فرهنگ و اندیشهٔ ریاضی
سال ۳۶، شمارهٔ ۶۱ (پاییز و زمستان ۱۳۹۶) صص. ۱۲۵ تا ۱۳۰

برهانی جدید برای قضیه‌ای کلاسیک در نظریهٔ گروه‌های متناهی

الهه‌سادات حقی و سید علی‌رضا اشرفی

چکیده

قضیه‌ای کلاسیک در نظریهٔ گروه‌ها می‌گوید اگر G یک ۲-گروه متناهی باشد که تنها یک عضو مرتبهٔ ۲ دارد، آن‌گاه G دوری است یا با یک ۲-گروه کواترنیون تعمیم‌یافته یکریخت است. هدف این نوشته، ارائهٔ برهانی جدید برای این قضیه است.

۱. سرآغاز

در سراسر این مقاله منظور از گروه، گروهی متناهی است. گیریم p یک عدد اول باشد. منظور از p-گروه، گروهی متناهی است که مرتبهٔ آن (یعنی تعداد عضوهای آن) توانی از p باشد. یک $p-$گروه آبلی مقدماتی گروهی آبلی است که مرتبهٔ هر عضو غیرهمانی آن p است. به‌ازای هر گروه متناهی G، اشتراک تمام زیرگروه‌های ماکسیمال G را با $\Phi(G)$ نشان می‌دهیم و آن را *زیرگروه فراتینی*[۱] G می‌نامیم. قضیه‌ای معروف از برنساید می‌گوید اگر G یک $p-$گروه باشد، آن‌گاه $G/\Phi(G)$ یک گروه آبلی مقدماتی است و اگر $|G/\Phi(G)| = p^r$، آن‌گاه کمترین تعداد عضوهای یک مجموعهٔ مولد برای گروه G برابر با r است ([۱]، قضیهٔ ۱۲.۲.۱). یکی از ویژگی‌های زیرگروه فراتینی این است که اگر G متناهی باشد، $C \subseteq G$ و $D \subseteq \Phi(G)$، آن‌گاه $G = \langle C, D\rangle$ ایجاب می‌کند که $G = \langle C\rangle$.

یادآوری می‌کنیم که ۲-گروه کواترنیون تعمیم‌یافته Q_{2^n}، $n \geq 3$، با مولدها و رابطه‌های زیر تعریف می‌شود:

$$Q_{2^n} = \langle a, b \,|\, a^{2^{n-1}} = 1, a^{2^{n-2}} = b^2, bab^{-1} = a^{-1}\rangle.$$

عبارات و کلمات کلیدی. گروه دوری؛ گروه کواترنیون تعمیم‌یافته؛ قضیهٔ برنساید؛ عضو مرتبهٔ ۲.

[۱] Frattini subgroup

می‌توان ثابت کرد که هر عضو این گروه به یکی از دو شکل a^i یا ba^i است که در آن، $1 \leq i \leq 2^{n-1}$. هدفِ این مقاله اثبات قضیهٔ زیر است:

قضیه ۱.۱. *فرض کنیم G یک ۲–گروه باشد که عضو مرتبهٔ ۲ در آن یکتا است. در این صورت G دوری است یا با ۲–گروه کواترنیون تعمیم‌یافته یکریخت است.*

۲. برهان قضیهٔ اصلی

در این بخش، قضیهٔ اصلی مقاله را ثابت می‌کنیم. لم زیر بیان می‌کند که در حد یکریختی، تنها گروه غیرآبلی از مرتبهٔ 2^n که زیرگروه دوری از مرتبهٔ 2^{n-1} دارد و عضو مرتبهٔ ۲ در آن یکتا است، ۲–گروه کواترنیون تعمیم‌یافته Q_{2^n} است. برهان لم زیر با تغییراتی جزئی در بخشی از برهان قضیهٔ ۴.۱ در [۲]، به‌دست آمده است.

