشند. در این صورت،

۱- $\hat{H}=H\times\{e_K\}=\{(h,e_k)\,|\,h\in H\}$ و $\hat{K}=\{e_h\}\times K$ زیر گروه $G=H\times K$ هستند، به طوری که $H\cong\hat{H}$، $K\cong\hat{K}$، و $G=H\times K\cong\hat{H}\times\hat{K}$.

۲- $\hat{H}\cap\hat{K}=\{(e_H,e_K)\}$.

۳- برای هر $\hat{h}\in\hat{H}$ و $\hat{k}\in\hat{K}$ داریم $\hat{h}\hat{k}=\hat{k}\hat{h}$.

۴- $G=H\times K=\hat{H}\hat{K}$

اثبات. اثبات این مطالب سرراست هستند. خلاصه‌ای از آن را می‌آوریم.

۱- روشن است که $\hat{e}=(e_H,e_K)$ عضو همانی $\widehat{H}$ و $\widehat{K}$ است. همچنین،

$$(h_1,e_K)(h_2,e_K)=(h_1h_2,e_K)\in\widehat{H}$$
$$(h,e_K)^{-1}=(h^{-1},e_K)\in\widehat{H}$$

از این رو، $\widehat{H}\leq H\times K=G$. به همین صورت، $\widehat{K}\leq H\times K=G$. به آسانی می‌توانید نشان دهید که توابع زیر یک‌ریختی هستند:

$$\varphi : H \to \widehat{H}, \qquad \psi : K \to \widehat{K}$$
$$h \mapsto \hat{h} = (h, e_K) \qquad k \mapsto \hat{k} = (e_H, k)$$

$$\Phi : H \times K \to \widehat{H} \times \widehat{K}$$
$$(h,k) \mapsto (\hat{h}, \hat{k}) = ((h, e_k), (e_K, k))$$

۲- توجه می‌کنیم که $(h, e_K) = (e_H, k)$ اگر و تنها اگر $h = e_H$ و $k = e_K$. کـه بنـد ۲ را اثبات می‌کند.

۳- برای هر $\hat{h} \in \widehat{H}$ و $\hat{k} \in \widehat{K}$، داریم

$$\hat{h}\hat{k} = (h, e_K)(e_H, k) = (he_H, e_K k) = (h,k)$$
$$\hat{k}\hat{h} = (e_H, k)(h, e_K) = (e_H h, k e_K) = (h,k)$$

۴- سرانجام توجه می‌کنیم که

$$\begin{aligned} \hat{H}\hat{K} &= \{(h, e_K) \mid h \in H\}\,\{(e_K, k) \mid k \in K\} \\ &= \{(h, e_K)(e_K, k) = (h,k) \mid h \in H, k \in K\} \\ &= H \times K = G \end{aligned}$$

۶.۷.۲ بحث در کلاس. قضیه‌ی بالا نشان می‌دهد که مولفـه‌هـای حاصـل‌ضـرب $H \times K$، یعنی H و K با زیرگروه‌هـایی چـون $\widehat{H}$ و $\widehat{K}$ از گـروه $H \times K$ یـک‌ریخـت هسـتند کـه ایـن زیرگروه‌ها دارای ویژگی‌های ۲، ۳، ۴ هستند. حال عکس این روند را بررسی می‌کنـیم. ادعـا مـی-کنیم که اگر گروهی دلخواه چون G دارای زیرگروه‌هایی چون H و K با ویژگی‌های همتـای ۲، ۳، ۴، باشند آنگاه $G \cong H \times K$.

۷.۷.۲ قضیه. فرض کنیم H و K زیرگروه‌هایی از گروه دلخواه G با ویژگی‌های زیر باشند:

(الف) برای هر $h \in H$ و $k \in K$، داشته باشیم $hk = kh$؛

(ب) $H \cap K = \{e\}$؛

(پ) $G = HK$.

در این صورت، $G \cong H \times K$.

اثبات. نشان می‌دهیم که

$$\begin{aligned}\varphi : H \times K &\to G \\ (h,k) &\mapsto hk\end{aligned}$$

یک‌ریختی مورد نظر است. روشن است که φ خوش‌تعریف و بنابر (پ) پوشا است. اثبات یک به یک بودن φ جالب است! توجه می‌کنیم که

$$\begin{aligned}\varphi(h_1,k_1)=\varphi(h_2,k_2) &\Rightarrow h_1k_1 = h_2k_2 \\ &\Rightarrow h_2^{-1}h_1 = k_2k_1^{-1} \in H \cap K = \{e\}\end{aligned}$$

(درستی سطر دوم را توضیح دهید). پس، $h_2^{-1}h_1 = e$ و $k_1k_2^{-1} = e$، و در نتیجه $h_1 = h_2$، $k_1 = k_2$، یعنی φ یک به یک است. در پایان، به آسانی می‌توان نشان داد که φ همریختی است (درستی مراحل زیر را توضیح دهید):

$$\begin{aligned}\varphi[(h_1,k_1)(h_2,k_2)] &\Rightarrow \varphi(h_1h_2,k_1k_2) = (h_1h_2)(k_1k_2) \\ &\Rightarrow (h_1k_1)(h_2k_2) \\ &\Rightarrow \varphi(h_1,k_1)\varphi(h_2,k_2)\end{aligned}$$

بنابراین، قضیه اثبات شده است. **راحت بود، نبود؟**

۸.۷.۲ بحث در کلاس

۱- قضیه‌های بالا **شرایط لازم و کافی برای تجزیه‌پذیری گروه** دلخواه G را ارائه می‌دهد. نمونه‌های زیر را ببینید.

۲- نشان می‌دهیم که K_4 تجزیه پذیر است. البته، قبلاً دیدیم که $K_4 \cong \mathbb{Z}_2 \times \mathbb{Z}_2$، ولی می‌خواهیم روش استفاده از قضیه‌ی بالا را نشان دهیم. به آسانی می‌توانید نشان دهید که زیرگروه‌های $H = \{e,a\}$ و $K = \{e,b\}$ از K_4 در شرایط قضیه صدق می‌کنند. توجه کنید که $c = ab$. در نتیجه، $K_4 \cong H \times K$. همچنین، چون $H \cong \mathbb{Z}_2$ و $K \cong \mathbb{Z}_2$، پس $K_4 \cong H \times K \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

۳- آیا $\mathbb{Z}_4$ تجزیه‌پذیر است؟ پاسخ منفی است، زیرا $H = K = \{0,2\}$ تنها زیرگروه نابدیهی $\mathbb{Z}_4$ است ولی در شرط‌های (ب) و (پ) قضیه صدق نمی‌کند.

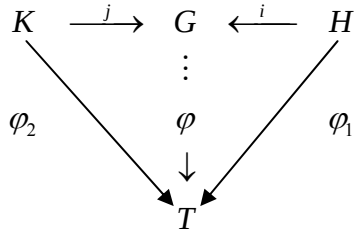
۴- به راحتی می‌توانید به دو روش، یکی با استفاده از قضیه‌ی ۱۵.۴.۲ و دیگری با استفاده از قضیه‌ی بالا، نشان دهید که $\mathbb{Z}_p$ و S_3 تجزیه ناپذیر هستند و $\mathbb{Z}_6$ تجزیه‌پذیر است.

۹.۷.۲ تعریف. فرض کنیم G گروه و H و K **زیرگروه** آن باشند به طوری که در شرط‌های قضیه‌ی **۷.۷.۲** صدق کنند، و در نتیجه $G \cong H \times K$. در این صورت، می‌گوییم که G **حاصل‌ضرب مستقیم درونی** H و K است.

۱۰.۷.۲ بحث در کلاس. قضیه‌ی **۵.۷.۲** نشان می‌دهد که اگر $G = H \times K$ حاصل ضرب **برونی** H و K باشد، آنگاه $\widehat{H}$ و $\widehat{K}$ در شرط‌های قضیه‌ی **۷.۷.۲** صدق می‌کنند و در نتیجه $G \cong \widehat{H} \times \widehat{K}$ حاصل‌ضرب **درونی** است. از این رو اساساً تفاوتی بین دو مفهوم حاصل‌ضرب برونی و حاصل ضرب درونی دو گروه وجود ندارد. از این رو، تنها وقتی از پسوندهای برونی و درونی استفاده می‌کنیم که بخواهیم بر زیرگروه بودن یا نبودن مؤلفه‌ها تاکید کنیم.

۱۱.۷.۲ همضرب گروه‌های آبلی. مفهوم همضرب را در **م.۵.۱** و بخش **۶** از فصل **۱** معرفی کردیم. اثبات وجود همضرب گروه‌های **غیر آبلی قدری پیچیده** است و در درس‌های دیگر مطرح می‌شود. در اینجا می‌خواهیم وجود همضرب را برای گروه‌های **آبلی** به اختصار بیاوریم.

فرض کنیم H و K گروه‌هایی **آبلی** باشند (که عمل‌های هر دو را با $+$ نشان می‌دهیم). به دنبال گروهی **آبلی** چون G همراه با دو همریختی $K \xrightarrow{i_2} G \xleftarrow{i_1} H$ با **ویژگی جهانی** زیر هستیم: برای هر گروه **آبلی** $(T;+)$ و هر جفت همریختی گروهی $K \xrightarrow{\varphi_2} T \xleftarrow{\varphi_1} H$، همریختی منحصر به فرد $\varphi : G \to T$ وجود داشته باشد به طوری که نمودار زیر تعویض‌پذیر باشد:



ادعا می‌کنیم که همان گروه $G = H \times K$ ولی همراه با همریختی‌های درون‌بری

$$K \xrightarrow{i_2} G = H \times K \xleftarrow{i_1} H$$
$$k \mapsto (\circ_H, k) \qquad (h, \circ_K) \leftarrow h$$

به جای همریختی‌های تصویری، گروه مورد نظر است. کافی است در نمودار بالا تعریف کنیم

$$\varphi : H \times K \to T$$
$$(h,k) \mapsto \varphi_1(h) + \varphi_2(k)$$

به آسانی می‌توانید نشان دهید که تابع φ نمودار بالا را تعویض‌پذیر می‌کند و با این ویژگی منحصر به فرد است. پس کافی است اثبات کنید که φ همریختی است. در اثبات آسان و سرراست این مطلب، **آبلی بودن** T را به کار خواهید برد.

چون گروه‌های بالا آبلی هستند، نمادهای جمعی را به کار برده‌ایم. از این رو، معمولاً همضرب گروه‌های آبلی H و K را با $G = H \oplus K$ نشان می‌دهیم و آن را **مجموع مستقیم** نیز می‌نامیم.

تمرین ۷.۲

آستین ها را بالا بزنید

دسته‌ی اول

۱- نشان دهید که گروه $G = \mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_n}$ با گروه $\mathbb{Z}_{m_1 \cdots m_n}$ یک‌ریخت است اگر و تنها اگر برای هر $i \neq j$، $(m_i, m_j) = 1$.

۲- در زیر، مرتبه‌ی هر عضو را در گروه داده شده بیابید:

(الف) $(4,9) \in \mathbb{Z}_{18} \times \mathbb{Z}_{18}$.

(ب) $(4,9) \in \mathbb{Z}_8 \times \mathbb{Z}_{12}$.

(پ) $(4,5,3) \in \mathbb{Z}_{18} \times \mathbb{Z}_{18} \times \mathbb{Z}_6$.

(ت) $(\rho_1, 4) \in S_3 \times \mathbb{Z}_6$.

۳- دو گروه نا آبلی، یکی از مرتبه‌ی ۱۸ و دیگری از مرتبه‌ی ۳۲ مثال بزنید.

۴- یک گروه G از مرتبه‌ی ۱۲۵ مثال بزنید که مرتبه‌ی هر عضو ناهمانی آن ۵ باشد.

نشان دهید که $Z(G_1 \times G_2) = Z(G_1) \times Z(G_2)$.

