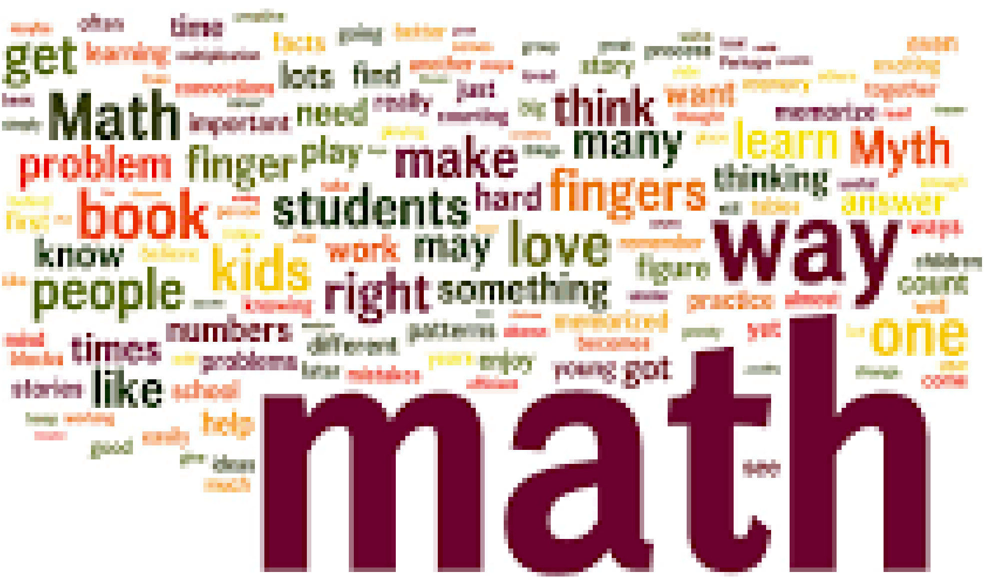
دانشگاه صنعتی اصفهان

دانشکده علوم ریاضی

مبانی جبر (دوره کارشناسی)

محمود بهبودی[1]



۲۸ اردیبهشت ۱۳۹۸

[1] دانشیار دانشکده ریاضی دانشگاه صنعتی اصفهان

این نوشتار جهت استفاده دانشجویان کارشناسی دانشکده ریاضی دانشگاه صنعتی اصفهان آماده شده است و استفاده از آن برای دیگر موسسات آموزش عالی و دانشجویان بلامانع است.

باعث افتخار نویسنده است که نقدها، ایرادات و پیشنهادهای خود را به آدرس ایمیل زیر ارسال نمایید.

mbehbood@cc.iut.ac.ir

مقدمه

متن پیش‌رو حاصل چندین سال تجربه تدریس جبر اینجانب برای دانشجویان دوره کارشناسی دانشکده ریاضی دانشگاه صنعتی اصفهان است...

فهرست مطالب

فصل ۱

یادآوری برخی مفاهیم مقدماتی

در این فصل به صورت خلاصه مفاهیم پایه‌ای و از قبل دانسته شده را یادآوری خواهیم کرد. بیشتر حجم این بخش مربوط به درس مبانی ریاضی است. اگر دانشجویی احساس تسلط بر مبانی ریاضی دارد می‌تواند از این فصل چشم پوشی نماید و به صورت مستقیم وارد فصل دوم شود. باید این مطلب را ذکر کنیم که مطالب این فصل به صورت فهرست‌وار آمده‌اند و برای دیدن جزییات بیشتر و مثال‌ها به کتاب‌های مربوطه مراجعه نمایید.

۱.۱ مجموعه‌ها، رابطه‌ها، تابع‌ها، عدد اصلی یک مجموعه

از مفاهیم اساسی در ریاضیات مجموعه‌ها هستند. در این بخش ما وارد جزییات بعضا فلسفی نظریه مجموعه‌ها نمی‌شویم. همانطور که بارها گفته شده است مجموعه از مفاهیم تعریف ناپذیر است. این بخش را با تعریف زیر شروع می‌کنیم که بیان نادقیقی از مجموعه است.

تعریف ۱.۱.۱. *مجموعه دسته‌ای از اشیا است که این اشیا به صورت دقیق مشخص و تکراری نیستند. معمولا مجموعه‌ها با حروف انگلیسی بزرگ نمایش داده می‌شوند.*

نمادگذاری ۲.۱.۱. *اگر X یک مجموعه باشد و x عنصری از X باشد گوییم x متعلق به X است و با $x \in X$ نشان می‌دهیم. مجموعه که هیچ عضوی ندارد را مجموعه تهی گوییم و با $\emptyset$ نشان می‌دهیم. اگر x عضوی از X نباشد می‌نویسیم $x \notin X$.*

تعریف ۳.۱.۱. *فرض کنیم A و B دو مجموعه باشند. اگر هر عضو از A در B باشد آنگاه گوییم A زیرمجموعه B است و با $A \subseteq B$ نشان می‌دهیم. اگر $A \subseteq B$ و $B \subseteq A$ آنگاه گوییم A و B دو مجموعه یکسان هستند و با $A = B$ نشان می‌دهیم. اگر $A \subseteq B$ و B عضوی داشته باشد که در A نیست، آنگاه گوییم A زیرمجموعه سره B است و با $A \subsetneq B$ نمایش می‌دهیم.*

تعریف ۴.۱.۱. *فرض کنیم X و Y دو مجموعه باشند. مجموعه همه زوج‌های مرتب (x, y) را که $x \in X$ و $y \in Y$ است حاصل ضرب دکارتی دو مجموعه گوییم و با $A \times B$ نشان می‌دهیم. به*

عبارت دیگر
$$A \times B = \{(x,y) \mid x \in X,\ y \in Y\}.$$

تعریف ۵.۱.۱. فرض کنیم A و B دو مجموعه باشند. به هر زیرمجموعه از $A \times B$ مانند R یک رابطه از A به B گوییم. مفهوم $(x,y) \in R$ را با xRy نشان می‌دهیم. اگر $A = B$ باشد آنگاه R را رابطه‌ایی روی A گوییم.

تعریف ۶.۱.۱. فرض کنیم X یک مجموعه و R رابطه‌ای روی X باشد. گوییم:
(۱) R انعکاسی (بازتابی) است هرگاه برای هر $x \in X$ داشته باشیم xRx.
(۲) R متقارن است هرگاه برای هر $x, y \in X$ که xRy نتیجه شود yRx.
(۳) R پاد متقارن است هرگاه برای هر $x, y \in X$ که xRy و yRx نتیجه شود $x = y$.
(۴) R متعدی است هرگاه برای هر $x, y, z \in X$ که xRy و yRz نتیجه شود xRz.

تعریف ۷.۱.۱. گوییم رابطه R روی X هم ارزی است هرگاه بازتابی، متقارن و متعدی باشد.

تعریف ۸.۱.۱. گوییم رابطه R روی X ترتیب جزیی است هرگاه بازتابی، پاد متقارن و متعدی باشد. به مجموعه X مرتب جزیی گوییم هرگاه رابطه R ترتیب جزیی باشد.

تعریف ۹.۱.۱. فرض کنیم رابطه R روی X ترتیب جزیی باشد. اگر برای هر $x, y \in X$ داشته باشیم xRy یا yRx آنگاه ترتیب جزیی را کلا مرتب یا زنجیر نامیم.

تعریف ۱۰.۱.۱. فرض کنیم R یک رابطه هم ارزی روی X باشد و $a \in X$. منظور از کلاس یا رده a تحت R که آن را با $[a]$ یا $\bar{a}$ نشان می‌دهیم، یعنی مجموعه زیر

$$[a] = \bar{a} = \{x \in X \mid xRa\}.$$

زیرمجموعه A از X را یک کلاس یا رده هم ارزی R در X گوییم هرگاه $a \in X$ موجود باشد که $A = \bar{a}$. مجموعه همه کلاس‌های هم ارزی R در X را مجموعه خارج قسمتی نامیم و با X/R نشان می‌دهیم. به عبارت دیگر

$$X/R = \{A \subseteq X \mid A = \bar{a} \text{ باشد که } X \text{ ای در } a\}.$$

تعریف ۱۱.۱.۱. فرض کنیم X یک مجموعه و $\mathcal{A}$ مجموعه‌ای باشد که عناصر آن زیرمجموعه‌های ناتهی از Xاند. اگر عنصرهای $\mathcal{A}$ دو به دو جدا از هم باشند و اجتماع آنها X باشد آنگاه به $\mathcal{A}$ یک افراز گوییم.

قضیه ۱۲.۱.۱. فرض کنیم R یک رابطه هم ارزی روی X باشد. در این صورت X/R یک افراز برای X است.

قضیه ۱۳.۱.۱. فرض کنیم $\mathcal{A}$ یک افراز برای X باشد. در این صورت رابطه هم ارزی R روی X چنان وجود دارد که $X/R = \mathcal{A}$.

قضیه ۱۴.۱.۱. فرض کنیم $\mathcal{A} = \{A_۱, ..., A_n\}$ یک افراز برای X باشد. در این صورت $|X| = \sum_{i=۱}^{n} |A_i|$.

تعریف ۱۵.۱.۱. فرض کنیم f یک رابطه از مجموعه A به مجموعه B باشد. گوییم رابطه f یک تابع است هرگاه برای هر $a \in A$ دقیقا یک $b \in B$ موجود باشد که xfy. اگر f تابعی از A به B باشد آنگاه می‌نویسیم $f : A \longrightarrow B$ یا $A \xrightarrow{f} B$. به A **دامنه** و به B **برد** گوییم. اگر xfy آنگاه می‌نویسیم $y = f(x)$ و به x پیش تصویر y و به y تصویر x گوییم.

تعریف ۱۶.۱.۱. به تابع $f : X \longrightarrow X$ که $f(x) = x$ تابع همانی گوییم و با id_X یا id نمایش می‌دهیم.

تعریف ۱۷.۱.۱. اگر $A \subseteq X$ باشد آنگاه به تابع $i : A \longrightarrow X$ که $i(a) = a$ تابع شمول گوییم.

تعریف ۱۸.۱.۱. فرض کنیم که $f : A \longrightarrow B$ یک تابع باشد. زیرمجموعه‌ای از B که تمام عناصر آن تصویری عنصر از A هستند تصویر f گویند و با $Im(f)$ نشان می‌دهند (دقت شود که برد تابع B است).

نمادگذاری ۱۹.۱.۱. منظور از نماد B^A یعنی مجموعه همه تابع‌ها از A به B.

تذکر ۲۰.۱.۱. اگر A مجموعه تهی باشد و B مجموعه دلخواه (حتی تهی) آنگاه فقط یک تابع از A به B وجود دارد. اما هیچ تابعی از B به A وجود ندارد (چرا؟).

تعریف ۲۱.۱.۱. تابع $f : A \longrightarrow B$ را یک‌به‌یک گوییم هرگاه برای هر $a, a' \in A$ که $f(a) = f(a')$ نتیجه شود که $a = a'$. گوییم f تابع پوشا است هرگاه برای هر $b \in B$ عنصر a در A وجود داشته باشد که $f(a) = b$. تابع f را تناظر گوییم هرگاه هم یک‌به‌یک و هم پوشا باشد. تناظرها را جایگشت نیز می‌نامیم.

قضیه ۲۲.۱.۱. فرض کنیم $f : X \longrightarrow Y$ یک تابع پوشا باشد. در این صورت

$$f^{-۱}(y) = \{x \in X \mid f(x) = y\}$$

یک افراز برای X است که در آن $y \in Y$.

قضیه ۲۳.۱.۱. اگر X مجموعه متناهی و $f : X \longrightarrow X$ یک تابع یک‌به‌یک باشد آنگاه f تناظر است.

تعریف ۲۴.۱.۱. فرض کنیم $f : A \longrightarrow B$ و $g : B \longrightarrow C$ دو تابع باشند. در این صورت منظور از ترکیب f با g یعنی تابع $h : A \longrightarrow C$ که $h(x) = g(f(x))$. تابع h را با gof یا gf نیز نمایش می‌دهیم.

قضیه ۲۵.۱.۱. ترکیب تابع‌ها (اگر مجاز باشیم) شرکت پذیر است یعنی اگر $f : A \longrightarrow B$، $g : B \longrightarrow C$ و $h : C \longrightarrow D$ آنگاه $h(gf) = (hg)f$.

قضیه ۲۶.۱.۱. *ترکیب توابع یک‌به‌یک (پوشا) یک تابع یک‌به‌یک (پوشا) است.*

تعریف ۲۷.۱.۱. *گوییم تابع $f : A \longrightarrow B$ دارای وارون است (وارون‌پذیر است) هرگاه تابع $g : B \longrightarrow A$ موجود باشد که $fg = id_B$ و $gf = id_A$. تابع g را با f^{-1} نشان می‌دهیم.*

قضیه ۲۸.۱.۱. *تابع f وارون‌پذیر است اگر و تنها اگر f تناظر باشد.*

تعریف ۲۹.۱.۱. *گوییم دو مجموعه X و Y همتوان هستند هرگاه یک تناظر بین X و Y موجود باشد. این مطلب را با $X \cong Y$ نشان می‌دهیم.*

تعریف ۳۰.۱.۱. *گوییم دو مجموعه X و Y دارای عدد اصلی یکسان (کاردینالیتی یکسان) هستند هرگاه همتوان باشند. عدد اصلی مجموعه X را با $|X|$ نشان می‌دهیم.*

نمادگذاری ۳۱.۱.۱. *عدد اصلی $\mathbb{N}$ را با $\aleph_0$ نمایش می‌دهیم (بخوانید "الف صفر").*

تعریف ۳۲.۱.۱. *گوییم مجموعه ناتهی X تعداد متناهی عضو دارد هرگاه عدد طبیعی n موجود باشد که یک تناظر بین X و $\{1, ..., n\}$ وجود داشته باشد. مجموعه‌ای که متناهی نباشد را نامتناهی گوییم. گوییم مجموعه X شمارا (شمارش پذیر) است هرگاه $|X| = \aleph_0$.*

قضیه ۳۳.۱.۱. *عدد اصلی $\mathbb{Z}$ و $\mathbb{Q}$ برابر $\aleph_0$ است.*

قضیه ۳۴.۱.۱. *هر زیرمجموعه یک مجموعه شمارا، متناهی یا شمارا است.*

قضیه ۳۵.۱.۱. *حاصل ضرب دکارتی و اجتماع مجموعه‌های شمارا، شمارا هستند.*

تعریف ۳۶.۱.۱. *مجموعه‌ای که شمارا نباشد را ناشمارا (شمارش ناپذیر) گوییم.*

قضیه ۳۷.۱.۱. *$\mathbb{R}$ ناشمارا است و $|\mathbb{R}| = 2^{\aleph_0}$.*

تعریف ۳۸.۱.۱. *فرض کنیم X و Y دو مجموعه باشند. گوییم $|X| \leq |Y|$ هرگاه یک تابع یک‌به‌یک از X به Y موجود باشد. اگر تابعی یک‌به‌یک از X به Y موجود باشد که پوشا نیست می‌نویسیم $|X| < |Y|$.*

قضیه ۳۹.۱.۱. *(شرودر– برنشتاین) اگر برای دو مجموعه X و Y داشته باشیم $|X| \leq |Y|$ و $|Y| \leq |X|$ آنگاه $|X| = |Y|$.*

قضیه ۴۰.۱.۱. *اگر $\mathbb{P}(X)$ نمایش مجموعه توانی مجموعه X باشد (مجموعه همه زیرمجموعه‌های X) آنگاه $|X| < |\mathbb{P}(X)|$.*

قضیه ۴۱.۱.۱. *عدد اصلی مجموعه B^A برابر است با $|B|^{|A|}$.*

در زیر تعریفی نادقیق از مفهوم خانواده را ارائه می‌کنیم.

تعریف ۴۲.۱.۱. *خانواده دسته‌ای از اشیا است که این اشیا به صورت دقیق مشخص هستند و یک شی می‌تواند تکرار شود.*

تعریف ۴۳.۱.۱. *فرض کنیم X یک مجموعه باشد. هر تابع $f : \mathbb{N} \longrightarrow X$ را یک دنباله از اعضای X گوییم. معمولا $f(n)$ را با f_n نشان می‌دهیم. یک دنباله را گاهی به صورت $(f_۱, f_۲, ...)$ یا $\{f_i\}_{i=۱}^{\infty}$ نشان می‌دهیم.*

تعریف ۴۴.۱.۱. *فرض کنیم X و I دو مجموعه باشند. هر تابع $f : I \longrightarrow X$ را یک خانواده از عناصر X گوییم و با $(f_i)_{i\in I}$ یا $\{f_i \mid i \in I\}$ نشان می‌دهیم. به مجموعه I مجموعه اندیس گذار گوییم.*

تعریف ۴۵.۱.۱. *فرض کنیم $\{A_i\}_{i\in I}$ یک خانواده اندیس گذاری شده با I از مجموعه‌ها باشد. حاصل ضرب دکارتی $\{A_i\}_{i\in I}$ را این چنین تعریف می‌کنیم*

$$\prod_{i\in I} A_i = \{f : I \longrightarrow \bigcup_{i\in I} A_i \mid \forall i \in I, \quad f(i) \in A_i\}.$$

در حالت خاص اگر برای هر $i \in I$، $A_i = A$ حاصل ضرب دکارتی $\prod_{i\in I} A_i$ همان A^I است. اگر I مجموعه متناهی باشد مانند $I = \{۱, ..., n\}$ آنگاه داریم

$$\prod_{i\in I} A_i = \prod_{i=۱}^{n} A_i = A_۱ \times ... \times A_n = \{(a_۱, ..., a_n) \mid a_i \in A_i\}.$$

اصل انتخاب را در قالب تعریف زیر بیان می‌کنیم. اصل انتخاب صورت‌های بسیار زیادی دارد که در زیر ساده‌ترین آن را مشاهده می‌کنید.

تعریف ۴۶.۱.۱. *(اصل انتخاب) حاصل ضرب دکارتی خانواده‌ای ناتهی از مجموعه‌های ناتهی، ناتهی است.*

تعریف ۴۷.۱.۱. *فرض کنیم X یک مجموعه مرتب جزیی با رابطه R و $A \subseteq X$ باشد.*
(الف) گوییم عنصر $y \in X$ کران بالا برای A است هرگاه برای هر $a \in A$ داشته باشیم aRy.
(ب) گوییم عنصر $y \in X$ کران پایین برای A است هرگاه برای هر $a \in A$ داشته باشیم yRa.
(ج) گوییم عنصر $y \in X$ ماکسیمال است هرگاه برای هر $x \in X$ که xRy نتیجه شود $x = y$.
(د) گوییم عنصر $y \in X$ مینیمال است هرگاه برای هر $x \in X$ که yRx نتیجه شود $y = x$.

تعریف ۴۸.۱.۱. *گوییم مجموعه کلا مرتب X خوشترتیب است هرگاه هر زیرمجموعه ناتهی از X عنصر مینیمال داشته باشد.*

قضیه ۴۹.۱.۱. *(لم زرن) اگر A (مجموعه ناتهی) یک مجموعه مرتب جزیی باشد، به طوری که هر زیرمجموعه کلا مرتب (زنجیر) آن، دارای کران بالا (در A) باشد، آنگاه A دارای عضو ماکسیمال است.*

قضیه ۵۰.۱.۱. *(اصل خوشترتیبی) هر مجموعه خوشترتیب شدنی است.*

۲.۱ اعداد طبیعی، صحیح، پیمانه‌ای، گویا، حقیقی و مختلط

در این بخش کمی راجع به اعداد صحبت خواهیم کرد و مشابه بخش قبل وارد جزییات نمی‌شویم. با تعریف اعداد طبیعی و صحیح در درس مبانی ریاضی آشنا شده‌اید و متوجه شده‌اید که چگونه با اصول پئانو اعداد طبیعی ساخته می‌شوند و با کمک رابطه هم ارزی اعداد صحیح ایجاد می‌شوند و سپس اعداد گویا از روی اعداد صحیح ساخته می‌شوند. در درس مبانی آنالیز یا مبانی ریاضی با نحوه ساخته شدن اعداد حقیقی آشنا شده‌اید. برای راحتی ما نمادهای را برای اعداد در زیر معرفی می‌کنیم و کمی قضیه‌های کاربردی و مورد استفاده خودمان را معرفی می‌کنیم.

نمادگذاری ۱.۲.۱. *مجموعه اعداد طبیعی، حسابی، صحیح، گویا و حقیقی را به ترتیب با* $\mathbb{N}$، $\mathbb{W}$، $\mathbb{Z}$، $\mathbb{Q}$ *و* $\mathbb{R}$ *نمایش می‌دهیم.*

قضیه ۲.۲.۱. *(استقرای ضعیف) فرض کنیم* S *زیرمجموعه* $\mathbb{N}$ *باشد که* $1 \in S$ *و اگر* $n \in S$ *آنگاه* $n+1 \in S$. *در این صورت* $S = \mathbb{N}$.

قضیه ۳.۲.۱. *(استقرای قوی) فرض کنیم* S *زیرمجموعه* $\mathbb{N}$ *که* $1 \in S$ *و اگر* $n \in S$ *آنگاه برای هر عدد صحیح مثبت* m *کمتر از* n، $m \in S$. *در این صورت* $S = \mathbb{N}$.

تعریف ۴.۲.۱. *گوییم عدد صحیح* b *یک مقسوم علیه عدد صحیح* a *است یا* a *مضربی از* b *است هرگاه عدد صحیح* c *موجود باشد که* $a = bc$. *گاهی این مفهوم را با* $b|a$ *نمایش می‌دهیم. اگر چنین* c*ای موجود نباشد آنگاه می‌نویسیم* $b \nmid a$.

تعریف ۵.۲.۱. *عدد صحیح* p *را اول گوییم هرگاه مخالف با* 1 *و* -1 *باشد و تنها مقسوم علیه‌های آن* 1، -1، p *و* $-p$ *باشند.*

قضیه ۶.۲.۱. *هر عدد صحیح مثبت یا* 1 *است یا می‌توان آن را به یک و تنها یک روش به صورت حاصل ضربی از اعداد اول مثبت نوشت.*

قضیه ۷.۲.۱. *(الگوریتم تقسیم) فرض کنیم* $a, b \in \mathbb{Z}$ *و* $b > 0$. *در این صورت اعداد صحیح یکتایی مانند* q *و* r *وجود دارند که* $a = bq + r$ *و* $0 \leq r < b$. *به* r *باقیمانده و به* q *را خارج قسمت نامیم.*

تعریف ۸.۲.۱. *گوییم عدد صحیح* d *بزرگترین مقسوم علیه مشترک دو عدد صحیح* a *و* b *است هرگاه* $d|a$ *و* $d|b$ *و اگر* $c|a$ *و* $c|b$ *آنگاه* $c|d$. *این مفهوم را با* $d = (a, b)$ *نشان می‌دهیم.*

تعریف ۹.۲.۱. *دو عدد صحیح* a *و* b *را نسبت به هم اول گوییم هرگاه* $(a, b) = 1$.

قضیه زیر به قضیه بزو[۱] معروف است.

قضیه ۱۰.۲.۱. *(بزو) برای هر دو عدد صحیح* a *و* b *با شرط* $d = (a, b)$ *اعداد صحیح* r *و* s *چنان وجود دارند که* $ar + bs = d$.

---

[۱] Bezout

قضیه ۱.۲.۱۱. اگر p عدد اول باشد که برای اعداد صحیح a و b داشته باشیم $p|ab$ آنگاه $p|a$ یا $p|b$.

تعریف ۱.۲.۱۲. مجموعه اعداد مختلط را مجموعه $\mathbb{R}\times\mathbb{R}$ با جمع و ضرب زیر تعریف می‌کنیم

$$(a,b)+(x,y)=(a+x,b+y) \qquad\qquad (a,b).(x,y)=(ax-by,ay+bx)$$

اعداد مختلط را با $\mathbb{C}$ نمایش می‌دهیم. به اعضای $\mathbb{C}$ اعداد مختلط گوییم

تذکر ۱.۲.۱۳. برای هر $(x,y)\in\mathbb{C}$ داریم که $(x,y).(۱,۰)=(x,y)$. یعنی $(۱,۰)$ مانند عدد حقیقی ۱ در اعداد حقیقی است. همچنین اگر فرض کنیم $i=(۰,۱)$ و $(a,۰)$ را با a یکی بگیریم آنگاه چون $(a,b)=(a,۰)+(۰,۱)b$ به نمایش $a+ib$ برای عدد مختلط (a,b) خواهیم رسید. به علاوه $i^۲=i.i=(-۱,۰)$ و در نتیجه طبق قرار داد ما $i^۲=-۱$. عضو $(۰,۰)$ را با ۰ نشان می‌دهیم که مانند عدد حقیقی ۰ در اعداد حقیقی است.

تعریف ۱.۲.۱۴. در عدد مختلط $a+ib$ به a بخش حقیقی و به b بخش موهمی گوییم.

قضیه ۱.۲.۱۵. عدد مختلط ناصفر $z=a+ib$ دارای وارون ضربی $z^{-۱}=\frac{a}{a^۲+b^۲}+i(\frac{b}{a^۲+b^۲})$ است یعنی داریم $zz^{-۱}=z^{-۱}z=۱$.

تذکر ۱.۲.۱۶. همواره داریم

$$\mathbb{N}\subseteq\mathbb{W}\subseteq\mathbb{Z}\subseteq\mathbb{Q}\subseteq\mathbb{R}\subseteq\mathbb{C}.$$

تعریف ۱.۲.۱۷. به مجموعه اعداد مختلط که به صورت $a+ib$ هستند و $a,b\in\mathbb{Z}$ اعداد گوسی گوییم و با $\mathbb{Z}[i]$ نمایش می‌دهیم.

نمادگذاری ۱.۲.۱۸. برای اعداد صحیح k، t و زیرمجموعه X از اعداد مختلط، منظور از $kX+t$ یعنی مجموعه $\{kx+t\mid x\in X\}$.

تعریف ۱.۲.۱۹. عدد طبیعی n را در نظر می‌گیریم. رابطه

$$a,b\in\mathbb{Z}:\quad aRb\ \Leftrightarrow\ n|a-b$$

هم ارزی است. حال داریم

$$\bar{۰}=[۰]=\{a\in\mathbb{Z}\mid aR۰\}=\{a\in\mathbb{Z}\mid n|a\}=n\mathbb{Z}$$

یعنی کلاس ۰ همه مضرب‌های صحیح عدد n است یا به عبارتی تمام اعداد صحیح که به n باقیمانده ۰ دارند. اما

$$\bar{۱}=[۱]=\{a\in\mathbb{Z}\mid aR۱\}=\{a\in\mathbb{Z}\mid n|a-۱\}=n\mathbb{Z}+۱$$

یعنی کلاس ۱ تمام اعداد صحیح که به n باقیمانده ۱ دارند. با ادامه این روند تا $n-۱$ به n تا کلاس دست خواهیم یافت. یعنی مجموعه‌ای به شکل زیر

$$\{n\mathbb{Z},n\mathbb{Z}+۱,n\mathbb{Z}+۲,...,n\mathbb{Z}+(n-۱)\}=\{\bar{۰},\bar{۱},...,\overline{n-۱}\}.$$

به مجموعه بالا اعداد پیمانه n گوییم و با $\mathbb{Z}_n$ نشان می‌دهیم.

تعریف ۲۰.۲.۱. *برای اعداد پیمانه‌ای جمع و ضرب به صورت زیر تعریف می‌شود.*

$$\bar{x}+\bar{y}=\overline{x+y} \qquad \bar{x}\cdot\bar{y}=\overline{xy}$$

نمادگذاری ۲۱.۲.۱. *فرض کنیم n عدد طبیعی و a، b اعداد صحیح باشند. گاهی به جای $n|a-b$ از نماد $a \overset{n}{\equiv} b$ استفاده می‌کنیم.*

قضیه ۲۲.۲.۱. (قضیه ویلسون) *برای هر عدد اول داریم $(p-1)! \overset{p}{\equiv} -1$.*

تعریف ۲۳.۲.۱. *تابع فی اویلر یا φ تابعی است که تعداد اعداد طبیعی کوچکتر از n که نسبت به n اول‌اند را می‌شمارد. اگر n یک عدد طبیعی مثبت باشد، آنگاه $\varphi(n)$ برابر است با تعداد اعداد طبیعی k در بازه ۱ تا n به طوری که $(k,n)=1$.*

قضیه ۲۴.۲.۱. (قضیه اویلر_ فرما) *فرض کنیم n عدد صحیح مثبت و $\varphi(n)$ تابع اویلرباشد. در این صورت برای هر عدد صحیح a که $(a,n)=1$ داریم $a^{\varphi(n)} \overset{n}{\equiv} 1$.*

قضیه ۲۵.۲.۱. (قضیه کوچک فرما) *برای هر $a,p\in\mathbb{Z}$ که p عددی اول است، داریم $a^p \overset{p}{\equiv} a$.*

۳.۱ ماتریس‌ها

در مقطع کارشناسی ماتریس‌ها بیشتر در درس جبر خطی مطالعه می‌شوند. اما ماتریس‌ها ابزار بسیار خوبی هستند تا بتوانیم مثال‌های متنوعی را در درس مبانی جبر فراهم کنیم. بنابراین مختصری در این بخش راجع به ماتریس‌ها خواهیم گفت.

تعریف ۱.۳.۱. *فرض کنیم m و n دو عدد طبیعی و X یک مجموعه باشد. هر تابع*

$$f : \{۱, ۲, ..., m\} \times \{۱, ۲, ..., n\} \longrightarrow X$$

را یک ماتریس $m \times n$ روی X گوییم. به $f((i, j))$ درایه گوییم که $i \in \{۱, ۲, ..., m\}$ و $j \in \{۱, ۲, ..., n\}$. برای راحتی آن را با f_{ij} نشان می‌دهیم. برای نمایشی بهتر از شکل زیر بهره می‌بریم.

$$\begin{pmatrix} f_{۱۱} & f_{۱۲} & \cdots & f_{۱n} \\ f_{۲۱} & f_{۲۲} & \cdots & f_{۲n} \\ & & \vdots & \\ f_{m۱} & f_{m۲} & \cdots & f_{mn} \end{pmatrix}_{m\times n}$$

همچنین یک ماتریس را گاهی با (f_{ij}) نمایش می‌دهیم.

تذکر ۲.۳.۱. *معمولا ماتریس‌ها را با حروف بزرگ انگلیسی نمایش می‌دهیم و مجموعه X را یکی از مجموعه‌های شناخته شده $\mathbb{N}$، $\mathbb{Z}$، $\mathbb{Q}$، $\mathbb{R}$ و یا $\mathbb{C}$ در نظر می‌گیریم.*

نمادگذاری ۳.۳.۱. *به ماتریس*

$$O = \begin{pmatrix} ۰ & ۰ & \cdots & ۰ \\ ۰ & ۰ & \cdots & ۰ \\ & & \vdots & \\ ۰ & ۰ & \cdots & ۰ \end{pmatrix}_{m\times n}$$

ماتریس صفر گوییم و اگر $m = n$ باشد آنگاه به ماتریس

$$I = \begin{pmatrix} ۱ & ۰ & \cdots & ۰ \\ ۰ & ۱ & \cdots & ۰ \\ & & \vdots & \\ ۰ & ۰ & \cdots & ۱ \end{pmatrix}_{n\times n}$$

ماتریس همانی گوییم که در آن $۰ \in \mathbb{C}$ و $۱ \in \mathbb{C}$.

تعریف ۴.۳.۱. *اگر $m = n$ باشد آنگاه به ماتریس مربعی گوییم و n را مرتبه ماتریس نامیم.*

نمادگذاری ۵.۳.۱. منظور از نماد $M_{m\times n}(X)$ یعنی مجموعه تمام ماتریس‌های $m\times n$ با درایه‌های از X. اگر $m=n$ باشد از نماد $M_n(X)$ استفاده می‌کنیم.

تعریف ۶.۳.۱. اگر $A=(a_{ij})\in M_{m\times n}(\mathbb{C})$ و $B=(b_{ij})\in M_{m\times n}(\mathbb{C})$ آنگاه جمع دو ماتریس به صورت زیر تعریف می‌شود

$$A+B=(a_{ij}+b_{ij}).$$

تعریف ۷.۳.۱. اگر $A=(a_{ij})\in M_{m\times n}(\mathbb{C})$ و $B=(b_{ij})\in M_{n\times l}(\mathbb{C})$ آنگاه ضرب دو ماتریس به صورت زیر تعریف می‌شود

$$C=AB=\begin{pmatrix} c_{۱۱} & c_{۱۲} & \cdots & c_{۱l} \\ c_{۲۱} & c_{۲۲} & \cdots & c_{۲l} \\ & & \vdots & \\ c_{m۱} & c_{m۲} & \cdots & c_{ml} \end{pmatrix}$$

که در آن $c_{ij}=\sum_{k=۱}^{n}a_{ik}b_{kj}$.

تعریف ۸.۳.۱. فرض کنیم A یک ماتریس $m\times n$ باشد. منظور از سطر iام یعنی ماتریس $۱\times n$ زیر

$$\begin{pmatrix} a_{i۱} & a_{i۲} & \cdots & a_{in} \end{pmatrix}$$

و منظور از ستون jام یعنی ماتریس $۱\times j$ زیر

$$\begin{pmatrix} a_{۱j} \\ a_{۲j} \\ \vdots \\ a_{mj} \end{pmatrix}$$

تعریف ۹.۳.۱. فرض کنیم A یک ماتریس $m\times n$ باشد. در این صورت به ماتریسی که از حذف سطر iام و ستون jام به دست می‌آید ماتریس کهاد یا خُرد گوییم و با $M_i^j(A)$ نمایش می‌دهیم. اگر بیم ابهام برای ماتریس A نباشد فقط از نماد M_i^j استفاده می‌کنیم.

تعریف ۱۰.۳.۱. دترمینان یک ماتریس مربعی از مرتبه ۲ با درایه‌های از $\mathbb{C}$ به صورت زیر است

$$det\begin{pmatrix} a_{۱۱} & a_{۱۲} \\ a_{۲۱} & a_{۲۲} \end{pmatrix}=a_{۱۱}a_{۲۲}-a_{۱۲}a_{۲۱}$$

و دترمینان یک ماتریس مربعی از مرتبه ۳ با درایه‌های از $\mathbb{C}$ به صورت زیر است

$$det\begin{pmatrix} a_{۱۱} & a_{۱۲} & a_{۱۳} \\ a_{۲۱} & a_{۲۲} & a_{۲۳} \\ a_{۳۱} & a_{۳۲} & a_{۳۳} \end{pmatrix}=$$
$$a_{۱۱}det\begin{pmatrix} a_{۲۲} & a_{۲۳} \\ a_{۳۲} & a_{۳۳} \end{pmatrix}+a_{۱۲}det\begin{pmatrix} a_{۲۱} & a_{۲۳} \\ a_{۳۱} & a_{۳۳} \end{pmatrix}+a_{۱۳}det\begin{pmatrix} a_{۲۱} & a_{۲۲} \\ a_{۳۱} & a_{۳۲} \end{pmatrix}=$$
$$a_{۱۱}det\,M_۱^۱+a_{۱۲}det\,M_۱^۲+a_{۱۳}det\,M_۱^۳$$

و با روند استقرایی دترمینان یک ماتریس مربعی از مرتبه n با درایه‌های از $\mathbb{C}$ به صورت زیر است

$$det\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ & & \vdots & \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix} = a_{11} det\ M_1^1 + a_{12} det\ M_1^2 + ... + a_{1n} det\ M_1^n$$

قضیه ۱۱.۳.۱. برای هر دو ماتریس مربعی A و B داریم $det\ AB = det\ A\ det\ B$.

تعریف ۱۲.۳.۱. گوییم ماتریس مربعی A وارون پذیر است هرگاه ماتریس مربعی B موجود باشد که $AB = BA = I$. ماتریس مربعی B را با A^{-1} نمایش می‌دهیم.

قضیه ۱۳.۳.۱. ماتریس مربعی A وارون پذیر است اگر و تنها اگر $det\ A$ مخالف با عدد صفر باشد.

تعریف ۱۴.۳.۱. فرض کنیم A یک ماتریس $n \times m$ باشد. ترانهاده A ماتریسی است $m \times n$ مانند B که از قرار دادن درایه iام jام از A در مکان jام iام ماتریس B به دست می‌آید.

فصل ۲

آشنایی با نظریه گروه‌ها

در جبر نوین نظریه گروه به مطالعه موجودات ریاضی می‌پردازد که به گروه‌ها معروف هستند. مفهوم گروه بخش مرکزی جبر نوین است و سایر موجودات جبر نوین مانند حلقه‌ها و فضاهای برداری بر پایه همین مفهوم گروه شکل گرفته‌اند. مطالعه گروه‌ها سایر شاخه‌های ریاضی را نیز تحت تاثیر قرار می‌دهد و کاربردهای آن در بسیار از بخش‌های ریاضی دیده می‌شود. به طور ویژه، گروه‌ها در جبر نوین جایگاه خاصی دارند که مهمترین آنها می‌توان به گروه‌های خطی و گروه لی[۱] اشاره کرد. در این فصل هدف ما آشنایی مختصر با نظریه گروه است و در درس جبر ۱ می‌توانید با مطالب تکمیلی از نظریه گروه آشنا شوید و در مقاطع بالاتر مطالب پیشرفته را بیاموزید.

۱.۲ عمل دوتایی

در این بخش شما را با مفهوم عمل دوتایی آشنا می‌کنیم و سپس منظور خود را از ساختار ریاضی بیان می‌کنیم. کار را با تعریف زیر آغاز می‌کنیم.

تعریف ۱.۱.۲. *فرض کنیم S یک مجموعه ناتهی باشد. هر تابع*

$$*: S \times S \longrightarrow S$$

را یک عمل دوتایی روی مجموعه S گوییم. در حقیقت عمل دوتایی روی زوج‌های مرتب از عنصرهای S دقیقا یک عنصر از S را نسبت می‌دهد. عمل دوتایی را به جای نماد متداول تابع مانند f، g و ... با $*$، $\cdot$ و یا o نمایش می‌دهیم.

مثال ۲.۱.۲. *فرض کنیم $S = \mathbb{Z}$ و $*$ را عمل جمع، $+$، در نظر می‌گیریم. واضح است که $+$ یک عمل دوتایی روی $\mathbb{Z}$ است. در واقع $+$ دو عدد صحیح را می‌گیرید و جمع عادی را روی آنها پیاده می‌کند.*

---
[۱] Lie

مثال ۳.۱.۲. *فرض کنیم $S=\mathbb{R}$ و $*$ را عمل ضرب، $\cdot$، در نظر می‌گیریم. واضح است که $\cdot$ یک عمل دوتایی روی $\mathbb{R}$ است. در واقع $\cdot$ دو عدد حقیقی را می‌گیرید و ضرب عادی را روی آنها پیاده می‌کند.*

مثال ۴.۱.۲. *فرض کنیم $S=M_n(\mathbb{R})$ و $*$ را عمل ضرب، $\cdot$، در نظر می‌گیریم. واضح است که $\cdot$ یک عمل دوتایی روی ماتریس‌ها است. در واقع $\cdot$ دو عدد ماتریس را می‌گیرید و ضرب عادی ماتریسی را روی آنها پیاده می‌کند.*

مثال ۵.۱.۲. *فرض کنیم S بازه $[-۱,۰]$ باشد. در این صورت $*: S\times S \longrightarrow S$ با ضابطه $a*b=|a-b|$ عمل نیست. زیرا اگر قرار دهیم $a=۰$ و $b=-۱$ آنگاه $a*b=۱\notin S$. پس $*$ تابع نیست.*

مثال ۶.۱.۲. *اگر X یک مجموعه باشد، $\mathbb{P}(X)$ را در نظر می‌گیریم. در این صورت اجتماع، اشتراک، تفاضل عمل‌های دوتایی روی $\mathbb{P}(X)$ هستند.*

مثال ۷.۱.۲. *مجموعه همه توابع روی مجموعه X را در نظر می‌گیریم یعنی مجموعه X^X. در این صورت ترکیب توابع یک عمل دوتایی روی X^X است.*

گزاره ۸.۱.۲. *اگر $|S|=n$ باشد آنگاه $n^{(n^۲)}$ عمل دوتایی روی S وجود دارد.*

اثبات. فرض کنیم $*: S\times S \longrightarrow S$ یک عمل دوتایی باشد. می‌دانیم که هر عمل دوتایی یک تابع است پس برای تعداد عمل‌هایی دوتایی در واقع می‌خواهیم تعداد توابع از $S\times S$ به S را به دست آوریم. اکنون واضح است که دامنه $*$، $n^۲=n\times n$ عضو دارد و برد آن تعداد n عضو. حال طبق قضیه ۴۱.۱.۱، تعداد چنین $*$هایی برابر است با $n^{(n^۲)}$. □

تعریف ۹.۱.۲. *گوییم عمل دوتایی $*: S\times S \longrightarrow S$ روی مجموعه S:*
(الف) جابجایی است هرگاه برای هر $s,s'\in S$ داشته باشیم $s*s'=s'*s$.
(ب) شرکت پذیر است هرگاه برای هر $s,s',s''\in S$ داشته باشیم $s*(s'*s'')=(s*s')*s''$.

مثال ۱۰.۱.۲. *عمل دوتایی $+$ روی $\mathbb{Z}$ یک عمل جابجایی و شرکت پذیر است.*

مثال ۱۱.۱.۲. *عمل دوتایی اجتماع روی $\mathbb{P}(X)$ یک عمل جابجایی و شرکت پذیر است.*

مثال ۱۲.۱.۲. *عمل ضرب ماتریسی روی $M_۲(\mathbb{R})$ جابجایی نیست. زیرا*

$$A=\begin{pmatrix} ۱ & ۰ \\ ۲ & ۳ \end{pmatrix},\ \ B=\begin{pmatrix} -۱ & ۰ \\ ۲ & -۱ \end{pmatrix}: \qquad A.B\neq B.A$$

مثال ۱۳.۱.۲. *فرض کنیم S برابر با بازه $[۰,۴]$ باشد. در این صورت $*: S\times S \longrightarrow S$ با ضابطه $a*b=|a-b|$ یک عمل دوتایی است (چرا؟) که شرکت پذیر نیست. زیرا*

$$۱*(۲*۳)=۱*(|۲-۳|)=۱*۱=۰\neq(۱*۲)*۳=$$
$$(|۱-۲|)*۳=۱*۳=|۱-۳|=۲.$$

تذکر ۱۴.۱.۲. *فرض کنیم $*$ عمل دوتایی شرکت پذیر روی S باشد. شرکت پذیری اجازه می‌دهد که در انجام عمل دوتایی روی سه عنصر از S قرار گرفتن پرانتز برای ما مهم نباشد و حاصل تغییری نکند. اما این سوال طبیعی است که اگر تعداد بیشتر از سه عنصر شود، باز هم می‌توان پرانتزها را هرگونه که بخواهیم قرار دهیم؟ مثلا برای ۴ عنصر a، b، c و d از S حالت‌های زیر را داریم*

$$a*((b*c)*d) \quad (a*b)*(c*d) \quad ((a*b)*c)*d \quad (a*(b*c))*d \quad (a*(b*(c*d)))$$

در ادامه می‌خواهیم نشان دهیم که اگر $*$ شرکت پذیر باشد جایگاه پرانتز در حاصل نهایی تفاوتی ایجاد نمی‌کند. برای این کار از حالت‌های پرانتز گذاری یک حالت که راحتر در ذهن می‌نشیند را در نظر می‌گیریم (حالت ۳ مثال بالا) و به آن استانده می‌گوییم و سپس نشان می‌دهیم باقی حالت‌ها با همین حالت استانده یکی است.

تعریف ۱۵.۱.۲. *فرض کنیم $*$ یک عمل دوتایی روی S باشد و a_1، ...، a_n عناصری از S. عمل استانده a_iها را با استقرا چنین تعریف می‌کنیم*

$$\prod_{i=1}^{1} a_i = a, \quad \prod_{i=1}^{2} a_i = (a_1 * a_2), \quad \prod_{i=1}^{3} a_i = (\prod_{i=1}^{2} a_i) * a_3, ..., \prod_{i=1}^{n} a_i = (\prod_{i=1}^{n-1} a_i) * a_n.$$

مثال ۱۶.۱.۲. *عمل استانده ۵ عنصر a_1، a_2، a_3، a_4 و a_5 برابر است با*

$$\prod_{i=1}^{5} a_i = (((a_1 * a_2) * a_3) * a_4) * a_5.$$

اکنون قضیه زیر را داریم.

قضیه ۱۷.۱.۲. *اگر عمل دوتایی $*$ روی S شرکت پذیر باشد و a_1، ...، a_n عناصری از S آنگاه هر نوع انجام عمل دوتایی با معنی برای a_iها برابر با عمل استانده a_iها است.*

اثبات. حکم را با استقرای قوی روی n اثبات می‌کنیم. اگر $n = 1$ باشد که چیزی برای اثبات نداریم. فرض کنیم $n > 1$ و برای هر $m < n$ حکم صحیح باشد. می‌خواهیم حکم را برای n اثبات کنیم. فرض کنیم $T(a_1, ..., a_n)$ نمایش عمل دوتایی با معنی باشد. اگر T یک عمل دوتایی با معنی از a_iها باشد آنگاه $1 \leq k \leq n$ چنان وجود دارد که $T(a_1, ..., a_n) = T(a_1, ..., a_k) * T(a_{k+1}, ..., a_n)$. طبق فرض استقرار داریم

$$T(a_1, ..., a_n) = T(a_1, ..., a_k) * T(a_{k+1}, ..., a_n) = (\prod_{i=1}^{k} a_i) * (\prod_{j=k+1}^{n} a_j).$$

دو حالت ممکن است رخ دهد.
حالت اول. $k = n - 1$. پس

$$T(a_1, ..., a_n) = T(a_1, ..., a_{n-1}) * T(a_n) = (\prod_{i=1}^{n-1} a_i) * a_n = \prod_{i=1}^{n} a_i.$$

یعنی در این حالت اثبات کامل است.
حالت دوم. $k < n - ۱$. در این صورت با کمک شرکت پذیری و تعریف عمل استانده داریم

$$T(a_۱, ..., a_n) = T(a_۱, ..., a_k) * T(a_{k+۱}, ..., a_n) = (\prod_{i=۱}^{k} a_i) * (\prod_{j=k+۱}^{n} a_j)$$

$$(\prod_{i=۱}^{k} a_i) * ((\prod_{j=k+۱}^{n-۱} a_j) * a_n) = ((\prod_{i=۱}^{k} a_i) * (\prod_{j=k+۱}^{n-۱} a_j)) * a_n$$

اما $(\prod_{i=۱}^{k} a_i) * (\prod_{j=k+۱}^{n-۱} a_j)$ عمل دوتایی با معنی از $(n-۱)$تا است یعنی $T(a_۱, ..., a_{n-۱})$. پس طبق فرض اسقرا داریم

$$(\prod_{i=۱}^{k} a_i) * (\prod_{j=k+۱}^{n-۱} a_j) = \prod_{i=۱}^{n-۱} a_i.$$

با جایگذاری در بالا و استفاده از تعریف عمل استانده داریم

$$T(a_۱, ..., a_n) = (\prod_{i=۱}^{n} a_i) * a_n = \prod_{i=۱}^{n} a_i$$

در این حالت هم اثبات کامل است. $\square$

تعریف ۱۸.۱.۲. *فرض کنیم $* : S \times S \longrightarrow S$ و $o : S \times S \longrightarrow S$ دو عمل دوتایی روی مجموعه S باشند. گوییم*

(الف) *$*$ روی o توزیعپذیر از سمت چپ است هرگاه برای هر $x, y, z \in S$* داشته باشیم

$$x * (yoz) = (x * y)o(x * z).$$

(ب) *$*$ روی o توزیعپذیر از سمت راست است هرگاه برای هر $x, y, z \in S$* داشته باشیم

$$(yoz) * x = (y * x)o(z * x).$$

(ج) *$*$ روی o توزیعپذیر است هرگاه توزیعپذیر چپ و راست باشد.*

مثال ۱۹.۱.۲. *روی $\mathbb{R}$ عمل دوتایی $*$ را جمع معولی و عمل دوتایی o را همان ضرب معمولی در نظر می‌گیریم. همان طوری که از دوران مدرسه تا کنون دیده‌اید جمع روی ضرب توزیعپذیر است.*

مثال ۲۰.۱.۲. *عمل دوتایی $*$ را اجتماع روی $\mathbb{P}(X)$ و عمل دوتایی o را اشتراک روی $\mathbb{P}(X)$ در نظر می‌گیریم. در این صورت $*$ روی o توزیعپذیر است. همچنین o روی $*$ توزیعپذیر است. زیرا از مبانی ریاضی دیده‌اید که*

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

بقیه حالت‌ها هم مشابه است.

مثال ۲.۱.۲۱. *روی اعداد حقیقی عمل $*$ را جمع و عمل o را قدرمطلق در نظر می‌گیریم. $*$ روی o توزیع‌پذیر (چپ ـ راست) نیست. زیرا*

$$۱ * (۲o۳) = ۱ * (|۲ - ۳|) = ۱ * ۱ = ۱ + ۱ = ۲$$

در حالی که

$$(۱ * ۲)o(۱ * ۳) = (۱ + ۲)o(۱ + ۳) = ۳o۴ = |۳ - ۴| = ۱.$$

تعریف ۲.۱.۲۲. *منظور از ساختار ریاضی یا دستگاه ریاضی یعنی مجموعه‌ای ناتهی مانند $*$ همراه با یک یا چند عمل دوتایی روی S مانند $*_۱$، ...، $*_n$ که معمولا با $(S, *_۱, ..., *_n)$ نمایش می‌دهیم.*

مثال ۲.۱.۲۳. *$(\mathbb{Z}, +)$ یک ساختار ریاضی است با یک عمل دوتایی است.*

مثال ۲.۱.۲۴. *$(\mathbb{R}, +, \cdot)$ یک ساختار ریاضی با دو عمل دوتایی است.*

تمرین‌های حل شده

تمرین ۲.۱.۲۵. *آیا $* : \mathbb{R} \times \mathbb{R} \longrightarrow \mathbb{R}$ با ضابطه $a * b = a^b$ یک عمل دوتایی است؟*

حل. $*$ یک عمل دوتایی نیست. زیرا اگر قرار دهیم $a = -۱$ و $b = \frac{۱}{۲}$ آنگاه $a^b = \sqrt{-۱}$ که همان $a * b$ است، معنی ندارد. یعنی $*$ یک تابع نیست.

تمرین ۲.۱.۲۶. *آیا $* : \mathbb{R} \times \mathbb{R} \longrightarrow \mathbb{R}$ با ضابطه $a * b = ۲^a \times ۳^b$ یک عمل دوتایی است؟*

حل. $*$ یک عمل دوتایی است. باید نشان دهیم $*$ تابع است. ابتدا دقت کنید باید نشان دهیم $a * b \in \mathbb{R}$. اگر a عددی گویا باشد یعنی $a = \frac{m}{n}$ آنگاه $۲^{\frac{m}{n}} = \sqrt[n]{۲^m}$ عددی حقیقی است. به صورت مشابه اگر b عدد گویا باشد باز هم ۳^b نیز عدد حقیقی است و حاصل ضرب دو عدد حقیقی باز هم عددی حقیقی است. بنابراین در این حالت $a * b \in \mathbb{R}$. اگر a عددی گویا نباشد آنگاه می‌دانیم که دنباله‌ای از اعداد گویا وجود دارد که به a میل می‌کند یعنی $a = \lim_{n\to\infty} x_n$ که x_nها گویا هستند. پس $۲^a = ۲^{\lim_{n\to\infty} x_n} = \lim_{n\to\infty}[۲^{x_n}]$. اما طبق حالت قبل ۲^{x_n} عددی حقیقی هستند که این نتیجه می‌دهد $۲^a \in \mathbb{R}$. پس در هر صورت، $a * b \in \mathbb{R}$. همچنین اگر $a = a'$ و $b = b'$ آنگاه $۲^a \times ۳^b = ۲^{a'} \times ۳^{b'}$. در نتیجه $*$ یک عمل دوتایی است.

تمرین ۲.۱.۲۷. *فرض کنیم $*$ عمل دوتایی شرکت پذیر روی مجموعه ناتهی S باشد و $a, b \in S$. اگر برای هر $x \in$ داشته باشیم $x * a = x$ و $b * x = x$ آنگاه نشان دهید که $a = b$.*

حل. طبق فرض می‌توانیم x را خود a یا b انتخاب کنیم. مثلا اگر $x=b$ در نظر بگیریم و در $x*a=x$ قرار دهیم آنگاه $b*a=b$ و به روش مشابه اگر $x=a$ را در $b*x=x$ قرار دهیم آنگاه $b*a=b$. پس $a=b$.

تمرین ۲.۱.۲۸. *فرض کنیم S یک مجموعه با عمل دوتایی شرکت پذیر $*$ باشد که برای $x, y, z \in S$ داریم $x*y=y*x$ و $x*z=z*x$. نشان دهید که x با $y*z$ جابجا می‌شود.*

حل. داریم

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

۲.۲ تعریف گروه، مثال‌ها و قضیه‌های اولیه

با تعریف ساختارهای ریاضی در بخش قبل آشنا شدید. اما بعضی ساختارهای ریاضی عمل‌های دوتایی آن خواص بیشتری دارند و مورد توجه قرار می‌گیرند. در این بخش (حتی کل این فصل) روی ساختار ریاضی تمرکز می‌کنیم که فقط یک عمل دوتایی دارد و آن عمل ویژگی‌های خاصی را دارا است. با تعریف زیر آغاز می‌کنیم.

تعریف ۱.۲.۲. *فرض کنیم S یک مجموعه ناتهی و $*$ یک عمل دوتایی روی S باشد. گوییم $(S, *)$ یک نیم‌گروه است هرگاه $*$ شرکت پذیر باشد.*

مثال ۲.۲.۲. *$(\mathbb{Z}, +)$ یک نیم‌گروه است. حتی $(\mathbb{R}, \cdot)$ نیز یک نیم‌گروه است.*

مثال ۳.۲.۲. *فرض کنیم S برابر با بازه $[۰, ۴]$ باشد. در این صورت $* : S \times S \longrightarrow S$ با ضابطه $a * b = |a - b|$ یک عمل دوتایی است (چرا؟) که شرکت پذیر نیست (چرا؟). بنابراین $(S, *)$ نیم‌گروه نیست.*

تعریف ۴.۲.۲. *فرض کنیم S یک مجموعه ناتهی و $*$ یک عمل دوتایی روی S باشد. گوییم:*
(الف) عنصر $e \in S$ عضو خنثی (همانی) چپ است هرگاه برای هر $s \in S$ داشته باشیم $e * s = s$.
(ب) عنصر $e \in S$ عضو خنثی (همانی) راست است هرگاه برای هر $s \in S$ داشته باشیم $s * e = s$.
(ج) عنصر $e \in S$ خنثی (همانی) است هرگاه هم خنثی چپ و هم خنثی راست باشد.

مثال ۵.۲.۲. *در $(\mathbb{Z}, +)$ عنصر ۰ خنثی (چپ_ راست) است. زیرا برای هر $x \in \mathbb{Z}$ داریم که $x + ۰ = ۰ + x = x$.*

مثال ۶.۲.۲. *فرض کنیم S برابر با بازه $[۰, ۴]$ باشد. در این صورت $* : S \times S \longrightarrow S$ با ضابطه $a * b = |a - b|$ یک عمل دوتایی است. برای هر $s \in S$ داریم $s * ۰ = s = ۰ * s$. پس ۰ عنصر خنثی است.*

مثال ۷.۲.۲. *$(\mathbb{R}, *)$ که در آن $a * b = ۳$ عضو خنثی ندارد.*

مثال ۸.۲.۲. *فرض کنیم $S = \{۱, ۲\}$ و برای هر $a, b \in S$ تعریف می‌کنیم $a * b = b$. در این صورت S عضو خنثی چپ دارد که یکتا هم نیست (چرا؟). در حالی که اصلا عضو خنثی راست ندارد!*

واضح است که اگر $*$ روی S جابجایی باشد و S عنصر خنثی چپ داشته باشد آنگاه این عنصر خنثی چپ، خنثی راست نیز می‌باشد. این مطلب و مثال قبل ما را به سمت گزاره زیر رهنمود می‌کند.

گزاره ۹.۲.۲. *فرض کنیم $*$ یک عمل دوتایی روی مجموعه S باشد. اگر $(S, *)$ دارای عضو خنثی چپ مانند e و عضو خنثی راست مانند f باشد آنگاه $e = f$. در نتیجه عضو خنثی یکتا است.*

اثبات. چون e عضو خنثی چپ است پس باید $e * f = f$ باشد. اما f عضو خنثی راست است پس $e * f = e$. بنابراین باید $e = f$. قسمت دوم بدیهی است چون هر عضو خنثی، خنثی چپ (راست) است. □

تعریف ۱۰.۲.۲. *فرض کنیم $(S, *)$ دارای عنصر خنثی مانند e باشد. گوییم*
(الف) عنصر $a \in S$ دارای وارون چپ است هرگاه عنصر $b \in S$ موجود باشد که $b * a = e$.
(ب) عنصر $a \in S$ دارای وارون راست است هرگاه عنصر $b \in S$ موجود باشد که $a * b = e$.
(ج) عنصر $a \in S$ وارون پذیر است هرگاه هم وارون چپ و هم وارون راست داشته باشد (وارون a را با a^{-1} نمایش می‌دهیم).

مثال ۱۱.۲.۲. *$(\mathbb{Z}, +)$ دارای عنصر خنثی ۰ نسبت به عمل دوتایی + است و برای هر عدد صحیح x داریم که $x + (-x) = (-x) + x = 0$. پس هر عنصر در $\mathbb{Z}$ وارون پذیر است.*

مثال ۱۲.۲.۲. *$(\mathbb{Z}, \cdot)$ دارای عنصر خنثی ۱ نسبت به عمل دوتایی $\cdot$ است. هر عدد صحیح مخالف با ۱ و ۱− وارون پذیر نیست. در حالی که ۱− وارون پذیر است.*

مثال ۱۳.۲.۲. *$(\mathbb{R}, \cdot)$ عضو خنثی ۱ دارد. همه عناصر ناصفر وارون دارند در حالی که ۰ ندارد.*

مثال ۱۴.۲.۲. *$(\mathbb{N}, \cdot)$ یک نیم‌گروه است که عضو خنثی ۱ دارد. اما هیچ عنصر وارون پذیری ندارد.*

مثال ۱۵.۲.۲. *فرض کنیم S برابر با بازه $[0, 4]$ باشد. در این صورت $* : S \times S \longrightarrow S$ با ضابطه $a * b = |a - b|$ یک عمل دوتایی است. برای هر $s \in S$ داریم $s * 0 = 0 * s = s$. پس ۰ عنصر خنثی است. جالب این که هر عنصر وارون خودش است!*

تذکر ۱۶.۲.۲. *فرض کنیم $(S, *)$ دارای عنصر خنثی مانند e باشد. واضح است که e وارون خودش است.*

مثال ۱۷.۲.۲. *فرض کنیم $S = \{1, 2\}$ و برای هر $a, b \in S$ تعریف می‌کنیم $a * b = b$. در این صورت ۱ عضو خنثی چپ است. همه عناصر وارون راست برابر با ۱ دارند. از طرفی ۲ نیز عضو خنثی چپ است و جالب این که همه عناصر وارون راست ۲ دارند. در حالی که اصلا عضو خنثی راست وجود ندارد! پس وارون چپ و راست بی معنی است!*

اگر عمل دوتایی $*$ جابجایی روی S باشد و S عنصر خنثی داشته باشد وارون چپ هر عنصر در صورت وجود وارون راست نیز می‌باشد. این مطلب و مثال بالا ما را به گزاره زیر رهنمود می‌کند.

گزاره ۱۸.۲.۲. *فرض کنیم نیم‌گروه $(S, *)$ دارای عنصر خنثی مانند e باشد. اگر x در S وارون چپ a و وارون راست b داشته باشد آنگاه $a = b$.*

اثبات. چون a وارون چپ x است پس $a * x = e$. به صورت مشابه $x * b = e$. اما با فرض نیم‌گروهی داریم

$$a = a * e = a * (x * b) = (a * x) * b = e * b = b.$$

اثبات کامل است. □

تذکر ۱۹.۲.۲. بعضی مراجع و کتاب‌ها به یک نیم‌گروه با عنصر خنثی تکواره یا مونوئید گویند.

مثال ۲۰.۲.۲. مجموعه توابع پیوسته روی $\mathbb{R}$ را با $C(\mathbb{R})$ نشان می‌دهیم. $C(\mathbb{R})$ با عمل دوتایی ترکیب عادی توابع یک نیم‌گروه با عنصر خنثی $id_{\mathbb{R}}$ است (قضیه ۲۵.۱.۱ را ببینید). اما می‌دانیم که توابعی وارون پذیر هستند که یک‌به‌یک و پوشا باشند (قضیه ۲۸.۱.۱ را ببینید). در حالی که همه عناصر $C(\mathbb{R})$ یک‌به‌یک یا پوشا نیستند.

اکنون آماده این مطلب هستیم که تعریف گروه را بیاوریم.

تعریف ۲۱.۲.۲. فرض کنیم G مجموعه ناتهی و $*$ یک عمل دوتایی روی G باشد. گوییم $(G, *)$ یک گروه است هرگاه:
(الف) $(G, *)$ نیم‌گروه باشد ($*$ شرکت پذیر باشد).
(ب) $(G, *)$ عضو خنثی داشته باشد.
(ج) هر عنصر G نسبت به عمل $*$ وارون داشته باشد.

مثال ۲۲.۲.۲. $(\mathbb{R}, +)$ یک گروه است.

مثال ۲۳.۲.۲. $(\mathbb{R}, \cdot)$ یک گروه نیست. زیرا ۰ وارون ندارد.

مثال ۲۴.۲.۲. $(\mathbb{R} \setminus \{۰\}, \cdot)$ یک گروه است.

مثال ۲۵.۲.۲. فرض کنیم S برابر با بازه $[۰, ۴]$ باشد. در این صورت $* : S \times S \longrightarrow S$ با ضابطه $a * b = |a - b|$ یک عمل دوتایی است. برای هر $s \in S$ داریم $۰ * s = s * ۰ = s$. پس ۰ عنصر خنثی است. هر عنصر وارون خودش است. اما $*$ شرکت پذیر نیست. پس $(S, *)$ نیم‌گروه نیست و در نتیجه گروه نیست.

مثال ۲۶.۲.۲. $(\mathbb{R}, *)$ که در آن $a * b = ۳$ عضو خنثی ندارد و در نتیجه گروه نیست.

مثال ۲۷.۲.۲. $(M_n(\mathbb{R}), +)$ یک گروه است ($+$ جمع عادی دو ماتریس). واضح است که ضرب ماتریس‌ها شرکت پذیر است و ماتریس O نقش عنصر خنثی را دارد. وارون هر ماتریس (a_{ij}) ماتریس $(-a_{ij})$ است.

مثال ۲۸.۲.۲. $(M_n(\mathbb{R}), \cdot)$ یک گروه نیست ($\cdot$ ضرب عادی دو ماتریس). زیرا همه ماتریس‌ها وارون ندارند (چرا؟). دقت شود که I عنصر خنثی است.

مثال ۲۹.۲.۲. فرض کنیم $GL_n(\mathbb{R})$ مجموعه همه ماتریس‌های مربعی وارون پذیر باشد (طبق قضیه ۱۳.۳.۱، همه ماتریس‌های که دترمینان ناصفر دارند). $(GL_n(\mathbb{R}), \cdot)$ یک گروه است (عمل $\cdot$ ضرب عادی دو ماتریس). دقت شود که I عنصر خنثی است. همچنین طبق قضیه ۱۱.۳.۱، اگر $A, B \in GL_n(\mathbb{R})$ آنگاه $A \cdot B \in GL_n(\mathbb{R})$. یعنی $\cdot$ روی $GL_n(\mathbb{R})$ تابع (عمل دوتایی) است. شرکت پذیری از $M_n(\mathbb{R})$ به $GL_n(\mathbb{R})$ ارث می‌رسد.

مثال ۳۰.۲.۲. فرض کنیم n یک عدد طبیعی باشد. در این صورت $(\mathbb{Z}_n, +)$ یک گروه است. برای تعریف اعداد پیمانه‌ای $\mathbb{Z}_n$ و عمل دوتایی جمع روی این مجموعه به فصل اول بخش دوم مراجعه نمایید. واضح است که $\bar{۰}$ عضو خنثی است. وارون عنصر $\bar{x}$ به صورت $\overline{n - x}$ است. با یک محاسبه سر راست این عمل جمع شرکت پذیر است.

مثال ۳۱.۲.۲. فرض کنیم n یک عدد طبیعی باشد. در این صورت $(\mathbb{Z}_n, \cdot)$ یک گروه نیست. برای تعریف اعداد پیمانه‌ای $\mathbb{Z}_n$ و عمل دوتایی ضرب روی این مجموعه به فصل اول بخش دوم مراجعه نمایید. واضح است که $\bar{۱}$ عضو خنثی است. اما وارون عنصر $\bar{۰}$ وجود ندارد. با یک محاسبه سر راست این عمل ضرب شرکت پذیر است.

مثال ۳۲.۲.۲. $(\mathbb{Z}_۴ \setminus \{\bar{۰}\}, \cdot)$ یک گروه نیست. برای تعریف اعداد پیمانه‌ای $\mathbb{Z}_n$ و عمل دوتایی ضرب روی این مجموعه به فصل اول بخش دوم مراجعه نمایید. واضح است که $\bar{۱}$ عضو خنثی است. اما وارون عنصر $\bar{۲}$ وجود ندارد (چرا؟).

مثال ۳۳.۲.۲. فرض کنیم p یک عدد اول باشد. در این صورت $(\mathbb{Z}_p \setminus \{\bar{۰}\}, \cdot)$ یک گروه است. برای تعریف اعداد پیمانه‌ای $\mathbb{Z}_p$ و عمل دوتایی ضرب روی این مجموعه به فصل اول بخش دوم مراجعه نمایید. واضح است که $\bar{۱}$ عضو خنثی است. با یک محاسبه سر راست این عمل ضرب شرکت پذیر است. اکنون وارون یک عضو مانند $\bar{x}$ را ارائه می‌کنیم. چون $\bar{x}$ مخاف با $\bar{۰}$ است پس در $\mathbb{Z}$ داریم $(x,p) = ۱$. طبق قضیه بزو، قضیه ۱۰.۲.۱ ، اعداد صحیح r و s وجود دارند که $rx + sp = ۱$. در نتیجه $\bar{۱} = \overline{rx} = \overline{rx+sp}$. پس $\bar{r} \cdot \bar{x} = \bar{۱}$. یعنی $\bar{x}$ وارون پذیر است.

مثال ۳۴.۲.۲. مجموعه ریشه‌های nام واحد با ضرب معمولی اعداد مختلط یک گروه است، یعنی

$$G = \{w \in \mathbb{C} \mid w^n = ۱\}.$$

اگر $w, w' \in G$ انگاه $(ww')^n = w^n w'^n = ۱$. پس $ww' \in G$ و به ضرب بسته است. شرکتپذیر از اعداد مختلط به ارث می‌رسد. عنصر خنثی برابر ۱ است و وارون هر عنصر w برابر $w^{n-۱}$ است.

تذکر ۳۵.۲.۲. گاهی کشیدن یک جدول برای گروه کار را ساده‌تر می‌کند. فرض کنیم G یک گروه باشد که کاردینال آن متناهی است. مثلا فرض کنیم $G = \{e, a_۱, a_۲, ..., a_{n-۱}\}$ که e عنصر خنثی برای G است. می‌توانیم به G جدولی مانند زیر وابسته کنیم.

	e	$a_۱$	$a_۲$	$\cdots$	$a_{n-۱}$
e	e	$a_۱$	$a_۲$	$\cdots$	$a_{n-۱}$
$a_۱$	$a_۱$	$a_۱a_۱$	$a_۱a_۲$	$\cdots$	$a_۱a_{n-۱}$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$a_{n-۱}$	$a_{n-۱}$	$a_{n-۱}a_۱$	$a_{n-۱}a_۲$	$\cdots$	$a_{n-۱}a_{n-۱}$

مثال ۳۶.۲.۲. برای گروه $(\mathbb{Z}_۴, +)$ نمایش جدولی به صورت زیر است

	$\bar{۰}$	$\bar{۱}$	$\bar{۲}$	$\bar{۳}$
$\bar{۰}$	$\bar{۰}$	$\bar{۱}$	$\bar{۲}$	$\bar{۳}$
$\bar{۱}$	$\bar{۱}$	$\bar{۱}+\bar{۱}$	$\bar{۱}+\bar{۲}$	$\bar{۱}+\bar{۳}$
$\bar{۲}$	$\bar{۲}$	$\bar{۲}+\bar{۱}$	$\bar{۲}+\bar{۲}$	$\bar{۲}+\bar{۳}$
$\bar{۳}$	$\bar{۳}$	$\bar{۳}+\bar{۱}$	$\bar{۳}+\bar{۲}$	$\bar{۳}+\bar{۳}$

که بعد از محاسبه داریم

	۰̄	۱̄	۲̄	۳̄
۰̄	۰̄	۱̄	۲̄	۳̄
۱̄	۱̄	۲̄	۳̄	۰̄
۲̄	۲̄	۳̄	۰̄	۱̄
۳̄	۳̄	۰̄	۱̄	۲̄

نمادگذاری ۳۷.۲.۲. *در سرتاسر این فصل منظور از e_G یا e یعنی عنصر خنثی گروه G. مگر این که به صراحت خلاف این مطلب را ذکر کنیم. اگر در مبحثی چند گروه مطرح باشد از نماد e_G، e_H و ... استفاده می‌کنیم تا ابهامی ایجاد نشود.*

تعریف ۳۸.۲.۲. *گروه $(G, *)$ را آبلی گوییم هرگاه $*$ جابجایی باشد.*

مثال ۳۹.۲.۲. *$(\mathbb{Z}, +)$ یک گروه آبلی است.*

مثال ۴۰.۲.۲. *$(GL_n(\mathbb{R}), \cdot)$ گروه آبلی نیست (ضرب ماترس‌ها (حتی وارون پذیرها) در حالت کلی جابجایی نیست).*

قضیه ۱۷.۱.۲ سبب می‌شود که پرانتز گذاری برای عمل دوتایی شرکت پذیر بی اهمیت شود که این منجر به تعریف زیر می‌شود.

تعریف ۴۱.۲.۲. *فرض کنیم $*$ عمل دوتایی شرکت پذیر روی S باشد (نیم‌گروه) و $n \in \mathbb{N}$. برای $a \in S$ توان a را به استقرا به صورت زیر تعریف می‌کنیم*

$$a^{۱} = a, \;\; a^{۲} = a * a, \;\; a^{۳} = a^{۲} * a, \;\; a^n = a^{n-۱} * a.$$

به طور ویژه، اگر S گروه با عنصر خنثی e باشد و $k \in \mathbb{Z}$ آنگاه برای $g \in S$ تعریف می‌کنیم

$$g^k = \begin{cases} \underbrace{g * g * \ldots * g}_{k\text{تا}} & k > ۰ \\ e & k = ۰ \\ \underbrace{g^{-۱} * g^{-۱} * \ldots * g^{-۱}}_{k\text{تا}} & k < ۰ \end{cases}$$

مثال ۴۲.۲.۲. *عمل دوتایی $+$ روی $\mathbb{Z}$ شرکت پذیر است و برای $x \in \mathbb{Z}$ و هر عدد طبیعی n داریم*

$$\underbrace{x + x + \ldots + x}_{n\text{تا}} = nx.$$

مثال ۴۳.۲.۲. *عمل دوتایی $\cdot$ روی $\mathbb{R}$ شرکت پذیر است و برای $x \in \mathbb{R}$ و هر عدد طبیعی n داریم*

$$\underbrace{x \cdot x \cdot \ldots \cdot x}_{n\text{تا}} = x^n.$$

قضیه ۴۴.۲.۲. *فرض کنیم $(S,*)$ گروه باشد و $a \in S$. برای اعداد صحیح m و n داریم.*
(الف) $(a^m)^n = a^{mn}$
(ب) $a^m * a^n = a^{m+n}$

اثبات. سر راست است. □

در ادامه قضیه‌های را خواهیم آورد که نشان می‌دهد در چه زمانی یک نیم‌گروه یک گروه است.

قضیه ۴۵.۲.۲. *نیم‌گروه $(G,*)$ گروه است اگر و تنها اگر برای هر $a,b \in G$ معادلات $a*x=b$ و $y*a=b$ جواب داشته باشند.*

اثبات. $(\Leftarrow)$. چون G گروه است، قرار می‌دهیم $x = a^{-1} * b$. در این صورت $a*x=b$ دارای جواب است. برای معادله دوم از $y = b * a^{-1}$ استفاده می‌کنیم.
$(\Rightarrow)$. چون G نیم‌گروه است شرکت پذیر است. نشان می‌دهیم G عضو خنثی دارد. چون معالات برای هر a و b جواب دارند، a را با b مساوی می‌گیریم. پس معادله $a*x=a$ دارای جواب e است. حال برای c، نشان می‌دهیم $c*e=c$ یعنی e خنثی چپ است. معادله $y*a=c$ دارای جواب f است. یعنی $f*a=c$. پس

$$c*e=(f*a)*e=f*(a*e)f*a=c.$$

با روش مشابه وجود عضو خنثی راست اثبات می‌شود. طبق گزاره ۹.۲.۲، e عضو خنثی گروه است. اکنون فرض کنیم $c \in G$ دلخواه باشد. نشان می‌دهیم c وارون پذیر است. معادله $c*x=e$ دارای جواب c' است و معادله $y*c=e$ دارای جواب c'' است. c' و c'' به ترتیب وارون راست و چپ برای c هستند. طبق گزاره ۱۸.۲.۲، $c'=c''$ و c وارون پذیر است. □

تعریف ۴۶.۲.۲. *فرض کنیم $*$ یک عمل دوتایی روی S باشد. گوییم:*
(الف) *قانون حذف از چپ در S برقرار است اگر $a,b,c \in S$ و $c*a=c*b$ آنگاه نتیجه شود $a=b$.*
(ب) *قانون حذف از راست در S برقرار است اگر $a,b,c \in S$ و $a*c=b*c$ آنگاه نتیجه شود $a=b$.*
(ج) *قانون حذف برقرار است هرگاه هم حذف چپ و هم حذف راست برقرار باشد.*

مثال ۴۷.۲.۲. *در گروه $(\mathbb{Z},+)$ قانون حذف داریم. زیرا $(\mathbb{Z},+)$ یک گروه آبلی است و فقط کافی است حذف چپ را نشان دهیم. فرض کنیم $c+a=c+b$. با جمع طرفین تساوی با $-c$ داریم $a=b$.*

مثال ۴۸.۲.۲. *در نیم‌گروه $(\mathbb{N},*)$ که $*$ همان عمل دوتایی ضرب معمولی است، قانون حذف (چپ– راست) برقرار است.*

مثال ۴۹.۲.۲. *$(\mathbb{R},*)$ که در آن $a*b=3$ نه حذف چپ برقرار است نه حذف راست.*

مثال ۵۰.۲.۲. *فرض کنیم $S=\{۱,۲\}$ و برای هر $a,b\in S$ تعریف می‌کنیم $a*b=b$. واضح است که اگر $c*a=c*b$ آنگاه $a=b$. پس حذف چپ برقرار است. یک بررسی ساده نشان می‌دهد حذف راست برقرار نیست.*

حال قضیه زیر را داریم.

