which yield homomorphisms

$$R^nT(A'',C) \to R^{n+1}T(A',C). \tag{3}$$

The independence of (3) from the choice of (2) follows readily from 2.3.

We similarly define the connecting homomorphisms

$$R^nT(A,C') \to R^{n-1}T(A,C'') \tag{4}$$

for each exact sequence

$$0 \to C' \to C \to C'' \to 0. \tag{5}$$

PROPOSITION 4.1. *Let*

$$\begin{array}{ccccccccc} 0 & \to & A' & \to & A & \to & A'' & \to & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \to & A_1' & \to & A_1 & \to & A_1'' & \to & 0 \end{array} \qquad \begin{array}{ccccccccc} 0 & \to & C_1' & \to & C_1 & \to & C_1'' & \to & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \to & C' & \to & C & \to & C'' & \to & 0 \end{array}$$

be commutative diagrams with [illegible] Then the following diagrams are commutative.

$$\begin{array}{ccccccc} R^nT(A'',C) & \to & R^{n+1}T(A',C) & & R^nT(A,C'') & \to & R^{n+1}T(A,C'') \\ \downarrow & & \downarrow & & \downarrow & & \downarrow \\ R^nT(A_1'',C) & \to & R^{n+1}T(A_1',C) & & R^nT(A,C_1'') & \to & R^{n+1}T(A,C_1'') \end{array}$$

$$\begin{array}{ccccccc} R^nT(A'',C) & \to & R^{n+1}T(A',C) & & R^nT(A,C') & \to & R^{n+1}T(A,C'') \\ \downarrow & & \downarrow & & \downarrow & & \downarrow \\ R^nT(A'',C_1) & \to & R^{n+1}T(A',C_1) & & R^nT(A_1,C') & \to & R^{n+1}T(A_1,C'') \end{array}$$

The diagram

$$\begin{array}{ccc} R^nT(A'',C') & \to & R^nT(A',C') \\ \downarrow & & \downarrow \\ R^{n+1}T(A'',C'') & \to & R^{n+2}T(A',C'') \end{array}$$

is anticommutative. The sequences

$$\cdots \to R^nT(A',C) \to R^nT(A,C) \to R^nT(A'',C) \to R^{n+1}T(A',C) \to \cdots \tag{6}$$

$$\cdots \to R^nT(A,C'') \to R^nT(A,C) \to R^nT(A,C') \to R^{n+1}T(A,C'') \to \cdots \tag{7}$$

are exact.

PROOF. The first four commutativity relations are trivial consequences of the definitions and of 2.3. The exactness of the sequences follows from the fact that these are homology sequences of suitable exact sequences of complexes. It remains to verify the anticommutativity relation.

PROPOSITION 3.2. *If T is defined for modules over hereditary rings, then $R^nT = 0$ if n exceeds the number of variables in T.*

PROOF. Consider the case of 2 variables as above. Since A is a module over a hereditary ring the injective resolution X of A may be chosen with $X^n = 0$ for $n > 1$. Similarly the projective resolution Y of C may be chosen with $Y_n = 0$ for $n > 1$. Thus in the complex $T(X, Y)$ we have $T^n(X, Y) = 0$ for $n > 2$. Thus $R^nT = 0$ for $n > 2$.

In defining RT we took injective resolutions for all covariant variables and projective resolutions for all contravariant variables. If instead we take projective resolutions for all the covariant variables and injective resolutions for all contravariant variables we obtain a functor $LT = \sum L_nT$, where L_nT is the *n-th left derived functor* of T. We have $L_nT = 0$ for $n < 0$; the indices have been lowered to avoid negative numbers.

As before if X is an acyclic left complex over A and Y is an acyclic right complex over C, we have the homomorphism

$$LT(A,C) \to H(T(X,Y)). \tag{2a}$$

If X is a projective left complex over A and Y is an injective right complex over C, then

$$H(T(X,Y)) \to LT(A,C). \tag{3a}$$

PROPOSITION 3.1a. *If A is projective and C is injective then $LT(A,C)$ coincides with $T(A,C)$, i.e. $L_nT(A,C) = 0$ for $n > 0$ and $L_0T(A,C) = T(A,C)$. If the functor T is exact then the same holds for all modules A and C.*

PROPOSITION 3.2a. *If T is defined for modules over hereditary rings then $L_nT = 0$ if n exceeds the number of variables in T.*

4. CONNECTING HOMOMORPHISMS

Consider a functor $T(A,C)$ as in 3, and let

$$0 \to A' \to A \to A'' \to 0 \tag{1}$$

be an exact sequence. By 2.2 there exists a sequence

$$0 \to X' \to X \to X'' \to 0 \tag{2}$$

which is an injective resolution of (1). Let further Y be a projective resolution of C. Since for each degree the sequence (2) splits, it follows that the sequence of complexes

$$0 \to T(X',Y) \to T(X,Y) \to T(X'',Y) \to 0$$

is exact. There result connecting homomorphisms

$$H^n(T(X'',Y)) \to H^{n+1}(T(X',Y))$$

بسم‌الله الرحمن الرحیم

مجلهٔ ریاضی مرکز نشر دانشگاهی

شمارهٔ ۸۵ خیابان پارک، خیابان دکتر بهشتی، تهران ۱۵۱۳۴

بهای این شماره ۵۵۰۰ ریال؛ حق اشتراک سالانه برای داخل کشور ۱۱۰۰۰ ریال.
(برای دانشجویان با ۳۰٪ تخفیف)

وجه اشتراک به حساب شمارهٔ ۹۰۰۰۹ بانک ملی شعبهٔ خیابان پارک تهران به نام مرکز نشر دانشگاهی واریز شود.

نشر ریاضی از انتشارات ادواری مرکز نشر دانشگاهی است که هر شش ماه یک بار منتشر می‌شود. هدفهای اصلی انتشار مجله عبارت است از

- معرّفی پیشرفتهای جدید ریاضیات؛
- معرّفی شاخه‌های جدید علوم ریاضی و همچنین مباحثی که مورد توجّه پژوهشگران است؛
- معرّفی جنبه‌های کاربردی، فرهنگی، فلسفی، و تاریخی ریاضیات؛
- معرّفی کارهای ریاضی پژوهان فارسی زبان و ایجاد ارتباط بین آنان؛
- طرح مسائل آموزشی ریاضیات، به ویژه مسائل مربوط به آموزش ریاضیات دانشگاهی در ایران.

نشر ریاضی از همکاری تمام علاقه‌مندان استقبال می‌کند. مقاله‌های ارسالی باید در چهارچوب هدفهای فوق و با سبکی مشابه با سبک مقاله‌های چاپ‌شده در *نشر ریاضی* باشد. به همکارانی که مایل‌اند مقاله‌ای را به فارسی برگردانند و برای درج به مجله بفرستند توصیه می‌شود ابتدا اصل مقاله را با ذکر منبع برای بررسی و تصویب ارسال دارند. ترجمهٔ آزاد پذیرفته نمی‌شود، و فرستادن اصل مقاله‌های ترجمه شده الزامی است. مقاله‌های ارسالی پس فرستاده نمی‌شود. هر مقاله‌ای مطابق ضوابط رایج داوری می‌شود. هیأت ویراستاران در رد، قبول، و حک و اصلاح مقالات آزاد است. ویرایش، نگارش، انتخاب واژه‌ها، و ضبط اسامی و اعلام مطابق ضوابط گروه ریاضی در مرکز نشر دانشگاهی انجام خواهد گرفت.

یادآوری

- متن مقاله روی یک طرف کاغذ، یک خط در میان، و با حاشیهٔ کافی ماشین، یا با خط خوانا نوشته شود.
- نحوهٔ نگارش، بخشبندی، فرمول‌نویسی، و شیوهٔ ارجاع به منابع حتی‌المقدور مطابق با مقاله‌های چاپ شدهٔ در *نشر ریاضی* باشد.
- فهرست معادلهای انگلیسی اصطلاحاتی که در مقاله به‌کار می‌رود همراه با مقاله فرستاده شود.

نشر ریاضی

سال ۱۱، شمارهٔ ۲

تاریخ انتشار: مهر ۱۳۷۹

شمارهٔ پیاپی: ۲۲

nashriaz@rose.ipm.ac.ir

صاحب امتیاز: مرکز نشر دانشگاهی

مدیر مسؤول: سیاوش شهشهانی

- دستیارفنی: زهرا دلاوری
- طراح: شکوه پیله‌فروشها
- حروفچین و صفحه‌آرا: سیده مریم طاهریان
- ناظر چاپ: علی صادقی
- لیتوگرافی: مردمک
- چاپ و صحافی: منفرد (میدان شهدا، خ شهید کفایی، شمارهٔ ۳۶)

فهرست

روی جلد

دو صفحه از کتاب جبر هومولوژیک اثر هانری کارتان و ساموئل آیلنبرگ

رک. «نقد ۳۲ کتاب مهم قرن»

گزارش

با گذشت بیش از نیمی از سال ۲۰۰۰، شاهد اجرای تعدادی از برنامه‌های پیش‌بینی‌شده برای سال جهانی ریاضیات بوده‌ایم. از جمله فعالیتهای مربوط به سال جهانی ریاضیات در کشورمان باید از تأسیس خانه‌های ریاضیات، کمک به ترجمه و نشر تعدادی از آثار معروف ریاضی، و کمک به برگزاری گردهمایی‌های متعددی در علوم ریاضی نام ببریم. سی‌ویکمین کنفرانس ریاضی کشور نیز که در شهریور ماه سال جاری در دانشگاه تهران برگزار شد، ویژگیهای خاصی به مناسبت تقارن با سال جهانی ریاضیات داشت. خبرنامهٔ سال جهانی ریاضیات که تاکنون ده شمارهٔ آن به چاپ رسیده است، حاوی آخرین گزارشها از فعالیتهای مربوط به سال جهانی ریاضیات در ایران است. برای دریافت این خبرنامه، خواستاران می‌توانند با نشانی زیر مکاتبه کنند:

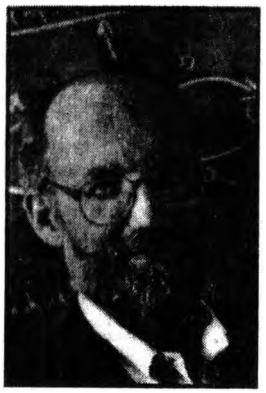
دبیرخانهٔ ستاد ملّی سال جهانی ریاضیات
دفتر معاونت پژوهشی وزارت علوم، تحقیقات و فناوری
تقاطع انقلاب و فلسطین، صندوق پستی ۵۵۴ـ۱۳۱۴۵

در بخشهای بعدی این گزارش، مطالبی دربارهٔ دو رویداد جهانی مرتبط با سال جهانی ریاضیات و نیز گزارش و اظهار نظری در بارهٔ سی‌ویکمین کنفرانس ریاضی کشور خواهد آمد.

جان باروایز (۱۹۴۲ـ۲۰۰۰)

جان باروایز[1] در صبح روز یکشنبه ۵ مارس ۲۰۰۰ در سن ۵۷ سالگی در بلومینگتن ایندیانا درگذشت. باروایز به‌خاطر تحقیقات وسیعش در منطق و شاخه‌های وابسته به آن، شامل فلسفه، علوم کامپیوتر، و زبانشناسی، شهرهٔ خاص و عام است. کارهای او مشخصاً در نظریهٔ مدلها، زبانهای نامتناهی، معناشناسی، زبان طبیعی، و نظریهٔ اطلاعات بود.

1. K. Jon Barwise



جان باروایز

او درجهٔ کارشناسی خود را در ریاضیات و فلسفه از دانشگاه ییل در ۱۹۶۳ و دکتری در ریاضیات را از دانشگاه استنفرد در ۱۹۶۷ زیر نظر سالومون ففرمن دریافت کرد. در همانجا اولین «مرکز مطالعهٔ زبان و اطلاعات» را بنیان گذاشت. باروایز در دانشگاههای مختلفی مثل ییل، ویسکانسین، و ایندیانا به تحقیق و تدریس پرداخت. در سال ۱۹۹۲، دانشگاه پنسیلوانیا دکتری افتخاری علوم را به او اعطا کرد.

از باروایز چندین کتاب، از جمله نظریهٔ مجموعه‌های پذیرفتنی[1] و دروغگو[2] (با همکاری اچمندی[3]) باقی‌مانده است. وی علاوه بر نوشتن دهها مقاله، ویراستاری کتاب معروف راهنمای منطق ریاضی[4] را هم به‌عهده داشت. باروایز علاوه بر اینکه منطقدان بزرگی بود، سازمان‌دهنده و الهامبخش نیز بود. نشر ریاضی امیدوار است در یکی از شماره‌های آینده مقاله‌ای را به بررسی آثار این عالم بزرگ منطق اختصاص دهد.

جوایز مؤسسهٔ کلی به مناسبت هزاره

در سال ۱۹۹۹، تأسیس یک بنیاد ریاضیات به همت یک سرمایه‌دار آمریکایی به نام لندن کلی[5] اعلام شد. این سازمان که «مؤسسهٔ ریاضیات کلی» نام دارد، اقدامات متعددی را در حمایت از پیشبرد علوم ریاضی در برنامهٔ خود قرار داده است که از آن جمله‌اند بورسها و جوایز تحقیقاتی در سطوح سنی مختلف، حمایت از تیم المپیاد ریاضی کشور آمریکا، برگزاری المپیاد ریاضی سال ۲۰۰۱ در کشور آمریکا، و اعلام هفت جایزهٔ یک میلیون دلاری در ریاضیات به مناسبت آغاز هزارهٔ سوم. در مراسمی که در تاریخ ۲۴ و ۲۵ ماه مه ۲۰۰۰ در کولژ دو فرانس در پاریس برگزار شد، این مؤسسه اعلام کرد که هفت جایزه هر یک به مبلغ یک میلیون دلار برای هفت مسألهٔ مهم حل‌نشدهٔ ریاضی در نظر گرفته است. این مسائل به شرح زیرند.

۱. $P \stackrel{?}{=} NP$. این مسألهٔ معروف برای نخستین بار در سال ۱۹۷۱ به وسیلهٔ استیون کوک عنوان شد. مقصود از P، مجموعهٔ مسائلی است که حل آنها با الگوریتمهای زمان‌چندجمله‌ای مقدور است و NP مجموعهٔ مسائلی است که صحت هر جواب پیشنهاد شده برای آنها را بتوان در زمانِ چندجمله‌ای تحقیق کرد.

۲. **فرضیهٔ ریمان.** این تنها مسأله در این مجموعهٔ هفت‌تایی است که در فهرست معروف ۲۳ مسألهٔ هیلبرت در آغاز قرن بیستم نیز قرار داشت

1. Admissible Set Theory 2. The Liar 3. J. Etchemendy
4. Handbook of Mathematical Logic 5. Landon T. Clay

و عبارت از این است که: آیا قسمت حقیقی همهٔ صفرهای نابدیهی تابع زتای ریمان برابر $\frac{1}{2}$ است؟

۳. حدس پوانکاره. معروفترین حدس حل‌نشده در توپولوژی مبنی بر اینکه هر خمینهٔ سه‌بعدی فشرده، بی‌لبه و ساده‌همبند، با کرهٔ سه‌بعدی همسانریخت است.

۴. حدس هاج. ریاضیدان انگلیسی هاج[1] حدود نیم قرن پیش این حدس را مطرح کرد که روی یک واریتهٔ [چندگونای] جبری افکنشی مختلط ناتکین، هر ردهٔ هاج یک ترکیب خطی با ضرایب گویا از رده‌های دورهای جبری است.

۵. حدسهای برچ و سوئینرتون-دایر[2]. برای هر خم بیضوی روی Q، مرتبهٔ صفرشدن تابع L آن در ۱، برابر رتبهٔ گروه آبلی نقاط گویا روی خم است.

۶. معادلات ناویر-استوکس. وجود و هسواری جوابهای این معادلات مهم مکانیک سیالات، تحت شرایط معقول اولیه و مرزی، هنوز به اثبات نرسیده است.

1. Hodge 2. Birch & Swinnerton-Dyer

۷. نظریهٔ یانگ-میلز. وجود میدانهای یانگ-میلز و نقصان جرم[1] برای معادلات کوانتومی یانگ-میلز هنوز به اثبات نرسیده است.

این هفت مسأله از میان مسائل گوناگونی که از طرف ریاضیدان سرشناس به‌عنوان مهمترین مسائل حل‌نشدهٔ ریاضیات اعلام شده بودند، توسط کمیتهٔ ویژه‌ای انتخاب شده‌اند. ضرب‌الاجلی برای حل این مسائل اعلام نشده است. قرار است هر حل پیشنهادیْ مسیر عادی چاپ و نشر در مجلات ریاضی را طی کند و چنانچه پس از گذشت حداقل دو سال از نشر مقالهٔ مربوط، اثر مورد قبول جامعهٔ ریاضی قرار گیرد، جایزه اعطا شود. کمیتهٔ مشاوران علمی جایزه متشکل است از الن کُن، اندرو وایلز، ادوارد ویتن، و آرتر جفی، برای اطلاع بیشتر از جوایز و سایر فعالیتهای مؤسسهٔ کلی خوانندگان می‌توانند به آدرس اینترنتی زیر مراجعه کنند:

http://www.claymath.org

1. mass gap

چالشهای ریاضی در قرن ۲۱

بزرگترین برنامهٔ انجمن ریاضی آمریکا به مناسبت سال جهانی ریاضیات، گردهمایی ۷ تا ۱۲ اوت ۲۰۰۰ در دانشگاه کالیفرنیای لس آنجلس (UCLA) بود. در این گردهمایی از سی ریاضیدان دعوت شده بود چالشهای بزرگی را که در قرن ۲۱ در مقابل ریاضیدانان قرار دارد توصیف کنند. فهرست سخنرانان و عنوان سخنرانیها را در جدول ملاحظه می‌کنید. [مرجع جدول: http://www.ams.org/amsmtgs/mathchall_speak.html]

نام سخنران	دانشگاه	عنوان سخنرانی
James G. Arthur	University of Toronto	The principle of functoriality
Alexander A. Beilinson	University of Chicago	On the Geometric Langlands Conjecture
Michael V. Berry	University of Bristol	Wave asymptotics and borderland physics
Haim Brezis	University of Paris XI/Rutgers University	The interplay between analysis and topology in some nonlinear PDEs
Alain Connes	College de France	Noncommutative geometry
David Leigh Donoho	Stanford University	High-dimensional data analysis: The blessings and curses of dimensionality
Charles L. Fefferman	Princeton University	Unsolved problems of fluid mechanics
Michael H. Freedman	Microsoft Research	The physics of computation
Ronald L. Graham	University of California, SanDiego	Mathematics in the 21st century: Problems and prospects
Helmut H. W. Hofer	Courant Institute, New York University	Dynamical systems at the interface of symplectic geometry and three-dimensional topology
Richard M. Karp	University of Washington	Algorithmic challenges from genomics and molecular biology
Sergiu Klainerman	Princeton University	On the analysis of geometric evolution equations

Maxim Kontsevich	Institut des Hautes Etudes Scientifiques	Operads of little discs in algebra and topology
Peter D. Lax	Courant Institute, New York University	Mathematics and computing
Simon Levin	Princeton University	Ecosystems as complex adaptive systems
László Lovász	Microsoft Research	Classical mathematics and new challenges
David Mumford	Brown University	Modeling perception and inference in intelligent systems
Peter Sarnak	Princeton University	Some problems in number theory and related analysis
Saharon Shelah	Hebrew University /Rutgers University	Logical dreams
Peter W. Shor	AT& T Labs	Quantum computation
Yakov G. Sinai	Princeton University	From renormalization in dynamics to renormalization in probability and statistical physics
Richard P. Stanley	Massachusetts Institute of Technology	Recent progress in algebraic combinatorics
Dennis P. Sullivan	The CUNY Graduate School	String topology
Clilford Taubes	Harvard University	Bliss and ignorance in 4-dimensions
Jean F. Taylor	Rutgers University	Mathematics and materials science
William P. Thurston	University of California, Davis	Three-dimensional topology and geometry
Karen Uhlenbeck	University of Texas, Austin	Geometric partial differential equations: From Hilbert's 23rd Problem to nonlinear waves
S. R. S. Varadhan	Courant Institute, New York University	Stochastic analysis and applications
Edward Witten	Institute for Advanced Study, Princeton University	The mathematical impact of quantum fields and strings
Shing-Tung Yau	Harvard University	Geometry and its relation to physics

نگاهی به سی‌ویکمین کنفرانس ریاضی ایران

زمان آن فرارسیده است که هدفهای برگزاری کنفرانسهای ریاضی کشور در مقطع زمانی جاری مورد توجه قرار گیرد. اگر کنفرانسها را صرفاً محلی برای عرضهٔ آخرین دستاوردهای علوم ریاضی کشور قلمداد کنیم این سؤال پیش می‌آید که چنانچه مقاله‌های ارائه شده در سطح تخصصی قابل قبول باشند آیا بهتر نیست در جمع محدودتر سمینارهای تخصصی، مانند سمینار جبر، سمینار آنالیز، سمینار ریاضیات کاربردی، سمینار گراف، ترکیبیات و ... عرضه شوند تا این سمینارها غنیتر شوند؟ به‌علاوه ارزیابی مقاله‌ها در سمینارهای تخصصی دقیقتر خواهد بود. پس لازم است جنبهٔ فرهنگی کنفرانسهای ریاضی را جنبهٔ غالب بدانیم. سخنرانیهای عمومی (البته با کیفیت ممتاز)، تبادل‌نظر بین متخصصان شاخه‌های مختلف ریاضی، دیدارها، مجمع عمومی و سایر فعالیتهای جمعی انجمن ریاضی ایران، و بالاخره مطرح کردن ریاضیدانان و ریاضیات کشور در کل جامعه و رسانه‌های گروهی، بخش مهمی از اهداف کنفرانسهای ریاضی را تشکیل می‌دهند. سی‌ویکمین کنفرانس ریاضی ایران نشان داد که جامعهٔ ریاضی به سطح فرهنگی بسیار خوبی رسیده است: مراسم افتتاحیه با پیام ریاست جمهوری، اهدای جوایز مختلف از قبیل جایزهٔ دکتر عباس ریاضی برای بهترین مقالهٔ کنفرانس قبلی، جایزهٔ دکتر محسن هشترودی برای بهترین مقالهٔ سمینار دانشجویی، جایزهٔ دکتر منوچهر وصال برای بهترین مقالهٔ سمینار آنالیز و بالاخره اعلام اسامی نخستین اعضای افتخاری انجمن ریاضی ایران، همگی نشانه‌های ارتقای فرهنگ جامعهٔ ریاضی در تقارن با سال جهانی ریاضیات بود. نهادینه شدن این جوایز نقش مهمی در ارتقای علمی کنفرانسها و سمینارهای ریاضی کشور خواهد داشت.

البته به موازات رسالت فرهنگی کنفرانس، رسالت علمی آن نیز باید مدنظر قرار گیرد. به اعتقاد بنده سخنرانان مدعو از خارج و از داخل کشور

نقش بسیار مهمی در کنفرانس ایفا می‌کنند و می‌توانند هم جنبهٔ فرهنگی و هم جنبهٔ علمی کنفرانس را غنیتر سازند.

در آذر ماه ۷۸، پروفسور دیوید آیزنباد رئیس مرکز تحقیقات علوم ریاضی در برکلی، پروفسور رانلد گراهام از بل‌لب، پروفسور رابرت ژیابرت از دانشگاه دلاویر، پروفسور حیدر رجوی از دانشگاه دالهوزی کانادا و پروفسور فریدون شهیدی از دانشگاه پردوی آمریکا با اشتیاق دعوت کنفرانس را پذیرفتند. لیکن به عللی سه نفر اول در فروردین ماه انصراف خود را اعلام نمودند که البته برای مسؤولان برگزاری بسیار دلسردکننده بود ولی رفع این علتها نه در امکان استادان مدعو بود و نه در محدودهٔ اختیارات مسؤولان کنفرانس. به‌هر حال مسائل جاری کشور مستقیماً روی همکاریهای بین‌المللی اثر می‌گذارد. علی‌رغم این مسأله با حضور فعال و سخنرانیهای دکتر شهیدی، دکتر رجوی، دکتر خرقانی و ریاضیدانان مدعو داخلی، نه تنها کمبودی احساس نمی‌شد بلکه جلسات سخنرانیهای عمومی افتخارآفرین بود. این تجربه نشان می‌دهد که دعوت از ریاضیدانان طراز اول ایرانی مقیم خارج از جنبه‌های مختلف مفیدتر است و با توجه به هزینهٔ زیاد بلیط هواپیما، در صورت امکان حضور یکی دو نفر از ریاضیدانان معروف خارجی در کنار ریاضیدانان ایرانی کفایت می‌کند.

کمیتهٔ علمی کنفرانس به کمک مشاورین علمیْ مقاله‌های ارسالی را به سه مقوله تقسیم کرد: مقالات پذیرفته شده برای ارائه و چاپ در مجموعهٔ مقالات، مقالات پذیرفته شده فقط برای ارائه در کنفرانس، و مقالات غیرقابل ارائه. مسلماً انتخاب داوران متخصص در زمینهٔ هر مقاله در جامعهٔ ریاضی محدود کشور تا حدی مشکل بود ولی در این راه تلاش شد و کمیتهٔ علمی در روند داوری بر اصالت مقالات تأکید داشت. البته با چشم‌پوشی از مواردی محدود، نتیجهٔ کار رضایت‌بخش به نظر می‌رسد. شرکت‌کنندگان از برگزاری جلسات سخنرانیهای تخصصی و نظم و سطح علمی آنها اظهار رضایت می‌کردند.

یکی از وجوه بارز این کنفرانس، چاپ مجموعهٔ مقالاتْ قبل از برگزاری بود که با کوشش همکاران جوان گروه ریاضی و علوم کامپیوتر دانشگاه تهران انجام گرفت. تعدادی از مؤلفان، فایل مناسبی برای پیاده کردن مقاله‌شان ارسال نکرده بودند که در نتیجه مسؤولان کنفرانس نتوانستند مقالهٔ آن عده از مؤلفان را چاپ کنند. در مجموع، خلاصهٔ ۱۳۱ سخنرانی در خلاصهٔ مقالات درج گردید و از ۸۱ مقالهٔ پذیرفته‌شده ۷۰ مقاله به طور کامل در مجموعهٔ مقالات چاپ شد که ۵۸ مقالهٔ آن در مجلد انگلیسی و بقیه در مجلد فارسی بود. امسال برای اولین بار در تاریخ کنفرانسهای ریاضی ایران، خلاصهٔ مقالات و مجموعهٔ مقالات در صفحهٔ وب کنفرانس در دسترس قرار گرفت و شاید در آینده این روش بتواند جایگزین چاپ مجموعهٔ مقالات بشود که کاری بسیار پرزحمت و پرهزینه است.

مسؤولان برگزاری کنفرانس برای تأمین هزینه‌های آن تلاشهای قابل توجهی کردند. ستاد ملی سال جهانی ۲۰۰۰، نهاد ریاست جمهوری، وزارت پست و تلگراف و تلفن و سازمان مدیریت و برنامه‌ریزی، تأمین هزینه‌های کنفرانس را برعهده گرفتند ولی دانشگاه تهران که میزبان کنفرانس بود نتوانست خود نیز بودجه قابل توجهی را به کنفرانس اختصاص دهد که با توجه به شرایط ویژهٔ این دانشگاه، تا حدی قابل درک است.

در کنار کنفرانس ریاضی در دانشگاه تهران، نمایشگاه کتاب برگزار نشد. علت این امر در وهلهٔ اول برگزاری نمایشگاههای اخیر کتاب در سطح وسیعی بود که تصور می‌شد برگزاری نمایشگاهی ضعیفتر لطفی ندارد. دلیل دوم، مشکلات بودجهٔ ارزی برای خرید بخشی از کتابهای نمایشگاه بود که تا روزهای آخر بدون نتیجه برای تأمین این بودجه تلاش شد.

چند نکته اساسی در مورد کنفرانسهای ریاضی کشور قابل ذکر است:

نخست اینکه در سالهای اخیر، دانشگاههای میزبان در برگزاری کنفرانس با مشکلات فراوانی روبه‌رو بوده‌اند. دانشگاه میزبان هر سال، تجربه‌های دانشگاههای دیگر را از نو تجربه می‌کند، و تشکل یا تیمی سازمان‌یافته مثلاً در انجمن ریاضی ایران، برای انتقال این تجربه‌ها وجود ندارد. تشکیل یک تیم انتشارات و یک تیم تدارکات عمومی کنفرانسها به صورت نیمه‌متمرکز که اغلب اعضای آنها حرفه‌ای و ثابت باشند و بقیهٔ اعضا برای هر کنفرانس از طرف دانشگاه میزبان تعیین شوند، می‌تواند گام بسیار مهمی در تداوم و تسهیل برگزاری کنفرانسها و تکامل آنها از جنبه‌های مختلف باشد و سبب ارتقای فرهنگی و علمی ریاضیکاران کشور گردد وهزینه‌های برگزاری را بسیار کاهش دهد. چارچوب این تشکل می‌تواند به گونه‌ای تدوین شود که جاذبه‌های برگزاری کنفرانس برای دانشگاههای میزبان افزایش یابد.

نکتهٔ دوم، موضوع برگزاری کنفرانس در هر سال است. به تجربهٔ کشورهای پیشرفته در مورد کنفرانسهایی از این قبیل توجه کنیم: برزیل هر دو سال یک‌بار و ایتالیا هر چهار سال یک‌بار کنفرانس عمومی مشابه دارند. با برگزاری سمینارهای تخصصی در کشور، محتوای علمی کنفرانسهای ریاضی نیز کاهش یافته است. بنابراین به نظر می‌رسد اگر کنفرانسهای ریاضی هر دو سال یک‌بار برگزار شوند مناسبتر است. در مقابل، شایسته است به سمینارهای تخصصی توجه بیشتری شود، مدت این سمینارها طولانیتر شود و برنامه‌های علمی آنها غنیتر گردند. دعوت از متخصصان خارجی برای این سمینارها هم معنی‌دارتر است. با برگزاری کنفرانسها در هر دو سال، مسألهٔ زمان برگزاری آن در تابستان یا عید نوروز نیز قابل حل است. دانشگاه میزبان به فراخور امکانات خود می‌تواند یکی از این دو زمان را انتخاب کند.

نکتهٔ سوم، طیف شرکت‌کنندگان در کنفرانس است. با برگزاری کنفرانسهای آموزش ریاضی محل مناسبی برای شرکت دبیران ریاضی کشور فراهم آمده است و در نتیجه این امکان پیدا شده که دانشجویان بیشتری بتوانند در کنفرانس ریاضی کشور شرکت کنند. به‌نظر می‌رسد این روال را باید تقویت کرد و در مورد نظم ثبت‌نام، مراعات «آخرین مهلت‌ها» و تعهدات شرکت‌کنندگانْ جدیتر عمل کرد.

آنچه مسلم است، امکانات بالفعل دانشگاه تهران برای برگزاری چنین کنفرانسهایی به هیچ‌وجه با جایگاه آن تناسب ندارد. برگزارکنندگان کنفرانس خیلی تلاش کردند رضایت شرکت‌کنندگان را حتی‌المقدور جلب کنند ولی مسلماً کمبودهای زیادی وجود داشت. به هر حال اگر دانشگاهِ مادر بضاعت برگزاری پرشکوه‌تر کنفرانس را نداشت، آغوشی پرمهر برای پذیرایی فرزندانش فراهم کرده بود.

رحیم زارع‌نهندی
دبیر کنفرانس

نشر ریاضی، سال ۱۱، شمارهٔ ۲، صص ۶ـ۱۰

تابع زتا و ماتریسهای تصادفی

مهرداد شهشهانی*

شاید نخستین شاهدی که برای نقش تابع زتا

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}, \qquad s = \sigma + it,\ \sigma > 1$$

در درک توزیع اعداد اول وجود دارد، اثبات اویلر از واگرایی سری

$$\sum_{p,\ \text{عدد اول}} \frac{1}{p}$$

است. قضیهٔ اویلر از دو جهت قابل توجه است. از یک سو این قضیه، قضیهٔ اقلیدس در مورد نامتناهی بودن مجموعهٔ اعداد اول را پربارتر می‌کند، و از سوی دیگر، و نکتهٔ مهمتر اینکه، روش اثبات ایده‌های جدیدی را مطرح می‌کند که منجر به نتایج بسیار عمیقی می‌شوند. رابطهٔ بیان تابع زتا و اعداد اول عمدتاً بر فرمول حاصلضربی زیر مبتنی است

$$\zeta(s) = \prod_{p,\ \text{عدد اول}} \frac{1}{1 - \frac{1}{p^s}}, \qquad \sigma > 1 \qquad (1)$$

برای اثبات قضیهٔ اویلر می‌توان به‌صورت زیر عمل کرد: از دو طرف رابطهٔ (۱) لگاریتم می‌گیریم و $\log(1 - \frac{1}{p^s})$ را برحسب توانهای p^s بسط می‌دهیم، یعنی

$$\log(1 - \frac{1}{p^s}) = -\sum_k \frac{1}{kp^{sk}}$$

اکنون سری مضاعف $\sum_p \log(1 - \frac{1}{p^s})$ را بدین صورت بازآرایی می‌کنیم که جملات مربوط به $k = 1$ و $k > 1$ را تفکیک می‌کنیم. جملات مربوط به $k > 1$ به‌ازای $s \geq 1$ همگرا می‌شوند و با استفاده از $\lim_{\sigma \to 1^+} \zeta(\sigma) = \infty$ (و کمی آنالیز مقدماتی) به اثبات قضیهٔ اویلر دست می‌یابیم.

پس از اویلر، لژاندر، گاوس، چبیشف و دیگران به بررسی توزیع اعداد اول پرداختند. به‌ازای هر عدد حقیقی مثبت x، $\pi(x)$ را تعداد اعداد اول کوچکتر یا مساوی x می‌گیریم. گاوس با استفاده از شواهد عددی گسترده‌ای، این حدس جسورانه را مطرح کرد که توزیع اعداد اول به‌طور مجانبی به‌صورت زیر است

$$\pi(x) \sim \int_2^x \frac{dt}{\log t} \overset{\text{تعریف}}{=} \mathrm{Li}(x)$$

(می‌گوییم f و g به‌طور مجانبی برابرند، و می‌نویسیم $f(x) \sim g(x)$، در صورتی‌که $\lim_{x \to \infty} \frac{f(x)}{g(x)} = 1$.) به نظر می‌آید که گاوس به هیچ‌گونه روش تحلیلی برای مرتبط ساختن $\mathrm{Li}(x)$ و $\pi(x)$ دست نیافته بوده است. یک نتیجهٔ حدس گاوس «قضیهٔ اعداد اول» است به این مضمون که

$$\pi(x) \sim \frac{x}{\log x}$$

گاوس می‌دانست که به‌ازای ثابتهای مناسب a و b نابرابریهای زیر برقرارند

$$a\frac{x}{\log x} \leq \pi(x) \leq b\frac{x}{\log x}$$

چبیشف نشان داد که این نابرابریها به‌ازای $a = 0.9212\cdots$ و $b = 1.0555\cdots$ برای xهای بزرگ صادق‌اند. استدلال چبیشف مبتنی بر فرمول مقدماتی

$$\log n! = \sum_{p^k \leq n} [\frac{n}{p^k}] \log p$$

است و تابع زتا در آن به کار گرفته نمی‌شود.

تحلیل ریمان از تابع زتا پایهٔ نظری ارتباط میان $\pi(x)$ و $\mathrm{Li}(x)$ را فراهم آورد. او نخست ثابت کرد که می‌توان $\zeta(s)$ را به تابعی برخه ریخت (مرومُرف)

بر $\mathbb{C}$ توسعه داد که فقط یک قطب ساده با ماندهٔ ۱ در نقطهٔ ۱ دارد و در معادلهٔ تابعی زیر صدق می‌کند.

$$\zeta(s) = 2^s \pi^{s-1} (\sin \frac{\pi s}{2}) \Gamma(1-s) \zeta(1-s)$$

در اینجا $\Gamma(s) = \int_0^\infty x^{s-1} e^{-x} dx$ تابع گاماست. برای مرتبط ساختن $\zeta(s)$ و $\pi(x)$، ریمان به معرفی تابع Jای به شرح زیر پرداخت. J تابعی پله‌ای و غیرنزولی است که روی $\mathbb{R}^+$ تعریف شده است، $J(x) = 0$ به‌ازای $x < 2$ و هرگاه که x از p^k، p عدد اول، می‌گذرد، مقدار J به‌اندازه $1/k$ افزایش می‌یابد. مثلاً $J(x) = 1$ به‌ازای $2 \le x < 3$، $J(x) = 5/2$ به‌ازای $4 \le x < 5$ و غیره. در این‌صورت $J(x)$ نمایش ساده‌ای برحسب $\pi(x)$ دارد:

$$J(x) = \pi(x) + \frac{1}{2}\pi(x^{\frac{1}{2}}) + \frac{1}{3}\pi(x^{\frac{1}{3}}) + \cdots \qquad (2)$$

توجه کنید که به‌ازای هر x، مجموع بالا در واقع یک مجموع متناهی است.

رابطهٔ میان J و ζ را دست‌کم به‌طور صوری می‌توان به سادگی توصیف کرد. با لگاریتم‌گیری از نمایش حاصلضربی اویلر از $\zeta(s)$، رابطهٔ زیر به‌دست می‌آید

$$\log \zeta(s) = \sum_{n,p} \frac{1}{n} p^{-s} \qquad (\text{وقتی } \sigma > 1) \qquad (3)$$

بنابراین به‌ازای $\sigma > 1$ داریم

$$\log \zeta(s) = \int_0^\infty x^{-s} dJ(x)$$

که در اینجا dJ باید به مفهوم توزیع تعبیر شود (یا انتگرال بالا را یک انتگرال ریمان‌ـاستیلتیس تصور کنید). بنابراین انتگرال بالا را با استفاده از انتگرال‌گیری جزء به جزء می‌توان به شکل زیر نوشت:

$$\frac{\log \zeta(s)}{s} = \int_0^\infty J(x) x^{-s} \frac{dx}{x} \qquad (4)$$

برای درک این انتگرال، توجه کنید که جایگزینی $x = e^y$ و در نتیجه $\frac{dx}{x} = dy$، انتگرال را به‌صورت

$$\int_{-\infty}^{+\infty} J(e^y) e^{-i\sigma y + yt} dy$$

در می‌آورد که همان تبدیل فوریه است. بدین ترتیب نمایش انتگرالی ذکر شده درواقع ترجمهٔ تبدیل فوریه ازگروه جمعی $(\mathbb{R}, +)$ به‌گروه ضربی $(\mathbb{R}^+, \cdot)$ است که معمولاً به تبدیل ملین[1] معروف است. به‌عبارت دیگر، (۴) مبین این امر است که تبدیل ملین $J(x)$ برابر $\frac{\log \zeta(s)}{s}$ است. چون هدف ما این است که $\pi(x)$ (یا $J(x)$) را به صریحترین شکل ممکن به $\mathrm{Li}(x)$ ربط دهیم، باید معکوس تبدیل ملین را به کار گیریم تا نمایشی انتگرالی برای $J(x)$ به‌دست آوریم. با ترجمهٔ فرمول معکوس انتگرال فوریه به تبدیل ملین، رابطهٔ زیر به‌دست می‌آید

$$J(x) = \frac{1}{2\pi i} \int_{a-i\infty}^{a+i\infty} \log \zeta(s) x^{s-1} ds \qquad (5)$$

1. Mellin transform

که در اینجا $a > 1$ و انتگرالگیری روی خط قائم با مقدار حقیقی a است. این نمایش انتگرالی ظاهراً فقط صوری است ولی در واقع با انتگرالگیری جزء به‌جزء به مفهوم توزیعها کاملاً معنی دارد. ریمان با استدلالی فوق‌العاده مبتکرانه نشان داد که $J(x)$، $x > 1$، برابر است با:

$$\mathrm{Li}(x) + \int_0^2 \frac{dt}{\log t} - \log 2 - \sum_{\mathrm{Im}\rho > 0} (\mathrm{Li}(x^\rho) + \mathrm{Li}(x^{1-\rho})) + \int_x^\infty \frac{dt}{t(t^2-1)\log t} \qquad (6)$$

که در اینجا ρ در مجموعهٔ صفرهای تابع زتا در نوار $0 < \sigma < 1$ مقدار می‌گیرد و انتگرال $\int_0^2 \frac{dt}{\log t}$ به مفهوم مقدار اصلی کوشی است. استخراج $\pi(x)$ از $J(x)$ کاری ساده است. در واقع استدلالی مقدماتی نشان می‌دهد که

$$\pi(x) = \sum_{n=2}^{\infty} \frac{\mu(n)}{n} J(x^{\frac{1}{n}}) = J(x) - \frac{1}{2} J(x^{\frac{1}{2}}) - \cdots + \frac{1}{6} J(x^{\frac{1}{3}}) - \cdots \qquad (7)$$

که در اینجا مقدار $\mu(n)$ (تابع موبیوس) صفر است اگر n یک مقسوم‌علیه مجذور داشته باشد و برابر $(-1)^k$ است در صورتی که n برابر حاصلضرب k عدد اول متمایز باشد، و $\mu(1) = 1$. بدین ترتیب فرمول ریمان برای $J(x)$ مبنایی برای مرتبط ساختن $\pi(x)$ به خواص تحلیلی ایجاد می‌کند، یا به‌طور دقیقتر، به صفرهای تابع زتا. امید این بوده است که سرشت نوسانی جملات

$$\sum_{\mathrm{Im}\rho > 0} (\mathrm{Li}(x^\rho) + \mathrm{Li}(x^{1-\rho}))$$

منجر به حذف جملات متعددی شود و نقش اصلی در مقدار $J(x)$ را $\mathrm{Li}(x)$ به عهده داشته باشد. وفور صفرهای $\zeta(s)$ در ناحیهٔ $0 \le \sigma \le 1$ اساساً از قضایای نظریهٔ توابع تام[1] دارای مرتبهٔ متناهی[2] که در آن قضایا آهنگ رشد تابع تام به نمای همگرایی صفرهایش ربط داده می‌شود، نتیجه می‌گردد. قضیهٔ فاکتورگیری آدامار[3] که توابع تام دارای مرتبهٔ متناهی را به‌صورت یک حاصلضرب نامتناهی نمایش می‌دهد، حربهٔ عمده در مرتبط ساختن صفرهای تابع به مرتبهٔ رشد آن است. این قضیه همچنین بسط حاصلضربی دیگری برای تابع زتا ارائه می‌کند که منجر به فرمولهای صریحی در نظریهٔ اعداد می‌شوند.

به جای بهره‌گیری مستقیم از نمایش انتگرالی $J(x)$، می‌توان نشان داد که صفرنشدن $\zeta(s)$ در نیمصفحهٔ بستهٔ $\sigma \ge 1$ نتیجه می‌دهد که $\pi(x)$ به‌طور مجانبی برابر $\frac{x}{\log x}$ است. این در واقع روشی است که آدامار و دُ لا واله پوسن مستقل از یکدیگر برای اثبات قضیهٔ اعداد اول به‌کار گرفتند. معلوم شده است که میزان خطا در نمایش مجانبی $\pi(x) \sim \frac{x}{\log x}$ در حد، $O(\frac{x}{(\log x)^2})$ است. می‌توان با تجزیه و تحلیل ناحیه‌های خالی از صفر تابع $\zeta(s)$ تخمینهای دقیقتری از خطا به‌دست آورد. به ادعای فرضیهٔ ریمان (RH)، همهٔ صفرهای $\zeta(s)$ که در $\sigma \ge 0$ قرار دارند روی خط $\sigma = \frac{1}{2}$ واقع می‌شوند. صحت این فرضیه خطا را به $O(\sqrt{x}\log x)$ تقلیل می‌دهد و به‌عکس. باید در اینجا

1. entire functions 2. finite order

3. Hadamard factorization theorem

خاطرنشان کرد که طبق شواهد عددی گسترده، تابع $\mathrm{Li}(x)$ تقریب بهتری از $\frac{x}{\log x}$ برای $\pi(x)$ است.

پس از اثبات قضیهٔ اعداد اول در سال ۱۸۹۶، پیشرفتهای گسترده‌ای در نظریهٔ توابع تام یک متغیر مختلط صورت گرفت. با عنایت به رابطهٔ میان مرتبهٔ رشد این توابع و توزیع صفرهای آنها، به نظر می‌رسید که تحلیل عمیقتری از توابع تام ممکن است منجر به اثبات فرضیهٔ ریمان شود. در واقع در سال ۱۹۰۰ هیلبرت ابراز خوشبینی کرد که طی چند دههٔ بعد اثباتی از RH پیدا شود. تاریخ خلاف این را نشان داده است و باورعمومی این است که نظریهٔ توابع نمی‌تواند به تنهایی اثبات RH را فراهم آورد.

معروفترین حدس در مورد ارتباط میان رشد یک تابع تام یا برخه‌ریخت و فرضیهٔ ریمان، فرضیهٔ لیندلاف[1] است. برای تابع برخه‌ریخت ϕ تعریف می‌کنیم:

$$\mu_\phi(\sigma) = \inf\{a \in \mathbb{R} | \phi(\sigma + it) = O(|t|^\alpha)\} \text{ ،} t \to \infty \text{ وقتی}\}$$

فرضیهٔ لیندلاف این است که

$$\mu_\zeta(\tfrac{1}{2}) = 0$$

برای توصیف رابطهٔ بین رشد ζ و صفرهای آن، تعداد صفرهای $\zeta(\sigma + it)$ در ناحیهٔ $\{\sigma > \rho, 0 \le t \le T\}$ را به $N(\rho, T)$ نمایش می‌دهیم. قضیهٔ معروفی در مورد تابع زتای ریمان حکم می‌کند که فرض لیندلاف معادل است با اینکه وقتی $T \to \infty$، به‌ازای $\rho > \frac{1}{2}$

$$N(\rho, T+1) - N(\rho, T) = o(\log T)$$

از این مطلب روشن است که صحت RH، صحت فرضیهٔ لیندلف را تضمین می‌کند، اما عکس موضوع صحیح نیست. تابع $N(\rho, T)$ مورد مطالعهٔ فراوان قرار گرفته است و می‌دانیم که

$$N(0, T) = \frac{T}{2\pi} \log \frac{T}{2\pi} - \frac{T}{2\pi} + O(\log T)$$

بدین ترتیب، آهنگ افزایش تعداد صفرهای $\zeta(s)$ در ناحیهٔ $T \le t \le T+1$ مانند $\log T$ است وقتی $T \to \infty$.

وفور صفرهای $\zeta(s)$ در نوار بحرانی $0 < \sigma < 1$ این نگرش را القاء می‌کند که تفاضل میان مقادیر موهومی متوالی صفرهای تابع زتا ممکن است ساختار جالب توجهی داشته باشد. به فرض صحت RH، صفرهای ζ در نیمصفحهٔ بالا به صورت $\frac{1}{2} + i\tau_j$ هستند که در آن $\tau_j < \tau_{j+1}$. در این‌صورت حدس زده می‌شود که توزیع زوجهای صفرهای تابع زتا به صورت

$$\frac{\#\{(\tau, \tau') | 0 < \tau < \tau' < T, \tau' - \tau \in [\frac{2\pi\alpha}{\log T}, \frac{2\pi\beta}{\log T}]\}}{\frac{T \log T}{2\pi}} \sim \int_\alpha^\beta \left(1 - (\frac{\sin \pi t}{\pi t})^2\right) dt$$

باشد که در آن $0 < \alpha < \beta$. این تخمین که به حدس همبستگی زوجی[2] برای صفرهای تابع زتا معروف است، توسط هیو مونتگمری با فرض صحت RH به دست آمد (به [M] و [RS] نگاه کنید). تحلیل عددی گسترده توسط اُدلیزکو صحت این حدس را تأیید می‌کند. حدس همبستگی زوجی است که به رابطهٔ میان صفرهای تابع زتا و توزیع ویژه‌مقدارهای ماتریسهای ارمیتی اشاره دارد، موضوعی که اکنون به آن خواهیم پرداخت.

طبق قضیه‌ای استاندارد در آنالیز برای هر گروه توپولوژیک موضعاً فشردهٔ G، اندازهٔ مثبت منحصر به فردی چون $d\mu$ (با تقریب ضرب در عدد ثابت) موسوم به اندازهٔ هار[1] وجود دارد که نسبت به ضرب در طرف چپ ناورداست، یعنی برای هر تابع پیوستهٔ ϕ و هر $x \in G$، داریم $\int_G \phi(xy) d\mu(y) = \int_G \phi(y) d\mu(y)$. اگر به علاوه گروه فشرده (یا آبلی) باشد، آنگاه $d\mu$ لزوماً نسبت به ضرب چپ و راست و نیز معکوس‌گیری در G ناورداست، یعنی

$$\int_G \phi(xy) d\mu(y) = \int_G \phi(yx) d\mu(y) = \int_G \phi(y^{-1}) d\mu(y)$$

اندازهٔ لبگ روی گروه جمعی $\mathbb{R}$ و $\frac{dt}{t}$ روی گروه ضربی $\mathbb{R}^+$ ساده‌ترین مثالهای اندازهٔ هار هستند. $d\mu$ را اندازهٔ هار بهنجارشده [نرمالشده] روی گروه یکانی[2] $U(n)$ بگیرید، پس $\mathrm{vol}(U(n)) = 1$. یک توصیف صریح برای اندازهٔ هار روی $U(n)$ با در نظر گرفتن حاصلضرب گوه‌ای[3] درایه‌های ماتریس $A^{-1}dA$ به‌دست می‌آید که در اینجا A می‌تواند هر پرمایش[4] گروه یکانی باشد و d نسبت به پرمایش اتخاذ شده محاسبه می‌شود. راه دیگری برای توصیف اندازهٔ هار روی $U(n)$، که با کامپیوتر به‌خوبی تقریب زده می‌شود، استفاده از متغیرهای تصادفی نرمال است. فرض کنید X و Y دو متغیر تصادفی مستقل نرمال با میانگین صفر و واریانس $\frac{1}{2}$ باشند. در این‌صورت $X + iY$ را یک متغیر تصادفی نرمال مختلط استاندارد می‌نامیم. حال فرض کنید n^2 متغیر تصادفی γ_{jk} داده شده‌اند که مستقل، مختلط و نرمال استاندارد هستند. با تشکیل ماتریس $[\gamma_{jk}]$ و استفاده از فرایند گرام‌ـاشمیت بر ستونهای ماتریس، یک ماتریس یکانی به دست می‌آوریم. حال یک تقریب برای اندازهٔ هار روی $U(n)$ به روش مونت‌کارلو به دست می‌آید. به بیان دیگر هر گاه زیرمجموعه‌ای چون W از $U(n)$ داده شده باشد، با انتخاب تصادفی نقاط $U(n)$ به روش فوق و محاسبهٔ نسبت انتخابهایی که در W قرار می‌گیرند، اندازهٔ هار W به‌دست می‌آید. از آنجا که شبیه‌سازی متغیر تصادفی نرمال و پیاده‌سازی روش گرام‌ـاشمیت هر دو به‌وسیلهٔ کامپیوتر عملی هستند، با این روش می‌توان اندازهٔ هار روی $U(n)$ را در عمل مورد استفاده قرار داد. بدین ترتیب می‌توان ماتریسهای یکانی تصادفی را به‌وسیلهٔ کامپیوتر ایجاد کرد. ویژه‌مقدارهای یک ماتریس یکانی A به شکل $\{e^{i\theta_j}\}$ هستند که در آن $0 \le \theta_1 \le \theta_2 \le \ldots \le \theta_n < 2\pi$. توزیع ویژه‌مقدارهای یک ماتریس یکانی تصادفی روی دایرهٔ واحد یکنواخت نیست بلکه به‌وسیلهٔ تابع چگالی

$$f(\theta_1, \cdots, \theta_n) = \frac{1}{2^n \pi^n n!} \prod_{j<k} |e^{i\theta_j} - e^{i\theta_k}|^2 \qquad (8)$$

1. Lindelöf 2. pair correlation conjecture

1. Haar measure 2. unitary 3. wedge product 4. parametrization

داده می‌شود. از این عبارت پیداست که ویژه‌مقدارهای ماتریس یکانی تصادفی تمایل به دفع یکدیگر دارند و نمایش تصویری آنها روی دایرهٔ واحد نشان می‌دهد که به صورتی «همفاصله‌تر» از اعداد مختلط با طول واحد که طبق توزیع یکنواخت انتخاب شده‌اند، قرار می‌گیرند. اکنون تابع همبستگی زوجی را برای ویژه‌مقدارهای یک ماتریس یکانی به صورت زیر تعریف می‌کنیم

$$r_2(A)(a,b) = \frac{\#\left\{j \neq k | n(\theta_j - \theta_k) \in [2\pi a, 2\pi b]\right\}}{n}$$

هرگاه $a < b$ اعداد حقیقی باشند. امید ریاضی

$$r_2(a,b) = \int_{U(n)} r_2(A)(a,b)d\mu(A)$$

وجود دارد و یک اندازه است که به هر بازهٔ $[a,b]$ عدد حقیقی مثبت $r_2(a,b)$ را نسبت می‌دهد. از ملاحظات کلی احتمالی (قانون اعداد بزرگ) می‌توان نتیجه گرفت که $r_2(A)(a,b)$ به $r_2(a,b)$ میل می‌کند وقتی $n \to \infty$. به علاوه، اندازهٔ $r_2(a,b)$ را می‌توان به‌صورت زیر نمایش داد

$$r_2(a,b) = \int_a^b \left(1 - \left(\frac{\sin \pi x}{\pi x}\right)^2\right) dx \qquad (9)$$

که شباهت قابل توجهی به توزیع زوجهای صفرهای تابع زتا دارد که قبلاً بحث آن رفت. محاسبات عددی گستردهٔ صفرهای $\zeta(s)$ و ویژه‌مقدارهای ماتریسهای یکانی تصادفی نشان می‌دهند که بافت‌نگارهای تفاضلهای صفرهای متوالی $\zeta(s)$ و $\theta_j - \theta_{j-1}$، پس از بهنجارسازی مناسب، روی خمهای تقریباً یکسان قرار می‌گیرند ([O] را ببینید). طبعاً می‌توان ماتریسهای متعامد یا گروههای همتافته[1] (فشرده) را نیز در نظر گرفت و توزیع ویژه‌مقدارهای آنها را نیز مورد مطالعه قرار داد. در این حالت، نتایجی مشابه ولی متفاوت برقرارند. مسألهٔ ذی‌ربط توزیع $\mathrm{Tr}(A^k)$، وقتی A یک ماتریس تصادفی از یک گروه کلاسیک فشرده باشد در [DS] حل شده است.

برای مقایسهٔ صفرهای تابع زتا و ویژه‌مقدارهای ماتریسهای یکانی تصادفی، کُرام[2] و دیاکونیس[3] این فرض آماری را که داده‌های تشکیل شده از صفرهای تابع زتا از چگالی (۸) ناشی شده‌اند مورد آزمون قرار دادند [CD]. به‌طور دقیقتر به یاد آورید که فاصلهٔ میان صفرهای متوالی $\zeta(s)$، $s = \sigma + it$، حدوداً برابر $2\pi/(\log t - \log 2\pi e)$ است و ویژه‌مقدارهای ماتریسهای یکانی تصادفی فاصلهٔ تقریبی $\frac{2\pi}{n}$ را از هم دارند. برای مقایسهٔ فاصلهٔ میان ۵۰۰۰۰ صفر ζ که از حدود 10^{20} امین صفر شروع شوند و فاصلهٔ بین ویژه‌مقدارهای ماتریسهای $n \times n$ یکانی، معقول است که فرض کنیم $n \sim \log \frac{t}{2\pi e}$. با محاسبه‌ای ساده معلوم می‌شود انتخاب $n = 42$ انتخاب خوبی است. در اینجا تفاضلهای $\delta_j = \tau_j - \tau_{j-1}$ بین ۵۰۰۰۰ صفر متوالی با شروع از حدود 10^{20} امین صفر محاسبه می‌شوند. از اینجا $\frac{50000}{42} \sim 1190$ بلوک از ۴۲ تفاضل متوالی به‌دست می‌آید. برای هر بلوک قرار می‌دهیم $\Delta_j = \sum_{k=1}^{j} \delta_k$ و

$$X_j = \exp\left[(2\pi i)\left(\frac{\Delta_j}{\Delta_{42}} + U\right)\right] \qquad (10)$$

1. symplectic groups 2. Coram 3. Diaconis

که در اینجا U توزیع یکنواخت روی $[0,1)$ است. به اصطلاح معمول آماری، «فرض صفر» این است که X_jها از مشاهدهٔ متغیری تصادفی با چگالی (۸) به‌دست آمده‌اند. با به‌کارگیری آزمونهای آماری بهینه، نشان داده می‌شود که فرض صفر در سطح ۱٪ رد نمی‌شود ولی در سطح ۵٪ مردود است. قابل توجه است که اگر به جای گروه یکانی، گروه متعامد یا گروههای همتافته (فشرده) را به‌کار گیریم، فرض صفر برخلاف پیش‌بینی [KS] حتی در سطح ۱٪ رد می‌شود.

رفتار صفرهای تابع زتا از جهات دیگری هم به ویژه‌مقدارهای ماتریسهای یکانی تصادفی شباهت دارد. کِلی ویاند[1] نشان داد که ساختار همبستگی به نسبت شگفت‌آوری بین تعداد ویژه‌مقدارهای ماتریسهای یکانی تصادفی در بازه‌های $(e^{2\pi i\alpha}, e^{2\pi i\beta})$ و $(e^{2\pi i\gamma}, e^{2\pi i\delta})$ وجود دارد [DE]. در واقع، وی نشان داد که:

۱. برای بازه‌های مجزا، همبستگی صفر است؛
۲. به‌ازای $\alpha < \gamma < \beta < \delta$ همبستگی صفر است؛
۳. به‌ازای $\alpha < \beta = \gamma < \delta$، ضریب همبستگی $-\frac{1}{2}$ است؛
۴. به‌ازای $\alpha = \gamma < \delta < \beta$، ضریب همبستگی $\frac{1}{2}$ است.

همچنان که قبلاً شرح داده شد، می‌توان بلوکهای اعداد مختلط با قدر مطلق ۱ را مطابق (۱۰) ساخت. در اینجا $\alpha < \beta$ را تثبیت می‌کنیم و یک پنجرهٔ متحرک $(e^{2\pi i\gamma}, e^{2\pi i\delta})$ در نظر می‌گیریم که در آن $\gamma = \alpha + \tau$ و $\delta = \beta + \tau$ و τ متغیر است. با در نظر گرفتن تابع همبستگی به‌عنوان تابعی از τ، تابعهای همبستگی تقریباً یکسان برای ماتریسهای یکانی تصادفی و صفرهای تابع زتا به‌دست می‌آیند.

یکی از انگیزه‌های بررسی توزیع ویژه‌مقدارهای ماتریسهای یکانی، مسائل فیزیک هسته‌ای بوده است. فضای برداری χ متشکل از ماتریسهای ارمیتی $n \times n$ با تابع چگالی احتمال $Ce^{-\mathrm{Tr}(A^*A)}$ (با انتخاب Cی مناسب) معمولاً «مجموعهٔ یکانی معظم»[2] (GUE) نامیده می‌شود. همین‌طور مجموعه‌های معظم متعامد[3] (GOE) و همتافته[4] (GSE) در نظر گرفته می‌شوند. ویگنر[5] بود که این نظر را مطرح کرد که طیف انرژی هسته‌های پیچیده را می‌توان برحسب ویژه‌مقدارهای ماتریسهای تصادفی متعلق به GUE، GOE و GSE مدلسازی کرد. قانون معروف نیمدایرهٔ ویگنر را می‌توان در چارچوب GOE استخراج کرد. از دههٔ ۱۹۵۰ توزیع ویژه‌مقدارهای ماتریسهای تصادفی موضوع کاوشهای گسترده‌ای بوده است. دایسن[6] نشان داد که توزیع ویژه‌مقدارها، یا به‌طور دقیقتر همبستگیهای ویژه‌مقدارهای ماتریسهای تصادفی از گروههای یکانی، متعامد، و همتافته (فشرده) همان خواص آماری GUE، GOE و GSE را دارا هستند. از بعضی جهات راحت‌تر است که گروههای کلاسیک فشرده را در نظر بگیریم تا مستقیماً GUE، GOE و GSE را. به نظر می‌رسد که فرمول مونتگمری (مبتنی بر RH) در مورد تابع همبستگی زوجی را دایسن مستقلاً حدس زده باشد بر این اساس که وی آن را مشابه تابع همبستگی زوجی ویژه‌مقدارهای تصادفی می‌پنداشت. این تقارن (اگر واقعیت داشته باشد) نقطهٔ شروع تحقیقات فراوانی در این مبحث بوده است. برای ملاحظهٔ

1. K. Wieand 2. Grand Unitary Ensemble 3. Grand Orthogonal Ensemble 4. Grand Symplectic Ensemble 5. Wigner 6. Dyson

شرحی در مورد مسائل فیزیکی که منجر به ماتریسهای تصادفی می‌شوند به [Me] و [BK] و مراجع مندرج در آنها مراجعه کنید.