۵- فرض کنید که $H_1 \leq G_1$ و $H_2 \leq G_2$. نشان دهید که $H_1 \times H_2 \leq G_1 \times G_2$.

۶- فرض کنید $G_1 \cong G_1'$ و $G_2 \cong G_2'$. نشان دهید که $G_1 \times G_2 \cong G_1' \times G_2'$.

۷- زیرگروه‌های $6\mathbb{Z} \cap 9\mathbb{Z}$ و $6\mathbb{Z} + 9\mathbb{Z}$ از گروه $\mathbb{Z}$ را مشخص کنید.

۸- زیرگروه‌های $H=<4>$ و $K=<6>$ از گروه $\mathbb{Z}_{12}$ را در نظر بگیرید و $H+K$ را مشخص کنید.

۹- گروه $\mathbb{Z}_{26}\times\mathbb{Z}_{15}$ دارای چند عضو از مرتبه‌ی ۵ و چند عضو از مرتبه‌ی ۱۵ است؟

دسته‌ی دوم

۱۰- ثابت کنید که گروه ضربی $(\mathbb{R}^*;\cdot)$ تجزیه‌پذیر است. تابع زیر را به کار ببرید:

$$f:\mathbb{R}^*\to\mathbb{R}^+\times\{1,-1\}$$
$$f(x)=\begin{cases}(x,1) & x>0\\(-x,-1) & x<0\end{cases}$$

۱۱- ابتدا با یک مثال نشان دهید که زیرگروه‌های گروه $G_1\times G_2$ لزوماً به صورت $H_1\times H_2$ نیستند. سپس ثابت کنید که اگر همه‌ی زیرگروه‌های گروه $G_1\times G_2$ به صورت $H_1\times H_2$ باشند، آنگاه $G_1\times G_2$ دوری است. آیا عکس این مطلب نیز درست است.

۱۲- (**تمرین جالب**) فرض کنید که $H,K\le G$. نشان دهید که G حاصل‌ضرب (مستقیم درونی) H و K است اگر و تنها اگر دو شرط زیر برقرار باشند:

(الف) برای هر $h\in H$ و $k\in K$، $hk=kh$؛

(ب) هر عضو $g\in G$ تجزیه‌ای یکتا به صورت $g=hk$ داشته باشد که در آن $h\in H$ و $k\in K$.

۱۳- فرض کنید که $H,K\le G$. نشان دهید که G حاصل‌ضرب مستقیم درونی H و K است اگر و تنها اگر تابع زیر یک یک‌ریختی گروهی باشد:

$$\varphi:H\times K\to G$$
$$(h,k)\mapsto hk$$

۱۴- فرض کنید $G=G_1\times\cdots\times G_n$ حاصل‌ضرب (برونی) گروه‌ها باشد. در این صورت، زیرگروه‌های $\hat{G}_i\le G$ وجود دارند به طوری که

(الف) برای هر i، $G_i\cong\hat{G}_i$.

(ب) برای هر $i\neq j$، $x\in\hat{G}_i$ و $y\in\hat{G}_j$، داریم $xy=yx$.

(پ) برای هر i، $\hat{G}_i \cap (\hat{G}_1 \cdots \hat{G}_{i-1}\hat{G}_{i+1} \cdots \hat{G}_n) = \{e_G\}$.

(ت) $G = \hat{G}_1\hat{G}_2 \cdots \hat{G}_n$.

(ث) $G \cong \hat{G}_1 \times \cdots \times \hat{G}_n$.

۱۵- مثال هایی از گروه‌های H_i و K_i $(i = 1, 2)$ ارائه دهید به طوری که $H_1 \times H_2 \cong K_1 \times K_2$ در حالی که هیچ یک از H_i با K_j ها یک‌ریخت نباشد.

۸.۲ گروه خارج قسمتی

یکی دیگر از روش‌های **بسیار مهم** ساختن دستگاه‌های ریاضی جدید (جبری یا غیر جبری) از یک دستگاه ریاضی داده شده، تشکیل خارج قسمت آن دستگاه است. در بخش **۷** از فصل **۱**، این روش را برای دستگاه‌های جبری کلی معرفی و ویژگی‌های جامع آن را بررسی کردیم. در این بخش می‌خواهیم مطالب بخش **۷.۱** را برای گروه‌ها با جزییات بیشتری بررسی کنیم.

۱.۸.۲ بحث در کلاس

۱- مطالب جالبی در فصل **۱**، به ویژه در بخش **۷.۱** ، مطرح شد که به نظر ما هر دانشجوی ریاضی، صرف نظر از اینکه با دستگاه‌های کلاسیک سروکار دارد یا روزی با دستگاه‌هایی جدید سروکار خواهد داشت، باید آن‌ها را بداند! باید خواستگاه، بنیاد، منبع، سرچشمه، و علت معرفی مفاهیم را بدانیم تا بهتر آن‌ها را به کار ببریم و خود، هنگام نیاز، سازنده‌ی مفاهیم جدید باشیم! **این طور نیست؟** در همان بخش **۷.۱ هشدار** دادیم که برای برخی از دستگاه‌های کلاسیک (از جمله، گروه‌ها و حلقه‌ها)، روش ساختن خارج قسمت به صورتی بسیار خاص انجام می‌شود که لزوماً در بسیاری از دستگاه‌های جبری، از جمله، نیم‌گروه‌ها، تکواره‌ها، مشبکه‌ها، ... به کار نمی‌آید!

۲- در اغلب کتاب‌های کلاسیک جبر، برای تعریف گروه خارج قسمتی گروه G، کار را با زیرگروه خاصی چون N به نام **زیرگروه نرمال** آغاز می‌کنند و از مجموعه‌ی هم‌مجموعه‌های چپ $L_N = \{aN \mid a \in G\}$ یا راست $R_N = \{Na \mid a \in G\}$، همراه با عمل طبیعی $(aN)(bN) = abN$ یا $(Na)(Nb) = Nab$، گروهی خارج قسمتی می‌سازند. در این روند نه تنها علت کار مشخص نمی‌شود، بلکه روشن نمی‌شود که آیا این تنها روش ساختن گروه خارج قسمتی است یا نیست؟ به عبارت دیگر، آیا تنها برای هر زیرگروه نرمال می‌توانیم خارج قسمتی از یک گروه بسازیم، یا به گونه‌ای دیگر نیز می‌توان یک گروه را تقسیم‌بندی (**افراز**) کرد و گروهی خارج قسمتی ساخت؟ متاسفانه در بسیاری از کتاب‌های کلاسیک پاسخی صریح به این سؤال‌ها داده نمی‌شود و مدرسانی که پاسخ را می‌دانند نیز، احتمالاً به دلیل کمبود وقت یا عدم نیاز برای

دستگاه‌های جبری مورد نظر آن‌ها، یعنی گروه‌ها و حلقه‌ها، از کنار آن می‌گذرند! ما نیز می‌توانیم همین روش کوتاه‌تر، ولی بسیار خاص، را به کار ببریم،

ولی قول دادیم که فوت و فن کار را نیز از شما پنهان نکنیم!

۳- در این فصل، هر دو روش کلاسیک یا متداول (که تنها برای معدودی از دستگاه‌های جبری به کار می‌آید) و روش جامع را (که برای همه‌ی دستگاه‌های جبری به کار می‌رود) برای ساختن گروه-های خارج قسمتی می‌آوریم. سپس نشان می‌دهیم که روش کلاسیک برای گروه‌ها (و در فصل **۳** برای حلقه‌ها) تصادفاً معادل با روش جامع است! در بحث زیر، که یادآوری مطالبی از بخش **۷** فصل **۱** است، شرکت کنید.

هشدار می‌دهیم که در این فصل با مجموعه‌هایی متشکل از مجموعه‌ها سر و کار داریم و عمل‌ها نیز روی این نوع مجموعه‌ها (ی نا بسیط) تعریف می‌شوند! از این رو باید بیشتر دقت کنیم.

۲.۸.۲ بحث در کلاس

در بخش **۷.۱** دیدیم که هر **خارج قسمت** دستگاه جبری A ، از نوع τ ، چیزی جز **افراز** خاصی از A نیست. همچنین دیدیم که این افراز باید به گونه‌ای خاص باشد که همراه با عمل‌هایی که حاصل از عمل‌های خود A است، دستگاهی جبری از نوع τ به دست دهد. برای رسیدن به این هدف در مورد گروه‌ها، در بخش **۷.۱** دیدیم که تنها باید آن رابطه‌های هم‌ارزی $\sim$ را روی گروه G در نظر بگیریم که عمل $[x]\overline{*}[y]=[x*y]$ روی افراز آن $G/\sim$ خوش تعریف باشد، یعنی

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

که معادل است با اینکه

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

یعنی $\sim$ رابطه‌ای **همنهشتی** باشد (تعریف **۱.۷.۱** را ببینید.) این مطلب را برای گروه‌ها دوباره در زیر اثبات می‌کنیم.

۳.۸.۲ قضیه

۱- رابطه‌ی هم‌ارزی $\sim$ روی گروه G رابطه‌ای همنهشتی است اگر و تنها اگر عمل $[x]\overline{*}[y]=[x*y]$ روی $G/\sim$ خوش‌تعریف باشد.

۲- اگر $\sim$ رابطه‌ای همنهشتی روی گروه G باشد، آنگاه افراز $G/\sim$ همراه با عمل $[x]\overline{*}[y]=[x*y]$ گروه است.

اثبات

۱- فرض کنیم $\sim$ رابطه‌ای همنهشتی باشد. در این صورت، داریم

$$\begin{cases}[x]=[x']\\ [y]=[y']\end{cases}\Rightarrow\begin{cases}x\sim x'\\ y\sim y'\end{cases}\Rightarrow x*y\sim x'*y'$$
$$\Rightarrow[x*y]=[x'*y']$$
$$\Rightarrow[x]\overline{*}[y]=[x']\overline{*}[y']$$

پس $\overline{*}$ خوش‌تعریف است. برعکس، فرض کنیم $\overline{*}$ خوش‌تعریف باشد. در این صورت، رابطه‌ی $\sim$ همنهشتی است، زیرا

$$\begin{cases}x\sim x'\\ y\sim y'\end{cases}\Rightarrow\begin{cases}[x]=[x']\\ [y]=[y']\end{cases}\Rightarrow[x]\overline{*}[y]=[x']\overline{*}[y']$$
$$\Rightarrow[x*y]=[x'*y']$$
$$\Rightarrow x*y\sim x'*y'$$

۲- اثبات شرکت‌پذیری $\overline{*}$ در $G/\sim$ به راحتی از شرکت‌پذیری $*$ در G نتیجه می‌شود. روشن است که $[e]$ عضو همانی $G/\sim$ است. زیرا

$$[x]\overline{*}[e]=[x*e]=[x]\quad\&\quad[e]\overline{*}[x]=[e*x]=[x]$$

در پایان، به راحتی می‌توانید نشان دهید که وارون $[x]$، یعنی $[x]^{-1}$، برابر با $[x^{-1}]$ است.
آسان بود، نبود؟

۴.۸.۲ تعریف. فرض کنیم $\sim$ رابطه‌ای همنهشتی روی گروه G باشد. گروه $(G/\sim;\overline{*})$ را **گروه خارج قسمتی** G بر $\sim$ می‌نامیم.

۵.۸.۲ بحث در کلاس در بالا روش کلی ساختن گروه‌های خارج قسمتی را آوردیم. قبل از آوردن روش کلاسیک، مثال‌ها و نکته‌هایی را در باره‌ی روش بالا ارائه می‌کنیم.

