جبر ۱
دانشگاه صنعتی اصفهان

مدرس: محسن خانی
گردآوری: علی‌سینا سلطانی

۷ اردیبهشت ۱۴۰۳

فهرست مطالب

۱ گروه‌ها ۲

۱.۱ تعریف گروه . . . ۲

۲.۱ زیرگروه و هم‌مجموعه . . . ۶

۳.۱ مرتبهٔ یک عنصر . . . ۸

۴.۱ تبدیل مجموعهٔ هم‌مجموعه‌ها به یک گروه، و زیرگروه نرمال . . . ۹

۵.۱ قضیهٔ کُشی . . . ۱۲

۶.۱ گروه باقی‌مانده‌ها بر n . . . ۱۳

۱.۶.۱ روش اول . . . ۱۳

۷.۱ روش دوم . . . ۱۵

۸.۱ گروه باقی‌مانده‌ها با عمل ضرب و قضیهٔ اویلر . . . ۱۶

۹.۱ قضیهٔ سیلو برای گروه‌های آبلی . . . ۱۸

۱۰.۱ همومرفیسم . . . ۱۹

۱۱.۱ تبدیل یک همومرفیسم پوشا به یک ایزمرفیسم . . . ۲۰

۱۲.۱ قضیهٔ اول همومرفیسم گروه‌ها . . . ۲۲

۲ تمرین‌های بخش گروه‌ها ۲۳

۱.۲ نوبت اول . . . ۲۳

فصل ۱

گروه‌ها

در نظریهٔ گروه‌ها به بررسی ساختارهای ساده‌ای پرداخته می‌شود که در آنها تنها یک عمل، به نام ضرب یا جمع وجود دارد. در فیزیک نظری، بررسی گروه‌های تقارنی بلورها، برای حل معادلهٔ دیفرانسیل تابع موج کاربرد دارد. در ریاضی، نظریهٔ گروه‌ها کاربردهای فراوانی دارد که یکی از آنها استفاده از قضایای سیلو و استفاده از گروه‌های حل‌پذیر، در نظریهٔ گالوا است.

۱.۱ تعریف گروه

تعریف ۱. فرض کنید G یک مجموعه باشد و

$$* : G \times G \longrightarrow G$$

یک تابع دارای ویژگی‌های زیر باشد:

۱. $\forall a, b, c \quad a * (b * c) = (a * b) * c$ (شرکت پذیری)

۲. $\exists e \quad \forall a \quad e * a = a * e = a$ (وجود حداقل یک عضو خنثی)

۳. اگر e یکی از عناصری باشد که شرط مورد دوم را برآورده می‌کند: $\forall a \quad \exists b \quad a * b = b * a = e$ (وجود حداقل یک عضو وارون)

شرط‌های دوم و سوم را می‌توان به صورت دقیق‌تر زیر نوشت:

$$\exists e \Big((\forall a \quad e * a = a * e = a) \wedge (\forall a \exists b \quad a * b = b * a = e) \Big).$$

گاهی در تعریف گروه می‌نویسند: باید برای هر $a, b \in G$ حاصل $a * b$ در G باشد؛ اما وقتی گفته‌ایم که $* : G \times G \to G$ منظورمان همین است!

توجه ۲.

۱. عمل گروه را می‌توان به جای $*$ با هر علامتی مثل $+$ یا $\cdot$ نیز نشان داد. در این صورت معمولا به جای $a * b$ خواهیم نوشت: ab یا $a.b$ یا $a + b$. ما بیشتر اوقات از علامت ab استفاده خواهیم کرد.

۲. تعریف می‌کنیم: $a^n = \underbrace{a \ldots a}_{n \text{بار}}$. وقتی عمل گروه را با علامت جمع نشان می‌دهیم، به جای a^n باید بنویسیم: na.

۳. ویژگی شرکت پذیری، عملاً به ما اجازه می‌دهد که به جای $a(bc)$ یا $(ab)c$ با خیال راحت بنویسیم: abc. در واقع وقتی می‌نویسیم abc هیچ ابهامی وجود ندارد. اما این قانون به ما اجازه نمی‌دهد که به جای abc بنویسیم acb یا bca. حتی اجازه نداریم به جای ab بنویسیم ba مگر در گروه‌های خاصی. به گروه‌هایی که در آن همواره ab با ba برابر است، گروه جابه‌جایی، یا آبلی گفته می‌شود.

یکی از مهم‌ترین مثال‌های گروه، گروه‌های تقارنی است:

مثال ۳. فرض کنید X یک مجموعه باشد. مجموعه تمام توابع یک به یک و پوشا از X به X را با $\mathbf{sym}(X)$ نشان می‌دهیم:[۱]

$$\mathbf{sym}(X) = \{f : X \to X \mid f : \text{یک به یک و پوشا}\}$$

ادعا می‌کنیم $\mathbf{sym}(X)$ با عمل ترکیب توابع یک گروه است. دقت کنید که ترکیب دو تابع یک به یک و پوشا روی X یک تابع یک به یک و پوشا روی X است؛ بنابراین عمل مورد نظر ما به صورت:

$$\circ : \mathbf{sym}(X) \times \mathbf{sym}(X) \to \mathbf{sym}(X)$$

است. حال باید درست بودن شرط‌های تعریف ۱ را بررسی کنیم.
فرض کنید $f, g, h \in \mathbf{sym}(X)$
شرط اول: باید بررسی کنیم که تابع $f \circ (g \circ h)$ با تابع $(f \circ g) \circ h$ برابر است. دقت کنید که دو تابع $h_1, h_2 : X \to X$ زمانی با هم برابر هستند که برای هر $x \in X$ داشته باشیم $h_1(x) = h_2(x)$. پس برای تحقیق شرط اول باید نشان دهیم که برای هر $x \in X$ داریم

$$(f \circ (g \circ h))(x) = ((f \circ g) \circ h)(x).$$

اما واضح است که داریم:

$$(f \circ (g \circ h))(x) = f((g \circ h)(x)) = f(g(h(x)))) = (f \circ g)(h(x)) = ((f \circ g) \circ h)(x).$$

شرط دوم: آیا آین گروه حداقل یک عضو خنثی دارد؟
تابع $\mathrm{id} : X \to X$، را با ضابطهٔ $\forall x \in X \quad \mathrm{id}(x) = x$ در نظر بگیرید (این تابع، همان تابع همانی است). واضح است که برای هر $f \in \mathbf{sym}(X)$ داریم $f \circ \mathrm{id} = \mathrm{id} \circ f$.
شرط سوم: از آنجا که هر f در $\mathbf{sym}(X)$ یک به یک و پوشا است، وارون پذیر است. پس تابع f^{-1} وجود دارد، به طوری که:

$$\mathrm{id} = f \circ f^{-1} = f^{-1} \circ f.$$

توجه ۴. علت این که گفتیم $\mathbf{sym}(X)$ یکی از مهم‌ترین مثال‌های گروه است، این است که به زودی ثابت خواهیم کرد که اساساً هر گروه G زیرگروهی از یک گروهِ به صورت $\mathbf{sym}(X)$ است، برای یک مجموعه‌ی X. به طور دقیق‌تر، اگر G یک گروه باشد، آنگاه یک مجموعه‌ی X وجود دارد، به طوری که $G \subseteq \mathbf{sym}(X)$.

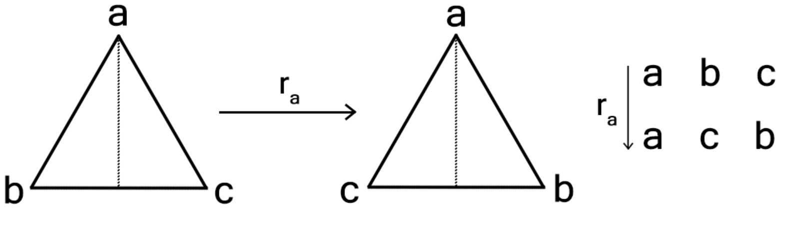
مثال ۵. مثلث متساوی الاضلاع به رئوسِ a, b, c را در نظر بگیرید. تابع $r_a : \mathbb{R}^2 \to \mathbb{R}^2$ را تابعی بگیرید که مثلث را نسبت به خطی که a را به ضلع رو به رو وصل می‌کند، بازتاب می‌کند (این تابع به نقاطی از $\mathbb{R}^2$ که روی مثلث نیستند، کاری ندارد، همچنین نقاط مثلث را به نقاط مثلث (به صورت مجموعه‌وار می‌برد). تابع r_a را می‌توان به گونهٔ دیگری نیز تجسم کرد:

$$r_a : \{a, b, c\} \to \{a, b, c\}$$

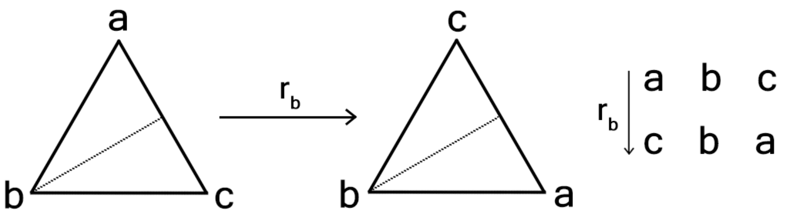
و

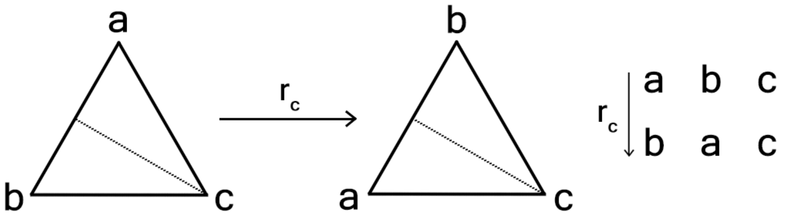
$$r_a(a) = a, r_a(b) = c, r_a(c) = b.$$

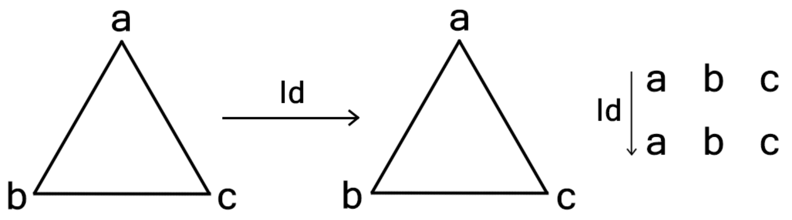
مشابهاً بازتاب‌های r_b, r_c را در نظر می‌گیریم.



---
[۱] مخفف symmetric به معنی تقارنی.

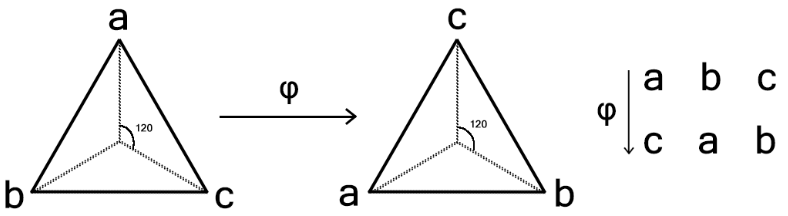


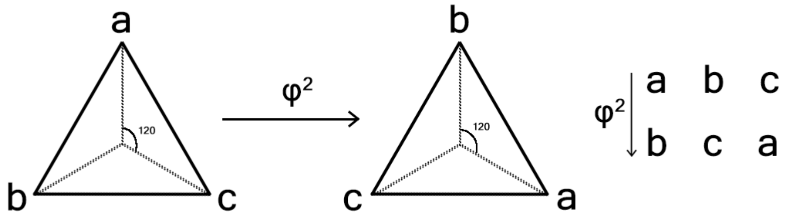




حالا با عمل ترکیب توابع داریم: $r_1r_1 = \mathrm{id}, \quad r_2r_2 = \mathrm{id}, \quad r_3r_3 = \mathrm{id}$

یک دوران به اندازه ۱۲۰ درجه حول نقطهٔ مرکزی، تابعی مانند $\varphi : \mathbb{R}^2 \to \mathbb{R}^2$ است به طوری که:





واضح است که $\varphi^2 = \mathrm{id}$.

