آشنایی با

نظریه گروهها

والتر لدرمن

ترجمهٔ محمدحسن بیژن‌زاده

آشنایی با

نظریه گروهها

والتر لدرمن

ترجمهٔ محمدحسن بیژن‌زاده

مرکز نشر دانشگاهی، تهران

ریاضی، آمار، و کامپیوتر
۴۴

مرکز نشردانشگاهی
۴۰۹

Introduction to Group Theory
Walter Ledermann
Oliver & Boyd, 1973

آشنایی با نظریه گروهها
تألیف والتر لدرمن
ترجمهٔ دکتر محمدحسن بیژن‌زاده
ویراستهٔ دکتر محمدهادی شفیعیها
مرکز نشر دانشگاهی، تهران
چاپ اول ۱۳۶۷
تعداد ۵۰۰۰
حروفچینی: عبدی
لیتوگرافی: کیان
چاپ و صحافی: سایه

لدرمن، والتر، ۱۹۱۱ -   Ledermann, Walter, 1911-
آشنایی با نظریه گروهها
عنوان اصلی: Introduction to group theory
واژه‌نامه: ص.
کتابنامه: ص.
۱. نظریه گروهها. الف. بیژن‌زاده، محمدحسن،   ، مترجم. ب. مرکز نشر دانشگاهی. ج. عنوان.
QA۱۷۱   ۵۱۲/۲۲

بسم الله الرحمن الرحیم

فهرست

عنوان	صفحه

عنوان	صفحه

پیشگفتار

درطی این بیست و پنج سالی که ازآغاز نخستین چاپ کتاب آشنایی با نظریهٔ گروههای متناهی من می گذرد، آموزش نظریهٔ گروهها بسیار تنوع و توسعه یافته است: اکنون همهٔ دانشجویان رشتهٔ ریاضی در دورهٔ لیسانس این موضوع را مطالعه می کنند، و مفاهیم بنیادی آن بخشی ازآموزش معلمان در دانشکده‌های تربیتی را تشکیل می‌دهد. درخلال این مدت، نظریهٔ گروهها در ریز مواد درسی مدارس جدید وارد شده است، و معمولاً یکی از عمومی‌ترین دروس به‌شمارمی‌آید. به‌سبب این علاقه‌مندی گسترده و پویا نسبت به‌گروهها، شگفت‌آور نیست اگر علائم پیری، که با یك تجدید نظر به‌آسانی مرتفع نمی‌گردد، در این متن ظاهر شده باشد.

لذا با کتاب آشنایی با نظریهٔ گروههای فعلی گام تازه‌ای برداشته شده است: نظام اصطلاحات و نمادها روزآمد شده‌اند، تأکیدکمتری برگروههای متناهی (همچنان که از عنوان کتاب برمی‌آید) شده است؛ و تعدادی مباحث اضافی از قبیل سریهای مرکزی و گروههای پوچتوان، به اختصار به‌آن افزوده شده‌اند. علی‌رغم این تغییرات سعی کرده‌ام تا ماهیت مقدماتی بودن کتاب پیشین را حفظ کنم. فصلهای نخستین کتاب برای آن دسته از دانش‌آموزان سال آخر دبیرستان که فکری کاوشگر دارند باید قابل درك باشد؛ بعلاوه کل کتاب بدین نیت فراهم آمده است تاهمهٔ مباحث نظریهٔ گروهها یك دورهٔ عالی‌را فراگیرد. همانند پیش، برای‌رسیدن به‌یك‌هدف خاص، درصورت یافتن راهی‌آموزنده‌تر و پرثمرتر، آن‌را همواره برراه‌کوتاهترترجیح داده‌ام. درصفحهٔ ۱۹۵ کتابهای پرمحتواتر وپیشرفته‌تری را ذکرکرده‌ام، که امیدوارم،خواننده برای مطالعهٔ عمیقتر نظریهٔ گروهها به‌آنها رجوع کند.

درطول این‌سالها، پیشنهادات و انتقادات بسیاری در باب کتاب قبلی دریافت داشته‌ام. همهٔ این‌تذکرات مفید بوده‌اند،و درهرجا که امکان داشته،دراین مجلد به‌آنها ترتیب اثرداده شده است. ولی، باید از پروفسور ج. آ. گرین تشکرمخصوصی بنمایم. ایشان‌نسخهٔ ماشین‌شدهٔ کتاب را با دقت زیاد مطالعه کرده و توصیه‌های ارزنده‌ای برایم ارسال داشته است که حاکی از تسلط کامل و آزمودگی ایشان در این زمینه است.

بالاخره، مایلم از ناشرین‌کتاب به‌خاطر لطف و همکاریهای صمیمانه‌شان تشکرکنم.

والتر لدرمن

۱

مفاهیم مربوط به گروهها

۱. مقدمه. اعمال اصلی حساب مشتمل‌اند بر ترکیب دوعدد a و b برطبق قواعدی کاملاً مشخص، برای به‌دست دادن عدد منحصر به‌فردی چون c. برای مثال، اگر **قانون ترکیب**، ضرب باشد، باید داشته باشیم $c = ab$. هروقت‌که a و b داده شده باشند عدد c قابل محاسبه است.

معلوم است‌که ضرب دو یا چند عدد، از قوانین صوری مشخصی پیروی می‌کندکه برای همهٔ حاصلضربها، صرفنظر از مقدار عددیشان، معتبرند؛ ازجمله:

$$ab = ba \qquad \text{(قانون تعویضپذیری)} \qquad (۱.۱)$$

$$(ab)c = a(bc) \qquad \text{(قانون شرکتپذیری)} \qquad (۲.۱)$$

$$۱a = a۱ = a \qquad (۳.۱)$$

ازمعادلهٔ آخر برای معرفی عدد خاصی به‌نام واحد استفاده می‌شود. دومین قانون، به‌طور روشنتر، حاکی است‌که هرگاه داشته باشیم $ab = s$ و $bc = t$، آنگاه تساوی $sc = at$ همواره درست است.

در بررسی اصل موضوعی حساب مرسوم است‌که مطلب را با وضع اصول موضوعه یا بنداشتهایی نظیر (۱.۱)، (۲.۱)، و(۳.۱) وچندین اصل معین‌دیگرکه با جمع ویاضرب سروکار دارند شروع می‌کنند، وسپس‌نتایج منطقی این‌اصول موضوع را به‌دست می‌آورند.

در وهلهٔ اول، این مطلب که نمادهای a، b، . . . برطبق معمول معرف اعداد یا ذوات ریاضی دیگری باشند و یا اصولاً تعبیری ملموس داشته باشند، برای ما مطرح نیست. دستگاههای اصل موضوعی زیادی ممکن است منطقاً وجود داشته باشند اما همهٔ آنها به‌یك میزان جالب یا مهم نیستند. تنوع و عمق کاربردهای یك دستگاه بنداشت متصور در ریاضیات محض و کاربردی است که موجب برتری آن بردیگری می‌شود.

۲. بنداشتهای نظریهٔ گروهها. نظریهٔ مجرد گروهها با مجموعه‌ای متناهی یا نامتناهی از عناصر، چون

$$G: a, b, c, \ldots$$

سروکار دارد که درآن تنهـا یك قانون ترکیب تعریف می‌شود. مطابق قرارداد، برای بیان این قانون ترکیب، از نمادگذاری و اصطلاح ضرب استفاده می‌شود. ازاین‌رو می‌پذیریم که هر دوعنصر a و b از G، چه مساوی وچه نامساوی، دارای‌یك حاصلضرب منحصر به‌فرد، چون c باشند و می‌نویسیم

$$ab = c$$

به‌بیان رسمی‌تر گفته می‌شود که به‌هر زوج مرتب (a, b) ازعناصر، یك عنصر منحصر به‌فرد چون c مربوط می‌گردد؛ اصطلاح زوج مرتب بدین معنی است که وقتی $a \neq b$، باید بین زوجهـای (a, b) و (b, a) تفاوت قایل شویم. یك ویژگی اساسی هرگروه این است که حاصلضرب هر دوعنصر آن مجدداً عنصری ازخود گروه است؛ یا به زبان فنی‌تر، گروه نسبت به‌ضرب بسته است. نوع ضربی که در گروهها به‌کار گرفته می‌شود باید از بنداشتهای معینی پیروی کند؛ این بنداشتها درتعریف زیر آمده‌اند.

تعریف ۱: مجموعه‌ای چون G که درآن یك قانون ترکیب («ضرب») تعریف شده است، درصورتی یك گروه تشکیل می‌دهد که درشرایط زیر صدق کند:

I. **قانون بستاری:** به هر زوج مرتب (a, b) از G عنصر منحصر به‌فردی چون c از G وابسته است که به‌صورت

$$c = ab$$

نوشته می‌شود وحاصلضرب a و b نام دارد.

II. **قانون شرکتپذیری:** اگر a، b، و c سه عنصر دلخواه G باشند، آنگاه

$$a(bc) = (ab)c$$

و لذا هریك ازدوطرف این تساوی را می‌توان با abc نمایش داد.

III. **قانون عنصر واحد:** مجموعهٔ G شامل عنصری است مـانند ۱ که **عنصرواحد**

(یا عنصر همانی یا عنصر خنثی) نامیده می‌شود و به‌ازای هر عنصر a از G:

$$a۱=۱a=a.$$

IV. قانون عنصر عکس: به‌ازای هرعنصر a از G عنصری مانند $a^{-۱}$ در G وجود دارد به‌طوری که

$$aa^{-۱}=a^{-۱}a=۱.$$

خواهید دیدکه این قوانین (یا بنداشتها) با بنداشتهای حاکم برضرب دستگاههای آشنای عددی، فی‌المثل اعدادگویـا، شباهت نزدیکی دارند، جز اینکه درحالت‌کلی لازم نیست قانون تعویضپذیری برای گروهها برقرار باشد.

تعریف ۲: هرگروه واجد این ویژگی اضافی راکه به‌ازای هر دوعنصرش تساوی

$$ab=ba$$

برقرارباشد یك گروه **آبلی**[۱] (یا **تعویضپذیر**) می‌نامند.

فقدان قانون تعویضپذیری برای گروهها مستلزم فرق‌گذاشتن بین ab و ba است، و دراین صورت به‌ترتیب می‌گوییم a ازچپ یا از راست در b ضرب شده است. درضمن اینکه لزومی به‌برقراری‌قانون تعویضپذیری درسراسرگروه نیست، مع‌هذا این امکان وجود داردکه این قانون برای زوجهای خاصی ازعناصر معتبر باشد.

تعریف ۳: عناصر a و b را با هم تعویضپذیر گویند هرگاه

$$ab=ba$$

برای مثال، ۱ با هرعنصری تعویضپذیر است وهمچنان‌که در IV تصریح شده‌است، همیشه a با $a^{-۱}$ تعویضپذیر است.

حال‌از‌این بنداشتها نتایجی چند استخراج می‌کنیم که ساختار گروه را روشنترمی‌سازند.

(i) قانون شرکتپذیری فقط بـرای سه عنصر وضع شده بود. امـا خواهیم دیدکه حاصلضرب n سازه (بـا یك ترتیب مشخص مفروض) دارای معنی منحصربه‌فردی است، و لذا به دلخواه می‌توان پرانتزها را درج یـا حذف‌کرد، با این شرط‌که سازه‌ها به ترتیب داده شده باقی بمانند. زیرا، بـا استفاده از بنداشت II به‌عنوان مبنای استقرا، می‌توانیم فرض‌کنیم کـه حاصلضرب هرتعـدادکمتر از n سازه، تعریف شده است، و بـا فرض $۱<s<r<n$ داریم:

$$a_۱a_۲\cdots a_r=(a_۱a_۲\cdots a_s)(a_{s+۱}\cdots a_r)$$

لازم است نشان دهیم

---

۱. مأخوذ از نام N. H. Abel (۱۸۰۲–۱۸۲۹).

$$(a_1 \cdots a_r)(a_{r+1} \cdots a_n) = (a_1 \cdots a_s)(a_{s+1} \cdots a_n) \qquad (۴.۱)$$

و این خود بدین معنی است که هر دوصورت پرانتزبندی به‌نتیجهٔ یکسان ختم می‌شوند. طرف چپ (۴.۱) را می‌توان به‌صورت

$$[(a_1 \cdots a_s)(a_{s+1} \cdots a_r)](a_{r+1} \cdots a_n) = [b_1 b_2]b_3$$

نوشت؛ در اینجا حاصلضربهای داخل پرانتزها به‌ترتیب با b_1، b_2، و b_3 نشان داده شده‌اند. طرف راست (۴.۱) را بعد از تفکیك سازهٔ دوم به‌کمك فرض استقرا می‌توان چنین نوشت:

$$(a_1 \cdots a_s)[(a_{s+1} \cdots a_r)(a_{r+1} \cdots a_n)] = b_1[b_2 b_3]$$

بنابر بنداشت II داریم:

$$[b_1 b_2]b_3 = b_1[b_2 b_3]$$

که مؤید ادعای (۴.۱) است. بنابراین ما حق داریم تمام پرانتزها را حذف کنیم و هریك از دو طرف تساوی را با

$$a_1 a_2 \cdots a_n$$

نشان دهیم. به‌ویژه، وقتی تمام سازه‌ها با هم‌مساوی باشند،همانندجبرمعمولی، خواهیم نوشت

$$aa = a^2$$

$$(aa)a = a(aa) = a^3$$

$$\cdots\cdots\cdots\cdots$$

از این‌رو وقتی n و m اعداد صحیح مثبتی باشند، داریم

$$a^m a^n = a^n a^m = a^{n+m} \qquad (۵.۱)$$

و

$$(a^m)^n = a^{mn} \qquad (۶.۱)$$

توجه به‌این نکته لازم است که قوانین آشنای (۵.۱) و (۶.۱) مربوط به‌توانها در نهایت به‌قانون شرکتپذیری ضرب متکی هستند.

ولی وقتی a و b تعویضپذیر نیستند، در حالت کلی می‌توان اثبات کرد که

$$(ab)^n \neq a^n b^n$$

اما در صورتی که a و b تعویضپذیر باشند،

$$(ab)^n = abab \cdots ab = a^n b^n \qquad (۷.۱)$$

و

$$a^m b^n = b^n a^m$$

زیرا در این حالت می‌توانیم سازه‌ها را به‌دلخواه مرتب کنیم.

(ii) بنداشت III وجود یك عنصر واحد دوطرفه را مسلم می‌گیرد. اکنون ثابت

می‌کنیم که این عنصر لزوماً منحصر به‌فرد است. زیرا فرض‌کنیم $1'$ عنصر دیگری با همان خواص ۱ باشد. پس $1 = 11'$؛ زیرا $1'$ به‌عنوان واحد از سمت راست بر ۱ اثرمی گذارد؛ و $1' = 11'$، زیرا ۱ به‌عنوان‌واحد از سمت چپ روی $1'$ عمل می‌کند. لذا $1' = 1$.

(iii) عنصر عکس (دوطرفه) که در بنداشت IV پذیرفتـه شده منحصربه‌فرد است. زیرا فرض‌کنیم، $aa_1 = 1$. پس $a^{-1}aa_1$ را می‌توان به‌دو راه محاسبه‌کرد، یعنی

$$a^{-1}aa_1 = (a^{-1}a)a_1 = 1a_1 = a_1$$

و

$$a^{-1}aa_1 = a^{-1}(aa_1) = a^{-1}1 = a^{-1}$$

که در اینجا $a_1 = a^{-1}$. به همین‌نحو معادلهٔ $a_2a = 1$ ایجاب می‌کند کـه $a_2 = a^{-1}$. در واقع ثابت کرده‌ایم که همهٔ عکسهای چپ و همهٔ عکسهای راست a با a^{-1} برابرند. معادلات

$$ya = b, \quad ax = b$$

به‌ترتیب دارای جوابهای

$$y = ba^{-1}, \quad x = a^{-1}b$$

هستند. در حالت‌کلی، $x \neq y$؛ و ما ناچاریم بین تقسیم از راست بر a و تقسیم از چپ بر آن فرق بگذاریم. این جوابها منحصر به‌فردند، زیرا اگر

$$ax = ax_1 = b$$

ضرب طرفین این تساوی از چپ در a^{-1} نتیجه می‌دهد $x = x_1$. به‌همین‌نحو اگر

$$ya = y_1a = b$$

نتیجه می‌گیریم که $y = y_1$.

به‌عبارت دیگر، می‌توانیم چنین بیان‌کنیم که درهر گروهی **قانون حذف** برقراراست؛ هم حذف از چپ و هم حذف از راست.

بدیهی است که به‌ازای هرعدد صحیح مثبت n،

$$1 = 1^2 = 1^3 = \ldots = 1^n \qquad (۸.۱)$$

چون a و a^{-1} تعویض‌پذیرند، از (۸.۱) و (۷.۱) تساوی

$$1^n = 1 = (aa^{-1})^n = a^n(a^{-1})^n$$

به‌دست می‌آید. بنا بر یکتایی‌عنصرعکس‌نتیجه می‌گیریم که $(a^{-1})^n$ عکس a^n است. مطابق معمول می‌نویسیم

$$(a^n)^{-1} = (a^{-1})^n = a^{-n} \qquad (۹.۱)$$

و به‌ازای هرعنصر a قرار می‌گذاریم که

$$a^{\circ} = ۱ \qquad (۱۰.۱)$$

خواننده برای اینکه خود را متقاعد سازد که m و n هر عـدد صحیح، مثبت، منفی یا صفر، باشند باز قواعد (۵.۱) و (۶.۱) برقرارند، با مشکلی مواجه نخواهد شد. بویژه مشاهده می‌کنیم که دو توان از یك عنصر همواره تعویضپذیـرند، حتی وقتی‌که نماها منفی یا صفر باشند:

$$a^k a^l = a^l a^k \qquad (۱۱.۱)$$

اگر a و b دو عنصر دلخواه باشند داریم

$$(ab)(b^{-۱}a^{-۱}) = abb^{-۱}a^{-۱} = ۱$$

و لذا بنا بریکتایی عکس داریم

$$(ab)^{-۱} = b^{-۱}a^{-۱} \qquad (۱۲.۱)$$

و در حالت کلیتر

$$(ab\ldots st)^{-۱} = t^{-۱}s^{-۱}\ldots b^{-۱}a^{-۱} \qquad (۱۳.۱)$$

سرانجام، متذکر می‌شویم که ۱ تنها عنصر **خود توان** گروه است. یعنی تنها جواب معادلهٔ

$$x^{۲} = x \qquad (۱۴.۱)$$

$x = ۱$ است. زیرا با ضرب (۱۴.۱) از چپ در $x^{-۱}$ به‌دست می‌آوریم

$$x^{-۱}x^{۲} = x^{-۱}x$$

و از این‌رو

$$x = ۱$$

اگر G متشکل از تعدادی متناهی عنصر باشد، آنگاه این تعداد را **مرتبهٔ** G می‌نامیم؛ درغیراین‌صورت می‌گوییم که G از مرتبهٔ نامتناهی‌است. مرتبهٔ G، متناهی چه نامتناهی، با

$$|G|$$

نمایش داده می‌شود.

گرچه برای ترکیب عناصر گروه ازاصطلاح ضرب بیش ازسایر اصطلاحات استفاده می‌شود، ولی‌گاه مناسب است‌که برای بیان ترکیب a و b از نمادهای دیگری چون

$$a \circ b$$

استفاده شود.

وقتی‌گروه آبلی باشد غالباً (و دراین‌کتاب هم صرفاً در این مورد) رجحان با نماد جمعی است. بدین‌ترتیب برای ترکیب a و b می‌نویسیم

$$a+b(=b+a)$$

قانون شرکتپذیری به‌صورت

$$(a+b)+c=a+(b+c)$$

در می‌آید. عنصر همانی (خنثی) با ۰ نشان داده می‌شود، و لذا

$$a+0=0+a=a$$

عکس a هم به‌صورت $-a$ نوشته می‌شود. در این حالت عبارت

$$a+a+\dots+a=na$$

مشابه a به «توان» n است. درسمت چپ، n جملهٔ متساوی وجود دارد. باید توجه داشت که عدد صحیح n در طرف راست معمولاً عنصری از گروه نیست؛ در واقع na چیزی جز یك شکل اختصاری برای عبارت سمت چپ نیست. حال «قوانین نمایی» به‌صورت

$$(n+m)a=na+ma$$

و

$$n(ma)=(nm)a$$

در می‌آیند، و ما نماد

$$-(na)=(-n)a$$

را هم معرفی می‌کنیم. چون گروه آبلی است رابطهٔ دیگر

$$n(a+b)=na+nb$$

را نیز خواهیم داشت.

۳. مثالی چند ازگروهها. در بیشتر شاخه‌های ریاضی به‌گروههای زیادی برمی‌خوریم. ما در اینجا چند مثال از گروههایی راکه درجاهای دیگر به‌آنها برمی‌خوریم جمع‌آوری می‌کنیم.

(i) مجموعهٔ تمام اعداد گویای مثبت نسبت به‌ضرب تشکیل یك‌گروه می‌دهد. در واقع حاصلضرب دو عدد گویای مثبت مجدداً یك عدد گویای مثبت است. عنصرواحد، عددگویای ۱ است. عکس یك عدد گویای مثبت نیز عددی است گویا و مثبت. شرکتپذیری یکی از قوانین‌حساب شناخته شده است. این، یك گروه آبلی نامتناهی‌است. بدیهی‌است‌که مجموعهٔ اعدادگویای منفی تشکیل یك گروه نمی‌دهد و همچنین است مجموعهٔ اعداد صحیح مثبت، زیرا هر عنصری بجز ۱ فاقد عکس است.

(ii) مجموعهٔ تمام اعداد صحیح نسبت به‌جمع تشکیل یك‌گروه آبلی می‌دهد. این گروه غالباً با Z نمایش داده می‌شود.

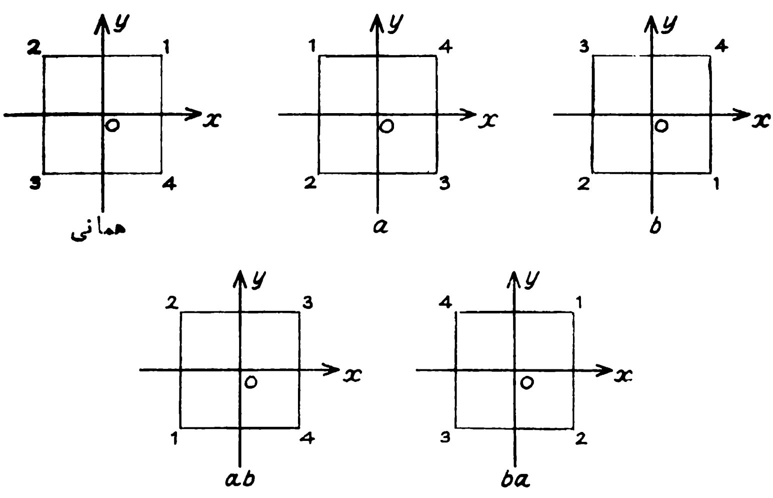
(iii) دورانهای حول یک نقطهٔ ثابت: اگر جسم (سه‌بعدی) صلبی آزادانه حول یك نقطهٔ ثابت O حرکت کند، هر تغییرمکان جسم معادل دورانی است به‌اندازهٔ زاویه‌ای مانند α حول خطی مار از O مانند l. چنین تغییرمکانی با (l, α) و یا مختصراً با حرف تنهایی مانند $a = (l, \alpha)$ نمایش داده می‌شود. اگر b تغییر مکان دیگری حول O باشد، حاصلضرب ab به عنوان تغییرمکان حاصل از b به‌دنبال a تعریف می‌شود. (در مورد این ترتیب، بعضی از نویسندگان قرارداد مغایری را که در آن حاصلضربها باید از راست به‌چپ خوانده شوند ترجیح می‌دهند.) تحت این‌قانون ترکیب، مجموعهٔ تمام تغییرمکانهای حولO، تشکیل یك‌گروه غیرآبلی می‌دهند. عمل همانی را می‌توان به‌صورت $(l, \circ)$ که در آن l دلخواه است، بیان کرد؛ و عکس (l, α) عبارت است از $(l, -\alpha)$. قانون شرکتپذیری از این واقعیت که دوران نوع خاصی است از تبدیل خطی، نتیجه می‌شود.

غالباً ما فقط به‌تغییرمکانهایی علاقمندیم که جسم را به‌حالت انطباق بر خودش در می‌آورند. این زیرمجموعه از تغییرمکانها نیز یك‌گروه تشکیل‌می‌دهد و **گروه تقارنی** جسم نام دارد.

شکل زیر این مطلب را که قانون تعویضپذیری همیشه برقرار نیست نشان می‌دهد: فرض‌کنید ۱۲۳۴ نمایش ورقهٔ مربع شکلی باشد که در بدو امر طبق شکل۱ در صفحهٔ (x, y) قرارداده شده است. محور z بر صفحهٔ ورقه در O عمود است. فرض می‌کنیم $Oxyz$ دستگاه مختصات مستقیمی ثابت در فضا باشد. با نمادهای فوق، اگر

$$a = \left(Oz, \frac{۱}{۲}\pi\right), \quad b = (Oz, \pi)$$

از دو نمودار آخر در می‌یابیم که ab و ba دو موضع مختلف از یك ورقه هستند.



شکل۱

(iv) **گروههای ماتریسها:** فرض براین است که خواننده با جبر مقدماتی ماتریسها به‌خصوص با ضرب ماتریسی آشنایی‌دارد. بعضی ازمهمترین مثال گروهها به‌توسط مجموعهٔ معینی از ماتریسها به‌دست می‌آیند.

(الف) فرض کنیم F یك میدان، مثلاً* میدان اعـداد حقیقی، باشد. تمام ماتریسهای عادی n در n راکه عناصرشان به‌دلخواه از میدان F انتخاب شده‌اند درنظر بگیرید. این مجموعه که تحت ضرب ماتریسی تشکیل یك گروه می‌دهد، با $GL(n, F)$ نشان داده می‌شود و **گروه خطی‌کلی** از درجهٔ n روی F نام دارد.

(ب) مجموعهٔ ماتریسهای قائـم ازدرجهٔ n روی F تحت عمل ضرب ماتریسی، یك گروه تشکیل می‌دهند.

(ج) مجموعهٔ ماتریسهای عادی n درn که عناصرشان اعداد صحیح باشند تحت ضرب بسته است، اما عکس این‌گونـه ماتریسها در حالت‌کلی به‌این مجموعه تعلق ندارد زیـرا تشکیل عکس مستلزم تقسیم بر دترمینان است. ولی مجموعهٔ ماتریسهای صحیح با دترمینان ± ۱ حتماً یك گروه تشکیل می‌دهد که **گروه تك هنگی**[۱] از درجهٔ n نامیده می‌شود.

(v) **رده‌های مانده‌ها:** فرض کنیم m عدد صحیح ثابتی بزرگتر از یك باشد، که در مقولهٔ حاضر از آن به‌عنوان **هنگ** یاد خواهیم‌کرد. دوعدد صحیح x و y برحسب هنگ m همنهشت هستند، یا همنهشت به‌هنگ mاند، هرگاه $x-y$ بر m قابل قسمت باشد. این مفهوم را به‌صورت نمادی، چنین می‌نویسیم:

$$x \equiv y \pmod m \qquad (۱۵.۱)$$

که هم‌ارز با این عبارت است‌که عدد صحیحی مانند k وجود دارد به‌قسمی که

$$x = y + km \qquad (۱۶.۱)$$

برای مثال $۳ \equiv ۱۸ \pmod ۵$، $-۲ \equiv ۱۴ \pmod ۸$، $۱۲ \equiv ۰ \pmod ۳$.

هرعدد صحیح دقیقاً با یکی از اعداد صحیح مجموعهٔ

$$Z_m : ۰, ۱, ۲, \dots, m-۲, m-۱ \qquad (۱۷.۱)$$

همنهشت به‌هنگ m است. و لذا آن را یك مجموعهٔ‌کامل مانده‌های به‌هنگ m می‌نامند. و اینها در واقع کمترین مانده‌های نامنفی به‌هنگ mاند.

تحقیق درستی قواعد ذیل در باب همنهشتیها آسان است:

اگر $x_۱ \equiv y_۱ \pmod m$ و $x_۲ \equiv y_۲ \pmod m$ آنگاه

$$x_۱ + x_۲ \equiv y_۱ + y_۲ \pmod m \qquad (۱۸.۱)$$

و

$$x_۱ x_۲ \equiv y_۱ y_۲ \pmod m \qquad (۱۹.۱)$$

---

۱. بعضی از مؤلفان این اصطلاح را فقط برای ماتریسهای با دترمینان واحد به‌کار می‌برند.

به‌موجب (۱۸.۱)، می‌توانیم از (۱۷.۱) یك گروه جمعی بسازیم با این قید که $a+b$ آن عنصر از (۱۷.۱) باشد که با $a+b$ همنهشت به‌هنگ m است. به‌عبارت دیگر ترکیب، همان جمع معمولی است همراه با، در صورت لزوم، تبدیل به کمترین ماندهٔ نامنفی به‌هنگ m. عنصر همانی صفر، و عکس a برابر $m-a$ است. پس Z_m یك گروه تشکیل می‌دهد که گروه جمعی مانده‌های به‌هنگ m نامیده می‌شود. برای مثال وقتی $m=5$، داریم $۳=۲+۱$، $۱=۲+۴$، $۰=۳+۲$، $۲=۴+۳$، و قس‌علیهذا.

ممکن است این سؤال پیش آید که آیا می‌توان به‌طریق مشابه از (۱۹.۱) استفاده کرد و به‌مجموعهٔ مانده‌ها یك ساخت گروه ضربی داد. اما به‌زودی خواهیم دید که حتی اگر ماندهٔ صفر را، که نمی‌تواند عنصر یك گروه ضربی از مرتبهٔ بزرگتر از یك باشد، حذف کنیم بازهم با اشکال مواجه می‌شویم. همچنان که دیده‌ایم (صفحهٔ ۷) قانون حذف ایجاب می‌کند که از $cx=cy$ تساوی $x=y$ به‌دست آید. اما، برای مثال داریم $۲۲\equiv ۴\pmod{۶}$، در صورتی که $۱۱\not\equiv ۲\pmod{۶}$؛ و لذا قانون حذف درحالت کلی برای ضرب به‌هنگ m برقرار نیست. ولی، همچنان که خواهیم دید، حذف در همنهشتیها در بعضی از حالات برقرار است. به‌منظور تحلیل این موضوع، ناچاریم نتایج وعلاماتی چند از نظریهٔ مقدماتی اعداد را به‌عاریت بگیریم: بزرگترین مقسوم‌علیه مشترك a و b با (a, b) نشان داده می‌شود؛ بالاخص، وقتی که $(a, b)=۱$، می‌گوییم که a و b **متباین** هستند. اگر a، b را عادکند می‌نویسیم $a|b$. احکام ذیل را بدون برهان ذکر می‌کنیم:

(i) اگر $m|kc$ و $(m, k)=۱$، آنگاه $m|c$؛

(ii) اگر $(m, a)=۱$ و $(m, b)=۱$، آنگاه $(m, ab)=۱$.

(iii) هرگاه $(m, a)=۱$، آنگاه اعداد صحیحی چون u و v وجود دارند به قسمی که $au+mv=۱$.

حال می‌توانیم بگوییم که هرگاه $(k, m)=۱$، آنگاه همنهشتی

$$kx\equiv ky \pmod{m} \tag{۲۰.۱}$$

نتیجه می‌دهد که $x\equiv y\pmod{m}$. زیرا که (۲۰.۱) هم‌ارز با $m|k(x-y)$ است که از آن، بنابر (i)، نتیجه می‌شود $m|x-y$. یعنی $x\equiv y\pmod{m}$.

هرگاه عاملی با m متباین باشد می‌توان آن را از دو طرف همنهشتی حذف‌کرد.

تعداد اعداد صحیح موجود در مجموعهٔ

$$۱, ۲, ۳, \ldots, m$$

را که با m متباین‌هستند با $\phi(m)$ **(تابع اویلر)** نشان می‌دهند. برای مثال، $\phi(۹)=۶$، زیرا ۶ عدد صحیح n وجود دارد که $۰\leqslant n\leqslant ۹$ و $(n, ۹)=۱$. وقتی p اول باشد تمام اعداد صحیح مجموعهٔ $\{۱, ۲, \ldots, p-۱, p\}$، بجز آخری، با p متباین‌اند؛ و بنابراین

$$\phi(p)=p-۱ \tag{۲۱.۱}$$

باز، هرگاه $m=p^r$ و r عدد صحیح مثبتی باشد. فقط مضارب p درمجموعهٔ $\{۱, ۲, \ldots, p^r\}$

نمی‌توانند بـا p متباین بـاشند؛ چون تعداد چنین مضاربی p^{r-1} است، از آنجـا نتیجه می‌شود که

$$\phi(p^r) = p^r - p^{r-1} \tag{۲۲.۱}$$

معمولاً چنین می‌گیرند:

$$\phi(1) = 1 \tag{۲۳.۱}$$

به‌طور کلی، فرض کنیم

$$R_m : a_1, a_2, \dots, a_{\phi(m)} \tag{۲۴.۱}$$

مجموعهٔ کمترین مانده‌های مثبت متباین با m باشد. از این‌رو ۱ $= (a_i, m)$ و $0 < a_i \leqslant m$. یکی از این مانده‌هـا، مثلاً a_1، برابر بـا ۱ است. بنابـر (ii)، حاصلضرب هر دوعنصر (۲۴.۱) مجدداً با m متباین است؛ وقتی که این حاصلضرب بزرگتر از m باشد در (۲۴.۱) نخواهد بود ولی بـا یکی ازعناصر (۲۴.۱) همنهشت خواهد بود، زیرا در واقع هرعدد صحیح متباین با m در (۲۴.۱) واقع است. لذا می‌توانیم بنویسیم

$$a_i a_k \equiv a_l \pmod m \tag{۲۵.۱}$$

و در R_m یك قانون ترکیب به صورت ضرب تعریف می‌کنیم، که درصورت لزوم به دنبالش تبدیل به‌کمترینماندهٔ مثبت به‌هنگ m هم بیاید. برای مثال

$$4 \times 5 \equiv 2 \pmod 9, \quad 4 \times 7 \equiv 1 \pmod 9.$$

اگرفراموش نشود که عمل‌محاسبه به‌هنگ m است و لذا «معادلات» صرفاً به‌هنگ m برقرار هستند، مناسب است که قانون ترکیب در R_m را به‌صورت سادهٔ زیر بنویسیم

$$a_i a_k = a_l \tag{۲۶.۱}$$

ازخواص‌همنهشتیها به‌سادگی نتیجه می‌شود که قوانین تعویض‌پذیری وشرکتپذیری برقرارند. و واضح است‌کـه $(= a_1)$ ۱ عنصر همانی است. بـاقی می‌ماند نشان دهیم که هرعنصر $a \in R_m$ یك عکس دارد. چون ۱ $= (a, m)$، می‌توانیم (iii) را به‌کار بگیریم و وجود معادله‌ای به‌شکل

$$au + mv = 1 \tag{۲۷.۱}$$

را استنتاج کنیم. این تساوی، هم‌ارز است با $au \equiv 1 \pmod m$. لذا u عکس a در R_m است. بدین طریق، تحت قانون ترکیب مذکور، R_m یك گروه آبلی ازمرتبهٔ $\phi(m)$ تشکیل می‌دهد.

۴. جدول‌ضرب. درنظریهٔ مجرد گروهها هیچ اشاره‌ای به‌ماهیت عناصر نمی‌شود. اگر همهٔ

حاصلضربهای ممکن ab معلوم باشند، ویا بوسیلهٔ قواعد مشخصی بتوان آنها را تعیین کرد، آن گروه کاملاً معلوم است. دریک گروه متناهی از مرتبهٔ g، تعداد چنین حاصلضربهایی $g^۲$ است که، همچنان که اولین بار به توسط ا. کیلی[۱] پیشنهاد شده است، می‌توان آنهـا را به‌طریقی‌مناسب دریک جدول‌ضرب $g \times g$ فهرست کرد. جدولهای ذیل به‌ترتیب گروههایی ازمراتب ۲، ۳، و ۴ را نمایش می‌دهند.

جدول (i)

	۱	a
۱	۱	a
a	a	۱

جدول (ii)

	۱	a	b
۱	۱	a	b
a	a	b	۱
b	b	۱	a

جدول (iii)

	۱	a	b	c
۱	۱	a	b	c
a	a	۱	c	b
b	b	c	۱	a
c	c	b	a	۱

جدول (iv)

	۱	a	b	c
۱	۱	a	b	c
a	a	b	c	۱
b	b	c	۱	a
c	c	۱	a	b

درهر مورد، حاصلضرب xy در محل تقاطع سطر مقابل به‌حرف x با ستون واقع در زیر حرف y قرار دارد. برای نمونه، در (iii)؛ داریم $ac=b$، درصورتی که در (iv) داریم $ac=۱$. خواننده مشاهده می‌کندکه همهٔ این گروهها آبلی هستند و این امر ازاین واقعیت ناشی می‌شودکه عناصر جدولها نسبت به‌قطر اصلی (خط واصل بین اولین عنصر سطر اول وآخرین عنصر سطر آخر) متقارن هستند.

مثال آموزنده‌تر گروه مرتبهٔ شش

$$G : ۱, a, b, c, d, e \qquad (۲۸.۱)$$

با جدول‌ضرب

---

1. A. Cayley, Phil. Mag., vol. vii (4), 1854.

جدول (v)

	۱	a	b	c	d	e
۱	۱	a	b	c	d	e
a	a	b	۱	e	c	d
b	b	۱	a	d	e	c
c	c	d	e	۱	a	b
d	d	e	c	b	۱	a
e	e	c	d	a	b	۱

(۲۹.۱)

است.

بعضی از ویژگیهای گروهی از روی جدول روشن می‌شود: بسته بودن واضح‌است، زیرا هر درایهٔ جدول یکی ازعناصر (۲۸.۱) است؛ اثر عنصر واحد برعناصر ذیگر متناظر با این واقعیت است که سطر و ستون اول مربع، متشکل از عناصر(۲۸.۱) با همان ترتیب اولیه هستند؛ وجود عکس هرعنصر و در واقع مقدار آن، آشکار است. زیرا درهر سطر و هرستون دقیقاً یك درایهٔ ۱ موجود است. تنها تحقیق درستی قانون شرکتپذیری دشوار است. تحقیق‌اینکه به‌ازای هر انتخاب x، y، و z، تساوی $x(yz)=(xy)z$ برقرار است، حتی برای یك گروه کوچك کار پرزحمتی است. درجدول فوق قانون شرکتپذیری حتماً برقرار است؛ برای مثال

$$(ac)d=ed=b,\ a(cd)=a^{۲}=b$$

اما برقراری آن درحالت‌کلی با بحثی غیرمستقیم، که ذیلاً توضیح داده می‌شود، به‌بهترین وجه تأمین می‌گردد.

گاه یك جدول مربعی راکه هرسطر و ستونش متشکل ازعناصری همانند ولی با ترتیبهای متفاوت‌باشند یك **مربع لاتینی** می‌نامند. لذا جدول‌ضرب یك‌گروه متناهی، همواره یك مربع لاتینی است. اما عکس این مطلب درست نیست، زیرا قانون شرکتپذیری ممکن است درست نباشد. مثلاً مربع لاتینی ۵ × ۵

	۱	a	b	c	d
۱	۱	a	b	c	d
a	a	۱	d	b	c
b	b	c	۱	d	a
c	c	d	a	۱	b
d	d	b	c	a	۱

را نمی‌توان به‌عنوان جدول‌ضرب گروهی پذیرفت چون $(ab)c=dc=a$، درصورتی که $a(bc)=ad=c$ که با قانون شرکتپذیری در تناقض است.

به‌سادگی می‌توان تحقیق کرد که مجموعهٔ متشکل ازشش ماتریس

$$\Gamma:\begin{cases} I=\begin{bmatrix} ۱ & ۰ \\ ۰ & ۱ \end{bmatrix}, & A=\begin{bmatrix} -۱ & -۱ \\ ۱ & ۰ \end{bmatrix}, & B=\begin{bmatrix} ۰ & ۱ \\ -۱ & -۱ \end{bmatrix} \\ C=\begin{bmatrix} ۰ & ۱ \\ ۱ & ۰ \end{bmatrix}, & D=\begin{bmatrix} ۱ & ۰ \\ -۱ & -۱ \end{bmatrix}, & E=\begin{bmatrix} -۱ & -۱ \\ ۰ & ۱ \end{bmatrix} \end{cases} \quad (۳۰.۱)$$

نسبت به‌ضرب ماتریسی بسته است؛ برای مثال

$$B=A^۲,\ A^۳=C^۲=D^۲=E^۲=I,\ AD=C,\ AC=E$$ و به همین قیاس

به‌علاوه ملاحظه می‌کنیم که کل جدول‌ضرب ۶×۶ این مجموعه بـا (۲۹.۱) یکی است، مشروط براینکه ۱ با I تعویض شود و حروف بزرگ به‌جای حروف کوچك نوشته شوند. بدین‌طریق طبق (۲۹.۱) اگر تساوی $xy=z$ بـرقرار باشد، ماتریسهای متناظر در رابطهٔ $XY=Z$ صدق می‌کنند؛ به‌عکس هر رابطهٔ ضربی در Γ بـا رابطهٔ متناظرش در G جور درمی‌آید. اما معلوم‌است که ضرب ماتریسی شرکتپذیر است، یعنی به‌ازای هرسه عنصر Γ، $(XY)Z=X(YZ)$. بنابراین ثابت کرده‌ایم که رابطهٔ $(xy)z=x(yz)$ در G برقرار، و از آنجا قانون شرکتپذیری در G اثبات شده است. این وضعیت را چنین توصیف می‌کنیم که Γ یك **نمایش صادق** G است. این یك موردی است کـه در آن از یك بخش ملموستر دانش ریاضی به‌نظریهٔ گروههای مجرد کمك شده است.

بجاست که متذکر شویم ساختار گروههای G و Γ یکسان است. این نمونه‌ای است ازیك مفهوم مهم که اینك با جزئیات بیشتر تشریح می‌شود. فرض‌کنیم

$$G:۱,\ a,\ b,\ c,\ \dots \quad (۳۱.۱)$$

و

$$G':۱',\ a',\ b',\ c',\ \dots \quad (۳۲.۱)$$

دو گروه (متناهی یا نامتناهی) باشندکه عناصر واحد آنها به‌ترتیب بـا ۱ و $۱'$ نشان داده شده‌اند. فرض می‌کنیم تناظری یك به‌یك مانند

$$\theta:G\leftrightarrow G' \quad (۳۳.۱)$$

بین عناصر G وعناصر G' وجود دارد؛ یعنی به‌هر x از G نگارهٔ یکتایی مـانند $x'=x\theta$ از G' وابسته می‌شود وهر y' از G' نگارهٔ عنصر منحصر به‌فرد yی از G است به طوری که $y'=y\theta$. به‌عبارت دیگر عناصر G و G' چنان قابل جفت‌کردن هستندکه هرعنصر G وهر عنصر G' فقط در یك زوج قرار می‌گیرند. به‌علاوه فـرض می‌کنیم این تناظر واجد

این ویژگی باشدکه $z = xy$ ، اگر وفقط اگر $x'y' = z'$؛ یا به‌طور صوریتر

$$(xy)\theta = (x\theta)(y\theta) \qquad (۳۴.۱)$$

دراین صورت گوییم گروههای G و G' **یکریخت** (ایزومورف واژهٔ یونانی برای یکریخت است)، هستند ومی نویسیم

$$G \cong G' \qquad (۳۵.۱)$$

هر رابطهٔ بین عناصر G بـا رابطه‌ای بین عناصر G' متناظر است و به عکس؛ ما صرفاً با برداشتن یا گذاشتن پریم‌های چسبیده به‌نمادهای عناصر ازیك گروه به‌گروه دیگرمی‌رسیم. این گروهها صرفاً درعلامت با هم فرق دارند ولی از دیدگاه تجرید، باید یکی تلقی‌شوند، زیرا جدول‌ضربشان یکی است. به‌بیان فنی‌تر می‌توان گفت که مفهوم یکریختی درمجموعهٔ تمام گروهها یك رابطهٔ هم‌ارزی ایجاد می‌کند زیرا آشکارا شرایط معمولی رابطهٔ هم‌ارزی برقرارنـد: (i) $G \cong G$ (انعکاسی)، (ii) اگـر $G \cong G'$، آنگاه $G' \cong G$ (تقارنی)، (iii) اگر $G \cong G'$ و $G' \cong G''$، آنگاه $G \cong G''$ (تعدی). چند مثال‌دیگر در روشن‌کردن این مفهوم بدما کمك می‌کند.

مثال ۱. گروههای مرتبهٔ ۴ زیرین یکریخت هستند؛ قانون ترکیب برای هریك در پرانتز ذکر شده است:

(۱) اعداد ۱، i، ۱ −، i − (ضرب معمولی.)

(۲) ماتریسهای

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$$

(ضرب ماتریسی).

(۳) مانده‌های ۱، ۲، ۳، ۴ به‌هنگ ۵ (ضرب وتبدیل به‌هنگ ۵)؛

اگر در هر حالت عناصر گروه را با ۱، a، b، c نشان دهیم، آنگاه جدول‌ضرب گروه به‌صورت (iv) ازصفحهٔ ۱۴ درمی‌آید.

مثال ۲. گروههای مرتبهٔ چهار زیرین با هم یکریخت هستند.

(۴) ماتریسهای

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$$

(ضرب ماتریسی).

(۵) مانده‌های ۱، ۳، ۵، ۷ به‌هنگ ۸ (ضرب وتبدیل به‌هنگ ۸)؛

اگر در هر حالت عناصر گروه را با ۱، a، b، c نشان دهیم، دیده می‌شود که جدول ضرب با جدول (iii) ازصفحهٔ ۱۴ یکی است.

واضح است که هرگاه دوگروه یکریخت باشند، باید یك تعداد عنصر داشته باشند. اما عکس این مطلب درست نیست؛ برای مثال گروههای مفروض با جداول (iii) و (iv) یکریخت نیستند زیرا در (iii) هرعنصر درمعادلهٔ $x^۲ = ۱$ صدق می‌کند، ولی در مورد جدول(iv) چنین امری صادق نیست. بدین‌طریق گروههایی‌که مرتبهٔ آنها یکی‌است، ممکن است ساختار متفاوت داشته باشند.

۵. گروههای دوری. مجموعهٔ

$$C : ۱(=x^{\circ}),\ x,\ x^{-۱},\ x^{۲},\ x^{-۲},\ \ldots,\ x^{n},\ x^{-n},\ \ldots \qquad (۳۶.۱)$$

ازنمادهای متمایز راکه درآن ضرب برطبق قاعدهٔ

$$x^{r}x^{s} = x^{r+s},\ (r,\ s = ۰,\ \pm ۱,\ \pm ۲,\ \ldots) \qquad (۳۷.۱)$$

تعریف می‌شود درنظر می‌گیریم. بر اثر این‌قانون ترکیب، C به یك‌گروه آبلی تبدیل می‌شود‌که به **گروه دوری نامتناهی** تولید شده به‌وسیلهٔ x، موسوم است. این‌گروه با گروه جمعی اعداد صحیح، یعنی با مجموعهٔ

$$Z : ۰,\ \pm ۱,\ \pm ۲,\ \ldots$$

که درآن ترکیب r و s به‌صورت $r+s$ تعریف می‌شود، یکریخت است. تناظری‌که این یکریختی را برقرار می‌کند به‌وسیلهٔ

$$x^{r}\theta = r$$

داده می‌شود؛ البته، دراینجا رابطهٔ

$$(x^{r}x^{s})\theta = x^{r}\theta + x^{s}\theta$$

باید به‌جای (۳۴.۱) قرارگیرد، زیرا گروه Z به‌صورت جمعی بیان شده است. پس تمام گروههای دوری نامتناهی یکریخت هستند.

وضعیت جالبتر زمانی نمایان می‌شودکه فرض شود نماد x درمعادلهٔ

$$x^{m} = ۱ \qquad (۳۸.۱)$$

که درآن m یك عدد صحیح مثبت و بزرگتر از واحد است، صدق می‌کند. دراین حالت مجموعهٔ

$$C_{m} : ۱,\ x,\ x^{۲},\ \ldots,\ x^{m-۱} \qquad (۳۹.۱)$$

متشکل ازنمادهای متمایز، تحت قاعدهٔ

$$x^r x^s = x^{r+s} (r, s = ۰, ۱, \dots, m-۱)$$

که در آن $s+r$ باید به‌کوچکترین ماندهٔ نامنفی به‌هنگ m تبدیل شود، تشکیل یك گروه آبلی ازمرتبهٔ m می‌دهد. این گروه گروه دوری ازمرتبهٔ m تولید شده بـه وسیلهٔ x نامیده می‌شود. این گروه با گروه جمعی مانده‌های به‌هنگ m، یعنی

$$Z_m : ۰, ۱, ۲, \dots, m-۱$$

که درصفحهٔ ۱۱ شرح داده شد یکریخت است. پس بـار دیگر نتیجه می‌گیریم کـه تمام گروههای دوری ازمرتبهٔ m با هم یکریخت‌اند. هرگاه در (۳۹.۱) x را با عدد مختلط

$$\varepsilon = \exp\left(\frac{۲\pi i}{m}\right)$$

تعویض کنیم نمایش دیگری ازهمان گروه بـه دست می‌آوریم. ضرب هرعدد مختلط در ε متناظر با دورانی است بـه اندازهٔ زاویهٔ $۲\pi/m$ در صفحهٔ مختلط. اگر این عمل m بار تکرار شود، هرنقطه یـك دور کامل را طی می‌کند، و این امـر اصطلاح گروه دوری را توجیه می‌کند.

اکنون فرض کنیم x عنصری از گروهی دلخواه بـاشد. دراین صورت دوحالت رخ می‌دهد: یا اینکه تمام توانهای فهرست شدهٔ x در (۳۶.۱) متمایزند یا اینکه دوعددصحیح k و l وجود دارند که $k > l$ و

$$x^k = x^l$$

وبنا براین

$$x^{k-l} = ۱$$

لذا دراین حـالت توان مثبت معینی از x برابر عنصر واحـد شده است. بنا براین بـاید کمترین توان مثبتی با همین ویژگی وجود داشته باشد. این‌نکته ما را به‌تعریف ذیل هدایت می‌کند.

تعریف ۴. فرض کنیم x عنصری از یك‌گروه باشد. اگر همهٔ توانهای x متمایز باشند، گوییم x از **مرتبهٔ نامتناهی** است. اگر همهٔ توانهای x متمایز نباشند،آنگاه کوچکترین عدد صحیح مثبتی چون h وجود دارد که مرتبهٔ (**دورهٔ تناوب**) x نامیده می‌شود و

$$x^h = ۱$$

البته، دریك گروه متناهی همهٔ عناصر ازمرتبهٔ متناهی هستند. اگر x ازمرتبهٔ h باشد، آنگاه $x^h = ۱$ ولی $x^k \neq ۱$، هرگاه $۰ < k < h$. مجدداً، اگر $m = hq$، داریم

$$x^m = (x^h)^q = ۱$$

عکس این نکته نیز درست است:

قضیه۱. اگر x از مرتبهٔ h باشد، آنگاه $x^m = 1$، اگر و فقط اگر m مضربی از h باشد.

برهان. m را بر h تقسیم و فرض می‌کنیم q خارج‌قسمت باشد و r باقیمانده:

$$m = hq + r$$

در اینجا داریم $0 \leqslant r < h$. از این‌رو

$$1 = x^m = (x^h)^q x^r = 1x^r = x^r$$

و این با ویژگی مینیمال بودن h در تناقض است مگر آنکه $r = 0$. پس

$$m = hq$$

صحت احکام ذیل در مورد مرتبهٔ عناصر گروه به‌سادگی قابل تحقیق هستند:

(i) عنصر واحد تنها عنصر از مرتبهٔ یك است.

(ii) عناصر x و x^{-1} دارای مرتبهٔ مساوی‌اند.

(iii) اگر رابطهٔ $y = t^{-1}xt$، که در آن t عنصری است دلخواه برقرار باشد ،آنگاه x و y از یك مرتبه‌اند.

قضیه۲. فرض‌کنیم x از مرتبهٔ h باشد. اگر s عدد صحیح مثبتی باشد، آنگاه x^s از مرتبهٔ $h/(h, s)$ است که در آن (h, s) معرف بزرگترین مقسوم‌علیه مشترك h و s است.

برهان. فرض‌کنیم $d = (h, s)$. پس داریم

$$h = dh', \ s = ds'$$

که در آن $(h', s') = 1$. باید نشان دهیم که x^s از مرتبهٔ h' است. حال گوییم

$$(x^s)^{h'} = x^{s'dh'} = (x^{h'd})^{s'} = (x^h)^{s'} = 1$$

زیرا x از مرتبهٔ h است. باقی می‌ماند اثبات اینکه اگر t عدد صحیح مثبتی باشد و

$$(x^s)^t = 1 \qquad (۴۰.۱)$$

آنگاه $t \geqslant h'$. فرض کنیم (۴۰.۱) برقرار باشد. پس بنا بر قضیهٔ ۱، $h|st$، یعنی $h'd|s'dt$ و از این‌رو $h'|s't$. اما h' با s' متباین است. بنابراین $h'|t$، و از آنجا داریم $h' \leqslant t$.

۶. نگاشتهای مجموعه‌ها.

فرض‌کنیم

$$\Sigma : \xi, \eta, \zeta, \ldots$$

مجموعه‌ای متناهی یا نامتناهی از اشیاء باشد. یك نگاشت

$$f : \Sigma \rightarrow \Sigma$$

از Σ به‌توی خود قاعده‌ای است که به‌توسط آن به هر $\xi \in \Sigma$ شیئی یکتا مانند $\eta \in \Sigma$ متناظر

می‌شود؛ η را نگارهٔ ξ بر اثر f می‌نامند. ما رسم‌الخط $\eta = \xi f$ را بر رسم‌الخط $\eta = f(\xi)$، که در آنالیز و توپولوژی بیشتر مرسوم است، ترجیح می‌دهیم. دو نگاشت f و g برابرند اگر، وفقط اگر، به‌ازای هر $\xi \in \sum$، $\xi f = \xi g$. ترکیب f و g نگاشت $f \circ g$ است که چنین تعریف می‌شود:

$$\xi(f \circ g) = (\xi f)g$$

و آن بدین‌معنی است که $f \circ g$ از f وسپس g حاصل می‌شود. بدین‌طریق اگر $\xi f = \eta$، آنگاه $\xi(f \circ g) = \eta g$.

فرض کنیم f، g و h سه نگاشت از $\sum$ به‌توی‌خود باشند. نشان می‌دهیم که ترکیب سه نگاشت همواره از قانون شرکتپذیری تبعیت می‌کند. فرض کنیم ξ شیئی از $\sum$ باشد. قرار می‌دهیم

$$\xi f = \eta, \quad \eta g = \zeta, \quad \zeta h = \tau$$

سپس

$$\xi[f \circ (g \circ h)] = (\xi f)(g \circ h) = \eta(g \circ h) = (\eta g)h = \zeta h = \tau$$

و

$$\xi[(f \circ g) \circ h] = [\xi(f \circ g)]h = [(\xi f)g]h = (\eta g)h = \zeta h = \tau$$

چون ξ عنصر دلخواهی از $\sum$ است، نتیجه می‌شود که

$$f \circ (g \circ h) = (f \circ g) \circ h \qquad (۴۱۰۱)$$

مثال ۱. فرض کنیم

$$\sum : \xi, \eta, \zeta, \ldots$$

یك فضای برداری n بعدی باشد، می‌توانیم اشیاء $\sum$ را به‌عنوان بردارهای سطری درنظر بگیریم. اگر A یك ماتریس $n \times n$ باشد، آنگاه $f : \xi \to \xi A$ نگاشتی از $\sum$ به‌توی خود است. هرگاه $g : \xi \to \xi B$ نگاشت دیگری ازاین نوع باشد، نگاشت مرکب، با رابطهٔ $f \circ g : \xi \to \xi AB$ داده می‌شود. بدین طریق بحث مذکور مؤید شرکتپذیر بودن ضرب ماتریسی است.

پس برای اینکه ثابت کنیم گردایه‌ای چون

$$G : f, g, h, \ldots$$

ازنگاشتها، یك گروه تشکیل می‌دهد فقط لازم است که صحت بنداشتهای (I)، (III)، و (IV) از صفحه ۴ را تحقیق کنیم. مشاهده می‌کنیم که f عکس دارد، اگر و فقط اگر، f یك به‌یك باشد و $\sum$ را به‌روی $\sum$ بنگارد؛ واین بدین‌معنی است که هر $\eta \in \sum$ نگارهٔ منحصراً یك شیء $\xi \in \sum$ است. بنابراین می‌توان رابطهٔ $\xi f = \eta$ را حل کرد و جواب منحصربه‌فرد

آن یعنی ξ را به‌شکل $\xi=\eta f^{-1}$ به‌دست آورد، و بدین‌گونه، نگاشت عکس یعنی f^{-1} را تعریف کرد.

مثال۲. به‌وضوح دیده می‌شود که گردایهٔ نگاشتهایی که یك جسم سه‌بعدی مفروض را بر خودش منطبق می‌سازد در(I)، (III) و (IV) صدق می‌کند و بنابراین تشکیل یك گروه می‌دهد.

مثال۳. فرض کنیم دامنهٔ تغییرات z صفحهٔ منبسط z باشد، یعنی z تمام اعداد مختلط و نقطهٔ بینهایت را اختیار کند. هریك از شش نگاشت

$$\left.\begin{aligned} &f_1 : z \to z \ (\text{همانی}),\ f_2 : z \to \frac{1}{1-z},\ f_3 : z \to \frac{z-1}{z} \\ &f_4 : z \to \frac{1}{z},\ f_5 : z \to 1-z,\ f_6 : z \to \frac{z}{z-1} \end{aligned}\right\} \qquad (۴۲۰۱)$$

صفحهٔ منبسط z را به‌خودش تبدیل می‌کند، و بنابراین تحت ترکیب (نگاشتها) تشکیل یك دستگاه شرکتپذیر می‌دهد. یك واقعیت قابل توجه این است که این دستگاه بسته است. برای مثال

$$z(f_2 \circ f_3) = (zf_2)f_3 = \frac{1}{1-z}\, f_3 = \frac{(1-z)^{-1}-1}{(1-z)^{-1}} = z = zf_1$$

و لذا $f_1 = f_2 \circ f_3$. و از این‌رو $f_3 = f_2^{-1}$.

$$z(f_4 \circ f_3) = (zf_4)f_3 = \frac{1}{z} f_3 = \frac{z^{-1}-1}{z^{-1}} = 1-z = zf_5$$

و لذا $f_5 = f_4 \circ f_3$، و به‌همین قیاس برای بقیه. جدول ضرب کامل آن به‌قرار زیراست:

جدول (vi)

	f_1	f_2	f_3	f_4	f_5	f_6
f_1	f_1	f_2	f_3	f_4	f_5	f_6
f_2	f_2	f_3	f_1	f_5	f_6	f_4
f_3	f_3	f_1	f_2	f_6	f_4	f_5
f_4	f_4	f_6	f_5	f_1	f_3	f_2
f_5	f_5	f_4	f_6	f_2	f_1	f_3
f_6	f_6	f_5	f_4	f_3	f_2	f_1

اگر به‌جای f_1، f_2، f_3، f_4، f_5، f_6 بنویسیم ۱، a، b، c، d، e، دیده می‌شود که جدول

(vi) همان جدول (v) از صفحهٔ ۱۵ است. بدین طریق یك نمایش صادق دیگری از این گروه مجرد را کشف کردیم.

۷. جایگشتها. مطالعهٔ نگاشتهایی که بریك مجموعهٔ متناهی Σ از اشیاء عمل می‌کنند از اهمیت خاصی برخوردار است. برای سهولت، اغلب اشیای‌متعلق به Σ را با اعداد صحیح ۱، ۲، ...، n نشان می‌دهیم. یك نگاشت از Σ به‌روی Σ یك جایگشت از **درجهٔ** n نامیده می‌شود. چنین جایگشتی را به‌صورتی روشن با نماد

$$\pi = \begin{pmatrix} ۱ & ۲ \ldots & j \ldots n \\ a_۱ & a_۲ \ldots & a_j \ldots a_n \end{pmatrix} \qquad (۴۳.۱)$$

که در آن $a_j = j\pi$ نگارهٔ j بر اثر π است توصیف می‌کنیم. پس سطر دوم (۴۳.۱) آرایش دیگری از همان اعداد صحیح ۱، ۲، ...، n است. با توجه به‌جبر مقدماتی، می‌دانیم که تعداد چنین آرایشهایی برابر است با $n!$. از این‌رو $n!$ جایگشت از درجهٔ n وجود دارد. مجموعهٔ کامل جایگشتها با S_n نمایش داده می‌شود.

ملاحظه می‌کنیم که اطلاعات مفروض در (۴۳.۱) را می‌توان به‌طرق معادل گوناگونی ارائه کرد. در واقع می‌توانیم ترتیب ستونهای این نماد را به‌هر نحوی که بخواهیم عوض کنیم. برای مثال، نمادهای

$$\begin{pmatrix} ۱ & ۲ & ۳ & ۴ \\ ۲ & ۳ & ۱ & ۴ \end{pmatrix} = \begin{pmatrix} ۲ & ۱ & ۴ & ۳ \\ ۳ & ۲ & ۴ & ۱ \end{pmatrix} = \begin{pmatrix} ۴ & ۲ & ۱ & ۳ \\ ۴ & ۳ & ۲ & ۱ \end{pmatrix} = \ldots$$

همگی یك جایگشت را نشان می‌دهند. نخستین این جایگشتها را که در آن سطر فوقانی مشتمل بر اعداد با ترتیب طبیعی آنهاست، **صورت استانده** می‌نامیم. واضح است که هر جایگشتی $n!$ صورت معادل دیگر هم دارد، زیرا سطر فوقانی می‌تواند به‌دلخواه انتخاب و اطلاعات مربوطه برطبق آن تنظیم شود.

فرض کنیم

$$\rho = \begin{pmatrix} ۱ & ۲ \ldots n \\ b_۱ & b_۲ \ldots b_n \end{pmatrix} = \begin{pmatrix} a_۱ & a_۲ \ldots a_n \\ c_۱ & c_۲ \ldots c_n \end{pmatrix} \qquad (۴۴.۱)$$

جایگشت دیگری باشد که در آن $b_j = j\rho$ و $c_j = a_j\rho$. ترکیب جایگشتها از قاعدهٔ ترکیب نگاشتها تبعیت می‌کند. با این‌حال برای سهولت، حاصلضرب را، به‌جای $\rho \circ \pi$، با $\pi\rho$ نشان می‌دهیم. بدین طریق $\pi\rho$ جایگشتی است که ابتدا از اعمال π و سپس از ρ نتیجه می‌شود. بعضی از نویسندگان قرارداد متقابل این را به‌کار می‌گیرند که بیشترمناسب زمانی است که نگارهٔ j بر اثر π با $\pi(j)$ نشان داده می‌شد و نه با $j\pi$ که مورد استفادهٔ ماست. وقتی ρ برای ضرب از چپ در π، همچنان که در (۴۴.۱) نشان داده شده است، «مهیا» باشد، فوراً می‌توان حاصلضرب $\pi\rho$ را به‌صورت

$$\pi\rho = \begin{pmatrix} 1 & 2 \cdots n \\ c_1 & c_2 \cdots c_n \end{pmatrix}$$

نوشت. زیرا به ازای هر j، $(j=1, 2, \ldots, n)$، $j\pi = a_j$ و $a_j\rho = c_j$. لذا $j\pi\rho = (j\pi)\rho = a_j\rho = c_j$.

برای مثال هرگاه

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}, \rho = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}$$

پس از اینکه ρ را به‌طریق مناسبی آرایش دهیم ملاحظه می‌کنیم که

$$\pi\rho = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \begin{pmatrix} 2 & 3 & 4 & 1 \\ 1 & 2 & 4 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix}$$

ضمناً:

$$\rho\pi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix} \begin{pmatrix} 3 & 1 & 2 & 4 \\ 4 & 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 3 & 1 \end{pmatrix}$$

که معرف این واقعیت است که ضرب جایگشتها، در حالت کلی، تعویضپذیر نیست.*

جایگشت

$$\iota = \begin{pmatrix} 1 & 2 \cdots n \\ 1 & 2 \cdots n \end{pmatrix} = \cdots = \begin{pmatrix} a_1 & a_2 \cdots a_n \\ a_1 & a_2 \cdots a_n \end{pmatrix}$$

که تمام اشیاء را ثابت نگاه می‌دارد، مسلماً در روابط $\pi = \pi\iota = \iota\pi$ صدق می‌کند و بنابراین، جایگشت همانی است. عکس π (به‌صورت غیر استانده) با نماد

$$\pi^{-1} = \begin{pmatrix} a_1 & a_2 \cdots a_n \\ 1 & 2 \cdots n \end{pmatrix}$$

مشخص می‌شود؛ زیرا به‌سادگی دیده می‌شود که

$$\pi\pi^{-1} = \pi^{-1}\pi = \iota$$

برای مثال

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 2 & 3 & 4 & 1 \\ 1 & 2 & 3 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$$

---

* وقتی قراردادی خلاف قرارداد بالا منظور باشد، باید جای $\pi\rho$ با $\rho\pi$ عوض شود.

هیچ نیازی به‌بررسی قانون شرکتپذیری نداریم. زیرا صحت این امر درخواص عمومی نگاشتها تحقیق شده است. بنابراین قضیهٔ ذیل را اثبات کرده‌ایم.

قضیهٔ اصلی ۱. مجموعهٔ همهٔ جایگشتهای n شیء، S_n، یك گروه ازمرتبهٔ $n!$، به‌نام **گروه متقارن** از درجهٔ n تشکیل می‌دهد؛ قانون ترکیب همان قانون ترکیب نگاشتهای اشیاء به‌روی خودشان است.

خواننده با اندکی تمرین به‌محاسبهٔ حاصلضرب دو یا چند جایگشت بدون نیاز به‌نوشتن مراحل واسطهٔ آماده‌سازی، عادت خواهدکرد. برای مثال، فرض‌کنیم

$$\alpha=\begin{pmatrix}۱&۲&۳&۴\\ ۲&۳&۱&۴\end{pmatrix},\quad \beta=\begin{pmatrix}۱&۲&۳&۴\\ ۴&۱&۲&۳\end{pmatrix},\quad \gamma=\begin{pmatrix}۱&۲&۳&۴\\ ۴&۳&۲&۱\end{pmatrix}$$

برای محاسبهٔ حاصلضرب $\alpha\beta\gamma$، به‌ترتیب تغییرات پشت سرهم هرشیء را تك‌تك تحت اعمال α، β و γ مورد بررسی قرار می‌دهیم. بدین طریق

$$۱\to۲\to۱\to۴$$

$$۲\to۳\to۲\to۳$$

$$۳\to۱\to۴\to۱$$

$$۴\to۴\to۳\to۲$$

که درآن پیکانهای هرسطر ازچپ به‌راست اشاره به‌تأثیرهای α ، β و γ (با همین‌ترتیب) دارد. ازاین‌رو

$$\alpha\beta\gamma=\begin{pmatrix}۱&۲&۳&۴\\ ۴&۳&۱&۲\end{pmatrix}$$

برای توضیح بیشتر شش جایگشت $S_۳$ را فهرست می‌کنیم

$$\left.\begin{array}{lll}\iota=\begin{pmatrix}۱&۲&۳\\ ۱&۲&۳\end{pmatrix}, & \alpha=\begin{pmatrix}۱&۲&۳\\ ۲&۳&۱\end{pmatrix}, & \beta=\begin{pmatrix}۱&۲&۳\\ ۳&۱&۲\end{pmatrix}\\ \gamma=\begin{pmatrix}۱&۲&۳\\ ۲&۱&۳\end{pmatrix}, & \delta=\begin{pmatrix}۱&۲&۳\\ ۳&۲&۱\end{pmatrix}, & \varepsilon=\begin{pmatrix}۱&۲&۳\\ ۱&۳&۲\end{pmatrix}\end{array}\right\}\quad (۴۵.۱)$$

هنگام بررسی ساختار گروهی درمی‌یابیم که $S_۳$ با گروه مجرد ارائه شده درجدول (۷) صفحهٔ ۱۵، یکریخت است. این یکریختی با جورکردن ۱ با ι، وهر حرف یونانی با حرف لاتینی متناظرش به‌دست می‌آید. برای مثال، بنابر قاعدهٔ ضرب جایگشتها درمی‌یابیم که

$$\alpha\gamma=\varepsilon,\quad \beta\gamma=\delta$$

که متناظر با روابط

$$ac=e, \quad bc=d$$

ازجدول (۷) است. بدین گونه باز هم نمایش دیگری از این گروه مجرد به‌دست می آید.

فرض کنیم مجموعهٔ $\sum$ به دومجموعهٔ دو به‌دو ازهم جدای مثلاً

$$\Sigma_۱=\{۱, ۲, \ldots, m\}, \quad \Sigma_۲=\{m+۱, m+۲, \ldots, n\}$$

تقسیم شده باشد و π و ρ جایگشتهایی از $\sum$ باشندکه π فقط بر $\Sigma_۱$ تأثیر می گذارد و عناصر $\Sigma_۲$ را تغییر نمی‌دهد، حال آنکه ρ بر $\Sigma_۲$ اثر می کند ولی هیچ یك از عناصر $\Sigma_۱$ را تغییر نمی‌دهد. پس روشن است که $\pi\rho=\rho\pi$، زیرا اثرهای π و ρ با یکدیگر تداخل ندارند. لذا ملاحظه می کنیم که جایگشتهایی که برمجموعه‌های دو به‌دو ازهم جدا اثرمی کنند با یکدیگر تعویضپذیرند.

