Київський національний університет імені Тараса Шевченка

Є.В. Бондаренко

ТЕОРІЯ КІЛЕЦЬ

Навчальний посібник

2012

УДК 512.552
ББК 22.144

Рецензенти:
Ю.В.Боднарчук – доктор фізико-математичних наук, професор
В.М.Бондаренко – доктор фізико-математичних наук, професор

Рекомендовано до друку вченою радою механіко-математичного факультету (протокол № 2 від 17 вересня 2012 року)

Бондаренко Є.В.

Теорія кілець: навчальний посібник. – 2012. – 64 с.

У посібнику викладено основні поняття теорії кілець в обсязі, передбаченому навчальними програмами механіко-математичних факультетів університетів. Наведено велику кількість прикладів, які ілюструють методи розв'язання багатьох стандартних задач і допоможуть кращому засвоєнню теоретичного матеріалу.

Посібник призначений для студентів других курсів вищих навчальних закладів, де вивчається дисципліна "Алгебра і теорія чисел".

УДК 512.552
ББК 22.144

Зміст

Передмова

Даний посібник укладено на основі курсу лекцій з теорії кілець, які автор читає на механіко-математичному факультеті Київського національного університету імені Тараса Шевченка. Посібник охоплює весь теоретичний матеріал з теорії кілець, який входить до навчальної програми нормативного курсу "Алгебра і теорія чисел", що викладається в четвертому семестрі для студентів за спеціальностями "Математика" і "Статистика". Викладення матеріалу проілюстровано на багатьох прикладах, які, як сподівається автор, допоможуть зрозуміти матеріал курсу і ознайомитися з основними конструкціями в елементарній теорії кілець. У читача цього посібника ми передбачаємо володіння основами лінійної алгебри та теорії груп.

Позначення

$\mathbb{N}$	натуральні числа
$\mathbb{Z}$	цілі числа
$\mathbb{Q}$	раціональні числа
$\mathbb{R}$	дійсні числа
$\mathbb{C}$	комплексні числа
$\mathbb{Z}_n$	кільце лишків за модулем n
$\mathbb{Z}[i]$	кільце цілих гаусових чисел
$\mathbb{H}$	тіло дійсних кватерніонів
$(R,+)$	адитивна група кільця R
R^* і $U(R)$	мультиплікативна група кільця R
R/I	факторкільце кільця R за ідеалом I
(X)	ідеал, породжений множиною X
$R[x]$	кільце многочленів над кільцем R
$R[[x]]$	кільце формальних степеневих рядів над кільцем R
R^X	кільце функцій з множини X в кільце R
$R_1 \times \ldots \times R_n$	прямий добуток кілець R_i
$M_n(F)$	множина матриць розмірності $n \times n$ над полем F
$GL_n(F)$	група невироджених матриць розмірності $n \times n$ над полем F
$\operatorname{Im}\varphi$	образ відображення φ
$\operatorname{Ker}\varphi$	ядро відображення φ
S_n	симетрична група на множині з n елементів
НСД(a,b)	найбільший спільний дільник чисел a і b
НСК(a,b)	найменше спільне кратне чисел a і b

§ 1 Означення і приклади

Означення 1. *Кільцем* називається непорожня множина R з двома бінарними операціями, додавання "$+$" і множення "$\cdot$", які задовольняють таким умовам:

1) $(R, +)$ є абелевою групою, яка називається *адитивною групою кільця*;

2) множення є асоціативним: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ для всіх $a, b, c \in R$;

3) виконуються дистрибутивні закони: для всіх $a, b, c \in R$

$$a \cdot (b + c) = a \cdot b + a \cdot c \quad \text{і} \quad (a + b) \cdot c = a \cdot c + b \cdot c.$$

Замість $a \cdot b$ ми зазвичай будемо писати просто ab. Нейтральний елемент для додавання називається *нулем* і позначається 0. Обернений до елемента $a \in R$ відносно операції додавання називається протилежним елементом і позначається $-a$. В цих позначеннях маємо $a + (-a) = 0$.

Зауваження 1. Таким чином визначені кільця називають також асоціативними кільцями. Для неасоціативних кілець вимагають тільки властивості 1) і 3).

Означення 2. Кільце R називається *комутативним*, якщо операція множення є комутативною, тобто $ab = ba$ для всіх $a, b \in R$.

Кільце R називається *кільцем з одиницею*, якщо існує одиниця для множення, тобто існує елемент $1 \in R$ такий, що $a \cdot 1 = 1 \cdot a = a$ для всіх $a \in R$.

Зауваження 2. Чому в означенні кільця вимагається, щоб $(R, +)$ було саме абелевою групою? Одна з причин – це, якщо $1 \in R$, то абелевість випливає з дистрибутивних законів:

$$\left.\begin{array}{rcl} (1+1)(a+b) & = & 1(a+b) + 1(a+b) = a+b+a+b \\ (1+1)(a+b) & = & (1+1)a + (1+1)b = a+a+b+b \end{array}\right\} \Rightarrow \begin{array}{c} a+b \\ \| \\ b+a \end{array}$$

Означення 3. Кільце R з 1, де $1 \neq 0$, називається *тілом*, якщо кожен ненульовий елемент $a \in R$ має обернений відносно множення, тобто $(R \setminus \{0\}, \cdot)$ є групою.

Комутативне тіло називається *полем*.

Умова $1 \neq 0$ рівносильна $R \neq \{0\}$ (див. твердження 1 нижче). Тобто поле або тіло містить принаймні два елементи 0 і 1.

Перш ніж розглянути приклади кілець, ми доведемо деякі прості тотожності, які виконуються в довільному кільці і які допоможуть робити обчислення в кільцях. Зокрема, ці тотожності показують, що операції додавання і множення в кільці добре узгоджені між собою.

Твердження 1 (прості властивості кілець)**.** *Нехай R – кільце. Тоді для всіх елементів $a, b, c \in R$ виконуються рівності:*

1) $0a = a0 = 0$*;*

2) $(-a)b = a(-b) = -(ab)$*;*

3) $(-a)(-b) = ab$*;*

4) $a(b-c) = ab - ac$ *і* $(a-b)c = ac - bc$*;*

5) $(a+b)^2 = a^2 + b^2 + ab + ba$*;*

6) $(a_1 + \ldots + a_n)(b_1 + \ldots + b_m) = \sum_{i,j} a_i b_j$*;*

7) якщо R – кільце з 1, то одиниця єдина і $(-1) \cdot a = -a$*;*

8) якщо R – кільце з 1 і $R \neq \{0\}$, то $1 \neq 0$.

Доведення. Ці властивості випливають з дистрибутивних законів і скорочення в адитивній групі кільця. Доведемо властивості 1), 2), 7), 8), а інші залишимо як вправу.

1) Використавши рівність $0 = 0+0$ і дистрибутивний закон, отримуємо

$$a0 = a(0+0) = a0 + a0.$$

Скорочуючи в адитивній групі кільця, маємо $a0 = 0$. Аналогічно $0a = 0$.

2) Використовуючи дистрибутивний закон і властивість 1), отримуємо

$$ab + (-a)b = (a + (-a))b = 0b = 0.$$

Отже, $(-a)b = -ab$. Аналогічно $a(-b) = -ab$.

7) Нехай 1 і $1'$ – дві одиниці кільця R. Тоді $1 = 1 \cdot 1' = 1'$.
Рівність $(-1)a = -a$ випливає з властивості 2).

8) Візьмемо ненульовий елемент $a \in R$. Тоді $a = a1 \neq a0 = 0$, отже, $1 \neq 0$.

□

Так само, як визначають підпростори у векторних просторах і підгрупи в групах, визначають підструктури і в кільцях.

Означення 4. Непорожня підмножина S кільця R називається *підкільцем*, якщо S є кільцем відносно операцій визначених в R.

Аналогічно доводиться наступний критерій.

Твердження 2 (критерій підкільця)**.** *Нехай S – непорожня підмножина кільця R. Наступні умови рівносильні:*

1) S є підкільцем R;

2) $(S, +)$ є підгрупою $(R, +)$ і S замкнена відносно множення;

3) $a - b, ab \in S$ для всіх $a, b \in S$.

Приклади кілець

Приклади 1. 1. **Числові кільця.** Множина цілих чисел $\mathbb{Z}$ зі стандартними операціями додавання і множення чисел є комутативним кільцем з 1. Кільце $\mathbb{Z}$ не є полем: не існує оберненого відносно множення, наприклад, для числа 2.

Множини раціональних чисел $\mathbb{Q}$, дійсних чисел $\mathbb{R}$ і комплексних чисел $\mathbb{C}$ зі стандартними операціями додавання і множення є комутативними кільцями з 1. Маємо ланцюжок підкілець $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$. Кільця $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ є полями.

2. Множина парних цілих чисел $2\mathbb{Z} = \{2n : n \in \mathbb{Z}\}$ є комутативним кільцем без 1. Кільце $2\mathbb{Z}$ є підкільцем $\mathbb{Z}$. Зауважте, що навіть якщо кільце має одиницю, ми не вимагаємо, щоб підкільце мало одиницю. Неважко описати всі підкільця в кільці $\mathbb{Z}$. Кожне підкільце має бути підгрупою адитивної групи кільця. Ми знаємо з теорії груп, що єдиними підгрупами в $\mathbb{Z}$ є $n\mathbb{Z}$ для $n \in \mathbb{N} \cup \{0\}$ (де $0\mathbb{Z} = \{0\}$). Кожна підмножина $n\mathbb{Z}$ замкнена відносно множення. Отже, всі вони є підкільцями $\mathbb{Z}$.

3. **Кільця лишків.** Основним прикладом скінченного кільця є циклічна група $\mathbb{Z}_n = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$ лишків за модулем n ($n \in \mathbb{N}$) з операцією множення $\overline{a} \cdot \overline{b} = \overline{a \cdot b}$. Кільце $\mathbb{Z}_n$ є комутативним кільцем з 1. Адитивна група кільця $\mathbb{Z}_n$ ізоморфна факторгрупі $\mathbb{Z}/n\mathbb{Z}$, і пізніше ми отримаємо $\mathbb{Z}_n$ як факторкільце $\mathbb{Z}/n\mathbb{Z}$. Зауважимо, що $\mathbb{Z}_n$ не є підкільцем $\mathbb{Z}_{n+1}$ або $\mathbb{Z}$. Пізніше ми доведемо, що кільце $\mathbb{Z}_n$ є полем тоді і лише тоді, коли n є простим числом.

   В кільці $\mathbb{Z}_n$ можуть виконуватись тотожності, які виглядають дивно для тих, хто звик працювати з цілими або дійсними числами. Наприклад, в кільці $\mathbb{Z}_6$ виконується $\overline{3} \cdot \overline{5} = \overline{3}$ або $\overline{2} \cdot \overline{3} = \overline{0}$, тобто, на відміну від звичних для нас цілих чисел $\mathbb{Z}$ або полів $\mathbb{Q}, \mathbb{R}, \mathbb{C}$, в інших кільцях добуток ненульових елементів може дорівнювати нулю. Цю властивість ми будемо досліджувати в наступному розділі.

4. **Кільця многочленів.** Раніше ми розглядали многочлени від однієї змінної над полями. Більш загально, можна розглядати многочлени над кільцями. Нехай R – комутативне кільце з 1. Тоді множина

$$R[x] = \{a_0 + a_1 x + \cdots + a_n x^n : a_i \in R, n \geq 0\}$$

   всіх многочленів від однієї змінної над R є комутативним кільцем з 1. Кільце R є підкільцем $R[x]$. Наприклад, ми будемо розглядати такі кільця многочленів: $\mathbb{Z}[x], \mathbb{Q}[x], \mathbb{R}[x], \mathbb{Z}_n[x]$ тощо.

5. **Матричні кільця.** Нехай R – кільце. Множина квадратних матриць $M_n(R)$ розмірності $n \times n$ з коефіцієнтами з кільця R із

стандартними операціями додавання і множення матриць є кільцем ($n \in \mathbb{N}$). Якщо R – кільце з 1, то одинична матриця E є одиницею в $M_n(R)$. Якщо $n \geq 2$ і в кільці R існує ненульовий добуток $ab \neq 0$, то кільце $M_n(R)$ – некомутативне (навіть якщо R – комутативне):

$$\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & ab \\ 0 & 0 \end{pmatrix} \quad \neq$$
$$\begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

Легко показати, якщо S – підкільце R, то $M_n(S)$ є підкільцем $M_n(R)$. Наприклад, маємо ланцюжок підкілець $M_n(2\mathbb{Z}) \subset M_n(\mathbb{Z}) \subset M_n(\mathbb{Q}) \subset M_n(\mathbb{R}) \subset M_n(\mathbb{C})$. Іншими прикладами підкілець є множина скалярних матриць, множини верхніх трикутних матриць і нижніх трикутних матриць.

6. **Тіло кватерніонів.** Розглянемо множину $\mathbb{H} = \mathbb{H}(\mathbb{R})$, яка складається з елементів вигляду $a + bi + cj + dk$, де $a, b, c, d \in \mathbb{R}$, а i, j, k – формальні символи (вираз $a + bi + cj + dk$ можна розглядати як многочлен від змінних i, j, k над полем $\mathbb{R}$). Додавання в $\mathbb{H}$ визначається покоординатно, як для многочленів:

$$\begin{aligned} & (a + bi + cj + dk) + (a' + b'i + c'j + d'k) = \\ = \quad & (a + a') + (b + b')i + (c + c')j + (d + d')k, \end{aligned}$$

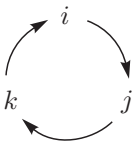
а множення – використовуючи співвідношення

$$i^2 = j^2 = k^2 = -1,\ ij = -ji = k,\ jk = -kj = i,\ ki = -ik = j$$

і розкриваючи дужки за дистрибутивними законами. Наприклад:

$$\begin{aligned} & (1 + 2i - j + 3k)(2i - k) = 1(2i - k) + 2i(2i - k) - \\ & -j(2i - k) + 3k(2i - k) = 2i - k + 4i^2 - 2ik - 2ji + \\ & +jk + 6ki - 3k^2 = 2i - k - 4 + 2j + 2k + i + 6j + 3 = \\ & = -1 + 3i + 8j + k. \end{aligned}$$

Правило множення i, j, k легко запам'ятати, використовуючи наступний рисунок: добуток двох елементів, які розташовані послідовно за стрілкою, дорівнює наступному елементу; а добуток проти стрілки – мінус наступний елемент.



Відносно цих операцій $\mathbb{H}$ є некомутативним кільцем з одиницею $1 = 1 + 0i + 0j + 0k$ (перевірте!), яке називається *кільцем (дійсних) кватерніонів*. Аналогічно можна визначати кільця раціональних кватерніонів $\mathbb{H}(\mathbb{Q})$ і цілих кватерніонів $\mathbb{H}(\mathbb{Z})$. Крім того, для кожного ненульового елемента існує обернений в $\mathbb{H}$:

$$(a + bi + cj + dk)^{-1} = \frac{a - bi - cj - dk}{a^2 + b^2 + c^2 + d^2} \in \mathbb{H}.$$

Отже, $\mathbb{H}$ є тілом, яке історично було одним з перших прикладів некомутативних тіл. Тіло кватерніонів є дійсним скінченно вимірним тілом, тобто тілом, яке містить поле $\mathbb{R}$ і є скінченно вимірним векторним простором над $\mathbb{R}$. Відомий результат Фробеніуса класифікує всі такі тіла.

Теорема 3 (Фробеніус)**.** *Кожне дійсне скінченно вимірне тіло ізоморфне* $\mathbb{R}$*,* $\mathbb{C}$ *або* $\mathbb{H}$*.*

7. **Кільця функцій.** Нехай X – довільна непорожня множина і R – деяке кільце. Тоді множина всіх функцій $R^X = \{f : X \to R\}$ є кільцем відносно операцій поточкового додавання і множення функцій:

$$(f + g)(x) = f(x) + g(x) \quad \text{і} \quad (fg)(x) = f(x)g(x).$$

Якщо кільце R – комутативне, то і кільце R^X – комутативне. Якщо R – кільце з 1, то і R^X є кільцем з 1, де одиниця – це константна функція $id(x) = 1$ для всіх $x \in X$.

Використовуючи властивості неперервних функцій важко не побачити, що множина $C[a, b] = \{f : [a, b] \to \mathbb{R} : f \text{ є неперервною}\}$

є комутативним кільцем з 1, підкільцем $\mathbb{R}^{[a,b]}$. Більш загально, ланцюжок підкілець $C[a,b] \supset C^1[a,b] \supset C^2[a,b] \supset \dots$ утворюють n-разів диференційовані функції $C^n[a,b]$ на відрізку $[a,b]$ $(n \geq 0)$.

