فرهنگ و اندیشهٔ ریاضی
سال ۴۰، شمارهٔ ۶۸ (بهار و تابستان ۱۴۰۰) صص. ۱۷۳ تا ۱۸۲

قضیه‌ای از فروبنیوس و کاربردهای آن *

دی. خورانا و اِی. خورانا

تقدیم به محمدرضا درفشه، علیرضا جمالی، علی ایرانمنش و بهروز خسروی

مترجم: علیرضا خلیلی اسبویی، سید صادق صالحی امیری

چکیده

در این مقاله، اثباتی مقدماتی از قضیهٔ فروبنیوس و کاربردهای آن در گروه‌های متناهی و نظریهٔ اعداد ارائه می‌شود. این قضیه را فروبنیوس بیش از یک‌صد سال قبل ثابت کرد. اثباتی که فروبنیوس ارائه داد، نتیجه‌ای از نظریهٔ نمایش گروه‌های متناهی است ولی در این مقاله، برهانی بسیار مقدماتی بدون استفاده از نظریهٔ نمایش گروه‌ها ارائه خواهد شد.

۱. سرآغاز

در هر گروه دوریِ متناهی، برای مقسوم‌علیهٔ دلخواه d از مرتبهٔ گروه، دقیقاً d عضو x وجود دارد که در $x^d = ۱$ صدق می‌کنند. در نتیجه در هر گروه آبلی متناهی، تعداد جواب‌های معادلهٔ $x^d = ۱$ مضربی از d است، زیرا آن را می‌توان به‌صورت حاصلضربی مستقیم از گروه‌های دوری نوشت. جالب توجه است که این حکم برای هر گروه متناهی هم صادق است. این نتیجه، یک قضیهٔ اساسی است که فروبنیوس[۱] در سال ۱۸۹۵ آن را ثابت کرده است. در واقع، او نشان داد که اگر d مقسوم‌علیهی از مرتبهٔ گروه متناهی

عبارات و کلمات کلیدی. قضیهٔ فروبنیوس؛ قضیهٔ سیلو؛ تابعِ فی اویلر.

* نام و نشان مقاله به زبان اصلی از این قرار است:
Khurana, D., Khurana, A., A Theorem of Frobenius and its applications, *Mathematics Magazine*, **78** (2005), no. 3, 220–225.

[۱] F. G. Frobenius

G باشد، آنگاه تعداد جواب‌های معادلهٔ $x^d = ۱$ در G مضربی از d است. این نتیجه که ما آن را قضیهٔ فروبنیوس می‌نامیم، انگیزه‌های فراوانی در حلّ معادلات در گروه‌ها ایجاد کرده است که جزئیات آن را می‌توان در فینکلشتاین[۱] یافت [۸]. این قضیه به روش‌های دیگری نیز ثابت شده و تعمیم یافته است که می‌توان آنها را در [۱]، [۲، ص. ۴۹]، [۳، ص. ۹۲]، [۱۱]، [۱۲، ص. ۱۳۶] و [۱۸، ص. ۷۷] ملاحظه کرد. اثباتی که فروبنیوس ارائه کرده است، نتیجه‌ای از نظریهٔ نمایش گروه‌ها است (برای مثال، می‌توانید به [۲۰] مراجعه کنید). اما در حال حاضر، اثبات‌های مقدماتی متعددی برای آن وجود دارد. با وجود ماهیت بنیادی قضیهٔ فروبنیوس، برخلاف قضیه‌های سیلو، جایگاه شایستهٔ خود را در کتاب‌های درسی دورهٔ کارشناسی پیدا نکرده است. در واقع، قضیهٔ فروبنیوس حتی در بیشتر کتاب‌های درسی پیشرفته در نظریهٔ گروه‌ها نیز مشاهده نمی‌شود. اثبات و کاربردهایی که در این مقاله ارائه می‌کنیم، صرفاً بر اساس اطلاعات مقدماتی از نظریهٔ گروه‌ها است. از این‌رو به خوانندگان توصیه می‌شود به کتاب هرشتاین[۲] [۱۳] مراجعه کنند. در بخش پایانی، دربارهٔ تعدادی از کاربردهای قضیهٔ فروبنیوس در نظریهٔ اعداد بحث می‌کنیم.

