بررسی تجزیه اعداد تام درجه دوم

پوهنیار سیدنسیم سیاوش

دیپارتمنت الجبر، پوهنځی ریاضیات، پوهنتون کابل، کابل، افغانستان
ایمیل: siawash.sns@gmail.com

چکیده

در این مقاله دومین‌های $\mathbb{Z}[\sqrt{d}]$ مورد بررسی قرارداده شده است. اهمیت این موضوع از لحاظ تاریخی در ایفأ نمودن نقش محوری در ظهور مفهوم ایدیال‌ها می‌باشد. در این‌جا نیز ابتدا به شرح مختصری از تاریخ‌چه‌ی این موضوع پرداخته شده، سپس نشان‌داده شده که هر عنصر در $\mathbb{Z}[\sqrt{d}]$ به‌عوامل تحویل‌ناپذیر قابل تجزیه است که ممکن این تجزیه یکتا نباشد. بعداً با استفاده از این دومین‌ها، نشان‌داده شده است که چگونه مفهوم ایدیال می‌تواند دربازگرداندن یکتایی تجزیه به بعضی از دومین‌های که فاقد این خاصیت هستند، به‌کار رود که هدف اصلی موضوع را تشکیل می‌دهد و در اخیر تعمیم یکتایی تجزیه، یک ایدیال به حاصل ضرب از ایدیال‌های اولیه در دومین‌های مورد نظر کومر بدون ترتیب عوامل، مورد بحث قرار گرفته شده است.

اصطلاحات کلیدی: دومین‌های $\mathbb{Z}[\sqrt{d}]$؛ عددتام مربع-آزاد؛ خاصیت یک‌تایی تجزیه؛ عدد الجبری؛ عددتام درجه دوم

Investigation the Factorization of Quardratic Integers

Jr Teaching Asstt. Sayed Nasim Siawash

Department of Algebra, Faculty of Mathematics, Kabul University, Kabul, Afghanistan
Email: siawash.sns@gmail.com

Abstract

In this paper, $\mathbb{Z}[\sqrt{d}]$ domains are examined. These domains often have no unique factorization property and are therefore a good example of problems that have historically played a pivotal role in the emergence of the concept of ideal. First, a brief history of the subject is given, then the $\mathbb{Z}[\sqrt{d}]$ domains show how the concept of an ideal can be used to "restore" the unique factorization of some domains that lack this property. Also, the unique generalization of the factorization of an ideal by the product of the prime ideals in the Kummer domains without sequence of factors is discussed.

Keywords: $\mathbb{Z}[\sqrt{d}]$ Domains; Square-free Integers; Unique Property of Factorization; Algebraic Number; Quardratic Integers