۱- آیا افراز

$$\mathcal{P}_1 = \{\{0,1\},\{2\},\{3\}\} \quad = \quad \begin{array}{|c|c|}\hline 0 & 2 \\ \hline 1 & 3 \\ \hline \end{array}$$

گروهی خارج قسمتی از گروه $\mathbb{Z}_4$ به دست می‌دهد؟ چطور به چنین سؤالی پاسخ دهیم؟ با توجه به قضیه‌ی ۳.۸.۲ باید نشان دهیم که رابطه‌ی هم‌ارزی $\sim$ متناظر با این افراز یک رابطه‌ی همنهشتی است، یعنی در شرط $(*)$ بالا صدق می‌کند. ولی، چون

$$\begin{cases} 0 \sim 1 \\ 2 \sim 2 \end{cases} \not\Rightarrow \quad 0 +_4 2 \sim 1 +_4 2$$

پس پاسخ به سؤال بالا منفی است.

۱- افراز $\mathcal{P}_2 = \{\{\circ,1\},\{2,3\}\}$ **چطور؟** اگر چه در این حالت داریم

$$\begin{cases} 0 \sim 1 \\ 2 \sim 2 \end{cases} \Rightarrow \quad 0 +_4 2 \sim 1 +_4 2$$

ولی مطلب زیر نشان می‌دهد که این افراز نیز منجر به گروهی خارج قسمتی حاصل از گروه $\mathbb{Z}_4$ نمی‌شود!

$$\begin{cases} 0 \sim 1 \\ 3 \sim 3 \end{cases} \not\Rightarrow \quad 0 +_3 3 \sim 1 +_3 3$$

۲- نشان دهید که هر یک از سه افراز

$$\mathcal{P}_3 = \{\{\circ,2\},\{1,3\}\}, \mathcal{P}_4 = \{\{\circ\},\{1\},\{2\},\{3\}\}, \mathcal{P}_5 = \{\{\circ,1,2,3\}\}$$

(و تنها این سه افراز) گروهی خارج قسمتی از $\mathbb{Z}_4$ به دست می‌دهند.

۳- نشان دهید که هر یک از افرازهای $\mathcal{P}_a = \{\{e,a\},\{b,c\}\}$ و $\mathcal{P}_b = \{\{e,b\},\{a,c\}\}$ گروهی خارج قسمتی از گروه کلاین K_4 به دست می‌دهد. سه افراز دیگر نیز چنین هستند، آن‌ها را مشخص کنید.

۶.۸.۲ **بحث در کلاس.** برای آگاهی از **فوت و فن** روش کلاسیک و متداول ساختن گروه‌های خارج قسمتی، ابتدا مطالبی از بحث ۱۲.۲.۲ را، که به اثبات قضیه‌ی مهم لاگرانژ انجامید، مرور می‌کنیم.

۱- فـرض کنـیم N **زیرگـروه** $(G;*)$ اسـت. بـرای هـر عضـو $a \in G$، مجموعـه‌ی $aN = \{an \mid n \in N\}$ (یا در نمادگذاری جمعی $a+N = \{a+n \mid n \in N\}$)، را یک **هم-مجموعه‌ی چپ** N نامیدیم. دیدیم که این هم‌مجموعه‌ها، رده‌های **رابطـه‌ی هـم‌ارزی** $a \sim_N b$ بـا تعریف

$$a \sim_N b \Leftrightarrow (\exists n \in N) \quad a = bn \Leftrightarrow b^{-1}a = n \in N \qquad (**)$$

هستند؛ زیرا

$$\begin{aligned}[a] &= \{x \in G \mid x \sim_N a\} \\ &= \{x \in G \mid (\exists n \in N)\, x = an\} \\ &= \{an \mid n \in N\} \\ &= aN\end{aligned}$$

بنابراین، با توجه به اینکه $[a] = [b]$ اگر و تنها اگر $a \sim_N b$، داریم

$$\begin{aligned}aN = bN &\Leftrightarrow a \sim_N b \Leftrightarrow (\exists n \in N) \quad a = bn \\ &\Leftrightarrow b^{-1}a = n \in N\end{aligned}$$

ویژگی‌های دیگر هم‌مجموعه‌های چپ و راسـت $Na = \{na \mid n \in N\}$ عبـارت هسـتند از $|aN| = |N| = |Na|$ و $|L_N| = |R_N|$، کـــــه در آن $R_N = \{Na \mid a \in G\}$ مجموعه‌ی هم‌مجموعه‌های راست N در G است.

۲- بنابر قضیه‌ی لاگرانژ، برای گروه متناهی G، داریم $|L_N| = |R_N| = \dfrac{|G|}{|N|}$، و ایـن عـدد را **اندیس** N در G نامیدیم و با $[G:H]$ نشان دادیم.

تا اینجای کار نیازی به ویژگی دیگری از زیرگروه N نشدا! ولی، آیا رابطه‌ی هـم‌ارزی متنـاظر با این افراز که در بند **۱** با $(**)$ داده شد همیشه **همنهشتی** است؟ مثال زیر پاسـخی منفـی بـه این سؤال است.

۳- زیرگروه $H = \{\rho_0, \mu_1\}$ را از گروه S_3 در نظر بگیرید. با استفاده از جدول گـروه S_3 کـه در بند **۴** بحث **۱.۶.۲** داده شد، به آسانی می‌توانید نشان دهید که $\mu_2 \sim_H \rho_2$ زیرا

$$\rho_2^{-1}\mu_2 = \rho_1\mu_2 = \mu_1 \in H$$

از طرفی، $\mu_1 \ {}_H\sim \rho_0$. در حالی که، $\mu_1\mu_2 = \rho_1$ با $\rho_\circ\rho_2 = \rho_2$ در رابطه نیست، زیرا $\rho_2^{-1}\rho_1 = \rho_1\rho_1 = \rho_2 \notin H$. در نتیجه،

$$\begin{cases}\mu_1 \ {}_H\sim \rho_0\\ \mu_2 \ {}_H\sim \rho_2\end{cases} \not\Rightarrow \mu_1\mu_2 \sim \rho_0\rho_2$$

۴- (به این بند **مهم** بیش‌تر توجه کنید) **تحت چه شرطی** روی زیر گروه N از گروه G رابطه‌ی $(**)$ یک همنهشتی می‌شود؟ توجه می‌کنیم که برای هر $n \in N$ و هر $x \in G$، شرط $x^{-1}nx \in N$ یک **شرط لازم** است. زیرا،

$$\begin{cases}n \sim e\\ x \sim x\end{cases} \Rightarrow \begin{cases}nx \sim ex = x\\ x^{-1} \sim x^{-1}\end{cases} \Rightarrow x^{-1}nx \sim x^{-1}x = e \Rightarrow x^{-1}nx \in N$$

آیا این شرط **کافی** نیز هست؟ **پاسخ مثبت است!** (دلیل هر مرحله‌ی زیر را توضیح دهید):

$$\begin{cases}a \ {}_N\sim b\\ x \ {}_N\sim y\end{cases} \Rightarrow \begin{cases}b^{-1}a \in N\\ y^{-1}x \in N\end{cases} \Rightarrow \begin{cases}y^{-1}(b^{-1}a)y \in N\\ y^{-1}x \in N\end{cases}$$
$$\Rightarrow y^{-1}(b^{-1}a)y(y^{-1}x) \in N$$
$$\Rightarrow (y^{-1}b^{-1})(ax) \in N$$
$$\Rightarrow (by)^{-1}(ax) \in N$$
$$\Rightarrow ax \ {}_N\sim by$$

موفق شدیم! حال چه واژه‌ای به چنین زیرگروه **خوبی** اختصاص دهیم. تعریف زیر را ببینید.

۷.۸.۲ تعریف. زیرگروه N از گروه G را **نرمال** می‌گوییم، و می‌نویسیم $N \trianglelefteq G$ اگر

$$(\forall x \in G) \quad (\forall n \in N) \qquad x^{-1}nx \in N$$

۸.۸.۲ قضیه. حکم‌های زیر برای زیرگروه N از گروه G معادل هستند:

(الف) زیرگروه N از گروه G نرمال است (تعریف **۷.۸.۲**).

(ب) رابطه‌ی $a \ {}_N\sim b \Leftrightarrow b^{-1}a \in N$ همنهشتی است.

(پ) عمل دوتایی $(aN)(bN)=abN$، که همان $[a]_{N\sim}[b]_{N\sim}=[ab]_{N\sim}$ است، در $G/_{N}\sim=\{aN \mid a\in G\}$ خوش‌تعریف است.

اثبات. از بند۴ بحث **۶.۸.۲** و قضیه‌ی **۳.۸.۲**، و اینکه، با توجه به بند **۱** از بحث **۶.۸.۲**، $[a]_{\sim_N}=aN=\{ax \mid x\in N\}$، نتیجه می‌شود.

۹.۸.۲ قضیه و تعریف. فرض کنیم N زیرگروهی نرمال از گروه G باشد. در این صورت، $G/_{N}\sim=\{aN \mid a\in G\}$ همراه با عمل $(aN)(bN)=abN$ گروه است.

معمولاً گروه $G/_{N}\sim$ را برای سادگی با G/N نشان می‌دهیم و آن را گروه خارج قسمت G بر N (به جای بر $\sim_N$) می‌نامیم.

۱۰.۸.۲ جمع بندی. قضیه‌ی **۹.۸.۲** روش کلاسیک ساختن گروه‌های خارج قسمتی را به سرانجام می‌رساند. حال، مجموعه‌های زیر را در رابطه با گروه G درنظر بگیرید:

$Q(G)=\{$مجموعه‌ی همه‌ی گروه‌های خارج قسمتی $(G/\sim;\overline{*})\}$
$Con(G)=\{$مجموعه‌ی همه‌ی رابطه‌های همنهشتی $\sim$ روی گروه $G\}$
$Nor(G)=\{$مجموعه‌ی همه‌ی زیرگروه‌های نرمال $G\}$

۱- قضیه‌ی **۳.۸.۲** نتیجه می‌دهد که تناظری دوسویی بین $Q(G)$ و $Con(G)$ وجود دارد. توجه می‌کنیم که، $(G/\sim;\overline{*})$ گروه است اگر و تنها اگر $\sim$ همنهشتی باشد.

۲- قضیه‌های **۸.۸.۲** و **۹.۸.۲** بیان می‌کنند که دو تابع یک به یک از $Nor(G)$ به $Con(G)$ و از $Nor(G)$ به $Q(G)$ وجود دارند؛ برای هر زیر گروه نرمال $N\leq G$، رابطه‌ی $\sim_N$ رابطه‌ای همنهشتی و $G/N=G/_{N}\sim$ گروهی خارج قسمتی است.

۳- بند **۲** بیان نمی‌کند که این توابع یک به یک، دوسویی نیز هستند. یعنی، بیان نمی‌کند که برای هر گروه خارج قسمتی $(G/\sim;\overline{*})$ زیر گروهی نرمال مانند N وجود دارد به طوری که $G/\sim=G/N$، و برای هر رابطه‌ی همنهشتی $\sim$ روی G، زیرگروهی نرمال مانند N وجود دارد به طوری که $\sim=\sim_N$! ولی، آیا امیدی به دوسویی بودن این توابع وجود دارد؟ خوشبختانه قضیه‌ی زیر پاسخ مثبت به این سؤال را دربر دارد!

۱۱.۸.۲ قضیه. فرض کنیم $\sim$ رابطه‌ای همنهشتی روی گروه G باشد. در این صورت، رده‌ی $N=[e]$ زیرگروه نرمال G است، و $G/\sim = G/[e] = G/N$.

