مجله‌ی ریاضی شریف
دوره‌ی سوم، شماره‌ی اول (بهار ۱۴۰۲)

جمع‌های گاوسی، از تقابل مربعی تا حدسیات ویل

علیرضا شاولی *

چکیده. در این مقاله درباره‌ی جمع‌های گاوسی و جمع‌های ژاکوبی و کاربردهای مختلف آن‌ها صحبت می‌شود. ابتدا با کمک این مجموع‌ها قانون تقابل مربعی را ثابت می‌کنیم و به قانون‌های تقابل درجات بالاتر نیز اشاره خواهیم کرد. سپس تعداد جواب‌های برخی معادلات چندجمله‌ای روی میدان‌های متناهی را تخمین می‌زنیم. پس از آن تابع زتای یک خم جبری تصویری روی یک میدان متناهی را معرفی کرده و حدس‌های آرتین در مورد این تابع را مطرح می‌کنیم. نهایتاً صورت حدسیات ویل را به عنوان تعمیم حدس‌های آرتین بیان خواهیم کرد.

۱. مقدمه

کارل فردریش گاوس [1] ریاضی‌دان شهیر آلمانی، در طول عمر خود دست‌کم شش اثبات مختلف از قانون تقابل درجه‌ی دوم ارائه کرد. یکی از دلایل گاوس برای ارائه‌ی اثبات‌های مختلف، پیدا کردن اثباتی بود که بتواند برای یافتن تقابل‌هایی از درجات بالاتر نیز استفاده شود. گاوس در ۱۸۱۸ میلادی، ششمین اثبات خود را منتشر کرد و عقیده داشت این اثبات قابل تعمیم برای یافتن تقابل‌هایی از درجات بالاتر نیز هست. این اثبات مبتنی بر مطالعه‌ی مجموع‌هایی بود که اکنون جمع‌های گاوسی [2] نامیده می‌شود. در اواسط قرن ۱۹، آیزنشتاین [3] و ژاکوبی [4] با استفاده از ایده‌های گاوس تقابل‌هایی از درجه‌ی سوم و چهارم را ثابت کردند. مجموع‌های گاوسی کاربردهای دیگری نیز در نظریه اعداد دارند که یکی از آن‌ها یافتن تعداد جواب‌های معادلات چندجمله‌ای به پیمانه‌ی یک عدد اول (و یا به طور کلی‌تر روی یک میدان متناهی) است که با کارهای افراد مختلفی از جمله امیل آرتین [5] و آندره ویل [6] در نیمه‌ی اول قرن بیستم، منجر به حدسیات مشهور ویل شد. این حدسیات سهم بسیار مهمی در جهت‌دهی به هندسه‌ی جبری مدرن در قرن بیستم داشتند.

۲. پیش‌نیازها

در این مقاله فرض شده است خواننده با نظریه اعداد و جبر مجرد در حد مقدماتی آشنایی دارد. برخی پیش‌نیازهایی که احتمال می‌رود برخی خوانندگان با آن آشنا نباشند، در حد بسیار مختصر در این بخش توضیح داده خواهند شد. خواننده برای مطالعه‌ی دقیق‌تر این مباحث می‌تواند به منابع معرفی‌شده در هر بخش مراجعه کند.

۱.۲. مانده و نامانده‌ی مربعی.

تعریف ۱.۲. فرض کنید p عددی اول و a عددی صحیح است و $p \nmid a$. گوییم a به پیمانه‌ی p یک مانده‌ی مربعی یا مانده‌ی درجه دوم است هرگاه عددی صحیح مانند x یافت شود که $x^2 \equiv a \pmod p$.

[1] Carl Friedrich Gauss
[2] Gauss sums
[3] Gotthold Eisenstein
[4] Carl Gustav Jacob Jacobi
[5] Emil Artin
[6] André Weil

برای راحتی مانده یا نامانده بودن به پیمانه‌ی یک عدد اول را با نماد لژاندر[1] نشان می‌دهند که به صورت زیر تعریف می‌شود:

$$\left(\frac{a}{p}\right)=\begin{cases}+۱ & a \text{ مانده مربعی} \\ -۱ & a \text{ نامانده مربعی} \\ ۰ & p \mid a\end{cases}$$

فرض کنید عدد اول p فرد باشد. حال دقت کنید که به روشنی همه‌ی اعداد $۱^۲, ۲^۲, \ldots, (\frac{p-۱}{۲})^۲$ مانده‌ی مربعی هستند. از طرفی هر مانده‌ی مربعی به پیمانه p با یکی از این اعداد هم‌نهشت است. (چرا؟) به علاوه اعداد فوق دوبه‌دو باقی‌مانده‌های متفاوتی بر p دارند. لذا دقیقاً $\frac{p-۱}{۲}$ تا از باقی‌مانده‌های مختلف بر p مانده‌ی مربعی هستند.

قضیه ۲.۲. (محک اویلر) اگر p عددی اول و فرد و a عددی صحیح باشد آنگاه

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-۱}{۲}} \pmod p.$$

اثبات. به مرجع [۲] مراجعه کنید. □

نتیجه ۳.۲. اگر a و b اعداد صحیح و p عددی اول باشد آنگاه

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

نتیجه ۴.۲. برای هر p اول و فرد، تابع $\chi:\left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^{\times} \to \{-۱,+۱\}$ با ضابطه‌ی $\chi(a)=\left(\frac{a}{p}\right)$ یک هم‌ریختی گروهی پوشا است.

از گزاره‌هایی که تا اینجا بیان کردیم نتیجه می‌شود اگر تجزیه‌ی عدد a به عوامل اول‌اش را به صورت $a=q_۱^{\alpha_۱}\ldots q_k^{\alpha_k}$ داشته باشیم آنگاه $\left(\frac{a}{p}\right)=\left(\frac{q_۱}{p}\right)^{\alpha_۱}\ldots\left(\frac{q_k}{p}\right)^{\alpha_k}$. لذا برای محاسبه $\left(\frac{a}{p}\right)$ کافی است برای p و q های اول، بتوانیم $\left(\frac{q}{p}\right)$ حساب کنیم. با کمک قانون تقابل مربعی ـ‌که در بخش‌های آینده درباره‌ی آن صحبت می‌کنیم‌ـ می‌توان الگوریتم ساده‌ای برای این کار ارائه کرد.

۲.۲. حلقه‌ی اعداد صحیح جبری.

تعریف ۵.۲. به یک عدد مختلط $\alpha \in \mathbb{C}$ جبری گوییم هرگاه ریشه‌ی یک چندجمله‌ای با ضرایب صحیح باشد. مثلاً $۱+\sqrt{۲}$ و $\frac{\sqrt[۳]{۲}}{۳}$ اعداد جبری هستند. (چرا؟)

تعریف ۶.۲. به یک عدد مختلط $\alpha \in \mathbb{C}$ صحیح جبری گوییم هرگاه ریشه‌ی یک چندجمله‌ای تکین با ضرایب صحیح باشد. مثلاً $۱+\sqrt{۲}$ یک عدد صحیح جبری است اما $\frac{\sqrt[۳]{۲}}{۳}$ صحیح جبری نیست. (چرا؟) مجموعه اعداد صحیح جبری را با نماد Ω نشان می‌دهیم.

قضیه ۷.۲. مجموعه‌ی اعداد جبری (با ضرب و جمع معمولی مختلط) یک میدان و مجموعه اعداد صحیح جبری یک زیرحلقه‌ی آن است.

اثبات. به مرجع [۲] مراجعه کنید. □

تعریف ۸.۲. گوییم عدد صحیح جبری a عدد صحیح جبری b را عاد می‌کند و می‌نویسیم $a \underset{\Omega}{\mid} b$، هرگاه عدد صحیح جبری c یافت شود که $ac=b$. مثلاً در Ω، $\sqrt{۶}$ بر $\sqrt{۲}$ بخش‌پذیر است.

تعریف ۹.۲. گوییم عدد صحیح جبری a با عدد صحیح جبری b به پیمانه‌ی m هم‌نهشت است و می‌نویسیم $a \underset{\Omega}{\equiv} b \pmod m$ هرگاه $m \underset{\Omega}{\mid} a-b$.

[1] Legendre symbol

لم ۱۰.۲. فرض کنید $P(x) = a_n x^n + \ldots + a_0$ یک چندجمله‌ای با ضرایب صحیح باشد و $\frac{p}{q}$، که p و q اعدادی صحیح و نسبت به هم اول هستند، ریشه‌ای گویا از آن باشد. آنگاه $q \mid a_n$.

اثبات لم فوق ساده است و آن را به عهده‌ی خواننده می‌گذاریم. نتیجه‌ی زیر فوراً از لم فوق حاصل می‌شود و در ادامه بسیار برای ما مفید خواهد بود.

نتیجه ۱۱.۲. اگر $a, b \in \mathbb{Z}$ و $a \underset{\Omega}{\mid} b$ آنگاه $a \underset{\mathbb{Z}}{\mid} b$.

لم ساده‌ی زیر که عیناً تعمیم لم مشابهی برای اعداد صحیح است، در آینده به کار خواهد آمد. برای اثبات آن کافی است از بسط دوجمله‌ای نیوتون استفاده کنید که آن را به خواننده واگذار می‌کنیم.

لم ۱۲.۲. برای عدد اول p و اعداد صحیح جبری a و b داریم

$$(a+b)^p \underset{\Omega}{\equiv} a^p + b^p \pmod{p}.$$

۳.۲. میدان‌های متناهی. ساده‌ترین مثال از یک میدان متناهی، میدان متناهی p عضوی برای یک p اول است که آن را با نماد $\mathbb{F}_p$ نشان می‌دهیم. البته میدان‌های متناهی دیگری نیز وجود دارند. در واقع برای هر p اول و k طبیعی، یک و تنها یک میدان p^k عضوی (در حد یک‌ریختی میدانی) وجود دارد. خواننده برای آشنایی مفصل با این میدان‌ها می‌تواند به هر کتاب مرجعی درباره نظریه‌ی میدان‌ها، مثلاً مرجع [۴]، رجوع کند.

۳. قانون تقابل مربعی

اولین بار اویلر[1] در قرن هجدهم میلادی صورت‌بندی دقیق قانون تقابل مربعی[2] را انجام داد. این قانون به طرز غیرمنتظره‌ای، برای p و q اول و فرد، داشتن یا نداشتن جواب برای معادله‌ی $x^2 \equiv p \pmod{q}$ را به داشتن یا نداشتن جواب برای معادله‌ی $x^2 \equiv q \pmod{p}$ مرتبط می‌سازد. این قضیه اولین بار توسط گاوس در سال ۱۷۹۶ میلادی به طور کامل ثابت شد. او این قضیه را یکی از زیباترین قضایای ریاضیات می‌دانست. همان طور که در مقدمه اشاره شد، گاوس اثبات‌های مختلفی برای این قضیه یافته‌بود. اثباتی که ما این جا می‌آوریم ساده‌شده‌ی آخرین اثبات گاوس از این قضیه است که در ۱۸۱۸ میلادی منتشر شد. قبل از این که صورت قانون تقابل مربعی را بیان و آن را ثابت کنیم، با استفاده از ایده‌ی آن اثبات، مقدار $\left(\frac{2}{p}\right)$ را برای p های اول حساب می‌کنیم.

