۱۵ ۲۴

جبر ۳

(قضیه‌های سیلو)

دانشگاه پیام نور

قضیه‌های سیلو
تألیف: محمد حسن بیژن‌زاده

برای درس جبر ۳ از دو منبع:

۱- قضیه‌های سیلو تألیف دکتر محمد حسن بیژن‌زاده

۲-گامهایی در جبر تعویض‌پذیر ترجمهٔ دکتر محمد مهدی ابراهیم

استفاده می‌شود.

جزوهٔ حاضر تمام منبع اول و فصل ۸ از منبع دوم را شامل می‌شود.
فصول ۱ تا ۷ از منبع دوم در دو قسمت قبلاً ارسال شده است.

هدف درس

قضیه اصلی لاگرانژ بیان می‌دارد که هرگاه G گروهی متناهی از مرتبهٔ g باشد، آنگاه مرتبهٔ هر زیرگروه G باید g را عاد کند. عکس این قضیه در حالت کلی برقرار نیست؛ چون دیده‌ایم گروههایی وجود دارند که زیرگروههایی ندارند که متناظر با برخی از مقسوم‌علیه‌های g باشند. با این حال، هرگاه p^b توانی از یک عدد اول p باشد به قسمتی که p^b مقسوم‌علیه g باشد، آنگاه G دارای حداقل یک زیرگروه از مرتبهٔ p^b خواهد بود. این حقیقت قابل توجه را ریاضیدان نروژی اِل. سیلو در سال ۱۸۷۲ میلادی کشف کرد و از آن به بعد به نام قضیهٔ سیلو مشهور است. این قضیه نتایج بسیاری مؤثری در نظریه گروهها دارد و یکی از گیراترین مثالها را در ارتباط ظریف بین ویژگیهای حسابی یک گروه (یعنی تعداد اعضای آن) و ویژگیهای ساختاری آن (یعنی وجود زیرگروهها) فراهم می‌سازد.

اثباتهای چندی از قضیه‌های سیلو را در فرهنگ ریاضی می‌توان یافت. ما در اینجا اثبات زیبایی را که منسوب به لج. ویلنت[1] (۱۹۵۹ میلادی) است عرضه می‌کنیم. در این برهان تنها اصول اوّلیه و عمومی ریاضیات به‌کار گرفته شده و فقط برخی از اندیشه‌های مقدماتی در باب جایگشتها مورد استفاده قرار گرفته است.

به‌عنوان کاربردهایی از قضیهٔ سیلو ثابت خواهیم کرد که هیچ گروه ساده‌ای از مرتبه ۲۰۰ وجود ندارد (مثال ۱ صفحهٔ   ) و یا آنکه ثابت خواهیم کرد که هر گروه از مرتبه ۱۲۲۵ آبلی است. (مثال ۳، صفحه   ).

---

1. Wilend

۲ نقشهٔ سیلو

دانشجو پس از مطالعهٔ این فصل باید بتواند از عهدهٔ تعریف مفاهیمی مانند، زیرگروه اول ـ توان، و p-زیرگروه سیلو برآید. و آنها را به‌خوبی درک کند.

دانشجو باید بتواند قضیه‌های سه‌گانهٔ سیلو را بیان کرده و از عهدهٔ اثبات آنها برآید.

با شیوه کاربردهای قضیه‌های سیلو آشنا شده و از عهده حل تمرینهای پایان فصل برآید.

پیش آزمون

۱. این مفاهیم را تعریف کنید و برای هر یک مثالی ذکر کنید.

(آ) زیرگروه نرمال،

(ب) گروه ساده،

(ج) گروه دوری،

(د) زیرگروههای مزدوج

۲. قضیه حاصلضرب درباب دو زیرگروه را بیان کنید.

۳. قضیه لاگرانژ را بیان کنید (روش اثبات آن را به‌طور خلاصه توضیح دهید).

۴. ثابت کنید هرگاه C یک گروه دوری از مرتبه n و e یک مقسوم‌علیه (دلخواه) n باشد آنگاه C یک و فقط یک زیرگروه از مرتبه e دارد.

۵. فرض کنید A و B زیرگروههایی نرمال از گروه G باشند به قسمی که $A \cap B = \{e\}$. ثابت کنید برای هر عضو A مانند u و هر عضو B مانند، v، $uv = vu$. e عنصر همانی G است.

[راهنمایی: عضو $c = u^{-1}v^{-1}uv$ را که در آن u و v به‌ترتیب عضوهای دلخواهی از A و B هستند، در نظر بگیرید.]

۶. فرض کنیم که G یک گروه و $a \in G$ مجموعهٔ همهٔ اعضایی از G را که با a تعویض‌پذیرند با $C(a)$ نشان می‌دهیم و آن را مرکزساز a می‌نامیم. لذا

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

ثابت کنید:

(آ) $C(a)$ یک زیرگروه G است.

(ب) هرگاه G گروهی غیربدیهی باشد، $|C(a)| \geq 2$.

۷. فرض کنیم G یک گروه و $y \in G$ و x. گوییم x با y مزدوج است هرگاه عضوی از G مانند t یافت شود به‌طوری که

$$x = t^{-1}yt \ .$$

ثابت کنید:

(آ) رابطهٔ مزدوجی یک رابطه هم‌ارزی در G برقرار می‌کند و لذا هرگاه $[a]$ رده هم‌ارزی شامل a باشد، آنگاه

$$[a] = \{t^{-1}at \mid t \in G\}$$

و G به رده‌های هم‌ارزی متمایز و از هم‌جدا افراز می‌شود:

$$G = [a] \cup [b] \cup [c] \cup \ldots$$

۱. قضیه فروبنیوس

قبل از آنکه به بیان قضیه‌های سیلو بپردازیم، به‌عنوان پیشتاز مفهوم هم‌مجموعه‌های مضاعف و قضیه فروبنیوس را که مورد نیازمان است بیان می‌داریم.

۱.۱ هم‌مجموعه‌های مضاعف

در سرتاسر این فصل از نماد ضربی برای گروهها استفاده شده است.

در مبحث قضیه لاگرانژ در درس جبر ۱ مداخله کردیم که تجزیه یک گروه به هم‌مجموعه‌ها نسبت به یک زیرگروه را می‌توان به‌عنوان نمونه‌ای از افراز یک مجموعه تلقی نمود. دیدیم که دو عضو x و y از گروه G برحسب زیرگروه H هم‌ارزند اگر و فقط اگر به یک هم‌مجموعه H تعلق داشته باشند. به عبارت دیگر $x \sim_H y$ اگر و فقط اگر برای عضوی از H مانند h داشته باشیم $x = yh$.