مجموعه‌ی همه‌ی شش تابعی را که تعریف کردیم را می‌نویسیم: $\{\mathrm{id}, r_a, r_b, r_c, \varphi, \varphi^2\}$

این مجموعه را مجموعهٔ **تقارن‌های یک سه ضلعی منتظم** می‌نامند و آن را با S_3 نشان می‌دهند. S_3 نیز با عمل ترکیب تقارن‌ها، یک گروه شش عضوی مهم تشکیل می‌دهد که غیر جابه‌جایی است، زیرا به عنوان مثال $r_1r_2 \neq r_2r_1$. بعداً در تمرین‌های درس نشان خواهیم داد که تنها گروه غیر جابه‌جایی ۶ عضوی، همین گروه است.

فعل و انفعالات موجود در گروه S_3 به صورت زیر است. می‌توان مشاهده کرد (فیلم جلسهٔ اول درس را ببینید):

$\varphi = r_3r_1 = r_1r_2 = r_2r_3$

$\varphi^2 = r_1r_3 = r_2r_1 = r_3r_2$

بنابراین می‌توان نوشت:

$r_1\varphi = r_1r_1r_2 = \mathrm{id}r_2 = r_2$،

$r_1\varphi^2 = r_1r_1r_3 = \mathrm{id}r_3 = r_3$

دقت کنید که $\{\mathrm{id}, r_a, r_b, r_c, \varphi, \varphi^2\}$ گروه است ولی $\{r_1, r_2, r_3\}$ یک گروه نیست چون حاصل ترکیب این اعضا در مجموعه وجود ندارد.

لم ۶ (قانون حذف از چپ)**.** فرض کنید G یک گروه باشد و a, b, c، عناصر دلخواهی در G باشند. در این صورت، اگر $ab = ac$ آنگاه $b = c$.

اثبات. فرض کنید $a, b, c \in G$ و $ab = ac$. بنابر ویژگی سوم گروه‌ها، می‌دانیم که عنصری مانند d وجود دارد به طوری که $ad = da = e$ و e عنصری خنثی است. حال داریم:

$$\begin{aligned} & ab = ac \\ \Longrightarrow\ & d(ab) = d(ac) \\ \Longrightarrow\ & (da)b = (da)c \\ \Longrightarrow\ & b = c. \end{aligned}$$

□

مشابهاً، اگر $ba = ca$، آنگاه $b = c$. (قانون حذف از راست).

اثبات.

$$\begin{aligned} & ba = ca \\ \Longrightarrow\ & (ba)d = (ca)d \\ \Longrightarrow\ & b(ad) = c(ad) \\ \Longrightarrow\ & b = c \end{aligned}$$

□

سوال ۱. اگر $ab = ca$ آیا در این صورت $b = c$؟

قوانین نظریهٔ گروه‌ها به ما نمی‌گویند که جواب سوال بالا مثبت است.

تعریف ۷ (عنصر خنثی)**.** فرض کنید G یک گروه باشد. عنصر $e \in G$ را **یک عنصر خنثی** می‌نامیم هرگاه در شرط ویژگی دوم گروه‌ها صدق کند، یعنی:

$$\forall a \in G \quad ae = ea = a.$$

لم ۸. در هر گروه G عنصر خنثی یکتاست (پس می‌شود به جای «یک عنصر خنثی» گفت «عنصر خنثی»).

اثبات. فرض کنید $e_1, e_2 \in G$ هر دو ویژگی خنثی بودن را داشته باشند. فرض کنید، $a \in G$ یک عضو دلخواه باشد. در این صورت:

$$\begin{aligned} & ae_1 = a, \quad ae_2 = a \\ \Longrightarrow\ & ae_1 = ae_2 \\ \Longrightarrow\ & e_1 = e_2. \end{aligned}$$

□

بنا به لم بالا، از این به بعد عضو خنثای یک گروه را با e نشان می‌دهیم.

تعریف ۹ (وارون یک عنصر)**.** فرض کنید $a \in G$ عنصر دلخواهی باشد. عنصر $b \in G$ را **یک عضو وارون برای** a می‌نامیم هرگاه:

$$ab = ba = e.$$

لم ۱۰. فرض کنید $a \in G$ در این صورت فقط یک عضو وارون برای a وجود دارد.

اثبات. فرض کنید a دارای دو وارون b_1 و b_2 باشد (b_1 و b_2 هر دو وارون a باشند). در این صورت:

$$\begin{aligned} ab_1 &= e, \quad ab_2 = e \\ \implies ab_1 &= ab_2 \\ \implies b_1 &= b_2. \end{aligned}$$

□

قرارداد ۱۱. گفتیم که هر عنصر a دارای وارونی یکتاست. وارون یک عنصر a را با a^{-1} نشان می‌دهیم. وقتی از نماد جمع برای عمل گروه استفاده می‌کنیم می‌توانیم وارون a را با $-a$ نیز نشان دهیم.

یک گروه G را بهتر است به صورت $(G, *, e)$ نشان داد تا تمام اجزایش در این نمادگذاری معلوم باشند.

۲.۱ زیرگروه و هم‌مجموعه

تعریف ۱۲. فرض کنید $(G, *, e)$ یک گروه باشد. همچنین فرض کنید $H \subseteq G$ یک **زیرمجموعه** باشد. می‌گوییم H یک **زیرگروه** از G است، هرگاه $(H, *, e)$ خودش یک گروه باشد. در واقع، زیرگروه یعنی زیرمجموعه‌ای که خودش گروه است.

لم ۱۳. فرض کنید G یک گروه و H زیرمجموعه‌ای از G باشد. در این صورت H یک زیرگروه از G است اگر و تنها اگر:

۱. $e_G \in H$.

۲. $\forall a \in H \quad a^{-1} \in H$. دقت کنید که منظور از a^{-1} در اینجا، وارون عنصر a در گروه G است. ما خواسته‌ایم که وارون a که در G است در مجموعهٔ H هم باشد.

۳. $\forall a, b \in H \quad a * b \in H$. دوباره دقت کنید که وقتی $a, b \in H$ آنگاه $a * b$ عنصری در G است، و ما خواسته‌ایم که این عنصر در H باشد.

تمرین ۱. $H \subseteq G$ یک زیرگروه است، اگر و تنها اگر به ازای هر $a, b \in H$ داشته باشیم $ab^{-1} \in H$.

تعریف ۱۴. فرض کنید H یک زیر گروه از G باشد و $a \in G$، یک عنصر دلخواه باشد. **تعریف** می‌کنیم:

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

توجه ۱۵. aH لزوما گروه نیست. اگر aH گروه باشد، باید عضو خنثی را داشته باشد پس یکی از اعضای H باید a^{-1} باشد تا داشته باشیم: $aa^{-1} = e \in aH$ و لزوما این طور نیست.

توجه ۱۶. فرض کنید H یک زیر گروه متناهی از گروه G باشد. در این صورت $|aH| = |H|$؛ یعنی تعداد اعضای مجموعهٔ aH با تعداد اعضای H برابر است.

اثبات. فرض کنید $H=\{h_1,h_2,\dots,h_n\}$، که در این صورت $aH=\{ah_1,ah_2,\dots,ah_n\}$. اگر $ah_1=ah_2$، آنگاه $h_1=h_2$، پس تک تک اعضای aH با هم متفاوتند. پس می‌توان یک تناظر یک به یک بین H و aH تعریف کرد به طوری که:

$$f:H\longrightarrow aH, h\mapsto ah.$$

این نگاشت، یک نگاشت یک به یک و پوشاست پس aH و H هم‌اندازه هستند. □

مشاهده ۱۷. $a\in aH$.

اثبات. واضح است که $a=ae$ و $e\in H$. پس $a\in aH$. □

مشاهده ۱۸. اگر $aH=bH$، واضح است که $a\in bH$ و $b\in aH$.
دقت کنید که وقتی می‌گوییم $aH=bH$، به هیچ عنوان منظورمان این نیست که برای هر $h\in H$ داریم $ah=bh$. بلکه منظور این است که مجموعهٔ ah ها با مجموعهٔ bh ها برابر شده است؛ یعنی هر ah با یک bh' برابر شده است.

مشاهده ۱۹. اگر $a\in bH$، در این صورت $aH\subseteq bH$.

اثبات. فرض کنید $a\in bH$. در این صورت، طبق تعریف bH برای یک عنصر $h_1\in H$، $a=bh_1$. فرض کنید $ah_2\in aH$، یک عنصر دلخواه باشد. در این صورت:

$$ah_2=b\underbrace{h_1h_2}_{\in H}\in bH$$

پس $aH\subseteq bH$. □

مشاهده ۲۰. اگر $a\in bH$، آنگاه $bH\subseteq aH$.

اثبات.

$$\begin{aligned} a\in bH &\implies \exists h_2\in H \quad a=bh_2\\ &\implies b=ah_2^{-1}\end{aligned}$$

بنابراین وقتی $a\in bH$ داریم $b\in aH$. بنا با مورد قبل از این نتیجه می‌شود که $bH\subseteq aH$. □

نتیجه ۲۱.

$$\begin{aligned} aH=bH &\iff a\in bH\\ &\iff b\in aH.\end{aligned}$$

مشاهده ۲۲. اگر $aH\cap bH\neq\varnothing$ در این صورت $aH=bH$.

اثبات. فرض کنید برای یک $h_1,h_2\in H$ داشته باشیم $ah_1=bh_2$. یعنی $aH\cap bH\neq\varnothing$. در این صورت $a=bh_2h_1^{-1}$ یعنی $a\in bH$ و از این رو $aH=bH$. □

نتیجه ۲۳. فرض کنید G یک گروه و H زیرگروهی از آن باشد و $a,b\in G$. در این صورت یا $aH\cap bH=\varnothing$ یا $aH=bH$.

مشاهده ۲۴. اگر $a\in H$ در این صورت $aH=H$.

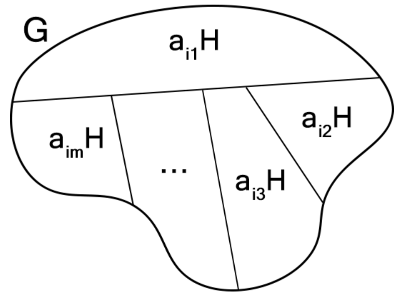
اثبات. $a\in H$ اگر در این صورت برای هر $h\in H$ داریم $ah\in H$. بنابراین $aH\subseteq H$. حال از آن‌جا که $|H|=|aH|$ پس $aH=H$.
اثبات راحت‌تر: اگر $a\in H$ در این صورت، از آن‌جا که H زیرگروه است، همچنین داریم $a^{-1}\in H$. پس $e=aa^{-1}h\in aH$ و از این رو $aH=eH=H$. □

قضیه ۲۵ (لاگرانژ). فرض کنید $G = \{a_1 a_2, \dots a_n\}$ و H یک زیرگروه از G باشد. در این صورت $|H| \mid |G|$ (یعنی تعداد اعضای H تعداد اعضای G را عاد می‌کند).

اثبات. دقت کنید که

$$a_1 H \subseteq G$$
$$a_2 H \subseteq G$$
$$\vdots$$
$$a_n H \subseteq G$$

توجه کنید که هر دو $a_i H$ و $a_j H$، یا با هم مساوی‌اند یا هیچ اشتراکی ندارند. فرض کنید $a_{i_1}H, a_{i_2}H, \dots, a_{i_m}H$ لیست کامل xHهایی باشد که باهم دوبه‌دو متفاوت‌اند. دقت کنید که $G = \bigcup a_i H$.



