فرهنگ و اندیشهٔ ریاضی
سال ۴۱، شمارهٔ ۷۱ (پاییز و زمستان ۱۴۰۱) صص. ۶۳ تا ۷۲

اثباتی برای قانون تقابل مربعی گاوس

محمدرضا درفشه

چکیده. قانون تقابل مربعی گاوسی یکی از مهم‌ترین قضیه‌های نظریهٔ اعداد است که گاوس آن را در نوزده سالگی ثابت کرد. در این مقاله، ابتدا مطالبی دربارهٔ سرشت گروه‌های آبلی متناهی ثابت می‌کنیم و سپس با استفاده از آن‌ها اثباتی برای قانون تقابل مربعی گاوس عرضه می‌کنیم.

۱ مقدمه

فرض کنید p یک عدد اول فرد باشد و $a \in \mathbb{Z}$ چنان باشد که $(a,p) = ۱$. گوییم a یک ماندهٔ درجهٔ دوم به پیمانهٔ p است اگر هم‌نهشتی $x^۲ \equiv a \pmod p$ دارای جواب باشد، درغیراین‌صورت گفته می‌شود a یک ماندهٔ درجهٔ دوم به پیمانهٔ p نیست. از نماد لُژاندر[1]، یعنی $(\frac{a}{p})$، برای نشان دادن اینکه a ماندهٔ درجهٔ دوم است یا نه استفاده می‌شود: می‌نویسیم $(\frac{a}{p}) = ۱$ اگر a ماندهٔ درجهٔ دوم به پیمانهٔ p باشد و درغیراین‌صورت $(\frac{a}{p}) = -۱$.

قانون تقابل مربعی گاوس[2] بیان می‌دارد که اگر p و q اعداد اول فرد متمایز باشند آنگاه

$$(\frac{p}{q})(\frac{q}{p}) = (-۱)^{\frac{(p-۱)(q-۱)}{۴}}.$$

این تساوی را ابتدا اویلر بیان کرد و سپس لژاندر آن را مورد بحث قرار داد و ادعا کرد این تساوی را ثابت کرده است. اما اولین اثبات این قانون را گاوس در [۴] ارائه کرد در حالی که فقط نوزده سال

عبارات و کلمات کلیدی: قانون تقابل مربعی گاوس، سرشت گروه متناهی، نماد لژاندر
نوع مقاله: پژوهشی؛ تاریخ دریافت: ۱۴۰۰/۷/۶؛ تاریخ پذیرش: ۱۴۰۱/۲/۲۰

[1] Legendre [2] Gauss's quadratic reciprocity law

doi: 10.30504/mct.2023.1239.1863

داشت. اما گاوس آن‌چنان به این نتیجه علاقه‌مند گردید که در طول زندگی‌اش شش اثبات متفاوت برای این قضیه پیدا کرد که در [۵] به چاپ رسیده است.

تاکنون اثبات‌های متعددی برای قانون تقابل مربعی پیدا شده است که تعدادشان به بیش از یک‌صدوپنجاه عدد می‌رسد و هیچ‌یک بدیهی به نظر نمی‌رسند ولی برخی از آن‌ها اشتراکاتی با هم دارند. اثبات‌های مقدماتی درکتاب‌های [۶، ۸] و مقاله‌های [۳، ۷] موجود است. در [۲] اثبات‌های متعدد قانون تقابل مربعی گاوس، از جمله اثبات‌های خود گاوس، گردآوری شده است. در این مقاله اثبات دیگری از این قضیه را با استفاده از نظریهٔ سرشت گروه‌های آبلی متناهی ارائه می‌دهیم.

۲ سرشت‌های گروه آبلی متناهی

با تعریف زیر این بخش را آغاز می‌کنیم.

تعریف ۱.۲. فرض کنید A یک گروه آبلی متناهی باشد. یک سرشت A روی میدان F عبارت است از هم‌ریختی $\chi : A \longrightarrow F^\times$ که در آن $F^\times$ گروه ضربی میدان F است.

