فرهنگ و اندیشهٔ ریاضی
شمارهٔ ۲۵(پاییز ۱۳۷۹)، صص. ۵۷ تا ۶۰

دامنه‌های ایده‌آل اصلی تقریباً اقلیدسی هستند

جان گرینِ

در بسیاری از کتاب‌های جبر مجرد دورهٔ کارشناسی نشان داده می‌شود که هر دامنهٔ اقلیدسی (ED) یک دامنهٔ ایده‌آل اصلی (PID)و هر دامنهٔ ایده‌آلِ اصلی یک دامنهٔ تجزیه یکتا (UFD) است. بنابراین زنجیری از استلزام‌های منطقی را به صورت $ED \Rightarrow PID \Rightarrow UFD$ داریم. بسیاری از کتاب‌ها (و نه همه!) خاطرنشان می‌کنند که عکس این استلزام‌ها درست نیستند. اگرچه به‌راحتی می‌توان دید که $\mathbb{Z}[x]$ مثالی از یک UFD است که یک PIDنیست، اما مثالی از یک PID که یک ED نباشد اندکی مشکل‌تر حاصل می‌شود. در [۲]، کمپولی با اثبات اینکه به قول او $\mathbb{Z}[\xi]$ (که در آن $\xi = \frac{(-۱+\sqrt{-۱۹})}{۲}$) «تقریباً اقلیدسی» است به روشی ساده اثبات کرد که $\mathbb{Z}[\xi]$ دارای خواص مطلوب است. در این نوشته نشان می‌دهیم که در واقع شرط تقریباً اقلیدسی معادل با شرط PID است.

تعریف. دامنهٔ صحیح D را تقریباً اقلیدسی می‌نامیم اگر تابع $d : D \to \mathbb{Z}^+ \cup \{۰\}$ (که یک تابع تقریباً اقلیدسی نامیده می‌شود) وجود داشته باشد به طوری که

۱. $d(۰) = ۰$، و اگر $a \neq ۰$ آنگاه $d(a) > ۰$،

۲. اگر $b \neq ۰$، آنگاه برای هر $a \in D$، $d(ab) \geqslant d(a)$،

۳. برای هر $a, b \in D$، اگر $b \neq ۰$ آنگاه یکی از دو شرط زیر برقرار باشند:

الف) برای یک $g \in D$، $a = bg$

ب) برای x و yای در D، $۰ < d(ax + by) < d(b)$

تابع dی موردنظر در این مقاله در شرط قویتر $'(۲)$ که می‌گوید برای هر $a, b \in D$، $d(ab) = d(a)d(b)$ صدق خواهد کرد که از آن شرط (۲) به‌راحتی حاصل می‌شود.

نتیجهٔ اصلی این مقاله به قرار زیر است:

قضیهٔ ۱. دامنهٔ صحیح D یک دامنهٔ ایده‌ال اصلی است اگر و فقط اگر تقریباً اقلیدسی باشد.

اثبات: کمپولی [۲] ثابت کرد که اگر یک حلقه تقریباً اقلیدسی باشد یک PID است. برای کامل بودن اثبات قضیه، برهان او را در اینجا می‌آوریم. فرض کنیم D تقریباً اقلیدسی باشد و فرض کنیم I ایده‌ال ناصفری از D باشد. در بین عناصر $x \in I$، فرض کنیم B عنصری با مینیمال مقدار مثبت برای $d(x)$ باشد. برای $a \in I$ مفروض، $ax + by$برای هر $x, y \in D$ در I قرار دارد. بنابر تعریف b، رابطهٔ $\circ < d(ax + by) < d(b)$ نمی‌تواند برقرار باشد، در نتیجه باید شرط دوم یعنی $a = bq$ برای یک $q \in D$ برقرار باشد. بنابراین $I = (b)$.

