تقابل مربعی در یک گروه متناهی•

ویلیام دوک،* کیمبرلی هاپکینز**

ترجمهٔ محمدرضا درفشه

۱. مقدمه

قانون تقابل مربعی یکی از گوهرهای گرانبهای نظریهٔ اعداد است. در این مقاله نشان می‌دهیم که این قانون دارای تفسیری طبیعی است که می‌توان آن را به هر گروه متناهی دلخواه تعمیم داد. نوشتهٔ ما منحصراً به مفاهیم و نتایجی متکی است که حداقل در یکصد سال اخیر شناخته‌شده بوده‌اند.[۱]

سرشتهای گروههای متناهی نقش اساسی در این نوشته دارند. یادآوری می‌کنیم که یک سرشت χ از یک گروه آبلی متناهی G، عبارت است از یک همریختی از G به $\mathbb{C}^*$، که $\mathbb{C}^*$ گروه ضربی اعداد مختلط ناصفر است. مجموعهٔ تمام سرشتهای متمایز تحت ضرب نقطه به نقطه، گروهی تشکیل می‌دهند که با G یکریخت است. بعداً به مفهوم سرشت گروه متناهی و دلخواه G نیاز داریم، که عبارت است از اثر یک نمایش متناهی‌بعدِ G.

سرشت χ از گروه رده‌های مانده‌ایِ کاهش‌یافته به پیمانهٔ عدد صحیح و مثبت n یعنی $\left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^*$ منجر به یک سرشت دیریکله به پیمانهٔ n می‌گردد که آن را هم با χ نمایش می‌دهیم، و تابعی از اعداد صحیح است که به صورت زیر تعریف می‌شود

$$\chi(a) = \begin{cases} \chi(a) & \text{اگر } a \text{ نسبت به } n \text{ اول باشد} \\ 0 & \text{در غیر این صورت} \end{cases}$$

در حالتی که $n = p$ یک عدد اول فرد باشد، $(\mathbb{Z}/p\mathbb{Z})^*$ گروه دوری از مرتبهٔ (زوج) $p-1$ است. بنابراین، سرشت یکتایی از مرتبهٔ ۲ دارد. سرشت دیریکلهٔ وابسته به آن نماد لژاندر $\left(\frac{\cdot}{p}\right)$ نامیده می‌شود. بنابراین، $\left(\frac{a}{p}\right) = 0$ اگر $p|a$، در غیر این صورت، $1-$ یا (a/p) اگر a به پیمانهٔ p مربع باشد، و $(a/p) = -1$ اگر a به پیمانهٔ p مربع نباشد.

در سال ۱۸۷۲، زولوتارف [۱۳] تفسیری از نماد لژاندر (a/p) ارائه داد که چندان مورد توجه قرار نگرفته است: این نماد، علامت جایگشتی از عناصر $G = \mathbb{Z}/p\mathbb{Z}$ را به دست می‌دهد که توسط ضرب عناصر این گروه در a، به شرط $p \nmid a$، القا می‌شود. برای ملاحظهٔ این مطلب، ابتدا توجه کنید که به این ترتیب، سرشتی از $(\mathbb{Z}/p\mathbb{Z})^*$ معین می‌شود. به‌علاوه، در حالتی که سرشت بدیهی نباشد، این سرشت باید از مرتبهٔ ۲ باشد و در نتیجه، نماد لژاندر است. اما این سرشت بدیهی نیست، زیرا هر مولد $(\mathbb{Z}/p\mathbb{Z})^*$ یک $(p-1)$-دور القا می‌کند که جایگشتی فرد است. با الهام گرفتن از این نکته، در بخش ۳ برای هر گروه متناهی G یک نماد مربعی تعریف خواهیم کرد.