اینک به پیروی از فروبنیوس[1] یک رابطه هم‌ارزی دیگری را که متضمن دو زیرگروه می‌باشد مورد بحث قرار می‌دهیم. فرض کنیم A و B دو زیرگروه G باشند، که لزوماً متمایز نیستند؛ دو عضو $x , y \in G$ را هم‌ارز می‌نامیم و می‌نویسیم $x \sim y$ (برحسب A و B)، هرگاه اعضایی چون u و v که $u \in A$ و $v \in B$ موجود باشند به قسمی که

$$y = uxv$$

به‌آسانی می‌توان بررسی کرد که این رابطه، یک رابطه هم‌ارزی در G است:

---

1. Frobinus

(الف) $x \sim x$ زیرا می‌توانیم بگیریم. $u = e$ و $v = e$.

(ب) اگـر $x \sim y$، آنگـاه $y \sim x$. زیـرا از (۱) لازم مـی‌آید کـه $x = u^{-1}yv^{-1}$ و البـته $u^{-1} \in A$ و $v^{-1} \in B$.

(ج) اگر $x \sim y$ و $y \sim z$، یعنی $y = uxv$ و $z = u'yv'$ که در آن $u, u' \in A$ و $v, v' \in B$ آنگاه $z = (uu')x(vv')$ و لذا $x \sim z$.

بنابراین می‌توان مجموعهٔ G را به رده‌های هم‌ارزی از هم‌جدا، که از تعریف این هم‌ارزی به وجود می‌آیند، افراز کرد. ردهٔ هم‌ارزی شامل x، عبارت است از مجموعهٔ همهٔ اعضایی از G که با x هم‌ارزند. امّا اگر y با x هم‌ارز باشد، $y = uxv$، که در آن $u \in A$ و $v \in B$. پس ردهٔ هم‌ارزی شامل x زیر مجموعهٔ

$$AxB = \{uxv \mid u \in A , v \in B\}$$

از G است. مجموعهٔ AxB را یک **هم‌مجموعه مضاعف** G نسبت به A و B می‌نامیم. واضح است که AxB شامل x است و از این رو گاهی (به خصوص وقتی که A و B در طول بحث ثابت فرض شده باشند) A و B را به‌طور صریح ذکر نکرده و AxB را ***هم‌مجموعه مضاعف شامل*** x نیز می‌نامند.

بنابر قضیه بنیادی رابطه‌های هم‌ارزی،

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

یک افراز G است که در آن I مجموعهٔ اندیس‌گذاری است که در تناظر یک به یک با مجموعهٔ هم‌مجموعه‌های مضاعف می‌باشد.

وقتی G نامتناهی باشد. I احتمالاً نامتناهی است. ولی اگر G متناهی باشد، I نیز الزاماً متناهی خواهد بود. (چرا؟).

وقتی G یک گروهٔ متناهی باشد. مطالب از جالبیت خاصی برخودار است. قبلاً به بیان یک لم می‌پردازیم.

۲.۱ لم

فرض کنیم G یک گروه متناهی و A و B دو زیرگروه G باشند، در این صورت

$$|AB| = \frac{|A|\ |B|}{|A \cap B|}$$

باید توجه داشت که در اینجا AB به‌عنوان یک زیر مجموعهٔ G مطرح است، صرفنظر از آنکه یک زیرگروه G باشد و یا زیرگروه G نباشد.

برهان

اثبات این لم که به قضیه حاصلضرب مشهور است به‌عنوان تمرین به دانشجویان محول می‌شود. (راهنمایی قرار دهید $D = A \cap B$. چون D زیرگروه B است از تجزیهٔ B به هم‌مجموعه‌های D استفاده کنید.)

۲.۱ قضیه فروبنیوس

فرض کنیم G گروهی متناهی از مرتبهٔ g و A و B زیرگروههایی از آن به‌ترتیب از مراتب a و b باشند. در این صورت اعضایی مانند t_1، t_2، . . . ، t_r وجود دارند به قسمی که G برابر اجتماع هم‌مجموعه‌های مضاعف از هم‌جدا می‌باشد. به عبارت روشنتر

$$G = At_1B \cup At_2B \cup \cdots \cup At_rB \qquad (\times\times)$$

تعداد عضوهای At_iB برابر ab/d_i است که در آن

$$d_i = \left| t_i^{-1}At_i \cap B \right|$$

در نتیجه

$$g = ab\sum_{i=1}^{r} d_i^{-1} \qquad (\times\times\times)$$

برهان

ابتدا ملاحظه می‌کنیم که ترکیبهای At_i ـ B و $(t_i^{-1}At_i)^B$ هم‌عدد (هم‌مرتبه) هستند، زیرا می‌توان اعضای آنها را با جورکردن ut_iv با $t_i^{-1}(ut_iv)$ در یک تناظر یک به یک قرارداد. لذا

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

اما $t_i^{-1}At_i$ یک زیرگروه G است که با A مزدوج است. پس

$$\left| t_i^{-1} A t_i \right| = |A| = a$$

با به کار بستن قضیه حاصلضرب برای زیرگروههای B و $t_i^{-1}At_i$، ملاحظه می‌کنیم که

$$\left| At_i B \right| = \frac{ab}{d_i}$$

که در آن $d_i = \left| t_i^{-1} A t_i \cap B \right|$. اکنون گوییم تساوی (×) حالت خاصی از تساوی (××) است. با شمارش اعضای دو طرف (××) رابطهٔ (×××) به‌دست می‌آید.

۲. قضیه‌های سیلو

۱.۲ قضیهٔ اصلی

فرض کنیم G گروهی متناهی از مرتبهٔ g و p عدد اولی باشد که p^b عدد g را عاد کند، و b عدد صحیح مثبتی است. در این صورت G دارای m زیرگروه از مرتبهٔ p^b است، که m عدد صحیح مثبتی است که در رابطهٔ $m \equiv 1 \pmod p$ صدق می‌کند.

برهان

(۱) می‌نویسیم

$$g = p^b z \tag{۱.۱.۲}$$

که z عدد صحیح مثبتی است که لزومی ندارد با p متباین باشد. فهرست کامل $\mathcal{K}$ از همهٔ زیر مجموعه‌هایی از G را که شامل p^b عنصراند تشکیل می‌دهیم. بدین‌گونه هرگاه n تا از این زیر مجموعه‌ها وجود داشته باشد، می‌نویسیم

$$\mathcal{K}: K_1, K_2, \cdots, K_n \tag{۲.۱.۲}$$

در حقیقت، n مساوی ضریب دو جمله‌ای $\binom{g}{p^b}$ است؛ اما این آگاهی از این به بعد مورد نیاز نخواهد بود. حکم قضیه این است که دست کم یکی از این زیر مجموعه‌های (۲.۱.۲) زیرگروه است.