جایگشتی که m شیء را به‌طریق دوری تعویض می کند یك دور از درجهٔ m نامیده می‌شود. بدین گونه اگر اشیاء با ۱، ۲، ...، m نشان داده شوند چنین جایگشتی با نماد

$$\gamma=\begin{pmatrix} ۱ & ۲ \ldots m-۱ & m \\ ۲ & ۳ \ldots m & ۱ \end{pmatrix} \tag{۴۶.۱}$$

توصیف می‌شود. اگر تصورکنیم که این m شیء بر m نقطه از محیط یك دایره قرار گرفته‌اند، آنگاه γ هر شیء را به نقطهٔ بعدی می برد؛ به طوری که، شیء آخر جای شیء اول را اشغال می کند. رسم چنین است که دورها را با نماد فشردهٔ

$$\gamma=(۱ \quad ۲ \ldots m)$$

نمایش می‌دهند و این نمایش باید هم‌ارز با (۴۶.۱) تلقی شود. بدین طریق

$$i\gamma=i+۱ \quad (i=۱, ۲, \ldots, m-۱), \quad m\gamma=۱ \tag{۴۷.۱}$$

چون مهم نیست که با کدام شیئی عمل را شروع می کنیم، می‌توانیم γ را به وسیلهٔ هریك ازصورتهای هم‌ارز

$$(۱ \quad ۲ \ldots m)=(۲ \quad ۳ \ldots m \quad ۱)=\ldots(m \quad ۱ \ldots m-۱)$$

هم بنویسیم.

تأثیر γ را می‌توان به‌وسیلهٔ معادلات (۴۷.۱) بیان کرد ویا به‌طور مختصرتر

$$j\gamma=j+۱ \pmod m \tag{۴۷.۱$'$}$$

با این دریافت که طرف راست $'$(۴۷.۱) باید به‌کوچکترین ماندهٔ مثبت به‌هنگ m تبدیل شود. به‌طریق مشابه، تأثیر توان rام γ به‌وسیلهٔ

$$j\gamma^r = j + r\,(\operatorname{mod} m) \qquad (۴۸.۱)$$

خلاصه‌می‌شود. بنا بر این بدیهی‌است که $\iota = \gamma^m$، درحالی که $\iota \neq \gamma^r$، هرگاه $0 < r < m$.
بدین‌گونه درمی‌یابیم که یك دور از درجهٔ m ازمرتبهٔ m نیز هست.

از این پس این قرارداد را به‌کار می‌بندیم که شیئی راکه براثر جایگشت π ثابت می‌ماند لزومی نداردکه درنماد π صراحتاً ذکرکنیم. برای مثال، هرگاه $n = ۳$،

$$(۱ \quad ۲ \quad ۳) = \begin{pmatrix} ۱ & ۲ & ۳ \\ ۲ & ۳ & ۱ \end{pmatrix}$$

وهرگاه $n = ۵$،

$$(۱ \quad ۲ \quad ۳) = \begin{pmatrix} ۱ & ۲ & ۳ & ۴ & ۵ \\ ۲ & ۳ & ۱ & ۴ & ۵ \end{pmatrix}$$

دقیقتر بگوییم، نماد (۳ ۲ ۱) در اینجا جایگشتهای متفاوت با درجات مختلف را نشان می‌دهد، اما عموماً به‌قرینه پیدا می‌شود که کلاً چند شیء را در بر می‌گیرد و لذا از این اشیاء کدام یك ثابت می‌ماند.

اغلب مناسب است که یك جایگشت به‌صورت‌حاصلضرب دورهایی که برمجموعه‌های ازهم جدا عمل می‌کنند نشان داده شود. بدین طریق، هرگاه $n = ۷$،

$$\pi = (۱ \quad ۲) \quad (۴ \quad ۶ \quad ۷)$$

نمایشگر جایگشت

$$\pi = \begin{pmatrix} ۱ & ۲ & ۳ & ۴ & ۵ & ۶ & ۷ \\ ۲ & ۱ & ۳ & ۶ & ۵ & ۷ & ۴ \end{pmatrix}$$

است. هر جایگشت را می‌توان به دورهای ازهم جدا تجزیه‌کرد. برای مشاهدهٔ این امر مفهوم **مدارها** براثر π را وارد می‌کنیم. شیء دلخواه p را انتخاب می‌کنیم و سرنوشت p را براثر کاربردهای مکرر π مورد بررسی قرار می‌دهیم: مجموعهٔ

$$p,\ p\pi,\ p\pi^2,\ \ldots \qquad (۴۹.۱)$$

مدار p نام دارد. چون اشیای موجود در (۴۹.۱) همگی نمی‌توانند متمایز باشند، باید اعدادی‌صحیح ونامنفی‌چون r و s وجود داشته باشندکه $s > r$ و $p\pi^s = p\pi^r$. ازاین‌رو $p\pi^{s-r} = p$. نتیجه اینکه‌کوچکترین عدد صحیح مثبتی مانند h وجود داردکه

$$p\pi^h = p \qquad (۵۰.۱)$$

اکنون واضح است که π، دور

$$(p,\ p\pi,\ p\pi^2,\ \ldots,\ p\pi^{h-1}) \qquad (۵۱.۱)$$

ازمرتبهٔ h را دربر دارد. اگر q، شیء دیگری باشد که در (۵۱.۱) نباشد، آنگاه فرض می‌کنیم k کوچکترین عدد صحیح مثبتی باشد که $q\pi^k = q$. بدین طریق q، دور

$$(q,\ q\pi,\ q\pi^{۲},\ \cdots,\ q\pi^{k-۱}) \qquad (۵۲.۱)$$

را تولید می‌کند. باید بداین مطلب مهم توجه کرد که دورهای (۵۱.۱) و (۵۲.۱) هیچ عنصر مشترکی ندارند. زیرا فرض کنیم

$$p\pi^a = q\pi^b$$

و بنابراین

$$q = p\pi^{a-b}$$

ازتقسیم $a-b$ بر h داریم

$$a-b = th+r$$

که در آن $h > r \geqslant ۰$. ازاین رو نتیجه می‌گیریم که

$$q = p\pi^r$$

که این با انتخاب q درتناقض است. اگر شیئی باقی باشد که در (۵۱.۱) یا (۵۲.۱) نباشد، آن شیء دور دیگری را تولید می‌کند که اشیائش ازاشیای دورهای قبلی متمایزند؛ ساختن دورها را ادامه می‌دهیم تا اینکه تمام اشیاء به‌حساب آیند. هرشیء که براثر π ثابت می‌ماند دوری به‌طول یك تولید می‌کند و بنابر قرارداد این دورها را می‌توان حذف کرد. به‌اصطلاح فنی‌تر می‌توان گفت که یك رابطهٔ هم‌ارزی بین اشیاء Σ برقرار کرده‌ایم؛ دوشیء هم‌ارزند اگر، وفقط اگر، به‌یك مدار ولذا به‌یك دور تعلق داشته باشند. چنانکه بر خواننده معلوم خواهد شد، هر رابطهٔ هم‌ارزی در روی Σ، همواره، به یك افراز Σ به‌رده‌های هم‌ارز از هم جدا. نتیجه می‌شود که در وضعیت موجود ما با عاملهای دوری π مربوط است. بنابراین ما قضیهٔ ذیل را اثبات کرده‌ایم.

قضیهٔ اصلی ۲. هر جایگشت را می‌توان به حاصلضرب دورهای ازهم جدا تجزیه کرد. این دورها دو به‌دو تعویض‌پذیرند و این تجزیه، صرفنظر از آرایشهای مختلف عاملهای دوری، منحصر به‌فرد است.

مثال. فرض کنیم

$$\pi = \begin{pmatrix} ۱ & ۲ & ۳ & ۴ & ۵ & ۶ & ۷ & ۸ \\ ۴ & ۵ & ۶ & ۱ & ۷ & ۸ & ۲ & ۳ \end{pmatrix}$$

با شروع از شیء ۱ متوجه می‌شویم که مدارش ۱ و ۴ است. ازاین‌رو π دور (۱ ۴) را دربردارد. با ادامهٔ این‌عمل و شروع باهرشیء که دراین‌دور نباشد، مثلاً ۲، مداری چون

۲، ۵، ۷ به‌دست می‌آید، که دور (۷ ۵ ۲) را به‌ما می‌دهد. سرانجام، به‌مدار ۳، ۶، ۸ وبنابراین به‌دور (۸ ۶ ۳) می‌رسیم. چون شیء دیگری که به حساب آید وجود ندارد، نشان داده‌ایم که

$$\pi=(۱\quad ۴)\quad (۲\quad ۵\quad ۷)\quad (۳\quad ۶\quad ۸)$$

تمرین

(۱) ثابت کنید که هریك از مجموعه‌های عددی ذیل نسبت به ضرب معمولی، گروههای آبلی نامتناهی تشکیل می‌دهند:

(الف) $\{۲^k \mid k=۰, \pm ۱, \pm ۲, \ldots\}$؛

(ب) $\left\{\frac{۱+۲m}{۱+۲n} \mid m, n=۰, \pm ۱, \pm ۲, \ldots\right\}$؛

(ج) $\{\cos\theta+i\sin\theta \mid$ عددی است گویا $\theta\}$.

(۲) چرا اعداد گویای مثبت، وقتی که قانون ترکیب a و b به‌صورت a/b تعریف می‌شود، یك گروه تشکیل نمی‌دهند؟

(۳) فرض کنیم a نگاشت $x \rightarrow \alpha x+\beta$ باشد که در آن α و β اعداد مختلط مفروضی هستند و $\alpha \neq ۱$. فرمولی برای a^n که در آن n عدد صحیح مثبتی است به‌دست آورید؛ ونشان دهید که مرتبهٔ a متناهی است اگر، وفقط اگر، α یکی از ریشه‌های واحد باشد.

درمثالهای ۴ تا ۸ فرض شده است که عناصر دریك گروه قراردارند ولذا قانون شرکتپذیری برای آنها صادق است.

(۴) اگر هریك ازعناصر a، b و ab ازمرتبهٔ ۲ باشند، ثابت کنید که a و b تعویضپذیرند.

(۵) ثابت کنید عناصر ab و ba دارای یك مرتبه‌اند.

(۶) اگر $ba=a^m b^n$، ثابت کنید عناصر $a^m b^{n-۲}$، $a^{m-۲} b^n$ و $ab^{-۱}$ دارای یك‌مرتبه‌اند.

(۷) اگر $b^{-۱}ab=a^k$، ثابت کنید $b^{-r}a^s b^r=a^{sk^r}$.

(۸) فرض کنید x عنصری از مرتبهٔ mn باشد و در آن $(m, n)=۱$. ثابت کنید x را می‌توان به‌صورت $x=yz$، که در آن y و z تعویضپذیر وبه‌ترتیب ازمرتبهٔ m و n هستند، نوشت.

(۹) ثابت کنید که هر گروه ازمرتبهٔ زوج تعداد فردی عنصر ازمرتبهٔ ۲ دارد.

(۱۰) مرتبهٔ هرعنصر از گروه ضربی مانده‌های ۱، ۲، ۳، ۴، ۵، ۶ به‌هنگ ۷ را پیدا کنید. نشان دهید که این گروه یك گروه دوری ازمرتبهٔ ۶ است.

(۱۱) نشان دهید ماتریسهای

$$\begin{bmatrix} ۱ & ۰ \\ ۰ & ۱ \end{bmatrix}, \begin{bmatrix} \omega & ۰ \\ ۰ & \omega^{۲} \end{bmatrix}, \begin{bmatrix} \omega^{۲} & ۰ \\ ۰ & \omega \end{bmatrix}, \begin{bmatrix} ۰ & ۱ \\ ۱ & ۰ \end{bmatrix}, \begin{bmatrix} ۰ & \omega^{۲} \\ \omega & ۰ \end{bmatrix}, \begin{bmatrix} ۰ & \omega \\ \omega^{۲} & ۰ \end{bmatrix}$$

که در آن $۱ = \omega^{۳}$ و $۱ \neq \omega$، نسبت به ضرب ماتریسی یك گروه از مرتبهٔ ۶ تشکیل می‌دهند. ثابت کنید که این گروه با گروه جدول (v) صفحهٔ ۱۵ یکریخت است.

(۱۲) نشان دهید که نگاشتهای

$$f_{۱}: z \to z,\ f_{۲}: z \to -z,\ f_{۳}: z \to \frac{۱}{z},\ f_{۴}: z \to -\frac{۱}{z}$$

از صفحهٔ منبسط z به‌روی خودش، یك گروه تشکیل می‌دهند و این گروه با گروه جدول (iii) صفحهٔ ۱۴ یکریخت است.

(۱۳) جایگشتهای (الف)

$$\begin{pmatrix} ۱ & ۲ & ۳ & ۴ & ۵ & ۶ & ۷ & ۸ & ۹ \\ ۴ & ۶ & ۹ & ۷ & ۲ & ۵ & ۸ & ۱ & ۳ \end{pmatrix}$$

و (ب)

$$\begin{pmatrix} a & b & c & d & e & f \\ c & e & d & f & b & a \end{pmatrix}$$

را به دورهای دو به‌دو ازهم جدا تجزیه کنید. مرتبهٔ این دو جایگشت را بیابید.

(۱۴) جایگشتهای ذیل را برحسب دورهای دو به‌دو ازهم جدا تجزیه کنید.

(الف) $(abc \cdots k)(al)$

(ب) $(a_{۱}a_{۲} \cdots a_{r}xyb_{۱}b_{۲} \cdots b_{s})(a_{r}a_{r-۱} \cdots a_{۱}xyc_{۱}c_{۲} \cdots c_{t})$

(ج) $(a_{۱}a_{۲} \cdots a_{r}xyzb_{۱}b_{۲} \cdots b_{s})(a_{r}a_{r-۱} \cdots a_{۱}xyzc_{۱}c_{۲} \cdots c_{t})$

(۱۵) تحقیق کنید که جایگشتهای

ι(همانی), (۱۲)(۳۴), (۱۳)(۲۴), (۱۴)(۲۳)

یك گروه آبلی ازمرتبهٔ ۴ تشکیل می‌دهند که با گروه داده شده درجدول (iii) صفحهٔ ۱۴ یکریخت است.

(۱۶) نشان دهید مجموعهٔ ماتریسهای

$$A(v)=\left(1-\frac{v^2}{c^2}\right)^{-1/2}\begin{bmatrix}1 & -v\\ -v/c^2 & 1\end{bmatrix}$$

که در آن c یك ثابت مثبت است و v در بازهٔ $-c<v<c$ تغییر می‌کند، با قانون ترکیب

$$A(v_1)A(v_2)=A(v_3)$$

$$v_3=\frac{v_1+v_2}{1+\frac{v_1 v_2}{c^2}}$$

یك گروه تشکیل می‌دهد (گروه لورنتس).

۲

زیرگروهها

۸. زیرمجموعه‌ها. چون یك گروه G گردایه‌ای ازعناصراست، تعاریف و نمادهای معمول نظریهٔ مجموعه‌ها را می‌توان برای G هم به کاربرد. لذا اگر A، B، C، . . . زیرمجموعه‌هایی از G باشند، برای بیان این واقعیت که هر عنصر A عنصر B نیز هست می‌نویسیم $A \subset B$؛ و این نماد حالتی را هم که A و B مساوی هستند شامل می‌شود. اجتماع $A \cup B$ مجموعهٔ تمام عناصری است که به A یا به B و یا به‌هردو تعلق دارند؛ اشتراك $A \cap B$ از تمام عناصری که هم به A و هم به B تعلق دارند تشکیل می‌شود. اگر چنین عنصری وجود نداشته باشد می‌نویسیم $A \cap A = \varnothing$ (مجموعهٔ تهی). نماد $a \in A$ بدین‌معنی‌است که عنصر a به A تعلق دارد. در بعضی موارد ما ازقرارداد (تاحدی غیرمنطقی) یکی گرفتن یك عنصر a. با مجموعهٔ متشکل از تنها عنصر a استفاده می‌کنیم. لذا اگر a_1، a_2، a_3، . . . عناصر A باشند می‌نویسیم:

$$A = a_1 \cup a_2 \cup a_3 \cup \cdots$$

اما ضربی که در G تعریف شده است، به‌زیرمجموعه‌های G یك ساختار اضافی می‌دهد. به‌ازای هردو زیرمجموعهٔ مفروض A و B عبارت

$$AB \tag{۱۰۲}$$

را به‌عنوان مجموعهٔ تمام عناصری که بتوانند به‌صورت ab، که در آن $a \in A$ و $b \in B$، نوشته شوند تعریف می‌کنیم. نیازی نیست که این حاصلضربها متمایز باشند، زیرا برحسب

اتفاق ممکن است $a_1 \neq a_2$ و $b_1 \neq b_2$ ولی تساوی $a_1b_1 = a_2b_2$ برقرار باشد. با این حال باید تأکید شود که AB صرفاً به‌عنوان یك مجموعه در نظر گرفته می‌شود، ولذا تکرار عناصر باید نادیده گرفته شود: برطبق معمول، زیرمجموعه‌ها تنها درصورتی متساوی‌اند که صرفنظر از عناصر تکراری شامل عناصر متمایز واحدی باشند. از این پس تساوی بین زیرمجموعه‌ها همواره بدین‌معنی تلقی خواهد شد. البته، در حالت کلی،

$$AB \neq BA$$

اما وقتی که $AB = BA$، این تساوی بدین‌معنی نیست که هر عنصر A با هر عنصر B تعویضپذیر است. ما فقط می‌توانیم نتیجه بگیریم که به‌ازای هر $a \in A$ و هر $b \in B$، عناصری چون $a' \in A$ و $b' \in B$ وجود دارند که $ab = b'a'$.

به‌سادگی می‌توان تحقیق کرد که ضرب زیرمجموعه‌ها شرکتپذیر است، یعنی

$$(AB)C = A(BC) \tag{۲.۲}$$

و لذا هریك از دو طرف (۲.۲) را به‌طور ساده با ABC می‌توان نمایش داد. با استفاده از یك کوتاه‌نویسی بدیهی، قرار می‌دهیم:

$$A^2 = AA, \quad A^3 = AAA, \; \ldots$$

بدین‌طریق A^2 گردایهٔ عناصری است که بتوانند به‌صورت a_1a_2، که حوزهٔ تغییرات a_1 و a_2 مجموعهٔ A است، نوشته شوند.

قواعد ذیل به‌سهولت اثبات می‌شوند:

$$(A \cup B)C = AC \cup BC$$

$$C(A \cup B) = CA \cup CB$$

$$(A \cap B)C = AC \cap BC$$

$$C(A \cap B) = CA \cap CB$$

اینك حالات خاصی را که در آنها بعضی از مجموعه‌ها از یك عنصر تنها تشکیل می‌شوند موردتوجه قرارمی‌دهیم. پس اگر x و y عناصری از G باشند، Ax مجموعهٔ کلیهٔ عناصری به‌صورت ax است، و yAx متشکل است از کلیهٔ عناصری به‌صورت yax، که در آن حوزهٔ تغییرات a، A است. ملاحظه می‌کنیم که

$$x^{-1}(A_1 \cap A_2 \cap \cdots A_r)x = x^{-1}A_1x \cap x^{-1}A_2x \cap \cdots \cap x^{-1}A_rx \tag{۳.۲}$$

وقتی که G یك گروه جمعی آبلی باشد. ترکیب دو زیرمجموعهٔ A و B چنین نوشته می‌شود

$$A + B$$

و این، مجموعهٔ کلیهٔ عناصری است که بتوانند به‌صورت $a + b$، که در آن $a \in A$ و $b \in B$، بیان شوند. بالاخص، زیرمجموعهٔ

$$A+A$$

(که به‌صورت $2A$ خلاصه می‌شود، صفحهٔ ۳۳ را ببینید) گردایهٔ همهٔ عناصر $a+a'$ است که در آن a و a' به A تعلق دارند. وقتی که x عنصر ثابتی از G باشد زیرمجموعهٔ

$$A+x$$

ازعناصر $a+x$ $(a \in A)$ تشکیل می‌شود، ونماد $A-x$ برای $A+(-x)$ به‌کار می‌رود.

درحالت کلی، قاعدهٔ حذف درمورد زیرگروهها صدق نمی‌کند. یعنی از $AC=BC$ نمی‌توان نتیجه گرفت کـه $A=B$. اما از $Ax=Bx$ لازم می‌آید که $A=B$، و $Ax=C$ هم‌ارز است با $A=Cx^{-1}$. برای ضرب یـك مجموعه از سمت چپ در یك عنصر تنها، نتایج مشابهی به‌دست می‌آیند. حالت مهمی کـه در فصل بعدی با آن مواجه خواهیم شد حالتی است که

$$x^{-1}Ax=A \quad \text{یا} \quad Ax=xA \tag{۴.۲}$$

واین بدان‌معنی‌است که به‌ازای هر $a \in A$ عنصری مانند $a' \in A$ وجود دارد که $ax=xa'$.

عدد اصلی A، یعنی تعداد عناصر متمایز A، خواه متناهی باشند یـا نامتناهی، اغلب با $|A|$ نشان داده می‌شود.

۹. زیرگروهها. ما مخصوصاً به‌زیرمجموعه‌هایی از یك گروه G علاقه‌مندیم کـه از اصول موضوعهٔ گروه پیروی کنند. چنین زیرمجموعه‌هایی را زیرگروههای G می‌نامند. پس H یك زیرگروه G است هرگاه در شرایط زیر صدق کند:

(۱) اگر $u \in H$ و $v \in H$، آنگاه $uv \in H$ (بنداشت بستاری)؛

(۲) وقتی‌که ۱ عنصر همانی باشد داریم $1 \in H$ (بنداشت عنصر همانی)؛

(۳) اگر $u \in H$، آنگاه $u^{-1} \in H$ (بنداشت عنصرعکس).

ما به‌قانون شرکتپذیری اشاره نکردیم، زیرا برقراری‌آن برای تمام G پذیرفته شده است.

وقتی که H یك زیرگروه G باشد می‌نویسیم:

$$H \leqslant G$$

و این نماد برنماد $H \subset G$ رجحان دارد. نماد $\leqslant$ فقط برای زیرمجموعه‌هایی کـه گروه هستند به‌کارخواهد رفت. شمول اکید بوسیلهٔ $<$ نشان داده می‌شود. اگر H یك زیرگروه و s یکی از عناصرآن باشد، آنگاه ویژگـی بستاری ایجاب می‌کند کـه $Hs \subset H$. از سوی دیگر، هرعنصر u از H را می‌توان چنین نوشت: $u=(us^{-1})s$. چون $us^{-1} \in H$، این نشان می‌دهد که $u \in Hs$ و از این‌رو $H \subset Hs$. بنابراین

$$Hs=H \tag{۵.۲}$$

و به‌طور مشابه

$$sH=H \tag{۵.۲}'$$

بعکس، فرض کنیم s عنصری از G است که در (۵.۲) صدق می کند. پس، درحالت خاص

$$s = 1s \in H$$

و لذا (۵.۲) یا $'$(۵.۲) شرط لازم وکافی است برای اینکه عنصری از G به زیرگروه H متعلق باشد.

خواننده می‌تواند نشان دهدکه این نکات به‌آسانی قابل تعمیم‌اند. در نتیجه قضیهٔ زیر را می‌توان بیان کرد.

قضیهٔ ۳. زیر مجموعهٔ S از G فقط و فقط وقتی به زیرگروه H تعلق داردکه

$$HS = SH = H$$

در حالت خاص، که $S = H$، داریم:

$$H^2 = H \tag{۶.۲}$$

جالب توجه این است که هرگاه H متناهی باشد، رابطهٔ (۶.۲) بدعکس، ایجاب می کندکه H یك گروه باشد.

قضیهٔ ۴. فرض‌کنیم H زیرمجموعه‌ای متناهی از G باشد. آنگاه H یك زیرگروه G است اگر، و فقط اگر، $H^2 = H$.

برهان. فقط باید ثابت‌کنیم که (۶.۲) گروه بودن H را ایجاب می کند. فرض کنید عناصر H به‌ترتیب زیر شماره‌گذاری شده باشند:

$$H: u_1, u_2, \dots, u_h \tag{۷.۲}$$

و u یکی از این عناصر باشد. در این‌صورت h عنصر

$$Hu: u_1u, u_2u, \dots, u_hu \tag{۸.۲}$$

همگی به H^2 و لذا بنابرفرض به H تعلق دارند. به‌علاوه، این عناصرمتمایزند زیرا کـه قانون حذف درG صدق می کند. از این‌رو مجموعه‌های (۷.۲) و(۸.۲) صرفنظرازترتیب آنها یکی هستند. بخصوص، عنصر u در (۸.۲) قراردارد. بدین‌طریق عدد صحیحی مانند j وجود دارد به‌قسمی که

$$u_ju = u$$

وازآنجا نتیجه می‌شود $u_j = 1 \in H$. بالاخره، عدد صحیحی‌مانند k وجود دارد به‌قسمی که

$$u_ku = 1 \ (= u_j)$$

یعنی، $u_k = u^{-1} \in H$، که ثابت می کند H یك گروه است.

وقتی‌که H یك زیرگروه (متناهی‌یا نامتناهی) G و x عنصری از G باشد زیرمجموعهٔ

$$H' = x^{-1} H x \tag{۹.۲}$$

نیز یك زیرگروه G است. زیرا اگر $x^{-1}ux$ و $x^{-1}vx$ دو عنصر دلخواه H' باشند و $u, v \in H$، آنگاه $(x^{-1}ux)(x^{-1}vx) = x^{-1}uvx \in H'$. همچنین $x^{-1}1x = 1 \in H'$ و $x^{-1}u^{-1}x = (x^{-1}ux)^{-1} \in H'$. به‌علاوه این‌دو گروه با هم یکریخت هستند، زیرا

$$u\theta = x^{-1}ux \, (u \in H)$$

نگاشتی است یك به‌یك از H به‌روی H' و با این ویژگی که

$$(u\theta)(v\theta) = (uv)\theta$$

پس:

$$H \cong H'$$

یادآورمی‌شویم که هر گروه G مسلماً زیرگروههای $\{1\} = H$ و $H = G$ را هم در بردارد؛ زیرگروهی را که بین این‌دو فرین قرار داشته باشد یك **زیرگروه حقیقی**[1] می‌نامند.

۱۰. همجموعه‌ها. فرض کنیم H یك زیرگروه G و x عنصری از G باشد. در این‌صورت

$$Hx$$

یك **همجموعهٔ راست** G نسبت به H یا به‌طور دقیقتر **همجموعهٔ راست تولیدشده** به‌وسیلهٔ x، یا **همجموعه با مولد** x، یا همجموعهٔ راست شامل x نامیده می‌شود؛ زیرا واضح است که $x \in Hx$، چون $1 \in H$.

چنانچه $x = u$، و u عنصری از H باشد، آنگاه بنا بر قضیهٔ ۳ داریم $Hu = H$، که نشان می‌دهد خود H هم یك همجموعه است و این همجموعه را می‌توان به شق دیگر $H1$ یا به‌صورت کلیتر Hu هم نوشت، در اینجا u عنصری دلخواه از H است.

همچنان که از این ملاحظات می‌توان دریافت، دو عنصر متمایز ممکن است یك همجموعه تولید کنند. حال اگر x و y، عناصری از G باشند. ببینیم شرط لازم و کافی برای برقراری تساوی

$$Hx = Hy \tag{۱۰.۲}$$

چیست؟ اگر (۱۰.۲) برقرار باشد، آنگاه بخصوص $x = 1x \in Hy$. از این‌رو عنصری مانند u از H وجود دارد به‌قسمی که

$$x = uy$$

یا

$$xy^{-1} \in H \tag{۱۱.۲}$$

---

۱. زیرگروههای $\{1\}$ و G را زیرگروههای بدیهی یا زیرگروههای خاص G وهر زیرگروه حقیقی سره را یك زیرگروه غیربدیهی نیز می‌نامند.ـ م.

و برعکس، اگر (۱۱۰۲) برقرار باشد، آنگاه

$$Hx = Huy = Hy$$

دوهمجموعه یا هردو یکی هستند و یا هیچ عنصر مشترکی ندارند؛ به‌عبارت دیگر، اگردو همجموعه عنصر مشترکی داشته باشند، آنگاه یکی هستند. زیرا فرض کنیم

$$z \in Hx \cap Hy$$

در این‌صورت در H عناصری چون u و v وجود دارند به‌قسمی که

$$z = ux = vy$$

از این‌رو

$$xy^{-1} = u^{-1}v \in H$$

و در نتیجه $Hx = Hy$. ما این نتایج را در قضیهٔ ذیل خلاصه می‌کنیم.

قضیهٔ ۵. فرض‌کنیم H یك زیرگروه‌ازگروه G باشد. دراین‌صورت همجموعه‌های Hx و Hy متساوی‌اند اگر، و فقط اگر، $xy^{-1} \in H$. هردوهمجموعه یا یکی هستند، یا هیچ عنصر مشترکی ندارند.

بهتر است این‌مورد را از دیدگاه مجردتری هم بررسی کنیم. دو عنصر $x, y \in G$ را هم‌ارز می‌خوانیم و می‌نویسیم $y \sim x$، هرگاه عنصری چون $u \in H$ وجود داشته باشد به‌طوری‌که $x = uy$، یا با عبارتی هم‌ارز با آن، هرگاه

$$Hx = Hy$$

یعنی هرگاه x و y هردو در یك همجموعهٔ راست H قرار گیرند. واضح است که این مطلب در واقع خود تعریف یك رابطهٔ هم‌ارزی است. زیرا (i) $x \sim x$، (ii) از $y \sim x$ نتیجه می‌شود $x \sim y$، و (iii) اگر $y \sim x$ و $z \sim y$، آنگاه x، y و z همگی در یك همجموعه واقع‌اند و لذا $z \sim x$.

به‌طور کلی، وقتی که یك رابطهٔ هم‌ارزی روی یك مجموعه تعریف شده باشد، این مجموعه را می‌توان به‌صورت اجتماع زیرمجموعه‌های ازهم جدا، یعنی اجتماع همهٔ رده‌های هم‌ارزی متمایز بیان کرد. درمورد کنونی، رده‌های هم‌ارزی همجموعه‌های راست هستند ولذا G اجتماع همهٔ همجموعه‌های متمایز است. برای آنکه این نتیجه را به‌گونهٔ صوریتر بیان کنیم، ازهرهمجموعه یك نماینده انتخاب می‌کنیم. اگر t_i یکی ازاین نماینده‌ها باشد همجموعه متناظر آن را می‌توان با Ht_i نمایش داد. گردایهٔ همجموعه‌های راست متمایز ممکن است نامتناهی یا حتی ناشمارا باشد. در این حالت از یك مجموعهٔ اندیسگذار I استفاده می‌کنیم که عناصرش در تناظر یك به‌یك با همجموعه‌ها هستند. حال این واقعیت را، که G اجتماع همهٔ همجموعه‌های متمایز است، با فرمول

$$G = \bigcup_{i \in I} Ht_i \qquad (۱۲۰۲)$$

بیان می‌کنیم. تعداد هممجموعه‌های راست متمایز، یعنی عدد اصلی I، را **اندیس** H در G می‌نامند و به

$$[G:H] \tag{۱۳.۲}$$

نمایش می‌دهند. وقتی که بینهایت هممجموعهٔ راست وجود داشته باشد می‌نویسیم $[G:H]=\infty$.

گردایهٔ $\{t_i, i \in I\}$ متشکل از نماینده‌ها را یك **تراگرد** راست H در G می‌نامند. با اینکه این اندیس به‌توسط H و G کاملاً معین می‌شود، بدیهی است که **تراگرد** منحصر به‌فرد نیست. اگر یك تراگرد، مثلاً t_i، معلوم باشد، کلیترین تراگرد به‌وسیلهٔ

$$\{u_i t_i | i \in I\}$$

که در آن u_iها عناصر دلخواهی از H هستند داده می‌شود.

به روشی مشابه می‌توانیم **هممجموعه‌های چپ** H را هم مورد بررسی قراردهیم. یك هممجموعهٔ چپ نمونه، به‌صورت xH $(x \in G)$ است. و به‌آسانی می‌توان تحقیق کرد که

$$xH = yH$$

اگر، وتنها اگر، عنصری چون $v \in H$ وجود داشته باشد به‌طوری که $x = yv$، یا به‌عبارت هم‌ارز با آن

$$y^{-1}x \in H \tag{۱۴.۲}$$

مانند قبل دو هممجموعهٔ چپ یا یکی هستند، و یا هیچ عنصر مشترکی ندارند. نتیجه اینکه G را می‌توان به‌اجتماع کلیهٔ هممجموعه‌های چپ متمایز افراز کرد؛ لذا

$$G = \bigcup_{j \in J} s_j H$$

در اینجا J یك مجموعهٔ اندیسگذار است که هممجموعه‌های چپ را می‌شمرد و $\{s_j\}$ مجموعه‌ای از نماینده‌های هممجموعه‌های چپ، یا به‌اصطلاح یك تراگرد چپ H در G است. با این‌حال، به‌سادگی می‌توان دیدکه مجموعه‌های اندیسگذار I و J دارای یك عدد اصلی هستند. در واقع، با آغاز از تجزیهٔ (۱۲.۲) نشان می‌دهیم که

$$G = \bigcup_{i \in I} t_i^{-1} H \tag{۱۵.۲}$$

یك تجزیه به هممجموعه‌های چپ است. ابتدا ملاحظه می‌کنیم که هممجموعه‌های (۱۵.۲) متمایزند. زیرا اگر

$$t_i^{-1}H = t_k^{-1}H$$

نتیجه می‌گیریم که

$$(t_k^{-1})^{-1} t_i^{-1} \in H, \; t_k t_i^{-1} \in H$$

و از این‌رو $Ht_k = Ht_i$؛ که ممکن نیست مگر آنکه $i = k$. بعد، هر عنصر $x \in G$ به‌سمت

راست اجتماع (۱۵.۲) تعلق دارد. زیرا x^{-1} باید در یکی از هممجموعه‌های راست موجود در تجزیهٔ (۱۲.۲)، فرضاً در Ht_m، قرارداشته باشد. از این‌رو $x \in t_m^{-1} H$، که مبین اثبات (۱۵.۲) است، و بدین‌گونه نشان داده‌ایم که هممجموعه‌های چپ را می‌توانیم باهمان مجموعهٔ اندیسگذاری که هممجموعه‌های راست را می‌شماریم، بشماریم. یادآور می‌شویم که H خود یک هممجموعه (راست یا چپ) است. وقتی که H مانند (۷.۲) متناهی باشد، عناصر Ht عبارت‌اند از

$$u_1 t, u_2 t, \dots, u_h t$$

پس هرهممجموعه از h عنصر تشکیل می‌شود.

اکنون می‌توانیم یکی از قدیمیترین و مهمترین نتایج در باب گروههای متناهی را اثبات کنیم.

قضیهٔ اصلی۳ (لاگرانژ): فرض‌کنیم G یک گروه متناهی از مرتبهٔ g باشد. اگر H زیرگروهی از مرتبهٔ h باشد، آنگاه

(i) h، g را عاد می‌کند، یعنی، $g = nh$، و

(ii) n با اندیس $[G:H]$ برابراست. و لذا تجزیه‌هایی مانند

$$G = \bigcup_{i=1}^{n} s_i H, \quad G = \bigcup_{i=1}^{n} Ht_i \qquad (۱۶.۲)$$

وجود دارند که به‌ترتیب تجزیه‌های G برحسب هممجموعه‌های راست وچپ H هستند.

برهان. با فرض اینکه n، اندیس باشد: وجود تجزیه‌های (۱۶.۲) را قبلاً درحالت کلی اثبات کرده‌ایم. فقط باید نشان دهیم که

$$g = nh$$

این تساوی فوراً با شمارش تعداد عناصر موجود در دوطرف یکی از تجزیه‌ها به‌دست می‌آید، زیرا دیده‌ایم که هرهممجموعه شامل h عنصر است و اجتماع n هممجموعهٔ مجزا همهٔ g عنصر مجموعهٔ G را به‌ما می‌دهد.

فرع ۱. اگر G یک گروه متناهی ازمرتبهٔ g باشد، مرتبهٔ هرعنصر عاملی از g است. تمام عناصر G در معادلهٔ

$$x^g = 1$$

صدق می‌کنند.

برهان. فرض‌کنیم u عنصری از G باشد. چون G متناهی است، مرتبهٔ u نیزمتناهی و مثلاً، برابر با r است. از این‌رو عناصر

$$1, u, u^2, \dots, u^{r-1} \quad (u^r = 1)$$

یك زیر گروه دوری از مرتبهٔ r تشکیل می‌دهند. بنا برقضیهٔ لاگرانژ r، g را عاد می‌کند. و لذا با فرض اینکه s عدد صحیحی باشد که $g=sr$،

$$u^g=(u^r)^s=۱$$

فرع ۲. یك‌گروه از مرتبهٔ اول زیرگروه حقیقی ندارد و لزوماً دوری است.

برهان. فرض کنیم G یك گروه ازمرتبهٔ p و p عددی اول باشد. مرتبهٔ هرزیر گروه یا برابر با یك است و یا برابر p؛ پس این زیر گروه یا متشکل از عنصر واحد است و یا بر G منطبق.

اگر u عنصر دلخواهی از G سوای ۱ باشد، آنگاه مرتبهٔ u بزر گتر از یك وعاملی از p است. از این‌رو u از مرتبهٔ p است، و عناصر

$$۱, u, u^۲, \ldots, u^{p-۱}$$

متمایزند و بنابراین همهٔ عناصر G هستند.

مثال. در گروه مرتبـهٔ ۶، داده شده در جدول ۷، صفحهٔ ۱۵، مرتبهٔ عناصر a، b، c، d، e به‌ترتیب برابر ۳، ۳، ۲، ۲، ۲ است.

وقتی G یك گروه جمعی آبلی وH یك زیر گروه G باشد، یك هممجموعهٔ نمونهٔ H به‌صورت

$$H+x$$

نوشته می‌شود و داریم:

$$H+x=H+y$$

اگر، و فقط اگر،

$$x-y\in H$$

یا به‌صورت هم‌ارز با آن

$$x=y+u$$

که در آن u عنصری است ازH. دراین حالت گاه می گوییم که x با y به‌هنگ H همنهشت است، و می‌نویسیم

$$x\equiv y \pmod H$$

۱۱. زیرگروههای یك‌گروه دوری. ابتدا در موردگروه دوری نامتناهی

$$C: ۱\ (=x^\circ),\ x,\ x^{-۱},\ x^۲,\ x^{-۲},\ \ldots \qquad (۱۷.۲)$$

به‌بررسی می‌پردازیـم. صرفنظر از زیر گروه بدیهی $\{۱\}$ می‌توان گفت هرزیر گروه H از

C از توانهای مشخص x، بدانضمام ۱، تشکیل می‌شود، ازاین‌رو

$$H: 1,\ x^{a},\ x^{b},\ \ldots$$

که در آن a و b اعداد صحیح مثبت یا منفی هستند. چون وقتی x^{a} عنصر H باشد x^{-a} نیز عنصر H است، نتیجه می‌گیریم هر زیرگروه حقیقی C شامل حداقل یك توان x با توان مثبت است. ازاین‌رو در H توانی از x باکوچکترین نمای مثبت: مثلاً x^{m}، وجود دارد. درنتیجه، H شامل تمام عناصری است که به‌شکل

$$x^{mq}(q=0,\ \pm 1,\ \pm 2,\ \ldots) \tag{۱۸.۲}$$

هستند. یعنی H گروه دوری با مولد x^{m} را در بر دارد. ما ادعا می‌کنیم که به‌غیر ازعناصری که در (۱۸.۲) فهرست شده‌اند عنصر دیگری در H وجود ندارد. زیرا فرض‌کنیم x^{a} عنصری از H باشد. a را بر m تقسیم می‌کنیم، لذا

$$a=mq+r$$

که در آن $0 \leqslant r < m$. دراین صورت

$$x^{a}=x^{mq}x^{r}$$

$$x^{a}x^{-mq}=x^{r}$$

چون دوعامل سمت چپ به H تعلق دارند، درنتیجه x^{r} هم عنصری از H می‌شود. اما این امر بـا حـداقل بودن m مغایرت دارد، مگر آنکـه $r=0$. ازاین‌رو $a=mq$، یعنی (۱۸.۲) تمام عناصر H را در بر دارد. می‌بینیم که هر زیرگروه حقیقی ازیك گروه دوری نامتناهی، خود نیز یك گروه دوری نامتناهی است وبنابراین با C یکریخت است.

وقتی‌که بـا زیرگروههای یـك گروه دوری متناهی سروکار داریم وضعیت جالبتر می‌شود. این نتیجه درقضیهٔ ذیل خلاصه می‌شود.

قضیهٔ اصلی ۴. فرض کنیم

$$C: 1,\ x,\ x^{2},\ \ldots,\ x^{g-1}(x^{g}=1) \tag{۱۹.۲}$$

یك گروه دوری ازمرتبهٔ g باشد. دراین صورت متناظر با هر مقسوم‌علیه h از g یك وفقط یك زیرگروه ازمرتبهٔ h وجود داردکه می‌تواند به وسیلهٔ $x^{g/h}$ تولید شود.

برهان. (i) فرض‌کنیم $g=hn$. عناصر

$$1,\ x^{n},\ x^{2n},\ \ldots,\ x^{(h-1)n} \tag{۲۰.۲}$$

متمایزند، زیرا هرتساوی بین آنها منجر به‌رابطه‌ای مانند

$$x^{ln}=1$$

می‌شود که در آن

$$\circ < ln < hn (= g)$$

که با فرض اینکه x ازمرتبهٔ g است در تناقض می‌باشد. پس (۲۰.۲) زیرگروهی ازمرتبهٔ h تشکیل می‌دهد که بەوسیلهٔ عنصر x^n از مرتبهٔ h تولید می‌شود.

(ii) برعکس، فرض کنیم $h|g$؛ فرضاً $g = hn$. همچنین فرض کنیم

$$H : ۱, u_۲, u_۳, \ldots, u_{h-۱}$$

یك زیرگروه ازمرتبهٔ h باشد. هر u_i توانی است از x. پس مثلاً

$$u_i = x^{\lambda_i}, \quad (i = ۲, ۳, \ldots, h-۱)$$

که در آن λ_i عددی است صحیح که درنامساویهای

$$\circ < \lambda_i < g$$

صدق می‌کند. چون H ازمرتبهٔ h است، فرع ۱ ایجاب می‌کند که

$$u_i^h = ۱$$

یعنی

$$x^{h\lambda_i} = ۱$$

بنا به فرع ۱، صفحهٔ ۳۹ نتیجه می‌گیریم که $g|h\lambda_i$. از این‌رو اعداد صحیحی چون k_i وجود دارند که

$$h\lambda_i = k_i g = k_i hn$$

$$\lambda_i = k_i n$$

این امر ثابت می‌کند که هرعنصر H توانی از x^n است. فقط h تا ازاین توانها متمایزند و این توانها در (۲۰.۲) فهرست شده‌اند. پس H زیرمجموعه‌ای از (۲۰.۲) است، اما چون H ازمرتبهٔ h است، باید با مجموعهٔ داده شده در (۲۰.۲) یکی باشد. این ثابت می‌کند که مجموعهٔ (۲۰.۲) تنها زیرگروه G است که ازمرتبهٔ h است.

۱۲. اشتراکها و مولدها. ساختار یك گروه اغلب به وسیلهٔ مطالعهٔ زیرگروههایش روشن می‌شود. بنابراین داشتن روشهایی برای ساختن زیرگروهها حائز اهمیت است.

واضح است که اگر $H \leqslant G$ و $K \leqslant H$، آنگاه $K \leqslant G$. حال، اگر H و K زیرگروههای G باشند، اشتراك آنها

$$D = H \cap K$$

نیز یك زیرگروه G است. زیراکه اگر x و y متعلق به D باشند، داریم $x, y \in H$ و

$x, y \in K$، بنابراین، $xy \in H$ و $xy \in K$، یعنی $xy \in D$؛ همچنین $1 \in D$، زیرا $1 \in H$ و $1 \in K$؛ بالاخره اگر $x \in D$، آنگاه $x^{-1} \in H$، $x^{-1} \in K$ و بنابراین $x^{-1} \in D$، که ثابت می‌کند D یك زیرگروه است. درحالت کلیتر، اشتراك هرتعداد از زیرگروهها

$$H \cap K \cap L \cap \cdots$$

هم یك زیرگروه است.

ازسوی دیگر، اجتماع دو زیرگروه H و K، یعنی

$$H \cup K$$

درحالت کلی، یك زیرگروه نیست. زیرا اگر $u \in H$ و $v \in K$، هیچ دلیلی در دست نیست که فکر کنیم uv یا در H قرار می‌گیرد یا در K و درنتیجه در $H \cup K$. برای به دست آوردن «کوچکترین» زیرگروهی که هم شامل H باشد و هم شامل K، بنای پیچیده‌تری مورد نیاز است.

فرض کنیم

$$a, b, c, \cdots \tag{۲۱.۲}$$

گردایه‌ای ازعناصر G باشد؛ مجموعهٔ تمام حاصلضربهای متشکل از تعداد متناهی عامل، احیاناً تکراری، منتخب از عناصر (۲۱.۲) یا عکسهایشان، مثلاً $a^2b^{-1}cab$، را در نظر می‌گیریم. به‌این حاصلضربها همواره حاصلضرب «تهی» را هم که با عنصر واحد G یکی گرفته می‌شود ضمیمه می‌کنیم. واضح است که مجموعهٔ این حاصلضربها تشکیل یك گروه می‌دهد. زیرا اگر دوتا از این حاصلضربهای با تعداد متناهی عامل، درهم ضرب شوند حاصلضرب دیگری ازاین نوع به‌دست می‌آید؛ وعکس یك حاصلضرب نیز به‌این مجموعه تعلق دارد. گروهی که بدین طریق ساخته می‌شود با

$$\mathrm{gp}\{a, b, c, \cdots\} = M \tag{۲۲.۲}$$

نشان داده می‌شود، و گروه با مولدهای a، b، c، ... نام دارد. آشکار است که هر گروهی که شامل عناصر (۲۱.۲) باشد باید شامل M نیز باشد و لذا این حکم که، M کوچکترین زیرگروه شامل این‌عناصر است، توجیه می‌شود. به‌بیان دیگر می‌توان گفت که M اشتراك تمام زیرگروههایی است که شامل عناصر (۲۱.۲) هستند. البته ممکن است نتیجه شود که $M = G$.

عناصر a، b، c، ... **مولدهای** M نامیده می‌شوند. با این حال، باید متذکر شد که مولدها نه منحصر به‌فردند و نه، درحالت کلی، غیر زاید فرض می‌شوند. برای مثال، مولد a زاید خواهد بود هرگاه

$$a \in \mathrm{gp}\{b, c, \cdots\}$$

که درچنین حالتی می‌توانیم به‌جای (۲۲.۲) قرار دهیم

$$M = \mathrm{gp}\{b, c, \ldots\}$$

نظر ما عمدتاً متوجه گروههایی است که از عناصر متناهی تولید شده‌اند. روشن است که چنین گروهی همواره دارای یك مجموعهٔ غیر زاید ازمولدهاست. در واقع می‌توان با هر مجموعه ازمولدها شروع، و عناصری را که می‌توانند برحسب مولدهای دیگر بیان شوند حذف کرد.

هر گروه G را می‌توان به‌شکل (۲۲.۲) بیان کرد؛ مثلاً روشن است که می‌توانیم تمام عناصر G را به‌عنوان مولدهای G تلقی کنیم ومتعاقب آن درصورت تمایل، مولدهای زاید را حذف نماییم. برای اکثر مقاصد عملی، کاهش تعداد مولدها تا سرحد امکان مورد نظر است.

گروهی که فقط یك مولد، x، داشته باشد گروه دوری با مولد x است، که دراین صورت می‌تواند به‌صورت $\mathrm{gp}\{x\}$ نوشته شود. برای روشن کردن این مطلب بار دیگر به گروه مرتبهٔ ۶ $(G(\cong S_۳)$ که درجدول (v) صفحهٔ ۱۵ نمایش داده شده، رجوع می‌کنیم. می بینیم که هریك ازشش عنصر آن را می‌توانیم برحسب a و c بیان کنیم، پس

$$۱ = c^۲(= a^۳),\ a = a,\ b = a^۲,\ c = c,\ d = ca,\ e = ca^۲ \qquad (۲۳.۲)$$

ازاین‌رو دراین حالت می‌توانیم بنویسیم

$$G = \mathrm{gp}\{a, c\} \qquad (۲۴.۲)$$

به‌طریق دیگر، می‌توان نشان داد که

$$G = \mathrm{gp}\{b, d\} \qquad (۲۵.۲)$$

زیرا a و c و لذا تمام عناصر گروه را می‌توان برحسب b و d بیان کرد، یعنی

$$a = b^۲, \quad c = db$$

مولدهای (۲۴.۲) و (۲۵.۲) یقیناً غیر زاید هستند، زیرا گروه مورد بحث غیرآبلی بوده، لذا نمی‌توان آن را به‌توسط فقط یك عنصر تولید کرد، چه دراین صورت دوری و بنابراین آبلی خواهد بود.

با این حال، خاطرنشان می‌شود که مولدهای غیر زاید ممکن است به‌وسیلهٔ روابطی غیربدیهی باهم در ارتباط باشند و این امر حائز اهمیت‌است. ازاین‌رو با مراجعه به‌جدول (v) می‌بینیم

$$ac = ca^۲ \qquad (۲۶.۲)$$

که با رابطهٔ

$$(ac)^۲ = ۱ \qquad (۲۶.۲)'$$

هم‌ارز است. زیرا

$$(ac)^۲ = acac = acca^۲ = a۱a^۲ = a^۳ = ۱$$

حل هریك ازاین معادلات به قسمی که یکی ازمولدها برحسب دیگری بیان شود، غیرممکن است. معادله‌ای‌نظیر (۲۶.۲) یا $'$(۲۶.۲) یك رابطهٔ معرف نامیده می‌شود. اغلب مصلحت این است که یك گروه خاصی را به توسط مجموعه‌ای ازمولدها و مجموعه‌ای از روابط معرف مشخص سازیم. ما بعداً (فصل ۵) با تفصیل بیشتری به‌این اصل باز می گردیم. اما اینجا درموردکنونی متذکر می‌شویم که معادلات

$$a^۳ = c^۲ = (ac)^۲ = ۱ \tag{۲۷.۲}$$

به‌عنوان مجموعه‌ای از روابط معرف به‌کار گرفته می‌شوند. در واقع، اطلاعات موجود در (۲۷.۲) برای ساختن کل جدول‌ضرب کافی است. ابتدا متذکر می‌شویم که شش عنصر

$$۱,\ a,\ a^۲,\ c,\ ca,\ ca^۲ \tag{۲۸.۲}$$

یقیناً متمایزند؛ برای مثال، اگر a مساوی $ca^۲$ می‌بود، نتیجه می‌شد $c = a^{-۱}$، که بـا این حقیقت‌که a و c مولدهای غیر زاید هستند، متناقض است. بعد، به‌موجب روابط (۲۷.۲) می‌توان تحقیق‌کرد که دستگاه (۲۸.۲) نسبت به‌ضرب بسته است؛ برای مثال

$$(ca)(ca^۲) = c(ac)a^۲ = cca^۲a^۲ = c^۲a^۴ = a$$
$$a^۲c = a(ac) = aca^۲ = ca^۴ = ca$$

وهمین‌طور برای بقیهٔ عناصر، که درآنها به‌موجب (۲۶.۲) یك عامل c منظماً به‌سمت چپ حرکت داده شده، تا اینکه حاصلضرب با یکی ازعناصر (۲۸.۲) مساوی شده است. با این قرارداد، جدول‌ضرب کامل چنین خواهد شد:

جدول (vii)

	۱	a	$a^۲$	c	ca	$ca^۲$
۱	۱	a	$a^۲$	c	ca	$ca^۲$
a	a	$a^۲$	۱	$ca^۲$	c	ca
$a^۲$	$a^۲$	۱	a	ca	$ca^۲$	c
c	c	ca	$ca^۲$	۱	a	$a^۲$
ca	ca	$ca^۲$	c	$a^۲$	۱	a
$ca^۲$	$ca^۲$	c	ca	a	$a^۲$	۱

واین صورت دیگری است ازگروهی که اول بار، درجدول (vi) صفحهٔ ۱۵ ارائه شده‌است.
اگر A، B، C، . . . زیرمجموعه‌هایی ازگروه G باشند، گروهی که اینها تولید می کنند با

$$\mathrm{gp}\,\{A,\ B,\ C,\ \cdots\} \qquad *$$

نشان داده شده و به‌عنوان گروهی متشکل از حاصلضربهای متناهی تعریف می‌شود که در آن هرعامل عنصری از A یا B یا C، . . . ویا عکس چنین عنصری است با ترتیبی دلخواه که با تکرار یا بدون تکرار انتخاب شده‌اند. هرگاه همهٔ عناصر $A\cup B\cup C\cup\cdots$ را به‌عنوان مولد بگیریم، مفهوم فوق همان مفهوم قبلی مولدها را به‌دست می‌دهد. به‌جای(*) می‌توان همچنین نوشت

$$\mathrm{gp}\,\{A\cup B\cup C\cup\cdots\}.$$

البته اگر A یك زیرگروه باشد خواهیم داشت: $A=\mathrm{gp}\,\{A\}$.

۱۳. حاصلضرب مستقیم. اینك روش ساده‌ای را برای ساختن یك گروه جدید از دوگروه مفروض مورد بحث قرار می‌دهیم. فرض کنیم H و K دوگروه دلخواه باشند و مجموعهٔ تمام زوجهای مرتب

$$(u,\ v),$$

راکه درآن u و v به‌ترتیب در H و K تغییرمی‌کنند، موردبررسی قرارمی‌دهیم. مجموعهٔ این زوجهای مرتب با

$$G=H\times K$$

نشان داده می‌شود و**حاصلضرب مستقیم (خارجی)** H وK نامیده می‌شود. با تخصیص قانون ترکیب

$$(u,\ v)(u',\ v')=(uu',\ vv') \qquad (۲۹.۲)$$

به‌مجموعهٔ G، این مجموعه به یك گروه تبدیل می‌شود. به‌آسانی تحقیق می‌شودکه قانون شرکتپذیری در G برقرار است. زیرا عمل ضرب در H و K شرکتپذیر است. عنصرواحد G عبارت است از زوج مرتب

$$(1_H,\ 1_K)$$

که درآن 1_H و 1_K به‌ترتیب عناصر واحد H و K هستند. همچنین

$$(u,\ v)^{-1}=(u^{-1},\ v^{-1})$$

اگر H و K گروههایی متناهی وبه‌ترتیب ازمراتب h و k باشند، آنگاه $H\times K$ گروهی ازمرتبهٔ hk خواهد بود.

درحالت کلیتر، اگر H_1، H_2، . . .، H_r گروههایی دلخواه باشند، حاصلضرب مستقیم

$$H_1\times H_2\times\cdots\times H_r$$

آنها از تمامی r-تایی‌های

$$(u_۱, u_۲, \cdots, u_r)$$

تشکیل می گردد که در آن $(i=۱, ۲, \cdots, r)u_i \in H_i$ وضرب درهر مؤلفهٔ r-تایی انجام می گیرد. واضح است که اگر هر H_i متناهی باشد، آنگاه

$$|H_۱ \times H_۲ \times \cdots \times H_r| = \prod_{i=۱}^{r} |H_i|$$

گاهی اتفاق می‌افتد که یك گروه G ، با حاصلضرب مستقیم دو زیرگروه خودش، H و K ، یکریخت می‌شود؛ بنابراین، می نویسیم

$$G \cong H \times K \qquad (۳۰.۲)$$

ویا با استفادهٔ اندك نابجا ازنماد، می‌نویسیم

$$G = H \times K \qquad (۳۰.۲)'$$

این وضعیت درموارد ذیل پیش می‌آید:

(۱) زیرگروههای H و K عنصر به عنصر با هم تعویضپذیرند. یعنی، اگر u و v بترتیب عناصر دلخواهی از H و K باشند، آنگاه

$$uv = vu \qquad (۳۱.۲)$$

(۲) هرعنصر $x \in G$ را می‌توان به‌صورت $x = uv$ ویا مختصرتر به‌صورت

$$G = HK \qquad (۳۲.۲)$$

بیان کرد.

(۳) اشتراك H و K عنصر واحد است، یعنی

$$H \cap K = ۱ \qquad (۳۳.۲)$$

یادآور می‌شویم که (۲) و (۳) با شرط یگانهٔ ذیل، هم‌ارزند:

('۲) هرعنصر $x \in G$ را می‌توان منحصراً به‌یك طریق به‌صورت $x = uv$ تجزیه‌کرد که در آن $u \in H$ و $v \in K$.

زیرا با پذیرفتن (۲) و (۳)، فرض می کنیم دوتجزیهٔ

$$x = uv = u_۱ v_۱$$

داشته باشیم. دراین صورت

$$u_۱^{-۱} u = v_۱ v^{-۱} \qquad (۳۴.۲)$$

و عنصرسمت چپ (۳۴.۲) متعلق به H وعنصر سمت راست آن متعلق به K است و بنابراین،

به‌موجب (۳)، لازم می‌آید که این عنصر برابر ۱ باشد. لذا $u=u_1$ و $v=v_1$، که یکتایی تجزیه را، همچنان‌که در ($'$۲) مورد نیاز است، به‌اثبات می‌رساند.

برعکس، فرض کنیم ($'$۲) برقرار باشد و $w \in H \cap K$. در این صورت $w=1w=w1$ دوتجزیهٔ w با عواملی به‌ترتیب از H و K می‌باشند؛ و ازشرط یکتایی نتیجه می‌گیریم که $w=1$.

شرط مذکور آشکارا بیان می‌کند که هرعنصر $x \in G$ به‌گونه‌ای منحصر به‌فرد زوج مرتبی مانند (u, v) را، که درآن $u \in H$ و $v \in K$، معین می‌کند و چنین زوجهای مرتبی وجود دارند، زیرا (u, v) متناظر با حاصلضرب $x=uv$ می‌باشد. تناظر

$$x\theta=(uv)\theta=(u, v)$$

یکریختی (۳۰.۲) را برقرار می‌کند. زیرا به‌موجب (۱) داریم

$$(uv)(u'v')\theta=(uu' vv')\theta=(uu', vv')$$

به‌طریق مشابه، داریم

$$G \cong H_1 \times H_2 \times \cdots \times H_r$$

که درآن H_i ها $(i=1, 2, \ldots, r)$ زیرگروههایی از G هستند، هرگاه شرایط ذیل برقرار باشند

(۱) هردوگروه H_i و H_j عنصر به‌عنصر تعویض‌پذیر باشند.

(۲) هرعنصر x از G را بتوان به‌صورت

$$x=u_1u_2\cdots u_r \qquad (۳۵.۲)$$

که درآن $u_i \in H_i$، بیان کرد.

$$H_i \cap H_1H_2\cdots H_{i-1}H_{i+1}\cdots H_r=\{1\} \qquad (۳)$$

یا به‌بیان دیگر به‌جای (۲) و (۳)، می‌توانیم بگذاریم

($'$۲) تجزیهٔ (۳۵.۲) به‌طور منحصر به‌فرد صورت می‌گیرد بخصوص، اگر

$$u_1u_2\cdots u_r=1$$

از ($'$۲) نتیجه می‌شود که

$$u_1=u_2=\cdots=u_r=1$$

زیرا $1\ldots 11=1$ تنها تجزیهٔ ۱ است.

وقتی گروهی به‌صورت حاصلضرب مستقیم زیرگروههایش بیان شود ما آن را یك **حاصلضرب مستقیم داخلی** می‌نامیم.

مثال. کوچکترین مانده‌های مثبت متباین به‌هنگ ۱۵ عبارت‌اند از

$$۱,\ ۲,\ ۴,\ ۷,\ ۸,\ ۱۱,\ ۱۳,\ ۱۴ \tag{۳۶.۲}$$

این مانده‌ها تشکیل یك گـروه آبلی مرتبهٔ ۸ می‌دهند (صفحهٔ ۱۳ ملاحظه شود) و چنانکه خواهیم دیـد با حاصلضرب مستقیم گروههای دوری با مولدهای ۲ و ۱۱ یکریخت است زیرا ماندهٔ ۲ گروهی دوری ازمرتبهٔ ۴، یعنی گروه

$$C_۴:\ ۱,\ ۲,\ ۴,\ ۸\ (۲^۴=۱۶\equiv ۱\ (\mathrm{mod}\ ۱۵))$$

را تولید می‌کند. به‌طریق مشابه، ۱۱ یك‌گروه دوری ازمرتبهٔ ۲

$$C_۲:\ ۱,\ ۱۱\ (۱۱^۲=۱۲۱\equiv ۱\ (\mathrm{mod}\ ۱۵))$$

را تولید می‌کند. چون تمامی گروه آبلی است، باید فقط شرایط (۲) و (۳) ازصفحهٔ ۴۷ را بررسی کنیم.وقتی که تمام حاصلضربهای‌ممکن را حساب‌کنیم، به‌دست می‌آوریم:

$$۱,\ ۲,\ ۴,\ ۸,\ ۱۱,\ ۲۲,\ ۴۴,\ ۸۸$$

که پس ازتبدیل به‌هنگ ۱۵ چنین می‌شود

$$۱,\ ۲,\ ۴,\ ۸,\ ۱۱,\ ۷,\ ۱۴,\ ۱۳$$

چون این‌گروه‌کاملی است، شرط (۲) برقرار است، و فوراً ملاحظه می‌کنیم‌که

$$C_۴\cap C_۲=\{۱\}$$

این تساوی نشان می‌دهد‌که این‌گروه با $C_۴\times C_۲$ یکریخت است.

از قضیهٔ سادهٔ ذیل، کـه مستقلاً مورد توجه ما خواهد بـود، دربخش آتیه استفاده خواهد شد.

قضیهٔ ۶. فرض کنیم G گروهی متناهی باشد که همهٔ عناصرش درمعادلهٔ

$$x^۲=۱ \tag{۳۷.۲}$$

صدق کنند، یعنی هرعنصرآن، به‌استثنای عنصر واحد، از مرتبهٔ ۲ باشد. دراین صورت G با یك گروه آبلی از نوع

$$C_۲\times C_۲\times\cdots\times C_۲$$

یکریخت است، و بنابراین مرتبهٔ G توانی از ۲ است.

برهان. بنابرفرع ۲،صفحهٔ ۴۵،وقتی‌که G (تنها) گروه مرتبهٔ ۲ باشد،قضیه بالبداهه برقرار است. پس فرض می‌کنیم G ازمرتبهٔ بزرگتر از ۲ و a و b عناصرمتمایزی از G،

غیر از ۱ باشند. بنابر فرض

$$a^{۲}=b^{۲}=۱$$

و لذا

$$a=a^{-۱},\ b=b^{-۱}$$

حال، عنصر ab را درنظر می‌گیریم. بنابر (۳۷.۲)، $(ab)^{۲}=۱$، از اینجا نتیجه می‌شود

$$ab=(ab)^{-۱}=b^{-۱}a^{-۱}=ba$$

این رابطه نشان می‌دهد که G آبلی است. فرض کنیم $u_{۱}$، $u_{۲}$، ...، u_{r} مجموعه‌ای از مولدهای غیر زاید G باشند. چون G آبلی است، حاصلضرب مولدها را می‌توان چنان مرتب کرد که هرعنصر بتواند به‌شکل «نرمال»

$$u_{۱}^{k_{۱}}u_{۲}^{k_{۲}}\cdots u_{r}^{k_{r}} \qquad (۳۸.۲)$$

درآید. اما بنابر (۳۷.۲) نماهای موجود در (۳۸.۲) به مقادیر ۰ و ۱ محدودند. دراین صورت همهٔ حاصلضربها متمایزند؛ زیرا وجود تساوی بین دو تا ازاین‌گونه حاصلضربها به‌رابطه‌ای مانند

$$u_{۱}^{l_{۱}}u_{۲}^{l_{۲}}\cdots u_{r}^{l_{r}}=۱$$

منجر می‌شود که درآن هر l_i یا ۰ است یا واحد. این امر ما را قادر می‌سازد که یکی از مولدها را برحسب بقیه بیان کنیم و این امر با غیرزاید بودن مولدها متناقض است. لذا صورت نرمال (۳۸.۲) منحصر به‌فرد است، یعنی می‌توانیم بنویسیم

$$G=\mathrm{gp}\{u_{۱}\}\times \mathrm{gp}\{u_{۲}\}\times\cdots\times \mathrm{gp}\{u_{r}\}$$

و ازاین رو

$$G\cong C_{۲}\times C_{۲}\times\cdots\times C_{۲}$$

(r عامل).

۱۴. بررسی گروههای تا مرتبهٔ ۸. تاکنون هیچ روش موفقیت‌آمیزی برای ساختن تمام گروههای مجرد ممکن ازمراتب موردنظر کشف نگردیده است؛ همچنین، جز درچند مورد ساده، ازقبل نمی‌دانیم که چند گروه از هرنوع وجود دارد.

اما وسایل اولیه‌ای که تاکنون فراهم کرده‌ایم، برای ارائه فهرست کاملی ازگروههایی که مرتبهٔ آنها بیش از هشت نیست کفایت می‌کنند. چون تاکنون گروههای مرتبهٔ اعداد اول مورد بحث قرار گرفته‌اند(فرع ۲، صفحهٔ ۴۵) فقط حالاتی‌راکه درآنها مرتبهٔ g برابر

۴ یا ۶ یا ۸

باشد به‌تفصیل مورد بحث قرار می‌دهیم.

دوگروه مرتبهٔ ۴ وجود دارند که هردو آبلی هستند.

زیرا اگر $g=۴$، آنگاه هر عنصر غیر از ۱ فقط می‌تواند یا از مرتبهٔ ۴ و یا از مرتبهٔ ۲ باشد (فرع ۱، صفحهٔ ۳۹).

(۱) اگر G شامل یك عنصر ازمرتبهٔ ۴ باشد، آنگاه این عنصر G را تولید می‌کند؛ زیرا، چهارعنصر G عبارت بخواهند بود از

$$۱,\ a,\ a^{۲},\ a^{۳}\ (a^{۴}=۱)$$

و داریم $G=C_{۴}$، گروه دوری مرتبه ۴ خواهد بود.

(۲) در غیر این‌صورت، فرض می‌کنیم G هیچ عنصری از مرتبهٔ ۴ نداشته باشد. پس کلیهٔ عناصر، به‌استثنای ۱، ازمرتبه ۲ هستند و ازقضیهٔ ۶ نتیجه می‌گیریم که

$$G=C_{۲}\times C_{۲}$$

لذا G به‌توسط دوعنصر a و b تولید می‌شود و چهارعنصر G عبارت‌اند از

$$۱,\ a,\ b,\ ab \qquad (۳۹.۲)$$

که درآن

$$a^{۲}=b^{۲}=۱,\ ab=ba \qquad (۴۰.۲)$$

این گروه، **گروه چارینه**، نامیده می‌شود (گروه چهارعنصری ف. کلاین[1]) و اغلب بـا V نشان داده می‌شود.[2]

چون هیچ‌حالت ممکن دیگری وجود ندارد، نتیجه می‌گیریم که هرگروه مرتبهٔ ۴ یا با $C_{۴}$ ویا با $V(\cong C_{۲}\times C_{۲})$ یکریخت است. جدولهای ضرب این گروهها با نمادهای دیگری در (iii) و (iv) ؛ صفحهٔ ۱۴ ارائه شده‌اند.

دوگروه مرتبهٔ ۶ وجود دارند که یکی دوری و دیگری غیرآبلی است.

(۱) اگر G دارای عنصری مانند a ازمرتبهٔ ۶ باشد، آنگاه

$$G=\mathrm{gp}\,\{a\}=C_{۶}$$

(۲) درغیر این‌صورت، فرض می‌کنیم G هیچ عنصر مرتبه ۶ نداشته باشد. بنابراین مرتبهٔ هـرعنصر بجز ۱، برابر ۲ یـا ۳ است (فرع ۱، صفحهٔ ۳۹). چون مرتبهٔ G توانی از ۲ نیست همهٔ عناصر آن نمی‌توانند در (۳۷.۲) صدق کنند. ازاین‌رو حداقـل یك عنصرمانند a ازمرتبه ۳ وجود دارد به‌طوری که عناصر

$$۱,\ a,\ a^{۲} \qquad (۴۱.۲)$$

---

1. F. Klein

۲. V حرف اول کلمهٔ آلمانی *Vier* و به‌معنی چهار است.ـــم.

سه عنصر متمایز G هستند و

$$a^۳ = ۱ \qquad (۴۲.۲)$$

اگر c عنصر دیگری از G باشد، همان گونه که درصفحهٔ ۴۵ در ارتباط با عناصر مذکور در (۲۸.۲) اشاره کردیم، شش عنصر

$$۱,\ a,\ a^۲,\ c,\ ca,\ ca^۲ \qquad (۴۳.۲)$$

متمایزند.

