فرهنگ و اندیشهٔ ریاضی

سال ۴۱، شمارهٔ ۷۱ (پاییز و زمستان ۱۴۰۱) صص. ۱۷۳ تا ۱۹۸

چرا آیزنشتاین محک آیزنشتاین را اثبات کرد و چرا اصلاً شونمان آن را کشف کرد*

دیوید آرچیبالد کاکس

ترجمهٔ آزاده نیک‌سرشت

چکیده. در این مقاله به بررسی تاریخچهٔ محک تحویل‌ناپذیری آیزنشتاین می‌پردازیم و شرح می‌دهیم که چطور تئودور شونمان این محک را قبل از آیزنشتاین کشف کرد. آیزنشتاین و شونمان از کتاب تحقیقات حسابی گاوس الهام گرفته بودند، اگرچه مسیرهای بسیار متفاوتی را برای اکتشافات خود در پیش گرفتند. در این مقاله موضوعات گوناگونی از نظریهٔ اعداد در قرن نوزدهم، از جمله لم گاوس، میدان‌های متناهی، خم پروانه، انتگرال‌های بیضوی، گروه‌های آبلی، اعداد صحیح گاوسی، و لم هِنزل مورد بحث قرار خواهند گرفت.

محک تحویل‌ناپذیری آیزنشتاین جزو آموخته‌های دوران تحصیل هر ریاضی‌دانی است. من نخستین‌بار زمانی‌که دانشجوی مقطع کارشناسی بودم آن را آموختم و مثل بسیاری از افراد دیگر، تحت تأثیر قدرت و سادگی آن قرار گرفتم. این مقاله به شرح تاریخچهٔ غنی و شگفت‌آورِ پیدایش محک آیزنشتاین و به‌ویژه نقش تئودور شونمان[1] در این زمینه می‌پردازد.

برای بیان این محک، از مقالهٔ دُرورت[2] با عنوان تحویل‌ناپذیری چندجمله‌ای‌ها به سال ۱۹۳۵ آغاز می‌کنیم [۹]. همان‌طورکه احتمالاً انتظار دارید، او مطلب را از آیزنشتاین شروع می‌کند:

عبارات و کلمات کلیدی: محک تحویل‌ناپذیری آیزنشتاین، تئودور شونمان، کارل گاوس، معادلات چندجمله‌ای، تحویل‌پذیری چندجمله‌ای

نوع مقاله: ترویجی؛ تاریخ دریافت: ۱۴۰۰/۱۱/۱۷؛ تاریخ پذیرش: ۱۴۰۱/۲/۱۸

* Cox, D. A., Why Eisenstein proved the Eisenstein criterion and why Schönemann discovered it first, *Amer. Math. Monthly*, **118** (2011), 3-21.

[1] Theodor Schönemann [2] Harold L. Dorwart

doi: 10.30504/mct.2023.1268.1883

اولین و شاید معروف‌ترین محک تحویل‌ناپذیری، قضیهٔ شونمان–آیزنشتاین است:
اگر در یک چندجمله‌ای صحیح

$$a_0 x^n + a_1 x^{n-1} + \cdots + a_n$$

همهٔ ضرایب به‌جز a_0 بر عدد اول p بخش‌پذیر باشند و a_n بر p^2 بخش‌پذیر نباشد، آنگاه چندجمله‌ای تحویل‌ناپذیر است.

اولین نکتهٔ عجیب اینجاست که دُرورت نام شونمان را قبل از آیزنشتاین می‌آورد. سپس او کاربردی کلاسیک از قضیه می‌آورد:

یک کاربرد مهم این قضیه، اثبات تحویل‌ناپذیریِ به‌اصطلاح «چندجمله‌ای دایره‌بُری»

$$f(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + 1$$

است که در آن p عددی اول است.
اگر به‌جای $f(x)$، $f(x+1)$را درنظر بگیریم، که در آن

$$f(x+1) = \frac{(x+1)^p - 1}{(x+1) - 1} = x^{p-1} + \binom{p}{1} x^{p-2} + \cdots + p,$$

قضیه به‌طور مستقیم قابل اعمال است و تحویل‌ناپذیریِ $f(x+1)$، تحویل‌ناپذیریِ $f(x)$ را نتیجه می‌دهد.

ترکیب «شونمان–آیزنشتاین» در اوایل قرن بیستم رایج بود. یک استثناء کتاب جذاب دُری تحت عنوان پیروزی ریاضیات [۸] به سال ۱۹۳۳است؛ که در آن عبارت «قضیهٔ شونمان»[1] به کار رفته است. استثناء دیگر، کتاب جبر نوین [۲۹] وان دِر واردن به سال ۱۹۳۰ است که در آن عبارت «قضیهٔ آیزنشتاین» دیده می‌شود.[2]

با توجه به تأثیر کتاب وان دِر واردن بر نسل‌های بعدی نویسندگان کتاب‌های درسی، می‌توان چگونگی حذف نام شونمان از این قضیه را فهمید. اما چگونه اسم شونمان اولِ عنوان آمده است؟ و موضوع مهم دیگر اینکه چگونه اسم آیزنشتاین به آن اضافه شده است؟ و چرا هر دو اسم آمده است؟ برای پاسخِ این سؤالات، نیاز به بررسی قسمت‌هایی از نظریهٔ اعداد در قرن نوزدهم داریم. موضوع گسترده است و بنابراین بحث من جامع نخواهد بود. ترجیح می‌دهم روی موضوعاتی خاص تمرکز و سیر تحول این مفاهیم را دنبال کنم. نقل قول‌های زیادی خواهم آورد تا روشن کنم که در آن زمان ریاضیات چگونه بود و چگونه به آن می‌پرداختند. بحث خود را با گاوس آغاز می‌کنیم.

---

[2] ویراستِ سال ۱۹۳۰ آن ارجاعی به شونمان دارد که در ویراست دوم به سال ۱۹۳۷ حذف شده است.

[1] Satz von Schoenemann

گاوس

تحقیقات حسابی [۱۳]، منتشرشده در سال ۱۸۰۱، حاوی مفاهیم شگفت‌انگیزی از ریاضیات است. در یک مورد گاوس ثابت می‌کند وقتی p اول باشد، چندجمله‌ای دایره‌بری $x^{p-1}+\cdots+x+1$ تحویل‌ناپذیر است. اثبات او نمایشی صریح از ریشه‌ها را به کار می‌گیرد و اثبات آسانی نیست. بااین‌حال، او از نتیجهٔ کلی زیر نیز استفاده می‌کند که تحویل‌ناپذیری روی $\mathbb{Z}$ را به تحویل‌ناپذیری روی $\mathbb{Q}$ مرتبط می‌کند:

۴۲.

اگر ضرایب $A, B, C \ldots N; a, b, c \ldots n$ از دو تابع به‌صورت

$$x^m + Ax^{m-1} + Bx^{m-2} + Cx^{m-3} \cdots + N \cdots\cdots (P)$$
$$x^\mu + ax^{\mu-1} + bx^{\mu-2} + cx^{\mu-3} \cdots + n \cdots\cdots (Q)$$

همگی گویا بوده و البته همگی صحیح نباشند، و اگر حاصل‌ضرب (P) و (Q)

$$= x^{m+\mu} + \mathfrak{A}x^{m+\mu-1} + \mathfrak{B}x^{m+\mu-2} + \text{etc.} + \mathfrak{Z}$$

باشد، آنگاه همهٔ ضرایب $\mathfrak{A}, \mathfrak{B} \ldots \mathfrak{Z}$ نمی‌توانند صحیح باشند.

این همان است که ما آن را «لم گاوس» می‌نامیم. اثبات او اساساً همان اثباتی است که در کتاب‌های جبر مجرد آمده است؛ گرچه او نتیجه را به شکلی کاملاً متفاوت بیان می‌کند و هرگز اصطلاح «چندجمله‌ای» را به‌کار نمی‌برد. گاوس همچنین از سه نقطه . . .، که امروزه در نگارش مرسوم است، استفاده نمی‌کند.

یکی دیگر از نتایج اصلی کتاب تحقیقات اثبات گاوس برای حل‌پذیری $x^n - 1 = 0$ به‌وسیلهٔ رادیکال‌هاست. نگاه جدید به حل‌پذیری به‌وسیلهٔ رادیکال‌ها امکان معرفیِ ریشه‌های دلخواهِ واحد را فراهم می‌سازد، که نشان می‌دهد $x^n - 1 = 0$ به‌وضوح حل‌پذیر است. گاوس ترجیح داد که روش استقراییِ لاگرانژ را به‌کار گیرد؛ روشی که ریشه‌ها را به‌طور بازگشتی با استفاده از چندجمله‌ای‌هایی از درجهٔ اکیداً کوچک‌تر از آن‌هایی که به‌وسیلهٔ رادیکال‌ها حل‌پذیرند می‌سازد. در کتاب‌های جدید، این روشْ توصیف صریحی از میدان‌های میانیِ توسیع $\mathbb{Q} \subseteq \mathbb{Q}(e^{2\pi i/p})$ به دست می‌دهد که در آن p عددی اول است. چون $x^{p-1}+\cdots+x+1$ تحویل‌ناپذیر است، درجهٔ این توسیع $p-1$ است. از همین‌جاست که گاوس نتیجهٔ شگفت‌آور خود را در مورد تقسیم دایره به n کمان مساوی با استفاده از خط‌کش و پرگار به دست آورد.

پاراگراف دوم از بخش هفتمِ تحقیقات با یک نقل‌قول معروف آغاز می‌شود:

> اصول نظریه‌ای که می‌خواهیم شرح دهیم درواقع بسیار فراتر از آن چیزی است که ما اشاره می‌کنیم. زیرا آن‌ها نه‌تنها برای توابع مستدیر بلکه برای توابع متعالی نیز به کار می‌روند؛ برای مثال، برای توابعی که به انتگرال $\int \frac{dx}{\sqrt{(۱-x^۴)}}$ و همچنین به انواع مختلف هم‌نهشتی‌ها ارتباط دارند. اما چون در حال فراهم کردن کاری بزرگ دربارهٔ آن توابع متعالی هستیم و هم‌نهشتی‌ها را در ادامهٔ این تحقیقات مورد بررسی قرار خواهیم داد، تصمیم گرفته‌ایم که در اینجا فقط توابع مستدیر را بررسی کنیم.

در این نقل‌قول، ارجاع به توابع مستدیر روشن است. اما در مورد توابع متعالی که به انتگرال $\int \frac{dx}{\sqrt{۱-x^۴}}$ بستگی دارند، چطور؟ در اینجا هر ریاضی‌دان قرن نوزدهمی، بی‌درنگ، به یاد پروانهٔ $r^۲ = \cos ۲\theta$ خواهد افتاد که طول کمان آن برابر $۴\int_۰^۱ \frac{dx}{\sqrt{۱-x^۴}}$ است. این انتگرال و رابطهٔ آن با پروانه را برادران برنولی، در اواخر قرن هفدهم، کشف کردند و نقش کلیدی در توسعهٔ مفهوم انتگرال‌های بیضوی، که در قرن هیجدهم توسط فاگنانو[1]، اویلر، و لژاندر گسترش یافت، ایفا کرد. «کار بزرگ» گاوس دربارهٔ این توابع هرگز منتشر نشد؛ اگرچه بخش‌هایی از آن که حاوی مفاهیم ریاضی شگفت‌انگیزی بود، بعد از مرگش پیدا شد ([۳] را ببینید).