یک زیرمجموعهٔ K فقط و فقط زمانی به $\mathcal{K}$ متعلق است که داشته باشیم

$$|K| = p^b$$

هرگاه x عضوی از G باشد، آنگاه $|Kx| = |K|$. از این رو Kx نیز به $\mathcal{K}$ تعلق خواهد داشت. در واقع، نگاشت

$$K_i \to K_i x \ (i = 1, 2, \cdots, n)$$

۱۵ اسلاید

یک جایگشت از $\mathcal{K}$ تشکیل می‌دهد. در این صورت گوییم که G بر $\mathcal{K}$ اثر می‌کند. با در نظر گرفتن این عمل می‌توانیم یک رابطهٔ هم‌ارزی، مطابق آنچه که ذیلاً می‌آید، در $\mathcal{K}$ تعریف کنیم؛ زیر مجموعه‌های K_i و K_j را هم‌ارز نامیم، هرگاه عضوی مانند x از G وجود داشته باشد به‌طوری که $K_i = K_j x$. خواننده در تحقیق اینکه بنداشتهای معمولی یک رابطهٔ هم‌ارزی برقرارند مشکلی نخواهد داشت. در نتیجه، $\mathcal{K}$ به دسته‌های هم‌ارزی دو به دو از هم جدا، که آنها را در این مبحث مدار می‌نامیم، افراز می‌شود. بدین‌گونه مدار K، که آن را به $o(K)$ نشان می‌دهیم، مشتمل بر همهٔ زیر مجموعه‌های Kx $(x \in G)$ است. وقتی x در G تغییر می‌کند، در حالت کلی، هر عضو مدار چندین مرتبه به‌دست می‌آید. تعداد زیر مجموعه‌های متمایز $o(K)$ به $|o(K)|$ نشان داده می‌شود. پس تجزیهٔ $\mathcal{K}$ به مدارها به صورت

$$\mathcal{K} = o(K) \cup o(K') \cup o(K'') \cup \cdots \qquad (۳.۱.۲)$$

بیان می‌شود که در آن K، K'، K''، ... مجموعه‌ای از نماینده‌های مدارهاست. با شمارش اعضای دو طرف به‌دست می‌آوریم

$$n = |o(K)| + |o(K')| + |o(K'')| + \cdots \qquad (۴.۱.۲)$$

(۲) اینک یکی از مدارها، مثلاً $o(K)$، را با جزئیات بیشتری مورد مطالعه و تحقیق قرار می‌دهیم. فرض کنیم S پایدارساز K تحت عمل G باشد، یعنی

$$S = \{ u \in G \mid Ku = K \}$$

خواننده به‌آسانی می‌تواند تحقیق کند که S یک زیرگروه G است. فرض کنیم که

$$G = \bigcup_{i=1}^{r} S t_i \qquad (t_1 = 1)$$

تجزیهٔ هم‌مجموعه‌ای راست G نسبت به S باشد. ادعا می‌کنیم که $o(K)$ از زیر مجموعه‌های

$$K t_1, K t_2, \cdots, K t_r \qquad (۵.۱.۲)$$

تشکیل شده است. بدیهی است که همهٔ این مجموعه‌ها به $o(K)$ تعلق دارند، و از هم متمایزند؛ زیرا اگر $Kt_i = Kt_j$، نتیجه می‌شود که $Kt_it_j^{-1} = K$، یعنی $t_it_j^{-1} \in S$ و بنابراین $St_i = St_j$، که ایجاب می‌کند $i = j$. در مرحلهٔ بعد، گوییم هر عضو دلخواهی از $o(K)$ به‌صورت Kx است. هرگاه x در هم‌مجموعه St_i واقع باشد، داریم $x = ut_i$ که در آن $u \in S$، و از این‌رو $Kx = Kut_i = Kt_i$. بدین‌گونه ثابت کرده‌ایم که

$$|o(k)| = [G:S] \tag{۶.۱.۲}$$

اصلاع بیشتر در مورد S را می‌توان از این واقعیت که عدد اصلی K به صورت عددی است اول ـ توان به‌دست آورد. ویژگی معروف پایدارساز را می‌توان به‌وسیلهٔ معادلهٔ

$$KS = k$$

که آن را به‌صورت رابطه‌ای بین زیر مجموعه‌هایی G تلقی می‌کنیم، بیان کرد. دقیقتر بگوییم اگر $k = v_1 \cup v_2 \cup v_3 \cup \ldots$، آنگاه داریم

$$K = v_1S \cup v_2S \cup v_3S \cup \cdots \tag{۷.۱.۲}$$

لذا K اجتماع هم‌مجوعه‌های چپ S است. می‌دانیم هر دو تا از این هم‌مجموعه‌ها یا متمایزند و یا یکی هستند و هر یک دارای $|S|$ عضو است. لذا هرگاه تعداد هم‌مجوعه‌های متمایز ۷.۱.۲ برابر f باشد، داریم

$$p^b = f\,|S| \tag{۷.۱.۲}$$

از اینجا نتیجه می‌شود که $|S|$ توانی از p است، مثلاً

$$|S| = p^c \tag{۸.۱.۲}$$

که در آن $c \le b$. اما دو حالت را باید از هم تمیز داد.

(الف) $|S| = p^b$. ولیّ 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 (۱.۱.۲) تعریف شده است. چون حالا $|S|$ بزرگترین مقدارش را اختیار می‌کند،

می‌توانیم $o(K)$ را یک مدار مینیمال بنامیم. چون بنابرفرض کنونی، K و S دارای یک عدد اصلی‌اند، از ۷.۱.۲ نتیجه می‌گیریم که K به یک هم‌مجموعه تنها بدل می‌شود، مثلاً

$$K = vS \quad (v \in K)$$

روشن است که زیر مجموعهٔ

$$H = Kv^{-1} = vSv^{-1}$$

متعلق به $o(K)$ و بنابراین یک زیرگروه است، یعنی گروهی که با S مزدوج است. لذا ما به این نتیجه رسیده‌ایم که هر مدار مینیمال شامل حداقل یک زیرگروه است. چون $|H| = p^b$، نتیجه می‌شود که

$$[G:H] = z = |o(K)|$$

فرض کنیم

$$Hw_1, Hw_2, \cdots, Hw_z \qquad (۹.۱.۲)$$

هم‌مجموعه‌های H در G باشند. هر یک 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 یک مدار مینیمال شامل یک، و فقط یک زیرگروه G است.

(ب) $|S| = p^c < p^b$. در این حالت مدار $o(K)$ مینیمال نیست و

$$|o(K)| = \frac{g}{p^b} = zp^{b-c}$$

- از این‌رو

$$|o(K)| \equiv 0 \pmod{pz} \qquad (۱۰.۱.۲)$$

یک مدار غیرمینیمال نمی‌تواند شامل یک زیرگروه باشد؛ زیرا در غیر این صورت می‌توانیم این زیرگروه را به‌عنوان یک مولد $o(K)$ اختیار کنیم؛ و لذا بی‌آنکه خللی به کلیت استدلال وارد شود می‌توانیم فرض کنیم که خود K یک گروه باشد. در این‌صورت K در پایدار سازش قرار خواهد گرفت، زیرا $KK = K$. لذا $|S| \geq |K| = p^b$، که با فرض (ب) ناسازگار

است.

