پردیس علوم
دانشکده ریاضی، آمار و علوم کامپیوتر

رده‌بندی ساده گروه‌های متناهی از مرتبه p^2q^2

نگارنده

انسیه میرزایی

استاد راهنما: دکتر محمدرضا درفشه

پایان‌نامه برای دریافت درجه کارشناسی
در رشته ریاضی محض

چکیده

فرض کنید G یک گروه از مرتبه p^2q^2 باشد که در آن $p > q$ اعداد اول هستند و فرض کنید P و Q به ترتیب برابر با p زیرگروه سیلو و q زیرگروه سیلوی G هستند. در این مقاله، نشان می‌دهیم که چهار گروه از مرتبه p^2q^2 با تقریب همریختی وجود دارند، هنگامی که Q و P دوری باشند. هنگامی که Q دوری و P یک گروه آبلی مقدماتی است، سه گروه وجود دارد، هنگامی که Q یک گروه آبلی مقدماتی و P یک گروه دوری است، $\frac{p^2+3p}{2+7}$ گروه وجود دارد و در نهایت، هنگامی که هم Q و P گروه‌هایی آبلی مقدماتی هستند، $p+5$ گروه وجود دارد.

فهرست مطالب

فصل ۱
یادآوری قضایای سیلو

در این فصل قضایای سیلو و نکاتی در رابطه با گروه های متناهی را با استفاده از [۲] بیان می‌کنیم.

بر طبق قضیه لاگرانژ داریم که مرتبه هر زیر گروه از گروه متناهی G، قرینه‌ی G را می‌شمارد. (عکس قضیه لاگرانژ برقرار نیست). اما اگر P یک عدد اول باشد و $Pk|G|$ آنگاه ثابت می‌شود که G دارای زیر گروه مرتبه Pk است . این خاصیت گروه‌های متناهی برای اولین بار توسط ریاضیدان نروژی، سیلو در مورد گروه‌های جایگشتی ثابت شد. اما بعدها این قضیه در مورد گروه‌های متناهی مجرد توسط فربینیوسی ثابت شد. سیلو وجود زیرگروه‌های مرتبه Pk را که k بزرگترین عدد صحیح و مثبتی است که Pk مرتبه G را می‌شمارد. در G ثابت کرد، اما قضایای دیگر در مورد تعداد چنین زیر گروه‌ها و مزدوج بودن آن‌ها ثابت شد که به طور کلی از آن‌ها به عنوان قضایای اول، دوم، سوم سیلو نام برده می‌شود. در زیر دو روش اثبات متفاوت برای قضیه اول سیلو آورده شده است.

تعریف ۱.۱. *فرض کنید G یک گروه متناهی است و P یک مقسوم علیه اول G است. می‌توان نوشت $|G| = P^n.m$ که m و n اعداد طبیعی‌اند به طوری که $(P, m) = 1$، در این صورت هر زیر گروه G از قرینه‌ی P^n را یک سیلو $P-$زیر گروه G و یا به طور خلاصه یک $SP-$زیر گروه G و یا $P-$سیلو زیرگروهی G می‌نامند. مجموعه ی تمام سیلو $P-$زیرگروه‌های G را با $\mathrm{Sylp}(G)$ نمایش می دهیم.*

تعریف ۱.۱ را می‌توان اینگونه هم بیان کرد که P یک سیلو $P-$زیر گروه گروه متناهی G

است، هرگاه P یک $P-$گروه بوده و $[G : P]$ نسبت به P اول باشد.
با توجه به این نکته که اگر مرتبه گروه متناهی G عددی زوج باشد، آنگاه G دارای عضو مرتبه ۲ است. در زیر حالت کلی این لم را ثابت می‌کنیم.

لم ۱.۱. *فرض کنید G یک گروه متناهی و P یک مقسوم علیه اول مرتبه G است. در این صورت G دارای عضو مرتبه P است.*

برهان. نشان می‌دهیم تعداد حل های معادله‌ی $x^p = 1$ در G مضربی از P است. قرار می دهیم $|G| = n$. بنابر فرض داریم $P|n$ مجموعه ی x را چنین تعریف می کنیم:

$$X = (a_1, a_2, \ldots, a_p)|a_i \in G, \quad a_1 a_2 \ldots a_p = 1$$

داریم $|X| = n^{(p-1)}$ اگر $(a_1, a_2, \ldots, a_p)$ عضوی از X بوده و تمام مولفه های مساوی و برابر a باشند آنگاه $a^p = 1$ از این رو اگر a غیر همانی باشد و مرتبه‌اش مساوی عدد اول p خواهد بود. رابطه‌ی " $\sim$ " را روی X چنین تعریف می کنیم: گوییم دو $P-$گانه در X هم ارزند، هرگاه یکی جایگشت دوری دیگری باشد. برای مثال $(a_1, a_2, \ldots, a_p) \sim (a_2, a_3, \ldots, a_p, a_1)$ به راحتی می توان ثابت کرد که به یک رابطه‌ی هم ارزی روی X است. همچنین واضح است که کلاس هم ارزی عضو $(a, a, \ldots, a) \in X$ تک عضوی است و اگر $(a_1, a_2, \ldots, a_p) \in X$ دست کم دارای دو مؤلفه نامساوی باشد، آنگاه کلاس هم ارزی آن شامل P عضو است. فرض کنید تعداد کلاس‌های هم ارزی تک عضوی r و تعداد کلاس‌های هم ارزی p عضوی، است. در این صورت باید داشته باشیم $r + ps = n^{(p-1)}$ چون P دست‌کم مساوی ۲ است و $p|n$. پس $p|r$ اما تعداد کلاس‌های هم ارزی تک عضوی دقیقاً همان تعداد حل های معادله $x^p = 1$ در G است و لم ثابت می‌شود. □

۱.۱ گروه خطی عام

$Gl_n(F)$ متشکل از ماتریس‌های وارون پذیر $n \times n$ روی میدان F را در نظر می‌گیریم. در حالتی که F یک میدان متناهی است مرتبه‌ی $Gl_n(F)$ را محاسبه می‌کنیم.

لم ۲.۱ (مرتبه ی گروه خطی عام)**.** *فرض می کنیم F یک میدان متناهی q عضوی باشد. در این صورت داریم:*

$$|Gl_n(F)| = q^{\binom{n}{2}}\Pi_{i=1}^{n}(q^i - 1)$$

یاد آوری فرمول مدار فرض کنید G روی Ω عمل می کند $\omega \in \Omega$. در این صورت داریم $[G: G_w] = |w^G|$ اگر عمل G روی انتقالی باشد، آنگاه برای هر $\omega \in \Omega$ داریم $[G: G_w] = |\Omega|$.

یادآوری فرمول مدار، فرض کنید G روی Ω عمل می‌کند $\omega \in \Omega$. در این صورت داریم $[G: G_w] = |w^G|$ اگر عمل G روی Ω انتقالی باشد، آنگاه برای هر $\omega \in \Omega$ داریم $[G: G_w] = |\Omega|$.

برهان. با استفاده از فرمول مدار این لم را ثابت خواهیم کرد.

فرض کنید V فضای برداری n بعدی روی میدان q عضوی F است. چون هر عضو V دارای نمایش منحصر به فرد $(X_1, X_2, \ldots, X_n)$ به صورت مختصاتی است که $x_i \in F$، پس $|V| = q^n$. می‌دانیم $Gl_n(F)$ گروه تبدیلات خطی وارون پذیر V است و $Gl_n(F)$ روی V به روش معمول عمل می‌کند. اما اگر Ω را مجموعه تمام زیر فضاهای یک بعدی در V فرض کنیم، آنگاه $G = Gl_n(F)$ نیز روی Ω عمل می‌کند. و مجموعه Ω چنین است:

$$\Omega = \{< V > | 0 \neq V \in V\}$$

چون تعداد بردار های ناصفر در V برابر است با $q^n - 1$ پس تعداد عناصر Ω برابر است با $\frac{q^n-1}{q-1}$ اما عمل G روی Ω چنین است: اگر A یک تبدیل خطی وارون پذیر روی V فرض شود و $0 \neq V \in V$ آنگاه:

$$< V >^A = < A(V) >$$

واضح است که $< A(V) > \in \Omega$ و به شرایط عمل برقرار است. اگر $< V >$ و $< u >$ عناصر متمایزی از Ω باشند آنگاه u و v استقلال خطی دارند. از این رو تبدیل خطی در G وجود دارد

که u را به v تبدیل کند و این بدان معناست که گروه G روی Ω انتقالی عمل می کند. اکنون می‌توان از فرمول مدار استفاده کرد. اگر بردار $e1 = (1, 0, 0, \ldots, 0)$ را در V در نظر بگیریم آنگاه پایدارساز عنصر $< e1 >$ از Ω تنها G عبارت است از گروه زیر:

$$G_{<e_1>} = \left\{ \left[\begin{array}{c|ccc} \lambda_1 & \lambda_2 & \ldots & \lambda_n \\ 0 & & & \\ 0 & & A & \\ \vdots & & & \\ 0 & & & \end{array} \right] \mid \lambda_i \in F, \lambda_1 \neq 0, \det A \neq 0 \right\}$$

