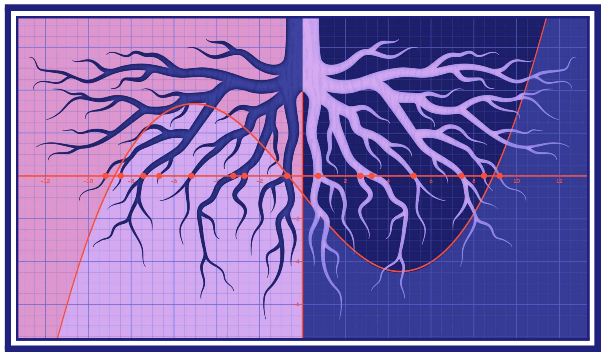
اثبات جدید ساختار پنهان معادلات رایج را روشن می‌کند*

لیلا اسلومن

مترجم: محمد فرخی درخشنده قوچان**

چکیده

حدس فان دِر وَرْدِن[1] ریاضی‌دانان را به مدت ۸۵ سال مجذوب خود کرد. راه‌حل آن نشان می‌دهد که ریشه‌های یک چندجمله‌ای چگونه به یکدیگر مربوط می‌شوند.



ریشه‌های معادلات چندجمله‌ای بسیاری از اسرار آن‌ها را آشکار می‌کند.

مَنْجول بارگاوا[2] استاد دانشگاه پرینستون آمریکا در یکی از آخرین مقالات خود حدسی با قدمت ۸۵ سال در مورد یکی از مسائل تاریخی ریاضیات را بررسی و حل می‌کند. این حدس بیان می‌کند ریشه‌های یک چندجمله‌ای داده‌شده مانند $x^2 - 3x + 2 = 0$ چه ارتباطی با هم دارند. به نقل از اَنْدرو گِرَنْوِل[3] استاد دانشگاه مونترال کانادا [4] «این یک مسئله مهم است، یک سؤال قدیمی مشهور. ایدهٔ جالب و نسبتاً متفاوت بارگاوا بسیار خلاقانه است».

برای شناخت چندجمله‌ای‌ها، ریاضی‌دانان معمولاً ریشه‌های آن‌ها را مطالعه می‌کنند، یعنی مقادیری از متغیر x که به ازای آن‌ها چندجمله‌ای مربوطه صفر می‌شود. اگر مقادیر ۱ یا ۲ را در چند جمله‌ای $x^2 - 3x + 2$ قرار دهیم، مقدار آن صفر می‌شود، یعنی ۱ و ۲ ریشه‌های این چندجمله‌ای هستند.

ازطرفی‌دیگر، چندجمله‌ای $x^2 - 5$ کمی متفاوت است. طبیعتاً این چندجمله‌ای در مجموعهٔ اعداد گویا (کسرهای به‌دست‌آمده از اعداد صحیح با مخرج ناصفر) ریشه‌ای ندارد. بنابراین، ریاضی‌دانان اعداد جدیدی مانند $\sqrt{5}$ را تعریف می‌کنند، یعنی عددی که مربع آن ۵ می‌شود و لذا ریشهٔ چندجمله‌ای $x^2 - 5$ خواهد بود. دراین‌صورت، واضح است که $-\sqrt{5}$ نیز ریشه چندجمله‌ای $x^2 - 5$ خواهد بود. این دو معادله تفاوت‌های دیگری هم با هم دارند. برای مثال ریشه‌های معادلهٔ $x^2 - 5 = 0$ می‌توانند در حل معادلات دیگر مانند $x^2 - 20 = 0$ نیز استفاده شوند (در این‌جا ما تنها چندجمله‌ای با ضرایب گویا را در نظر می‌گیریم). همان‌گونه که دیدیم $\sqrt{5}$ و $-\sqrt{5}$ می‌توانستند به‌جای هم در معادلهٔ $x^2 - 5 = 0$ قرار گیرند. این مسئله در مورد معادلهٔ $x^2 - 20 = 0$ نیز صدق می‌کند و $2\sqrt{5}$ و $-2\sqrt{5}$ نیز همین ویژگی را دارند. هرجا $\sqrt{5}$ استفاده شود، $-\sqrt{5}$ نیز استفاده می‌شود، هرجا $2\sqrt{5}$ استفاده شود، $-2\sqrt{5}$ نیز استفاده می‌شود.

