فرهنگ و اندیشهٔ ریاضی
شماره ۴۸ (پاییز ۱۳۹۰) صص. ۴۷ تا ۵۹

قضیهٔ اصلی حساب و یکتایی تجزیه

عبدعلی کوچک‌پور و منصور معتمدی

چکیده

مفهوم یکتایی تجزیه در جبر، ریشه در قضیهٔ اصلی حساب و نظریهٔ جبری اعداد دارد. هدف این نوشتار، بررسی مفهوم تجزیه و یکتایی آن است. در بخش اول، پیشینهٔ تاریخی قضیهٔ اصلی حساب مورد بررسی قرار می‌گیرد. در بخش دوم، تجزیه در نیم‌گروه‌ها را با ذکر چند مثال مورد توجه قرار می‌دهیم. هدف بخش سوم، معرفی حوزه‌های نیم‌عاملی و مفهوم کشسانی[1] [۱] در حوزه‌های صحیح است. در بخش چهارم، ناورداهایی که دوری از اول بودن و دوری از یکتایی تجزیه را اندازه می‌گیرند، معرفی و به اختصار مطالعه می‌شوند.

۱. پیشینهٔ تاریخی

بیان قضیهٔ اصلی حساب چنین است که **هر عدد طبیعی بزرگ‌تر از ۱، صرف نظر از جای عوامل، به‌صورت یکتا به حاصل‌ضرب اعداد اول تجزیه می‌شود.** پیشینهٔ تاریخی قضیهٔ اصلی حساب به‌طور دقیق روشن نیست و در کتاب اصول اقلیدس به‌صورت فوق بیان نشده است. با این حال، اقلیدس نقش تعیین‌کننده‌ای در پیدایش آن دارد. به‌طور مشخص، فصل‌های هفت و نه کتاب اصول شامل گزاره‌هایی راجع به قضیهٔ اصلی حساب است [۱]. کمال‌الدین فارسی، متوفی در ۱۳۲۰ میلادی در کتاب تذکرة‌الاحباب فی بیان‌الانتحاب بخش وجودی تجزیهٔ اعداد طبیعی به اعداد اول را اثبات و زمینه را برای اثبات یکتایی آن فراهم می‌کند. در گزارهٔ ۹ مندرج در این کتاب، تمام

1) Elasticity

مقسوم‌علیه‌های یک عدد طبیعی مشخص می‌شود. این اولین اثبات شناخته شده از وجود تجزیه است [۲، ٦، ۱۰]. پرسته[1] [۲] ریاضی‌دان فرانسوی سدهٔ هفده میلادی هم اثباتی شبیه اثبات کمال‌الدین فارسی ارائه داده است [۱۰]. اویلر بخش وجودی قضیهٔ اصلی حساب را دانسته فرض کرده و نتایجی بسیار نزدیک به نتایج کمال‌الدین فارسی و پرسته به‌دست آورده است. لژاندر بخش وجودی قضیهٔ اصلی را اثبات کرده است، اما بیان او صریح نیست. اولین اثبات وجود و یکتایی قضیهٔ اصلی حساب توسط گاوس در اثر ماندگار وی با نام «پژوهش‌های حسابی[2]» [۳] آمده است. پس از گاوس دیگران نیز اثبات‌های گوناگونی از آن ارائه داده‌اند.

می‌توان از اصل خوش ترتیبی برای اثبات وجود تجزیه استفاده کرد به این ترتیب که فرض کنیم n کوچک‌ترین عدد طبیعی است که تجزیه‌ای برای آن وجود ندارد. پس n اول نیست و اعداد طبیعی n_1 و n_2 وجود دارند به‌طوری که $n = n_1 n_2$، $1 < n_1 < n$ و $1 < n_2 < n$. بنا به تعریفِ n، n_1 و n_2 حاصل‌ضرب اعداد اول هستند و از این‌رو n نیز حاصل‌ضرب اعداد اول خواهد شد که تناقض است. برای اثبات یکتایی تجزیه، به‌طور معمول از لم زیر که به لم اقلیدس معروف و در بخش نظریهٔ اعداد کتاب اصول اقلیدس مندرج است، استفاده می‌شود.

لم اقلیدس. اگر عدد اول p حاصل‌ضرب ab را بشمرد، آن‌گاه p، a یا b را می‌شمرد.