برای اینکه به اهمیت قضیهٔ فروبنیوس پی ببرید، نتیجه‌ای استاندارد را که معمولاً با استفاده از قضیه‌های سیلو در اکثر کتاب‌های کارشناسی در زمینهٔ جبر ثابت شده است، یادآوری می‌کنیم. می‌دانیم که هر گروه از مرتبهٔ اول، دوری است. آیا عدد طبیعی دیگری مانند n وجود دارد به‌طوری که هر گروه از این مرتبه، دوری باشد؟ در ادامه یک روش متداول با استفاده از قضیه‌های سیلو برای $n = pq$ که در آن، p و q دو عدد اول هستند و $p < q$ بیان می‌کنیم. فرض کنیم G گروهی از مرتبهٔ pq است. عدد صحیح نامنفی k وجود دارد به‌طوری که تعداد q-زیرگروه‌های سیلوی G برابر با $۱ + kq$ است و $p \mid (۱ + kq)$. چون $p < q$ پس $k = ۰$. بنابراین زیرگروهی یکتا از مرتبهٔ q وجود دارد که نتیجه می‌دهد این زیرگروه نرمال است. اگر $p \nmid (q - ۱)$، آنگاه p-زیرگروه سیلوی G نیز نرمال است. از این‌رو G حاصلضرب مستقیم زیرگروه‌هایی از مرتبهٔ p و q خواهد بود و لذا G دوری است. اما قضیهٔ فروبنیوس نتیجه‌ای قوی‌تر دارد و به‌کمک آن می‌توان گروه‌های دوری از مرتبهٔ n را شناسایی کرد. در واقع، این nها در شرط $(n, \phi(n)) = ۱$ (که در آن، $\phi(n)$ تعداد اعداد صحیح مثبت کوچکتر از n است که نسبت به n اول‌اند) صادق هستند.

گروه G را *ساده* می‌نامیم اگر $\{۱\}$ و G تنها زیرگروه‌های نرمال آن باشند. برای مثال، تنها گروه‌های ساده آبلی، گروه‌های دوری از مرتبهٔ عددی اول هستند. گروه G را *حل‌پذیر* می‌نامیم در صورتی که سری نرمالی مانند $\{۱\} = N_۰ \lhd N_۱ \lhd \cdots \lhd N_r = G$ داشته باشد که به‌ازای هر i که $۱ \le i \le r$، گروه خارج‌قسمتی $N_i/N_{i-۱}$ آبلی باشد؛ مخصوصاً یک گروه حل‌پذیر غیرآبلی، ساده نیست.

[۱] H. Finkelstein [۲] I. N. Herstein

همان‌طور که در بالا اشاره شد، در گروهی از مرتبهٔ pq که در آن، p و q دو عدد اول باشند $(p < q)$، q- زیرگروه سیلو در G نرمال است. بنابراین G ساده نیست. با کمی تلاش بیشتر و با استفاده از قضیه‌های سیلو می‌توان نشان داد که هر گروهی از مرتبهٔ pqr به‌طوری که p، q و r سه عدد اول باشند و $p < q < r$، دارای r-زیرگروه سیلوی نرمال است. اما قضیه‌های سیلو برای گروهی که مرتبهٔ آن حاصلضرب بیش از سه عدد اول متمایز باشد، کارایی ندارد.

با استفاده از قضیهٔ فروبنیوس، به‌آسانی می‌توان نشان داد که اگر هر p-زیرگروه سیلوی G دوری (برای مثال، اگر مرتبهٔ گروه خالی از مربع باشد) و q بزرگترین مقسوم‌علیه اول مرتبهٔ گروه باشد، آن‌گاه q-زیرگروه سیلو در G نرمال است و بنابراین G ساده نیست. برنساید[۱] [۲] حدس زده بود که گروهی ساده از مرتبهٔ فرد وجود ندارد. ادعای وی با اثبات حل‌پذیریِ گروه‌های از مرتبهٔ فرد توسط فیت[۲] و تامسون[۳] [۷] در سال ۱۹۶۳ تأیید شد. در واقع، آنها نشان دادند اگر G گروهی غیرآبلی از مرتبهٔ فرد باشد، آن‌گاه زیرگروه مشتق G، یعنی G' زیرگروهِ سرهٔ نرمال G است و لذا G ساده نیست. با استفاده از قضیهٔ فروبنیوس به‌آسانی می‌توان نشان داد که گروهی که همهٔ سیلو زیرگروه‌های آن دوری باشند، حل‌پذیر است.

