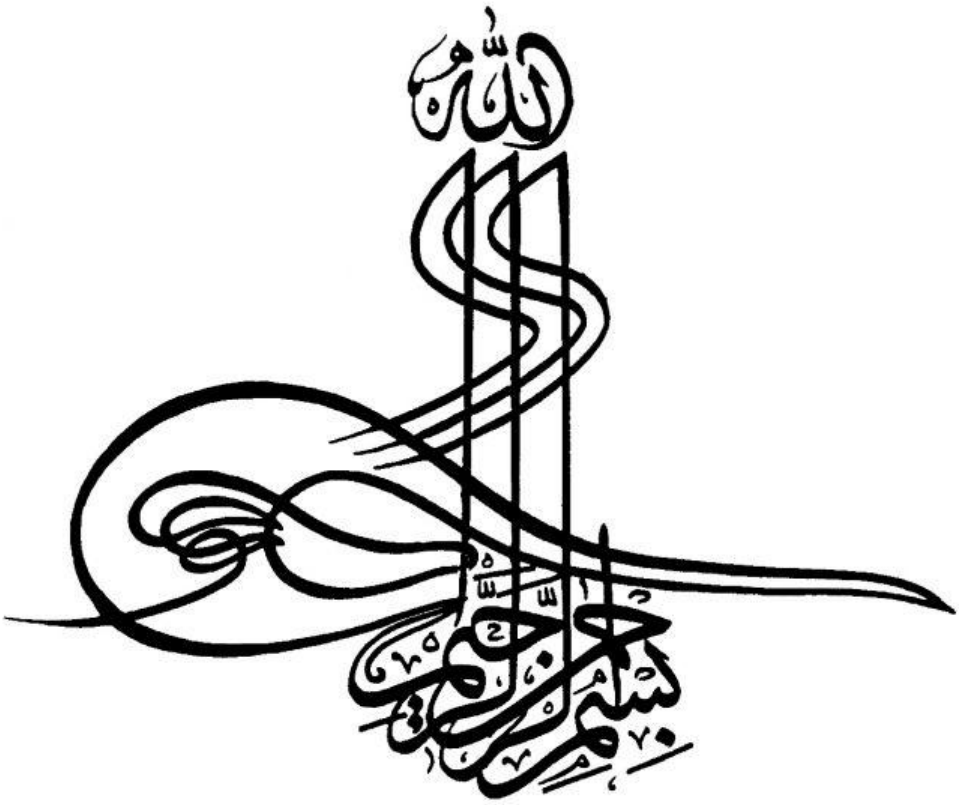
الله
بسم الله الرحمن الرحيم

تعهدنامه‌ی اصالت اثر و رعایت حقوق دانشگاه

تمامی حقوق مادی و معنوی مترتب بر نتایج، ابتکارات، اختراعات و نوآوری‌های ناشی از انجام این پژوهش، متعلق به **دانشگاه محقق اردبیلی** می‌باشد. نقل مطلب از این اثر، با رعایت مقررات مربوطه و با ذکر نام دانشگاه محقق اردبیلی، نام استاد راهنما و دانشجو بلامانع است.

اینجانب زهرا شهبازی دانش‌آموخته مقطع کارشناسی ارشد رشته‌ی ریاضی محض گرایش جبر دانشکده‌ی علوم ریاضی دانشگاه محقق اردبیلی به شماره‌ی دانشجویی ۹۰۲۲٤۱۳۱۱٤ که در تاریخ ۹۲/۱۱/۰۷ از پایان‌نامه‌ی تحصیلی خود تحت عنوان "درباره‌ی تعداد جواب‌های معادله $x^{p^k} = a$ در یک p-گروه متناهی"، دفاع نموده‌ام متعهد می‌شوم که:

۱) این پایان‌نامه را قبلاً برای دریافت هیچ‌گونه مدرک تحصیلی یا به عنوان هرگونه فعالیت پژوهشی در سایر دانشگاه‌ها و مؤسسات آموزشی و پژوهشی داخل و خارج از کشور ارائه ننموده‌ام.

۲) مسئولیت صحّت و سقم تمامی مندرجات پایان‌نامه‌ی تحصیلی خود را بر عهده می‌گیرم.

۳) این پایان‌نامه، حاصل پژوهش انجام شده توسط اینجانب می‌باشد.

٤) در مواردی که از دستاوردهای علمی و پژوهشی دیگران استفاده نموده‌ام، مطابق ضوابط و مقرّرات مربوطه و با رعایت اصل امانتداری علمی، نام منبع مورد استفاده و سایر مشخصات آن را در متن و فهرست منابع و مآخذ ذکر نموده‌ام.