در این‌جا اثباتی برای یکتایی تجزیه بیان می‌کنیم که در آن از لم اقلیدس استفاده نمی‌شود [۱۳]. بنابر اصل خوش ترتیبی، فرض کنیم k کوچکترین عدد طبیعی باشد که دارای دو تجزیه متفاوت است، یعنی

$$k = p_1 p_2 \cdots p_n = q_1 q_2 \cdots q_m$$

پس هیچ یک از p_i ها نمی‌توانند مساوی یکی از q_j ها باشند و همچنین k نمی‌تواند اول باشد. پس $m, n \geq 2$ و از این‌رو به‌ازای یک i، $p_i^2 \leq k$ و به‌ازای یک j، $q_j^2 \leq k$. فرض کنیم $i = j = 1$. در این صورت $p_1 q_1 \leq k$ و چون $p_1 \neq q_1$، داریم $p_1 q_1 < k$. از این‌جا نتیجه می‌شود که $k - p_1 q_1$ دارای تجزیهٔ یکتاست. دو عدد اول p_1 و q_1 عدد $k - p_1 q_1$ را می‌شمرند و بنابراین باید در تجزیهٔ یکتای آن وجود داشته باشند. پس به‌ازای یک عدد طبیعی b داریم

---

1) Jean Prestet 2) Disquisitiones arithmeticae

$$k - p_1 q_1 = p_1 q_1 b$$

و

$$k = p_1 q_1 (1 + b) = p_1 \cdots p_n$$

اینک با حذف p_1 از طرفین تساوی و دریافت دو تجزیهٔ متمایز برای k/p_1، تناقض لازم به‌دست می آید.

اثبات‌هایی که برای بخش یکتایی قضیهٔ اصلی حساب ارائه می‌شوند، مشکل‌تر از اثبات وجودی آن هستند. در اثبات وجود تجزیه، به‌طور مستقیم از تعریف عدد اول و اصل استقرای ریاضی یا هم‌ارز آن، اصل خوش ترتیبی، استفاده می‌شود. اما در اثبات بخش یکتایی، فقط از اعمال ضرب و تقسیم استفاده نمی‌شود؛ گویا جایی باید از جمع و تفریق نیز استفاده کرد.

۲. تجزیه در نیم‌گروه‌ها

در ادامهٔ مقاله، مقصود از یک نیم‌گروه، نیم‌گروهی است تعویض‌پذیر با عضو واحد. عضو واحد نیم‌گروه H را با $1_H = 1$ نشان می‌دهیم. رابطهٔ هم‌ارزی $\sim$ را روی H،هم‌نهشتی می‌نامیم هرگاه برای هر $a, b, c \in H$، $a \sim b$ ایجاب کند که $ac \sim bc$. گیریم $H^\times$ گروه عضوهای وارون‌پذیر H را نشان دهد. دو عضو $a, b \in H$ وابسته نامیده می‌شوند و می‌نویسیم $a \cong b$ اگر $u \in H^\times$ وجود داشته باشد که $a = ub$. این یک رابطهٔ هم‌نهشتی روی H است و برای هر $a \in H$، ردهٔ هم‌ارزی a، برابر است با $aH^\times$. نیم‌گروه $H_{red} = H/\cong$ را نیم‌گروه تحویل‌یافتهٔ H می‌نامیم. نیم‌گروه H را تحویل‌یافته می‌نامیم هرگاه $H^\times = \{1\}$ که در این صورت $H = H_{red}$. عضو $a \in H$ را حذف‌پذیر می‌نامیم اگر برای هر $b, c \in H$، از $ab = ac$ بتوان نتیجه گرفت $b = c$. نیم‌گروه H را یک تکواره می‌نامیم هرگاه هر عضو آن حذف‌پذیر باشد.

$A \subseteq H$ را s ـ ایدالِ[1] H می‌نامیم هرگاه $AH = A$. به‌موجب تعریف، $\emptyset$ و H، s ـ ایدال‌های H هستند و H یک گروه است اگر و تنها $\emptyset$ و H تنها s ـ ایدال‌های H باشند. برای $a \in H$، aH ایدال اصلی تولید شده با a نامیده می‌شود. اگر A یک s ـ ایدال H باشد، A را اول می‌نامیم هرگاه $H \setminus A$ زیرنیم‌گروه H باشد. همچنین نیم‌گروه تولید شده توسط $X \subseteq H$ را با $[X]$ نشان می‌دهیم.

تعریف ۱.۲. ۱) عضو $a \in H$ را تحویل‌ناپذیر یا اتم می‌نامیم هرگاه $u \notin H^\times$ و برای هر

۱) حرف s به‌خاطر حرف اول واژهٔ Semigroup انتخاب شده است.

$u = ab$ ،$a, b \in H$ ایجاب کند که $a \in H^\times$ یا $b \in H^\times$. مجموعهٔ تمام عضوهای تحویل‌ناپذیر H را با $A(H)$ نشان می‌دهیم.

۲) تکوارهٔ H را اتمی می‌نامیم اگر هر عضو وارون‌ناپذیر آن حاصل‌ضرب تعداد متناهی از عضوهای تحویل‌ناپذیر (اتم‌های H) باشد، یعنی $H = [A(H) \cup H^\times]$.