۲. قضیهٔ فروبنیوس

در ادامه G را گروهی متناهی و $o(g)$ را مرتبهٔ عضو g از G می‌گیریم. اگر S مجموعه‌ای متناهی باشد، آن‌گاه منظور از $|S|$، تعداد عضوهای S است. اگر H زیرگروه (زیرگروه نرمال) G باشد، آن را با نماد $H \leq G$ $(H \trianglelefteq G)$ نشان می‌دهیم. اگر d مرتبهٔ G را بشمارد، آن‌گاه A_d را به‌صورت زیر تعریف می‌کنیم:

$$A_d = \{x \in G : x^d = 1\}.$$

اگر $S \subseteq G$، آن‌گاه *زیرگروه تولیدشده* توسط S را با نماد $\langle S \rangle$ نشان می‌دهیم. بزرگترین مقسوم‌علیه مشترک و کوچکترین مضرب مشترک m و n را به‌ترتیب با نمادهای $\gcd(m,n)$ و $\operatorname{lcm}(m,n)$ نشان می‌دهیم. برای عضو $a \in G$،

$$N(a) = \{g \in G : ag = ga\}$$

مرکزساز a و

$$C(a) = \{gag^{-1} : g \in G\}$$

ردهٔ تزویج a است. برای اثبات قضیهٔ فروبنیوس، ابتدا لم زیر را ثابت می‌کنیم که به‌دفعات در این مقاله مورد استفاده قرار خواهد گرفت.

[۱] W. Burnside [۲] W. Feit [۳] J. G. Thompson

لم ۱.۲. *به‌ازای هر عدد طبیعی n، تعداد عضوهای از مرتبهٔ n درگروه G، صفر یا مضربی از $\phi(n)$ است. به‌علاوه اگر $d = p^{\alpha}s$ مقسوم‌علیهی از $|G|$ باشد به‌طوری که $p^{\alpha+1} \mid |G|$ و $\gcd(p,s) = 1$، آن‌گاه مجموعهٔ $A = A_{dp} \setminus A_d$ یا تهی است یا تعداد عضوهای آن، مضربی از $\phi(p^{\alpha+1})$ است.*

اثبات. رابطهٔ زیر را روی گروه G تعریف می‌کنیم:

$$x \text{ با } y \text{ رابطه دارد اگر و تنها اگر } \quad \langle x \rangle = \langle y \rangle.$$

به‌روشنی این، یک رابطهٔ هم‌ارزی روی G است. چون $o(x^t) = o(x)$ اگر و تنها اگر $(t, o(x)) = 1$، پس ردهٔ هم‌ارزی x دارای $\phi(o(x))$ عضو است. چون G اجتماعی از رده‌های هم‌ارزی است، پس مجموعهٔ عضوهای از مرتبهٔ n اجتماعی از رده‌های هم‌ارزی است. بنابراین عدد اصلی آن، مضربی از $\phi(n)$ است. برای اثبات قسمت دوم، توجه داریم که مجموعهٔ A را می‌توان به‌صورت

$$A = \{x \in G : o(x) = p^{\alpha+1}s_1, s_1 \mid s\}$$

نوشت. اگر $A \neq \emptyset$، آن‌گاه A اجتماع رده‌های هم‌ارزی عضوهایی مانند x است که $o(x) = p^{\alpha+1}s_1$ و عدد اصلی آن، مضربی از $\phi(p^{\alpha+1})$ است، زیرا $\phi(p^{\alpha+1}s_1) = \phi(p^{\alpha+1})\phi(s_1)$. بنابراین تعداد اعضای A مضربی از $\phi(p^{\alpha+1})$ است. □

قبل از اینکه به اثبات قضیهٔ فروبنیوس بپردازیم، گزارهٔ زیر را یادآوری می‌کنیم. فرض کنیم G گروهی متناهی باشد، $x \in G$ و $o(x) = mn$ به‌طوری که $\gcd(m,n) = 1$. در این صورت، y و z در G وجود دارند که $x = yz$، $o(y) = m$، $o(z) = n$ و $yz = zy$. (راهنمایی: اعداد صحیح m و n وجود دارند که $am + bn = 1$. اکنون قرار دهید $y = x^{bn}$ و ...)