۵) چنانچه بعد از فراغت از تحصیل، قصد استفاده یا هر گونه بهره‌برداری اعم از نشر کتاب، ثبت اختراع و ... از این پایان‌نامه را داشته باشم، از حوزه‌ی معاونت پژوهشی و فنّاوری دانشگاه محقق اردبیلی، مجوزهای لازم را اخذ نمایم.

٦) در صورت ارائه‌ی مقاله‌ی مستخرج از این پایان‌نامه در همایش‌ها، کنفرانس‌ها، سمینارها، گردهمایی‌ها و انواع مجلات، نام دانشگاه محقق اردبیلی را در کنار نام نویسندگان (دانشجو و اساتید راهنما و مشاور) ذکر نمایم.

۷) چنانچه در هر مقطع زمانی، خلاف موارد فوق ثابت شود، عواقب ناشی از آن (منجمله ابطال مدرک تحصیلی، طرح شکایت توسط دانشگاه و ...) را می‌پذیرم و دانشگاه محقق اردبیلی را مجاز می‌دانم با اینجانب مطابق ضوابط و مقرّرات مربوطه رفتار نماید.

نام و نام خانوادگی دانشجو : زهرا شهبازی

امضا

تاریخ

دانشکده‌ی علوم ریاضی
گروه ریاضیات و کاربردها

پایان‌نامه برای دریافت درجه کارشناسی ارشد
در رشته‌ی ریاضی محض گرایش جبر

عنوان:

درباره‌ی تعداد جواب‌های معادله $x^{p^k} = a$ در یک p- گروه متناهی

استاد راهنما:

دکتر حسین عبدل‌زاده

استاد مشاور:

مهندس قادر قاسمی

پژوهشگر:

زهرا شهبازی

بهمن ۹۲

دانشکده‌ی علوم ریاضی
گروه ریاضیات و کاربردها

پایان‌نامه برای دریافت درجه کارشناسی ارشد
در رشته‌ی ریاضی محض گرایش جبر

عنوان:

درباره‌ی تعداد جواب‌های معادله $x^{p^k} = a$ در یک p-گروه متناهی

پژوهشگر:

زهرا شهبازی

ارزیابی و تصویب شده‌ی کمیته داوران پایان‌نامه با درجه‌ی .....

نام و نام خانوادگی	مرتبه‌ی علمی	سمت	امضا
دکتر حسین عبدل‌زاده	استاد راهنما و رئیس کمیته داوران	استادیار	.....
مهندس قادر قاسمی	استاد مشاور	مربی	.....
دکتر احمد یوسفیان‌دارانی	داور	دانشیار	.....

بهمن ۱۳۹۲

نام خانوادگی: شهبازی نام: زهرا

عنوان پایان‌نامه:
درباره‌ی تعداد جواب‌های معادله $x^{p^k} = a$ در یک p–گروه متناهی

استاد راهنما: دکتر حسین عبدل‌زاده
استاد مشاور: مهندس قادر قاسمی

مقطع تحصیلی: کارشناسی ارشد
رشته: ریاضی محض گرایش: جبر
دانشگاه: محقق‌اردبیلی دانشکده: علوم ریاضی
تاریخ دفاع:۹۲/۱۱/۰۷ تعداد صفحات: ۹۰

چکیده

تعیین تعداد جواب‌های معادله‌ای به شکل $x^{p^k} = a$ که در آن a عضوی از گروه مفروض است در مشخص کردن ساختار آن گروه تعیین کننده است. در سال ۱۹۳۱ کولاکف ثابت کرد که در یک p –گروه غیر دوری (p فرد) تعداد جواب‌های $x^{p^k} = 1$ مضربی از p^{k+1} است به شرط آنکه نمای گروه مضربی از p^k باشد. در این پایان نامه با رفع محدودیت $a = 1$ نشان خواهیم داد هرگاه a عضو دلخواهی از گروه باشد در اینصورت تعداد جواب‌های معادله‌ی $x^{p^k} = a$ برای p –گروه غیر دوری که ۲–گروه رده ماکسیمال نیست و نمای آن حداقل $p^k|a|$ است مضربی از p^{k+1} می‌باشد. همچنین در ادامه نشان می‌دهیم که اگر k عددی طبیعی و G یک p–گروه غیر استثنایی باشد بطوریکه نمای G حداقل p^k است آنگاه تعداد جواب‌های معادله‌ی $x^{p^k} = a$ در گروه G مضربی از p^{k+p-1} خواهد بود.

کلیدواژه‌ها: p –گروه، p –گروه استثنایی، p –گروه رده ماکسیمال، p –گروه منتظم

فهرست مطالب

مقدمه

در سرتاسر این پایان‌نامه، p یک عدد اول و G یک pـگروه متناهی فرض شده است. در سال ۱۹۳۱ کولاکف ثابت کرد که در یک pـگروه متناهی غیر دوری G، اگر $exp\, G \geq p^k$ آنگاه تعداد جواب معادله $x^{p^k} = e$ بر p^{k+1} بخش‌پذیر است که در آن k یک عدد صحیح مثبت است.