شرایط بیان‌شده در پاراگراف قبل متداول‌ترین حالات ممکن هستند، به‌این‌معنا که در میان همهٔ چندجمله‌ای‌های ممکن به‌ندرت می‌توان یک چندجمله‌ای یافت که ریشه‌های آن از هم مستقل باشند. در مثال اولی ۱ و ۲ مستقل از هم هستند و هیچ‌کدام نمی‌تواند هنگام کار با چندجمله‌ای‌ها به جای دیگری استفاده شود. به قول فْرَنْک تُورْن[5] یکی از همکاران مَنْجول بارگاوا و استاد دانشگاه کالیفرنیای جنوبی[6] «اگر جای ۱ و ۲ را عوض کنیم تمام محاسبات به‌هم خواهد ریخت».

حدس فان دِر وَرْدِن که در سال ۱۹۳۶ توسط ریاضی‌دان هلندی بارتِل لیندِرْت فان دِر وَرْدِن ارائه شده است، بیان می‌کند که از بین همهٔ چندجمله‌ای‌های ممکن چه نسبتی از آن‌ها دارای ریشه‌های مستقل از هم هستند. اگرچه در چند دههٔ اخیر پیشرفت‌هایی در حل این مسئله انجام شده است، اما چشمگیر نبوده است. بااین‌وجود، اخیراً این پیشرفت‌ها شتاب بیشتری گرفته است و نتایج حاصله از آن به‌طورکلی باعث پیشرفت‌هایی در نظریهٔ اعداد نیز شده است. به‌نظر رایْنِر دیتْمَن[7] استاد دانشگاه رویال هالُووِی لندن[8] «به‌صورت ملموس‌تر، پرسش‌های کلاسیک در نظریهٔ اعداد در ۲۰ سال اخیر دوباره مورد توجه قرار گرفته‌اند». به‌دلایل بیان‌شده در بالا، برخی از ریاضی‌دانان این دستاوردهای جدید را به بارگاوا که در سال ۲۰۱۴

[1] Bartel Leendert van der Waerden [2] Manjul Bhargava [3] Andrew Granville [4] University of Montreal [5] Frank Thorne [6] University of South California [7] Rainer Dietmann [8] Royal Holloway University of London

برندهٔ مدال فیلدز، بالاترین نشان افتخار در ریاضیات نیز شده است نسبت می‌دهند. بنا به گفتهٔ تورْن «بارگاوا درهای جدید بسیاری را به روی نظریهٔ اعداد گشوده است و سایر ریاضی‌دانان را به اکتشافات جدید ترغیب می‌کند». در تابستان ۲۰۲۱ تحقیقات جدید بسیاری روی حدس فان دِر وَرْدِن انجام شده است. دیتْمن و همکارش سَم چاوْ[9] استاد دانشگاه ریک[10] انگلستان که پیش از این حالت‌هایی از حدس فان دِر وَرْدِن را حل کرده بودند، مقالهٔ جدیدی را در ۲۸ جون منتشر کرده‌اند که نتایج مهمی ارائه می‌کند. تنها یک هفته بعد، یک گروه شش‌نفره از ریاضی‌دانان مقالهٔ دیگری منتشر می‌کنند که نتایج مهمی دربردارد. در میانه این نتایج، بارگاوا در ۱ جولای یک سخنرانی برخط ارائه می‌کند و در آن اثباتی از یک نسخهٔ کمی متفاوت از حدس فان دِر وَرْدِن را بیان می‌کند. آن‌گونه که تورْن بیان می‌کند «او در حد یک تار مو به مسئله نزدیک شده بود».

تنها دو هفته بعد، بارگاوا در یک سخنرانی برخط در کنگرهٔ ریاضی آمریکا، کارهای جدید خود در مورد حالت کلی حدس فان دِر وَرْدِن را با سایر ریاضی‌دانان حاضر به اشتراک می‌گذارد. بارگاوا در نوامبر مقالهٔ خود را نیز در سایت آرکایو[11] منتشر می‌کند.