می‌دانیم اگر $x \in G$، آنگاه $x \in xH$. اما xH یکی از $a_i H$ های ماست؛ زیرا $a_i H$ را در نظر گرفته‌ایم که همهٔ xH های ممکن در میان آن‌ها باشند. بنابراین G توسط تعدادی مجموعه با اندازه‌ی برابر با $|H|$ پوشیده می‌شود که این مجموعه‌ها هیچ اشتراکی با هم ندارند. پس $|H| \mid |G|$. □

۳.۱ مرتبهٔ یک عنصر

توجه ۲۶. فرض کنید G یک گروه متناهی و $a \in G$ یک عضو دلخواه باشد. در این صورت، اعداد طبیعی m و n وجود دارند به طوری که $a^m = a^n$. زیرا اگر تک تک a^i هابه ازای هر $i \in \mathbb{N}$ متفاوت باشند، متناهی بودن G نقض می‌شود.

لم ۲۷. اگر G یک گروه متناهی و $a \in G$ یک عضو دلخواه باشد، در این صورت توانی از a برابر با e است.

اثبات. اگر توانِ یکِ a برابر با e باشد، کار تمام است. در غیر این صورت بنا به مشاهدهٔ قبل اعداد طبیعی m و n وجود دارند به طوری که $a^m = a^n$. فرض کنید مثلاً $m > n$. وارون a^n عنصر $(a^{-1})^n$ است، زیرا:

$$\underbrace{aa\cdots aaaaa}_{n}\underbrace{a^{-1}a^{-1}\cdots a^{-1}a^{-1}a^{-1}a^{-1}a^{-1}}_{n} = e.$$

دو طرف عبارت $a^m = a^n$ را در وارون a^n ضرب می‌کنیم:

$$a^{m-n} = e.$$

توجه داشته باشید که حاصل‌ضرب a^m در وارون a^n برابر با a^{m-n} می‌شود، و این خود نیاز به اثبات دارد! □

تعریف ۲۸. اگر G یک گروه متناهی باشد، منظور از مرتبه یک عنصر $a \in G$، که آن را با $o(a)$ نشان می‌دهیم، کوچکترین عدد طبیعیِ n است به طوری که $a^n = e$.

بنا به لم قبل، وقتی گروه G متناهی است، **هر عنصر دارای یک مرتبه است،** زیرا حداقل یک توان از آن برابر با e است و می‌توان کوچکترین توانِ دارای این ویژگی را در نظر گرفت. همچنین تنها عنصری که مرتبهٔ آن برابر با یک است، عنصر همانی است.

مشاهده ۲۹. فرض کنید G متناهی باشد و $a \in G$ و $o(a) = n$. قرار دهید:

$$\langle a \rangle_G = \{a^1, a^2, \dots, a^n = e\} \subseteq G.$$

$\langle a \rangle_G$ را دور عنصر a در G می‌نامیم. به راحتی می‌توان دید که $\langle a \rangle_G$ زیرگروهی از G است. به این زیرگروه، زیر گروه تولید شده توسط a در G گفته می‌شود. به $\langle a \rangle_G$ همچنین یک گروه دوری گفته می‌شود.

واضح است که $a^{o(a)} = e$ زیرا $o(a)$ کوچکترین عدد با این ویژگی است.

لم ۳۰. فرض کنید G یک گروه متناهی باشد و $a \in G$. اگر $a^n = e$ در این صورت، $o(a) \mid n$.

اثبات. اگر $o(a)$ عدد n را عاد نکند،

$$n = ko(a) + r$$

که در آن $r < o(a)$. پس

$$e = a^n = a^{ko(a)+r} = a^{ko(r)}a^r = a^{o(r)^k}a^r = e^k a^r = a^r$$

اما این که $a^r = e$ یک تناقض است، زیرا کوچکترین توان a که برابر با e است باید مرتبهٔ a باشد ولی $r < o(a)$. □

قضیه ۳۱. فرض کنید G یک گروه متناهی و $a \in G$ عنصری دلخواه باشد. در این صورت $o(a) \mid |G|$ (یعنی عدد مرتبهٔ هر عنصر، عدد تعداد اعضای گروه را عاد می‌کند).

اثبات. قرار دهید $H = \langle a \rangle$، یعنی H را زیرگروه دوری تولید شده توسط a در نظر بگیرید. واضح است که تعداد اعضای این زیرگروه برابر با $o(a)$ است. حال بنا به قضیهٔ لاگرانژ داریم $|H| = o(a) \mid |G|$. □

نتیجه ۳۲. اگر G یک گروه متناهی باشد، برای هر $a \in G$ داریم $a^{|G|} = e$.

اثبات. از آن جا که $|G| = ko(a)$ داریم $a^{|G|} = (a^{o(a)})^k = e^k = e$. □

قضیه ۳۳. فرض کنید G یک گروه با اندازه‌ی p باشد که p یک عدد اول است. در ابن صورت، G یک عدد دوری است؛ یعنی عنصر $a \in G$ موجود است، به طوری که $G = \{a^1, a^2, \dots, a^p = e\}$.

اثبات. فرض کنید $e \neq a \in G$. بنابر قضیه‌ی قبل، $o(a) \mid p$، پس $o(a) = 1$ یا $o(a) = p$. اگر $o(a) = 1$، آنگاه $a = e$ که یک تناقض است، پس نتیجه می‌گیریم $o(a) = p$. بنابراین $\langle a \rangle_G = G$. □

۴.۱ تبدیل مجموعهٔ هم‌مجموعه‌ها به یک گروه، و زیرگروه نرمال

تعریف ۳۴. اگر G یک گروه و H زیرگروهی از آن باشد، به هر مجموعه به صورت $aH = \{ah \mid h \in H\}$ یک **هم‌مجموعه‌ی** چپ از G نسبت به H گفته می‌شود. به طور مشابه، به هر مجموعه به صورت $Ha = \{ha \mid h \in H\}$، یک هم‌مجموعه‌ی راست گفته می‌شود.

فرض کنید G یک گروه و H یک زیرگروه از آن باشد. مجموعهٔ $\{aH : a \in G\}$، یعنی مجموعهٔ متشکل از همهٔ هم‌مجموعه‌های چپِ G در H را در نظر بگیرید. علاقه‌مندیم که با تعریف یک عمل، در صورت امکان این مجموعه را نیز به یک گروه تبدیل کنیم. طبیعی‌ترین عملی که به احتمالاً به ذهنمان می‌رسد، عمل زیر است:

$$aHbH = abH.$$

عمل بالا، یک مشکل جدی دارد، و آن **خوش‌تعریفی** است. در واقع عمل ضرب گروه، باید یک تابع باشد، یعنی وقتی $(aH, bH) = (a'H, b'H)$ آنگاه حاصلضرب aH در bH همان حاصل ضرب $a'H$ در $b'H$ شود.

فرض کنید $(aH, bH) = (a'H, b'H)$. در این صورت $a \in a'H$ و $b \in b'H$. حال، بنا به گونه‌ای که ضرب را تعریف کرده‌ایم، خواهیم داشت:

$$aHbH = abH, \quad a'Hb'H = a'b'H.$$

باید چک کنیم که آیا $abH = a'b'H$؟

می‌دانیم که $a \in a'H$ پس $a = a'h_1$. همچنین $b \in b'H$ پس $b = b'h_2$. برای تحقیق این که $abH = a'b'H$ یک عنصر abh را در نظر بگیرید. داریم:

$$abh = a'h_1b'h_2$$

اگر می‌شد به نحوی h_1b' را به صورت $b'h_3$ بنویسیم، مطمئن می‌شدیم که $abh \in a'b'H$. ایدهٔ تعریف **زیرگروه نرمال** همین است.

تعریف ۳۵. فرض کنید G یک گروه باشد و N یک زیرگروه از آن باشد. می‌گوییم N یک زیرگروه نرمال از G است، هرگاه برای هر $a \in G$ داشته باشیم:

$$aN = Na$$

به بیان دیگر:

$$\{an \mid n \in N\} = \{na \mid n \in N\}.$$

توجه ۳۶. توجه کنید که در تعریف ۳۵ فقط خواسته‌ایم که مجموعه‌ی $\{an \mid n \in N\}$ با مجموعه‌ی $\{na \mid n \in N\}$ برابر باشد.
یعنی فقط خواسته‌ایم که هر an با یک $n'a$ برابر شود، و **نخواسته‌ایم** که هر an با na برابر شود. پس N یک زیرگروه نرمال از G است، هرگاه *مقداری* جابه‌جایی به صورت زیر برقرار باشد:

$$\forall a \in G\ \forall n \in N\ \exists n' \in N \quad an = n'a.$$

لم ۳۷. فرض کنید G یک گروه و $a \in G$، یک عضو دلخواه و $N \subseteq G$ یک زیرگروه باشد. در این صورت، موارد زیر باهم معادل‌اند:

۱. $aN = Na$، یعنی هم‌مجموعه‌های چپی که با a ساخته می‌شود، با هم‌مجموعه‌ی راستی که با a ساخته می‌شود برابر است.

۲. برای یک $b \in G$، $aN = Nb$؛ یعنی هم‌مجموعه‌ی چپی که با a به دست می‌آید، با یک هم‌مجموعه‌ی راست دیگر مساوی باشد.

اثبات.

از ۱ به ۲: اگر $aN = Na$ و قرار دهیم $b = a$، در نتیجه $aN = Nb$.

از ۲ به ۱: فرض کنید $b \in G$ به گونه‌ای باشد که $aN = Nb$. در این صورت، ادعا می‌کنیم $aN = Na$.
از آن‌جا که $a \in aN$ و $aN = Nb$ داریم $a \in Nb$. اما می‌دانیم که a در Na هم هست؛ پس دو هممجموعهٔ راستِ Na و Nb با هم اشتراک دارند؛ پس با هم برابرند.

□

توجه ۳۸. ادعا نکردیم که اگر عنصر $b \in G$ وجود داشته باشد که $aN = Nb$، آنگاه $a = b$. فقط گفتیم که اگر عنصر $b \in G$ وجود داشته باشد که $aN = Nb$، آنگاه، به عنوان دو مجموعه: $Na = Nb$.

نتیجه ۳۹. فرض کنید G، یک گروه و N یک زیرگروه از آن باشد. آنگاه موارد زیر باهم معادل‌اند:

۱. N یک زیرگروه نرمال است.

۲. مجموعه‌ی $\{aN \mid a \in G\}$ با مجموعه‌ی $\{Nb \mid b \in G\}$ برابر است.