ما تعداد جواب معادله $x^{p^k} = a$ در گروه G را با $N(a, G, k)$ نشان می‌دهیم که a عضوی از گروه G می‌باشد. نتایجی که بدست می‌آید برای حالت $p = ۲$ نیز برقرار است. فیلیپ هال در سال ۱۹۳۳ تعریف pـگروه منتظم را ارائه کرد و با استفاده از قضیه مشهورش که در همین سال اثبات کرده است، برکوویچ تعریف pـگروه نامنتظم را بیان کرد. در سال ۱۹٦۱ بلکبرن، تعریف pـگروه کاملاً منتظم را بیان کرد. با استفاده از تعاریف بدیهی است که یک pـگروه کاملاً منتظم، منتظم است. اگر G یک pـگروه منتظم و $exp\, \langle x \in G | x^{p^k} = e \rangle \leq p^k$ آنگاه $N(e, G, k) = |\{x \in G | x^{p^k} = e\}| = |\langle x \in G | x^{p^k} = e \rangle|$. بنابراین تعیین $N(e, G, k)$ برای pـگروه‌های نامنتظم دشوار است. فرض کنیم $p = ۲$ بدیهی است که یک ۲ـگروه کاملاً منتظم دوری است ثابت می‌کنیم که یک ۳ـگروه کاملاً منتظم فرا دوری است. طبق اثبات کولاکف، اگر $p > ۲$ و G یک pـگروه غیر دوری باشد و $exp\, G \geq p^k$ آنگاه $N(e, G, k)$ بر p^{k+1} بخش‌پذیر است.

pـگروه G را غیر استثنایی گوییم اگر کاملاً منتظم باشد یا از رده ماکسیمال باشد. بلکبرن در سال ۱۹٦۱ نشان داد که هر pـگروه غیر استثنایی، شامل یک زیرگروه نرمال از مرتبه p^p و نمای p است. طبق نتایجی که برکویچ بدست آورده، اگر ۲ـگروه G غیر استثنایی باشد آنگاه $N(e, G, ۱)$ بر ٤ بخش‌پذیر است. برکویچ در سال ۱۹۷۱ نتیجه فوق را تعمیم داد و در سال ۱۹۷۳ بلکبرن ثابت کرد که اگر G یک pـگروه غیر استثنایی باشد آنگاه $N(e, G, ۱)$ بر p^p بخش‌پذیر است و این بهترین نتیجه ممکن بود.

اگر $a \neq e$ پیدا کردن $N(a, G, k)$ آسان نخواهد بود. لَم در سال ۱۹۸۸ ثابت کرد که اگر $p > ۲$ و

pـگروه G غیر دوری باشد آنگاه $N(a,G,k)$ بر $p^{۲}$ بخش‌پذیر است. لَم در مقاله خود تحت عنوان « تعداد جواب‌های معادله $x^{p^k}=a$ در یک pـگروه » می‌نویسد: " به نظر می‌رسد که در حالت کلی برای هر عضو مرکزی مانند a از مرکز G، تعداد جواب معادله $x^{۲}=a$ در یک ۲ـگروه غیر استثنایی G بر ٤ بخش‌پذیر است، اما من قادر به پیدا کردن اثبات برای این ادعا نیستم."

در این پایان‌نامه ثابت می‌کنیم که حدس لَم درست بوده است و اگر $exp\ G \geq p^k$ آنگاه $N(e,G,k)$ بر $p^{k+۱}$ بخش‌پذیر است و نیز نشان می‌دهیم که در یک pـگروه غیر استثنایی G، اگر $exp\ G \geq p^k$ آنگاه $N(e,G,k)$ بر $p^{k+p-۱}$ بخش‌پذیر است.

از G' به عنوان زیرگروه مشتق G و $\Phi(G)$ زیرگروه فراتینی G استفاده می‌کنیم. اگر A زیرمجموعه‌ای از گروه G باشد آنگاه $C_G(A)$ مرکزساز A در G و $N_G(A)$ نرمال‌ساز A در G خواهد بود و $|\Re|$ تعداد اعضای مجموعه‌ی $\Re$ را نشان می‌دهد.