مقدمه

به سادگی می‌توان جواب‌های تام خلاف صفر زیادی، از جمله ۵،۴،۳ و یا ۱۳،۱۲،۵ برای معادله $x^2 + y^2 = z^2$ یافت. اما تاحال حل‌های تام غیرصفری برای $x^3 + y^3 = z^3$ یا $x^4 + y^4 = z^4$ یافت نشده است. این امر منجر به این حدس شد که وقتی $n > 2$، معادله $x^n + y^n = z^n$ دارای هیچ جواب تام غیرصفری نیست.حدس فوق به "قضیه آخر فرما" معروف شده است وی در اواخر دهه‌ی ۱۶۳۰، در حاشیه‌یی از کتاب حساب دیوفانتی این حدس را نوشته و اضافه کرده بود که "من اثبات چشم‌گیری کشف کرده‌ام که در این حاشیه نمی‌گنجد متأسفانه اثبات فرما تاکنون یافت نشده است و بیشتر ریاضی‌دانان مطمئن نیستند که آیا او اثبات معتبری برای این حدس داشت یا خیر. (این قضیه بعداً در سال ۱۹۹۳ توسط اندریو وایلس اثبات شد). می‌دانیم که هر عدد طبیعی قابل تجزیه به عوامل ضربی تحویل‌ناپذیر (اولیه) بوده و این تجزیه بدون در نظر گرفتن ترتیب عوامل یکتا نیز است (خاصیت یکتایی جزیه در ست اعداد طبیعی). اما آیا در $\mathbb{Z}[\sqrt{d}]$ = $\{r + s\sqrt{d} : r, s \in \mathbb{Z}\}$ خاصیت یکتایی تجزیه صدق می‌کند یا خیر؟ پاسخ طور عموم منفی است. مثلاً در $\mathbb{Z}[\sqrt{-5}]$، $(1 + \sqrt{-5})(1 - \sqrt{-5}) = 2 \times 3.6 =$ حال این سؤال مطرح می‌شود چگونه می‌توان نوع از یکتایی تجزیه را در دومین‌های که خاصیت یکتایی تجزیه در آن صادق نیست، بر قرار نمود؟ در این پرسش کومر به اساس تمرکز روی ایدیال‌ها به‌جای عناصر، پاسخ داد. کومر به جای تجزیه‌ی یک عنصر a به حاصل ضرب عناصر تحویل‌ناپذیر، ایدیال اصلی (a) را به حاصل ضرب از ایده‌آل‌های اولیه تجزیه کرد. کومر اعداد ایدیال را ابداع نموده و ثابت کرد که خاصیت یکتایی تجزیه برای این اعداد ایدیال برقرار است. یعنی موفق شد نشان دهد که در دومین‌های مورد نظر او، به‌جز احتمالاً در ترتیب عوامل، تجزیه یک ایدیال به حاصل ضربی از ایدیال‌های اولیه یکتاست.

کار او به اثبات قضیه فرما برای تقریباً همه اعداد اولیه کوچک‌تر از صد شد. این پیشرفت چشم‌گیر به‌طور عمیقی تقریباً بر همه کارهای که بعدها روی این مسأله انجام گرفت، تأثیر گذاشت. اما کار او حتا اهمیت بیشتری در توسعه‌ی الجبر مدرن داشت، زیرا "اعداد ایدیال" کومر چیزهای هستند که ما امروزه آن‌ها را ایدیال می‌نامیم.

مسأله بر می‌گردد در اوایل قرن نوزدهم که گوس «قانون تقابل دو مربعی» را ثابت کرد. این قانون روش سریع‌تری برای تعیین این که آیا تطابق $x^4 \equiv c \pmod{n}$ دارای جواب است یا خیر را فراهم می‌کند. گرچه صورت این قضیه تنها اعداد تام را در برداشت اما اثبات گوس در دومین

بزرگ‌تر $\mathbb{Z}[i]$ بنا شده بود. او این حقیقت را که $\mathbb{Z}[i]$ یک دومین یکتایی تجزیه است، اثبات کرد و از آن استفاده نمود.

چون اثبات گوس دومین $\mathbb{Z}[i]$ را در برداشت که در آن i جذر چهارم مختلط 1 بود، ریاضی‌دان آلمانی کومر را دراین فکر فرو برد که در اثبات قضایای مشابه تطابق‌های از درجه p ممکن است بتوان از خاصیت یکتایی تجزیه در دومین

$$\mathbb{Z}[\omega] = \{a_0 + a_1\omega + a_2\,\omega^2 + \cdots + a_{p-1}\omega^{p-1};\ a_i \in \mathbb{Z}\}$$

ا ستفاده کرد که در آن $\omega = \cos\left(\frac{2\pi}{p}\right) + i\ \sin\left(\frac{2\pi}{p}\right)$ یک جذر p-ام عدد 1 است. او قادر به توسعه قضایای تقابل از مرتبه بالاتر نشد، زیرا کشف نمود که $\mathbb{Z}[\omega]$ ممکن است یک دومین یکتایی تجزیه نباشد.

در سال ۱۸۴۷، ریاضی‌دان فرانسوی لَمه، با استفاده از این حقیقت که برای هر عدد اولیه مثبت طاق p معدله $x^p + y^p$ می‌تواند به صورت زیر در دامنه $\mathbb{Z}[\omega]$ که در بالا توصیف شد، تجزیه شود:

$$x^p + y^p = (x+y)(x+\omega y)(x+\omega^2 y)\ \ldots\ldots\ldots (x+\omega^{p-1}y).$$

او باورداشت که برهانی از قضیه‌ی آخر فرما وقتی‌که n یک عدد اولیه باشد را ارائه کرده است.