بنابراین برای هر $a, b \in A$ داریم $\chi(a+b) = \chi(a)\chi(b)$؛ قانون ترکیب در A را جمعی و عضو خنثی را 0 درنظر می‌گیریم. به‌این‌ترتیب خواهیم داشت $\chi(0) = 1$ و $\chi(-a) = \chi(a)^{-1}$. سرشت بدیهی A هم‌ریختی $\chi : A \longrightarrow F^\times$ است با ضابطهٔ $\chi(a) = 1$ برای هر $a \in A$. درحالتی‌که $F = \mathbb{C}$، χ را یک سرشت معمولی گروه A می‌نامیم و درحالتی‌که $|A| \mid \mathrm{char}(F)$، سرشت χ را پیمانه‌ای می‌نامیم که در آن $\mathrm{char}(F)$ مشخصهٔ میدان F است.

اگر $|A| = n$ فرض شود آنگاه برای هر $a \in A$ داریم $na = 0$. پس اگر χ سرشتی از A باشد، داریم

$$\chi(na) = \chi(a)^n = \chi(a) = 1$$

یعنی $\chi(a)$ ریشهٔ nام واحد است. بنابراین، در تعریف χ فرض می‌کنیم میدان F شامل ریشه‌های nام واحد است. اگر χ سرشتی از A باشد آنگاه $\overline{\chi} : A \longrightarrow F^\times$ با ضابطه $\overline{\chi}(a) = \chi(-a)$، برای هر $a \in A$، نیز یک سرشت از A است.

گزاره ۲.۲. فرض کنید A یک گروه آبلی متناهی و χ و φ سرشت‌هایی از آن باشند. دراین‌صورت

(الف)

$$\sum_{x\in A}\chi(x)\overline{\varphi}(x)=\begin{cases}|A| & \chi=\varphi\\ ۰ & \chi\neq\varphi\end{cases}$$

(ب)

$$\sum_{x\in A}\chi(x)=\begin{cases}|A| & \text{اگر } \chi \text{ سرشت بدیهی باشد}\\ ۰ & \text{درغیراین‌صورت}\end{cases}$$

اثبات. برای اثبات قسمت اول (الف)، ابتدا توجه کنید که اگر $\chi=\varphi$ آنگاه به‌ازای هر $x\in A$ برابری $\chi(x)\overline{\varphi}(x)=\chi(x)\chi(-x)=۱$ برقرار است. همچنین اگر فرض کنیم $\chi\neq\varphi$ و $y\in A$ عضوی باشد که $\chi(y)\varphi(-y)\neq ۱$، دراین‌صورت

$$\chi(y)\varphi(-y)\sum_{x\in A}\chi(x)\varphi(-x)=\sum_{x\in A}\chi(xy)\varphi(-xy)=\sum_{x\in A}\chi(x)\varphi(-x),$$

درنتیجه

$$(\chi(y)\varphi(-y)-۱)\sum_{x\in A}\chi(x)\varphi(-x)=۰$$

که از آن $\sum_{x\in A}\chi(x)\varphi(-x)=۰$ حاصل می‌گردد و به‌این‌ترتیب (الف) ثابت می‌شود.

برای اثبات قسمت (ب) کافی است φ را سرشت بدیهی درنظر بگیریم و از (الف) استفاده کنیم. □

تعریف ۳.۲. فرض کنید p یک عدد اول فرد، F یک میدان، $\chi:\mathbb{Z}_p\longrightarrow F^\times$ سرشتی از گروه جمعی $\mathbb{Z}_p$، و $\varphi:\mathbb{Z}_p^\times\longrightarrow F^\times$ سرشتی از گروه ضربی $\mathbb{Z}_p^\times$ باشد. دراین‌صورت عبارت

$$G=G(\chi,\varphi)=\sum_{x\in\mathbb{Z}_p^\times}\chi(x)\varphi(x)$$

را یک مجموع گاوسی وابسته به $\mathbb{Z}_p$ می‌نامند.

مشاهده می‌کنیم که G عضوی از میدان F است و در حالتی‌که $F=\mathbb{C}$، آن‌وقت G عددی مختلط است. همچنین با توجه به تعریف G می‌توان تعریف کرد

$$\overline{G}=\sum_{x\in\mathbb{Z}_p^\times}\chi(-x)\varphi(x^{-۱}).$$

گزاره ۴.۲. اگر χ و φ سرشت‌های نابدیهی باشند آنگاه $G\,.\,\overline{G} = p$.

