دانشگاه علم و صنعت ایران

دانشکده ریاضی

گروه‌های جایگشتی با حرکت کراندار

مهدی خیاطی قاسم‌خیلی

پایان نامه برای دریافت درجه دکتری

در رشته ریاضی محض

استاد راهنما: دکتر اکبر حسنی

شهریور ۱۳۷۷

بسم الله الرحمن الرحيم

تقدیم به

استاد فرزانه مرحوم دکتر حسنی

پدر و مادر بزرگوارم

همسر مهربان و فرزندانم هادی و هومان

چکیده

فرض کنیم G یک گروه جایگشتی روی مجموعهٔ Ω با بدون نقطه ثابت روی Ω باشد و فرض کنیم m یک عدد صحیح مثبت باشد. اگر برای هر $\Gamma \subseteq \Omega$ اندازه $|\Gamma^g \setminus \Gamma|$ برای هر $g \in G$ کراندار باشد، آنگاه حرکت Γ را به صورت $\text{move}\,(\Gamma) = \max_{g\in G} |\Gamma^g \setminus \Gamma|$ تعریف می‌کنیم. اگر برای هر $\Gamma \subseteq \Omega$، $\text{move}\,(\Gamma) \leq m$ آنگاه G را با حرکت کراندار گوئیم و حرکت G را $\max_{\Gamma\subseteq\Omega}(\text{move}\,(\Gamma))$ تعریف می‌کنیم. در حالتی که $\text{move}\,(G) = m$، پروفسور Praeger نشان داده است که تعداد Gـمدارها در Ω و طول هر یک از آنها محدود به تابعی بر حسب m است. به ویژه، اگر G روی Ω انتقالی باشد به طوری که G یک ۲ـگروه نباشد و p کوچکترین عدد اول فردی باشد که $|G|$ را عادکند، آنگاه $|\Omega| \leq \lfloor 2mp/(p-1) \rfloor$. برای $p = 3$، کران بالای $|\Omega|$ برابر $3m$ است و همه گروههایی که از درجه ماکسیمال $3m$ هستند، توسط Gardiner، Mann و Praeger رده‌بندی شده‌اند. اینجا ما نشان می‌دهیم که برای $p \geq 5$ گروه‌های از درجه ماکسیمال عبارتند از: (۱) $G = Z_{2^a} \propto Z_p$، $|\Omega| = p$ که در آن برای بعضی $a \geq 1$، $2^a | (p-1)$؛ (۲) $G = P \propto K$، $|\Omega| = 2^s p$ که در آن $1 < 2^s < p$، K یک ۲ـگروه با p مدار از طول 2^s، و $P = Z_p$ بدون نقطه ثابت روی Ω است. (۳) G یک pـگروه است. در این رساله علاوه بر رده‌بندی گروه‌های فوق، کران بالای $|\Omega|$ را در هر گروه با حرکت کراندار بهبود می‌بخشیم، و نهایتاً تعمیمی از گروه‌های با حرکت کراندار را ارائه می‌دهیم.

تقدیر و تشکر

بنام خداوند جـان و خـرد *کزین برتر اندیشه برنگذرد*

سپاس خداوند یکتا را که به من توانایی گام نهادن در راه علم و دانش عطا فرمود. امیدوارم که خداوند متعال همه ما را در راه تعلیم و تعلم که رسالت پیامبران نیز بر آن استوار بوده است، موفق کند. از آنجائیکه موفقیت هر کس حاصل رنج و تلاش عده‌ای از اساتید بزرگوار می‌باشد، این امر در مورد من نیز مستثنی نبوده و در دوران تحصیل از محضر اساتید ارزنده و با ایمان بهره بردم و اینجا برخود واجب می‌دانم که به زحمات همه آنها ارج نهم.

با نهایت احترام و فروتنی از زحمات بی‌دریغ و راهنماییهای ارزشمند استاد فرزانه مرحوم دکتر اکبر حسنی در دورهٔ دکترا و تدوین این رساله که همواره شامل حال من بوده است، سپاسگزاری می‌کنم و از خداوند متعال طلب آمرزش و آرزوی سعادت اخروی برای آن بزرگوار می‌نمایم. همچنین از جناب آقای دکتر تولائی به خاطر راهنماییهای دلسوزانه و زحمات بی‌دریغ‌شان در تدوین و ارائه این رساله کمال تشکر را دارم.

