مقاله کلاسیک

یکتایی تجزیه•

پیر ساموئل

ترجمهٔ روشن تجرد، روزبه حضرت

۱. مقدمه

می‌دانیم که هر عدد طبیعی را تنها به یک روش می‌توان به‌صورت حاصلضرب اعداد اول نوشت. به‌منظور تعمیم این مطلب بهتر است خاصیت یکتایی تجزیه را در حلقهٔ $\mathbb{Z}$ از اعداد صحیح بیان کنیم. بنابراین اگر مجموعهٔ اعداد اول را با P نشان دهیم، هر عدد غیرصفر $x \in \mathbb{Z}$ را می‌توانیم به‌طور یکتا به‌صورت زیر بنویسیم

$$x = \pm 1 \prod_{p \in P} p^{\nu_p(x)} \qquad (1)$$

برای اینکه فرمول (۱) از لحاظ ریاضی با معنا باشد، فرض می‌کنیم نمای $\nu_p(x)$ نمایشگر اعداد صحیح مثبتی است که تقریباً همه صفرند (یعنی بجز تعدادی متناهی از آنها، بقیه ۰اند). فرمول نسبتاً انتزاعی (۱) که حاصلضرب موجود در آن ظاهراً نامتناهی است این مزیت بزرگ را دارد که نحوهٔ وابستگی نماهای $\nu_p(x)$ به x را نشان می‌دهد: در صورت منظور کردن نماهای منفی، فرمول (۱) برای تمام اعداد گویای غیرصفر برقرار است. همچنین می‌توان دید که به‌ازای هر جفت (x, y) از اعداد گویای ناصفر داریم

$$\nu_p(xy) = \nu_p(x) + \nu_p(y), \ \nu_p(x+y) \geq \inf(\nu_p(x), \nu_p(y)) \qquad (2)$$

جبردانان فرمول (۲) را به این صورت بیان می‌کنند که نگاشت $\nu_p : Q^* \to \mathbb{Z}$ یک ارزهٔ گسسته از میدان [هیأت] اعداد گویاست.

به‌طور کلی، حلقهٔ تجزیه‌ای (یا «دامنهٔ تجزیهٔ یکتا»، U.F.D) را به‌عنوان دامنهٔ صحیح Aای تعریف می‌کنیم که دارای زیرمجموعه‌ای چون P است چنانکه هر عنصر غیرصفر x از A را بتوان به‌طور یکتا به‌صورت

$$x = u \prod_{p \in P} p^{\nu_p(x)} \qquad (1')$$

نوشت که در آن u یک عنصر وارونپذیر در A است و نماهای $\nu_p(x)$ اعداد صحیح مثبت و تقریباً همه صفرند. به آسانی می‌توان ثابت کرد که زیرمجموعهٔ P به‌صورت یکتا (صرف‌نظر از ضریبهای وارونپذیر) مشخص می‌شود. به‌بیان دقیقتر، مجموعهٔ $(Ap)_{p \in P}$ از ایده‌آلهای اصلی به‌طور یکتا مشخص می‌شود و با مجموعهٔ همه ایده‌آلهای اصلی ماکسیمالِ متمایز از A یکی است. توجه کنید که ایده‌آل اصلی Ab از یک دامنهٔ A ماکسیمال است (در میان ایده‌آلهای اصلیِ متمایز از A) اگر و تنها اگر هر مقسوم‌علیه b مانند d یا وارونپذیر و یا چنان باشد که db^{-1} وارونپذیر باشد؛ در این‌صورت b را عضو تحویل‌ناپذیر A می‌نامیم.

برای یک حلقهٔ A، تجزیه‌ای بودن خاصیت بسیار مفیدی است. دست‌کم برای مسائلی که به ساختمان ضربی حلقه مربوط می‌شود، حساب در هر حلقهٔ تجزیه‌ای A به‌زیباییِ حساب در حلقهٔ $\mathbb{Z}$ از اعداد صحیح معمولی است. یادآور می‌شویم که در قرن نوزدهم، ریاضیدانانی مانند کومر و ددکیند متوجه شدند که برخی از حلقه‌های اعداد صحیح جبری، تجزیه‌ای نیستند. روابط

$$2 \times 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}) \ , \ 3 \times 3 = (\sqrt{10} + 1)(\sqrt{10} - 1)$$

پیر ساموئل (Pierre Samuel) (متولد ۱۹۲۱) ریاضیدان فرانسوی معاصر و استاد بازنشستهٔ دانشگاه پاریس است. آثار تحقیقاتی او عمدتاً در زمینهٔ نظریهٔ جبری اعداد و هندسهٔ جبری است. ساموئل نویسندهٔ چند کتاب مشهور است که از آن میان کتابهای زیر شهرت دارند: کتاب دو جلدی جبر جابه‌جایی (با همکاری ریاضیدان فقید اسکار زاریسکی، ۱۹۵۸، ۱۹۶۰)، نظریهٔ جبری اعداد (۱۹۶۷)، و هندسهٔ افکنشی [تصویری] (۱۹۸۶). مقالهٔ حاضر برندهٔ جایزهٔ شوونه (Chauvenet) در زمینهٔ تألیف مقالات توصیفی شده است.