قضیه ۵۱.۲.۲. *نیم‌گروه متناهی $(G,*)$ گروه است اگر و تنها اگر قانون حذف در G برقرار باشد.*

اثبات. $(\Leftarrow)$. فرض کنیم برای $a,b,c\in G$ داشته باشیم $c*a=c*b$. چون G گروه است پس c در G وارون دارد. با انجام عمل دوتایی طرفین تساوی بالا از سمت چپ در $c^{-۱}$ داریم

$$c^{-۱}*c*a=c^{-۱}*c*b \;\Rightarrow\; e*a=e*b \;\Rightarrow\; a=b.$$

قانون حذف از راست مشابه بالا اثبات می‌شود و در نتیجه قانون حذف داریم.
$(\Rightarrow)$. فرض کنیم $G=\{a_۱,a_۲,...,a_n\}$. طبق قضیه ۴۵.۲.۲، برای این که نشان دهیم G گروه است، کافی است نشان دهیم برای $a,b\in G$، معادلات $a*x=b$ و $y*a=b$ جواب دارند. مجموعه زیر را در نظر می‌گیریم

$$A=\{a*a_۱,a*a_۲,...,a*a_n\}.$$

واضح است که $A\subseteq G$ (چرا؟). حال اگر $a*a_i=a*a_j$ که $۱\le i,j\le n$، آنگاه بر طبق فرض قانون حذف از چپ بر قرار است و درنتیجه $a_i=a_j$. این نشان می‌دهد که اعضای A متمایز هستند و باید $|A|=n$ (چرا؟). یعنی داریم

$$A=\{a*a_۱,a*a_۲,...,a*a_n\}=G=\{a_۱,a_۲,...,a_n\}.$$

فرض کنیم $b=a_i$. پس a_j چنان وجو دارد که $a*a_j=a_i$ و این یعنی معادله $ax=b$ دارای جواب $x=a_j$ است. به روش مشابه و با در نظر گرفتن

$$B=\{a_۱*a,a_۲*a,...,a_n*a\}$$

می‌توان نشان داد که $y*a=b$ جواب دارد. بنابراین بر طبق قضیه ۴۵.۲.۲ اثبات کامل است. □

اکنون این بخش را با قضیه زیر که منسوب به شخص هَیز[۲] است به پایان می‌رسانیم.

قضیه ۵۲.۲.۲. *(هَیز) نیم‌گروه $(G,*)$ گروه است اگر و تنها اگر برای هر عنصر a در G، عنصر یکتای $a'\in G$ وجود داشته باشد که $aa'a=a$.*

اثبات. $(\Leftarrow)$. چون G گروه است کافی است a' را همان $a^{-۱}$ در نظر بگیریم و این یعنی دست کم یک a' وجود دارد که $a*a'*a=a$. حال اگر داشته باشیم $a*a''*a=a$ که $a''\in G$. پس $a*a''*a=a*a'*a$. با دوبار استفاده از قضیه ۵۱.۲.۲، داریم $a'=a''$.

[۲] Hays

$(\Rightarrow)$. برای اثبات این قسمت ابتدا دو ادعای زیر را اثبات می‌کنیم:
ادعا ۱: عنصر b در G چنان وجود دارد که $b^{۲} = b$.
اثبات ادعا ۱: فرض کنیم $a \in G$. طبق فرض عنصر یکتای $a' \in G$ وجود دارد که $a * a' * a = a$.
قرار می‌دهیم $b = a * a'$ و داریم

$$b^{۲} = b * b = (a * a') * (a * a') = (a * a' * a) * a' = a * a' = b$$

پس ادعای ۱ اثبات شد.
ادعا ۲: فقط یک عنصر در $b \in G$ وجود دارد که $b^{۲} = b$.
اثبات ادعا ۲: فرض کنیم $c \in G$ و $c^{۲} = c$. واضح است که $b * c \in G$ (چرا؟) و در نتیجه طبق فرض $(b * c)'$ وجود دارد که

$$(b * c) * (b * c)' * (b * c) = b * c.$$

حال داریم

$$\begin{aligned}
&(b * c) * [(b * c)' * b] * (b * c) = (b * c) * (b * c)' * (b * b) * c = \\
&(b * c) * (b * c)' * b^{۲} * c = (b * c) * (b * c)' * b * c = \\
&(b * c) * (b * c)' * (b * c) = b * c.
\end{aligned}$$

چون فرض یکتایی را داریم پس باید $(b * c)' * b = (b * c)'$. به روش مشابه داریم

$$\begin{aligned}
&(b * c) * [c * (b * c)'] * (b * c) = b * (c * c) * (b * c)' * (b * c) = \\
&b * c^{۲} * (b * c)' * (b * c) = b * c * (b * c)' * (b * c) = \\
&(b * c) * (b * c)' * (b * c) = b * c.
\end{aligned}$$

چون فرض یکتایی را داریم پس باید $c * (b * c)' = (b * c)'$. از سوی دیگر داریم

$$\begin{aligned}
&(b * c) * [(b * c)' * (b * c) * (b * c)'] * (b * c) = \\
&[(b * c) * (b * c)' * (b * c)] * (b * c)' * (b * c) = \\
&(b * c) * (b * c)' * (b * c) = b * c.
\end{aligned}$$

چون فرض یکتایی را داریم پس باید

$$(b * c)' * (b * c) * (b * c)' = (b * c)' \qquad (I)$$

حال

$$\begin{aligned}
&((b * c)')^{۲} = (b * c)' * (b * c)' = \\
&[(b * c)' * b] * [c * (b * c)'] = (b * c)' * (b * c) * (b * c)' = (b * c)'
\end{aligned}$$

یعنی $(b*c)' = ((b*c)')^{۲}$. بنابراین

$$(b*c)' * (b*c)' * (b*c)' = (b*c)' \qquad (II)$$

اما (I) و (II) همراه با فرض یکتایی نشان می‌دهند که $(b*c)' = b*c$. در نتیجه $(b*c)^{۲} = b*c$ (چرا؟). حال داریم

$$(b*c)*b*(b*c) = (b*c)*(b*b)*c = (b*c)*b^{۲}*c =$$
$$(b*c)*b*c = (b*c)*(b*c) = (b*c)^{۲} = b*c.$$

به روش مشابه $(b*c)*c*(b*c) = b*c$ (بررسی کنید). از فرض یکتایی باید $b = c$. اثبات ادعای ۲ کامل است.
اکنون نشان می‌دهیم G گروه است. طبق ادعا ۱، G دارای عنصری مانند e است که $e^{۲} = e$. طبق ادعا ۲، e یکتا است. حال فرض کنیم $g \in G$ دلخواه باشد. طبق فرض $g' \in G$ وجود دارد که $g*g'*g = g$. واضح است که $(g*g')^{۲} = g*g'$. چون e یکتا است پس $g*g' = e$. از طرفی دیگر $(g'*g)^{۲} = g'*g$. یکتایی e نتیجه می‌دهد که $g'*g = e$. بنابراین $e*g = g = g*e$. این یعنی e عنصر همانی است. چون $g*g' = e$ و $g'*g = e$ پس g وارون پذیر است. اثبات این که G گروه است. □

تمرین‌های حل شده

تمرین ۵۳.۲.۲. *عمل دوتایی $a*b = \dfrac{ab}{۱۳}$ را روی $\mathbb{Q}$ در نظر بگیرید. عضو خنثی و وارون هر عضو را معلوم کنید.*

حل. دقت شود که این عمل جابجایی است (چرا؟) پس صحبت از چپ و راست بی معنی است.
معرفی عضو خنثی: فرض کنیم $x \in \mathbb{Q}$ عضو خنثی این عمل دوتایی باشد. پس برای هر $a \in \mathbb{Q}$ داریم $a*x = a$. یعنی $\dfrac{ax}{۱۳} = a$. در نتیجه $x = ۱۳$ و این یعنی $e = ۱۳$ عنصر خنثی است.
معرفی وارون هر عضو: عنصر دلخواه $x \in \mathbb{Q}$ را درنظر می‌گیریم. وارون پذیری x معادل با این است که عنصر $a \in \mathbb{Q}$ موجود باشد که $a*x = e = ۱۳$. یعنی $\dfrac{ax}{۱۳} = ۱۳$. این نشان می‌دهد که اگر a ناصفر باشد آنگاه دارای وارون $a^{-۱} = \dfrac{۱۳^{۲}}{a}$ است.

تمرین ۵۴.۲.۲. *فرض کنیم*

$$S = \{\begin{pmatrix} a & b \\ ۰ & ۰ \end{pmatrix} \mid a, b \in \mathbb{Z}\}.$$

روی S عمل دوتایی $*$ را همان ضرب عادی ماتریسی بگیرید. آیا $*$ شرکت پذیر است؟ آیا $*$ عضو خنثی (چپ‌ـ راست) دارد؟

حل. ابتدا دقت شود که ضرب عادی ماتریسی از S خارج نمی‌شود. زیرا

$$\begin{pmatrix} a & b \\ ۰ & ۰ \end{pmatrix} \cdot \begin{pmatrix} a' & b' \\ ۰ & ۰ \end{pmatrix} = \begin{pmatrix} aa' & ab' \\ ۰ & ۰ \end{pmatrix} \in S.$$

چون ضرب عادی ماتریسی در حالت کلی شرکت پذیر است پس روی S نیز شرکت پذیری را داریم.
برای هر عدد صحیح x عنصر

$$\begin{pmatrix} ۱ & x \\ ۰ & ۰ \end{pmatrix}$$

در S یک عنصر خنثی چپ است. زیرا

$$\begin{pmatrix} ۱ & x \\ ۰ & ۰ \end{pmatrix} \cdot \begin{pmatrix} a & b \\ ۰ & ۰ \end{pmatrix} = \begin{pmatrix} a & b \\ ۰ & ۰ \end{pmatrix}.$$

یعنی S نامتناهی خنثی چپ دارد. اما S نمی‌تواند خنثی راست داشته باشد. زیرا اگر S خنثی راست داشته باشد آنگاه طبق گزاره ۹.۲.۲، آنگاه نامتناهی عنصر خنثی راست داریم در حالی که طبق گزاره ۹.۲.۲، عنصر خنثی یکتا باید باشد.

تمرین ۵۵.۲.۲. *فرض کنیم نیم‌گروه $(S, *)$ دارای عضو خنثی e و دو عنصر a و b وارون پذیر (چپ_ راست) باشند. آنگاه نشان دهید که $a * b$ وارون پذیر (چپ_ راست) است. سپس وارون $a_۱ * a_۲ * \ldots * a_n$ را پیدا کنید.*

حل. فقط کافی است وارون چپ داشتن $a * b$ را اثبات کنیم، وارون راست مشابه است. فرض کنیم وارون چپ a، c باشد یعنی $c * a = e$ و وارون چپ b، d باشد یعنی $d * b = e$. ادعا می‌کنیم $a * b$ دارای وارون $d * c$ است. زیرا با فرض نیم‌گروه داریم

$$(d * c) * (a * b) = d * c * a * b = d * e * b = d * b = e.$$

برای قسمت دوم، واضح است که با استقرای ضعیف، وارون عنصر $a_۱ * a_۲ * \ldots * a_n$ برابر است با $a_n^{-۱} * \ldots * a_۲^{-۱} * a_۱^{-۱}$.

تمرین ۵۶.۲.۲. *برای گروه $(G, *)$ نشان دهید که $(a^{-۱})^{-۱} = a$.*

حل. داریم که $a * a^{-۱} = e$. پس a وارون $a^{-۱}$ است و طبق تعریف وارون مسئله حل است.

تمرین ۵۷.۲.۲. *فرض کنیم $\mathbb{Q}[\sqrt{۲}] = \{a + b\sqrt{۲} \mid a, b \in \mathbb{Q}\}$. نشان دهید که $\mathbb{Q}[\sqrt{۲}]$ با عمل دوتایی زیر یک گروه است.*

$$(a + b\sqrt{۲}) + (a' + b'\sqrt{۲}) = (a + a') + (b + b')\sqrt{۲}$$

حل. *ابتدا شرکت پذیری را بررسی می‌کنیم.*

$$(a + b\sqrt{۲}) + [(a' + b'\sqrt{۲}) + (a'' + b''\sqrt{۲})] =$$
$$(a + b\sqrt{۲}) + [(a' + a'') + (b' + b'')\sqrt{۲}] = (a + a' + a'') + (b + b' + b'')\sqrt{۲} =$$
$$[(a + b\sqrt{۲}) + (a' + b'\sqrt{۲})] + (a'' + b''\sqrt{۲})$$

واضح است که $۰ + ۰\sqrt{۲}$ عنصر خنثی است. وارون $a + b\sqrt{۲}$ برابر است با $-a - b\sqrt{۲}$.

تمرین ۵۸.۲.۲. *نشان دهید که برای یک مجموعه X، $(\mathbb{P}(X), \cap)$ گروه نیست.*

حل. اگر $A, B \in \mathbb{P}(X)$ آنگاه واضح است که $A \cap B \in \mathbb{P}(X)$، یعنی اشتراک یک عمل دوتایی است. شرکت پذیری عمل دوتایی اشتراک واضح است. مجموعه X در نقش عنصر خنثی است. اگر $A \neq X$ آنگاه واضح است که برای هر زیرمجموعه Y از X همواره $A \cap Y \subsetneq X$، یعنی A وارون ندارد. پس $(\mathbb{P}(X), \cap)$ گروه نیست.

تمرین ۵۹.۲.۲. *فرض کنیم n یک عدد طبیعی باشد. عناصر وارون پذیر $\mathbb{Z}_n$ نسبت به عمل ضرب را با $U(\mathbb{Z}_n)$ نشان می‌دهیم. ثابت کنید که:*
(الف) $U(Z_n) = \{\bar{x} \mid (x, n) = ۱\}$.
(ب) *$U(\mathbb{Z}_n)$ با همان ضرب $\mathbb{Z}_n$ یک گروه است.*

حل. (الف) فرض کنیم $T = \{\bar{x} \mid (x, n) = ۱\}$ و $\bar{x} \in U(Z_n)$. پس عنصر $\bar{y}$ چنان وجود دارد که $\bar{x} \cdot \bar{y} = \bar{۱}$ یا معادلا $\overline{xy} = \bar{۱}$. این نتیجه می‌دهد که $n|xy - ۱$. پس $(n, xy) = ۱$ و در نتیجه $(n, x) = ۱$. پس $\bar{x} \in T$ و $U(Z_n) \subseteq T$.
فرض کنیم $\bar{x} \in T$. پس $(x, n) = ۱$ و در نتیجه از قضیه بزو، قضیه ۱۰.۲.۱، اعداد صحیح r و s وجود دارند که $rx + sn = ۱$. در نتیجه $\overline{rx + sn} = \overline{rx} = \bar{۱}$. پس $\bar{r} \cdot \bar{x} = \bar{۱}$. یعنی $\bar{x}$ وارون پذیر است. بنابراین $T \subseteq U(Z_n) \ni \bar{x}$.
(ب) طبق تمرین ۵۵.۲.۲، حاصل ضرب دو عنصر وارون پذیر، وارون پذیر است، یعنی $\cdot$ روی $U(\mathbb{Z}_n)$ عمل دوتایی است. $\bar{۱}$ عضو خنثی است و شرکت پذیری هم از $\mathbb{Z}_n$ به ارث می‌رسد.

تمرین ۶۰.۲.۲. *اگر $(G, *)$ یک گروه متناهی بیشتر از ۲ عضو با عنصر خنثی e باشد آنگاه عنصر $e \neq g \in G$ وجود دارد که $g^۲ = g$ $(g^۲ = g * g)$.*

حل. فرض کنید $g \in G$. مجموعه $T = \{g^۲, g^۴, g^۸, ...\}$ را در نظر می‌گیریم. چون G نیم‌گروه است، برای هر عدد طبیعی k داریم که $g^k \in G$. در نتیجه $T \subseteq G$. اما G متناهی است، پس باید برای اعداد طبیعی متمایز i و j داشته باشیم $g^{۲^i} = g^{۲^j}$. بدون کم شدن از کلیت فرض کنیم $۱ \leq i < j$. پس طبق قضیه ۴۴.۲.۲ داریم

$$g^{۲^j} = (g^{۲^i})^{۲^{j-i}} = g^{۲^i}.$$

قرار می‌دهیم $k = ۲^{j-i}$ و $h = g^{۲^i}$. پس $h^k = h$. حال دو حالت رخ می‌دهد.
حالت اول. $k = ۲$ که کار تمام است و h همان مطلوب مسئله است.
حالت دوم. $k > ۲$ که با قضیه ۴۴.۲.۲ داریم

$$h^{k-۲} * h^k = h^{k-۲} * h \;\Rightarrow\; (h^{k-۱})^۲ = h^{k-۱}.$$

در این حالت $h^{k-۱}$ همان مطلوب مسئله است.

تمرین ۶۱.۲.۲. *فرض کنیم G گروهی باشد که برای هر عنصر $g \in G$ داریم $g^۲ = e$. نشان دهید G آبلی است.*

حل. برای هر $a \in G$، چون $a^{۲} = e$ پس $a = a^{-۱}$. فرض کنیم $g, h \in G$. در نتیجه طبق فرض داریم $(g * h)^{۲} = e$. پس

$$g * h * g * h = e \ \Rightarrow \ g^{-۱} * g * h * g * h = g^{-۱} \ \Rightarrow \ h * g * h = g^{-۱} = g.$$

حال طرفین تساوی آخر از سمت چپ در $h^{-۱}$ عمل دوتایی می‌کنیم

$$h * g * h = g \ \Rightarrow \ h^{-۱} * h * g * h = h^{-۱} * g = h * g \ \Rightarrow \ g * h = h * g.$$

تمرین ۶۲.۲.۲. *برای گروه $(G, *)$ و عدد طبیعی n نشان دهید که* $a*b^n*a^{-۱} = (a*b*a^{-۱})^n$.

حل. داریم

$$(a * b * a^{-۱})^n = \underbrace{a * b * a^{-۱} * a * b * a^{-۱} * \ldots * a * b * a^{-۱}}_{n\text{تا}}$$

چون $a^{-۱} * a = e$ و $b * e = b$ پس سمت راست تساوی با قضیه ۴۴.۲.۲، برابر است با $a * b^n * a^{-۱}$.

تمرین ۶۳.۲.۲. *نشان دهید هر گروه حداکثر ۵ عضو آبلی است.*

حل. برای گروه یک عضوی و دو عضوی چیزی برای اثبات نداریم. فرض کنیم G گروه سه عضوی باشد. یعنی $G = \{e, a, b\}$ که e عنصر همانی است. مشکل اساسی ما $a * b$ است! اگر $a * b = a$ باشد آنگاه داریم $a^{-۱} * a * b = a^{-۱} * a = e$ یعنی $b = e$ است که تناقض با سه عضوی بودن گروه است. مشابه اگر $a * b = b$ باشد آنگاه داریم $a * b * b^{-۱} * = b * b^{-۱} = e$ یعنی $a = e$ است که تناقض با سه عضوی بودن گروه است. اگر $a * b$ برابر e شود آنگاه a و b وارون هم هستند و لذا جابجا می‌شوند. حال فرض کنیم گروه چهار عضوی باشد. فرض کنیم e عنصر خنثی گروه باشد. دو عنصر متمایز از هم و متمایز از e مانند a و b انتخاب می‌کنیم. مشابه استدلال گروه سه عضوی، باید $a * b$ عنصر چهارم باشد. حال $b * a$ باید یکی از e، a، b و $a * b$ باشد. اگر $b * a = e$ آنگاه a و b وارون هم هستند و در نتیجه گروه سه عضوی می‌شود که تناقض است. اگر $b * a = a * b$ آنگاه چیزی برای اثبات نداریم. دو حالت دیگر هم رخ نمی‌دهد چون a و b مخالف e هستند. برای گروه پنج عضوی روند بالا را تکرار کنید.

تمرین ۶۴.۲.۲. *آیا در قضیه ۴۵.۲.۲، وجود جواب برای یک معادله مثلا $ax = b$ برای گروه شدن G کافی است؟*

حل. خیر کافی نیست و مثال نقض وجود دارد. فرض کنیم $G = \{۱, ۲\}$ و برای هر $a, b \in S$ تعریف می‌کنیم $a * b = b$. واضح است که G نیم‌گروه است و برای $a, b \in G$ همواره $ax = b$ دارای جواب $x = b$ است. اما G گروه نیست. زیرا عضو خنثی راست وجود ندارد.

تمرین ۶۵.۲.۲. *آیا در قضیه ۵۱.۲.۲ شرط متناهی بودن لازم است؟*

حل. نیم‌گروه نامتناهی $(\mathbb{N}, \cdot)$ را در نظر می‌گیریم. در این نیم‌گروه قانون حذف برقرار است در حالی که گروه نیست (چرا؟).

تمرین ۶۶.۲.۲. *فرض کنیم $(G, *)$ یک گروه با عضو خنثی e باشد و $a, b \in G$. اگر $a^{۴} = e$ و $a^{۲} * b = b * a$ آنگاه نشان دهید که $a = e$.*

حل. چون G گره است پس اعضا وارون دارند و با عمل دوتایی طرفین تساوی $a^{۲} * b = b * a$ از چپ با $b^{-۱}$ داریم $b^{-۱} * a^{۲} * b = a$. طبق تمرین ۶۲.۲.۲، داریم

$$a^{۲} = (b^{-۱} * a^{۲} * b)^{۲} = b^{-۱} * a^{۴} * b.$$

چون $a^{۴} = e$ در نتیجه باید $a^{۲} = e$ باشد. اما فرض $a^{۲} * b = b * a$ ایجاب می‌کند که $b * a = b$. با عمل دوتایی طرفین تساوی آخر از سمت چپ در $b^{-۱}$ داریم $a = e$.

تمرین ۶۷.۲.۲. *فرض کنیم $(G, *)$ یک گروه متناهی باشد که $|G|$ عدد زوج است. نشان دهید $e \neq a \in G$ وجود دارد که $a^{۲} = e$ (e عضو خنثی گروه است).*

حل. مجموعه

$$A = \{g \in G \mid g \neq g^{-۱}\}$$

را در نظر می‌گیریم. واضح است که اگر $g \in A$ آنگاه $g^{-۱} \in A$ (چرا؟). از طرفی چون $A \subseteq G$ و G متناهی پس $|A|$ باید عدد زوج باشد (چرا؟). اکنون مجموعه $B = \{e\} \cup A$ یک مجموعه متناهی است و کاردینال آن عدد فرد است. این نشان می‌دهد که $B \subsetneq G$. پس عنصر $a \in G \setminus B$ وجود دارد که $a = a^{-۱}$ و این یعنی $a^{۲} = e$.

تمرین ۶۸.۲.۲. *فرض کنیم $(G, *)$ یک گروه با عنصر خنثی e باشد که برای $a, b \in G$ داریم $a * b = b * a^{-۱}$ و $b * a = a * b^{-۱}$. نشان دهید که $a^{۴} = b^{۴} = e$.*

حل. از فرض نتیجه می‌شود که $a = b * a^{-۱} * b^{-۱}$. و در نتیجه

$$b * a = a * b^{-۱} = b * a^{-۱} * b^{-۱} * b^{-۱} = b * a^{-۱} * b^{-۲}.$$

با انجام عمل دوتایی طرفین تساوی بالا از سمت چپ با $b^{-۱}$ داریم

$$a = a^{-۱} * b^{-۲}.$$

تساوی آخر نشان می۲دهد که $a^{۲} = b^{-۲}$. بنابراین

$$a^{۴} = a^{۲} * a^{۲} = a^{۲} * b^{-۲} = a * (a * b^{-۱}) * b^{-۱} = a * (b * a) * b^{-۱} =$$
$$(a * b) * a * b^{-۱} = (b * a^{-۱}) * a * b^{-۱} = b * a^{-۱} * a * b^{-۱} = e$$

با روندی مشابه اثبات می‌شود که $b^{۴} = e$.

تمرین ۶۹.۲.۲. *نشان دهید که اگر در گروه $(G,*)$ ، برای سه عدد صحیح متوالی مانند n داشته باشیم $(a*b)^n = a^n * b^n$ آنگاه G آبلی است.*

حل. فرض کنیم

$$(a*b)^{n+۲} = a^{n+۲} * b^{n+۲} \qquad (a*b)^{n+۱} = a^{n+۱} * b^{n+۱} \qquad (a*b)^n = a^n * b^n$$

پس

$$a^{n+۱} * b^{n+۱} = (a*b)^{n+۱} = (a*b)*(a*b)^n = a*b*a^n*b^n.$$

با انجام عمل دوتایی مناسب در طرفین تساوی داریم $a^n * b = b * a^n$ (چگونه؟). از طرفی دیگر

$$a^{n+۲} * b^{n+۲} = a^{n+۱} * b^{n+۱} = (a*b)*(a*b)^{n+۱} = a*b*a^{n+۱}*b^{n+۱}.$$

با انجام عمل دوتایی مناسب در طرفین تساوی داریم $a^{n+۱} * b = b * a^{n+۱}$ (چگونه؟). بنابراین

$$b * a^{n+۱} = a^{n+۱} * b = a * a^n * b = a * b * a^n.$$

با انجام عمل دوتایی مناسب در طرفین تساوی داریم $a*b = b*a$. یعنی G آبلی است.

۳.۲ چند مثال خاص از گروه‌ها

در این قسمت چند مثال ویژه از گروه‌ها را به دست می‌دهیم. این مثال‌ها بسیار با اهمیت هستند و لازم است که دانشجو روی آن ها مسلط شود. در بخش‌های آینده برای ساختن مثال‌ها مناسب از مفاهیم جدید تسلط دانشجو بر مثال‌های زیر بسیار کمک کننده است. از این رو این مثال‌ها را در یک بخش جمع آوری کرده‌ایم.

همین قدر از اهمیت این مثال‌ها بدانید که در آرم شرکت‌های معروف مانند مرسدس بنز (گروه $D_۳$)، تا ملکول‌های مواد مانند $NH_۳$ (گروه $D_۳$)، تا زیبایی خانه‌های لوکس (گروه $D_۵$)، تا لوگوی معروف کرایسلر[۳] (گروه $D_۵$)، تا دانه‌های برف و کریستال و شن و ماسه، تا موجودات زنده مانند ستاره دریایی یا حتی غشای بیرونی ویروس HIV و ... گروه‌های متقارن ظاهر می‌شوند!

تعریف ۱.۳.۲. *هر تابع یک‌به‌یک و پوشا روی یک مجموعه مانند X را یک جایگشت نامیم. مجموعه همه جایگشت‌ها روی X را با S_X نمایش می‌دهیم. اگر $X = \{۱, ۲, ..., n\}$ باشد آنگاه از نماد S_n به جای S_X استفاده می‌کنیم.*

قضیه ۲.۳.۲. *اگر X یک مجموعه ناتهی باشد آنگاه S_X با عمل ترکیب یک گروه است.*

اثبات. ابتدا دقت کنید طبق قضیه ۲۶.۱.۱ به واقع ترکیب توابع یک عمل است و طبق قضیه ۲۵.۱.۱ این عمل شرکت پذیر است. واضح است که تابع همانی، id_X، عضو خنثی است و طبق قضیه ۲۸.۱.۱، هر عنصر در S_X وارونپذیر است. □

تعریف ۳.۳.۲. *به گروه S_X گروه متقارن روی مجموعه X گوییم. به گروه S_n، گروه متقارن روی n حرف یا گروه متقارن از درجه n گوییم. اعضای این گروه را معمولا با حروف σ، τ و ... نشان می‌دهیم.*

نمادگذاری ۴.۳.۲. *فرض کنیم $\sigma \in S_n$، یعنی σ یک تناظر روی $\{۱, ۲, ..., n\}$ است.* همچنین *می‌دانیم که σ عنصر i از S_n را به $\sigma(i)$ نظیر می‌کند یعنی $i \mapsto \sigma(i)$. این مطلب سبب می‌شود که بتوانیم اعضای S_n را به شکل جالبی نمایش دهیم و بتوانیم با این اعضا به صورت راحتتر مواجه شویم*

$$\sigma = \begin{pmatrix} ۱ & ۲ & ... & n \\ \sigma(۱) & \sigma(۲) & ... & \sigma(n) \end{pmatrix}.$$

اگر

$$\tau = \begin{pmatrix} ۱ & ۲ & ... & n \\ \tau(۱) & \tau(۲) & ... & \tau(n) \end{pmatrix}$$

[۳] Chrysler

جایگشت دیگری باشد آنگاه مثلا عنصر ۳ توسط σ به $j = \sigma(۳)$ نگاشته می‌شود و τ عنصر j را به $\tau(j)$ می‌نگارد. پس ترکیب به شکل زیر اعمل می‌شود

$$\sigma\tau = \begin{pmatrix} ۱ & ۲ & \dots & n \\ \tau\sigma(۱) & \tau\sigma(۲) & \dots & \tau\sigma(n) \end{pmatrix}.$$

مثال ۵.۳.۲. *اگر $X = \{۱\}$ باشد آنگاه $S_۱$ فقط عنصر $\sigma = \begin{pmatrix} ۱ \\ ۱ \end{pmatrix}$ را دارد که همان عنصر خنثی است.*

مثال ۶.۳.۲. *اگر $X = \{۱, ۲\}$ باشد آنگاه $S_۲$ فقط دو عنصر*

$$\sigma_۱ = \begin{pmatrix} ۱ & ۲ \\ ۱ & ۲ \end{pmatrix} \qquad \sigma_۲ = \begin{pmatrix} ۱ & ۲ \\ ۲ & ۱ \end{pmatrix}$$

را دارد که $\sigma_۱$ همان عنصر خنثی است. وارون عنصر $\sigma_۲$ خودش است.

مثال ۷.۳.۲. *اگر $X = \{۱, ۲, ۳\}$ باشد آنگاه $S_۳$ شش عنصر*

$$\sigma_۱ = \begin{pmatrix} ۱ & ۲ & ۳ \\ ۱ & ۲ & ۳ \end{pmatrix} \qquad \sigma_۲ = \begin{pmatrix} ۱ & ۲ & ۳ \\ ۲ & ۳ & ۱ \end{pmatrix} \qquad \sigma_۳ = \begin{pmatrix} ۱ & ۲ & ۳ \\ ۳ & ۱ & ۲ \end{pmatrix}$$

$$\sigma_۴ = \begin{pmatrix} ۱ & ۲ & ۳ \\ ۱ & ۳ & ۲ \end{pmatrix} \qquad \sigma_۵ = \begin{pmatrix} ۱ & ۲ & ۳ \\ ۳ & ۲ & ۱ \end{pmatrix} \qquad \sigma_۶ = \begin{pmatrix} ۱ & ۲ & ۳ \\ ۲ & ۱ & ۳ \end{pmatrix}$$

را دارد که $\sigma_۱$ همان عنصر خنثی است. وارون عنصر $\sigma_۲$ عنصر $\sigma_۳$ است. همچنین

$$\sigma_۳\sigma_۵ = \begin{pmatrix} ۱ & ۲ & ۳ \\ ۲ & ۱ & ۳ \end{pmatrix} = \sigma_۶.$$

قضیه ۸.۳.۲. *برای هر عدد طبیعی n، همواره داریم $|S_n| = n!$.*

اثبات. برای عنصر ۱ تعداد n حالت انتخاب ممکن است و برای عنصر ۲ تعداد $(n - ۱)$ حالت انتخاب ممکن است. دقت شود که قرار است تناظر باشد! روند را ادامه می‌دهیم و طبق اصل ضرب داریم

$$|S_n| = n \times (n - ۱) \times (n - ۲) \times \dots \times ۳ \times ۲ \times ۱ = n!$$

و اثبات کامل است. □

قضیه ۹.۳.۲. *وارون عنصر*

$$\begin{pmatrix} ۱ & ۲ & \dots & n \\ \sigma(۱) & \sigma(۲) & \dots & \sigma(n) \end{pmatrix}$$

برابر

$$\begin{pmatrix} \sigma(۱) & \sigma(۲) & \dots & \sigma(n) \\ ۱ & ۲ & \dots & n \end{pmatrix}$$

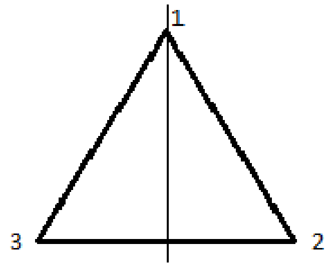
است.

اثبات. سر راست است. $\square$

تذکر ۱۰.۳.۲. *در قسمت تمرینات حل شده بخش دوم از فصل دوم مشاهده کردید که گروه‌های حداکثر پنج عضوی آبلی هستند اما $S_۳$ یک گروه ۶ $=|S_۳|$ عضوی است که غیر آبلی است زیرا $\sigma_۲\sigma_۴ \neq \sigma_۴\sigma_۲$.*

به مثال زیر توجه کنید.

مثال ۱۱.۳.۲. *یک مثلث متساوی الاضلاع را در نظر بگیرید که رئوس آن را با $X = \{۱, ۲, ۳\}$ شماره گذاری کرده‌ایم خطوط تقارن از راس‌ها رسم می‌کنیم یعنی*



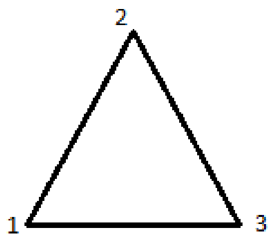
می‌توان به شکل بالا با کمک انعکاس جایگشت

$$\sigma_۱ = \begin{pmatrix} ۱ & ۲ & ۳ \\ ۱ & ۳ & ۲ \end{pmatrix}$$

را نظیر کرد. اگر بقیه خطوط تفارن را رسم کنیم به جایگشت‌های

$$\sigma_۲ = \begin{pmatrix} ۱ & ۲ & ۳ \\ ۲ & ۱ & ۳ \end{pmatrix} \qquad \sigma_۳ = \begin{pmatrix} ۱ & ۲ & ۳ \\ ۳ & ۲ & ۱ \end{pmatrix}$$

می‌رسیم. حال فرض کنید رئوس مثلث را به اندازه ۱۲۰ درجه در جهت خلاف عقربه ساعت دوران دهیم، یعنی



می‌توان به شکل بالا جایگشت

$$\tau_۱ = \begin{pmatrix} ۱ & ۲ & ۳ \\ ۳ & ۱ & ۲ \end{pmatrix}$$

را نظیر کرد. با دوران ۲۴۰ درجه و ۳۶۰ درجه داریم

$$\tau_{۲} = \begin{pmatrix} ۱ & ۲ & ۳ \\ ۲ & ۳ & ۱ \end{pmatrix} \qquad \tau_{۳} = \begin{pmatrix} ۱ & ۲ & ۳ \\ ۱ & ۲ & ۳ \end{pmatrix}$$

می‌رسیم. حال یک بررسی ساده نشان می‌دهد که

$$D_{۳} = \{\sigma_{۱}, \sigma_{۲}, \sigma_{۳}, \tau_{۱}, \tau_{۲}, \tau_{۳}\}$$

یک گروه است با عنصر همانی $\tau_{۳}$.

تعریف ۱۲.۳.۲. یک nـ ضلعی منتظم در نظر بگیرید. گروه متشکل از nتا انعکاس نسبت به محور تقارن و nتا دوران نسبت به مرکز چند ضلعی منتظم با زاویه $\frac{۲k\pi}{n}$ که $k \in \{۱, ..., n\}$ را گروه دو وجهی مرتبه n گوییم. این گروه را با D_n نشان می‌دهیم.

مثال ۱۳.۳.۲. گروه دو وجهی یک برف ریزه

گروه $D_{۶}$ است.

قضیه ۱۴.۳.۲. تعداد اعضای D_n برابر $۲n$ است.

اثبات. با توجه به ساختن D_n، nتا انعکاس و nتا دوران داریم پس $|D_n| = n + n = ۲n$. □

تعریف ۱۵.۳.۲. گروه چهارتایی کلاین دارای چهار عضو a، b، c و e است که e عضو همانی است. ضرب اعضای آن به صورت زیر تعریف می‌شود

$$ea = ae = a \quad eb = be = b \quad ec = ce = c \quad ee = e$$
$$a^{۲} = b^{۲} = c^{۲} = e \quad ab = ba = c \quad ac = ca = b \quad bc = cb = a$$

و این گروه را با $\mathbb{K}_{۴}$ نمایش می‌دهیم.

مثال ۱۶.۳.۲. جدول گروه $\mathbb{K}_4$ به شکل زیر است و این گروه آبلی است.

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

تعریف ۱۷.۳.۲. گروه کوترنیون‌ها دارای هشت عضو به صورت

$$\{1, -1, i, -i, j, -j, k, -k\}$$

است و ضرب اعضای آن به صورت زیر تعریف می‌شود

$$i^2 = j^2 = k^2 = -1 \qquad ij = k \qquad jk = i$$
$$ki = j \qquad ik = -j \qquad ji = -k \qquad kj = -i$$

و این گروه را با $\mathbb{Q}_8$ نمایش می‌دهیم. عنصر خنثی ۱ است.

مثال ۱۸.۳.۲. گروه $\mathbb{Q}_8$ غیر آبلی است. زیرا داریم $ij = k \neq ji = -k$.

مثال ۱۹.۳.۲. در گروه $\mathbb{Q}_8$ وارون عنصر j برابر $-j$ است. زیرا داریم

$$j(-j) = jik = (ji)k = -kk = (-1)kk = (-1)k^2 = (-1)(-1) = 1.$$

مواردی که در زیر می‌آید دست ما را برای داشتن گروه‌های متنوع باز می‌گذارد. هر چند این موارد را آنچنان که شایسته است گسترش نمی‌دهیم و فقط جهت آشنایی می‌آوریم.

تعریف ۲۰.۳.۲. فرض کنیم $\{G_i\}_{i\in I}$ خانواده‌ای ازگروه‌ها باشد. تمام دنباله‌ها به صورت $(x_i)_{i\in I}$ که برای هر $i \in I$، $x_i \in G_i$ را در نظر می‌گیریم. عمل دوتایی را به صورت

$$(x_i)_{i\in I} * (y_i)_{i\in I} = (x_i y_i)_{i\in I}$$

تعریف می‌کنیم و این دنباله‌ها را به یک گروه تبدیل می‌کنیم. در واقع، در مکان i ام عمل دوتایی گروه G_i پیاده می‌شود. گروه جدید را حاصل ضرب مستقیم یا حاصل ضرب دکارتی G_i ها گوییم و با $\prod_{i\in I} G_i$ نشان می‌دهیم. اگر I متناهی باشد از نماد $G_1 \times \ldots \times G_k$ نیز استفاده می‌کنیم که $k = |I|$. اگر I تهی باشد تعریف می‌کنیم $\prod_{i\in I} G_i = 0$.

تعریف ۲.۳.۲۱. *فرض کنیم $\{G_i\}_{i\in I}$ خانواده‌ای از گروه‌ها باشد. تمام دنباله‌ها به صورت $(x_i)_{i\in I}$ از $\prod_{i\in I} G_i$ را در نظر می‌گیریم که به جز تعداد متناهی اندیس بقیه مولفه‌ها عناصر خنثی هستند. با همان عمل دوتایی $\prod_{i\in I} G_i$ این دنباله‌ها گروه تشکیل می‌دهند. گروه جدید (در واقع زیرگروه $\prod_{i\in I} G_i$) را حاصل جمع مستقیم G_i ها گوییم و با $\bigoplus_{i\in I} G_i$ نشان می‌دهیم. اگر I متناهی باشد از نماد $G_1 \oplus \ldots \oplus G_k$ نیز استفاده می‌کنیم که $k = |I|$. اگر I تهی باشد تعریف می‌کنیم $\bigoplus_{i\in I} G_i = 0$.*

مثال ۲.۳.۲۲. *عنصر همانی گروه $\prod_{i\in I} G_i$ به صورت $(e_i)_{i\in I}$ است که e_i عنصر خنثی گروه G_i است.*

مثال ۲.۳.۲۳. *وارون عنصر $(x_i)_{i\in I}$ از گروه $\prod_{i\in I} G_i$ به صورت $(x_i^{-1})_{i\in I}$ است.*

مثال ۲.۳.۲۴. *فرض کنیم $G = S_3$ و $H = \mathbb{Z}_4$. دراین صورت*

$$G \times H = \{(\sigma, \bar{i}) \mid \sigma \in G, \;\; \bar{i} \in H\}$$

با عمل زیر

$$(\sigma, \bar{i}) * (\tau, \bar{j}) = (\sigma\tau, \bar{i} + \bar{j})$$

یک گروه است.

مثال ۲.۳.۲۵. *فرض کنیم $H = G = \mathbb{Z}_2$. دراین صورت*

$$G \times H = \{(\bar{i}, \bar{j}) \mid \bar{i}, \bar{j} \in H\}$$

با عمل زیر

$$(\bar{i}, \bar{j}) * (\bar{i}', \bar{j}') = (\overline{ii'}, \overline{jj'})$$

یک گروه است.

تمرین‌های حل شده

تمرین ۲.۳.۲۶. *آیا در گروه S_3 عنصری مانند σ وجود دارد که $\sigma\sigma$ همانی شود؟*

حل. با توجه به متن درس که اعضای S_3 را به دست آورده‌ایم، قرار می‌دهیم

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}.$$

حال داریم

$$\sigma\sigma = \sigma^2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}.$$

تمرین ۲.۳.۲۷. *آیا در گروه $S_۳$ عنصری مانند σ وجود دارد که $\sigma\sigma\sigma$ همانی شود؟*

حل. با توجه به متن درس که اعضای $S_۳$ را به دست آورده‌ایم، قرار می‌دهیم

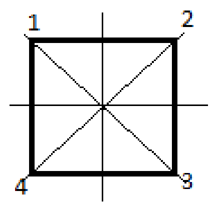
$$\sigma = \begin{pmatrix} ۱ & ۲ & ۳ \\ ۲ & ۳ & ۱ \end{pmatrix}.$$

حال داریم

$$\sigma\sigma\sigma = \sigma^۳ = \begin{pmatrix} ۱ & ۲ & ۳ \\ ۱ & ۲ & ۳ \end{pmatrix}.$$

تمرین ۲.۳.۲۸. *اعضای گروه $D_۴$ را بنویسید.*

حل. یک مربع را در نظر بگیرید که رئوس آن را با $X = \{۱, ۲, ۳, ۴\}$ شماره گذاری کرده‌ایم. خطوط تقارن مربع چهارتا است، یعنی



حال می‌توان به شکل بالا با کمک انعکاس جایگشت‌های

$$\sigma_۱ = \begin{pmatrix} ۱ & ۲ & ۳ & ۴ \\ ۱ & ۴ & ۳ & ۲ \end{pmatrix} \qquad \sigma_۲ = \begin{pmatrix} ۱ & ۲ & ۳ & ۴ \\ ۳ & ۲ & ۱ & ۴ \end{pmatrix}$$

$$\sigma_۳ = \begin{pmatrix} ۱ & ۲ & ۳ & ۴ \\ ۲ & ۱ & ۴ & ۳ \end{pmatrix} \qquad \sigma_۴ = \begin{pmatrix} ۱ & ۲ & ۳ & ۴ \\ ۴ & ۳ & ۴ & ۱ \end{pmatrix}$$

را نظیر کرد. حال فرض کنید رئوس مربع را به اندازه۹۰، ۱۸۰، ۲۷۰ و ۳۶۰ درجه در جهت خلاف عقربه ساعت دوران دهیم، جایگشت‌های

$$\tau_۱ = \begin{pmatrix} ۱ & ۲ & ۳ & ۴ \\ ۴ & ۱ & ۲ & ۳ \end{pmatrix} \qquad \tau_۲ = \begin{pmatrix} ۱ & ۲ & ۳ & ۴ \\ ۳ & ۲ & ۱ & ۴ \end{pmatrix}$$

$$\tau_۳ = \begin{pmatrix} ۱ & ۲ & ۳ & ۴ \\ ۲ & ۳ & ۴ & ۱ \end{pmatrix} \qquad \tau_۴ = \begin{pmatrix} ۱ & ۲ & ۳ & ۴ \\ ۱ & ۲ & ۳ & ۴ \end{pmatrix}$$

حال داریم

$$D_۴ = \{\sigma_۱, \sigma_۲, \sigma_۳, \sigma_۴, \tau_۱, \tau_۲, \tau_۳, \tau_۴\}$$

که یک گروه هشت عضوی است با عنصر همانی $\tau_۴$.

تمرین ۲.۳.۲۹. *برای $\mathbb{K}_4$ یک نمایش ماتریسی به دست آورید.*

حل. اعضای

$$E=\begin{pmatrix}1&0\\0&1\end{pmatrix}\qquad A=\begin{pmatrix}1&0\\0&-1\end{pmatrix}\qquad B=\begin{pmatrix}-1&0\\0&1\end{pmatrix}\qquad C=\begin{pmatrix}-1&0\\0&-1\end{pmatrix}$$

از $M_2(\mathbb{R})$ را در نظر می‌گیرم. با فرض $A=a$، $B=b$، $C=c$ و $E=e$ و ضرب ماتریسی عادی همان گروه $\mathbb{K}_4$ حاصل می‌شود.

تمرین ۲.۳.۳۰. *برای $\mathbb{Q}_8$ یک نمایش ماتریسی به دست آورید.*

حل. اعضای

$$A=\begin{pmatrix}1&0\\0&1\end{pmatrix}\qquad B=\begin{pmatrix}i&0\\0&-i\end{pmatrix}\qquad C=\begin{pmatrix}0&1\\-1&0\end{pmatrix}\qquad D=\begin{pmatrix}0&i\\i&0\end{pmatrix}$$

از $M_2(\mathbb{C})$ را در نظر می‌گیرم. با فرض $A=1$، $B=i$، $C=j$ و $D=k$ و ضرب ماتریسی عادی همان گروه $\mathbb{Q}_8$ حاصل می‌شود.

۴.۲ زیرگروه

در این بخش بررسی می‌کنیم چه زمانی یک زیرمجموعه ناتهی از یک گروه، خود یک گروه است.

تعریف ۱.۴.۲. *فرض کنیم G با عمل $*$ یک گروه باشد و $H \subseteq G$. گوییم H زیرگروه G است و با $H \leq G$ نمایش می‌دهیم هرگاه H با عمل $*$ که از G الحاق می‌شود، به گروه تبدیل شود.*

مثال ۲.۴.۲. *می‌دانیم که $(\mathbb{R}, +)$ یک گروه است. زیرمجموعه‌های $\mathbb{Z}$ و $\mathbb{Q}$ با عمل جمع الحاق شده از $\mathbb{R}$ گروه هستند. زیرا جمع الحاق شده روی $\mathbb{Z}$ بسته و شرکتپذیری است و همچنین عضو خنثی و وارون پذیری در $\mathbb{Z}$ و $\mathbb{Q}$ برقرار است و لذا $\mathbb{Z} \leq \mathbb{R}$ و $\mathbb{Q} \leq \mathbb{R}$.*

مثال ۳.۴.۲. *اگر e عنصر خنثی گروه G باشد آنگاه $\{e\}$ یک زیرگروه است. همچنین به وضوح G زیرگروه G است. به این دو زیرگروه که در هرگروه وجود دارد، زیرگروه‌های بدیهی گوییم.*

مثال ۴.۴.۲. *زیرمجموعه $۲\mathbb{Z} = \{۲k \mid k \in \mathbb{Z}\}$ یک زیرگروه از $(\mathbb{Z}, +)$ است. واضح است که برای هر $k, k' \in \mathbb{Z}$ داریم $۲(k + k') = ۲k + ۲k' \in ۲\mathbb{Z}$. پس $۲\mathbb{Z}$ نسبت به عمل دوتایی $+$ بسته است. صفر عنصر از $۲\mathbb{Z}$ است و به وضوح عضو خنثی است. شرکتپذیری و وارونپذیری نیز واضح است.*

بررسی زیرگروه بودن با کمک تعریف بالا شاید خسته کننده باشد. قضیه زیر یک محک ساده در اختیار ما قرار می‌دهد.

قضیه ۵.۴.۲. *فرض کنیم G گروه باشد. در این صورت موارد زیر معادل هستند.*
(۱) زیرمجموعه ناتهی H از G زیرگروه است.
(۲) برای هر $a, b \in H$ داشته باشیم $ab \in H$ و $a^{-۱} \in H$.
(۳) برای هر $a, b \in H$ داشته باشیم $ab^{-۱} \in H$.

اثبات. (۱) $\Leftarrow$ (۲). فرض کنیم $a, b \in H$. چون H زیرگروه است پس $a^{-۱}$ در H قرار دارد. چون H زیرگروه است نسبت به عمل القایی بسته است و لذا $ab \in H$.
(۲) $\Leftarrow$ (۳). فرض کنیم $x, y \in H$. طبق فرض $y^{-۱}$ در H قرار دارد (در حقیقت $a = y$ فرض کرده ایم). دوباره طبق فرض باید $xy^{-۱}$ در H باشد (در حقیقت $a = x$ و $b = y^{-۱}$ فرض کرده‌ایم).
(۳) $\Leftarrow$ (۱). ابتدا دقت شود که H ناتهی است. فرض کنیم $x \in H$. طبق فرض $xx^{-۱} \in H$، در حقیقت فرض کرده‌ایم $a = b = x$. اما در گروه G داریم $xx^{-۱} = e$. لذا $e \in H$. حال برای هر $a \in H$ داریم $a = ae = ea$ و در نتیجه H عنصر خنثی e را دارد.
حال فرض کنیم $x \in H$. اکنون قرار می‌دهیم که $a = e$ و $b = x$. بنابراین بر طبق فرض $ab^{-۱} = ex^{-۱} = x^{-۱} \in H$. یعنی وارون هر عضو از H در خود H قرار دارد.
فرض کنیم $x, y \in H$. طبق قسمت بالا $y^{-۱} \in H$ و لذا طبق فرض باید $xy = x(y^{-۱})^{-۱} \in H$ باشد. در حقیقت فرض کرده‌ایم $a = x$ و $b = y^{-۱}$ (دقت شود که طبق تمرین ۵۶.۲.۲ داریم $(y^{-۱})^{-۱} = y$). پس H نسبت به عمل الحاقی بسته است.

چون H زیرمجموعه G است شرکتپذیری از G به H ارث می‌رسد و لذا طبق تعریف H زیرگروه است. $\square$

مثال ۶.۴.۲. *گروه $(\mathbb{R} \setminus \{\circ\}, .)$ را در نظر بگیرید. در این صورت $\mathbb{R}^+$، مجموعه اعداد حقیقی مثبت، یک زیرگروه است. فرض کنیم $a, b \in \mathbb{R}^+$. در این صورت $b^{-۱} = \frac{۱}{b}$ عضوی از $\mathbb{R}^+$ است و به وضوح $ab^{-۱} = \frac{a}{b} \in \mathbb{R}^+$. حال طبق قضیه ۲ .۴ .۵ باید $\mathbb{R}^+$ زیرگروه باشد.*

مثال ۷.۴.۲. *گروه $(\mathbb{R} \setminus \{\circ\}, .)$ را در نظر بگیرید. در این صورت $A = \{a \in \mathbb{R} \mid |a| \in \mathbb{N}\}$ یک زیرگروه نیست. واضح است که $۲ \in A$. اما $۲^{-۱} = \frac{۱}{۲}$ عضوی از A نیست. زیرا داریم $|۲^{-۱}| = \frac{۱}{۲} \notin A$. حال طبق قضیه ۲ .۴ .۵، A زیرگروه نیست. این در حالی است که اگر قرار دهیم $B = \{a \in \mathbb{R} \mid |a| \in \mathbb{Q}\}$ آنگاه B زیرگروه است.*

مثال ۸.۴.۲. *می‌خواهیم تمام زیرگروه‌های $(\mathbb{Z}, +)$ را شناسایی کنیم. ادعا می‌کنیم تمام زیرگروه‌های $\mathbb{Z}$ با عمل دوتایی جمع به صورت*

$$n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}$$

است که در آن $n \in \mathbb{Z}$. واضح است که $\circ \in n\mathbb{Z}$ و لذا $n\mathbb{Z}$ ناتهی است. حال فرض کنیم $nk, nk' \in \mathbb{Z}$. در گروه $\mathbb{Z}$ عنصر nk' دارای وارون $-nk'$ است و داریم

$$nk + (-nk') = nk - nk' = n(k - k') = nk''.$$

واضح است که $nk'' \in n\mathbb{Z}$. حال طبق قضیه ۲ .۴ .۵، $n\mathbb{Z}$ زیرگروه است. اکنون فرض کنیم H یک زیرگروه دلخواه از $\mathbb{Z}$ باشد. اگر $H = \{\circ\}$ باشد چیزی برای اثبات نداریم! فرض کنیم $H \neq \{\circ\}$. پس x ناصفری در H قرار دارد. H حتما شامل یک عنصر مثبت است. زیرا اگر x مثبت نبود آنگاه چون H عنصر خنثی $\circ$ را دارد (چرا؟)، پس طبق قضیه ۲ .۴ .۵، $\circ - x = -x$ که مثبت است در H قرار دارد. بنابراین فرض کنیم n کوچکترین عدد صحیح مثبت در H باشد (چرا چنین فرضی معتبر است؟). نشان می‌دهیم $H = n\mathbb{Z}$. چون $n \in H$ مشابه استدلال بالا داریم $-n \in H$ و لذا طبق قضیه ۲ .۴ .۵، $n - (-n) = n + n = ۲n$ در H قرار دارد. این روند را تکرار کنید! پس هر مضربی از n در H قرار دارد و این یعنی $n\mathbb{Z} \subseteq H$. حال فرض کنیم $t \in H$ دلخواه باشد. طبق قضیه الگوریتم تقسیم، قضیه ۱ .۲ .۷، $t = nq + r$ که $\circ \leq r < n$. طبق مطلبی که بالا نشان دادیم $nq \in H$. پس طبق قضیه ۲ .۴ .۵، $r = t - nq \in H$ و این کوچکترین بودن n را نقض می‌کند مگر این که $r = \circ$. پس $t \in n\mathbb{Z}$ و $H \subseteq n\mathbb{Z}$.

قضیه زیر برای گروه‌های متناهی و زیرگروه بودن یک زیرمجموعه آن محک ساده‌تری ارائه می‌کند.

قضیه ۹.۴.۲. *فرض کنیم G گروه متناهی باشد. زیرمجموعه ناتهی H از G زیرگروه است اگر و تنها اگر برای هر $a, b \in H$ داشته باشیم $ab \in H$.*

اثبات. $(\Leftarrow)$. فرض کنیم $a, b \in H$. چون H زیرگروه است نسبت به عمل القایی بسته است و لذا $ab \in H$.

$(\Rightarrow)$. ابتدا دقت شود که H ناتهی است. فرض کنیم $x, y \in H$. طبق فرض باید $xy \in H$ باشد.

پس H نسبت به عمل الحاقی بسته است. چون H زیرمجموعه G است شرکتپذیری از G به H ارث می‌رسد و لذا طبق تعریف H نیم‌گروه متناهی است. اگر $a,x,y \in H$ و $ax = ay$ آنگاه چون G گروه است داریم $a^{-1}ax = a^{-1}ay$ یعنی $x = y$. لذا حذف از چپ برقرار است. به صورت مشابه حذف از راست نیز برقرار است. حال طبق قضیه ۵۱.۲.۲ باید H با عمل الحاقی گروه باشد و این یعنی H زیرگروه G است. $\square$

تذکر ۱۰.۴.۲. *متناهی بودن در قضیه قبل شرط اساسی است. زیرا برای هر $a,b \in \mathbb{N}$ داریم $ab \in \mathbb{N}$. اما می‌دانیم که $\mathbb{N}$ با عمل دوتایی ضرب معمولی یک گروه نیست.*

مثال ۱۱.۴.۲. *گروه $(\mathbb{Z}_m,+)$ را در نظر بگیرید. فرض کنیم $k \in \mathbb{N}$. در این صورت*

$$k\mathbb{Z}_m = \{\bar{k}\bar{i} \mid \bar{i} \in \mathbb{Z}_m\}$$

یک زیرگروه است. فرض کنیم $\bar{x},\bar{y} \in k\mathbb{Z}_m$. پس $\bar{x} = \bar{k}\bar{i}$ و $\bar{y} = \bar{k}\bar{j}$. حال داریم

$$\bar{x}+\bar{y} = \bar{k}\bar{i}+\bar{k}\bar{j} = \bar{k}(\bar{i}+\bar{j}) = \bar{k}\overline{i+j}$$

و لذا طبق قضیه ۹.۴.۲ زیرگروه بودن حاصل می‌شود.

اکنون گزاره زیر را داریم.

گزاره ۱۲.۴.۲. *فرض کنیم G یک گروه و $\{H_i\}_{i\in I}$ خانواده‌ای از زیرگروه‌های G باشد. در این صورت $H = \bigcap_{i\in I} H_i$ یک زیرگروه است.*

اثبات. می‌دانیم که برای هر $i \in I$، عنصر خنثی e عضوی از H_i است (چرا؟). لذا $e \in \bigcap_{i\in I} H_i$ و در نتیجه $e \in H$ و H ناتهی است. حال فرض کنیم که $a,b \in H$. پس برای هر $i \in I$ داریم $a,b \in H_i$. چون برای هر $i \in I$، H_i زیرگروه است باید $b^{-1} \in H_i$ (چرا؟). لذا برای هر $i \in I$ طبق قضیه ۵.۴.۲ داریم $ab^{-1} \in H_i$. این یعنی $ab^{-1} \in H$ و طبق قضیه ۵.۴.۲ باید $H \leq G$. $\square$

تذکر ۱۳.۴.۲. *جالب است که اجتماع زیرگروه‌های لازم نیست که زیرگروه باشد. مثلا در گروه $(\mathbb{Z},+)$ زیرگروه‌های $۲\mathbb{Z}$ و $۳\mathbb{Z}$ را در نظر بگیرید. در این صورت $۲,۳ \in ۲\mathbb{Z} \cup ۳\mathbb{Z}$. اما داریم $۲+۳ = ۵ \notin ۲\mathbb{Z}\cup ۳\mathbb{Z}$.*

برای اجتماع زیرگروه‌های گزاره زیر را داریم.

گزاره ۱۴.۴.۲. *فرض کنیم G یک گروه و $H,K \leq G$. در این صورت $H \cup K$ زیرگروه است اگر و تنها اگر $H \subseteq K$ یا $K \subseteq H$.*

اثبات. $(\Leftarrow)$. به برهان خلف فرض کنیم $K \nsubseteq H$ و $H \nsubseteq K$. حال عناصر $h \in H \setminus K$ و $k \in K \setminus H$ را در نظر می‌گیریم. اما واضح است که $h \in H \cup K$ و $k \in H \cup K$. لذا $hk \in H \cup K$ (چرا؟). اکنون باید $hk \in H$ یا $hk \in K$. اگر $hk \in H$ باشد آنگاه چون H

زیرگروه است داریم $h^{-۱} \in H$ و لذا $h^{-۱}hk = k \in H$ و این تناقض است. اگر $hk \in K$ باشد آنگاه چون K زیرگروه است داریم $k^{-۱} \in K$ و لذا $hkk^{-۱} = h \in K$ و این نیز تناقض است.
$(\Rightarrow)$. طبق فرض $H \cup K = H$ یا $H \cup K = K$ و چیزی برای اثبات نداریم. $\square$

مثال ۱۵.۴.۲. *گروه چهارتایی کلاین $\mathbb{K}_۴$ را به یاد آورید! قرار می‌دهیم*

$$A = \{e, a\} \qquad B = \{e, b\} \qquad C = \{e, c\}$$

در این صورت A، B و C با یک بررسی ساده زیرگروه‌های سره از $\mathbb{K}_۴$ هستند و $\mathbb{K}_۴ = A \cup B \cup C$.

سوال ۱۶.۴.۲. *آیا می‌توانیم گزاره قبل را برای اجتماع سه زیرگروه یا تعداد دلخواه زیرگروه تعمیم دهیم؟*

سوال ۱۷.۴.۲. *به نظر شما گروهی که اجتماع دو زیرگروه سره خود است، چگونه است؟ گروهی که اجتماع سه زیرگروه سره خود است، چطور؟*

در ادامه می‌خواهیم دو زیرگروه بسیار مهم از یک گروه را برای شما معرفی کنیم. با تعریف زیر شروع می‌کنیم.

تعریف ۱۸.۴.۲. *فرض کنیم G یک گروه باشد. به مجموعه*

$$Z(G) = \{x \in G \mid xa = ax \qquad \forall a \in G\}$$

مرکز گروه G گوییم.

مثال ۱۹.۴.۲. *اگر G یک گروه آبلی باشد آنگاه بسیار واضح است که $Z(G) = G$.*

مثال ۲۰.۴.۲. *اگر $G = S_۳$ باشد آنگاه در بخش قبل دیده‌اید که $S_۳$ یک گروه غیر آبلی است و با توجه به این که عناصر $S_۳$ را می‌شناسیم می‌توان دید که اگر e عضو خنثی گروه $S_۳$ باشد آنگاه $Z(S_۳) = \{e\}$.*

مثال ۲۱.۴.۲. *اگر $G = \mathbb{Q}_۸$ باشد آنگاه در بخش قبل دیده‌اید که $\mathbb{Q}_۸$ یک گروه غیر آبلی است و با توجه به این که عناصر ان را می‌شناسیم می‌توان دید که $Z(\mathbb{Q}_۸) = \{۱, -۱\}$.*

گزاره ۲۲.۴.۲. *برای هر گروه G داریم $Z(G) \leq G$.*

اثبات. واضح است که $e \in Z(G)$ و لذا $Z(G)$ ناتهی است. حال فرض کنیم $x, y \in Z(G)$. لذا برای هر $a \in G$ داریم $xa = ax$ و $ay = ya$. بنابراین برای هر $a \in G$

$$a(xy) = (ax)y = (xa)y = xay = x(ay) = x(ya) = xya = (xy)a.$$

درنتیجه $xy \in Z(G)$. چون برای هر $a \in G$ داریم $xa = ax$ پس با ضرب طرفین از راست در $x^{-۱}$ داریم $xax^{-۱} = a$ و با ضرب طرفین تساوی آخر از سمت چپ در $x^{-۱}$ داریم $ax^{-۱} = x^{-۱}a$. لذا $x^{-۱} \in Z(G)$. حال طبق قضیه ۵.۴.۲ باید $Z(G) \leq G$. $\square$

تعریف ۲.۴.۲۳. فرض کنیم G یک گروه و A زیرمجموعه ناتهی از G باشد. به مجموعه

$$C_G(A) = \{x \in G \mid xa = ax \qquad \forall a \in A\}$$

مرکز ساز A در گروه G گوییم. اگر $A = \{a\}$ آنگاه به مجموعه

$$C_G(a) = \{x \in G \mid xa = ax\}$$

مرکز ساز عنصر a در گروه G گوییم. اگر بیم ابهام نباشد از نمادهای $C(A)$ و $C(a)$ نیز استفاده می‌کنیم.

مثال ۲.۴.۲۴. اگر G یک گروه با عنصر خنثی e باشد آنگاه بسیار واضح است که $C_G(e) = G$.

مثال ۲.۴.۲۵. اگر $G = S_3$ باشد و

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

آنگاه می‌خواهیم $C_{S_3}(\sigma) = C(\sigma)$ را به دست آوریم. فرض کنیم

$$\tau = \begin{pmatrix} 1 & 2 & 3 \\ a & b & c \end{pmatrix}$$

عنصری در $C(\sigma)$ باشد. پس داریم $\sigma\tau = \tau\sigma$. لذا

$$\tau\sigma = \begin{pmatrix} 1 & 2 & 3 \\ a & c & b \end{pmatrix}.$$

حال اگر a برابر ۲ یا ۳ باشد با یک بررسی ساده تساوی $\sigma\tau = \tau\sigma$ نقض می‌شود و لذا باید $a = 1$. اگر $b = 2$ باشد انگاه $c = 3$ است و لذا τ همان عنصر خنثی e از S_3 است. اگر $b = 3$ باشد آنگاه $c = 2$ است یعنی $\tau = \sigma$ و تساوی $\sigma\tau = \tau\sigma$ حفظ می‌شود. لذا $C(\sigma) = \{e, \sigma\}$.

گزاره ۲.۴.۲۶. برای هر گروه G و $\emptyset \neq A \subseteq G$ داریم $C_G(A) \leq G$.

اثبات. واضح است که $e \in C_G(A)$ و لذا $C_G(A)$ ناتهی است. حال فرض کنیم $x, y \in C_G(A)$. لذا برای هر $a \in A$ داریم $xa = ax$ و $ay = ya$. بنابراین برای هر $a \in A$ نتیجه می‌شود که

$$a(xy) = (ax)y = (xa)y = xay = x(ay) = x(ya) = xya = (xy)a.$$

درنتیجه $xy \in C_G(A)$. اما برای هر $a \in A$ داریم $xa = ax$، پس با ضرب طرفین از راست در x^{-1} نتیجه می‌شود که $xax^{-1} = a$ و با ضرب طرفین تساوی آخر از سمت چپ در x^{-1} داریم $ax^{-1} = x^{-1}a$. لذا $x^{-1} \in C_G(A)$. حال طبق قضیه ۲.۴.۵ باید $C_G(a) \leq G$. $\square$

تعریف ۲.۴.۲۷. فرض کنیم G یک گروه باشد و $H, K \leq G$. منظور از HK یعنی

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

مثال زیر نشان می‌دهد که لزومی ندارد HK زیرگروه باشد.

مثال ۲.۴.۲۸. *فرض کنیم $G = Gl_2(\mathbb{R})$ (عمل دوتایی ضرب عادی ماتریس است). دو زیرگروه G به صورت*

$$H = \{\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \mid x \in \mathbb{R}\} \qquad K = \{\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \ \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\}$$

را در نظر می‌گیریم. حال داریم

$$HK = \{\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}, \ \begin{pmatrix} x & 1 \\ 1 & 0 \end{pmatrix} \mid x \in \mathbb{R}\}.$$

اکنون

$$A = \{\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \qquad B = \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix}$$

اعضای HK هستند. اما BA عضوی از HK نیست. زیرا اعضای HK یک درایه صفر دارند اما BA اصلا درایه صفر ندارد. لذا HK زیرگروه G نیست!

حال گزاره زیر را داریم.

گزاره ۲.۴.۲۹. *فرض کنیم G یک گروه باشد و $H, K \leq G$. در این صورت HK زیرگروه است اگر و تنها اگر $HK = KH$.*

اثبات. $(\Leftarrow)$. نشان می‌دهیم $KH \subseteq HK$. فرض کنیم $x \in KH$. لذا $x = kh$ که $k \in K$ و $h \in H$. اکنون طبق تمرین ۲.۲.۵۵ داریم $x^{-1} = h^{-1}k^{-1}$ و در نتیجه $x^{-1} \in HK$. اما طبق فرض HK زیرگروه است پس $x \in HK$ و این یعنی $KH \subseteq HK$. اکنون فرض کنیم $x \in HK$. چون HK زیرگروه است پس $x^{-1} \in HK$. فرض کنیم $x^{-1} = hk$ که $h \in H$ و $k \in K$. طبق تمرین ۲.۲.۵۶ و تمرین ۲.۲.۵۵ داریم که $x = (x^{-1})^{-1} = k^{-1}h^{-1} \in KH$. بنابراین $HK \subseteq KH$.
$(\Rightarrow)$. چون H و K زیرگروه هستند دارای عنصر خنثی e هستند و در نتیجه $e = ee \in HK$ و لذا HK ناتهی است. فرض کنیم $x, y \in HK$. بنابراین $x = ab$ و $y = uv$ که $u, a \in H$ و $b, v \in K$. می‌خواهیم قضیه ۲.۴.۵ را به کار ببریم. طبق تمرین ۲.۲.۵۵ داریم $xy^{-1} = abv^{-1}u^{-1}$. اما $bv^{-1} \in K$ پس $bv^{-1}u^{-1} \in KH$. لذا از فرض $bv^{-1}u^{-1} \in HK$. پس فرض کنیم $bv^{-1}u^{-1} = hk$ که $h \in H$ و $k \in K$. حال داریم

$$xy^{-1} = abv^{-1}u^{-1} = ahk = (ah)k = h'k \in HK.$$

اکنون طبق قضیه ۲.۴.۵ داریم $HK \leq G$. □

سوال ۳۰.۴.۲. *اگر H و K زیرگروه‌های گروه G باشند آنگاه می‌توان از $hk \in HK$ نتیجه گرفت که $h \in H$ و $k \in K$؟*

این بخش را با قضیه کاربردی و مهم زیر به پایان می‌رسانیم.

قضیه ۳۱.۴.۲. *فرض کنیم G گروه متناهی باشد و $H, K \leq G$. در این صورت همواره داریم $|HK| = \frac{|H|\,|K|}{|H \cap K|}$. این قضیه برای زیرگروه‌های متناهی از یک گروه نه لزوما متناهی نیز صادق است.*

اثبات. قرار می‌دهیم

$$f : H \times K \longrightarrow HK, \quad f((h,k)) = hk.$$

f یک تابع است (بررسی کنید). اگر $x \in HK$ انگاه $x = hk$ که $h \in H$ و $k \in K$. در نتیجه $f((h,k)) = hk = x$. یعنی f یک تابع پوشا است. حال طبق قضیه ۲۲.۱.۱ داریم که $f^{-1}(x)$ها که $x \in HK$ یک افراز است. لذا $H \times K = \bigcup_{x \in HK} f^{-1}(x)$. اکنون برای هر $x \in HK$ ادعا می‌کنیم $|f^{-1}(x)| = |H \cap K|$. فرض کنیم $x = hk \in HK$. اگر $y \in H \cap K$ آنگاه

$$f((hy, y^{-1}k)) = hyy^{-1}k = hk = x.$$

لذا $(hy, y^{-1}k) \in f^{-1}(x)$. در نتیجه

$$T = \{(hy, y^{-1}k) \mid y \in H \cap K\} \subseteq f^{-1}(x).$$

اکنون فرض کنیم $(a,b) \in f^{-1}(x)$. پس

$$ab = f((a,b)) = x = hk = f((h,k)).$$

لذا با ضرب‌های مناسب از سمت چپ و راست داریم $h^{-1}a = kb^{-1}$. واضح است که $h^{-1}a \in H$ و $kb^{-1} \in K$. پس باید $h^{-1}a = kb^{-1} = y \in H \cap K$. بنابراین از $h^{-1}a = y$ نتیجه می‌شود $a = hy$ و از $kb^{-1} = y$ نتیجه می‌شود $b = y^{-1}k$. یعنی $(a,b) = (hy, y^{-1}k)$ و لذا $f^{-1}(x) \subseteq T$. بنابراین $f^{-1}(x) = T$. اما واضح است که $|T| = |H \cap K|$. پس ادعا اثبات می‌شود. حال چون H و K متناهی هستند، داریم $|H \times K| = |H|\,|K|$. بنابراین طبق قضیه ۱۴.۱.۱ داریم

$$|H|\,|K| = |H \times K| = \sum_{x \in HK} |f^{-1}(x)| =$$

$$\sum_{x \in HK} |H \cap K| = |HK|\,|H \cap K|$$

و اثبات کامل است. $\square$

مثال ۳۲.۴.۲. *فرض کنیم G یک گروه متناهی باشد و $n = |G|$. اگر H و K دو زیرگروه G باشند که تعداد اعضای آنها از $\sqrt{n}$ بیشتر باشد آنگاه حتما H و K اشتراک غیر بدیهی دارند یعنی $H \cap K \neq \{e\}$. زیرا طبق قضیه ۳۱.۴.۲ داریم*

$$n \geq |HK| = \frac{|H|\,|K|}{|H \cap K|} > \frac{n}{|H \cap K|}$$

و لذا باید $H \cap K \neq \{e\}$.

تمرین‌های حل شده

تمرین ۳۳.۴.۲. *زیرگروه‌های $(\mathbb{Z}_6, +)$ را بنویسید.*

حل. واضح است که $\{\bar{0}\}$ و $\mathbb{Z}_6$ دو زیرگروه بدیهی هستند. دو مجموعه

$$2\bar{Z}_6 = \{\bar{0}, \bar{2}, \bar{4}\} \qquad 3\bar{Z}_6 = \{\bar{0}, \bar{3}\}$$

نیز با یک برسی ساده زیرگروه هستند. حال فرض کنیم H زیرگروه متمایز از زیرگروه‌های باشد که شناسایی کرده‌ایم. پس H باید شامل $\bar{1}$ یا $\bar{5}$ باشد. اگر شامل $1\,bar$ باشد آنگاه H برابر $\mathbb{Z}_6$ است. زیرا H زیرگروه است پس $\bar{2} = \bar{1} + \bar{1}$ در H قرار دارد. همینطور $\bar{3} = \bar{1} + \bar{2}$ در H قرار دارد. با ادامه این روند H باید خود گروه باشد و این تناقض است. اگر H شامل $\bar{5}$ باشد آنگاه $\bar{4} = \bar{5} + \bar{5}$ عضو H است. همینطور $\bar{3} = \bar{4} + \bar{5}$ در H قرار دارد. با تکرار این روند باید H خود گروه باشد که باز تناقض است. پس تمام زیرگروه‌ها شناسایی شد!

تمرین ۳۴.۴.۲. *فرض کنیم G یک گروه متناهی باشد و H زیرمجموعه ناتهی باشد. اگر $HH = H$ آنگاه نشان دهید که $H \leq G$.*

حل. فرض کنیم $a, b \in H$. واضح است که $ab \in HH$ و لذا طبق فرض $ab \in H$. حال طبق قضیه ۹.۴.۲ باید $H \leq G$.

تمرین ۳۵.۴.۲. *فرض کنیم G یک گروه باشد و $H \leq G$. نشان دهید که برای $x \in G$،*

$$T = xHx^{-1} = \{xhx^{-1} \mid h \in H\}$$

زیرگروه G است و $|xHx^{-1}| = |H|$.

حل. فرض کنیم $a, b \in T$. پس $a = xhx^{-1}$ و $b = xh'x^{-1}$ که $h, h' \in H$. طبق تمرین ۵۵.۲.۲ و تمرین ۵۶.۲.۲ داریم که $b^{-1} = (x^{-1})^{-1}h'^{-1}x^{-1} = xh'^{-1}x^{-1}$. پس

$$ab^{-1} = xhx^{-1}xh'^{-1}x^{-1} = xhh'^{-1}x^{-1} = xh''x^{-1} \in T$$

و لذا طبق قضیه ۵.۴.۲ زیرگروه بودن T حاصل می‌شود. برای قسمت دوم، تعریف می‌کنیم

$$f: H \longrightarrow T, \quad f(h) = xhx^{-1}.$$

بررسی کنید که f یک تابع خوشتعریف است. اگر $x = xhx^{-1} \in T$ آنگاه $f(h) = x$ و این یعنی f پوشا است. اگر $f(h) = f(h')$ آنگاه $xhx^{-1} = xh'x^{-1}$. با ضرب طرفین تساوی آخر از سمت چپ در x^{-1} و از سمت راست در x به دست می‌آید که $h = h'$. یعنی f یک‌به‌یک است. لذا $|H| = |xHx^{-1}|$.