میان رفتار ویژه‌مقدارهای ماتریسهای یکانی تصادفی و صفرهای تابع زتا تفاوتهای مفهومی قابل ملاحظه‌ای نیز وجود دارد. برای کمّی ساختن این تفاوت، مفهوم «واریانس عددی» برای دنباله‌ای از کمیتهای تصادفی با رشد خطی را مطرح می‌کنیم. به‌طور دقیق، فرض کنید $N(x)$ نمایش‌دهندهٔ کمیتهای تصادفی حقیقی باشد، $x \in \mathbb{Z}^+$، با این خاصیت که $N(x+y) \sim N(x)+N(y)$ و $N(x+y)-N(x)-N(y)$ دارای میانگین صفر باشد. در این صورت برای مقادیر (بزرگ) ثابت x و متغیر t، واریانس عددی عبارت است از کمیت

$$\frac{1}{l}\sum_{t=1}^{l}\mathrm{Var}[N(x+t)-N(x)-N(t)]$$

برای به‌کارگیری واریانس عددی در مورد ویژه‌مقدارهای ماتریسهای یکانی تصادفی و صفرهای تابع زتا بهنجارسازی مناسبی مورد نیاز است که شرط $x, t \in \mathbb{Z}^+$ را تأمین کند. می‌توان نشان داد که برای ویژه‌مقدارهای ماتریسهای یکانی تصادفی، واریانس عددی تابعی یکنوای صعودی نسبت به l است. ولی برای صفرهای تابع زتا، واریانس عددی دیگر تابعی صعودی نیست و نوسانات زیادی به‌ازای صفرهای بزرگ (بزرگتر از 10^{20}امین صفر) دارد. تفاوت دو کمیت را می‌توان به صورت کمی به شکل مجموعهایی برحسب اعداد اول و مقادیر تابع زتا بیان کرد. برای ملاحظهٔ بحثی پیرامون این مسأله به [BK] نگاه کنید. احتمالاً شباهت بین توابع همبستگی ویژه‌مقدارهای ماتریسهای یکانی تصادفی و صفرهای تابع زتا در نواحی نوسان یا نزول واریانس عددی صفرها رو به نقصان می‌رود.

مفهوم مشابه تابع زتا برای واریته‌ها [چندگوناها] روی میدانها [هیأتها]ی متناهی، یعنی تابع زتای ویل اساساً تابع مولد تعداد نقاط گویای واریته است وقتی که میدان زیربنایی تعریف، توسعه می‌یابد. تابع زتای ویل بسیار بهتر از تابع زتای ریمان درک شده است. نتایجی در مورد رابطهٔ فاصلهٔ بین صفرهای تابع زتای ویل و ماتریسهای یکانی تصادفی وجود دارد که در [KS] و مراجع آن به آن پرداخته شده است. موفقیتی که در درک تابع زتای ویل به‌دست آمده است مرهون پیشرفت نظریهٔ کوهومولوژی مناسب (نظریهٔ l-ایک[1]) برای واریته‌ها روی میدانهای متناهی است که در آن قضایای مشابه «دوگانی پوانکاره»، قضیهٔ نقطهٔ ثابت لفشتس، و قضیهٔ سخت لفشتس[2] معتبرند. در این وضعیت نقاط گویای واریتهٔ تعریف شده روی میدان متناهی $\mathbb{F}_q$، نقاط ثابت خودریختی فروبنیوس $x \to x^q$ هستند. محاسبهٔ تابع مولد برای تعداد نقاط ثابت در اینجا به‌وسیلهٔ قضیهٔ نقطهٔ ثابت لفشتس خطی‌سازی می‌شود. اثرها[3]ی عملگرهای خطی که توسط خودریختی فروبنیوس روی گروههای کوهومولوژی l-ایک القاء می‌شوند تابع زتای ویل را پدید می‌آورند. این امر، به مفهوم کلی، همراستا با دیدگاه (منسوب به هیلبرت و پولیا) است که درک عمیقتر تابع زتای ریمان ممکن است از طریق مرتبط ساختن آن به عملگر یکانی یا ارمیتی مناسب روی یک فضای هیلبرت حاصل شود. برای ملاحظهٔ نظریه‌پردازیهایی در این وادی به فصل ۵ مرجع [P] نگاه کنید.

1. l-adic 2. Hard Lefschetz theorem 3. traces

مراجع

[BK] Berry, M. V. and J. P. Keating, "The Riemann zeros and eigenvalue asymptotics", *SIAM Review*, (2) **41**, 236-266.

[CD] Coram, M. and P. Diaconis, "New tests of the correspondence between unitary eigenvalues and zeros of Riemann's zeta function", *Preprint*, Department of Statistics, Stanford University (2000).

[DE] Diaconis, P. and S. Evans, "Linear functionals of eigenvalues of random matrices", *Preprint*, Department of Statistics, Stanford University (2000).

[DS] Diaconis, P. and M. Shahshahani, "On the eigenvalues of random matrices", *Jour. Appl. Prob.*, Special Volume **31 A**, 696-730.

[E] Edwards, H. M., *Riemann's Zeta Function*, Academic Press (1974).

[KS] Katz, N. and P. Sarnak, "Zeros of zeta functions and symmetry", *Bull. AMS*, (1) **36** (1999) 1-26.

[M] Montgomery, H., "The pair correlation of zeros of zeta function", *Proc. Symp. Pure Math.*, **24** (1973) 171-183.

[Me] Mehta, M., *Random Matrices*, Academic Press (1967).

[O] Odlyzko, A., "The 10^{20}-th zero of Riemann zeta function and 70 million of its neighbors", *Preprint*, ATT (1989).

[P] Patterson, S. J., *An Introduction to the Theory of the Riemann Zeta Function*, Cambridge University Press (1988).

[RS] Rudnick, Z. and P. Sarnak, "Zeros of principal L-functions and random matrix theory", *Duke Math. Jour.*, **81** (1996) 269-322.

[T] Titchmarsh, E. C., *The Theory of Riemann Zeta Function*, Oxford University Press (1986).

* * * * * *

* مهرداد شهشهانی، پژوهشگاه دانشهای بنیادی

mehrdads@karun.ipm.ac.ir

شبه‌تصادفی بودن•

اودت گُلدرایش*

ترجمهٔ محمدقاسم وحیدی

این مقاله به شیئهایی متناهی می‌پردازد که به‌وسیلهٔ دنباله‌های دودویی متناهی به نام رشته کدگذاری می‌شوند. وقتی از توزیعها سخن به میان می‌آوریم، منظورِ ما توزیعهای احتمال گسسته‌اند با تکیه‌گاهی متناهی که مجموعه‌ای از رشته‌هاست. توجهِ خاصی به توزیع یکنواخت داریم که به ازای پارامترِ طولی مانند n (که در طول بحث به‌صراحت یا به‌طور ضمنی مطرح می‌شود)، به هر رشتهٔ nبیتی مانند $x \in \{0,1\}^n$ احتمالی برابر (یعنی، احتمال 2^{-n}) را تخصیص می‌دهد. وقتی به‌صورت محاوره‌ای صحبت از «رشته‌های کاملاً تصادفی» می‌کنیم، منظورِ ما رشته‌هایی هستند که مطابق با چنین توزیع یکنواختی برگزیده شده‌اند.

نیمهٔ دوم این سده شاهد پیدایش و بسط سه نظریه دربارهٔ تصادفی بودن بوده است، مفهومی که اندیشمندان را در طول اعصار سردرگم کرده است. نخستین نظریه (رک. [۳]) که آغازگرِ آن شانُن[1] بود، ریشه در نظریهٔ احتمال دارد و توجه آن معطوف به توزیعهایی است که کاملاً تصادفی نیستند. نظریهٔ اطلاع شانُن تصادفی بودن کامل را به عنوان حالتی کرانگینی[2] مشخص می‌کند که در آن گنجایش اطلاع ماکسیمم می‌شود (و هیچ زیادی[3]ای در بین نیست)[4]. بنابراین، تصادفی بودن کامل وابسته به توزیعی یکتاست ــ همان توزیع یکنواخت. به‌ویژه، بنابر تعریف، نمی‌توان چنان رشته‌های تصادفی کامل را از رشته‌های تصادفی کوتاهتر تولید کرد.

1. Shannon 2. extreme 3. redundancy

۴. در حالت کلی، میزان اطلاع در توزیعی مانند D به صورت $-\sum_x D(x)\log_2 D(x)$ تعریف می‌شود. بنابراین، توزیع یکنواخت بر رشته‌هایی به طول n دارای اندازهٔ اطلاع n است، و هر توزیع دیگر روی رشته‌های nبیتی اندازهٔ اطلاع کمتری دارد. همچنین، برای تابعی مانند

$$f : \{0,1\}^n \to \{0,1\}^m$$

با $m > n$، توزیعِ حاصل از اعمالِ f بر رشته‌ای nبیتی با یک توزیع یکنواخت، اندازهٔ اطلاعی حداکثر n دارد که اکیداً کمتر از طول خروجی است.

نظریهٔ دوم (رک. [۱۱]، [۱۲])، منسوب به سولومونوف[1]، کولموگوروف، و شایتین[2]، ریشه در نظریهٔ محاسبه‌پذیری و به‌ویژه در مفهوم یک زبانِ جهانی (معادل با ماشین یا ابزار محاسبهٔ جهانی) دارد. در این نظریه، پیچیدگی شئ برحسب کوتاهترین برنامه (برای ماشینِ جهانیِ ثابتی) اندازه گرفته می‌شود که این شئ را تولید می‌کند[3]. مانند نظریهٔ شانُن، پیچیدگی کولموگوروفی، کمّی است، و شیئهای تصادفی کامل به عنوان حالتهای کرانگینی مطرح می‌شوند. جالب توجه اینکه در این رهیافت، می‌توان گفت که یک شئ واحد، و نه یک توزیع بر روی شیئها، کاملاً تصادفی است. با این حال، رهیافت کولموگوروف ذاتاً اجرا نشدنی است (یعنی پیچیدگی کولموگوروفی محاسبه‌ناپذیر است)، و، بنابر تعریف، نمی‌توان رشته‌هایی با پیچیدگی کولموگوروفی بیشتر را از روی رشته‌های تصادفی کوتاه تولید کرد.

نظریهٔ سوم، که آغازگران آن بلوم، گولدواسر، میکالی[4]، و یائو [۸، ۲، ۱۳] بودند، ریشه در نظریهٔ پیچیدگی دارد و کانون توجه این مقاله است. این رهیافت صراحتاً به دنبالِ تدارکِ نظریه‌ای در بارهٔ تصادفی بودن کامل است که در عین حال امکانِ تولیدِ کارآیِ رشته‌های کاملاً تصادفی از رشته‌های تصادفی کوتاهتر را فراهم آورد. لُبِّ این رهیافت، عبارت از این پیشنهاد است که شیئها را برابر تلقی کنیم در صورتی که نتوان آنها را با هیچ شیوهٔ کارآیی از هم تمیز داد. در نتیجه، توزیعی که نشود آن را به صورت کارآ از توزیع یکنواخت تمیز داد، تصادفی (یا بهتر است بگوییم «تصادفی برای کلیهٔ مقاصد عملی» که آن را «شبه‌تصادفی» می‌نامیم) تلقی می‌شود. بنابراین، تصادفی بودن، خاصیت «ذاتی» اشیا (یا توزیعها) نیست بلکه وابسته به

1. Solomonov 2. Chaitin

۳. مثلاً رشتهٔ 1^n دارای پیچیدگی کولموگوروفی $O(1) + \log_2 n$ است (بر مبنای برنامهٔ «n تا ۱ چاپ کن» که طولی نابیشتر از n (مثلاً، در دستگاه دودویی)) دارد. در مقابل، استدلال شمارشی ساده‌ای نشان می‌دهد که اغلب رشته‌های nبیتی دارای پیچیدگی کولموگوروفی حداقل n اند.

4. Micali

مشاهده‌گر (و قابلیتهای محاسباتی وی) است. برای توضیح این رهیافت، تجربهٔ ذهنی زیر را در نظر می‌گیریم.

> آلیس و باب به یکی از چهار روش زیر شیر یا خط بازی می‌کنند. در هر چهار روش، آلیس سکه‌ای را به هوا پرتاب می‌کند به‌طوری که تا ارتفاع زیادی بالا رود، و از باب خواسته می‌شود که برآمد آن را پیش از برخورد سکه با زمین حدس بزند. این روشها از لحاظ اطلاعی که باب پیش از حدس زدن در اختیار دارد، با هم متفاوت‌اند. در شق اول، باب باید حدس خود را پیش از پرتاب سکه اعلام کند. روشن است که در این حالت باب با احتمال ۱/۲ برنده می‌شود. در شق دوم، باب باید حدس خود را زمانی که سکه در هوا چرخ می‌خورد، اعلام کند. گرچه این برآمد در اساس با حرکت سکه تعیین می‌شود، باب اطلاع دقیقی در مورد حرکتِ آن ندارد و بنابراین معتقدیم که در این حالت نیز باب با احتمال ۱/۲ برنده می‌شود. شقِ سوم، مشابهِ دومی است، بجز اینکه باب ابزار پیچیده‌ای در اختیار دارد که قادر است اطلاع دقیقی در موردِ حرکتِ سکه و نیز شرایط محیط که بر برآمد تأثیر می‌گذارد، تهیه کند. با این حال، باب نمی‌تواند این اطلاع را به موقع پردازش کند که حدسِ خود را بهبود بخشد. در شق چهارم، دستگاه ثبات باب مستقیماً به کامپیوتر قدرتمندی وصل است که برای حل معادلاتِ حرکت برنامه‌ریزی شده و خروجی آن یک پیشگویی است. قابل درک است که در چنین حالتی باب می‌تواند حدس خود از برآمد را به میزان قابل ملاحظه‌ای بهبود بخشد.

نتیجه می‌گیریم که تصادفی بودنِ یک پیشامد به اطلاع و منابع محاسباتی که در اختیار داریم، بستگی دارد. بدین ترتیب، یک مفهوم طبیعیِ شبه‌تصادفی بودن، مطرح می‌شود: توزیع را شبه‌تصادفی گوییم هرگاه هیچ شیوهٔ کارآیی نتواند آن را از توزیع یکنواخت تمیز دهد که در آن شیوه‌های کارآ به الگوریتمهای زمانْ‌چندجمله‌ای (احتمالاتی) وابسته‌اند.

الگوریتمی را زمانْ‌چندجمله‌ای می‌نامند هرگاه یک چندجمله‌ای مانند p موجود باشد به‌طوری که برای هر ورودی x، الگوریتم در مدت زمانی با کران $p(|x|)$ اجرا شود که در آن $|x|$ طول رشتهٔ x را نشان می‌دهد. بنابراین، زمان اجرای چنان الگوریتمی میانه روانه به صورت تابعی از ورودی آن رشد می‌کند. الگوریتم احتمالاتی، الگوریتمی است که می‌تواند گامهایی تصادفی را اختیار کند که در آن، بی‌آنکه از کلیت کاسته شود، می‌توان گفت هرگام تصادفی عبارت است از اتخاذ تصمیم در بارهٔ اینکه کدام‌یک از دو گام از پیش تعیین شده باید در مرحلهٔ بعدی انتخاب شود به‌طوری که هرگام ممکن با احتمالِ ۱/۲ اختیار شود. این گزینه‌ها، «پرتابهای سکهٔ درونیِ» الگوریتم نامیده می‌شوند.

تعریف مولدهای شبه‌تصادفی

به بیانی نادقیق، هر مولد شبه‌تصادفی برنامه‌ای (یا الگوریتمی) کارآست که رشته‌های تصادفی کوتاه را کش می‌آورد و آنها را به دنباله‌های شبه‌تصادفی بلند تبدیل می‌کند. ما بر سه جنبهٔ بنیادین در مفهوم مولدِ شبه‌تصادفی تأکید می‌کنیم:

۱. **کارآیی.** مولد باید کارآ باشد. از آنجا که کارایی محاسبه را به زمانْ‌چندجمله‌ای بودن آن وابسته می‌دانیم، فرض می‌کنیم که این مولد به کمک یک الگوریتم زمانْ‌چندجمله‌ای تعیّنی قابل اجرا باشد.

این الگوریتم رشته‌ای به نام بذر را به عنوانِ ورودی دریافت می‌کند. این بذر، مقداری کراندار از تصادفی بودن را در اختیار خود می‌گیرد که به‌وسیلهٔ ابزاری که «دنباله‌های شبه‌تصادفی را تولید می‌کند» به کار گرفته می‌شود. این فرمولبندی، چنان ابزاری را شیوه‌ای تعیّنی تلقی می‌کند که بر بذری تصادفی اِعمال می‌شود.

۲. **کش‌آوری.** از مولد انتظار می‌رود که بذر ورودی را کش بیاورد و به دنبالهٔ خروجی طولانیتری تبدیل کند. به طور مشخص، مولدْ بذرهای به طول n بیت را به خروجیهای طولانیتر $l(n)$ بیتی کش می‌آورد که در آن $l(n) > n$. تابع l اندازهٔ کش‌آوری (یا تابع کش‌آوری) مولد نامیده می‌شود.

۳. **شبه‌تصادفی بودن.** خروجیِ مولد از دیدِ هر مشاهده‌گر کارآیی باید تصادفی به نظر آید. یعنی، هیچ شیوهٔ کارآیی نباید قادر به تمیز دادنِ خروجی یک مولد (روی بذری تصادفی) از یک دنبالهٔ واقعاً تصادفی با همان طول باشد. جملهٔ اخیر به مفهومی عام از «تمایزناپذیری [از نظر] محاسباتی» اشاره دارد که قلبِ کلِ این رهیافت است.

برای روشن شدن مطالب بالا، طرحِ زیر را برای یک موادِ شبه‌تصادفی در نظر بگیرید. بذر آن متشکل از جفتی از اعداد صحیح ۳۲بیتی مانند x و N است، و خروجی ۱۰۰۰۰۰بیتی آن با مجذورکردن مکرر عدد جاری x به پیمانهٔ N و بیرون آوردن بیتِ با کمترین معنی در هر نتیجه در مراحل بینابینی به دست می‌آید. (یعنی، فرض کنید (به پیمانهٔ N) $x_i \leftarrow x_{i-1}^2$، برای $i = 1, \cdots, 10^5$، و خروجیها b_1، b_2، $\cdots$، b_{10^5} هستند، که در آن $x_0 \overset{\text{تعریف}}{=} x$ و b_i بند با کمترین معنای x_i است). این فرایند را می‌توان به بذرهایی به طول n (در اینجا ما از $n = 64$ استفاده کرده‌ایم) و خروجیهایی به طول $l(n)$ (در اینجا $l(n) = 10^5$) تعمیم داد. چنان فرایندی مطمئناً فقره‌های (۱) و (۲)ی بالا را برآورده می‌کند، در حالی که این پرسش که آیا فقرهٔ (۳) برقرار است یا خیر، قابل بحث است (پس از آنکه تعریفی دقیق برای آن ارائه شد). با اشارهٔ پیشاپیش به بخشی از بحثهای آتی، متذکر می‌شویم که، تحت این فرض که تجزیهٔ اعداد صحیح بزرگ، دشوار است، صورت اندک تغییریافته‌ای از فرایند بالا درواقع یک مولد شبه‌تصادفی است.

تمایزناپذیری [از نظر] محاسباتی

از لحاظ شهودی، دو شئ از نظر محاسباتی تمایزناپذیرند هرگاه هیچ شیوهٔ کارآیی نتواند آنها را از هم تمیز دهد. مطابق آنچه در نظریهٔ پیچیدگی معمول است، صورتبندی ظریف این موضوع مستلزم تحلیلی مجانبی است (یا بهتر است بگوییم بررسی زمان اجرای الگوریتمها به عنوان تابعی از طول ورودی آنها)[1]. بنابراین، شیئهای مورد بحث، دنباله‌هایی نامتناهی از توزیعها هستند که در آنها هر توزیع تکیه‌گاهی متناهی دارد. چنان دنباله‌ای یک جرگهٔ[2] توزیعی نامیده می‌شود. ما جرگه‌های توزیعی به شکل $\{D_n\}_{n\in\mathbb{N}}$ را در نظر می‌گیریم که در آن برای تابعی مانند $l : \mathbb{N} \to \mathbb{N}$، تکیه‌گاه هر D_n زیرمجموعه‌ای از $\{0,1\}^{l(n)}$ است. به علاوه نوعاً l یک چندجمله‌ای مثبت خواهد بود. برای

۱. بررسی مجانبی (یا تابعی) در این رهیافت جنبهٔ اساسی ندارد. می‌توان کلِ رهیافت را برحسب ورودیهای با طولهای ثابت و مفهومی مناسب از پیچیدگی الگوریتمها به پیش برد. ولی چنان شیوه‌ای پرزحمت‌تر است.

2. ensemble

چنان D_nای، فرایندِ انتخابِ e مطابقِ توزیع D_n را با $e \sim D_n$ نشان می‌دهیم. بنابراین، برای محمولی مانند P، احتمال آن را که $P(e)$ برقرار باشد وقتی که e مطابق با D_n توزیع (یا انتخاب) شده باشد با $\Pr_{e\sim D_n}[P(e)]$ نشان می‌دهیم.

تعریف ۱. (تمایزناپذیری محاسباتی [۸، ۱۳]). دو جرگهٔ احتمال $\{X_n\}_{n\in\mathbb{N}}$ و $\{Y_n\}_{n\in\mathbb{N}}$ تمایزناپذیرِ محاسباتی نامیده می‌شوند هرگاه برای هر الگوریتم زمانْ‌چندجمله‌ای احتمالاتی مانند A، هر چندجمله‌ای مثبت مانند p، و همهٔ nهای به قدر کافی بزرگ،

$$\left|\Pr_{x\sim X_n}[A(x)=1]-\Pr_{y\sim Y_n}[A(y)=1]\right|<\frac{1}{p(n)}$$

احتمال روی X_n (به‌ترتیب، Y_n) و نیز روی پرتابهای سکهٔ الگوریتم A اختیار می‌شود.

در اینجا چند تذکر لازم است. نخست اینکه اجازه داده‌ایم الگوریتم A، که متمایزکننده نام دارد، احتمالاتی باشد. این کار، شرط را صرفاً قویتر می‌کند، و برای چندین جنبهٔ مهم رهیافت ما اساسی به نظر می‌رسد. دوم، ما پیشامدهایی را که کران بالای احتمال رخ‌دادن آنها عکس یک، چندجمله‌ای است، صرف‌نظرکردنی تلقی می‌کنیم. این امر با مفهوم کارآیی (یعنی محاسبات زمانْ‌چندجمله‌ای) به‌خوبی جفت‌وجور می‌شود: پیشامدی که با احتمالی صرف‌نظرکردنی (به‌عنوان تابعی از پارامتری مانند n) رخ می‌دهد در صورتی هم که آزمایش به دفعاتی برابر یک، چندجمله‌ای برحسب n تکرار شود، با احتمالی صرف‌نظرکردنی رخ خواهد داد. سوم، وقتی در تعریف بالا به A اجازه دهیم که تابعی دلخواه (به جای الگوریتم زمانْ‌چندجمله‌ای احتمالاتی) باشد، یک مفهوم تمایزناپذیری آماری را به‌دست خواهیم آورد. مفهوم اخیر معادل با این شرط است که فاصلهٔ تغییرات بین X_n و Y_n (یعنی $\sum_z |X_n(z)-Y_n(z)|$) (نسبت به n) ناچیز است.

یادآور می‌شویم که تمایزناپذیری محاسباتی مفهومی بسیار آزادتر از تمایزناپذیری آماری است (رک. [۱۳]). حالتی مهم، آن است که توزیعها به توسط یک مولدِ شبه‌تصادفی (به صورتی که ذیلاً تعریف می‌شود) تولید شوند: چنان توزیعهایی از نظر محاسباتی از توزیع یکنواخت تمایزناپذیرند، اما از نظر آماری از توزیع یکنواخت غیرقابل تمایز نیستند.

تعریف ۲. (مولدهای شبه‌تصادفی [۲، ۱۳]). یک الگوریتم زمانْ‌چندجمله‌ایِ تعیینی مانند G مولد شبه‌تصادفی نامیده می‌شود هرگاه تابعی کش‌آورنده مانند $l:\mathbb{N}\to\mathbb{N}$ موجود باشد به‌طوری که دو جرگهٔ احتمال زیر، که با $\{G_n\}_{n\in\mathbb{N}}$ و $\{R_n\}_{n\in\mathbb{N}}$ نشان داده می‌شوند، تمایزناپذیر محاسباتی باشند:

۱. توزیع G_n به عنوان خروجی G روی بذری که به‌طور یکنواخت انتخاب شده، در $\{0,1\}^n$ تعریف می‌شود.

۲. توزیع R_n به‌عنوان توزیع یکنواخت بر $\{0,1\}^{l(n)}$ تعریف می‌شود.

یعنی، با نشان دادنِ توزیع یکنواخت روی $\{0,1\}^m$ با U_m، قید می‌کنیم که برای هر الگوریتم زمانْ‌چندجمله‌ای احتمالاتی مانند A، هر چندجمله‌ای مثبت مانند p، و همهٔ nهای به‌قدر کافی بزرگ،

$$\left|\Pr_{s\sim U_n}[A(G(s))=1]-\Pr_{r\sim U_{l(n)}}[A(r)=1]\right|<\frac{1}{p(n)}$$

بنابراین، مولدهای شبه‌تصادفی برنامه‌های تعینی کارآ (یعنی زمانْ‌چندجمله‌ای) هستند که بذرهای کوتاهِ به تصادف انتخاب شده را منبسط کرده به صورت دنباله‌های بیتی شبه‌تصادفی بلندتر درمی‌آورند به‌طوری که دنباله‌های اخیر به صورت تمایزناپذیر محاسباتی از دنباله‌های واقعاً تصادفی، به وسیلهٔ الگوریتمهای کارآ (یعنی، زمانْ‌چندجمله‌ای) تعریف می‌شوند. نتیجه می‌گیریم که هر الگوریتم تصادفی‌شدهٔ کارآ نحوهٔ اجرای خود را، در صورتی که به‌جای پرتابهای سکهٔ درونی دنباله‌هایی قرار دهیم که به‌وسیلهٔ یک مولد شبه‌تصادفی تولید شده‌اند، حفظ می‌کند. یعنی

ساختمان ۳. (کاربرد نوعیِ مولدهایِ شبهِ تصادفی). فرض کنید که A یک الگوریتم زمانْ‌چندجمله‌ای احتمالاتی باشد، و فرض کنید که $\rho(n)$ معرف کرانی بالا برای پیچیدگی تصادفی بودن آن (یعنی تعداد سکه‌هایی که A روی ورودیهای n بیتی پرتاب می‌کند) باشد. همچنین تصورکنید که $A(x,r)$ معرفِ خروجی A روی ورودی x و دنبالهٔ پرتاب سکهٔ $r\in\{0,1\}^{\rho(|x|)}$ باشد. حال فرض کنید که G یک مولد شبه‌تصادفی با تابع کش‌آورندهٔ $l:\mathbb{N}\to\mathbb{N}$ باشد. در این صورت A_G یک الگوریتم تصادفی‌شده است که روی ورودی x به صورت زیر عمل می‌کند. عدد $k=k(|x|)$ را به‌عنوان کوچکترین عدد صحیح به‌طوری که $l(k)\geq\rho(|x|)$ قرار می‌دهد، به‌طور یکنواخت $s\in\{0,1\}^k$ را انتخاب می‌کند، و خروجی $A(x,r)$ را می‌دهد که در آن r پیشوندِ به طول $\rho(|x|)$ بیتِ $G(s)$ است.

می‌توان ثابت کرد که پیدا کردن xهای بلندی که روی آنها رفتارِ ورودی–خروجی A_G به‌طور محسوس متفاوت از آنِ A باشد، نشدنی است، گرچه A_G ممکن است از تعداد پرتابهای به مراتب کمتری در مقایسه با A استفاده کند. این موضوع در قضیهٔ زیر مدوّن شده است که در آن F معرف الگوریتمی است در پی یافتن x به گونه‌ای که $A(x)$ و $A_G(x)$ (به کمک الگوریتمی مانند D) قابل تمیز باشند.

قضیهٔ [فرعی] ۴. فرض کنید A و G به‌صورتی باشند که در بالا گفته شد. برای هر الگوریتم D، فرض کنید $\Delta_{A,D}(x)$ معرف اختلاف در رفتار A و A_G، به قضاوت D، روی ورودی x باشد یعنی $\Delta_{A,D}(x)$ به صورت زیر تعریف شود

$$\Big|\Pr_{r\sim U_{\rho(n)}}[D(x,A(x,r))=1] - \Pr_{s\sim U_{k(n)}}[D(x,A_G(x,s))=1]\Big|$$

که در آن احتمالها روی همهٔ U_mها و نیز روی کلیهٔ پرتابهای سکهٔ D گرفته شده‌اند. در این صورت برای هر جفت از الگوریتمهای زمانْ‌چندجمله‌ای احتمالاتی F و D، هر چندجمله‌ای مثبت p، و همهٔ nهای به قدر کافی بزرگ داریم

$$\Pr\left[\Delta_{A,D}(F(1^n))>\frac{1}{p(n)}\right]<\frac{1}{p(n)}$$

که در آن احتمال روی همهٔ پرتابهای سکه F گرفته می‌شود.

این قضیه با نشان دادن این موضوع ثابت می‌شود که یک سه‌تایی (A,F,D) را که حکم را نقض می‌کند می‌توان به الگوریتمی مانند D'

برگرداند که خروجی G را از توزیع یکنواخت متمایز می‌کند، و این برخلاف فرض است. با استدلالهای مشابهی می‌توان ثابت کرد که فرایند تصادفی‌شدهٔ کارآ (خواه مانند بالا الگوریتمی باشد و خواه محاسبه‌ای چندبخشی)، اگر شبه‌تصادفی بودن (با تعریف بالا) جانشین تصادفی بودن واقعی شود، رفتارش را حفظ می‌کند. بنابراین، با در دست داشتن مولدهای شبه‌تصادفی با تابع کش‌آوری بزرگ، می‌توان به‌طور قابل ملاحظه‌ای پیچیدگی تصادفی را در هر کاربرد کارآ کاهش داد.

تقویت تابع کش‌آوری

از مولدهای شبه‌تصادفی، به صورتی که در بالا تعریف شده‌اند، تنها انتظار می‌رود که ورودی خود را یک بیت کش بیاورند؛ مثلاً، کش‌آوردن ورودیهای به طول nبیت به خروجیهای به طول $(n+1)$بیت کفایت می‌کند. روشن است که مولدهایی با چنین تابعهای کش‌آوری میانه‌روی در عمل کمتر به درد می‌خورند. در مقابل، می‌خواهیم مولدهای شبه‌تصادفی با تابعهای کش‌آوریِ به دلخواه طویل داشته باشیم. بنابر شرط کارآیی، تابع کش‌آوری می‌تواند حداکثر چندجمله‌ای باشد. نتیجه آن می‌شود که مولدهای شبه‌تصادفی با کوچکترین تابعهای کش‌آوری ممکن را می‌توان برای ساختن مولدهای شبه‌تصادفی با هر تابع کش‌آوری چندجمله‌ای موردنظر به کار برد. (بنابراین، وقتی بحث از وجود مولدهای شبه‌تصادفی در میان است، می‌توانیم تابعهای کش‌آوری مشخص را نادیده بگیریم.)

قضیهٔ ۵. [۵، بخش ۲.۳.۳]. فرض کنید G یک مولد شبه‌تصادفی با تابع کش‌آوری $l(n) = n+1$ باشد و تصور کنید که l' هر تابع کش‌آوری دلخواه باشد به‌طوری که $l'(n)$ در زمان چندجمله‌ای برحسب n قابل محاسبه باشد. همچنین فرض کنید $G_1(x)$ معرف پیشوندِ به طول $|x|$ بیت $G(x)$ باشد، و $G_2(x)$ معرف آخرین بیت $G(x)$ باشد (یعنی $G(x) = G_1(x)G_2(x)$). در این صورت

$$G'(S) \overset{\text{تعریف}}{=} \sigma_1\sigma_2\cdots\sigma_{l'(|s|)}$$

که در آن $x_0 = s$، $\sigma_i = G_2(x_{i-1})$، و $x_i = G_1(x_{i-1})$ به ازای

$$i = 1, \cdots, l'(|s|)$$

یک مولد شبه‌تصادفی با تابع کش‌آوری l' است.

چگونگی ساختن مولدهای شبه‌تصادفی

روشهای شناخته شده برای ساختن این مولدها، مشکل محاسباتی را در قالب تابعهای یکطرفه (که در زیر تعریف می‌شود) به مولدهای شبه‌تصادفی بودن تبدیل می‌کنند. به بیان غیردقیق، یک تابع محاسبه‌پذیر زمانْ‌چندجمله‌ای، یکطرفه نامیده می‌شود هرگاه هر الگوریتم کارآ بتواند آن را تنها با احتمال موفقیت صرف‌نظرکردنی وارون کند. برای سهولت، تنها تابعهای یکطرفهٔ طول نگهدار را در نظر می‌گیریم.

تعریف ۶. (تابع یکطرفه). هر تابع یکطرفه مانند f، یک تابع محاسبه‌پذیر زمانْ‌چندجمله‌ای است به‌طوری که برای هر الگوریتم زمانْ‌چندجمله‌ای احتمالاتی مانند A'، هر چندجمله‌ای مثبت $p(\cdot)$، و همهٔ nهای به قدر کافی بزرگ،

$$\Pr_{x\sim U_n}\left[A'(f(x)) \in f^{-1}(f(x))\right] < \frac{1}{p(n)}$$

که در آن U_n توزیع یکنواخت بر $\{0,1\}^n$ است.

در مورد تابعهای یکطرفه، کاندیداهای رایج بر مهارناپذیری[1] حدسِ تجزیهٔ اعداد صحیح به عوامل اول، مسألهٔ لگاریتمی گسسته، و کدگشایی کدهای تصادفی خطی مبتنی هستند. ناشدنی بودن وارونسازی f، مفهومی ضعیف از پیشگویی‌ناپذیری را عاید می‌کند: فرض کنید $b_i(x)$ معرف بیت i ام x باشد. در این صورت، برای هر الگوریتم زمانْ‌چندجمله‌ای مانند

$$\Pr_{i,x}\left[A(i, f(x)) \neq b_i(x)\right] > 1/2n$$

که درآن احتمال به‌طوریکنواخت روی $i \in \{1, 2, \cdots, n\}$ و $x \in \{0,1\}^n$ گرفته شده است. مفهومی قویتر (و در واقع، قویترین مفهوم ممکن) از پیشگویی‌ناپذیری همانا محمول «هسته‌ای» است. به بیانِ غیردقیق، یک محمول قابل محاسبهٔ زمانْ‌چندجمله‌ای چون b، هستهٔ [اصلی] تابعی مانند f نامیده می‌شود هرگاه هر الگوریتم کارآ، با معلوم‌بودن $f(x)$، بتواند $b(x)$ را با احتمال موفقیتی که تنها به‌طور صرف‌نظرکردنی بیشتر از نیم باشد، حدس بزند.

تعریف ۷. (محمولِ هسته‌ای [۲]). یک محمول قابل محاسبهٔ زمانْ‌چندجمله‌ای مانند $b : \{0,1\}^* \to \{0,1\}$ هستهٔ [اصلی] تابعی مانند f نامیده می‌شود هرگاه برای هر الگوریتم زمانْ‌چندجمله‌ای احتمالاتی مانند A'، هر چندجمله‌ای مثبت $p(\cdot)$، و همهٔ nهای به قدرِ کافی بزرگ،

$$\Pr_{x\sim U_n}\left[A'(f(x)) = b(x)\right] < \frac{1}{2} + \frac{1}{p(n)}$$

آشکار است که هرگاه b هستهٔ تابع یک‌به‌یک محاسبه‌پذیر زمانْ‌چندجمله‌ای f باشد، آنگاه f باید یکطرفه باشد[2]. نتیجه آنکه هر تابع یکطرفه را می‌توان اندکی بهبود بخشید به‌طوری که محمولی هسته‌ای داشته باشد.

قضیهٔ ۸. (یک هستهٔ عام [۷]). فرض کنید که f تابع یکطرفهٔ دلخواهی باشد و تصور کنید g به صورت $g(x,r) \overset{\text{تعریف}}{=} (f(x), r)$ تعریف شود که در آن $|x| = |r|$. حال فرض کنید $b(x,r)$ معرف ضرب داخلی بردارهای دودویی x و r به پیمانهٔ ۲ باشد. در این صورت محمول b یک هستهٔ تابع g است.

برهانی از این قضیه را می‌توان در [۵، پیوست C ۲۰] یافت. سرانجام به ساختمان مولدهای شبه‌تصادفی می‌رسیم.

قضیهٔ [فرعی] ۹. (شیوهٔ ساده‌ای برای ساخت مولدهای شبه‌تصادفی).

1. intractability

۲. تابعهایی که یک‌به یک نیستند، ممکن است محمولهای هسته‌ای با ماهیت نظریهٔ اطلاعی داشته باشند، اما این تابعها در اینجا به درد ما نمی‌خورند. مثلاً، تابعهایی به شکل

$$f(\sigma, x) = 0f'(x)$$

(برای $\sigma \in \{0,1\}$) دارای یک محمول هسته‌ای «نظریهٔ اطلاعی» مانند $b(\sigma, x) = \sigma$ هستند.

فرض کنید b یک محمول هسته‌ای تابع محاسبه‌پذیر زمانْ‌چندجمله‌ای f باشد، در این صورت

$$G(s) \stackrel{\text{تعریف}}{=} f(s)b(s)$$

(یعنی $f(s)$ و پس از آن $b(s)$) یک مولد شبه‌تصادفی است.

به یک معنی، نکتهٔ اصلی در برهان قضیهٔ بالا عبارت از اثبات آن است که پیشگویی‌ناپذیری خروجی G (که بنا به تعریف واضح است) مستلزم شبه‌تصادفی بودن آن است. این حقیقت که پیشگویی‌ناپذیری (بیت بعدی) و شبه‌تصادفی بودن در حالت کلی معادل‌اند، در توصیف دیگری از موضوع که در زیر می‌آید، به صراحت ثابت می‌شود.

توصیف دیگر

شیوه‌ای که برای ساخت مولدهای شبه‌تصادفی، از طریق قضیه‌های ۵ و ۹، عرضه کردیم، متفاوت اما مشابه با طرز ساخت مولدهای شبه‌تصادفی است که به‌وسیلهٔ بلوم و میکالی [۲] مطرح شده است: با مفروض بودن تابع کش‌آوری دلخواه $l : \mathbb{N} \to \mathbb{N}$ و یک تابع یکطرفهٔ یک‌به‌یک با هستهٔ b، تعریف می‌کنیم

$$G(s) \stackrel{\text{تعریف}}{=} b(x_0)b(x_1)\cdots b(x_{l(|s|)-1})$$

که در آن $x_0 = s$ و $x_i = f(x_{i-1})$ به ازای $i = 1, \cdots, l(|s|) - 1$. یک مصداق ملموس، بر مبنای این فرض که تجزیهٔ اعداد صحیح بزرگ کاری دشوار است، در شکل ۱ شرح داده شده است. شبه‌تصادفی بودن G در دو گام با استفاده از مفهوم پیشگویی‌ناپذیری (بیت بعدی) برقرار شده است. جرگه‌ای چون $\{Z_n\}_{n\in\mathbb{N}}$ پیشگویی‌ناپذیر نامیده می‌شود هرگاه هیچ ماشین زمانْ‌چندجمله‌ای احتمالاتی که پیشوندی از Z_n را به‌دست می‌آورد، قادر به پیشگویی بیتِ بعدی آن با احتمالی که به طور صرف‌نظرناکردنی بزرگتر از ۱/۲ است، نباشد.

گام ۱. ابتدا ثابت می‌کنیم که جرگهٔ $\{G(U_n)\}_{n\in\mathbb{N}}$، که در آن U_n توزیع یکنواخت روی $\{0,1\}^n$ است، پیشگویی‌ناپذیر (از لحاظ بیت بعدی) است (از راست به چپ [۲]). به بیانی غیردقیق، اگر بتوان $b(x_i)$ را از روی $b(x_{i+1})\ldots b(x_{l(|s|)-1})$ پیشگویی کرد آنگاه می‌توان $b(x_i)$ را با مفروض‌بودن $f(x_i)$ پیشگویی کرد (یعنی، با محاسبهٔ x_{i+1}، ...، $x_{l(|s|)-1}$ و به این ترتیب، به‌دست آوردن $b(x_{i+1})\cdots b(x_{l(|s|)-1})$). اما این نتیجه با فرض هسته در تناقض است.

گام ۲. سپس از نتیجه‌گیری یائو استفاده می‌کنیم که بنابر آن یک جرگهٔ شبه‌تصادفی است اگر و تنها اگر پیشگویی‌ناپذیر (از لحاظ بیت بعدی) باشد (رک. ۴، بخش ۳.۳.۴).

روشن است که اگر بتوان بیت بعدی را در یک جرگه پیشگویی کرد، آنگاه می‌توان این جرگه را از جرگهٔ یکنواخت تمیز داد (که صرف‌نظر از توان محاسبه، پیشگویی‌ناپذیر است). ولی ما طرف دیگر را که کمتر بدیهی است لازم داریم. می‌توان نشان داد که پیشگویی‌ناپذیری (بیت بعدی) مستلزم تمایزناپذیری از جرگهٔ یکنواخت است. به طور مشخص، توزیعهای «دورگه»ای را در نظر بگیرید که در آن دورگهٔ iام، i بیت نخست را از جرگهٔ مورد بحث و بقیه

فرض می‌کنیم که تجزیهٔ اعداد صحیحی که حاصلضرب دو عدد اول بزرگ اند (هر یک همنهشت با ۳ به پیمانهٔ ۴) ناشدنی باشد. تحت این فرض، مجذورکردن به پیمانهٔ چنان اعداد صحیحی یک تابع یکطرفه خواهد بود. به علاوه، مجذورکردن به پیمانهٔ چنان Nای روی مانده‌های مربعی به پیمانهٔ N یک‌به‌یک است، و کم‌معناترین بیتِ شناسه، یک هستهٔ متناظر است [۱].

مولد شبه‌تصادفی زیر از یک الگوریتم زمانْ‌چندجمله‌ای استفاده می‌کند که وقتی $4m$ بیت به آن خورانده شود، عددی mبیتی تولید می‌کند به‌طوری که وقتی ورودیهای $4m$بیتی به صورت یکنواخت توزیع شده باشند، خروجی اساساً یک عدد اول تصادفی mبیتی (همنهشت با ۳ به پیمانهٔ ۴) است.

ورودی: یک بذر nبیتی $s = abc$، که در آن $|a| = |b| = 4n/10$.

گامهای آغازی:

۱. با استفاده از a، عدد اول $n/10$ بیتی (به پیمانهٔ ۴) $p \equiv 3$ را تولید کنید.

۲. به همین نحو، از b استفاده کرده، (به پیمانهٔ ۴) $q \equiv 3$ را تولید کنید.

۳. p را در q ضرب کنید و N را به‌دست آورید.

۴. فرض کنید (به پیمانهٔ N) $x_0 \leftarrow c^2$.

تکرارها: برای $i = 0, \cdots, l(n) - 1$

۵. فرض کنید b_i کم‌معناترین بیت x_i باشد.

۶. فرض کنید (به پیمانهٔ N) $x_{i+1} \leftarrow x_i^2$.

خروجی: $b_0, b_1, \cdots, b_{l(n)-1}$.

شکل۱ یک مولد شبه‌تصادفی بر مبنای اجرا نشدنی بودن تجزیه به عاملها.

را از توزیع یکنواخت اختیار می‌کند. بنابراین، تمیزدادن دورگه‌های کرانگینی مستلزم تمیزدادن برخی دورگه‌های همسایه است که به نوبهٔ خود مستلزم پیشگویی‌ناپذیری بیت بعدی (در جرگهٔ مورد بحث) است.

شرطی عام برای وجود مولدهای شبه‌تصادفی

به خاطر آورید که با مفروض بودن هر تابع یک‌به‌یک یکطرفه، می‌توان به‌آسانی یک مولد شبه‌تصادفی ساخت. درواقع، می‌توان شرط یک‌به‌یک بودن را کنار گذاشت، اما شیوهٔ فعلاً معلوم برای ساخت ــ در حالت کلی ــ کاملاً پیچیده است. با این‌حال، داریم:

قضیهٔ ۱۰. (دربارهٔ وجود مولدهای شبه‌تصادفی [۹]). مولدهای شبه‌تصادفی موجودند اگر و تنها اگر تابعهای یکطرفه موجود باشند.

برای نشان دادن اینکه وجودِ مولدهای شبه‌تصادفی مستلزم وجود تابعهای یکطرفه است، مولدی شبه‌تصادفی مانند G را با تابع کش‌آوری $l(n) = 2n$ درنظربگیرید. برای هر $x, y \in \{0,1\}^n$، تعریف کنید $f(x,y) \stackrel{\text{تعریف}}{=} G(x)$

به طوری که f محاسبه‌پذیر زمانْ‌چندجمله‌ای (و طول نگهدار) باشد. باید f یکطرفه باشد چه در غیر این‌صورت می‌توان $G(U_n)$ را از U_{2n}، با تلاش برای وارون کردن و امتحان کردن نتیجه، تمیز داد: وارون کردن f روی توزیع دامنهٔ آن به توزیع $G(U_n)$ باز می‌گردد، درحالی که احتمال اینکه U_{2n} تحت f دارای وارون باشد، صرف‌نظرکردنی است.

مسیر جالب توجه، ساختن مولدهای شبه‌تصادفی براساس هر تابع یکطرفه دلخواه است. در حالت کلی (وقتی که f ممکن است یک به یک نباشد)، جرگهٔ $f(U_n)$ ممکن است شبه‌تصادفی نباشد، و بنابراین ساختمان ۹، (یعنی $G(s) = f(s)b(s)$، که در آن b یک هستهٔ f است) نمی‌تواند مستقیماً مورد استفاده قرار گیرد. در عوض این ساختمان همراه با چند ایدهٔ دیگر به‌کار می‌رود (رک. [۹]). متأسفانه، این ایده‌ها و بیشتر از آن، جزئیات به اجرا درآوردن آنها به‌مراتب پیچیده‌تر از آن هستند که بتوان در اینجا توصیفشان کرد. درواقع شیوهٔ دیگری برای ساخت مولدهای شبه‌تصادفی بر مبنای هر تابع یکطرفهٔ دلخواه ارزش بیشتری دارد.

تابعهای شبه‌تصادفی

مولدهای شبه‌تصادفی امکان تولیدِ کارآیِ دنباله‌های شبه‌تصادفی بلند را از بذرهای تصادفی کوتاه فراهم می‌آورند. تابعهای شبه‌تصادفی (که در زیر تعریف می‌شوند) از این هم نیرومندترند: آنها امکان دسترسی کارآیِ مستقیم به دنبالهٔ شبه‌تصادفی عظیمی را (که بررسی بیت به بیت آن ناشدنی است) فراهم می‌آورند. به عبارت دیگر، تابعهای شبه‌تصادفی را می‌توان در هرکاربرد کارآ (مثلاً، قابل ذکرتر از همه در رمزنگاری) به جای تابعهای واقعاً تصادفی قرار داد. یعنی، تابعهای شبه‌تصادفی از تابعهای تصادفی به‌وسیلهٔ ماشینهای کارآیی که مقادیر تابعها را در شناسه‌هایی به انتخاب خود به‌دست می‌آورند، قابل تمایز نیستند. چنان ماشینهایی «ماشینهای مکاشفه»[1] نامیده می‌شوند؛ و اگر M چنان ماشینی باشد و f یک تابع باشد، آنگاه $M^f(x)$ معرف محاسبهٔ M روی ورودی x است وقتی پرسشهای M به‌وسیلهٔ تابع f پاسخ داده می‌شوند.

تعریف ۱۱. (تابعهای شبه‌تصادفی [۶]). یک تابع شبه‌تصادفی (جرگه)، با پارامترهای طول $l_D, l_R : \mathbb{N} \to \mathbb{N}$، مجموعه‌ای از تابعهای

$$F \overset{\text{تعریف}}{=} \{f_s : \{0,1\}^{l_D(|s|)} \to \{0,1\}^{l_R(|s|)}\}_{s\in\{0,1\}^*}$$

است که در شرطهای زیر صدق می‌کند:

- (محاسبهٔ کارآ). یک الگوریتم کارآی (تعینی) موجود است به‌طوری که وقتی یک بذر s و یک شناسهٔ $l_D(|s|)$ بیتی، x، داده شده باشد، مقدار $f_s(x)$ به طول $l_R(|s|)$ را باز می‌گرداند.

  (بنابراین، بذر s «توصیف کارآیی» از تابع f_s است.)
- (شبه‌تصادفی بودن). برای هر ماشین مکاشفهٔ زمانْ‌چندجمله‌ای احتمالاتی مانند M، هر چندجمله‌ای مثبت مانند p، و همهٔ nهای به قدر کافی بزرگ،

$$\left|\Pr_{f\sim F_n}[M^f(1^n) = 1] - \Pr_{\rho\sim R_n}[M^\rho(1^n) = 1]\right| < \frac{1}{p(n)}$$

که در آن F_n معرف توزیع روی $f_s \in F$ است که با انتخاب s به‌طور یکنواخت در $\{0,1\}^n$ به‌دست آمده است و R_n معرف توزیع یکنواخت روی کلیهٔ تابعهایی است که $\{0,1\}^{l_D(n)}$ را به $\{0,1\}^{l_R(n)}$ می‌نگارند.

برای سهولت فرض کنید که $l_D(n) = n$ و $l_R(n) = 1$. در این صورت تابعی که به‌طور یکنواخت از بین 2^n تابع (از یک جرگهٔ شبه‌تصادفی) انتخاب شده است، در زمان چندجمله‌ای برحسب n، یک رفتار ورودی-خروجی تمایزناپذیر از رفتار تابعی که به تصادف از بین کلیهٔ 2^{2^n} تابع بولی انتخاب شده است، نشان می‌دهد. این را با توزیعی روی 2^n دنباله، که با یک مولد شبه‌تصادفی به کار رفته در مورد یک بذر تصادفی nبیتی تولید شده است، مقایسه کنید. بذر اخیر غیرقابل تمایز از دنباله‌ای است که به‌طور یکنواخت از بین همهٔ چندجمله‌ای برحسب 2^n دنباله انتخاب شده است. در عین حال، تابعهای شبه‌تصادفی را می‌توان از روی هر مولد شبه‌تصادفی ساخت.

قضیهٔ ۱۲. (چگونگی ساختن تابعهای شبه‌تصادفی [۶]). فرض کنید که G یک مولد شبه‌تصادفی با تابع کش‌آوری $l(n) = 2n$ باشد، همچنین فرض کنید $G_0(s)$ (به ترتیب، $G_1(s)$) معرف نخستین (به ترتیب، آخرین) $|s|$ بیت در $G(s)$ باشد، و

$$G_{\sigma_{|s|}\cdots\sigma_2\sigma_1}(s) \overset{\text{تعریف}}{=} G_{\sigma_{|s|}}(\cdots G_{\sigma_2}(G_{\sigma_1}(s))\cdots)$$

در این صورت، جرگهٔ تابعی $\{f_s : \{0,1\}^{|s|} \to \{0,1\}^{|s|}\}_{s\in\{0,1\}^*}$، که در آن $f_s(x) \overset{\text{تعریف}}{=} G_x(s)$، شبه‌تصادفی با پارامترهای طول، $l_D(n) = l_R(n) = n$ است.

شیوهٔ ساخت بالا را می‌توان به آسانی در مورد هر نوع پارامترهای طول (که کرانی به صورت چندجمله‌ای داشته باشند):

$$l_D, l_R : \mathbb{N} \to \mathbb{N}$$

به کار برد.

متذکر می‌شویم که تابعهای شبه‌تصادفی برای استخراج نتایج منفی در نظریهٔ یادگیری محاسباتی و نظریهٔ پیچیدگی به‌کار رفته‌اند.

کاربردپذیری مولدهای شبه‌تصادفی

شبه‌تصادفی بودن نقشی با اهمیت روزافزون در محاسبات ایفا می‌کند: اغلب در طرح الگوریتمهای دنباله‌ای، موازی، و توزیع شده به‌کارگرفته می‌شود و البته نقشی مرکزی در رمزنگاری دارد. هر چند طرح چنین الگوریتمهایی با استفادهٔ آزادانه از تصادفی بودن، آسان است اما در عین حال مطلوب آن است که استفاده از تصادفی بودن در اجراهای واقعی به حداقل برسد زیرا تولید کردن بیتهای کاملاً تصادفی از طریق سخت‌افزار ویژه بسیار گران است. بنابراین، مولدهای شبه‌تصادفی (به‌صورتی که در بالا تعریف شدند) جزء اصلی در یک «جعبه ابزار الگوریتمی» است: این مولدها برنامه‌های مترجم خودکاری برای برگرداندن برنامه‌هایی که آزادانه از تصادفی بودن استفاده می‌کنند به برنامه‌هایی که استفادهٔ صرفه‌جویانه‌ای از تصادفی بودن به‌عمل می‌آورند، در اختیار می‌گذارند.

درواقع، «مولدهای اعداد شبه‌تصادفی» با نخستین کامپیوترها به عرصه درآمدند. با این‌حال، در اجراهای نوعی از مولدهایی استفاده می‌کنند که

1. oracle machines

بنابر تعریف بالا شبه‌تصادفی نیستند. در عوض، نشان داده می‌شود که این مولدها، در بهترین حالت، برخی آزمونهای آماری خاص را با موفقیت از سر می‌گذرانند. (رک. [۱۰]). با این‌حال، این حقیقت که یک «مولد اعداد شبه‌تصادفی» برخی آزمونهای آماری را با موفقیت می‌گذراند، به این معنی نیست که آزمون جدیدی را خواهد گذراند یا برای کاربردی (آزمون نشده) در آینده مناسب خواهد بود. به‌علاوه، رهیافتِ قراردادنِ مولد در معرض برخی آزمونهای خاص، قادر به تأمین نتایج کلی از نوعی که در بالا بیان شد، نیست (یعنی، به شکل «برای کلیهٔ مقاصد عملی، استفاده از خروجیِ مولد، همان حسن را دارد که استفاده از پرتابهای سکهٔ نااریب واقعی»). در مقابل، رهیافتی که در تعریف ۲ مندرج است، چنان کلیتی را هدف خود قرار می‌دهد و درواقع برای به‌دست آوردن آن طرح‌ریزی شده است: مفهوم تمایزناپذیری محاسباتی، که زمینهٔ تعریف ۲ است، کلیهٔ کاربردهای ممکن کارآ را دربرمی‌گیرد و مبتنی بر این فرض است که برای همهٔ آنها، دنباله‌های شبه‌تصادفی به‌خوبی دنباله‌های واقعاً تصادفی‌اند.

مولدها و تابعهای شبه‌تصادفی در رمزنگاری اهمیت اساسی دارند. آنها نوعاً برای ایجاد طرحهای رمزگذاری کلیدْ شخصی[1] و تعیین صحت به‌کار می‌روند (رک. [۵، بخشهای ۲.۵.۱ و ۲.۶.۱]). به عنوان مثال، فرض کنید که دو گروه در یک رشتهٔ تصادفی nبیتی مانند s، که یک تابع شبه‌تصادفی را (مطابق تعریف ۱۱ با $l_D(n) = l_R(n) = n$) مشخص می‌کنند، شریک‌اند، و s برای رقیب آنها نامعلوم است. در این صورت دو گروه مزبور می‌توانند پیامهایی رمزی را با XOR[2] کردن پیام با مقدار f_s در نقطه‌ای تصادفی به یکدیگر ارسال کنند، یعنی برای رمزگذاری $m \in \{0,1\}^n$، فرستنده به‌طور یکنواخت $r \in \{0,1\}^n$ را انتخاب و $(r, m \oplus f_s(r))$ را به گیرنده می‌فرستد. امنیت این طرح رمزگذاری بر این حقیقت متکی است که برای هر رقیبِ از نظر محاسباتی ممکن (نه تنها برای استراتژیهای رقیب که به تصور درآمده و مورد امتحان قرارگرفته‌اند)، مقادیر تابع f_s روی چنان rهایی تصادفی به نظر می‌رسد.

درونمایه‌های نظری مولدهای شبه‌تصادفی

اینک به اختصار برخی جنبه‌های نظری مولدهای شبه‌تصادفی را، به صورتی که در بالا تعریف شدند، مورد بحث قرار می‌دهیم.

رفتارشناخت در برابر هستی‌شناخت

تعریف ما از مولدهای شبه‌تصادفی مبتنی بر مفهوم تمایزناپذیری محاسباتی است. ماهیت رفتارشناختی مفهوم اخیر به بهترین نحو از مقایسهٔ آن با رهیافت کولموگوروف شایتین به تصادفی بودن، مدلل می‌شود. به بیان غیردقیق، یک رشتهٔ تصادفی-کولموگوروفی است هرگاه طول آن برابر با طول کوتاهترین برنامه‌ای باشد که آن را تولید می‌کند. این کوتاهترین برنامه را می‌توان «توضیح واقعیِ» پدیده‌ای که به‌وسیلهٔ آن رشته توصیف می‌شود، تلقی کرد. بنابراین یک رشتهٔ تصادفی-کولموگوروفی رشته‌ای است که توضیح اساساً ساده‌تری (یعنی کوتاهتری) در مقایسه با خودش نداشته باشد. در نظرگرفتن ساده‌ترین توضیح یک پدیده را می‌توان رهیافتی هستی‌شناختی تلقی کرد. در مقابل، در نظرگرفتن تأثیر پدیده (بر یک مشاهده‌گر) به‌عنوان زمینهٔ تعریفِ شبه‌تصادفی بودن، یک رهیافت رفتارشناختی است. به علاوه، توزیعهای احتمالی موجودند که یکنواخت نیستند (و حتی از نظر آماری به یک توزیع یکنواخت نزدیک نیستند) اما به وسیلهٔ هیچ شیوهٔ کارآیی از یک توزیع یکنواخت قابل تمایز نیستند. بنابراین، توزیعهایی که از نظر هستی‌شناختی بسیار متفاوت باشند، بنابر دیدگاه رفتارشناختی که در تعریف بالا اتخاذ شد، معادل تلقی می‌شوند.

دیدگاه نسبی‌گرایانه‌ای در بارهٔ تصادفی بودن

شبه‌تصادفی بودن در بالا نسبت به مشاهده‌گر آن تعریف شد. منظور از آن، توزیعی است که نمی‌توان آن را به‌وسیلهٔ هیچ مشاهده‌گر کارآ (یعنی، زمانْ‌چندجمله‌ای) از یک توزیع یکنواخت تمیز داد. با این‌حال، دنباله‌های شبه‌تصادفی را می‌توان از دنباله‌های تصادفی به‌وسیلهٔ کامپیوترهای بینهایت قدرتمند (که در اختیار ما نیستند!) تمیز داد. به‌طور مشخص، یک ماشین زمانْ‌نمایی می‌تواند به آسانی، خروجی یک مولد شبه‌تصادفی را از رشته‌ای با همان طول که به‌طور یکنواخت انتخاب شده است، تمیز دهد (مثلاً، فقط با امتحان کردن کلیهٔ بذرهای ممکن). بنابراین، شبه‌تصادفی بودن، امری ذهنی، و وابسته به تواناییهای مشاهده‌گر است.

تصادفی بودن و دشواری محاسباتی

شبه‌تصادفی بودن و دشواری محاسباتی نقشهایی دوگان یکدیگر دارند: تعریف شبه‌تصادفی بودن بر این حقیقت متکی است که قراردادن محدودیتهای محاسباتی بر مشاهده‌گر به توزیعهایی منجر می‌شود که یکنواخت نیستند ولی با این‌حال نمی‌توان آنها را از توزیع یکنواخت تمیز داد. به‌علاوه، ساختمان مولدهای شبه‌تصادفی متکی بر حدسهایی در بارهٔ دشواری محاسباتی (یعنی، وجود تابعهای یکطرفه) است، و این امر اجتناب‌ناپذیر است: با مفروض بودن یک مولد شبه‌تصادفی، می‌توانیم تابعهای یکطرفه بسازیم. بنابراین، شبه‌تصادفی بودنِ نابدیهی و دشواری محاسباتی را می‌توان با هم جابه‌جا کرد.

تعمیم

شبه‌تصادفی بودن را به‌صورتی که در بالا مرور شد، می‌توان حالت خاص مهمی از یک پارادیم [الگوی] کلی تلقی کرد. یک صورتبندی عام مولدهای شبه‌تصادفی عبارت است از مشخص کردن سه جنبهٔ بنیادی — اندازهٔ کش‌آوری مولدها، ردهٔ متمایزکنندگانی که انتظار می‌رود مولدها فریبشان بدهند (یعنی الگوریتمهایی که نسبت به آنها تمایزناپذیری محاسباتی باید برقرار باشد)، و منابعی که مولدها مجاز به استفاده از آنها هستند (یعنی، پیچیدگی محاسباتی خود آنها). در توصیف بالا، ما بر مولدهای زمانْ‌چندجمله‌ای عطف توجه کردیم (بنابراین اندازهٔ کش‌آوری چندجمله‌ای را داشتیم) که هر مشاهده‌گر زمانْ‌چندجمله‌ای احتمالاتی را فریب می‌دهد. حالتهای گوناگون دیگری نیز مورد توجه‌اند، و به اختصار بعضی از آنها را مورد بحث قرار می‌دهیم. برای تفصیل بیشتر، رک. [۵].