قانون تقابل مربعی کلاسیک حاکی است که به‌ازای اعداد اول و متمایز p و q داریم

$$\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\left(\frac{p}{q}\right), \qquad \left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$$

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}. \qquad (1)$$

روابط فوق را ابتدا گاوس در سال ۱۷۹۶ در ۱۹ سالگی ثابت کرد. او تا سال ۱۸۱۸ شش اثبات برای آنها ارائه کرد.[۱] ایدهٔ نهفته در اثبات ششم وی [۵] (نیز رک، [۲]، ص. ۱۹)، که بر پایهٔ مجموع گاوسی بود، منشأ اثبات قانون تقابل مربعی با استفاده از حساب میدانهای دایره‌ای و خودریختی فروبنیوس بود که این هم در سال ۱۸۹۶ در [۳] معرفی شد.

با ترکیب این روشِ کلاسیک با ابداع دیگری از فروبنیوس که در سال ۱۸۹۶ در [۴] عرضه شد، یعنی جدول سرشت، قانون تقابل را برای نماد مربعی هر گروه متناهی G ثابت خواهیم کرد. پیامدی از نتیجهٔ ما، که در بخش ۳ آمده است، قانون تقابل مربعی کلاسیک را در حالت $G = \frac{\mathbb{Z}}{p\mathbb{Z}}$ نتیجه می‌دهد و همچنین تعمیمی از تعبیر زولوتارف دربارهٔ هر گروه متناهی از مرتبهٔ فرد نیز هست.

۱. برای ملاحظهٔ شرح زیبایی از بیشتر مطالب جبر و نظریهٔ اعداد قرن نوزدهم که به آنها استناد خواهیم کرد، به ([۲]، فصل ۱) رجوع کنید.

۱. مرجع خوبی برای بسیاری از اثباتهای شناخته‌شدهٔ قانون تقابل مربعی، [۸] است. اخیراً یک اثبات کوتاه مقدماتی توسط کیم [۷] به دست آمده است.

۲. نماد کرونکر

قبل از تشریح این تعمیم، قانون تقابل مربعی را با معرفی نمادهای ژاکوبی و کرونکر در یک فرمول می‌نویسیم. نماد ژاکوبی در واقع توسیعی از نماد لژاندر به $\left(\frac{\cdot}{n}\right)$ به‌ازای هر عدد صحیح و مثبت فرد n توسط ضرب است: اگر $n > 1$ و $n = p_1 \dots p_r$ تجزیهٔ n به حاصلضرب اعدادی اول (نه لزوماً متمایز) باشد، داریم

$$\left(\frac{a}{n}\right) = \prod_{k=1}^{r} \left(\frac{a}{p_k}\right)$$

در حالی که $\left(\frac{a}{1}\right) = 1$.

مبین عبارت است از یک عدد صحیح ناصفر d که به پیمانهٔ ۴ همنهشت با یکی از اعداد ۰ یا ۱ است.[1] برای مبین d، نماد کرونکر $\left(\frac{d}{\cdot}\right)$ نماد ژاکوبی را با استفاده از تعریف زیر گسترش می‌دهد

$$\left(\frac{d}{2}\right) = \begin{cases} 0 & \text{اگر } d \text{ زوج باشد} \\ 1 & \text{اگر (پیمانهٔ ۸) } d \equiv 1 \\ -1 & \text{اگر (پیمانهٔ ۸) } d \equiv 5 \end{cases}$$

و همچنین $\left(\frac{d}{-1}\right)$ را علامت d تعریف می‌کنیم. در این صورت، مقدار $\left(\frac{d}{a}\right)$ به‌ازای همهٔ اعداد صحیح a با استفاده از ضرب معین می‌گردد، که در آن قرار می‌دهیم $\left(\frac{d}{0}\right) = 0$ اگر $d \neq 1$ و $\left(\frac{1}{0}\right) = 1$. با این توسیعها، قانون تقابل مربعی (۱) به‌ازای nهای مثبت و فرد و هر عدد صحیح دلخواه a شکل زیبایی به خود می‌گیرد:

$$\left(\frac{a}{n}\right) = \left(\frac{n^*}{a}\right) \qquad (2)$$

که در آن $n^* = (-1)^{\frac{n-1}{2}} n$. توجه کنید که n^* یک مبین است زیرا n فرد است.