۳) $p \in H$ را عضو اول یااول می‌نامیم هرگاه وارون‌پذیر نباشد و برای هر $a, b \in H$ ،$p \mid ab$ ایجاب کند که $p \mid a$ یا $p \mid b$.

۴) تکوارهٔ H را عاملی می‌نامیم در صورتی که هر عضو وارون‌ناپذیر آن حاصل ضرب تعداد متناهی عضوهای اول H باشد.

با توجه به تعریف بالا، می‌توان گفت که حوزهٔ صحیح R اتمی (عاملی) است اگر تکوارهٔ متشکل از عضوهای ناصفر آن، اتمی (عاملی) باشد. بدیهی است که این تعریف با تعریف متداول در کتاب‌های جبر مطابقت دارد، زیرا مجموعهٔ عضوهای ناصفر در هر حوزهٔ صحیح با عمل ضرب، یک تکواره است.

پیش از ارائهٔ مثال، به بیان دو قضیه می‌پردازیم که یک تعبیر ایدالی از عضوهای تحویل‌ناپذیر یا اتم‌ها و عضوهای اول به‌دست می‌دهند.

قضیه ۲.۲ فرض کنیم H یک تکواره باشد و $u \in H$.

۱) u عضو تحویل‌ناپذیر H است اگر و تنها اگر ایدال اصلی uH نسبت به رابطهٔ شمول در مجموعهٔ ایدال‌های اصلی H به‌جز H، ماکسیمال باشد؛

۲) عضو u اول است اگر و تنها uH یک s ـ ایدال اولِ H باشد؛

۳) هر عضو اول H یک عضو تحویل‌ناپذیر H است.

اثبات: ۱) فرض کنیم u یک عضو تحویل‌ناپذیر H و $a \in H \setminus H^\times$ چنان باشد که $uH \subseteq aH$. در این صورت به‌ازای یک $b \in H$، $u = ab$ و چون u تحویل‌ناپذیر است، نتیجه می‌گیریم $b \in H^\times$ و بنابراین $aH = uH$. اینک فرض کنیم uH در مجموعهٔ

$$\{aH | a \in H, aH \neq H\}$$

ماکسیمال است و $a, b \in H$ چنان‌اند که $u = ab$. اگر $a \in H^\times$ داریم $uH \subseteq aH \subseteq H$ و بنابراین $uH = aH$ که از آن نتیجه می‌شود $b \in H^\times$. از این رو u تحویل‌ناپذیر است.

۲) به‌موجب تعریف، pH یک s ـ ایدال اول است اگر و تنها برای هر $a, b \in H \setminus pH$ داشته باشیم $ab \in H \setminus pH$. به طور معادل برای هر $a, b \in H$ اگر $p \mid ab$، آن‌گاه $p \mid a$ یا $p \mid b$. بنابراین pH یک s ـ ایدال اول است اگر و تنها اگر p عضو اول باشد.

۳) فرض کنیم $p \in H$ یک عضو اول و $a, b \in H$ چنان باشند که $p = ab$. در این صورت $p \mid ab$ و از این‌رو $p \mid a$ یا $p \mid b$. بنابراین $p \cong a$ یا $p \cong b$. پس $a \in H^\times$ یا $b \in H^\times$ که نشان می‌دهد p عضو تحویل‌ناپذیر H است.

تعریف ۳.۲ گوییم H در شرط زنجیری فزاینده برای ایدال‌های اصلی صدق می‌کند هرگاه هر دنبالهٔ افزایشیِ ایدال‌های اصلی H ایستا باشد بدین معنی که اگر $\{a_i\}_{i \geq 0}$ دنباله‌ای در H باشد که

$$a_0 H \subseteq a_1 H \subseteq a_2 H \subseteq \cdots$$

آن‌گاه $m \in \{0, 1, 2, \cdots\}$ وجود داشته باشد که برای هر $n \geq m$، $a_n H = a_m H$.

قضیه ۴.۲ اگر H در شرط زنجیری فزاینده برای ایدال‌های اصلی صدق کند، آن‌گاه H اتمی است.

اثبات: فرض کنیم H اتمی نباشد. قرار می‌دهیم

$$\Omega = \{a \in H \setminus H^\times : \quad a \text{ حاصل‌ضرب تعداد متناهی اتم نباشد}\}$$

در این صورت Ω تهی نیست و اگر $a \in \Omega$، آن‌گاه $a = bc$ که $b, c \in H \setminus H^\times$ و $b \in \Omega$ یا $c \in \Omega$. از این‌رو برای هر $a \in \Omega$ یک $a' \in \Omega$ وجود دارد که $aH \subsetneq a'H$. با شروع از $a_0 \in \Omega$، دنبالهٔ $\{a_n\}_{n \geq 0}$ را در Ω به‌طور بازگشتی با $a_{n+1} = a'_n$ تعریف می‌کنیم تا این‌که دنبالهٔ افزایشیِ ایدال‌های

$$a_0 H \subsetneq a_1 H \subsetneq \cdots$$

که ایستا نیست به‌دست آید.