اثبات او براین فرض بود که $\mathbb{Z}[\omega]$ یک دومین یکتایی تجزیه است. اما زمانی‌که از کار کومر خبر شد، به نامعتبری اثباتش پی برد (۵).

اکنون، ابتدا به بررسی تجزیه در دومین $\mathbb{Z}[\sqrt{d}\,]$ می‌پردازیم، این دومین‌ها مشابه دومین‌های کومر هستند. سپس به تجزیه‌ی ایدیال‌ها به ایدیال‌های اولیه به شکل یکتا، تعمیم این موضوع و چگونگی استفاده از آن‌ها در بازگرداندن نوع از یکتایی تجزیه در دومین‌های که خاصیت یکتایی تجزیه را ندارند، خواهیم پرداخت.

تجزیه اعداد تام درجه دوم

قبل از پرداختن به تجزیه اعداد تام درجه دوم بهتر است، چند تعریف مقدماتی مورد نیاز را در نظر گرفته و سپس تجزیه‌پذیری اعداد تام درجه دوم را طور مفصل مورد برسی قرار دهیم.

عدد تام d، مربع – آزاد نامیده می‌شود که اگر دارای هیچ عامل تام به‌صورت c^2 (بجز $(\pm 1^2)$) نباشد. فرض می‌کنیم که عدد تام d، مربع – آزاد است، تابع زیر کلید تجزیه در

$$\mathbb{Z}[\sqrt{d}\,] = \{r + s\sqrt{d}\ : r, s \in \mathbb{Z}\}$$

است. هر عنصر ست فوق یک عدد تام درجه دوم گفته می‌شود.

تعریف: تابع $N: \mathbb{Z}[\sqrt{d}] \to \mathbb{Z}$ با فورمول

$$N(s+t\sqrt{d}) = (s+t\sqrt{d})(s-t\sqrt{d}) = s^2 - dt^2$$

تابع نُرم در $\mathbb{Z}[\sqrt{d}]$ نامیده می‌شود. مثلاً؛ در $\mathbb{Z}[\sqrt{3}]$

$$N(5+2\sqrt{3}) = 5^2 - 3\times 2^2 = 13 \text{ و } N(2-4\sqrt{3}) = 2^2 - 3(-4)^2 = -44$$

توجه کنید که:

وقتی $d<0$، نُرم هر عنصر نامنفی است. مثلاً، در $\mathbb{Z}[\sqrt{-5}]$

$$N(s+t\sqrt{-5}) = s^2 - (-5)t^2 = s^2 + 5t^2 \geq 0$$

تابع نرم، $\mathbb{Z}[i] = \mathbb{Z}[\sqrt{-1}]$ را به یک دومین اقلیدسی تبدیل می‌کند. اما این مطلب در حالت کلی درست نیست، قضیه زیر را در این مورد در نظر می‌گیریم:

قضیه ۱. اگر d یک عدد تام مربع – آزاد باشد، دراین صورت برای هر $a,b \in \mathbb{Z}[\sqrt{d}]$

$$N(a) = 0 \ (1) \text{ اگر وتنها اگر } a = o.$$

$$N(ab) = N(a)N(b) \ (2).$$

ثبوت (۱). اگر $a = s + t\sqrt{d}$، دراین صورت $N(a) = s^2 - dt^2$، لذا $N(a) = 0$ اگر و تنها اگر $s^2 = dt^2$ هر عامل اولیه در تجزیه s^2 و t^2 به تعداد جفت از دفعات تکرار می‌شود. اما عوامل اولیه d تکرار نمی‌شوند زیرا d مربع – آزاد است. بنابراین، اگر p یک عامل اولیه d باشد، باید به تعداد طاق از دفعات در تجزیه dt^2 اتفاق افتد. بنا به یکتایی تجزیه در $\mathbb{Z}$، معادله $s^2 = dt^2$ غیرممکن است مگر این‌که $s = 0 = t$، یعنی $a = 0$.

