УДК 512.552.3, 511.14

Голубкова О.В., Пащенко З.Д.

[1] *студентка 5 курсу фізико-математичного факультету, ДВНЗ «ДДПУ»*

[2] *кандидат фізико-математичних наук, доцент кафедри алгебри, ДВНЗ «ДДПУ»*

e-mail: olgolubko@mail.ru, pashchenko_zd@mail.ru

АРИФМЕТИКА НЕФАКТОРІАЛЬНИХ ОБЛАСТЕЙ ЦІЛІСНОСТІ З «ІДЕАЛЬНИМИ» МНОЖНИКАМИ

В роботі розглядається нефакторіальне кільце $Z[\sqrt{-5}]$ та розклад його елементів на прості множники. Відсутність однозначності такого розкладу порушує окремі властивості подільності факторіальних кілець, зокрема виявляються відсутніми найбільший спільний дільник та найменше спільне кратне для окремих чисел. Дана робота показує шляхи відшукання НСД та НСК для таких чисел за допомогою «ідеальних» множників, які знаходяться за межами $Z[\sqrt{-5}]$.

Ключові слова: *простий елемент, складений елемент, регулярний елемент, дільник одиниці, НСД, НСК.*

Вступ

Однією із задач, яка призвела до побудови теорії кілець, була задача про розклад на прості множники. В деяких кільцях кожний складений елемент володіє однозначним розкладом, в інших кільцях розклад на прості множники існує, але не виконується умова однозначності, в третіх — існують складені елементи, які не мають розкладу на прості множники.

Області цілісності, що володіють однозначним розкладом на прості множники називають факторіальними. Вони є достатньо відомими і глибоко дослідженими. В даній статті розглядаються нефакторіальні кільця. Неоднозначність розкладу окремих її елементів приводить до того, що виникають суперечності з відомими властивостями факторіальних кілець, виникають проблеми із визначенням найбільших спільних дільників та найменших спільних кратних деяких пар елементів нефакторіальних кілець. Дана стаття показує, яким чином можна вирішити окремі з цих проблем.

Поштовхом до відкриття та вивчення областей з неоднозначним розкладом на прості множники стали спроби довести Велику теорему Ферма. В 1844 році німецький математик Ернст Куммер, вивчаючи публікації в Трудах Французької Академії, аналізував доведення Коші і Ламе. На думку Куммера, основна проблема полягала в тому, що доведення Коші і Ламе спиралися

на використання властивості цілих чисел, відомої під назвою єдиності розкладу на прості множники. Обидва представлених Академії доведення спиралися на комплексні числа. Куммер звернув увагу на те, що хоча теорема про єдиність розкладу на прості множники виконується для цілих чисел, вона не обов'язково повинна виконуватися, якщо використовуються комплексні числа. Дана проблема розглядається також в [1, 2, 3].

В роботі розглядається кільце $Z[\sqrt{-5}] = \{a+b\sqrt{5}i| \quad a, b \in Z\}$, окремі його числа, що не володіють однозначним розкладом. Приєднуючи до $Z[\sqrt{-5}]$ числа, які названо «ідеальними», вдається одержати однозначні розклади, які і вирішують проблеми визначення НСД та НСК для довільних чисел, хоча ці значення знаходяться за межами кільця $Z[\sqrt{-5}]$

Основні означення та зауваження

Представлення елемента a у вигляді добутку $a = p_1p_2 \dots p_n \ (n \geqslant 1)$ простих елементів з умовою, що в кожному такому представленні елемента a число n обмежено зверху натуральним числом, яке залежить тільки від кільця K і елемента a, називається ***факторизацією елемента*** a.

Нагадаємо, що всі ненульові елементи, які не є дільниками одиниці, називаються ***регулярними*** елементами.

Елемент d називають ***найбільшим спільним дільником*** a і b, якщо він є спільним дільником a і b та довільний інший їх спільний дільник ділить d.

Елементи a і b ***взаємно простими***, якщо вони мають тільки оборотні спільні дільники $((a, b) = 1)$.

Теорема 1. (Критерій кільця з факторизацією.) *Область цілісності є кільцем з факторизацією тоді і тільки тоді, коли на множині її регулярних елементів можна визначити функцію θ із значенням в множині $\mathbb{N}$, що володіє наступною властивістю: для будь-яких регулярних елементів a і b $\theta(ab) > \theta(a)$.*

(Таку функцію будемо називати ***нормою***.)