قضیه ۲.۲ (فروبنیوس). *اگر d مقسوم علیهی از $|G|$ باشد، آن‌گاه d مقسوم‌علیهی از A_d است.*

اثبات. استقرای دوگانه را روی $|G|$ و d به‌کار می‌گیریم. اگر $d = |G|$ یا $d = 1$، آن‌گاه حکم بدیهی است. فرض کنیم $|G| > 1$، $d < |G|$ و حکم برای هر مقسوم‌علیه ماکسیمال $|G|$ و گروه‌هایی از مرتبهٔ کمتر از $|G|$ برقرار باشد. فرض کنیم p مقسوم‌علیه اول دلخواهی از $\frac{|G|}{d}$ باشد و $d = p^{\alpha}s$ که در آن، $(p,s) = 1$). فرض کنیم $A = A_{dp} \setminus A_d$. توجه داریم که $|A_{dp}| = |A_d| + |A|$. از طرفی بنابر فرض استقرا، $|A_{dp}| \mid d$. بنابراین کافی است نشان دهیم که $|A| \mid d$. اگر $A = \emptyset$، آن‌گاه حکم برقرار است. پس فرض می‌کنیم $A \neq \emptyset$. با استفاده از لم قبل، $|A|$ مضربی از $\phi(p^{\alpha+1}) = p^{\alpha}(p-1)$ است. در نتیجه کافی است نشان دهیم که $s \mid\mid |A|$. چون

$$A = \{x \in G : o(x) = p^{\alpha+1}s_1, s_1 \mid s\},$$

پس هر عضو x از A به‌شکل $yz = zy$ است که در آن، $o(y) = p^{\alpha+1}$ و $z^s = 1$. متناظر با $a \in G$ از مرتبهٔ $p^{\alpha+1}$، S_a را به‌صورت زیر تعریف می‌کنیم:

$$S_a = \{ab \in G : b \in N(a), b^s = 1\};$$

همچنین $S_{C(a)}$ را به‌صورت زیر تعریف می‌کنیم:

$$S_{C(a)} = \bigcup \{S_x : x \in C(a)\}.$$

در این صورت، A اجتماعی از S_aها است. اینک نشان می‌دهیم که عضوهای این اجتماع دوبه‌دو مجزا هستند. فرض کنیم $o(a) = o(a_1) = p^{\alpha+1}$، $ab = a_1b_1$ و $b^s = b_1^s = 1$ که در آن، $ab = ba$ و $a_1b_1 = b_1a_1$. چون $(ab)^s = (a_1b_1)^s$، پس $a^s = a_1^s$. از آنجا که $a^{p^{\alpha+1}} = a_1^{p^{\alpha+1}}$ و $\gcd(p^{\alpha+1}, s) = 1$، داریم $a = a_1$ که نشان می‌دهد A اجتماع مجزایی از S_aها است. بنابراین کافی است نشان دهیم که s مقسوم‌علیهی از $|S_{C(a)}|$ است. با توجه به اینکه نگاشت

$$\varphi : S_a \longrightarrow S_{xax^{-1}}$$

با ضابطهٔ $\varphi(ab) = xax^{-1}xbx^{-1}$ دوسویی است، داریم $|S_{C(a)}| = |C(a)||S_a|$. فرض کنیم $o(N(a)/\langle a\rangle) = k$ و $m = \gcd(s, k)$. در این صورت، نگاشت

$$\varphi_1 : S_a \longrightarrow \{y \in N(a)/\langle a\rangle : y^s = 1\} = \{y \in N(a)/\langle a\rangle : y^m = 1\}$$

با ضابطهٔ $\varphi_1(ab) = b\langle a\rangle$ دوسویی است. چون $|N(a)/\langle a\rangle| < |G|$، بنابر فرض استقرا، عددی طبیعی مانند c وجود دارد که

$$|\{y \in N(a)/\langle a\rangle : y^m = 1\}| = |S_a| = cm;$$

همچنین

$$|S_{C(a)}| = |C(a)||S_a| = |G||S_a|/|N(a)| = |G|cm/kp^{\alpha+1}.$$

چون k و s هر دو مقسوم‌علیه $|G|$ هستند، داریم $\operatorname{lcm}(k, s) = ks/m$ که نشان می‌دهد s مقسوم‌علیه $|G|cm/k$ است. سرانجام، چون $p^{\alpha+1}$ مقسوم‌علیهی از $|G|cm/k$ است و $\gcd(p, s) = 1$، نتیجه می‌گیریم که s مقسوم‌علیه $|S_{C(a)}|$ است. □