(۲). فرض کنید $a = r + s\sqrt{d}$ و $b = m + n\sqrt{d}$, اثبات با انجام محاسبه‌ی مستقیم انجام می‌شود.

قضیه ۲. فرض کنید d یک عدد تام مربع – آزاد باشد، دراین‌صورت $u \in \mathbb{Z}[\sqrt{d}]$ واحد است اگر و تنها اگر $N(u) = \pm 1$

ثبوت. اگر u واحد باشد، دراین‌صورت برای بعضی $v \in \mathbb{Z}[\sqrt{d}]$, $uv = 1$ و طبق قضیه ۱ داریم

$$N(u)N(v) = N(uv) = N(1) = 1^2 - d\times 0^2 = 1,$$

چون $N(u)$و $N(v)$اعداد تام اند پس تنها حالات ممکن عبارتند از $N(u) = \pm 1$ و $N(v) = \pm 1$ بر عکس اگر $u = s + t\sqrt{d}$ و $N(u) = \pm 1$ باشد، با در نظر گرفتن $\bar{u} = s - t\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$ طبق تعریف نرم، $u\bar{u} = N(u) = \pm 1$. بنابر این $u(\pm\bar{u}) = 1$ و u واحد است.

بر طبق قضیه ۲ با یافتن همه جواب‌های تام (برای s و t) معادلات $s^2 - dt^2 = \pm 1$، می‌توانیم تمام واحدهای $s + t\sqrt{d}$ در $\mathbb{Z}[\sqrt{d}]$ را تعین کنیم. وقتی $d > 1$، این معادلات دارای تعداد نامتناهی جواب می‌باشند (۲).

وقتی $d = -1$، این معادلات به معادله $s^2 + t^2 = 1$ کاهش می‌یابد. تنها جواب‌های تام عبارتند از $s = \pm 1$، $t = 0$ و $s = 0$، $t = \pm 1$. بنابراین، تنها واحدهای $\mathbb{Z}[i] = \mathbb{Z}[\sqrt{-1}]$ عبارت اند از ± 1 و $\pm i$. اگر $d < -1$، مثلاً $d = -k$ با $k > 1$، دراین‌صورت معادلات به $s^2 + kt^2 = 1$ کاهش می‌یابد. چون $k > 1$، تنها جواب‌های تام عبارت اند از $s = \pm 1$، $t = 0$. بنابراین، نتیجه زیر را داریم.

نتیجه ۱. فرض کنید d یک عدد تام مربع – آزاد باشد. اگر $d > 1$، دراین‌صورت $\mathbb{Z}[\sqrt{d}]$ دارای تعداد نامتناهی واحد است. واحدهای $\mathbb{Z}[\sqrt{-1}]$ عبارتند از ± 1 و $\pm i$. اگر $d < -1$، دراین‌صورت واحدهای $\mathbb{Z}[\sqrt{d}]$ عبارتند از ± 1.

نتیجه ۲. فرض کنید d یک عدد تام مربع – آزاد باشد. اگر $p \in \mathbb{Z}[\sqrt{d}]$ و $N(p)$ یک عدد تام اولیه در $\mathbb{Z}$ باشد، دراین‌صورت p در $\mathbb{Z}[\sqrt{d}]$ تحویل‌ناپذیر است.

ثبوت. چون $N(p)$ اولیه است، $N(p) \neq \pm 1$، لذا طبق قضیه ۲، p در $\mathbb{Z}[\sqrt{d}]$ واحد نیست. اگر $p = ab$ در $\mathbb{Z}[\sqrt{d}]$، دراین‌صورت، $N(p) = N(a)N(b)$ در $\mathbb{Z}$.چون $N(a)$، $N(b)$ و $N(p)$ اعداد تام اند و $N(p)$ اولیه است باید $N(a) = \pm 1$ یا $N(b) = \pm 1$ باشد. بنابراین، طبق قضیه ۲، a یا bواحد است. پس p تحویل‌ناپذیر است.