قضیه ۱.۳. برای هر p اول و فرد داریم:

$$\left(\frac{2}{p}\right) = \begin{cases} +1 & p \equiv \pm 1 \pmod{8} \\ -1 & p \equiv \pm 3 \pmod{8} \end{cases}$$

اثبات. فرض کنید $\zeta = e^{\frac{2\pi i}{8}}$ یک ریشه هشتم واحد باشد. در این صورت به سادگی $\sqrt{2} = \zeta + \zeta^{-1}$. پس $2^{\frac{p-1}{2}} = (\zeta + \zeta^{-1})^{p-1}$. حال به یاد بیاورید $\left(\frac{2}{p}\right) \equiv 2^{\frac{p-1}{2}} \pmod{p}$. از طرفی دقت کنید اعداد ζ و ζ^{-1} اعداد صحیح جبری هستند. (چرا؟) پس

$$2^{\frac{p-1}{2}} \times (\zeta + \zeta^{-1}) = \left(\zeta + \zeta^{-1}\right)^p \underset{\Omega}{\equiv} \zeta^p + \zeta^{-p} \pmod{p}$$

حال چون ζ ریشه هشتم واحد بود، اگر $p \equiv \pm 1 \pmod{8}$ آن‌گاه $\zeta^p + \zeta^{-p} = \zeta + \zeta^{-1}$ و اگر $p \equiv \pm 3 \pmod{8}$ آن‌گاه $\zeta^p + \zeta^{-p} = -\left(\zeta + \zeta^{-1}\right)$ بنابراین اگر $p \equiv \pm 1 \pmod{8}$ آن‌گاه

$$2^{\frac{p-1}{2}} \times (\zeta + \zeta^{-1}) \underset{\Omega}{\equiv} \zeta + \zeta^{-1} \pmod{p}$$

و اگر $p \equiv \pm 3 \pmod{8}$ آن‌گاه

$$2^{\frac{p-1}{2}} \times (\zeta + \zeta^{-1}) \underset{\Omega}{\equiv} -\left(\zeta + \zeta^{-1}\right) \pmod{p}$$

[1] Leonhard Euler
[2] law of quadratic reciprocity

با یک استدلال ساده می‌توان نشان داد در حلقه‌ی Ω عدد p و $\zeta+\zeta^{-1}$ نسبت به هم اول اند و با ساده‌کردن $\zeta+\zeta^{-1}$ از دو طرف هم‌نهشتی‌ها و استفاده از نتیجه‌ی ۱۱.۲ و محک اویلر می‌توان حکم را ثابت کرد. ولی اینجا استدلال مقدماتی دیگری می‌آوریم.

با ضرب‌کردن هر یک از هم‌نهشتی‌های بالا در $(\zeta+\zeta^{-1})$ و توجه به این که $(\zeta+\zeta^{-1})^2=2$ داریم اگر $p\equiv\pm 1 \pmod 8$ آن‌گاه

$$2^{\frac{p-1}{2}}\times 2 \underset{\Omega}{\equiv} 2 \pmod p$$

و اگر $p\equiv\pm 3 \pmod 8$ آنگاه

$$2^{\frac{p-1}{2}}\times 2 \underset{\Omega}{\equiv} -2 \pmod p$$

حال چون دو طرف این هم‌نهشتی‌ها اعداد صحیح اند، طبق نتیجه‌ی ۱۱.۲ این هم‌نهشتی‌ها در $\mathbb{Z}$ هم برقرارند و لذا چون p فرد است با ساده کردن ۲ از دو طرف هم‌نهشتی‌ها حکم نتیجه می‌شود. $\square$

نکته‌ی کلیدی در اثبات بالا نمایش عدد $\sqrt{2}$ به شکل مجموع $\zeta+\zeta^{-1}$ بود که به محاسبه‌ی $2^{\frac{p-1}{2}}$ کمک کرد. اگر بتوانیم به جای عدد ۲، برای عدد اول دل‌خواه p چنین نمایشی برای $\sqrt{p}$ پیدا کنیم، می‌توان به محاسبه‌ی $\left(\frac{p}{q}\right)$ با روشی مشابه امیدوار بود. در ادامه با معرفی اولین نوع از مجموع‌های گاوسی یعنی مجموع‌های گاوسی مربعی[1] این کار را انجام خواهیم داد.

۱.۳. مجموع‌های گاوسی مربعی.

تعریف ۲.۳. فرض کنید p عددی اول و فرد و a عددی صحیح است. همچنین $\zeta=e^{\frac{2\pi i}{p}}$ یک ریشه‌ی pام واحد باشد. در این صورت مجموع گاوسی مربعی متناظر a به صورت زیر تعریف می‌شود:

$$g_a=\sum_{i=0}^{p-1}\left(\frac{i}{p}\right)\zeta^{ia}$$

برای راحتی از این پس g_1 را تنها با نماد g نشان می‌دهیم. لم بعدی نشان می‌دهد g_a و g ربط خیلی روشنی به هم دارند.

لم ۳.۳. برای هر a صحیح $g_a=\left(\frac{a}{p}\right).g$

اثبات. اولاً دقت کنید اگر a بر p بخش‌پذیر باشد، دو طرف صفرند و حکم واضح خواهد بود. لذا فرض کنید a بر p بخش‌پذیر نیست. چون $\left(\frac{a}{p}\right)=\pm 1$ کافیست نشان دهیم $\left(\frac{a}{p}\right)g_a=g$. حال دقت کنید مقدار $\left(\frac{j}{p}\right)$ و ζ^j تنها به باقیمانده‌ی j بر p بستگی دارد و چون a نسبت به p اول است، $j=ai$ برای $i=0,\cdots,p-1$ تمام باقی‌مانده‌های مختلف به پیمانه‌ی p را می‌دهد. لذا:

$$\begin{aligned}\left(\frac{a}{p}\right)g_a&=\left(\frac{a}{p}\right)\sum_{i=0}^{p-1}\left(\frac{i}{p}\right)\zeta^{ia}=\sum_{i=0}^{p-1}\left(\frac{a}{p}\right)\left(\frac{i}{p}\right)\zeta^{ia}\\&=\sum_{i=0}^{p-1}\left(\frac{ia}{p}\right)\zeta^{ia}=\sum_{j=0}^{p-1}\left(\frac{j}{p}\right)\zeta^{j}=g\end{aligned}$$

$\square$

با توجه به نکته‌ای که در اثبات قضیه‌ی قبل بیان شد، مقدار $\left(\frac{i}{p}\right)$ و ζ^i تنها به باقی‌مانده‌ی i بر p بستگی دارد؛ بنابراین می‌توان تعریف مجموع گاوسی مربعی متناظر a را به صورت زیر در نظر گرفت:

$$g_a=\sum_{i\in\mathbb{F}_p}\left(\frac{i}{p}\right)\zeta^{ia}$$

همان طور که قبلاً اشاره شد به دنبال یافتن نمایشی برای $\sqrt{p}$ هستیم؛ مشابه نمایشی که برای $\sqrt{2}$ به صورت $e^{\frac{2\pi i}{8}}+e^{-\frac{2\pi i}{8}}$ داشتیم. قضیه‌ی بعدی نشان می‌دهد مجموع‌های گاوسی مربعی در واقع چنین نمایشی را برای ما فراهم می‌کنند.

قضیه ۴.۳. برای عدد اول و فرد p داریم $g^2=(-1)^{\frac{p-1}{2}}\times p$.

[1] quadratic Gauss sums

اثبات. مجموع $\sum_{a=0}^{p-1} g_a g_{-a}$ را به دو روش مختلف حساب می‌کنیم:

$$\sum_{a=0}^{p-1} g_a g_{-a} = \sum_a \left(\frac{a}{p}\right) g \left(\frac{-a}{p}\right) g = \sum_a \left(\frac{-a^2}{p}\right) g^2$$
$$= g^2 \times (p-1) \times \left(\frac{-1}{p}\right) = g^2 \times (p-1) \times (-1)^{\frac{p-1}{2}}$$

از طرف دیگر با محاسبه‌ی مستقیم داریم:

$$\sum_{a=0}^{p-1} g_a g_{-a} = \sum_a \left(\sum_{x=1}^{p-1} \left(\frac{x}{p}\right) \zeta^{ax}\right) \left(\sum_{y=1}^{p-1} \left(\frac{y}{p}\right) \zeta^{-ay}\right)$$
$$= \sum_a \left(\sum_x \sum_y \left(\frac{x}{p}\right) \left(\frac{y}{p}\right) \zeta^{a(x-y)}\right)$$
$$= \sum_x \sum_y \left(\frac{x}{p}\right) \left(\frac{y}{p}\right) \sum_a \zeta^{a(x-y)}$$

حال دقت کنید اگر $x \neq y$ باشد $\sum_{a=0}^{p-1} \zeta^{a(x-y)} = 0$. (چرا؟) بنابراین کافی است مجموع فوق را روی $x = y$ حساب کنیم:

$$\sum_{a=0}^{p-1} g_a g_{-a} = \sum_{x=1}^{p-1} \left(\frac{x^2}{p}\right) \sum_{a=0}^{p-1} 1 = \sum_{x=1}^{p-1} \sum_{a=0}^{p-1} 1 = p(p-1)$$

با برابر قراردادن دو مقدار بالا که از محاسبه‌ی $\sum_a g_a g_{-a}$ حاصل شد، حکم نتیجه می‌شود. □

طبق قضیه‌ی قبل در حالتی که باقی‌مانده‌ی p بر ۴ برابر ۱ باشد $g^2 = p$ و در حالتی که باقی‌مانده‌ی p بر ۴ برابر ۳ باشد $g^2 = -p$ است. پس در حالت اول g یکی از دو مقدار $\sqrt{p}$ یا $-\sqrt{p}$ و در حالت دوم یکی از دو مقدار $i\sqrt{p}$ یا $-i\sqrt{p}$ را خواهد داشت. این که در هر حالت کدام مورد رخ خواهد داد مسئله‌ی مشکلی است. گاوس در ۱۸۰۱ حدس زده‌بود که در هر دو حالت مورد اول رخ می‌دهد؛ اما چهار سال طول کشید تا بتواند این ادعا را ثابت کند. در اینجا به این مسئله نخواهیم پرداخت.

۲.۳. اثبات قانون تقابل مربعی. در این بخش صورت قانون تقابل مربعی را بیان و با کمک نتایج بخش قبل آن را ثابت می‌کنیم. همانطور که گفته شد قانون تقابل مربعی ارتباطی بین وجود جواب برای دو معادله‌ی $x^2 \equiv p \pmod q$ و $x^2 \equiv q \pmod p$ برای دو عدد اول فرد p و q برقرار می‌کند. یعنی ارتباطی بین دو مقدار $\left(\frac{p}{q}\right)$ و $\left(\frac{q}{p}\right)$؛ که به طرز غیرمنتظره‌ای ساده است.