(۳) اکنون به ۴.۱.۲ باز می‌گردیم و جملات مینیمال را، در صورت وجود، از بقیه جدا می‌کنیم. در هر مدار مینیمال دقیقاً یک 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 است که در قضیهٔ اصلی تعریف شده است. (با این حال متذکر می‌شویم که در این مرحله هنوز نمی‌دانیم که آیا m مثبت است یا نیست.) بنابراین کل سهامی که از همهٔ مدارهای مینیمال به (۴.۱.۲) مربوط می‌شود برابر m است از آنجا که، بنابر (۱۰.۱.۲)، هر یک از جملات باقیمانده در (۴.۱.۲)،(۱۱.۱.۲) بر pz بخشپذیر است، می‌توانیم وضع را با همنهشتی

$$n \equiv mz \pmod{Pz} \qquad (۲۰۱۰۱۱)$$

خلاصه کنیم. این یک جنبهٔ مهم این برهان است که عدد n، که در صفحهٔ ۱۳ تعریف شد، فقط بستگی به مرتبهٔ گروه G دارد نه به ساختار آن. از این‌رو، n برای همهٔ گروههای از مرتبهٔ P^bz یکی است، در حالی که m برای یک n ثابت تغییر می‌کند. بنابراین باید (۱۱.۱.۲) را صریحاً چنین بنویسیم

$$n = m_G z + k_G Pz$$

که در آن m_G و k_G اعداد صحیحی هستند که به G بستگی دارند. برای آنکه اطلاعی دربارهٔ n به‌دست آوریم این نتیجه را برای گروه دوری C از مرتبهٔ $p^b z$ به‌کار می‌بریم. می‌دانیم که C دقیقاً یک زیرگروه از مرتبهٔ p^b دارد.

بنابراین $m_c = ۱$ و لذا

$$n = z + k_c Pz$$

از مساوی قراردادن دو عبارتی که برای n پیدا کردیم خواهیم داشت

$$z + k_c pz = m_G z + k_c Pz$$

از اینجا با تقسیم دو طرف تساوی بر z، خواهیم داشت

$$m_G \equiv ۱ \pmod{p}$$

و این همان چیزی است که ادعا شده بود و لذا برهان تمام است.

۲.۲ نتیجه (قضیه کوشی)

اگر $p \mid |G|$ آنگاه G زیرگروهی p عضوی دارد.

برهان

این قضیه نتیجهٔ فوری قضیهٔ قبل است.

معمولاً نتایج سیلو در سه قضیهٔ اصلی عرضه می‌شوند که ما آنها را در این بخش بیان می‌کنیم.

۳.۲ قضیه (اولین قضیهٔ سیلو)

هرگاه p^a بزرگترین توانی از عدد اول p باشد که مرتبهٔ گروه G را عاد می‌کند، آنگاه G دارای حداقل یک زیرگروه از مرتبهٔ p است.

برهان

این یک حالت خاص قضیهٔ ۱.۲ است. این قضیه متناظر با بزرگترین مقدار ممکن برای نمای b است.

۴.۲ تعریف

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 یک p-زیرگروه سیلوی G می‌نامند.

به ازای یک عدد اول، یک گروه G ممکن است بیش از یک زیرگروه سیلو داشته باشد. در واقع، هرگاه p زیرگروهی از مرتبهٔ p^a و x عضو دلخواهی از G باشد، $x^{-1}Px$ نیز یک زیرگروه از مرتبهٔ p^a است. به عبارت دیگر، مزدوج یک زیرگروه سیلو نیز یک گروه سیلو است. البته لزومی ندارد که گروههای مزدوجی متمایز باشند اما قضیهٔ بعدی به ما می‌گوید که هیچ‌گروه سیلوی دیگری وجود ندارد؛ یعنی همهٔ گروههای سیلویی که نظیر یک عدد اول هستند با هم مزدوج‌اند.

۵.۲ قضیه (دومین قضیهٔ سیلو)

همهٔ گروههای سیلوی G که متناظر با یک عدد اول هستند با یکدیگر در G مزدودج‌اند.

برهان

همچون تعریف ۳.۲ قرار می‌دهیم $|G| = g = p^a g'$ ، که در آن ۱ = (g', p). فرض کنیم A و B دو زیرگروه از مرتبهٔ p^a باشند. از تجزیهٔ مضاعف G نسبت به A و B که در قضیه ۳.۱ ذکر شد استفاده می‌کنیم، لذا در حالت کنونی

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

$$g = p^{2a} \sum_{i=1}^{r} d_i^{-1} \qquad (۱.۴.۲)$$

$$d_i = \left| t_i^{-1}At_i \cap B \right| \qquad (۲.۴.۲)$$

از تقسیم سراسر ۱.۴.۲ بر p^a به‌دست می‌آوریم

$$g' = p^a \sum_{i=1}^{r} d_i^{-1} \qquad (۳.۴.۲)$$

اما d_i مرتبهٔ یک زیرگروه B است و لذا باید با توانی نامنفی از p برابر باشد. از این‌رو هر جملهٔ ۳.۴.۲ یا برابر یک 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 یک باشد، مثلاً $p^a d_j^{-1} = 1$، یعنی $d_j = p^a$. پس داریم

$$p^a = \left| t_j^{-1}At_j \cap B \right|$$

چون گروههای $t_j^{-1}At_j$ و B هر دو از مرتبهٔ p^a هستند، اشتراک آنها فقط وقتی می‌تواند از مرتبهٔ p^a باشد که این گروهها یکی باشند. لذا

$$B = t_j^{-1}At_j$$

یعنی، همان‌گونه که می‌خواستیم ثابت کنیم، A و B مزدوج هستند.

۶.۲ نتیجه

یک گروه متناهی G متناظر با یک عدد اول مفروض p فقط و فقط وقتی دارای یک زیرگروه سیلوی

یکتای P است که P در G نرمال باشد.

برهان

شرط یکتایی با این حکم که به ازای هر x از G، تساوی $x^{-1}Px = P$ برقرار است هم‌ارز است؛ اما این بدان‌معنی است که P یک زیرگروه نرمال است.

قضیهٔ اصلی بعدی اطلاعات دقیقتری دربارهٔ تعداد p-زیرگروههای سیلو به‌دست می‌دهد. قبل از آن به بیان یک لم می‌پردازیم

۷.۲ لم

فرض کنیم H یک زیرگروه از گروه G باشد. در این صورت تعداد زیرگروههای مزدوج با H برابر است با $[G:N(H)]$.