نقل‌قول بالا همچنین به «انواع مختلف هم‌نهشتی‌ها» که «در ادامهٔ این تحقیقات» مورد بحث قرار می‌گیرند، اشاره می‌کند. نسخهٔ منتشرشدهٔ تحقیقات حاوی هفت بخش بود؛ اما گاوس پیش‌نویسی از بخش هشتم تحت عنوان تحقیقات کلی دربارهٔ هم‌نهشتی[2] را تهیه کرد که در آن هم‌نهشتی‌های چندجمله‌ای‌ها به‌صورت $f(x) \equiv ۰$ (به‌پیمانهٔ عدد اولی مثل p) برای $f \in \mathbb{Z}[x]$ را بررسی کرده بود (ص ۲۱۲-۲۴۲ از [۱۴، ج ۲] یا ۶۰۲-۶۲۹ از [۱۳] را ببینید). به بیان امروزی، گاوس حلقهٔ چندجمله‌ای $\mathbb{F}_p[x]$ را مورد بررسی قرار می‌دهد. بعضی از نتایج او را می‌آوریم:

- وجود و یکتاییِ تجزیه‌های چندجمله‌ای‌ها به پیمانهٔ p.
- فرمولی برای تعداد چندجمله‌ای‌های تکین تحویل‌ناپذیر از درجهٔ n و به پیمانهٔ p. نتیجهٔ او این است

$$\frac{۱}{n}(p^n - \sum p^{\frac{n}{a}} + \sum p^{\frac{n}{ab}} - \sum p^{\frac{n}{abc}} \text{ etc.})$$

که در آن مجموع $\sum p^{\frac{n}{a}}$ روی همهٔ عوامل اولِ متمایز n، $\sum p^{\frac{n}{ab}}$ روی همهٔ جفت‌عوامل اولِ متمایز n محاسبه می‌شوند، و برای بقیهٔ جملات فرمول نیز همین‌طور.

گاوس همچنین نظریه‌ای دربارهٔ میدان‌های متناهی داشت؛ اگرچه رویکرد او برای خوانندگان امروزی

[1] Fagnano [2] Disquisitiones generales de congruentiis

جبر آسان نیست زیراکه او از ریشه‌های هم‌نهشتی‌های چندجمله‌ای‌ها روی‌گردان بود. در اینجا نظر گاوس را دربارهٔ هم‌نهشتی $\xi \equiv 0$ (به پیمانهٔ p)، وقتی‌که ξ چندجمله‌ای با ضرایب صحیح است، می‌آوریم.

> ... اما هیچ چیز مانع از تجزیهٔ ξ به عواملی از بُعد [درجهٔ] دو، سه، یا بیشتر نمی‌شود؛ درنتیجه، به‌نوعی، ریشه‌های موهومی را می‌توان به آن‌ها نسبت داد. درواقع، ما می‌توانستیم همهٔ تحقیقات بعدی‌مان را بی‌اندازه کوتاه کنیم اگر تصمیم به معرفی چنین کمیت‌های موهومی، با همان آزادی‌ای که برخی ریاضی‌دانان جدیدتر اختیار کرده‌اند، داشتیم؛ ...

روی اعداد مختلط، گاوس نخستین کسی بود که وجود ریشه‌های چندجمله‌ای‌ها را ثابت کرد. او از کسانی که به‌سادگی فرض می‌کردند ریشه وجود دارد انتقاد می‌کرد؛ پس او به‌وضوح نمی‌خواست فرض بگیرد که هم‌نهشتی‌های درجهٔ بالا دارای جواب‌اند.

برای شرح کامل‌تری از کار گاوس روی میدان‌های متناهی، خواننده را به [۱۱] ارجاع می‌دهیم. متأسفانه هیچ‌یک از این آثار تا پیش از مرگ گاوس در سال ۱۸۵۵ در دسترس نبودند. به‌ویژه شونمان تا دههٔ ۱۸۴۰، که بسیاری از نتایج گاوس را مجدد کشف کرد، از آن‌ها بی‌خبر بود.

آبل

نظرات پیچیدهٔ گاوس در مورد انتگرال $\int \frac{dx}{\sqrt{1-x^4}}$ در کتاب تحقیقات، آبل را به‌شدت تحت تأثیر قرار داد. او نظریهٔ توابع بیضوی را (مثل ژاکوبی) بر پایهٔ معادلهٔ

$$y^2 = (1 - c^2x^2)(1 + e^2x^2), \tag{1}$$

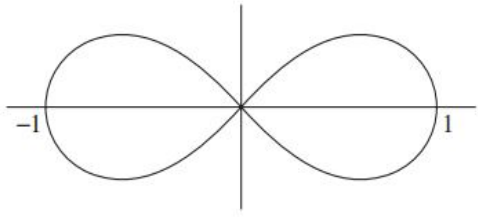
گسترش داد؛ توابع بیضویِ او، توابع معکوسِ انتگرال‌های بیضوی

$$\int \frac{dx}{y} = \int \frac{dx}{\sqrt{(1 - c^2x^2)(1 + e^2x^2)}} \tag{2}$$

بودند. اگر $e = c$ را برابر ۱ بگیریم به $\int \frac{dx}{\sqrt{1-x^4}}$ می‌رسیم. در زمان آبل، می‌دانستند که این انتگرال رابطهٔ نزدیکی با طول کمانِ پروانهٔ شکل ۱ دارد (برای تاریخچهٔ این ارتباط [۳] را ببینید).

درنتیجه، تقسیم یک کمان پروانه به m قطعه کمان با طول مساوی، با شروع از مبدأ، می‌تواند به‌صورت رابطهٔ بین انتگرال‌ها تفسیر شود، که آبل و آیزنشتاین احتمالاً آن را به‌صورت

$$\int_0 dy/\sqrt{1 - y^4} = m \int_0 dx/\sqrt{1 - x^4} \tag{3}$$



شکل ۱. پروانهٔ $r^۲ = \cos ۲\theta$

نوشته‌اند. این «مسئلهٔ m–تقسیم‌کردن»[1] پروانه است. وقتی کل پروانه به m قطعه با طول مساوی تقسیم بشود، معادلهٔ (۳) آبل و آیزنشتاین (و قبل از آن‌ها، در نوشته‌ای منتشرنشده، گاوس) را به چندجمله‌ای $P_m(x)$ از درجهٔ $m^۲$ می‌رساند که مختصات قطبیِ m نقطهٔ تقسیمِ پروانه در آن صدق می‌کند. چگونگی این کار را بعداً، موقع صحبت از آیزنشتاین، بیان خواهیم کرد.

این ریاضیات مورد بحث به‌طرز شگفت‌آوری غنی و وسیع است. مطالعهٔ انتگرال‌های بیضوی همانند (۲) نهایتاً منجر به مطالعهٔ «خم‌های بیضوی»، همانند آنچه در (۱) آمده، می‌شود. کتاب [۲۲] مقدمهٔ خوبی برای خم‌های بیضوی و رابطهٔ آن‌ها با انتگرال‌های بیضوی است. اخیراً، مسئلهٔ m–بخش‌کردن برای انتگرال‌های بیضوی برحسب m نقطهٔ تقسیم روی خم‌های بیضوی بیان شده است. برای اطلاعات بیشتر دربارهٔ این موضوع مهم در نظریهٔ جدید اعداد، [۲۲، ۲۸] را ببینید.

برای آبل و معاصرانش یک سؤال اساسی این بود که آیا معادله‌های چندجمله‌ای، $P_m(x) = ۰$، «از نظر جبری حل‌پذیر»ند یا نه، که امروزه به معنای حل‌پذیری به‌وسیلهٔ رادیکال‌ها است. آبل تنها کسی بود که شایستگی طرح این سؤال را داشت زیراکه درست چهار سال قبل از آن، ثابت کرده بود که، در حالت کلی، درجه‌پنجمی‌ها به‌وسیلهٔ رادیکال‌ها حل‌پذیر نیستند.

آبل در مقالهٔ فوق‌العادهٔ خود تحت عنوان بررسی توابع بیضوی [۱، ص ۲۶۳–۳۸۸] که در مجلدهای ۲ و ۳ از مجلهٔ کرله[2] در سال‌های ۱۸۲۷ و ۱۸۲۸ منتشر شد، معادلهٔ $P_{۲n+۱}(x) = ۰$ را، که از مسئلهٔ $(۲n + ۱)$–تقسیم برای انتگرال‌های بیضویِ (۲) ناشی می‌شود، بررسی می‌کند. گفتنی‌های او دربارهٔ این معادله این است:

---

[2] Journal für die reine und angewandte Mathematik، که توسط آگوست لئوپولت کرِله [August Leopold Crelle] در ۱۸۲۶ تأسیس شد.

[1] m-division problem

بنابراین حل معادلهٔ $P_{۲n+۱} = ۰$ نهایتاً به حل یک معادلهٔ تکین از درجهٔ $۲n+۲$ تحویل[1] می‌شود؛ اما در حالت کلی به‌نظر نمی‌رسد که این معادله از نظر جبری حل‌پذیر باشد. باوجوداین، می‌توان آن را در بسیاری از موارد خاص به‌طور کامل حل کرد؛ برای مثال، وقتی $e = c$، $e = c\sqrt{۳}$، $e = c(۲ \pm \sqrt{۳})$ و غیره. در طی این یادداشت من به این موارد خواهم پرداخت، خصوصاً مورد اول، هم به دلیل سادگی راه‌حلِ آن و هم کاربرد زیبای آن در هندسه، مورد توجه است.

درواقع علاوه‌بر قضیه‌های دیگر به این قضیه رسیدم:

«می‌توان کل محیط پروانه را فقط با استفاده از خط‌کش و پرگار به m بخش تقسیم کرد به‌شرطی‌که m به‌صورت ۲^n یا $۲^{n+۱}$ باشد، که عدد دوم می‌باید اول نیز باشد، یا اینکه m حاصل‌ضربی از اعدادی به این دو صورت باشد.»

همان‌طورکه می‌بینیم، این قضیه، دقیقاً مشابه قضیهٔ آقای گاوس، در مورد دایره است.

تحویل مسئله به معادله‌ای از درجهٔ $۲n + ۲$ با استفاده از روش‌های کلاسیک لاگرانژ انجام می‌شد. نتیجهٔ شگفت‌انگیز ترسیم‌های خط‌کش و پرگار برای پروانه ($e = c$) را می‌توان به‌طور رسمی‌تر به‌صورت زیر بیان کرد.

قضیهٔ آبل دربارهٔ پروانه پروانه را می‌توان با استفاده از خط‌کش و پرگار به m کمانِ با طولِ مساوی تقسیم کرد اگر و فقط اگر m به‌صورت حاصل‌ضربی از اعداد اولِ متمایزِ فرما به تعداد توانی از ۲ باشد.

بعداً در مورد قضیهٔ آبل بیشتر صحبت خواهیم کرد. وقتی از دیدگاه جدیدِ خم‌های بیضوی به مقالهٔ آبل نگاه کنیم، جنبه‌های دیگر نوشتهٔ او نیز به‌همان اندازه شگفت‌انگیزند:

- حالت‌های $e = c$، $e = c\sqrt{۳}$، $e = c(۲ \pm \sqrt{۳})$، و غیره که آبل می‌تواند آن‌ها را با استفاده از رادیکال‌ها حل کند، متناظر با خم‌های بیضوی دارای ضرب مختلط‌اند (برای آشنایی با این مفاهیم به [۴] مراجعه کنید). آبل اولین کسی بود که این دستهٔ مهم از خم‌های بیضوی را شناسایی کرد.
- بنابر نظریهٔ میدان رده[2]، نقاط تقسیمِ خم‌های بیضوی با ضرب مختلط، توسیع آبلی تولید می‌کنند و بنابراین دارای گروه‌های گالوای آبلی‌اند. چون گروه‌های آبلی حل‌پذیرند، از نظریهٔ گالوا نتیجه می‌شود که معادلات مربوط به تقسیم، $P_{۲n+۱}(x) = ۰$، به‌وسیلهٔ رادیکال‌ها حل‌پذیرند.
- در مواقعی‌که این خم‌ها ضرب مختلط نداشتند، آبل محتاط‌تر عمل می‌کرد: «به‌نظر نمی‌رسد که آن‌ها از نظر جبری حل‌پذیر باشند.» بنابر نتایج عمیق سِر[3] دربارهٔ نمایش‌های گالوایِ

[1] reduce [2] class field theory [3] Serre

خم‌های بیضوی [۲۷]، اکنون می‌دانیم که جز تعداد متناهی حالت خاص، این معادلات به‌وسیلهٔ رادیکال‌ها حل‌پذیر نیستند.