لم ۱.۲. *فرض کنیم G یک ۲–گروه غیرآبلی متناهی از مرتبهٔ 2^n است. در این صورت اگر G عضوی از مرتبهٔ 2^{n-1} داشته باشد و عضو مرتبهٔ ۲ در آن یکتا باشد، آن‌گاه G با گروه Q_{2^n} یکریخت است.*

اثبات. فرض کنیم x عضوی از مرتبهٔ 2^{n-1} در G است و $M = \langle x \rangle$. در این صورت عضو y در G موجود است که $G = \langle x, y \rangle$. چون G غیرآبلی است، $n \geq 3$. چون اندیس زیرگروه M برابر با ۲ است، پس $y^2 \in M$ و چون M نرمال و دوری است، $y^{-1}xy = x^r$ که در آن، $r \not\equiv 1 \pmod{2^{n-1}}$. همچنین y^2 مولد M نیست، زیرا در این صورت G دوری می‌شود. در نتیجه $y^2 = x^{2s}$. از آنجا که به‌ازای $t = r^i$ داریم $y^{-i}xy^i = x^t$، پس $r^2 \equiv 1 \pmod{2^{n-1}}$. قرار می‌دهیم $t = 2m = 2^n$. چون

$$x^{2s} = y^2 = y^{-1}x^{2s}y = x^{2sr},$$

خواهیم داشت $2(r-1)s \equiv 0 \pmod{m}$. بنابراین

$$(x^\lambda y)^2 = x^\lambda y^2 (y^{-1}x^\lambda y) = x^{\lambda(1+r)+2s}$$

و $x^\lambda y \notin M$. چون $G \setminus M$ شامل عضو مرتبهٔ ۲ نیست، پس همنهشتی

$$(r+1)\lambda + 2s \equiv 0 \pmod{m}$$

برحسب λ جواب ندارد. قرار می‌دهیم

$$r + 1 = 2^e r' \quad \text{و} \quad 2s = 2^f s'$$

که در آن، r' و s' اعداد فرد هستند. پس $f \geq ۱$ و همنهشتی $r'\lambda' + s' \equiv ۰ \pmod m$ برحسب λ' جواب دارد. اگر $e \leq f$، آنگاه $۲^{f-e}\lambda' = \lambda$ در همنهشتی قبل صدق می‌کند که تناقض است و لذا $e > f \geq ۱$. به‌ویژه $r+۱$ بر ۴ بخش‌پذیر است و در نتیجه $r-۱$ بر ۴ بخش‌پذیر نیست. به‌راحتی دیده می‌شود $۲(r-۱)s$ بر m بخش‌پذیر است و از این‌رو $f \geq n-۲$. از آنجا که $y^۲ \neq ۱$، داریم $f = n-۲$ و $y^۲ = x^{۲s} = x^{۲^{n-۲}}$. به‌علاوه

$$r+۱ = ۲^e r' \equiv ۰ \pmod m$$

و لذا می‌توانیم قرار دهیم $r = -۱$ که ثابت می‌کند $G \cong Q_t$. □

در ادامه با استفاده از لم قبل به بیان اثباتی جدید از قضیهٔ اصلی مقاله می‌پردازیم.

اثبات. فرض کنیم $|G| = ۲^n$. حکم را با استقرا روی n ثابت می‌کنیم. به‌آسانی می‌توان نشان داد که برای گروه‌هایی که مرتبهٔ آنها ۲، ۴ و ۸ است و در شرط قضیه صدق می‌کنند، حکم برقرار است. حال فرض کنیم حکم برای تمام ۲-گروه‌هایی که عضو مرتبهٔ ۲ در آنها یکتا است و مرتبهٔ آنها کمتر از مرتبهٔ G است، برقرار باشد و $|G| = ۲^n$ که $n \geq ۴$. زیرگروه ماکسیمال M از G را در نظر می‌گیریم. چون $|M| < |G|$ و عضو مرتبهٔ ۲ در M یکتا است، M دوری است و یا $M \cong Q_{۲^{n-۱}}$. اگر M دوری و G غیرآبلی باشد، آنگاه بنابر لم قبل، $G \cong Q_{۲^n}$ و اگر $M = \langle a \rangle$ و G آبلی و غیردوری باشد، آنگاه $G \cong \langle a \rangle \times H$. از این‌رو G دست‌کم دو عضو از مرتبهٔ ۲ دارد که تناقض است. پس اگر G آبلی باشد، آنگاه G دوری است. بنابراین اگر G دست‌کم یک زیرگروه ماکسیمال دوری داشته باشد، حکم برقرار است. حال فرض کنیم تمام زیرگروه‌های ماکسیمال G، گروه کواترنیون تعمیم‌یافته از مرتبهٔ $۲^{n-۱}$ هستند. فرض کنیم

$$M_i = \langle x_i, y_i | x_i^{۲^{n-۲}} = ۱, y_i^۲ = x_i^{۲^{n-۳}}, y_i x_i = x_i^{-۱} y_i \rangle, \quad ۱ \leq i \leq r$$

