Г.М.КУДРЯВЦЕВА, А.С.ОЛІЙНИК

КІЛЬЦЯ.
ПРИКЛАДИ І ЗАДАЧІ

Київський Національний Університет імені Тараса
Шевченка

Г.М.КУДРЯВЦЕВА, А.С.ОЛІЙНИК

КІЛЬЦЯ.
ПРИКЛАДИ І ЗАДАЧІ

Навчальний посібник

Київ — 2005

Даний посібник укладено на основі практичних занять, які автори ведуть на механіко–математичному факультеті Київського національного університету імені Тараса Шевченка. Може бути використаний усіма, хто вивчає теорію кілець, зокрема студентами математичних спеціальностей університетів.

Укладачі: Г.М.Кудрявцева, канд. фіз.-мат. наук
А.С.Олійник, канд. фіз.-мат. наук

Рецензенти: В.В.Кириченко, д-р фіз.-мат. наук, професор
В.М.Бондаренко, д-р. фіз.-мат. наук

Затверджено до друку Вченою Радою
механіко–математичного факультету
Київського національного університету
імені Тараса Шевченка
(протокол №7 від 17 січня 2005 року)

Зміст

Передмова 4

1 Кільця та підкільця 5
Приклади розв'язування задач 7
Задачі 13

2 Дільники нуля, оборотні та нільпотентні елементи 16
Приклади розв'язування задач 17
Задачі 20

3 Ідеали 23
Приклади розв'язування задач 23
Задачі 26

4 Гомоморфізми та факторкільця 28
Приклади розв'язування задач 29
Задачі 37

5 Подільність, розкладні і нерозкладні елементи 40
Приклади розв'язування задач 40
Задачі 42

6 Факторіальні кільця 45
Приклади розв'язування задач 46
Задачі 49

7 Евклідові кільця 51
Приклади розв'язування задач 52
Задачі 55

Список рекомендованої літератури 59

Передмова

Даний посібник укладено на основі матеріалів практичних занять з нормативного курсу алгебри і теорії чисел, які автори ведуть на механіко–математичному факультеті Київського національного університету імені Тараса Шевченка. В цьому курсі основи теорії кілець розглядають, як правило, протягом першої половини четвертого семестру. Посібником охоплюється весь матеріал з теорії кілець, який входить до навчальної програми курсу алгебри і теорії чисел. Для найкращого оволодіння матеріалом посібника необхідним є знайомство з основами теорії груп, елементарної теорії чисел, математичного аналізу та теоретико–множинною технікою.

Розділи посібника складаються з трьох частин. На початку кожного з них наводяться необхідні теоретичні відомості. Далі розглядаються приклади розв'язування типових задач, причому деякі з них використовуються при розв'язуванні інших задач. Третю частину кожного розділу складають задачі для самостійного розв'язування, що дозволяє використовувати цей посібник і як задачник.

Кожен розділ може бути основою одного або двох практичних занять. Для розгляду на такому занятті рекомендується використовувати як приклади, наведені в посібнику, так і задачі для самостійного розв'язування. Для домашнього завдання задачі слід підбирати саме з третьої частини кожного розділу.

В кінці наводиться список рекомендованої літератури. Він містить зокрема збірники задач, а також підручники та монографії, за якими можна вивчати як основи теорії кілець, так і її подальші розділи.

1 Кільця та підкільця

Нехай R — довільна непорожня множина. Бінарною операцією на множині R називається довільне відображення з декартового добутку $R \times R$ в R. Бінарні операції позначають, як правило, символами "$+$", "$\cdot$", "$*$", "$\circ$" і т.д. При цьому значення бінарної операції $*$ на парі елементів $(x, y) \in R \times R$ позначається $x * y$. Якщо для довільних елементів x, y з деякої підмножини S множини R значення $x * y$ міститься в S, то множину S називають замкненою відносно операції $*$.

Означення 1. Кільцем називається непорожня множина R з двома бінарними операціями на ній, які називають додаванням і множенням та позначають символами "$+$" і "$\cdot$" відповідно, що задовольняє таким умовам:

1) для довільних $x, y, z \in R$ $(x + y) + z = x + (y + z)$ (асоціативність додавання);

2) для довільних $x, y \in R$ $x + y = y + x$ (комутативність додавання);

3) існує такий елемент $0 \in R$ (його називають нулем кільця), що для довільного елемента $x \in R$ $x + 0 = x$ (існування нуля);

4) для довільного елемента $x \in R$ існує елемент $y \in R$ (його називають протилежним до x і позначають $-x$) такий, що $x + y = 0$ (існування протилежного елемента);

5) для довільних $x, y, z \in R$ $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ (асоціативність множення);

6) для довільних $x, y, z \in R$ $x \cdot (y + z) = x \cdot y + x \cdot z$ і $(y + z) \cdot x = y \cdot x + z \cdot x$ (дистрибутивність множення відносно додавання зліва і справа).

Іншими словами, непорожня множина з операціями додавання і множення є кільцем, якщо відносно додавання — це абелева група, відносно множення — напівгрупа і має місце дистрибутивність множення відносно додавання як зліва, так і справа. Абелева група $(R, +)$ називається адитивною групою кільця R.

Зауважимо, що так визначені кільця називають асоціативними, за рахунок асоціативності дії множення. Якщо замінити цю умову на певну іншу умову, одержимо означення інших типів кілець, зокрема кілець Лі, йорданових кілець, альтернативних кілець і т.д. Але в даному посібнику

ніяких інших кілець, крім асоціативних, розглядати не будемо, і тому далі термін "кільце" означатиме "асоціативне кільце".

Кільце R називається комутативним, якщо для довільних елементів $x, y \in R$ виконується рівність $x \cdot y = y \cdot x$, тобто множення в цьому кільці є комутативним.

Елемент e кільця R називається правою (відповідно лівою) одиницею цього кільця, якщо для довільного $a \in R$ маємо $ae = a$ (відповідно $ea = a$). Елемент кільця R називають одиницею цього кільця, якщо він є одночасно і лівою, і правою одиницею. Кільце, в якому існує одиниця, називається кільцем з одиницею. Іншими словами, кільце з одиницею — це кільце, в якому відносно множення існує нейтральний елемент.

Твердження 1. У кожному кільці нульовий елемент єдиний. У кожному кільці з одиницею одиничний елемент єдиний.

Одиничний елемент кільця з одиницею позначають, як правило, символом 1.

Означення 2. Непорожня підмножина A елементів кільця R називається підкільцем, якщо вона є кільцем відносно тих же операцій, відносно яких кільцем є R.

Іншими словами, A підкільце, якщо A є замкненою відносно операцій множення і додавання, а також взяття протилежного елемента. Слід зауважити, що підкільце A кільця R з одиницею також може бути кільцем з одиницею, яка не обов'язково рівна одиниці початкового кільця. Якщо ж одиниця підкільця A рівна одиниці кільця R, то A називають підкільцем кільця з одиницею. Таким чином, для кілець з одиницею слід розрізняти поняття підкільця і підкільця кільця з одиницею.

Перетин довільної родини підкілець кільця R також буде підкільцем R. Для підкільця A кільця R і довільної підмножини B елементів R назвем підкільцем, породженим A і B, перетин всіх підкілець, що містять A і B (одним з них є саме R). Це кільце є найменшим підкільцем, котре містить A і B. Будемо його позначати $A[B]$.

Нехай R_1, R_2 — деякі кільця. На декартовому добутку $R_1 \times R_2$ визначимо покоординатно операції додавання та множення. Отримаємо нове кільце, яке називається декартовим добутком кілець R_1 і R_2. Аналогічно визначається декартів добуток довільної скінченної кількості кілець. При цьому декартів добуток комутативних кілець є комутативним, а декартів добуток кілець з одиницею є кільцем з одиницею.

Приклади розв'язування задач

Приклад 1. Довести, що $a \cdot 0 = 0 \cdot a = 0$ для будь-якого елемента a кільця R.

Використовуючи дистрибутивність множення відносно додавання, маємо

$$a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 + a \cdot 0.$$

Додамо тепер до обох частин цієї рівності $-a \cdot 0$ і отримаємо $0 = a \cdot 0$.

Приклад 2. Довести, що якщо R є ненульовим кільцем з одиницею, то $1 \neq 0$.

Візьмемо якийсь ненульовий елемент $a \in R$ (за умовою, в R є такі елементи). Від супротивного, припустимо, що $1 = 0$. Але тоді

$$a = a \cdot 1 = a \cdot 0 = 0,$$

всупереч вибору елемента a. Отже, зроблене припущення хибне, і $1 \neq 0$.

Приклад 3. Довести, що для будь-яких елементів a, b кільця R виконується рівність $(-a) \cdot (-b) = a \cdot b$.

Спираючись на приклад 1, запишемо рівності

$$0 = 0 \cdot b = (a - a) \cdot b = a \cdot b + (-a) \cdot b;$$

$$0 = a \cdot 0 = a \cdot (b - b) = a \cdot b + a \cdot (-b).$$

Звідси, використовуючи, що з рівності $0 = x + y$ у групі випливає $-x = y$, отримаємо

$$-a \cdot b = (-a) \cdot b = a \cdot (-b).$$

Використовуючи цю рівність, маємо

$$0 = 0 \cdot 0 = (a - a) \cdot (b - b) = a \cdot b + a \cdot (-b) + (-a) \cdot b + (-a) \cdot (-b) = \\ a \cdot b - a \cdot b - a \cdot b + (-a) \cdot (-b) = -a \cdot b + (-a) \cdot (-b).$$

Таким, чином, елементи $-a \cdot b$ і $(-a) \cdot (-b)$ є взаємно протилежними у адитивній групі кільця R, що рівносильно потрібній нам рівності.

У прикладах 4-10 досліджується, чи будуть кільцями зі звичайними операціями додавання та множення задані числові множини:

Приклад 4. $\mathbb{Z}$.

По-перше, відносно операції додавання $\mathbb{Z}$ є абелевою групою: всім зі школи добре відомо, що додавання цілих чисел асоціативне і комутативне, $0+a=a+0=a$ для будь-якого цілого a і для кожного цілого числа a протилежне до нього $-a$ є єдиним розв'язком рівняння $a+x=0$. Далі, відносно операції множення $\mathbb{Z}$ є комутативною напівгрупою: множення цілих чисел, очевидно, асоціативне і комутативне. Крім того, множення цілих чисел дистрибутивне відносно додавання і число 1 є нейтральним елементом відносно множення. Отже, $\mathbb{Z}$ є комутативним кільцем з одиницею.