اگر بخواهیم که عناصر (۴۳.۲) تشکیل یك گروه مرتبهٔ ۶ بدهند، باید بنداشت بستاری برقرار باشد. بویژه، باید $c^۲$ یکی از این عناصر باشد. ما نمی‌توانیم معادله‌ای به صورت $c^۲ = ca^i$ $(i = ۰, ۱, ۲)$ داشته باشیم، زیرا ازچنین معادله‌ای حاصل می‌شود که c به مجموعهٔ (۴۱.۲) تعلق دارد. فقط سه امکان ذیل باقی می‌ماند

$$(\alpha)\, c^۲ = ۱,\quad (\beta)\, c^۲ = a,\quad (\gamma)\, c^۲ = a^۲ \qquad (۴۴.۲)$$

در شرایط (β) و (γ)، مرتبهٔ عنصر c نمی‌تواند ۲ باشد و بنابراین باید ۳ باشد. اما با ضرب (β) و (γ) ازچپ در c به ترتیب به دست می‌آوریم $ca = ۱$ و $ca^۲ = ۱$، که هیچ یك درست نیست. ازاین‌رو نتیجه می‌گیریم که باید (α) برقرار باشد، یعنی

$$c^۲ = ۱ \qquad (۴۵.۲)$$

حال ac را درنظر می‌گیریم. این عنصر باید برابر یکی ازعناصر (۴۳.۲) باشد. چون نمی‌تواند برابر c یا برابر توانی از a باشد، حالات دیگری که برای ما می‌مانند عبارت‌اند از

$$ac = ca,\ \text{یا}\ \ ac = ca^۲ \qquad (۴۶.۲)$$

اگر تساوی اولی برقرار باشد گروه آبلی می‌شود. بیاییم در این حالت مرتبهٔ ac را پیدا کنیم. بدین طریق

$$(ac)^۲ = a^۲c^۲ = a^۲ \neq ۱,\quad (ac)^۳ = a^۳c^۳ = c^۳ = c \neq ۱$$

و عنصر ac بالاجبار ازمرتبهٔ ۶ می‌شود که با مفروضات اولیه‌مان مغایرت دارد. ازاین‌رو باید معادلهٔ دوم (۴۶.۲) برقرار باشد، یعنی

$$ac = ca^۲\text{، یا، هم‌ارز با آن، } (ac)^۲ = ۱.$$

به (۲۶.۲) و $'$(۲۶.۲) مراجعه می‌کنیم. به‌طورخلاصه می‌توانیم بگوییم که اگر گروهی از مرتبهٔ ۶ غیر از $C_۶$ وجود داشته باشد، آنگاه

$$G = \mathrm{gp}\,\{a,\ c\}$$

مشروط برآنکه روابط

$$a^3=c^2=(ac)^2=1$$

برقرار باشند، که این روابط وجود چنین گروهی را اثبات نمی‌کنند. اما اتفاقاً می‌دانیم که چنین‌چیزی وجود دارد، در واقع جدول‌ضرب این گروه درصفحهٔ ۴۵ نشان داده شده است. بدین‌گونه می‌بینیم که دقیقاً دوگروه مرتبهٔ ۶ وجود دارند.

پنج‌گروه مرتبهٔ ۸ وجود دارند، که ازمیان آنها سه تا آبلی هستند و دوتا غیرآبلی.

سه‌گروه آبلی مرتبهٔ ۸ را به‌سادگی می‌توان نوشت، بدین قرار:

(۱) $C_8=\mathrm{gp}\,\{a\}$، که درآن $a^8=1$ (جدول (viii) صفحهٔ ۵۵).

(۲) $C_4\times C_2=\mathrm{gp}\,\{a\}\times\mathrm{gp}\,\{b\}$، که در آن $a^4=b^2=1$، $ab=ba$. (جدول (ix) صفحهٔ ۵۶).

(۳) $C_2\times C_2\times C_2=\mathrm{gp}\,\{a\}\times\mathrm{gp}\,\{b\}\times\mathrm{gp}\,\{c\}$، که درآن $a^2=b^2=c^2=1$، $ab=ba$، $bc=cb$، $ca=ac$. (جدول (x)، صفحهٔ ۵۶).

با توجه به‌نظریهٔ کلی گروهها، که در فصل ۴ مطالعه خواهیم کرد، نتیجه خواهد شد که همهٔ گروههای آبلی ممکن از مرتبهٔ ۸ همینها هستند، اما در اینجا این نتیجه را از اصول نخستین به‌دست می‌آوریم. اگر گروه شامل عنصری از مرتبهٔ ۸ باشد، آن گروه باید گروه C_8 باشد، و اگر تمام عناصر آن، بجز ۱، ازمرتبهٔ ۲ باشند، آنگاه آن گروه با گروه (۳) یکریخت است.

ازاین‌رو فرض می‌کنیم که هرعنصر، غیر ازمرتبهٔ ۴ باشد یا ازمرتبهٔ ۲ و حداقل یك عنصر مانند a ازمرتبهٔ ۴ وجود دارد که

$$a^4=1,\ a^2\neq 1 \qquad (۴۷.۲)$$

اگر b عنصری ازگروه غیرواقع در $\mathrm{gp}\,\{a\}$ باشد، آنگاه هشت عنصر

$$1,\ a,\ a^2,\ a^3,\ b,\ ab,\ a^2b,\ a^3b \qquad (۴۸.۲)$$

متمایزند و بنابراین همهٔ گروه را تشکیل می‌دهند، هرگاه چنین گروهی وجود داشته باشد.

اما b^2 باید یکی ازاین‌عناصر باشد و درحقیقت باید یکی ازچهارعنصرنخست باشد، زیرا b برابر توانی از a نیست. باید معادلات $b^2=a$ و $b^2=a^3$ کنار گذاشته شوند، زیرا این معادلات ایجاب می‌کنند که b ازمرتبهٔ ۸ باشد. ازاین‌رو حالات ممکنی که باقی می‌مانند عبارت‌اند از

$$(\alpha)\ b^2=1 \quad \text{یا} \quad (\beta)\ b^2=a^2 \qquad (۴۹.۲)$$

(α): فرض‌کنیم $b^2=1$. حاصلضرب ba باید برابر یکی از سه عنصر آخر در (۴۸.۲) باشد.

(α, i): اگر $ba=ab$ ، گروه آبلی است و همان گروه مذکور در (۲) می‌باشد.
(α, ii): اگر $ba=a^{۲}b$ ، می‌توان نتیجه گرفت که $b^{-۱}a^{۲}b=a$ ، که ازاین رابطه چنین به‌دست می‌آید

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

که غیرممکن است. ازاین رو باید نتیجه بگیریم که

(α, iii): $ba=a^{۳}b$ ؛ یا، معادل با آن، $(ab)^{۲}=۱$.

گروهی که با روابط

$$a^{۴}=b^{۲}=(ab)^{۲}=۱ \qquad (۵۰.۲)$$

تعریف شده در حقیقت موجود است. این گروه به $D_{۴}$ نشان داده شده و **گروه دو وجهی** مرتبهٔ ۸ نامیده می‌شود (جدول (xi) صفحهٔ ۵۷). این گروه تعلق به‌رده‌ای از گروهها دارد که بعداً (صفحهٔ ۵۷)، هنگامی که قانون شرکت‌پذیری مورد تأیید باشد، مورد بحث قرار خواهد گرفت (همچنین تمرین ۷، صفحهٔ ۶۱ ملاحظه شود).
(β): فرض کنیم $b^{۲}=a^{۲}$. دراین حالت a و b هردو از مرتبهٔ ۴ هستند. باز، ba باید یکی از سه‌عنصر آخر در (۴۸.۲) باشد که به‌ترتیب مورد بررسی قرار می‌دهیم:
(β, i): اگر $ba=ab$ ، گروه آبلی است. عنصر $c=ab^{-۱}$ از مرتبهٔ ۲ است و چون $b=c^{-۱}$ ازمرتبهٔ ۲ و $b=c^{-۱}a$ ، می‌توان c را به‌جای‌مولد b قرار داد. بنابراین می‌توان هشت عنصر گروه را، مانند (۴۸.۲)، که در آن c به‌جای b گذاشته می‌شود، نوشت. باردیگر به گروه (۲) می‌رسیم.
(β, ii): رابطهٔ $ba=a^{۲}b$ غیرممکن است، زیرا ایجاب می‌کند که $ba=b^{۲}b$ ، یعنی $a=b^{۲}$ ، که غیرقابل قبول است.
(β, iii): تنها شق باقیمانده، که عبارت است از $ba=a^{۳}b$ ، شدنی است و، همچنان که خواهیم دید، ما را به گروهی که با روابط

$$a^{۴}=۱,\ a^{۲}=b^{۲},\ ba=a^{۳}b \qquad (۵۱.۲)$$

تعریف می‌شود می‌رساند. برای آنکه نشان دهیم چنین گروهی حقیقتاً وجود دارد، یك نمایش ماتریسی صادق در (۵۱.۲) پیدا می‌کنیم. فرض کنیم

$$A=\begin{bmatrix}\sqrt{-۱} & ۰\\ ۰ & -\sqrt{-۱}\end{bmatrix},\quad B=\begin{bmatrix}۰ & ۱\\ ۱ & ۰\end{bmatrix}$$

خواننده به آسانی می‌تواند تحقیق کند که این ماتریسها با تغییر نماد مناسب در روابط (۵۱.۲) صدق می‌کنند و هشت ماتریس

$$I,\ A,\ A^{۲},\ A^{۳},\ B,\ AB,\ A^{۲}B,\ A^{۳}B$$

متمایزند و بنابراین یک گروه ضربی ماتریسی تشکیل می‌دهند که با گروهی که در (β, iii) درنظر گرفته شد یکریخت است.

این گروه به **گروه چارتاییها** (کواترنیون) معروف است (جدول (xii)، صفحهٔ ۵۷). یادآوری می‌کنیم که یک چارتایی عبارتست از یک عدد ابر مختلط

$$a_{۰}۱+a_{۱}i+a_{۲}j+a_{۳}k,$$

که درآن $a_{۰}$، $a_{۱}$، $a_{۲}$، $a_{۳}$ اعداد حقیقی و نمادهای

$$۱, i, j, k$$

در روابط

$$i^{۲}=j^{۲}=-۱,\ \ ij=-ji=k$$

یا، در روابط هم‌ارز با آنها

$$i^{۴}=۱,\ i^{۲}=j^{۲},\ ji=i^{۳}j$$

صدق می‌کنندکه این روابط، جز درحروف، با (۵۱.۲) مطابقت دارند.

برای آنکه بحث خود را در باب گروههای مرتبهٔ ۸ خلاصه‌کنیم جدول‌ضربهای کامل پنج گروه مجرد ممکن ازاین مرتبه را ضمیمه می‌کنیم:

جدول(viii)

$$C_{۸}=\mathrm{gp}\{a\},\ a^{۸}=۱$$

	۱	a	$a^{۲}$	$a^{۳}$	$a^{۴}$	$a^{۵}$	$a^{۶}$	$a^{۷}$
۱	۱	a	$a^{۲}$	$a^{۳}$	$a^{۴}$	$a^{۵}$	$a^{۶}$	$a^{۷}$
a	a	$a^{۲}$	$a^{۳}$	$a^{۴}$	$a^{۵}$	$a^{۶}$	$a^{۷}$	۱
$a^{۲}$	$a^{۲}$	$a^{۳}$	$a^{۴}$	$a^{۵}$	$a^{۶}$	$a^{۷}$	۱	a
$a^{۳}$	$a^{۳}$	$a^{۴}$	$a^{۵}$	$a^{۶}$	$a^{۷}$	۱	a	$a^{۲}$
$a^{۴}$	$a^{۴}$	$a^{۵}$	$a^{۶}$	$a^{۷}$	۱	a	$a^{۲}$	$a^{۳}$
$a^{۵}$	$a^{۵}$	$a^{۶}$	$a^{۷}$	۱	a	$a^{۲}$	$a^{۳}$	$a^{۴}$
$a^{۶}$	$a^{۶}$	$a^{۷}$	۱	a	$a^{۲}$	$a^{۳}$	$a^{۴}$	$a^{۵}$
$a^{۷}$	$a^{۷}$	۱	a	$a^{۲}$	$a^{۳}$	$a^{۴}$	$a^{۵}$	$a^{۶}$

جدول (ix)

$$C_۴ \times C_۲ = \text{gp}\{a\} \times \text{gp}\{b\}, \quad a^۴ = b^۲ = ۱$$

	۱	a	$a^۲$	$a^۳$	b	ab	$a^۲b$	$a^۳b$
۱	۱	a	$a^۲$	$a^۳$	b	ab	$a^۲b$	$a^۳b$
a	a	$a^۲$	$a^۳$	۱	ab	$a^۲b$	$a^۳b$	b
$a^۲$	$a^۲$	$a^۳$	۱	a	$a^۲b$	$a^۳b$	b	ab
$a^۳$	$a^۳$	۱	a	$a^۲$	$a^۳b$	b	ab	$a^۲b$
b	b	ab	$a^۲b$	$a^۳b$	۱	a	$a^۲$	$a^۳$
ab	ab	$a^۲b$	$a^۳b$	b	a	$a^۲$	$a^۳$	۱
$a^۲b$	$a^۲b$	$a^۳b$	b	ab	$a^۲$	$a^۳$	۱	a
$a^۳b$	$a^۳b$	b	ab	$a^۲b$	$a^۳$	۱	a	$a^۲$

جدول(x)

$$C_۲ \times C_۲ \times C_۲ = \text{gp}\{a\} \times \text{gp}\{b\} \times \text{gp}\{c\}, \; a^۲ = b^۲ = c^۲ = ۱$$

	۱	a	b	c	ab	ac	bc	abc
۱	۱	a	b	c	ab	ac	bc	abc
a	a	۱	ab	ac	b	c	abc	bc
b	b	ab	۱	bc	a	abc	c	ac
c	c	ac	bc	۱	abc	a	b	ab
ab	ab	b	a	abc	۱	bc	ac	c
ac	ac	c	abc	a	bc	۱	ab	b
bc	bc	abc	c	b	ac	ab	۱	a
abc	abc	bc	ac	ab	c	b	a	۱

جدول(xi)

گروه دو وجهی: $a^{۴}=b^{۲}=(ab)^{۲}=۱$

	۱	a	$a^{۲}$	$a^{۳}$	b	ab	$a^{۲}b$	$a^{۳}b$
۱	۱	a	$a^{۲}$	$a^{۳}$	b	ab	$a^{۲}b$	$a^{۳}b$
a	a	$a^{۲}$	$a^{۳}$	۱	ab	$a^{۲}b$	$a^{۳}b$	b
$a^{۲}$	$a^{۲}$	$a^{۳}$	۱	a	$a^{۲}b$	$a^{۳}b$	b	ab
$a^{۳}$	$a^{۳}$	۱	a	$a^{۲}$	$a^{۳}b$	b	ab	$a^{۲}b$
b	b	$a^{۳}b$	$a^{۲}b$	ab	۱	$a^{۳}$	$a^{۲}$	a
ab	ab	b	$a^{۳}b$	$a^{۲}b$	a	۱	$a^{۳}$	$a^{۲}$
$a^{۲}b$	$a^{۲}b$	ab	b	$a^{۳}b$	$a^{۲}$	a	۱	$a^{۳}$
$a^{۳}b$	$a^{۳}b$	$a^{۲}b$	ab	b	$a^{۳}$	$a^{۲}$	a	۱

جدول(xii)

گروه چارتاییها: $a^{۴}=۱$, $a^{۲}=b$, $ba=a^{۳}b$

	۱	a	$a^{۲}$	$a^{۳}$	b	ab	$a^{۲}b$	$a^{۳}b$
۱	۱	a	$a^{۲}$	$a^{۳}$	b	ab	$a^{۲}b$	$a^{۳}b$
a	a	$a^{۲}$	$a^{۳}$	۱	ab	$a^{۲}b$	$a^{۳}b$	b
$a^{۲}$	$a^{۲}$	$a^{۳}$	۱	a	$a^{۲}b$	$a^{۳}b$	b	ab
$a^{۳}$	$a^{۳}$	۱	a	$a^{۲}$	$a^{۳}b$	b	ab	$a^{۲}b$
b	b	$a^{۳}b$	$a^{۲}b$	ab	$a^{۲}$	a	۱	$a^{۳}$
ab	ab	b	$a^{۳}b$	$a^{۲}b$	$a^{۳}$	$a^{۲}$	a	۱
$a^{۲}b$	$a^{۲}b$	ab	b	$a^{۳}b$	۱	$a^{۳}$	$a^{۲}$	a
$a^{۳}b$	$a^{۳}b$	$a^{۲}b$	ab	b	a	۱	$a^{۳}$	$a^{۲}$

۱۵. قضیهٔ اصلی حاصلضرب. در آغاز این فصل حاصلضرب دو زیرمجموعه را تعریف کردیم. اینك حالتی راکه این‌دو زیرمجموعه زیرگروههای یك گروه هستند، مورد بررسی قرار می‌دهیم. آشکار خواهد شدکه حاصلضرب دو زیرگروه همیشه یك زیرگروه نیست،

اما درحالت متناهی‌بودن این‌زیر گروهها اطلاعات روشنی دربارهٔ تعداد عناصر حاصلضرب می‌توان به‌دست آورد.

قضیهٔ اصلی ۵ (قضیهٔ حاصلضرب). (i) فرض‌کنیم A و B دو زیرگروه باشند. در این صورت AB یك زیرگروه است اگر، و فقط اگر،

$$AB = BA \tag{۵۲.۲}$$

(ii) در حالتی‌که زیرگروهها متناهی باشند، فرض می‌کنیم $a = |A|$، $b = |B|$، $d = |A \cap B|$. در این صورت، صرفنظر از برقرار بودن یا نبودن (۵۲.۲)،

$$|AB| = |BA| = \frac{ab}{d}$$

برهان. (i) چون A و B گروه هستند، داریم $A^{۲} = A$ و $B^{۲} = B$. ابتدا فرض می‌کنیم (۵۲.۲) برقرار باشد و قرار می‌دهیم $H = AB$. در این‌صورت

$$H^{۲} = ABAB = A^{۲}B^{۲} = AB = H$$

که بستاری H را ثابت می‌کند. بدیهی است‌که $۱ \in H$، زیرا $۱ \in A$ و $۱ \in B$. بالاخره هرگاه a و b به‌ترتیب عناصری دلخواه از A و B باشند، آنگاه $b^{-۱}a^{-۱} \in BA$؛ و از این‌رو، بنابر (۵۲.۲)، $b^{-۱}a^{-۱} \in AB = H$؛ یعنی $(ab)^{-۱} \in H$، که برهان گروه‌بودن H را کامل می‌کند.

بعکس، فرض‌کنیم $H = AB$ یك گروه باشد. از این‌رو اگر a و b به ترتیب عناصر دلخواهی از A و B باشند، $ab \in H$، $a^{-۱}b^{-۱} \in H$، و همچنین $(a^{-۱}b^{-۱})^{-۱} \in H$، یعنی $ba \in H$. این بدان‌معنی است که

$$BA \subset AB$$

به‌ویژه، $b^{-۱}a^{-۱} = a_۱b_۱$، که در آن $a_۱$ و $b_۱$ به‌ترتیب عناصر A و B می‌باشند. ازاین‌رو

$$(b^{-۱}a^{-۱})^{-۱} = ab = b_۱^{-۱}a_۱^{-۱}$$

یعنی

$$AB \subset BA$$

لذا نتیجه می‌گیریم که $AB = BA$.

(ii) فرض‌کنیم $D = A \cap B$. چون D زیرگروه B است، می‌توانیم B را به‌هممجموعه‌هایی برحسب D، مانند

$$B = Dt_۱ \cup Dt_۲ \cup \cdots \cup Dt_n \tag{۵۳.۲}$$

تجزیه‌کنیم که در آن

$$Dt_i \neq Dt_j \quad \text{هرگاه} \quad i \neq j \tag{۵۴.۲}$$

و

$$n=\frac{b}{d} \tag{۵۵.۲}$$

چنانچه (۵۳.۲) را ازچپ در A ضرب و توجه کنیم که $AD=A$، چون $D \subset A$، به‌دست می‌آوریم

$$AB=At_{1} \cup At_{2} \cup \cdots \cup At_{n} \tag{۵۶.۲}$$

ادعا می‌کنیم کـه هیچکدام از دو هممجموعهٔ سمت راست (۵۶.۲) عنصر مشترك ندارند؛ چون در غیر این‌صورت، باید معادله‌ای به‌صورت

$$u_{1}t_i=u_{2}t_j$$

که در آن $u_{1}, u_{2} \in A$ و $i \neq j$، داشته باشیم. لذا

$$t_it_j^{-1}=u_{1}^{-1}u_{2}$$

اما عنصرسمت چپ، بنابر (۵۳.۲) متعلق به B است؛ وعنصرسمت راست در A قراردارد. از ایـن‌رو هریك از دوطرف عنصری از D است. امـا از $t_it_j^{-1} \in D$ نتیجه می‌شود کـه $Dt_i=Dt_j$، که با (۵۴.۲) درتناقض است. لذا هممجموعه‌های (۵۶.۲) جدا ازهم‌هستند، و چون هریك متشکل از a عنصرند، داریم

$$|AB|=an=\frac{ab}{d}$$

واضح است که این بحث نسبت به A و B متقارن است، به‌طوری‌که داریم

$$|BA|=\frac{ab}{d}$$

۱۶. هممجموعه‌های مضاعف. در صفحهٔ ۳۷ دیدیم کـه تجزیهٔ یك‌گروه به‌هممجموعه‌ها نسبت‌به‌یك‌زیرگروه را می‌توان به‌عنوان نمونه‌ای از افراز یك‌مجموعه به‌رده‌های هم‌ارزی نسبت به‌یك رابطهٔ هم‌ارزی که به‌نحو مناسبی تعریف شده است تلقی نمود.

اینك به‌پیروی از فروبنیوس[1] یك رابطهٔ هم‌ارزی دیگری راکه متضمن دوزیرگروه می‌باشد، مورد بحث قرارمی‌دهیم.فرض‌کنیم A و B دوزیرگروه G، که لزوماً متمایزنیستند، باشند؛ دو عنصر $x, y \in G$ را هم‌ارز می‌نامیم، ومی‌نویسیم $y \sim x$، هرگاه عناصری مانند $u \in A$ و $v \in B$ موجود باشند به‌قسمی که

$$y=uxv \tag{۵۷.۲}$$

1. Frobenius

به‌سادگی می‌توان بررسی کرد که این رابطه، یك رابطهٔ هم‌ارزی در G است. زیرا
(الف) $x \sim x$، زیرا می‌توانیم بگیریم ۱ $=u$ و ۱ $=v$؛
(ب) اگر $x \sim y$، آنگاه $y \sim x$، زیرا از (۵۷.۲) لازم می‌آید که $x = u^{-1}yv^{-1}$.
(ج) اگر $x \sim y$ و $y \sim z$، یعنی $y = uxv$ و $z = u'yv'$، که در آن $u' \in A$ و $v' \in B$، آنگاه $z = (u'u)x(vv')$، به‌طوری که $x \sim z$.

لذا می‌توان مجموعهٔ G را به‌رده‌های هم‌ارزی ازهم جدا، که از تعریف این هم‌ارزی به‌وجود می‌آیند، افراز کرد. ردهٔ هم‌ارزی شامل x، ترکیب AxB است که یك هممجموعهٔ مضاعف G نسبت به A و B نامیده می‌شود. از هر رده یك نماینده انتخاب می‌کنیم و تجزیهٔ

$$G = \bigcup_{i \in I} At_iB \tag{۵۸.۲}$$

را به‌دست می‌آوریم که در آن I مجموعهٔ اندیسگذاری است احتمالاً نامتناهی که با مجموعهٔ هممجموعه‌های مضاعف در تناظر یك به‌یك است. واضح است که با اختیار A یا B به‌عنوان زیرگروه بدیهی $\{1\}$، (۵۸.۲) تعمیمی از تجزیهٔ از راست یا از چپ، هممجموعه است. برخلاف تجزیه به‌هممجموعه‌های منفرد، هممجموعه‌های مضاعف در (۵۸.۲)، در حالت کلی، دارای یك عدد اصلی *نیستند*.

وقتی G یك گروه متناهی باشد مطلب را بیشتر دنبال می‌کنیم. فرض کنیم $g = |G|$، $a = |A|$، و $b = |B|$. ابتدا ملاحظه می‌کنیم که ترکیبات At_iB و $(t_i^{-1}At_i)B$ دارای یك عدد اصلی هستند، زیرا می‌توان عناصر آنها را با جور کردن ut_iv با $t_i^{-1}(ut_iv)$ در یك تناظر یك به‌یك قرارداد. لذا

$$|At_iB| = |(t_i^{-1}At_i)B|$$

اما $t_i^{-1}At_i$ یك زیرگروه است (صفحهٔ ۳۶ ملاحظه شود)، و

$$|t_i^{-1}At_i| = |A| = a$$

با به‌کار بستن قضیهٔ ۵ برای زیرگروههای $t_i^{-1}At_i$ و B، ملاحظه می‌کنیم که

$$|At_iB| = \frac{ab}{d_i}$$

که در آن $d_i = |t_i^{-1}At_i \cap B|$. از جمعبندی این نتایج قضیهٔ ذیل را به‌دست می‌آوریم.

قضیهٔ اصلی ۶ (فروبنیوس). فرض کنیم G گروهی متناهی از مرتبهٔ g و A و B زیرگروههایی از آن به ترتیب از مراتب a و b باشند. در این صورت عناصری مانند t_1، t_2، . . .، t_r وجود دارند به‌قسمی که G برابر اجتماع هممجموعه‌های مضاعف ازهم جدا می‌باشد، به‌عبارت روشنتر

$$G = At_1B \cup At_2B \cup \cdots \cup At_rB$$

تعداد عناصر At_iB برابر ab/d_i است، که در آن

$$d_i = |t_i^{-1} A t_i \cap B|$$

و در نتیجه

$$g = ab \sum_{i=1}^{r} d_i^{-1} \tag{۵۹.۲}$$

تمرین

(۱) فرض کنیم $D = X \cap Y$ و $M = \mathrm{gp}\{X, Y\}$، و X و Y زیرمجموعه‌های ناتهی از یك زیرگروه G باشند. نشان دهید که اگر Z زیرمجموعهٔ دیگری از G باشد، آنگاه

$$X \cap Y \cap Z = D \cap Z, \ \mathrm{gp}\{X, Y, Z\} = \mathrm{gp}\{M, Z\}.$$

(۲) فرض کنیم $D = A \cap B$، که A و B زیرگروههایی از G هستند. ثابت کنید که اگر $u, v \in At \cap Bs$، $(s, t \in G)$، آنگاه $Du = Dv$. نتیجه بگیرید، وقتی $[G : A]$ و $[G : B]$ متناهی باشند آنگاه $[G : D] \leqslant [G : A][G : B]$ (قضیهٔ پوانکاره).

(۳) ثابت کنید اگر A و B زیرگروههایی متناهی باشند که مرتبه‌های آنها نسبت به‌هم اول هستند، آنگاه $A \cap B$ فقط شامل عنصر واحد است.

(۴) ثابت کنید که یك گروه متناهی که مرتبهٔ آن مرکب باشد دارای یك زیرگروه حقیقی است.

(۵) کلیهٔ زیرگروههای مرتبهٔ ۴ گروه دو وجهی مرتبهٔ ۸ را پیدا کنید (صفحهٔ ۵۷ جدول xi).

(۶) نشان دهید می‌توان گروه جدول (v) (صفحهٔ ۱۵) را به‌وسیلهٔ روابط

$$c^2 = d^2 = (cd)^3 = 1$$

تعریف کرد.

(۷) فرض کنیم $\varepsilon = \exp(2\pi i/n)$، و n عدد صحیح مثبتی بزرگتر از یك باشد. ثابت کنید ماتریسهای

$$A = \begin{bmatrix} \varepsilon & 0 \\ 0 & 1/\varepsilon \end{bmatrix}, \quad B = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

یك نمایش‌صادق از گروه دو وجهی $D_n = \mathrm{gp}\{a, b\}$ ازمرتبهٔ $2n$، با روابط معرف

$$a^n = b^2 = (ab)^2 = 1$$

تشکیل می‌دهند.

(۸) فرض کنیم $\theta = \exp(\pi i/m)$، m عدد صحیح مثبتی بزرگتر از یک، باشد. ثابت کنید ماتریسهای

$$A = \begin{bmatrix} \theta & ۰ \\ ۰ & ۱/\theta \end{bmatrix}, \quad B = \begin{bmatrix} ۰ & ۱ \\ -۱ & ۱ \end{bmatrix}$$

یک نمایش صادق از **گروه دوری** مضاعف از مرتبهٔ $۴m$ می‌سازند که روابط معرف آن چنین‌اند

$$a^{۲m} = ۱,\ b^{۲} = (ab)^{۲} = a^{m}$$

(۹) ثابت کنید هرگاه یک گروه تعویضناپذیر مرتبهٔ ۱۲ شامل عنصری از مرتبهٔ ۶ باشد، آنگاه این گروه یا با گروه دو وجهی و یا با گروه دوری مضاعف از همان مرتبه یکریخت است.

(۱۰) نشان دهید که مانده‌های متباین با ۲۱، یک گروه (ضربی) آبلی تشکیل می‌دهند که با $C_۶ \times C_۲$ یکریخت است.

(۱۱) گیریم $X = \mathrm{gp}\,\{x\}$ گروه دوری نامتناهی با مولد x باشد، و فرض کنیم $R = \mathrm{gp}\,\{x^r\}$، و r عدد صحیح مثبتی باشد. ثابت کنید $[X : R] = r$.

۳

زیرگروههای نرمال

۱۷. رده‌های مزدوج. درصفحهٔ ۳۷ روشی برای افراز یك گروه G به رده‌های هم‌ارزی نسبت به‌یك زیرگروه G، را موردبحث قرار دادیم. حال یك رابطهٔ هم‌ارزی ازنوع دیگر را معرفی می‌کنیم.

تعریف ۵. عناصر a و b از G را **مزدوج** خوانیم هرگاه عنصری چون t از G موجود باشد به‌قسمی‌که

$$b = t^{-1}at \qquad (۱.۳)$$

گوییم t، a را به b تبدیل می‌کند؛ دراین مقام ما علاقهٔ خاصی به عنصری‌که این تبدیل را انجام می‌دهد نداریم و باید توجه داشته باشیم‌که، وقتی a و b داده شده باشند، همچنین امکان دارد بیش ازیك عنصر t یافت شودکه در (۱.۳) صدق‌کند. گاهی طرف راست (۱.۳) به‌صورت‌کوتاه a^t نشان داده می‌شود، یعنی قرار می‌دهند

$$a^t = t^{-1}at \qquad (۲.۳)$$

هرگاه رابطه‌ای مانند (۱.۳) بەازای مقداری از t وجود داشته باشد، موقتاً آن را چنین می‌نویسیم $a \sim b$. تحقیق می‌کنیم که این، یك رابطهٔ هم‌ارزی است، بدین‌طریق:

(۱) $a \sim a$ (ویژگی انعکاسی)، با انتخاب $t = 1$؛

(۲) از $a \sim b$ لازم می‌آیدکه $b \sim a$ (ویژگی تقارنی)؛ زیرا اگر (۱.۳) برقرار باشد، آنگاه $a = tbt^{-1} = (t^{-1})^{-1}bt^{-1}$، لذا $b \sim a$.

(۳) اگر $a \sim b$ و $b \sim c$، آنگاه $a \sim c$ (ویژگی تعدی)؛ زیرا داریم $a = t^{-1}bt$ و $b = s^{-1}cs$، که از حذف b بین این روابط به‌دست می‌آوریم $a = (st)^{-1}c(st)$، یعنی $a \sim c$.

بعلاوه متذکر می‌شویم که ازدواج از قاعدهٔ مهم ضربی

$$(xy)^t = x^t y^t \qquad (۳.۳)$$

پیروی می‌کند، که در آن x، y و t عناصر دلخواهی از G هستند، زیرا

$$(xy)^t = t^{-1}xyt = (t^{-1}xt)(t^{-1}yt) = x^t y^t$$

واضح است که می‌توان (۳.۳) را برای هر تعدادی ازعامل تعمیم داد، لذا

$$(x_1 x_2 \cdots x_n)^t = x_1^t x_2^t \cdots x_n^t$$

با قراردادن $y = x^{-1}$ در (۳.۳) و توجه به‌اینکه $1^t = 1$، نتیجه می‌گیریم

$$1 = x^t (x^{-1})^t$$

یعنی

$$(x^t)^{-1} = (x^{-1})^t \qquad (۳.۳)'$$

یادآوری می‌کنیم که وقتی یك رابطهٔ هم‌ارزی در یك مجموعه تعریف شده باشد، این مجموعه به‌رده‌های ازهم جدا تجزیه می‌شود. هر رده از کلیهٔ عناصری تشکیل می‌شود که با عنصر خاصی هم‌ارزند. در وضعیت حاضر، ما از **رده‌های مزدوج** صحبت می‌کنیم. ردهٔ مزدوجی که شامل عنصر بخصوص a باشد به (a) نشان داده می‌شود؛ این رده شامل کلیهٔ عناصری است که با a مزدوج‌اند، ازجمله خود a. لذا

$$(a) = t_1^{-1}at_1 \cup t_2^{-1}at_2 \cup \cdots$$

ومی‌توانیم فرض کنیم $t_1 = 1$. اگر b عنصری باشد که در (a) نباشد، آنگاه b یك ردهٔ مزدوج جدیدی تولید می‌کند

$$(b) = s_1^{-1}bs \cup s_2^{-1}bs_2 \cup \cdots$$

و ویژگی تعدی رابطهٔ مزدوجی ما را مطمئن می‌کند که (a) و (b) هیچ عنصر مشترکی ندارند. اگر به‌همین‌ترتیب جلو رویم و عمل را ادامه دهیم، تجزیهٔ G به رده‌های مزدوج را به‌دست می‌آوریم. لذا

$$G = (a) \cup (b) \cup (c) \cup \cdots$$

ما a، b، c، ... را نماینده‌های رده‌های مختلف می‌خوانیم، لیکن باید به‌خاطر داشته‌باشیم که این نماینده‌ها منحصر به فرد نیستند؛ در حقیقت $(a) = (a')$، اگر و فقط اگر، $a' = x^{-1}ax$ $(x \in G)$.

وقتی G نامتناهی است، ممکن است بینهایت ردهٔ مزدوج موجود باشد، و یك ردهٔ

مزدوج خاص ممکن است شامل بینهایت عنصر باشد. بـه‌دست‌آوردن اطلاعات دقیقتر در بارهٔ عناصری که یك ردهٔ مفروض را تشکیل می‌دهند و تعیین مقدار این رده، وقتی این رده متناهی باشد، حائز اهمیت است. روشن است که ردهٔ (۱) فقط ازعنصر ۱ تشکیل می‌شود، زیرا به‌ازای هر t از G، $t^{-1}1t=1$.

به منظور بررسی مفصلتر این مسئله، ما مفهوم **مرکزساز** را وارد می‌کنیم. فرض کنیم a عنصر ثابتی از G باشد؛ مجموعهٔ تمام عناصری از G را که با a تعویضپذیرند، به $C(a)$ نشان می‌دهیم.* لذا

$$C(a)=\{t\in G\,|\,ta=at\}$$

به‌آسانی تحقیق می‌شود که $C(a)$ یك زیرگروه‌G است. زیرا (الف) اگر $s,t\in C(a)$، آنگاه $a(st)=sat=(st)a$، لذا $st\in C(a)$؛ (ب) $1\in C(a)$، و(ج) اگر $t\in C(a)$، آنگاه $t^{-1}a=at^{-1}$، یعنی $t^{-1}\in C(a)$.

ضمناً، $|C(a)|\geqslant 2$، مگر آنکه $G=\{1\}$؛ زیرا اگر $a=1$، آنگاه $C(a)=G$؛ و اگر $a\neq 1$، آنگاه $a\in C(a)$ و $1\in C(a)$.

حال، تجزیهٔ هممجموعه‌های G نسبت به $C(a)$، یعنی

$$G=\bigcup_i C(a)t_i\quad(i\in I)$$

را، کـه در آن I مجموعـهٔ اندیسگذار مناسبی است، درنظر می‌گیریم. ادعـا می‌کنیم که هممجموعه‌های $C(a)$ با عناصر (a) تناظر یك به‌یك دارند؛ این تناظر به‌وسیلهٔ نگاشت

$$\theta:C(a)x\rightarrow x^{-1}ax\tag{۴.۳}$$

برقرار می‌شود. ابتدا باید نشان دهیم که θ تعریف روشنی دارد. به‌خاطر داریم که می‌توان $C(a)x$ را به‌صورت $C(a)ux$ نیز نوشت که u عنصر دلخواهی از $C(a)$ است. بدین‌ترتیب باید نشان دهیم که قراردادن ux به‌جای x، سمت راست (۴.۳) را تغییرنمی‌دهد. درواقع،

$$(ux)^{-1}a(ux)=x^{-1}u^{-1}aux=x^{-1}ax$$

زیرا $u\in C(a)$. چون x عنصر دلخواهی از G است، واضح است کـه نگاشت θ بر روی ردهٔ (a) نگاشتی است پوشا. بالاخره، ملاحظه می‌کنیم که θ یك به‌یك نیز هست؛ زیرا اگر $x^{-1}ax=y^{-1}ay$، آنگاه $xy^{-1}\in C(a)$. از اینجا نتیجه می گیریم $C(a)x=C(a)y$. لذا، همچنان که ادعا کرده بودیم، تناظر یك به‌یك می‌باشد.

این نتایج را در ذیل جمع می کنیم:

قضیهٔ ۰۷ فرض کنیم a عنصری از G و $C(a)$ مرکزساز a باشد. دراین صورت عناصر ردهٔ مزدوجی a با هممجموعه‌های $C(a)$ در G در تناظر یك به‌یك می‌باشند. به‌ویژه وقتی‌که اندیس $C(a)$ متناهی باشد،آنگاه $|(a)|=[G:C(a)]$.

---

* $C(a)$ را مرکزساز a می‌نامیم.ـم.

فرع. اگر G گروهی متناهی از مرتبهٔ g و h_a تعداد عناصر (a) باشد، آنگاه $h_a|g$.

برهان. فرض کنیم $|C(a)| = c_a$. پس بنا بر قضیهٔ ۷، $h_a = g/c_a$، یعنی $g = c_a h_a$.
فرض کنیم گروه متناهی G دارای k ردهٔ مزدوجی متمایز باشد. فرض کنیم $a_1(=1)$، a_2، . . .، a_k مجموعه‌ای از نمایندهها و $h_i = |(a_i)|$. دراین صورت

$$G = (a_1) \cup (a_2) \cup \cdots \cup (a_k),$$

ازاین‌رو، با شمارش عناصر هرطرف این تساوی نتیجه می‌شود

$$g = h_1 + h_2 + \cdots + h_k \tag{۵.۳}$$

این تساوی، **معادلهٔ رده‌ای** G خوانده می‌شود.

۱۸. مرکز گروه. مجموعهٔ Z ازعناصری که باهرعنصر G تعویضپذیر باشد، **مرکز** G نامیده می‌شود. لذا

$$Z = \{z | tz = zt,\ \text{به‌ازای هر } t \in G\}$$

این مجموعه یك زیرگروه G است؛ زیرا (الف) اگر $tz_1 = z_1 t$ و $tz_2 = z_2 t$، آنگاه $tz_1 z_2 = z_1 t z_2 = z_1 z_2 t$، پس $z_1 z_2 \in Z$؛ (ب) اگر $tz = zt$، آنگاه $z^{-1}t = tz^{-1}$، لذا $z^{-1} \in Z$؛ (ج) $1 \in Z$. البته Z همواره آبلی است، اما ممکن است گروه واحد باشد؛ برای مثال، درگروه غیرآبلی مرتبهٔ ۶ (صفحهٔ ۱۵، جدول (v) ملاحظه شود) مرکز فقط ازعنصر واحد تشکیل می‌شود. روشن است که $G = Z$، اگر وفقط اگر G آبلی باشد.
هر عنصر مرکز به‌وسیلهٔ این واقعیت که خودش به‌تنهایی یك ردهٔ مزدوجی تشکیل می‌دهد مشخص می‌شود، زیرا اگر z فقط با خودش مزدوج باشد، آنگاه به‌ازای هر $t \in G$، $t^{-1}zt = z$، و این بدان معنی است که $z \in Z$. بدین علت گاهی یك عنصر مرکزی را **خود - مزدوج** می‌خوانند. قضیهٔ ذیل ازاین لحاظ جالب است که وجود یك مرکز غیربدیهی را برای دسته مهمی از گروهها اثبات می‌کند.

قضیهٔ اصلی ۷. اگر G یك گروه متناهی باشد به‌قسمی که $|G| = p^m$، p یك عدد اول و $m > 0$، آنگاه مرکز G ازمرتبهٔ p^μ است، $0 < \mu \leqslant m$.

برهان. معادلهٔ رده‌ای (۵.۳) دراین حالت چنین می‌شود

$$p^m = h_1 + h_2 + \cdots + h_k \tag{۶.۳}$$

که $h_\alpha | p^m$ $(\alpha = 1, 2, \ldots, k)$. چون p عددی است اول، پس لازم است که هر h_α یا برابر واحد باشد ویا توانی از p. قبلاً می‌دانستیم که $h_1 = 1$. فرض کنیم دقیقاً $l(\geqslant 1)$ مقدار برای α وجود داشته باشد به‌قسمی که $h_\alpha = 1$. دراین صورت می‌توانیم به ازای عدد صحیحی مانند s، (۶.۳) را به‌صورت

$$p^m = l + ps$$

بنویسیم. از اینجا نتیجه می‌شود که l بر p قابل‌قسمت است و چون l مثبت است، نتیجه می‌گیریم که $p \leqslant l$. لذا حداقل p عنصرخود-مزدوج وجود دارد، یعنی Z غیر بدیهی‌است. چون Z یك زیرگروه G است، قضیهٔ لاگرانژ این‌اطلاع را به‌ما می‌دهد که $|Z| = p^\mu$، که $0 < \mu \leqslant m$.

۱۹. زیرگروههای نرمال. می‌توان مفهوم مرکزساز را برای هرزیرمجموعهٔ ناتهی A از G تعمیم داد. لذا مرکز ساز $C(A)$ از A، شامل کلیهٔ عناصری از G است که با هرعنصر A تعویضپذیرند، یعنی

$$C(A) = \{t \mid ta = at,\ \text{به‌ازای هر } a \in A\}$$

همانند قبل، مرکزساز همواره یك زیرگروه G، شاید زیرگروه واحد باشد. در واقع، این زیرگروه اشتراك گروههای $C(a)$ است که a در A تغییرمی‌کند. هرگاه وابستگی مرکزساز به‌گروه دربرگیرندهٔ G موردنظر باشد، به‌طور دقیقتر $C_G(A)$ می‌نویسیم. متذکر می‌شویم که در حالت کلی

$$C_G(G) = G \text{ مرکز}$$

اینك به‌مفهوم دیگری از تعویضپذیری می‌پردازیم: فرض‌کنیم زیرمجموعهٔ ناتهی A داده شده باشد. عناصری مانند s از G را درنظر می‌گیریم که در رابطهٔ

$$sA = As \tag{۷.۳}$$

به‌عنوان رابطه‌ای بین زیرمجموعه‌ها، صدق‌کنند. لذا (۷.۳) بدین‌معنی است‌که به‌ازای هر $a \in A$، عناصری مانند a_1 و a_2 از A وجود دارند به‌قسمی‌که $sa = a_1 s$ و $as = sa_2$. تحقیق سرراست این واقعیت که مجموعهٔ عناصر s که در (۷.۳) صدق می‌کنند، تشکیل‌یك زیرگروه G می‌دهند، به‌خواننده واگذار می‌شود. این زیرگروه **نرمالساز** A نامیده می‌شود و به

$$N(A)\text{، یا دقیقتر به } N_G(A)$$

نمایش داده می‌شود. واضح است که هرعنصر $C(A)$ یقیناً در (۷.۳) صدق می‌کند، چون چنین عنصری «عنصر به‌عنصر» با عناصر A تعویضپذیر است. لذا

$$C(A) \leqslant N(A)$$

اما، در حالت کلی، نرمالساز از مرکزساز بزرگتر است.

ما بخصوص، به حالتی علاقه‌مندیم که در آن A زیرگروهی مانند H از G باشد. همچنانکه قبلاً دیده‌ایم (صفحهٔ ۳۶)، وقتی x عنصر دلخواهی از G باشد، $H' = x^{-1}Hx$ نیز زیرگروهی است یکریخت با H، گرچه در حالت کلی متمایز از آن است. H و H' را **مزدوج** می‌نامیم. با این حال ممکن است مزدوج سازی توسط عناصر متمایز x و y

زیرگروه واحدی تولید کند. در واقع، معادلهٔ

$$x^{-1}Hx = y^{-1}Hy \qquad (۸.۳)$$

هم ارز است با $Hxy^{-1} = xy^{-1}H$، وبنابراین $xy^{-1} \in N(H)$. ازاین‌رو (۸.۳) فقط و فقط وقتی برقرار است که $x = sy$، که $s \in N(H)$. گروه H از جملهٔ مزدوجهای خودش به‌شمار می‌آید، و رابطهٔ $H = s^{-1}Hs$ فقط و فقط وقتی برقرار است که $s \in N(H)$.

واضح است که $H \leqslant N(H)$، زیرا اگر $u \in H$، آنگاه $u^{-1}Hu = H$ (قضیهٔ ۳، صفحهٔ ۳۵ ملاحظه شود).

زیرگروههایی از G که به‌مراتب جالبترند آنهایی هستند که نرمالساز آنها تمام گروه G باشد. وقتی $N(H) = G$، گوییم H یک زیرگروه **نرمال** یا زیرگروه **پایای** G می‌باشد و (در این مورد) نماد مخصوص

$$H \lhd G$$

را به‌کار می‌بریم.

اینك کمی بیشتر دربارهٔ این‌مفهوم مهم صحبت می‌کنیم. یك زیرگروه نرمال به‌توسط این حقیقت مشخص می‌شود که جزخودش هیچ گروه مزدوجی ندارد، یعنی

$$\text{به‌ازای هر } x \in G،\ H = x^{-1}Hx \text{ یا } xH = Hx \qquad (۹.۳)$$

به‌طور روشنتر، اگر x عنصر دلخواهی از G و u عنصری از زیرگروه نرمال H باشد، آنگاه عنصری چون $u' \in H$ هست که

$$x^{-1}ux = u'$$

در واقع، برای آنکه نشان دهیم $H \lhd G$ کافی است تحقیق کنیم که به‌ازای هر $x \in G$،

$$x^{-1}Hx \subset H \qquad (۱۰.۳)$$

زیراکه اگر این رابطه برقرار باشد، می‌توانیم به‌جای x، x^{-1} گذاشته به‌دست آوریم

$$H \subset x^{-1}Hx$$

این رابطه و(۱۰.۳) با هم ایجاب می‌کنند که داشته باشیم $H = x^{-1}Hx$. درهرگروه G، زیرگروه واحد $\{1\}$ و خود G، زیرگروههای نرمال G هستند. یك گروه از مرتبهٔ بزرگتر ازیك را **ساده** نامیم هرگاه غیر از این زیرگروههای بدیهی هیچ زیرگروه نرمال دیگری نداشته باشد. البته، یك گروه ازمرتبهٔ اول لزوماً ساده است؛ اما مثالهای جالبی از زیرگروههای ساده از مرتبهٔ مرکب نیز وجود دارد (صفحهٔ ۱۵۰ ملاحظه شود). هر زیرگروه یك گروه آبلی، خود به‌خود نرمال است، زیرا (۹.۳) نتیجه‌ای از تعویضپذیری است.

برای اینکه ببینیم آیا H در G نرمال است یا نه، اغلب ازیکی ازدستورالعملهای ذیل استفاده می‌کنیم:

(۱) فرض کنیم G برحسب مولدهایش داده شده باشد (صفحهٔ ۴۳ ملاحظه شود) یعنی

$$G = \mathrm{gp}\{a, b, c, \dots\}$$

اگر بتوانیم نشان دهیم که

$$a^{-1}Ha = H,\ b^{-1}Hb = H,\ c^{-1}Hc = H, \dots$$

آنگاه a، b، c، . . . به $N(H)$ تعلق خواهند داشت. اما چون این عناصر تمامی G را تولید می‌کنند، نتیجه می‌گیریم که $G = N(H)$، یعنی $H \lhd G$.

(۲) اگر H برحسب مولدها داده شده باشد، یعنی

$$H = \mathrm{gp}\{x_1, x_2, x_3, \dots\}$$

آنگاه اگر به‌ازای هر $t \in G$،

$$x_i^t \in H \quad (i = 1, 2, \dots)$$

آنگاه $H \lhd G$. زیرا بنابر (۳.۳)، این ما را مطمئن می‌کند که هر حاصلضرب (متناهی) از x_iها بر اثر ازدواج با t در H باقی می‌ماند، و بنابراین $t^{-1}Ht \subset H$.

برای مثال، فرض کنیم G گروه دو وجهی مرتبهٔ ۸ درجدول (xi) صفحهٔ ۵۷ باشد، همچنین فرض کنیم

$$H = \mathrm{gp}\{a\}$$

گروه دوری مرتبهٔ ۴ با مولد a باشد. واضح است که $a \in N(H)$. همچنین $bab^{-1} = a^3$، و از این‌رو $bHb^{-1} \leqslant H$؛ اما گروههای bHb^{-1} و H یکریخت‌اند و بنابراین از یك مرتبه می‌باشند. لذا $bHb^{-1} = H$. این بدان معنی‌است کـه $b(=b^{-1})$ متعلق به $N(H)$ است که ثابت می کند $N(H) = G$.

حال حقایق مقدماتی چندی را در باب زیرگروههای نرمال گرد آوری می کنیم.

(الف) مرکز یك‌گروه همواره زیـر گروهی است نرمـال: زیـرا شرط (۹.۳) یعنـی $x^{-1}Zx = Z$ یقیناً بـه‌ازای هر $x \in G$ برقرار است. در واقـع، حتی داریم به‌ازای هر z از Z، $x^{-1}zx = z$.

(ب) اگـر N_1، N_2، . . .، N_r زیرگروههای نرمـال باشند، اشتراك‌آنها نیز زیرگروه نرمال است: زیرا چون $x^{-1}N_ix = N_i$، $(i = 1, 2, \dots, r)$، نتیجه می گیریم

$$x^{-1}(N_1 \cap N_2 \cap \dots \cap N_r)x = N_1 \cap N_2 \cap \dots \cap N_r$$

(ج) زیرگروه H در G فقط و فقط وقتی نرمال استکـه برابر اجتماعی از رده‌های مزدوجی‌کامل G باشد، یعنی

$$H = (1) \cup (u) \cup (v) \cup \dots \qquad (11.3)$$

زیرا به‌وضوح دیده می‌شود کـه (۱۱.۳) هم‌ارز این گزاره است کـه هر گاه w به H تعلق داشته باشد، $x^{-1}wx$ که در آن x عنصر دلخواهی از G است، نیز به H متعلق است. این

بدان‌معنی است که $x^{-1}Hx \subset H$، و از این‌رو $H \lhd G$.

(د) اگر اندیس H در G برابر ۲ باشد، آنگاه $H \lhd G$. در این حالت دقیقاً دو هممجموعه از H در G وجود دارند، یکی H است و دیگری متشکل از $G \mid H$، یعنی عناصری از G که به H تعلق ندارد. لذا اگر $t \in G \mid H$، آنگاه $G \mid H = Ht$؛ همین استدلال را برای هممجموعه‌های چپ نیز می‌توان به‌کار برد. به‌طوری که $G \mid H = tH$، و بنابراین داریم $Ht = tH$، هرگاه $t \notin H$. از سوی دیگر، اگر $w \in H$، آنگاه $H = Hw = wH$. از این‌رو معادلهٔ $xH = Hx$ به‌ازای کلیهٔ xهای متعلق به G برقرار است، یعنی $H \lhd G$. برای مثال، از این روش بلافاصله نتیجه می‌شود که $\mathrm{gp}\{a\}$ یك زیرگروه نرمال گروه دو وجهی است.

۲۰. گروههای خارج‌قسمت (گروههای عامل). اهمیت برتر زیرگروههای نرمال بر این حقیقت استوار است که می‌توان به گردایهٔ هممجموعه‌های یك زیرگروه نرمال، یك ساختار گروهی بخشید. فرض کنیم $H \lhd G$، وحاصلضرب دو هممجموعهٔ Hx و Hy را (به‌عنوان دو زیرمجموعه) درنظر می‌گیریم. چون $xH = Hx$ و $H^2 = H$، خواهیم داشت

$$HxHy = HHxy = Hxy. \tag{۱۲.۳}$$

از این‌رو حاصلضرب دوهممجموعه مجدداً یك هممجموعه می‌شود. مهم این است که توجه کنیم (۱۲.۳) رابطه‌ای است واقعی بین هممجموعه‌ها که مستقل از نماینده‌هاست. دقیقتر بگوییم، ادعامی‌کنیم که هرگاه $Hx = Hx'$ و $Hy = Hy'$، آنگاه $Hxy = Hx'y'$. در واقع مفروضات ایجاب می‌کنند که داشته باشیم: $x' = ux$ و $y' = vy$، $u, v \in H$، ازاینجا نتیجه می‌شود

$$x'y' = uxvy = uv'xy$$

که در آن v' عنصر مناسبی از H است. از این‌رو $Hxy = Hx'y'$، همچنان که می‌خواستیم.

این مطلب را می‌توان با استفاده از مفهوم هم‌ارزی نسبت به H به‌گونه‌ای نه‌چندان متفاوت بیان کرد. همانند فصل ۲ صفحهٔ ۳۷، می‌نویسیم $x' \sim x$، هرگاه عنصری چون $u \in H$ موجود باشد که $x' = ux$. چون $Hx = xH$، به‌طریقی دیگرمی‌توانستیم درعوض قید کنیم که $x' = xu'$، که در آن $u' \in H$. بنابراین ردهٔ هم‌ارزی $[x]$ از عنصر بخصوص $x \in G$ با هممجموعهٔ $Hx(= xH)$ یکی است، و (۱۲.۳) بیانگر ضربی برای رده‌های هم‌ارزی است؛ یعنی

$$[x][y] = [xy] \tag{۱۳.۳}$$

که از نماینده‌های رده‌ها مستقل است.

بنابر (۱۲.۳)، مجموعهٔ هممجموعه‌ها نسبت به‌ضرب زیرمجموعه‌ها بسته است. این مطلب امید به‌تشکیل گروه‌دادن هممجموعه‌ها را افزایش می‌دهد. هیچ مشکلی‌در بارهٔ قانون شرکتپذیری وجود ندارد. زیرا این امردرمورد کلیهٔ زیرمجموعه‌ها برقراراست. (صفحهٔ ۳۳

ملاحظه شود.) برای ضرب هممجموعه‌ها، گروه H. که به‌عنوان یکی از هممجموعه‌ها درنظر گرفته می‌شود، عنصر واحد به‌شمار می‌آید. زیرا

$$H(Ht)=(Ht)H=Ht$$

بالاخره، عکس Ht عبارتست از Ht^{-1}، زیرا

$$(Ht)(Ht^{-1})=H=(Ht^{-1})(Ht)$$

گروه هممجموعه‌هایی که ما ساخته‌ایم به G/H نشان داده می‌شود و گروه **خارج قسمت** (یا **گروه عامل**) G بر H خوانده می‌شود. مرتبهٔ G/H برابر است با اندیس H در G، یعنی

$$\left|\frac{G}{H}\right|=[G:H] \qquad (۱۴.۳)$$

مفهوم گروه خارج قسمت درنظریهٔ گروهها یك مفهوم اساسی و در واقع یکی از مهمترین مفاهیم در ریاضیات است. بنابراین بعضی ازنکات مربوط به‌آن را تکرار می‌کنیم:

(۱) عناصر G/H هممجموعه‌های متمایز Hاندکه قانون ترکیب، آنها ضرب زیرمجموعه‌هاست (و یا جمع هممجموعه‌هاست، درگاه G به‌صورت جمعی نوشته شده باشد، صفحهٔ ۴۵ ملاحظه شود).

(۲) عنصر همانی (خنثی) آن، گروه H است، که به‌عنوان یکی از هممجموعه‌ها درنظر گرفته می‌شود.

(۳) اینکه هممجموعه‌های راست یا هممجموعه‌های چپ را به‌کار گیریم فرقی نمی‌کند، زیرا $Ht=tH$، زیراکه H نرمال است.

(۴) خاطر نشان می‌سازیم که نمایندهٔ یك هممجموعه بخصوص، منحصر به‌فرد نیست (صفحهٔ ۳۷ ملاحظه شود).

(۵) اصطلاح گروه خارج قسمت ونماد G/H فقط وقتی به‌کار می‌رود که H یك زیرگروه نرمال باشد.

اینك مفهوم یك گروه خارج قسمت را با طرح چند مثال روشن می‌سازیم.

(الف) فرض کنیم Z گروه (جمعی) کلیهٔ اعداد صحیح و $m>۱$ عدد صحیح ثابتی باشد. در این صورت مجموعه

$$H:\circ,\ \pm m,\ \pm ۲m,\ \cdots,\ \pm km,\ \cdots$$

یك زیرگروه از Z را تشکیل می‌دهد. چون Z آبلی است. این یك زیرگروه نرمال است. اگر x عدد صحیح دلخواهی باشد، می‌توانیم بنویسیم $x=qm+r$، که $\circ\leqslant r<m$. چون qm در H واقع است، x درهممجموعهٔ $H+r$ واقع خواهد شد (صفحهٔ ۳۷ ملاحظه شود). وقتی که مقادیر ممکن r را منظور کنیم، می‌بینیم که

$$H(=H+\circ),\ H+۱,\ H+۲,\ \cdots,\ H+(m-۱) \qquad (۱۵.۳)$$

همجموعه‌های متمایز، یعنی عناصر Z/H هستند. این همجموعه‌ها درتناظر یك به‌یك با عناصر Z_m می‌باشند ((۱۷.۱) ملاحظه شود). هرگاه، موقتاً، عناصر Z_m به‌وسیلهٔ $\bar{0}$، $\bar{1}$، . . .، $\overline{m-1}$ نمایش داده شوند، می‌توانیم این تناظر را بدین صورت بیان کنیم

$$H+r \leftrightarrow \bar{r}$$

اینك مشاهده می‌کنیم که قانون ترکیب به‌وسیلهٔ این تناظر محفوظ می‌ماند، زیرا رابطهٔ

$$(H+r)+(H+s)=H+t$$

که در آن $t\equiv r+s \pmod m$ و $0\leqslant t<m$، دقیقاً مانند

$$\bar{r}+\bar{s}=\bar{t}$$

است که برطبق قاعدهٔ ترکیب در Z_m به‌دست می‌آید. ازاین‌رو نتیجه می‌گیریم که

$$\frac{Z}{H}\cong Z_m$$

(ب) در گروه چارتاییها (جدول (xii)، صفحهٔ ۵۷) بدیهی است که عنصر $a^2=b^2$ با a و b و در نتیجه با هرعنصر تعویضپذیر است، زیرا a و b تمامی گروه را تولید می‌کنند. از این‌رو

$$H=1\cup a^2 \quad (a^4=1)$$

یك زیر گروه نرمال (درواقع مرکز گروه) است. عناصر G/H را می‌توان‌چنین‌فهرست‌کرد

$$H,\ Ha,\ Hb,\ Hab. \tag{۱۶.۳}$$

زیراازپیش‌می‌دانیم که تعداد $[G:H]=8/2=4$ همجموعه‌وجود دارد وهمجموعه‌های (۱۶.۳)، همچنان‌که به‌سادگی تحقیق می‌شود، متمایزند؛ برای مثال $Hb=b\cup a^2b$. اما G/H یك گروه مرتبهٔ ۴ است وبنابراین باید یا با C_4 یکریخت باشد و یا با $C_2\times C_2$ (صفحهٔ ۵۱ ملاحظه شود). این موضوع با ملاحظهٔ اینکه مربع هرعنصر G/H برابر عنصر واحد است نشان داده می‌شود؛ در واقع

$$(Ha)^2=Ha^2=H$$

زیرا $a^2\in H$؛ به‌طریق مشابه $(Hb)^2=H$. بالاخره چون G/H ازمرتبهٔ ۴ و لزوماً آبلی است، داریم

$$(Hab)^2=(Ha)^2(Hb)^2=H$$

ازاین‌رو $G/H\cong C_2\times C_2$ (قضیهٔ ۶ صفحهٔ ۴۹ نیز ملاحظه شود).

(ج) فرض کنیم $G=GL(n,F)$ گروه خطی کلی درجهٔ n روی F (مثال (iv)

صفحهٔ ۱۱ ملاحظه شود)، یعنی مجموعـهٔ کلیهٔ مـاتریسهای عادی $n\times n$ $\mathbf{a}=(a_{ij})$ بـا عناصری از F باشد. دراین صورت ماتریسهای با دترمینان واحد تشکیل زیرگروهی مانند U مـی‌دهند. زیـرا اگـر $\det \mathbf{u}=\det \mathbf{v}=1$، آنگـاه $\det(\mathbf{uv})=1$؛ همچنین $\det \mathbf{u}^{-1}=1$ وماتریس‌واحد نیزبه U تعلق دارد. بعلاوه $G \triangleright U$ زیرا اگر $\mathbf{x}\in G$، آنگاه

$$\det(\mathbf{x}^{-1}\mathbf{ux})=\det \mathbf{u}=1$$

اینك به‌آسانی دیده می‌شودکه دو ماتریس $\mathbf{a}$ و $\mathbf{b}$ فقط وفقط وقتی به‌یك همجموعه از U تعلق دارنـدکـه $\det \mathbf{a}=\det \mathbf{b}$؛ زیـرا ایـن بـا $\mathbf{ab}^{-1}\in U$ هم‌ارز است، چون که $\det(\mathbf{ab}^{-1})=1$. واضح است‌که دترمینان (این‌گونه ماتریسها) هرمقدار غیرصفر از F را اختیار می‌کند. اغلب مجموعهٔ عناصر غیرصفر F به $F^{\times}$ نشان داده می‌شود. لذا داریم

$$\frac{G}{U}\cong F^{\times}$$

یك تراگرد برای U در G (صفحهٔ ۳۸ ملاحظه شود)، فی‌المثل، به‌کمك ماتریسهای‌قطری $\operatorname{diag}(d,1,1,\ldots,1)$ که درآن d در $F^{\times}$ تغییر می‌کند، تهیه می‌شود.

بالاخره، نتیجه‌ای را درمورد مرکز گروه، که گاهی مفید می‌افتد ذکر می‌کنیم.

قضیهٔ ۸. اگر G غیرآبلی ومرکز آن Z باشد، درآن‌صورت G/Z هیچگاه دوری نیست.

برهان. اگر G/Z یك گروه دوری می‌بود، آنگاه کلیهٔ همجموعه‌های Z می‌توانستند به‌صورت Zt^i بیان شوند، که درآن t عنصر مناسبی است از G که در Z نیست و

$$i=0,\pm 1,\pm 2,\ldots$$

اما اگر x و y عناصر دلخواهی از G و به‌ترتیب متعلق به Zt^k و Zt^l باشند، باید داشته باشیم:

$$x=z_1t^k,\quad y=z_2t^l$$

که $z_1, z_2\in Z$ وبنابراین

$$xy=z_1t^kz_2t^l=z_1z_2t^{k+l}=yx$$

یعنی G آبلی خواهد بود، که با فرض ما درتناقض است.

فرع. یك گروه ازمرتبهٔ p^2، که p، عدد اول باشد، لزوماً آبلی است.

برهان. بنابر قضیهٔ اصلی ۷، $|Z|$ برابر p و یا برابر p^2 است. اگر $|Z|=p^2$، آنگاه $G=Z$، وگروه‌آبلی است. درغیر این‌صورت $|Z|=p$ و $|G/Z|=p$. بنابراین G/Z دوری خواهد بود، که بنابرقضیهٔ پیش قابل قبول نیست.

۲۱. همریختی. ساختار یك گروه متضمن قانونی است‌که به‌توسط آن کلیهٔ حاصلضربهای

ممکن ab ارزیابی می‌شوند. درفصل ۱ (صفحهٔ ۱۷) مواردی راکه در آن دو گروه یکریخت بودند، یعنی، دارای یك ساختار بودند، مورد بحث قرار دادیم. اکنون به‌بررسی رابطهٔ کلیتری که درآن گروهها، دارای ساختارهای «مشابه»اند یعنی گروههای همریخت ـ که اصطلاح یونانی آن **هوموورف** است ـ می‌پردازیم. بـه منظور دقیقتر کردن این مفهوم، فرض کنیم نگاشتی مانند

$$\theta : G \to G'$$

ازیك گروه G به‌توی گروه G' داشته باشیم. همانند قبل، نگارهٔ $x \in G$ با $x\theta$ نشان داده می‌شود. به‌طوری‌که $x' = x\theta$ عنصر منحصر به‌فردی از G' است‌که به‌توسط نگاشت θ با x متناظر می گردد. θ را یك نگاشت همریخت، یا مختصراً، یك همریختی از G به‌توی G' نامیم هرگاه به‌ازای هر $x, y \in G$،

$$(x\theta)(y\theta) = (xy)\theta \qquad (۱۷.۳)$$

این تنها شرطی است‌که برای θ قائل می‌شویم. نکات ذیل را باید دقیقاً متذکر شویم:

(الف) فرض کنیم ۱ و $'۱$ به‌ترتیب عناصر واحد G و G' باشند. با اختیار کردن $x = y = ۱$ داریم $۱\theta = (۱\theta)^۲$. لذا ۱θ عنصری است خودتوان از G'، و بنابراین (صفحهٔ ۸)

$$۱\theta = ۱' \qquad (۱۸.۳)$$

یعنی، هرهمریختی عنصر واحد G را به‌عنصر واحد G' می‌نگارد. بعلاوه، اگر قرار دهیم $y = x^{-۱}$، از (۱۷.۳) نتیجه می گیریم که

$$x^{-۱}\theta = (x\theta)^{-۱} \qquad (۱۹.۳)$$

(ب) ما خواستار آن نیستیم که این نگاشت یك به‌یك باشد، لذا ممکن است چنین اتفاق‌افتدکه $x_۱\theta = x_۲\theta$ ولی $x_۱ \neq x_۲$. با این‌حال، اگر همواره ازمعادلهٔ $x_۱\theta = x_۲\theta$ لازم آیـدکه $x_۱ = x_۲$، آنگاه گوییم θ یك **تکریختی** یا یك نگاشت **یك به‌یك** (انژکتیو) است.

(ج) درحالت کلی، فرض براین نیست‌که θ پوشا باشد. به‌عبارت دیگر، ممکن‌است عناصری از G' موجود باشندکه نگارهٔ عناصری از G نباشند. مجموعهٔ نگاره‌ها با $\mathrm{im}\,\theta$، یا به‌نحومناسبتر با $G\theta$، نشان داده می‌شود. به‌آسانی دیده می‌شودکه $G\theta$ یك زیر گروه‌از G است (که ممکن است بر G' منطبق باشد)؛ در واقع اگر $x', y' \in G\theta$، عناصری از G مانند x و y وجود دارند به‌قسمی که $x' = x\theta$ و $y' = y\theta$. ازاین‌رو $x'y' = (xy)\theta \in G\theta$. همچنین بنابر (۱۸.۳)، $۱' \in G\theta$ و اگر $x' \in G\theta$، $(x')^{-۱} \in G\theta$. ازطرف دیگر، اگر θ پوشا باشد، یعنی اگر

$$G\theta = G' \qquad (۲۰.۳)$$

آنگاه θ را یك بر ریختی (**اپی مورفیسم**) می‌نامیم. هریکریختی (به‌معنی قبلی) به‌وسیلهٔ این حقیقت مشخص می‌شود که هم یك‌به‌یك است و هم‌پوشا، یا به‌طور خلاصه **یك‌به‌یك دوسویی** (بیژکتیو) است. این حالت را با نماد $G \cong G'$ نشان می‌دهیم.

اکنون این حقیقت مهم را ثابت می‌کنیم که هر نگاشت همریخت G، به‌یك زیرگروه نرمال G وابسته است. فرض‌کنیم K مجموعهٔ عناصری از G باشد که به $'۱$ نگاشته می‌شود. این مجموعه هستهٔ (مرکزی) θ خوانده می‌شود و اغلب به صورت $\ker\theta$ نوشته می‌شود. حالا نشان می‌دهیم که K یك زیرگروه G است؛ اگر $u, v \in K$، آنگاه $u\theta = v\theta = 1'$ و ازاین‌رو، بنابر(۱۷۰۳)، $(uv)\theta = 1'$؛ همچنین بنابر(۱۸۰۳)، $1 \in K$ و بنابر (۱۹۰۳)، $u^{-1} \in K$. بعلاوه، K یك زیرگروه نرمال است، زیرا اگر $x \in G$ و $u \in K$، آنگاه

$$(x^{-1}ux)\theta = (x\theta)^{-1}(u\theta)(x\theta) = (x\theta)^{-1}1'(x\theta) = 1'$$

که بدین‌معنی است که $x^{-1}ux \in K$. لذا تحقیق کرده‌ایم که (۱۰۰۳) برای گروه K برقرار می‌باشد، یعنی

$$K \lhd G \qquad (۲۱۰۳)$$

البته، ممکن است چنان اتفاق افتد که K زیرگروه واحد G باشد. دراین باره تذکر نتیجهٔ ذیل مفید است.

قضیهٔ ۹. همریختی θ یك به‌یك (انژکتیو) است اگر، و فقط اگر، $\ker\theta$ فقط از عنصر واحد تشکیل شده باشد.

برهان. فرض‌کنیم θ یك به‌یك و $u \in \ker\theta$. پس

$$1\theta = u\theta = 1'$$

لذا $u = 1$، زیرا θ یك به‌یك است. بعکس، فرض‌کنیم $\ker\theta = \{1\}$، و فرض می‌کنیم که $x\theta = y\theta$. دراین صورت

$$(xy^{-1})\theta = (x\theta)(y\theta)^{-1} = 1'$$

پس $xy^{-1} \in \ker\theta$، و بنابراین $xy^{-1} = 1$، یعنی $x = y$، که ثابت می‌کند θ یك‌به‌یك است.

اکنون به‌حالت کلی برمی‌گردیم و در موقعیتی هستیم که می‌توانیم یکی از مهمترین حقایق نظریه‌گروهها را ثابت کنیم.

قضیهٔ اصلی ۸ (نخستین قضیهٔ یکریختی*). فرض‌کنیم $\theta: G \to G'$ یك همریختی

---

* همچنان‌که خواهیم دید چندین‌قضیهٔ اصلی دربارهٔ یکریختی وجود دارد. متأسفانه، درفرهنگ ریاضی هیچ اتفاق‌آرایی درباره شماره‌گذاری آنها وجود ندارد.