فصل ۱
مفاهیم اولیه‌ی نظریه‌ی گروه‌ها

در این فصل به طور خلاصه برخی از تعاریف و قضیه‌های اصلی نظریه‌ی گروهها که در فصل‌های بعدی مورد استفاده قرار می‌گیرند را مرور می‌کنیم. علامت های $\mathbb{N}$ ، $\mathbb{Z}$ و $\mathbb{C}$ به ترتیب برای نشان دادن مجموعه‌های اعداد طبیعی، اعداد صحیح و اعداد مختلط به کار خواهیم برد. هرگاه n و m دو عدد صحیح باشند به طوری که m مقسوم‌علیهی از n باشد، خواهیم نوشت $m|n$. همچنین بزرگترین مقسوم‌علیه مشترک دو عدد n و m را با (m,n) نشان خواهیم داد. حلقه اعداد صحیح به پیمانه m را با $\mathbb{Z}_m$ نشان خواهیم داد.به اختصار اعضای این حلقه را با $0, 1, \ldots, m-1$ نمایش می‌دهیم.

۱.۱ مقدمات

قرارداد ۱.۱.۱. در سرتاسر این پایان‌نامه، p یک عدد اول[۱] و G یک p–گروه متناهی[۲] فرض شده است.

تعریف ۲.۱.۱. تعداد اعضای مجموعه متناهی G را مرتبه[۳] گروه G می نامیم و آن را با $|G|$ نشان می دهیم.

تعریف ۳.۱.۱. فرض کنیم G یک گروه باشد. در این صورت مرکز[۴] G که آن را با نماد $Z(G)$ نمایش می دهیم، زیرگروهی[۵] از G است که بصورت زیر تعریف می‌کنیم:

$$Z(G) = \{g \in G | \forall x \in G,\ xg = gx\}. \qquad (۱.۱)$$

از تعریف روشن است که مرکز گروه، یک گروه آبلی است.

تعریف ۴.۱.۱. فرض کنیم G یک گروه باشد. زیرگروه H را مرکزی[۶] گوییم هرگاه $H \leq Z(G)$.

[۱] prime
[۲] finite p-group
[۳] order
[۴] center
[۵] subgroup
[۶] central

تعریف ۱.۱.۵. اگر G یک گروه و H زیرگروه آن باشد، H را زیرگروه سره[۱] از G گوییم اگر $H \neq G$.

تعریف ۱.۱.۶. فرض کنیم G یک گروه و M زیرگروه سره از G باشد. M را زیرگروه ماکسیمال[۲] از G گوییم اگر برای هر زیرگروه H از G، هرگاه $M \leq H \leq G$، آنگاه $H = G$ یا $H = M$.

تعریف ۱.۱.۷. فرض کنیم G یک گروه باشد، زیرگروه نرمال[۳] M از G را یک زیرگروه نرمال ماکسیمال[۴] گوییم هرگاه $M \neq G$، و برای هر زیرگروه نرمال H از G هرگاه $M \leq H$، آنگاه $H = M$ یا $H = G$.

تعریف ۱.۱.۸. فرض کنیم G یک گروه باشد زیرگروه H را نرمال مینیمال[۵] گوییم هرگاه $H \trianglelefteq G$، $H > \{۱\}$ و به ازای هر زیرگروه نرمال N از G که $N < H$ نتیجه بگیریم که $N = \{۱\}$.

تعریف ۱.۱.۹. فرض کنیم G یک گروه باشد، زیرگروه $G' = \langle [u,v] | u, v \in G \rangle$ را زیرگروه مشتق[۶] G می‌نامیم که در آن $[u,v] = u^{-۱}v^{-۱}uv$.

تعریف ۱.۱.۱۰. گروه G را تام[۷] گوییم هرگاه $G = G'$.

تعریف ۱.۱.۱۱. فرض کنیم G یک گروه و $A, B \leq G$. زیرگروه $\langle [a,b] | a \in A, b \in B \rangle$ از G را زیرگروه تعویضگر A و B می‌نامیم و آن را با علامت $[A,B]$ نشان می‌دهیم.

تعریف ۱.۱.۱۲. فرض کنیم G یک گروه و H زیرگروهی از آن باشد. مغز[۸] H عبارت است از زیرگروه نرمال تولید شده با همه‌ی زیرگروه‌های نرمال G که جزء Hاند. مغز H را با $Core_G(H)$ نشان می‌دهیم.

تعریف ۱.۱.۱۳. فرض کنیم S زیرمجموعه‌ای از گروه G، و g عضو ثابتی از G باشد. زیرمجموعه شامل همه‌ی عناصر به فرم $g^{-۱}xg$ $(x \in S)$ را مزدوج S توسط عضو g گوییم، و با نماد $g^{-۱}Sg$ یا S^g نشان می دهیم. به عبارت دیگر، $S^g = \{g^{-۱}xg | x \in S\}$.