نشان می‌دهند که حلقه‌های $\mathbb{Z}[\sqrt{-5}]$ و $\mathbb{Z}[\sqrt{-10}]$ تجزیه‌ای نیستند. این امر، کومر و ددکیند را به معرفی مفهوم مهم ایده‌آل و تجزیهٔ یکتایی ایده‌آلها به جای تجزیهٔ یکتایی عناصر هدایت کرد و بدین ترتیب، نظریهٔ مربوط به حلقه‌هایی که امروز آنها را «حلقه‌های ددکیند» می‌نامیم پایه‌گذاری شد. کمبود وقت مرا از بحث بیشتر در بارهٔ این نظریهٔ مهم و زیبا باز می‌دارد.

اهمیت حلقه‌های تجزیه‌ای تنها به دلیل جنبه‌های حسابی آنها نیست. تجزیه‌ای‌بودن یک تعبیر خیلی سادهٔ هندسی نیز دارد. در هندسه، و به‌طور دقیقتر در مطالعهٔ واریته [چندگونا]های جبری، تحلیلی، یا صوری، یک حلقهٔ A به‌عنوان حلقه‌ای از توابع (جبری یا تحلیلی، برحسب مورد) روی واریته‌ای مانند V یا در همسایگی نقطه‌ای از V مطرح می‌شود. در اینجا، دامنه بودن A به معنی تحویل‌ناپذیری V است. اگر بعد V را به n نشان دهیم، تجزیه‌ای‌بودن A، قطع نظر از جزئیات، بدین معنی است که هر زیرواریتهٔ W با بعد $n-1$ از V را می‌توان با یک معادلهٔ تنها تعریف کرد. به‌بیان دقیقتر، توابع $f \in A$ که روی W صفر می‌شوند، ایده‌آلی مانند $p(W)$ در A تشکیل می‌دهند و تجزیه‌ای‌بودن حلقه معادل این است که این ایده‌آلهای $p(W)$ (برای Wهای با بعد $n-1$) ایده‌آل اصلی باشند.

۲. چگونگی اثباتِ تجزیه‌ای‌بودن

دیدیم که تجزیه‌ای‌بودن خاصیت مطلوبی برای یک حلقه است. ولی اثبات اینکه حلقه‌ای این خاصیت را دارد، اغلب بدیهی نیست. پس شناختن مشخصات هر چه بیشتری از حلقه‌های تجزیه‌ای مفید واقع خواهد شد.

همان‌طور که در بخش یک دیدیم، تجزیه‌ای‌بودن A به این معنی است که هر عضو غیرصفر A را بتوان به حاصلضرب اعضای تحویل‌ناپذیر تجزیه کرد، و چنین تجزیه‌ای صرف‌نظر از ضرایب وارون‌پذیر، یکتا باشد. وجود یا عدم وجود چنین تجزیه‌ای معمولاً به‌آسانی معلوم می‌شود و می‌توان آن را از «شرط زنجیره» برای ایده‌آلهای اصلی نتیجه گرفت (که در هر حلقهٔ تجزیه‌ای برقرار است):

(۳) هر دنبالهٔ اکیداً صعودی از ایده‌آلهای اصلی A متناهی است، که این با «شرط ماکسیمال» معادل است:

($'$۳) هر خانوادهٔ غیرتهی از ایده‌آلهای اصلی A یک عضو ماکسیمال دارد.

به‌عنوان مثال، (۳) یا ($'$۳) هنگامی که حلقهٔ A نوتری باشد، برقرار است و بیشتر حلقه‌هایی که در حساب [نظریهٔ جبری اعداد] و هندسه با آنها سروکار داریم نوتری هستند. به‌علاوه، با احتیاط کامل [در نظر گرفتن کلیهٔ شرایط] خاصیت (۳) می‌تواند در حد مستقیم هم درست باشد. بنابراین، از این پس فرض می‌کنیم که شرط (۳) برقرار باشد.

اما در مورد یکتایی تجزیه، موضوع چندان ساده نیست. یکتایی تجزیه در یک حلقهٔ A بدین معناست که هر عضو تحویل‌ناپذیر p از A این خاصیت قویتر را دارد که:

(۴) اگر p حاصلضرب ab را عاد کند، آنگاه p، a یا b را عاد می‌کند.

برعکس، با فرض (۳) و با به‌کار بردن اثباتی از نظریهٔ مقدماتی اعداد، می‌توان دید که (۴)، یکتایی تجزیه به عوامل تحویل‌ناپذیر را نتیجه می‌دهد. عضوی چون p که خاصیت (۴) را داراست، یک عضو اول A نامیده می‌شود. این بدان معنی است که ایده‌آل اصلی Ap، ایده‌آلی اول است. ($ab \in Ap \Rightarrow a \in Ap$ یا $b \in Ap$) و معادلش این است که حلقهٔ خارج قسمتی A/Ap یک دامنه است. همچنان که در نظریهٔ مقدماتی اعداد نشان داده می‌شود، خاصیت (۴) معادل است با

($'$۴) هر دو عضو A، دارای بزرگترین مقسوم‌علیه مشترک‌اند.