8. **Кільця формальних степеневих рядів.** Нехай R – комутативне кільце з 1. Елементами кільця формальних степеневих рядів $R[[x]]$ є всі формальні нескінченні суми $\sum_{n=0}^{\infty} a_n x^n$, де $a_n \in R$ для всіх n. Додавання і множення визначаються як і для многочленів:

$$\begin{aligned} \sum_{n=0}^{\infty} a_n x^n + \sum_{n=0}^{\infty} b_n x^n &= \sum_{n=0}^{\infty} (a_n + b_n) x^n \\ \sum_{n=0}^{\infty} a_n x^n \cdot \sum_{n=0}^{\infty} b_n x^n &= \sum_{n=0}^{\infty} \left(\sum_{k=0}^{n} a_k b_{n-k} \right) x^n. \end{aligned}$$

Кільце $R[[x]]$ є комутативним кільцем з 1.

9. **Квадратичні поля.** Нехай $D \in \mathbb{Z}$ є вільним від квадратів, тобто D не ділиться на квадрат жодного цілого числа більше 1. Множина $\mathbb{Q}[\sqrt{D}] = \{a+b\sqrt{D} : a, b \in \mathbb{Q}\} \subset \mathbb{C}$ зі стандартними операціями додавання і множення комплексних чисел утворює поле, яке називається *квадратичним полем*. Замкненість відносно операцій легко бачити, а обернений до ненульового елемента можна знайти за формулою

$$(a + b\sqrt{D})^{-1} = \frac{a - b\sqrt{D}}{a^2 - Db^2} \in \mathbb{Q}[\sqrt{D}].$$

В полі $\mathbb{Q}[\sqrt{D}]$ визначають *норму* $N : \mathbb{Q}[\sqrt{D}] \to \mathbb{Q}$ за правилом

$$N(a + b\sqrt{D}) = (a + b\sqrt{D})(a - b\sqrt{D}) = a^2 - Db^2.$$

Важливою властивістю норми N є її *мультиплікативність*:

$$N(xy) = N(x)N(y)$$

для всіх $x, y \in \mathbb{Q}[\sqrt{D}]$ (перевірте!).
Умова, що D є вільним від квадратів є природньою: перевірте, що розглядаючи $\mathbb{Q}[\sqrt{D}]$ для довільного $D \in \mathbb{Q}$, ми не отримаємо нових кілець.

10. **Кільцем цілих гаусових чисел** називається множина

$$\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$$

комплексних чисел, у яких дійсна та уявна частини є цілими числами. Легко бачити, що $\mathbb{Z}[i]$ є підкільцем $\mathbb{C}$, оскільки воно замкнене відносно додавання і множення.

Більш загально, для $D \in \mathbb{Z}$ вільного від квадратів визначають кільце $\mathbb{Z}[\sqrt{D}] = \{a + b\sqrt{D} : a, b \in \mathbb{Z}\}$. Кільце $\mathbb{Z}[\sqrt{D}]$ є підкільцем поля $\mathbb{Q}[\sqrt{D}]$. Норму $N(\cdot)$, яку ми визначали в полі $\mathbb{Q}[\sqrt{D}]$, можна звузити на кільце $\mathbb{Z}[\sqrt{D}]$, при цьому важливо, що норма на кільці $\mathbb{Z}[\sqrt{D}]$ приймає тільки цілі значення.

11. **Групові кільця.** Нехай $G = \{g_1, g_2, \ldots, g_n\}$ – скінченна група з мультиплікативною операцією і R – комутативне кільце з 1. *Груповим кільцем* RG групи G над кільцем R називається множина формальних сум $a_1g_1+a_2g_2+\ldots+a_ng_n$, де $a_i \in R$, з покоординатною операцією додавання

$$(a_1g_1+\ldots+a_ng_n)+(b_1g_1+\ldots+b_ng_n) = (a_1+b_1)g_1+\ldots+(a_n+b_n)g_n,$$

а множення визначається для елементів ag_i та bg_j за правилом $(ag_i)(bg_j) = abg_k$, де $g_k = g_ig_j$, і розповсюджується для всіх сум за дистрибутивністю.

Наприклад, в груповому кільці $\mathbb{Z}S_3$ симетричної групи S_3 маємо:

$$\begin{aligned}&\big(5(1\,2) + (1\,3) - 3(1\,2\,3)\big)\big(2(1\,2) + 7(1\,3\,2)\big) = 5(1\,2)\big(2(1\,2) + \\ &+7(1\,3\,2)\big) + (1\,3)\big(2(1\,2) + 7(1\,3\,2)\big) - 3(1\,2\,3)\big(2(1\,2) + \\ &+7(1\,3\,2)\big) = 10\varepsilon + 35(2\,3) + 2(1\,3\,2) + 7(1\,2) - 6(2\,3) - 21\varepsilon = \\ &= -11\varepsilon + 7(1\,2) + 29(2\,3) + 2(1\,3\,2).\end{aligned}$$

Якщо група G – абелева, то кільце RG – комутативне. Якщо S є підкільцем R, то SG є підкільцем RG. Крім того, якщо H є підгрупою G, то RH є підкільцем RG.

Вправи

1. Доведіть, що перетин підкілець кільця є підкільцем.

2. Чи утворює підкільце в кільці $M_n(\mathbb{R})$ множина матриць $S = \{A \in M_n(\mathbb{R}) : \det(A) = \pm 1\}$?

3. Нехай 2^M – це множина всіх підмножин множини M. Доведіть, що множина 2^M утворює кільце відносно операцій перетину $\cap$ і симетричної різниці множин $\triangle$.

4. Перевірте мультиплікативність норми $N(\cdot)$, яка визначена на квадратичному полі $\mathbb{Q}[\sqrt{D}]$ в прикладі 1.9.

§ 2 Дільники нуля і оборотні елементи

Дільники нуля

Нехай R – довільне кільце.

Означення 5. Ненульовий елемент $a \in R$ називається *лівим дільником нуля*, якщо існує ненульовий елемент $b \in R$ такий, що $ab = 0$. Аналогічно ненульовий елемент $a \in R$ називається *правим дільником нуля*, якщо існує ненульовий елемент $b \in R$ такий, що $ba = 0$. *Дільником нуля* називається елемент, який є одночасно лівим і правим дільником нуля.

Означення 6. Комутативне кільце з $1 \neq 0$ і без дільників нуля називається *областю цілісності*.

Для того, щоб довести, що комутативне кільце з $1 \neq 0$ є областю цілісності, потрібно розглянути рівняння $ab = 0$ і довести, що a або b дорівнює нулю.

Приклади 2. 1. Кільце $\mathbb{Z}$ є областю цілісності.

2. Кожне поле є областю цілісності. Дійсно, якщо $ab = 0$ і $a \neq 0$, то $b = a^{-1}ab = a^{-1}0 = 0$. Отже, поля не містять дільників нуля. Зокрема, поля $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ є областями цілісності.

3. В області цілісності будь-яке підкільце з $1 \neq 0$ теж є областю цілісності. Зокрема, кільце цілих гаусових чисел $\mathbb{Z}[i]$ і квадратичні кільця $\mathbb{Z}[\sqrt{D}]$ є областями цілісності, оскільки вони є підкільцями поля комплексних чисел.

4. Кільце многочленів $R[x]$ над областю цілісності R теж є областю цілісності. Дійсно, якщо $f(x), g(x) \in R[x]$ – ненульові многочлени зі старшими коефіцієнтами $a_n x^n$ і $b_m x^m$ відповідно, то многочлен $f(x)g(x)$ має старший коефіцієнт $a_n b_m x^{n+m}$. Оскільки R – область цілісності, $a_n \neq 0$ і $b_m \neq 0$, то і $a_n b_m \neq 0$. Отже, $f(x)g(x) \neq 0$ і $R[x]$ не містить дільників нуля.

   Зокрема, кільця $\mathbb{Z}[x], \mathbb{R}[x]$ є областями цілісності.

5. Кільце $\mathbb{Z}_n$ не завжди є областю цілісності. Наприклад, в кільці $\mathbb{Z}_6$ виконується $\overline{2} \cdot \overline{3} = \overline{0}$ і, отже, $\overline{2}, \overline{3}$ є дільниками нуля.

   Доведемо, що кільце $\mathbb{Z}_n$ є областю цілісності тоді і лише тоді, коли n – просте число. Припустимо, що $n = ab$ для $a, b \geq 2$. Тоді $\overline{a}, \overline{b} \neq \overline{0}$, але $\overline{a} \cdot \overline{b} = \overline{n} = \overline{0}$. Більш загально, якщо НСД$(a, n) = d > 1$ і $1 < a < n$, то $\overline{a}$ є дільником нуля, оскільки $\overline{a}\overline{b} = \overline{0}$ для $b = \frac{n}{d}$. Отже, $\mathbb{Z}_n$ не є областю цілісності. Навпаки, нехай n – просте число і розглянемо ненульовий елемент $\overline{a}$. Тоді a і n взаємно прості і за узагальненим алгоритмом Евкліда існують $u, v \in \mathbb{Z}$ такі, що $ua + vn = 1$, тобто $\overline{u} \cdot \overline{a} = \overline{1}$. Отже, кожен ненульовий елемент має обернений. Значить $\mathbb{Z}_n$ є полем для простого n і, зокрема, областю цілісності. Ми довели більш сильний факт: $\mathbb{Z}_n$ є полем $\Leftrightarrow$ n – просте число.

6. Кільце матриць $M_n(R)$ містить дільники нуля при $n \geq 2$ і $R \neq \{0\}$. Наприклад, в $M_2(\mathbb{Z})$ маємо

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix},$$

   і, отже, матриці в добутку є дільниками нуля (опишіть всі дільники нуля!).

7. Розглянемо кільце функцій R^X для $|X| \geq 2$ і $R \neq \{0\}$. Нехай $f(x) \in R^X$ – ненульова функція, яка приймає значення нуль в деякій точці $a \in X$. Розглянемо функцію $g(x)$, яка дорівнює нулю в усіх точках крім a. Тоді $f(x)g(x) = 0$ і, отже, $f(x)$ є дільником нуля.

Твердження 4. *Комутативне кільце R з $1 \neq 0$ є областю цілісності тоді і лише тоді, коли в ньому можна скорочувати, тобто для довільних $a, b, c \in R$ з умови $ab = ac$, $a \neq 0$, випливає $b = c$.*

Доведення. Нехай R – область цілісності. Якщо $ab = ac$ для $a \neq 0$, то $ab - ac = a(b - c) = 0$. Оскільки в R немає дільників нуля і $a \neq 0$, то $b = c$.

Навпаки, якщо в R виконується $ab = 0$ для $a \neq 0$, то з умови $ab = 0 = a0$ випливає $b = 0$. Отже, R не містить дільників нуля і тому є областю цілісності. □

Теорема 5. *Скінченна область цілісності є полем.*

Доведення. Візьмемо довільний елемент $a \in R$, $a \neq 0$. Потрібно довести, що існує елемент $b \in R$ такий, що $ab = 1$. Розглянемо відображення $R \to R$, $x \mapsto ax$. Це відображення є ін'єктивним, оскільки з умови $ax = ay$ випливає $x = y$ за твердженням 4. Оскільки $|R| < \infty$, то відображення $x \mapsto ax$ також є сюр'єктивним (це стандартний факт, якщо X – скінченна множина, то відображення $X \to X$ є сюр'єктивним тоді і лише тоді, коли воно є ін'єктивним). Отже, існує $b \in R$, який відображається в одиницю кільця, тобто $ab = 1$. Звідси випливає, що кожен ненульовий елемент має обернений і R є полем. □

Цікаво, що для скінченного кільця комутативність випливає з існування обернених елементів, тобто справедлива наступна теорема (без доведення).

Теорема 6 (Веддерберн)**.** *Скінченне тіло є полем.*

Означення 7. Елемент $a \in R$ називається *нільпотентним*, якщо існує $n \in \mathbb{N}$ таке, що $a^n = 0$.

Перевірте, що ненульові нільпотентні елементи є дільниками нуля.

Оборотні елементи

Нехай R – кільце з $1 \neq 0$.

Означення 8. Елемент $a \in R$ називається *оборотним справа* або *лівим дільником одиниці*, якщо існує $b \in R$ такий, що $ab = 1$. Аналогічно елемент $a \in R$ називається *оборотним зліва* або *правим дільником одиниці*, якщо існує $b \in R$ такий, що $ba = 1$.

Елемент $a \in R$, який є оборотним зліва і справа, називається *оборотним* або *дільником одиниці*.

Зауваження 3.

1. Елемент $a \in R$ є оборотним тоді і лише тоді, коли існує $b \in R$ такий, що $ab = ba = 1$ (доведіть).
2. Якщо $ab = 1 = ca$, то $b = 1b = cab = c1 = c$. Тобто, якщо a є оборотним, то його обернений визначається однозначно і позначається a^{-1}.

Твердження 7. *Дільники нуля не є оборотними.*

Доведення. Нехай $a \in R$ – оборотний елемент. Тоді, якщо $ab = 0$, то $b = 1b = a^{-1}ab = a^{-1}0 = 0$ і a не є лівим дільником нуля. Аналогічно з $ba = 0$ випливає $b = b1 = baa^{-1} = 0a^{-1} = 0$, і a не є правим дільником нуля. □

Наслідок 8. *Кожне поле не містить дільників нуля.*

Твердження 9. *Множина всіх оборотних елементів кільця утворює групу відносно множення. Ця група позначається*

$$R^* = U(R) = \{a \in R : a \text{ – оборотний}\}$$

і називається мультиплікативною групою кільця.

Доведення. Перевіримо аксіоми групи. Нехай a і b – оборотні елементи. Тоді $ab \cdot b^{-1}a^{-1} = 1$ і $b^{-1}a^{-1} \cdot ab = 1$. Отже, ab є оборотним і належить множині R^*. Множення є асоціативним за означенням кільця. Одиниця кільця є оборотним елементом і належить множині R^*. Якщо елемент a є оборотним, то і a^{-1} є оборотним (з оберненим a). Отже, R^* є замкненим відносно взяття обернених елементів. □

Приклади 3. 1. В кільці $\mathbb{Z}$ оборотними елементами є 1 і -1, тобто $\mathbb{Z}^* = \{\pm 1\} \cong C_2$.

2. Розглядаючи дільники нуля в кільці $\mathbb{Z}_n$, ми довели, що елемент $\overline{k}$ є оборотним тоді і лише тоді, коли k і n взаємно прості. Отже, мультиплікативною групою кільця $\mathbb{Z}_n$ є група $\mathbb{Z}_n^* = \{\overline{k} : (k, n) = 1\}$. Зокрема, кожен ненульовий елемент кільця $\mathbb{Z}_n$ є або дільником нуля, або дільником одиниці.

3. Нехай R – область цілісності. Тоді мультиплікативною групою кільця многочленів $R[x]$ є група R^*. Дійсно, якщо $p(x)q(x) = 1$ в $R[x]$, то $\deg p(x) + \deg q(x) = 0$ і, отже, $p(x), q(x) \in R$. А оскільки $p(x)q(x) = 1$, то $p(x), q(x) \in R^*$.

   Якщо R містить дільники нуля, то це спостереження може не виконуватись. Наприклад, в $\mathbb{Z}_4[x]$ елемент $\overline{2}x + \overline{1}$ є оборотним, оскільки $(\overline{2}x + \overline{1})^2 = \overline{1}$.

4. Мультиплікативною групою кільця матриць $M_n(\mathbb{R})$ є загальна лінійна група $GL_n(\mathbb{R})$.

5. В кільці функцій $R = \{f : [a, b] \to \mathbb{R}\}$ оборотними елементами є функції $f(x)$ такі, що $f(x) \neq 0$ для всіх $x \in [a, b]$, з оберненою функцією $\frac{1}{f(x)}$.

6. Знайдемо обернені в кільці цілих гаусових чисел $\mathbb{Z}[i]$. Для цього використаємо норму $N(a+bi) = a^2+b^2$. Нехай $\alpha = a+bi$ – оборотний елемент і $\alpha\beta = 1$ для деякого $\beta \in \mathbb{Z}[i]$. Тоді

$$N(\alpha\beta) = N(\alpha)N(\beta) = 1 \quad \Rightarrow \quad N(\alpha) = a^2 + b^2 = 1 \quad \Rightarrow$$
$$\Rightarrow \quad a = \pm 1,\, b = 0 \;\text{ або }\; a = 0,\, b = \pm 1.$$

   Отже, $(\mathbb{Z}[i])^* = \{\pm 1, \pm i\}$.

   Аналогічні міркування можна застосовувати в інших квадратичних кільцях. Наприклад, в $\mathbb{Z}[\sqrt{2}]$ знаходження дільників одиниці зводиться до розв'язання рівняння Пеля $a^2 - 2b^2 = \pm 1$ в цілих числах.

Вправи

1. Опишіть дільники нуля, дільники одиниці і нільпотентні елементи в кільцях $\mathbb{Z}_{40}$, $\mathbb{Z}[\sqrt{-2}]$, $\mathbb{Z} \times \mathbb{Q}$, $\mathbb{R}[x]$, $\mathbb{Z}\left[\frac{2}{15}\right]$, $M_2(\mathbb{R})$.