توجه می‌کنیم که اثبات فوق در واقع همان اثباتِ بخش وجودی قضیهٔ اصلی حساب است.

به‌موجب قضیهٔ ۴.۲، هر حوزهٔ صحیح که در شرایط زنجیری افزایشی برای ایدال‌های اصلی صدق کند و به‌ویژه هر حوزهٔ نویتری یک حوزهٔ اتمی است. به‌علاوه، حوزهٔ صحیح غیرنویتری دیگری وجود دارد که فاقد اتم است (صفحهٔ ۵۷ در [۷] را ببینید). همچنین گرمس[1] [۱۵] با ذکر یک مثال

1) A. Ggrams

نشان داده است که لازم نیست یک حوزهٔ اتمی در شرط فزاینده برای ایدال‌های اصلی صدق کند.

مثال ۵.۲ حلقهٔ $\bar{\mathbb{Z}}$ متشکل از تمام اعداد صحیح جبری در $\mathbb{C}$ اتمی نیست. در واقع اگر $u \in \bar{\mathbb{Z}} \setminus \bar{\mathbb{Z}}^{\times}$، $u \neq 0$، آن‌گاه $\sqrt{u} \in \bar{\mathbb{Z}} \setminus \bar{\mathbb{Z}}^{\times}$ و $u = (\sqrt{u})^2$. بنابراین $\bar{\mathbb{Z}}$ دارای عضو تحویل‌ناپذیر نیست و چون $\bar{\mathbb{Z}}$ یک هیأت نیست، نمی‌تواند اتمی باشد.

مثال ۶.۲ تکوارهٔ $H = 1 + 4\mathbb{N}_0$ (منسوب به هیلبرت) مثالی است که اغلب در متون درسی برای لزوم اثبات یکتایی از آن استفاده می‌شود. بدیهی است که عضوهای تحویل‌ناپذیر این تکواره عبارتند از اعداد اول به‌شکل $p \equiv 1 \pmod 4$ و qq' هایی که در شرط $q \equiv q' \equiv -1 \pmod 4$ صدق می‌کنند. تحویل‌پذیرهایی از نوع دوم، اول نیستند، زیرا $q^2, q'^2 \in H$ و $qq' | q^2 q'^2$، اما $qq' \nmid q^2$ و $qq' \nmid q'^2$. به لحاظ نبود یکتایی تجزیه، توجه می‌کنیم که

$$693 = 9 \times 77 = 21 \times 33.$$

و این که هر یک از اعداد ۹، ۷۷، ۲۱ و ۳۳ در H تحویل‌ناپذیرند.

مثال ۷.۲ فرض می‌کنیم F یک هیأت باشد. قرار می‌دهیم

$$R = \{a_0 + a_1 x^2 + \cdots + a_n x^n | a_i \in F\}.$$

R یک حوزهٔ صحیح است. به‌سادگی دیده می‌شود که x^2 در R تحویل‌ناپذیر است، اما عضو اول R نیست، زیرا $x^6 = x^3.x^3$ و از این قرار $x^2 | x^3.x^3$، اما رابطهٔ بخش‌پذیری $x^2 | x^3$ در R برقرار نیست.

در قضیهٔ ۲.۲ دیدیم که هر عضو اول در یک تکواره، تحویل‌ناپذیر است. مثال فوق نشان می‌دهد که یک عضو تحویل‌ناپذیر می‌تواند اول نباشد. اینک به قضیهٔ زیر توجه می‌کنیم.

قضیه ۸.۲ فرض کنیم R یک حوزهٔ صحیح باشد. در این صورت دو بیان زیر هم‌ارزند:

۱) R یک حوزهٔ تجزیهٔ یکتاست؛

۲) هر عضو ناصفر و وارون‌ناپذیر، تحویل‌ناپذیر است اگر و تنها اگر اول باشد.

اثبات: [۱۴] قضیهٔ (۱.۱.۱۵) را ببینید.

۳. حوزه‌های نیم‌عاملی[1] و کشسانی

یادآوری می‌کنیم که حوزهٔ اتمی R را یک حوزهٔ تجزیه یکتا می‌نامیم هرگاه، از

1) Half factorial domain

$$\alpha_1\alpha_2\cdots\alpha_m = \beta_1\beta_2\cdots\beta_n$$

که در آن، α_iها و β_iها تحویل‌ناپذیرند بتوان نتیجه گرفت $n = m$ و جایگشتی مانند σ روی مجموعهٔ $\{1, 2, \ldots, n\}$ وجود دارد که برای هر i، α_i و $\beta_{\sigma(i)}$ وابسته‌اند.