برهان

می‌دانیم هر زیرگروه مزدوج با H به فرم $t^{-1}Ht$ است که t در G تغییر می‌کند. تناظر

$$\theta: t^{-1}Ht \to N(H)t$$

نگاشتی بین مجموعهٔ زیرگروههای مزدوج با H و هم‌مجموعه‌های $N(H)$ در G تعریف می‌کند. چون در سمت چپ ضابطهٔ تعریف θ، t در سرتاسر G تغییر می‌کند، پس در سمت راست آن نیز t در سرتاسر G تغییر کرده و لذا $N(H)t$. همه هم‌مجموعه‌های زیرگروه $N(H)$ هستند؛ لذا A پوشا است. θ یک به یک است: زیرا اگر

$$N(H)t = N(H)s$$

آنگاه بنابر شرط تساوی هم‌مجموعه‌ها، $ts^{-1} \in N(H)$؛ در نتیجه

$$ts^{-1}H = Hts^{-1}$$

از این‌رو

$$s^{-1}Hs = t^{-1}Ht$$

۸.۲ قضیه (سومین قضیهٔ سیلو)

فرض کنیم r تعداد p-زیرگروههای سیلوی G باشد. در این صورت r عددی است صحیح به صورت $pk+1$ و مقسوم‌علیهی است از مرتبهٔ G

برهان

این حقیقت که $r \equiv 1 \pmod p$، قبلاً در قضیهٔ اصلی ۱.۲ ثابت شده است باقی‌می‌ماند اثبات اینکه $r|g$، که در آن $|G| = g$. فرض کنیم

$$\mathcal{P}: P_1 (=P), P_2, \ldots, P_r$$

مجموعهٔ کلیهٔ p-زیرگروههای سیلوی G باشد. در این صورت، بنابرقضیهٔ ۴.۲، $\mathcal{P}$ یک مجموعهٔ کامل از مزدوجهای P است. اما بنابر لم ۶.۲

$$r = [G:N(P)] \tag{۱.۷.۲}$$

که در آن $N(P)$ نرمالساز P در G است. لذا، اگر $n = |N(P)|$، آنگاه $g = nr$، که نشان می‌دهد $r|g$. رابطهٔ (۱.۷.۲) مشابه (۶.۱.۲) است. در واقع، می‌توانیم از مربوط کردن نگاشت

$$P \to x^{-1}Px \quad (P \in \mathcal{P})$$

به یک عنصر دلخواه x از G روی مجموعهٔ $\mathcal{P}$ راکه موجب یک جایگشت از $\mathcal{P}$ می‌شود، تعریف می‌کند، همهٔ عضوهای $\mathcal{P}$ به دست 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 در مقولهٔ حاضر پایدارساز برابر نرمالساز است. از نوشتن $N(P)$ به جای S، می‌بینیم که ۶.۱.۲ به ۱.۷.۲ تبدیل می‌شود.

۳. معادلهٔ کلاس و p-گروهها

در سرتاسر این بخش p نمایش یک عدد اول است گروه متناهی G را یک p-گروه نامیم هرگاه مرتبه G توانی از p باشد. ابتدا معادلهٔ کلاس یک گروه متناهی را ثابت می‌کنیم و سپس نشان می‌دهیم که هر گروه از مرتبه p^2 یک گروه آبلی است. از مطالبی که در پیش آزمون ذکر شد، به‌ویژه‌بندیهای ۶ و ۷ بهره می‌گیریم.

۱.۳ قضیه

فرض‌کنیم a عضوی از G و $C(a)$ مرکزساز a باشد. در این صورت اعضای $[a]$، کلاس مزدوجی a، با هم‌مجموعه‌های $C(a)$ در G در تناظر یک به یک هستند. به ویژه وقتی که اندیس $C(a)$

متناهی باشد، آنگاه $|[a]| = [G : C'(a)]$.

برهان

نگاشت

$$\theta : C(a)x \to x^{-1}ax$$

را در نظر می‌گیریم. (θ هر عضو مجموعهٔ هم‌مجموعه‌های $C(a)$ را به عضوی از $[a]$ می‌نگارد.) ابتدا باید نشان دهیم که خوش‌تعریف است فرض کنیم $C(a)x = C(a)y$. در این صورت $C(a)ux = C(a)x$ که u عضو دلخواهی از $C(a)$ است (چرا؟). بدین‌ترتیب باید نشان دهیم که قراردادن ux به جای x، سمت راست تعریف θ را تغییر نمی‌دهد. در واقع،

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

زیرا $u \in C'(a)$. چون x عضو دلخواهی از G است، واضح است که نگاشت θ بر روی کلاس $[a]$ نگاشتی پوشا نیز می‌باشد. بالاخره، ملاحظه می‌کنیم که θ یک به یک نیز هست؛ زیرا اگر $x^{-1}ax = y^{-1}ay$، آنگاه $xy^{-1} \in C(a)$. از اینجا نتیجه می‌گیریم که $C(a)x = C(a)y$. لذا، چنانکه ادعا کرده بودیم، تناظر فوق یک به یک است.

۲.۳ نتیجه

اگر G گروهی متناهی از مرتبهٔ g و h_a تعداد اعضای $[a]$ باشد، آنگاه $h_a | g$.

برهان

فرض کنیم $C_a = |C(a)|$. پس بنابر قضیهٔ قبل، $h_a = |C_a|$، یعنی $g = c_a h_a$. فرض کنیم گروهی متناهی G دارای K کلاس مزدوجی متمایز باشد. فرض می‌کنیم $a_1 (=e)$، a_2، ...، a_k مجموعه‌ای از نماینده‌ها باشد و $h_i = |(a_i)|$. در این صورت

$$G = [a_1] \cup [a_2] \cup \cdots \cup [a_k]$$

از این‌رو، با شمارش اعضای دو طرف این تساوی نتیجه می‌شود

$$g = h_1 + h_2 + \cdots + h_k$$

این تساوی، معادلهٔ کلاس G خوانده می‌شود.

۳.۳ تبصره

یادآوری می‌کنیم که هر عضو G که متعلق به مرکز G باشد با این واقعیت که خودش به تنهایی یک کلاس مزدوجی می‌سازد، مشخص می‌شود، زیرا اگر z فقط با خودش مزدوج باشد، آنگاه به ازای هر $t \in G$، $t^{-1}zt = z$، و این بدان‌معنی است که $z \in Z$ که در آن Z مرکز G است. بدین علت، گاهی یک عضو مرکزی را خود-مزدوج نیز می‌خوانند.

قضیهٔ زیر از این لحاظ جالب است که وجود یک مرکز غیر بدیهی را برای دستهٔ مهمی از گروهها اثبات می‌کند.

۴.۳ قضیه

اگر G یک گروه متناهی باشد به قسمی که $|G| = p^m$، P یک عدد اول و $m > 0$، آنگاه مرکز G از مرتبهٔ p^{μ} است که $0 < \mu \leq m$.

برهان

معادلهٔ کلاس G در این حالت چنین می‌شود

$$p^m = h_1 + h_2 + \cdots + h_k$$

که در آن برای هر $1 \leq \alpha \leq k$، $h_\alpha \mid p^m$. چون p عددی اول است، پس لازم است که $h_\alpha \mu$ یا برابر واحد باشد و یا توانی از p. قبلاً می‌دانستیم که $h_1 = 1$. فرض کنیم دقیقاً $e\ (\geq 1)$ مقدار برای α وجود داشته باشد به قسمی که $h_\alpha = 1$. در این صورت می‌توانیم به ازای عدد صحیحی مانند s، تساوی فوق را به صورت

$$p^m = l + p^s t$$

بنویسیم. از اینجا نتیجه می‌شود که l بر p بخش‌پذیر است و چون l مثبت است، نتیجه می‌گیریم که $e \geq p$. لذا حداقل p عضو خود مزدوج وجود دارد. یعنی Z غیر بدیهی است. چون Z یک زیرگروه G است، قضیه لاگرانژ این اطلاع را به ما می‌دهد که $|Z| = p^{\mu}$، که در آن $0 < \mu \geq m$.