تمرین ۳۶.۴.۲. *فرض کنیم H زیرگروهی از گروه G باشد. نشان دهید که برای $a \in G$، $Ha = H$ اگر و تنها اگر $a \in H$.*

حل. فرض کنیم $Ha = H$. چون H زیرگروه است دارای عنصر خنثی e است. لذا طبق فرض $ea \in H$ و درنتیجه $a \in H$.
اکنون فرض کنیم $a \in H$. اگر $h \in H$ آنگاه چون H زیرگروه است داریم $ha \in H$. بنابراین به وضوح $Ha \subseteq H$. اما a^{-1} و ha^{-1} عضو H هستند، به این دلیل که H زیرگروه است. پس برای هر $h \in H$ داریم $h = he = ha^{-1}a = (ha^{-1})a \in Ha$. لذا $H \subseteq Ha$ و اثبات کامل است.

تمرین ۳۷.۴.۲. *برای گروه G نشان دهید که $Z(G) = \bigcap_{a\in G} C_G(a)$.*

حل. فرض کنیم $x \in \bigcap_{a\in G} C_G(a)$. پس برای هر $a \in G$ داریم $x \in C_G(a)$. پس برای هر $a \in G$ داریم $xa = ax$. لذا $x \in Z(G)$ و در نتیجه $\bigcap_{a\in G} C_G(a) \subseteq Z(G)$.
فرض کنیم $x \in Z(G)$. پس برای هر $a \in G$ داریم $xa = ax$. چون x با a جابجا می‌شود داریم $x \in C_G(a)$ و در نتیجه $Z(G) \subseteq \bigcap_{a\in G} C_G(a)$ و اثبات کامل است.

تمرین ۳۸.۴.۲. *مرکز گروه S_n را به دست آورید.*

حل. طبق تمرین ۶۳.۲.۲، اگر $n \leq ۲$ باشد آنگاه S_n آبلی است و لذا $Z(S_n) = S_n$. فرض کنیم $n \geq ۳$ و $e \neq \sigma \in S_n$. چون σ عنصر خنثی نیست، پس عناصر متمایز i و j در $\{۱, ۲, ..., n\}$ چنان وجود دارند که $\sigma(i) = j$. حال چون $n \geq ۳$ است می‌توانیم $l \neq j$ را در $\{۱, ۲, ..., n\}$ و عنصر $\tau \in S_n$ را چنان انتخاب کنیم که $\tau(j) = l$ و $\tau(i) = i$. اکنون داریم

$$l = \tau(j) = \tau(\sigma(i)) = \tau\sigma(i) = \sigma\tau(i) = \sigma(\tau(i)) = \sigma(i) = j$$

که تناقض آشکار است. پس σ عنصر خنثی است و $Z(S_n) = \{e\}$.

تمرین ۳۹.۴.۲. *فرض کنیم G یک گروه ۱۲ عضوی باشد و $H, K \leq G$. اگر $H \cap K = \{e\}$، $|H| = ۲$ و $|K| = ۶$ باشد آنگاه نشان دهید که $G = HK$.*

حل. طبق قضیه ۳۱.۴.۲ داریم

$$|HK| = \frac{|H|\,|K|}{|H \cap K|} = ۱۲$$

و چون $HK \subseteq G$، لذا باید $G = HK$.

تمرین ۴۰.۴.۲. *فرض کنیم G یک گروه آبلی باشد و $H, K \leq G$. اگر $HK = H \cup K$ آنگاه نشان دهید که $K \subseteq H$ یا $H \subseteq K$.*

حل. فرض کنیم $hk \in HK$. چون G آبلی است پس باید $hk = kh$ باشد. لذا $HK \subseteq KH$ و $KH \subseteq HK$. یعنی $HK = KH$ و طبق گزاره ۲۹.۴.۲ باید HK زیرگروه باشد. چون $HK = H \cup K$ است پس طبق گزاره ۱۴.۴.۲ باید $H \subseteq K$ یا $K \subseteq H$.

تمرین ۴۱.۴.۲. *فرض کنیم G یک گروه، H و K زیرگروه‌های متناهی از G باشند. نشان دهید که $H \cap K = \{e\}$ اگر و تنها اگر $|HK| = |H|\,|K|$.*

حل. فرض کنیم $H \cap K = \{e\}$. بنابراین $|H \cap K| = ۱$ و لذا طبق قضیه ۳۱.۴.۲ داریم $|HK| = |H|\,|K|$.
برای برعکس، به برهان خلف، فرض کنیم $H \cap K \neq \{e\}$. لذا $|H \cap K| > ۱$. در نتیجه طبق قضیه ۳۱.۴.۲ داریم
$$|H|\,|K| = |HK| = \frac{|H|\,|K|}{|H \cap K|}$$
و این تناقض آشکار است.

۵.۲ مولد یک گروه و گروه‌های دوری

در این بخش می‌خواهیم ببینیم که آیا می‌شود با داشتن تعداد منتخبی از عناصر یک گروه، تمام گروه را تولید کرد. اگر چنین اتفاقی رخ دهد مطالعه گروه کمی ساده می‌شود.

تعریف ۱.۵.۲. *فرض کنیم G یک گروه باشد و X یک زیرمجموعه از G باشد. در این صورت اشتراک همه زیرگروه‌های G که شامل X هستند را با $< X >$ نمایش می‌دهیم، یعنی*

$$< X >= \bigcap_{X\subseteq H\leq G} H.$$

دو نکته مهم را باید مد نظر قرار دهیم. اول اینکه اشتراک بالا بامعنی است. زیرا دست کم خود G شامل X است. دوم اینکه طبق گزاره ۲.۴.۱۲، $< X >$ یک زیرگروه از G است. از این رو به $< X >$ زیرگروه تولید شده توسط X گوییم. اگر $X = \emptyset$ آنگاه قرار می‌دهیم $< X >= \{e\}$.

مثال ۲.۵.۲. گروه $G = (\mathbb{Z}, +)$ را در نظر بگیرید. فرض کنیم $X = \{۲\}$. با توجه به مثال ۲.۴.۸ می‌دانیم تمام زیرگروه‌های G به صورت $n\mathbb{Z}$ است. لذا تنها زیرگروه G که شامل X باشد به صورت $۲\mathbb{Z}$ است. پس $< X >= ۲\mathbb{Z}$.

مثال ۳.۵.۲. گروه $G = (\mathbb{Z}, +)$ را در نظر بگیرید. فرض کنیم $X = \{۲, ۴\}$. با توجه به مثال ۲.۴.۸ می‌دانیم تمام زیرگروه‌های G به صورت $n\mathbb{Z}$ است. لذا زیرگروه‌های G که شامل X باشد به صورت $۲\mathbb{Z}$ یا $۴\mathbb{Z}$ است. پس $< X >= ۴\mathbb{Z}$.

مثال‌های بالا این تصور را به وجود می‌آورد که شناسایی $< X >$ کار ساده‌ای نیست و باید تسلط روی تمام زیرگروه‌های یک گروه داشت. اما این تصور اشتباه است! در ادامه نتایجی را خواهیم آورد که شناسایی $< X >$ آسانتر شود.

لم ۴.۵.۲. *فرض کنیم G یک گروه باشد و $X \subseteq G$. در این صورت $< X >$ (نسبت به رابطه $\subseteq$) کوچکترین زیرگروه G است که شامل X است.*

اثبات. فرض کنیم K زیرگروهی از G باشد که $X \subseteq K$. پس K حتما در اشتراک $\bigcap_{X\subseteq H\leq G} H$ ظاهر شده است. لذا $< X >\subseteq K$ و این یعنی $< X >$ کوچکترین زیرگروه G است که شامل X است. $\square$

قضیه زیر برای محاسبه $< x >$ کمک کننده است.

قضیه ۵.۵.۲. *اگر G یک گروه باشد و $\emptyset \neq X \subseteq G$ آنگاه*

$$< X >= \{x_۱^{\epsilon_۱} x_۲^{\epsilon_۲} \ldots x_n^{\epsilon_n} \mid x_i \in X, \ \epsilon_i \in \{-۱, ۱\}, \ n \in \mathbb{N}\}.$$

اثبات. برای راحتی فرض کنیم

$$T = \{x_۱^{\epsilon_۱} x_۲^{\epsilon_۲} ... x_n^{\epsilon_n} \mid x_i \in X, \ \ \epsilon_i \in \{-۱, ۱\}, \ \ n \in \mathbb{N}\}.$$

باید نشان دهیم $T = < X >$. نشان می‌دهیم که $T \leq G$. واضح است که $X \subseteq T$. زیرا قرار می‌دهیم $n = ۱$ و $\epsilon_۱ = ۱$. لذا T ناتهی است. حال فرض کنیم $a, b \in T$. پس

$$a = x_۱^{\epsilon_۱} x_۲^{\epsilon_۲} ... x_n^{\epsilon_n} \qquad b = y_۱^{\epsilon'_۱} y_۲^{\epsilon'_۲} ... y_n^{\epsilon'_m}$$

حال واضح است که طبق تمرین ۵۵.۲.۲ داریم

$$b^{-۱} = y_m^{-\epsilon'_m} ... y_۲^{-\epsilon'_۲} y_۱^{-\epsilon'_m}.$$

چون $-\epsilon_j \in \{-۱, ۱\}$ لذا

$$ab^{-۱} = x_۱^{\epsilon_۱} x_۲^{\epsilon_۲} ... x_n^{\epsilon_n} y_m^{-\epsilon'_m} ... y_۲^{-\epsilon'_۲} y_۱^{-\epsilon'_m}$$

نیز به شکل اعضای T است یعنی $ab^{-۱} \in T$. بنابراین طبق قضیه ۵.۴.۲، T یک زیرگروه شامل X است. لذا طبق لم ۴.۵.۲ باید $< X > \subseteq T$.
حال فرض کنیم

$$a = x_۱^{\epsilon_۱} x_۲^{\epsilon_۲} ... x_n^{\epsilon_n} \in T.$$

چون $X \subseteq < X >$ پس برای هر j که $\epsilon_j = ۱$ باشد، داریم $x_j^{\epsilon_j} \in X \subseteq < X >$. اگر $\epsilon_j = -۱$ آنگاه $x_j^{-\epsilon_j} \in X \subseteq < X >$. چون $< X >$ زیرگروه است پس $x_j^{\epsilon_j} \in < X >$. دوباره چون $< X >$ زیرگروه است پس نسبت به عمل دوتایی بسته است لذا $a \in < X >$ و $T \subseteq < X >$. اثبات کامل است. $\square$

مثال ۶.۵.۲. *گروه $G = (\mathbb{Z}, +)$ را در نظر بگیرید. فرض کنیم $X = \{۱\}$. حال طبق قضیه ۵.۵.۲ و این مطلب که گروه جمعی است، داریم*

$$< X > = \{\epsilon_۱ x_۱ + \epsilon_۲ x_۲ + ... + \epsilon_n x_n \mid x_i \in X, \ \ \epsilon_i \in \{-۱, ۱\}, \ \ n \in \mathbb{N}\} = \{\underbrace{\pm ۱ \pm ۱ \pm ... \pm ۱}_{n \text{تا}} \mid n \in \mathbb{N}\} = \{m \mid m \in \mathbb{Z}\} = \mathbb{Z}.$$

مثال ۷.۵.۲. *گروه $G = (\mathbb{Z}, +)$ را در نظر بگیرید. فرض کنیم $X = \{۲\}$. حال طبق قضیه ۵.۵.۲ و این مطلب که گروه جمعی است، داریم*

$$< X > = \{\epsilon_۱ x_۱ + \epsilon_۲ x_۲ + ... + \epsilon_n x_n \mid x_i \in X, \ \ \epsilon_i \in \{-۱, ۱\}, \ \ n \in \mathbb{N}\} = \{\underbrace{\pm ۲ \pm ۲ \pm ... \pm ۲}_{n \text{تا}} \mid n \in \mathbb{N}\} = \{۲m \mid m \in \mathbb{Z}\} = ۲\mathbb{Z}.$$

مثال ۸.۵.۲. گروه $G=(GL_2(\mathbb{R}),.)$ را در نظر بگیرید. فرض کنیم $X=\{\begin{pmatrix} 2 & 0\\ 0 & 1\end{pmatrix}\}$. حال طبق قضیه ۵.۵.۲ و این مطلب که گروه ضربی است، داریم

$$< X >= \{x_1^{\epsilon_1}x_2^{\epsilon_2}...x_n^{\epsilon_n} \ \mid \ x_i\in X,\ \ \epsilon_i\in\{-1,1\},\ \ n\in\mathbb{N}\} =$$
$$\{\underbrace{\begin{pmatrix} 2 & 0\\ 0 & 1\end{pmatrix}^{\pm 1}\begin{pmatrix} 2 & 0\\ 0 & 1\end{pmatrix}^{\pm 1}...\begin{pmatrix} 2 & 0\\ 0 & 1\end{pmatrix}^{\pm 1}}_{\text{تا}\ n} \ \mid \ n\in\mathbb{N}\} =$$
$$\{\begin{pmatrix} 2 & 0\\ 0 & 1\end{pmatrix}^{m} \ \mid \ m\in\mathbb{Z}\} = \{\begin{pmatrix} 2^m & 0\\ 0 & 1\end{pmatrix} \ \mid \ m\in\mathbb{Z}\}.$$

نمادگذاری ۹.۵.۲. اگر $X=\{x_1,...,x_n\}$ باشد آنگاه $< X >$ را با $< x_1,...,x_n >$ نمایش می‌دهیم.

حال نتیجه زیر را داریم.

نتیجه ۱۰.۵.۲. فرض کنیم G یک گروه باشد و $\emptyset\neq X\subseteq G$.

(۱) اگر G یک گروه آبلی باشد آنگاه

$$< X >= \{x_1^{k_1}x_2^{k_2}...x_n^{k_n} \ \mid \ x_i\in X,\ \ x_i\neq x_j,\ \ k_i\in\mathbb{Z},\ \ n\in\mathbb{N}\}.$$

(۲) اگر $X=\{x_1,x_2,...,x_n\}$ و G آبلی باشد آنگاه برای گروه ضربی داریم

$$< x_1,x_2,...,x_n >= \{x_1^{k_1}x_2^{k_2}...x_n^{k_n} \ \mid \ k\in\mathbb{Z}\}$$

و برای گروه جمعی داریم

$$< x_1,x_2,...,x_n >= \{k_1x_1+k_2x_2+...+k_nx_n \ \mid \ k\in\mathbb{Z}\}.$$

(۳) اگر $X=\{x\}$ و G آبلی باشد آنگاه برای گروه ضربی داریم

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

و برای گروه جمعی داریم

$$< x >= \{kx \ \mid \ k\in\mathbb{Z}\}.$$

اثبات. (۱) چون گروه آبلی است آنقدر اعضا را جابجا می‌کنیم تا مشابه‌ها کنار هم قرار بگیرند و دیگر مشابه‌ای در مکان دیگری نباشد. حال طبق قضیه ۴۴.۲.۲ توان‌ها جمع می‌شوند و عددی صحیح خواهند بود.

(۲) نتیجه مستقیم (۱) است.

(۳) نتیجه مستقیم (۲) است. □

اکنون مثال‌های زیر را دنبال کنید.

مثال ۱۱.۵.۲. گروه $G=(\mathbb{Z},+)$ را در نظر بگیرید. فرض کنیم $X=\{۲,۳\}$. واضح است که G آبلی طبق نتیجه ۱۰.۵.۲ داریم

$$<۲,۳>=\{۲k+۳k' \mid k,k'\in\mathbb{Z}\}=\mathbb{Z}.$$

مثال ۱۲.۵.۲. گروه $G=(\mathbb{Z},+)$ را در نظر بگیرید. فرض کنیم $X=\{۲,۴,۶\}$. واضح است که G آبلی طبق نتیجه ۱۰.۵.۲ داریم

$$<۲,۴,۶>=\{۲k+۴k'+۶k'' \mid k,k',k''\in\mathbb{Z}\}=$$
$$\{۲(k+۲k'+۳k'') \mid k,k',k''\in\mathbb{Z}\}=۲\mathbb{Z}.$$

مثال ۱۳.۵.۲. گروه $G=\mathbb{Q}_۸$ را در نظر بگیرید. فرض کنیم $X=\{i\}$. این گروه غیر آبلی است و چون $i^۲=i^{-۲}=-۱$ پس $i^۴=i^{-۴}=۱$ و $i^۳=i^{-۳}=-i$. بنابراین

$$<X>=\{x^k \mid k\in\mathbb{Z}\}=\{i^k \mid k\in\mathbb{Z}\}=\{۱,-۱,i,-i\}.$$

گزاره ۱۴.۵.۲. برای هر گروه G و $x\in G$ همواره $<x>$ آبلی است.

اثبات. فرض کنیم $a,b\in<x>$. پس طبق نتیجه ۱۰.۵.۲ اعداد صحیح k و k' وجود دارند که $a=x^k$ و $b=x^{k'}$. لذا داریم

$$ab=x^kx^{k'}=x^{k+k'}=x^{k'+k}=x^{k'}x^k=ba$$

و اثبات تمام است. □

تعریف ۱۵.۵.۲. فرض کنیم G یک گروه باشد و $X\subseteq G$. گوییم X مجموعه مولد برای G هرگاه $G=<X>$. همچنین

(الف) اگر $|X|=۱$ باشد آنگاه به $<x>$ زیرگروه دوری گوییم.

(ب) اگر $|X|<\infty$ باشد آنگاه به $<X>$ زیرگروه متناهیا تولید شده گوییم.

(ج) اگر $|X|=۱$ باشد و $G=<x>$ آنگاه به G گروه دوری گوییم.

(د) اگر $|X|<\infty$ باشد و $G=<X>$ آنگاه به G گروه متناهیا تولید شده گوییم.

مثال ۱۶.۵.۲. گروه $(\mathbb{Z},+)$ دوری است. زیرا $\mathbb{Z}=<۱>$.

مثال ۱۷.۵.۲. گروه $(\mathbb{Z}_۴,+)$ دوری است. زیرا $\mathbb{Z}_۴=<\bar{۱}>$.

مثال ۱۸.۵.۲. *گروه جمعی $G = \mathbb{Z}\times\mathbb{Z}$ دوری نیست. به برهان خلف، فرض کنیم که داشته باشیم $G =< (a,b) >$. پس طبق نتیجه ۱۰.۵.۲ داریم*

$$< (a,b) >= \{k(a,b) \mid k \in \mathbb{Z}\} = \{(ka,kb) \mid k \in \mathbb{Z}\}.$$

اما واضح است که $(۱,۰) \in G$. پس عدد صحیح k چنان وجود دارد که $(ka,kb) = (۱,۰)$. پس $kb = ۰$ و لذا باید $b = ۰$. اما واضح است که $(۰,۱) \in G$. پس عدد صحیح k چنان وجود دارد که $(ka,kb) = (۰,۱)$. پس $ka = ۰$ و لذا باید $a = ۰$. بنابراین $\mathbb{Z}\times\mathbb{Z} =< (۰,۰) >$ این تناقض آشکار است.

مثال ۱۹.۵.۲. *گروه جمعی $G = \mathbb{Z}\times\mathbb{Z}$ متناهیا تولید شده است. زیرا این گروه آبلی است و طبق نتیجه ۱۰.۵.۲ داریم*

$$< (۱,۰),(۰,۱) >= \{k_۱(۱,۰) + k_۲(۰,۱) \mid k_۱,k_۲ \in \mathbb{Z}\} =$$
$$\{(k_۱,۰) + (۰,k_۲) \mid k_i \in \mathbb{Z}\} = \{(k_۱,k_۲) \mid k_۱,k_۲ \in \mathbb{Z}\} = \mathbb{Z}\times\mathbb{Z}.$$

مثال ۲۰.۵.۲. *گروه آبلی جمعی $G = \mathbb{Q}$ متناهیا تولید شده نیست. به برهان خلف فرض کنیم که $G =< \frac{m_۱}{n_۱},\dots,\frac{m_t}{n_t} >$. چون اعداد اول نامتناهی هستند، می‌توانیم عدد اول p را چنان انتخاب کنیم که $p \nmid n_i$. اما $\frac{۱}{p} \in G$ و لذا طبق نتیجه ۱۰.۵.۲ داریم $\frac{۱}{p} = k_۱\frac{m_۱}{n_۱} + \dots + k_t\frac{m_t}{n_t}$ که $k_i \in \mathbb{Z}$.*

$$\frac{۱}{p} = k_۱\frac{m_۱}{n_۱} + \dots + k_t\frac{m_t}{n_t} = \frac{k_۱m_۱n_۲\dots n_t + \dots + k_tm_tn_۱\dots n_{t-۱}}{n_۱\dots n_t} =$$
$$\frac{s}{n_۱\dots n_t}$$

لذا $n_۱\dots n_t = ps$ و اندیس i چنان وجود دارد که $p|n_i$ و این تناقض است.

تذکر ۲۱.۵.۲. *واضح است که برای هر گروه G داریم $G =< G >$. لذا هر گروه مجموعه مولد دارد، دست کم خودش!*

حال این بخش را با قضیه مهم زیر را پایان می‌بریم.

قضیه ۲۲.۵.۲. *هر زیرگروه از یک گروه دوری G، دوری است.*

اثبات. فرض کنیم $G =< x >$ که $x \in G$ و $H \le G$. اگر H زیرگروه بدیهی باشد انگاه چیزی برای اثبات نداریم. فرض کنیم H زیرگروه سره باشد. چون H زیرگروه است پس ناتهی است. از طرفی $H \subseteq G$ پس طبق نتیجه ۱۰.۵.۲، H دارای عضوی به شکل x^i است که $i \in \mathbb{Z}$. چون H زیرگروه است پس x^{-i} هم در H قرار دارد. در نتیجه می‌توانیم فرض کنیم کوچکترین عدد صحیح مثبت k وجود دارد که $x^k \in H$ (چگونه؟). ادعا می‌کنیم $H =< x^k >$. طبق لم ۴.۵.۲ واضح است که $< x^k >\subseteq H$. فرض کنیم $y \in H$. لذا $y = x^j$ چرا که $H \subseteq G$. طبق الگوریتم تقسیم، قضیه ۷.۲.۱، داریم $j = kq + r$ که $۰ \le r < k$. اما داریم

$$x^r = x^{j-kq} = x^jx^{-kq} = x^j(x^q)^{-k}.$$

سمت راست تساوی بالا در H قرار دارد (چرا؟). در نتیجه $x^r \in H$. این تناقض با انتخاب ما از k دارد و لذا باید $r = ۰$. بنابراین $y = x^j = x^{kq} = (x^k)^q \in < x >$ و $H \subseteq < x^k >$. اثبات کامل است. $\square$

شاید برای شما این سوال ایجاد شود که آیا زیرگروه یک گروه متناهیا تولید شده، متناهیا تولید شده است؟ در پاسخ به این سوال باید همین قدر اشاره کنیم که خیر اینگونه نیست! ساختن چنین مثالی نیاز به داشتن اطلاعاتی بیشتر در مورد گروه‌ها دارد! خواننده علاقمند می‌تواند با دیدن گروه‌های آزاد در مراجع انتهای جزوه یا اینترنت به راحتی چنین مثالی را ارائه کند. هر چند در بخش تمرینات حل شده این بخش با پذیرفتن یک مطلب از نظریه گروه مثالی را ارائه کرده‌ایم.

تمرین‌های حل شده

تمرین ۲۳.۵.۲. *نشان دهید که زیرگروه‌های متناهیا تولید شده $\mathbb{Q}$ دوری هستند.*

حل. فرض کنیم $H =< \frac{n_۱}{m_۱}, \dots, \frac{n_t}{m_t} >$ زیرگروه $\mathbb{Q}$ باشد. قرار می‌دهیم که $x = m_۱ m_۲ \dots m_t$. ادعا می‌کنیم که $H \leq < \frac{۱}{x} >$. داریم

$$\frac{n_i}{m_i} = n_i m_۱ m_۲ \dots m_{i-۱} m_{i+۱} \dots m_t \, \frac{۱}{x}.$$

پس هر مولد H در $< \frac{۱}{x} >$ قرار دارد پس $H \leq < \frac{۱}{x} >$. اما طبق قضیه ۲۲.۵.۲ باید H دوری باشد.

تمرین ۲۴.۵.۲. *برای دو عدد صحیح k و m نشان دهید که گروه $G = m\mathbb{Z} + k\mathbb{Z}$ با m و $k + ۷m$ تولید می‌شود.*

حل. واضح است که $m \in m\mathbb{Z} \subseteq m\mathbb{Z} + k\mathbb{Z}$. همچنین $۷m + k \in m\mathbb{Z} + k\mathbb{Z}$. لذا $< m, k + ۷m > \subseteq G$. فرض کنیم $ma + kb \in G$. داریم

$$ma + kb = (a - ۷b)m + b(k + ۷m).$$

لذا $ma + kb \in < m, k + ۷m >$. بنابراین $G =< m, k + ۷m >$.

تمرین ۲۵.۵.۲. *فرض کنیم G گروهی باشد که اصلا زیرگروه سره نابدیهی ندارد. نشان دهید که G دوری است. یک مثال از چنین گروهی را ارائه نمایید.*

حل. اگر $G = \{e\}$ چیزی برای اثبات نداریم. فرض کنیم $G \neq \{e\}$ و $x \in G$ یک عنصر مخالف عنصر خنثی باشد. حال واضح است که $< x >$ زیرگروه G است و $< x > \neq \{e\}$. طبق فرض باید $G =< x >$. برای قسمت دوم، کافی است گروه $G = (\mathbb{Z}_۲, +)$ در نظر بگیریم (حتی برای هر عدد اول p، $G = (\mathbb{Z}_p, +)$).

تمرین ۲۶.۵.۲. *فرض کنیم H زیرگروهی از گروه G باشد که توسط دو عنصر x و y تولید شده است. نشان دهید که اگر $xy = yx$ آنگاه H آبلی است.*

حل. طبق فرض داریم که $H =< x, y >$. فرض کنیم $a, b \in H$. طبق قضیه ۵.۵.۲ داریم

$$a = x^{\epsilon_1} y^{\epsilon_2} ... x^{\epsilon_{n-1}} y^{\epsilon_n} \qquad (\epsilon_i \in \{-1, 1\}, \ \ n \in \mathbb{N})$$
$$b = x^{\epsilon'_1} y^{\epsilon'_2} ... x^{\epsilon'_{n-1}} y^{\epsilon'_n} \qquad (\epsilon'_i \in \{-1, 1\}, \ \ n \in \mathbb{N})$$

چون $xy = yx$ پس با تعدادی جابجایی مناسب داریم

$$a = x^s y^l \qquad b = x^{s'} y^{l'} \qquad (s, l, s', l' \in \mathbb{Z})$$

لذا دوباره با کمک $xy = yx$ و تعداد جابجایی مناسب داریم

$$ab = x^s y^l x^{s'} y^{l'} = x^s x^{s'} y^l y^{l'} = x^{s+s'} y^{l+l'} = x^{s'} x^s y^{l'} y^l = x^{s'} y^{l'} x^s y^l = ba.$$

تمرین ۲۷.۵.۲. *برای زیرگروه سره H از گروه G نشان دهید که $G =< G \setminus H >$.*

حل. واضح است که $G = H \cup < G \setminus H >$. بنابراین طبق گزاره ۱۴.۴.۲ داریم که $H \subseteq < G \setminus H >$ یا $< G \setminus H > \subseteq H$. اگر $< G \setminus H > \subseteq H$ آنگاه $G = H$ و این تناقض با فرض است. پس $H \subseteq < G \setminus H >$ و لذا $G =< G \setminus H >$.
پس

تمرین ۲۸.۵.۲. *با دانسته فرض کردن مطلب زیر یک گروه متناهیا تولید شده چنان ارائه کنید که یک زیرگروه آن متناهیا تولید شده نباشد.*
"گروه G متناهیا تولید شده است اگر و تنها اگر برای هر زنجیر از زیرگروه‌های G به شکل

$$H_0 \leq H_1 \leq H_2 \leq H_3 \leq ...$$

عدد طبیعی n موجود باشد که $H_n = H_{n+1} = ...$، یعنی زنجیر متوقف شود."

حل. در گروه ضربی $GL_2(\mathbb{R})$ دو ماتریس زیر را در نظر می‌گیریم

$$A = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \qquad B = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

و قرار می‌دهیم $G =< A, B >$ که گروهی متناهیا تولید شده است. حال فرض کنیم H مجموعه همه آن اعضا از G باشد که روی قطر اصلی آنها درایه ۱ قرار دارد. H ناتهی است. زیرا ماتریس همانی را دارد و یک بررسی ساده با کمک قضیه ۵.۴.۲ نشان می‌دهد که H زیرگروه است. همچنین برای هر $n \in \mathbb{W}$، $A^n B A^{-n} = A^n B (A^{-1})^n$ یک عضو از H است (بررسی کنید). دقت کنید که A وارونپذیر است. اما داریم

$$A^{n+1} B A^{-(n+1)} = A^{n+1} B A^{-n-1} = A(A^n B A^{-n}) A^{-1}.$$

این نشان می‌دهد که $< A^{n+1} B A^{-(n+1)} > \ \leq \ < A^n B A^{-n} >$. حال قرار می‌دهیم $H_i =< A^i B A^{-i} >$. حال زنجیر زیر از زیرگروه‌های H به شکل

$$H_0 \leq H_1 \leq H_2 \leq H_3 \leq ...$$

متوقف نمی‌شود. پس H متناهیا تولید شده نیست.

۶.۲ مرتبه گروه و عناصر گروه

در این بخش ابزاری را معرفی می‌کنیم تا به کمک آن بتوانیم خواص بیشتری از گروه‌ها را کشف کنیم. با تعریف زیر کار را آغاز می‌کنیم. تمرینات حل شده این بخش را با دقت مطالعه نمایید.

تعریف ۱.۶.۲. *فرض کنیم G یک گروه باشد. عدد اصلی مجموعه G را مرتبه گروه نامیم و آن را با $|G|$ یا $o(G)$ نمایش می‌دهیم. واضح است که اگر $o(G)$ متناهی باشد آنگاه به گروه G یک گروه متناهی و در غیر این صورت به G یک گروه نامتناهی گوییم.*

مثال ۲.۶.۲. *گروه $G = (\mathbb{Z}_m, +)$ از مرتبه m است یعنی $o(G) = m$. واضح است که این گروه متناهی است.*

مثال ۳.۶.۲. *گروه $G = (\mathbb{Z}, +)$ از مرتبه نامتناهی است یعنی $o(G) = \infty$.*

مثال ۴.۶.۲. *برای هر عدد طبیعی $n \geq ۲$، گروه $G_n = (\mathbb{Z}_n, +)$ از مرتبه متناهی است. اما $\prod_{n=۲}^{\infty} G_n$ گروهی نامتناهی است.*

مثال ۵.۶.۲. *گروه $G = S_n$ از مرتبه $n!$ است، یعنی $o(G) = n!$. واضح است که این گروه متناهی است.*

مثال ۶.۶.۲. *گروه $G = (\mathbb{Z}_p, .)$ که p عددی اول، از مرتبه p است یعنی $o(G) = p$. واضح است که این گروه متناهی است.*

مثال ۷.۶.۲. *با توجه به تمرین ۲. ۲. ۵۹، گروه $U(\mathbb{Z}_n)$ از مرتبه $\varphi(n)$ است یعنی $o(G) = \varphi(n)$ (φ تابع اویلر است، فصل اول را ببینید). واضح است که این گروه متناهی است.*

تعریف ۸.۶.۲. *فرض کنیم G یک گروه با عنصر خنثی e باشد و $x \in G$. اگر کوچکترین عدد طبیعی n موجود باشد که $x^n = e$ آنگاه n را مرتبه x نامیم و با $o(x)$ نمایش می‌دهیم. اگر چنین عدد طبیعی موجود نباشد آنگاه گوییم x از مرتبه نامتناهی است و می‌نویسیم $o(x) = \infty$.*

مثال ۹.۶.۲. *عنصر $\bar{۲}$ در گروه $(\mathbb{Z}_۶, +)$ دارای مرتبه سه است. زیرا $\bar{۰} = \bar{۲} + \bar{۲} + \bar{۲}$. بنابراین $o(\bar{۲}) = ۳$.*

مثال ۱۰.۶.۲. *عنصر $\bar{۳}$ در گروه $(\mathbb{Z}_۴, +)$ دارای مرتبه چهار است. زیرا $\bar{۰} = \overline{۱۲} = ۴\bar{۳}$. بنابراین $o(\bar{۳}) = ۴$.*

مثال ۱۱.۶.۲. *در گروه $\mathbb{K}_۴$ مرتبه هر عنصر به جز عنصر خنثی e، برابر دو است. زیرا در این گروه داریم $a^۲ = b^۲ = c^۲ = e$. در نتیجه $o(a) = o(b) = o(c) = ۲$.*

مثال ۱۲.۶.۲. *عنصر i در گروه $\mathbb{Q}_۸$ دارای مرتبه چهار است. زیرا $i^۴ = ۱$. بنابراین $o(i) = ۴$.*

مثال ۱۳.۶.۲. *عنصر ۳ در گروه $(\mathbb{Z}, +)$ دارای مرتبه نامتناهی است. بنابراین $o(۳) = \infty$.*

آیا ارتباطی بین مرتبه گروه و مرتبه عناصر آن وجود دارد؟ گزاره زیر به همین مطلب پاسخ می دهد.

گزاره ۱۴.۶.۲. *فرض کنیم G گروهی از مرتبه متناهی n باشد. در این صورت هر عنصر G مرتبه متناهی دارد.*

اثبات. فرض کنیم $x \in G$. مجموعه زیر را در نظر می‌گیریم

$$T = \{x, x^۲, x^۳, ...\}.$$

واضح است که T زیرمجموعه G است و چون G متناهی است باید T متناهی باشد. پس اعداد طبیعی i و j چنان وجود دارند که $x^i = x^j$. بدون کم شدن از کلیت فرض کنیم $i > j$. چون $x^j \in G$ و G گروه است، x^j دارای وارون x^{-j} در G است (چرا؟). پس با ضرب طرفین در x^{-j} داریم $x^{i-j} = x^۰ = e$. $\square$

مرتبه متناهی بودن همه عناصر گروه نمی‌تواند به گروه اجبار کند که متناهی باشد! مثال زیر را به دقت مطالعه کنید.

مثال ۱۵.۶.۲. *فرض کنیم $G = \mathbb{P}(\mathbb{N})$. عمل دوتایی روی G را همان تقاضل متقارن مجموعه‌ها در نظر می‌گیریم. یعنی برای هر $A, B \in G$*

$$A * B = (A \cup B) \setminus (A \cap B).$$

یک بررسی ساده نشان می‌دهد که $(G, *)$ یک گروه آبلی است که $\emptyset$ عنصر خنثی آن است. اما برای هر $A \in G$ داریم

$$A^۲ = A * A = (A \cup A) \setminus (A \cap A) = \emptyset.$$

این یعنی $o(A) = ۲$. دقت شود که G یک گروه نامتناهی است ولی هر عنصر آن مرتبه متناهی دارد!

به عنوان مثالی دیگر، مثال زیر را ببینید.

مثال ۱۶.۶.۲. *فرض کنیم برای هر عدد طبیعی i، قرار می‌دهیم $G_i = (\mathbb{Z}_۲, +)$. مرتبه هر عنصر گروه $\prod_{i=۱}^{\infty} G_i$ متناهی است و دقیقا برابر ۲ است. اما این گروه نامتناهی است.*

حال گزاره زیر را داریم.

گزاره ۱۷.۶.۲. *فرض کنیم G یک گروه با عنصر خنثی e باشد و $x \in G$.*

(۱) اگر برای عدد صحیحی مانند m داشته باشیم $x^m = e$ آنگاه $o(x)$ متناهی است و $o(x)|m$.

(۲) اگر $o(x) = n$ آنگاه به ازای هر عدد صحیح مثبت k، $x^k = x^r$ که در آن $k \overset{n}{\equiv} r$.

اثبات. (۱) چون $x^m = e$ پس $x^{-m} = e$. در نتیجه کوچکترین عدد طبیعی n وجود دارد که $x^n = e$ (چرا؟) یعنی $o(x) = n$. طبق الگوریتم تقسیم، قضیه ۷.۲.۱ داریم $m = nq + r$ که $\circ \leq r < n$. بنابراین $e = x^m = x^{nq+r} = x^{nq}x^r = (x^n)^q x^r = x^r$ که این در تناقض با انتخاب ما از n است. لذا $r = \circ$ و $n|m$.
(۲) طبق الگوریتم تقسیم، قضیه ۷.۲.۱ داریم $k = nq + r$ که $\circ \leq r < n$. بنابراین $x^k = x^{nq+r} = (x^n)^q x^r = x^r$ بدیهی است که $k \overset{n}{\equiv} r$. □

اکنون قضیه مهم زیر را داریم.

قضیه ۱۸.۶.۲. *فرض کنیم G یک گروه باشد و $x \in G$. در این صورت $< x >$ مرتبه n است اگر و تنها اگر $o(x) = n$.*

اثبات. فرض کنیم $H =< x >$ از مرتبه متناهی n باشد، یعنی $|H|= n$. طبق گزاره ۱۴.۶.۲ باید مرتبه x متناهی باشد. فرض کنیم $o(x) = m$. طبق نتیجه ۱۰.۵.۲ و گزاره ۱۷.۶.۲ قسمت (۲) داریم

$$< x >= \{x^k \mid k \in \mathbb{Z}\} = \{x^k = x^r \mid k \overset{m}{\equiv} r\} = \{x^r \mid r = \circ, ۱, ۲, ..., m - ۱\} = \{e, x, x^۲, ..., x^{m-۱}\}$$

پس H دارای عدد اصلی m است و این تناقض است مگر این که $m = n$.
برعکس، فرض کنیم $o(x) = n$. در این صورت باید عناصر e، x، ...، $x^{n-۱}$ متمایز باشند. زیرا اگر برای $\circ \leq i < j \leq n - ۱$ داشته باشیم $x^i = x^j$ آنگاه $x^{j-i} = e$ و طبق گزاره ۱۷.۶.۲ قسمت (۱)، باید $o(x) = n|j - i$ که تناقض آشکار است. طبق نتیجه ۱۰.۵.۲ و گزاره ۱۷.۶.۲ قسمت (۲) داریم

$$< x >= \{x^k \mid k \in \mathbb{Z}\} = \{x^k = x^r \mid k \overset{n}{\equiv} r\} = \{x^r \mid r = \circ, ۱, ۲, ..., n - ۱\} = \{e, x, x^۲, ..., x^{n-۱}\}$$

و لذا $|< x >|= n$. □

نتیجه ۱۹.۶.۲. *اگر G یک گروه متناهی و $e \in G$ عنصر خنثی باشد آنگاه عدد طبیعی k چنان وجود دارد که برای $x \in G$ داریم $x^k = e$.*

اثبات. چون G متناهی است پس زیرگروه $H =< x >$ نیز متناهی است که $x \in G$. اگر $|H|= n_x$ باشد آنگاه طبق قضیه ۱۸.۶.۲ داریم $o(x) = n_x$. اکنون قرار می‌دهیم $k = \prod_{x\in G} n_x$. واضح است که برای $x \in G$ داریم $x^k = e$. □

این بخش را با قضیه زیر به پایان می‌رسانیم.

قضیه ۲۰.۶.۲. *فرض کنیم G یک گروه دوری متناهی مرتبه n باشد و $d|n$. در این صورت G دقیقا یک زیرگروه مانند H دارد که $|H|= d$.*

اثبات. فرض کنیم $G =< x >$ که $x \in G$. پس طبق قضیه ۱۸.۶.۲ داریم $o(x) = n$. اگر $d = ۱$ و یا $d = n$ آنگاه به ترتیب $H = \{e\}$ و یا $H = G$، لذا چیزی برای اثبات نداریم. فرض کنیم $۱ < d < n$. طبق فرض، عدد صحیح m چنان وجود دارد که $n = dm$. عنصر $y = x^m$ از G را در نظر می‌گیریم و نشان می‌دهیم که $o(y) = d$. واضح است که $y^d = x^{md} = x^n = e$. لذا طبق قسمت (۱) از گزاره ۱۴.۶.۲ داریم $o(y)|d$. لذا $o(y) \leq d$. اگر $o(y) = t < d$ آنگاه $x^{mt} = y^t = e$. حال طبق گزاره ۱۴.۶.۲ قسمت (۱) باید $o(x) = n|mt$. بنابراین $mt < md = n$ و لذا $t < d$ که تناقض آشکار است. در نتیجه $o(y) = d$ و طبق قضیه ۱۸.۶.۲ $H =< y >$ از مرتبه d است. فقط مانده این مطلب که یکتایی H را نشان دهیم. فرض کنیم زیرگروه H' از G موجود باشد که $|H'|= d$. چون G دوری است لذا طبق قضیه ۲۲.۵.۲ باید H' نیز دوری باشد. بنابراین می‌توانیم فرض کنیم $H' =< x^t >$. طبق قضیه ۱۸.۶.۲ داریم $o(x^t) = d$. لذا $(x^t)^d = x^{td} = e$ و از گزاره ۱۴.۶.۲ قسمت (۱) باید $o(x) = n = md|td$. این نشان می‌دهد که $m|t$. فرض کنیم $t = lm$. در این صورت $x^t = x^{lm} = (x^m)^l$. بنابراین $H' \subseteq H$. اما دو مجموعه متناهی H و H' عدد اصلی d دارند و یکی زیرمجموعه دیگری است لذا باید $H = H'$. اثبات کامل است. $\square$

مثال ۲۱.۶.۲. *می‌دانیم که گروه $G = (\mathbb{Z}_{۱۲}, +)$ یک گروه دوری متناهی است.* دقت شود که $G =< \bar{۱} >$. *از طرفی عدد ۳ مرتبه گروه یعنی عدد ۱۲ را می‌شمارد. لذا طبق قضیه ۲۰.۶.۲ در G فقط یک زیرگروه H مرتبه ۳ وجود دارد. چون G دوری است لذا طبق قضیه ۲۲.۵.۲ باید H نیز دوری باشد. فرض کنیم $H =< \bar{x} >$. پس طبق قضیه ۱۸.۶.۲ داریم $o(\bar{x}) = ۳$. اما در G عنصر $\bar{۴}$ مرتبه ۳ دارد. بنابراین*

$$H =< \bar{۴} >= \{\bar{۰}, \bar{۴}, \bar{۸}\}.$$

تمرین‌های حل شده

تمرین ۲۲.۶.۲. *فرض کنیم G گروهی از مرتبه زوج باشد. نشان دهید که دقیقا تعداد فردی عنصر در G وجود دارد که از مرتبه ۲ هستند.*

حل. می‌دانیم که $x^۲ \neq e$ اگر و تنها اگر $x \neq x^{-۱}$. مجموعه زیر را در نظر می‌گیرم

$$T = \{(x, x^{-۱}) \mid x \in G, \ \ x \neq x^{-۱}\}.$$

به وضوح $|T|$ عدد زوج است. در نتیجه تعداد زوج عنصر مانند x هست که $x^۲ \neq e$. چون مرتبه گروه زوج است، تعداد زوجی عنصر مانند y در G هستند که $y^۲ = e$. چون e یکی از عناصری هست که $e^۲ = e$، پس تعداد فردی عنصر در G مانند y وجود دارد که $y^۲ = e$.

تمرین ۲۳.۶.۲. *فرض کنیم G یک گروه مرتبه متناهی باشد و برای دو زیرمجموعه ناتهی A و B از G داشته باشیم $|A|+|B|> |G|$. نشان دهید که $G = AB$.*

حل. واضح است که $AB \subseteq G$. قرار می‌دهیم

$$A^* = \{a^{-۱} \ \mid \ a \in A\}.$$

فرض کنیم $g\in G$. یک بررسی ساده نشان می‌دهد که رابطه

$$f: A \longrightarrow A^*g,\quad f(a)=a^{-1}g$$

یک تابع خوشتعریف یک‌به‌یک و پوشا است. لذا $|A|=|A^*g|$. اما داریم

$$|A|+|B|>|G|\geq |A^*g\cup B|=|A^*g|+|B|-|A^*\cap B|=|A|+|B|-|A^*g\cap B|.$$

لذا باید $|A^*g\cap B|\geq 1$. یعنی $A^*g\cap B$ ناتهی است. فرض کنیم $b\in A^*g\cap B$. پس عنصر $a^{-1}\in A^*$ وجود دارد که $b=a^{-1}g$. لذا $g=ab\in AB$ و $G\subseteq AB$.

تمرین ۲.۶.۲۴. *نشان دهید که برای هر عضو x از گروه G داریم* $o(x)=o(x^{-1})$.

حل. فرض کنیم $o(x)=t$ و $o(x^{-1})=k$. پس $(x^{-1})^t=(x^t)^{-1}=e$ و لذا طبق گزاره ۲.۶.۱۷ داریم $k|t$. اما $e=(x^{-1})^k=(x^k)^{-1}$ و لذا باید $x^k=e$. حال طبق گزاره ۲.۶.۱۷ داریم $t|k$. در نتیجه $k=t$.

تمرین ۲.۶.۲۵. *اگر x و y عناصری دلخواه در گروه G باشند آنگاه نشان دهید که* $o(xy)=o(yx)$.

حل. فرض کنیم $o(xy)=t$ و $o(yx)=k$. حال داریم

$$(yx)^t=\underbrace{yxyx...yx}_{t\text{تا}}=y\,\underbrace{xyxy...xy}_{(t-1)\text{تا}}\,x=y(xy)^{t-1}x.$$

از سمت چپ تساوی بالا را در y ضرب می‌کنیم

$$(yx)^ty=y(xy)^{t-1}xy=y(xy)^t=y.$$

حال طرفین را در y^{-1} از سمت چپ ضرب می‌کنیم $(yx)^t=e$. حال طبق گزاره ۲.۶.۱۷ داریم $k|t$. با روش مشابه $t|k$ و لذا $t=k$.

تمرین ۲.۶.۲۶. *اگر x و y عناصری در گروه G باشند آنگاه نشان دهید که* $o(y)=o(x^{-1}yx)$.

حل. حتما قبل از دیدن حل، تمرین ۲.۲.۶۲ را یکبار دیگر مطالعه نمایید. اکنون فرض کنیم $o(x^{-1}yx)=t$ و $o(y)=k$. پس داریم

$$(x^{-1}yx)^k=\underbrace{x^{-1}yx\,x^{-1}yx\,x^{-1}yx...x^{-1}yx}_{k\text{تا}}=x^{-1}y^kx=x^{-1}x=e.$$

حال طبق گزاره ۲.۶.۱۷ داریم $t|k$. حال داریم

$$y^t=xx^{-1}y^txx^{-1}=x(x^{-1}yx)^tx^{-1}=xx^{-1}=e.$$

پس $t|k$ و لذا $t=k$.

تمرین ۲.۶.۲۷. *فرض کنیم G گروهی باشد که دقیقا یک عنصر از مرتبه n مانند x دارد. نشان دهید که $x \in Z(G)$ و $n = ۲$.*

حل. طبق تمرین حل شده قبل، می‌دانیم که برای هر $y \in G$ داریم $o(x) = o(y^{-۱}xy)$. چون فقط یک عنصر از مرتبه n وجود دارد پس باید $x = y^{-۱}xy$ و لذا $yx = xy$. این نشان می‌دهد که $x \in Z(G)$. از طرفی $o(x) = o(x^{-۱})$ (چرا؟)، پس باید $x = x^{-۱}$ و این یعنی $x^۲ = e$. یعنی $n = ۲$.

تمرین ۲.۶.۲۸. *فرض کنیم در گروه G برای $x \in G$ داشته باشیم $o(x) = n$. اگر برای عدد صحیح m رابطه $(m, n) = ۱$ برقرار باشد آنگاه $o(x^m) = n$.*

حل. فرض کنیم $o(x^m) = k$. پس $e = (x^m)^k = x^{mk}$. طبق گزاره ۲.۶.۱۷، داریم $n|mk$. چون $(m, n) = ۱$ پس $n|k$. اما $(x^m)^n = x^{mn} = (x^n)^m = e$. دوباره طبق گزاره ۲.۶.۱۷، داریم $k|n$ و لذا $k = n$.

تمرین ۲.۶.۲۹. *فرض کنیم که G یک گروه و $x \in G$. اگر $o(x) = n$ و برای عدد صحیح m داشته باشیم $(m, n) = d$ آنگاه نشان دهید که $o(x^m) = \frac{n}{d}$.*

حل. فرض کنیم $o(x^m) = k$. پس $e = (x^m)^k = x^{mk}$. طبق گزاره ۲.۶.۱۷، داریم $n|mk$ و در نتیجه $\frac{n}{d}|\frac{m}{d}k$. چون $(m, n) = d$ پس $(\frac{m}{d}, \frac{n}{d}) = ۱$ و لذا $\frac{n}{d}|k$. از طرفی دیگر داریم $(x^m)^{\frac{n}{d}} = x^{\frac{nm}{d}} = (x^n)^{\frac{m}{d}} = e$. دوباره طبق گزاره ۲.۶.۱۷، داریم $k|\frac{n}{d}$ و لذا $k = \frac{n}{d}$.

تمرین ۲.۶.۳۰. *نشان دهید هر گروه دوری از مرتبه نامتناهی فقط دو مولد دارد.*

حل. فرض کنیم $G =< x >$ یک گروه دوری نامتناهی باشد. واضح است که $G =< x^{-۱} >$. زیرا $x^n = (x^{-۱})^{-n}$. پس دو مولد را پیدا کرده‌ایم یکی x و دیگری $x^{-۱}$. حال فرض کنیم $G =< y >$. عدد صحیح n چنان وجود دارد که $y = x^n$ (چرا؟). همچنین عدد صحیح m چنان وجود دارد که $x = y^m$ (چرا؟). لذا

$$x = y^m = (x^n)^m = x^{mn}.$$

با ضرب طرفین تساوی در $x^{-۱}$ داریم $x^{mn-۱} = e$، یعنی $o(x)$ متناهی است. حال طبق قضیه ۲.۶.۱۸ باید $G =< x >$ متناهی باشد. این تناقض آشکار است، مگر این که $mn = ۱$. این معادل است با $m = n = ۱$ و یا $m = n = -۱$. پس $y = x$ یا $y = x^{-۱}$.

تمرین ۲.۶.۳۱. *فرض کنیم G یک گروه باشد و $G =< x, y >$ به طوری که $o(x) = ۲$، $o(y) = ۳$ و $o(xy) = ۲$. نشان دهید که $o(G) = ۶$.*

حل. چون $x^۲ = e$ پس $x = x^{-۱}$. چون $y^۳ = e$ و $y^۲ = y^{-۱}$. اما $(xy)^۲ = xyxy = e$ و لذا $xy = y^{-۱}x^{-۱} = y^۲x$. یعنی $xy = y^۲x$. با توجه به قضیه ۲.۵.۵ و رابطه $xy = y^۲x$ داریم

$$G =< x, y >= \{x^my^n \mid m \in \{۰, ۱\}, \ n \in \{۰, ۱, ۲\}\}.$$

حال داریم ۶ $\le |G|= o(G)$. اکنون فرض می‌کنیم $H =< x >$ و $K =< y >$. طبق قضیه ۱۸.۶.۲ داریم ۲ $|H|=$ و ۳ $|K|=$. اما همه اعضای H مرتبه ۲ هستند و همه اعضای K مرتبه ۳ (بررسی کنید)، بنابراین باید $H \cap K = \{e\}$. لذا طبق قضیه ۳۱.۴.۲ نتیجه می‌شود که

$$|G|\ge |HK|= \frac{|H|\ |K|}{|H \cap K|} = |H|\ |K|= ۶.$$

در نتیجه ۶ $|G|= o(G) =$.

تمرین ۳۲.۶.۲. *برای گروه D_n یک مجموعه مولد دو عضوی مانند $\{\sigma, \tau\}$ پیدا کنید یعنی نشان دهید*

$$D_n =< \{\sigma, \tau \mid \sigma^n = \tau^۲ = (\tau\sigma)^۲ = e\} >= \{e, \sigma, \sigma^۲, ..., \sigma^{n-۱}, \tau, \sigma\tau, \sigma^۲\tau, ..., \sigma^{n-۱}\tau\}.$$

حل. فرض کنیم

$$\sigma = \begin{pmatrix} ۱ & ۲ & ... & n \\ ۲ & ۳ & ... & ۱ \end{pmatrix}$$

که دوران به اندازه $\frac{۲\pi}{n}$ و

$$\tau = \begin{pmatrix} ۱ & ۲ & ... & n \\ ۱ & n & ... & ۲ \end{pmatrix}$$

که انعکاس نسبت به راس ۱ است. یک بررسی ساده نشان می‌دهد که $o(\sigma) = n$ و ۲ $o(\tau) =$. همچنین ۲ $o(\tau\sigma) =$. رابطه آخر و این که $\tau = \tau^{-۱}$ روابط

$$\tau\sigma = \sigma^{-۱}\tau^{-۱} = \sigma^{-۱}\tau \qquad \tau\sigma^k\tau = \sigma^{-k}$$

را می‌دهد. پس

$$H =< \{\sigma, \tau \mid \sigma^n = \tau^۲ = (\tau\sigma)^۲ = e\} >= \{\sigma^i, \sigma^i\tau \mid ۰ \le i \le n - ۱\} = \{e, \sigma, \sigma^۲, ..., \sigma^{n-۱}, \tau, \sigma\tau, \sigma^۲\tau, ..., \sigma^{n-۱}\tau\}.$$

اما $H \subseteq D_n$ و $|H|= ۲n$ پس طبق قضیه ۱۴.۳.۲ باید $H = D_n$.

تمرین ۳۳.۶.۲. *فرض کنیم $G =< x >$ و $H =< y >$ دو گروه دوری به ترتیب از مرتبه m و n باشند که ۱ $(m, n) =$. نشان دهید که $G \times H$ دوری و از مرتبه mn است.*

حل. فرض کنیم $o((x, y)) = k$. حال داریم

$$(x, y)^{mn} = (x^{mn}, y^{mn}) = (e_G, e_H).$$

یعنی $k|mn$ (چرا؟). اما

$$(e_G, e_H) = (x, y)^k = (x^k, y^k).$$

پس باید $x^k = e_G$ و $y^k = e_H$. لذا $m|d$ و $n|d$، در نتیجه $mn|d$. بنابراین $k = mn$. طبق قضیه ۱۸.۶.۲، $|< (x, y) >| = mn$. اما $|G \times H|= mn$ و $< (x, y) >\subseteq G \times H$، پس باید $< (x, y) >= G \times H$.

۷.۲ هم‌دسته‌ها و قضیه لاگرانژ

برای مطالعه گروه‌ها در این یک ابزار قدرتمند دیگر معرفی می‌کنیم.

تعریف ۱.۷.۲. فرض کنیم G یک گروه، $H \leq G$ و $a \in G$.

(الف) به مجموعه

$$aH = \{ah \mid h \in H\}$$

هم دسته چپ H در G گوییم.

(ب) به مجموعه

$$Ha = \{ha \mid h \in H\}$$

هم دسته راست H در G گوییم.

(ج) عنصر a را نماینده هم دسته چپ aH یا هم دسته راست Ha نامیم.

مثال ۲.۷.۲. گروه $G = (\mathbb{Z}, +)$ و زیرگروه $H = ۳\mathbb{Z}$ را در نظر می‌گیرم. فرض کنیم $a \in \mathbb{Z}$. طبق الگوریتم تقسیم، قضیه ۷.۲.۱ نتیجه می‌شود که $a = ۳q + r$ که $۰ \leq r < ۳$. لذا چون گروه جمعی است داریم

$$a + H = \{k + h \mid h \in H\} = \{a + ۳k \mid ۳k \in H\} =$$
$$\{۳q + r + ۳k \mid ۳k \in H, \ ۰ \leq r < ۳\} = \{r + ۳k' \mid ۳k' \in H, \ ۰ \leq r < ۳\}.$$

پس هم دسته‌های چپ H در G به صورت $۳\mathbb{Z}$، $۳\mathbb{Z} + ۱$ و $۳\mathbb{Z} + ۲$ هستند. اگر a مضربی از عدد ۳ باشد، هم دسته $H = ۳\mathbb{Z}$ حاصل می‌شود. اگر a بر عدد ۳ باقیمانده ۱ داشته باشد هم دسته $۳\mathbb{Z} + ۱$ حاصل می‌شود. اگر a بر عدد ۳ باقیمانده ۲ داشته باشد هم دسته $۳\mathbb{Z} + ۲$ حاصل می‌شود.
برای زیرگروه دلخواه $n\mathbb{Z}$ به صورت مشابه، هم دسته‌های چپ $n\mathbb{Z}$، $n\mathbb{Z} + ۱$، ...، $n\mathbb{Z} + (n - ۱)$ هستند.

تذکر ۳.۷.۲. اگر G گروهی آبلی باشد آنگاه هم دسته چپ و راست یکی هستند، یعنی $aH = Ha$.
هم دسته‌های چپ یا راست زیرمجموعه گروه هستند ولی لزوما زیرگروه نیستند! مثلا هم دسته $۳\mathbb{Z} + ۱$ زیرگروه نیست.

مثال ۴.۷.۲. فرض کنیم

$$G = \{\begin{pmatrix} a & b \\ ۰ & a \end{pmatrix} \mid a, b \in \mathbb{Z}_۳, \ a \neq \bar{۰}\}.$$

G با ضرب عادی ماتریسی یک گروه است. قرار می‌دهیم

$$H = \{\begin{pmatrix} \bar{۱} & c \\ ۰ & \bar{۱} \end{pmatrix} \mid c \in \mathbb{Z}_۳\}.$$

واضح است که $H \leq G$. برای هر

$$\begin{pmatrix} a & b \\ ۰ & a \end{pmatrix} \in G$$

داریم

$$\begin{pmatrix} a & b \\ ۰ & a \end{pmatrix} = \begin{pmatrix} a & ۰ \\ ۰ & a \end{pmatrix} \begin{pmatrix} \bar{۱} & a^{-۱}b \\ ۰ & \bar{۱} \end{pmatrix}.$$

عنصر دوم از ضرب سمت راست تساوی بالا عضوی از H است. حال نوشتن هم دسته‌های چپ بسیار ساده است زیرا طبق تساوی بالا شکل aH ظاهر شده است. چون $a \neq \bar{۰}$، هم دسته‌های چپ با انتخاب $a = \bar{۱}$ و $a = \bar{۲}$ حاصل می‌شوند. یعنی

$$\begin{pmatrix} \bar{۱} & ۰ \\ ۰ & \bar{۱} \end{pmatrix} H = H$$

$$\begin{pmatrix} \bar{۲} & ۰ \\ ۰ & \bar{۲} \end{pmatrix} H = \{\begin{pmatrix} \bar{۲} & \bar{۲}c \\ ۰ & \bar{۲} \end{pmatrix} \ \mid \ c \in \mathbb{Z}_۳\}$$

هم دسته‌های چپ هستند.

مثال ۵.۷.۲. فرض کنیم

$$G = \{\begin{pmatrix} a & b \\ ۰ & a \end{pmatrix} \ \mid \ a, b \in \mathbb{Z}_۳, \ \ a \neq \bar{۰}\}.$$

G با ضرب عادی ماتریسی یک گروه است. قرار می‌دهیم

$$H = \{\begin{pmatrix} \bar{۱} & c \\ ۰ & \bar{۱} \end{pmatrix} \ \mid \ c \in \mathbb{Z}_۳\}.$$

واضح است که $H \leq G$. برای هر

$$\begin{pmatrix} a & b \\ ۰ & a \end{pmatrix} \in G$$

داریم

$$\begin{pmatrix} a & b \\ ۰ & a \end{pmatrix} = \begin{pmatrix} \bar{۱} & ba^{-۱} \\ ۰ & \bar{۱} \end{pmatrix} \begin{pmatrix} a & ۰ \\ ۰ & a \end{pmatrix}.$$

عنصر اول از ضرب سمت راست تساوی بالا عضوی از H است. حال نوشتن هم دسته‌های راست بسیار ساده است زیرا طبق تساوی بالا شکل Ha ظاهر شده است. چون $a \neq \bar{۰}$، هم دسته‌های راست با انتخاب $a = \bar{۱}$ و $a = \bar{۲}$ حاصل می‌شوند. یعنی

$$H \begin{pmatrix} \bar{۱} & ۰ \\ ۰ & \bar{۱} \end{pmatrix} = H$$

$$H \begin{pmatrix} \bar{۲} & ۰ \\ ۰ & \bar{۲} \end{pmatrix} = \{\begin{pmatrix} \bar{۲} & \bar{۲}c \\ ۰ & \bar{۲} \end{pmatrix} \ \mid \ c \in \mathbb{Z}_۳\}$$

هم دسته‌های راست هستند.

در مثال‌های بالا هم دسته‌های چپ با هم دسته‌های راست مساوی شدند! زیرا زیرگروه H یک زیرگروه خاص است که در بخش بعد مطالعه خواهیم کرد. اکنون مثال زیر را ببینید.

مثال ۶.۷.۲. *گروه $G = S_3$ را در نظر می‌گیریم. طبق نمادهای مثال ۷.۳.۲ قرار می‌دهیم*

$$\sigma_6 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \qquad H =< \sigma_6 >= \{\sigma_1, \sigma_6\}.$$

اگر حوصله کنید و با دقت محاسبات را انجام دهید آنگاه هم دسته‌ها چپ

$$\begin{aligned} \sigma_1 H &= H = \sigma_6 H \\ \sigma_2 H &= \{\sigma_2, \sigma_5\} = \sigma_5 H \\ \sigma_3 H &= \{\sigma_3, \sigma_4\} = \sigma_4 H \end{aligned}$$

هستند و هم دسته‌های راست

$$\begin{aligned} H\sigma_1 &= H = H\sigma_6 \\ H\sigma_2 &= \{\sigma_2, \sigma_4\} = H\sigma_4 \\ H\sigma_3 &= \{\sigma_3, \sigma_5\} = H\sigma_5 \end{aligned}$$

هستند! هم دسته‌های چپ با هم دسته‌های راست یکی نیست، یعنی

$$\{H, \sigma_2 H, \sigma_3 H\} \neq \{H, H\sigma_2, H\sigma_3\}.$$

مثال‌های بالا در سه مطلب مشترک هستند. یکی این که عدد اصلی هم دسته چپ aH و راست Ha یکسان است. دوم این که عدد اصلی مجموعه همه هم دسته‌های چپ و راست یکسان است و آخر آن که اجتماع آن ها برابر خود گروه می‌شود! در ادامه این بخش همین نکات مشترک به شدت مورد توجه ما است.

کار را با گزاره زیر شروع می‌کنیم.

گزاره ۷.۷.۲. *موارد زیر برای گروه G، $H \leq G$ و $a \in G$ بر قرار است.*

(۱) اگر $a \in H$ آنگاه $aH = Ha = H$.

(۲) همواره داریم $|aH| = |Ha| = |H|$.

اثبات. (۱) چون H زیرگروه است پس برای هر $h \in H$ داریم $ah \in H$ و $ha \in H$. زیرا $a \in H$. بنابراین بدیهی است که $aH = Ha = H$.

(۲) رابطه

$$f : H \longrightarrow aH, \quad f(h) = ah$$

یک تابع خوشتعریف یک‌به‌یک و پوشا است (بررسی کنید). پس $|aH| = |H|$. رابطه

$$g : H \longrightarrow Ha, \quad f(h) = ha$$

یک تابع خوشتعریف یک‌به‌یک و پوشا است (بررسی کنید). پس $|Ha| = |H|$. اثبات کامل است. □

حال قضیه مهم زیر را داریم.

قضیه ۸.۷.۲. *فرض کنیم G یک گروه و $H \leq G$. برای هر $u, v \in G$، تعریف می‌کنیم*

$$u \doteqdot v \iff u^{-1}v \in H.$$

در این صورت موارد زیر بر قرار است.
(۱) $\doteqdot$ رابطه هم ارزی روی G است.
(۲) کلاس هم ارزی $a \in G$ برابر است با aH یعنی $[a] = aH$.
(۳) هم دسته‌های چپ برای G یک افراز هستند.
(۴) داریم $G/\doteqdot = \{aH \mid a \in G\}$.

اثبات. (۱) برای هر $u \in G$ داریم $u^{-1}u = e \in H$ و لذا $u \doteqdot u$، یعنی $\doteqdot$ انعکاسی است. فرض کنیم $v \doteqdot u$. پس $u^{-1}v \in H$. اما H زیرگروه است، لذا طبق تمرین ۵۵.۲.۲ و تمرین ۵۶.۲.۲ داریم $v^{-1}u = (u^{-1}v)^{-1} \in H$. این یعنی $u \doteqdot v$ و $\doteqdot$ تقارنی است. اکنون فرض کنیم $v \doteqdot u$ و $w \doteqdot v$. پس $u^{-1}v \in H$ و $v^{-1}w \in H$. چون H زیرگروه است، باید $u^{-1}vv^{-1}w = u^{-1}w \in H$. یعنی $u \doteqdot w$ و لذا $\doteqdot$ تعدی و در نتیجه هم ارزی است.
(۲) طبق تعریف کلاس هم ارزی داریم

$$[a] = \{g \in G \mid g \doteqdot a\} = \{g \in G \mid a \doteqdot g\} =$$
$$\{g \in G \mid a^{-1}g \in H\} \overset{a^{-1}g=h}{=} \{ah \mid h \in H\} = aH.$$

(۳) طبق قضیه ۱۲.۱.۱، $G/\doteqdot$ یک افراز برای G است.
(۴) طبق تعریف داریم (صفحه دوم از فصل اول را ببینید)

$$G/\doteqdot = \{A \subseteq G \mid A = [a] \text{ که باشد} G \text{ای در} a\} =$$
$$\{A \subseteq G \mid A = aH \text{ که باشد} G \text{ای در} a\} =$$
$$\{aH \mid a \in G\}$$

و اثبات کامل است. $\square$

قضیه بالا ما را به سمت تعریف زیر سوق می‌دهد.

تعریف ۹.۷.۲. *مجموعه هم دسته‌های چپ زیرگروه H در گروه G را با نماد $(G/H)_l$ نشان می‌دهیم. یعنی*

$$(G/H)_l = G/\doteqdot = \{aH \mid a \in G\}.$$

مثال ۱۰.۷.۲. *به ترتیب در اولین، دومین وچهارمین مثال این بخش داریم*

$$\mathbb{Z} = ۳\mathbb{Z} \cup (۳\mathbb{Z} + ۱) \cup (۳\mathbb{Z} + ۲) \qquad (\mathbb{Z}/۳\mathbb{Z})_l = \{۳\mathbb{Z}, ۳\mathbb{Z} + ۱, ۳\mathbb{Z} + ۲\}$$

$$G = \begin{pmatrix} \bar{۱} & \bar{۰} \\ \bar{۰} & \bar{۱} \end{pmatrix} H \cup \begin{pmatrix} \bar{۲} & \bar{۰} \\ \bar{۰} & \bar{۲} \end{pmatrix} H \qquad (G/H)_l = \{\begin{pmatrix} \bar{۱} & \bar{۰} \\ \bar{۰} & \bar{۱} \end{pmatrix} H, \begin{pmatrix} \bar{۲} & \bar{۰} \\ \bar{۰} & \bar{۲} \end{pmatrix} H\}$$

$$S_۳ = H \cup \sigma_۱ H \cup \sigma_۲ H \qquad (S_۳/H)_l = \{H, \sigma_۱ H, \sigma_۲ H\}$$

حال قضیه زیر را داریم.

قضیه ۱۱.۷.۲. *فرض کنیم G یک گروه و $H \leq G$. برای هر $u, v \in G$، تعریف می‌کنیم*

$$u \Bumpeq v \iff uv^{-۱} \in H.$$

در این صورت موارد زیر بر قرار است.
(۱) *$\Bumpeq$ رابطه هم‌ارزی روی G است.*
(۲) *کلاس هم‌ارزی $a \in G$ برابر است با aH یعنی $[a] = aH$.*
(۳) *هم دسته‌های راست برای G یک افراز هستند.*
(۴) *داریم $G/\Bumpeq = \{Ha \mid a \in G\}$.*

اثبات. مشابه قضیه قبل است. □

قضیه بالا ما را به سمت تعریف زیر سوق می‌دهد.

تعریف ۱۲.۷.۲. مجموعه هم دسته‌های راست زیرگروه H در گروه G را با نماد $(G/H)_r$ نشان می‌دهیم. یعنی

$$(G/H)_r = G/\Bumpeq = \{Ha \mid a \in G\}.$$

مثال ۱۳.۷.۲. *به ترتیب در اولین، دومین و چهارمین مثال این بخش داریم*

$$\mathbb{Z} = ۳\mathbb{Z} \cup (۳\mathbb{Z} + ۱) \cup (۳\mathbb{Z} + ۲) \qquad (\mathbb{Z}/۳\mathbb{Z})_r = \{۳\mathbb{Z}, ۳\mathbb{Z} + ۱, ۳\mathbb{Z} + ۲\}$$

$$G = H \begin{pmatrix} \bar{۱} & \bar{۰} \\ \bar{۰} & \bar{۱} \end{pmatrix} \cup H \begin{pmatrix} \bar{۲} & \bar{۰} \\ \bar{۰} & \bar{۲} \end{pmatrix} H \qquad (G/H)_r = \{H \begin{pmatrix} \bar{۱} & \bar{۰} \\ \bar{۰} & \bar{۱} \end{pmatrix}, H \begin{pmatrix} \bar{۲} & \bar{۰} \\ \bar{۰} & \bar{۲} \end{pmatrix}\}$$

$$S_۳ = H \cup H\sigma_۱ \cup H\sigma_۲ \qquad (S_۳/H)_r = \{H, H\sigma_۱, H\sigma_۲\}$$

نتیجه ۱۴.۷.۲. *اگر هم دو هم دسته چپ (راست) دست کم در یک عنصر مشترک باشند آنگاه با هم مساوی هستند*

اثبات. طبق قضیه‌های بالا هم دسته‌های چپ و راست افراز برای گروه می‌باشند و افرازها اشتراک ندارند مگر این که مساوی باشند. □

لم ۱۵.۷.۲. *فرض کنیم G یک گروه و $H \leq G$. برای هر $a, b \in G$ موارد زیر معادل هستند.*
(۱) $aH = bH$.
(۲) $Ha^{-۱} = Hb^{-۱}$.
(۳) $aH \subseteq bH$.
(۴) $a \in bH$.
(۵) $a^{-۱}b \in H$.

اثبات. (۱) $\Leftarrow$ (۲). فرض کنیم $x \in Ha^{-1}$. پس عنصر $h \in H$ وجود دارد که $x = ha^{-1}$. طبق تمرین ۵۶.۲.۲ و تمرین ۵۵.۲.۲ داریم که $x^{-1} = ah^{-1} \in aH = bH$. لذا $x^{-1} = bh'$ که $h' \in H$. دوباره طبق تمرین ۵۶.۲.۲ و تمرین ۵۵.۲.۲ داریم $x = (x^{-1})^{-1} = h'^{-1}b^{-1}$. حال واضح است که $x \in Hb^{-1}$ و لذا $Ha^{-1} \subseteq Hb^{-1}$. برعکس، $Hb^{-1} \subseteq Ha^{-1}$، مشابه است. پس $Ha^{-1} = Hb^{-1}$.
(۲) $\Leftarrow$ (۳). فرض کنیم $x \in aH$. پس عنصر $h \in H$ وجود دارد که $x = ah$. طبق تمرین ۵۶.۲.۲ و تمرین ۵۵.۲.۲ داریم که $x^{-1} = h^{-1}a^{-1} \in Ha^{-1} = Hb^{-1}$. لذا $x^{-1} = h'b^{-1}$ که $h' \in H$. دوباره طبق تمرین ۵۶.۲.۲ و تمرین ۵۵.۲.۲ داریم $x = (x^{-1})^{-1} = bh'^{-1}$. حال واضح است که $x \in bH$ و لذا $aH \subseteq bH$.
(۳) $\Leftarrow$ (۴). چون $e \in H$ پس داریم $a = ae \in aH \subseteq bH$.
(۴) $\Leftarrow$ (۵). طبق قضیه ۸.۷.۲ داریم که $bH = [b]$. پس $a \doteq b$ و لذا $a^{-1}b \in H$.
(۵) $\Leftarrow$ (۱). طبق قضیه ۸.۷.۲ داریم که $a^{-1}b \in H$ اگر و تنها اگر $a \doteq b$. طبق تعریف کلاس هم ارزی بدیهی است که $aH = [a] = bH = [b]$. $\square$

لم ۱۶.۷.۲. *فرض کنیم G یک گروه و $H \leq G$. برای هر $a, b \in G$ موارد زیر معادل هستند.*
(۱) $Ha = Hb$.
(۲) $a^{-1}H = b^{-1}H$.
(۳) $Ha \subseteq Hb$.
(۴) $a \in Hb$.
(۵) $ab^{-1} \in H$.

اثبات. مشابه لم ۱۵.۷.۲ اثبات می‌شود. $\square$

اکنون قضیه مهم زیر را داریم.

قضیه ۱۷.۷.۲. *برای هر گروه G و $H \leq G$ داریم*
$$|(G/H)_l| = |(G/H)_r|.$$

اثبات. ضابطه
$$f : (G/H)_l \longrightarrow (G/H)_r, \ \ f(aH) = Ha^{-1}$$
را در نظر می‌گیریم. ابتدا خوشتعریفی را بررسی می‌کنیم. اگر $aH = bH$ باشد آنگاه طبق لم ۱۵.۷.۲ داریم $Ha^{-1} = Hb^{-1}$ و این یعنی $f(aH) = f(bH)$.
یک‌به‌یک بودن هم مشابه خوشتعریفی نتیجه مستقیم لم ۱۵.۷.۲ است. پوشایی هم واضح است. بنابراین حکم به دست می‌آید. دقت کنید که اگر رابطه
$$f : (G/H)_r \longrightarrow (G/H)_l, \ \ f(Ha) = a^{-1}H$$
را در نظر می‌گرفتیم، لم ۱۶.۷.۲ کارساز بود. $\square$

قضیه بالا ما را به تعریف زیر رهنمود می‌کند.

تعریف ۱۸.۷.۲. *طبق قضیه ۱۷.۷.۲ به عدد اصلی و یکتای* $|(G/H)_l|=|(G/H)_r|$ *اندیس زیرگروه* H *در* G *گوییم و با* $[G:H]$ *نمایش می‌دهیم.*

مثال ۱۹.۷.۲. *طبق مثال اول این بخش داریم* $[\mathbb{Z}:۳\mathbb{Z}]=۳$.

مثال ۲۰.۷.۲. *طبق مثال دوم این بخش داریم* $[G:H]=۲$.

مثال ۲۱.۷.۲. *طبق مثال چهارم این بخش داریم* $[S_۳:H]=۳$.

برای دیدن یک مثال از یک گروه و زیرگروه آن که اندیس نامتناهی دارد، مثال زیر را دنبال کنید.

مثال ۲۲.۷.۲. *فرض کنیم* $G=(\mathbb{Q},+)$ *و* $H=\mathbb{Z}$. *همچنین فرض کنیم* $\{p_i\}_{i=۱}^{\infty}$ *مجموعه اعداد اول باشد. چون گروه آبلی و جمعی است، برای هر* i*، یک هم دسته چپ یا راست به صورت*

$$\frac{۱}{p_i}+H=\{\frac{۱}{p_i}+k \mid k\in\mathbb{Z}\}$$

خواهیم داشت. حال اگر برای $i\neq j$ *داشته باشیم* $x\in(\frac{۱}{p_i}+\mathbb{Z})\cap(\frac{۱}{p_j}+\mathbb{Z})$ *آنگاه*

$$\frac{۱}{p_i}+k=x=\frac{۱}{p_i}+k'$$

که $k,k'\in\mathbb{Z}$. *پس* $\frac{۱}{p_i}-\frac{۱}{p_j}=k'-k\in\mathbb{Z}$ *و لذا باید* $p_ip_j|p_j-p_i$. *چون* $p_i|p_ip_j$ *پس* $p_i|p_j-p_i$. *لذا باید* $p_i|p_j$ *که تناقض آشکار است. پس هم دسته‌ها هیچ اشتراکی ندارند و تعداد آنها نامتناهی است. یعنی* $[\mathbb{Q}:\mathbb{Z}]=\infty$.