اینجا هم با ریاضیات بسیار غنی‌ای مواجه هستیم.

آبل دربارهٔ اینکه چرا معادلاتی به‌صورت $P_{۲n+۱}(x) = ۰$، وقتی خم آن‌ها دارای ضرب مختلط است، به‌وسیلهٔ رادیکال‌ها حل‌پذیرند خیلی فکر کرد. او متوجه شد که دلیل اصلی آن، ساختار ریشه‌ها و نحوهٔ ارتباط آن‌ها با یکدیگر است. نتیجهٔ کلی او در یادداشتی دربارهٔ یک ردهٔ خاص از معادلاتی که از نظر جبری حل‌پذیرند [۱، ص ۴۷۸–۵۰۷] در مجلهٔ کرِله، به سال ۱۸۲۹، قابل مشاهده است. آن مقاله به این صورت آغاز می‌شود:

> اگرچه حل جبریِ معادلات در حالت کلی امکان‌پذیر نیست، باوجوداین معادلات خاصی از همهٔ درجه‌ها وجود دارند که به‌صورت جبری حل‌پذیرند. مثال آن‌ها معادلاتی به‌صورت $x^n - ۱ = ۰$اند. حل این معادلات براساس روابط معینی که بین ریشه‌ها وجود دارد صورت می‌گیرد.

جملهٔ اول اشاره دارد به نتیجهٔ آبل در مورد حل‌ناپذیری معادلاتِ درجهٔ پنجم در حالت کلی و حل معادله $x^n - ۱ = ۰$ که گاوس آن را در کتاب تحقیقات به‌طور مشروح بیان کرده است. آبل برای اینکه منظور خود را از عبارت «روابطی که بین ریشه‌ها وجود دارد» به خواننده منتقل کند، عدد اول n و معادلهٔ دایره‌بری $x^{n-۱} + \cdots + x + ۱ = ۰$ را در نظر می‌گیرد. با فرض $\theta(x) = x^\alpha$ که در آن α یک ریشهٔ اولیه به‌پیمانهٔ n است، ریشه‌ها به‌صورت x، $\theta(x) = x^\alpha$، $\theta^۲(x) = x^{\alpha^۲}$، $\theta^۳(x) = x^{\alpha^۳}$، ...، $\theta^{n-۱}(x) = x^{\alpha^{n-۲}}$ که در آن $\theta^{n-۲}(x) = x$ به دست می‌آیند. آبل، در ادامه، اشاره می‌کند که خاصیت مشابهی در ردهٔ معینی از معادلات ظاهر می‌شود که او آن را در نظریهٔ توابع بیضوی یافته است. او سپس قضیهٔ اصلی مقاله را بیان می‌کند:

> من قضیهٔ زیر را در حالت کلی ثابت کرده‌ام:
> اگر ریشه‌های معادله‌ای از درجهٔ دلخواه به این‌صورت با یکدیگر مرتبط باشند که همهٔ آن‌ها برحسب یکی از آن‌ها، که آن را با x نشان می‌دهیم، به‌صورت گویا قابل بیان باشند؛ و به‌علاوه اگر دو ریشهٔ دلخواه دیگر را با θx و $\theta_۱ x$ نشان دهیم، داشته باشیم $\theta\theta_۱ x = \theta_۱\theta x$، آنگاه معادلهٔ مورد بحث همیشه از نظر جبری حل‌پذیر است . . .

«ردهٔ ویژهٔ»[1] آبل از همهٔ چندجمله‌ای‌هایی که در فرض قضیهٔ او صدق می‌کنند تشکیل شده است. به بیان امروزی، فرض کنید $K \subseteq L$ یک توسیع گالوا با عنصر اولیهٔ[2] α باشد. برای هر عضو σ_i از گروه گالوای $\mathrm{Gal}(L/K)$ یک چندجمله‌ای $\theta_i(x) \in K[x]$ وجود دارد به‌طوری‌که $\sigma_i(\alpha) = \theta_i(\alpha)$.

[1] classe particulière [2] primitive element

اکنون به‌سادگی می‌توان نتیجه گرفت که $\sigma_i\sigma_j(\alpha) = \theta_j(\theta_i(\alpha))$. تعویض اندیس‌ها، صحیح و امکان‌پذیر است ــ دلیل آن را بررسی کنید. چون σ_i بنابر مقدارش روی α تعیین می‌شود، داریم

$$\sigma_i\sigma_j = \sigma_j\sigma_i \quad \Longleftrightarrow \quad \theta_j(\theta_i(\alpha)) = \theta_i(\theta_j(\alpha)).$$

با توجه به اینکه $\theta_i(\alpha)$ها ریشه‌های چندجمله‌ای مینیمال $f(x)$ برای α روی K هستند، ملاحظه می‌کنیم که $f(x)$ متعلق به «ردهٔ ویژه» است اگر و فقط اگر $\mathrm{Gal}(L/K)$ جابه‌جایی باشد. اکنون قضیهٔ آبل به‌سادگی از نظریهٔ گالوا نتیجه می‌شود، زیرا هر گروه گالوای جابه‌جایی، حل‌پذیر است.

آبل علاوه‌بر اثبات قضیهٔ کلی خود، بنا داشت دو کاربرد نیز ارائه دهد:

پس از توسعهٔ این نظریه برای حالت کلی، آن را برای توابع مستدیر و بیضوی به کار خواهم برد.

نسخهٔ منتشرشده در مجلهٔ کِرله دارای بخشی در مورد توابع مستدیر است ولی با پانویسی از کِرله پایان می‌پذیرد:

*) نویسندهٔ این مقاله کاربردهایی برای توابع بیضوی در آینده ارائه خواهد داد.

افسوس که آبل مدت کوتاهی بعد از انتشار آن مقاله درگذشت.

پس از آبل

«ردهٔ ویژهٔ» آبل تاثیر عمیقی روی کرونکر[1]، ژوردان[2]، و وِبر[3] گذاشت. دقیق‌تر اینکه

- در سال ۱۸۵۳، کرونکر [۱۸، ج ۴، ص ۱۱] $f(x) = 0$ را «آبلی» نامید به‌شرطی‌که ریشه‌های آن x، $\theta(x)$، ...، $\theta^{n-1}(x)$، $x = \theta^n(x)$ باشند. در اینجا نیز همانند تعریف آبل، θ تابعی گویا است. این حالتِ خاص از «ردهٔ ویژهٔ» آبل متناظر است با چندجمله‌ای‌هایی با گروه گالوای دوری.
- در سال ۱۸۷۰، ژوردان [۱۷، ص ۲۸۷] «آبلی» بودنِ $f(x) = 0$ را براساس گروه گالوای آن تعریف کرد:

  بنابراین معادلاتی را معادلات آبلی می‌نامیم که گروه آن‌ها فقط دارای جانشانی‌هایی[4] است که به یکدیگر قابل تبدیل‌اند[5].

  «قابل تبدیل» در اینجا همان اصطلاح ژوردان برای «جابه‌جایی» است. سپس او ثابت می‌کند [۱۷، ص ۲۸۸] که برای معادلات تحویل‌ناپذیر، تعریفش معادل همان «ردهٔ ویژهٔ» آبل است.
- دو جلدِ اولِ اثر ماندگار وِبر با عنوان کتاب درسی جبر در سال‌های ۱۸۹۴ و ۱۸۹۶ به چاپ

[1] Kronecker [2] Jordan [3] Weber [4] substitutions [5] exchangeable

رسید. او «ردهٔ ویژهٔ» آبل را «آبلی» می‌نامد [۳۰، ج ۱، ص ۵۷۶] و بعداً گروه‌های جابه‌جایی را «آبلی» نام‌گذاری می‌کند [۳۰، ج ۲، ص ۶]. تا جایی‌که من اطلاع دارم، این اولین جایی است که اصطلاح «گروه آبلی» به معنای امروزی آن ظاهر می‌شود.[۱]

تعریفِ «گروه آبلی» در دروس جبر مقدماتی، بسیار ساده به نظر می‌رسد. اما، دراصل، دارای تاریخچهٔ بسیار گسترده‌ای است که گاوس، آبل، مفهوم پروانه، توابع بیضوی، ضرب مختلط، و حل‌پذیری به‌وسیلهٔ رادیکال‌ها را در بر می‌گیرد.

شونمان

برخلاف افرادی که تا به اینجا از آن‌ها نام برده شد، تئودور شونمان فرد شناخته‌شده‌ای محسوب نمی‌شود. او زندگی‌نامه‌ای در پایگاه تاریخچهٔ ریاضیاتِ مک‌توتر [۲۱] ندارد. براساس زندگی‌نامهٔ آلمانی عمومی [۲، ج ۳۲، ص ۲۹۳-۲۹۴]، شونمان در سال ۱۸۱۲ متولد شد و در سال ۱۸۶۸ درگذشت. او تحت راهنمایی ژاکوبی و اشتاینر[۲] در کونیگسبرگ[۳] و برلین به تحصیل پرداخت. مدرک دکترای خود را در سال ۱۸۴۲ اخذ کرد و مربی ارشد و نهایتاً استاد دبیرستانی در براندنبورگ آن دِر هافل[۴] شد. کتاب لمرماير [۱۹] چندین ارجاع به کارهای شونمان در نظریهٔ اعداد دارد؛ بعضی از نتایج شونمان در کتاب معروف دیکسون [۷] ذکر شده‌اند، خصوصاً در فصل مربوط به هم‌نهشتی‌ها از درجهٔ بالا در جلد اول.

مهم‌ترین اثر شونمان برای ما، مقالهٔ طولانی‌ای است که در سال‌های ۱۸۴۵ و ۱۸۴۶ در دو بخش در مجلهٔ کرِله به چاپ رسیده است. قسمت اول [۲۴]، شامل بخش‌های ۱ تا ۵۰، با عنوان مبانی نظریه‌ای کلی دربارهٔ هم‌نهشتی‌ها از درجهٔ بالا که پیمانهٔ آن‌ها یک عدد اول حقیقی است منتشر شد. شونمان در مقدمهٔ آن به گاوس اشاره می‌کند:

> نویسندهٔ معروف تحقیقات حسابی در بخش هشتم کتابش، درصدد ارائه نظریه‌ای کلی دربارهٔ هم‌نهشتی‌ها از درجهٔ بالا بود. اگرچه آن بخش هشتم منتشر نشد و همچنین، تا جایی‌که من اطلاع دارم، نویسنده دربارهٔ این موضوع هیچ مطلبی منتشر و هیچ چیز روشنی بیان نکرد.

شونمان حدس می‌زند که شاید گاوس در انتشار نتایج بر او پیش‌دستی کند، اما غصّهٔ آن را ندارد:

> . . . جبران از دست دادن عنوان اولین ابداع‌کننده این است که من خودم می‌دانم از راهی مخصوص

---

[۱] در سال ۱۸۷۰، ژوردان اصطلاح «groupe abélien» را برای اشاره به گروهی که ارتباط نزدیکی به گروه همتافته [symplectic group] روی یک میدان متناهی دارد به کار برد [۱۷، ج ۲، بخش ۸].

[2] Steiner [3] Königsberg [4] Brandenburg an der Havel

خودم و مستقل از آن شخص به آن مفهوم رسیده‌ام.

عملاً، گاوس و، همان‌طور که بعداً خواهیم دید، گالوا در استفاده از نتایج او بر او پیش‌دستی کردند. ازاین‌رو باید در نقل‌قول بالا «آن شخص» را به «آن اشخاص» تغییر داد، که دراین‌صورت نظر درست‌تری می‌شود.