۵.۳ قضیه

اگر G غیر آبلی و مرکز آن Z باشد، آنگاه G/Z هیچگاه دوری نیست.

برهان

اگر G/Z یک گروه دوری می‌بود (فرض خلف)، آنگاه کلیه هم‌مجموعه‌های Z می‌توانستند به‌صورت Zt^i بیان شوند که در آن t عضو مناسبی است از G که در Z نیست و

$$i = 0, \pm 1, \pm 2, \dots$$

اما اگر x و y اعضای دلخواهی از G و به ترتیب متعلق به Zt^i و Zt^k باشند، باید داشته باشیم:

$$x = z_1 t^i, \qquad y = z_2 t^k$$

که $z_1, z_2 \in Z$ و بنابراین

$$xy = z_1 t^i z_2 t^k = z_1 z_2 t^{i+k} = yx$$

یعنی G آبلی خواهد بود که با فرض ما در تناقض است.

۶.۳ نتیجه

هر گروه از مرتبهٔ p^2، که p عدد اول باشد، لزوماً آبلی است.

برهان

بنابر قضیهٔ قبل، $|Z|$ برابر p و یا برابر p^2 است. اگر $|Z| = p^2$ آنگاه $G = Z$ و گروه آبلی است. در غیر این صورت فرض کنیم $|Z| = p$ (فرض خلف). پس ~~$G \neq Z$~~ و لذا G ~~غیر آبلی~~ است. اما در این حالت، $|G/Z| = P$ و بنابراین G/Z دوری خواهد بود که بنابر ~~قضیهٔ پیش قابل قبول نیست~~. G آبلی

۴. کاربردهای و مثالها

قضیه‌های سیلو ابزاری توانا برای مطالعهٔ ساختار یک گروه متناهی به دست می‌دهند. استفاده از این قضیه‌ها، به ویژه وقتی مؤثر است که گروه مورد مطالعه به ازای یک عدد اول، منحصراً یک زیرگروه سیلو داشته باشد.

۱.۴ قضیه

فرض‌کنیم G از مرتبهٔ pq باشدکه p و q اعداداولی‌هستند با شرایط $p < q$ و $q \not\equiv 1 \pmod p$. در این صورت G لزوماً آبلی است.

برهان

فرض کنیم تعداد p-زیرگروههای سیلو G برابر r باشد بنابر قضیه ۸ـ۲، $r|pq$ و $r = 1 + pk$. لذا $(r,p) = 1$ و از اینرو $r|q$. چون p اول است، نتیجه می‌شود که $r = 1$ یا $r = q$. معنی حالت دوم این است که $p = 1 + pk$، یعنی $q \equiv 1 \pmod p$، که بنابر فرض کنار گذاشته شده است. لذا بنا نتیجهٔ ۶.۲، G فقط یک زیرگروه P از مرتبهٔ p داردکه لزوماً دوری می‌باشد. مولد این زیرگروه را به u نشان می‌دهیم. بنابراین

$$P \lhd G, P = \langle u \rangle \qquad (۲.۷.۲)$$

در مرحله بعد، فرض کنیم تعداد q-زیرگروهای سیلوی G برابر s باشد. پس $s|pq$ و $s = 1 + ql$. چون $(s,p) = 1$، بایدداشته‌باشیم $s|p$ و لذا $s \le p$. اگر $l \ge 1$، آنگاه $s \ge 1 + q > p$ که یک تناقض است. نتیجه می‌شود که $l = 0$ و G دارای یک زیرگروه نرمال مانند Q از مرتبهٔ q و با مولدی چون v است. لذا

$$Q \lhd G, Q = \langle v \rangle \qquad (۳.۷.۲)$$

چون مرتبه‌های P و Q متناهی‌اند، داریم

$$P \cap Q = \{I\} \qquad (۴.۷.۲)$$

از مسأله ۵ پیش آزمون نتیجه می‌شود که اعضای P و Q دو به دو تعویض‌پذیرند. به ویژه حاصلضربهای

$$u^{\alpha} v^{\beta} (\alpha = 0, 1, \cdots, p-1, \quad \beta = 0, 1, \cdots, q-1)$$

متمایزند، زیرا هر تساوی بین آنها با ۴.۷.۲ در تناقض است. از اینرو این اعضا تمام گروه را تشکیل می‌دهند چونکه تعداد آنها برابر pq می‌باشد. چون u^i و v^j ($0 \le i \le p-1$، $0 \le j \le q-1$) با هم تعویض‌پذیرند آبلی بودن گروه اکنون واضح است.

مثال ۱. هیچ گروه سادهٔ مرتبهٔ ۲۰۰ وجود ندارد.

زیرا چون $200 = 5^2 \times 8$، این گروه شامل r گروه سیلو از مرتبه ۲۵ است که در آن r به صورت $5k + 1$ و یک مقسوم علیه ۲۰۰ نیز هست. چون $(r, 5) = 1$، باید داشته باشیم $r \mid 8$، که ناممکن است مگر آنکه $k = 0$. از این‌رو این گروه شامل یک زیرگروه نرمال منحصر به فرد از مرتبه ۲۵ بوده و بنابراین ساده نیست.

مثال ۲. هیچ گروه سادهٔ مرتبهٔ ۳۰ وجود ندارد.
برای آنکه چنین گروهی وجود داشته باشد. هیچ یک از زیرگروههای سیلو منحصر به فرد نمی‌شود. لذا $5 + 1\ (= 6)$ زیرگروه سیلوی متمایز مرتبهٔ ۵ موجود خواهد بود که شامل $6 \times 4\ (= 24)$ عضو مرتبهٔ ۵ هستند (چرا؟). به طریق مشابه، $3 \times 3 + 1\ (= 10)$ زیرگروه سیلوی متمایز مرتبهٔ ۳ خواهیم داشت که ۲۰ عضو مرتبهٔ ۳ به دست می‌دهند (چرا؟). بدین طریق تعداد کل اعضا گروه از ۳۰ تجاوز خواهد کرد که این امر ناممکن است.

مطلب را با یک نتیجهٔ کلیتر دربارهٔ زیرگروههای سیلو ادامه می‌دهیم.

۳.۴ قضیه

فرض کنیم H یک زیرگروه سیلو از یک گروه متناهی G شامل نرمالساز P باشد. در این صورت H نرمالساز خودش است.