[۱] proper
[۲] maximal
[۳] normal
[۴] normal maximal
[۵] normal minimal
[۶] derived
[۷] perfect
[۸] core

تعریف ۱.۱.۱۴. فرض کنیم G_1 و G_2 دو گروه باشند، تابع $\varphi : G_1 \longrightarrow G_2$ را همریختی[۱] گوییم هرگاه برای دو عضو دلخواه a و b از گروه G_1 داشته باشیم $\varphi(ab) = \varphi(a)\varphi(b)$.

تعریف ۱.۱.۱۵. هرگاه تابع $f : G_1 \longrightarrow G_2$ یک همریختی پوشا باشد، آن‌گاه G_2 را تصویر همریخت G_1 می‌نامیم.

تعریف ۱.۱.۱۶. دو گروه G_1 و G_2 را یکریخت[۲] می‌نامیم اگر یک همریختی دوسویی از یکی به دیگری مانند $\varphi : G_1 \longrightarrow G_2$ وجود داشته باشد. در این حالت می‌نویسیم $G_1 \cong G_2$.

تعریف ۱.۱.۱۷. برای گروه G، مجموعه‌ی همه‌ی گروههایی که با G یکریخت هستند را رده‌ی[۳] یکریختی G می‌نامیم.

قضیه ۱.۱.۱۸. فرض کنیم G یک گروه دوری[۴] باشد. در این‌صورت:

الف) اگر G نامتناهی باشد، آن‌گاه G با گروه جمعی[۵] $\mathbb{Z}$ یکریخت است.

ب) اگر G متناهی با n عنصر باشد، آن‌گاه G با گروه جمعی $\mathbb{Z}_n$ یکریخت است.

برهان. الف) فرض کنیم $G = \langle a \rangle$ یک گروه دوری نامتناهی باشد. تابع f را توسط $f(k) = a^k$، برای هر $k \in \mathbb{Z}$ تعریف می‌کنیم. چون $G = \{a^k | k \in \mathbb{Z}\}$، پس f پوشاست. فرض کنیم به ازای $k, j \in \mathbb{Z}$، $f(k) = f(j)$ یعنی $a^k = a^j$. لذا $k = j$. پس f یک به یک است. همچنین برای هر $k, j \in \mathbb{Z}$ داریم:

$$f(k + j) = a^{k+j} = a^k a^j = f(k)f(j) \qquad (۲.۱)$$

در نتیجه $G \cong \mathbb{Z}$.

ب) فرض کنیم $G = \langle a \rangle$ یک گروه دوری n عضوی باشد. در این صورت $G = \{e, a, \ldots, a^{n-1}\}$ که

[۱] homomorphism
[۲] isomorphism
[۳] class
[۴] cyclic
[۵] additive

در آن e عضو همانی G است. تابع $f : \mathbb{Z}_n \longrightarrow G$ را توسط $f([r]) = a^r$، برای هر $[r] \in \mathbb{Z}_n$، تعریف می‌کنیم. f خوش‌تعریف است. چون $\mathbb{Z}_n = \{[۰], [۱], \ldots, [n-۱]\}$ پس f پوشا و لذا دوسویی است. همچنین برای هر $[r], [s] \in \mathbb{Z}_n$ داریم:

$$f([r] + [s]) = f[r + s] = a^{r+s} = a^r a^s = f([r])f([s]) \qquad (۳.۱)$$

در نتیجه $G \cong \mathbb{Z}_n$. □

تعریف ۱.۱.۱۹. اگر یک n–ضلعی منتظم را در یک صفحه در نظر بگیریم، آن‌گاه توسط n دوران حول مرکز n–ضلعی به اندازه $\frac{۲k\pi}{n}$ رادیان، برای هر k که عضوی از مجموعه‌ی $\{۱, ۲, \ldots, n\}$ انتخاب می‌شود، در خلاف جهت عقربه‌های ساعت و n انعکاس نسبت به n محور تقارن n ضلعی می‌توان n–ضلعی را بر خودش منطبق نمود. اگر مجموعه این دورانها و انعکاسها را با $D_{۲n}$ نمایش دهیم، آن‌گاه $D_{۲n}$ با عمل تعریف شده زیر یک گروه است.

" انجام دو عمل دوران یا انعکاس یکی پس از دیگری"

تذکر ۱.۱.۲۰. $D_{۲n}$ با زیر گروهی از گروه جایگشتی S_n یکریخت است و $|D_{۲n}| = ۲n$.

تعریف ۱.۱.۲۱. مجموعه‌ی $Q_۸ = \{\pm۱, \pm i, \pm j, \pm k\}$ با عمل ضرب بصورت $ij = -ji = k$ و

$-۱ = k^۲ = j^۲ = i^۲$ و $jk = -kj = i$ یک گروه از مرتبه‌ی ۸ است که آن را گروه کواترنیون[۱] می‌نامیم. این گروه یک گروه غیر آبلی است به طوری که همه‌ی زیرگروه‌های غیر بدیهی‌اش نرمال هستند.