Аналогічно встановлюється, що множина $\mathbb{Q}$ всіх раціональних чисел відносно додавання і множення є комутативним кільцем з одиницею. Із властивостей додавання і множення дійсних чисел випливає, що комутативним кільцем з одиницею є множина всіх дійсних чисел $\mathbb{R}$, звідки неважко вивести аналогічне твердження про множину $\mathbb{C}$ усіх комплексних чисел.

Приклад 5. $n\mathbb{Z}$.

Можна просто перевірити аксіоми кільця: так само, як і у попередньому прикладі. Але досить зауважити, що сума і добуток двох чисел із $n\mathbb{Z}$ належать до $n\mathbb{Z}$ і для $a \in n\mathbb{Z}$ очевидно, що $-a \in n\mathbb{Z}$. Сказане означає, що $n\mathbb{Z}$ є замкненою відносно додавання, множення та взяття протилежного елемента. Враховуючи попередній приклад і те, що $n\mathbb{Z} \subset \mathbb{Z}$, всі аксіоми кільця для $n\mathbb{Z}$ виконуються автоматично. Зауважимо, що для $n > 1$ на відміну від кільця $\mathbb{Z}$ кільце $n\mathbb{Z}$ не містить одиниці.

Приклад 6. $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\}$.

Покажемо, що $\mathbb{Z}[\sqrt{2}]$ — комутативне кільце. Для числа $a + b\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$ назвемо a його першою координатою, а b— другою. Асоціативність і комутативність додавання є фактично наслідками того, що додавання $Z[\sqrt{2}]$ є покоординатним, а додавання координат (цілих чисел) асоціативне і комутативне. Розпишемо в деталях доведення асоціативності додавання. Візьмемо $a + b\sqrt{2}$, $c + d\sqrt{2}$, $e + f\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$. Маємо:

$$\left(\left(a + b\sqrt{2}\right) + \left(c + d\sqrt{2}\right)\right) + \left(e + f\sqrt{2}\right) = \left((a + c) + (b + d)\sqrt{2}\right) +$$
$$\left(e + f\sqrt{2}\right) = (a + c + e) + (b + d + f)\sqrt{2} = \left(a + b\sqrt{2}\right) +$$
$$\left((c + e) + (d + f)\sqrt{2}\right) = \left(a + b\sqrt{2}\right) + \left(\left(c + d\sqrt{2}\right) + \left(e + f\sqrt{2}\right)\right).$$

Нейтральним елементом для додавання є, очевидно, число $0 = 0+0\sqrt{2}$, а (єдиним) протилежним елементом для $a+b\sqrt{2}$ є $-a-b\sqrt{2}$. Ми Нейтральним елементом для додавання є, очевидно, число $0 = 0 + 0\sqrt{2}$, а (єдиним) протилежним елементом для $a+b\sqrt{2}$ є $-a-b\sqrt{2}$. Для встановлення асоціативності множення візьмемо $a + b\sqrt{2}$, $c + d\sqrt{2}$, $e + f\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$. Маємо:

$$\begin{aligned}\left(\left(a + b\sqrt{2}\right) \cdot \left(c + d\sqrt{2}\right)\right) \cdot \left(e + f\sqrt{2}\right) = \\ \left((ac + 2bd) + (ad + bc)\sqrt{2}\right) \cdot \left(e + f\sqrt{2}\right) = \\ ((ac + 2bd)e + 2(ad + bc)f) + ((ac + 2bd)f + (ad + bc)e)\sqrt{2} = \\ (ace + 2(bde + adf + bcf)) + ((acf + ade + bde) + 2bdf)\sqrt{2};\end{aligned}$$

аналогічні підрахунки призводять до рівності

$$\begin{aligned}\left(a + b\sqrt{2}\right) \cdot \left(\left(c + d\sqrt{2}\right) \cdot \left(e + f\sqrt{2}\right)\right) = \\ (ace + 2(bde + adf + bcf)) + ((acf + ade + bde) + 2bdf)\sqrt{2}.\end{aligned}$$

В останніх двох рівностей збігаються праві частини, а отже, і ліві частини, що доводить асоціативність множення. Операція множення буде до того ж комутативною. Це випливає з того, що переставивши у виразі $(ac + 2bd) + (ad + bc)\sqrt{2}$ відповідно a з c і b з d ми одержимо той самий вираз. Останній штрих — доведення дистрибутивності — лишаємо читачеві.

Ми могли міркувати інакше, зауваживши, що $\mathbb{Z}[\sqrt{2}]$ є підмножиною кільця дійсних чисел, замкненою відносно дій додавання і множення.

Приклад 7. $A = \{a + b\sqrt[3]{2} : a, b \in \mathbb{Z}\}$.

Дана множина не буде кільцем відносно звичайних операцій додавання і множення чисел, оскільки звичайне множення чисел не є бінарною операцією на A. Пригадаємо, що бінарна операція $\cdot$ на множині M — це правило, яке кожній впорядкованій парі (a, b) елементів з M ставить у відповідність елемент $a \cdot b \in M$. Нехай $a = b = \sqrt[3]{2} \in A$. Покажемо, що $a \cdot b = \sqrt[3]{4} \notin A$. Від супротивного, припустимо, що $\sqrt[3]{4} = c + d\sqrt[3]{2}$ для деяких цілих чисел c і d. Це означає що $\sqrt[3]{2}$ є коренем многочлена $f(x) = x^2 - dx - c$. Поділимо многочлен $x^3 - 2$ на $f(x)$ в кільці $\mathbb{Z}[x]$ з остачею:

$$x^3 - 2 = f(x)q(x) + r(x),$$

де $r(x)$ - многочлен не вище першого степеня з цілими коефіцієнтами. Але підставивши в обидва боки останньої рівності $\sqrt[3]{2}$, отримаємо, що $r(\sqrt[3]{2}) = 0$. Ця суперечність доводить, що $\sqrt[3]{4} \notin A$. Отже, ми показали, що множина A не замкнена відносно звичайного множення чисел.

Приклад 8. $\mathbb{Z}[\sqrt[3]{2}] = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} : \ a, b, c \in \mathbb{Z}\}$.

На відміну від попереднього прикладу, множина $\mathbb{Z}[\sqrt[3]{2}]$ є замкненою відносно звичайних додавання та множення чисел: для того, щоб додати або помножити два елементи з $\mathbb{Z}[\sqrt[3]{2}]$ треба їх додати або помножити як звичайні числа, а потім "звести подібні результат, очевидно, буде належати до $\mathbb{Z}[\sqrt[3]{2}]$. Нехай, наприклад, $a = 1 + 2\sqrt[3]{2} - 3\sqrt[3]{4}$, $b = 4 - \sqrt[3]{2} + 2\sqrt[3]{4}$. Тоді $a + b = 5 + \sqrt[3]{2} - \sqrt[3]{4}$,

$$a \cdot b = (1 + 2\sqrt[3]{2} - 3\sqrt[3]{4}) \cdot (4 - \sqrt[3]{2} + 2\sqrt[3]{4}) =$$
$$4 - \sqrt[3]{2} + 2\sqrt[3]{4} + 8\sqrt[3]{2} - 2\sqrt[3]{4} + 8 - 12\sqrt[3]{4} + 6 - 12\sqrt[3]{2} = 18 - 5\sqrt[3]{2} - 12\sqrt[3]{4}.$$

Перевірка виконання аксіом (комутативного) кільця аналогічна відповідній перевірці із приклада 6.

Приклад 9. Множина раціональних чисел, у нескоротному записі яких знаменники є дільниками фіксованого цілого числа n, $n \neq \pm 1$.

У цьому прикладі, так само, як і у прикладі 7, множина, що розглядається, не є замкненою відносно множення. Для того, щоб у цьому переконатися, нам треба навести два числа a і b із нашої множини, добуток яких до нашої множини вже не належить. Очевидно, що такою парою чисел є, наприклад, $a = b = 1/n$.

Приклад 10. Множина A_d комплексних чисел вигляду $(x + y\sqrt{d})/2$, де d фіксоване ціле число, що не ділиться на квадрат простого числа, x, y — цілі числа однакової парності.

Почнемо з перевірки, чи є множина A_d замкненою відносно додавання та множення. Нехай $a = (x_1 + y_1\sqrt{d})/2$, $b = (x_2 + y_2\sqrt{d})/2 \in A_d$. В залежності від парностей чисел x_1, y_1, x_2, y_2 можливі такі випадки:

1. Всі числа x_1, y_1, x_2, y_2 однакової парності (або всі парні, або всі непарні). Тоді числа $x_1 + x_2$ і $y_1 + y_2$ парні, а тому $a + b = ((x_1 + x_2) + (y_1 + y_2)\sqrt{d})/2 \in A_d$.

2. x_1 і x_2 різної парності (тобто x_1, y_1 — парні, x_2, y_2 — непарні, або навпаки, x_1, y_1 — непарні, а x_2, y_2 — парні). Тоді числа $x_1 + x_2$ і $y_1 + y_2$ обидва непарні, а тому $a + b = ((x_1 + x_2) + (y_1 + y_2)\sqrt{d})/2 \in A_d$.

Отже, ми довели, що при будь-якому можливому d множина A_d є замкненою відносно додавання.

Переходимо тепер до дослідження замкненості A_d відносно множення. Припустимо, що A_d замкнена відносно множення. Візьмемо $a = (1+\sqrt{d})/2$, $b = (1-\sqrt{d})/2 \in A_d$. Отримаємо

$$a \cdot b = (1+\sqrt{d})/2 \cdot (1-\sqrt{d})/2 = ((1-d)/2 + 0\sqrt{d})/2.$$

Оскільки елемент $a \cdot b$ повинен належати до A_d, то $(1-d)/2$ мусить бути парним числом, звідки випливає, що d дає остачу 1 при діленні на 4 (будемо записувати цей факт так: $d \equiv 1 (\mathrm{mod}\, 4)$). Отже, якщо множина A_d замкнена відносно множення, то $d \equiv 1 (\mathrm{mod}\, 4)$.

Покажемо, що отриманого обмеження на d і достатньо для замкненості відносно множення. Отже, нехай $d = 4k+1, k \in \mathbb{Z}$ і $a = (x_1 + y_1\sqrt{d})/2$, $b = (x_2 + y_2\sqrt{d})/2 \in A_d$. Тоді

$$a \cdot b = ((x_1x_2 + dy_1y_2)/2 + ((x_1y_2 + y_1x_2)/2)\sqrt{d})/2.$$

Ми прагнемо показати, що $x_3 = (x_1x_2 + dy_1y_2)/2$ та $y_3 = (x_1y_2 + y_1x_2)/2$ — цілі числа однакової парності. Це еквівалентно тому, що їх різниця $x_3 - y_3$ — парне число. Розглянемо три можливі випадки:

1. x_1 і y_1 — парні. Маємо:

$$x_3 - y_3 = x_1(x_2 - y_2)/2 + y_1(dy_2 - x_2)/2.$$

Оскільки числа x_2 і y_2 однакової парності і d — непарне, то $(x_2 - y_2)/2$ і $(dy_2 - x_2)/2$ — цілі числа. Отже, $x_3 - y_3$ — парне число.