برهان

باید ثابت کنیم که $N(H) = H$. چون همواره $H \subseteq N(H)$ (چرا؟) کافی است جزئیت $N(H) \subseteq H$ را نشان دهیم. برای این کار فرض کنیم $u \in N(H)$؛ پس
$u^{-1}Hu = H$. اما $P \le N(P) \le H$، و از اینرو $u^{-1}Pu \le u^{-1}Hu = H$. لذا $u^{-1}Pu$ نیز، که با P هم مرتبه است (چرا؟) یک زیرگروه سیلوی H است. با به کاربردن قضیهٔ ۵.۲ برای H نتیجه می‌گیریم که عضوی مانند h_1 از H وجود دارد به قسمی که

$$h_1^{-1}(u^{-1}Pu)h_1 = P$$

این بدان معنی است که

$$(uh_1)^{-1}P(uh_1) = P$$

یعنی $uh_1 \in N(P)$. چون بنابر فرض، $N(P) \subseteq H$، از اینجا نتیجه می‌شود که $= h_1$

uh_1، که در آن $h_2 \in H$. لذا $u \in H$، و قضیه ثابت می‌شود.

۴.۴ چند مثال دیگر

مثال ۳. فرض کنیم G یک گروه از مرتبه ۱۲۲۵ باشد. داریم:

$$1225 = 5^2 \times 7^2$$

اکنون ۵ زیرگروههای سیلوی G را بررسی می‌کنیم. گیریم s برابر ۵ زیرگروههای سیلوی G باشد. سپس $s = 1 + 5k$ ؛ $s \mid 5^2 \times 7^2$. لذا $s \mid 7^2$ در نتیجه $s = 1$ یا $s = 7$ و یا $s = 49$. چون $s = 1 + 5k$ پس $s = 7$ و $s = 49$ درست نیستند و $s = 1$. لذا G تنها یک ۵ زیرگروه سیلو مانند H دارد ؛ پس H در G نرمال است. چون $|H| = 5^2$ ، H آبلی است.

سپس ۷ ـ زیرگروههای سیلوی G را بررسی می‌کنیم. فرض کنیم t برابر تعداد ۷ زیرگروهای سیلوی باشد. پس $t = 1 + 7k$ و $t \mid 5^2 \times 7^2$، چون $(t, 7) = 1$، باید $t \mid 5^2$. لذا $t = 1$ یا $t = 5$ یا $t = 5^2$. چون $t = 1 + 7k$. نتیجه می‌گیریم که $t = 1$ و G تنها یک ۷ ـ زیرگروه سیلو مانند K دارد پس بنابر نتیجهٔ ۵.۲، K یک زیرگروه نرمال G است. چون $|K| = 7^2$ ، K آبلی است.

در مرحله بعد، ادعا می‌کنیم که

$$G \cong H \times k \qquad \text{(حاصلضرب مستقیم)}$$

زیرا

$$|H \times K| = \frac{|H|\,|K|}{|H \cap K|} = \frac{5^2 \times 7^2}{1} = 5^2 \times 7^2 = |G|$$

چون H و K در G نرمال‌اند و $H \cap K = 1$ برای هر عضو H مانند h و هر عضو K مانند k داریم $hk = kh$ (چرا؟) پس نتیجه می‌گیریم که

$$G \cong H \times K$$

چون H و K آبلی‌اند، حاصلضرب مستقیم آنها نیز آبلی است. لذا G آبلی است

مثال ۴. ثابت کنید هیچ گروهی از مرتبهٔ ۲۴ ساده نیست.

حل داریم

$$24 = 2^3 \times 3$$

فرض کنیم تعداد ۲-زیرگروههای سیلوی G برابر r باشد. لذا $r = 1 + 2k$ و $r \mid 3 \times 2^3$. پس $r = 1$ یا $r = 3$.

همچنین فرض می‌کنیم تعداد ۳-زیرگروههای سیلوی G برابر s باشد. لذا $s = 1 + 3k$ و $s \mid 2^3 \times 3$. پس $s = 1$ و یا $s = 4$. ادعا می‌کنیم که حداقل یکی از r و s باید برابر ۱ باشد. زیرا در غیر این صورت، $r = 3$ و $s = 4$ یعنی در گروه ۲۴ عضوی G، ۳ زیرگروه ۸ عضوی متمایز و ۴ زیرگروه ۳ عضوی متمایز خواهیم داشت که غیرممکن است (چرا؟).

لذا $r = 1$ و یا $s = 4$. که در این صورت تنها یک ۲-زیرگروه سیلو و یا تنها یک ۳-زیرگروه سیلو خواهیم داشت که الزاماً نرمال خواهند بود ودر نتیجه G ساده نیست.

۳.۵ تمرین

(۱) نشان دهید که A_4 یک گروه سیلو از مرتبهٔ ۴ و چهار گروه سیلو از مرتبهٔ ۳ دارد.

(۲) یکی از ۲-زیرگروههای سیلوی S_4 را به‌دست آورید. این گروه با کدامیک از گروههای یکریخت است؟ چند ۲-زیرگروه سیلو وجود دارد؟

(۳) ثابت کنید که هیچ گروه سادهٔ مرتبه ۵۶ وجود ندارد.

(۴) فرض کنیم G گروهی است از مرتبهٔ p^2q که در آن p و q اول‌اند و q کوچکتر از p و عامل $p^2 - 1$ نیست. ثابت کنید 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، به قسمی که $|K|$ توانی از p باشد، آنگاه K حداقل در یک p-زیرگروه سیلو قرار دارد.

(۶) نشان دهید که هر 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 سیلوی H است.

(۸) ثابت کنید هیچ گروه ساده‌ای از مرتبهٔ ۴۸ وجود ندارد.

(۹) ثابت کنید هیچ گروه ساده‌ای از مرتبهٔ ۱۰۲، ۱۰۶، و یا ۱۶۰ وجود ندارد.

(۱۰) هرگاه G یک گروه و $|G| = p^k m$ که $(p, m) = 1$، $n \ge 1$، آنگاه ثابت کنید برای هر $1 \le i \le n - 1$، هر زیرگروه G از مرتبه p^i که جز یک زیرگروه از مرتبهٔ p^{i+1} عضو

باشد در آن زیرگروه نرمال است.

(۱۱) فرض کنیم q ،p دو عدد اول باشند به قسمی که $p < q$، ثابت کنید:

(الف) هیچ گروه از مرتبهٔ pq ساده نیست

(ب) اگر $p \nmid q - 1$ آنگاه هر گروه G از مرتبهٔ pq دوری است.

۳.۶ راهنمای تمرین

(۱) A_4 زیرگروهی دارد که چهارگروه کلاین V یکریخت است (V متشکل از عضوهای ۱، a، b، ab است که در آن $a^2 = b^2 = 1$ و $ab = ba$) این زیرگروه در A_4 نرمال بوده و از مرتبه ۴ است. بنابراین (قضیهٔ ۴.۲) تنها زیرگروه سیلو از این مرتبه است. هر سه-دور یک ۳-زیرگروه سیلو تولید می‌کند. منجمله (۱۲۳)، (۱۳۲). تعداد چهار تا از این گروههای مرتبه ۳ وجود دارد، که هر یک متناظر با یک انتخاب سه شیی از بین چهار شیی هستند که A_4 بر آنها اثر می‌کند.