اکنون وقت آن است که شما را با یکی از مهمترین و پرکاربردترین قضایای جبر و نظریه گروه آشنا کنیم. افسوس (از این جهت که در برخی مسایل تحقیقاتی اگر عکس قضیه لاگرانژ صحیح باشد بسیار کار راحت می‌شود) که عکس قضیه لاگرانژ صحیح نیست! برای دیدن مثال نقض باید تا بخش آخر این فصل صبر کنید! اما برای گروه‌های خاص مانند گروه دوری متناهی، طبق قضیه ۲۰.۶.۲ عکس قضیه لاگرانژ صحیح است. هر چند همین صحیح نبودن عکس قضیه لاگرانژ سبب پیدایش قضایای کلیدی در نظریه گروه شده است، از جمله قضایای سیلو[۴]!

قضیه ۲۳.۷.۲. *(قضیه لاگرانژ) فرض کنیم* G *یک گروه متناهی باشد و* $H\leq G$. *در این صورت* $|G|\;|\;|H|$ *یا به عبارتی* $[G:H]=\frac{|G|}{|H|}$.

[۴]Sylow

اثبات. می‌دانیم که طبق قضیه ۸.۷.۲ هم دسته‌های چپ گروه G را افراز می‌کنند. و چون G متناهی است می‌توانیم فرض کنیم $G = \bigcup_{i=1}^{t} a_iH$. پس $[G : H] = t$. اما طبق گزاره ۷.۷.۲ داریم $|a_iH| = |H|$. بنابراین

$$|G| = \sum_{i=1}^{t} |a_iH| = \sum_{i=1}^{t} |H| = t|H| = [G : H]\, |H|$$

و این یعنی $|G| \mid |H|$ یا به عبارتی $[G : H] = \frac{|G|}{|H|}$. □

چند نتیجه بدیهی از قضیه لاگرانژ را در ادامه ببینید.

نتیجه ۲۴.۷.۲. *فرض کنیم G گروهی متناهی از مرتبه n باشد. در این صورت برای هر $x \in G$ داریم $|G| \mid o(x)$. در نتیجه $x^n = e$.*

اثبات. قرار می‌دهیم $H =< x >$. طبق قضیه ۱۸.۶.۲ داریم $|H| = o(x)$ و لذا طبق قضیه لاگرانژ، قضیه ۲۳.۷.۲ باید $|G| = n \mid o(x)$. □

نتیجه ۲۵.۷.۲. *هر گروه متناهی G با مرتبه عدد اول دوری و در نتیجه آبلی است.*

اثبات. فرض کنیم $|G| = p$ که p عددی اول است. همچنین فرض کنیم $e \neq x \in G$. طبق نتیجه قبل باید $p|o(x)$. در نتیجه $o(x) = 1$ یا $o(x) = p$. چون x عنصر خنثی نیست باید $o(x) = p$. طبق قضیه ۱۸.۶.۲ داریم $|< x >| = p$ و لذا باید $G =< x >$. زیرا $< x > \subseteq G$. طبق گزاره ۱۴.۵.۲ باید G آبلی باشد. □

نتیجه ۲۶.۷.۲. *در گروه متناهی G، برای زیرگروه‌های H و K که $(o(H), o(K)) = 1$، داریم $H \cap K = \{e\}$.*

اثبات. طبق قضیه لاگرانژ، قضیه ۲۳.۷.۲، داریم $|H| \mid |H \cap K|$ و $|K| \mid |H \cap K|$. بنابراین باید $(|H|, |K|) \mid |H \cap K| = 1$. یعنی $H \cap K = \{e\}$. □

مثال ۲۷.۷.۲. *قضیه اویلر_ فرما، قضیه ۲۴.۲.۱، می‌گوید که اگر عدد صحیح n نسبت به عدد صحیح m اول باشد آنگاه $n^{\varphi(m)} \overset{m}{\equiv} 1$ که φ تابع اویلر است. این مطلب اکنون اثبات ساده‌ای دارد. کافی است گروه $G = U(\mathbb{Z}_m)$ را در نظر بگیریم. طبق تمرین ۵۹.۲.۲ داریم که $\bar{n}$ در G قرار دارد و باید $|G| = \varphi(m)$ باشد. طبق قضیه لاگرانژ، قضیه ۲۳.۷.۲، $\bar{n}^{\varphi(m)} = \bar{1}$. پس در $\mathbb{Z}$ داریم $n^{\varphi(m)} \overset{m}{\equiv} 1$.*

مثال ۲۸.۷.۲. *می‌دانیم که ضریب جملات در بسط دو جمله‌ای به صورت $\binom{n}{k} = \frac{n!}{k!(n-k)!}$ است. می‌خواهیم نشان دهیم که این حاصل یک عدد صحیح است! اگر $n = m$ و یا $k = 0$ باشد چیزی برای اثبات نداریم. حال گروه S_n را در نظر می‌گیریم. طبق قضیه ۸.۳.۲ داریم $|S_n| = n!$. فرض*

کنیم H مجموعه‌ای از اعضای S_n باشد که
روی مجموعه $\{۱, ۲, ..., k\}$ جایگشت و روی $\{k+۱, k+۲, ..., n\}$ ثابت عمل کند،
روی مجموعه $\{۱, ۲, ..., k\}$ ثابت و روی $\{k+۱, k+۲, ..., n\}$ جایگشت عمل کند.
یک بررسی نشان می‌دهد که $H \leq S_n$. طبق قضیه لاگرانژ، قضیه ۲۳.۷.۲ داریم $|H| \mid n!$. اما به طبق اصل ضرب $|H|= k!\,(n-k)!$ است.

مثال ۲۹.۷.۲. *برای اعداد طبیعی m و n، آیا $\frac{(mn)!}{(m!)^n}$ یک عدد صحیح است؟ پاسخ مثبت است. اعداد ۱ تا mn را به شکل*

$$۱, ۲, ..., m;\; m+۱, m+۲, ..., ۲m;\; ۲m+۱, ۲m+۲, ..., ۳m;\; ...;\; (n-۱)m+۱, (n-۱)m+۲, ..., nm$$

می‌نویسیم. n تا m عدد توسط نقطه ویرگول‌ها جدا شده‌اند! حال گروه S_{mn} را در نظر می‌گیریم. طبق قضیه ۸.۳.۲ داریم $|S_{mn}|= (mn)!$. فرض کنیم H مجموعه‌ای از اعضای S_{mn} باشد که
روی مجموعه $\{۱, ۲, ..., m\}$ جایگشت و روی بقیه اعداد بین نقطه ویرگول ثابت عمل کند،
روی مجموعه $\{m+۱, , ..., ۲m\}$ جایگشت و روی بقیه اعداد بین نقطه ویرگول ثابت عمل کند،
روی مجموعه $\{۲m+۱, , ..., ۳m\}$ جایگشت و روی بقیه اعداد بین نقطه ویرگول ثابت عمل کند، ...
روی مجموعه $\{(n-۱)m, ..., nm\}$ جایگشت و روی بقیه اعداد بین ویرگول ثابت عمل کند.
یک بررسی نشان می‌دهد که $H \leq S_n$. طبق قضیه لاگرانژ، قضیه ۲۳.۷.۲ داریم $|H| \mid n!$. اما به طبق اصل ضرب $|H|= m!\ m! ... m! = (m!\,)^n$ است.

این بخش را با سه قضیه به پایان می‌بریم. قبل از آوردن این قضیه‌ها مقدماتی برای اثبات آنها لازم داریم. ابتدا مفهوم تراگشتی[۵] را معرفی می‌کنیم.

تعریف ۳۰.۷.۲. *فرض کنیم G یک گروه باشد و $H \leq G$. گوییم $T \subseteq G$*
(الف) تراگشتی چپ برای H در G است اگر هر هم دسته چپ دقیقا حاوی یک عنصر از T باشد.
(ب) تراگشتی راست برای H در G است اگر هر هم دسته چپ دقیقا حاوی یک عنصر از T باشد.
(ج) تراگشتی برای H در G است اگر تراگشتی چپ و تراگشتی راست باشد.

مثال ۳۱.۷.۲. *اولین مثال این بخش را به یاد بیاورید! زیرمجموعه $T = \{۰, ۱, ۲\}$ یک تراگشتی برای $۳\mathbb{Z}$ در $\mathbb{Z}$ است.*

مثال ۳۲.۷.۲. چهارمین مثال این بخش را به یاد بیاورید! *زیرمجموعه $T = \{\sigma_۱, \sigma_۲, \sigma_۳\}$ یک تراگشتی برای H در $S_۳$ است. زیرمجموعه $T = \{\sigma_۱, \sigma_۴, \sigma_۵\}$ یک تراگشتی دیگر برای H در $S_۳$ است.*

---
[۵] transversal

تذکر ۳۳.۷.۲. *وجود مجموعه تراگشتی چپ (راست) با کمک اصل انتخاب تضمین شده است! زیرا کافی است از هم دسته‌های چپ دقیقا یک عنصر انتخاب کنیم. دقت کنید که همه دسته‌های چپ از هم مجزا هستند چون برای گروه افراز هستند. لذا بسیار بدیهی است که اگر T یک تراگشتی چپ (راست) برای زیرگروه H از G باشد آنگاه $|T|=[G:H]$.*

تذکر ۳۴.۷.۲. *یک تراگشتی چپ برای یک زیرگروه لزوما یک تراگشتی راست نیست. در مثال‌های بالا تراگشتی‌های چپ، راست هم بودند! علت این مطلب زیرگروه نرمال است که در بخش بعد مطالعه می‌کنیم. در واقع اثبات می‌شود (ما بدون اثبات می‌پذیریم) که یک تراگشتی چپ یک تراگشتی راست برای زیرگروه H از گروه G است اگر و تنها اگر H زیرگروه نرمال باشد.*

لم ۳۵.۷.۲. *فرض کنیم G یک گروه باشد و $H \leq G$. اگر T یک تراگشتی چپ برای H در G باشد آنگاه $G=\bigcup_{t\in T} tH$ و هر عنصر G به صورت یکتا به شکل th است که $t\in T$ و $h\in H$.*

اثبات. طبق قضیه ۸.۷.۲ هم دسته‌های چپ H در G گروه G را افراز می‌کنند، یعنی می‌توانیم فرض کنیم مجموعه I چنان وجود دارد که $[G:H]=|I|=|T|$ و $G=\bigcup_{i\in I} a_iH$. حال از هم دسته چپ a_iH نماینده t_i در T قرار دارد. پس اکنون هم دسته چپ a_iH و t_iH در عنصر t_i مشترک هستند و لذا طبق نتیجه ۱۴.۷.۲ باید $a_iH=t_iH$. این نشان می‌دهد که

$$G=\bigcup_{i\in I} a_iH=\bigcup_{t\in T} tH.$$

فرض کنیم $g\in G$ به صورت $t'h'=g=th$ نوشته شود که $t,t'\in T$ و $h,h'\in H$. پس $th\in t'H$ و این یعنی دو هم دسته tH و $t'H$ عنصر مشترک دارند. لذا طبق نتیجه ۱۴.۷.۲ باید $tH=t'H$. چون T تراگشتی چپ است باید $t=t'$ و لذا $th=th'$ و باید $h=h'$ باشد. □

قضیه ۳۶.۷.۲. *فرض کنیم G یک گروه باشد و $K\leq H\leq G$. در این صورت*

$$[G:K]=[G:H]\,[H:K].$$

اثبات. می‌دانیم (تذکر اول بالا) که تراگشتی‌های چپ $T\subseteq G$ و $S\subseteq H$ چنان وجود دارند که $|T|=[G:H]$ و $|S|=[H:K]$. طبق قضیه ۸.۷.۲ داریم

$$G=\bigcup_{t\in T} tH \qquad\qquad H=\bigcup_{s\in S} sK$$

و لذا

$$G=\bigcup_{t\in t} t(\bigcup_{s\in S} sK)=\bigcup_{t\in T}\bigcup_{s\in S} tsK=\bigcup_{(t,s)\in T\times S} tsK.$$

اگر نشان دهیم که هم‌دسته‌های چپ tsK مجزا هستند آنگاه باید

$$[G:K]=|T\times S|=|T|\,|S|=[G:H]\,[H:K].$$

پس فرض کنیم $tsK = t's'K$. لذا $ts \in t's'K$ و این یعنی $ts = t's'k$ که $k \in K$. چون $s \in K \leq H$ پس $tsH = t(sH) = tH$. بنابراین با روشی کاملا مشابه خواهیم داشت $tsH = t's'kH = t'(s'k'H) = t'H$. پس $tH = t'H$. اما T تراگشتی چپ برای H در G است لذا باید $t = t'$. بلافاصله داریم $s = s'k$. یعنی $sK = s'kK = s'(kK) = s'K$. اما S تراگشتی چپ برای K در H است لذا باید $s = s'$. $\square$

مثال ۳۷.۷.۲. *می‌خواهیم اندیس زیرگروه $۱۵\mathbb{Z}$ در گروه $G = (۳\mathbb{Z}, +)$ را پیدا کنیم. طبق اولین مثال این بخش داریم $[\mathbb{Z} : ۳\mathbb{Z}] = ۳$ و $[\mathbb{Z} : ۱۵\mathbb{Z}] = ۱۵$. طبق قضیه ۳۶.۷.۲ داریم*

$$[۳\mathbb{Z} : ۱۵\mathbb{Z}] = \frac{[\mathbb{Z} : ۱۵\mathbb{Z}]}{[\mathbb{Z} : ۳\mathbb{Z}]} = ۵.$$

قضیه ۳۸.۷.۲. *فرض کنیم G یک گروه باشد و $H, K \leq G$. در این صورت*

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

همچنین وقتی $[G : K] < \infty$، در بالا تساوی رخ می‌دهد اگر و تنها اگر $G = KH$.

اثبات. ابتدا دقت کنید که $H \cap K$ زیرگروه H و K است. حال ضابطه

$$f : (H/(H \cap K))_l \longrightarrow (G/K)_l, \quad f(h(H \cap K)) = hK$$

یک تابع خوشتعریف است. زیرا اگر فرض کنیم $h(H \cap K) = h'(H \cap K)$ آنگاه از لم ۱۵.۷.۲ باید $h^{-۱}h' \in H \cap K \leq K$. دوباره طبق لم ۱۵.۷.۲ باید $hK = h'K$ یعنی $f(h(H \cap K)) = f(h'(H \cap K))$.

حال اگر برای $h, h' \in H$ داشته باشیم $hK = h'K$ آنگاه از لم ۱۵.۷.۲ $h^{-۱}h' \in K$. اما $h^{-۱}h \in H$ پس $h^{-۱}h' \in H \cap K$ و طبق لم ۱۵.۷.۲ باید $h(H \cap K) = h'(H \cap K)$. یعنی f یک‌به‌یک است. پس

$$[G : H \cap K] = |(H/(H \cap K))_l| \leq |(G/K)_l| = [G : K].$$

برای قسمت دوم، فرض کنیم $[G : H \cap K] = [G : K]$. این یعنی f پوشا است. زیرا f یک‌به‌یک و $|(G/K)_l| = [G : K] < \infty$ است. حال فرض کنیم $g \in G$. هم دسته چپ gK را درنظر می‌گیریم. چون f پوشا است، عنصر $h \in H$ چنان وجود دارد که

$$hK = (fh(H \cap K)) = gK.$$

طبق لم ۱۵.۷.۲ داریم $h^{-۱}g \in K$. پس $g = hh^{-۱}g = h(h^{-۱}g) \in HK$ و لذا $G \subseteq HK$.
واضح است که $HK \subseteq G$. پس $G = HK$ و طبق گزاره ۲۹.۴.۲ باید $G = KH$.
اکنون فرض کنیم $G = KH$. طبق گزاره ۲۹.۴.۲ باید $G = HK$. هم دسته چپ gK را در نظر می‌گیریم. پس $g = hk$ که $h \in H$ و $k \in K$. حال داریم

$$f(h(H \cap K)) = hK = hkk^{-۱}K = (hk)k^{-۱}K = hkK = gK$$

یعنی f پوشا است و اثبات کامل است. $\square$

قضیه ۳۹.۷.۲. (قضیه پوانکاره) *فرض کنیم H و K زیرگروه‌های با اندیس متناهی در گروه G باشند. در این صورت داریم که $[G : H \cap K] < \infty$ و*

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

همچنین در بالا تساوی رخ می‌دهد اگر و تنها اگر $G = KH$.

اثبات. می‌دانیم که $(H \cap K) \leq H \leq G$. طبق قضیه ۳۶.۷.۲ و طبق قضیه ۳۸.۷.۲ داریم که

$$[G : (H \cap K)] = [G : H]\,[H : (H \cap K)] \leq [G : H]\,[G : K] < \infty.$$

برای قسمت دوم، طبق قضیه ۳۸.۷.۲ در بالا (آخرین کوچکتر یا مساوی منظور ما است) تساوی رخ می‌دهد اگر و تنها اگر $[H : (H \cap K)] = [G : K]$ اگر و تنها اگر $G = HK$. □

تمرین‌های حل شده

تمرین ۴۰.۷.۲. *برای زیرگروه $H = \{۱, -۱, j, -j\}$ از گروه $\mathbb{Q}_۸$ هم دسته‌های چپ را بنویسید.*

حل. یکی از هم دسته‌ها خود H است. حال داریم

$$\begin{aligned} iH &= \{i, -i, ij, i(-j)\} = \{i, -i, k, -k\} = (-i)H \\ jH &= \{j, -j, j^۲, -j^۲\} = \{j, -j, -۱, ۱\} = H = (-j)H \\ kH &= \{k, -k, kj, k(-j)\} = \{k, -k, -i, i\} = (-k)H \end{aligned}$$

پس دو هم دسته چپ داریم یکی H و دیگری $\{i, -i, k, -k\}$.

تمرین ۴۱.۷.۲. *فرض کنیم $G = (\mathbb{R}, +)$ باشد. برای گروه $G \times G$ و زیرگروه*

$$H = \{(x, ۰) \in G \times G \mid \ x \in \mathbb{R}\}$$

هم دسته‌های چپ را معلوم کنید ($G \times G$ همان صفحه مختصات است و H محور xها).

حل. برای عنصر دلخواه ولی ثابت $(u, v) \in G \times G$، چون گروه جمعی است داریم

$$\begin{aligned} &(u, v) + H = \{(u, v) + (x, ۰) \mid \ (x, ۰) \in H\} = \\ &\{(u + x, v) \mid \ x, u, v \in \mathbb{R}\} \end{aligned}$$

و این یعنی همه نقاط در صفحه مختصات که همواره عرض v دارند. یعنی خطوط موازی محور xها! پس بیشمار هم دسته چپ داریم.

تمرین ۴۲.۷.۲. *برای گروه $G = (\mathbb{R}, +)$ و زیرگروه $\mathbb{Z}$ هم دسته‌های چپ را معلوم کنید.*

حل. هر عدد حقیقی r به صورت $n+\epsilon$ است که n عدد صحیح و $0 \leq \epsilon < 1$. چون گروه جمعی است داریم

$$\begin{aligned}&r+\mathbb{Z}=\{r+x \mid \ x\in\mathbb{Z}\}=\{n+\epsilon+x \mid \ x\in\mathbb{Z}\}=\\&\{m+\epsilon \mid \ m\in\mathbb{Z}\}=\end{aligned}$$

و این یعنی هم دسته‌های چپ به صورت $\mathbb{Z}+\epsilon$ هستند که $0 \leq \epsilon < 1$. پس بیشمار هم دسته چپ داریم.

تمرین ۴۳.۷.۲. *فرض کنیم G یک گروه دوری باشد و H یک زیرگروه مخالف با $\{e\}$. نشان دهید $[G:H]$ متناهی است.*

حل. فرض کنیم $G=<x>$. طبق قضیه ۲۲.۵.۲ داریم $H=<x^k>$ که $k\in\mathbb{N}$ (چرا؟). حال برای عنصر دلخواه و ثابت $x^i\in G$ داریم

$$\begin{aligned}&x^iH=\{x^ih \mid h\in H\}=\{x^i(x^k)^j \mid j\in\mathbb{Z}\}=\\&\{x^ix^{jk} \mid j\in\mathbb{Z}\}=\{x^{i+jk} \mid j\in\mathbb{Z}\}.\end{aligned}$$

برای این که هم دسته چپ تکراری حاصل نشود باید i از مجموعه $\{0,1,2,\dots,k-1\}$ انتخاب شود. یعنی $[G:H]=k$.

تمرین ۴۴.۷.۲. *فرض کنیم G یک گروه و $H\leq G$. در این صورت $G\setminus H$ متناهی است اگر و تنها اگر $G=H$ یا G متناهی باشد.*

حل. فرض کنیم $G\setminus H$ متناهی است و $G\neq H$. نشان می‌دهیم G متناهی است. طبق قضیه ۸.۷.۲ هم دسته‌های چپ گروه G را افراز می‌کنند. یکی از این هم دسته‌های چپ خود H است. پس می‌توانیم بنویسیم

$$G=H\cup(\bigcup_{e\neq a\in G} aH)$$

که در آن $\bigcup_{e\neq a\in G} aH$ حتما ناتهی است، زیرا $G\neq H$. به روشنی $\bigcup_{e\neq a\in G} aH\subseteq(G\setminus H)$. یعنی $\bigcup_{e\neq a\in G} aH$ متناهی است. این نشان می‌دهد که H نیز باید متناهی باشد. زیرا اگر H نامتناهی باشد آنگاه در H نامتناهی عنصر متمایز مانند h_1، h_2، h_3 و ... وجود دارد. چون $\bigcup_{e\neq a\in G} aH$ متناهی است، پس aH متناهی است و لذا باید $ah_i=ah_j$. این نشان می‌دهد که $h_i=h_j$ (چگونه؟) که تناقض آشکار است. حال H متناهی و $\bigcup_{e\neq a\in G} aH$ متناهی پس باید G متناهی باشد.
برعکس، بسیار بدیهی است.

تمرین ۴۵.۷.۲. *برای اعداد اول p و q نشان دهید که هر زیرگروه سره از یک گروه pq عضوی دوری است.*

حل. برای زیرگروه سره که فقط شامل عنصر خنثی است، چیزی برای اثبات نداریم. فرض کنیم H یک زیرگروه سره نابدیهی از G باشد. طبق قضیه لاگرانژ، قضیه ۲۳.۷.۲، باید $|H| \mid pq$. پس $|H|$ برابر با p و یا q است. در هر صورت طبق نتیجه ۲۵.۷.۲ کار تمام است.

تمرین ۴۶.۷.۲. *فرض کنیم G گروهی از مرتبه عدد اول باشد. نشان دهید G زیرگروه سره نابدیهی ندارد.*

حل. فرض کنیم H زیرگروه سره نابدیهی از G باشد. طبق قضیه لاگرانژ، قضیه ۲۳.۷.۲، $|H|$ باید مرتبه گروه را بشمارد. اما این یعنی عدد اول شمارنده غیر ۱ و خودش دارد که تناقض آشکار است.

تمرین ۴۷.۷.۲. *فرض کنیم G گروهی متناهی و $d(G)$ کمترین تعداد اعضای از G باشد که G را تولید می‌کند. نشان دهید که $|G|\geq ۲^{d(G)}$.*

حل. برای راحتی فرض می‌کنیم $d(G)=k$. همچنین فرض کنیم $G=< g_۱,g_۲,...,g_k >$. قرار می‌دهیم $H=< g_۱,...,g_{k-۱} >$. ادعا می‌کنیم $d(H)=k-۱$. فرض کنیم $d(H)=t<k-۱$. پس $H=< h_۱,...,h_t >$ و لذا با یک بررسی داریم

$$G=< g_۱,...,g_k >=< H,g_k >=<< h_۱,...,h_t >,g_k >=< h_۱,...,h_t,g_k > .$$

این یعنی G با تعداد کمتر از k عنصر تولید می‌شود که در تناقض با انتخاب ما از k است. پس $d(H)=k-۱$. حال حکم را با اسقرا اثبات می‌کنیم. اگر $k=۰$ آنگاه $G=<\emptyset>=\{e\}$ و به وضوح حکم برقرار است. حال فرض کنیم حکم برای هر گروه H' که $d(H')<k$ درست باشد، یعنی $|H'|\geq ۲^{d(H')}$. چون $d(H)<k$ داریم $|H|\geq ۲^{k-۱}$. اما طبق قضیه لاگرانژ، قضیه ۲۳.۷.۲، داریم $|G|=l\,|H|$ که $l\in\mathbb{N}$. اگر $l=۱$ باشد آنگاه $G=H$ و این یعنی G با تعداد کمتر از k عنصر تولید می‌شود که در تناقض با انتخاب ما از k است. پس $l\geq ۲$. لذا داریم

$$|G|=l\,|H|\geq ۲\;۲^{k-۱}=۲^k.$$

تمرین ۴۸.۷.۲. *فرض کنیم G یک گروه متناهی باشد و $H,K\leq G$. قرار دهید $[G:H]=m$ و $[G:K]=n$. نشان دهید $c\leq[G:(H\cap K)]\leq mn$ که در آن c کوچکترین مضرب مشترک m و n است. در نتیجه اگر m و n نسبت به هم اول باشند تساوی رخ می‌دهد.*

حل. می‌دانیم که $(H\cap K)\leq H\leq G$ و $(H\cap K)\leq K\leq G$. پس طبق قضیه ۳۶.۷.۲ داریم

$$\begin{aligned}[G:(H\cap K)]&=[G:H]\,[H:(H\cap K)]=m[H:(H\cap K)]\\ [G:(H\cap K)]&=[G:K]\,[K:(H\cap K)]=n[K:(H\cap K)].\end{aligned}$$

پس $m|[G:(H\cap K)]$ و $n|[G:(H\cap K)]$ و لذا $c|[G:(H\cap K)]$. اما طبق قضیه پوانکاره، قضیه ۳۹.۷.۲، داریم

$$[G:(H\cap K)]\leq[G:H]\,[G:K]=mn.$$

برای قسمت دوم، چون $c=mn$ است چیزی برای اثبات نداریم.

تمرین ۴۹.۷.۲. *فرض کنیم H و K زیرگروه‌هایی از گروه متناهی G باشند به طوری که داشته باشیم $([G:H],[G:K])=۱$. نشان دهید که $G=HK$ و در نتیجه $HK=KH$.*

حل. طبق نتیجه ۲.۷.۲۶ داریم $H \cap K = \{e\}$. پس طبق تمرین قبلی داریم

$$|G| = [G : \{e\}] = [G : (H \cap K)] = [G : H]\,[G : K].$$

اما طبق قضیه لاگرانژ، قضیه ۲.۷.۲۳ داریم $|G| = |H|\,[G : H]$ و $|G| = |K|\,[G : K]$. این ایجاب می‌کند که $|G| = |K|\,|H| = [G : H][G : K]$. اکنون طبق قضیه ۲.۴.۳۱ باید $|G| = |K|\,|H| = |HK|$. چون $G \subseteq HK$ نتیجه می‌شود که $G = HK$. قسمت دوم نتیجه بدیهی از گزاره ۲.۴.۲۹ است.

۸.۲ زیرگروه‌های نرمال و گروه خارج قسمتی

برای شناخت بهتر گروه‌ها نیاز به ابزاری جدید داریم. لازم نیست همه زیرگروه‌ها را زیر ذره‌بین قرار دهیم. این بخش زیرگروه جدیدی را معرفی می‌کنیم.

تعریف ۱.۸.۲. *فرض کنیم G یک گروه باشد و $N \leq G$. گوییم زیرگروه N در G نرمال است هرگاه برای هر $x \in G$ و هر $n \in N$ داشته باشیم $xnx^{-1} \in N$. این مطلب معادل است با این که $xNx^{-1} \subseteq N$. زیرگروه نرمال را با $N \trianglelefteq G$ نشان می‌دهیم.*

مثال ۲.۸.۲. *برای هر گروه G واضح است که $G \trianglelefteq G$ و $\{e\} \trianglelefteq G$.*

مثال ۳.۸.۲. چون برای گروه G، $Z(G)$ آبلی است، نتیجه می‌شود که برای هر $x \in G$ داریم $Z(G) = xZ(G)x^{-1} \trianglelefteq G$.

مثال ۴.۸.۲. *هر زیرگروه از یک گروه آبلی یک زیرگروه نرمال است.*

مثال ۵.۸.۲. *یک بررسی ساده نشان می‌دهد که*

$$H = \{\begin{pmatrix} a & b \\ ۰ & c \end{pmatrix} \mid a, b, c \in \mathbb{R}, \ \ a \neq ۰, \ c \neq ۰\}$$

یک زیرگروه از $GL_۲(\mathbb{R})$ است. اما این زیرگروه نرمال نیست. زیرا برای

$$\begin{pmatrix} ۰ & ۱ \\ ۱ & ۰ \end{pmatrix} \in GL_۲(\mathbb{R}) \qquad\qquad \begin{pmatrix} ۱ & ۱ \\ ۰ & ۱ \end{pmatrix} \in H$$

داریم

$$\begin{pmatrix} ۰ & ۱ \\ ۱ & ۰ \end{pmatrix} \begin{pmatrix} ۱ & ۱ \\ ۰ & ۱ \end{pmatrix} \begin{pmatrix} ۰ & ۱ \\ ۱ & ۰ \end{pmatrix}^{-۱} = \begin{pmatrix} ۱ & ۰ \\ ۱ & ۰ \end{pmatrix} \notin H.$$

مثال ۶.۸.۲. *برای هر گروه G زیرگروه*

$$N =< \{x^۲ \mid x \in G\} >$$

نرمال است. فرض کنیم $y \in N$. طبق قضیه ۵.۵.۲ داریم

$$y = (x_۱^۲)^{\epsilon_۱} (x_۲^۲)^{\epsilon_۲} \ldots (x_k^۲)^{\epsilon_k} = (x_۱^{\epsilon_۱})^۲ (x_۲^{\epsilon_۲})^۲ \ldots (x_k^{\epsilon_k})^۲.$$

اکنون برای هر $g \in G$ با کمک تمرین ۶۲.۲.۲ داریم

$$\begin{aligned} gyg^{-۱} &= g(x_۱^{\epsilon_۱})^۲ (x_۲^{\epsilon_۲})^۲ \ldots (x_k^{\epsilon_k})^۲ g^{-۱} = \\ & g(x_۱^{\epsilon_۱})^۲ g^{-۱} \ g(x_۲^{\epsilon_۲})^۲ g^{-۱} \ g \ldots g^{-۱} \ g(x_k^{\epsilon_k})^۲ g^{-۱} = \\ & (gx_۱^{\epsilon_۱} g^{-۱})^۲ \ (gx_۲^{\epsilon_۲} g^{-۱})^۲ \ g \ldots g^{-۱} \ (gx_k^{\epsilon_k} g^{-۱})^۲ \end{aligned}$$

عبارات داخل پرانتز عضوی از N هستند (چرا؟). پس $gyg^{-۱}$ عنصر N است. لذا باید N نرمال باشد.

مثال ۷.۸.۲. *طبق نمادهای مثال ۷.۳.۲، زیرگروه* $N=<\sigma_6>=\{\sigma_1,\sigma_6\}$ *از* S_3 *نرمال نیست. زیرا* $\sigma_2\sigma_6\sigma_2^{-1}\notin N$.

گزاره زیر در برخی موارد بسیار راه گشا است. ساختن مثال از زیرگروه نرمال را نیز ساده می‌کند.

گزاره ۸.۸.۲. *فرض کنیم* G *یک گروه باشد،* $N\leq G$ *و* $[G:N]=2$. *در این صورت* $N\trianglelefteq G$.

اثبات. اگر $g\in N$ آنگاه واضح است که $gNg^{-1}\subseteq N$. پس فرض کنیم $g\notin N$. پس باید $gN\neq N$ و $Ng\neq N$. زیرا اگر مثلاً $Ng=N$ آنگاه $ng=n'$ که $n,n'\in N$. پس $g=n^{-1}n'\in N$ و این تناقض است. حال هم دسته چپ gN و هم دسته راست Ng طبق قضیه ۸.۷.۲ و قضیه ۱۱.۷.۲ با کمک N، G را افراز می‌کنند، یعنی $N\cup gN=G=N\cup Ng$، زیرا $[G:N]=2$. حال $gN\cap N=\emptyset$ و $Ng\cap N=\emptyset$، پس باید $gN=Ng$. باضرب طرفین در g^{-1} از سمت چپ داریم $gNg^{-1}=N$. بنابراین N نرمال است. $\square$

مثال ۹.۸.۲. *در گروه غیر آبلی* $\mathbb{Q}_8$ *زیرگروه* $N=\{1,-1,i,-i\}$ *نرمال است. زیرا طبق قضیه لاگرانژ، قضیه ۲۳.۷.۲، داریم* $[G:N]=\frac{|G|}{|N|}=2$. *پس طبق گزاره ۸.۸.۲ باید* N *نرمال باشد (چه زیرگروه‌های نرمال دیگری از* $\mathbb{Q}_8$ *می‌شناسید؟).*

به آسانی مشاهده می‌شود که اگر $G\leq H\leq K$ آنگاه $G\leq K$. اما در زیرگروه نرمال این خاصیت برقرار نیست. مثال زیر را ببینید.

مثال ۱۰.۸.۲. *فرض کنیم* $G=D_4$. *طبق تمرین ۳۲.۶.۲ قرار می‌دهیم*

$$N=\{e,\tau\},\quad N'=\{e,\sigma^2,\tau,\sigma^2\tau\}.$$

به آسانی می‌توان دید که $N\leq N'\leq G$. *اما* $[G:N']=2$ *و* $[N':N]=2$ *(چرا؟) پس از گزاره ۸.۸.۲ داریم* $N\trianglelefteq N'$ *و* $N'\trianglelefteq G$. *این درحالی است که* $N\ntrianglelefteq G$. *زیرا* $\sigma\tau\sigma^{-1}\notin N$.

قضیه زیر را با گزاره ۸.۸.۲ مقایسه کنید.

قضیه ۱۱.۸.۲. *فرض کنیم* G *یک گروه متناهی از مرتبه* k *باشد،* $N\leq G$ *و* $[G:N]=p$ *که در آن* p *کوچکترین عدد اول با شرط* $p\mid k$. *در این صورت* $N\trianglelefteq G$.

اثبات. اول ادعاهای زیر را اثبات می‌کنیم:

ادعا ۱: اگر $x\notin N$ آنگاه برای هر $1\leq m\leq p-1$ داریم $x^m\notin N$.

چون p کوچکترین عدد اول است که k را می‌شمارد، پس برای هر عدد اول q که $q\mid k$ داریم $(m,q)=1$. این ایجاب می‌کند که $(m,k)=1$ (چگونه؟). پس طبق قضیه بزو، قضیه ۱۰.۲.۱، اعداد صحیح r و s وجود دارند که $rk+sm=1$. اکنون به برهان خلف، فرض کنیم $x^m\in N$. پس طبق نتیجه ۲۴.۷.۲ داریم

$$x=x^{rk+sm}=x^{rk}x^{sm}=x^{sm}.$$

سمت چپ تساوی بالا در N قرار دارد و لذا $x \in N$ و این تناقض است و ادعا اثبات می‌شود.
ادعای ۲: اگر $x \notin N$ آنگاه

$$N \cup xN \cup x^{۲}N \cup ... \cup x^{p-۱}N$$

افراز برای G است.
فرض کنیم $x^iN = x^jN$ که $۰ \leq i < j \leq p - ۱$. پس $x^{j-i}N = N$ و لذا باید $x^{j-i} \in N$ (چرا؟). این ادعا ۱ را نقض می‌کند. حال چون $[G : N] = p$ پس

$$N \cup xN \cup x^{۲}N \cup ... \cup x^{p-۱}N$$

افراز برای G است.
فرض کنیم $y \in G$. اگر $y \in N$ آنگاه به وضوح داریم $yNy^{-۱} \subseteq N$. بنابراین فرض کنیم $y \notin N$. اگر $yNy^{-۱} \not\subseteq N$ آنگاه عنصر $n \in N$ چنان وجود دارد که $z = yny^{-۱} \notin N$. در ادعای ۱ و ادعای ۲، قرار می‌دهیم $x = z$. پس

$$N \cup zN \cup z^{۲}N \cup ... \cup z^{p-۱}N$$

یک افراز از G است. از طرفی $y \notin N$ و لذا در ادعای ۱ و ادعای ۲، قرار می‌دهیم $x = y$. پس

$$N \cup yN \cup y^{۲}N \cup ... \cup y^{p-۱}N$$

یک افراز از G است. پس $۰ \leq i \leq p - ۱$ وجود دارد که $yN = z^iN$. طبق تمرین ۵۵.۲.۲ داریم $yN = yn^iy^{-۱}N$ و لذا $N = n^iy^{-۱}N$. در نتیجه باید $n^iy^{-۱} \in N$. چون N زیرگروه و $n \in N$، پس $n^i \in N$ است و $y^{-۱} = n^{-i}n^iy^{-۱} \in N$. اما دوباره N زیرگروه است و لذا $y \in N$ که تناقض آشکار است. بنابراین $yNy^{-۱} \subseteq N$ و N زیرگروه نرمال است. $\square$

گزاره زیر تعریف‌های معادل دیگری از زیرگروه نرمال به دست می‌دهد.

گزاره ۱۲.۸.۲. *فرض کنیم G یک گروه باشد و $N \leq G$. در این صورت شرایط زیر معادل هستند.*
(۱) *N زیرگروه نرمال است.*
(۲) *برای هر $g \in G$ داریم $gNg^{-۱} = N$.*
(۳) *برای هر $g \in G$ داریم $gN = Ng$.*
(۴) *برای هر g و g' در G داریم $(gN)(g'N) = (gg')N$.*

اثبات. (۱) $\Leftarrow$ (۲). می‌دانیم که برای هر $g \in G$، $gNg^{-۱} \subseteq N$. اما برای هر $g \in G$ داریم که $g^{-۱} \in G$ و لذا $g^{-۱}N(g^{-۱})^{-۱} = g^{-۱}Ng \subseteq N$ (چرا؟). حال با ضرب طرفین از سمت چپ در g و از سمت راست در $g^{-۱}$ نتیجه می‌شود که $N \subseteq gNg^{-۱}$. بنابراین حکم حاصل می‌شود.
(۲) $\Leftarrow$ (۳). واضح است (طرفین را در عبارت‌های مناسب ضرب کنید).
(۳) $\Leftarrow$ (۴). با کمک فرض داریم که

$$(gN)(g'N) = gNg'N = (gNg')N = (gg'N)N = gg'NN = gg'N = (gg')N.$$

(۴) $\Leftarrow$ (۱). چون فرض برای هر g و g' برقرار است، قرار می‌دهیم $g' = g^{-1}$. پس

$$(gNg^{-1})N = (gN)(g^{-1}N) = (gg^{-1})N = N.$$

لذا باید $gNg^{-1} \subseteq N$. زیرا در غیر این صورت می‌توانیم فرض کنیم $x \in gNg^{-1} \setminus N$. پس داریم $yn = n'$ که $n, n' \in N$. بنابراین $y = n'n^{-1} \in N$ که تناقض آشکار است. □

اکنون نتایج زیر را داریم.

نتیجه ۱۳.۸.۲. *فرض کنیم G یک گروه باشد و $H \leq G$ و $N \trianglelefteq G$. در این صورت موارد زیر برقرار است.*
(الف) $HN \leq G$.
(ب) $H \cap N \trianglelefteq H$.
(ج) $HN = NH$.
(د) $N \trianglelefteq NH$.

اثبات. (الف) طبق گزاره ۲۹.۴.۲ کافی است نشان دهیم $HN = NH$. فرض کنیم $hn \in HN$. چون N نرمال است پس از گزاره ۱۲.۸.۲ داریم $hN = Nh$ و لذا $hn = n'h \in NH$ که $n' \in N$. بنابراین $HN \subseteq NH$ و به روش مشابه $NH \subseteq HN$. اثبات کامل است.
(ب) زیرگروه بودن $H \cap N$ طبق گزاره ۱۲.۴.۲ به دست می‌آید. حال فرض کنیم $x \in H \cap N$ و $h \in H$. واضح است که $hxh^{-1} \in H$. اما N نرمال است پس $hxh^{-1} \in N$. لذا باید $hxh^{-1} \in H \cap N$ یعنی $H \cap N \trianglelefteq H$.
(ج) تمرین ۳۷.۸.۲ را ببینید.
(د) فرض کنیم $nh \in NH$. چون N نرمال است طبق گزاره ۱۲.۸.۲ داریم $hN = Nh$ و $nN = Nn$. لذا

$$(nh)N = n(hN) = n(Nh) = (nN)h = (Nn)h = N(nh)$$

و طبق گزاره ۱۲.۸.۲ حکم حاصل می‌شود. □

نتیجه ۱۴.۸.۲. *فرض کنیم G یک گروه باشد و $N, N' \trianglelefteq G$. در این صورت NN' نرمال است.*

اثبات. فرض کنیم $g \in G$. طبق قسمت (۳) از گزاره ۱۲.۸.۲ داریم

$$gNN'g^{-1} = NgN'g^{-1} = NN'gg^{-1} = NN'$$

و لذا NN' نرمال است. □

نتیجه ۱۵.۸.۲. فرض کنیم N زیرگروه نرمال گروه G باشد. در این صورت موارد زیر برقرار است.
(الف) همواره داریم $(G/N)_l = (G/N)_r$ (و آن را از این لحظه با G/N نمایش می‌دهیم و به آن مجموعه هم دسته‌ها گوییم).
(ب) مجموعه همه دسته‌های یعنی

$$G/N = \{gN \mid g \in G\} = \{Ng \mid g \in G\}$$

با عمل دوتایی

$$(Ng)(Ng') = N(gg') \qquad (gN)(g'N) = (gg')N$$

یک گروه است.

اثبات. (الف) حالت (۳) گزاره ۱۲.۸.۲ چیزی برای اثبات باقی نمی‌گذارد.
(ب) دقت شود که $(gg')N$ یک هم دسته (چپ) است و اگر $xN = x'N$ و $yN = y'N$ باشد آنگاه

$$(xy)N = (xN)(yN) = (x'N)(y'N) = (x'y')N$$

و این یعنی عمل دوتایی بالا یک تابع است یا به اصطلاح خوشتعریف است. هم دسته چپ $eN = N$ عنصر خنثی است. وارون هم دسته (چپ) gN به صورت $g^{-1}N$ است. شرکت پذیری هم از G ارث می‌رسد. $\square$

تعریف ۱۶.۸.۲. به گروهی که در نتیجه ۱۵.۸.۲ حاصل شد، گروه خارج قسمتی گوییم.

مثال ۱۷.۸.۲. در بخش قبل دیدیم که

$$\mathbb{Z}/۳\mathbb{Z} = \{۳\mathbb{Z}, ۳\mathbb{Z}+۱, ۳\mathbb{Z}+۲\}.$$

$۳\mathbb{Z}+i$ یعنی اعدادی که بر ۳ باقیمانده $۰ \leq i < ۳$ دارند، پس با تعویض نماد $۳\mathbb{Z}+i$ با $\bar{i}$ عملا داریم

$$\mathbb{Z}/۳\mathbb{Z} = \{\bar{۰}, \bar{۱}, \bar{۲}\}.$$

که همان گروه آشنای $(\mathbb{Z}_۳, +)$ است.

مثال ۱۸.۸.۲. یک بررسی ساده نشان می‌دهد که $\mathbb{Z}$ زیرگروه نرمال $\mathbb{Q}$ (با عمل جمع) است. پس می‌توانیم گروه خارج قسمتی $\mathbb{Q}/\mathbb{Z}$ را تشکیل دهیم و

$$G = \mathbb{Q}/\mathbb{Z} = \{\frac{a}{b} + \mathbb{Z} \mid \frac{a}{b} \in \mathbb{Q}\}.$$

برای گروه G عنصر خنثی $\mathbb{Z}$ است! جالب این که مرتبه هر عنصر متناهی است. زیرا

$$b(\frac{a}{b} + \mathbb{Z}) = a + \mathbb{Z} = \mathbb{Z}.$$

اکنون برخی خواص مفید گروه خارج قسمتی را بیان می‌کنیم. قبل از آن باید یک زیرگروه نرمال مهم را معرفی کنیم.

تعریف ۲.۸.۱۹. *فرض کنیم G یک گروه باشد. در این صورت برای هر $a, b \in G$، عنصر $x = aba^{-۱}b^{-۱}$ را یک جابجاگر گوییم. گروه تولید شده توسط جابجاگرهای G را زیرگروه مشتق G نامیم و با G' نمایش می‌دهیم. همچنین به استقرا می‌توانیم تعریف کنیم که $G'' = (G')'$، ...، $G^{(n)} = (G^{(n-۱)})'$ و به آن گروه مشتق مرتبه nام گوییم.*

مثال ۲.۸.۲۰. *اگر G یک گروه آبلی باشد تنها جابجاگر آن e است و لذا $G' = \{e\}$. به همین دلیل انتگرال گروه به معنی ضد گروه مشتق نداریم! چون همه گروه‌های آبلی جواب $\int \{e\}$ هستند!!!*

مثال ۲.۸.۲۱. *اگر $x = aba^{-۱}b^{-۱} \in G$ یک جابجاگر باشد آنگاه طبق تمرین ۲.۲.۵۵ عنصر $x^{-۱}$ نیز یک جابجاگر است.*

مثال ۲.۸.۲۲. *بدون اثبات می‌پذیریم که زیرگروه مشتق گروه $GL_n(\mathbb{R})$ برای $n \geq ۲$ برابر همه ماتریس‌هایی است که دترمینان ۱ دارند.*

مثال ۲.۸.۲۳. *اگر $x = aba^{-۱}b^{-۱} \in G$ یک جابجاگر باشد آنگاه برای هر $y \in G$، $yxy^{-۱}$ نیز جابجاگر است. زیرا داریم*

$$yxy^{-۱} = yaba^{-۱}b^{-۱}y^{-۱} = yay^{-۱}\ yby^{-۱}\ ya^{-۱}y^{-۱}\ yb^{-۱}y^{-۱} = (yay^{-۱})\ (yby^{-۱})\ (ya^{-۱}y^{-۱})\ (yb^{-۱}y^{-۱}) = uvu^{-۱}v^{-۱}.$$

مثال ۲.۸.۲۴. *یک محاسبه سر راست نشان می‌دهد که $\mathbb{Q}'_۸ = \{-۱, ۱\}$ و لذا $\mathbb{Q}''_۸ = \{۱\}$.*

قضیه ۲.۸.۲۵. *فرض کنیم G یک گروه باشد. در این صورت موارد زیر برقرار است.*

(الف) $G' \trianglelefteq G$.

(ب) G/G' آبلی است.

(ج) اگر $N \trianglelefteq G$ آنگاه G/N آبلی است اگر و تنها اگر $G' \subseteq N$.

اثبات. (الف) زیرگروه بودن G' از تعریف واضح است. حال فرض کنیم $x \in G'$. پس طبق گزاره ۲.۵.۵ داریم

$$x = (a_۱b_۱a_۱^{-۱}b_۱^{-۱})^{\epsilon_۱}(a_۲b_۲a_۲^{-۱}b_۲^{-۱})^{\epsilon_۲}...(a_kb_ka_k^{-۱}b_k^{-۱})^{\epsilon_k} \qquad \epsilon_i \in \{-۱, ۱\}$$

در ابتدا دقت شود که اگر $\epsilon_i = -۱$ آنگاه طبق تمرین ۲.۲.۵۵ و تمرین ۲.۲.۵۶، $(a_ib_ia_i^{-۱}b_i^{-۱})^{-۱}$ باز هم جابجاگر است. اکنون برای هر $g \in G$ داریم

$$gxg^{-۱} = g[(a_۱b_۱a_۱^{-۱}b_۱^{-۱})^{\epsilon_۱}(a_۲b_۲a_۲^{-۱}b_۲^{-۱})^{\epsilon_۲}...(a_kb_ka_k^{-۱}b_k^{-۱})^{\epsilon_k}]g^{-۱} = g(a_۱b_۱a_۱^{-۱}b_۱^{-۱})^{\epsilon_۱}g^{-۱}\ \ g(a_۲b_۲a_۲^{-۱}b_۲^{-۱})^{\epsilon_۲}g^{-۱}\ \ ...\ g(a_kb_ka_k^{-۱}b_k^{-۱})^{\epsilon_k}g^{-۱} = gx_۱^{\epsilon_۱}g^{-۱}\ \ gx_۲^{\epsilon_۲}g^{-۱}\ \ ...\ gx_k^{\epsilon_k}g^{-۱}$$

اما طبق مثال بالا هر کدام از $gx_i^{\epsilon_i}g^{-1}$ جابجاگر هستند و لذا چون G' زیرگروه است خواهیم داشت $gxg^{-1} \in G'$ و (الف) اثبات می‌شود.
(ب) طبق تعریف گروه خارج قسمتی، می‌دانیم اعضای G/G' به شکل aG' هستند. حال فرض کنیم $a, b \in G$. می‌دانیم که جابجاگر $b^{-1}a^{-1}ba$ در G' قرار دارد. پس $b^{-1}a^{-1}baG' = G'$ و لذا با ضرب‌های مناسب از سمت چپ داریم $abG' = baG$. بنابراین $aG'bG' = bG'aG'$ و (ب) اثبات می‌شود.
(ج) ($\Rightarrow$) فرض کنیم $a, b \in G$. واضح است که $b^{-1}a^{-1}ba \in G'$ و لذا طبق فرض داریم $b^{-1}a^{-1}ba \in N$. از این رو $b^{-1}a^{-1}baN = N$ و در نتیجه با ضرب‌های مناسب از سمت چپ داریم $abN = baN$. بنابراین $aNbN = bNaN$.
($\Leftarrow$) فرض کنیم aN و bN دلخواه باشند. طبق فرض داریم $aNbN = bNaN$ یا معادلا هم $abN = baN$. با ضرب‌ای مناسب داریم $b^{-1}a^{-1}baN = N$. چون $e \in N$ پس $b^{-1}a^{-1}ba \in N$. یعنی تمام جابجاگرها در N قرار دارند. اما G' کوچکترین زیرگروه شامل همه جابجاگرها است (چرا؟) و لذا باید $G' \subseteq N$. $\square$

اکنون قضیه مهم زیر را داریم.

قضیه ۲.۸.۲۶. *اگر G یک گروه و $G/Z(G)$ دوری باشد آنگاه G آبلی است.*

اثبات. یادآوری می‌کنیم که $Z(G)$ زیرگروه نرمال است و لذا گروه خارج قسمتی $G/Z(G)$ با معنی است. فرض کنیم $x, y \in G$. از فرض عنصر $a \in G$ وجود دارد که $G/Z(G) =< aZ(G) >$. لذا چون $xZ(G), yZ(G) \in G/Z(G)$ داریم $xZ(G) = a^m Z(G)$ و $yZ(G) = a^n Z(G)$ که در آن m و n اعداد صحیح هستند. اما $e \in Z(G)$ و در نتیجه $x = a^m z$ و $y = a^n z'$ که $z, z' \in Z(G)$. بنابراین

$$xy = a^m z a^n z' = a^m a^n z z' = a^{m+n} z z' = a^n a^m z' z = a^n z' a^m z = yx$$

و اثبات کامل است. $\square$

مثال ۲.۸.۲۷. *هیچ گروه G وجود ندارد که $|G/Z(G)| = p$ که p عددی اول است. زیرا طبق نتیجه ۲.۷.۲۵، $G/Z(G)$ دوری است و لذا طبق قضیه ۲.۸.۲۶ باید G آبلی باشد یعنی $G = Z(G)$ و در نتیجه $|G/Z(G)| = ۱$ که تناقض آشکار است!*

تذکر ۲.۸.۲۸. *ممکن است وسوسه شوید و بخواهید شرط دوری در قضیه ۲.۸.۲۶ را با آبلی جایگزین کنید! این وسوسه شدن طبیعی است زیرا طبق گزاره ۲.۵.۱۴ هر گروه دوری آبلی است. اما این وسوسه شیطانی است و نتیجه صحیح ندارد! می‌دانیم که $\mathbb{Q}_8$ یک گروه غیرآبلی است و همچنین $Z(\mathbb{Q}_8) = \{-1, 1\}$. اما گروه $\mathbb{Q}_8/Z(\mathbb{Q}_8)$ چهار عضوی است و لذا آبلی است (تمرین ۲.۲.۶۳ را ببینید).*

بخش را با چند مطلب دیگر به پایان می‌رسانیم.

تعریف ۲.۸.۲۹. *فرض کنیم G یک گروه باشد و $\emptyset = S \subseteq G$. نرمال ساز S در G به صورت زیر تعریف می‌شود*
$$N_G(S) = \{x \in G \mid xSx^{-1} = S\}.$$
اگر $S = \{g\}$ آنگاه $N_G(S)$ را با $N_G(g)$ نمایش می‌دهیم. اگر بیم ابهام نباشد از نمادهای $N(G)$ و $N(g)$ نیز استفاده می‌کنیم.

مثال ۲.۸.۳۰. *برای هر عنصر a از گروه G داریم $N_G(a) = C_G(a)$. اما در حالت کلی داریم $C_G(S) \subseteq N_G(S)$ (برای مثال، با نمادهای مثال ۲.۳.۷ قرار دهید $S = \{\sigma_1, \sigma_2, \sigma_3\}$ و داریم $C_{S_3}(S) \subsetneq N_{S_3}(S) = S_3$).*

مثال ۲.۸.۳۱. *اگر H یک زیرگروه نرمال از گروه G باشد آنگاه واضح است که $N_G(H) = G$.*

قبل از دیدن یک مثال مهم، گزاره زیر را داریم.

گزاره ۲.۸.۳۲. *برای هر گروه G همواره داریم $N_G(S) \leq G$. همچنین اگر $S \leq G$ آنگاه (نسبت به رابطه شمول) $N_G(S)$ بزرگترین زیرگروه G است که $S \trianglelefteq N_G(S)$.*

اثبات. واضح است که $e \in N_G(S)$ و لذا $N_G(S)$ تهی نیست. حال فرض کنیم $x, y \in N_G(S)$. پس $ySy^{-1} = S$ و در نتیجه $S = y^{-1}Sy$. حال داریم
$$(xy^{-1})S((xy^{-1})^{-1}) = (xy^{-1})S(yx^{-1}) = x(y^{-1}Sy)x^{-1} = xSx^{-1} = S.$$
لذا باید $xy^{-1} \in N_G(S)$. پس طبق قضیه ۲.۴.۵ حکم به دست می‌آید.
برای قسمت دوم، از تعریف و گزاره ۲.۸.۱۲ به روشنی دیده می‌شود که $S \trianglelefteq N_G(S)$. حال فرض کنیم $S \trianglelefteq H$. نشان می‌دهیم که $H \subseteq N_G(S)$. فرض کنیم $h \in H$. چون $S \trianglelefteq H$، طبق گزاره ۲.۸.۱۲ داریم $hSh^{-1} = S$. در نتیجه $h \in N_G(S)$ و این یعنی $H \subseteq N_G(S)$. □

مثال زیر نشان می‌دهد که $N_G(S)$ لزوما زیرگروه نرمال نیست.

مثال ۲.۸.۳۳. *گروه D_8 را در نظر می‌گیریم. طبق تمرین ۲.۶.۳۲ داریم*
$$D_8 = \{e, \sigma, \sigma^2, ..., \sigma^7, \tau, \sigma\tau, \sigma^2\tau, ..., \sigma^7\tau\}.$$
قرار می‌دهیم $S =< \tau >= \{e, \tau\}$. با کار حوصله سر بر داریم
$$N_{D_8}(S) = \{e, \tau, \sigma^4, \sigma^4\tau\}.$$
جالب این که
$$N_{D_8}(N_{D_8}(S)) = \{e, \tau, \sigma^2, \sigma^4, \sigma^6, \sigma^2\tau, \sigma^4\tau, \sigma^6\tau\} \neq D_n.$$
بنابراین از مثال قبل، $N_{D_8}(S)$ زیرگروه نرمال نیست. جالبتر این که
$$N_{D_8}(N_{D_8}(N_{D_8}(S))) = D_8.$$

گزاره ۳۴.۸.۲. *برای هر گروه G و زیرگروه H داریم* $C_G(H) \trianglelefteq N_G(H)$.

اثبات. یک بررسی ساده نشان می‌دهد که $C_G(H) \leq N_G(H)$. حال فرض کنیم $x \in C_G(H)$ و $y \in N_G(H)$. همچنین عنصر دلخواه $h \in H$ را در نظر بگیرید. چون H در $N_G(H)$ نرمال است، عنصر $h' \in H$ وجود دارد که $hy = yh'$. اما طبق تعریف $h'x = xh'$ و لذا

$$hyxy^{-۱} = yh'xy^{-۱} = yxh'y^{-۱} = yx(yh'^{-۱})^{-۱} = yx(h^{-۱}y)^{-۱} = yxy^{-۱}h.$$

بنابراین $yxy^{-۱} \in C_G(H)$ و حکم به دست می‌آید. $\square$

تمرین‌های حل شده

تمرین ۳۵.۸.۲. *برای هر گروه G زیرگروه*

$$N =< \{x^k \mid x \in G\} >$$

نرمال است که $k \in \mathbb{Z}$.

حل. فرض کنیم $y \in N$. طبق قضیه ۵.۵.۲ داریم

$$y = (x_۱^k)^{\epsilon_۱}(x_۲^k)^{\epsilon_۲} \dots (x_t^k)^{\epsilon_t} = (x_۱^{\epsilon_۱})^k(x_۲^{\epsilon_۲})^k \dots (x_t^{\epsilon_t})^k.$$

اکنون برای هر $g \in G$ با کمک تمرین ۶۲.۲.۲ داریم

$$\begin{aligned}&gyg^{-۱} = g(x_۱^{\epsilon_۱})^k(x_۲^{\epsilon_۲})^k \dots (x_t^{\epsilon_t})^k g^{-۱} =\\ &g(x_۱^{\epsilon_۱})^k g^{-۱}\ g(x_۲^{\epsilon_۲})^k g^{-۱}\ g \dots g^{-۱}\ g(x_t^{\epsilon_t})^k g^{-۱} =\\ &(gx_۱^{\epsilon_۱}g^{-۱})^k\ (gx_۲^{\epsilon_۲}g^{-۱})^k\ g \dots g^{-۱}\ (gx_t^{\epsilon_t}g^{-۱})^k\end{aligned}$$

عبارات داخل پرانتز عضوی از N هستند (چرا؟). پس $gyg^{-۱}$ عنصر N است. لذا باید N نرمال باشد.

تمرین ۳۶.۸.۲. *فرض کنیم G یک گروه باشد و* $N, N' \trianglelefteq G$. *اگر* $N \cap N' = \{e\}$ *آنگاه نشان دهید که برای هر $a \in N$ و هر $b \in N'$ داریم* $ab = ba$.

حل. چون N زیرگروه است پس $a^{-۱} \in N$. چون N نرمال است پس $ba^{-۱}b^{-۱} \in N$. دوباره چون N زیرگروه است پس $aba^{-۱}b^{-۱} \in N$. از سوی دیگر چون N' نرمال است پس $aba^{-۱} \in N'$. چون N زیرگروه است پس $b^{-۱} \in N'$ و لذا $aba^{-۱}b^{-۱} \in N'$. بنابراین $aba^{-۱}b^{-۱} \in N \cap N' = \{e\}$. یعنی $aba^{-۱}b^{-۱} = e$ و در نتیجه با ضرب‌های مناسب داریم $ab = ba$.

تمرین ۳۷.۸.۲. *اگر N زیرگروه نرمال از گروه G باشد آنگاه نشان دهید که برای هر زیرگروه H داریم* $NH = HN$.

حل. فرض کنیم $hn \in HN$. چون N نرمال است پس طبق گزاره ۱۲.۸.۲ داریم $nH = Hn$. اما $hn \in Hn = nH$ و در نتیجه $hn = nh'$ که $h' \in H$. این نشان می‌دهد که $hn \in NH$. یعنی $HN \subseteq NH$. به روش مشابه داریم $HN \subseteq NH$ و لذا $HN = NH$.

تمرین ۳۸.۸.۲. *فرض کنیم N زیرگروه نرمال از گروه متناهی G باشد و $(|N|, [G:N]) = ۱$. نشان دهید که برای هر $x \in G$ که $o(x) \mid |N|$ داریم $x \in N$.*

حل. فرض کنیم $x \in G$ که $o(x) \mid |N|$ و همچنین برای راحتی فرض کنیم که $[G:N] = n$ و $|N| = m$. طبق قضیه بزو، قضیه ۱۰.۲.۱ داریم $rm + sn = ۱$ که $r, s \in \mathbb{Z}$. چون مرتبه گروه G/N برابر با n است، لذا از نتیجه ۲۴.۷.۲ داریم $(xN)^n = N$. همچنین طبق فرض $m = to(x)$ پس $x^m = e$. اکنون داریم

$$xN = (xN)^۱ = (xN)^{rm+sn} = (xN)^{rm}(xN)^{sn} = (x^mN)^r((xN)^n)^s = NN = N$$

و چون $e \in N$ پس باید $x \in N$.

تمرین ۳۹.۸.۲. *برای گروه G که فقط یک زیرگروه مرتبه متناهی N دارد، نشان دهید که N نرمال است.*

حل. فرض کنیم $x \in G$. طبق تمرین ۳۵.۴.۲ داریم که $xNx^{-۱}$ زیرگروه G است و همچنین $|N| = |xNx^{-۱}|$. لذا از فرض باید $N = xNx^{-۱}$ و از قضیه ۱۲.۸.۲، N است

تمرین ۴۰.۸.۲. *فرض کنیم G گروهی باشد که اجتماع زیرگروه‌های نرمال سره متمایز خود باشد. نشان دهید که G آبلی است.*

حل. فرض کنیم $G = N_۱ \cup \ldots \cup N_k$ که $N_i \trianglelefteq G$ و $N_i \cap N_j = \{e\}$. همچنین $x, y \in G$. اگر $x \in N_i$ و $y \in N_j$ که $i \neq j$ آنگاه طبق تمرین ۳۶.۸.۲ چون $N_i \cap N_j = \{e\}$ داریم $xy = yx$. پس فرض کنیم $x, y \in N_i$. چون N_i سره است و $G = N_۱ \cup \ldots \cup N_k$، حتما اندیس $i \neq j$ وجود دارد که $N_j \neq \{e\}$. فرض کنیم $e \neq z \in N_j$. حال $xz \notin N_i$. زیرا اگر $xz \in N_i$ آنگاه چون N_i زیرگروه است پس $z = x^{-۱}xz \in N_i$ و این یعنی $z \in N_i \cap N_j$ که تناقض است. بنابراین طبق حالت قبل باید $zy = yz$ همچنین $y(xz) = (xz)y$. بنابراین داریم

$$yxz = y(xz) = (xz)y = xzy = xyz.$$

با یک ضرب مناسب داریم $xy = yx$ و این یعنی G آبلی است.

تمرین ۴۱.۸.۲. *نشان دهید که گروه خارج قسمتی یک گروه دوری، دوری است.*

حل. فرض کنیم $G =< a >$. حال فرض کنیم N یک زیرگروه نرمال دلخواه باشد. ادعا می‌کنیم که $G/N =< aN >$. واضح است که $< aN > \subseteq G/N$. فرض کنیم $xN \in G/N$ که $x \in G$. بنابراین $x = a^m$ که $m \in \mathbb{Z}$. پس داریم

$$xN = a^mN = \underbrace{aN\, aN \ldots aN}_{m\text{تا}} = (aN)^m.$$

پس $xN \in < aN >$ و در نتیجه $G/N =< aN >$.

تمرین ۴۲.۸.۲. *فرض کنیم G یک گروه و $N \leq H \leq G$. نشان دهید که $H \trianglelefteq G$ اگر و تنها اگر H/N زیرگروه نرمال G/N باشد.*

حل. فرض کنیم $H \trianglelefteq G$ و $h'N, hN \in H/N$. داریم $h'Nh^{-۱}N = h'h^{-۱}N$ و لذا چون H زیرگروه است باید $h'h^{-۱} \in H$ و طبق قضیه ۵.۴.۲ باید H/N زیرگروه G/N باشد. دقت شود که $eN = N \in H/N$ و ناتهی بودن H/N بدیهی است. حال فرض کنیم $gN \in G/N$. چون H در G نرمال است داریم $ghg^{-۱} \in H$. در نتیجه

$$(gN)(hN)(gN)^{-۱} = (gN)(hN)(g^{-۱}N) = (ghg^{-۱})N \in H/N$$

و بنابراین H/N در G/N نرمال است.
برعکس، فرض کنیم H/N در G/N نرمال است و $h \in H$. برای هر $g \in G$، طبق فرض داریم

$$(gN)(hN)(gN)^{-۱} = (gN)(hN)(g^{-۱}N) = (ghg^{-۱})N \in H/N$$

و بنابراین $ghg^{-۱} \in H$ درنتیجه H در G نرمال است.

تمرین ۴۳.۸.۲. *اگر N زیرگروه نرمالی از گروه G باشد که $N \cap G' = \{e\}$ آنگاه ثابت کنید که $N \subseteq Z(G)$. سپس نتیجه بگیرید $Z(G/N) = Z(G)/N$.*

حل. فرض کنیم $x \in N$. برای هر $y \in G$ داریم $xyx^{-۱}y^{-۱} \in G'$. چون N زیرگروه است پس $x^{-۱} \in N$. از طرفی N نرمال است پس $yx^{-۱}y^{-۱} \in N$. دوباره چون N زیرگروه است داریم $xyx^{-۱}y^{-۱} \in N$. طبق فرض باید $xyx^{-۱}y^{-۱} = e$ و باضرب‌های مناسب داریم $xy = yx$. در نتیجه $x \in Z(G)$ و کار قسمت اول تمام است.
قسمت دوم، فرض کنیم $z \in Z(G)$. پس برای هر $g \in G$ داریم

$$gNzN = gzN = zgN = zNgN$$

و لذا $Z(G)/N \subseteq Z(G/N)$. حال فرض کنیم $zN \in Z(G/N)$. پس برای هر $g \in G$ داریم $gNzN = zNgN$. لذا $gzN = zgN$ و ضرب‌های مناسب داریم $g^{-۱}z^{-۱}gzN = N$. چون $e \in N$ پس $g^{-۱}z^{-۱}gz \in N$. واضح است که $g^{-۱}z^{-۱}gz \in G'$. طبق فرض باید $g^{-۱}z^{-۱}gz = e$. در نتیجه $gz = zg$ و لذا $z \in Z(G)$. بنابراین $zN \in Z(G)/N$ و $Z(G/N) \subseteq Z(G)/N$.

تمرین ۴۴.۸.۲. *اگر N زیرگروهی از گروه G باشد که برای هر $x \in G$ داشته باشیم $x^۲ \in N$ آنگاه ثابت کنید که N نرمال و G/N آبلی است.*

حل. فرض کنیم $y \in N$ و $g \in G$. داریم

$$gyg^{-۱} = gy\,gy\,y^{-۱}\,g^{-۱}\,g^{-۱} = (gy)^۲\,y^{-۱}\,(g^{-۱})^۲.$$

چون N زیرگروه است پس $y^{-۱} \in N$. طبق فرض $(gy)^۲ \in N$ و $(g^{-۱})^۲ \in N$. لذا داریم $gyg^{-۱} \in N$. یعنی N نرمال است. برای قسمت دوم، عنصر دلخواه $gN \in G/N$ را در نظر می‌گیریم و داریم $(gN)^۲ = (gN)(gN) = g^۲N = N$. حال طبق تمرین ۶۱.۲.۲ باید گروه G/N آبلی باشد.

تمرین ۴۵.۸.۲. *فرض کنیم N زیرگروه نرمال از گروه G باشد که ۲ $=|N|$. نشان دهید که $N \subseteq Z(G)$. آیا این مطلب صحیح است که $N \subseteq G'$؟ اگر G دقیقا یک عنصر مانند x از مرتبه ۲ داشته باشد آنگاه نشان دهید که $x \in Z(G)$.*

حل. فرض کنیم $N = \{e, y\}$. چون N نرمال است پس برای هر $g \in G$ داریم $gyg^{-۱} \in N$. پس $gyg^{-۱} = e$ یا $gyg^{-۱} = y$. اگر $gyg^{-۱} = e$ آنگاه $y = e$ که تناقض آشکار است. بنابراین باید $gyg^{-۱} = y$ و لذا $gy = yg$ و این یعنی $y \in Z(G)$. در نتیجه $N \subseteq Z(G)$.
برای قسمت دوم، این مطلب صحیح نیست. برای مثال فرض کنیم $N = G = \mathbb{Z}_۲$. واضح است که $G' = \{e\}$ و $N \not\subseteq G'$.
برای قسمت سوم، طبق قضیه ۱۸.۶.۲ داریم ۲ $=|< x >|$. حال طبق تمرین ۳۹.۸.۲ باید $< x >$ نرمال باشد و لذا طبق قسمت اول داریم $x \in < x > \subseteq Z(G)$.

تمرین ۴۶.۸.۲. *فرض کنیم G یک گروه و $H, K \leq G$. اگر $K \leq N_G(H)$ آنگاه نشان دهید که H زیرگروه نرمال KH است.*

حل. چون $K \leq N_G(H)$ پس برای هر $k \in K$ داریم $kHk^{-۱} = H$ و لذا $kH = Hk$. در نتیجه $KH = HK$ و طبق گزاره ۲۹.۴.۲ باید KH زیرگروه $N_G(H)$ باشد. اما واضح است که $H \subseteq KH$. حال چون H در $N_G(H)$ نرمال است (چرا؟)، پس H در KH نرمال است.

۹.۲ قضایای یکریختی گروهی

اکنون آماده هستیم تا مهمترین بخش این فصل را ارائه کنیم. این بخش برای مطالعه گروه‌ها بسیار با اهمیت است. در حقیقت هدف این بخش را می‌توان اینگونه معرفی کرد با کمک برخی توابع خاص یک گروه ناشناخته را به یک گروهی که از قبل می‌شناسیم یا اطلاعاتی از آن داریم مرتبط می‌کنیم و از این ارتباط برای شناسایی بیشتر گروه بهره می‌بریم.

تعریف ۱.۹.۲. *فرض کنیم دو گروه $(G, .)$ و $(H, *)$ را در اختیار داریم. در این صورت تابع $f : G \longrightarrow H$ را یک همریختی گروهی (همومورفیسم گروهی) گوییم هرگاه برای هر $x, y \in G$ داشته باشیم $f(x.y) = f(x) * f(y)$.*

مثال ۲.۹.۲. *داریم که*

$$f : (\mathbb{Z}, +) \longrightarrow (\mathbb{Z}_۲, +), \quad f(x) = \bar{x}$$

یک همریختی است. زیرا برای هر $x, y \in \mathbb{Z}$ داریم

$$f(x + y) = \overline{x + y} = \bar{x} + \bar{y} = f(x) + f(y).$$

مثال ۳.۹.۲. *داریم که*

$$f : (\mathbb{R}^+, .) \longrightarrow (\mathbb{R}, +), \quad f(x) = \ln x$$

یک همریختی است. زیرا برای هر $x, y \in \mathbb{R}^+$ داریم

$$f(x.y) = \ln(x.y) = \ln x + \ln y = f(x) + f(y).$$

مثال ۴.۹.۲. *داریم که*

$$f : (\mathbb{Z}_۲, +) \longrightarrow (\mathbb{Z}, +), \quad f(\bar{x}) = x$$

یک همریختی نیست. زیرا اصلا تابع نیست

$$\bar{۱} = \bar{۳} \quad \not\Rightarrow \quad ۱ = f(\bar{۱}) = f(\bar{۳}) = ۳.$$

مثال ۵.۹.۲. *داریم که*

$$f : (\mathbb{Z}, +) \longrightarrow (\mathbb{Z}, +), \quad f(x) = ۲x + ۱$$

یک همریختی نیست. زیرا برای هر $x, y \in \mathbb{Z}$ داریم

$$f(x + y) = ۲(x + y) + ۱ = ۲x + ۲y + ۱ \neq ۲x + ۱ + ۲y + ۱ = f(x) + f(y).$$

تذکر ۶.۹.۲. *از این لحظه به بعد وقتی گروهی را می‌نویسیم از نوشتن عمل دوتایی آن برای راحتی خودداری می‌کنیم و انتظار ما این است که دانشجو خود متوجه عمل دوتایی شود، مگر این که گروه جدیدی را معرفی کنیم یا این که بخواهیم عمل دوتایی را تغییر دهیم. پس مثلا دیگر نمی‌نویسیم $(\mathbb{Z}, +)$ و می‌نویسیم $\mathbb{Z}$ و یا مثلا دیگر نمی‌نویسیم $(GL_n(\mathbb{R}), .)$ و می‌نویسیم $GL_n(\mathbb{R})$ و الی آخر. همچنین دیگر $*$ و . ، وقتی f را اثر می‌دهیم، نمی‌نویسیم و انتظار داریم که دانشجو متوجه باشد که عمل دوتایی در دامنه است یا در برد همریختی گروهی!*

تعریف و مثال ۷.۹.۲. *داریم که*

$$f : G \longrightarrow H, \quad f(x) = e_H$$

یک همریختی گروهی است. زیرا $f(xx') = e_H = e_He_H = f(x)f(x')$. به این همریختی گروهی، همریختی بدیهی گوییم.

تعریف ۸.۹.۲. *فرض کنیم $f : G \longrightarrow H$ یک همریختی گروهی باشد. اگر f پوشا باشد آنگاه به f همریختی گروهی پوشا (اپی‌مورفیسم گروهی) گوییم. اگر f یک‌به‌یک باشد آنگاه به f همریختی گروهی یک‌به‌یک (منومورفیسم گروهی) گوییم. اگر f همریختی گروهی پوشا و یک‌به‌یک باشد آنگاه به f یکریختی گروهی (ایزومورفیسم گروهی) گوییم و می‌نویسیم $G \cong H$.*

مثال ۹.۹.۲. *داریم که*

$$f : \mathbb{Z} \longrightarrow \mathbb{Z}_۲, \quad f(x) = \bar{x}$$

یک همریختی پوشا است که یک‌به‌یک نیست.

مثال ۱۰.۹.۲. *داریم که*

$$f : \mathbb{Z} \longrightarrow \mathbb{R}, \quad f(x) = ۲x$$

یک همریختی یک‌به‌یک است که پوشا نیست.

مثال ۱۱.۹.۲. *داریم که*

$$f : (\mathbb{R}^+, .) \longrightarrow (\mathbb{R}, +), \quad f(x) = \ln x$$

یک همریختی یک‌به‌یک و پوشا است، یعنی یکریختی است، $(\mathbb{R}^+, .) \cong (\mathbb{R}, +)$.