اثبات. فرض کنید N یک زیرگروه نرمال از G باشد. در این صورت $\{aN \mid a \in G\} = \{Na \mid a \in G\}$. یعنی مجموعه‌ی همه‌ی هم‌مجموعه‌های چپ برابر است با مجموعه‌ی همه‌ی هم‌مجموعه‌های راست؛ پس ۱ به ۲ واضح است.
حال فرض کنید ۲ برقرار باشد، یعنی مجموعه‌ی همه‌ی هم‌مجموعه‌های چپ با مجموعه‌ی همه‌ی هم‌مجموعه‌های راست یکی باشد. ادعا می‌کنیم N نرمال است. یعنی برای هر $a \in G$ داریم $aN = Na$. فرض کنید $a \in G$ دلخواه باشد. aN متعلق به مجموعه‌ی همهِ‌ی هم‌مجموعه‌های چپ است. پس aN با یک هم‌مجموعه‌ی راست مانند Nb برابر است. بنابر لم قبل $aN = Na$. □

حال فرض کنید G یک گروه و N یک زیرگروه نرمال از آن باشد. قرار دهید $A = \{aN \mid a \in G\}$. عمل ضرب برای A را به صورت زیر تعریف کنید:

$$aH \star_A bH = (a \star_G b)H$$

سوال ۲. آیا عملی که ما در نظر گرفته‌ایم، خوش تعریف است؟ یعنی اگر $a'N = aN$ و $b'N = bN$، آنگاه آیا چنین است که $aN\ \ bN =$ $a'N\ \ b'N$ ؟

اثبات. داریم:

$$\begin{aligned} aN = a'N &\implies a \in a'N \\ &\implies \exists n \in N \quad a = a'n \\ bN = b'N &\implies b \in b'N \\ &\implies \exists n' \in N \quad b = b'n' \end{aligned}$$

برای این که نشان دهیم $abN = a'b'N$ کافی است نشان دهیم هر عنصر به صورت abn'' در $a'b'N$ است و هر عنصر به صورت $a'b'n''$ در abN است. اولی را نشان می‌دهیم و دومی مشابه است.

عنصر دلخواه abN'' را در نظر بگیرید. داریم

$$abn'' = a'nb'n'n''$$

از آن جا که N یک زیرگروه نرمال است، nb' برابر با یک عنصر به صورت n_1b' است، پس داریم

$$abn'' = a'nb'n'n'' = a'b'n_1n'n'' \in a'b'N.$$

□

سوال ۳. آیا ضرب بالا A را تبدیل به یک گروه می‌کند؟

اثبات. **شرط شرکت‌پذیری:** باید نشان بدهیم$aN(bNcN) = (aNbN).cN$.

داریم:

$$aN(bNcN) = aN(bcN) = abcN$$

و

$$(aNbN)cN = (abN)cN = abcN$$

پس این ضرب شرکت‌پذیر است.

شرط وجود عضو خنثی: ادعا می‌کنیم eN عضو خنثی است. داریم:

$$eNaN = aNeN = aN$$

توجه کنید که $eN = N$ زیرا $eN = \{en \mid n \in N\}$.

شرط وجود عضو وارون: وارون aN برابر است با $a^{-1}N$ زیرا

$$aNa^{-1}N = aa^{-1}N = eN.$$

□

تعریف ۴۰. گروه A (با عمل جمع بالا را) با علامت $\frac{G}{N}$ نشان می‌دهیم و آن را **گروه خارج قسمتی** G نسبت به N می‌نامیم.

توجه ۴۱. وقتی گروه G متناهی است، تعداد اعضای گروه $\frac{G}{N}$ برابر است با $\frac{|G|}{|N|}$؛ زیرا تعداد اعضای گروه $\frac{G}{N}$ برابر است با تعداد همدسته‌های چپ N در G. این همدسته‌ها هر کدام هم‌اندازه با N هستند و با هم G را می‌پوشانند. پس

$$|G| = (|N| \times \text{تعداد همدسته‌ها})$$

یعنی

$$\text{تعداد همدسته‌ها} = \frac{|G|}{|N|}.$$

۵.۱ قضیهٔ کُشی

فرض کنید G یک گروه متناهی باشد. در این صورت، G حداقل دو زیرگروه به نام «زیرگروه‌های بدیهی» دارد که عبارت‌اند از G و $\{e\}$ که e عضو خنثی گروه G است.

لم ۴۲. فرض کنید G هیچ زیرگروهی به جز زیرگروه‌های بدیهی نداشته باشد. در این صورت، G یک گروه دوری است و اندازه‌ی G (یعنی تعداد اعضای G) یک عدد اول است.

اثبات. فرض کنید $|G| = n$. می‌دانیم که هر عنصر $a \in G$ دارای یک مرتبهٔ متناهی است. اگر عنصری مانند $a \in G$ داشته باشیم که مرتبه‌اش عددی غیر از n باشد، آنگاه G دارای زیرگروهی به اندازهٔ مرتبهٔ آن عنصر خواهد بود: یعنی زیرگروه دوری آن عنصر. پس هر عنصر غیر از e دارای مرتبه‌ای برابر با $|G|$ است؛ به طور خاص G دوری است.

اگر n، یعنی اندازهٔ G به یک عدد $m < n$ بخش‌پذیر باشد، مثلاً داشته باشیم: $n = mk$، آنگاه برای هر $a \in G$ داریم

$$(a^k)^m = a^{mk} = e.$$

یعنی G دارای عنصری با مرتبه‌ای کمتر از اندازهٔ G می‌شود؛ که این با گفتهٔ بند قبل تناقض دارد. □

قبلاً (در صفحهٔ ۹) گفته بودیم که مرتبهٔ هر عنصر باید $|G|$ را عاد کند. حال طبیعی از خود بپرسیم که اگر عددی اندازهٔ G را عاد کند، آیا لزوماً عنصری با مرتبهٔ آن عدد در G وجود دارد. قضیهٔ کُشی پاسخی نسبی به این سوال می‌دهد:

قضیه ۴۳ (کُشی). فرض کنید G یک گروه آبلی متناهی باشد (یعنی برای هر $a, b \in G$ داشته باشیم $ab = ba$). همچنین فرض کنید p یک عدد اول است به طوری که $p \mid |G|$. در این صورت، G دارای عنصری با مرتبه‌ی p است، یعنی

$$\exists a \in G \quad o(a) = p.$$

اثبات. اگر گروه G فقط یک عضو داشته باشد، حکم به انتفاء مقدم برقرار است: اگر عددی مانند p اندازهٔ گروه را عاد می‌کرد، عنصری با آن مرتبه پیدا می‌شد!

یک گروه G به طور دلخواه در نظر بگیرید. نشان می دهیم که اگر حکم، برای گروه‌های با اندازهٔ $|G| >$ برقرار باشد، برای G برقرار است. به این ترتیب، حکم برای گروه‌های دو عضوی برقرار است، چون برای یک عضوی‌ها برقرار بوده، برای گروه‌های سه عضوی برقرار است چون برای دو عضوی ها برقرار بوده و به همین ترتیب.

فرض کنید G هیچ زیرگروهی (غیر از زیرگروه‌های G و $\{e\}$) نداشته باشد. بنابر تمرین قبل، $|G| = p$ و G دوری است و چیزی برای اثبات باقی نمی‌ماند. در واقع همان عنصری که دورِ آن برابر با گروه G است دارای مرتبهٔ p است. دقت کنید که در این حالت، فقط یک عدد p هست که می‌تواند اندازهٔ گروه را عاد کند و حکم دربارهٔ همان عدد درست است.

حال فرض کنید گروه G دارای زیرگروهی مانند N باشد به طوری که $N \neq \{e\}$ و $N \neq G$. توجه کنید که N یک زیرگروه نرمال است چون G آبلی است:

$$\forall a \in G \, \forall n \in N \quad an = na.$$

فرض کنید p یک عدد اول باشد که اندازهٔ G را عاد می‌کند. از آن جا که N زیرگروه G است، تعداد اعضای آن کمتر از تعداد اعضای G است. اگر $p \mid |N|$ بنابه فرض استقرا، N دارای عنصری با مرتبه‌ی p است. همان عنصر در G است و دارای مرتبهٔ p است و اثبات حکم به پایان می‌رسد.

فرض کنید $p \nmid |N|$. گروه $\frac{G}{N}$ را در نظر بگیرید. می‌دانیم که

$$|\frac{G}{N}| = \frac{|G|}{|N|}.$$

چون $p \mid |G|$ و $p \nmid |N|$ پس $p \mid \frac{|G|}{|N|} = |\frac{G}{N}|$.

تعداد اعضای گروه $\frac{G}{N}$ کمتر از تعداد اعضای گروه G است و p این تعداد اعضا را عاد می‌کند. بنا به فرض استقراء، گروه $\frac{G}{N}$ دارای عنصری با مرتبه‌ی p است. فرض کنید این عنصر aN باشد. دقت کنید که $a \notin N$ زیرا در غیر این صورت مرتبهٔ aN یک می‌شد. پس

$$a^p N = N.$$

اما عبارت بالا به معنی عبارت زیر است:

$$a^p \in N.$$

بنا به قضیهٔ ۳۱ در صفحهٔ ۹ داریم

$$(a^p)^{|N|} = (a^{|N|})^p = e.$$

یعنی $a^{|N|}$ عنصری در G است که مرتبهٔ آن p را عاد می‌کند. یعنی ممکن است مرتبهٔ $a^{|N|}$ برابر با یک یا p باشد. نشان می‌دهیم که حالت اول رخ نمی‌دهد.

اگر $a^{|N|} = e$ خواهیم داشت:

$$(aN)^p = e \text{ و } (aN)^{|N|} = e.$$

پس $p \mid |N|$ که با فرض اول ما در تناقض است. □

قضیهٔ کُشی قضیهٔ بسیار مهمی در مورد گروه‌های «آبلی» است. همهٔ قضیه‌هایی که تا پیش از این گفته بودیم، تنها با در دست گرفتن یک خودکار و نوشتن فرضیات اثبات می‌شدند. اما تا این لحظه، قضیهٔ کُشی اولین قضیه در این درس با اثباتی غیر مستقیم بوده است. پس خوب است که خلاصهٔ اثبات آن را با هم مرور کنیم.

خلاصهٔ اثبات قضیهٔ کُشی. فرض کنید G یک گروه آبلی متناهی باشد و $p \mid |G|$. فرض کنید G یک زیرگروه نرمال به نام N داشته باشد. اگر $p \mid |N|$ بنا به فرض استقراء، N دارای عنصری با مرتبهٔ p است و همین عنصر در G نیز قرار دارد. اگر $p \nmid |N|$ آنگاه $p \mid |\frac{G}{N}|$ و دوباره بنا به فرض استقراء $\frac{G}{N}$ عنصری با مرتبهٔ p دارد؛ یعنی عنصری مانند $x \in G$ وجود دارد به طوری که $x^p \in N$. حال $(x^p)^{|N|} = e$ یعنی $(x^{|N|})^p = e$. پس $x^{|N|}$ عنصر مورد نظر ماست.

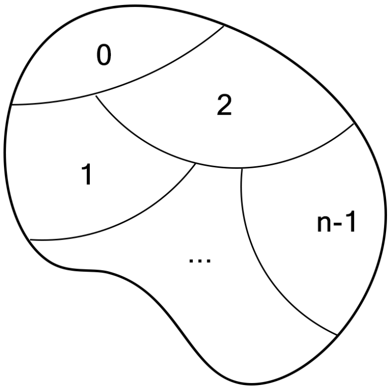
تمرین ۲. فهرستی از لم‌ها و قضایایی که در اثبات قضیهٔ کُشی مورد استفاده قرار گرفته‌اند، تهیه کنید.

۶.۱ گروه باقی‌مانده‌ها بر n

در این قسمت از درس قرار است با یک دستهٔ مهم از گروه‌ها آشنا شویم.

۱.۶.۱ روش اول

مجموعه‌ی اعداد صحیح را در نظر بگیرید که آن را با $\mathbb{Z}$ نشان می‌دهیم. $\mathbb{Z}$ را بر حسب باقی‌مانده اعداد بر n دسته‌بندی کنید.



دسته اعدادی که باقی‌مانده آن‌ها بر n برابر x است، را با $[x]$ نشان می‌دهیم. مثلا $[0]$ به معنای دسته اعدادی است که بر n بخش‌پذیر هستند.

قرار دهید $\mathbb{Z}_n = \{[x] \mid x \in \mathbb{Z}\}$. واضح است که مجموعهٔ $\mathbb{Z}_n$ دارای n عضو است (هر عضو آن یک دسته است). می‌خواهیم $\mathbb{Z}_n$ را به یک گروه تبدیل کنیم. برای این منظور، باید روی آن یک **عمل** تعریف کنیم. این عمل را می‌توانیم با هر علامت مورد علاقهٔ خود نشان دهیم. ما در این جا از علامت $+$ استفاده خواهیم کرد.