اثبات. **(الف)** ابتدا نشان می‌دهیم که $N=[e]$ زیرگروه G است. برای اثبات این مطلب، کافی است نشان دهیم که $N=[e]$ نسبت به عمل $*$ **بسته** است، $e\in N$، و برای هر $a\in N$ داریم $a^{-1}\in N$. روشن است که چون $e\sim e$ (انعکاسی بودن $\sim$) پس $e\in N$. حال، اگر $x,y\in N=[e]$، آنگاه $x\sim e$ و $y\sim e$. در نتیجه، بنا بر **شرط سازگاری** $\sim$، داریم $x*y\sim e*e=e$ و در نتیجه $x*y\in[e]=N$. حال، نشان می‌دهیم که برای هر $a\in N$ داریم $a^{-1}\in N$. چون $a\in N=[e]$، پس $a\sim e$. از طرفی، بنابر انعکاسی بودن $\sim$، داریم $a^{-1}\sim a^{-1}$. حال، **شرط سازگاری** $\sim$ ایجاب می‌کند که $a^{-1}*a\sim a^{-1}*e$، یعنی $e\sim a^{-1}$، و در نتیجه $a^{-1}\in N=[e]$. پس، $N=[e]$ زیرگروه G است.

(ب) برای اثبات نرمال بودن، فرض می‌کنیم $x\in G$ و $n\in N=[e]$ دلخواه باشند. باید نشان دهیم که $x^{-1}nx\in N=[e]$. مراحل زیر را توضیح دهید.

$$\begin{cases} n\sim e \\ x\sim x \end{cases} \Rightarrow \begin{cases} nx\sim x \\ x^{-1}\sim x^{-1} \end{cases}$$
$$\Rightarrow x^{-1}nx\sim x^{-1}x=e$$
$$\Rightarrow x^{-1}nx\in[e]=N$$
$$\Rightarrow N\trianglelefteq G$$

(پ) اثبات زیر را، که نشان می‌دهد $G/\sim = G/N$، توضیح دهید:

$$y\in[x]_{\sim} \Leftrightarrow y\sim x \Leftrightarrow x^{-1}y\sim x^{-1}x=e \Leftrightarrow x^{-1}y\in[e]=N$$
$$\Leftrightarrow xN=yN \Leftrightarrow y\in xN$$

تساوی $[x]=xN=x[e]$ به این معنی است که رده‌ی $N=[e]$ **سازنده‌ی همه‌ی رده‌ها است!** ولی، همان طور که بارها در این فصل و فصل **۱** گفتیم، احکام بسیار جالب قضیه‌ی بالا، **بسیار نادر هستند**، و از آنجا که در دستگاه‌های جبری کلاسیک مانند گروه، حلقه، مدول، و فضای برداری رخ می‌دهند، این **تصور نادرست** را در دانشجویان کارشناسی و حتی بالاتر ایجاد می‌کند که برای تمام دستگاه‌های جبری درست هستند، در حالی که حتی برای نیمگروه و تکواره هم لزوماً **درست نیستند!** (بند **۱** بحث **۴.۷.۱** را ببینید).

۱۲.۸.۲ بحث در کلاس. حال که به اهمیت زیرگروه‌های نرمال پی بردیم، چند شرط دیگر معادل با تعریف نرمال بودن را، علاوه بر آن‌هایی که در قضیه‌ی ۸.۸.۲ آمد، می‌آوریم که در اثبات قضیه‌ها و حل تمرین‌ها به کار خواهند رفت. این احکام را به عنوان تمرین اثبات کنید. فرض کنیم G گروه است.

۱- زیرگروه N از G نرمال است اگر و تنها اگر

$$(\forall x \in G) \quad (\forall n \in N) \qquad xnx^{-1} \in N$$

۲- زیرگروه N از G نرمال است اگر و تنها اگر برای هر $x \in G$، $xN = Nx$. توجه می‌کنیم که $xN = Nx$ به معنی این شرط قوی که برای هر $n \in N$، $xn = nx$ نیست (**به چه معنی است؟**) توجه می‌کنیم که

$$nx = x(x^{-1}nx) \in xN \qquad \& \qquad xn = (xnx^{-1})x \in Nx$$

۳- (ضعیف تر از بند ۲) زیرگروه N از G نرمال است اگر و تنها اگر

$$(\forall x \in G)(\exists y \in G) \quad xN = Ny$$

به عبارت دیگر، هر هم‌مجموعه‌ی چپ یک هم‌مجموعه‌ی راست است و بر عکس، یعنی $L_N = R_N$ که در آن

$$L_N = \{xN \mid x \in G\}, \qquad R_N = \{Ny \mid y \in G\}$$

۴- احکام زیر بلاواسطه از تعریف ۷.۸.۲ زیرگروه نرمال و بند ۱ بالا به دست می‌آیند:

$$\begin{aligned} N \trianglelefteq G \quad &\Leftrightarrow (\forall x \in G) \quad x^{-1}Nx \subseteq N \\ &\Leftrightarrow (\forall x \in G) \quad xNx^{-1} \subseteq N \end{aligned}$$

۵- احکام زیر را با استفاده از بند ۳ اثبات کنید (به سور عمومی توجه کنید):

$$\begin{aligned} N \trianglelefteq G \quad &\Leftrightarrow (\forall x \in G) \quad x^{-1}Nx = N \\ &\Leftrightarrow (\forall x \in G) \quad xNx^{-1} = N \end{aligned}$$

۶- روشن است که برای هرگروه G، زیرگروه‌های $\{e\}$ و G نرمال هستند.

۷- روشن است که **اگر گروه G آبلی** باشد، آنگاه **هر زیرگروه آن نرمال** است.

۸- بـرای هـر گـروه G، مرکـز آن $Z(G)=\{g\in G\mid(\forall x\in G)\quad xg=gx\}$، و هـر زیرگروه مرکز، در G نرمال است.

۹- نشان دهید که گروه خطی خاص $SL(n,\mathbb{R})$ در گروه خطی عام $GL(n,\mathbb{R})$ نرمال اسـت. باید نشان دهید که برای هر ماتریس $n\times n$ وارون‌پذیر چون A و هر ماتریس $n\times n$ چون B با دترمینان ۱، داریم $\det(A^{-1}BA)=1$.

۱۰- نشان دهید که A_3 در S_3، و به طور کلی A_n (متشکل از جایگشت‌های زوج)، در S_n نرمـال است. (به نظر شما اگر $\delta\in A_n$ زوج باشد، $\sigma^{-1}\delta\sigma$ زوج است یا فرد؟)

۱۱- فرض کنید که $N\leq G$ به طوری کـه $[G:N]=2$ (یعنـی، $L_N=\{N,aN\}$). نشـان دهید که $N\trianglelefteq G$. (حال سؤال بند ۱۰ را با استفاده از این مطلب نیز پاسخ دهید).

۱۳.۸.۲ مشتق گروه. همان طور که (در بنـد ۲ بحـث ۴.۷.۱) قـول دادیـم، و بـه بهانـه‌ی معرفی یک زیرگروه نرمال مهم (به نام زیرگروه مشتق)، در اینجا **فوت و فنی** را که در بند ۲ بحث ۴.۷.۱ معرفی کردیم برای گروه‌ها به نمایش می‌گذاریم.

فرض کنیم G گروه است و می‌خواهیم کوچک‌ترین رابطه‌ی همنهشتی $\sim$ را بیابیم بـه طـوری که گروه خارج قسمتی $G/\sim$ آبلی باشد، یعنی برای هر $x,y\in G$، عبارت‌های معادل زیر برقـرار باشند:

$$[x][y]=[y][x]\Leftrightarrow[xy]=[yx]\Leftrightarrow xy\sim yx$$

از این رو، کافی است که $\sim$ را کوچک‌ترین رابطه‌ی همنهشتی روی گـروه G در نظـر بگیـریم بـه طـوری کـه بـرای هـر $x,y\in G$، $xy\sim yx$. از ایـن عبـارت نتیجـه مـی‌گیـریم کـه $xyx^{-1}y^{-1}\sim e$ (چطـور؟) یعنـی $xyx^{-1}y^{-1}\in[e]$. ازطرفـی، مـی‌دانـیم کـه $N=[e]$ زیرگروه نرمال G است. بنابراین، باید به دنبال کوچک‌ترین زیرگروهی نرمال چـون N باشـیم بـه طوری که

$$(\forall x,y)\quad xyx^{-1}y^{-1}\in N$$

به دلیل اهمیت این عبارت، نمادگذاری $[x,y]=xyx^{-1}y^{-1}$ را برای آن به کار مـی‌بـریم و آن را (با توجه به قضیه‌ی ۱۴.۸.۲) یک **جا به جا گر** یا **تعویض‌گر** می‌نامیم.

برای رسیدن به مقصود، مراحل زیر را انجـام مـی‌دهـیم. ابتـدا بـا اسـتفاده از قضـیه‌ی ۹.۳.۲، زیرگروه تولید شده توسط مجموعه‌ی تعویض‌گرها، یعنی

$$< X = \{[x,y] = xyx^{-1}y^{-1} \mid x,y \in G\} >$$
$$= \{[x_1,y_1][x_2,y_2]\cdots[x_n,y_n] \mid n \in \mathbb{N}, [x_i,y_i] \in X \cup X^{-1}\}$$

را به دست می‌آوریم. ولی، چون تصادفاً داریم

$$[x,y]^{-1} = (xyx^{-1}y^{-1})^{-1} = yxy^{-1}x^{-1} = [y,x] \in X$$

یعنی، $X = X^{-1}$ و $X \cup X^{-1} = X$، عبارت بالا قدری ساده‌تر نوشته می‌شود:

$$< X > = \{[x_1,y_1][x_2,y_2]\cdots[x_n,y_n] \mid n \in \mathbb{N}, x_i, y_i \in G\}$$

حال باید کوچک‌ترین زیرگروه **نرمال** G را بیابیم که شامل $< X >$ باشد. خوشبختانه، ولی تصادفاً، $< X >$ به خودی خود نرمال نیز می‌شود. این زیرگروه نرمال G را معمولاً با G' یا $[G,G]$ نشان می‌دهیم و آن را **زیرگروه تعویض‌گر** یا **مشتق** G می‌نامیم. قضیه‌ی زیر نشان می‌دهد که به مقصود رسیده‌ایم و G' همان **کوچک‌ترین زیرگروه نرمال** G است به طوری که G/G' **آبلی** است.

۱۴.۸.۲ قضیه. فرض کنیم G گروه است. در این صورت،

۱- اگر $G' \subseteq H \leq G$، آنگاه H در G نرمال است. به ویژه، $G' \leq G$.

۲- اگر $N \leq G$ آنگاه G/N آبلی است اگر و تنها اگر $G' \subseteq N$. به ویژه G/G' آبلی است.

اثبات

۱- فرض کنیم $h \in H$ و $g \in G$. نشان می‌دهیم که $ghg^{-1} \in H$. بنابر تعریف G'، داریم $[g,h] = ghg^{-1}h^{-1} \in G'$ و چون $G' \subseteq H$، $[g,h] = ghg^{-1}h^{-1} \in H$ و در نتیجه $ghg^{-1} = ghg^{-1}h^{-1}h \in H$.

۲- توجه می‌کنیم که برای هر $x,y \in G$، داریم

$$
\begin{aligned}
(xN)(yN) = (yN)(xN) &\Leftrightarrow xyN = yxN \\
&\Leftrightarrow (yx)^{-1}(xy) \in N \\
&\Leftrightarrow x^{-1}y^{-1}xy \in N \\
&\Leftrightarrow [x, y] \in N \\
&\Leftrightarrow G' \subseteq N
\end{aligned}
$$

(مرحله‌ی آخر را توضیح دهید. **جالب است**). در نتیجه، گروه G / N آبلی است اگر و تنها اگر $G' \subseteq N$.

۱۵.۸.۲ بحث در کلاس

۱- ابتدا توجه می‌کنیم که گروه G آبلی است اگر و تنها اگر $G' = \{e\}$. **چطور؟** پس، برای مثال $\mathbb{Z}' = \{0\} = \mathbb{Z}'_n$، ولی برای $n \geq 3$، $S'_n \neq \{\rho_0\}$.