تعریف و مثال ۱۲.۹.۲. *فرض کنیم N یک زیرگروه نرمال از گروه G باشد. قرار می‌دهیم*

$$\pi : G \longrightarrow G/N, \quad \pi(x) = xN.$$

π یک تابع است. زیرا واضح است که برای هر $x \in G$ ، $\pi(x) = xN$ یک هم دسته (چپ) است و لذا در G/N قرار دارد. همچنین اگر $x = x'$ باشد آنگاه $xN = x'N$ و لذا $\pi(x) = \pi(x')$. به روشنی مشخص است که π یک تابع پوشا نیز می‌باشد. اما π یک همریختی گروهی است. زیرا به کمک گزاره ۱۲.۸.۲ داریم

$$\pi(xx') = xx'N = (xx')N = xN\, x'N = \pi(x)\pi(x').$$

به همریختی گروهی پوشا π همریختی گروهی طبیعی گوییم.

مثال ۱۳.۹.۲. داریم که

$$f:(M_۲(\mathbb{R}),+)\longrightarrow(\mathbb{R}^۴,+),\quad f(\begin{pmatrix}a & b\\ c & d\end{pmatrix})=(a,b,c,d)$$

همریختی است. زیرا

$$\begin{aligned}&f(\begin{pmatrix}a & b\\ c & d\end{pmatrix}+\begin{pmatrix}a' & b'\\ c' & d'\end{pmatrix})=f(\begin{pmatrix}a+a' & b+b'\\ c+c' & d+d'\end{pmatrix})=\\&(a+a',b+b',c+c',d+d')=(a,b,c,d)+(a',b',c',d')=\\&f(\begin{pmatrix}a & b\\ c & d\end{pmatrix})+f(\begin{pmatrix}a' & b'\\ c' & d'\end{pmatrix}).\end{aligned}$$

پوشا و یک‌به‌یک بودن f واضح است. پس f همریختی یک‌به‌یک و پوشا است، یعنی یکریختی است، $(M_۲(\mathbb{R}),+)\cong(\mathbb{R}^۴,+)$.

مثال ۱۴.۹.۲. داریم که $\mathbb{K}_۴\cong\mathbb{Z}_۲\times\mathbb{Z}_۲$. زیرا $f:\mathbb{K}_۴\longrightarrow\mathbb{Z}_۲\times\mathbb{Z}_۲$ با ضابطه زیر همریختی گروهی یک‌به‌یک و پوشا است

$$f(e)=(\bar{۰},\bar{۰}),\quad f(a)=(\bar{۱},\bar{۰}),\quad f(b)=(\bar{۰},\bar{۱}),\quad f(c)=(\bar{۱},\bar{۱}).$$

تذکر ۱۵.۹.۲. به همریختی گروهی یک‌به‌یک $f:G\longrightarrow H$ بعضا نشاننده نیز گوییم و آن را با $G\hookrightarrow H$ نشان می‌دهیم. علت نامگذاری نشاننده قضیه اول یکریختی گروهی است که در ادامه خواهیم دید.

تعریف و مثال ۱۶.۹.۲. فرض کنیم G یک گروه باشد و $H\leq G$. واضح است که $i:H\longrightarrow G$ با ضابطه $i(x)=x$ یک همریختی گروهی یک‌به‌یک (نشاننده) است و به آن همریختی گروهی شمول گوییم.

تذکر ۱۷.۹.۲. یک مزیت همریختی نسبت به تابع این است که لازم نیست اثر همریختی مانند تابع روی همه اعضای دامنه مشخص باشد. مثلا کافی است اثر همریختی را روی مولدهای گروه متناهی تولید بدانیم. مثلا مولد گروه $\mathbb{Z}$ برابر با ۱ است. فرض کنیم $f(۱)=k$ باشد. از همریختی بودن f داریم

$$f(n)=f(\underbrace{۱+۱+...+۱}_{n\text{تا}})=nf(۱)=nk.$$

تعریف ۱۸.۹.۲. به همریختی $f:G\longrightarrow G$، درون‌ریختی (اندومورفیسم) روی گروه G گوییم. درون‌ریختی که یکریختی باشد به آن خودریختی (اتومورفیسم) گوییم.

تعریف و مثال ۱۹.۹.۲. فرض کنیم G یک گروه باشد. واضح است که $id_G:G\longrightarrow G$ با ضابطه $id_G(x)=x$ یک خودریختی است که به آن همریختی گروهی همانی گوییم.

مثال ۲.۹.۲۰. داریم که $f : \mathbb{Z} \longrightarrow \mathbb{Z}$ با ضابطه $f(x) = ۵x$ یک درون‌ریختی گروهی روی $\mathbb{Z}$ است. حتی $f : \mathbb{Z} \longrightarrow \mathbb{Z}$ با ضابطه $f(x) = ۴x$ یک درون‌ریختی گروهی دیگر روی $\mathbb{Z}$ است.

مثال ۲.۹.۲۱. داریم که $f : \mathbb{R} \longrightarrow \mathbb{R}$ با ضابطه $f(x) = ۵x$ یک خودریختی گروهی است. حتی $f : \mathbb{R} \longrightarrow \mathbb{R}$ با ضابطه $f(x) = \frac{۱}{۲}x$ یک خودریختی گروهی دیگر است.

حال گزاره زیر را داریم.

گزاره ۲.۹.۲۲. *فرض کنیم $f : G \longrightarrow H$ یک همریختی گروهی باشد. در این صورت موارد زیر برقرار است.*
(الف) همواره داریم $f(e_G) = e_H$.
(ب) $f(x^{-۱}) = (f(x))^{-۱}$.
(ج) برای هر عدد صحیح n داریم $f(x^n) = (f(x))^n$.

اثبات. (الف) داریم که $f(e_G) = f(e_Ge_G) = f(e_G)f(e_G)$. طرفین را در $(f(e_G))^{-۱}$ ضرب می‌کنیم و چون در گروه H این ضرب صورت می‌گیرد نتیجه می‌شود

$$e_H = (f(e_G))^{-۱}f(e_G) = (f(e_G))^{-۱}f(e_G)f(e_G) = e_Hf(e_G) = f(e_G).$$

(ب) طبق (الف) داریم $e_H = f(e_G) = f(xx^{-۱}) = f(x)f(x^{-۱})$. حال طرفین را در $(f(x))^{-۱}$ ضرب می‌کنیم و لذا $f(x^{-۱}) = (f(x))^{-۱}$.
(ج) فرض کنیم n مثبت باشد داریم

$$f(x^n) = f(\underbrace{x\ x\ ...\ x}_{n\text{تا}}) = \underbrace{f(x)\ f(x)\ ...\ f(x)}_{n\text{تا}} = (f(x))^n.$$

اگر n منفی باشد آنگاه $-n$ مثبت است و طبق (ب) و قسمت قبل داریم

$$f(x^n) = f((x^{-۱})^{-n}) = f(\underbrace{x^{-۱}\ x^{-۱}\ ...\ x^{-۱}}_{-n\text{تا}}) =$$
$$\underbrace{f(x^{-۱})\ f(x^{-۱})\ ...\ f(x^{-۱})}_{-n\text{تا}} = (f(x^{-۱}))^{-n} = (f(x)^{-۱})^{-n} = (f(x))^n.$$

اثبات کامل است. □

گزاره ۲.۹.۲۳. *موارد زیر برقرار است.*
(الف) وارون یکریختی گروهی $f : G \longrightarrow H$ یک یکریختی است.
(ب) اگر $f : G \longrightarrow H$ و $g : H \longrightarrow K$ همریختی گروهی باشند آنگاه $gf : G \longrightarrow K$ همریختی گروهی است.
(ج) یکریخت بودن گروه‌ها یک رابطه هم ارزی است.

اثبات. (الف) چون f یک‌به‌یک و پوشا است طبق قضیه ۲۸.۱.۱ وارون دارد و وارون f به صورت $G \longrightarrow H : f^{-1}$ است که خود تابعی یک‌به‌یک و پوشا است. پس کافی است نشان دهیم که f^{-1} همریختی گروهی است. فرض کنیم $u, v \in H$. چون f پوشا است اعضای $x, y \in G$ وجود دارند که $f(x) = u$ و $f(y) = v$. چون f همریختی است پس $f(xy) = f(x)f(y) = uv$. در نتیجه از یک‌به‌یک بودن f داریم

$$f^{-1}(uv) = xy = f^{-1}(u)f^{-1}(v).$$

(ب) فرض کنیم که $x, y \in G$ داریم

$$gf(xy) = g(f(xy)) = g(f(x)f(y)) = g(f(x))\, g(f(y)) = gf(x)\, gf(y).$$

(ج) هر گروه G با خودش یکریخت است یعنی با کمک $id_G : G \longrightarrow G$ یکریختی گروهی حاصل می‌شود. قسمت (الف) خاصیت تقارنی را به دست می‌دهد. قسمت (ب) و قضیه ۲۶.۱.۱ خاصیت تعدی را می‌دهد. □

از فصل اول یادآوری می‌کنیم که برای تابع $f : X \longrightarrow Y$ به

$$Im(f) = \{f(x) \mid x \in X\}$$

برد تابع گوییم. اکنون گزاره زیر را داریم.

گزاره ۲۴.۹.۲. *فرض کنیم G و H دو گروه و $f : G \longrightarrow H$ همریختی گروهی باشد.*
(الف) همواره داریم $Im(f) \leq H$.
(ب) اگر $K \leq G$ آنگاه $f(K) = \{f(k) \mid k \in K\}$ زیرگروه H است.
(ج) اگر $K \trianglelefteq G$ آنگاه $f(K) \trianglelefteq Im(f)$. در نتیجه اگر f پوشا باشد آنگاه $f(K) \trianglelefteq H$.
(د) اگر $L \leq H$ آنگاه $f^{-1}(L) = \{x \in G \mid f(x) \in L\}$ زیرگروه G است.
(ه) اگر $L \trianglelefteq H$ آنگاه $f^{-1}(L)$ زیرگروه نرمال G است.

اثبات. (الف) طبق گزاره قبل $f(e_G) = e_H$ و لذا $e_H \in Im(f)$. پس $Im(f)$ ناتهی است. فرض کنیم $u, v \in Im(f)$. لذا $x, y \in G$ چنان وجود دارند که $f(x) = u$ و $f(y) = v$. طبق گزاره قبل، $v^{-1} = (f(y))^{-1} = f(y^{-1})$ و لذا

$$uv^{-1} = f(x)f(y^{-1}) = f(xy^{-1}) \in Im(f).$$

حال طبق قضیه ۵.۴.۲ باید $Im(f) \leq H$.
(ب) چون $e_G \in K$، پس طبق گزاره قبل $f(e_G) = e_H$ و لذا $e_H \in f(K)$. پس $f(K)$ ناتهی است. فرض کنیم $u, v \in f(K)$. لذا $x, y \in K$ چنان وجود دارند که $f(x) = u$ و $f(y) = v$. طبق گزاره قبل، $v^{-1} = (f(y))^{-1} = f(y^{-1})$ و لذا چون K زیرگروه G است داریم $xy^{-1} \in K$ و

$$uv^{-1} = f(x)f(y^{-1}) = f(xy^{-1}) \in f(K).$$

حال طبق قضیه ۵.۴.۲ باید $f(K) \leq H$.
(ج) زیرگروه بودن $f(K)$ در (ب) بررسی شده است. فرض کنیم $h \in Im(f)$. پس $z \in G$ وجود دارد که $f(z) = h$ و همچنین از گزاره قبل $f(z^{-1}) = h^{-1}$. حال فرض کنیم $u \in f(K)$. پس $x \in K$ وجود دارد که $f(x) = u$. چون K در G نرمال است، داریم $zxz^{-1} \in K$ و لذا

$$huz^{-1} = f(z)f(x)f(z^{-1}) = f(zxz^{-1}) \in f(K).$$

پس $f(K)$ در $Im(f)$ نرمال است. قسمت دوم، واضح است چون $Im(f) = H$.
(د) واضح است که $e_H \in L$ و طبق گزاره قبل $f(e_G) = e_H$ و لذا $e_G \in f^{-1}(L)$. پس $f^{-1}(L)$ ناتهی است. فرض کنیم $x, y \in f^{-1}(L)$. بنابراین $u, v \in L$ وجود دارد که $f(x) = u$ و $f(y) = v$. از زیرگروه بودن L در H و گزاره قبل داریم $f(y^{-1}) = v^{-1} \in L$. پس

$$f(xy^{-1}) = f(x)f(y^{-1}) = uv^{-1} \in L$$

و لذا باید $xy^{-1} \in f^{-1}(L)$. حال طبق قضیه ۵.۴.۲ باید $f^{-1}(L) \leq G$.
(ه) زیرگروه بودن $f^{-1}(L)$ در (د) بررسی شده است. فرض کنیم $g \in G$ و $x \in f^{-1}(L)$. پس $f(x) \in L$ و چون L در H نرمال است داریم $f(g)f(x)(f(g))^{-1} \in L$ و در نتیجه

$$f(gxg^{-1}) = f(g)f(x)f(g^{-1}) = f(g)f(x)(f(g))^{-1} \in L.$$

پس $gxg^{-1} \in f^{-1}(L)$. □

تذکر ۲۵.۹.۲. *فرض کنیم $f : G \longrightarrow H$ یک همریختی گروهی باشد. لزومی ندارد که $Im(f)$ در H نرمال باشد. طبق نمادهای مثال ۷.۳.۲، زیرگروه $N =< \sigma_6 >= \{\sigma_1, \sigma_6\}$ و همریختی شمول $i : N \longrightarrow S_3$ را در نظر بگیرید. واضح است که $Im(i) = N$. اما N در S_3 نرمال نیست. زیرا $\sigma_2\sigma_6\sigma_2^{-1} \notin N$.*

تعریف ۲۶.۹.۲. *برای همریختی گروهی $f : G \longrightarrow H$*
(الف) *به $Im(f)$ تصویر همریختی f گوییم.*
(ب) *$f^{-1}(\{e_H\}) = \{x \in G \mid f(x) = e_H\}$ هسته همریختی f گوییم و با نماد $Ker(f)$ آن را نمایش می‌دهیم ($Ker(f) = \{x \in G \mid f(x) = e_H\}$).*
(ج) *اگر f پوشا باشد آنگاه به H تصویر همریخت G گوییم.*

مثال ۲۷.۹.۲. *داریم که*

$$f : (\mathbb{R}, +) \longrightarrow (\mathbb{R} \setminus \{0\}, .), \quad f(x) = e^x$$

یک همریختی است که به وضوح $Im(f) = \mathbb{R}^+$. اما

$$Ker(f) = \{x \in \mathbb{R} \mid f(x) = 1\} = \{x \in \mathbb{R} \mid e^x = 1\} = \{0\}.$$

دقت شود که f یک‌به‌یک است! ارتباط جالبی بین یک‌به‌یک بودن همریختی و هسته همریختی وجود دارد که در ادامه خواهیم دید.

مثال ۲.۹.۲۸. *داریم که*
$$f : \mathbb{Z} \longrightarrow \mathbb{Z}_۳, \quad f(x) = \bar{x}$$
یک همریختی است که به وضوح $Im(f) = \mathbb{Z}_۳$ یعنی f پوشا است. لذا $\mathbb{Z}_۳$ تصویر همریخت $\mathbb{Z}$ است. اما

$$Ker(f) = \{x \in \mathbb{Z} \mid f(x) = \bar{۰}\} = \{x \in \mathbb{Z} \mid \bar{x} = \bar{۰}\} = ۳\mathbb{Z}.$$

دقت شود که f یک‌به‌یک نیست! *ارتباط جالبی بین یک‌به‌یک بودن همریختی و هسته همریختی وجود دارد که در ادامه خواهیم دید(شاید همین الان حدس زده باشید!).*

تذکر ۲.۹.۲۹. *فرض کنیم $f : G \longrightarrow H$ یک همریختی گروهی باشد. طبق قسمت (ه) گزاره بالا، $Ker(f) = f^{-۱}(\{e_H\})$ یک زیرگروه نرمال از G است. زیرا $\{e_H\}$ زیرگروه نرمال از H است.*

اکنون گزاره زیر را داریم.

گزاره ۲.۹.۳۰. *هر زیرگروه نرمال مانند N از گروه G هسته یک همریختی است.*

اثبات. همریختی گروهی طبیعی

$$\pi : G \longrightarrow G/N, \ \ \pi(x) = xN$$

را در نظر می‌گیریم. داریم

$$Ker(\pi) = \{x \in G \mid \pi(x) = N\} = \{x \in G \mid xN = N\} = N$$

و اثبات کامل است. □

گزاره ۲.۹.۳۱. *برای هر زیرگروه نرمال مانند N از گروه G، G/N تصویر همریخت G است.*

اثبات. همریختی گروهی طبیعی

$$\pi : G \longrightarrow G/N, \ \ \pi(x) = xN$$

پوشا است. □

گزاره زیر نشان می‌دهد که برای فهمیدن یک‌به‌یک بودن یک همریختی گروهی کافی است هسته آن بررسی شود. دقت کنید که این گزاره را برای هر تابعی به کار نبرید، فقط همریختی!

گزاره ۲.۹.۳۲. *فرض کنیم $f : G \longrightarrow H$ یک همریختی گروهی باشد. در این صورت f یک‌به‌یک است اگر و تنها اگر $Ker(f) = \{e_G\}$.*

اثبات. ($\Leftarrow$) فرض کنیم $x \in Ker(f)$. لذا باید $f(x) = e_H$. اما می‌دانیم که $f(e_G) = e_H$ (چرا؟) و در نتیجه $f(x) = f(e_G)$. چون f یک‌به‌یک است، $x = e_G$.
($\Rightarrow$) فرض کنیم $f(x) = f(y)$ که $x, y \in G$. با ضرب مناسب داریم

$$e_H = f(x)(f(y))^{-۱} = f(x)f(y^{-۱}) = f(xy^{-۱}).$$

لذا $xy^{-۱} \in Ker(f) = \{e_G\}$. پس $xy^{-۱} = e_G$ و لذا $x = y$. یعنی f یک‌به‌یک است. $\square$

در اولین اقدام می‌خواهیم گروه‌های دوری را رده‌بندی کنیم. منظور از رده‌بندی یعنی این که بگوییم یک گروه دلخواه با یک سری خواص، دقیقا گروهی است که ما آن را از قبل می‌شناسیم و در مثال‌های شناخته شده ما قرار دارد، مثلا گروه $M_۲(\mathbb{R})$ است. تحت یکریختی فقط دوتا گروه دوری داریم که از قبل آنها را نیز می‌شناسیم (تمریناتی که در مورد گروه دوری حل کرده‌اید، تقریبا بدیهی بوده‌اند ☺☺☺).

قضیه ۳۳.۹.۲. *فرض کنیم G گروهی دوری باشد.*
(الف) اگر G نامتناهی باشد آنگاه G با $\mathbb{Z}$ یکریخت است.
(ب) اگر G متناهی باشد آنگاه عدد طبیعی n وجود دارد که G با $\mathbb{Z}_n$ یکریخت است.

اثبات. (الف) فرض کنیم $G =< a >= \{a^k \mid k \in \mathbb{Z}\}$. تعریف می‌کنیم

$$f : \mathbb{Z} \longrightarrow G, \ \ f(m) = a^m.$$

واضح است که f خوشتعریف است. همچنین داریم

$$f(m + m') = a^{m+m'} = a^m a^{m'} = f(m)f(m')$$

پس f همریختی گروهی است. پوشایی f بدیهی است. حال فرض کنیم $m \in Ker(f)$. لذا $f(m) = e_G$، یعنی $a^m = e_G$. پس طبق قضیه ۱۸.۶.۲ و گزاره ۱۷.۶.۲ باید $|G|\leq m$ که تناقض آشکار با فرض است، مگر این که $m = ۰$ باشد. بنابراین $Ker(f) = \{۰\}$ و طبق گزاره ۳۲.۹.۲، f یک‌به‌یک است. در نتیجه f یکریختی است و $G \cong \mathbb{Z}$.
(ب) فرض کنیم که $|G|= n$ و $G =< a >= \{e, a, a^۲, ..., a^{n-۱}\}$. تعریف می‌کنیم

$$f : \mathbb{Z}_n \longrightarrow G, \ \ f(\bar{m}) = a^m.$$

نشان می‌دهیم که f خوشتعریف است. برای هر $\bar{m}$ واضح است که $a^m \in G$. حال فرض کنیم $\bar{m} = \bar{m'}$. بنابراین $n \mid m - m'$ و لذا $m - m' = nt$ که $t \in \mathbb{Z}$. طبق قضیه ۱۸.۶.۲ داریم

$$f(\bar{m'}) = a^{m'} = a^{m-nt} = a^m a^{-nt} = a^m = f(\bar{m}).$$

پس f خوشتعریف است. همچنین داریم

$$f(\bar{m} + \bar{m'}) = f(\overline{m + m'}) = a^{m+m'} = a^m a^{m'} = f(\bar{m})f(\bar{m'})$$

پس f همریختی گروهی است. پوشایی f بدیهی است. حال فرض کنیم $\bar{m} \in Ker(f)$. لذا $f(\bar{m}) = e_G$، یعنی $a^m = e_G$. پس طبق قضیه ۱۸.۶.۲ و گزاره ۱۷.۶.۲ باید $o(a) = n \mid m$. پس $m = tn$ که $t \in \mathbb{Z}$ و این یعنی $\bar{m} = 0$. بنابراین $Ker(f) = \{\bar{0}\}$ و طبق گزاره ۳۲.۹.۲، f یک‌به‌یک است. در نتیجه f یکریختی است و $G \cong \mathbb{Z}_n$. □

نتیجه ۳۴.۹.۲. *هر دو گروه دوری با مرتبه یکسان (متناهی یا نامتناهی) یکریختند.*

اثبات. قضیه ۳۳.۹.۲ و گزاره ۲۳.۹.۲ قسمت (ج) چیزی برای اثبات باقی نمی‌گذارند. □

اکنون اولین قضیه یکریختی گروهی که بسیار پر کاربرد است را بیان و اثبات می‌کنیم.

قضیه ۳۵.۹.۲. (*قضیه اول یکریختی گروهی*) *فرض کنیم* $f : G \longrightarrow H$ *یک همریختی گروهی باشد. در این صورت داریم* $G/Ker(f) \cong Im(f)$. *به ویژه اگر* f *پوشا باشد آنگاه* $G/Ker(f) \cong H$.

اثبات. طبق مطلبی که در بالا اشاره کردیم $Ker(f)$ زیرگروه نرمال G است و گروه خارج قسمتی $G/Ker(f)$ با معنی است. حال قرار می‌دهیم

$$\varphi : G/Ker(f) \longrightarrow Im(f), \;\; \varphi(xKer(f)) = f(x).$$

ضابطه φ در بالا خوشتعریف است. زیرا برای هر $xKer(f) \in G/Ker(f)$ واضح است که داریم $\varphi(xKer(f)) = f(x) \in Im(f)$. همچنین اگر $xKer(f) = yKer(f)$ آنگاه $y^{-1}xKer(f) = Ker(f)$ و لذا باید $y^{-1}x \in Ker(f)$. بنابراین $f(y^{-1}x) = e_H$. چون f همریختی گروهی است داریم $(f(y))^{-1}f(x) = e_H$. بنابراین $f(x) = f(y)$ و لذا $\varphi(xKer(f)) = \varphi(yKer(f))$.
φ همریختی گروهی است

$$\begin{aligned}\varphi(xKer(f)\, yKer(f)) &= \varphi(xyKer(f)) = f(xy) = \\ f(x)f(y) &= \varphi(xKer(f))\, \varphi(yKer(f)).\end{aligned}$$

φ پوشا است. زیرا اگر $u \in Im(f)$ آنگاه $f(x) = u$ که $x \in G$. لذا $\varphi(xKer(f)) = f(x)$.
φ همریختی گروهی یک‌به‌یک است. زیرا اگر فرض کنیم $xKer(f) \in Ker(\varphi)$ آنگاه خواهیم داشت $\varphi(xKer(f)) = e_H \in Im(f) \leq H$. یعنی $f(x) = e_H$ و در نتیجه $x \in Ker(f)$. لذا $xKer(f) = Ker(f)$. بنابراین $Ker(\varphi) = \{Ker(f)\}$ و طبق گزاره ۳۲.۹.۲ باید φ یک‌به‌یک است. در نتیجه φ یکریختی است و $G/Ker(f) \cong Im(f)$.
برای قسمت آخر، اگر f پوشا باشد آنگاه $Im(f) = H$ و لذا $G/Ker(f) \cong H$. □

مثال ۳۶.۹.۲. همریختی گروهی $f : \mathbb{Z} \longrightarrow \mathbb{Z}_5$ *با ضابطه* $f(x) = \bar{x}$ *پوشا است.* به علاوه $Ker(f) = 5\mathbb{Z}$ *و لذا طبق قضیه اول یکریختی گروهی، قضیه* ۳۵.۹.۲، *داریم* $\mathbb{Z}/5\mathbb{Z} \cong \mathbb{Z}_5$. *با همین تکنیک برای هر* $n \in \mathbb{N}$ *داریم* $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$.

تذکر ۳۷.۹.۲. اگر برای زیرگروه نرمال N از گروه G داشته باشیم $G/N=\{e\}$ آنگاه $G=N$. همچنین همواره داریم $G/\{e\}=G$.

قضیه ۳۸.۹.۲. (قضیه دوم یکریختی گروهی) فرض کنیم G یک گروه باشد، $N,H\leq G$ و $N\trianglelefteq G$. در این صورت داریم $NH/N\cong H/(H\cap N)$. همچنین $HN/N\cong H/(H\cap N)$.

اثبات. ابتدا باید توجه کنیم که طبق نتیجه ۱۳.۸.۲ قسمت (ب) و (د) داریم $H\cap N\trianglelefteq H$ و $N\trianglelefteq HN$. لذا گروه‌های خارج قسمتی $H/(H\cap N)$ و NH/N با معنی هستند. اکنون قرار می‌دهیم

$$\varphi: H\longrightarrow NH/N,\ \ \varphi(x)=xN.$$

φ خوشتعریف است. زیرا واضح است که $H\subseteq NH$ و برای هر $x\in H\subseteq HN/N$، xN یک هم دسته (چپ) NH در N است. همچنین اگر $x=x'$ آنگاه $xN=x'N$ و لذا $\varphi(x)=\varphi(x')$.
φ یک همریختی گروهی است

$$\varphi(xy)=xyN=(xN)\,(yN)=\varphi(x)\varphi(y).$$

φ پوشا است. زیرا اگر $uN\in NH/N$ آنگاه $u=nh$ که $n\in N$ و $h\in H$. طبق زیرگروه بودن N داریم $nN=N$ و لذا $uN=hnN=hN=\varphi(h)$.
اما

$$Ker(\varphi)=\{x\in H\mid \varphi(x)=N\}=\{x\in H\mid xN=N\}=$$
$$\{x\in H\mid x\in N\}=H\cap N.$$

اکنون طبق قضیه اول یکریختی گروهی، قضیه ۳۵.۹.۲ داریم

$$H/(H\cap N)=H/Ker(\varphi)\cong Im(\varphi)=NH/N.$$

برای قسمت آخر، طبق نتیجه ۱۳.۸.۲ قسمت (ج) داریم $NH=HN$، اکنون قسمت اول را به کار ببینید. $\square$

مثال ۳۹.۹.۲. زیرگروه‌های $۴\mathbb{Z}$ و $۶\mathbb{Z}$ از $\mathbb{Z}$ را در نظر بگیرید. طبق قضیه دوم یکریختی، قضیه ۳۸.۹.۲ داریم (گروه آبلی است و تمام زیرگروه‌ها نرمالند و شرایط قضیه دوم یکریختی برقرار است)

$$۴\mathbb{Z}/(۴\mathbb{Z}\cap ۶\mathbb{Z})=۴\mathbb{Z}/۱۲\mathbb{Z}\cong(۴\mathbb{Z}+۶\mathbb{Z})/۶\mathbb{Z}=۲\mathbb{Z}/۶\mathbb{Z}.$$

به طور کلی، فرض کنیم $m,n\in\mathbb{N}$. اگر d بزرگترین مقسوم علیه مشترک m، n و c کوچکترین مضرب مشترک m، n باشد آنگاه طبق قضیه دوم یکریختی گروهی، قضیه ۳۸.۹.۲ داریم

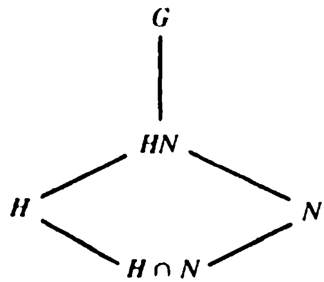
$$m\mathbb{Z}/c\mathbb{Z}\cong d\mathbb{Z}/n\mathbb{Z}.$$

زیرا $c\mathbb{Z}=m\mathbb{Z}\cap n\mathbb{Z}$ و $d\mathbb{Z}=m\mathbb{Z}+n\mathbb{Z}$.

تذکر ۴۰.۹.۲. فرض کنیم G یک گروه باشد و $N, H \trianglelefteq G$. شرایط قضیه دوم یکریختی گروهی، قضیه ۳۸.۹.۲ برقرار است و داریم

$$NH/N \cong H/(H \cap N) \qquad NH/H \cong N/(H \cap N)$$

تذکر ۴۱.۹.۲. به سبب شکل زیر به قضیه دوم یکریختی بعضا قضیه لوزی نیز گوییم



قضیه ۴۲.۹.۲. (قضیه سوم یکریختی گروهی) فرض کنیم G یک گروه باشد، $H, N \trianglelefteq G$ و $N \leq H$. در این صورت داریم

$$(G/N)/(H/N) \cong G/H.$$

اثبات. ابتدا دقت شود که $N \trianglelefteq H$ و گروه خارج قسمتی H/N با معنی است. همچنین طبق تمرین ۴۲.۸.۲، H/N زیرگروه نرمال G/N است و گروه خارج قسمت $(G/N)/(H/N)$ با معنی است. اکنون قرار می‌دهیم

$$\varphi : G/N \longrightarrow G/H, \ \ \varphi(xN) = xH.$$

φ خوشتعریف است. زیرا واضح است که برای هر $x \in G$، xH یک هم دسته (چپ) G در H است. همچنین اگر $xN = x'N$ آنگاه $(x')^{-1}xN = N$ و لذا $(x')^{-1}x \in N$. در نتیجه $(x')^{-1}x \in H$ و این یعنی $(x')^{-1}xH = H$. بنابراین $xH = x'H$ و $\varphi(xN) = \varphi(x'N)$.
φ یک همریختی گروهی است

$$\varphi(xN\,yN) = \varphi(xyN) = xyH = xH\,yH = \varphi(xN)\varphi(yN).$$

به وضوح φ پوشا است. اما

$$Ker(\varphi) = \{xN \in G/N \mid \varphi(xN) = H\} = \{xN \in G/N \mid xH = H\} = \{xN \in G/N \mid x \in H\} = H/N.$$

اکنون طبق قضیه اول یکریختی گروهی، قضیه ۳۵.۹.۲ داریم

$$(G/N)/(H/N) = (G/N)/Ker(\varphi) \cong Im(\varphi) = G/H.$$

□

مثال ۴۳.۹.۲. *زیرگروه‌های $\mathbb{Z}$۴ و $\mathbb{Z}$۸ از $\mathbb{Z}$ را در نظر بگیرید. طبق قضیه سوم یکریختی، قضیه ۴۲.۹.۲ داریم (گروه آبلی است و تمام زیرگروه‌ها نرمالند و شرایط قضیه سوم یکریختی برقرار است)*

$$(\mathbb{Z}/۸\mathbb{Z})/(۴\mathbb{Z}/۸\mathbb{Z}) \cong \mathbb{Z}/۴\mathbb{Z} \cong \mathbb{Z}_۴.$$

تذکر ۴۴.۹.۲. *به قضیه سوم یکریختی بعضا قضیه یکریختی خارج قسمتی مضاعف نیز گویند (برخی در ایران این قضیه را به دور در دور و نزدیک در نزدیک نیز می‌شناسند! چون بسیار شبیه به ساده‌سازی تقسیم دو عدد گویا است).*

قبل از بیان قضیه تناظر، به لم زیر نیاز داریم.

لم ۴۵.۹.۲. *فرض کنیم $f : G \longrightarrow H$ یک همریختی گروهی باشد.*
(الف) اگر $K \leq G$ و $Ker(f) \subseteq K$ آنگاه $K = f^{-۱}(f(K))$.
(ب) اگر $L \leq H$ و f پوشا باشد آنگاه $L = f(f^{-۱}(L))$.

اثبات. (الف) برای هر تابع f همواره داریم $K \subseteq f^{-۱}(f(K))$، از جمله برای همریختی! حال فرض کنیم $x \in f^{-۱}(f(K))$. پس $f(x) \in f(K)$ و در نتیجه برای $k \in K$ داریم $f(x) = f(k)$. با ضرب مناسب و استفاده از ویژگی‌های همریختی خواهیم داشت $f(k^{-۱}x) = e_H$. لذا $k^{-۱}x \in Ker(f) \subseteq K$. با ضرب مناسب و این مطلب که K زیرگروه است داریم $x \in K$. پس $f^{-۱}(f(K)) \subseteq K$ و لذا $K = f^{-۱}(f(K))$.
(ب) یک بررسی ساده با کمک عضو گیری است (این قسمت را حتما در مبانی ریاضی دیده‌اید). □

قضیه ۴۶.۹.۲. (*قضیه تناظر برای گروه*) *فرض کنیم $f : G \longrightarrow H$ یک همریختی گروهی پوشا باشد. یک تناظر بین خانواده زیرگروه‌های G که شامل $Ker(f)$ هستند و خانواده زیرگروه‌های H وجود دارد. همچنین یک تناظر بین خانواده زیرگروه‌های نرمال G که شامل $Ker(f)$ هستند و خانواده زیرگروه‌های نرمال H وجود دارد.*

اثبات. قرار می‌دهیم

$$\mathcal{A} = \{K \leq G \mid Ker(f) \subseteq K\} \qquad \mathcal{B} = \{L \mid L \leq H\}$$

و تعریف می‌کنیم

$$\theta : \mathcal{A} \longrightarrow \mathcal{B}, \ \ \theta(K) = f(K).$$

θ خوشتعریف است. زیرا برای هر $K \leq G$، طبق گزاره ۲۴.۹.۲ قسمت (ب) داریم $f(K) \leq H$ و در نتیجه $\theta(K) = f(K) \in \mathcal{B}$. همچنین اگر $K_۱ = K_۲$ آنگاه واضح است که داریم $f(K_۱) = f(K_۲)$ و لذا $\theta(K_۱) = \theta(K_۲)$.
θ پوشا است. فرض کنیم $L \in \mathcal{B}$. طبق گزاره ۲۴.۹.۲ قسمت (د)، $f^{-۱}(L)$ زیرگروه G است. حال طبق لم ۴۵.۹.۲ قسمت (ب) داریم

$$\theta(f^{-۱}(L)) = f(f^{-۱}(L)) = L.$$

θ یک‌به‌یک است. زیرا اگر فرض کنیم $\theta(K_1) = \theta(K_2)$ یعنی $f(K_1) = f(K_2)$ آنگاه $f^{-1}(f(K_1)) = f^{-1}(f(K_2))$. حال طبق لم ۴۵.۹.۲ قسمت (الف) باید $K_1 = K_2$ باشد.
برای قسمت دوم، همین روش بالا را به کار می‌گیریم. فقط از قسمت (ج) و (ه) گزاره ۲۴.۹.۲ استفاده می‌کنیم. لم ۴۵.۹.۲ نیز برقرار است، زیرا هر زیرگروه نرمال، زیرگروه نیز می‌باشد. □

حال نتیجه بسیار مهم زیر را داریم.

تذکر ۴۷.۹.۲. *اگر $f : G \longrightarrow H$ یک همریختی دلخواه باشد انگاه قضیه تناظر زمانی صحیح است که H را با $Im(f)$ عوض کنیم.*

تذکر ۴۸.۹.۲. *قضیه تناظر را با نام‌های قضیه چهارم یکریختی گروهی و یا قضیه مشبکه نیز می‌شناسند.*

نتیجه ۴۹.۹.۲. *فرض کنیم N زیرگروه نرمالی از گروه G باشد. برای هر زیرگروه L از G/N زیرگروه یکتایی مانند K از G وجود دارد که $L = K/N$. به علاوه $K \trianglelefteq G$ اگر و تنها اگر $K/N \trianglelefteq G/N$.*

اثبات. همریختی گروهی طبیعی

$$\pi : G \longrightarrow G/N, \;\; \pi(x) = xN$$

پوشا است و $Ker(\pi) = N$. حال طبق قضیه تناظر، قضیه ۴۶.۹.۲، زیرگروه‌های G/N در تناظر با زیرگروه‌های از G هستند که شامل N می‌باشند. به عبارتی دیگر اگر L زیرگروهی از G/N باشد آنگاه زیرگروهی مانند مانند K شامل N از G وجود دارد که $L = \pi(K) = K/N$. اگر K' شامل N چنان باشد که $L = \pi(K') = K'/N$ آنگاه واضح است $K = K'$. زیرا مثلا فرض کنیم $y \in K$. پس $yN \in K/N = K'/N$ و لذا $yN = y'N$ که $y' \in K'$. در نتیجه $y^{-1}y'N = N$ یعنی $y^{-1}y' \in N \subseteq K'$. اما K' زیرگروه است و با ضرب از سمت راست در y' داریم $y^{-1} \in K'$ و لذا $y \in K'$. پس $K \subseteq K'$. به روش مشابه $K' \subseteq K$ و در نتیجه $K = K'$.
قسمت دوم، مشابه است و از قسمت دوم قضیه تناظر، قضیه ۴۶.۹.۲ استفاده می‌شود (برای اثبات مستقیم تمرین ۴۲.۸.۲ را ببینید). □

خودریختی‌های روی یک گروه مانند G اهمیت بسیار زیادی در شناسایی گروه G دارند. در ادامه کمی در این مورد خواهیم گفت.
با گزاره زیر شروع می‌کنیم.

گزاره ۵۰.۹.۲. *فرض کنیم G یک گروه باشد و قرار می‌دهیم*

$$Aut(G) = \{f : G \longrightarrow G \mid \text{یک خودریختی گروهی است } f\}.$$

در این صورت $Aut(G)$ با عمل ترکیب توابع یک گروه است (به جای fog می‌نویسیم fg و به جای ff می‌نویسیم f^2 و الی آخر).

اثبات. قضیه ۲۵.۱.۱، قضیه ۲۶.۱.۱ و قضیه ۲۸.۱.۱ چیزی برای اثبات نمی‌گذارند. دقت نمایید که $id_G : G \longrightarrow G$ عنصر خنثی است. □

مثال ۵۱.۹.۲. *گروه $G = \mathbb{Z}_۳$ را در نظر می‌گیریم. دو خودریختی زیر را داریم*

$$\begin{cases} id_G : G \longrightarrow G \\ \qquad id_G(\bar{۰}) = \bar{۰} \\ \qquad id_G(\bar{۱}) = \bar{۱} \\ \qquad id_G(\bar{۲}) = \bar{۲} \end{cases} \qquad\qquad \begin{cases} f : G \longrightarrow G \\ \qquad f(\bar{۰}) = \bar{۰} \\ \qquad f(\bar{۱}) = \bar{۲} \\ \qquad f(\bar{۲}) = \bar{۱} \end{cases}$$

لذا $Aut(G) = \{id_G, f\}$.

مثال ۵۲.۹.۲. *می‌خواهیم $Aut(\mathbb{Z})$ را به دست آوریم. می‌دانیم $\mathbb{Z}$ دارای دو مولد ۱ و ۱− است. فعلا مولد ۱ را در نظر می‌گیریم. اگر همریختی f بخواهد ۱ را به عدد صحیحی غیر از ۱ و ۱− مانند k نظیر کند آنگاه پوشا نمی‌شود و $Im(f) = k\mathbb{Z}$ خواهد بود و لذا خودریختی دریافت نخواهیم کرد. در نتیجه $f(۱)$ برابر ۱ یا ۱− است. اگر $f(۱) = ۱$ باشد خودریختی $id_{\mathbb{Z}}$ را به دست می‌آوریم. اگر $f(۱) = -۱$ آنگاه $f(x) = -x$ را به دست می‌آوریم. همین استدلال برای مولد ۱− نیز صادق است. بنابراین $Aut(\mathbb{Z})$ فقط دو عنصر $id_{\mathbb{Z}}$ و $f(x) = -x$ را دارد.*

تذکر ۵۳.۹.۲. *از ما بدون اثبات بپذیرید که برای $n \neq ۲, ۶$ همواره داریم $Aut(S_n) \cong S_n$.*

تعریف و مثال ۵۴.۹.۲. *فرض کنیم G یک گروه باشد و $x \in G$. قرار می‌دهیم*

$$f_x : G \longrightarrow G, \quad f_x(y) = xyx^{-۱}.$$

واضح است که f_x خوشتعریف است. اما

$$f_x(yy') = xyy'x^{-۱} = xyx^{-۱}\, xy'x^{-۱} = f_x(y)f_x(y')$$

و لذا f_x یک همریختی (درون‌ریختی) است. اگر $y \in Ker(f_x)$ آنگاه $e = f_x(y) = xyx^{-۱}$ و لذا باید $y = e$. پس طبق گزاره ۳۲.۹.۲ باید f_x یک‌به‌یک باشد. اگر $y \in G$ دلخواه باشد آنگاه

$$f_x(x^{-۱}yx) = x\, x^{-۱}yx\, x^{-۱} = y.$$

پس f_x پوشا است. در حقیقت نشان داده‌ایم f_x یک خودریختی است. برای اعضای مختلف G مثل x، می‌توان خودریختی‌های متنوعی ساخت. مثلا

$$f_{x^{-۱}} : G \longrightarrow G, \quad f_{x^{-۱}}(y) = x^{-۱}yx.$$

همچنین $f_e = id_G$ است. به چنین خودریختی‌های، خودریختی داخلی گوییم.

گزاره ۵۵.۹.۲. *فرض کنیم G یک گروه باشد و*

$$Inn(G) = \{f_x : G \longrightarrow G \mid x \in G, \text{ یک خودریختی داخلی گروهی است } f_x\}.$$

در این صورت $Inn(G) \trianglelefteq Aut(G)$.

اثبات. چون $e \in G$ پس واضح است که $f_e = id_G \in Inn(G)$ و لذا $Inn(G)$ ناتهی است. حال فرض کنیم $f_x, f_y \in Inn(G)$. داریم که $(f_y)^{-۱} = f_{y^{-۱}}$. زیرا $f_y f_{y^{-۱}} = f_{y^{-۱}} f_y = f_e$. پس برای هر $z \in G$ داریم

$$f_x f_{y^{-۱}}(z) = f_x(y^{-۱}zy) = xy^{-۱}zyx^{-۱} = f_{xy^{-۱}}(z).$$

لذا $f_x f_{y^{-۱}} \in Inn(G)$ و طبق گزاره ۵.۴.۲، $Inn(G)$ زیرگروه $Aut(G)$ است.
اکنون فرض کنیم $f \in Aut(G)$. برای هر $z \in G$ داریم

$$ff_xf^{-۱}(z) = f(f_x(f^{-۱}(z))) = f(xf^{-۱}(z)x^{-۱}) =$$
$$f(x)\, f(f^{-۱}(z))\, f^{-۱}(x) = f(x)\, z\, f^{-۱}(x) f_{f(x)}(z) \in Inn(G)$$

و لذا $Inn(G)$ زیرگروه نرمال $Aut(G)$ است. □

تذکر ۵۶.۹.۲. *اگر G گروهی آبلی باشد آنگاه واضح است که $Inn(G) = \{e\}$.*

اکنون قضیه مهم زیر را داریم.

قضیه ۵۷.۹.۲. *فرض کنیم G گروه باشد. در این صورت $G/Z(G) \cong Inn(G)$.*

اثبات. قرار می‌دهیم

$$\theta : G \longrightarrow Inn(G), \;\; \theta(x) = f_x.$$

θ خوشتعریف است. واضح است که برای هر $x \in G$، داریم $f_x \in Inn(G)$. و اگر $x = x'$ آنگاه $f_x = f_{x'}$ یعنی $\theta(x) = \theta(x')$.
θ همریختی است. زیرا برای هر $z \in G$ داریم

$$\theta(xy)(z) = f_{xy}(z) = xyz(xy)^{-۱} = xyzy^{-۱}x^{-۱} =$$
$$f_x(yzy^{-۱}) = f_xf_y(z) = \theta(x)\theta(y)(h).$$

پس $\theta(xy) = \theta(x)\theta(y)$. پوشایی θ واضح است و داریم

$$Ker(\theta) = \{x \in G \mid \theta(x) = f_e\} = \{x \in G \mid f_x = f_e\} =$$
$$\{x \in G \mid f_x(z) = f_e(z) \quad \forall z \in G\} = \{x \in G \mid xzx^{-۱} = z \quad \forall z \in G\} =$$
$$\{x \in G \mid xz = zx \quad \forall z \in G\} = Z(G)$$

اکنون طبق قضیه اول یکریختی گروهی، قضیه ۳۵.۹.۲، $G/Z(G) \cong Inn(G)$. □

مثال ۵۸.۹.۲. *می‌دانیم که* $Z(S_3)=\{e\}$ (تمرین ۳۸.۴.۲ *را ببینید*). *طبق قضیه* ۵۷.۹.۲ *داریم* $Inn(S_3)\cong S_3/Z(S_3)\cong S_3$.

حال نتیجه جالب زیر را داریم.

نتیجه ۵۹.۹.۲. *اگر* $Inn(G)$ *گروهی دوری باشد آنگاه* G *آبلی است.*

اثبات. طبق قضیه ۵۷.۹.۲ و فرض باید $G/Z(G)$ دوری باشد. اکنون طبق قضیه ۲۶.۸.۲ باید G آبلی باشد. □

قضیه ۶۰.۹.۲. *فرض کنیم* G *یک گروه و* $H\leq G$. *در این صورت* $N_G(H)/C_G(H)$ *با زیرگروهی از* $Aut(H)$ *یکریخت است. به ویژه اگر* G *متناهی باشد آنگاه* $|N_G(H)/C_G(H)|\mid|Aut(H)|$.

اثبات. طبق گزاره ۳۴.۸.۲ گروه خارج قسمتی $N_G(H)/C_G(H)$ با معنی است. اکنون قرار می‌دهیم

$$\theta:N_G(H)\longrightarrow Aut(H),\ \ \theta(x)=f_x \qquad\qquad (f_x:H\longrightarrow H,\ \ f_x(h)=xhx^{-1})$$

یک بررسی سر راست نشان می‌دهد که θ خوشتعریف است. حال برای هر $h\in H$ داریم

$$\theta(xy)(h)=f_{xy}(h)=xyh(xy)^{-1}=xyhy^{-1}x^{-1}=f_xf_y(h)=\theta(x)\theta(y)(h).$$

لذا $\theta(xy)=\theta(x)\theta(y)$. یعنی θ همریختی گروهی است. اما

$$\begin{aligned}&Ker(\theta)=\{x\in N_G(H)\mid\theta(x)=f_e\}=\{x\in N_G(H)\mid f_x=f_e\}=\\&\{x\in N_G(H)\mid f_x(z)=f_e(z)\qquad\forall z\in H\}=\\&\{x\in N_G(H)\mid xzx^{-1}=z\qquad\forall z\in H\}=\\&\{x\in N_G(H)\mid xz=zx\qquad\forall z\in H\}=C_G(H).\end{aligned}$$

اکنون طبق قضیه اول یکریختی گروهی، قضیه ۳۵.۹.۲، $N_G(H)/C_G(H)\cong Im(\theta)$. اما طبق گزاره ۲۴.۹.۲ قسمت (الف)، $Im(\theta)\leq Aut(H)$ و حکم اثبات شده است. قسمت دوم، نتیجه بدیهی قضیه لاگرانژ، قضیه ۲۳.۷.۲ است و داریم $|N_G(H)/C_G(H)|=|Im(\theta)|\mid|Aut(H)|$. □

این بخش را با مطالبی در مورد گروه ساده به پایان می‌رسانیم.

تعریف ۶۱.۹.۲. *فرض کنیم* G *یک گروه باشد. گوییم زیرگروه* M *ماکسیمال است هرگاه* $M\neq G$ *و از* $M\leq H\leq G$ *بتوان نتیجه گرفت که* $M=H$ *یا* $G=H$ *(یعنی هیچ زیرگروهی بین* M *و* G *نباشد).*

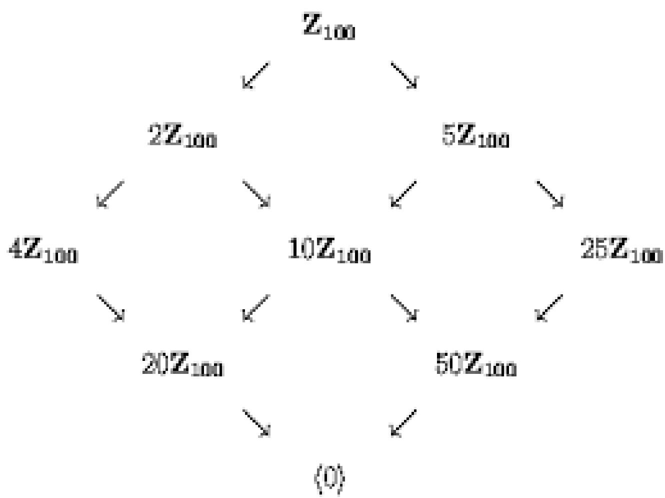
مثال ۶۲.۹.۲. گروه $\mathbb{K}_۴$ را در نظر می‌گیریم. *این گروه سه زیرگروه ماکسیمال دارد و لذا زیرگروه ماکسیمال لزوما یکتا نیست*

$$M_۱ = \{e, a\} \qquad M_۱ = \{e, b\} \qquad M_۳ = \{e, c\}$$

مثال ۶۳.۹.۲. *زیرگروه $n\mathbb{Z}$ از $\mathbb{Z}$ ماکسیمال است اگر و تنها اگر n عدد اول باشد.* فرض کنیم $n\mathbb{Z}$ ماکسیمال است ولی n اول نباشد. پس $n = km$ که $k \neq ۱$ و $m \neq ۱$. حال واضح است که داریم $\mathbb{Z} \lneq k\mathbb{Z} \lneq n\mathbb{Z}$ و این تناقض آشکار با ماکسیمال بودن است.
برعکس، فرض کنیم n عددی اول است. به وضوح $\mathbb{Z} \neq n\mathbb{Z}$. حال اگر $\mathbb{Z} \leq m\mathbb{Z} \leq n\mathbb{Z}$ آنگاه $n \in m\mathbb{Z}$ و لذا $n = mt$. اما n اول است و در نتیجه $m = ۱$ یا $t = ۱$. بنابراین $m\mathbb{Z} = \mathbb{Z}$ یا $n\mathbb{Z} = m\mathbb{Z}$.

مثال ۶۴.۹.۲. گروه $\mathbb{Q}_۸$ را در نظر می‌گیریم. در این گروه غیر آبلی زیرگروه $\{-۱, ۱, i, -i\}$ ماکسیمال است. ولی زیرگروه $\{۱, -۱\}$ ماکسیمال نیست.

مثال ۶۵.۹.۲. فرض کنیم G یک گروه متناهی مرتبه n باشد و M یک زیرگروه G باشد که مرتبه آن بزرگترین شمارنده نابرابر با n است. در این صورت M ماکسیمال است. زیرا اگر $M \leq H \leq G$ آنگاه طبق قضیه لاگرانژ، قضیه ۲۳.۷.۲ داریم $|G| \mid |H|$ و $|H| \mid |M|$. اکنون به سادگی می‌توان نشان داد که $H = M$ یا $H = G$. البته ممکن است که مرتبه زیرگروهی بزرگترین شمارنده نابرابر با مرتبه گروه نباشد ولی ماکسیمال باشد. مثلا گروه $\mathbb{Z}_{۱۰۰}$ را در نظر بگیرید. زیرگروه‌های این گروه نموداری به شکل زیر دارند



همانطوری که از نمودار مشخص است زیرگروه تولید شده توسط $\bar{۲}$ یعنی $۲\mathbb{Z}_{۱۰۰}$ مرتبه ۵۰ دارد یعنی بزرگترین شمارنده ۱۰۰، از این رو ماکسیمال است. اما زیرگروه تولید شده توسط $\bar{۵}$ یعنی $۵\mathbb{Z}_{۱۰۰}$ مرتبه ۲۰ دارد و ۲۰ بزرگترین شمارنده ۱۰۰ نیست. در حالی که به وضوح هیچ زیرگروهی بین $۵\mathbb{Z}_{۱۰۰}$ و $\mathbb{Z}_{۱۰۰}$ وجود ندارد و این یعنی $۵\mathbb{Z}_{۱۰۰}$ ماکسیمال است.

چون گروه‌های متناهی تعداد متناهی زیرگروه دارند، پس حتما زیرگروه ماکسیمال دارند. اما اینطور نیست که هر گروهی زیرگروه ماکسیمال داشته باشد! به مثال زیر توجه کنید.

مثال ۲.۹.۶۶. گروه $\mathbb{Q}$ را در نظر بگیرید. این گروه زیرگروه ماکسیمال ندارد. به برهان خلف، فرض کنیم M زیرگروه ماکسیمال این گروه است. واضح است که M باید ناصفر باشد. فرض کنیم $\frac{x}{y} \in \mathbb{Q} \setminus M$ و $0 \neq \frac{a}{b} \in M$. بنابراین $a \in M$ (چرا؟). حال عنصر

$$\frac{\frac{a}{b}}{\frac{x}{y}} = \frac{ay}{bx}$$

ناصفر است، زیرا $ay \neq 0$. عنصر

$$\frac{\frac{ay}{1}}{\frac{x}{y}} = \frac{ay^2}{x}$$

را در نظر می‌گیریم. ادعا می‌کنیم $\frac{x}{ay^2} \notin M + <\frac{x}{y}>$. چون اگر $\frac{x}{ay^2} \in M + <\frac{x}{y}>$ آنگاه $\frac{x}{ay^2} = m + k\frac{x}{y}$ که $m \in M$ و $k \in \mathbb{Z}$. بنابراین

$$x = may^2 + kaxy \in M$$

که تناقض است. پس داریم

$$M \lneq M + <\frac{x}{y}> \lneq \mathbb{Q}$$

و لذا M ماکسیمال نیست.

مثال بعدی به شدت خاص است و فقط آن را در گوشه ذهنتان داشته باشید!

مثال ۲.۹.۶۷. گروه خارج قسمتی $\mathbb{Q}/\mathbb{Z}$ را در نظر بگیرید. تمام عناصر این گروه که مرتبه آنها توانی از عدد ۲ است را در نظر بگیرید و آن را با نماد $\mathbb{Z}_{2^\infty}$ نشان دهید. مثلا $\frac{3}{4} + \mathbb{Z}$ مرتبه 2^2 دارد و در $\mathbb{Z}_{2^\infty}$ قرار دارد. می‌توان نشان داد که $\mathbb{Z}_{2^\infty}$ یک گروه است و زیرگروه ماکسیمال ندارد (می‌پذیریم!). این کار را با هر عدد اول p می‌توانید انجام دهید و گروه $\mathbb{Z}_{p^\infty}$ را بسازید. به این گروه که بسیار مهم نیز می‌باشد، در لحظه پیدایشش به گروه pـ شبه دوری مشهور شد اما ریاضیدان‌های غربی و امروزی به آن گروه پروفر[۶] گویند.

تعریف ۲.۹.۶۸. فرض کنیم G یک گروه باشد. گوییم زیرگروه نرمال M نرمال ماکسیمال است هرگاه $G \neq M$ و از $M \leq H \trianglelefteq G$ بتوان نتیجه گرفت که $H = M$ یا $H = G$ (یعنی هیچ زیرگروه نرمالی بین M و G نباشد).

مثال ۲.۹.۶۹. چون در هر گروه آبلی، همه زیرگروه‌ها نرمال هستند، لذا هر زیرگروه ماکسیمال، نرمال ماکسیمال است.

مثال ۲.۹.۷۰. گروه $\mathbb{Q}_8$ را در نظر می‌گیریم. در این گروه غیر آبلی زیرگروه $\{-1, 1, i, -i\}$ نرمال است. زیرا اندیس این زیرگروه برابر دو است. واضح است که این زیرگروه نرمال ماکسیمال است.

[۶] prufer

زیرگروه‌های ماکسیمال لزوما نرمال نیستند.

مثال ۷۱.۹.۲. *طبق نمادهای مثال ۷.۳.۲، زیرگروه $\{\sigma_1, \sigma_6\} =< \sigma_6 >= N$ ماکسیمال است اما زیرگروه نرمال از S_3 نیست. زیرا $\sigma_2\sigma_6\sigma_2^{-1} \notin N$.*

تعریف ۷۲.۹.۲. *گروه G را ساده گوییم هرگاه تنها زیرگروه‌های نرمال آن $\{e\}$ و G باشند.*

مثال ۷۳.۹.۲. *گروه $\mathbb{Z}_2$ ساده است. به طور کلی برای هر عدد اول p، گروه $\mathbb{Z}_p$ ساده است. چون p عدد اول است و شمارنده غیر از خودش و ۱ ندارد، از قضیه لاگرانژ، قضیه ۲۳.۷.۲، زیرگروهی نابدیهی ندارد. یعنی اصلا زیرگروه نابدیهی ندارد تا بخواهد زیرگروه نرمال باشد.*

مثال ۷۴.۹.۲. *گروه $\mathbb{K}_4$ ساده نیست.*

قضیه زیر یک روش ساختن گروه ساده را به دست می‌دهد و ارتباط آن را با زیرگروه نرمال ماکسیمال نشان می‌دهد.

قضیه ۷۵.۹.۲. *فرض کنیم N زیرگروه سره نرمال گروه G باشد. در این صورت N نرمال ماکسیمال است اگر و تنها اگر G/N ساده باشد.*

اثبات. $(\Leftarrow)$ طبق نتیجه ۴۹.۹.۲، فرض کنیم K/N زیرگروه نرمال G/N باشد که K شامل N است. دوباره طبق نتیجه ۴۹.۹.۲ داریم K در G نرمال است. چون G ساده است، پس $K = N$ یا $K = G$. این بدان معنی است که گروه G/N زیرگروه نرمال غیربدیهی ندارد.
$(\Rightarrow)$ فرض کنیم $G \trianglelefteq K \leq N$. پس طبق نتیجه ۴۹.۹.۲ داریم $K/N \trianglelefteq G/N$. اما G/N گروه ساده است، پس K/N برابر زیرگروه‌های بدیهی است. یعنی $K = N$ یا $K = G$ و لذا N نرمال ماکسیمال است. $\square$

حال نتیجه زیر را داریم.

نتیجه ۷۶.۹.۲. *فرض کنیم N و N' دو زیرگروه نرمال ماکسیمال متمایز از گروه G باشند. در این صورت $N \cap N'$ زیرگروه نرمال ماکسیمال از N و N' است.*

اثبات. همه شرایط قضیه دوم یکریختی، قضیه ۳۸.۹.۲، برقرار است و داریم

$$N/(N \cap N') \cong NN'/N'.$$

طبق نتیجه ۱۴.۸.۲، NN' زیرگروه نرمال است. همچنین طبق نتیجه ۱۳.۸.۲ داریم $N' \trianglelefteq NN'$. بنابراین $N \trianglelefteq NN' \trianglelefteq G$. اما N ماکسیمال است، پس $N = NN'$ و یا $N = G$. اگر $N = NN'$ آنگاه $N \subseteq N'$ و این تناقض آشکار با تمایز N و N' است. پس $G = NN'$ و لذا طبق قضیه ۷۵.۹.۲، $G/N = NN'/N$ ساده است و باید $N/(N \cap N')$ ساده باشد. بنابراین دوباره طبق قضیه ۷۵.۹.۲، $N \cap N'$ زیرگروه نرمال ماکسیمال از N است. به صورت مشابه $N \cap N'$ زیرگروه نرمال ماکسیمال از N' است. $\square$

شاید اینطور به نظرتان بیاید که گروه ساده چیزی ندارد! اما به سود شما است که از مواضع خود عقب نشینی کنید! اسمش ساده است، اما ساده نیست! همین قدر بدانید که هنوز ریاضیدانان نتوانسته‌اند گروه‌های ساده نامتناهی را به صورت کامل شناسایی کنند. اما گروه‌های ساده متناهی چطور؟! خوشبختانه در این زمینه باید بگوییم تمام گروه‌های متناهی ساده ، به تلاش ریاضیدانانی بزرگ از جمله گالوا، آبل، کیلی، سیلو، فربنیوس، برنساید، دیکسون، هال، برائور، زاسن‌هاوس، فیت، تامپسون، گرونشتاین، آزباکر و گونتیر (از ریاضیدانانی که اسم برده نشدند، پوزش می‌طلبیم، تعدادتان زیاد است ☺) رده‌بندی شده‌اند. در حقیقت تلاش این ریاضیدانان از ۱۸۳۲ میلادی آغاز و به صورت دقیق و کامل در سال ۲۰۱۲ میلادی خاتمه یافت. بیش صد مجله معتبر ریاضی در همین زمینه مقاله چاپ کرده‌اند که سبب شده طولانی‌ترین اثبات ریاضی متعلق به شاخه جبر باشد. از کنار هم قرار دادن این مقالات بیشتر از ۱۰۰۰۰ صفحه اثبات حاصل خواهد شد! در این بین از همه راحتتر گروه ساده متناهی آبلی است که در قضیه زیر آن را برای شما رده‌بندی می‌کنیم.

قضیه ۷۷.۹.۲. *G یک گروه ساده آبلی اگر و تنها اگر عدد اول p وجود داشته باشد که $G \cong \mathbb{Z}_p$.*

اثبات. ($\Leftarrow$) چون G آبلی است پس هر زیرگروه آن نرمال است. حال فرض کنیم $e \neq a \in G$. زیرگروه $< a >$ نابدیهی است و لذا باید $G =< a >$، یعنی G گروه دوری است. پس طبق قضیه ۳۳.۹.۲ داریم $G \cong \mathbb{Z}$ یا $G \cong \mathbb{Z}_n$ که $n \in \mathbb{N}$. اگر $G \cong \mathbb{Z}$ آنگاه ساده نیست! زیرا $\mathbb{Z}$ بیشمار زیرگروه نرمال نابدیهی به شکل $k\mathbb{Z}$ دارد. پس $G \cong \mathbb{Z}_n$ که $n \in \mathbb{N}$. نشان می‌دهیم n اول است. فرض کنیم n اول نباشد. در نتیجه $n = tl$ که $t, l > ۱$. در این صورت $t\mathbb{Z}_n =< \bar{t} >$ زیرگروه نابدیهی نرمال است و این تناقض آشکار است. لذا n عدد اول است.
($\Rightarrow$) در مثال بالا شرح داده شد که $\mathbb{Z}_p$ گروه ساده است. □

تذکر ۷۸.۹.۲. *در بخش بعد برای شما مثالی خواهیم آورد از یک گروه غیر آبلی G که ساده است اما زیرگروه نابدیهی دارد.*

تمرین‌های حل شده

تمرین ۷۹.۹.۲. *نشان دهید که گروه G آبلی است اگر و تنها اگر $f : G \longrightarrow G$ با ضابطه $f(x) = x^{-۱}$ همریختی گروهی باشد.*

حل. فرض کنیم G آبلی باشد. برای هر $x, y \in G$ داریم

$$f(xy) = (xy)^{-۱} = y^{-۱}x^{-۱} = x^{-۱}y^{-۱} = f(x)f(y)$$

و لذا f همریختی گروهی است. اکنون برعکس، فرض کنیم f همریختی گروهی باشد. برای هر $x, y \in G$ داریم

$$y^{-۱}x^{-۱} = f(y)f(x) = f(yx) = (yx)^{-۱} = x^{-۱}y^{-۱}$$

و لذا از $y^{-۱}x^{-۱} = x^{-۱}y^{-۱}$ با ضرب‌های مناسب نتیجه می‌شود که $xy = yx$.

تمرین ۸۰.۹.۲. *هسته همریختی گروهی $f:\mathbb{Q}_۸\longrightarrow\mathbb{Z}_۲$ را ضابطه $f(i)=\bar{۰}$ و $f(j)=\bar{۱}$ را پیدا کنید.*

حل. ابتدا دقت کنید که $k=ij$ و لذا $f(k)=f(ij)=f(i)+f(j)=\bar{۰}+\bar{۱}=\bar{۱}$. همچنین باید $f(۱)=\bar{۰}$. زیرا همریختی گروهی عنصر خنثی را به عنصر خنثی می‌نگارد. داریم $f(-۱)=-f(۱)=\bar{۰}$. در نتیجه $f(-i)=f((-۱)i)=f(-۱)+f(i)=\bar{۰}$. پس

$$Ker(f)=\{x\in\mathbb{Q}_۸\mid f(x)=\bar{۰}\}=\{۱,-۱,i,-i\}$$

تمرین ۸۱.۹.۲. *نشان دهید همریختی گروهی از $S_۳$ به $\mathbb{Z}_۳$ وجود ندارد.*

حل. فرض کنیم $f:S_۳\longrightarrow\mathbb{Z}_۳$ یک همریختی گروهی باشد. طبق قضیه اول یکریختی، قضیه ۳۵.۹.۲، داریم $S_۳/Ker(f)\cong Im(f)$. اما $\mathbb{Z}_۳$ یک گروه آبلی ساده است (چرا؟) و لذا تمام زیرگروه‌های آن نرمال هستند از جمله $Im(f)$. بنابراین $Im(f)=\{\bar{۰}\}$ یا $Im(f)=\mathbb{Z}_۳$. اگر $Im(f)=\{\bar{۰}\}$ آنگاه $Ker(f)=S_۳$ و باید f همریختی بدیهی باشد. اگر $Im(f)=\mathbb{Z}_۳$ آنگاه چون مرتبه $S_۳$ برابر با ۶ است و $|\mathbb{Z}_۳|=۳$، باید $|Ker(f)|=۲$ باشد (چگونه؟). پس $Ker(f)$ یک زیرگروه مرتبه ۲ است و لذا از نتیجه ۲۵.۷.۲ دوری است. زیرگروه‌های مرتبه ۲ باید با عنصر مرتبه ۲ تولید شوند (چرا؟). اما طبق نمادهای مثال ۷.۳.۲، چنین زیرگروه‌های $S_۳$ نرمال نیستند. مثلا زیرگروه $N=<\sigma_۶>=\{\sigma_۱,\sigma_۶\}$ نرمال نیست. زیرا $\sigma_۲\sigma_۶\sigma_۲^{-۱}\notin N$.

تمرین ۸۲.۹.۲. *گروه‌های مرتبه کمتر از ۶ را رده‌بندی کنید.*

حل. فرض کنیم G گروهی از مرتبه کمتر از ۶ باشد. اگر $|G|=۱$ آنگاه واضح است $G=\{e\}$. پس فقط یک گروه مرتبه ۱ وجود دارد. حال فرض کنیم مرتبه G اعداد اول ۲، ۳ و ۵ باشد. چنین گروه حتما ساده است (چرا؟) و طبق تمرین ۶۳.۲.۲ آبلی هستند. پس طبق قضیه ۷۷.۹.۲ باید G به ترتیب $\mathbb{Z}_۲$، $\mathbb{Z}_۳$ و $\mathbb{Z}_۵$ باشد. اکنون فرض کنیم $|G|=۴$ یعنی $G=\{e,a,b,c\}$ که e عنصر خنثی است. حال از نتیجه ۲۴.۷.۲ دو حالت داریم.
(الف) یک عنصر از بین a، b و c مرتبه ۴ است. در این صورت طبق قضیه ۱۸.۶.۲، G دوری از مرتبه ۴ است. پس طبق قضیه ۳۳.۹.۲ باید $G\cong\mathbb{Z}_۴$.
(ب) همه عناصر a، b و c از مرتبه ۲ هستند. واضح است که اگر $ab=e$ آنگاه $b=a^{-۱}$ و لذا $a=b$ و این تناقض است. اگر $ab=a$ انگاه $b=e$ که تناقض است. اگر $ab=b$ آنگاه $a=e$ که باز هم تناقض است. پس باید $ab=c$. با روندی مشابه $bc=a$ و $ac=b$. این کدام گروه است؟ واضح است $\mathbb{K}_۴$ است. در خلال متن درس هم که دیده‌اید، $\mathbb{K}_۴\cong\mathbb{Z}_۲\times\mathbb{Z}_۲$.

تمرین ۸۳.۹.۲. *فرض کنیم $f:G\longrightarrow H$ یک همریختی گروهی باشد و $x\in G$. نشان دهید که $o(f(x))\mid o(x)$. اگر f یک‌به‌یک باشد آنگاه تساوی برقرار است.*

حل. فرض کنیم $o(x)=n$ و $o(f(x))=m$. حال چون $x^n=e$ و f همریختی گروهی است داریم $e_H=f(e_G)=f(x^n)=(f(x))^n$ و لذا طبق گزاره ۱۷.۶.۲ باید $m|n$.
برای قسمت دوم، چون $f(x^m)=(f(x))^m=e_H$، پس $x^m\in Ker(f)$. اما طبق گزاره ۳۲.۹.۲ باید $x^m=e_G$. لذا طبق گزاره ۱۷.۶.۲ باید $n|m$. درنتیجه $m=n$ است.

تمرین ۸۴.۹.۲. *یک همریختی گروهی از گروه S_3 به گروه دوری نابدیهی پیدا کنید.*

حل. یک گروه دوری طبق قضیه ۳۳.۹.۲ باید $\mathbb{Z}$ یا $\mathbb{Z}_n$ باشد که $n \in \mathbb{N}$. اگر $f : S_3 \longrightarrow \mathbb{Z}$ یک همریختی گروهی نابدیهی باشد آنگاه $Im(f)$ یک زیرگروه متناهی از $\mathbb{Z}$ است (چرا؟). اما $\mathbb{Z}$ زیرگروه متناهی ندارد، مگر این که $Im(f) = \{0\}$. این یعنی f همریختی بدیهی است که تناقض است. فرض کنیم $f : S_3 \longrightarrow \mathbb{Z}_n$ یک همریختی گروهی نابدیهی باشد که $n \in \mathbb{N}$. طبق قضیه اول یکریختی، قضیه ۳۵.۹.۲، داریم $S_3/Ker(f) \cong Im(f)$. اگر $Ker(f) = \{e\}$ باشد آنگاه S_3 یک گروه آبلی می‌شود که تناقض آشکار است. اگر $Ker(f) = S_3$ آنگاه f همریختی بدیهی است که تناقض است. چون مرتبه S_3 برابر با ۶ است پس طبق قضیه لاگرانژ، قضیه ۲۳.۷.۲، فقط حالت‌های $ker(f)$ از مرتبه ۲ و ۳ مانده است. فرض کنیم $Ker(f)$ یک زیرگروه مرتبه ۲ باشد. لذا از نتیجه ۲۵.۷.۲ دوری است. زیرگروه‌های مرتبه ۲ باید با عنصر مرتبه ۲ تولید شوند (چرا؟). اما طبق نمادهای مثال ۷.۳.۲، چنین زیرگروه‌های S_3 نرمال نیستند. مثلا زیرگروه $N =< \sigma_6 >= \{\sigma_1, \sigma_6\}$ نرمال نیست. زیرا $\sigma_2\sigma_6\sigma_2^{-1} \notin N$.

فرض کنیم $Ker(f)$ یک زیرگروه مرتبه ۳ باشد. لذا از نتیجه ۲۵.۷.۲ دوری است. زیرگروه‌های مرتبه ۳ باید با عنصر مرتبه ۳ تولید شوند (چرا؟). اما طبق نمادهای مثال ۷.۳.۲، داریم

$$Ker(f) =< \sigma_2 >= \{\sigma_1, \sigma_2, \sigma_3\}.$$

حال کافی گروه دوری مرتبه ۲ از $\mathbb{Z}_2$ انتخاب کنیم و سپس اعضای $Ker(f)$ را به $\bar{0}$ بنگاریم و باقیمانده اعضا S_3 را به عضو $\bar{1}$ بنگاریم.

تمرین ۸۵.۹.۲. *فرض کنیم $f : G \longrightarrow H$ یک یکریختی گروهی باشد. نشان دهید که $x^n = e_G$ اگر و تنها اگر $(f(x))^n = e_H$. آیا این مطلب برای همریختی صحیح است؟*

حل. فرض کنیم $x^n = e_G$. داریم $e_H = f(e_G) = f(x^n) = (f(x))^n$. برعکس، فرض کنیم $(f(x))^n = e_H$. پس $f(x^n) = e_H$. اما $f(e_G) = e_H$ و چون f یک‌به‌یک است باید $x^n = e_G$.

برای قسمت دوم، این مطلب برای هر همریختی صحیح نیست. طبق نمادهای مثال ۷.۳.۲، داریم

$$N =< \sigma_2 >= \{\sigma_1, \sigma_2, \sigma_3\}.$$

حال کافی گروه $\mathbb{Z}_2$ را انتخاب کنیم و سپس اعضای N را به $\bar{0}$ بنگاریم و باقیمانده اعضا S_3 را به عضو $\bar{1}$ بنگاریم. واضح است که $\sigma_2^3 = \sigma_1$. اما σ_2 به عنصر خنثی $\bar{0}$ نگاشته می‌شود که مرتبه ۱ است.

تمرین ۸۶.۹.۲. *نشان دهید که D_n با گروه مرتبه ۲ همریخت است.*

حل. طبق تمرین ۳۲.۶.۲ داریم

$$D_n = \{e, \sigma, ..., \sigma^{n-1}, \tau, \sigma\tau, \sigma^2\tau, ..., \sigma^{n-1}\tau\}.$$

اکنون قرار می‌دهیم

$$f : D_n \longrightarrow \mathbb{Z}_2 \qquad f(e) = f(\sigma^i) = \bar{0}, \;\; f(\tau) = f(\sigma^i\tau) = \bar{1}.$$

یک بررسی سر راست نشان می‌دهد که f همریختی گروهی پوشا است.

تمرین ۸۷.۹.۲. نشان دهید که $Aut(S_3) \cong S_3 \cong Inn(S_3)$ *(چنین گروهی را کامل نامند).*

حل. به یاد آورید که $Z(S_3) = \{e\}$ (تمرین ۳۸.۴.۲). پس طبق قضیه ۵۷.۹.۲ داریم $S_3/Z(S_3) \cong S_3 \cong Inn(S_3)$. حال فرض کنیم $f : S_3 \longrightarrow S_3$ یک خودریختی باشد. طبق نمادهای مثال ۷.۳.۲ و تمرین ۸۵.۹.۲، چون σ_2 مرتبه ۳ دارد، پس f باید آن را به σ_2 یا σ_3 بنگارد. همچنین، چون σ_4 مرتبه ۲ دارد، پس f باید آن را به σ_4 و یا σ_5 و یا σ_6 بنگارد. اما واضح است که σ_2 و σ_4 مولدهای S_3 هستند. لذا طبق اصل ضرب $6 = 3 \times 2$ انتخاب برای f وجود دارد. اما $Inn(S_3) \subseteq Aut(S_3)$ و $|Inn(S_3)| = 6$، پس $Aut(S_3) = Inn(S_3)$.