اکنون فرض کنید D یک PID باشد. پس D یک UFD است، لذا می‌توان تابع d را به شکل زیر تعریف کرد: قرار می‌دهیم $d(\circ) = \circ$ و برای هر $a \neq \circ$، اگر $a = \epsilon p_{۱} \dots p_n$ که در آن ϵ یک عضو واحد و $p_{۱}$ و ... و p_n تحویل‌ناپذیرند، قرار می‌دهیم $d(a) = ۲^n$. چون $d(ab) = d(a)d(b)$ روشن است که d در شرایط (۱) و (۲) از تعریف صدق می‌کند. بنابراین فرض کنید $a, b \in D$ با $b \neq \circ$. فرض کنید $I = \{ax + by | x, y \in D\}$. از آنجا که I ایده‌آلی در D است، برای یک $r \in D$ با $r \neq \circ$ داریم $I = \langle r \rangle$. اگر $a = bq$ برای یک $g \in D$، آنگاه $I = \langle b \rangle$، در غیر این صورت $I \neq \langle b \rangle$. چون $b \in I$، لذا $b = xr$ برای یک $x \in D$، پس $d(b) \geqslant d(r)$. چون $I \neq \langle b \rangle$، لذا x یک عضو واحد نیست. پس $d(x) > ۱$، در نتیجه $d(r) < d(b)$. اگر $r = x_\circ(a) + y_\circ b$، آنگاه داریم $\circ < d(r) < d(b)$ و شرط (۳) برای d برقرار می‌شود. ■

مثال‌های دامنهٔ اقلیدسی در کتاب‌های جبر مجرد تقریباً همواره به صورت‌های $D = F[x]$ که F یک میدان است، و یا حلقهٔ اعداد صحیح در $Q[\sqrt{d}]$ برای مقادیر صحیح کوچک d می‌باشند. در حالت آخر، این‌گونه از کتاب‌ها ابتدا نرم یک عنصر این حلقه را معرفی کرده و سپس قدرمطلق آن را به‌عنوان تابع اقلیدسی مورد استفاده قرار می‌دهند. در حالت کلی، اگر F یک میدان عددی جبری (یک توسیع متناهی از Q) باشد، آنگاه F را می‌توان به عنوان یک فضای برداری با بعد متناهی روی Q درنظر گرفت. اگر $a \in F$، دراین صورت نگاشت $T_a(x) = ax$ آشکارا یک $\mathbb{Q}$ـتبدیل خطی از F به توی F خواهد بود. حال، نرم a، $N(a)$ برابر دترمینان این تبدیل خطی تعریف می‌شود. این نرم دارای خواص زیر است:

۱. $N(ab) = N(a)N(b)$ برای هر $a, b \in F$،

۲. $N(a) = \circ$ اگر و فقط اگر $a = \circ$،

۳. اگر a یک عدد صحیح جبری باشد، آنگاه $N(a) \in \mathbb{Z}$،

۴. یک عدد جبری a، یک عضو واحد است اگر و فقط اگر $N(a) = \pm ۱$،

خواص (۱) و (۲) خواص اولیه دترمینان هستند، خاصیت (۳) در [۵، صفحهٔ ۱۷۵] ذکر شده است و خاصیت (۴) نتیجهٔ ساده‌ای از (۱)، (۲) و (۳) است.

قضیهٔ ۲. اگر D مجموعهٔ اعداد صحیح در یک میدان عددی جبری و D یک دامنهٔ ایده‌ال اصلی باشد، آنگاه قدرمطلق نرم در شرایط تابع تقریباً اقلیدسی صدق می‌کند.

اثبات: خواص تابع d در قضیهٔ ۱ که در اثبات آن مورد استفاده قرار گرفتند عبارتند از:

۱. $d(ab) = d(a)d(b)$

۲. $a \in D$، آنگاه $d(a) = 1$ اگر و فقط اگر a یک عضو واحد است.