برای مثال عنصر $1 - i$ در $\mathbb{Z}[i]$ تحویل‌ناپذیر است زیرا $N(1 - \sqrt{-1}) = 2$ به طور مشابه $1 + i$ نیز تحویل‌ناپذیراست بنابر این تجزیه ۲ به عنوان حاصل ضرب از عناصر تحویل‌ناپذیردر $\mathbb{Z}[i]$ به‌صورت $2 = (1 + i)(1 - i)$ می باشد (۵).

عکس نتیجه ۲ غلط است. برای نمونه، در $\mathbb{Z}[\sqrt{-5}]$ نرم $1+\sqrt{-5}$ مساوی ۶ است که اولیه نمی‌باشد. اما $1+\sqrt{-5}$ تحویل‌ناپذیراست.

تجزیه عناصر به‌صورت حاصل ضرب از عوامل تحویل‌ناپذیر در $\mathbb{Z}[\sqrt{d}]$ همواره ممکن است، اما این تجزیه ممکن یکتا نباشد. یعنی $\mathbb{Z}[\sqrt{d}]$ ممکن است یک دومین یکتایی تجزیه نباشد.

قضیه ۳. فرض کنید d یک عدد تام مربع – آزاد باشد. دراین‌صورت هر عنصر خلاف واحد، خلاف صفر در $\mathbb{Z}[\sqrt{d}]$ حاصل ضرب از عناصر تحویل‌ناپذیراست.

ثبوت: فرض کنید S ست همه خلاف واحدهای خلاف صفر در $\mathbb{Z}[\sqrt{d}]$ باشد که حاصل ضرب از عناصر تحویل‌ناپذیر نیستند. نشان می‌دهیم که S خالی است. طور غیرمستقیم فرض کنید که S خلاف خالی باشد؛ دراین‌صورت ست $W=\{|N(t)|: t\in S\}$ ست خلاف خالی از اعداد تام مثبت است. طبق اصل خوش‌ترتیبی W دارای کوچک‌ترین عنصر است. پس عنصر $a\in S$ وجود دارد، طوری‌که برای هر $t\in S$ $|N(a)|\le |N(t)|:$. چون $a\in S$، لذا خود a تحویل‌ناپذیر نیست. بنابراین، خلاف واحدهای $b,c\in\mathbb{Z}[\sqrt{d}]$ وجود دارند. طوری‌که $a=bc$. دراین‌صورت یکی از b،c باید در S باشد (در غیر این صورت a باید حاصل ضرب از عناصر تحویل‌ناپذیر باشد و بنابراین در S نیست)، مثلاً $b\in S$. چون b و c خلاف واحد اند طبق قضیه ۲، $|N(b)|>1$ و $|N(c)|>1$. اما طبق قضیه ۱

$$|N(a)|=|N(b)||N(c)|$$

لذا: باید داشته باشیم:

$$1<|N(b)|<|N(a)|$$

اما $b\in S$، پس بدلیل انتخاب a، $|N(a)|\le|N(b)|$ که یک تناقض است. بنابراین، S خالی است. این اثبات قضیه را کامل می‌کند.

وقتی که یکتایی تجزیه برقرار نیست، یک عنصر تحویل‌ناپذیرp، ممکن است فاقد این خاصیت باشد که p|cd نتیجه دهد p|c یا p|d پیامد دیگری از نبود خاصیت یکتایی تجزیه، احتمال عدم وجود بزرگ‌ترین قاسم مشترک است.

حال پرسش این است: چگونه می‌توان نوع از یکتایی تجزیه را در دومین‌های که فاقد خاصیت یکتایی تجزیه اند، بر قرار نمود؟ پاسخ کومر، تمرکز روی ایدیال‌ها به‌جای عناصر بود. حاصل ضرب

IJ از دو ایدیال I و J بنا به تعریف عبارت است از ست همه عناصری به‌صورت ab که در آن $a \in I$ و $b \in J$ یعنی،

$$IJ = \{a_1b_1 + a_2b_2 \dots + a_nb_n / n \geq 1, a_k \in I. b_k \in J\}$$

می‌دانیم IJ یک ایدیال است. کومر به جای تجزیه یک عنصر a به حاصل ضرب عناصر تحویل‌ناپذیر، ایدیال اصلی (a) را به حاصل ضرب از ایدیال‌های اولیه تجزیه کرد.