تعریف کنید

$$[x] + [y] = [x + y].$$

مثلاً برای $\mathbb{Z}_3$ داریم:

$$[2] + [1] = [0]$$

یا

$$[2] + [2] = [4] = [1].$$

سوال ۴. آیا عمل جمع فوق خوش تعریف است؟ یعنی اگر $[x'] = [x]$ و $[y'] = [y]$ ، در این صورت آیا می‌توان نتیجه گرفت که:

$$[x] + [y] = [x'] + [y']$$

دقت کنید که خوش‌تعریفی عمل جمع در بالا، بدین معنی است که حاصل جمع یک جفت به صورت $([x], [y])$ همیشه یکسان باشد. یعنی اگر جفت $([x'], [y'])$ با جفت $([x], [y])$ یکسان باشد، حاصل جمع جفت اول نیز با حاصل جمع جفت دوم یکسان شود.

اثبات خوش‌تعریفی جمع تعریف شده. فرض کنید $[x'] = [x]$ و $[y'] = [y]$. داریم:

$$[x] = [x'] \implies \exists k \in \mathbb{Z} \quad x - x' = nk$$
$$[y] = [y'] \implies \exists k' \in \mathbb{Z} \quad y - y' = nk$$

در نتیجه

$$\begin{aligned}(x + y) - (x' + y') &= x - x' + y - y' \\ &= nk + nk' \\ &= n(k + k')\end{aligned}$$

یعنی $[x + y] = [x' + y']$ و جمع تعریف شده خوش تعریف است. □

تا این جا، فقط یک عمل خوش‌تعریف داریم. اما:

سوال ۵. آیا $\mathbb{Z}_n$ با عمل فوق یک گروه است؟

<u>شرکت‌پذیری:</u>

باید بررسی کنیم که آیا چنین است که: $[x] + ([y] + [z]) = ([x] + [y]) + [z]$. اما داریم:

$$[x] + ([y] + [z]) = [x] + [y + z] = [x + y + z]$$
$$([x] + [y]) + [z] = [x + y] + [z] = [x + y + z]$$

وجود عضو خنثی:

$[0]$ عضو خنثی است چون $[x] + [0] = [x + 0] = [x]$

وارون پذیری:

وارون عنصر $[x]$ برابر است با $[n - x]$ چون $[x] + [n - x] = [0]$.

نتیجه ۴۴. برای هر عدد $n \in \mathbb{N}$ یک گروه $(\mathbb{Z}_n, +)$ وجود دارد که دوری است. همچنین می‌دانیم که $(\mathbb{Z}_n, +)$ یک گروه آبلی است.

تمرین ۳. در گروه $\mathbb{Z}_n$ کدام عناصر مولد هستند؟

۷.۱ روش دوم

در این زیربخش، یک طرز نگاه دیگر به $\mathbb{Z}_n$ را بررسی می‌کنیم که منطبق بر دانسته‌های قبلی‌مان دربارهٔ گروه‌های خارج قسمتی است.

فرض کنید که n یک عدد طبیعی باشد. مجموعه‌ی $n\mathbb{Z} = \{nx \mid x \in \mathbb{Z}\}$ را در نظر بگیرید. ادعا می‌کنیم که $n\mathbb{Z}$ (طبیعتاً با همان جمع معمولی اعداد صحیح) یک زیرگروه از $\mathbb{Z}$ است؛ در زیر بسته بودن این مجموعه، تحت عمل جمع و عمل وارون‌گیری را تحقیق کرده‌ایم:

$$nx + ny = n(x + y) \in n\mathbb{Z}$$
$$(nx)^{-1} = -nx = n(-x) \in n\mathbb{Z}$$

بنابراین $n\mathbb{Z}$ یک زیرگروه است.

حال ادعا می‌کنیم $n\mathbb{Z}$ یک زیرگروه نرمال است.

توجه ۴۵. اگر G یک گروه آبلی باشد، همه‌ی زیرگروه‌های آن نرمال هستند. گفتیم که زیرگروه N از G زمانی نرمال است که برای هر $g \in G$ و $n \in N$ عنصری مانند $n' \in N$ وجود داشته باشد که $gn = n'g$. وقتی G آبلی است، عنصر $n' = n$ برای این منظور کار می‌کند.

قرار دهید $G = \mathbb{Z}$ و $H = n\mathbb{Z}$ ، با توجه به ماهیت جمعی گروه، به جای aH ، بهتر است بنویسیم $a + H$.

توجه ۴۶. می‌دانیم که $aH = bH$ هرگاه $a \in bH$ و یا معادلاً هرگاه $ab^{-1} \in H$.

حالا اگر $G = \mathbb{Z}$ و $H = n\mathbb{Z}$ ، $a + H = b + H$ هرگاه $a - b \in H$. پس داریم:

$$a + H = b + H \iff a - b \in H$$
$$a + n\mathbb{Z} = b + n\mathbb{Z} \iff a - b \in n\mathbb{Z}$$
$$\iff n \mid a - b$$

پس $\{a + n\mathbb{Z} \mid a \in \mathbb{Z}\} = \{[x]_n \mid n \in \mathbb{Z}\} = \{\bar{n} \mid n \in \mathbb{Z}\}$ یعنی گروه $\mathbb{Z}_n$ که در بخشِ ۱.۶.۱ در صفحهٔ ۱۳ معرفی شد، همان گروه $\frac{\mathbb{Z}}{n\mathbb{Z}}$ است.

$$\mathbb{Z}_n = \frac{\mathbb{Z}}{n\mathbb{Z}}.$$

۸.۱ گروه باقی‌مانده‌ها با عمل ضرب و قضیهٔ اویلر

مجموعه‌ی $\mathbb{Z}_n = \{[0]_n, [1]_n, \ldots, [n-1]_n\}$ را همان طور که در بخش قبل معرفی کردیم در نظر بگیرید. تعریف کنید

$$[x] \cdot [y] = [xy]$$

آیا مجموعه‌ی $\mathbb{Z}_n$ با عمل ضرب فوق نیز یک گروه است؟

بررسی خوش تعریفی عمل. فرض کنید $[x] = [x']$ و $[y] = [y']$. آیا $[xy] = [x'y']$ ؟

$$[x] = [x'] \implies n \mid x - x'$$
$$[y] = [y'] \implies n \mid y - y'$$

داریم

$$\begin{aligned} xy - x'y' &= xy - xy' + xy' - x'y' \\ &= (x - x')y + x'(y - y') \end{aligned}$$

واضح است که $n \mid xy - x'y'$، یعنی $[xy] = [x'y']$؛ و از این رو، عملی که در نظر گرفته‌ایم از نظر خوش‌تعریفی ایرادی ندارد.

برقراری ویژگی شرکت پذیری بدیهی است.

توجه کنید که طبق تعریف ما $[0] = [x].[0]$. پس نمی‌توان انتظار داشت که صفر وارون داشته باشد. پس برای گروه بودن، بیایید صفر را کنار بگذاریم و مجموعه‌ی $\mathbb{Z}_n \backslash \{[0]\}$ را در نظر می‌گیریم.

توقع ما این است که $[1]$ عنصر خنثی باشد، زیرا واضح است که:

$$\forall x \in \mathbb{Z}_n \backslash \{[0]\} \quad [1].[x] = [x].[1] = [x]$$

در زیر بررسی می‌کنیم که کدام عناصر تحت این عمل، دارای وارون هستند. برای این منظور، نیازمند یادآوری نظریهٔ اعداد دبیرستانی هستیم:

توجه ۴۷. اگر $d = \gcd(m, n)$، آنگاه اعداد صحیح x و y وجود دارند به طوری که $mx + ny = d$.

اثبات. فرض کنیم $n > m$. بنا به الگوریتم تقسیم، قرار می‌دهیم $n = mk_1 + r_1$.

توجه کنید که $\gcd(n, m) = \gcd(m, r_1)$، چون هر عددی که m و r_1 را عاد کند، m و n را عاد می‌کند. حالا باقی‌مانده تقسیم m بر r_1 را حساب می‌کنیم

$$m = r_1k_2 + r_2$$

پس $\gcd(m, n) = \gcd(m, r_1) = \gcd(r_1, r_2)$ و این کار را آنقدر تکرار می‌کنیم تا به باقی‌مانده صفر برسیم. وقتی به باقی‌مانده صفر رسیدیم، باقی‌مانده تقسیم مرحله‌ی قبل، ب.م.م مورد نظر ما است. مثلاً اگر $r_{s+1} = 0$ داریم:

$$\gcd(m, n) = \gcd(m, r_1) = \gcd(r_1, r_2) = \ldots = \gcd(r_{s-1}, r_s) = r_s$$

ادعا می‌کنیم که r_s یک ترکیب خطی از m, n است. تحقیق این امر ساده است. برای ساده شدن استدلال بیاید فرض کنید که این کار در همان مرحلهٔ دوم به پایان می‌رسد:

$$r_1 = r_2k_3$$

آنگاه داریم

$$\begin{aligned} r_1 = r_2k_3 \implies r_2 &= m - r_1k_2 \\ &= m - (n - mk_1)k_2 \end{aligned}$$

که یک ترکیب از m و n است. □

نتیجه ۴۸. $\gcd(m,n)=1$ اگر و تنها اگر اعداد صحیح x و y وجود داشته باشند به طوری که $mx+ny=1$.

اثبات. اگر $\gcd(m,n)=1$ اعداد x,y با ویژگی مورد نظر، بنا به توجه قبل وجود دارند. حال فرض کنید اعداد x,y به گونه‌ای باشند که $mx+ny=1$. هر عددی که m,n را عاد کند باید ۱ را عاد کند. پس هیچ عددی غیر از ۱ نمی‌تواند m,n را عاد کند. □

فرض کنید $\gcd(x,n)=1$. یعنی

$$\exists y\,\exists k\quad xy+nk=1$$

بنابراین

$$xy\equiv^n 1$$

. پس اگر $\gcd(x,n)=1$ آنگاه $[x]$ دارای وارون است.

حالا فرض می‌کنیم $[x]\in\mathbb{Z}_n$ وارون داشته باشد. در این صورت y وجود دارد به طوری که $[x].[y]=[xy]=[1]$ به بیان دیگر عنصر y وجود دارد به طوری که

$$xy\equiv^n 1.$$

یعنی k وجود دارد به طوری که $xy-1=nk$ بنابراین $xy-nk=1$.
پس عنصر x زمانی وارون پذیر است که نسبت به n اول باشد.

نتیجه ۴۹. در $\mathbb{Z}_n-\{[0]\}$ با ضرب تعریف شده، $[x]$ وارون دارد اگر و تنها اگر $\gcd(x,n)=1$.

تعریف ۵۰. قرار دهید

$$U_n=\{[x]\mid x\in\mathbb{Z}_n\backslash\{[0]\},\ (x,n)=1\}$$

آنگاه $(U_n,.)$ یک گروه تشکیل می‌دهد.

توجه ۵۱. اگر p یک عدد اول باشد، $(\mathbb{Z}_p,.)$ یک گروه است که $p-1$ عضو دارد. در واقع هر عدد مخالفِ صفرِ کمتر از p نسبت به آن اول است.