۳. چند کاربرد قضیهٔ فروبنیوس در نظریهٔ گروه‌ها

در این بخش، تعدادی از کاربردهای قضیهٔ فروبنیوس را که در مقدمه به آنها اشاره شد، بیان می‌کنیم. در ادامه از این گزاره به‌دفعات استفاده می‌کنیم: اگر d مقسوم‌علیه‌ای از $|G|$ و $d = |A_d|$، آنگاه هر زیرگروه مانند H از مرتبهٔ d با A_d برابر است و لذا در G نرمال است.

کاربرد ۱. فرض کنیم G گروهی از مرتبهٔ $p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_r^{\alpha_r}$ باشد که $p_1 < p_2 < \cdots < p_r$ اعدادی اول هستند. اگر هر p-زیرگروه سیلو G دوری باشد، آنگاه p_r-زیرگروه سیلوی G در G نرمال است. به‌علاوه G حل‌پذیر است. در حالت خاص، اگر $|G|$ عددی خالی از مربع و p بزرگترین مقسوم‌علیه اول $|G|$ باشد، آنگاه p-زیرگروه سیلوی G در G نرمال و G حل‌پذیر است.

اثبات. نشان می‌دهیم برای هر مقسوم‌علیه d از $|G|$ به‌شکل $p_k^{\beta_k}p_{k+1}^{\alpha_{k+1}}\cdots p_r^{\alpha_r}$ که در آن، $k \le r$ و $\beta_k \le \alpha_k$، داریم $d = |A_d|$. برای $d = |G|$ نتیجه بدیهی است، پس فرض می‌کنیم $d < |G|$ و نتیجه برای هر مقسوم‌علیه بزرگتر از d برقرار باشد. فرض کنیم p بزرگترین مقسوم‌علیه اول $\frac{|G|}{d}$ باشد و $A = A_{dp} \setminus A_d$. چون هر p-زیرگروه سیلو G دوری است، پس $A \neq \emptyset$. با توجه به فرض $|A_{dp}| = dp$ و بنابر قضیهٔ فروبنیوس، عددی طبیعی مانند t وجود دارد که $1 \le t \le p$ و $|A_d| = dt$. بنابر لم بالا، $(p-1) \mid dp - dt = d(p-t)$. چون هر مقسوم‌علیه اول d بزرگتر یا مساوی p است، پس $\gcd(p-1, d) = 1$. از این‌رو $p - 1 \mid p - t$ و $t = 1$. بنابراین $|A_d| = d$ و در حالت خاصِ $|A_{p_r^{\alpha_r}}| = p_r^{\alpha_r}$ نتیجه می‌شود که p-زیرگروه سیلو مانند N در G نرمال است. اینک با استفاده از استقرا روی $|G|$، ثابت می‌شود که N و $\frac{G}{N}$ حل‌پذیرند و بنابراین G حل‌پذیر است. چون هر گروه از مرتبهٔ عددی اول دوری است، حالت خاص آن روشن است. □

کاربرد ۲. فرض کنیم n یک عدد صحیح مثبت باشد. در این صورت، هر گروه از مرتبهٔ n دوری است اگر و تنها اگر $(n, \phi(n)) = 1$.

اثبات. به‌آسانی ملاحظه می‌شود که $(n, \phi(n)) = 1$ اگر و تنها اگر n عددی خالی از مربع باشد و برای هر دو مقسوم‌علیه p و q از n داشته باشیم $p \nmid q - 1$. فرض کنیم $(n, \phi(n)) \neq 1$. نشان می‌دهیم که گروه غیردوری از مرتبهٔ n وجود دارد. اگر برای عددی اول مانند p، $p^2 \mid n$ آنگاه $\mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_{n/p^2}$ یک گروه غیردوری از مرتبهٔ n است (یادآوری می‌کنیم که گروه $\mathbb{Z}_m \times \mathbb{Z}_n$ دوری است اگر و تنها اگر $\gcd(m, n) = 1$). حال فرض کنیم n خالی از مربع باشد و p و q دو مقسوم‌علیه اول n باشند به‌طوری که $p < q$ و $p \mid q - 1$. چون $\mathbb{Z}_q \setminus \{0\}$ نسبت به عمل ضرب به پیمانهٔ q تشکیل گروه می‌دهد و $p \mid q - 1$، پس دارای زیرگروه H از مرتبهٔ p است. یک عمل دوتایی روی مجموعهٔ $\mathbb{Z}_q \times H$ به‌صورت