مثل گاوس، شونمان بررسی دقیقی دربارهٔ چندجمله‌ای‌های دارای تجزیهٔ یکتا به‌پیمانهٔ p انجام داد. اما بعد از آن، در بخش ۱۴، کاری متفاوت کرد. فرض بگیریم $f(x) \in \mathbb{Z}[x]$ یک چندجمله‌ای تکین از درجهٔ n و تحویل‌ناپذیر به‌پیمانهٔ p باشد و $\alpha \in \mathbb{C}$ ریشه‌ای از $f(x)$ باشد (که گاوس وجود آن را ثابت کرده بود). برای چندجمله‌ای‌های مفروض $\varphi, \psi \in \mathbb{Z}[x]$، شونمان $\varphi(\alpha)$ و $\psi(\alpha)$ را هم‌نهشت به‌پیمانهٔ (p, α) می‌نامد، و می‌نویسند $\varphi(\alpha) \equiv \psi(\alpha)$ (به‌پیمانهٔ p، α)، هرگاه برای $R \in \mathbb{Z}[x]$ی داشته باشیم $\varphi(\alpha) = \psi(\alpha) + pR(\alpha)$. سپس او ثابت می‌کند که «صورت کلیِ کوچک‌ترین باقیمانده»[1] به شکل $a_{\circ}\alpha^{n-1} + a_{1}\alpha^{n-2} + \cdots + a_{n-1}$ است که در آن $a_i \in \{\circ, \ldots, p-1\}$. از اینجا میدانی با p^n عضو به دست می‌آید.

روش ساخت شونمان را می‌توان به‌صورت زیر نیز بازگو کرد. ریشهٔ α یک عدد صحیح جبری و $\mathbb{Z}[\alpha]$ یک حلقه تحت عمل ضرب است. رابطهٔ هم‌ارزی $\varphi(\alpha) \equiv \psi(\alpha)$ (به‌پیمانهٔ p، α) به این معنی است که $\varphi(\alpha)$ و $\psi(\alpha)$ هم‌دستهٔ یکسانی را در حلقهٔ خارج‌قسمتیِ $\mathbb{Z}[\alpha]/\langle p\rangle$ می‌دهند، که در آن $\langle p\rangle = p\mathbb{Z}[\alpha]$ ایده‌آل تولیدشده به‌وسیلهٔ p است. بعداً خواهیم دید که $\mathbb{Z}[\alpha]/\langle p\rangle$ میدان است، زیرا $f(x)$ به‌پیمانهٔ p تحویل‌ناپذیر است. بنابراین $\mathbb{Z}[\alpha]/\langle p\rangle$ نسخهٔ جدیدی از میدان متناهیِ شونمان است. در ادامه، $\mathbb{F}_{p^n}$ را به‌جای $\mathbb{Z}[\alpha]/\langle p\rangle$ به‌کار خواهیم برد، زیرا این میدان دارای p^n عضو است. در اینجا بعضی نتایج دیگر شونمان را مشاهده می‌کنید:

- عناصرِ $\mathbb{F}_{p^n}$، ریشه‌های $x^{p^n} - x$ هستند. او این عبارت را به‌صورت $x^{p^n} - x \equiv \circ$ (به‌پیمانهٔ p، α) می‌نویسد.
- $f(x) \equiv (x-\alpha)(x-\alpha^p)\cdots(x-\alpha^{p^{n-1}})$ (به‌پیمانهٔ p، α). بنابراین $\mathbb{F}_{p^n}$ میدان شکافندهٔ $f(x)$ به‌پیمانهٔ p است. گروه گالوا (ابداعی فروبنیوس[2]) در این تجزیه از f مستتر است.

قسمت اول مقالهٔ شونمان در بخش ۵۰ با اثبات جذابی از تحویل‌ناپذیریِ

$$\Phi_p(x) = x^{p-1} + \cdots + x + 1$$

[1] allgemeine Form eines kleines Restes [2] Frobenius

به اوج خود می‌رسد. اثبات آن را با نمادگذاری‌های مرسوم می‌آوریم. عدد اول $p \neq \ell$ و تجزیهٔ به عوامل اول $\Phi_p(x) \equiv f_1(x) \cdots f_r(x)$ (به پیمانهٔ ℓ) را درنظر بگیرید که در آن f_iها به‌پیمانهٔ ℓ تحویل‌ناپذیرند. از خواص معمول میدان‌های متناهی، برای هر $i = 1, \ldots, r$، نتیجه می‌شود که

$$\begin{aligned} \deg(f_i) &= \text{کوچک‌ترین } n\text{ی که } \mathbb{F}_{\ell^n}^* \text{ یک عضو از مرتبهٔ } p \text{ دارد} \qquad (۴) \\ &= \text{کوچک‌ترین } n\text{ی که } \ell^n \equiv 1 \text{ به‌پیمانهٔ } p \text{ است} \\ &= \text{مرتبهٔ ردهٔ هم‌نهشتیِ } l \text{ در } (\mathbb{Z}/p\mathbb{Z})^* \end{aligned}$$

بررسی این رابطه را به‌عنوان تمرینی ساده به خواننده واگذار می‌کنیم. بنابر قضیهٔ دیریکله دربارهٔ اعداد اول موجود در تصاعدهای حسابی (که درست چند سال قبل از مقالهٔ شونمان اثبات شد)، هر ردهٔ هم‌نهشتی به‌پیمانهٔ p یک عدد اول دارد. درحالت‌خاص، ردهٔ هم‌نهشتیِ یک ریشهٔ اولیه شامل یک عدد اول ℓ است. یک ریشهٔ اولیه به‌پیمانهٔ p، یک ردهٔ هم‌نهشتی از مرتبهٔ $p-1$ در $(\mathbb{Z}/p\mathbb{Z})^*$ ایجاد می‌کند، بنابراین برای این ℓ از (۴) داریم $n = p-1$. از این نتیجه می‌شود که $\Phi_p(x)$ به‌پیمانهٔ ℓ تحویل‌ناپذیر است و ازاین‌رو روی $\mathbb{Z}$ نیز تحویل‌ناپذیر است. بنابراین طبق لم گاوس، $\Phi_p(x)$ روی $\mathbb{Q}$ تحویل‌ناپذیر است.

این اثبات از اثبات گاوس ساده‌تر است؛ اگرچه اطلاعاتی از میدان‌های متناهی را لازم دارد و از نتیجهٔ کلاسیک دیریکله استفاده می‌کند. استفاده از عدد اول کمکی ℓ بسیار ظریف و زیباست. زمانی‌که من در مقطع کارشناسی ارشد، در دههٔ ۱۹۷۰، هندسهٔ جبری را به سبک گروتِندیک می‌خواندم، از اینکه در استدلالی عددی اول غیر از مشخصهٔ مانده‌ای[1] اختیار می‌شد لذت می‌بردم؛ خیلی جدید و پیشرفته به نظرم می‌رسید. کمی بعد متوجه شدم که شونمان ۱۲۰ سال قبل، همین روش را به کار برده است.

قسمت دوم مقالهٔ شونمان [۲۵] تحت عنوان بررسی پیمانه‌هایی که توانی از اعداد اول‌اند شامل بخش‌های ۵۱–۶۶ است. در این مقاله، شونمان تجزیهٔ چندجمله‌ای‌ها به‌پیمانهٔ p^m، و به‌ویژه تغییرات تجزیه در اثرِ تغییرِ m، را بررسی می‌کند. یکی از نتایج مهم او، در بخش ۵۹، همان نتیجه‌ای است که امروزه آن را لم هِنزل[2] می‌نامیم:

لم. اگر یک چندجمله‌ای تکین[3] با متغیر x قابل تجزیه به دو عامل تکین به‌پیمانهٔ p باشد به‌طوری‌که

[3] شونمان، «Ausdruck» (به‌معنای عبارت) را برای چندجمله‌ای و «einfach» (به‌معنای ساده) را برای تکین به کار می‌برد.

[1] residue characteristic [2] Hensel

> این دو عامل به‌پیمانهٔ p، دارای مقسوم‌علیه مشترکی نباشند: آنگاه این چندجمله‌ای به‌طور یکتا به دو عامل به‌پیمانهٔ p^m قابل تجزیه است، که این دو عامل با دو عامل نخستین به‌پیمانهٔ p هم‌نهشت‌اند.[۱]

یک نتیجه این است که هرگاه یک چندجمله‌ای تحویل‌ناپذیر به‌پیمانهٔ p^m به‌پیمانهٔ p تحویل یابد، حاصل باید توانی از یک چندجمله‌ای تحویل‌ناپذیر به‌پیمانهٔ p باشد. شونمان در بخش ۶۱ در مورد عکس این مطلب سؤال زیر را مطرح می‌کند.

> مسئله. بررسی کنید که آیا توانی از یک چندجمله‌ای تحویل‌ناپذیر به‌پیمانهٔ p، به‌پیمانهٔ p^m تحویل‌ناپذیر است یا خیر؟

یک مثال بسیار ساده برای این موردْ چندجمله‌ای $(x-a)^n$ است و در مورد چندجمله‌ای هم‌نهشت با $(x-a)^n$ (به‌پیمانهٔ p) اولین امکانی که تحویل‌ناپذیری را برای آن باید بررسی کنیم، پیمانهٔ p^2 است. پاسخ شونمان چنین است:

> ... ازاین‌رو می‌توان این قضیه را بیان کرد: **$(x-a)^n+pFx$ به‌پیمانهٔ p^2 تحویل‌ناپذیر است هرگاه عامل $(x-a)$ به‌پیمانهٔ p در Fx قرار نداشته باشد** ...

این قضیه به این شکل کاملاً درست نیست ـلازم است فرض کنیم که $\deg(F)\le n$.[۲] از آنجایی که $x-a$ چندجمله‌ای $F(x)$ را به‌پیمانهٔ p عاد می‌کند اگر و فقط اگر $F(a)\equiv 0$ (به‌پیمانهٔ p)، بنابراین نتیجهٔ شونمان را می‌توانیم به‌صورت زیر بیان کنیم.

محک تحویل‌ناپذیری شونمان فرض کنید $f(x)\in\mathbb{Z}[x]$ از درجهٔ $n>0$ باشد و عدد اول p و عدد صحیح a وجود داشته باشند به‌طوری‌که

$$f(x)=(x-a)^n+pF(x),\quad F(x)\in\mathbb{Z}[x].$$

اگر $F(a)\not\equiv 0$ (به‌پیمانهٔ p)، آنگاه $f(x)$ به‌پیمانهٔ p^2 تحویل‌ناپذیر است.

در اینجا، اثباتی، برای راحتی کار خواننده، می‌آوریم.

اثبات. فرض کنید $(x-a)^n+pF(x)$ دارای یک تجزیهٔ نابدیهی به‌پیمانهٔ p^2 باشد

$$(x-a)^n+pF(x)\equiv G(x)H(x)\ (\text{به‌پیمانهٔ } p^2). \tag{۵}$$

---

[۱] یکتایی تجزیه به ما امکان می‌دهد که وقتی $m\to\infty$ حد بگیریم و تجزیه‌ای روی اعداد صحیح pای، $\mathbb{Z}_p$، به‌دست آوریم که به تجزیهٔ داده‌شده به‌پیمانهٔ p تحویل می‌یابد. این شکلِ لم هِنزل در [۱۶، قضیهٔ ۶.۴.۳] مطرح شده است و بحث [۱۶، ص ۷۲] آن‌را به این شکل شناخته‌شده‌تر لم هِنزل مرتبط می‌کند: برای $f(x)\in\mathbb{Z}_p[x]$، یک جواب معادلهٔ $f(x)\equiv 0$ (به‌پیمانهٔ p) با چندگانگی یک، به جوابی از معادلهٔ $f(x)=0$ در $\mathbb{Z}_p$ انتقال می‌یابد. [۲] برای مثال، فرض کنید $F(x)=x^3-p^2x+1$. پس $x^2+pF(x)=(px+1)(x^2-p^2x+p)$، هرچند $F(0)\not\equiv 0$ (به‌پیمانهٔ p).

