دانشگاه صنعتی اصفهان

دانشکده علوم ریاضی

تعداد مرکزسازهای یک گروه متناهی

کارشناسی ارشدگرایش جبر

عبداله صفیان بلداجی

استاد راهنما

دکتر بیژن طائری

۱۳۹۰

دانشگاه صنعتی اصفهان

دانشکده علوم ریاضی

کارشناسی ارشدگرایش جبرآقای‌عبداله صفیان بلداجی

تحت عنوان

تعداد مرکزسازهای یک گروه متناهی

در تاریخ ۲۰ تیرماه ۱۳۹۰ توسط کمیته تخصصی زیر مورد بررسی و تصویب نهائی قرار گرفت.

۱– استاد راهنمای پایان‌نامه	دکتر بیژن طائری
۲– استاد مشاور پایان‌نامه	دکتر محمد مشکوری
۳– استاد داور ۱	محمد رضا ریسمانچیان (دانشگاه شهرکرد)
۴– استاد داور ۲	دکتر محمد رضا ودادی

سرپرست تحصیلات تکمیلی دانشکده دکتر اعظم اعتماد

تقدیم به همسرم و پسرم

کلیه حقوق مادی مترتب بر نتایج مطالعات، ابتکارات و نوآوری‌های ناشی از
تحقیق موضوع این پایان‌نامه متعلق به دانشگاه صنعتی اصفهان است.

فهرست مطالب

چکیده:

در این پایان نامه تعداد مرکز سازهای یک گروه متناهی را بررسی می‌کنیم. فرض کنیم G یک گروه باشد، مجموعه‌ی مرکزسازهای G را با $\mathrm{Cent}(G)$ نشان می‌دهیم. بررسی ارتباط ساختار گروه و $|\mathrm{Cent}(G)|$ موضوع جالبی است. یک گروه G، $n-$مرکزساز نامیده می‌شود اگر $|\mathrm{Cent}(G)| = n$. هم‌چنین یک گروه G را $n-$ مرکزساز اولیه می‌گوییم اگر $|\mathrm{Cent}(G)| = |\mathrm{Cent}(\frac{G}{Z(G)})|$، که در آن $Z(G)$ مرکز G است. در این پایان نامه گروه‌های ۴$-$مرکزساز تا۸$-$مرکزساز را بررسی می‌کنیم. نشان می‌دهیم گروه ۴$-$مرکزساز اولیه و ۸$-$مرکزساز اولیه وجود ندارد. با توجه به قضایا و نتایج بدست آمده، $\mathrm{Cent}(G)$ و هم‌چنین $|\mathrm{Cent}(G)|$ را برای گروه خطی ویژه تصویری و گروه سوزوکی روی میدانی با q عنصر بدست می‌آوریم و تمام گروه‌های نیم‌ساده متناهی G با $|\mathrm{Cent}(G)| \leq ۷۳$ را مشخص می‌کنیم.

کلمات کلیدی: مرکزساز، مرکز گروه، $n-$مرکزساز، $n-$مرکزساز اولیه، پوشش، گروه خطی ویژه تصویری، گروه سوزوکی

فصل ۱

مقدمه

در این پایان نامه گروه‌های مورد نظر متناهی هستند و فرض بر این است که خواننده با مفاهیم و تعاریف مقدماتی نظریه گروه‌ها و جبرخطی آشنایی دارد. ابتدا مقدمه و سپس به یادآوری تعریف‌ها، قضیه‌ها و لم‌های موردنیاز در این پایان نامه می‌پردازیم.

۱—۱ مقدمه

تعریف ۱.۱ گروه دوری از مرتبه n را با C_n نشان می‌دهیم. هم‌چنین گروه تولید شده به صورت

$$\langle x, y \mid y^{۲} = ۱ \,,\; x^n = ۱ \,,\; xy = yx^{n-۱} \rangle$$

را گروه دووجهی از مرتبه $۲n$ می‌نامیم و با $D_{۲n}$ نشان می‌دهیم.

تعریف ۲.۱ اگر G یک گروه و $x \in G$، مرکزساز x در G عبارت است از $C_G(x) = \{g \in G \mid gx = xg\}$ و مجمو عه‌ی مرکزسازهای G را با$\mathrm{Cent}(G)$ نشان می‌دهیم. هم‌چنین مرکز گروه G عبارت است از $C_G(G)$ که آن را با $Z(G)$ نشان می‌دهیم و داریم $Z(G) = \{a \in G \mid \forall x \in G : \; xa = ax\}$.

تعریف ۳.۱ فرض کنیم G یک گروه و H زیرگروه G باشد. در این صورت مجموعه $\{g \in G \mid g^{-1}Hg = H\}$ نرمال ساز H در G می‌نامند و با $N_G(H)$ نشان می‌دهند. به سادگی می‌توان دید $N_G(H) \leq G$.

بل کاسترو و شرمن در سال ۱۹۹۴ در مورد مرکزسازهای یک گروه متناهی G نتایجی به شرح زیر بدست آوردند:

الف) اگر G گروه ناآبلی باشد، آن‌گاه $|\mathrm{Cent}(G)| \geq ۴$.