2. Нехай R – скінченне кільце і $a \in R$ – не дільник нуля. Доведіть, що R є кільцем з 1 і a є оборотним.

3. Нехай R – кільце з 1. Доведіть, що сума довільного нільпотентного і оборотного елементів є оборотним елементом.

4. Нехай R – область цілісності. Доведіть, що кільце формальних степеневих рядів $R[[x]]$ теж є областю цілісності.

5. Опишіть всі області цілісності R, в яких $a^2 = 1$ для всіх $a \in R$.

§ 3 Ідеали

Нехай R – кільце.

Означення 9. Підкільце I кільця R називається *лівим ідеалом*, якщо $ra \in I$ для всіх $a \in I$, $r \in R$ ($RI \subset I$). Аналогічно підкільце I називається *правим ідеалом*, якщо $ar \in I$ для всіх $a \in I$, $r \in R$ ($IR \subset I$).

Підкільце I кільця R називається *ідеалом* або *двостороннім ідеалом*, якщо I є лівим і правим ідеалом.

Зрозуміло, що в комутативному кільці кожен лівий ідеал є правим і навпаки. Тому має сенс говорити тільки про просто ідеали.

Як ми побачимо далі, ідеали в кільцях відіграють роль подібну до нормальних підгруп в групах. Аналогічно до критерію підкільця доводиться наступний критерій ідеалу.

Твердження 10 (критерій ідеалу)**.** *Непорожня підмножина $I \subset R$ є ідеалом тоді і лише тоді, коли*

1) $a - b \in I$ для всіх $a, b \in I$;

2) $ra \in I$ і $ar \in I$ для всіх $a \in I$, $r \in R$.

Приклади 4. 1. В довільному кільці R підмножини $\{0\}$ і R завжди є ідеалами, які називаються *тривіальними ідеалами*. В кожному полі є тільки тривіальні ідеали. Це випливає з того, що кожен ненульовий ідеал I містить деякий оборотний елемент a, а отже, і кожен елемент кільця: $b = ba^{-1}a \in I$ для всіх b. Аналогічно доводиться, що в будь-якому кільці, якщо ідеал містить деякий оборотний елемент, то він співпадає з усім кільцем.

Ідеал I називається *власним*, якщо $I \neq R$.

2. Для кожного n підкільце $n\mathbb{Z}$ є ідеалом в $\mathbb{Z}$.

3. Взагалі кажучи, не кожне підкільце є ідеалом. Наприклад, в кільці матриць $M_2(\mathbb{Z})$ множина діагональних матриць є підкільцем, але не є ідеалом. Також лівий ідеал не завжди є правим: в $M_2(\mathbb{Z})$ множини

$$I = \left\{ \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} : a, b \in \mathbb{Z} \right\} \quad J = \left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} : a, b \in \mathbb{Z} \right\}$$

є лівим і правим ідеалом відповідно, але не є двосторонніми ідеалами. Двосторонніми ідеалами є, наприклад, $M_2(n\mathbb{Z})$ для довільного n. Більш загально, якщо I – ідеал в R, то $M_n(I)$ – ідеал в $M_n(R)$ (чи є інші ідеали?).

4. Нехай R – комутативне кільце з 1. Для довільного $a \in R$ множина $(a) = \{ar : r \in R\}$ є ідеалом в R, який містить a. Це випливає з наступних тотожностей:

$$ar - ar' = a(r - r') \in I \quad \text{та} \quad (ar)r' = a(rr') \in I$$

для всіх $r, r' \in R$. Наприклад, в $\mathbb{Z}$ маємо $(3) = 3\mathbb{Z}$.

Властивості ідеалів

Твердження 11. *Перетин довільної родини (лівих, правих) ідеалів кільця R є (лівим, правим) ідеалом.*

Доведення. Нехай $\{I_\lambda\}_{\lambda\in\Lambda}$ – родина ідеалів в кільці R. Застосуємо критерій ідеалу до перетину $I = \cap_{\lambda\in\Lambda} I_\lambda$:

$$\begin{aligned} a, b \in I \quad &\Rightarrow \quad a, b \in I_\lambda \text{ для всіх } \lambda \in \Lambda \\ &\Rightarrow \quad a - b, ar \in I_\lambda \text{ для всіх } \lambda \in \Lambda, r \in R \\ &\Rightarrow \quad a - b, ar \in I \end{aligned}$$

□

Означення 10. Нехай A – довільна підмножина кільця R. Ідеал

$$(A) = \bigcap_{A\subset I,\ I \text{ – ідеал}} I$$

називається *ідеалом, породженим множиною* A. Еквівалентно, (A) – це найменший (за включенням) ідеал, який містить A (зрозумійте чому).

Ідеал, породжений одним елементом, називається *головним*. Ідеал, породжений скінченною множиною, називається *скінченно породженим*.

Твердження 12 (будова головних ідеалів)**.** *Нехай R – кільце, $a \in R$ і $A \subset R$. Тоді:*

1) $(a) = \{ra+as+na+r_1as_1+\ldots+r_mas_m : r, s, r_i, s_i \in R, n \in \mathbb{Z}, m \in \mathbb{N}\}$;

2) якщо $1 \in R$, *то*

$$(a) = RaR = \{r_1as_1 + \ldots + r_mas_m : r_i, s_i \in R, m \in \mathbb{N}\};$$

3) якщо $1 \in R$ *і* R *– комутативне, то*

$$(a) = aR = Ra = \{ar : r \in R\};$$

4) $aR = \{ar : r \in R\}$ *– правий ідеал;*
$Ra = \{ra : r \in R\}$ *– лівий ідеал;*

5) якщо $1 \in R$ *і* R *– комутативне, то*

$$(A) = \{r_1a_1 + \ldots + r_na_n : r_i \in R, a_i \in A, n \in \mathbb{N}\}.$$

Доведення. Ми доведемо пункт 1), інші пункти доводяться аналогічно. Зрозуміло, що оскільки ідеал (a) містить елемент a, то він має містити всі добутки $ra, as, r_i a s_i, na$ та їх суми (ви зрозуміли, що таке na?). Отже, множина з лівого боку рівності, позначимо її I, міститься в (a). З іншого боку, неважко перевірити, що множина I задовольняє критерію ідеалу, і сама є ідеалом. Оскільки (a) – це найменший ідеал, що містить a, і $a \in I$, то отримуємо $(a) = I$. □

Приклади 5. 1. Нульовий ідеал в будь-якому кільці є головним: $(0) = \{0\}$. Все кільце не обов'язково є головним ідеалом (можна взяти довільний неголовний ідеал як саме кільце, див. приклад 4 нижче). Але, якщо кільце містить одиницю, то $R = (1)$.

2. В кільці $\mathbb{Z}$ всі ідеали головні, оскільки кожен ідеал має вигляд $n\mathbb{Z}$ і $n\mathbb{Z} = (n)$.

3. Аналогічно в кільці многочленів $F[x]$ над полем F всі ідеали головні. Доведемо цей факт. Нехай I – нетривіальний ідеал в $F[x]$, тобто $I \neq \{0\}$ і $I \neq F[x]$. Ідеал I містить деякий ненульовий многочлен $g(x)$ найменшого степеня. Причому $g(x)$ не може бути константою, оскільки інакше $g(x) \in F^*$ є оборотним, і тоді $I = F[x]$. Отже, $\deg g(x) \geq 1$. Візьмемо довільний ненульовий $f(x) \in I$ і поділимо $f(x)$ на $g(x)$ з остачею:

$$f(x) = g(x)q(x) + r(x), \quad \text{де } r(x) \equiv 0 \text{ або } \deg r(x) < \deg g(x).$$

Випадок $\deg r(x) < \deg g(x)$ є неможливим, оскільки $r(x) = f(x) - g(x)q(x)$ належить ідеалу I і не може мати степінь менше $g(x)$ за вибором $g(x)$. Отже, $r(x) \equiv 0$ і $f(x)$ ділиться на $g(x)$. Звідси маємо $I = (g(x))$.

4. Вкажемо приклад не головного ідеалу. В кільці $\mathbb{Z}[x]$ розглянемо ідеал

$$\begin{aligned}(2, x) &= \{2f(x) + xg(x) : f(x), g(x) \in \mathbb{Z}[x]\} = \\ &= \{2m + a_1 x + \ldots + a_n x^n : m, a_i \in \mathbb{Z}, n \in \mathbb{N}\}.\end{aligned}$$

Припустимо цей ідеал є головним і $(2, x) = (a(x))$ для деякого $a(x) \in \mathbb{Z}[x]$. Оскільки $2 \in (a(x))$, то $2 = a(x)b(x)$ і, отже, $a(x) \in \{\pm 1, \pm 2\}$. Якщо $a(x) = \pm 1$, то $(1) = (-1) = \mathbb{Z}[x] \neq (2, x)$. Якщо $a(x) = \pm 2$, то $(2) = (-2) = \{2f(x) : f(x) \in \mathbb{Z}[x]\} \not\ni x$ і $(2) \neq (2, x)$. Протиріччя. Отже, ідеал $(2, x)$ в кільці $\mathbb{Z}[x]$ не є головним.

Твердження 13. *Нехай R – комутативне кільце з $1 \neq 0$. Тоді R є полем тоді і лише тоді, коли єдиними ідеалами в R є тривіальні ідеали $\{0\}$ і R.*

Доведення. В прикладі 4.1 ми довели твердження в один бік: поле містить тільки тривіальні ідеали. Навпаки, візьмемо ненульовий елемент $a \in R$. Тоді ідеал (a) – ненульовий і, отже, має співпадати з R (інших ідеалів немає). Оскільки $1 \in R = (a)$, то існує $b \in R$ такий, що $ab = 1$. Отже, кожен ненульовий елемент є оборотним, і R є полем. □

Операції з ідеалами

Нехай I, J – ідеали кільця R.

Означення 11. *Сумою ідеалів I* і *J* називається множина $I + J = \{a + b : a \in I, b \in J\}$.

Добутком ідеалів I і *J* називається множина $IJ = \{a_1b_1 + \ldots + a_nb_n : a_i \in I, b_i \in J, n \in \mathbb{N}\}$.

Зауваження 4. Сума $I + J$ – це найменший ідеал кільця R, що містить I і J. Дійсно, неважко перевірити, що $I + J$ є ідеалом і I та J містяться в $I + J$. З іншого боку, кожен ідеал, який містить I та J, повинен містити суми $a + b$ для $a \in I$, $b \in J$, а отже, має містити $I + J$. Тому для головних ідеалів можна записати рівність $(a) + (b) = (a, b)$.

Зауважимо, що для $a \in I$, $b \in J$ добуток ab міститься і в I, і в J, а отже, і в перетині $I \cap J$. Зокрема, $IJ \subset I \cap J$.

Твердження 14. *Нехай $I_1, \ldots, I_n$ – ідеали в кільці R. Тоді*

1) $I_1 + I_2 + \ldots + I_n$ і $I_1I_2 \ldots I_n$ – ідеали;

2) $(I_1I_2)I_3 = I_1(I_2I_3)$;

3) $J(I_1 + \ldots + I_n) = JI_1 + \ldots + JI_n$, $(I_1 + \ldots + I_n)J = I_1J + \ldots + I_nJ$.

Доведення. 1) Достатньо довести для $n = 2$ та ідеалів I, J. Застосуємо критерій ідеалу до суми $I + J$:

$$\begin{aligned} (a+b) - (a'+b') &= (a-a') + (b-b') \in I + J, \\ r(a+b) = ra + rb \in I + J, &\qquad (a+b)r = ar + br \in I + J \end{aligned}$$

для всіх $a, a' \in I$, $b, b' \in J$, $r \in R$. Аналогічно для добутку IJ:

$$\begin{aligned} & (a_1b_1 + \ldots + a_nb_n) - (a'_1b'_1 + \ldots + a'_mb'_m) = \\ = \; & a_1b_1 + \ldots + a_nb_n + (-a'_1)b'_1 + \ldots + (-a'_m)b'_m \in I + J, \\ & r(a_1b_1 + \ldots + a_nb_n) = (ra_1)b_1 + \ldots + (ra_n)b_n \in I + J, \\ & (a_1b_1 + \ldots + a_nb_n)r = a_1(b_1r) + \ldots + a_n(b_nr) \in I + J \end{aligned}$$

для всіх $a_i, a'_i \in I$, $b_i, b'_i \in J$, $r \in R$.

2),3) – самостійно. □

Приклади 6. В кільці $\mathbb{Z}$ виконується

$$n\mathbb{Z} + m\mathbb{Z} = d\mathbb{Z}, \quad n\mathbb{Z} \cap m\mathbb{Z} = l\mathbb{Z}, \quad n\mathbb{Z} \cdot m\mathbb{Z} = nm\mathbb{Z},$$

де $d = \text{НСД}(n, m)$ і $l = \text{НСК}(n, m)$. Для прикладу, розглянемо ідеали $6\mathbb{Z}$ і $10\mathbb{Z}$. Тоді

$$\begin{aligned} 6\mathbb{Z} + 10\mathbb{Z} &= \{6n + 10m : n, m \in \mathbb{Z}\} = 2\mathbb{Z}, \\ 6\mathbb{Z} \cdot 10\mathbb{Z} &= \{(6n_1)(10m_1) + \ldots + (6n_k)(10m_k) : n_i, m_i \in \mathbb{Z}\} = 60\mathbb{Z}, \\ 6\mathbb{Z} \cap 10\mathbb{Z} &= 30\mathbb{Z}. \end{aligned}$$

Вправи

1. Доведіть пункти 2)-5) твердження 12.

2. Нехай S – підкільце кільця R. Доведіть, що $S \cap I$ є ідеалом кільця S для кожного ідеалу I кільця R. Наведіть приклад, коли не кожен ідеал в S має вигляд $S \cap I$ для деякого ідеалу I в R.

3. Нехай R – комутативне кільце. Доведіть, що множина нільпотентних елементів $N(R)$ утворює ідеал. Наведіть приклад некомутативного кільця R, в якому $N(R)$ не є ідеалом.

4. Нехай R – кільце з 1. Доведіть, що кожен ідеал в кільці матриць $M_n(R)$ має вигляд $M_n(I)$ для деякого ідеалу I в R.

5. Доведіть, що добуток двох скінченно породжених ідеалів в комутативному кільці є скінченно породженим ідеалом.

§ 4 Гомоморфізми і факторкільця

Нехай R і S – кільця.

Означення 12. Відображення $\varphi : R \to S$ називається *гомоморфізмом кілець*, якщо для всіх $a, b \in R$ виконується

$$\varphi(a+b) = \varphi(a) + \varphi(b) \quad \text{і} \quad \varphi(ab) = \varphi(a)\varphi(b).$$

Означення 13. Бієктивний гомоморфізм називається *ізоморфізмом*. Кільця R і S називаються *ізоморфними*, позначається $R \cong S$, якщо існує ізоморфізм $\varphi : R \to S$.

Ізоморфізм $R \to R$ називається *автоморфізмом* кільця R.

Сюр'єктивний гомоморфізм називається *епіморфізмом*.

Ін'єктивний гомоморфізм називається *мономорфізмом*. Мономорфізм кілець $R \to S$ також називається *вкладенням* R в S.

Гомоморфізм кілець також є гомоморфізмом відповідних адитивних груп. Тому ми можемо застосовувати відомі теореми про гомоморфізми груп до гомоморфізмів кілець. Так само, як в теорії груп, важливу роль відіграє ядро гомоморфізму.

Означення 14. *Ядром гомоморфізму* $\varphi : R \to S$ називається множина $\operatorname{Ker}\varphi = \{r \in R : \varphi(r) = 0\}$.

Приклади 7. 1. Для кожного $n \in \mathbb{N}$ відображення $\varphi_n : \mathbb{Z} \to \mathbb{Z}_n$, $\varphi_n(a) = a \bmod n$, є гомоморфізмом кілець з ядром $n\mathbb{Z}$.

2. Гомоморфізм адитивних груп кілець не обов'язково є гомоморфізмом кілець. Наприклад, розглянемо відображення $\varphi_n : \mathbb{Z} \to \mathbb{Z}$, визначене за правилом $\varphi_n(a) = na$ $(n \in \mathbb{Z})$. Відображення φ_n є гомоморфізмом адитивних груп для всіх n:

$$\varphi_n(a+b) = n(a+b) = na + nb = \varphi_n(a) + \varphi_n(b).$$

Але $\varphi_n(ab) = nab$, а $\varphi_n(a)\varphi_n(b) = n^2ab$. Отже, φ_n є гомоморфізмом кілець тільки, коли $n^2 = n$, тобто $n = 0, 1$.

3. Відображення $\varphi : \mathbb{R}[x] \to \mathbb{R}$, визначене за правилом $\varphi(f(x)) = f(0)$, є гомоморфізмом кілець:

$$\varphi(f(x) + g(x)) = (f+g)(0) = f(0) + g(0) = \varphi(f(x)) + \varphi(g(x)),$$
$$\varphi(f(x)g(x)) = (fg)(0) = f(0)g(0) = \varphi(f(x)) + \varphi(g(x)).$$

Більш загально, розглянемо кільце функцій $R^X = \{f : X \to R\}$ з множини X в кільце R. Для кожної точки $a \in X$ відображення "обчислення в точці"

$$\varphi_a : R^X \to R, \quad \varphi_a(f(x)) = f(a)$$

є гомоморфізмом кілець (доводиться як і вище).