چون A یک ماتریس وارون پذیر $(n-1) \times (n-1)$ است پس :

$$|G_{<e_1>}| = (q-1)q^{n-1}|GL_{n-1}(q)$$

پس بنا به فرمول مدار داریم:

$$|G| = |\Omega||G_{<e_1>}| = \frac{q^n - 1}{q-1} \times (q-1)q^{n-1}|GL_{n-1}(F)| = q^{n-1}(q^n - 1)|GL_{n-1}(F)|$$

پس فرمول استقرایی زیر به دست می آید:

$$|GL_{n-1}(F)| = q^{n-1}(q^n - 1)|GL_{n-1}(F)|$$

با استفاده از استقرا و اینکه $GL_1(F) = F^x$، لم ثابت می‌شود. □

نتیجه ۱.۱. *گروه $Zp \cong GL_1(F)F$ دارای سیلو $P-$زیرگروه است .*

برهان. بنا بر لم قبل داریم:

$$|Gl_n(F)| = q^{\binom{n}{2}} \Pi_{i=1}^{n}(q^i - 1)$$

چون $q^i - 1$ برای هر $1 \leq i \leq n$ نسبت به P اول است پس سیلو $P-$زیرگروه $Gl_n(F)$ در صورت وجود، از مرتبه $q^{\binom{n}{2}}$ است. اما مجموعه تمام ماتریس های با ۱۱ مثلثی $n \times n$ که روی قطر اصلی شان یک است تشکیل زیرگروهی چونG از $Gl_n(F)$ می‌دهد که $|G| = q^{\binom{n}{2}}$ در نتیجهG یک سیلو $P-$زیر گروه $Gl_n(F)$ است و نتیجه ثابت می‌شود. □

لم ۳.۱. *فرض کنید G یک گروه متناهی است و $P||G|$ عددی اول است . فرض کنید P یک سیلو $P-$زیر گروه G است . در این صورت به ازای هر زیر گروه H از G عنصر $x \in G$ وجود دارد به گونه ای که $H \cap P^x$ یک سیلو $P-$زیر گروه H باشد .*

برهان. برهان : همرده های مضاعف H و P را در G در نظر می‌گیریم. می دانیم که اگر $[G : H]$ متناهی باشد که G گروه H و P زیرگروه های آن هستند ، آنگاه $[G : H] = \Sigma_{x\in X}[PP \cap H^x]$ که X مجموعه کاملی از نماینده‌های همرده‌های مضاعف مجزای H و Pدر G است در حالتی که $[G : k]$ متناهی باشد . به طور مشابه داریم:

$$[G : P] = \Sigma_{x\in X}[H : H \cap P^x] \qquad (۱.۱)$$

چون P یک سیلو $P-$زیر گروه G فرض شده پس $[G : P]$ نسبت به P اول است. بنابراین سمت راست تساوی (۱.۱) نیز باید نسبت به P اول باشد. پس $x \in X$ وجود دارد به گونه ای که $[H : H \cap P^x]$ نسبت به P اول است. اما چون $H \cap P^x$ زیر گروهی از P^x است، پس یک $P-$گروه است، که ثابت می‌شود $H \cap P^x$ یک سیلو $P-$زیر گروه G است. □

اکنون قضیه اول سیلو که درباره وجود سیلو $P-$زیر گروه در هر گروه متناهی است ثابت می‌کنیم.

قضیه ۱.۱ (قضیه اول سیلو)**.** *فرض کنید G یک گروه متناهی است و $p||G|$ یک عدد اول است. در این صورت G دارای سیلو $P-$زیر گروه است.*

برهان. □

با استفاده از برهان خلف ثابت می‌کنیم G دارای سیلو $P-$زیرگروه است. فرض می‌کنیم چنین نباشد و G کوچکترین مثال نقض باشد . یعنی G دارای سیلو $P-$زیر گروه نیست، ولی هر گروه متناهی که مرتبه‌اش از مرتبه‌ی G کوچکتر بوده و مضربی از P باشد دارای سیلو $P-$زیرگروه است .

ادعا می‌کنیم $P||Z(G)|$. فرض می‌کنیم چنین نباشد و $P \nmid |Z(G)|$ معادله کلاس را در نظر می‌گیریم :

$$|G| = |Z(G)| + \Sigma_{x \in z(G)}[G : C_G(x)]$$

که x روی مجموعه‌ای از نماینده‌های کلاس تزویج G تغییر می‌کند که تک عضوی نباشند . چون $P||G|$، از تساوی بالا نتیجه می‌شود که xای وجود دارد به گونه‌ای که $P \nmid [G : C_G(x)], x \notin Z(G)$. اگر فرض کنیم $|G| = P^n.m$ آنگاه از اینکه $(m, p) = 1$ مضرب P نیست و $C_G(x)$ زیرگروه G است نتیجه می‌شود $|C_G(x)| = P^n.m'$ که $(m', P) = 1$. چون $x \notin Z(G)$ پس $C_G(x) \overset{<}{\neq} G$ از این رو نباید فرض $C_G(x)$ دارای سیلو $P-$زیر گروه P است. با توجه به مرتبه‌ی $C_G(x)$ داریم $|P| = P^n|$ که از آن نتیجه می‌شود P یک سیلو $P-$زیر گروه G نیز هست که تناقض با $(P||Z(G)|)$ فرض است. بنابر لم قضیه کشی، گروه $Z(G)$ دارای عضو مرتبه P است. داریم $H \trianglelefteq G$ از این رو G/H گروهی است که مرتبه‌اش کمتر از مرتبه‌ی G و در نتیجه دارای سیلو $P-$زیر گروه P/H از مرتبه P^{n-1} است.

$$\frac{P}{H} \leq \frac{G}{H} \Rightarrow H \trianglelefteq P \leq G$$
$$\left|\frac{P}{H}\right| = P^{n-1} \Rightarrow |P| = |H|P^{n-1} = P^n$$

پس P یک سیلو $P-$زیرگروه G است که باز هم یک تناقض است بدین ترتیب فرض نداشتن سیلو $P-$زیر گروه در G به تناقض می‌رسد و قضیه ثابت می‌شود.

قضیه ۲.۱ (قضیه دوم سیلو)**.** *هر دو سیلو $P-$زیر گروه گروه متناهی G در G مزدوج‌اند. به علاوه هر $P-$زیرگروه G مشمول در یک سیلو $P-$زیر گروه G است.*

برهان. P را یک سیلو $P-$زیر گروه G در نظر می‌گیریم. فرض کنید Q یک $P-$زیرگروه G است. بنابراین لم اخیر عنصر $x \in G$ وجود دارد به گونه‌ای که $Q \cap P^x$ یک سیلو $P-$زیر گروه Q باشد. چون Q خود یک $P-$گروه است پس:

$$Q \cap P^x = Q \Rightarrow Q \leq P^x$$

چون $|P| = |P^x|$، پس P^x یک سیلو $P-$زیرگروه است G است. از این رو ثابت می‌شود که هر $P-$زیر گروه G مشمول در یک سیلو $P-$زیرگروه G است. در حالت خاص اگر Q یک سیلو $P-$زیرگروه G باشد، آنگاه از برابری مرتبه‌های Q و P^x نتیجه می‌شود $Q = P^x$ که ثابت می‌کند هر دو سیلو $P-$زیرگروه G در G مزدوج‌اند . □

نتیجه ۲.۱. *فرض کنید G یک گروه متناهی است و P عددی اول است ، به طوری که $P||G|$. فرض کنیدP یک سیلو $P-$زیر گروه G است. در این صورت $P \trianglelefteq G$ ، اگر و تنها اگر P تنها سیلو $P-$زیر گروه G باشد.*

برهان. فرض کنید $x \in G$ در این صورت p^x نیز یک سیلو $P-$زیرگروه G است. بنا به قضیه دوم سیلو تمام سیلو $P-$زیر گروه‌های G مزدوج‌اند. بنابراین P منحصر به فرد است، اگر و تنها اگر $P^x = P$ که نتیجه می‌دهد $P \trianglelefteq G$ و برعکس. □

قضیه ۳.۱ (قضیه سوم سیلو)**.** *تعداد سیلو $P-$زیر گروه‌های متناهی G مقسوم علیه‌ای از مرتبه G است و تعدادشان همنهشت است با یک به پیمانه‌ی P.*