ب) یک گروه متناهی G، ۴−مرکزساز است اگر و تنها اگر $\frac{G}{Z(G)} \cong C_۲ \times C_۲$.

ج) یک گروه متناهی G، ۵− مرکزساز است اگر و تنها اگر $\frac{G}{Z(G)} \cong C_۳ \times C_۳$ یا $S_۳$.

د) اگر p عدد اول باشد و $\frac{G}{Z(G)} \cong C_p \times C_p$، آن‌گاه $|\mathrm{Cent}(G)| = p + ۲$ و اگر p عدد اول فرد باشد و $\frac{G}{Z(G)} \cong D_{۲p}$، آن‌گاه $|\mathrm{Cent}(G)| = p + ۲$.

و) گروه n− مرکزساز برای $n = ۲, ۳$ وجود ندارد.

بل کاسترو و شرمن در مقاله خود دو سوال زیر را مطرح کردند:

۱) برای عدد صحیح $n \geq ۴$ آیا گروهی با $|\mathrm{Cent}(G)| = n$ وجود دارد؟

۲) گروهی متناهی به غیر از $Q_۸$ و $D_{۲p}$ وجود دارد که $\frac{|\mathrm{Cent}(G)|}{|G|} \geq \frac{۱}{۲}$؟

سوال اول توسط اشرفی در سال ۲۰۰۰ در [۵] پاسخ داده شد. او نشان داد که برای عدد صحیح مثبت $n \geq ۴$ گروهی با $|\mathrm{Cent}(G)| = n$ وجود دارد و ساختار گروه‌هایی با $|\mathrm{Cent}(G)| = n$ را بررسی کرد. او در سال ۲۰۰۰ در [۴] نشان داد که اگر گروه G، ۶−مرکزساز باشد ، آن‌گاه

$$\frac{G}{Z(G)} \cong D_۸ \text{ یا } A_۴ \text{ یا } C_۲ \times C_۲ \times C_۲ \text{ یا } C_۲ \times C_۲ \times C_۲ \times C_۲.$$

هم‌چنین اگر گروه G، ۷−مرکزساز اولیه باشد، آن‌گاه $\frac{G}{Z(G)} \cong A_۴$. اشرفی اثبات کرد اگر $\frac{G}{Z(G)} \cong A_۴$، آن‌گاه ۸ یا $۶ = |\mathrm{Cent}(G)|$. پاسخ مثبت به سوال دوم نیز توسط اشرفی در [۵] داده شد. اشرفی و طائری در [۶] در سال ۲۰۰۵ ساختار گروه‌های متناهی با بیشتر از ۲۱ عضو مرکزساز را بررسی کردند و با استفاده از رده بندی گروه‌های ساده‌ی متناهی ثابت کردند که اگر G یک گروه ساده متناهی و $|\mathrm{Cent}(G)| = ۲۲$، آن‌گاه $G \cong A_۵$. آن‌ها در این مقاله نشان دادند که اگر G گروه متناهی و $\frac{G}{Z(G)} \cong A_۵$، آن‌گاه ۳۲ یا $۲۲ = |\mathrm{Cent}(G)|$ و سوال زیر را مطرح کردند:

برای گروه ساده و متناهی G و H اگر $|\mathrm{Cent}(G)| = |\mathrm{Cent}(H)|$، آیا می‌توان نتیجه گرفت که $G \cong H$؟

به این سؤال توسط زرین در [۱۹] پاسخ منفی داده شد که در این پایان نامه بررسی شده است.

۱–۲ تعاریف و قضایای مورد نیاز

تعریف ۴.۱ اگر G یک گروه باشد یک همریختی از G به G را یک درون ریختی G گوییم. یکریختی از G به G را خود ریختی گوییم. مجموعه‌ی همه‌ی خود ریختی‌های G را با $\mathrm{Aut(G)}$ نشان می‌دهیم. $\mathrm{Aut(G)}$ تحت عمل ترکیب توابع یک گروه است. اگر $g \in G$، آن‌گاه تابع $\phi_g : G \to G$ را با ضابطه‌ی $\phi_g(x) = gxg^{-1}$، خود ریختی داخلی G گوییم. مجموعه تمام خود ریختی‌های داخلی را با $\mathrm{Inn}(G)$ نشان می‌دهیم. به سادگی می‌توان دید $\mathrm{Inn}(G)$ تحت عمل ترکیب توابع گروه است.

لم ۵.۱ اگر G یک گروه متناهی و $x \in G$ وجود داشته باشد به طوری که $C_G(x) = Z(G)$، آن‌گاه G آبلی است.