Твердження 15. *Нехай $\varphi : R \to S$ – гомоморфізм кілець. Тоді*

1) образ $\operatorname{Im}\varphi$ є підкільцем в S;

2) ядро $\operatorname{Ker}\varphi$ є ідеалом в R.

Доведення. 1) Застосовуємо критерій підкільця: для всіх $s_1, s_2 \in \operatorname{Im}\varphi$ виконується

$$\begin{array}{l} s_1 = \varphi(r_1) \\ s_2 = \varphi(r_2) \end{array} \Rightarrow \begin{array}{l} \varphi(r_1 - r_2) = s_1 - s_2 \in \operatorname{Im}\varphi \\ \varphi(r_1 r_2) = s_1 s_2 \in \operatorname{Im}\varphi \end{array} \Rightarrow \operatorname{Im}\varphi \text{ — підкільце.}$$

2) Застосовуємо критерій ідеалу: для всіх $a_1, a_2 \in \operatorname{Ker}\varphi$ і $r \in R$ виконується

$$\varphi(a_1) = \varphi(a_2) = 0 \;\Rightarrow\; \varphi(a_1 - a_2) = 0 \;\Rightarrow\; r_1 - r_2 \in \operatorname{Ker}\varphi,$$
$$\varphi(ra) = \varphi(r)\varphi(a) = \varphi(r)0 = 0 \;\Rightarrow\; ra \in \operatorname{Ker}\varphi,$$
$$\varphi(ar) = \varphi(a)\varphi(r) = 0\varphi(r) = 0 \;\Rightarrow\; ar \in \operatorname{Ker}\varphi.$$

Отже, $\operatorname{Ker}\varphi$ є ідеалом в кільці R. □

Факторкільця

Нехай I – ідеал кільця R. Тоді I є підгрупою адитивної групи кільця $(R,+)$, а оскільки остання група є абелевою за означенням кільця, то I є нормальною підгрупою. Ми можемо розглянути факторгрупу R/I, елементами якої є класи суміжності $a+I, a \in R$, а операція додавання визначається за правилом

$$(a+I)+(b+I)=(a+b)+I.$$

Визначимо операцію множення $(a+I)(b+I)=ab+I$.

Твердження 16. *Група R/I з таким чином визначеною операцією множення є кільцем, яке називається факторкільцем.*

Якщо R – комутативне, то R/I теж комутативне.

Якщо R – кільце з 1, то R/I теж кільце з $1=1+I$.

Доведення. Перевіримо коректність множення, тобто, що воно не залежить від вибору представників класів. Нехай $a+I=a'+I$ і $b+I=b'+I$, і нам потрібно перевірити, що $a'b'+I=ab+I$. Маємо $a'=a+i$ і $b'=b+j$ для деяких $i,j \in I$. Використовуючи властивості ідеалів, отримуємо

$$a'b'+I=(a+i)(b+j)+I=ab+aj+ib+ij+I=ab+I,$$

де остання рівність випливає з $aj+ib+ij \in I$. Зверніть увагу, що з коректності множення можна вивести означення ідеалу (як?).

Інші властивості перевіряються безпосередньо і залишаються як вправа. □

Як в теорії груп існує тісний зв'язок між нормальними підгрупами і гомоморфізмами груп, так і в теорії кілець ідеали тісно пов'язані з гомоморфізмами кілець. Наступні теореми є прямими аналогами відповідних теорем з теорії груп (див. [3, Розділ 4.2]).

Теорема 17 (Перша теорема про гомоморфізм). *1. Якщо $\varphi : R \to S$ – гомоморфізм кілець, то* $\operatorname{Im}\varphi \cong R/\operatorname{Ker}\varphi$.

2. Якщо I – ідеал кільця R, то відображення

$$\pi : R \to R/I, \qquad \pi(a) = a + I$$

є сюр'єктивним гомоморфізмом з ядром I, який називається канонічною проекцією з R на R/I або канонічним епіморфізмом.

Зокрема, множина ідеалів в кільці R співпадає з множиною ядер гомоморфізмів, визначених на R.

Доведення. 1) З першої теореми про гомоморфізм груп ми знаємо, що відображення

$$\psi : R/\mathrm{Ker}\,\varphi \to \mathrm{Im}\,\varphi, \qquad \psi(a + \mathrm{Ker}\,\varphi) = \varphi(a)$$

є ізоморфізмом адитивних груп. Залишається перевірити, що ψ зберігає множення:

$$\begin{aligned} \psi((a + \mathrm{Ker}\,\varphi)(b + \mathrm{Ker}\,\varphi)) &= \psi(ab + \mathrm{Ker}\,\varphi) = \varphi(ab) = \\ &= \varphi(a)\varphi(b) = \psi(a + \mathrm{Ker}\,\varphi)\psi(b + \mathrm{Ker}\,\varphi). \end{aligned}$$

Отже, ψ є ізоморфізмом кілець.

2) Аналогічно з теорії груп ми знаємо, що π є сюр'єктивним гомоморфізмом адитивних груп з ядром I. Перевіряємо, що π зберігає множення:

$$\pi(ab) = ab + I = (a + I)(b + I) = \pi(a)\pi(b).$$

□

Наступні теореми доводяться по такій самій схемі. З теорії груп відомо, що результат виконується для адитивних груп кілець, і просто перевіряємо, що при цьому зберігається множення.

Теорема 18 (Друга теорема про гомоморфізм)**.** *Нехай J – підкільце і I – ідеал кільця R. Тоді $I + J$ – підкільце R, $I \cap J$ – ідеал R і $(I + J)/I \cong I/(I \cap J)$.*

Теорема 19 (Третя теорема про гомоморфізм)**.** *Нехай I, J – ідеали кільця R і $I \subset J$. Тоді J/I – ідеал в R/I і $(R/I)/(J/I) \cong R/J$.*

Теорема 20 (Теорема про відповідність ідеалів)**.** *Нехай I – ідеал кільця R. Існує взаємно однозначна відповідність між множинами*

$$\{\textit{Ідеали } J \textit{ в кільці } R, \textit{ що містять } I\} \;\leftrightarrow\; \{\textit{Ідеали в } R/I\},$$

яка визначається за правилом $J \mapsto J/I$. Зокрема, кожен ідеал в R/I має вигляд J/I для деякого ідеалу J в R, що містить I.

Приклади 8. 1. З прикладу 7 ми знаємо, що $\varphi : \mathbb{Z} \to \mathbb{Z}_n$, $\varphi(a) = a \bmod n$, є гомоморфізмом кілець з ядром $\operatorname{Ker}\varphi = n\mathbb{Z}$. Отже, за першою теоремою про гомоморфізм маємо ізоморфізм кілець $\mathbb{Z}_n \cong \mathbb{Z}/n\mathbb{Z}$.

2. В полі F єдиними ідеалами є тривіальні ідеали $\{0\}$ і F. Отже, факторкільцями поля будуть лише $F/\{0\} = F$ і $F/F = \{0\}$, і нічого цікавого ми таким способом не отримуємо.

   Аналогічно, якщо $\varphi : F \to P$ – ненульовий гомоморфізм полів, то ядро $\operatorname{Ker}\varphi$ не співпадає з F. Отже, $\operatorname{Ker}\varphi = \{0\}$ (інших ідеалів немає) і φ є ін'єктивним. Тому для полів має сенс говорити тільки про вкладення. В той же час, поля можна отримувати як факторкільця деяких кілець.

3. Важливу роль в теорії кілець і полів відіграють факторкільця кільця многочленів. Розглянемо, наприклад, факторкільце $\mathbb{R}[x]/(f(x))$ кільця $\mathbb{R}[x]$ по головному ідеалу $(f(x))$. Ідеал $(f(x))$ складається з усіх многочленів, що діляться на $f(x)$. Тому якщо $\deg f(x) = n$, то в кожному класі суміжності $g(x) + (f(x))$ існує єдиний многочлен степеня $< n$ – це в точності остача при діленні $g(x)$ на $f(x)$ (доведіть!). Многочлени степеня $< n$ часто вибирають у якості представників класів суміжності, і тоді факторкільце записують у вигляді

   $$\mathbb{R}[x]/(f(x)) = \{a_0 + a_1x + \ldots + a_{n-1}x^{n-1} + (f(x)) : a_i \in \mathbb{R}\}.$$

   Також використовується позначення

   $$\overline{a_0 + a_1x + \ldots + a_{n-1}x^{n-1}} = a_0 + a_1x + \ldots + a_{n-1}x^{n-1} + (f(x)).$$

Сума таких многочленів обчислюється стандартно (покоординатно). При множенні ми можемо отримати многочлен степеня $\geq n$. В цьому випадку додатково обчислюють остачу при діленні на $f(x)$. Наприклад, в $\mathbb{R}[x]/(x^2+1)$ маємо

$$\overline{2-3x}\cdot\overline{1+2x}=\overline{2+x-6x^2}=\overline{8+x-6(x^2+1)}=\overline{8+x}.$$

А в кільці $\mathbb{R}[x]/(x^2)$ виконується $\overline{x}\cdot\overline{x}=\overline{x^2}=\overline{0}$, тобто елемент $\overline{x}$ є дільником нуля. Отже, факторкільце області цілісності може не бути областю цілісності.

4. Розглянемо кільце $C[a,b]$ неперервних дійсних функцій на відрізку $[a,b]$. Для кожного $c\in[a,b]$ відображення

$$\varphi: C[a,b]\to\mathbb{R},\qquad \varphi(f(x))=f(c)$$

є сюр'єктивним гомоморфізмом кілець з ядром $\operatorname{Ker}\varphi=\{f(x)\in C[a,b]: f(c)=0\}$. Отже, $C[a,b]/\operatorname{Ker}\varphi\cong\mathbb{R}$.

Аналогічно в довільному кільці функцій R^X виконується

$$R^X/\{f\in R^X: f(c)=0\}\cong R$$

для кожного $c\in X$.

5. Використаємо першу теорему про гомоморфізм, щоб довести $\mathbb{R}[x]/(x^2+1)\cong\mathbb{C}$. Для цього розглянемо гомоморфізм

$$\varphi:\mathbb{R}[x]\to\mathbb{C},\qquad \varphi(f(x))=f(i).$$

Оскільки $\varphi(a+bx)=a+bi$ для всіх $a,b\in\mathbb{R}$, то φ є сюр'єктивним. Знайдемо ядро $\operatorname{Ker}\varphi$. За означенням многочлен $f(x)\in\mathbb{R}[x]$ належить $\operatorname{Ker}\varphi$ тоді лише тоді, коли $f(i)=0$. Оскільки $f(x)$ має дійсні коефіцієнти, то з $f(i)=0$ випливає $f(-i)=0$. Отже, $f(x)$ має ділитися на $(x-i)(x+i)=x^2+1$. І навпаки, якщо $f(x)$ ділиться на x^2+1, то $f(i)=0$. Отже, ядро складається з многочленів, які діляться на x^2+1, тобто співпадає з головним ідеалом (x^2+1). За першою теоремою про гомоморфізм отримуємо $\mathbb{R}[x]/(x^2+1)\cong\mathbb{C}$.

6. Побудуємо матричне зображення поля комплексних чисел $\mathbb{C}$. В кільці $M_2(\mathbb{R})$ розглянемо підкільце

$$S = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} : a, b \in \mathbb{R} \right\}$$

і визначимо відображення

$$\varphi : S \to \mathbb{C}, \qquad \varphi\left(\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \right) = a + bi.$$

Неважко перевірити, що φ є ізоморфізмом.

7. Нехай R – кільце і I – ідеал в R. Тоді $M_n(I)$ – ідеал в кільці матриць $M_n(R)$. Відображення $\varphi : M_n(R) \to M_n(R/I)$, яке діє за правилом $(a_{ij}) \mapsto (a_{ij} + I)$, є сюр'єктивним гомоморфізмом з ядром $M_n(I)$. Отже, $M_n(R)/M_n(I) \cong M_n(R/I)$.

8. Опишемо факторкільце $\mathbb{Z}[i]/(3+i)$. Для цього розглянемо гомоморфізм

$$\varphi : \mathbb{Z} \to \mathbb{Z}[i]/(3+i), \qquad \varphi(n) = \overline{n} = n + (3+i).$$

В кільці $\mathbb{Z}[i]/(3+i)$ виконується $\overline{3+i} = \overline{0}$, і тому $\overline{i} = \overline{-3}$. Тоді

$$\varphi(a - 3b) = \overline{a - 3b} = \overline{a} + \overline{-3b} = \overline{a} + \overline{i}\overline{b} = \overline{a + bi},$$

і, отже, φ є сюр'єктивним. Доведемо, що $\operatorname{Ker}\varphi = 10\mathbb{Z}$. Оскільки $10 = (3+i)(3-i)$, то $10\mathbb{Z} \subset \operatorname{Ker}\varphi$. Навпаки, якщо $n \in \operatorname{Ker}\varphi$, то n ділиться на $3+i$ та існують $a, b \in \mathbb{Z}$ такі, що

$$n = (3+i)(a+bi) = (3a - b) + i(a + 3b).$$

Оскільки $n \in \mathbb{Z}$, то уявна частина з рівності має дорівнювати нулю. Отже, $a = -3b$ і $n = -10b \in 10\mathbb{Z}$. Таким чином, ми отримуємо, що $\mathbb{Z}[i]/(3+i) \cong \mathbb{Z}_{10}$. Також можна безпосередньо перевірити, що відображення

$$\psi : \mathbb{Z}[i]/(3+i) \to \mathbb{Z}_{10}, \qquad \psi(a+bi) = a - 3b$$

є ізоморфізмом кілець (тут важливо, що $\overline{3}^2 = -\overline{1}$, тобто $\overline{3}$ є коренем з $-\overline{1}$ в кільці в $\mathbb{Z}_{10}$, так само, як i в $\mathbb{C}$). Можна описати і всі факторкільця кільця цілих гаусових чисел, але це не так просто і ми не будемо цього робити. Зацікавлений читач може почитати як це робиться в роботі [6].

Вправи

1. Чи є слід і детермінант гомоморфізмами кільця $M_n(\mathbb{R})$?
2. Перевірте, що відображення $\varphi : S \to \mathbb{C}$, визначене в прикладі 8.6., є ізоморфізмом.
3. Побудуйте таблицю множення для факторкільця $\mathbb{Z}_2[x]/(x^2+1)$.
4. Доведіть, що кільце $M_4(\mathbb{R})$ містить підкільце ізоморфне тілу кватерніонів $\mathbb{H}$.
5. Чи ізоморфні кільця $\mathbb{R}[x]/(x^2-1)$, $\mathbb{R}[x]/(x^2+1)$ і $\mathbb{R}[x]/(x^2)$?

§ 5 Прості ідеали та максимальні ідеали

На даний момент ми знаємо не так багато полів: $\mathbb{Q}, \mathbb{Q}[\sqrt{D}], \mathbb{R}, \mathbb{C}$ і $\mathbb{Z}_p$ для простого p. Крім того, на відміну від кілець, де є конструкції факторкільця, прямого добутку, кільця многочленів, кільця матриць, кільця функцій тощо, які дозволяють будувати нові кільця з вже відомих, ми не маємо конструкції, яка б дозволила будувати нові поля. Далі ми спробуємо зрозуміти, для яких ідеалів факторкільце є полем, що дозволить будувати нові поля з кілець.

Означення 15. Ідеал M кільця R називається *максимальним*, якщо $M \neq R$ і єдиними ідеалами, що містять M, є M і R.

$$M \subseteq J \subseteq R \;\Rightarrow\; J = M \text{ або } J = R$$

Не в кожному кільці існують максимальні ідеали, але в кільці з $1 \neq 0$ можна довести, використовуючи лему Цорна, що кожен ідеал міститься в максимальному ідеалі.

Теорема 21. *Нехай R – комутативне кільце з 1 і M – ідеал в R. Тоді M є максимальним тоді і лише тоді, коли факторкільце R/M є полем.*

Доведення. Щоб краще розібратися, ми доведемо теорему двома способами. Перший спосіб буде оснований на теоремі про відповідність ідеалів, а другий – за означенням.

Перше доведення. За теоремою 20 існує взаємно однозначна відповідність між ідеалами в R, що містять M, та ідеалами в R/M. За означенням ідеал M є максимальним тоді і лише тоді, коли проміжні ідеали тільки M та R. Це еквівалентно умові, що єдиними ідеалами в R/M є тривіальні ідеали $\{0+M\}$ та R/M. За твердженням 13 це можливо тоді і лише тоді, коли R/M є полем. Помітимо, що $M \neq R$, оскільки в полі R/M не менше двох елементів.