اثبات. باتوجه به تعریف χ و φ می‌توان نوشت

$$\begin{aligned} G\,.\,\overline{G} &= \sum_{u,t\in\mathbb{Z}_p^\times} \chi(t)\chi(-u)\varphi(t)\varphi(u^{-1}) \\ &= \sum_{u,t\in\mathbb{Z}_p^\times} \chi(t-u)\varphi(tu^{-1}) = \sum_{x\neq 0}\varphi(x)\sum_{u\neq 0}\chi(u(x-1)). \end{aligned}$$

با استفاده از گزارهٔ ۲.۲ داریم $\sum_{x\neq 0}\chi(x) = -1$ و $\sum_{y\neq 0,1}\varphi(y) = -1$. درنتیجه

$$G\,.\,\overline{G} = p-1+\sum_{x\neq 0,1}\varphi(x)\sum_{u\neq 0}\chi(u(x-1)) = p-1-\sum_{x\neq 0,1}\varphi(x) = p.$$

□

فرض کنید p یک عدد اول فرد و F میدانی باشد که مشخصهٔ آن p نیست ولی شامل ریشه‌های pام واحد است. تابع $\chi : \mathbb{Z}_p^\times \longrightarrow F^\times$ با ضابطهٔ $\chi(a) = (\frac{a}{p})$ به‌ازای هر $a \in \mathbb{Z}_p^\times$، یک سرشت $\mathbb{Z}_p^\times$ است، زیرا بنابه خواص مقدماتی نماد لژاندر داریم

$$(\frac{ab}{p}) = (\frac{a}{p})(\frac{b}{p}).$$

اگر ξ یک ریشهٔ pام اولیهٔ واحد در F باشد، تابع $\varphi : \mathbb{Z}_p \longrightarrow F^\times$ با ضابطهٔ $\varphi(a) = \xi^a$، $a \in \mathbb{Z}_p$، یک سرشت برای گروه جمعی $\mathbb{Z}_p$ است. بنابراین، نسبت به χ و φ، داریم

$$G(\chi,\varphi) = \sum_{a\in\mathbb{Z}_p^\times}(\frac{a}{p})\xi^a.$$

مجموع گاوسی کلاسیک درحالتی‌که $F = \mathbb{C}$ عددی مختلط است و چنین تعریف می‌شود

$$G_p = \sum_{a=1}^{p-1}(\frac{a}{p})\xi^a.$$

فرض کنید p یک عدد اول فرد و ξ یک ریشهٔ pام اولیهٔ واحد در $\mathbb{C}$ باشد. از جبر مقدماتی می‌دانیم چندجمله‌ای مینیمال ξ عبارت است از $\frac{x^p-1}{x-1} = x^{p-1}+x^{p-2}+\cdots+x+1$ و

درنتیجه

$$\xi^{p-1} + \xi^{p-2} + \cdots + \xi + 1 = 0.$$

اگر تعریف کنیم

$$\mathbb{Z}[\xi] = \left\{ \sum_{i=0}^{p-2} a_i \xi^i : a_i \in \mathbb{Z} \right\}$$

آنگاه دیده می‌شود که $\mathbb{Z}[\xi]$ تحت جمع و ضرب بسته است و لذا دارای ساختار حلقه است. توجه کنید که تمام توان‌های ξ^k را می‌توان برحسب ترکیبات عناصر مجموعهٔ $\{1, \xi, \ldots, \xi^{p-2}\}$ با ضرایب در $\mathbb{Z}$ نوشت.

گزاره ۵.۲. $\mathbb{Z}[\xi] \cap \mathbb{Q} = \mathbb{Z}$.

اثبات. روشن است که $\mathbb{Z} \subseteq \mathbb{Z}[\xi] \cap \mathbb{Q}$. اکنون فرض کنید $\alpha \in \mathbb{Z}[\xi] \cap \mathbb{Q}$ آنگاه $\alpha = \sum_{i=0}^{p-2} a_i \xi^i$ که در آن $a_i \in \mathbb{Z}$ به‌ازای $1 \leq i \leq p-2$. پس $\sum_{i=0}^{p-2} a_i \xi^i - \alpha = 0$ و درنتیجه ξ ریشه‌ای از چندجمله‌ای $\sum_{i=0}^{p-2} a_i x^i - \alpha = 0$ است که ضرایبش همگی در $\mathbb{Q}$اند. چون درجهٔ چندجمله‌ای مینیمال ξ مساوی $p-1$ است، نتیجه می‌شود که $a_0 - \alpha = 0$ و لذا $\alpha \in \mathbb{Z}$. □