زیر تعریف می‌کنیم:

$$(x,h)(y,k)=(x+hy,hk).$$

مجموعهٔ $H\times\mathbb{Z}_q$ با این عمل، تشکیل یک گروه با عضو همانی $(۰,۱)$ می‌دهد به‌طوری که وارون عضو دلخواه (x,h) از آن، عبارت است از $(x,h)^{-۱}=(-h^{-۱}x,h^{-۱})$. از طرفی، چون برای هر $h\neq ۱$ داریم $(۱,h)(۱,۱)\neq(۱,۱)(۱,h)$، پس $G:=\mathbb{Z}_q\times H$ یک گروه غیرآبلی است. بنابراین $G\times\mathbb{Z}_{n/pq}$ یک گروه غیرآبلی از مرتبهٔ n است. حال فرض کنیم $(n,\phi(n))=۱$. برای هر مقسوم‌علیه d از $|G|$ ثابت می‌کنیم که $|A_d|=d$. با استفاده از استقرا روی d ادامه می‌دهیم. اگر $d=|G|$، آن‌گاه حکم واضح است. فرض کنیم $d<|G|$ و نتیجه برای هر مقسوم‌علیه بزرگتر از d برقرار باشد. فرض کنیم p مقسوم‌علیه دلخواهی از $|G|/d$ باشد و $A=A_{pd}\setminus A_d$. به‌روشنی $A\neq\emptyset$. بنابر فرض استقرا، $|A_{dp}|=dp$ و به‌موجب قضیهٔ فروبنیوس، عددی طبیعی مانند t وجود دارد که $۱<t<p$ و $|A_d|=dt$. با بحثی مشابه آن که در کاربرد ۱ ارائه شد، می‌توان نشان داد که $t=۱$. بنابراین $|A_d|=d$. در حال خاص، برای هر مقسوم‌علیه اول $|G|$ مانند p داریم $|A_p|=p$. در نتیجه هر p-زیرگروه سیلوی G در G نرمال است. از این‌رو G حاصلضرب مستقیم p-زیرگروه‌های دوری‌اش است که مرتبهٔ آنها دوبه‌دو نسبت به هم اول‌اند و لذا G دوری است. □

دیکسون[۱] نشان داد که به‌ازای چه مقادیری از n، هرگروه از مرتبهٔ n دوری است [۶]. میلر[۲] و مورِنو[۳] روی گروه‌های غیرآبلی‌ای که هر زیرگروه آنها آبلی است، مطالعه کردند. آنها نشان دادند که مرتبهٔ هر گروه غیرآبلی که هر زیرگروه آن آبلی است، حداکثر دارای دو عامل اول متمایز است [۱۷]. همان‌طور که قبلاً اشاره شد، اگر $|A_d|=d$، آن‌گاه هر زیرگروهی که با A_d برابر باشد، نرمال است. عکس این مطلب همواره برقرار نیست، یعنی یک زیرگروه نرمال ممکن است با A_d برابر نباشد. برای مثال، اگر $G=\mathbb{Z}_۲\times\mathbb{Z}_۲$ و $N=\langle(۱,۰)\rangle$، آن‌گاه $N\trianglelefteq G$ و $|N|=۲$. اما $|A_۲|=۴$؛ در حالی که اگر $N\trianglelefteq G$ و $\gcd(|N|,|G/N|)=۱$، آن‌گاه $N=A_{|N|}$. برای اثبات این مطلب، فرض کنیم $a\in A_{|N|}$. در این صورت، $aN\in G/N$ که نتیجه می‌شود $a^{|G/N|}\in N$ و $a\in A_{|N|}$. بنابراین $a^{|N|}=۱\in N$. با توجه به اینکه $\gcd(|N|,|G/N|)=۱$، نتیجه می‌گیریم $a\in N$.