حالتی را فرض می‌کنیم که در آن $G(x)$ و $H(x)$ تکین‌اند. دراین‌صورت از هم‌نهشتی $(x-a)^n \equiv G(x)H(x)$ (به‌پیمانهٔ p) و یکتایی تجزیه، نتیجه می‌گیریم که $G(x) \equiv (x-a)^i$ (به‌پیمانهٔ p) و $H(x) \equiv (x-a)^j$ (به‌پیمانهٔ p) که در آن $i,j > 0$ و $i+j=n$. با قرار دادن $x=a$ در این هم‌نهشتی‌ها، مشاهده می‌کنیم که p هم $G(a)$ و هم $H(a)$ را عاد می‌کند زیرا $i,j > 0$. نهایتاً با قرار دادن $x=a$ در (۵) داریم $pF(a) \equiv 0$ (به‌پیمانهٔ p^2) که تناقض است. □

جالب اینجاست که از این قضیه محک آیزنشتاین نتیجه می‌شود. برای این منظور، فرض کنید $f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n$ در فرض محک آیزنشتاین صدق کند. با ضرب کردن در یک عدد صحیح مناسب، می‌توان فرض کرد که $a_0 \equiv 1$ (به‌پیمانهٔ p). پس می‌توان نوشت $f(x) = x^n + pF(x)$. همچنین توجه کنید که $F(0) \not\equiv 0$ (به‌پیمانهٔ p) زیرا p^2 ضریب a_n را عاد نمی‌کند. درنتیجه، بنابر محک شونمان، $f(x)$ به‌پیمانهٔ p^2 تحویل‌ناپذیر است. این مطلب تحویل‌ناپذیری روی $\mathbb{Z}$ و، بنابر لم گاوس، روی $\mathbb{Q}$ را ایجاب می‌کند.

همان‌طورکه شاید حدس بزنید، شونمان، بی‌درنگ، محک تحویل‌ناپذیری خود را روی یک چندجمله‌ای معروف به کار می‌برد:

> اجازه دهید این نتیجه را برای $\dfrac{x^n-1}{x-1}$ به کار ببریم که در آن n عددی اول است. در این حالت، $x^n - 1 \equiv (x-1)^n$ (به‌پیمانهٔ n)، و بنابراین نتیجه می‌گیریم
>
> $$\frac{x^n-1}{x-1} = x^{n-1} + x^{n-2} + \cdots + x + 1 = (x-1)^{n-1} + nFx.$$
>
> برای $x=1$ داریم $n = nF(1)$ و بنابراین $F(1)=1$ و $F(1) \not\equiv 0$ (به‌پیمانهٔ n). از اینجا نتیجه می‌شود که $\dfrac{x^n-1}{x-1}$ همواره به‌پیمانهٔ n^2 تحویل‌ناپذیر است به‌شرطی‌که n عددی اول باشد؛ ازاین‌رو، این عبارت از نظر جبری قطعاً تحویل‌ناپذیر است.
>
> سادگی اثبات این قضیه درخور توجه است زیرا اثبات گفته‌شده در کتاب «تحقیقات» به ذکاوت بیشتری نیاز دارد و بسیار پیچیده‌تر است. (بخش ۵۰، تذکر ۲ را ببینید.)

در این روش، تحویل‌ناپذیریِ $x^{n-1} + \cdots + x + 1$ بدون تعویض متغیر $x \leftrightarrow x+1$، که حین استفاده از محک آیزنشتاین مورد نیاز است، اثبات می‌شود. بدیهی است که شونمان از اینکه اثباتش بسیار ساده‌تر از اثبات گاوس است خشنود بود. (عبارت داخل پرانتز در پایان نقل‌قول بالا به اثبات قبلی شونمان که در مورد تحویل‌ناپذیری در بخش ۵۰ی مقالهٔ او آمده است اشاره دارد.)

محک شونمان زیبا است اما برای بسیاری از ریاضی‌دانان ناشناخته است. اما من چگونه متوجه آن شدم؟ در کتاب من با موضوع نظریهٔ گالوا [۵] اثبات آیزنشتاین برای قضیهٔ آبل دربارهٔ خم

پروانه آمده است. برای اینکه اثبات آیزنشتاین را بهتر بفهمم نگاهی به کتاب شگفت‌انگیز لمرماير با عنوان قوانین متقابل [۱۹] انداختم، در آنجا ارجاعی به شونمان دیدم. موقع خواندن مقالهٔ شونمان نتوانستم محک آینشتاین را در آن پیدا کنم، شاید یک دلیلش این بود که مقاله طولانی بود و زبان آلمانیِ من خیلی خوب نیست و یا شاید من دنبال صورتی از این محک بودم که آیزنشتاین داده بود نه خودِ شونمان. دوباره سراغ کتاب لمرماير رفتم و متوجه شدم که لمرماير از مایکل فیلاستا[1] برای اشاره به مقالهٔ شونمان تشکر کرده است. به فیلاستا نامه نوشتم و او پاسخ داد که شونمان محکی برای تحویل‌ناپذیری چندجمله‌ای‌ها به‌پیمانهٔ p^2 ثابت کرده است. با این پاسخ من یک‌راست به بخش ۶۱ مقاله رسیدم که همان‌جایی است که شونمان نتیجهٔ خود را بیان کرده است.

بازگشت به گاوس

شونمان علاوه‌بر کشف محک آیزنشتاین قبل از آیزنشتاین، لم هِنزل را نیز قبل از هِنزل کشف کرد. از بخت بد، گاوس نتایج شونمان و هِنزل را جلوتر از آن‌ها یافته بود. در پیش‌نویس چاپ‌نشدهٔ بخش هشتم از تحقیقات، گاوس (ص ۶۲۷ از [۱۳] یا ص ۲۳۸ از [۱۴، ج ۲]) چندجمله‌ای X با ضرایب صحیح را در نظر گرفته، رفتار آن را به‌پیمانهٔ p و p^2 مطالعه می‌کند:

> مسئله. اگر تابع X به‌پیمانهٔ p به عوامل دوبه‌دو نسبت به‌هم اولِ ξ، ξ'، ξ'' و ... تجزیه شود، آنگاه X به‌طور مشابه به‌پیمانهٔ p^2 به عوامل Ξ، Ξ'، Ξ'' و ... تجزیه می‌شود به‌طوری‌که
>
> $$\xi \equiv \Xi,\ \xi' \equiv \Xi',\ \xi'' \equiv \Xi'',\ \ldots \quad (\text{به‌پیمانهٔ } p)$$

گاوس این مسئله را ثابت می‌کند و سپس شرح می‌دهد که چگونه قاعدهٔ مشابهی برای پیمانهٔ p^k ، برای هر k دلخواه، نتیجه می‌شود. «مسئلهٔ» او از «لمِ» شونمان ضعیف‌تر است زیرا یکتایی تجزیهٔ انتقال‌یافته را بیان نمی‌کند. بنابراین، دراصل، آنچه که گاوس ثابت کرد، یک «الگوی نخستین لم هِنزل»[2] بود. باوجوداین، گاوس آن‌قدر از این نتیجه راضی بود که آن را در دفترچهٔ یادداشت روزانهٔ ریاضیاتش یادداشت کند [۱۵]. یادداشت شمارهٔ ۷۹ آن، به تاریخ ۹ سپتامبر ۱۷۹۷، این است:

> شروع کشفِ اصولی که به‌موجب آن‌ها حل هم‌نهشتی‌ها براساس پیمانه‌های چندگانه به هم‌نهشتی‌ها براساس پیمانه‌های خطی تحویل یابد.

در اینجا، «حل هم‌نهشتی‌ها براساس پیمانه‌های چندگانه» به‌معنایِ تجزیهٔ چندجمله‌ای‌ها به‌پیمانهٔ p^k است و به‌طور مشابه، «هم‌نهشتی‌های براساس پیمانه‌های خطی» به‌معنای کار کردن با پیمانهٔ p

[1] Michael Filaseta [2] proto-Hensel's lemma

است. این برداشت از یادداشت روزانهٔ گاوس به‌طور دقیقی در [۱۱] توجیه شده است.

گاوس علاوه‌بر این شکل مقدماتی لم هِنزل، حالتی را در نظر گرفت که در آن عوامل تجزیه به‌پیمانهٔ p متمایز نیستند. برای مثال، هم‌نهشتی $X \equiv X'(x-a)^m$ (به‌پیمانهٔ p) حدوداً در آخر پیش‌نویس گاوس از بخش هشتم دیده می‌شود. اگر او این موضوع را ادامه داده باشد، کاملاً محتمل به نظر می‌رسد که همان مسیر شونمان را طی و محک آیزنشتاین را نیز کشف کرده باشد. اما دست‌نوشته در وسط یک هم‌نهشتی یک‌دفعه به پایان می‌رسد: آخرین چیزی که گاوس نوشته است این است:

$$\circ \equiv$$

مثل خیلی دیگر از کارهایش، گاوس هرگز به سراغ مطالعهٔ جامع هم‌نهشتی‌ها[1] نمی‌آید تا آن را تمام کند. تنها بعد از انتشارش جزو جلد دوم مجموعهٔ آثارش در سال ۱۸۶۳ است که این اثر شناخته شد، و امروز هم هنوز در سایهٔ همتای مشهورترش یعنی تحقیقات حسابی است.

مطالب بیشتری دربارهٔ میدان‌های متناهی

علاوه بر گاوس و شونمان، گالوا نیز در توسعهٔ نظریهٔ میدان‌های متناهی نقش داشت. گالوا در مقالهٔ خود تحت عنوان دربارهٔ نظریهٔ اعداد، منتشرشده در مجلهٔ بولتن علوم ریاضیِ فروسک [۱۲، ص ۱۱۳-۱۲۷] به سال ۱۸۳۰، از هم‌نهشتی $F(x) \equiv \circ$ (به‌پیمانهٔ p)، یا آن‌طورکه او نوشته $Fx = \circ$، آغاز می‌کند؛ در اینجا $F(x)$ به‌پیمانهٔ p تحویل‌ناپذیر است. سپس ریشه‌ها را بررسی می‌کند:

باید ریشه‌های این هم‌نهشتی را نوعی نماد موهومی در نظر گرفت . . .

او سپس به اثبات نتایجی در مورد میدان‌های متناهی می‌پردازد که بعدها شونمان نیز آن‌ها را به دست آورد. به نظر می‌رسد که شونمان از کار گالوا بی‌اطلاع بوده است.

گاوس به این ریشه‌ها، که گالوا از وجود آن‌ها سرسری گذشته بود، بسیار حساس بود. در عوض، روش ساخت شونمان از طریق $\mathbb{Z}[\alpha]/\langle p\rangle$ دقیق بود زیراکه او ریشهٔ مختلطی مانند $\alpha \in \mathbb{C}$ از $f(x)$ را به کار می‌برد. اما قضیهٔ اساسی جبر، دراصل، قضیه‌ای از آنالیز است چون درنهایت به کامل بودن اعداد حقیقی بستگی دارد. برای بیان صورت جبری روش شونمان، توجه کنید که چون $f(x) \in \mathbb{Z}[x]$ تکین و تحویل‌ناپذیر است، $x \mapsto \alpha$ یکریختی حلقه‌ای $\mathbb{Z}[x]/\langle f(x)\rangle \simeq \mathbb{Z}[\alpha]$

[1] Disquisitiones generales de congruentiis

را القاء می‌کند. تحویل $f(x)$ به‌پیمانهٔ p، چندجمله‌ای $\bar{f} \in \mathbb{F}_p[x]$ را نتیجه می‌دهد که شونمان آن را تحویل‌ناپذیر در نظر می‌گیرد. لذا حلقهٔ خارج‌قسمتی $\mathbb{F}_p[x]/\langle \bar{f}(x)\rangle$ میدان است. اکنون یکریختی‌های

$$\mathbb{F}_p[x]/\langle \bar{f}(x)\rangle \simeq \mathbb{Z}[x]/\langle p, f(x)\rangle \simeq \mathbb{Z}[\alpha]/\langle p\rangle$$

نشان می‌دهند که حلقهٔ شونمان $\mathbb{Z}[\alpha]/\langle p\rangle$ دراصل میدانی متناهی با p^n عضو است.