گزاره ۶.۲. فرض کنید q یک عدد اول فرد است. برای $\alpha_i \in \mathbb{Z}[\xi]$، که $1 \leq i \leq k$، داریم

$$\left(\sum_{i=1}^{k} \alpha_i \right)^q \equiv \sum_{i=1}^{k} \alpha_i^q \pmod{q}.$$

اثبات. با استفاده از بسط چندجمله‌ای داریم

$$\left(\sum_{i=1}^{k} \alpha_i \right)^q = \sum_{i_1 + \cdots + i_k = q} \frac{q!}{i_1! \cdots i_k!} \alpha_1^{i_1} \cdots \alpha_k^{i_k}.$$

مشاهده می‌کنیم که همهٔ ضرایب مضرب qاند، به‌جز آن‌هایی که فقط یک اندیس i_j مساوی q دارند، و بقیهٔ اندیس‌ها نیز مساوی صفرند. به‌این‌ترتیب گزاره ثابت می‌شود. □

گزاره ۷.۲ (معیار اویلر). اگر p یک عدد اول فرد باشد آنگاه $\left(\frac{a}{p}\right) = 1$ اگر و تنها اگر $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$. یا به‌طورمعادل $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$؛

اثبات. مجموعهٔ مربعات عناصر ناصفر در $\mathbb{Z}_p$ را A می‌نامیم که $(p-1)/2$ عنصر دارد. می‌توان نشان داد که مجموعهٔ B مرکب از جواب‌های متمایز معادلهٔ

$$x^{\frac{p-1}{2}} \equiv 1 \pmod{p}$$

نیز $(p-1)/2$ عضو دارد. ادعا می‌کنیم $A = B$. زیرا اگر $a \in A$ آنگاه عضو $b \in B$ وجود دارد که $b^2 \equiv a \pmod{p}$ و بنابه قضیهٔ فرما

$$b^{p-1} \equiv a^{\frac{p-1}{2}} \equiv 1 \pmod{p}.$$

درنتیجه a جوابی برای معادلهٔ $x^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ است، پس $a \in B$. ازاین‌رو $A \subseteq B$، که چون هر دو مجموعه یک تعداد عضو دارند نتیجه می‌گیریم که $A = B$ و حکم ثابت می‌شود. □

۳ قانون تقابل مربعی گاوس

حکم قانون تقابل مربعی گاوس از این قرار است.

قضیه ۱.۳. اگر p و q اعداد اول فرد متمایز باشند آنگاه

$$(\frac{p}{q})(\frac{q}{p}) = (-1)^{\frac{(p-1)(q-1)}{4}}.$$

برای اثبات نیاز به لم زیر داریم.

گزاره ۲.۳. $G_p^2 = (-1)^{\frac{p-1}{2}} p$.

اثبات. با توجه به تعریف G_p، می‌توان $\overline{G_p}$ را به‌صورت زیر محاسبه کرد

$$\overline{G_p} = \sum_{a=1}^{p-1} (\frac{-a}{p}) \xi^{-a} = (\frac{-1}{p}) \sum_{a=1}^{p-1} (\frac{a}{p}) \xi^{-a} = (\frac{-1}{p}) G_p.$$

از گزارهٔ ۷.۲ نتیجه می‌شود که $(\frac{-1}{p}) = (-1)^{\frac{p-1}{2}}$ و درنتیجه $\overline{G_p} = (-1)^{\frac{p-1}{2}} G_p$. اکنون با استفاده از گزارهٔ ۴.۲ می‌توان نوشت

$$G_p \overline{G_p} = (-1)^{\frac{p-1}{2}} G_p^2 = p;$$

به‌این‌ترتیب گزاره ثابت می‌شود. □

اثبات قضیهٔ ۱.۳. می‌دانیم $G_p = \sum_{a=1}^{p-1}(\frac{a}{p})\xi^a$ که در آن ξ یک ریشهٔ pام واحد است. با استفاده از گزارهٔ ۶.۲ می‌توان نوشت

$$G_p^q \equiv \sum_{a=1}^{p-1}(\frac{a}{p})^q\xi^{aq} \equiv \sum_{a=1}^{p-1}(\frac{a}{p})\xi^{aq} \pmod q.$$