برخود لازم می‌دانم که از مدیر تحصیلات تکمیلی دانشکده جناب آقای دکتر مالک نژاد به دلیل مدیریت دلسوزانه و قوی ایشان که همواره با نظرات ارزشمند خویش ما را بهره‌مند نموده‌اند و در حل مشکلات دورهٔ دکترا از هیچ کمکی دریغ نکرده‌اند، تشکر و قدردانی نمایم. از سرکار خانم دکتر جذبی ریاست محترم دانشکدهٔ ریاضی به دلیل همکاری فراوان در برگزاری جلسه دفاعیه و داوری این رساله تشکر می‌کنم. همچنین از اساتید مدعو جناب آقای دکتر درفشه استاد دانشگاه تهران بخاطر تنظیم و داوری این رساله و شرکت در جلسه دفاعیه و آقای دکتر ذکایی استاد دانشگاه خواجه نصیر بخاطر شرکت در جلسه دفاعیه و داوری این رساله کمال امتنان و سپاسگزاری خود را ابراز می‌دارم. از کلیه اساتید و کارمندان دانشکده ریاضی به ویژه سرکار خانم یوسفی مسئول دفتر تحصیلات تکمیلی و همچنین از کلیه دوستان و دانشجویان مقاطع دکترا و کارشناسی ارشد که همواره مشوق من بودند و در جلسه دفاعیه شرکت نموده‌اند سپاسگزارم. در پایان از سیاست گذاری صحیح مسئولین محترم دانشگاه که موجب تسریع و پیشرفت کار اینجانب گردید کمال تشکر را دارم.

خدایا چنان کن سرانـجام کـار *تو خشنود باشی و ما رسـتگار*

فهرست مطالب

پیشگفتار

فرض کنیم G یک گروه جایگشتی روی مجموعهٔ Ω با بدون نقطهٔ ثابت‌بوده، و فرض کنیم m یک عدد صحیح مثبت باشد. برای یک زیر مجموعهٔ Γ از Ω، اگر برای هر $g \in G$ اندازه‌های $|\Gamma^g \setminus \Gamma|$ متناهی و کراندار باشند، آنگاه حرکت (movement) Γ را به صورت زیر تعریف می‌کنیم و آنرا با نماد $\text{move}\ (\Gamma)$ نشان می‌دهیم.

$$\text{move}\ (\Gamma) := \max_{g \in G} |\Gamma^g \backslash \Gamma|$$

بعلاوه Γ را با *تحدید حرکت* (restricted movement) گوئیم هر گاه $\text{move}\ (\Gamma) < |\Gamma|$. اگر برای هر زیر مجموعهٔ Γ از Ω داشته باشیم $\text{move}\ (\Gamma) \leq m$، آنگاه گروه G را دارای حرکت کراندار (bounded movement) گوئیم و حرکت G را ماکزیمم $\text{move}\ (\Gamma)$ روی همه زیر مجموعه‌های Γ از Ω تعریف می‌کنیم. به عبارت دیگر می‌توان نوشت:

$$\text{move}\ (G) := \max_{\Gamma \subseteq \Omega} (\text{move}\ (\Gamma))$$

یکی از اهداف مهم این رساله رده بندی (classification) همه گروه‌های جایگشتی انتقالی از درجهٔ $\lfloor 2mp/(p-1) \rfloor$ است که در آن G دارای حرکت کراندار مساوی با m است و G یک ۲ـگروه نیست و همچنین p کوچکترین عدد اول فردی است که $|G|$ عاد می‌کند. (برای هر عدد حقیقی x، $\lfloor x \rfloor$ یعنی بزرگترین عدد صحیح کوچکتر از x.)

بررسی رده‌بندی گروههای با شرایط فوق، پاسخ به سوال زیر می‌باشد که این سوال به عنوان مسئله ۳ توسط پروفسور Praeger در [۲۸] مطرح گردید.

مسئله. فرض کنیم m یک عدد صحیح مثبت و p یک عدد اول باشد. در این صورت همهٔ گروههای جایگشتی انتقالی مانند G روی یک مجموعهٔ Ω با درجه $\lfloor 2mp/(p-1) \rfloor$ را پیدا کنید که در آن G دارای حرکت کراندار مساوی با m است و p کوچکترین عدد اول فردی است که $|G|$ را عاد می‌کند.