اینک حوزهٔ اتمی R را یک حوزهٔ نیم‌عاملی می‌نامیم هرگاه اولین نتیجهٔ فوق برقرار باشد. قضیهٔ زیر نشان می‌دهد که این تعریف ریشه در نظریهٔ جبری اعداد دارد. در این‌جا فرض می‌کنیم که خواننده با مفهوم عدد رده‌ای آشناست. از جمله R یک حوزهٔ تجزیهٔ یکتاست اگر و تنها اگر عدد رده‌ای آن برابر ۱ باشد. در این مورد می‌توانید به هر کتاب معتبر نظریهٔ جبری اعداد مراجعه کنید.

قضیه ۱.۳ (کارلیتز[1]) [۱۲] فرض کنیم R حلقه اعداد صحیح در یک توسیع متناهی هیات K از اعداد گویا باشد. R یک حوزهٔ نیم‌عاملی است اگر و تنها اگر عدد رده‌ای آن برابر ۱ یا ۲ باشد.
اثبات [۱۲] را ببینید.

مثال ۲.۳ (اندرسون[2]، اندرسون[3]، ظفرالله[4]) حلقه‌های $\mathbb{R} + X\mathbb{C}[X]$ و $\mathbb{Q} + X\mathbb{R}[X]$ هر دو حوزهٔ نیم‌عاملی هستند. هیچ کدام حوزهٔ تجزیهٔ یکتا نیستند، زیرا $X^2 = XX = (iX)(-iX)$ و $x^2 = (\sqrt{2}x)(\frac{1}{\sqrt{2}}x)$ به‌ترتیب تجزیه‌های نایکتا در هر حوزه هستند. فرض کنیم عضو x یک عضو ناصفر و وارون‌ناپذیر حوزهٔ صحیح R باشد و $r = x_1x_2\cdots x_m$ که در آن x_i ها تحویل‌ناپذیرند. در این صورت، m را طول این تجزیه می‌نامیم. طول کوچک‌ترین تجزیهٔ x را با $\ell_R(x)$ و کران بالای این طول‌ها را با $L_R(x)$ نشان می‌دهیم. این کران بالا می‌تواند متناهی باشد که در این صورت همان طول بزرگترین تجزیهٔ x است. این کران بالا می‌تواند نامتناهی باشد. بدیهی است که $L_R(x) = \ell_R(x) = 1$ اگر و تنها اگر x تحویل‌ناپذیر باشد. اگر x تحویل‌ناپذیر نباشد، آن‌گاه $L_R(x) \geq \ell_R(x) \geq 2$. چنانچه x وارون‌پذیر باشد، قرار می‌دهیم $L_R(x) = 0$ و اگر $x = 0$، $L_R(x)$ را برابر ∞ تعریف می‌کنیم. همچنین روشن است که

$$L_R(xy) \geq L_R(x) + L_R(y)$$

اینک قرار می‌دهیم $\rho(x) = L_R(x)/\ell_R(x)$ (که می‌تواند نامتناهی باشد) و کشسانی R که آن را با $\rho(R)$ نشان می‌دهیم برابر کوچک‌ترین کران بالای $\rho(x)$ ها تعریف می‌کنیم، یعنی

$$\rho(R) = \sup\{\frac{m}{n} | x_1x_2\cdots x_m = y_1y_2\cdots y_n\}$$

---

1) L. Carlitz 2) D. D. Anderson 3) D. F. Anderson 4) M. Zafrullah

که در آن x_i ها و y_i ها عضوهای تحویل‌ناپذیر R هستند. به‌روشنی $\infty \leq \rho(R) \leq ۱$ و $\rho(R) = ۱$ اگر و تنها اگر R یک حوزهٔ نیم‌عاملی باشد. گوییم حوزهٔ صحیح R حوزهٔ تجزیهٔ کراندار است هرگاه برای هر عضو ناصفر و وارون‌ناپذیر $x \in R$، $L_R(x) < \infty$ یا به عبارتی $\rho(x) < \infty$. در ادامه، مثالی ارائه می‌دهیم که نشان می‌دهد کشسانی یک حوزهٔ صحیح می‌تواند نامتناهی باشد. فرض کنیم R یک حوزهٔ صحیح و F هیأت کسرهای آن باشد. به‌سادگی دیده می‌شود که

$$Int(R) = \{f \in F[x] : f(R) \subseteq R\}$$

یک زیرحلقهٔ F است و در واقع

$$R \subseteq Int(R) \subseteq F.$$

این حلقه را حلقهٔ چندجمله‌ای‌های صحیح ـ مقدار R می‌نامیم. اگر $R = \mathbb{Z}$، حالت کلاسیک به‌دست می‌آید. در واقع $Int(\mathbb{Z})$ یک $\mathbb{Z}$– مدول آزاد با پایهٔ

$$۱, x, \frac{x(x-۱)}{۲!}, \frac{x(x-۱)(x-۲)}{۳!}, \ldots$$

است.