اثبات. چون $C_G(x) = Z(G)$، کافی است نشان دهیم $C_G(x) = G$. می‌دانیم

$$C_G(x) = Z(G) = \bigcap_{y \in G} C_G(y).$$

بنابراین برای هر $g \in G$ داریم $C_G(x) \subseteq C_G(g)$، یعنی برای هر $g \in G$ داریم، $xg = gx$. از این‌رو $C_G(x) = G$. بنابراین نتیجه می‌گیریم که $Z(G) = G$ و G آبلی است. ∎

تعریف ۶.۱ گروه G را یک گروه $n-$ مجموع گوییم هرگاه بتوان آن را به صورت اجتماع n زیرگروه سره‌اش و نه تعداد کمتر از n نوشت در این حالت می‌نویسیم $\sigma(G) = n$. بنابراین گروه G، n مجموع است اگر و تنها اگر زیرگروه‌های سره‌ی $H_1, \dots, H_n$ از G وجود داشته باشند که $G = \bigcup_{i=1}^{n} H_i$ و $\bigcap_{i=1, i\neq j}^{n} H_i \subsetneqq H_j$ و به علاوه نتوان G را به صورت اجتماع تعداد کمتر از n زیرگروه نوشت.

لم ۷.۱ گروه G را نمی‌توان به صورت اجتماع دو زیرگروه سره‌اش نوشت.

اثبات. فرض کنیم زیرگروه‌های A و B از گروه G وجود داشته باشند که $G = A \cup B$. ولی می‌دانیم $A \cup B$ وقتی زیرگروه G است که $A \subseteq B$ یا $B \subseteq A$. بنابراین G به صورت اجتماع یک زیرگروه سره‌اش نوشته می‌شود که تناقض است. ∎

قضیه ۸.۱ گروه G، اجتماع (نابدیهی) سه‌زیرگروه سره خودش است اگر و تنها اگر G تصویر همریخت ۴− گروه کلاین، V، باشد.

اثبات. قضیه‌ی ۷.۱.۹ در [۲۰] را ببینید. ■

تعریف ۹.۱ فرض کنیم G یک گروه باشد. در این صورت $N \neq <e>$ را زیرگروه نرمال مینیمال از G گوییم اگر $N, <e>$ تنها زیرگروه‌های نرمال از G و مشمول در N باشند.

لم ۱۰.۱ فرض کنیم N زیرگروه نرمال مینیمال از G باشد. در این صورت برای هر زیرگروه نرمال M از G داریم $N \cap M = e$ یا $N \leq M$.

اثبات. فرض کنیم M زیرگروه نرمال از G باشد. پس داریم $M \cap N \trianglelefteq G$ و $M \cap N \leq N$. بنابراین چون N زیرگروه نرمال مینیمال است پس $M \cap N = e$ یا $N \leq M$. ■

لم ۱۱.۱ فرض کنیم M یک مجموعه متناهی از زیرگروه‌های نرمال مینیمال از گروه متناهی G باشند و $M = \prod\limits_{N \in M} N$. در این صورت زیرگروه‌های نرمال مینیمال $N_1, N_2, ..., N_n \in M$ وجود دارند به طوری که $N = N_1 \times ... \times N_n$.

اثبات. فرض کنیم U یک زیرگروه نرمال از G باشد. بنابر لم ۱۰.۱ برای هر $N \in M$ که $N \nleq U$ داریم $U \cap N = e$ و $UN = U \times N$. فرض کنیم مجموعه $\{N_1, ..., N_n\}$ یک زیرمجموعه ماکسیمال از M با این خاصیت که

$$U(\prod_{i=1}^{n} N_i) = U \times N_1 \times ... \times N_n =: X.$$

ادعا می‌کنیم $X = UM$، چون اگر $X \neq UM$ پس $N \in M$ وجود دارد به طوری که $N \nleq X$. بنا بر لم ۱۰.۱ داریم

$$XN = X \times N = U \times N_1 \times ... \times N_n \times N.$$

که این تناقض با انتخاب ماکسیمال بودن $\{N_1, ..., N_n\}$ دارد. بنابراین $X = UM$. حال اگر $U = e$ فرض کنیم داریم $M = N_1 \times ... \times N_n$. ■

قضیه ۱۲.۱ فرض کنیم $G = \bigcup_{i=1}^{n} H_i$ به طوری که $|G : H_1| \leq |G : H_2| \leq \ldots \leq |G : H_n|$. دراین صورت داریم $|G| \leq \sum_{=2}^{n} |H_i|$ و تساوی برقرار است اگر و تنها اگر

الف) برای $i \neq 1$، $H_1 H_i = G$.

ب) برای $i \neq j$، $H_i \cap H_j \subset H_1$.

اثبات. تعداد عناصر H_i که در H_1 قرار ندارند برابر است با

$$\begin{aligned} |H_i| - |H_1 \cap H_i| &= |H_i| - \frac{|H_1||H_i|}{|H_1 H_i|} \\ &\leq |H_i| - \frac{|H_1||H_i|}{|G|} = |H_i|(1 - \frac{|H_1|}{|G|}). \end{aligned}$$

بنابراین

$$\begin{aligned} |G| = |\bigcup_{i=1}^{n} H_i| &\leq |H_1| + \sum_{i=2}^{n} (|H_i| - (|H_1 \cap H_i|)) \\ &\leq |H_1| + (1 - \frac{|H_1|}{|G|}) \sum_{i=2}^{n} |H_i|. \end{aligned} \qquad (1)$$

که از آن نامساوی موردنظر $|G| \leq \sum_{i=2}^{n} |H_i|$ حاصل می‌شود. تساوی برقرار است اگر و تنها اگر $|G| = |H_1 H_i|$، یعنی $G = H_1 H_i$. در (۱) تساوی برقرار است اگر و تنها اگر هیچ دو زیرگروهی عضو مشترکی نداشته باشند که در H_1 نیز نباشد، یعنی برای هر $i \neq j$، $H_i \cap H_j \subset H_1$. ■

لم ۱۳.۱ فرض کنیم $\sigma(G) = n$ و $G = \bigcup_{i=1}^{n} H_i$. با فرض این که
$|G : H_1| \leq |G : H_2| \leq \cdots \leq |G : H_n|$.
در این صورت داریم $|G : H_2| \leq n - 1$.