مرور تاریخی

در این قسمت یک مرور تاریخی از بررسی‌هایی که بر روی گروههای جایگشتی با حرکت کراندار شده است، خواهیم داشت و نحوهٔ پیدایش تعاریف در این چنین گروهها را مورد مطالعه قرار می‌دهیم. فرض کنیم G یک گروه جایگشتی روی مجموعهٔ Ω باشد، و فرض کنیم Γ و Δ (که لزوما متمایز نیستند) زیر مجموعه‌هایی از Ω باشند. می‌توان سوال کرد که تحت چه شرایطی روی گروه، یا روی زیر مجموعه‌های Γ و Δ ممکن است که Γ از Δ بوسیلهٔ یک عنصر از G جدا (separate) شوند؟ یعنی برای بعضی از عناصر $g \in G$ داشته باشیم $\Gamma^g \cap \Delta = \emptyset$. در سال ۱۹۷۶ میلادی، P. M. Neumann در قضیهٔ ۳.۲ از [۲۵] ثابت کرد که اگر همهٔ مدارهای G در Ω نامتناهی باشند، آنگاه هر زیر مجموعهٔ متناهی از Ω می‌تواند تحت اثر عضوی از G از خودش جدا شود. ما از این نتیجهٔ مهم به عنوان قضیهٔ جداسازی (separation theorem) نام خواهیم برد و آن را چنین بیان می‌کنیم.

قضیه (قضیه جداسازی) اگر G یک گروه جایگشتی روی مجموعهٔ Ω باشد به طوری که همه مدارهای آن در Ω نامتناهی باشند، آنگاه برای هر زیر مجموعهٔ متناهی Γ از Ω عضوی مانند $g \in G$ وجود دارد به طوری که $\Gamma^g \cap \Gamma = \emptyset$ (در نتیجه $|\Gamma| = $ move (Γ)).

در [۲۵] نشان داده شده است که این نتیجهٔ اساسی در گروههای جایگشتی معادل با یک نتیجهٔ قدیمی از B. H. Neumann ، (لم ۱.۴ از [۲۴]) است که آن نتیجه دربارهٔ پوشش یک گروه بوسیلهٔ تعداد متناهی از همدسته‌های زیر گروههای سرهٔ آن می‌باشد.
پس اگر یک زیر مجموعه متناهی مانند Γ از Ω چنان موجود باشد که move $(\Gamma) < |\Gamma|$ ، آنگاه G دارای حداقل یک مدار متناهی است و این نیز از قضیهٔ جداسازی ناشی می‌شود و معمولاً در این گونه مسایل، قضیه جداسازی را باید بکار گرفت. همچنین این سوال را می‌توان مطرح کرد که در این حالت، طول این مدار متناهی چیست؟ آیا اندازهٔ آن به اندازهٔ مجموعهٔ متناهی Γ بستگی دارد؟ آیا برای حالتی که Γ نامتناهی است، ادعای مشابهی ممکن است؟ پاسخ به این گونه از سوالات باعث می‌شود که تعمیمی از قضیهٔ جداسازی حاصل گردد.

همچنین در سال ۱۹۷۶ میلادی یک نتیجه که ما آن را به عنوان یک کاربرد از قضیهٔ جداسازی تلقی می‌کنیم، توسط B. J. Birch ، R. G. Burns ، S. O. Macdonald و P. M. Neumann ارائه گردید که در آن نتیجه، یک کران بالا برای مدارهای متناهی G بر حسب اندازهٔ متناهی Γ بدست می‌آید. اینک به بیان این نتیجهٔ مهم می‌پردازیم و در رساله از آن به عنوان قضیهٔ BBMN یاد خواهیم کرد.

قضیهٔ BBMN . [قضیهٔ ۱،۲] فرض کنیم G یک گروه جایگشتی روی مجموعهٔ Ω و همچنین فرض کنیم که زیر مجموعه‌هایی مانند Δ و Γ از Ω چنان موجود باشند به طوری که برای هر g از G داشته باشیم $\Gamma^g \cap \Delta \neq \emptyset$. در این صورت یک $G-$مدار در Ω از طول حداکثر $|\Gamma||\Delta|$ وجود دارد. به ویژه، اگر $\mathrm{move}\ (\Gamma) < |\Gamma|$ آنگاه بعضی از مدارهای G در Ω دارای طول حداکثر $|\Gamma|^2$ هستند.