با بحثی مشابه می‌توان نشان داد که اگر $K\trianglelefteq N\trianglelefteq G$ و $\gcd(|K|,|N/K|)=۱$، آن‌گاه $K\trianglelefteq G$، زیرا اگر $k\in K$ و $g\in G$، آن‌گاه $x=gkg^{-۱}\in N$. بنابراین $x^{|N/K|}\in K$ و $x^{|K|}=۱\in K$، که نتیجه می‌دهد $x\in K$. اما این نتیجه برای هر سری زیرنرمال درست نیست. برای مثال، فرض کنیم $G=Alt_۴$ و

$$N=V_۴=\{۱,(۱۲)(۳۴),(۱۳)(۲۴),(۱۴)(۲۳)\}$$

[۱] L. E. Dickson [۲] G. A. Miller [۳] H. C. Moreno

و $K = \{۱, (۱۲)(۳۴)\}$. در این صورت، $K \trianglelefteq N \trianglelefteq G$ ولی K در G نرمال نیست. دلیل نادرستی آن این است که $\gcd(|K|, |N/K|) \neq ۱$.

در سال ۱۸۹۵ فروبنیوس حدس زد که اگر $|A_d| = d$، آنگاه A_d تشکیل یک زیرگروه می‌دهد [۹]. بسیاری از متخصصین نظریهٔ گروه‌ها برای اثبات این حدس تلاش کردند. سرانجام، این حدس در سال ۱۹۹۱ در [۱۴] ثابت و جزئیات آن بعداً در [۱۵] منتشر شد. فرض کنیم G گروهی از مرتبهٔ $p^\alpha m$ است که در آن، $(p, m) = ۱$ و p کوچکترین مقسوم‌علیه $|G|$ است. اگر p-زیرگروه سیلوی G دوری باشد، آنگاه همان‌طور که در کاربرد ۱ بحث شد، برای هر β که $۱ \leq \beta \leq \alpha$ داریم $|A_{n/p^\beta}| = n/p^\beta$. بنابراین از حدس فروبنیوس نتیجه می‌شود که G زیرگروهی از مرتبهٔ n/p^β دارد.

۴. چند کاربرد قضیهٔ فروبنیوس در نظریهٔ اعداد

پژوهشگران متعددی A_d را روی گروه متقارن مطالعه کرده‌اند [۴، ۵، ۱۶، ۱۹]. می‌دانیم که دو عنصر در S_n مزدوج هستند اگر و تنها اگر دارای ساختار دوری یکسانی باشند. بنابراین اگر ساختار دوری $\sigma \in S_n$ شامل $l_۱$ دور به‌طول ۱، $l_۲$ دور به‌طول ۲، ... و l_m دور به طول m باشد به‌طوری که $\sum_{i=۱}^{m} l_i n_i = n$، آنگاه می‌توان نشان داد که تعداد مزدوج‌های σ در S_n برابر است با

$$\frac{n!}{\prod_{i=۱}^{m} l_i^{n_i} \prod_{i=۱}^{m} n_i!}; \tag{۱.۴}$$

همچنین تعداد r-دورها در S_n برابر با $n!/r(n-r)!$ است. با انتخاب مناسب d در گروه متقارن S_n و محاسبه $|A_d|$ می‌توان روابط سودمند فراوانی در نظریهٔ اعداد به‌دست آورد.

کاربرد ۳. برای هر عدد اول p و هر عدد طبیعی n که $n \geq p$ داریم

$$\sum_{k=۱}^{t} \frac{n!}{p^k (n-kp)! k!} \equiv -۱ \pmod{p}$$

که در آن، t بزرگترین عدد طبیعی است که $tp \leq n$.

اثبات. چون A_p در S_n فقط شامل دورهایی به طول ۱ و p است، با استفاده از (۱.۴) داریم

$$|A_p| = ۱ + \sum_{k=۱}^{t} \frac{n!}{p^k (n-kp)! k!}$$

که در آن، t تعداد جایگشت‌هایی به‌صورت حاصلضرب k تا p-دور و $n-kp$ تا ۱-دور است و جمعوند ۱ هم جایگشت همانی را می‌شمارد. اکنون به‌کمک قضیهٔ فروبنیوس نتیجه حاصل می‌شود. □

قابل توجه است که اگر در کاربرد ۳، n را برابر با p فرض کنیم آن‌گاه قضیهٔ معروفِ ویلسون نتیجه می‌شود که می‌گوید برای عدد اول p، $(p-1)! \equiv -1 \pmod{p}$.