2. x_2 і y_2 парні. Оскільки

$$x_3 - y_3 = x_2(x_1 - y_1)/2 + y_2(dy_1 - x_1)/2,$$

числа x_1 і y_1 однакової парності і d — непарне, то $(x_1 - y_1)/2$ і $(dy_1 - x_1)/2$ — цілі числа. Отже, і в цьому випадку $x_3 - y_3$ — парне число.

3. Всі числа x_1, y_1, x_2, y_2 — непарні. Маємо

$$2(x_3 - y_3) = x_2(x_1 - y_1) + y_2((4k+1)y_1 - x_1).$$

Нам потрібно показати, що це число ділиться на 4. Подільність вказаного числа на 4 рівносильна подільності на 4 числа

$$x_2(x_1 - y_1) + y_2(y_1 - x_1) = (x_1 - y_1)(x_2 - y_2).$$

Але отримане число ділиться на 4 як добуток двох парних чисел.

Таким чином ми довели, що A_d замкнена відносно множення тоді й лише тоді, коли $d \equiv 1 (\mathrm{mod}\, 4)$. Перевірка аксіом (комутативного) кільця аналогічна відповідній перевірці із прикладу 6.

У прикладах 11-12 досліджується чи утворюють кільця відносно операцій поточкового додавання та множення функцій задані множини дійсних функцій дійсного аргумента.

Приклад 11. Множина $\mathrm{C}[a, b]$ всіх функцій, неперервних на відрізку $[a, b]$.

Нехай $f(x), g(x) \in \mathrm{C}[a, b]$. Із курсу аналізу відомо, що функції $(f + g)(x)$ і $(f \cdot g)(x)$ також належать до $\mathrm{C}[a, b]$. Асоціативність і комутативність операцій додавання і множення, а також дистрибутивність випливають відповідно із асоціативності додавання і множення, а також із дистрибутивності для операцій над дійсними числами і того, що функції додаються і множаться поточково. Розпишемо в деталях, наприклад, доведення асоціативності додавання. Нехай $f(x), g(x), h(x) \in \mathrm{C}[a, b]$. Тоді для будь-якої точки $x \in [a, b]$ внаслідок асоціативності додавання дійсних чисел маємо

$$((f + g) + h)(x) = (f + g)(x) + h(x) = (f(x) + g(x)) + h(x) =$$
$$f(x)+(g(x)+h(x)) = f(x)+(g(x)+h(x)) = f(x)+(g+h)(x) = (f+(g+h))(x).$$

Очевидно, що нейтральним елементом для операції додавання буде нульова функція 0, а протилежною функцією для $f(x)$ буде $-f(x)$. Отже, $\mathrm{C}[a, b]$ є комутативним кільцем.

Приклад 12. $A = \{f \in \mathrm{C}[a, b] : f(x) = 0, x \in I \subset [a, b]\}$

Очевидно, що множина A замкнена відносно операцій додавання та множення. Крім того, якщо $f \in A$, то $-f \in A$. Звідси і з попереднього прикладу випливає, що множина A є підкільцем в $\mathrm{C}[a, b]$.

Приклад 13. Доведіть, що множина $(\mathbb{R}[x], +, \circ)$ всіх многочленів від дійсної змінної x відносно операцій $+$ поточкового додавання та $\circ$ суперпозиції не утворює кільце.

В прикладі 11 доведено, що $(\mathbb{R}[x], +)$ є абелевою групою. Крім того, супераозиція многочленів, є, очевидно, многочленом і добре відомо, що операція суперпозиції функцій є асоціативною. Але ми зараз покажемо,

що у множині $(\mathbb{R}[x], +, \circ)$ не виконується дистрибутивний закон. Нехай, наприклад, $f(x) = x^2$, $g(x) = h(x) = x$, $x \in \mathbb{R}$. Тоді

$$(f(g+h))(x) = f((g+h)(x)) = f(2x) = (2x)^2 = 4x^2, x \in \mathbb{R}.$$

З іншого боку,

$$(fg + fh)(x) = f(g(x)) + f(h(x)) = f(x) + f(x) = x^2 + x^2 = 2x^2, x \in \mathbb{R}.$$

Задачі

1.1 Довести, що для будь-яких елементів кільця $\mathbb{R}$ справедливі рівності:

a) $a \cdot (b - c) = a \cdot b - a \cdot c$; b) $(a - b) \cdot c = a \cdot c - b \cdot c$.

1.2 Довести, що для будь-яких елементів $a, b_1, \ldots, b_n$ кільця $\mathbb{R}$ справедливі рівності:

a) $a \cdot (b_1 + \cdots + b_n) = a \cdot b_1 + \ldots a \cdot b_n$;

b) $(b_1 + \cdots + b_n) \cdot a = b_1 \cdot a + \cdots + b_n \cdot a$.

1.3 Чи утворюють кільця відносно звичайних операцій додавання та множення наступні числові множини:

a) множина всіх цілих невід'ємних чисел;

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

c) множина $\mathbb{Z}[\varepsilon] = \{a_0 + a_1\varepsilon + a_2\varepsilon^2 + \cdots + a_{n-1}\varepsilon^{n-1} \in \mathbb{C} : a_i \in \mathbb{Z}$ для $i \in \{0, 1, \ldots, n-1\}$, ε — первісний корінь степеня n з $1\}$.

d) множина всіх тих раціональних чисел, у нескоротному записі яких знаменники є степенями фіксованого простого числа p.

1.4 Нехай B — множина всіх можливих функцій $f : \mathbb{R}^+ \to \mathbb{R}$ вигляду $f(x) = a_1 x^{b_1} + \cdots + a_n x^{b_n}$, де $n \in \mathbb{N}$, $a_i \in \mathbb{R}$, $b_i \in \mathbb{Q}^+ \cup \{0\}$. Доведіть, що відносно звичайних дій додавання і множення функцій B є комутативним кільцем з одиницею.

1.5 Довести, що множина $\mathbb{Z}_n$ лишків за модулем n $(n \geq 1)$ є комутативним кільцем з одиницею відносно операцій додавання і множення лишків.

1.6 Чи утворюють кільця відносно звичайних операцій поточкового додавання та множення функцій наступні множини функцій:

a) $A = \{f \in \mathrm{C}[a,b] : f(a) \in \mathbb{Q}\}$;

b) $B = \{f \in \mathrm{C}[a,b] : f(a)$ — ірраціональне число$\}$;

c) Множина раціональних функцій від дійсної змінної;

d) Множина функцій, що мають другу похідну на інтервалі (a,b)?

1.7 Довести, що множина

$$F[[x]] = \left\{ \sum_{k=0}^{\infty} a_k x^k : a_k \in F, k \geq 0 \right\}$$

всіх формальних степеневих рядів над полем F є комутативним кільцем з одиницею відносно звичайних додавання і множення рядів.

1.8 Чи утворює кільце множина многочленів від змінної t із операціями "+" — звичайне додавання та "$\circ$" — суперпозиція, тобто $(f \circ g)(t) = f(g(t))$?

1.9 Нехай M— множина, $\mathcal{B}(M)$ — множина всіх її підмножин. Доведіть, що $(\mathcal{B}(M), \triangle, \cap)$ є комутативним кільцем (тут $\triangle$ і $\cap$ — операції симетричної різниці та перетину множин, що розглядаються як додавання і множення відповідно).

1.10 Перевірити, чи є множина A підкільцем кільця $\mathrm{C}[a,b]$:

a) $A = \{f \in \mathrm{C}[a,b] : f(a) = 0\}$;

b) $A = \{f \in \mathrm{C}[a,b] : f(a) = f(b)\}$;

c) $A = \{f \in \mathrm{C}[a,b] : f(\frac{a+b}{2}) \in \mathbb{Q}\}$;

d) $A = \{f \in \mathrm{C}[a,b] : \int_a^b f(x)dx = 0\}$.

1.11 Перевірити, чи є множина A підкільцем кільця $M_2(\mathbb{R})$:

a) $A = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \in M_2(\mathbb{R}) : a,b,c \in \mathbb{R} \right\}$;

b) $A = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \in M_2(\mathbb{R}) : a,c \in \mathbb{Q}, b \in \mathbb{R} \right\}$;

c) $A = M_2(\mathbb{Q})$;

d) $A = \{T \in M_2(\mathbb{R}) : \det T = 0\}$;

e) $A = \{T \in M_2(\mathbb{R}) : \det T \in \mathbb{Q}\}$.

1.12 Довести, що кільце $\mathbb{Z}[\frac{1}{p}]$ рівне кільцю із задачі 1.3d.

1.13 Довести, що підкільця $\mathbb{Z}[\frac{1}{10}]$ та $\mathbb{Z}[\frac{2}{5}, \frac{3}{16}]$ кільця $\mathbb{Q}$ рівні.

1.14 Знайти найменше натуральне число n таке, що кільце $\mathbb{Z}[\frac{1}{n}]$ рівне кільцю:

$$\mathbb{Z}\left[\frac{1}{4}\right]; \quad \mathbb{Z}\left[\frac{5}{18}\right]; \quad \mathbb{Z}\left[\frac{4}{45}, \frac{4}{75}\right]; \quad \mathbb{Z}\left[\frac{7}{24}, \frac{8}{63}\right]; \quad \mathbb{Z}\left[\frac{2}{9}, \frac{7}{12}, \frac{3}{20}\right].$$

1.15 Навести приклад кільця R з одиницею 1 і його підкільця S, яке також є кільцем з одиницею e, причому $e \neq 1$.

1.16 Довести, що кільце, в якому для кожного елемента x виконана рівність $x^2 = x$, є комутативним. Чи правильне аналогічне твердження за умови заміни останньої рівності на $x^3 = x$?

2 Дільники нуля, оборотні та нільпотентні елементи

Нехай R — це деяке кільце.

Означення 3. Ненульовий елемент $a \in R$ називається лівим (відповідно правим) дільником нуля, якщо існує ненульовий елемент $b \in R$ такий, що $ab = 0$ (відповідно $ba = 0$). Дільником нуля називається такий елемент $a \in R$, що a є як лівим, так і правим дільником нуля.

Елемент 0 будемо називати тривіальним дільником нуля. Зрозуміло, що у комутативному кільці лівий дільник нуля буде правим дільником нуля, і навпаки. Тому для комутативних кілець розглядають лише поняття дільника нуля, не виділяючи окремо правих чи лівих дільників нуля.