برهان. فرض کنید P یک سیلو $P-$زیرگروه G است. بنا به قضیه دوم سیلو تمامی سیلو $P-$زیر گروه‌های G مزدوج‌اند. از این رو $Sylp(G) = P^x | x \in G$. می‌دانیم که اگر $H \leq G$ آنگاه تعداد مزدوج‌های H در G برابر است با $|Syl_p(G)| = [G : N_G(H)]$

در نتیجه: $|Syl_p(G)|||G|$ و قسمت اول قضیه اثبات می‌شود. برای اثبات قسمت آخر قضیه فرض می‌کنیم P یک سیلو $P-$زیرگروه G است و قرار می‌دهیم $H = N_G(P)$. با در نظر گرفتن همرده‌های مضاعف G نسبت به H و Pو بنابر لم پیش از این بیان شد می‌توان نوشت:

$$[G : H] = \Sigma_x [P : P \cap H^x]$$

اما $[P : P \cap H^x]$ توانی ازP است و در زیر تعیین می‌کنیم تحت چه شرایطی برابر با یک است:

$$[P : P \cap H^x] = 1 \Leftrightarrow P = P \cap H^x$$
$$\Leftrightarrow P \subseteq H^x \Leftrightarrow P \subseteq x^{-1}Hx \Leftrightarrow xPx^{-1} \subseteq H = N_G(P)$$

اما چون $|xPx^{-1}| = |P|$ و بنابر نتیجه‌ی قبل گروه $N_G(P)$ فقط یک سیلو $P-$زیر گروه دارد که همان P است. نتیجه می‌شود: $xpx^{-1} = p \leftrightarrow x \in N_G(p) = H$ اما اگر $x \in H$، آن‌گاه $Hxp = HP$ و فقط یک همرده‌ی مضاعف به نمایندگی چنین xای داریم. پس فقط یک نماینده‌ی x وجود دارد که $[p : p \cap H^x]$ مساوی ۱ باشد و در سایر موارد این اندیس مضرب p است. درنتیجه: $[G : H] \equiv 1 (mod\, p)$ قضیه ثابت می‌شود. □

قضیه ۴.۱ (قضیه استدلال فراتینی)**.** *فرض کنید G گروه متناهی است و H زیر گروه نرمالی از G است. اگر P یک سیلو $P-$زیرگروه H باشد، آن‌گاه داریم:*

$$G = N_G(P)H$$

برهان. عضو دلخواه $g \in G$ را در نظر می‌گیریم. مرتبه‌ی گروه‌های p^g و p با هم برابرند و چون $p \leq H \trianglelefteq G$، نتیجه می‌شود $p^g \leq H$. پس p^g و p سیلو $P-$زیرگروه‌های Hاند که بنا بر قضیه دوم سیلو باید در H مزدوج باشند:

$$\exists h \in H \ni p = (p^g)^h = p^g h \leftrightarrow gh \in N_G(p)$$
$$\leftrightarrow g \in N_G(p)h^{-1} \leftrightarrow g \in N_G(p)H$$
$$\leftrightarrow G \leq N_G(p)H$$

پس نتیجه می‌شود $G \leq N_G(p)H$ و حکم ثابت می‌شود. □

نتیجه ۳.۱. *نتیجه: فرض کنید G یک گروه متناهی است و p یک سیلو $P-$زیر گروه G است اگر H زیر گروهی از G بوده به‌طوری که شامل $N_G(p)$ باشد آن‌گاه $N_G(H) = H$.*

برهان. چون $p \leq N_G(P) \trianglelefteq H$ پس P یک سیلو $P-$زیرگروه H است. چون $H \trianglelefteq N_G(H)$ پس با استفاده از استدلال فراتینی می‌توان نوشت: $N_G(H) = N_K(p)H$ جایی‌که $K = N_G(H)$. اما داریم:

$$N_K(p) \leq N_G(p) \leq H$$

که از آن نتیجه می‌شود $N_G(H) = N_k(p)H \leq H$ بنابراین $N_G(H) = H$ □

فصل ۲

خود ریختی گروه‌های آبلی

در این فصل قضایای خودریختی و نکاتی در رابطه با گروه های آبلی را با استفاده از [۱] بیان میکنیم.

قضیه ۱.۲ (قضیه دوم یکریختی)**.** *اگر G یک گروه و $H \leq G$ و $K \trianglelefteq G$، آنگاه $H/H\cap K \cong HK/K$.*

برهان. داریم $H \cap K \trianglelefteq H$ و $K \trianglelefteq HK$ نگاشت $f : H \to HK/K$ را چنین تعریف می‌کنیم:

$$f(h) = hk, \forall h \in H$$

چون $H \subseteq HK$ سپس نگاشت فوق خوش تعریف است. به سادگی می‌توان نشان داد که f یک هم‌ریختی است. حال ثابت می‌کنیم که f پوششی است. اگر $x \in HK/K$ آنگاه $X = xKx \in HK$ پس اعضای $h \in H$ و $k \in K$ وجود دارند به‌طوریکه $x = hk$ حال داریم: $f(h) = hk = hkK = xK = X$ یعنی f پوشش است. اکنون هسته f را بدست می‌آوریم. اگر $h = kerf$ آنگاه $hk = k$ بنابراین $h \in K$، که از آن نتیجه می‌شود $h \in H \cap K$. پس $kerf = H \cap K$. طبق خواص یکریختی داریم:

$$H/kerf = Im(f) \to H/H \cap K \cong HK/K$$

□

لم ۱.۲. *اگر $f : G_1 \to G_2$ یک هم‌ریختی و e_2 و e_1 به‌ترتیب اعضای بی‌اثر گروه‌های G_1 و G_2 باشند، آنگاه $H \leq G_1$ آنگاه $f(H) \leq G_2$.*

برهان. چون $f(e_1) = e_(2) \in K$ پس $e_1 \in f^{-1}(K)$. اگر $x, y \in f^{-1}(K)$، آنگاه طبق تعریف $f^{-1}(K)$ اعضای $a, b \in K$ وجود دارند به‌طوری‌که $f(x) = af(y) = b$. بنابراین $f(x^{-1}y) = f(x^{-1})f(y)$ و درنتیجه $a^{-1}b \in Kx^{-1}y \in f^{-1}(K)$

□

لم ۲.۲. *فرض می‌کنیم G یک گروه $G_i, 1 \leq i \leq n$ زیر گروه‌های نرمال G می‌باشند. فرض کنید $n \leq i \leq 1 |G_i| = g_i$ و به ازای $i \neq j$ داریم $(g_i, y_j) = 1$ اگر $|G| = g_1 g_2 g_n$، آنگاه:*

الف) $G \cong G_1 \times G_2 \times \ldots \times G_n$

ب) $Au + G \cong Au + G_1 \times \ldots \times Au + G_n$

برهان. الف) چون هرکدام از G_i ها زیرگروهی نرمال از G است لذا $G_1 G_2 G_{i-1}$ زیر گروهی از G بوده و داریم $|G_1 G_2 \ldots G_{i-1}| = g_1 g_2 \ldots g_{i-1}$، زیرا مرتبه‌های G_i دو به دو نسبت به هم اولند. حال چون g_i و $g_1 g_2 \ldots g_(i-1)$ نیز نسبت به هم اول‌اند. لذا داریم: $G_1 G_2 \ldots G_(i-1) \cap G_i = 12 \leq i \leq n$. همچنین به علت اینکه: $|G_1 G_2 \ldots G_n| = g_1 g_2 \ldots g_n = |G|$ داریم $G = G_1 G_2 \ldots G_n$. در نتیجه G حاصل‌ضرب مستقیم G_i هاست یعنی: $G \cong G_1 \times G_2 \times \ldots \times G_n$.
ب) ابتدا نشان می‌دهیم که G_i تنها زیرگروه مرتبه‌ی g_i در G است. فرض کنید $H \leq G$ و $|H| = g_i$. چون $G_i \trianglelefteq G$ پس $G_i H \leq G$ و بنا بر قضیه دوم یکریختی، می‌توان نوشت:

$$|G_i H / G_i| = |H / G_i \cap H|$$

اما $|G_i H / G_i|$ نسبت به y_i اول است و چون $|H / G_i \cap H||H| = g_i$ بنابراین باید داشته باشیم $|H / G_i \cap H| = 1$ یا اینکه $H = G_i \cap H$ که از آن نتیجه می‌شود $H \subseteq G_i$. چون $|H| =$

$|G_i|$ پس $H = G_i$، یعنی G_i تنها زیرگروه G از مرتبه‌ی g_i است. اکنون اگر $\xi \in Aut$، داریم $\xi(G_i) \leq G$. (طبق لم ۱.۲) که چون ξ دو سویی است پس $|\xi(G_i)| = |G_i| = g_i$ بنا بر آنچه در ابتدا ثابت شد باید داشته باشیم $1 \leq i \leq n \xi(G_i) = G_i$ اگر قرار دهیم: $\xi_i \in Aut(G_i)$. آنگاه: $\xi_i = \xi|_{c_i}\ G_i \to G_i, 1 \leq i \leq n$ بنابراین طبیعی است که نگاشت:

$$f : AutG \to AutG_1 \times \ldots \times AutG_n$$

را به صورت زیر تعریف کنیم

$$f : \xi \to (\xi_1, \ldots, \xi_n), \xi_i = \xi|_{c_i}, \quad 1 \leq i \leq n$$