همان طوری که ملاحظه می‌شود، قضیهٔ فوق اطلاعات دقیق تری از قضیهٔ جداسازی به ما می‌دهد و قضیهٔ جداسازی نیز می‌تواند از این قضیه بدست آید (زیرا عدد بدست آمده برای حد اکثر مقدار طول مدار نشان دهندهٔ وجود یک مدار متناهی است). اما همانطوری که در [۲۸] اشاره گردید، تا کنون هیچ گونه اثبات مستقیمی برای این قضیه ارائه نشد، مگر آن که از قضیهٔ جداسازی استفاده شده باشد. لازم به تذکر است که این مطلب اخیر بعنوان سوال ۱ در [۲۸] چنین مطرح شده است که آیا اثباتی برای قضیهٔ فوق وجود دارد که از قضیهٔ جداسازی استفاده نشود؟

یکی دیگر از کاربردهای قضیهٔ جداسازی، در گروههای جایگشتی با حرکت کراندار است و به طور کلی می‌توان گفت که قضیهٔ جداسازی اساس تشکیل گروههای با حرکت کراندار است. با توجه به تعریف حرکت در گروههای جایگشتی ، ملاحظه می‌شود که این شرط یک محدودیت قوی روی گروهها اعمال می‌کند و لذا این طبیعی است که بپرسیم چه گروههای جایگشتی دارای حرکت کراندارند؟ پروفسور Praeger در [۲۷] و [۲۸] بیان می‌کند که این سوال برای اولین بار توسط Carlo Casolo در سال ۱۹۸۹ میلادی در طی یک گفتگو که بین آنها جریان داشت، مطرح گردید. بعد از مطرح شدن سوال، کار توسط Praeger دنبال گردید و بعد از یک سال از طرح سوال، کارهای جالبی توسط ایشان در [۲۷] بیان شد. به ویژه ثابت کرد که شرط با حرکت کراندار بودن باعث می‌شود که Ω متناهی باشد. در ادامهٔ کار، افرادی نیز بطور مشترک با ایشان مقاله‌هایی ارائه کردند که نتایج خوبی را در بر داشت. بعلاوه سعی گردید که کران بدست آمده برای $|\Omega|$ را در هر مرحله کاهش دهند. ما نیز در این رساله کار در مورد گروههای جایگشتی با حرکت کراندار را ادامه دادیم و ضمن رده بندی این چنین گروههابا درجه خاص، سعی در بهبود کران بالا برای $|\Omega|$ خواهیم داشت.

نتایج و ساختارهای رساله

این رساله به صورت زیر مرتب شده است. در فصل اول به جمع آوری بعضی تعاریف و نتایج مقدماتی پرداختیم که همهٔ آنها کراراً در فصل‌های بعد مورد استفاده قرار خواهند گرفت و سعی کردیم از نمادهایی استفاده کنیم که در کتاب‌های معروف نظریهٔ گروهها معمول است. در فصل دوم با توجه

به تعاریف حرکت یک زیر مجموعه از Ω و حرکت یک گروه جایگشتی G روی مجموعهٔ Ω ابتدا نتایج اساسی و اولیه از گروههای جایگشتی با حرکت کراندار را ارائه کردیم و سپس با بیان مثال‌هایی از گروههای جایگشتی انتقالی و با حرکت کراندار، کران بالای بدست آمده برای $|\Omega|$ را کمی بهبود بخشیدیم. یعنی با اعمال شرایطی خاص بر روی گروهها، کران بالای $|\Omega|$ را کاهش می‌دهیم. در فصل سوم ابتدا فرض کردیم که عمل G روی Ω غیر انتقالی باشد، در این صورت نتایجی را برای گروه‌های با حرکت کراندار بدست آوردیم. در بخشهای بعدی این فصل بحث را در مورد گروه‌های جایگشتی انتقالی اختصاص دادیم. یکی از نتیجهٔ اساسی که در فصل سوم بدست آمده است، این است که اگر G یک گروه جایگشتی انتقالی و دارای حرکت کراندار مساوی با m باشد، آنگاه $|\Omega| \leq ۳m$. در این فصل ضمن ارائهٔ مثال‌هایی از گروه‌های با حرکت کراندار از درجهٔ $۳m$، به رده بندی این دسته از گروهها می‌پردازیم. یعنی تمام گروه‌های انتقالی از درجهٔ $۳m$ که دارای حرکت کراندار مساوی با m هستند را رده‌بندی می‌کنیم. بیشتر مطالب و نتایجی را که در فصل‌های دوم و سوم آمده است می‌توانید در [۳]، [۶]، [۸]، [۲۱]، [۲۳]، [۲۷]، [۲۸] و [۲۹] ملاحظه کنید.