مفاهیم ضعیفتر تمایزناپذیری محاسباتی

هرگاه منظور ما این باشد که به جای دنباله‌های تصادفی، که به‌وسیلهٔ الگوریتمی به‌کارگرفته شده‌اند، دنباله‌های شبه‌تصادفی را قرار دهیم، می‌توان

1. private-key 2. exclusive or

تلاش کرد که از اطلاعات مربوط به الگوریتم هدف سود برده شود. در بالا صرفاً از این حقیقت استفاده کرده‌ایم که الگوریتم هدف در زمان چندجمله‌ای اجرا می‌شود. ولی اگر مثلاً بدانیم که الگوریتم از فضای کاری بسیار کمی استفاده می‌کند، آنگاه ممکن است قادر باشیم بهتر عمل کنیم. همین‌طور ممکن است بتوانیم بهتر عمل کنیم هرگاه بدانیم که تحلیل الگوریتم تنها به برخی خاصیتهای دنبالهٔ تصادفی که به‌کار می‌برد، و وابسته است (مثلاً، استقلال دوبه‌دوی عناصر آن). در حالت کلی، مفاهیم ضعیفتر تمایزناپذیری محاسباتی نظیر فریب‌دادن الگوریتمهای فضا کراندار، مدارهای ژرفا ثابت، و حتی آزمونهای مشخص (مثلاً، آزمون کردن استقلال دوبه‌دوی دنباله) به‌طور طبیعی پیش می‌آیند. مولدهایی که دنباله‌هایی را تولید می‌کنند که چنان آزمونهایی را فریب می‌دهند، در کاربردهای گوناگونی مفیدند؛ اگر در کاربرد مورد نظر، تصادفی بودن به‌طریقی محدود به کاربرده شود، در این صورت دادن دنباله‌هایی با کیفیت تصادفی پایین به خورد آن، ممکن است کافی باشد. نیازی به گفتن نیست که نویسنده از صورتبندی دقیق مشخصه‌هایی با چنان کاربردها و ساخت دقیق مولدهایی هواداری می‌کند که آن نوع از آزمونها را که پیش می‌آیند، فریب دهد.

سایر مفاهیم کارآیی مولدها

پاراگراف پیشین بر یک جنبه از مسألهٔ شبه‌تصادفی بودن تمرکز داشت: منابع یا نوع مشاهده‌گر (یا متمایزکنندهٔ بالقوه). پرسش مهم دیگر این است که آیا چنان دنباله‌های شبه‌تصادفی را می‌توان از دنباله‌های بسیار کوتاهتر تولید کرد و به چه بهایی (یعنی با چه میزان پیچیدگی). در سرتاسر این مقاله شرط کرده‌ایم که فرایند تولید دست‌کم به قدر متمایزکننده، کارآ باشد[1]. این شرط درواقع، «منصفانه» و طبیعی است. مجاز داشتن مولد به اینکه پیچیده‌تر از متمایزکننده باشد (یعنی، از زمان یا فضای بیشتر استفاده کند)، غیرمنصفانه به نظر می‌رسد اما باز هم پیامدهای جالب توجهی در چارچوب تلاش برای «پادتصادفی‌سازی[2]» رده‌های پیچیدگی تصادفی دارد. به عنوان مثال، می‌توان مولدهایی را در نظر گرفت که نسبت به طول بذر در زمان نمایی کار می‌کنند. در برخی حالتها، چنین آسانگیریهایی (یعنی مجازداشتن مولدهای زمان‌نمایی) چیزی از دست نمی‌دهیم. برای ملاحظهٔ دلیل آن، یک استدلال نوعیِ مبتنی بر پادتصادفی‌سازی را در نظر می‌گیریم که مرکب از دو گام است: ابتدا به جای دنباله‌های واقعاً تصادفی الگوریتم، دنباله‌های تصادفی تولید شده از بذرهای بسیار کوتاهتر را قرار می‌دهیم، و سپس به‌طور تعینی به تمام بذرهای ممکن رجوع می‌کنیم و در پی یافتن رفتارِ با بیشترین فراوانیِ الگوریتم اصلاح‌شده برمی‌آییم. در چنین حالتی، پیچیدگی تعینی در هر حال نسبت به طول بذر، نمایی است. نفع این کار آن است که ساختن مولدهای زمان‌نمایی ممکن است آسانتر از ساختن مولدهای زمان‌چندجمله‌ای باشد.

۱. درواقع شرط کرده‌ایم که مولد کارآتر از متمایزکننده باشد: یعنی شرط کرده‌ایم که مولد یک الگوریتم زمان‌چندجمله‌ای ثابت باشد، در حالی که متمایزکننده مجاز است که هر الگوریتمی با زمان اجرای چندجمله‌ای باشد.

2. derandomization

مراجع

1. W. Alexi, B. Chor, O. Goldreich, and C. P. Schnorr, RSA/Rabin functions: Certain parts are as hard as the whole, *SIAM J. Comput.* **17** (1988), 194-209.
2. M. Blum and S. Micali, How to generate cryptographically strong sequences of pseudo-random bits, *SIAM J. Comput.* **13** (1984), 850-864.
3. T. M. Cover and G. A. Thomas, *Elements of Information Theory*, Wiley, New York, 1991.
4. O. Goldreich, *Foundation of Cryptography–Fragments of a Book*, February 1995, available from `http://theory.lcs.mit.edu/~oded/frag.html`.
5. ———, *Modern Cryptography, Probabilistic Proofs and Pseudorandomness*, Algorithms and Combinatorics, vol. 17, Springer-Verlag, New York, 1998.
6. O. Goldreich, S. Goldwasser, and S. Micali, How to construct random functions, *J. ACM* **33** (1986), 792-807.
7. O. Goldreich and L. A. Levin, Hard-core predicates for any one-way function, *21st ACM Symposium on the Theory of Computing*, 1989, pp. 25-32.
8. S. Goldwasser and S. Micali, Probabilistic encryption, *J. Comput. System Sci.* **28** (1984), 270-299.
9. J. Hastad, R. Impagliazzo, L. A. Levin, and M. Luby, A pseudorandom generator from any one-way function, *SIAM J. Comput.* **28** (1999), 1364-1396.
10. D. E. Knuth, *Seminumerical Algorithms*, The Art of Computer Programming, Vol. 2, Addison-Wesley, Reading, MA, 1969; second edition. 1981.
11. L. A. Levin, Randomness conservation inequalities: Information and independence in mathematical theories, *Inform. and Control* **61** (1984), 15-37.
12. M. Li and P. Vitanyi, *An Introduction to Kolmogorov Complexity and Its Applications*, Springer-Verlag, New York, 1993.
13. A. C. Yao, Theory and application of trapdoor functions, *23rd IEEE Symposium on Foundations of Computer Science*, 1982, pp. 80-91.

* * * * * *

• Oded Goldreich, "Pseudorandomness", *Notices Amer. Math. Soc.*, (10) **46** (1999) 1209-1216.

* اودت گُلدرایش، مؤسسهٔ علوم وایزمن، اسرائیل

oded@wisdom.weizmann.ac.il

آیا ریاضیات به اصول موضوع جدید نیاز دارد؟•

سالومون ففرمن*
ترجمهٔ هاله المعی

این سؤال تقریباً از هر لحاظ ابهام دارد:
منظور از «ریاضیات» چیست؟
منظور از «نیاز» چیست؟
منظور از «اصل موضوع» چیست؟

حتی می‌شود پرسید منظور از «آیا» چیست؟

بخشی از این ابهام به خاطر این است که این سؤال را از دیدگاههای مختلفی می‌توان مطرح کرد. مهمترین اختلاف، بین دیدگاه ریاضیکاران است و دیدگاه منطقدانانی که سروکار با مبانی ریاضیات دارند. شاید بعضی منطقدانان به این تمایز اعتراض کنند چون آنها هم خودشان را ریاضیدانهایی می‌دانند که ازقضا تخصصشان منطق ریاضی است. شکی نیست که منطق جدید شاخهٔ بسیار معتبری از ریاضیات شده است و درواقع چند نشریهٔ کاملاً تخصصی منطق داریم که در یک نگاه اجمالی، مطالبشان، گذشته از موضوع، هیچ فرقی با نشریه‌های ریاضی ندارد، مثل انالز آو پیور اند اپلاید لاجیک و جورنال آو سیمبالیک لاجیک. حتی دقیقتر که نگاه کنیم، می‌شود مقاله‌ای پیدا کرد، مثلاً، دربارهٔ نیم‌مشبکهٔ درجات حل‌ناپذیری یا نظریهٔ مدلهای میدانها که از لحاظ سرشت کلی هیچ فرقی با مقاله‌ای در باب نظریهٔ ترکیبیاتی گرافها یا همانستگی [کوهومولوژی] گروهها نداشته باشد؛ اینها به اصطلاح به یک چارچوب ذهنی تعلق دارند. اما اگر مقالهٔ گودل دربارهٔ ناتمامیت دستگاههای اصل موضوعی برای ریاضیات، یا قضیه‌های او و کوهن در بارهٔ سازگاری و استقلال اصل موضوع انتخاب نسبت به اصل موضوعهای نظریهٔ مجموعه‌ها را در نظر بگیریم، در چارچوب ذهنی دیگری خواهیم بود، چون داریم کاری را می‌کنیم که هیلبرت فرا‌ریاضیات می‌نامد: مطالعهٔ خودِ ریاضیات به‌وسیلهٔ منطق ریاضی از طریق صورتبندی آن در دستگاه اصل موضوعی. و این موضع است که می‌خواهم آن را متمایز کنم از موضع ریاضیدانانی که کارشان آنالیز یا جبر یا توپولوژی یا درجات حل‌ناپذیری و از این قبیل چیزهاست. صحبت از منطقدان به منزلهٔ فراریاضیدان ناخوشایند است، و من از منطق این‌طور صحبت نخواهم کرد، اما این چیزی است که در ذهن دارم.

با اینکه اصلاً نمی‌خواهم دیدگاه ریاضیکاران را ندیده بگیرم، در این مقاله عمدتاً سؤال مورد بحث را از دیدگاه منطقدانان بررسی می‌کنم، و به‌خصوص از چشم‌انداز یکی از منطقدانان بسیار مهم: کورت گودل. گودل از زمان انتشار قضیهٔ چشمگیر ناتمامیت در سال ۱۹۳۱ تا پایان عمر درصدد پیداکردن اصول موضوع جدیدی برای حل و فصل مسائل بلاتکلیف حساب بود. و علاوه بر این از سال ۱۹۴۷ به بعد با انتشار مقالهٔ نامتعارفش «مسأله پیوستار کانتور چیست؟» [۱۲] به دنبال اصول موضوع تازه‌ای برای به سامان رساندن حدس مشهور کانتور در بارهٔ عدد کاردینال پیوستار بود. در هر دو مورد، به عقیدهٔ او این اصول موضوع جدید باید در شِماهای بینهایتِ [مراتب] بالاتر در نظریهٔ مجموعه‌ها جستجو می‌شد. در سالهای اخیر منطقدانان مطالب زیادی آموخته‌اند که به برنامهٔ گودل مربوط می‌شود، اما در بارهٔ اینکه از یافته‌های آنها چه نتایجی عاید می‌شود، هنوز خیلی حرفها هست. من در این مورد اصلاً بی‌طرف نیستم و آخر مقاله می‌بینید چه نتیجه‌ای از این بحثها می‌گیرم، اما سعی می‌کنم سایر مواضع را هم منصفانه ارائه کنم تا خودتان هر طور می‌خواهید نتیجه‌گیری کنید.

فرهنگ انگلیسی آکسفورد «اصل موضوع» را درکاربرد منطق و ریاضی چنین تعریف می‌کند: «گزاره‌ای بدیهی که برای اثبات صدق آن نیازی به برهان صوری نیست، بلکه به محض بیان، پذیرفته و تأیید می‌شود.» فکر می‌کنم وقتی صحبت از اصل موضوع ریاضی می‌شود اولین چیزی که در ذهن

داریم کم‌وبیش همین تعریف است: من این را معنای آرمانی کلمه می‌نامم. جای تعجب است که معنای اصل موضوع عملاً چه در ریاضیات و چه در منطق این‌قدر از مفهوم آرمانی دور شده است. بعضی حتی آن را به معنای فرض دلخواه به‌کار می‌برند و به این ترتیب اصلاً جدی نمی‌گیرند که اصل موضوع قرار است در خدمت چه هدفی باشد.

وقتی ریاضیکاری صحبت از اصل موضوع می‌کند، معمولاً منظورش اصول موضوع مربوط به بخش خاصی از ریاضیات مثل گروه، حلقه، فضای برداری، فضای توپولوژیک، فضای هیلبرت و امثال آن است. این اصول موضوع نه‌کاری به‌گزاره‌های بدیهی دارند، نه مبادی اختیاری برای شروع کارند. اینها صرفاً تعاریف انواع ساختارهایی هستند که دیده شده در وضعیتهای ریاضی مختلف ظاهر می‌شوند. اما نقش اصل موضوع را دارند به این معنا که چارچوبی فراهم می‌آورند که در آن بعضی از انواع عملیات یا برخی شیوه‌های استدلال صحیح‌اند و بعضی نیستند. و همین‌که وارد ساختاری با دستگاهی از این اصل موضوعها شدیم ــ مثلاً گروهی که به یک معادله یا یک فضای توپولوژیک وابسته است ــ کلی نتایج اثبات‌شده برای کارهای بعدی در اختیار داریم. من بی‌آنکه بیشتر در این‌باره بحث کنم، اهمیت این نوع اصول موضوع ساختاری را در سازماندهی ریاضیات مسلّم می‌دانم. تازه، باز هم از این نوع اصل موضوعها باید در کار بیاوریم و فکر می‌کنم این نیاز روزمره به اصول موضوع جدید ادامه دارد تا بتوانیم معلوماتمان را به‌صورتی قابل درک، جمع‌وجور کنیم و مبادله کنیم.

حالا، برخلاف اصول موضوع ساختاری ریاضیکاران، وقتی منطقدانی صحبت از اصل موضوع می‌کند، منظورش اولاً قوانین استدلال معتبری است که باید در همهٔ بخشهای ریاضیات قابل اعمال باشد، و ثانیاً اصول موضوعی است برای مفاهیم اولیه مثل عدد، مجموعه و تابع که زیربنای همهٔ مفاهیم ریاضی‌اند. اصول موضوع اخیر را می‌خواهم اصول موضوع بنیادی بنامم. در اینجا وارد این بحث نمی‌شوم که آیا اصلاً ریاضیات نیاز به چنین اصل موضوعهایی دارد یا نه؛ تاریخ تحول ریاضیات جواب این سؤال را می‌دهد. البته این اصل موضوعها با چنان اجزای بنیادی موضوع ما ربط دارند که در کار روزمره [ریاضی] اصلاً لازم نیست حرفشان را بزنیم و خیلی ریاضیدانها ممکن است یک عمر کارشان را بکنند و یک دفعه هم از این اصول حرفی نزنند. اما این به این معنی نیست که در آخر کار برای توجیه عمل نیازی به این اصول نباشد، یا اینکه در هر شرایطی بشود این اصول را نادیده گرفت. در هر حال، من در ادامهٔ بحث، ضرورت اصول موضوع بنیادی را برای ریاضیات مسلم فرض می‌کنم.

من به‌خصوص با دو دستگاه اصل موضوع در دو حد مفهومی کار دارم. اصول موضوع ددکیند-پئانو برای نظریهٔ اعداد، و اصول موضوع تسرملو-فرنکل برای نظریهٔ مجموعه‌ها. فرض می‌کنم با این اصول آشنایی کلی دارید، بنابراین از فرمولبندی دقیق آنها، که به درد بحث ما هم نمی‌خورند، می‌گذرم؛ اما مجبورم در بارهٔ سیر پیدایش و رشد آنها و دلایل قبولشان، چیزهایی بگویم. در هر دو مورد، شروع کار از یک دستگاه «طبیعی» غیرصوری بوده که بعد تبدیل به یک دستگاه صوری به مفهوم دقیق ریاضی شده است.

در اصول موضوع ددکیند [۳] برای اعداد طبیعی $\mathbb{N} = \{0, 1, 2, \ldots\}$، عنصر آغازی ۰ [ددکیند از یک شروع کرد] و عمل تالی $x \to x'(= x + 1)$ پایه‌ای فرض می‌شوند، و اصول موضوع بدیهی عبارت‌اند از اینکه ۰ تالی هیچ عنصری نیست و اینکه تالی یک‌به‌یک است. استقرا به زبان نظریهٔ مجموعه‌ها به این صورت فرمولبندی می‌شود: $\mathbb{N}$ کوچکترین مجموعه است که حاوی عنصر ۰ است و تحت عمل تالی بسته است. اینجا مفهوم غیرصوری مجموعهٔ دلخواه از اعداد طبیعی بدیهی فرض می‌شود و به این ترتیب اصول موضوع، جازم و لذا کامل‌اند. ددکیند اصل استقرا را به‌کار گرفت تا نشان بدهد که می‌توان توابع را با بازگشت ساده روی $\mathbb{N}$ تعریف کرد. در اینجا تعیین می‌کنیم که تابع چگونه در ۰ تعریف می‌شود و نیز چگونه در عنصر تالی x' تعریف می‌شود برحسب اینکه چگونه در x تعریف شده است؛ از این‌کار به‌ویژه در اثبات جازمیت استفاده می‌شود. توابع یک یا چند متغیر مستقل از $\mathbb{N}$ به $\mathbb{N}$ که با تعریفهای صریح و سادهٔ بازگشتی تولید می‌شوند، امروز، توابع بازگشتی اولیه نام گرفته‌اند.

پئانو [۲۴] ابتدا تلاش کرد اصول موضوعی در بارهٔ اینکه کدام مجموعه‌ها وجود دارند (به اصول موضوع ددکیند) اضافه کند. گفت هر خاصیتی مجموعه‌ای تعیین می‌کند، و بعد شرطهای بستاری برای این خاصیتها در نظر گرفت. در اصول موضوع پئانو استقرا معادل این است که بگوییم هر خاصیت اعداد طبیعی که برای صفر برقرار باشد و تحت تالی بسته باشد برای تمام اعداد طبیعی برقرار است.

اگر بپذیریم که مفاهیم مجموعه یا خاصیت نیاز به تحلیل بیشتر ندارند به نظرم اصول موضوع ددکیند-پئانو به معنای آرمانی این واژه در فرهنگ لغت کاملاً نزدیک شده است. اما از دیدگاه ریاضی همهٔ مفاهیمی که در یک دستگاه اصل موضوعی به‌کار می‌روند و همهٔ فرضهای مربوط به آنها باید طور کامل روشن شوند. برای این منظور، یک زبان صوری برای نظریهٔ اعداد تعیین می‌کنیم و تنها آن خواصی از اصل استقرا را که در این زبان با فرمولها درست‌ساخت قابل بیان است اختیار می‌کنیم. دستگاه صوری حاصل امروز حساب پئانو نام دارد و با PA نشان داده می‌شود. در زبان صوری PA، رابطهٔ پایه‌ای‌اش رابطهٔ برابری، =، است باید نمادهایی برای عملیات + و ·، نمادهای ۰ و ′ اضافه کنیم که معادلات تعریفهای بازگشتی آنها اصل موضوع باشد؛ با اینکه + و · در نظریهٔ مجموعه‌ها برحسب این معادلات بنا به نتیجه ددکیند قابل تعریف‌اند، در زبان مرتبهٔ اولی که برای حساب صوری به می‌رود تعریف‌شدنی نیستند. اما گودل نشان داد [۱۰] که وقتی ۰، ′، + ·، را داشته باشیم، همه توابع بازگشتی اولیه در PA قابل تعریف‌اند.

برخلاف اصول موضوع ددکیند-پئانو که منشأ شهودی واضحی دارند اصول موضوع تسرملو از یک نیاز ناشی شدند، نیاز به مبنایی برای کار انقلابی کانتور در زمینهٔ نظریهٔ مجموعه‌ها که به نظر خیلیها اشکال داشت. به‌خصوص اینکه، کانتور از اصل خوش‌ترتیبی (WO) استفادهٔ اساسی کرده بود. مطابق این اصل هر مجموعه‌ای را می‌توان خوش‌ترتیب کرد. کانتور با این اصل احکام مختلفی را در حساب کاردینالی ثابت کرد، به‌خصوص اینکه برای کاردینالهای نامتناهی κ و μ داریم

$$\kappa + \mu = \kappa \cdot \mu = \max(\kappa, \mu) \text{، که } \kappa < 2^{\kappa}$$

به‌علاوه، کانتور با استفاده از WO نشان داد که کاردینالهای نامتناهی

می‌توان با استفاده از اعداد ترتیبی α به‌عنوان اندیس، مرتب کرد:

$$\aleph_0 < \aleph_1 < \aleph_2 < \cdots < \aleph_\alpha < \aleph_{\alpha+1} < \cdots < \aleph_\lambda < \cdots$$

که در آن هر $\aleph_{\alpha+1}$ کوچکترین کاردینالِ بزرگتر از $\aleph_\alpha$ است، و برای λهای حدی $\aleph_\lambda$، حد همهٔ $\aleph_\alpha$هایی است که $\alpha < \lambda$. این درجه‌بندی، همراه با این واقعیت که $\aleph_0 < 2^{\aleph_0}$، بلافاصله ما را به حدسی می‌رساند که معروف به فرضیهٔ پیوستار (CH) است:

$$2^{\aleph_0} = \aleph_1 \qquad \text{(CH)}$$

زیرا $2^{\aleph_0}$ عدد کاردینال پیوستار $\mathbb{R}$ است. توسیع این حدس به همهٔ αها را فرضیهٔ تعمیم‌یافتهٔ پیوستار (GCH) می‌نامیم:

$$2^{\aleph_\alpha} = \aleph_{\alpha+1} \qquad \text{(GCH)}$$

توجیه اصل خوش‌ترتیبی دغدغه‌ای برای کانتور بود. ابتدا ادعا کرد این یک «قانون تفکر» است، بعد سعی کرد آن را بر مبنای اصل واضحتری ثابت کند اما چیز رضایتبخشی پیدا نشد. چنین اصلی را اول بار در سال ۱۹۰۴ تسرملو به صورت اصل موضوع انتخاب (AC) مطرح کرد [۳۱]. تسرملو ثابت کرد AC مستلزم WO است؛ درواقع اینها هم‌ارزند، اما بحث تسرملو این بود که WO به همان شکل AC بدیهی نیست. به دنبال انتشار این اثر نه تنها پذیرش AC بلکه صحت برهان استلزام هم زیر سؤال رفت. برای رفع ایرادهایی که به برهان استلزام گرفته می‌شد، تسرملو در [۳۲] اصول موضوعی مطرح کرد که روشن می‌کرد دقیقاً کدام اصول از مجموعه‌ها را در استدلالش به‌کار گرفته است. این اصول موضوع عبارت‌اند از: هم‌مصداقی، مجموعهٔ تهی، زوجهای نامرتب، مجموعهٔ توانی، بینهایت و تفکیک. اصل موضوع تفکیک می‌گوید برای هر خاصیت معین اشیاء ($P(x)$)، و هر مجموعهٔ مفروض a مجموعه‌ای هم مانند b وجود دارد به‌طوری که $b = \{x : x \in a \& P(x)\}$. این اصل به‌خاطر ابهامی که در تعیین خاصیت معین داشت مورد اعتراض قرار گرفت. چیزی نگذشت که وایل، اسکولم و فرَنکل هر یک جداگانه پیشنهادهای دقیقی مطرح کردند که خاصیتها را محدودتر کنند. همهٔ این پیشنهادها در اصل به این ختم می‌شد که خاصیتهای معین را فقط آن خاصیتهایی به‌شمار آوریم که در زبان صوری نظریهٔ مجموعه‌ها با نمادهای پایه‌ای $=$ و $\in$ بیان می‌شوند. اصلاح دیگر به خاطر این بود که مطابق اصول تسرملو نمی‌شد وجود $\aleph_\alpha$ را برای αی نامتناهی اثبات کرد؛ فرَنکل اصل موضوع جایگذاری را به این اصول اضافه کرد. اصول موضوع تسرملو فرَنکل به عنوان یک دستگاه صوری را با ZF نشان می‌دهیم، و اگر AC را به آن اضافه کنیم ZFC خوانده می‌شود. اینجا نکتهٔ کوچک قابل توجه این است که طبق اصول تسرملو وجود «عنصر اولیه»[1] ممکن بود، یعنی وجود اشیایی (غیر از مجموعهٔ تهی) که هیچ عنصری نداشته باشند. در ZF از این اشیا صرف‌نظر شده چون برای مبانی نظریهٔ مجموعه‌ها ضروری نیستند.

بعد از این اصلاحات، آنچه بی‌پاسخ ماند این بود که اصول موضوع تسرملو-فرَنکل دقیقاً اصل موضوع چه چیزی هستند. اگر اینها را اصل موضوع به معنای آرمانی فرهنگ لغت بگیریم باید برای مفهومی که پیش از وضع این اصول در ذهن خود داریم بدیهی باشند. مفهوم مجموعهٔ دلخواه ــ بدون هیچ قیدی روی آن ــ که در اولین وهله می‌توانست نامزدی برای پاسخ این مسأله باشد قابل قبول نیست، چون ظاهراً یک مشخصهٔ بدیهی این مفهوم این است که برای هر خاصیت $P(x)$ مجموعهٔ تمام xهایی که در P صدق کنند وجود دارد. اما می‌دانیم که این به تناقضهایی کشید که ساده‌ترینشان را راسل با خاصیت: $\neg(x \in x)$ بیان کرد ($\neg$ علامت نقیض است). و دقیقاً همین نوع تناقض است که اصل موضوع تفکیک تسرملو جلویش را می‌گیرد، چون خاصیت P را فقط بر اعضای یک مجموعهٔ «از قبل موجود» [مفروض] a اعمال می‌کند. این مفهوم تناقض‌دار از مجموعه، و نه کلیتر از آن، چه توجیهی دارد؟ جوابی که اول بار تسرملو در سال ۱۹۳۰ داد [۳۳] برحسب چیزی بود که سلسله مراتب تجمعی مجموعه‌ها نام گرفت. در این تصویر، مجموعه‌ها از پایین به بالا طبقه‌طبقه بنا می‌شوند. شروع از پایینترین مرحله با عناصر اولیه است. چون امروزه از آنها صرف‌نظر کرده‌ایم، از مجموعهٔ تهی شروع می‌کنیم که معمولاً با ۰ نشان داده می‌شود. در هر مرحله، تمام مجموعه‌هایی را که در طبقهٔ قبلی به‌دست آمده‌اند در یک تک‌مجموعهٔ a جمع می‌کنیم. در مرحلهٔ بعدی همهٔ اعضای مجموعهٔ توانی $\mathcal{P}(a)$، یعنی مجموعهٔ همهٔ زیرمجموعه‌های a به هم ملحق می‌شوند. سرانجام، این فرایند به صورت ترامتناهی تکرار می‌شود. اما برای درک این مدل توجه به مفاهیم زیر در نظریهٔ مجموعه‌ها لازم است: مرحله‌ها با اعداد ترتیبی مشخص می‌شوند. مجموعهٔ (یا عالم جزئیِ) اشیایی که در مرحلهٔ α به‌دست آمده‌اند با V_α مشخص می‌شود.

$$V_0 = 0$$

$$V_{\alpha+1} = V_\alpha \cup \mathcal{P}(V_\alpha)$$

$$V_\lambda = \{V_\alpha : \alpha < \lambda\} \text{ اجتماع}$$

برای عددهای ترتیبی حدی λ

امروزه دست‌اندرکاران نظریهٔ مجموعه‌ها ادعا می‌کنند که اصول موضوع ZFC برای عالم V از مجموعه‌های شامل همهٔ اشیای یک V_α، بدیهی‌اند. اما درک شهودی این با شهودی که منجر به قبول اصول موضوع ددکیند-پئانو شد، زمین تا آسمان فرق می‌کند. گذشته از چیزهای دیگر، آنچه اینجا محرز فرض می‌شود مفهوم عینی زیرمجموعهٔ دلخواه از یک مجموعه مفروض است. این تصور افلاطونی از ریاضیات است که در مورد نظریهٔ مجموعه‌ها به‌کار گرفته شود و از لحاظ فلسفی محل جدل است؛ در این‌باره بعداً بیشتر صحبت خواهیم کرد.

حالا برگردیم به سرچشمه‌های برنامهٔ گودل برای یافتن اصول موضوع جدید در مقاله‌ای که به سال ۱۹۳۱ در بارهٔ ناتمامیت برای دستگاههای صوری حساب نوشت [۱۰]. می‌خواهم به اختصار این نتایج را یادآوری کنم ولی برای بیان آنها به مفاهیمی نیاز داریم که کمی تخصصی‌اند. ساده‌ترین گزاره‌ها در نظریهٔ اعداد به صورت عمومی محض $(\forall x) f(x) = 0$ و به صورت وجودی محض $(\exists x) f(x) = 0$اند که در اینجا f یک تابع بازگشتی اولیه است. این گزاره‌ها تحت عمل نفی، صورتهای دوگان‌اند یعنی $\neg(\forall x) f(x) = 0$ معادل است با $(\exists x) g(x) = 0$ که در آن $g(x)$ صفر است اگر $f(x) \neq 0$ و یک است، اگر $f(x) = 0$. دستگاه صوری S که زبان آن شامل PA است برای ردهٔ K از گزاره‌ها صحیح است اگر بتوانیم بگوییم هرگاه $S \vdash \phi$

1. urelement

است برای ردهٔ K از گزاره‌ها صحیح است اگر بتوانیم بگوییم هرگاه $S \vdash \phi$ (S نتیجه می‌دهد ϕ) و $\phi \in K$، آنگاه ϕ در اعداد طبیعی صادق است. به‌سادگی می‌توان نشان داد که اگر S سازگار باشد و شامل PA (یا حتی پارهٔ ضعیفتری از آن) باشد برای گزاره‌های عمومی (محض) صحیح است اما (همان‌طور که گودل نشان داد) برای گزاره‌های وجودی الزاماً این‌طور نیست. S را ۱ـسازگار می‌گوییم تنها در صورتی‌که برای گزاره‌های وجودی صحیح باشد. توجه داشته باشید که ۱ـسازگاری، سازگاری را نتیجه می‌دهد. (خود گودل از مفهومی کمی قویتر به نام ω‌ـسازگاری استفاده کرد.)

دستگاه S از لحاظ صوری کامل است اگر برای هر فرمول بستهٔ ϕ، یا $S \vdash \phi$ یا $S \vdash \neg\phi$. هیلبرت دو حدس اصلی در بارهٔ PA داشت: اینکه سازگاری PA به‌صورت متناهی‌وار[1] اثبات‌پذیر است و اینکه PA از لحاظ صوری کامل است. هر دو حدس با قضایای ناتمامیت سال ۱۹۳۱ گودل نفی شد [۱۰]. به‌علاوه این قضایا بر دستگاههای صوری Sای که (به طرز کارایی عرضه شده باشند و) PA را به‌صورت بسیار کلیتری بسط بدهند قابل اعمال هستند. گودل به هر چنین دستگاهی یک گزارهٔ عمومی محض θ_S نسبت داد، که خود این گزاره، از طریق عدد گودلِ خودش، نشان می‌داد که در S اثبات‌پذیر نیست. قضیهٔ اول ناتمامیت گودل دو بخش دارد. بخش اول به ما می‌گوید اگر S سازگار باشد آنگاه θ_S واقعاً در S اثبات‌پذیر نیست، پس بنا به ساخت خودش صادق است. بخش دوم می‌گوید اگر S، ۱ـسازگار باشد آنگاه $\neg\theta_S$ هم در S اثبات‌پذیر نیست. چون در غیر این صورت، $\neg\theta_S$، که معادل یک گزارهٔ وجودی است، اگر در S اثبات‌پذیر باشد، باید صادق باشد، و این خلاف بخش اول است. قضیهٔ دوم ناتمامیت گودل به ما می‌گوید که گزارهٔ نظریهٔ اعدادیِ $\mathrm{Con}(S)$ که مبین سازگاری S است، اگر S سازگار باشد در S اثبات‌پذیر نیست. این امر از صورتبندی برهان بخش اول قضیهٔ اول حاصل می‌شود. به این دلیل اگر S دستگاهی باشد که در آن همهٔ استدلالهای متناهی‌وار قابل صورتبندی باشند، آنگاه برنامهٔ کلی سازگاری متناهی‌وار هیلبرت برای S انجام‌پذیر نیست. حالا عموماً پذیرفته‌اند که تمام استدلال متناهی‌وار، اگر نه در دستگاههای بسیار ضعیفتر، ولی در PA قابل صورتبندی است، و اینجاست که برنامهٔ سازگاری متناهی‌وار هیلبرت محدودیتهایش را دارد.

نه تنها نتایج گودل، بلکه توضیح خود او در مورد علت اعتبار آنها هم تکان‌دهنده بود. این توضیح در پانوشتی آمده که ظاهراً به‌عنوان بعدالتحریر در مقالهٔ [۱۰] گنجانده شده است، چون شماره‌اش ۴۸ª است. اما بیانگر اعتقادی اساسی است که بعدها در سراسر زندگی گودل تکرار شد، و همین اعتقاد است که ما را به اصل سؤال این مقاله می‌رساند. قراینی وجود دارد که به نظر او چنین دیدگاهی برای مکتب هیلبرت غیرقابل قبول بوده، و او از هرگونه اظهار نظری از این قبیل پرهیز داشته است. در پانوشت آمده:

> ... دلیل واقعی ناتمامیت ذاتیِ همهٔ دستگاههای صوری ریاضیات این است که تشکیل انواع هر چه بالاتر را می‌توان به صورت نامتناهی ادامه داد ... [چون] گزاره‌های تصمیم‌ناپذیری که اینجا ساخته می‌شوند، با اضافه‌شدن انواعِ بالاترِ مناسب، تصمیم‌پذیر می‌شوند [۱۰، صفحهٔ ۱۹۱].

1. finitarily

اما، ارتباط ناتمامیت و نظریهٔ مجموعه‌ها اینجا توضیح داده نمی‌شود؛ دلیل ناگفته‌اش این است که سازگاری دستگاه S در دستگاهی قابل اثبات است که دامنهٔ متغیرهای مجموعه‌هایش، زیرمجموعه‌های دلخواه عالم مقالِ S است، که به‌وسیلهٔ آنها می‌توان یک تعریف صدق برای زبان S عرضه کرد. تا اواسط دههٔ ۱۹۴۰ چیزی مثل پانوشت ۴۸ª از گودل شنیده نشد. در این موقع گودل در مؤسسهٔ مطالعات پیشرفتهٔ پرینستن جای محکمی داشت، هیلبرت هم مرده بود و رفته بود پی کارش.

در این فاصله، گودل در [۱۱] دومین حکم انقلابیش را ثابت کرده بود: اگر ZF سازگار باشد با اضافه کردن AC و GCH سازگار می‌ماند. روش گودل برای اثبات این ادعا ایجاد یک سلسله مراتب تجمعی جدید به‌عنوان مدلی از نظریهٔ مجموعه‌ها بود که از لحاظ صوری داخل نظریهٔ مجموعه‌ها تعریف می‌شود، به این صورت که در هر مرحله مجموعه‌های ارائه شده منحصر می‌شود به همهٔ زیرمجموعه‌هایی از مرحلهٔ قبلی که در زبان نظریهٔ مجموعه‌ها برای آن مرحله تعریف‌پذیر باشند. مجموعه‌های ساخته‌شده به این طریق، در مرحلهٔ α با L_α نشان داده می‌شوند و تعریفشان دقیقاً مثل مجموعه‌های V_α است، بجز اینکه در مراحل تالی فرض می‌کنیم

$$L_{\alpha+1} = L_\alpha \cup Def(L_\alpha)$$

که $Def(a)$ برای هر مجموعهٔ a مجموعهٔ تمام زیرمجموعه‌های تعریف‌پذیر b از مجموعهٔ a است. گودل مجموعه‌ای را ساختپذیر خواند که متعلق به یک L_α باشد؛ آنگاه L برای گردایهٔ همهٔ مجموعه‌های ساختپذیر به‌کار می‌رود. اصل موضوع ساختپذیری می‌گوید همهٔ مجموعه‌ها ساختپذیرند، و به‌صورت $V = L$ نشان داده می‌شود. از این «اصل موضوع» به‌عنوان واسطهٔ مناسبی در برهان سازگاری نسبی گودل به‌صورت زیر استفاده می‌شود:

۱. اگر ZF سازگار باشد آنگاه $\mathrm{ZF} + V = L$ سازگار است.

۲. $\mathrm{ZF} + V = L \vdash \mathrm{AC\&GCH}$.

از جاگذاری صوری $V = L$ در ۱ و ۲ که بگذریم، این گزاره را به چه معنا می‌توانیم یک اصل موضوع قابل قبول برای نظریهٔ مجموعه‌ها بدانیم؟ گودل در زمان ارائهٔ برهانش (حدود ۱۹۳۸) اظهار داشت این اصل موضوع نوعی مکمل طبیعی برای اصول موضوع نظریهٔ مجموعه‌هاست، چون دقیقاً مشخص می‌کند از کدام مجموعه‌ها داریم صحبت می‌کنیم ــ کاری که ZF نمی‌کند. اما در دههٔ بعد، گودل با دیدگاهی به‌شدت افلاطونی در مورد اینکه نظریهٔ مجموعه‌ها باید در بارهٔ چه چیزی باشد، صریحاً اصل موضوع بودن $V = L$ را رد می‌کرد. این موضع اولین بار در مقاله‌ای در باب منطق ریاضی راسل در سال ۱۹۴۴ عنوان شد، اما در مقالهٔ سال ۱۹۴۷ گودل بود که با صراحت و با اشارهٔ به‌خصوص به مسائل حل‌نشدهٔ نظریهٔ مجموعه‌ها مطرح شد. این مقاله با عنوان «مسأله پیوستار کانتور چیست؟» [۱۲] شامل نکات زیر بود:

> ۱. نظریهٔ مجموعه‌ها در بارهٔ عالمی چون V از اشیایی است که مستقل از افکار و تعبیرات بشر وجود دارند. این عالم تشکیل می‌شود از نتیجهٔ تکرار نامتناهی عمل مجموعهٔ توانیِ پر، یعنی عمل تشکیل مجموعهٔ زیرمجموعه‌های دلخواهِ هر مجموعهٔ مفروض. (بنابراین، هیچ دلیلی ندارد که قبول کنیم $V = L$، که می‌گوید همهٔ مجموعه‌ها با تعریفهای متوالی به‌دست می‌آیند.)

۲. گزاره‌های نظریهٔ مجموعه‌ها ارزش صدق معینی (در V) دارند. به‌ویژه، همهٔ اصول موضوع ZFC در V صادق‌اند.
۳. بنابراین CH نیز ارزش صدق معینی دارد. مطابق بحث گودل در [۱۲]، CH احتمالاً کاذب است.
۴. بنابراین CH باید مستقل از ZFC باشد. (درواقع پال کوهن بالاخره در سال ۱۹۶۳ این را ثابت کرد [۲].)
۵. و به این ترتیب برای تعیین وضعیت $\aleph_\omega$ از $2^{\aleph_\omega}$ در درجه‌بندی الف‌ها، [بی‌تردید] نیاز به افزودن اصول موضوع جدیدی به ZFC داریم.
۶. این اصول موضوع جدید را می‌شود با توسیع مستقیم همان استدلالهای غیرصوری که منجر به پذیرش ZFC شد، فرمولبندی کرد و پذیرفت. به عبارت دقیقتر: ساده‌ترین اینها [اصول موضوع جدید] ... بیان‌کنندهٔ وجود اعداد [قویاً] دست‌نیافتنی بزرگتر از $\aleph_0$ است. [این] اصل موضوع، به بیان ساده، چیزی جز این نیست که کلیهٔ مجموعه‌هایی که فقط با استفاده از فرایندهای ساخت مجموعه‌ها، مذکور در اصول موضوع دیگر، به‌دست می‌آیند، خودشان دوباره یک مجموعه تشکیل می‌دهند (و، بنابراین مبنای جدیدی برای کاربرد دوبارهٔ این فرایندها می‌شوند.) اصول موضوع دیگر بینهایت را پ. مالو فرمولبندی کرده است ... این اصول به‌وضوح نشان می‌دهند که نه تنها دستگاه اصل موضوعی نظریهٔ مجموعه‌ها به‌صورتی که امروز می‌شناسیم، ناتمام است، بلکه می‌توان این دستگاه را بدون هیچ‌گونه دلبخواهی بودنی با اصول موضوع جدیدی که تنها ادامهٔ طبیعی اصول موضوع فعلی‌اند، تقویت کرد. [۱۲، صفحهٔ ۵۲۰].

یک کاردینال ناشمارا (قویاً) دست‌نیافتنی است اگر تحت به توان رساندن و حدود کاردینالهای کوچکتر بسته باشد. در نتیجه اگر κ دست‌نیافتنی باشد آنگاه V_κ مدلی از اصول موضوع ZFC است. پس اگر فرض کنیم که کاردینالی دست‌نیافتنی وجود دارد، آنگاه یک نتیجهٔ منطقی عبارت است از سازگاری ZFC، Con(ZFC)، و بنابراین، طبق قضیهٔ دوم ناتمامیت گودل این نتیجه در ZFC اثبات‌پذیر نیست (اگر ZFC سازگار باشد). به همین ترتیب اگر فرض کنیم تعداد معینی کاردینال دست‌نیافتنی وجود دارد، نمی‌توانیم وجود کاردینالهای دست‌نیافتنی بزرگتر را اثبات کنیم. اصول موضوع مالو ابتدا وجود دست‌نیافتنی‌های به دلخواه بزرگ را بیان می‌کند و آنگاه وجود نقطه‌های ثابتِ دست‌نیافتنیِ به دلخواه بزرگِ شمارش دست‌نیافتنی‌ها را، و ... که به صورت ترامتناهی تکرار می‌شوند. یک راه غیرصوری برای توجیه وجود آنها، و درواقع به طور کلی برای توجیه وجود کاردینالهای نامتناهی، با ارجاع به «امر مطلق کانتور» است: عالم همهٔ مجموعه‌ها فراتر از دسترسی با هر شرط بستاری روی مجموعه‌هاست؛ بلکه، هر چنین شرطی همیشه به یک مجموعه می‌انجامد. به عبارت روشنتر، هر خاصیت بستاری P که عالم همهٔ مجموعه‌ها یعنی V در آن صدق کند، κی به دلخواه بزرگی وجود خواهد داشت که به‌ازای آن V_κ، در P صدق کند: روایت صوری این مطلب که از ریل لوی [۲۰] و پاول برنایس [۱] ارائه کردند در نظریهٔ مجموعه‌ها اصول بازتاب نام دارد. اینها پشتوانهٔ ادعای گودل برای نیاز به اصول موضوع جدیدند، اصول موضوعی از نوع مالو، «بدون دلبخواهی بودن» و به صورت «ادامهٔ طبیعی» آن اصول موضوعی که از قبل پذیرفته‌ایم. اما ادامهٔ صحبت او چنین است [از نقل قول قبلی]

> [اینجا هم] مثل مسألهٔ پیوستار، زیاد امیدی نیست که مشکل را با آن اصول موضوع بینهایت، که بر مبنای قواعدی که امروز می‌شناسیم ساخته می‌شوند، بشود حل کرد ... [همان.]

دلیلش این است که اصول موضوع مالو با $V = L$ سازگارند، و چون GCH در L صادق است و گودل معتقد بود CH کاذب است، کذب آن از این طریق قابل اثبات نبود. گودل ادامه می‌دهد،

> علی‌رغم این ... احتمالاً [اصول موضوع] دیگری وجود دارند که مبتنی بر اصولی‌اند که تاکنون آنها را نشناخته‌ایم ... اصول موضوعی که درک عمیقتر مفاهیم زیربنایی ریاضیات و منطق ما را به تشخیص آنها، آن‌طور که این مفاهیم مستلزمشان هستند، قادر می‌کند. [همان.]

در واقع مثالی از نوع بزرگتر کاردینال را مدتی قبل از آن، در سال ۱۹۳۰، استانیسلاو اولام پیشنهاد کرده بود. اولام کاردینال شمارای κ را اندازه‌پذیر خواند اگر یک اندازهٔ دوارزشی κ-جمعی روی $P(\kappa)$ وجود داشته باشد. قدر این پیشنهاد تا سال ۱۹۶۱ ناشناخته ماند. در آن زمان دِینا اسکات در [۲۵] ثابت کرد که وجود کاردینالهای اندازه‌پذیر (MC) ایجاب می‌کند که $V \neq L$، بنابراین MC از آن پس راه نجاتی برای حل‌وفصل CH شد. چند سال بعد آلفرد تارسکی همراه شاگردانش ویلیام هانف و اچ. جروم کیسلر در [۱۶] و [۱۹] ثابت کردند که اگر κ یک کاردینال اندازه‌پذیر باشد، بسیار بزرگ، است، چون V_κ در اصول موضوع نوع مالو و دیگر اصول موضوع قدرتمند بینهایت صدق می‌کند. این امر منجر به مفهوم کاردینال قویاً فشرده شد که وجود آن، وجود کاردینالهای اندازه‌پذیر را ایجاب می‌کند. اما بعد تارسکی و گودل هر دو در فرض وجود چنین کاردینالهای عظیمی مردد شدند. تارسکی می‌گوید:

> اعتقاد به وجود کاردینالهای دست‌نیافتنی ... (و حتی کاردینالهای به دلخواه بزرگی از این دست) ظاهراً نتیجهٔ طبیعی دریافتهای شهودی اساسی است که مبنای نظریهٔ «طبیعی» مجموعه‌ها را تشکیل می‌دهد، و دلالت دارد بر آنچه که «امر مطلق کانتور» می‌توان نامید. برعکس، در حال حاضر هیچ دلیل شهودی محکمی نمی‌بینیم که ما را در مورد وجود کاردینالها[ی قویاً فشرده] متقاعد کند، یا لااقل این را کاملاً موجه کند که فرضهای حاکی از وجود چنین کاردینالهایی با اصول موضوع آشنای نظریهٔ مجموعه‌ها سازگار است [۲۷، صفحهٔ ۱۳۴].

گودل در تجدیدنظری که سال ۱۹۶۴ بر مقالهٔ سال ۱۹۴۷ خود داشت [۱۳]، این دیدگاه تارسکی را کاملاً تأیید می‌کند، ولی بعد اضافه می‌کند:

> اما [اصول موضوع جدید] با استدلال قویتر شباهت تقویت می‌شوند ... ([۱۳، صفحهٔ ۲۶۴. پانوشت ۲۰]، تأکید از من است)

به علاوه گودل در سال ۱۹۴۷ استدلال نوع دیگری مطرح کرده بود که می‌توانست منجر به قبول بعضی گزاره‌ها به‌عنوان اصل موضوع جدید بشود، حتی اگر این گزاره‌ها متکی به همان نوع شواهدی نباشند که منجر به قبول ZFC در وهلهٔ اول شد. یعنی:

> [سرانجام، باید به دنبال اصول موضوعی باشیم که] آن‌قدر نتایج منطقی قابل اثبات به‌بار بیاورند ... که صرف‌نظر از ضرورت ذاتی‌شان

مجبور به فرض وجود آنها باشیم، همان کاری که با یک نظریهٔ فیزیکی جاافتاده می‌کنیم. ([۱۲]، ص ۵۲۱]، تأکید از من است)

اصول موضوع بالاتر بینهایت، یا به اصطلاح «کاردینالهای بزرگ» در نظریهٔ مجموعه‌ها از دههٔ ۱۹۶۰ به بعد موضوع پژوهشهای عمیقی شده است و کاردینالهای جدید بسیاری با خواص ویژهٔ نظریهٔ مجموعه‌ای در این مطالعات به‌دست آمده‌اند[۱]. در کتاب اخیر اکی کاناموری، بینهایت بالاتر [۱۷، ص ۴۷۱] و مقالهٔ توضیحی قبلی کاناموری و مناخیم مگی‌دور [۱۸]، شبکهٔ پیچیده‌ای از روابط به استناد جدولها درج شده است. بین کاردینالهای بزرگِ «کوچک» و کاردینالهای بزرگِ «بزرگ»، بسته به اینکه، با یک معیار منطقی، ضعیفتر یا قویتر از کاردینالهای اندازه‌پذیر باشند، تفاوت نه چندان دقیقی قائل شده‌اند. آن عده از دست‌اندرکاران نظریه مجموعه‌ها که در این تحول دست دارند سعی کرده‌اند توجیهاتی برای تأیید هر دو نوع این کاردینالها پیدا کنند. پنه‌لوپ مدی، فیلسوف، در دو مقالهٔ جالب با عنوان «ایمان به اصول موضوع»، استدلالهای مختلف برای این اصول موضوع و انواع دیگر اصلهای موضوع قوی را تحلیل کرده و شواهد موجود برای آنها را خلاصه کرده است [۲۱]. در حالت کلی، استدلالها یا مبتنی بر دلایل درونی‌اند یا دلایل بیرونی. قواعد بازتابی که قبلاً گفتیم نمونه‌هایی از دلایل درونی‌اند اما این دلایل ما را از کاردینالهای بزرگ «کوچک» جلوتر نمی‌برند. از دلایل بیرونی برای بالاتر رفتن، این است که فرض کاردینالهای بزرگ «بزرگ» ــ چنان‌که در پژوهشهای خیره‌کنندهٔ سالووی، مارتین، فورمن، مگی‌دور، شلاه، استیل، وودین و دیگران آمده است ــ در گسترش خواص «استاندارد» بورل و زیرمجموعه‌های تحلیلی پیوستار، مثل اندازه‌پذیری لبگ، خاصیت بئر، خاصیت زیرمجموعهٔ تام، معین‌بودن بازیهای نامتناهی وابسته، و غیره، به رده‌های بسیار بزرگتر، نتیجه‌بخش بوده است.

اما علی‌رغم همهٔ این پیشرفتها، نکتهٔ تکان‌دهنده این است که برخلاف امیدهای گودل، با وجود اضافه شدن این اصول موضوع، فرضیهٔ پیوستار همچنان بلاتکلیف مانده است، چون معلوم شده است که مستقل از همهٔ اصول موضوع «به‌زور حق به جانب» بینهایت، ازجمله MC، است که تا به حال در نظر گرفته‌ایم (به فرض سازگاربودن آنها)[۲]. حالا ممکن است نه تنها به برنامهٔ گودل بلکه به خودِ پیش‌فرضهایش هم شک کنیم. آیا CH آن‌طور که گودل و بسیاری نظریه‌مجموعه‌دانهای اخیر اعتقاد دارند یک مسألهٔ معین است؟ اصلاً خودِ پیوستار یک موجود ریاضی معین است؟ اگر پیوستار فقط وجود افلاطونی دارد، چطور می‌توانیم به خاصیتهایش دست پیدا کنیم؟ به همین منوال، ممکن است مدعی باشیم که پیوستار در فضا و/یا در زمان وجودِ فیزیکی دارد. اما آن‌وقت می‌شود پرسید آیا ساختار ریاضی دستگاه اعداد حقیقی را می‌توان با ساختار فیزیکی یکی گرفت، یا اینکه ساختار ریاضی صرفاً یک مدل ریاضی آرمانی از ساختار فیزیکی است، همان‌طور که قوانین فیزیکی فرمولبندی‌شده به زبان ریاضی، مدلهای بسیار آرمانی از نمودهای واقعیت فیزیکی‌اند. (هرمان وایل در رسالهٔ سال ۱۹۱۸اش با عنوان پیوستار[۱] دقیقاً چنین سؤالهایی را مطرح کرد [۲۹].) اما حتی اگر نوعی وجود مستقل، انتزاعی یا فیزیکی، هم برای پیوستار قائل شویم، برای فرمولبندی CH باید به زیرمجموعه‌های دلخواهی از پیوستار و نگاشتهای ممکن بین آنها رجوع کنیم، و آن‌وقت سروکارمان با اشیایی یک پله انتزاعی‌تر است که ماهیت وجودشان حتی بیشتر از خود پیوستار مسأله‌ساز است. دیگر داریم گرفتار بحر عمیق تفکر فلسفی می‌شویم. عجالتاً کمی کنار بکشیم.

در حالی که برنامهٔ گودل برای پیداکردن اصول موضوع جدیدی که تکلیف CH را روشن کند عملی نشده است، در بارهٔ سرچشمه‌های برنامهٔ او در قضایای ناتمامیت برای نظریهٔ اعداد چه می‌توان گفت؟ همان‌طور که دیدیم گودل یک عمر معتقد بود ما به اصول موضوع جدید هر چه قویتری در نظریهٔ مجموعه‌ها نیاز داریم تا مسائل حل‌نشدهٔ حساب، حتی ساده‌ترین و کلیترین نوعشان را ــ که او مسائل نوع گلدباخ می‌نامید ــ حل‌وفصل کنیم. واقعاً هم حدس گلدباخ را می‌شود به این صورت نوشت. اما قضیهٔ ناتمامیت به خودی خود هیچ گواهی بر این نیست که مسائل حل‌نشدهٔ حساب ــ یا معادل آن، مسائل ترکیبیاتی متناهی ــ که اهمیت ریاضی دارند ــ نیاز به چنین اصول موضوع جدیدی داشته باشند. بر اهمیت ریاضی تأکید می‌کنم چون مثالهای خودِ گودل از گزاره‌های تصمیم‌ناپذیر برای هر S سازگار شامل PA دو نوع بودند: یکی θ_S که با ساخت قطری برپا می‌شود تا ناتمامیت را ثابت کند، و طبق همان قضیه‌ای که برای اثباتش به‌کار می‌رود، صادق است، و دیگری، $\mathrm{Con}(S)$ که قطعاً اهمیت ریاضی دارد، اما نه به معنای معمولی کلمه. در اواسط دههٔ ۱۹۷۰، منطقدانان تلاشی برای اصلاح این وضعیت شروع کردند. آنها گزاره‌هایی ترکیبیاتی متناهی، با اهمیت ریاضی آشکار ارائه کردند که مستقل از چنین Sهایی بودند. اولین نمونه را جف پاریس و لئو هرینگتون ارائه کردند. آنها در [۲۳] نشان دادند که یک صورت اصلاح‌شده (PH) از قضیهٔ رمزی متناهی در بارهٔ وجود مجموعه‌های همگن برای بعضی انواع افرازها در PA قابل اثبات نیست. PH به‌عنوان یک نتیجهٔ سادهٔ قضیهٔ نامتناهی رمزی، صادق شناخته می‌شود؛ استقلال آن منوط به نشان‌دادن این است که PH، $\mathrm{Con}(\mathrm{PA})$ را نتیجه می‌دهد؛ درواقع PH معادل است با $1-\mathrm{Con}(\mathrm{PA})$. چند سال بعد؛ هاروی فریدمن، کن مک‌آلون، و استیون سیمپسن، با ارتقا به یک دستگاه بالاتر، یک نوع ترکیبیاتی متناهی (FGP) از قضیهٔ گالوین-پریکری[۲] (GP) ارائه کردند که مستقل از دستگاه تحلیل محمولی ففرمن-شوته بود (در اینجا آن را FS می‌نامیم)[۳]. اتفاقاً خود GP صورت بسیار قویتر قضیهٔ رمزی نامتناهی است و FGP شباهتهای معینی با PH دارد. باز هم ثابت می‌شود که این‌گونهٔ متناهی‌وار FGP به‌عنوان یک نتیجهٔ سادهٔ GP صادق

۱. این مبحث چنان گسترش یافته است که برای نامیدن مفاهیم مختلف کاردینالهای بزرگ با کمبود اصطلاح مواجه شده‌اند. نمونه‌های آن (تقریباً به ترتیب افزایش قدرت) عبارت‌اند از: «دست‌نیافتنی»، «مالو»، «فشردهٔ ضعیف»، «وصف‌ناشدنی»، «ظریف»، «بیان‌نشدنی»، «رمزی»، «اندازه‌پذیر»، «قوی»، «وودین»، «ابرقوی»، «قویاً فشرده»، «ابرفشرده»، «تقریباً عظیم»، «عظیم» و «ابرعظیم».

۲. مقایسه کنید با مارتین [۲۲]؛ وضعیتی که در آنجا در سال ۱۹۷۶ گزارش می‌شود تا امروز تغییری نکرده است.

1. *Das Kontinuum* 2. Galvin-Prikry

۳. فریدمن، مک‌آلون و سیمپسن با یک دستگاه ATR. کار کردند که نشان داده شده است از لحاظ نظریهٔ برهان، هم‌ارز با دستگاه FS از آنالیز انشعابی تا عدد ترتیبی Γ_0 است. فریدمن بعداً گونه‌ای متناهی از قضیهٔ کروسکال (KT) پیدا کرد که مستقل از ATR. بود. قضیهٔ نامتناهی‌وار KT، که محور اساسی ترکیبیات نظریهٔ گرافی است، خوش‌شبه‌ترتیبی رابطهٔ قابلیت نشاندن بین درختهای متناهی را بیان می‌کند. کار فریدمن در این باره در [۲۶] گزارش شده است.

است، در حالی‌که استقلال آن مبتنی بر نشان‌دادن این است که از FGP می‌توان Con(FS) را نتیجه گرفت؛ درواقع FGP معادل ۱ـسازگاری آنالیز محمولی است. نتایج دیگری از این دست، برای دستگاههای آنالیز باز هم قویتر توسط این پژوهشگران و دیگران به‌دست آمده‌اند[۱]. در حالی‌که در هر مورد نشان داده می‌شود گزارهٔ ϕ مستقل از S معادل با ۱ـسازگاری آن است، اقامهٔ دلیل برای صدق ϕ از طریق استدلال معمولی ریاضی است.

چند سالی فریدمن سعی داشت با ارائهٔ گزاره‌های ϕی ترکیبیاتی متناهی واضح از نظر ریاضی، که اثبات آنها مستلزم وجود چندین اصل موضوع مالو یا حتی اصل موضوعهای قویتر بینهایت بود، از این جلوتر برود، و مصادیقی هم برای این پیدا کرد ([۷] حاوی جدیدترین کار در این زمینه است). از لحاظ فراریاضیات این نوع نتیجه همان خصوصیت کار قبلی را دارد؛ یعنی، برای بعضی دستگاههای بسیار قوی S در نظریهٔ مجموعه‌ها، ϕ هم‌ارز با ۱ـسازگاری S است. اما نتیجهٔ حاصل به روشنی نتیجهٔ کار قبلی نیست چون صدق ϕ حالا یک نتیجهٔ حاصل از استدلال معمولی ریاضی نیست، بلکه اساساً بستگی به قبول $\mathrm{Con}(S)$ـ۱ دارد. اینکه ادعا کنیم به این دلیل ما نیاز به اصول موضوعی در بارهٔ کاردیناله‌های بزرگ برای اثبات صدق ϕ داریم، نوعی مصادره به مطلوب است، چون تنها دلیل ما برای قبول این صدق در اعتقاد به ۱ـسازگاری آن اصول موضوع نهفته است. هر قدر هم به نظر ما موجه باشد، شاید با ساختن تصویری از مدلهای چنین اصول موضوعی، باز هم دلیل نمی‌شود خود آن اصول موضوع را به‌عنوان اصلهای درجهٔ اول ریاضی قبول کنیم. بالاخره باید به این واقعیت توجه داشت که تا به حال، هیچ مسأله فرمولبندی‌شدهٔ حل‌نشده‌ای در نظریهٔ اعداد یا ترکیبیات متناهی، مثل حدس گلدباخ یا فرض ریمان یا حدس عددهای اول دوقلو، یا مسأله $P = NP$، دیده نشده که مستقل از انواع دستگاههای صوری مورد بحث ما، یا حتی مستقل از PA باشد. اگر چنین چیزی به صورتی که در مثالهای بالا آوردیم (PH، FGP و غیره) اثبات شود، آنگاه صدق آنها هم در همان حال اثبات می‌شود. به نظر من احتمالاً همان‌طور که در مورد «قضیهٔ آخرفرما» نشان داده شد، سرانجام اثبات صدق اینها ــ اگر شدنی باشد ــ از طریق استدلالهای معمولی ریاضیاتی بدون هیچ گذاری به فراریاضیات انجام خواهد گرفت، و تنها بعد از آن است که ممکن است ببینیم دقیقاً کدام قواعد اصل موضوعی اساسی برای اثبات آنها لازم است.

اگر از حوزهٔ حساب و ترکیبیات متناهی فراتر برویم، چه دلیلی دارد که برای ریاضیات روزمره محتاج اصول موضوع جدیدی باشیم؟ بدون شک درست است که نشان داده‌اند قسمتهای مختلف نظریهٔ توصیفی مجموعه‌ها نیاز به اصول موضوع بینهایت [مراتب] بالاتر دارند و در بعضی موارد بسیار فراتر از حوزهٔ مقادیر کاردیناله‌های بزرگ «کوچک». اما این هم نوعی مصادره به مطلوب است، چون باور ما به صدق این نتایج جدید اساساً بستگی به

۱. دستگاههای مورد بحث و گزاره‌های مستقل مربوط به آنها توضیح پیچیده‌تری می‌طلبند که از حوصلهٔ این مقاله خارج است، اما اقلاً یک نتیجه در ارتباط با پانوشت قبلی به نشان‌دادنش می‌ارزد. فریدمن یک گونهٔ بسط‌یافتهٔ EKT از KT پیدا کرد که مستقل از اصل تصریح $\prod^1_1$ غیرحملی در آنالیز بود ([۲۶] را ببینید). بعداً معلوم شد EKT رابطهٔ نزدیک ریاضی و فراریاضی با قضیهٔ ماینورگراف رابرتسن و سیمور دارد، که در [۹] نشان داده شده است.

این دارد که کم‌وبیش درستی یا سازگاری این گزاره‌های «بالاتر» را باور داشته باشیم. به‌علاوه، فکر می‌کنم بشود گفت که این نوع نتایج در حاشیهٔ ریاضیات معمولی ما قرار می‌گیرد یعنی در حاشیهٔ مسائلی که ریاضیدان به طور روزمره با آنها سروکار دارد[۱]. آنچه در حاشیه نیست به سادگی در ZFC صورتبندی می‌شود، و درواقع با دستگاههای بسیار ضعیفتر نیز این کار ممکن است، همان‌طور که بسیاری از مطالعات موردی سالهای اخیر نشان داده است.