به‌این‌ترتیب

$$\sum_{a=1}^{p-1}(\frac{a}{p})\xi^{aq} = \sum_{a=1}^{p-1}(\frac{aq}{p})(\frac{q}{p})\xi^{aq} = (\frac{q}{p})G_p.$$

لذا خواهیم داشت $G_p^q \equiv (\frac{q}{p})G_p \pmod q$. اما از گزاره‌های ۷.۲ و ۲.۳ نتیجه می‌شود که

$$G_p^{q-1} = (-1)^{\frac{(p-1)(q-1)}{4}}p^{\frac{q-1}{2}} = (-1)^{\frac{(p-1)(q-1)}{4}}(\frac{p}{q}).$$

درنتیجه

$$G_p^q = (-1)^{\frac{(p-1)(q-1)}{4}}(\frac{p}{q})G_p = (\frac{q}{p})G_p$$

با حذف G_p از دو طرف تساوی اخیر داریم

$$(-1)^{\frac{(p-1)(q-1)}{4}}(\frac{p}{q}) = (\frac{q}{p}).$$

اگر دو طرف این تساوی را در $(\frac{p}{q})$ ضرب کنیم، قانون تقابل مربعی گاوس به‌دست می‌آید. □

۴ حالتی که مقدار سرشت، عدد مختلط نیست

مجموع گاوسی G_p، که در بخش ۲ تعریف شد، عددی مختلط است، زیرا سرشت‌ها روی میدان مختلط تعریف می‌شوند. اما می‌توان سرشت‌ها را پیمانه‌ای فرض کرد و مجموع گاوسی را به‌طور مشابه تعریف و سپس قانون تقابل مربعی را اثبات کرد.

تعریف ۱.۴. فرض کنید p یک عدد اول فرد و F یک میدان باشد. همچنین، فرض کنید $\mathrm{char}(F) \neq p$ و F شامل ریشه‌های pام واحد باشد. هرگاه $\xi \in F$ یک ریشهٔ اولیه واحد

باشد مجموع گاوسی روی F را چنین تعریف می‌کنند

$$S_p = \sum_{a=۱}^{p-۱} (\frac{a}{p})\xi^a.$$

در تعریف بالا S_p عضوی از میدان F است. اتحادی که در گزارهٔ ۲.۳ نوشتیم در مورد S_p نیز برقرار است و اثباتی متفاوت دارد.

گزاره ۲.۴. $S_p^۲ = (-۱)^{\frac{p-۱}{۲}} p$.

اثبات. باتوجه به تعریف S_p داریم

$$S_p^۲ = \sum_{a,b=۱}^{p-۱} (\frac{ab}{p})\xi^{a+b}$$

اگربنویسیم $b \equiv ac \pmod p$ آنگاه تساوی بالا به‌صورت زیر در می‌آید

$$S_p^۲ = \sum_{a=۱}^{p-۱}\sum_{c=۱}^{p-۱} (\frac{a^۲c}{p})\xi^{a+ac} = \sum_{c=۱}^{p-۱} \left(\sum_{a=۱}^{p-۱} \xi^{a(۱+c)}\right) (\frac{c}{p});$$

زیرا $(\frac{a^۲}{p}) = ۱$.

اگر $۱ + c \equiv ۰ \pmod p$، یعنی $c = p - ۱$، آنگاه $\xi^{a(۱+c)} = ۱$، و لذا

$$S_p^۲ = \sum_{c=۱}^{p-۱} (p-۱)(\frac{c}{p}) = (p-۱)(\frac{p-۱}{p}) = (p-۱)(\frac{-۱}{p}).$$

و اگر $۱ + c \not\equiv ۰ \pmod p$ آنگاه اعداد $\xi^{۱+c}$،...، $\xi^{(p-۱)(۱+c)}$ همهٔ pتا ریشهٔ متمایز چندجمله‌ای $x^p - ۱$اند و درنتیجه $\sum_{a=۰}^{p-۱} \xi^{a(۱+c)} = ۰$. پس با استفاده از گزارهٔ ۷.۲ داریم

$$S_p^۲ = (p-۱)(\frac{-۱}{p}) - \sum_{c=۱}^{p-۲} (\frac{c}{p}) = p(\frac{-۱}{p}) = p(-۱)^{\frac{p-۱}{۲}}.$$

□

حالا با استفاده از S_p اثباتی برای قانون تقابل مربعی گاوس می‌آوریم. فرض می‌کنیم مشخصهٔ

میدان F مساوی q است.