این بیان جبری از میدان‌های متناهی را ددکیند در سال ۱۸۵۷ در مقاله‌ای با عنوان بیان کلی نظریه‌ای دربارهٔ هم‌نهشتی‌ها از درجهٔ بالا به‌پیمانهٔ یک عدد اول حقیقی صریحاً بیان کرده است [۶]. ددکیند مقالهٔ خود را با ذکر این نکته آغاز می‌کند که این موضوع را ابتدا گاوس مطرح و سپس گالوا و شونمان آن را بررسی کردند. ددکیند از عمق کاری که گاوس انجام داده بود آگاه نبود، هرچند او بعدها ویراستار مسئول انتشارِ مطالعهٔ جامع هم‌نهشتی‌ها در مجلد دوم از مجموعه آثار گاوس در سال ۱۸۶۳ شد.

روش ددکنید اساساً همان است که در بالا با حلقهٔ خارج‌قسمتی $\mathbb{Z}[x]/\langle p, f(x)\rangle$ انجام دادیم که در آن $f(x)$ به‌پیمانهٔ p تحویل‌ناپذیر است؛ اگرچه نوشتهٔ ددکنید مربوط به زمانی است که هنوز مفهوم حلقهٔ خارج‌قسمتی به‌طور کامل شکل نگرفته بود. باوجوداین، او نشان می‌دهد که آن مجموعه میدانی متناهی با p^n عضو است که در آن $n = \deg(f)$. در بیشتر قرن نوزدهم، منظور از «میدان متناهی» همین شیء بوده است. این شیء این مزیت را داشت که کار با آن ساده بود (حتی امروزه، رایانه‌ها میدان‌های متناهی را به همین صورت نمایش می‌دهند)، اما، از نظر ریاضی، چون به انتخاب $f(x)$ بستگی دارد اساساً شکل متعارفی نیست.

یکی از اولین تعریف‌های کاملاً انتزاعی برای میدان متناهی را مور در مقاله‌ای بیان کرده است؛ مقالهٔ او [۲۰] در مجموعهٔ مقالات کنگرهٔ بین‌المللی ریاضی‌دانان به سال ۱۸۹۳ به چاپ رسید. تعریف او به این صورت است:

> فرض کنید دستگاهی از s نماد یا نشانه‌های* متمایز داریم، μ_1، ...، μ_s (s یک عدد صحیح مثبت متناهی است) و همچنین فرض کنید که این نشانه‌ها می‌توانند با چهار عمل اصلی جبری ـجمع، تفریق، ضرب، و تقسیمـ با هم ترکیب شوند. این عمل‌ها، اعمالی هستند که در اتحادهای مربوط به عمل‌ها [1] در جبر مجرد معمولی صدق می‌کنند
>
> $$\mu_i + \mu_j = \mu_j + \mu_i;\ \mu_i\mu_j = \mu_j\mu_i;\ (\mu_i + \mu_j)\mu_k = \mu_i\mu_k + \mu_j\mu_k;\ \ldots.$$
>
> همچنین هنگامی‌که با هم ترکیب شوند، حاصل این عمل‌ها در هر مورد به‌طور یکتا مشخص می‌شود

[1] operational identities

و نتیجهٔ آن عضو دستگاه نشانه‌ها است. چنین دستگاهی را یک میدان از مرتبهٔ s می‌نامیم و با نماد $F[s]$ نمایش می‌دهیم.

بی‌درنگ به اینجا می‌رسیم که همهٔ این میدان‌های $F[s]$ از مرتبهٔ s را تعیین کنیم.

دو واژهٔ «دستگاه» و «نشانه‌ها» حاکی از آن است که نوشتهٔ مور مربوط به دوران ماقبل استانداردسازی زبان نظریهٔ مجموعه‌ها است. مور در ادامه نشان می‌دهد که تعریف او با نمایشی که ددکیند برای میدان متناهی عرضه کرده است معادل است. به‌این‌ترتیب سرانجام در سال ۱۸۹۳ نظریهٔ جدیدی برای میدان‌های متناهی حاصل می‌شود.

واژهٔ «نشانه‌ها» در نقل‌قول گفته‌شده از مور به پانویس زیر اشاره دارد:

* لازم است که تمام انگاره‌های کمّی[1] از نشانه‌های مفهومی[2] مستثنی شوند. توجه کنید که علائم $>, <$ در این نظریه ظاهر نمی‌شوند.

مخاطب مور در این نوشته افرادی با سطح ریاضی بالا بودند، اما او فرض را بر آشنایی آن‌ها با مفاهیم نظریهٔ مجموعه‌ها نگذاشته بود ــ منظور او از آن پانویس این بود که آن‌ها ماهیت انتزاعی مطالب او را درک کنند. این امر را موقع تدریس جبر مجرد به دانشجویان دورهٔ کارشناسی باید در نظر داشته باشیم.

آیزنشتاین

سرانجام به آیزنشتاین می‌رسیم، کسی که کار او روی قضیهٔ آبل در مورد خم پروانه در یک مقالهٔ طولانی دو بخشی در مجلهٔ کِرله در سال ۱۸۵۰ به اوج خود رسید [۱۰، ص ۵۳۶-۶۱۹]. مقدمتاً، معادلهٔ قطبی $r^۲ = \cos ۲\theta$ را برای پروانه و r را به‌عنوان تابعی از طول کمان s در نظر می‌گیریم. لذا $r = \varphi(s)$ بدین معنی است که اگر از مبدأ آغاز کنیم و شاخهٔ پروانه در ربع اول را برای طول s دنبال کنیم، آنگاه در نهایت به نقطه‌ای با مختصات قطبی (r, θ) می‌رسیم. شکل ۲ آنچه را که در دنبال کردن مسیر این خم تا ربع چهارم رخ می‌دهد نمایش می‌دهد.

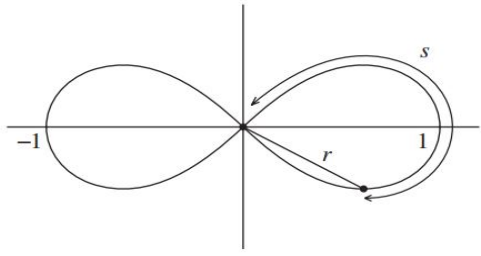
محاسبهٔ طول کمان [۵، بخش ۲.۱۵] نشان می‌دهد که s از طریق معادلهٔ زیر به r وابسته است

$$s = \int_۰^r \frac{dr}{\sqrt{۱ - r^۴}}.$$

(مثل نمادگذارهای قرن نوزدهم، متغیر و حدود انتگرال‌گیری را با یک حرف نشان داده‌ایم.) با در نظر گرفتن $r = \varphi(s)$ به‌دست می‌آوریم

$$r = \varphi(s) \quad \Longleftrightarrow \quad s = \int_۰^r \frac{dr}{\sqrt{۱ - r^۴}}. \tag{۶}$$

[1] quantitative ideas [2] concept marks



شکل ۲. $r = \varphi(s)$ روی پروانه

به‌عبارت‌دیگر، تابع پروانه $r = \varphi(s)$ تابعِ معکوسِ انتگرال بیضوی $\int_0^r \frac{dr}{\sqrt{1-r^4}}$ است که آن را نخستین‌بار در بخش هفتم از کتاب تحقیقات ملاحظه کردیم.

در معادلهٔ (۶)، $0 \le r \le 1$ متناظر است با $0 \le s \le \varpi = \int_0^r \frac{dr}{\sqrt{1-r^4}}$، بنابراین ϖ یک‌چهارمِ طول کمانِ پروانه است. به‌ویژه، $\varphi(\varpi) = 1$ و $\varphi(2\varpi) = 0$؛ و برای هر عدد صحیح مثبت m، شعاع $r = \varphi(k.2\varpi/m)$، $k = 1, \dots, m$، نقاطی را به دست می‌دهد که نیمهٔ سمت راستِ پروانه را به m قطعهٔ مساوی تقسیم می‌کند.

با تعویض متغیر $r = iu$ در (۶) آبل به تعریف $\varphi(is) = i\varphi(s)$ رسید، و حالا قانون جمع اویلر، تعریف $\varphi(z) = \varphi(s + it)$ را به تابعی از متغیر مختلط $z \in \mathbb{C}$ بدل می‌کند.[1] استفادهٔ مجدد از قانون جمع نشان می‌دهد که برای هر عدد صحیح گاوسی $m \in \mathbb{Z}[i]$، $\varphi(mz)$ تابعی گویا از $\varphi(z)$ و مشتق آن به‌صورت $\varphi'(z)$ است. این همانی است که برای تابع پروانه φ از آن به ضرب مختلط تعبیر می‌شود.

اگر $m = a + ib$ یک عدد صحیح گاوسی فرد باشد، به این معنی که $a + b$ فرد است، آنگاه $\varphi(mz)$ تابعی گویا بسیار خاصی از $\varphi(z)$است. دقیق‌تر اینکه، با داشتن چنین mی، چندجمله‌ای‌های $U(x)$ و $V(x)$ با ضرایبِ متعلق به $\mathbb{Z}[i]$ وجود دارند به‌طوری‌که $y = \varphi(mz)$ و $x = \varphi(z)$ به‌صورت

$$y = \frac{U(x)}{V(x)} = \frac{A_0 x + A_1 x^5 + \cdots + A_{(N(m)-1)/4} x^{N(m)}}{1 + B_1 x^4 + \cdots + B_{(N(m)-1)/4} x^{N(m)-1}}, \qquad (۷)$$

به یکدیگر ارتباط می‌یابند که در آن $N(m) = a^2 + b^2$ نرمِ $m = a + ib$ (تعریف‌شده در نظریهٔ

[1] گاوس مسیر مشابهی را در سال ۱۷۹۷ دنبال کرد، اگرچه او هرگز یافته‌های خود را منتشر نکرد. [۳] را برای جزئیات بیشتر ملاحظه کنید.

جبری اعداد) است. اثبات جدیدی برای این مطلب در [۵، قضیهٔ ۴.۴.۱۵] آمده است. با استفاده از (۶) نتیجه می‌گیریم که

$$\int_{۰}^{y} \frac{dy}{\sqrt{۱-y^۴}} = m \int_{۰}^{x} \frac{dx}{\sqrt{۱-x^۴}} \quad \Longleftrightarrow \quad y = \frac{U(x)}{V(x)}.$$

با زبان قرن نوزدهم، رابطهٔ $y = U(x)/V(x)$ یک انتگرال جبری برای این تساوی از انتگرال‌هاست. این رابطه، معادلهٔ (۳) را، که جلوتر ذکر کردیم، روشن می‌کند.

وقتی m عدد صحیح فرد معمولی باشد، می‌دانیم که $r = \varphi(k \cdot ۲\varpi/m)$، mـنقطهٔ تقسیمِ روی پروانه را مشخص می‌کند. اگر

$$x = \varphi(k \cdot ۲\varpi/m) = r \quad \text{و} \quad y = \varphi(m \cdot (k \cdot ۲\varpi/m)) = \varphi(k \cdot ۲\varpi) = ۰$$

را در (۷) جانشان کنیم مشاهده می‌کنیم که $U(r)/V(r) = ۰$، و بنابراین $U(r) = ۰$. این ثابت می‌کند که شعاع تقسیم[۱] r، ریشه‌های معادلهٔ چندجمله‌ای $U(x) = ۰$ اند. وقتی $m = ۲n+۱$، این تساوی دقیقاً معادلهٔ $P_{۲n+۱}(x) = ۰$ است که آبل بررسی کرد.