Друге доведення. Необхідність. Нехай M – максимальний ідеал в кільці R. Кільце R/M є комутативним з $1 = 1+M$, причому $1+M \neq 0+M$, оскільки $M \neq R$. Візьмемо ненульовий елемент $a + M \in R/M$ (тобто $a \notin M$) і доведемо, що він має обернений.

Розглянемо множину $J = \{ra + m : r \in R, m \in M\}$. Тоді $M \subsetneq J$. Покажемо, що J – ідеал кільця R. За критерієм ідеалу маємо:

$$\begin{aligned}(r_1a + m_1) - (r_2a + m_2) &= (r_1 - r_2)a + (m_1 - m_2) \in J,\\ r'(ra + m) &= r'ra + r'm \in J\end{aligned}$$

для всіх $r, r', r_i \in R$ та $m_i \in M$. Оскільки ідеал M є максимальним, то $J = R$. Отже, $1 \in J$ та існують $b \in R$ і $m \in M$ такі, що $ba + m = 1$. Тоді

$$1 + M = ab + m + M = ab + M = (a + M)(b + M).$$

Отже, $b + M$ є оберненим до $a + M$, і R/M є полем.

Достатність. Нехай факторкільце R/M є полем. Тоді $0+M \neq 1+M$ і, отже, $M \neq R$. Нехай J – ідеал в R і $M \subsetneq J$. Візьмемо довільний елемент $a \in J$, $a \notin M$. Тоді $a + M \neq 0 + M$ і елемент $a + M$ має обернений в полі R/M: існує $b + M$ такий, що $(a + M)(b + M) = ab + M = 1 + M$. Отже, існує $m \in M$ такий, що $ab + m = 1$. Але $ab + m \in J$ за властивостями ідеалів. Отже, $1 \in J$ і $J = R$. □

Приклади 9. 1. В кільці $\mathbb{Z}$ ідеал $n\mathbb{Z}$ є максимальним тоді і лише тоді, коли n – просте число, оскільки тільки в цьому випадку $\mathbb{Z}/n\mathbb{Z}$ є полем.

2. Розглянемо кільце $\mathbb{Z}[i]$ і доведемо, що ідеал

$$M = (3) = \{a + bi \in \mathbb{Z}[i] : a \text{ і } b \text{ діляться на } 3\}$$

є максимальним. Нехай M міститься в деякому ідеалі J і $M \neq J$. Візьмемо елемент $a+bi \in J$ такий, що a або b не ділиться на 3. Тоді a^2+b^2 теж не ділиться на 3 (доведіть!). Отже, НСД$(3, a^2+b^2) = 1$ і існують $u, v \in \mathbb{Z}$ такі, що $3u + (a^2+b^2)v = 1$. За визначенням $3 \in J$, а оскільки J – ідеал, то і $a^2+b^2 = (a+ib)(a-ib) \in J$. Отже, $1 \in J$ і $J = \mathbb{Z}[i]$. Ми довели, що M – максимальний ідеал, а $\mathbb{Z}[i]/M$ є полем (скільки в ньому елементів?).

Не для кожного простого числа p головний ідеал (p) в кільці $\mathbb{Z}[i]$ є максимальним. Наприклад, ідеал (5) не є максимальним. Це випливає з того, що $5 = (2+i)(2-i)$ і в факторкільці $\mathbb{Z}[i]/(5)$ маємо дільники нуля $2 \pm i + (5)$. Пізніше ми опишемо всі такі прості числа.

3. Ідеал (x) в $\mathbb{R}[x]$ є максимальним, оскільки $\mathbb{R}[x]/(x) \cong \mathbb{R}$ – поле. Але в $\mathbb{Z}[x]$ ідеал (x) – не максимальний, оскільки $\mathbb{Z}[x]/(x) \cong \mathbb{Z}$ – не поле; також можна вказати проміжний ідеал: $(x) \subset (2, x) \subset \mathbb{Z}[x]$. Оскільки $\mathbb{Z}[x]/(2, x) \cong \mathbb{Z}_2$ є полем, то ідеал $(2, x)$ – максимальний. Коли ми будемо вивчати поля, то доведемо, що кожне скінченне поле можна побудувати як факторкільце кільця $\mathbb{Z}[x]$ по деякому максимальному ідеалу.

4. В кільці функцій $R = \{f : [a, b] \to \mathbb{Q}\}$ для кожної точки $c \in [a, b]$ ідеал

$$M_c = \{f(x) \in R : f(c) = 0\}$$

є максимальним, оскільки $R/M_c \cong \mathbb{Q}$ – поле.

Нехай R – комутативне кільце.

Означення 16. Ідеал I кільця R називається *простим*, якщо $I \neq R$ і для довільних $a, b \in R$ з умови $ab \in I$ випливає $a \in I$ або $b \in I$.

$$ab \in I \;\Rightarrow\; a \in I \text{ або } b \in I$$

Термін "простий ідеал" пояснюється аналогією з наступною властивістю простих чисел: якщо просте число p ділить добуток цілих чисел ab, то p ділить a або b.

Теорема 22. *Нехай R – комутативне кільце з 1 і I – ідеал в R. Тоді I є простим тоді і лише тоді, коли R/I є областю цілісності.*

Доведення. Необхідність. Нехай I – простий ідеал. Кільце R/I є комутативним з $1 = 1 + I$, причому $1 + I \neq 0 + I$, оскільки $I \neq R$. Шукаємо дільники нуля:

$$ab + I = (a + I)(b + I) = 0 + I \;\Rightarrow\; ab \in I \;\Rightarrow\; a \in I \text{ або } b \in I,$$

тобто $a + I = 0 + I$ або $b + I = 0 + I$. Отже, дільників нуля немає і R/I є областю цілісності.

Достатність. Нехай R/I – область цілісності. З умови $1 + I \neq 0 + I$ випливає, що $I \neq R$. Нехай $ab \in I$ для деяких $a, b \in R$. Тоді $(a+I)(b+I) = ab + I = 0 + I$, а оскільки R/I не містить дільників нуля, то $a + I = 0 + I$ або $b + I = 0 + I$, іншими словами $a \in I$ або $b \in I$. Отже, ідеал I – простий. □

Оскільки кожне поле є областю цілісності, ми отримуємо наступний результат.

Наслідок 23. *Кожний максимальний ідеал в комутативному кільці з 1 є простим ідеалом.*

Приклади 10. 1. В кільце $\mathbb{Z}$ ідеал $n\mathbb{Z}$ є простим тоді і лише тоді, коли n є простим числом або $n = 0$. Зокрема, додатне ціле число n є простим тоді і лише тоді, коли $n\mathbb{Z}$ є простим ідеалом в $\mathbb{Z}$. Це дає пояснення слову "простий" в означенні простого ідеалу.

2. Як ми зауважили в попередньому прикладі, ідеал (x) в $\mathbb{Z}[x]$ не є максимальним, але є простим, оскільки $\mathbb{Z}[x]/(x) \cong \mathbb{Z}$ – область цілісності. Також нульовий ідеал $\{0\}$ є простим в $\mathbb{Z}[x]$, але не є максимальним.

3. Розглянемо головні ідеали $(f(x))$ в кільці многочленів $F[x]$ над полем F. Якщо многочлен $f(x)$ – незвідний, то кожен многочлен $g(x) \notin (f(x))$ є взаємно простим з $f(x)$. Отже, існують $u(x), v(x) \in F[x]$ такі, що $u(x)f(x) + v(x)g(x) = 1$. Тому в факторкільці $F[x]/(f(x))$ маємо $\overline{v(x)} \cdot \overline{g(x)} = \overline{1}$ і елемент $\overline{g(x)}$ є оборотним. Отже, $F[x]/(f(x))$ є полем, а ідеал $(f(x))$ – максимальний і простий. Навпаки, якщо ідеал $(f(x))$ є максимальним, то він є простим. Якщо припустити, що $f(x)$ – звідний і $f(x) = a(x)b(x)$, то $a(x)b(x) \in (f(x))$. Звідси отримуємо $a(x) \in (f(x))$ або $b(x) \in (f(x))$, тобто $f(x)$ ділить $a(x)$ або $b(x)$. Отже, $f(x)$ є незвідним.

   Наприклад, за основною теоремою алгебри маємо, що максимальні ідеали в $\mathbb{C}[x]$ мають вигляд $(x - z)$ для $z \in \mathbb{C}$. Цікаво (і це не випадково), що існує взаємно однозначна відповідність $z \mapsto (x - z)$ між $\mathbb{C}$ та множиною максимальних ідеалів в $\mathbb{C}[x]$.

Вправи

1. Доведіть, що ідеал $(2 + i)$ є максимальним в кільці $\mathbb{Z}[i]$.

2. Знайдіть всі максимальні ідеали в кільці формальних степеневих рядів $F[[x]]$ над полем F.

3. Нехай R – скінченне комутативне кільце з 1. Доведіть, що кожен простий ідеал в R є максимальним.

4. Нехай P – простий ідеал в комутативному кільці R. Доведіть, що якщо $IJ \subset P$ для деяких ідеалів I і J, то $I \subset P$ або $J \subset P$.

5. Нехай R – комутативне кільце з 1. Доведіть, що R містить точно один простий ідеал тоді і лише тоді, коли кожен необоротний елемент кільця є нільпотентним.

§ 6 Китайська теорема про остачі

В цьому розділі всі кільця будуть комутативними з $1 \neq 0$.

Означення 17. *(Зовнішнім) прямим добутком* кілець $R_1, \ldots, R_n$ називається множина $R_1 \times \ldots \times R_n = \{(a_1, \ldots, a_n) : a_i \in R_i\}$ з операціями

$$\begin{aligned}(a_1, \ldots, a_n) + (b_1, \ldots, b_n) &= (a_1 + b_1, \ldots, a_n + b_n),\\ (a_1, \ldots, a_n) \cdot (b_1, \ldots, b_n) &= (a_1 b_1, \ldots, a_n b_n).\end{aligned}$$

Легко перевірити, що $R_1 \times \ldots \times R_n$ є комутативним кільцем з 1. Кожне кільце R_k вкладається в прямий добуток, а також є гомоморфним образом прямого добутку:

$$\begin{array}{rcl} \imath_k : R_k & \to & R_1 \times \ldots \times R_n, \\ a_k & \mapsto & (0, \ldots, a_k, \ldots, 0), \end{array} \qquad \begin{array}{rcl} \pi_k : R_1 \times \ldots \times R_n & \to & R_k \\ (a_1, \ldots, a_n) & \mapsto & a_k \end{array}$$

є ін'єктивним і сюр'єктивним гомоморфізмом відповідно. Образи

$$I_k = \operatorname{Im} \imath_k = \{0\} \times \ldots \times R_k \times \ldots \times \{0\}$$

є ідеалами в кільці $R_1 \times \ldots \times R_n$. З будови цих ідеалів одразу видно, що виконуються такі властивості:

$$I_1 + \ldots + I_n = R_1 \times \ldots \times R_n,$$
$$I_k \cap (I_1 + \ldots + I_{k-1} + I_{k+1} + \ldots + I_n) = \{0\} \text{ для всіх } k = 1, \ldots, n.$$

Наступне твердження показує, що ці властивості повністю характеризують прямий добуток.

Твердження 24. *Нехай $I_1, \ldots, I_n$ – ідеали в кільці R такі, що*

1) $I_1 + \ldots + I_n = R$;

2) $I_k \cap (I_1 + \ldots + I_{k-1} + I_{k+1} + \ldots + I_n) = \{0\}$ для $k = 1, \ldots, n$.

Тоді $R \cong I_1 \times I_2 \times \ldots \times I_n$.

Доведення. З теорії груп ми знаємо, що за умов 1), 2) відображення

$$\varphi : I_1 \times \ldots \times I_n \to R, \qquad \varphi((a_1, \ldots, a_n)) = a_1 + \ldots + a_n$$

є ізоморфізмом адитивних груп. Залишається перевірити, що φ зберігає множення. Зауважимо, що з умови 2) випливає $I_i \cap I_j = \{0\}$ при $i \neq j$. Оскільки для $a_i \in I_i$, $a_j \in I_j$ виконується $a_i a_j \in I_i \cap I_j = \{0\}$, то $a_i a_j = 0$. Отже,

$$(a_1 + \ldots + a_n)(b_1 + \ldots + b_n) = a_1 b_1 + \ldots + a_n b_n$$

і φ є гомоморфізмом кілець. □

Якщо кільце R і ідеали $I_1, \ldots, I_n$ задовольняють умовам 1), 2) з твердження, то кажуть, що R розкладається у *(внутрішній) прямий добуток своїх ідеалів* $I_1, \ldots, I_n$.

Теорема 25 (Китайська теорема про остачі)**.** *Нехай $I_1, I_2, \ldots, I_n$ – ідеали кільця R. Тоді відображення*

$$\begin{aligned} \varphi : \quad & R \to R/I_1 \times R/I_2 \times \ldots \times R/I_n, \\ & r \mapsto (r + I_1, r + I_2, \ldots, r + I_n) \end{aligned}$$

є гомоморфізмом кілець з ядром $I_1 \cap I_2 \cap \ldots \cap I_n$.

Якщо $I_i + I_j = R$ для всіх $i \neq j$, то $I_1 \cap I_2 \cap \ldots \cap I_n = I_1 I_2 \ldots I_n$ і φ – сюр'єктивне. Зокрема,

$$R/I_1 I_2 \ldots I_n \cong R/I_1 \times R/I_2 \times \ldots \times R/I_n.$$

Доведення. Спочатку розглянемо випадок $n = 2$. Нехай $I = I_1$ і $J = I_2$. З означення факторкільця одразу отримуємо, що відображення

$$\varphi : R \to R/I \times R/J \qquad \varphi(r) = (r + I, r + J)$$

є гомоморфізмом. Знаходимо ядро:

$$\begin{aligned} \operatorname{Ker} \varphi &= \{r \in R : r + I = I \text{ і } r + J = J\} = \\ &= \{r \in R : r \in I, r \in J\} = I \cap J. \end{aligned}$$

Ті самі міркування працюють для довільного n. Нехай тепер $I+J=R$ і доведемо, що $\operatorname{Im}\varphi = R$. Оскільки $I+J=R$ і $1\in R$, то існують $a\in I, b\in J$ такі, що $a+b=1$. Тоді

$$\begin{aligned}\varphi(a) &= (a+I, a+J) = (I, 1-b+J) = (I, 1+J),\\ \varphi(b) &= (b+I, b+J) = (1-a+I, b+J) = (1+I, J).\end{aligned}$$

Для всіх $(r_1+I, r_2+J)\in R/I\times R/J$ виконується

$$\begin{aligned}\varphi(r_2a+r_1b) = \varphi(r_2)\varphi(a)+\varphi(r_1)\varphi(b) &= (r_2+I, r_2+J)(I, 1+J)+\\ &+(r_1+I, r_1+J)(1+I, J) = (I, r_2+J)+(r_1+I, J) =\\ &= (r_1+I, r_2+J).\end{aligned}$$

Отже, φ – сюр'єкція.

Перевіримо, що $I\cap J = IJ$. Включення $IJ\subset I\cap J$ виконується для ідеалів завжди. Навпаки, нехай $c\in I\cap J$. Тоді $c = c\cdot 1 = ca+cb\in IJ$. Отже, $I\cap J\subset IJ$.

За індукцією випадок довільного n зводиться до $n=2$ і двох ідеалів I_1 та $I_2\dots I_n$. Потрібно тільки довести, що виконується умова $I_1+I_2I_3\dots I_n = R$. Оскільки $I_1+I_j=R$, то $a_j+b_j=1$ для деяких $a_j\in I_1$ і $b_j\in I_j$. Тоді

$$1 = (a_2+b_2)\cdot\ldots\cdot(a_n+b_n) = a+b_2\cdots b_n,$$

де $a\in I_1$. Отже, ідеал $I_1+I_2\dots I_n$ містить одиницю і збігається з R. □

Зауваження 5. Умову $1\in R$ можна замінити на $R^2+I_k=R$ для всіх k.

Ідеали I та J кільця R, для яких $I+J=R$, називаються *взаємно простими*. Назва пояснюється наступним спостереженням: в кільці $\mathbb{Z}$ головні ідеали (n) і (m) є взаємно простими тоді і лише тоді, коли числа n і m є взаємно простими.

Наслідок 26. *Нехай $n = p_1^{n_1}p_2^{n_2}\dots p_k^{n_k}$ – канонічний розклад у добуток простих. Тоді маємо ізоморфізм кілець*

$$\mathbb{Z}/n\mathbb{Z}\cong\mathbb{Z}/p_1^{n_1}\mathbb{Z}\times\mathbb{Z}/p_2^{n_2}\mathbb{Z}\times\ldots\times\mathbb{Z}/p_k^{n_k}\mathbb{Z}$$

та ізоморфізм відповідних мультиплікативних груп

$$(\mathbb{Z}/n\mathbb{Z})^* \cong (\mathbb{Z}/p_1^{n_1}\mathbb{Z})^* \times (\mathbb{Z}/p_2^{n_2}\mathbb{Z})^* \times \ldots \times (\mathbb{Z}/p_k^{n_k}\mathbb{Z})^* .$$

Або в інших позначеннях: $\mathbb{Z}_n^* \cong \mathbb{Z}_{p_1^{n_1}}^* \times \mathbb{Z}_{p_2^{n_2}}^* \times \ldots \times \mathbb{Z}_{p_k^{n_k}}^*$.