و نیز با

($''$۴) هر دو عضو A دارای کوچکترین مضرب مشترک‌اند.

صورت مفیدی از ($''$۴) چنین است

($'''$۴) اشتراک هر دو ایده‌آل اصلی A، یک ایده‌آل اصلی است.

اگر با یک دامنهٔ نوتری A سروکار داشته باشیم، می‌توانیم ثابت کنیم که هر عضو غیروارون‌پذیر در A متعلق به یک ایده‌آل اول به ارتفاع ۱ است (ایده‌آل اول غیرصفری که مینیمال باشد). از این به‌سادگی نتیجه می‌شود که دامنهٔ نوتری A، تجزیه‌ای است اگر و تنها اگر

(۵) هر ایده‌آل اول به ارتفاع ۱، ایده‌آلی اصلی از A باشد.

این شرط را پیش از این در آخر بخش (۱)، هنگامی‌که تعبیر هندسی تجزیه‌ای‌بودن را مورد بحث قرار دادیم، دیده‌ایم.

مشخصات فنی‌تر حلقه‌های تجزیه‌ای در چارچوب نظریهٔ حلقه‌های کرول[1] ارائه می‌شود. برای این منظور خواننده را به جبر جابه‌جایی، فصل هفتم، نوشتهٔ بورباکی [۴] ارجاع می‌دهیم. در اینجا فقط اشاره می‌کنیم که ردهٔ حلقه‌های کرول، شامل ردهٔ حلقه‌های تجزیه‌ای است و این ردهٔ گسترده‌تر (کرول) تحت عملهای نظریهٔ حلقه‌ها پایدارتر است. به‌علاوه، به‌طور کلی مشخص‌کردن اینکه حلقه‌ای کرول است یا نه، کار ساده‌ای است. بنابراین مسأله این است که امتحان کنیم آیا حلقهٔ کرول داده شده، تجزیه‌ای است و اگر نیست، میزان «تجزیه‌ای‌نبودن» آن چقدر است.

۳. خواصی قویتر از تجزیه‌ای بودن

برای اثبات اینکه $\mathbb{Z}$، تجزیه‌ای است، معمولاً در ابتدا نشان می‌دهند که $\mathbb{Z}$ اصلی است (یعنی هر ایده‌آل $\mathbb{Z}$ اصلی است). در این‌صورت برقراری شرط زنجیره (۳) و شرط ($'''$۴) واضح است. مثال حلقهٔ چندجمله‌ای با چندین متغیر روی یک میدان، نشان می‌دهد که اصلی‌بودن خاصیتی قویتر از تجزیه‌ای‌بودن است؛ بنابراین ممکن است تمرکز روی این خاصیت قویتر برای اثبات تجزیه‌ای‌بودن، خطرناک به‌نظر رسد. لیکن معیار قابل اعتمادی در دست داریم که به ما می‌گوید آیا خطری وجود دارد یا نه. در حقیقت متخصصان جبر جابه‌جایی نظریهٔ جامعی در بارهٔ بُعد یک حلقه به‌وجود آورده‌اند و روشهای بسیاری نیز برای محاسبهٔ این بُعد به‌دست آورده‌اند. به‌علاوه حلقه‌های اصلی به‌عنوان حلقه‌های تجزیه‌ای با بُعد ۰ یا ۱ مشخص شده‌اند. بنابراین، بُعد حلقهٔ مورد نظر A نشان می‌دهد که آیا کوشش برای اثبات اصلی بودن این حلقه معقول خواهد بود یا خیر.

در بیشتر مواردِ هندسی، برای اثبات اصلی‌بودن، تجزیه‌ای‌بودن و یک‌بعدی بودن به‌طور جداگانه ثابت می‌شود. اما در نظریهٔ جبری اعداد، روشهایی

1 Krull rings

برای اثبات مستقیم اصلی‌بودن یک حلقه وجود دارد. برای نمونه، فرض کنیم K یک میدان اعداد با درجهٔ متناهی n روی اعداد گویا باشد. فرض کنیم A حلقهٔ اعداد صحیح جبری K و d مبین مطلق A، و $2r_2$ تعداد مزدوجهای غیرحقیقی K در $\mathbb{C}$ باشد. در این‌صورت می‌توان با استفاده از نظریهٔ مینکوفسکی در بارهٔ نقاط شبکه‌ای در مجموعه‌های محدب ثابت کرد که هر ایده‌آل غیرصفر $\mathfrak{U}$ از A را می‌توان به‌صورت $\mathfrak{U} = xb$ نوشت که در آن x عضوی از K^* است و b ایده‌الی در A است که برای آن داریم

$$\text{card}(A/b) < \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n}(|d|^{\frac{1}{2}}) \qquad (6)$$