Означення 4. Комутативне кільце з одиницею без (нетривіальних) дільників нуля називається областю цілісності.

Прикладами областей цілісності є кільце цілих чисел $\mathbb{Z}$, кільце цілих гаусових чисел $\mathbb{Z}[i]$, кільце многочленів $\mathbb{R}[x]$. Натомість декартів добуток ненульових кілець завжди містить нетривіальні дільники нуля.

Кільця, які є областями цілісності, можна охарактеризувати за допомогою умови скоротності таким чином:

Твердження 2. Комутативне кільце R з одиницею є областю цілісності тоді й лише тоді, коли для довільного ненульового елемента $a \in R$ і елементів $b, c \in R$ з рівності $ab = ac$ випливає рівність $b = c$.

Означення 5. Елемент a кільця R називається нільпотентним, якщо для деякого натурального числа n маємо $a^n = 0$. Найменше таке n, що $a^n = 0$, називається ступенем нільпотентності a.

Зв'язок між нільпотентними елементами і дільниками нуля встановлює

Твердження 3. Кожен нільпотентний елемент є дільником нуля.

Обернене твердження є, взагалі кажучи, неправильним.

Нехай тепер R — кільце з одиницею.

Означення 6. Елемент $a \in R$ називається лівим (відповідно правим) дільником одиниці, якщо існує такий $b \in R$ що $ab = 1$ (відповідно $ba = 1$). Якщо елемент є одночасно і лівим, і правим дільником одиниці, то його називають дільником одиниці.

Дільники одиниці, а також ліві та праві дільники одиниці називають відповідно оборотними елементами, оборотними справа та зліва. Для комутативних кілець розглядають лише оборотні елементи.

Приклади розв'язування задач

Приклад 14. Доведіть, що у будь-якому кільці з одиницею R лівий дільник нуля не є правим дільником 1.

Від супротивного, припустимо, що лівий дільник нуля $a \in R$ є правим дільником одиниці. Тоді, згідно з означеннями, знайдуться $0 \neq b \in R$ і $c \in R$, такі, що $0 = ab$ і $1 = ca$. Домноживши останню рівність з правого боку на b, отримаємо $b = cab = c \cdot 0 = 0$, що суперечить вибору елемента b.

Приклад 15. Описати дільники нуля у кільці $\mathbb{Z}_n$.

Нехай $a \in \mathbb{Z}_n$ — дільник нуля. Це означає, що знайдеться такий ненульовий елемент $b \in \mathbb{Z}_n$, що в $\mathbb{Z}_n$ справджується рівність $ab = 0$. Ця рівність, в свою чергу, еквівалентна тому, що ціле число ab ділиться на n. Якби a і n були взаємно простими, то тоді би b ділилося на n, але на n ділиться лише нульовий елемент $\mathbb{Z}_n$. Суперечність. Таким чином, ми довели, що якщо $a \in \mathbb{Z}_n$ — дільник нуля, то a і n не взаємно прості.

Але умова $d_1 > 1$ є також і достатньою для того, щоб елемент $a \in \mathbb{Z}_n$ був дільником нуля. Дійсно, позначимо $b = \frac{n}{d_1}$. Тоді $b \in \mathbb{Z}_n$, $b \neq 0$ і $ab = 0$ в $\mathbb{Z}_n$.

Приклад 16. Описати оборотні елементи у кільці $\mathbb{Z}_n$.

Нехай $a \in \mathbb{Z}_n$ — оборотний елемент. Позначимо $d = \text{НСД}(a, n)$, $a_1 = \frac{a}{d_1}$. Рівність $ab = 1$ в $\mathbb{Z}_n$ рівносильна тому, що ціле число $ab-1 = a_1db-1$ ділиться на n. Звідси і з того, що n ділиться d і ab ділиться d випливає, що 1 мусить ділитися на d. Отже, $d = 1$.

Покажемо, що рівність $d = 1$ є також і достатньою умовою для того, щоб елемент $a \in \mathbb{Z}_n$ був оборотним. Отже, припустимо, що $d = 1$. Покажемо, що числа $a, 2a, \ldots, na$ дають попарно різні остачі при діленні

на n. Припустимо супротивне: ia і ja дають однакові остачі при діленні на n для деяких різних i і j, кожне з яких не менше від одиниці і не більше за n. Тоді $ia - ja = (i-j)a$ ділиться на n. Звідси, враховуючи умову $d = 1$, випливає, що $j - i$ ділиться на n. Але ж $|j - i| < n$. Тому $j = i$, всупереч зробленому припущенню. Таким чином, серед остач, які дають числа $a, 2a, \ldots, na$ при діленні на n, зустрічається, зокрема, і 1 — позначимо через ka число, що дає цю остачу. Але тоді в $\mathbb{Z}_n$ виконується рівність $ka = 1$.

Приклад 17. Описати нільпотентні елементи в кільцях
а) $\mathbb{Z}_{12}$;
б) $\mathbb{Z}_n$.

а) Припустимо, що $k \in \mathbb{Z}_{12}$ — нільпотентний елемент. За означенням, це рівносильно тому, що знайдеться натуральне число t таке, що в Z_{12} виконується рівність $k^t = 0$. Ця рівність еквівалентна тому, що ціле число k^t ділиться на $12 = 2^2 \cdot 3$. Звідси випливає, що k повинно ділитись на 2 і на 3, тобто для k фактично лишається дві можливості $k = 0$ $k = 6$. Звичайно, 0 є нільпотентним елементом (у будь-якому кільці). Нільпотентність елемента 6 випливає з рівності $6^2 \equiv 0 (\mathrm{mod}\, 12)$.

б) Будемо міркувати так само, як в пункті а): якщо $k \in \mathbb{Z}_n$ — нільпотентний елемент, то k^t мусить ділитися на n. Нехай $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_m^{\alpha_m}$ ($\alpha_i \geq 1$ для всіх i)— канонічний розклад числа n на прості множники. З того, що k^t ділиться на p_i, випливає, що k ділиться на p_i $(1 \leq i \leq m)$. А це тягне за собою, що k ділиться на $p_1 p_2 \ldots p_m$.

Покажемо, що будь-який елемент $k = Ap_1 p_2 \ldots p_m \in \mathbb{Z}_n$ є нільпотентним. Покладемо $\alpha = max\{\alpha_1, \ldots, \alpha_m\}$. Тоді натуральне число $k^\alpha = A^\alpha p_1^\alpha p_2^\alpha \ldots p_m^\alpha$ ділиться на n, що тягне нільпотентність елемента $k \in \mathbb{Z}_n$.

Приклад 18. Знайти всі оборотні елементи кільця $\mathbb{Z}[i]$.

Нехай $a + bi$ — оборотний елемент кільця $\mathbb{Z}[i]$. Тоді знайдеться такий елемент $c + di \in \mathbb{Z}[i]$, що $(a + bi)(c + di) = 1$. Звідси випливає рівність для квадратів модулів $(a^2 + b^2)(c^2 + d^2) = 1$, звідки одержуємо рівність $a^2 + b^2 = 1$.

Розглянемо 4 можливих випадки:
1. $a = 1$, $b = 0$. Тоді $z = 1$.
2. $a = -1$, $b = 0$. Тоді $z = -1$.
3. $a = 0$, $b = 1$. Тоді $z = i$.
4. $a = 0$, $b = -1$. Тоді $z = -i$.

Отже, оборотними елементами кільця $\mathbb{Z}[i]$ є $1, -1, i, -i$ і лише вони.

Відзначимо також, що дільників нуля та нільпотентних елементів $\mathbb{Z}[i]$ не має, оскільки таких елементів не має $\mathbb{C}$, підкільцем якого є $\mathbb{Z}[i]$.

Приклад 19. Описати дільники нуля та оборотні елементи у кільці $\mathbb{Z}_p \times \mathbb{Z}_p$, де p — просте число.

Очевидно, елементи вигляду $(0,t), (t,0)$ $(t \in \mathbb{Z}_p)$ є дільниками нуля, оскільки наприклад $(0,t)(1,0) = (t,0)(0,1) = (0,0)$. Покажемо, що інших дільників нуля немає. Нехай $(a,b) \in \mathbb{Z}_p \times \mathbb{Z}_p$ і $a \neq 0, b \neq 0$. З рівності $(a,b)(c,d) = (0,0)$ випливає, що $ac = bd = 0$. Але внаслідок відсутності дільників нуля в кільці $\mathbb{Z}_p$ звідси маємо $c = d = 0$.

Нехай тепер $(a,b) \in \mathbb{Z}_p \times \mathbb{Z}_p$ — оборотний елемент. Тоді знайдеться такий елемент $(c,d) \in \mathbb{Z}_p \times \mathbb{Z}_p$, що $(ac, bd) = (a,b) \cdot (c,d) = (1,1)$. Ця умова рівносильна тому, що a і b є оборотними елементами в $\mathbb{Z}_p$. Але якщо в прикладі 16 покласти $n = p$ ми негайно отримаємо, що оборотними є всі ненульові елементи із $\mathbb{Z}_p$. Таким чином, із того, що $(a,b) \in \mathbb{Z}_p \times \mathbb{Z}_p$ — оборотний елемент, випливає, що $a \neq 0$ і $b \neq 0$.

Покажемо, що умова $a \neq 0$ і $b \neq 0$ є і достатньою для того, щоб елемент $(a,b) \in \mathbb{Z}_p \times \mathbb{Z}_p$ був оборотним. Дійсно, якщо ця умова виконана, то знайдуться $c, d \in \mathbb{Z}_p$ такі, що $ac = 1$ і $bd = 1$ в $\mathbb{Z}_p$. Але тоді $(a,b) \cdot (c,d) = (1,1)$ в $\mathbb{Z}_p \times \mathbb{Z}_p$, звідки випливає, що (a,b) — оборотний елемент.

Приклад 20. Нехай R— скінченне кільце без дільників нуля. Довести, що R має одиницю, і що всі ненульові елементи із R оборотні.

Зафіксуємо якийсь ненульовий елемент $a \in R$ і розглянемо відображення $\varphi_a : R \to R$, визначене правилом $x \mapsto xa$. Відображення φ_a ін'єктивне, оскільки із $xa = ya$ випливає $(x-y)a = 0$, звідки, внаслідок відсутності в R дільників нуля, $x = y$. Але будь-яке ін'єктивне перетворення скінченної множини є бієктивним, тому φ_a — бієктивне. Так само встановлюється бієктивність відображення $\psi_a : R \to R$, визначеного правилом $x \mapsto ax$. Сюр'єктивність відображення ψ_a гарантує існування елемента $e_a \in R$, такого, що $a = \psi_a(e_a) = ae_a$. Покажемо, що e_a є правою одиницею кільця R. Для цього візьмемо будь-яке $b \in R$ і покладемо $y = \varphi^{-1}(b)$. Тоді $b = ya = yae_a = be_a$. Сюр'єктивність відображення φ_a гарантує існування елемента $e'_a \in R$, такого, що $a = \varphi_a(e'_a) = e'_a a$. Міркування, аналогічні попереднім, доводять, що e'_a є лівою одиницею в R. Але тоді $e'_a = e'_a e_a = e_a$ (насправді ми встановили корисний факт: якщо у довільному кільці є ліва і права одиниці, то вони збігаються!). Таким чином, перше твердження — R має одиницю — ми довели.