۲- می‌خواهیم، به عنوان نمونه، زیرگروه مشتق گروه متقارن S_3 را بیابیم. محاسبه‌ی مستقیم G' معمولاً طولانی است و بهتر است برنامه‌ای کامپیوتری بنویسید یا به روش‌های نظری دیگر به نتیجه برسید. برای نمونه، این مثال را به دو روش حل می‌کنیم. روشن است که برای هر $x, y \in S_3$، تعویض‌گر $[x, y] = xyx^{-1}y^{-1}$ جایگشتی زوج است. **چرا؟** پس $\{\rho_0\} \leq S'_3 \leq A_3$. ولی، چون S_3 آبلی نیست، پس $S'_3 \neq \{\rho_0\}$، از طرفی A_3 زیرگروه نابدیهی ندارد. پس $S'_3 = A_3$. برای تمرین، ρ_1 را به صورت کروشه‌ی تعویض‌گر $[-,-]$ بنویسید.

روش دیگر این است که، بنابر بند **۱** قضیه‌ی **۱۴.۸.۲**، S'_3 در S_3 نرمال است. همچنین، $S_3 / A_3 \cong \mathbb{Z}_2$ آبلی است. پس، بنابر بند **۲** همان قضیه، $\{\rho_0\} \leq S'_3 \leq A_3$. از این رو، مانند بالا، $S'_3 = A_3$.

تمرین ۸.۲

بدون تلاش برای حل کردن تمرین‌ها، مطالب درس را خوب نیاموخته‌اید

دسته اول

۱- اعضای گروه‌های خارج قسمتی $\mathbb{Z}_8 / \{0, 4\}$ و $\mathbb{Z}_{12} / <3>$ را بیابید و جدول‌های کیلی آن‌ها را تعیین کنید.

۲- نشان دهید که خارج قسمت هر گروه آبلی گروهی آبلی است. با یک مثال نشان دهید که عکس این مطلب در حالت کلی درست نیست؟

۳- نشان دهید که خارج قسمت هر گروه دوری، گروهی دوری است. با یک مثال نشان دهید که عکس این مطلب در حالت کلی درست نیست؟

۴- در زیر، مرتبه‌ی هر یک از عضوهای داده شده را در گروه مورد نظر بیابید:

(الف) $12+<6>, 14+<6>, 7+<6> \in \mathbb{Z}_{24}/<6>$.

(ب) $12+<6>, 14+<6>, 7+<6> \in \mathbb{Z}_{18}/<6>$.

۵- مرتبه‌ی هر یک از گروه‌های زیر را تعیین کنید:

$$\mathbb{Z}_{24}/<6>, \mathbb{Z}_{24}/<8>, \mathbb{Z}_4 \times \mathbb{Z}_6/<(0,2)>, \mathbb{Z}_4 \times \mathbb{Z}_6/<2> \times <3>$$

۶- فرض کنید که $H \leq G$. نشان دهید که $N_G(H) = N(H) = \{g \in G \mid g^{-1}Hg = H\}$ بزرگ‌ترین زیرگروه G است به طوری که $H \trianglelefteq N(H)$. این زیرگروه را **نرمالساز** H در G می‌نامیم. نتیجه بگیرید که $H \trianglelefteq G$ اگر و تنها اگر $N(H) = G$.

۷- فرض کنید که $N \leq G$ و برای هر $a \in G$، $a^2 \in N$. نشان دهید که $N \trianglelefteq G$ و گروه G/N آبلی است.

۸- فرض کنید H تنها زیرگروه n عضوی گروه G باشد. نشان دهید که H در G نرمال است.

۹- فرض کنید G گروه است، $H, K \trianglelefteq G$، و $H \cap K = \{e\}$. نشان دهید که برای هر $h \in H$ و $k \in K$، $hk = kh$.

۱۰- فرض کنید G گروه، $N \trianglelefteq G$، و $H \leq G$. ثابت کنید که:

(الف) $HN \leq G$ (ب) $H \cap N \trianglelefteq H$

(پ) $N \trianglelefteq HN$ (ت) اگر $H \trianglelefteq G$، آنگاه $HN \trianglelefteq G$

۱۱- فرض کنید که $N \leq G$ و $[G:N] = 2$. (بند ۱۱ بحث ۱۲.۸.۲ را ببینید). نشان دهید که برای هر $a \in G$، $a^2 \in N$. با استفاده از این مطلب نشان دهید که، اگر چه $6 \mid 12$ ولی گروه متناوب ۱۲ عضوی A_4 زیرگروه ۶ عضوی ندارد.

۱۲- فرض کنید G گروهی متناهی است، $N \trianglelefteq G$، و $(|N|, [G:N]) = 1$. ثابت کنید که، برای هر $x \in G$، اگر $x^{|N|} = e$ آنگاه $x \in N$.

۱۳- فرض کنید G گروهی دلخواه، $N \trianglelefteq G$، و $[G:N]$ متناهی باشد. ثابت کنید که اگر $H \leq G$ زیرگروهی متناهی باشد به طوری که $(([G:N],|H|)=1$، آنگاه $H \subseteq N$.

۱۴- فرض کنید G گروهی دلخواه، $N \trianglelefteq G$، و $|N|$ متناهی باشد. ثابت کنید که اگر $H \leq G$ زیرگروهی با اندیس متناهی باشد به طوری که $(([G:H],|N|)=1$، آنگاه $N \subseteq H$.

۱۵- فرض کنید N زیرگروهی دوری و نرمال در G است. ثابت کنید که هر زیرگروه N در G نرمال است.

۱۶- با یک مثال نشان دهید که نرمال بودن زیرگروه‌ها خاصیت تعدی ندارد. یعنی، گروهی با زیرگروه‌های $H, N \leq G$ بیابید به طوری که H در N و N در G نرمال هستند، ولی H در G نرمال نیست.

۱۷- فرض کنید که هر زیرگروه دوری در گروه G نرمال است. نشان دهید که همه‌ی زیرگروه‌های G در آن نرمال هستند.

۱۸- ثابت کنید که اگر N زیرگروهی نرمال از گروه متناهی G باشد و $(([G:N],|N|)=1$، آنگاه N تنها زیرگروه G با مرتبه‌ی $|N|$ است.

۱۹- فرض کنید که عضو a از گروه G دقیقاً دارای دو مزدوج $b^{-1}ab$ و $c^{-1}ac$ است. ثابت کنید که G زیرگروهی سره و نابدیهی نرمال دارد.

۲۰- فرض کنید $H=\{e,a\}$ زیرگروهی از گروه G است. ثابت کنید که $N_G(H)=C_G(H)$ و نتیجه بگیرید که اگر $N_G(H)=G$، آنگاه $H \subseteq Z(G)$.

۲۱- فرض کنید G گروهی متناهی، $N \trianglelefteq G$ از مرتبه‌ی p باشد به طوری که p کوچک‌ترین عدد اولی باشد که $|G|$ را می‌شمارد. ثابت کنید که $N \subseteq Z(G)$.

۲۲- فرض کنید G گروهی متناهی و p کوچک‌ترین عدد اولی باشد که $|G|$ را می‌شمارد. نشان دهید که هر زیرگروه $H \leq G$ با اندیس p در G نرمال است.

۲۳- فرض کنید N زیرگروهی نرمال از گروه G باشد به طوری که $N \cap G' = \{e\}$. ثابت کنید که $N \subseteq Z(G)$ و نتیجه بگیرید که $Z(\frac{G}{N}) = \frac{Z(G)}{N}$.

۲۴- فرض کنید که G گروه، N زیرگروه نرمال G، و $M_1, M_2 \leq G$ شامل N باشند به طوری که $\frac{M_1}{N} = \frac{M_2}{N}$. ثابت کنید که $M_1 = M_2$.

۲۵- مثالی از یک گروه ناآبلی ارایه دهید که همه‌ی زیرگروه‌های آن نرمال باشند.

۲۶- فرض کنید N زیرگروهی نرمال در گروه G باشد و $a \in G$. نشان دهید که مرتبه‌ی aN (به عنوان عضوی از گروه G/N) مرتبه‌ی a را می‌شمارد.

(الف) فرض کنید که $G = < a >$ گروهی دوری از مرتبه‌ی n باشد، $d \mid n$، و $H = < a^d >$. همه‌ی زیرگروه‌های گروه خارج قسمت G / H را تعیین کنید.

(ب) حکم بند **(الف)** را برای $\mathbb{Z}_{36}$ و $H = < 6 >$ بررسی کنید.

۲۷- فرض کنید G گروه، $H, K \leq G$، و K متناهی باشد. ثابت کنید که $[H,K] = \{[h,k] \mid h \in H, k \in K\}$ زیرگروه K است اگر و تنها اگر $H \subseteq N_G(K)$.

۲۸- فرض کنید G گروه، $H, K \leq G$، و $H \subseteq K$. ثابت کنید که $[K,G] \leq H$ اگر و تنها اگر $\frac{K}{H} \subseteq Z(G / H)$.

۲۹- فرض کنید G گروه و $[G, Z(G)] = n$. نشان دهید که G دارای حداکثر n^2 تعویض‌گر متمایز است.

۳۰- فرض کنید G گروه و G' زیرگروه مشتق G از مرتبه‌ی متناهی m باشد. نشان دهید که هر عضو G دارای حداکثر m مزدوج متمایز در G است.

۳۱- فرض کنید G گروهی دلخواه و A گروهی آبلی باشد. ثابت کنید که

(الف) اگر $\varphi : G \to A$ همریختی باشد آنگاه $G' \subseteq Ker\,\varphi$.

(ب) $Hom(G, A) \cong Hom(G / G', A)$.

۳۲- فرض کنید p و q اعدادی اول و G گروهی ناآبلی از مرتبه‌ی pq است. نشان دهید که مرکز G بدیهی است.

۳۳- فرض کنید G گروه است و $H \leq G$. نشان دهید که هسته‌ی H در G، یعنی

$$Cor_G(H) = \bigcap_{g \in G} gHg^{-1}$$

بزرگ‌ترین زیرگروه نرمال در G مشمول در H است.

۹.۲ قضیه‌های اساسی همریختی‌ها

با همریختی‌ها و یک‌ریختی‌های دستگاه‌های جامع جبری در بخش ۵.۱ آشنا شدیم و برخی از ویژگی‌های آن‌ها را در رابطه با گروه‌ها در این فصل دیدیم. یکی از هدف‌های این بخش ارائه‌ی اثبات قضیه‌ی اساسی همریختی‌ها به زبان متداول گروه‌ها است، که حالت کلی آن در قضیه‌ی ۸.۷.۱ برای دستگاه‌های جامع جبری داده شد، و همچنین اثبات قضیه‌های دوم و سوم یک‌ریختی که قول آن را در بخش ۷.۱ دادیم. این قضیه‌های بسیار جالب و مهم در مورد ارتباط بین سه مفهوم زیرگروه نرمال (که در تناظر با همنهشتی‌ها هستند)، گروه خارج قسمتی، و همریختی هستند. از این رو، ابتدا قضیه‌ی زیر را در باره‌ی حفظ و انعکاس زیرگروه‌های نرمال تحت همریختی‌ها می‌آوریم.