وان دِر وَرْدِن دنبال این مسئله بود که چه تعداد از چندجمله‌ای‌ها دارای ریشه‌های مستقل از هم هستند. اما با توجه به نامتناهی بودن تعداد چندجمله‌ای‌ها، باید روی چندجمله‌ای‌های موردنظر محدودیت‌هایی قائل می‌شد.

در ابتدا او چندجمله‌ای‌های با درجهٔ داده‌شده را درنظر گرفت. مثلا چندجمله‌ای $x^{۲} + ۱$ از درجهٔ ۲ یا چندجمله‌ای $x^{۱۷} - ۴$ از درجهٔ ۱۷ است. سپس او تنها خود را محدود به چندجمله‌ای‌های با ضریب پیشرو ۱ کرد. این چندجمله‌ای‌ها را چندجمله‌ای‌های تکین[12] می‌نامند. توجه کنید که مضارب ناصفر یک چندجمله‌ای، ریشه‌های یکسانی دارند، مثلاً ریشه‌های چندجمله‌ای $۲x^{۲} - ۶x + ۴$ همان ریشه‌های چندجمله‌ای $x^{۲} - ۳x + ۲$ هستند. با حذف چندجمله‌ای‌های ناتکین از شمردن چندجمله‌ای‌های مشابه اجتناب می‌شود.

در آخرین مرحله، او روی بقیهٔ ضرایب چندجمله‌ای نیز محدودیت گذاشت، به‌این‌صورت که بقیهٔ ضرایب می‌توانند در بازه‌ای مانند $[-H, H]$ از اعداد صحیح که در آن H یک عدد طبیعی است، تغییر کنند.

حدس فان دِر وَرْدِن بیان می‌کند که در بین چندجمله‌ای‌های بیان‌شده، یعنی چندجمله‌ای‌های تکین از درجهٔ n و ضرایب صحیح در بازهٔ $[-H, H]$ تقریباً $H^{n-۱}$ چندجمله‌ای وجود دارد که دارای ریشه‌های مستقل هستند، چیزی که بارگاوا در مقالهٔ خود آن را اثبات می‌کند.

مَنجول بارگاوا

اثبات بارگاوا چندین سال زمان برده است تا به‌شکل کنونی و نهایی خود برسد. آن‌گونه که بارگاوا خود می‌گوید «من بین هفت تا هشت سال روی این مسئله فکر کرده بودم. هربار که ایده‌ای به‌نظرم می‌رسید حتی اگر در مورد مسائل دیگری بود از خود می‌پرسیدم آیا ممکن است آن ایده برای حل این مسئله (حدس فان دِر وَرْدِن) هم مفید باشد؟»

راه‌حل نهایی، مجموعهٔ بزرگی از شگردها را به‌کارمی‌برد که بارگاوا در طول سالیان دراز جمع‌آوری کرده بود. در حقیقت، بارگاوا به‌جای این که تمام چندجمله‌ای‌ها را با هم بررسی کند، آن‌ها را به سه‌دسته جدا از هم تقسیم می‌کند. این دسته‌ها بر حسب مبین[13] چندجمله‌ای‌ها (که یک پارامتر عددی وابسته به ضرایب و لذا ریشه‌های چندجمله‌ای‌ها است) مشخص می‌شوند. بارگاوا به هر دسته با روش‌های متفاوتی حمله و آن را تجزیه و تحلیل می‌کند.

بارگاوا می‌گوید «روش‌های زیادی برای حل مسئله استفاده شد و این چیزی است که آن را برای من بسیار هیجان‌انگیز می‌کند. ایده‌های متنوع از شاخه‌های مختلف ریاضی همچون یک پازل جورچین کنار هم قرار گرفتند و منجر به حل کامل مسئله برای هر سه دسته شدند».

گرچه مقاله بارگاوا حدس فان دِر وَرْدِن را اثبات می‌کند، اما هنوز سؤالات بیشماری وجود دارند. به قول گِرَنْوِل «یکی از چیزهای مهمی که در مورد افرادی مثل بارگاوا می‌توان گفت، نبوغی است که منجر به طرح مسائل زیادی در حل مسئله اصلی می‌شود و این به

[9] Sam Chow [10] University of Warwick [11] https://arxiv.org/abs/2111.06507 [12] Monic polynomial [13] Discrimiant