Позначимо $b = \varphi_a^{-1}(1)$, $c = \psi_a^{-1}(1)$. Тоді $ba = 1$, $ac = 1$. Покажемо, що тоді $b = c$. Справді, $b = b \cdot 1 = b \cdot ac = ba \cdot c = 1 \cdot c = c$. Таким чином, елемент a є оборотним. Оскільки ненульовий елемент $a \in R$ було обрано довільним чином, то всі ненульові елементи із R оборотні.

Приклад 21. Нехай R — кільце з одиницею без дільників нуля. Довести, що кожен елемент, котрий має односторонній обернений, є оборотним.

Припустимо, що елемент $a \in R$ має правий обернений, скажімо, елемент $b \in R$. Тоді $a \neq 0$ і $ab = 1$. Покладемо $y = ba$. Домноживши останню рівність з правого боку на a, отримаємо

$ay = a \cdot ba = ab \cdot a = 1 \cdot a = a$,

звідки $a(y - 1) = 0$. Ця рівність, відсутність дільників нуля в R і умова $a \neq 0$ тягнуть $y = 1$. Таким чином, $ba = 1$, внаслідок чого b є двостороннім оберненим до a. Отже, елемент a — оборотний.

Приклад 22. Нехай x, y — такі елементи кільця R з одиницею без дільників нуля, що елемент xy — оборотний. Довести, що x і y також є оборотними.

За умовою, кільце R має одиницю 1 і існує елемент $a \in R$, такий що $xy \cdot a = a \cdot xy = 1$. Оскільки $x \cdot ya = 1$, то ya — правий обернений до x. Покажемо, що ya буде і лівим оберненим до x. Для цього покладемо $z = ya \cdot x$ і покажемо, що насправді $z = 1$. Помножимо передостанню рівність з лівого боку на x:

$xz = x \cdot ya \cdot x = 1 \cdot x = x$.

Таким чином $x(z - 1) = 0$. Звідси, враховуючи $x \neq 0$ і відсутність в R дільників нуля, робимо висновок, що $z = 1$.

Задачі

2.1 Навести приклад лівого дільника нуля, який не є правим дільником нуля.

2.2 Описати дільники нуля, оборотні та нільпотентні елементи у кільцях

а) $\mathbb{Z}_{32}$;

б) $\mathbb{Z}_{45}$;

в) $\mathbb{Z}_{30}$;

г) $\mathbb{Z}_{p^2}$, p — просте число;

д) $\mathbb{Z}_p^n$, p — просте число;

е) $\mathbb{Z} \times \mathbb{Z}$;

ж) $\mathbb{Z}_{p^{k_1}} \times \cdots \times \mathbb{Z}_{p^{k_r}}$, p — просте число, $k_1, \ldots, k_r$ — натуральні числа.

2.3 Знайти дільники нуля та оборотні елементи кільця $\mathbb{Z}[i\sqrt{d}]$, $d \in \mathbb{N}$, d не є квадратом натурального числа.

2.4 Знайти дільники нуля та оборотні елементи кільця $\mathbb{Z}[\frac{1}{6}]$.

2.5 Знайти дільники нуля та оборотні елементи у кільцях

а) $\mathbb{R} \times \mathbb{R}$;

б) $\mathbb{R} \times \mathbb{Z}$.

2.6 Описати дільники нуля, оборотні та нільпотентні елементи кільця

а) $M_2(\mathbb{R})$;

б) $UT_n(F)$, де F — поле.

2.7 Описати дільники нуля, оборотні та нільпотентні елементи кільця $(\mathcal{B}(M), \triangle, \cap)$ із задачі 1.9.

2.8 Довести, що кільце функцій B із задачі 1.4 є областю цілісності.

2.9 Описати дільники нуля, оборотні та нільпотентні елементи кільця всіх функцій $f : [a, b] \to \mathbb{R}$.

2.10 Довести, що у кільці R з одиницею множина оборотних елементів утворює групу відносно множення. (Цю групу називають мультиплікативною групою кільця R і позначають R^*.)

2.11 Довести, що якщо елемент a^2 кільця R є дільником нуля, то і a є дільником нуля.

2.12 Нехай R — скінченне кільце з одиницею. Довести, що кожен елемент із R, що має односторонній обернений, є оборотним.

2.13 Нехай R — скінченне кільце з одиницею. Довести, що кожен лівий дільник нуля із R буде і правим дільником нуля.

2.14 Нехай x, y — такі елементи кільця R з одиницею, що xy та yx — оборотні елементи. Довести, що x і y також є оборотними.

2.15 Нехай x, y — такі елементи скінченного кільця з одиницею, що елемент xy — оборотний. Довести, що x і y також є оборотними.

2.16 Нехай x, y — такі елементи кільця R з одиницею, що $1 - ab$ — оборотний елемент. Довести, що елемент $1 - ba$ також є оборотним. (Вказівка. Якщо c — елемент, обернений до $1 - ab$, то елемент $1 + bca$ буде оберненим до $1 - ba$.)

3 Ідеали

Для елемента a кільця R і підмножини $B \subset R$ покладемо $aB = \{ab : b \in B\}$. Аналогічний зміст має позначення Ba.

Означення 7. Підкільце I кільця R називається лівим (правим) ідеалом цього кільця, якщо для довільного елемента $a \in R$ має місце включення $aI \subseteq I$ ($Ia \subseteq I$). Двостороннім ідеалом (або просто ідеалом) називають підкільце, котре є лівим і правим ідеалом одночасно.

Очевидними прикладами ідеалів кільця R є нульовий ідеал (містить лише елемент 0 і також позначається 0) і саме R. Ці ідеали називають тривіальними. Кільце, у якого нема нетривіальних ідеалів, називається простим.

В комутативних кільцях поняття лівого, правого та двостороннього ідеалів не розрізняють. Для довільного елемента a комутативного кільця R з одиницею позначимо $(a) = aR$. Легко бачити, що (a) є ідеалом R. Цей ідеал називається головним ідеалом, породженим елементом a. Він є мінімальним серед ідеалів які містять елемент a. Аналогічно в некомутативних кільцях визначаються головні лівий, правий та двосторонній ідеали, породжені елементом цього кільця. Так само можна визначити ідеал, породжений довільною скінченною множиною елементів кільця.

Ідеал I кільця R називається максимальним, якщо $I \neq R$ і для довільного ідеала J кільця R із включень $I \subset J \subset R$ випливає $J = R$ або $J = I$. Комутативне кільце з одиницею називається локальним, якщо воно містить єдиний максимальний ідеал. Ненульовий ідеал I кільця R називається мінімальним, якщо для довільного ідеала J кільця R із включень $0 \subset J \subset I$ випливає $J = 0$ або $J = I$.

Нехай I, J — ідеали кільця R. Тоді перетин $I \cap J$ також є ідеалом, який називається перетином ідеалів I, J. Множина $I + J = \{a + b : a \in I, b \in J\}$ також є ідеалом. Цей ідеал називається сумою ідеалів I, J. Нарешті множина $I \cdot J$, яка складається з усіх можливих сум вигляду $a_1b_1 + \ldots + a_kb_k$, $a_i \in I, b_i \in J$ $(1 \leq i \leq k)$, $k \in \mathbb{N}$, також є ідеалом, котрий називають добутком ідеалів I, J.

Приклади розв'язування задач

Приклад 23. Нехай I — ідеал кільця R. Довести, що коли I містить хоча б один оборотний елемент, то $I = R$.

Нехай $a \in R$ — оборотний елемент. Оскільки I є ідеалом, то $ab \in R$ для будь-якого $b \in R$, зокрема $aa^{-1} = 1 \in I$. Те, що $1 \in I$, означає, що $b = 1 \cdot b \in I$ для всіх b із R, тобто $R \subseteq I$. Таким чином $R = I$.

Із приклада 23 випливає, що будь-який ненульовий ідеал поля F збігається з F. Отже, поле має лише тривіальні ідеали: нульовий ідеал і все поле.

Приклад 24. Довести, що множина всіх оборотних елементів жодного кільця не є ідеалом.

Відомо (задача 2.10), що множина всіх оборотних елементів будь-якого кільця є групою відносно операції множення. Але в жодному кільці множина всіх оборотних елементів не є групою відносно додавання. Справді, інакше б нуль належав до цієї групи, а нуль не є оборотним елементом. Отже, за означенням ідеала множина оборотних елементів довільного кільця таким не є.

Приклад 25. Знайти всі натуральні числа n, такі, що множина всіх необоротних елементів кільця $\mathbb{Z}_n$ утворює ідеал.

Нехай спочатку $n = p^k$, p — просте число. Переконаємось, що в цьому разі множина необоротних елементів кільця $\mathbb{Z}_n$ утворює ідеал. Із опису оборотних елементів кілець $\mathbb{Z}_n$ (приклад 16) випливає, що елемент $m \in \mathbb{Z}_{p^k}$ буде необоротним тоді й лише тоді, коли m ділиться на p, тому множина необоротних елементів збігається з (p) — головним ідеалом, породженим елементом p.

Нехай тепер $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_m^{\alpha_m}$ — канонічний розклад числа n на прості множники і $m \geq 2$ (прості числа $p_1, p_2, \dots, p_m$ попарно різні). Припустимо, що і в цьому випадку необоротні елементи кільця $\mathbb{Z}_n$ утворюють ідеал, який позначимо I. Позначимо $n_1 = p_1^{\alpha_1}$, $n_2 = p_2^{\alpha_2} \dots p_m^{\alpha_m}$. Позаяк n_1 і n_2 не взаємно прості з n, то, враховуючи приклад 16, $n_1, n_2 \in I$. Але $(n_1, n_2) = 1$ і тому знайдуться цілі d_1 і d_2 такі, що $1 = n_1 d_1 + n_2 d_2$. За означенням ідеала, права частина останньої рівності (за модулем n) потрапляє до I. Тому $1 \in I$. Але 1 — оборотний елемент! Суперечність.

Резюмуємо вищесказане. Множина необоротних елементів кільця $\mathbb{Z}_n$ утворює ідеал тоді й тільки тоді, коли $n = p^k$, p — просте число.

