قضیه‌ی اساسی جبر و اثبات جبری گاوس

دکتر امیر جعفری

حل معادلات جبری به شکل

$$a_0x^n + a_1x^{n-1} + \cdots + a_n = 0 \qquad (1)$$

که $a_0, \ldots, a_n$ ضرایب عددی مشخص هستند، از دیرباز ذهن بشر را به خود مشغول کرده است. روش حل این معادلات برای معادلات درجه ۲ به زمان‌های باستان باز می‌گردد. روش کلی حل توسط ریاضی‌دان ایرانی، خوارزمی در کتاب جبر و مقابله ارائه شد. حل معادلات درجه ۳ با روش‌های هندسی توسط خیام بررسی شد. روش او حتی برای معادلات درجه ۴ نیز قابل تعمیم است ولی قادر به حل کلی این معادلات نیست. در قرن پانزده و شانزده میلادی، ریاضیدانان ایتالیایی موفق به حل کلی معادلات درجه ۳ و ۴ نیز شدند. آن‌ها برای این منظور مجبور به تعریف مجموعه‌ی بزرگتری از اعداد یعنی همان اعداد مختلط:

$$\mathbb{C} = \{a + ib \mid a, b \in \mathbb{R}\} \qquad (2)$$

شدند و عدد موهومی $i = \sqrt{-1}$ ریشه‌ی ابداعی آن‌ها برای معادله $x^2 = -1$ بود. این که آیا هر معادله‌ی جبری به شکل (۱) در این مجموعه‌ی بزرگتر از اعداد جواب دارد یا خیر، موضوع قضیه‌ی اساسی جبر است که در این نوشته به آن می‌پردازیم. حل‌ناپذیری کلی معادلات درجه بزرگتر از ۴ نیز موضوعی بسیار جذاب است که در نهایت با تلاش‌های ریاضیدانانی چون رافینی، آبل و گالوا اثبات شد. البته باید تعریفی دقیق از حل‌ناپذیری ارائه شود که از مجال این نوشته کوتاه خارج است.

با اینکه تعریف دقیق پیوستگی و خواص آن، سال‌ها طول کشید که بدست آید ولی از قرن شانزدهم برای ریاضیدانان معلوم بود که معادلات جبری از درجه فرد:

$$x^{2n+1} + a_1x^{2n} + a_2x^{2n-1} + \cdots + a_{2n+1} = 0 \qquad (3)$$

در اعداد حقیقی جواب دارند. دلیل ساده این امر آن است که چون جمله غالب معادله فوق x^{2n+1} است برای xهای بسیار بزرگ مثبت، عددی مثبت و برای xهای بسیار بزرگ منفی، عددی منفی خواهد بود و با توجه به خاصیت مقدار میانی توابع پیوسته باید حداقل یک صفر داشته باشد.

نکته‌ی دیگر درباره‌ی اعداد مختلط آن است که فرمول صریح $x = \frac{-b\pm\sqrt{b^2-4ac}}{2a}$ برای ریشه‌های معادله‌ی $ax^2+bx+c=0$ نشان می‌دهد که هر معادله درجه ۲ در اعداد مختلط جواب دارد.

گاوس با یک اثبات استقرایی هوشمندانه نشان داد همین دو حقیقت ساده به تنهایی کافی هستند که نشان دهیم:

قضیه اساسی جبر: هر معادله به شکل (۱) و ضرایب حقیقی در اعداد مختلط جواب دارد.

تذکر: اگر معادله (۱) ضرایب مختلط داشته باشد در صورت ضرب در مزدوج آن به معادله‌ای با ضرایب حقیقی می‌رسیم بنابراین در قضیه فوق می‌توان شرط حقیقی بودن ضرایب را حذف کرد. با ادامه استفاده از قضیه‌ی فوق می‌توان ثابت کرد که معادله (۱) قابل تجزیه به صورت

$$a_0(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)$$

است که $\alpha_1, \ldots, \alpha_n$ اعدادی مختلط ریشه‌های معادله (۱) خواهند بود.

گاوس در طول عمر خود، ۵ اثبات مختلف برای این قضیه ارائه داد. در واقع موضوع رساله دکتری او نیز همین قضیه بود که در سال ۱۷۹۹ به چاپ رسید. البته اثبات اولیه او دارای خلل و فرجی است که بعدها توسط استروفسکی رفع شد.

اثبات جبری گاوس

هر عدد طبیعی n را می‌توان به‌طور یکتا به صورت $۲^k m$ که $k \geq ۰$ و m عددی فرد است، نوشت. استقراء گاوس روی توان k است. برای $k=۰$ می‌دانیم هر معادله درجه فرد در اعداد حقیقی ریشه دارد.

اگر $f(x)$ یک معادله درجه $۲^k m$ باشد گاوس معادله‌ی $F(x)$ از درجه $\binom{۲^k m}{۲} = \frac{۲^k m(۲^k m-۱)}{۲} = ۲^{k-۱}m(۲^k m-۱)$ را طوری می‌سازد که وجود ریشه برای آن، وجود ریشه‌ای برای $f(x)$ را نتیجه دهد. اما بنابرفرض استقرا $F(x)$ ریشه دارد و کار تمام می‌شود. روش ساختن $F(x)$ بسیار هوشمندانه است. فرض کنید در یک میدان بزرگ ریشه‌های معادله‌ی $f(x)$، $x_۱, \dots, x_n$ باشند. برای $x \in \mathbb{R}$ (یا $c \in \mathbb{C}$) تعریف کنید:

$$\alpha_{ij}(c) = x_i + x_j + cx_ix_j$$

و تعریف کنید:

$$F_c(x) = \prod_{۱\leq i<j\leq n} (x - \alpha_{ij}(c))$$

چون ضرایب $F_c(x)$ عباراتی متقارن برحسب $x_۱, \dots, x_n$ هستند بنابراین بر حسب ضرایب $f(x)$ قابل بیان بوده و در نتیجه اعدادی حقیقی هستند. بنابر فرض استقرا $F_c(x)$ حداقل یک ریشه‌ی مختلط دارد. چون بی‌نهایت انتخاب برای c داریم می‌توان دو عدد متمایز $c_۱$ و $c_۲$ را یافت به طوری که $i < j$ وجود داشته باشند که $x_i + x_j + c_۱x_ix_j$ و $x_i + x_j + c_۲x_ix_j$ هر دو حقیقی باشند بنابراین با حل یک دستگاه دو معادله دو مجهول (مجهول‌ها $x_i + x_j, x_ix_j$) بدست می‌آید که $x_i + x_j$ و x_ix_j هردو حقیقی هستند پس چون برای $A, B \in \mathbb{R}$

$$\begin{cases} x_i + x_j = A \\ x_ix_j = B \end{cases}$$

آن‌ها ریشه‌های معادله‌ی $x^۲ - Ax + B = ۰$ هستند و در نتیجه اعدادی مختلط می‌باشند.
این اثبات گاوس قابل تعمیم است.

قضیه ۱. *فرض کنید p یک عدد اول داده شده باشد و K میدانی باشد که هرچندجمله‌ای با ضرایب در K که درجه‌اش نسبت به p اول است حداقل یک ریشه در K داشته باشد. فرض کنید L یک توسیع K باشد که هر معادله با ضرایب در K و درجه p در L ریشه داشته باشد. آنگاه هر معادله با ضرایب در K در L حداقل یک ریشه دارد.*

در حالتی که $p=۲$، $K = \mathbb{R}$، $L = \mathbb{C}$ همان قضیه اساسی خواهد بود.

اثبات. هر عدد n را به‌طور یکتا می‌توان بصورت $p^k m$ نوشت که $k \geq ۰$ و m نسبت به p اول است. اثبات با استقرا روی k انجام می‌گیرد. $k=۰$ فرض قضیه است که هر معادله با درجه اول نسبت به p جواب دارد. اگر $f(x)$ یک معادله درجه $p^k m$ باشد یک معادله $F(x)$ از درجه

$$\binom{p^k m}{p} = \frac{p^k m(p^k m-۱)\cdots(p^k m-p+۱)}{p!} = p^{k-۱}\frac{m(p^k m-۱)\cdots(p^k m-p+۱)}{(p-۱)!}$$

می‌سازیم که بنابر فرض استقرا در K جواب دارد و نشان می‌دهیم این جواب، جوابی برای معادله‌ی $f(x)$ بدست می‌دهد و کار تمام می‌شود. روش ساختن $F(x)$ با تقلید از گاوس خواهد بود.

فرض کنید $x_۱, \dots, x_n$ ریشه‌های معادله $f(x)$ در یک میدان بزرگ باشند. برای هر pتایی $۱ \leq i_۱ < i_۲ < \cdots < i_p \leq n$ و عدد $c \in K$ تعریف کنید:

$$\alpha_{i_۱\dots i_p}(c) = \sum x_{i_k} + c\sum x_{i_k}x_{i_l} + c^۲\sum x_{i_k}x_{i_l}x_{i_q} + \cdots + c^{p-۱}x_{i_p}\dots x_{i_p}$$

(جملات جمع x_{i_n} جمع ضرب دوتایی آن‌ها، جمع ضرب سه‌تایی آن‌ها، ... تا ضرب همه آن‌ها است.)
دوباره:

$$F_c(x) = \prod(x - \alpha_{i_۱\dots i_p}(c))$$

را تشکیل می‌دهیم که بنابرفرض استقرا ریشه‌ای در K دارد. چون شرط قضیه نتیجه می‌دهد که K نامتناهی است (چرا؟) آنگاه می‌توان اعداد متمایز $c_1, \ldots, c_p$ در K یافت به طوری که $0 \le i_1 < \cdots < i_p \le n$ وجود داشته باشند که $\alpha_{i_1 \ldots i_p}(c_k)$ برای $k = 1, \ldots p$ در K باشند. با حل یک دستگاه p–معادله p مجهول بدست می‌آید که

$$\begin{cases} \sum x_{i_k} = A_1 \in K \\ \sum x_{i_k} x_{i_l} = A_2 \in K \\ . \\ . \\ . \\ x_{i_1} \cdots x_{i_p} = A_p \in K \end{cases}$$

بنابراین $x_{i_1}, \ldots, x_{i_p}$ ریشه‌های معادله $x^p - A_1 x^{p-1} + A_2 x^{p-2} - \cdots \pm A_p = 0$ هستند که مجددا بنابرفرض قضیه جوابی در K دارد، بنابراین یکی از x_{i_k}ها در K است و این همان چیزی است که می‌خواستیم ثابت کنیم. $\square$

تمرین: فرض کنید K یک میدان باشد که هر معادله درجه p که p یک عدد اول دلخواه است، در آن حداقل یک جواب داشته باشد ثابت کنید K بسته جبری است یعنی هر معادله درجه دلخواه در آن جواب دارد. اگر از اعداد اول تنها، یک عدد اول استثنا شود می‌توان مثال نقض برای این حکم پیدا کرد.