۳. نماد مربعی برای یک گروه متناهی

فرض کنید G یک گروه متناهی مرتبهٔ n است. عدد صحیح a که نسبت به n اول است جایگشتی از رده‌های مزدوجی G یعنی $C_1 = \{1\}$، C_2، ...، C_m القا می‌کند، که آن را ϕ می‌نامیم، و این جایگشت عضو g را به g^a می‌فرستد و در نتیجه، ردهٔ C_j به ردهٔ C_j^a تبدیل می‌شود. نماد مربعی برای G به‌ازای هر عدد صحیح a چنین تعریف می‌شود

$$\left(\frac{a}{G}\right) = \begin{cases} 0 & \text{اگر } (a,n) \neq 1 \\ 1 & \text{اگر } \phi \text{ زوج باشد} \\ -1 & \text{اگر } \phi \text{ فرد باشد} \end{cases} \qquad (3)$$

به‌سادگی دیده می‌شود که $\left(\frac{\cdot}{G}\right)$ یک سرشت دیریکلهٔ حقیقی به پیمانهٔ n تعریف می‌کند.[2] مطابق تعبیر زولوتارف که در مقدمه ذکر شد، نماد مربعی برای $G = \mathbb{Z}/p\mathbb{Z}$، که p یک عدد اول فرد است، همان نماد لژاندر است:

$$\left(\frac{a}{G}\right) = \left(\frac{a}{|G|}\right). \qquad (4)$$

ردهٔ مزدوجی Cی برای گروه دلخواه G حقیقی نامیده می‌شود هرگاه $C^{-1} = C$ و در غیر این صورت آن را مختلط می‌نامیم. در اینجا C^{-1} تصویر C تحت نگاشت $g \mapsto g^{-1}$ است. به روشنی دیده می‌شود که رده‌های مزدوجی مختلط به‌صورت زوجهای C و C^{-1} ظاهر می‌شوند و داریم $|C| = |C^{-1}|$. رده‌های مزدوجی را طوری مرتب می‌کنیم که r_1تای اول حقیقی باشند. بنابراین $m = r_1 + 2r_2$، که در آن r_2 نصف تعداد رده‌های مزدوجی مختلط است. سپس قرار می‌دهیم

$$d = d(G) = (-1)^{r_2} |G|^{r_1} \prod_{j=1}^{r_1} |C_j|^{-1} \qquad (5)$$

که یک عدد صحیح ناصفر است، زیرا برای هر ردهٔ مزدوجی C و هر عضو g از C داریم $|G|/|C| = |C_G(g)|$ که $C_G(g)$ مرکزساز g در G است ([۲]، ص. ۴۲). واضح است که d مضربی از $n = |C_G(1)|$ است و عوامل اول آن با عوامل اول n یکی هستند. d را مبین G می‌نامیم، نامی که اولین جملهٔ نتیجهٔ اصلی‌مان آن را توجیه می‌کند.

قضیهٔ ۱. فرض کنید G یک گروه متناهی با مبین d مطابق تعریف (۵) باشد. در این صورت (پیمانهٔ ۴) $d \equiv 1$ یا 0، و به‌ازای هر عدد صحیح a داریم

$$\left(\frac{a}{G}\right) = \left(\frac{d}{a}\right). \qquad (6)$$

به‌ویژه، $\left(\frac{\cdot}{G}\right)$ بدیهی است اگر و تنها اگر d مربع کامل باشد.

در حالتی که مرتبهٔ G فرد باشد تعمیم مستقیم زیر برای قانون تقابل مربعی کلاسیک (۲) حاصل می‌شود.