Приклад 26. Описати ідеали кільця $\mathbb{Z}_n$.

За означенням, ідеал кільця є підгрупою його адитивної групи. Покажемо, що у випадку $\mathbb{Z}_n$ ідеалом буде будь-яка підгрупа адитивної групи

$\mathbb{Z}_n$. Відомо, що підгрупи із $\mathbb{Z}_n$ знаходяться у взаємно-однозначній відповідності із дільниками числа n і є циклічними групами із твірними елементами $\frac{n}{d_1}, \frac{n}{d_2}, \ldots, \frac{n}{d_k}$, де $d_1, d_2, \ldots, d_k$ — всі дільники числа n. Візьмемо будь-яку з цих підгруп, скажімо, підгрупу I, породжену числом $k = \frac{n}{d}$, де d — якийсь дільник n. Елементами групи I є всі елементи із $\mathbb{Z}_n$, які кратні k. Тобто

$$I = \{k, 2k, \ldots, (d-1)k, dk = 0\}.$$

Для будь-яких елементів $ik \in I$ і $j \in \mathbb{Z}_n$ їх добуток $ijk (\mathrm{mod}\, n)$ знов буде елементом із I. Справді, $ijk (\mathrm{mod}\, n) = ijk - nl$ для якогось $l \in \mathbb{Z}$. Але оскільки права частина останньої рівності ділиться на k, то на k ділиться також і ліва частина. Отже, I є ідеалом кільця $\mathbb{Z}_n$.

Приклад 27. Довести, що в кільці $M_n(F)$, де F — поле, немає двосторонніх ідеалів, відмінних від нульового і $M_n(F)$, тобто це кільце є простим.

Припустимо, що I — ненульовий ідеал кільця $M_n(F)$. Візьмемо будь-яку, відмінну від нульової, матрицю $A \in I$. Нехай r — ранг матриці A. Із курсу лінійної алгебри відомо, що за допомогою елементарних перетворень типів 1,2,3 над рядками і стовпчиками (тип 1: до одного рядка (стовпчика) додаємо інший, домножений на $\lambda \in F$, тип 2: множимо рядок (стовпчик) на $\lambda \in F, \lambda \neq 0$, тип 3: переставляємо будь-які два рядки (стовпчики)) матриця A зводиться до матриці

$$A' = \begin{pmatrix} 1 & 0 & \ldots & 0 & 0 & \ldots & 0 \\ 0 & 1 & \ldots & 0 & 0 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & 1 & 0 & \ldots & 0 \\ 0 & 0 & \ldots & 0 & 0 & \ldots & 0 \\ 0 & 0 & \ldots & 0 & 0 & \ldots & 0 \end{pmatrix}$$

, причому кількість одиничок на діагоналі матриці A' дорівнює r. Згадаємо тепер, що виконати елементарне перетворення над рядками чи стовпчиками матриці — це те саме, що помножити матрицю справа (зліва) на відповідну елементарну матрицю. Враховуючи це зауваження і те, що I — ідеал, отримуємо, що $A' \in I$. Оскільки $A'E_{11} = E_{11}$, то $E_{11} \in I$ (нагадаємо, що через E_{ij} звичайно позначається матриця, в якої елемент на перетині i-го рядка та j-го стовпчика дорівнює 1, а решта елементів — нулі). Переставляючи в матриці E_{11} перший і i-ий рядки, а потім перший і i-ий стовпчики отримаємо матрицю E_{ii} $(2 \leq i \leq n)$. Отже, E_{ii} може бути одержана із E_{11} множенням зліва і справа на деякі елементарні матриці, тому $E_{ii} \in I$,

$1 \leq i \leq n$. Тепер, зважаючи на замкненість I відносно додавання, маємо $E_{11} + E_{22} + \cdots + E_{nn} = E \in I$. Але ж ідеал кільця, що містить одиницю цього кільця, збігається з усім кільцем (див. розв'язок приклада 23). Таким чином, $I = M_n(F)$, а це ми і прагнули довести.

Задачі

3.1 Довести, що у кільці $\mathbb{Z}$ будь-яке підкільце є ідеалом.

3.2 Довести, що множина всіх нільпотентних елементів кільця $\mathbb{Z}_n$ утворює ідеал.

3.3 Нехай A — комутативне кільце і $c \in A$. Довести, що множина $cA = \{ca \in A : a \in A\}$ є ідеалом кільця A.

3.4 Наведіть приклад кільця K та його підкільця K_1, таких, що K_1 не є ідеалом K.

3.5 Нехай $R = \{f : [0,1] \to \mathbb{R}\}$. Які з наступних множин функцій утворюють ідеал кільця R:

а) $A_1 = \{f \in R : f(0) \in \mathbb{Q}\}$;

б) $A_2 = \{f \in R : f(0) = f(1)\}$;

в) $A_3 = \{f \in R : f(x) = 0, 1 < x < 1\}$;

г) $A_4 = \{f \in R : \int_0^1 f(x)dx = 0\}$?

3.6 Опишіть всі ліві і праві ідеали кільця $M_2(F)$.

3.7 Нехай A і B — кільця з одиницями. Доведіть, що кожний ідеал кільця $A \times B$ має вигляд $I_1 \times I_2$, де I_1 і I_2 — ідеали кілець A і B відповідно.

3.8 Навести приклад такого ідеала кільця $2\mathbb{Z}_8 \times 2\mathbb{Z}_8$, який не може бути подано у вигляді $I_1 \times I_2$, де I_1 і I_2 — ідеали кільця $2\mathbb{Z}_8$.

3.9 Описати максимальні і мінімальні ідеали кілець:

а) $\mathbb{Z}_{60}$;

б) $\mathbb{Z}_n$;

в) $\mathbb{Z}$;

г) $K[x]$

3.10 Нехай R — кільце неперервних функцій на відрізку $[0,1]$,

$$I_c = \{f(x) \in R : f(c) = 0\}(0 \leq c \leq 1).$$

Довести, що I_c — максимальний ідеал R. Чи правда, що будь-який максимальний ідеал R збігається з I_c для деякого c?

3.11 Довести, що для довільного простого p кільце $\mathbb{Z}_{(p)} = \{\frac{m}{n} : m \in \mathbb{Z}, n \in \mathbb{N}, (n,p) = 1\}$ є локальним.

3.12 Довести, що кільце $F[[x]]$ формальних степеневих рядів над полем F є локальним.

4 Гомоморфізми та факторкільця

Нехай R_1 і R_2 — довільні кільця.

Означення 8. Відображення $\varphi : R_1 \to R_2$ називається гомоморфізмом кілець, якщо воно узгоджене з операціями додавання і множення в цих кільцях, тобто для довільних $a, b \in R_1$ мають місце рівності:
1) $\varphi(a + b) = \varphi(a) + \varphi(b)$;
2) $\varphi(ab) = \varphi(a)\varphi(b)$.

Нехай R_1 і R_2 є кільцями з одиницями 1 і e відповідно. Гомоморфізм кілець $\varphi : R_1 \to R_2$ називається гомоморфізмом кілець з одиницею, якщо $\varphi(1) = e$.

Гомоморфізм φ кілець називається епіморфізмом, мономорфізмом чи ізоморфізмом, якщо φ є сюр'єкцією, ін'єкцією чи бієкцією відповідно.

Кільця R_1, R_2 називаються ізоморфними (позначають $R_1 \simeq R_2$), якщо між ними існує ізоморфізм.

З кожним гомоморфізмом $\varphi : R_1 \to R_2$ пов'язують його ядро, тобто множину $Ker\varphi = \{a \in R_1 : \varphi(a) = 0\}$, і образ, тобто множину $Im\varphi = \{\varphi(a) : a \in R_1\}$.

Твердження 4. Ядро гомоморфізму $\varphi : R_1 \to R_2$ є ідеалом в R_1, а образ — підкільцем у R_2.

Нехай тепер I — це ідеал кільця R. Тоді I є підгрупою адитивної групи кільця R, яка є абелевою, а тому множина R/I лівих класів суміжності R за I є абелевою групою відносно операції додавання, визначеної рівністю

$$(a + I) + (b + I) = (a + b) + I, \quad a, b \in R.$$

Визначимо на множині R/I операцію множення, поклавши

$$(a + I) \cdot (b + I) = (ab) + I, \quad a, b \in R.$$

Таке визначення є коректним, тобто не залежить від вибору представників класів суміжності (для доведення якраз і використовується умова з означення ідеала, яка вирізняє його серед підкілець).

Твердження 5. Множина R/I з вищеозначеними операціями додавання і множення є кільцем.

Кільце R/I називається факторкільцем кільця R за ідеалом I.

Твердження 6. Факторкільце комутативного кільця (кільця з одиницею) є комутативним (кільцем з одиницею).

Важливим інструментом для доведення ізоморфності кілець є така теорема про гомоморфізми.

Теорема 1. Нехай $\varphi : R_1 \to R_2$ — гомоморфізм кілець. Тоді

$$R_1/Ker\varphi \simeq Im\varphi.$$

Ідеал I комутативного кільця R з одиницею називається простим, якщо для довільних $a, b \in R$ з включення $ab \in I$ випливає $a \in I$ або $b \in I$.

Твердження 7. Ідеал I комутативного кільця R з одиницею є простим тоді й лише тоді, коли факторкільце R/I є областю цілісності.

Твердження 8. Ідеал I комутативного кільця R з одиницею є максимальним тоді й лише тоді, коли факторкільце R/I є полем.

Приклади розв'язування задач

Приклад 28. Нехай $\varphi : R_1 \to R_2$ — епіморфізм, 1 — одиниця кільця R_1. Довести, що $\varphi(1)$ є одиницею кільця R_2.

Покладемо $c = \varphi(1) \in R_2$. Нехай $b \in R_2$ — довільний елемент. Ми маємо показати, що $cb = bc = b$. Із того, що φ — епіморфізм, випливає, що $b = \varphi(a)$ для якогось $a \in R_1$. Але рівність $a \cdot 1 = 1 \cdot a = 1$ в кільці R_1 тягне відповідну рівність для φ-образів в R_2: $\varphi(a) \cdot \varphi(1) = \varphi(1) \cdot \varphi(a) = \varphi(a)$, тобто $cb = bc = b$, що нам й потрібно.

Приклад 29. Нехай $\varphi : R_1 \to R_2$ — ізоморфізм, $a \in R_1$ — дільник нуля. Довести, що $\varphi(a)$ — дільник нуля в R_2.