از G به‌توی G' با گروه نگارهٔ $G\theta$ و هستهٔ K باشد. دراین صورت

$$\frac{G}{K} \cong G\theta \tag{۲۲.۳}$$

برهان. باید یك همریختی دوسویی بین دو گروه مذکور در (۲۲.۳) پدید آوریم. این امر به‌کمك نگاشتی مانند ϕ، وابسته به θ و یا «القاشده» به‌وسیلهٔ θ، انجام می‌گیرد، که درحالت کلی متمایز از θ است. خاطرنشان می‌سازیم که عناصر G/K همجموعه‌های Kx هستند، درصورتی که عناصر $G\theta$ به‌صورت $x\theta$ اند، که در آنها $x \in G$، وکلیهٔ عناصر Kx دارای یك نگاره می‌باشند. لذا فکر وجود تناظری یك‌به‌یك مانند ϕ براساس تعریف

$$(Kx)\phi = x\theta \tag{۲۳.۳}$$

در ذهن قوت می‌گیرد. بـا اینکه صحت این نظر معلوم خواهد شد، تعریف (۲۳.۳) بدون توجیه بیشتر نمی‌تواند قابل‌قبول باشد. زیرا می‌دانیم (قضیهٔ ۵، صفحهٔ ۳۷) که عنصر مولد x در Kx منحصر به‌فرد نیست، و ما ناچاریم خود را متقاعد کنیم که هرگاه

$$Kx = Ky \tag{۲۴.۳}$$

آنگاه $x\theta = y\theta$. فقط دراین شرایط است کـه ϕ به‌کمك (۲۳.۳) تعریف مشخصی پیدا می‌کند، وجلوی ناسازگاریهای زیانبار گرفته می‌شود. حال گوییم (۲۴.۳) با گزارهٔ $y = ux$ که در آن $u \in K$، هم‌ارز است. بنابر تعریف K، $u\theta = 1'$ و لذا $y\theta = u\theta\, x\theta = x\theta$، یعنی همان چیزی که ما می‌خواستیم. اکنون می‌توانیم نشان دهیم که ϕ کلیهٔ خواصی را که درجستجوی آنیم داراست.

(۱) ϕ یك همریختی است؛ زیرا

$$((Kx)(Ky))\phi = (Kxy)\phi = (xy)\theta = (x\theta)(y\theta) = (Kx)\phi(Ky)\phi$$

(۲) ϕ پوشاست؛ این واضح است، زیرا در (۲۳.۳) x می‌تواند هر عنصر G را اختیار کند، به‌طوری که کلیهٔ عناصر مجموعهٔ نگاره $x\theta$ براثر ϕ پوشیده می‌شوند.

(۳) ϕ یك‌به‌یك (انژکتیو) است؛ باید ثابت کنیم که تساوی

$$(Kx)\phi = (Ky)\phi \tag{۲۵.۳}$$

وجود تساوی $Kx = Ky$ را ایجاب می‌کند. اگـر (۲۵.۳) مفروض باشد، آنگاه بنابر تعریف ϕ، $x\theta = y\theta$. این بـدان معنی است کـه $xy^{-1} \in K$، کـه هم‌ارز است بـا $Kx = Ky$.

با این تساوی برهان قضیه به‌اثبات می‌رسد. این قضیه را می‌تـوان به‌عبارت دیگر چنین بیان کرد کـه هرنگارهٔ همریخت G با یك گروه خارج‌قسمت G، یعنی خارج‌قسمت G برهستهٔ مربوطه، یکریخت است.

برای آنکه این موضوع را به‌طرز مناسبی به پایان برسانیم، متذکر می‌شویم که هر زیرگروه نرمال G به‌صورت هستهٔ همریختی مناسبی درمی‌آید. فرض کنیم $N \lhd G$ و نگاشت $\nu: G \to G/N$ راکه با ضابطهٔ

$$x\nu = Nx \quad (x \in G) \qquad (۲۶.۳)$$

تعریف می‌شود، درنظرمی‌گیریم. پس، دراین‌حالت، $G' = G/N$. به‌آسانی تحقیق‌می‌شود که (۲۶.۳) یك همریختی است؛ زیرا

$$(x\nu)(y\nu) = NxNy = Nxy = (xy)\nu$$

واضح است که ν در واقع یك برریختی است، زیرا در (۲۶.۳) x می‌تواند هرعنصر G باشد، و بنابراین تمامی G/N پوشیده شده است. هستهٔ ν متشکل ازآن عناصر $u \in G$ است‌که به‌ازای آنها $Nu = N$ (N عنصر واحد در G/N است)؛ این با شرط $u \in N$ هم‌ارز است. لذا $\ker\nu = N$. نگاشت تعریف‌شده در (۲۶.۳) **نگاشت طبیعی** G به‌روی G/N خوانده می‌شود.

برای روشن ساختن مطلب، به مثال (ج) صفحهٔ ۷۲ برمی‌گردیم، که در آن $G = GL(n, F)$. اگر $\mathbf{a} \in G$، همریختی

$$\delta: G \to F$$

راکه به‌وسیلهٔ

$$\mathbf{a}\delta = \det \mathbf{a}$$

تعریف می‌شود درنظر می‌گیریم. دراین حالت $G\delta = F^{\times}$، و هسته ازگروه

$$U = \{\mathbf{a} \mid \det \mathbf{a} = ۱\}$$

تشکیل می‌گردد. و این خود به خود یك زیرگروه نرمال G است. بنابرقضیهٔ اصلی ۸، همچنان‌که قبلاً داشتیم، داریم

$$\frac{G}{U} \cong F^{\times}$$

نخستین قضیهٔ یکریختی بینش روشنتری درمورد تأثیر همریختی $\theta: G \to G'$ به‌ما می‌دهد: کلیهٔ عناصر Kx دارای نگارهٔ $x' = x\theta$ هستند؛ بخصوص، وقتی‌که $|K|$ متناهی است، گروه‌نگارهٔ $G\theta$ دقیقاً $|K|$ مرتبه پوشیده می‌شود. بعلاوه وقتی‌که اندیس $[G:K]$ متناهی باشد، داریم

$$|G\theta| = [G:K] \qquad (۲۷.۳)$$

۲۲. زیرگروههای گروههای خارج‌قسمت. فرض کنیم $N \lhd G$ زیر گروه نرمالی از G باشد. می‌خواهیم زیرگروههای G/N را بررسی و رابطهٔ آنها را با زیرگروههای

G مطالعه کنیم. به منظور احتراز از تشتت لازم است موقتاً علاماتی را که اندکی ابتکاری‌تر هستند برای عناصر G/N وارد کنیم. حال یك عنصر نمونه از G/N را به‌صورت (Nx) می‌نویسیم تا از زیر مجموعهٔ Nx که از $|N|$ عنصر G تشکیل شده تمیز داده شود. یك زیر گروه A' از G/N گردایه‌ای است ازعناصر مانند

$$A'=(N)\cup(Na)\cup(Nb)\cup\cdots \qquad (۲۸.۳)$$

که در بنداشتهای گروه مربوط به‌قانون ترکیب G/N صدق می‌کنند. از حذف پرانتزها زیرمجموعهٔ زیرین از G را به‌دست می‌آوریم

$$A=N\cup Na\cup Nb\cup\cdots \qquad (۲۹.۳)$$

گوییم که‌درحقیقت A یك زیر گروه G است. بدیهی‌است که $N\subset A$ و ازاین‌رو $1\in A$. بعد، اگر x و y عناصری از A باشند، آنگاه Nx و Ny عناصری از A' اند؛ چون A' یك‌زیر گروه است، لذا $(Nxy)\in A'$، که به‌نوبهٔ خود ایجاب‌می‌کند که $xy\in A$. بالاخره، اگر $x\in A$ ، آنگاه $(Nx^{-1})\in A'$، و ازاین‌رو $x^{-1}\in A$. پس نشان داده‌ایم که A یك گروه است، و دقیقتر ازآن نشان داده‌ایم که

$$N\leqslant A\leqslant G \qquad (۳۰.۳)$$

بعکس، اگر A زیر گروهی دلخواه از G باشد که در (۳۰.۳) صدق کند، متذکر می‌شویم که درواقع $N\lhd A$ ؛ زیرا رابطهٔ $x^{-1}Nx=N$ که برای کلیهٔ عناصر x از G برقرار می‌باشد، بویژه‌برای کلیهٔ x هایی که در A واقع‌اند نیز برقرار است. بنابراین‌تشکیل گروه خارج قسمت A/N بجا می‌باشد. حال گوییم هرگاه (۲۹.۳) تجزیهٔ هممجموعه‌ای A نسبت به N باشد، آنگاه با درج پرانتزها، A/N را به‌دست می‌آوریم که یك زیر گروه G/N است. روشن است که، زیر گروههای متمایز A' و B' از G/N زیر گروههای متمایز A و B از G را به‌دست می‌دهند که هر یك متضمن N است وبعکس. لذا یك تناظر یك‌به‌یك بین زیر گروههای G/N و زیر گروههایی از G که شامل N اند وجود دارد.

پرسش جالب این است که بخواهیم بدانیم چگونه زیر گروههای نرمال G/N را دراینجا می‌توانیم بیان کنیم. می‌توانیم فرض کنیم کـه چنین زیر گروهی به‌صورت A/N بیان می‌شود که در آن A در (۳۰.۳) صدق می‌کند. اما

$$\frac{A}{N}\lhd\frac{G}{N} \qquad (۳۱.۳)$$

فقط و فقط وقتی که، به‌ازای هر $x\in G$ و هر $a\in A$، داشته باشیم

$$(Nx)^{-1}(Na)(Nx)=(Nx^{-1}ax)\in\frac{A}{N}$$

و این هم‌ارز است با شرط

$$x^{-1}ax \in A$$

به‌عبارت دیگر، با این شرط که $A \lhd G$. این نتایج را به‌طریق ذیل خلاصه می‌کنیم.

قضیهٔ ۱۰. کلیهٔ زیرگروههای G/N می‌توانند به‌صورت A/N بیان شوند، که

$$N \leqslant A \leqslant G$$

فقط و فقط وقتی $A/N \lhd G/N$، که

$$N \lhd A \lhd G$$

هر گاه کار را با G/N شروع و فرض کنیم که (۳۱.۳) برقرار است، آنگاه می‌توانیم گروه خارج‌قسمت

$$\left(\frac{G}{N}\right) \bigg/ \left(\frac{A}{N}\right)$$

را بسازیم. خوشبختانه، پیچیدگی ناشی از تشکیل یك خارج‌قسمت ازگروههای خارج‌قسمت با قضیهٔ آتیه کمتر می‌شود.

قضیهٔ اصلی ۹ (دومین قضیهٔ اصلی یکریختی). فرض‌کنیم $N \lhd G$ و A یك زیرگروه نرمال G باشد که

$$N \lhd A \lhd G$$

در این صورت

$$\left(\frac{G}{N}\right) \bigg/ \left(\frac{A}{N}\right) \cong \frac{G}{A} \qquad (۳۲.۳)$$

برهان. نگاشت

$$\phi : G/N \to G/A$$

را که به‌توسط قاعدهٔ

$$(Nx)\phi = (Ax) \quad (x \in G) \qquad (۳۳.۳)$$

تعریف شده درنظر می‌گیریم. ابتدا باید بررسی کنیم که (۳۳.۳) در واقع یك تعریف بامعنی است. می‌توان عنصر x سمت‌چپ را با ux، که در آن $u \in N$، تعویض کرد بی‌آنکه همجموعه Nx تغییر کند؛ وما باید نشان دهیم که این جانشین‌سازی، طرف راست(۳۳.۳) را عوض نمی‌کند. چون $N \leqslant A$، داریم $u \in A$، که ازآنجا نتیجه می‌شود $Au = A$ (قضیهٔ ۳ صفحهٔ ۳۵). و درنتیجه $Aux = Ax$، واین همان چیزی است که می‌خواستیم. ملاحظه

می‌کنیم که ϕ یك همریختی است؛ زیرا به‌دلیل نرمال بودن A،

$$(Nx)\phi(Ny)\phi=(Ax)(Ay)=(Axy)=(Nxy)\phi$$

واضح است که ϕ پوشاست، زیرا، در (۳۳.۳)، x عنصر دلخواهی از G است، وبنابراین کلیهٔ هممجموعه‌های A درطرف راست (۳۳.۳) ظاهر می‌شوند؛ پس

$$\left(\frac{G}{N}\right)\phi=\frac{G}{A} \qquad (۳۴.۳)$$

باقی می‌ماند اینکه هستهٔ ϕ را پیداکنیم. اکنون گوییم $(Nx)\in\ker\phi$، فقط و فقط وقتی که $(A)=(Ax)$ یعنی عنصر واحد G/A باشد؛ که با شرط $x\in A$ هم‌ارز است. ازاین‌رو $\ker\phi$ اجتماع هممجموعه‌های (Na) است، که a در A تغییر می‌کند. به‌عبارت دیگر

$$\ker\phi=\frac{A}{N} \qquad (۳۵.۳)$$

با استفاده از (۳۴.۳) و (۳۵.۳) بدین نتیجه می‌رسیم که (۳۲.۳) نتیجهٔ بلافصل قضیهٔ اول یکریختی است.

بار دیگر به‌حالت کلی همریختی

$$\theta: G\rightarrow G' \qquad (۳۶.۳)$$

برمی‌گردیم، ومی‌خواهیم بدانیم چگونه این نگاشت بر زیرگروه مفروض A از G تأثیر می‌کند. این بدان معنی است که ما نگاشت تحدید

$$\theta_A: A\rightarrow G' \qquad (۳۷.۳)$$

راکه به‌توسط قاعدهٔ بدیهی

$$a\theta_A=a\theta \quad (a\in A)$$

تعریف شده درنظر بگیریم. ممکن است واردکردن نماد جدید θ_A، امر زایدی به‌نظرآید، وعملاً نیزگاهی ازاختلاف بین θ و θ_A صرفنظرمی‌شود. ولی می‌توان براین نکته‌پافشاری کردکه (۳۶.۳) و (۳۷.۳) نگاشتهای متمایزی هستند زیرا «حوزهٔ تعریف» متفاوتی دارند. همانندکلیهٔ همریختیها گروه نگارهٔ

$$A'=A\theta_A \quad (=A\theta)$$

یك زیرگروه G' می‌باشد، وحال آنکه روشن است که هستهٔ آن متشکل از عناصری از A است که درهستهٔ θ قرار دارند، یعنی

$$\ker\theta_A=A\cap\ker\theta \qquad (۳۸.۳)$$

اکنون هنگام آن است که به‌بررسی مفصلتر حالتی که این برریختی طبیعی

$$\nu : G \to \frac{G}{N}, \quad x\nu = (Nx)$$

به‌زیرگروه A از G محدود شده است بپردازیم. می‌توان گروه نگاره را به‌گونهٔ توضیحی چنین نوشت

$$A' = A\nu_A = \bigcup_a (Na) \tag{۳۹.۳}$$

که a در A تغییر می‌کند، باوجود این باید متذکر شویم که ممکن است این اجتماع شامل جملات زایدی باشد. ازطرف دیگر A' یك زیرگروه G/N است، وهمچنان‌که در صفحهٔ ۷۸ ملاحظه‌کرده‌ایم، باید به‌صورت $A' = B/N$ باشد، که $N \leqslant B \leqslant G$. در وضعیت حاضر نمی‌توان گفت که $B = A$، زیرا A لزوماً شامل N نیست به‌طوری که A/N بیمعنی خواهد بود. قاعدهٔ یافتن B درصفحهٔ ۷۸ داده شده است وآن عبارتست از برداشتن پرانتزها در (۳۹.۳)، لذا

$$B = \bigcup Na, \quad (a \in A)$$

می‌توان این را برحسب قرارداد زیرمجموعه‌ها خلاصه‌تر بیان کرد، بدین قرار

$$B = NA$$

آموزنده است که زیرگروه بودن B را بـه روش دیگری نیز تحقیق کنیم. زیرا چون N نرمال است، به‌ازای هر $a \in A$ داریم $Na = aN$ وبنابراین $NA = AN$. لذا بنابرقضیهٔ اصلی حاصلضرب (صفحهٔ ۵۸)، B یك گروه است. ضمناً متذکر می‌شویم که

$$A\nu_A = \frac{NA}{N} \tag{۴۰.۳}$$

اما بعد، چون $\ker \nu = N$، از (۳۸.۳) نتیجه می گیریم که

$$\ker \nu_A = A \cap N \tag{۴۱.۳}$$

و متذکر می‌شویم که چون $A \cap N$ یك هسته است، پس در A نرمال است.

قضیهٔ اصلی اول یکریختی راکه بر ν_A اعمال‌کنیم بیان می‌دارد که

$$\frac{A}{\ker \nu_A} \cong A\nu_A$$

از قراردادن (۴۰.۳) و (۴۱.۳) دراین رابطه، این نتیجه را به‌طریق ذیل به‌شکلی جدید مطرح می‌کنیم.

قضیهٔ اصلی ۱۰ (سومین قضیهٔ اصلی یکریختی). فرض‌کنیم N یك زیرگروه نرمال و A یك زیرگروه دلخواه G باشند. دراین صورت

$$\frac{A}{A\cap N}\cong\frac{NA}{N}$$

حال‌جا دارد که به بررسی حاصلضرب مستقیم داخلی (صفحهٔ ۴۸) برحسب زیر گروههای نرمال بپردازیم. اگر

$$G=H\times K \qquad (۴۲.۳)$$

آنگاه هرعنصر H با هرعنصر K تعویضپذیر است؛ لـذا اگر $v\in K$، به‌طور قطع داریم $v^{-۱}Hv=H$. همچنین اگـر $u\in H$، آنگاه $u^{-۱}Hu=H$ (قضیهٔ ۳، صفحهٔ ۳۵). چون هرعنصر $x\in G$ می‌تواند به‌صورت $x=uv$ بیان شود، ازاینجا نتیجه‌می‌شود که $x^{-۱}Hx=H$. بنابراین $H\lhd G$. و، به‌طریق مشابه، $K\lhd G$، یعنی، در یك حاصلضرب مستقیم، هر عامل یك زیرگروه نرمال است.

بعد، ملاحظه می‌کنیم که

$$G/K\cong H \qquad (۴۳.۳)$$

این رابطه بلافاصله از قضیهٔ اصلی سوم یکریختی نتیجه‌می‌گردد، هر گاه قرار دهیم $K=N$ و $H=A$، و توجه‌کنیم که $KH=H\times K=G$، آنگاه $H\cap K=\{۱\}$. به‌طریق دیگر، بااستفاده از یك بحث مستقیم‌تر ملاحظه می‌کنیم که هرهمجموعهٔ K در G به‌صورت Ku است کـه در آن $u\in H$، برای آنکه هر گاه $x=uv$($u\in H$ و $v\in K$) عنصر دلخواهی از G باشد، آنگاه

$$Kx=Kuv=Kvu=Ku$$

زیرا $Kv=K$. همچنین، اگر $Ku_۱=Ku_۲$، که $u_۱, u_۲\in H$، آنگاه

$$u_۱u_۲^{-۱}\in H\cap K=\{۱\}$$

وبنابراین $u_۱=u_۲$. از این‌رو

$$Ku\rightarrow u$$

یك همریختی یك‌به‌یك دوسویی بین گروههای G/K و H پدید می‌آورد.

واضح است که به‌موجب تناظر

$$(u,v)\leftrightarrow(v,u),\ (u\in H, v\in K)$$

خواهیم داشت:

$$H\times K\cong K\times H$$

۲۳. گروه مشتق. به ازای هردو عنصر x و y از یـك گروه G، **تعویضگر** آنها را چنین تعریف می‌کنیم

$$[x, y] = x^{-1}y^{-1}xy$$

روشن است که فقط و فقط وقتی $[x, y] = 1$، که $xy = yx$. ما می‌خواهیم مجموعهٔ کلیهٔ تعویضگرها را مطالعه کنیم وقتی که x و y روی G تغییر می‌نمایند. ولی این مجموعه درحالت کلی تشکیل یك گروه نمی‌دهد، زیرا حاصلضرب دو تعویضگر را نمی‌توان همیشه به‌صورت یك تعویضگر بیان کرد. (حقیقت جالب این است که این نقص فقط در گروههای نسبتاً پیچیده آشکار می‌شود.) به‌هرحال، می‌توانیم گروهی بسازیم که به‌وسیلهٔ کلیهٔ تعویضگرها تولید شده باشد؛ این گروه، **گروه مشتق** یا **گروه تعویضگر** G خوانده می‌شود و معمولاً به G' نشان داده می‌شود، یعنی

$$G' = \operatorname{gp}\{[x, y] \mid x, y \in G\} \tag{۴۴.۳}$$

لذا یك عنصر نوعی از G'، حاصلضربی متناهی از تعویضگرهاست. واضح است که فقط وفقط وقتی $G' = \{1\}$، که G آبلی باشد ویژگیهای اصلی G' در قضیهٔ ذیل گردآورده شده‌اند:

قضیهٔ اصلی ۱۱. (الف) گروه مشتق G' یك زیرگروه نرمال G است، و G/G' آبلی می‌باشد. (ب) اگر H یك زیرگروه نرمال دلخواه G باشد به‌قسمی‌که G/H آبلی باشد، آنگاه $G' \leqslant H$.

برهان. (الف) برای آنکه نشان دهیم $G' \lhd G$، کافی است ثابت کنیم که به‌ازای هر $t \in G$

$$[x, y]^t \in G'$$

(به (۲.۳) و (۱۰.۳) مراجعه شود.) به‌موجب قواعد (۳.۳) و $'$(۳.۳) داریم

$$[x, y]^t = [x^t, y^t]$$

چون سمت‌راست این تساوی یك تعویضگر است، پس به G' تعلق دارد. ازاین‌رو $G' \lhd G$. اما بعد، ثابت می‌کنیم که هممجموعه‌های $G'x$ و $G'y$ تعویضپذیرند یا به‌صورتی دیگر

$$[G'x, G'y] = G'$$

اما

$$\begin{aligned}[G'x, G'y] &= (G'x)^{-1}(G'y)^{-1}(G'x)(G'y)\\ &= G'x^{-1}y^{-1}xy = G'[x, y] = G'\end{aligned}$$

زیرا $[x, y] \in G'$. لذا G/G' آبلی است.

(ب) اگر $H \lhd G$، می‌توانیم محاسبهٔ فوق را به‌جای G' با H تکرار وپیدا کنیم

$$[Hx, Hy] = H[x, y]$$

هرگاه G/H آبلی باشد. سمت چپ این تساوی به‌عنصر واحد G/H، یعنی به H،

تبدیل می‌یابد و از آنجا نتیجه می‌گیریم که $[x, y] \in H$. چون x و y دلخواه‌اند، نتیجه می‌گیریم که هرمولد G' در H قراردارد، و از اینجا نتیجه می‌شود که $G' \leqslant H$.

این بخش را با اثبات قضیهٔ ذیل به‌پایان می‌رسانیم.

قضیهٔ ۱۱. فرض کنیم A و B زیرگروههای نرمال G باشند به‌قسمی‌که $A \cap B = \{1\}$. در این صورت هرعنصر A با هرعنصر B تعویض‌پذیر است.

برهان. تعویضگر

$$c = a^{-1}b^{-1}ab$$

را که a و b به‌ترتیب عناصر دلخواهی از A و B می‌باشند، در نظر می‌گیریم. چون $A \lhd G$، پس $a_1 = b^{-1}ab \in A$ و بنابراین $c = a^{-1}a_1 \in A$؛ به‌طریق مشابه $c \in B$. لذا $c \in A \cap B = \{1\}$، که از اینجا نتیجه می‌شود $c = 1$، یعنی $ab = ba$.

۲۴. خود ریختیها. یك نوع جالب ازیکریختی G زمانی پیدا می‌شود که گروه نگاره بر G منطبق باشد. هر یکریختی مانند

$$\alpha : G \rightarrow G$$

از G به‌روی خودش را یك **خود ریختی** از G می‌نامیم. به‌ویژه، α یك نگاشت یك به یك دوسویی از G به‌روی خودش است، یعنی α تمامی عناصر G را با هم عوض می‌کند. البته عکس این درست نیست، زیرا علاوه براین α باید دررابطهٔ

$$(xy)\alpha = (x\alpha)(y\alpha) \quad (x, y \in G) \tag{۴۵.۳}$$

نیز صدق کند. بااعمال ملاحظات صفحهٔ ۲۱، نتیجه می‌گیریم که گردایهٔ کلیهٔ خود ریختیهای G نسبت به‌ترکیب نگاشتها یك گروه تشکیل می‌دهند. اگر

$$\beta : G \rightarrow G$$

یك خود ریختی دیگـر باشد، حاصلضرب α و β را به‌جای $\alpha \circ \beta$، به $\alpha\beta$ نشان می‌دهیم. لذا اثر $\alpha\beta$ برعنصری چون $x \in G$ به‌وسیلهٔ قاعده

$$x(\alpha\beta) = (x\alpha)\beta$$

تعـریف می‌شود. گـروه کلیهٔ خـود ریختیهای G بـه $A(G)$ نشان داده می‌شود و **گروه خود ریختیهای** G نامیده می‌شود. عنصر واحد $A(G)$ خود ریختی همانی ι است که‌هرعنصر G را ثابت نگه می‌دارد، یعنی

$$x\iota = x \quad (x \in G) \tag{۴۶.۳}$$

عکس α با α^{-1} نشان داده می‌شود. لذا $x\alpha^{-1}$ عنصر منحصر به‌فرد y از G است کـه در $y\alpha = x$ صدق می‌کند؛ به‌ازای هر x چنین عنصری وجود دارد زیرا که α پوشاست.

چون α یك به‌یك است، $\ker\alpha=\{1\}$. از اینجا نتیجه می‌شود که α مرتبهٔ هرعنصر را حفظ می‌کند. زیرا اگر $x\alpha=y$ و $x^m=1$، آنگاه بنابر (۴۵.۳)،

$$1=x^m\alpha=(x\alpha)^m=y^m$$

بنابراین مرتبهٔ y کوچکتر از مرتبه x نیست. با استفاده از α^{-1} به‌جای α، می‌توانیم نامساوی عکس آن را اثبات کنیم. لذا x و y دارای یك مرتبه می‌باشندکه ممکن است این مرتبه نامتناهی باشد. با یك عنصر ثابت t از G نگاشت

$$\tau: G\to G$$

با ضابطهٔ

$$x\tau=x^t\ \ (=t^{-1}xt)\ \ (x\in G) \qquad (۴۷.۳)$$

را وابسته می‌کنیم. معادلهٔ (۳.۳) نشان‌می‌دهدکه τ یك‌همریختی از G به‌روی G می‌باشد. درواقع این یك خود ریختی است. زیرا، $x^t=1$ نتیجه می‌دهد که $x=1$؛ لذا هستهٔ τ به‌عنصر واحد بدل می‌شودکه از این، بنابرقضیهٔ ۹، نتیجه می‌شودکه τ یك‌به‌یك (انژکتیو) است. باز، اگر y عنصری از G باشد،عنصری‌چون x هست که $x^t=y$، یعنی $x=tyt^{-1}$؛ لذا τ پوشاست. یك خود ریختی نظیر (۴۷.۳)، که به‌وسیلهٔ ازدواج نتیجه می‌شود، یك **خود ریختی داخلی** G خوانده می‌شود. یك خود ریختی که خود ریختی داخلی نباشد، **خود ریختی خارجی** نامیده می‌شود.

حال نشان می‌دهیم که گردایهٔ کلیهٔ خود ریختیهای داخلی یك گروه، $I(G)$، نسبت به‌ترکیب نگاشتنها یك گروه تشکیل می‌دهد. پس، فرض می‌کنیم σ خود ریختی داخلی دیگری باشدکه با رابطهٔ

$$x\sigma=s^{-1}xs\quad (x\in G)$$

داده شده است. دراین‌صورت

$$x\tau\sigma=(t^{-1}xt)\sigma=s^{-1}t^{-1}xts$$
$$=(ts)^{-1}x(ts)$$

یعنی

$$x^tx^s=x^{ts} \qquad (۴۸.۳)$$

بنابراین نگاشت مرکب $\tau\sigma$ بدازدواج به‌توسط ts متناظر می‌شود،که بسته بودن $I(G)$ را ثابت می‌کند. روشن است که $\iota\in I(G)$: زیرا می‌توان t را مساوی ۱ انتخاب کرد، و τ^{-1} متناظر بدازدواج به‌توسط t^{-1} خواهد شد؛ یعنی

$$x\tau^{-1}=txt^{-1}\ \ (x\in G)$$

اطلاع دقیقتر درموردگروه $I(G)$ به‌توسط قضیهٔ ذیل داده شده است.

قضیهٔ ۱۲. فرض‌کنیم Z مرکز G باشد. در این صورت

$$I(G)\cong G/Z$$

برهان. تناظر بین یك عنصر t و خودریختی‌داخلی τ، که از t ناشی می‌شود، به‌وسیلهٔ نگاشت

$$\Phi : G \to I(G) \tag{۴۹.۳}$$

بیان، و با ضابطهٔ

$$t\Phi=\tau \quad (t\in G)$$

تعریف شده است. اما معادلهٔ (۴۸.۳) نشان می‌دهد که

$$(ts)\Phi=(t\Phi)(s\Phi)$$

یعنی Φ یك همریختی‌است. واضح است که Φ پوشا نیز می‌باشد زیراهرخودریختی‌داخلی به‌وسیلهٔ اعمال Φ برعنصر مناسبی از G به‌دست‌آمده است؛ بنابراین

$$G\Phi=I(G)$$

بعد، می‌خواهیم $\ker\Phi$ را بیابیم. اما رابطهٔ $t\in\ker\Phi$ فقط وفقط زمانی برقرار است‌که خود ریختی داخلی حاصل از t خود ریختی همانی باشد

$$x^t=x \quad (x\in G)$$

اما ایـن معادله هم‌ارز بـا حکم $t\in Z$ است. پس $\ker\Phi=Z$. استفاده از اولین قضیهٔ اصلی یکریختی، بلافاصله ادعای ما را ثابت می‌کند.

در یك گروه آبلی کلیهٔ خود ریختیهای داخلی به‌نگاشت همانی بـدل می‌شوند، پس خود ریختیهای خارجی تنها خود ریختیهای نابدیهی‌اند. مثالهای سادهٔ ذیل توضیحی‌برای منظور ما هستند.

(۱) گروه دوری نامتناهی $C=\mathrm{gp}\{x\}$. هرهمریختی α به‌محض معلـوم‌شدن $x\alpha$، مثلاً* $x\alpha=x^s$، (s عددی صحیح)، مشخص می‌شود. اگر x^k عنصری دلخواه از C باشد، آنگاه $x^k\alpha=(x\alpha)^k=x^{ks}$. لذا گروه نگاره عبارت است از $C\alpha=\mathrm{gp}\{x^s\}$. اما برای یك خود ریختی، داریم $C\alpha=C$. بنابرایـن باید داشته باشیم ۱ $=s$ یـا ۱ $-=s$. هردو حالت امکان‌پذیرند، درحالت اول نگاشت‌مورد بحث نگاشت همانی است. لذا C دقیقاً دارای دوخودریختی می‌شود.

(۲) گروه دوری متناهی $C_m=\mathrm{gp}\{x|x^m=1\}$. مانند مثال قبل، فقط $x\alpha=x^s$ احتیاج به‌مشخص شدن دارد. درهرخود ریختی مرتبهٔ هرعنصر حفظ می‌شود. از این‌رو x^s باید از مرتبهٔ m باشد؛ و این امر فقط وفقط وقتی اتفاق می‌افتدکه ۱ $=(s, m)$ (قضیهٔ ۲، صفحهٔ ۲۵ ملاحظه‌شود)، وهرچنین انتخابی از s، منجر به پیدایش یك خود ریختی می‌شود. لذا C_m دارای $\phi(m)$خود ریختی‌است که‌در آن ϕ تابع اویلر تعریف شده‌درصفحهٔ ۱۲ است.

(۳) گروه چاروینه $V=\mathrm{gp}\{a, b|a^{۲}=b^{۲}=۱, ab=ba\}$. این گروه سه عنصر مرتبهٔ دو دارد که فقط این سه‌عنصر بر اثر α به‌هم تبدیل می‌شوند. نتیجه اینکه هریك از این شش جایگشت یك خود ریختی را معین می‌کند؛ برای آنکه هر گاه سه‌عنصر مرتبهٔ دو به x، y، z نشان داده شده باشند (به‌هر ترتیبی)، آنگاه $xy=z$. بنابراین اگر $x\alpha=x'$، $y\alpha=y'$ و $z\alpha=z'$، آنگاه $x'y'=z'$. در نتیجه V دارای شش خود ریختی بوده و $A(V)\cong S_{۳}$ (صفحهٔ ۲۵ ملاحظه شود).

اگر α یك خود ریختی G باشد، می‌توانیم اثر آن را بر یك زیرگروه H از G مطالعه کنیم. در کلیهٔ حالات نگارهٔ H بر اثر α، یعنی $H\alpha$ یك زیرگروه G است. اگر تساوی

$$H\alpha=H \tag{۵۰.۳}$$

برقرار باشد (به‌عنوان معادله‌ای بین زیرمجموعه‌ها)، آنگاه گوییم که H بر اثر α پایاست. برای مثال H در G فقط و فقط وقتی نرمال است که بر اثر همهٔ خودریختیهای داخلی پایا باشد. دراین‌حالت، به‌ازای هر $t\in G$، نگاشت $H\to t^{-۱}Ht$ یك خودریختی از H می‌باشد.

یك زیرگروه H که بر اثر کلیهٔ خود ریختیها پایا باشد یك **زیرگروه مشخصه** نامیده می‌شود. البته، زیرگروههای مشخصه نرمال‌اند. برای مثال، مرکز گروه، Z، یك زیرگروه مشخصه است؛ زیرا اگر $t\in Z$، آنگاه به‌ازای هر $x\in G$، $tx=xt$. لذا، به ازای هر $\alpha\in A(G)$، داریم $(t\alpha)(x\alpha)=(x\alpha)(t\alpha)$؛ اما چون α پوشاست، $x\alpha$ را می‌توان برابر هرعنصرمانند $y\in G$ گرفت. لذا تساوی $(t\alpha)y=y(t\alpha)$ به‌ازای هر $y\in G$ برقرار است. یعنی

$$Z\alpha\subset Z$$

اگر به‌جای α قراردهیم $\alpha^{-۱}$، به‌نامساوی عکس می‌رسیم، لذا $Z\alpha=Z$.

ما این بخش را با اثبات قضیهٔ زیر به‌پایان می‌رسانیم.

قضیهٔ ۱۳. فرض کنیم N یك زیرگروه نرمال G و H یك زیرگروه مشخصه از N باشد. در این صورت H در G نرمال است.

برهان. فرض کنیم $t\in G$. در این صورت، همچنان که هم‌اکنون متذکر شدیم، نگاشت τ که در (۴۷.۳) تعریف‌شده یك خود ریختی از N است. بنابراین، چون H یك زیرگروه مشخصه در N است، داریم $H\tau=H$. لذا $t^{-۱}Ht=H$، یعنی H در G نرمال است.

تمرین

(۱) نشان دهید که عناصر مزدوج، هم‌مرتبه‌اند.

(۲) دو همجموعهٔ (a) و $(a^{-۱})$، که به‌وسیلهٔ عناصرعکس هم تولید شده‌اند، رده‌های عکس نامیده می‌شوند. ثابت کنید (الف) رده‌های عکس شامل یك تعداد عنصرند.

(ب) یك گروه از مرتبهٔ زوج شامل حداقل یك رده غیر از رده‌ای است که از عنصر واحد تشکیل شده و با عکس خودش متحد است.

(۳) فرض کنیم $G=GL(n, F)$ (صفحهٔ ۱۱ ملاحظه شود)، که در آن $n \geqslant ۲$ و F یـك میدان نامتناهی است. ثابت کنید مرکز G از کلیهٔ عناصر مضارب عددی ماتریس واحد تشکیل می‌شود.

(۴) Z، مرکز گروه دووجهی مرتبهٔ ۸، را پیدا (جدول (xi) صفحهٔ ۵۷)وساختار G/Z را معین کنید.

(۵) نشان دهید که مجموعهٔ

$$T=\{\mathbf{t}=(t_{ij})|t_{ij}=۰ \text{ هرگاه } i>j,\ t_{ii}\neq ۰\}$$

از ماتریسهای عادی بالا-مثلثی $n\times n$ روی یـك میدان، نسبت به‌ضرب ماتریسی یـك گروه تشکیل می‌دهند. ثابت کنید زیرمجموعهٔ E که درآن $t_{ii}=۱$ $(i=۱,\ ۲,\ \dots,\ n)$، یك زیرگروه نرمال T است، ونشان دهید که $T/E\cong D$، که D مجموعهٔ ماتریسهای قطری عادی است.

(۶) ثابت کنید هرگاه H یك زیرگروه G باشد، تعداد زیرگروههای مزدوج با H برابر $[G:N(H)]$ است.

(۷) گیریم N یك‌زیرگروه نرمال G با اندیس متناهی n باشد. همچنین فرض کنیم به‌ازای یك عنصرمفروض $t\in G$، h کوچکترین عدد صحیح مبتنی باشد که $t^h\in N$. ثابت کنید $h|r$، همچنین نشان دهید که، اگر t از مرتبهٔ متناهی r باشد، آنگاه $h|r$.

(۸) فرض کنیم a و b عناصری از یك گروه باشند به‌قسمی که تعویضگر آنها $c=[a, b]$ با a و b تعویضپذیر باشد. نشان دهید که اگر k یـك عـدد صحیـح باشد، (الف) $a^kb=ba^kc^k$ و (ب) $(ab)^k=b^ka^kc^{(۱/۲)k(k+۱)}$.

(۹) فرض کنیم N یك زیرگروه نرمال G با اندیس متناهی n باشد. نشان دهید که، اگر A زیرگروهی دلخواه از G باشد، آنگاه $s=[A:A\cap N]$ متناهی است و $s|n$.

(۱۰) گروه مشتق این گروهها را پیدا کنید: (الف) گروه دووجهی مرتبهٔ ۸ و (ب) گروه کواترنیون (چارتاییها).

(۱۱) ثابت کنید که مرکز ساز یك زیرگروه نرمال G، یك زیرگروه نرمال G است.

(۱۲) ثابت کنید که دریك گروه آبلی نگاشت $x\theta=x^{-۱}$ یك خودریختی است.

(۱۳) ثابت کنید $I(G)$ یك زیرگروه نرمال $A(G)$ است.

(۱۴) نشان‌دهید که G' یك زیرگروه مشخصهٔ G است.

۴

گروههای آبلی متناهی-مولود

۲۵. مقدمات. در این فصل، فقط با گروههای آبلی سروکار داریم، و بی‌مناسبت نیست که قرارداد نمادهـای جمعی (به‌صفحهٔ ۸ و ۹ مراجعه شود) به‌کار گرفته شود. یادآوری می‌کنیم کـه، در این حالت، همهٔ زیرگروهها نرمال‌اند؛ اگر $H \leqslant G$، گروه خارج قسمت G/H از همجموعه‌هـای $H + x(x \in G)$ تشکیل می‌یابد. گروه G **متناهی-مولود** یـا مختصراً گروه (مم) نامیـده می‌شود، هرگـاه تعداد متناهی عناصر u_1، u_2، . . . ، u_n به‌نام **مولد**، در G موجود باشند به‌قسمی که

$$G = \mathrm{gp}\{u_1, u_2, \ldots, u_n\}$$

در این‌صورت هرعنصر x از G، حاصلجمعی است متناهی از تعـدادی از این مولدها یا منفی (عکس) آنها به‌هرترتیب، تکرار نیز مجاز است. ولی به‌موجب قانون تعویضپذیری، می‌توانیم جملاتی راکه متضمن یك مولدند جمع‌آوری کرده و بنویسیم

$$x = a_1u_1 + a_2u_2 + \cdots + a_nu_n \tag{۱.۴}$$

که در آن a_iها اعداد صحیح (مثبت، منفی یـا صفر) هستند. بعکس، به ازای هر انتخاب ضرایب صحیح، (۱.۴) نمایشگر عنصری از G است. اما فرض براین نیستکـه مولدها غیر زاید هستند، و حتی وقتی که چنین باشند، ممکن است در روابط غیربدیهی

$$c_1u_1 + c_2u_2 + \cdots + c_nu_n = 0 \tag{۲.۴}$$

که در آن همهٔ ضرایب با هم صفر نیستند، صدق کنند. چون ضرایب کسری غیر مجازند، ما

درحالت کلی نمی‌توانیم (۲.۴) را نسبت به‌یکی از مولدها، برحسب مولدهای دیگر «حل» کنیم.

درقسمتهای بعد اغلب نیازخواهیم داشت که یك مجموعه از مولدها را تغییردهیم، و بنابراین لازم است شرایطی راکه تحت آن دو مجموعه از عناصر بتوانند به‌عنوان مولدهای یك گروه آبلی به‌کار آیند مورد مطالعه قرار دهیم. پس فرض می کنیم

$$G = \mathrm{gp}\{u_1, u_2, \cdots, u_n\} = \mathrm{gp}\{v_1, v_2, \cdots, v_m\} \qquad (۳.۴)$$

برای آنکه (۳.۴) برقرار باشد لازم وکافی است که هر u برحسب vها و، بعکس، هر v برحسب uها قابل بیان باشد. لذا معادلاتی به‌صورت

$$\left.\begin{aligned} u_i &= \sum_{j=1}^{m} p_{ij} v_j \quad (i = 1, 2, \cdots, n) \\ v_j &= \sum_{k=1}^{n} q_{jk} u_k \quad (j = 1, 2, \cdots, m) \end{aligned}\right\} \qquad (۴.۴)$$

خواهیم داشت که در آن ماتریسهای $\mathbf{p} = (p_{ij})$ و $\mathbf{q} = (q_{jk})$ دارای ضرایب صحیح، یا مختصرتر بگوییم، دارای درایه‌های صحیح هستند. ما به‌دستگاه معادلات (۴.۴) به‌عنوان یك تبدیل از مجموعهٔ مولدهای u_1، u_2، $\cdots$، u_n به‌مجموعهٔ v_1، v_2، $\cdots$، v_m اشاره می کنیم.

متداولترین نوع تبدیل مولدها به‌قرار زیرند

(α) ممکن‌است مولدها را به‌هرکیفیتی پس و پیش کرد.

(β) اگر $i \neq j$، به‌جای مولد u_i می‌توان مولد $u_i + hu_j$ را، که در آن h یك‌عدد صحیح دلخواه است، گذاشت و بقیهٔ مولدها را ثابت نگاه داشت.

(γ) به‌جای هرمولد u_i می‌توان $-u_i$ گذاشت.

(δ) اگر مولدی صفر باشد می‌توان آن را حذف کرد.

اعمال (α)، (β) و (γ) تبدیلات مقدماتی نامیده می‌شوند. اینك می‌پرسیم که آیا (β) در واقع در (۴.۴) صدق می کند یا نه؟ برای سهولت. فرض‌می کنیم $i = 1$، $j = 2$. لذا تبدیل

$$v_1 = u_1 + hu_2,\ v_2 = u_2,\ \cdots,\ v_n = u_n$$

را داریم که عکس آن از معادلات

$$u_1 = v_1 - hv_2,\ u_2 = v_2,\ \cdots,\ u_n = v_n$$

بدست می‌آید.

اعمال مذکور در بالا را می‌توانیم آنقدر تکرارکنیم تا آنکه به دستگاه مولدی که برای مقاصدمان مناسبتر باشد برسیم.

در اینجا ذکر یك نکته‌که جنبهٔ فنی اندکی دارد ضروری است. برای آنکه ثابت

کنیم زیرمجموعهٔ X از G یك گروه تشکیل می‌دهد کافی است تحقیق کنیم هرگاه x و y به X تعلق داشته باشند آنگاه

$$x-y\in X$$

زیرا اگر این حکم برقرار باشد، می‌توان x را مساوی y اختیار کرد و به‌دست آورد که $\circ\in X$. بار دیگر، با انتخاب $x=\circ$، پیدا می‌کنیم که $-y\in X$؛ یا بالاخره با تعویض y با $-y$ نتیجه می‌گیریم که $x+y\in X$، لذا همهٔ شرایط (بخش ۹، صفحهٔ ۳۴) برای زیرگروه بودن X تحقق یافته است.

ما خود را به گروههای آبلی متناهی-مولود محدود می‌کنیم، و هدفمان این است که شرح کاملی از کلیهٔ انواع گروههای ممکن در این رده (با رعایت یکریختیها) به‌دست دهیم. این امر از راه تجزیهٔ G به‌یك **حاصلجمع مستقیم** چند زیرگروه، مشابه با مفهوم حاصلضرب مستقیم (بخش ۱۳، صفحهٔ ۴۶)، انجام خواهد گرفت. یك حاصلجمع مستقیم چنین نوشته می‌شود

$$G=H\oplus K \tag{۵.۴}$$

دراینجا ما به‌حاصلجمعهای مستقیم داخلی علاقه‌مندیم. لذا (۵.۴) بدین‌معنی است که دو زیرگروه H و K از G با ویژگیهای ذیل وجود دارند: عناصر G از کلیهٔ حاصلجمعهای ممکن

$$x=u+v \tag{۶.۴}$$

که در آن u و v مستقلاً به‌ترتیب در H و K تغییر می‌کنند، تشکیل می‌شوند، و این نمایش منحصر به‌فرد است. لذا اگر

$$u_1+v_1=u_2+v_2 \tag{۷.۴}$$

که $u_1, u_2\in H$ و $v_1, v_2\in K$، آنگاه $u_1=u_2$ و $v_1=v_2$. بخصوص، اگر $u_\circ+v_\circ=\circ$ ($u_\circ\in H$ و $v_\circ\in K$)، آنگاه $u_\circ=v_\circ=\circ$. بعکس این حکم، یکتایی (۶.۴) را تضمین می‌کند؛ زیرا از (۷.۴) چنین به‌دست می‌آید که $(u_1-u_2)+(v_1-v_2)=\circ$ و بنا براین $u_1=u_2$ و $v_1=v_2$. باز، برای آنکه (۵.۴) را ثابت کنیم کافی است نشان دهیم که

$$\text{(الف)}\quad G=H+K \quad \text{و} \quad \text{(ب)}\quad H\cap K=\{\circ\}$$

شرط دوم وقتی H و K زیرگروههایی متناهی از مراتب متباین باشند یقیناً برقرار است.

وقتی G به‌صورت حاصلجمع مستقیم چندین زیرگروه بیان شده باشد، نماد

$$G=\sum_{i=1}^{r}\oplus H_i=H_1\oplus H_2\oplus\cdots\oplus H_r \tag{۸.۴}$$

را به‌کار می‌بریم و خاطرنشان می‌سازیم که، با رعایت یکریختی، تشکیل حاصلجمعهای مستقیم هم تعویضپذیر وهم شرکتپذیر است. در واقع، (۸.۴) بیان می‌دارد که G با گروهی

که عناصر آن r-تاییهای $(u_1, u_2, \dots, u_r)$ هستند و u_i در H_i تغییر می‌کند و ترکیب عناصر جداگانه برهر مؤلفه انجام می‌گیرد، یکریخت است.

برای مثال، هرگاه

$$G = H_1 + H_2 + \dots + H_r \quad \text{(الف)}$$

و

(ب) مرتبه‌های H_i و H_j $(i \neq j)$ متباین‌اند

(۸.۴) یقیناً برقرار خواهد بود زیرا در چنین حالتی واضح است که

$$H_i \cap H_1 + \dots + H_{i-1} + H_{i+1} + \dots + H_r = \{0\}$$

۲۶. گروههای آبلی متناهی-مولود آزاد. در این بخش ما گروههای آبلی‌متناهی-مولود

$$F = \mathrm{gp}\{u_1, u_2, \dots, u_n\} \qquad (۹.۴)$$

راکه مولدهای آن در هیچ رابطهٔ غیربدیهی صدق نکنند، یعنی که وجود رابطهٔ

$$c_1u_1 + c_2u_2 + \dots + c_nu_n = 0 \qquad (۱۰.۴)$$

در آن، همواره مستلزم تساویهای $c_1 = c_2 = \dots = c_n = 0$ باشد، مورد مطالعه قرار می‌دهیم. اگر چنین دستگاهی از مولدها وجود داشته باشد F را یك **گروه آبلی آزاد** می‌نامیم. به‌طور دقیقتر، گوییم F به‌وسیلهٔ u_1، u_2، ...، u_n **آزادانه تولید شده** است. در این صورت، چنین دستگاهی از مولدها یك مجموعه از مولدهای آزاد نامیده می‌شود و ما قرارداد

$$F = \langle u_1, u_2, \dots, u_n \rangle \qquad (۱۱.۴)$$

را برای آن به‌کار می‌گیریم. لذا (۱۱.۴) هم‌ارز با این بیان است که عناصر F به‌گونهٔ منحصر به‌فردی به‌صورت

$$x = a_1u_1 + a_2u_2 + \dots + a_nu_n \qquad (۱۲.۴)$$

که در آن a_iها اعداد صحیح دلخواهی هستند، قابل بیان‌اند.

واضح است که در یك گروه آبلی آزاد کلیهٔ عناصر، جزصفر، از مرتبهٔ نامتناهی‌اند. زیرا اگر $x \neq 0$ و $h > 0$، معادلهٔ $hx = 0$ فوراً به‌یك رابطهٔ غیر بدیهی برای مولدها منجر می‌شود. بخصوص، هرمولد از مرتبهٔ نامتناهی است، و (۱۱.۴) هم‌ارز است با

$$F = \mathrm{gp}\{u_1\} \oplus \mathrm{gp}\{u_2\} \oplus \dots \oplus \mathrm{gp}\{u_n\} \qquad (۱۳.۴)$$

حاصلجمع مستقیم از n گروه دوری نامتناهی است.

به‌آسانی می‌توان مثالی از یك گروه آبلی آزاد با n مولد ارائه داد: فرض کنیم Z^n مجموعهٔ کلیهٔ n-تاییهای $x = [a_1, a_2, \dots, a_n]$ باشد که a_1، a_2، ...، a_n مستقلاً همهٔ اعداد صحیح را اختیار می‌کنند. قانون ترکیب در Z^n را به‌صورت جمع مؤلفه‌ای تعریف می‌کنیم، بنابراین از Z^n یك گروه آبلی می‌سازیم. n-تاییهای ویژهٔ

$$u_1=[1, 0, \ldots, 0], u_2=[0, 1, \ldots, 0], \ldots, u_n=[0, 0, \ldots, 1]$$

Z^n را تولید می‌کنند، زیرا، به‌ازای هر $x \in Z^n$ می‌توانیم بنویسیم.

$$x=a_1u_1+a_2u_2+\cdots+a_nu_n$$

بعلاوه این مولدها آزادند زیرا تساوی

$$c_1u_1+c_2u_2+\cdots+c_nu_n=[c_1, c_2, \ldots, c_n]=0$$

مستلزم تساویهای زیر است:

$$c_1=c_2=\cdots=c_n=0$$

اکنون ارتباط بین‌مجموعه‌های مختلف مولدهای‌آزاد را مورد بررسی‌قرارمی‌دهیم. اگرداشته باشیم:

$$F=\langle u_1, u_2, \ldots, u_n\rangle=\langle v_1, v_2, \ldots, v_m\rangle \qquad (۱۴.۴)$$

آنگاه دودستگاه مولد به‌توسط معادلات (۴.۴) در ارتباط‌اند. اما چون این‌مولدها آزادند، ما اطلاعات دقیقتری در اختیار داریم. از حذف v_j در (۴.۴) چنین پیدا می‌کنیم:

$$u_i=\sum_{j=1}^{m}\sum_{k=1}^{n} p_{ij}q_{jk}u_k \quad (i=1, 2, \ldots, n)$$

این یك رابطهٔ غیربدیهی بین uها خواهد بود، مگرآنکه ضرایب متناظر در طرفین با هم مساوی باشند. پس باید داشته باشیم

$$\sum_{j=1}^{m} p_{ij}q_{jk}=\delta_{ik} \quad (i, k=1, 2, \ldots, n)$$

که $\delta_{ik}=0$، هرگاه $i \neq k$ و $\delta_{ii}=1$؛ یا با قرارداد ماتریسی

$$\mathbf{pq}=\mathbf{i}_n \qquad (۱۵.۴)$$

که $\mathbf{i}_n$ ماتریس واحد درجهٔ n است. به‌طریق مشابه، از حذف uها خواهیم داشت

$$\mathbf{qp}=\mathbf{i}_m \qquad (۱۶.۴)$$

دانشجویانی‌که مختصر اطلاعی از جبر خطی داشته باشند، به‌آسانی می‌توانند از(۱۵.۴) و (۱۶.۴) نتیجه بگیرندکه $m=n$؛ به‌گونه‌ای دیگر، می‌توانیم این واقعیت را از راه محاسبهٔ حاصلجمع عناصر قطری در (۱۵.۴) و (۱۶.۴) تحقیق‌کنیم، بدین‌قرار

$$\sum_{i=1}^{n}\sum_{j=1}^{m} p_{ij}q_{ji}=n, \quad \sum_{j=1}^{m}\sum_{i=1}^{n} q_{ji}p_{ij}=m$$

چون عبارات سمت چپ ایـن تساویها مساوی هستند نتیجه می‌شودکه $m=n$. لذا تعداد مولدهای آزاد یك پایایی برای F است، یعنی، این‌عدد برای هردستگاه از مولدهای‌آزاد یکی است. این عـدد رتبهٔ F نامیده می‌شود. بعـلاوه، دو گروه مم آبلی‌آزاد فقط و فقط

وقتی یکریخت هستندکه دارای یك رتبه باشند؛ زیرا، اگر این رتبه برابر n باشد، هر دو گروه با گروه متشکل از n-تاییهای صحیح یکریخت هستند.

با دترمینان‌گیری از (۱۵.۴) یا (۱۶.۴) ملاحظه می کنیم که

$$(\det \mathbf{p})(\det \mathbf{q}) = ۱ \qquad (۱۷.۴)$$

اما ضرایب $\mathbf{p}$ و $\mathbf{q}$ اعدادی صحیح‌اند، و بنابراین دترمینانهای آنها نیز اعدادی صحیح هستند. از این‌رو از (۱۷.۴) نتیجه می گیریم که $\det \mathbf{p} = \det \mathbf{q} = \pm ۱$؛ یعنی $\mathbf{p}$ و $\mathbf{q}$ ماتریسهای یکهنگی هستند و بنابراین دترمینانهای عکسهای آنها اعداد صحیح‌اند. (مثال (iv)، قسمت (ج) صفحهٔ ۱۱ ملاحظه شود). لذا انتقال از یك دستگاه مولدهای آزاد به دیگری بهوسیلهٔ یك تبدیل یکهنگی

$$u_i = \sum_{j=۱}^{n} p_{ij} v_j \quad (i = ۱, ۲, \cdots, n) \qquad (۱۸.۴)$$

انجام می گیرد؛ و واضح است که هر ماتریس یکهنگی $\mathbf{p}$ را می‌توان بدین‌منظور به‌کار برد. چون (۱۸.۴) را به‌توسط معادلات

$$v_j = \sum_{k=۱}^{n} q_{jk} u_k \quad (j = ۱, ۲, \cdots, n) \qquad (۱۹.۴)$$

که درآنها $\mathbf{q} = \mathbf{p}^{-۱}$ مجدداً یك ماتریس با دترمینان صحیح است، می‌توان عکس کرد، لذا، (۴.۴) محقق می گردد.

اعمال (α)، (β)، و(γ) که درصفحهٔ ۹۵ تشریح شده‌اند مثالهای ساده‌ای از تبدیلات یکهنگی هستند. وقتی‌که چند تا از این اعمال به‌توالی انجام گیرد، ماتریسهای متناظر درهم ضرب می‌شوند.

بزرگترین مقسوم‌علیه مشترك (بمم) مجموعه‌ای از اعداد صحیح $a_۱$، $a_۲$، ...، a_n که همه با هم صفر نیستند، چنین نوشته می‌شود:

$$(a_۱, a_۲, \cdots, a_n)$$

وبنابر تعریف، عددی است صحیح ومثبت. بخصوص، وقتی تساوی

$$(a_۱, a_۲, \cdots, a_n) = ۱$$

برقرار باشد می گوییم این اعداد صحیح نسبت به‌هم متباین‌اند.واضح این است که در یك ماتریس یکهنگی ضرایبی که یك سطر یا یك ستون را تشکیل می‌دهند باید نسبت به هم متباین باشند. زیرا اگر دترمینان چنین ماتریسی برحسب یك سطر (ستون) بسط داده شود، آشکار است که‌این دترمینان بر بمم این سطر (ستون) قابل‌قسمت می‌باشد. اما، بنابرفرض، این دترمینان برابر ± ۱ است، که از آنجا نتیجه می‌شودکه بمم فقط می‌تواند برابر یك باشد. لذا اگر مجموعه‌ای جدید ازمولدهای آزاد به توسط (۱۹.۴) معرفی گردد،هر مولد

جدید ترکیبی است خطی از مولدهـای قدیم با ضرایب متباین. درقضیهٔ ذیل عکس جزئی این واقعیت اثبات می‌شود.

قضیه* ۴.۱۴ فرض کنیم $F=\langle u_1, u_2, \ldots, u_n\rangle$ باشد و

$$v=b_1u_1+b_2u_2+\cdots+b_nu_n$$

عنصری از F به‌قسمی که

$$(b_1, b_2, \ldots, b_n)=1 \tag{۲۰.۴}$$

در این صورت عناصری مانند v_2، v_3، $\ldots$، v_n از F وجود دارند به‌قسمی که

$$F=\langle v, v_2, v_3, \ldots, v_n\rangle \tag{۲۱.۴}$$

به‌عبارت دیگر، (۲۰.۴) شرط لازم وکافی برای‌آن است‌که عنصری بتواند دریك مجموعه از مولدهای آزاد درج شود.

برهان. فرض‌کنیم $s=|b_1|+|b_2|+\cdots+|b_n|$. اگر $s=1$، آنگاه به‌ازای مقداری از j، $v=\pm u_j$، و واضح است‌که v می‌تواند دریك مجموعه ازمولدهای آزاد درج شود. اینك از استقراء بـه s استفاده می‌کنیم و درعین حال این حق را بـرای خود محفوظ نگاه‌می‌داریم که مولدهای F را تغییر دهیم تا آنکه (۲۱.۴) برقرار شود. اگر $s>1$، حداقل دوتـا از bها غیرصفرنـد، چون درغیر این صورت $(b_1, b_2, \ldots, b_n)>1$. بی‌آنکه خللی به‌کلیت استدلال وارد شود می‌توان فرض‌کردکه $b_1 \geqslant b_2 > 0$، زیـرا همواره می‌توان این شرط را بـا تبدیل مولدها وتغییر علامت آنهـا (اعمال (α) و (γ)، صفحهٔ ۹۰) برقرارکرد. اکنون فرض‌می‌کنیم

$$u_1'=u_1,\ u_2'=u_2+u_1,\ u_j'=u_j \quad (j\geqslant 3)$$

واضح است که $F=\langle u_1', u_2', \ldots, u_j'\rangle$ (بنابر عمل (β)). امـا عبارتی‌که v را بیان می‌کند چنین می‌شود:

$$v=(b_1-b_2)u_1'+b_2u_2'+\cdots+b_nu_n'$$

روشن است‌که $(b_1-b_2, b_2, b_3, \ldots, b_n)=1$ اما

$$|b_1-b_2|+|b_2|+|b_3|+\cdots+|b_n|<s$$

---

* ملاحظه‌کنید

R. Rado, 'A proof of the basis theorem for finitely generated Abelian groups', *Journal of the London Mathematical Society* (1951), 26, 74–75.

از این‌رو بنابر فرض استقراء، v می‌تواند دریك مجموعه ازمولدهای آزاد درج شود.

اکنون توجه خویش را به‌زیرگروههای H ازیك گـروه آبلی مم آزاد F معطوف می‌کنیم. ممکن است سؤال شود که آیا H نیز مم وآزاد است. به‌این سؤال درقضیهٔ آتیه به‌شکلی مثبت پاسخ داده شده است، که برای نظریهٔ گروههای آبلی نقشی حیاتی دارد. در این قضیه این نتیجهٔ عمیقتر نیز اثبات می‌شودکه مولدهای H می‌توانند به‌نحو شگفت‌آوری ساده بیان شوند مشروط برآنکه مولدهای F به‌گونه‌ای مناسب انتخاب شده باشند.

قضیهٔ اصلی ۱۲. فـرض کنیم F یك گروه آبلی مم آزاد از رتبهٔ n، و H زیرگروهی غیرصفر از F باشد. دراین صورت H نیز گروه‌آبلی مم آزاد واز رتبهٔ $m\leqslant n$ است. بعلاوه می‌توان مجموعه‌ای ازمولدهای آزاد v_1، v_2، . . . ، و v_n را برای F بـه‌گونه‌ای انتخاب کردکه

$$H=\langle h_1v_1,\ h_2v_2,\ \ldots,\ h_mv_m\rangle \qquad (۲۲.۴)$$

که h_1، h_2، . . . ، h_m اعدادی صحیح‌اند و در روابط $h_i|h_{i-1}$ $(i=1,\ 2,\ \ldots,\ m-1)$ صدق می‌کنند.

برهان. (الف) فرض کنیم‌که F از ابتدا برحسب مولدهای‌آزاد u_1، u_2، . . . ، u_n داده شده باشد. بـه هرعنصر غیرصفر $x=a_1u_1+a_2u_2+\cdots+a_nu_n$ از F ما بمم ضرایب آن را نسبت به‌این مجموعه از مولدها وابسته می‌کنیم، بدین قرار

$$\delta(x)=(a_1,\ a_2,\ \ldots,\ a_n)$$

ولی این عدد مستقل ازانتخاب مولدهاست. زیرا اگر u_1'، u_2'، . . . ، u_n' مجموعه‌ای دیگر ازمولدهای‌آزاد F باشد داریم $u_i=\sum_{j=1}^{n}p_{ij}u_j'$ که در آن (p_{ij}) ماتریس‌یکهنگی‌است. پس

$$x=a_1'u_1'+a_2'u_2'+\cdots+a_n'u_n'$$

که $a_j'=\sum_{i=1}^{n}a_ip_{ij}$. لذا هر مقسوم‌علیه مشترك a_iها باید همهٔ a_j'ها را عادکند، وبنا براین

$$(a_1',\ a_2',\ \ldots,\ a_n')\geqslant(a_1,\ a_2,\ \ldots,\ a_n)$$

اگر نقش این دومجموعه از مولدهـا را از راه عکس‌کردن مـاتریس (p_{ij}) تعویض‌کنیم می‌توانیم نامساوی عکس آن را اثبات نماییم. بنابراین

$$(a_1',\ a_2',\ \ldots,\ a_n')=(a_1,\ a_2,\ \ldots,\ a_n)$$

که پایایی $\delta(x)$ را اثبات می‌کند.

(ب) درمیان عناصر غیرصفر H گیریم

$$y_1=b_1u_1+b_2u_2+\cdots+b_nu_n$$

به‌قسمی باشد که δی آن به‌حداقل مقدارش برسد، یعنی $\delta(y_1)=h_1 \geqslant 1$. دراین صورت می‌توانیم بنویسیم

$$y_1 = h_1(c_1u_1 + c_2u_2 + \cdots + c_nu_n) = h_1v_1$$

که

$$v_1 = c_1u_1 + c_2u_2 + \cdots + c_nu_n$$

عنصری از F با ویژگی

$$(c_1, c_2, \ldots, c_n) = 1$$

می‌باشد. بنابر قضیهٔ ۱۴ عناصری چون v'_2، v'_3، ...، v'_n وجود دارند به‌قسمی که

$$F = \langle v_1, v'_2, v'_3, \ldots, v'_n \rangle \tag{۲۳.۴}$$

با استفاده ازاین مجموعه‌مولدها فرض می‌کنیم

$$y = d_1v_1 + d_2v'_2 + \cdots + d_nv'_n$$

عنصری دلخواه از H باشد. می‌دانیم که

$$y_1 = h_1v_1 \in H \tag{۲۴.۴}$$

وحال می‌گوییم که $h_1 | d_1$. زیرا درغیر این‌صورت، می‌توانیم اعدادی صحیح مانند q و r بیابیم به‌قسمی که $d_1 = qh_1 + r$، که درآن $0 < r < h_1$. لذا

$$y - qy_1 = rv_1 + d_2v'_2 + \cdots + d_nv'_n$$

عنصری از H خواهد بود به‌قسمی که

$$\delta(y - qy_1) = (r, d_2, \ldots, d_n) \leqslant r < h_1$$

که با حداقل بودن h_1 درتناقض است. بنابراین نتیجه می‌گیریم که $r = 0$، یعنی

$$y - qy_1 = d_2v'_2 + \cdots + d_nv'_n \tag{۲۵.۴}$$

(ج) برهان به‌استقراء بر n انجام می‌گیرد. وقتی $n = 1$، که بلافاصله به‌منظور خود رسیده‌ایم. زیرا در این حالت، باید به‌جای طرف راست (۲۵.۴) صفر گذاشته شود، و $y = qy_1 = qh_1v_1$. این ناظر بر این حکم است که $F = \langle v_1 \rangle$ و $H = \langle h_1v_1 \rangle$، که همان است که قضیه خواسته است وقتی $n = m = 1$. اکنون فرض می‌کنیم کـه $n > 1$، و قرار می‌دهیم

$$F_1 = \langle v'_2, v'_3, \ldots, v'_n \rangle, \quad H_1 = H \cap F_1 \tag{۲۶.۴}$$

متذکر می‌شویم که سمت راست (۲۵.۴) به F_1 تعلق دارد درحالی که سمت چپ آن در H است. لذا (۲۵.۴) معرف عنصری است از H_1. باید دوحالت در نظر گرفته شود: نخست

آنکه اگر $H_1=\{0\}$، آنگاه داریم $y=qy_1=qh_1v_1$، و مانند قبل $H=\langle h_1v_1\rangle$.
این تساوی به‌انضمام (۲۳.۴)، قضیه را وقتی‌که $m=1$ و n دلخواه است اثبات می‌کند.
بعد،وقتی‌که H_1 زیرگروهی غیر از صفر از F_1 باشد، فرض استقراء را برای F_1 و H_1 به‌کار می‌بریم. لذا می‌توانیم عناصر v_2، v_3، ...، v_n از F_1 را چنان پیداکنیم که

$$F_1=\langle v_2, v_3, \ldots, v_n\rangle$$

$$H_1=\langle h_2v_2, h_3v_3, \ldots, h_mv_m\rangle \qquad (۲۷.۴)$$

که m عدد صحیحی است که در $2\leqslant m\leqslant n$ صدق می‌کند و

$$(i=2, 3, \ldots, m-1)\ h_i|h_{i+1}$$

این دو مجموعه مولدهای آزاد برای F_1 به‌وسیلهٔ معادلات:

$$v_i=\sum_j p_{ij}v'_j, \quad v'_i=\sum_j q_{ij}v_j \quad (i, j=2, 3, \ldots, n)$$

با هم مربوط می‌شوند. حال گوییم:

$$F=\langle v_1, v_2, \ldots, v_n\rangle \qquad (۲۸.۴)$$

زیرا با بیان vها برحسب v'ها در (۲۳.۴)، می‌بینیم که v_1، v_2، ...، v_n به‌طور قطع F را تولید می‌کنند. بعلاوه، این عناصر مولدهای آزادند؛ زیرا فرض‌کنیم که یك رابطهٔ غیربدیهی به‌شرح زیر وجود داشته باشد:

$$c_1v_1+c_2v_2+\ldots+c_nv_n=0 \qquad (۲۹.۴)$$

مشاهده می‌کنیم که $c_1\neq 0$؛ زیرا در غیراین‌صورت، باید رابطه‌ای بین v_2، v_3، ...، v_n داشته باشیم که با (۲۷.۴) متناقض است. حال اگر در (۲۹.۴) به‌جای v_2، v_3، ...، v_n مقادیر آنها را برحسب v'_2، v'_3، ...، v'_n بگذاریم، رابطه‌ای بین v_1، v'_2، ...، v'_n به‌دست خواهیم آورد که درآن c_1 ضریب v_1 است. این امر با (۲۳.۴) ناسازگار است. لذا (۲۸.۴) اثبات شده است. ازترکیب (۲۴.۴) و(۲۵.۴) و (۲۷.۴)، ملاحظه می‌کنیم که عناصر

$$h_1v_1(=y_1), h_2v_2, \ldots, h_mv_m$$

H را تولید می‌کنند. درواقع، اینها مولدهایی آزادند، زیرا هر رابطهٔ غیربدیهی بین آنها، رابطه‌ای بین v_1, v_2، ...، v_m، ...، v_n نیز خواهد بود، وبنابراین‌متناقض با (۲۸.۴). لذا

$$H=\langle h_1v_1, h_2v_2, \ldots, h_mv_m\rangle$$

برای اتمام برهان باز باید نشان دهیم که $h_1|h_2$. اما $y_0=h_1v_1+h_2v_2$ عنصری از H است. از این‌رو بنابرمینیمال بودن h_1، باید $\delta(y_0)=(h_1, h_2)\geqslant h_1$. با توجه به‌تعریف بمم، $(h_1, h_2)\leqslant h_1$. بنابراین $(h_1, h_2)=h_1$؛ یعنی $h_1|h_2$.