(۲) جایگشتهای (۱۲۳۴) = a و (۳۴) = b زیرگروهی از مرتبه ۸ تولید می‌کنند که از جایگشتهای زیر تشکیل شده است

(۲۳)،(۱۴)،(۲۴)،(۱۳)،(۳۴)،(۱۳)،(۳۴)،(۱۲)،(۱۳)،(۳۴)،(۱۴۳۲)،(۱۲۳۴)،(۱)

این یک ۲-زیرگروه سیلو است. چون $a^4 = b^2 = (ab)^2 = 1$، لذا این گروه با گروه دو وجهی یکریخت است. واضح است که این زیرگروه سیلو نرمال نیست و لذا منحصر به فرد نمی‌باشد. سه ۲-زیرگروه سیلو وجود دارد. یادآوری می‌شود که گروه دو وجهی با جدول ضرب زیر مشخص می‌شود

$a^4 = b^2 = (ab)^2 = 1$:گروه دو جهی

	1	a	a^2	a^3	b	ab	a^2b	a^3b
1	1	a	a^2	a^3	b	ab	a^2b	a^3b
a	a	a^2	a^3	1	ab	a^2b	a^3b	b
a^2	a^2	a^3	1	a	a^2b	a^3b	b	ab
a^3	a^3	1	a	a^2	a^3b	b	ab	a^2b
b	b	a^3b	a^2b	ab	1	a^3	a^2	a
ab	ab	b	a^3b	a^2b	a	1	a^3	a^2
a^2b	a^2b	ab	b	a^3b	a^2	a	1	a^3
a^3b	a^3b	a^2b	ab	b	a^3	a^2	a	1

(۳) چنین گروهی (در صورت وجود) می‌بایست دارای هشت زیرگروه مرتبه ۷ و هفت زیرگروه مرتبه ۸ باشد که در یک گروه مرتبهٔ ۵۶ غیرممکن است. (چرا؟)

(۴) تعداد $xp+1$، p-زیرگروه سیلو وجود دارد که در آن لازم است $xp+1 \mid p^2q$. لذا $xp+1 \mid q$ که ایجاب می‌کند که $x=0$. تعداد $yq+1$، q-زیرگروه سیلو وجود دارد و $yq+1 \mid p^2q$ و لذا $yq+1 \mid p^2$. از اینجا لازم می‌آید که $yq+1$ مساوی ۱، p یا p^2 است. در هر دو حالت آخر داریم $q \mid p^2-1$، که کنار گذاشته شده است. لذا $G = P \times Q$، که $P = |p|$ و $|Q| = q$. چون P و Q آبلی‌اند، G نیز آبلی است.

(۵) فرض کنیم $|G| = p^m g^r$، که $(g', P) = 1$، و $|K| = p^\mu$. از تجزیه مضاعف G نسبت به K و یک زیرگروه سیلوی دلخواه مانند P استفاده کنید. مثلاً

$$G = Kt_1P \cup Kt_2P \cup \cdots \cup Kt_2P$$

همانند برهان قضیه ۴.۲، نشان داده می‌شود که حداقل یک اندیس j وجود دارد به‌طوری که $|t_j^{-1}Pt_j \cap K| = p^\mu$، یعنی $K \subseteq t_j^{-1}Pt_j$

(۶) به استناد تمرین (۵)، $t_jKt_j^{-1} \subseteq P$، چون $K \trianglelefteq G$، $t_jKt_j^{-1} = K$ لذا $K \subseteq P$.

(۷) فرض می‌کنیم که $|G| = p^m s$، که در آن $(p, s) = 1$. پس $|P| = p^m$. حال HP یک گروه است، زیرا $H \trianglelefteq G$ (چطور؟). روشن است که $P \subseteq HP$. لذا $|HP| = p^m t$، که $(p, t) = 1$. و بنابر قضیهٔ لاگرانژ $t \mid s$. رابطهٔ $HP/P \cong P/H \cap p$ (دومین قضیهٔ یکریختی گروهها)، نشان می‌دهد که HP/P یک P-گروه است، زیرا این امر برای زیرگروه سمت راست رابطه یکریختی فوق بدیهی است؛

(الف) کافی است نشان داده شود که $|G|H| : |HP/P|$ با P متباین است؛ اما این خارج‌قسمت برابر است با $s:t = |G| : |HP|$، که در واقع با P متباین است.

(ب) مجدداً بنابر دومین قضیهٔ یکریختی،

$$|H| : |H \cap P| = |HP| : |P| = t$$

و این حکم (ب) را ثابت می‌کند. (چرا؟).

(۸) $2^4 \times 3 = 48$. فرض کنید r تعداد ۳-سیلو زیرگروهها، s برابر تعداد ۲-سیلو زیرگروههای G باشد. باید نشان دهید که یا $r = 1$ و یا $s = 1$ و در آن صورت G یک زیرگروه نرمال خواهد داشت و لذا ساده نمی‌باشد.

فرض کنیم (فرض خلف) $s \neq 1$ و $r \neq 1$ و با استفاده از قضیه سوم به تناقض

برسید.

(۹) روش حل این مساله مانند روش مساله (۸) است.

(۱۱) (الف) فرض کنیم s تعداد qـ سیلوزیرگروههای G باشد. پس $s = 1 + kq$ و $s|pq$ چون $(s,q) = 1$ لذا می‌بایست $s|P$. پس $s = 1$ یا $s = qp$. ادعا می‌کنیم که $s = 1$. اگر $s = p$ لذا $p = 1 + kq$ که $x \geq 1$ و این با فرض $p > q$ در تناقض است پس G فقط یک q سیلو دارد و این نرمال است.

(ب) فرض کنیم $p \times q - 1$. به آسانی ثابت می‌شود که G فقط یک pـ زیرگروه سیلو دارد که آن را P می‌نامیم. پس P در G نرمال است. بنابراین (الف) G فقط یک qـ زیرگروه سیلو دارد که آن را Q می‌نامیم و a نیز نرمال است. چون $P \cap Q = 1$ (چرا؟) بنابر تمرینهای پیش آزمون Pـ و Q عضو به عضو تعویض‌پذیرند. لذا چون P و Q از مرتبه اول‌اند دوری بوده پس هرگاه $P = \langle u \rangle$ و $Q = \langle v \rangle$، برای هر i و j، v^j و u^i باهم تعویضپذیرند. درنتیجه $G = P \times Q$. و $G = \langle uv \rangle$ و لذا G نیز دوری است زیرا مرتبهٔ uv برابر pq است.

منابع

۱. آشنایی با نظریه گروهها؛ تالیف والتر لدرمن. ترجمه دکتر محمدحسن بیژن‌زاده، ناشر: مرکز نشر دانشگاهی، تهران ۱۳۶۷.

۲. یادداشتهای درسی، نظریه گروهها، دکتر محمدحسن بیژن‌زاده.