اثبات. طبق قضیه ۱۲.۱، داریم $|G| \leq |H_2| + \cdots + |H_n|$. چون

$$|H_1| \geq |H_2| \geq \cdots \geq |H_n|.$$

داریم

$$\frac{|G|}{|H_2|} \leq 1 + \frac{|H_3|}{|H_2|} + \cdots + \frac{|H_n|}{|H_2|} \leq \underbrace{1 + \cdots + 1}_{n-1=\text{بار}} = n - 1.$$

بنابراین نتیجه حاصل است. ■

لم ۱۴.۱ $\sigma(G)=3$ اگر و تنها اگر G حداقل دو زیرگروه با شاخص ۲ داشته باشد.

اثبات. فرض کنیم $G=H_1\cup H_2\cup H_3$. دراین‌صورت با قراردادهای بالا و با استفاده از لم ۱۳.۱ داریم $|G:H_2|\le 2$. چون $H_2\le G$، داریم $|G:H_2|=2$. از طرف دیگر چون $|G:H_1|\le|G:H_2|=2$، داریم $|G:H_1|=2$. بنابراین H_1 و H_2 دو زیرگروه با شاخص ۲ هستند.
برعکس اگر G دو زیرگروه H_1 و H_2 با شاخص ۲ داشته باشد، آن‌گاه H_1 و H_2 در G نرمال اند. در نتیجه $N=H_1\cap H_2$ در G نرمال است. چون

$$\frac{G}{N}=\frac{G}{H_1\cap H_2}\hookrightarrow\frac{G}{H_1}\times\frac{G}{H_2}\cong C_2\times C_2.$$

بنابراین $\frac{G}{N}\cong C_2\times C_2$ و طبق قضیه ۸.۱، G گروه ۳-مجموع است. ■

لم ۱۵.۱ اگر G یک گروه متناهی و $\mathrm{Cent}(G)=\{G,C_G(x_1),\ldots,C_G(x_n)\}$، آن‌گاه داریم
الف) $G=\bigcup_{i=1}^{n}C_G(x_i)$
ب) به ازای $a\in Z(G)$، $C_G(x_i)=C_G(ax_i)$ برای $i=1,\ldots,n$.

اثبات. الف) فرض کنیم $x\in G$، عنصری دلخواه باشد. می‌دانیم $x\in C_G(x)$ و $i\in\{1,\ldots,n\}$ وجود دارد به طوری که $C_G(x_i)=C_G(x)$. بنابراین داریم $G\subseteq\bigcup_{i=1}^{n}C_G(x_i)$. از طرفی $\bigcup_{i=1}^{n}C_G(x_i)\subseteq G$. بنابراین خواهیم داشت $G=\bigcup_{i=1}^{n}C_G(x_i)$.
ب) فرض کنیم $x\in C_G(x_i)$. حال چون $a\in Z(G)$. در این صورت داریم

$$\begin{aligned} xax_i &= axx_i\\ &= ax_ix. \end{aligned}$$

از این‌رو خواهیم داشت $x\in C_G(ax_i)$. بنابراین $C_G(x_i)\subseteq C_G(ax_i)$. حال فرض کنیم $x\in C_G(ax_i)$. از این‌رو داریم

$$\begin{aligned} ax_ix &= xax_i\\ &= axx_i \qquad (a\in Z(G)\ \text{چون}). \end{aligned}$$

بنابراین خواهیم داشت $x_ix=xx_i$، یعنی $x\in C_G(x_i)$. از این‌رو $C_G(ax_i)\subset C_G(x_i)$. بنابراین داریم $C_G(ax_i)=C_G(x_i)$. ■

تعریف ۱۶.۱ یک زیرمجموعه ناتهی $X = \{x_1, \ldots, x_n\}$ از گروه متناهی G را یک مجموعه با عناصر دو به دو تعویض ناشونده گوییم، اگر برای هر $i \neq j,\ i, j \in \{1, \ldots, n\}$ داشته باشیم $x_i x_j \neq x_j x_i$. هم‌چنین یک مجموعه از عناصر دو به دو تعویض ناشونده از گروه G را دارای اندازه‌ی ماکسیمال می‌گوییم، هرگاه تعداد اعضای این مجموعه، از تعداد اعضای تمام مجموعه‌های با عناصر دو به دو تعویض ناشونده از گروه G، بزرگ‌تر باشد.