۲۷. گروههای آبلی متناهی-مولود. اکنون به‌بحث درپیرامون گروه آبلی‌متناهی-مولود

دلخواه برمی گردیم. البته همهٔ گروههای آبلی متناهی به‌این رده تعلق دارند. فرض می کنیم داشته باشیم

$$A = \mathrm{gp}\{s_1, s_2, \ldots, s_n\}$$

که در آن اکنون پذیرفته‌ایم که مولدهای s_1، s_2، . . .، s_n ممکن است در روابطی غیربدیهی صدق کنند. ما به A، گروه آبلی آزاد

$$F = \langle u_1, u_2, \ldots, u_n \rangle$$

را وابسته می کنیم که به‌وسیلهٔ نمادهای u_1، u_2، . . .، u_n آزادانه تولید شده است. برای آنکه بین A و F ارتباطی برقرار کنیم، نگاشت

$$\theta : F \rightarrow A$$

راکه به‌وسیلهٔ رابطهٔ

$$(a_1u_1 + a_2u_2 + \cdots + a_nu_n)\theta = a_1s_1 + a_2s_2 + \cdots + a_ns_n \qquad (۳۰.۴)$$

تعریف می‌شود وارد می کنیم. تحقیق سادهٔ این مطلب راکه θ در واقع یك همریختی می‌باشد به‌عهدهٔ دانشجو واگذار می کنیم. آشکار است کـه θ پوشاست، زیرا هرعنصر A می‌تواند در طرف راست (۳۰.۴) ظاهر شود. فرض می کنیم R هستهٔ θ باشد؛ می‌دانیم کـه R یك زیرگروه F است. لذا عنصر $a_1u_1 + a_2u_2 + \cdots + a_nu_n$ فقط و فقط وقتی بـه R تعلق داردکه تساوی $a_1s_1 + a_2s_2 + \cdots + a_ns_n = 0$ برقرار باشد. این رابطه‌ای است بین مولدهای A و می‌توان گفت کـه عناصر R در تناظر یك به‌یك با کلیهٔ روابطی هستندکه مولدهای A در آنها صدق می کنند. اما نخستین قضیهٔ اصلی یکریختی (قضیهٔ اصلی ۸ صفحهٔ ۷۵) به‌ما می گویدکه

$$A \cong \frac{F}{R} \qquad (۳۱.۴)$$

وما می‌توانیم از راه بررسی F/R ساختار A را، که به‌کمك بخش پیشین برای آن آمادگی پیدا کرده‌ایم، کشف کنیم. بنابراین می‌توانیم مولدهای آزادی مانند v_1، v_2، . . .، v_n برای F چنان انتخاب کنیم که

$$F = \langle v_1, v_2, \ldots, v_n \rangle, \quad R = \langle h_1v_1, h_2v_2, \ldots, h_mv_m \rangle \qquad (۳۲.۴)$$

$(m \leqslant n)$ و $h_i | h_{i+1}$ $(i = 1, 2, \ldots, m-1)$، مشروط برآنکه $R \neq \{0\}$

برسبیل آمادگی، حالتی را که در آن $n = 1$، درنظر می گیریم. سه حالت را باید ازهم تمیزدهیم:

(الف) $F = \langle v \rangle$ و $R = \{0\}$. پس $F/R \cong F$ گروه دوری نامتناهی است که به‌وسیلهٔ v تولید شده است.

(ب) $F = \langle v \rangle$ و $R = \langle hv \rangle$، که $h \geqslant 2$. در این‌صورت $F/R \cong C_h$ گروه دوری از مرتبهٔ h است.

(ج) $F=\langle v\rangle$ و $R=\langle v\rangle$ $(h=1)$. در این‌صورت $F/R\cong\{0\}$، زیرا $F=R$.
در وضعیت کلی همین‌صورتها ظاهر می‌شوند، و بجاست که علامتهایی برای این سه نوع مولد به‌کار گرفته شود. اگر $r=n-m>0$، r مولد در F وجود دارند که در R وجود ندارند؛ این مولدها به x_1، x_2، . . . ، x_r نشان داده می‌شوند. اگر $h_1=h_2=\ldots=h_l=1$، مولدهای متناظر آنها، مثلاً z_1، z_2، . . . ، z_l هم در F وجود دارند و هم در R. اگر $n=r+l+k$، k مولد باقیمانده با مقادیری از h که بزرگتر از یك هستند متناظرند، و مناسب است که آنها را به‌ترتیب نزولی اندازه‌هاشان مرتب کرده و آنها را e_1، e_2، . . . ، و e_k بنامیم. بنابراین می‌نویسیم

$$F=\langle x_1, x_2, \ldots, x_r, y_1, y_2, \ldots, y_k, z_1, z_2, \ldots, z_l\rangle \qquad (۳۳.۴)$$

$$R=\langle e_1y_1, e_2y_2, \ldots, e_ky_k, z_1, z_2, \ldots, z_l\rangle \qquad (۳۴.۴)$$

که $e_{\kappa+1}|e_\kappa$ $(\kappa=1, 2, \ldots, k-1)$، $n=r+k+l$ و $m=k+l$، که معلوم است برحسب مواقعی که این یا آن نوع وجود ندارند تغییر می‌کنند.
اگر $x\in F$، فرض کنیم $\bar{x}=x+R$ نگارهٔ x بر اثر بر ریختی طبیعی $F\to F/R$ حاصل شده باشد. بخصوص، با توجه به مولدهای F در هر حالت می‌بینیم که (اولاً) $\bar{x}_\rho$ $(\rho=1, 2, \ldots, r)$ عنصری از مرتبهٔ نامتناهی است زیرا هیچ مضربی (غیرصفر) از x_ρ در R قرار ندارد؛ (ثانیاً) $\bar{y}_\kappa$ ازمرتبهٔ e_κ است $(\kappa=1, 2, \ldots, k)$؛ (ثالثاً) $\bar{z}_\lambda$ $(\lambda=1, 2, \ldots, l)$ عنصر صفر $(\bar{0})$ از F/R است زیرا $z_\lambda\in R$. اماعنصر عمومی F را می‌توان به‌صورت

$$x=\sum_{\rho=1}^{r} a_\rho x_\rho+\sum_{\kappa=1}^{k} b_\kappa y_\kappa+\sum_{\lambda=1}^{l} c_\lambda z_\lambda$$

بیان کرد. از اینجا نتیجه می‌شود که یك عنصر نوعی F/R باید چنین باشد:

$$\bar{x}=\sum_{\rho=1}^{r} a_\rho \bar{x}_\rho+\sum_{\kappa=1}^{k} b_\kappa \bar{y}_\kappa \qquad (۳۵.۴)$$

لذا F/R به‌وسیلهٔ $\bar{x}_1$، . . . ، $\bar{x}_r$، $\bar{y}_1$، . . . ، $\bar{y}_k$ تولید شده است. ولی ما می‌گوییم که در واقع

$$\frac{F}{R}=\mathrm{gp}\{\bar{x}_1\}\oplus\mathrm{gp}\{\bar{x}_2\}\oplus\cdots\oplus\mathrm{gp}\{\bar{x}_r\}\oplus\mathrm{gp}\{\bar{y}_1\}\oplus\cdots\oplus\mathrm{gp}\{\bar{y}_k\} \qquad (۳۶.۴)$$

یعنی تصدیق می‌کنیم که طرف راست (۳۵.۴) فقط وفقط وقتی می‌تواند صفر شود که همهٔ جملات آن صفرشوند. فرض کنیم:

$$\sum_{\rho=1}^{r} a_\rho \bar{x}_\rho+\sum_{\kappa=1}^{k} b_\kappa \bar{y}_\kappa=\bar{0}$$

که بدین‌معنی است که

$$\sum_{\rho=1}^{r} a_\rho x_\rho + \sum_{\kappa=1}^{k} b_\kappa y_\kappa \in R$$

یك نظر اجمالی به (۳۴.۴) نشان می‌دهد که $a_\rho = 0$ $(\rho = 1, 2, \ldots, r)$، زیرا x_ρ در R وجود ندارد. بعلاوه، باید b_κ بر e_κ قابل‌قسمت باشد $(\kappa = 1, 2, \ldots, k)$؛ مثلاً $b_\kappa = d_\kappa e_\kappa$. ازاین‌رو $b_\kappa \bar{y}_\kappa = d_\kappa e_\kappa \bar{y}_\kappa = \bar{0}$. زیرا $e_\kappa \bar{y}_\kappa = \bar{0}$، که رابطهٔ (۳۶.۴) را اثبات می‌کند. چون، بنابر (۳۱.۴) می‌توانیم گروه مفروض A را با F/R یکی بگیریم، پس قضیهٔ بنیادی ذیل را ثابت کرده‌ایم:

قضیهٔ اصلی ۱۳ (قضیهٔ مبنا برای گروههای آبلی‌مم). هرگروه آبلی مم A حاصلجمع مستقیم گروههای دوری است، که مشتمل بر r $(r \geqslant 0)$ گروه دوری نامتناهی و k $(k \geqslant 0)$ گروه دوری متناهی است؛ لذا

$$A = \mathrm{gp}\{t_1\} \oplus \cdots \oplus \mathrm{gp}\{t_r\} \oplus \mathrm{gp}\{w_1\} \oplus \cdots \oplus \mathrm{gp}\{w_k\} \qquad (۳۷.۴)$$

که در آن t_ρ $(\rho = 1, 2, \ldots, r)$ از مرتبهٔ نامتناهی است، در صورتی که w_κ $(\kappa = 1, 2, \ldots, k)$ از مرتبهٔ متناهی e_κ $(\kappa \geqslant 2)$ است. بعلاوه

$$e_{\kappa+1} | e_\kappa \quad (\kappa = 1, 2, \ldots, k-1) \qquad (۳۸.۴)$$

این‌قضیه به‌نحو مؤثری‌مسئلهٔ بیان ساختاری کلیهٔ گروههای آبلی مم را حل‌می‌کند.مولدهایی که در تجزیهٔ مستقیم (۳۷.۴) وجود دارند یك **مبنا** برای A می‌باشند. تکرار می کنیم که این مولدها، برخلاف عناصر تشکیل‌دهندهٔ مبنای یك فضای برداری، نه‌آزادند و نه مستقل اما واجد این ویژگی‌اند که دریك رابطهٔ غیربدیهی هرجمله‌شان صفر می‌شود.

وقتی $r = 0$، گروه A متناهی‌و $|A| = e_1 e_2 \ldots e_k$؛ درحالت قرین دیگر، وقتی که $k = 0$، A یك‌گروه‌آبلی‌آزاد است.صرفنظر از اینکه A آزاد باشد یا نباشد،عدهٔ‌مولدهای آزاد، یعنی r، **رتبه** A نامیده می‌شود.

تجزیهٔ مذکور در قضیهٔ اصلی ۱۳ یك **صورت قانونی** برای A خوانده می‌شود. این اصطلاح نسبتاً مبهم، وقتی به‌کار می‌رود که ساختار یك شیء ریاضی به‌نحوی ساده و اساساً منحصر به‌فرد نمایش داده شده باشد. مسئلهٔ یکتایی‌که تا به‌حال ازکنار آن گذشته‌ایم، در بخش بعد مورد بحث قرارخواهد گرفت.

۲۸. مقسوم‌علیه‌های پایا و اولیه. یکتایی که هم‌اکنون از آن صحبت‌کردیم به‌کمك قضیهٔ اصلی ذیل به‌صورت دقیقی بیان می‌شود.

قضیهٔ اصلی۱۴. فرض کنیم A یك گروه آبلی متناهی-مولود باشد وفرض می‌کنیم‌که

$$A = \mathrm{gp}\{x_1\} \oplus \cdots \oplus \mathrm{gp}\{x_r\} \oplus \mathrm{gp}\{u_1\} \oplus \cdots \oplus \mathrm{gp}\{u_k\} \qquad (۳۹.۴)$$

$$= \mathrm{gp}\{y_1\} \oplus \cdots \oplus \mathrm{gp}\{y_s\} \oplus \mathrm{gp}\{v_1\} \oplus \cdots \oplus \mathrm{gp}\{v_l\} \qquad (۴۰.۴)$$

که در آن $x_\rho\ (\rho=1,\ldots,r)$ و $y_\sigma\ (\sigma=1,2,\ldots,s)$ عناصری ازمراتب نامتناهی هستند و $|u_\kappa|=d_\kappa\ (\kappa=1,2,\ldots,k)$، $d_{\kappa+1}|d_\kappa$، $|v_\lambda|=e_\lambda\ (\lambda=1,2,\ldots,l)$، $e_{\lambda+1}|e_\lambda$. دراین صورت (۱) $r=s$ و(۲) $k=l$، e_κ، $d_\kappa=e_\kappa\ (\kappa=1,2,\ldots,k)$.

برهان این قضیه بیشتراین بخش را در برخواهد گرفت و به‌چند مرحله تقسیم‌می‌شود.

(الف) فرض‌کنیم T گردایهٔ آن عناصری‌از A باشدکه از مرتبهٔ متناهی هستند. اگر $u, v\in T$، آن‌گاه اعداد صحیح مثبتی چون m و n هست که $mu=nv=0$. از این‌رو $mn(u-v)=0$ به‌طوری که $u-v\in T$. از اینجا نتیجه می‌شود که $u-v\in T$ و این نکته ثابت می‌کندکه T یك زیر گروه است (صفحهٔ ۹۱ ملاحظه شود). این گروه **زیرگروه پیچشی** A خوانده می‌شود، عبارتی که از توپولوژی به‌عاریت گرفته شده است. البته T ذاتاً به A مربوط می‌شود، یعنی، به‌انتخاب عناصر مبنا بستگی ندارد. اما گروههای

$$X=\sum_{\rho=1}^{r}\oplus\,\mathrm{gp}\,\{x_\rho\}\quad و\quad Y=\sum_{\sigma=1}^{s}\oplus\,\mathrm{gp}\,\{y_\sigma\}$$

گروههایی آبلی وبه‌ترتیب از رتبهٔ r و s هستند. از مفروضات (۳۹.۴) و(۴۰.۴) به‌دست می‌آیدکه

$$A=X\oplus T=Y\oplus T \tag{۴۱.۴}$$

زیرا واضح است‌که گروه پیچشی نمی‌تواند هیچ مولدی از مرتبهٔ نامتناهی را در برگیرد، در حالی‌که لزوماً شامل کلیهٔ مولدهایی ازمرتبهٔ متناهی است. از (۴۱.۴) نتیجه می گیریم که $A/T\cong X$ و $A/T\cong Y$، که از این روابط نتیجه می‌شود $X\cong Y$. اما رتبهٔ یك گروه آبلی آزاد عددی است پایا (صفحهٔ ۹۳). از این‌رو $s=r$ و قسمت اول قضیهٔ اصلی۱۴ اثبات شده است.

(ب) از این به‌بعد ما منحصراً با گروههای آبلی متناهی در ارتباط هستیم. یعنی، از مولدهای نامتناهی در (۳۹.۴) و (۴۰.۴) صرفنظر می کنیم. ما با حالت خاصی‌که در آن A یك p-گروه آبلی است شروع می کنیم، یعنی فرض می کنیم که $|A|=p^m$، کـه p یك عدد اول و m عدد صحیحی است. پس مرتبهٔ هرعنصر توانی است از p، و بخصوص‌قرار می‌دهیم $|v_\lambda|=e_\lambda=p^{\varepsilon_\lambda}$، $(\lambda=1,2,\ldots,l)$، $|u_\kappa|=d_\kappa=p^{\delta_\kappa}\ (\kappa=1,2,\ldots,k)$.

شرط $d_{\kappa+1}|d_\kappa$ هم‌ارزاست با $\delta_\kappa\geqslant\delta_{\kappa+1}$؛ به‌طورمشابه، $\varepsilon_\lambda\geqslant\varepsilon_{\lambda+1}$. تطابق دادن قضیهٔ اصلی۱۴ با p-گروهها به‌قضیهٔ زیر منجر می‌شود.

قضیهٔ اصلی۱۵. فرض کنیم A یك p-گروه آبلی متناهی باشد. فرض می‌کنیم

$$A=\sum_{\kappa=1}^{k}\oplus\,\mathrm{gp}\,\{u_\kappa\}=\sum_{\lambda=1}^{l}\oplus\,\mathrm{gp}\,\{v_\lambda\} \tag{۴۲.۴}$$

کـه $|u_\kappa|=p^{\delta_\kappa}\ (\kappa=1,2,\ldots,k)$، $|v_\lambda|=p^{\varepsilon_\lambda}\ (\lambda=1,2,\ldots,l)$ و $\delta_\kappa\geqslant\ldots\geqslant\delta_2\geqslant\delta_1$ و $\varepsilon\geqslant\ldots\geqslant\varepsilon_2\geqslant\varepsilon_1$. دراین‌صورت $k=l$ و $\delta_\kappa=\varepsilon_\kappa\ (\kappa=1,2,\ldots,k)$.

برهان. اگر $|A|=p^m$، آنگاه از مقایسهٔ مرتبه‌های موجود در (۴۲۰۴) به دست می‌آید که

$$m=\sum_{\kappa}\delta_{\kappa}=\sum_{\lambda}\varepsilon_{\lambda}$$

وقتی ۱ $=m$، قضیه بدیهی است. بنابراین می‌توانیم با استقراء بر m عمل کنیم.

فرض کنیم A_p مجموعهٔ عناصری باشد که در $px=0$ صدق می‌کنند. چون $p(x-y)=px-py$، نتیجه می‌شود که A_p یك زیرگروه A است (که ممکن است با A مساوی باشد). مرتبهٔ A_p را به‌آسانی می‌توان تعیین کرد. برای این کار فرض می‌کنیم $x\in A_p$. بااستفاده از مبنای u_1، u_2، ...، u_k برای A داریم

$$x=\sum_{i=1}^{k}a_iu_i$$

که در آن می‌توان فرض کرد که $0\leqslant a_i<p^{\delta_i}$، زیرا $|u_i|=p^{\delta_i}$. اما اگر $px=0$، آنگاه به‌ازای هر i، $pa_iu_i=0$، و ازاین‌رو $p^{\delta_i}|pa_i$. لذا $a_i=b_ip^{\delta_i-1}$، که b_i باید در $0\leqslant b_i<p$ صدق کند. بدین‌سان به‌ازای هر iی ثابت، دقیقاً p مقدار ممکن برای b_i و درنتیجه برای a_i، وجود دارد به‌قسمی که $px=0$. این نشان می‌دهد که $|A_p|=p^k$. به‌همین طریق بااستفاده از مبنای دوم در (۴۲۰۴) پیدا می‌کنیم که $|A_p|=p^l$. اما A_p مستقل از مبناست. بنابراین $k=l$، همچنان‌که خواسته شده بود.

در مرحلهٔ بعد، مجموعهٔ A^p را مشتمل بر کلیهٔ عناصر x از A تعریف می‌کنیم که مضرب pام (مشابه جمعی توان pام) یك عنصر دیگر باشند. به‌آسانی تحقیق می‌شود که A^p درواقع یك گروه‌است؛ زیرا اگر $x=px'$، $y=py'$، آنگاه $x-y=p(x'-y')$. اگر هر عنصر مبنای A را در p ضرب کنیم به آسانی یك تجزیهٔ مستقیم از A^p بەدورها به‌دست می‌آوریم. اما باید توجه کرد که این عمل کلیهٔ عناصر مرتبهٔ p را «ازبین می‌برد». ازاین‌رو فرض می‌کنیم

$$\delta_1\geqslant\delta_2\geqslant\dots\geqslant\delta_K>1,\ \delta_{K+1}=\delta_{K+2}=\dots=\delta_K=1$$

که K عدد صحیح معینی است که در $0\leqslant K\leqslant k$ صدق می‌کند. پس

$$A^p=\sum_{i=1}^{K}\oplus\,\mathrm{gp}\,\{pu_i\}\quad\text{و}\quad |pu_i|=p^{\delta_i-1}$$

مشابهاً، اگر $1\leqslant\varepsilon_L\leqslant\dots\leqslant\varepsilon_2\leqslant\varepsilon_1$، $\varepsilon_{L+1}=\varepsilon_{L+2}=\dots=\varepsilon_l=1$، می‌توانیم بنویسیم

$$A^p=\sum_{j=1}^{L}\oplus\,\mathrm{gp}\,\{pv_j\}$$

که در آن $|pv_j|=p^{\varepsilon_j-1}$. وقتی که $K=0$، کلیهٔ عناصر A از مرتبهٔ pاند، و از آنجا نتیجه می‌شود $A^p=\{0\}$. دراین‌حالت همچنین $L=0$، زیرا A^p مستقل از مبنا می‌باشد. از این به‌بعد، فرض می‌کنیم که $K>0$. روشن است که داریم $|A|>|A^p|$، و می‌توانیم

فرض استقراء را بر A^p اجرا کنیم. بدین‌سان نتیجه‌می گیریم که $K = L$ و $\varepsilon_i - ۱ = \delta_i - ۱$، یعنی $\delta_i = \varepsilon_i$ $(i = ۱, ۲, \ldots, K)$. چون δها و εهای باقیمانده مساوی یك‌اند، برهان قضیه تمام است.

پایاهای

$$p^{\delta_۱}, p^{\delta_۲}, \ldots, p^{\delta_k} \tag{۴۳.۴}$$

از یك p-گروه آبلی A **مقسوم علیه‌های اولیه** A نیز خوانده می‌شوند. ازاین‌رو دو p-گروه آبلی یکریخت‌اند اگر، و فقط اگر، دارای مقسوم‌علیه‌های اولیهٔ یکسان باشند که به‌ترتیبی منظم شده باشند. وقتی مقدار p معلوم شده باشد، کافی است نماهای موجود در (۴۳.۴) را نام ببریم، و گوییم که A **از نوع** $(\delta_۱, \delta_۲, \ldots, \delta_k)$ است. به‌ویژه، A یك p-گروه آبلی اولیه نامیده می‌شود هرگاه ازنوع $(۱, ۱, \ldots, ۱)$ باشد.

(ج) مرحلهٔ بعد مشتمل بر شکستن یك گروه آبلی متناهی و تجزیهٔ آن به p-گروههاست. ما با یك لم که فقط مربوط به‌یك زیرگروه دوری است شروع می‌کنیم و، به‌صورت ضربی آن، برای گروههای غیرآبلی نیز به‌کار می‌بریم (تمرین ۸، فصل ۱ ملاحظه شود).

لم. فرض کنیم w عنصری از مرتبهٔ mn باشد که $(m, n) = ۱$. در این صورت

$$\mathrm{gp}\{w\} = \mathrm{gp}\{nw\} \oplus \mathrm{gp}\{mw\} \tag{۴۴.۴}$$

برهان. عناصر $u = nw$ و $v = mw$ به‌ترتیب از مراتب m و nاند. قرار می‌دهیم $W = \mathrm{gp}\{w\}$ و $U = \mathrm{gp}\{u\}$، $V = \mathrm{gp}\{v\}$. گوییم که

$$W = U \oplus V \tag{۴۵.۴}$$

چون $(m, n) = ۱$، اعداد صحیحی مانند a و b وجود دارند که $an + bm = ۱$. ازاین‌رو

$$\begin{aligned} w &= (an + bm)w = a(nw) + b(mw) \\ &= au + bv \end{aligned}$$

این رابطه نشان می‌دهد که $w \in U + V$. اما w، W را تولید می‌کند، که ازاین نتیجه می‌شود $W \subset U + V$. چون $U \subset W$ و $V \subset W$، برعکس داریم $U + V \subset W$ و بنابراین $W = U + V$. برای آنکه ثابت کنیم. حاصلجمع مستقیم است ملاحظه می‌کنیم که $U \cap V = \{۰\}$، زیرا U و V گروههایی از مرتبه‌های متباین‌اند.

نتیجهٔ (۴۴.۴) را می‌توان برای بیش از دوجمله تعمیم داد. به‌ویژه، فرض کنیم

$$m = p_۱^{\alpha_۱} p_۲^{\alpha_۲} \ldots p_t^{\alpha_t}$$

که $p_۱$، $p_۲$، ...، p_t اعداد اول متمایز باشند. دراین صورت داریم

$$\mathrm{gp}\{w\} = \sum_{\tau=۱}^{t} \oplus\, \mathrm{gp}\{w_\tau\} \tag{۴۶.۴}$$

که در آن $w_\tau=(m/p_\tau^{\alpha_\tau})w$ از مرتبهٔ $p_\tau^{\alpha_\tau}$ است. وقتی بعضی از αها صفر باشند، فرمول (۴۶.۴) بازهم می‌تواند مورد استفاده قرار گیرد. درآن‌صورت، جمعوند متناظرش به‌گروه صفر بدل شده، می‌تواند حذف شود.

فرض‌کنیم p عددی اول و P مجموعهٔ عناصری از A است‌که مرتبه‌شان توانی است از p، یعنی عناصری‌که در معادله‌ای به‌صورت $p^\mu x=0$ $(\mu\geqslant 0)$ صدق می‌کنند. بدیهی است که P یک زیرگروه است؛ زیرا اگر $p^\mu x=p^\nu y=0$، آنگاه $p^{\mu+\nu}(x-y)=0$. اگر p، $|A|$ را عاد نکند، آنگاه $P=\{0\}$. P را p-**امین مؤلفهٔ اولیه** A می‌خوانیم. بعداً نشان می‌دهیم که وقتی $|A|$ بر بیش از یک عدد اول قابل قسمت باشد، مؤلفه‌های اولیهٔ یك تجزیهٔ A را به‌دست می‌دهد.

قضیهٔ اصلی ۱۶. فرض می‌کنیم $|A|=p_1^{\nu_1}p_2^{\nu_2}\ldots p_n^{\nu_n}$، و P_i، p_i-امین مؤلفهٔ اولیهٔ A باشد. در این صورت

$$A=P_1\oplus P_2\oplus\cdots\oplus P_n \qquad (۴۷.۴)$$

برهان. اگر w عنصر دلخواهی از A باشد، آنگاه (۴۶.۴) نشان می‌دهد که $w\in P_1+P_2+\cdots+P_n$، وبنابراین $A\subset P_1+P_2+\cdots+P_n$. بعکس، هر P_i در A قراردارد. که از این‌رو نتیجه می‌شود $A=P_1+P_2+\cdots+P_n$. بعلاوه این جمع یك حاصلجمع مستقیم است زیرا جملات آن دارای مراتبی دوبه‌دو متباین‌اند (صفحهٔ ۴۸، (۳) ملاحظه شود). تجزیهٔ (۴۷.۴) به‌معنی ذیل منحصربه‌فرد است؛ فرض‌کنیم

$$A=P_1^*\oplus P_2^*\oplus\cdots\oplus P_n^*$$

که درآن P_i^* یك p_i-گروه‌آبلی است $(i=1,2,\ldots,n)$. دراین‌صورت $P_i^*=P_i$. زیرا فرض‌کنیم $|P_i^*|=p_i^{\mu_i}$؛ با محاسبهٔ مرتبهٔ گروه در هرطرف (۴۷.۴)، می‌بینیم که $|A|=\prod p_i^{\mu_i}$، از این‌رو بنابر تجزیهٔ یکتای $|A|$ به‌عوامل اول، نتیجه می‌شود $\mu_i=\nu_i$. لذا $|P_i|=|P_i^*|$. اما بنابرتعریف P_i، هر P_i^* در P_i واقع است،یعنی $P_i^*\subset P_i$. چون‌این دوگروه از یك مرتبه‌اند، نتیجه می‌گیریم که $P_i^*=P_i$.

(۱) سرانجام، به اثبات قضیهٔ اصلی ۱۴ برمی‌گردیم. قراردادهای قضیهٔ اصلی ۱۶ به‌قوت خود باقی هستند. آنچه برای ما معلوم است عبارت است از:

$$A=\sum_{\kappa=1}^{k}\oplus\,\mathrm{gp}\,\{u_\kappa\}\quad,\quad |u_\kappa|=d_\kappa\,,\ d_{\kappa+1}|d_\kappa \qquad (۴۸.۴)$$

راه اثبات این است‌که هرجمله را به‌مؤلفه‌های اولیه‌اش تجزیه‌کنیم و از این‌رو مقسوم‌علیه‌های اولیهٔ P_1، P_2، ...، P_n را،که یکتایی آنها درقضیهٔ اصلی ۱۵ ثابت شده است، به‌دست آوریم. فرض‌کنیم

$$d_\kappa=\prod_{i=1}^{n}p_i^{\delta_{\kappa i}}\quad(\kappa=1,2,\ldots,k) \qquad (۴۹.۴)$$

که $\delta_{\kappa i} \geqslant 0$ و $\delta_{\kappa+1, i} \leqslant \delta_{\kappa i}$. هرگاه (۴۶.۴) را روی هر u_κ اثر دهیم می‌توانیم بنویسیم

$$\mathrm{gp}\,\{u_\kappa\} = \sum_{i=1}^{n} \oplus\, \mathrm{gp}\,\{u_{\kappa i}\}$$

که درآن $|u_{\kappa i}| = p^{\delta_{\kappa i}}$. لذا می‌توانیم A را به‌صورت یک حاصلجمع مضاعف از p-گروهها بیان کنیم، یعنی

$$A = \sum_{\kappa=1}^{k} \sum_{i=1}^{n} \oplus\, \mathrm{gp}\,\{u_{\kappa i}\} \tag{۵۰.۴}$$

به‌ازای یك i ثابت، پیدا می‌کنیم که

$$P_i = \sum_{\kappa=1}^{k} \oplus\, \mathrm{gp}\,\{u_{\kappa i}\}$$

این تساوی نشان‌می‌دهد که مقسوم‌علیه‌های اولیهٔ P_i، عناصرغیرواحد رشتهٔ نزولی‌یکنواخت

$$p^{\delta_{1i}},\ p^{\delta_{2i}},\ \dots,\ p^{\delta_{\kappa i}}$$

هستند.

این وضع به‌وسیلهٔ جدول ذیل خلاصه شده‌است که درآن برای‌سهولت اصلاً نماهای توانهای اول آورده شده‌اند.

$$\begin{array}{c|cccc} & p_1 & p_2 & \cdots & p_n \\ \hline d_1 & \delta_{11} & \delta_{12} & \cdots & \delta_{1n} \\ d^2 & \delta_{21} & \delta_{22} & \cdots & \delta_{2n} \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ d_k & \delta_{k1} & \delta_{k2} & \cdots & \delta_{kn} \end{array} \tag{۵۱.۴}$$

سطرهای این جدول با (۴۹.۴) متناظرند، درصورتی که عناصر غیرصفر ستونها مقسوم‌علیه‌های اولیه P_1، P_2، ...، P_n را تعیین می‌کنند. درایه‌های هرستون برحسب بزرگی‌شان به‌طور غیرصعودی منظم شده‌اند، و سطر آخر تماماً صفر نیست، زیرا $d_k \geqslant 2$.

اکنون فرض‌کنیم به‌جای dها مجموعهٔ eها را، که همان نقش را ایفا می‌کنند بگذاریم:

$$e_\lambda = \prod_{j=1}^{n} p^{\varepsilon_{\lambda j}} \quad (\lambda = 1, 2, \dots, l)$$

قضیهٔ اصلی ۱۵ تضمین می‌کند که در جداول (δ_{κ_i}) و $(\varepsilon_{\lambda_i})$ ستونهای متناظر، درایه‌های غیرصفر همانندی دارند. چون حداقل یك ستون از $(\delta_{\kappa i})$ دارای k درایهٔ غیرصفر است،

نتیجه می‌شود که $k \geqslant l$؛ به طریق مشابه، بنابر تقارن، $l \geqslant k$. ازاین‌رو $k = l$ و جداول $(\delta_{\kappa i})$ و $(\varepsilon_{\lambda i})$ یکی می‌شوند. واین نکته پایان برهان قضیهٔ اصلی ۱۴ است. اعداد صحیح d_1، d_2، . . . ، d_k **پایاهای** A خوانده می‌شوند و فرض براین است که همواره در شرط بخشپذیری $d_{\kappa+1} | d_\kappa$ صدق می‌کنند. **مقسوم‌علیه‌های اولیهٔ** A عبارت‌اند از مجموعهٔ مقسوم‌علیه‌های اولیهٔ مؤلفه‌های اولیهٔ $P_i (i = 1, 2, \ldots, n)$. برهان پیشین نشان می‌دهد که اگر پایاها معلوم باشند، مقسوم‌علیه‌های اولیه مشخص می‌شوند و بعکس. هریك ازاین مجموعه‌ها ساختار A راکاملاً تشریح می‌کند، وکلیهٔ دسته‌های یکریخت گروههای مم آبلی با معلوم بودن پایاها یا مقسوم‌علیه‌های اولیه به‌دست می‌آیند. مقسوم‌علیه‌های اولیه تجزیهٔ (۵۰.۴) راکه شامل بیشترین شمار جمعیده‌های دوری هستند به‌ما می‌دهند. درصورتی‌که پایاها تجزیهٔ (۴۸.۴) را باکمترین عدهٔ جملات دراختیار ما می‌گذارند.

مثال ۱. پایاهای گروهی را پیداکنید که مقسوم‌علیه‌های اولیه‌اش اعداد 2^3، ۲، ۲، ۳، ۳ باشند جدول (۵۱.۴) به‌جدول زیر بدل می‌شود.

	۲	۳
d_1	۳	۱
d_2	۱	۱
d_3	۱	۰

ازاینجا نتیجه می‌شود که $d_1 = 2^3 \times 3 = 24$، $d_2 = 2 \times 3 = 6$، $d_3 = 2$. مرتبهٔ گروه عبارت است از

$$|A| = 24 \times 6 \times 2 = 2^5 \times 3^2 = 288$$

مثال آتیه روشن می‌کندکه چگونه یك حاصلجمع مستقیم گروههای دوری می‌توانند به‌یکی از دوصورت متعارف، که به‌ترتیب با مقسوم‌علیه‌های اولیه یا پایاها متناظرند، منجر شود.

مثال ۲. مقسوم‌علیه‌های اولیه وپایاهای گروه

$$A = C_{30} \oplus C_{12}$$

را پیداکنید.

این حاصلجمع به‌صورت متعارف نیست، زیرا $30 \nmid 12$. ابتدا، هر جمله را به گروههایی ازمرتبه‌های متباین، تجزیه می‌کنیم، لذا

$$A = (C_2 \oplus C_3 \oplus C_5) \oplus (C_4 \oplus C_3)$$

باگردآوری جملات متعلق به‌هرعدد اول دریك پرانتز داریم

$$A=(C_{۴}\oplus C_{۲})\oplus(C_{۳}\oplus C_{۳})\oplus C_{۵}$$

این تساوی نشان می‌دهد که مقسوم‌علیه‌های اولیه که بـا اعداد اول ۲، ۳، و ۵ متناظرنـد به‌ترتیب (۴, ۲)، (۳, ۳) و ۵ هستند. در واقع، جدول (۵۱.۴) چنین می‌شود

	۲	۳	۵
$d_{۱}$	۲	۱	۱
$d_{۲}$	۱	۱	۰

از اینجا نتیجه می‌شود $d_{۱}=۲^{۲}\times ۳\times ۵=۶۰$، $d_{۲}=۲\times ۳=۶$. لذا

$$A=C_{۶۰}\oplus C_{۶}$$

صورت متعارف A است که پایاهای آن را نشان می‌دهد.

۲۹. روش تجزیـه. ما در بخش **۲۷** این نتیجهٔ اساسی را کـه هر گروه مم آبلی بـا یك حاصلجمع مستقیم از گروههای دوری یکریخت‌است بررسی کردیم. اما بحثی که در برهان این قضیه از آن‌استفاده شده مستقیماً به‌یك روش عملی برای تعیین جمعیده‌های دوری منجر می‌شود. هدف بخش حاضر تبیین روشی منظم برای حل این مسئله درحالات واقعی است.

فرض کنیم A برحسب مولدها و رابطه‌ها داده شده باشد. لذا فرض می‌کنیم

$$A=\mathrm{gp}\{x_{۱}, x_{۲}, \ldots, x_{n}\}$$

که در آن $x_{۱}$، $x_{۲}$، ...، x_{n} بستگی به N رابطه

$$\sum_{j=۱}^{n} b_{ij}x_{j}=۰ \quad (i=۱, ۲, \ldots, N)$$

دارند. ماتریس $N\times n$ صحیح $B=(b_{ij})$ ماتریس رابطه خوانده می‌شود. همچنان‌که در بخش **۲۷** داشتیم این مسئله را با واردکردن یك گروه آبلی آزاد

$$F=\langle u_{۱}, u_{۲}, \ldots, u_{n}\rangle \qquad (۵۲.۴)$$

ویك رابطهٔ زیرگروهی

$$R=\mathrm{gp}\{r_{۱}, r_{۲}, \ldots, r_{N}\} \qquad (۵۳.۴)$$

به‌صورت دیگر بیان می‌کنیم، که در آن

$$r_{i}=\sum_{j=۱}^{n} b_{ij}u_{j} \quad (i=۱, ۲, \ldots, N)$$

باید متذکر شدکه بنابرتعریف، u_iها مولدهای آزاد Fاند، درحالی‌که r_iها صرفاً R را تولید می‌کنند. سپس همچنان‌که در (۳۱.۴) دیده‌ایم، گروه A به‌صورت F/R ظاهر می‌شود وساختار آن زمانی آشکار می‌شودکه مولدهای جدید به‌طریقی انتخاب شده باشند که (۳۲.۴) برقرار باشد. نسبت به‌این مولدها ماتریس رابطه دارای این ویژگی ساده است که‌کلیهٔ عناصر غیرقطری آن صفرند. بعکس، اگر داشته باشیم

$$B=\begin{pmatrix} d_1 & 0 & 0 & \dots \\ 0 & d_2 & 0 & \dots \\ 0 & 0 & d_3 & \dots \end{pmatrix} \qquad (۵۴.۴)$$

تجزیهٔ Z به‌گروههای دوری می‌تواند صورت گیرد. ولی، این نتیجه با صورت متعارف تبیین شدهٔ درقضیهٔ اصلی ۱۳ مطابقت ندارد مگر آنکه شرایط دیگر $d_{i+1}|d_i$ برقرار باشند. به دلایل فنی نادیده‌گرفتن این شرایط درمرحلهٔ اول و توجه به‌یك تبدیل موقتی متناظر به یك ماتریس رابطه‌که صرفاً قطری است، رجحان دارد (مثال ۲، صفحهٔ ۱۰۷ ملاحظه شود).

می‌توان مسئله را به‌صورت جدولی به‌طریق ذیل بیان کرد

$$\begin{array}{c|cccc} & u_1 & u_2 & \dots & u_n \\ \hline r_1 & b_{11} & b_{12} & \dots & b_{1n} \\ r_2 & b_{21} & b_{22} & \dots & b_{2n} \\ \vdots & \vdots & \vdots & & \vdots \\ r_N & b_{N1} & b_{N2} & & b_{Nn} \end{array} \qquad (۵۵.۴)$$

ستونهای این جدول با مولدهای F متناظرند، درحالی‌که سطرهای‌آن نمایشگر مولدهای Rاند: چون درانتخاب مولدها هم برای F وهم برای R مختار هستیم، می‌توانیم اعمال (α)، (β)، (γ)، و (δ) (صفحهٔ ۹۵) را برای هریك ازمولدها بدون تغییرساختار F/R به‌کار بندیم. اما دربارهٔ R، این امر بدین‌معنی است‌که اعمالی برسطرهای جدول (۵۵.۴) انجام می‌گیرد، ولی پی‌بردن به‌اثر تغییر مولدهای F نیاز به‌دقت بیشتری دارد. فرض کنیم بخواهیم مولدهای جدیدی برای F با استفاده ازتبدیلات

$$u'_1=u_1+qu_2,\ u'_2=u_2,\ u'_3=u_3,\ \dots,\ u'_n=u_n \qquad (۵۶.۴)$$

که در آن q عدد صحیح دلخواهی است، وارد نماییم، وگیریم

$$r=b_1u_1+b_2u_2+\dots+b_nu_n$$

یك عنصرکلی از زیرگروه رابطه باشد. باتوجه به‌مولدهای جدید، این رابطه چنین‌می‌شود

$$r=b_1u'_1+(b_2-qb_1)u'_2+b_3u'_3\dots+b_nu'_n$$

لذا به‌جای سطر اول (۵۵.۴)، مقادیر (۵۶.۴) گذاشته می‌شود درصورتی‌که، درماتریس B، q برابرستون اول ازستون دوم کم شده‌است. این عملی‌است ازنوع (β) که برستونها اعمال شده است.

ما اکنون یك رشته مراحلی را نشان می‌دهیم که B را به‌صورت قطری (۵۴.۴) تبدیل می‌کند.

(الف) وقتی $B = \circ$، $A = F$ یك گروه آبلی آزاد است،ومسئله روشن است. لذا حالا فرض می‌کنیم که $B \neq \circ$. با جایگشت سطرها وستونها، و، درصورت لزوم، تغییرعلامت یکی ازآنها، می‌توانیم چنان ترتیبی بدهیم که لولای b_{11} در

$$b_{11} > \circ,\ b_{11} \leqslant |b_{i1}|,\ b_{11} \leqslant |b_{1j}| \quad (i > 1,\ j > 1)$$

صدق کند.

(ب) ممکن است چنین اتفاق افتدکه همهٔ عناصر B که با b_{11} دریك ستون یا دریك سطر قرار دارند بر b_{11} قابل‌قسمت باشند. درچنین حالتی می‌توانیم کلیهٔ این عناصر را با کم‌کردن مضارب مناسبی ازسطر (ستون) اول از دیگر سطرها (ستونها) به‌صفر بدل کنیم. پس ازانجام این عمل، ماتریس رابطه چنین می‌شود:

$$\begin{pmatrix} b_{11} & \circ \\ \circ & B_1 \end{pmatrix} \tag{۵۷.۴}$$

و به‌همان قیاس روی B_1 عمل می‌کنیم تا آنکه به (۵۴.۴) برسیم.

(ج) ازسوی دیگر، هرگاه یکی از b_{i1} یا b_{ij}ها بر b_{11} قابل‌قسمت نباشد، یك عمل ازنوع (β) موجب خواهد شدکه به‌جای‌این عنصرکوچکترین باقیماندهٔ مثبت به‌هنگ b_{11} گذاشته شود. برای مثال، ممکن است داشته باشیم که

$$b_{i1} - qb_{11} = b'_{i1}$$

که درآن $b_{11} > b'_{i1} > \circ$. سپس b'_{i1} را جملهٔ مقدم‌می‌گیریم وعمل‌کاهش با لولای‌جدید را تکرار می‌کنیم. واضح است که این روند باید بعد ازچند مرحلهٔ معین به‌پایان برسد، به‌طوری‌که وضعیت مذکور در (ب) نهایتاً به وجود آید، زیرا یك رشتهٔ نزولی از اعداد صحیح مثبت وضعیت لولایی دارند.

مثال ۳. پیداکنید پایاهای گروه آبلی A راکه به‌وسیلهٔ a، bو c تولید می‌شود ودر آن روابط ذیل برقرارند

$$۳a - ۲b + ۵c = \circ,\ ۵a + ۲۷c = \circ$$

انجام رشته عملیات ذیل برماتریس رابطه‌ای، منجر به‌صورت متعارف درآمدنی آن می‌شود:

$$\begin{matrix} 3 & -2 & 5 \\ 5 & 0 & 27 \end{matrix} \xrightarrow{(1)} \begin{matrix} 1 & -2 & 5 \\ 5 & 0 & 27 \end{matrix} \xrightarrow{(2)} \begin{matrix} 1 & -2 & 5 \\ 0 & 10 & 2 \end{matrix}$$

$$\xrightarrow{(3)} \begin{matrix} 1 & 0 & 0 \\ 0 & 10 & 2 \end{matrix} \xrightarrow{(4)} \begin{matrix} 1 & 0 & 0 \\ 0 & 0 & 2 \end{matrix} \xrightarrow{(5)} \begin{matrix} 1 & 0 & 0 \\ 0 & 2 & 0 \end{matrix}$$

اینك گذار به‌مولدهای جدید و رابطه‌ها را، که به‌مراحل مختلف مربوط‌اند، نشان می‌دهیم:

(۱) مولدها $u_1=u'_1,\ u_2=u'_1+u'_2,\ u_3=u'_3$

(۲) رابطه‌ها $r'_1=r_1,\ r'_2=r_2-5r_1$

(۳) مولدها $u'_1=u''_1+2u''_2-5u''_3,\ u'_2=u''_2,\ u'_3=u''_3$

(۴) مولدها $u''_1=u'''_1,\ u'_2=u'''_2,\ u''_3=u'''_3-5u'''_2$

(۵) مولدها $u'''_1=v_1,\ u'''_2=v_3,\ u'''_3=v_2$

این مراحل، تبدیل را کامل می‌کند. بـا استفاده از قرارداد صفحهٔ ۹۹ می‌بینیم که F/R بـه وسیلهٔ v_1، v_2، v_3 تـولید شده است که $v_1=0$، $2v_2=0$. در ضمن v_3 از مرتبهٔ نامتناهی است.

بنابراین

$$A \cong C_2 \oplus C_\infty$$

از حذف مولدهای واسط به‌دست می‌آوریم

$$v_1=3u_1-2u_2+5u_3,\ v_2=5u_1+5u_2+u_3,\ v_3=-u_1+u_2$$

و دانشجو می‌تواند تحقیق کند که این یك تبدیل یکهنگی است.

هرگاه ثبت تغییر مولدها غیرضروری به‌نظر آید، ساختار دوری را می‌توان بااعمال عملیات لولایی برماتریس رابطه، تا حصول صورت قطری آشکار کرد. درمثال ذیل، کـه در آن عملیات ستونی کافی هستند، ستون j زام به c_j نشان داده شده است.

مثال ۲. تجزیهٔ متعارف گروه آبلی با مولدهای a، b، c، d و رابطه‌های

$$3a+9b-3c=0,\ 4a+2b-2d=0$$

را پیداکنید.

ماتریس رابطه را می‌توان به‌طریق ذیل تبدیل کرد:

$$\begin{matrix} 3 & 9 & -3 & 0 \\ 4 & 2 & 0 & -2 \end{matrix} \qquad \to \begin{matrix} 3 & 9 & -3 & 0 \\ 0 & 0 & 0 & -2 \end{matrix}$$

$$(c_1 \to c_1+2c_4,\ c_2 \to c_2+c_4)$$

$$\rightarrow \begin{matrix} 3 & 0 & 0 & 0 \\ 0 & 0 & 0 & 2 \end{matrix} \qquad\qquad \rightarrow \begin{matrix} 3 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \end{matrix}$$

$$(c_2 \rightarrow c_2 - 3c_1,\ c_3 \rightarrow c_3 + c_1,\ c_4 \rightarrow -c_4) \qquad (c_2 \rightarrow c_4,\ c_4 \rightarrow c_2)$$

ازآنجا نتیجه می‌شود که دومولد آزاد باقی می‌مانند، درحالی‌که دوتای دیگر به‌گروههای دوری به‌ترتیب ازمراتب ۳ و ۲ مربوط می‌شوند. لذا گروه با

$$C_3 \oplus C_2 \oplus C_\infty \oplus C_\infty$$

یکریخت است.

تمرین

(۱) ثابت‌کنید که هرگاه b_1، b_2، . . .، b_n اعدادی صحیح باشند به قسمی که $(b_1, b_2, \ldots, b_n) = 1$، یک ماتریس یکهنگی وجود دارد که سطر اول آن $b_1, b_2, \ldots, b_n$ است.

(۲) نشان دهید هرگاه رتبهٔ یک گروه آبلی متناهی برمربع هیچ عددی (بزرگتر از ۱) بخشپذیر نباشد، آنگاه این گروه دوری است.

(۳) ثابت‌کنید که دریک گروه آبلی متناهی (۱) مرتبهٔ ماکسیمال یک عنصر برابر است با بزرگترین پایای گروه و (۲) مرتبهٔ هرعنصر، مرتبهٔ ماکسیمال را عاد می‌کند.

(۴) نشان دهیدکه گروه (ضربی) رده‌های مانده‌های اعداد متباین با ۲۴، گروه اولیهٔ آبلی از مرتبهٔ ۸ است.

(۵) مقسوم‌علیه‌های اولیه وپایاهای گروههای آبلی ذیل راکه به توسط مولدها و رابطه‌ها تعریف شده‌اند پیداکنید: (الف) $15a = 4b = 0$، (ب) $20a = 6b = 5c = 0$.

(۶) گروه آبلی A به‌وسیلهٔ a ، b ، c و رابطه‌های معرف $3a + 9b + 9c = 0$، $6a - 12b = 0$ تولید شده است. A را به‌صورت حاصلجمع مستقیم گروههای دوری بیان کنید.

(۷) رتبه وپایاهای گروههای آبلی ذیل را پیداکنید: (الف) با مولدهای a، b، ورابطهٔ $2(a + b) = 0$؛ (ب) با مولدهای a، b، c، d و رابطه‌های $3a + 5b - 3c = 0$، $4a + 2b - 2d = 0$.

(۸) گروه آبلی آزاد F به‌وسیلهٔ مولدهای u_1، u_2، u_3 تولید شده است و R زیرگروهی است که بدوسیلهٔ

$$r_1 = ku_1 + u_2 + u_3,\ r_2 = u_1 + ku_2 + u_3,\ r_3 = u_1 + u_2 + ku_3$$

(k عدد صحیحی بزرگتر از ۱)، تولید شده است. مولدهای v_1، v_2، v_3 از F و s_1، s_2، s_3 از R را چنان پیدا کنید که $s_i = e_i v_i$ $(i = 1, 2, 3)$ و e_1، e_2، e_3 اعدادی صحیح‌اند که در $e_1 | e_2 | e_3$ صدق می کنند.

(۹) نشان دهید که در یک گروه آبلی ازمرتبهٔ g متناظر با هر عاملی از g که قبلاً اختیار کنیم حداقل یك زیر گروه ازهمان مرتبه وجود دارد. (عکس قضیهٔ اصلی لاگرانژ برای گروههای آبلی.)

(۱۰) تحقیق کنید که یك گروه آبلی اولیه ازمرتبهٔ p^k (p عدد اول) را می‌توان به‌صورت یك فضای برداری k-بعدی برمیدان اعداد اول درنظر گرفت که عناصر آن ۰، ۱، . . . ، $p-1$ باشند.

(۱۱) نشان دهید که در یك گروه آبلی اولیه ازمرتبهٔ p^3 یك مبنای «مرتب» را می‌توان به‌تعداد $p^3(p^3-1)(p^2-1)(p-1)$ طریق انتخاب کرد. [مبناهایی که عناصر آنها یکی ولی ترتیب‌شان مختلف هستند متمایز گرفته می‌شوند.]

(۱۲) ثابت کنید که نتایج بخش **۲۷** به قضیهٔ اصلی بنیادی ذیل در مورد ماتریسها منتج می‌شود: اگر B یك ماتریس صحیح $m \times n$ ازمرتبهٔ k باشد، ماتریسهای یکهنگی مانند P و Q به ترتیب ازمراتب m و n وجود دارند به‌قسمی که $PBQ = D$، که در $D = (d_{ij})$ کلیهٔ عناصر صفرند بجز نخستین k عنصر قطری و $d_{11} | d_{22} \cdots | d_{kk}$.

۵

مولدها و رابطه‌ها

۳۰. گروههای متناهی‌ـمولود وگروههای مربوط به آنها. در فصل قبل دیدیم که می‌توان ساختار یك گروه آبلی را به‌نحو رضایت‌بخشی تعیین کرد مشروط برآنکه این گروه به‌توسط تعداد متناهی عنصر که درتعداد متناهی رابطه صدق می‌کنند تولید شده باشد. طبعاً این‌سؤال پیش می‌آیدکه آیا نظریهٔ مشابهی برای گروههای غیرآبلی وجود دارد. دربخش ۱۲ به‌این مسئله مختصری اشاره شد، و ما به‌چند مثال ازگروههای غیرآبلی که برحسب مولدها و رابطه‌ها بیان شده بودند برخوردکردیم. همچنان‌که می‌توان انتظار داشت، نبودن قانون تعویضپذیری موجب پیچیدگی خیلی بیشتر این حالت می‌شود، وظرفیت این کتاب نیز فقط به ما اجازه می‌دهد ساده‌ترین مفاهیم و حقایق این مبحث دامنه‌دار را در اینجا عرضه کنیم.

در آغاز کار ما خود را به‌گروههایی، که بنابرفرض می‌توان به‌وسیلهٔ تعداد متناهی عنصر با تعداد متناهی رابطه تولید نمود، محدود می‌کنیم. این گونه گروهها راگروههای با مولدها و رابطه‌های متناهی می‌خوانیم.

۳۱. گروههای آزاد. نمادهای تعویضناپذیر x_1، . . . ،x_2، . . . ، x_n را وارد می‌کنیم و با آنها **واژه‌های ریاضی**، یعنی حاصلضربهای صوری مانند

$$w = x_a^{\alpha} x_b^{\beta} \cdots x_r^{\rho} \qquad (۱۰۵)$$

متشکل از تعداد متناهی عامل را، تشکیل‌می‌دهیم. زیرنمایه‌های a، b، . . . ، r ازمجموعهٔ

اعداد صحیح ۱، ۲، . . . ، n انتخاب شده‌اند. چون عاملها تعویضپذیر نیستند، تکرارمجاز گرفته شده است. نماهای α، β، . . . ، ρ اعـداد صحیح مثبت و یا منفی‌انـد. یك **واژهٔ ریاضی**ـ یا به‌اختصار یك واژهـ را می‌توان به‌عنوان تابعی از x_1، x_2، . . . ، x_n در نظر گرفت و بنابراین w را به‌طور روشنتر به‌صورت $w(x_1, x_2, \ldots, x_n)$ نوشت.

بجاست که **واژهٔ خالی**، یعنی، واژه‌ای را که در آن تعداد عاملها صفر است معرفی کنیم. واژهٔ خالی به e نشان داده و چنین تعریف می‌شود:

$$x_i^{\circ} = e \quad (i = 1, 2, \ldots, n)$$

یك واژه را وقتی **کاسته** نامیم که یا خالی و یا حاصلضربی به‌صورت (۱.۵) باشد که در آن هیچ دو x متوالی دارای یك زیرنمایه نباشند.

ضرب دو واژهٔ غیرخالـی u و v چنین تعریف می‌شود: حاصلضرب صوری p است متشکل ازعاملهای u که عاملهای v به‌دنبال آنها آمده‌اند. اگر اتفاقاً p یك واژهٔ کاسته باشد، آن را با uv تعریف می کنیم. در غیر این صورت، فرض می کنیم

$$u = u_{\circ} x^{\alpha}, \quad v = x^{\beta} v_{\circ}$$

و $u_{\circ}$ به x منتهی نگردد و $v_{\circ}$ با x شروع نشود. سپس p را با اعمال قاعدهٔ

$$x^{\alpha} x^{\beta} = x^{\alpha+\beta} \tag{۲.۵}$$

ساده می کنیم. اگر $\alpha+\beta = \circ$، عامل $x^{\alpha+\beta}$، ازبین می‌رود و ممکن است ساده‌سازیها و حذفهای دیگری امـکان‌پذیر باشند. این عمل ادامـه می‌یابد تا آنکه به‌یك واژهٔ کاسته $p_{\circ}$ برسیم. در این صورت چنین تعریف می کنیم

$$uv = p_{\circ}$$

باید متذکرشویم که روندکاسته‌سازی منحصربه‌فرد است به‌نحوی کـه uv دارای یـك معنی خالی از ابهام است. به‌کمك قاعدهٔ بدیهی

$$ue = eu = u$$

قانون ترکیب تکمیل می‌شود، یعنی عبارت خالی همچون عنصر واحد عمل می کند. عکس (۱.۵) به‌توسط

$$w^{-1} = x_r^{-\rho} \cdots x_b^{-\beta} x_a^{-\alpha}$$

داده می‌شودکه آشکارا واژه‌ای است‌کاسته. تحقیق مستقیم قانون شرکتپذیری

$$(uv)w = u(vw) \tag{۳.۵}$$

اندکی به‌کار زیاد نیاز دارد* و بهترین راه آن در چند مرحله به‌شرح ذیل است.

(الف) گیریم x یك‌مولد منفرد باشد،و $u_{\circ}$ و $w_{\circ}$ واژه‌های کاسته (احتمالاً خالی) باشند

---

* رجوع کنید به A. G. Kurosh, 1955, *The theory of groups*, 1, p, 126.

به‌قسمی‌که نه آخرین عامل $u_\circ$ توانـی از x با نمای غیرصفر باشد و نه اولین عامل $w_\circ$.
در این صورت به‌سهولت دیده می‌شود‌که

$$(u_\circ x^\alpha)(x^\beta w_\circ)=u_\circ(x^{\alpha+\beta}w_\circ)=(u_\circ x^{\alpha+\beta})w_\circ$$

(ب) اگر u و v واژه‌های‌کاسته و x مولدی دلخواه باشند، آنگاه

$$(ux^\alpha)w=u(x^\alpha w) \tag{۴.۵}$$

زیرا فرض‌کنیم

$$u=u_\circ x^\pi,\quad w=x^\phi w_\circ$$

که $u_\circ$ و $w_\circ$ همان $u_\circ$ و $w_\circ$ در (الف) هستند و π و ϕ اعدادی صحیح‌اندکه ممکن‌است صفر باشند. لذا داریم

$$\begin{aligned}(ux^\alpha)w&=[(u_\circ x^\pi)x^\alpha](x^\phi w_\circ)\\&=(u_\circ x^{\pi+\alpha})(x^\phi w_\circ)\\&=u_\circ(x^{\pi+\alpha+\phi}w_\circ)\\&=u_\circ[x^\pi(x^{\alpha+\phi}w_\circ)]\\&=u_\circ[x^\pi(x^\alpha w)]\\&=(u_\circ x^\pi)(x^\alpha w)\\&=u(x^\alpha w)\end{aligned}$$

(ج) بالاخره، برای اثبات (۳.۵) در حالت‌کلـی، به‌استقراء برتعداد عاملهـای v متوسل‌می‌شویم. حالتی‌کـه v به‌فقط یك عامل x^α تبدیـل می‌شود به‌توسط (۴.۵) تـأمین می‌شود. حال فرض‌کنیم‌که

$$v=v_\circ x^\alpha$$

و قانون شرکتپذیری به‌جای v با $v_\circ$ برقرار باشد. در این‌صورت داریم

$$\begin{aligned}(uv)w=(uv_\circ x^\alpha)w&=[(uv_\circ)x^\alpha]w\\&=(uv_\circ)(x^\alpha w)=u[v_\circ(x^\alpha w)]\\&=u[(v_\circ x^\alpha)w]=u(vw)\end{aligned}$$

این امر تحقیق (۳.۵) را در تمام حالات‌کامل می‌کند.

مجموعهٔ واژه‌های‌کاسته در نمادهای x_1، x_2، . . . ، x_n با قانون ترکیبی که هم‌اکنون تعریف‌کردیم **گروه آزاد** با x_1، x_2، . . . ، x_n نامیده می‌شود. گروه آزاد با یك مولد منفرد x، گروه دوری نامتناهی است (بخش۵ ملاحظه شود). در حالتی‌که دو مولد x و y داده شده باشند، حاصلضربهای نوعی عبارت‌اند از

$$(xy^{-۲}x)(yx)=xy^{-۲}xyx$$
$$(xy^{۲})(y^{-۱}x)=xyx$$
$$(xyx^{-۱})(xy^{-۱}x)=x^{۲}$$

بدطور خلاصه می‌توان گفت که گروه آزاد با $x_۱$، $x_۲$، . . . ، x_n متشکل از همهٔ واژه‌های کاسته در این نمادها هستند که صرفاً تابع شرایط بدیهی

$$x_ix_i^{-۱}=x_i^{-۱}x_i=e \quad (i=۱, ۲, \dots, n) \qquad (۵.۵)$$

و نتایج آنها هستند. باید متذکر شد که یك گروه آبلی آزاد با بیش از یك متغیر، یك گروه آزاد نیست، زیرا رابطهٔ بدیهی $xyx^{-۱}y^{-۱}=e$ در یك گروه آبلی برقرار است اما در یك گروه آزاد برقرار نیست.

۳۲. رابطه‌ها. فرض کنیم G گروهی باشد که به‌توسط n تا از عناصرش مثل:

$$G=\mathrm{gp}\{g_۱, g_۲, \dots, g_n\}$$

تولید شده باشد. پس هرعنصر G حاصلضربی به‌صورت $g_a^{\alpha}g_b^{\beta}\dots g_r^{\rho}$ دارد. و درحالتی که G یك گروه آزاد نباشد، معادلاتی غیربدیهی مانند

$$g_a^{\alpha}g_b^{\beta}\dots=g_c^{\gamma}g_d^{\delta}\dots$$

یا با نماد مختصرتر

$$r(g_۱, g_۲, \dots, g_n)=۱ \qquad (۶.۵)$$

وجود دارند که در آن، سمت چپ معرف

$$(g_a^{\alpha}g_b^{\beta}\dots)(g_c^{\gamma}g_d^{\delta}\dots)^{-۱}$$

است. به‌منظور تجزیه وتحلیل مفصلتر این مورد، گروه‌آزاد F با n نماد $x_۱$، $x_۲$، . . . ، x_n را درنظر می‌گیریم و سپس نگاشت

$$\theta : F \to G$$

را از F به‌روی G با ضابطهٔ

$$w(x_۱, x_۲, \dots, x_n)\theta=w(g_۱, g_۲, \dots g_n) \qquad (۷.۵)$$

تعریف می کنیم، که بدین‌معنی است که نگارهٔ هر حاصلضرب از xها بر اثر θ عبارت‌است از حاصلضرب gهای متناظرشان؛ به‌ویژه

$$e\theta=۱$$

حقیقت مهمی که باید تذکر داده شود این‌است که θ یك همریختی است. لذا اگر $w_۱$ و $w_۲$ دو عنصر دلخواه F باشند، آنگاه

$$(w_1 w_2)\theta = (w_1\theta)(w_2\theta) \qquad (۸.۵)$$

زیرا $w_1 w_2$ به‌عنوان واژهٔ کاسته‌ای تعریف شده که از پهلوی هم قراردادن w_1 و w_2 و سپس ساده‌کردن آن به‌استناد قواعد (۲.۵) و (۵.۵) به‌دست آمده است. اما این قواعد در هر گروه برقرارند، و هرعملی که بر x_i انجام گرفته باشد برای g_i نیز معتبر است و همهٔ منظور (۸.۵) نیز همین است. به‌موجب این واقعیت که θ یك همریختی است می‌توانیم آن را به‌گونه‌ای ساده‌تر با

$$x_i\theta = g_i \quad (i = ۱, ۲, \ldots, n) \qquad (۹.۵)$$

مشخص سازیم که از استفادهٔ مکرر آن (۷.۵) نتیجه می‌شود. گیریم R هستهٔ θ، یعنی کلیهٔ واژه‌های $r(x_1, x_2, \ldots, x_n)$ از F باشد که بر اثر θ به‌سمتهای چپ رابطه‌های (۶.۵) از G نگاشته می‌شوند. یادآوری می‌کنیم که بنا بر اولین قضیهٔ اصلی یکریختی

$$G \cong \frac{F}{R} \qquad (۱۰.۵)$$

از جمعبندی نتایج خود می‌توانیم قضیهٔ اصلی ذیل را بیان کنیم.

قضیهٔ اصلی ۱۷. فرض کنیم F گروه آزاد با x_1، x_2، ...، x_n باشد. در این صورت هرگروه G که بتواند به وسیلهٔ nتا از عناصرش تولید گردد، به موجب نگاشت $x_i\theta = g_i$ $(i = ۱, ۲, \ldots, n)$، یك نگاشت همریخت F است. هستهٔ θ مرکب از کلیهٔ واژه‌هایی از F است که در G بر اثر θ به‌رابطه بدل شوند.

زوج F و R از گروه را که در طرف راست (۱۰.۵) ظاهر می‌شوند یك **نمای** G گویند. یك گروه ممکن‌است که تعداد زیادی از این‌گونه نماها داشته باشد. بعکس، با انتخاب یك زیرگروه نرمال R از F، G به‌صورت F/R تعریف می‌شود. در این‌صورت G دارای مولدهای $g_i = x_iR$ $(i = ۱, ۲, \ldots, n)$ و رابطه‌های $r(g_1, g_2, \ldots, g_n) = ۱$ است، که $r(x_1, x_2, \ldots, x_n)$ در R تغییر می‌کند؛ زیرا $q(g_1, g_2, \ldots, g_n) = ۱$ فقط و فقط وقتی یك رابطه برای G است که $q(x_1, x_2, \ldots, x_n)R = R$، یعنی

$$q(x_1, x_2, \ldots, x_n) \in R$$

بدین ترتیب عناصر R با رابطه‌هایی که مولدهای G در آنها صدق می‌کنند یك تناظر یك‌بدیك برقرار می‌کنند. بدین‌سبب R را **گروه رابطه‌ای** G می‌نامیم.

۳۳. تعریف یك گروه. اکنون می‌خواهیم منظور خود را از گروهی که به توسط n مولد g_1، g_2، ...، g_n و m رابطهٔ

$$\rho_k(g_1, g_2, \ldots, g_n) = ۱ \quad (k = ۱, ۲, \ldots, m) \qquad (۱۱.۵)$$

تولید می‌شود به‌طور مفصلتر شرح دهیم. اگر $\sigma(g_1, g_2, \ldots, g_n) = ۱$ و $\tau(g_1, g_2, \ldots, g_n) = ۱$ دو رابطه در G باشند، آنگاه

$$\sigma(g_1, g_2, \quad , g_n) \quad \tau(g_1, g_2, \quad , g_n) = 1$$
$$\{\sigma(g_1, g_2, \quad , g_n)\}^{-1} = 1$$
و
$$g^{-1}\{\sigma(g_1, g_2, \quad , g_n)\}g = 1$$
که در آن g یك عنصر دلخواه G است، نیز در G رابطه‌اند. هر رابطه مانند

$$\rho(g_1, g_2, \quad , g_n) = 1 \tag{۱۲.۵}$$

حاصل از رابطه‌های مفروض (۱۱.۵) با اجرای عملیات فوق، به‌هر چند بار که باشد، یك **نتیجهٔ** (۱۱.۵) خوانده می‌شود.

با استفاده از گروه‌آزاد F با x_1، x_2، . . . ، x_n واژهٔ $r = \rho(x_1, x_2, \ldots, x_n)$ را به‌رابطهٔ (۱۲.۵) وابسته می‌سازیم. بی‌آنکه به‌کلیت استدلال خللی وارد شود می‌توانیم فرض کنیم که این یك واژهٔ کاسته است و بنا بر این یك عنصر واجد شرط F؛ برای‌مثال رابطهٔ

$$g_1 g_2 g_2^{-2} g_1 g_2^{-1} = 1$$

را مجاز نمی‌شماریم بلکه به‌جای آن

$$g_1 g_2^{-1} g_1 g_2^{-1} = 1$$

را می‌گذاریم. رابطه‌های (۱۱.۵) متناظر با واژه‌های

$$r_k = \rho_k(x_1, x_2, \ldots, x_n) \quad (k = 1, 2, \ldots, m) \tag{۱۳.۵}$$

هستند. این رابطه‌ها و نتایج آنها کوچکترین زیرگروه نرمال R_0 از F که شامل r_1، r_2، . . . ، r_m می‌باشد، تشکیل می‌دهند. این گروه به

$$R_0 = \{r_1, r_2, \ldots, r_m\}^F$$

نشان داده و **بستار نرمال** r_1، r_2، . . . ، r_m نامیده می‌شود. این گروه دقیقاً زیرگروهی از F است که به‌توسط عناصر $w^{-1}r_k w$، که r_k در r_1، r_2، . . . ، r_m است و w عنصردلخواهی از F، تولید می‌شود. متذکرمی‌شویم که R_0 به‌وسیلهٔ مجموعهٔ (۱۱.۵) و F کاملاً مشخص می‌شود. به‌موجب قضیهٔ اصلی ۱۷، G با F/R یکریخت است که R گروه رابطهٔ G است. چون R مجموعهٔ تمام واژه‌هایی است نظیر $r(x_1, x_2, \quad , x_n)$ به قسمی که $r(g_1, g_2, \quad , g_n) = 1$ یك رابطه در G است. از آنجا نتیجه می‌شود که هرعنصر R_0 به R تعلق دارد، یعنی

$$R_0 \leqslant R \tag{۱۴.۵}$$

دراین مقام گوییم G به‌وسیلهٔ مولدهای g_1، g_2، . . . ، g_n و رابطه‌های (۱۱.۵) تعریف شده‌است، یا به‌طور دقیقتر، گوییم (۱۱.۵) یك **مجموعه از رابطه‌های معرف** برای G است،

هرگاه داشته باشیم

$$R_{\circ} = R \qquad (۱۵.۵)$$

به‌زبان غیررسمی‌تر، شرط (۱۵.۵) حاکی ازاین است‌که شرایط (۱۱.۵) و نتایج آنها متضمن هرگونه اطلاع قابل تصوری در مورد ساختار G هستند مشروط برآنکه از آغاز فرض کنیم‌که G به‌توسط n عنصر تولید شده است. ضمناً ما قید نمی‌کنیم‌که مولدها و یا صورت رابطه‌ها باید غیر زاید باشند. در بیشتر موارد عملی، برای تعریف یك گروه تعداد کمی از رابطه‌ها کفایت می‌کنند. با وجود این جز درمواردی‌که (۱۱.۵) خالی است، بستار نرمال $R_{\circ}$ یك گروه نامتناهی است و متأسفانه محاسبهٔ آن معمولاً دشوار است و ممکن است برای بیان G به‌روشهای غیرمستقیم توسل جست.

حال باید مسئلهٔ وجودی ذیل را مورد بررسی قرار دهیم: هرگاه یك مجموعه از رابطه‌های (۱۱.۵) داده شده باشند، آیا گروهی مانند G با n مولد وجود داردکه به‌ازای آن (۱۱.۵) یك مجموعه از رابطه‌های معرف باشد؟ یك ساختمان ساده نشان می‌دهدکه جواب این‌سؤال مثبت‌است. باشروع از (۱۱.۵) بستار نرمال $R_{\circ}$ را تشکیل وقرار می‌دهیم

$$G_{\circ} = \frac{F}{R_{\circ}} \qquad (۱۶.۵)$$

این‌گروه به‌وسیلهٔ n هممجموعهٔ

$$g_i^{\circ} = x_i R_{\circ} (i = ۱, ۲, \ldots, n)$$

تولید شده‌که درهمهٔ رابطه‌های (۱۱.۵) صدق می‌کنند. در واقع

$$\rho_k(g_۱^{\circ}, g_۲^{\circ}, \ldots, g_n^{\circ}) = \rho_k(x_۱, x_۲, \ldots, x_n) R_{\circ} = r_k R_{\circ} = R_{\circ}$$

زیرا $r_k \in R_{\circ}$. اینك فرض می‌کنیم R همان گروه رابطه‌ای $G_{\circ}$ باشدکه در پایان بخش ۳۲ (صفحهٔ ۱۱۸) تعریف شده است. در این صورت

$$G_{\circ} \cong \frac{F}{R}$$

اگر $r(x_۱, x_۲, \ldots, x_n)$ عنصر دلخواهی از R باشد، چنانچه به‌جای x_i، g_i° $(i = ۱, ۲, \ldots, n)$ گذاشته شود، به‌رابطه‌ای برای $G_{\circ}$ بدل می‌شود و داریم

$$r(g_۱^{\circ}, g_۲^{\circ}, \ldots, g_n^{\circ}) = r(x_۱, x_۲, \ldots, x_n) R_{\circ} = R_{\circ}$$

که ازاین‌نتیجه می‌شود $r \in R_{\circ}$. این بدان‌معنی‌است‌که $R \leqslant R_{\circ}$، ازاین رابطه و (۱۴.۵)، رابطهٔ (۱۵.۵) به‌دست می‌آید. ازاین‌رو (۱۱.۵) یك مجموعه از رابطه‌های معرف برای $G_{\circ}$ است. وقتی که $R_{\circ} = F$، فقط گروه بدیهی در (۱۱.۵) صدق می‌کند.