واضح است کهf یک هم‌ریختی است، اگر $(\alpha_1, , \alpha_n) \in AutG_1 \times \ldots \times AutG_n$ آنگاه برای $\alpha : G \to G$ که‌به صورت $\alpha(g_1, , g_n) = (\alpha_1(g_1), \ldots, \alpha_n(g_n))$ تعریف می‌شود داریم $\alpha \in Aut(G)$ و این ایجاب می‌کند که f پوششی باشد. حال اگر $\xi_i = \xi|_{G_i},\ 1in$ آنگاه $\epsilon \xi ker f$ مانند عضو بی اثر $Aut\ G_i$ عمل می‌کند، یعنی $\xi_i(g_i) = g_i 1 \leq i \leq n$. بنابراین

$$\xi(g_1, \ldots, g_n) = (\xi_1(g_1), \ldots, \xi_n(g_n)) = (g_1, \ldots, g_n)$$

یعنی ξ خوریختی همانی G است و درنتیجه fیک به یک است. به این ترتیب ثابت می‌شود که f یکریختی بوده و

$$Aut(G) \cong Aut(G_1) \times \ldots \times Aut(G_n)$$

□

لم ۳.۲. *اگر G یک گروه دوری مرتبه‌ی mn و $(m, n) = 1$ آنگاه G با حاصل‌ضرب مستقیم دو زیرگروه دوری خود از مرتبه های m و n یکریخت است. یعنی در واقع $Z_m n \cong Z_m \times Z_n$ به‌شرطی که $(m, n) = 1$.*

برهان. می‌دانیم که هر زیرگروه از گروه دوری G و خود نیز دوری و زیرگروهی نرمال است. هم‌چنین می‌دانیم گروه G دارای زیرگروه‌های P و Q به‌ترتیب از مرتبه‌های m و n می‌باشد و

بنابراین

$$Z_m \cong P \trianglelefteq GZ_n \cong Q \trianglelefteq G$$

حال چون $(M,N) = 1$ باید داشته باشیم $P \cap Q = 1$ و از طرف دیگر چون $P \trianglelefteq G$ پس $PQ \leq G$ و چون $|PQ| = |P| \times |Q|/|PQ|$ بنابراین $|PQ| = mn$ که از آن حاصل می‌شود $G = PQ$ در نتیجه داریم $G \cong P \times Q$ یا $Z_m n \cong Z_m \times Z_n$. □

قضیه ۲.۲. *فرض کنید $n \in \mathbb{N}$ و $n = n_1 n_2 \dots n_k$ به‌طوری که n_i ها دو به دو نسبت به هم اول هستند. آن‌گاه*

الف) $\cup(Z_n) \cong \cup(Z_{n_1}) \dots \times \cup(Z_{n_k})$

ب) اگر $p > 2$ عددی اول باشد، آنگاه $\cup(Z_{P^M})$ گروهی دوری با مرتبه‌ی $(p-1)(p^{m-1})$ است و اگر $p = 2$ آنگاه $\cup(Z_{2^M})$ گروهی آبلی از نوع $(2^{m-2}, 2)$ است، $m \geq 3$ همچنین داریم: $|\cup(Z_4)| = 2$ و $|\cup(Z_2)| = 1$

برهان. الف) فرض می‌کنیم $G = \langle x \rangle$ گروهی دوری از مرتبه‌ی n باشد. $(G \cong Z_n)$. قرار می‌دهیم $x_i = x^{k_i} k_i = n|_{n_i}$. اگر گروه دوری $G_i = \langle x_i \rangle$ را در نظر بگیریم داریم: $|G| = n_i$ و همچنین $G_i \cong Z_{n_i}$. چون تمام G_i ها زیر گروه‌های نرمال G هستند و مرتبه‌شان دو به دو نسبت به هم اول است، و داریم $|G| = n = n_1 n_2, \dots, n_k$ پس بنا بر لم ۲.۲ باید داشته باشیم: $G \cong G_1 \times \dots \times G_n$ در نتیجه با توجه به قسمت (ب) لم ۲.۲ می‌توان نوشت: $AutG \cong AutG_1 \times \dots \times AutG_n$ اما با توجه به این نکته که اگر G گروهی دوری از مرتبه n باشد، آنگاه $AutG \cong \cup(Z_u)$ بنابراین

$$\cup(Z_n) \cong \cup(Z_{n_1}) \times \dots \times \cup(Z_{n_k})$$

ب) فرض کنید p عددی اول فردی است و قرار می¬دهیم $G = \cup(Z_{p^m})$. واضح است که $|G| = \xi(p^m) = (p-1)(p^{m-1})$ همچنین روشن است که $\cup(Z_p) = \bar{1}, \bar{2}, \dots, \overline{P-1}$

گروهی دوری از مرتبه$p-1$ می‌باشد. حال نگاشت ξ از G به $\cup(Z_p)$ را چنین تعریف می‌کنیم: برای $\bar{x} \in G$ اگر $x \equiv t(mod\ p)$ آنگاه قرار می‌دهیم $\xi(\bar{x}) = \bar{t}$. این نگاشت خوش تعریف است زیرا اگر $\bar{x} = \bar{y}$ آنگاه $x \equiv y(mod\ P^M)$، و به طریق اولی $x \equiv y(modP)$. پس xو y هر دو دارای باقی‌مانده‌های یکسانی نسبت به p می‌باشند و درنتیجه $\xi(\bar{x}) = \xi(\bar{y})$. روشن است که ξ پوششی است، و اگر $\bar{x} \in ker\xi$، آنگاه باید داشته باشید $x \equiv y(mod\ P)$. پس $kerf = \{\bar{x} \in G | x \equiv 1(mod\ p)\}$.

که اگر قرار دهیم $H = kerf$ آنگاه طبق قضیه‌ی اول یکریختی داریم $G/H \cong \cup(Z_p)$ که چون $|\cup(Z_p)| = P-1$ پس $|H| = P^{m-1}$. ولی در ابتدای اثبات قضیه تذکر دادیم که $\cup(Z_p) \cong Z_{1+p}$، پس $G/H \cong Z_{1+p}$. اکنون نشان می‌دهیم کهH گروهی دوری است. با توجه به ساختمان H می‌دانیم که $(\overline{1+p}) \in H$ و اگر نشان دهیم که مرتبه‌ی $(\overline{1+p})$ برابر P^{m-1} است، از آنجایی‌که $|H| = P^{m-1}$ نتیجه خواهد شد $H = \langle(\overline{1+p})\rangle$. ابتدا با استفاده از روش استقرار روی m ثابت می‌کنیم

$$(1-p)^{P^{m-1}} \equiv 1(mod\ p^m)$$

برای $m = 1$ هم‌نهشتی فوق واضح است. پس فرض می‌کنیم رابطه برای $m = k$ درست باشد و ثابت می‌کنیم برای $m = k+1$ نیز درست است. قرار می‌دهیم

$$(1-p)^{P^{k-1}} \equiv 1 + kp^k$$

چون طرفین تساوی فوق را به توان p برسانیم، خواهیم داشت: $(1-p)^{P^k} \equiv (1+kp^k)^p$. اکنون با استفاده از قضیه‌ی دو جمله‌ای بدست می‌آوریم $(1+kp^k)^p = 1(mod\ p^{k+1})$ به این ترتیب ثابت می‌شود $(1-p)^{P^{m-1}} \equiv 1(modp^m)$، و این بدان معناست که $O(\overline{1+p})|P^{m-1}$. حال با توجه به اینکه P عددی اول است، اگر ثابت کنیم که $(1-p)^{P^{m-2}} \not\equiv 1(mod\ p^m)$ آنگاه نتیجه می‌شود $O(\overline{1+p})|P^{m-1}$.