در نظریهٔ اعداد، تعداد اعداد طبیعی کمتر از n است که نسبت به n اول هستند را با $\varphi(n)$ نشان می‌دهند. بنا بر آن چه گفته شد:

$$|U_n|=\varphi(n)\qquad|\mathbb{Z}_p|=p-1$$

با استفاده از روش بالا، می‌توان دو قضیه در نظریهٔ اعداد را اثبات کرد:

نتیجه ۵۲ (اویلر)**.** برای هر عدد طبیعی n،

$$a^{\varphi(n)}\overset{n}{\equiv}1$$

اثبات. قبلاً در نتیجه ۳۲ در صفحهٔ ۹ دیدیم که اگر G یک گروه باشد و $a\in G$ آنگاه $a^{|G|}=e$. گروه U_n را در نظر بگیرید. داریم $[a]^{\varphi(n)}=e$ که دقیقاً یعنی $a^{\varphi(n)}\equiv^n 1$. □

نتیجه ۵۳ (لاگرانژ)**.** برای هر عدد اول p داریم:

$$a^{p-1}\equiv^p 1.$$

اثبات. همان اثبات قبلی را برای $n=p$ به کار ببرید. □

۹.۱ قضیهٔ سیلو برای گروه‌های آبلی

آنچه در این بخش مورد بررسی قرار گرفته است، قضیهٔ سیلو (تلفظ درست‌ترِ نروژی: سولُف) برای گروه‌های آبلی است. توجه کنید که این قضیه برای گروه‌های غیر آبلی هم برقرار است و بعداً اثبات این را هم خواهیم دید. همچنین توجه کنید که از این قضیه برای «شناسایی کامل» گروه‌های آبلی متناهی استفاده می‌شود. به این کار هم در درسهای بعدی خواهیم پرداخت.

فرض کنید G یک گروه آبلی متناهی و p یک عدد اول باشد به طوری که $p^\alpha \mid |G|$ و $p^{\alpha+1} \nmid |G|$. در واقع p یک عامل از $|G|$ است و داریم: $|G| = p^\alpha m$ که در آن $p \nmid m$. تعریف کنید:

$$
\begin{aligned}
S &= \{x \in G \mid \exists n \in \mathbb{N} \quad x^{p^n} = e\} \\
&= \{x \in G \mid x^p = e\} \cup \{x \in G \mid x^{p^2} = e\} \cup \{x \in G \mid x^{p^3} = e\} \cup \dots
\end{aligned}
$$

به راحتی می‌توان دید که

$$S = \{x \in G : x^{p^\alpha} = e\}.$$

توجه ۵۴. $S \subseteq G$ یک زیرگروه است.

اثبات. ابتدا نشان می‌دهیم S تحت عمل گروه بسته است.
فرض کنید $x, y \in S$. باید نشان دهیم $xy \in S$.

$$
\begin{aligned}
x \in S &\implies \exists n_1 \in \mathbb{N}, \quad x^{p^{n_1}} = e \\
y \in S &\implies \exists n_2 \in \mathbb{N}, \quad x^{p^{n_2}} = e
\end{aligned}
$$

دقت کنید که

$$
\begin{aligned}
(xy)^{p^{n_1+n_2}} &= x^{p^{n_1+n_2}} + y^{p^{n_1+n_2}} \\
&= (x^{p^{n_1}})^{p^{n_2}}.(y^{p^{n_1}})^{p^{n_2}} = e
\end{aligned}
$$

پس $xy \in S$. توجه کنید که G یک گروه متناهی است. بنابراین وارون هر $x \in G$ ، توانی از آن در است و در نتیجه S نسبت به وارون‌گیری بسته است. □

توجه ۵۵. اگر G یک گروه متناهی باشد و $S \subseteq G$ همینکه S تحت عمل ضرب بسته باشد، برای زیرگروه بودن آن کافی است. علت این است که در گروه‌های متناهی، همواره توانی از a برابر با e است، یعنی وارون هر عنصر، توانی از آن است.

سوال ۶. آیا در S عنصری نابدیهی وجود دارد؟

پاسخ. بنابر قضیه‌ی کشی، عنصری در G با مرتبه‌ی p وجود دارد. یعنی

$$\exists x \in G \quad (x \neq e \wedge x^p = e)$$

□

سوال ۷. S چند عضو دارد؟

ادعا می‌کنیم $|S|$ توانی از p است.

اثبات. فرض کنید یک عدد اول $q \neq p$ اندازه‌ی S را عاد کند. در این صورت بنابر قضیه‌ی کشی، S یک عنصر نابدیهی مانند a دارد به طوری که $a^q = e$. از آنجا که $a \in S$ می‌دانیم $\exists n \in \mathbb{N}\ a^{p^n} = e$. پس باید داشته باشیم $q \mid p^n$ و این امر امکان‌پذیر نیست. □

بنابراین از آنجا که S یک زیرگروه G است، $|S| \mid |G|$ پس $|S| \in \{p, p^2, p^3, \dots, p^\alpha\}$.

ادعا ۵۶. $|S| = p^\alpha$.

اثبات. فرض کنید $(i < \alpha) \quad |S| = p^i$. گروه $\frac{G}{S}$ را در نظر بگیرید. واضح است که $p \mid |\frac{G}{S}|$. بنابر قضیه‌ی کشی، یک عنصر نابدیهی در $\frac{G}{S}$ مانند bS وجود دارد که $(bS)^p = e$. پس $b^pS = e$ و $b^p \in S$. بنابراین عدد n وجود دارد که $(b^p)^{p^n} = e$. یعنی $b^{p^{n+1}} = e$. در نتیجه $b \in S$؛ و این تناقض با غیر بدیهی بودن bS دارد. □

قضیه ۵۷ (سیلو). فرض کنید G یک گروه متناهی آبلی باشد و $p^\alpha \mid |G|$ در حالی که $p^{\alpha+1} \nmid |G|$. در این صورت G دارای یک زیرگروه با اندازه‌ی p^α است.

توجه ۵۸.

۱. در اثبات قضیهٔ بالا، می‌شد به راحتی بنویسیم:

$$S = \{x \in G : x^{p^\alpha} = e\}$$

در واقع مجموعهٔ فوق، برابر با مجموعهٔ S است که در اثبات به کار رفته است.

۲. قضیهٔ سیلو همان طور که قبلاً هم گفتیم برای گروه‌های غیر آبلی هم درست است (بعداً اثبات خواهیم کرد).

۳. قضیهٔ سیلو به صورت زیر هم درست است: فرض کنید G یک گروه آبلی (یا غیر آبلی)باشد و $p^\alpha \mid |G|$. در این صورت G دارای زیر گروهی با اندازهٔ p^α است (بعداً ثابت خواهیم کرد).

> خلاصهٔ اثبات قضیهٔ سیلو. فرض کنید G یک گروه آبلی متناهی باشد و $p^\alpha \mid |G|$ و $p^{\alpha+1} \nmid |G|$. در این صورت مجموعهٔ $S = \{x \in G : x^{p^\alpha} = e\}$ یک زیرگروه از G با اندازهٔ p^α است.

۱۰.۱ همومرفیسم

فرض کنید $(G_1, \star_{G_1})$ و $(G_2, \star_{G_2})$ گروه باشند. فرض کنید $\varphi: G_1 \longrightarrow G_2$ یک تابع باشد. این تابع در چه صورت می‌تواند «شباهت» یا «یکسان» بودن این دو گروه را بیان کند.

فرض کنید تابع φ عنصر a_1 در G_1 را به a_2 در G_2 و عنصر b_1 در G_1 را به b_2 در G_2 ببرد. برای این که φ «حافظ اطلاعات» باشد،لازم است که حاصل جمع a_1 و b_1 در G_1 را به حاصل جمع a_2 و b_2 در G_2 ببرد. یعنی

$$a_1 \mapsto a_2 \quad b_1 \mapsto b_2 \quad a_1 *_{G_1} b_1 \mapsto a_2 *_{G_2} b_2$$

چنین نگاشتی را یک «همومرفیسم» می‌نامیم.

تعریف ۵۹. می‌گوییم $\varphi : G_1 \to G_2$ یک همومورفیسم است هرگاه

$$\forall a, b \in G_1 \quad \varphi(a \star_{G_1} b) = \varphi(a) \star_{G_2} \varphi(b).$$

تعریف ۶۰. در صورتی که φ یک همومورفیسم یک به یک و پوشا باشد، آن را یک ایزومورفیسم می‌نامیم.

مثال ۶۱. تابع نمایی، یعنی تابعِ $e^x : \mathbb{R} \longrightarrow \mathbb{R}^{>0}$ یک ایزمرفیسم بین $(\mathbb{R}, +)$ و $(\mathbb{R}^{>0}, \times)$ است. زیرا به طوری که $e^{x+y} = e^x.e^y$. همچنین e^x هم یک به یک و هم پوشاست.

مثال ۶۲. تابعِ $\varphi: \mathbb{Z} \longrightarrow \mathbb{Z}_3$ با ضابطهٔ $x \longmapsto [x]_3$ یک همومورفیسم است چون $[x+y] = [x] + [y]$.

تمرین ۴. گروه‌های $G_1 = (\mathbb{R}\backslash\{0\}, \times)$ و $G_2 = (\{+,-\}, \star)$ با عمل مثبت در مثبت برابر با مثبت و منفی در مثبت برابر با منفی و منفی در منفی برابر با مثبت را در نظر بگیرید. تعریف کنید

$$\varphi\colon G_1 \longrightarrow G_2, \quad \varphi(x) = \begin{cases} + & x \geqslant 0 \\ - & x < 0 \end{cases}$$

بررسی کنید چرا این تابع یک هومومورفیسم است.

مثال ۶۳. تابع $\varphi\colon \mathbb{Z} \longrightarrow \mathbb{Z}_3$ با ضابطهٔ $x \longmapsto [x]_3$ یک هومومورفیسم است چون

$$[x+y]_3 = [x]_3 + [y]_3.$$

در واقع، تعریف عمل جمع در گروه $\mathbb{Z}_3$ به گونه‌ای است که نگاشت فوق، خود به خود یک هومومرفیسم می‌شود.

۱۱.۱ تبدیل یک هومومرفیسم پوشا به یک ایزمرفیسم

گفتیم که یک هومومرفیسمِ یک‌به‌یک و پوشا را ایزومرفیسم می‌نامیم. اکنون می‌پرسیم که چگونه می‌شود یک هومومورفیسم را به یک ایزومورفیسم تبدیل کرد؟ در ادامه خواهیم دید که چگونه (با دسته‌بندی دامنه) کاری خواهیم کرد یک هومومرفیسم پوشای $\varphi\colon G_1 \longrightarrow G_2$ یک‌به‌یک شود. پیش از آن لازم است کمی اطلاعات در مورد هومومرفیسم‌ها جمع‌آوری کنیم. نخستین لم ما در پایین، بیان می‌کند که هر هومومرفیسم، عنصر خنثای گروه مبدأ را به عنصر خنثای گروه مقصد می‌برد.

لم ۶۴. فرض کنید $\varphi : G_1 \to G_2$ یک هومومرفیسم باشد. در این صورت:

$$\varphi(e_{G_1}) = e_{G_2}.$$

اثبات. نخست دقت کنید که

$$e_{G_1}e_{G_1} = e_{G_1} \implies \varphi(e_{G_1})\varphi(e_{G_1}) = \varphi(e_{G_1})$$

بنابراین اگر قرار دهیم $a = \varphi(e_{G_1})$، مشاهده می‌کنیم که a عنصری در G_2 است که $aa = a$. تنها عنصر در G_2 که این ویژگی را دارد، e_{G_2} است. □

لم پایین بیان می‌کند که اگر b وارون a در گروه G_1 باشد، آنگاه $\varphi(b)$ وارون $\varphi(a)$ در گروه G_2 است.