گروه $G_{\circ}$ که بدین‌گونه ساخته شده است «بزرگترین» یا «آزادترین» گروهی‌است

که در (۱۱.۵) صدق می‌کند. این مطلب به‌وسیلهٔ قضیهٔ اصلی ذیل دقیقتر بیان شده است.

قضیهٔ اصلی ۱۸. فرض کنیم $G=\mathrm{gp}\{g_1, g_2, \ldots, g_n\}$ گروهی با رابطه‌های معرف

$$\rho_k(g_1, g_2, \ldots, g_n)=1_G(k=1, 2, \ldots, m) \qquad (۱۷.۵)$$

باشد و فرض می‌کنیم که $H=\mathrm{gp}\{h_1, h_2, \ldots, h_n\}$ در همین رابطه‌ها

$$\rho_k(h_1, h_2, \ldots, h_n)=1_H(k=1, 2, \ldots, m)$$

و احتمالاً در نسبتهای دیگری که نتیجهٔ آنها نیستند صدق کند، در این صورت H یك نگارهٔ همریخت G براثر نگاشت $\varepsilon: G\rightarrow H$ می‌باشد که با ضابطهٔ

$$g_i\varepsilon=h_i \quad (i=1, 2, \ldots, n)$$

داده شده است.

برهان. چون G و H هردو، n مولد دارند، بر ریختیهایی مانند

$$\theta: F\rightarrow G \qquad \eta: F\rightarrow H$$

با هسته‌های R و S، که به‌ترتیب گروههای رابطه‌ای G و H هستند. وجود دارند. با استفاده ازقرارداد (۱۴.۵) داریم

$$R=R_o$$

زیرا (۱۷.۵) یك مجموعه از رابطه‌های معرف برای G است. فرضی که در مورد H داریم هم‌ارز است با عبارت

$$S\geqslant R_c(=R) \qquad (۱۸.۵)$$

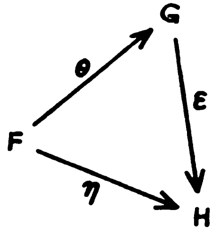
اینك به‌ساختمان نگاشت

$$\varepsilon: G\rightarrow H$$

باز می‌گردیم (شکل ۲ ملاحظه شود). فرض کنیم $u=w(g_1, g_2, \ldots, g_n)$ عنصر دلخواهی از G باشد. چون θ یك بریختی است؛ عنصری مانند z از F نظیر $z=w(x_1, x_2, \ldots, x_n)$ موجود است به‌قسمی که

$$z\theta=u \qquad (۱۹.۵)$$

((۷.۵) را ملاحظه کنید). وقتی که u مفروض باشد کلیترین جواب (۱۹.۵) عبارت است از zr، که r عنصری از R است. زیرا تساوی $z\theta=z'\theta$ **فقط وفقط وقتی** برقرار است که $z^{-1}z'$ متعلق به R باشد. اکنون گوییم که اگر z درمعادلهٔ (۱۹.۵) صدق کند معادلهٔ



شکل ۲

$$u\varepsilon = z\eta \tag{۲۰.۵}$$

یك نگاشت با تعریف کاملاً مشخص از G به روی H را معین می‌کند؛ یعنی، باید تحقیق کنیم که هرگاه zr به‌جای z گذاشته شود، طرف راست (۲۰.۵) تغییر نمی‌کند. اما

$$(zr)\eta = (z\eta)(r\eta) = z\eta$$

زیرا بنابر (۱۸.۵)، $r \in S$ و ازاین‌رو $r\eta = 1_H$. به‌آسانی می‌توان درستی تساوی

$$(u_1\varepsilon)(u_2\varepsilon) = (u_1u_2)\varepsilon,$$

را تحقیق‌کرد و دیدکه ε در واقع یك بریختی است. به‌ویژه، وقتی $u = g_i$، می‌توانیم قرار دهیم $z = x_i$ و پیدا می‌کنیم

$$g_i\varepsilon = x_i\eta = h_i \quad (i = 1, 2, \ldots, n)$$

که روشن است ε را کاملاً مشخص می‌کند. این نشان می‌دهدکه ε یك بریختی است.

آموزنده است که این برهان را درمورد گروهی که قبلاً به‌طور غیررسمی (صفحهٔ ۴۴ و ۴۵) مطالعه‌کرده بودیم دنبال‌کنیم. پس، همچنان‌که در (۲۷.۲) آمده بود، فرض می‌کنیم $G = \mathrm{gp}\{a, c\}$ به‌وسیلهٔ رابطه‌های

$$a^3 = c^2 = (ac)^2 = 1 \tag{۲۱.۵}$$

تعریف شده باشد. از گروه آزاد F با مولدهای x و y استفاده و به سه رابطهٔ مفروض در (۲۱.۵) عناصر

$$r_1 = x^3, \quad r_2 = y^2, \quad r_3 = (xy)^2$$

را وابسته می‌کنیم. فرض کنیم

$$R_0 = \{r_1, r_2, r_3\}^F$$

و $G_0 = F/R_0$. عناصر G_0 عبارت‌اند از هممجموعه‌های wR_0 که $w \in F$، و به‌آسانی می‌توان دیدکه هرهمجموعه برابر یکی ازهمجموعه‌های

$$R_\circ,\ xR_\circ,\ x^\text{۲}R_\circ,\ yR_\circ,\ yxR_\circ,\ yx^\text{۲}R_\circ \qquad (\text{۲۲.۵})$$

است. برای مثال، $xyR_\circ=yx^\text{۲}R_\circ$، زیرا $xy=yx^\text{۲}r$ که در آن

$$r=r_\text{۱}^{-\text{۱}}(xr_\text{۲}^{-\text{۱}}x)r_\text{۳}$$

عنصری از $R_\circ$ است. دراین مرحله نمی‌توانیم بگوییم که شش هممجموعهٔ (۲۲.۵) متمایزند؛ زیرا ممکن است نتایج نهفته‌ای از (۲۱.۵) وجود داشته باشندکه موجب تساوی بین این هممجموعه‌ها شوند. ولی، $|G_\circ|\leqslant \text{۶}$، ومی‌دانیم که هرگاه H گروه دلخواهی با دو مولد باشدکه در (۲۱.۵) صدق کند، آنگاه H یك نگارهٔ همریخت G بوده و لذا $|H|\leqslant|G_\circ|$. اما تصادفاً $H=S_\text{۳}$ واجد این شرایط است. زیرا $S_\text{۳}$ به‌وسیلهٔ

$$\alpha=(\text{۱ ۲ ۳}) \quad \text{و} \quad \gamma=(\text{۱ ۲})$$

تولید می‌شود و

$$\alpha^\text{۳}=\gamma^\text{۲}=(\alpha\gamma)^\text{۲}=\text{۱}$$

چون $|S_\text{۳}|=\text{۶}$، نتیجه می گیریم که $|G_\circ|=\text{۶}$، وبنابراین $G_\circ\cong S_\text{۳}$.

به‌عنوان یك کاربرد بیشتر این مطالب، ما رویهٔ ساختن یك‌گروه آبلی از یك‌گروه G، یعنی گذار از G به G/G' راکه بزرگترین همریخت آبلی G می‌باشد ذکر می‌کنیم. این امر منجر به‌افزوده شدن رابطه‌های

$$g_i^{-\text{۱}}g_j^{-\text{۱}}g_ig_j=\text{۱} \quad (i<j)$$

به رابطه‌های موجود می‌شود. دراین صورت ساختار G/G' را می‌توان مستقیماً به وسیلهٔ روشهای فصل ۴ پیداکرد.

مثال: ساختار G/G' را وقتی G گروه چارتاییهای

$$a^\text{۴}=\text{۱},\quad a^\text{۲}=b^\text{۲},\quad ba=a^\text{۳}b \qquad (\text{۲۳.۵})$$

باشد پیداکنید.

گروه آبلی G/G' به وسیلهٔ $\bar{a}=aG'$ و $\bar{b}=bG'$ تولید می‌شودکه با قرارداد جمعی در رابطه‌های ذیل، که از (۲۳.۵) مشتق شده‌اند، صدق می کنند:

$$\text{۴}\bar{a}=\circ,\quad \text{۲}\bar{a}=\text{۲}\bar{b},\quad \bar{b}+\bar{a}=\text{۳}\bar{a}+\bar{b}$$

این معادلات به

$$\text{۲}\bar{a}+\text{۲}\bar{b}=\circ$$

تبدیل می‌شوند. ماتریس رابطه‌ای متناظر با آن قبلاً به‌صورت قطری بوده است، ازاینجا به‌دست می‌آوریم که

$$\frac{G}{G'} \cong C_2 \oplus C_2$$

لذا اگر گروه آزاد F با x_1، x_2، . . . ، x_n بدین طریق آبلی شود، ملاحظه می‌کنیم که $F/F' = \langle \bar{x}_1, \bar{x}_2, \ldots, \bar{x}_n \rangle$ (صفحهٔ ۹۳ ملاحظه شود)، کـه $\bar{x}_i = x_i F'$. لذا F/F' یك گـروه آبلی آزاد با n مولد است. ضمناً، از این گفته چنین نتیجه می‌شود کـه گروههای آزاد با تعداد مختلفی از مولدها نمی‌توانند یکریخت باشند. زیرا، فرض کنیم F_m و F_n گروههای آزادی به ترتیب با m n مولد بـاشند، و فرض کنیم که اینها یکریخت باشند. پس F_m/F'_m و F_n/F'_n نیز یکریخت‌اند. اما اینها گروههای آبلی آزادی به‌ترتیب بـا m و n مولدند، و می‌دانیم که نمی‌توانند یکریخت باشند مگر آنکه $m = n$ (صفحهٔ ۹۳ ملاحظه شود). بالاخره، ما این قضیهٔ اصلی مهم ولی دشوار: هر زیرگروه از یك گروه آزاد، گروهی است آزاد، را بدون اثبات ذکر می‌کنیم.*

تمرین

(۱) نشان دهید که گروه مشتق از یك گروه آزاد از واژه‌هایی تشکیل می‌شود که در آنهـا مجموع توانها برای هرمولد مساوی صفر است (مثلاً $x_1 x_2^{-1} x_1^{-2} x_2 x_1$).

(۲) ساختار G/G' را در هر یك از حالات ذیل تعیین کنید: (الف) $a^6 = b^2 = (ab)^2 = 1$؛ (ب) $a^6 = 1$؛ (ج) $b^2 = (ab)^2 = a^3$.

(۳) ثابت کنید که اگر G به‌وسیلهٔ a و b مقید به‌رابطه‌های $a^{-1}ba = b^2$، $b^{-1}ab = a^2$ تولید شده باشد، آنگاه $G = \{1\}$.

---

* رجوع کنید به Marshall Hall, Jr., *loc. cit.*, p. 96.

۶

سری زیرگروهها

۳۴. زیرگروههای تو در تو. در ریاضیات مطالعهٔ موجودات پیچیده از راه تجزیهٔ آنها به‌مؤلفه‌های ساده‌تری که «تجزیه‌ناپذیر» باشند عملی متداول است. مثلاً اعداد صحیح به‌حاصلضرب اعداد اول تجزیه می‌شوند، چند جمله‌ایها به‌عوامل تجزیه‌ناپذیر شکسته می‌شوند، وقس‌علیهذا. برای آنکه چنین تجزیه‌ای با معنی باشد باید جنبه‌هایی از یکتایی‌را که به‌ویژگیهای ذاتی ساختار تحت مطالعه (تحقیق) مربوط است نشان دهد.

این روش، در مورد گروهی چون G، شامل بررسی رشته‌های نزولی یا صعودی زیرگروههایی است نظیر

$$A_1 \geqslant A_2 \geqslant \cdots \quad \text{یا} \quad B_1 \leqslant B_2 \leqslant \cdots \tag{۱.۶}$$

با خصوصیات اضافی و مناسب دیگر.

هریک ازاین زیرگروههای تودرتو چنان تعیین شده‌اندکه ساختار G را تا حدی روشن می‌سازند؛ اما، چنانکه معلوم خواهد شد هیچ‌یک G را به‌طورکامل‌مشخص‌نمی‌سازد. دراین‌متن‌ازرشته‌های (۱.۶) به‌عنوان سری زیرگروهها نام برده‌خواهدشد.(باپوزش‌طلبی از آنالیزدانها).

۳۵. قضیهٔ اصلی جوردن ـ هولدر. یادآوری می‌کنیم که یك گروه وقتی‌ساده خوانده می‌شود (صفحهٔ ۶۸)که مرتبهٔ آن بزرگتر از یك و فاقد زیرگروه غیربدیهی نرمال‌باشد. برای گروههای دلخواه، در تعریف ذیل‌نوع مهمی از زیرگروه نرمال تعریف شده است.

تعریف ۶: یك زیرگروه نرمال A $(A \neq G)$ **زیرگروه نرمال ماکسیمال G** خوانده می‌شود هرگاه، بجز G و A، هیچ زیرگروه نرمال دیگری چون H وجود نداشته باشد که

$$G \rhd H \rhd A$$

بنا بر قضیهٔ ۱۰ (صفحهٔ ۷۹)، این تعریف با این حکم که G/A زیرگروه نرمال حقیقی ندارد هم‌ارز است. لذا تعریف فوق را می‌توان مجدداً در قالب زیر مطرح کرد.

ضابطه. یك زیرگروه نرمال A $(A \neq G)$ فقط وفقط وقتی یك زیرگروه نرمال ماکسیمال G است که G/A یك گروه ساده باشد.

ممکن است یك گروه دارای چندین زیرگروه نرمال ماکسیمال باشد که هم در ساختار و هم در مرتبهٔ متفاوت باشند. اگر G/A از مرتبهٔ اول باشد آنگاه A یك زیرگروه نرمال ماکسیمال است. مثال دیگر، اگر G ساده باشد، آنگاه $\{1\}$ تنها زیرگروه نرمال ماکسیمال است.

در مابقی این بخش برای آنکه بحث ساده‌تر شود ما خود را به گروههای متناهی محدود می‌کنیم. نتایج حاصله برای ردهٔ معینی از گروههای نامتناهی نیز برقرار است. (برای مثال مراجعه کنید به کتاب آ. ژ. کوروش: نظریهٔ گروهها، جلد اول، صفحات ۱۱۵ــ۱۱۶.) اما کاربردهای موردنظر ما گروههای متناهی هستند. هرگاه G ساده نباشد، فرض می‌کنیم A_1 یکی از زیرگروههای نرمال ماکسیمال آن باشد، باردیگر، فرض می‌کنیم A_2 یکی از زیرگروههای نرمال ماکسیمال A_1 باشد، فرض می‌کنیم A_3 یکی از زیرگروههای نرمال ماکسیمال A_2 باشد وقس‌علیهذا. چون گروههایی را که تعریف کرده‌ایم ازمرتبه‌های اکیداً نزولی هستند، باید سرانجام به گروه واحد برسیم. لذا به تعریف ذیل هدایت می‌شویم.

تعریف ۷. رشتهٔ زیرگروههای

$$A_1, A_2, \ldots, A_r \qquad (2.6)$$

از یك گروه $G(=A_0)$ **یك سری ترکیبی** G نامیده می‌شود هرگاه

$$G \rhd A_1 \rhd A_2 \rhd \cdots \rhd A_r \rhd \{1\} \qquad (3.6) \quad \text{(الف)}$$

و هرگاه

$$\frac{G}{A_1}, \frac{A_1}{A_2}, \ldots, \frac{A_{r-1}}{A_r}, A_r \qquad (4.6) \quad \text{(ب)}$$

گروههایی ساده باشند.

باید به‌روشنی فهمیده شود که ضمن آنکه A_i در A_{i-1} نرمال، و درواقع نرمال ماکسیمال است، نیازی نیست که درهیچ یك از گروههای پیش از خود در رشتهٔ (۳.۶) نرمال باشد. بویژه، درمیان گروههای (۲.۶) فقط A_1 لزوماً یك زیرگروه نرمال G است. گروههای خارج‌قسمت مذکور در (۲.۶) **گروههای خارج‌قسمت ترکیبی یا عاملهای ترکیبی** نامیده می‌شوند.

چون: در حالت کلی، زیرگروههای نرمال ماکسیمال منحصر به‌فرد نیستند، یك گروه ممکن است دارای بیش از یك سری ترکیبی باشد. ولی، قضیهٔ اصلی بنیادی ذیل حکم می‌کند که عاملهای ترکیبی، در صورت تغییر ترتیب و رعایت یکریختی، منحصر به‌فردند. بنابراین مجموعهٔ عاملهای ترکیبی یك خصوصیت ذاتی از گروه را تشکیل می‌دهد. ما این نتیجه را فقط برای گروههای متناهی اثبات می‌کنیم.

قضیهٔ اصلی ۱۹. (جوردن-هولدر). در هر دو سری ترکیبی از یک گروه متناهی، عاملهای ترکیبی، صرفنظر از توالی آنها، دوبه‌دو یکریخت‌اند.

برهان. ابتدا این حکم را مشروحتر تحلیل می‌کنیم: فرض می‌کنیم

$$G(=A_0) \rhd A_1 \rhd A_2 \rhd \cdots \rhd A_r \rhd \{1\} \qquad (I)$$

و

$$G(=B_0) \rhd B_1 \rhd B_2 \rhd \cdots \rhd B_s \rhd \{1\} \qquad (II)$$

دو سری ترکیبی از G باشند. هرگاه چنین رخ دهد که عاملهای ترکیبی

$$\frac{G}{A_1}, \frac{A_1}{A_2}, \ldots, \frac{A_{r-1}}{A_r}, A_r \qquad (I)'$$

و

$$\frac{G}{B_1}, \frac{B_1}{B_2}, \ldots, \frac{B_{s-1}}{B_s}, B_s \qquad (II)'$$

صرفنظر از تغییر ترتیب، دوبه‌دو یکریخت باشند، می‌نویسیم $(II) \sim (I)$. واضح است که این رابطه یك رابطهٔ هم‌ارزی درمجموعهٔ کلیه سریهای ترکیبی ممکن برقرار می‌کند، و هدف ما این است که نشان دهیم با این تعبیر همهٔ سریهای ترکیبی هم‌ارزند. بویژه، توجه داریم که از $(II) \sim (I)$ نتیجه می‌شود که $r = s$.

وقتی که G ساده باشد، تنها سری ترکیبی ممکن عبارت است از سری

$$G \rhd \{1\}$$

دراین حالت یقیناً سریهای (I) و (II) یکی‌هستند وداریم $r = s = 0$. از این‌رو این‌قضیه برای همهٔ گروههای ساده وبالاخص برای همهٔ گروههای ازمرتبهٔ کوچکتر ازچهار، بالبداهه صادق است.

ما به‌استقراء بر $|G|$ می‌پردازیم و از گروههای ساده صرفنظر می‌کنیم. یعنی، ازاین به‌بعد، فرض می‌کنیم که $1 \leqslant r$ و $1 \leqslant s$. دو حالت باید ازهم تمیز داده شوند.

(الف) $A_1 = B_1$. با حذف جملات اول در (I) و (II) دوسری‌ترکیبی برای A_1 به‌دست می‌آوریم، بدین‌قرار

$$A_1 \rhd A_2 \rhd \cdots \rhd A_r \rhd \{1\}$$

و

$$A_1 \rhd B_2 \rhd \cdots \rhd B_s \rhd \{1\}$$

چون $|G|>|A_1|$، فرض استقراء ایجاب می‌کند که عاملهای ترکیبی

$$\frac{A_1}{A_2}, \frac{A_2}{A_3}, \ldots, \frac{A_{r-1}}{A_r}, A_r$$

و

$$\frac{A_1}{B_1}, \frac{B_2}{B_3}, \ldots, \frac{B_{s-1}}{B_s}, B_s$$

دو به‌دو یکریخت باشند. چون در این حالت جملات اول $(I)'$ و $(II)'$ یکی هستند، داریم $(II)\sim(I)$، و قضیه در این حالت برقرار است.

(ب) $A_1 \neq B_1$. چون داریم $A_1 \rhd G$ و $G \rhd B_1$، پس گروه

$$C = A_1B_1 \quad (= B_1A_1)$$

در G نرمال بوده هم A_1 و هم B_1 را در برمی‌گیرد؛ بویژه

$$G \geqslant C \geqslant A_1$$

اما A_1 یك زیرگروه نرمال ماکسیمال G است. از این‌رو یا $C=G$ ویا $C=A_1$. حالت اخیر بایدکنار گذاشته شود؛ زیرا، چون $B_1 \leqslant C$، پس لازم می‌آیدکه $G>A_1>B_1$، که با این واقعیت که B_1 ماکسیمال است مطابقت ندارد. لذا

$$G = A_1B_1$$

فرض‌کنیم $D=A_1 \cap B_1$. با استفاده ازقضیهٔ اصلی ۱۰ (صفحهٔ ۸۱) چنین‌پیدا می‌کنیم

$$\frac{G}{A_1} \cong \frac{B_1}{D}, \quad \frac{G}{B_1} \cong \frac{A_1}{D} \tag{۵.۶}$$

بنابر شیوهٔ ساخت، G/A_1 و G/B_1 گروههایی ساده‌اند، از این‌رو B_1/D و A_1/D نیز ساده خواهند بود، یعنی D یك زیرگروه نرمال ماکسیمال از هردو گروه A_1 و B_1 است.
فرض کنیم

$$D \rhd D_1 \rhd \cdots \rhd D_t \rhd \{1\}$$

یك سری ترکیبی از D باشد. دراین صورت می‌توانیم دو سری ترکیبی برای G بسازیم، بدین‌قرار

$$G \rhd A_1 \rhd D \rhd D_1 \rhd \cdots \rhd D_t \rhd \{1\} \qquad (III)$$

و

$$G \rhd B_1 \rhd D \rhd D_1 \rhd \cdots \rhd D_t \rhd \{1\} \qquad (IV)$$

در واقع کلیهٔ عاملهای ترکیبی

$$\frac{G}{A_1}, \frac{A_1}{D}, \;\Big|\; \frac{D}{D_1}, \frac{D_1}{D_2}, \ldots, \frac{D_{t-1}}{D_t}, D_t \qquad (III)'$$

و

$$\frac{G}{B_1}, \frac{B_1}{D}, \;\Big|\; \frac{D}{D_1}, \frac{D_1}{D_2}, \ldots, \frac{D_{t-1}}{D_t}, D_t \qquad (IV)'$$

همان گونه که دیده‌ایم، گروههایی ساده‌اند. عاملهای ترکیبی طرف راست خط عمودی در $(III)'$ و $(IV)'$ مشترك‌اند. درحالی که عاملهای سمت چپ، وقتی که دوبه‌دو به‌طورصلیبی، x، مرتب شوندبا هم یکریخت‌اند. لذا $(IV) \sim (III)$. اما (I) و (III) دردوجملهٔ اول باهم‌مطابقت‌دارند واین‌وضعیتی‌است که ما در(الف) بحث کردیم. ازاین‌رو$(III) \sim (I)$. به‌طریق مشابه، $(IV) \sim (II)$. از اینجا نتیجه می گیریم $(II) \sim (I)$، که برهان کامل می‌شود.

این قضیهٔ اصلی را با ذکر دو مثال که نسبتاً پیش پا افتاده‌اند روشن می کنیم، زیرا هنوز گروههای ساده از مرتبهٔ مرکب را ندیده‌ایم (صفحهٔ ۱۵۰ ملاحظه شود).

(۱) فرض کنیم G گروه غیرآبلی مرتبهٔ ۶ (صفحهٔ ۵۲) باشد. این گروه را بوسیلهٔ رابطه‌های

$$a^3 = b^2 = (ab)^2 = 1$$

می توانیم تعریف کنیم. مرتبهٔ زیرگروه $A = \text{gp}\{a\}$ مساوی ۳ و اندیس‌آن در G مساوی ۲ است. از این‌رو $A \lhd G$ (صفحهٔ ۷۵ (د))، و

$$G \rhd A \rhd \{1\}$$

یك سری ترکیبی است، زیرا عاملهای

$$A \cong C_3 \quad \text{و} \quad \frac{G}{A} \cong C_2 \qquad (6.6)$$

از مرتبهٔ اول. و بنابراین ساده‌اند.

(۲) فرض کنیم $G = \text{gp}\{s\}$ گروه دوری مرتبهٔ ۶ باشد. در این صورت $A_2 = \text{gp}\{s^2\}$ یك زیرگروه مرتبهٔ ۳ است، و چون همهٔ زیرگروههای یك گروه آبلی نرمال‌اند، سری ترکیبی

$$G \rhd A_2 \rhd \{1\}$$

را با عاملهای ترکیبی

$$A_۲ \cong C_۳ \quad و \quad \frac{G}{A_۲} \cong C_۲ \qquad (۷.۶)$$

داریم. به‌روش دیگر، می‌توانیم با زیرگروه مرتبهٔ دوم $A_۳ = \mathrm{gp}\{s^۳\}$ شروع کنیم و سری ترکیبی

$$G \rhd A_۳ \rhd \{۱\}$$

را که عاملهای آن

$$A_۳ \cong C_۲ \quad و \quad \frac{G}{A_۳} \cong C_۳$$

همان‌عاملهای (۷.۶) ولی به‌ترتیب معکوس‌اند، بسازیم. ملاحظه می‌کنیم با اینکه گروههای مثالهای (۱) و (۲) هم‌ریخت نیستند عاملهای ترکیبی پدیدآمده یکی‌هستند. در هردوحالت عاملهای ترکیبی ازمرتبهٔ اول هستند. این‌ویژگی ردهٔ خیلی مهمی ازگروهها راکه دربخش آتیه آنها را مطالعه می‌کنیم مشخص خواهدکرد.

۳۶. گروههای حلپذیر

تعریف ۸. یك گروه متناهی را **حلپذیر** نامیم هرگاه کلیهٔ عاملهای ترکیبی آن از مرتبه‌های اول باشند.

برای اظهارنظر دربارهٔ حلپذیر بودن یا حلپذیر نبودن یك گروه مفروض، اغلب قضیه ذیل مفید واقع می‌شود.

قضیهٔ ۱۵. گروه متناهی G فقط و فقط وقتی حلپذیر است که شامل زیرگروه نرمالی چون H باشد به‌قسمی‌که H و G/H حلپذیر باشند.

برهان. اگر این شرایط محقق باشند، سریهای ترکیبی

$$H \rhd H_۱ \rhd \dots \rhd H_r \rhd \{۱\} \qquad (۸.۶)$$

و

$$\frac{G}{H} \rhd \frac{G_۱}{H} \rhd \dots \rhd \frac{G_s}{H} \rhd H \qquad (۹.۶)$$

را خواهیم داشت. (باید متذکر شدکه هر زیرگروه G/H را می‌توان به‌صورت A/H نوشت، که H عنصر واحد G/H است.) بنابر فرض، عاملهای ترکیبی (۸.۶) و (۹.۶) از مراتب اول‌اند و بویژه مرتبهٔ G_s/H عددی است اول. چون بنابر قضیهٔ اصلی ۹ (صفحهٔ ۷۹)

$$\frac{G_{i-1}/H}{G_i/H} \cong \frac{G_{i-1}}{G_i} \qquad (G_0 = G)$$

نتیجه می‌گیریم که

$$G \rhd G_1 \rhd \dots \rhd G_s \rhd H \rhd H_1 \rhd \dots \rhd H_r \rhd \{1\}$$

یک‌سری ترکیبی برای G است که هر عامل ترکیبی آن ازمرتبهٔ اول‌است. لذا G حلپذیر است. سودمندی این نتیجه به‌توسط کاربردهای ذیل نشان داده شده است.

قضیهٔ ۱۶. کلیهٔ گروههای آبلی متناهی حلپذیرند.

برهان. فرض کنیم A یک گروه آبلی متناهی باشد. اگر $|A| = p$ (p عدد اول)، آنگاه سری ترکیبی

$$A \rhd \{1\}$$

حلپذیری A را نشان می‌دهد. اینک از استقراء بر $|A|$ استفاده و فرض می‌کنیم که A از مرتبهٔ مرکبی باشد. دراین‌صورت A دارای یک زیرگروه خاص‌است که لزوماً در A نرمال است (تمرین ۴، فصل ۲ ، صفحهٔ ۶۱). چون H و G/H گروههایی آبلی و از مراتب کوچکتر از $|A|$ هستند، از فرض استقراء نتیجه می‌شود که H و G/H حلپذیرند. لذا بنابرقضیهٔ ۱۵، A حلپذیر است.

قضیهٔ ۱۷. کلیهٔ p-گروههای متناهی حلپذیرند.

برهان. فرض کنیم P یک گروه متناهی باشد به قسمی که $|P| = p^n$، که p عددی است اول. وقتی $n = 1$، این گروه مطمئناً حلپذیر است؛ بنابراین‌می‌توانیم از استقراء نسبت به n استفاده‌کنیم. بنابرقضیهٔ اصلی ۷ (صفحهٔ ۶۶)، مرکز P یعنی Z، غیربدیهی است و البته $Z \lhd P$. حال گوییم Z حلپذیر است زیرا آبلی است، بعلاوه P/Z یک p-گروه است که مرتبهٔ آن کوچکتر از p^n است. از این‌رو P/Z، بنابرفرض استقراء، حلپذیر است؛ و بنابراین به‌موجب قضیهٔ ۱۵، P نیز حلپذیر است.

بالاخره، یکی از مشخصات گروههای حلپذیر را ذکر می‌کنیم که ظاهراً شرایطی ضعیفتر از شرایط تعریف اصلی (صفحهٔ ۱۳۰) را به‌میان می‌آورد.

قضیهٔ ۱۸. گروه متناهی G فقط و فقط وقتی حلپذیر است که دارای زیرگروههایی مانند B_1، B_2، . . . ، B_s باشند چنانکه داشته باشیم

$$G \rhd B_1 \rhd B_2 \rhd \dots \rhd B_s \rhd \{1\} \quad (G = B_0,\ \{1\} = B_{s+1}) \qquad (10.6)$$

و هریک از

$$\frac{B_{i-۱}}{B_i} \qquad (i=۱, ۲, \ldots, s+۱) \tag{۱۱.۶}$$

آبلی باشد.

برهان. اگر G حلپذیر باشد، آنگاه بنابر تعریف ۷ یك سری مانند (۱۰.۶) وجود دارد که در آن $B_{i-۱}/B_i$ ازمرتبهٔ اول و بنابراین آبلی است. بعکس، فرض کنیم (۱۰.۶) و (۱۱.۶) برقرار باشند. می‌توانیم فرض کنیم که هیچ جملهٔ زایدی در (۱۰.۶) وجود ندارد به‌طوری که می‌توان گفت هر گروه یك زیر گروه حقیقی قبل از خودش است. به استقراء بر $|G|$ عمل می‌کنیم. اگر اولین جملهٔ (۱۰.۶) را نادیده بگیریم یك سری برای $B_۱$ به‌دست می‌آوریم که، بنابراستقراء، نتیجه می‌شود $B_۱$ حلپذیر است. باقراردادن $i=۱$ در (۱۱.۶)، می‌بینیم که $G/B_۱$ آبلی و لذا حلپذیر است. از این‌رو، بنابرقضیهٔ ۱۵، G حلپذیر است.

۳۷. سریهای مشتق. گروه مشتق G' از G و بعضی از ویژگیهای آن دربخش **۳۲** معرفی شدند. خاطرنشان می‌سازیم که G' کوچکترین زیرگروه نرمالی است که دارای یك گروه خارج قسمت آبلی است (قضیهٔ اصلی ۱۱). روند تشکیل گروه مشتق می‌تواند تکرار شود. بدین ترتیب رشتهٔ

$$G(=G^{\circ}),\ G',\ G''=(G')',\ \ldots,\ G^{(i)}=(G^{(i-۱)})',\ \ldots$$

را می‌سازیم. چون $G^{(i)} \leqslant G^{(i-۱)}$، می‌توانیم بنویسیم

$$G \geqslant G' \geqslant G'' \geqslant \ldots \geqslant G^{(i)} \geqslant \ldots \tag{۱۲.۶}$$

این سری **سری مشتق** G خوانده می‌شود. هر گروه، در (۱۲.۶)، نه تنها درگروه پیش از خودش نرمال است بلکه یك زیرگروه مشخصه و لذا نرمال خود G نیز می‌باشد (تمرین ۱۴، فصل ۳، ملاحظه شود). این سری ممکن است متوقف شود، یعنی به‌ازای مقداری از i داشته باشیم $G^{(i+۱)}=G^{(i)}$. البته وقتی G متناهی باشد وقوع این‌امر حتمی است. ولی، جالبترین حالت آن است که (۱۲.۶) به گروه واحد ختم‌شود، زیرا این‌حالت بیان دیگری از گروههای حلپذیر را به‌دست می‌دهد.

قضیهٔ اصلی ۲۰. گروه متناهی G فقط و فقط وقتی حلپذیر است که سری مشتق آن به‌گروه واحد ختم شود، یعنی به‌ازای عدد صحیحی نامنفی مانند s، $G^{(s)}=\{۱\}$.

برهان. (الف) فرض کنیم که $G^{(s)}=\{۱\}$، به‌طوری که سری

$$G > G' > \ldots > G^{(s-۱)} > \{۱\} \tag{۱۳.۶}$$

سری مشتق باشد. بنابرقضیهٔ اصلی ۱۱، $G^{(i-۱)}/G^{(i)}$ آبلی است. از این‌رو (۱۳.۶) از نوع سریهایی است که در قضیهٔ ۱۸ بررسی شده است. از اینجا نتیجه می‌شود که G حلپذیر است.

(ب) فرض کنیم که G حلپذیر باشد، از این‌رو دارای یك رشته زیرگروه است که در (۱۰.۶) و (۱۱.۶) صدق می‌کنند. ما ادعا می‌کنیم که

$$G^{(i)} \leqslant B_i \quad (i=1,2,\cdots) \tag{۱۴.۶}$$

زیرا چون G/B_1 آبلی است، از قضیهٔ اصلی ۱۱ نتیجه می‌گیریم که $G' \leqslant B_1$. اکنون به‌استقراء فرض می‌کنیم که $G^{(i-1)} \leqslant B_{i-1}$. ازخود تعریف یك گروه مشتق روشن است که هرگاه $K \leqslant L$، آنگاه $K' \leqslant L'$. از این‌رو

$$G^{(i)} = (G^{(i-1)})' \leqslant B'_{i-1}$$

چون B_{i-1}/B_i آبلی است، با یکبار دیگر استناد به‌قضیهٔ اصلی ۱۱، نتیجه می‌گیریم که $B'_{i-1} \leqslant B_i$، از اینجا نتیجه می‌شود $G^{(i)} \leqslant B_i$. این‌رابطهٔ (۱۴.۶) را ثابت می‌کند. وقتی i برابر $s+1$ باشد، این نتیجه به‌صورت

$$G^{(s+1)} \leqslant B_{s+1} = \{1\}$$

در می‌آید. لذا سری مشتق به‌گروه واحد ختم می‌شود.

۳۸. گروههای پوچتوان. دراین‌بخش رده‌ای از گروهها راکه ساختارشان بعد از ساختار گروههای آبلی، بیش از همه پاسخگوی مسائل آنالیز است، معرفی خواهیم‌کرد. از راه تعمیم مفهوم تعویضگر، کــه در بخش **۲۳** (صفحهٔ ۸۳) تعریف کـردیم، مطلب را شروع می‌کنیم. متناظر با هردوزیرمجموعهٔ A ، B از G می‌توانیم زیرگروه

$$[A,B] = \mathrm{gp}\,\{[a,b] \mid a \in A,\ b \in B\} \tag{۱۵.۶}$$

را تشکیل دهیم. چون داریم

$$[a,b]^{-1} = (a^{-1}b^{-1}ab)^{-1} = b^{-1}a^{-1}ba = [b,a]$$

از آنجا نتیجه می‌شود که

$$[A,B] = [B,A] \tag{۱۶.۶}$$

زیرا عکس کردن هر مولد در (۱۵.۶) گروه حاصله را تغییرنمی‌دهد. بدیهی‌است که، اگر $B \leqslant C$، آنگاه $[A,B] \leqslant [A,C]$.

بدیك گروه دلخواه G یك‌رشته زیرگروه مربوط می‌کنیم که به‌طریق‌استقراء به‌گونهٔ زیر تعریف می‌شوند:

$$\Gamma_1 = G,\ \Gamma_2 = [G,G] = G',\ \ldots,\ \Gamma_{k+1} = [\Gamma_k, G] \tag{۱۷.۶}$$

حال‌نشان می‌دهیم که $\Gamma_{k+1} \leqslant \Gamma_k$ $(k = 1, 2, \ldots)$. وقتی‌که $k=1$، این‌امر بدیهی‌است. با فرض $\Gamma_k \leqslant \Gamma_{k-1}$ $(k>1)$، نتیجه می‌گیریم که

$$\Gamma_{k+1}=[\Gamma_k, G]\leqslant[\Gamma_{k-1}, G]=\Gamma_k$$

لذا (۱۷.۶) درواقع یك سری نزولی است

$$G=\Gamma_1\geqslant\Gamma_2\geqslant\cdots\geqslant\Gamma_k\geqslant\Gamma_{k+1}\geqslant\cdots \qquad (۱۸.۶)$$

هر Γ_k یك زیرگروه مشخصهٔ G است، یعنی، اگر α یك خودریختی G باشد، آنگاه $\Gamma_k\alpha=\Gamma_k$ (صفحهٔ ۸۷، (۵۰.۳) ملاحظه شود). زیرا، چون $\alpha: G\to G$ یك همریختی است، داریم $[a, b]\alpha=[a\alpha, b\alpha]$ و از این‌رو $[A, B]\alpha=[A\alpha, B\alpha]$. اما $G\alpha=G$ و $\Gamma_{k+1}\alpha=[\Gamma_k\alpha, G]$. اگر نشان داده باشیم که $\Gamma_k\alpha=\Gamma_k$، که در صورت $k=1$ بدیهی است، نتیجه می‌شود که

$$\Gamma_{k+1}\alpha=[\Gamma_k, G]=\Gamma_{k+1}$$

که تساوی زیر را ثابت می کند

$$\Gamma_k\alpha=\Gamma_k(k=1, 2, 3, \ldots)$$

درنتیجه $G \rhd \Gamma_k$، $(k=1, 2, 3, \ldots)$، و به‌طریق اولی $\Gamma_k \rhd \Gamma_{k+1}$. یك ویژگی که وضوح آن از (۱۸.۶) کمتر است درقضیهٔ ذیل بیان شده است.

قضیهٔ ۱۹. گروه خارج‌قسمت Γ_k/Γ_{k+1} درمرکز G/Γ_{k+1}، $(k=1, 2, \ldots)$ قرارداداد.

برهان. فرض کنیم $\nu: G\to\Gamma_{k+1}$ نگاشت طبیعی G به‌روی G/Γ_{k+1} باشد، یعنی مثلاً $\bar{x}=x\Gamma_{k+1}=x\nu$ که $x\in G$. هستهٔ ν برابر است با Γ_{k+1}. یك عنصر نوعی از Γ_k/Γ_{k+1} به‌وسیلهٔ $\bar{u}=u\Gamma_{k+1}$ داده می‌شود که در آن u عنصری‌دلخواه از Γ_k است. باید نشان دهیم که $\bar{u}$ و $\bar{x}$ به‌ازای جمیع مقادیر x تعویضپذیرند، یعنی باید ثابت کنیم که $[\bar{u}, \bar{x}]=\bar{1}$، که $\bar{1}(=\Gamma_{k+1})$ عنصر واحد G/Γ_{k+1} می‌باشد. اما

$$[\bar{u}, \bar{x}]=[u\nu, x\nu]=[u, x]\nu$$

بنا بر تعریف Γ_{k+1}، داریم $[u, x]\in\Gamma_{k+1}$. لذا $[u, x]\nu=\bar{1}$، که ادعای مارا ثابت‌می‌کند.

در قسمت بعد یك‌سری‌صعودی برای یك گروه دلخواه G را تعریف‌می کنیم. ساختمان این سری بر اساس مطلب زیر صورت گرفته است.

لم. فرض کنیم U یك زیرگروه مشخصهٔ G و V/U مرکز G/U باشد. دراین صورت V یك زیرگروه مشخصهٔ G است.

برهان. گروه V را می‌توان به‌صورت بزرگترین زیرگروه G که با G «به هنگ U» تعویضپذیر است توصیف کرد، یعنی

$$[V, G]\leqslant U$$

در واقع، اگر از نگاشت طبیعی $\mu: G\to G/U$، که U را «بی‌اثر می کند» استفاده کنیم، این رابطه چنین می‌شود

$$[V\mu,\, G\mu]=\{\bar{1}\}$$

که در آن $\bar{1}$ عنصر واحد G/U است؛ این بدان معنی است که هرعنصر $V/U\ (=V\mu)$ با عنصر $G/U\ (=G\mu)$ تعویضپذیر است. اکنون فرض می‌کنیم که α یك خودریختی G باشد. پس $[V\alpha,\, G]\leqslant U\alpha$. بنابر فرض داریم $U\alpha=U$ و بنابراین $[V\alpha,\, G]\leqslant U$. از این‌رو به‌موجب ماکسیمال بودن V داریم $V\alpha\subset V$. اگر به عوض α، از خودریختی α^{-1} استفاده کنیم، به‌طریق مشابه نتیجه می‌گیریم که $V\alpha^{-1}\subset V$، یعنی $V\subset V\alpha$، و از آنجا نتیجه می‌شود که $V\alpha=V$. بدین طریق V یك زیرگروه مشخصه است.

اکنون قرار می‌دهیم $Z_0=\{1\}$، و فرض می‌کنیم Z_1 مرکز G باشد. چون Z_1 یك زیرگروه مشخصه‌است، از لم فوق‌الذکر نتیجه می‌گیریم که یك زیرگروه مشخصهٔ Z_2 وجود دارد به‌قسمی که Z_2/Z_1 مرکز G/Z_1 است. با عمل به‌استقراء، Z_{j+1} را با این ویژگی تعریف می‌کنیم که Z_{j+1}/Z_j مرکز G/Z_j باشد. بدین‌گونه یك سری صعودی از زیرگروههای مشخصه ساخته‌ایم:

$$\{1\}=Z_0\leqslant Z_1\leqslant\cdots\leqslant Z_j\leqslant\cdots \tag{۱۹.۶}$$

همچنان‌که متذکر شدیم، سریهای (۱۸.۶) و (۱۹.۶) برای هر گروه G وجود دارند، اما اگر تساوی $G=G'\,(=\Gamma_2)$ ویا $Z_1=\{1\}$ به‌ترتیب برقرار باشد، آنگاه ممکن‌است که این سریها درجملهٔ اول مستهلك شوند. ما بیشتر به‌حالت عکس آن علاقه‌مندیم که در آن این سریها حد اعلای طول خود را پیدا می‌کنند و از خودگروه G شروع و تا گروه واحد $\{1\}$ کشیده می‌شوند.

تعریف ۹. (الف) گوییم‌گروه G دارای **یك سری مرکزی زیرین** به‌طول r است هرگاه

$$G=\Gamma_1>\Gamma_2>\cdots>\Gamma_k>\cdots>\Gamma_r>\Gamma_{r+1}=\{1\} \tag{۲۰.۶}$$

که $\Gamma_{k+1}=[\Gamma_k,\, G]$ $\quad(k=1,\, 2,\, \ldots,\, r)$

(ب) گوییم گروه G دارای **یك سری مرکزی زبرین** به‌طول s است هرگاه

$$\{1\}=Z_0<Z_1<\cdots<Z_j<\cdots<Z_s=G \tag{۲۱.۶}$$

که Z_j/Z_{j-1} مرکز G/Z_{j-1} است $(j=1,\, 2,\, \ldots,\, s)$.

همچنان‌که درلم بالا داشتیم، می‌توان Z_j را به‌عنوان زیرگروهی با ویژگی

$$[Z_j,\, G]\leqslant Z_{j-1} \tag{۲۲.۶}$$

از G توصیف کرد.

بین جملات این دوسری مرکزی چند رابطهٔ قابل توجه وجود دارد. در واقع، خواهیم دیدکه اگر یکی‌از دوسری وجود داشته باشد دیگری نیز وجود دارد، و هر دو سری طول واحدی دارند.

ابتدا فرض می‌کنیم که G دارای یك سری مرکزی زیرین به‌طول r باشد به‌طوری که (۲۰.۶) برقرار باشد، وسری (۱۹.۶) را برای این گروه درنظر می‌گیریم. می‌گوییم

$$\Gamma_{r+1-i} \leqslant Z_i \quad (i=0, 1, \ldots, r) \tag{۲۳.۶}$$

بدیهی است که وقتی $i=0$، این نامساوی برقرار است. زیـرا چنین فرض شده است کـه $Z_0=\{1\}=\Gamma_{r+1}$. حال از این فرض استقرایی که (۲۳.۶) به‌ازای یك مقدار خاص i برقـرار است استفاده وثابت می‌کنیم کـه $\Gamma_{r-i} \leqslant Z_{i+1}$. چـون $\Gamma_{r+1-i}=[\Gamma_{r-1}, G]$ فرض ما بیان می‌دارد که $[\Gamma_{r-1}, G] \leqslant Z_i$. بنابر (۲۲.۶)، Z_{i+1} بزرگترین زیرگروهی است که $[Z_{i+1}, G] \leqslant Z_i$. از آنجا نتیجه می‌شود که $\Gamma_{r-i} \leqslant Z_{i+1}$، ولذا (۲۳.۶) برای کلیهٔ مقادیر i اثبات شده است. بویژه، وقتی که $i=r$، ملاحظه می‌کنیم که $\Gamma_1=G \leqslant Z_r$. این بدین معنی است کـه $Z_r=G$. از این‌رو (۱۹.۶) بعد از حداکثر r مرحله به G ختم می‌شود، یعنی G دارای یك سری مرکزی زبرین است که طول آن، s، در رابطهٔ

$$s \leqslant r \tag{۲۴.۶}$$

صدق می‌کند. در مرحلهٔ دوم فرض می‌کنیم که (۲۱.۶) برای G بـرقرار بـاشد و سری (۱۸.۶) را برای این گروه مورد بررسی قرار می‌دهیم. اینك گوییم که

$$\Gamma_i \leqslant Z_{s+1-i} \quad (i=1, 2, \ldots, s+1) \tag{۲۵.۶}$$

این نامساوی هنگامی که $i=1$، برقرار است زیرا فرض کرده‌ایم کـه $Z_s=G=\Gamma_1$. با عمل استقراء فرض می‌کنیم که (۲۵.۶) به‌ازای مقدار خاصی از i برقـرار باشد و نشان خواهیم داد که $\Gamma_{i+1} \leqslant Z_{s-i}$. در واقع، داریم

$$\Gamma_{i+1}=[\Gamma_i, G] \leqslant [Z_{s+1-i}, G] \leqslant Z_{s-i}$$

که همان چیزی است که می‌خواستیم. در (۲۵.۶)، قرار می‌دهیم $i=s+1$ و مـلاحظه می‌کنیم که $\Gamma_{s+1} \leqslant Z_0=\{1\}$؛ یعنی $\Gamma_{s+1}=\{1\}$. لذا بعد از حداکثر $s+1$ مرحلـه، (۱۸.۶) به $\{1\}$ ختـم می‌شود. این مطلب ثابت می‌کند کـه G دارای یك سری مـرکزی زیرین است کـه طول آن، r، در نامساوی $r \leqslant s$ صدق می‌کند؛ و این همراه با (۲۴.۶) نشان می‌دهد که $s=r$.

این بررسیها سرانجام ما را قادر می‌سازد که تعریف آن رده ازگروهها راکـه در عنوان این بخش ذکر شده بودند صورتبندی می‌کنیم.

تعریف ۱۰. گروه G را **پوچتوان** خوانیم هـرگاه یك سری مرکزی زیرین و یا، هم‌ارز با آن، یك سری مـرکزی زبرین داشته باشد. طـول مشترك این سریها ردهٔ پـوچتوانی G نامیده می‌شود.

مثال ۱. اگر A یك گروه آبلی از مرتبهٔ بزرگتر از یك باشد، آنگاه سری مرکزی زبرین آن به

$$\{1\} = Z_0 < Z_1 = A$$

بدل می‌شود. بدین ترتیب، مجموعهٔ گروههای آبلی ($\neq \{1\}$) با مجموعهٔ گروههای پوچتوان از ردهٔ یك، یکی است.

مثال ۲. p-گروههای متناهی پوچتوان هستند. اگر P یك p-گروه متناهی باشد، آنگاه بنابر قضیهٔ اصلی ۷ (صفحهٔ ۶۶) مرکز آن، Z_1، دارای مرتبه‌ای بزرگتر از یك است. حال گوییم P/Z_1 نیز یك p-گروه است و بنابراین مرکز آن Z_2/Z_1 غیر بدیهی است، یعنی $Z_1 < Z_2$. مشابهاً P/Z_2 دارای یك مرکز Z_3/Z_2 است که در آن $Z_2 < Z_3$. اگر به‌همین روش ادامه دهیم یك سری اکیداً صعودی به‌صورت

$$\{1\} = Z_0 < Z_1 < Z_2 < Z_3 < \cdots$$

می‌سازیم.

چون P متناهی است، این سری باید به‌جمله‌ای ختم شود. این امر مثلاً وقتی $Z_r = P$، اتفاق می‌افتد. لذا P دارای یك سری مرکزی زبرین و بنابراین پوچتوان است. ازمیان نتایج بسیار در باب گروههای پوچتوان، یك واقعیت جالب را انتخاب کرده‌ایم که در پایان این کتاب مجدداً به‌آن اشاره خواهیم کرد.

قضیهٔ ۲۵. اگر H یك زیرگروه خاص ازیك گروه پوچتوان G باشد، آنگاه نرمالساز H، یعنی $N(H)$، اکیداً از H بزرگتر است.

برهان. فرض کنیم G یك گروه پوچتوان از ردهٔ r باشد. بدیهی است که $Z_0 = \{1\} \leqslant H$. از سوی دیگر، چون H یك زیرگروه خاص است $G = Z_r \nleqslant H$. از این‌رو عدد صحیح منحصر به‌فردی مانند k وجود دارد که $0 \leqslant k \leqslant r-1$ و

$$Z_k \leqslant H, \; Z_{k+1} \nleqslant H \qquad (۲۶.۶)$$

لذا عنصری‌مانند u هست که $u \in Z_{k+1}$ و $u \notin H$. کافی‌است‌نشان‌دهیم که $u \in N(H)$، یعنی

$$u^{-1}Hu = H \qquad (۲۷.۶)$$

فرض کنیم h_1 عنصر دلخواهی از H باشد. لذا بنابر (۲۲.۶) و (۲۶.۶) داریم

$$[u, h_1] \in [Z_{k+1}, G] = Z_k \leqslant H$$

این بدین معنی‌است که داریم $u^{-1}h_1^{-1}uh_1 = h_2$، که $h_2 \in H$. ازاین‌رو $u^{-1}h_1^{-1}u \in H$. چون h_1 یا h_1^{-1} همهٔ مقادیر H را اختیار می‌کند، پس نشان داده‌ایم که $u^{-1}Hu \subset H$. با استفاده از همین برهان، وقتی که به‌جای u، u^{-1} گذاشته شود، نتیجه می‌گیریم که

$H\subset u^{-1}Hu$ یعنی $uHu^{-1}\subset H$. این رابطهٔ (۲۷.۶) را اثبات می‌کند.

تمرین

(۱) یک‌سری ترکیبی (الف) برای گروه دو وجهی مرتبهٔ ۸ (صفحهٔ ۵۷ ، جدول(xi)) و (ب) گروه چارتاییها (صفحهٔ ۵۷ ، جدول xii) پیدا کنید. درهر حالت عاملهای ترکیبی را تعیین نمایید.

(۲) ثابت کنید که هر زیرگروه و گروه خارج قسمت یک گروه حلپذیر، حلپذیر است.

(۳) تحقیق کنید که هرگاه x، y، z عناصری از یک گروه باشند، داریم

(الف) $[xy, z]=[x, z]^{y}[y, z]$

(ب) $[x, yz]=[x, z][x, y]^{z}$

که درآن $a^{t}=t^{-1}at$.

(۴) نشان دهید اگر G یک گروه پوچتوان از ردهٔ ۲ باشد، آنگاه G' در مرکز G واقع است و برای چنین گروهی اتحادهای

$$[xy, z]=[x, z][y, z],\ [x, yz]=[x, z][x, y]$$

را نتیجه بگیرید.

(۵) ثابت کنید هر زیر گروه و گروه خارج قسمت یک گروه پوچتوان، پوچتوان است.

(۶) فرض کنیم G پوچتوان و از ردهٔ ۳ باشد. نشان دهید، اگر $y\in G'$ و $x\in G$، آنگاه $x^{y}=cx$، که درآن $c\in Z$ و Z مرکز G است. نتیجه بگیرید که G' آبلی است.

(۷) ثابت کنید اگر M یک زیرگروه ماکسیمال از یک گروه پوچتوان G باشد، آنگاه $M\lhd G$ و $|G/M|=p$، که p عددی است اول. [یک زیر گروه ماکسیمال، یک زیرگروه خاص است که درهیچ زیرگروه خاص دیگری قرار ندارد. احتیاجی نیست که گروههای نامتناهی گروههای ماکسیمال داشته باشند.]

(۸) فرض کنیم $D(2^{n})$ گروه دو وجهی مرتبهٔ 2^{n+1} باشد (فصل ۲ ، تمرین ۷، صفحهٔ ۶۱) که با رابطهٔ

$$a^{2^{n}}=b^{2}=(ab)^{2}=1$$

داده‌شده‌است. ثابت کنید اگر Z_1 مرکز $D(2^{n})$ باشد، آنگاه $D(2^{n})/Z_1\cong D(2^{n-1})$؛ نتیجه بگیرید که $D(2^{n})$ پوچتوان و از ردهٔ n است.

۷

گروههای جایگشتی

۳۹. رده‌های مزدوج S_n: در بخش ۷ (صفحات ۲۳ـ۲۹) خانوادهٔ گروههای متقارن S_n ($n = ۱, ۲, \ldots$) را معرفی کردیم و بعضی از ویژگیهای مقدماتی آنها را برشمردیم. فصل حاضر، به‌مطالعهٔ مفصلتر این گروهها، که با زیرگروههایشان نقشی اساسی در نظریهٔ گروههای متناهی دارند، اختصاص یافته است.

در این بخش مسئلهٔ تجزیهٔ S_n به‌رده‌های مزدوج را موردبررسی قرارمی‌دهیم (بخش ۱۷ ملاحظه شود). برای این منظور به‌روشی احتیاج داریم تا حاصلضرب $\tau^{-1}\alpha\tau$ را، که درآن α و τ عناصر دلخواهی از S_n اند، حساب کنیم. با استفاده از نمادهای (۴۳.۱) (صفحهٔ ۲۳) فرض می‌کنیم

$$\alpha = \begin{pmatrix} ۱ & ۲ \ldots n \\ a_۱ & a_۲ \ldots a_n \end{pmatrix} \qquad (۱.۷)$$

این نماد را به‌صورت اختصاری

$$\alpha = \begin{pmatrix} i \\ a_i \end{pmatrix} \qquad (۲.۷)$$

می‌نویسیم که درآن $i = ۱, ۲, \ldots, n$. به‌منظور ساده‌سازی بیشتر این نمادها قرارمی‌دهیم

$$\tau=\begin{pmatrix}۱ & ۲\cdots n\\ ۱' & ۲'\cdots n'\end{pmatrix}=\begin{pmatrix}i\\ i'\end{pmatrix}\qquad (۳.۷)$$

که در آن $۱'۲'۳'\ldots n'$ ترتیبی از $۱\ ۲\ ۳\ldots n$ متناظر با τ هستند. همچنان که درصفحهٔ ۲۳ یادآوری کردیم، ممکن است ترتیبات اعداد قرارگرفته در τ همچنین، به صورتی غیراستانده عرضه شوند، و بویژه بتوانیم بنویسیم

$$\tau=\begin{pmatrix}a_i\\ a_i'\end{pmatrix}\qquad (۴.۷)$$

که سطر اول (۴.۷) همان سطر دوم (۱.۷) است. اما داریم

$$\tau^{-۱}\alpha\tau=\begin{pmatrix}i'\\ i\end{pmatrix}\begin{pmatrix}i\\ a_i\end{pmatrix}\begin{pmatrix}a_i\\ a_i'\end{pmatrix}=\begin{pmatrix}i'\\ a_i'\end{pmatrix}$$

این نتیجه را می‌توان چنین بیان کرد: برای به‌دست‌آوردن $\tau^{-۱}\alpha\tau$، نتیجهٔ اثر τ را برعبارت α یعنی بردوسطر (۱.۷) به‌دست می‌آوریم. لذا

$$\tau^{-۱}\alpha\tau=\begin{pmatrix}i\tau\\ a_i\tau\end{pmatrix}\qquad (۵.۷)$$

مثال. فرض‌کنیم $n=۴$ و

$$\alpha=\begin{pmatrix}۱&۲&۳&۴\\ ۲&۴&۱&۳\end{pmatrix},\ \tau=\begin{pmatrix}۱&۲&۳&۴\\ ۱&۴&۲&۳\end{pmatrix}$$

با اعمال τ بر هرنماد α ملاحظه می‌کنیم که

$$\tau^{-۱}\alpha\tau=\begin{pmatrix}۱&۴&۲&۳\\ ۴&۳&۱&۲\end{pmatrix}=\begin{pmatrix}۱&۲&۳&۴\\ ۴&۱&۲&۳\end{pmatrix}$$

بعد، این روش را برای یك دوره از درجهٔ m، مانند

$$\gamma=(a_۱a_۲\cdots a_m)=\begin{pmatrix}a_۱ & a_۲\cdots a_{m-۱} & a_m\\ a_۲ & a_۳\cdots a_m & a_۱\end{pmatrix}$$

به‌کار می‌بریم. در این صورت بنابر (۵.۷) داریم

$$\tau^{-۱}\gamma\tau=\begin{pmatrix}a_۱' & a_۲'\cdots a'_{m-۱} & a_m'\\ a_۲' & a_۳'\cdots a_m' & a_۱'\end{pmatrix}=(a_۱'a_۲'\cdots a'_m)$$

یا به‌طور خلاصه‌تر

$$\tau^{-1}\gamma\tau=(\alpha_1\tau,\ \alpha_2\tau,\ \ldots,\ a_m\tau) \qquad (۶.۷)$$

چنانکه دیده‌ایم (قضیهٔ اصلی ۲، صفحهٔ **۲۸**) هرجـایگشت α را می‌توان به‌روشی اساساً یکتا به‌صورت حاصلضربی از دورهای ازهم جدا نوشت، از این‌رو داریم

$$\alpha=\gamma_1\gamma_2\cdots\gamma_r \qquad (۷.۷)$$

که در آن γ_1، γ_2، . . .، γ_r دورهایی ازهم جدا هستند که بترتیب شامل

$$m_1,\ m_2,\ \ldots,\ m_r \qquad (۸.۷)$$

شیء می‌باشند.

برای بحث حاضر مناسب آن است که دورهای به‌طول واحد را نگهداریم به‌طوری که همگی n شیء در حاصلضرب (۷.۷) ثبت شوند. اعداد صحیح (۸.۷) **قالب دوری** α خوانده‌می‌شوند. مناسب آن‌است که اعداد (۸.۷)را به‌ترتیب صعودی اندازه‌هایشان مرتب کنیم. لذا کلیهٔ قالبهای دوری‌ممکن S_n، بامجموعه‌های اعداد (۸.۷) درتناظریك‌به‌یك هستند که این اعداد در

$$1\leqslant m_1\leqslant m_2\leqslant\cdots\leqslant m_r$$

و در

$$m_1+m_2+\cdots+m_r=n \qquad (۹.۷)$$

صدق می‌کنند، کـه r عددی است دلخواه. به‌عبارت دیگر، اگر α شامل e_1 دور از درجهٔ ۱ و e_2 دور از درجهٔ ۲، . . .، و e_n دور از درجهٔ n بـاشد، قالب دوری α را می‌توان به‌وسیلهٔ اعداد صحیح نامنفی

$$e_1,\ e_2,\ \ldots,\ e_n$$

بیان‌کرد که در تساوی

$$e_1+2e_2+\cdots+ne_n=n \qquad (۱۰.۷)$$

صدق می‌کنند.

قضیهٔ آتیه قالبهای دوری را با رده‌های مزدوج مربوط می‌سازد.

قضیهٔ ۲۱. دو جایگشت فقط وفقط وقتی در S_n مزدوج‌اندکـه دارای قالبهای دوری واحدی باشند.

برهان. فرض‌کنیم α به‌دورهای ازهم‌جدا تجزیه شده باشد، لذا

$$\alpha=\gamma_1\gamma_2\cdots\gamma_r=(x_1x_2\cdots)(y_1y_2\cdots)\cdots(w_1w_2\cdots)$$

که در آن γ_i از درجهٔ m_i است و

$$m_1+m_2+\cdots+m_r=n$$

اگر τ جایگشتی دلخواه باشد، همچنانکه در (۳.۷) نشان داده شده است، آنگاه

$$\beta=\tau^{-1}\alpha\tau=(\tau^{-1}\gamma_1\tau)(\tau^{-1}\gamma_2\tau)\cdots(\tau^{-1}\gamma_r\tau)$$
$$=(x_1'x_2'\cdots)\ (y_1'y_2'\cdots)\cdots(w_1'w_2'\cdots)=\gamma_1'\gamma_2'\cdots\gamma_r'$$

که در آن γ_1'، γ_2'، ...، γ_r' دورهایی ازهمجدایند، زیرا τ نگاشتی یک‌به‌یک است. ازاین‌رو β دارای همان قالب دوری است که α دارا می‌باشد.

بعکس، اگر، همچنانکه فوقاً آمده α و β دارای قالبهای دوری واحدی باشند، جایگشت

$$\tau=\begin{pmatrix}x_1 & x_2,\cdots,y_1 & y_2,\cdots,w_1 & w_2,\cdots\\ x_1' & x_2',\cdots,y_1' & y_2',\cdots,w_1' & w_2',\cdots\end{pmatrix}$$

دارای این ویژگی است که $\tau^{-1}\alpha\tau=\beta$، به‌طوری‌که α و β مزدوج هستند.

ازاین‌رو، به‌تعداد قالبهای دوری ممکن رده‌های مزدوج در S_n وجود دارد؛ به‌بیان دیگر، عدهٔ رده‌های مزدوج S_n، k، برابر است با تعداد افرازهای n درجمعیده‌های مثبت (۹.۷) یا تعداد افرازهای n در جمعیده‌های نامنفی (۱۰.۷). وقتی‌که از تعبیر اخیر (افرازهای به‌صورت (۱۰.۷)) استفاده شود، اغلب افراز مربوط به‌وسیلهٔ

$$1^{e_1}2^{e_2}\cdots n^{e_n} \tag{۱۱.۷}$$

نشان داده می‌شود، معمولاً در مثالهای واقعی‌مؤلفه‌های با نماینده‌های صفر حذف می‌شوند؛ برای مثال

$$1^3\quad 3\quad 4^2$$

عبارت‌است از افراز عدد ۱۴ به‌صورت ۴+۴+۳+۱+۱+۱. متأسفانه هیچ‌فرمول ساده‌ای‌که عدد رده‌ای k را به‌صورت تابعی‌از n بیان‌نماید وجود ندارد. جدول ذیل‌مقدار k را برای چند مقدار اولیهٔ n به‌دست می‌دهد

جدول (xiii)

n	۱	۲	۳	۴	۵	۶	۷	۸
k	۱	۲	۳	۵	۷	۱۱	۱۵	۲۲

برای مثال، وقتی‌که $n=5$، افرازهای (۱۱.۷) عبارت‌اند از

$$1^5,\ 1^3\ 2,\ 1^2\ 3,\ 1\ 2^2,\ 1\ 4,\ 2\ 3,\ 5$$

از طرف دیگر، به‌آسانی می‌توان گفت که چه تعداد از عناصر در یك ردهٔ مزدوج خاص S_n قرار دارد.

قضیهٔ ۲۲ (کوشی). فرض کنیم α دارای یك قالب دوری متناظر با افراز $1^{e_1}2^{e_2}\ldots n^{e_n}$ باشد. دراین صورت تعداد جایگشتهایی از S_n که با α مزدوج‌اند برابر است با

$$h_\alpha=\frac{n!}{1^{e_1}e_1!\,2^{e_2}e_2!\ldots n^{e_n}e_n!} \tag{۱۲.۷}$$

برهان. قالب دوری α را می‌توان به‌وسیلهٔ دیاگرام

$$\underbrace{(\cdot)(\cdot)\ldots(\cdot)}_{e_1}\quad\underbrace{(\cdot\,\cdot)(\cdot\,\cdot)\ldots(\cdot\,\cdot)}_{e_2}\ \ldots \tag{۱۳.۷}$$

که متناظر با افراز (۱۱.۷) است نشان داد.

در (۱۳.۷) دقیقاً n جای خالی وجود دارد و به‌وسیلهٔ پرکردن آنها با n شیء به‌هر طریق، عنصری از S_n را به‌دست می‌آوریم. در هرحال یك جایگشت به‌دست می‌آوریم که دارای همان قالب دوری α است. تعداد $n!$ راه برای ترتیبات این n شیء وجود دارد، اما چنین نیست که کلیهٔ این ترتیبات، عناصر متمایزی از S_n باشند. e_j دور از درجهٔ j را که در (۱۳.۷) ظاهر می‌شوند در نظر می‌گیریم $(1\leqslant j\leqslant n)$. قبل از همه، این e_j دوره درمیان خود به $e_j!$ طریق می‌توانند تعویض شوند، بی‌آنکه درعنصر حاصله در S_n تغییری رخ دهد؛ بعداً هر دور

$$(a_1a_2\ldots a_j)$$

را به j طریق مختلف می‌توان نوشت، زیرا

$$(a_1a_2\ldots a_j)=(a_2a_3\ldots a_ja_1)=\ldots=(a_ja_1\ldots a_{j-1})$$

لذا هرعنصر S_n تاکنون تا آنجاکه به‌دورهای درجهٔ j مربوط است $j^{e_j}e_j!$ بارشمرده شده است. رویهمرفته، این عنصر بخصوص از ردهٔ مزدوج α ، $1^{e_1}e_1!\,2^{e_2}e_2!\ldots n^{e_n}e_n!$ بار تکرار شده است. از این‌رو تعداد عناصر متمایز در ردهٔ مورد نظر با رابطهٔ (۱۲.۷) داده می‌شود.

از قضیهٔ ۷ (صفحهٔ ۶۵) پیداست که h_α اندیس مرکزساز α درگروه S_n است. لذا نتیجهٔ ذیل را داریم.

قضیهٔ ۲۳. اگر α جایگشتی با قالب دوری (۱۱.۷) باشد، آنگاه مرکزساز α در S_n از مرتبهٔ

$$1^{e_1}e_1!\,2^{e_2}e_2!\ldots n^{e_n}e_n! \qquad (۱۴.۷)$$

است.

مثال. فرض کنیم ϕ دوری متضمن تمامی n شیء باشد، مثل

$$\phi=(1\ 2\ldots n)$$

دراین حالت، $e_1=e_2\ldots=e_{n-1}=0$ و $e_n=1$. ازاین‌رو بنابر(۱۴.۷) مرکزساز ϕ از مرتبهٔ n می‌باشد. اما ϕ مطمئناً با $\iota(=\phi^0)$، ϕ، ϕ^2، ...، ϕ^{n-1} که n عنصر متمایز S_nاند تعویض می‌شود. لذا دراین حالت مرکزساز ϕ با گروه دوری تولید شده بدوسیلهٔ ϕ یکی می‌شود.

۴۰. ترانهشها. یک‌دورهٔ درجهٔ ۲ یک **ترانهش** خوانده‌می‌شود. لذا یک‌ترانهش نوعی، مانند

$$\tau=(ab) \qquad (۱۵.۷)$$

جای a و b را با هم عوض می‌کند و بقیهٔ نمادهای دیگر را ثابت باقی می‌گذارد. متذکر می‌شویم که

$$\tau^2=\iota,\ \tau=\tau^{-1}$$

که درآن ι جایگشت همانی است. گروه S_n شامل $(1/2)n(n-1)$ ترانهش است.

بعد، فرض می‌کنیم S_n برمجموعهٔ نامعین

$$x_1,\ x_2,\ \ldots,\ x_n \qquad (۱۶.۷)$$

اثرکند. لذا اگر α، i را به a_i بفرستد، آن را چنین تعریف می‌کنیم

$$x_i\alpha=x_{a_i}\quad (i=1,2,\ldots,n)$$

و، به‌طورکلیتر، اگر f تابعی دلخواه از کمیتهای نامعین (۱۶.۷) باشد، قرار می‌دهیم

$$f(x_1,x_2,\ldots,x_n)\alpha=f(x_{a_1},x_{a_2},\ldots,x_{a_n}) \qquad (۱۷.۷)$$

بویژه، **حاصلضرب تفاضلی** زیر را در نظر می‌گیریم

$$\begin{aligned}\Delta=\prod_{i<j}(x_i-x_j)&=(x_1-x_2)(x_1-x_3)(x_1-x_4)\ldots(x_1-x_n)\\&\times(x_2-x_3)(x_2-x_4)(x_2-x_5)\ldots(x_2-x_n)\\&\times(x_3-x_4)\ldots(x_3-x_n)\\&\ldots\\&\times(x_{n-1}-x_n)\end{aligned} \qquad (۱۸.۷)$$

روشن است، اگر این کمیتهای نامعین تحت تأثیر جایگشت α قرار گیرند، تابع Δ یا تغییر نمی‌کند و یا در ۱ − ضرب می‌شود. لذا با قرارداد (۱۷.۷) داریم

$$\Delta\alpha = \zeta(\alpha)\Delta \tag{۱۹.۷}$$

که در آن $\zeta(\alpha) = \pm 1$.