Доведення.

Необхідність. Нехай K – кільце з факторизацією і a – його регулярний елемент. Розглянемо всі різні факторизації елемента a і покладемо $\theta(a)$ рівним максимальному числу простих, не обов'язково різних, співмножників в факторизаціях елемента a. Якщо $a = p_1p_2 \dots p_{\theta(a)}$ – факторизація елемента a з максимальним числом простих співмножників і $b = q_1q_2 \dots q_n$ – деяка факторизація елемента b, то $ab = p_1p_2 \dots p_{\theta(a)}q_1q_2 \dots q_n$ є деяка факторизація елемента ab і тому $\theta(ab) > \theta(a)$.

Достатність. Множину всіх значень функції θ позначимо через A. Так як A – не порожня множина натуральних чисел, то вона містить мінімальний елемент. Нехай θ_1 – мінімальний елемент множини A. Якщо $A\backslash\{\theta_1\} \neq \emptyset$, то позначимо її мінімальний елемент через θ_2. Продовжуючи ці міркування, отримаємо монотонно зростаючу послідовність $\theta_1, \ldots, \theta_n, \ldots$ всіх значень функції θ. Методом математичної індукції доведемо, що кожний регулярний елемент допускає факторизацію. Індукцію проведемо за номерами значень функції θ.

Якщо для деякого p $\theta(p) = \theta$, то p – простий елемент. Дійсно, нехай $p = p_1p_2$, де p_1, p_2 - регулярні елементи, тоді $\theta(p) = \theta(p_1p_2) > \theta(p_1) > \theta_1$, тобто $\theta(p) > \theta_1$, що суперечить вибору елементу p. Так як простий елемент допускає факторизацію, то будь-який елемент x, для якого $\theta(x) = \theta_1$, допускає факторизацію.

Припустимо, що будь-який елемент a з умовою $\theta(a) < \theta_n$ допускає факторизацію. Нехай $\theta(b) = \theta_n$. Якщо b – простий елемент, то він допускає факторизацію, в протилежному випадку $b = cd$, де c і d – регулярні елементи. Із означення функції θ випливає, що $\theta(c) < \theta_n$ і $\theta(d) < \theta_n$, отже, c і d допускають факторизацію і елемент d можна представити у вигляді скінченого добутку простих множників. Методом від супротивного покажемо, що для всіх можливих представлень елемента b у вигляді добутку простих елементів число співмножників обмежене. Нехай

$$b = p_1p_2 \ldots p_s, \qquad s \geqslant \theta(b) + 1 \tag{1}$$

Має місце тотожність:

$$\begin{gathered}\theta(b) = (\theta(b) - \theta(p_2 \ldots p_s)) + (\theta(p_2 \ldots) - \theta(p_3 \ldots p_s)) + \ldots \\ \cdots + (\theta(p_{s-1}p_s) - \theta(p_s)) + \theta(p_s)\end{gathered} \tag{2}$$

Із означення функції θ випливає, що кожний доданок в правій частині тотожності (2) не менше одиниці, тому із тотожності (2) випливає, що $\theta(b) \geqslant s$, що суперечить умові (1).

□

Основна частина

Розглянемо кільце $Z[\sqrt{-5}] = \{a + b\sqrt{-5} \quad | a, b \in \mathbb{Z}\}$. Неважко перевірити, що $Z[\sqrt{-5}] \simeq Z[x]/(x^2 + 5)$ є областю цілісності. Визначимо функцію θ на $Z[\sqrt{-5}]$ наступним чином: $\theta(a + b\sqrt{5}i) = a^2 + 5b^2$. Легко доводиться, що

$$\theta((a + b\sqrt{5}i)(c + d\sqrt{5}i)) = \theta(a + b\sqrt{5}i)\theta(c + d\sqrt{5}i) \tag{3}$$