لم ۶۵. فرض کنید $\varphi : G_1 \to G_2$ یک هومومرفیسم باشد. در این صورت: $\varphi(a^{-1}) = (\varphi(a))^{-1}$

اثبات. نخست دقت کنید که

$$\begin{aligned} & a \star_{G_1} a^{-1} = e_{G_1} \\ & \implies \varphi(a) \star_{G_2} \varphi(a^{-1}) = \varphi(e_{G_1}) \\ & = e_{G_2} \quad \text{بنا به لم قبل} \end{aligned}$$

یعنی $\varphi(a^{-1})$ وارون $\varphi(a)$ در گروه G_2 است؛ یعنی در گروه G_2 داریم

$$\overbrace{(\varphi(a))^{-1}}^{G_2\text{وارون‌گیری در}} = \varphi(\overbrace{a^{-1}}^{G_1\text{وارون‌گیری در }}).$$

□

گفتیم که اگر φ یک هومورفیسم باشد، $\varphi(e) = e$. اما فقط $\varphi(e)$ نیست که با e برابر است. اعضای دیگری مانند x ممکن است وجود داشته باشند به طوری که $\varphi(x) = e$. این اعضا، یک زیرگروه مهم از گروه G_1 را تشکیل می‌دهند. در ادامه این گفته را اثبات خواهیم کرد.

قضیه ۶۶. $\{x \in G_1 \mid \varphi(x) = e_{G_2}\}$ یک زیرگروه از G_1 است.

اثبات. قرار دهید $H = \{x \in G_1 \mid \varphi(x) = e_{G_2}\}$. فرض کنید $x, y \in H$، در این صورت $\varphi(x) = e$ و $\varphi(y) = e$. از این رو $xy \in H$ چون $\varphi(xy) = \varphi(x)\varphi(y) = e$.

همچنین اگر $x \in H$ عنصر دلخواهی باشد، داریم $\varphi(x) = e$. پس $\varphi(x^{-1}) = (\varphi(x))^{-1} = e$ یعنی: $x^{-1} \in H$. □

تعریف ۶۷. فرض کنید $\varphi: G_1 \longrightarrow G_2$ یک هومورفیسم باشد. تعریف می‌کنیم

$$\mathrm{Ker}(\varphi) = \{x \in G_1 \mid \varphi(x) = e\}$$

$\mathrm{Ker}(\varphi)$ را هستهٔ هومرفیسمِ φ می‌نامیم.

در قضیهٔ ۶۶ گفتیم که هسته‌ی φ یک زیرگروه از G_1 است. در لم بعدی نشان می‌دهیم که این زیرگروه، نرمال است.

لم ۶۸. هسته‌ی φ یک زیرگروه نرمال از گروه G_1 است.

اثبات. فرض کنید $x \in G$ و $n \in \mathrm{Ker}(\varphi)$. باید نشان دهیم که عنصری مانند $n' \in \mathrm{Ker}(\varphi)$ وجود دارد به طوری که $xn = n'x$. برای این منظور کافی است نشان دهیم که $xnx^{-1} \in \mathrm{Ker}(\varphi)$. داریم:

$$\begin{aligned}\varphi(xnx^{-1}) &= \varphi(x)\varphi(n)\varphi(x^{-1})\\ &= \varphi(x)\varphi(x^{-1}) \qquad (\varphi(n) = e)\\ &= \varphi(x)(\varphi(x))^{-1}\\ &= e.\end{aligned}$$

□

مثال ۶۹. فرض کنید N یک زیرگروه نرمال از گروه G باشد. گروه $\frac{G}{N}$ را قبلا تعریف کرده بودیم که هر عضو آن یک هم‌مجموعهٔ چپ (معادلاً راست) از N در G است:

$$\frac{G}{N} = \{xN \mid x \in G\}$$

نگاشت φ را به صورت زیر در نظر بگیرید:

$$\varphi: G \longrightarrow \frac{G}{N} \quad x \longmapsto xN$$

نگاشت φ یک هومورفیسم است. برای اثبات این گفته باید نشان دهیم برای هر $x, y \in G$ داریم $\varphi(xy) = \varphi(x)\varphi(y)$. دقت کنید که

$$\begin{aligned}\varphi(xy) &= xyN\\ &= xNyN\\ &= \varphi(x)\varphi(y)\end{aligned}$$

به این هومورفیسم، **هومورفیسم کانونی** می‌گوییم. هستهٔ این هومرفیسم، همان طور که در زیر ثابت کرده‌ایم، همان گروه N است:

$$\begin{aligned}\mathrm{Ker}(\varphi) &= \{x \in G \mid \varphi(x) = n\}\\ &= \{x \in G \mid xN = N\}\\ &= \{x \in G \mid x \in N\}\\ &= N.\end{aligned}$$

قبلاً نشان دادیم که اگر $\varphi: G_1 \to G_2$ یک هومرفیسم باشد، آنگاه $\mathrm{Ker}(\varphi)$ یک زیرگروه نرمال از G_1 است. همچنین در بالا دیدیم که اگر N یک زیرگروه نرمال از گروه G_1 باشد، آنگاه N هستهٔ یک هومرفیسم از G_1 به یک گروه دیگر است. بنابراین:

نتیجه ۷۰. به طور کلی، N یک زیرگروه نرمال از گروه G است اگر و تنها اگر یک گروه G' و یک هومومورفیسم $\varphi: G \longrightarrow G'$ موجود باشد به طوری که $N = \mathrm{Ker}(\varphi)$.

توجه ۷۱ (شرط یک به یک بودن همومرفیسم‌ها)**.** فرض کنید $\varphi: G_1 \longrightarrow G_2$ یک هومومورفیسم باشد. فرض کنید $\varphi(x) = \varphi(y)$ در این صورت خواهیم داشت:

$$\begin{aligned}\varphi(x)(\varphi(y))^{-1} = e_{G_2} &\implies \varphi(x)\varphi(y^{-1}) = e_{G_2}\\ &\implies \varphi(xy^{-1}) = e_{G_2}\\ &\implies xy^{-1} \in \mathrm{Ker}(\varphi)\\ &\implies x\mathrm{Ker}(\varphi) = y\mathrm{Ker}(\varphi).\end{aligned}$$

یعنی: اگر $\varphi(x) = \varphi(y)$ آنگاه x و y نسبت به $\mathrm{Ker}(\varphi)$ یک همدسته یکسان می‌سازند. به بیان دیگر، اگر $\varphi(x) = \varphi(y)$ آنگاه در گروه $\frac{G_1}{\mathrm{Ker}(\varphi)}$ دو عنصر $x\mathrm{Ker}(\varphi)$ و $y\mathrm{Ker}(\varphi)$ با هم برابر هستند. عکس این گفته هم درست است: فرض کنید $xy^{-1} \in \mathrm{Ker}(\varphi)$. در این صورت

$$\begin{aligned}&\varphi(xy^{-1}) = e\\ &\Rightarrow \varphi(x)\varphi(y^{-1}) = e\\ &\Rightarrow \varphi(x)(\varphi(y))^{-1} = e\\ &\Rightarrow \varphi(x) = \varphi(y)\end{aligned}$$

به طور خلاصه، اگر $\varphi : G_1 \to G_2$ یک همومرفیسم باشد، آنگاه

$$\varphi(x) = \varphi(y) \iff xy^{-1} \in \mathrm{Ker}(\varphi) \iff x\mathrm{Ker}(\varphi) = y\mathrm{Ker}(\varphi).$$

یک اهمیت هستهٔ همومرفیسم، کمک آن به تشخیص یک‌به‌یک بودن است: همومرفیسمی یک به یک است که هستهٔ آن یک زیرگروه بدیهی از گروه مبدأ باشد. لم زیر را مشاهده کنید:

لم ۷۲. فرض کنید $\varphi : G_1 \longrightarrow G_2$ ، یک هومومورفیسم باشد. در این صورت φ یک به یک است، اگر و تنها اگر $\mathrm{Ker}(\varphi) = \{e\}$.

اثبات. فرض کنید φ یک به یک باشد، می‌دانیم که $\varphi(e) = e$. چون φ یک به یک است، فقط e تنها عنصری است که $\varphi(e) = e$. پس $\mathrm{Ker}(\varphi) = \{e\}$.

حال فرض کنید $\mathrm{Ker}(\varphi) = \{e\}$. در این صورت اگر $\varphi(x) = \varphi(y)$ آنگاه $xy^{-1} \in \mathrm{Ker}(\varphi)$ یعنی $xy^{-1} = e$. پس $x = y$. □

۱۲.۱ قضیهٔ اول همومرفیسم گروه‌ها

فصل ۲

تمرین‌های بخش گروه‌ها

۱.۲ نوبت اول

تمرین ۵. فرض کنید G یک گروه متناهی باشد. نشان دهید وارون هر عنصر توانی از خودش است.

راهنمایی. فرض کنید $a \in G$ عنصر دلخواهی باشد. اگر داشته باشیم $a^1 \neq a^2 \neq a^3 \neq \ldots \neq a^n \neq$ آنگاه G نمی‌تواند یک گروه متناهی باشد. پس حداقل دو توانِ m, n از a با هم برابر هستند. □

تمرین ۶. اگر G یک گروه باشد و $a, b \in G$، معکوس عنصر ab را پیدا کنید.

راهنمایی. نشان دهید که $b^{-1}a^{-1}$ وارون عنصر ab است. □

تمرین ۷. فرض کنید G یک گروه دلخواه باشد و $x \in G$ عنصری با مرتبهٔ متناهی باشد. نشان دهید که

$$o(x) = o(x^{-1}).$$

راهنمایی. کافی است نشان دهید که $x^n = e$ معادل است با $(x^{-1})^n = e$. برای این منظور نیز کافی است نشان دهید که $(x^{-1})^n = e$ وارون x^n است. □

تمرین ۸. فرض کنید G یک گروه است که در آن مرتبه همه عناصر ۲ است. نشان دهید G آبلی است.

راهنمایی.

$$\begin{aligned}
a^2 = e &\implies a = a^{-1} \\
\forall a, b \in G \quad abab = e &\implies (ab)^{-1} = ab \\
&\implies b^{-1}a^{-1} = ab \\
&\implies ba = ab \quad (b = b^{-1},\ a = a^{-1})
\end{aligned}$$

□

تمرین ۹. اگر G یک گروه باشد و $a^2 = b^2$ آنگاه آیا $a = b$ ؟

راهنمایی.

- در گروه S_3 داریم: $r_1^2 = e, r_2^2 = e$ ولی $r_1 \neq r_2$.
- در گروه $(\mathbb{R}, .)$ یعنی مجموعه اعداد حقیقی همراه با ضرب متعارف اعداد حقیقی داریم: $(-2)^2 = 4,\ 2^2 = 4$ ولی $2 \neq -2$

– به طور کلی در هر گروه مانند G که مرتبه همه عناصر آن ۲ باشد داریم $\forall a, b \in G, \quad a^2 = b^2 = e$
ولی لزوما $a = b$ برقرار نیست. □

تمرین ۱۰. اگر G یک گروه با تعداد عناصر زوج باشد، نشان دهید G عنصری با مرتبه ۲ دارد.

راهنمایی. قصد نداریم از قضیهٔ کشی استفاده کنیم. فرض کنید G دارای $2n$ عضو باشد. می‌دانیم در هر گروه مانند G یک عضو خنثی e وجود دارد و $e = e^{-1}$.
پس حداقل یک عضو داریم که وارون آن خودش است. حال تمام زوج‌های (x, x^{-1}) را در نظر بگیرید. اگر برای هر $x \neq e$ داشته باشیم $x \neq x^{-1}$
در این صورت تعداد اعضای گروه $2k + 1$ می‌شود. □

تمرین ۱۱. اگر G یک گروه غیر آبلی با اندازه ۶ باشد، آنگاه نشان دهید G دارای حداقل یک عنصر با مرتبه‌ی ۲ و حداقل یک عنصر با مرتبه‌ی ۳ است.