۱.۹.۲ قضیه. فرض کنیم $\varphi : G_1 \to G_2$ همریختی گروه‌ها باشد. در این صورت،

۱- همریختی φ زیرگروه‌های نرمال را تا نگاره حفظ می‌کند. یعنی،

$$N \trianglelefteq G_1 \quad \Rightarrow \quad \varphi(N) \trianglelefteq Im\varphi = \varphi(G)$$

۲- همریختی φ زیرگروه‌های نرمال را منعکس می‌کند. یعنی،

$$K \trianglelefteq G_2 \quad \Rightarrow \quad \varphi^{-1}(K) = \check{\varphi}(K) \trianglelefteq G_1$$

اثبات

۱- دانشجویان معمولاً در اثبات این بند مشکلی ندارند. دلیل هر مرحله‌ی زیر را بیان کنید:

$$\begin{aligned}\varphi(g)^{-1}\varphi(n)\varphi(g) &= \varphi(g^{-1})\varphi(n)\varphi(g)\\ &= \varphi(g^{-1}ng) \in \varphi(N)\end{aligned}$$

۲- همان طور که در اثبات زیرگروه بودن $\varphi^{-1}(K)$ در قضیه‌ی ۳.۵.۲ نیز گفتیم، مبتدیان گاهی با نگاره‌ی معکوس اندکی مشکل دارند (البته یقیناً تا بحال ای مشکل احتمالی حل شده است). برای اثبات نرمال بودن، باید نشان دهیم که

$$(\forall g \in G_1) \quad (\forall a \in \check{\varphi}(K)) \quad \Rightarrow \quad g^{-1}ag \in \check{\varphi}(K)$$

یعنی، بنابر تعریف نگاره‌ی معکوس، باید نشان دهیم که $\varphi(g^{-1}ag) \in K$. ولی، چون K در G_2 نرمال است و $\varphi(a) \in K$ (چرا؟) داریم (دلیل هر مرحله‌ی زیر را توضیح دهید)،

$$\varphi(g^{-1}ag)=\varphi(g^{-1})\varphi(a)\varphi(g)=\varphi(g)^{-1}\varphi(a)\varphi(g)\in K$$

بنابراین $\varphi^{-1}(K)=\tilde{\varphi}(K)\leq|G_1$.

برای ادامه‌ی کار، نیاز به معرفی مفهوم **هسته‌ی همریختی**‌های بین گروه‌ها داریم. این مفهوم را برای همریختی‌های $f:A\to B$ بین دستگاه‌های کلی جبری در **۶.۷.۱ به صورت** $\sim_f=K_f=\{(a,a')\in A\times A\mid f(a)=f(a')\}$، یعنی

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

تعریف کردیم و دربحث **۱۲.۷.۱** بدون اثبات بیان کردیم که این تعریف در مورد گروه‌ها معادل با تعریف زیر است.

۲.۹.۲ تعریف. فرض کنیم $f:A\to B$ همریختی گروه‌ها و e_B عضو همانی گروه B باشد. در این صورت، نگاره‌ی معکوس e_B تحت f ، یعنی،

$$f^{-1}(e_B)=\tilde{f}(e_B)=\{a\in A\mid f(a)=e_B\}$$

را (فعلاً) **پوچ‌خانه‌ی** f (و کمی بعد، **هسته‌ی** f) می‌نامیم.

چطور دو مفهوم به ظاهر متفاوت **پوچ‌خانه**‌ی همریختی گروه‌ها (همچنین برای حلقه‌ها، مدول‌ها، و فضاهای برداری) و **هسته**‌ی f معادل هستند؟ لم زیر را ببینید.

۳.۹.۲ لم. *فرض کنیم $f:A\to B$ همریختی گروه‌ها باشد. در این صورت، هسته‌ی f و **پوچ خانه**‌ی f یکدیگر را کاملاً مشخص می‌کنند. به این معنی که،*

۱- رده‌ی شامل عضو همانی e_A، تحت رابطه‌ی هم‌ارزی هسته $\sim_f=K_f$، برابر با پوچ‌خانه‌ی f است:

$$f^{-1}(e_B)=\tilde{f}(e_B)=[e_A]_{\sim_f}$$

۲- پوچ‌خانه‌ی f هسته‌ی f را کاملاً مشخص می‌کند. یعنی

$$a\sim_f a'\Leftrightarrow a*a'^{-1}\in f^{-1}(e_B)$$

اثبات. با کمی دقت به اثبات لم، متوجه می‌شویم که این احکام برای چه دستگاه‌های جبری می‌توانند برقرار باشند.

۱- چون f عضو همانی را حفظ می‌کند، یعنی، $f(e_A)=e_B$ (**چرا؟**)، داریم

$$\begin{aligned} a\in f^{-1}(e_B) &\Leftrightarrow f(a)=e_B \\ &\Leftrightarrow f(a)=f(e_A) \\ &\Leftrightarrow a\sim_f e_A \\ &\Leftrightarrow a\in [e_A]_{\sim_f} \end{aligned}$$

۲- **(به این قسمت بیش‌تر توجه کنید)** چون هر عضو گروه دارای وارون است و همریختی f - وارون‌ها را حفظ می‌کند، داریم

$$\begin{aligned} aK_f a' &\Leftrightarrow f(a)=f(a') \\ &\Leftrightarrow f(a)*f(a')^{-1}=e_B \\ &\Leftrightarrow f(a)*f(a'^{-1})=e_B \\ &\Leftrightarrow f(a*a'^{-1})=e_B \\ &\Leftrightarrow a*a'^{-1}\in f^{-1}(e_B) \end{aligned}$$

با توجه به قضیه‌ی بالا، ریاضی‌دانان اغلب واژه‌ی **هسته** را برای **پوچ‌خانه**‌ی همریختی گروه‌ها (حلقه‌ها، و مدول‌ها) به کار می‌برند، و ما **موقتاً** از واژه‌ی **پوچ‌خانه** استفاده کردیم! همچنین، از این پس نماد **رابطه**‌ی همنهشتی K_f (یا $Kerf$) را برای **زیرگروه** نرمال هسته یا پوچ خانه‌ی همریختی f بین گروه‌ها (و حلقه‌ها در فصل **۳**) نیز به کار می‌بریم، و اشتباهی نیز پیش نمی‌آید. قضیه‌ی مهم و طبیعی زیر را بسیار به کار خواهیم برد.

۴.۹.۲ قضیه. فرض کنیم $N\trianglelefteq G$. در این صورت، تابع طبیعی زیر همریختی پوشای گروه‌ها است:

$$\begin{aligned} \gamma : G &\to G/N \\ x &\mapsto xN \end{aligned}$$

اثبات. نکته‌ی جالب این است که عمل دوتایی روی G/N طوری تعریف شده است که این تابع طبیعی همریختی شود. توجه کنید که

$$\gamma(ab)=abN=(aN)(bN)=\gamma(a)\gamma(b)$$

پوشا بودن γ روشن است.

لم زیر همتای لم های م.۹.۱ و ۷.۷.۱ است.

۵.۹.۲ لم. *فرض کنیم* $\varphi: G_1 \to G_2$ *همریختی گروهی باشد. در این صورت،*

۱- *هسته‌ی* φ *در* G_1 *نرمال است.*

۲- *بر عکس، هر زیرگروه نرمال* G_1 *هسته‌ی یک همریختی با دامنه‌ی* G_1 *است.*

۳- *همریختی* φ *یک به یک است اگر و تنها اگر* $K_\varphi = \{e_1\}$.

اثبات

۱- توجه می‌کنیم که $K_\varphi = \tilde{\varphi}(e_2)$ و $\{e_2\}$ در G_2 نرمال هستند. حال، بند ۲ قضیه‌ی ۱.۹.۲ را به کار ببرید. (تمرین خوبی است که حکم را به طور مستقیم، بدون استفاده از قضیه‌ی ۱.۹.۲، نیز اثبات کنید).

۲- فرض کنیم $N \trianglelefteq G$. ادعا می‌کنیم که N هسته‌ی همریختی طبیعی $\gamma: G \to G/N$ است (مراحل اثبات زیر را توضیح دهید):

$$x \in K_\gamma \Leftrightarrow \gamma(x) = e_{G/N} \Leftrightarrow xN = N \Leftrightarrow x \in N$$

۳- فرض کنیم $K_\varphi = \{e_1\}$. مراحل اثبات یک به یک بودن φ را در زیر توضیح دهید:

$$\begin{aligned}
\varphi(a) = \varphi(b) &\Rightarrow \varphi(a)\varphi(b)^{-1} = e_2 \\
&\Rightarrow \varphi(a)\varphi(b^{-1}) = e_2 \\
&\Rightarrow \varphi(ab^{-1}) = e_2 \\
&\Rightarrow ab^{-1} \in K_\varphi = \{e_1\} \\
&\Rightarrow ab^{-1} = e_1 \\
&\Rightarrow a = b
\end{aligned}$$

بر عکس، فرض کنیم φ یک به یک باشد. حال، مراحل اثبات $K_\varphi = \{e_1\}$ را در زیر توضیح دهید:

$$\begin{aligned}
x \in K_\varphi &\Rightarrow \varphi(x) = e_2 \\
&\Rightarrow \varphi(x) = \varphi(e_1) \\
&\Rightarrow x = e_1
\end{aligned}$$

با توجه به بندهای ۱ و ۲ لم بالا، می‌گوییم که **دو مفهوم زیرگروه نرمال و هسته‌ی همریختی‌ها اساساً یکسان هستند!** قضیه‌ی اساسی همریختی‌های گروه‌ها نیز بیان می‌کند که

تفاوتی اساسی بین گروه‌های خارج قسمتی و همریختی‌های پوشا وجود ندارد! ایـن قضـیه همتای قضیه‌ی اساسی **۶.۷.۱** است.

۶.۹.۲ قضیه(ی اساسی همریختی‌گروه‌ها). *فرض کنیم* $\varphi : G_1 \to G_2$ *همریختی گروهی و* K_φ *هسته‌ی آن باشد. در این صورت،*

$$G_1 / K_\varphi \cong \varphi(G_1)$$

به ویژه، اگر φ *پوشا باشد آنگاه* $G_1 / K_\varphi \cong G_2$.

اثبات. در اثبات قضیه‌ی **م.۱۰.۱** دیدیم که تابع

$$\begin{aligned} \overline{\varphi} : G_1 / K_\varphi &\to \varphi(G_1) \\ xK_\varphi &\mapsto \varphi(x) \end{aligned}$$

خوش‌تعریف، **یک به یک**، و **پوشا** است (**اثبات را در اینجا بنویسید**). کافی است ثابـت کنـیم که $\overline{\varphi}$ همریختی گروهی است، که آن نیز مانند حالت کلی **۸.۷.۱** به راحتی انجام می‌شود. مراحل اثبات زیر را توضیح دهید:

$$\begin{aligned} \overline{\varphi}[(aK_\varphi)(bK_\varphi)] &= \overline{\varphi}(abK_\varphi) \\ &= \varphi(ab) = \varphi(a)\varphi(b) \\ &= \overline{\varphi}(aK_\varphi)\overline{\varphi}(bK_\varphi) \end{aligned}$$

بنابراین، $G_1 / K_\varphi \cong \varphi(G_1)$. حکم آخر قضیه روشن است.

۷.۹.۲ بحث در کلاس

۱- اثبات قضیه‌ی اساسی نشان می‌دهد که نمودار زیر تعویض‌پذیر است، یعنی $\overline{\varphi} \circ \gamma = \varphi$:

$$\begin{array}{ccccc} G_1 & \xrightarrow{\varphi} & \varphi(G_1) & \xrightarrow{i} & G_2 \\ \gamma \searrow & & \nearrow \overline{\varphi} & & \\ & G_1 / K_\varphi & & & \end{array}$$

۲- توجه می‌کنیم که چون γ پوشا و در نتیجه از راست حذف‌پذیر است، $\overline{\varphi}$ با ویژگی $\overline{\varphi} \circ \gamma = \varphi$ منحصر به فرد است. **چطور؟**

۳- اگر φ پوشا باشد آنگاه، چون دامنه‌های φ و γ برابر و نگاره‌های آن‌ها یک‌ریخت هستند، می‌گوییم که هر همریختی پوشا φ اساساً با یک همریختی طبیعی پوشا γ یکسان است، و این مطلب اهمیت همریختی‌های طبیعی γ را نشان می‌دهد!

۴- مثال‌های داده شده در بحث ۱۱.۷.۱ را یک‌بار دیگر ببینید.