Оскільки $\theta(1) = 1$, то дільниками одиниці є лише числа $\varepsilon = x + y\sqrt{5}i$, $x, y \in Z$ такі, що $\theta(\varepsilon) = 1$, тобто $x^2 + 5y^2 = 1 \Rightarrow x = \pm 1, y = 0 \Rightarrow \varepsilon = \pm 1$. Так як $\theta(\beta) \in \mathbb{N} \quad \forall \beta \in Z[\sqrt{-5}], \beta \neq 0$, то для регулярного β маємо, що $\theta(\beta) > 1$. Тоді, враховуючи (3) для довільних регулярних α і β виконується умова:

$$\theta(\alpha, \beta) = \theta(\alpha)\theta(\beta) > \theta(\alpha).$$

За критерієм кільця з факторизацією, будь-який ненульовий елемент кільця $Z[\sqrt{-5}]$, що не є дільником одиниці, розкладається в добуток простих елементів, але такий розклад не є єдиним. Наприклад,

$$21 = (1 + 2\sqrt{5}i)(1 - 2\sqrt{5}i) = 3 \cdot 7.$$

Покажемо, що цілі числа

$$\alpha = 1 + 2\sqrt{5}i, \qquad \alpha' = 1 - 2\sqrt{5}i,$$

$$\beta = 3, \qquad \rho = 7$$

нерозкладні в $Z[\sqrt{-5}]$. Справді, якби $\beta = 3$ розкладалось в добуток $\gamma\delta$, в якому обидва множники відмінні від одиниці, то ми мали б

$$9 = \theta(3) = \theta(\gamma)\theta(\delta).$$

Але розклад числа 9 на натуральні множники, із яких жоден не дорівнює одиниці, можливий лише у вигляді $9 = 3 \cdot 3$, так що мало б бути $\theta(\gamma) = \theta(\delta) = 3$, і для $\gamma = x + y\sqrt{5}i$ з цілими раціональними x, y ми мали б $x^2 + 5y^2 = 3$, $x^2 \leqslant 3$, $y^2 \leqslant 3$, що, очевидно, неможливо. Отже, $\beta = 3$ нерозкладне в $Z[\sqrt{-5}]$. Аналогічно впевнюємося в тому, що $\rho = 7$ нерозкладне. Нарешті, якби α розкладалося в добуток $\gamma\delta$ з $\theta(\gamma) \neq 1$ і $\theta(\delta) \neq 1$, то ми мали б $\theta(\gamma)\theta(\delta) = \theta(\alpha) = 21$, отже, або $\theta(\gamma) = 3, \theta(\delta) = 7$, або навпаки. Але ми вище показали, що не може бути ніякого цілого γ з $\theta(\gamma) = 3$. Отже, α, а тому і спряжене йому α', нерозкладні.

Таким чином, число 21 двома суттєво різними способами представлене у вигляді добутку нерозкладних в $Z[\sqrt{-5}]$ цілих чисел:

$$21 = (1 + 2\sqrt{5}i)(1 - 2\sqrt{5}i) = 3 \cdot 7.$$

$$(21 = \alpha\alpha' = \beta\rho)$$

Отримали суперечність з традиційною теорією подільності, бо нерозкладне число 3 є дільником добутку $(1 + 2\sqrt{5}i)(1 - 2\sqrt{5}i)$, але не входить в жоден з його множників $(1 + 2\sqrt{5}i)$ і $(1 - 2\sqrt{5}i)$. З усього сказаного маємо, що числа $\alpha = 1 + 2\sqrt{5}i$ і $\beta = 3$ не мають спільних дільників, крім ± 1, бо кожне з них нерозкладне, $\alpha \nmid \beta$ і $\beta \nmid \alpha$. Тобто, $(\alpha, \beta) = 1$ за означенням.

Ми можемо спостерігати суперечності і при знаходженні НСД і НСК. Наприклад, $(21, 7\alpha)$. Нетривіальними дільниками числа 21 є $\pm\alpha, \pm\alpha', \pm 3, \pm 7$, а числа 7α — $\pm 1, \pm\alpha, \pm 7$. 7 і α є спільними дільниками 21 і 7α, причому $(7, \alpha) = 1$. Але $7\alpha \nmid 21$, бо $\frac{21}{7\alpha} = \frac{3}{\alpha}$, а $(3, \alpha) = 1$. Тому $(21, 7\alpha) \neq 7\alpha$. Також $(21, 7\alpha) \neq 7$, бо інший спільний дільник α не ділить 7. З цієї ж причини $(21, 7\alpha) \neq \alpha$. Не може бути $(21, 7\alpha) = 1$, оскільки взаємно прості елементи це ті, які не мають інших спільних дільників, крім дільників одиниці.