اثبات قضیهٔ ۱.۳. با استفاده از گزارهٔ ۲.۴ می‌توان نوشت

$$S_p^{q-1} = (-1)^{\frac{(p-1)(q-1)}{4}} p^{\frac{q-1}{2}} = (-1)^{\frac{(p-1)(q-1)}{4}} (\frac{p}{q}).$$

بنابراین

$$S_p^q = (-1)^{\frac{(p-1)(q-1)}{4}} (\frac{p}{q}) S_p.$$

با استفاده از بسط چندجمله‌ای، اتحاد معروفِ دانشجوی سال اول[1]، و اینکه $\mathrm{char}(F) = q$ خواهیم داشت

$$S_p^q = \sum_{a=1}^{p-1} (\frac{a}{p})^q \xi^{aq} = \sum_{a=1}^{p-1} (\frac{a}{p}) \xi^{aq}.$$

می‌نویسیم $c \equiv aq \pmod p$ و توجه می‌کنیم که $(\frac{q^{-1}}{p}) = (\frac{q}{p})$ پس داریم

$$S_p^q = \sum_{c=1}^{p-1} (\frac{q^{-1}c}{p}) \xi^c = \sum_{c=1}^{p-1} (\frac{q}{p})(\frac{c}{p}) \xi^c = (\frac{q}{p}) S_p.$$

اکنون دو عبارت برای S_p^q به دست آوردیم:

$$(-1)^{\frac{(p-1)(q-1)}{4}} (\frac{p}{q}) S_p = (\frac{q}{p}) S_p.$$

اگر $S_p \neq 0$ را از دو طرف تساوی بالا حذف کنیم و سپس در $(\frac{p}{q})$ ضرب کنیم، آنگاه

$$(\frac{p}{q})(\frac{q}{p}) = (-1)^{\frac{(p-1)(q-1)}{4}}.$$

□

مراجع

[۱] دوک، ویلیام؛ هاپکینز، کیمبرلی، تقابل مربعی در یک گروه متناهی، ترجمهٔ محمدرضا درفشه، نشر ریاضی، شمارهٔ ۳۵ (۱۳۹۰)، ۷-۱۰.

[1] freshman's dream

[2] Baumgurt, O., *The Quadratic Reciprocity Law; A Collection of Classical Proofs* (ed. and trans. F. Lemmermeyer), Birkhäuser, Cham, 2015.
[3] Brown, E., The first proof of the quadratic reciprocity law revisited, *Amer. Math. Monthly*, **44** (1981), 257-264.
[4] Gauss, C. F., *Disquisitiones Arithmetica*, Werke, Vol. I, Leipzig, 1801; English translation by A. A. Clarke, Yale University Press, New Haven, 1966.
[5] Gauss, C. F., Theorematis fundamentalis in doctrina de residuis quadraticis demonstrationes et ampliationes novae, in *Werke*, Vol. II, 1818, 47-64.
[6] Niven, I., Zuckerman, H. S., *An Introduction to the Theory of Numbers*, 2nd ed., John Wiley and Sons, New York, 1960.
[7] Rousseau, G., On the quadratic reciprocity law, *J. Aust. Math. Soc.*, **51** (1991), 423-425.
[8] Serre, J. P., *A Course in Arithmetic*, Springer, Berlin, 1979.

محمدرضا درفشه: دانشگاه تهران، دانشکدهٔ ریاضی، آمار و علوم کامپیوتر
رایانامه: darafsheh@ut.ac.ir

Farhang va Andishe-ye Riyazi
Volume 41, Number 71, Fall/Winter 2022, Pages 63–72
doi: 10.30504/mct.2023.1239.1863

A Proof of the Gauss Quadratic Reciprocity Law

M. R. Darafsheh[1]

School of Mathematics, Statistics and Computer Science, University of Tehran, Iran

Abstract. The Gauss quadratic reciprocity law is one of the most important theorems in number theory which Gauss proved it in nineteen years old. In this paper, we first prove some facts about the character of finite abelian groups. Then, using them, we provide a proof for the Gauss quadratic reciprocity law.

Keywords: the law of quadratic reciprocity, character on finite group, Legendre symbol
Article history: Recieved 28 September 2021; Accepted 10 May 2022

[1]darafsheh@ut.ac.ir

ISSN 1022-6443/