بقیهٔ ریاضی‌دانان نیز فرصت فکر کردن و توسعهٔ آن‌ها را می‌دهد». برای مثال، ریاضی‌دانان می‌توانند از خود بپرسند اگر به‌جای اعداد گویا ضرایب چندجمله‌ای‌ها از یک مجموعهٔ بزرگتری انتخاب شوند (یعنی یک میدان شامل اعداد گویا) چه اتفاقی خواهد افتاد. آن‌ها سپس می‌توانند جزئیات مطرح‌شده در حدس فان دِر وَرْدِن را بررسی کنند، مثلاً اگر ریشه‌ها به‌شکل مورد نظر قابلیت جایگزینی نداشته باشند، به چه روش‌های دیگری می‌توان آن‌ها را جابه‌جا کرد؟ آیا الگو یا نظم خاصی در این بین وجود دارد؟

تورْن معتقد است «حتی اگر روش‌های استفاده‌شده توسط بارگاوا به‌طورمستقیم منجر به نتایج مهم دیگری در نظریهٔ اعداد نشوند، مقاله بارگاوا همچنان تأثیرات زیادی، اگر چه غیرملموس، از خود به‌جای خواهد گذاشت. به‌نظر من، برای درک بهتر مقاله (یا مسئله)، همچنان می‌توان فرض کرد مسئله باز است و به این فکر کرد که چه‌طور می‌توان آن نتایج را دوباره اثبات کرد. بارگاوا باور داشت این کار ممکن است و نشان داد حق با او بوده است.»

فرمول‌بندی دقیق حدس فان دِر وَرْدِن (مترجم)

فرض کنید

$$p(x) = a_n x^n + \cdots + a_1 x + a_0,$$

یک چندجمله‌ای با ضرایب متعلق به میدان $F := \mathbb{Q}$ [۱۴] باشد. بنابر قضیهٔ اساسی جبر می‌دانیم چندجمله‌ای $p(x)$ در میدان $\mathbb{C}$ [۱۵] دارای ریشه است و به‌صورت خطی تجزیه می‌شود، یعنی اعداد مختلطی مانند $\alpha_1, \dots, \alpha_n$ وجود دارند به‌طوری‌که

$$p(x) = a_n (x - \alpha_1) \cdots (x - \alpha_n).$$

اگر $E := F(\alpha_1, \dots, \alpha_n)$ کوچک‌ترین میدانی باشد که شامل F و ریشه‌های $\alpha_1, \dots, \alpha_n$ از $p(x)$ است، آن‌گاه E را توسیع شکافندهٔ چندجمله‌ای $p(x)$ روی میدان F می‌نامند. توسیع E از F را به‌صورت E/F نیز نمایش می‌دهند. نگاشت دوسویی $\theta : E \longrightarrow E$ را یک خودریختی میدان E گوییم هرگاه به‌ازای هر $x, y \in E$،

$$\theta(x+y) = \theta(x) + \theta(y) \quad \text{و} \quad \theta(xy) = \theta(x)\theta(y),$$

یعنی θ اعمال جمع و ضرب میدان را حفظ کند. مجموعه تمام خودریختی‌های میدان E را با نماد $\mathrm{Aut}(E)$ نشان می‌دهیم که خود با عمل ترکیب توابع تشکیل یک گروه می‌دهد. خودریختی θ از میدان E را یک خودریختی توسیع E/F گوییم هر گاه θ عناصر F را ثابت نگه دارد. دراین‌صورت، گروه خودریختی‌های توسیع E/F را می‌توان به‌صورت زیر تعریف کرد

$$\mathrm{Aut}(E/F) = \{\theta \in \mathrm{Aut}(E) \colon \ \alpha|_F = \mathrm{id}_F\},$$

که به آن گروه گالوای[۱۶] توسیع میدان E/F یا گروه گالوای چندجمله‌ای $p(x)$ روی میدان F نیز می‌گویند و با نماد $\mathrm{Gal}(E/F)$ نیز نشان می‌دهند. به‌سادگی می‌توان دید هر عنصر $\mathrm{Aut}(E/F)$ مانند θ جایگشت یکتایی مانند π_θ روی ریشه‌های چندجمله‌ای $p(x)$ القا می‌کند. در حقیقت به‌ازای هر $\alpha \in E$،

$$\begin{aligned} \theta(p(\alpha)) &= \theta(a_n \alpha^n + \cdots + a_1 \alpha + a_0) \\ &= a_n \theta(\alpha)^n + \cdots + a_1 \theta(\alpha) + a_0 \\ &= p(\theta(\alpha)), \end{aligned}$$