در فصل چهارم فرض کردیم که G یک گروه جایگشتی انتقالی و با حرکت کراندار مساوی با m، روی مجموعه Ω باشد به طوری که p کوچکترین عدد اول فردی است که مرتبه G را عاد می‌کند و G یک ۲ـگروه نیست. در این صورت در فصل دوم نشان داده شده است که $|\Omega| \leq \lfloor ۲mp/(p-۱) \rfloor$. ابتدا نتایج فصل دوم را برای این کران جدید $|\Omega|$ تعمیم داده‌ایم و سپس مثال‌هایی از گروه‌های جایگشتی انتقالی و با حرکت کراندار مساوی با m که از درجهٔ $\lfloor ۲mp/(p-۱) \rfloor$ هستند را ارائه کردیم، که در آن $p \geq ۵$ کوچکترین عدد اول فردی است که مرتبهٔ گروه را عاد می‌کند. با تکمیل نتایج مهم و ضروری در فصل چهارم، سپس در فصل پنجم به رده‌بندی این خانواده از گروهها پرداختیم و نتایج جالبی نیز بدست آورده‌ایم. مطالبی که در فصل‌های چهارم و پنجم ارائه شد، تعمیمی از کارهای Gardiner و Li و Mann و Praeger است که در بالا به آنها اشاره شد. مطالب این دو فصل را می‌توان در [۸] و [۱۰] ملاحظه کرد. خلاصه اینکه در فصل پایانی این رساله یعنی فصل ششم دو بخش مهم داریم. بخش اول این فصل را به تعمیم نتیجه‌ای از [۲۹] اختصاص داده‌ایم که آن را می‌توان در [۹] ملاحظه کرد و بخش دوم این فصل نیز شامل نتایج جالبی است که در حالت کلی، کران بالای $|\Omega|$ را که در فصل ۳ ارائه شد، برای گروه‌های جایگشتی با حرکت کراندار کاهش می‌دهد و قسمتی از آن را می‌توان در [۱۷] دید.

فصل ۱

تعاریف و نتایج مقدماتی

در این فصل بعضی از تعاریف را جمع‌آوری کرده و سپس به بیان نتایج مقدماتی می‌پردازیم. سعی شده است که از منابع معروف نظریه گروه‌ها و از مراجع قابل دسترس استفاده شود. لازم به تذکر است که این فصل شامل مطالبی است که مورد استفادهٔ این رساله می‌باشد. این فصل باتوجه به وابستگی مطالب در سه بخش مجزای گروه‌های مجرد، گروه‌های جایگشتی و نظریه اعداد تنظیم گردیده است.

۱.۱ نظریهٔ گروه‌ها

همهٔ گروه‌هایی که در این رساله مورد استفاده قرار می‌گیرند، متناهی هستند. نمادها و اصطلاحات مورد استفاده در این رساله، همگی معمول و استاندارد در نظریهٔ گروه‌ها می‌باشند و بیشتر آنها را می‌توان در [۴]، [۵]، [۳۰]، [۳۱]، [۳۳] و [۳۷] ملاحظه کرد.

یک گروه را ساده (simple) گوئیم اگر و فقط اگر جز زیر گروه همانی و خودش زیر گروه نرمال دیگری نداشته باشد. به طور مشابه، اگر N یک زیر گروه از یک گروه G باشد به طوری که برای هر اتومورفیسم $\alpha \in Aut(G)$ و هر $x \in N$ داشته باشیم $x^{\alpha} \in N$، آنگاه N را یک زیر گروه مشخصه (characteristic subgroup) از G گوئیم و آن را با نماد $N\text{char}\ G$ نشان می‌دهیم. اگر گروه G جز زیر گروه همانی و خودش هیچ زیر گروه مشخصهٔ دیگری نداشته باشد، آنگاه G را مشخصاً ساده (characteristically simple) گوئیم. اینک لم‌های زیر را در مورد

زیر گروه‌های مشخصه و گروه‌های مشخصاً ساده داریم.