می‌خواهیم ایدیال اصلی (٦) در $\mathbb{Z}[\sqrt{-5}]$ را به حاصل ضربی از ایدیال‌های اولیه تجزیه کنیم. طبیعی است که کار خود را با تجزیه ٦ به اعداد اول $2 \times 3 = 6$ شروع کنیم. به سادگی می‌توان دید که ایدیال (٦) برابر ایدیال حاصل ضرب (٣) (٢) می‌باشد. اما (٢) یک ایدیال اولیه نیست (برای مثال در (٢) داریم $6 = (1 - \sqrt{-5})(1 + \sqrt{-5})$ اما هیچ یک از عوامل این تجزیه در (٢) قرار ندارند). بنابراین، باید به طریق دیگری عمل کنیم. فرض کنید P ایدیال در $\mathbb{Z}[\sqrt{-5}]$ باشد که توسط ٢و $(1 + \sqrt{-5})$ تولید شده است، یعنی

$$P = \{2a + (1 + \sqrt{-5})b : a. b \in \mathbb{Z}[\sqrt{-5}]\}$$

P یک ایدیال است. $r + s\sqrt{-5} \in P$ اگر وتنها اگر r و s یا هر دو جفت و یا هر دو طاق باشند. در نتیجه تنها کوست‌های مختلف در $\mathbb{Z}[\sqrt{-5}] / P$ عبارتند از $0 + P$ و $1 + P$؛ برای این که اگر در عنصر دل‌خواه $m + n\sqrt{-5}$، m طاق n جفت باشد. دراین‌صورت:

$(m + n\sqrt{-5}) - 1 = (m - 1) + n\sqrt{-5} \in P$ زیرا $m - 1$ و n جفت هستند. بنابراین

$$(m + n\sqrt{-5}) + p = 1 + p$$

به‌طور مشابه اگر m جفت و n طاق باشد، دراین‌صورت $(m - 1) + n\sqrt{-5} \in P$ زیرا $m - 1$ و n طاق هستند. در نتیجه رینگ خارج قسمت $\mathbb{Z}[\sqrt{-5}] / P$ ایزومورف با $\mathbb{Z}_2$ است. بنابراین، pیک ایدیال اولیه در $\mathbb{Z}[\sqrt{-5}]$ است. استدلال مشابه نشان می‌دهد که ایدیال‌های Q_1 و Q_2 ذیل، ایدیال‌های اولیه می‌باشند.

$$Q_1 = \{3a + (1 + \sqrt{-5})b : a, b \in \mathbb{Z}[\sqrt{-5}]\}$$

$$Q_2 = \{3a + (1 - \sqrt{-5})b : a, b \in \mathbb{Z}[\sqrt{-5}]\}$$

ایدیال حاصل ضرب $P^2 = PP$ دقیقاً مساوی به ایدیال (٢) است و این که $Q_1Q_2 = (3)$. بنابراین، ایدیال (٦) حاصل ضربی از چهار ایدیال اولیه می‌باشد:

$$(6) = (2)(3) = P^2Q_1Q_2$$

کومر موفق شد نشان دهد که در دومین‌های مورد نظر او، به‌جز احتمالاً در ترتیب عوامل، تجزیه یک ایدیال به حاصل ضربی از ایدیال‌های اولیه یکتاست. این نتیجه بعداً توسط ددکیند تعمیم داده شد. به‌منظور بیان دقیق این تعمیم لازم است برخی مقدمات را ذکر نماییم:

یک عدد الجبری عبارت است از یک عدد مختلط که جذر یک پولینوم مونیک خلاف صفر با ضرایب ناطق باشد. اگر t یک عدد جبری بوده و جذر یک پولینوم از درجه n در $\mathbb{Q}(x)$باشد، دراین‌صورت؛

$$\mathbb{Q}(t) = \{a_0 + a_1 t + a_2\, t^2 \; + \cdots + a_{n-1}\omega^{n-1}\,, a_i \in \mathbb{Q}\,\}$$