تمام زیرگروه‌های ماکسیمال G هستند. چون برای هر i، $|G/M_i| = ۲$، پس برای هر x در G داریم $x^۲ \in M_i$ و لذا $\langle x_۱^۲ \rangle \subseteq \Phi(G)$. از این‌رو

$$|\langle x_۱^۲ \rangle| = ۲^{n-۳} \leq |\Phi(G)|.$$

حال مرتبهٔ $\Phi(G)$ را در نظر می‌گیریم:

(۱) $|\Phi(G)| = ۲^{n-۱}$. در این صورت G تنها یک زیرگروه ماکسیمال دارد. اما تنها ۲-گروهی که زیرگروه ماکسیمال یکتا دارد، ۲-گروه دوری است و این با فرض غیرآبلی بودنِ G تناقض دارد.

(۲) $|\Phi(G)| = ۲^{n-۲}$. در این حالت داریم $|G/\phi(G)| = ۴$ و از این‌رو $\frac{G}{\phi(G)} \cong Z_۲ \times Z_۲$. چون $\frac{G}{\phi(G)}$ سه زیرگروه ماکسیمال دارد، روشن است که $\mathbf{A} = \{x_i, y_i | ۱ \leq i \leq ۳\}$ یک مجموعهٔ مولد برای G است و از آنجا که $|G/\Phi(G)| = ۲^۲$، یک زیرمجموعهٔ دو عضوی از $\mathbf{A}$ موجود است که G را تولید می‌کند. حالت‌های مختلف برای این مجموعهٔ مولد را در نظر می‌گیریم:

(آ) $G = \langle x_p, y_q \rangle$. اگر $p = q$، آنگاه $G = M_p$ که تناقض است. پس $p \neq q$ و $|\Phi(G)| = |M_i|/۲$. قرار می‌دهیم

$$
\begin{aligned}
A_۱ &= \{۱, x_p^۲, \ldots, x_p^{۲^{n-۳}}\},\\
A_۲ &= \{x_p, x_p^۳, \ldots, x_p^{۲^{n-۳}+۱}\},\\
A_۳ &= \{y_p, y_p x_p^۲, \ldots, y_p x_p^{۲^{n-۳}}\},\\
A_۴ &= \{y_p x_p, y_p x_p^۳, \ldots, y_p x_p^{۲^{n-۳}+۱}\}.
\end{aligned}
$$