حالا اختصاصاً آن بخش از ریاضیات را که کاربرد علمیش اجتناب‌ناپذیر است، در نظر بگیریم. می‌دانیم که این قسمت از ریاضیات، ازجمله، شامل بخش وسیعی از آنالیز است. اگر معتقد به دیدگاه افلاطونی نباشید یکی از استدلالها برای قبول هر نظریه‌ای در مورد مجموعه‌ها را ویلارد ون اورمان کواین و هیلری پاتنم ارائه کرده‌اند: یک نظریهٔ مجموعه‌ها برای مبانی آنالیز لازم است، و ریاضیات حاصل با کاربرد اساسی و موفقیت‌آمیز آن در یک نظریهٔ فیزیکی جاافتاده، تأیید می‌شود. اما این استدلال با یک سری تحقیقات موردی متزلزل شد. شروع این‌کار از رسالهٔ معروف هرمان وایل با عنوان پیوستار [۲۹] در سال ۱۹۱۸ بود که در آن وایل علی‌الاصول نشان داد که چگونه می‌توان کل آنالیز توابع تکه‌ای‌ـپیوستهٔ قرن نوزدهم را در یک دستگاه S تحویلپذیر به PA، صورتبندی کرد؛ از اواسط دههٔ ۱۹۷۰ این کار با بررسیهای افرادی از جمله گایسی تاکیوتی[۲]، هاروی فریدمن، استیون سیمپسن و من، برای گسترش این بحث به بخشهای اساسی آنالیز قرن بیستم از جمله بخش اعظم آنالیز تابعی و نظریهٔ اندازه، دنبال شده است. در نتیجهٔ این مطالعات، من به این حدس رسیده‌ام که تقریباً همهٔ ریاضیات قابل کاربرد در علم را می‌توان در دستگاههای تحویلپذیر به PA صورتبندی کرد، یا همان‌طور که در [۴] شعار داده‌ام «از کم خیلی کارها برمی‌آید». در مقابل، در مواردی در رهیافتهایی به مبانی نظریهٔ میدان کوانتومی فهمیده‌ام که ظاهراً باید از منابع PA فراتر برویم، اما نظریه‌های فیزیکی محتاج این منابع اضافی، بیشتر گمانه‌زنی‌اند. در هر حال، ریاضیات لازم در این موارد را می‌توان در زیردستگاههای نسبتاً ضعیف آنالیز غیرحملی، به انجام رساند، حتی اگر PA کفایت نکند. اصلاً منظورم این نیست که عمل روزمرهٔ ریاضی باید منحصر به کار در چنین دستگاههای فرعی باشد. ارزش ابزاری مفاهیم گسترده‌تر و «بالاتر» نظریه مجموعه‌ها غیرقابل انکار است، اما اینجا اصل مطلب این است که ببینیم: چه چیزی، اساساً برای چه چیزی ضروری است؟

وقت جمع‌بندی است، امیدوارم قدری خوراک فکری به شما داده باشم که کمک کند خودتان در بارهٔ سؤالاتی نظیر اینکه «آیا فرضیهٔ پیوستار معین است؟» نتیجه‌گیری کنید، و اینکه اگر چنین باشد، با فرض ناکافی بودن اصول موضوع فعلی، چه چیزی باید این مسائل را رفع ورجوع کند. اول مقاله قول داده بودم نظر خودم را در بارهٔ این چیزها مطرح کنم. تا حالا، حتماً حدس زده‌اید چه می‌خواهم بگویم، اما بگذارید با صدای بلند نظرم را اعلام کنم: به اعتقاد من فرضیهٔ پیوستار یک مسألهٔ ذاتاً مبهم است، که هیچ اصل موضوع

۱. یک دیدگاه مخالف، و شرح زیبایی از نیاز به اصول موضوع جدید در این باره در رودین [۳۰] آمده است.

2. Gaisi Takeuti

جدیدی هم به صورت قانع‌کننده‌ای دوای دردش نیست[۱]. بعد هم، فکر می‌کنم فلسفهٔ افلاطونی ریاضیات که فعلاً ادعای توجیه نظریهٔ مجموعه‌ها و به طور کلی، ریاضیات را دارد، به هیچ‌وجه رضایت‌بخش نیست و به نظر من باید فلسفهٔ دیگری مبتنی بر دریافتهای بین‌الاذهانی بشر پیدا کرد که عالم عینی ریاضیات را توصیف کند. سرانجام اینکه، من هیچ دلیلی نمی‌بینم که برای حل مسائل حل‌نشدهٔ ترکیبیاتی متناهی و حساب، عملاً نیازی به اصول موضوع جدید داشته باشیم. حل مسألهٔ فرما نمونه‌ای است که نشان می‌دهد ما فقط باید با این اصول موضوع پایه‌ای که داریم بیشتر کار کنیم. اما برای منطقدانان از لحاظ نظری بسیار جالب است که ببینند اگر از قبل اصول معینی را پذیرفته باشیم چه اصول موضوع جدیدی باید پذیرفته شود، مثلاً گودل فکر می‌کرد اگر اصول موضوع تسرملو فرنکل را پذیرفتیم، اصول موضوع کاردینالهای دست‌نیافتنی و مالو را باید بپذیریم. راستش را بخواهید من بیشتر از سی سال است که دارم از راههای مختلف روی این موضوع کار می‌کنم؛ طی سال گذشته به این نتیجه رسیدم که آنچه در سر دارم رضایت‌بخش‌ترین فرمولبندی کلی این موضوع است به صورت چیزی که من اسمش را می‌گذارم «گشودن یک دستگاه صوری شماتیک» [۵]. و این در اصل برمی‌گردد به مبدأ «طبیعی» فرمولبندی شماتیک اصولی نظیر استقرا در نظریهٔ اعداد و تفکیک، در نظریهٔ مجموعه‌ها، وقتی در مفهوم ماقبل نظریه‌ای خاصیت دلخواه «معین» به‌کار می‌روند. این با کاربرد روزمرهٔ ما بیشتر تطبیق دارد، که چنین اصولی را، بدون قید و شرط روی اینکه در چه زبان به‌خصوصی فرمولبندی شده‌اند، به صورت نامحدود به کار می‌بریم. اما می‌توانیم به صورتی روشمند آنچه را که در یک موضوع مفروض، معنی‌دار می‌یابیم غنیتر کنیم، به این صورت که همان اصول را با نوعی روش پسخورد دوباره به کار بگیریم. مثل وقتی که اصل استقرا را به کار می‌گیریم تا ثابت کنیم که یک تابع یا محمول از اعداد طبیعی که به طور ضمنی با معادلات بازگشتی تعریف می‌شود، تمام است و بنابراین می‌تواند به زبان ما اضافه شود. در کاری که مشترکاً با توماس اشترام انجام می‌دهیم، تاکنون نتایجی قطعی برای سیستمهای خاص با به کارگیری فرایند «گشودن» حاصل شده است [۶]، ما در این کار با گروهی از مسائل تازه و جالب روبه‌رو هستیم که باید به نوبت با آنها دست و پنجه نرم کنیم. اما این داستان دیگری است برای وقتی دیگر.

مراجع

1. P. Bernays, Zur Frage der Unendlichkeitsschemata in der axiomatischen Mengenlehre, in (Y. Bar-Hillel, et al., eds.) *Essays on the Foundations of Mathematics*, Magnes Press, Jerusalem, 1961, pp. 3-49. (English translation in (G. H. Müller, ed.) *Sets and Classes*, North-Holland, Amsterdam, 1976, pp. 121-172.)

2. P. J. Cohen, The independence of the Continuum Hypothesis. I. *Proc. Nat. Acad. Sci., U.S.A.* 50 (1963) 1143-1148, and II. *ibid.* 51 (1964) 105-110.

3. R. Dedekind, *Was sind und was sollen die Zahlen?*, F. Vieweg, Braunschweig, 1888. (English translation, in *Essays on the Theory of Numbers*, Dover, New York, 1963, pp. 29-115.)

4. S. Feferman, Why a little bit goes a long way: Logical foundations of scientifically applicable mathematics, *PSA* 1992, *Vol. II* (1993), pp. 442-455.

5. S. Feferman, Gödel's program for new axioms: Why, where, how and what?, in (P. Hájek, ed.) *Gödel '96', Lecture Notes in Logic* 6 (1996), pp. 3-22.

6. S. Feferman and T. Strahm, The unfolding of non-finitist arithmetic (to appear).

7. H. Friedman, Finite functions and the necessary use of large cardinals, *Ann. of Math.* (2) (to appear).

8. H. Friedman, K. McAloon, and S. G. Simpson, A finite combinatorial principle which is equivalent to the 1-consistency of predicative analysis, in (G. Metakides, ed.) *Patras Logic Symposion*, North-Holland, Amsterdam, 1982, pp. 197-230.

9. H. Friedman, N. Robertson, and P. D. Seymour, The metamathematics of the graph minor theorem, in (S. G. Simpson, ed.) *Logic and Combinatorics*, Contemporary Mathematics 65, Amer. Math. Soc., Providence, 1987, pp. 229-261.

10. K. Gödel, Über formal unentscheidbare Sätze der *Principia Mathematica* und verwandter Systeme I, *Monatsh. Math. Physik* 38 (1931), 173-198. (Reprinted with English translation in [14, pp. 144-195].)

11. K. Gödel, The consistency of the axiom of choice and of the generalized continuum hypothesis, *Proc. Nat. Acad. Sci., U.S.A.* 24 (1938), 556-557. (Reprinted in [**15**, pp. 26-27].)

12. K. Gödel, What is Cantor's continuum problem?, *Amer. Math. Monthly* 54 (1947), 515-525; errata 55, 151. (Reprinted in [**15**, pp. 176-187].)

ترجمهٔ فارسی با عنوان «مسألهٔ پیوستار کانتور چیست؟»، نشر ریاضی، سال ۲، شمارهٔ ۱، صص ۴۶-۵۴.

13. K. Gödel, What is Cantor's continuum problem? (Revised and expanded version of [12], in (P. Benacerraf and H. Putnam, eds.) *Philosophy of Mathematics: Selected Readings*, Prentice-Hall, Englewood Cliffs, 1964, 258-273; reprinted in [15, pp. 254-270].)

14. K. Göded, *Collected Works, Vol. I. Publications* 1929-1936 (S. Feferman, et al., eds.), Oxford University Press, New York, 1986.

15. K. Göded, *Collected Works, Vol. II. Publications* 1938-1974 (S. Feferman, et al., eds.), Oxford University Press, New York, 1990.

۱. CH فقط برجسته‌ترین نمونه در میان نمونه‌های بسیاری از احکام نظریهٔ مجموعه‌هاست که من فکر می‌کنم ذاتاً مبهم‌اند. البته می‌توان با اطمینان در داخل خود نظریهٔ مجموعه‌ها (یعنی در ZFC) در مورد این گزاره‌ها طوری بحث کرد که گویی معنی معینی دارند.

16. W. Hanf, Incompactness in languages with infinitely long expressions, *Fund. Math.* 53 (1964), 309-324.

17. A. Kanamori, *The Higher Infinite*, Springer-Verlag, Berlin, 1994.

18. A. Kanamori and M. Magidor, The evolution of large cardinal axioms in set theory, in (G. H. Müller and D. S. Scott, eds.) *Higher Set Theory*, Lecture Notes in Mathematics 669 (1978), 99-275.

19. H. J. Keisler and A. Tarski, From accessible to inaccessible cardinals, *Fund. Math.* 53 (1964), 225-308; errata 57 (1965), 119.

20. A. Levy, Axiom schemata of strong infinity in axiomatic set theory, *Pacific J. Math.* 10 (1960), 223-238.

21. P. Maddy, Believing the axioms, I, *J. Symbolic Logic* 53 (1988), 481-511, and II, *ibid.*, 736-764.

22. D. A. Martin, Hilbert's first problem: The Continuum Hypothesis, in (F. Browder, ed.) *Mathematical Developments Arising from Hilbert Problems*, Proc. Symposia Pure Math. 28, Amer. Math. Soc., Providence, 1976, pp. 81-92.

23. J. Paris and L. Harrington, A mathematical incompleteness in Peano arithmetic, in (J. Barwise, ed.) *Handbook of Mathematical Logic*, North-Holland, Amsterdam, 1977, pp. 1133-1142.

24. G. Peano, *Arithmetices Principia, Nova Methodo Exposita*, Bocca, Turin (1889). (Reprinted in *Opeara Scelte, Vol.* 2, Edizioni Cremonese, Rome, 1958, pp. 20-55, and in English translation in [28, pp. 83-97].)

25. D. S. Scott, Measurable cardinals and constructible sets, *Polish Acad. Sci. Math.* 9 (1961), 521-524.

26. S. G. Simpson, Nonprovability of certain combinatorial properties of finite trees, in (L. A. Harrington et al., eds.) *Harvey Friedman's Research on the Foundations of Mathematics*, North-Holland, Amsterdam, 1985, pp. 87-117.

27. A. Tarski, Some problems and results relevant to the foundations of set theory, in (E. Nagel, et al., eds.) *Logic, Methodology and Philosophy of Science. Proceedings of the* 1960 *International Congress*, Stanford University Press, Stanford, 1962, pp. 125-135.

28. J. van Heijenoort, *From Frege to Gödel. A Source Book in Mathematical Logic*, 1879-1931, Harvard University Press, Cambridge, 1967.

29. H. Weyl, *Das Kontinuum. Kritische Untersuchungen über die Grundlagen der Analysis*, Veit, Leipzig, 1918. (English translation: *The Continuum. A critical examination of the foundations of analysis*, University Press of America, Latham, 1987.)

30. H. Woodin, Large cardinal axioms and independence: The continuum problem revisited, *Math. Intelligencer* 16 (1994), 31-35.

ترجمهٔ فارسی با عنوان «اصول موضوع عددهای اصلی بزرگ، و استقلال ...» در نشر ریاضی، سال ۶، شمارهٔ ۱ و ۲، صص ۲۱ـ۲۵.

31. E. Zermelo, Beweis, dass jede Menge wohlgeordnet werden kann, *Math. Ann.* 59 (1904), 514-516. (English translation in [28, pp. 139-141].)

32. E. Zermelo, Untersuchungen über die Grundlagen der Mengenlehre, I, *Math. Ann.* 65 (1908), 261-281. (English translation in [28, pp. 199-215].)

33. E. Zermelo, Über Grenzzahlen und Mengenbereiche: Neue Untersuchungen über die Grundlagen der Mengenlehre, *Fund. Math.* 16 (1930), 29-47.

******

• Solomon Feferman, "Does mathematics need new axioms?", *Amer. Math. Monthly*, (2) **106** (1999) 99-111.

* سالومون ففرمن، استاد ریاضیات و فلسفه در دانشگاه استنفرد، آمریکا

sf@csli.stanford.edu

جیان‌کارلو روتا در ژانویهٔ ۱۹۹۸، چند ماهی قبل از مرگش، سه سخنرانی مستقل از هم در نشست سالانهٔ انجمن ریاضی آمریکا ایراد کرد که متن یکی از آنها را با عنوان «احتمال هندسی» در شمارهٔ ۲ی سال ۱۰ نشر ریاضی خواندید. مقالهٔ زیر و مقالهٔ بعدی، ترجمهٔ متن دو سخنرانی دیگر اوست.

دو نقطهٔ عطف در نظریهٔ ناورداها•

جیان‌کارلو روتا*

ترجمهٔ شهرام محسنی‌پور

نظریهٔ ناورداها داستان بزرگ رمانتیک ریاضیات است. به مدت ۱۵۰ سال، از آغاز پیدایش آن با کارهای بول تا میانهٔ این قرن یعنی زمانی‌که نظریهٔ ناورداها به شاخه‌های مختلف و مستقلی تقسیم شد، اعتقاد مشترک به ناورداها زمینهٔ پیوند ریاضیدانان همهٔ سرزمینها بود: در انگلستان کیلی، مک مائن، سیلوستر و سالمن[1]، و بعدها آلفرد یانگ، ایتکن[2]، لیتلوود و ترنبال و در آلمان، کلبش[3]، گوردان، گراسمان، سوفوس لی و اشتودی[4] و در فرانسه ارمیت، ژوردان و لاگر و در ایتالیا کاپلی، بریوسکی[5]، ترودی[6] و کورادو سگرس[7] و دوویدیو[8]، و در آمریکا گِلِن، دیکسن، کاروس (که تکنگاشتهای کاروس به افتخار او نامگذاری شده است.)، اریک تمپل بل و بعدها هرمان وایل. در تاریخ، به ندرت دیده شده است که اجتماعی بین‌المللی از محققین به خاطر آرمانی مشترک چنین احساس وحدتی در چنین دورهٔ طولانی از زمان داشته باشند. در قرن ما نظریهٔ لی، هندسهٔ جبری، جبر دیفرانسیل و ترکیبیات جبری ثمره‌های نظریهٔ ناورداها هستند. هیچ نظریه‌ای در ریاضیات بجز نظریهٔ توابع مختلط تأثیری چنین ژرف و ماندگار در رشد ریاضیات نداشته است.

و سرانجام نظریهٔ ناورداها قربانی موفقیت خود شد. امروزه خودِ اصطلاح «نظریهٔ ناورداها» برای نظریه‌های پدید آمده از آن به‌کار می‌رود به‌گونه‌ای که دیگر تقریباً معنای خود را از دست داده است. پس عجیب نخواهد بود اگر شما از عنوان این سخنرانی دچار سردرگمی شوید که در بارهٔ کدام نظریهٔ ناورداهاست.

این سخنرانی در بارهٔ نظریهٔ کلاسیک ناورداهاست. رساله‌های قدیمی را که در انبار کتابخانه‌ها نگاهداری می‌شوند غبارروبی می‌کنیم، آنها را بازخوانی و از نو تعبیر کرده به زبانی موافق با استانداردهای دقت امروزی ارائه می‌کنیم. برنامهٔ نظریهٔ کلاسیک ناورداها را که زمانی کنار گذاشته شده بود چون آن را بی‌ثمر می‌پنداشتند، دوباره دنبال می‌کنیم، و شاید سرانجام موفقیت در دسترس باشد.

من دو نقطهٔ عطف را در تاریخ نظریهٔ ناورداها مرور خواهم کرد. اولی که «جدید» است در حوالی آغاز قرن رخ داد و هنوز هم تأثیرش در سراسر ریاضیات احساس می‌شود. دومی که «قدیمی» است خیلی زود وارد میدان شد و منجر به سوء تعبیری جدی گردید که تا به امروز باقی مانده است.

تعریفی کم‌مایه از نظریهٔ ناورداها می‌تواند چنین باشد: نظریهٔ ناورداها عبارت است از مطالعهٔ مدارهای کنشهای گروه. چنین تعریفی صحیح است ولی باید با ارائهٔ یک برنامهٔ اجرایی کامل شود. هرمان وایل در مقدمهٔ کتاب *گروههای کلاسیک*، برنامهٔ نظریهٔ ناورداها را در دو حکم خلاصه می‌کند. اولی اینکه «همهٔ واقعیات هندسی با صفرشدن ناورداها نمایش داده می‌شوند» و دومی اینکه «همهٔ ناورداها ناوردای تانسورها هستند».

اجازه دهید مختصری در بارهٔ این جملات با شکوه صحبت کنیم. واقعیت هندسی چیست؟ واقعیتی مربوط به فضاست که از دستگاه مختصات انتخاب شده مستقل است. این واقعیتها به‌وسیلهٔ معادلاتی توصیف می‌شوند که نیازمند انتخاب دستگاه مختصات‌اند. در فضای برداری V با بعد n می‌توان یک دستگاه مختصات x_1، x_2، $\cdots$، x_n انتخاب کرد. از زمان دکارت یادگرفته‌ایم که واقعیتهای هندسی را با معادلاتی در مختصات x_1، x_2، $\cdots$، x_n نمایش دهیم. با این همه در حدود ۱۰۰ سال پیش ریاضیدانان و فیزیکدانان کشف تکان‌دهنده‌ای کردند مبنی بر اینکه معادلات معمول (معادلاتی در حلقهٔ جابجایی تولید شده توسط متغیرهای x_1، x_2، $\cdots$، x_n) برای توصیف بسیاری از واقعیتهای هندسی و فیزیکی ناکافی‌اند. این کشف انگیزه‌ای شد برای معرفی حلقه‌ای تعمیم‌یافته، یعنی حلقهٔ چندجمله‌ای‌های ناجابجایی در مختصات x_1، $\cdots$، x_n. عناصر همگن این حلقه (چندجمله‌ای‌های

1. Salmon 2. Aitken 3. Clebsch 4. Study 5. Brioschi
6. Trudi 7. Corrado Segres 8. d'Ouidio

ناجابجایی همگن با متغیرهای x_1، ...، x_n) تانسور نامیده می‌شوند. اگر فلسفهٔ هرمان وایل را باور کنیم، متقاعد می‌شویم که معادلات جبر تانسوری برای توصیف هر واقعیت هندسی که تاکنون با آن برخورد داشته‌ایم، کافی خواهد بود. علاوه بر این، اگر قرار باشد معادلات فوق بیان‌کنندهٔ ویژگیهای هندسی باشند، در هر دستگاه مختصات انتخابی باید برقرار باشند. به بیان دیگر، معادلاتی که واقعیتهای هندسی را توصیف می‌کنند باید تحت تعویض مختصات ناوردا باشند. برنامهٔ نظریهٔ ناورداها از زمان بول تا به امروز دقیقاً ترجمهٔ واقعیتهای هندسی به معادلات جبری ناورداست که با عبارتهای تانسوری بیان می‌شوند.

این برنامهٔ ترجمهٔ هندسه به جبر قرار بود در دو گام انجام شود. گام نخست عبارت بود از تجزیهٔ جبر تانسوری به مؤلفه‌های تحویل‌ناپذیر تحت تعویض مختصات. گام دوم عبارت بود از ابداع نمادی کارامد برای نمایش ناورداهای هر مؤلفهٔ تحویل‌ناپذیر. در این قرن گام نخست با موفقیت برداشته شد ولی گام دوم زمانی در دههٔ ۲۰ رها شد و تنها اخیراً مورد توجه قرار گرفته است.

تجزیهٔ جبر تانسوری به مؤلفه‌های تحویل‌ناپذیر تقریباً به‌طور همزمان در حوالی آغاز قرن توسط ایسایی شور[1] و آلفرد یانگ کشف شد. ایدهٔ اصلی در این تجزیه یکی از مهمترین پیشرفتها در ریاضیات در همهٔ دورانهاست، و ارائهٔ آن به شکلی قابل استفاده برای دانشجویان دورهٔ کارشناسی، سودمند خواهد بود.

تابعی سه‌متغیره مانند $f(x_1, x_2, x_3)$ در نظر بگیرید. دو ردهٔ معروف توابع سه‌متغیره عبارت‌اند از (یک) توابع متقارن که به ازای هر جایگشتی که اندیسهای (۱, ۲, ۳) را به (i_1, i_2, i_3) تبدیل می‌کند، در معادلات زیر صدق می‌کنند

$$f_s(x_1, x_2, x_3) = f_s(x_{i_1}, x_{i_2}, x_{i_3})$$

و (دو) توابع پادمتقارن که با معادلات زیر تعریف می‌شوند

$$f_a(x_1, x_2, x_3) = \pm f_a(x_{i_1}, x_{i_2}, x_{i_3})$$

که بسته به اینکه جایگشت تبدیل‌کنندهٔ (۱, ۲, ۳) به (i_1, i_2, i_3) زوج یا فرد باشد علامت فوق ۱+ یا ۱− است.

چنین نیست، که هر تابع سه متغیره مجموع تابعی متقارن و تابعی پادمتقارن باشد. نوع سومی از تابع لازم است که تابع دوری نامیده می‌شود و با معادلهٔ زیر مشخص می‌گردد:

$$f_c(x_1, x_2, x_3) + f_c(x_3, x_1, x_2) + f_c(x_2, x_3, x_1) = 0$$

هر تابع سه متغیره را می‌توان به‌طور یکتا به‌صورت مجموع توابعی متقارن، پادمتقارن و دوری نوشت و به بیان نمادی:

$$f(x_1, x_2, x_3) = f_s(x_1, x_2, x_3) + f_a(x_1, x_2, x_3) + f_c(x_1, x_2, x_3)$$

هریک از این سه ردهٔ تقارنی از توابع، تحت جایگشتها ناوردایند. این مطلب برای توابع متقارن و پادمتقارن واضح است ولی برای توابع دوری چندان واضح نیست. این سه زیرفضای ناوردای توابع همان نقشی را برای گروه جایگشتهای یک مجموعهٔ سه‌عضوی بازی می‌کنند که ویژه بردارها برای ماتریسهای متقارن.

برای توابع چهارمتغیرهٔ $f(x_1, x_2, x_3, x_4)$ پنج ردهٔ تقارنی وجود دارد که به شرح زیر تعریف می‌شوند:

۱. توابع متقارن

۲. توابع پادمتقارن

۳. توابع دوری‌ـمتقارن که در چهار معادلهٔ زیر صدق می‌کنند

$$f(x_1, x_2, x_3, x_4) + f(x_1, x_4, x_2, x_3) + f(x_1, x_3, x_4, x_2) = 0$$

$$f(x_1, x_2, x_3, x_4) + f(x_4, x_2, x_1, x_3) + f(x_3, x_2, x_4, x_1) = 0$$

$$f(x_1, x_2, x_3, x_4) + f(x_4, x_1, x_3, x_2) + f(x_2, x_4, x_3, x_1) = 0$$

$$f(x_1, x_2, x_3, x_4) + f(x_3, x_1, x_2, x_4) + f(x_2, x_3, x_1, x_4) = 0$$

۴. توابعی که در چهار معادلهٔ زیر صدق می‌کنند

$$\begin{aligned} &f(x_1, x_2, x_3, x_4) + f(x_2, x_1, x_3, x_4) \\ &\qquad + f(x_1, x_2, x_4, x_3) + f(x_2, x_1, x_4, x_3) = 0 \\ &f(x_1, x_2, x_3, x_4) + f(x_3, x_2, x_1, x_4) \\ &\qquad + f(x_1, x_4, x_3, x_2) + f(x_3, x_4, x_1, x_2) = 0 \\ &f(x_1, x_2, x_3, x_4) + f(x_1, x_3, x_2, x_4) \\ &\qquad + f(x_4, x_2, x_3, x_1) + f(x_4, x_3, x_2, x_1) = 0 \\ &\sum \operatorname{sign}(\sigma) f(x_{\sigma 1}, x_{\sigma 2}, x_{\sigma 3}, x_{\sigma 4}) = 0 \end{aligned}$$

۵. توابعی که در معادلات زیر صدق می‌کنند

$$\begin{aligned} &f(x_1, x_2, x_3, x_4) - f(x_2, x_1, x_3, x_4) \\ &\qquad - f(x_1, x_2, x_4, x_3) + f(x_2, x_1, x_4, x_3) = 0 \\ &f(x_1, x_2, x_3, x_4) - f(x_3, x_2, x_1, x_4) \\ &\qquad - f(x_1, x_4, x_3, x_2) + f(x_3, x_4, x_1, x_2) = 0 \\ &f(x_1, x_2, x_3, x_4) - f(x_1, x_3, x_2, x_4) \\ &\qquad - f(x_4, x_2, x_3, x_1) + f(x_4, x_3, x_2, x_1) = 0 \\ &\sum f(x_{\sigma 1}, x_{\sigma 2}, x_{\sigma 3}, x_{\sigma 4}) = 0 \end{aligned}$$

هر تابع چهارمتغیره به‌طور یکتا قابل نمایش به‌صورت مجموع پنج تابع است که هر کدام به یکی از این رده‌های تقارنی تعلق دارد. هر ردهٔ تقارنی تحت جایگشتها ناورداست.

به‌طور کلیتر، هر تابع nمتغیرهٔ $f(x_1, x_2, \cdots, x_n)$ را می‌توان به‌طور یکتا به‌صورت مجموع p_n تابع نوشت که هر یک به رده‌ای تقارنی متفاوت با دیگری تعلق دارد. در اینجا p_n مساوی است با تعداد افرازهای عدد صحیح n. یافتن معادلاتی که هر ردهٔ تقارنی را تعریف می‌کند مشکل نیست.

این تجزیه پس از چند تعویض صوری نمادها برای تانسورها هم برقرار است. تا به امروز تنها دو ردهٔ تقارنیِ تانسورها به‌طور مشروح بررسی شده‌اند: یکی تانسورهای متقارن که همان چندجمله‌ای‌های تعویض‌پذیر معمولی هستند و استفاده از آنها را در هندسه تحلیلی یاد گرفته‌ایم و دیگری تانسورهای پادمتقارن، که چندجمله‌ای‌هایی در مختصات $x_1, x_2, \cdots, x_n$ با شرط

1. Issai Schur

$x_ix_j = -x_jx_i$، هستند. تانسورهایی غیر از تانسورهای متقارن و پاد متقارن نیز در فیزیک و هندسه ظاهر می‌شوند که به رده‌های تقارنی تعلق دارند. با این همه، این‌گونه رده‌های تقارنی خیلی کم بررسی شده‌اند و راهی طولانی تا فهم آنها در پیش است. خوب، این از کلمهٔ «جدید»، در مقدمهٔ این سخنرانی. حال کمی هم حق کلمهٔ «قدیمی» را ادا کنیم. من در اینجا غریبترین جنبهٔ نظریهٔ کلاسیک ناورداها را توصیف خواهم کرد، یعنی نمادگذاری سمبلیک یا شبح‌وار[1] که اریک تمپل بل «سخنرانیهای سمینار»ش را در سال ۱۹۲۷ به این موضوع اختصاص داده است. من ساده‌ترین گروه یعنی گروه انتقالهای خط را بررسی خواهم کرد. وجوه غیرعادی روش سمبلیک در همین حالت خاص آشکار خواهد شد.

فرض کنید $p(x)$ و $q(x)$ چندجمله‌ای‌هایی یکین[2] با متغیر x باشند. من آنها را با نمادگذاری جالب زیر می‌نویسم:

$$p(x) = x^n + \binom{n}{1}a_1x^{n-1} + \binom{n}{2}a_2x^{n-2} + \cdots + \binom{n}{n-1}a_{n-1}x + a_n$$

و

$$q(x) = x^k + \binom{k}{1}b_1x^{k-1} + \binom{k}{2}b_2x^{k-2} + \cdots + \binom{k}{k-1}b_{k-1}x + b_k$$

فرض می‌کنم که درجهٔ $q(x)$ از درجهٔ $p(x)$ کمتر است. یعنی $k \leq n$.

عملگر انتقال T^c روی چندجمله‌ای $p(x)$ را به‌صورت زیر تعریف می‌کنیم:

$$T^cp(x) = p(x+c)$$

و می‌نویسیم

$$p(x+c) = x^n + \binom{n}{1}p_1(c)x^{n-1} + \binom{n}{2}p_2(c)x^{n-2} + \cdots + \binom{n}{n-1}p_{n-1}(c)x + p_n(c)$$

jامین ضریب، $p_j(c)$، از چندجمله‌ای $p(x+c)$ چنین محاسبه می‌شود

$$p_j(c) = a_j + \binom{j}{1}a_{j-1}c + \binom{j}{2}a_{j-2}c^2 + \cdots + c^j$$

چندجمله‌ای $I(a_1, a_2, \cdots, a_n, b_1, b_2, \cdots, b_k)$ با متغیرهای a_1، a_2، $\cdots$، a_n و b_1، b_2، $\cdots$، b_k، ناوردای دو چندجمله‌ای $p(x)$ و $q(x)$ نامیده می‌شود هرگاه به‌ازای هر عدد مختلط c داشته باشیم

$$I(a_1, a_2, \cdots, a_n, b_1, b_2, \cdots, b_k) = I(p_1(c), p_2(c), \cdots, p_n(c), q_1(c), q_2(c), \cdots, q_k(c))$$

با قدری تسامح در نمادگذاری می‌نویسیم $I(p(x), q(x))$ و از I به عنوان ناوردای چندجمله‌ای‌های $p(x)$ و $q(x)$ یاد می‌کنیم. در این نمادگذاری تسامح‌آمیز، چندجمله‌ای I ناوردای چندجمله‌ای‌های $p(x)$ و $q(x)$ نامیده می‌شود هرگاه برای هر ثابت c داشته باشیم

$$I(T^cp(x), T^cq(x)) = I(p(x), q(x))$$

نظریهٔ ناورداها به این مسأله می‌پردازد: تعیین همهٔ ناورداهای مجموعه‌ای داده شده از چندجمله‌ای‌ها و نیز وجه اهمیت ناورداها.

«وجه اهمیت» یک ناوردا چیست؟ من در اینجا به هرمان وایل متوسل می‌شوم. «هر» ویژگی چندجمله‌ای‌ها که تحت گروه انتقالها ناوردا باشد با صفرشدن دسته‌ای از ناورداها قابل نمایش است. به بیان دیگر «هر» مجموعه‌ای از چندجمله‌ای‌ها که تحت انتقالها ناوردا باشد همانند مجموعه‌ای از چندجمله‌ای‌هاست که از مساوی صفر قراردادن دسته‌ای از ناورداهای چنین چندجمله‌ای‌هایی به‌دست می‌آیند. درک این گفته بی‌آوردن مثال ممکن نیست.

بیایید ساده‌ترین و قدیمیترین مثال را بررسی کنیم. خاصیت «ریشهٔ مضاعف داشتن» برای چندجمله‌ای درجهٔ دو

$$q(x) = x^2 + 2b_1x + b_2$$

تحت انتقالها ناورداست. به عبارت دیگر اگر چندجمله‌ای $q(x)$ ریشهٔ مضاعف داشته باشد، چندجمله‌ای $q(x+c)$ نیز به ازای هر ثابت c چنین خواهد بود. به تبعیت از هرمان وایل ناوردایی را جستجو می‌کنیم که صفربودنش نمایانگر این خاصیت باشد. به آسانی می‌توان امتحان کرد که مبین

$$D(b_1, b_2) = b_1^2 - b_2$$

همان ناوردای مطلوب است. این مثالِ منسوب به بول جرقه‌ای بود که منجر به پیدایش نظریهٔ ناورداها شد.

اغلب، با اشاره‌ای به قضیهٔ پایه هیلبرت، گفته می‌شود که «هیلبرت نظریهٔ ناورداها را از بین برد». این حقیقت ندارد. هیلبرت نظریهٔ ناورداها را بسیار دوست می‌داشت و پس از اینکه قضیهٔ پایه‌اش را ثابت کرد همچنان به انتشار مقالاتی چشمگیر در نظریهٔ ناورداها ادامه داد. تعدادی از جذابترین نتایج در نظریهٔ ناورداها در بیست سال اول این قرن کشف شد، یعنی در دوره‌ای طولانی پس از اثبات قضیه پایهٔ هیلبرت.

پس علت زوال موقت نظریهٔ ناورداها که پس از آن پیش آمد چه بود؟ یک دلیل آن شیوع بیماری‌گونهٔ استفاده از نمادگذاری سمبلیک یا شبح‌وار بود.

دیودونه نوشته است که نیمی از موفقیت هر شاخه‌ای از ریاضیات بستگی به انتخاب مناسب نمادها دارد. تهیه فهرستی از نمادگذاری‌های بدفرجام که منجر به از بین رفتن بخشهای مختلفی از ریاضیات شده‌اند به‌همراه فهرستی از نمادگذاری‌های بجا و مناسب که به پیشرفت ریاضیات کمک کرده‌اند، جالب توجه خواهد بود. نمادگذاری سمبلیک یا شبح‌وار، فاجعه‌آمیز بود. شماری از ریاضیدانان تلاش کردند که به روش سمبلیک معنی ببخشند، ولی موفق نشدند. هرمان وایل، اریک تمپل بل و ادوارد هگلر کاروس سه تا از سرشناس‌ترین‌ها بودند. بل نتوانست نمادگذاری شبح‌وار را درست تعریف کند و کتاب حساب جبری وی تا به امروز کتاب «سربه‌مهر» باقی مانده است. اگر وایل و بل ۵۰ سال بیشتر زنده می‌ماندند تا از پیشرفتهای آنچه در آن

1. umbral 2. monic

روز «جبر نوین» نامیده می‌شد، برخوردار شوند، بی‌شک در تعریف درست نمادگذاری شبح‌وار موفق می‌شدند.

در زمان ما، همان‌طورکه به شما نشان خواهم داد این کار آسان است و تنها چند دقیقه وقت می‌گیرد. قبل از اینکه سیل تعاریف را به طرفتان سرازیر کنم بگذارید بگویم که چه چیزی را نخواهم گفت. می‌توان نشان داد که نمادگذاری شبح‌وار با نمادگذاری دیگری که در زمانهٔ ما سوءشهرت بسیار دارد هم‌ارز (یا نهانریخت[1]، واژهٔ ابداعی دوست مرحومم گرت برکاف) است، یعنی نمادگذاری جبرهای هوپف. من نمی‌خواهم برای این اظهارات مبهم دلیل بیاورم. نه به این علت که مشکل است، بلکه به این دلیل که نیازی به این کار نیست.

حال می‌پردازیم به تعریف نمادگذاری شبح‌وار. به موازات دو چندجمله‌ای $p(x)$ و $q(x)$، جبر چندجمله‌ای $\mathbb{C}[x,\alpha,\beta]$ را نسبت به سه متغیر x، α و β همراه با تابعک خطی E که روی فضای برداری زمینهٔ $\mathbb{C}[x,\alpha,\beta]$ تعریف می‌شود در نظر می‌گیریم. تعریف تابعک خطی E نکته‌ای اساسی است و در گامهای زیر انجام می‌شود:

گام اول: به ازای هر عدد صحیح نامنفی j قرار می‌دهیم

$$E(x^j) = x^j$$

و لذا $E(1) = 1$. پس برد تابعگون خطی E، $\mathbb{C}[x]$ است.

گام دوم: قرار می‌دهیم

$$E(\alpha^j) = a_j$$

و لذا به ازای $j > n$، $E(\alpha^j) = 0$.

گام سوم: قرار می‌دهیم

$$E(\beta^j) = b_j$$

و لذا اگر $j > k$، $E(\beta^j) = 0$.

گام چهارم: این گام، گام اصلی است. قرار می‌دهیم

$$E(\alpha^i\beta^j x^l) = E(\alpha^i)E(\beta^j)x^l$$

به پیروی از سیلوستر، متغیرهای α و β، شبح نامیده می‌شوند. به عبارت دیگر، تابعک خطی E روی اشباح متمایز، ضربی است.

گام پنجم: تعریف را به‌طور خطی توسیع می‌دهیم.

به این ترتیب، تعریف تابعک خطی E به انجام می‌رسد.

حال به نگران‌کننده‌ترین جنبه از نمادگذاری شبح‌وار می‌رسیم. فرض کنید $f(\alpha,\beta,x)$ و $g(\alpha,\beta,x)$ دو چندجمله‌ای با متغیرهای α، β، و x باشند؛ می‌نویسیم

$$f(\alpha,\beta,x) \cong g(\alpha,\beta,x)$$

وقتی که

$$E(f(\alpha,\beta,x)) = E(g(\alpha,\beta,x))$$

1. cryptomorphic

نماد $\cong$ را بخوانید «هم‌ارز است با».

«قدما» کمی از حد مجاز فراتر رفتند و نماد تساوی معمولی را جایگزین نماد $\cong$ کردند و نوشتند

$$f(\alpha,\beta,x) = g(\alpha,\beta,x)$$

آنها از این اشتباه آگاه بودند و هر چند با مهارت و استادیِ هوشمندانه‌ای از خطاهای محاسباتی اجتناب می‌کردند، قادر نبودند از این استفادهٔ نابجا از نمادها اجتناب کنند.

روش شبح‌وار یا سمبلیک، عبارت است از اینکه به جای همهٔ ضرایب ظاهرشده در چندجمله‌ای‌های $p(x)$ و $q(x)$، اشباح و هم‌ارزی‌ها را قرار دهیم. به عنوان مثال

$$p(x) \cong (x+\alpha)^n$$

و

$$q(x) \cong (x+\beta)^k$$

بیایید با دقت هم‌ارزی اول را امتحان کنیم.

طبق تعریف هم‌ارزی باید نشان دهیم

$$E(p(x)) = E((x+\alpha)^n)$$

چون برای هر عدد صحیح نامنفی j، $E(x^j) = x^j$، عبارت بالا معادل است با

$$p(x) = E((x+\alpha)^n)$$

با بسط دادن طرف راست، طبق قضیهٔ دوجمله‌ای به‌دست می‌آوریم:

$$E((x+\alpha)^n) = E\Big(x^n + \binom{n}{1}\alpha x^{n-1} + \binom{n}{2}\alpha^2 x^{n-2} + \cdots + \binom{n}{n-1}\alpha^{n-1}x + \alpha^n\Big)$$

بنا به خطی بودن، این مساوی است با

$$x^n + \binom{n}{1}E(\alpha)x^{n-1} + \binom{n}{2}E(\alpha^2)x^{n-2} + \cdots + \binom{n}{n-1}E(\alpha^{n-1})x + E(\alpha^n)$$

با محاسبهٔ تابعک خطی E می‌بینیم که عبارت بالا مساوی است با

$$x^n + \binom{n}{1}a_1x^{n-1} + \binom{n}{2}a_2x^{n-2} + \cdots + \binom{n}{n-1}a_{n-1}x + a_n$$

که همان است که انتظار داشتیم. عبارت

$$(x+\alpha)^n$$

نمایش شبح‌وار چندجمله‌ای $p(x)$ نامیده می‌شود.

در نمادگذاری شبح‌وار، عدد مختلط r ریشهٔ معادلهٔ چندجمله‌ای $p(x)=0$ است اگر و تنها اگر

$$(r+\alpha)^n \cong 0$$

همین‌طور، در نمادگذاری شبح‌وار، چندجمله‌ای $T^c p(x)=p(x+c)$ را می‌توان به‌صورت زیر نمایش داد

$$p(x+c) \cong (x+\alpha+c)^n$$

و از اینجا نمایش شبح‌وار ضرایب $p_j(c)$ از چندجمله‌ای $p(x+c)$ یعنی

$$p_j(c) \cong (\alpha+c)^j$$

به دست می‌آید.

حال خواهیم دید که نمادگذاری شبح‌وار چگونه به ناورداها مربوط می‌شود. فرض کنید چندجمله‌ای‌های $p(x)$ و $q(x)$ از درجهٔ n باشند. ناوردای A از چندجمله‌ای‌های $p(x)$ و $q(x)$ را می‌توان به‌صورت زیر تعریف کرد:

$$A(q(x),p(x)) \cong (\beta-\alpha)^n$$

محاسبهٔ ناوردای A برحسب ضرایب $p(x)$ و $q(x)$ به‌صورت زیر انجام می‌شود:

$$\begin{aligned}
A(q(x),p(x)) &= E((\beta-\alpha)^n)\\
&= E\left(\beta^n-\binom{n}{1}\beta^{n-1}\alpha+\cdots+(-1)^{n-1}\binom{n}{n-1}\beta\alpha^{n-1}\right.\\
&\quad\left.+(-1)^n\alpha^n\right) = E(\beta^n)-E\left(\binom{n}{1}\beta^{n-1}\alpha\right)+\cdots\\
&\quad+(-1)^{n-1}E\left(\binom{n}{n-1}\beta\alpha^{n-1}\right)+(-1)^nE(a^n)\\
&= E(\beta^n)-\binom{n}{1}E(\beta^{n-1})E(\alpha)+\cdots\\
&\quad+(-1)^{n-1}\binom{n}{n-1}E(\beta)E(\alpha^{n-1})+(-1)^nE(\alpha^n)\\
&= b_n-\binom{n}{1}b_{n-1}a_1+\binom{n}{2}b_{n-2}a_2-\cdots\\
&\quad+\cdots+(-1)^{n-1}\binom{n}{n-1}b_1b_{n-1}+(-1)^na_n
\end{aligned}$$

چرا A ناورداست؟ این را به بهترین وجه می‌توان در نمادگذاری شبح‌وار دید:

$$A(T^cq(x),T^cp(x)) \cong (\beta+c-\alpha-c)^n=(\beta-\alpha)^n$$

ناوردای A ناوردای ناهم‌قطبی نامیده می‌شود. دو چندجمله‌ای $p(x)$ و $q(x)$ را که دارای خاصیت $A(q(x),p(x))=0$ باشند ناهم‌قطب گوییم. در نمادگذاری شبح‌وار دو چندجمله‌ای ناهم‌قطب‌اند اگر

$$(\beta-\alpha)^n \cong 0$$

مفهوم ناهم‌قطبی پیشینه‌ای مشعشع دارد که به آپولونیوس می‌رسد.

وجه اهمیت ناوردای ناهم‌قطبی چیست؟ معنای ناهم‌قطب بودن دو چندجمله‌ای چه می‌تواند باشد؟ این سؤال در قضیهٔ زیر پاسخ داده می‌شود:

قضیهٔ ۱. فرض کنید که r ریشهٔ چندجمله‌ای $q(x)$ باشد، یعنی $q(r)=0$. در این صورت چندجمله‌ای‌های $q(x)$ و $p(x)=(x-r)^n$ ناهم‌قطب‌اند.

برهان. از $p(x)=(x-r)^n$ به‌دست می‌آوریم $\alpha^j \cong (-r)^j$، و بنابراین

$$A(q(x)),p(x)) \cong (\beta-(-r))^n=(\beta+r)^n \cong 0$$

فهوالمطلوب.

نتیجه. اگر چندجمله‌ای $q(x)$ دارای n ریشهٔ متمایز r_1، r_2، $\cdots$، r_n باشد، و اگر چندجمله‌ای $p(x)$ با $q(x)$ ناهم‌قطب باشد، آنگاه ثابتهای c_1، c_2، $\cdots$، c_n موجودند به‌طوری که

$$p(x)=c_1(x-r_1)^n+c_2(x-r_2)^n+\cdots+c_n(x-r_n)^n$$

برهان. بعد زیرفضای آفین همهٔ چندجمله‌ای‌های (نه لزوماً یکین) $p(x)$ که با $q(x)$ ناهم‌قطب‌اند، n است. ولی اگر ریشه‌های چندجمله‌ای $q(x)$ ساده باشند آنگاه طبق قضیهٔ بالا چندجمله‌ای‌های

$$(x-r_1)^n,\ (x-r_2)^n,\ \cdots,\ (x-r_n)^n$$

مستقل خطی‌اند و با $q(x)$ ناهم‌قطب‌اند. بنابراین چندجمله‌ای $p(x)$ ترکیب خطی چندجمله‌ای‌های فوق است و این، برهان را کامل می‌کند.

بنابراین، می‌بینیم که ناهم‌قطبی جوابی بدیهی به سؤال زیر می‌دهد: چه وقت می‌توان چندجمله‌ای $p(x)$ را به صورت ترکیبی خطی از چندجمله‌ای‌هایی به شکل $(x-r_1)^n$، $(x-r_2)^n$، $\cdots$، $(x-r_n)^n$ نوشت؟

قضیه‌ای زیبا در بارهٔ ناهم‌قطبی توسط ریاضیدان بریتانیایی جان هیلتن گریس[1] اثبات شده است. من آن را بدون برهان بیان می‌کنم:

قضیهٔ گریس. اگر دو چندجمله‌ای $p(x)$ و $q(x)$ از درجهٔ n ناهم‌قطب باشند، آنگاه هر قرصی در صفحهٔ مختلط که همهٔ صفرهای $p(x)$ را دربرداشته باشد حداقل شامل یک صفر $q(x)$ است.

قضیهٔ گریس نمونه‌ای است از قضایایی که می‌توان آنها را قضایای سرسخت[2] نامید. تقریباً ۱۰۰ سال است که این قضیه در برابر تمام اقدامات برای تعمیم آن مقاومت کرده است. تقریباً همهٔ نتایج شناخته شده در بارهٔ توزیع صفرهای چندجمله‌ای‌ها در صفحهٔ مختلط، پیامد قضیهٔ گریس هستند.

من اکنون ناوردای ناهم‌قطبی را به حالتی که چندجمله‌ای‌های $p(x)$ و $q(x)$ از درجات مختلف n و k $(n \geq k)$ باشند، تعمیم خواهم داد. به این منظور اجازه دهید مفهوم ناوردا را به شرح زیر، اندکی تعمیم دهیم:

چندجمله‌ای $I(a_1,a_2,\cdots,a_n,b_1,b_2,\cdots,b_k,x)$ با متغیرهای a_1، a_2، $\cdots$، a_n، b_1، $\cdots$، b_k، x، ناوردای چندجمله‌ای‌های $p(x)$ و $q(x)$ خوانده می‌شود هرگاه برای هر عدد مختلط c

$$\begin{aligned}
I(a_1,a_2,\cdots,a_n,b_1,b_2,\cdots,b_k,x) &= I(p_1(c),p_2(c),\cdots,\\
&\quad p_n(c),q_1(c),q_2(c),\cdots,q_k(c),x+c)
\end{aligned}$$

1. Grace 2. sturdy

این ناورداهای تعمیم‌یافته‌تر گاهی هموردا نامیده می‌شوند.

حال ناوردای ناهم‌قطبی تعمیم‌یافته را چنین تعریف می‌کنیم:

$$A(q(x), p(x)) \cong (\beta - \alpha)^k (x - \alpha)^{n-k}$$

مجدداً گوییم دو چندجمله‌ای $p(x)$ و $q(x)$ ناهم‌قطب‌اند هرگاه $A(q(x), p(x))$ متحد با صفر باشد، یعنی به ازای هر x، صفر باشد. قضیهٔ ۱ در اینجا هم درست است. یعنی اگر $q(r) = 0$، آنگاه چندجمله‌ای $p(x) = (x - r)^n$ با $q(x)$ ناهم‌قطب است.

بیایید حالتی خاص را در نظر بگیریم. فرض کنید $q(x)$ یک چندجمله‌ای درجهٔ دو و $p(x)$ یک چندجمله‌ای درجهٔ سه باشد:

$$q(x) = x^2 + 2b_1 x + b_2$$

و

$$p(x) = x^3 + 3a_1 x^2 + 3a_2 x + a_3$$

در این صورت در نمادگذاری شبح‌وار خواهیم داشت

$$A(q(x), p(x)) \cong (\beta - \alpha)^2 (x - \alpha) =$$
$$(\beta^2 - 2\alpha\beta + \alpha^2)x - \alpha\beta^2 + 2\alpha^2\beta - \alpha^3$$

با محاسبهٔ تابعگون خطی E، نمایش صریح زیر را برای ناوردای ناهم‌قطبی به‌دست می‌آوریم

$$A(q(x), p(x)) = E((\beta^2 - 2\alpha\beta + \alpha^2)x - \alpha\beta^2 + 2\alpha^2\beta - \alpha^3)$$
$$= (b_2 - 2a_1 b_1 + a_2)x - a_1 b_2 + 2a_2 b_1 - a_3$$

بنابراین چندجمله‌ای درجهٔ دوی $q(x)$ و چندجمله‌ای درجهٔ سهٔ $p(x)$ ناهم‌قطب‌اند اگر و تنها اگر ضرایبشان در دو معادلهٔ زیر صدق کنند

$$b_2 - 2a_1 b_1 + a_2 = 0$$
$$-a_1 b_2 + 2a_2 b_1 - a_3 = 0$$

با به کارگیری این معادلات می‌توانیم دو قضیهٔ مهم را ثابت کنیم:

قضیهٔ ۲. به ازای هر چندجمله‌ای درجهٔ سهٔ داده شده، در حالت کلی، دقیقاً یک چندجمله‌ای درجهٔ دو (یکین) وجود دارد.

برهان. در واقع معادلات بالا را باید به‌صورت زیر بازنویسی کنیم

$$b_2 - 2a_1 b_1 = -a_2,$$
$$-a_1 b_2 + 2a_2 b_1 = a_3$$

جوابهای b_1 و b_2 به ازای a_1، a_2، و a_3ی داده شده، در حالت کلی یکتا هستند.

قضیهٔ ۳. همواره یک فضای یک‌بعدی از چندجمله‌ای‌های (یکین) درجهٔ سه موجود است که با یک چندجمله‌ای درجهٔ دوی مفروض ناهم‌قطب‌اند.

برهان. در واقع، برای b_1 و b_2ی داده شده، می‌توانیم جوابهای a_1، a_2، و a_3 را از معادلات زیر به‌دست آوریم:

$$-2a_1 b_1 + a_2 = -b_2,$$
$$-a_1 b_2 + 2a_2 b_1 = a_3$$

در قدیم معمول بود که بگویند این معادلات همواره بینهایت جواب دارند.

قضایای ۲ و ۳ روشی ساده و صریح برای حل معادلات درجهٔ ۳ به‌دست می‌دهند. این روش، از این قرار است. چندجمله‌ای درجهٔ سهٔ

$$p(x) = x^3 + 3a_1 x^2 + 3a_2 x + a_3$$

داده شده است. ابتدا، طبق قضیهٔ ۲، چندجمله‌ای درجهٔ دوی یکتای $q(x)$ را پیدا می‌کنیم که ناهم‌قطب با $p(x)$ باشد. این چندجمله‌ای در حالت کلی دارای دو ریشهٔ مختلف r_1 و r_2 است. بنا به قضیهٔ ۱، چندجمله‌ای‌های درجهٔ سهٔ $(x - r_1)^3$ و $(x - r_2)^3$ با $q(x)$ ناهم‌قطب‌اند. در ادامه، بنا به قضیهٔ ۳، فضای خطی آفین چندجمله‌ای‌های درجهٔ سهٔ ناهم‌قطب با $q(x)$ دارای بعد ۲ است. چون $p(x)$ ناهم‌قطب با $q(x)$ است، نتیجه می‌گیریم که $p(x)$ ترکیب خطی $(x - r_1)^3$ و $(x - r_2)^3$ است. به زبان نمادی، به ازای ثابتی مثل c:

$$p(x) = c(x - r_1)^3 + (1 - c)(x - r_2)^3$$

می‌بینید که c، r_1، و r_2 با حل معادلات خطی و درجهٔ دو محاسبه می‌شوند. با این روش، حل معادلهٔ درجهٔ سهٔ $p(x) = 0$ به حل معادلهٔ

$$c(x - r_1)^3 = -(1 - c)(x - r_2)^3$$

تبدیل می‌شود و این معادله با به‌دست آوردن ریشهٔ سوم به آسانی حل می‌شود. این روش حل معادلهٔ درجهٔ سوم تنها روشی است که من می‌توانم به یاد بیاورم.

اجازه دهید با ذکر یک خاطرهٔ شخصی بامزه کمی از بحث خارج شوم. چند سال قبل من مشغول سخنرانی در بارهٔ این موضوع در کنفرانسی در زمینهٔ ترکیبیات در محل دانشگاه مینه سوتا بودم. پرسی دایاکونیس در ردیف جلو نشسته بود و می‌توانم بگویم هنگامی‌که من شروع به صحبت کردم او داشت به خواب می‌رفت. بالاخره شروع به چرت‌زدن کرد ولی در لحظه‌ای که من کلمات جادویی «حل معادلهٔ درجهٔ سه» را ذکر کردم، با تکانی از خواب پرید و گفت: «راستی! چطور؟»

دو قضیهٔ پیشین به آسانی تعمیم می‌یابند.

قضیهٔ ۴. در حالت کلی، اگر $k \leq n$، بعد فضای همهٔ چندجمله‌ای‌های (یکین) از درجهٔ k که با یک چندجمله‌ای از درجهٔ n ناهم‌قطب‌اند، $2k - n$ است.

قضیهٔ ۵. اگر $k \leq n$، بعد فضای همهٔ چندجمله‌ای‌های (یکین) از درجهٔ n که ناهم‌قطب با یک چندجمله‌ای از درجهٔ k اند، برابر k است.

سعی می‌کنیم معادلهٔ درجهٔ ۵ را به همان روشی حل کنیم که معادلهٔ درجهٔ ۳ را حل کردیم. چندجمله‌ای درجهٔ ۵

$$p(x) = x^5 + 5a_1 x^4 + 10a_2 x^3 + 10a_3 x^2 + 5a_4 x + a_5 = 0$$

داده شده است. قضیهٔ ۴ تضمین می‌کند که در حالت کلی یک چندجمله‌ای درجهٔ سهٔ یکتای $q(x)$ موجود است که با $p(x)$ ناهم‌قطب است. این چندجمله‌ای درجهٔ سه در حالت کلی دارای سه ریشهٔ متمایز r_1، r_2، و r_3 است. بنا به قضیهٔ ۱، چندجمله‌ای‌های $(x-r_1)^5$، $(x-r_2)^5$ و $(x-r_3)^5$ مستقل خطی‌اند و با $q(x)$ ناهم‌قطب‌اند. طبق قضیهٔ ۵، بعد فضای همهٔ چندجمله‌ای‌های ناهم‌قطب با $q(x)$ برابر با ۳ است. ولی چندجمله‌ای $p(x)$ ناهم‌قطب با $q(x)$ است. بنابراین به ازای ثابتهای مناسب c_i، $p(x)$ را می‌توان به‌صورت زیر نوشت:

$$p(x) = c_1(x-r_1)^5 + c_2(x-r_2)^5 + c_3(x-r_3)^5$$

پس می‌بینیم که چندجمله‌ای عمومی درجهٔ ۵ را می‌توان به‌صورت ترکیبی خطی از توانهای پنجم سه چندجمله‌ای خطی نوشت. اینها را می‌شود با حل‌کردن معادلات خطی، درجهٔ دو و درجهٔ سه محاسبه کرد. این‌گونه تحویل معادلهٔ درجهٔ ۵ به یک شکل متعارف، بیشترین حدی است که می‌توان به حل معادلهٔ درجهٔ ۵ نزدیک شد.

در این لحظه، یکی از حضار دستش را بلند خواهد کرد و خواهد گفت: «ببخشید، ولی این روش شبح‌وار که شما معرفی کرده‌اید حتی برای نمایش مبین معادلهٔ درجهٔ دو هم کافی نیست».

کاملاً درست است. تعاریف اشباح و تابعک خطی E تعمیمی سرراست به هر تعداد چندجمله‌ای $p_1(x)$، $p_2(x)$، $\cdots$، $p_l(x)$ دارند. کافی است فضای چندجمله‌ای‌های

$$\mathbb{C}[x, \alpha_1, \alpha_2, \cdots, \alpha_l]$$

را در نظر گرفت و $E(\alpha_i^j)$ را مساوی jامین ضریب چندجمله‌ای $p_i(x)$ قرار داد. نکتهٔ حیاتی آن است که تابعک خطی E باز هم نسبت به اشباح متمایز، ضربی باشد:

$$E(\alpha_1^i\alpha_2^j\alpha_3^k\cdots x^l) = E(\alpha_1^i)E(\alpha_2^j)E(\alpha_3^k)\cdots x^l$$

در اینجا نکتهٔ ظریف جریان پدیدار می‌شود: چندجمله‌ای‌های $p_1(x)$، $p_2(x)$، $\cdots$، $p_l(x)$ لزومی ندارد متمایز باشند. درواقع مهمترین حالت وقتی اتفاق می‌افتد که هر یک از چندجمله‌ای‌های $p_1(x)$، $p_2(x)$، $\cdots$، $p_l(x)$ مساوی یک $p(x)$ باشند. در این حالت تعریف تابعک خطی E می‌تواند به شکل زیر ساده شود

۱. برای هر i

$$E(\alpha_i^j) = a_j$$

۲. به ازای همهٔ اعداد صحیح نامنفی i، j، k، $\cdots$، l

$$E(\alpha_1^i\alpha_2^j\alpha_3^k\cdots x^l) = a_i a_j a_k \cdots x^l$$

اشباح α_1، α_2، $\cdots$، α_l را که در موارد ۱ و ۲ صدق می‌کنند اشباح مبادله‌پذیر گویند. پس برای اشباح مبادله‌پذیری داریم

$$(x+\alpha_1)^n \cong (x+\alpha_2)^n$$

اریک تمپل بل که به جای $\cong$ می‌نوشت $=$، از این نکته که دو شبح می‌توانند مبادله‌پذیر باشند بی‌آنکه برابر باشند، متحیر بود.

من اکنون می‌توانم قضیهٔ اصلی نظریهٔ ناورداها را در حالت یک چندجمله‌ای بیان کنم.

قضیهٔ ۶. هر ناوردای چندجمله‌ای $p(x)$ به‌صورت یک چندجمله‌ای از تفاضلهای $\alpha_i - \alpha_j$ و $\alpha_i - x$ است که α_i و α_j اشباح مبادله‌پذیرند، به‌عکس، هر چندجمله‌ای از چنین تفاضلهایی با یک ناوردای چندجمله‌ای $p(x)$ هم‌ارز است.

برهان بی‌اندازه ساده است، ولی در اینجا نمی‌آید.

بیایید چند مثال کلاسیک را مرور کنیم. مبین چندجمله‌ای درجهٔ دوم $p(x) = x^2 + 2a_1x + a_2$ را می‌توان به‌صورت شبح‌وار نمایش داد:

$$D(p(x)) \cong (\alpha_1 - \alpha_2)^2/2$$

که α_1 و α_2 اشباحی مبادله‌پذیرند. درواقع

$$\begin{aligned} E((\alpha_1-\alpha_2)^2) &= E(\alpha_1^2) - 2E(\alpha_1\alpha_2) + E(\alpha_2^2) \\ &= a_2 - 2a_1^2 + a_2 = 2(a_2 - a_1^2) \end{aligned}$$

فهوالمطلوب.

برای مثال بعدی، چندجمله‌ای درجهٔ سهٔ

$$p(x) = x^3 + 3a_1x^2 + 3a_2x + a_3$$

را در نظر بگیرید. مبین این چندجمله‌ای که آن را با $D(p(x))$، نمایش می‌دهیم مساوی است با عبارت زیر (با صرفنظرکردن از یک ثابت ضربی)

$$D(p(x)) = 6a_1^2a_2^2 - 8a_2^3 - 8a_1^3a_3 + 12a_1a_2a_3 - 2a_3^2$$

ولی نمایش شبح‌وار مبین را راحت‌تر می‌توان به خاطر سپرد:

$$D(p(x)) \cong (\alpha_1-\alpha_2)^2(\alpha_3-\alpha_4)^2(\alpha_1-\alpha_4)(\alpha_2-\alpha_3)$$

همان‌طور که می‌بینید مبین صفر است اگر و تنها اگر معادلهٔ درجهٔ سهٔ $p(x) = 0$ دارای ریشهٔ مضاعف باشد.