قضیه ۱.۱.۲۲. هر گروه متناهی از مرتبه‌ی یک عدد اول مانند p دوری است. بنابراین با $\mathbb{Z}_p$ یکریخت است.

برهان. به منبع ($Suzuki$،۱۹۸۰[۲]) مراجعه شود. □

[۱] quaternion group
[۲] Michio Suzuki (1926-1998)

تعریف ۲۳.۱.۱. گروه G را فرادوری[۱] گوییم هرگاه دارای زیرگروه نرمالی مانند N باشد به طوری که N و $\frac{G}{N}$ هر دو دوری باشند.

قضیه ۲٤.۱.۱ (قضیه‌ی لاگرانژ[۲]). اگر G یک گروه متناهی و H زیرگروه G باشد، آنگاه

$$.|G| = |G : H||H|$$

برهان. به منبع ($Suzuki$،۱۹۸۰) مراجعه شود. □

نتیجه ۲۵.۱.۱. مرتبه هر زیر گروه از یک گروه متناهی، مرتبه گروه را می‌شمارد.

تعریف ۲٦.۱.۱. گروه G یک گروه ساده[۳] نامیده می‌شود هرگاه G زیرگروه نرمال غیربدیهی نداشته باشد.

مثال ۲۷.۱.۱. بنا بر قضیه‌ی لاگرانژ، هر گروه از مرتبه‌ی یک عدد اول فقط دارای دو زیرگروه بدیهی است. لذا یک گروه ساده است.

تعریف ۲۸.۱.۱. فرض کنیم H یک زیرگروه از گروه G باشد. نرمال ساز[٤] H در G را به صورت زیر تعریف می‌کنیم:

$$N_G(H) = \{a|a \in G, aH = Ha\} \qquad (٤.١)$$

قضیه ۲۹.۱.۱. اگر H یک زیرگروه از گروه G باشد آنگاه:

الف) $N_G(H)$ بزرگترین زیرگروه G است که H در آن نرمال است.

ب) H یک زیرگروه نرمال G است اگر و فقط اگر $N_G(H) = G$.

[۱] metacyclic
[۲] J.L.Lagrange (1736-1813)
[۳] simple
[٤] normalizer

برهان. فرض کنیم $a, b \in N_G(H)$ در این صورت $aH = Ha$ و $bH = Hb$ پس

$$(ab)H = a(bH) = a(Hb) = (aH)b = (Ha)b = H(ab) \qquad (۵.۱)$$

بنابراین $ab \in N_G(H)$. چون $eH = H = He$ پس $e \in N_G(H)$. اگر $a \in N_G(H)$ در این صورت داریم:

$$aH = Ha \Rightarrow a^{-۱}(aH)a^{-۱} = a^{-۱}(Ha)a^{-۱} \Rightarrow Ha^{-۱} = a^{-۱}H \qquad (۶.۱)$$

پس $a^{-۱} \in N_G(H)$ لذا $N_G(H) \leq G$. اکنون چون،

$$\forall h \in H \quad hH = H = Hh \Longrightarrow h \in N_G(H) \qquad (۷.۱)$$

پس $H \subseteq N_G(H)$. از طرفی طبق تعریف $N_G(H)$ واضح است که H زیرگروه نرمال $N_G(H)$ است. حال اگر K زیرگروه G باشد به طوری که H در آن نرمال است. در این صورت برای هر $k_۱ \in K$ داریم $k_۱H = Hk_۱$ در نتیجه $k_۱ \in N_G(H)$ بنابراین $K \subseteq N_G(H)$، یعنی $N_G(H)$ بزرگترین زیرگروه G است که H در آن نرمال است.

ب)اگر H در G نرمال باشد در این صورت برای هر $a \in G$ ، $aH = Ha$. لذا $a \in N_G(H)$ در نتیجه $G = N_G(H)$.

برعکس، اگر $G = N_G(H)$ آنگاه برای هر $a \in G$ داریم $aH = Ha$ و در نتیجه H یک زیرگروه نرمال G است. □

قضیه ۳۰.۱.۱. اگر H و K زیرگروه‌های گروه G باشند، آنگاه:

الف) $H \leq K \Longrightarrow N_K(H) = N_G(H) \cap K$،

ب) $N_G(H) \cap N_G(K) \leq N_G(H \cap K)$،

ج) $\forall x \in G; \quad N_G(H^x) = (N_G(H))^x$،

د) $H \leq N_G(K) \Longrightarrow HK \leq G$.

برهان. الف) فرض کنیم $x \in N_K(H)$ لذا طبق تعریف نرمال‌ساز داریم: $xH = Hx$ که $x \in K$. چون K زیرگروهی از G است پس $x \in G$ و در نتیجه $x \in N_G(H)$ چون $x \in K$ و $x \in N_G(H)$ لذا $x \in N_G(H) \cap K$ پس $N_K(H) \subseteq N_G(H) \cap K$.