این بار نیز با استفاده از روش استقرا روی m می‌توان ثابت کرد

$$(1-p)^{P^{m-2}} \equiv 1 + p^{m-1}(mod\ p^m)$$

پس با استفاده از هم‌نهشتی اخیر دیده می‌شود که

$$(1-p)^{P^{m-2}} \equiv 1 + p^{m-1}(modp^m) \not\equiv 1(mod\, p^m)$$

بنابراین $O(\overline{1+p})|P^{m-1}$ ، و درنتیجه $H = \langle\overline{1+p}\rangle$. گروهی دوری است. حال چون $H = (p-1)p^m$ و $(p, p-1) = 1$ پس $H \in Sylp\ (G)$. و چون G گروهی دوری است با استفاده از قضیه اساسی گروه‌های آبلی متناهی می‌توان نوشت

$$G \cong H \oplus G_1 \oplus G_2 \oplus \ldots \oplus G_r$$

که در آن G_iها، $1 \leq i \leq r$ گروه‌های دوری بوده و بستگی به تجزیه عدد $p-1$ به اعداد اول دارند ولی داریم $G/H \cong Z_{1+p}$ و از طرف دیگر با استفاده از مجموع مستقیم فوق $G_1 \oplus G_2 \oplus \ldots \oplus G_r \cong Z_{p-1}$ پس $G/H \cong \oplus G_1 \oplus G_2 \oplus \ldots \oplus G_r$ و درنتیجه $G \cong H \oplus Z_{1+p}$. حال چون H و Z_{1+p} هر دو گروه‌های دوری بوده و مرتبه‌شان نسبت به هم اول است بنابراین می‌توان نوشت:

$$G \cong Z_{P^M}(P-1)$$

به‌این ترتیب اثبات قسمت (ب) قضیه در حالتی که P فرد است کامل می‌شود. حال فرض می‌کنیم $p = 2$. واضح است که در این صورت $|\cup(Z_2)| = 1$ و هم‌چنین $\cup(Z_4) = \bar{1}, \bar{3}$ گروهی از مرتبه ۲ و درنتیجه دوری است. سپس قرار می‌دهیم $m \geq 3$ $G = \cup(Z_{2^m})$. در این حالت نگاشت ξ از G به $\cup(Z_4)$ را چنین تعریف می‌کنیم:

$$\xi(x) = \begin{cases} \bar{1} & \text{اگر } x \equiv 1\ (mod\ 4) \\ \bar{3} & \text{اگر } x \equiv 3\ (mod\ 4) \end{cases}$$

که در آن $\bar{x} = \cup(Z_{2^m})$. روش است که ξ پوششی و خوش تعریف است و هسته‌ی ξ عبارت است از

$$H = ker\ f = \{\bar{x} \in G | x \equiv 1(mod 4)\}$$

بنابراین طبق قضیه‌ی اول یکریختی می‌توان نوشت $G/H \cong \cup(Z_4)$. چون $|\bar{G}| = \xi(2^m) = 2^{m-1}$ پس $|H| = 2^{m-2}$. حال $\bar{5} \in H$ و دوباره با استفاده از روش استقرا روی m می‌توان نشان داد $O(\bar{5}) = 2^{m-2}$. پس $H = \langle \bar{5} \rangle$ گروهی دوری از مرتبه‌ی 2^{m-2} است: حال $\overline{-1} \in G$ و $O(\overline{-1}) = 2$ بنابراین $H = \langle \overline{-1} \rangle$ زیرگروهی از مرتبه ۲ در G است. اگر $\overline{-1} \neq \bar{x} \in H \cap K$ آنگاه چون $|K| = 2$ پس باید داشته باشیم $K \subseteq H$ و اما چون برای تمام $\alpha \in \mathbb{N}$ داریم $5^\alpha \not\equiv 1 (mod\ 2^m)$، پس به یک تناقض می‌رسیم. بنابراین باید داشته باشیم $\{\overline{-1}\} \langle \bar{5} \rangle \cap \langle \overline{-1} \rangle$. اکنون H و K هر دو زیرگروه‌های نرمال G هستند و با مقایسه‌ی مرتبه‌های G و HK نتیجه می‌گیریم $G = HK$ و بنا بر نکته ۱.۲:

نکته ۱.۲. *فرض کنید G یک گروه و H و K زیرگروه‌های آن هستند. اگر داشته باشیم*

الف) $H \trianglelefteq G$ *و* $H \trianglelefteq G$

ب) $H \cap K = 1$

ج) $G = HK$ *آنگاه* $G \cong H \times K$.

داریم $G \cong H \oplus K$ یعنی G از نوع $(2^{m-2}, 2)$ است و به این ترتیب قضیه ثابت می‌شود. □

فصل ۳

یک رده‌بندی ساده گروه‌های متناهی از مرتبه p^2q^2

۱.۳ مقدمه

تمام گروه های متناهی را می توان به یک سری از گروه‌های ساده متناهی تبدیل کرد که به آنها بلوک‌های حاصل از گروه‌های متناهی می‌گویند. تاریخچه گروه های ساده متناهی از سال ۱۸۳۰ به وسیله اواریست گالوییس و جواب معادلات چندجمله‌ای درجه پنج سرچشمه می‌گیرد. در قرن بیستم، شناخت اهمیت گروه‌های ساده متناهی الهام گرفته از تلاشی بزرگ برای یافتن تمام گروه‌های ساده متناهی است، مقاله [۱۱] را برای جزییات بیشتر مشاهده کنید. اما رده‌بندی گروه‌های متناهی هنوز هم مسئله‌ای باز و حل نشده است. در این مقاله، تمام گروه‌های مرتبه p^2q^2 را به وسیله یک روش ساده با استفاده از مفهوم [۳] تعیین می‌کنیم.

مقدمات و نمادگذاری

در این بخش، ابتدا برخی از مفاهیم، نمادگذاری‌ها و نتایج مربوط به نظریه گروه را یادآوری می‌کنیم که در بخش بعدی مورد استفاده قرار می‌گیرند. از اصطلاحات و نمادگذاری‌های نظریه گروه اساسی استاندارد استفاده می‌کنیم، [۴، ۶، ۷، ۹، ۱۲، ۱۳] و همچنین [۸، ۱۰] را مشاهده کنید. مجموعه

تمام p زیرگروه‌های سیلوی G را با $Syl_p(G)$ نمایش می‌دهیم. یک ضرب نیمه مستقیم، تعمیمی از یک ضرب مستقیم است. فرض کنید Nیک زیرگروه نرمال G باشد، در این صورت هر عنصر $g \in G$ معرف یک خودریختی $N, n \longrightarrow gng^{-1}$ است و همریختی زیر را تعریف می‌کند

$$\theta : G \longrightarrow Aut(N),\ g \longrightarrow i_g|N$$

اگر یک زیرگروهQ از G موجود باشد به طوری که $G \longrightarrow G/N$، Q را به طور همریخت به G/N بنگارد، آنگاه می‌توانیم G را از طریق N, Q و محدودیت θ برای Q بازسازی کنیم. در واقع، یک عنصر $g \in G$ را می‌توان به طور یکتا به فرم زیر نوشت

$$g = nq, \quad n \in N \quad q \in Q$$

Q می بایست عنصری منحصربفرد از Q نگاشته شده به $gN \in G/N$ باشد و n نیز باید برابر با gq^{-1} باشد. از این رو، ما دارای یک تناظر یک به یک از مجموعه‌های زیر هستیم

$$G \leftrightarrow N \times Q$$

اگر $g = nq$ و $g' = n'q'$، آنگاه

$$gg' = (nq)(n'q') = n(qn'q^{-1})qq' = n\theta(q)(n').qq'$$

به طور معادل، G یک ضرب نیمه مستقیم از زیرگروه‌های N و Q است، هرگاه

$$N \trianglelefteq G,\ NQ = G,\ N \cap Q = \{1\}$$

توجه داشته باشید که Q نیازی ندارد تا یک زیرگروه نرمال G باشد. هنگامی که G ضرب نیمه داخلی زیرگروه‌های Nو Q است، می‌نویسیم: $G = N \rtimes Q$ یا $N \rtimes_\varphi Q$.

قضیه ۱.۳. *فرض کنید P یک p گروه، Q یک q گروه و $\psi, \varphi \to Aut(P)$ دو همریختی باشند. در این صورت، $Q \ltimes_\varphi P \cong Q \ltimes_\psi P$ اگر و تنها اگر $\gamma \in Aut(Q)$ و φ برای برخی از $\psi \circ \gamma$ در $Aut(P)$ نرمال باشند.*

لم ۱.۳. *تا یک تک ریختی، یک تناظر یک به یک بین گروه‌های* $G = Q \ltimes_\varphi P$ *و اعداد مدارهای فعال* $Aut(P) \times Aut(Q)$ *روی مجموعه* $Hom(Q, Aut(P))$ *وجود دارد که در آن برای هر* $\alpha \in Aut(P), \beta \in Aut(Q)$ *و* $y \in Q$ *داریم:*

$$\varphi^{(\alpha,\beta)}(y) = \alpha \circ [\varphi \circ \beta^{-1}(y)] \circ \alpha^{-1}$$

فرض کنید $Q = \langle y \rangle$ *یک* p *گروه دوری است.* $Q_y = \langle \varphi(y) \rangle$ *برای هر همریختی بدیهی:* $\varphi : Q \to Aut(P)$*، یک زیرگروه* $Aut(P)$ *از مرتبه* $|Q|$ *است. از سوی دیگر، تمام خودریختی‌های* Qy *را به* y^j *برای برخی از* j*ها می‌نگارانند و از این رو* $Q_{y^j} = (Q_y)^j = Q_y$*. در نتیجه، ما می‌توانیم نتیجه زیر را استنتاج کنیم.*

لم ۲.۳. *فرض کنید* Q *یک گروه دوری باشد، در این صورت تا یک تکریختی، تمام گروه‌های به فرم* $G = Q \ltimes P$ *متناظر با رده های تزویج زیرگروه‌های* $Aut(P)$ *از مرتبه تقسیم* $|Q|$ *هستند.*

گروه خطی کلی مرتبه n، مجموعه‌ای از ماتریس‌های غیرمنفرد $n \times n$ همراه با ضرب معمولی ماتریس‌ها به عنوان عملیات دودویی آن است. به دلیل اینکه ضرب دو ماتریس نامنفرد، مجددا نامنفرد است و معکوس یک ماتریس نامنفرد نیز ماتریسی نامنفرد است، در نتیجه آن یک گروه را می‌دهد. در حالت کلی، گروه خطی کلی درجه n روی هر میدان F، مجموعه‌ای از ماتریس های نامنفرد با درایه‌هایی از F است که توسط $GL_n(F)$ یا $GL(n, F)$ مشخص می‌شود.