قضیه ۱۷.۱ فرض کنیم $\{x_1, \ldots, x_n\}$ زیرمجموعه‌ای با اندازه ماکسیمال از عناصر دو به دو تعویض ناشونده‌ی گروه G باشد. در این صورت:

الف) $G = \bigcup_{i=1}^{n} C_G(x_i)$

ب) $Z(G) = \bigcap_{i=1}^{n} C_G(x_i)$

اثبات. الف) اگر $x \in G \setminus (\bigcup_{i=1}^{n} C_G(x_i))$، آن‌گاه به ازای هر $1 \leq i \leq n$، داریم $x \notin C_G(x_i)$. از این‌رو $\{x_1, \ldots, x_n, x\}$ مجموعه‌ای از عناصر دو به دو تعویض ناشونده با اندازه‌ی $n + 1$ است، که این خلاف فرض است.

ب) از یک طرف واضح است که $Z(G) \subseteq \bigcap_{i=1}^{n} C_G(x_i)$. از طرف دیگر اگر عضوی مثل $a \in (\bigcap_{i=1}^{n} C_G(x_i)) \setminus Z(G)$ وجود داشته باشد، آن‌گاه عضو $b \in G$ وجود دارد که $ab \neq ba$. برای هر $1 \leq i \leq n$ تعریف می‌کنیم

$$y_i = \begin{cases} x_i & \text{اگر} \quad [x_i, b] \neq 1 \\ ax_i & \text{اگر} \quad [x_i, b] = 1. \end{cases}$$

در این صورت $\{y_1, \ldots, y_n, b\}$ مجموعه‌ای از عناصر دو به دو تعویض ناشونده، با اندازه‌ی $n + 1$ است. این خلاف ماکسیمال بودن n است. ∎

قضیه ۱۸.۱ فرض کنیم G گروهی دلخواهی باشد. در این صورت اگر $\frac{G}{Z(G)}$ دوری باشد، آن‌گاه G آبلی است.

اثبات. قرار دهید $Z = Z(G)$. فرض کنیم $\frac{G}{Z} = <gZ>$ و $a, b \in G$. در این صورت اعداد صحیح $m, n \in \mathbb{Z}$، وجود دارند که $bZ = g^m Z$ و $aZ = g^n Z$. از این‌رو $a \in g^n Z$ و $b \in g^m Z$. بنابراین $d, h \in \mathbb{Z}$ وجود دارند که $a = g^n d$ و $b = g^m h$. داریم

$$ab = (g^n d)(g^m h)$$

$$\begin{aligned} &= g^n g^m dh = g^{n+m} hd \\ &= g^m g^n hd = g^m hg^n d = ba. \end{aligned}$$

بنابراین G آبلی است. ■

قضیه ۱۹.۱ فرض کنیم G گروه و p عددی اول باشد. در این صورت اگر $|G| = p^n$، آن‌گاه $Z(G) \neq \{e\}$.

اثبات. قضیه ۱۳.۱۲.۳ در [۲۰] را ببینید. ■

نتیجه ۲۰.۱ هر گروه G ازمرتبه p^2 آبلی است.

اثبات. با توجه به فرض مرتبه G توانی از عدد اول p است. پس بنا به قضیه ۱۹.۱، داریم p^2 یا $|Z(G)| = p$. پس خواهیم داشت p یا $|\frac{G}{Z(G)}| = 1$. بنابراین اگر $|\frac{G}{Z(G)}| = 1$، آن‌گاه $G = Z(G)$. ازاین‌رو G آبلی است. هم‌چنین اگر $|\frac{G}{Z(G)}| = p$، آن‌گاه $\frac{G}{Z(G)}$ دوری است و طبق قضیه ۱۸.۱، G آبلی است. ■

لم ۲۱.۱ فرض کنیم G گروهی دلخواه باشد. در این صورت داریم $\frac{G}{Z(G)} \cong \mathrm{Inn}(G)$.

اثبات. تابع $h : G \to \mathrm{Inn}(G)$ را برای هر $g \in G$ با ضابطه $h(g) = \rho_g$ تعریف می‌کنیم که در آن $\rho_g : G \to G$ خودریختی داخلی با ضابطه $\rho_g(x) = gxg^{-1}$ است. به سادگی می‌توان دید که h همریختی است. داریم $\ker h = Z(G)$. به وضوح h پوشاست و طبق قضیه‌ی اول یکریختی داریم $\frac{G}{\ker h} \cong h(G)$. بنابراین خواهیم داشت $\frac{G}{Z(G)} \cong \mathrm{Inn}(G)$. ■

تعریف ۲۲.۱ فرض کنیم G یک گروه باشد و $x, y \in G$. در این صورت تعویض‌گر x, y را به صورت $[x, y] = x^{-1}y^{-1}xy$ تعریف می‌کنیم. هم‌چنین زیرگروه تولید شده توسط همه تعویض‌گرهای $[x, y]$ را زیرگروه مشتق G می‌گوییم و با G' نمایش می‌دهیم.

لم ۲۳.۱ فرض کنیم G یک گروه و $H \leq G$. در این صورت $\frac{G}{H}$ آبلی است اگر و تنها اگر $G' \leq H$.