برای مطالعهٔ خواص تجزیه‌ای $Int(R)$ ابتدا باید عضوهای وارون‌پذیر و تحویل‌ناپذیر R مشخص شوند. در این مورد، لم زیر به‌راحتی اثبات می‌شود.

لم ۳.۳ فرض کنیم R یک حوزهٔ صحیح باشد.

۱) عضوهای وارون‌پذیر $Int(R)$ همان عضوهای وارون‌پذیر R هستند؛

۲) عضو $a \in R$ تحویل‌ناپذیر است اگر و تنها اگر در $Int(R)$ تحویل‌ناپذیر باشد.

قضیه ۴.۳ هریک از چندجمله‌ای‌های

$$x, \frac{x(x-۱)}{۲}, \ldots, \binom{x}{n}, \ldots$$

در $Int(\mathbb{Z})$ تحویل‌ناپذیرند.

اثبات: مرجع [۱۱] صفحه ۱۳۰ را ملاحظه کنید.

قضیه ۵.۳ حوزهٔ صحیح $Int(\mathbb{Z})$ حوزهٔ تجزیهٔ کراندار است و علاوه بر آن، اگر $f \in Int(\mathbb{Z})$ و $a \in \mathbb{Z}$، داریم $L_{Int(\mathbb{Z})}(f) \leq deg f + L_{\mathbb{Z}}(f(a))$.

اثبات: فرض کنیم

$$f = p_1 p_2 \cdots p_r g_1 g_2 \cdots g_s$$

که p_i ها اعداد اول و g_i ها چندجمله‌ای‌های تحویل‌ناپذیر در $Int(\mathbb{Z})$ باشند. آشکار است که $s \leq deg f$. اگر $f(a) = 0$، بنابر قرارداد، $L_{Int(\mathbb{Z})}(f(a)) = \infty$ و نامساوی برقرار است. اگر a ریشهٔ f نباشد (چنین عضوی در $\mathbb{Z}$ وجود دارد، زیرا $\mathbb{Z}$ نامتناهی است)، $f(a)$ بر حاصل‌ضرب $p_1 p_2 \cdots p_r$ بخش‌پذیر است و از این‌رو $r \leq L_{\mathbb{Z}}(f(a))$.

اگر n یک عدد صحیح مثبت باشد، $\phi(R, n)$ تعداد طول‌های ممکن تجزیه‌هایی است که دارای تجزیه‌ای به طول n نیز هستند. به عبارت دیگر $\phi(R, n)$ عدد اصلی مجموعهٔ

$$\{m \mid x_1 x_2 \cdots x_m = y_1 y_2 \cdots y_n \quad \text{تحویل‌ناپذیرند در } R \text{ و } y_i \text{ها } x_i\text{ها}\}$$

می‌باشد. به‌روشنی $\phi(R, 1) = 1$ و $\phi(R, n+1) \geq \phi(R, n)$ و حوزهٔ صحیح R یک حوزهٔ نیم‌تجزیه است اگر و تنها اگر برای هر n، $\phi(R, n) = 1$.

قضیهٔ ۶.۳ کشسانی حلقهٔ چندجمله‌ای‌های صحیح ـ مقدار، $Int(\mathbb{Z})$، نامتناهی است. در واقع

$$\phi(Int(\mathbb{Z}), 2) = \infty.$$

اثبات: برای هر عدد صحیح $n \geq 2$ داریم

$$n\binom{X}{n} = (X - n + 1)\binom{X}{n-1}$$

با توجه به قضیهٔ ۵.۳، در سمت راست دو عامل تحویل‌ناپذیر وجود دارد، حال آن‌که در سمت چپ می‌توان n را چنان انتخاب کرد که تعداد دلخواهی عامل اول داشته باشد.

۴. دوری از اول بودن

فرض کنیم R یک حوزهٔ صحیح، $R = R\backslash\{0\}$ و $U(R)$ گروه عناصر وارون‌پذیر R باشد. در این بخش، دو ناوردای $\omega(R, x)$ و $\omega(R)$ را که به‌ترتیب دوری $x \in R$ را از اول بودن و دوری R را از حوزهٔ تجزیهٔ یکتا بودن اندازه می‌گیرد، معرفی می‌کنیم.