کاربرد ۴. اگر $n/2 < p_1 < p_2 < \cdots < p_k < n$ که در آن، $n \in \mathbb{N}$ و p_iها اعدادی اول هستند، آن‌گاه

$$\sum_{t=1}^{k} \frac{n!}{p_t(n-p_t)!} \equiv -1 \pmod{p_1 p_2 \cdots p_k}$$

اثبات. کافی است $|A_{p_1 p_2 \cdots p_k}|$ را در S_n مانند کاربرد ۳ به‌دست آوریم. □

با ادامهٔ این روش، می‌توان روابطی مشابه روابط بالا به‌دست آورد.

مراجع

[1] Brauer, R., On a theorem of Frobenius, *Amer. Math. Monthly,* **76** (1969), 12–15.

[2] Burnside, B., *The Theory of Groups of Finite Order*, 2nd ed., Dover, New York, 1955.

[3] Carmichael, R. D., *Introduction to the Theory of Groups of Finite Order*, Dover, New York, 1956.

[4] Chowla, S., Herstein, I. N., Moore, W. K., On recursions connected with symmetric groups I, *Canad. J. Math.,* **3** (1951) , 328–334.

[5] Chowla, S., Herstein, I. N., Scott, W. R., The solutions of $X^d = 1$ in symmetric groups, *Norske Vid. Selsk. Forh. (Trondheim),* **25** (1952), 29–31.

[6] Dickson, L. E., Definitions of a group and a field by independent postulates, *Trans. Amer. Math. Soc.,* **6** (1905), 198–204.

[7] Feit, W., Thompson, J. G., Solvability of groups of odd orders, *Pacific J. Math.,* **13** (1963), 775–1029.

[8] Finkelstein, H., Solving Equations in Groups, *Period. Math. Hungar,* **9** (1978), 187–204.

[9] Frobenius, F. G. (1895), Verallgemeinerung des Sylowschen Satzes, Berliner Sitz., 981-993.

[10] Frobenius, F. G. (1895), Über endliche gruppen, Berliner Sitz., 81–112.

[11] Frobenius, F. G. (1903), Über einen Fundamentalsatzd er GruppentheorieB, erliner Sitz., 987-991.

[12] Hall, M., *The Theory of Groups*, Macmillan, New York, 1959.

[13] Herstein, I. N., *Topics in Algebra*, Blaisdell, New York, 1964

[14] Iiyori, N., Yamaki, H., On a conjecture of Frobenius, *Bull. Amer. Math. Soc.,* **25** (1991), 413–416.

[15] Iiyori, N., A conjecture of Frobenius and the simple groups of Lie type IV, *J. Algebra,* **154** (1993), 188–214.

[16] Jacobstal, E., Sur le nombre d'éléments du groupe symétrique S_n dont l'ordre est un nombre premier, *Norske Vid. Selsk. Forh. (Trondheim),* **21** (1949), 49–51.

[17] Miller, G. A., Moreno, H. C., Non-abelian groups in which every subgroup is abelian, *Trans. Amer. Math. Soc.,* **4** (1903) , 398–404.

[18] Miller, G. A., Blichfeldt, H. F., Dickson, L. E., *Theory and Application of Finite Groups*, Dover, New York, 1961.

[19] Moser, L., Wyman, M., On solutions of $x^d = ۱$ in symmetric groups, *Canad. J. Math.,* **7** (1955), 159–168.

[20] Serre, J. P., *Linear Representations of Finite Groups*, Springer-Verlag, GTM **42,** 1997.

تاریخ ارسال: ۱۳۹۸/۵/۳۰؛ تاریخ بازنگری: ۱۳۹۸/۶/۲۸؛ تاریخ پذیرش: ۱۳۹۸/۷/۵

علیرضا خلیلی اسبویی: تهران، دانشگاه فرهنگیان، گروه آموزش ریاضی.

رایانامه: khaliliasbo@yahoo.com

سید صادق صالحی امیری: بابل، دانشگاه آزاد اسلامی واحد بابل، گروه ریاضی.

رایانامه: salehisss@baboliau.ac.ir