Доведення. Розглянемо ідеали $I_1 = p_1^{n_1}\mathbb{Z}$, $\ldots$, $I_k = p_k^{n_k}\mathbb{Z}$ в кільці $\mathbb{Z}$. Згадаємо, що $a\mathbb{Z} + b\mathbb{Z} = \text{НСД}(a,b)\mathbb{Z}$. Оскільки $\text{НСД}(p_i^{n_i}, p_j^{n_j}) = 1$ при $i \neq j$, то $I_i + I_j = \mathbb{Z}$, і виконуються умови попередньої теореми. Маючи $I_1 \ldots I_k = I_1 \cap \ldots \cap I_k = n\mathbb{Z}$ і застосувавши теорему, отримуємо потрібний результат. □

Наслідок 27 (Класична китайська теорема про остачі)**.** *Нехай* $n_1, n_2, \ldots, n_k$ *– взаємно прості натуральні числа, тобто* $\text{НСД}(n_i, n_j) = 1$ *при* $i \neq j$*. Тоді для довільних цілих чисел* $a_1, a_2, \ldots, a_k \in \mathbb{Z}$ *система конгруенцій*

$$\begin{aligned} x &\equiv a_1 \bmod n_1 \\ x &\equiv a_2 \bmod n_2 \\ &\vdots \\ x &\equiv a_k \bmod n_k \end{aligned}$$

має розв'язок в $\mathbb{Z}$*, який визначається однозначно по модулю* $n = n_1 n_2 \ldots n_k$.

Розв'язок можна знайти за допомогою наступного алгоритму. Покладемо $n = n_1 n_2 \ldots n_k$.

1. Обчислюємо $n_i' = \frac{n}{n_i} = n_1 \ldots n_{i-1} n_{i+1} \ldots n_k$ для $i = 1, \ldots, k$.
2. Знаходимо $t_i \in \mathbb{Z}$ таке, що $t_i n_i' \equiv 1 \bmod n_i$, тобто t_i є оберненим до n_i' в кільці $\mathbb{Z}_{n_i}$ $(i = 1, \ldots, k)$. Це можна зробити, оскільки $\text{НСД}(n_i, n_i') = 1$ і, отже, n_i' є оборотним в $\mathbb{Z}_{n_i}$.
3. Тоді розв'язком є $x = a_1 t_1 n_1' + a_2 t_2 n_2' + \ldots + a_k t_k n_k' \bmod n$.

Перевіряємо: $x \equiv a_i t_i n_i' \equiv a_i \bmod n_i$ для всіх i.

Приклади 11. Розв'яжемо систему конгруенцій

$$\begin{cases} x & \equiv & 2 \mod 3 \\ x & \equiv & 2 \mod 4 \\ x & \equiv & 3 \mod 5 \end{cases}.$$

За алгоритмом отримуємо: $n = 60$, $n_1' = 20$, $n_2' = 15$, $n_3' = 12$.

$$\begin{array}{lcllcl} 20t_1 \equiv 1 \mod 3 & \Rightarrow & 2t_1 \equiv 1 \mod 3 & \Rightarrow & t_1 \equiv 2 \mod 3, \\ 15t_2 \equiv 1 \mod 4 & \Rightarrow & 3t_2 \equiv 1 \mod 4 & \Rightarrow & t_2 \equiv 3 \mod 4, \\ 12t_3 \equiv 1 \mod 5 & \Rightarrow & 2t_3 \equiv 1 \mod 5 & \Rightarrow & t_3 \equiv 3 \mod 5. \end{array}$$

Отже, $x \equiv 2 \cdot 2 \cdot 20 + 2 \cdot 3 \cdot 15 + 3 \cdot 3 \cdot 12 \equiv 278 \equiv 38 \mod 60$.

Вправи

1. Нехай I_k – ідеал в кільці R_k для $k = 1, \ldots, n$. Доведіть, що $I_1 \times \ldots \times I_n$ є ідеалом в прямому добутку $R_1 \times \ldots \times R_n$. Доведіть, якщо всі R_k є кільцями з 1, то кожен ідеал в $R_1 \times \ldots \times R_n$ має вигляд $I_1 \times \ldots \times I_n$. Наведіть приклад двох кілець R_1, R_2 (без одиниці) та ідеалу I в $R_1 \times R_2$, який не можна представити у вигляді $I_1 \times I_2$ для деяких ідеалів I_1, I_2.

2. Розв'яжіть рівняння $x^4 + 12x^3 + 3x^2 + 8 \equiv 0 \mod 20$.

§ 7 Подільність в кільцях

Основна відмінність полів від кілець полягає в тому, що в полях довільний елемент можна поділити на довільний ненульовий елемент. В кільцях ситуація з подільністю більш цікава. Одні елементи діляться на інші, може існувати ділення з остачею, або кожен елемент може розкладатися у добуток простих. Розглядаючи можливі узагальнення ділення з остачею, виділяють кілька важливих класів кілець. Серед них евклідові кільця, кільця голових ідеалів і факторіальні кільця, які ми будемо вивчати в цьому розділі.

Всі кільця в цьому розділі будемо вважати комутативними.

7.1 Евклідові кільця

Такі відомі області цілісності як кільце цілих чисел $\mathbb{Z}$ та кільце многочленів $F[x]$ над полем F мають певні спеціальні властивості, які не розділяють всі області цілісності. Наприклад, в цих кільцях існує ділення з остачею та алгоритм Евкліда. Наступне означення виділяє клас кілець з цією властивістю.

Означення 18. Область цілісності R називається *евклідовим кільцем*, якщо існує функція $N : R \setminus \{0\} \to \mathbb{N} \cup \{0\}$ така, що:

1) для всіх ненульових $a, b \in R$ виконується $N(a) \leq N(ab)$;

2) для всіх $a, b \in R$ і $b \neq 0$ існують $q, r \in R$ такі, що

$$a = qb + r \quad \text{і} \quad r = 0 \text{ або } N(r) < N(b).$$

Функція $N(\cdot)$ називається *евклідовою нормою*.

Зауваження 6. 1. Можна показати, що умова 1) є зайвою: якщо в області цілісності існує норма з властивістю 2), то існує норма з властивостями 1) і 2) (доведіть!).

2. Умову 2) можна переформулювати в термінах ідеалів: для кожного ненульового головного ідеалу $I = (b)$ в кільці R кожен ненульовий клас в факторкільці R/I має представника r з $N(r) < N(b)$.

Приклади 12. 1. Кожне поле F є евклідовим кільцем. Норму можна визначити як $N(a) = 0$ для всіх $a \in F$. Умова 1) очевидно виконується, а умова 2) випливає з того, що кожен елемент можна поділити без остачі на довільний ненульовий елемент: $a = (ab^{-1})b + 0$.

2. Кільце $\mathbb{Z}$ є евклідовим кільцем з нормою $N(a) = |a|$. Поділивши довільне ціле число a з остачею на ненульове число b, отримаємо $a = qb + r$, де $r = 0$ або $|r| < |b|$. Зауважте, що q, r можуть визначатися не однозначно. Наприклад, $5 = 2 \cdot 2 + 1 = 3 \cdot 2 + (-1)$.

3. Кільце многочленів $F[x]$ над довільним полем F є евклідовим кільцем. Норма многочлена $f(x) \in F[x]$ визначається як $N(f(x)) = \deg f(x)$. Алгоритм ділення з остачею дає нам $f(x) = q(x)g(x)+r(x)$, де $r(x) \equiv 0$ або $\deg r(x) < \deg g(x)$.

4. Кільце цілих гаусових чисел $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$ є евклідовим кільцем. Доведемо це. Визначимо норму $N(a+bi) = a^2+b^2 = |a+bi|^2$ як квадрат модуля комплексного числа. Використавши мультиплікативність модуля, отримуємо:

$$N((a+bi)(c+di)) = |(a+bi)(c+di)|^2 = |a+bi|^2 \cdot |c+di|^2 \geq N(a+bi),$$

де останню нерівність ми отримали з $|c + di|^2 = c^2 + d^2 \geq 1$ для ненульового $c+di \in \mathbb{Z}[i]$. Перевіримо другу умову. Нехай $\alpha = a+bi \in \mathbb{Z}[i]$, $\beta = c + di \in \mathbb{Z}[i]$, $\beta \neq 0$. Поділимо α на β в полі $\mathbb{C} \supset \mathbb{Z}[i]$:

$$\frac{\alpha}{\beta} = \frac{a + bi}{c + di} = \frac{ac + bd}{c^2 + d^2} + \frac{bc - ad}{c^2 + d^2} i = r + si,$$

де $r, s \in \mathbb{Q}$ – це відповідно дійсна та уявна частини числа. Наблизимо r і s цілими числами n і m так, що $|r-n| \leq 1/2$ і $|s-m| \leq 1/2$. Тоді $\alpha = (n + mi)\beta + \gamma$ для деякого $\gamma \in \mathbb{Z}[i]$. Перевіримо, що $N(\gamma) < N(\beta)$:

$$\begin{aligned}
\gamma &= \alpha - (n + mi)\beta = ((r - n) + (s - m)i)\beta \qquad \Rightarrow \\
N(\gamma) &= N((r - n) + (s - m)i)N(\beta) \leq \\
&\leq \left((r - n)^2 + (s - m)^2\right) N(\beta) \leq \\
&\leq \left(\frac{1}{2^2} + \frac{1}{2^2}\right) N(\beta) \leq \frac{1}{2} N(\beta) < N(\beta).
\end{aligned}$$

Отже, $N(\cdot)$ є евклідовою нормою, а $\mathbb{Z}[i]$ – евклідовим кільцем.

Аналогічне доведення працює і для кільця $\mathbb{Z}[\sqrt{-2}]$. Але, наприклад, кільце $\mathbb{Z}[\sqrt{-5}]$ – не евклідове. Для того, щоб це показати, за означенням, потрібно довести, що на кільці не можна визначити евклідову норму. Напряму це довести може бути складно. Тому часто використовують властивості характерні для евклідових кілець. Якщо кільце не має такої властивості, то воно – не евклідове.

Теорема 28. *Кожен ідеал в евклідовому кільці є головним.*

Доведення. Нехай R – евклідове кільце і I – ідеал в R. Якщо $I = \{0\}$, то $I = (0)$ і ідеал головний. Нехай $I \neq \{0\}$, і знайдемо ненульовий елемент $b \in I$, який має найменшу норму, тобто $N(b) = \min\{N(a) : a \in I, a \neq 0\}$. Очевидно $(b) \subset I$. Доведемо, що $I \subset (b)$. Візьмемо довільний елемент $a \in I$ і поділимо з остачею на b:

$$a = qb + r, \text{ де } r = 0 \text{ або } N(r) < N(b).$$

Оскільки $a \in I$ і $qb \in I$, то $r = a - qb \in I$. З вибору елемента b і умови $N(r) < N(b)$ випливає $r = 0$. Отже, $a = qb \in (b)$ і $I = (b)$. □

7.2 Кільця головних ідеалів

Означення 19. Область цілісності, в якій кожен ідеал є головним, називається *кільцем головних ідеалів*.

Приклади 13. 1. Евклідові кільця є кільцями головних ідеалів за теоремою 28. Зокрема, в кільці $\mathbb{Z}[i]$ всі ідеали головні.

2. В кільці $\mathbb{Z}[x]$ ідеал $(2, x)$ не є головним (див. приклад 5). Отже, $\mathbb{Z}[x]$ не є кільцем головних ідеалів і не є евклідовим кільцем.

3. Повернемося до кільця $\mathbb{Z}[\sqrt{-5}]$ і доведемо, що воно не є кільцем головних ідеалів. Дійсно, розглянемо норму $N(a+b\sqrt{-5}) = a^2+5b^2$, яка є мультиплікативною (але не евклідовою). Розглянемо ідеал $I = (2, 1 + \sqrt{-5})$ і доведемо, що він не головний. Зауважимо, що норми $N(2) = 4$ і $N(1+\sqrt{-5}) = 6$ діляться на 2, тому норма кожного елемента ідеалу ділиться на 2. Зокрема, $I \neq \mathbb{Z}[\sqrt{-5}]$. Припустимо цей ідеал є головним і $I = (a+b\sqrt{-5})$ для деяких $a, b \in \mathbb{Z}$. Оскільки $2 \in (a + b\sqrt{-5})$, то отримуємо:

$$\begin{aligned} &2 = \alpha(a + b\sqrt{-5}) \text{ для деякого } \alpha \in \mathbb{Z}[\sqrt{-5}] \quad \Rightarrow \\ &4 = N(2) = N(\alpha)(a^2 + 5b^2) \quad \Rightarrow \quad a^2 + 5b^2 = 1, 2 \text{ або } 4. \end{aligned}$$

Розглянемо ці випадки. Якщо $a^2 + 5b^2 = 1$, то $a + b\sqrt{-5} = \pm 1$ і $I = \mathbb{Z}[\sqrt{-5}]$; протиріччя. Рівняння $a^2 + 5b^2 = 2$ не має розв'язків в

цілих числах (доведіть!). Якщо $a^2+5b^2=4$, то $N(\alpha)=1$ і $\alpha=\pm 1$. Тоді $a+b\sqrt{-5}=\pm 2$, але $1+\sqrt{-5}\notin(2)$; протиріччя. Отже, ідеал I – не головний.

Нагадаємо, що кожен максимальний ідеал в комутативному кільці з 1 є простим (див. наслідок 23). Простий ідеал – не завжди максимальний. Наприклад, в $\mathbb{Z}$ нульовий ідеал – не максимальний. Але всі ненульові прості ідеали в $\mathbb{Z}$ є максимальними. Ця властивість виконується для всіх кілець головних ідеалів.

Твердження 29. *Кожен ненульовий простий ідеал в кільці головних ідеалів є максимальним.*

Доведення. Нехай (p) – ненульовий простий ідеал в кільці головних ідеалів R. Нехай $(p)\subset(a)$, і нам потрібно довести, що $(a)=(p)$ або $(a)=R$. Оскільки $p\in(a)$, то $p=ar$ для деякого $r\in R$. Тоді $ar\in(p)$ і з простоти ідеалу (p) випливає, що $a\in(p)$ або $r\in(p)$. Якщо $a\in(p)$, то $(a)=(p)$. Якщо $r\in(p)$, то $r=ps$ для деякого $s\in R$. Підставляємо в $p=ar$ і отримуємо $p=ra=psa$. Оскільки R – область цілісності, то ми можемо скоротити p і отримуємо $sa=1$. Отже, $a\in R^*$ і $(a)=R$. □

Нагадаємо, що кільце многочленів $F[x]$ над полем F є евклідовим кільцем, а отже, і кільцем головних ідеалів. В той же час, кільце $\mathbb{Z}[x]$ не є кільцем головних ідеалів.

Наслідок 30. *Якщо кільце многочленів $R[x]$ є кільцем головних ідеалів, то R є полем.*

Доведення. Кільце R є підкільцем $R[x]$. Оскільки $R[x]$ – область цілісності, то і R – область цілісності. За теоремою 22 ідеал (x) є ненульовим простим ідеалом, оскільки $R[x]/(x)\cong R$ – область цілісності. За попереднім твердженням, (x) є максимальним ідеалом. Отже, за теоремою 21 факторкільце $R[x]/(x)\cong R$ є полем. □

Твердження 31. *В кільці головних ідеалів R довільний зростаючий ланцюг ідеалів $I_1\subset I_2\subset I_3\subset\ldots$ стабілізується, тобто існує n таке, що $I_n=I_{n+1}=\ldots$.*

Доведення. Доведемо, що $I = \cup_{i=1}^{\infty} I_i$ є ідеалом в R. Якщо $a, b \in I$, то $a \in I_i$ та $b \in I_j$ для деяких $i, j \in \mathbb{N}$. Можна вважати $i \leq j$. Тоді $a, b \in I_j$ і тому $a - b \in I_j \subset I$. Також $ra \in I_j \subset I$ для всіх $r \in R$. Отже, I – ідеал.

Оскільки R – кільце головних ідеалів, то існує елемент $a \in R$ для якого $I = (a)$. Існує $n \in \mathbb{N}$ таке, що $a \in I_n$ і тому $I_n = I = (a)$. Зокрема, $I_n = I_{n+1} = \ldots$. □

Зауваження 7. Не кожне кільце головних ідеалів є евклідовим кільцем. Прикладом є кільце $\mathbb{Z}[\frac{1+\sqrt{-19}}{2}]$, доведення можна знайти в [7, ст. 282].