اثبات. $\frac{G}{H}$ آبلی است اگر و تنها اگر به ازای هر $a, b \in G$، $aHbH = bHaH$ اگر و تنها اگر $abH = baH$ اگر و تنها اگر $a^{-۱}b^{-۱}abH = H$ اگر و تنها اگر $[a, b] \in H$. این به این معنی است که $\frac{G}{H}$ آبلی است اگر و تنها اگر $G' = \langle [a, b] | a, b \in G\rangle \leq H$. ■

لم ۲۴.۱ فرض کنیم G یک گروه باشد و $a, b, c, d \in G$. در این صورت اگر $G' \leq Z(G)$، آن‌گاه داریم
الف) $[a, bc] = [a, b][a, c]$ ب) $[ab, cd] = [a, c][a, d][b, c][b, d]$

اثبات. الف)

$$\begin{aligned}[a, bc] &= a^{-۱}c^{-۱}b^{-۱}abc \\ &= a^{-۱}c^{-۱}acc^{-۱}a^{-۱}b^{-۱}abc \\ &= [a, c]c^{-۱}[a, b]c \qquad (\text{چون } G' \leq Z(G)) \\ &= [a, c][a, b]c^{-۱}c \\ &= [a, c][a, b].\end{aligned}$$

ب) اثبات به طور مشابه است. ■

لم ۲۵.۱ اگر G یک گروه و برای هر $x \in G$ داشته باشیم $x^{۲} \in Z(G)$، آن‌گاه $G' \leq Z(G)$ و $[x, y]^{۲} = ۱$.

اثبات. چون $x^{۲} \in Z(G)$ از این‌رو مرتبه هر عضو نابدیهی $\frac{G}{Z(G)}$ برابر ۲ است. بنابراین $\frac{G}{Z(G)}$ آبلی است. ازاین‌رو $G' \leq Z(G)$. چون $x^{۲} \in Z(G)$ بنابراین برای هر $x, y \in G$ داریم $[x, y^{۲}] = ۱$. از طرفی بنابر لم ۲۴.۱ داریم

$$[x, y^{۲}] = [x, y][x, y] = [x, y]^{۲}.$$

بنابراین نتیجه می‌گیریم $[x, y]^{۲} = ۱$. ■

لم ۲۶.۱ فرض کنیم G یک گروه و $A, B \trianglelefteq G$ و $Z(G) = A \cap B$. در این صورت $\frac{G}{A\cap B} \cong \frac{G}{A} \times \frac{G}{B}$.

اثبات. تابع

$$\begin{cases} f: & G \to \frac{G}{A} \times \frac{G}{B} \\ & g \to (gA, gB) \end{cases}$$

را درنظر می‌گیریم. به وضوح f همریختی است و $\ker f = A \cap B$ و f پوشاست. حال طبق قضیه اول همریختی خواهیم داشت $\frac{G}{A\cap B} \cong \frac{G}{A} \times \frac{G}{B}$. ■

تعریف ۲۷.۱ گوییم گروه G روی مجموعه‌ی غیرتهی X عمل می‌کند، هرگاه برای هر $g \in G$ و هر $t \in X$ عضو یکتای $gt \in X$ وجود داشته باشد به طوری که به ازای هر $x \in X$ و هر $g_۱, g_۲ \in G$ داشته باشیم

$$(g_۱ g_۲)x = g_۱(g_۲ x), \quad ex = x.$$

مثال ۲۸.۱ فرض کنیم X یک مجموعه‌ی غیرتهی و $G \leq S_X$. (S_X گروه جایگشت‌های روی مجموعه‌ی X است). در این صورت G روی مجموعه‌ی X عمل می‌کند. در این مورد هر عضو $g \in G$ نگاشتی از X به X است و برای $x \in X$، gx تصویر x تحت نگاشت g است. شرط اول گفته شده در تعریف ۲۷.۱، با توجه به تعریف ترکیب توابع برقرار است و شرط دوم با توجه به این‌که ex نگاشت همانی روی X است، برقرار است. این عمل، عمل طبیعی روی X نامیده می‌شود.

قضیه ۲۹.۱ فرض کنیم گروه G روی مجموعه‌ی X عمل می‌کند. در این صورت به هر عضو $g \in G$ یک نگاشت $\rho_g : X \to X$ با ضابطه‌ی $\rho_g : x \longmapsto gx$ متناظر می‌شود و این نگاشت یک جایگشت روی X است. هم‌چنین نگاشت $\rho : G \to S_X$ با ضابطه‌ی $\rho : g \longmapsto \rho_g$ یک همریختی گروهی است که نمایش جایگشت متناظر عمل گروه G نامیده می‌شود.

اثبات. برهان راحت است. ■

قضیه ۳۰.۱ فرض کنیم σ یک همریختی از گروه G به توی گروه S_X باشد که X یک مجموعه‌ی غیرتهی است. اگر برای هر $x \in X$ و هر $g \in G$ تعریف کنیم $gx = (g\sigma)x$، آن‌گاه G روی مجموعه‌ی X عمل می‌کند. که σ نمایش جایگشت متناظر عمل G است.