قضیه ۵.۳. (تقابل مربعی) برای هر دو عدد اول فرد $p \neq q$ داریم

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

اثبات. طبق قضیه‌ی قبل $g^2 = (-1)^{\frac{p-1}{2}} \times p$ پس

$$g^{q-1} = (-1)^{\frac{p-1}{2} \times \frac{q-1}{2}} \times p^{\frac{q-1}{2}}$$

در نتیجه

$$(-1)^{\frac{p-1}{2} \times \frac{q-1}{2}} \times \left(\frac{p}{q}\right) \times g \underset{\Omega}{\equiv} g^q \underset{\Omega}{\equiv} \left(\sum_{i=0}^{p-1} \left(\frac{i}{p}\right) \zeta^i\right)^q$$
$$\underset{\Omega}{\equiv} \sum_{i=0}^{p-1} \left(\frac{i}{p}\right)^q \zeta^{iq} = \sum_{i=0}^{p-1} \left(\frac{i}{p}\right) \zeta^{iq} = g_q = \left(\frac{q}{p}\right) \times g$$

که همنهشتی‌های بالا همگی به پیمانه q هستند. پس

$$(-1)^{\frac{p-1}{2} \times \frac{q-1}{2}} \times \left(\frac{p}{q}\right) \times g \underset{\Omega}{\equiv} \left(\frac{q}{p}\right) \times g \pmod q$$

با ضرب کردن دو طرف در g داریم

$$(-۱)^{\frac{p-۱}{۲}\times\frac{q-۱}{۲}} \times \left(\frac{p}{q}\right) \times g^۲ \underset{\Omega}{\equiv} \left(\frac{q}{p}\right) \times g^۲$$

و چون دو طرف صحیح هستند، طبق نتیجه ۱۱.۲ این هم‌نهشتی در $\mathbb{Z}$ هم برقرار است و چون $g^۲ = (-۱)^{\frac{p-۱}{۲}} \times p$ نسبت به q اول است با ساده کردن $g^۲$ از دو طرف حکم ثابت می‌شود.

□

۴. قانون تقابل درجه سوم

در این بخش تنها می‌خواهیم صورت قانون تقابل درجه سوم را که توسط آیزنشتاین ثابت شده است، بیان کنیم. هیچ‌یک از گزاره‌های این بخش را ثابت نخواهیم کرد. مطالب این بخش در بخش‌های بعدی استفاده نخواهد شد. خواننده‌ی علاقه‌مند می‌تواند برای دیدن اثبات مطالب این بخش به مرجع [۲] مراجعه کند.

تقابل درجه سوم در حلقه‌ای بزرگ‌تر از حلقه‌ی اعداد صحیح مطرح است. این حلقه که به حلقه‌ی اعداد آیزنشتاین معروف است، از قرن نوزدهم و حتی شاید قبل از آن شناخته‌شده بود. فرض کنید ω یک ریشه سوم اولیه واحد، یا معادلاً ریشه‌ی چندجمله‌ای $x^۲ + x + ۱$ باشد. در این صورت حلقه مورد نظر به شکل زیر تعریف می‌شود:

$$\mathbb{Z}[\omega] = \{a + b\omega | a, b \in \mathbb{Z}\}$$

می‌توان نشان داد که این حلقه یک دامنه‌ی تجزیه یکتا است.

تعریف ۱.۴. برای هر عنصر $z = a + b\omega$ در $\mathbb{Z}[\omega]$ نرم آن به صورت $N(z) = a^۲ - ab + b^۲$ تعریف می‌شود.

گزاره ۲.۴. عناصر یکه (وارون‌پذیر) حلقه $\mathbb{Z}[\omega]$ دقیقاً $\{۱, -۱, \omega, -\omega, \omega^۲, -\omega^۲\}$ هستند.

تعریف ۳.۴. دو عنصر در $\mathbb{Z}[\omega]$ را هم‌ارز گوییم هرگاه نسبت‌شان یکه باشد.

تعریف ۴.۴. عدد اول $\pi = a + b\omega$ در $\mathbb{Z}[\omega]$ را اولیه گوییم هرگاه $a \equiv ۲ \pmod ۳$ و $b \equiv ۰ \pmod ۳$. به سادگی می‌توان نشان داد هر عدد اول در $\mathbb{Z}[\omega]$ که با $۱ - \omega$ هم‌ارز نباشد، دقیقاً یک هم ارز اولیه دارد. دقت کنید تفاوت بین یک عدد اول اولیه با هم‌ارزهایش مانند تفاوت دو عدد اول p و $-p$ در اعداد صحیح است. لذا این تعریف اصلاً غیرطبیعی نیست.

از این پس در همه‌ی گزاره‌های بعدی فرض کنید عدد اول π با $۱ - \omega$ هم ارز نیست. این فرض دقیقاً مشابه فرض فردبودن اعداد اول است که در اکثر قضایای بخش ۳ وجود داشت.

گزاره ۵.۴. در حلقه‌ی $\mathbb{Z}[\omega]$ برای هر عدد اول π و هر a که بر آن بخش‌پذیر نباشد، $a^{\frac{N(\pi)-۱}{۳}}$ با یکی از سه عدد ۱ یا ω یا $\omega^۲$ به پیمانه‌ی π همنهشت است. مقدار $\left(\frac{a}{\pi}\right)_۳$ را در هر یک از این سه حالت به ترتیب ۱ یا ω یا $\omega^۲$ تعریف می‌کنیم.

گزاره ۶.۴. برای عدد اول π در $\mathbb{Z}[\omega]$ و هر a که بر آن بخش‌پذیر نباشد، $\left(\frac{a}{\pi}\right)_۳ = ۱$ است اگر و تنها اگر a به پیمانه‌ی π مانده‌ی مکعبی باشد، یعنی با یک مکعب کامل در $\mathbb{Z}[\omega]$ هم‌نهشت باشد.

گزاره ۷.۴. برای هر π اول، تابع $\chi : \left(\frac{\mathbb{Z}[\omega]}{\pi\mathbb{Z}[\omega]}\right)^\times \to \{۱, \omega, \omega^۲\}$ با ضابطه‌ی $\chi(a) = \left(\frac{a}{\pi}\right)_۳$ یک هم‌ریختی گروهی پوشا است.

قضیه ۸.۴. (تقابل درجه سوم) اگر π و ρ دو عدد اول متمایز و اولیه در حلقه‌ی $\mathbb{Z}[\omega]$ باشند و با $۱ - \omega$ هم‌ارز نباشند آنگاه $\left(\frac{\rho}{\pi}\right)_۳ = \left(\frac{\pi}{\rho}\right)_۳$.

۵. تعداد جواب‌های معادلات چندجمله‌ای

یکی کاربردهای جالب مجموع‌هایی از نوع مجموع‌های گاوسی، یافتن تعداد جواب‌های برخی معادلات چندجمله‌ای به پیمانه‌ی یک عدد اول است. در ابتدای این بخش با کمک مفهوم مانده‌ی مربعی تعداد جواب‌های یک معادله‌ی ساده از درجه دو را محاسبه می‌کنیم و سپس جمع‌های گاوسی و ژاکوبی را در حالت کلی معرفی کرده و به کمک آن‌ها تعداد جواب‌های برخی معادلات از درجات بالاتر را هم حساب می‌کنیم. در این مقاله برای سادگی، ما تمرکز خود را بر روی معادلات دو متغیره (و در حالت تصویری، سه متغیره) که در واقع خم جبری هستند می‌گذاریم؛ ولی تمام این محاسبات را می‌توان به حالت nمتغیره تعمیم داد.

فرض کنید p عددی اول و فرد باشد. هدف ما در ابتدای این بخش یافتن تعداد جواب‌های معادله‌ی $x^۲ + y^۲ \equiv ۱ \pmod p$ است. به بیان دیگر می‌خواهیم در میدان $\mathbb{F}_p$ تعداد جواب‌های معادله‌ی $x^۲ + y^۲ = ۱$ را بیابیم. دو لم زیر تقریباً کار را تمام می‌کند.

لم ۱.۵. برای هر $۰ \neq a \in \mathbb{F}_p$ تعداد جواب‌های معادله $x^۲ = a$ در $\mathbb{F}_p$ برابر $۱ + \left(\frac{a}{p}\right)$ است.

اثبات. اگر a مانده‌ی مربعی باشد به روشنی معادله دو جواب (قرینه‌ی هم) دارد و اگر مانده نباشد، هیچ جوابی ندارد. لذا حکم واضح است. $\square$

لم ۲.۵. اگر p عددی اول و فرد باشد

$$\sum_{a\in\mathbb{F}_p} \left(\frac{a}{p}\right)\left(\frac{۱-a}{p}\right) = (-۱)^{\frac{p+۱}{۲}}.$$

اثبات. یک بررسی ساده نشان می‌دهد تابع

$$f : \mathbb{F}_p - \{۱\} \to \mathbb{F}_p - \{-۱\}$$

با ضابطه‌ی $f(a) = \frac{a}{۱-a}$ یک به یک و در نتیجه پوشاست. بنابراین

$$\begin{aligned}\sum_{a\in\mathbb{F}_p} \left(\frac{a}{p}\right)\left(\frac{۱-a}{p}\right) &= \sum_{a\in\mathbb{F}_p\setminus\{۱\}} \left(\frac{a}{p}\right)\left(\frac{(۱-a)^{-۱}}{p}\right)\\ &= \sum_{a\in\mathbb{F}_p\setminus\{۱\}} \left(\frac{f(a)}{p}\right) = ۰ - \left(\frac{-۱}{p}\right) = (-۱)^{\frac{p+۱}{۲}}\end{aligned}$$

$\square$

حال می‌توانیم تعداد جواب‌های معادله‌ی $P : x^۲ + y^۲ = ۱$ را در میدان $\mathbb{F}_p$ بیابیم. برای راحتی تعداد جواب‌های معادله P را با نماد $N(P)$ نشان می‌دهیم.

قضیه ۳.۵. برای هر p اول و فرد داریم تعداد جواب‌های معادله‌ی $x^۲ + y^۲ = ۱$ در میدان $\mathbb{F}_p$ برابر $p + (-۱)^{\frac{p+۱}{۲}}$ است. به طور مختصر $N(x^۲ + y^۲ = ۱) = p + (-۱)^{\frac{p+۱}{۲}}$.

اثبات.

$$\begin{aligned}N(x^۲ + y^۲ = ۱) &= \sum_{a+b=۱} N(x^۲ = a)N(y^۲ = b)\\ &= \sum_{a+b=۱} \left(۱ + \left(\frac{a}{p}\right)\right)\left(۱ + \left(\frac{b}{p}\right)\right)\\ &= p + \sum_{a+b=۱}\left(\frac{a}{p}\right) + \sum_{a+b=۱}\left(\frac{b}{p}\right) + \sum_{a+b=۱}\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)\\ &= p + (-۱)^{\frac{p+۱}{۲}}\end{aligned}$$

$\square$

۱.۵. فضای تصویری. همان طور که دیدیم تعداد جواب‌های معادله‌ی $x^۲ + y^۲ = ۱$ به پیمانه‌ی عدد اول و فرد p برابر $p + (-۱)^{\frac{p+۱}{۲}}$ است. بنابراین در حالتی که p به فرم $۴k + ۱$ باشد تعداد جواب ها $p - ۱$ و در حالت $۴k + ۳$ تعداد جواب‌ها $p + ۱$ است. این دوگانگی کمی ناخوشآیند است. در واقع این مسئله را گاوس هم بررسی کرده و تعداد جواب‌ها را در هر حالت $p + ۱$ به دست آورده است. دلیل این امر این است که گاوس برای حالت $۴k + ۱$ دو جواب در بی‌نهایت برای معادله در نظر گرفته است که در محاسبات ما از قلم افتاده‌اند. برای دقیق کردن این ایده لازم است فضای تصویری را معرفی کنیم. در اینجا تنها توضیحی مختصر در این‌باره می آید. خواننده می‌تواند جهت مطالعه‌ی مفصل‌تر به کتاب‌های هندسه‌ی جبری، مانند مرجع [۱]، مراجعه کند.