هسیان[1] چندجمله‌ای درجهٔ سه به زیبایی در نمادگذاری شبح‌وار نمایش داده می‌شود:

$$H(p(x)) \cong (\alpha_1-\alpha_2)^2(\alpha_1-x)(\alpha_2-x)$$

هسیان صفر می‌شود اگر و تنها اگر چندجمله‌ای درجهٔ سه، توان سوم یک چندجمله‌ای درجهٔ یک باشد.

اجازه دهید یک‌بار دیگر حاشیه بروم. پس از شنیدن اینکه صفرشدن هسیان شرط مکعب کامل بودن چندجمله‌ای درجهٔ سه است، به‌طور طبیعی این سؤال کلی پیش می‌آید: کدام ناوردای یک چندجمله‌ای از درجهٔ n صفر می‌شود اگر و تنها اگر آن چندجمله‌ای kامین توان یک چندجمله‌ای از

1. Hessian

درجهٔ n/k باشد؟ در اینجا k یک مقسوم‌علیه n است. من مدتها فکر می‌کردم پاسخ این پرسش در دسترس نیست تا اینکه یک روز، هنگامی‌که داشتم جلد دوم مجموعهٔ آثار هیلبرت را ورق می‌زدم، تصادفاً متوجه شدم که هیلبرت مسأله را به‌طور کامل حل کرده است. جواب مسأله با ظرافت تمام در نمادگذاری شبح‌وار قابل نمایش است. این تنها یکی از نتایج درخشان هیلبرت در نظریهٔ ناورداهاست که به دست فراموشی سپرده شده است.

حال ناوردای دیگری از چندجمله‌ای درجهٔ پنج را در نظر می‌گیریم. قضیهٔ ۳ به ما می‌گوید که چندجمله‌ای درجهٔ پنجم

$$p(x) = x^5 + 5a_1x^4 + 10a_2x^3 + 10a_3x^2 + 5a_4x + a_5$$

دارای چندجمله‌ای ناهم‌قطب یکتای درجهٔ سهٔ $q(x)$ است. چندجمله‌ای $q(x)$ یک ناوردای $p(x)$ است. آیا $q(x)$ نمایش ساده‌ای در نمادگذاری شبح‌وار دارد؟ جواب مثبت و به صورت زیر است:

$$q(x) \cong$$
$$(\alpha_2-\alpha_3)^2(\alpha_3-\alpha_1)^2(\alpha_1-\alpha_2)^2(\alpha_1-x)(\alpha_2-x)(\alpha_3-x)$$

در آثار قدما ناوردای فوق را با حروف j نمایش می‌دادند.

هنگامی‌که ناوردای j صفر می‌شود چندجمله‌ای درجهٔ پنج $p(x)$ چه خاصیتی پیدا می‌کند؟

جواب این پرسش دلپسند است. ناوردای j از یک چندجمله‌ای درجهٔ پنج، متحد با صفر است اگر و تنها اگر آن چندجمله‌ای درجهٔ پنج با یک چندجمله‌ای نابدیهی از درجهٔ دو، ناهم‌قطب باشد. ولی در این‌صورت قضیهٔ ۵ به ما می‌گوید که چندجمله‌ای درجهٔ پنج را می‌توان به‌صورت زیر نوشت

$$p(x) = c(x-r_1)^5 + (1-c)(x-r_2)^5$$

که r_1 و r_2 ریشه‌های یک معادلهٔ درجهٔ دو هستند. بنابراین صفرشدن ناوردای j یک شرط لازم وکافی است برای آنکه چندجمله‌ای درجهٔ پنجی مانند $p(x)$ را بتوان به‌صورت مجموع دو توان پنجم (به جای سه توان پنجم) از چندجمله‌ای‌های خطی نوشت. در این حالت معادلهٔ درجهٔ پنج $p(x) = 0$ را می‌توان با رادیکالها حل کرد:

با استدلالهای مشابهی می‌توان همهٔ ناورداهایی را محاسبه کرد که صفرشدنشان، حلپذیری الگوریتمی معادلهٔ درجهٔ پنج را با رادیکالها ایجاب کند. کیلی اولین کسی بود که نشان داد بیست‌وسه ناوردا در این ماجرا نقش دارند.

قضیهٔ هیلبرت در بارهٔ متناهی‌مولد بودن حلقهٔ ناورداها را می‌توان در زبان اشباح بازنویسی کرد و اثباتی ترکیبیاتی برای آن به‌دست داد که مستقل از قضیه پایهٔ هیلبرت باشد.

در خاتمه، بگذارید کمی در بارهٔ دلیل دیگر کنار گذاشته شدن روش سمبلیک در نظریهٔ ناورداها صحبت کنیم. گفتن حقیقت در ریاضیات بی‌اندازه دشوار است. توصیف صوری ریاضیات همهٔ حقیقت را نمی‌گوید. حقیقت یک نظریهٔ ریاضی را محتملاً وقتی بیشتر درک می‌کنیم که اشارات خودمانی متخصصی، انگیزه‌های پنهان نظریه را لو می‌دهد، یا بر مثالهای نوعی مسلط می‌شویم، یا وقتی کشف می‌کنیم که مسائل واقعی در پس مسائل نمایشی چه بوده‌اند. فلاسفه و روانشناسان باید توضیح دهند که چرا ما ریاضیدانان عادت کرده‌ایم به‌طور حساب شده‌ای ردپای خود را محو کنیم. دانشوران رشته‌های دیگر همواره با دیدهٔ تعجب و تردید به این عادت ریاضیدانان می‌نگریسته‌اند، عادتی که از زمان فیثاغورس تا امروز تغییر چندانی نکرده است.

هدف نهانی روش سمبلیک در نظریهٔ ناورداها صرفاً یافتن عبارت ساده‌ای برای ناورداها نبود. اعتقادی عمیقتر راهنمای این روش بوده است. انتظار می‌رفت که نمایش ناورداها با روش سمبلیک نهایتاً ما را به سمت انتخاب ناورداهای «ذی‌ربط» یا «مهم» از بین انواع نامتناهی آنها سوق دهد. این امید وجود داشت که تعبیر صفرشدن یک ناوردا را بتوان از نمایش شبح‌وار آن به‌دست آورد. از بین رفتن این اعتقاد دلیل اصلی زوال نظریهٔ کلاسیک ناورداها بود و امروز احیاء آن دلیل تجدید حیات نظریهٔ ناورداهاست.

اینکه در جایی که قدما شکست خورده‌اند موفق شویم یا نشویم، مشخص نیست. چند سالی منتظر باشید. اگر اعتقادی به موفقیت نداشتم، این سخنرانی را ارائه نمی‌کردم.

از توجه شما سپاسگزارم.

مراجع

1. Di Crescenzo, Antonio, and Rota, Gian-Carlo, Sul calcolo umbrale, *Ricerche Matematica* **XLIII** (1994), 129-162.

2. Ehrenborg, Richard, and Rota, Gian-Carlo, Apolarity and canonical forms for homogeneous polynomials, *Eur. J. Combinatorics* **14** (1993), 157-181.

3. Grosshans, Frank D., Rota, Gian-Carlo, and Stein, Joel A., *Invariant Theory and Superalgebras*, CBMS Regional Conferences in Mathematics Vol. 69, Providence, RI: American Mathematical Society (1987).

4. Kung, J. P. S., and Rota, Gian-Carlo, The invariant theory of binary forms, *Bull. Am. Math. Soc.* (2) **10** (1984), 27-85.

5. Metropolis, N., and Rota, Gian-Carlo, Symmetry classes: functions of three variables, *Am. Math. Monthly* **98** (1991), 328-332.

6. Metropolis, N., Rota, G.-C. and Stein, Joel A., Theory of symmetry classes, *Proc. Nat. Acad. Sci.* **88** (1991), 8415-8419.

7. Metropolis, N., Rota, Gian-Carlo, and Stein, Joel A., Symmetry classes of functions, *J. Alg.* **171** (1995), 845-866.

8. Rota, Gian-Carlo, and Taylor, B. D. The classical umbral calculus, *SIAM J. Math. Anal.* **25** (1994), 694-711.

* * * * * *

• Gian-Carlo Rota, "Two turning points in invariant theory", *Math. Intelligencer*, (1) **21** (1999) 20-27.

این سخنرانی، متن دومین سخنرانی از سخنرانیهای سمینار (Colloquium Lectures) در نشست سالانهٔ انجمن ریاضی آمریکاست که در ۸ ژانویهٔ ۱۹۹۸ ایراد شده است.

* جیان‌کارلو روتا در هنگام نوشتن این مقاله در دانشگاه ام. آی. تی مشغول کار بوده است.

تصویرهای ترکیبیاتی•

جیان‌کارلو روتا*
ترجمهٔ روزبه توسرکانی

وقتی که به دبیرستان می‌رفتم، دبیر ادبیات انگلیسی داستانی از جیمز تربر[1] به نام «زندگی پنهان والتر می‌تی»[2] را برای مطالعه به من داد. من هر چند سال یک‌بار این داستان را خوانده‌ام، و به این نتیجه رسیده‌ام که هر کس یک «عقدهٔ والتر می‌تی» دارد.

یک راه برای شناختن یک شخص می‌تواند کشف «خیالبافی‌های والتر می‌تی» او باشد.

بیشتر افکار ریاضی ما در دبیرستان یا در دورهٔ پیش‌دانشگاهی خیالبافی‌های والتر می‌تی بودند. هنگامی که مطلب ریاضی جدیدی را فرا می‌گرفتیم، خودمان را در حال خیالبافی در بارهٔ تعمیمهای احتمالی آن مطلب می‌یافتیم. همین که ضرایب دوجمله‌ای را فهمیدیم، در بارهٔ تعمیم آن به حالتی که مخرج منفی است، خیالبافی کردیم. به محض آنکه چیزی در بارهٔ مشتقات آموختیم، به سمت مشتقات از مرتبهٔ کسری خیز برداشتیم. اگر زمانی با تابع زتای ریمان آشنا شده‌ایم، دچار افکار رمانتیکی در بارهٔ تعبیر جدیدی از این تابع که راز آن را آشکار کند شده‌ایم.

به این سخنرانی می‌بایست عنوان دیگری داده می‌شد. باید «دورهٔ بعدی زندگی والتر می‌تی» نام می‌گرفت. این سخنرانی شامل یک رشته «تصویر» جسورانه است که توسط یک والتر می‌تی که خجالت را کنار گذاشته، نمایش داده می‌شوند. هر تصویر با یک خیالبافی سرخوشانه سروکار خواهد داشت که کم‌وبیش به حقیقت پیوسته است.

اولین تصویر: مثالی از ترکیبیات پیش‌متناهی

بیایید با یک داستان تاریخی‌ـتخیلی آغاز کنیم و تصور کنیم که ریمان چگونه ممکن است تابع زتای ریمان را کشف کرده باشد.

پروفسور ریمان می‌دانست که چگالی حسابی از اهمیتی بنیادی در نظریهٔ اعداد برخوردار است. اگر A زیرمجموعه‌ای از مجموعهٔ اعداد صحیح مثبت $\mathbb{N}$ باشد، آنگاه چگالی حسابی مجموعهٔ A، هرگاه حد زیر وجود داشته باشد، به صورت زیر تعریف می‌شود

$$\operatorname{dens}(A) = \lim_{n\to\infty} \frac{1}{n}||A \cap \{1, 2, \cdots, n\}||$$

به عنوان مثال $\operatorname{dens}(\mathbb{N}) = 1$. اگر A_p مجموعهٔ مضربهای عدد اول p باشد، آنگاه $\operatorname{dens}(A_p) = 1/p$. جالبتر از همه اینکه با محاسبهٔ ساده‌ای می‌توان نشان داد که برای هر دو عدد اول p و q، $\operatorname{dens}(A_p \cap A_q) = 1/pq$. اگر چگالی یک اندازهٔ احتمال (شمارا‌ـجمعی) بود، نتیجه می‌گرفتیم که پیشامدهای بخش‌پذیربودن یک عدد به‌تصادف انتخاب شده بر هر یک از دو عدد اول مستقل هستند. متأسفانه، چگالی حسابی برخی ــ و نه همهٔ ــ ویژگیهای یک اندازهٔ احتمال را دارد. از همه واضحتر اینکه شمارا‌ـجمعی نیست.

پروفسور ریمان پس از یک دوره کنکاش و تعمق در اندیشه‌هایش، موفق شد چاره‌ای برای برخی کاستیهای چگالی حسابی پیدا کند. وی یک عدد حقیقی $s > 1$ را انتخاب و اندازهٔ عدد صحیح مثبت n را مساوی $1/n^s$ تعریف کرد. به این ترتیب اندازهٔ مجموعهٔ $\mathbb{N}$ مساوی مقدار زیر به‌دست آمد

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

بنابراین او توانست یک اندازهٔ احتمال (شمارا‌ـجمعی) P_s روی مجموعهٔ اعداد صحیح مثبت $\mathbb{N}$ با قراردادن

$$P_s(A) = \frac{1}{\zeta(s)} \sum_{n\in A} \frac{1}{n^s}$$

1. James Thurber

۲. این داستان تحت همین عنوان به قلم احمد گلشیری ترجمه شده و در مجموعهٔ «داستان و نقد داستان» جلد اول، به چاپ رسیده است ــ م.

تعریف کند. سپس ریمان به سمت اثبات آنچه در تمام مدت احساس می‌کرد گام برداشت، یعنی ویژگی بنیادی

$$P_s(A_p \cap A_q) = P_s(A_p)P_s(A_q) = \frac{1}{pq}$$

به عبارت دیگر پیشامدهای A_p و A_q یعنی بخش‌پذیری یک عدد صحیح به تصادف انتخاب شدهٔ n بر هر یک از دو عدد اول p یا q نسبت به احتمال P_s مستقل هستند.

بالاخره تابع زتای ریمان به درد چیزی می‌خورد.

من اکنون از ترفندی لفظی استفاده خواهم کرد که بوخنر یکی از استادان دورهٔ کارشناسیم آن را به‌طور مؤثری به‌کار می‌گرفت. در کلاس درس، پروفسور بوخنر کلمات زیر را به‌عنوان پیش‌درآمد صورت قضیه بیان می‌کرد: «براساس فرضهایی فنی، قضیهٔ زیر درست است»، صد البته بدون آنکه هرگز فاش کند که فرضهای فنی او چه بوده‌اند.

سپس پروفسور ریمان به نشان‌دادن این موضوع پرداخت که براساس فرضهایی فنی روی مجموعه A،

$$\lim_{s \to 1} P_s(A) = \mathrm{dens}(A)$$

پس گرچه چگالی حسابیْ یک تابع احتمال نیست، تحت شرایط مناسبی حد توابع احتمال است.

مدتها پس از درگذشت ریمان، مجدداً براساس فرضهایی فنی، نشان داده شد که احتمالهای P_s تنها احتمالهایی هستند که روی مجموعهٔ اعداد طبیعی $\mathbb{N}$ تعریف می‌شوند به‌طوری که برای آنها پیشامدهای بخش‌پذیری بر اعداد اول متفاوت مستقل هستند. به نظر می‌رسد که این واقعیت پشتوانه‌ای برای برنامهٔ اثبات حکمهایی در نظریهٔ اعداد به وسیله روشهای احتمالاتی براساس تابع زتای ریمان است.

چرا پروفسور ریمان هرگز این ایدهٔ درخشانش را منتشر نکرد؟ یافتن پاسخ چندان دشوار نیست. درست است که با استفاده از این فرایند حدی برخی از قضیه‌های نظریهٔ اعداد به‌صورت احتمالاتی قابل اثبات هستند ــ مانند قضیهٔ دیریکله در بارهٔ اعداد اول در تصاعدهای حسابی ــ اما تاکنون قضایای عمیقتر نظریهٔ اعداد از دسترس این رهیافت دور مانده‌اند. به‌عنوان مثال هیچ‌کس با این روش موفق به اثبات قضیهٔ اعداد اول نشده است. پروفسور ریمان با آگاهی از این کاستی، یادداشتهای خودش را در سطل زباله انداخت و از راهی کاملاً متفاوت، با بیان فرضی که نام او را بر خود دارد و تا امروز حل نشده باقی مانده است، به برقراری پیوند بین تابع زتای ریمان و توزیع اعداد اول پرداخت.

چرا این داستان تاریخی‌ـتخیلی کوتاه را برای شما نقل می‌کنم؟ چون می‌خواهم تعبیر احتمالاتی دیگری از تابع زتای ریمان پیشنهاد کنم که با تعبیری که هم اینک مطرح شد به کلی متفاوت است.

بیایید به بررسی یک مسألهٔ شمارشی ترکیبیاتی بپردازیم. یک گروه دوری مرتبهٔ r، مانند C_r را در نظر می‌گیریم. هر مشخصهٔ χ از گروه C_r، هسته‌ای دارد که زیرگروهی از C_r است. در حالت کلی هر دنبالهٔ χ_1، χ_2، $\cdots$، χ_s از مشخصه‌های C_r هستهٔ توأمی دارند که زیرگروهی از C_r است؛ هستهٔ توأم دنباله‌ای از مشخصه‌ها چیزی نیست جز اشتراک هسته‌های آنها. اگر یک دنبالهٔ χ_1، χ_2، $\cdots$، χ_s از s مشخصه به طور مستقل و تصادفی انتخاب شده باشند، احتمال آنکه هستهٔ توأم دنباله مساوی زیرگروه داده شده‌ای از C_r مانند C_n باشد، چقدر است؟

احتمال این پیشامد که هستهٔ یک مشخصهٔ به تصادفْ انتخاب شده، شامل زیرگروه C_n باشد $1/n$ است، چون r مشخصه برای گروه C_r وجود دارد و r/n تا از چنین مشخصه‌هایی روی C_n صفر خواهند شد. بنابراین احتمال آنکه هستهٔ توأم یک دنبالهٔ به تصادف انتخاب شدهٔ χ_1، χ_2، $\cdots$، χ_s از s مشخصه، شامل زیرگروه C_n باشد برابر است با $(1/n)^s$. اگر احتمال آن را که هستهٔ توأم مشخصه‌های χ_1، χ_2، $\cdots$، χ_s مساوی زیرگروه C_n شود با P_{C_n} نمایش دهیم، آنگاه اتحاد زیر را داریم

$$\frac{1}{n^s} = \sum_{n|d|r} P_{C_d}$$

اینجا از این واقعیت استفاده کرده‌ایم که مجموعهٔ جزئاً مرتب زیرگروههای یک گروه دوری C_r با مجموعهٔ جزئاً مرتب شمارنده‌های عدد صحیح r یکریخت است.

اکنون از فرمول وارون موبیوس در نظریهٔ اعداد استفاده می‌کنیم. از این طریق به‌دست می‌آوریم

$$P_{C_n} = \sum_{n|d|r} \mu\left(\frac{d}{n}\right)\frac{1}{d^s}$$

اینجا $\mu(j)$ تابع موبیوس در نظریه اعداد است.

پس از تعویض متغیر $d = nj$ می‌توانیم عبارت سمت راست را به‌صورت زیر بازنویسی کنیم:

$$P_{C_n} = \frac{1}{n^s}\sum_{j} \mu(j)\frac{1}{j^s}$$

متغیر j در سمت راست روی زیرمجموعه‌ای از شمارنده‌های عدد صحیح r که لازم نیست نگران آن باشیم تغییر می‌کند.

حال اگر مجموع سمت راست روی همهٔ اعداد صحیح مثبت j تغییر می‌کرد، آنگاه عبارت سمت راست مساوی می‌شد با

$$\frac{1}{n^s}\,\frac{1}{\zeta(s)}$$

یعنی عبارت سمت راست می‌توانست برحسب عکس تابع زتای ریمان بیان شود. اگر بتوانیم مسألهٔ ترکیبیاتی خود را چنان تغییر دهیم که در سمت راستْ یک مجموع نامقید به‌دست آوریم، آنگاه یک تعبیر احتمالاتی از تابع زتای ریمان خواهیم داشت.

برای این کار به‌جای گروه دوری متناهی C_n، یک گروه دوری پیش‌متناهی در نظر گرفته می‌شود. گروه C_∞ از اعداد گویا به پیمانهٔ ۱ را در نظر بگیرید. برای هر عدد صحیح مثبت n، گروه C_∞ یک زیرگروه متناهی یکتای C_n

با n عضو دارد. گروه مشخصهٔ C^*_∞ از C_∞ یک گروه فشرده است؛ و یک اندازهٔ هار دارد که یک اندازهٔ احتمال P است. گروه C^*_∞، گروه پیش‌متناهی مطلوب است که روی آن می‌توانیم محاسبهٔ پیشین را تعمیم دهیم.

مجموعهٔ همهٔ مشخصه‌های گروه C_∞ (یعنی مجموعهٔ همهٔ عضوهای گروه C^*_∞) که روی یک زیرگروه C_n از C_∞ صفر می‌شوند، دارای اندازهٔ هار $1/n$ است. پس اگر یک دنبالهٔ χ_1، χ_2، $\cdots$، χ_s از s مشخصهٔ C_∞ را به‌طور مستقل و به تصادف انتخاب کنیم، احتمال آنکه هستهٔ توأم آنها شامل گروه C_n باشد مساوی $(1/n)^s$ است. اگر مجدداً احتمال آن‌را که هستهٔ توأم دنبالهٔ χ_1، χ_2، $\cdots$، χ_s از s مشخصه مساوی گروه C_n گردد با P_{C_n} نمایش دهیم، آنگاه اتحاد زیر را داریم

$$\frac{1}{n^s} = \sum_{n|d} P_{C_d}$$

که اکنون مجموع سمت راستْ نامتناهی است. دوباره با استفاده از فرمول وارون موبیوس به‌دست می‌آوریم

$$P_{C_n} = \sum_{n|d} \mu(\frac{d}{n})\frac{1}{d^s} = \frac{1}{n^s}\frac{1}{\zeta(s)}$$

این همان تعبیر احتمالاتی موعود برای تابع زتای ریمان است. با استفاده از این تعبیر برخی ویژگیهای تابع زتای ریمان به‌طور احتمالاتی قابل اثبات هستند ــ به‌عنوان مثال فرمول ضرب. باقی می‌ماند که ببینیم کدام ویژگیهای دیگر تابع زتای ریمان به این طریق قابل اثبات هستند.

بحث بالا نمونه‌ای از تعمیم یک مسألهٔ شمارش روی مجموعه‌ای متناهی به شمارش روی یک مجموعهٔ پیش‌متناهی است. چنین جایگزین کردن یک مجموعهٔ متناهی با یک «مجموعهٔ» پیش‌متناهی در دیگر مسأله‌های ترکیبیاتی نیز میسر است. آیا هرگز یک ترکیبیات پیش‌متناهی، شانه به شانهٔ ترکیبیات مجموعه‌های متناهی خواهیم داشت؟

دومین تصویر: مشتق دوری

مشتق معمولی یک چندجمله‌ای یک‌متغیره توسط هاوسدورف به چندجمله‌ایها و سریهای توانی صوری با متغیرهای ناجابجایی به صورت زیر تعمیم داده شده است. جبر شرکت‌پذیر $\mathbb{C}\langle a, b, \cdots, c, x\rangle$ را که توسط مجموعه‌ای از حرفها مانند $\{a, b, \cdots, c, x\}$ تولید شده در نظر بگیرید. حرف x متغیر نامیده می‌شود. همه حرفهای دیگر ثابت نامیده می‌شوند. یک تک‌جمله‌ای در این جبر شرکت‌پذیر همان چیزی است که فکر می‌کنید باید باشد، کلمه‌ای مانند

$$m = axbax^3bcxd$$

هر چندجمله‌ای، ترکیبی خطی از تک‌جمله‌ای‌هاست و سری توانی صوری به صورت مجموع نامتناهی تک‌جمله‌ای‌ها با قیدهای مناسبی روی رشد درجات جمعوندها تعریف می‌شود. سریهای توانی صوری با متغیرهای ناجابجایی، یک جبر $\mathbb{C}\langle\langle a, b, c, \cdots, x\rangle\rangle$ تشکیل می‌دهند. ما چنین سریهای توانی صوری را با $f(x)$ نمایش می‌دهیم.

مشتق هاوسدورف تک‌جمله‌ای m به صورت زیر محاسبه می‌گردد

$$\begin{aligned} H(m) &= H(axbax^3bcxd) \\ &= abax^3bcxd + 3axbax^2bcxd + axbax^3bcd \end{aligned}$$

این تعریف با استفاده از خطی بودن به چندجمله‌ای‌ها و سریهای توانی صوری تعمیم می‌یابد.

اگر m' یک تک‌جمله‌ای دیگر باشد، قاعدهٔ مورد انتظار برای یافتن مشتق هاوسدورف یک حاصلضرب را داریم:

$$H(mm') = H(m)m' + mH(m')$$

مشتق هاوسدورف یک نارسایی بزرگ دارد. به نظر می‌رسد که هیچ قاعده‌ای مشابه قاعدهٔ زنجیری برای مشتق‌گیری از یک تابع مرکب وجود ندارد، به‌عنوان مثال، مشتق هاوسدورف چندجمله‌ای $(ax)^n$، هنگامی‌که حرفهای a و x جابجا نمی‌شوند مساوی $n(ax)^{n-1}a$ نیست. در این مورد هیچ الگوی واضحی مشاهده نمی‌شود.

صورت دیگری از مفهوم مشتق وجود دارد که در یک قاعدهٔ زنجیری ساده تحت ترکیب تابعی صدق می‌کند. این همان مشتق دوری است که با حرف D نمایش داده می‌شود. مشتق دوری به‌صورت زیر تعریف می‌شود. ابتدا عملگر گرد کردن T را به‌صورت زیر تعریف می‌کنیم:

(الف) اگر اولین حرفِ یک تک‌جمله‌ای m، متغیر x نباشد، قرار می‌دهیم $T(m) = 0$.

(ب) اگر اولین حرفِ یک تک‌جمله‌ای m متغیر x نباشد به‌طوری که $m = xm'$، قرار می‌دهیم $T(m) = m'$.

(پ) این را با استفاده از خطی بودن به $\mathbb{C}\langle\langle a, b, \cdots, c, x\rangle\rangle$ تعمیم می‌دهیم.

مشتق دوری یک تک‌جمله‌ای m برحسب عملگر گرد کردن به‌صورت زیر تعریف می‌شود.

(الف) فرض می‌کنیم p یک چندجمله‌ای باشد که از جمع کردن همهٔ جایگشتهای دوری تک‌جمله‌ای m به‌دست آمده باشد.

(ب) قرار می‌دهیم $D(m) = T(p)$.

(پ) این را با استفاده از خطی بودن به همهٔ سریهای توانی صوری تعمیم می‌دهیم.

به‌عنوان مثال مشتق دوری تک‌جمله‌ای m در بالا، درگامهای زیر محاسبه می‌شود:

گام ۱. همهٔ جایگشتهای دوری تک‌جمله‌ای $axbax^3bcxd$ را می‌نویسیم. این جایگشتها عبارت‌اند از:

$$xbax^3bcxda,\ bax^3bcxdax,\ ax^3bcxdaxb,$$
$$x^3bcxdaxba,\ x^2bcxdaxbax,\ xbcxdaxbax^2,$$
$$bcxdaxbax^3,\ cxdaxbax^3b,\ xdaxbax^3bc,\ daxbax^3bcx$$

گام ۲. در فهرست بالا یکی از عملیات زیر را اجرا می‌کنیم:

(الف) اگر اولین حرف یک تک‌جمله‌ایْ x نباشد، آن تک‌جمله‌ای را از فهرست حذف می‌کنیم.

(ب) اگر اولین حرف یک تک‌جمله‌ای x باشد، حرف اول را حذف می‌کنیم.

وقتی که عملیات (a) و (b) را روی هر یک از تک‌جمله‌ای‌های فهرست بالا اجرا کنیم، فهرست کوتاه‌تری به دست می‌آوریم، یعنی

$$bax^{۳}bcxda,\ x^{۲}bcxdaxba,\ xbcxdaxbax,$$
$$bcxdaxbax^{۲},\ daxbax^{۳}bc$$

گام ۳. تک‌جمله‌ای‌ها را با هم جمع می‌کنیم تا مشتق دوری به‌دست آید:

$$\begin{aligned} D(m) &= D(axbax^{۳}bcxd) \\ &= bax^{۳}bcxda + x^{۲}bcxdaxba + xbcxdaxbax \\ &\quad + bcxdaxbax^{۲} + daxbax^{۳}bc \end{aligned}$$

مثالی دیگر به‌صورت زیر است: مشتق دوری تک‌جمله‌ای $axbxcxdx$ مساوی است با

$$\begin{aligned} &D(axbxcxdx) \\ &\quad = bxcxdxa + cxdxaxb + dxaxbxcx + axbxcxd \end{aligned}$$

بنابراین مشتق دوری تک‌جمله‌ای $(ax)^n$ مساوی $n(ax)^{n-۱}a$ است.

با محاسبهٔ مشابهی می‌توان به‌دست آورد $D(x+a)^n = n(x+a)^{n-۱}$ و برای سریهای توانی صوری خواهیم داشت $D(e^{x+a}) = e^{x+a}$ و $D(e^{ax}) = e^{ax}a$. به یاد داشته باشید که حرفهای a و x جابجا نمی‌شوند! در این مثالها مشتق هاوسدورف متناظر به‌هیچ‌وجه الگوی واضحی ندارد.

مشتق دوری از همهٔ ویژگیهای مورد انتظار مشتق معمولی برخوردار است، به‌ویژه در قاعدهٔ زنجیری برای ترکیب دو سری توانی صوری صدق می‌کند.

برای بیان قاعده‌های مشتق‌گیری دوری در حالت کلی، به عملگر دیگری که عملگر درهم‌پیچش[1] نامیده می‌شود، نیاز داریم. عملگر درهم‌پیچش به صورت زیر تعریف می‌شود. فرض کنید $c_۱$، $c_۲$، $\cdots$، c_n حرفهای دلخواهی باشند. اگر $g(x)$ یک سری توانی صوری باشد، قرار می‌دهیم

$$\begin{aligned} \langle Cc_۱c_۲\ldots c_n|g(x)\rangle &= c_۱c_۲\ldots c_ng(x) + c_۲\ldots c_ng(x)c_۱ \\ &\quad + c_۳\ldots c_ng(x)c_۱c_۲ + \ldots + c_ng(x)c_۱c_۲\ldots c_{n-۱} \end{aligned}$$

اگر $f(x)$ یک سری توانی صوری باشد، عملگر درهم‌پیچش

$$\langle Cf(x)|g(x)\rangle$$

با استفاده از خطی بودن تعریف می‌شود.

تعریف می‌کنیم

$$\langle D(f(x))|g(x)\rangle = T\langle Cf(x)|g(x)\rangle$$

به عنوان مثال

$$\langle D(f(x))|۱\rangle = D(f(x))$$

مشتق دوری حاصلضرب دو «تابع» توسط اتحاد زیر داده می‌شود

1. wrapping

$$D(f(x)g(x)) = \langle D(f(x))|g(x)\rangle + \langle D(g(x))|f(x)\rangle$$

به عنوان مثال به‌دست می‌آید

$$\begin{aligned} &D((۱-ax)^{-۱}(۱-bx)^{-۱}) = \\ &\qquad (۱-ax)^{-۱}(۱-bx)^{-۱}(۱-ax)^{-۱}a \\ &\qquad + (۱-bx)^{-۱}(۱-ax)^{-۱}(۱-bx)^{-۱}b \end{aligned}$$

چنین اتحادی برای مشتق هاوسدورف برقرار نیست.

مشتق دوری حاصلضرب هر دنباله‌ای از سریهای توانی صوری به‌طور مشابه با استفاده از عملگر درهم‌پیچش محاسبه می‌شود:

$$\begin{aligned} &D(f_۱(x)f_۲(x)\cdots f_n(x)) \\ &\quad = \langle D(f_۱(x))|f_۲(x)\cdots f_n(x)\rangle \\ &\quad + \langle D(f_۲(x))|f_۳(x)\cdots f_n(x)f_۱(x)\rangle \\ &\quad + \cdots + \langle D(f_n(x))|f_۱(x)f_۲(x)\cdots f_{n-۱}(x)\rangle \end{aligned}$$

اکنون به ویژگی اصلی مشتق دوری می‌رسیم: قاعدهٔ زنجیری. دو سری توانی صوری $f(x)$ و $g(x)$ در $\mathbb{C}\langle\langle a, b, \cdots, c, x\rangle\rangle$ داده شده است. فرض کنید که سری توانی صوری $g(x)$ جملهٔ ثابت ندارد. تحت این شرایط، ترکیب $f(g(x))$ با جایگذاری $g(x)$ در هر جایی که متغیر x در سری توانی صوری $f(x)$ ظاهر شده، خوش‌تعریف است. برای نمایش سری توانی صوری حاصل از جایگذاری $g(x)$ در هر جا که x در $D(f(x))$ یعنی مشتق دوری سری توانی صوری x، ظاهر شده است، می‌نویسیم $D_g(f(x))$. آنگاه قاعدهٔ زنجیری برای مشتق دوری به صورت زیر خواهد بود:

$$D(f(g(x))) = \langle Dg(x)|D_g(f(x))\rangle$$

به‌عنوان مثال داریم

$$D(e^{axbx}) = bxe^{axbx}a + e^{axbx}axb$$

یک مثال زیباتر به صورت زیر است:

$$D(e^{(۱-ax)^{-۱}}) = (۱-ax)^{-۱}e^{(۱-ax)^{-۱}}(۱-ax)^{-۱}a$$

می‌توان ثابت کرد که مشتق دوری یک سری توانی صوری گویا برحسب حرفهای ناجابجایی باز یک سری توانی ناجابجایی گویاست و همچنین مشتق دوری یک سری توانی صوری جبری برحسب حرفهای ناجابجایی باز یک سری توانی صوری جبری است.

با وجود شواهدِ دال بر اینکه مشتق دوریْ صورت طبیعی مشتق برای جبرهای ناجابجایی است، وضعیت کنونی این نظریه رضایت‌بخش نیست. مشتق دوری یک کشف تجربی است. لازم است که این نظریه در پناه یک نظریهٔ جبری گسترده‌تر قرار گیرد، همان‌طور که مشتق هاوسدورف در پناه نظریهٔ جبرهای هوپف قرار گرفته است.

سومین تصویر: لگاریتم و قضیهٔ دوجمله‌ای

فرمول مجموعیابی اویلر-مک‌لورن یکی از چشمگیرترین فرمولهای ریاضیات است. برای یک تابع مناسب $f(x)$ از یک متغیر حقیقی یا مختلط، این فرمول به صورت زیر بیان می‌شود:

$$\begin{aligned} f(x)+f(x+1)+f(x+2)+\cdots+f(x+n) \\ = B_0\int_x^{x+n+1} f(y)dy + B_1(f(x+n+1)-f(x)) \\ + \frac{B_2}{2!}D(f(x+n+1)-f(x)) \\ + \frac{B_3}{3!}D^2(f(x+n+1)-f(x))+\cdots \end{aligned}$$

B_nها اعداد برنولی‌اند و D عملگر مشتق معمولی است.

مفید بودن فرمول اویلر-مک‌لورن از کاربرد ۲۰۰ سالهٔ آن معلوم می‌شود. با این همه فرمول اویلر-مک‌لورن یک نارسایی جدی دارد. سری سمت راست تقریباً هرگز همگرا نیست، مگر آنکه به یک مجموع متناهی تقلیل یابد.

پرسش ما این است: آیا یک فضای برداری از توابع که شامل حداکثر ممکن از توابع مقدماتی باشد، و یک توپولوژی روی چنین فضای برداری که نسبت به آن، سمت راست فرمول اویلر-مک‌لورن یک سری همگرا باشد، وجود دارد؟

پاسخ این پرسش به‌طور غیرمنتظره‌ای به پاسخ پرسش دیگری مربوط است. تعمیم «راستین» ضرایب دوجمله‌ای $\binom{n}{k}$، هنگامی که k بتواند یک عدد صحیح منفی باشد کدام است؟ این پرسش به نوبهٔ خود ما را به پرسش سومی رهنمون می‌گردد. چگونه می‌توانیم دریابیم که تعمیمی از ضرایب دوجمله‌ای «راستین» است؟ پاسخ پرسش سوم آسان است: تعمیم ضرایب دوجمله‌ای «راستین» است اگر به تعمیمی ملموس از قضیهٔ دوجمله‌ای منجر شود:

$$(a+x)^n = \sum_{k=0}^{n}\binom{n}{k}a^k x^{n-k}$$

در جوانی قضیهٔ دوجمله‌ای را بدیهی می‌پنداشتم. [اما] فکر می‌کنم [بعداً] درسم را فرا گرفتم. یک فیلسوف مشهور، که نمی‌توانم نامش را به یاد بیاورم نوشته است که همهٔ عالم را می‌توان از روی یک دانه شن استنباط کرد. او می‌بایست اضافه می‌کرد که بخش بزرگی از ریاضیات را می‌توان با تأمل در قضیهٔ دوجمله‌ای استنتاج کرد.

چاره‌ای نیست جز اینکه وارد گود شویم و تعمیم «راستین» ضرایب دوجمله‌ای را بیان کنیم. ما معمولیترین راه را در پیش می‌گیریم، و ابتدا تعریف فاکتوریل را تعمیم می‌دهیم. پس، فرض کنید n یک عدد صحیح مثبت یا منفی باشد. فاکتوریل رومی $[n]!$ را به صورت زیر تعریف می‌کنیم:

$$[n]! = n! \qquad \text{اگر } n \geq 0$$

$$[n]! = \frac{(-1)^{n+1}}{(-n-1)!} \qquad \text{اگر } n < 0$$

این تعریف از کجا آمده است؟ می‌توانم به سادگی بگویم که این تعریف به کار ما می‌آید، اما این همهٔ حقیقت نیست. مقدار فاکتوریل رومی $[n]!$ برای n منفی برابر است با ماندهٔ تابع گاما به‌ازای عدد صحیح $-n-1$. با استفاده از فاکتوریل رومی، ضرایب رومی را به صورت زیر تعریف می‌کنیم:

$$\begin{bmatrix} n \\ k \end{bmatrix} = \frac{[n]!}{[k]![n-k]!}$$

هنگامی که $n \geq k \geq 0$، ضرایب رومی با ضرایب دوجمله‌ای یکسان هستند. برای همهٔ عددهای صحیح n و k، ضرایب رومی از همهٔ ویژگیهای مقدماتی ضرایب دوجمله‌ای، مانند مثلث پاسکال و غیره، بهره‌مند هستند. اما شگفتیهایی نیز در انبان دارند. به عنوان مثال داریم

$$\begin{bmatrix} 0 \\ -k \end{bmatrix} = \begin{bmatrix} 0 \\ k \end{bmatrix} = \frac{(-1)^{k+1}}{k}$$

آیا این هیچ معنای ملموسی دارد؟ بله، زیرا می‌توانیم با استفاده از این، تعمیمی از قضیهٔ دوجمله‌ای بیابیم. این تعمیم به صورت زیر است.

بسط سری توانی لگاریتم را به یاد آورید:

$$\log(x+a) = \log x + \sum_{k=1}^{\infty}\frac{(-1)^{k+1}}{k}\frac{a^k}{x^k}$$

این بسط سری توانی را می‌توانیم برحسب ضرایب رومی به صورت زیر بازنویسی کنیم

$$\log(x+a) = \log x + \sum_{k=1}^{\infty}\begin{bmatrix} 0 \\ k \end{bmatrix}\frac{a^k}{x^k}$$

به نظر می‌رسد این فرمول بتواند شبیه تعمیمی از قضیهٔ دوجمله‌ای شود که در آن لگاریتم نقش توان صفرم را ایفا می‌کند. بسط سری توانی دیگری که در آن ضرایب رومی ظاهر می‌شوند به صورت زیر است

$$\begin{aligned} (x+a)(\log(x+a)-1) = \\ x(\log x - 1) + a\log x + \sum_{k=2}^{\infty}\begin{bmatrix} 1 \\ k \end{bmatrix} a^k x^{1-k} \end{aligned}$$

آیا الگویی مشاهده می‌کنیم؟ بسیار خوب، بگذارید بسط سری توانی دیگری را آزمایش کنیم:

$$\begin{aligned} (x+a)^2\left(\log(x+a)-1-\frac{1}{2}\right) \\ = x\left(\log x - 1 - \frac{1}{2}\right) + \begin{bmatrix} 2 \\ 1 \end{bmatrix} ax(\log x - 1) \\ + \begin{bmatrix} 2 \\ 2 \end{bmatrix} a^2 \log x + \sum_{k=3}^{\infty}\begin{bmatrix} 2 \\ k \end{bmatrix} a^k x^{2-k} \end{aligned}$$

اکنون می‌توانیم به سوی یک تعمیم خیز برداریم. برای توابع مناسب $f(x)$ فرض می‌کنیم

$$D^{-1}f(x)$$

انتگرال نامعین یکتایی از تابع $f(x)$ باشد که جملهٔ ثابت صفر دارد. نگران نباشید، این عبارت لحظه‌ای دیگر معنی‌دار خواهد شد.

تعریف می‌کنیم

$$\lambda_n^{(1)}(x) = [n]!D^{-n}\log x$$

اینجا n یک عدد صحیح مثبت یا منفی است. تابعهای $\lambda_n^{(1)}(x)$، لگاریتمهای همساز مرتبهٔ ۱ نامیده می‌شوند. برای n مثبت داریم

$$\lambda_n^{(1)}(x) = x^n\left(\log x - 1 - \frac{1}{2} - \frac{1}{3} - \cdots - \frac{1}{n}\right)$$

و

$$\lambda_{-n}^{(1)}(x) = \frac{1}{x^n}$$

البته همچنین داریم

$$\lambda_0^{(1)}(x) = \log x$$

اکنون در وضعیتی هستیم که می‌توانیم تعمیم قضیهٔ دوجمله‌ای را با کمک لگاریتمهای همساز بیان کنیم. این تعمیم به صورت زیر است

$$\lambda_n^{(1)}(x+a) = \sum_{k=0}^{\infty}\begin{bmatrix} n \\ k \end{bmatrix} a^k \lambda_{n-k}^{(1)}(x)$$

سه اتحاد بالا حالتهای خاص این اتحاد به‌ازای $n = 0, 1, 2$ هستند.

از آنجا که تعمیم قضیهٔ دوجمله‌ای به لگاریتمهای همساز در مورد نماهای منفی به اتحاد زیر تقلیل می‌یابد، در این مورد هیچ چیز جدیدی به‌دست نمی‌دهد

$$(x+a)^{-n} = \sum_{k=0}^{\infty}\binom{-n}{k} a^k x^{-n-k}$$

اما برای نماهای مثبت یک تعمیم اصیل و حیرت‌انگیز از قضیهٔ دوجمله‌ای به‌دست می‌آوریم. این تعمیم بیان می‌کند که تابعهای $\lambda_n^{(1)}(x)$ برای n مثبت، در قضیهٔ دوجمله‌ای معمولی به پیمانهٔ توانهای منفی x صدق می‌کنند. به عبارت دیگر اتحاد زیر را داریم

$$(x+a)^n\left(\log(x+a) - 1 - \frac{1}{2} - \frac{1}{3} - \cdots - \frac{1}{n}\right)$$
$$\cong \sum_{k=0}^{n}\binom{n}{k} a^k x^{n-k}\left(\log x - 1 - \frac{1}{2} - \frac{1}{3} - \cdots - \frac{1}{n-k}\right)$$

این اتحاد به پیمانهٔ توانهای منفی x برقرار است. معجزات حذف در این اتحاد آشکار می‌شوند. ای کاش تعبیری ترکیبیاتی یا احتمالاتی از این تعمیم لگاریتمی قضیهٔ دوجمله‌ای می‌دانستم.

تا اینجا فرض کرده‌ایم که همهٔ سریها نسبت به توپولوژی اعداد مختلط همگرا هستند. اکنون در حالی‌که همگرایی را حفظ می‌کنیم، توپولوژی را تغییر خواهیم داد.

سرچشمه و زمینهٔ توپولوژی الگاریتمی که می‌خواهیم تعریف کنیم، جبر سریهای لورن صوری است. این جبر توپولوژیک را می‌توان با تعریف یک توپولوژی روی جبر تابعهای گویا با متغیر x و سپس تکمیل کردن این جبر نسبت به توپولوژی، تعریف کرد. این توپولوژی چنان انتخاب شده که داشته باشیم $\lim_{n\to\infty} x^{-n} = 0$. هر عضو جبر تکمیل شده یک سری لورن صوری یعنی یک سری به‌صورت

$$\sum_{n<d} a_n x^n$$

از کار درمی‌آید. ما می‌خواهیم فرایند تکمیل کردن مشابهی روی یک جبر دیگر اجرا کنیم: جبر تولیدشده توسط همهٔ تابعهای به شکل $x^n(\log x)^t$ که در آن n یک عدد صحیح مثبت یا منفی دلخواه و t یک عدد صحیح نامنفی است. برای مشخص کردن اینکه کدام عضوهای این جبر به سمت صفر همگرا می‌شوند، به پایهٔ خوش‌رفتارتری ازاین جبر نیاز داریم. این پایه توسط لگاریتمهای همساز با مرتبهٔ دلخواه t فراهم می‌شود. این لگاریتمها به صورت زیر تعریف می‌شوند.

$$\lambda_n^{(t)}(x) = [n]!D^{-n}(\log x)^t$$

برای هر عدد صحیح نامنفی t و هر عدد صحیح n. به عنوان مثال برای هر عدد صحیح نامنفی n داریم

$$\lambda_n^{(0)} = x^n$$

و برای n منفی

$$\lambda_n^{(0)}(x) = 0$$

فرمولهای صریحی برای لگاریتمهای همساز شناخته شده‌اند. برای لگاریتمهای همساز مرتبهٔ ۲ داریم $\lambda_0^{(2)}(x) = (\log x)^2$ و برای n مثبت

$$\lambda_n^{(2)}(x) = x^n\left((\log x)^2 - \left(2 + \frac{2}{2} + \cdots + \frac{2}{n}\right)\log x + 2 + \frac{2}{2}\left(1 + \frac{1}{2}\right) + \cdots + \frac{2}{n}\left(1 + \frac{1}{2} + \cdots + \frac{1}{n}\right)\right)$$

و

$$\lambda_{-n}^{(2)}(x) = 2x^{-n}\left(\log x - 1 - \frac{1}{2} - \cdots - \frac{1}{n-1}\right)$$

برای هر عدد صحیح نامنفی t، لگاریتمهای همساز مرتبهٔ t در همان تعمیم قضیهٔ دوجمله‌ای که هم‌اکنون برای لگاریتمهای همساز مرتبهٔ ۱ دیده‌ایم صدق می‌کنند:

$$\lambda_n^{(t)}(x+a) = \sum_{k=0}^{\infty}\begin{bmatrix} n \\ k \end{bmatrix} a^k \lambda_{n-k}^{(t)}(x)$$

لگاریتمهای همساز پایه‌ای برای جبر تولید شده توسط همهٔ تابعهای $x^n(\log x)^t$ هستند. یک توپولوژی روی این جبر با این شرط برای هر عدد صحیح نامنفی t

$$\lim_{n\to-\infty}\lambda_n^{(t)}(x) = 0$$

تعریف می‌کنیم. این توپولوژی، توپولوژی لگاریتمی نامیده می‌شود. تکمیل شدهٔ این جبر نسبت به توپولوژی لگاریتمی، جبر سریهای توانی صوری از نوع لگاریتمی یا جبر لگاریتمی است.

هر عضو جبر لگاریتمی یک ترکیب خطی از سریهای توانی همگرا به صورت

$$f(x) = \sum_{t,n\leq d} b_{n,t}\lambda_n^{(t)}(x)$$

است که در آنها مجموعیابی روی یک مجموعهٔ متناهی از مقادیر t انجام می‌شود.

اکنون می‌توانیم به فرمول مجموعیابی اویلر-مک‌لورن بازگردیم:

قضیه. برای هر عضو $f(x)$ از جبر لگاریتمی، سمت راست سری اویلر-مک‌لورن در توپولوژی لگاریتمی همگراست.

به عنوان مثال، سری نامتناهی زیر در توپولوژی لگاریتمی همگراست.

$$\begin{aligned}\log x + \log(x+1) + \log(x+2) + \cdots + \log(x+n)\\ = B_0((x+n+1)\log(x+n+1) - x\log x - n - 1)\\ + B_1(\log(x+n+1) - \log x)\\ + \frac{B_2}{2!}\left(\frac{1}{x+n+1} - \frac{1}{x}\right) + \cdots.\end{aligned}$$

مثالی دیگر به صورت زیر است. همان‌طور که می‌دانید مجموع

$$x^k + (x+1)^k + (x+2)^k + \cdots + (x+n)^k$$

را می‌توان توسط فرمول اویلر-مک‌لورن به صورت بسته بیان کرد. قضیهٔ پیش‌گفته به عبارتهای بسته‌صورت مشابهی برای مجموعیابی به شکل زیر منجر می‌شود

$$\begin{aligned}x^k\log x + (x+1)^k\log(x+1) + (x+2)^k\log(x+2)\\ + \cdots + (x+n)^k\log(x+n)\end{aligned}$$

لگاریتمهای همساز کاربردهای دیگری دارند. اجازه دهید یکی از آنها را در خاتمه ذکر کنم.

تعریف عملگر تغییر جا را در حساب تفاضلهای متناهی به یاد آورید:

$$E^a f(x) = f(x+a)$$

برای یک عدد صحیح نامنفی n، عملگر E_1 را به صورت زیر تعریف کنید

$$E_1\lambda_n^{(0)}(x) = \lambda_n^{(1)}(x)$$

با نمادگذاری معمولی، این مانند آن است که بگوییم

$$E_1 x^n = x^n(\log x - 1 - 1/2 - 1/3 - \cdots - 1/n)$$

می‌توان دو گزارهٔ زیر را ثابت کرد:

گزاره. عملگرهای E^a و E_1 جابجا می‌شوند.

گزاره. تحدید عملگر مشتقی D به زیرجبری از جبر لگاریتمی که توسط لگاریتمهای همساز $\lambda_n^{(t)}(x)$ برای tی مثبت تولید می‌شود (یعنی به‌استثنای توانهای نامنفی x) وارون‌پذیر است.

از این دو گزاره می‌توان برای به‌دست آوردن «توسیعهای لگاریتمی» توابع خاص استفاده کرد. بگذارید بحث را با ساده‌ترین مثال خاتمه دهیم: توسیع لگاریتمی دنبالهٔ فاکتوریلهای زیرین، یعنی چندجمله‌ای‌های $(x)_n = x(x-1)(x-2)\cdots(x-n+1)$ را محاسبه می‌کنیم. این دنبالهٔ چندجمله‌ای‌ها در معادلهٔ تفاضلی زیر صدق می‌کند

$$\Delta(x)_n = n(x)_{n-1}$$

که در آن Δ عملگر تفاضلی است: $\Delta f(x) = f(x+1) - f(x)$. این دنباله را می‌توان با قراردادن

$$(x)_{-n} = \frac{1}{(x+1)(x+2)\cdots(x+n)}$$

به nهای منفی توسیع داد؛ و داریم

$$\Delta(x)_{-n} = -n(x)_{-n-1}$$

برای n مثبت، می‌توانیم توسیع لگاریتمی این دنباله را با قراردادن

$$(x)_{-n}^{(1)} = (x)_{-n} = \frac{1}{(x+1)(x+2)\cdots(x+n)}$$

تعریف کنیم. به عنوان مثال، $x_{-1}^{(1)} = \frac{1}{x+1}$.

عناصر $x_{-n}^{(1)}$ به زیرمدولی از جبر لگاریتمی تعلق دارند که توسط $\lambda_n^{(1)}(x)$ وقتی که n همهٔ اعداد صحیح را می‌پذیرد، تولید می‌شود. عملگر Δ روی این زیرمدول وارون‌پذیر است و بنابراین می‌توانیم برای همهٔ عددهای صحیح نامنفی n قرار دهیم

$$(x)_n^{(1)} = \Delta^{-n-1}\frac{1}{x+1}$$

نتیجه می‌شود که عنصر $(x)_0^{(1)}$ توسط سری زیر داده می‌شود، که در توپولوژی لگاریتمی همگراست:

$$(x)_0^{(1)} = \log(x+1) + \frac{B_1}{1+x} - \frac{B_2}{2(1+x)^2} + \frac{B_3}{3(1+x)^3} - \cdots$$

اما این یک شیء آشناست: این همان Ψ-تابع است که گاوس آن را با گمانه‌زنی معرفی کرد. گاوس Ψ تابع را به عنوان جواب «راستین» معادلهٔ تفاضلی

$$\Delta\Psi(x+1) = \frac{1}{x+1}$$

معرفی کرد. ما اکنون درستی حدس گاوس را به‌طور دقیق ثابت کرده‌ایم. محاسبات بیشتر نشان می‌دهند که عنصرهای $(x)_1^{(1)}$ و $(x)_2^{(1)}$ نیز با تابعهای خاص معرفی شده توسط گاوس، یعنی تابعهای دوگاما و سه‌گاما یکسان هستند، که سرانجام به طور دقیق توسط سریهای نامتناهی همگرا در توپولوژی لگاریتمی تعریف شده‌اند.

در حال و هوای مشابهی می‌توان توسیعهای لگاریتمی چندجمله‌ای‌های برنولی، چندجمله‌ای‌های ارمیتی و غیره را تعریف کرد و آشکار می‌شود که بسطهای مجانبی این چندجمله‌ای‌ها به طور طبیعی به عنوان اعضای توسیعهای لگاریتمی این توابع دوباره ظاهر می‌شوند. درواقع توپولوژی لگاریتمی به ما اجازه می‌دهد که به جای بسطهای مجانبی، سریهایی را که در توپولوژی لگاریتمی همگرا هستند قرار دهیم.

در خاتمه، دو مسألهٔ حل نشده را می‌توان ذکر کرد. نخست اینکه عبارتی به صورت بسته برای ضرایب بسط حاصلضربی مانند

$$\lambda_n^{(t)}(x\lambda_n^{(s)}(x))$$

به سری توانی لگاریتمی شناخته نشده است. دوم اینکه در حالت کلی، تعبیری ترکیبیاتی یا احتمالاتی از ضرایب رومی $\left[{n \atop k}\right]$ در دست نداریم.

از اینکه به سخنانم گوش فرا دادید متشکرم.

مراجع

1. Alexander, Kenneth S., Kenneth Baclawski, and Gian-Carlo Rota, A stochastic interpretation of the Riemann zeta function, *Proceedings of the National Academy of Sciences* 90 (1993), 697-699.

2. Kung, J.P.S (ed.), *Gian-Carlo Rota on Combinatorics*, Boston: Birkhäuser (1996).

3. Kung, J.P.S., M. Ram Murty, and Gian-Carlo Rota, On the Rédei zeta function, *Journal of Number Theory* 12 (1980), 421-436.

4. Loeb, Daniel E., and Gian-Carlo Rota, Formal power series of logarithmic type, *Advances in Mathematics* 75 (1989), 1-118.

5. Rota, Gian-Carlo, Bruce Sagan, and Paul R. Stein, A cyclic derivative in noncommutative algebra, *Journal of Algebra* 64 (1980), 54-75.

* * * * * *

• Gian-Carlo Rota, "Combinatorial snapshots", *Math. Intelligencer*, (2) **21** (1999) 8-14.

این نوشته، متن سومین سخنرانی از سخنرانیهای سمینار (Colloquium Lectures) در نشست سالانهٔ انجمن ریاضی آمریکاست که در ۹ ژانویهٔ ۱۹۹۸ ایراد شده است.

* جیان‌کارلو روتا در هنگام نوشتن این مقاله در بخش ریاضی دانشگاه ام. آی. تی. کار می‌کرده است.

مقاله کلاسیک

آیا منظومهٔ شمسی پایدار است؟•

یورگن موزر*
ترجمهٔ روح‌الله جهانی‌پور

مسألهٔ پایداری

مسألهٔ پایداری در مکانیک کلاسیک، یعنی پایداری منظومهٔ شمسی، قرنهاست که منجمین و ریاضیدانان را مجذوب خود ساخته است. بیان ساده‌ای از این مسأله این است که آیا منظومهٔ شمسی در آیندهٔ دور همین شکل کنونی خود را حفظ خواهد کرد یا پس از زمانی طولانی، بعضی از این سیاراتْ منظومهٔ شمسی را ترک می‌کنند و یا برخوردهایی رخ خواهد داد که به یک تغییر فاجعه‌آمیز منجر می‌شود. قوانین حاکم بر حرکت سیارات از زمان نیوتن یعنی حدود ۳۰۰ سال است که شناخته شده‌اند. در تخمین اولیه، سیارات در مدارهای بیضی‌شکلی حرکت می‌کنند که خورشید در یکی از کانونهای بیضی قرارگرفته است. اما این فقط یک تقریب خام از حرکت واقعی سیارات است. نیروهای بین سیارات، اختلالهایی ایجاد می‌کنند که باعث تغییر مداوم اما بسیار آرام شکل این مدارهای بیضوی می‌شوند. توصیف این تغییرات یا به‌اصطلاح اختلالهای دیدیا[1] ی این مدارهای بیضوی، مسأله‌ای است که در چارچوب نظریهٔ کلاسیک اختلال بررسی می‌شود. امروزه قابل تصور است که نیروهای نسبتاً ضعیف بین سیارات بعد از مدت زمانی به اندازهٔ کافی طولانی، به قدری مدارهای کنونی را تغییر دهند که یک سیاره از منظومه خارج شود و یا اینکه برخوردی رخ دهد. برای مثال می‌توان تصور کرد که خروج از مرکز یک سیاره به‌طور پیوسته افزایش یابد تا اینکه فاصلهٔ نزدیکترین نقطهٔ مدار آن به خورشید [حضیض خورشیدی[2]] آنقدر کم شود که سیاره با رویداد ناگواری مواجه گردد. هر چند چنین سرانجامی با مشاهدات ما طی میلیونها سال گذشته همخوانی ندارد، ولی ارائهٔ یک اثبات ریاضی برای رخ‌ندادن این وضعیت به کمک معادلات حرکت، بحث کاملاً متفاوتی است.

درواقع در نوشتگان ریاضی موجود، تعداد قابل ملاحظه‌ای اثبات پایداری وجود دارد. تقریباً ۱۰۰ سال پس از انتشار کتاب پرینکیپیا ی نیوتن، لاگرانژ اثبات مشهور خود را برای پایداری منظومهٔ شمسی ارائه کرد. لاپلاس و پواسن

1. secular perturbations 2. perihelion

هم اثباتهای دیگری از این دست ارائه دادند، و ممکن است این سؤال پیش بیاید که چرا دوباره پس از ۲۰۰ سال، این مسأله دوباره مطرح شده است. به‌طور کلی برای درستی یک حکم، یک اثبات کافی است و عرضهٔ چندین اثبات ممکن است شنوندهٔ نقاد را به درستیِ مطلب مشکوک کند. اما در اینجا، مسأله، تقریبهای محاسبهٔ نیروی اختلال‌زا تا توانهای اول و دوم جرم سیاره است، که این تقریبها درجات دقت متفاوتی دارند. یعنی عملاً مدت زمان زیادی لازم است تا تغییر در مدارهای بیضوی به حد قابل ملاحظه‌ای برسد. زومرفلد[1] در کتاب مشترک خود با کلاین، خیلی موجز از «شبه‌اثبات» لاپلاس برای پایداری منظومهٔ شمسی سخن می‌گوید. با این حال باید دید این تقریبها تا چه اندازه اعتبار دارند. اگر ملاحظات خود را به چند دهه یا چند قرن محدود کنیم، این اثباتهای پایداری، نتایج درستی به‌دست می‌دهند، لکن از این نمی‌توان نتیجه‌ای در بارهٔ حرکت طی میلیونها سال به‌دست آورد. در قدیم محاسبهٔ عملی مکانهای سیارات یا به‌اصطلاح استخراج تقویم نجومی، که مورد توجه بابلیان هم قرار گرفته بود، بیش از تخمینهای طولانی‌بُرد مورد علاقه بود. نظریهٔ اختلال درواقع برآمده از لزوم محاسبهٔ مدارها با دقت هر چه بیشتر است. این مسأله را امروزه می‌توان حل کرد، ولی در آن نکتهٔ یأس‌آوری برای نظریه‌پردازان وجود دارد؛ زیرا اکنون می‌توان به کمک ماشینهای محاسبهٔ نوین نتایج را به‌طور مستقیم و حتی دقیقتر از آنچه از نظریهٔ اختلال به دست می‌آید محاسبه کرد. امروزه تقویمها در سالنامهٔ نجومی دریایی در واشینگتن[2] به همین روش حساب می‌شوند.