آیزنشتاین از ساختاری شبیه به آبل استفاده کرد. او برای اثبات قضیهٔ آبل دربارهٔ پروانه، مسئله را به‌حالتی‌که $m = a + ib$ یک عدد اول گاوسی فرد است تقلیل داد. ازآنجایی‌که x عاملی از $U(x)$ است، پس $U(x) = xW(x)$، و آیزنشتاین برای اثبات قضیه سعی می‌کند نشان دهد که $W(x)$ تحویل‌ناپذیر است. همین‌که این حکم ثابت شود، قضیه آبل نتیجه می‌شود ـ[۵، بخش ۵.۱۵] را ببینید.[۲]

اما آیزنشتاین چگونه ثابت کرد که چندجمله‌ای $W(x)$ تحویل‌ناپذیر است؟ مسئلهٔ ساده‌ای نیست. گام اساسی را آیزنشتاین زمانی برداشت که متوجه ضرایبِ $W(x)$ شد. او در نامه‌ای به تاریخ ۱۸ اوت ۱۸۴۷ نظراتش را با گاوس در میان گذاشت [۱۰، ص ۸۴۵]:

> قبلاً نشان داده بودم که وقتی $m = a + ib$ یک عدد صحیح مختلط و فرد با نرم p است و
>
> $$y = \frac{U}{V} = \frac{A_۰x + A_۱x^۵ + \cdots + A_{(p-۱)/۴}x^p}{۱ + B_۱x^۴ + \cdots + B_{(p-۱)/۴}x^{p-۱}}$$

---

[۲] برای اثباتی کامل از قضیهٔ آبل دربارهٔ پروانه، خواننده بهتر است [۲۲، ۵، ۲۳] را ملاحظه کند. در [۲۳] اثبات جدیدی با استفاده از نظریهٔ میدان رده‌ها آمده است.

[1] division radii

انتگرال جبریِ معادلهٔ

$$\int_{\circ} dy/\sqrt{1-y^4} = m\int_{\circ} dx/\sqrt{1-x^4}$$

است، برای عدد اول مختلطِ دوبخشی[1] m ضرایبِ عبارت صورت تا آخری، که عدد مختلط واحدی است، و ضرایب مخرج به‌جز اولی، که $= 1$، همگی بر m بخش‌پذیرند. حدس زده‌ام که این گزاره وقتی m یک عدد اول یک‌بخشی باشد ($\equiv 3$ (به‌پیمانهٔ ۴) صرف‌نظر از علامت یا ضریبی به شکل یک عدد مختلط واحد) نیز درست است؛

در قسمت اول این نقل قول، آیزنشتاین صورت مسئله را بیان و تنظیم می‌کند، و بعد از نوشتن معادله، ساختار ضرایب صورت و مخرج را بیان می‌کند. یادآوری می‌کنیم که اعداد اول فردِ گاوسی دو نوع‌اند:

- اعداد اول دوبخشی به شکل $m = a + ib$ که در آن $p = a^2 + b^2$ اول است و $p \equiv 1$ به‌پیمانهٔ ۴.
- اعداد اول یک‌بخشی به شکل $m = \varepsilon q$ که در آن ε یکه‌ای در $\mathbb{Z}[i]$ است و $q \equiv 3$ به‌پیمانهٔ ۴.

اکنون چندجمله‌ای

$$W(x) = \frac{1}{x}U(x) = A_\circ + A_1 x^4 + \cdots + A_{(p-1)/4}x^{p-1}$$

را در نظر بگیرید. برای عدد اولِ دوبخشی m، آیزنشتاین اظهار می‌کند که قبلاً ثابت کرده است که آخرین ضریب $A_{(p-1)/4}$ یک عدد مختلط واحد است و سایر ضرایب $A_\circ, \ldots, A_{(p-1)/4-1}$ بر m بخش‌پذیرند. و حدس می‌زند که همین حکم برای اعداد اول یک‌بخشی نیز صادق است.

این حکم بوی محک آیرنشتاین را می‌دهد، به‌خصوص که طبقِ نوشتهٔ آیزنشتاین در آن نامه، جملهٔ ثابت $A_\circ$ برابر m است، که بر m^2 بخش‌پذیر نیست. تنها فرقش در این است که m و ضرایبِ W اعداد صحیح گاوسی‌اند. آیزنشتاین، کمی جلوتر در همان‌جا، حالتی را بررسی می‌کند که W روی $\mathbb{Q}(i)$ تحویل‌پذیر نباشد [۱۰، ص ۸۴۸-۸۴۹]:

> ... اگر این امکان وجود داشته باشد که W حاصل‌ضربِ دو چندجمله‌ای[2] از x با ضرایبِ صحیح گاوسی باشد و درجه‌های آن‌ها $< p - 1$. فرض کنید $W = PQ$؛ چون جملهٔ ثابتِ W برابر

[2] آیزنشتاین اصطلاح «rationalen ganzen Funktionen»، توابع گویای تام، را به کار می‌برد.

[1] two-term complex prime number

m است، لذا اگر m یک عدد اول مختلط باشد، جملهٔ ثابت در یکی از دو چندجمله‌ایِ P و Q برابر ۱ است و سایر جملات برابر mاند؛ درنتیجه اگر ضرایبِ P و Q گویا باشند، باید الزاماً صحیح باشند؛ چنانکه از ملاحظات مشابهی که حضرت‌عالی[۱] در نظریهٔ اعداد حقیقی به کار برده‌اید (تحقیقات، بخش اول) نتیجه می‌شود.

در اینجا مراد از «نظریهٔ اعداد حقیقی» نظریهٔ اعداد روی $\mathbb{Z}$ است نه $\mathbb{Z}[i]$، و از ارجاع به تحقیقات منظور همان اولین نقل قولی از گاوس است که در ابتدای مقاله آوردیم. پس آیزنشتاین دارد به گاوس می‌گوید که لم گاوس در مورد اعداد صحیح گاوسی صادق است؛ حیرت‌آور است. بعد از آن آیزنشتاین شروع به اثبات تحویل‌ناپذیریِ W می‌کند با استفاده از یکی از اثبات‌های متعارف محک آیزنشتاین.[۲] خلاصه اینکه، اولین اثبات آیزنشتاین برای محکش

- روی اعداد صحیح گاوسی بود؛
- برای یک چندجمله‌ای وابسته به مسئلهٔ تقسیمِ پروانه به کار رفت؛ و
- در نامه‌ای به گاوس مطرح شد.

هنگامی‌که آیزنشتاین نتایجش را آمادهٔ چاپ می‌کرد، متوجه شد که محک به دست آمده بسیار کلی‌تر است. عنوان بخش اول مقالهٔ سال ۱۸۵۰ او بررسی تحویل‌ناپذیری و برخی خواص دیگر معادلاتی که به تقسیم پروانه وابسته‌اند [۱۰، ص ۵۳۶-۵۵۵]، است. این مقاله روایت خودِ آیزنشتاین از محک آیزنشتاین را دارد:

> اگر در یک چندجمله‌ای $F(x)$ با متغیر x از درجهٔ دلخواه، ضریب بیشترین جملهٔ $= ۱$ باشد، و همهٔ ضرایب بعد از آن صحیح (حقیقی یا مختلط) باشند، که در آن یک عدد اول (به‌ترتیب،حقیقی یا مختلط) معینِ m ظاهر می‌شود، به‌علاوه اگر آخرین ضریب $= \varepsilon m$ که در آن ε نشان‌دهندهٔ عددی است که بر m بخش‌پذیر نیست: آنگاه ممکن نیست که $F(x)$ به‌صورت
>
> $$(x^\mu + a_1 x^{\mu-1} + \cdots + a_\mu)(x^\nu + b_1 x^{\nu-1} + \cdots + b_\nu)$$
>
> دربیاید که در آن $\mu, \nu \geq ۱$، درجهٔ $F(x) = \mu + \nu$، و همهٔ a و bها صحیح (به‌ترتیب، حقیقی یا مختلط) باشند؛ و درنتیجه معادلهٔ $F(x) = ۰$ تحویل‌ناپذیر است.[۳]

آیزنشتاین، بعد از اثبات قضیه، محک خود را برای معادلهٔ $W = ۰$ مربوط به تقسیمِ پروانه و همچنین برای چندجمله‌ای محبوب ما $x^{p-1} + \cdots + ۱$ به کار می‌برد. اثبات آیزنشتاین برای

[۲] دو اثبات متعارف برای محک آیزنشتاین وجود دارد. یکی از اثبات‌ها (منسوب به آیزنشتاین) مبتنی‌بر بررسی بخش‌پذیری ضرایبِ عوامل بر یک عدد اول است. اثبات دیگر (منسوب به شونمان) که آن را جلوتر بیان کردیم از تحویل به‌پیمانهٔ p و یکتایی تجزیه در $F_p[x]$ استفاده می‌کند. [۳] محک آیزنشتاین برای هر حوزهٔ تجزیهٔ یکتا قابل استفاده است ـ کتاب وان دِر واردن [۲۹] را ببینیدـ و ازاین‌رو برای $\mathbb{Z}$ و $\mathbb{Z}[i]$ به کار می‌رود.

[1] Eminence

اثبات تحویل‌ناپذیریِ دومی، اساساً با آنچه در صفحهٔ اول آوردیم یکسان است.

این برهان کلاسیک برای تحویل‌ناپذیریِ $x^{p-1}+\cdots+1$ نخستین‌بار در مقالهٔ آیزنشتاین ظاهر شده است. او آشکارا از یافتن چنین استدلال باشکوهی خرسند بود:

> ... بنابراین از این، اگر بخواهید، اثباتی جدید و بسیار ساده برای تحویل‌ناپذیریِ معادلهٔ $x^{p-1}+\cdots+x+1=0$ نتیجه می‌شود؛ و برخلاف اثبات‌های قبلی**)، این اثبات مستلزم شناخت ریشه‌ها و روابط میان آن‌ها نیست.
>
> **) به‌غیراز اثبات **گاوس**، تنها از اثبات **کرونکر** در مجلد ۲۹، صفحهٔ ۲۸۰، این مجله اطلاع دارم.

از اثبات گاوس اطلاع داریم و می‌دانیم که اثبات کرونکر [۱۸، ج ۱، ص ۱-۴] به سال ۱۸۴۵، از آن ساده‌تر است، ولی بازهم از روابط صریحِ بین ریشه‌ها استفاده می‌کند. اما توجه کنید که پانویس یادشده به یک چیز اشاره نمی‌کند: دو اثبات شونمان برای تحویل‌ناپذیریِ $x^{p-1}+\cdots+1$ در مقاله‌هایش به سال ۱۸۴۵ و ۱۸۴۶. بااین‌حال مقالهٔ آیزنشتاین در سال ۱۸۵۰ در همان مجله چاپ شده است!

گلایهٔ شونمان

مقالهٔ آیزنشتاین، با پاورقی مشکل‌دارش، در مجلد سی‌ونهم مجلهٔ کرِله چاپ شد. شونمان در مجلد چهلم آن مجله یک یادداشت [۲۶] به چاپ رساند که با ذکر دو قضیه از مقالهٔ آیزنشتاین شروع می‌شد:

- محک آیزنشتاین برای اعداد اول حقیقی (در $\mathbb{Z}$) و اعداد اول مختلط (در $\mathbb{Z}[i]$).
- تحویل‌ناپذیریِ چندجمله‌ای دایره‌بری $x^{p-1}+\cdots+1$ که با استفاده از محک آیزنشتاین ثابت شده بود.

سپس شونمان می‌نویسد:

> ... ازآنجایی‌که **آیزنشتاین** صریحاً اشاره کرده است که او برای قضیهٔ دوم فقط از اثبات‌های گاوس و کرونکر خبر دارد، به این نتیجه رسیدم که یادآوری کنم که در بخش ۶ام مقالهٔ من با عنوان «مبانی نظریه‌ای کلی دربارهٔ هم‌نهشتی‌ها از درجهٔ بالا ...» در مجلد ۳۱ام همین مجله، من قضیهٔ اول [محک آیزنشتاین] را برای اعداد اول حقیقی ثابت کردم و قضیهٔ دوم [تحویل‌ناپذیریِ $x^{p-1}+\cdots+1$] را از اولی نتیجه گرفتم، و همچنین روش آیزنشتاین تفاوت قابل توجهی با روشِ من ندارد. به‌علاوه من حتی برای قضیهٔ دوم اثباتی کاملاً متفاوت در بخش ۵۰ از بخشِ اول مقاله‌ام آورده‌ام.