۱.۱.۱. لم. فرض کنیم N، G و M سه گروه باشند به طوری که $M \text{char } G$ و G نرمال در N است. در این صورت M در N نیز نرمال است.

برهان. فرض کنیم M در G مشخصه باشد. در این صورت بنابه تعریف، برای هر $m \in M$ و هر $\alpha \in Aut(G)$ داریم $m^\alpha \in M$. همچنین، چون G نرمال در N است، لذا بنا به تعریف برای هر $g \in G$ و هر $n \in N$ داریم $n^{-1}gn \in G$. بدیهی است که نگاشت $\beta : g \longmapsto n^{-1}gn$ یک اتومورفیسم از G است. بنابراین $\beta \in Aut(G)$ و در نتیجه برای هر $m \in M$ و هر $n \in N$ داریم $m^\beta = n^{-1}mn \in M$ (زیرا از مشخصه بودن m داریم که m تحت هر اتومورفیسم G پایاست). پس M نرمال در N می‌باشد.□

۲.۱.۱. لم. فرض کنیم N یک زیر گروه نرمال مینیمال از یک گروه G باشد. در این صورت N مشخصاً ساده است.

برهان. فرض کنیم که N یک زیر گروه نرمال مینیمال از یک گروه G باشد به طوری که مشخصاً ساده نباشد. در این صورت N شامل یک زیر گروه مشخصهٔ سره و غیر بدیهی است، که در نتیجه بنا به لم فوق، نرمال در G می‌باشد و این با نرمال مینیمال بودن N در G تناقض دارد.□

فرض کنیم Π مجموعهٔ بعضی از اعداد اول بوده و Π' متمم (complement) Π نسبت به همهٔ اعداد اول باشد. یک گروه G را $\Pi-$ گروه نامیم اگر همهٔ اعداد اولی که $|G|$ را عاد می‌کنند در Π باشند. اگر $\Pi = \{p\}$، آنگاه Π' را به صورت p' نیز نمایش می‌دهیم. یک زیر گروه H از G را $\Pi-$زیر گروه هال گوئیم، هرگاه H یک $\Pi-$گروه باشد و $(|G|/|H|, |H|) = 1$. اگر $\Pi = \{p\}$، آنگاه یک Π زیر گروه هال را یک $p-$زیر گروه سیلو نیز می‌نامیم. اینک قضایای معروف هال و سیلو را در زیر بیان می‌کنیم.

۳.۱.۱. قضیه (قضایای سیلو). فرض کنیم G یک گروه متناهی و p یک عدد اول باشد که $|G|$ را عاد کند. در این صورت یک $p-$زیر گروه سیلو از G وجود دارد. هر دو $p-$زیر گروه سیلو در G مزدوجند. هر $p-$زیر گروه از G مشمول در یک $p-$زیر گروه سیلو است.□

۴.۱.۱. قضیه (قضیه هال). فرض کنیم G یک گروه حل پذیر متناهی باشد و Π یک مجموعه از اعداد اولی باشد که $|G|$ را عاد می‌کنند. در این صورت یک Π−زیر گروه هال وجود دارد. هر دو Π−زیر گروه هال در G مزدوجند. هر Π−زیر گروه مشمول در یک Π−زیر گروه هال است.$\square$

فرض کنیم X یک زیر مجموعه از یک زیر گروه G باشد. در این صورت زیر گروه تولید شده توسط X را بصورت $< X >$ نمایش می‌دهیم و عبارت است از اشتراک همهٔ زیرگروه‌های شامل X. اگر x و y دو عضو دلخواه از G باشند، آنگاه جابجاگر (commutator) $[x, y]$ را بصورت $x^{-1}y^{-1}xy$ تعریف می‌کنیم. حال فرض کنیم که Y, X دو زیر مجموعه از G باشند. در این صورت

$$[X, Y] =< [x, y]; x \in X, y \in Y >$$

به طوری که دیده می‌شود، $[X, Y]$ همیشه یک زیر گروه از G است. به ویژه $G' = [G, G]$ نیز یک زیر گروه از G هست و آن را زیر گروه مشتق G می‌نامیم. همواره داریم $G' \text{char } G$. اگر H یک زیر مجموعه از گروه G باشد و $x \in G$، آنگاه زیر مجموعهٔ $x^{-1}Hx$ را بصورت H^x و برای هر $x \in G$، زیر گروه تولید شده توسط H^x را به صورت H^G نمایش می‌دهیم. به‌وضوح H^G یک زیر گروه نرمال در G است و آن را بستار نرمال (normal closure) H در G می‌نامیم.