نتیجهٔ ۱. اگر G از مرتبهٔ فرد n باشد، آنگاه $d = n^*$ و به‌ازای هر عدد صحیح a داریم

$$\left(\frac{a}{G}\right) = \left(\frac{n^*}{a}\right). \qquad (7)$$

همچنین، $\left(\frac{\cdot}{G}\right)$ بدیهی است اگر و تنها اگر n مربع کامل باشد.

با استفاده از (۷) و (۲) نتیجه می‌گیریم که رابطهٔ زولوتارف (۴) برای هر گروه G از مرتبهٔ فرد برقرار است.

۴. برهانها

برای نتایج اساسی مورد نیاز دربارهٔ سرشتهای گروههای متناهی و میدانهای عددی جبری، خواننده را به [۶] و [۱۰] ارجاع می‌دهیم.

فرض کنید G یک گروه متناهی با رده‌های مزدوجی $C_1 = \{1\}$، C_2، ...، C_m است. جدول سرشت G (رک. [۶]، ص. ۱۵۹)

۱. ما حالتی را هم که d مربع باشد در نظر می‌گیریم، که معمولاً مجاز نیست.

۲. در واقع، به‌پیمانهٔ کوچک‌ترین مضرب مشترک مرتبه‌های تمام عناصر G تعریف می‌شود.

ماتریس $m \times m$ زیر است

$$M = \begin{pmatrix} \chi_1(C_1) & \cdots & \chi_1(C_m) \\ \vdots & & \vdots \\ \chi_m(C_1) & \cdots & \chi_m(C_m) \end{pmatrix} \quad (۸)$$

که در آن $\chi_1 = 1$، χ_2، ...، χ_m سرشتهای تحویل‌ناپذیر G هستند ([۶]، ص.۱۱۹). در اینجا از قرارداد $\chi(C) = \chi(g)$ به‌ازای هر $g \in C$ استفاده می‌کنیم. بنا به روابط (دوم) تعامد سرشتها ([۶]، قضیهٔ ۴.۱۶ (۲)، ص.۱۶۱) داریم

$$M^*M = \begin{pmatrix} |G||C_1|^{-1} & & 0 \\ & \ddots & \\ 0 & & |G||C_m|^{-1} \end{pmatrix} \quad (۹)$$

که یک ماتریس قطری است. در بالا M^* ترانهادهٔ مزدوج ماتریس M است. چون رابطهٔ $\chi(C^{-1}) = \bar{\chi}(C)$ به‌ازای هر سرشت χ و هر ردهٔ مزدوجی C برقرار است، به‌سادگی دیده می‌شود که

$$\det\bar{M} = (-1)^{r_2}\det M. \quad (۱۰)$$

با استفاده از (۹) و (۵) به برابری زیر می‌رسیم

$$(\det M)^2 = \ell^2 d \quad (۱۱)$$

که ℓ یک عدد صحیح مثبت است.

هر درایهٔ $\chi_i(C_j)$ از M یک عدد صحیح جبری در میدان دایره‌بری $\mathbb{Q}(\zeta_n)$ است، که $\zeta_n = e^{\frac{2\pi i}{n}}$. اکنون $\mathbb{Q}(\zeta_n)$ یک توسیع گالوای $\mathbb{Q}$ است که گروه گالوای آن یکریخت با $(\mathbb{Z}/n\mathbb{Z})^*$ است که این یکریختی توسط نگاشت $\sigma_a \mapsto a$ معین می‌شود و σ_a در $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ روی ζ_n چنین عمل می‌کند

$$\sigma_a(\zeta_n) = \zeta_n^a$$

([۱۰]، قضیهٔ ۱، ص.۹۲).

با استفاده از این اطلاعات، بررسی صحتِ برابری زیر مشکل نیست

$$\sigma_a\left(\chi(g)\right) = \chi\left(g^a\right) \quad (۱۲)$$

که χ یک سرشت دلخواه و g عضوی از G است.