برای میدان دلخواه F مجموعه‌ی

$$A^n(F) = \{(x_۰, x_۱, ..., x_{n-۱}) | x_۰, x_۱, ..., x_{n-۱} \in F\}$$

را فضای آفین nـبعدی روی میدان F می‌نامند. حال روی مجموعه‌ی $A^{n+۱}(F) - ۰$ یک رابطه هم‌ارزی قرار می‌دهیم. دو نقطه x و x' در این مجموعه را هم‌ارز گوییم و می‌نویسیم $x \sim x'$ هرگاه $\lambda \in F^\times$ یافت شود که $x = \lambda x'$. بررسی اینکه این یک رابطه هم‌ارزی است را به عهده‌ی خواننده می‌گذاریم. فضای تصویری n بعدی روی میدان F به صورت کلاس‌های هم‌ارزی این رابطه تعریف می‌شود

$$P^n(F) = \frac{A^{n+۱}(F) - ۰}{\sim}$$

مثلاً اگر نقطه صوری ∞ را به $A^۱(F)$ بیفزایید، تناظر یک‌به‌یک طبیعی بین $P^۱(F)$ و $A^۱(F) \bigcup \{\infty\}$ وجود دارد. خواننده را تشویق می‌کنیم که این تناظر را دقیقاً بسازد.

در این مقاله ما تنها با مجموعه $P^۲(F)$ سروکار داریم. لذا کمی آن را دقیق‌تر مطالعه می‌کنیم. دقت کنید طبق تعریف برای $\lambda \in F^\times$، دو نقطه‌ی $(x_۰, x_۱, x_۲)$ و $(\lambda x_۰, \lambda x_۱, \lambda x_۲)$ در یک کلاس هم‌ارزی هستند. برای تاکید بر این نکته که تنها نسبت بین x_iها اهمیت دارد، کلاس هم‌ارزی شامل $(x_۰, x_۱, x_۲)$ را با نماد $(x_۰ : x_۱ : x_۲)$ نشان می‌دهیم. بنابراین $(x_۰ : x_۱ : x_۲) = (\lambda x_۰ : \lambda x_۱ : \lambda x_۲)$. حال نقاط $P^۲(F)$ را به دو دسته تقسیم می‌کنیم. اول نقاطی که $x_۲ \neq ۰$. به وضوح برای هر هم‌کلاس این نقطه هم مولفه سوم ناصفر است. لذا با ضرب‌کردن در λ مناسب می‌توان مولفه سوم را یک کرد. در این صورت $x_۰$ و $x_۱$ اعضای دلخواهی از F هستند. لذا این‌گونه نقاط در تناظر طبیعی با $A^۲(F)$ هستند. دسته‌ی دوم نقاطی هستند که $x_۲ = ۰$ و لذا مولفه سوم هر هم‌کلاس این نقطه هم صفر است. پس برای این نقاط، دو مولفه دیگر می‌توانند در هر $\lambda \in F^\times$ ضرب شوند. لذا این نقاط در تناظر یک‌به‌یک با $P^۱(F)$ هستند.

بنابراین $P^۲(F)$ اجتماع یک کپی از $A^۲(F)$ (نقاطی که به شکل $(x_۰ : x_۱ : ۱)$ هستند) و یک کپی از $P^۱(F)$ است (نقاطی که به شکل $(x_۰ : x_۱ : ۰)$ هستند) که آن‌ها را اصطلاحاً نقاط در بی‌نهایت گویند. خود این نقاط در بی‌نهایت هم دو دسته اند. یک کپی از $A^۱(F)$ (نقاطی که به شکل $(x_۰ : ۱ : ۰)$ هستند) و یک تک نقطه $(۱ : ۰ : ۰)$.

حال دقت کنید اگر یک چندجمله‌ای همگن سه‌متغیره مانند $f(x_۰, x_۱, x_۲)$ داشته باشیم، اگر $f(x_۰, x_۱, x_۲) = ۰$، برای هر λ ناصفر $f(\lambda x_۰, \lambda x_۱, \lambda x_۲) = ۰$. بنابراین مجموعه ریشه‌های چنین چندجمله‌ای روی $P^۲(F)$ خوش تعریف است. به عنوان مثال اگر $f(x_۰, x_۱, x_۲) = x_۰{}^۲ + x_۱{}^۲ - x_۲{}^۲$ و f روی یک نقطه صفر شود، روی تمام کلاس هم‌ارزی آن نقطه صفر می‌شود.

حال برای عدد اول p میدان F را میدان p عضوی $\mathbb{F}_p$ بگیرید و چندجمله‌ای $f(x_۰, x_۱, x_۲) = x_۰{}^۲ + x_۱{}^۲ - x_۲{}^۲$ را روی این میدان در نظر بگیرید، می‌خواهیم تعداد ریشه آن را در $P^۲(F)$ حساب کنیم. تعداد ریشه‌هایی که $x_۲$ مخالف صفر یا مساوی صفر باشد را جدا حساب می‌کنیم. اگر $x_۲$ ناصفر باشد میتوان آن را برابر یک فرض کرد و لذا باید جواب های $x_۰{}^۲ + x_۱{}^۲ - ۱ = ۰$ را در $A^۲(F)$ حساب کنیم که در بخش قبل حساب کردیم و در حالت $p = ۴k + ۱$ برابر $p - ۱$ و در حالت $p = ۴k + ۳$ برابر $p + ۱$ بود. حال جواب‌هایی که $x_۲ = ۰$ را می‌شماریم. پس باید جواب‌های $x_۰{}^۲ + x_۱{}^۲ = ۰$ در $P^۱(F)$ بشماریم. نقاط با $x_۲ = ۰$ هم دو دسته بودند. یک تک نقطه $(۱ : ۰ : ۰)$ که در معادله صدق نمی‌کند و مجموعه نقاط به شکل $(x_۰ : ۱ : ۰)$. اگر چنین نقطه‌ای در معادله صدق کند باید $x_۰{}^۲ + ۱ = ۰$ که در حالت $p = ۴k + ۱$ چون -۱ مانده‌ی مربعی است دو جواب دارد و اگر $p = ۴k + ۳$ چون -۱ نامانده‌ی مربعی است جوابی ندارد (دقت کنید $(۰ : ۰ : ۰)$ نقطه ای از $P^۲(F)$ نیست و

هر عضو $P^{۲}(F)$ دست کم یک مولفه ناصفر دارد). لذا در حالت $p = ۴k + ۱$ دو جواب در بی‌نهایت بجز جواب‌هایی که در $A^{۲}(F)$ داشتیم اضافه شدند و لذا در هر حالت تعداد جواب ها $p + ۱$ است.

۲.۵. کاراکترها. برای معرفی مجموع‌های گاوسی در حالت کلی لازم است ابتدا مفهوم کاراکتر را تعریف کنیم. همانطور که در قضیه ۴.۲ دیدیم $\left(\frac{a}{p}\right)$ یک همریختی گروهی از $\left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^{\times}$ به ± ۱ است. همین هم‌ریختی گروهی بودن ویژگی اساسی بود که خواص جمع‌های گاوسی مربعی را نتیجه می‌داد و همین طور کمک کرد تعداد جواب‌های معادله‌ی $x^{۲} + y^{۲} = ۱$ را در $\mathbb{F}_p$ بیابیم. لذا تعریف کلی‌تر زیر را انجام می‌دهیم.

تعریف ۴.۵. منظور از یک کاراکتر به پیمانه عدد اول p، یک هم‌ریختی گروهی به شکل زیر است

$$\chi : \left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^{\times} \to \mathbb{C}^{\times}$$

با توجه به اینکه هر عضو گروه $\left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^{\times}$ اگر به توان $p - ۱$ برسد برابر یک می‌شود، لذا تصویر آن عضو تحت χ یک ریشه $(p - ۱)$ام واحد است و به علاوه $\chi(a^{-۱}) = \chi(a)^{-۱} = \overline{\chi(a)}$.

به عنوان مثال به وضوح $\left(\frac{a}{p}\right)$ یک کاراکتر است. به علاوه نگاشت ثابت ۱ روی $\left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^{\times}$ نیز یک کاراکتر است. این کاراکتر خاص را با نماد ε نشان می‌دهیم و آن را کاراکتر بدیهی می‌نامیم. لذا برای هر $a \in \left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^{\times}$ داریم $\varepsilon(a) = ۱$. همان‌طور که نماد $\left(\frac{a}{p}\right)$ را برای حالتی که a بر p بخش‌پذیر باشد هم تعریف کردیم، مشابهاً برای هر کاراکتر غیر بدیهی اگر a بر p بخش‌پذیر باشد تعریف می‌کنیم $\chi(a) = ۰$. برای کاراکتر بدیهی تعریف می‌کنیم $\varepsilon(a) = ۱$.

پیش از تعریف جمع‌های گاوسی در حالت کلی لازم است برخی خواص مقدماتی کاراکترها را مطالعه کنیم. اولاً حاصل ضرب دو کاراکتر یک کاراکتر است. همچنین وارون یک کاراکتر هم خود کاراکتر است. پس مجموعه کاراکترها خود یک گروه است.

گزاره ۵.۵. مجموعه کاراکترها یک گروه دوری از مرتبه $p - ۱$ است و برای هر $a \in \mathbb{F}_p$ $۱ \neq$ کاراکتر χ وجود دارد که $\chi(a) \neq ۱$.

اثبات. می‌دانیم گروه $\mathbb{F}_p^{\times}$ دوری است. فرض کنید g یک مولد آن باشد. لذا هر کاراکتر χ با تعیین $\chi(g)$ به طور یکتا تعیین می‌شود. از طرفی $\chi(g)$ باید یک ریشه $p - ۱$ام واحد باشد و انتخاب هر یک از این $p - ۱$ تا ریشه‌ی $p - ۱$ام واحد یک کاراکتر به ما می‌دهد. لذا تعداد کاراکترها $p - ۱$ است. از طرفی اگر مقدار $\chi(g)$ را برابر یک ریشه‌ی اولیه‌ی $p - ۱$ام واحد انتخاب کنیم، این کاراکتر یک مولد برای گروه کاراکترها خواهد بود. (چرا؟) این مولد را λ بنامید. در این صورت چون $\lambda(g)$ یک ریشه‌ی $p - ۱$ام اولیه‌ی واحد است، لذا برای هر $a \in \mathbb{F}_p$ $۱ \neq$ داریم $\lambda(a) \neq ۱$. □

گزاره ۶.۵. برای هر کاراکتر غیربدیهی χ داریم $\sum_{a\in\mathbb{F}_p} \chi(a) = ۰$.

اثبات. چون $\chi \neq \varepsilon$ لذا $b \neq ۰$ وجود دارد که $\chi(b) \neq ۱$ حال

$$\chi(b) \sum_{a\in\mathbb{F}_p} \chi(a) = \sum_{a\in\mathbb{F}_p} \chi(ab) = \sum_{c\in\mathbb{F}_p} \chi(c) = \sum_{a\in\mathbb{F}_p} \chi(a)$$

پس $(\chi(b) - ۱) \sum \chi(a) = ۰$ و چون $\chi(b) \neq ۱$ حکم نتیجه می‌شود. □

گزاره ۷.۵. برای هر $a \neq ۱$ در $\mathbb{F}_p$ داریم $\sum_{\chi} \chi(a) = ۰$ که جمع روی همه‌ی کاراکترهاست.

اثبات. طبق گزاره ۵.۵ کاراکتر λ موجود است که $\lambda(a) \neq ۱$. پس

$$\lambda(a) \sum_{\chi} \chi(a) = \sum_{\chi} \lambda(a)\chi(a) = \sum_{\chi} (\lambda\chi)(a) = \sum_{\chi} \chi(a)$$

و چون $\lambda(a) \neq ۱$ حکم نتیجه می‌شود.