حال، سمت راست نابرابری (۶) را می‌توان با روشهای متعارف محاسبه کرد، و در سمت چپ هم تعداد ایده‌آلهایی مانند b که برای آنها A/b کاردینال مفروض c را داشته باشند، متناهی است و در صورتی که c خیلی بزرگ نباشد، به‌راحتی می‌توان آنها را مشخص کرد. اگر تمام ایده‌آلهای b که در (۶) صدق می‌کنند، اصلی باشند، آنگاه حلقهٔ A نیز اصلی خواهد بود. خواننده می‌تواند این روش را برای حلقهٔ $A = \mathbb{Z}[i]$ از اعداد صحیح گاوسی به‌کار برد (در اینجا $r = 2$ و $r_2 = 1$، $|d| = 4$)، پس سمت راست نابرابری (۶)، کوچکتر از ۲ خواهد بود و از این نابرابری نتیجه می‌شود که $b = A$). ممکن است به‌نظر بیاید که این، روش بسیار پیچیده‌ای برای اثبات اصلی‌بودن حلقهٔ $\mathbb{Z}[i]$ است! در حقیقت، در اثبات معمول برای حلقه‌های $\mathbb{Z}$، $\mathbb{Z}[i]$ و همچنین حلقهٔ چندجمله‌ای $k[X]$ روی میدان k، از این مطلب که این حلقه‌ها اقلیدسی هستند استفاده می‌شود. یادآوری می‌کنیم که دامنهٔ صحیح A را اقلیدسی گویند اگر نگاشتی مانند $\phi : A \to N$ (N مجموعهٔ اعداد صحیح مثبت) وجود داشته باشد چنانکه به‌ازای هر عضو غیرصفر b در A، هر ردهٔ به‌پیمانهٔ Ab نماینده‌ای چون r با ضابطهٔ $\phi(r) < \phi(b)$ داشته باشد (یعنی هر عضو a از A را بتوان به‌صورت $a = bq + r$ نوشت چنانکه $\phi(r) < \phi(b)$).

هر حلقهٔ اقلیدسی A اصلی است زیرا برای هر ایده‌آل غیرصفر b در A، می‌توان عضو غیرصفری مانند x از b انتخاب کرد به‌طوری که مقدار $\phi(x)$ مینیمم باشد، و ملاحظه کرد که عضو x ایده‌آل b را تولید می‌کند. برای این اثبات لازم نیست فرض کنیم که مقادیر ϕ در N هستند؛ به‌جای مجموعهٔ N در برد ϕ هر مجموعهٔ خوشترتیب W را می‌توان به‌کار برد. نگاشت $\phi : A \to W$ را که در بالا تعریف شد یک الگوریتم روی A می‌نامند. اگر حلقهٔ مفروض A و یک مجموعهٔ خوشترتیب W را که به‌اندازهٔ کافی بزرگ باشد در نظر بگیریم (مثلاً به‌طوری که $\text{card}(W) > \text{card}(A)$)، نظریهٔ مجموعه‌های خوشترتیب نشان می‌دهد که هر الگوریتم روی A با الگوریتمی که مقادیرش در W است یکریخت (به مفهوم واضح) است. به‌علاوه اگر $\phi_\alpha : A \to W$ خانواده‌ای از الگوریتمها روی A باشد، $\phi = \inf_\alpha \phi_\alpha$ نیز یک الگوریتم خواهد بود، بنابراین A (اگر اقلیدسی باشد) دارای کوچکترین الگوریتم است. اگر میدانهای مانده‌ای A متناهی باشند، در حقیقت این کوچکترین الگوریتم، $\phi_\circ$، مقادیر خود را از مجموعهٔ اعداد صحیح N خواهد گرفت (حالت کلی هنوز حل نشده است). ولی این الگوریتم لزوماً الگوریتم معمولی نیست: در حالت $\mathbb{Z}$، $\phi_\circ(n)$ تعداد رقمهای دودویی عدد صحیح $|n|$ ($n \in \mathbb{Z}$) است. ولی برای چندجمله‌ایهای برحسب X روی یک میدان k، $\phi_\circ(P(X))$ درجهٔ چندجمله‌ای $P(X)$ است.

ریاضیدانان تلاشهای زیادی برای مشخص کردن میدانهای اعداد جبری که حلقهٔ اعداد جبری آنها اقلیدسی است، انجام داده‌اند. بیشتر آنان به بررسی این مسألهٔ محدودتر پرداخته‌اند که آیا «تابع نُرم» معمولی (یعنی $\phi(x) = \text{card}(A/Ax)$ به‌ازای $x \neq 0$) الگوریتم است یا نه. برای میدانهای درجه دوم موهومی، پنج میدان $Q(\sqrt{-d})$ به‌ازای $d = 1, 2, 3, 7, 11$، تنها میدانهایی هستند که نرم برای آنها الگوریتم است و همچنین تنها میدانهایی هستند که حلقهٔ اعداد جبری آنها اقلیدسی است. اما چهار حلقهٔ اصلی غیراقلیدسی برای میدانهای درجه دوم موهومی، به‌ازای $d = 19, 47, 67, 163$، وجود دارد. (وجود پنجمین حلقه که مسأله‌ای پیچیده بود، به‌تازگی نفی شده ست) در مورد میدانهای درجه دوم حقیقی $Q(\sqrt{m})$ که $m > 0$، فهرست آنهایی که با نرم معمولیشان اقلیدسی‌اند، معلوم شده است:

$$m = 2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 56, 73$$

و اصلی‌بودن بسیاری دیگر نیز معلوم شده است، اما نمی‌دانیم که آیا تعداد آنها متناهی است یا نه. همچنین در حال حاضر نمی‌دانیم که آیا ممکن است بعضی از آنها برای الگوریتم دیگری غیر از نُرم، اقلیدسی نباشند. شواهدی نویسنده را قانع می‌کند که میدان $Q(\sqrt{14})$ شایسته است از این لحاظ مطالعه شود. (ر.ک. [۵] و [۶]). نتیجه اینکه، می‌توان گفت نظریهٔ حلقه‌های اقلیدسی دارای سرشتی متفاوت با تجزیه‌ای‌بودن است.

۴. قضیهٔ ناگاتا

ماسایوشی ناگاتا قضیه‌ای ثابت کرد که برای مشخص کردن حلقه‌های تجزیه‌ای بسیار مفید است. یادآور می‌شویم که اگر A یک دامنهٔ صحیح با میدان خارج‌قسمتی K باشد و S یک زیرمجموعهٔ ضربی‌بسته از A ($0 \notin S$)، آنگاه کسرهای a/s که در آن $a \in A$ و $s \in S$، زیرحلقه‌ای از K را تشکیل می‌دهند که با $S^{-1}A$ نشان داده و حلقهٔ خارج‌قسمتهای A نسبت به S نامیده می‌شود. اکنون فرض کنیم که A در شرط متناهی‌بودن (۳) (ر.ک. بخش ۲) صدق کند و S به‌وسیلهٔ عناصر اول تولید شود و همچنین $S^{-1}A$ یک حلقهٔ تجزیه‌ای باشد؛ در این صورت قضیهٔ ناگاتا حاکی است که حلقهٔ A نیز تجزیه‌ای است. اگر S به‌وسیلهٔ تعداد متناهی عناصر اول تولید شود می‌توان از شرط (۳) صرف‌نظر کرد. صورت بسیار ساده‌ای از عکس قضیهٔ ناگاتا چنین است که هر حلقهٔ خارج‌قسمتهای یک حلقهٔ تجزیه‌ای، خودش تجزیه‌ای است.

یک نتیجهٔ سادهٔ قضیهٔ ناگاتا، لم گاوس در مورد حلقه‌های چندجمله‌ای است. فرض کنیم R حلقه‌ای تجزیه‌ای و L میدان خارج‌قسمتی آن و $S = R - \{0\}$ باشد. چون هر عضو اول p از R در حلقهٔ چندجمله‌ای $A = R[X]$ نیز اول خواهد ماند (زیرا $A/pA = (R/pR)[X]$ یک دامنه است)، بنابراین S به‌وسیلهٔ اعضای اول A تولید می‌شود. اما $S^{-1}A = L[X]$ یک حلقهٔ چندجمله‌ای یک متغیره روی یک میدان است، بنابراین اقلیدسی و تجزیه‌ای است. پس طبق قضیهٔ ناگاتا، $A = R[X]$ نیز تجزیه‌ای است. همین نتیجه با استقرا برای حلقه‌های چندجمله‌ای چندمتغیره روی یک حلقهٔ تجزیه‌ای نیز به‌دست می‌آید.

در اینجا سه مثال دیگر از کاربرد قضیهٔ ناگاتا را به‌اجمال بیان می‌کنیم (اثبات کامل آنها را به خواننده واگذار می‌کنیم).

(الف) فرض کنیم k میدانی جبری‌بسته با مشخصهٔ مخالف ۲ و $F(X_1, \ldots, X_n)$ یک فرم درجه دوم ناتبهگون روی k باشد ($n \geq 5$). در این صورت $A = \frac{k[X_1,\ldots,X_n]}{(F)}$، تجزیه‌ای است. (با تعویض متغیر قرار

می‌دهیم $F = X_1X_2 + G(X_3, \ldots, X_n)$؛ اکنون تصویر X_j در A را به x_j نشان می‌دهیم؛ در این صورت چون G تحویل‌ناپذیر است ($n \geq 5$)، x_1 اول می‌باشد. اکنون قرار می‌دهیم $S = \{1, x_1, \ldots, x_1^j, \ldots\}$. خواهیم دید $S^{-1}A = k[x_1, x_2, \ldots, x_n][1/x_1]$ به‌عنوان حلقهٔ خارج‌قسمتهای یک حلقهٔ چندجمله‌ای، تجزیه‌ای است.)

(ب) فرض کنیم k میدانی باشد که در آن $\sqrt{-1} \notin k$، و قرار می‌دهیم $A = k[X, Y, Z]/(X^2 + Y^2 + Z^2 - 1)$ («حلقهٔ کرهٔ دوبعدی»). در این‌صورت A تجزیه‌ای است. تصاویر X، Y، Z در A را به x، y، z نشان می‌دهیم؛ خواهیم داشت $x^2 + y^2 = (1 + z)(1 - z)$؛ S را مجموعه‌ای تولید شده به‌وسیلهٔ $z - 1$ که اول است در نظر می‌گیریم. اکنون بنابر آنچه در (الف) دیده‌ایم، $S^{-1}A$ یک حلقهٔ تجزیه‌ای است.