برای اثبات اولین قسمتِ قضیهٔ ۱، از استدلالی که شور در [۱۲] در اثبات قضیهٔ استیکلبرگر دربارهٔ مبین یک میدان عددی به کار برد استفاده می‌کنیم. توجه کنید که بنا به تعریف دترمینان داریم

$$\det M = \sum \mathrm{sgn}(\rho)\chi_1\left(C_{\rho(1)}\right)\chi_2\left(C_{\rho(2)}\right)\cdots\chi_m\left(C_{\rho(m)}\right)$$

که در آن مجموعیابی به‌ازای تمام جایگشتهای ρ از مجموعهٔ اعداد صحیح $\{1, 2, \ldots, m\}$ انجام می‌شود و بر حسب زوج یا فرد بودن ρ،

$$\mathrm{sgn}(\rho) = \pm 1.$$

عبارت سمت راست برابری فوق را به‌صورت $A - B$ می‌نویسیم که A مجموع جایگشتهای زوج و B مجموع جایگشتهای فرد است. بنا به (۱۲) هر دو عدد صحیح جبری $A + B$ و AB تحت گروه گالوا ناوردا هستند، در نتیجه باید اعداد صحیح معمولی باشند. به‌ویژه، با به کار گرفتن (۱۱) می‌توان نوشت

$$\begin{aligned} \ell^2 d = (A-B)^2 &= (A+B)^2 - 4AB \\ &\equiv (A+B)^2 \equiv 0, 1 \quad (\text{پیمانهٔ } 4) \end{aligned}$$

که به این ترتیب اولین قسمت قضیه به اثبات می‌رسد.

با استفاده از (۸) و (۱۲) آشکار است که

$$\sigma_a(\det M) = \left(\frac{a}{G}\right)\det M \quad (۱۳)$$

و لذا طبق (۱۱) می‌توان نوشت

$$\sigma_a(\sqrt{d}) = \left(\frac{a}{G}\right)\sqrt{d} \quad (۱۴)$$

چون $(\frac{\cdot}{G})$ به‌پیمانهٔ n یک سرشت است، برای اثبات (۶) کافی است آن را به‌ازای $a = p$ با شرط $p \nmid n$ و همچنین به‌ازای $a = -1$ ثابت کنیم. اگر $p \nmid n$، از خودریختی σ_p، که خودریختی فروبنیوس p نامیده می‌شود، استفاده می‌کنیم. گوییم عدد اول p در یک میدان عددی جبری K شکافته می‌شود اگر ایده‌آل اصلی تولید شده توسط p در حلقهٔ اعداد صحیح K به حاصلضرب $[K : \mathbb{Q}]$ ایده‌آل اول متمایز تجزیه گردد که در آن $[K : \mathbb{Q}]$ درجهٔ K روی $\mathbb{Q}$ است. خودریختی فروبنیوس σ_p دارای این خاصیت است که p در هر زیرمیدان $\mathbb{Q}(\zeta_n)$ شکافته می‌شود اگر و تنها اگر σ_p آن زیرمیدان را نقطه به نقطه پایدار نگه دارد ([۱۰]، ص.۹۱). بنابراین، p در $\mathbb{Q}(\sqrt{d})$ شکافته می‌شود اگر و تنها اگر $\sigma_p(\sqrt{d}) = \sqrt{d}$. به‌علاوه، نماد کرونکر دارای این خاصیت اساسی است که p در $\mathbb{Q}(\sqrt{d})$ شکافته می‌شود اگر و تنها اگر $(\frac{d}{p}) = 1$ ([۱۰]، ص.۷۷). بنابراین، با استفاده از (۱۴) نتیجه می‌گیریم که اگر $p \nmid n$ آنگاه

$$\left(\frac{p}{G}\right) = \left(\frac{d}{p}\right).$$

با استفاده از (۱۰) و (۵) داریم

$$\left(\frac{-1}{G}\right) = (-1)^{r_2} = \left(\frac{d}{-1}\right) \quad (۱۵)$$

که به این ترتیب اثبات (۶) به انجام می‌رسد.