□

از نظریه اعداد مقدماتی می‌دانیم برای $a \in \mathbb{F}_p$ ناصفر، معادله‌ی $x^n = a$ در میدان $\mathbb{F}_p$ جواب دارد، اگر و تنها اگر $a^{\frac{p-1}{d}} = 1$ که $d = (p-1, n)$. لزوم این شرط به دلیل قضیه‌ی کوچک فرما و کفایت آن به دلیل وجود ریشه‌ی اولیه به پیمانه p است. به علاوه به آسانی می‌توان دریافت تعداد جواب‌ها دقیقاً برابر d است. از این به بعد فرض کنید $p-1$ بر n بخش‌پذیر است تا محاسبات راحت‌تر باشد. لذا معادله‌ی $x^n = a$ دقیقاً n جواب متمایز خواهد داشت اگر و تنها اگر $a^{\frac{p-1}{n}} = 1$. به کمک کاراکترها می‌توان فرمولی برای این تعداد جواب‌ها نوشت. قضیه‌ی بعد را به عنوان تعمیمی از لم ۱.۵ ببینید.

قضیه ۸.۵. اگر $n|p-1$ آنگاه

$$N(x^n = a) = \sum_{\chi^n = \varepsilon} \chi(a)$$

که مجموع فوق روی همه‌ی کاراکترهایی است که مرتبه‌ی آن‌ها در گروه کاراکترها، n را می‌شمارد.

اثبات. اولاً چون گروه کاراکترها دوری است، دقیقاً n کاراکتر وجود دارد که مرتبه آن‌ها n را بشمارد (این برای هر گروه دوری درست است). برای $a = 0$ حکم واضح است. برای $a \neq 0$ اگر $x^n = a$ جواب داشته باشد، برای هر یک کاراکترهایی که مرتبه آن‌ها n را بشمارد داریم:

$$\chi(a) = \chi(x^n) = \chi^n(x) = \varepsilon(x) = 1$$

و لذا $n = \sum_{\chi^n=\varepsilon} 1 = \sum_{\chi^n=\varepsilon} \chi(a)$ که همان تعداد جواب‌های معادله است. در حالتی که $x^n = a$ جواب نداشته باشد باید نشان دهیم مجموع مورد نظر صفر است که عیناً مشابه اثبات گزاره‌ی ۷.۵ است و به خواننده واگذار می‌شود. (دقت کنید مجموعه‌ی کاراکترهایی که مرتبه آن‌ها n را می‌شمارد یک گروه است.) □

۳.۵. جمع‌های گاوسی. حال می‌توانیم مجموع‌های گاوسی را در حالتی کلی‌تر معرفی کنیم. اثبات تمام قضایای این بخش عیناً مشابه اثبات‌هایی است که در حالت مجموع‌های گاوسی مربعی برای آن‌ها ارائه کردیم، لذا از تکرار اثبات‌ها می‌پرهیزیم. توصیه می‌کنیم خواننده شخصاً اثبات‌ها را کامل کند.

تعریف ۹.۵. برای هر p اول، $a \in \mathbb{F}_p$ و کاراکتر χ به پیمانه‌ی p، جمع گاوسی متناظر آن‌ها به شکل زیر تعریف می‌شود

$$g_a(\chi) = \sum_{i \in \mathbb{F}_p} \chi(i)\zeta^{ia}$$

که $\zeta = e^{\frac{2\pi i}{p}}$ ریشه‌ی pاُم واحد است.

برای راحتی از این پس g_1 را تنها با نماد g نشان می‌دهیم. لم زیر تعمیم لم ۳.۳ است. اثبات آن نیز کاملاً شبیه لم ۳.۳ است و به خواننده واگذار می‌شود.

لم ۱۰.۵. برای هر a و χ داریم $g_a(\chi) = \chi^{-1}(a)g(\chi) = \overline{\chi(a)}g(\chi)$

قضیه بعدی تعمیم قضیه ۴.۳ است که مهم‌ترین قضیه در بخش جمع‌های گاوسی مربعی بود.

قضیه ۱۱.۵. برای هر کاراکتر غیربدیهی χ داریم

$$g(\chi)g(\overline{\chi}) = \chi(-1)p$$

و از طرفی چون $g(\overline{\chi}) = \chi(-1)\overline{g(\chi)}$ بنابراین $|g(\chi)| = \sqrt{p}$.

اثبات. با محاسبه دوگانه‌ی $\sum_a g_a(\chi)\overline{g_a(\chi)}$ کاملاً مشابه اثبات قضیه‌ی ۴.۳ حکم حاصل می‌شود. تکمیل اثبات را به عهده‌ی خواننده می‌گذاریم. □

۴.۵. جمع‌های ژاکوبی. در بخش‌های قبلی، برای اثبات قضیه ۳.۵ نیاز به محاسبه‌ی مجموع $\sum_{a+b=1}\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$ داشتیم که این کار را در لم ۲.۵ انجام دادیم. این مجموع حالت خاصی از مجموع‌های کلی‌تری است که ژاکوبی در اواسط قرن ۱۹ آن‌ها را مطالعه می‌کرد. این مجموع‌ها برای محاسبه‌ی تعداد جواب‌های معادلات چندجمله‌ای به پیمانه‌ی یک عدد اول بسیار مفید هستند. در این بخش مجموع‌های ژاکوبی را معرفی کرده و یک قضیه‌ی اساسی در مورد آن‌ها ثابت می‌کنیم که هم ارتباط آن‌ها با جمع‌های گاوسی را روشن خواهد کرد و هم در بخش‌های بعدی به کرات از آن استفاده خواهیم کرد.

تعریف ۱۲.۵. فرض کنید χ و λ دو کاراکتر به پیمانه‌ی عدد اول p باشند. مجموع ژاکوبی آن‌ها به صورت زیر تعریف می‌شود:

$$J(\chi,\lambda)=\sum_{a+b=1}\chi(a)\lambda(b).$$

قضیه ۱۳.۵. اگر ε کاراکتر بدیهی و χ و λ دو کاراکتر غیربدیهی باشند و $\chi\lambda\neq\varepsilon$ آنگاه

الف) $J(\varepsilon,\varepsilon)=p$

ب) $J(\varepsilon,\chi)=0$

ج) $J(\chi,\chi^{-1})=-\chi(-1)$

د) $J(\chi,\lambda)=\frac{g(\chi)g(\lambda)}{g(\chi\lambda)}$ و بنابراین $|J(\chi,\lambda)|=\sqrt{p}$

اثبات. قسمت الف طبق تعریف واضح است و قسمت ب همان گزاره ۶.۵ است. اثبات قسمت ج نیز عیناً همان اثبات لم ۲.۵ است. لذا تنها قسمت د را ثابت می‌کنیم. ابتدا $g(\chi)g(\lambda)$ را باز می‌کنیم:

$$g(\chi)g(\lambda)=\left(\sum_x\chi(x)\zeta^x\right)\left(\sum_y\lambda(y)\zeta^y\right)$$

$$=\sum_{x,y}\chi(x)\lambda(y)=\sum_t\left(\sum_{x+y=t}\chi(x)\lambda(y)\right)\zeta^t$$

پس کافی است مجموع را برای tهای مختلف حساب کنیم. برای $t=0$ مجموع $\left(\sum_{x+y=0}\chi(x)\lambda(y)\right)$ به سادگی برابر صفر است. (چرا؟) برای t ناصفر با تقسیم‌کردن x و y بر t می‌توان جمع را به یک مجموع ژاکوبی معمولی تبدیل کرد.

$$\left(\sum_{x+y=t}\chi(x)\lambda(y)\right)=\sum_{\frac{x}{t}+\frac{y}{t}=1}\chi(t)\lambda(t)\chi(\frac{x}{t})\lambda(\frac{y}{t})$$

$$=\chi(t)\lambda(t)\sum_{\frac{x}{t}+\frac{y}{t}=1}\chi(\frac{x}{t})\lambda(\frac{y}{t})=(\chi\lambda)(t)J(\chi,\lambda)$$

در نتیجه

$$g(\chi)g(\lambda)=\sum_t(\chi\lambda(t))J(\chi,\lambda)\zeta^t=J(\chi,\lambda)g(\chi\lambda)$$

و لذا حکم ثابت می‌شود. حال با توجه به اینکه $|g(\chi)|=\sqrt{p}$ به روشنی داریم $|J(\chi,\lambda)|=\sqrt{p}$. □

۵.۵. محاسبه تعداد جواب‌ها با کمک مجموع ژاکوبی. با کمک مجموع‌های ژاکوبی که در قسمت قبل معرفی شد می‌توان تعداد جواب‌های بسیاری از معادلات چندجمله‌ای دومتغیره را در میدان $\mathbb{F}_p$ محاسبه کرد. در واقع مجموع ژاکوبی را می‌توان برای تعداد دل‌خواهی کاراکتر نیز تعریف کرد و به کمک آن تعداد جواب‌های معادلات با تعداد متغیر بیشتر را نیز محاسبه کرد ولی ما این جا برای سادگی تنها با معادلات دو متغیره کار می‌کنیم. در این بخش با کمک مجموع‌های ژاکوبی تعداد جواب‌های یک معادله‌ی درجه‌ی سوم خاص را به پیمانه‌ی عدد اول p حساب می‌کنیم. روشی که استفاده می‌کنیم قابل استفاده برای معادلات بسیار متنوعی است. آندره ویل در مقاله‌ی تاریخی خود (مرجع [۳]) این محاسبات را در حالت بسیار کلی انجام داده است که خواننده‌ی علاقه‌مند می‌تواند به آن مراجعه کند. ما اینجا به یک مثال خاص بسنده می‌کنیم.

فرض کنید p یک عدد اول $3k+1$ باشد. در این صورت سه کاراکتر وجود دارند که مرتبه آن‌ها ۳ را می‌شمارد. کاراکتر بدیهی و دو کاراکتر نابدیهی که آن‌ها را χ و λ می‌نامیم. این سه کاراکتر خود یک گروه (یک‌ریخت با $\frac{\mathbb{Z}}{3\mathbb{Z}}$) می‌سازند. لذا $\chi^2=\lambda$ و از طرف دیگر $\overline{\chi}=\chi^{-1}=\chi^2$. (چرا؟) در قضیه‌ی بعد به کمک این کاراکترها تعداد جواب‌های معادله‌ی $x^3+y^3=1$ را به پیمانه p حساب می‌کنیم.