یک میدان F که شامل تعدادی متناهی عنصر است را میدان گالویس می‌نامیم. یک میدان متناهی از مرتبه q موجود است اگر و تنها اگر q یک توان اولیه p^k باشد که در آن p یک عدد اولیه و k یک عدد صحیح مثبت است. تمام میدان‌های یک مرتبه داده شده خودریخت هستند. با این مفهوم، اگر F یک میدان متناهی با $q = p^n$ عنصر باشد، آنگاه گروه خطی کلی مرتبه n روی میدان F توسط $GL(n, q)$ مشخص می‌شود.

قضیه ۲.۳. *رده‌های تزویج* $GL(2, p)$ *برابر با مقادیر گزارش شده در جدول ۱.۳ هستند. در این جدول* ρ, σ *به ترتیب عناصر اولیه* $GF(p)$ *و* $GF(p^2)$ *هستند.*

جدول ۱.۳: رده‌های تزویج گروه $GL(2,p)$

Canjugacy classes	Number of such classes	No. Elements
$\begin{pmatrix} \rho^a & 0 \\ 0 & \rho^a \end{pmatrix}$	$(p-1)$	1
$\begin{pmatrix} \rho^a & 1 \\ 0 & \rho^a \end{pmatrix}$	$(p-1)$	$(p-1)(p+1)$
$\begin{pmatrix} \rho^a & 0 \\ 0 & \rho^b \end{pmatrix}$	$\frac{1}{2}(p-1)(p-2)$	$p(p+1)$
$\begin{pmatrix} \sigma^a & 0 \\ 0 & \sigma^{ap} \end{pmatrix}$	$\frac{1}{2}(p-1)$	$p(p-1)$

۲.۳ نتایج اصلی

در این بخش، نتایج قضایای سیلو، حالاتی هستند که در آن اندازه G به منظور دارا بودن یک زیرگروه نرمال غیربدیهی اجرا می‌شود.

قضیه ۳.۳. *فرض کنید G یک گروه از مرتبه p^2q^2 باشد. اگر $pq \neq 6$، آنگاه G با یکی از گروه‌های زیر خودریخت است.*

1. C_{36},
2. $C_{18} \times C_2$,
3. $C_6 \times C_6$,
4. $C_{12} \times C_3$,
5. $D_6 \times C_6 \cong S_3 \times C_6 \cong D_{12} \times C_3$,
6. $D_6 \times D_6 \cong S_3 \times S_3$,
7. $D_{18} \times C2$,

8. $A_4 \times C_3$,

9. D_{36},

10. $H \times C_3$,

11. $K \times C_2$,

12. $\langle a, b, c | a^3 = b^3 = c^4 = [a, b] = 1, c^{-1}ac = b, c^{-1}bc = a^{-1} \rangle$,

13. $\langle a, b, c | a^2 = b^2 = c^9 = [a, b] = 1, c^{-1}ac = b, c^{-1}bc = a^b \rangle$,

14. $\langle a, b, c | a^3 = b^3 = c^4 = [a, b] = 1, c^{-1}ac = a^{-1}, c^{-1}bc = b^{-1} \rangle$,

که در آن

$$H = \langle x, y | x^4 = y^3 = 1, x^{-1}yx = y^{-1} \rangle$$

و

$$K = \langle a, b, c | a^2 = b^2 = c^2 = (abc)^2 = (a, b)^3 = (ac)^3 = 1 \rangle.$$

اگر $pq \neq 6$ ، آنگاه G دارای ساختارهای زیر است:

$$C_{q^2} \ltimes C_{p^2}, C_{q^2} \ltimes (C_p \times C_p), (C_q \times C_q) \ltimes C_{p^2}, (C_q \times C_q) \ltimes (C_p \times C_p).$$

برهان. اگر $pq = 6$،آنگاه اثبات واضح است. فرض کنید $pq \neq 6$ ،

از آنجایی که طبق قضیه سیلو، $p > q$ می‌باشد، واضح است کهp زیرگروه سیلویG نرمال است. فرض می‌کنیم که $P \in Syl_p(G)$ و $Q \in Syl_q(G)$ باشند. این ایجاب می کند که $Q \cap P = \langle 1 \rangle, P \lhd G, G = PQ$. از این رو، G همراه با ضرب نیمه مستقیم $Q \ltimes_\varphi P$ خودریختی است که در آن $\varphi : Q \longrightarrow Aut(P)$ یک همریختی است. به دلیل اینکه هر گروه از مرتبه p^2 گروهی آبلی است، در این صورت

$$Syl_p(G) = \{C_{p^2}, C_p \times C_p\} \; and \; Syl_q(G) = \{C_{q^2}, C_q \times C_q\}$$

گروه Gهمراه با یکی از نمایش‌های زیر با استفاده از لم ۱.۳ و قضیه ۱.۳، خودریختی است:

$$C_{q^2} \ltimes_{\varphi} C_{p^2} \ltimes_{\varphi} C_{p^2}, C_{q^2} \ltimes_{\varphi} (C_p \times C_p), (C_q \times C_q) \ltimes_{\varphi} (C_p \times C_p).$$

در ادامه، ما نمایش تمام این گروه‌ها را تعیین می‌کنیم. به این منظور، می‌توانیم حالات زیر را در نظر بگیریم:

۱. $G \cong C_{q^2} \ltimes_{\varphi} C_{p^2}$، آنگاه $Aut(C_{p^2}) \cong C_{p(p-1)}$ و همریختی $\varphi : C_{q^2} \hookrightarrow C_{p(p-1)}$ را در نظر بگیرید. اگر $Im\varphi \cong \langle 1 \rangle$، آنگاه $G \cong C_{q^2} \times C_{p^2}$. اگر $Im\varphi \cong C_q$ و $q|(p-1)|$، به دلیل $Aut(P)$ اینکه دوری است آن‌گاه بر اساس لم ۲.۳، تنها یک گروه با نمایش زیر وجود دارد:

$$\begin{aligned} G &\cong \langle a, b | a^{q^2} = b^{p^2} = 1, a^{-1}ba = b^r, r^q \equiv 1 mod\, p^2 \rangle \\ &= \langle a, b | a^{q^2} = b^{p^2} = 1, a^{-1}ba = b^r, r = r_0^{\frac{(p-1)p}{q}} \rangle \end{aligned}$$

که در آن r_0، p^2 امین ریشه اتحاد است. اگر $m\varphi \cong C_{q^2}$ و $q^2|(p-1)$، به دلیل اینکه $Aut(P)$ دوری است، آن‌گاه تنها یک گروه با نمایش زیر به وسیله لم ۲.۳ وجود دارد:

$$\begin{aligned} G &\cong \langle a, b | a^{q^2} = b^{p^2} = 1, a^{-1}ba = b^r, r^{q^2} \equiv 1 mod\, p^2 \rangle \\ &= \langle a, b | a^{q^2} = b^{p^2} = 1, a^{-1}ba = b^r, r = r_0^{\frac{(p-1)p}{q^2}} \rangle \end{aligned}$$

که در آن r_0 ، p^2امین ریشه اتحاد است.

۲. $C \cong (C_q \times C_q) \ltimes_{\varphi} C_{p^2}$ و فرض کنید که تصویر φ بدیهی نیست که در آن $\varphi : C_q \times C_q \hookrightarrow Aut(C_{p^2})$ می‌باشد. اگر $Im\varphi \cong \langle 1 \rangle$، آن‌گاه $G \cong C_q \times C_q \times C_{p^2}$. روابط $Im\varphi \cong C_q$ و $q|(p-1)$ را در نظر بگیرید. چون $Aut(P)$ دوری است، آن‌گاه تنها یک گروه با نمایش زیر با استفاده از لم ۱.۳ وجود دارد:

$$G \cong \langle a, b, c | a^q = b^q = c^{p^2} = 1, [a, b] = [b, c] = 1, a^{-1}ca = c^r \rangle$$

که در آن r_0 برابر با p^2امین ریشه اتحاد است و $r^q \equiv 1 (mod\, p^2)$ می‌باشد.