Так само не можливо знайти і $[21, 7\alpha]$. Це можна показати двома способами.

1) Формула взаємозв'язку НСД і НСК $\left([a, b] = \frac{ab}{(a,b)}\right)$ має місце завжди, якщо існує (a, b). В даному випадку ми не можемо нею скористатися.

2) За означенням НСК (a, b), це спільне кратне a і b, яке ділить довільне інше спільне кратне a і b. Серед кратних $147\alpha = 21 \cdot 7\alpha$, $147 = 21 \cdot 7$, 21α – не існує НСК:

   а) $\frac{147\alpha}{21} = 7\alpha$, $\frac{147\alpha}{7\alpha} = 21 \in Z[\sqrt{-5}]$, але $\frac{21\alpha}{147\alpha} = \frac{1}{7} \notin Z[\sqrt{-5}]$. Тобто $[21, 7\alpha] \neq 147\alpha$.

   б) $\frac{21\alpha}{21} = \alpha$, $\frac{21\alpha}{7\alpha} = 3 \in Z[\sqrt{-5}]$, але $21\alpha \nmid 147$, оскільки $\frac{147}{21\alpha} = \frac{7}{\alpha} \notin Z[\sqrt{-5}]$, тому $[21, 7\alpha] \neq 21\alpha$

   в) Аналогічно 147 і всі інші спільні кратні не можуть бути НСК $(21, 7\alpha)$.

Відмітимо далі, що хоча нерозкладні в $Z[\sqrt{-5}]$ числа $\alpha = 1 + 2\sqrt{5}i$ і $\beta = 3$, і не мають нетривіального спільного множника, який належав би $Z[\sqrt{-5}]$, але мають спільний множник (який не є одиницею) в іншому кільці. Справді, квадрати $\alpha^2 = -19 + 4\sqrt{5}i$ і $\beta^2 = 9$ діляться на ціле число $\lambda = 2 + \sqrt{5}i$, яке не є одиницею:

$$\alpha^2 = (2 + \sqrt{5}i)(-2 + 3\sqrt{5}i), \qquad \beta^2 = (2 + \sqrt{5}i)(2 - \sqrt{5}i).$$

Отже, $\frac{\alpha^2}{\lambda}$ і $\frac{\beta^2}{\lambda}$ - цілі. Так само квадрати α'^2 і ρ^2 діляться на $\tau = -2 - 3\sqrt{5}i$:

$$\alpha'^2 = (2 - \sqrt{5}i)(-2 - 3\sqrt{5}i), \qquad \rho^2 = 7^2 = (-2 - 3\sqrt{5}i)(-2 + 3\sqrt{5}i),$$

тобто $\frac{\alpha'^2}{\tau}$ і $\frac{\rho^2}{\tau}$ -цілі.

Тепер число $\sqrt{\lambda}$ (яке не належить кільцю $Z(\sqrt{-5})$) має властивості найбільшого спільного дільника чисел α і β.

Подвійний розклад $\alpha\alpha' = \beta\rho$ на нерозкладні в $Z[\sqrt{-5}]$ множники виявляється можливим тому, що

$$\alpha = \sqrt{\lambda}\sqrt{\tau'}, \quad \alpha' = \sqrt{\lambda'}\sqrt{\tau}, \qquad \beta = \sqrt{\lambda}\sqrt{\lambda'}, \qquad \rho = \sqrt{\tau}\sqrt{\tau'}$$

і в добутку $21 = \sqrt{\lambda}\sqrt{\lambda'}\sqrt{\tau}\sqrt{\tau'}$ чотири «ідеальні» множники, які не належать $Z[\sqrt{-5}]$, можуть декількома способами бути з'єднані в пари, які при множенні дають числа із $Z[\sqrt{-5}]$, причому всі вони попарно взаємно прості.