قضیه ۱۴.۵. اگر p عددی اول و $p = 3k+1$ باشد و χ و λ کاراکترهای معرفی‌شده در بالا باشند آنگاه

$$N(x^3+y^3=1) = p-2+J(\chi,\chi)+J(\lambda,\lambda)$$

بنابراین از آنجا که $|J(\chi,\chi)| = |J(\lambda,\lambda)| = \sqrt{p}$ لذا

$$|N(x^3+y^3=1)-p-2| < 2\sqrt{p}.$$

اثبات. استدلال صرفاً استفاده‌ی مکرر از قضیه ۸.۵ و ۱۳.۵ است.

$$\begin{aligned}
N(x^3+y^3=1) &= \sum_{a+b=1} N(x^3=a)N(y^3=b)\\
&= \sum_{a+b=1} (1+\chi(a)+\lambda(a))(1+\chi(b)+\lambda(b))\\
&= p+\sum_{a+b=1}\chi(a)\chi(b)+\sum_{a+b=1}\lambda(a)\lambda(b)+2\sum_{a+b=1}\chi(a)\lambda(b)\\
&= p+J(\chi,\chi)+J(\lambda,\lambda)+2J(\chi,\lambda)\\
&= p+J(\chi,\chi)+J(\lambda,\lambda)+2J(\chi,\chi^{-1})\\
&= p+J(\chi,\chi)+J(\lambda,\lambda)-2\chi(-1)\\
&= p+J(\chi,\chi)+J(\lambda,\lambda)-2
\end{aligned}$$

□

جواب‌های در بی‌نهایت معادله‌ی قبل را از قلم انداخته‌ایم که سعی می‌کنیم آن‌ها را اضافه کنیم. معادله‌ی همگن شده‌ی معادله‌ی قبل $x^3+y^3=z^3$ است. باید جواب‌های آن را در $P^2(\mathbb{F}_p)$ بیابیم. اگر z ناصفر باشد که می‌توان آن را یک کرد و همان جواب‌های قضیه قبل به دست می‌آیند. اگر $z=0$ باشد (جواب‌های در بی‌نهایت) باید جواب‌های $x^3+y^3=0$ را بیابیم. این نقاط خود دو دسته هستند. یک تک نقطه $(0:0:1)$ که جواب نیست و یک دسته نقاطی که y آن‌ها ناصفر است، که اگر آن را یک کنیم باید جواب‌های $x^3+1=0$ را بیابیم. طبق حرف‌هایی که در بخش کاراکترها زدیم این معادله ۳ جواب دارد. (دقت کنید $3|p-1$.) لذا با احتساب این ۳ جواب در بی‌نهایت تعداد جواب‌های معادله در فضای تصویری برابر $p+1+J(\chi,\chi)+J(\lambda,\lambda)$ است.

۶.۵. جمع‌های گاوسی و ژاکوبی روی میدان متناهی. ما تا اینجا همواره روی میدان $\mathbb{F}_p$ که p عددی اول است کار کرده‌ایم ولی برای ادامه مسیر لازم است جواب‌های معادلات چندجمله‌ای روی سایر میدان‌های متناهی را هم در نظر بگیریم. لذا لازم است مفهوم کاراکتر، مجموع گاوسی و مجموع ژاکوبی را روی یک میدان متناهی دلخواه تعریف کنیم. تنها قسمت نابدیهی ماجرا این خواهد بود که ζ^a تنها به باقی‌مانده‌ی a بر p بستگی داشت و لذا برای $a \in \mathbb{F}_p$ معنادار بود؛ ولی روشن نیست که چطور این را به میدان متناهی دلخواه توسعه دهیم. برای این کار باید از مفهوم اثر[1] استفاده کرد.

می‌دانیم هر میدان متناهی از مشخصه‌ی p دارای $q=p^k$ عضو است، برای یک k مناسب. می‌خواهیم تابع خطی $tr:\mathbb{F}_q \to \mathbb{F}_p$ را تعریف کنیم. اگر با مفهوم اثر یک توسیع میدانی متناهی آشنایی دارید این اثر که ما اینجا تعریف خواهیم کرد در واقع اثر توسیع $\mathbb{F}_q/\mathbb{F}_p$ است. برای هر $a \in \mathbb{F}_q$ تعریف کنید

$$tr(a) = a+a^p+a^{p^2}+...+a^{p^{k-1}}.$$

می‌توان نشان داد $tr(a) \in \mathbb{F}_p$ است و به علاوه tr تابعی خطی و پوشاست. ما در اینجا این احکام را ثابت نمی‌کنیم. خواننده می‌تواند به مرجع [۲] مراجعه کند. حال می‌توانیم به کمک تابع tr مفاهیم قبلی را روی میدان متناهی دلخواه تعریف کنیم. در همه‌ی تعریف‌های زیر $q=p^k$ است.

[1] trace

تعریف ۱۵.۵. منظور از یک کاراکتر روی میدان $\mathbb{F}_q$، یک هم‌ریختی گروهی به شکل زیر است:

$$\chi : \mathbb{F}_q^{\times} \to \mathbb{C}^{\times}$$

تعریف ۱۶.۵. برای هر میدان متناهی $\mathbb{F}_q$، $a \in \mathbb{F}_q$ و کاراکتر χ روی آن، جمع گاوسی متناظر آن‌ها، به شکل زیر تعریف می‌شود:

$$g_a(\chi) = \sum_{i \in \mathbb{F}_q} \chi(i) \zeta^{tr(ia)}$$

که $\zeta = e^{\frac{2\pi i}{p}}$ ریشه‌ی pام واحد است.

تعریف ۱۷.۵. فرض کنید χ و λ دو کاراکتر روی میدان متناهی $\mathbb{F}_q$ باشند. مجموع ژاکوبی آن‌ها به صورت زیر تعریف می‌شود:

$$J(\chi, \lambda) = \sum_{a+b=1} \chi(a)\lambda(b)$$

تمامی قضایایی که برای جمع‌های گاوسی و ژاکوبی ثابت کرده بودیم برای این جمع‌های جدید هم صادق است، فقط لازم است همه‌ی $\sqrt{p}$ ها به $\sqrt{q}$ تبدیل شود. عیناً همان اثبات‌های قبلی کار می‌کنند لذا از تکرار آن‌ها پرهیز می‌کنیم. به عنوان تمرین تکرار اثبات‌های قبلی توصیه می‌کنیم خواننده بررسی کند که تعداد جواب‌های معادله‌ی $x_2^2 = x_1^2 + x_0^2$ در $P^2(\mathbb{F}_q)$ برابر $q + 1 = p^k + 1$ است. همچنین اگر $p = 3k + 1$ باشد و χ' و λ' کاراکترهای مرتبه‌ی سه روی $\mathbb{F}_q$، آن‌گاه تعداد جواب‌های معادله‌ی $x^3 + y^3 = z^3$ در فضای تصویری برابر $q + 1 + J(\lambda', \lambda') + J(\chi', \chi')$ خواهد بود. به علاوه اگر χ و λ کاراکترهای مرتبه‌ی سه روی $\mathbb{F}_p$ باشند، می‌توان نشان داد $J(\chi', \chi') = -(-J(\chi, \chi))^k$ و $J(\lambda', \lambda') = -(-J(\lambda, \lambda))^k$؛ لذا اگر $\pi = J(\chi, \chi)$، تعداد جواب‌ها $p^k + 1 - (-\pi)^k - (-\overline{\pi})^k$ خواهد بود.

نتیجه ۱۸.۵. اگر p عددی اول باشد و $3|p-1$ و χ یکی از دو کاراکتر مرتبه سه به پیمانه‌ی p باشد و $\pi = J(\chi, \chi)$، آن‌گاه تعداد جواب‌های معادله‌ی $x^3 + y^3 = 1$ در میدان $\mathbb{F}_{p^k}$ (با احتساب نقاط در بی‌نهایت) برابر $p^k + 1 - (-\pi)^k - (-\overline{\pi})^k$ است.

۶. تابع زتای یک خم جبری

منظور ما از یک خم جبری آفین روی میدان F مجموعه جواب‌های یک معادله چندجمله‌ای به شکل $f(x, y) = 0$ است. مجموعه جواب‌های معادله همگن متناظر آن روی فضای تصویری را یک خم جبری تصویری گوییم. اولین بار امیل آرتین با الهام از تابع زتای ریمان و تابع زتای ددکیند، مفهوم تابع زتای یک خم جبری روی یک میدان متناهی را در تز دکترای خود مطرح کرد. پس از آرتین، آندره ویل تابع زتا را برای یک واریته‌ی جبری دل‌خواه تعریف کرد که بعداً به آن اشاره خواهیم کرد. تعریفی که آرتین از تابع زتای یک خم جبری ارائه داده، تعمیم طبیعی تابع زتای ریمان و ددکیند است و شباهت بین این توابع زتا را بیش‌تر نشان می‌دهد؛ اما نسبت به تعریف ویل جامعیت کمتری دارد. به علاوه تعریف ویل بسیار راحت‌تر قابل بیان است. به همین دلیل ما در این بخش تعریف ویل را در نظر خواهیم گرفت و در بخش هفتم، تعریف آرتین را خواهیم آورد.

تعریف ۱.۶. فرض کنید یک خم جبری (آفین یا تصویری) با معادله‌ی $f(x, y) = 0$ داده شده است که $f \in \mathbb{F}_p[x, y]$ چندجمله‌ای تحویل ناپذیر است. اگر تعداد جواب‌های معادله $f(x, y) = 0$ در میدان $\mathbb{F}_{p^k}$ را با N_k نشان دهیم آنگاه تابع زتای این خم جبری روی میدان $\mathbb{F}_p$ به شکل زیر تعریف می‌شود

$$\zeta(s) = exp\left(\sum_{k=1}^{\infty} \frac{N_k p^{-sk}}{k}\right)$$

که منظور از exp تابع نمایی است و s مختلط است.

با توجه به اینکه N_k در حالت خم آفین از p^{2k} و در حالت خم تصویری از $p^{2k} + p^k + 1$ بیشتر نیست (چرا؟)، لذا مجموع فوق برای $Re(s) > 2$ همگراست. در واقع با تقریب‌های بهتر برای N_k می‌توان نشان داد برای $Re(s) > 1$ همگراست.

نمایش متداول دیگری نیز برای تابع زتا وجود دارد که از تغییر متغیر $T = p^{-s}$ حاصل می‌شود. لذا تعریف می‌کنیم

$$Z(T) = exp\left(\sum_{k=1}^{\infty} \frac{N_k T^k}{k}\right)$$

بنابراین خواهیم داشت $Z(p^{-s}) = \zeta(s)$. این دو تابع تفاوت چندانی با هم ندارد و با یک تغییر متغیر ساده به هم تبدیل می‌شوند، دلیل تعریف Z صرفاً این است که گاهی کار کردن با تابع Z نسبت به ζ راحت‌تر است. در منابع مختلف هر دو این توابع را به عنوان تابع زتای خم جبری معرفی می‌کنند.

در ادامه تابع زتا را برای دو خم ساده که تعداد نقاط آن‌ها را در قسمت‌های قبل بدست آوردیم، محاسبه خواهیم کرد. ابتدا به عنوان یک مثال ساده چندجمله‌ای $f(x,y) = x^۲ + y^۲ - ۱$ را در نظر بگیرید. خم جبری تصویری متناظر آن را در نظر بگیرید. پیش‌تر نشان دادیم که تعداد نقاط این خم روی $\mathbb{F}_{p^k}$ برابر $p^k + ۱$ است. بنابراین $N_k = ۱ + p^k$ لذا داریم

$$Z(T) = exp\left(\sum_{k=۱}^{\infty} \frac{(p^k + ۱)T^k}{k}\right) = exp\left(\sum_{k=۱}^{\infty} \frac{p^kT^k + T^k}{k}\right)$$

$$= exp\left(\sum_{k=۱}^{\infty} \frac{T^k}{k}\right) exp\left(\sum_{k=۱}^{\infty} \frac{(pT)^k}{k}\right)$$

$$= exp(-log(۱ - T))exp(-log(۱ - pT)) = \frac{۱}{۱ - T} \times \frac{۱}{۱ - pT}$$

$$= \frac{۱}{(۱ - T)(۱ - pT)}$$

بنابراین تابع $Z(T)$ یک تابع گویا بر حسب T است. می‌توان تابع $\zeta(s)$ را هم با جای‌گذاری $T = p^{-s}$ در رابطه‌ی فوق به دست آورد. دقت کنید تابع $\zeta(s)$ تنها برای $Re(s) > ۱$ هم‌گرا بود؛ اما تابع فوق برای هر s هم‌گراست. لذا این رابطه در واقع یک توسیع مرومورف از تابع زتا به کل صفحه‌ی مختلط بدست می‌دهد.