یک نتیجهٔ استاندارد ([۹]، قضیهٔ ۳.۳، ص.۷۲) این است که اگر d مربع کامل نباشد آنگاه $(\frac{d}{\cdot})$، و از این‌رو $(\frac{\cdot}{G})$، نابدیهی است. بنابراین قضیهٔ ۱ اثبات می‌شود.

اکنون فرض کنید مرتبهٔ G عددی فرد است. برنساید ([۱]، بخش ۲۲۲، ص.۲۹۴) خاطرنشان کرد که C_1 تنها ردهٔ مزدوجی حقیقی است. برای ملاحظهٔ این مطلب، فرض کنید g در یک ردهٔ مزدوجی حقیقی است. بنابراین، در حالت خاص به‌ازای hای داریم $h^{-1}gh = g^{-1}$. در نتیجه، $h^{-2}gh^2 = g$ که ثابت می‌کند h^2 در $C_G(g)$ واقع است. چون n فرد است، مرتبهٔ h نیز فرد، مثلاً $2\ell + 1$، است. در نتیجه $h = (h^2)^{\ell+1}$ که از آن نتیجه می‌شود

h متعلق به $C_G(g)$ است. بنابراین، $g = g^{-1}$. چون مرتبهٔ g فرد فرض شده است، پس $g = 1$.

چون $r_1 = 1$، از (۵) به وضوح نتیجه می‌شود که $d = (-1)^{\frac{m-1}{2}} n$. بنا به قسمت اول قضیهٔ ۱ باید داشته باشیم:

$$d = (-1)^{\frac{n-1}{2}} n = n^*$$

زیرا n فرد است.[۱] آخرین قسمت نتیجهٔ ۱، از قضیهٔ ۱ به‌دست می‌آید زیرا هنگامی که n فرد است n^* مربع کامل است اگر و تنها اگر n مربع کامل باشد.

۵. چند مثال

مبین چند گروه از مرتبهٔ زوج را پیدا می‌کنیم. ابتدا فرض کنید که G آبلی است و زیرگروه G متشکل از ۱ و عناصر مرتبهٔ ۲، دارای مرتبهٔ 2^t است. در این صورت $r_1 = 2^t$، لذا

$$d = (-1)^{\frac{n-2^t}{2}} n^{2^t}.$$

نتیجه می‌گیریم که برای گروه آبلی G از مرتبهٔ زوج n، نماد $\left(\frac{\cdot}{G}\right)$ نابدیهی است اگر و تنها اگر $4|n$ و $t = 1$، که در این حالت داریم

$$\left(\frac{a}{G}\right) = (-1)^{\frac{a-1}{2}}$$

که در آن $(a, n) = 1$. شرط $t = 1$ مثلاً در حالتی که G دوری باشد، برقرار است.

در حالت کلی، اگر سرشتهای G گویا باشند، آنگاه به‌سادگی از (۱۲) نتیجه می‌شود که $\left(\frac{\cdot}{G}\right)$ سرشت بدیهی است و از این رو d مربع کامل است. این مطلب در حالت خاصی که $G = S_k$ گروه متقارن باشد نیز برقرار است که در این حالت می‌توان d را به‌طور صریح محاسبه کرد.

از طرف دیگر، به‌آسانی می‌توان گروههایی ناآبلی به دست آورد که فقط سرشتهای حقیقی و نماد مربعی نابدیهی داشته باشند. به‌عنوان مثال، خانوادهٔ گروههای ساده $G_r = \mathrm{SL}(2, \mathbb{F}_q)$، $q = 2^r$، $r > 1$، را در نظر بگیرید (یعنی گروه ماتریسهای 2×2 با دترمینان ۱ و درایه‌های متعلق به میدان $\mathbb{F}_q$ از مرتبهٔ q). بنا به ([۱۱])، ص. ۱۳۴) داریم $n = q(q^2 - 1)$، $m = r_1 = q + 1$، و