(پ) فرض کنیم k یک میدان باشد و $A = k[X, Y, Z]/(x^r + Y^s + Z^t)$ که r، s، t دو به دو نسبت به هم اول‌اند. در این‌صورت A تجزیه‌ای است. (تصاویر X، Y، Z در A را به x، y، z نشان می‌دهیم. بنابراین $z^t = -(x^r + y^s)$. ابتدا فرض می‌کنیم که $t \equiv 1 \pmod{rs}$، یعنی $t = 1 + drs$. S را مجموعهٔ تولید شده به‌وسیلهٔ z (که اول است) می‌گیریم و قرار می‌دهیم $x' = \frac{x}{z^{ds}}$ و $y' = \frac{y}{z^{dr}}$. در این‌صورت $z = -(x'^r + y'^s)$، و $S^{-1}A = k[x', y'][1/z]$، تجزیه‌ای است. به‌طور کلی می‌توان عدد صحیحی مانند j چنان انتخاب کرد که $jt \equiv 1 \pmod{rs}$ و jامین ریشهٔ w را جانشین z کرد.

۵. نتایج دیگر

امروزه نظریهٔ حلقه‌های تجزیه‌ای بسیار گسترده‌تر از حدی است که در بالا به اجمال شرح داده شد. به‌عنوان مثال در [۲] در حدود ۸۰ صفحه یادداشت درسی که کاملاً به حلقه‌های تجزیه‌ای اختصاص دارد آمده است که برای مطالعهٔ آن، آشنایی به مطالب زیادی در زمینهٔ جبر جابه‌جایی و هومولوژیک لازم است. به‌علاوه این یادداشت درسی شامل تمام مطالب این مبحث در زمان نوشته شدن یادداشت (۱۹۶۳) نمی‌شود و از آن زمان به بعد هم نظریه پیشرفت کرده است. بنابراین ما فقط نکات مهم این نظریه را به اجمال و بدون ذکر بعضی از تعریفها شرح می‌دهیم؛ خواننده برای ملاحظهٔ جزئیات تعریفها، اثباتها، و نتایج وابسته می‌تواند به مراجع انتهای مقاله رجوع کند.

۱. سریهای توانی. در بخش ۴، لم گاوس در بارهٔ چندجمله‌ایها بیان شد. این لم، نمونه خاصی است از «انتقال» خواص حلقهٔ A به حلقه چندجمله‌ای $A[X]$. انتقالهای مشابه بسیاری تاکنون شناخته شده‌اند، و همچنین انتقالهایی که خواص حلقهٔ A را به حلقه سریهای توانی صوری $A[[X]]$ منتقل می‌سازند. بنابراین معقول می‌نمود که حدس بزنیم اگر A یک حلقهٔ تجزیه‌ای باشد، $A[[X]]$ نیز چنین خواهد بود. ولیکن این حدس رد شده است (رک. [۷]). در اولین مثال ناقضِ ارائه شده، حلقهٔ A حلقه‌ای موضعی و غیرکامل بود و در نظر گرفتن سری توانی صوری روی یک حلقهٔ غیرکامل و موضعی A از دید برخی از ریاضیدانان غیرطبیعی (و حتی قبیح) جلوه می‌کرد. اخیراً سایمن [۱۳] حلقهٔ Aای ساخت که کامل، موضعی و تجزیه‌ای است ولی $A[[X]]$ تجزیه‌ای نیست، و به این ترتیب هرگونه شک و شبهه برطرف شد.

۲. حلقه‌های منظم. حلقهٔ منظم در جبر جابه‌جایی تعریف می‌شود. در حالت هندسی، این حلقه متناظر با یک واریتهٔ ناتکین است. در ۱۹۵۷، اوسلندر[1] و بوخسباوم[2] با استفاده از روشهای هومولوژیک ثابت کردند هر حلقهٔ منظم و موضعی، تجزیه‌ای است. صورت کارامدتری از اثبات آنها را کاپلانسکی در [۱] و [۲] و بورباکی در [۴] آورده‌اند.

از طرف دیگر اگر A حلقه‌ای منظم و تجزیه‌ای (نه لزوماً موضعی) باشد آنگاه $A[X]$ و $A[[X]]$ هر دو تجزیه‌ای هستند.

۳. پایین‌برِ گالوایی[3]. فرض کنیم A حلقه‌ای تجزیه‌ای باشد و G زیرگروهی متناهی از خودریختیهای A؛ اعضایی از A که تحت G ناوردا می‌مانند تشکیل زیرحلقه‌ای از A می‌دهند که معمولاً به‌صورت A^G نشان داده می‌شود. فرض کنیم A^* گروه ضربیِ اعضایِ وارونپذیر A باشد، در این‌صورت اگر گروه کوهومولوژی $H^1(G, A^*)$ صفر شود، حلقهٔ A^G تجزیه‌ای است ([۲] و [۳] و [۱۷]).