Завдяки введенню «ідеальних» множників вдається відновити закон однозначності розкладу на прості множники і побудувати арифметику, подібну до звичайної. Так, наприклад, оскільки

$$21 = \sqrt{\lambda}\sqrt{\lambda'}\sqrt{\tau}\sqrt{\tau'} \qquad 7\alpha = \sqrt{\tau}\sqrt{\tau'}\sqrt{\lambda}\sqrt{\tau'},$$

то легко знаходяться

$$(21, 7\alpha) = \sqrt{\lambda}\sqrt{\tau}\sqrt{\tau'} = 7\sqrt{\lambda} = \alpha\sqrt{\tau} \notin Z[\sqrt{-5}]$$

$$[21, 7\alpha] = \sqrt{\lambda}\sqrt{\lambda'}\sqrt{\tau}\sqrt{\tau'} = 21\sqrt{\tau'} = 7\alpha\sqrt{\lambda'} \notin Z[\sqrt{-5}].$$

Висновки

Досліджуючи техніку виділення «ідеальних множників» у нефакторіальних областях цілісності, ми зустрілися з фактами, які суперечать властивостям подільності в факторіальних кільцях. Опишемо ці суперечності.

Для факторіальної області цілісності K, якщо $(a, b) = 1 \quad (a, b \in K)$, то $(a^2, b^2) = 1$. В кільці $Z[\sqrt{-5}]$, якщо $\alpha = 1 + 2\sqrt{5}i$, то як було зазначено, $(\alpha, 3) = 1$, але $\alpha^2 = \lambda\tau', \quad 3^2 = \lambda\lambda'$, звідки $(\alpha^2, 3^2) = \lambda \neq 1$.

Наступна суперечність виникає з властивістю простих в K:

$$(a, b) = 1, \quad ac \vdots b \Rightarrow c \vdots b,$$

Оскільки $(\alpha, 3) = 1$ і $21 \vdots 3$, то розглядаючи $21 = \alpha \cdot \alpha'$ та враховуючи, що α' – просте, отримуємо, що $3 \nmid \alpha'$.

В кільці K маємо властивість НСД: $(ac, bc) = c(a, b)$. В нашому прикладі $(\alpha, 3) = 1$, але $(21, 7\alpha) = (7 \cdot 3, 7 \cdot \alpha) \neq 7$.

При використанні «ідеальних» множників, всі ці суперечності зникають. Та виникає питання, чи можна побудувати таке розширення кільця $Z[\sqrt{-5}]$, яке було б факторіальним. Проста перевірка показує, що розширення $Z[\sqrt{-5}][\sqrt{\lambda}, \sqrt{\lambda'}, \sqrt{\tau}, \sqrt{\tau'}]$ не розв'язує цього питання, оскільки, наприклад

$$6 = 2 \cdot 3 = (1 + \sqrt{5}i)(1 - \sqrt{5}i)$$

$$3^2 = \lambda \cdot \lambda' \qquad (\lambda = 2 + \sqrt{5}i)$$
$$2^2 = 4 = (-2)(-2) \Rightarrow 2 = (\sqrt{2}i)(-\sqrt{2}i)$$
$$(1 + \sqrt{5}i)^2 = -4 + 2\sqrt{5}i = (-2)\lambda'$$
$$(1 - \sqrt{5}i)^2 = -4 - 2\sqrt{5}i = (-2)\lambda,$$

отже

$$6 = \sqrt{\lambda}\sqrt{\lambda'}(\sqrt{2}i)(-\sqrt{2}i),$$

а числа $\sqrt{2}i$ і $-\sqrt{2}i \notin Z[\sqrt{-5}][\sqrt{\lambda}, \sqrt{\lambda'}, \sqrt{\tau}, \sqrt{\tau'}]$.

Також цікаво, для яких кілець типу $Z[\sqrt{-p}]$ можна застосовувати використання «ідеальних» множників? Яка будова кілець кілець $Z[\sqrt[3]{p}]$?

Література

[1] *Боревич З.І.* Теорія чисел / З.І. Боревич, І.Р. Шафаревич. — М.: Наука, 1985. — 504 с.

[2] *Гекке Е.* Лекции по теории алгебраических чисел / Е. Гекке; [пер. з нім. Г.І. Ольшанський, Д.А. Райков]. — М.: Гос. изд. технико-теоретической литературы, 1940. — 261 с.

[3] *Требенко Д.Я.* Алгебра і теорія чисел / Д.Я. Требенко, О.О. Требенко. — К.: НПУ ім. М.П. Драгоманова, 2006. — 400, [1] с.