اما درست همین جاست که مسألهٔ ریاضی آغاز می‌شود. استخراج ویژگیهای اساسی یک مسأله و ایده‌آل کردن آن از روشهای آزموده شده و درست ریاضی است. به خاطر همین، ما به خودِ سیارات منظومهٔ شمسی که اجرام گسترده‌ای هستند نمی‌پردازیم و از همهٔ انواع نیروها از قبیل بادهای خورشیدی و اثرات نسبیتی صرفنظر می‌کنیم. در عوض یک، مسأله ایده‌آل

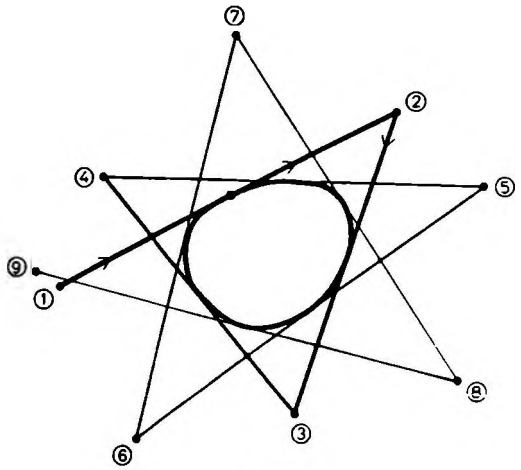
1. Sommerfeld 2. Nautical Almanac in Washington

شده را در نظر می‌گیریم و n نقطهٔ جرمی را که براساس قوانین نیوتن در فضای سه‌بعدی در حال حرکت هستند، مطالعه می‌کنیم. معمولاً فرض می‌شود که $n-1$ تا از این نقطه‌های جرمی خیالی در مقایسه با آن نقطهٔ باقیمانده که قرار است نقش خورشید را داشته باشد، جرمهای خیلی کوچکی دارند. به‌علاوه به دنبال بررسی حرکت در یک بازهٔ زمانی محدود نیستیم، بلکه می‌خواهیم حرکت را تا ∞ مطالعه کنیم. اکنون، این یک مسألهٔ کاملاً ریاضی است که جواب آن مصداق خیلی محدودی در دنیای واقعی دارد، ولی به جهت اینکه حرکت را برای تمام زمانها توصیف می‌کند، به نکات ظریف بسیار حیرت‌انگیزی منجر می‌شود. حتی این مسأله ریاضی ایده‌آل شده هم دست‌کم ۱۰۰ سال پیش صورت‌بندی شد و اصطلاحاً با عنوان مسألهٔ n جسم شناخته می‌شود. در قرن گذشته، این مسأله محل توجه فراوانی بود و همان‌طور که خواهیم دید، دیریکله که امروزه به خاطر کارهای ماندگارش در نظریهٔ اعداد مشهور است، و وایرشتراس که متخصص نظریهٔ توابع بود و پوانکاره، ریاضیدان همه فن حریف، نقشهای اساسی در بررسی این مسأله بازی کردند. به این ترتیب، این مسأله عبارت است از توصیف رفتار اختلالهای دیرپا روی بازه‌های زمانی طولانی و حتی برای تمام زمانها. آیا تغییر در شکل و مکان مدارها می‌تواند پیکربندی منظومهٔ سیاره‌ای را به‌طور کامل تغییر دهد؟ لاگرانژ در ارتباط با اثبات قضیهٔ پایداریش، نشان داد که اختلالات تحت تأثیر نوسانهای دوره‌ای هستند و از این رو بدون کران افزایش نمی‌یابند. دورهٔ این نوسانها نسبتاً طولانی است و از 5×10^4 تا 2×10^6 سال تغییر می‌کند. اما باید توجه کرد که در اینجا با یک تقریب سروکار داریم و این گفته را به معنای خاصی می‌توان تظریفی از توصیف دیرینهٔ مدارهای سیارات به‌وسیلهٔ افلاک تدویر[1] در نظر گرفت.

اما در بازه‌های زمانی به طول چند میلیون سال چه رخ می‌دهد؟ این سؤال نوعی مسألهٔ تشدید[2] است که در آن حرکات هشت سیارهٔ منظومهٔ شمسی، نقش نوسانگرها را بازی می‌کنند. البته تشدید در سیستمهایی رخ می‌دهد که دارای فرکانسی منطبق بر یکی از ویژه‌فرکانسهای آن سیستم یا مضرب صحیحی از آن باشد. ساده‌ترین پدیدهٔ تشدید مربوط به هل‌دادن یک تاب است. با نیروهای نسبتاً کوچکی که به تناوب و با همان فرکانس تاب وارد شود می‌توان دامنهٔ نوسان تاب را به اندازهٔ دلخواه افزایش داد یا حتی می‌توان باعث وارونه شدن تاب شد. در مورد منظومهٔ شمسی این قبیل پدیده‌ها نقش اساسی ایفا می‌کنند. درواقع چون هیچ اصطکاکی درکار نیست، اگر نوسانی یک بار رخ دهد، دیگر از بین نمی‌رود. به همین دلیل است که در سیستمهای نامیرا، برعکس همهٔ آزمایشهای فیزیکی روزمره و تابهای معمولی، اثرات تشدید تا این اندازه حساس است. در منظومهٔ شمسیِ ما تشدیدهای زیادی وجود دارد. مثلاً معلوم شده است که نسبت فرکانس مشتری به زحل حدود ۵/۲ است و این یعنی اینکه بعد از ۵ سال زحلی، مشتری ۲ بار دور خورشید می‌گردد، البته در صورتی که نیروها پس از این دوره در همان جهت قبلی اثر کنند. درواقع این وضعیت اثری قوی روی مدار مشتری می‌گذارد، اختلالی که دورهٔ آن در تقریب اولیه حدود ۹۰۰ سال است.

ولی درواقعیت باید چنین تشدیدهایی را برای تمام نسبتهای فرکانسی گویا و حتی تشدیدهایی که در آنها ترکیبی خطی از فرکانسهای با ضرایب صحیح

1. epicycles 2. resonance



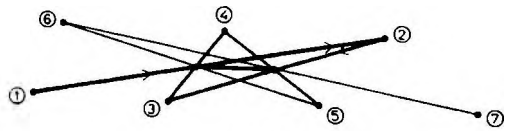
شکل۱

صفر می‌شود (فرکانسهای متوافق) هم انتظار داشته باشیم. اما طبعاً این امر نامعقول است زیرا اعداد گویا چگال‌اند و از نظر فیزیکی فرقی بین فرکانسهای گویا وگنگ وجود ندارد. ولی در حوزهٔ ریاضی این قبیل تمایزها کاملاً ضروری‌اند و لذا با یک موقعیت تعارض‌آمیز مواجه می‌شویم. نوشتن معادلات حرکت برای مسألهٔ n جسم کار خیلی ساده‌ای است، لکن درک شهودی آنها غیرممکن است. بنابراین بهتر است یک مسألهٔ هندسی خیلی ساده را توضیح دهیم که حاوی بعضی از مشکلات مسألهٔ n جسم است و می‌تواند الگوی خاصی برای حرکت سیارات هم باشد (شکل ۱). یک شکل تخم‌مرغی در صفحه در نظر می‌گیریم و «حرکت مداری» در خارج آن را به این صورت تعریف می‌کنیم: از نقطهٔ ۱ در خارج این شکل یکی از دو مماس را رسم می‌کنیم و آن را تا نقطهٔ ۲ که هم‌فاصله با نقطهٔ ۱ تا محل تماس است، امتداد می‌دهیم. از نقطهٔ ۲ مماس بعدی را رسم می‌کنیم و آن را تا نقطهٔ ۳ که مجدداً هم‌فاصله با نقطهٔ ۲ تا محل تماس است، امتداد می‌دهیم. با ادامهٔ این کار، «مدار» نقطهٔ ۱ به‌دست می‌آید. آیا این دنباله از نقاط می‌تواند بیکران باشد؟ این مسأله، نظیر مسألهٔ پایداری است. هر چند این مسأله کاملاً ابتدایی به نظر می‌رسد ولی واقعاً مشکل است. می‌توان نشان داد برای خمهایی که به اندازهٔ کافی هموارند (۵ بار مشتق‌پذیرند) و انحنای مثبت دارند، مدارها همواره کراندارند، یعنی پایداری برقرار است.

قابل توجه است که در این مسألهٔ ساده، هموار بودن خم مرزی باید نقش داشته باشد، اما اگر وجود گوشه را برای مرز مجاز بدانیم چه رخ می‌دهد؟ ساده‌ترین حالت، یک چندضلعی است. درواقع این نگاشت در این حالت پیوسته نیست ولی مسألهٔ پایداری هنوز معنای روشنی دارد. با این حال برای چندضلعی در حالت کلی، اینکه آیا مدارها کراندارند یا نه یک مسألهٔ حل‌نشده باقی‌مانده است. ولی دو حالت خاص وجود دارد که می‌توان آنها را به‌طور کامل بررسی کرد:

۱) وقتی تخم‌مرغ به یک دوضلعی تباهیده می‌شود، هر مدار در امتداد یک جفت خط مستقیم به بینهایت می‌رود (شکل ۲).

۲) اگر تخم‌مرغ یک مثلث باشد، همهٔ مدارها بسته‌اند اما دوره‌های متفاوت دارند. نقاط متعلق به مدارهای هم‌دوره، شش‌ضلعی‌ها و مثلثهایی تشکیل می‌دهند که یک خانه‌بندی جالب از صفحه به وجود می‌آورد. نقاط روی شش‌ضلعی‌ها دارای دوره‌های ۳، ۹، ۱۵، ۲۱، ... و به‌طور



شکل۲

کلی $3(2j-1)$، $j = 1, 2, \ldots$، و نقاط روی مثلثها دارای دوره‌های ۱۲، ۲۴، ۳۶، ... و به‌طور کلی $12j$، $j = 2, 3, \ldots$، هستند (شکل ۳). برای مربع هم می‌توان مسأله را به‌راحتی بررسی کرد، اما حتی برای یک چهارضلعی کلی هم مسألهٔ فوق هنوز حل نشده است.

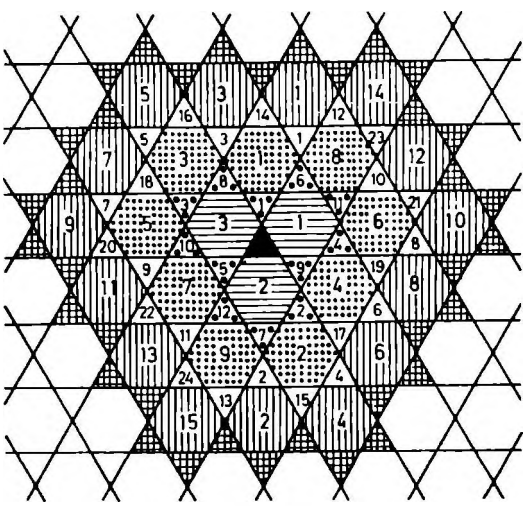
مسألهٔ جایزه‌دار

اکنون به حرکت سیارات و صورتبندی ریاضی مسأله و حل آن برمی‌گردیم. تلاش می‌کنیم مختصات اختلالهای دیرپا را به‌طور تحلیلی به کمک سریهای فوریهٔ تعمیم‌یافته تشریح کنیم. اینها سریهایی هستند که جملات آنها به شکل

$$A_j \cos(j_1\omega_1 + \ldots + j_s\omega_s)t +$$
$$B_j \sin(j_1\omega_1 + \ldots + j_s\omega_s)t$$

با فرکانسهای معین ω_1، ...، ω_s و فرکانسهای ترکیبی $j_1\omega_1+\cdots+j_s\omega_s$ اند. این دیدگاه چندان متفاوت با نظریهٔ فلک تدویر نیست ولی از نظر ریاضی دقیقتر است. این قبیل توابع، امروزه به توابع شبه‌تناوبی موسوم‌اند. درواقع ریاضیدانان مختلفی، مثلاً وایرشتراس، موفق شده‌اند با فرض اینکه ω_1، ...، ω_s نامتوافق هستند (یعنی نسبت گویا ندارند) چنین بسط سری را به‌طور صوری به‌دست آورند. اما ممکن است این سریها همگرا نباشند و بنابراین سودمندی آنها محل تردید است. ولی اگر این سریها همگرا باشند، نوسانات کوچک، در تغییرات بیضی را توصیف می‌کنند. تغییرات عناصری که به این ترتیب توصیف می‌شوند، همواره در یک محدودهٔ مفروض قرار می‌گیرند.

مسألهٔ ریاضی مورد نظر را این‌طور می‌توان بیان کرد: «برای یک دستگاه دلخواه از نقطه‌های جرمی که یکدیگر را براساس قوانین نیوتن جذب می‌کنند،



شکل۳

با فرض اینکه هیچ دو نقطه‌ای با هم برخورد ندارند، مختصات هر نقطه را برای تمام زمانها به‌صورت مجموع یک سری یکنواخت ـ همگرا که جملاتش از توابع شناخته‌شده تشکیل شده‌اند، ارائه دهید.» این، ترجمهٔ لغت به لغت مسألهٔ جایزه‌داری است که اُسکار دوم پادشاه سوئد در سال ۱۸۸۵، یعنی حدود ۹۰ سال قبل، مطرح کرد. جایزه را هانری پوانکاره بُرد هر چند او واقعاً مسأله را حل نکرد. کار بزرگ او درواقع نشان داد که این بسطهای سری، علی‌رغم تمام انتظارات، واگرا هستند و از این‌رو وجود ندارند. تعجب‌برانگیزتر اینکه در سال ۱۹۶۳ یک ریاضیدان جوان و برجسته موفق شد در میانهٔ دههٔ سوم زندگی خود این مسأله را حل کند و وجود چنین جوابهایی را با دقت کامل دست‌کم در مورد مسألهٔ ۳ جسم به اثبات رساند. این ریاضیدان، ولادیمیر آرنولد از شاگردان کولموگوروف بود که خود چند سال قبل از آن سنگ این اثبات را بنا نهاده بود. البته روایت دقیقتر این است که این کشف براساس کارهای بسیاری از ریاضیدانان دیگر صورت گرفت و اساساً ایده‌های اثبات به نتایج کارهای پوانکاره برمی‌گردد.

در دههٔ ۱۹۴۰، زیگل اولین مسأله از این دست را حل کرد، اما صورتبندی او از مسأله، ایده‌آل‌شده‌تر بود و واقعاً قابل استفاده در مسائل مکانیکی نبود. در سال ۱۹۵۴ کولموگوروف نشان داد که برای بعضی از سیستمهای مکانیکی، به یک معنی، اکثر جوابها شبه‌تناوبی‌اند. او به یکی از روشهای ممکن حل اشاره کرد. اما اثبات واقعی را ۸ سال بعد آرنولد و در حالت خاص نویسندهٔ این مقاله ارائه دادند. در تداول امروزی، این نظریه با علامت اختصاری KAM شناخته می‌شود[1]. نتیجهٔ اصلی این نظریه، تضمین وجود جوابهای شبه‌تناوبی برای رده‌های معینی از معادلات دیفرانسیل است که مسألهٔ n جسم را هم دربرمی‌گیرند. بسطهای سری مورد بحث به‌ازای انتخابهای خاصی از فرکانسها همگرا هستند، اما برای فرکانسهای دیگر بی‌معنی‌اند. نتیجهٔ اخیر را قبلاً پوانکاره ثابت کرده بود. مدارهایی که چنین نمایشی [همگرا] دارند، دقیقاً همانهایی‌اند که هیچ تشدیدی برای آنها رخ نمی‌دهد. اما چون این مدارهای فاقد تشدید می‌توانند به دلخواه به مدارهای دیگر نزدیک باشند، امکان دارد یک اختلال به دلخواه کوچک در مقادیر اولیه، یک مدار شبه‌تناوبی پایدار را به مداری ناپایدار تبدیل کند. با این حال می‌توان نشان داد که مدارهای ناپایدار خیلی نادرند، یا به زبان تخصصی‌تر، اندازهٔ آنها در فضای فاز نسبتاً کوچک است. این مطلب به مفهوم جدیدی از پایداری منجر می‌شود که در آن محدودیتها فقط روی اکثریت مدارهایی خاص اعمال می‌شوند. اینکه آیا مدارهای ناپایدار نسبتاً نادر، واقعاً وجود دارند یا نه هنوز یک مسألهٔ حل نشده است. در اینجا باید بگوییم ــ و بعداً نشان خواهیم داد ــ که این مفهوم ضعیف پایداری کاملاً بامعنی است و از نظر کاربردهای فیزیکی، رضایت‌بخش است.

کاربردهای جدید

اما پیشرفت بزرگ در این زمینه در کدام قسمت بوده است؟ اگر تعیین مدارها را بتوان به خوبی به کمک ماشینهای محاسبه انجام داد، چنین اثباتی بیهوده و دست‌کم از نظر تاریخی دیر به نظر می‌رسد. به این ایراد این‌گونه می‌توان پاسخ داد که:

۱. مرکب از حرف اول نامهای کولموگوروف، آرنولد، و موزر.

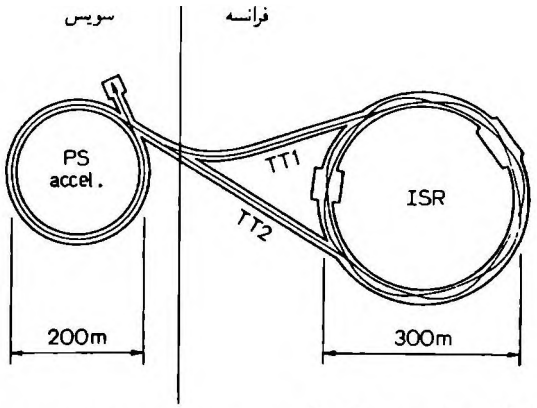
۱. پایداری سیستمهای نامیرا برای همهٔ زمانها اساساً با محاسبات متناهی قابل تعیین نیست و از این‌رو از حیطهٔ کاری ماشینهای محاسبه خارج است.

۲. مهمتر اینکه، چنین نتیجه‌ای که اتفاقاً به‌خودی خود از نظر ریاضی مورد علاقهٔ فراوان است، در تحقیقات نظری در مکانیک آماری اهمیت اساسی دارد. پیشرفت مکانیک آماری این امید را پدید آورده است که اغلب سیستمهای مکانیکی، دست‌کم وقتی از تعداد زیادی ذره تشکیل شده باشند، ارگودیک هستند؛ به این معنی که پس از مدت زمانی به اندازهٔ کافی طولانی، رفتارشان کاملاً مستقل از شرایط اولیه است. اما این مطلب در تقابل صریح با پایداری قرار دارد. در واقع، طی قرن گذشته، فیزیکدانان تلاش کرده‌اند با چنین دیدگاهی نشان دهند که اگر مدت زمانی طولانی صبر کنیم، تمام سیستمهای مکانیکی چنین رفتار ناپایداری از خود بروز می‌دهند. اما به کمک کارهایی که در دههٔ گذشته انجام شده، اکنون یک‌بار و برای همیشه ثابت شده است، که بسیاری از سیستمهای واقعی این‌گونه نیستند.

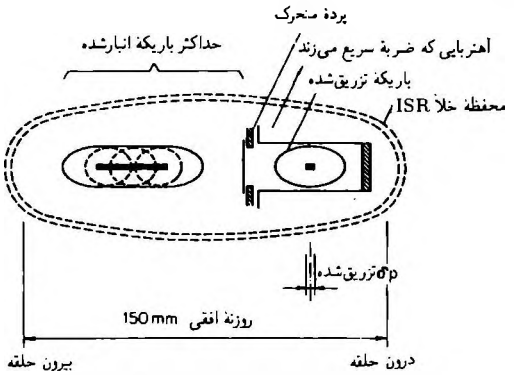
۳. بالاخره دلیل سومی هم وجود دارد که کم‌وبیش تصادفی به نظر می‌رسد: قضایای ریاضی نظریهٔ KAM فقط دربارهٔ منظومه‌های سیاره‌ای نیست بلکه با سیستمهای هامیلتونی کلی (و در نتیجه سیستمهایی که فرایندهای حرکتی نامیرا را توصیف می‌کنند) سروکار دارد و بنابراین قابل استفاده برای بسیاری از مسائل دیگر هم هست. این دقیقاً نمونه‌ای از سودمندی یک صورت‌بندی ریاضی کلی است. یکی از این کاربردها، مسألهٔ پایداری شتابدهنده‌های پروتون است که از دههٔ ۱۹۵۰ تاکنون به تعداد هر چه زیادتر و اندازه‌های بزرگتر ساخته شده‌اند. هدف این ماشینها، شتاب‌دادن به الکترونها و پروتونها تا رسیدن به سرعتهای خیلی زیاد و آنگاه پرتاب آنها به سمت یک هدف است، تا نتایج تجزیهٔ حاصل از این برخورد یعنی ذرات بنیادی جدید مشاهده شوند. هر چه انرژی ذره بیشتر باشد، مشاهدات حاصل هم جالبتر خواهند بود. برای رسیدن به چنین سرعت بالایی، پروتونها در یک محفظهٔ دایره‌ای آنقدر شتاب داده می‌شوند تا ذرات به سرعتی نزدیک سرعت نور برسند. این محفظه، مثلاً در مورد سنکروترن پروتون[1] در سرن[2] در ژنو، محیطی به طول بیش از ۶۰۰ متر دارد، و برای ایجاد خلأ کامل و جلوگیری از برخورد ذرات به مولکولهای هوا، هوای آن کاملاً تخلیه می‌شود. به کمک تعدادی آهنربا، میدانی مغناطیسی ایجاد می‌شود که این میدان ذرات را در یک مسیر تقریباً دایره‌ای حفظ می‌کند. اینجاست، که مسألهٔ پایداری مطرح می‌شود، زیرا میدان مغناطیسی باید طوری ایجاد شود که پروتونها خیلی از مسیر دایره‌ای موردنظر منحرف نشده و انرژی خود را در برخورد با دیوارهٔ محفظه از دست ندهند. در این فرایند، ذرات میلیونها بار دور محفظهٔ خلأ می‌گردند.

در ساختن این شتابدهنده‌ها، مسألهٔ پایداری نکته‌ای اساسی است. هر چند در آغاز به این قانع بودند که آزمونهایی با ماشین محاسبه انجام دهند، اما خیلی زود معلوم شد که پس از چند تکرار، خطای اجتناب‌ناپذیر محاسباتی، از کنترل خارج می‌شود و دنبال کردن یا تخمین‌زدن مسیرها غیرممکن می‌گردد. بنابراین به نتایجی نظری نیاز بود که نشان دهد می‌توان پایداری را در چنین سیستمی روی بازهٔ زمانی خیلی طولانی تضمین کرد و این دقیقاً اهمیت نظریه‌ای را می‌رساند که مشغول توصیف آن هستیم. آخرین پردهٔ این نمایش را حلقه‌های انبارنده[3] اجرا می‌کنند که یکی از آنها از سال ۱۹۷۱ تاکنون در سرن مشغول فعالیت است. (شکل ۴). به‌طور کلی، کار این دستگاهها،

1. proton synchrotron 2. CERN 3. storage rings



شکل ۴ الف مقطعی از محفظهٔ خلأ در محل منحرف‌کنندهٔ باریکه، که فرایند انبارکردن را نشان می‌دهد



شکل ۴ ب آرایش حلقه‌های انبارندهٔ متقاطع (ISR)

شتاب دادن پروتونها در دو محفظهٔ دایره‌ای در جهتهای مخالف و سپس برخورددادن آنها با یکدیگر است. به این طریق، نه تنها مطابق انتظار، انرژی حاصل از برخورد دو برابر می‌شود، بلکه به دلیل اثرات نسبیتی، انرژی تا توان دوم افزایش می‌یابد. برای حرکت دادن پروتونها در دو جهت مختلف، این حلقه‌های انبارنده (حلقه‌های انبارندهٔ متقاطع، ISR) به سنکروترون پروتون متصل می‌شوند و تعداد زیادی پروتون به تناوب، از یک جهت یا جهت مخالف به درون حلقهٔ انبارنده وارد می‌شود. این پروتونها طی فرایندی که ۳ تا ۱۱ ساعت طول می‌کشد، در آنجا انبار می‌شوند تا با یکدیگر برخورد داده شوند.

ساختن این دستگاه مشکلات فنی غیرقابل باوری دارد و آن‌قدر محتاج دقت است که ممکن است کارخانجات ساعت‌سازی سوئیس هم از عهدهٔ چنین دقتی برنیایند. در اینجا باید مقایسه‌ای انجام دهیم که برای مسألهٔ پایداری ما اهمیت دارد. طی فرایند انبارش، بسته‌های کوچک پروتون باید 10^{10} تا 10^{11} بار دور یک مسیر دایره‌ای بگردند و در این مدت درون تونلی بمانند که مقطع آن ۱۶ در ۵٫۲ سانتی‌متر است. اگر یک دوران پروتون را در حلقهٔ انبارنده معادل با یک سال در مسألهٔ نجومی بگیریم، آنگاه عدد فوق زمانی بیش از عمر زمین را نشان می‌دهد، یعنی در این قیاس باید پروتونها را در مدت زمانی طولانیتر از عمر منظومهٔ شمسی در شکل کنونیش، دنبال کنیم. گذشته از این فیزیکدانان و مهندسین می‌توانند شرایط و پارامترها را به دلخواه خود عوض کنند. این مثال را به این دلیل مطرح کردیم که نیازمند پایداری روی بازه‌هایی زمانی است که از هر آنچه در ۱۰۰ سال قبل در نجوم

تصور می‌شد، طولانیتر است و بنابراین به یک معنی، مسألهٔ پایداریِ ایده‌آل‌شده روی بازه‌های زمانی نامتناهی را توجیه می‌کند، البته اگر چنین توجیهی لازم باشد. وقتی نتایج نظریهٔ KAM را برای این حالت به‌کار می‌بریم، معلوم می‌شود که اغلب پروتونهای شتاب‌یافته در مسیر دایره‌ای درون حلقه‌های انبارنده باقی می‌مانند، اما مدارهای نسبتاً نادری هم هستند که به کند شدن و کمی هدر رفتن باریکه‌های پروتون منجر می‌شوند. این هدر رفتن‌ها در این مورد اجتناب‌ناپذیرند و مشاهده هم می‌شوند. اینکه آیا آن مدارهای خاص را می‌توان مسبب این هدر رفتن دانست، هنوز باید حل‌نشده تلقی شود به این دلیل که بسیاری از نیروها و اثرات اضافی که بر ذرات اثر می‌گذارند و ممکن است آنها را منحرف کنند، لحاظ نشده است. این کاربردها انگیزه‌های خوبی برای تحقیقات ریاضی‌اند. یقیناً باید پرسید چگونه است که این مسألهٔ دیرینهٔ پایداری، در حالی‌که جاذبهٔ خود را برای منجمین از دست داده است، ناگهان مطرح و حل می‌شود؟ یک پاسخ خوب به این پرسش این است که گسترش شتابدهنده‌های پروتون در احیای دلبستگی به این مسأله مؤثر بوده است.

پایداری مدارهای تناوبی

می‌خواهیم پدیدهٔ تشدید دیگری را توضیح دهیم که هم در نجوم و هم در فیزیک انرژی بالا پدید می‌آید. این پدیده، مسألهٔ پایداری مدارهای تناوبی، یعنی جوابهایی است که بعد از یک زمان معین به وضعیت اولیهٔ خود برمی‌گردند. در اینجا به دنبال شرایطی هستیم که تحت آنها مدارهایی که شرایط اولیه‌شان نزدیک به یک مدار تناوبی است، همیشه نزدیک آن باقی بمانند. چنین مدارهایی، پایدار نامیده می‌شوند. فقط همین مدارهای پایدار هستند که معمولاً قابل مشاهده‌اند. بهترین مثالِ آن هم مدار دایره‌ای در حلقه‌های انبارنده است که در بالا تشریح شد. در این مدارها اختلالهای کوچک، به تغییرات بزرگ منجر نمی‌شود. برای اینکه معلوم کنیم آیا این مدارهای دایره‌ای پایدارند یا نه باید از فرکانسهای بتراترون ω_r و ω_z و فرکانس مداری ω_0 که متعلق به نوسانهای دستگاه خطی‌شده هستند استفاده کرد. نظریه نشان می‌دهد که در حالت کلی تشدید غیرخطی یا ناپایداری زمانی رخ می‌دهد که این فرکانسها در رابطهٔ $n\omega_r + m\omega_z = p\omega_0$ صدق کنند که در آن n، m و p اعدادی صحیح‌اند که $|n| + |m| \leq 4$. از طرف دیگر رابطه‌هایی از این دست با فرض $|n| + |m| > 4$ چندان ضرری ندارند. درواقع آزمایشها نشان می‌دهند که در حالت اول، هدررفتگی در باریکه‌های پروتون مشاهده می‌شود ولی در حالت دوم این هدر رفتن قابل چشم‌پوشی است. به بیان نادقیق، تشدیدهای با مرتبهٔ کوچکتر یا مساوی ۴ خطرناک و تشدیدهای با مرتبهٔ بیش از ۴ بی‌ضرر هستند.

پدیدهٔ مشابهی هم در نجوم رخ می‌دهد. همان‌طورکه می‌دانید، در منظومهٔ شمسی علاوه بر سیاره‌های اصلی، هزاران سیارک نیز موجودند که به دور خورشید می‌گردند و مدارهای آنها عمدتاً بین مریخ و مشتری قرار دارد. چون جرم این سیارکها خیلی کوچک است، اثری بر سیاره‌ها ندارند ولی مشتری حرکت آنها را شدیداً دچار اختلال می‌کند. شاهد این مدعا، مشاهده‌ای است که توسط کرک‌وود[1] انجام شده است. او متذکر می‌شود که فرکانسهای سیارکها به‌طور یکنواخت روی یک بازه توزیع نشده‌اند بلکه شکافهایی، موسوم به شکافهای کرک‌وود، در آنها مشاهده می‌شود. این وضعیت را می‌توان مشابه با شکافهای موجود در حلقه‌های زحل انگاشت زیرا آنجا هم پدیده‌ای شبیه به این رخ می‌دهد. اگر حرکت میانگین سیارکها را با ω_a و حرکت میانگین مشتری را با ω_j نشان دهیم، محسوسترین شکافها با فرمول

$$\frac{\omega_j}{\omega_a} = \frac{n}{m}, \qquad |n-m| = 1, 2, 3, 4$$

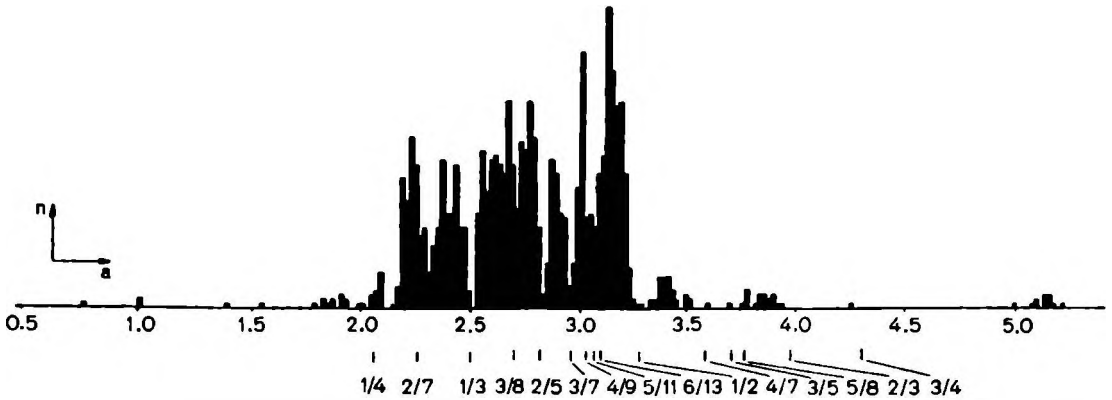
مشخص می‌شوند و این یعنی تشدید از مرتبهٔ کوچکتر یا مساوی ۴. می‌ماند آن مدارهای تناوبی را مشخص کنیم که پایداریشان متناظر با شرایط فوق است. فرض می‌کنیم مشتری روی یک مدار دقیقاً دایره‌ای حرکت می‌کند و سیارکها روی مدارهایی تقریباً دایره‌ای در همان صفحه در حال حرکت هستند، به‌طوری که این آرایه یعنی مثلث تشکیل شده از خورشید، مشتری و سیارک پس از یک دورهٔ زمانی معین به وضعیت اولیهٔ خود برگردد. پوانکاره قبلاً این مدارهای تناوبی را به‌دست آورده بود. مدارهایی که تشدید مذکور در بالا برای آنها رخ نمی‌دهد پایدارند و در نتیجه وضعیت کاملاً روشن است: شکافها متناظرند با مدارهای ناپایدار. هر چند اینها همه تقریبهای خامی از وضعیت واقعی هستند، ولی پدیدهٔ وجود شکافها را به‌خوبی توصیف می‌کنند. شرح ریاضی این پدیده به‌طور دقیق در نظریهٔ KAM داده می‌شود، هر چند ایده‌های اصلی را می‌توان درکارهای برکاف که کار پوانکاره را دنبال کرد یافت.

یادداشت تاریخی

شرح تاریخی مختصر زیر، مسألهٔ پایداری و چگونگی پیشرفت عظیم آن را روشن می‌سازد. چاپ نامه‌های وایرشتراس به سونیا کووالفسکی که چندی پیش صورت گرفت، شرایط مساعدی فراهم آورد که انگیزهٔ این یادداشت بوده است. این نامه‌ها حاوی مطالب بسیار جالبی در بارهٔ موضوع مورد بحث ماست و اگر نامه‌ها چاپ نمی‌شدند، آن مطالب حتی برای ریاضیدانان هم چندان شناخته شده نبودند. وایرشتراس نقش بسیار اساسی در ریاضیات نیمهٔ دوم قرن ۱۹ داشت و ریاضیدانانی از سراسر دنیا به برلین می‌آمدند تا سخنرانیهای او را بشنوند. علاقهٔ اصلی و دامشغولی تمام زندگیش، نظریهٔ توابع بود اما علاقه‌ای جدی هم به نجوم داشت و در سال ۱۸۸۰ـ۱۸۸۱ سمیناری دربارهٔ نظریهٔ اختلال در نجوم ارائه داد. او ایده‌هایش را در این باره و مخصوصاً در بارهٔ مسألهٔ پایداری در چندین نامه به سونیا کووالفسکی تشریح کرد. نظر به اینکه وایرشتراس نتایج خود را خیلی به اکراه و پس از بازبینی همه‌جانبه به چاپ می‌رساند، این مکاتبات غیررسمی از ارزش خاصی برخوردارند.

سونیا کووالفسکی در ۲۰ سالگی برای تحصیل ریاضیات از روسیه به برلین آمد که در آن زمان اقدام واقعاً ماجراجویانه‌ای به‌شمار می‌آمد. یقیناً داشتن دانشجوی دختر در آن زمان مرسوم نبوده است و به همین دلیل سونیا از حضور در کلاس محروم بود. در نتیجه وایرشتراس به‌طور خصوصی به او آموزش می‌داد. در اثر این روابط، دوستی عمیقی بین آن دو ایجاد شد که تا پایان عمر کووالفسکی دوام داشت. کووالفسکی، ریاضیدان برجسته و مشهوری شد و به مقام استادی ریاضیات در دانشگاه استکهلم رسید، گرچه متأسفانه او این شغل را دو سال قبل از مرگ نابهنگامش در ۴۱ سالگی به‌دست آورد. گذشته از روابط شخصی، نامه‌های وایرشتراس به سونیا کووالفسکی

1. Kirkwood



شکل۵ تعداد سیارکها به عنوان تابعی از a، نصف طول قطر بزرگ. مقادیر aی متناظر با کسرهای معینی از دورهٔ گردش مشتری در زیر شکل مشخص شده‌اند. برخی از این «تشدیدها» شکافهایی در توزیع سیارکها ایجاد کرده‌اند.

حاوی تعداد زیادی ایده و پیشنهاد ریاضی است که اطلاعاتی ارزشمند از نحوهٔ تفکر او به‌دست می‌دهند. اما نشانه‌های بسیار مشخصی، مثلاً در نامهٔ ۱۵ اوت ۱۸۷۸، یافت می‌شود از اینکه او از قبل وقت خود را مصروف بسطهای سری صوری برای جوابهای شبه‌تناوبی مسألهٔ n جسم و همگرایی آنها کرده بود. به این ترتیب شکی نیست که وایرشتراس در تعقیب همان مسأله‌ای بوده که اکنون بالاخره حل شده است.

چرا وایرشتراس این‌قدر مطمئن بود که نمایشهای سری او عملاً همگرا هستند؟ پاسخ این سؤال هم معلوم شده است. دیریکله، جانشین گاوس در گوتینگن، قبلاً در سال ۱۸۵۸ به شاگردش کرونکر گفته بود که روشی کاملاً نوین برای بررسی و حل مسائل مکانیک یافته است. دیریکله سال بعد مُرد بدون اینکه هیچ نوشته‌ای دربارهٔ کشفیات خود برجای گذاشته باشد. اما کرونکر یادداشتهای دیریکله را به سراسر دنیای ریاضیات که در جستجوی کشف این ایده‌های مفقود بود، رساند. امروزه نام دیریکله اساساً با نظریهٔ اعداد که در واقع موضوع علاقهٔ اصلی او بود عجین شده است، حال آنکه کارهای او در فیزیک ریاضی کمتر شناخته شده‌اند. این کارها مشتمل‌اند بر مبانی نظریهٔ سریهای فوریه، محاسبات پایداری شاره‌های در حال دوران، کارهایی در هیدرودینامیک، محکهای پایداری نقاط تعادل و غیره. چون آثار منتشرشدهٔ دیریکله به خاطر دقت زیاد در روشها و اثباتها شهرت داشتند، شکی نبود که یادداشت دیریکله می‌بایست جدی به‌حساب آورده می‌شد و وایرشتراس مخصوصاً علاقه‌مند بود این مسأله را روشن سازد و این گنج را کشف کند. وقتی در سال ۱۸۸۵ به تشویق میتاگ‌ـلفلر، جایزه‌ای برای یک اکتشاف ریاضی مهم تعیین شد، وایرشتراس این مسأله را به‌عنوان یکی از سؤالهای جایزه‌دار مطرح کرد. کمیتهٔ جایزه هم از وایرشتراس، ارمیت و میتاگ‌ـلفلر تشکیل شده بود. و این جریان بود که بعداً به نوشتهٔ ۲۰۰ صفحه‌ای پوانکاره منجر شد، کاری که اثر زیادی بر پیشرفتهای بعدی این موضوع گذاشت. این کار پوانکاره برای وایرشتراس دلسردکننده بود هر چند عمیقترین تحسینها را نسبت به آن ابراز کرد. دلیلش این بود که پوانکاره نشان داد بسط سری در نظریهٔ اختلال در حالت کلی واگراست و به این ترتیب امیدهای وایرشتراس مبدل به یأس شد. ضمناً این پدیدهٔ واگرایی برای خود پوانکاره هم کمی دردسر درست کرد که او با روشی کاملاً جسورانه بر آن فائق آمد. بسطهای سری مجانبی که در نظریهٔ شاره‌ها و موضوعات کاربردی دیگر از آنها استفاده می‌شود و نیز کاربرد سریهای واگرا در محاسبات عددی همگی به ایده‌های پوانکاره باز می‌گردند. با این حال وایرشتراس همچنان مسألهٔ همگرایی را دنبال کرد و دریافت که هر چند استدلالهای پوانکاره کاملاً درست‌اند، اما واقعاً ثابت نمی‌کنند که سری مورد بحث واگراست. قضایای وجودی برای جوابهای شبه‌تناوبی که امروزه شناخته شده‌اند، حاکی از آن‌اند که چنین سریهایی به‌ازای فرکانسهایی معین همگرا هستند و این دقیقاً همان نکته‌ای بود که وایرشتراس به آن اشاره کرد. بالاخره پس از ۷۰ سال اکنون می‌توان به این سؤال وایرشتراس در بارهٔ همگرایی پاسخ مثبت داد. طبیعی است که دیگر تعیین اینکه آیا نتایج جدید واقعاً با تلاشهای دیریکله تطابق یا ارتباط دارند یا نه غیرممکن است.

آنچه در این مقاله بیان شد نباید این اعتقاد نادرست را به وجود آورد که ریاضیات صرفاً به‌وسیله کاربردهای عملی هدایت می‌شود یا اینکه علت وجودی آن را باید در حل این قبیل مسائل جست، بلکه همواره تعامل بین حوزه‌های مختلف مطالعاتی است که منجر به خلق مفاهیم جدید می‌شود. بالاخره آیا منظومهٔ شمسی پایدار است؟ صریحاً بگوییم، پاسخ هنوز نامعلوم است و این سؤال به نتایج خیلی عمیقی منجر شده است که احتمالاً مهمتر از پاسخ اصل سؤال هستند.

* * * * * *

• Jürgen Moser, "Is the solar system stable?", *The Mathematical Intelligencer*, (1) **2** (1980) 65-71.

این مقاله براساس نخستین سخنرانی از مجموعهٔ سه سخنرانی پائولی تنظیم شده که در ژانویهٔ سال ۱۹۷۵ در «مؤسسهٔ عالی فنی فدرال» در زوریخ ارائه شده است. مقاله ابتدا در مجلهٔ نویه زورخر تسایتونگن، شمارهٔ ۱۴ مه ۱۹۷۵ به زبان آلمانی به چاپ رسیده است.

* یورگن موزر در زمان نوشتن این مقاله در مؤسسهٔ علوم ریاضی کورانت در نیویورک، مشغول کار بوده است.

نشر ریاضی، سال ۱۱، شمارهٔ ۲، صص ۵۰-۵۲

مسأله

مسأله‌هایی از کتاب اسکاتلندی

کیوان ملاحی‌کارای *

۱. کمی تاریخ...

اردوش جملهٔ مشهوری دارد که «ریاضیدانْ ماشینی است که قهوه را به قضیه تبدیل می‌کند!» شاید بهترین مصداق برای این جمله، قهوه‌خانه‌ای است به اسم «کافهٔ اسکاتلندی» که در میدان کوچکی در شهر لووف[1] لهستان قرار دارد. حتماً نامهای باناخ، اولام، میزر و اشتاینهاوس را تاکنون بارها شنیده‌اید، اما امیدوارم داستانی که اکنون می‌خواهم تعریف کنم برایتان تازگی داشته باشد. در سالهای میانی دههٔ ۱۹۳۰، این قهوه‌خانه پاتوق گروهی از ریاضیدانهای برجستهٔ آن زمان لهستان (شامل آنهایی که در بالا نام بردم) بود که ساعاتی از روز خود را در آنجا با گفتگوهای ریاضی می‌گذراندند. روزی از همین روزها، باناخ با خودش فکر کرد که چه خوب است خلاصهٔ بحثها و ایده‌هایشان را در جایی بنویسند تا در گذر زمان فراموش نشوند، و دفترچهٔ بزرگ و تمیزی تهیه کرد تا مسأله‌هایی را که با هم در مورد آنها بحث می‌کردند در آنجا ثبت کنند. تاریخ ثبت اولین مسأله ۱۷ ژوئیهٔ ۱۹۳۵ است! این دفترچه همیشه در قهوه‌خانه بود و هر وقت که باناخ و میزر وارد می‌شدند با سفارش «دفترچه، لطفاً!»، دفترچه به همراه دو فنجان قهوه روی میز حاضر می‌شد ....

این دفترچه که یادآور روزهای طلایی ریاضیات لهستان است، توسط دانیل ماولدین ویرایش شده و به صورت کتابی با نام

The Scottish Book,
Mathematics from the Scottish Café

تدوین گردیده است. اکنون می‌خواهیم گشت‌وگذاری کنیم در ریاضیات آن دوران...

۱. Lwów، این شهر اکنون در کشور اوکراین قرار دارد.

۲. پارادُکس باناخ و تارسکی

هنگامی که نظریهٔ مجموعه‌ها دوران کودکی خود را می‌گذراند، باناخ و تارسکی قضیه‌ای را به کمک اصل انتخاب ثابت کردند که به پارادکس باناخ-تارسکی شهرت پیدا کرد. این قضیه ادعا می‌کند که می‌توان یک پرتقال را به شکلی مناسب برید و قطعه‌های کوچک را به شکلی دیگر کنار هم قرار داد و دو پرتقال به اندازهٔ پرتقال اولی به‌دست آورد! به بیان دیگر، باناخ و تارسکی نشان دادند که می‌توان گوی واحد سه‌بعدی را یک بار به مجموعه‌های A_1، ...، A_n، B_1، ...، B_n و بار دیگر به مجموعه‌های C_1، ...، C_n افراز کرد به طوری که $A_i \equiv B_i \equiv C_i$. در اینجا $X \equiv Y$ به این معنی است که X و Y دو مجموعهٔ همنهشت هستند، یعنی می‌توان هر یک از آنها را با یک تبدیل طولپا (مثل انتقال، دوران، ...) به دیگری تبدیل کرد. «پارادُکس» بالا را می‌توان چنین تعبیر کرد که نمی‌توان مفهومی به نام «حجم» برای همهٔ زیرمجموعه‌های فضا تعریف کرد که این دو انتظار طبیعی ما را برآورده کند: اول اینکه تحت تبدیلات طولپا، پایا باشد و دوم اینکه حجم اجتماع (متناهی) از مجموعه‌های مجزا برابر مجموع حجمهای آنها باشد.

در انتهای این بخش، هدف ما این است که بفهمیم که پارادُکس باناخ-تارسکی چگونه اتفاق می‌افتد! ابتدا مفهوم گروه رام را معرفی می‌کنیم. فرض کنید که G یک گروه توپولوژیک موضعاً فشرده و μ اندازهٔ هار[1] چپ (یعنی اندازهٔ بورل پایا تحت انتقال از چپ) روی G باشد. همچنین فرض کنید $L^\infty(G,\mu)$ فضای خطی توابع μ-اندازه‌پذیر تقریباً همه جا کراندار

1. Harr

روی G باشد. تابعک خطی $m : L^\infty(G) \to \mathbb{R}$ را یک میانگین می‌نامیم هرگاه $m(1) = 1$ که در اینجا 1 تابع ثابت با مقدار ۱ است و همچنین برای هر تابع نامنفی $f \in L^\infty(G,\mu)$ داشته باشیم $m(f) \geq 0$. مثلاً فرض کنید که $G = \{g_1, \dots, g_n\}$ یک گروه متناهی باشد و

$$m(f) = \frac{1}{n}(f(g_1) + \cdots + f(g_n))$$

در این صورت به سادگی می‌توان دید که m یک میانگین روی G است. اگر G فشرده باشد نیز با استدلالی مشابه (انتگرال‌گیری!) می‌توان یک میانگین روی G تعریف کرد. همچنین دقت کنید که این میانگینها تحت عمل G روی $L^\infty(G,\mu)$ پایا هستند، یعنی اگر تابع h توسط $h(x) = f(gx)$ تعریف شود داریم $m(h) = m(f)$.

در حالت کلی نمی‌توان روی هر گروه موضعاً فشردهٔ G، یک میانگین که تحت عمل G پایا باشد، پیدا کرد. گروههایی را که روی آنها چنین میانگینی وجود دارد رام[1] می‌نامند. مارکوف و کاکوتانی[2] ثابت کردند که هر گروه آبلی رام است. اکنون نشان می‌دهیم که گروه آزاد با دو مولد (همراه با توپولوژی گ.....ته)، رام نیست. فرض کنید که F گروه آزاد با مولدهای a و b باشد. مجموعهٔ A^+ (به ترتیب A^-) را مجموعه همهٔ کلمه‌هایی می‌گیریم که با a (به ترتیب a^{-1}) شروع می‌شوند. همین‌طور مجموعه‌های B^+ و B^- را نیز می‌توان تعریف کرد. اکنون به سادگی می‌توان دید که،

$$F = A^+ \cup A^- \cup B^+ \cup B^- = A^+ \cup aA^- = B^+ \cup bB^-$$

حال فرض کنید که m یک میانگین روی F باشد و 1_X را تابع مشخصهٔ مجموعهٔ X بگیرید. چون m تحت انتقال پایاست داریم

$$\begin{aligned} 1 &= m(1_{A^+}) + M(1_{A^-}) + m(1_{B^+}) + m(1_{B^-}) \\ &= m(1_{A^+}) + m(1_{A^-}) = m(1_{B^+}) + m(1_{B^-}) \end{aligned}$$

که غیرممکن است! پس F رام نیست! حال فرض کنید که X یک مجموعه باشد و F روی X عمل کند و در ضمن بدانیم که برای هر $1 \neq g \in F$ و هر $x \in X$ داریم $g \cdot x \neq x$. (اصطلاحاً می‌گویند که F به طور آزاد روی X عمل می‌کند، کلمه آزاد ربطی به آزادبودن F ندارد.) در این صورت می‌توان پیش‌پرده‌ای از پارادکس باناخ-تارسکی را روی X تماشا کرد! برای این کار ابتدا از هر مدار یک عضو «انتخاب» می‌کنیم (البته بی‌سروصدا!)، و با آنها مجموعهٔ M را می‌سازیم. حال قرار می‌دهیم

$$X_{A^+} = \{g \cdot x | g \in A^+, x \in M\}$$

مجموعه‌های X_{A^-}، X_{B^+} و X_{B^-} را نیز به طور مشابه تعریف می‌کنیم. حال داریم

$$\begin{aligned} X &= X_{A^+} \cup X_{A^-} \cup X_{B^+} \cup X_{B^-} = X_{A^+} \cup aX_{A^-} \\ &= X_{B^+} \cup bX_{B^-} \end{aligned}$$

1. ameanable 2. Kakutani

تقریباً به پایان ماجرا رسیده‌ایم! کرهٔ S^3 را در نظر بگیرید. گروه $SO(4)$ یعنی گروه دورانهای S^3 روی S^3 عمل می‌کند. به‌عنوان تمرین ثابت کنید که $SO(4)$ شامل یک زیرگروه آزاد ۲ عضوی است که به طور آزاد روی S^3 عمل می‌کند. اکنون به‌جای یک S^3، دو تا S^3 دارید!

۳. مسألهٔ باناخ-روزیویچ

این مسأله هم به اندازه‌های روی کره nبعدی مربوط است. همه می‌دانیم که اندازهٔ لبگ روی زیرمجموعه‌های بورل S^n اندازه‌ای متناهی‌ْجمع‌پذیر است که تحت دوران (یعنی عمل $SO(n+1)$) پایاست. سؤالی که باناخ و روزیویچ[1] مطرح کردند، این بود که آیا اندازهٔ دیگری نیز با این دو خاصیت وجود دارد؟ اگر $n = 1$، جواب مثبت است. درواقع چون گروه جمعی $\mathbb{R}$ آبلی است، پس رام است و تابعک خطی $m : L^\infty(\mathbb{R},\mu) \to \mathbb{R}$ وجود دارد که تحت انتقال پایاست. برای هر $f \geq 0$ داریم $m(f) \geq 0$. حال اگر اندازهٔ μ را با رابطهٔ $\mu(A) = m(1_A)$ تعریف کنیم، با انتخاب تابعکهای مختلف می‌توان اندازه‌های جدید به‌دست آورد. (این استدلال کامل نیست! سعی کنید آن را کامل کنید.) اما دقت کنید که برای $n \geq 2$، گروه تقارنهای S^n گروه غیررام $SO(n+1)$ است و تکرار استدلال بالا ممکن نیست. درواقع روزنبلات، مارگولیس و سالیوان نشان دادند که برای $n \geq 4$ اندازهٔ لبگ تنها اندازهٔ با ویژگیهای بالاست. دو سال بعد، درینفلد، با اثبات حکم به‌ازای $n = 2$ و $n = 3$، پاسخ به سؤال باناخ و روزیویچ را کامل کرد.

۴. هندسهٔ فضاهای باناخ

فرض کنید که X یک فضای باناخ باشد. کرهٔ واحد X را در نظر می‌گیریم:

$$S = \{x : ||x|| = 1\}$$

S از نظر توپولوژیک چگونه موجودی است؟ اگر بعد X متناهی باشد، جواب سؤال روشن است، چون S با کرهٔ واحد nبعدی S^n $(n = \dim X)$ همسانریخت است و توپولوژی S^n نیز شناخته شده است. پس فرض کنید که X نامتناهی‌بعد است.

برای شروع به سراغ مشهورترین دوستمان یعنی l^2 می‌رویم. می‌دانید که l^2 فضای خطی همهٔ دنباله‌های $(x_1, x_2, \cdots)$ از اعداد حقیقی است که $||x|| = (\sum x_n^2)^{1/2} < \infty$. در اینجا می‌خواهیم نشان دهیم که کرهٔ واحد l^2 انقباض‌پذیر است، یعنی می‌توان آن را روی خودش به یک نقطه تبدیل کرد!

یک اثبات رسمی! فرض کنید T مجموعهٔ همهٔ دنباله‌های $(x_1, x_2, \cdots)$ باشد که مؤلفهٔ اول آنها صفر است یعنی $x_1 = 0$. تابع $f : S \to T$ را توسط $f(x_1, x_2, \cdots) = (0, x_1, x_2, \cdots)$ تعریف می‌کنیم. قرار دهید

$$\varphi(x,t) = \frac{tx + (1-t)f(x)}{||tx + (1-t)f(x)||}$$

1. Ruziewicz

دقت کنید که تحت هوموتوپی φ، همهٔ S روی T جمع می‌شود. همچنین روشن است که می‌توان T را با هوموتوپی مشابهی روی نقطهٔ $a = (1, 0, 0, \cdots)$ منقبض کرد:

$$\psi(x,t) = \frac{tx + (1-t)a}{||tx + (1-t)a||}$$

پس همهٔ کره روی نقطهٔ a منقبض شد.

نکته جالب اینجاست که حکم مشابه برای همهٔ فضاهای باناخ نامتناهی‌بعد برقرار است. درواقع می‌توان نشان داد که اگر X یک فضای باناخ نامتناهی‌بعد و $K \subseteq X$ فشرده باشد، آنگاه X و $X - K$ همسانریخت هستند. پس بالاخص X و $X - \{0\}$ نیز همسانریخت هستند و دقت کنید که X به‌وضوح انقباض‌پذیر است و $X - \{0\}$ و S دارای نوع هوموتوپی یکسان هستند!

۵. چند مسأله، بدون حل

مسأله‌های زیر از کتاب اسکاتلندی انتخاب شده‌اند؛ بعضی از آنها ساده و بعضی «دشوار» هستند:

۱. (اولام) فرض کنید E خانواده‌ای ازمجموعه‌های متناهی باشد که هر یک از آنها حداکثر n عضو دارند و اشتراک هر $n+1$ تای آنها ناتهی است. ثابت کنید اشتراک همهٔ آنها ناتهی است.

۲. (میزر، آوربرباخ، اولام و باناخ) فرض کنید $\{K_n\}_{n\geq 1}$ خانواده‌ای از اجسام محدب (جسم محدب یعنی مجموعهٔ فشرده محدب که درون آن ناتهی است) باشد که قطر هر یک از آنها حداکثر a است و مجموع حجم آنها حداکثر b. در این صورت مکعبی به ضلع $f(a,b)$ وجود دارد که می‌توان همهٔ این اجسام محدب را بدون اینکه با یکدیگر تلاقی داشته باشند در آن قرار داد.

کاربرد: یک کیلوگرم سیب‌زمینی را می‌توان در یک جعبه متناهی جای داد!

۳. (میزر) دنبالهٔ $\{a_n\}_{n\geq 1}$ را در نظر بگیرید. می‌گوییم که این دنباله در میانگین به a همگراست هرگاه

$$\lim_{n\to\infty} \frac{a_1 + \cdots + a_n}{n} = a$$

همچنین می‌گوییم که سری $\sum a_n$ در میانگین به S همگراست هرگاه دنبالهٔ $\{S_n\}_{n\geq 1}$ که $S_n = a_1 + \cdots + a_n$ در میانگین به S همگرا باشد. فرض کنید که L مجموعهٔ همهٔ اعداد حقیقی S باشد به طوری که جایگشت $\sigma : \mathbb{N} \to \mathbb{N}$ وجود داشته باشد که سری $\sum_{n=1}^{\infty} a_{\sigma(n)}$ به S همگرا باشد. نشان دهید اگر L بیش از یک عضو داشته باشد و $L \neq \mathbb{R}$، آنگاه L یک تصاعد حسابی است.

۴. (آوربرباخ) فرض کنید $\phi : \mathbb{R} \to \mathbb{R}$ تابعی پیوسته باشد و

(۱) $\phi \not\equiv 0, 1, \phi(x) \geq 0$

(۲) $\phi(a+b) \leq \phi(a) + \phi(b)$

(۳) $\phi(ab) = \phi(a)\phi(b)$.

در این صورت $0 < \alpha \leq 1$ وجود دارد که $\phi(x) = |x|^{\alpha}$.

۵. (اشتاینهاوس) فرض کنید $z = f(x,y)$ یک رویهٔ پیوسته را نشان دهد که دارای این خاصیت باشد که در هر نقطه آن بتوان دقیقاً دو خط راست گذراند که کاملاً روی رویه قرار گیرند. در این صورت این رویه حتماً یک سهمیوار هذلولوی است!

۶. (باناخ) فرض کنید که $\{A_{ij}\}_{i,j\geq 1}$ یک ماتریس نامتناهی باشد. در این صورت هر جایگشت از درایه‌های این ماتریس را می‌توان به‌صورت ترکیبی از جایگشتهایی نوشت که هر یک از آنها، هر سطر را به یک سطر و هر ستون را به یک ستون می‌برند.

۷. فرض کنید Ω کوچکترین اُردینال ناشمارا باشد و $\alpha < \beta < \Omega$. در این صورت دو فضای باناخ $C[0, \alpha+1]$ و $C[0, \beta+1]$ یکریخت هستند اگر و تنها اگر $\beta < \alpha^{\omega}$.

۸. (میزر) فرض کنید $\mathcal{F}$ خانواده‌ای از دنباله‌های اعداد حقیقی باشد که برای هر دو دنبالهٔ (α_n) و (β_n) در $\mathcal{F}$ داریم

$$\sum \alpha_n \beta_n = 0$$

آیا $\mathcal{F}$ شماراست؟ (دقت کنید! نمی‌دانیم که اعضای $\mathcal{F}$، در l^2 قرار دارند!)

۹. (اولام) فرض کنید A و B دو فضای توپولوژیک باشند که $A \times A$ و $B \times B$ همسانریخت از آب درآمده‌اند! آیا A و B همسانریخت هستند؟ (توضیح: A و B هیولاهای توپولوژیک نیستند. مثال ناقضی وجود دارد که A و B دو خمینهٔ سه‌بعدی‌اند!)

۱۰. (اولام و آوربرباخ) نشان دهید هر گروه لی نیمه‌ساده و همبند G دارای زیرگروه آزاد با دو مولد است که در G چگال است.

۱۱. (شرایر و اولام) فرض کنید S_{∞} گروه همهٔ جایگشتهای مجموعهٔ اعداد طبیعی باشد. آیا گروه جمعی اعداد حقیقی در S_{∞} می‌نشیند؟ گروه $SO(3)$ چطور[1]؟

۱۲. (اولام) منظور از یک مجموعهٔ مستطیلی در $[0,1]^2$ مجموعه‌ای به صورت $A \times B$ است که $A, B \subseteq [0,1]$. آیا σـجبر تولید شده توسط مجموعه‌های مستطیلی، همهٔ زیرمجموعه‌های $[0,1]^2$ را دربرمی‌گیرد؟

(توضیح: اگر فرض پیوستار یا اصل مارتین را بپذیریم جواب مثبت است!)

۱۳. (شرایر) فرض کنید σ یک یکریختی گروه G است که برای هر $g \in G$ دو عضو g و $\sigma(g)$ مزدوج هستند. آیا σ لزوماً یک خودریختی درونی است؟

۱۴. (اولام) اگر $n \geq 2$، نشان دهید که همسانریختی $h : \mathbb{R}^n \to \mathbb{R}^n$ وجود دارد که مدار نقطهٔ O یعنی $\{h^n(O)\}_{n\geq 1}$ چگال است.

* * * * * *

* کیوان ملاحی‌کارای، دانشگاه ییل آمریکا

keivan@math.yale.edu

۱. طبق اظهار ویراستاران کتاب مورد بحث، جواب این قسمت سؤال در زمان نگارش کتاب معلوم نبوده است.

کتاب

نقد ۳۲ کتاب مهم قرن

مجموعهٔ نقدهایی که در زیر می‌خوانید، تصویری از رشد ریاضیات در دو ثلث اول قرن بیستم به‌دست می‌دهد. در این نقدها اکثر کتابهایی که اثری دیرپا بر تحولات دانش ریاضی در قرن بیستم داشته‌اند بررسی شده‌اند و نویسندگان کتابها و ناقدان نیز از ریاضیدانان سرشناس قرن هستند. سی تا از این نقدها از میان مجموعه‌ای که بولتن انجمن ریاضی آمریکا در شمارهٔ ژانویهٔ سال ۲۰۰۰ خود آورده، برگزیده و ترجمه شده‌اند. این مجلهٔ نقدهایی را که در دو سوم اول قرن در مورد مهمترین کتابها به چاپ رسانده، با حذف قطعاتی از آنها در این شماره تجدید چاپ کرده است. دو نقد دیگر ــ «درآمدی به ریاضیات، اثر کاینی» و «نظریهٔ مجموعه‌ها و فرضیهٔ پیوستار، اثر کوهن» ــ از جورنال آو سیمبالیک لاجیک گرفته شده‌اند و ترجمهٔ آنها با حذف قطعاتی در اینجا می‌آید.

مبانی هندسه، اثر هیلبرت

Foundations of geometry, by David Hilbert

اصول بنیادی هندسه کدام‌اند؟ خاستگاه، ماهیت، و قلمرو آن چیست؟ اینها پرسشهایی هستند که در همهٔ اعصار توجه ریاضیدانان و اندیشمندان را به خود معطوف داشته‌اند، ولی در حدود یک قرن قبل به یُمن اندیشه‌های لوباچفسکی و بویویی، جنبهٔ کاملاً جدیدی یافته‌اند.

قرنها سعی می‌کردیم گزارهٔ معروف به اصل اقلیدس را ثابت کنیم، و همواره در این کار ناکام می‌شدیم. امروز می‌دانیم که دلیل این شکستها چیست. لوباچفسکی توانست نظامی منطقی بسازد که به اندازهٔ هندسهٔ اقلیدس سازگار است، ولی این اصل معروف در آن صادق نیست و مجموع زاویه‌های مثلث همواره کوچکتر از دو قائمه است. ریمان نظام منطقی دیگری ابداع کرد که همان‌قدر عاری از تناقض است، ولی در آن مجموع زوایای مثلث همواره بزرگتر از دو قائمه است. این دو هندسه، هندسهٔ لوباچفسکی و هندسهٔ ریمان، همان چیزهایی هستند که هندسه‌های نااقلیدسی نامیده می‌شوند. پس اصل اقلیدس قابل اثبات نیست؛ و این امکان‌ناپذیری همان‌قدر مسلم و قطعی است که هر حقیقت ریاضی دیگر ــ ولی این امر مانع از آن نیست که هر سال اثباتهای تازهٔ متعددی به آکادمی علوم [فرانسه] برسد، اثباتهایی که طبیعتاً کونت رندو[1] [نشریهٔ آکادمی علوم فرانسه] با روی خوش از آنها استقبال نمی‌کند.