راهنمایی. می‌دانیم که مرتبهٔ هر عنصر گروه باید عدد 6 را عاد کند؛ پس مرتبهٔ هر عنصر یا۱ یا ۲ یا ۳ یا ۶ است. اگر مرتبه‌ی همه عناصر G عدد ۶ باشد، آنگاه G یک گروه دوری و آبلی است، پس به این حالت کاری نداریم.
طبق تمرین ۱۰ چون مرتبه‌ی G زوج است، پس حداقل یک عضو از مرتبه‌ی ۲ دارد. اما اگر همه مرتبه عناصر G ۲ باشند، آنگاه بنا به تمرین ۸ G یک گروه آبلی است. پس حداقل یک عضو با مرتبه ۳ در G وجود دارد. □

تمرین ۱۲. نشان دهید تمرین قبل برای گروه‌های دوری مرتبه ۶ هم برقرار است.

راهنمایی. دقت کنید که اگر مرتبه‌ی همه عناصر گروه G ۶ باشد، آنگاه داریم:

$$\forall a \in G \quad O(a) = 6 \implies a^6 = e$$
$$\implies (a^2)^3 = (a^3)^2 = 3$$

پس G عنصر مرتبه ۳ و ۲ دارد. □

تمرین ۱۳. فرض کنید G یک گروه با اندازه ۶ باشد و اعضای $a, b \in G$ به گونه‌ای باشند که $O(a) = 2$ و $O(b) = 3$.
واضح است که $H = \{b, b^2, e\}$ و $\{a, e\}$ زیر گروه‌های G هستند.
اگر قرار دهیم $aH = \{ab, ab^2, a\}$ و $eH = \{b, b^2, e\}$ نشان دهید $eH \neq aH$. سپس اعضای G را بنویسید.

راهنمایی. $eH = aH$ زمانی رخ می‌دهد که $a \in eH$؛ یعنی $a = e$ یا $a = b$ یا $a = b^2$.
می‌دانیم $a \neq e$ پس $a = b$ یا $a = b^2$.
$a \neq b$ چون $O(a) = 2$ و $O(b) = 3$.
$a \neq b^2$ چون اگر $a = b^2$ آنگاه $a^2 = b^4$ و در نتیجه $b^4 = e$.
بنابراین $a \notin eH$ و $aH \neq eH$.
پس G برابر است با $G = \{a, b, b^2, ab, ab, ab^2, a\}$ که در آن $O(a) = 2$ و $O(b) = 3$. □

تمرین ۱۴. می‌خواهیم جدول ضرب گروه ۶تایی $G = \{e, a, ab, ab^2, b, b2\}$ را رسم کنیم. نخست حاصل ضربهای مشخص را به صورت زیر می‌نویسیم:

$\star$	e	a	ab	ab^2	b	b^2
e	a	ab	ab^2	b	b	b^2
a	a	?	?	?	ab	ab^2
ab	ab	?	?	?	ab^2	a
ab^2	ab^2	?	?	?	a	ab
b	b	?	?	?	b^2	a
b^2	b^2	?	?	?	e	b

در جدول فوق، در مورد عناصر زیر اطلاعی نداریم:

$$\begin{matrix} aba & abab & abab^2 \\ abba & abbab & abbabb \\ ba & bab & bba \\ b^2ab \end{matrix}$$

عنصر ba در همه عناصر بالا حضور دارد. پس ابتدا مشخص می‌کنیم ba چه می‌تواند باشد.
عنصر ba باید متعلق به گروه $G = \{e, a, ab, ab^2, b, b^2\}$ باشد. طبق تمرین قبل، $ba \in \{ab, ab^2, a\}$ یا $ba \in \{b, b^2, e\}$.

- فرض کنیم $ba \in \{b, b^2, e\}$:
اگر $ba = b$ ، آنگاه $a = e$.
اگر $b^2 = b$ ، آنگاه $a = b$.
اگر $ba = e$ ، آنگاه $a = b^2$.

- فرض می‌کنیم $ba \in \{ab, ab^2, a\}$.
اگر $ba = a$ ، آنگاه $b = e$.
بنابراین ba می‌تواند ab یا ab^2 باشد.
اگر $ba = ab$ ، آنگاه

$$\begin{matrix} aba = a^2b & abab = a^2b^2 & abab^2 = a^2b^3 \\ abba = a^2b^2 & abbab = a^2b^3 & abbabb = a^2b^4 \\ ba = ab & bab = ab^2 & bba = ab^2 \\ b^2ab = ab^3 \end{matrix}$$

و اگر $ba = ab^2$ ، آنگاه

$$\begin{matrix} aba = a^2b^2 & abab = a^2b^3 & abab^2 = a^2b^4 \\ abba = a^2b^4 & abbab = a^2b^5 & abbabb = a^2b^6 \\ ba = ab^2 & bab = ab^3 & bba = ab^4 \\ b^2ab = ab^5 \end{matrix}$$

تمرین ۱۵. نشان دهید تنها دو گروه ۶ عضوی وجود دارد.

اثبات. همانطور که در تمرین ۱۴ نشان دادیم، یک گروه ۶ عضوی تنها دو جدول ضرب می‌تواند داشته باشد. پس تنها دو گروه ۶ عضوی وجود دارد و بقیه گروه‌ها، نوشتار متفاوتی از همین دو گروه هستند. دو گروه متفاوت ۶ عضوی، S_3 و $\mathbb{Z}_6$ هستند.
در تمرین ۱۴ اگر $ba = ab$ آنگاه جدول ضرب گروه $\mathbb{Z}_6$ به دست می‌آمد. و اگر $ba = ab^2$ آنگاه جدول ضرب گروه S_3 را پیدا می‌کردیم. □

تمرین ۱۶. (بدون استفاده از ابزارهای پیشرفته مثل معادلهٔ رده‌ای) نشان دهید هر گروه ۹ عضوی آبلی است.

اثبات. فرض کنید $|G| = 9$. اگر G دوری باشد، حتما آبلی است. حالا اگر G دوری نباشد، آنگاه مرتبه‌ی هر عنصر غیر بدیهی آن ۳ است. دو عضو متفاوت مانند $a, b \in G$ در نظر می‌گیریم. قرار می‌دهیم:

$$H = \{b, b^2, e\}, \quad \{a, a^2, e\}$$

نشان می‌دهیم eH ، aH و a^2H همدسته‌های متفاوتی هستند.

$$eH \neq aH \neq a^2H$$

یعنی:

$$a \notin H, \quad a^2 \notin H, \quad a \notin aH$$

- فرض کنید $a \in eH$. آنگاه $a = b$ یا $a = b^2$ یا $a = e$.
می‌دانیم که $a \neq e$ چون $O(a) = 3$ و $a \neq b$ (طبق فرض مسئله).
حالا اگر $a = b^2$ ، آنگاه داریم:

$$a = b^2 \implies ab = b^3 = e$$

- فرض کنید $a^2 \in eH$. آنگاه $a^2 = b$ یا $a^2 = b^2$ یا $a^2 = e$.
واضح است که $a^2 \neq e$. اگر $a^2 = b^2$ ، آنگاه:

$$a^2 = b^2 \implies a^2b = e \implies b = a$$

اگر $a^2 = b$ ، آنگاه

$$a^2 = b \implies ab = e$$

- چون $a \notin H$ ، واضح است که $aa^{-1} \in H$. پس این سه هم‌دسته متفاوت هستند.
برای اینکه نشان دهیم G آبلی است، باید نشان دهیم ba فقط می‌تواند ab باشد.

- فرض کنید $ba \in eH = \{b, b^2, e\}$.

$$ba = b \implies a = e$$
$$ba = b^2 \implies a = b$$
$$ba \neq e$$

- اگر $ba \in a^2H = \{a^2b, a^2b^2, a^2\}$.

$$ba = a^2 \implies b = a$$
$$ba = a^2b^2 \implies bab = a^2$$
$$\implies baba = e$$
$$ba = a^2b \implies aba = b$$
$$\implies abab = b^2$$

- و اگر $ba \in aH = \{ab, ab^2, a\}$.

$$ba = a \implies b = e$$
$$ba = ab^2 \implies a = b$$
$$ba \stackrel{?}{=} ab$$

بنابراین، ba فقط می‌تواند با ab برابر باشد. □

تمرین ۱۷. فرض کنید G یک گروه و H یک زیرگروه از آن باشد به طوری که تنها دو همدسته چپ داشته باشد. نشان دهید H یک زیرگروه نرمال است.

راهنمایی. برای هر عنصر $a \in G$ دو همدسته چپِ H و aH را می‌توان برای H در نظر گرفت. حالا جون تعداد هم‌دسته‌های چپ و راست باهم برابرند، پس H دارای همدسته‌های راست H و Ha است. Ha با H برابر نیست پس باید با aH برابر باشد. □

تمرین ۱۸.

الف) آیا $(\mathbb{Z}, -)$ (یعنی با عمل تفریق) یک گروه است؟

ب) برای مجموعه X مجموعهٔ توانی یعنی $P(X)$ را در نظر بگیرید. آیا $P(X)$ با عمل اجتماع یک گروه است؟

ج) آیا $P(X)$ با عمل اشتراک تشکیل گروه می‌دهد؟

د) اثبات کنید $(P(X), \Delta)$ یک گروه است. منظور از Δ عمل تفاضل متقارن است که به صورت زیر تعریف می‌شود:

$$A\Delta B = (A \cup B) - (A \cap B).$$

راهنمایی.

الف) به عنصر خنثی فکر کنید.

ب) به عنصر خنثی و سپس به وارون یک عنصر فکر کنید.

ج) مشابه مورد قبل.

د) پاسخِ این قسمت سوال مثبت است. □

تمرین ۱۹.

۱. مجموعهٔ اعداد مختلط، مجموعهٔ اعدادی به صورت $a + bi$ است که در آن a, b عدد حقیقی هستند و i یک موجود است که تنها در مورد آن می‌دانیم که $i^2 = -1$. نشان دهید که مجموعهٔ اعداد مختلط با عمل ضرب تشکیل گروه می‌دهد (در این عمل ضرب، همه چیز عادی پیش می‌رود ولی هر جا i^2 ظاهر شود، عدد منهای یک به جای آن نوشته می‌شود.)

۲. قرار دهید

$$A = \{\begin{bmatrix} a & b \\ -b & a \end{bmatrix} \mid a, b \in \mathbb{R}, \quad a, b \neq 0\}$$

نشان دهید A با عمل ضرب ماتریس‌ها، گروه است.

۳. نشان دهید گروه‌های مورد ۱ و ۲ با هم ایزومرف هستند.

تمرین ۲۰. فرض کنید G یک گروه، N یک زیرگروه نرمال، و H یک زیرگروه از G باشند. نشان دهید $NH = \{nh \mid n \in N, h \in H\}$ یک زیرگروه از G است.

راهنمایی. بسته بودن NH نسبت به ضرب و وجود عنصر وارون در آن را مستقیماً بررسی کنید. □

تمرین ۲۱.

الف) فرض کنید H_1 و H_2 دو زیرگروه از گروه G باشند. نشان دهید $H_1 \cap H_2$ یک زیر گروه است.

ب) فرض کنید N_1 و N_2 دو زیرگروه نرمال از گروه G باشند. نشان دهید $N_1 \cap N_2$ یک زیر گروه نرمال است.

تمرین ۲۲. فرض کنید N و M دو زیرگروه نرمال از گروه G باشند به طوری که $M \cap N = \{e\}$.
نشان دهید

$$\forall n \in N \; \forall m \in M \quad mn = nm$$

راهنمایی. کافی است نشان دهید که $mn(nm)^{-1} = e$؛ و برای این کافی است نشان دهید که $mn(nm)^{-1}$ هم در M و هم در N است. □