تعریف ۱.۴ فرض کنیم R یک حوزهٔ صحیح باشد.

۱) برای $x \in R^*\backslash U(R)$، $\omega(R,x)$ کوچک‌ترین عدد صحیح m است که اگر x_1، ... ، x_n عناصر R باشند و $x \mid x_1 \cdots x_n$، آن‌گاه به‌ازای یک $t \leq m$ و یک زیرمجموعهٔ $\{1,\ldots,n\}$ مانند $\{i_1,\ldots i_t\}$ داشته باشیم $x \mid x_{i_1} \ldots x_{i_t}$. اگر چنین عدد صحیحی وجود نداشته باشد، قرار می‌دهیم $\omega(R,x) = \infty$.

۲) اگر $x \in U(R)$، آن‌گاه $\omega(R,x) = 0$.

۳) $\omega(R) = \sup\{\omega(R,x) \mid$ {عضو x در R تحویل‌ناپذیر است $\}$.

۴) اگر R یک هیأت باشد، آن‌گاه $\omega(R) = 0$.

۵) اگر R هیأت نباشد و عضو تحویل‌ناپذیر هم نداشته باشد، $\omega(R) = \infty$.

نتایج زیر بی‌درنگ از تعریف بالا به‌دست می آیند.

نتیجه ۲.۴ اگر $x \in R^*\backslash U(R)$ ، آن‌گاه $1 < \omega(R,x) = m < \infty$.

نتیجه ۳.۴ اگر $\{x_1,\ldots,x_n\} \subset R$، $n \geq m$ و $x \mid x_1 \cdots x_n$، آن‌گاه به‌ازای یک زیرمجموعهٔ $\{i_1,\ldots,i_m\} \subseteq \{1,\ldots,n\}$، $x \mid x_{i_1} \cdots x_{i_m}$.

نتیجه ۴.۴ عناصر x_1، ... ، x_m در R وجود دارند به‌طوری که $x \mid x_1 \cdots x_m$ اما x هیچ زیر حاصل‌ضرب x_i ها را نمی‌شمرد.

نتیجه ۵.۴ $\omega(R,x) = 1$ اگر و تنها اگر x در R اول باشد.

نتیجه ٦.۴ اگر x_1، ... ، x_n در R اول باشند، آنگاه $\omega(R,x_1,\ldots,x_n) = n$.

نتیجه ۷.۴ اگر حوزهٔ اتمی R هیات نباشد، آن‌گاه R یک حوزهٔ تجزیهٔ یکتاست اگر و تنها اگر $\omega(R) = 1$.

قضیهٔ زیر نشان می‌دهد که عناصر x_1، ... ، x_n در تعریف $\omega(R,x)$ را می‌توان عناصر تحویل‌ناپذیر اختیار کرد.

قضیه ۸.۴ فرض کنیم R یک حوزهٔ اتمی باشد و $x \in R^*\backslash U(R)$. در این صورت بیان‌های زیر هم‌ارزند:

۱) $\omega(R,x) = m < \infty$؛

۲) m کوچک‌ترین عدد طبیعی است که اگر x_1، ... ، x_n عناصر تحویل‌ناپذیر R باشند و $x \mid x_1 \cdots x_n$، آن‌گاه به‌ازای یک $t \leq m$ و یک زیرمجموعهٔ $\{1,\ldots,n\}$ مانند $\{i_1,\ldots,i_t\}$،

$x \mid x_{i_1} \cdots x_{i_t}$؛

۳) اگر $n \geq m$ و x_1، ... ، x_n در R تحویل‌ناپذیر باشند، آن‌گاه به‌ازای یک زیرمجموعهٔ $\{1, \ldots, n\}$ مانند $\{i_1, \ldots, i_m\}$، داریم $x \mid x_{i_1} \cdots x_{i_m}$ اما x هیچ زیرحاصل‌ضرب x_{i_k} ها را نمی‌شمرد.

اثبات: [۹] را ببینید.

قضیه ۹.۴ فرض کنیم R یک حوزهٔ اتمی باشد، اگر $\omega(R) \leq ۲$، آن‌گاه R یک حوزهٔ نیم‌عاملی است.