قبلاً مطالب زیادی دربارهٔ هندسه‌های نااقلیدسی نوشته شده است؛ زمانی این هندسه‌ها اسباب دستپاچگی ما می‌شدند؛ حالا دیگر به تعارضات آنها عادت کرده‌ایم؛ بعضیها تا آنجا پیش رفته‌اند که در درستی این اصل شک کرده‌اند و این پرسش را مطرح کرده‌اند که آیا فضای واقعی، چنانکه اقلیدس فرض می‌کرد، مسطح است و آیا ممکن نیست مختصری انحنا داشته باشد. آنها حتی تصور می‌کردند که با آزمایش می‌توان پاسخی به این پرسش داد. نیازی به گفتن ندارد که این تصور کاملاً ناشی از بدفهمیِ ماهیت هندسه است، که علمی تجربی نیست.

ولی چرا در میان همهٔ اصول موضوع هندسه فقط این یک اصل را می‌توان

1. Comptes rendus

انکار کرد بدون اینکه تخلفی از منطق صورت گیرد؟ این جنبهٔ انحصاری را از کجا یافته است؟ به نظر می‌رسد هیچ دلیل محکمی برای این امر وجود نداشته باشد، و بسیاری راههای دیگر هم ممکن است.

اما ظاهراً خیلی از هندسه‌دانان معاصر چنین نمی‌اندیشند. آنها بدون تردید فکر می‌کنند که با به رسمیت شناختن دعاوی دو هندسهٔ جدید، تا آخرین حد ممکن سازش کرده‌اند. به همین دلیل به چیزی که هندسهٔ عام یا جامع می‌نامند، باور دارند که نظامهای اقلیدس، لوباچفسکی، و ریمان سه حالت خاص از آن هستند و نظام دیگری هم در آن نیست. همین کلمهٔ جامع به روشنی نشان می‌دهد که در نظر آنها، هیچ هندسهٔ دیگری قابل تصور نیست.

این اشخاص اگر اثر پروفسور هیلبرت را بخوانند از این توهم بیرون خواهند آمد، و خواهند دید که در این اثر، حصارهایی که دوست داشتند ما را پشت آنها محبوس کنند در همه جا فرو می‌ریزند.

برای اینکه این اقدام جدید را خوب درک کنیم باید به یاد آوریم که سیر تکامل اندیشهٔ ریاضی در صد سال گذشته، نه فقط در هندسه بلکه همچنین در حساب و آنالیز، چگونه بوده است. مفهوم عدد روشنتر و دقیقتر شده است و در عین حال، در جهات گوناگونی تعمیم یافته است. در میان این تعمیمها، ارزشمندتر از همه برای آنالیز، واردکردن موهومی‌هاست که ریاضیدان نوین اکنون نمی‌تواند از آنها اجتناب کند؛ ولی ما در اینجا توقف نکرده‌ایم؛ تعمیمهای دیگری از عدد یا، در اصطلاح ما، رسته‌های دیگری از عددهای مختلط، وارد علم شده‌اند.

عملهای حساب نیز در معرض نقادی قرار گرفته‌اند، و کواترنیونهای همیلتن نمونه‌ای از یک عمل به‌دست داده‌اند که تشابه تقریباً کاملی با ضرب دارد و می‌توان آن‌را به همین نام نامید ولی این عمل تعویض‌پذیر نیست، یعنی حاصلضرب دو عامل در صورتی که ترتیب عاملها معکوس شود، تغییر می‌کند. این امر انقلابی در حساب بود، بسیار شبیه انقلابی که لوباچفسکی در هندسه پدید آورد.

تصور ما از بینهایت نیز دگرگون شده است. پروفسور گئورگ کانتور به ما آموخته است که درجاتی برای خودِ بینهایت قائل شویم (که البته به بینهایت کوچکهایِ از مراتب مختلف که لایب‌نیتس آنها را برای حساب بینهایت‌کوچکهای معمولی ابداع کرد ربطی ندارد). مفهوم پیوستار، که مدتهای مدید یک مفهوم اولیه قلمداد می‌شد، مورد تحلیل و تقلیل به عناصرش قرار گرفته است.

و نیز اگر اجازه بدهید، از تلاش ایتالیاییها برای ساختن یک نظام نمادی منطقی عام و فروکاهش استدلال ریاضی به قاعده‌های مکانیکی محض یاد می‌کنم.

همهٔ اینها را باید به یاد آوریم تا درک کنیم که چگونه مفاهیمی که برای خود اباچوفسکی، علی‌رغم انقلابی‌بودنش، می‌توانست تکان‌دهنده باشد، ممکن است امروز به نظر ما تقریباً طبیعی برسد و پروفسور هیلبرت بتواند آنها را در نهایت آرامش و خونسردی مطرح کند.

هانری پوانکاره

******

نقل از

Bull. Amer. Math. Soc. **10** (1903-04), 1-23.

درسهایی دربارهٔ گروههای پیوسته . . . ، اثر سوفوس لی

Vorlesungen über continuirliche Gruppen mit geometrischen und anderen Anwendungen, by Sophus Lie. Bearbeitet und ausgeben von Dr. Georg Scheffers, Leipzig, Teubner, 1893, 8vo., xi+810 pp.

در مورد نظریهٔ گروههای تبدیلات، ما مدیون پروفسور لی هستیم که این بخش بسیار جالب و مهم از ریاضیات مدرن را پدید آورده است. اهمیت خود مفهوم گروه از مدتها قبل درکاربردش در نظریهٔ جایگذاریها شناخته شده بود، و بعضی تبدیلهای پیوسته، از قبیل تبدیل پدالی[1] [پادکی]، قبل از تحقیقات لی به‌کار می‌رفتند بدون اینکه ارتباط آنها با ایدهٔ گروه کشف شده باشد؛ این کشف و عرضهٔ نتایج آن به‌صورتی روشمند، کار پروفسور لی است.

تا جایی که به گروههای تبدیلات مربوط می‌شود، این نتایج از مجله‌های مختلفی که برای نخستین بار در آنها چاپ شده‌اند، گردآوری شده و به‌صورت تحلیلی کاملی در نظریهٔ گروههای تبدیلات در دسترس قرار گرفته‌اند.

در آن کتاب، پروفسور انگل[2] درکار دشوار ارائهٔ نظریهٔ کلی به شیوه‌ای دقیق و روشن، توفیق بسیار یافته است. ولی مشکلات این بحث کلی اندک نیست، و برای تهیهٔ درآمدی به آن، درسهایی در بارهٔ گروههای پیوسته نوشته شد. در عین حال، هدف این بود که همین کتاب به تنهایی، دست‌کم رئوس نظریهٔ کلی را ارائه کند و بعضی از زمینه‌های کاربرد آن را نشان دهد. دکتر شفرز[3] به هر دو هدف نائل شده است. در بخش اول، بحثی از گروههای تبدیلات یک و دومتغیره، با توجه به گروههای تصویری [فرافکنشی[4]] و مهمترین زیرگروههایشان آمده است. تمام اصول لازم هندسهٔ تصویری [فرافکنشی] که به‌کار رفته‌اند، استنتاج شده‌اند، و اطلاعات بسیار مقدماتی ریاضی برای مطالعهٔ این بخش از کتاب کفایت می‌کند. در بخش دوم، نظریهٔ کلی گروههای پیوستهٔ nمتغیره مورد بحث قرار گرفته‌اند.

ج. م. بروکس

******

نقل از

Bull. Amer. Math. Soc. **1** (1894-95), 241-248.

درس آنالیز ریاضی، اثر گورسا

Cours d'analyse mathématique, by Édouard Goursat, Professeur à la Faculté des Sciences de Paris, Tome I, Gauthier-Villars, Paris, 1902

1. pedal transformation 2. Engel 3. Scheffers 4. projective

تجدیدنظر در اصول بنیادی حساب دیفرانسیل و انتگرال، که به‌وسیلهٔ کوشی و آبل شروع شد و وایرشتراس و پیروان مکتبش آن را ادامه دادند، به پروراندن اثبات ϵ ای (که کوشی اول بار مطرح کرده بود) و صورتبندی دقیق تعریفها و قضیه‌ها انجامید. در آلمان و ایتالیا گرایشی ظهور کرد که در تعریفها و قضایا فقط به آن محدودیتهایی اکتفا کنند که طبیعت موضوع ضرورتاً تحمیل می‌کند. مثلاً تابعهایی که در سراسر هیچ بازه‌ای پیوسته نیستند، فقط به دلیل شکل تعریف انتگرال وقتی بر رده‌ای از این توابع اعمال می‌شود، به‌عنوان انتگرالدهٔ انتگرالی معین پذیرفته شدند و این پرسش مورد بررسی قرار گرفت که قضیه‌های عادی حساب انتگرال تا چه حدی برای این‌گونه توابع برقرارند. و باز، قضیهٔ $\partial^2\mu/\partial x\partial y = \partial^2\mu/\partial y\partial x$ با محدودیتی کمتر از پیوستگی همهٔ مشتقات مربوطه ثابت شد. هر چند این شیوه تا جایی که مسألهٔ تحقیق در زمینه‌ای خاص مطرح باشد کاملاً موجه است، نباید این واقعیت را از نظر دور داشت که این‌گونه تحقیقات فقط نمود بسیار خاصی از آنالیز نوین هستند، و حتی متخصصان آنالیز ممکن است هرگز نیازی نداشته باشند خودشان را در مورد انتگرالهای توابعی بجز آنها که پیوسته‌اند (مگر در تعداد متناهی از نقاط) به زحمت بیندازند. آنچه برای هر ریاضیدانی که از حساب دیفرانسیل و انتگرال استفاده می‌کند ضروری است، صورتبندی ساده‌ای از قضیه‌ها و آزمونهای ساده‌ای برای تحقیق در اعتبار فرایندهای این حساب است که از زمان اویلر و پیش از او دست به دست گشته و به ما رسیده‌اند ــ از سری همگرایی از توابع پیوسته چه موقعی می‌توان جمله به جمله انتگرال گرفت، چه وقتی می‌توان از یک انتگرال معین که انتگرالدهٔ آن در شرایط قابل قبول پیوستگی صدق می‌کند، در زیر علامت انتگرال، مشتق گرفت؟ این پرسشها مورد علاقهٔ عموم ریاضیدانان هستند. ریاضیدانان فرانسوی به اهمیتِ دادن جوابهای ساده و زیبا به این پرسشها واقف‌اند. آنها در عین مقیدبودن به معیارهای نوین دقت، نگذاشته‌اند حقایق اصلی آنالیز در انبوه جزئیات دست‌وپاگیر گم شود.

کتابی که پیش روی ماست، از نوع بهترین نوشتگان نوین فرانسوی در بارهٔ حساب دیفرانسیل و انتگرال است. این کتاب مبتنی بر درسهای دانشگاهی پروفسور گورساست. طبق برنامهٔ آموزشی فرانسه، محصل ریاضیات در لیسه [مدرسه] معنی و کاربرد مشتق را، بدون آشناشدن با دیفرانسیل، و نیز مقدمات تحلیل جبری را فرا می‌گیرد. بنابراین، مدرس دانشگاه می‌تواند فرض کند که دانشجو با مفهوم حد و روشهای مقدماتی حساب دیفرانسیل و انتگرال آشناست، و پختگی کافی برای فهم بحثی در این حساب، در سطح آنچه در دانشگاههای آمریکایی به‌عنوان درس دوم یا سوم عرضه می‌شود، دارد.

آن دسته از دانشجویان ریاضی که می‌خواهند به مطالعهٔ فیزیک ریاضی یا برخی از شاخه‌های گوناگون آنالیز ــ نظریهٔ توابع، معادلات دیفرانسیل، حساب وردشها، و غیره ــ بپردازند به‌شدت به چنین کتابی در زمینهٔ حساب دیفرانسیل و انتگرال که کل موضوع را به دقت و به نحوی جذاب عرضه کند و همچنین در حال و هوای آنالیز نوین باشد، نیاز داشته‌اند. کتاب پروفسور گورسا نیاز این دانشجویان را به نحو کاملاً رضایت‌بخش رفع می‌کند و ما مطالعهٔ آن را از صمیم قلب به آنها توصیه می‌کنیم. مدرس حساب دیفرانسیل و انتگرال پیشنهادهای بسیاری در کتاب خواهد یافت که در بهتر کردن تدریس او مفید خواهند بود، و در بسیاری موارد حتی خواهد توانست به محصلان کلاس مقدماتی توصیه کند از بخشهای مقدماتیتر این کتاب برای مطالعهٔ جنبی استفاده کنند. حوزهٔ مطالب کتاب گسترده است. هر چند کتاب از مبانی حساب دیفرانسیل و انتگرال شروع می‌کند، خواننده را به جایی می‌برد که بتواند از منابع اصلی استفاده کند و اندیشهٔ نهفته در اثباتهای ϵای را بفهمد. تاریخدان آینده وقتی بخواهد تحقیق کند که حساب دیفرانسیل و انتگرال در نظر ریاضیدانان اواخر قرن نوزدهم چگونه چیزی بوده است، می‌تواند با اطمینان به کتاب پروفسور گورسا مراجعه کند که مفاهیم و روشهای مهم حساب دیفرانسیل و انتگرالِ این عصر را به‌خوبی تشریح می‌کند.

ویلیام آسگود

******

نقل از

Bull. Amer. Math. Soc. **9** (1902-03), 547-555.

یادنامه صدمین زاد روز کومر . . .

Festschrift zur Feier des 100 Geburtstages Eduard Kummers mit Briefen an seine Mutter und an Leopold Kronecker, Herausgegeben vom Vorstande der Berliner Maethematischen Gesellschaft, Leipzig, Teubner, 1910, 103 pp.

انتخاب هنزل برای ایراد سخنرانی یادبود کومر بسیار مناسب بوده است، زیرا تحقیقات برجستهٔ وی در بارهٔ اعداد جبری به او امکان می‌دهد به‌عنوان مرجعی ذی‌صلاح در بارهٔ شاهکار کومر، یعنی ابداع اعداد ایده‌آل، سخن بگوید. در این متن، شرح مقدماتی و جذابی در بارهٔ توجه اولیه کومر به معادلهٔ فرما، $x^\lambda + y^\lambda + z^\lambda = 0$، که λ عددی اول است، آمده است. این توجه، کومر را به تحقیق در عددهای $a + b\alpha + \ldots + k\alpha^{\lambda-1}$ که در آنها α یک ریشهٔ مختلط λام واحد است و a، b، ...، k عددهایی صحیح‌اند، واداشت. شواهد قانع‌کننده‌ای وجود دارد که کومر در اوایل گمان می‌کرد اثبات کامل امکان‌ناپذیریِ معادلهٔ فرما را در دست دارد، و دستنوشته‌ای در اختیار دیریکله قرار داد که ادعا می‌کرد حاوی چنین اثباتی است. دیریکله در پاسخ خاطرنشان کرد که هر چند او [کومر] ثابت کرده است هر عدد $f(\alpha)$ حاصلضرب عاملهایی تجزیه‌ناپذیر است، ولی فرض کرده است که چنین تجزیه‌ای یکتاست، حال آنکه این فرض در حالت کلی درست نیست. کومر پس از سالها بررسی به این نتیجه رسید که وضعیت آشفتهٔ حاصل از نایکتایی تجزیه، ناشی از این حقیقت است که حوزهٔ عددهای $f(\alpha)$ آنقدر کوچک است که اجازهٔ ورود به

عددهای اول واقعی نمی‌دهد، و از اینجا به کارِ دورانساز خود، ابداع عددهای ایده‌آل، رهنمون شد. هنزل در سخنرانی خود بدون اینکه سعی کند در بارهٔ فوت‌وفن پیچیدهٔ روش کومر توضیح بدهد ــ روشی که آنقدر پیچیده و ظریف است که متخصصان باید آن را با بیشترین دقت و احتیاط به‌کار گیرند و امروز با توجه به نظریهٔ ساده‌تر و کلیتر ددکیند، عمدتاً اهمیت تاریخی دارد ــ به این اکتفا می‌کند که شرح مقدماتی روشنگری از ویژگیهای اساسی روش کومر به صورتی که برای مجموعهٔ خاصی از عددهای صحیح ارائه می‌شود، بدهد. باید خاطرنشان کرد که هر چند اتخاذ دیدگاه جدیدتر در بارهٔ مبنای نظریهٔ ایده‌آلها مرجح است، ولی این تغییر دیدگاه، اعتبار مجموعهٔ غنیِ نتایج بنیادی کومر را خدشه‌دار نساخته است. شرح مختصر صفحهٔ ۳۰ در بارهٔ روش کومر در اثبات امکان‌ناپذیری معادلهٔ فرما وقتی‌که λ یک عدد اول منظم است، به‌طور مستقیم فقط برای حالت اول از دو حالتی که کومر در نظر گرفته است صادق است. ولی همین نوع استفاده از عدد رده‌ای در حالت دوم هم میسر است و این نکته‌ای است که هنزل بر آن تأکید کرده است. همهٔ تحسین‌کنندگان کومر از خواندن این Gedächtnisrede [خطابهٔ یادبود] استادانه لذت فراوان خواهند برد.

۵۶ صفحه نامه‌های کومر به شاگرد مورد علاقه، و مستعدترین شاگردش، کرونکر، ارزش تاریخی دارد. این نامه‌ها روایت دست اولی از پیشرفت گام‌به‌گام کومر در ساختن اثر ماندگارش به‌دست می‌دهند.

ل. دیکسن

******

نقل از

Bull. Amer. Math. Soc. **17** (1910-11), 371-372.

تحلیل جا، اثر وبلن

The Cambridge Colloquium, 1916, Part II. *Analysis Situs*, by Oswald Veblen, The American Mathematical Society, New York, 1922, vii+150 pp.

این ناقد اکنون در وضعی نادر قرار گرفته که کاری را برای بار دوم انجام می‌دهد. رضایت خاطر زیادی که از این امر به‌دست می‌آورد ناشی از آن است که بعد از نوشته‌شدن نقد اول، استفادهٔ فراوانی از کتاب مورد نقد به‌عنوان ابزار تحقیق کرده و امیدوار است تجربیات جدیدی که به این نحو به‌دست آورده نه فقط برای خودش بلکه برای خوانندگانش نیز سودمند باشد.

بلافاصله باید بگویم که این کتاب در عمل بسیار موفق از آب درآمده است. قبل از آن، فردی مبتدی که مجذوب مبحث جذاب و دشوار تحلیل جا می‌شد، مجبور بود به سختی و با صرف وقت زیاد مقاله‌های بسیار پراکنده‌ای را، که از مقالهٔ کلاسیک ۱۸۹۵ پوانکاره در ژورنال دُ اِکول پلی‌تکنیک و ضمیمه‌های متعدد آن شروع می‌شدند، مطالعه کند. او در هر مرحله با استدلالهای دشوار، نمادهای نامناسب و گیج‌کننده‌تر از همه، به بن‌بست رسیدن شهود هندسی در زمانی که بیشترین نیاز به آن وجود دارد، روبه‌رو می‌شد. هیچ شاهراهی که از درون این جنگل انبوه بگذرد نمی‌توان احداث کرد، ولی بررسی خوب و عمیقی از مبانی، نمادگذاری، و اصطلاحات، می‌تواند مسیر را تا حدی هموار کند. این و بسیاری چیزهای دیگر را می‌توان در کتاب وبلن دید. علاقه‌مندان مبحث تحلیل جا، که تعدادشان مسلماً رو به افزایش است، می‌دانند که کمتر کسی، هم از لحاظ روحیه و هم به لحاظ سوابق علمی، ذی‌صلاح‌تر از این مؤلف برای خلق چنین اثری بوده است. از آنجا که این مبحثْ مسائل دشوارِ فراوان و روشهای کلی اندک دارد، به این افزایش علاقه‌مندان باید امید بسیار بست.

دو جریان در تحلیل جا وجود دارد: یکی به نظریهٔ مجموعهٔ نقاط مربوط می‌شود و دیگری عمدتاً ماهیت ترکیبیاتی دارد و در آن خمینه‌ها بررسی می‌شوند که مثلاً در حالت دوبعدی قابل تصویر کردن روی چندوجهیهایی با تعداد متناهی وجوه چندضلعیِ مسطح هستند. این کتاب تقریباً به‌طور کامل به جریان دوم اختصاص یافته است. با این حال مؤلف شاید بیشترین مهارت ریاضی خود را در نقاط تقاطع این دو جریان نشان داده باشد، مثلاً با آن نوع مسأله‌ای که با مطرح‌کردن خمهای ژوردان روی یک چندوجهی نماینده مطرح می‌شود.

این اثر از بهترین نمونه‌های رشته انتشارات *Colloquium Lectures* است که ریاضیات آمریکایی می‌تواند به آن افتخار کند، و سزاوار آن است که مورد توجه و استقبال همکاران در این رشته و در کل جامعهٔ ریاضی قرار گیرد، و قرار خواهد گرفت.

سالومون لفشتس

******

نقل از

Bull. Amer. Math. Soc. **30** (1924), 357-358.

درسهایی در نظریهٔ اعداد، اثر لانداو

Vorlesungen über Zahlentheorie, by Edmund Landau, Volume I: *Aus der elementaren und additiven Zahlentheorie*, xii+360 pp.; Volume II: *Aus der analytischen und geometrischen Zahlentheorie*, vii+308 pp.; Volume III: *Aus der algebraischen Zahlentheorie und über die Fermatsche Vermutung*, vii+341 pp.; Leipzig, S. Hirzel, 1927

این کتاب سه‌جلدی که به طرز عالی تدوین و چاپ شده است، اثر فوق‌العاده مهمی است که به نوشتگان نظریهٔ اعداد افزوده شده است. خوانندهٔ آشنا با مفاهیم بنیادی نظریهٔ توابع متغیر حقیقی و مختلط می‌تواند از طریق این کتاب بسیاری از پیشرفتهای حیرت‌انگیز اخیر در این مبحث جذاب را تعقیب کند. توجه و علاقهٔ خواننده فوراً جذب می‌شود و با دقت، مهارت، و شور و شوقی که لانداو در کنار هم چیدن حقایق آنالیز و ساده‌سازی انبوه جزئیات به خرج داده است، تا آخر باقی می‌ماند

هدف اصلی این بخش، تشریح نظریهٔ ایده‌آلها در حد لازم برای اثبات قضایای معروفی است که با حدس مشهور فرما ارتباط دارند، یعنی این حدس که معادلهٔ

$$x^n + y^n = z^n$$

به‌ازای $n > ۲$، جواب صحیح x، y، zای با ضابطهٔ $xyz \neq ۰$ ندارد. به‌خصوص، اثبات قضیهٔ کومر مبنی بر اینکه این حدس به‌ازای $n = p$، p عدد اول منظم، درست است، به‌طور کامل آمده است. بخش پایانی به بعضی نتایج اخیر فورت‌وینگلر[1] (۱۹۱۲)، ویفریش[2] (۱۹۰۹)، میریمانوف (۱۹۱۰) و فان‌دیور[3] می‌پردازد.

دنیای ریاضی به پروفسور لانداو که این همه دستاوردهای عالی جدید در نظریهٔ اعداد را قابل دسترس ساخته است دین بسیار بزرگی دارد.

جورج دیوید برکاف

******

نقل از

Bull. Amer. Math. Soc. **35** (1929), 401-403.

دستگاههای دینامیکی، اثر برکاف

Dynamical systems, by G. D. Birkhoff, American Mathematicasl Society Colloquium Publications, vol. IX, 295 pp.

با نشر این رشته سخنرانیها، مؤلف ایده‌ها و نتایجی را که در تحقیقات بیست سال اخیرش در زمینهٔ نظریهٔ دینامیکی به‌دست آورده است، در یک جلد عرضه می‌کند. این همان دینامیک نوین به مفهومی است که سرچشمهٔ آن اندیشه‌های پوانکاره است. برای پی‌بردن به اینکه قلمرو بحث کتاب چیست، باید جزئیات آن را در نظر گرفت.

...

1. Furtwängler 2. Wieferich 3. Vandiver

وقتی از بررسی جزئیات اثر به بررسی کلی آن روی می‌آوریم، کار دشواری در پیش داریم: به نقد یک کتاب می‌پردازیم و خود را در حال نظردادن دربارهٔ یک نظریه می‌یابیم. صرف این واقعیت گویاتر از هر اظهار نظر ماست.

در بارهٔ ارزش یک موضوع ریاضی چگونه باید داوری کرد؟ آیا ارزش آن در منظره‌ای از دنیای واقعی است که به ما نشان می‌دهد و بدون کمک آن موضوع نمی‌توانستیم آن را ببینیم؟ اگر چنین باشد، مباحثی که در اینجا موردنظر ما هستند، بسیار نویدبخش‌اند زیرا منشأ تاریخی آنها کاملاً فیزیکی است. اما آنها از سرچشمه‌های خود بسیار دورافتاده‌اند و اکنون این نظریه به تحلیل عمیقِ روشهایی می‌پردازد که کارایی آنها در گذشته به ثبوت رسیده است نه به مطالعهٔ مستقیم واقعیت فیزیکی. از آن گذشته، واقعیت نگران‌کننده این است که ویژگیهایی که اغلب مورد بررسی قرار می‌گیرند ویژگیهایی هستند که با تغییر بینهایت کوچکی در شرایط فیزیکی حاکم بر مسأله یا با کوچکترین تغییر در داده‌های اولیه، کلاً تغییر می‌کنند. در دنیای اندازه‌گیری، چنین ویژگیهایی مطرح نیستند.

آیا ارزش یک رشته به روابطش با بخشهای دیگر علم وابسته است؟ اگر نقد ما نتوانسته باشد نشان دهد که این موضوع نه تنها روابط گسترده‌ای با دانشهای موجود دارد بلکه نویدبخش شروع پیشرفتهای بیشتر در ریاضیات است، در کار خود ناکام مانده است.

ولی یک محک روشنفکرانه هست که محک غایی است و با محکهایی که در جستجوی ارزش نظریه در خارج آن هستند تفاوت دارد و آن، داوری در بارهٔ نظریه براساس ارزش زیبایی‌شناختی و اهمیت ساختار آن است. شاید نظریهٔ دینامیکی چنین ارزشی را به طرز نمایانتر و برجسته‌تری کسب کرده باشد تا مثلاً هندسهٔ تصویری، یا نظریهٔ گروهها. و امتیاز چنین موفقیتی بیشتر از هر کسی به مؤلف این کتاب تعلق می‌گیرد.

ب. اُ. کوپمن[1]

******

نقل از

Bull. Amer. Math. Soc. **36** (1930), 162-166.

جبر نوین، اثر وان در وردن

Moderne algebra, by B. L. van der Waerden, Unter Benutzung von Vorlesungen von E. Artin und E. Noether, Springer, Berlin, 1931, Vol. I, viii+243 pp., Vol. II, vii+216 pp.

هر کسی که کتاب جدید وان در وردن را بخواند، فوراً برایش آشکار می‌شود که جبر نوینْ موضوعی کاملاً متفاوت با جبر کلاسیک است که در آخرین دورهٔ

1. B. O. Koopman

طلایی خود با دستاوردهای ددکیند، وبر، فروبنیوس، و کرونکر به اوج رسید. درست است که با مطالعهٔ دقیقتر معلوم می‌شود تفاوت اصلی در بسیاری موارد در شکل عرضهٔ مطلب نهفته است، ولی این هم درست است که مسائل جبر نوین در خیلی از موارد گسترده‌تر و دارای خصلتی متفاوت‌اند.

مکتب جدید جبر مجرد به صورت یکی از قویترین شاخه‌های ریاضیات امروزی در آلمان درآمده است. اصول اساسی آن ارتباط نزدیکی با ایده‌های هیلبرت در بارهٔ صوری‌سازی ریاضیات، یعنی تحویل همهٔ نظریه‌ها به یک، پایهٔ اصل موضوعی مرکب از ویژگیهای روابط بین عناصر تعریف‌نشده، دارند. البته ساختن نظریه‌ای ریاضی با استفاده از اصول موضوع آن چیز تازه‌ای نیست؛ ولی مسألهٔ اصلی جبر مجرد تعیین همهٔ سیستمها با یک پایهٔ عملیاتی مفروض یعنی یافتن ویژگیهای ساختاریِ همهٔ این‌گونه سیستمهاست. ملاحظهٔ اینکه این کار تا چه حد قابل توجهی میسر بوده است، جالب است. یک پیامد مستقیم آن، شناخت عمیق مفروضات بنیادی هر نظریه و قضیه است؛ ولی از این هم مهمتر، شناخت مبنای انتزاعی بسیاری از تحقیقات ریاضی، از جمله در خارج از خودِ جبر، است که جبر مجرد را به‌صورت مبحثی وحدت‌بخش که در این عصر تخصص‌گرایی به‌شدت مورد نیاز است، درآورده است.

یکی از مقاله‌های بسیار مهم جبر مجرد، تحلیل معروف اشتاینیتس[1] از ساختار هیأتهاست. به دنبال آن پژوهشهای زیادی در بارهٔ ساختار گروهها، حلقه‌ها، ایده‌آلها، دستگاههای فرامختلط[2] و غیره انجام شده است که با نام آرتین، کرول، نوتر، و دیگران همراه است. در مورد دستگاههای فرامختلط، تحقیقات ودربرن و دیکسن برجسته و بارز است.

این کتاب جدید جبر می‌خواهد راهنمایی برای این‌گونه تحقیقات باشد، و از بسیاری لحاظ بیش از آن است. وان در وردن تحقیقات گوناگون را هماهنگ ساخته و سعی کرده است آنها را از کلیترین دیدگاه ممکن بررسی کند. بنابراین محتوای کتاب او بیش از خلاصهٔ نظریهٔ قبلی است و این کتاب تا سالهایِ سال جایگاه شامخی در میان کتابهای جبر خواهد داشت. این متنْ کتاب درسی به مفهوم متعارف آن نیست و برای مطالعهٔ آن لازم است خواننده اطلاعات مقدماتی وسیعی داشته باشد، هر چند بحث در مورد هر یک از موضوعها از مبانی آن آغاز شده است. با این حال، من مطمئنم که دانشجویان پیشرفته و ریاضیدانان علاقه‌مند به جبر آن را با لذت فراوان خواهند خواند.

اُیستاین اُر

******

نقل از

Bull. Amer. Math. Soc. **38** (1932), 327-329.

1. Steinitz 2. hypercomplex

مفاهیم بنیادی حساب احتمالات، اثر کولموگوروف

Grundbegriffe der Wahrscheinlichkeitsrechnung, by A. Kolmogoroff, Julius Springer, Berlin, 1933, 62 pp.

هدف این تکنگاشتْ شرح و بسط نظریهٔ احتمال از دیدگاه اصل موضوعی است. به این منظور یک میدان احتمال به‌صورت گردایه‌ای با اعداد منسوب به ترتیب خاص که در دستگاه اصول موضوع صدق می‌کنند، تعریف می‌شود. شرح مختصری در بارهٔ ساختن این‌گونه میدانها و نحوهٔ ارتباط دادن چارچوب این دستگاه اصل موضوعی به کاربردهای پدیده‌ها داده می‌شود. قضیه‌های جمع و ضرب بلافاصله نتیجه می‌شوند. به‌علاوه قضیهٔ بیز هم که در مورد اعتبار آن مشاجرات بسیاری وجود داشته است، پیامدی تقریباً مستقیم از این دستگاه اصول موضوع است، ولی ناقد گمان نمی‌کند که با این استنتاج قضیهٔ بیز، منازعهٔ قدیمی بر سر اعتبار استنتاج خصوصیات یک جامعهٔ آماری از روی یک نمونه با استفاده از قضیهٔ بیز، فیصله یابد.

از نظریه‌های اندازه و انتگرالگیری لبگ در این کتاب استفاده می‌شود. درواقع عقیده بر این است که بررسی مبانی منطقی احتمال بدون این نظریه‌ها تقریباً بی‌نتیجه است.

این شرح شامل ارائهٔ میدانهای نامتناهی احتمال به‌وسیلهٔ یک اصل موضوع اضافی، توزیعهای احتمال در فضای بسیار بعدی، مشتقگیری و انتگرالگیری از امید ریاضی، و قانون اعداد بزرگ است. به نظر این ناقد، این کتاب کوچک خدمت مهمی است در جهت عرضهٔ نظریهٔ احتمال به‌صورت منطقیتر.

هـ. ل. ریتس[1]

******

نقل از

Bull. Amer. Math. Soc. **40** (1934), 522-523.

توپولوژی I، اثر الکساندروف و هوپف

Topologie I, by Paul Alexandroff and Heinz Hopf, Springer, Berlin, 1935, xiii+636 pp.

توپولوژیْ موضوع جدیدی نیست. اگر آغاز پیدایش آن را طرح مسألهٔ هفت پل کونیکسبرگ به‌وسیلهٔ اویلر در ۱۷۳۶ بدانیم، امسال دویستمین سالگرد تولد آن است. ولی مطالعهٔ نظام‌مندِ توپولوژی تازگی دارد و از پژوهشهای پوانکاره در آغاز این قرن شروع شده است. «کنفرانس بین‌المللی در بارهٔ توپولوژی» که سپتامبر گذشته در مسکو برگزار شد، نشان داد که این موضوع به درجهٔ معینی از بلوغ و پختگی و به نفوذ گسترده‌ای بر سایر شاخه‌های ریاضیات دست یافته است ولی هنوز هم در حال رشد سریع و تغییر و تحول است. به محض اینکه فعالیت در زمینهٔ توپولوژی رو به کاهش می‌گذارد، پیدایش دیدگاه جدیدی دوباره باعث تکاپو و تشدید فعالیت در این زمینه می‌شود. نمونه‌ای از آن مطرح‌شدن «دورهای دوگان»[2] الکساندر و کولموگوروف در سال گذشته است.

1. H. L. Rietz 2. dual cycles

کتاب در زمینهٔ توپولوژی آنقدرکم است که درآمدن هرکتاب تازه‌ای، واقعهٔ مهمی است. کتابی که پیش روی ماست بسیار تحسین‌برانگیز است، نه فقط به خاطر حجم و جامعیت خودش بلکه همچنین به دلیل آنکه اولین جلد از سه‌جلد کتابی است که قرار است روی هم شامل بحث و بررسی مبسوطی از کل توپولوژی باشند. مؤلفان هندسه‌دانان ممتازی هستند که در ارتباط نزدیک با مراکز متعدد توپولوژی در اروپا و آمریکا بوده‌اند. آنها کار دشوارشان را چندین سال پیش به پیشنهاد کورانت آغاز کردند و این کتاب به ویراستاری او به عنوان چهل‌وپنجمین اثر در سری معروف اشپرینگر انتشار می‌یابد. بسیاری از ما از این پروژه آگاه بوده و بیصبرانه در انتظار پایان کار بوده‌ایم.

مؤلفان در تشریح توپولوژی به مفهوم عام راه میانه‌ای برگزیده‌اند که بین نظریهٔ مجموعه‌های نقاط از یک سو و توپولوژی جبری از سوی دیگر قرار دارد. این کار را خیلی راحت انجام داده‌اند زیرا هر دوی آنها در تحقیقات خودشان از روشهای ترکیبیاتی برای حل مسائلی با ماهیت نظریهٔ مجموعه‌ای استفاده کرده‌اند؛ بهترین مثال از این‌گونه اختلاط، نظریهٔ الکساندروف در بارهٔ بعد است. مفهوم مرکزی این جلد اول، چندوجهی (اقلیدسی) است، یعنی زیرمجموعه‌ای از فضای اقلیدسی چندبعدی که به روش معمول قابل افراز به حجره‌ها[1]ی محدب تخت است. در برنامهٔ مؤلفان، چندوجهی در موضعی میانی، بین فضای مجرد که خیلی کلی است و خمینه که خصلت خاصی دارد، قرار گرفته است. مثلاً می‌توان با تقریب مناسبی از چندوجهی به فضاهای متری فشرده رسید و با تخصیص مناسبی، از چندوجهی به خمینه. طبق این برنامه، جلد دوم به مسائل نظریهٔ مجموعه‌ای از قبیل بعد خواهد پرداخت و جلد سوم به خمینه‌ها.

آلبرت تاکر

******

نقل از

Bull. Amer. Math. Soc. **42** (1936), 782-784.

رویه‌های جبری، اثر زاریسکی

Algebraic surfaces, by Oscar Zariski, Ergebnisse der Mathematischen Wissen-schaften, Volume 3, Berlin, 1935, v+198 pp.

امروز در هندسهٔ دوگویا[2]ی رویه‌ها و چندگونا [واریته]ها، بیشتر از هر مبحث دیگر ریاضیات، نیاز آشکاری به شرح و توصیف کامل و نقادانه داریم. در مورد رشته‌ای که در این همه جهات گوناگون رشد یافته است، این کار مسلماً بسیار دشوار است، ولی مطمئناً ضروری است، به دو دلیل: نخست اینکه، بررسی روشمند مواضع تسخیر شده ارزش قابل توجهی در مبارزات بعدی خواهد داشت؛ دوم اینکه سرزمینی که تاکنون فتح شده و صحیح و سالم نگهداری شده، فوق‌العاده زیباست و سزاوار آن است که نه تنها گروه پرقدرت ولی کوچکِ لشکریان فاتح بلکه گردشگران عادی نیز این زیبایی را تحسین کنند. اگر بخواهیم کمتر از زبان استعاره استفاده کنیم، باید بگوییم نقادی و سنجشگری از نوع «کانتوری» در این بخش از ریاضیات برخلاف بخشهای دیگر عمیقاً رخنه نکرده است. نتیجهٔ این وضع، شک و تردید رایج نسبت به این علم است که همه علاقه دارند هر چه سریعتر رفع شود. هیچ چیزی بیشتر از کتاب عالی زاریسکی به این هدف شایسته خدمت نمی‌کند. واقعاً اولین بار است که متخصصی با صلاحیت، آگاه از همهٔ مراحل و جوانب موضوع، آن را به دقت و نقادانه بررسی کرده است. حاصل کار، تکنگاشتی بسیار جالب و ارزشمند برای عموم ریاضیدانان و در عین حال کتاب راهنمایی استاندارد و ضروری برای همهٔ دانشجویان این مباحث است.

خوب می‌دانیم که اگر سعی کنیم از هندسهٔ دوگویای یک‌بعدی به ابعاد بالاتر برویم، مشکلات صد چندان می‌شود. بسیاری از قضایا اصلاً صادق نمی‌مانند، یا اگر صادق بمانند جنبهٔ بسیار پیچیده‌ای پیدا می‌کنند یا اثبات بسیار دشواری می‌طلبند.

به عنوان نمونه، این دو مسأله را در نظر بگیرید: (الف) تحویل تکینه‌ها؛ (ب) تعمیم ویژگیهای گونهٔ خم جبری. مدتها، اثباتهای کامل و رضایت‌بخشی برای این حکم داشته‌ایم که هر خم جبری تحویل‌ناپذیر به طور دوگویا قابل تبدیل به یک خم ناتکین در یک فضا یا به یک خم مسطح با تکینه‌های ساده و بی‌آزار است. حکم مشابهی به طور مسلم در مورد رویه‌ها و چندگوناها برقرار است. صرف‌نظر از چندگوناها که در مورد آنها ابهام کامل حکمفرماست، اثبات حکم در مورد رویه‌ها نیز به سردرگمیِ بسیار انجامیده است. در تکنگاشت زاریسکی نخستین بررسی انتقادی و کامل از این وضعیت را ملاحظه می‌کنیم. در ضمن این بررسی آشکار می‌شود که تنها اثبات «قابل تأیید»ی که فعلاً موجود است، اثبات واکر[1] (آنالز آو متمتیکس، آوریل ۱۹۳۵) است.

مطالب پیشگفته ممکن است خواننده را به این قضاوت نامنصفانه رهنمون شود که زاریسکی همّ خود را عمدتاً مصروف بررسی نقادانه کارهایی کرده است که خیلی قبل انجام شده است. ولی واقعیت این است که این نقادیها فقط نیمی از تکنگاشت را دربرمی‌گیرد و در بقیهٔ آن به مسائل نوین پرداخته شده است. مثلاً ساختار توپولوژیک رویه با دقت بسیار بررسی شده است؛ قضایای جدید و بسیار برجستهٔ هاج[2] چنانکه باید و شاید تشریح شده‌اند؛ همین‌طور خلاصه‌ای از نظریهٔ سری نقطه‌ای هم‌ارزی بر رویه‌ها که به تازگی، عمدتاً به وسیلهٔ سوری[3]، پرورانده شده، همراه با ارتباطات این نظریه با نظریهٔ توپولوژیک نقطهٔ ثابت این ناقد، آورده شده است. روی‌هم‌رفته این کتاب را قویاً به همهٔ دوستداران هندسه، در هر شکل آن، توصیه می‌کنیم. آنها با مطالعهٔ

1. cells 2. birational

1. R. J. Walker 2. Hodge 3. Severi

این تکنگاشت زیبایی و سرزندگیِ این شاخه فوق‌العاده جذاب از پژوهشهای ریاضی نوین را تصدیق خواهند کرد.

سالومون لفشتس

******

نقل از

Bull. Amer. Math. Soc. **42** (1936), 13-14.

سریهای مثلثاتی، اثر زیگموند

Trigonometric series, by Antoni Zygmund, Warsaw, Monografje Matematyczne, Volume V, 1935, iv+320 pp.

این ناقد چند بار سعادت آن را یافته است که احساس تحسین خود را نسبت به استانداردهای بالا و کیفیت عالیِ رشته تکنگاشتهایی که اکنون به بررسی جلد پنجم آنها می‌پردازد، ابراز دارد. هر جلد از این سری که تاکنون انتشار یافته است نشان‌دهندهٔ رویداد مهمی در پیشرفت پژوهشهای ریاضی است، و جلد حاضر نیز از این قاعده مستثنا نیست. هر کس به فهرست طویل کتابهایی که در بارهٔ سری فوریه نوشته شده نگاهی بیندازد، ناگزیر احساس خواهد کرد که حتی حجیمترین آنها نتوانسته‌اند تصویر گویایی از وضعیت فعلی این مبحث ارائه کنند. نه تنها مبتدیان بلکه متخصصان نیز عدم وجود رساله‌ای را که چنین تصویری به‌دست دهد، به شدت احساس می‌کردند، و شکست تلاشهای بسیار برای نوشتن کتابی واقعی در بارهٔ سری فوریه این احساس را پدید آورد که چنین کاری تقریباً نشدنی است. مؤلف تکنگاشت حاضر در رفع این «عقدهٔ حقارت» کاملاً موفق بوده و کتابی پدید آورده است که نه تنها خواننده را وارد قلمرو گستردهٔ نظریهٔ سریهای فوریه می‌کند بلکه بدون آنکه برای خواننده چندان محسوس باشد او را با آخرین دستاوردها نیز روبه‌رو می‌سازد، دستاوردهایی که بسیاری از آنها مرهون خود مؤلف است. سبک کتاب دقیق و مستحکم و بیان آن شیوا و حتی در کوچکترین جزئیات، واضح است.

مؤلف بدون آنکه وقت خود و خواننده را با چیزهای غیراساسی تلف کند کوشیده است هر مسألهٔ خاص را با روشهایی بررسی کند که آن مسأله را از دیدگاهی کلی روشن سازند، و نیز جایگاه آن مسأله را در کل ساختار موضوع نشان داده است. چنین شیوه‌ای در عرضهٔ مطلب، برای مبتدیان فوق‌العاده مفید و برای متخصصان دلپذیر است.

ج. د. تامارکین

******

نقل از

Bull. Amer. Math. Soc. **42** (1936), 11-13.

سریهای مثلثاتی (ویراست دوم)، اثر زیگموند

Trigonometric series, by A. Zygmund, 2d. ed., vols. I and II, Cambridge University Press, NewYork, 1959, 12+383 pp. and 7+354 pp., $15.00 each or $27.50 set

پروفسور لیتلوود در درس خود در دانشگاه کیمبریج، نخستین ویراست کتاب زیگموند را «ام‌الکتاب» می‌نامید. این ویراست دوم، که تقریباً بیست‌وپنج سال پس از اولی از چاپ درآمده است، بدون شک حتی بیشتر از ویراست اول سزاوارِ آن لقب است، نه تنها به دلیل آنکه دستاوردهای این مبحث در طی این دوره در آن ملحوظ شده است بلکه همچنین به خاطر اینکه نویسنده، که از تجربیات جدیدی بهره‌مند شده و دائماً درکار قبلی خود تأمل می‌کرده است، بسیاری از موضوعاتی را که در ویراست اول کنار گذاشته بود در این ویراست آورده است.

کتاب به دو ریاضیدان درگذشتهٔ لهستانی، راچمان[1] و مارسینکیوویچ[2] تقدیم شده است که هر دونفر در جریان جنگ جهانی دوم سرنوشت غم‌انگیزی یافتند: راچمان را نازیها اعدام کردند و مارسینکیوویچ در شرایطی که هنوز کاملاً معلوم نشده است جان سپرد. اولی را زیگموند «معلم» و دومی را «شاگرد» خود می‌نامد، ولی هر دو نفر تأثیر قابل ملاحظه‌ای بر تفکر ریاضی زیگموند داشته‌اند و او برای نبوغ این دو ریاضیدانِ متعلق به مکتب مشهور ریاضی لهستان به یک اندازه احترام قائل بوده است.

چنانکه مؤلف در پیشگفتار گفته است، او عمداً همهٔ تعمیمهای جدید نظریه به هیأتهای مجرد را کنار گذاشته است و ویراست دوم نیز، مانند ویراست اول، به نظریهٔ کلاسیک اختصاص دارد.

رافائل سلم[3]

******

نقل از

Bull. Amer. Math. Soc. **66** (1960), 6-12.

نظریهٔ گروههای متناهی ... ، اثر کارتان

La théorie des groupes finis et continus et la géométrie différentielle traitées par méthode du repère mobile, by Élie Cartan, Cahiers Scientifiques, no. 18, Gauthier-Villars, Paris, 1937, 6+269 pp.

1. A. Rajchman 2. J. Marcinkiewics 3. R. Salem

این کتاب که منشأ آن رشته درسهایی است که در سالهای ۱۹۳۱ـ۱۹۳۲ در سوربن ارائه شده است، اساساً همان مطالب جلد شمارهٔ ۱۹۴ (سال ۱۹۳۵) از سری کتابهای «رویدادهای جاری علمی و فنی»[1] را به صورتی صریحتر دربردارد. مؤلف با استفاده از روش کنج متحرک، به بررسی خمینه‌های داخواه M_λ در فضای کلاینی R می‌پردازد که هندسه‌اش با گروه همریختیهایش توصیف می‌شود. هدف اصلی این نقد نشان دادن مبانی اصل موضوعی این نظریه است.

کتاب مورد نقد منظور سه‌جانبه‌ای دارد: این کتاب شامل (۱) توصیفی از نظریهٔ کلی گروههای لی پیوستهٔ متناهی با استفاده از اصطلاحاتی متناسب با کاربردهای آن در هندسهٔ دیفرانسیل، (۲) توصیفی کلی از روش کنج متحرک؛ و (۳) کاربرد آن در تعدادی مثال مهم است. ترتیب مطالب بیشتر براساس هدفهای آموزشی است تا طبق اسلوب و قاعده.

همهٔ کتابهای این مؤلف، که اثر حاضر هم از آنها مستثنا نیست، بسیار تفکر برانگیز، مملو از دیدگاههای اصیل، و سرشار از ریزه‌کاریهای هندسی جالب است. کارتان بی‌تردید بزرگترین استاد زندهٔ هندسهٔ دیفرانسیل است. این نقد ناقص است زیرا فقط سعی کرده است ریشه‌ها را نشان دهد نه آنکه برگهای سبز فراوان درختی را که کتاب جلو چشمان خواننده قرار می‌دهد توصیف کند. باید از شایستگی ژان لری[2] نیز یاد کرد که یادداشتهای درسی را در چنان قالبی ریخته است که حاصل کار یک کتاب واقعی است ولی از شور و سرزندگی اصل درسها نیز تا حدی برخوردار است. با این حال، باید اعتراف کنم که خواندن این کتاب را، مانند بیشتر نوشته‌های کارتان، دشوار یافتم. آیا دلیل آن در سنت هندسی پربار فرانسه نهفته است که کارتان از آن بهره می‌گیرد، و در سبک و محتوایی که او کمابیش به‌عنوان زمینهٔ مشترک برای همهٔ هندسه‌دانان مفروض می‌گیرد درحالی که ما، که در کشورهای دیگر زاده شده و تحصیل کرده‌ایم، در آن شریک نیستیم؟

هرمان وایل

******

نقل از

Bull. Amer. Math. Soc. **44** (1938), 598-601.

روشهای فیزیک ریاضی، اثر کورانت و هیلبرت

Methoden der mathematischen Physik, Vol. 2, by R. Courant and D. Hilbert, Die Grundlehren der mathematischen Wissenschaften in Einzeldarstellungen, vol. 48, Springer, Berlin, 1937, 16+544 pp.

1. *Actualités Scientifiques et Industrielles* 2. Jean Leray

سیزده سال از انتشار جلد اول اثر کورانت و هیلبرت با عنوان «روشهای فیزیک ریاضی» می‌گذرد، و این دومین جلد و جلد پایانی آن است. این دو جلد کتاب، یادگاری زیبا، ماندگار، و اثرگذار از کارهایی است که کورانت، با الهام از معلم کبیرش هیلبرت و با همکاری بسیاری از شاگردان با استعدادش، هم در زمینهٔ پژوهش و هم در آموزش پیشرفته، در گوتینگن انجام داد. کورانت زمانی به گوتینگن رفت که آلمان درگیر مسائل سیاسی و اقتصادی بیشمار و وارث مشکلات بسیار بود، زمانی که عصر قهرمانان، کلاین، هیلبرت، و مینکوفسکی به پایان خود نزدیک می‌شد. ولی او با تحقیق و تدریسش، با روابط شخصیش، و با ایجاد و ادارهٔ «مؤسسهٔ ریاضیات» جدید به شیوه‌ای مثال زدنی، تمام تلاشی را که در توان یک فرد انسانی است انجام داد تا سنت ریاضی قدیم گوتینگن را ترویج کند و تکامل بخشد. اینکه سرزمین پدریش چگونه پاداش او را داد، داستان معروفی است. به نظر ناقد، انتشار جلد حاضر فرصت مناسبی پیش آورده است که قدردانی بقیهٔ جهان ریاضی از کارهای او ابراز شود.

جلد نخست این کتاب به مبحثی بسته و تقریباً یکپارچه یعنی نظریهٔ ویژه‌مقدارها و ویژه تابعها اختصاص داشت. آن جلد موفقیت عظیمی، به‌خصوص در میان فیزیکدانان، به دست آورد زیرا مدت کوتاهی پس از انتشار آن، این موضوعات به یمن معادلهٔ موج شرودینگر اهمیت غیرمنتظره‌ای در فیزیک کوانتومی کسب کرد. این جلد در بارهٔ همهٔ جنبه‌هایی از نظریهٔ معادلات دیفرانسیل جزئی است که در مسائل فیزیک اهمیت دارد. بنابراین، فهرست مندرجات آن ضرورتاً خیلی متنوعتر و مفصلتر است و در نتیجه این جلد نتوانسته است به آن کمال زیبایی که جلد اول به خاطر وحدت موضوع دارد، نائل شود. ولی غنای مطالب آن، این نقیصه را جبران می‌کند، و از جنبهٔ آموزشی نیز مانند جلد اول بسیار موفق است. امروز بسیاری از کتابهای ریاضی به نظر نمی‌رسد به قلم شخص زنده‌ای نوشته شده باشند که نه تنها می‌داند بلکه شک می‌کند، می‌پرسد، و حدس می‌زند، شخصی که جزئیات را در منظر واقعیشان می‌بیند ــ روشنی در محاصرهٔ تاریکی ــ شخصی که، برخوردار از حافظه‌ای محدود، در تاریک و روشن پرسشگری، کشف، و تسلیم و رضا، تار و پودی به هم می‌بافد که ناقص اما تکامل یابنده است و اجزای آن درجات مختلفی از اهمیت دارند. این‌گونه کتابها تقریباً مانند دستگاه جک پات هستند که در ازای سکه‌ای که در آن می‌اندازید، مخلوطی از اصل موضوع، تعریف، لم، و قضیه به شما می‌دهد و سپس بی‌حرکت می‌ماند، هر چند آن را تکان بدهید. کورانت در مورد مبحثی که جنبه‌های گوناگونی دارد بینش عمیقی به خواننده می‌دهد و روشهایی عرضه می‌کند بدون اینکه آنها را به رشتهٔ گسسته‌ای از قضایا تجزیه کند، و با این حال، قضایای اساسی به‌وضوح برجسته می‌شوند. با مثالهای جالب فراوان به نظریه‌های کلی روح می‌بخشد و آنها را روشن می‌سازد. من این جلد را از جنبهٔ دیگری هم تسلی‌بخش می‌یابم: کسی که همچون بسیاری از ما خودش را در باغهای گل جبر مجرد یا توپولوژی گم کرده است در اینجا، شاید با شگفتی، می‌بیند که باغ آنالیز کلاسیک چقدر بزرگ و پرمیوه است.

در سراسر جلد حاضر، نکته‌های روشنگر کوچک و جدیدی به وفور دیده می‌شود که در این نقد باید از آنها بگذریم. مؤلف پوزش خواسته است که به علت کمبود وقت نتوانسته است کتاب را به نمایهٔ کاملی از نوشتگان

موجود و سازوبرگهایی از این قبیل مجهز سازد. ممکن است وجود معدودی اشتباه چاپی نیز که گاه خواننده را گیج می‌کند به همین علت باشد. ولی شاید این اشکالات جزئی هم سزاوار ستایش باشد نه سرزنش. می‌دانم که افتخار هر استادکاری این است که کارش تا حد امکان، حتی در ریزترین و غیراساسی‌ترین جزئیات، بی‌نقص و آراسته باشد. ولی گاهی به این فکر می‌کنم که آیا ما در صرف وقت برای آراستن کتاب بیش از حدّ گشاده‌دست نیستیم؟ و بهتر نیست این وقت را صرف چیزهای مهمتری کنیم؟

هرمان وایل

* * * * * *

نقل از

Bull. Amer. Math. Soc. **44** (1938), 602-604.

گروههای کلاسیک، اثر هرمان وایل

The classical groups, by Hermann Weyl, University Press, Princeton, 1939, 11+302 pp.

واقعیتی تعجب‌آور این است که در حالی‌که تقریباً همهٔ کتابهای درسی جبر عالی قبل از سال ۱۹۳۰ فضای قابل توجهی را به موضوع ناورداها اختصاص می‌دادند، کتابهای اخیر در این زمینه که از دیدگاه اصل موضوعی نگاشته شده‌اند آن را کاملاً نادیده گرفته‌اند. به علت این غفلت، عبارت «نظریهٔ ناورداها» معمولاً موضوعی را به ذهن می‌آورد که زمانی جاذبه و اهمیت بسیار داشت ولی بر پیشرفتهای نوین جبر تأثیر خیلی کمی داشته است. بنابراین پروفسور وایل در این کتاب کار مهم و اصیلی کرده است که نظریهٔ ناورداها را به جریان اصلی جبر مربوط ساخته و نشان داده است که این موضوع نه تنها گذشتهٔ درخشان بلکه آینده‌ای هم دارد.

نظریهٔ ناورداها در این بررسی به‌صورت بخشی از نظریهٔ نمایشها درآمده است. بنابراین، طبیعی‌ترین راه برای شروع مطالعهٔ ناورداهای یک گروه خاص، تعیین نمایشهای آن است. بخش بزرگی از کتاب مربوط به این مسأله است وقتی برگروههای «کلاسیک» $GL(n)$، گروه خطی کامل، گروه متعامد $O(n)$، و گروه همتافته[1] (مختلط یا آبلی) $S(n)$ اعمال می‌شود.

در بحث نمایشهای یک گروه مجرد g مناسب است به مجموعهٔ ماتریسهای نمایشگر، ترکیبات خطی آنها را الحاق کنیم. مجموعهٔ حاصل یک جبر است، جبر پوشانندهٔ[2] مجموعهٔ اصلی، و نمایشی از یک جبر مجرد خاص را تعریف می‌کند که جبر گروهی است یعنی با g و هیأت ضریبها کاملاً معین می‌شود. به این طریق، نظریهٔ جبر قابل کاربرد است. مؤلف از نیازهای مستقیمی که

1. symplectic 2. enveloping algebra

در بحث در این زمینه داشته قدری فراتر می‌رود. بنابراین کتاب او می‌تواند به‌عنوان درآمد بسیار خوبی بر این نظریه نیز به‌کار آید.

نیتان جیکوبسن

* * * * * *

نقل از

Bull. Amer. Math. Soc. **46** (1940), 592-595.

سازگاری اصل موضوع انتخاب و ...، اثر کورت گودل

Consistency of the axiom of choice and of the generalized continuum-hypothesis with the axioms of set theory, by Kurt Gödel, Annals of Mathematics Studies, no. 3, University Press, Princeton; Humphrey Milford and Oxford University Press, London, 1940, 66 pp., $1.25

در این بررسی ثابت شده است که اصل موضوع انتخاب و فرض تعمیم‌یافتهٔ پیوستار کانتور با سایر اصول موضوع نظریهٔ مجموعه‌ها سازگارند. به شرط آنکه اصول اخیر خودشان سازگار باشند. دستگاه $\sum$ از اصول موضوع که برای نظریهٔ مجموعه‌ها پذیرفته شده است اساساً همان دستگاه برنایس[1] (جورنال آو سیمبالیک لاجیک، جلد ۲، ص ۶۵) است.

سی. سی. تورنس[2]

* * * * * *

نقل از

Bull. Amer. Math. Soc. **47** (1941), 191-192.

نظریهٔ بازیها و رفتار اقتصادی، اثر فون نویمان و مورگنسترن

Theory of games and economic behavior, by John von Neumann and Oskar Mor-genstern, Princeton University Press, 1944, 18+625 pp., $10.00

1. P. Bernays 2. C. C. Torrance

آیندگان ممکن است این کتاب را یکی از دستاوردهای علمی مهم نیمهٔ اول قرن بیستم به شمار آورند. این ارزیابی بدون شک صحیح خواهد بود اگر مؤلفان توانسته باشند یک علم دقیقِ تازه ــ علم اقتصاد ــ را ایجاد کنند. پایه‌ای که به این منظور گذاشته‌اند فوق‌العاده نویدبخش است. چون برای پیشرفتهای بعدی این نظریه هم به ریاضیدانان و هم به اقتصاددانان نیاز خواهد بود، شرحی در بارهٔ زمینهٔ لازم برای مطالعهٔ این کتاب مناسبت دارد. ریاضیات لازم فراتر از جبر و هندسهٔ تحلیلی در کتاب تشریح شده است. ولی خواننده‌ای که آموزش ریاضی ندیده است لازم است شکیبایی زیادی داشته باشد تا نظریه را بفهمد. خوانندهٔ ریاضی‌خوانده، استدلالها را جالب و فکربرانگیز خواهد یافت. در مورد اقتصاد، اطلاعات محدودی کفایت می‌کند.

مؤلفان دریافته‌اند که دادوستد تجاری دارای بسیاری از ویژگیهای بازی است و در این کتاب بررسی گسترده‌ای از استراتژی بازیها با در نظر داشتن این تشابه انجام داده‌اند (عنوان کتاب از اینجا می‌آید) در بازی زندگی، آنچه به‌دست می‌آورند یا از دست می‌دهند لزوماً پول نیست بلکه ممکن است از نوع مطلوبیت باشد. در بحث از مطلوبیتها، مؤلفان صلاح دیده‌اند به جای نظریهٔ مطلوبیت نهایی که پرسش‌برانگیز است نظریهٔ جدیدی را که برای تحلیلشان مناسبتر است به کار گیرند. آنها خاطرنشان می‌کنند که در بازی زندگی، و نیز در بازیهای اجتماعی، بازیکنان غالباً لازم است شقی را از بین شقوق مختلف برگزینند، شقوقی که با احتمال همراه‌اند نه با قطعیت. مؤلفان نشان می‌دهند که اگر بازیکنی همواره بتواند این‌گونه شقوق شانسی را به ترتیب ترجیحاتش مرتب کند آنگاه می‌توان به هر شق یک عدد یا مطلوبیت عددی که بیانگر میزان اولویت و ترجیح آن شق در نظر آن بازیکن باشد نسبت داد، این انتساب منحصر به فرد نیست ولی دو تا از این‌گونه انتسابها باید با ترکیبی خطی به هم مربوط باشند.

ا. ه. کوپلند[1]

* * * * * *

نقل از

Bull. Amer. Math. Soc. **51** (1945), 498-504.

نظریهٔ توابع جبری یک‌متغیره، اثر شواله

Introduction to the theory of algebraic functions of one variable, by C. Chevalley, Mathematical Surveys, no. 6, American Mathematical Society, NewYork, 1951, 12+188 pp., $4.00

این جبر است با شدت و حدتی تمام؛ ناب‌نگری جبری از این بیشتر نمی‌توانست باشد. مؤلف می‌گوید «ما سعی نکرده‌ایم دابستگی خود را به رویکرد جبری پنهان کنیم». بله نکرده است، ولی اگر اشاراتی معدود در مقدمه و نکته‌ای ضمنی در انتهای فصل چهار نیامده بود، ممکن بود گمان کنیم که چیزی دربارهٔ خمهای جبری به گوش او نخورده است و یا هیچ علاقه‌ای به آن ندارد. هیأت و فقط هیأت است که موضوع بررسی اوست. هیأتی مفروض است، یا بهتر بگوییم دو هیأت: یکی هیأت R مرکب از توابع و دیگری هیأت K مرکب از ثابتها؛ K در R به طور جبری بسته است، و R متناهی‌مولد و دارای درجهٔ تعالی ۱ روی K است. همه چیز باید «درونی» باشد یعنی از اینها به وسیلهٔ عملیاتی متعارف تولید شود. پس از آن محدودهٔ خانواده گسترده‌تر می‌شود و هیأت دیگری از توابع، S، وارد کار می‌شود که شامل R است، با هیأت L مرکب از ثابتها که شامل K است، و بخش بزرگی از کتاب به روابط متقابل R و S اختصاص می‌یابد؛ ولی در هیچ جا بجز در یک یا دو لم اجازهٔ ورود به هیچ عنصری داده نمی‌شود مگر اینکه در این هیأتها باشد یا به صورت مجاز از آنها تولید شود.