Позначимо $c = \varphi(a) \in R_2$. За умовою, знайдеться ненульовий елемент $b \in R_1$, такий що $ab = 0$. Переходячи до φ-образів, отримаємо $\varphi(a) \cdot \varphi(b) = \varphi(0)$ в R_2. Оскільки ізоморфізм кілець є ізоморфізмом їх адитивних груп, то $\varphi(0) = 0$ (у лівій частині стоїть нуль кільця R_1, а у правій — нуль R_2). Оскільки φ — бієктивне відображення, то $d = \varphi(b) \neq 0$. Отже, в R_2 справджується рівність $cd = 0$, причому $d \neq 0$. Таким чином, c — дільник нуля в R_2.

Приклад 30. Довести, що кільце $\mathbb{Z}_{15}/(5)$ ізоморфне кільцю $\mathbb{Z}_5$.

Якщо ми побудуємо епіморфізм $\varphi : \mathbb{Z}_{15} \to \mathbb{Z}_5$, ядром якого є (5), то потрібне нам твердження буде випливати із теореми про гомоморфізм кілець. Правило побудови такого епіморфізму винайти неважко: всі елементи із $\mathbb{Z}_{15}$, кратні 5, повинні перейти в 0, крім того, епіморфний образ $\mathbb{Z}_{15}$ повинен складатися з п'яти елементів, тому спадає на думку перевести $a \in \mathbb{Z}_{15}$ в остачу, яку a дає при діленні на 5. Тобто ми будуємо відображення $\varphi : \mathbb{Z}_{15} \to \mathbb{Z}_5$, $a \mapsto a(\mathrm{mod}\, 5)$. Тепер ми повинні акуратно перевірити, що φ дійсно є епіморфізмом, ядром якого є (5):

$$\varphi(a+b) = (a+b)(\mathrm{mod}\, 5) = a(\mathrm{mod}\, 5) + b(\mathrm{mod}\, 5) = \varphi(a) + \varphi(b);$$

$$\varphi(a \cdot b) = (a \cdot b)(\mathrm{mod}\, 5) = a(\mathrm{mod}\, 5) \cdot b(\mathrm{mod}\, 5) = \varphi(a) \cdot \varphi(b).$$

Крім цього, очевидно, будь-який елемент $a \in \mathbb{Z}_5$ має φ-прообраз, наприклад, $a \in \mathbb{Z}_{15}$ (оскільки $a = \varphi(a)$), і на додачу,

$$\varphi(a) = 0 \Leftrightarrow a(\mathrm{mod}\, 5) = 0 \Leftrightarrow a \in (5).$$

Приклад 31. Знайти кількість елементів факторкільця

$$\mathbb{Z}_8[x,y]/(2, x^5, y^7).$$

Кожен клас — елемент факторкільця — містить єдиний многочлен вигляду

$$\sum_{0 \le i \le 4,\ 0 \le j \le 6} a_{ij} x^i y^j,$$

де a_{ij} може дорівнювати 0 або 1. Звідси негайно випливає, що кількість елементів факторкільця дорівнює кількості вказаних многочленів, а саме 2^{35}.

Приклад 32. Довести, що $\mathbb{R}[x]/(x^2+1) \simeq \mathbb{C}$.

Перший спосіб. Уведемо позначення $I = (x^2+1)$. За означенням факторкільця, елементами $\mathbb{R}[x]/I$ є класи вигляду $f + I$, де $f \in \mathbb{R}[x]$, причому $f + I = g + I$ тоді й лише тоді, коли многочлен $f - g$ належить до I, тобто кратний до x^2+1. Остання умова рівносильна тому, що f і g дають однакові остачі при діленні на x^2+1. Тому $f + I = f \mod (x^2+1) + I$ для будь-якого $f \in \mathbb{R}[x]$ (через $f \mod (x^2+1)$ ми позначаємо остачу від ділення f на x^2+1). Оскільки множиною остач від ділення на x^2+1 є $\{a+bx :\ a,b \in \mathbb{R}\}$, то $\mathbb{R}[x]/I = \{a+bx+I :\ a,b \in \mathbb{R}\}$, причому $a + bx + I = c + dx + I$ тоді й лише тоді, коли $a + bx = c + dx$ (тобто $a = c$ і $b = d$).

Розглянемо відображення $\varphi : \mathbb{R}[x]/I \to \mathbb{C}$, визначене правилом $a + bx + I \mapsto a + bi$. Пересвідчимось, що воно є ізоморфізмом.

Ін'єктивність. Нехай $a + bx + I \neq c + dx + I$, але $a + bi = c + di$. Два комплексних числа рівні, коли в них однакові дійсні та уявні частини, тому $a = c$ і $b = d$. Але ж це призводить до суперечності: $a + bx + I = c + dx + I$. Отже із $a + bx + I \neq c + dx + I$ завжди випливає $a + bi \neq c + di$. Сюр'єктивність випливає із того, що $a + bi = \varphi(a + bx)$ для будь-якого комплексного числа $a + bi$.

Гомоморфність. Те, що φ зберігає додавання, випливає із ланцюга рівностей

$$\varphi(a + bx + c + dx + I) = \varphi((a + c) + (b + d)x + I) = \\ a + c + (b + d)i = a + bi + c + di = \varphi(a + bx + I) + \varphi(c + dx + I).$$

Лишилось встановити, що φ зберігає множення. Справді,

$$\varphi((a + bx + I) \cdot (c + dx + I)) = \varphi((bd)x^2 + (bc + ad)x + ac + I) = \\ \varphi((ac - bd) + (bc + ad)x + I) = (ac - bd) + (bc + ad)i = (a + bi) \cdot (c + di) = \\ \varphi(a + bx) \cdot \varphi(c + dx).$$

Третя рівність останнього ланцюга виконується, оскільки при діленні на $x^2 + 1$ многочлен $(bd)x^2 + (bc + ad)x + ac$ дає остачу $(ac - bd) + (bc + ad)x$ (найпростіше прийти до цього через такі міркування: x^2, очевидно, дає остачу -1 при діленні на $x^2 + 1$, звідки $(bd)x^2$ дає остачу $-bd$, звідки, в свою чергу, $(bd)x^2 + (bc + ad)x + ac$ дає остачу $-(bd) + (bc + ad)x + ac = (ac - bd) + (bc + ad)x$).

Другий спосіб. Оскільки потрібно довести ізоморфізм двох кілець, одне з яких є факторкільцем, то можна спробувати застосувати теорему про гомоморфізм кілець. Розглянемо відображення $\varphi : \mathbb{R}[x]/(x^2 + 1) \to \mathbb{C}$, таке, що $f(x) \mapsto f(i)$.

Почнемо з перевірки, що φ — гомоморфізм кілець:

$$\varphi(f(x) + g(x)) = \varphi((f + g)(x)) = (f + g)(i) = \\ f(i) + g(i) = \varphi(f(x)) + \varphi(g(x));$$

$$\varphi(f(x) \cdot g(x)) = \varphi((fg)(x)) = (f \cdot g)(i) = f(i) \cdot g(i) = \varphi(f(x)) \cdot \varphi(g(x)).$$

Оскільки $a + bi = \varphi(a + bx)$ для довільного комплексного числа $a + bi$, то відображення φ — сюр'єктивне.

Нарешті покажемо, що $\mathrm{Ker}(\varphi) = (x^2+1)$. $f(x) \in \mathrm{Ker}(\varphi)$ тоді й лише тоді, коли i — корінь $f(x)$. Але оскільки $f(x)$ має дійсні коефіцієнти, то останнє еквівалентне тому, що $i, -i$ — корені $f(x)$, тобто $f(x)$ кратний до $(x+i)(x-i) = x^2+1$.

Приклад 33. Нехай $f_1(x) = x^2+1$, $f_2(x) = x^2$, $f_3(x) = x^2+x+1$, $f_4(x) = x^2+x \in \mathbb{Z}_2[x]$ (це повний список многочленів степеня 2 над $\mathbb{Z}_2$). Для кожного i, $1 \le i \le 4$ через K_i позначимо факторкільце $\mathbb{Z}_2[x]/(f_i)$. Описати елементи факторкільця K_i, виписати таблички додавання та множення в K_i для кожного i $(1 \le i \le 4)$; розбити множину $\{K_1, K_2, K_3, K_4\}$ на класи попарно ізоморфних кілець. З'ясувати, які з кілець K_1, K_2, K_3, K_4 є полями.

Нехай $1 \le i \le 4$. Елементи K_i — це класи вигляду $f+(f_i)$, $f \in \mathbb{Z}_2[x]$, причому $f+(f_i) = g+(f_i)$ тоді й лише тоді, коли f і g дають однакові остачі (а саме $f \mod f_i = g \mod f_i$) при діленні на f_i. Оскільки f_i — многочлен степеня 2, то кожен клас $f+(f_i)$ містить єдиний многочлен степеня не вище 1, тобто многочлен вигляду $ax+b, a, b \in \mathbb{Z}_2$. Таких многочленів всього 4: $0, 1, x, x+1$. Звідси випливає, що K_i складається із чотирьох елементів:

$$K_i = \{0+(f_i), 1+(f_i), x+(f_i), x+1+(f_i)\}.$$

Табличка додавання для кожного з K_i $(1 \le i \le 4)$ має вигляд

$+$	$0+(f_i)$	$1+(f_i)$	$x+(f_i)$	$x+1+(f_i)$
$0+(f_i)$	$0+(f_i)$	$1+(f_i)$	$x+(f_i)$	$x+1+(f_i)$
$1+(f_i)$	$1+(f_i)$	$0+(f_i)$	$x+1+(f_i)$	$x+(f_i)$
$x+(f_i)$	$x+(f_i)$	$x+1+(f_i)$	$0+(f_i)$	$1+(f_i)$
$x+1+(f_i)$	$x+1+(f_i)$	$x+(f_i)$	$1+(f_i)$	$0+(f_i)$

Для того, щоб обчислити, наприклад, $(x+1+(f_i))+(x+(f_i))$ ми скористалися означенням додавання елементів факторкільця $f+(f_i)+g+(f_i) = f+g+(f_i)$ і правилом додавання многочленів над $\mathbb{Z}_2$: $x+1+x = 1$.