یک ساحه‌ی فرعی $\mathbb{C}$است و هر عنصر $\mathbb{Q}(t)$ یک عدد الجبری است. یک عدد تام الجبری عبارت است از یک عدد مختلط که جذر یک پولینوم مونیک خلاف صفر با ضرایب تام باشد. می‌توان نشان داد که ست همه اعداد تام الجبری در $\mathbb{Q}(t)$ یک انتیگرال دومین است (۱). اگر ω یک جذر مختلط $x^p - 1$ باشد دراین‌صورت دومین $\mathbb{Z}[\omega]$ که کومر مورد استفاده قرار داد، در واقع دومین همه اعداد تام الجبری در $\mathbb{Q}(\omega)$ است (٦).

بنابراین، نتایج کومر حالت خاصی از قضیه زیر می‌باشد.

قضیه ۴. فرض کنید t یک عدد الجبری و R دومین همه اعداد تام الجبری در $\mathbb{Q}(t)$ باشد. دراین‌صورت هر ایدیال در R (بجز ۰ وR) حاصل ضرب از ایدیال‌های اولیه است و این تجزیه، به‌جز در ترتیب عوامل، یکتاست. برای اثبات به (٦) مراجعه شود.

بیشتر رینگ‌های $\mathbb{Z}[\sqrt{d}\,]$ نیز حالات خاص از قضیه ۴ می‌باشد، زیرا اگر d یک عدد تام مربع – آزاد باشد، دراین‌صورت $t = \sqrt{d}$ یک عددالجبری است (زیرا یک جذر $x^2 - d$ است) و

$$\mathbb{Q}[\sqrt{d}\,] = \{a_0 + a_1\sqrt{d} \,:\, a_i \in \mathbb{Q}\,\}$$

اعداد تام الجبری در ساحه‌ی $\mathbb{Q}[\sqrt{d}\,]$، اعدادتام درجه دوم نامیده می‌شوند. هر عضو $r + s\sqrt{d}$ از رینگ $\mathbb{Z}[\sqrt{d}\,]$ یک عددتام درجه دوم در $\mathbb{Q}[\sqrt{d}\,]$ است، زیرا جذر یک پولینوم مونیک در $\mathbb{Z}[x]$ می‌باشد:

$$x^2 - 2rx + (r^2 - ds^2) = (x - (r + s\sqrt{d}))(x - (r - s\sqrt{d}))$$

وقتی‌که (مود ۴) $d \equiv 2$ یا ۳ در این‌صورت $\mathbb{Z}[\sqrt{d}\,]$ عبارت از دومین R، متشکل از همه اعداد تام درجه دوم در $\mathbb{Q}[\sqrt{d}\,]$ است اما وقتی (مود ۴) $d \equiv 1$، اعدادتام درجه دوم در R وجود دارند که در $\mathbb{Z}[\sqrt{d}\,]$ نیستند. در رابینسون (۷) اثبات ساده از قضیه ۴ برای حالت اعدادتام درجه دوم ارایه شده است.

قضیه ۴ در نظریه اعداد الجبری بسیار مفید است. وقتی که $d < 0$، R یک دومین یکتایی تجزیه است، اگر تنها d یکی از اعداد ۱-، ۲-، ۳-،۷-، ۱۱-، ۱۹-، ۴۳-،۶۷-، ۱۶۳- باشد (۹). وقتی $d > 0$، ثابت شده است که برای dهایی مثل ۲،۳،۵،۶،۷،۱۱،۱۳،۱۷،۱۹،۲۱،۲۲،۲۳،۲۹ و بسیاری مقادیر دیگر، R یک دومین یکتایی تجزیه است، اما در این حالت هیچ فهرست کامل مانند آن‌چه برای حالت $d < 0$ ارایه شده وجود ندارد، حدس زده شده است که برای تعداد نامتناهی مقادیر R،d یک دومین یکتایی تجزیه است است.