۵.۱.۱. لم. (قضیه۲.۱از [۵]) فرض کنیم x، y و z عناصری از یک گروه G باشند. در این صورت داریم:

$$\begin{aligned} i)\quad & [xy, z] = [x, z]^y[y, z] \\ ii)\quad & [x, yz] = [x, z][x, y]^z \square \end{aligned}$$

۶.۱.۱. لم. (لم۲.۲ از [۵]) فرض کنیم y و z دو عضو دلخواه از یک گروه G باشند و همچنین فرض کنیم $z := [x, y]$ با هر دو عضو y, x جابجا شود. در این صورت داریم:

$$\begin{aligned} i)\quad & [x^i, y^j] = z^{ij} && (\text{برای هر } i \text{ و } j) \\ ii)\quad & (yx)^i = z^{\frac{1}{2}i(i-1)}y^ix^i && (\text{برای هر } i) \end{aligned}$$

۷.۱.۱. تعریف. گروه $G =< x, y;\ x^n = y^2 = 1, y^{-1}xy = x^{-1} >$ را گروه دو وجهی D_{2n} (Dihedral group) از مرتبهٔ $2n$ نامیم. اگر زیر گروه دوری تولید شده بوسیلهٔ x را با Z_n و زیر گروه تولید شده به وسیلهٔ y را با Z_2 نمایش دهیم، آنگاه به آسانی می‌توان نتیجه گرفت که $D_{2n} \cong Z_2 \propto Z_n$.$\square$

۸.۱.۱. تعریف. مجموعهٔ تمام ماتریس‌های معکوس‌پذیر $n \times n$ روی میدان متناهی F با q عنصر (که در آن q توانی از عدد اول p می‌باشد) یک گروه ضربی است که آن را گروه خطی عمومی (General linear group) نامیده و با نماد $GL(n,q)$ نشان می‌دهیم.□

۹.۱.۱. لم. فرض کنیم n یک عدد صحیح مثبت و q توانی از یک عدد اول مانند p باشد. در این صورت

$$\begin{aligned} |GL(n,q)| &= \Pi_{k=۱}^{n}(q^n - q^{k-۱}) \\ &= q^{n(n-۱)/۲}(q^n-۱)(q^{n-۱}-۱)\ldots(q-۱)\text{.} \quad \square \end{aligned}$$

۱۰.۱.۱. تعریف. فرض کنیم F یک میدان متناهی با q عنصر باشد که در آن $q = p^n$ و p یک عدداول است. برای هر عضو مخالف صفر a و هر عضو b از F، نگاشت

$$f_{a,b} : F \longrightarrow F$$

را با ضابطه $f_{a,b}(x) = ax + b$ $(x \in F)$ در نظر می‌گیریم. نگاشت $f_{a,b}$ را تبدیل آفین (Affine transformation) می‌نامیم. از

$$f_{a,b}(x) = f_{a,b}(y) \Leftrightarrow xa = ya \Leftrightarrow x = y$$

نتیجه می‌گیریم که $f_{a,b}$ یک جایگشت از F هست. حال اگر $f_{a,b} = f_{a',b'}$، آنگاه

$$a = f_{a,b}(۱) - b = f_{a',b'}(۱) - b' = a'$$

و

$$b = f_{a,b}(\circ) = f_{a',b'}(\circ) = b'$$

مجموعهٔ همهٔ تبدیلات آفین از F تشکیل یک زیر گروه از $Sym(F)$ می‌دهند که آن را گروه ۱ـبعدی آفین روی میدان F می‌نامیم و با علامت $AGL(۱,q)$ نمایش می‌دهیم و $|AGL(۱,q)| = q(q-۱)$.□

در ادامه، به بیان یک تعریف و چند قضیه دربارهٔ زیر گروه هیوز (Hughes) می‌پردازیم. البته متذکر می‌شویم که بحث اصلی در مورد این زیر گروه را، در بخش ۴.۵ ارائه خواهیم کرد.