اثبات: اگر $\omega(R) \leq ۱$، آن‌گاه R یک حوزهٔ تجزیهٔ یکتاست. پس فرض کنیم $\omega(R) = ۲$. اگر R یک حوزهٔ نیم‌عاملی نباشد، تجزیه‌ای مانند $x_1 \cdots x_n = y_1 \cdots y_m$ که در آن، x_i ها و y_j ها عناصر تحویل‌ناپذیر R هستند وجود دارد و $۲ \leq n < m$. فرض کنیم n کوچکترین عدد طبیعی با این ویژگی باشد. از آن‌جا که $\omega(D) = ۲$، می‌توان فرض کرد $x_1 \mid y_1 y_2$. پس $y_1 y_2 = x_1 z_1 \cdots z_k$ که در آن z_i ها تحویل‌ناپذیرند و $k \geq ۱$. بنابراین $x_2 \cdots x_n = z_1 \cdots z_k y_3 \cdots y_m$ که در آن $n - ۱ < k + (m - ۲)$. توجه می‌کنیم که تعداد عامل‌های تحویل‌ناپذیر در تجزیهٔ سمت راست برابر است با $k + (m - ۲) \geq m - ۱ \geq n \geq ۲$. پس باید در تجزیهٔ سمت چپ هم $n - ۱ \geq ۲$ عضو تحویل‌ناپذیر وجود داشته باشد. وجود این تجزیهٔ جدید با فرض مینمال بودن n در تناقض است. بنابراین R یک حوزهٔ نیم‌عاملی است.

در قضیهٔ بعد ارتباط بین دو ناوردای $\rho(R)$ و $\omega(R)$ مشخص می‌شود. اثبات آن در [۹] یافت می‌شود.

قضیه ۱۰.۴ فرض کنیم R یک حوزهٔ اتمی باشد که هیأت نیست. در این صورت اولاً $\rho(R) \leq \omega(R)$ و ثانیاً اگر $\rho(R) = \frac{m}{۳}$ و $x_1 \cdots x_n = y_1 y_2$ که x_i ها و y_j های در R تحویل‌ناپذیرند، آن‌گاه $\rho(R) \leq \omega(R)/۲$.

نوشتار خود را با قضیهٔ زیر به پایان می‌بریم.

قضیه ۱۱.۴ فرض کنیم R حلقهٔ اعداد صحیح جبری در یک هیأت جبری اعداد باشد. در این صورت بیان‌های زیر هم‌ارزند:

۱) عدد رده‌ای R برابر ۲ است؛

۲) $\omega(R) = ۲$؛

۳) R یک حوزه نیم‌عاملی است.

مراجع

[۱] ال‌هیث، تامس، اصول اقلیدس سیزده مقاله، ترجمهٔ محمدهادی شفیعی‌ها، مرکز نشر دانشگاهی، چاپ اول ۱۳۸۷.

[۲] قربانی، ابوالقاسم، فارسی‌نامه، احوال و آثار کمال‌الدین فارسی، ریاضی‌دان و نورشناس ایرانی. مؤسسهٔ نشر هما، اسفند ۱۳۳۶.

[۳] معتمدی، منصور، آشنایی با نظریهٔ حلقه‌ها، ویرایش سوم، انتشارات دانشگاه شهید چمران اهواز، ۱۳۸۷.

[4] A. G. Agaragun, & C. R. Fletcher. "al-Farsi and Fundamental Theorem of Arithmatic", *Historica Mathematica*, **21**(1994), 162-173.

[5] A. G. Agaragun, & E. Mehmet Ozkan, "A historical survey of the Fundamental Theorem of Arithmatic", *Historica Mathematica*, **28** (2001), 207-214.

[6] A. G. Agaragun & C. R. Fletcher, "The Fundamental Theorem of Arithmatic dissected", *Mathematical Gazette*, **81**(1997), 53-57

[7] S. Alaca, & K. S. Williams, *Introductory algebraic number theory*, Cambridge University Press, 2004.

[8] D. D. Anderson, & D. F, Anderson and M. Zafrullah, "Factorization in integral domain", *J. Pure. App. Algebra*, **69** (1990), 1-19.

[9] D. F. Anderson & S. Chapman, "How far is an element from being prime?", *Journal of algebra and its applications*, **9**(2010), 1-11.

[10] R. P. Burn, *A pathway into number theory*, second edition, Cambridge University Press, 1997.

[11] P. J. Cahen, & J-L Chabert, *Integer-Valued Polynomials*, Mathematical Survey and Monographs, vol. 48, American Mathematical Society, 1997.

[12] L. Carlitz, "A characterization of algebraic number fields with class number two", *Proc. Am. Math Society*, **11**(1960), 391-392.

[13] H. Davenport, *The higher arithmatic*, Hutchinson House, 1952.

[14] A. Geroldingen, & F. Holter-koch, *Nonunique factorizations, Algebraic, Combiniatorial and Analytic theory*, Chapman, & Hall/CRC, 2006.

[15] A. Grams, "Atomic rings and the ascending chain condition for principal ideals", *Proc. Camb. Philo. Soc.*, **75**(1974), 321-329.

عبدعلی کوچک‌پور koochak_a@scu.ac.ir

منصور معتمدی motamedi_m@scu.ac.ir

دانشگاه شهید چمران اهواز، گروه ریاضی