مثال جالبی در دست است که نویسنده نمی‌تواند از بیان آن خودداری کند. حلقهٔ A را به‌صورت حلقهٔ چندجمله‌ای $A = k[X_1, \ldots, X_n]$ (k یک میدان و $n \geq 5$) و G را گروه متناوب A_n در نظر بگیرید که روی A به‌وسیلهٔ جایگشتهای متغیرها عمل می‌کند. در اینجا حلقهٔ A^G روی k به‌وسیلهٔ توابع متقارن مقدماتی s_1، $\ldots$، s_n و «مبین» $d = \prod_{i<j}(X_i - X_j)$ تولید می‌شود. می‌دانیم $d^2 = P(s_1, \ldots, s_n)$، که P یک چندجمله‌ای روی k است. به‌علاوه G روی $A^* = k^*$ به‌صورت بدیهی عمل می‌کند. بنابراین $H^1(G, A^*) = \mathrm{Hom}(G, k^*)$ (فرمول کلاسیک در کوهومولوژی گروهها). چون $G = A_n$ یک گروه ساده است ($r \geq 5$) و چون k^* جابه‌جایی است، خواهیم داشت $\mathrm{Hom}(G, k^*) = 0$ و لذا A^G تجزیه‌ای است.

با همین روش مثالی از یک حلقهٔ تجزیه‌ای به‌دست می‌آید که یک حلقهٔ مکولی[4] [۱۸] نیست. توجه کنید که مورتی[5] ثابت کرده است که هر حلقهٔ مکولی و تجزیه‌ای لزوماً یک حلقهٔ گورنشتاین است.

در مشخصهٔ $p \neq 0$، نظریهٔ مشابهی موجود است که در آن، مشتقها به‌جای خودریختیها قرار می‌گیرند. ([۲]، [۹]، [۱۶]). مانند بالا، در اینجا نیز اثباتهای تجزیه‌ای تا حدی محاسباتی هستند و گاه (مخصوصاً در مشخصه ۲) اجرای کامل این محاسبات در مقایسه با حالت خودریختیها آسانتر است.

۴. مقاطع کامل. یک حلقهٔ موضعی A «مقطع کامل» نامیده می‌شود اگر یکریخت با یک R/I باشد که R حلقهٔ منظم و موضعی و I ایده‌آلی تولید شده توسط Rـ دنباله‌ای منظم باشد (بدین معنا که I بتواند به‌وسیلهٔ عناصر $\dim(R) - \dim(R/I)$ تولید شود). گروتندیک با به‌کار بردن روشهای قدرتمند نظریهٔ اسکیمها[6] ثابت کرد که اگر A مقطع کامل باشد به‌طوری‌که A_p تجزیه‌ای باشد هرگاه $\dim(A_p) \leq 3$، آنگاه A تجزیه‌ای خواهد بود ([۱۹]). این تعمیمی از قضیهٔ هندسی سوِری[7]، افشتز، و آندره‌اوتی[8] است. تاکنون هیچ اثباتی از قضیهٔ گروتندیک که صرفاً مبتنی بر نظریهٔ حلقه‌ها باشد ارائه نشده است.

۵. حلقه‌های تجزیه‌ای دوبعدی. قبلاً گفتیم که حلقه‌های تجزیه‌ای یک‌بعدی، اصلی‌اند. در میان آنها حلقه‌های موضعی همان حلقه‌های ارزهٔ گسسته هستند که فرض کرده‌ایم خواننده با آنها آشناست. در بُعد ۲، مثالهای زیادی از حلقه‌های تجزیه‌ای را دیده‌ایم، مثلاً، حلقه‌های رویه‌های $x^i + y^j + z^k = 0$

---

1. M. Auslander 2. D. Buchsbaum 3. Goloision going-down
4. Macaulay 5. P. Murthy 6. Schemes 7. F. Severi
8. A. Andreotti

(که i، j، و k دو به دو نسبت به هم اول‌اند) و همچنین حلقه‌های کرهٔ $x^۲ + y^۲ + z^۲ - ۱ = ۰$. با موضعی‌سازیِ اولین گروه از این حلقه‌ها در مبدأ، تعداد زیادی حلقهٔ موضعی غیرمنظم تجزیه‌ای دوبعدی به‌دست می‌آوریم. این حلقه‌های موضعی کامل نیستند و به‌علاوه، تجزیه‌ای‌بودن حلقهٔ کامل‌شده[1]‌های آنها، یعنی، $C = K[[x, y, z]]$ مورد شک بود. ابتدا شجا[2] و مامفورد نشان دادند که حلقهٔ کامل C از رویهٔ $x^۲ + y^۳ + z^۵ = ۰$، تجزیه‌ای است. سپس سالمن، برای ارائهٔ مثال ناقض خود که در (۱) به آن اشاره کردیم، همین مطلب را برای رویهٔ $x^۲ + y^۳ + tz^۶ = ۰$ روی میدان K، که $K = k(t)$ و در آن t روی k غیرجبری است، ثابت کرد.