تعریف ۱۱. جایگشت α را **زوج** یا **فرد** گویند هرگاه بترتیب $\zeta(\alpha) = 1$ و یا $\zeta(\alpha) = -1$. تابع $\zeta(\alpha)$ **شاخص تناوبی** S_n خوانده می‌شود.

مهمترین خصوصیت این تابع در قضیهٔ ذیل بیان شده است.

قضیهٔ ۲۴. اگر α و β جایگشتهایی دلخواه باشند، آنگاه

$$\zeta(\alpha\beta) = \zeta(\alpha)\zeta(\beta) \tag{۲۰.۷}$$

یعنی حاصلضرب دوجایگشت زوج یا دوجایگشت فرد یك جایگشت زوج است، درحالی که حاصلضرب یك جایگشت فرد در یك جایگشت زوج جایگشتی است فرد.

برهان. نتیجهٔ اثر β را بر دوطرف (۱۹.۷) به‌دست می‌آوریم، و متذکر می‌شویم که بنا بر تعریف ترکیب عملیاتی

$$(\Delta\alpha)\beta = \Delta(\alpha\beta)$$

لذا

$$\Delta(\alpha\beta) = \zeta(\alpha)\Delta\beta$$

مقدار ثابت $\zeta(\alpha)$ بر اثر β تغییر *نمی‌کند*. از اعمال (۱۹.۷) بر $\alpha\beta$ و β رابطهٔ

$$\zeta(\alpha\beta)\Delta = \zeta(\alpha)\zeta(\beta)\Delta$$

را به‌دست می‌آوریم که از آنجا حکم قضیه نتیجه می‌شود. درحالت کلیتر

$$\zeta(\alpha_1\alpha_2\cdots\alpha_r) = \zeta(\alpha_1)\zeta(\alpha_2)\cdots\zeta(\alpha_r) \tag{۲۱.۷}$$

می‌توان تعریف $\zeta(\alpha)$ را چنان سامان داد که تابع Δ دیگر آشکارا ظاهر نشود. هرعامل $(x_i - x_j)$ از Δ متناظر یك زوج (i, j) از اعداد صحیح است به‌قسمی که $1 \leqslant i < j \leqslant n$. بعد از اثردادن α، که i را به α_i و j را به α_j بدل می‌کند، این عامل به صورت $(x_{\alpha_i} - x_{\alpha_j})$ درمی‌آید. این پرانتز عاملی است از Δ هرگاه $\alpha_i < \alpha_j$، درحالی که Δ شامل $-(x_{\alpha_i} - x_{\alpha_j})$ است هرگاه $\alpha_i > \alpha_j$. گوییم که زوج (i, j) موجب یك **انعکاس** می‌شود هرگاه $i - j$ و $\alpha_i - \alpha_j$ مختلف‌العلامه باشند. فرض کنیم وقتی که کلیهٔ زوجهای (i, j) را مورد توجه قرار می‌دهیم تعداد کل انعکاسها t باشد. دراین صورت

$$\zeta(\alpha)=(-۱)^{t}$$

عدد t فوراً به‌طریق زیر پیدا می‌شود: جایگشت α را به‌صورت استانده می‌نویسیم، برای مثال

$$\alpha=\begin{pmatrix} ۱ & ۲ & ۳ & ۴ & ۵ & ۶ \\ ۳ & ۴ & ۶ & ۲ & ۵ & ۱ \end{pmatrix}$$
$$\begin{matrix} || & || & ||| & | & | & \end{matrix} \qquad (t=۹)$$

فرض کنیم k عددی دلخواه از سطر دوم باشد. اگر بعد از k، $s(\geqslant ۰)$ عدد صحیح کوچکتر از k آمده باشد گوییم k دارای s امتیاز است. به ازای هر k، امتیاز مربوط به‌آن را ثبت می‌کنیم، از آنجا امتیاز کل، یعنی t، به‌سادگی پیدا می‌شود. برای مثال، ۳ دارای دو امتیاز است، زیرا ۲ و ۱ بعداز آن آمده‌اند، و ۶ دارای سه امتیاز است، زیرا ۲، ۵ و ۱ بعد از آن آمده‌اند. درمثال حاضر $t=۹$، و بنابراین $\zeta(\alpha)=-۱$.

روشن است که جایگشت همانی، ι، Δ را تغییر نمی‌دهد به‌طوری که

$$\zeta(\iota)=۱ \tag{۲۲.۷}$$

حال برای هر جایگشت α، داریم

$$\zeta(\alpha)\zeta(\alpha^{-۱})=\zeta(\iota)=۱$$

که از اینجا نتیجه می‌شود

$$\zeta(\alpha)=\zeta(\alpha^{-۱}) \tag{۲۳.۷}$$

یعنی، جایگشتهای عکس یك شاخص دارند.

اگر α و β جایگشتهای دلخواهی باشند

$$\zeta(\beta^{-۱}\alpha\beta)=\zeta(\beta^{-۱})\zeta(\alpha)\zeta(\beta)=\zeta(\alpha)$$

لذا جایگشتهای مزدوج یك شاخص دارند، یعنی مقدار ζ برای هر ردهٔ مزدوج از S_n ثابت است.

فرض کنیم τ یك ترانهش، نظیر ترانهشی که در (۱۵.۷) آمده است باشد. در این صورت بنابر قضیهٔ ۲۱، τ با ترانهش خاص $\sigma=(۱۲)$ مزدوج است. براثر σ، علامت $x_۱-x_۲$ عوض می‌شود و به‌جای عوامل باقیمانده در سطر اول (۱۸.۷)، عوامل سطردوم بدون دخالت علامتهای منها، گذاشته می‌شوند. لذا $\zeta(\sigma)=-۱$ وبنابراین $\zeta(\tau)=-۱$.

پس نتیجه می‌شود که کلیه ترانهشها جایگشتهایی فردند. برای پیداکردن شاخص یك دور درجهٔ m، از فرمول

$$(a_۱a_۲\cdots a_m)=(a_۱a_۲)(a_۱a_۳)\cdots(a_۱a_m) \tag{۲۴.۷}$$

که با ارزیابی حاصلضرب طرف راست به‌سادگی تحقیق می‌شود، استفاده می‌کنیم:

$$a_۱ \to a_۲,\ a_۲ \to a_۱ \to a_۳,\ a_۳ \to a_۱ \to a_۴$$

و قس علیهذا.

چون $(m-۱)$ عامل ترانهش دخالت دارند، به‌دست می‌آوریم

$$\zeta(a_۱, a_۲, \ldots, a_m) = (-۱)^{m-۱} \qquad (۲۵.۷)$$

نتیجهٔ حاصل از (۲۴.۷) به شرح زیر قابل بیان است.

قضیهٔ اصلی ۲۱. هر جایگشت را می‌توان، به طرق بسیاری، به‌صورت حاصلضربی از ترانهشها بیان کرد. تعداد عاملهای ترانهش در هر یك از این حاصلضربها، برحسب آنکه جایگشت مفروض زوج یا فرد باشد، یا همواره زوج و یا همواره فرد است.

برهان. فرض کنیم α جایگشت مفروض باشد. قبلاً دیده‌ایم (صفحهٔ ۲۸) که α را می‌توان به‌صورت حاصلضربی از دوره‌ها بیان کرد. بنابر (۲۴.۷) هر دوره حاصلضربی است از ترانهشها بدین طریق مسلماً داریم

$$\alpha = \tau_۱\tau_۲\cdots\tau_s \qquad (۲۶.۷)$$

که در آن هر τ یك ترانهش‌است. این حاصلضرب منحصر به‌فرد نیست؛ برای مثال می‌توانیم زوجهایی از عوامل نظیر

$$(ab)(ba)$$

راکه هم‌ارز جایگشت همانی‌اند، در α درج کنیم. می‌توان گفت، البته با بداهت کمتر، اگر $a \neq ۱$ و $b \neq ۱$، رابطهٔ

$$(ab) = (۱a)(۱b)(۱a) \qquad (۲۷.۷)$$

را خواهیم داشت، و روابط مشابهی وجود دارند که در آنها به‌جای شیء ۱ هر شیء دیگری بجز a و b گذاشته شده است. اما (۲۶.۷) ایجاب می‌کند که $\zeta(\alpha) = (-۱)^s$، و چون $\zeta(\alpha)$ منحصراً به‌وسیلهٔ α معین شده است، از آنجا نتیجه می‌شود، برحسب آنکه α زوج یا فرد باشد، s زوج یا فرد خواهد بود.

با استفاده از دستگاه نامگذاری که در بخش ۱۲ (صفحهٔ ۴۲) معرفی کردیم، داریم،

فرع. گروه S_n به‌وسیلهٔ مجموعهٔ ترانهشها تولید می‌شود. به‌موجب (۲۷.۷) می‌توان این نتیجه را دقیقتر بیان کرد.

قضیهٔ ۲۵. گروه S_n به‌وسیلهٔ $n-۱$ ترانهش:

$$(۱\ ۲), (۱\ ۳), \ldots, (۱\ n)$$

تولید شده است.

۴۱. گروه متناوب. حال بـه نحوهٔ تشخیص جـایگشتهای فـرد و زوج ازهم، کـه در تعریف ۱۱ (صفحهٔ ۱۴۵) واردکرده بودیم، برمی گردیـم و مطلب را با قضیهٔ سادهای در باب یك گروه جایگشتی دلخواه، یعنـی یك زیرگروه S_n بـهازای مقدار مناسب n، آغاز می کنیم.

قضیهٔ ۲۶. در هر گروه جایگشتی G، جایگشتهای زوج تشکیل یك زیرگروه نـرمال می‌دهند که یا با G مساوی و یا دارای اندیس دو در G است.

برهان. فرض کنیم H مجموعهٔ جایگشتهای زوج در G باشد. بـهموجب (۲۰.۷)، (۲۲.۷)، و (۲۳.۷) H یك زیرگروه G است. اگر $H=G$، حکم ثابت شده است. اگر $G \neq H$، آنگاه G شامل حداقل یك جایگشت فرد مانند σ است وهممجموعهٔ $H\sigma$ متمایز از H است. فرض کنیم δ یك جایگشت فرد دلخـواه از G باشد. پس $\sigma\delta^{-1}$ زوج است، یعنی $\sigma\delta^{-1} \in H$ واز اینرو $H\sigma = H\delta$ (صفحهٔ ۳۷، قضیهٔ ۵). لـذا دقیقاً دوهممجموعه از H در G وجود دارند، بهطوریکه $[G:H]=۲$ همان گونه کـه ادعا شده است. بنابر حالت (د) صفحهٔ ۷۵، H در G نرمال است.

حالت $G=S_n$ حالتی است که ما بیشتر بهآن خواهیم پرداخت.

تعریف ۱۲. مجموعهٔ کلیـهٔ جایگشتهای زوج S_n $(n \geqslant ۲)$ یك گروه A_n از مـرتبهٔ $(۱/۲)n!$ تشکیل می‌دهد، این گروه **گروه متناوب** درجهٔ n خوانده می‌شود.

برای مثال، گروه $A_۴$ از مرتبهٔ $۱۲ = (۴!)(۱/۲)$ است و از جایگشتهای ذیل (که برطبق ردههای مزدوج $S_۴$ مرتب شدهاند) تشکیل می‌شود

$$A_۴ = C_۰ \cup C_۱ \cup C_۲$$

که در آن

$$C_۰ = \iota$$

$$C_۱ = (۱۲)(۳۴) \cup (۱۳)(۲۴) \cup (۱۴)(۲۳) \qquad (۲۸.۷)$$

$$C_۲ = (۱۲۳) \cup (۱۲۴) \cup (۱۳۲) \cup (۱۳۴) \cup (۱۴۲) \cup (۱۴۳) \cup (۲۳۴) \cup (۲۴۳)$$

ممکن است سؤال شود که آیا S_n علاوه بر A_n دارای زیرگروه نرمال خاص دیگری نیز هست؟ اگـر حالتهای پیشپا افتادهٔ $n=۱$ و $n=۲$ را نـادیده بگیریم، ما بـدین سؤال وقتی جواب مـیدهیم کـه $n=۳$ یا $n=۴$. و بـرای این امر با استفاده از حالت (ج) (صفحهٔ ۶۹) مبنی برآنکه یك زیرگروه نرمال باید اجتماع ردههای مزدوج کامل، منجمله ردهٔ متشکل از عنصر واحد، باشد استفاده خواهیم کرد.

ردههای $S_۳$ عبارتانداز

$$\iota,\ (۱۲) \cup (۱۳) \cup (۲۳) \quad \text{و} \quad (۱۲۳) \cup (۱۳۲)$$

که بترتیب شامل ۱، ۳ و ۲ عنصر می‌باشند. تنها هنگامی که عنصر واحد را بـه‌ردهٔ آخری منضم کنیم مجموعه‌ای به‌دست می‌آوریم کـه تعداد عناصرش $(6=)|S_3|$ را عاد می‌کند، که این شرط لازم برای زیرگروه بودن است. در واقع

$$A_3 = \iota \cup (123) \cup (132)$$

و لذا این تنها زیرگروه نرمال خاص S_3 است.

گـروه S_4 دارای پنج ردهٔ‌مزدوج است (صفحهٔ ۱۴۲، جدول xiii ملاحظه شود). سه‌تا از این رده‌ها، که شامل جایگشتهای زوج‌اند، در (۲۸.۷) فهرست شده‌انـد. دوتای باقیمانده عبارت‌انداز

$$C_3 = (12) \cup (13) \cup (14) \cup (23) \cup (24) \cup (34)$$

و

$$C_4 = (1234) \cup (1243) \cup (1324) \cup (1342) \cup (1423) \cup (1432)$$

چون $|C_0| = 1$، $|C_1| = 3$، $|C_2| = 8$، $|C_3| = |C_4| = 6$، فقط

$$V = C_0 \cup C_1 \quad \text{و} \quad A_4 = C_0 \cup C_1 \cup C_2$$

دارای اعداد اصلی عادکننده $(24=)|S_4|$ هستند، همچنان که مورد نیاز زیرگروههاست. قبلاً دیده‌ایم که $S_4 \rhd A_4$. وحقیقت شایان توجه این است که

$$V = \iota \cup (12)(34) \cup (13)(24) \cup (14)(23)$$

تصادفاً یك گروه باشد. زیرا اگـر قرار دهیم $\alpha = (12)(34)$ و $\beta = (13)(24)$ آنگاه $\alpha\beta = \beta\alpha = (14)(23)$ و $\alpha^2 = \beta^2 = \iota$. لذا $S_4 \rhd V$ و V دارای ساختار گروه چارینه (صفحهٔ ۵۱) می‌باشند. اینك ثابت کردیم کـه A_4 و V تنها زیرگروههای نرمال خاص S_4 هستند. ضمناً چون V فقط از جایگشتهای زوج تشکیل می‌یابد. داریم $A_4 \rhd V$. در سریهای ترکیبی (بخش ۳۵)

$$S_3 \rhd A_3 \rhd \{\iota\}$$

$$S_4 \rhd A_4 \rhd V \rhd \{\iota\}$$

کلیهٔ عاملهای تـرکیبی از مـراتب اول‌اند. این ثابت می‌کند کـه S_3 و S_4 گـروههای حلپذیرند (بخش ۳۶). بعداً خواهیم دید که وقتی $n > 4$، S_n دراین مورد رفتار دیگری پیدا می‌کند.

بجاست که مجموعهٔ نسبتاً سرراستی از مولدها برای گروه A_n در اختیار داشته‌باشیم.

قضیهٔ ۲۷. وقتی که $n \geqslant 3$، گروه A_n می‌تواند به‌وسیلهٔ $n-2$ دورهٔ سه‌تایی

$$(123), (124), \ldots, (12n) \qquad (29.7)$$

تولید شود.

برهان. بنابر قضیهٔ ۲۵، هر جایگشت می‌تواند به‌صورت حاصلضربی از ترانهشهای نوع $(۱i)$ بیان شود. برای یك جایگشت زوج، تعداد عاملهای ترانهش باید زوج باشد. بنابراین A_n به‌وسیلهٔ زوج عاملهای $(۱ \ \ i)(۱ \ \ j)$ تولید می‌شود. چون $\iota = (۱ \ \ i)^۲$، می‌توانیم فرض کنیم که در هر زوج $j \neq i$. اما

$$(۱ \ \ i)(۱ \ \ j) = (۱ \ \ i \ \ j) \qquad (۳۰.۷)$$

اگر $i = ۲$، این زوج ترانهشها مساوی یکی از دورهای سه‌تایی مذکور در (۲۹.۷) می‌باشند. اگر $j = ۲$، ملاحظه می‌کنیم که

$$(۱ \ \ i)(۱ \ \ ۲) = (۱ \ \ i \ \ ۲) = (۱ \ \ ۲ \ \ i)^۲$$

بالاخره، اگر $i > ۳$ و $j > ۲$، از رابطهٔ

$$(۱ \ \ i \ \ j) = (۱ \ \ ۲ \ \ j)(۱ \ \ ۲ \ \ i)(۱ \ \ ۲ \ \ j)^{-۱}$$

استفاده می‌کنیم. ازاین رو در تمامی حالات، طرف راست (۳۰.۷) را می‌توان برحسب مولدهای (۲۹.۷) بیان کرد.

با توجه به‌مفهوم گروه ساده (صفحهٔ ۶۸)، اکنون یك قضیهٔ مشهور دربارهٔ گروههای متناوب را، که منسوب به ا. گالوا[1] است، ثابت کنیم.

قضیهٔ اصلی ۲۲. وقتی‌که $n \neq ۴$، گروه A_n گروهی است ساده.

برهان. قبلاً دیده‌ایم (صفحهٔ ۶۸) که V یك زیرگروه نرمال خاص $A_۴$ است. از این‌رو $A_۴$ ساده نیست. از اینجا به‌بعد فرض می‌کنیم که $n > ۴$. قضیهٔ بالا با حکم‌ذیل هم‌ارز است: اگر $N \lhd A_n$ و $|N| > ۱$، آنگاه $N = A_n$. فرض‌قاطع این‌است که N در A_n نرمال است. لذا اگر $\alpha \in N$ و δ یك جایگشت‌زوج دلخواه باشد، آنگاه $\delta^{-۱}\alpha\delta \in N$، وبنابراین $\delta^{-۱}\alpha\delta\alpha^{-۱}$ نیز به N تعلق دارد. برهان‌این قضیه به‌چندین‌مرحله تقسیم شده‌است.

(الف) فرض کنیم N شامل یك دور سه‌تایی، مثلاً

$$\alpha = (a \ \ b \ \ c)$$

باشد. دراین حالت ثابت خواهیم کرد که N شامل همهٔ دورهای سه‌تایی

$$\xi = (x \ \ y \ \ z)$$

است، که در آن x، y، z اشیایی متمایز و دلخواه‌اندکه ازقبل درنظرگرفته شده‌اند. بنابر قضیهٔ ۲۷ این مطلب بلافاصله ایجاب می‌کند که $N = A_n$.

جایگشت

1. E. Galois

$$\phi=\begin{pmatrix}a & b & c\\ x & y & z\end{pmatrix}$$

عنصری از S_n است با این برداشت که هر شیئی که در ϕ ذکر نشده است ثابت می‌ماند. بنابر (۷.۷) داریم

$$\phi^{-1}\alpha\phi=\xi$$

چون $n\geqslant ۵$، حداقل ۲ شیء e، f وجود دارند که α شامل آنها نمی‌باشد. ترانهش $\tau=(e\ \ f)$ با α تعویضپذیر است و از آنجا نتیجه می‌شود که

$$(\tau\phi)^{-1}\alpha(\tau\phi)=\xi$$

به‌سادگی دیده می‌شود که یا ϕ و یا $\tau\phi$ به A_n تعلق دارد. بنابراین α در A_n با ξ مزدوج بوده نتیجه می‌گیریم که $\xi\in A_n$.

(ب) در مرحلهٔ بعد فرض می‌کنیم N شامل جایگشت

$$\omega=\gamma\delta\varepsilon\ldots, \qquad (۳۱.۷)$$

باشد که در آن γ، δ، ε، .. دورهایی از هم جدا بوده و درجهٔ γ از سه بیشتر است، یعنی

$$\gamma=(a_۱,\, a_۲,\, a_۳,\, a_۴,\, \ldots,\, a_m),\ m>۳$$

اما $\sigma=(a_۱a_۲a_۳)$ یك جایگشت زوج است که با کلیهٔ دورهای (۳۱.۷) بجز اولی تعویضپذیر است. لذا

$$\omega_۱=\sigma^{-۱}\omega\sigma=(\sigma^{-۱}\gamma\sigma)\delta\varepsilon\ldots$$

به N تعلق دارد، همچنین است $\omega_۱\omega^{-۱}$. چون δ، ε، ... با هر دوی γ و $\sigma^{-۱}\gamma\sigma$ تعویضپذیر است ملاحظه می‌کنیم که

$$\begin{aligned}\omega_۱\omega^{-۱}&=\sigma^{-۱}\gamma\sigma\gamma^{-۱}\\&=(a_۲a_۳a_۱a_۴\ldots a_m)(a_ma_{m-۱}\ldots a_۴a_۳a_۲a_۱)\\&=(a_۱a_۳a_m)\end{aligned}$$

از این‌رو N شامل یك دور سه تایی است واز (الف) نتیجه می‌گیریم که $N=A_n$. از این به‌بعد می‌توانیم فرض کنیم که همهٔ جایگشتهای N حاصلضربهایی از دورهای از هم جدا باشند، که درجات این دورها ۲ یا ۳ هستند.

(ج) فرض کنیم N شامل جایگشتی مانند ω است که حداقل با ۲ دور سه‌تایی مانند

$$\omega=\alpha\beta\lambda$$

سروکار دارد که در آن $\alpha=(a_۱a_۲a_۳)$، $\beta=(b_۱b_۲b_۳)$، و λ به a_i یا b_i $(i=۱,\, ۲,\, ۳)$

بستگی ندارد. با انتخاب

$$\sigma=(a_2a_3b_1)$$

مشاهده می کنیم که σ با λ جا به‌جا می‌شود. از این‌رو N شامل عنصر

$$\begin{aligned}\sigma^{-1}\omega\sigma\omega^{-1}&=(\sigma^{-1}\alpha\sigma)(\sigma^{-1}\beta\sigma)(\alpha^{-1}\beta^{-1})\\&=(a_1a_3b_1)(a_2b_2b_3)(a_3a_2a_1)(b_3b_2b_1)\\&=(a_1a_2b_1a_3b_3)\end{aligned}$$

است که با فرض آنکه هیچ دوری بالاتر از درجهٔ سه در N پیدا نمی‌شود متناقض است.

(د) وقتی کــه فقط وجود یك دور سه‌تایــی در میان عاملها مجاز باشد، یك عنصر نوعی آن به‌صورت

$$\omega=(a_1a_2a_3)\lambda$$

است که λ حاصلضربی از ترانهشهای ازهم جداست. لذا $\lambda^2=\iota$ و N شامل عنصر

$$\omega^2=(a_1a_3a_2)$$

است که ما را به (حالت) (الف) برمی گرداند.

(هـ) بالاخره، باید حالتی را کــه در آن کلیهٔ عناصر N بجز ι، حــاصلضربهایی از ترانهشهای از هم‌جدا می‌باشند مورد بحث قــرار دهیم. هرگاه $n=4$، این وضعیت واقعاً رخ می‌دهــد و به گروه V مذکور درصفحهٔ ۱۴۹ ختم می گردد. ولی چون فرض می کنیم که $n>4$، می‌توانیم چنین استدلال کنیم: چون تعداد عاملهای ترانهش باید زوج باشد، یك عنصر نوعی N به‌صورت

$$\omega=(a_1a_2)(b_1b_2)\lambda$$

هست که در آن λ شامل a_1، a_2، b_1، b_2 نیست. با انتخاب عنصر پنجمی مانند c، متمایز از آنهایی که هم‌اکنون‌نام بردیم، به‌نوبت از عناصر مبدل $\sigma=(a_2b_1b_2)$ و $\delta=(a_1b_2c)$ استفاده می کنیم تا بتوانیم از ω عناصر دیگری از N را به‌روش ذیل بسازیم:

$$\omega_1=\sigma^{-1}\omega\sigma=(a_1b_1)(b_2a_2)\lambda$$

$$\begin{aligned}\omega_2=\omega_1\omega^{-1}&=(a_1b_1)(b_2a_2)(a_1a_2)(b_1b_2)\\&=(a_1b_2)(a_2b_1)\end{aligned}$$

$$\omega_3=\delta^{-1}\omega_2\delta=(b_2c)(a_2b_1)$$

$$\begin{aligned}\omega_3\omega_2^{-1}&=(b_2c)(a_2b_1)(a_1b_2)(a_2b_1)\\&=(a_1b_2c)\end{aligned}$$

لذا، برخلاف فرضی که کرده بودیم، سرانجام N شامل یك دور سه‌تایی می‌شود و برهان قضیه تمام.

اکنون می‌توانیم به‌سؤال مربوط به‌زیرگروههای نرمال S_n، وقتی $n>۴$، برگردیم.

قضیهٔ ۲۸. وقتی $n>۴$، تنها زیرگروه حقیقی نرمال S_n، گروه متناوب A_n است.

برهان. فرض کنیم $H \triangleleft S_n$ و $|H|>۱$. نخست نشان می‌دهیم که H نمی‌تواند ازمرتبهٔ ۲ باشد. برای این منظور فرض می‌کنیم

$$H=\{\iota, \xi | \xi^۲=\iota\}$$

در این صورت ξ یا باید یك ترانهش باشد و یا حاصلضربی از ترانهشهای ازهم جدا. درحالت اول فرض کنیم $\xi=(ab)$. شیئی مانند c متمایز از a و b وجود دارد. چون $H \triangleleft S_n$، عنصر $(bc)=(ac)^{-۱}(ab)(ac)$ به H تعلق خواهد داشت، و H بیش از دو عنصر خواهد داشت. بعد، فرض می‌کنیم که $\xi=(a_۱a_۲)(b_۱b_۲)\lambda$، که درآن λ مستقل از $a_۱$، $a_۲$، $b_۱$، $b_۲$ است. دراین صورت، اگر $\sigma=(a_۲b_۱b_۲)$، آنگاه $\sigma^{-۱}\xi\sigma \in H$، اما $\sigma^{-۱}\xi\sigma \neq \xi$، که با فرض $|H|=۲$ تناقض دارد، لذا $|H|>۲$. بنابرقضیهٔ ۲۶، حداقل نصف عناصر H زوج‌اند، ازاین‌رو، اگر $D=H \cap A_n$، آنگاه $|D|>۱$. واضح است که $D \triangleleft A_n$. چون A_n ساده است، $D=A_n$، که بدان معنی است که

$$A_n \leqslant H \qquad (۳۲.۷)$$

چون H یك زیرگروه‌خاص S_n است، داریم $|H| \leqslant (۱/۲)n!$. بنابراین $|H|=|A_n|$، و از (۳۲.۷) نتیجه می‌گیریم که $A_n=H$.

۴۲. نمایشهای جایگشتی. تا آغاز سدهٔ بیستم مفهوم یك گروه کاملاً مورد قبول و تصدیق ریاضیدانان واقع نشده بود. نوشته‌هایی‌که قبلاً در باب این موضوع وجود داشتند، از جمله‌کارهای کلاسیك کوشی[1]، گالوا، و ك. ژوردان[2]، می‌توان گفت منحصراً از گروههای جایگشتی، یعنی زیرگروههای گروههای متقارن S_n، بحث می‌کردند. ولی، بسیاری از نتایج آنها دقیقاً برای‌گروههای متناهی دلخواه نیز به‌کار می‌رفتند و مستقل از این‌فرض بودند‌که عناصر گروه مورد بحث جایگشت می‌باشند. حتی در زمینهٔ نظریهٔ جدید‌گروهها مطالعهٔ گروههای جایگشتی مبحثی‌سخت مورد علاقه است. این گروهها نه‌تنها تعداد زیادی ازمثالهای‌نسبتاً سهل‌الوصول از گروههای متناهی‌را دراختیار قرارمی‌دهند بلکه،همچنان‌که آ. کیلی در ۱۸۵۴ اشاره کرده است، هر گروه متناهی بایك گروه جایگشتی یکریخت است. فرض کنیم

$$G: a_۱, a_۲, \cdots, a_g \qquad (۳۳.۷)$$

---

1. Cauchy 2. C. Jordan

گـروهی متناهی از مرتبهٔ g بـاشد. هـرگاه x عنصر دلخواهی از این عناصر بـاشد، حاصلضربهای

$$a_1x,\ a_2x,\ \cdots,\ a_gx \tag{۳۴.۷}$$

g عنصر متمایز G هستند و بنابراین تمامی گروه را تشکیل می‌دهند. لذا (۳۴.۷) یك ترتیب دیگری از (۳۳.۷) است، یعنی می‌توانیم جایگشت

$$x\rho=\begin{pmatrix}a_1 & a_2 & \cdots a_g\\ a_1x & a_2x & \cdots a_gx\end{pmatrix}$$

را که از درجهٔ g است به x مربوط کنیم. اشیایی کـه این جایگشت بر آنها اثر می‌کنند خود، عناصر گروه‌اند. استفاده از قرارداد علامتی

$$x\rho=\begin{pmatrix}a_i\\ a_ix\end{pmatrix}\quad (i=1,2,\cdots,g) \tag{۳۵.۷}$$

اغلب موجب سادگی می‌شود. اثر $x\rho$ بر G را می‌توان به‌اختصار با این گفته که هر عنصر G از راست در x ضرب می‌شود بیان کرد. ترتیب ذکر عناصر مهم نیست. بویژه، اگر u عنصر ثابتی از G باشد، حاصلضربهای a_iu $(i=1,2,\ldots,g)$، همچنان‌که در (۳۴.۷) متذکر شده‌ایم، همگی عناصر G هستند. بنابراین می‌توانیم بنویسیم

$$x\rho=\begin{pmatrix}a_iu\\ a_iux\end{pmatrix} \tag{۳۶.۷}$$

اینك فرض کنیم y عنصر دیگری از G و

$$y\rho=\begin{pmatrix}a_i\\ a_iy\end{pmatrix} \tag{۳۷.۷}$$

جایگشت وابسته به y باشد. اگر حاصلضرب جایگشتهای (۳۵.۷) و (۳۷.۷) را محاسبه کنیم به‌موجب (۳۶.۷)، خواهیم داشت

$$(x\rho)(y\rho)=\begin{pmatrix}a_i\\ a_ix\end{pmatrix}\begin{pmatrix}a_i\\ a_iy\end{pmatrix}=\begin{pmatrix}a_i\\ a_ix\end{pmatrix}\begin{pmatrix}a_ix\\ a_ixy\end{pmatrix}=\begin{pmatrix}a_i\\ a_ixy\end{pmatrix}$$

لذا

$$(x\rho)(y\rho)=(xy)\rho \tag{۳۸.۷}$$

که نشان می‌دهد نگاشت

$$\rho: G\rightarrow S_g$$

یك‌همریختی از G به‌توی S_g است. بعلاوه، ρ یك به‌یك است، یعنی‌هستهٔ آن تنها ازعنصر همانی ۱ از G تشکیل می‌شود (قضیهٔ ۹، صفحهٔ ۷۵). زیرا فرض کنیم

$$x\rho = \iota$$

که ι عنصرهمانی S_g باشد. معنی آن این است که

$$a_i x = a_i \quad (i = ۱, ۲, \cdots, g)$$

که‌آشکارا نتیجه می‌دهدکه $x = ۱$. درواقع اگر $x \neq ۱$، $x\rho$ جای هرعنصر G را عوض می‌کند. چون ρ یك به‌یك است نگارهٔ G بر اثر ρ با زیرگروهی از S_g یکریخت است.

درمرحلهٔ بعد، $x\rho$ را به‌دوره‌های ازهم‌جدا تجزیه و فرض می‌کنیم x از مرتبهٔ r باشد، لذا

$$x^r = ۱ \tag{۳۹.۷}$$

با هرعنصر a از G که شروع کنیم می‌دانیم که اثر $x\rho$، a را به ax بدل می‌کندکه به‌نوبهٔ خود به $ax^۲$ بدل می‌شود؛ نگارهٔ $ax^۲$ عبارت است‌از $ax^۳$، و همین‌طور ادامه می‌یابد تا آنکه به $ax^{r-۱}$ می‌رسد که نگارهٔ آن، بنابر (۳۹.۷)، برابر است بـا a. از این‌رو $x\rho$ متضمن دور

$$(a, ax, ax^۲, \cdots, ax^{r-۱}) \tag{۴۰.۷}$$

است که شامل r عنصر متمایز G می‌باشد. هرگاه $r < g$، عنصری مانند b، که در (۴۰.۷) نباشد، انتخاب می‌کنیم و بدین‌نحو می‌توانیم یك دور دیگری نظیر

$$(b, bx, bx^۲, \cdots, bx^{r-۱}) \tag{۴۱.۷}$$

بسازیم. روشن‌است که (۴۰.۷) و (۴۱.۷) هیچ عنصرمشترکی ندارند؛ زیرا اگر می‌داشتند، نتیجه می‌شدکه $b = ax^t\ (۰ \leqslant t \leqslant r - ۱)$، که با انتخاب b درتناقض است. با ادامهٔ این روش‌دورهایی‌را، که هریك شامل r عنصرند، می‌سازیم، تا آنکه تمامی g عنصر G به‌حساب آیند. لذا فی‌المثل

$$x\rho = (a, ax, \cdots, ax^{r-۱})(b, bx, \cdots, bx^{r-۱}) \cdots (f, fx, \cdots, fx^{r-۱})$$

جایگشتی را کـه کلیهٔ دورهای متشکلهٔ آن دارای یك طول باشند **جایگشت منظم** می‌نامند. ضمناً، فرمول اخیر مؤید آن است که r، یك عامل g است.

نتایج خود را به‌صورت ذیل خلاصه می‌کنیم:

قضیهٔ اصلی ۲۳. (کیلی). فرض کنیم

$$G : a_۱, a_۲, \cdots, a_g$$

گروهی مجرد از مرتبهٔ g باشد. به هرعنصر x از G جایگشت منظم

$$x\rho=\begin{pmatrix}a_۱ & a_۲ \cdots a_g\\ a_۱x & a_۲x\cdots a_gx\end{pmatrix}$$

را وابسته می‌کنیم. نگاشت $\rho: G \to S_g$ که بدین طریق تعریف می‌شود یك همریختی یك به‌یك است، به‌طوری که G با زیرگروهی از S_g یکریخت است. اگر x از مرتبهٔ r باشد، آنگاه $x\rho$ حاصلضرب g/r دور از درجهٔ r است.

وقتی که یك گروه مجرد G با یك گروه G' کـه عناصر آن موجودات واقعی ریاضی از قبیل جایگشتها یـا ماتریسها هستند، گوییم G' یك **نمایش صادق** G بـرحسب جایگشتها یا ماتریسهاست. G' کلیهٔ ویژگیهای G را نیز دارد. بعکس، هراطلاعی در باب G'، کـه به‌ماهیت خـاص عناصر آن بستگی نداشته بـاشد، موجب همان اطلاع از G نیز می‌شود. از آنجا کـه اغلب انجام محاسبات بـا عناصر حقیقی ساده‌تـر است، وجود یك نمایش صادق می‌تواند در روشن ساختن ساختار یك گروه مجرد ما را یاری کند. این روش شبیه استفاده از محورهای مختصات دربحث از مسائل هندسی است. نمایش خاصی که به‌وسیلهٔ قضیهٔ اصلی کیلی فـراهم آمده است به **نمایش منظم راست** G معروف است. وقتی کـه G به‌وسیلهٔ جدول‌ضربش (بخش ۴، صفحهٔ ۱۳) داده شده بـاشد، نمایش منظم راست آن را می‌توان فوراً تعیین‌کرد؛ درنماد دوسطری برای $x\rho$، سطراول با ۱ و سطردوم با x شروع می‌شود؛ در واقع هر اطلاعی ازیك نمایش‌منظم‌راست، بالقوه هم‌ارز ساختمان جدول‌ضرب است.

مثال. درحالت گروه غیرآبلی‌مرتبهٔ ۶که درجدول (v)، صفحهٔ ۱۵، داده‌شده است، عناصر نمایش منظم راست، به‌طریق ذیل، به‌دورهایی تجزیه می‌شوند

$$۱\rho=\begin{pmatrix}۱ & a & b & c & d & e\\ ۱ & a & b & c & d & e\end{pmatrix}=(۱)\ (a)\ (b)\ (c)\ (d)\ (e)$$

$$a\rho=\begin{pmatrix}۱ & a & b & c & d & e\\ a & b & ۱ & d & e & c\end{pmatrix}=(۱\quad a\quad b)(c\quad d\quad e)$$

$$b\rho=\begin{pmatrix}۱ & a & b & c & d & e\\ b & ۱ & a & e & c & d\end{pmatrix}=(۱\quad b\quad a)(c\quad e\quad d)$$

$$c\rho=\begin{pmatrix}۱ & a & b & c & d & e\\ c & e & d & ۱ & b & a\end{pmatrix}=(۱\quad c)(a\quad e)(b\quad d)$$

$$d\rho=\begin{pmatrix}۱ & a & b & c & d & e\\ d & c & e & a & ۱ & b\end{pmatrix}=(۱\quad d)(a\quad c)(b\quad e)$$

$$e\rho=\begin{pmatrix}۱ & a & b & c & d & e\\ e & d & c & b & a & ۱\end{pmatrix}=(۱\quad e)(a\quad d)(b\quad c)$$

گاهی اوقات مناسبتر آن است که به جای $x\rho$، یك عنصر نوعی از نمایش منظم راست ρ_x نوشته شود. لذا می‌توان ρ_x را به‌طور خلاصه با فرمول

$$a\rho_x=ax(a\in G) \tag{۴۲.۷}$$

بیان کرد.

درحالت کلیتر می توانیم همریختیهای

$$\theta:G\to S_n$$

را که لزوماً یك‌به‌یك (صادق) نیستند ودر آنها n یك‌عدد صحیح مناسبی‌است.درنظر بگیریم. وقتی که چنین همریختی وجود داشته باشد، گوییم G دارای یك **نمایش‌جایگشتی** از درجهٔ n است. یك روش نسبتاً کلی برای ساختن چنین نمایشها روش ذیل است: فرض کنیم H یك زیر گروه G و

$$G=Ht_۱\cup Ht_۲\cup\cdots\cup Ht_n \tag{۴۳.۷}$$

تجزیهٔ G به‌هممجموعه‌های راست نسبت به H باشد.که در اینجا $n=[G:H]$، (صفحهٔ ۳۸ را ملاحظه کنید). اگر x عنصری ثابت از G باشد، هممجموعه‌های راست Ht_ix $(i=۱,۲,\ldots,n)$ متمایزند و بنابراین باید همانهایی باشند که در (۴۳.۷) ذکر شده‌اند. لذا

$$x\theta=\begin{pmatrix}Ht_۱ & Ht_۲ & \cdots Ht_n\\ Ht_۱x & Ht_۲x & \cdots Ht_nx\end{pmatrix}$$

یك‌جایگشت درجهٔ n است که اشیاء آن n هممجموعهٔ راست H در G می باشند. با استدلالی مشابه آنچه که درصفحهٔ ۷۵ آورده شد به‌آسانی می توان نشان داد که θ یك همریختی است یعنی

$$(x\theta)(y\theta)=(xy)\theta$$

اگر k درهستهٔ θ باشد. باید داشته باشیم

$$Ht_ik=Ht_i\quad(i=۱,۲,\ldots,n)$$

که هم‌ارز با این شرط است که $t_ik\in Ht_i$ یا $k\in t_i^{-۱}Ht_i$ $(i=۱,۲,\ldots,n)$. اما هرزیر گروه مزدوج با H، به‌ازای مقدار مناسبی‌از i به‌صورت $t_i^{-۱}Ht_i$ است. زیرا اگر y عنصری دلخواه از G باشد، آنگاه باید دریکی از هممجموعه‌ها قرار داشته باشد، یعنی مثلاً $y\in Ht_i$، یعنی $y=ut_i$، که در آن $u\in H$. از این‌رو

$$y^{-1}Hy = t_i^{-1}u^{-1}Hut_i = t_i^{-1}Ht_i$$

لذا می‌توانیم بگوییم که هستهٔ θ از اشتراك کلیهٔ گروههای مزدوج با H تشکیل شده است. ما کلیهٔ این نتایج را درقضیهٔ اصلی ذیل گردآورده‌ایم.

قضیهٔ اصلی ۲۴. فرض کنیم H زیرگروهی از G با اندیس متناهی n، و t_1، t_2، . . .، t_n یك تراگرد H (صفحهٔ ۳۸) در G باشد. به هر عنصر x از G جایگشت

$$x\theta = \begin{pmatrix} Ht_1 & Ht_2 & \cdots Ht_n \\ Ht_1x & Ht_2x & \cdots Ht_nx \end{pmatrix}$$

را وابسته می‌کنیم. نگاشت $\theta : G \longrightarrow S_n$ که بدین‌گونه تعریف می‌شود یك همریختی است. هستهٔ θ از اشتراك تمامی زیرگروههایی که با H مزدوج‌اند تشکیل می‌شود.

ما این بخش را با مثالی به‌پایان می‌بریم که نشان می‌دهد چگونه از این مفاهیم می‌توان برای دستیابی به‌اطلاعاتی درباب ساختار یك گروه استفاده کرد.

مثال. گروه متناوب A_5 هیچ زیرگروهی از مراتب ۳۰، ۲۰، یا ۱۵ ندارد. به عبارت دیگر، ما ادعا می‌کنیم که هرگاه H یك زیرگروه حقیقی A_5 باشد، آنگاه $[A_5 : H] \geqslant 5$. فرض کنیم H یك زیرگروه حقیقی A_5 باشد و قرار می‌دهیم $n = [A_5 : H]$. بنابرقضیهٔ اصلی۲۴، همریختی‌چون $\theta : A_5 \longrightarrow S_n$ وجود دارد. فرض کنیم K هستهٔ θ باشد. می‌دانیم (صفحهٔ ۷۵) که K یك‌زیرگروه نرمال A_5 است. اما A_5 یك گروه ساده است (قضیهٔ اصلی ۲۲). از این‌رو یا $K = \{1\}$ و یا $K = A_5$. شق دوم را فوراً می‌توان کنار گذاشت، زیرا بنابر قضیهٔ ۲۴، K در H قرارداد و ازآنجا $|K| \leqslant |H| < |A_5|$ و بنابراین باید داشته باشیم $K = \{1\}$، یعنی θ یك به‌یك است. لذا نگارهٔ A_5 بر اثر θ، از ۶۰ عنصرمتمایز S_n تشکیل شده است، و این غیرممکن است مگرآنکه $n \geqslant 5$.

۴۳. گروههای ترایا. دراین بخش و بخش‌بعدی ما جایگشتهایی از درجهٔ ثابت n، یعنی زیرگروههای G از گروه متقارن خاص S_n را مورد بررسی قرار می‌دهیم. اشیایی را که G برآنها اثر می‌کند به ۱، ۲، . . .، n و یا به‌وسیلهٔ حروف a، b، . . . نشان می‌دهیم.

تعریف ۱۳. یك‌گروه از جایگشتها را **ترایا** خوانیم هرگاه به ازای هرزوج از حروف مفروض a و b (که لزومی ندارد متمایز باشند)، حداقل یك جایگشت درگروه وجود داشته‌باشد که a را به b تبدیل کند. درغیر این‌صورت‌گروه را **ناترایا** می‌نامیم.

باید توجه داشت که این‌مفهوم فقط در گروههای جایگشتی به‌کارمی‌رود.

جایگشتی که‌aرا به b تبدیل کندبه θ_{ab} نشان داده‌می‌شود، بی آنکه تأثیر آن برنمادهای دیگر موردنظر قرار گیرد. البته ممکن است برای‌یك زوج مفروض a و b تعداد زیادی از این گونه‌جایگشتها وجود داشته باشد. متذکر می‌شویم که θ_{ab}^{-1}، b را به a تبدیل می‌کند.

واضح است که گروه متقارن S_n ترایاست، چون شامل تمام جایگشتهای ممکن از جمله ترانهش (a, b) است که به‌صورت θ_{ab} به‌کار می‌رود.
ازسوی دیگر گروه مرتبهٔ ۴:

$$V_1: (1), \ (12), \ (34), \ (12)\ (34)$$

ناترایاست زیرا هیچ یك از جایگشتهای آن ۱ را به ۳ تبدیل نمی‌کند. اتفاقاً این گروه با گروه

$$V_2: (1), \ (12)\ (34), \ (13)\ (24), \ (14)\ (23)$$

که بعکس V_1 ترایاست، یکریخت است. هردوی این گروهها با گروه مرتبهٔ چهار (جدول (iii) صفحهٔ ۱۴) یکریخت‌اند.
مجموعهٔ جایگشتهایی از G که نماد ۱ را تغییر نمی‌دهند یك زیرگروه مانند G_1 تشکیل می‌دهند؛ زیرا جایگشت همانی یقیناً به‌این مجموعه تعلق دارد، همچنین است عکس هرعنصر آن و حاصلضرب هردوتای آنها. G_1 را **پایدارساز** ۱ می‌نامیم. به طریق مشابه پایدارساز یك شیء a، با G_a تعریف می‌شود.

قضیهٔ اصلی ۲۵. یك گروه جایگشتی G از درجهٔ n فقط و فقط وقتی ترایاست که پایدارساز G_1 در G دارای اندیس n باشد.

برهان. (الف) فرض کنیم G ترایا باشد. بنابر فرض، G شامل جایگشتهای

$$\theta_{11}, \ \theta_{12}, \ \cdots, \ \theta_{1n} \qquad (۴۴.۷)$$

است که بترتیب (ازچپ به‌راست) ۱ را به ۱، ۲،...، و n تبدیل می‌کنند. هممجموعه‌های راست

$$G_1\theta_{11}, \ G_1\theta_{12}, \ \cdots, \ G_1\theta_{1n} \qquad (۴۵.۷)$$

متمایزند، زیرا همهٔ عناصر $G_1\theta_{1i}$، ۱ رابه i تبدیل می‌کنند و بنابراین، وقتی‌که $i \neq j$، با عناصر $G_1\theta_{1j}$ مغایرند. باقی می‌ماند ثابت کنیم که (۴۵.۷) فهرستی است کامل از هممجموعه‌ها. فرض می‌کنیم ξ عنصری دلخواه از G باشد که ۱ را به a تبدیل کند. پس $\xi\theta_{1a}^{-1}$، ۱ را ثابت نگاه می‌دارد، یعنی $\xi\theta_{1a}^{-1} \in G_1$. از این‌رو $\xi \in G_1\theta_{1a}$، که ثابت می‌کند که اجتماع هممجموعه‌های (۴۵.۷) تمامی گروه را تشکیل می‌دهد لذا $[G : G_1] = n$.
(ب) بعکس، فرض کنیم G_1 دارای اندیس n و

$$G = G_1\tau_1 \cup G_1\tau_2 \cup \cdots \cup G_1\tau_n$$

یك تجزیهٔ هممجموعه‌ای G نسبت به G_1 باشد. ابتدا مشاهده می‌کنیم که هیچ دوجایگشتی

از جایگشتهای

$$\tau_1, \tau_2, \cdots, \tau_n \qquad (۴۶.۷)$$

اثر واحدی برشیء ۱ ندارند. زیرا فرض کنیم τ_i و τ_j، هردو ۱ را به a بدل کنند. در این صورت $\tau_i\tau_j^{-1}$، ۱ را ثابت نگاه می‌دارد به طوری که $\tau_i\tau_j^{-1} \in G_1$ و بنابراین $G_1\tau_i = G_1\tau_j$ (قضیهٔ ۵، صفحهٔ ۳۷) که غیرممکن است مگر آنکه $i = j$. بنابراین جایگشتهای (۴۶.۷) را می‌توان بترتیبی، به‌جای جایگشتهای (۴۴.۷) اختیار کرد. مناسب آن است که (۴۶.۷) را به‌طریقی مرتب کنیم که تساوی $\theta_{ij} = \tau_i$ $(i = 1, 2, \cdots, n)$ برقرار باشد. بالاخره، اگر a و b زوج دلخواهی از نمادها باشند، $\tau_a^{-1}\tau_b$ عنصر a را به b تبدیل می‌کند. این نکته ثابت می‌کند که G تراياست.

چون مرتبهٔ یك گروه متناهی بر اندیس هریك از زیر گروههایش بخشپذیر است (قضیهٔ اصلی ۳، صفحهٔ ۳۹) قضیهٔ سودمند ذیل حاصل می‌شود.

قضیهٔ ۲۹. مرتبهٔ یك گروه ترایای درجهٔ n، بر n بخشپذیر است.

مفهوم ترایایی را می‌توان تعمیم داد.

تعریف ۱۴. یك گروه G از جایگشتها را **ترایای k تایی** نامیم هرگاه شامل حداقل یك جایگشت θ باشد که یك مجموعهٔ مرتب از k شیء متمایز a_1، a_2، ...، a_k را به یك مجموعهٔ k شیء دیگر b_1، b_2، ...، b_k تبدیل کند (این دو مجموعه ممکن است عناصر مشترکی داشته باشند)؛ یعنی $a_i\theta = b_i$ $(i = 1, 2, \cdots, k)$.

واضح است که اگر G از درجهٔ n باشد، آنگاه $k \leqslant n$. همچنین اگر G ترایای k تایی باشد و $k > l$، آنگاه به‌طریق اولی G ترایای l تایی نیز هست.

وقتی k یکی از اعداد صحیح ۱، ۲، ...، n باشد، گروه S_n ترایای k تایی خواهد بود.

فرض کنیم r عدهٔ مجموعه‌های مرتبی شامل k شیء، منتخب از همهٔ n شیء که G بر آنها اثر می‌کند، باشد. دراین صورت

$$r = n(n-1)\cdots(n-k+1)$$

اکنون فرض کنیم که G ترایای k تایی و H زیر گروهی باشد که هریك از اشیاء

$$1, 2, \cdots, k$$

را تغییر ندهد. با استدلالی مشابه آنچه که در برهان قضیهٔ اصلی ۲۵ به‌کار برده شد می‌توان نشان داد که اندیس H در G برابر r است. و هممجموعه‌های H با r مجموعهٔ k شیء در تناظر یك به یك هستند. لذا قضیهٔ زیر را داریم:

قضیهٔ اصلی ۲۶. مرتبهٔ یك گروه ترایای k تایی درجهٔ n، بر

$$n(n-۱)\cdots(n-k+۱)$$

قابل قسمت است.

به گونه دیگر، می‌توانستیم مفهوم ترایایی چندگانه را با استقراء و با استفاده از ضابطهٔ ذیل گسترش دهیم.

قضیهٔ ۳۰. گروه G ترایای k تایی است هرگاه (الف) G ترایا باشد و (ب) پایدارساز $G_۱$ نسبت به اشیاء ۲، ۳، ...، و n ترایای $(k-۱)$ تایی باشد.

برای مثال، در حالت $A_۴$، که در (۲۸.۷) نشان داده شده است، پایدارساز ۱ عبارت است از

$$G_۱ : \iota,\ (۲۳۴),\ (۲۴۳)$$

لذا $۴ = ۱۲/۳ = [A_۴ : G_۱]$، که مؤید ترایایی $A_۴$ است. اما $G_۱$ برای ۲، ۳، ۴ ترایاست؛ این امر را می‌توان یا مستقیماً تحقیق کرد، یا به‌طریق دیگر، از توجه به‌اینکه پایدارساز ۲ در $G_۱$، مثلاً $G_{۱۲}$، به ι بدل می‌شود و بنابراین اندیس آن در $G_۱$ برابر ۳ است، نتیجه گرفت. چون $G_{۱۲}$ برای اشیاء باقی‌مانده ۳ و ۴ ترایا نیست، نتیجه‌ می‌گیریم که $A_۴$ (دقیقاً) ترایای مضاعف است.

۴۴. گروههای اولیه. فرض کنیم G یک گروه ترایا باشد. همچنین فرض می‌کنیم n شیء که G بر آنها اثر می‌کند بتوانند در آرایه‌ای با r سطر و s ستون $rs = n$ ($۱ < r$، $۱ < s$) چیده شوند. لذا

$$\left.\begin{array}{llll} a_۱, & a_۲, & \cdots, & a_s \\ b_۱, & b_۲, & \cdots, & b_s \\ \cdot & \cdot & \cdots & \cdot \\ k_۱, & k_۲, & \cdots, & k_s \end{array}\right\} \text{(r سطر)} \qquad (۴۶.۷)$$

چنان است که جایگشتهای G یا جای اشیای هر سطر را با جای اشیای همان سطر عوض می‌کنند و یا جای اشیاء یک سطر را با جای اشیای سطر دیگر (بترتیبی) تعویض می‌نمایند. لذا دو شیء که درسطرهای مختلف (۴۶.۷) قرار دارند هرگز به‌اشیای یک سطر تبدیل نمی‌شوند، بعکس دوشیء ازیک‌سطر، براثر G هرگز به‌سطرهای مختلف فرستاده نمی‌شوند. یک گروه ترایا که دارای این‌ویژگی باشد غیراولیه و آرایهٔ (۴۶.۷) یک **دستگاه غیراولیه** نامیده می‌شود. گروهی که برای آن هیچ دستگاه غیراولیه‌ای وجود نداشته باشد گروه اولیه نامیده می‌شود. باید متذکر شد که این‌مفهوم فقط برای گروههای ترایا به‌کار می‌رود.

مثال ۱. گروه دوری $G = \mathrm{gp}\{(۱۲۳۴)\}$، که ازجایگشتهای

$$\iota,\ (۱۲۳۴),\ (۱۳)(۲۴),\ (۱۴۳۲)$$

تشکیل شده است، غیراولیه و دارای دستگاه غیراولیهٔ

$$\begin{array}{c|}۱۳\\ ۲۴\end{array}$$

است. در واقع، چهار جایگشت G این دستگاه را بترتیب به

$$\begin{array}{c|}۱۳\\ ۲۴\end{array},\quad \begin{array}{c|}۲۴\\ ۳۱\end{array},\quad \begin{array}{c|}۳۱\\ ۴۲\end{array},\quad \begin{array}{c|}۴۲\\ ۱۳\end{array}$$

بدل می‌کنند.

مثال ۲. یك گروه ممکن است دارای بیش از یك دستگاه غیراولیه باشد. لـذا در حالت گروه چارینه

$$\iota,\ (۱۲)(۳۴),\ (۱۳)(۲۴),\ (۱۴)(۲۳)$$

هریك از آرایه‌های

$$\begin{array}{c|}۱۲\\ ۳۴\end{array},\quad \begin{array}{c|}۱۳\\ ۲۴\end{array},\quad \begin{array}{c|}۱۴\\ ۲۳\end{array}$$

می‌توانند به‌عنوان یك دستگاه غیراولیه به‌کار روند.

یك گروه ترایای مضاعف همواره گروه اولیه است. زیرا یك گروه ترایای مضاعف اجباراً شامل جایگشتی می‌شود که زوج $a_۱$ و $a_۲$ را به‌زوج $a_۱$ و $b_۲$ می‌فرستد. ولی این امر با وجود یك دستگاه غیراولیه همچون (۴۶.۷) سازگاری ندارد.

بویژه کلیهٔ گروههای متقارن S_n اولیه هستند.

۴۵. گروههای تقارن. فرض‌کنیم Σ مجموعه‌ای متناهی یا نامتناهی از نقاط واقع در یك فضای اقلیدسی سه‌بعدی به مبدأ o باشد. هردوران حـول یك محور مار بر o کـه Σ را به‌خودش تبدیل‌کند یك تقارن Σ نسبت به o خوانده می‌شود. از بخش ۶ فصل ۱ (صفحهٔ ۲۵) نتیجه می‌شود که تقارنهای Σ بر اثر ترکیب نگاشتها یك گروه تشکیل می‌دهند. هرگاه هیچ دوران غیربدیهی که Σ را برخودش منطبق‌کند وجود نداشته باشد، آنگاه گروه‌تقارن Σ به‌تبدیل همانی بدل می‌شود.

در این بخش، گروههای تقارن را برای بعضی از شکلبندیهای هندسی از جمله پنج جسم منتظم مورد بحث قرار می‌دهیم. گروههایی که به‌دست می‌آیند از اول بر ما معلوم‌اند.

(الف) گروههای دووجهی. یك ورقهٔ مسطح را که به شکل یك چند ضلعی منتظم با n رأس باشد درنظر می‌گیریم، و فرض می‌کنیم که هر دوطرف ورقه کاملاً شبیه هم باشند (شکل ۳ حالت $n=6$ را نشان می‌دهد). محورهای مختصات را به‌طریقی‌انتخاب می‌کنیم که ورقهٔ ما درصفحهٔ (x, y) قرارگیرد و مرکز آن برمبدأ منطبق شود و محور x ها از رأس خاصی که آن را با ۱ شماره‌گذاری می‌کنیم بگذرد. $2n$ دوران، ازجمله عمل‌همانی، وجود دارندکه ورقه را برخودش منطبق می‌کنند در وهلهٔ اول، اگر α معرف دورانی‌حول محور z به‌اندازهٔ $2\pi/n$ باشد، n عمل تقارن:

$$\iota(=\alpha^0),\ \alpha,\ \alpha^2,\ \ldots,\ \alpha^{n-1}$$

خواهیم داشت که

$$\alpha^n=\iota \qquad (۴۷.۷)$$

یك عمل تقارن دیگر، مانند β، از پشت‌و روکردن ورقه تشکیل می‌شود. می‌توان این را با دورانی حول محور x به‌اندازه π انجام داد (محورهـای مختصات در فضا ثـابت فرض می‌شوند). واضح است که

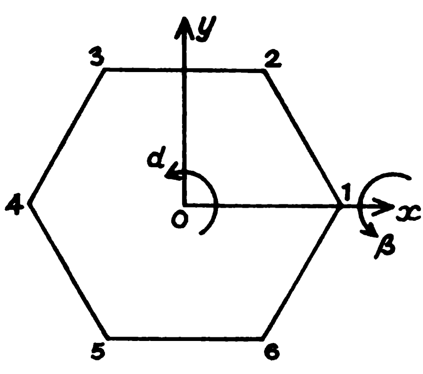
$$\beta^2=\iota \qquad (۴۸.۷)$$

زیرا β^2 متناظر دورانی به اندازهٔ 2π و بنابراین با عمل‌همانی برابر است. اما $2n$ عمل

$$\alpha^k\beta^l(k=0,\ 1,\ \ldots,\ n-1;\ l=0,\ 1)$$

کلیهٔ تقارنهای این‌ورقه را تشکیل‌می‌دهند؛ زیرا این تبدیلات هررأس را با پشت‌و روکردن ورقه، یا بدون پشت‌و روکردن آن به‌موضع هر رأس دیگرمی برد. برای‌آنکه ساختار گروه تقارن معین شود مجبوریم بین عملهای α و β رابطه‌ای پیدا کنیم. یك بررسی‌سادهٔ هندسی نشان می‌دهد که

$$\alpha\beta=\beta\alpha^{-1}$$



شکل ۳

که به‌موجب (۴۸.۷)، معادل است با

$$(\alpha\beta)^{۲}=\iota \qquad (۴۹.۷)$$

(به‌خواننده توصیه می‌شود که با رسم نمودارهایی مشابه با نمودارهای صفحهٔ ۱۵ این‌امر را تحقیق کند). نتیجهٔ خود را می‌توانیم چنین خلاصه کنیم:

گروه تقارن یك ورقهٔ n ضلعی منتظم همان‌گروه دووجهی مرتبهٔ $۲n$ است که با روابط معرف

$$\alpha^{n}=\beta^{۲}=(\alpha\beta)^{۲}=\iota \qquad (۵۰.۷)$$

داده می‌شود.

یادآوری می‌کنیم که این گروه درفصل ۲، تمرین ۷ (صفحهٔ ۶۱) ذکرشده بود.

نظر ما، به‌دست آوردن عباراتی تحلیلی برای عملهای گروه دووجهی است. فرض کنیم x متغیری باشد که اعداد صحیح ۱، ۲، ... و n را اختیارکند و معرف رئوس ورقه بترتیب درخلاف جهت حرکت عقربه‌های ساعت باشد. عمل α بدوسیلهٔ همنهشتی

$$x\alpha\equiv x+۱\,(\operatorname{mod} n) \qquad (۵۱.۷)$$

بیان می‌شود. باز، اگر بنویسیم $x=۱+z$، آنگاه $۱-z$ نگارهٔ x بر اثر β خواهد شد. لذا داریم

$$x\beta\equiv ۲-x\,(\operatorname{mod} n) \qquad (۵۲.۷)$$

کلیهٔ روابط بین عناصر مولد α و β را می‌توان از (۵۱.۷) و (۵۲.۷) به‌دست آورد؛ فی‌المثل، داریم

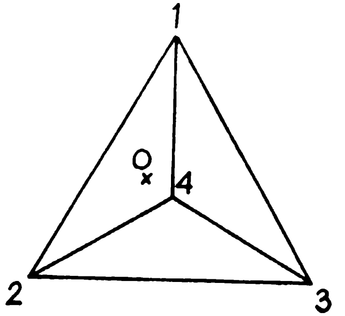
$$x\alpha\beta\equiv(x+۱)\beta\equiv ۲-(x+۱)\equiv ۱-x$$

$$x(\alpha\beta)^{۲}\equiv(۱-x)\alpha\beta\equiv ۱-(۱-x)\equiv x$$

که مؤید رابطهٔ $(\alpha\beta)^{۲}=\iota$ است.

(ب) گروه چهاروجهی. این نامی است که به‌گروه تقارن یك چهاروجهی منتظم که به‌آزادی حول مبدأش o دوران می‌کند، داده شده است. دوازده دوران وجود دارند که چهاروجهی را برخودش منطبق می‌کنند. ابتدا چهارعملی راکه رأس ۱ را به‌موضع هریك از رئوس ۱، ۲، ۳ یا ۴ می‌برند انتخاب می‌کنیم. بعد از آن،هرگاه ۱ موضع x را اشغال کند، جسم می‌تواند حول خط ox به‌اندازهٔ زاویهٔ ۰ یا $۲\pi/۳$ و یا $۴\pi/۳$ دوران کند، که در نتیجهٔ آن سه‌وجهی که در x متلاقی‌اند به‌طور دوری با هم تعویض می‌شوند. لذا درمجموع $۱۲=۳\times۴$ عمل خواهیم داشت.

عملهای این گروه چهاروجهی به‌طریقی چهار رأس را با هم‌تعویض می‌کنند؛ بنابراین این‌گروه با یك زیرگروه از $S_{۴}$ یکریخت است. وقتی که یك رأس ثابت باشد، سه رأس



شکل ۴

باقیمانده، یعنی a، b، c، می‌توانند به‌طور دوری تعویض‌شوند. از این‌رو گروه چهاروجهی کلیهٔ دورهای (a, b, c) را دربرمی‌گیرد. بنابرقضیهٔ ۲۷، این دورها گروه تناوبی A_4 را تولید می‌کنند. چون هردو گروه ازمرتبهٔ ۱۲ هستند، پس ثابت‌کرده‌ایم که گروه چهاروجهی با A_4 یکریخت است.

(ج) گروه هشت (شش) وجهی. مراکز وجوه یک هشت‌وجهی منتظم را می‌توان به عنوان رئوس یک مکعب (شش‌وجهی) درنظر گرفت، و بعکس در هرمکعب می‌توان یک هشت‌وجهی محاط کرد که رئوس آن برمراکز وجوه مکعب قرار داشته باشند. لذا این دوجسم دارای یک تقارن هستند. یعنی اگر یکی را به خودش تبدیل کنیم، دیگری نیز به‌خودش بدل خواهد شد. بنابراین گروههای هشت‌وجهی و شش‌وجهی یکی هستند، گو آنکه فقط نام اول متداول است. در بحث حاضر ساده‌تر می‌بینیم که تقارنهای مکعب را به‌جای تقارنهای هشت‌وجهی مورد مطالعه قرار دهیم.

ملاحظه می‌کنیم که گروه مکعب دارای ۲۴ عمل است. برای آنکه، در وهلهٔ اول، یک‌رأس مفروض می‌تواند به‌وضع هریک از هشت رأس درآید. وقتی که این‌کار انجام‌شد، این جسم می‌تواند حول قطری که از این رأس می‌گذرد به‌اندازهٔ زاویه‌های ۰، $2\pi/3$، و $4\pi/3$ دوران کند و درمجموع $8 \times 3 = 24$ دوران، ازجمله دوران همانی‌را به‌دست‌دهد.

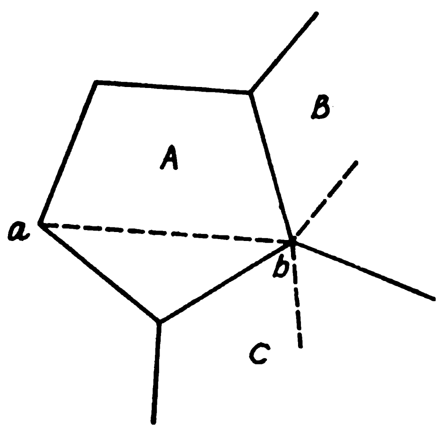
مکعب دارای چهارقطر (خطوط ماربر o که یک زوج از رئوسی راکه متقاطرهستند بههم وصل می‌کنند) است. وقتی که مکعب به‌خودش تبدیل شد، این چهار قطر به‌طریقی با هم تعویض می‌شوند. لذا گروه مکعب به‌طور همریخت به S_4 نگاشته می‌شود. حال، هستهٔ این همریختی را تعیین می‌کنیم. هرگاه قطر خاصی به‌خودش تبدیل شود، آنگاه یا این‌قطر برمحور دوران منطبق است و یا دوسر آن با هم تعویض می‌شوند؛ درحالت اخیر، محور دوران با این قطر زاویه قائمه می‌سازد و زاویه دوران برابر π است. دورانی که به‌هسته متعلق باشد هر یک از چهار قطر را به خودش تبدیل خواهدکرد. بنابراین‌محور این دوران اجباراً با حداقل سه تا از قطرها زاویه قائمه می‌سازد. واضح است که این‌شدنی نیست، مگر آنکه‌عمل همان عمل همانی باشد. از این‌رو هستهٔ زیرگروه بدیهی بوده وگروه هشت وجهی

با S_4 یکریخت است.

(د) گروه بیست (دوازده) وجهی. اکنون به‌دو تا آخرین چند وجهی منتظم می‌پردازیم، و مشاهده می‌کنیم کــه بیست وجهی و دوازده وجهی دارای یك تقارن هستند. زیرا مراکز وجوه یك بیست‌وجهی را می‌توان به‌هم وصل کرد تا یك دوازده‌وجهی منتظم تشکیل شود؛ و، بعکس، مراکز دوازده‌وجه یك دوازده‌وجهی را می‌توان به‌عنوان رئوس یك بیست‌وجهی درنظر گرفت. بدین‌ترتیب گروههای بیست وجهی و دوازده وجهی یکی هستند. هــر یك از این اجسام را می‌توان برای مطالعهٔ این گروه مورد استفاده قــرارداد. ما دوازده‌وجهی را انتخاب می‌کنیم.

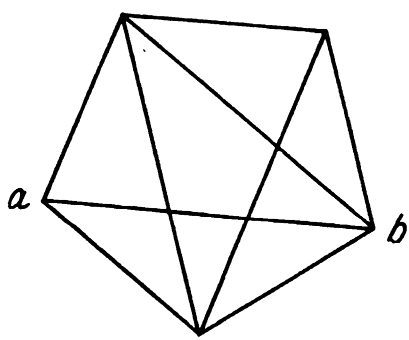
ابتدا متذکر می‌شویم که‌گروه دوازده‌وجهی متشکل از ۶۰ عمل است. زیرا هر رأس را می‌توان به‌وضع هریك از بیست رأس درآورد. وقتی‌که این رأس به‌وضع نهایی‌خود بــرسد، جسم را می‌توان حول قطر مار بر آن رأس دوران داد. این عمل موجب تعویض دوری سه‌وجهی می‌شود که در دوسر این‌قطرهمدیگر را تلاقی می‌کنند. لذا زوایای ممکن دوران‌عبارت‌اندازه، $2\pi/3$، $4\pi/3$ یا 3. ازآنجا نتیجه‌می‌شود که درمجموع $3 \times 20 = 60$ عمل، ازجمله عمل همانی، وجود داردکه دوازده‌وجهی را برخودش منطبق می‌کند.