تمرین ۸۸.۹.۲. نشان دهید که $|Aut(\mathbb{Z}_n)| = \varphi(n)$ *(φ تابع اویلر است).*

حل. فرض کنیم $f : \mathbb{Z}_n \longrightarrow \mathbb{Z}_n$ یک خودریختی باشد. می‌دانیم $\mathbb{Z}_n =< \bar{1} >$. پس کافی است اثر f را روی $\bar{1}$ بدانیم تا کل f برای ما معلوم شود. فرض کنیم $f(\bar{1}) = \bar{t}$. چون $\bar{1}$ مولد است، باید $\bar{t}$ نیز بر طبق تمرین ۸۵.۹.۲، مولد باشد. پس باید $o(\bar{t}) = n$. لذا طبق تمرین ۲۹.۶.۲ باید $(n,t) = 1$. زیرا اگر $(n,t) = d \neq 1$ آنگاه $o(\bar{t}) = \frac{n}{d}$ که تناقض است. حال طبق تمرین ۵۹.۲.۲ باید $\bar{t} \in U(\mathbb{Z}_n)$. حال تعریف می‌کنیم

$$\theta : Aut(\mathbb{Z}_n) \longrightarrow U(\mathbb{Z}_n), \quad \theta(f) = f(\bar{1}).$$

با مطلب بالا، خوشتعرفی θ واضح است. θ همریختی گروهی است. زیرا

$$\begin{aligned}
&\theta(fg) = fg(\bar{1}) = f(g(\bar{1})) \overset{g(\bar{1})=\bar{t}}{=} f(\bar{t}) = \\
&f(\underbrace{\bar{1} + \bar{1} + ... + \bar{1}}_{\text{تا}t}) = tf(\bar{1}) = g(\bar{1})f(\bar{1}) = \\
&f(\bar{1})g(\bar{1}) = \theta(f)\theta(g).
\end{aligned}$$

θ یک‌به‌یک است. زیرا اگر $f \in Ker(\theta)$ آنگاه $\theta(f) = \bar{1}$ و این یعنی $f(\bar{1}) = \bar{1}$. پس برای هر $\bar{m} \in \mathbb{Z}_n$ داریم

$$\bar{m} = m.\bar{1} = mf(\bar{1}) = \underbrace{f(\bar{1}) + ... + f(\bar{1})}_{\text{تا}m} = f(\underbrace{\bar{1} + \bar{1} + ... + \bar{1}}_{\text{تا}m}) = f(\bar{m})$$

یعنی $f = id_{\mathbb{Z}_n}$. حال طبق گزاره ۳۲.۹.۲ باید θ یک‌به‌یک باشد.
θ پوشا است. زیرا اگر $\bar{m} \in U(\mathbb{Z}_n)$ آنگاه $(m,n) = 1$ و طبق مطلبی که در اول اشاره شد، $\bar{m}$ مولد است و لذا می‌توانیم خودریختی

$$f : \mathbb{Z}_n \longrightarrow \mathbb{Z}_n, \;\; f(\bar{1}) = \bar{m}$$

را در نظر بگیریم و $\theta(f) = \bar{m}$. بنابراین $Aut(\mathbb{Z}_n) \cong U(\mathbb{Z}_n)$ و می‌دانیم $|U(\mathbb{Z}_n)| = \varphi(n)$.

تمرین ۸۹.۹.۲. *نشان دهید که:*
(الف) اگر $H \cong G$ آنگاه $Aut(G) \cong Aut(H)$.
(ب) $Aut(\mathbb{K}_4)$ را به دست آورید.
(ج) سپس نتیجه بگیرید که اگر $Aut(G) \cong Aut(H)$ آنگاه لزومی ندارد که $G \cong H$.

حل. (الف) فرض کنیم $f : G \longrightarrow H$ یکریختی بین G و H را معلوم کند. حال تعریف می‌کنیم

$$\theta : Aut(G) \longrightarrow Aut(H), \;\; \theta(g) = fgf^{-۱}.$$

خوشتعرفی θ واضح است. θ همریختی گروهی است. زیرا

$$\theta(gg') = fgg'f^{-۱} = fgf^{-۱}\; fg'f^{-۱} = \theta(g)\theta(g').$$

θ یک‌به‌یک است. زیرا اگر $g \in Ker(\theta)$ آنگاه $\theta(f) = id_H$ و این یعنی $fgf^{-۱} = id_H$. لذا با ضرب‌های (در حقیقت ترکیب توابع مناسب) مناسب داریم $f = id_G$. حال طبق گزاره ۳۲.۹.۲ باید θ یک‌یه‌یک باشد.
θ پوشا است. زیرا اگر $h \in Aut(H)$ آنگاه $f^{-۱}hf \in Aut(G)$ و $\theta(f^{-۱}hf) = h$. بنابراین $Aut(G) \cong Aut(H)$.
(ب) هر هریختی گروهی عنصر خنثی را به عنصر خنثی می‌نگارد. پس برای تعیین $f \in Aut(\mathbb{K}_۴)$ کافی است اثر f را روی سه عنصر a، b و c از $\mathbb{K}_۴$ بدانیم. از طرفی می‌خواهیم f یک‌به‌یک و پوشا باشد! پس f مشابه یک جایگشت روی سه شی a، b و c است که همواره $f(e) = e$. تعداد چنین جایگشت‌های ۶ تا است و از این رو این گروه همان گروه $S_۳$ است که فقط شکل ظاهری عناصر آن تغییر کرده و $f(e) = e$ به هر عنصر اضافه شده است (حتما تمرین ۷۰.۱۲.۲ را ببینید).
(ج) در تمرین بالا دیدیم که $Aut(S_۳) \cong S_۳ \cong Aut(\mathbb{K}_۴)$. در حالی که به وضوح داریم $S_۳ \ncong \mathbb{K}_۴$.

تمرین ۹۰.۹.۲. *فرض کنیم G یک گروه متناهی باشد که دقیقا یک زیرگروه ماکسیمال دارد. نشان دهید که G دوری است.*

حل. فرض کنیم M تنها زیرگروه ماکسیمال از G باشد و $a \in G \setminus M$. اکنون ادعا می‌کنیم $G =< a >$. به برهان خلف فرض کنیم $G \neq< a >$. چون G متناهی است، تعداد زیرگروه‌ها نیز متناهی است و لذا هر زیرگروه یا خودش ماکسیمال است یک در یک زیرگروه ماکسیمال قرار می‌گیرید. در نتیجه $< a >$ باید ماکسیمال باشد یا در زیرگروه ماکسیمال قرار گیرد. اما طبق فرض تنها یک زیرگروه ماکسیمال در G وجود دارد. پس باید $M =< a >$ یا $< a >\subseteq M$ که هر دو شرط $a \in G \setminus M$ را نقض می‌کنند. ادعا اثبات شد.

تمرین ۹۱.۹.۲. *نشان دهید که برای زیرگروه ماکسیمال M از گروه G، یا M نرمال است یا برای هر $g \in G$ داریم $g \in< M, gMg^{-۱} >$.*

حل. می‌دانیم که $M \leq N_G(M) \leq G$. چون M زیرگروه ماکسیمال است، باید $M = N_G(M)$ یا $N_G(M) = G$. اگر $N_G(M) = G$ آنگاه M نرمال است. حال فرض کنیم $N_G(M) = M$ و $g \in G$. اگر $gMg^{-۱} \neq M$ آنگاه $M \lneq< M, gMg^{-۱} >\leq G$. چون M ماکسیمال است باید $G =< M, gMg^{-۱} >$ و لذا $g \in< M, gMg^{-۱} >$. اگر $M = gMg^{-۱}$ آنگاه $g \in N_g(M)$. اما $N_G(M) = M$ و لذا $g \in< M, gMg^{-۱} >$.

تمرین ۹۲.۹.۲. *آیا گروه $G = (\mathbb{Q} \setminus \{۰\}, .)$ زیرگروه (نرمال) ماکسیمال دارد؟*

حل. ابتدا دقت کنید که گروه آبلی است و لذا همه زیرگروه‌ها نرمال هستند. حال ادعا می‌کنیم

$$\mathbb{Q}^+ = \{x \in G \mid x > ۰\} = M$$

زیرگروه ماکسیمال است. فرض کنیم $M \lneq M' \leq G$. پس عنصر $x \in M' \setminus M$ وجود دارد که $x < ۰$. لذا $-x \in Q^+ = M$ و در نتیجه $-x \in M'$. چون M' زیرگروه است پس $\frac{۱}{x} \in M'$ و لذا $-x.\frac{۱}{x} \in M'$. دوباره طبق زیرگروه بودن داریم $-۱ = \mathbb{Q}^- = -\mathbb{Q}^+ \subseteq M'$. در نتیجه $G = \mathbb{Q}^+ \cup \mathbb{Q}^- = M'$. پس M زیرگروه (نرمال) ماکسیمال است.

تمرین ۹۳.۹.۲. *فرض کنیم G گروهی آبلی متناهی از مرتبه n باشد و m عدد صحیحی باشد که نسبت به n اول است. در این صورت $f: G \longrightarrow G$ با ضابطه $f(x) = x^m$ خودریختی است.*

حل. چون G آبلی است، f همریختی است. زیرا

$$f(xy) = (xy)^m = \underbrace{xy\ xy\ ...\ xy}_{m\text{تا}} = x^m y^m = f(x)f(y).$$

اگر $x \in Ker(f)$ آنگاه $f(x) = e$ و لذا $x^m = e$. پس $o(x) \mid m$ (چرا؟). اما $x^n = e$ (چرا؟) پس $o(x) \mid n$. در نتیجه $o(x) \mid (m,n) = ۱$ و لذا $x = e$. حال طبق گزاره ۳۲.۹.۲ باید f یک‌به‌یک باشد. فرض کنیم $y \in G$. طبق قضیه بزو، قضیه ۱۰.۲.۱ داریم $rn + sm = ۱$ که $r, s \in \mathbb{Z}$. بنابراین $y = y^{rn+sm} = (y^s)^m$. بنابراین داریم $f(y^s) = y$. یعنی f پوشا است.

تمرین ۹۴.۹.۲. *نشان دهید هر گروه G دارای عنصری مانند y باشد که $y^۲ \neq e$، داری دست کم دو خودریختی است.*

حل. برای هر گروه G همواره id_G یک همریختی گروهی است. اکنون اگر G آبلی باشد آنگاه

$$f: G \longrightarrow G, \quad f(x) = x^{-۱}$$

یک همریختی است (اولین تمرین حل شده این بخش). فقط دقت کنید که چون $y^۲ \neq e$ پس $y \neq y^{-۱}$ و لذا $f \neq id_G$. اگر G آبلی نباشد آنگاه برای هر $x \in G \setminus Z(G)$، همریختی داخلی f_x را خواهیم داشت.

تمرین ۹۵.۹.۲. *تمام همریختی‌ها از $\mathbb{Q}$ به $\mathbb{Z}$ را پیدا کنید.*

حل. فرض کنیم $f: \mathbb{Q} \longrightarrow \mathbb{Z}$ یک همریختی گروهی باشد. همچنین فرض کنیم $f(۱) = t$. حال برای هر عدد طبیعی n داریم

$$t = f(۱) = f(n.\frac{۱}{n}) = f(\underbrace{\frac{۱}{n} + ... + \frac{۱}{n}}_{n\text{تا}}) = nf(\frac{۱}{n}).$$

اما $f(\frac{۱}{n}) \in \mathbb{Z}$ و تساوی بالا یعنی برای هر عدد طبیعی n داریم $t \mid n$. پس t بیشمار شمارنده دارد که چنین چیزی امکان ندارد مگر این که $t = ۰$. پس $f(۱) = ۰$ و این یعنی $f(-۱) = ۰$. اما برای هر عدد طبیعی n داریم

$$۰ = f(۱) = f(n.\frac{۱}{n}) = f(\underbrace{\frac{۱}{n} + ... + \frac{۱}{n}}_{n\text{تا}}) = nf(\frac{۱}{n}).$$

در نتیجه $f(\frac{۱}{n}) = ۰$ و لذا $f(\frac{-۱}{n}) = ۰$. اکنون عدد گویا و مثبت $\frac{m}{n}$ را در نظر بگیرید. داریم

$$f(\frac{m}{n}) = f(m.\frac{۱}{n}) = f(\underbrace{\frac{۱}{n} + ... + \frac{۱}{n}}_{m\text{تا}}) = mf(\frac{۱}{n}) = ۰.$$

به روش مشابه برای اعداد گویای منفی نیز مطلب بالا صحیح است. لذا f فقط همریختی بدیهی است.

تمرین ۹۶.۹.۲ *$Aut(\mathbb{Q})$ را به دست آورید.*

حل. فرض کنیم $f : \mathbb{Q} \longrightarrow \mathbb{Q}$ یک خودریختی گروهی باشد. واضح است که $f(۰) = ۰$. فرض کنیم $t = f(۱)$. حال برای هر عدد طبیعی n داریم

$$f(n) = \underbrace{۱ + ۱ + ... + ۱}_{n\text{تا}} = nf(۱) = nt$$

همچنین $۰ = f(۰) = f(n-n) = f(n)+f(-n) = nt+f(-n)$ و لذا $f(-n) = -nt$. پس برای هر $n \in \mathbb{Z}$ نشان داده‌ایم که $f(n) = nt$. حال فرض کنیم $x = \frac{n}{m} \in \mathbb{Q}$. داریم

$$nt = f(n) = f(mx) = mf(x)$$

در نتیجه $f(x) = t\frac{n}{m} = tx$. یک بررسی ساده نشان می‌دهد که

$$f : \mathbb{Q} \longrightarrow \mathbb{Q}, \;\; f(x) = tx$$

یک خودریختی گروهی است. چون f دلخواه بود تمام خودریختی‌ها شناسایی شد.

۱۰.۲ قضایای گروه‌های جایگشتی

بسیار خوب! به آخرین بخش این فصل رسیدیم. بخشی که تمام نظریه گروه است. اگر شخصی قضیه کیلی را بداند، جمله قبل زیاده گویی نیست. در اولین قدم، قضیه کیلی را اثبات می‌کنیم. سپس به شما نشان می‌دهیم که چرا با وجود دانستن قضیه کیلی باز هم مطالعه نظریه گروه دشوار است (حتما بخش سوم این فصل را با دقت مطالعه نمایید).

قضیه ۱.۱۰.۲. (*قضیه کیلی*) *هر گروه G با گروه جایگشتی یکریخت است (هر زیرگروه، گروه متقارن را گروه جایگشتی گوییم).*

اثبات. فرض کنیم $a \in G$. قرار می‌دهیم

$$l_a : G \longrightarrow G, \;\; l_a(x) = ax.$$

l_a یک تناظر است. خوشتعریفی l_a واضح است. داریم

$$l_a(x) = l_a(y) \;\Rightarrow\; ax = ay \;\Rightarrow\; x = y$$

و لذا l_a یک تابع یک‌به‌یک است. اگر $y \in G$ باشد آنگاه $a^{-۱}y \in G$ و داریم $l_a(a^{-۱}y) = aa^{-۱}y = y$. پس l_a پوشا است. اکنون فرض کنیم S_G گروه متقارن روی مجموعه (گروه) G باشد (قضیه ۲.۳.۲ را ببینید). قرار می‌دهیم

$$\theta : G \longrightarrow S_G, \;\; \theta(x) = l_x.$$

در بالا نشان دادیم که l_x تناظر است و لذا خوشتعریفی θ واضح است. θ همریختی گروه است. زیرا برای هر $g \in G$ داریم

$$\theta(xy)(g) = l_{xy}(g) = xyg = x(yg) = x(l_y(g)) = l_x l_y(g) = \theta(x)\theta(y)(g).$$

پس $\theta(xy) = \theta(x)\theta(y)$. اما θ یک نشاننده است یعنی یک‌به‌یک است. زیرا اگر $x \in Ker(\theta)$ آنگاه $\theta(x) = id_G = l_e$ و لذا $l_x = l_e = id_G$. بنابراین باید $x = e$ (چگونه؟). پس طبق گزاره ۳۲.۹.۲، باید θ نشاننده باشد. طبق قضیه اول یکریختی، قضیه ۳۵.۹.۲ داریم $G \cong Im(\theta) \leq S_G$ و اثبات تمام است. $\square$

قضیه کیلی آنقدر واضح انگیزه مطالعه گروه‌های جایگشتی را مشخص می‌کند که لازم به پر حرفی نیست! اما ما نمی‌توانیم گروه‌های جایگشتی دلخواه را در همین دوره مقدماتی بررسی کنیم. از این رو تمرکز اصلی ما در ادامه روی گروه S_n است و خواهید دید که همین گروه متناهی مطالعه‌اش به حد کافی دردسر دارد.

تعریف ۲.۱۰.۲. *فرض کنیم $\sigma \in S_n$. اگر اعداد طبیعی $x_۱$، $x_۲$، ...، x_r از مجموعه $\{۱, ۲, ..., n\}$ موجود باشد که $\sigma(x_i) = x_{i+۱}$ و برای $x \notin \{x_۱, ..., x_r\}$ داشته باشیم $\sigma(x) = x$، گوییم σ یک دور به طول r است و از نمایش ماتریسی σ پرهیز می‌کنیم و می‌نویسیم $(x_۱ \; x_۲ \; ... \; x_r)$.*

مثال ۳.۱۰.۲. طبق نمادهای مثال ۷.۳.۲ داریم

$$\sigma_۲ = (۱\ ۲\ ۳) \qquad \sigma_۵ = (۱\ ۲)$$

مثال ۴.۱۰.۲. $(۲\ ۴\ ۵\ ۷) = \sigma$ یک دور به طول ۴ در $S_۷$ است. در این دور $\sigma(۱) = ۱$، $\sigma(۳) = ۳$ و $\sigma(۶) = ۶$ است.

تعریف ۵.۱۰.۲. هر دور به طول ۲ را یک ترانهش گوییم.

مثال ۶.۱۰.۲. $(۱\ ۷) = \sigma$ یک ترانهش در $S_۷$ است. طبق نمادهای مثال ۷.۳.۲، $\sigma_۴ = (۲\ ۳)$، $\sigma_۵ = (۱\ ۳)$ و $\sigma_۶ = (۱\ ۲)$ ترانهش در $S_۳$ هستند.

تعریف ۷.۱۰.۲. دو دور $(x_۱\ x_۲\ \dots\ x_r)$ و $(y_۱\ y_۲\ \dots\ y_s)$ مجزا گوییم هرگاه

$$\{x_۱ x_۲, \dots, x_r\} \cap \{y_۱, y_۲, \dots, y_s\} = \emptyset.$$

مثال ۸.۱۰.۲. دو دور $(۱\ ۲\ ۳)$ و $(۴\ ۵\ ۶\ ۷)$ مجزا هستند. اما دو دور $(۱\ ۷)$ و $(۱\ ۲\ ۶\ ۵)$ مجزا نیستند.

حال گزاره زیر را داریم.

گزاره ۹.۱۰.۲. موارد زیر در S_n برقرار هستند.
(الف) هر دور به طول r دارای مرتبه r است.
(ب) هر دو دور مجزا با هم جابجا می‌شوند.

اثبات. (الف) فرض کنیم $\sigma = (x_۱\ x_۲\ \dots\ x_r)$ یک دور به طول r باشد. حال داریم که

$$\sigma^۲ = \begin{pmatrix} x_۱ & x_۲ & x_۳ & \dots & x_{r-۱} & x_r \\ x_۳ & x_۴ & x_۵ & \dots & x_۱ & x_۲ \end{pmatrix}$$

واضح است که بعد از r مرحله به جایگشت همانی می‌رسیم.
(ب) فرض کنیم $\sigma = (x_۱\ x_۲\ \dots\ x_r)$ و $\tau = (y_۱\ y_۲\ \dots\ y_s)$ دو دور مجزا باشند. بدون کم شدن از کلیت فرض کنیم

$$\{۱, ۲, \dots, n\} = \{x_۱, x_۲, \dots, x_r, y_۱, y_۲, \dots, y_s, z_۱, \dots, z_t\}.$$

اکنون داریم

$$\sigma\tau = \begin{pmatrix} x_۱ & \dots & x_r & y_۱ & \dots & y_s & z_۱ & \dots & z_t \\ x_۲ & \dots & x_۱ & y_۱ & \dots & y_s & z_۱ & \dots & z_t \end{pmatrix} \begin{pmatrix} x_۱ & \dots & x_r & y_۱ & \dots & y_s & z_۱ & \dots & z_t \\ x_۱ & \dots & x_r & y_۲ & \dots & y_۱ & z_۱ & \dots & z_t \end{pmatrix}$$
$$= \begin{pmatrix} x_۱ & x_۲ & \dots & x_r & y_۱ & \dots & y_s & z_۱ & \dots & z_t \\ x_۲ & x_۳ & \dots & x_۱ & y_۲ & \dots & y_۱ & z_۱ & \dots & z_t \end{pmatrix} =$$
$$\begin{pmatrix} x_۱ & \dots & x_r & y_۱ & \dots & y_s & z_۱ & \dots & z_t \\ x_۱ & \dots & x_r & y_۲ & \dots & y_۱ & z_۱ & \dots & z_t \end{pmatrix} \begin{pmatrix} x_۱ & \dots & x_r & y_۱ & \dots & y_s & z_۱ & \dots & z_t \\ x_۲ & \dots & x_۱ & y_۱ & \dots & y_s & z_۱ & \dots & z_t \end{pmatrix}$$
$$= \tau\sigma$$

و اثبات کامل است. □

حال گزاره زیر را داریم.

گزاره ۲.۱۰.۱۰. *اگر $\sigma \in S_n$ آنگاه σ به صورت حاصل ضربی از دورهای مجزا تجزیه نمود که صرف نظر از ترتیب آمدن دورها، این تجزیه یکتا است.*

اثبات. حکم را با استقرا روی n اثبات می‌کنیم. اگر $n = ۱$ باشد آنگاه چیزی برای اثبات نداریم. فرض کنیم حکم برای هر عدد طبیعی کمتر از n برقرار باشد و سپس برای عدد n حکم را اثبات می‌کنیم. طبق قضیه ۸.۳.۲ داریم $|S_n| = n!$ و لذا طبق نتیجه ۱۹.۶.۲، عدد طبیعی k وجود دارد که $\sigma^k = I$. پس می‌توانیم فرض کنیم کوچکترین عدد طبیعی r با شرط $\sigma^r(i) = i$ موجود است که $i \in \{۱, ۲, ..., n\}$ و برای هر $s < r$، $\sigma^s(i) \neq i$. پس یک دور به شکل زیر در دل σ وجود دارد

$$\sigma_۱ = (i \ \sigma(i) \ \sigma^۲(i) \ ... \ \sigma^{r-۱}(i)).$$

حال فرض کنیم

$$A = \{۱, ۲, ..., n\} \setminus \{i, \sigma(i), \sigma^۲(i), ..., \sigma^{r-۱}(i)\}.$$

اگر A تهی باشد آنگاه σ یک دور است و ما اثبات را تمام کرده‌ایم. اگر A ناتهی باشد آنگاه $\tau = \sigma|_A$ یک جایگشت روی $n - r$ حرف است و طبق فرض استقرا داریم $\tau = \sigma_۲\sigma_۳...\sigma_k$ که تجزیه به دورهای مجزا از هم برای τ است. حال واضح است که $\sigma = \sigma_۱\tau = \sigma_۱\sigma_۲\sigma_۳...\sigma_k$.
برای قسمت یکتایی، فرض کنیم σ به دو شکل تجزیه به دورهای مجزا داشته باشد، یعنی

$$\sigma_۱\sigma_۲\sigma_۳...\sigma_k = \sigma = \tau_۱\tau_۲...\tau_l.$$

حال عنصر $m \in \{۱, ۲, ..., n\}$ را در نظر بگیرید. اگر m در هیچ کدام از σ_iها ظاهر نشود آنگاه باید $\sigma(m) = m$ باشد و لذا m در هیچ کدام از τ_iها هم ظاهر نمی‌شود. پس فرض کنیم $\sigma_۱(m) \neq m$ و لذا m در یک σ_j ظاهر شود، مثلا در $\sigma_۱$. لذا داریم $\sigma_۱ = (m \ \ \sigma(m) \ \ \sigma^۲(m) \ ... \ \sigma^{t-۱}(m))$ که در آن t کوچکترین عدد طبیعی است که $\sigma^t(m) = m$. از سوی دیگر m توسط σ حرکت می‌کند، لذا باید τ_j چنان موجود باشد که m در آن ظاهر شود. از این رو باید هر $\sigma^s(m)$ در τ_j ظاهر شود. این یعنی $\sigma_۱ = \tau_j$ و از مجزا بودن دورها و گزاره قبل قسمت (ب) داریم

$$\sigma_۱\sigma_۲\sigma_۳...\sigma_k = \tau_j\tau_۲\tau_{j-۱}...\tau_{j+۱}\tau_l.$$

از طرفین $\sigma_۱ = \tau_j$ را ساده می‌کنیم و برای

$$\sigma_۲\sigma_۳...\sigma_k = \tau_۲\tau_{j-۱}...\tau_{j+۱}\tau_l.$$

روند بالا را تکرار می‌کنیم. لذا باید $k = l$ و $\sigma_i = \tau_j$. □

مثال ۱۱.۱۰.۲. در $S_۸$ داریم

$$\begin{pmatrix} ۱ & ۲ & ۳ & ۴ & ۵ & ۶ & ۷ & ۸ \\ ۲ & ۳ & ۵ & ۶ & ۴ & ۱ & ۸ & ۷ \end{pmatrix} = (۱\ ۲\ ۳\ ۵\ ۴\ ۶)\ (۷\ ۸)$$

یعنی حاصل ضرب دو دور مجزا است به طول ۶ و ۲ است. همچنین

$$\begin{pmatrix} ۱ & ۲ & ۳ & ۴ & ۵ & ۶ & ۷ & ۸ \\ ۲ & ۳ & ۱ & ۶ & ۴ & ۵ & ۷ & ۸ \end{pmatrix} = (۱\ ۲\ ۳)\ (۴\ ۶\ ۵)$$

یعنی حاصل ضرب دو دور مجزا به طول ۳ است که ۷ و ۸ را ثابت نگه می‌دارد. همچنین

$$\begin{pmatrix} ۱ & ۲ & ۳ & ۴ & ۵ & ۶ & ۷ & ۸ \\ ۴ & ۳ & ۲ & ۱ & ۶ & ۵ & ۸ & ۷ \end{pmatrix} = (۱\ ۴)\ (۲\ ۳)\ (۵\ ۶)\ (۷\ ۸)$$

یعنی حاصل ضرب چهار دور (ترانهش) مجزا است. همچنین

$$\begin{pmatrix} ۱ & ۲ & ۳ & ۴ & ۵ & ۶ & ۷ & ۸ \\ ۷ & ۱ & ۲ & ۳ & ۴ & ۵ & ۸ & ۶ \end{pmatrix} = (۶\ ۵\ ۴\ ۳\ ۲\ ۱\ ۷\ ۸)$$

یعنی حاصل ضرب یک دور است.

نتیجه ۱۲.۱۰.۲. هر جایگشت را می‌توان به تعدادی ترانهش تجزیه کرد.

اثبات. طبق گزاره ۱۰.۱۰.۲ هر جایگشت حاصل ضربی از دورها است. حال دور $(x_۱\ x_۲\ \dots\ x_r)$ را می‌توان به شکل

$$(x_۱\ x_۲)\ (x_۲\ x_۳)\ \dots\ (x_{r-۱}\ x_r)$$

به ترانهش‌ها تجزیه کرد. اثبات کامل است. □

مثال ۱۳.۱۰.۲. می‌خواهیم نشان دهیم که

$$S_n =< (۱\ ۲\ ۳\ \dots\ n-۱),\ (n-۱\ \ n) > .$$

یک بررسی ساده نشان می‌دهد که برای هر $۱ \leq k \leq n-۱$ داریم

$$(۱\ ۲\ ۳\ \dots\ n-۱)^k(n-۱\ \ n)(۱\ ۲\ ۳\ \dots\ n-۱)^{-k} = (k\ n).$$

یعنی تمام اعضا به شکل $(k\ n)$ را در اختیار داریم و در نتیجه خواهیم داشت

$$(i\ j) = (i\ n)\ (j\ n)\ (i\ n)$$

و لذا تمام ترانهش‌ها را در اختیار داریم. اکنون با کمک نتیجه ۱۲.۱۰.۲ ، تمام جایگشت‌ها را می‌توانیم تولید کنیم.

تذکر ۲.۱۰.۱۴. *دورها را نمی‌توان لزوما به ترانهش‌های مجزا تجزیه کرد. مثلا دور* $(۱\ ۲\ ۳)$ *سه حرف را حرکت می‌هد و اگر به دو ترانهش مجزای* $(a\ b)\ (c\ d)$ *تجزیه شود آنگاه ۴ حرف حرکت داد می‌شود که امکان پذیر نیست.*

نیاز به تعریف دو مفهوم داریم.

تعریف ۲.۱۰.۱۵. *فرض کنیم* $\sigma \in S_n$ *و* $\sigma = \sigma_۱\sigma_۲...\sigma_k$ *تجزیه به دورهای مجزا با دو ویژگی زیر باشد.*
(۱) دورهای به طول ۱ را در این تجزیه نوشته باشیم.
(۲) دورها از روی طول‌شان صعودی مرتب شده باشند. یعنی اگر σ_i *دارای طول* n_i *باشد آنگاه* $n_۱ \leq n_۲ \leq ... \leq n_k$ *(دقت شود که دورها متمایزند و می‌توانیم در صورت لزوم آن ها جابجا کنیم).*
حال به هر σ *بردار منحصر به فرد* $(n_۱, n_۲, ..., n_k)$ *با شرط* $n_۱ \leq n_۲ \leq ... \leq n_k$ *نسبت می‌دهیم که* $\sum_{i=۱}^k n_i = n$*. به این بردار ساختمان دوری* σ *گوییم.*

مثال ۲.۱۰.۱۶. جایگشت $\sigma = (۱\ ۲\ ۳)\ (۶\ ۸)$ *را داخل* $S_۸$ *در نظر بگیرید. اگر دورهای طول ۱ را وارد کنیم و با توجه به طول آن ها از دور با طول کم به دور با طول زیاد مرتب کنیم، آنگاه داریم* $\sigma = (۴)\ (۵)\ (۷)\ (۶\ ۸)\ (۱\ ۲\ ۳)$*. لذا ساختمان دوری* σ *بردار* $(۱, ۱, ۱, ۲, ۳)$ *است و دقت کنید که* $۸ = ۳ + ۲ + ۱ + ۱ + ۱$.

تذکر ۲.۱۰.۱۷. *دقت شود که هر ساختمان دوری یک جایگشت را مشخص می‌کند. اما این جایگشت لزوما یکتا نیست. در مثال قبل ساختمان دوری* $(۱, ۱, ۱, ۲, ۳)$ *علاوه بر* σ *مثلا نمایش جایگشت زیر نیز می‌باشد*

$$\tau = (۶)\ (۷)\ (۸)\ (۱\ ۲)\ (۳\ ۴\ ۵) = (۱\ ۲)\ (۳\ ۴\ ۵).$$

اما چطور می‌توانیم از روی ساختمان دوری، روی جایگشت‌ها متفاوتی که حاصل می‌شود کنترل داشته باشیم؟ پاسخ این سوال در قضیه زیر است.

تعریف ۲.۱۰.۱۸. گوییم $\sigma \in S_n$ *مزدوج* $\tau \in S_n$ *است هرگاه* $\alpha \in S_n$ *موجود باشد که* $\tau = \alpha\sigma\alpha^{-۱}$.

مثال ۲.۱۰.۱۹. جایگشت $(۱\ ۲\ ۴)$ مزدوج جایگشت $(۱\ ۴\ ۲)$ *است. زیرا*

$$(۱\ ۲)\ (۱\ ۲\ ۴)\ (۱\ ۲)^{-۱} = (۱\ ۲)\ (۱\ ۲\ ۴)\ (۱\ ۲) = (۱\ ۴\ ۲).$$

تذکر ۲.۱۰.۲۰. *یک بررسی ساده نشان می‌دهد که رابطه مزدوج بودن در جایگشت‌ها یک رابطه هم ارزی است.*

قضیه ۲.۱۰.۲۱. *هر دو جایگشت مزدوج ساختمان دوری یکسان دارند. برعکس، اگر دو جایگشت دارای ساختمان دوری یکسان باشند، مزدوج هستند.*

اثبات. فرض کنیم σ و $\tau = \alpha\sigma\alpha^{-1}$ که $\alpha \in S_n$ در S_n مزدوج باشند. طبق گزاره ۱۰.۱۰.۲، σ و τ حاصل ضرب مجزایی از دورها هستند. چون ساختمان دوری در ارتباط مستقیم با دور به طول r است، کافی است حکم را برای دور به طول r اثبات کنیم. یعنی نشان دهیم دور به طول r که در σ ظاهر شده است دقیقا در τ نیز ظاهر می‌شود. پس فرض کنیم $\sigma = (x_1\ x_2\ ...\ x_r)$ یک دور به طول r در σ باشد. چون α^{-1} جایگشت است، از نقطه نظر مجموعه‌ای داریم

$$\{1, 2, ..., n\} = \{\alpha^{-1}(1), \alpha^{-1}(2), ..., \alpha^{-1}(n)\}.$$

فرض کنیم $\alpha^{-1}(x) \notin \{x_1, ..., x_r\}$. پس

$$\alpha\ (x_1\ x_2\ ...\ x_r)\alpha^{-1}(x) = x.$$

اگر $\alpha^{-1}(x) = x_i$ آنگاه

$$\alpha\ (x_1\ x_2\ ...\ x_r)\alpha^{-1}(x) = \alpha(x_{i+1}).$$

پس نشان داده‌ایم

$$\alpha\ (x_1\ x_2\ ...\ x_r)\alpha^{-1} = (\alpha(x_1)\ \alpha(x_2)\ ...\ \alpha(x_r)).$$

که یک دور τ است.
فرض کنیم $(n_1, n_2, ..., n_k)$ ساختمان دوریب σ و τ باشد. لذا داریم

$$\begin{aligned}\sigma &= (x_1\ x_2\ ...\ x_{n_1})\ (x_{n_1+1}\ ...\ x_{n_1+n_2})\ ...\ (x_{n-n_k+1}\ ...\ x_{n_k})\\ \tau &= (y_1\ y_2\ ...\ y_{n_1})\ (y_{n_1+1}\ ...\ y_{n_1+n_2})\ ...\ (y_{n-n_k+1}\ ...\ y_{n_k})\end{aligned}$$

حال تعریف می‌کنیم $\alpha(x_i) = y_i$. واضح است که $\alpha \in S_n$. یک بررسی ساده نشان می‌دهد $\tau = \alpha\sigma\alpha^{-1}$. □

حال گزاره زیر را داریم.

قضیه ۲۲.۱۰.۲. *فرض کنیم σ در S_n حاصل ضربی از r ترانهش و همچنین حاصل ضربی از s ترانهش باشد. در این صورت r و s هر دو زوج یا هر دو فرد هستند.*

اثبات. فرض کنیم $\sigma_1...\sigma_r = \sigma = \tau_1...\tau_s$. قرار می‌دهیم

$$P = (x_1 - x_2)(x_1 - x_3)...(x_1 - x_n)\ (x_2 - x_3)\ ...\ (x_2 - x_n)\ ...\ (x_{n-1} - x_n) = \prod_{1 \le i < j \le n} (x_i - x_j).$$

همچنین برای هر $\alpha \in S_n$ تعریف می‌کنیم

$$\alpha(P) = \prod_{1 \le i < j \le n} (x_{\alpha(i)} - x_{\alpha(j)}).$$

برای ترانهش $\alpha=(l\ t)$ که $l<t$ نشان می‌دهیم $\alpha(P)=-P$. اگر x_l-x_t یک عامل P باشد آنگاه واضح است که $x_{\alpha(l)}-x_{\alpha(k)}$ یک عامل $\alpha(P)$ است. حال سه حالت زیر رخ می‌دهد.
(الف) زمانی که $i,j\not\in\{l,t\}$ واضح است که $x_{\alpha(i)}-x_{\alpha(j)}=x_i-x_j$. همچنین عامل x_l-x_t در P به عامل $x_{\alpha(l)}-x_{\alpha(t)}=x_t-x_l=-(x_l-x_t)$ در $\alpha(P)$ تبدیل می‌شود. یعنی در این حالت داریم $\alpha(P)=-P$.
(ب) زمانی که $i\not\in\{l,t\}$ یک حالت $l<i<t$ است، ضرب‌های $(x_l-x_i)(x_t-x_l)(x_i-x_t)$ در P وجود دارند. پس حاصل ضرب

$$\begin{aligned}&(x_{\alpha(l)}-x_{\alpha(i)})(x_{\alpha(t)}-x_{\alpha(l)})(x_{\alpha(i)}-x_{\alpha(t)})=\\&(x_t-x_i)(x_l-x_t)(x_i-x_l)=-(x_l-x_i)(x_t-x_l)(x_i-x_t)\end{aligned}$$

در $\alpha(P)$ وجود دارد. یعنی در این حالت داریم $\alpha(P)=-P$. حالت‌های باقیمانده مانند $l<t<i$ را خودتان بررسی کنید.
(ج) برای زمانی که $i,j\in\{l,t\}$ داریم که عامل x_i-x_j در P به عامل

$$x_{\alpha(i)}-x_{\alpha(j)}=x_t-x_l=-(x_l-x_t)$$

در $\alpha(P)$ تبدیل می‌شود. سایر عوامل تغییری نمی‌کنند، یعنی در این حالت داریم $\alpha(P)=-P$.
بنابراین اثر ترانهش ها یک تغییر علامت است و لذا

$$(-۱)^rP=\sigma_۱...\sigma_r(P)=\sigma(P)=\tau_۱...\tau_s(P)=(-۱)^sP.$$

در نتیجه $(-۱)^s=(-۱)^r$ و لذا r و s هر دو زوج یا هر دو فرد هستند. $\square$

قضیه بالا ما را به سمت تعریف زیر سوق می‌دهد.

تعریف ۲۳.۱۰.۲. گوییم $\sigma\in S_n$ زوج (فرد) است هرگاه بتوان آن را حاصل ضرب زوج (فرد) ترانهش نوشت.

مثال ۲۴.۱۰.۲. در $S_۸$ جایگشت

$$\sigma=\begin{pmatrix}۱&۲&۳&۴&۵&۶&۷&۸\\۴&۳&۲&۱&۶&۵&۸&۷\end{pmatrix}=(۱\ ۴)\ (۲\ ۳)\ (۵\ ۶)\ (۷\ ۸)$$

زوج است. جایگشت

$$\tau=\begin{pmatrix}۱&۲&۳&۴&۵&۶&۷&۸\\۴&۳&۲&۱&۶&۵&۷&۸\end{pmatrix}=(۱\ ۴)\ (۲\ ۳)\ (۵\ ۶)$$

فرد است.

برای ادامه به یک تابع مهم نیاز داریم که در تعریف زیر می‌آوریم.

تعریف ۲.۱۰.۲۵. گروه ضربی $\mathbb{Z}_2 = \{-1, 1\}$ را در نظر بگیرید. به تابع

$$\begin{cases} sgn : S_n \longrightarrow S_n \\ \qquad sgn(\sigma) = \begin{cases} 1 & \sigma \text{زوج} \\ -1 & \sigma \text{فرد} \end{cases} \end{cases}$$

تابع علامت گوییم.

مثال ۲.۱۰.۲۶. در S_8 جایگشت

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

زوج است و لذا $sgn(\sigma) = 1$. جایگشت

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

فرد است و لذا $sgn(\tau) = -1$. اگر σ زوج (فرد) باشد آنگاه σ^{-1} زوج (فرد) است.

تذکر ۲.۱۰.۲۷. جایگشت همانی را زوج حساب می‌کنیم. چون تعداد صفر دور است!

لم ۲.۱۰.۲۸. sgn یک همریختی گروهی است.

اثبات. اگر σ و τ هر دو زوج باشند آنگاه $\sigma\tau$ زوج است و لذا

$$sgn(\sigma\tau) = 1 = 1.1 = sgn(\sigma)sgn(\tau).$$

اگر σ و τ هر دو فرد باشند آنگاه $\sigma\tau$ زوج است و لذا

$$sgn(\sigma\tau) = 1 = (-1).(-1) = sgn(\sigma)sgn(\tau).$$

اگر σ زوج و τ فرد باشد آنگاه $\sigma\tau$ فرد است و لذا

$$sgn(\sigma\tau) = -1 = 1.(-1) = sgn(\sigma)sgn(\tau).$$

اثبات کامل است. $\square$

لم ۲.۱۰.۲۹. مجموعه همه جایگشت‌های زوج، A_n، یک زیرگروه نرمال ماکسیمال S_n است (و به آن گروه متناوب مرتبه n گوییم). به علاوه $|A_n| = \frac{n!}{2}$.

اثبات. اگر $n = ۱$ باشد چیزی برای اثبات نداریم. فرض کنیم $n \geq ۲$. واضح است که جایگشت همانی زوج است و A_n ناتهی است. اما

$$Ker(sgn) = \{\sigma \in S_n \mid sgn(\sigma) = ۱\} = A_n.$$

چون هسته هر همریختی زیرگروه نرمال است، A_n زیرگروه نرمال است. از نتیجه ۴۹.۹.۲ و این که گروه مرتبه ۲ ساده است، ماکسیمال بودن A_n حاصل می‌شود. برای قسمت دوم، چون $n \geq ۲$، $\sigma = (a\ b)$ دور به طول ۱ است و $sgn(\sigma) = -۱$. عنصر خنثی گروه $\mathbb{Z}_۲$ یعنی ۱ با جایگشت همانی پوشش داده می‌شود و لذا sgn پوشا است. طبق قضیه اول یکریختی، قضیه ۳۵.۹.۲ داریم $S_n/A_n \cong \mathbb{Z}_۲$. حال طبق قضیه لاگرانژ، قضیه ۲۳.۷.۲ داریم $[S_n : A_n] = \frac{|S_n|}{|A_n|} = |\mathbb{Z}_۲| = ۲$ و $|A_n| = \frac{n!}{۲}$. □

حال قضیه مهم زیر را داریم.

قضیه ۳۰.۱۰.۲. *A_n توسط تمام دورهای به طول ۳ تولید می‌شود.*

اثبات. فرض کنیم $(a\ b\ c)$ یک دور به طول ۳ باشد. داریم

$$(a\ b\ c) = (a\ b)\ (a\ c).$$

این نشان می‌دهد که تمام سه دورها جایگشت‌های زوج هستند و لذا در A_n قرار می‌گیرند. حال فرض کنیم σ یک جایگشت زوج باشد. طبق تعریف باید σ حاصل ضرب زوج تا ترانهش باشد، یعنی

$$\sigma = (a_۱\ b_۱)\ (a_۲\ b_۲)\ \ldots\ (a_{۲k}\ b_{۲k}).$$

اکنون برای ترکیب دو ترانهش $(a\ b)\ (c\ d)$ که همانی نیست و مجزا نباشند یعنی $b = c$، داریم

$$(a\ b)\ (c\ d) = (a\ b)\ (b\ d) = (a\ b\ d).$$

برای ترکیب دو ترانهش $(a\ b)\ (c\ d)$ که همانی نیست و مجزا هستند، داریم

$$(a\ b)\ (c\ d) = (a\ b\ c)\ (b\ c\ d).$$

این یعنی σ حاصل ضرب دورهای به طول ۳ است. دقت شود که چون تعداد دورها زوج است می‌توانیم دو تا دو تا ترانهش از σ انتخاب کنیم. □

نتیجه ۳۱.۱۰.۲. *برای $n \geq ۳$ داریم* $S'_n = A_n$.

اثبات. در اثبات لم ۲۹.۱۰.۲ دیدیم که $S_n/A_n \cong \mathbb{Z}_۲$. اما $\mathbb{Z}_۲$ آبلی است و طبق قضیه ۲۵.۸.۲ باید $S'_n \subseteq A_n$. اما هر دور به طول ۳ یک جابجاگر است. زیرا

$$(a\ b\ c) = (a\ b)\ (a\ b\ c)\ (a\ b)^{-۱}\ (a\ b\ c)^{-۱}.$$

لذا هر دور به طول ۳ در S'_n قرار دارد و $A_n \subseteq S'_n$. اثبات کامل است. □

نتیجه زیر را بدون اثبات از ما بپذیرید.

نتیجه ۳۲.۱۰.۲. *اگر $n > ۴$ آنگاه گروه A_n ساده است و گروه مشتق مرتبه iام گروه S_n برابر A_n است، یعنی $S_n^{(i)} = A_n$.*

وقت آن است که به وعده خود عمل کنیم و نشان دهیم عکس قضیه لاگرانژ صحیح نیست! فصل اول را با همین مثال به پایان می‌رسانیم.

مثال ۳۳.۱۰.۲. *طبق لم ۲۹.۱۰.۲ داریم $|A_۴| = ۱۲$. نشان می‌دهیم $A_۴$ زیرگروه مرتبه ۶ ندارد هر چند $۶|۱۲$. فرض کنیم H زیرگروه مرتبه ۶ از $A_۴$ باشد. داریم که $[A_۴ : H] = ۲$ و طبق گزاره ۸.۸.۲ باید H نرمال باشد. حال سه جایگشت*

$$\sigma = (۱\ ۲)(۳\ ۴) \qquad \tau = (۱\ ۳)(۲\ ۴) \qquad \beta = (۱\ ۴)(۲\ ۳)$$

را در نظر بگیرید. جایگشت همانی را الحاق کنید به سه جایگشت بالا، یک بررسی ساده نشان می‌دهد که یک زیرگروه چهار عضوی در $A_۴$ ساخته‌اید (که اتفاقا یکریخت با $\mathbb{K}_۴$ است). این زیرگروه را K بنامید. $H \cap K$ هم زیرگروه H است و هم زیرگروه K و طبق قضیه لاگرانژ، قضیه ۲۳.۷.۲، باید $|H \cap K|\ |\ |K|$ و $|H \cap K|\ |\ |H|$. لذا $|H \cap K|$ باید ۱ یا ۲ باشد. اگر $|H \cap K| = ۱$ آنگاه طبق قضیه ۳۱.۴.۲ داریم $|HK| = ۲۴$ که تناقض آشکار است. پس $|H \cap K| = ۲$. حال فرض کنیم $v = (i\ j)\ (a\ b)$ هر بار یکی از σ، τ و β باشد. چون H نرمال است، پس $(i\ j\ a)v(i\ j\ a)^{-۱} = (j\ a)(i\ b) \in H$. این یعنی $|H \cap K| > ۲$ و تناقض است.

تمرین‌های حل شده

تمرین ۳۴.۱۰.۲. *نشان دهید که $S_n =< (۱\ ۲), (۱\ ۳), ..., (۱\ n) >$.*

حل. یک بررسی ساده نشان می‌دهد که $(i\ j) = (۱\ i)\ (۱\ j)\ (۱\ i)$ و لذا تمام ترانهش‌ها را در اختیار داریم. پس طبق نتیجه ۱۲.۱۰.۲ دیگر چیزی برای حل نداریم.

تمرین ۳۵.۱۰.۲. *نشان دهید که $S_n =< (۱\ ۲), (۲\ ۳), ..., (n-۱\ \ n) >$.*

حل. فرض کنیم $H =< (۱\ ۲), (۲\ ۳), ..., (n-۱\ \ n) >$. نشان می‌دهیم $(۱\ j) = (۱\ \ j-۱)\ (j-۱\ \ j)\ (۱\ \ j-۱)$ که در آن $j \geq ۲$. اگر $j = ۲$ باشد آنگاه واضح است که $(۱\ ۲) \in H$. اگر $j = ۳$ باشد آنگاه $(۱\ ۲)\ (۲\ ۳)\ (۱\ ۲) \in H$. اما حاصل $(۱\ ۲)\ (۲\ ۳)\ (۱\ ۲)$ برابر است با $(۱\ ۳)$. در نتیجه $(۱\ ۳) \in H$. اگر $j = ۴$ باشد آنگاه $(۱\ ۳)\ (۳\ ۴)\ (۱\ ۳) \in H$. اما حاصل $(۱\ ۳)\ (۳\ ۴)\ (۱\ ۳)$ برابر است با $(۱\ ۴)$. در نتیجه $(۱\ ۴) \in H$. استقرایی ادامه دهید. لذا تمام $(۱\ j)$ را در اختیار داریم و طبق تمرین قبل حل کامل است.

تمرین ۳۶.۱۰.۲. *نشان دهید که $S_n =< (۱\ ۲\ ...\ n),\ (۱\ ۲) >$.*

حل. یک بررسی ساده نشان می‌دهد که $(i\ \ i+۱) = (۱\ ۲\ ...\ n)^{i-۱}\ (۱\ ۲)\ (۱\ ۲\ ...\ n)^{-(i-۱)}$ که در آن $i \geq ۱$. لذا تمام $(i\ \ i+۱)$ را در اختیار داریم و طبق تمرین قبل حل کامل است.

تمرین ۳۷.۱۰.۲. جایگشت $(۱\ ۷\ ۶\ ۵)\ (۶\ ۲\ ۴\ ۳)\ (۵\ ۱\ ۲\ ۴) = \sigma$ را به صورت دورهای جدا از هم بنویسید.

حل. با کمی محاسبه داریم که

$$\sigma = \begin{pmatrix} ۱ & ۲ & ۳ & ۴ & ۵ & ۶ & ۷ \\ ۴ & ۶ & ۲ & ۱ & ۳ & ۷ & ۵ \end{pmatrix} = (۱\ ۴)(۲\ ۶\ ۷\ ۵\ ۳).$$

تمرین ۳۸.۱۰.۲. *نشان دهید که مرتبه هر $\sigma \in S_n$ برابر است با کوچکترین مضرب مشترک دورهای که در تجزیه σ ظاهر می‌شوند.*

حل. فرض کنیم $\sigma = \sigma_۱ ... \sigma_k$ تجزیه به دورهای مجزای σ باشد. همچنین فرض کنیم $o(\sigma_i) = m_i$، $o(\sigma) = m$ و c کوچکترین مضرب مشترک m_i ها باشد. طبق گزاره ۹.۱۰.۲ دورها مجزا با هم جابجا می‌شوند لذا

$$e = \sigma^m = \sigma_۱^m ... \sigma_k^m \ \Rightarrow\ \sigma_i^m = e.$$

پس باید $m_i \mid m$ (چرا؟). در نتیجه $c \mid m$. اما $c = l_i m_i$ و لذا

$$\sigma^c = \sigma_۱^c ... \sigma_k^c = (\sigma_۱^{m_۱})^{l_۱} ... (\sigma_k^{m_k})^{l_k} = e.$$

بنابراین $m \mid c$ و حل کامل است.

تمرین ۳۹.۱۰.۲. *فرض کنیم $H \lneq S_n$ و $H \nsubseteq A_n$. نشان دهید دقیقا نصف جایگشت‌های H زوج هستند.*

حل. طبق لم ۲۹.۱۰.۲، A_n یک زیرگروه ماکسیمال (حتی نرمال ماکسیمال) است و $|A_n| = \frac{n!}{۲}$. طبق نتیجه ۱۳.۸.۲ داریم $A_n \trianglelefteq A_n H$ و لذا از نرمال ماکسیمال بودن A_n و فرض $H \nsubseteq A_n$ باید $A_n H = S_n$. حال طبق قضیه ۳۱.۴.۲ داریم

$$n! = |S_n| = |A_n H| = \frac{|A_n|\ |H|}{|H \cap A_n|} \leq |A_n|\ |H| = \frac{n!}{۲}|H|.$$

پس $|H| \geq \frac{n!}{۲}$. چون $|H| \mid n!$ (چرا؟) باید $|H| = \frac{n!}{۲}$. در نتیجه

$$n! = |S_n| = |A_n H| = \frac{|A_n|\ |H|}{|H \cap A_n|} = \frac{n!\ n!}{۴|H \cap A_n|}.$$

لذا $|H \cap A_n| = \frac{n!}{۴} = \frac{۱}{۲}|H|$ و چون تمام جایگشت‌های زوج در A_n حضور دارند، ادعای تمرین صحیح است.

تمرین ۴۰.۱۰.۲. *تعداد دورهای به طول r را در S_n حساب کنید.*

حل. برای ساختن یک دور به طول r در S_n نیاز به انتخاب r شی از n شی را داریم که تکرار هم مجاز نیست، این یعنی $P(n,r)=\frac{n!}{(n-r)!}$. اما می‌دانیم که در یک دور عنصر شروع کننده مهم نیست، یعنی مثلا دور (۳ ۲ ۱) با دور (۱ ۳ ۲) یکسان است. اما تعداد چنین دورهای به طول r که عنصر شروع کننده مهم نباشد دقیقا r تا است. لذ تعداد دورهای به طول r برابر است با $\frac{n!}{r(n-r)!}$.

تمرین ۴۱.۱۰.۲. *فرض کنیم σ یک دور به طول m در S_n باشد. تعداد مزدوج‌های σ را حساب کنید.*

حل. طبق قضیه ۲۱.۱۰.۲ می‌دانیم که σ و مزدوج‌هایش دورهای به طول m هستند. لذا طبق تمرین قبل باید تعداد دورها به طول m را حساب کنیم یعنی $\frac{n!}{m(n-m)!}$.

تمرین ۴۲.۱۰.۲. *نشان دهید که اگر $n>4$ انگاه A_n تنها زیرگروه نرمال نابدیهی از S_n است.*

حل. فرض کنیم H زیرگروه نرمال نابدیهی از S_n باشد. اگر $H\cap A_n=\{e\}$ آنگاه طبق قضیه ۳۱.۴.۲ و لم ۲۹.۱۰.۲ داریم

$$|A_nH|=\frac{|A_n|\,|H|}{|A_n\cap H|}=|A_n|\,|H|\leq n!\,.$$

پس $|H|\leq 2$. اما H نابدیهی است پس $H=\{e,\sigma\}$. چون H نرمال است، باید برای هر $\alpha\in S_n$ داشته باشیم $\alpha\sigma\alpha^{-1}=\sigma$. این یعنی $\sigma\in Z(S_n)$. می‌دانیم که $Z(S_n)=\{e\}$ (تمرین ۳۸.۴.۲) و لذا $\sigma=e$ که تناقض است. لذا $H\cap A_n\neq\{e\}$. در این صورت طبق نتیجه ۱۳.۸.۲، $H\cap A_n$ در A_n نرمال است. اما طبق نتیجه ۳۲.۱۰.۲، A_n ساده است و لذا $H\cap A_n=A_n$. پس $A_n\subseteq H$ و نرمال ماکسیمال بودن A_n از لم ۲۹.۱۰.۲ باید $H=A_n$ یا $H=S_n$.

تمرین ۴۳.۱۰.۲. *نشان دهید که A_n تنها زیرگروه S_n از اندیس ۲ است.*

حل. طبق لم ۲۹.۱۰.۲ و قضیه لاگرانژ، قضیه ۲۳.۷.۲ می‌دانیم که $[S_2:A_n]=\frac{S_n}{A_n}=2$. حال فرض کنیم $S_n\not\leq H$ و $[S_n:H]=2$. چون اندیس H در G برابر ۲ است، طبق گزاره ۸.۸.۲، H نرمال است. از این رو مرتبه گروه G/H برابر با ۲ است و لذا اگر (۳ ۲ ۱) در H نباشد آنگاه $H\in$ (۳ ۲ ۱)^2 $=$ (۲ ۳ ۱) است (چرا؟). اما طبق قضیه ۲۱.۱۰.۲ همه دورها با طول ۳ با (۲ ۳ ۱) مزدوج هستند و چون H نرمال است، شامل تمام ۳ دورها است. پس طبق قضیه ۳۰.۱۰.۲داریم $H\subseteq A_n$ و طبق لم ۲۹.۱۰.۲، A_n نرمال ماکسیمال است و باید $H=A_n$.

۱۱.۲ تاریخچه

اواریست گالوا (۲۵ اکتبر ۱۸۱۱– ۳۱ مه ۱۸۳۲) ریاضی‌دان فرانسوی بود. گالوا از پیشگامان مطالعه نظریه گروه‌ها است؛ و با کارهای او بود که نقطه عطفی در جبر ایجاد شد و محاسبات اهمیت خود را از دست دادند و به جای آنها مفاهیم و ساختارهایی همانند گروه، حلقه و میدان اهمیت پیدا کردند. از دستاوردهای مهم نظریه گالوا حل چند مسئلهٔ مشهور بود که از زمانهای دور مطرح بودند. یکی از آنها اثبات این مطلب است که حل جبری کلی (به کمک رادیکال‌ها) برای چندجمله‌ای‌های درجه ۵ و بالاتر وجود ندارد. همین‌طور با کمک نظریات گالوا ثابت شد مسئله‌های کهن تثلیث زاویه و تربیع دایره حل ناپذیر هستند.

در ۱۲ سال اوّل زندگی، گالوا توسط مادرش تعلیم دید و او زمینهٔ خوبی از آموزش کلاسیک را به وی منتقل نمود. گالوا در دو سال اوّل مدرسه خوب ظاهر شد و اولین جایزه را نیز تصاحب کرد اما بعداً کم‌حوصلگی شروع شد و مجبور شد که کلاس‌های سال آخر را تکرار نماید و این امر ملال خاطر وی را بدتر کرد. در همین دوره بود که گالوا به ریاضیات علاقه‌مند شد. او به نسخه‌ای از نوشته لژاندر به نام «اصول هندسه» برخورد کرد که محتوای پر ارزش آن، اصول اقلیدسی هندسه متداول در مدرسه را نقض می‌کرد. گفته می‌شود که وی این نوشته را شبیه به یک داستان خواند و در یک مرتبه خواندن بر آن مسلّط گردید. کتاب‌های درس جبر دبیرستان قادر بر برابری با شاهکار لژاندر نبودند لذا گالوا به مقالات علمی لژاندر و آبل روی آورد. در ۱۵ سالگی مطالبی را مطالعه می‌کرد که برای ریاضی‌دانان حرفه‌ای نوشته شده بود. این کار باعث عدم اشتیاق به مطالب کلاسی گردید و به نظر می‌رسد که رغبت‌هایش به فراگیری مطالب کلاسی از بین رفته باشد. معلّمانش او را درک نمی‌کردند و با تکبّر و تبحّر وی را طرد می‌نمودند.

همان‌گونه که از بعضی از نسخه‌های خطّی او دیده می‌شود، گالوا در کارهایش نامرتّب بود و مایل بود که کارهایش را در مغز خود انجام دهد و تنها نتایج عملیّات ذهنی خود را روی کاغذ منتقل می‌کرد. معلمّش ورنیه از او می‌خواست که به‌طور منظّم کار کند اما گالوا به توصیه‌های او توجه نمی‌کند. او بدون آمادگی کافی در امتحانات ورودی مدرسه پلی‌تکنیک شرکت کرد. گذشتن از این امتحان احتمالاً موفقیّت او را تضمین می‌کرد زیرا پلی‌تکنیک مکان مناسبی برای رشد ریاضیات فرانسه بود، اما او در این امتحانات با داستانی عجیب قبول نشد. دو دهه بعد دانشمند فرانسوی تراکوم سردبیر مجله ی علمی Mathématiques de Annales Nouvelles این شرح را نوشت: «داوطلبی با نبوغ عالی توسط ممتحنی با استعداد کم رد می‌شود...»

در سال ۱۸۲۸ گالوا وارد دانشسرای عالی شد که سایه کم رنگی از پلی‌تکنیک بود و در یک کلاس پیشرفته ریاضیات توسط ریاضی دان فرانسوی ریشارد(Richard) شرکت نمود. ایشان نسبت به گالوا نظر کاملاً موافقی داشتند. ریشارد دارای این عقیده بود که گالوا بایستی بدون امتحان در پلی‌تکنیک پذیرفته شود. سال بعد، اولین مقاله گالوا را که نشانی از نبوغ او نداشت دربارهٔ کسرهای مسلسل مشاهده کرد. در همین حال گالوا در نظریه معادلات چند جمله‌ای‌ها به کشفیّات اساسی دست‌یافت و برخی از نتایج آن را نیز به آکادمی علوم ارائه نمود. داور آگوستین لویی کوشی (۱۸۵۷–۱۷۸۹) بود که قبلاً در مورد رفتار توابع تحت جایگشت متغیّرها که موضوع مرکزی نظریه گالوا بود، کارش را به چاپ رسانده بود. کشی مقاله را رد کرد و مقاله دیگری نیز که هشت روز بعد ارائه شد به همین حال دچار شد. نسخه‌های خطّی گم شد و دیگر پیدا نشدند.

گالوا بر اثر فعالیت‌های ضد حکومت فرانسه به زندان سنت پلاژی انداخته شد و پس از مدتی به

دلیل وضع وخیم جسمانی، وی را به درمانگاه فرستادند و از آنجا با فردی به نام «آنتوان» آشنا می‌شود. اواریست طی ملاقاتی که برای هم اتاقی وی یعنی آنتوان ترتیب داده شده بود دو دختر را می‌بیند که یکی از آنها ژانا نام دارد و گویا دوست دختر آنتوان است. گالوا سخت از همراه ژانا خوشش می‌آید و طی پرسش و پاسخی از آنتوان متوجه می‌شود که نام آن دختر «اوا سورل» (از وی اغلب به عنوان D Stephanie یاد می‌شود) بوده و آن دختر هم متقابلاً مجذوب گالوا است و گویا او را قهرمان خود می‌داند. بهرحال گالوا و دختر مورد علاقه وی طی جلساتی با هم آشنا شده و سرانجام گالوا از علاقه خود پرده برداشته و اوا را متوجه این موضوع می‌کند. در مقابل دختر هم از وی یک روز فرصت می‌خواهد تا بیشتر فکر کند. روز بعد اوا سورل طبق قرار از پیش تعیین شده اواریست را می‌بیند و به وی می‌گوید «دیروز قول دادم که بیایم. این آخرین دیدار ماست ...شما خودتان گفتید که به صراحت نیاز دارید، گوش کنید، من معشوقه کسی هستم که او را خیلی دوست دارم. او میهن‌پرست است. او شش هفته در پاریس نبود. می‌خواستم کسی مرا به رستوران‌ها و چایخانه‌های درجه اول ببرد و دربارهٔ انقلاب و آزادی برایم صحبت کند...» اواریست که از این سخنان سخت عصبانی شده بود، ردیفی از ناسزا را نثار وی کرد و مکالمات آنها سرانجام با این سخن اوا سورل پایان میابد: «از من دوری کنید. سوگند می‌خورم از آنچه گفته‌اید پشیمان خواهید شد آقای گالوا، این حرف آخر من است» در پی این مشاجرات سرانجام دو نفر به نام‌های «موریس لورن» که پسر عموی اوا سورل هم بود و دیگری «پشو دربنویل» (D'Herbinville) گالوا را به دوئلی در بین ویل فرا خواندند. در آخر گالوا در بیست ونهم ماه مه، در شب دوئل آسیبی جدی می‌بیند و در بیمارستان زندگی وی پایان می‌پذیرد.

گالوا به دلیل قضیه اساسی خود که رابطی بین گروه‌ها و حلقه‌ها است و امروزه آن را قضیه گالوا می‌خوانند بسیار مورد توجه است. شاید اگر گاوا به مرگ طبیعی دچار می‌شد و در سنین جوانی از دنیا نمی‌رفت، ریاضیات قرن ۱۹ رشد بسیار زیادتری می‌داشت و آن رشد ریاضیات امروز را نیز تحت تاثیر قرار می‌داد. آن گونه که از تاریخ بر می‌آید، گالوا شاید به شکل پیوسته چند ماه از عمر خود را به ریاضی پرداخته است و در این مدت کم دستاوردش بسیار بسیار عمیق بوده است.

۱۲.۲ تمرین‌های کل فصل

تمرین‌هایی که با علامت $(\star)$ یا $(\star\star)$ مشخص شده‌اند، زحمت بیشتری را می‌طلبند.

تمرین ۱.۱۲.۲. آیا $\mathbb{C} \longrightarrow \mathbb{C} \times \mathbb{C} : *$ با ضابطه $a * b = a^b$ یک عمل دوتایی است؟

تمرین ۲.۱۲.۲. اگر S مجموعه متناهی باشد آنگاه چند عمل دوتایی جابجایی روی S وجود دارد؟

تمرین ۳.۱۲.۲. آیا $\mathbb{R} \longrightarrow \mathbb{R} \times \mathbb{R} : *$ با ضابطه $a * b = \min\{a, b\}$ جابجایی است؟ شرکت پذیر چطور؟

تمرین ۴.۱۲.۲. نشان دهید که $(\mathbb{R}, *)$ که $a * b = a + b + ab$ یک گروه است.

تمرین ۵.۱۲.۲. نشان دهید که $\mathbb{Q}[\sqrt{۲}] \setminus \{۰ + ۰\sqrt{۲}\}$ با عمل دوتایی زیر یک گروه است.

$$(a + b\sqrt{۲}) \cdot (a' + b'\sqrt{۲}) = (aa' + ۲bb') + (a'b + ab')\sqrt{۲}$$

تمرین ۶.۱۲.۲. نشان دهید که ماتریس‌های وارون پذیر با درایه‌های از اعداد حقیقی که دترمینان برابر با ۱ دارند با عمل دوتایی ضرب عادی ماتریس، یک گروه است (این گروه را با $SL_n(\mathbb{R})$ نشان می‌دهیم).

تمرین ۷.۱۲.۲. برای مجموعه X، $(\mathbb{P}(X), *)$ که در آن $*$ همان تفاضل متقارن مجموعه‌ها (یعنی $A * B = (A \cup B) \setminus (A \cap B)$) است، یک گروه آبلی است.

تمرین ۸.۱۲.۲. فرض کنیم G یک نیم‌گروه متناهی باشد که برای هر $x, y, z \in G$ اگر $xy = yz$ باشد آنگاه $x = z$. نشان دهید که G آبلی است.

تمرین ۹.۱۲.۲. فرض کنیم $G = (-۱, ۱)$ و $a * b = \frac{a+b}{۱+ab}$. نشان دهید که $(G, *)$ گروه است.

تمرین ۱۰.۱۲.۲. فرض کنیم G گروهی باشد که برای هر دو عنصر $g, h \in G$ داریم $g^۲h^۲ = (gh)^۲$. نشان دهید G آبلی است.

تمرین ۱۱.۱۲.۲. فرض کنیم m و n دو عدد نسبت به هم اول باشند. نشان دهید که اگر در گروه G همه توان‌ها mام با همه توان‌های nام جابجا شوند، آنگاه G آبلی است.

تمرین ۱۲.۱۲.۲. فرض کنیم G یک گروه متناهی با عنصر خنثی e باشد. نشان دهید که برای هر $a \in G$ عدد طبیعی n وجود دارد که $a^n = e$.

تمرین ۱۳.۱۲.۲. فرض کنیم $(G, *)$ نیم‌گروه متناهی با عنصر خنثی e باشد. نشان دهید که G گروه است اگر و تنها اگر (فقط) یک عنصر $a \in G$ وجود داشته باشد که $a^۲ = a$.

تمرین ۱۴.۱۲.۲. فرض کنیم $(G, *)$ یک گروه با عنصر خنثی e باشد و $a, b \in G$. اگر $a^۲ = e$ و $a * b^۴ * a = b^۷$ آنگاه نشان دهید که $b^{۳۳} = e$.

تمرین ۱۵.۱۲.۲. نیم‌گروه $(G,*)$ گروه است اگر و تنها اگر G دو شرط زیر را داشته باشد:
(الف) عنصر $e\in G$ موجود است که برای هر $a\in G$ داریم $e*a=a$.
(ب) برای هر $a\in G$ عنصر $b\in G$ وجود دارد که $b*a=e$.

تمرین ۱۶.۱۲.۲. نشان دهید که $(G,*)$ گروه آبلی است اگر و تنها اگر برای هر $a,b\in G$ داشته باشیم $(a*b)^{-۱}=a^{-۱}*b^{-۱}$.

تمرین ۱۷.۱۲.۲. در گروه $D_۴$ یک عنصر چنان پیدا کنید که با خودش ترکیب شود عنصر همانی شود.

تمرین ۱۸.۱۲.۲. برای چه اعداد طبیعی n، S_n و D_n به تعداد یکسان عضو دارند؟

تمرین ۱۹.۱۲.۲. زیرگروه‌های $S_۳$ و $D_۴$ را بنویسید.

تمرین ۲۰.۱۲.۲. نشان دهید که $D_n\leq S_n$.

تمرین ۲۱.۱۲.۲. فرض کنیم H زیرگروهی از گروه G باشد. نشان دهید که برای $A\subseteq G$، $HA=H$ اگر و تنها اگر $A\subseteq H$.

تمرین ۲۲.۱۲.۲. فرض کنیم G یک گروه باشد و $H\leq G$. نشان دهید که $H\cap Z(G)\leq Z(H)$.

تمرین ۲۳.۱۲.۲. در گروه S_n برای $m<n$ یک زیرگروه $m!$ عضوی پیدا کنید.

تمرین ۲۴.۱۲.۲. نشان دهید که $n\mathbb{Z}\times m\mathbb{Z}$ زیرگروه $\mathbb{Z}\times\mathbb{Z}$ است. آیا تمام زیرگروه‌های $\mathbb{Z}\times\mathbb{Z}$ به صورت $n\mathbb{Z}\times m\mathbb{Z}$ است؟

تمرین ۲۵.۱۲.۲. مرکز گروه D_n را به دست آورید.

تمرین ۲۶.۱۲.۲. مرکز ساز زیرمجموعه‌های ناتهی گروه $S_۳$ را به دست آورید.

تمرین ۲۷.۱۲.۲. نشان دهید که گروه $\mathbb{K}_۴$ دوری نیست.

تمرین ۲۸.۱۲.۲. یک زیرگروه مرتبه ۶ در گروه جمعی $\mathbb{Z}_{۲۴}$ پیدا کنید.

تمرین ۲۹.۱۲.۲. $(\star)$ فرض کنیم G یک گروه و H زیرگروهی نابدیهی از G باشد که در هر زیرگروه نابدیهی قرار می‌گیرید. نشان دهید که H در $Z(G)$ قرار می‌گیرید.

تمرین ۳۰.۱۲.۲. فرض کنیم در گروه G برای اعضای x و y داشته باشیم $xy=yx$. همچنین $o(x)=m$ و $o(y)=n$. نشان دهید که اگر $(m,n)=۱$ آنگاه $o(xy)=mn$.

تمرین ۳۱.۱۲.۲. فرض کنیم G گروهی متناهی و T و S زیرمجموعه‌های G باشند که $G\neq ST$. نشان دهید که $|G|>|S|+|T|$.

تمرین ۳۲.۱۲.۲. قضیه ویلسون، قضیه ۲۲.۲.۱، را با کمک نظریه گروه اثبات کنید.

تمرین ۳۳.۱۲.۲. $(\star)$ فرض کنیم p یک عدد اول باشد و عناصر $a_۱$، $a_۲$، ...، $a_{p-۱}$ یک جایگشت از مجموعه $\{۱,۲,...,p-۱\}$ باشد. نشان دهید $i\neq j$ وجود دارد که $ia_i\overset{p}{\equiv}ja_j$.

تمرین ۳۴.۱۲.۲. اگر در گروه G عناصر x و y مرتبه متناهی باشند آنگاه آیا xy مرتبه متناهی است؟

تمرین ۳۵.۱۲.۲. آیا مرتبه همه عناصر گروه جمعی $\prod_{i=1}^{\infty} \mathbb{Z}_{2^i}$ متناهی است؟

تمرین ۳۶.۱۲.۲. فرض کنیم در گروه G برای اعضای x و y داشته باشیم $xy = yx$. همچنین $o(x) = m$ و $o(y) = n$. نشان دهید که عنصر z در G وجود دارد که $o(z)$ کوچکترین مضرب مشترک m و n است.

تمرین ۳۷.۱۲.۲. نشان دهید که در هر گروه آبلی مجموعه همه عناصر از مرتبه متناهی، یک زیرگروه است. برای گروه غیر آبلی یک مثال نقض ارائه کنید.

تمرین ۳۸.۱۲.۲. نشان دهید که اگر گروه G فقط یک عنصر از مرتبه n مانند g داشته باشد آنگاه $C_G(g) = G$.

تمرین ۳۹.۱۲.۲. نشان دهید اندیس زیرگروه $SL_n(\mathbb{R})$ روی $GL_n(\mathbb{R})$ نامتناهی است.

تمرین ۴۰.۱۲.۲. برای هر زیرگروه از یک گروه داده شده، نشان دهید که وارون‌های عناصر یک هم دسته چپ، تشکیل یک هم دسته راست می‌دهند.

تمرین ۴۱.۱۲.۲. $(\star)$ برای اعداد طبیعی m و n، آیا $\frac{(mn)!}{(m!)^n n!}$ یک عدد صحیح است؟

تمرین ۴۲.۱۲.۲. $(\star)$ فرض کنیم G یک گروه باشد و $H \leq G$ که $[G : H] = n$. موارد زیر را رد یا اثبات کنید.
(الف) اگر $g \in G$ آنگاه $g^n \in H$.
(ب) اگر $g \in G$ آنگاه برای $1 \leq i \leq n$ داریم $a^i \in H$.

تمرین ۴۳.۱۲.۲. $(\star)$ گروه G دقیقا سه زیرگروه دارد اگر و تنها اگر G دوری و از مرتبه p^2 باشد که p عدد اول است.

تمرین ۴۴.۱۲.۲. فرض کنیم H_1، H_2، ...، H_n زیرگروه‌های با اندیس متناهی در گروه G باشند. نشان دهید که $[G : \bigcap_{i=1}^{n} H_i] < \infty$ و

$$[G : \bigcap_{i=1}^{n} H_i] \leq \prod_{i=1}^{n} [G : H_i].$$

تمرین ۴۵.۱۲.۲. فرض کنیم N زیرگروه با اندیس دو در گروه G باشد و x و y اعضای N نباشند. نشان دهید که $xy \in N$.

تمرین ۴۶.۱۲.۲. $(\star)$ گروه $G = (\mathbb{C} \setminus \{0\}, .)$ را در نظر بگیرید. اگر H یک زیرگروه باشد که $[G : H] < \infty$ آنگاه نشان دهید که $G = H$.

تمرین ۴۷.۱۲.۲. $(\star\star)$ برای گروه دلخواه G نشان دهید که $[G : Z(G)] < \infty$ اگر و تنها اگر G برابر با اجتماع تعداد متناهی از زیرگروه‌های آبلی خود باشد.

تمرین ۴۸.۱۲.۲. نشان دهید که $SL_n(\mathbb{R})$ در $GL_n(\mathbb{R})$ نرمال است.

تمرین ۴۹.۱۲.۲. فرض کنیم N زیرگروه نرمال گروه G باشد که $[G:N] < \infty$. اگر H یک زیرگروه مرتبه متناهی باشد که ۱ $= ([G:N], |H|)$ آنگاه نشان دهید که $H \subseteq N$.

تمرین ۵۰.۱۲.۲. $(\star)$ در گروه $SL_۲(\mathbb{R})$ نشان دهید که $-I_۲$ (قرینه ماتریس همانی)جابجاگر نیست.

تمرین ۵۱.۱۲.۲. $(\star\star)$ فرض کنیم $G =< x, y \mid xyx^{-۱}y^{-۱} = x >$. در این صورت نشان دهید که $G'' = \{e\}$.

تمرین ۵۲.۱۲.۲. نشان دهید گروه خارج قسمتی یک گروه آبلی، آبلی است.

تمرین ۵۳.۱۲.۲. $(\star)$ برای هر عدد طبیعی k، نشان دهید که در گروه $\mathbb{Q}/\mathbb{Z}$ دقیقا یک زیرگروه دوری از مرتبه k وجود دارد.

تمرین ۵۴.۱۲.۲. برای زیرگروه نرمال N از G و $x \in G$ با شرط ۱ $= (o(x), [G:N])$ نشان دهید که $x \in N$.