فرض کنیم $x \in N_G(H) \cap K$ پس $x \in K$ و $x \in N_G(H)$ لذا $x \in K$ و برای x از G داریم: $xH = Hx$ بنابراین $x \in N_K(H)$ و در نتیجه $N_G(H) \cap K \subseteq N_K(H)$ لذا برهان کامل می‌شود.

ب) فرض کنیم x عضو دلخواهی از $N_G(H) \cap N_G(K)$ باشد در این صورت $x \in N_G(H)$ و $x \in N_G(K)$ لذا $xH = Hx$ و $xK = Kx$. قرار می‌دهیم $T = H \cap K$. چون x با H و K جابجا می‌شود پس با T نیز جابجا می‌شود. لذا $x(H \cap K) = (H \cap K)x$ در نتیجه $x \in N_G(H \cap K)$. بنابراین $N_G(H) \cap N_G(K) \subseteq N_G(H \cap K)$. بدیهی است که $N_G(H) \cap N_G(K)$ زیرگروه $N_G(H \cap K)$ است زیرا اشتراک دو زیرگروه، زیرگروه است.

ج) به ازای عضو دلخواه g از گروه G داریم:

$$g \in N_G(H^x) \iff (H^x)^g = H^g \tag{۸.۱}$$

$$\iff H^{xg} = H^x \tag{۹.۱}$$

$$\iff H^{xgx^{-1}} = H \tag{۱۰.۱}$$

$$\iff xgx^{-1} \in N_G(H) \tag{۱۱.۱}$$

$$\iff g^{x^{-1}} \in N_G(H) \tag{۱۲.۱}$$

$$\iff g \in N_G(H)^x. \tag{۱۳.۱}$$

د) چون $e = ee \in HK$ پس $HK \neq \varnothing$ از طرفی

$$h_1k_1, h_2k_2 \in HK; \quad (h_1k_1)(h_2k_2) = h_1(k_1h_2)k_2 \tag{۱۴.۱}$$

لذا $h_1(h_2k_1)k_2 = (h_1h_2)(k_1k_2) \in HK$ و همچنین برای hk از HK داریم:

$(hk)^{-1} = (kh)^{-1} = h^{-1}k^{-1} \in HK$. پس HK زیرگروهی از G است. □

تعریف ۳۱.۱.۱. فرض کنیم G یک گروه و H زیرگروهی از آن باشد. مرکزساز[1] H در G را به صورت زیر تعریف می‌کنیم و با نماد $C_G(H)$ نشان می‌دهیم.

$$C_G(H) = \{g \in G | \forall h \in H;\ hg = gh\} \qquad (۱۵.۱)$$

تذکر ۳۲.۱.۱. مرکزساز H در G، زیرگروهی از G است.

قضیه ۳۳.۱.۱. هرگاه H و K زیرگروه‌های گروه G باشند آنگاه

الف) $C_G(H) \leq N_G(H)$

ب) $H \leq K \Longrightarrow C_K(H) = C_G(H) \cap K$

ج) H مرکزی است اگر و فقط اگر گروه G با مرکزساز H در G برابر باشد.

د) H آبلی است اگر و فقط اگر H زیرگروهی از $C_G(H)$ باشد.

برهان. الف) فرض کنیم x عضو دلخواهی از $C_G(H)$ باشد در اینصورت طبق تعریف ۳۱.۱.۱، x عضوی از G است و به ازای عضوی از H مانند h داریم $xh = hx$. چون تساوی فوق به ازای هر عضو از H برقرار است پس $xH = Hx$. لذا $x \in N_G(H)$ و در نتیجه $C_G(H) \subseteq N_G(H)$. بدیهی است که $C_G(H)$ زیرگروهی از $N_G(H)$ است.

ب) برهان این قسمت ساده و مشابه قضیه قبل قسمت (ب) به راحتی با استفاده از تعاریف بدست می‌آید.

ج) فرض کنیم $H \leq Z(G)$ ، به ازای h از H داریم $h \in Z(G)$ بنابراین برای عضوی مانند x از G داریم $hx = xh$ در نتیجه $x \in C_G(H)$. لذا $G \leq C_G(H)$ از طرفی بدیهی است که $C_G(H) \leq G$ بنابراین $G = C_G(H)$. برعکس، فرض کنیم $G = C_G(H)$ لذا بدیهی است که H مرکزی است.