بعد ما سعی می‌کنیم یك نمایش جایگشتی‌صادق از گروه دوازده‌وجهی پیدا می‌کنیم. مسئله منجر به این می‌شود کــه این‌گروه با زیرگروهی از S_5 یکریخت است. لــذا وقتی دوازده‌وجهی دوران می‌کند و برخودش منطبق‌می‌شود، ۵ شیء را که باهم تعویض می‌شوند شرح خواهیم داد. به‌موجب ساختمان‌کلاسیك اقلیدس می‌توان یك مکعب را به‌طریق ذیل دریك دوازده‌وجهی محاط کرد: یك وجه مانند A را انتخاب و یك قطرآن، مثلاً ab، را رسم می‌کنیم (قطرخطی است کــه دو رأس غیرمجاور از یك وجه را به‌هم وصل می‌کند). درنقطهٔ b، وجه A به دووجه دیگر، مثلاً B و C، برمی‌خورد. سپس می‌توان نشان داد که



شکل ۵

در هریك از دو وجه B و C دقیقاً یك‌قطر وجود دارد کـه با ab زاویهٔ قائمه می‌سازد، و این دو قطر جدید نیز برهمدیگر عمودند. اکنون همین شیوه ساختمان با قطرهای موجود در وجوه مذکور B و C تکرار می‌شود؛ در سر دیگر هریك از این اقطار دوقطر دیگر در وجوه مجاور تعیین می‌کنیم تـا یـك‌کنج سه قائمه ساخته شود؛ و همینطور عمل را ادامه می‌دهیم. (معتبربودن این احکام با بررسی یك مدل به‌بهترین وجه تحقیق می‌شود). لذا، با شروع از ab، ما درهریك از دوازده وجه یك قطرمنحصر به‌فرد جدا کرده‌ایم و این اقطار یالهای یك مکعب محاط در دوازده‌وجهی را تشکیل می‌دهند. اما هر وجه دارای پنج قطر است (شکل ۶)، وما می‌توانستیم‌ساختمان فوق‌الذکر را با هریك‌از این‌اقطار شروع کنیم. لذا پنج مکعب می‌تواند محاط شود و این اشیاء در هرعمل تقارن از دوازده‌وجهی با هم عوض می‌شوند. بنابراین ما یك نمایش جایگشتی از درجهٔ پنج پیدا کرده‌ایم. بعلاوه، این نمایش صادق است؛ یعنی، هردورانی‌که هر یك از این پنج مکعب را برخود منطبق سازد، لزوماً به‌عمل همانی تبدیل می‌شود (مـا از خواننده می‌خواهیم کـه این حقیقت را بدون برهان‌قبول کند). از اینجا نتیجه می‌شود که گروه دوازده‌وجهی با زیر گروهی‌از S_5 یکریخت است؛ چون انـدیس آن برابر دو است، بـاید یك زیر گروه نرمال باشد (مطلب د، صفحهٔ ۷۵)، از اینجا و از قضیهٔ ۲۸ نتیجه می گیریم کـه گروه دوازده (بیست) وجهی بـا A_5 یکریخت است.



شکل ۶

تمرین

(۱) نشان دهید

$$(ab\ldots lx)(x\alpha\beta\ldots\lambda)=(ab\ldots l\alpha\beta\ldots\lambda x)$$

که a، b، . . . ، l، x، α، β، . . . ، λ نمادهایی متمایزند.

(۲) ثابت کنید هرگاه یك‌جایگشت درجهٔ n، حاصلضرب r دور دوبه‌دو ازهم‌جدا (ازجمله

دورهای مرتبهٔ ۱) باشد، زوج یا فرد است برحسب اینکه $n-r$ زوج یا فرد باشد.

(۳) نشان دهید که S_n را می‌توان به‌وسیلهٔ ترانهشهای

$$(۱۲), (۲۳), \ldots, (n-۱, n)$$

تولید کرد.

(۴) نشان دهید که S_n می‌تواند به‌وسیلهٔ جایگشتهای

$$\gamma = (۱۲\cdots n) \quad و \quad \tau = (۱۲)$$

تولید شود.

(۵) ثابت کنید که یك جایگشت منظم را می‌توان برحسب توانی از یك دور بیان کرد، و بعکس، اگر $\gamma = (۱۲\ldots m)$، آنگاه γ^s یك جایگشت منظم است متشکل از d دور درجهٔ r، که در آن $d = (m, s)$ و $r = m/d$.

(۶) ثابت کنید که مرکزساز $\gamma = (a_۱, a_۲, \ldots, a_n)$ در S_n از ι، γ، $\gamma^۲$، ...، $\gamma^{n-۱}$ تشکیل شده است.

(۷) ثابت کنید که وقتی $n > ۲$، مرکزساز $\lambda = (a_۱, a_۲, \ldots, a_{n-۱})$ در S_n از ι، λ، $\lambda^۲$، ...، $\lambda^{n-۲}$ تشکیل شده است.

(۸) ثابت کنید که وقتی $n > ۲$، مرکز S_n فقط از جایگشت همانی تشکیل شده است.

(۹) **نمایش منظم چپ** از یك گروه G چنین تعریف می‌شود: به‌ازای یك عنصر ثابت u از G یك جایگشت λ_u وجود دارد که طبق قاعدهٔ $a\lambda_u = u^{-۱}a$ $(a \in G)$ برعناصر G اثر می‌کند. تحقیق کنید کـه (الف) $\lambda_u\lambda_v = \lambda_{uv}$؛ (ب) $\lambda_u = \iota$ فقط و فقط وقتی که $u = ۱$؛ (ج) $\lambda_u\rho_x = \rho_x\lambda_u$، کـه تعریف ρ_x در (۴۲۰۷) آمده است؛ (د) اگر θ جایگشتی از عناصر G تعویض‌پذیر با همهٔ λ_uها بـاشد، آنگاه بـه‌ازای مقداری از x، $\theta = \rho_x$، و هرگاه η با همهٔ ρ_xها تعویض‌پذیر باشد، آنگاه به‌ازای مقداری از u، $\eta = \lambda_u$.

(۱۰) ثابت کنید که اگر G یك گروه ساده از مرتبهٔ ۱۶۸ و H یك زیرگروه حقیقی G باشد، آنگاه $[G : H] \geqslant ۶$.

(۱۱) گروه تقارن یك ورقهٔ مستطیل شکل (نه مربع شکل) را به‌دست آورید.

(۱۲) ثابت کنید هرگاه g عنصر از یك گروه ترایـای درجه n به‌صورت حـاصلضربهای دورهای دوبه‌دو منفصل با مراتب بزرگتر از یك نوشته شده باشد، آنگاه این دورها درمیان خود $g(n-۱)$ حرف دارند.

۸

قضیه‌های سیلو

۴۶. زیرگروههای اول ـ توان. قضیهٔ اصلی لاگرانژ بیان می‌داردکه هرگاه G گروهی متناهی ازمرتبهٔ g باشد، آنگاه مرتبهٔ یك زیرگروه G باید g را عادکند. عکس این قضیه برقرار نیست؛ چون دیده‌ایم(مثال‌صفحهٔ ۱۵۸)گروههایی وجود دارندکه زیرگروههایی ندارند. که متناظر با برخی از مقصوم‌علیه‌های g باشند. با این‌حال، هرگاه p^b توانی از عدد اول p باشد به‌قسمی‌که p^b مقصوم‌علیه g باشد،آنگاه G دارای‌حداقل یك زیرگروه ازمرتبهٔ p^b خواهد بود. این‌حقیقت قابل‌توجه را درسال۱۸۷۲ ریاضیدان نروژی ل. سیلو کشف‌کرد. این قضیه نتایج بسیار مؤثری درنظریهٔ‌گروهها دارد و یکی ازگیراترین مثالها را در ارتباط ظریف بین ویژگیهای حسابی (عـددی) و ویژگیهای ساختاری یك گـروه فراهم می‌سازد. براهین‌چندی از قضیه‌های مشهور ل. سیلو را می‌توان درفرهنگ ریاضی یافت. ما دراینجا* برهان زیبایی راکه منسوب به ه. ویلنت(۱۹۵۹) است عرضه می‌کنیم؛ در این برهان اصول اولیه به‌کار بـرده شده و تنها برخی از اندیشه‌های مقدماتی در باب جایگشتها مورد استفاده قرارگرفته است.

قضیهٔ اصلی ۲۷. فرض کنیم G گروهی متناهی از مرتبهٔ g و p عدد اولی باشد که p^b عدد g را عاد کند، b عدد صحیح مثبتی است. دراین صورت G دارای m زیرگروه از

---

* توصیف ما به‌پیروی از P. Huppert ، گـروههای متناهی I ، (Springer ، ۱۹۶۷، صفحهٔ ۳۳) صورت‌گرفته است.

مرتبهٔ p^b است، که m عدد صحیح مثبتی است که در رابطهٔ $m=1(mod\ p)$ صدق می‌کند.

برهان. (۱) می‌نویسیم

$$g=p^b z \qquad (۱.۸)$$

که z عدد صحیح مثبتی است که لزومی ندارد با p متباین باشد. فهرست کامل $\mathcal{K}$ از همهٔ زیرمجموعه‌هایی از G را که شامل p^b عنصراند تشکیل می‌دهیم. بدین گونه هرگاه n تا ازاین زیرمجموعه‌ها وجود داشته باشد، می‌نویسیم

$$\mathcal{K}: K_1, K_2, \cdots, K_n \qquad (۲.۸)$$

درحقیقت، n مساوی‌ضریب دوجمله‌ای $\binom{g}{p^b}$ است؛ اما این آگاهی ازاین به‌بعد موردنیاز نخواهد بود. حکم قضیه این است که دست‌کم یکی ازاین زیرمجموعه‌های (۲.۸) یك زیرگروه است.

یك زیر مجموعهٔ K فقط و فقط زمانی به $\mathcal{K}$ متعلق است که با نمادگذاری صفحهٔ ۳۴ داشته باشیم

$$|K|=p^b$$

هرگاه x عنصری از G باشد، آنگاه $|Kx|=|K|$. ازاین‌رو Kx نیز به $\mathcal{K}$ تعلق خواهد داشت. درواقع، نگاشت

$$K_i \to K_i x \quad (i=1, 2, \cdots, n)$$

یك جایگشت از $\mathcal{K}$ تشکیل می‌دهد. دراین مقام گوییم که G بر $\mathcal{K}$ اثر می‌کند. با درنظر گرفتن این عمل می‌توانیم یك‌رابطهٔ هم‌ارزی، مطابق‌آنچه که ذیلاً می‌آید، در $\mathcal{K}$ تعریف کنیم؛ زیرمجموعه‌های K_i و K_j را هم‌ارز نامیم، هرگاه عنصری مانند x از G وجود داشته باشد به‌طوری که $K_i=K_j x$. خواننده درتحقیق اینکه بنداشتهای معمولی یك‌رابطهٔ هم‌ارزی برقرارند مشکلی نخواهد داشت. درنتیجه، $\mathcal{K}$ به‌دسته‌های هم‌ارزی دو به‌دو ازهم جدا، که آنها را در این مبحث مدار می‌نامیم، افراز می‌شود. بدین گونه مدار K، که آن را به $o(K)$ نشان می‌دهیم، مشتمل برهمهٔ زیرمجموعه‌های Kx $(x\in G)$ است. وقتی x در G تغییر می‌کند، درحالت کلی، هرعنصر مدار چندین مرتبه به‌دست می‌آید. تعداد زیرمجموعه‌های متمایز $o(K)$ به $|o(K)|$ نشان داده می‌شود. پس تجزیهٔ $\mathcal{K}$ به مدارها به‌صورت

$$\mathcal{K}=o(K)\cup o(K')\cup o(K'')\cup \cdots \qquad (۳.۸)$$

بیان می‌شود که درآن K، K'، K''، ... مجموعه‌ای ازنماینده‌های مدارهاست. با شمارش عناصر هرطرف به‌دست می‌آوریم

$$n=|o(K)|+|o(K')|+|o(K'')|+\cdots \qquad (۴.۸)$$

(۲) اینك یکی از مدارها، مثلاً $o(K)$، را با جزئیات بیشتری مورد مطالعه وتحقیق قرارمی‌دهیم. فرض کنیم S پایدارساز K تحت عمل G باشد، یعنی

$$S=\{u \in G \mid Ku=K\}$$

خواننده به‌آسانی می‌تواند تحقیق کند (صفحهٔ ۱۵۸ ملاحظه شود) که S یك‌زیرگروه G است. فرض کنیم که

$$G=\bigcup_{i=1}^{r} St_i \quad (t_1=1)$$

تجزیهٔ هممجموعه‌ای‌راست G نسبت به S باشد. ادعا می‌کنیم که $o(K)$ از زیرمجموعه‌های

$$Kt_1, Kt_2, \ldots, Kt_r \tag{۵.۸}$$

تشکیل‌شده است. بدیهی‌است که همهٔ این مجموعه‌ها به $o(K)$ تعلق‌دارند، و ازهم‌متمایزند؛ زیرا اگر $Kt_i=Kt_j$،‌نتیجه‌می‌شودکه $Kt_it_j^{-1}=K$،یعنی $t_it_j^{-1} \in S$ و بنا براین $St_i=St_j$، که ایجاب می‌کند $j=i$. درمرحلهٔ بعد،گوییم هرعنصر دلخواهی از $o(K)$ به‌صورت Kx است. هرگاه x درهممجموعهٔ St_i واقع باشد. داریم $x=ut_i$ کـه درآن $u \in S$، و از این‌رو $Kx=Kut_i=Kt_i$. بدین‌گونه ثابت‌کرده‌ایم که

$$|o(K)|=[G:S] \tag{۶.۸}$$

اطلاع بیشتردر مورد S را می‌توان از این واقعیت که عدد اصلی K به‌صورت عددی است اول‌ـتوان به‌دست آورد. ویژگی معرف پایدارساز را می‌توان به‌وسیلهٔ معادلهٔ

$$KS=K$$

که‌آن را به‌صورت رابطه‌ای بین زیرمجموعه‌های G تلقی‌می‌کنیم، بیان‌کرد. دقیقتر بگوییم اگر $K=v_1 \cup v_2 \cup v_3 \cup \ldots$، آنگاه داریم

$$K=v_1S \cup v_2S \cup v_3S \cup \cdots \tag{۷.۸}$$

لذا K اجتماع هممجموعه‌های چپ S است. می‌دانیم هر دوتا از این هممجموعه‌ها یا متمایزند ویا یکی‌هستند وهریك دارای $|S|$ عنصرمی‌باشند. لذا هرگاه‌تعداد هممجموعه‌های متمایز در (۷.۸) برابر f باشد، داریم

$$p^b=f|S|$$

از اینجا نتیجه می‌شودکه $|S|$ توانی از p است، مثلاً

$$|S|=p^c \tag{۸.۸}$$

که درآن $c \leqslant b$. اما دوحالت را باید ازهم تمیز داد.

(الف) $|S| = p^b$. ولی هنوز نمی‌دانیم که آیا این حالت می‌تواند رخ دهد یا نه. اما اگر این حالت رخ دهد، آنگاه داریم

$$|o(K)| = \frac{g}{p^b} = z$$

که z در (۱.۸) تعریف شده است. چون حالا $|S|$ بزرگترین مقدارش را اختیار می‌کند، می‌توانیم $o(K)$ را یك مدار مینیمال اصطلاح کنیم. چون بنابر فرض کنونی، K و S دارای یك عدد اصلی‌اند، از (۸.۷) نتیجه می‌گیریم که K به یك هممجموعهٔ تنها بدل می‌شود، مثلا

$$K = vS \quad (v \in K)$$

روشن است که زیرمجموعهٔ

$$H = Kv^{-1} = vSv^{-1}$$

متعلق به $o(K)$ و بنابراین یك زیرگروه است، یعنی گروهی که با S مزدوج است. لذا ما به این نتیجه رسیده‌ایم که هرمدار مینیمال شامل حداقل یك زیرگروه است. چون $|H| = p^b$، نتیجه می‌شود که

$$[G : H] = z = |o(K)|$$

فرض کنیم

$$Hw_1, \; Hw_2, \; \cdots, \; Hw_z \tag{۹.۸}$$

هممجموعه‌های H در G باشند. هریك از این z هممجموعه به $o(K)$ تعلق دارد؛ زیرا که H به آن تعلق دارد؛ و چون این هممجموعه‌ها متمایزند، تمام $o(K)$ را تشکیل می‌دهند. اما می‌دانیم که دقیقاً یکی از این هممجموعه‌ها، یعنی H، زیرگروه است. از این رو نشان داده‌ایم که یك مدار مینیمال شامل یك، و فقط یك زیرگروه G است.

(ب) $|S| = p^c < p^b$. در این حالت مدار $o(K)$ مینیمال نیست و

$$|o(K)| = \frac{g}{p^c} = zp^{b-c}$$

از این رو

$$|o(K)| \equiv ۰ (\bmod pz) \tag{۱۰.۸}$$

یك مدار غیرمینیمال نمی‌تواند شامل یك زیرگروه باشد؛ زیرا درغیراین‌صورت می‌توانیم این زیرگروه را به‌عنوان یك‌مولد $o(K)$ اختیار کنیم، ولذا بی‌آنکه‌خللی به کلیت استدلال وارد شود می‌توانیم فرض کنیم که خود K یك گروه باشد. دراین‌صورت K در پایدارسازش قرار خواهدگرفت، زیرا $KK = K$ ((۶.۲) صفحهٔ ۳۵ ملاحظه شود). لذا $|S| \geqslant |K| = p^b$، که با فرض (ب) ناسازگار است.

(۳) اکنون به (۴.۸) باز می‌گردیم و جملات مینیمال‌را، درصورت وجود، از بقیه جدا می‌کنیم. در هرمدار مینیمال دقیقاً یك زیرگروه وجود دارد؛ و مدارهای متمایز شامل زیرگروههای متمایزند، زیرا مدارها متمایزند. برای هر مدار مینیمال عدد اصلی $|o(K)|$ برابر z و عدهٔ چنین مدارهایی برابر m است، که m عدد صحیحی است‌که درقضیهٔ اصلی تعریف شده است. (با این‌حال متذکر می‌شویم‌که در این مرحله هنوز نمی‌دانیم‌که آیا m مثبت است یا نیست.) بنابراین کل سهامی‌که از همهٔ مدارهای مینیمال به (۴.۸) مربوط می‌شود برابر mz است. ازآنجاکه، بنابر (۱۰.۸)، هریك ازجملات باقیمانده در (۴.۸) بر pz بخشپذیر است، می‌توانیم وضع را با همنهشتی

$$n \equiv mz (\mathrm{mod}\ pz) \qquad (۱۱.۸)$$

خلاصه‌کنیم. این یك جنبهٔ مهم این برهان است‌که عدد n، که درصفحهٔ ۱۷۵ تعریف شد، فقط بستگی به‌مرتبهٔ‌گروه G دارد نه به‌ساختار آن. از این‌رو، n برای همهٔ گروههای از مرتبهٔ $p^b z$ یکی‌است، درحالی‌که m برای یك n ثابت تغییرمی‌کند. بنابراین‌باید (۱۱.۸) را صریحاً چنین بنویسیم

$$n = m_G z + k_G pz$$

که درآن m_G و k_G اعداد صحیحی هستندکه به G بستگی دارند. برای آنکه اطلاعی درباب n به‌دست‌آوریم این نتیجه را برای‌گروه دوری C از مرتبهٔ $p^b z$ به‌کار می‌بریم. به‌استناد قضیهٔ اصلی ۴ (صفحهٔ ۴۱) می‌دانیم که C دقیقاً یك‌زیرگروه ازمرتبهٔ p^b دارد. بنابراین $m_C = ۱$ و لذا

$$n = z + k_C pz$$

ازمساوی قراردادن دوعبارتی‌که برای n پیدا کردیم خواهیم داشت

$$z + k_C pz = m_G z + k_G pz$$

از اینجا با تقسیم دوطرف تساوی بر z، خواهیم داشت

$$m_G \equiv ۱ (\mathrm{mod}\ p)$$

و این همان چیزی است‌که ادعا شده بود.

۴۷. قضیه‌های سیلو. معمولاً نتایج سیلو درضمن سه قضیهٔ اصلی عرضه می‌شوند که ما آنها را در این بخش بیان می‌کنیم.

قضیهٔ اصلی ۲۸. (اولین قضیهٔ اصلی سیلو): هرگاه p^a بزرگترین توانی از عدداول p باشد که مرتبهٔ گروه G را عاد می‌کند، آنگاه G دارای حداقل یك زیرگروه از مرتبهٔ p است.

برهان. این یك حالت خاص قضیهٔ اصلی ۲۷ است. این قضیه متناظر با بزرگترین مقدار ممکن برای نمای b است.

تعریف ۱۵. فرض کنیم G گروهی متناهی از مرتبهٔ g باشد. فرض کنیم $g = p^a g'$، که p عددی است اول و $(g', p) = 1$. در این صورت هر زیرگروه G از مرتبهٔ p^a را یك **pـگروه سیلوی G** می‌نامند.

به ازای یك عدد اول، یك گروه G ممکن است بیش از یك گروه سیلو داشته باشد. در واقع، هرگاه P زیرگروهی از مرتبهٔ p^a و x عنصر دلخواهی از G باشد، $x^{-1}Px$ نیز یك زیرگروه از مرتبهٔ p^a است. به‌عبارت دیگر، مزدوج یك گروه سیلو نیز یك گروه سیلو است. البته لزومی ندارد که گروههای مزدوجی متمایز باشند اما قضیهٔ بعدی به‌ما می‌گوید که هیچ گروه سیلوی دیگری وجود ندارد.

قضیهٔ اصلی ۲۹ (دومین قضیهٔ اصلی سیلو). همهٔ گروههای سیلوی G که متناظر با یك عدد اول هستند با یکدیگر در G مزدوج‌اند.

برهان. همچون تعریف ۱۵، قرار می‌دهیم $|G| = g = p^a g'$، که‌در آن $(g', p) = 1$. فرض کنیم A و B دو زیرگروه از مرتبهٔ p^a باشند. از تجزیهٔ مضاعف G نسبت به A و B (قضیهٔ اصلی ۶، صفحهٔ ۶۵) استفاده می‌کنیم، لذا درحالت‌کنونی

$$G = At_1B \cup At_2B \cup \cdots \cup At_rB$$

$$g = p^{2a}\sum_{i=1}^{r} d_i^{-1} \qquad (۱۲.۸)$$

$$d_i = |t_i^{-1}At_i \cap B| \qquad (۱۳.۸)$$

از تقسیم سراسر (۱۲.۸) بر p^a به‌دست می‌آوریم

$$g' = p^a\sum_{i=1}^{r} d_i^{-1} \qquad (۱۴.۸)$$

اما d_i مرتبهٔ یك زیرگروه B است و لذا باید با توانی نامنفی از p برابر باشد. از این‌رو هرجملهٔ (۱۴.۸) یا برابر یك است و یا برابر توانی از p با نمای مثبت. اما g' بر p بخشپذیر نیست. بنابراین حداقل یکی از جملات سمت راست باید مساوی یك باشد، مثلاً $p^a d_j^{-1} = 1$، یعنی $d_j = p^a$. پس داریم

$$p^a = |t_j^{-1}At_j \cap B|$$

چون گروههای $t_j^{-1}At_j$ و B هردو از مرتبهٔ p^a هستند، اشتراك آنها فقط وقتی می‌تواند از

مرتبهٔ p^a باشد که این گروهها یکی باشند. لذا

$$B = t_j^{-1} A t_j$$

یعنی، همان گونه که می‌خواستیم ثابت کنیم، A و B مزدوج هستند.

فرع ۱. یك گروه متناهی G متناظر بـا یك عدد اول مفروض p فقط و فقط وقتی دارای یك گروه سیلوی یکتای P است که P در G نرمال باشد.

برهان. شرط یکتایی با این حکم که به‌ازای هـر x از G، تساوی $x^{-1}Px = P$ برقرار است هم‌ارز است؛ اما این بدان‌معنی است که P یك زیر گروه نرمال است.

در مورد گروههای آبلی متناهی، گروههای سیلو لزوماً یکتا هستند. مفهوم یك گروه سیلو بامفهوم p-امین مؤلفهٔ اولیهٔ (صفحهٔ ۱۰۵) مطابقت‌دارد. در دستگاه به‌اصطلاح ضربی، قضیهٔ اصلی ۱۶ (صفحهٔ ۱۰۵) را می‌توان به‌صورت زیر مجدداً بیان کرد.

فرع ۲. یك گروه آبلی متناهی حاصلضرب مستقیم گروههای سیلوی خودش است.

قضیهٔ اصلی بعدی اطلاعات دقیقتری دربارهٔ تعداد p-گروههای سیلو به‌دست‌می‌دهد.

قضیهٔ اصلی ۳۰: (سومین قضیهٔ اصلی سیلو). فرض‌کنیم r تعداد p-گروههای سیلوی G بـاشد. دراین صورت r عددی است صحیح به‌صورت $1 + pk$ و مقسوم علیهی است از مرتبهٔ G.

برهان. این‌حقیقت‌که $r \equiv 1 \pmod p$، قبلاً درقضیهٔ اصلی ۲۷ ثابت شده است. باقی می‌ماند اثبات اینکه $r|g$، که درآن $|G| = g$. فرض کنیم

$$\mathcal{P} : P_1(=P),\ P_2,\ \dots,\ P_r$$

مجموعهٔ کلیهٔ p-گروههای سیلوی G باشد. دراین صورت، بنا بـر قضیهٔ اصلی ۲۹، $\mathcal{P}$ یك مجموعهٔ کامل ازمزدوجهای P است. خواننده‌ای که از عهـدهٔ حل تمرین ۶ فصل ۳ (صفحهٔ ۸۸) برآمده می‌داند که

$$r = [G : N(P)] \qquad (۱۵.۸)$$

که درآن $N(P)$ نرمالساز P در G است. لذا، اگر $n = |N(P)|$، آنگاه $g = nr$، که نشان می‌دهد $r|g$. رابطهٔ (۱۵.۸) مشابه (۶.۸) است. در واقـع، می‌تـوانیم از مربوط کردن نگاشت

$$P \rightarrow x^{-1}Px \quad (P \in \mathcal{P})$$

به یك عنصر دلخواه x از G یك‌عمل از G روی مجموعهٔ $\mathcal{P}$ را که موجب یك جایگشت

از $\mathcal{P}$ می‌شود، تعریف کنیم. وقتی x در G تغییر می‌کند، همهٔ عناصر $\mathcal{P}$ به‌دست می‌آیند، یعنی تمام $\mathcal{P}$ مدار P است، و داریم

$$|o(P)|=r$$

پایدارساز P مشتمل بر آن عناصر u از G است که برای آنها $u^{-1}Pu=P$. لذا درمقولهٔ حاضر پایدارساز برابر نرمالساز است. از نوشتن $N(P)$ به‌جای S، می‌بینیم که (۶.۸) به (۱۵.۸) تبدیل می‌شود.

۴۸. کاربردها و مثالها. قضایای اصلی سیلو ابزاری توانا برای مطالعه ساختار یک گروه متناهی به‌دست می‌دهند. استفاده از آنها، بخصوص وقتی مؤثر است که گروه مورد مطالعه به‌ازای یک عدد اول، منحصراً دارای یک گروه سیلو باشد.

قضیهٔ ۳۱. فرض کنیم G از مرتبهٔ pq باشد که p و q اعداد اولی هستند با $p<q$ و $q\not\equiv 1 \pmod p$. در این صورت G لزوماً آبلی است.

برهان. فرض کنیم تعداد p-زیرگروههای سیلوی G برابر r باشد. بنابرقضیهٔ اصلی ۳۰، $r|pq$ و $r=1+pk$. لذا $(r,p)=1$ و از این‌رو $r|q$. چون q اول است، نتیجه می‌شود که $r=1$ یا $r=q$. معنی حالت اخیر این است که $q=1+pk$، یعنی $q\equiv 1 \pmod p$، که بنابرفرض کنار گذاشته شده است. لذا بنابرفرع ۱، G فقط یک زیرگروه P از مرتبهٔ p دارد که لزوماً دوری می‌باشد. مولد این زیرگروه را به u نشان می‌دهیم. بنابراین

$$P\lhd G,\ P=\mathrm{gp}\{u\} \tag{۱۶.۸}$$

درمرحلهٔ بعد، فرض کنیم تعداد q-زیرگروههای سیلوی G برابر s باشد. پس $s|pq$ و $s=1+ql$. چون $(s,q)=1$، باید داشته باشیم $s|p$، و لذا $s\leqslant p$. اگر $l\geqslant 1$، آنگاه $s\geqslant 1+q>p$ که یک تناقض است. نتیجه می‌شود که $l=0$ و G دارای یک زیرگروه نرمال Q از مرتبهٔ q با مولد v است. لذا

$$Q\lhd G,\ Q=\mathrm{gp}\{v\} \tag{۱۷.۸}$$

چون مرتبه‌های P و Q متباین‌اند، داریم

$$P\cap Q=\{1\} \tag{۱۸.۸}$$

از قضیهٔ ۱۱ (صفحهٔ ۸۴) نتیجه می‌شود که عناصر P و Q دوبه‌دوتعویضپذیرند. بویژه

$$uv=vu \tag{۱۹.۸}$$

حاصلضربهای

$$u^{\alpha}v^{\beta}(\alpha=۰, ۱, \ldots, p-۱;\ \beta=۰, ۱, \ldots, q-۱)$$

متمایزند، زیرا هر تساوی بین آنها با (۱۸.۸) در تناقض است. از این‌رو این عناصر تمام گروه را تشکیل می‌دهند، و (۱۹.۸) آبلی بودن گروه را روشن می‌کند.

مثال ۱. هیچ گروه سادهٔ مرتبهٔ ۲۰۰ وجود ندارد.
زیرا چون $۲۰۰=۵^۲\times۸$، این گروه شامل r گروه سیلو از مرتبهٔ ۲۵ است که در آن r به‌صورت $۱+۵k$ و یك مقسوم‌علیه ۲۰۰ نیز هست. چون $(r, ۵)=۱$، باید داشته باشیم $r|۸$، که نامممکن‌است مگر آنکه $k=۰$. از این‌رو این گروه شامل یك زیرگروه نرمال یکتا از مرتبهٔ ۲۵ بوده و بنابراین ساده نیست.

مثال ۲. هیچ گروه سادهٔ مرتبهٔ ۳۰ وجود ندارد.
برای آنکه اگر چنین گروهی وجود داشته باشد، هیچ یك از گروههای سیلو یکتا نمی‌شود. لذا $۱+۵(=۶)$ گروه سیلوی متمایز مرتبهٔ ۵ موجود خواهد بود که شامل $۶\times۴(=۲۴)$ عنصر مرتبهٔ ۵ هستند. به طریق مشابه، $۱+۳\times۳(=۱۰)$ گروه سیلوی متمایز مرتبهٔ ۳ خواهیم داشت که ۲۰ عنصر مرتبهٔ ۳ به‌دست می‌دهند. بدین‌طریق تعداد کل عناصر از ۳۰ تجاوز خواهدکرد.
مطلب را با یك نتیجهٔ کلیتر درباب گروههای سیلو ادامه می‌دهیم.

•

قضیهٔ اصلی ۳۱. فرض‌کنیم P یك زیرگروه سیلو از یك‌گروه متناهی G، و H زیرگروهی از G شامل نرمالساز P باشد. دراین صورت H نرمالساز خودش است.

برهان. فرض کنیم $u\in N(H)$، نرمالساز H، یعنی $u^{-۱}Hu=H$ باشد. اما $P\leqslant N(P)\leqslant H$، و از این‌رو $u^{-۱}Pu\leqslant u^{-۱}Hu=H$. لذا $u^{-۱}Pu$ نیز، که با P هم‌مرتبه است، یك گروه سیلوی H است. با به‌کاربردن قضیهٔ اصلی ۲۹ برای H نتیجه می‌گیریم که عنصری مانند $h_۱$ از H وجود دارد به‌قسمی که

$$h_۱^{-۱}(u^{-۱}Pu)=P$$

این بدین‌معنی است که $uh_۱$، P را نرمال می‌سازد. چون، بنابرفرض، $N(P)\leqslant H$، از اینجا نتیجه می‌شود که $uh_۱=h_۲$، که درآن $h_۲\in H$. لذا $u\in H$، و قضیه‌ثابت می‌شود.
بالاخره، نشان می‌دهیم که ویژگی مذکور درفرع ۲ صفحهٔ ۱۷۵، درحقیقت مشخصهٔ تمام‌گروههای پوچتوان متناهی است.

قضیهٔ اصلی ۳۲. فرض‌کنیم G گروهی متناهی از مرتبهٔ $p_۱^{\alpha_۱}p_۲^{\alpha_۲}\ldots p_r^{\alpha_r}$ و $P_۱$، $P_۲$، ...، P_r مجموعه‌ای از گروههای سیلوی G باشند که بترتیب متناظر با اعداد اول $P_۱$، $P_۲$، ...، P_r هستند. دراین صورت G فقط و فقط وقتی پوچتوان است که

$$(\text{الف})\quad P_i \lhd G \quad (i = ۱, ۲, \ldots, r)$$

و

$$(\text{ب})\quad G = P_۱ \times P_۲ \times \cdots \times P_r \qquad (۲۰.۸)$$

برهان. ابتدا فرض می‌کنیم که (۲۰.۸) برقرار باشد. می‌دانیم کـه هر عامل در یك حاصلضرب مستقیم، یك زیر گروه نرمال است (صفحهٔ ۸۴). همچنین، بنا بر مثال ۲، صفحهٔ ۱۳۷، هر گروه سیلو پوچتوان است. باقی می‌ماند نشان دهیم کـه حاصلضرب مستقیم گروههای پوچتوان گروهی است پوچتوان. از این‌رو فرض می‌کنیم که K و L پوچتوان باشند و گروه $K \times L$ را درنظر می‌گیریم. اگر $\Gamma_i(K)$، $\Gamma_i(L)$، $\Gamma_i(K \times L)$ بترتیب جملات نوعی سری (۱۶.۸) بترتیب برای گروههای K، L و $K \times L$ باشند، آنگاه واضح است که

$$\Gamma_i(K \times L) = \Gamma_i(K) \times \Gamma_i(L) \quad (i = ۱, ۲, \ldots)$$

از این‌رو اگر $\Gamma_i(K)$ و $\Gamma_i(L)$ به‌ازای مقادیر به‌قدر کافی بزرگ i به گروه یکانی تبدیل شوند، آنگاه $\Gamma_i(K \times L)$ نیز به گروه یکانی تبدیل می‌شود. یعنی $K \times L$ پوچتوان است. بنابراین (۲۰.۸) پوچتوانی G را ایجاب می‌کند.

بعکس، فرض کنیم G یك گروه متناهی پوچتوان باشد؛ فرض کنیم P یك گروه‌سیلو از G متناظر با یك عدد اول خاصی باشد و قرارمی‌دهیم $H = N(P)$. گوییم که $H = G$، یعنی $P \lhd G$. زیـرا، درغیر این صورت اگر H یك‌زیر گروه خـاص باشد، آنگاه بنابر قضیهٔ ۲۵ (صفحهٔ ۱۳۷) $N(H) > H$؛ ازطرف دیگر، بنابرقضیهٔ اصلی ۳۱، $N(H) = H$. این تناقض نشان می‌دهد که $H = G$. از این‌رو $P_i \lhd G$ $(i = ۱, ۲, \ldots, r)$.

روشن‌است که وقتی $i \neq j$، $P_i \cap P_j = \{۱\}$. ازاین‌رو بنابرقضیهٔ ۱۱ (صفحهٔ ۸۴) و بنابرتعریف حاصلضرب مستقیم داخلی (صفحهٔ ۴۸).

$$P_۱ P_۲ \cdots P_r = P_۱ \times P_۲ \times \cdots \times P_r$$

این یك‌زیر گروه از مرتبهٔ $p_۱^{\alpha_۱} p_۲^{\alpha_۲} \cdots p_r^{\alpha_r}$ بوده بنابراین با G یکی است.

تمرین

(۱) نشان دهیدکه $A_۴$ یك گروه سیلو از مرتبهٔ ۴ و چهار گروه سیلو از مرتبهٔ ۳ دارد.

(۲) یکی از ۲ـگروههای سیلوی $S_۴$ را بدست آورید. این گروه با کدامیك از گروههای داده شده درصفحات ۵۰ و ۵۱ یکریخت است؟ چند ۲ـگروه سیلو وجود دارد؟

(۳) ثابت کنیدکه هیچ گروه سادهٔ مرتبه ۵۶ وجود ندارد.

(۴) فرض‌کنیم G گروهی است از مرتبهٔ $p^۲q$ که درآن p و q اول‌اند و q کوچکتر از p و عامل $p^۲ - ۱$ نیست. ثابت‌کنید G آبلی است.

(۵) فرض کنیم p عدد اولی باشد که مرتبهٔ گروه G را عاد می‌کند. ثابت کنید که اگر K یک زیرگروه G باشد، به‌قسمی که $|K|$ توانی از p باشد، آنگاه K حداقل در یک p-گروه سیلو قرار دارد.

(۶) نشان دهید که یک p-زیرگروه نرمال، در همهٔ p-زیرگروههای سیلو واقع است.

(۷) فرض کنیم P یک p-زیرگروه سیلو از یک گروه متناهی G و H یک زیرگروه نرمال G باشد. ثابت کنید که (الف) HP/H یک p-زیرگروه سیلوی G/H است و (ب) $H \cap P$ یک p-زیرگروه سیلو از H است.

جواب تمرینها

فصل ۱

(۲) قانون شرکتپذیری برقرار نیست.

(۳) $xa^n=\alpha^n x+\beta(\alpha^n-1)/(\alpha-1)$.

(۴) $ab=(ab)^{-1}=b^{-1}a^{-1}=ba$.

(۵) $ba=a^{-1}(ab)a^{-1}$. صفحهٔ ۲۰ (iii) ملاحظه شود.

(۶) توجه کنید که $a^{m-2}b^n=a^{-1}(a^{-1}b)a$ و $a^mb^{n-1}=b(ab^{-1})b^{-1}$.

(۸) اعداد صحیحی مانند u و v موجودند بهقسمی که $um+vn=1$؛ قرار دهید $y=x^{vn}$ و $z=x^{um}$.

(۹) آن عناصری که در معادلهٔ $x^2=1$ صدق نمی‌کنند می‌توانند بهزوجهای متمایز (u, u^{-1})، (v, v^{-1})، ... طبقه‌بندی شوند. بنابراین این معادله دارای تعداد زوجی جواب است که یکی از آنها ۱ است.

(۱۰) مرتبه‌ها بترتیب عبارت‌اند از ۱، ۳، ۶، ۳، ۶، ۲ و ۳ یا ۵ را می‌توان به‌عنوان‌مولد اختیار کرد.

(۱۳) (الف) (۳۹) (۲۶۵) (۱۴۷۸)؛ (ب) $(acdf)(be)$.

(۱۴) (الف) $(abc\ \dots\ k)$؛ (ب) $(a_ryb_1\ \dots\ b_sxc_1\ \dots\ c_t)$؛ (ج) $(xzb_1b_2\ \dots\ b_s)(a_ryc_1c_2\ \dots\ c_r)$.

فصل ۲

(۲) هرگاه $u, v\in At\cap Bs$، آنگاه $uv^{-1}\in A\cap B$؛ وبنابراین $Du=Dv$. تعداد همجموعه‌های متمایز D ازتعداد اشتراکهای غیرخالی $At\cap Bs$ نمی‌تواند تجاوز کند، و هرعنصر G دریکی ازاین اشتراکها قرار دارد.

(۳) چون $|A\cap B|$ هم $|A|$ وهم $|B|$ را عاد می‌کند، درنتیجه $|A\cap B|=1$.

(۴) هر گاه G دوری باشد، نتیجه از قضیهٔ اصلی ۴ به دست می‌آید. هر گاه G دوری نباشد، قرار می‌دهیم $x \in G$ و $x \neq 1$؛ در این صورت $\mathrm{gp}\{x\}$ یك زیر گروه‌حقیقی است.

(۵) $\mathrm{gp}\{a\}$، $\mathrm{gp}\{a^2, b\}$، $\mathrm{gp}\{ab, a^3b\}$.

(۶) کافی است نشان دهیم این روابط وجود نتایجی را که در صفحهٔ ۵۲ آمده است ایجاب می‌کنند، بدین گونه $a = cd$، $ac = cdc$، از این‌رو $a^3 = 1$، $(ac)^2 = 1$.

(۹) عناصر را به‌صورت a^k، a^kb $(0 \leqslant k \leqslant 5)$ بنویسید، عنصر $c = b^{-1}ab$ بایدتوانی از a و از همان مرتبهٔ a باشد. چون $c = a$ استثنا شده است، نتیجه می‌شود که $c = a^{-1}$. باز، $b^2 = a^l$ برای مقدار مناسبی از l و ازاین‌رو

$$b^2 = b^{-1}b^2b = b^{-1}a^lb = a^l$$

بنابراین $a^{2l} = 1$، و از اینجا یا $l = 0$ یا $l = 3$.

(۱۰) برای مثال، $\{-1\} \times g\{2\}$ gp، یعنی $\mathrm{gp}\{2\} \times \mathrm{gp}\{20\}$.

فصل ۳

(۱) هر گاه $b = t^{-1}at$، آنگاه $a^m = 1$ ایجاب می‌کند که $b^m = 1$، و برعکس.

(۲) (الف) هر گاه $C(a)$ مرکزساز a باشد، آنگاه $C(a) = C(a^{-1})$، از اینجا با توجه به‌قضیهٔ ۷ نتیجه حاصل می‌شود، (ب) از معادلهٔ رده‌ای (۵.۳) که در آن می‌تواند $h_1 = 1$ فرض شود استفاده کنید؛ اگر ادعا درست نباشد، می‌توان جملات باقیمانده را به‌زوجهای با جملات متساوی گروه‌بندی کرد، که در آن هرزوج متناظر بادسته‌های عکس باشد. اما در آن‌صورت g فرد خواهد شد که با فرض ما در تناقض است.

(۳) فرض کنیم $a = (a_{ij}) \in Z$، مرکز G باشد. پس $\mathbf{ax} = \mathbf{xa}$ به ازای هر $\mathbf{x} \in G$. بخصوص می‌توانیم $\mathbf{x} = \mathrm{diag}(x_1, x_2, \dots, x_n)$ اختیار کنیم، که یك ماتریس قطری با درایه‌های قطری متمایز است. ازاینجا نتیجه می‌شود که $a_{ij}x_j = x_ia_{ij}$؛ ازاین‌رو وقتی $i \neq j$، $a_{ij} = 0$؛ بدین گونه خود $\mathbf{a}$ یك ماتریس قطری است. سپس x را ماتریس جایگشتی $\mathbf{p} = (p_{ij})$ بگیرید که در آن $p_{i, i+1} = 1$ $(i < n)$، $p_{n, 1} = 1$ و بقیهٔ $p_{ij} = 0$. معادله $\mathbf{ap} = \mathbf{pa}$ نتیجه می‌دهد که $a_{11} = a_{22} = \dots = a_{nn}$، یعنی $\mathbf{a}$ یك ماتریس عددی است.

(۴) $Z = \mathrm{gp}\{a^2\}$. عناصر G/Z عبارت‌اند از Z، Za، Zb، Zab، $G/Z \simeq V$ (صفحهٔ ۵۱).

(۵) هر گاه $\mathbf{s}$ و $\mathbf{t}$ ماتریس مثلثی زبرین باشند، آنگاه $\mathbf{st}$ نیز یك ماتریس مثلثی زبرین با قطر $s_{11}t_{11}$، $t_{22}s_{22}$، ...، $s_{nn}t_{nn}$ است. ازاین‌رو ویژگی گروهی T به‌آسانی قابل تحقیق است. فرض کنیم $\theta : T \to D$ نگاشتی باشد که به‌وسیلهٔ $\mathbf{t}\theta = \mathrm{diag}(t_{11}, t_{22}, \dots, t_{nn})$ تعریف می‌شود. دراین صورت E هستهٔ θ است وحکم ازقضیهٔ اول یکریختی نتیجه می‌شود.

(۶) توجه کنید که $x^{-1}Hx = y^{-1}Hy$ اگر، وفقط اگر $xy^{-1} \in N(H)$، یعنی $N(H)x = N(H)y$. (برهان قضیهٔ ۷، صفحهٔ ۶۵ را ملاحظه کنید.)

(۷) G/N گروهی متناهی از مرتبهٔ n است، وعنصر Nt از G/N از مرتبهٔ h. از این‌رو، بنا بر قضیهٔ اصلی لاگرانژ، $h|n$. همچنین $N = Nt^r = (Nt)^r$، ازاین‌رو h/r (قضیهٔ ۱ صفحهٔ ۲۵).

(۸) هردو قسمت با استقراء روی k و با استفاده از $ab = bac$ و $ac = ca$ و $bc = cb$ اثبات می‌شود.

(۹) بنا بر سومین قضیهٔ اصلی یکریختی، $A/A \cap N \cong NA/N$ که یك زیرگروه از گروه متناهی G/N از مرتبه n است. ازاین‌رو $|A/A \cap N|$، n را عاد می‌کند.

(۱۰) مرکز هریك از این گروهها برابر $Z = \mathrm{gp}\{a^2\}$ است. چون $a^2 = [a, b]$، $a^2 \in G'$ و از این‌رو $Z \leqslant G'$. از طرف دیگر G/Z از مرتبهٔ ۴ ولذا آبلی است. بنابراین (قضیهٔ اصلی ۱۱)، $G' \leqslant Z$، و از اینجا $G' = Z = \mathrm{gp}\{a^2\}$.

(۱۱) فرض کنیم $N \lhd G$ و $C = C(N)$ (صفحهٔ ۶۷). لذا اگر $c \in C$ آنگاه به‌ازای هر $u \in N$، $cu = uc$. اگر $t \in G$، آنگاه $c^t u^t = u^t c^t$؛ اما u^t می‌تواند با هرعنصر N مساوی باشد. لذا $c^t \in C$، وبنابراین $C \lhd G$.

(۱۲) $(xy)\theta = (xy)^{-1} = y^{-1}x^{-1} = x^{-1}y^{-1} = (x\theta)(y\theta)$. به آسانی نشان داده می‌شود که θ یك بدیك دوسویی است.

(۱۳) فرض کنیم $x\tau = t^{-1}xt$ یك خود ریختی داخلی و α یك همریختی دلخواه باشد؛ قرار می‌دهیم $s = t\alpha$ و $x\sigma = s^{-1}xs$. در این صورت $x\alpha\sigma = s^{-1}(x\alpha)s$ و $x\tau\alpha = (t^{-1}xt)x$، $\alpha = s^{-1}(x\alpha)s$. لذا $\alpha\sigma = \tau\alpha$، $\alpha^{-1}\tau\alpha \in I(G)$، $I(G) \lhd A(G)$.

(۱۴) فرض کنیم $\alpha \in A(G)$؛ در این صورت $[a, b]\alpha = [a\alpha, b\alpha] \in G'$. از این‌رو $G'\alpha \subset G'$. مشابهاً، $G'\alpha^{-1} \subset G'$. بدین گونه $G' \subset G'\alpha$، ازاینجا به‌دست می‌آید که $G'\alpha = G'$.

فصل ۴

(۱) یك گروه آبلی آزاد مانند $F = \langle u_1, u_2, \ldots, u_n\rangle$ بسازید و قرار دهید $v_1 = b_1u_1 + b_2u_2 + \ldots + b_nu_n$. عناصری مانند v_2، v_3، …، v_n هستند به‌قسمی که $F = \langle v_1, v_2 \ldots, v_n\rangle$ و $v_i = \sum_j b_{ij}u_j$ که در آن (b_{ij}) یك ماتریس یکهنگی با ویژگی مطلوب است.

(۲) قرار دهید $|A| = p_1p_2 \ldots p_n$. در (۴۷.۴) مؤلفهٔ اولیهٔ $\mathbf{P}_i$ از مرتبهٔ p_i ولذا یك گروه دوری است. مثلا $P_i = \mathrm{gp}\{x_i\}$. دراین صورت $x = x_1x_2 \ldots x_n$ عنصری ازمرتبهٔ $p_2p_3 \ldots p_n$ و ازاین‌رو A را تولید می‌کند.

(۳) فرض کنیم e_1 بزرگترین پایا باشد. t_ρها در (۳۷.۴) وجود ندارند، w_1 ازمرتبهٔ

$e_۱$ و هرعنصر در $\circ = e_۱ x$ صدق می‌کند.

(۴) هریك از $(۸ =)(۲۴)\phi$ طبقهٔ باقیمانده‌ها در $x^۲ \equiv ۱ (\mathrm{mod}\ ۲۴)$ صدق می‌کنند.

(۵) (الف) ۴، ۳، ۵؛ (ب) $(۲, ۴)$، ۳، $(۵, ۵)$؛ ۶۰، ۱۰.

(۶) $C_\infty \oplus C_۲ \oplus C_۶$.

(۷) (الف) $r = ۱$، $e_۱ = ۲$؛ (ب) $r = ۲$، $e_۱ = ۲$.

(۸) $v_۱ = u_۱ + u_۲ + ku_۳$ و $v_۲ = u_۲ - u_۳$ و $v_۳ = -u_۳$؛
$s_۱ = r_۳$، $s_۲ = r_۲ - r_۳$، $s_۳ = r_۱ + r_۲ - (k+۱) r_۳$؛
$e_۱ = ۱$، $e_۲ = k - ۱$، $e_۳ = (k-۱)(k+۲)$.

(۹) به‌موجب قضیهٔ اصلی ۱۶ کافی است حکم را برای یك گروه توان-اول آبلی مانند P اثبات کنیم. فرض کنیم $|P| = p^m$. باید نشان دهیم هرگاه $n \leqslant m$، زیرگروهی مانند P' هست به‌قسمی که $|P'| = p^n$. فرض کنیم که $P = \sum_i \oplus P_i$، که در آن $|P_i| = p^{\delta_i}$. در این صورت $m = \sum_i \delta_i$. روشن است که می‌توانیم بنویسیم $n = \sum_i \lambda_i$ که $\circ \leqslant \lambda_i \leqslant \delta_i$. بنابر قضیهٔ اصلی ۴، زیرگروهی مانند P'_i هست که $P'_i \subset P_i$ و P'_i ازمرتبهٔ p^{λ_i} است. قرار می‌دهیم $P' = \sum_i P'_i$.

(۱۱) فرض کنیم عناصر گروه $p^۳$ بردار $\mathbf{a} = (\alpha_۱, \alpha_۲, \alpha_۳)$ باشند که $\circ \leqslant \alpha_i < p$ $(i = ۱, ۲, ۳)$. اولین بردار مبنای $\mathbf{a}_۱$ می‌تواند یکی از $p^۳ - ۱$ بردار غیر صفر باشد. دومین بردار مبنا، $\mathbf{a}_۲$، می‌تواند هر برداری باشد که مضرب عددی $\mathbf{a}_۱$ نیست؛ $p^۳ - p$ عدد از این‌گونه بردارها وجود دارد. بالاخره $\mathbf{a}_۳$ مبنا را کامل کند به‌شرطی که $\mathbf{a}_۳$ ترکیب خطی از $\mathbf{a}_۱$ و $\mathbf{a}_۲$ نباشد تعداد $p^۳ - p^۲$ بردار از این‌گونه بردارها وجود دارند. لذا به‌تعداد

$$(p^۳ - ۱)(p^۳ - p)(p^۳ - p^۲)$$

انتخاب داریم.

(۱۲) یك گروه آبلی آزاد مانند $F = \langle u_۱, u_۲, \dots, u_n \rangle$ و زیرگروه

$$R = \mathrm{gp}\,\{r_۱, r_۲, \dots, r_m\}$$

را با تساوی $r_i = \sum_j b_{ij} u_j$ درنظرمی‌گیریم. تغییرمولدها در F و R معادل‌است با ضرب B از راست در Q و ازچپ در P می‌شود.

فصل ۵

(۱) فرض کنیم F یك گروه آزاد باشد. فرض کنیم U گردایهٔ واژه‌هایی باشد که در آنها حاصلجمع نمایندهای هرمولد صفر باشد. دراین صورت U یك زیرگروه بوده و روشن است که $F' \subset U$. برعکس، براثر نگاشت طبیعی $F \to F/F'$ هرعنصر

U به‌توی F' نقش می‌شود. از این‌رو $U \subset F'$. به‌طوری که $U = F'$.

(۲) (الف) $C_۲ \times C_۲$. (ب) $C_۴$.

(۳) روابط را می‌توان به‌صورت $a^{-۱}b^{-۱}ab = a$، $b^{-۱}a^{-۱}ba = b$ نوشت که از ضرب آنها نتیجه می‌شود $ab = ۱$. بنابراین $b = a^{-۱}$ و درمی‌یابیم که $a = b = ۱$.

فصل ۶

(۱) در هر دو حالت $G \rhd \mathrm{gp}\{a\} \rhd \mathrm{gp}\{a^۲\} \rhd \{۱\}$ را می‌توان به‌صورت سری ترکیبی درآورد. همهٔ عاملهای ترکیبی ازمرتبهٔ ۲ هستند.

(۲) فرض کنیم $G^{(s)} = \{۱\}$. هرگاه $H \leqslant G$، آنگاه $H^{(i)} \leqslant G^{(i)}$ $(i = ۱, ۲, \ldots)$. اگر $N \lhd G$، آنگاه $G/N = G\nu$، که در آن $\nu : G \to G/N$ بریختی طبیعی G به‌روی G/N است. توجه داریم که $(G\nu)^{(i)} = G^{(i)}\nu$ $(i = ۱, ۲, \ldots)$ لذا سری مشتق برای H و $G\nu$ بعد از حداکثر s مرحله، به‌گروه یکانی ختم می‌شوند.

(۴) چون $\Gamma_۳ = [\Gamma_۲, G] = [G', G] = \{۱\}$، G' در مرکز قرار دارد. در فرمولهای تمرین (۳)، داریم $[x, z]^y = [x, z]$، $[x, y]^z = [x, y]$.

(۵) همچون تمرین (۲) است.

(۶) چون $\Gamma_۴ = \{۱\}$، پس $\Gamma_۳ = [G', G]$ درمرکز قرار دارد؛ بخصوص، $[\nu, x^{-۱}] = c \in Z$، یعنی $\nu^{-۱}x\nu = cx$. همچنین، هرگاه $y \in G$، آنگاه $\nu^{-۱}y\nu = dy$، که در آن $d \in Z$. اما

$$\nu^{-۱}[x, y]\nu = \nu^{-۱}(x^{-۱}y^{-۱}xy)\nu = c^{-۱}d^{-۱}cd[x, y] = [x, y]$$

لذا ν با هرعنصر G' تعویضپذیر است.

(۷) بنابر قضیهٔ ۲۵۰ $(M) \cdot$ $M < N(M)$؛ از این‌رو $N(M) = G$، یعنی $M \lhd G$. همچنین G/M نمی‌تواند دارای یك زیرگروه حقیقی باشد، چون چنین زیرگروهی باید شامل M باشد. بنابراین $|G/M|$ یك عدد اول است.

(۸) عناصر $D(z^n)$ را می‌توان به صورت $a^\alpha b^\beta$ $(\alpha = ۰, ۱, \ldots, ۲^n - ۱)$ و $(\beta = ۰, ۱)$ بیان کرد. چون $b^{-۱}ab = a^{-۱}$، یك عنصر مرکزی باید در رابطهٔ $a^\alpha b^\beta = a^{-\alpha}b^\beta$ صدق کند، از اینجا نتیجه‌می‌شود که $\alpha = ۰$ یا $\alpha = ۲^{n-۱}$ و $\beta = ۰$ زیرا b در مرکز قرارندارد. لذا $Z_۱ = \{۱, a^{۲^{n-۱}}\}$. اگر $\bar{a} = aZ_۱$، $\bar{b} = bZ_۱$، آنگاه $(\bar{a})^{۲^{n-۱}} = \bar{b}^۲ = (\overline{ab})^۲ = \bar{۱}$. جملات متوالی از سری مرکزی زیرین دارای اندیس ۲ هستند.

فصل ۷

(۲) فرض کنیم $\xi = \sigma_۱\sigma_۲ \ldots \sigma_r$، که σ_i یك دور از درجهٔ m_i است، $(i = ۱, ۲, \ldots, r)$. دراین صورت $n = m_۱ + m_۲ + \ldots + m_r$. بااستفاده از (۲۵.۷) پیدامی‌کنیم که $\zeta(\xi) = (-۱)^v$، که در آن $v = \sum_i (m_i - ۱) = n - r$.

(۳) ملاحظه می‌کنیم که $(۱۳)=(۱۲)(۲۳)(۱۲)$، $(۱۴)=(۱۳)(۳۴)(۱۳)$، و غیره سپس به‌قضیهٔ ۲۵ استناد کنید.

(۴) عبارتهای $\gamma^{-r}\tau\gamma^{r}$ $(r=۰, ۱, \ldots, r-۲)$ را درنظر بگیرید و از تمرین قبلی استفاده کنید.

(۵) قسمت اول از فرمول

$$\prod_{\lambda=۱}^{k}(a_{۱}^{(\lambda)}a_{۲}^{(\lambda)}\ldots a_{r}^{(\lambda)})=(a_{۱}^{(۱)}a_{۱}^{(۲)}\ldots a_{۱}^{(k)}a_{۲}^{(۱)}a_{۲}^{(۲)}\ldots a_{۲}^{(k)}a_{۳}^{(۱)}\ldots)^{k}$$

نتیجه می‌شود. قسمت دوم نتیجه‌یی از قضیهٔ اصلی کیلی و این واقعیت است که γ^{s} از مرتبهٔ m/d است (قضیهٔ ۲، صفحهٔ ۲۰ ملاحظه شود).

(۶) بنا بر قضیهٔ ۲۲ ردهٔ مزدوج γ شامل $(n-۱)!$ عنصر است. لذا $|C(\gamma)|=n$ (قضیهٔ ۷، صفحهٔ ۶۵). اما یقیناً $C(\gamma)$ شامل n توان γ بوده وبنا براین شامل هیچ عنصر دیگری نیست.

(۷) ردهٔ مزدوج λ شامل $n!/(n-۱)$ عنصر است. از این‌رو $|C(\lambda)|=n-۱$؛ اما $C(\lambda)$ شامل $n-۱$ توان λ است.

(۸) هرگاه Z مرکز S_n باشد، آنگاه $Z<C(\gamma)\cap C(\lambda)=\{\iota\}$ که در آن γ و λ در تمرینات (۶) و (۷) تعریف شده‌اند.

(۹) (الف) $a\lambda_u\lambda_v=u^{-۱}a\lambda_v=v^{-۱}u^{-۱}a=(uv)^{-۱}a=a\lambda_{uv}$؛ (ب) $\lambda_u=i$ اگر، وفقط اگر به‌ازای هر $a\in G$، $u^{-۱}a=a$، لذا $u=۱$؛
(ج) $a\lambda_u\rho_x=u^{-۱}ax=a\rho_x\lambda_u(a\in G)$؛
(د) فرض کنید که $(\forall a, u\in G)a\theta\lambda_u=a\lambda_u\theta$. قرار دهید $a=۱$ وتعریف کنید $۱\theta=x$. دراین صورت $x\lambda_u=۱\lambda_u\theta$، یعنی $u^{-۱}x=u^{-۱}\theta$. چون وقتی u در G تغییرمی‌کند $u^{-۱}$ نیز در G تغییر می‌کند، نتیجه می‌شود که $\theta=\rho_x$ همچنین وقتی که $a\eta\rho_x=a\rho_x\eta$، داریم $\eta=\lambda_u$. که در آن $۱\eta=u^{-۱}$.

(۱۰) قراردهید $[G:H]=n$. دراین صورت یك‌همریختی یك‌به‌یك مانند $\theta: G\to S_n$ وجود دارد. ازاین‌رو $n!\geqslant ۱۶۹=|G\theta|$ وبنا براین $n\geqslant ۶$.

(۱۱) هرگاه مرکز مستطیل در مبدأ قرار داشته و اضلاع آن بترتیب با محور x و محور y موازی باشند، آنگاه تقارنهای آن تقارن همانی و دورانهای به‌اندازهٔ π حول هریك از محورهای مختصات هستند. این گروه باگروه چارینه یکریخت است.

(۱۲) دربسط (تجزیه) همجموعه‌ای G نسبت به $G_۱$، حرف ۱ دقیقاً در آن جایگشتهایی پیدا می‌شود که به $G_۱$ تعلق ندارند، یعنی به تعداد $g-(g/n)$ مرتبه؛ عین همین مطلب برای هریك از حروف دیگر نیز صادق است.

فصل ۸

(۱) گروه V (صفحهٔ ۵۱) یك زیرگروه نرمال $A_۴$ از مرتبهٔ ۴ و بنا براین تنها گروه‌سیلو

از این مرتبه است. هر سه‌ـدور یك ۳ـگروه سیلو تولید می‌کند، مثل ۱، (۱۲۳)، (۱۳۲). تعداد چهارتا ازاین گروههای مرتبه ۳ وجود دارد، که هریك متناظر بایك انتخاب سه شیء از بین چهار شیء هستندکه A_4 برآنها اثر می‌کند.

(۲) جایگشتهای $a=(1234)$ و $b=(24)$ زیرگروهی از مرتبهٔ ۸ تولید می‌کنند که از جایگشتهای زیر تشکیل شده است.

$$(1), (1234), (1432), (24), (13), (12)(34), (13)(24), (14)(23)$$

این یك ۲ـگروه سیلو می‌باشد. چون $a^4=b^2=(ab)^2=1$، لذا این گروه با گروه دووجهی (جدول (xi)، صفحهٔ ۵۷) یکریخت است. واضح است که این گروه سیلو نه نرمال است و نه‌منحصر به‌فرد. سه ۲ـگروه سیلو وجود دارد.

(۳) چنین گروهی دارای هشت زیرگروه مرتبهٔ ۷ و هفت زیرگروه مرتبهٔ ۸ خواهد بود، که دریك گروه مرتبهٔ ۵۶ غیرممکن است.

(۴) تعداد $1+xp$، pـگروه سیلو وجود دارد و $1+xp|p^3q$. لذا $1+xp|q$ که ایجاب می‌کند $x=0$. تعداد $1+yq$، qـگروه سیلو وجود دارد و $1+yq|p^3q$ و $1+yq|p^2$. مگراینکه $y=0$، از اینجا لازم می‌آید که $1+yq$ مساوی p یا مساوی p^2 باشد؛ در هردوحالت، $q|p^2-1$، که کنار گذاشته شده است. لذا $G=P\times Q$، که $|P|=p$ و $|Q|=q$. چون P و Q آبلی‌هستند، G نیزآبلی‌است.

(۵) فرض کنیم $|G|=p^m g'$، که $(g', p)=1$، و $|K|=p^\mu$. از تجزیهٔ مضاعف G نسبت به K و یك pـگروه سیلوی دلخواه مانند P استفاده‌کنید، مثلاً؛

$$G=Kt_1P\cup Kt_2P\cup\cdots\cup Kt_rP$$

همچون برهان قضیهٔ اصلی ۲۹، نشان داده می‌شودکه حداقل یك اندیس j وجود دارد به‌طوری که $|t_j^{-1}Pt_j\cap K|=p^\mu$، یعنی $K\leqslant t_j^{-1}Pt_j$.

(۶) به استناد تمرین (۵)، $t_jKt_j^{-1}\leqslant P$؛ چون $K\lhd G$، $t_jKt_j^{-1}=K$. لذا $K\leqslant P$.

(۷) فرض کنیم $|G|=p^m s$، که $(p, s)=1$. پس $|P|=p^m$. حال گوییم، HP یك گروه است چون $H\lhd G$ وازاین‌رو $HP=PH$ (قضیهٔ اصلی ۵، صفحهٔ ۵۸). روشن‌است که، $P\leqslant HP$. لذا $|HP|=p^m t$، که $(p, t)=1$. و بنابر قضیهٔ‌اصلی لاگرانژ $t|s$. رابطهٔ $HP/P\cong P/H\cap P$ (قضیهٔ اصلی ۱۵، صفحهٔ ۸۱) نشان می‌دهد که HP/P یك pـگروه‌است، زیرا این امر برای سمت راست بدیهی‌است.
(الف) کافی است نشان داده شود که $|G/H|:|HP/H|$ با p متباین است؛ اما این‌خارج‌قسمت برابراست با $s:t=|G|:|HP|$، که در واقع با p متباین است.
(ب) باز، بنابر قضیهٔ اصلی ۱۵، $t=|P|:|HP|=|H\cap P|:|H|$، که همان چیزی است که بدان نیاز داشتیم.

واژه‌نامهٔ انگلیسی به‌فارسی

alternating character	شاخص تناوبی
alternating group	گروه تناوبی
automorphism	خود ریختی
canonical form	صورت قانونی
cardinal number	عدد اصلی
centralizer	مرکزساز
central series	سری مرکزی
characteristic subgroup	زیرگروه مشخصه
class equation	معادلهٔ رده‌ای
commutative group	گروه تعویضپذیر
commutator group	گروه تعویضگر
conjugacy class	ردهٔ مزدوج
conjugate element	عنصر مزدوج
conjugate groups	گروههای مزدوج
coprime numbers	اعداد متباین
coset	هممجموعه
cycle	دور
cyclic group	گروه دوری
cyclic Pattern	قالب دوری
derived group	گروه مشتق

derived series	سری مشتق
dihedral group	گروه دووجهی
direct product	حاصلضرب مستقیم
direct sum	حاصلجمع مستقیم
dodecahedral group	گروه دوازده‌وجهی
double coset	همجموعهٔ مضاعف
epimorphism	برریختی
factor group	گروه عاملی
faithful representation	نمایش صادق
finitely generated group	گروه متناهی-مولود
four-group	گروه چارینه
syn:vierergruppe	
free group	گروه آزاد
general linear map	نگاشت خطی عمومی
generator	مولد
hexahedral group	گروه شش‌وجهی
homomorphic group	گروه همریخت
icosahedral group	گروه بیست‌وجهی
idempotent element	عنصرخودتوان
identity element	عنصرهمانی
imprimitive group	گروه غیراولیه
intransitive group	گروه ناترایا
invariant subgroup	زیرگروه پایا
isomorphic groups	گروههای یکریخت
isomorphism	یکریختی
kernel	هسته
k-ply transitive	ترایایی k-تایی
latin square	مربع‌لاتین

left regular representation — نمایش منظم چپ
lower central series — سری مرکزی زیرین

maximal normal subgroup — زیرگروه نرمال ماکسیمال
modulus — هنگ
monomorphism — تکریختی

nested subgroups — زیرگروههای تودرتو
neutral element — عنصرخنثی
nilpotent group — گروه پوچتوان
normal closure — بستار نرمال
normalizer — نرمال ساز

octahedral group — گروه هشت‌وجهی
order — مرتبه

pattern — قالب
period — دورهٔ تناوب
permutation representation — نمایش جایگشتی
primary component — مؤلفهٔ اولیه
proper subgroup — زیرگروه حقیقی

quaternion group — گروه چارتایی
quotient group — گروه خارج‌قسمت

rank — رتبه
reduced word — واژهٔ کاسته
right regular permutation — جایگشت منظم راست

self-conjugate group — گروه خودمزدوج
soluble group — گروه حلپذیر
stabilizer — پایدارساز
standard form — صورت استانده
symmetric group — گروه متقارن

tetrahedral group	گروه چهاروجهی
torsion subgroup	زیرگروه پیچشی
transitive group	گروه ترایا
transposition	ترانهش
transversal	تراگرد
unimodular group	گروه یکهنگی
unit subgroup	زیرگروه واحد

vierergruppe → four-group

واژه‌نامهٔ فارسی به‌انگلیسی

اعداد متباین	coprime numbers
بر ریختی	epimorphism
بستار نرمال	normal closure
پایدار ساز	stabilizer
تراگرد	transversal
ترانهش	transposition
ترایایی k-تایی	k-ply transitive
تکریختی	monomorphism
جایگشت منظم راست	right regular permutation
حاصلجمع مستقیم	direct sum
حاصلضرب مستقیم	direct product
خودریختی	automorphism
دور	cycle
دورهٔ تناوب	period
رتبه	rank

conjugacy class	ردهٔ مزدوج
subgroup	زیر گروه
invariant subgroup	ـ پایا
torsion subgroup	ـ پیچشی
proper subgroup	ـ خاص
Characteristic subgroup	ـ مشخصه
maximal normal subgroup	ـ نرمال ماکسیمال
unit subgroup	ـ واحد
nested subgroups	ـ های تودرتو
central series	سری مرکزی
lower central series	ـ زیرین
derived series	سری مشتق
alternating character	شاخص تناوبی
standard form	صورت استانده
canonical form	صورت قانونی
cardinal number	عدد اصلی
neutral element	عنصرخنثی
idempotent element	عنصرخودتوان
conjugate element	عنصر مزدوج
identity element	عنصرهمانی
pattern	قالب
cyclic pattern	ـ دوری
group	گروه
free group	ـ آزاد
icosahedral group	ـ بیست‌وجهی
nilpotent group	ـ پوچتوان
transitive group	ـ ترایا
commutative group	ـ تعویضپذیر

ـ تعویضگر	commutator group
ـ تناوبی	alternating group
ـ چارتایی	quaternion group
ـ چارینه	four-group, vierergruppe
ـ چهاروجهی	tetrahedral group
ـ حلپذیر	soluble group
ـ خارج‌قسمت	quotient group
ـ خودمزدوج	self-conjugate group
ـ دوازده‌وجهی	dodecahedral group
ـ دوری	cyclic group
ـ دووجهی	dihedral group
ـ شش‌وجهی	hexahedral group
ـ عاملی	factor group
ـ غیراولیه	imprimitive group
ـ متقارن	symmetric
ـ متناهی-مولود	finitely generated group
ـ مشتق	derived group
ـ ناترایا	intransitive group
ـ های مزدوج	conjugate groups
ـ های یکریخت	isomorphic group
ـ هشت‌وجهی	octahedral group
ـ همریخت	homomorphic groups
ـ یکهنگی	unimodular group
مؤلفهٔ اولیه	primary component
هممجموعهٔ مضاعف	double coset
مربع لاتین	latin square
مرتبه	order
مرکزساز	centralizer
معادلهٔ رده‌ای	class equation
مولد	generator
نرمالساز	normalizer
نگاشت خطی عمومی	general linear map
نمایش جایگشتی	permutation representation

faithful representation	نمایش صادق
left regular representation	نمایش منظم چپ
word	واژه
reduced word	ـ کاسته
kernel	هسته
coset	هممجموعه
modulus	هنگ
isomorphism	یکریختی

مراجع

Burnside, W., 1911. *Theory of groups of finite order*, 2nd edition. (Reprint by Dover Publications, 1955.)

Coxeter, H. S. M., and Moser, W. O., 1965. *Generators and relations for discrete groups*, 2nd edition (Springer).

Hall, Marshall Jr., 1959. *The theory of groups* (Macmillan).

Hupert, B., 1967. *Endliche Gruppen* I (Springer).

Kurosh, A.G., *The theory of groups*, 2 vols. (transl. from the Russian by K. A. Hirsch, Chelsea, 1955).

Miller, G. A., Blichfeld, H. F., and Dickson, L. E., 1916. *Theory and application of finite groups* (John Wiley: reprint by Dover Publications, 1961).

Zassenhaus, H., *The theory of groups* (transl. from the German by S. Kraivety, 2nd edition New York, 1958)

فهرست راهنما

مرکز نشر دانشگاهی