اثبات. برهان راحت است. ■

تعریف ۳۱.۱ فرض کنیم که گروه G روی مجموعه‌ی X عمل می‌کند. در این صورت عمل را وفادار گوییم هرگاه نمایش متناظر عمل گروه G، یک به یک باشد. در مثال ۲۸.۱، نمایش جایگشت مورد نظر، نگاشت شمول $i : G \to S_X$ است که به وضوح یک به یک است.

لم ۳۲.۱ فرض کنیم گروه G روی مجموعه‌ی X عمل می‌کند. رابطه‌ی $\sim$ را روی مجموعه‌ی X این‌گونه تعریف می‌کنیم $x_1 \sim x_2$ اگر و تنها اگر عضو $g \in G$ وجود داشته باشدبه طوری که $x_1 g = x_2$. آن‌گاه $\sim$ یک رابطه‌ی هم‌ارزی روی X است.

اثبات. قضیه‌ی ۶.۴ در [۱۶] را ببینید. ■

تعریف ۳۳.۱ فرض کنیم G روی مجموعه‌ی X عمل می‌کند. در این صورت X نسبت به رابطه‌ی هم‌ارزی $\sim$، به رده‌های هم‌ارزی مجزا از هم افراز می‌شود. این رده‌های هم‌ارزی مدارها یا رده‌های ترایایی عمل نامیده می‌شود. برای هر $x \in X$ رده‌ی شامل عضو x مدار x نامیده می‌شود که آن را با $\mathrm{orb(x)}$ نشان می‌دهیم و $\mathrm{orb(x)} := \{gx \mid g \in G\}$.

لم ۳۴.۱ فرض کنیم G روی مجموعه‌ی X عمل می‌کند و $x \in X$. قرار دهید

$$\mathrm{stab}_G(x) := \{g \in G \mid gx = x\}.$$

در این صورت $\mathrm{stab}_G(x)$ یک زیرگروه G است که ثابت‌ساز x در G نامیده می‌شود.

اثبات. قضیه‌ی ۸.۴ در [۱۶] را ببینید. ■

لم ۳۵.۱ فرض کنیم گروه G روی مجموعه‌ی X عمل کند و $x \in X$. در این صورت داریم

$$|\mathrm{orb}(x)| = |G : \mathrm{stab}_G(x)|.$$

اثبات. قضیه‌ی ۱۱.۴ از [۱۶] را ببینید. ■

تعریف ۳۶.۱ فرض کنیم G روی مجموعه‌ی X عمل می‌کند. در این صورت این عمل را متعدی گوییم هرگاه فقط و فقط دارای یک مدار باشد.

گزاره ۳۷.۱ فرض کنیم G رو ی مجموعه‌ی X عمل می‌کند و ρ نمایش جایگشت متناظر این عمل است. در این صورت $\ker\rho = \bigcap_{x\in X} \mathrm{stab}_G(x)$

اثبات. فرض کنیم $t \in \ker\rho$ عضوی دلخواه باشد. دراین صورت داریم

$$\begin{aligned} \rho_t = ۱_X &\iff \rho_t(x) = x,\ \forall x \in X \\ &\iff tx = x,\ \forall x \in X \\ &\iff t \in \mathrm{stab}_G(x),\ \forall x \in X \\ &\iff t \in \bigcap_{x\in X} \mathrm{stab}_G(x). \end{aligned}$$

ازاین‌رو به وضوح حکم مورد نظر برقرار است. ■

مثال ۳۸.۱ فرض کنیم $H \leq G$ و X مجموعه‌ی هم‌مجموعه‌های چپ H در G باشد. در این صورت G روی X از چپ عمل می‌کند، یعنی به هر $g \in G$ و هر $xH \in X$، هم‌مجموعه‌ی چپ $gxH \in X$ متناظر می‌شود. تحقیق شرایط این عمل ساده است. این عمل متعدی است، زیرا برای هر $x_۱H, x_۲H \in X$ داریم $x_۲H = (x_۱^{-۱}x_۲)(x_۱H)$. اکنون داریم

$$\begin{aligned} \mathrm{stab}_G(xH) &= \{g \in G | gxH = xH\} \\ &= \{g \in G | g \in xHx^{-۱}\} \\ &= xHx^{-۱}. \end{aligned}$$

بنابر لم ۱—۲.۳۰ داریم $|G : H| = |G : xHx^{-۱}| = |X|$. نمایش جایگشت این عمل را با ρ^H نشان می‌دهیم. هسته‌ی این همریختی به صورت زیر است

$$\ker\rho^H = \bigcap_{x\in G} xHx^{-۱} = H_G = \mathrm{Core}_G(H).$$

زیرگروه H_G را هسته‌ی H در G نامیم. با فرض این‌که $|G : H| < \infty$ و با توجه این‌که $S_X \cong S_{|G:H|}$، می‌توان گفت که ρ^H یک همریختی گروهی از G به توی $S_{|G:H|}$ است. در نتیجه با توجه به به قضیه‌ی اول یکریختی $\frac{G}{H_G}$ را می‌توان در $S_{|G:H|}$ نشاند. بنابراین $|G : H|! = |S_{|G:H|}| \mid |\frac{G}{H_G}|$.