Властивість бути кільцем головних ідеалів можна охарактеризувати через існування спеціальної норми на кільці, схожу на евклідову норму, яка називається нормою Дедекінда-Хассе. Детальніше про це можна прочитати в [7, Розділ 8.2].

Вправи

1. Доведіть, що кільце $\mathbb{Z}[\sqrt{2}]$ є евклідовим кільцем.
2. Доведіть, що кільце $\mathbb{Z}[\sqrt{-3}]$ не є кільцем головних ідеалів.
3. Нехай R – область цілісності, в якій кожен спадний ланцюг ідеалів стабілізується. Доведіть, що R – поле.
4. Доведіть, що факторкільце кільця головних ідеалів за простим ідеалом є кільцем головних ідеалів.
5. Доведіть, що кільце $\mathbb{Z}[\frac{-1+\sqrt{-3}}{2}]$ є евклідовим кільцем.

7.3 Подільність в кільцях

Нехай R – комутативне кільце.

Означення 20. Кажуть, що ненульовий елемент $b \in R$ *ділить* елемент $a \in R$, якщо існує $x \in R$ такий, що $a = bx$. Позначають $b \mid a$.

Елементи $a, b \in R$ називають *асоційованими*, якщо $a \mid b$ і $b \mid a$.

Одразу з означення випливають такі властивості відношення подільності.

Твердження 32. *1. Якщо $a \mid b$ і $b \mid c$, то $a \mid c$.*

2. Якщо $a \mid b$ і $a \mid c$, то $a \mid (b \pm c)$.

3. Якщо $a \mid b$, то $a \mid br$ для всіх $r \in R$.

4. Елемент u є оборотним тоді і лише тоді, коли $u \mid 1$.

Твердження 33. *Нехай R – комутативне кільце з 1 і $a, b, u \in R$. Тоді*

1) $b \mid a$ тоді і лише тоді, коли $(a) \subset (b)$;

2) a і b є асоційованими тоді і лише тоді, коли $(a) = (b)$;

3) відношення асоційованості є відношенням еквівалентності;

4) якщо $a = bu$ для $u \in R^*$, то a і b – асоційовані;

5) якщо R – область цілісності, то a і b – асоційовані тоді і лише тоді, коли існує $u \in R^*$ такий, що $a = bu$.

Доведення. 1) Згадаємо, що в комутативному кільці з 1 головний ідеал складається з елементів $(b) = \{br : r \in R\}$. Отже, $a = bx$ для деякого $x \in R$ тільки, коли $a \in (b)$, що еквівалентно $(a) \subset (b)$.

2) випливає з 1).

3) випливає з 2).

4) Якщо $a = bu$ для $u \in R^*$, то $b = au^{-1}$. Отже, $a \mid b$ і $b \mid a$, і елементи a, b асоційовані.

5) Нехай R – область цілісності. Нехай a і b – асоційовані та можемо вважати, що вони ненульові. Існують $x, y \in R$ такі, що $a = bx$ і $b = ay$. Тоді

$$a = ayx \quad \Rightarrow \quad a(1 - yx) = 0, a \neq 0 \quad \Rightarrow \quad 1 - yx = 0 \quad \Rightarrow \quad xy = 1.$$

Отже, x, y є оборотними елементами, що і потрібно було довести.

□

7.4 Найбільший спільний дільник

Нехай R – комутативне кільце.

Означення 21. *Найбільшим спільним дільником* елементів $a, b \in R$ (одночасно не рівних нулю) називається ненульовий елемент $d \in R$ такий, що

1) $d \mid a$ і $d \mid b$ (тобто d є спільним дільником a і b);

2) якщо $d' \mid a$ і $d' \mid b$ для $d' \in R$, то $d' \mid d$.

Позначають НСД(a, b).

Нехай R – кільце з 1. Найбільший спільний дільник можна визначити на мові ідеалів таким чином. Нехай (a, b) – ідеал породжений елементами a і b. Тоді елемент d є НСД(a, b), якщо

1) $(a, b) \subset (d)$;

2) якщо $(a, b) \subset (d')$ для $d' \in R$, то $(d) \subset (d')$.

З цього переформулювання означення одразу випливає наступне твердження.

Твердження 34. *Нехай R – комутативне кільце з* 1. *Якщо для ненульових елементів $a, b \in R$ ідеал (a, b) є головним і $(a, b) = (d)$, то d є* НСД(a, b).

Тому часто найбільший спільний дільник позначається так само як ідеал породжений елементами a, b, тобто через (a, b).

Твердження 35. *Нехай R – область цілісності. Якщо d і d' – найбільші спільні дільники елементів a і b, то існує $u \in R^*$ такий, що $d' = du$. Зокрема, якщо для елементів a, b існує найбільший спільний дільник, то він визначається однозначно з точністю до асоційованості.*

Доведення. З означення найбільшого спільного дільника маємо $(d) = (d')$ і можемо застосувати твердження 33. □

Наслідок 36. *Нехай R – кільце головних ідеалів і $a, b \in R$, $a, b \neq 0$. Нехай головний ідеал (a, b) породжується елементом d. Тоді:*

1) $d \in$ НСД(a, b) і визначається однозначно з точністю до множення на оборотний в R;

2) d є R-лінійною комбінацією елементів a і b, тобто існують $x, y \in R$ такі, що $d = ax + by$.

Приклади 14. 1. В $\mathbb{Z}$ найбільшим спільним дільником чисел 6 і 10 є ± 2. В термінах ідеалів маємо $(6, 10) = (2) = (-2)$.

2. В кільці $\mathbb{Q}[x]$ найбільшим спільним дільником многочленів $x^2 - 2x$ та $x^3 + x$ є многочлени ax для всіх $a \in \mathbb{Q}^*$.

3. Найбільший спільний дільник може не існувати. Наприклад, розглянемо кільце парних чисел $2\mathbb{Z} = \{\ldots, -4, -2, 0, 2, 4, \ldots\}$. Число 2 взагалі не має дільників в $2\mathbb{Z}$! Тому числа 2 і 4 не мають найбільшого спільного дільника.

   Інший приклад. Розглянемо елементи 4 і $2 + 2\sqrt{-3}$ кільця $\mathbb{Z}[\sqrt{-3}]$. Знаходимо дільники числа 4: ± 1, ± 2, $\pm 1 \pm \sqrt{-3}$, ± 4. Перевіряємо, які з них ділять число $2 + 2\sqrt{-3}$ і, таким чином, знаходимо спільні дільники: $\pm 1, \pm 2, \pm 1 \pm \sqrt{-3}$. Серед спільних дільників немає дільника, який би ділився на решту дільників: числа $\pm 1, \pm 1 \pm \sqrt{-3}$ не діляться на 2, а ± 2 не діляться на $1 + \sqrt{-3}$. Отже, НСД$(4, 2 + 2\sqrt{-3})$ в кільці $\mathbb{Z}[\sqrt{-3}]$ не існує.

4. Як ми побачили в твердженні 34, якщо ідеал, породжений елементами a і b, є головним, то найбільший спільний дільник НСД(a, b) існує. Але НСД(a, b) може існувати, навіть якщо цей ідеал – не головний. Наприклад, в кільці $\mathbb{Z}[x]$ ідеал $(2, x)$ – не головний. Спільними дільниками 2 і x є тільки ± 1, і тому 1 є НСД$(2, x)$. Або в термінах ідеалів: ідеал $(2, x)$ є максимальним, і тому $\mathbb{Z}[x] = (1)$ є єдиним головним ідеалом, що містить $(2, x)$. В той же час $(1) \neq (2, x)$.

Кожне евклідове кільце є кільцем головних ідеалів, і тому в евклідових кільцях найбільший спільний дільник існує для довільної пари елементів. Більш того, в евклідових кільцях найбільший спільний дільник можна знайти алгоритмічно за допомогою алгоритму Евкліда.

Теорема 37 (Алгоритм Евкліда)**.** *Нехай R – евклідове кільце і $a, b \in R$, $a, b \neq 0$. Послідовно поділимо з остачею:*

$$\begin{aligned}
a &= q_0 b + r_0, \quad N(b) > N(r_0),\\
b &= q_1 r_0 + r_1, \quad N(r_0) > N(r_1),\\
r_0 &= q_2 r_1 + r_2, \quad N(r_1) > N(r_2),\\
&\vdots\\
r_{n-2} &= q_n r_{n-1} + r_n, \quad N(r_{n-1}) > N(r_n),\\
r_{n-1} &= q_{n+1} r_n,
\end{aligned}$$

де r_n – це остання ненульова остача. Тоді $d = r_n$ є найбільшим спільним дільником елементів a і b.

$$\text{НСД}(a, b) = \textit{остання ненульова остача.}$$

Доведення. Згідно наслідку 36, достатньо довести, що $(d) = (a, b)$. З попередніх рівностей послідовно отримуємо

$$d \,|\, r_n, \quad d \,|\, q_{n+1} r_n = r_{n-1}, \quad d \,|\, q_n r_{n-1} + r_n = r_{n-2}, \quad \ldots \quad d \,|\, b, \quad d \,|\, a.$$

Отже, $(d) \supset (a, b)$. Навпаки, виражаємо остачі і отримуємо:

$$r_0 = a - q_0 b \in (a, b), \quad r_1 = b - q_1 r_0 \in (a, b), \quad \ldots, \quad r_n = d \in (a, b).$$

Отже, $(d) \subset (a, b)$, що і потрібно було довести. □

Зверніть увагу, що алгоритм Евкліда дозволяє не тільки знайти найбільший спільний дільник, а і його R-лінійне зображення $d = ax + by$. Для цього потрібно послідовно виражати d через попередні остачі:

$$\begin{aligned}
d &= r_{n-2} - q_n r_{n-1} = r_{n-2} - q_n (r_{n-3} - q_{n-1} r_{n-2}) =\\
&= -q_n r_{n-3} + (1 + q_n q_{n-1}) r_{n-2} = \ldots = ax + by.
\end{aligned}$$

Вправи

1. Знайдіть НСД елементів $8-6i$ і $1-7i$ кільця $\mathbb{Z}[i]$.
2. Чи існує НСД елементів $1+4\sqrt{-3}$ і $2+\sqrt{-3}$ кільця $\mathbb{Z}[\sqrt{-3}]$?

7.5 Факторіальні кільця

В множині натуральних чисел $\mathbb{N}$ важливу роль відіграють прості числа. Відомо, що кожне число розкладається у добуток простих, причому однозначно з точністю до порядку множників. В кільці многочленів $F[x]$ над полем F роль простих чисел відіграють незвідні (нерозкладні) многочлени і кожен многочлен розкладається у добуток незвідних. Визначимо поняття простого і нерозкладного елемента в довільній області цілісності.

Нехай R – область цілісності.

Означення 22. Елемент $r \in R$ називається *нерозкладним*, якщо

1) r – ненульовий і необоротний;
2) з умови $r = ab$ для деяких $a, b \in R$ випливає, що a або b є оборотним.

Ненульовий необоротний елемент $r \in R$ називається *розкладним*, якщо він розкладається у добуток $r = ab$, де a і b – необоротні.

Означення 23. Ненульовий елемент $p \in R$ називається *простим*, якщо ідеал (p) є простим ідеалом. Іншими словами, ненульовий елемент p є простим тоді і лише тоді, коли

1) p не є оборотним;
2) якщо $p \mid ab$ для деяких $a, b \in R$, то $p \mid a$ або $p \mid b$.

Твердження 38. *В області цілісності кожен простий елемент є нерозкладним.*

Доведення. Нехай (p) – простий ідеал і $p = ab$. Тоді $ab \in (p)$ і з означення простого ідеалу маємо, що $a \in (p)$ або $b \in (p)$. Можна вважати $a \in (p)$ і, отже, $a = pr$ для деякого $r \in R$. Тоді $p = ab = prb$. В області цілісності можна скорочувати, скорочуємо p і маємо $rb = 1$. Отже, b є оборотним, що і потрібно було довести. □

Приклади 15. 1. Нагадаємо, що натуральне число $n > 1$ називається простим, якщо воно має тільки два натуральних дільники 1 і n. В кільці $\mathbb{Z}$ простими елементами є $\pm p$, де p – просте число, які також є нерозкладними елементами. Так само в кільці многочленів $F[x]$ над полем F поняття простого і нерозкладного елемента збігаються – ними є незвідні многочлени.

2. В довільній області цілісності нерозкладні елементи не обов'язково прості. Наприклад, розглянемо кільце $\mathbb{Z}[\sqrt{-3}]$ і доведемо, що число 2 є нерозкладним, але не є простим. Якщо припустити, що 2 розкладається у добуток

$$2 = (a + b\sqrt{-3})(c + d\sqrt{-3}),$$

то, взявши норму, отримуємо

$$4 = (a^2 + 3b^2)(c^2 + 3d^2) \quad \Rightarrow \quad a^2 + 3b^2 = 1,\ 2 \text{ або } 4.$$

Розглянемо випадки. Якщо $a^2 + 3b^2 = 1$, то $a = \pm 1$, $b = 0$ і $a + b\sqrt{-3} = \pm 1$ є оборотним. Рівняння $a^2 + 3b^2 = 2$ не має розв'язків в цілих числах. Якщо $a^2 + 3b^2 = 4$, то $c^2 + 3d^2 = 1$, і $c + d\sqrt{-3} = \pm 1$ є оборотними. Отже, число 2 є нерозкладним елементом.

В той же час 2 не є простим, оскільки

$$2 \mid (1 + \sqrt{-3})(1 - \sqrt{-3}) = 4,$$

але 2 не ділить $1 \pm \sqrt{-3}$.

3. В кільці многочленів $\mathbb{Q}[x, y]$ від двох змінних x, y розглянемо підкільце $R = (x^2, y^2, xy)$. Елементи x^2, y^2, xy є нерозкладними в кільці R. Але xy – не простий: xy ділить добуток x^2y^2, але не ділить ні x^2, ні y^2.

Твердження 39. *В кільці головних ідеалів елемент є нерозкладним тоді і лише тоді, коли він простий.*

Доведення. Нехай p – нерозкладний елемент і доведемо, що (p) є не тільки простим, а і максимальним ідеалом. Нехай (p) міститься в ідеалі

M. Оскільки всі ідеали головні, то $M = (a)$ для деякого $a \in R$. Тоді $p \in (a)$ і $p = ra$ для деякого $r \in R$. Оскільки p – нерозкладний, то r або a є оборотним. Якщо r – оборотний, то a і p асоційовані, і $(a) = (p)$. Якщо a – оборотний, то $(a) = R$. Отже, ідеал (p) є максимальним, а кожен максимальний ідеал є простим за наслідком 23. □

Приклади 16. Кільце многочленів $F[x]$ над полем F є кільцем головних ідеалів. Застосувавши попередній результат до кільця $F[x]$, ми отримуємо факт, який вже доводили раніше: многочлен $f(x)$ є незвідним (нерозкладним) $\Leftrightarrow$ ідеал $(f(x))$ є максимальним $\Leftrightarrow$ факторкільце $F[x]/(f(x))$ є полем.

Означення 24. Область цілісності R називається *факторіальним кільцем*, якщо виконуються умови:

1) кожен ненульовий необоротний елемент $a \in R$ можна розкласти в добуток $a = p_1 p_2 \dots p_n$, де p_i – нерозкладні елементи;

2) розклад в 1) визначається однозначно з точністю до асоційованих елементів, тобто якщо

$$a = p_1 p_2 \dots p_n = q_1 q_2 \dots q_m,$$

де p_i, q_i – нерозкладні, то $n = m$, і існує перестановка $\sigma \in S_n$ така, що p_i і $q_{\sigma(i)}$ є асоційованими для всіх i.

Приклади 17.

1. Кільце $\mathbb{Z}$ є факторіальним кільцем за основною теоремою арифметики. Кожне число розкладається у добуток простих. Розклад не однозначний, наприклад, $6 = 2 \cdot 3 = (-2) \cdot (-3)$, але однозначний з точністю до порядку і множення на ± 1.

2. Кільце многочленів $F[x]$ над полем F є факторіальним кільцем: існування і єдиність розкладу многочленів у добуток незвідних множників доводиться в курсі лінійної алгебри.

3. Кільце $\mathbb{Z}[\sqrt{-5}]$ є областю цілісності, але не є факторіальним кільцем. Число 6 має два різні розклади у добуток нерозкладних:

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

Аналогічно кільце $\mathbb{Z}[\sqrt{-3}]$ не є факторіальним, оскільки можна розглянути розклади $4 = 2 \cdot 2 = (1 + \sqrt{-3})(1 - \sqrt{-3})$.

В той же час, кільце цілих гаусових чисел $\mathbb{Z}[i]$ є факторіальним. Це буде випливати з теореми 42, яку ми сформулюємо нижче.