۳. $G \cong C_{q^2} \ltimes_{\varphi} (C_p \times C_p)$ و از این رو $Aut(C_p \times C_p) \cong GL(2,p)$. اگر $Im\varphi \cong \langle 1 \rangle$ ، آنگاه $G \cong C_{q^2} \times (C_p \times C_p)$ و در نتیجه G آبلی است. اگر $Im\varphi \cong C_q$ ، آنگاه برای همریختی داده شده $\varphi : C_{q^2} \to GL(2,p)$، یا C_q یا C_{q^2} را داریم. فرض کنید زیرگروه‌های مرتبه q در اولین رده در جدول ۱.۳ هستند. از این رو، $q|p-1$ و α یک ریشه اولیه اتحاد است و در نتیجه

$$Im\varphi \cong C_q \cong \langle \begin{pmatrix} \beta & 0 \\ 0 & \beta \end{pmatrix} | \beta = \alpha^{\frac{p-1}{q}} \rangle$$

این ایجاب می‌کند که

$$G \cong \langle a, b, c | a^{q^2} = b^p = c^p = 1, a^{-1}ba = b^{\beta}, a^{-1}ca = c^{\beta}, bc = cb \rangle$$

فرض کنید زیرگروه‌های مرتبه q در دومین رده از جدول ۱.۳ باشند. واضح است که در این حالت، نمی‌توان یک نمایش جدید برای G یافت. فرض کنید زیرگروه‌های مرتبه q در سومین رده باشند. اگر $q = 2$، آنگاه

$$Im\varphi \cong C_q \cong \langle \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \rangle$$

و از این رو

$$G \cong \langle a, b, c | a^{q^2} = b^p = c^p = 1, ab = ba, a^{-1}ca = c^{-1}, bc = cb \rangle$$

$q|(p-1)$ و $q \neq 2$ را در نظر بگیرید، در این صورت α برابر با pامین ریشه اتحاد است و $\beta = \alpha^{\frac{p-1}{q}}$. تمام جواب های معادله $x^q \equiv 1$ (مد p) برابر هستند با

$$x_1 = 1, x_2 = \beta, x_3 = \beta^2, \ldots, x_q = \beta^{q-1}$$

این بدان معناست که $\frac{q+1}{2}$ گروه‌های دوری غیرمزدوج از مرتبه q به صورت زیر وجود دارند:

$$\langle \begin{pmatrix} 1 & 0 \\ 0 & \beta \end{pmatrix} \rangle, \langle \begin{pmatrix} \beta & 0 \\ 0 & \beta^i \end{pmatrix} \rangle$$

که در آن $i = 2, 3, \ldots, \frac{q-1}{2}$ و $q-1$. از این رو، در این حالت، می‌توان تایید کرد که

$$G \cong \langle a, b, c | a^{q^2} = b^p = c^p = 1, ab = ba, a^{-1}ca = c^\beta, bc = cb \rangle,$$
$$G \cong \langle a, b, c | a^{q^2} = b^p = c^p = 1, a^{-1}ba = b^\beta, a^{-1}ca = c^\beta, bc = cb \rangle.$$

در نهایت، فرض کنید زیرگروه‌های مرتبه q در چهارمین ریشه در جدول ۱.۳ باشند. برای $q = 2$، هیچ گروهی از مرتبه دو وجود ندارد. اگر $q \neq 2$ و $q|p-1$ ، آنگاه یک زیرگروه از مرتبه q وجود ندارد، اما اگر q به $p+1$ تقسیم شود، آنگاه می‌توانیم یک زیرگروه از مرتبه q به صورت زیر ایجاد کنیم:

فرض کنید σ یک ریشه اولیه‌ی $GF(p)$ باشد و $\alpha_0 = \sigma^{\frac{p^2-1}{q}}$، در این صورت

$$\alpha_0 = \sigma^{\frac{p^2-1}{q}} = \alpha + \beta\sqrt{D} : \alpha, \beta, D \in GF(p), \beta \neq 0, D$$

مربعی نیست و از این رو

$$\begin{pmatrix} \alpha_0 & 0 \\ 0 & \alpha_0^p \end{pmatrix} \in \left[\begin{pmatrix} \alpha & \beta D \\ \beta & \alpha \end{pmatrix} \right]$$

که در آن $[g]$ برای یک عنصر $g \in G$ به معنای رده مزدوجی g در G است. این بدان معناست که

$$G \cong \langle a, b, c | a^{q^2} = b^p = c^p = 1, a^{-1}ba = b^\beta c^{\beta D}, a^{-1}ca = b^\beta c^\alpha, bc = cb \rangle$$

فرض کنید $Im\varphi \cong C_{q^2}$ باشد، در این صورت، تمام زیرگروه‌های دوری غیرمزدوج مرتبه در $GL(2,p)$ به صورت زیر هستند:

a) زیرگروه‌های دوری مرتبه q^2 در اولین ریشه از جدول ۱.۳ هستند. علاوه بر این، q^2 بر $p-1$ تقسیم می‌شود و α یک ریشهp اولیه از اتحاد در F_p است، بنابراین

$$Im\varphi \cong C_{q^2} \cong \langle \begin{pmatrix} \beta & 0 \\ 0 & \beta \end{pmatrix} \rangle, \quad \beta = \alpha^{\frac{p-1}{q^2}}$$

از این رو

$$G \cong \langle a, b, c | a^{q^2} = b^p = c^p = 1, a^{-1}ba = b^\beta, a^{-1}ca = c^\beta, bc = cb \rangle$$

b) زیر گروه‌های دوری مرتبه q^2 در دومین ریشه هستند. در این حالت، یک زیرگروه دوری از مرتبه q^2 وجود ندارد.

c) زیر گروه‌های دوری مرتبه q^2 در سومین ریشه هستند. اگر q^2 بر $p-1$ تقسیم شود، آنگاه معادله $x^{q^2} \equiv 1$ (مد p) دقیقا دارای q^2 ریشه است. در میان آن ها، $q(q-1)$ زیرگروه از مرتبه q^2 هستند و از این رو $\frac{q^2+q}{2}$ زیرگروه غیرمزدوج از مرتبه q^2 به صورت زیر وجود دارند:
فرض کنید α یک ریشه p اولیه‌ی اتحاد باشد، در این صورت

$$\beta = \alpha^{\frac{p-1}{q^2}} \; and \; C^i_{q^2} = \langle \begin{pmatrix} \beta & 0 \\ 0 & \beta^i \end{pmatrix} \rangle$$

که در آن $2 \leq i \leq (q^2-1)/2$ یا $i = kg(k \geq (q+1)/2$ یا $i = q^2 - 1$. بنابراین، $(q^2+q)/2$ گروه با نمایش زیر وجود دارند:

$$G_i \cong \langle a, b, c | a^{q^2} = b^p = c^p = 1, a^{-1}ba = b^\beta, a^{-1}ca = c^{\beta^i}, bc = cb \rangle$$

d) زیرگروه‌های دوری مرتبه q^2 در چهارمین ریشه هستند. اگر $q = 2$، آنگاه دو حالت زیر برقرار است:

i. $p = 4k+1$ و از این رو $(p^2-1)/q^2 = 2k(2k+1)$. در نتیجه، یک گروه دوری از مرتبه q^2 وجود ندارد.

ii. $p = 4k+3$ و در نتیجه $p^2 - 1 = 8(k+1)(2k+1)$. این منجر به تایید این می‌شود که $(p^2-1)q^2 = 2(k+1)(2k+1)$ می‌باشد.
در این حالت، می‌توانیم یک زیرگروه دوری به صورت زیر ایجاد کنیم:
فرض کنید σ یک مولد از گروه ضربی $GF(p^2)$ باشد، در این صورت $\sigma^{\frac{p^2-1}{4}} = \alpha + \beta\sqrt{D} : \alpha, \beta, D \in GF(p), \beta \neq 0, D$ مربعی نیست، و از این رو

$$G \cong \langle a, b, c | a^4 = b^p = c^p = 1, a^{-1}ba = b^\alpha c^{\beta D}, a^{-1}ca = b^\beta c^\alpha, bc = cb \rangle$$