حال سراغ مثالی اساسی‌تر $f(x,y) = x^۳ + y^۳ - ۱$ می‌رویم. با همان نمادهای به‌کاررفته در نتیجه ۱۸.۵ کار خواهیم کرد. می‌خواهیم تابع زتای خم تصویری متناظر با f را حساب کنیم. طبق نتیجه ۱۸.۵ داریم $N_k = p^k + ۱ - (-\pi)^k - (-\overline{\pi})^k$. بنابراین

$$Z(T) = exp\left(\sum_{k=۱}^{\infty} \frac{\left(p^k + ۱ - (-\pi)^k - (-\overline{\pi})^k\right) T^k}{k}\right)$$

$$= exp\left(\sum_{k=۱}^{\infty} \frac{(pT)^k + T^k}{k}\right) exp\left(\sum_{k=۱}^{\infty} \frac{-(-\pi T)^k - (-\overline{\pi}T)^k}{k}\right)$$

$$= \frac{exp\left(\sum_{k=۱}^{\infty} \frac{-(-\pi T)^k}{k}\right) exp\left(\sum_{k=۱}^{\infty} \frac{-(-\overline{\pi}T)^k}{k}\right)}{(۱ - T)(۱ - pT)}$$

$$= \frac{(۱ + \pi T)(۱ + \overline{\pi}T)}{(۱ - T)(۱ - pT)}$$

همان طور که می‌بینید تابع Z برای این خم هم یک تابع گویا بر حسب T شد و این رابطه توسیع تحلیلی مرومورفی برای Z و ζ به کل صفحه می‌دهد. به اضافه تابع Z دارای دو ریشه $-\frac{۱}{\pi}$ و $-\frac{۱}{\overline{\pi}}$ هم می‌باشد. طبق قضایایی که برای جمع‌های ژاکوبی ثابت کرده بودیم می‌دانیم $|\pi| = \sqrt{p}$ لذا نرم این دو ریشه $p^{-\frac{۱}{۲}}$ است. پس اگر تغییر متغیر $T = p^{-s}$ را اعمال کنیم تابع $\zeta(s)$ دارای ریشه‌هایی با بخش حقیقی $\frac{۱}{۲}$ است (دقت کنید $|p^{-s}| = p^{-Re(s)}$). سعی کنید همه‌ی این ریشه‌ها را دقیقاً بیابید.

امیل آرتین در سال ۱۹۲۳ در تز دکترای خود تابع زتا را برای خم‌هایی به شکل $y^۲ = P(x)$ که به آن‌ها خم‌های ابربیضوی[۱] می‌گویند، برای برخی چندجمله‌ای‌های خاص P محاسبه کرد. آرتین از روی این محاسبات حدس زد که برای هر خم جبری تصویری بدون تکینگی، تابع $Z(T)$ یک تابع گویا است و به علاوه تمام ریشه‌های آن دارای نرم $p^{-\frac{۱}{۲}}$ هستند یا به عبارت دیگر همه ریشه‌های تابع $\zeta(s)$ روی خط $Re(s) = \frac{۱}{۲}$ قرار دارند. تعریف تکینگی را در ادامه آورده‌ایم.

تعریف ۲.۶. گوییم خم $f(x,y) = ۰$ در نقطه‌ی $(x_۰, y_۰)$ دارای تکینگی است هرگاه $f(x_۰, y_۰) = ۰$ (یعنی آن نقطه روی خم باشد) و به علاوه $\frac{\partial f}{\partial x}(x_۰, y_۰) = ۰$ و $\frac{\partial f}{\partial y}(x_۰, y_۰) = ۰$.

(دقت کنید مشتق یک چندجمله‌ای روی هر میدان دلخواه به طور صوری قابل تعریف است.)

[1] hyperelliptic curve

حدس آرتین دوگان حدس ریمان برای تابع زتای ریمان است. در بخش بعدی بیش‌تر درباره‌ی شباهت این دو صحبت می‌کنیم. در سال ۱۹۳۴ هلموت هسه[1] موفق شد حدس‌های آرتین را برای حالتی که P درجه‌ی سه باشد (حالت خم بیضوی) ثابت کند. در سال ۱۹۴۸ آندره ویل حدس‌های آرتین را برای خم دل‌خواه ثابت کرد و تعمیمی از حدسیات آرتین برای واریته‌ی تصویری دل‌خواه ارائه کرد.

۷. توابع زتا

در این بخش تعریف تابع زتای ریمان و ددکیند را یادآوری می‌کنیم و نحوه‌ی تعریف تابع زتا توسط آرتین را بازگو می‌کنیم. هدف این بخش صرفاً دادن شهودی درباره شباهت این دو نوع تابع زتا است و چیز خاصی اثبات نخواهیم کرد. هم‌چنین در بخش‌هایی فرض می‌کنیم خواننده با مفاهیم اولیه‌ی نظریه جبری اعداد آشناست.

۱.۷. تابع زتای ریمان. همان‌طور که احتمالاً می‌دانید، در اواسط قرن نوزدهم، مطالعه‌ی حدس اعداد اول که توسط گاوس مطرح شده بود، ریمان را به سمت مطالعه‌ی تابع زتا که به صورت زیر تعریف می‌شود سوق داد.

$$\zeta(s) = \sum_{n=۱}^{\infty} \frac{۱}{n^s}$$

در واقع افراد مختلفی از جمله اویلر نیز این تابع را برای s های حقیقی مطالعه کرده‌بودند؛ ولی ریمان احتمالاً اولین شخصی است که این تابع را به عنوان تابعی مختلط مطالعه کرده است. به سادگی می‌توان دید این تابع برای $Re(s) > ۱$ یک تابع هولومورف است. ریمان نشان داد این تابع گسترشی مرومورف به کل صفحه‌ی مختلط دارد که تنها یک قطب ساده در $s = ۱$ خواهد داشت. اگر به یاد داشته باشید، تابع زتای یک خم جبری تصویری نیز برای $Re(s) > ۱$ تابعی هولومورف بود و اگر حدس آرتین مبنی بر گویا بودن تابع $Z(T)$ را بپذیریم گسترشی مرومورف به کل صفحه خواهد داشت.

ریمان متوجه شد که می‌تواند حدس گاوس در مورد توزیع اعداد اول را به مکان صفرهای توسیع مرومورف تابع زتای ریمان مرتبط سازد. کلید ارتباط بین تابع زتا و اعداد اول، فرمول حاصل ضربی زیر است که اویلر نیز از آن مطلع بود و درستی آن صرفاً به دلیل وجود یکتایی تجزیه در اعداد طبیعی است.

$$\sum_{n=۱}^{\infty} \frac{۱}{n^s} = \prod_{p\in Primes} \left(\sum_{n=۱}^{\infty} \frac{۱}{p^{ns}}\right) = \prod_{p\in Primes} \left(\frac{۱}{۱-p^{-s}}\right)$$

به دلایلی که ذکر شد ریمان به مطالعه‌ی صفرهای این تابع علاقه‌مند شد. می‌توان نشان داد تابع زتای ریمان در نقاط $s = -۲k$ که k عددی طبیعی است ریشه دارد. اگر این ریشه‌ها را کنار بگذاریم، ریمان حدس زد که تمام ریشه‌های دیگر تابع زتا روی خط $Re(s) = \frac{۱}{۲}$ قرار دارند. این حدس که به فرضیه‌ی ریمان مشهور است، همچنان یکی از مهم‌ترین مسائل باز در نظریه‌ی اعداد و در تمام ریاضیات است.

۲.۷. میدان‌های عددی و تابع زتای ددکیند. ددکیند از بنیان‌گذاران نظریه جبری اعداد در قرن نوزدهم بود. او با الهام از کارهای ریمان، تابع زتا را برای یک توسیع متناهی دلخواه از اعداد گویا تعریف کرد که در این بخش آن را توضیح خواهیم داد. فرض کنید α یک عدد جبری روی $\mathbb{Q}$ و لذا $K = \mathbb{Q}(\alpha)$ یک توسیع متناهی $\mathbb{Q}$ باشد. به چنین میدان‌هایی میدان‌های عددی[2] گویند. حلقه‌ی اعداد صحیح میدان عددی K به صورت $O_K = K \cap \Omega$ تعریف می‌شود که Ω حلقه‌ی همه‌ی اعداد صحیح جبری است که در بخش ۲ آن را معرفی کردیم. حلقه‌ی O_K در نظریه اعداد کاربرد زیادی دارد. این حلقه‌ها در حالت کلی دامنه‌ی تجزیه‌ی یکتا[3] نیستند. کارهای کومر و ددکیند برای حل این مشکل، منجر به تعریف مفهوم ایده‌آل در حلقه‌ها شد. در واقع گرچه این حلقه‌ها دارای تجزیه یکتا نیستند؛ اما هر ایده‌آل در این حلقه‌ها را می‌توان به صورت یکتا به حاصل‌ضرب ایده‌آل‌های اول تجزیه کرد. یعنی یکتایی تجزیه در مورد ایده‌آل ها برقرار است. به چنین حلقه‌ای یک حوزه‌ی ددکیند می‌گویند. (حوزه‌ی ددکیند یک حوزه‌ی صحیح است که هر ایده‌آل آن را بتوان به طور یکتا به ضرب ایده‌آل‌های اول تجزیه کرد.)

[1] Helmut Hasse
[2] number fields
[3] unique factorization domain (UFD)

برای هر ایده‌آل I ناصفر در O_K، نرم I که آن را با نماد $N(I)$ نشان می‌دهیم، به صورت $|\frac{O_K}{I}|$ تعریف می‌شود. می‌توان نشان داد در حلقه‌هایی به صورت O_K (و نه در یک حوزه‌ی ددکیند دل‌خواه) نرم هر ایده‌آل ناصفر متناهی است. مثلا برای حالت $K = \mathbb{Q}$ حلقه‌ی O_K برابر $\mathbb{Z}$ خواهد بود و لذا ایده‌آل‌های ناصفر آن به صورت $n\mathbb{Z}$ هستند، که n عددی طبیعی است و نرم این ایده‌آل n است. لذا اعداد طبیعی دقیقاً نرم ایده‌آل‌های $\mathbb{Z}$ هستند.

ددکیند با الهام از کارهای ریمان، برای هر میدان عددی K تابع زتای ددکیند آن را به صورت زیر تعریف کرد:

$$\zeta_K(s) = \sum_{I \lhd O_K} \frac{1}{N(I)^s}$$

با توجه به وجود یکتایی تجزیه برای ایده‌آل‌های حلقه‌ی O_K فرمول حاصل‌ضربی مشابهی برای این تابع زتا نیز به صورت زیر برقرار است

$$\sum_{I \lhd O_K} \frac{1}{N(I)^s} = \prod_{\wp} \left(\frac{1}{1 - N(\wp)^{-s}} \right)$$

که حاصل‌ضرب روی همه‌ی ایده‌آل‌های اول ناصفر $\wp$ است.

ددکیند نشان داد این تابع گسترش مرومورفی به کل صفحه‌ی مختلط دارد و نیز حدس زد که همانند تابع زتای ریمان، تمام ریشه‌های نابدیهی (ریشه‌هایی که بخش حقیقی آن ها بین ۰ و ۱ است) این تابع نیز روی خط $Re(s) = \frac{1}{2}$ قرار دارند. به این حدس، حدس ریمان گسترش یافته[1] می‌گویند.