نتیجه‌گیری

از موضوعات برسی‌شده دراین مقاله می‌توان گفت که در $\mathbb{Z}[\sqrt{d}]$ تجزیه‌ی عناصر به‌صورت حاصل ضرب از عوامل تحویل‌ناپذیر همواره ممکن است، اما این تجزیه ممکن یکتا نباشد. یعنی $\mathbb{Z}[\sqrt{d}]$ ممکن است یک دومین یکتایی تجزیه نباشد در دومین‌های فاقد خاصیت یکتایی تجزیه، یک عنصر تحویل‌ناپذیر p، ممکن است فاقد این خاصیت باشد که، $p|cd$ نتیجه دهد $p|c$ یا $p|d$ و احتمال عدم وجود بزرگ‌ترین قاسم مشترک در آن‌ها نیز وجود دارد. دراین دومین‌ها به‌جای تجزیه‌ی یک عنصر a به حاصل ضرب عناصر تحویل‌ناپذیر، می‌توان ایدیال اصلی (a) را به حاصل ضرب از ایدیال‌های اولیه تجزیه کرد، هم‌چنین دیده شد که:

اگر d یک عدد تام مربع – آزاد باشد و تابع

$$N: \mathbb{Z}[\sqrt{d}] \to \mathbb{Z}$$

$$N(s + t\sqrt{d}) = (s + t\sqrt{d})(s - t\sqrt{d}) = s^2 - dt^2$$

موسوم به تابع نُرم باشد، دراین صورت برای هر $a, b \in \mathbb{Z}[\sqrt{d}]$

$$a = o\ N(ab) = N(a)N(b)\ (2)\text{ , اگر وتنها اگر } N(a) = 0\ (1)$$

اگر $d > 1$، دراین‌صورت $\mathbb{Z}[\sqrt{d}]$ دارای تعداد نامتناهی واحد است. واحدهای $\mathbb{Z}[\sqrt{-1}]$ عبارت اند از ± 1 و $\pm i$. اگر $d < -1$، در این‌صورت واحدهای $\mathbb{Z}[\sqrt{d}]$ عبارت اند از ± 1. اگر $p \in \mathbb{Z}[\sqrt{d}]$ و $N(p)$ یک عدد تام اولیه در $\mathbb{Z}$ باشد، دراین‌صورت p در $\mathbb{Z}[\sqrt{d}]$ تحویل‌ناپذیر است. هر عنصر خلاف واحد، خلاف صفر در $\mathbb{Z}[\sqrt{d}]$ حاصل ضرب از عناصر تحویل‌ناپذیر است. و اگر t یک عدد الجبری و R دومین همه اعداد تام الجبری در $\mathbb{Q}(t)$ باشد. دراین‌صورت هر ایدیال در R (به‌جز ۰ و R) حاصل ضرب از ایدیال‌های اولیه است و این تجزیه، بدون ترتیب عوامل، یکتاست.

منابع

(1) Birkhoff G, Mac Lane S. A Survey of Modern Algebra. 4th edition. New York: Macmillan. 1977.

(2) Burton D. M. Abstract Algebra. Dbuque, Iowa; Wm. C. Brown. 1988.

(3) Burton D. M. Elementary Number Theory. Boston; Allyn and Bacon. 1980.

(4) Dudley U. Elementary Number Theory. 2nd edition. A Francisco: Freeman. 1978.

(5) Hungerford T.W. Abstract Algebra: An Introduction. 3th edition. Cengage Learning; 2014, pp. 344-350.

(6) Ireland K, and Rosen M. A Classical Introduction to Modern Number Theory. New York: Springer-Verlag. 1982.

(7) Robinson A. Numbers and Ideal. San Francisco; Holden Day. 1965.

(8) Rosen K. H. Elementary Number Theory and its Applications. 2nd edition Reading: Mass; Addison Wesley. 1988.

(9) Stark H. A Complete Determination of Complex Quadratic Fields of Class Number One. Michigan Mathematical Journal 14. 1967, PP. 1-27.