Твердження 40. *В факторіальних кільцях елемент є простим тоді і лише тоді, коли він нерозкладний.*

Доведення. Ми вже знаємо, що прості елементи є нерозкладними. Доведемо, що нерозкладні елементи є простими. Нехай елемент p – нерозкладний і $p \mid ab$. Тоді $ab = pc$ для деякого $c \in R$. Нам потрібно довести, що $p \mid a$ або $p \mid b$. Розкладемо a і b у добуток нерозкладних $a = p_1 p_2 \dots p_s$ і $b = q_1 q_2 \dots q_t$, і підставимо в $ab = pc$:

$$p_1 p_2 \dots p_s q_1 q_2 \dots q_t = pc.$$

З однозначності розкладу випливає, що p є асоційованим з деяким p_i або q_j, нехай з p_i. Тоді $p_i = pu$ для оборотного $u \in R$. Отже, $a = (pu)p_1 \dots p_{i-1} p_{i+1} \dots p_s$ і $p \mid a$. □

Для знаходження найбільшого спільного дільника в кільці $\mathbb{Z}$ можна використовувати не тільки алгоритм Евкліда, а і розклад чисел у добуток простих. Аналогічний результат справедливий для всіх факторіальних кілець.

Твердження 41. *Нехай R – факторіальне кільце і $a, b \in R$, $a, b \neq 0$. Нехай*

$$a = u p_1^{k_1} p_2^{k_2} \dots p_n^{k_n} \quad і \quad b = v p_1^{m_1} p_2^{m_2} \dots p_n^{m_n},$$

де $u, v \in R^*$ оборотні, p_i – попарно неасоційовані нерозкладні, $k_i, m_i \geq 0$. Тоді елемент

$$d = p_1^{\min(k_1, m_1)} p_2^{\min(k_2, m_2)} \dots p_n^{\min(k_n, m_n)}$$

є НСД(a, b). *Зокрема, у факторіальному кільці довільні два ненульові елементи мають найбільший спільний дільник.*

Доведення. За побудовою, d ділить a і b. Нехай d' ділить a і b. Тоді в розкладі $d' = q_1 q_2 \dots q_m$ у добуток нерозкладних кожен q_i є асоційованим з деяким p_j. Крім того, степінь, в якому p_j входить в розклад d', не може перевищувати степені, в якому p_j входить в розклад a і b. Отже, d' ділить d. □

Теорема 42. *Кожне кільце головних ідеалів є факторіальним кільцем.*

Доведення. Нехай R – кільце головних ідеалів. Спочатку доведемо, що кожен ненульовий необоротний елемент розкладається у добуток нерозкладних, а потім доведемо єдиність такого розкладу.

Існування розкладу. Нехай $a \in R$, $a \neq 0$ і $a \notin R^*$. Спочатку доведемо, що існує розклад $a = p_1 b$, де p_1 – нерозкладний. Якщо a – нерозкладний, то доведено. Якщо ні, то $a = a_1 b_1$, де a_1 і b_1 – необоротні. Отже, $(a) \subsetneq (a_1)$. Якщо a_1 – нерозкладний, то доведено. Якщо ні, то $a_1 = a_2 b_2$, де a_2 і b_2 – необоротні. Отже, $(a_1) \subsetneq (a_2)$ і т.д. Якщо цей процес не закінчиться за скінченну кількість кроків, то ми отримаємо нескінченний зростаючий ланцюг ідеалів

$$(a) \subset (a_1) \subset (a_2) \subset \dots,$$

де всі ідеали різні. Це протирічить твердженню 31: в кільці головних ідеалів кожен зростаючий ланцюг ідеалів стабілізується. Отже, цей процес закінчиться на деякому a_n, тобто a_n – нерозкладний дільник a, що ми й хотіли довести.

Тепер доведемо, що a розкладається у добуток нерозкладних елементів. Нехай $a = p_1 b_1$, де p_1 – нерозкладний і $(a) \subset (b_1)$. Якщо b_1 – нерозкладний, то доведено. Якщо ні, то $b_1 = p_2 b_2$, де p_2 – нерозкладний, і $(b_1) \subset (b_2)$. Знову отримаємо зростаючий ланцюг ідеалів

$$(a) \subset (b_1) \subset (b_2) \subset \dots,$$

який повинен стабілізуватися, тобто процес закінчиться через скінченну кількість кроків. Отже, $a = p_1 p_2 \dots p_n$.

Єдиність розкладу. Індукція за кількістю множників в розкладі. При $n = 1$ елемент a нерозкладний. Тому в довільному іншому розкладі $a = pb$

з нерозкладним p елемент b має бути оборотним. Нехай $n \geq 1$ і ми маємо два розклади

$$a = p_1 p_2 \dots p_n = q_1 q_2 \dots q_m, \tag{1}$$

де p_i, q_j – нерозкладні. За твердженням 39 елементи p_i, q_j є простими. Оскільки $p_1 \mid q_1 q_2 \dots q_m$, то p_1 ділить деякий q_i, нехай q_1. Оскільки q_1 – нерозкладний, то $q_1 = p_1 u$ з оборотним u. Отже, p_1 і q_1 є асоційованими. Підставляємо $q_1 = p_1 u$ в (1), скорочуємо p_1 і отримуємо розклад

$$p_2 p_3 \dots p_n = (u q_2) q_3 \dots q_m = q_2' q_3 \dots q_m,$$

що містить менше n множників. Застосовуємо припущення індукції. □

Теорема 43 (без доведення)**.** *Нехай R – факторіальне кільце. Тоді кільце многочленів $R[x]$ теж є факторіальним.*

Приклади 18. Кільце $\mathbb{Z}[x]$ є факторіальним, але не є кільцем головних ідеалів. Оскільки $\mathbb{Z}[x_1, x_2, \dots, x_k] = \mathbb{Z}[x_1, \dots, x_{k-1}][x_k]$, то за індукцією отримуємо, що всі ці кільця є факторіальними.

В цьому розділі ми розглянули кілька важливих класів кілець і довели, що справедливі наступні включення:

$$\begin{array}{ccccccc}
\text{поля} & \subset & \begin{array}{c}\text{евклідові}\\ \text{кільця}\end{array} & \subset & \begin{array}{c}\text{кільця головних}\\ \text{ідеалів}\end{array} & \subset & \\
\mathbb{Z} & & \mathbb{Z}[\frac{1+\sqrt{-19}}{2}] & & & & \mathbb{Z}[x] \\
\subset & \begin{array}{c}\text{факторіальні}\\ \text{кільця}\end{array} & \subset & \begin{array}{c}\text{області}\\ \text{цілісності}\end{array} & \subset & \begin{array}{c}\text{комутативні}\\ \text{кільця}\end{array} & \\
\mathbb{Z}[x] & & \mathbb{Z}[\sqrt{-3}] & & \mathbb{Z}_4 & &
\end{array}$$

де під знаками включення вказано приклади кілець, які розділяють суміжні класи.

Вправи

1. Чи має елемент $10 + 4\sqrt{-5}$ кільця $\mathbb{Z}[\sqrt{-5}]$ однозначний розклад у добуток нерозкладних?

2. Знайдіть кількість дільників елемента $86 - 162i$ в кільці $\mathbb{Z}[i]$.

3. Доведіть, що в кільці з мультиплікативною нормою кожен елемент розкладається у добуток нерозкладних елементів.

4. Доведіть, що область цілісності R є факторіальним кільцем тоді і лише тоді, коли кожен ненульовий простий ідеал в R містить простий елемент.

7.6 Прості числа в $\mathbb{Z}[i]$ і розклад натуральних чисел у суму двох квадратів

Коли ціле число n розкладається у суму двох квадратів, тобто $n = a^2 + b^2$ для $a, b \in \mathbb{Z}$? Це цікаве питання тісно пов'язане з кільцем цілих гаусових чисел $\mathbb{Z}[i]$. Оскільки норма в $\mathbb{Z}[i]$ визначається за правилом $N(a + bi) = a^2 + b^2$, то справедливе твердження:

> число $n \in \mathbb{Z}$ розкладається у суму двох квадратів $n = a^2 + b^2$
> тоді і лише тоді, коли n є нормою цілого гаусового числа $a + bi$.

З мультиплікативності норми випливає, що добуток сум квадратів є сумою квадратів. Ми знаємо, що кільце $\mathbb{Z}[i]$ є факторіальним і кожен елемент розкладається у добуток простих елементів. Отже, кожна сума квадратів є добутком норм простих елементів в $\mathbb{Z}[i]$. Тому питання зводиться до опису простих елементів в $\mathbb{Z}[i]$. Прості елементи в $\mathbb{Z}[i]$ будемо називати *простими гаусовими числами*. Оскільки $\mathbb{Z} \subset \mathbb{Z}[i]$, то натуральні числа, які є простими гаусовими числами, є звичайними простими числами. Але не кожне просте ціле число залишається простим в $\mathbb{Z}[i]$.

Твердження 44. *Просте число p не є простим гаусовим числом тоді і лише тоді, коли p є сумою двох квадратів.*

Доведення. Якщо $p = a^2 + b^2$, то воно розкладається у добуток $p = (a + bi)(a - bi)$ і не є нерозкладним/простим в $\mathbb{Z}[i]$. Навпаки, нехай p – не простий елемент в $\mathbb{Z}[i]$. Оскільки кільце $\mathbb{Z}[i]$ факторіальне, то p розкладається у добуток простих гаусових чисел $p = p_1 p_2 \dots p_k$ $(k \geq$

2). Використавши мультиплікативність норми, отримаємо добуток цілих чисел

$$p^2 = N(p) = N(p_1)N(p_2)\dots N(p_k).$$

Нагадаємо, що $N(\alpha) = 1$ для $\alpha \in \mathbb{Z}[i]$ тоді і лише тоді, коли $\alpha \in (\mathbb{Z}[i])^* = \{\pm 1, \pm i\}$. Оскільки $N(p_i) > 1$ і p – просте число, то з однозначності розкладу в $\mathbb{Z}$ випливає, що $k = 2$ і $N(p_1) = N(p_2) = p$. Отже, число p є нормою цілого гаусового числа і тому розкладається у суму двох квадратів. □

Теорема 45 (Теорема Ферма про суму двох квадратів)**.** *Просте число p є сумою двох квадратів тоді і лише тоді, коли $p = 2$ або $p \equiv 1 \bmod 4$.*

Доведення. Доведемо, що якщо непарне число n розкладається у суму двох квадратів, то $n \equiv 1 \bmod 4$. Квадрат цілого числа може давати тільки остачі 0 або 1 при діленні на 4. Отже, сума квадратів дає остачі 0, 1 або 2 при діленні на 4, але 0 і 2 неможливі для непарного n. З цього випливає твердження в один бік.

Доведемо достатність. Число 2 є сумою квадратів $2 = 1^2 + 1^2$. Нехай $p \equiv 1 \bmod 4$ і покладемо $k = \frac{p-1}{2}$. Розглянемо число $n = k!$ і помітимо, що

$$n = (-1)(-2)\dots(-k) \equiv (p-1)(p-2)\dots(p-k) \bmod p,$$

де ми використали парність числа k. Тоді

$$n^2 \equiv 1 \cdot 2 \cdot \ldots \cdot k \cdot (k+1) \cdot \ldots \cdot (p-2) \cdot (p-1) \equiv (p-1)! \bmod p,$$

де ми використали $p-k = k+1$. За теоремою Вілсона, $(p-1)! \equiv -1 \bmod p$. Отже, $n^2 \equiv -1 \bmod p$ і значить p ділить $n^2+1 = (n-i)(n+i)$. Припустимо, що p є простим гаусовим числом. Тоді p ділить $n-i$ або $n+i$. З рівняння $n - i = p(a + bi)$ або $n + i = p(a + bi)$ ми отримуємо $p \mid 1$, що неможливо. Отже, p не є простим в $\mathbb{Z}[i]$, і ми можемо використати твердження 44. □

Наслідок 46. *Простими елементами в кільці $\mathbb{Z}[i]$ є:*

1) $1 + i$ і асоційовані з ним;

2) прості числа $p \in \mathbb{Z}$ такі, що $p \equiv 3 \bmod 4$, і асоційовані з ними;

3) $a+bi$ *для кожного розкладу* $p = a^2 + b^2$, $a, b \in \mathbb{Z}$, *де* $p \in \mathbb{Z}$ – *просте число і* $p \equiv 1 \bmod 4$.

Доведення. Доведемо, що якщо $N(a+bi)$ є простим числом, то $a+bi$ є простим гаусовим. Нехай $a+bi = \alpha\beta$ для $\alpha, \beta \in \mathbb{Z}[i]$. Тоді $N(a+bi) = N(\alpha)N(\beta)$ є розкладом простого числа. Отже, $N(\alpha) = 1$ або $N(\beta) = 1$ і відповідний елемент є оборотним, що і потрібно було довести. З цього випливає простота елементів з пунктів 1) і 3). Числа з пункту 2) є простими за твердженням 44 і теоремою 45.

Навпаки, нехай $a+bi$ є простим гаусовим числом. Тоді $(a+bi)(a-bi) = a^2 + b^2$ є цілим числом, і воно розкладається у добуток простих цілих чисел. Отже, $a+bi$ ділить деяке просте число p і має норму p або p^2. Тому пункти 1), 2), 3) охоплюють всі прості гаусові числа. □

Наслідок 47. *Натуральне число* $n \geq 2$ *можна представити у вигляді суми квадратів двох цілих чисел тоді і лише тоді, коли в розкладі* n *у добуток простих кожне просте* $p \equiv 3 \bmod 4$ *з'являється в парному степені.*

Доведення. Як ми вже зауважували, добуток сум квадратів є сумою квадратів. Оскільки число 2 і прості числа $p \equiv 1 \bmod 4$ розкладаються у суму квадратів, а прості $p \equiv 3 \bmod 4$ входять в парному степені, то добуток теж є сумою квадратів.

Навпаки, нехай $n = a^2 + b^2 = N(a+bi)$ для $a, b \in \mathbb{Z}$. Розклавши $a+bi$ у добуток простих гаусових чисел, маємо, що n є добутком норм простих елементів в $\mathbb{Z}[i]$. Знаходимо норми простих гаусових чисел з наслідку 46:

1) $N(1+i) = 2$;

2) $N(p) = p^2$, де $p \equiv 3 \bmod 4$;

3) $N(a+bi) = p$, де $p \equiv 1 \bmod 4$.

Звідси випливає розклад числа n. □

Приклади 19. 1. Просте число 5 розкладається у суму двох квадратів $5 = 2^2 + 1^2 = (2-i)(2+i)$, $5 \equiv 1 \bmod 4$ і не є простим

в $\mathbb{Z}[i]$. Просте число 7 не розкладається у суму двох квадратів, $7 \equiv 3 \bmod 4$, і тому залишається простим в $\mathbb{Z}[i]$.

2. Число $315 = 3^2 \cdot 5 \cdot 7$ не розкладається у суму двох квадратів, оскільки $7 \equiv 3 \bmod 4$ входить в розклад в непарному степені. Число $2205 = 3^2 \cdot 5 \cdot 7^2$ є сумою квадратів: $2205 = 42^2 + 21^2$.

3. Розкладемо число 150 у добуток простих елементів $\mathbb{Z}[i]$. Для цього спочатку розкладемо число у добуток простих в $\mathbb{Z}$: $150 = 2 \cdot 3 \cdot 5^2$. Тепер кожне просте $p \not\equiv 1 \bmod 4$ розкладемо у суму двох квадратів $2 = 1^2 + 1^2 = (1+i)(1-i)$ і $5 = 2^2 + 1^2 = (2+i)(2-i)$ і підставимо:

$$150 = (1-i)(1+i)3(2+i)^2(2-i)^2.$$

Вправи

1. Чи розкладаються у суму двох квадратів числа 380, 4165?

2. Розкладіть у добуток простих гаусових чисел числа $100, 460$.

Предметний покажчик

Список рекомендованої літератури

[1] Ван дер Варден. *Алгебра.* – М.: Мир, 1976.

[2] Винберг Э.Б. *Курс алгебры.* 3-е изд. – М.: Факториал Пресс, 2002.

[3] Каргаполов М.И., Мерзляков Ю.И. *Основы теории групп.* 3-е изд. – М.: Наука, 1982.

[4] Кострикин А.И. *Введение в алгебру.* Часть I: Основы алгебры. 3-е изд. – М.: Физматлит, 2004.

[5] Кострикин А.И. *Введение в алгебру.* Часть III: Основные структуры. 3-е изд. – М.: Физматлит, 2004.

[6] Dresden G., Dynàček W.M. *Finding Factors of Factor Rings over the Gaussian Integers* // MMA Monthly. – 2005. – Vol. 112. – P. 602 – 611.

[7] Dummit D.S., Foote R.M. *Abstract algebra.* 3rd ed. – Wiley Intern. Ed., Chichester: Wiley, 2004.

[8] Judson T.W. *Abstract algebra: theory and applications.* – An open-source textbook available at http://abstract.ups.edu, 2012.

[9] Herstein I.N. *Abstract algebra.* 3rd ed. – Upper Saddle River, NJ: Prentice Hall, 1996.

Навчальне видання

БОНДАРЕНКО Євген Володимирович

ТЕОРІЯ КІЛЕЦЬ

Навчальний посібник