۵- در بند ۵(ت) بحث ۲.۵.۲ دیدیم که تابع دترمینان از گروه ضربی **خطی عام** $GL(n,\mathbb{R})$ به گروه ضربی اعداد حقیقی $(\mathbb{R}^*;\cdot)$ همریختی است. این همریختی پوشا است. **چطور؟** همچنین هسته‌ی آن برابر است با

$$\begin{aligned} K_{\det} &= \{A \in GL(n,\mathbb{R}) \mid \det A = 1\} \\ &= SL(n,\mathbb{R}) \end{aligned}$$

در نتیجه، بنابر قضیه‌ی اساسی همریختی گروه‌ها،

$$GL(n,\mathbb{R}) / SL(n,\mathbb{R}) \cong \mathbb{R}^* .$$

دو قضیه‌ی مهم دیگر که مشابه با قضیه‌ی اساسی هستند پایان بخش این فصل است. برخی قضیه‌ی اساسی را اولین قضیه‌ی یک‌ریختی می‌نامند. از این رو دو قضیه‌ای را که می‌آوریم، دومین و سومین می‌نامیم. برای بیان هر یک نیاز به آوردن لم‌هایی است که مربوط به آن قضیه نیز هستند. تکرار می‌کنیم که در اینجا اغلب با مجموعه‌ای متشکل از مجموعه‌ها سر و کار داریم و نیاز به توجه بیشتری است.

۸.۹.۲ لم. فرض کنیم G گروه و H، N زیرگروه آن باشند به طوری که $N \trianglelefteq G$. در این صورت،

۱- اشتراک $H \cap N$ درگروه G و در نتیجه در H نیز نرمال است.

۲- HN زیرگروه G است و $N \trianglelefteq HN$.

۳- اگر H نیز در G نرمال باشد، آنگاه $HN \trianglelefteq G$.

اثبات. تمرین ۹ بخش ۸.۲ را ببینید.

۹.۹.۲ بحث در کلاس. با توجه به بند ۲ لم بالا، گروه خارج قسمتی HN / N وجود دارد. دومین قضیه‌ی یک‌ریختی بیان می‌کند که این گروه با چه گروهی یک‌ریخت است. شاید بگویید، با حذف N از صورت و مخرج، با H یک‌ریخت است!

۱۰.۹.۲ قضیه(ی دوم یکریختی). فرض کنیم H و N زیرگروه G باشند و $N \trianglelefteq G$. در این صورت،

$$\frac{HN}{N} \cong \frac{H}{H \cap N}$$

اثبات. اثبات این قضیه برایتان چندان مشکل نیست. خلاصه‌ای را از دو روش اثبات برای این قضیه می‌آوریم. روش اول فنی‌تر است و قضیه‌ی اساسی را به کار می‌برد.

روش اول: ابتدا به آسانی می‌توانید نشان دهید که تابع زیر همریختی پوشا است:

$$\begin{aligned} \Phi : H &\to \frac{HN}{N} \\ h &\mapsto heN = hN \end{aligned}$$

حال هسته‌ی آن را محاسبه می‌کنیم (یادآوری می‌کنیم که N عضو همانی گروه HN/N است. مراحل زیر را توضیح دهید):

$$\begin{aligned} K_\Phi &= \{h \in H \mid \Phi(h) = e_{HN/N}\} \\ &= \{h \in H \mid hN = N\} \\ &= \{h \in H \mid h \in N\} = H \cap N \end{aligned}$$

سرانجام می‌گوییم که بنابر قضیه‌ی اساسی، $H/K_\Phi \cong HN/N$، یعنی

$$\frac{H}{H \cap N} \cong \frac{HN}{N}$$

روش دوم: (اختیاری) نشان دهید که تابع زیر خوش‌تعریف، همریختی، و دوسویی است:

$$\begin{aligned} \Psi : \frac{H}{H \cap N} &\to \frac{HN}{N} \\ h(H \cap N) &\mapsto heN = hN \end{aligned}$$

مراحل اثبات خوش‌تعریفی را، که در زیر می‌آوریم، توضیح دهید: برای $h_1, h_2 \in H$، داریم

$$\begin{aligned} h_1(H \cap N) = h_2(H \cap N) &\Rightarrow h_2^{-1}h_1 \in H \cap N \\ &\Rightarrow h_2^{-1}h_1 \in N \\ &\Rightarrow h_1N = h_2N \end{aligned}$$

بقیه‌ی اثبات را به عنوان تمرین به عهده‌ی شما **عزیزان** می‌گذاریم.

۱۱.۹.۲ بحث در کلاس. بنابر قضیه‌ی دوم یک‌ریختی، داریم

$$\frac{4\mathbb{Z}}{4\mathbb{Z}\cap 6\mathbb{Z}} \cong \frac{4\mathbb{Z}+6\mathbb{Z}}{6\mathbb{Z}}$$

یعنی، $2\mathbb{Z}/6\mathbb{Z} \cong 4\mathbb{Z}/12\mathbb{Z}$.

قضیه‌ی سوم یک‌ریختی در باره‌ی خارج قسمت گروه خارج قسمتی G/N است. ابتدا قضیه‌ی مهم زیر را ببینید که شکل زیرگروه‌ها و زیرگروه‌های نرمال G/N را مشخص می‌کند. این قضیه را **قضیه‌ی تناظر** یا **قضیه‌ی چهارم یک‌ریختی** نیز می‌نامند. این قضیه نشان می‌دهد که **تناظری دوسویی** بین مجموعه‌ی زیرگروه‌های گروه خارج قسمتی G/N، یعنی $Sub(G/N)$، و زیرگروه‌های G که شامل N هستند، یعنی $\{H \leq G \mid N \subseteq H\}$، وجود دارد. به همین صورت، **تناظری دوسویی** بین مجموعه‌ی زیرگروه‌های **نرمال** گروه خارج قسمتی G/N، یعنی $Nor(G/N)$، و زیرگروه‌های **نرمال** G که شامل N هستند، یعنی $\{H \trianglelefteq G \mid N \subseteq H\}$، وجود دارد.

۱۲.۹.۲ قضیه (**قضیه‌ی تناظر**). فرض کنیم G گروه و N زیرگروه نرمال G باشد. در این صورت،

۱- $\mathcal{T}$ زیرگروه G/N است اگر و تنها اگر $\mathcal{T} = H/N$ که در آن $N \leq H \leq G$.

۲- $\mathcal{T}$ زیرگروه نرمال G/N است اگر و تنها اگر $\mathcal{T} = H/N$ که در آن $N \trianglelefteq H \trianglelefteq G$.

اثبات. اگر چه اثبات این قضیه چندان مشکل نیست، جزییات قسمت‌هایی از آن را برای آموزش می‌آوریم.

۱-(الف) ابتدا فرض می‌کنیم $N \leq H \leq G$ و نشان می‌دهیم که H/N زیرگروه G/N است. روشن است که عضو همانی گروه G/N، یعنی $eN = N$، متعلق به H/N است، زیرا $e \in H$. حال، فرض کنیم $xN, yN \in H/N$، که در آن $x, y \in H$. چون $xy^{-1} \in H$، پس

$$(xN)(yN)^{-1} = (xN)(y^{-1}N) = xy^{-1}N \in H/N$$

(ب) برعکس، فرض کنیم $\mathcal{T}$ زیرگروه G/N باشد. (توجه می‌کنیم که $\mathcal{T}$ مجموعه‌ای از مجموعه‌های به صورت aN است). ادعا می‌کنیم که زیرگروه H از گروه G وجود دارد که شامل

N اســـت و $\mathcal{T} = H/N = \{hN \mid h \in H\}$. حـــدس مـــی زنیـــد کـــه چـــون $\mathcal{T} = \{aN, bN, \ldots\}$، H کدام زیرمجموعه‌ی G ممکن است باشد؟ درست حـدس زده‌ایـد، اجتماع عضوهای $\mathcal{T}$:

$$H = \{a \in G \mid aN \in \mathcal{T}\}$$
$$= \bigcup \mathcal{T} = \bigcup_{aN \in \mathcal{T}} aN$$

حال به راحتی می توانید ادعای بالا را اثبات کنید. (توجه کنید که، پـس از اثبـات زیرگـروه بـودن H در G و $N \subseteq H$، روشن است که چون N در G نرمال است، پـس در جـای کوچـک‌تـر H نیز نرمال است).

۲- اثبات این حکم مشابه حکم **۱** است. در قسمت **(الف)** باید نشان دهیم که اگر H در G نرمال باشد، آنگاه H/N در G/N نرمال است. برای اثبات این مطلـب، توجـه کنیـد کـه بـرای هـر $x \in G$ و هر $h \in H$، داریم $xhx^{-1} \in H$ و در نتیجه

$$(xN)(hN)(xN)^{-1} = (xN)(hN)(x^{-1}N) = (xhx^{-1})N \in H/N$$

برعکس، در قسمت **(ب)** باید اثبات کنیم که اگر $\mathcal{T}$ زیرگروه نرمال G/N باشد، آنگاه

$$H = \{a \in G \mid aN \in \mathcal{T}\}$$

در G نرمال است. بـرای اثبـات ایـن مطلـب، فـرض مـی‌کنـیم $x \in G$ و $a \in H$، و در نتیجـه $aN \in \mathcal{T}$. در این صورت، بنابر نرمال بودن $\mathcal{T}$ در G/N، داریم

$$(xN)(aN)(xN)^{-1} \in \mathcal{T} \Rightarrow (xax^{-1})N \in \mathcal{T} \Rightarrow xax^{-1} \in H$$

و بنابراین قضیه اثبات شده است.

۱۳.۹.۲ قضیه (**سوم یکریختی**). فرض کنیم H و N زیرگروه‌هایی نرمال از G باشند به طوری که $N \subseteq H$. در این صورت،

$$\frac{G/N}{H/N} \cong G/H$$

اثبات. ابتدا، با توجه به نرمال بودن H و N در G، گـروه‌هـای خـارج قسـمتی G/H و G/N با معنی هستند. همچنین، با توجـه بـه قضـیه‌ی تنـاظر **۱۲.۹.۲**، H/N در G/N

نرمال، و در نتیجه گروه خارج قسمتی $\frac{G/N}{H/N}$ نیز با معنی، والبته هر عضو آن به صورت $(gN)(H/N)$ است.

حال، مشابه اثبات قضیه‌ی دوم یک‌ریختی، قضیه را به دو صورت زیر می‌توان اثبات کرد.

روش اول: ابتدا نشان دهید که تابع

$$\begin{aligned}\varphi : G/N &\to G/H \\ gN &\mapsto gH\end{aligned}$$

خوش‌تعریف، همریختی، و پوشا است. حال توضیح دهید که

$$\begin{aligned}Ker\varphi &= \{gN \in G/N \mid \varphi(gN) = gH = 0_{G/H} = H\} \\ &= \{gN \mid g \in H\} = H/N\end{aligned}$$

در پایان، قضیه‌ی اساسی همریختی‌ها را به کار ببرید.

روش دوم: نشان دهید که تابع زیر یک همریختی دوسویی است:

$$\begin{aligned}\psi : \frac{G/N}{H/N} &\to G/H \\ (gN)(H/N) &\mapsto gH\end{aligned}$$

اثبات خوش‌تعریفی ψ را در زیر توضیح و بقیه اثبات را ارائه دهید:

$$\begin{aligned}(g_1N)(H/N) = (g_2N)(H/N) &\Rightarrow (g_1N)(g_2N)^{-1} \in H/N \\ &\Rightarrow (g_1 g_2^{-1})N \in H/N \\ &\Rightarrow g_1 g_2^{-1} \in H \\ &\Rightarrow g_1 H = g_2 H\end{aligned}$$

۱۴.۹.۲ گروه‌های ساده. (اختیاری) یادآوری می‌کنیم که هر عدد اول p مقسوم علیهی بجز ۱ و p ندارد. از دو تعبیر این واقعیت به زبان گروه‌ها، یکی این است که هیچ زیرگروه (نرمال) $\mathbb{Z}$ بجز $\mathbb{Z}$ و $p\mathbb{Z}$ گروه $p\mathbb{Z}$ را شامل نمی‌شود، و دیگری اینکه گروه $\mathbb{Z}_p$ (که با $\mathbb{Z}/p\mathbb{Z}$ یک‌ریخت است) زیرگروهی (نرمال) بجز $\{0\}$ و خودش ندارد. قبل از بیان همتای این مفاهیم برای گروه‌های دلخواه، حالت کلی آن‌ها را برای دستگاه‌های جامع جبری از فصل ۱ یادآوری تا زیربنای این مفاهیم را بیاموزید و خودتان هنگام نیاز سازنده باشید.