د) فرض کنیم H آبلی باشد و فرض می‌کنیم x عضو دلخواهی از H باشد. چون H زیرگروهی از G

[1] centralizer

است پس x عضوی از G نیز می‌باشد. از طرفی H آبلی است لذا به ازای هر عضو دلخواهی از H مانند y، $xy = yx$ و در نتیجه $x \in C_G(H)$. بنابراین $H \subseteq C_G(H)$. بدیهی است که H زیرگروهی از $C_G(H)$ است. برعکس، فرض کنیم $H \leq C_G(H)$. طبق تعریف مرکزساز بدیهی است که H آبلی است. □

قضیه ۱.۱.۳٤. فرض کنیم G یک گروه باشد در این صورت:

الف) G' یک زیرگروه نرمال G است و $\frac{G}{G'}$ یک گروه آبلی است.

ب) برای هر زیرگروه نرمال H از G، گروه $\frac{G}{H}$ آبلی است اگر و فقط اگر $G' \leq H$.

برهان. به منبع (هانگرفورد،۱۹۸۰) مراجعه شود. □

تعریف ۱.۱.۳۵. فرض کنیم G یک گروه باشد. یک همریختی از G به G را یک درون ریختیِ[۱] G گوییم. مجموعه‌ی همه‌ی درون‌ریختی‌های G را با نماد $End(G)$ نشان می‌دهیم.

تعریف ۱.۱.۳٦. هر یکریختی از گروه G به خود G را یک خودریختی[۲] G می‌نامیم و مجموعه‌ی همه‌ی خودریختی‌های G را با نماد $Aut(G)$ نشان می‌دهیم.

تذکر ۱.۱.۳۷. $Aut(G)$ با عمل ترکیب توابع یک گروه است.

تعریف ۱.۱.۳۸. فرض کنیم G یک گروه بوده و $a \in G$ ثابت باشد. تابعی که هر عضو x از گروه G را به عضو $a^{-1}xa$ از گروه G می‌برد یک خودریختی G است. این خودریختی را خودریختی داخلی[۳] G القا شده با a می‌نامیم و با نماد φ_a نشان می‌دهیم. همچنین مجموعه‌ی همه‌ی خودریختی‌های داخلی G را با $Inn(G)$ نشان می‌دهیم. $Inn(G)$ زیرگروه نرمال $Aut(G)$ است.

قضیه ۱.۱.۳۹. فرض کنیم G یک گروه باشد، گروه خودریختی‌های داخلی G با گروه خارج‌قسمتی $\frac{G}{Z(G)}$ یکریخت است .

[۱] endomorphism
[۲] automorphism
[۳] inner automorphism

برهان. به منبع (جمالی،۱۳۸۰) مراجعه شود. □

نتیجه ۴۰.۱.۱. اگر $Z(G) = \{1\}$، آنگاه $G \cong Inn(G)$.

قضیه ۴۱.۱.۱. فرض کنیم G یک گروه غیر بدیهی از مرتبه‌ی n باشد. در این صورت $|Aut(G)| \leq n^a$ که در آن $a = [\log_2 n]$.

برهان. به منبع (جمالی،۱۳۸۰) مراجعه شود. □

تعریف ۴۲.۱.۱. برای گروه متناهی G، کوچکترین مضرب مشترک مرتبه‌های عضوهای G را نمای[۱] G گوییم و با نماد $\exp G$ نشان می‌دهیم.

تعریف ۴۳.۱.۱. هرگاه R یک حلقه[۲]ی یکدار و جابجایی[۳] باشد آنگاه گروه ضربی $M_n(R)$ (یعنی مجموعه‌ی عناصر وارونپذیر $M_n(R)$ همراه با ضرب ماتریس‌ها) را با $GL(n, R)$ نشان می‌دهیم.

تعریف ۴۴.۱.۱. فرض کنیم R حلقه‌ای جابجایی و یکدار و G یک گروه باشد. یک نمایش ماتریسی G از رتبه‌ی n بر R عبارتست از همریختی گروه‌های به صورت: $\varphi : G \longrightarrow GL(n, R)$.

تعریف ۴۵.۱.۱. فرض کنیم G یک گروه و K یک میدان و V یک Kـفضای برداری از بعد متناهی باشد. همچنین فرض کنیم $T : G \longrightarrow GL(n, R)$ یک نمایش[۴] باشد تابع $\chi : G \longrightarrow K$ با ضابطه $g \longmapsto tr(T(g))$ را یک سرشت[۵] گروه G بر میدان K القا شده توسط نمایش T گوییم.

تعریف ۴۶.۱.۱. فرض کنیم G یک گروه باشد. H را زیرگروهِ مشخِص[۶] G گوییم اگر به ازای هر خودریختی G مانند φ، داشته باشیم $H\varphi = H$ و با $H \; ch \; G$ نشان می‌دهیم.

[۱] exponent
[۲] ring
[۳] commutative
[۴] representation
[۵] character
[۶] characteristic