۳.۷. میدان‌های تابعی و ایده‌ی آرتین. در نظریه‌ی اعداد تشابه جالبی که بین میدان‌های عددی و میدان‌های تابعی یک متغیره روی میدان‌های متناهی وجود دارد، الهام‌بخش بسیاری از تعاریف در هر یک از این دو زمینه بوده است. ابتدا کمی در مورد میدان‌های تابعی یک متغیره روی $\mathbb{F}_p$ صحبت می‌کنیم.

اگر میدان $\mathbb{F}_p(x)$ را به عنوان آنالوگی برای میدان $\mathbb{Q}$ در نظر بگیریم، حلقه‌ی $\mathbb{F}_p[x]$ نیز آنالوگ $\mathbb{Z}$ خواهد بود. در این تصویر، آنالوگی طبیعی برای میدان‌های عددی –که توسیع‌هایی به شکل $\mathbb{Q}(\alpha)$ از $\mathbb{Q}$ هستند که α روی $\mathbb{Q}$ جبری است– توسیع‌هایی به شکل $\mathbb{F}_p(x)(y)$ از $\mathbb{F}_p(x)$ هستند که y روی $\mathbb{F}_p(x)$ جبری است. لذا y در یک چندجمله‌ای با ضرایب در $\mathbb{F}_p(x)$ صدق می‌کند؛ یا به بیان دیگر x و y در یک چندجمله‌ای دو متغیره مانند $f(x,y)$ با ضرایب در $\mathbb{F}_p$ صدق می‌کنند. لذا یک آنالوگ برای حلقه‌ی O_K در یک میدان عددی K می‌تواند حلقه‌ی $O = \frac{\mathbb{F}_p[x,y]}{(f)}$ باشد. مشابه O_K این حلقه نیز یک حوزه‌ی ددکیند خواهد بود و می‌توان نشان داد (مثلاً با کمک لم زاریسکی) که هر ایده‌آل ماکسیمال آن دارای نرم متناهی است. از آن جا که در یک حوزه‌ی ددکیند ایده‌آل‌های ناصفر اول و ماکسیمال یکی هستند بنابراین می‌توان مشابه تابع زتای ددکیند، برای آن نیز تابع زتا را به صورت زیر تعریف کرد

$$\zeta(s) = \prod_{\wp \lhd O} \left(\frac{1}{1 - N(\wp)^{-s}} \right)$$

که حاصل ضرب روی همه‌ی ایده‌آل‌های اول ناصفر (ماکسیمال) است. این همان تابع زتای خم جبری f است که ما آن را در بخش‌های قبلی به شکلی دیگر تعریف کردیم. تعریفی که اینجا آوردیم همان تعریف آرتین است که وعده داده بودیم. آرتین حدس زد که همان طور که این تابع آنالوگ تابع زتای ریمان و ددکیند است، باید مشابهاً دارای گسترش مرومورف باشد و احتمالاً ریشه‌های نابدیهی آن روی خط $Re(s) = \frac{1}{2}$ باشند. محاسبات آرتین برای تعداد زیادی از خم‌های ابربیضوی، این حدس‌ها را تصدیق می‌کرد.

در واقع قبل از آرتین هم ریاضیدانی آلمانی به نام کُرنبلام[2] تابع زتا را برای حالت خاص $O = \mathbb{F}_p[x]$ بررسی کرده بود؛ ولی آرتین اولین کسی بود که تابع زتا را برای توسیع‌های درجه دو این میدان‌ها (یا معادلاً خم‌های ابربیضوی) مطالعه کرد و حدس‌های آنالوگ فرضیه‌ی ریمان را در این حالات مطرح نمود. خواننده برای دیدن ایده‌های کرنبلام می‌تواند به منبع [5] مراجعه کند.

[1] extended Riemann hypothesis
[2] Kornblum

۸. حدسیات ویل

همان طور که قبلاً گفتیم، هسه در سال ۱۹۳۴ موفق شد حدس‌های آرتین را برای خم‌های بیضوی بطور کامل ثابت کند و آندره ویل در ۱۹۴۸ آن‌ها را در حالت کلی ثابت کرد. در واقع ویل مسئله را در حالتی بسیار کلی‌تر از آنچه آرتین در نظر گرفته بود نیز مطالعه کرد و حدس‌های مهمی در این مورد زد که برخی از آن‌ها تعمیم طبیعی حدس‌های آرتین بودند. در این جا به طور مختصر حدسیات آندره ویل را مطرح می‌کنیم و کمی درباره‌ی تاریخچه‌ی آن‌ها توضیح می‌دهیم.

تا این جا تمام بحث‌هایی که ما مطرح کردیم درباره مجموعه‌ی صفرهای یک چندجمله‌ای دومتغیره $f(x,y)$ بوده است که در واقع همگی خم‌های جبری بوده‌اند. می‌توان هم تعداد متغیرها و هم تعداد معادلات را اضافه کرد. به بیان دقیق‌تر می‌توان مجموعه‌ی صفرهای مشترک m معادله‌ی چندجمله‌ای n متغیره را در نظر گرفت. به چنین مجموعه‌ای که در واقع زیرمجموعه‌ای از $A^n(F)$ است یک واریته‌ی جبری آفین گویند. اگر معادلات را چندجمله‌ای‌های همگن در نظر بگیرید، مجموعه صفرها روی فضای تصویری خوش‌تعریف خواهد بود که چنین مجموعه‌ای را یک واریته‌ی جبری تصویری می‌گوییم. اگر همه‌ی چندجمله‌ای ها را با ضرایب در میدان $\mathbb{F}_p$ در نظر بگیریم، می‌توان برای هر k تعداد جواب‌های دستگاه در میدان $\mathbb{F}_{p^k}$ را در نظر گرفت. این تعداد را N_kبنامید. می‌توان تابع زتای واریته را به طور مشابه به شکل زیر تعریف کرد.

$$\zeta(s) = exp\left(\sum_{k=1}^{\infty} \frac{N_k p^{-sk}}{k}\right)$$

یا مشابهاً

$$Z(T) = exp\left(\sum_{k=1}^{\infty} \frac{N_k T^k}{k}\right)$$

آندره ویل با مطالعه‌ی این تابع زتا برای واریته‌های تصویری دل‌خواهی که تکینگی ندارند و با الهام‌گرفتن از ایده‌های توپولوژی جبری به حدسیات معروف خود رسید. در واقع نکته‌ی درخشان در کارهای آندره ویل توجه به ارتباط این مسئله (با وجود ماهیت گسسته آن) با قضایایی از توپولوژی جبری بود.

اینجا اشاره‌ای به صورت حدسیات ویل می‌کنیم. حدسایت ویل درمورد تابع زتای یک واریته‌ی جبری تصویری بدون نقطه‌ی تکینگی روی یک میدان متناهی، مثلاً میدان $\mathbb{F}_p$ است.

حدس اول ویل این است که تابع $Z(T)$ برای چنین واریته‌ای حتماً تابعی گویا بر حسب T است. در واقع حدس ویل دقیق‌تر است و حتی فرم این تابع گویا را پیش‌بینی می‌کند.

حدس دوم ویل این است که ریشه‌های $\zeta(s)$ برای چنین واریته‌هایی، همگی روی خط $Re(s) = \frac{1}{2}$ هستند. این حدس را فرضیه ریمان برای میدان‌های تابعی روی یک میدان متناهی گویند.

حدس سوم آندره ویل این است که تابع زتا در یک معادله تابعی (مشابه معادله تابعی که برای تابع زتای ریمان و ددکیند وجود دارد) که $\zeta(s)$ و $\zeta(n-s)$ را به هم مرتبط می‌کند صدق می‌کند. در واقع این معادله تابعی به شکل زیر است.

$$\zeta(n-s) = \pm p^{\frac{nE}{2} - Es}\zeta(s)$$

در این رابطه n بعد واریاته (مثلا برای خم‌ها $n = 1$ است) و E شاخص اویلر است که در این مقاله به آن‌ها اشاره‌ای نمی‌کنیم. خواننده می‌تواند به کتاب‌های استاندارد هندسه‌ی جبری مراجعه کند.

علاوه بر این سه حدس ویل حدس دیگری نیز دارد که درجه‌ی چندجمله‌ای‌هایی را که در تجزیه تابع گویای $Z(T)$ ظاهر می‌شوند، به عدد بتی[1] یک فضای توپولوژیک مناسب مرتبط می‌سازد. در مورد این حدس نیز صحبت بیشتری نمی‌کنیم.

آندره ویل علاوه بر مطرح‌کردن این حدس‌ها مسیری کلی به سمت اثبات آن‌ها نیز ترسیم کرد. در واقع ویل متوجه شده‌بود وجود یک نظریه‌ی کوهومولوژی استاندارد برای واریته‌های روی یک میدان متناهی، مشابه نظریه کوهومولوژی که برای واریته‌های مختلط شناخته شده بود، می‌تواند برخی حدس‌های او را نتیجه دهد. مشاهدات ویل انگیزه‌ی اصلی برای تعریف نظریه‌های کوهومولوژی مختلف برای واریته‌های مجرد در سال‌های آتی شد و مسیر هندسه‌ی جبری را در نیمه‌ی دوم قرن بیستم مشخص کرد. حدس اول ویل یعنی گویا بودن $Z(T)$ را برنارد دوورک[2] در ۱۹۶۰ با استفاده از روش‌های pـادیک ثابت کرد. با الهام از

[1] Betti number
[2] Bernard Dwork

ایده‌هایی که اولین بار توسط ژان پیر سِر[1] مطرح شده بود، الکساندر گروتندیک[2] با همکاری مایکل آرتین[3] موفق شدند در ۱۹۶۵ یک نظریه کوهومولوژی مناسب ایجاد کنند که سه تا از حدسیات ویل (بجز فرضیه‌ی ریمان برای میدان‌های تابعی) را نتیجه می‌داد. گروتندیک برای این نتایج (و نتایجی دیگر) در سال ۱۹۶۶ برنده‌ی جایزه‌ی فیلدز شد. سرانجام سخت‌ترین قسمت حدسیات ویل یعنی فرضیه ریمان در حالت میدان‌های تابعی روی یک میدان متناهی در ۱۹۷۴ توسط پیر دلین[4] ثابت شد. دلین برای این اثبات در ۱۹۷۸ جایزه‌ی فیلدز را برد.

مراجع

[1] Fulton, W. (2008). *Algebraic Curves: An Introduction to Algebraic Geometry.* W. A. Benjamin.

[2] Ireland, K., & Rosen, M. (1982). *A classical introduction to modern number theory*. Graduate texts in mathematics (Vol. 84). New York, NY: Springer New York.

[3] Weil, A. (1949). Numbers of solutions of equations in finite fields. *Bulletin of the American Mathematical Society*, 55(5), 497-508.

[4] Morandi, P. (1996). *Field and galois theory*. Graduate texts in mathematics (Vol. 167). New York, NY: Springer New York.

[5] Kato, K., Kurokawa, N., Saitō, T., Kurihara, M. (2000). Number Theory: introduction to class field theory. American Mathematical Soc.

* دانشجوی دکتری ریاضی، دانشگاه هایدلبرگ

رایانامه: alireza.shavali@iwr.uni-heidelberg.de

[1] Jean-Pierre Serre
[2] Alexander Grothendieck
[3] Michael Artin
[4] Pierre Deligne