نتیجه ۳۹.۱ فرض کنیم G یک گروه متناهی و p کوچکترین شمارنده‌ی اول $|G|$ باشد. در این صورت اگر $H \leq G$ و $|G:H| = p$، آن‌گاه $H \trianglelefteq G$.

اثبات. در ابتدا از این‌که $H_G \leq H \leq G$، داریم

$$|G : H_G| = |G : H||H : H_G| = p|H_G : H|.$$

حال فرض کنیم $|H : H_G| > ۱$ و q شمارنده‌ی اول $|H : H_G|$ باشد. در این صورت $q \mid |G|$ و $q \mid |G : H_G|$. بنا به فرض قضیه داریم $q \geq p$. از طرفی با توجه به مثال ۳۸.۱، $|\frac{G}{H_G}| \mid p!$. از این‌رو داریم $q \mid (p-۱)!$. چون q عددی اول است، بایستی یکی از اعداد ۱ یا ۲ ... $p-۱$ را بشمارد. بنابراین $q < p$ که تناقض است. پس داریم $|H : H_G| = ۱$. در نتیجه $H = H_G \trianglelefteq G$. ■

گزاره ۴۰.۱ فرض کنیم $H \leq G$ و $|G : H| = ۲$. در این صورت H زیرگروه نرمال G است.

اثبات. با توجه به نتیجه‌ی ۳۹.۱، برهان واضح است. ■

تعریف ۴۱.۱ گروه متناهی G یک $p-$ گروه است اگر و تنها اگر، $|G|$ توانی از عدد p باشد.

تعریف ۴۲.۱ فرض کنیم G یک گروه متناهی باشد اگر $|G| = p^n m$ که p عدد اول و $p \nmid m$، آن‌گاه هر زیرگروه G از مرتبه p^n را $p-$زیرگروه سیلوی G می‌نامیم و مجموعه $p-$زیرگروه سیلوهای G را با $\mathrm{Syl}_p(G)$ نشان می‌دهیم.

قضیه ۴۳.۱ (قضیه‌ی دوم سیلو) اگر G یک گروه متناهی باشد، آن‌گاه هر دو $p-$ زیرگروه سیلوی G، در G مزدوجند.

اثبات. به قضیه ۴.۵.۵ در [۲۰] مراجعه کنید. ■

قضیه ۴۴.۱ (قضیه سوم سیلو) اگر $|G| = p^n m$، که در آن p عدد اول و $p \nmid m$، آن‌گاه $n_p \equiv ۱ \pmod p$ که منظور n_p تعداد $p-$ سیلو زیرگروه‌های G است.

اثبات. به قضیه ۸.۵.۵ در [۲۰] مراجعه کنید. ■

تعریف ۴۵.۱ گروه G را ساده گویند هرگاه تنها زیرگروه‌های نرمال آن، G و $\{e\}$ باشند.

لم ۴۶.۱ اگر G یک گروه باشد و $|G| = pq$، که در آن p و q اعداد اول متمایز هستند به طوری که $q \not\equiv ۱ \pmod p$، آن‌گاه $p-$ زیرگروه سیلوی G در G نرمال است.

اثبات. بنا به قضایای سیلو، $n_p \mid q$ و $n_p \equiv ۱ \pmod p$. اگر $n_p = q$، آن‌گاه $q \equiv ۱ \pmod p$ که خلاف فرض است. بنابراین $n_p = ۱$ و $p-$ زیرگروه سیلوی G یکتا و در G نرمال است. ■

لم ۴۷.۱ اگر $|G| = pq$ (p و q اعداد اول متمایز)، آن‌گاه G ساده نیست.

اثبات. بدون کم شدن از کلیت مساله می‌توان فرض کرد $p > q$. بنابراین $p > q > q - ۱$ و $p \not| \, q - ۱$. از این رو طبق لم ۴۶.۱، $p-$ زیرگروه سیلوی G در G نرمال است. ■

لم ۴۸.۱ اگر $|G| = pq$ (که در آن p و q اعداد اول متمایز هستند) و $p \not\equiv ۱ \pmod q$ و $q \not\equiv ۱ \pmod p$، آن‌گاه G دوری است.

اثبات. اگر $P \in \mathrm{Syl}_p(G)$ و $Q \in \mathrm{Syl}_q(G)$، آن‌گاه طبق لم ۴۶.۱، $P \trianglelefteq G$ و $Q \trianglelefteq G$. از طرفی چون $|P \cap Q|$ هم p و هم q را می‌شمارد، داریم $|P \cap Q| = ۱$، یعنی $P \cap Q = \{۱\}$. بنابراین $|PQ| = |P||Q| = pq = |G|$ که نتیجه می‌دهد $G = PQ$. بنابراین $G = P \times Q$. چون P و Q دوری‌اند و مرتبه‌هایشان نسبت به هم اول است، G نیز دوری است. ■

لم ۴۹.۱ A_n برای $n \geq ۵$، یک گروه ساده است.

اثبات. قضیه ۱۳.۱۰.۳ از [۲۰] را ببینید. ■

تعریف ۵۰.۱ گروه G را نیم ساده گویند اگر G دارای زیرگروه آبلی نرمال غیربدیهی نباشد.