چون قدرمطلق نرم نیز دارای این خواص است، اثبات همانگونه که در قضیهٔ ۱ آمده است نتیجه می‌شود. بنابراین برای $a, b \in D$ داده شده، با شرط $b \neq 0$، فرض کنیم $I = \{ax+by|x, y \in D\} = \langle r \rangle$. اگر برای یک q در D داشته باشیم $a = bq$، آنگاه $I = \langle b \rangle$. در غیراین صورت $0 < |N(r)| < |N(b)|$، زیرا $b = xr$ برای یک عنصر ناواحد $x \in D$. ■

اگر D حلقه اعداد صحیح در یک توسیع متناهی F از Q باشد، اکنون با بررسی این نکته که آیا D همراه با قدرمطلق نرم تقریباً اقلیدسی است یا خیر می‌توان تحقیق کرد که آیا D یک دامنهٔ ایده‌ال اصلی است. بنابراین میدان‌های عددی از اهمیت ویژه‌ای برخوردار هستند. مثال دیگری از این نوع به قرار زیر است: در یک میدان عددی، D یک UFD است اگر و فقط اگر D یک PID باشد [۶، صفحهٔ ۱۴۶]. کمپولی [۲] برای نشان دادن اینکه این حلقه یک PID است از این حقیقت استفاده کرد که $\mathbb{Z}[\xi]$ با $\xi = \frac{(-1+\sqrt{-19})}{2}$ تقریباً اقلیدسی است. شیوهٔ برهان او را می‌توان به سادگی تعمیم داد تا نشان دهیم اگر ۱۹− را با ۴۳− یا ۱۶۳− جایگزین کنیم نتیجهٔ قبل همچنان برقرار خواهد بود. درحقیقت با کمی کوشش اثبات نتیجه مشهور [۱، صفحهٔ ۱۳۷] امکان‌پذیر است: حلقهٔ اعداد صحیح در $Q[\sqrt{1-4d}]$ که $d > 0$ یک PID است اگر و فقط اگر چندجمله‌ای $x^2 + x + d$ برای همه اعداد صحیح x با شرط $0 \leqslant x \leqslant d-2$، اول باشد.

تذکر آخر: اگر D زیرحلقه‌ای تقریباً اقلیدسی از یک میدان عددی باشد، قضیه ۲ بیان می‌کند که می‌توان از تابع قدرمطلق نرم به عنوان یک تابع که دارای خواص بسیار نزدیک به یک تابع اقلیدسی است استفاده کرد. فرض کنیم D واقعاً اقلیدسی باشد. آیا تابع قدرمطلق نرم به عنوان یک تابع اقلیدسی عمل می‌کند؟ ذکر این نکته حائز اهمیت است که هاردی و رایت [۴، صفحهٔ ۲۱۲] یک دامنهٔ اقلیدسی را نه به شکل متداول آن بلکه به طور صریح با استفاده از نرم به‌عنوان تابع اقلیدسی تعریف کردند. در هر صورت، پاسخ به سؤال بالا این است که نرم ممکن است به عنوان تابع اقلیدسی عمل نکند. در حقیقت، در [۳] نشان داده شده است که $\mathbb{Z}[\xi]$ با $\xi = \frac{(1+\sqrt{69})}{2}$ مثالی از یک حلقه است که اقلیدسی است اما نه نسبت به تابع قدرمطلق نرم.

سپاسگزاری: مایلم از جو گالیان و داور مقاله به‌خاطر تذکرات مفیدشان، و اعضاء گروه خبری شبکه‌ای Sci.math، به‌ویژه هنری کوهن به خاطر مرجع مربوط به حلقه‌ای که اقلیدسی است ولی نرم‌ـاقلیدسی

نیست تشکر نمایم.

مراجع

[1] Paulo Ribenboim, The Book of Prime Records, Springer-Verlag, New York, 1988.

[2] Oscar Campoli, A Principal Ideal Domain Is Not a Euclidean Domain, *American Mathematical Monthly*, **95** (1988) 868-871.

[3] David Clark, A quadratic field which is Euclidean but not norm-Euclidean, *Manuscripta Math.* **83**(1994), no 3-4, 327-330.

[4] G. Hardy and E. Wright, *An Introduction to the Theory of Numbers,* 5th Edition, Oxford University Press, Oxford.

[5] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory,* Springer-Verlag, New York, 1992.

[6] Edwin Weiss, *Algebraic Number Theory,* McGraw-Hill, New York, 1963.

مترجم: علی معدنشکاف

سمنان، دانشکدهٔ تربیت دبیر مهدی‌شهر، گروه ریاضی

پست الکترونیک: madansh@cic.aku.ac.ir