که از آن نتیجه می‌شود $p(\alpha) = 0$ اگر و تنها اگر $p(\theta(\alpha)) = 0$. همچنین با توجه به اینکه میدان E توسط F و ریشه‌های $p(x)$ به‌دست می‌آید و θ به‌عنوان خودریختی توسیع E/F عناصر F را ثابت نگه می‌دارد اثر θ روی ریشه‌های $p(x)$ آن را به‌طور کامل مشخص می‌کند. بنابراین، $\mathrm{Aut}(E/F)$ با گروهی از جایگشت‌های ریشه‌های $p(x)$، یعنی $\alpha_1, \dots, \alpha_n$ یکریخت است.

برای مثال اگر چندجمله‌ای $x^2 - 5$ را در نظر بگیریم، آن‌گاه

$$E = \mathbb{Q}(\sqrt{5}, -\sqrt{5}) = \{a + b\sqrt{5} \colon \ a, b \in \mathbb{Q}\},$$

و

$$\mathrm{Aut}(E/F) = \{\mathrm{id}_E, \theta\},$$

که در آن به ازای هر $a, b \in \mathbb{Q}$،

$$\theta(a + b\sqrt{5}) = a - b\sqrt{5}.$$

---

[۱۴] در حالت کلی F می‌تواند هر میدان دلخواهی باشد. [۱۵] در حالت کلی می‌توان بستار جبری میدان دلخواه F را درنظر گرفت، یعنی میدانی مانند $\bar{F}$ که ریشه‌های هر چندجمله‌ای با ضرایب متعلق به F در $\bar{F}$ است. بستار جبری هر میدان دلخواه وجود دارد و تا حد یکریختی یکتاست. برای مثال بستار میدان اعداد گویا، میدان اعداد جبری و بستار میدان اعداد حقیقی، میدان اعداد مختلط است. [۱۷] در مبحث جایگشت‌ها نماد () برای جایگشت همانی و نماد $(\alpha\ \beta)$ برای جایگشتی که α را به β و β را به α تبدیل می‌کند استفاده می‌شود.

[16] Galois group

ازآنجایی‌که

$$\pi_{\mathrm{id}_E} = () \quad \text{و} \quad \pi_\theta = (-\sqrt{5}\ \sqrt{5})^{[17]},$$

هر دو جایگشت ممکن روی مجموعهٔ ریشه‌های $p(x)$ هستند، داریم $\mathrm{Aut}(E/F) \cong S_2$.

با توجه به مطالب بیان‌شده در بالا فرمول‌بندی کامل حدس فان دِر وَرْدِن به صورت زیر خواهد بود:

حدس فان دِر وَرْدِن. فرض کنید H یک عدد طبیعی باشد. در این صورت تعداد چندجمله‌ای‌های تکین از درجه n با ضرایب صحیح به‌صورت

$$p(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0,$$

که در آن

$$|a_0|, \ldots, |a_{n-1}| \leq H,$$

و گروه گالوای $p(x)$ روی میدان اعداد گویا با S_n یکریخت نیست برابر با $O(H^{n-1})$ است، یعنی با مضرب ثابتی از H^{n-1} به‌عنوان تابعی از H مجانب است.

با توجه به اینکه $(2H+1)^n$ چندجمله‌ای تکین با ضرایب صحیح متعلق به بازهٔ $[-H, H]$ وجود دارد، حدس فان دِر وَرْدِن بیان می‌کند تقریباً تمام این چندجمله‌ای‌ها دارای گروه گالوایی هستند که با S_n یکریخت است، یعنی ریشه‌های چندجمله‌ای‌های مربوطه از تقارن کامل برخورداند و هر جایگشت از ریشه‌ها همان ویژگی‌های جبری‌ای دارد که ترتیب اولیه از ریشه‌ها دارد.

*Leila Sloman, New Proof Illuminates the Hidden Structure of Common Equations, Quanta Magazine, April 21, 2022.

**دانشگاه تحصیلات تکمیلی علوم پایه زنجان