در مثال آخر، میدان K جبری-بسته نیست. بریسکورن[3] با استفاده از روشهای هندسهٔ جبری نشان داده است که در میان تمام حلقه‌های موضعی کامل دوبعدی روی یک میدان جبری-بسته، تنها ۲ نوع از آنها تجزیه‌ای است: حلقهٔ منظم $K[[X, Y]]$ (سری توانی صوری) و حلقهٔ $K[[x, y, z]]$ با $x^۲ + y^۳ + z^۵ = ۰$ (رک. [۱۳]). شایان ذکر است که حلقهٔ دوم حلقهٔ ناورداهای یک گروه بیست وجهی است که بر حلقهٔ اول عمل می‌کند [۱].

کتابشناسی حلقه‌های تجزیه‌ای

شرحی مقدماتی از موضوع در مرجع زیر آمده است:

1. P. Samuel, Anneaux Factoriels (red. A. Micali), Bol. Soc. Mat., São Paulo, 1964.

بحث کاملتر در مرجع زیر آمده است:

2. P. Samuel, Lectures on unique factorization domains, (notes by Pavman Murthy) Tata Institute for Fundamental Research lectures, No 30, Bombay, 1964.

3. ———, Lectures in commutative algebra (notes by M. Bridger), mimeographed by Brandeis University, Waltham, Mass., 1964-65.

برای مطالعهٔ بحث حلقه‌های تجزیه‌ای در چارچوب حلقه‌های کرول، رک:

4. N. Bourbaki, Algèbre Commutative, Chap. VII "Diviseurs," Hermann, Paris, 1966.

برای حالت میدانهای اعداد، رک:

5. Hardy-Wright, An introduction to the theory of numbers, Clarendon, Oxford, 1960

و نیز جدولهای موجود در

6. Borovič-Safarevič, Théorie des nombres, Gauthier-Villars, Paris, 1966. (German and English translations also available.)

بیشتر نتایج به‌دست آمده دربارهٔ حلقه‌های تجزیه‌ای تا سال ۱۹۶۴ در مراجع [۱]، [۲]، [۳] آمده‌اند. ولی برای راحتی خواننده، مراجع دیگری نیز ذکر می‌کنیم:

7. P. Samuel, On unique factorization domains, Ill. J. Math., 5 (1961) 1-17.

8. ———, Sur les anneaux factoriels, Bull. SMF, 89 (1961) 155-173.

9. ———, Classes de diviseurs et dérivées logarithmiques, Topology, 3, Supp. 1 (1964) 81-96.

10. ———, Modules réflexifs et anneaux factoriels, In Colloque International de Clermont-Ferrand, ed. CNRS, Paris, 1965.

11. P. Samuel, Sur les séries formelles restreintes, C.R. Acad. Sci., Paris, 1962.

حلقهٔ رویهٔ $x^۲ + y^۳ + z^۵ = ۰$ در منبع زیر بررسی شده است:

12. F. Klein, Lectures on the icosahedron, Dover, NewYork, 1956, Chap. 2, Sections 12 and 13.

13. E. Brieskorn, Local rings which are UFD's, (preprint, MIT, Oct. 1966).

و نیز در مقالات G. Scheja (Math. Ann., 1965) و D. Mumford (Publ. I. H. E. S., 9, 1961).

نخستین مثال از یک حلقهٔ موضعی کامل A که به‌ازای آن $A[[t]]$ تجزیه‌ای نیست در مرجع زیر آمده است:

14. P. Salmon, Sulla non-factorialita..., Rend. Lincei, June 1966.

برای مطالعهٔ بحث کاملتری دربارهٔ این مثال، رک:

15. N. Zinn-Justin, Dérivations des corps et anneaux de caractéristique p, (Thèse Paris 1967); in print in Mémoires Soc. Math. France, 1967.

برای «پایین‌بر کاملاً تفکیک‌ناپذیر»، رک:

16. N. Hallier, Utilisation des groupes de cohomologie dans la théorie de la descente p radicielle, C.R. Acad. Sci. Paris, 261 (1965) 3922-3924.

و نیز در [۱۵]. (Hallier نام دوشیزگی خانم Zinn-Justin است).

برای دیدن مثالهایی از «پایین‌بر گالوایی» رک:

17. M. J. Dumas, Sous anneaux d'invariants d'anneaux de polynômes, C.R. Acad. Sci. Paris, 260 (1965) 5655-5658.

18. M. J. Bertin, Sous groupes cycliques d'ordre p^n ..., C.R. Acad. Sci. Paris, April 1967.

(Dumas نام دوشیزگی خانم Bertin است).

اثباتی از قضیهٔ گروتندیک دربارهٔ تجزیه‌ای بودنِ بعضی مقطعهای کامل در مرجع زیر آمده است:

19. A. Grothendieck, Séminaire de Géometrie Algébrique 1961-1962, exposé XI, mimeographed by the Institut des Hautes Etudes Scientifiques, 35 route de Chartres, 92-Bures sur Yvette. France.

* * * * * *

• Pierre Samuel, "Unique factorization", Amer. Math. Monthly, (9) 75 (1968) 945-952.

1. completion 2. G. Scheja 3. E. Brieskorn