تمرین ۵۵.۱۲.۲. تمام زیرگروه‌های نرمال D_n را پیدا کنید.

تمرین ۵۶.۱۲.۲. $(\star)$ فرض کنیم G یک گروه متناهی با زیرگروه نرمال N باشد به طوری که ۱ $= (|N|, [G:N])$. نشان دهید که N تنها زیرگروه G از مرتبه $|N|$ است.

تمرین ۵۷.۱۲.۲. فرض کنیم در گروه خارج قسمتی G/N مرتبه gN متناهی باشد. نشان دهید که مرتبه gN مرتبه g را می‌شمارد. همچنین نشان دهید که $g^m \in N$ اگر و تنها اگر $o(gN) \mid m$.

تمرین ۵۸.۱۲.۲. فرض کنیم G یک گروه و برای هر عدد طبیعی ۲ $m \geq$ و هر $x, y \in G$ داشته باشیم $(xy)^m = x^m y^m$. نشان دهید که $N_m = \{a^m \mid a \in G\}$ نرمال است. مرتبه عناصر گروه G/N_m متناهی است یا نامتناهی؟

تمرین ۵۹.۱۲.۲. $(\star)$ نشان دهید که گروه $\mathbb{Q}/\mathbb{Z}$ زیرگروه سره با اندیس متناهی ندارد.

تمرین ۶۰.۱۲.۲. $(\star)$ فرض کنیم G یک گروه ۱۸۲ عضوی باشد. اگر G یک زیرگروه نرمال از مرتبه ۲ داشته باشد آنگاه نشان دهید که G دوری است.

تمرین ۶۱.۱۲.۲. فرض کنیم G گروهی از مرتبه ۱۰ باشد که یک زیرگروه نرمال مرتبه ۲ دارد. نشان دهید که G آبلی است.

تمرین ۶۲.۱۲.۲. $(\star)$ فرض کنیم G یک گروه باشد که سه زیرگروه نرمال $N_۱$، $N_۲$ و $N_۳$ دارد. اگر برای $i \neq j$ داشته باشیم $N_i \cap N_j = \{e\}$ و $G = N_i N_j$ آنگاه نشان دهید که G آبلی است.

تمرین ۶۳.۱۲.۲. $(\star)$ فرض کنیم G یک گروه باشد که حاوی هیچ زیرگروه از اندیس ۲ نیست. نشان دهید که زیرگروه‌های با اندیس ۳ باید نرمال باشند.

تمرین ۶۴.۱۲.۲. $(\star\star)$ فرض کنید G یک گروه باشد که ۱۳۹۶ عنصر از آن در $Z(G)$ قرار ندارند. ثابت کنید G یک گروه ۱۴۰۰ عضوي است و سپس یک مثال از چنین گروهی ارائه دهید.

تمرین ۶۵.۱۲.۲. ($\star$) فرض کنیم G گروهی است فقط یک زیرگروه غیر نرمال دارد. نشان دهید که هر زیرگروه نامتناهی G نرمال است.

تمرین ۶۶.۱۲.۲. ($\star\star$) فرض کنیم G گروهی از مرتبه ۴۴ باشد که یک زیرگروه غیر دوری مرتبه ۴ دارد. نشان دهید که ۲۰ عضو از G مرتبه بزرگتر از ۲ دارند.

تمرین ۶۷.۱۲.۲. ($\star$) اگر $G = Z(G)G'$ آنگاه نشان دهید که $G' = G''$.

تمرین ۶۸.۱۲.۲. نشان دهید که گروه G آبلی است اگر و تنها اگر $f : G \longrightarrow G$ با ضابطه $f(x) = x^{۲}$ همریختی گروهی باشد.

تمرین ۶۹.۱۲.۲. نشان دهید همریختی گروهی از $S_۳$ به $\mathbb{Z}_۳$ وجود ندارد.

تمرین ۷۰.۱۲.۲. همریختی‌های گروهی از $\mathbb{K}_۴$ به $S_۳$ را پیدا کنید.

تمرین ۷۱.۱۲.۲. نشان دهید هر گروه غیر آبلی از مرتبه ۶ با $S_۳$ یکریخت است.

تمرین ۷۲.۱۲.۲. ($\star$) فرض کنیم G یک گروه ساده باشد و H زیرگروهی دوری از G باشد که نرمال است. در این صورت نشان دهید که عدد اول p وجود دارد که $G \cong \mathbb{Z}_p$.

تمرین ۷۳.۱۲.۲. ($\star$) فرض کنیم G یک گروه و $f : G \longrightarrow G$ یک خودریختی با این ویژگی باشد که $f(x) = x$ اگر و تنها اگر $x = e$. نشان دهید که برای هر $x \in G$ عنصر $y \in G$ وجود دارد که $x = y^{-۱}f(y)$. سپس نتیجه بگیرید که اگر $f^{۲} = id_G$ آنگاه G آبلی است.

تمرین ۷۴.۱۲.۲. نشان دهید هر گروه دوری مرتبه ۸ با گروه دوری مرتبه ۴ همریخت است.

تمرین ۷۵.۱۲.۲. برای یک گروه دوری متناهی از مرتبه n مانند G نشان دهید که $f : G \longrightarrow G$ با ضابطه $f(x) = x^m$ خودریختی است اگر و تنها اگر $(m, n) = ۱$.

تمرین ۷۶.۱۲.۲. ($\star$) فرض کنیم M زیرگروه ماکسیمال گروه G باشد و $M \neq N_G(M)$. نشان دهید $[G : M]$ عددی اول است.

تمرین ۷۷.۱۲.۲. ($\star$) فرض کنیم G یک گروه با عمل جمع باشد. اگر $f : G \longrightarrow G$ و $g : G \longrightarrow G$ دو همریختی گروهی دلخواه باشند، آنگاه دو همریختی گروهی $S : G \longrightarrow G$ با ضابطه $S(x) = x - fg(x)$ و $T : G \longrightarrow G$ با ضابطه $T(x) = x - gf(x)$ را در نظر بگیرید. حال موارد زیر را رد یا اثبات کنید.
(الف) فرض کنیم G آبلی باشد. در این صورت $Ker(S)$ با $Ker(T)$ یکریخت است.
(ب) S پوشا است اگر و تنها اگر T پوشا باشد.

تمرین ۷۸.۱۲.۲. ($\star$) فرض کنیم $G = \mathbb{Q}$ و $H = (\mathbb{Q}^+, .)$. تمام همریختی‌های گروهی از G به H را پیدا کنید.

تمرین ۷۹.۱۲.۲. ($\star$) برای هر گروه G نشان دهید که $G^{(n)}$ (گروه مشتق مرتبه nام) در G نرمال است.

تمرین ۸۰.۱۲.۲. اگر G گروهی دوری باشد انگاه نشان دهید که $Aut(G)$ آبلی است.

تمرین ۸۱.۱۲.۲. $(\star\star)$ فرض کنیم G گروهی ساده، $H \lneq G$ و $[G:H]=n$. در این صورت G با زیرگروهی از S_n یکریخت است.

تمرین ۸۲.۱۲.۲. $(\star\star)$ فرض کنیم G یک گروه $H \leq G$ و $[G:H]=n$ به طوری که $|G| \nmid n!$. در این صورت G ساده نیست.

تمرین ۸۳.۱۲.۲. نشان دهید که دو دور در S_n مزدوج هستند اگر و تنها اگر طول یکسان داشته باشند.

تمرین ۸۴.۱۲.۲. تمام اعضای $A_۴$ را بنویسید و سپس نشان دهید $A_۴$ فقط یک زیرگروه نرمال دارد.

تمرین ۸۵.۱۲.۲. $(\star)$ فرض کنیم σ یک دور به طول n در S_n باشد. $C_{S_n}(\sigma)$ را حساب کنید.

تمرین ۸۶.۱۲.۲. چند عنصر در $S_۸$ با (۸ ۶ ۳) (۲ ۱) مزدوج هستند؟

تمرین ۸۷.۱۲.۲. فرض کنیم $\sigma, \tau \in S_n$. اگر σ زوج (فرد) باشد آنگاه نشان دهید $\tau\sigma\tau^{-۱}$ زوج (فرد) است.

تمرین ۸۸.۱۲.۲. یک عنصر مرتبه ۲۰ در $S_۸$ پیدا کنید. آیا $S_۸$ عنصر مرتبه ۱۸ دارد؟

تمرین ۸۹.۱۲.۲. $(\star)$ نشان دهید که S_n با یک زیرگروه از $A_{n+۲}$ یکریخت است.

تمرین ۹۰.۱۲.۲. $(\star\star)$ فرض کنیم H یک زیرگروه مرتبه ۱۱۱۱ از گروه $S_{۹۹۹}$ باشد. نشان دهید که عنصر $\sigma \in G$ چنان وجود دارد که برای هر $i \in \{۱, ۲, ..., ۹۹۹\}$ داریم $\sigma(i)=i$.

فصل ۳

آشنایی با نظریه حلقه‌ها

در جبر نوین نظریه حلقه به مطالعه موجودات ریاضی می‌پردازد که به حلقه‌ها معروف هستند. مفهوم حلقه بخش مهمی از جبر نوین است و سایر موجودات جبر نوین مانند گروه‌ها و نظریه اعداد تاثیر گذار است و کاربردهای آن در بسیاری از بخش‌های ریاضی دیده می‌شود. در این فصل هدف ما آشنایی مختصر با نظریه حلقه است و در درس جبر ۱ می‌توانید با مطالب تکمیلی از نظریه گروه آشنا شوید و در مقاطع بالاتر مطالب پیشرفته را بیاموزید.

۱.۳ تعریف حلقه، مثال‌ها و قضیه‌های اولیه

در فصل قبل با مفهوم گروه آشنا شدید. دیدید که گروه یک مجموعه ناتهی همراه با یک عمل دوتایی است. در این فصل یک مجموعه ناتهی را همرا با دو عمل دوتایی که در خواص ویژه صدق می‌کند، در حد مقدماتی بررسی می‌کنیم.

تعریف ۱.۱.۳. *فرض کنیم R یک مجموعه ناتهی همراه با دو عمل دوتایی $*$ و . باشد. اگر خواص*

(۱) $(R, *)$ *یک گروه آبلی باشد.*

(۲) $(R, .)$ *یک نیم‌گروه باشد.*

(۳) *توزیعپذیری از سمت چپ . روی $*$، یعنی برای هر a، b و c از R داشته باشیم*

$$a.(b * c) = a.b \ * \ a.c$$

(۴) *توزیعپذیری از سمت راست . روی $*$، یعنی برای هر a، b و c از R داشته باشیم*

$$(a * b).c = a.c \ * \ b.c$$

برقرار باشد آنگاه به $(R, *, .)$ یک حلقه گوییم.

(به خواص (۳) و (۴) هم زمان توزیعپذیری . روی $*$ گوییم).

مثال ۲.۱.۳. *فرض کنیم $R = \mathbb{Z}$، $*$ همان جمع عادی اعداد صحیح باشد و . همان ضرب عادی*

اعداد صحیح. سال‌ها است که می‌دانید $\mathbb{Z}$ یک حلقه است و در خواص حلقه صدق می‌کند.

مثال ۳.۱.۳. *فرض کنیم $R = \mathbb{Q}$، $*$ همان جمع عادی اعداد گویا باشد و. همان ضرب عادی اعداد گویا. سال‌ها است که می‌دانید $\mathbb{Q}$ یک حلقه است.*

مثال ۴.۱.۳. *فرض کنیم $R = \mathbb{R}$، $*$ همان جمع عادی اعداد حقیقی باشد و. همان ضرب عادی اعداد حقیقی. سال‌ها است که می‌دانید $\mathbb{Z}$ یک حلقه است.*

مثال ۵.۱.۳. *فرض کنیم $R = \mathbb{C}$، $*$ همان جمع عادی اعداد مختلط باشد و. همان ضرب عادی اعداد مختلط. اخیرا! می‌دانید $\mathbb{C}$ یک حلقه است.*

قبل از دیدن مثال‌های متنوع از حلقه تذکر زیر لازم است.

تذکر ۶.۱.۳. *در ادامه از عمل دوتایی $*$ در تعریف حلقه تحت عنوان جمع یاد می‌کنیم و از عمل دوتایی. در تعریف حلقه تحت عنوان ضرب یاد خواهیم کرد و به جای $a.b$ می‌نویسیم ab. اگر بیم ابهام نباشد به جای حلقه $(R, +, .)$ می‌نویسیم R. عنصر خنثی گروه آبلی حلقه R را به جای e با ۰ نمایش می‌دهیم. طبق معمول وارون جمعی عنصر a از حلقه R را با $-a$ نمایش می‌دهیم. لذا $a + (-a) = ۰$ است و به علاوه به جای $a + (-b)$ می‌نویسیم $a - b$.*

مثال ۷.۱.۳. *فرض کنیم $R = \mathbb{P}(X)$ که X یک مجموعه است، جمع را همان عمل دوتایی تفاضل متقارن در نظر بگیرید و ضرب را همان عمل دوتایی اشتراک گیری مجموعه‌ها. یک بررسی ساده نشان می‌دهد که R یک حلقه است.*

مثال ۸.۱.۳. *فرض کنیم $R = \mathbb{R}^X$ که X یک مجموعه است، جمع را همان عمل دوتایی جمع عادی توابع در نظر بگیرید و ضرب را همان عمل ضرب عادی توابع یعنی $fg(x) = f(x)g(x)$. یک بررسی ساده نشان می‌دهد که R یک حلقه است.*

مثال ۹.۱.۳. *فرض کنیم $R = C(\mathbb{R})$، جمع را همان عمل دوتایی جمع عادی توابع (پیوسته) در نظر بگیرید و ضرب را همان عمل ضرب عادی توابع (پیوسته) یعنی $fg(x) = f(x)g(x)$. یک بررسی ساده نشان می‌دهد که R یک حلقه است.*

تعریف و مثال ۱۰.۱.۳. *فرض کنیم R یک گروه آبلی دلخواه با عنصر خنثی ۰ باشد. روی R ضرب بدیهی $ab = ۰$ را قرار می‌دهیم. یک بررسی ساده نشان می‌دهد که R یک حلقه است و به این حلقه، حلقه بدیهی گوییم. همچنین به حلقه $R = \{۰\}$ حلقه صفر گوییم.*

مثال ۱۱.۱.۳. *فرض کنیم R همان زیرگروه $۲\mathbb{Z}$ از گروه جمعی $\mathbb{Z}$ باشد. با همان جمع و ضرب عادی اعداد صحیح، R یک حلقه است.*

مثال ۱۲.۱.۳. *فرض کنیم $R = M_n(\mathbb{R})$. با همان جمع و ضرب عادی ماتریس‌ها، R یک حلقه است.*

مثال ۱۳.۱.۳. *فرض کنیم $R = \mathbb{Z}_n$ که n یک عدد طبیعی است. با همان جمع و ضرب عادی اعداد پیمانه‌ای، R یک حلقه است.*

تعریف ۱۴.۱.۳. گوییم حلقه R جابجایی (یا تعویض پذیر) است هرگاه عمل دوتایی ضرب آبلی باشد، یعنی برای هر $a, b \in R$ داشته باشیم $ab = ba$. اگر حلقه‌ای جابجایی نباشد به آن ناجابجایی گوییم.

مثال ۱۵.۱.۳. حلقه‌های $\mathbb{Z}$، $\mathbb{Q}$ و $\mathbb{R}$ جابجایی هستند.

مثال ۱۶.۱.۳. با انتخاب دو ماتریس مربعی مناسب، می‌توان دید که ضرب ماتریس‌ها جابجایی نیست و لذا حلقه $M_n(\mathbb{Q})$ ناجابجایی است!

تعریف ۱۷.۱.۳. گوییم حلقه R یکدار است هرگاه عمل دوتایی ضرب R دارای عنصر خنثی باشد. این عنصر خنثی (برای ضرب) را با ۱ نشان می‌دهیم و در این نوشتار به آن همانی گوییم (در بعضی منابع، همانی را یکه یا واحد نیز گویند). حلقه‌هایی که همانی ندارند را غیر یکال (نایکال، نا یکه) گوییم.

مثال ۱۸.۱.۳. حلقه‌های $\mathbb{Z}$، $\mathbb{Q}$ و $\mathbb{R}$ جابجایی و یکدار هستند.

مثال ۱۹.۱.۳. حلقه $M_n(\mathbb{Q})$ ناجابجایی و یکدار است! ماتریس همانی، همانی حلقه است.

مثال ۲۰.۱.۳. حلقه‌های بدیهی غیر یکال (غیر یکدار) هستند.

مثال ۲۱.۱.۳. حلقه $۲\mathbb{Z}$ غیر یکال (غیر یکدار) است.

تذکر ۲۲.۱.۳. دقت کنید که در حلقه R واژه عنصر خنثی را برای عنصر خنثی جمع یعنی ۰ استفاده می‌کنیم و برای ۱ واژه همانی (یکه، واحد) را استفاده می‌کنیم.

تعریف ۲۳.۱.۳. گوییم حلقه جابجایی R یک میدان است هرگاه همه عناصر آن جز عنصر خنثی ۰ تحت عمل ضرب تشکیل یک گروه دهند.

مثال ۲۴.۱.۳. حلقه‌های $\mathbb{Q}$، $\mathbb{R}$ و $\mathbb{C}$ میدان هستند.

مثال ۲۵.۱.۳. حلقه $M_n(\mathbb{Q})$ میدان نیست! چون اصلا جابجایی نیست.

مثال ۲۶.۱.۳. حلقه‌های بدیهی هرگز میدان نیستند چون غیر یکال (غیر یکدار) هستند.

مثال ۲۷.۱.۳. حلقه $\mathbb{Z}$ با وجود یکدار بودن، میدان نیست. زیرا ۲ وارون ضربی ندارد.

تعریف ۲۸.۱.۳. گوییم حلقه R یک دامنه است اگر $xy = ۰$ که $x, y \in R$ ایجاب کند $x = ۰$ یا $y = ۰$. اگر R جابجایی و دامنه باشد به آن دامنه صحیح گوییم.

مثال ۲۹.۱.۳. همه میدان‌ها دامنه صحیح هستند. زیرا واضح است که میدان‌ها جابجایی هستند و اگر $xy = ۰$ باشد و $x \neq ۰$ آنگاه x وارون دارد و با ضرب طرفین در وارون x نتیجه می‌شود که $y = ۰$. دقت کنید که حلقه $\mathbb{Z}$ دامنه صحیح است ولی میدان نیست.

مثال ۳.۱.۳۰. حلقه $M_n(\mathbb{Q})$ دامنه نیست (دو ماتریس ناصفر چنان بیابید که ضربشان صفر شود)!

مثال ۳.۱.۳۱. حلقه $\mathbb{Z}_۴$ دامنه صحیح نیست. زیرا $\bar{۰} = \bar{۴} = \bar{۲}\bar{۲}$ ولی $\bar{۰} \neq \bar{۲}$.

تذکر ۳.۱.۳۲. در بخش بعد مثالی خواهیم آورد که دامنه باشد ولی دامنه صحیح نباشد. پس فعلا صبور باشید!

تعریف ۳.۱.۳۳. گوییم عنصر x در حلقه R یک مقسوم علیه صفر چپ است هرگاه عنصر ناصفری مانند y موجود باشد که $xy = ۰$. گوییم عنصر x در حلقه R یک مقسوم علیه صفر راست است هرگاه عنصر ناصفری مانند y موجود باشد که $yx = ۰$. اگر عنصری هم مقسوم علیه صفر چپ و هم راست باشد به آن مقسوم علیه صفر گوییم.

مثال ۳.۱.۳۴. در حلقه $M_۲(\mathbb{R})$ عنصر

$$\begin{pmatrix} ۱ & ۰ \\ ۰ & ۰ \end{pmatrix}$$

مقسوم علیه صفر است. زیرا

$$\begin{pmatrix} ۱ & ۰ \\ ۰ & ۰ \end{pmatrix}\begin{pmatrix} ۰ & ۰ \\ ۰ & ۱ \end{pmatrix} = \begin{pmatrix} ۰ & ۰ \\ ۰ & ۱ \end{pmatrix}\begin{pmatrix} ۱ & ۰ \\ ۰ & ۰ \end{pmatrix} = \begin{pmatrix} ۰ & ۰ \\ ۰ & ۰ \end{pmatrix}.$$

مثال ۳.۱.۳۵. برای هر حلقه ناصفر R عنصر ۰ مقسوم علیه صفر است. زیرا $a \neq ۰$ در R چنان وجود دارد که $a۰ = ۰a = ۰$. واضح است که اگر R حلقه صفر باشد داریم $۱ = ۰$ و عنصر ۰ مقسوم علیه صفر نیست. چون اصلا عنصر ناصفری وجود ندارد!

تذکر ۳.۱.۳۶. دقت کنید که حلقه R یک دامنه است اگر و تنها اگر غیر از ۰ هیچ مقسوم علیه صفر چپ یا راست دیگری نداشته باشد.

مثال ۳.۱.۳۷. با ضرب و جمع عادی ماتریس‌ها می‌توانید نشان دهید که

$$R = \{\begin{pmatrix} a & x \\ ۰ & b \end{pmatrix} \;|\; a, b \in \mathbb{Z},\;\; x \in \mathbb{Z}_۴\}$$

یک حلقه با عنصر خنثی $\begin{pmatrix} ۰ & \bar{۰} \\ ۰ & ۰ \end{pmatrix}$ است. حال عنصر $A = \begin{pmatrix} ۲ & \bar{۰} \\ ۰ & ۱ \end{pmatrix}$ مقسوم علیه صفر چپ است. زیرا

$$\begin{pmatrix} ۲ & \bar{۰} \\ ۰ & ۱ \end{pmatrix}\begin{pmatrix} ۰ & \bar{۲} \\ ۰ & ۰ \end{pmatrix} = \begin{pmatrix} ۰ & \bar{۴} \\ ۰ & ۰ \end{pmatrix}\begin{pmatrix} ۰ & \bar{۰} \\ ۰ & ۰ \end{pmatrix}.$$

با یک بررسی سر راست می‌توانید مشاهده کنید که A مقسوم علیه صفر راست نیست.

تعریف ۳.۱.۳۸. *فرض کنیم R حلقه یکدار باشد. گوییم $a \in R$ دارای وارون چپ است هرگاه $b \in R$ موجود باشد که $ba = ۱$. گوییم $a \in R$ دارای وارون‌راست است هرگاه $b \in R$ موجود باشد که $ab = ۱$. اگر $a \in R$ هم وارون راست داشته باشد هم وارون چپ گوییم وارون پذیر است. مجموعه همه عناصر وارون پذیر R را با $U(R)$ نمایش می‌دهیم.*

تذکر ۳.۱.۳۹. *دقت شود که در حلقه یکدار R، اگر $ab = ۱$ و $ca = ۱$ باشد آنگاه $c = b$ است (چرا؟) و این یعنی a وارن پذیر ست.*

مثال ۳.۱.۴۰. *در حلقه $\mathbb{Z}_۴$ عناصر $\bar{۱}$ و $\bar{۳}$ وارون پذیر هستند. زیرا داریم $\bar{۱} = \bar{۹} = \bar{۳}\bar{۳}$.*

مثال ۳.۱.۴۱. *فرض کنیم R یک میدان باشد. در این صورت $U(R) = R \setminus \{۰\} = R^*$.*

تذکر ۳.۱.۴۲. *همین قدر بدانید که حلقه‌هایی وجود دارند که در آنها عنصری مانند a وجود دارد که وارون چپ دارد ولی اصلا وارون راست ندارد! چنین حلقه‌های اگر علاقه مند به گرایش جبر باشید در مقاطع بالاتر خواهید دید. واضح است که چنین حلقه‌های حتما ناجابجایی هستند.*

خواص مقدماتی حلق را در قضیه زیر جمع آوری می‌کنیم.

قضیه ۳.۱.۴۳. *فرض کنیم R یک حلقه باشد. در این صورت برای هر a، b و c در R داریم*
(۱) $a۰ = ۰a = ۰$.
(۲) $a(-b) = -(ab) = (-a)b$.
(۳) $a(b-c) = ab - ac$.
(۴) $(a-b)c = ac - bc$.

اثبات. (۱) داریم $a۰ = a(۰ + ۰) = a۰ + a۰$. بنابراین با حذف $a۰$ از طرفین با کمک گروه جمعی بودن R داریم $a۰ = ۰$. به روش مشابه $۰a = ۰$.
(۲) داریم $ab + a(-b) = a(b + (-b)) = a۰ = ۰$. پس $a(-b) = -(ab)$. بقیه موارد مشابه اثبات می‌شود.
(۳) داریم $a(b-c) = a(b + (-c)) = ab + a(-c) = ab - ac$.
(۴) مشابه با (۳) اثبات می‌شود. $\square$

با کمک مطالب بخش اول و دوم از فصل اول قضیه‌ها و گزاره‌های زیر به راحتی اثبات می‌شوند. قضیه زیر قانون شرکت پذیری تعمیم یافته برای ضرب نام دارد و این قضیه بیان می‌کند پرانتز گذاری در ضرب حلقه در حاصل نهایی تاثیر ندارد.

قضیه ۴۴.۱.۳. *برای هر a_1، a_2، ...، a_{m+n} در حلقه R داریم*

$$\left(\prod_{i=1}^{m} a_i\right)\left(\prod_{j=1}^{n} a_{m+j}\right) = \prod_{i=1}^{m+n} a_i.$$

در نتیجه برای $a \in R$ و $m \in \mathbb{Z}$ داریم

$$a^m = \underbrace{aa...a}_{m\text{تا}}.$$

اگر R یکدار باشد می‌نویسیم $a^0 = 1$.

قضیه زیر قانون توزیع‌پذیری تعمیم یافته نام دارد.

قضیه ۴۵.۱.۳. *برای a_1، ...، a_k و b_1، ...، b_t در حلقه R داریم*

$$(a_1 + ... + a_k)(b_1 + ... + b_t) = a_1b_1 + ... + a_kb_t.$$

در نتیجه برای $a \in R$ و $m \in \mathbb{Z}$ داریم

$$ma = \underbrace{a + ... + a}_{m\text{تا}}.$$

حال گزاره‌ها زیر را داریم.

گزاره ۴۶.۱.۳. *برای اعداد صحیح مثبت m و n و عنصر a در حلقه R داریم*
(الف) $a^m a^n = a^{m+n}$.
(ب) $(a^m)^n = a^{mn}$.

گزاره ۴۷.۱.۳. *برای اعداد صحیح m و n و عنصرهای a و b در حلقه R داریم*
(الف) $ma + na = (m+n)a$.
(ب) $m(na) = (mn)a$.
(ج) $(ma)(nb) = (mn)(ab) = (na)(mb)$.

بخش را با دو تعریف مهم در نظریه حلقه به پایان می‌رسانیم.

تعریف ۴۸.۱.۳. *گوییم عنصر a در حلقه R پوچتوان است هرگاه عدد طبیعی مانند n باشد که $a^n = 0$. به کوچکترین عدد طبیعی n که $a^n = 0$ باشد مرتبه پوچتوانی گوییم.*

مثال ۴۹.۱.۳. در حلقه $\mathbb{Z}_4$ عنصر $\bar{2}$ پوچتوان است. زیرا $\bar{0} = \bar{2}^2$.

مثال ۵۰.۱.۳. در حلقه $M_4(\mathbb{R})$ عنصر $A=\begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}$ *پوچتوان است. زیرا* $A^3 = 0$.

مثال ۵۱.۱.۳. *در حلقه $\mathbb{Z}$ فقط عنصر ۰ پوچتوان است (چرا؟). آیا می‌توانید در یک دامنه عناصر پوچتوان را پیدا کنید؟*

تعریف ۵۲.۱.۳. *گوییم عنصر a در حلقه R خودتوان است هرگاه $a^2 = a$.*

مثال ۵۳.۱.۳. در حلقه $M_4(\mathbb{R})$ عنصر $A=\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$ *خودتوان است. زیرا* $A^2 = A$.

مثال ۵۴.۱.۳. *در حلقه $\mathbb{Z}_4$ عنصر خودتوان فقط $\bar{0}$ و $\bar{1}$ است.*

مثال ۵۵.۱.۳. *در حلقه $\mathbb{Z}$ فقط عنصر ۰ و ۱ خودتوان است (چرا؟). آیا می‌توانید در یک دامنه عناصر خودتوان را پیدا کنید؟*

تمرین‌های حل شده

تمرین ۵۶.۱.۳. *فرض کنیم R یک حلقه باشد و برای $x \in R$ عنصر یکتای a چنان موجود باشد که $xa = x$. نشان دهید که $ax = x$.*

حل. داریم $x(a + ax - x) = xa + xax - x = x + x^2 - x^2 = x$. پس طبق فرض یکتایی $a + ax - x = a$. لذا $ax = x$.

تمرین ۵۷.۱.۳. *نشان دهید که اگر برای هر عنصر x از حلقه R داشته باشیم $x^2 = x$ آنگاه باید R جابجایی باشد.*

حل. برای هر $x \in R$ داریم که

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

لذا $2x = 0$. این نتیجه می‌دهد که برای هر $x \in R$ داریم $x = -x$. حال برای هر $x, y \in R$ داریم

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

لذا $xy + yx = 0$ و در نتیجه $xy = -yx = yx$ و حل تمام است.

تمرین ۵۸.۱.۳. *(کاپلانسکی) فرض کنیم R یک حلقه یکدار باشد که یک عنصر مانند a دارد و a بیش از یک وارون راست دارد. نشان دهید که a بیشمار وارون راست دارد.*

حل. دقت کنید که اگر a وارون چپ داشته باشد طبق تذکر متن درس، aوارون پذیر است و لذا فقط یک وارون راست دارد که تناقض است. پس a وارون چپ ندارد. حال قرار می‌دهیم

$$A = \{x \in R \mid ax = ۱\}.$$

طبق فرض A بیش از یک عنصر دارد. فرض کنیم $y \in A$. تعریف می‌کنیم

$$f : A \longrightarrow A, \;\; f(x) = xa + y - ۱.$$

f یک تابع روی A است. زیرا

$$a(xa + y - ۱) = axa + ay - a = a + ۱ - a = ۱.$$

اما f واضحا یک تابع یک به یک است. دقت شود که f پوشا نیست. زیرا y تصویر هیچ عنصری نیست. حال اگر A متناهی باشد آنگاه چون f یک به یک است باید طبق قضیه ۲۳.۱.۱، f پوشا باشد که تناقض است. لذا A نامتناهی است.

تمرین ۵۹.۱.۳. *فرض کنیم a عنصری در حلقه یکدار R باشد. اگر عنصر وارون پذیر y چنان باشد که $aya = a$ آنگاه نشان دهید که چنانچه $ax = ۱$ باید $xa = ۱$.*

حل. طرفین $aya = a$ را در x ضرب می‌کنیم، $ayax = ax$ و لذا $ay = ۱$. چون y وارون پذیر است داریم $ya = ۱$ و با ضرب طرفین در x داریم $yax = x$ و این یعنی $y = x$. لذا $xa = ۱$.

تمرین ۶۰.۱.۳. *اگر R یک حلقه جابجایی باشد و x، y عناصری پوچتوان باشند آنگاه نشان دهید $x + y$ پوچتوان است. آیا شرط جابجایی قابل حذف است؟*

حل. طبق فرض اعداد طبیعی m و n وجود دارند که $x^m = ۰ = y^n$. حال فرض کنیم k ماکزیمم m و n باشد. در این صورت $(x+y)^{۲k} = ۰$. دقت شود که چون حلقه R جابجایی است جملات در بسط دو جمله‌ای $(x+y)^{۲k}$ به شکل $c_i x^{۲k-i} b^i$ هستند که c_i ضریب است. با توجه به مقدار تغییرات i و این که k ماکزییم m و n است همواره یکی از دو مقدار $a^{۲k-i}$ یا b^i صفر است.
برای قسمت دوم، حلقه ناجابجایی $M_۲(\mathbb{R})$ را در نظر بگیرید. دو عنصر

$$\begin{pmatrix} ۰ & ۰ \\ ۱ & ۰ \end{pmatrix} \qquad\qquad \begin{pmatrix} ۰ & ۱ \\ ۰ & ۰ \end{pmatrix}$$

پوچتوان از مرتبه پوچتوانی دو هستند. اما جمع آنها پوچتوان نیست.

تمرین ۶۱.۱.۳. *نشان دهید حلقه R عنصر پوچتوان ناصفری ندارد اگر و تنها اگر برای هر $x \in R$ که $x^۲ = ۰$ نتیجه شود $x = ۰$.*

حل. اگر R عنصر پوچتوان ناصفری نداشته باشد آنگاه واضح است که برای هر $x \in R$ که $x^۲ = ۰$ نتیجه می‌شود $x = ۰$. حال برعکس، فرض کنیم $y^k = ۰$ که $y \in R$ و $k \in \mathbb{N}$. بدون کم شدن از کلییت فرض کنیم k کوچکترین عدد طبیعی با خاصیت $y^k = ۰$ باشد. حال داریم

$$(y^{k-۱})^۲ = y^{۲k-۲} = y^{۲k} y^{-۲} = ۰.$$

طبق فرض باید $y^{k-۱} = ۰$. این تناقض با کوچکترین مقدار بودن k دارد مگر این که $y = ۰$.

۲.۳ زیرحلقه و مشخصه یک حلقه

در فصل اول دیدید که گاهی در داخل یک گروه یک گروه دیگر وجود داشت و آن را زیرگروه نامیدیم. اکنون می‌خواهیم در داخل حلقه‌ها چه زیرمجموعه‌های یک حلقه خواهند شد.

تعریف ۱.۲.۳. *فرض کنیم $(R, +, .)$ یک حلقه باشد. زیرمجموعه ناتهی S از R را زیرحلقه گوییم هرگاه $(S, +, .)$ یک حلقه باشد.*

مثال ۲.۲.۳. *همواره $\{0\}$ و R زیرحلقه‌های حلقه R هستند که به زیرحلقه‌های بدیهی معروف می‌باشند.*

مثال ۳.۲.۳. *$2\mathbb{Z}$ یک زیرحلقه از $\mathbb{Z}$ است. همین طور $\mathbb{Z}$ زیرحلقه‌ای از $\mathbb{Q}$ است.*

تذکر ۴.۲.۳. *زیرحلقه می‌تواند عنصر همانی داشته باشد یا نداشته باشد (مثال بالا)! یا حتی عنصر همانی متمایز از خود حلقه داشته باشد (مثال زیر)!.*

مثال ۵.۲.۳. *می‌دانیم که $\mathbb{Z}_{10}$ یک حلقه یکدار با عنصر همانی $\bar{1}$ است. اما یک بررسی ساده نشان می‌دهد که زیرمجموعه $S = \{\bar{0}, \bar{2}, \bar{4}, \bar{6}, \bar{8}\}$ یک زیرحلقه است که همانی آن $\bar{6}$ است!*

محک زیر در تشخیص زیرحلقه بودن یا نبودن کارساز است.

قضیه ۶.۲.۳. *زیرمجموعه ناتهی S از حلقه R یک زیرحلقه است اگر و تنها اگر برای هر $a, b \in S$ داشته باشیم $a - b \in S$ و $ab \in S$.*

اثبات. $(\Leftarrow)$. طبق قضیه ۵.۴.۲، $(S, +)$ یک زیرگروه جمعی از $(R, +)$ است. یک بررسی ساده نشان می‌دهد که شرط $ab \in S$ نیم‌گروه بودن $(S, .)$ را به دست می‌دهد. قوانین توزیعپذیری (چپ و راست) از R به S ارث می‌رسد.

$(\Rightarrow)$. واضح است. □

مثال ۷.۲.۳. *با کمک محک بالا، زیرمجموعه $\{a + bi \mid a, b \in \mathbb{Z}\}$ یک زیرحلقه از $\mathbb{C}$ است که به حلقه اعداد گوسی معروف است.*

مثال ۸.۲.۳. *با کمک محک بالا، زیرمجموعه $\{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ یک زیرحلقه از $\mathbb{R}$ است.*

مثال ۹.۲.۳. *با کمک محک بالا، زیرمجموعه اعداد فرد صحیح یک زیرحلقه از $\mathbb{Z}$ نیست.*

تعریف ۱۰.۲.۳. *فرض کنیم R یک حلقه باشد. به مجموعه*

$$C(R) = \{a \in R \mid xa = ax \qquad \forall x \in R\}$$

مرکز حلقه R گوییم.

مثال ۱۱.۲.۳. *مرکز هر حلقه جابجایی R خود حلقه R است.*

مثال ۱۲.۲.۳. *بدون اثبات از ما بپذیرید که مرکز حلقه ناجابجایی $M_n(\mathbb{R})$ برابر مجموعه همه ماتریس‌های قطری است که مضربی از ماتریس همانی هستند.*

قضیه ۱۳.۲.۳. *مرکز حلقه R یک زیرحلقه R است.*

اثبات. واضح است که $\circ \in C(R)$ و لذا $C(R)$ ناتهی است. فرض کنیم $a, b \in C(R)$. حال داریم
$$(a-b)x = ax - bx = xa - xb = x(a-b)$$
و لذا $a - b \in C(R)$. همچنین
$$(ab)x = abx = a(bx) = a(xb) = axb = (ax)b = (xa)b = xab = x(ab)$$
و لذا $ab \in C(R)$. طبق قضیه ۶.۲.۳ باید $C(R)$ زیرحلقه باشد. □

تعریف ۱۴.۲.۳. *فرض کنیم R یک حلقه باشد و X یک زیرمجموعه از R باشد. در این صورت اشتراک همه زیرحلقه‌های R که شامل X هستند را با $< X >$ نمایش می‌دهیم، یعنی*
$$< X >= \bigcap_{X \subseteq S \leq R} S.$$
دو نکته مهم را باید مد نظر قرار دهیم. اول اینکه اشتراک بالا بامعنی است. زیرا دست کم خود R شامل X است. دوم اینکه به آسانی می‌توان دید که، $< X >$ یک زیرحلقه از R است. از این رو به $< X >$ زیرحلقه تولید شده توسط X گوییم. اگر $X = \emptyset$ آنگاه قرار می‌دهیم $< X >= \{\circ\}$.

حال گزاره زیر را داریم.

گزاره ۱۵.۲.۳. *فرض کنیم X زیرمجموعه‌ای از حلقه R باشد. در این صورت $< X >$ کوچکترین زیرحلقه از R (نسبت به رابطه شمول) است که شامل X است.*

اثبات. سر راست است. □

لم زیر کمک می‌کند که زیرحلقه تولید شده را برای یک مورد خاص به دست آوریم.

لم ۱۶.۲.۳. *فرض کنیم a عنصری از حلقه R باشد. در این صورت داریم*
$$< a >= \{n_۱ a + n_۲ a^۲ + ... + n_k a^k \mid n_i \in \mathbb{Z}, \ k \in \mathbb{N}\}.$$

اثبات. طبق قضیه ۶.۲.۳ زیرحلقه تولید شده توسط a باید شامل توان‌های a یعنی a^i که $i \in \mathbb{N}$، باشد. همچنین باید جمع‌های به شکل $n_i a^i + n_j a^j$ که $i, j \in \mathbb{N}$ و $n_i, n_j \in \mathbb{Z}$ را در بر داشته باشد. پس بسیار طبیعی است که داشته باشیم
$$T = \{n_۱ a + n_۲ a^۲ + ... + n_k a^k \mid n_i \in \mathbb{Z}, \ k \in \mathbb{N}\} \subseteq < a > .$$

واضح است که $a \in T$ (چرا؟). از طرفی T یک زیرحلقه است (چرا؟). بنابراین طبق گزاره بالا، باید $T = < a >$. □

مثال ۱۷.۲.۳. *در حلقه $\mathbb{Z}$ برای $n \in \mathbb{Z}$ داریم*

$$< n >= \{n_1 n + n_2 n^2 + ... + n_k n^k \mid n_i \in \mathbb{Z},\ k \in \mathbb{N}\} =$$
$$\{n(n_1 + n_2 n + ... + n_k n^{k-1}) \mid n_i \in \mathbb{Z},\ k \in \mathbb{N}\} = \{nt \mid t \in \mathbb{Z}\} = n\mathbb{Z}.$$

تعریف ۱۸.۲.۳. *اگر عدد صحیح و مثبت مانند n موجود باشد که برای هر عنصر a از حلقه R داشته باشیم $na = 0$ آنگاه کوچکترین عدد صحیح مثبت با این خاصیت را مشخصه R گوییم و با $Char(R)$ نمایش می‌دهیم. اگر چنین عدد صحیح مثبتی موجود نباشد می‌نویسیم $Char(R) = 0$.*

مثال ۱۹.۲.۳. *واضح است که $Char(\mathbb{Z}_n) = n$ و $Char(\mathbb{R}) = 0$.*

بخش را با قضیه مهم زیر به پایان می‌رسانیم.

قضیه ۲۰.۲.۳. *مشخصه دامنه یکدار R برابر با ۰ یا عدد اول p است.*

اثبات. فرض کنیم $n = Char(R) \neq 0$. به برهان خلف فرض کنیم n اول نباشد. لذا $n = kt$ که $k \lneq n$ و $t \lneq n$. طبق تعریف داریم $n1 = 0$ یا معادلا $kt1 = 0$. در نتیجه $(k1)(t1) = 0$. چون R دامنه است پس باید $k1 = 0$ و $t1 = 0$. پس برای هر $a \in R$ داریم $k1a = ka = 0$ یا $t1a = ta = 0$. در هر صورت داریم $Char(R) \leq max\{k, t\} \lneq n$ که تناقض است. لذا باید n اول باشد. □

تمرین‌های حل شده

تمرین ۲۱.۲.۳. *فرض کنیم e در حلقه R خودتوان باشد. نشان دهید که*

$$eRe = \{ere \mid r \in R\}$$

یک زیرحلقه R است و عنصر همانی آن ممکن است با R فرق داشته باشد.

حل. چون $0 \in R$ پس $e0e = 0 \in eRe$ و لذا eRe ناتهی است. فرض کنیم $ere \in eRe$ و $ese \in eRe$. داریم

$$ere - ese = e(r - s)e \in eRe.$$

چون $e^2 = e$ داریم

$$ere\, ese = ere^2se = erese = e(res)e \in eRe.$$

لذا طبق قضیه ۶.۲.۳ باید eRe زیرحلقه R باشد.
برای قسمت دوم، داریم
$$ere\,e = ere^{۲} = ere$$
و
$$e\,ere = e^{۲}re = ere$$
یعنی e همانی برای حلقه eRe است. اگر e خودتوانی مخالف با $۱ \in R$ باشد آنگاه مطلب اشاره شده صحیح است.

تمرین ۲۲.۲.۳. *اگر برای عنصر x در حلقه R داشته باشیم $x^{۳} = x$ آنگاه نشان دهید که R جابجایی است.*

حل. طبق فرض داریم $(x+x)^{۳} = x+x$ و ایجاب می‌کند که $۶x = ۰$. از طرفی دیگر $(x^{۲}-x)^{۳} = x^{۲}-x$ پس از ساده کردن نتیجه می‌دهد که $۳x = ۳x^{۲}$. با کمک قضیه ۶.۲.۳ داریم که $S = \{۳x \mid x \in R\}$ یک زیرحلقه R است. اگر $y = ۳x \in S$ باشد آنگاه
$$y^{۲} = (۳x)^{۲} = ۹x^{۲} = ۶x^{۳} + ۳x^{۲} = ۳x^{۲} = ۳x = y.$$
اکنون طبق تمرین ۶۱.۱.۳ داریم که جابجایی است. لذا $(۳x)(۳x') = (۳x')(۳x)$ و یا معادلا $۹xx' = ۹x'x$. این ایجاب می‌کند که $۳xx' = ۳x'x$. اکنون با ساده سازی $(x+y)^{۳} = x+y$ داریم
$$xy^{۲} + x^{۲}y + xyx + yx^{۲} + yxy + y^{۲}x = ۰$$
و با ساده سازی $(x-y)^{۳} = x-y$ داریم
$$xy^{۲} - x^{۲}y - xyx - yx^{۲} + yxy + y^{۲}x = ۰.$$
با جمع دو رابطه اخیر نتیجه می‌شود که $۲xy^{۲} + ۲yxy + ۲y^{۲}x = ۰$. طرفین رابطه اخیر را از سمت چپ در y ضرب می‌کنیم یعنی $۲yxy^{۲} + ۲y^{۲}xy + ۲y^{۳}x = ۰$. سپس از سمت راست در y ضرب می‌کنیم یعنی $۲xy^{۳} + ۲yxy^{۲} + ۲y^{۲}xy = ۰$. با تفریق دو رابطه آخر و استفاده از فرض داریم $۲xy = ۲yx$. چون $۳xy = ۳yx$ است پس $xy = yx$ و R جابجایی است.

تمرین ۲۳.۲.۳. *اگر R عنصر پوچتوانی به جز صفر نداشته باشد آنگاه نشان دهید که تمام خودتوان‌ها در مرکز R قرار دارند.*

حل. فرض کنیم $e^{۲} = e \in R$ خودتوان باشد. حال برای هر $x \in R$ داریم
$$(ex-exe)^{۲} = exex - exexe - exex + exexe = ۰$$
پس طبق فرض $ex - exe = ۰$ و لذا $ex = exe$. به صورت مشابه
$$(xe-exe)^{۲} = xexe - xexe - exexe + exexe = ۰$$
پس طبق فرض $xe - exe = ۰$ و لذا $xe = exe$. بنابراین $ex = xe$ و $e \in C(R)$.

تمرین ۲۴.۲.۳. *اگر برای عنصر x در حلقه R داشته باشیم $x = x^{۴}$ آنگاه نشان دهید که خودتوان‌ها مرکزی هستند.*

حل. فرض کنیم $xy = ۰$. داریم

$$yx = (yx)^{۴} = yx\,yx\,yx\,yx = yxyxyxyx = ۰.$$

حال فرض کنیم $e = e^{۲}$ خودتوان باشد. برای هر $y \in R$ داریم

$$e(y - ey) = ey - e^{۲}y = ey - ey = ۰.$$

طبق آنچه که در بالا اثبات کردیم باید $(y - ey)e = ۰$. یعنی $ye = eye$. به صورت مشابه برای هر $y \in R$ داریم

$$(ye - y)e = ye^{۲} - ye = ye - ye = ۰.$$

طبق آنچه که در بالا اثبات کردیم باید $e(ye - y) = ۰$. یعنی $ey = eye$. پس $ey = ye$ و لذا $e \in C(R)$.

۳.۳ چند مثال خاص از حلقه‌ها

در این بخش چند مثال مهم از حلقه‌های خاص را مطرح می‌کنیم. این بخش برای یافتن مثال‌های نقض یا داشتن مثال‌های متنوع بسیار کمک کننده است.

با تعریف میدان در بخش قبل آشنا شدید. این بخش یک حلقه جدید را معرفی می‌کنیم که بسیار شبیه میدان است اما فقط خاصیت جابجایی میدان را ندارد.

تعریف ۱.۳.۳. *گوییم حلقه R یک حلقه تقسیم (شبه میدان) است هرگاه همه عناصر آن جز عنصر خنثی ۰ تحت عمل ضرب تشکیل یک گروه دهند.*

ساختن حلقه تقسیم بدون اطلاعات تخصصی کار ساده‌ای نیست. ساختن اولین حلقه تقسیم چندین سال طول کشید. هر چند امروزه با کمک قضیه‌هایی می‌توانیم به راحتی حلقه تقسیم مثال بزنیم، اما ساختن مثال زیر از حلقه تقسیم ۷ سال به طول انجامید!

تعریف و مثال ۲.۳.۳. مجموعه

$$\mathbb{H}(\mathbb{R}) = \{\begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix} \mid a, b \in \mathbb{C}\}$$

یک زیرحلقه $M_{۲}(\mathbb{C})$ است (منظور از $\bar{a}$ مزدوج مختلط، عدد مختلط $a = x + iy$ است) که همه اعضای غیر صفر آن مانند

$$\begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix}$$

دارای وارون به شکل

$$\begin{pmatrix} \frac{\bar{a}}{\delta} & \frac{-b}{\delta} \\ \frac{\bar{b}}{\delta} & \frac{a}{\delta} \end{pmatrix}$$

است که در آن $\delta = a\bar{a} + b\bar{b} \neq ۰$ (دترمینان ماتریس بالا است و وارون مانند ماتریس‌های با درایه‌های حقیقی محاسبه می‌شود) است. این حلقه ناجابجایی است، زیرا

$$\begin{pmatrix} i & ۱ \\ ۱ & -i \end{pmatrix} \begin{pmatrix} ۱ & ۲ \\ ۳ & ۴ \end{pmatrix} \neq \begin{pmatrix} ۱ & ۲ \\ ۳ & ۴ \end{pmatrix} \begin{pmatrix} i & ۱ \\ ۱ & -i \end{pmatrix}$$

لذا یک حلقه تقسیم است. به این حلقه، حلقه تقسیم کوترنیون‌های حقیقی گوییم (علت واژه حقیقی را در کادر زیر شرح می‌دهیم. البته برای درک کادر زیر اطلاعات مختصری از جبر خطی نیاز دارید).

واضح است که $\mathbb{H}(\mathbb{R})$ یک فضای برداری از بعد چهار روی میدان $\mathbb{R}$ است. پایه این فضای برداری با کمک نامگذاری اعضای به شکل زیر

$$1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad i = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \qquad j = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \qquad k = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$

است. لذا داریم

$$\mathbb{H}(\mathbb{R}) = \{a + bi + cj + dk \mid a, b, c, d \in \mathbb{R}\}$$

و جمع روی $\mathbb{H}(\mathbb{R})$ به شکل

$$\begin{aligned}&(a + bi + cj + dk) + (a' + b'i + c'j + d'k) = \\ &(a + a') + (b + b')i + (c + c')j + (d + d')k\end{aligned}$$

قابل تعریف است. اما برای ضرب، جدول روابط زیر به آسانی حاصل می‌شود:

	i	j	k
i	-1	k	$-j$
j	$-k$	-1	i
k	j	$-i$	-1

با کمک این جدول ضرب به آسانی قابل تعریف است، کافی است مولفه به مولفه در هم ضرب کنیم. برای مثال

$$\begin{aligned}&(1 + 2i)(j + 3k) = j + 3k + 2ij + 6ik = \\ &j + 3k + 2k - 6j = -5j + 5k.\end{aligned}$$

با این نماد جدید مرکز $\mathbb{H}(\mathbb{R})$ برابر $\mathbb{R}$ است. از این رو به $\mathbb{H}(\mathbb{R})$ حلقه تقسیم کوترنیون‌های حقیقی گوییم. وارون عنصر ناصفر $a + bi + cj + dk$ به شکل $\frac{1}{a^2+b^2+c^2+d^2}(a - bi - cj - dk)$ است.

مثال ۳.۳.۲. *داریم*

$$(1 + i + 3k)(j - k) = j - k + ij - ik + 3kj - 3k^2 = 3 - 3i.$$

مثال ۴.۳.۲. *وارون عنصر ناصفر $2 + i - j + 3k$ به شکل $\frac{1}{15}(2 - i + j - 3k)$ است.*

تعریف ۵.۳.۲. *فرض کنیم R یک حلقه باشد. منظور از حلقه متضاد یعنی همان اعضای حلقه R با همان جمع که ضرب آن به صورت $a.b = ba$ است (بررسی کنید که حلقه است). حلقه متضاد را با R^{op} نمایش می‌دهیم.*

مثال ۶.۳.۳. *واضح است که حلقه R یکدار است اگر و تنها اگر R^{op} یکدار باشد. همچنین اگر R جابجایی باشد R و R^{op} ساختار ضرب یکسان دارند. به آسانی مشخص است که $R = (R^{op})^{op}$.*

مثال بعدی حلقه چندجمله‌ای‌ها نام دارد که جایگاه ویژه‌ای در جبر و حتی سایر رشته‌های ریاضی دارد. مطالعه این حلقه‌ها برای نظریه میدان از اهمیت بالایی برخوردار است. اکنون شما را تا حدی با این حلقه‌های مهم آشنا می‌کنیم.

تعریف ۷.۳.۳. *فرض کنیم R یک حلقه باشد. مجموعه چندجمله‌ای‌های با ضرایب روی R و یک متغیر x به صورت زیر تعریف می‌شود*

$$R[x] = \{r_n x^n + r_{n-۱} x^{n-۱} + ... + r_۱ x + r_۰ \mid n \in \mathbb{N},\ r_i \in R\}.$$

به هر عضو $R[x]$ یک چندجمله‌ای گوییم.

مثال ۸.۳.۳. $f(x) = x^۲ + x + ۳$ *یک چندجمله‌ای در $\mathbb{Z}[x]$ است. این چندجمله‌ای در $\mathbb{Q}[x]$ نیز قرار دارد.*

تعریف ۹.۳.۳. *فرض کنیم $f(x) = r_n x^n + ... + r_۱ x + r_۰ \in R[x]$. اگر $r_n \neq ۰$ آنگاه به n درجه چندجمله‌ای و به $r_۰$ ثابت $f(x)$ گوییم. به هر $r_i x^i$ جمله $f(x)$ گوییم. به r_n ضریب پیشرو و جمله $r_n x^n$ را جمله پیشرو نامیم.*

مثال ۱۰.۳.۳. $f(x) = ۲x^۳ + x + ۳$ *یک چندجمله‌ای از درجه ۳ و ثابت ۳ در $\mathbb{Z}[x]$ است که سه جمله دارد. ۲ ضریب پیشرو و $۲x^۳$ جمله پیشرو است.*

تذکر ۱۱.۳.۳. *دو چندجمله‌ای مساویند اگر درجه‌های آنها مساوی و ضرایب جمله‌های هم درجه مساوی باشند.*

تذکر ۱۲.۳.۳. *گاهی لازم است دو عضو از $R[x]$ را در تعداد جملات یکسان کنیم. برای این کار از $۰ \in R$ کمک می‌گیریم. به این صورت عمل می‌کنیم که اگر درجه $f(x)$ برابر n و درجه $g(x)$ برابر m و $m < n$ آنگاه به تعداد $n - m$ تا جمله به $g(x)$ اضافه می‌کنیم یعنی*

$$g(x) = ۰x^n + ۰x^{n-۱} + ... + ۰x^{m+۱} + g_m x^m + ... + g_۱ x + g_۰.$$

اکنون می‌خواهیم $R[x]$ را به حلقه تبدیل کنیم. برای تبدیل $R[x]$ به یک حلقه نیاز به تعریف جمع و ضرب داریم. قبل از تعریف جمع و ضرب نیاز است که قرار داد زیر را بیان کنیم.

قرار داد ۱۳.۳.۳. *همواره فرض بر این است که عناصر حلقه R با x جابجا می‌شوند یعنی $rx = xr$ برای هر $r \in R$. به علاوه $x^i x^j = x^{i+j}$. اما واضح است که اگر R حلقه ناجابجایی باشد آنگاه حتما $R[x]$ ناجابجایی است. همچنین R زیرحلقه از $R[x]$ است.*

تعریف ۱۴.۳.۳. فرض کنیم

$$f(x) = \sum_{i=1}^{n} r_i x^i \qquad g(x) = \sum_{i=1}^{m} s_i x^i$$

دو عضو دلخواه از $R[x]$ باشند. اگر نیاز باشد تعداد جملات $f(x)$ و $g(x)$ را طبق تذکر ۱۲.۳.۳، یکسان می‌کنیم (یعنی زمانی که مثلا $m < n$) پس می‌توانیم فرض کنیم

$$f(x) = \sum_{i=1}^{n} r_i x^i = r_n x^n + ... + r_0 \qquad g(x) = \sum_{i=1}^{n} s_i x^i = s_n x^n + ... + s_0$$

حال جمع را به صورت زیر تعریف می‌کنیم

$$f(x) + g(x) = \sum_{i=1}^{n} r_i x^i + \sum_{i=1}^{m} s_i x^i = \\ (r_n + s_n)x^n + ... + (r_1 + s_1)x + (r_0 + s_0).$$

ضرب به شکل زیر تعریف می‌شود (نیاز به یکسان سازی تعداد جملات نیست)

$$f(x)g(x) = (r_n x^n + ... + r_0)(s_m x^m + ... + s_0) = \\ (r_n s_m)x^{n+m} + ... + (r_1 s_0 + s_1 r_0)x + r_0 s_0.$$

یا گاهی خلاصه تر

$$f(x)g(x) = (\sum_{i=1}^{n} r_i x^i)(\sum_{j=1}^{m} s_j x^j) = \sum_{k=0}^{n+m} c_k x^k$$

که در آن $c_k = \sum_{t=0}^{k} r_t s_{k-t}$.

مثال ۱۵.۳.۳. فرض کنیم

$$f(x) = \bar{2}x^2 + \bar{2} \qquad g(x) = \bar{2}x + \bar{3}$$

دو عنصر در $\mathbb{Z}_4[x]$ باشند. داریم

$$f(x) + g(x) = \bar{2}x^2 + \bar{2}x + \bar{1}$$

و

$$f(x)g(x) = \bar{0}x^3 + \bar{2}x^2 + \bar{0}x + \bar{2} = \bar{2}x^2 + \bar{2}.$$

حال لم زیر نشان می‌دهد که $R[x]$ یک حلقه است.

لم ۱۶.۳.۳. *با جمع و ضرب داده شده در تعریف بالا، $R[x]$ یک حلقه است. اگر R جابجایی و یکدار باشد آنگاه $R[x]$ جابجایی و یکدار است.*

اثبات. بررسی سر راست نشان می‌دهد که $(R[x], +)$ یک گروه آبلی است. البته این تذکر لازم است که چون $R \ni ۰$ چندجمله‌ای

$$o(x) = ۰x^n + ۰x^{n-۱} + ... + ۰x + ۰$$

عضو خنثی جمعی است. همچنین $(R[x], .)$ یک نیم‌گروه است. البته این تذکر لازم است که چون $R \ni ۱$ چندجمله‌ای

$$i(x) = ۰x^n + ۰x^{n-۱} + ... + ۱x + ۰$$

عضو خنثی جمعی است. به علاوه ضرب روی جمع توزیع‌پذیر از هر دو طرف است یعنی $R[x]$ یک حلقه یکدار است. از طرفی R جابجایی است پس طبق قرار داد بالا، $R[x]$ جابجایی است. $\square$

نمادگذاری ۱۷.۳.۳. *برای راحتی کار صفر و یک حلقه $R[x]$ را با ۰ و ۱ نشان می‌دهیم. فرض کنیم $f(x) \in R[x]$ در این صورت منظور از $deg(f(x))$ همان درجه $f(x)$ است. گاهی اوقات برای راحتی نمایش عناصر حلقه $R[x]$ از x در $f(x)$ صرف نظر می‌کنیم.*

در ادامه چند حلقه دیگر را نیز معرفی می‌کنیم که بسیار شبیه به حلقه چندجمله‌ای‌ها هستند. جزییات را حذف می‌کنیم و خلاصه مطلب را در کادر زیر قرار می‌دهیم.

فرض کنیم R یک حلقه باشد. مجموعه سری‌ها با ضرایب روی R و یک متغیر x به صورت زیر تعریف می‌شود

$$R[[x]] = \{r_۰ + r_۱x + r_۲x^۲ + ... \mid r_i \in R\}.$$

به هر عضو $R[x]$ یک سری توانی گوییم. $R[[x]]$ با جمع معمولی و ضرب عادی سری‌ها (مولفه به مولفه) یک حلقه است و به آن حلقه سری‌های توانی گوییم. گاهی یک سری را به صورت $\sum_{n=۰}^{\infty} r_n x^n$ نمایش می‌دهیم. واضح است که $R[x]$ زیرحلقه $R[[x]]$ است.

مثال ۱۸.۳.۳. *در حلقه $\mathbb{R}[[x]]$ داریم*

$$(۱ + x + x^۲ + ...)(۱ + ۲x + ۳x^۲ + ...) = ۱ + ۳x + ۶x^۲ + ...$$

فرض کنیم R یک حلقه باشد و $m \in \mathbb{W}$. مجموعه سری‌ها لورن با ضرایب روی R و یک متغیر x به صورت زیر تعریف می‌شود

$$R < x >= \{r_{-m}x^{-m} + r_{-m+1}x^{-m+1} + ... + r_{-1}x^{-1} + r_0 + r_1 x + r_2 x^2 + ... \mid r_i \in R\}.$$

$R < x >$ با جمع معمولی و ضرب عادی سری‌ها (مولفه به مولفه) یک حلقه است و به آن حلقه سری‌های لورن گوییم. گاهی یک سری را به صورت $\sum_{n=-m}^{\infty} r_n x^n$ نمایش می‌دهیم. واضح است که $R[[x]]$ زیرحلقه $R < x >$ است.

مثال ۱۹.۳.۳. *در حلقه $\mathbb{Z} < x >$ عنصر ناصفر $x + 1$ وارونپذیر است. زیرا*

$$(1 + x)(1 - x + x^2 - x^3 + ...) = 1.$$

وارون عنصر x به صورت x^{-1} است. به صورت کلی اگر R میدان باشد آنگاه $R < x >$ نیز میدان است (چگونه؟).

حلقه زیر در جبر جایگاه ویژه‌ای دارد.

تعریف ۲۰.۳.۳. *فرض کنیم G یک گروه باشد. قرار می‌دهیم*

$$End(G) = \{f : G \longrightarrow G \mid \text{همریختی گروهی است } f\}.$$

جمع عادی توابع را روی $End(G)$ در نظر می‌گیریم و ضرب را ترکیب توابع در نظر می‌گیریم. در ین صورت $End(G)$ یک حلقه (یکدار) است که به آن حلقه اندومورفیسم روی G گوییم.

مواردی که در زیر می‌آید دست ما را برای داشتن حلقه‌های متنوع باز می‌گذارد. هر چند این موارد را آنچنان که شایسته است گسترش نمی‌دهیم و فقط جهت آشنایی می‌آوریم.

تعریف ۲۱.۳.۳. *فرض کنیم $\{R_i\}_{i\in I}$ خانواده‌ای از حلقه‌ها باشد. تمام دنباله‌ها به صورت $(x_i)_{i\in I}$ که برای هر $i \in I$، $x_i \in R_i$ را در نظر می‌گیریم. عمل دوتایی جمع و ضرب را به صورت*

$$(x_i)_{i\in I} + (y_i)_{i\in I} = (x_i + y_i)_{i\in I} \qquad (x_i)_{i\in I}(y_i)_{i\in I} = (x_i y_i)_{i\in I}$$

تعریف می‌کنیم و این دنباله‌ها را به یک حلقه تبدیل می‌کنیم. در واقع، در مکان i ام عمل جمع و ضرب حلقه R_i پیاده می‌شود. حلقه جدید را حاصل ضرب مستقیم یا حاصل ضرب دکارتی R_i ها گوییم و با $\prod_{i\in I} R_i$ نشان می‌دهیم. اگر I متناهی باشد از نماد $R_1 \times ... \times R_k$ نیز استفاده می‌کنیم که $k = |I|$. اگر I تهی باشد تعریف می‌کنیم $\prod_{i\in I} R_i = 0$.

مثال ۲۲.۳.۳. *عنصر همانی حلقه $\prod_{i\in I} R_i$ به صورت $(1_i)_{i\in I}$ است که 1_i عنصر همانی حلقه R_i است.*

تعریف ۲۳.۳.۳. فرض کنیم $\{R_i\}_{i\in I}$ خانواده‌ای از حلقه‌ها باشد. تمام دنباله‌ها به صورت $(x_i)_{i\in I}$ از $\prod_{i\in I} R_i$ را در نظر می‌گیریم که به جز تعداد متناهی اندیس بقیه مولفه‌ها عناصر خنثی هستند. با همان جمع و ضرب $\prod_{i\in I} R_i$ این دنباله‌ها حلقه تشکیل می‌دهند. حلقه جدید را حاصل جمع مستقیم R_i ها گوییم و با $\bigoplus_{i\in I} R_i$ نشان می‌دهیم. اگر I متناهی باشد از نماد $R_۱\oplus...\oplus R_k$ نیز استفاده می‌کنیم که $k = |I|$. اگر I تهی باشد تعریف می‌کنیم $\bigoplus_{i\in I} R_i = ۰$.

مثال ۲۴.۳.۳. *اگر I نامتناهی و $\{R_i\}_{i\in I}$ خانواده‌ای از حلقه‌های نابدیهی باشد آنگاه حتما حلقه $\bigoplus_{i\in I} R_i$ یکدار نیست، حتی اگر همه R_i ها یکدار باشند.*

مثال ۲۵.۳.۳. *حلقه $\mathbb{Z}\times\mathbb{Z}_۴$ دامنه نیست. زیرا*

$$(۱, \bar{۰})(۰, \bar{۱}) = (۰, \bar{۰}).$$

به طور کلی حاصل ضرب حلقه‌ها دامنه نیست (بررسی کنید).

تمرین‌های حل شده

تمرین ۲۶.۳.۳. *نشان دهید که یک دامنه متناهی حلقه تقسیم است.*

حل. فرض کنیم $R = \{۰, a_۱, ..., a_n\}$ باشد. چون R حلقه است، R با عمل ضرب یک نیم‌گروه است. عنصر دلخواه و ناصفر a_j را در R در نظر بگیرید. چون R دامنه است $a_ja_۱$، $a_ja_۲$، ...، a_ja_n ناصفر متمایز هستند. پس برای هر عنصر ناصفر $a_k \in R$ عنصر $a_l \in R$ چنان وجود دارد که $a_ja_l = a_k$. اگر $a_k = ۰$ باشد آنگاه عنصر a_l را همان صفر حلقه انتخاب می‌کنیم. این یعنی برای هر $a, b \in R$ معادله $ax = b$ دارای جواب است. به طریق مشابه معادله $ya = b$ نیز دارای جواب است. لذا طبق قضیه ۴۵.۲.۲ نیم‌گروه $R \setminus \{۰\}$ گروه است و R یک حلقه تقسیم است.

تمرین ۲۷.۳.۳. *فرض کنیم که $R[x]$ مقسوم علیه صفر دارد. نشان دهید که R نیز مقسوم علیه صفر دارد.*

حل. فرض کنیم که $f(x)$ و $g(x)$ دو عنصر ناصفر در $R[x]$ باشند که $f(x)g(x) = ۰$. چون $f(x)$ ناصفر است پس می‌توانیم جمله r_ix^i را در $f(x)$ چنان انتخاب کنیم که مینیمم درجه در جملات $f(x)$ باشد و r_i نیز ناصفر باشد. به همین صورت فرض کنیم s_jx^j مینیمم درجه در جملات $g(x)$ باشد و s_j نیز ناصفر باشد. حال واضح است که $r_is_jx^{i+j}$ مینیمم درجه در چندجمله‌ای $f(x)g(x)$ است. اما $f(x)g(x) = ۰$ پس باید $r_is_j = ۰$ و این یعنی R مقسوم علیه صفر دارد.

تمرین ۲۸.۳.۳. *اگر منظور از $U(R)$ مجموعه تمام عنصرهای یکال حلقه R باشد آنگاه نشان دهید که $U(R_۱ \times ... \times R_n) = U(R_۱) \times ... \times U(R_n)$.*

حل. فرض کنیم $x=(r_1,\dots,r_n)\in U(R_1\times\dots\times R_n)$. پس عنصر $(s_1,\dots,s_n)$ چنان وجود دارد که
$$(r_1,\dots,r_n)(s_1,\dots,s_n)=(1,\dots,1).$$
پس برای هر i، داریم $r_is_i=1$. یعنی $r_i\in U(R_i)$. پس $x\in U(R_1)\times\dots\times U(R_n)$. حال برعکس؛ اگر $x=(r_1,\dots,r_n)\in U(R_1)\times\dots\times U(R_n)$ آنگاه برای هر i، عنصر s_i چنان موجود است که داریم $r_is_i=1$. پس
$$(r_1,\dots,r_n)(s_1,\dots,s_n)=(1,\dots,1).$$
یعنی $x=(r_1,\dots,r_n)\in U(R_1\times\dots\times R_n)$ و اثبات کامل است.

تمرین ۲۹.۳.۳. *نشان دهید $(r_1,\dots,r_n)\in R_1\times\dots\times R_n$ پوچتوان است اگر و تنها اگر برای هر i، r_i پوچتوان باشد.*

حل. اگر $x=(r_1,\dots,r_n)$ دارای مرتبه پوچتوانی k باشد آنگاه
$$(0,\dots,0)=(r_1,\dots,r_n)^k=(r_1^k,\dots,r_n^k).$$
یعنی برای i، $r_i^k=0$. حال برعکس؛ فرض کنیم برای هر i عدد صحیح و نامنفی k_i چنان باشد که $r_i^{k_i}=0$. قرار می‌دهیم $k=k_1+\dots+k_n$. بوضوح داریم
$$(0,\dots,0)=(r_1^k,\dots,r_n^k)=(r_1,\dots,r_n)^k$$
و اثبات کامل است.

تمرین ۳۰.۳.۳. *نشان دهید حلقه R حلقه تقسیم است اگر و تنها اگر R^{op} حلقه تقسیم باشد.*

حل. واضح است که عنصر $a\in R$ وارونپذیر است اگر و تنها اگر عنصر $b\in R$ موجود باشد که $ab=ba=1$ اگر و تنها اگر $b.a=a.b=1$ در R^{op} رخ دهد.

تمرین ۳۱.۳.۳. *فرض کنیم R یک حلقه با بیشتر از یک عنصر باشد که برای هر عنصر $a\in R$ عنصر یکتای $b\in R$ موجود باشد طوری که $aba=a$. موارد زیر را نشان دهید.*
(الف) R هیچ مقسوم علیه صفر ناصفری ندارد.
(ب) $bab=b$.
(ج) R یکدار است.
(د) R حلقه تقسیم است.

حل. (الف) فرض کنیم a یک مقسوم علیه صفر ناصفر باشد. پس $ac=0$ که $0\neq c\in R$. لذا $a(b+c)a=aba=a$. طبق فرض یکتایی باید $b+c=b$ و در نتیجه $c=0$ که تناقض است.
(ب) داریم
$$a(bab)a=ababa=(aba)ba=aba=a.$$

طبق فرض یکتایی و این که $aba = a$ باید $bab = b$.
(ج) ابتدا دقت کنید که ab خودتوان است. زیرا

$$(ab)^۲ = abab = (aba)b = ab.$$

حال نشان می‌دهیم که ab عنصر یک حلقه است. برای هر $x \in R$ داریم که

$$ab(abx - x) = ababx - abx = abx - abx = ۰ = xab - xab = xabab - xab = (xab - x)ab.$$

طبق قسمت (الف)، باید $abx - x = ۰$ یا معادلا $abx = x$. به طریق مشابه $xab = x$ و لذا ab عنصر یک است.
(د) در قسمت (ج)، نشان دادیم که حلقه R یکدار است. برای راحتی از علامت ۱ استفاده می‌کنیم. حال از $aba = a$ داریم که $a(ba - ۱) = ۰ = (ab - ۱)a$. پس طبق قسمت (الف)، $ab = ba = ۱$ و هر عنصر ناصفر R یکال است و R باید حلقه تقسیم باشد.

۴.۳ ایده‌آل و حلقه خارج قسمتی

این بخش به زیرمجموعه‌های خیلی ویژه از حلقه R می‌پردازیم که به آنها ایده‌آل گوییم. در مقاطع بالاتر خواهیم دید که ایده‌آل‌ها مطالعه حلقه را راحتتر می‌کنند و اطلاعات بسیار جالبی در مورد حلقه می‌دهند. مطالعه حلقه با بررسی تک به تک عناصر حلقه بعضا دشوار است و بررسی ایده‌آل‌ها مفیدتر است.

تعریف ۱.۴.۳. *به زیرمجموعه ناتهی I از حلقه R ایده‌آل چپ گوییم هرگاه شرایط زیر برقرار باشد.*
(۱) برای هر $a, b \in I$ داشته باشیم $a - b \in I$.
(۲) برای هر $a \in I$ و هر $r \in R$ داشته باشیم $ra \in I$.
همچنین، به زیرمجموعه ناتهی I از حلقه R ایده‌آل راست گوییم هرگاه شرایط زیر برقرار باشد.
(۱) برای هر $a, b \in I$ داشته باشیم $a - b \in I$.
(۲) برای هر $a \in I$ و هر $r \in R$ داشته باشیم $ar \in I$.
اگر I هم ایده‌آل چپ و هم ایده‌آل راست باشد آنگاه به I ایده‌آل گوییم.

نمادگذاری ۲.۴.۳. *نمادهای متداول برای نشان داد ایده‌ال چپ (راست) بودن I در حلقه R به صورت $I \leq_l R$ ($I \leq_r R$) است. بعضی منابع نیز از $I \trianglelefteq_l R$ ($I \trianglelefteq_r R$) استفاده می‌کنند. همچنین $I \leq R$ ($I \trianglelefteq R$) ایده‌آل بودن I در R را نشان می‌دهد.*

مثال ۳.۴.۳. *در حلقه $\mathbb{Z}$ هر زیرمجموعه $n\mathbb{Z}$ یک ایده‌آل است.*

مثال ۴.۴.۳. *هر ایده‌آل واضحا یک ایده‌آل چپ (راست) است. در هر حلقه جابجایی هر ایده‌آل چپ یک ایده‌آل راست است و برعکس.*

تعریف و مثال ۵.۴.۳. *هر حلقه R دو ایده‌آل $\{0\}$ و R دارد که به ایده‌آل‌های بدیهی معروف هستند.*

تذکر ۶.۴.۳. *فرض کنیم R یک حلقه یکدار باشد و I یک ایده‌آل (چپ، راست). اگر $1 \in I$ آنگاه $I = R$. فرض کنیم $x \in R$. در این صورت طبق تعریف ایده‌آل، $x = x1 \in I$ و لذا $R \subseteq I$.*

مثال ۷.۴.۳. *هر حلقه تقسیم D فقط دو ایده‌آل (چپ، راست) دارد! فرض کنیم I ایده‌آل ناصفر D باشد و $0 \neq a \in I$. در حلقه D عنصر a وارونپذیر است یعنی $ab = ba = 1$ که $b \in D$. اما I یک ایده‌آل چپ است و طبق تعریف باید $ba = 1 \in I$. پس باید $I = D$.*

به مثال زیر توجه کنید! این مثال نشان می‌دهد ایده‌آل چپ بودن، راست بودن متمایز هم هستند.

مثال ۸.۴.۳. *حلقه (ناجابجایی) $M_2(\mathbb{Z})$ را در نظر بگیرید. یک بررسی ساده نشان می‌دهد که زیرمجموعه ناتهی*

$$I = \{\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} \mid a, b \in \mathbb{Z}\}$$

یک ایده‌آل چپ است. اما ایده‌آل راست نیست. زیرا

$$\begin{pmatrix} ۱ & ۰ \\ ۱ & ۰ \end{pmatrix} \begin{pmatrix} ۱ & ۲ \\ ۰ & ۰ \end{pmatrix} = \begin{pmatrix} ۱ & ۲ \\ ۱ & ۲ \end{pmatrix} \notin I.$$

همچنین، یک بررسی ساده نشان می‌دهد که زیرمجموعه ناتهی

$$J = \{\begin{pmatrix} a & b \\ ۰ & ۰ \end{pmatrix} \mid a, b \in \mathbb{Z}\}$$

یک ایده‌آل راست است. اما ایده‌آل چپ نیست. زیرا

$$\begin{pmatrix} ۱ & ۰ \\ ۳ & ۰ \end{pmatrix} \begin{pmatrix} ۱ & ۱ \\ ۰ & ۰ \end{pmatrix} = \begin{pmatrix} ۱ & ۱ \\ ۳ & ۳ \end{pmatrix} \notin J.$$

جالب این که این حلقه بیشمار ایده‌آل دارد! به عبارت بهتر برای هر ایده‌آل $n\mathbb{Z}$ از حلقه $\mathbb{Z}$، $M_۲(n\mathbb{Z})$ یک ایده‌آل از $M_۲(\mathbb{Z})$ است (بررسی کنید).