$q \neq 2$ و $q^2|p+1$ یا $q^2|p-1$ را در نظر بگیرید. اگر $q^2|p-1$ ، آنگاه $q|p-1$ و از این رو، نمی‌توانیم یک نمایش جدید را ایجاد کنیم. $q^2|p+1$ را در نظر بگیرید و فرض کنید σ یک زیرگروه ضربی از $GF(p^2)$ باشد. در این صورت

$$G \cong \langle a, b, c | a^{q^2} = b^p = c^p = 1, a^{-1}ba = b^{\alpha}c^{\beta D}, a^{-1}ca = b^{\beta}c^{\alpha}, bc = cb \rangle$$

۴. $G \cong (C_q \times C_q) \ltimes_{\varphi} (C_p \times C_p)$، ابتدا توجه داشته باشید که $Aut(C_p \times C_p) \cong GL(2,p)$. ما درباره تمام خودریختی‌های علاقه‌مند به فرم $\varphi : (C_a \times C_a) \hookrightarrow$ هستیم. اگر $Im\varphi \cong \langle 1 \rangle$، آنگاه $G \cong C_q \times C_q \times C_p \times C_p$ یک گروه آبلی از مرتبه p^2q^2 است. اگر $Im\varphi \cong C_q$، آنگاه تمام زیرگروه‌های غیرمزدوج مرتبه q در $GL(2,p)$ به صورت زیر هستند:

a. زیرگروه‌های متعلق به اولین ریشه در جدول ۱.۳ اگر $q|(p-1)$ و α یک ریشه p اولیه‌ی اتحاد باشد، آنگاه

$$Im\varphi \cong C_q \cong \langle \begin{pmatrix} \beta & 0 \\ 0 & \beta \end{pmatrix} \rangle, \quad \beta = \alpha^{\frac{p-1}{q}}$$

و از این رو

$$G \cong \langle a, b, c, d | a^q = b^q = c^p = d^p = 1, b^{-1}cb = c^{\beta}b^{-1}db = d^{\beta} \rangle$$

که در آن $[a,c] = [a,d] = [a,b] = [c,d] = 1$

b. زیرگروه‌های متعلق به دومین ریشه در جدول ۱.۳ در این حالت، هیچ عنصری از مرتبه q وجود ندارد.

c. زیرگروه‌های متعلق به سومین ریشه در جدول ۱.۳ اگر $q = 2$، آنگاه

$$Im\varphi \cong C_q \cong \langle \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \rangle$$

و از این رو

$$G \cong \langle a,b,c,d | a^q = b^q = c^p = d^p = 1, b^{-1}cb = c^{-1}db = d^\beta \rangle$$

که در آن $[a,b] = [a,c] = [a,d] = [b,d] = [c,d] = 1$. اگر $q \neq 2, q|(p-1)$، آنگاه α یک ریشه اتحاد است و $\beta = \alpha^{\frac{p-1}{q}}$. بنابراین، تمام ریشه‌های معادله $x^q \equiv 1$ (مد p) برابر هستند با

$$x_1 = 1, x_2 = \beta, x_3 = \beta^2, \ldots, x_q = \beta^{q-1}$$

از این رو، $(q+1)/2$ زیرگروه دوری غیر مزدوج زیر وجود دارند

$$\langle \begin{pmatrix} 1 & 0 \\ 0 & \alpha \end{pmatrix} \rangle, \langle \begin{pmatrix} \beta & 0 \\ 0 & \beta^i \end{pmatrix} \rangle$$

که در آن $i = 1, 2, 3, 4, \ldots, \frac{q-1}{2}$ یا $i = q-1$. مشابه با بحث قبلی ما، دو نمایش را برای G اختیار می‌کنیم که جدید نیستند.

d. زیرگروه مرتبه q متعلق به چهارمین ریشه در جدول ۱.۳ مشاهده چنین موضوعی دشوار نیست که اگر در این حالت $q \neq 2$، $p-1 \neq kq$ و $q|p+1$ باشند، آنگاه یک گروه از مرتبه q وجود دارد. فرض کنید σ یک ریشه از اتحاد در $GF(p^2)$ باشد و $\alpha_0 = \sigma^{\frac{p^2}{q}} = \alpha + \beta\sqrt{D} : \alpha, \beta, D \in GF(p), \beta \neq 0, D$ مربعی نیست در این صورت

$$\begin{pmatrix} \alpha_0 & 0 \\ 0 & \alpha_0^p \end{pmatrix} \in \left[\begin{pmatrix} \alpha & \beta D \\ \beta & \alpha \end{pmatrix} \right]$$

و از این رو

$$G \cong \langle a,b,c,d | a^q = b^q = c^p = d^p = 1, b^{-1}cb = c^\alpha d^{\beta D}, b^{-1}db = c^\beta d^\alpha \rangle$$

که در آن $[a,b] = [a,c] = [a,d] = [c,d] = 1$. در نهایت، $Im\varphi \cong C_q \times C_q$ را در نظر بگیرید. فرض کنید α، pامین ریشه اولیه‌ی اتحاد باشد، و همچنین $\beta = \alpha^{\frac{p-1}{q}}$

و $q|p-1$ را هم داشته باشیم. در این صورت

$$C_q \times C_q \cong \langle \begin{pmatrix} \beta & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & \beta \end{pmatrix} \rangle$$

و در نتیجه

$$G \cong \langle a, b, c, d | a^q = b^q = c^p = d^p = 1, a^{-1}ca = c^\beta, b^{-1}db = d^\beta \rangle$$

که در آن $[a, b] = [b, c] = [c, d] = [a, d] = 1$ که این اثبات را کامل می‌کند.

□

مراجع

[۱] دکتر محمدرضا درفشه، مقدمه‌ای بر نظریه گروه‌ها، چاپ سوم، انتشارات دانشگاه تهران

[۲] دکتر محمدرضا درفشه، جبر، جلد اول، گروه، چاپ اول، انتشارات دانشگاه تهران

[3] W. Burnside, Theory of Groups of Finite Order, 2d ed. *Dover Publications*, Inc., New York, 1955.

[4] D. S. Dummit, R. M. Foote, Abstract Algebra, Third Edition, *John Wiley & Sons*, Inc., Hoboken, NJ, 2004.

[5] M. Hall, On the number of Sylow subgroups in a finite group, *J. Algebra 7* (1967) 363–371.

[6] B. Huppert, Endliche Gruppen I:, *Springer-Verlag*, Berlin, 1967.

[7] C. Leedham-Green, S. McKay, The Structure of Groups of Prime Power Order, London Mathematical Society Monographs. New Series, 27. Oxford Science Publications. *Oxford University Press*, Oxford, 2002.

[8] L. Pyber, Enumerating finite groups of given order, *Ann. of Math.* 137 (1993) 203–220.

[9] D. J. S. Robinson, A Course in the Theory of Groups, *Springer-Verlag*, New York, 1982.

[10] J. J. Rotman, An Introduction to the Theory of Groups, Fourth edition, Graduate Texts in Mathematics, 148, *Springer-Verlag*, New York, 1995.

[11] R. Solomon, A brief history of the classification of the finite simple groups, *Bull. Amer. Math. Soc. (N.S.)*, 38, (2001), 315–352.

[12] M. Suzuki, Group Theory I:, *Springer-Verlag*, Berlin-New York, 1982.

[13] M. Suzuki, Group Theory II:, *Springer-Verlag*, Berlin-New York, 1986.

واژه‌نامه

آبلی ..... Abelian
تبدیلات خطی ..... Linear transformation
خطی ..... Linear
خودریختی ..... Automorphism
دوری ..... Cyclic
رده‌بندی ..... Classification
ریشه ..... Root
زیرگروه خطی نرمال ..... Normal Linear Subgroup
زیرفضا ..... Sub Space
کلاس هم‌ارزی ..... Equivalence class
گروه ..... Group
مرتبه ..... Order
متناهی ..... Finite
مزدوج ..... Conjugate
میدان متناهی ..... Finite Group
ماتریس بالا مثلثی ..... Upper Triangle Matrix
وارونپذیر ..... Invertible
همرده مضاعف ..... Extra Coset

همریختی Homomorphism

همنهشتی Syntactic

یکریختی Isomorphism

Abstract

Assume that G is a group while its order is p^2q^2while p and q are prime numbers that $p > q$. Assume that P and Q are p-Sylow subgroup and q-Sylow subgroup of G, respectively. In this paper, we'll show that there are four groups with p^2q^2 order according to homomorphic estimation, while P and Q are cyclic groups. While Q is cyclic group and P is a primary abelian group, there are three groups, according to mentioned property, when Q is a primary abelian group and P is cyclic group, there are $\frac{p^2+3p}{2+7}$ groups and Finally, when both P and Q are primary abelian groups, there are $p + 5$ groups.

College of Science
School of Mathematics, Statistics, and Computer Science

A Simple Classification of Finite Groups of Order p^2q^2

Ensiyeh mirzaei

Supervisor: Mohammadreza derafsheh

A thesis submitted to Graduate Studies Office
in partial fulfillment of the requirements for the degree of
B.Sc.
Pure Mathematics