۱۵.۹.۲ تعریف. فرض کنیم θ رابطه‌ای همنهشتی روی دستگاه جبری A باشد. در این صورت،

۱- رابطه‌ی θ را رابطه‌ی همنهشتی **ماکسیمال** روی A می‌گوییم اگر $\theta \neq \nabla (= A\times A)$ و هیچ رابطه‌ی همنهشتی بجز ∇ و θ رابطه‌ی θ را شامل نشود. یعنی، برای هر رابطه‌ی همنهشتی $\sim$ روی A،

$$\theta \subseteq \sim \subseteq \nabla \quad \Rightarrow \theta = \sim \quad \vee \quad \sim = \nabla$$

۲- دستگاه جبری نابدیهی A را **ساده** می‌گوییم اگر Δ و ∇ تنها رابطه‌های همنهشتی روی A باشند؛ یعنی، $Con(A) = \{\Delta, \nabla\}$.

با توجه به اینکه در گروه‌ها، زیرگروه‌های نرمال همتای رابطه‌های همنهشتی هستند، به راحتی می‌توانید تعبیر این مفاهیم را برای گروه‌ها به صورت زیر بیان کنید.

۱۶.۹.۲ تعریف. فرض کنید M زیرگروه نرمال گروه G است. در این صورت،

۱- M را زیرگروه نرمال **ماکسیمال** G می‌گوییم اگر $M \neq G$ و هیچ زیرگروه نرمالی از G، بجز G و M آن را شامل نشود. یعنی، برای هر زیرگروه نرمال H از G،

$$M \subseteq H \subseteq G \quad \Rightarrow \quad M = H \quad \vee \quad H = G$$

۲- گروه نابدیهی G را **ساده** می‌گوییم اگر G و $\{e\}$ تنها زیرگروه‌های نرمال آن باشند. یعنی، $Nor(G) = \{\{e\}, G\}$.

۱۷.۹.۲ بحث در کلاس

۱- زیرگروه متناوب A_3 در S_3 نرمال ماکسیمال است. توجه کنید که هر سه گروه $\{\rho_0, \mu_1\}$، $\{\rho_0, \mu_2\}$، $\{\rho_0, \mu_3\}$ در S_3 ماکسیمال هستند ولی **نرمال** ماکسیمال نیستند. **چطور؟** هر سه گروه $\{e, a\}$، $\{e, b\}$، و $\{e, c\}$ زیرگروه نرمال ماکسیمال گروه کلاین K_4 هستند (یادآوری می‌کنیم که هر زیرگروه از یک گروه آبلی، نرمال نیز هست). برای هر عدد اول p، زیرگروه $p\mathbb{Z}$ در گروه $\mathbb{Z}$ نرمال ماکسیمال است. زیرگروه $\{0\}$ در هر $\mathbb{Z}_p$ نرمال ماکسیمال است. گروه $(\mathbb{Q}; +)$ زیرگروه نرمال ماکسیمال ندارد. **چرا؟**

۲- مثال‌های بند ۱ نشان می‌دهند که یک گروه ممکن است هیچ زیرگروه نرمال ماکسیمال نداشته باشد یا بیش از یکی داشته باشد. ولی، هر گروه متناهی نابدیهی G دست کم دارای یک زیرگروه نرمال ماکسیمال است. (راهنمایی: روند زیر را ادامه دهید و از متناهی بودن G به نتیجه‌ی

مطلوب برسید. اگر $N_1 = \{e\}$ در G نرمال ماکسیمال نباشد، زیرگروه نرمال N_2 از G وجود دارد به طوری که $N_1 \subset N_2 \subset G$).

۳- بنابر قضیه‌ی لاگرانژ،گروه $\mathbb{Z}_n$ ساده است اگر و تنها اگر n اول باشد (چرا؟). روشن است که گروه $\mathbb{Z}$ ساده نیست؛ زیرا، برای هر عدد طبیعی $n \neq 1$، $n\mathbb{Z}$ یک زیرگروه نرمال $\mathbb{Z}$ است. در واقع، گروه آبلی نابدیهی G ساده است اگر و تنها اگر دوری و یکریخت با $\mathbb{Z}_p$ باشد. زیرا، چون G ساده است، برای هر $g \neq 0$ در G، $G = < g >$ (چرا؟) و در نتیجه، G دوری است. حال، چون $G \ncong \mathbb{Z}$ (چرا؟)، پس $G \cong \mathbb{Z}_p$. چرا؟

۴- این مطلب را اثبات نمی‌کنیم که برای هر $n \geq 5$، گروه متناوب (ناآبلی) A_n ساده است. این گروه‌ها از اولین مثال‌های گروه‌های ساده بودند که گالوا برای اثبات قضیه‌ی بسیار مهم خود از آن‌ها استفاده کرد. قضیه‌ی جالب گالوا را در درس بعدی جبر یا در درس نظریه‌ی گالوا خواهید دید. این قضیه بیان می‌کند که ریشه‌های چندجمله‌ای‌های از درجه‌ی ۵ و بیشتر را لزوماً نمی‌توان با فرمولی رادیکالی به دست آورد (مانند $x = -b \pm \sqrt{b^2 - 4ac}\ /2a$ برای ریشه‌های معادله‌ی درجه‌ی دوم $ax^2 + bx + c = 0$)!

۵- دیدیم که گروه خارج قسمتی $\mathbb{Z} / n\mathbb{Z} \cong \mathbb{Z}_n$ ساده است اگر و تنها اگر n اول باشد. قضیه‌ی پایانی این بخش این مطلب را در حالت کلی اثبات می‌کند. (مطالعه‌ی بیش‌تر و جامع‌تر گروه‌های ساده خارج از بحث این کتاب و درس مبانی جبر است).

۱۸.۹.۲ قضیه. فرض کنیم M زیرگروه نرمال گروه G است. در این صورت، گروه G / M ساده است اگر و تنها اگر M زیرگروه نرمال ماکسیمال G باشد.

اثبات. بنابر قضیه‌ی تناظر **۱۲.۹.۲**،

$$Nor(G / M) \cong \{N \in Nor(G) \mid M \subseteq N\}$$

از طرفی، G / M ساده است اگر و تنها اگر $Nor(G / M) = \{\{M\}, G / M\}$ و M زیرگروه نرمال ماکسیمال G است اگر و تنها اگر $\{N \in Nor(G) \mid M \subseteq N\} = \{M, G\}$. این مطالب قضیه را اثبات می‌کند. چطور؟ تمرین خوبی است که قضیه را به طور مستقیم نیز اثبات کنید.

تمرین ۹.۲

تلاش برای حل کردن تمرین‌ها نه تنها آموزنده است، لذت بخش نیز هست

دسته اول

۱- زیرگروه‌هایی چون H و K از گروه $G=\mathbb{Z}_2\times\mathbb{Z}_4$ بیابید به طوری که $H\cong K$ ولی $G/H\ncong G/K$.

۲- زیرگروه‌هایی چون H و K از گروه $G=\mathbb{Z}_2\times\mathbb{Z}_4$ بیابید به طوری که $H\ncong K$ ولی $G/H\cong G/K$.

۳- نشان دهید که $Inn(G)\cong G/Z(G)$.

۴- نشان دهید که زیرگروه N در گروه G نرمال است اگر و تنها اگر تحت هر خودریختی درونی $\psi_a\in Inn(G)$ پایا (ناوردا) باشد. یعنی، $\psi_a(N)\subseteq N$.

۵- فرض کنید که G گروه و $G=HK$، که در آن $H,K\leq G$. ثابت کنید که $\frac{G}{H\cap K}\cong\frac{G}{H}\times\frac{G}{K}$.

۶- فرض کنید G گروهی متناهی و $f:G\to H$ همریختی باشد. ثابت کنید که $|f(G)|\,|\,|G|$.

دسته دوم

۷- می‌گوییم که زیرگروه H در G **ویژه** یا **مشخصه** است، و می‌نویسیم $H\overset{c}{\leq}G$، اگر تحت **هر** خودریختی دلخواه $\varphi:G\to G$ پایا (ناوردا) باشد؛ یعنی، $\varphi(H)\subseteq H$. روشن است که هر زیرگروه مشخصه در G نرمال است (**چرا؟**). نشان دهید که عکس این مطلب لزوماً درست نیست.

۸- نشان دهید که $Z(G)$ و G' در گروه G مشخصه هستند.

۹- فرض کنید G گروه، $N\overset{c}{\leq}G$، و $H\overset{c}{\leq}N$. ثابت کنید که $H\overset{c}{\leq}G$.

۱۰- فرض کنید G گروه، $N\leq G$ و $H\overset{c}{\leq}N$. ثابت کنید که $H\leq G$.

۱۱- فرض کنید G گروهی متناهی باشد و $H\leq G$. نشان دهید که اگر $(|H|,[G:H])=1$، آنگاه $H\overset{c}{\leq}G$.

۱۲- فرض کنید G گروه، $H,K\overset{c}{\leq}G$، و $G=H\times K$. ثابت کنید که

$$Aut(G)\cong Aut(H)\times Aut(K)$$

۱۳- فرض کنید G گروه و $f:G\to G$ همریختی است به طوری که $f^2=f$ و $\operatorname{Im} f \leq G$. ثابت کنید که $G\cong \operatorname{Im} f \times Kerf$.

۱۴- فرض کنید S_n گروه متقارن و H زیرگروه تولید شده توسط ترانهش‌های $(i,i+1)$ باشد که در آن $1\le i\le n-1$. تعیین کنید که HA_n/A_n با کدام گروه شناخته شده‌ای یک‌ریخت است.

۱۵- فرض کنید G یک گروه و $G'\subseteq Z(G)$. ثابت کنید که برای هر $a\in G$، $C_G(a)\leq G$ و $G/C_G(a)$ با زیرگروهی از G' یک‌ریخت است.

۱۶- گروه G را **شبه آبلی** می‌گوییم اگر دارای یک زیرگروه آبلی نرمال N باشد به طوری که G/N نیز آبلی است.

(الف) مثالی از یک گروه شبه آبلی ارائه دهید که آبلی نباشد.

(ب) فرض کنید $\varphi:G\to K$ یک همریختی پوشا و G شبه آبلی باشد. نشان دهید که K نیز شبه آبلی است.

۱۷- فرض کنید $f:G_1\to G_2$ یک همریختی بین گروه‌ها است و $H\leq G_1$. نشان دهید که اگر $f|_H:H\to G_2$ یک‌ریختی باشد آنگاه $G_1\cong H\times Kerf$.

۱۸- (**تعمیم قضیه‌ی اساسی همریختی**) فرض کنید $f:A\to B$ و $g:A\to C$ همریختی بین گروه‌ها باشند به طوری که g پوشا است. نشان دهید که

(الف) همریختی f از طریق g تجزیه می‌شود (یعنی، همریختی $\overline{f}:C\to B$ با ویژگی $f=\overline{f}\circ g$ وجود دارد) اگر و تنها اگر $K_g\subseteq K_f$.

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

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

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

(ث) قضیه‌ی اساسی همریختی گروه‌ها حالت خاص این قضیه است.