مطالب کافی گفته شده است تا معلوم شود که، علی‌رغم عیبهایی که وظیفه داشتیم آنها را خاطرنشان کنیم، این کتابْ ارزشمند و مفید و نیز انتشار آن بموقع است. هر چند این نوشته فاقد گیرایی و جاذبهٔ اثر کلاسیک ددکیند و وبر یا مفهوم رویهٔ ریمانی اثر هرمان وایل است، ولی حاوی مطالب بسیار بیشتری از اولی است، و حتی در فصل آخرش چندان وجه اشتراکی با دومی ندارد. بسیار مطلوب بود که اصول نظریهٔ توابع جبری دست‌کم یک‌بار با کلیت کامل و به‌وسیلهٔ روشهای کاملاً جبری بررسی شود، و این کاری است که مؤلف انجام داده است، به صورتی که شاید کس دیگری جز خودش نمی‌توانست انجام دهد، و از این جهت حق دارد که انتظار قدردانی از جامعهٔ ریاضی را داشته باشد. رویکرد او به موضوع به اعتراف خودش یک‌جانبه است؛ ولی این اثر نه فقط از دید کسانی که همواره روشهای جبری را فی‌نفسه ترجیح می‌دهند بلکه همچنین از نظر آنها که می‌خواهند هم دامنه و هم محدودیتهای روشهای جبری را بشناسند، باارزش است. درواقع به نظر می‌رسد هم‌اکنون می‌توان در این مورد اظهارنظر کرد که به اختصار به آن خواهیم پرداخت.

پس به نظر می‌رسد ادعاهای مؤلف تا حدی مبالغه‌آمیز است، و او زیاد از حد نسبت به روشی که در دلِ جبریش عزیز است تعصب ورزیده است. چه کسی نخستین سنگ را به‌سوی او پرتاب خواهد کرد؟ تا اندازه‌ای مایهٔ تسلی است که این‌گونه علائم ضعف انسانی را در کتابی که با این شدت انسان‌زدایی شده است می‌بینیم. فقط می‌ماند که به مؤلف از بابت خدمتی که به جامعهٔ ریاضی عرضه داشته است تبریک بگوییم، البته قدری هم باید به مسائل چاپی کتاب توجه کنیم.

مطالعهٔ تفصیلی این کتاب بدون اینکه خواننده دائماً آنچه را روی کاغذ از هم جدا شده در ذهنش بازسازی کند، دشوار است؛ و صرف‌نظر از ملاحظات زیبایی‌شناختی، چنین شیوه‌هایی [در چاپ] که در این کشور به سرعت به‌صورت قاعده، نه استثنا درمی‌آید، ممکن است به زودی خواندن بسیاری

1. A. H. Copeland

از کتابهای ریاضی ما را در حد غیرقابل تحملی دشوار سازد. وقت آن است که واکنشی در برابر گرایش به چپاندن مقدار هر چه بیشتری مطلب در هر صفحه، برای به حداقل رساندن هزینه و بدون توجه به اثر آن بر خواننده، نشان داده شود. این امر مستلزم تلاش هماهنگ مؤلفان، ویراستاران، و بنگاههای نشر است. مؤلفان که بدون شک تا اندازه‌ای مسؤول وضعیت فعلی هستند، باید در هنگام آماده‌سازی دستنوشته‌هایشان بیشتر به این مسائل توجه کنند. ویراستاران و کمک‌ویراستاران نیز باید بیشتر از میزان فعلی با آنها همکاری کنند. بنگاه نشر می‌تواند به حروفچینها، که کار بسیار مهم حروفچینی پیچیده‌ترین فرمولها را انجام می‌دهند، به سادگی آموزش دهد که از شکستن فرمولها اجتناب کنند. کاملاً می‌توان به قضاوت خود حروفچینها در نمایش بعضی فرمولهای طویل، حتی وقتی مؤلف یا ویراستار علامت و نشانه‌ای نگذاشته باشد، اعتماد کرد. در مورد فرمولهای کوتاه، در اکثر موارد، تنها کاری که لازم است، تعدیل فاصلهٔ بین کلمه‌هاست؛ این کار ممکن است بیشتر از حروفچینی مکانیکی وقت بگیرد، ولی باز هم بسیار کم‌هزینه‌تر از تصحیحات نمونهٔ چاپی است که ممکن است کل یک پاراگراف را تغییر بدهد. شاید، دست‌کم در دوران گذار و تا وقتی که حروفچینان تجربهٔ کافی در این‌گونه امور به‌دست آورند، میانگین هزینهٔ صفحهٔ چاپی در متنهای ریاضی کمی افزایش یابد؛ ممکن است لازم باشد تعداد صفحاتی که هر سال مجله‌های ریاضی چاپ می‌کنند تا حدی کاهش یابد. ولی امید است فایدهٔ حاصل بیشتر از زیان این‌کار باشد.

آندره ویل

******

نقل از

Bull. Amer. Math. Soc. **57** (1951), 384-398.

نظریهٔ گروههای لی، اثر شواله

The theory of Lie groups, I, by Claude Chevalley, Princeton Mathematical Series, no. 8, Princeton University Press, 1946, 9+217 pp., $3.00

در این شاهکار فشرده‌نویسی، اجزای مفهوم گروه لی با استادی و مهارت تمام ترکیب و تلفیق شده است. حاصل کار، اثری است جذاب و شایستهٔ غور و تعمق، که مجهز به سه ساختار مرتبط با هم جبری، توپولوژیک، و آنالیزی است. هیچ قسمت و مطلب مسامحه‌آمیز و تردیدبرانگیزی در این کتاب نیست. اکنون می‌توان آزادانه در گروه لی به گشت‌وگذار پرداخت بدون نگرانی از اینکه بحث و نتیجه‌گیریها مانند معمول، فقط در فاصله‌ای از عنصر خنثی معتبر باشد.

ناقد به خصوص از این لحاظ تحت تأثیر قرار گرفته است که این همه در چنین حجم کوچکی انجام یافته است. یکی از چیزهایی که این کار را امکان‌پذیر ساخته، کارایی تعریفهاست ــ که همه بر خاصیتی تأکید دارند که به سرعت قابل کاربرد در بحث است و بیشترین تناسب را با منطق وضعیت دارد. این تأکید بر نامیدن چیزها با نام صحیح آنها ممکن است گاهی ناراحت‌کننده باشد زیرا به نادیده‌گرفتن معانی شهودی می‌انجامد. به‌عنوان مثال، بردار مماس در نقطه‌ای چون p بر خمینه‌ای تحلیلی، به‌عنوان نوع خاصی از نگاشتها روی خانوادهٔ توابعی که در p تحلیلی هستند تعریف شده است. ولی در نهایت، این کتاب برای اکثر خوانندگان آسانتر و بسیار ارضاکننده‌تر از هر متنی است که در سطحی نادقیقتر دربارهٔ این موضوع نوشته شده است. کتاب مورد بحث، مبنای استواری است برای جلدهای II، III، ... که در پی خواهند آمد.

پ. ا. اسمیت

******

نقل از

Bull. Amer. Math. Soc. **53** (1947), 884-887.

مبانی هندسهٔ جبری، اثر آندره ویل

Foundations of algebraic geometry, by André Weil, American Mathematical Society Colloquium Publications, vol. 29, American Mathematical Society, New York, 1946, 20+288 pp., $5.50

هدف اصلی این کتاب به گفتهٔ مؤلف آن «ارائهٔ بحث مبسوط و به هم پیوسته‌ای دربارهٔ ویژگیهای چندگانگیهای تقاطعی، شامل همهٔ مطالب لازم و کافی برای مشروع ساختن استفاده از این چندگانگیها در هندسهٔ جبری کلاسیک، به‌خصوص مکتب ایتالیایی» است. شک نیست که ویل کاملاً به این هدف نائل شده است. وی پس از تدارکی دقیق و طولانی (فصلهای I_IV) در دو فصل مرکزی (V و VI) نظریه‌ای دربارهٔ تقاطع عرضه می‌کند که از حیث کامل بودن و کلیت، هیچ کم ندارد. او از بررسیهای قبلی این مبحث بنیادی به دست سوری و وان در وردن بسیار فراتر می‌رود و مطالب را با دقت مطلقی که در هندسهٔ جبری دارد متداول می‌شود، عرضه می‌کند. کتاب، هماهنگ با عنوان آن، خودکفاست و موضوع از آغاز تشریح می‌شود.

یک جنبهٔ قابل توجه این کتاب این است که ــ به استثنای یک مورد (فصل III) ــ در آن هیچ استفاده‌ای از روشهای پیشرفتهٔ جبر مدرن نشده است. مؤلف تصمیم گرفته است بخشهایی از جبر نوین را که «فراتر از ساده‌ترین حقایق دربارهٔ هیأتهای مجرد و توسیعهای آنها و مقدمات نظریهٔ ایده‌آلها» هستند

مفروض نگیرد یا مورد استفاده قرار ندهد. توفیق ویل در تحقق دقیق این برنامهٔ صرفه‌جویی ریاضی به‌خودی‌خود دستاوردی به شمار می‌رود. این رهیافت در برخی موارد به «بهترین» اثباتهای «ممکن» می‌انجامد. ولی به طورکلی، ممکن است کسی حکمت این ریاضت‌کشی خود تحمیلی را زیر سؤال ببرد. تحویل روشمند نظریه ــ که هم مشکل و هم ظریف است ــ به مقدمات جبر، مسلماً کار بسیار پرزحمتی است. در نتیجه، خواننده خود را در وضعیت شخصی می‌یابد که باید مقدار عظیمی پول نقد را که بیشترش به صورت پول خیلی خرد است جمع کند. مؤلف شیوهٔ خود را با استدلالی معطوف به تداوم و پیوستگی تاریخی، با درخواست بازگشت، به «کاخهایی که به طور طبیعی از آن ماست» توجیه می‌کند. ولی خیلی بعید است که پیشینیان ما عمارت آشنای خود را، هر چند به‌صورت تعمیر و تکمیل‌شده، در کتاب ویل تشخیص دهند. اگر از هندسه‌دان سنتی دعوت شود که بین «ساختارهای موقتی مملو از حلقه‌ها، ایده‌آلها، و ارزه[1]ها» از یک طرف و «ساختارهای مملو از هیأتهای به طور خطی مجزا، توسیعهای منظم، توسیعهای مستقل، تخصیصهای نوعی، تخصیصهای متناهی و تخصیصهای تخصیصها روی یکدیگر»، یکی را انتخاب کند، او به احتمال قوی از این انتخاب سر باز خواهد زد و خواهد گفت «لعنت به هر دو!». حالا که چنین است بهتر است خودمان از جبر نوین تا بیشترین حد ممکن استفاده ببریم.

کتاب ویل اولین توصیف حسابی محض از بخش مهمی از هندسهٔ جبری است، و بنابراین نقطهٔ عطفی در نوشتگان این مبحث است. این امر و صلاحیت مؤلف اهمیت افزونتری به کتاب می‌بخشد.

در مورد باقیماندهٔ کتاب، مایلیم به‌خصوص مطالعهٔ فصل جالبی با عنوان بحث و نظر را توصیه کنیم که در آن مسائل حل نشدهٔ متعددی مورد بحث قرار می‌گیرند و جهات ممکن پژوهشهای آینده نشان داده می‌شود. این کتاب فهرستی عالی از تعریفها و جدولی از نمادها دارد.

اُسکار زاریسکی

******

نقل از

Bull. Amer. Math. Soc. **54** (1948), 671-675.

درآمدی به نظریهٔ احتمال و کاربردهایش، اثر ویلیام فلر

An introduction to probability theory and its applications, Vol. I, by William Feller, Wiley, New York, 1950, 12+419 pp., $6.00

1. valuation

این اولین جلد از کتابی است که قرار است در دو جلد منتشر شود. این جلد، به منظور اجتناب از مسائل اندازه‌پذیری و دشواریهای آنالیزی، محدود به بررسی فضاهای نمونه‌ای گسسته است. این امر مانع از ارائهٔ مطالب زیادی که همهٔ آنها جالب توجه‌اند و بیشترشان در هیچ‌یک از کتابهای موجود نیامده‌اند و بعضی‌شان دست اول‌اند، نشده است. در نتیجه، کتاب حتی برای آن قسمت از جامعهٔ ریاضی که هیچ اطلاع قبلی از احتمال ندارد، بسیار خواندنی است. پس مضمون کتاب، قسمت اول عنوان آن را به‌خوبی توجیه می‌کند زیرا به خواننده‌ای که قدری پختگی ریاضی دارد ولی معلوماتی در احتمال ندارد، اطلاعات قابل‌توجهی در بارهٔ احتمال می‌دهد و او را به پایهٔ لازم برای ادامهٔ مطالعه مجهز می‌سازد. اثباتها در حال و هوای نظریهٔ احتمال‌اند و به خواننده در شناخت موضوع کمک می‌کنند.

امروز نظریهٔ احتمال شاخهٔ دقیق و پررونقی از آنالیز است که از لحاظ خصلت و ماهیت و نیز نوع مسأله‌ها، مثلاً متمایز از نظریهٔ اندازه است. درست است که نظریهٔ احتمال، همچون هندسه، ریشه در بعضی مسائل عملی دارد. ولی این نظریه، مانند هندسه، اکنون خود به مسائلی می‌پردازد که فی‌نفسه اهمیت دارند، بسیاری از آنها خیلی ایده‌آلی شده هستند و فقط ارتباط دوری با مسائل عملی دارند و یا فعلاً هیچ ارتباط مشهودی ندارند. در عین حال، مسأله‌های مبارزطلبی که در حوزه‌های گوناگون کاربرد مطرح می‌شوند، دائماً باعث حرکت و پیشرفت علم می‌گردند. این کتاب حاوی تعداد کثیری مثال است که تقریباً هر جنبه از نظریهٔ مورد بحث را روشن می‌سازند. این مثالها بسیار جالب توجه‌اند و ابداً از نوع موردی و خاص نیستند. آوردن این همه مثال جالب در یک کتاب، کار سترگی است. این مثالها جاذبهٔ این نظریه را حتی برای ریاضیدان محض افزایش می‌دهند، و فقط شاید مرتجعان افراطی، پیروان مکتب «خداوند ریاضیات را از کاربردهایش نجات دهاد»، تحت تأثیر قرار نگیرند.

رئوس مندرجات کتاب به‌صورتی که در بالا آورده شد، خیلی ناقص است. ولی چون محتوای کتاب بحث یکپارچه‌ای از معدودی موضوع نیست، در این مجال اندک کار دیگری نمی‌توان کرد. خلاصه اینکه، اثر مورد بحث عالی و مطالعهٔ آن مطبوع است. گردآوری این همه مطلب به چنین شیوهٔ درخشانی، نشان‌دهندهٔ زحمت طاقت‌فرسایی است که جامعهٔ ریاضی بسیار مرهون آن است. ناقد به نویسنده تبریک می‌گوید زیرا او معیاری عالی برای نویسندگان آتی کتابهای مشابه به‌جا گذاشته است.

جیکوب ولفوویتس[1]

******

نقل از

Bull. Amer. Math. Soc. **57** (1951), 156-159.

1. J. Wolfowitz

آنالیز مختلط، اثر آلفرس

Complex analysis, by L. V. Ahlfors, McGraw-Hill, New York, 1953, 12+247 pp., $5.00

در درس آنالیز مختلط در دانشگاههای آمریکایی، اغلب حساب دیفرانسیل و انتگرال پیشرفته با معیارهای نوین دقت مرور می‌شود. این شیوه، که به‌وضوح معایبی دارد، تا حدی بر دورهٔ تحصیلات تکمیلی ما تحمیل می‌شود و این کتاب برای چنین دوره‌ای نوشته شده است. در آنالیز مختلط، وسوسهٔ مبتنی ساختن اثباتها بر استدلالهای شهودی بسیار قوی است. کارِ دشوار این است که اثباتها ساده و به‌طور شهودی واضح شوند و در عین حال، طوری باشند که خواننده بتواند مراحل لازم برای دقیق کردن استدلال را به‌راحتی به آنها بیفزاید. مؤلف این کتاب با استادی تمام از عهدهٔ این کار دشوار برآمده است.

... این کتاب اثر مهمی است که وارد مجموعهٔ نوشتگان ریاضی شده است. در هر مرور، دقت و هوشمندیی را که مؤلف برای دقیق ساختن و خواندنی کردن اثباتهایش به‌کاربرده ملاحظه می‌کنیم. کتاب برای دانشجوی جدی نوشته شده و مطالعهٔ آن کاملاً ارزش ساعاتی را که صرف این کار می‌شود، دارد.

آلبرت شیفر[1]

******

نقل از

Bull. Amer. Math. Soc. **59** (1953), 464-467.

درسهایی در آنالیز تابعی، اثر ریس و ناج

Leçons d'analyse functionelle, by F. Riesz and B. Sz.-Nagy, Akadémiai Kiadó, Budapest, 8+448 pp., about $7.50

کتابی است عالی.

در زمینهٔ مورد بحث این کتاب، هیچ کتابی قابل مقایسه با آن نیست و در آیندهٔ نزدیک نیز نخواهد بود. این اثر، رساله‌ای برای متخصصان که هدف اصلیش گزارش دادن نتایج پیشرفته و پیچیده باشد نیست و در عین حال به‌صورت یک کتاب درسی برای دانشجوی سالهای اول نیز نوشته نشده است. هدف آن خیلی بالاتر و ظریفتر است، و مؤلفان برای رسیدن به این هدف یک رسالهٔ پیشرفتهٔ بسیار خوب و یک متن درسی غیرمقدماتی بسیار خوب را با هم ترکیب کرده‌اند. هدف این بوده است که بخش مرکزی و منسجمی از ریاضیات، در چارچوب برنامه‌ای که مؤلفان در نظر گرفته‌اند، به‌صورت نهایی و قطعی درآید، و در این چارچوب، این روایتْ نهایی و درست است. اینکه آیا این تنها روایت ممکن است یا نه، بحث دیگری است و پاسخ آن در اینجا مهم نیست. مشخصهٔ بارز این اثر رعایت توازن و خوش‌سلیقگی است: چه در انتخاب موضوعها، چه در دامنه و جزئیات بحث در بارهٔ آنها، چه در روشهای به‌کاررفته برای عرضهٔ آنها، و چه در مسألهٔ اساسی سبک و نحوهٔ بیان مطالب.

موضوعهای مورد بحثْ نظریهٔ نوین انتگرالگیری و مشتقگیری، و نظریهٔ عملگرهای خطی است که مبتنی بر این مفاهیم است. بنابراین می‌بینیم که فضای L^2 مرکب از توابع انتگرال‌پذیر مربعی، فضای مجرد هیلبرت، و فضای C مرکب از توابع پیوسته مورد بحث قرار می‌گیرند. مفهوم اخیر بنا به تناظر بنیادی بین تابعکهای خطی و اندازه‌ها به نظریهٔ اندازه مربوط است. این به بحث مختصری در بارهٔ فضاهای L^p، $p \geq 1$، فضاهای بازتابی، و بالاخره، فضاهای باناخ می‌انجامد. برای این فضاهای گوناگون، نظریهٔ عملگرهای مورد بحث شامل عملگرهای انتگرالی، عملگرهای کاملاً پیوسته به طور کلی، عملگرهای کاملاً پیوستهٔ متقارن (یعنی خودالحاق)، عملگرهای متقارن کراندار، عملگرهای خودالحاق بیکران، و نظریهٔ طیفی در فضاهای باناخ کلی است.

شیوهٔ عرضهٔ مطالب آمیزه‌ای از استقرایی و اصل موضوعی است. مثلاً انتگرالگیری نخست برای خط تشریح می‌شود، سپس در فضای n بعدی، و بالاخره انتگرالهای مجرد و اندازه مطرح می‌شوند.

ادگار لورچ[1]

******

نقل از

Bull. Amer. Math. Soc. **59** (1953), 270-281.

اصول ریاضیات، اثر بورباکی

Éléments de mathématique, by N. Bourbaki, Book II, *Algebra*, Chaps. I-VII, Actualités Scientifiques et Industrielles, nos. 934, 1032, 1044, 1102, 1179, Hermann, Paris, 1942, 1947, 1948, 1950, 1952

عصر ما شاهد ایجاد یک اثر عظیم و ماندگار است: توصیفی از کلِ ریاضیات امروزی. این توصیف چنان انجام می‌شود که پیوند بین شاخه‌های گوناگون ریاضیات به‌روشنی نمایان شود، چارچوبی که تکیه‌گاه کل ساختار است در

1. A. C. Schaeffer

1. E. R. Lorch

کوتاه‌مدت منسوخ و متروک نگردد، و به آسانی بتواند ایده‌های نو را جذب کند. بورباکی سعی می‌کند با ارائهٔ هر مفهوم درکلیترین و انتزاعیترین شکل ممکن به این هدف نائل شود. اصطلاحات و نمادهای آن با دقت کامل انتخاب می‌شوند و هر روز تعداد هر چه بیشتری از ریاضیدانان آنها را می‌پذیرند. با اتمام این برنامه، دائرةالمعارف استانداردی در دسترس ما قرار خواهد گرفت. جلد مربوط به توپولوژی عمومی که به اتمام رسیده است، از قبل به ویژه در میان نسل جوانتر با اشتیاق مورد استفاده قرارگرفته است. اثر بورباکی را نباید با دائرةالمعارف علوم ریاضی[1] مقایسه کرد. هدف آن دائرةالمعارف متفاوت بود، اثباتی در آن دیده نمی‌شد و مقاله‌ها را مؤلفان مختلف نوشته بودند.

امیدوارم این‌کار با همین نگرش و همین شور و حرارت ادامه یابد. من ترجمهٔ آن را به زبان انگلیسی توصیه می‌کنم.

مجلداتی که در بارهٔ جبر انتشار یافته‌اند همان ویژگیهای بقیهٔ اثر بورباکی را دارند. تمرینهای متعدد، که بسیاری از آنها فوق‌العاده جالب‌اند، در انتهای هر پاراگراف آمده‌اند. گهگاه سیر تکامل مفاهیم در یادداشتهای تاریخی عالی تشریح شده است. مسلماً بیشتر مطالب جنبهٔ متعارف دارند، و من در بحث تفصیلی‌تر زیر عمدتاً به مفاهیم تازه‌ای که در این اثر ظاهر شده اشاره می‌کنم.

پیش از این بحث باید چند نکتهٔ کلی را ذکر کنم. ما همه عقیده داریم که ریاضیاتْ هنر است. مؤلف یک کتاب یا مدرس یک کلاس درس می‌کوشد زیبایی ساختاری ریاضیات را به خوانندگان یا شنوندگانش نشان دهد. ولی در این تلاش معمولاً موفق نمی‌شود. ریاضیات مسلماً منطقی است؛ هر حکمی از گزاره‌هایی که قبلاً ثابت شده‌اند استنتاج می‌شود. ولی کل ریاضیات، به مثابهٔ یک اثر هنری واقعی، «خطی» نیست؛ و بدتر اینکه درک آن باید در یک آن صورت پذیرد. ما همه، در موارد نادری، از اینکه شنوندگانمان را قادر ساخته‌ایم کل ساختار ریاضیات و همهٔ شعبات آن را در یک نگاه ببینند احساس شعف کرده‌ایم. چگونه می‌توان به این حالت دست یافت؟ اصرار اجوجانه بر تسلسل منطقی مانع از مجسم‌سازی کل ریاضیات می‌شود، ولی در عین حال ساختار منطقی باید حکمفرما باشد و گرنه هرج‌ومرج پیش می‌آید. بورباکی از این معضل به‌خوبی آگاه است. تقسیم کل اثر به چند کتاب و عرضهٔ تمرینهایی که در آنها از بخشهای پیشرفته‌تر نظریه استفاده می‌شود نشان‌دهندهٔ این آگاهی است. ولی من احساس می‌کنم که در بعضی موارد، تقسیم به چند کتاب کافی نیست. این عدم کفایت، چنانکه خواهیم دید، در فصل پنج به شدت احساس می‌شود

در خاتمه مایلم بار دیگر بر توفیق کامل این اثر تأکید کنم. شیوهٔ عرضهٔ مطالبْ انتزاعی است، به طرز بیرحمانه‌ای انتزاعی است؛ ولی خواننده‌ای که بر دشواریهای اولیه فائق آید، در ازای زحماتش پاداش پُربهایی خواهد گرفت که عبارت است از بصیرت عمیقتر و فهم کاملتر.

امیل آرتین

******

نقل از

Bull. Amer. Math. Soc. **59** (1953), 474-479.

1. Encyclopädie der mathematischen Wissenschaften

درآمدی به فراریاضیات، اثر کلینی

Introduction to metamathematics, by Stephen Cole Kleene, North-Holland Publishing Co., Amsterdam, and P. Noordhoff, Groningen, 1952; D. van Nostrand Company, New York and Toronto 1952; X+550 pp.

این کتاب ــ از طریق شرح روشن و بسیار دقیقی از منطق ریاضی ــ خواننده را با آخرین پژوهشها در «مبانی ریاضیات» آشنا می‌سازد. به‌خصوص حساب تابعی مرتبهٔ اول، نظریهٔ مقدماتی اعداد، و نظریهٔ توابع بازگشتی به نحو بسیار جامعی با توجه به نتایج جدید به‌دست آمده در این زمینه‌ها مورد بحث قرارگرفته‌اند. سایر شاخه‌ها یا به اختصار بررسی شده‌اند یا نادیده گرفته شده‌اند (مثلاً حساب تابعی مراتب بالاتر، نظریهٔ انواع، نظریهٔ اصل موضوعی مجموعه‌ها، روشهای جبری به‌کار رفته در پژوهشهای فراریاضی).

نکتهٔ شایان تأکید، سطح فنی بسیار بالای کتاب است.

بخش نخست کتاب شامل مفاهیم بنیادی نظریهٔ شهودی مجموعه‌ها، و شرحی از پارادکسهای نظریهٔ مجموعه‌ای و معناشناختی، و بنابراین بحثی در روشهای شناخته‌شده برای رفع این پارادکسها (منطقگرایی، شهودگرایی، صورتگرایی) است. در انتهای این بخش، مؤلف نظر خودش را در بارهٔ ریاضیات بیان می‌کند: «فرانظریه[1] به ریاضیات شهودی و غیررسمی تعلق دارد (مگر آنکه فرانظریه خودش از دیدگاه یک فرافرانظریه فرمولبندی شود که ما در اینجا به آن نمی‌پردازیم). . . . روشهای به‌کار رفته در فرانظریه محدود به روشهایی خواهد بود که صورتگرایان آنها را متناهی‌وار[2] می‌نامند . . . در این کتاب ما فقط وقتی کلمهٔ «فرا» را به‌کار می‌بریم که روشها متناهی‌وار باشند.» این برنامه را مؤلف در بقیه کتاب اجرا می‌کند. قضایایی از فرانظریه که اثباتهایشان ساختی نیست، با الحاق اندیس C به شمارهٔ قضیه، متمایزگشته‌اند.

موضوع بخش دوم، نظریهٔ مقدماتی کلاسیکِ صوری‌شدهٔ اعداد همراه با حساب جمله‌ها و حساب تابعی مرتبهٔ اول است که به‌عنوان اجزای این دستگاه صوری مورد بحث قرارگرفته‌اند. نویسنده در هر یک از این دستگاهها بین قسمتی که مبتنی بر منطق شهودگرایانه است (حساب شهودگرایانهٔ تابعی و حساب شهودگرایانهٔ جمله‌ها، نظریهٔ شهودگرایانهٔ اعداد) و دستگاه کلاسیک متناظر فرق گذاشته است؛ قضایایی که فقط در مورد دستگاههای کلاسیک صادق‌اند با اندیس o مشخص شده‌اند. این بخش، از جمله، شامل دو قضیهٔ معروف گودل است: قضیهٔ ناتمامیت (به شکل اصلی و به شکل «راسر[3]»ی) و قضیهٔ راجع به امکان‌ناپذیریِ اثبات سازگاری به‌وسیلهٔ روشهای صوری‌شدنی در خود دستگاه.

در بخش سوم که به نظریهٔ تابعهای بازگشتی اختصاص دارد، مرور کامل و بسیار خوبی بر همهٔ نتایج بنیادی این حوزه ــ به استثنای شاخه‌هایی که هیچ کاربردی در پژوهش فراریاضیاتی ندارند (مانند اعداد اُردینال ساختی و آنالیز محاسبه‌پذیر) به عمل آمده است. همهٔ مفاهیم و مسائل به شیوه‌ای بسیار طبیعی و آموزنده مطرح شده‌اند. تابعهای بازگشتی ابتدایی به صورت تعریف‌پذیر با عملهای استقرا (بازگشت ابتدایی) و جانشانی به دفعات

1. metatheory 2. finitary 3. Rosser

متناهی، معرفی گشته‌اند. گذار از مفهوم تابع بازگشتی ابتدایی به تابع بازگشتی کلی (تعریف‌پذیر به‌وسیلهٔ دستگاهی متناهی از معادلات که از آنها می‌توان مقادیر تابع را با جانشانی و جایگزینی محاسبه کرد) به صورتی شهودی تشریح می‌شود. در این بخش توضیح قانع‌کننده‌ای دربارهٔ ماشینهای تورینگ و اثباتی از هم‌ارزی مفاهیم بازگشتی‌بودن و محاسبه‌پذیری تورینگ، دیده می‌شود.

آخرین بخش کتاب شامل بررسیهای فراریاضیاتی دیگری در ارتباط با منطق ریاضی است، مثلاً قضیهٔ تمامیت گودل برای حساب تابعی مرتبهٔ اول، قضیهٔ لوونهایم، تعمیم اسکولم و پارادکس اسکولم، قضیهٔ اسکولم در بارهٔ امکان‌ناپذیری توصیف کامل حساب، قضیهٔ چرچ در بارهٔ تصمیم‌ناپذیری حساب تابعی مرتبهٔ اول، قضیه‌های تارسکی در بارهٔ تصمیم‌ناپذیری اساسی، و اثباتهایی از سازگاری که در آنها روش گنتسن به‌کار می‌رود.

و بالاخره، مؤلف به دستگاههای شهودگرایانه می‌پردازد. در اینجا، ازجمله، قضایایی می‌بینیم که با روش گنتسن به‌سادگی قابل اثبات‌اند ــ مانند اثبات تصمیم‌پذیری حساب شهودگرایانهٔ جمله‌ها، تحویلهای گوناگون دستگاههای کلاسیک به شهودگرایانه (ازجمله دستگاه گودل)، و تحقیقات جدید در بارهٔ مفهوم موردنظر مؤلف از تحقق‌پذیری[1] بازگشتی.

کتاب چنان نوشته شده است که هم برای متخصص، که مطالب ارزشمند زیادی (صورتهای جرح و تعدیل‌یافته اثباتها و بعضی قضایای جدید) در آن می‌یابد بسیار جالب است و هم برای دانشجو، که می‌تواند از آن به‌عنوان کتاب درسی استفاده کند. به نظر ناقد، این کتاب یکی از بهترین آثاری است که در بیست سال اخیر در این زمینه منتشر شده است.

ه. رزیوا[2]

******

نقل از

J. Symbolic Logic, (3) **19** (Sept. 1954) 215-216.

جبر هومولوژیک، اثر کارتان و آیلنبرگ

Homological algebra, by Henri Cartan and Samuel Eilenberg, The Princeton University Press, Princeton, 1956, 15+390 pp., $7.50

بالاخره این اثر تأثیرگذار و پر از شور و سرزندگی در دسترس همگان قرار گرفت. سه سال طول کشید تا متن دستنویس آن به‌صورت کتاب صحافی شده درآید. شاید انتشارات پرینستن را از بابت این تأخیر باید جریمه کرد!

جبر هومولوژیک هم به هومولوژی دستگاههای جبری و هم به جنبه‌های جبری نظریهٔ هومولوژی می‌پردازد. مبحث اول شامل نظریه‌های هومولوژی و کوهومولوژیِ گروهها، جبرهای شرکت‌پذیر، و جبرهای لی است. مبحث دوم به پروراندن دنباله‌های دقیق و دنباله‌های طیفی، و نیز کار با تابعگونهای مجتمعهای زنجیره‌ای اختصاص دارد. به‌عنوان نمونه، مسألهٔ کونت[1] چنین است: با مفروض بودن هومولوژی مجتمعهای K و L، هومولوژی $K \otimes L$ چیست؟ و مسألهٔ ضرایب عام[2] نیز از این قرار است: گروه G و هومولوژی مجتمعی چون K مفروض‌اند، هومولوژی مجتمعهای $K \otimes G$ و $\mathrm{Hom}(K, G)$ چیست؟ این مسأله‌ها و این دو تابعگون، یعنی حاصلضرب تانسوری و Hom، نه فقط برای گروهها، بلکه در تعمیم مناسبی برای مدولهای چپ روی حلقهٔ دلخواه Λ نیز بررسی می‌شوند.

شاید ریاضیات امروز با چنان سرعتی در حال رشد باشد ــ و تا حدی به یمن آثار سرزنده و وحدت‌بخشی چون این کتاب ــ که هیچ تلاشی برای وحدت بخشیدن به ریاضیات نتواند روزآمد باشد. ناقد همچنین این عقیدهٔ کاملاً شخصی خود را به این نکته می‌افزاید که مؤلفان تمایز بین مقالهٔ تحقیقاتی و کتاب را به اندازهٔ کافی در نظر نداشته‌اند: مقالهٔ تحقیقاتی خوب، ایده‌ای را که خوش آتیه به نظر می‌رسد در هنگامی که هنوز داغ است ــ و هیچ‌کس با اطمینان نمی‌داند که واقعاً مفید از آب در خواهد آمد یا نه ــ عرضه می‌کند؛ کتاب تحقیقاتی خوب ایده‌هایی را (که هنوز مورد توجه‌اند) پس از آنکه سودمندیشان در کارهای افراد مختلفی به ثبوت رسیده است، ارائه می‌دهد.

سهم ایده‌های جدید درخشان در این کتاب، بیش از حد و نامتناسب است. در بارهٔ آنها چیزی نمی‌شود گفت جز اینکه تر و تازه و نویدبخش‌اند: ماهواره‌ها[3] (که در فصل III ظاهر می‌شوند و در فصلهای بعد به تدریج ناپدید می‌گردند)، تابعگونهای اشتقاقی[4] همه چیز بجز Hom و $\otimes$ (ناقد نتوانست مثالهای دیگری بیابد)، حلقه‌های نیمه‌موروثی، تابعگونهای اشتقاقی نسبت به چند متغیر، جبرهای تکمیل‌شده[5] و هومولوژی تکواره‌ها[6]. همین نکته در مورد دنباله‌های طیفی صادق است. ارزش این دنباله‌ها در توپولوژی معلوم شده است ولی آنها هنوز به نتایج مشخصی در هومولوژی دستگاههای جبری نینجامیده‌اند: نتیجه این است که خوانندهٔ بی‌تجربه نمی‌تواند امید داشته باشد که با خواندن سه فصلی که در این کتاب به دنباله‌های طیفی اختصاص یافته است، بفهمد این دنباله‌ها کلاً به چه دردی می‌خورند. ناقد ادعا نمی‌کند که دنباله‌های طیفی و آن مفاهیم دیگر بعدها کاربردهای جبری مهمی نخواهند داشت: بعضی از آنها خواهند داشت، ولی تا وقتی آن زمان نرسیده است، حضور آنها کتاب را شلوغ و آشفته می‌کند.

ساندرز مک‌لین

******

نقل از

Bull. Amer. Math. Soc. **62** (1956), 615-624.

1. realizability 2. H. Rasiowa

1. Künneth 2. universal coefficient problem 3. satellites
4. derived functors 5. supplemented algebras 6. monoids

مبانی توپولوژی جبری، اثر آیلنبرگ و استینراد

Foundations of algebraic topology, by S. Eilenberg and N. Steenrod, Princeton University Press, 1952 (second printing, 1957), 15+328 pp., $7.50

این کتاب تأثیر عمیقی بر پیشرفت توپولوژی، هم قبل و هم بعد از انتشارش، داشته است. طی پنج سالی که از نخستین چاپ آن می‌گذرد، به‌صورت یک کتاب درسی استاندارد و مرجعی برای همهٔ علاقه‌مندان به توپولوژی درآمده است.

نخستین درس در توپولوژی جبری معمولاً درس مشکلی برای دانشجو است زیرا او با انبوهی از ابزارهای ناآشنای جبری روبه‌رو می‌شود که فهم علت و انگیزهٔ طرح آنها دشوار است وکاربردپذیریشان نیز خیلی بعد معلوم می‌شود. با توجه به این امر، مؤلفان رهیافتی اصل موضوعی به نظریهٔ هومولوژی در پیش گرفته‌اند. آنها با هفت اصل موضوع مربوط به جبر و هندسه که به سادگی بیان شده‌اند شروع کرده‌اند (و فقط مفاهیم بنیادی جبر و توپولوژی مجموعهٔ نقاط را به‌عنوان پیشنیازْ مفروض گرفته‌اند) و نشان داده‌اند که چه قضایای مهم و جالبی را می‌توان مستقیماً با استفاده از این اصول موضوع ثابت کرد. خودِ این اصول موضوع بدون انگیزش و زمینه‌سازی ذکر شده‌اند ولی کاربرد بلافاصلهٔ آنها باعث می‌شود دانشجو آسانتر آنها را بپذیرد. تنها پس از آنکه خواننده توان و امکانات نظریه را ملاحظه کرد، جزئیات مربوط به وجود و یکتایی نظریه‌های هومولوژی مطرح می‌شود.

خواه رهیافت اصل موضوعی را رهیافت خوبی برای دانشجویان مبتدی بدانیم و خواه ندانیم، دلایل زیادی وجود دارد که این کتاب به‌عنوان کتاب درسی (که شاید بیش از همه برای سال دوم دورهٔ پس از کارشناسی مناسب باشد) توصیه شود. بحث آن در بارهٔ نظریه‌های تکین[1] و چک[2]، نوین وکامل است و خواننده خودش می‌تواند آنها را بخواند. نمودارهای همریختیها، که امروز این‌قدر زیاد به‌کار می‌روند، نخستین بار در این کتاب به‌طور نظام‌یافته مورد استفاده قرار گرفت، هم برای نشان‌دادن راه اثبات و هم برای کمک به خواننده در فهم استدلالها. هر فصل کتاب با مقدمه‌ای شروع می‌شود حاکی از محتوای فصل و جایگاه آن در طرح کلی کتاب. یادداشتهایی در انتهای فصل آمده‌اند که سیر تاریخی موضوع و رابطه‌های آن با مباحث دیگر را بازگو می‌کنند. ارجاعاتی به نوشتگان موجود نیز در این یادداشتها هست. در انتهای هر فصل، مجموعه‌ای از تمرینها آمده است. بعضی از این تمرینها آسان و برخی دشوارند ولی بیشترشان جالب‌اند، و دانشجویی که به حل آنها می‌پردازد مطالب زیادی یاد خواهد گرفت.

ادوین اسپنیر[3]

******

نقل از

Bull. Amer. Math. Soc. **64** (1958), 190-192.

1. singular 2. Čech 3. E. H. Spanier

اصول هندسهٔ جبری، اثر گروتندیک

Éléments de géométrie algébrique, by A. Grothendieck, rédigés avec la collaboration de J. Dieudonné, Publications de l'Institut des Hautes Études Scientifiques No. 4, Paris, 1960, 228 pp., 27 NF

اثر حاضر، که اکنون فصلهای ۰ و ۱ آن با هم چاپ شده است، نقطهٔ عطف مهمی در سیر پیشرفت هندسهٔ جبری است. این اثر، طبق برنامه، سرانجام همهٔ دانسته‌ها در بارهٔ هندسهٔ جبری روی حلقه‌های زمینهٔ دلخواه، و البته بسیاری چیزهای دیگر، را دربرخواهد گرفت. فهرست موقتی فصلهای آن چنین است:

برای اینکه تصور دقیقتری از فصلهای آتی داشته باشید باید به متن سخنرانی گروتندیک، خطاب به کنگرهٔ بین‌المللی در ادینبورو در سال ۱۹۵۸ مراجعه کنید و همچنین به رشته سخنرانیهای او در سمینار بورباکی در دو سال گذشته، که در آنها طرحی از اثباتهای قضایای مهمی که در فصلهای آتی می‌آیند عرضه شده است. متن این سخنرانیها موجز، صریح، و هیجان‌انگیز، و حاوی انگیزش و زمینهٔ لازم برای کل اثر است. ولی در خود اثر که بسیار روشن، کاملاً سازمان‌یافته، و خیلی دقیق نوشته می‌شود جایی برای این‌گونه زمینه‌چینی‌ها نیست. در اینجا باید از دیودونه بسیار سپاسگزار بود که مشکلات نوشتن و انتشار این اثر بدون همکاری او قابل رفع نمی‌بود.

گروتندیک در هندسهٔ جبری برخی از مسأله‌های کلاسیک را برحسب نمایش تابعگونها صورتبندی می‌کند، مثلاً مسألهٔ ساختن طرحهای پیکار[1] را. با مفروض بودن X روی S، تابعگون پیکار عبارت است از اینکه به هر T روی S، رده‌های بخشیاب X که بر T گویا هستند منسوب شود. (این را البته می‌توان دقیق کرد.) طرح پیکار، در صورت وجود، این تابعگون را نمایش می‌دهد. گروتندیک اخیراً شرطی نسبتاً کلی روی تابعگونها در رستهٔ طرحها به‌دست آورده است، که تحت آن شرط می‌تواند ثابت کند یک تابعگون نمایش‌پذیر است. این دیدگاه نشان‌دهندهٔ گسست کاملی از رویکردهای قبلی است و به مفهومی، اولین رویکردِ اساساً نو است که پس از مکتب ایتالیایی وارد هندسهٔ جبری شده است.

از این پس، درستی قضیه دیگر به این دلیل نیست که می‌توان تصویری برای آن رسم کرد، بلکه به این دلیل خواهد بود که یک واقعیت تابعگونی[2] است.

در خاتمهٔ این نقد باید نکته‌ای را تذکر دهم که عدم توجه به آن ممکن است باعث گمراهی شود. بعضیها ممکن است بپرسند: اگر قرار باشد هندسه جبری از این کتاب (دست‌کم) سیزده فصلی در ۲۰۰۰ صفحه و همهٔ جبر تعویض‌پذیر تشکیل شود، دنبال‌کردن آن دیگر چگونه می‌تواند مقدور باشد؟

1. Picard schemes 2. functorial

پاسخ واضح است. از یک سو، برای پرداختن به موضوعهای خاص که ممکن است جاذبهٔ به‌خصوصی داشته باشند، فقط بخشهایی از تمام این اثر لازم است، و می‌توان از راههای میانبری برای سریعتر رسیدن به هدفهای خاص استفاده کرد. پس می‌توان انتظار همزیستی بین همانی ویل و این کتاب را برای مدتی داشت. فقط تاریخ مشخص خواهد کرد که کدام‌یک دیگری را از صحنه خارج می‌کند. روشهای تصویری [فرافکنشی] که برای بعضی هندسه‌دانان فی‌نفسه جاذبهٔ خاصی دارند، و حائز بیشترین اهمیت در بخشی از جوانب هندسه هستند، مثلاً در نظریهٔ ارتفاعها، لزوماً در رویکرد موضعی این کتاب به حاشیه فرستاده می‌شوند ولی در بررسی مسائل خاص از دیدگاه خاص ممکن است به‌عنوان نقطهٔ شروع مطرح شوند.

ولی از این مهمتر اینکه هنوز هم قضایا و حدسهایی در مورد مثالهای خاص، مانند خمهای بیضوی یا صورتهای مکعب روی عددهای گویا، کشف و آزمایش می‌شوند و ریاضیدان برای تعیین تکلیف اینها به ابزارهای زیادی نیاز ندارد و کافی است کوشش و تخیل خود را به کاربرد تا سر از اسرار اینها درآورد. پس مانند گذشته مواد خام کافی در اطراف هست که با سلیقه و ذائقهٔ هر کسی جور باشد، ولی کسانی که ذائقهٔ آنها مانع هضم این کتاب نشود، پاداشی بسزا خواهند یافت.

سرژ لانگ

******

نقل از

Bull. Amer. Math. Soc. **67** (1961), 239-246.

هومولوژی، اثر مک‌لین

Homology, by Saunders Mac Lane, Die Grundlehren der Mathematischen Wissenschaften, Bd. 114, Springer, Berlin, 1963; Academic Press, New York, 1963, 422 pp. illus, $15.50

تقریباً هفت سال بین انتشار نخستین کتاب در بارهٔ هومولوژی که نوشتهٔ کارتان و آیلنبرگ بود و انتشار این کتاب در همان زمینه به قلم ساندرز مک لین فاصله افتاده است. چون هر دو کتاب به موضوعی می‌پردازند که اساساً یکی است، شاید ناگزیر باشیم نقد دومی را با ذکر نکاتی که در مقایسهٔ آن دو به نظر می‌آید، آغاز کنیم.

کتاب اولی به تشریح موضوعی جدید ــ جبر هومولوژیک ــ می‌پرداخت. در زمان تدوین آن (بیش از ده سال قبل) روشن نبود که این موضوع تازه دقیقاً در چه مسیرهایی حرکت خواهد کرد، و موفقیت عمدهٔ آن کشف این نکته بود که با قراردادن مدولهای تصویری [فرافکنشی] به جای مدولهای آزاد می‌توان تابعگونهای اشتقاقی Hom و حاصلضرب تانسوری را تعریف کرده Ext و Tor را به‌دست آورد و از این طریق، نظریه‌های موجود هومولوژی ساختارهای جبری را تحت لوای واحدی درآورد. بنابراین مؤلفان آن کتاب توجه خود را معطوف به تشریح موشکافانهٔ تحلیلها[1]ی فرافکنشی و درافکنشی[2]، تابعگونهای اشتقاقی، ماهواره‌ها، بعد هومولوژیک، حاصلضربها، و دنباله‌های طیفی کردند و با شوق و مسرت، رابطه‌های بین این پدیده‌های جدید و پدیده‌های قدیمتر از قبیل هومولوژی گروهها، جبرها و جبرهای لی، قضیهٔ هیلبرت در بارهٔ سیزیجی‌ها[3] و فرمول کونت را نشان دادند.

از آن زمان به بعد، روشهای جبر هومولوژیک، به طرز گسترده‌ای در بسیاری از مباحث به‌کار رفته‌اند، و تکنیکهای هومولوژیک پالایش‌یافته، شرح و بسط داده شده، و تعمیم یافته‌اند. از آن گذشته، ریاضیدانان متعددی ارزش ابزارهای هومولوژیک و رهیافت مبتنی بر تابعگونها را تصدیق کرده‌اند. بنابراین مک‌لین نه چون شعبده‌بازی با انبانی از ترفندها بلکه به‌عنوان شارحی که می‌خواهد نشان دهد چگونه یک نظریهٔ منسجم کارامد، روشنگر پرسشهای بامعناست، به این موضوع می‌پردازد. پس طرح کلی او، گذار از خاص به عام، و روشن‌ساختن مسیر تا حد امکان است.

البته باید در نظر داشت که صرفِ گذشت زمان و رشد و تکامل موضوع به تنهایی علت وضوح و روشنیِ بیشتر مطالب‌عرضه‌شده در کتاب نیست. مؤلف آشکارا به مثالهای ملموس و کاربردهای ملموس ابزارهای کلی معتقد است و در چارچوب محدود این کتاب، در فراهم کردن آنها بسیار کوشیده است.

دیوید بوکسباوم

******

نقل از

Bull. Amer. Math. Soc. **70** (1964), 329-331.

نظریهٔ طیفی (بخش II از عملگرهای خطی)، اثر دانفرد و شوارتس

Linear operators. Part II. *Spectral theory*, by Nelson Dunford and Jacob T. Schwartz, with the assistance of William G. Bade and Robert G. Bartle, Interscience, New York, 1963, pp. 859-1923, $35.00

اگر یک سیاح ریاضی، متعلق به قرنی دیگر، سری به دوران ما بزند و جویای اطلاع از وضعیت فعلی آنالیز ریاضی باشد ورق زدن این کتاب تقریباً برایش

1. resolutions 2. injective 3. syzygies

کفایت می‌کند. با انتشار جلد دوم کتاب که مدتهای طولانی در انتظارش بودیم، اکنون چشم‌اندازی وسیع، سرشار از جزئیات رنگارنگ، از تمام دستاوردهای مکتبی در آنالیز ریاضی در برابر دیدگان ماست که با کارهای واترا و فرشه در حوالی آغاز قرن آغاز شد و در لهستان، مجارستان، اتحاد شوروی، و نیز در شیکاگو و ییل در دهه‌های سی و چهل به اوج خود رسید.

تنها با ذکر مندرجات کتاب، چنانکه در نقدها معمول شده است، نمی‌توان حق مطلب را در بارهٔ این کتاب ادا کرد؛ به جای این کار، توجه خود را به بعضی از ارزشمندترین بخشهای کتاب که نمونهٔ بارز محتویات آن است معطوف می‌کنیم و خواننده را به نقد مبسوط هالموس بر جلد اول ارجاع می‌دهیم که در آن، شیوه‌های عرضهٔ مطالب کتاب تشریح شده است.

ایده‌ای که کل اثر معطوف به آن است، نظریهٔ طیفی تک عملگر خطی و کاربردهای گوناگون آن است.

در دورانی که رشته‌ها به شاخه‌های باریک و باریکتر تجزیه می‌شوند، در زمانی‌که بعضی ریاضیدانان افتخار می‌کنند که از کاربردهای دستاوردشان بی‌اطلاع‌اند، توجه دائم مؤلفان به Zusammenhang [به‌هم پیوستگی] نظریه و کاربرد، و به‌هم پیوستگی شاخه‌های مختلف ریاضیات، باعث افزایش حجم کتاب به میزان نامتعارف شده است.

هر کسی این کتاب را از آغازش دنبال کرده، و بیشتر آموزش و الهام ریاضیش را از آن کسب کرده است، مانند ناقد که چنین کرده و نسل کاملی از آنالیزخوانان که چنین خواهند کرد، نمی‌تواند تلاش عظیم انسانی و دقت و توجه عاشقانه‌ای را که در تألیف آن به‌کار رفته، فراموش کند. وقتی کسی کتاب را می‌خواند، کل دنیای آنالیز ریاضی امروزی در جلو چشمانش جان می‌گیرد. از زمان پیکار و گورسا کتابی درسی در چنین مقیاس عظیمی وجود نداشته است. مؤلفان از عهدهٔ کاری برآمده‌اند که به نظر خیلیها ناممکن می‌آمده است.

داشتن منظرهٔ کاملی از تمام یک مبحث، آنالیز تابعی، که از طریق بحث منسجمی (که امیدواریم با انتشار $n-2$ جلد باقیمانده سرانجام به چند هزار صفحه بالغ شود) ارائه می‌شود، مزیتی است که رشته‌های ریاضی معدودی از آن برخوردار شده‌اند. می‌توان اثر فریکه-کلاین و نیز راسل-وایتهد را نمونه‌های قبلی کم‌رنگی از آن دانست. مسلماً این کتاب تأثیر قاطعی بر پیشرفت آتیِ تمام آنالیز، و نیز بر قسمت اعظم فیزیک ریاضی و سایر شاخه‌های مجاور خواهد داشت.

هیچ دانشجوی جدی آنالیز نمی‌تواند این اثر را نادیده بگیرد. مؤلفان بیش از آنکه سزاوار سپاس و قدردانی ما باشند، سزاوار آن‌اند که هر کسی که علاقه‌مند به آموختنِ نتایج یک عصر کامل از ریاضیات است، اثرشان را بخواند.

جیان‌کارلو روتا

******

نقل از

Bull. Amer. Math. Soc. **71** (1965), 705-708.

نظریهٔ مجموعه‌ها و فرضیه پیوستار، اثر کوهن

Set theory and the continuum hypothesis, by Paul J. Cohen, W. A. Benjamin, Inc., New York and Amsterdam 1966, vi+154 pp.

هدف اصلی این کتاب، ارائهٔ قضیه‌های استقلالیِ مؤلف در نظریهٔ مجموعه‌هاست. برای مطالعهٔ کتاب لازم نیست خواننده منطق بداند، ولی آشنایی با نظریهٔ طبیعی مجموعه‌ها، ازجمله ویژگیهای بنیادی کاردینالها و اُردینالها، مفروض است. مطالب پایه‌ای لازم در منطق و نظریهٔ اصل موضوعی مجموعه‌ها در سه فصل اول کتاب عرضه می‌شود؛ فصل چهارم و آخر به بحث در بارهٔ اظهار[1] می‌پردازد.

مؤلف در آغاز فصل چهار، به‌عنوان مثالی از اثبات به سبک اظهار، نشان می‌دهد که $V = L$ از $ZF + AC + GCH$ مستقل است. وی سپس به توصیف مفهوم تعمیم‌یافته‌ای از اظهار می‌پردازد و آن را برای اثبات استقلال GCH از $ZF + AC$، و AC از ZF به‌کار می‌گیرد. نتایجی دیگر نیز، که از آنِ اوی و ففرمن است در این فصل می‌آیند، ازجمله استقلال AC از اصل ترتیب، و سازگاری این دو گزاره، که $\aleph_1$ با ω همپایان[2] است و پیوستارْ اجتماعی شمارا از مجموعه‌های شماراست. و بالاخره، اثبات سیرپینسکی از این حکم که GCH مستلزم AC است، می‌آید. کتاب با طرح نظراتی فلسفی، ازجمله اینکه فرض پیوستار احتمالاً غلط است، پایان می‌پذیرد.

مؤلف در مقدمه می‌نویسد: «چون آرزوی صمیمانه ما این بوده است که این نوشته برای طیف وسیعی از غیرمتخصصانِ علاقه‌مند به این مسأله قابل فهم باشد، سبک بسیار صورتگرایانه‌ای را که در بعضی کتابهای درسی منطق دیده می‌شود اتخاذ نکرده‌ایم.» درواقع شیوهٔ تشریح مطالب کاملاً غیررسمی است و این ویژگی، خواندن کتاب را برای خواننده، اگر منطقدان باشد، لذت‌بخش می‌سازد. ولی متأسفانه خطاها و بی‌دقتیهای زیاد، و نیز بی‌توجهی کلی به جزئیات، متن را ضایع کرده است. این موضوع همراه با اختصار و ایجاز بسیار، که برای فشرده‌سازی همهٔ مطالب فوق‌الذکر در کتابی ۱۵۴ صفحه‌ای ضروری بوده است، فهم کتاب را برای بیشتر غیرمتخصصان دشوار ساخته است.

کنت کیونن[3]

******

نقل از

J. Symbolic Logic, (4) **35** (Dec., 1970); 591-592.

1. forcing 2. cofinal 3. Kenneth Kunen

دیدگاه

ریاضیاتی خوب با فلسفه‌ای بد

در شمارهٔ قبلی نشر ریاضی (سال ۱۱، شمارهٔ ۱) مقاله‌ای از ریاضیدان فقید ریچارد همینگ با عنوان «ریاضیات در سیاره‌ای دوردست» و دو دیدگاه در بارهٔ آن به قلم آقایان سیاوش شهشهانی (دیدگاه دوم) و کاوه لاجوردی (دیدگاه اول) به چاپ رسید. عنوان این دیدگاه، یعنی «ریاضیاتی خوب با فلسفه‌ای بد»، توصیف من از نظریهٔ همینگ در مقالهٔ فوق‌الذکر است. من برخلاف دیدگاه اول، همینگ را به بی‌اطلاعی متهم نمی‌کنم و برخلاف دیدگاه دوم، او را از زمرهٔ قهرکنندگان از ریاضیات معاصر نمی‌دانم. ریاضیات همینگ را به این دلیل ریاضیاتی خوب می‌دانم که «قابل حصول» است (بخوانید «قابل ساختن»)، اما فلسفهٔ ریاضی او که مبتنی بر ابزارگرایی[1] می‌باشد، باب طبع من نیست. ریاضیات همینگ نه به این دلیل مستحکم است که «به‌طور مستقیم و ضروری بازتابی در جهان خارج دارد» (دیدگاه دوم)، بلکه چون مستحکم است، ریاضیاتی واقعی است. اگر به دنبال دلایل استحکام ریاضیات همینگ، البته غیر از بازتاب آن در جهان خارج، بگردیم، فلسفهٔ خوبی برای ریاضیاتِ خوب، همینگ بنا می‌کنیم.

قصد من در این نوشتار به هیچ‌وجه دفاع همه‌جانبه از نظرات همینگ نیست. علاوه بر آن، نمی‌خواهم به همهٔ «اشکالات» دیدگاه اول و همه «سؤالات» دیدگاه دوم پاسخ دهم. اما توجه نویسندگان دو دیدگاه را به چند مسألهٔ اساسی جلب می‌کنم، که به‌نظرم عدم توجه به آنها، منشاء سوءتفاهم‌ها شده است.

۱. اگر در ریاضیات همینگ به پیوستاری دست یابیم که در آن علاوه بر اختلافات دیگر با پیوستار کلاسیک، تساوی بین اعداد حقیقی تصمیم‌ناپذیر باشد و به‌دنبال آن به این نتیجه برسیم که ضرورتاً هر زیرمجموعهٔ کراندار از اعداد حقیقی دارای کوچکترین کران بالا نیست، آنگاه صحبت از اینکه «تابعی در یک، دستگاه مختصات پیوسته و در دستگاه دیگر ناپیوسته است» چه معنایی می‌تواند داشته باشد؟ یا چه معنایی دارد که بگوییم حکم معادل قضیهٔ کانتور، یعنی «به‌ازای هر دنبالهٔ $\{c_j\}_{j\in\mathbb{N}}$ از اعداد حقیقی، عدد حقیقی‌ای هست که هیچ‌یک از c_jها نیست» را به راحتی می‌توان از خاصیت کوچکترین کران بالا اثبات کرد؟

۲. اگر همینگ اصل انتخاب را باور نداشته باشد، توسل به مدلهای شمارا یا ناشمارای ZFC (قضیهٔ لوونهایم-اسکولم) پاسخ قانع‌کننده‌ای برای پاراداکس اسکولم مهیا نمی‌کند.

۳. هیچ الگوریتمی وجود ندارد که بتواند در بارهٔ برنامه بودن رشته‌ای دلخواه تصمیم بگیرد.

۴. پیش‌فرض همینگ، در بارهٔ ساکنان سیارات دوردست این است که «آنها نیز باید با همان قوانین فیزیکی حاکم بر ما، در جهت سازگاری هر چه بیشتر با محیط، مرحله به مرحله تکامل یافته باشند ...». می‌توان برخلاف همینگ معتقد بود که ممکن است ساکنان سیارات دوردست ادراکی کاملاً گسسته (دیجیتالی) از جهان داشته باشند (دیدگاه دوم). در آن‌صورت انبوهی از سؤالات را، که محتملاً در حال حاضر بلاجواب‌اند، می‌توان مطرح کرد.

۵. کم‌لطفی همینگ نسبت به منطق و بخشهایی دیگر از ریاضیات مؤید «کل حزب، بما لدیهم فرحون» است. این نگرش حزبی، یا به تعبیر کلیتر، نگرش ایدئولوژیک به موضوعات علمی، نه پدیده‌ای جدید است و نه غریب. پُر دور نرویم، به مضمون نوشته‌ها یا نانوشته‌ها (و کردارها)ی اطرافیان خوب بنگریم. تعیین اهمیت یک شاخه از ریاضیات یا کیفیت تحقیقات، بدون شک، امری دشوار است. تا زمانی‌که به «عوامل درونی» تعیین اهمیت یا کیفیت تکیه داریم، می‌توان تا حدودی قضاوت عینی داشت و کار قابل کنترل است. دشواری زمانی آغاز می‌شود که «عوامل بیرونی» ظهور می‌کنند.

محمد اردشیر
دانشگاه صنعتی شریف
ardeshir@karun.ipm.ac.ir

1. instrumentalism

NASHR-E RIYĀZI

Volume 11, Number 2, October 2000

Nashr-e Riyāzi is a Persian-language, expository mathematics journal published biannually (in April and October) by Iran University Press.

Annual subscription rates (including airmail postage) are: Middle East £ 19, Europe & Asia £ 21, North America & Far East £ 26.

For more information write to Iran University Press, 85 Park Avenue, Tehrān 15134, Iran, or contact ⟨nashriaz@vax.ipm.ac.ir⟩.

CONTENTS

* An asterisk indicates that the article was originally published elsewhere. Complete address of the original article appears at the end of the article.

ISSN: 1015-2857

از کتابهای مرکز نشر دانشگاهی

- **نظریهٔ گراف و کاربردهای آن**
  باندی، مورتی
  ترجمهٔ دارا معظمی
- **تحلیل رگرسیونی کاربردی**
  نورمن دریپر، هری اسمیت
  ترجمهٔ غلامحسین شاهکار، ابوالقاسم بزرگ‌نیا
- **معادلات دیفرانسیل و کاربرد آنها**
  جرج ف. سیمونز
  ترجمهٔ علی‌اکبر بابایی، ابوالقاسم میامئی
- **مقدمات معادلات دیفرانسیل و مسائل مقدار مرزی (جلد اول)**
  ویلیام ا. بویس، ریچارد ک. دیپریما
  ترجمهٔ محمدرضا سلطانپور، بیژن شمس
- **آشنایی با تاریخ ریاضیات (در دو جلد)**
  هاورد و. ایوز
  ترجمهٔ محمدقاسم وحیدی‌اصل
- **اصول آنالیز حقیقی**
  ربرت جی بارتل
  ترجمهٔ جعفر زعفرانی