ظاهراً معلوم است که آیزنشتاین با اسم نبردن از مقالهٔ شونمان کار را خراب کرده است. اما ابهامات و اشکالاتی در اینجا وجود دارد. اول اینکه، شونمان به بخش ۶ام مقالهٔ خودش [۲۴] در مجلد ۳۱ام مجلهٔ کرِله اشاره می‌کند، درحالی‌که محک تحویل‌ناپذیری او و کاربرد آن برای چندجمله‌ای $x^{p-1}+\cdots+1$ در بخش ۶۱ام از قسمت دومِ مقاله‌اش آمده است، که در مجلد ۳۲ام چاپ شده است. همچنین «بخش ۶»ام آن یادداشتِ مورد اشاره، می‌بایست نوشته می‌شد «بخش ۶۱». این یکی از دلایلی است که من را در یافتن محک آیزنشتاین با مشکل مواجه می‌کرد ــ در بخش نادرستی دنبال آن می‌گشتم!

اما آیزنشتاین هم برای من کمتر از این دردسر نداشت. همان‌طور که قبلاً اشاره شد، مطالعات آیزنشتاین در مورد معادلاتِ تقسیمِ پروانه، در یک مقالهٔ دوبخشی در مجلهٔ کرِله به چاپ رسید. پانویس ذکرشده در بالا در بخش اول مقاله آمده است، در شمارهٔ دوم از مجلد ۳۹. بخش دوم مقاله، بررسی برخی خواص کلی معادلاتی که به مسئلهٔ تقسیمِ پروانه وابسته‌اند، به‌همراه کاربردهایی در نظریهٔ اعداد [۱۰، ص ۵۵۵–۶۱۹]، در شمارهٔ سوم از همان مجلد منتشر شده است. این مقاله ارجاعی روشن به اثبات اولِ شونمان برای تحویل‌ناپذیریِ $x^{p-1}+\cdots+1$ دارد (همان اثبات بخش پنجاهم از مقالهٔ شونمان در مجلد ۳۱). باوجوداین، آیزنشتاین موقع نوشتن بخش اول مقاله‌اش به دلایلی از این اثبات خبر نداشت. می‌توان دربارهٔ این اتفاق گمانه‌زنی کرد، اما هرگز دلیل قطعی آن را نخواهیم دانست.

نتیجه‌گیری

اینک در پایانِ داستان شگفت‌انگیز کشف محک‌های شونمان و آیزنشتاین هستیم. ازآنجایی‌که شونمان نخستین‌بار این محک را کشف کرد، نام «محک شونمان–آیزنشتاین»، آن‌طورکه دُرورت گفته است، از نظر تاریخی نامی دقیق است. اما اغلب افراد از صورت متعلق به آیزنشتاین استفاده می‌کنند و بنابراین نام «محک آیزنشتاین–شونمان» نیز موجه است.

گاوس، در قسمت نقل‌شده از بخش هفتم کتاب تحقیقات، به دو مورد از کارهای ناتمام خود اذعان می‌کند: مسئلهٔ توسیع توابع مستدیر به توابع متعالی از قبیل تابع پروانهٔ آبل، φ، و بررسی هم‌نهشتی‌ها از درجهٔ بالا. هر دوی این‌ها به پیدایشِ حوزه‌های مهمی از ریاضیات جدید انجامیدند (اولی به خم‌های بیضوی و ضربِ مختلط، و دومی به اعداد pای و روش‌های موضعی در نظریهٔ اعداد)، و هر دوتا منجر به کشف محک شونمان–آیزنشتاین شدند. شونمان هم‌نهشتی‌ها از درجهٔ

بالا را تا رسیدن به لم هِنزل راجع‌به تحویل‌ناپذیری به‌پیمانهٔ p پی گرفت: محک او به‌صورتی کاملاً طبیعی در این اثنا ظاهر می‌شود. آیزنشتاین تحقیقات آبل دربارهٔ خم پروانه را پی گرفت و ضرایب چندجمله‌ای‌های حاصل از تقسیم آن را مورد بررسی قرار داد: محک او، در جایی کاملاً متفاوت با شونمان، به‌صورتی کاملاً طبیعی در این اثنا ظاهر می‌شود. بااین‌همه منشأ هردوی این‌ها در بندی از تحقیقات بود. همان‌طورکه گفتم، این داستان، داستان شگفت‌انگیزی است.

مراجع

[1] Abel, N. H., *Oeuvres complètes de Niels Henrik Abel*, vol. I, L. Sylow, S. Lie, eds., Grøndahl & Søn, Christiana, 1881.

[2] *Allgemeine Deutsche Biographie*, Duncker & Humblot, Leipzig, 1875–1912; also available at `http://www.deutsche-biographie.de/ ndb/adb_index.html` and `http://de.wikisource.org/wiki/Allgemeine_Deutsche_Biographie`.

[3] Cox, D. A., The arithmetic-geometric mean of Gauss, *Enseign. Math.*, **30** (1984), 275-330; reprinted in *Pi: A Source Book*, L. Berggren, J. Borwein, P. Borwein, eds., 3rd ed., Springer, New York, 2003, 481-536.

[4] Cox, D. A., *Primes of the Form* $x^2 + ny^2$, Wiley, Hoboken, NJ, 1989.

[5] Cox, D. A., *Galois Theory*, Wiley, Hoboken, NJ, 2004.

[6] Dedekind, R., Abriß einer Theorie der höheren Kongruenzen in bezug auf einen reellen Primzahl-Modulus, *J. Reine Angew. Math.*, **54** (1857), 269-325; reprinted in *Gesammelte mathematische Werke*, vol. I, E. Noether, O. Ore, eds., Vieweg, Braunschweig, 1930, 40-67.

[7] Dickson, L. E., *History of the Theory of Numbers*, Carnegie Institute, Washington, DC, 1919-1923; reprinted by Chelsea, AMS Chelsea, Providence, RI, 1969.

[8] Dorrie, H., *Triumph der Mathematik: Hundert berühmte Probleme aus zwei Jahrtausenden mathematischer Kultur*, Fredrich Hirt, Breslau, 1933; English trans. of 5th ed. by D. Antin, *100 Great Problems of Elementary Mathematics: Their History and Solution*, Dover, Mineola, NY, 1965.

[9] Dorwart, H. L., Irreducibility of polynomials, *Amer. Math. Monthly*, **42** (1935), 369-381.

[10] Eisenstein, F. G., *Mathematische Werke*, vol. II; reprinted by Chelsea, AMS Chelsea, Providence, RI, 1989.

[11] Frei, G., The unpublished section eight: On the way to function fields over a finite field, in *The Shaping of Arithmetic after C. F. Gauss's Disquisitiones Arithmeticae*, C. Goldstein, N. Schappacher, J. Schwermer, eds., Springer, Berlin, 2007, 159-198.

[12] Galois, E., *Écrits et Mémoires Mathématiques D'Évariste Galois*, R. Bourgne, J.-P. Azra, eds., Gauthier-Villars, Paris, 1962.

[13] Gauss, C. F., *Disquisitiones Arithmeticae*, G. Fleischer, Leipzig, 1801; reprinted in 1863 as vol. I of [14]; German trans. by H. Maser, *Untersuchungen über Höhere Arithmetik*, Springer, Berlin, 1889; reprinted by Chelsea, New York and AMS Chelsea, Providence, RI, 1965; English trans. by A. A. Clarke, Yale University Press, New Haven, 1966; reprinted by Springer, New York, 1986.

[14] Gauss, C. F.,*Werke*, König. Gesell. Wissen., Göttingen, 1863-1927; vols. I–IX available at `http://www. wilbourall.org` (search for "Carl").

[15] Gauss, C. F., Mathematical Diary (original manuscript in Latin): Handscriftenabteilung Niedersächsische Staats- und Universitätsbibliotek Göttingen, Cod. Ms. Gauß Math. 48 Cim. Ed. (Latin with German annotations); reproduced as Abrdruck des Tagebuchs (Notizenjournals), [14, vol. X.1, pp. 483–575]; French trans. by P. Eymard and J.-P. Lafon, Le journal mathématique de Gauss, *Rev.*

Hist. Sci. Appl. **9** (1956), 21-51; English trans. by J. Gray, A commentary on Gauss's mathematical diary, 1796–1814, *Expo. Math.*, **2** (1984), 97-130; German trans. by E. Schumann, with historical introduction by K.-R. Biermann, and annotations by H. Wußing and O. Neumann, *Mathematisches Tagebuch 1796-1814*, 4th ed., Ostwalds Klassiker der exakten Wissenschaften **256**, Akademische Verlagsgesellschaft Geest & Portig, Leipzig, 1985.

[16] Gouvêa, F., *p-adic Numbers: An Introduction*, Springer, New York, 1993.

[17] Jordan, C., *Traité des substitutions et des équations algébriques*, Gauthier-Villars, Paris, 1870; 2nd ed., 1957.

[18] Kronecker, L., *Werke*, B. G. Teubner, Leipzig, 1895-1931; reprinted by Chelsea, AMS Chelsea, Providence, RI, 1968.

[19] Lemmermeyer, F., *Reciprocity Laws*, Springer, New York, 2000.

[20] Moore, E. H., A doubly-infinite system of simple groups, in *Mathematical Papers Read at the International Mathematical Congress, 1893*, Cambridge University Press, Cambridge, 1896.

[21] O'Connor J. J., Robertson, E. F., Mactutor History of Mathematics Archive, available at `http://www-history.mcs.st-andrews.ac.uk/history/index.html`.

[22] Prasolov V., Solovyev, Y., *Elliptic Functions and Elliptic Integrals*, American Mathematical Society, Providence, RI, 1997.

[23] Rosen, M., Abel's theorem on the lemniscate, *Amer. Math. Monthly*, **88** (1981), 387-395.

[24] Schönemann, T., Grundzüge einer allgemeinen Theorie der höhern Congruenzen, deren Modul eine reelle Primzahl ist, *J. Reine Angew. Math.*, **31** (1845), 269-325.

[25] Schönemann, T., Von denjenigen Moduln, welche Potenzen von Primzahlen sind, *J. Reine Angew. Math.*, **32** (1846), 93-105.

[26] T. Schönemann, Notiz, *J. Reine Angew. Math.*, **40** (1850), 188.

[27] Serre, J.-P., Propriétés galoisiennes des points d'ordre fini des courbes elliptiques, *Invent. Math.*, **15** (1972), 259-331.

[28] Silverman J., Tate, J., *Rational Points on Elliptic Curves*, Springer, New York, 1992.

[29] van der Waerden, B. L., *Moderne Algebra*, Springer, Berlin, 1930.

[30] Weber, H., *Lehrbuch der Algebra*, 2nd ed., Vieweg, Braunschwieg, 1898-1908; reprinted by Chelsea, AMS Chelsea, Providence, RI, 1961.

آزاده نیک‌سرشت: دانشگاه آیت‌الله العظمی بروجردی، گروه ریاضی
رایانامه: `a.nikseresht@abru.ac.ir`

Farhang va Andishe-ye Riyazi
Volume 41, Number 71, Fall/Winter 2022, Pages 173–198
doi: 10.30504/mct.2023.1268.1883

Why Eisenstein Proved the Eisenstein Criterion and Why Schönemann Discovered It First

D. A. Cox
Translated by A. Nikseresht[1]

Department of Mathematics, Ayatollah Boroujerdi University, Iran

Abstract. This article explores the history of the Eisenstein irreducibility criterion and explains how Theodor Schönemann discovered this criterion before Eisenstein. Both were inspired by Gauss's *Disquisitiones Arithmeticae*, though they took very different routes to their discoveries. The article will discuss a variety of topics from 19th-century number theory, including Gauss's lemma, finite fields, the lemniscate, elliptic integrals, abelian groups, the Gaussian integers, and Hensel's lemma.

Keywords: the Eisenstein irreducibility criterion, Theodor Schonemann, Carl Gauss, polynomial equations, reducibility of polynomial
Article history: Recieved 6 February 2022; Accepted 8 May 2022

[1] a.nikseresht@abru.ac.ir

ISSN 1022-6443/