مثال ۹.۴.۳. حلقه (ناجابجایی) $M_۲(\mathbb{R})$ و عدد طبیعی n را در نظر بگیرید. یک بررسی ساده نشان می‌دهد که زیرمجموعه ناتهی

$$I_n = \{\begin{pmatrix} a & ۰ \\ b & ۰ \end{pmatrix} \mid a, b \in n\mathbb{Z}\}$$

یک ایده‌آل چپ است. اما ایده‌آل راست نیست. زیرا

$$\begin{pmatrix} n & ۰ \\ n & ۰ \end{pmatrix} \begin{pmatrix} ۱ & ۲ \\ ۰ & ۰ \end{pmatrix} = \begin{pmatrix} n & ۲n \\ n & ۲n \end{pmatrix} \notin I_n.$$

همچنین، یک بررسی ساده نشان می‌دهد که زیرمجموعه ناتهی

$$J_n = \{\begin{pmatrix} a & b \\ ۰ & ۰ \end{pmatrix} \mid a, b \in n\mathbb{Z}\}$$

یک ایده‌آل راست است. اما ایده‌آل چپ نیست. زیرا

$$\begin{pmatrix} ۱ & ۰ \\ ۳ & ۰ \end{pmatrix} \begin{pmatrix} n & n \\ ۰ & ۰ \end{pmatrix} = \begin{pmatrix} n & n \\ ۳n & ۳n \end{pmatrix} \notin J_n.$$

یعنی این حلقه بیشمار ایده‌آل چپ (راست) دارد. اما جالب این که این حلقه فقط ایده‌آل‌های بدیهی دارد (قضیه زیر را ببینید).

قضیه زیر را بدون اثبات می‌پذیریم.

قضیه ۱۰.۴.۳. *فرض کنیم R یک حلقه یکدار باشد. A یک ایده‌آل حلقه $M_n(R)$ است اگر و تنها اگر ایده‌آل I از حلقه R موجود باشد که $A = M_n(I)$.*

نتیجه زیر از قضیه بالا به دست می‌آید.

نتیجه ۱۱.۴.۳. *فرض کنیم D یک حلقه تقسیم باشد. در این صورت $M_n(D)$ ایده‌آل نابدیهی ندارد.*

اثبات. در مثال‌های بالا دیدید که حلقه تقسیم D ایده‌آل نابدیهی ندارد. لذا طبق قضیه بالا $M_n(D)$ ایده‌آل نابدیهی ندارد. □

دو نکته مهم در مورد قضیه و نتیجه بالا وجود دارد که در مثال‌های زیر بیان می‌کنیم.

مثال ۱۲.۴.۳. *فرض کنیم D یک حلقه تقسیم باشد. دیدیم که $M_n(D)$ ایده‌آل نابدیهی ندارد. اما $M_n(D)$ ایده‌آل چپ (راست) نابدیهی دارد. کافی است مانند مثال‌های بالا مجموعه همه ماتریس‌هایی را در نظر بگیریم یک ستون (سطر) ناصفر دارند.*

مثال ۱۳.۴.۳. *یکدار بودن R در صورت قضیه بالا لازم است. مثلا فرض کنیم $R = \mathbb{Z}_p$ حلقه بدیهی باشد (با ضرب صفر، که یکدار نیست). اگر I زیرگروه $(R, +)$ باشد آنگاه برای هر $x \in I$ و هر $r \in R$ داریم $xr = rx = ۰$. لذا زیرمجموعه‌های ناتهی R ایده‌آل هستند اگر و تنها اگر زیرگروه $(R, +)$ باشند. بنابراین این حلقه اصلا ایده‌ال نابدیهی ندارد. چرا که طبق قضیه ۷۷.۹.۲، $(R, +)$ گروه ساده است. اکنون طبق قضیه بالا $M_۲(R)$ ایده‌آل‌های نابدیهی ندارد. اما این صحیح نیست. چرا که یک بررسی ساده نشان می‌دهد*

$$I = \{\begin{pmatrix} a & b \\ ۰ & ۰ \end{pmatrix} \mid a, b \in R\}$$

یک ایده‌آل نابدیهی $M_۲(R)$ است و تناقض آشکار رخ داده است.

مثال ۱۴.۴.۳. *فرض کنیم R یک حلقه باشد. برای هر $x \in R$ دو زیرمجموعه ناتهی*

$$Rx = \{rx \mid r \in R\} \qquad\qquad xR = \{xr \mid r \in R\}$$

از R به ترتیب ایده‌آل چپ و راست هستند.

تذکر ۱۵.۴.۳. *اگر I یک ایده‌آل چپ (راست) از حلقه R باشد واضح است که $I = RI$ ($I = IR$). برای ایده‌آل I داریم $I = RIR$.*

حال گزاره زیر را داریم.

گزاره ۱۶.۴.۳. *فرض کنیم R یک حلقه و $\{I_\alpha\}_{\alpha\in\Gamma}$ خانواده‌ای از ایده‌آل‌های چپ (راست) R باشد. در این صورت $I = \bigcap_{\alpha\in\Gamma} I_\alpha$ یک ایده‌آل چپ (راست) است.*

اثبات. برای هر $\alpha \in \Gamma$ داریم که $0 \in I_\alpha$. لذا $0 \in I$ و I ناتهی است. حال اگر $x, y \in I$ آنگاه برای هر $\alpha \in \Gamma$ داریم $x, y \in I_\alpha$ و چون I_α ایده‌آل چپ است، $x - y \in I_\alpha$. در نتیجه $x - y \in I$.
اکنون برای هر $r \in R$ و هر $\alpha \in \Gamma$ داریم $rx \in I_\alpha$، زیرا I_α ایده‌آل چپ است. در نتیجه $rx \in I$ و طبق تعریف I ایده‌آل چپ است. به طریق مشابه سمت راست نیز نتیجه می‌شود. $\square$

سوال ۱۷.۴.۳ . *در مورد اجتماع خانوده‌ای از ایده‌آل‌های چپ (راست) چه نتیجه می‌توان گرفت؟*

تعریف ۱۸.۴.۳ . *فرض کنیم R یک حلقه باشد و X یک زیرمجموعه از R باشد. در این صورت اشتراک همه ایده‌آل‌های چپ R که شامل X هستند را با $< X >_l$ نمایش می‌دهیم، یعنی*

$$< X >_l = \bigcap_{X \subseteq I \leq_l R} I.$$

دو نکته مهم را باید مد نظر قرار دهیم. اول اینکه اشتراک بالا بامعنی است. زیرا دست کم خود R شامل X است. دوم اینکه به آسانی می‌توان دید که، $< X >_l$ یک ایده‌آل چپ از R است. از این رو به $< X >_l$ ایده‌آل چپ تولید شده توسط X گوییم. اگر $X = \emptyset$ آنگاه قرار می‌دهیم $< X >_l = \{0\}$. به روش مشابه $< X >_r$ و $< X >$ تعریف می‌شوند.
اگر X مجموعه متناهی $\{x_1, x_2, ..., x_k\}$ باشد به جای $< X >_l$ بعضا از نماد $< x_1, x_2, ..., x_k >_l$ استفاده می‌کنیم.

مثال ۱۹.۴.۳ . *اگر فرض کنیم $X = \{2, 4\}$ آنگاه در حلقه $\mathbb{Z}$ داریم*

$$< X >_l = < X >_r = < X > = 2\mathbb{Z}.$$

مثال ۲۰.۴.۳ . *فرض کنیم $a \neq 0$ عنصری در حلقه تقسیم D باشد. در این صورت*

$$< a >_l = < a >_r = < a > = D$$

گزاره ۲۱.۴.۳ . *فرض کنیم X زیرمجموعه‌ای از حلقه R باشد. در این صورت $< X >_l$ کوچکترین ایده‌آل چپ از R (نسبت به رابطه شمول) است که شامل X است. حکم مشابه برای $< X >_r$ و $< X >$ برقرار است.*

اثبات. سر راست است. $\square$

تعریف ۲۲.۴.۳ . *گوییم ایده‌آل چپ I از حلقه R تولید متناهی (متناهیا تولید شده) است، هرگاه زیرمجموعه متناهی X از R چنان باشد که $I = < X >_l$. مفهوم مشابه برای ایده‌آل راست متناهی تولید و ایده‌آل متناهی تولید نیز تعریف می‌شود.*
گوییم ایده‌ال چپ I اصلی است هرگاه عنصر a از R چنان باشد که $I = < a >_l$. مفهوم مشابه برای ایده‌آل راست اصلی و ایده‌آل اصلی نیز تعریف می‌شود.

مثال ۲۳.۴.۳. *فرض کنیم R یک حلقه یکدار باشد. در این صورت واضح است که $R=<1>_l=<1>$. همچنین برای حلقه $\mathbb{Z}$ داریم $<2,3>=\mathbb{Z}=<1>$.*

گزاره زیر برای ما اهمیت بسیار زیادی دارد و اثبات آن را به عنوان تمرین رها می‌کنیم.

گزاره ۲۴.۴.۳. *فرض کنیم R حلقه دلخواه باشد و $a \in R$. در این صورت*
(۱) $<a>=\{\sum_{i\ \text{جمع متناهی روی}} r_ias_i + ra + as + na \mid r, s, r_i, s_i \in R,\ n \in \mathbb{Z}\}$.
(۲) $<a>_l=\{ra+na \mid r\in R,\ n\in\mathbb{Z}\}$.
(۳) $<a>_r=\{ar+na \mid r\in R,\ n\in\mathbb{Z}\}$.
اگر R حلقه یکدار باشد، آنگاه داریم
(۱) $<a>=\{\sum_{i\ \text{جمع متناهی روی}} r_ias_i \mid r_i, s_i\in R\}$.
(۲) $<a>_l=\{ra \mid r\in R\}$.
(۳) $<a>_r=\{ar \mid r\in R\}$.

اثبات. به عنوان تمرین رها می‌کنیم. □

نمادگذاری ۲۵.۴.۳. *برخی موارد به جای نمادهای $<a>$، $<a>_l$ و $<a>_r$ از نمادهای RaR، Ra و aR استفاده می‌کنیم.*

مثال ۲۶.۴.۳. *در حلقه ناجابجایی یکدار $M_2(\mathbb{R})$ داریم*

$$<\begin{pmatrix}1&0\\0&0\end{pmatrix}>_l=\{\begin{pmatrix}a&b\\c&d\end{pmatrix}\begin{pmatrix}1&0\\0&0\end{pmatrix} \mid \begin{pmatrix}a&b\\c&d\end{pmatrix}\in M_2(\mathbb{R})\}=$$
$$\{\begin{pmatrix}a&0\\c&0\end{pmatrix} \mid a,c\in\mathbb{R}\}.$$

تذکر ۲۷.۴.۳. *برای یک حلقه یکدار به آسانی می‌توان دید که*

$$<a_1,a_2,...,a_k>_l=\{r_1a_1+...+r_ka_k \mid r_i\in R\}=$$
$$<a_1>_l+...+<a_k>_l=Ra_1+...+Ra_k.$$

مثال ۲۸.۴.۳. *در حلقه ناجابجایی یکدار $M_2(\mathbb{R})$ داریم*

$$<\begin{pmatrix}1&0\\0&0\end{pmatrix},\begin{pmatrix}0&1\\0&0\end{pmatrix}>_l=$$
$$\{\begin{pmatrix}a&b\\c&d\end{pmatrix}\begin{pmatrix}1&0\\0&0\end{pmatrix}+\begin{pmatrix}a'&b'\\c'&d'\end{pmatrix}\begin{pmatrix}0&1\\0&0\end{pmatrix} \mid \begin{pmatrix}a&b\\c&d\end{pmatrix},\begin{pmatrix}a'&b'\\c'&d'\end{pmatrix}\in M_2(\mathbb{R})\}=$$
$$\{\begin{pmatrix}a&0\\c&0\end{pmatrix}+\begin{pmatrix}0&a'\\0&c'\end{pmatrix} \mid a,c,a',c'\in\mathbb{R}\}=M_2(\mathbb{R}).$$

در درس جبر ۱ خواهید دید که حلقه‌های که همه ایده‌آل‌های چپ آن اصلی هستند برای ما اهمیت بسیار ویژه‌ای دارند و در آن دوره درسی آنها زیر ذره بین قرار می‌دهیم. در حد آشنایی بدانید که چنین حلقه‌ای را ایده‌آل اصلی چپ گوییم و یک مثال آن $\mathbb{Z}$ است.

تعریف ۲۹.۴.۳. *فرض کنیم R یک حلقه و A_1، A_2، ...، A_k زیرمجموعه‌های ناتهی از R باشند. منظور از جمع این مجموعه‌ها یعنی*

$$A_1 + ... + A_k = \{a_1 + a_2 + ... + a_k \mid a_i \in A_i\}$$

و منظور از حاصل ضرب این مجموعه‌ها یعنی

$$A_1 A_2 ... A_k = \{\sum_{j=1}^{n} a_{1j} a_{2j} ... a_{kj} \mid a_{ij} \in A_i,\ n \in \mathbb{N}\}.$$

اگر $A_k = ... = A_1 = A$ آنگاه از نماد A^k استفاده می‌کنیم. همچنین اگر $\{x\} = A_1$ آنگاه به جای $A_1 A_2$ می‌نویسیم xA_2.

قبل از آوردن مثال، قضیه زیر را داریم.

قضیه ۳۰.۴.۳. *فرض کنیم R یک حلقه و A_1، A_2، ...، A_k ایده‌آل‌های چپ (راست) از R باشند. در این صورت موارد زیر بر قرار است.*

(الف) $A_1 + ... + A_k$ ایده‌آل چپ (راست) است.

(ب) $A_1 A_2 ... A_k$ ایده‌آل چپ (راست) است.

(ج) $A_1 + (A_2 + A_3) = (A_1 + A_2) + A_3$.

(د) $A_1(A_2 A_3) = (A_1 A_2) A_3$.

(ه) $A_1(A_2 + A_3) = A_1 A_2 + A_1 A_3$ و $(A_1 + A_2)A_3 = A_1 A_3 + A_2 A_3$.

اثبات. اثبات سر راست است و به عنوان تمرین رها می‌شود. □

مثال ۳۱.۴.۳. در حلقه جابجایی R و برای $a, b \in R$ داریم $< a >< b >=< ab >$. زیرا

$$< a >< b >= \{\sum_{j=1}^{n} x_j y_j \mid x_j \in < a >,\ y_j \in < b >, n \in \mathbb{N}\} =$$
$$\{\sum_{j=1}^{n} r_j a s_j b \mid r_j, s_j \in R,\ n \in \mathbb{N}\} = \{\sum_{j=1}^{n} r_j s_j ab \mid r_j, s_j \in R,\ n \in \mathbb{N}\} =$$
$$\{rab \mid r \in R\} =< ab > .$$

تذکر ۳۲.۴.۳. *اگر I یک ایده‌آل چپ (راست) از حلقه R باشد واضح است که $I = RI$ ($I = IR$). برای ایده‌آل I داریم $I = RIR$.*

در فصل دوم دیدید که چگونه با زیرگروه نرمال مشخصات یک گروه دانسته می‌شود. همچنین مشاهده کردید که با کمک زیرگروه نرمال چگونه یک گروه جدید به نام گروه خارج قسمتی می‌سازیم. جالب این که در حلقه‌ها ایده‌آل تقریبا نقشی شبیه به زیرگروه نرمال دارد و کمک می‌کند که حلقه را بهتر بشناسیم و حلقه‌های جدید بسازیم.

فرض کنیم حلقه R را در اختیار داریم. می‌دانیم که $(R,+)$ یک گروه آبلی است و لذا هر زیرگروه آن نرمال است. حال ایده‌آل I از R را در نظر بگیرید. واضح است که I زیرگروه نرمال $(R,+)$ است و در نتیجه می‌توانیم گروه آبلی $(R/I,+)$ را تشکیل دهیم. به یادآورید که اعضای R/I به شکل $r+I$ هستند که در آن $r\in R$. با این مقدمه قضیه زیر را ببینید.

قضیه ۳۳.۴.۳. *فرض کنیم R یک حلقه و I ایده‌آل R باشد. در این صورت R/I با جمع و ضرب زیر یک حلقه است که به آن حلقه خارج قسمتی گوییم.*

$$(a+I)+(b+I)=a+b+I$$
$$(a+I)(b+I)=ab+I$$

اثبات. این که عمل جمع خوشتعریف است، بدیهی است. اما عمل ضرب بالا خوشتعریف است. زیرا اگر $a+I=c+I$ و $b+I=d+I$ آنگاه $a-c\in I$ و $b-d\in I$. حال چون I ایده‌آل است، داریم

$$ab-cd=a(b-d)+(a-c)d\in I.$$

لذا $ab+I=cd+I$ و خوشتعریفی حاصل می‌شود. $o+I$ عنصر خنثی است.بقیه خواص حلقه یک بررسی سر راست است. □

مثال ۳۴.۴.۳. *اگر R حلقه یکدار باشد و I ایده‌آل R آنگاه واضح است که $I+۱$ عنصر همانی R/I است. همچنین اگر R جابجایی باشد آنگاه R/I نیز جابجایی است.*

مثال ۳۵.۴.۳. *اگر R یک حلقه و $I=R$ باشد آنگاه R/I حلقه صفر است.*

مثال ۳۶.۴.۳. *در فصل قبل دیدید که*

$$\mathbb{Z}/۳\mathbb{Z}=\{۳\mathbb{Z},۳\mathbb{Z}+۱,۳\mathbb{Z}+۲\}.$$

$۳\mathbb{Z}+i$ یعنی اعدادی که بر ۳ باقیمانده $۰\le i<۳$ دارند، پس با تعویض نماد $۳\mathbb{Z}+i$ با $\bar{i}$ عملا داریم

$$\mathbb{Z}/۳\mathbb{Z}=\{\bar{۰},\bar{۱},\bar{۲}\}.$$

لذا طبق قضیه بالا حلقه خارج قسمتی $\mathbb{Z}/۳\mathbb{Z}$ را خواهیم داشت. این کار را می‌توان با هر ایده‌آل $n\mathbb{Z}$ از حلقه $\mathbb{Z}$ تکرار نمود.

مثال ۳۷.۴.۳. *فرض کنیم R یک حلقه یکدار باشد. ایده‌آل $<x>$ از حلقه (یکدار) $R[x]$ را در نظر بگیرید. طبق گزاره ۲۴.۴.۳، $I=<x>$ همه چندجمله‌ای‌های است که جمله ثابت ندارند. حال فرض کنیم $f(x)=a_۰+a_۱x+\ldots+a_kx^k$ یک عنصر دلخواه از $R[x]$ باشد. واضح است که $a_۱x$، $a_۲x^۲$، ...، a_kx^k عناصری از I هستند. لذا*

$$R[x]/I=\{a+I\mid a\in R\}.$$

تمرین‌های حل شده

تمرین ۳۸.۴.۳. *نشان دهید که در حلقه*

$$R = \{\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mid a,b,c \in \mathbb{R}\}$$

مجموعه

$$I = \{\begin{pmatrix} 0 & x \\ 0 & 0 \end{pmatrix} \mid x \in \mathbb{R}\}$$

ایده‌آل است.

حل. واضح است که I ناتهی است. حال فرض کنیم

$$A = \begin{pmatrix} 0 & x \\ 0 & 0 \end{pmatrix}, \ \ B = \begin{pmatrix} 0 & y \\ 0 & 0 \end{pmatrix} \in I.$$

بدیهی است که داریم $A - B \in I$. حال برای عنصر دلخواه $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \in R$ داریم

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}\begin{pmatrix} 0 & x \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & ax \\ 0 & 0 \end{pmatrix} \in I.$$

همچنین

$$\begin{pmatrix} 0 & x \\ 0 & 0 \end{pmatrix}\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} = \begin{pmatrix} 0 & xc \\ 0 & 0 \end{pmatrix} \in I.$$

تمرین ۳۹.۴.۳. *فرض کنیم R یک حلقه یکدار باشد که هیچ ایده‌ال چپ نابدیهی ندارد. نشان دهید R حلقه تقسیم است.*

حل. فرض کنیم $0 \neq a \in R$. بنابراین $< a >_l$ یک ایده‌آل چپ ناصفر است. طبق فرض باید $R =< a >_l$. چون $1 \in R$ پس عنصر $0 \neq b \in R =< a >_l$ چنان وجود دارد که $ba = 1$. با استدلالی مشابه عنصر ناصفر $c \in R$ چنان وجود دارد که $cb = 1$. لذا b عنصری وارونپذیری است و این ایجاب می‌کند که a وارونپذیر باشد زیرا $a = b^{-1}$. در نتیجه عناصر ناصفر R وارونپذیر هستند و R حلقه تقسیم است.

تمرین ۴۰.۴.۳. *در حلقه R و برای ایده‌آل‌های I و J از R نشان دهید که $IJ \subseteq I \cap J$. سپس نتیجه بگیرید که اگر R جابجایی و $I + J = R$ آنگاه $I \cap J = IJ$. با یک مثال نشان دهید که $IJ \subsetneq I \cap J$.*

حل. فرض کنیم $x \in IJ$. پس $x = \sum_{l=1}^{n} x_l y_l$ که $x_l \in I$ و $y_l \in J$. چون $y_l \in J$ و J ایده‌آل (چپ) پس $x_l y_l \in J$، لذا $x \in J$. به صورت مشابه، چون $x_l \in I$ و I ایده‌آل (راست)

پس $x_l y_l \in I$، لذا $x \in I$. بنابراین $x \in I \cap J$.
برای قسمت دوم، طبق قضیه متن درس داریم

$$I \cap J = R(I \cap J) = (I+J)(I \cap J) = I(I \cap J) + J(I \cap J) \subseteq$$
$$IJ + JI = IJ + IJ = IJ.$$

و طبق قسمت قبل $IJ = I \cap J$.
برای قسمت آخر، حلقه بدیهی (ضرب صفر) $\mathbb{Z}_۴$ را در نظر بگیرید. واضح است که $I = \{\bar{۰}, \bar{۲}\}$ یک ایده‌آل است و $I^۲ = II = \bar{۰}$. اما $I \cap I = I$.

تمرین ۴۱.۴.۳. *تمام اعضای حلقه* $R = \mathbb{Z}_۲[x]/< x^۲ + \bar{۱} >$ *را بنویسید.*

حل. واضح است که $x^۲ + \bar{۱} \in < x^۲ + \bar{۱} >$. لذا در R داریم $x^۲ = -\bar{۱} = \bar{۱}$. بنابراین

$$x^۳ + < x^۲ + \bar{۱} > = xx^۲ + < x^۲ + \bar{۱} > = x + < x^۲ + \bar{۱} > .$$

همچنین

$$x^۴ + < x^۲ + \bar{۱} > = x^۲x^۲ + < x^۲ + \bar{۱} > = \bar{۱}\,\bar{۱} + < x^۲ + \bar{۱} > = \bar{۱} + < x^۲ + \bar{۱} >$$

و

$$x^۵ + < x^۲ + \bar{۱} > = xx^۴ + < x^۲ + \bar{۱} > = x + < x^۲ + \bar{۱} > .$$

با تکرار روند بالا همواره برای توان‌های فرد به $x + < x^۲ + \bar{۱} >$ از R و برای توان‌های زوج به $\bar{۱} + < x^۲ + \bar{۱} >$ از R دست می‌یابیم. پس برای چندجمله‌ای دلخواه $\bar{a}_۰ + \bar{a}_۱ x + ... + \bar{a}_n x^n$ در حلقه $\mathbb{Z}_۲[x]$ داریم

$$\bar{a}_۰ + \bar{a}_۱ x + ... + \bar{a}_n x^n + < x^۲ + \bar{۱} > = \bar{b}_۰ + \bar{b}_۱ x + < x^۲ + \bar{۱} > .$$

زیرا توان‌های بیشتر از دو را با مقدارهایی که بالا به دست آوردیم، جایگزین می‌کنیم. لذا با توجه به این که $\bar{b}_i \in \mathbb{Z}_۲$ داریم

$$R = \{\bar{۰},\ \bar{۱} + < x^۲ + \bar{۱} >,\ x + < x^۲ + \bar{۱} >,\ \bar{۱} + x + < x^۲ + \bar{۱} >\}.$$

۵.۳ قضایای یکریختی حلقه‌ای

اکنون آماده هستیم تا مهمترین بخش این فصل را ارائه کنیم. این بخش برای مطالعه حلقه‌ها بسیار با اهمیت است. در حقیقت هدف این بخش را می‌توان اینگونه معرفی کرد که با کمک برخی توابع خاص یک حلقه ناشناخته را به یک حلقه که از قبل می‌شناسیم یا اطلاعاتی از آن داریم مرتبط می‌کنیم و از این ارتباط برای شناسایی بیشتر حلقه بهره می‌بریم.

تعریف ۱.۵.۳. *فرض کنیم دو حلقه $(R, +, .)$ و $(S, \oplus, \odot)$ را در اختیار داریم. در این صورت تابع $f : R \longrightarrow S$ را یک همریختی حلقه‌ای (هomomorphism حلقه‌ای) گوییم هرگاه برای هر $x, y \in R$ داشته باشیم $f(x + y) = f(x) \oplus f(y)$ و $f(x.y) = f(x) \odot f(y)$.*

مثال ۲.۵.۳. *داریم که*

$$f : (\mathbb{Z}, +, .) \longrightarrow (\mathbb{Z}_۲, +, .), \quad f(x) = \bar{x}$$

یک همریختی حلقه‌ای است. زیرا برای هر $x, y \in \mathbb{Z}$ داریم

$$f(x + y) = \overline{x + y} = \bar{x} + \bar{y} = f(x) + f(y).$$

همچنین

$$f(x.y) = \overline{x.y} = \bar{x}.\bar{y} = f(x).f(y).$$

مثال ۳.۵.۳. *تابع*

$$f : (\mathbb{R}, +, .) \longrightarrow (\mathbb{R}, +, .), \quad f(x) = e^x$$

یک همریختی حلقه‌ای نیست. زیرا داریم

$$f(۱ + ۰) = e^{۱+۰} = e \neq e + ۱ = f(۱) + f(۰).$$

مثال ۴.۵.۳. *داریم که*

$$\theta(\mathbb{Z}[x], +, .) \longrightarrow (\mathbb{Z}, +, .), \quad \theta(a_۰ + a_۱x + ... + a_nx^n) = a_۰$$

یک همریختی حلقه‌ای است.

تذکر ۵.۵.۳. *از این لحظه به بعد وقتی حلقه‌ای را می‌نویسیم از نوشتن عمل جمع و ضرب آن برای راحتی خودداری می‌کنیم و انتظار ما این است که دانشجو خود متوجه عمل‌ها شود، مگر این که حلقه جدیدی را معرفی کنیم یا این که بخواهیم عمل دوتایی را تغییر دهیم. پس مثلا دیگر نمی‌نویسیم $(\mathbb{Z}, +, .)$ و می‌نویسیم $\mathbb{Z}$ و یا مثلا دیگر نمی‌نویسیم $(M_n(\mathbb{R}), +, .)$ و می‌نویسیم $M_n(\mathbb{R})$ و الی آخر. همچنین دیگر $+$ و $.$، وقتی f را اثر می‌دهیم، نمی‌نویسیم و انتظار داریم که دانشجو متوجه باشد که عمل در دامنه است یا در برد همریختی حلقه‌ای!*

تعریف و مثال ۶.۵.۳. داریم که

$$f: R \longrightarrow S, \ \ f(x) = \circ_S$$

یک همریختی حلقه‌ای است. به این همریختی حلقه‌ای، همریختی حلقه‌ای بدیهی گوییم.

تعریف ۷.۵.۳. فرض کنیم $f : R \longrightarrow S$ یک همریختی حلقه باشد. اگر f پوشا باشد آنگاه به f همریختی حلقه‌ای پوشا (اپی‌مورفیسم حلقه‌ای) گوییم. اگر f یک‌به‌یک باشد آنگاه به f همریختی حلقه‌ای یک‌به‌یک (منومورفیسم حلقه‌ای) گوییم. اگر f همریختی حلقه‌ای پوشا و یک‌به‌یک باشد آنگاه به f یکریختی حلقه‌ای (ایزومورفیسم حلقه‌ای) گوییم و می‌نویسیم $R \cong S$.

مثال ۸.۵.۳. داریم که

$$f: \mathbb{Z} \longrightarrow \mathbb{Z}_۲, \quad f(x) = \bar{x}$$

یک همریختی حلقه‌ای پوشا است که یک‌به‌یک نیست.

مثال ۹.۵.۳. داریم که

$$f: \mathbb{Z} \longrightarrow \mathbb{R}, \quad f(x) = x$$

یک همریختی حلقه‌ای یک‌به‌یک است که پوشا نیست.

مثال ۱۰.۵.۳. داریم که

$$f: \mathbb{C} \longrightarrow T, \quad f(a+ib) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$$

که در آن

$$T = \{\begin{pmatrix} x & y \\ -y & x \end{pmatrix} \mid a, b \in \mathbb{R}\}$$

است، یک همریختی یک‌به‌یک و پوشا است، یعنی یکریختی است، $\mathbb{C} \cong T$.

تعریف و مثال ۱۱.۵.۳. فرض کنیم I یک ایده‌آل از حلقه R باشد. قرار می‌دهیم

$$\pi : R \longrightarrow R/I, \ \ \pi(x) = x + I.$$

π یک تابع است. زیرا واضح است که برای هر $x \in R$، $\pi(x) = x + I$ یک هم دسته (چپ) است و لذا در R/I قرار دارد. همچنین اگر $x = x'$ باشد آنگاه $x + I = x' + I$ و لذا $\pi(x) = \pi(x')$. به روشنی مشخص است که π یک تابع پوشا نیز می‌باشد. اما π یک همریختی حلقه‌ای است. زیرا

$$\pi(xx') = xx' + I = (x+I)\ (x'+I) = \pi(x)\pi(x').$$

به همریختی حلقه‌ای پوشا π همریختی حلقه‌ای طبیعی گوییم.

تذکر ۱۲.۵.۳. به همریختی حلقه‌ای یک‌به‌یک $f : R \longrightarrow S$ بعضا نشاننده نیز گوییم و آن را با $R \hookrightarrow S$ نشان می‌دهیم. علت نامگذاری نشاننده قضیه اول یکریختی حلقه‌ای است که در ادامه خواهیم دید.

تعریف و مثال ۱۳.۵.۳. فرض کنیم R یک حلقه و S زیرحلقه R باشد. به وضوح $i : S \longrightarrow R$ با ضابطه $i(x) = x$ یک همریختی حلقه‌ای یک‌به‌یک (نشاننده) است و به آن همریختی حلقه‌ای شمول گوییم.

تعریف ۱۴.۵.۳. به همریختی حلقه‌ای $f : R \longrightarrow R$، درون‌ریختی (اندومورفیسم) روی حلقه R گوییم.

تعریف و مثال ۱۵.۵.۳. فرض کنیم R یک حلقه باشد. واضح است که $id_R : R \longrightarrow R$ با ضابطه $id_R(x) = x$ یک درون‌ریختی است که به آن درون‌ریختی حلقه‌ای همانی گوییم.

مثال ۱۶.۵.۳. حلقه $R = \mathbb{Q}[x]$ را در نظر بگیرید. یک بررسی ساده نشان می‌دهد که تابع

$$\theta : R \longrightarrow R,\ \ \theta(f(x)) = f(x^۲)$$

یک درون‌ریختی است.

حال گزاره زیر را داریم.

گزاره ۱۷.۵.۳. فرض کنیم $f : R \longrightarrow S$ یک همریختی حلقه‌ای باشد. در این صورت موارد زیر برقرار است.
(الف) همواره داریم $f(\circ_R) = \circ_S$.
(ب) $f(-a) = -f(a)$.
(ج) برای هر عدد صحیح n داریم $f(a^n) = (f(a))^n$.
(د) اگر R یکدار باشد آنگاه $f(۱_R)$ یک حلقه S است.

اثبات. (الف) برای هر $a \in R$، داریم که $f(a) = f(a + \circ_R) = f(a) + f(\circ_R)$. لذا $f(\circ_R) = \circ_S$.
(ب) طبق (الف) داریم $\circ_S = f(\circ_R) = f(a - a) = f(a) - f(a)$ و چیزی برای اثبات نداریم.
(ج) و (د) سر راست است. □

گزاره ۱۸.۵.۳. موارد زیر برقرار است.
(الف) وارون یکریختی حلقه‌ای $f : R \longrightarrow S$ یک یکریختی حلقه‌ای است.
(ب) اگر $f : R \longrightarrow S$ و $g : S \longrightarrow T$ همریختی حلقه‌ای باشند آنگاه $gf : R \longrightarrow T$ همریختی حلقه‌ای است.
(ج) یکریخت بودن حلقه‌ها یک رابطه هم ارزی است.

اثبات. مشابه اثبات قضیه ۲۳.۹.۲ است. $\square$

از فصل اول یادآوری می‌کنیم که برای تابع $f : X \longrightarrow Y$ به

$$f(X) = Im(f) = \{f(x) \mid x \in X\}$$

برد تابع گوییم. اکنون گزاره زیر را داریم.

گزاره ۱۹.۵.۳. *فرض کنیم R و S دو گروه و $f : R \longrightarrow S$ همریختی حلقه‌ای باشد.*
(الف) $Im(f)$ زیرحلقه S است (که تصویر هم ریخت تحت f نامیده می‌شود).
(ب) اگر $I \leq_l R$ آنگاه $Im(f) \leq_l f(I)$. در نتیجه اگر f پوشا باشد آنگاه $H \leq_l f(K)$. حکم مشابه برای ایده‌آل راست برقرار است.
(ج) اگر $S \leq_l J$ آنگاه $f^{-1}(J) = \{x \in R \mid f(x) \in J\}$ ایده‌آل چپ R است. حکم مشابه برای ایده‌آل راست برقرار است.

اثبات. (الف) طبق گزاره قبل $f(0) = 0$ و لذا $0 \in Im(f)$. پس $Im(f)$ ناتهی است. فرض کنیم $u, v \in Im(f)$. لذا $x, y \in R$ چنان وجود دارند که $f(x) = u$ و $f(y) = v$ و درنتیجه

$$u - v = f(x) - f(y) = f(x - y) \in Im(f).$$

از سوی دیگر،

$$uv = f(x)f(y) = f(xy) \in Im(f).$$

حال طبق قضیه ۶.۲.۳ باید $Im(f) \leq S$.

(ب) چون $0 \in I$، پس طبق گزاره قبل $f(0) = 0$ و لذا $0 \in f(I)$. پس $f(I)$ ناتهی است. اما زیر گروه جمعی بودن $f(I)$ واضح است (چرا؟ از کدام مطلب؟). فرض کنیم $u \in f(I)$. لذا $x \in I$ چنان وجود دارند که $f(x) = u$. حال فرض کنیم $r \in Im(f)$ و لذا $r = f(y)$ که $y \in R$. چون I ایده‌آل چپ است داریم $yx \in I$ و

$$ru = f(y)f(x) = f(yx) \in f(I).$$

حال طبق کار تمام است. قسمت دوم، نتیجه مستقیم قسمت اول است.

(ج) واضح است که $0 \in J$ و طبق گزاره قبل $f(0) = 0$ و لذا $0 \in f^{-1}(J)$. پس $f^{-1}(J)$ ناتهی است. اما زیر گروه جمعی بودن $f(I)$ واضح است (چرا؟ از کدام مطلب؟). فرض کنیم $x \in f^{-1}(J)$. بنابراین $u \in J$ وجود دارد که $f(x) = u$. حال فرض کنیم $r \in R$. لذا $f(r) \in S$. چون J ایده‌آل چپ S است داریم $f(r)u = f(r)f(x) = f(rx) \in J$. در نتیجه $rx \in f^{-1}(J)$. $\square$

تذکر ۲۰.۵.۳. *فرض کنیم $f : R \longrightarrow S$ یک همریختی حلقه‌ای باشد. اگر R جابجایی باشد واضح است که $Im(f)$ جابجایی است.*

تذکر ۲۱.۵.۳. فرض کنیم $f : R \longrightarrow S$ یک همریختی حلقه‌ای باشد. لزومی ندارد که $Im(f)$ در S ایده‌آل (چپ، راست) باشد. برای مثال همریختی حلقه‌ای

$$f : \mathbb{Z} \longrightarrow M_۲(\mathbb{Z}), \;\; f(n) = \begin{pmatrix} n & ۰ \\ ۰ & ۰ \end{pmatrix}.$$

را در نظر بگیرید. واضح است که f همریختی حلقه‌ای است (بررسی کنید). اما

$$Im(f) = \{ \begin{pmatrix} n & ۰ \\ ۰ & ۰ \end{pmatrix} \mid n \in \mathbb{Z}\}$$

ایده‌آل چپ $M_۲(\mathbb{Z})$ نیست (بررسی کنید). همچنین $\begin{pmatrix} ۱ & ۰ \\ ۰ & ۰ \end{pmatrix} \in Im(f)$ عنصر یک زیرحلقه $Im(f)$ است اما یک حلقه $M_۲(\mathbb{Z})$ نیست.

تعریف ۲۲.۵.۳. برای همریختی حلقه‌ای $f : R \longrightarrow S$
(الف) به $Im(f)$ تصویر همریختی f گوییم.
(ب) $f^{-۱}(\{۰\}) = \{x \in R \mid f(x) = ۰\}$ هسته همریختی f گوییم و با نماد $Ker(f)$ آن را نمایش می‌دهیم ($Ker(f) = \{x \in R \mid f(x) = ۰\}$). دقت شود که چون $\{۰\}$ ایده‌آل است، $Ker(f)$ نیز ایده‌آل است.
(ج) اگر f پوشا باشد آنگاه به S تصویر همریخت R گوییم.

مثال ۲۳.۵.۳. همریختی حلقه‌ای

$$f : \mathbb{Z} \longrightarrow M_۲(\mathbb{Z}), \;\; f(n) = \begin{pmatrix} n & ۰ \\ ۰ & ۰ \end{pmatrix}.$$

را در نظر بگیرید. داریم

$$Ker(f) = \{x \in \mathbb{Z} \mid f(x) = ۰\} = \{x \in \mathbb{Z} \mid \begin{pmatrix} n & ۰ \\ ۰ & ۰ \end{pmatrix} = \begin{pmatrix} ۰ & ۰ \\ ۰ & ۰ \end{pmatrix}\} = \{۰\}.$$

دقت شود که f یک‌به‌یک است! ارتباط جالبی بین یک‌به‌یک بودن همریختی و هسته همریختی وجود دارد که در ادامه خواهیم دید.

مثال ۲۴.۵.۳. داریم که

$$f : \mathbb{Z} \longrightarrow \mathbb{Z}_۳, \quad f(x) = \bar{x}$$

یک همریختی است که به وضوح $Im(f) = \mathbb{Z}_۳$ یعنی f پوشا است. لذا $\mathbb{Z}_۳$ تصویر همریخت $\mathbb{Z}$ است. اما

$$Ker(f) = \{x \in \mathbb{Z} \mid f(x) = \bar{۰}\} = \{x \in \mathbb{Z} \mid \bar{x} = \bar{۰}\} = ۳\mathbb{Z}.$$

دقت شود که f یک‌به‌یک نیست! ارتباط جالبی بین یک‌به‌یک بودن همریختی و هسته همریختی وجود دارد که در ادامه خواهیم دید(شاید همین الان حدس زده باشید!).

اکنون گزاره زیر را داریم.

گزاره ۲۵.۵.۳. *هر ایده‌آل مانند I از حلقه R هسته یک همریختی حلقه‌ای است.*

اثبات. همریختی حلقه‌ای طبیعی

$$\pi : R \longrightarrow R/I,\ \ \pi(x) = x + I$$

را در نظر می‌گیریم. داریم

$$Ker(\pi) = \{x \in R \mid \pi(x) = I\} = \{x \in R \mid x + I = I\} = I$$

و اثبات کامل است. □

گزاره ۲۶.۵.۳. *برای هر ایده‌آل مانند I از حلقه R، R/I تصویر همریخت R است.*

اثبات. همریختی حلقه‌ای طبیعی

$$\pi : R \longrightarrow R/I,\ \ \pi(x) = x + I$$

پوشا است. □

گزاره زیر نشان می‌دهد که برای فهمیدن یک‌به‌یک بودن یک همریختی حلقه‌ای کافی است هسته آن بررسی شود. دقت کنید که این گزاره را برای هر تابعی به کار نبرید، فقط همریختی!

گزاره ۲۷.۵.۳. *فرض کنیم $f : R \longrightarrow S$ یک همریختی حلقه‌ای باشد. در این صورت f یک‌به‌یک است اگر و تنها اگر $Ker(f) = \{0\}$.*

اثبات. ($\Leftarrow$) فرض کنیم $x \in Ker(f)$. لذا باید $f(x) = 0$. اما می‌دانیم که $f(0) = 0$ (چرا؟) و در نتیجه $f(x) = f(0)$. چون f یک‌به‌یک است، $x = 0$.
($\Rightarrow$) فرض کنیم $f(x) = f(y)$ که $x, y \in R$. داریم

$$0 = f(x) - f(y) = f(x - y).$$

لذا $x - y \in Ker(f) = \{0\}$. پس $x = y$ و f یک‌به‌یک است. □

تذکر ۲۸.۵.۳. *فرض کنیم $f : R \longrightarrow S$ یک همریختی حلقه‌ای باشد. اگر $Ker(f) = R$ یا $Im(f) = \{0\}$ باشد آنگاه f همریختی بدیهی ($f = 0$) است.*

اکنون اولین قضیه یکریختی حلقه‌ای که بسیار پر کاربرد است را بیان و اثبات می‌کنیم. مطالبی که در ادامه می‌آید بسیار شبیه به بخش ۹ از فصل دوم است. تکنیک‌های اثبات شبیه به آن چیزی است که در گروه‌ها دیده‌اید.

قضیه ۲۹.۵.۳. (*قضیه اول یکریختی حلقه‌ای*) *فرض کنیم $f : R \longrightarrow S$ یک همریختی حلقه‌ای باشد. در این صورت داریم (به صورت حلقه‌ای) $R/Ker(f) \cong Im(f)$. به ویژه اگر f پوشا باشد آنگاه $R/Ker(f) \cong S$.*

اثبات. طبق مطلبی که در بالا اشاره شد $Ker(f)$ ایده‌آل R است و حلقه خارج قسمتی $R/Ker(f)$ با معنی است. حال قرار می‌دهیم

$$\varphi : R/Ker(f) \longrightarrow Im(f),\ \ \varphi(x + Ker(f)) = f(x).$$

ضابطه φ در بالا خوشتعریف است. زیرا برای هر $x + Ker(f) \in R/Ker(f)$ واضح است که داریم $\varphi(x + Ker(f)) = f(x) \in Im(f)$. همچنین اگر $x + Ker(f) = y + Ker(f)$ آنگاه $x - y + Ker(f) = Ker(f)$ و لذا باید $x - y \in Ker(f)$. بنابراین $f(x - y) = ۰$. چون f همریختی حلقه‌ای است داریم $f(x) - f(y) = ۰$. بنابراین $f(x) = f(y)$ و لذا $\varphi(x + Ker(f)) = \varphi(y + Ker(f))$.
واضح است که φ همریختی گروهی (جمعی) است و فقط باید همریختی حلقه‌ای را بررسی کنیم. یعنی

$$\begin{aligned}&\varphi((x + Ker(f))\ (y + Ker(f))) = \varphi(xy + Ker(f)) = f(xy) = \\ &f(x)f(y) = \varphi(x + Ker(f))\ \varphi(y + Ker(f)).\end{aligned}$$

φ پوشا است. زیرا اگر $u \in Im(f)$ آنگاه $f(x) = u$ که $x \in R$. لذا $\varphi(x+Ker(f)) = f(x)$.
φ همریختی حلقه‌ای یک‌به‌یک است. زیرا اگر فرض کنیم $x + Ker(f) \in Ker(\varphi)$ آنگاه خواهیم داشت $\varphi(x + Ker(f)) = ۰ \in Im(f) \subseteq S$. یعنی $f(x) = ۰$ و در نتیجه $x \in Ker(f)$. لذا $x + Ker(f) = Ker(f)$. بنابراین $Ker(\varphi) = \{Ker(f)\}$ و طبق گزاره ۲۷.۵.۳ باید φ یک‌به‌یک باشد. در نتیجه φ یکریختی است و $M/Ker(f) \cong Im(f)$.
برای قسمت آخر، اگر f پوشا باشد آنگاه $Im(f) = S$ و لذا $R/Ker(f) \cong S$. $\square$

مثال ۳۰.۵.۳. *همریختی حلقه‌ای $f : \mathbb{Z} \longrightarrow \mathbb{Z}_۵$ با ضابطه $f(x) = \bar{x}$ پوشا است. به علاوه $Ker(f) = ۵\mathbb{Z}$ و لذا طبق قضیه اول یکریختی حلقه‌ای، قضیه ۲۹.۵.۳، داریم $\mathbb{Z}/۵\mathbb{Z} \cong \mathbb{Z}_۵$. با همین تکنیک برای هر $n \in \mathbb{N}$ داریم $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$.*

تذکر ۳۱.۵.۳. *اگر برای ایده‌آل I از حلقه R داشته باشیم $R/I = \{۰\}$ آنگاه $R = I$. همچنین همواره داریم $R/\{۰\} = R$.*

قضیه ۳۲.۵.۳. *(قضیه دوم یکریختی حقله‌ای) فرض کنیم R یک حلقه و I ایده‌آل R باشد. همچنین فرض کنیم S زیرحلقه R است. در این صورت داریم $(S + I)/I \cong S/(S \cap I)$.*

اثبات. ابتدا باید توجه کنیم که $S \cap I$ یک ایده‌آل S است. همچنین $S + I$ زیرحلقه‌ای از R است که I ایده‌آل آن است. لذا حلقه‌های خارج قسمتی $S/(S \cap I)$ و $(S + I)/I$ با معنی هستند. اکنون قرار می‌دهیم

$$\varphi : S \longrightarrow (S + I)/I,\ \ \varphi(x) = x + I.$$

φ خوشتعریف است (بررسی کنید). φ یک همریختی حلقه‌ای است

$$\varphi(xy) = xy + I = (x + I)\ (y + I) = \varphi(x)\varphi(y).$$

φ پوشا است. زیرا اگر $u+I \in (S+I)/I$ آنگاه $u = s+i$ که $s \in S$ و $i \in I$. طبق زیرگروه بودن I داریم $i+I = I$ و لذا $u+I = s+i+I = s+I = \varphi(s)$.
اما

$$Ker(\varphi) = \{x \in S \mid \varphi(x) = I\} = \{x \in S \mid x+I = I\} = \{x \in S \mid x \in I\} = S \cap I.$$

اکنون طبق قضیه اول یکریختی حلقه‌ای، قضیه ۲۹.۵.۳ داریم

$$S/(S\cap I) = S/Ker(\varphi) \cong Im(\varphi) = (S+I)/I$$

و اثبات کامل است. □

مثال ۳۳.۵.۳. *زیرحلقه (غیر یکدار) $۴\mathbb{Z}$ و ایده‌آل $۶\mathbb{Z}$ از $\mathbb{Z}$ را در نظر بگیرید. طبق قضیه دوم یکریختی، قضیه ۳۲.۵.۳ داریم*

$$۲\mathbb{Z}/۶\mathbb{Z} = (۴\mathbb{Z}+۶\mathbb{Z})/۶\mathbb{Z} \cong ۴\mathbb{Z}/(۶\mathbb{Z}\cap ۴\mathbb{Z}) = ۴\mathbb{Z}/۱۲\mathbb{Z}.$$

قضیه ۳۴.۵.۳. *(قضیه سوم یکریختی حلقه‌ای) فرض کنیم R یک حلقه باشد، $I, J \trianglelefteq R$ و $I \subseteq J$. در این صورت داریم*

$$(R/I)/(J/I) \cong R/J.$$

اثبات. ابتدا دقت شود که $I, J \trianglelefteq R$ و حلقه‌های خارج قسمتی R/I و R/J با معنی هستند. همچنین J/I ایده‌آل R/I است و حلقه خارج قسمت $(R/I)/(J/I)$ با معنی است. اکنون قرار می‌دهیم

$$\varphi : R/I \longrightarrow R/J, \quad \varphi(x+I) = x+J.$$

φ خوشتعریف است. زیرا واضح است که برای هر $x \in R$، $x+J$ یک عضو از R/J است. همچنین اگر $x+I = x'+I$ آنگاه $x'-x+I = I$ و لذا $x'-x \in I$. در نتیجه $x'-x \in J$ و این یعنی $x'-x+J = J$. بنابراین $x+J = x'+J$ و $\varphi(x+I) = \varphi(x'+I)$.
φ یک همریختی حلقه‌ای است (جمعی واضح است)

$$\varphi((x+I)(y+I)) = \varphi(xy+I) = xy+J = (x+J)(y+J) = \varphi(x+I)\varphi(y+I).$$

به وضوح φ پوشا است. اما

$$Ker(\varphi) = \{x+I \in R/I \mid \varphi(x+I) = I\} = \{x+I \in R/I \mid x+J = J\} = \{x+I \in R/I \mid x \in J\} = J/I.$$

اکنون طبق قضیه اول یکریختی حلقه‌ای، قضیه ۲۹.۵.۳ داریم

$$(R/I)/(J/I) = (R/I)/Ker(\varphi) \cong Im(\varphi) = J/I.$$

اثبات کامل است. □

مثال ۳۵.۵.۳. *ایده‌آل‌های $۴\mathbb{Z}$ و $۸\mathbb{Z}$ از $\mathbb{Z}$ را در نظر بگیرید. طبق قضیه سوم یکریختی حلقه‌ای، قضیه ۳۴.۵.۳ داریم*
$$(\mathbb{Z}/۸\mathbb{Z})/(۴\mathbb{Z}/۸\mathbb{Z}) \cong \mathbb{Z}/۴\mathbb{Z} \cong \mathbb{Z}_۴.$$

تذکر ۳۶.۵.۳. *به قضیه سوم یکریختی بعضا قضیه یکریختی خارج قسمتی مضاعف نیز گویند (برخی در ایران این قضیه را به دور در دور و نزدیک در نزدیک نیز می‌شناسند! چون بسیار شبیه به ساده‌سازی تقسیم دو عدد گویا است).*

حال قضیه تناظر را بیان می‌کنیم.

قضیه ۳۷.۵.۳. (قضیه تناظر برای حلقه) *فرض کنیم $f : R \longrightarrow S$ یک همریختی حلقه‌ای پوشا باشد. یک تناظر بین خانواده ایده‌آل‌های R که شامل $Ker(f)$ هستند و خانواده ایده‌آل‌های S وجود دارد. همچنین یک تناظر بین خانواده ایده‌آل‌های چپ (راست) R که شامل $Ker(f)$ هستند و خانواده ایده‌آل‌های چپ (راست) S وجود دارد.*

اثبات. قضیه را برای ایده‌آل‌های چپ اثبات می‌کنیم، بقیه موارد کاملا مشابه است. قرار می‌دهیم
$$\mathcal{A} = \{I \leq R \mid Ker(f) \subseteq I\} \qquad \mathcal{B} = \{J \mid J \trianglelefteq S\}$$
و تعریف می‌کنیم
$$\theta : \mathcal{A} \longrightarrow \mathcal{B}, \ \ \theta(I) = f(I).$$
θ خوشتعریف است. زیرا برای هر $I \leq_l R$، طبق گزاره ۱۹.۵.۳ قسمت (ب) داریم $f(I) \leq_l S$ و در نتیجه $\theta(I) = f(I) \in \mathcal{B}$. همچنین اگر $I_۱ = I_۲$ آنگاه واضح است که داریم $f(I_۱) = f(I_۲)$ و لذا $\theta(I_۱) = \theta(I_۲)$.
θ پوشا است. فرض کنیم $J \in \mathcal{B}$. طبق گزاره ۱۹.۵.۳ قسمت (ج)، $f^{-۱}(J)$ ایده‌آل چپ R است. حال طبق لم ۴۵.۹.۲ قسمت (ب) داریم
$$\theta(f^{-۱}(J)) = f(f^{-۱}(J)) = J.$$
θ یک‌به‌یک است. زیرا اگر فرض کنیم که $\theta(I_۱) = \theta(I_۲)$ یعنی $f(I_۱) = f(I_۲)$ آنگاه خواهیم داشت $f^{-۱}(f(I_۱)) = f^{-۱}(f(I_۲))$. حال طبق لم ۴۵.۹.۲ قسمت (الف) باید $I_۱ = I_۲$ باشد. □

حال نتیجه بسیار مهم زیر را داریم.

تذکر ۳۸.۵.۳. *اگر $f : R \longrightarrow S$ یک همریختی دلخواه باشد آنگاه قضیه تناظر زمانی صحیح است که S را با $Im(f)$ عوض کنیم.*

تذکر ۳۹.۵.۳. *قضیه تناظر را با نام‌های قضیه چهارم یکریختی گروهی و یا قضیه مشبکه نیز می‌شناسند.*

بخش را با نتیجه زیر به پایان می‌رسانیم.

نتیجه ۴۰.۵.۳. *فرض کنیم I ایده‌آل (چپ_ راست) از حلقه R باشد. برای هر ایده‌آل (چپ_ راست) L از R/I ایده‌آل (چپ_ راست) مانند J از R شامل I وجود دارد که $L = J/I$.*

اثبات. با کمک همریختی طبیعی حلقه‌ای و قضیه تناظر، قضیه ۳۷.۵.۳، یک بررسی ساده است. □

تمرین‌های حل شده

تمرین ۴۱.۵.۳. *تمام همریختی‌های حلقه‌ای از $\mathbb{Z}$ به $\mathbb{Z}$ را پیدا کنید.*

حل. فرض کنبم $f:\mathbb{Z}\longrightarrow\mathbb{Z}$ یک همریختی حلقه‌ای باشد. داریم

$$(f(۱))^۲=f(۱)f(۱)=f(۱.۱)=f(۱).$$

لذا در $\mathbb{Z}$ داریم $f(۱)(f(۱)-۱)=۰$. چون $\mathbb{Z}$ دامنه است باید $f(۱)=۰$ یا $f(۱)=۱$. اگر $f(۱)=۰$ آنگاه برای هر $n\in BbbZ$ داریم $f(n)=f(n.۱)=f(n)f(۱)=۰$. لذا همریختی حلقه‌ای بدیهی حاصل می‌شود. اگر $f(۱)=۱$ آنگاه برای هر $n\in\mathbb{Z}$ داریم

$$f(n)=\begin{cases} f(\underbrace{۱+...+۱}_{n})=\underbrace{f(۱)+...+f(۱)}_{n}=\underbrace{۱+...+۱}_{n}=n & n>۰\\ f(\underbrace{-۱-...-۱}_{-n})=\underbrace{f(-۱)+...+f(-۱)}_{-n}=n & n<۰\\ ۰ & n=۰\end{cases}$$

یعنی همریختی حلقه‌ای همانی حاصل می‌شود.

تمرین ۴۲.۵.۳. *نشان دهید که $\mathbb{Z}[x]/<x^۲+۱>\cong\mathbb{Z}[i]$ (i همان است که در اعداد مختلط معرفی شده است و $\mathbb{Z}[i]$ همه اعداد مختلط با ضرایب اعداد صحیح است).*

حل. تابع

$$\theta:\mathbb{Z}[x]\longrightarrow\mathbb{Z}[i],\ \ \theta(f(x))=f(i)$$

یک همریختی حلقه‌ای پوشا است. زیرا داریم

$$\theta(f(x)+g(x))=f(i)+g(i)=\theta(f(x))+\theta(g(x))$$

و

$$\theta(f(x)g(x))=f(i)g(i)=\theta(f(x))\theta(g(i)).$$

فرض کنیم $a+bi\in\mathbb{Z}[i]$. حال داریم

$$\theta(a+bx)=a+bi$$

یعنی θ پوشا است. فرض کنیم که $f(x)\in Ker(\theta)$ یعنی $\theta(f(x))=۰$ و $f(x)=a_nx^n+....+a_۰$. بنابراین $f(i)=a_ni^n+...+a_۰=۰$ و این یعنی i ریشه $f(x)$ است. از طرفی i ریشه $x^۲+۱$ است و در نتیجه $f(x)=(x^۲+۱)g(x)$. این نشان می‌دهد که $f(x)\in<x^۲+۱>$. لذا $Ker(\theta)=<x^۲+۱>$. حال طبق قضیه اول یکریختی، قضیه ۲۹.۵.۳ داریم $\mathbb{Z}[x]/<x^۲+۱>\cong\mathbb{Z}[i]$.

تمرین ۴۳.۵.۳. *فرض کنیم F یک میدان باشد و R حلقه‌ای دلخواه. نشان دهید که هر همریختی ناصفر $f:F\longrightarrow R$ یک‌به‌یک است.*

حل. می‌دانیم که $Ker(f)$ ایده‌آل F است و چون F میدان است، $Ker(f) = \{0\}$ یا $Ker(f) = F$. اگر $Ker(f) = F$ آنگاه f همریختی صفر است که تناقض با فرض است. لذا $Ker(f) = \{0\}$ و طبق گزاره ۲۷.۵.۳، f یک‌به‌یک است.

تمرین ۴۴.۵.۳. *فرض کنیم R یک حلقه و I ایده‌آل R باشد. نشان دهید که $M_n(R/I) \cong M_n(R)/M_n(I)$.*

حل. تابع

$$\theta : M_n(R) \longrightarrow M_n(R/I), \;\; \theta((a_{ij})) = (a_{ij} + I)$$

یک همریختی حلقه‌ای پوشا است. زیرا داریم

$$\begin{aligned} &\theta((a_{ij}) + (b_{ij})) = \theta((a_{ij} + b_{ij})) = (a_{ij} + b_{ij} + I) = \\ &(a_{ij} + I) + (b_{ij} + I) = \theta((a_{ij})) + \theta((b_{ij} + I)) \end{aligned}$$

و

$$\begin{aligned} &\theta((a_{ij})(b_{ij})) = \theta((\sum_{k=1}^{n} a_{ik}b_{kj})) = (\sum_{k=1}^{n} a_{ik}b_{kj} + I) = \\ &(a_{ij} + I)(b_{ij} + I) = \theta((a_{ij}))\theta((b_{ij} + I)). \end{aligned}$$

فرض کنیم $(a_{ij} + I) \in M_n(R/I)$. حال داریم

$$\theta((a_{ij})) = (a_{ij} + I)$$

یعنی θ پوشا است. فرض کنیم که $(a_{ij}) \in Ker(\theta)$ یعنی $\theta((a_{ij})) = 0$ و لذا $a_{ij} + I = I$. بنابراین $a_{ij} \in I$ و لذا $Ker(\theta) = M_n(I)$. حال طبق قضیه اول یکریختی، قضیه ۲۹.۵.۳ داریم $M_n(R/I) \cong M_n(R)/M_n(I)$.

تمرین ۴۵.۵.۳. *تمام ایده‌آل‌های $\mathbb{Z}_n$ را مشخص کنید.*

حل. طبق مثال بعد از قضیه اول یکریختی داریم $\mathbb{Z}_n \cong \mathbb{Z}/n\mathbb{Z}$. حال فرض کنیم I ایده‌آل $\mathbb{Z}/n\mathbb{Z}$ باشد. طبق نتیجه ۴۰.۵.۳ داریم $I = k\mathbb{Z}/n\mathbb{Z}$ که $n\mathbb{Z} \subseteq k\mathbb{Z}$. این ایجاب می‌کند که $k|n$. پس به تعداد مقسوم علیه‌های مثبت عدد n ایده‌آل داریم.

تمرین ۴۶.۵.۳. *حلقه $R \times S$ را در نظر بگیرید و فرض کنیم*

$$T = \{(x, 0) \mid x \in R\} \qquad\qquad T' = \{(0, y) \mid y \in S\}$$

نشان دهید که T و T' ایده‌آل‌های $R \times S$ هستند و سپس نشان دهید که به عنوان حلقه داریم $T \cong R$ و $T' \cong S$.

حل. واضح است که $(\circ, \circ) \in T$ و T ناتهی است. حال برای هر $(x, \circ), (x', \circ) \in T$ و هر $(r, s) \in R \times S$ داریم

$$\begin{aligned} (x, \circ) - (x', \circ) &= (x - x', \circ) \in T \\ (r, s)(x, \circ) &= (rx, \circ) \in T \\ (x, \circ)(r, s) &= (xr, \circ) \in T \end{aligned}$$

و لذا T ایده‌آل است. به روش مشابه T' ایده‌آل است. یک بررسی سر راست نشان می‌دهد که تابع

$$f : R \longrightarrow T, \quad f(r) = (r, \circ)$$

یکریختی حلقه‌ای است و لذا $T \cong R$. با روش مشابه $S \cong T'$.

تمرین ۴۷.۵.۳. *فرض کنیم R یک حلقه باشد. نشان دهید که هر همریختی ناصفر*

$$f : M_n(\mathbb{R}) \longrightarrow R$$

یک نشاننده است.

حل. کافی است نشان دهیم f یک‌به‌یک است. طبق گزاره ۲۷.۵.۳ کافی است نشان دهیم $Ker(f) = \{\circ\}$. می‌دانیم $Ker(f)$ ایده‌آل $M_n(\mathbb{R})$ است. لذا طبق قضیه ۱۰.۴.۳ داریم که $Ker(f) = M_n(I)$ که I ایده‌آل $\mathbb{R}$ است. اما I یا $\{\circ\}$ یا $\mathbb{R}$ است (چرا؟). اگر $I = \mathbb{R}$ باشد آنگاه $Ker(f) = M_n(\mathbb{R})$ و لذا f همریختی صفر (بدیهی) است که تناقض با فرض است. در نتیجه $I = \{\circ\}$ و لذا $Ker(f) = \{\circ\}$.

تمرین ۴۸.۵.۳. *تمام همریختی‌های حلقه‌ای از $\mathbb{Q}$ به $\mathbb{Z}$ را مشخص کنید.*

حل. فرض کنیم $f : \mathbb{Q} \longrightarrow \mathbb{Z}$ یک همریختی حلقه‌ای باشد. f همریختی گروهی (جمعی) نیز می‌باشد. با تکرار استدلال تمرین ۹۵.۹.۲ باید f همریختی بدیهی (صفر) باشد.

تمرین ۴۹.۵.۳. *ایا یک حلقه جابجایی یکدار R وجود دارد که $R[x] \cong \mathbb{Z}$؟*

حل. فرض کنیم چنین Rای موجود باشد که $R[x] \cong \mathbb{Z}$. واضح است که R زیرحلقه $R[x]$ است. لذا باید R با یک زیرحلقه یکدار از $\mathbb{Z}$ یکریخت باشد. اما $(R, +)$ باید با یک زیرگروه جمعی $(\mathbb{Z}, +)$ یکریخت باشد و لذا $R \cong n\mathbb{Z}$. اما R یکدار استدر حالی که $n\mathbb{Z}$ یکدار نیست مگر این که $n = ۱$. در نتیجه بدون کم شدن از کلیت فرض کنیم $R = \mathbb{Z}$. اما $\mathbb{Z}$ با $\mathbb{Z}[x]$ یکریخت نیست. زیرا همه ایده‌آل‌های $\mathbb{Z}$ دوری هستند در حالی که $< ۲, x >$ از $\mathbb{Z}[x]$ دوری نیست (چرا؟).

۶.۳ تاریخچه

نظریه حلقه از نظر تاریخی، پیشینه‌ایی طولانی دارد. شاید اولین حلقه از نظر تاریخی که کشف شد همان حلقه اعداد صحیح باشد. معادله سیاله یا معادلهٔ دیوفانتی در ریاضیات معادله‌ای چند جمله‌ای با متغیرهای صحیح است که در آن بیش از یک متغیر (مجهول) داشته باشیم. حل این معادلات در زمان‌های قدیم در حلقه اعداد صحیح مورد توجه بوده است.

مطالعه به شکل امروزی نظریه حلقه با کارهای عمیق ریاضیدانانی چون گالوا در اوایل قرن نوزدهم شروع شد و سبب پیدایش نظریه‌ی میدان شد. گالوا کارهای عمیقی در نظریه میدان انجام داده است و دو شاخه مهم جبر را به هم مربوط کرده است. قضیه اساسی گالوا ارتباطی بین نظریه گروه و نظریه میدان به دست می‌دهد. اما در حدود همان سال‌های حیات گالوا مطالعه حلقه‌های جبری اعداد توسط ریاضیدانانی شاخص چون گاوس، کومر و ددکیند نیز آغاز شد. نظریه همنهشتی یا حساب پیمانه‌ای سیستمی برای محاسبه با اعداد صحیح است که به وسیله گاوس در کتاب رساله حساب در سال ۱۸۰۱ معرفی شد.

بخش دیگری از مطالعات روی نظریه حلقه‌ها، به ماتریس برمی‌گردد. پیشگامان مطالعه روی حلقه‌ی ماتریس‌ها ریاضیدانانی مانند کیلی، فروبنیوس و هامیلتون بودند. هامیلتون اولین شخصی است که توانست یک حلقه تقسیم (میدانی که شرط جابجایی ندارد) را بسازد و این باور را که حلقه ناجابجایی که نزدیک به میدان باشد وجود ندارد را نقض نمود. این کار هامیلتون سبب پیدایش شاخه جدیدی در نظریه حلقه شد. اما باور دیگری نیز وجود داشت که تنها حلقه‌های ناجابجایی حلقه ماتریس‌ها است. حتی حلقه ناجابجایی هامیلتون نیز به نوعی زیر حلقه‌ای از حلقه ماتریس‌ها روی میدان اعداد مختلط بود. این باور نیز توسط جبردان‌ها نقض شد. جبردان‌های مثل نوتر و ویل در کارهای عمیقی توانستند حلقه‌های ناجابجایی غیر از حلقه مانریس‌ها بسازند. این حلقه‌ها که حلقه‌های چندجمله با روابط خیلی خاص بودن مورد توجه ریاضیدان‌ها قرار گرفتند.

پژوهش روی نظریه حلقه هنوز ادامه دارد و مسایل حل نشده بسیاری در این شاخه مطرح است که برخی از آنها حتی ارتباط بسیاری نزدیکی با شاخه‌های دیگر مثل نظریه اعداد دارند. پژوهش‌های جدید خیلی تخصصی‌تر شده‌اند و بدون گذراندن درس‌های تخصصی این رشته مطالعه مقالات مرتبط دشوار است. اکنون دو شاخه مهم در نظریه حلقه وجود دارد که به حلقه‌های جابجایی و حلقه‌های ناجابجایی نامگذاری شده‌اند. گاهی مرز این دو زیر شاخه به شدت به هم نزدیک می‌شود و گاهی بسیار از هم فاصله می‌گیرند. نظریه‌های جدیدی نیز برای مطالعه حلقه‌ها ایجاد شده است که به شناسایی حلقه‌ها کمک می‌کند مانند نظریه مدول.

۷.۳ تمرین‌های کل فصل

تمرین‌هایی که با علامت ($\star$) یا ($\star\star$) مشخص شده‌اند، زحمت بیشتری را می‌طلبند.

تمرین ۱.۷.۳. *یک حلقه با نامتناهی مقسوم علیه‌های صفر ناصفر مثال بزنید.*

تمرین ۲.۷.۳. *عناصر وارون پذیر حلقه $\mathbb{Z}_n$ را مشخص کنید.*

تمرین ۳.۷.۳. *یک حلقه R با نامتناهی عنصر پوچتوان و با نامتناهی عنصر خودتوان مثال بزنید.*

تمرین ۴.۷.۳. *فرض کنیم R یک دامنه صحیح باشد و $x, y \in R$. اگر $x^m = y^m$، $x^n = y^n$ و $(m, n) = ۱$ آنگاه نشان دهید که $x = y$.*

تمرین ۵.۷.۳. ($\star$) *فرض کنیم R حلقه یکداری باشد. اگر برای عنصر $x \in R$ عنصر یکتایی مانند y موجود باشد که $xyx = x$ آنگاه نشان دهید که x وارون پذیر است.*

تمرین ۶.۷.۳. *اگر $ab \in R$ پوچتوان باشد آنگاه نشان دهید که ba نیز پوچتوان است.*

تمرین ۷.۷.۳. *فرض کنیم R حلقه یکدار باشد. نشان دهید هر عنصر خودتوان متمایز از ۰ و ۱ مقسوم علیه صفر است.*

تمرین ۸.۷.۳. *یک حلقه و یک زیرحلقه چنان مثال بزنید که حلقه یکدار نباشد اما زیرحلقه یکدار باشد.*

تمرین ۹.۷.۳. ($\star$) *اگر برای عنصر x در حلقه R داشته باشیم $x = x^۴$ آنگاه نشان دهید که R جابجایی است.*

تمرین ۱۰.۷.۳. *اگر برای عنصر x در حلقه R داشته باشیم $x = x^۶$ آنگاه نشان دهید که $x = x^۲$ است.*

تمرین ۱۱.۷.۳. *اگر برای هر عنصر a در حلقه R، از $a^۲ = ۰$ نتیجه شود که $a = ۰$، آنگاه نشان دهید که تمام خودتوان‌ها در مرکز R قرار دارند.*

تمرین ۱۲.۷.۳. *در مورد جابجایی بودن حاصل ضرب دکارتی خانواده‌ای از حلقه چه می‌توان گفت؟*

تمرین ۱۳.۷.۳. ($\star$) *فرض کنیم R یک حلقه با بیشتر از یک عنصر باشد. نشان دهید که اگر معادله $ax = b$ برای تمام عناصر ناصفر $a \in R$ و تمام عناصر $b \in R$ دارای جواب باشد آنگاه R حلقه تقسیم است.*

تمرین ۱۴.۷.۳. ($\star$) *فرض کنیم R یک حلقه با عنصر همانی راست e باشد. نشان دهید که اگر برای هر عنصر ناصفر $a \in R$ عنصر $b \in R$ موجود باشد که $ba = e$ آنگاه R حلقه تقسیم است.*

تمرین ۱۵.۷.۳. *نشان دهید که یک حلقه با تعداد کمتر از ۸ عضو جابجایی است.*

تمرین ۱۶.۷.۳. *فرض کنیم R یک حلقه با $p^۲$ عنصر باشد که p عدد اول است. نشان دهید R جابجایی است.*

تمرین ۱۷.۷.۳. نشان دهید که یک حلقه متناهی با بیش از یک عنصر و بدوم مقسوم علیه صفر، حلقه تقسیم است.

تمرین ۱۸.۷.۳. برای حلقه جابجایی R با مشخصه عدد اول p و عدد طبیعی n نشان دهید همواره داریم $(a+b)^{p^n} = a^{p^n} + b^{p^n}$ که در آن $a, b \in R$.

تمرین ۱۹.۷.۳. $(\star\star)$ یک حلقه ناجابجایی غیر یکدار مانند R چنان مثال بزنید که هر ایده‌ال راست R یک ایده‌آل باشد اما در R ایده‌آل چپی موجود باشد که ایده‌ال نیست.

تمرین ۲۰.۷.۳. $(\star)$ فرض کنیم F یک میدان باشد. نشان دهید در حلقه $F[[x]]$ هر ایده‌آل ناصفر به صورت $< x^k >$ است که در آن $k \in \mathbb{W}$.

تمرین ۲۱.۷.۳. نشان دهید که مجموعه عناصر پوچتوان در حلقه جابجایی R یک ایده‌آل است. در مورد حلقه ناجابجایی چه نتیجه‌ای می‌توان گرفت؟

تمرین ۲۲.۷.۳. برای حلقه R نشان دهید که $M_n(R^{op}) \cong (M_n(R))^{op}$.

تمرین ۲۳.۷.۳. مشخصه حلقه $\mathbb{Z}_n \times \mathbb{Z}_m$ را پیدا کنید.

تمرین ۲۴.۷.۳. نشان دهید که $\mathbb{Z}_۴ \times \mathbb{Z}_۴$ سه زیرحلقه یکدار دارد.

تمرین ۲۵.۷.۳. $(\star)$ فرض کنیم $S = M_۲(\mathbb{Q})$ و R مجموعه همه ماتریس‌های مربعی ۲ × ۲ باشد که با $\begin{pmatrix} ۱ & ۰ \\ ۰ & ۱ \end{pmatrix}$ جابجا می‌شوند. نشان دهید که R زیرحلقه S است و $R \cong \mathbb{Q}[x]/< x^۲ >$.

تمرین ۲۶.۷.۳. اگر برای عنصر x در حلقه R داشته باشیم $x^۲ = x$ آنگاه نشان دهید که هر ایده‌آل تولید متناهی دوری است.

تمرین ۲۷.۷.۳. $(\star)$ فرض کنیم R یک حلقه جابجایی و یکدار با ایده‌آل I باشد که $I^۲ = I$. اگر I تولید متناهی باشد آنگاه نشان دهید که $I =< e >$ که $e^۲ = e$.

تمرین ۲۸.۷.۳. تمام حلقه‌های یکدار غیریکریخت ۴ عضوی را شناسایی کنید.

تمرین ۲۹.۷.۳. فرض کنیم F میدان باشد. نشان دهید گروه‌های $U(F)$ و $(F, +)$ یکریخت نیستند.

تمرین ۳۰.۷.۳. $(\star)$ نشان دهید که حلقه تقسیم D که تعداد متناهی درون‌ریختی دارد جابجایی است.

تمرین ۳۱.۷.۳. $(\star)$ فرض کنیم R حلقه متناهی باشد. نشان دهید اعداد طبیعی m و n با شرط $m > n$ چنان وجود دارند که برای هر $x \in R$ داریم $x^m = x^n$.

تمرین ۳۲.۷.۳.

تمرین ۳۳.۷.۳. $(\star)$ فرض کنیم R حلقه یکدار و متناهی باشد و x عنصری از R باشد که مقسوم علیه صفر نیست. نشان دهید که x وارونپذیر است.

تمرین ۳۴.۷.۳. $(\star\star)$ عدد اصلی تمام زیرحلقه‌های $\mathbb{Q}$ را پیدا کنید (حتما پاسخ با دلیل ریاضی ارائه نمایید).

تمرین ۳۵.۷.۳. $(\star\star)$ فرض کنیم R یک حلقه یکدار و دامنه صحیح باشد و G زیرگروهی متناهی از $U(R)$. نشان دهید که G دوری است.

کتاب‌نامه

[1] Bhattacharya, P. B.; Jain, S. K.; Nagpaul, S. R. Basic abstract algebra. Second edition. Cambridge University Press, Cambridge, 1994.

[2] Herstein, I. N. Abstract algebra. Third edition. With a preface by Barbara Cortzen and David J. Winter. Prentice Hall, Inc., Upper Saddle River, NJ, 1996.

[3] Hungerford, Thomas W. Algebra. Reprint of the 1974 original. Graduate Texts in Mathematics, 73. Springer-Verlag, New York-Berlin, 1980.

[4] Malik, D.S.; Mordeson, J.N.; Sen, M.K. Fundamentals of abstract algebra. McGraw-Hill, 1997.

[5] Rotman, J. Advanced modern algebra, 2002.

[6] Rotman, J. An introduction to homological algebra, 1997.