این مجموعه‌ها افرازی برای M_p تشکیل می‌دهند به‌طوری که $A_۱ \subseteq \Phi(G)$. همچنین اگر یک عضو از هر یک از A_iها، $i = ۲, ۳, ۴$، متعلق به $\Phi(G)$ باشد، آنگاه $A_i \subseteq \Phi(G)$. بنابراین $\Phi(G) = \langle x_p \rangle$ یا $\Phi(G) = \langle x_p^۲, y_p x_p \rangle$. حال اگر $\Phi(G) = \langle x_p \rangle$، آنگاه $G = \langle y_p \rangle$ که تناقض است. در نتیجه خواهیم داشت $\Phi(G) = \langle x_p^۲, y_p x_p \rangle$. چون برای هر i، $x_p^۲ \in M_i$، پس عددی فرد مانند s موجود است که $x_p^۲ = x_i^{۲s}$. قرار می‌دهیم $x_i' = x_i^s$. به‌آسانی دیده می‌شود که $M_i = \langle x_i', y_i \rangle$. برای سادگیِ نمادها، x_i' را مجدداً با x_i نمایش می‌دهیم. همچنین اگر $y_q \in \Phi(G)$، آنگاه $G = \langle x_p \rangle$. پس $y_q x_q \in \Phi(G)$ و برای $i \neq q$ اگر $\Phi(G) = \langle x_i^۲, y_i \rangle$، آنگاه قرار می‌دهیم $y_i' = y_i x_i$. روشن است که $M_i = \langle x_i, y_i' \rangle$ و $\Phi(G) = \langle x_i^۲, y_i' x_i \rangle$. مجدداً y_i' را با y_i نمایش می‌دهیم. با توجه به مرتبهٔ G، $\Phi(G)$ و M_iها، برای هر $i \neq j$ داریم $M_i \cap M_j = \Phi(G)$. قرار می‌دهیم $M_i' = M_i \setminus \Phi(G)$. به‌سادگی می‌توان دید که حاصل‌ضرب هر دو عضو از M_i'، عضوی از $\Phi(G)$ و حاصل‌ضرب هر عضو از M_i' در عضوی از M_j'، عضوی از M_k' است که در آن، i، j و k متمایزند. حال توجه می‌کنیم که چون عضو مرتبهٔ ۲ در G یکتا است، $x_p^{۲^{n-۳}} = y_p^۲ = y_q^۲$ و لذا $y_q^۲$ با x_p جابه‌جا می‌شود. همچنین $x_p^{۲k} = x_q^{۲k}$ و از این‌رو $y_q x_p^{۲k} = x_p^{-۲k} y_q$. از طرفی توان زوج هر عضو G را می‌توان به‌صورت توانی زوج از x_p نوشت. پس دو حالت ممکن برای y_l $(l \neq p, q)$ عبارت‌اند از:

(اول) $y_l = x_p^{2k'+1}(y_q x_p)^{2m} y_q = x_p^{2k+1} y_q$. در این حالت از آنجا که $y_l^2 = y_q^2$، داریم

$$y_l^2 = x_p^{2k} y_q x_p x_p^{2k} y_q x_p = x_p^{2k} x_p^{-2k} y_q x_p y_q x_p = y_q^2$$

و در نتیجه $x_p y_q x_p = y_q$. گروه $G = \langle x_p, y_q \rangle$ را در نظر می‌گیریم:

$$G = \langle x_p, y_q \mid x_p^{2^{n-2}} = 1, y_q^2 = x_p^{2^{n-3}}, y_q x_p = x_p^{-1} y_q \rangle.$$

بنابراین $G \cong Q_{2^{n-1}}$ که تناقض است.

(دوم) $y_l = x_p^{2k'}(y_q x_p)^{2m+1} = x_p^{2k} y_q x_p$ که در آن، $m, k, k' \in Z$. در این حالت نیز با روشی مشابه با روش بالا به تناقض می‌رسیم. پس مورد (آ) اتفاق نمی‌افتد.

(ب) $G = \langle x_p, x_q \rangle$. در این حالت اگر

$$y_q = x_q^{2k+1} x_p x_q \text{ ، } y_q = x_p^{2k+1} x_q \text{ ، } y_q = x_q^{2k+1} x_p \text{ ، } y_q = x_p^{2k+1} \text{ یا } y_q = x_q^{2k+1},$$

آن‌گاه مشابه با آنچه در قسمت (آ) گفته شد، به تناقض می‌رسیم و اگر $y_q = x_p^{2k+1} x_q x_p$، آن‌گاه $x_q = x_p^{-2k-1} y_q x_p^{-1}$ و در نتیجه $G = \langle x_p, y_q \rangle$ که همان حالت (آ) رخ می‌دهد و دوباره تناقض آشکار می‌شود.

(پ) $G = \langle y_p, y_q \rangle$. در این حالت نیز با در نظر گرفتن عضو x_p و مشابه با روند اثبات قسمت (آ) به تناقض می‌رسیم.

پس حالت (۲) اتفاق نمی‌افتد.