$$d = q^2(q+1)(q^2-1)^{\frac{q}{4}}$$

که مربع کامل است اگر و تنها اگر $r = 3$. گزارهٔ اخیر از آنجا ناشی می‌شود که اگر $q + 1 = x^2$، آنگاه $2^r = x^2 - 1 = (x-1)(x+1)$. بنابراین $x = 2\ell + 1$ و لذا $2^{r-2} = \ell(\ell+1)$ که از آن نتیجه می‌شود $r = 3$. اگر $r = 2$، آنگاه $G_2 = A_5$ و

$$\left(\frac{a}{A_5}\right) = \left(\frac{5}{a}\right).$$

اگر $r = 16$، آنگاه

$$\left(\frac{a}{G_{16}}\right) = \left(\frac{65537}{a}\right)$$

که $65537 = 2^{16} + 1$ یک عدد اول است.

۱. نتیجهٔ قوی‌تری که برنساید کشف کرد ([۱]، ص. ۲۹۵) چنین است: $n \equiv m \pmod{16}$.

مراجع

1. W. Burnside, *Theory of Groups of Finite Order*, 2nd ed., Cambridge University Press, Cambridge, 1911.
2. C. W. Curtis, *Pioneers of Representation Theory: Frobenius, Burnside, Schur and Brauer*, American Mathematical Society, Providence, 1999.
3. F. G. Frobenius, Über Beziehungen zwischen den Primidealen eines algebraischen Körpers und den Substitutionen seiner Gruppe, *S'ber. Akad. Wiss. Berlin* (1896) 689-703; also in *Gesammelte Abhandlungen*, vol. 2, Springer-Verlag, Berlin, 1968, pp. 719-733.
4. ——, Über Gruppencharaktere, *S'ber. Akad. Wiss. Berlin* (1896) 985-1021; also in *Gesammelte Abhandlungen*, vol. 3, Springer-Verlag, Berlin, 1968, pp. 1-37.
5. C. F. Gauss, Theorematis fundamentalis in doctrina de residuis quadraticus demonstrationes et ampliationes novæ, 1818; also in *Werke*, vol. 2, pp. 47-64.
6. G. G. James and M. Liebeck, *Representations and Characters of Groups*, 2nd ed., Cambridge University Press, New York, 2001.
7. S. Y. Kim, An elementary proof of the quadratic reciprocity law, this MONTHLY **111** (2004) 48-50.
8. F. Lemmermeyer, *Reciprocity Laws. From Euler to Eisenstein*, Springer-Verlag, Berlin, 2000.
9. H. E. Rose, *Course in Number Theory*, 2nd ed., Clarendon Press, Oxford, 1996.
10. P. Samuel, *Algebraic Theory of Numbers* (trans. A. J. Silberger), Houghton Mifflin, Boston, 1970.
11. I. Schur, Untersuchungen über die Darstellung der endliche Gruppen durch gebrochene lineare Substitutionen, *J. Reine Angewant. Math.* **132** (1907) 85-137; also in *Gesammelte Abhandlungen*, vol. 1, Springer-Verlag, Berlin, 1973, pp. 198-250.
12. ——, Elementarer Beweis eines Satzes von L. Stickelberger, *Math. Zeit.* **29** (1928) 464-465; also in *Gesammelte Abhandlungen*, vol. 3, Springer-Verlag, Berlin, 1973, pp. 87-88.
13. G. Zolotarev, Nouvelle démonstration de la loi de réciprocité de Legendre, *Nouvelles Ann. Math.* (2) **11** (1872) 354-362.

* * * * * *

- William Duke and Kimberly Hopkins, "Quadratic reciprocity in a finite group", *Amer. Math. Monthly*, (3) **112** (2005) 251-256.

* ویلیام دوک، دانشگاه کالیفرنیا در لُس آنجلس، آمریکا

duke@math.ucla.edu

** کیمبرلی هاپکینز، دانشگاه تگزاس در آستین، آمریکا

khopkins@math.utexas.edu