(۳) $|\Phi(G)| = 2^{n-3}$. چون $|G| = 2^n$ و $|M_i| = 2^{n-1}$ و $1 \le i \le r$، پس $r \ge 3$. برای هر $i \neq j$، $|M_i \cap M_j| = 2^{n-2}$ و یا $|M_i \cap M_j| = 2^{n-3}$. فرض کنیم p و q موجودند که $|M_p \cap M_q| = 2^{n-3}$. در این صورت با توجه به مرتبهٔ G و M_iها، برای هر l نامساوی با p و q داریم

$$G = M_p \cup M_l \cup M_q \text{ و } |M_l \cap M_p| = |M_l \cap M_q| = 2^{n-2}.$$

اگر $M_p \cap M_l = \langle x_l^2, y_l x_l \rangle$ و $M_q \cap M_l = \langle x_l^2, y_l \rangle$، آن‌گاه چون $x_q \notin M_l$ و $y_l \notin M_q$، پس $x_q y_l$ عضوی از M_p است که این منجر به تناقض می‌شود. بنابراین

$$M_p \cap M_l = \langle x_p \rangle \quad \text{و} \quad M_q \cap M_l = \langle x_p^2, y_l \rangle.$$

چون $y_p x_q \in M_l \setminus (M_q \cup M_p)$، k موجود است که $y_p x_q = x_p^{2k+1} y_l$ و لذا $x_p^{-1} y_p \in M_q$ که تناقض است. پس برای هر i و j که $i \neq j$ داریم $|M_i \cap M_j| = 2^{n-2}$. اگر p، q و l موجود باشند

که $G = M_p \cup M_q \cup M_l$، آن‌گاه

$$M_p \cap M_q = M_p \cap M_l = M_q \cap M_l = H.$$

فرض کنیم $H = \langle x_p \rangle$. در این صورت s موجود است که $M_p \cap M_s \neq \langle x_p \rangle$. گیریم

$$M_p \cap M_s = \langle x_s^2, y_s \rangle \quad \text{و} \quad M_q \cap M_s = \langle x_s^2, y_s x_s \rangle.$$

با در نظر گرفتنِ هر زیرگروه 2^{n-1} عضوی ممکن برای $M_l \cap M_s$ به تناقض می‌رسیم. حالت‌های $H = \langle x_p^2, y_p \rangle$ و $H = \langle x_p^2, y_p x_p \rangle$ به‌طور مشابه به تناقض می‌رسند. اکنون گیریم هیچ سه زیرگروه ماکسیمالی با شرایط فوق وجود نداشته باشند و $G = M_p \cup M_l \cup M_q \cup M_s$. بدون کم شدن از کلیّت مسئله، می‌توان فرض کرد

$$M_p \cap M_s = \langle x_p^2, y_p \rangle \text{ ، } M_p \cap M_q = \langle x_p \rangle \quad \text{و} \quad M_p \cap M_l = \langle x_s y_p, x_p^2 \rangle.$$

آن‌وقت می‌توان ثابت کرد که

$$M_q \cap M_s = \langle x_s y_s, x_p^2 \rangle \quad \text{و} \quad M_q \cap M_l = \langle x_p^2, y_l \rangle$$

و لذا $M_l \cap M_s = \langle x_s \rangle$. توجه می‌کنیم که اگر $y_l \in M_s$، آن‌گاه $M_q \cap M_l = M_s \cap M_l$. حال عضو $x = y_l y_p$ را در نظر می‌گیریم. فرض‌های $x \in M_p$، $x \in M_q$، $x \in M_s$ و $x \in M_l$ به‌ترتیب ایجاب می‌کنند که $y_l \in M_p$، $y_p \in M_q$، $y_l \in M_s$ و $y_p \in M_s$ و در هر چهار مورد به تناقض می‌رسیم. □

سپاسگزاری: نویسندگان این مقاله سپاس خود را از سردبیر محترم مجله که بارها مقاله را مطالعه و ویرایش کرده‌اند، ابراز می‌دارند.

مراجع

[1] Hall Jr., M., *The Theory of Groups*, MacMillan, New York, 1959.

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

الهه‌سادات حقی: دانشگاه کاشان، دانشکدهٔ علوم ریاضی
رایانامه: elsahaghi@grad.kashanu.ac.ir

سید علی‌رضا اشرفی: دانشگاه کاشان، دانشکدهٔ علوم ریاضی
رایانامه: ashrafi@kashanu.ac.ir