Таблички множення для K_1, K_2, K_3, K_4 відповідно наступні:

$K_1, \cdot$	$0+I_1$	$1+I_1$	$x+I_1$	$x+1+I_1$
$0+I_1$	$0+I_1$	$0+I_1$	$0+I_1$	$0+I_1$
$1+I_1$	$0+I_1$	$1+I_1$	$x+I_1$	$x+1+I_1$
$x+I_1$	$0+I_1$	$x+I_1$	$1+I_1$	$x+1+I_1$
$x+1+I_1$	$0+I_1$	$x+1+I_1$	$x+1+I_1$	$0+I_1$

$K_2, \cdot$	$0+I_2$	$1+I_2$	$x+I_2$	$x+1+I_2$
$0+I_2$	$0+I_2$	$0+I_2$	$0+I_2$	$0+I_2$
$1+I_2$	$0+I_2$	$1+I_2$	$x+I_2$	$x+1+I_2$
$x+I_2$	$0+I_2$	$x+I_2$	$0+I_2$	$x+I_2$
$x+1+I_2$	$0+I_2$	$x+1+I_2$	$x+I_2$	$1+I_2$

$K_3, \cdot$	$0+I_3$	$1+I_3$	$x+I_3$	$x+1+I_3$
$0+I_3$	$0+I_3$	$0+I_3$	$0+I_3$	$0+I_3$
$1+I_3$	$0+I_3$	$1+I_3$	$x+I_3$	$x+1+I_3$
$x+I_3$	$0+I_3$	$x+I_3$	$x+1+I_3$	$1+I_3$
$x+1+I_3$	$0+I_3$	$x+1+I_3$	$1+I_3$	$x+I_3$

$K_4, \cdot$	$0+I_4$	$1+I_4$	$x+I_4$	$x+1+I_4$
$0+I_4$	$0+I_4$	$0+I_4$	$0+I_4$	$0+I_4$
$1+I_4$	$0+I_4$	$1+I_4$	$x+I_4$	$x+1+I_4$
$x+I_4$	$0+I_4$	$x+I_4$	$x+I_4$	$0+I_4$
$x+1+I_4$	$0+I_4$	$x+1+I_4$	$0+I_4$	$x+1+I_4$

Як було обчислено, наприклад, $(x+1+I_3)(x+I_3)$ в K_3? $(x+1+I_3)(x+I_3) = x^2+x+I_3 = x^2+x+1+1+I_3 = 1+I_3$ (остання рівність грунтується на тому, що $x^2+x+1+1$ і 1 дають однакові остачі при діленні на x^2+x+1).

Із табличок множення легко видно, чи є елемент кільця дільником нуля або оборотним елементом. Візьмемо, наприклад, табличку множення для K_1. У горизонтальному рядку елемента $x+I_1$ зустрічається одиничка, отже $x+I_1$ — оборотний елемент. А от у горизонтальному рядку елемента $x+1+I_1$ одиничи немає, але 0 зустрічається двічі: перше входження нуля — результат множення на 0, а друге входження нуля — результат множення на $x+1+I_1$ — свідчить про те, що $x+1+I_1$ — дільник нуля.

Із побудованих табличок множення видно, що K_3 — єдине з факторкілець, в якому кожен ненульовий елемент має обернений, отже, K_3 і лише воно є полем. Далі, кільце K_4 має 2 дільники нуля, в той час як K_1 і K_2 — по одному дільнику нуля. Оскільки ізоморфізм є бієкцією, що переводить дільник нуля в дільник нуля, то $K_4 \not\cong K_1$ і $K_4 \not\cong K_2$.

Кільця K_1 K_2 не є полями, кожне з них має по 2 дільники нуля. Сказане, однак, не тягне за собою ізоморфності цих кілець. Для того, щоб з'ясувати, чи ізоморфні наші кільця, треба перевірити, чи можна встановити ізоморфізм між ними. Якщо $\varphi : K_1 \to K_2$ — ізоморфізм, то

$\varphi(0+I_1)=0+I_2$, $\varphi(1+I_1)=1+I_2$, оскільки при ізоморфізмі нуль переходить в нуль, а одиниця — в одиницю. Оскільки при ізоморфізмі образ дільника нуля є дільником нуля, то повинно бути $\varphi(x+I_1)=x+1+I_2$, $\varphi(x+1+I_1)=x+I_2$. Ми побудували бієкцію $\varphi: K_1\to K_2$. Якщо тепер в табличках додавання і множення для K_1 кожне входження $0+I_1$ замінити на $0+I_2$, $1+I_1$ — на $1+I_2$, $x+I_1$ — на $x+1+I_2$, $x+1+I_1$ — на $x+I_2$, то ми отримаємо відповідно таблички додавання і множення для K_2. Оскільки фактично ми замінили кожен елемент із K_1 на його $\varphi-$образ, то встановлено, що φ є гомоморфізмом. Отже, $K_1\simeq K_2$. Зауважимо, що ізоморфність кілець K_1 і K_2 безпосередньо випливає ще й з наступного прикладу 34. Таким чином, класи попарно ізоморфних кілець такі: $\{K_1,K_2\}$, $\{K_3\}$, $\{K_4\}$.

Приклад 34. Нехай $a\neq b$ і $c\neq d$ — елементи поля F. Доведіть ізоморфність факторкілець $F[x]/\left((x-a)(x-b)\right)$ і $F[x]/\left((x-c)(x-d)\right)$.

Позначимо $K_1=F[x]/\left((x-a)(x-b)\right)$, $K_2=F[x]/\left(x(x-1)\right)$, $I_1=((x-a)(x-b))$, $I_2=(x(x-1))$. Оскільки відношення ізоморфності на множині кілець є транзитивним, досить показати, що $K_1\simeq K_2$. Спочатку опишемо дільники нуля кілець K_1 і K_2. Якщо $\alpha x+\beta+I_1$ — дільник нуля із K_1, то знайдеться елемент $\gamma x+\delta+I_1\in K_1$, такий, що $(\alpha x+\beta+I_1)(\gamma x+\delta+I_1)=0+I_1$, звідки $(\alpha x+\beta)(\gamma x+\delta)+I_1=0+I_1$, тобто многочлен $(\alpha x+\beta)(\gamma x+\delta)$ ділиться на $(x-a)(x-b)$. Але якщо один многочлен другого степеня ділиться на інший многочлен другого степеня, то ці многочлени пропорційні. Таким чином, для деякого ненульового скаляра $k\in F$ $\alpha x+\beta=k(x-a)$ або ж $\alpha x+\beta=k(x-b)$. Отже встановлено, що дільник нуля в K_1 повинен мати вигляд $k(x-a)+I_1$ або $k(x-b)+I_1$. Навпаки, будь-який елемент із K_1 вигляду $k(x-a)+I_1$ або $k(x-b)+I_1$ є дільником нуля, оскільки $(x-a+I_1)(x-b+I_1)=0+I_1$. Отже, дільниками нуля в K_1 є $k(x-a)+I_1$, $k(x-b)+I_1$ і лише вони.

Якщо покласти $a=0$, $b=1$, отримаємо опис дільників нуля в K_2 — це класи $kx+I_2$, $k(x-1)+I_2$ $(k\in F\setminus\{0\})$ і лише вони.

Нехай $\varphi: K_2\to K_1$ — ізоморфізм. Оскільки при ізоморфізмі дільник нуля відображується у дільник нуля, то $\varphi(x+I_2)=k(x-a)+I_1$ або $\varphi(x+I_2)=k(x-b)+I_1$ для деякого $k\in F$. Нехай, для визначеності, $\varphi(x+I_2)=k(x-a)+I_1$. Якщо б для деякого $m\in F$ справджувалось $\varphi(x-1+I_2)=m(x-a)+I_1$, то тоді б

$$\varphi(1+I_2)=\varphi((x+I_2)-(x-1+I_2))=$$
$$(k(x-a)+I_1)-(m(x-a)+I_1)=(k-m)(x-a)+I_1.$$

Однак, при ізоморфізмі одиниця мусить відображатися в одиницю, тому повинно було б бути $(k-m)(x-a)+I_1 = 1+I_1$. Звідси випливає, що многочлен $(k-m)(x-a)-1$ ділився би на $(x-a)(x-b)$. Тобто $(k-m)(x-a)-1=0$, звідки $k=m$. Але остання рівність суперечить ін'єктивності φ. Оскільки $\varphi(x-1+I_2)$ — дільник нуля в K_1 і випадок $\varphi(x-1+I_2) = m(x-a)+I_1$ неможливий, то $\varphi(x-1+I_2) = m(x-b)+I_1$ для деякого $m \in F$. Тепер скористаємось тим, що $\varphi(1+I_2) = 1+I_1$:

$$1+I_1 = \varphi(1+I_2) = \varphi((x+I_2)-(x-1+I_2)) = \varphi(x+I_2)-\varphi((x-1)+I_2) = (k(x-a)+I_1)-(m(x-b)+I_1) = (k-m)x+(mb-ka)+I_1.$$

Таким чином, $(k-m)x+(mb-ka-1) \in I_1$, звідки многочлен $(k-m)x+(mb-ka-1)$ ділиться на $(x-a)(x-b)$, звідки випливає, що $(k-m)x+(mb-ka-1)=0$. Оскільки в нульового многочлена всі коефіцієнти рівні нулю, $k=m=\frac{1}{b-a}$. Отже,

$$\varphi(x+I_2) = \frac{x-a}{b-a}+I_1, \quad \varphi(x-1+I_2) = \frac{x-b}{b-a}+I_1. \tag{1}$$

Покажемо тепер, що відображення φ, визначене за допомогою 1, продовжується до ізоморфізму.

Будь-який елемент із K_2 подається у вигляді лінійної комбінації $(x+I_2)$ та $(x-1+I_2)$: $px+q+I_2 = p(x+I_2)+q(x+I_2-(x-1+I_2))$ $= (p+q)x+I_2-q((x-1)+I_2)$. Покладемо:

$$\varphi(px+q(x-1)+I_2) = p\varphi(x+I_2)+q\varphi(x-1+I_2) = p\frac{x-a}{b-a}+q\frac{x-b}{b-a}+I_1 = \frac{1}{b-a}(p(x-a)+q(x-b))+I_1.$$

Покажемо, що побудоване відображення $\varphi : K_2 \to K_1$ є ізоморфізмом. Те, що φ зберігає додавання, випливає безпосередньо із визначення. Оскільки $\frac{x-a}{b-a}$ і $\frac{x-b}{b-a}$ лінійно незалежні, то φ бієктивне. Пересвідчимось нарешті, що φ зберігає множення:

$$\varphi((px+q(x-1)+I_2)\cdot(p_1x+q_1(x-1)+I_2)) = \varphi(pp_1x^2+qq_1(x-1)^2+I_2) = \varphi(pp_1x^2-qq_1(x-1)+I_2) = pp_1\frac{x-a}{b-a}+qq_1\frac{x-b}{b-a}+I_1, \tag{2}$$

$$\varphi(px+q(x-1)+I_2)\cdot\varphi(p_1x+q_1(x-1)+I_2)=$$
$$(p\frac{x-a}{b-a}+q\frac{x-b}{b-a}+I_1)(p_1\frac{x-a}{b-a}+q_1\frac{x-b}{b-a}+I_1)=$$
$$pp_1\frac{(x-a)^2}{(b-a)^2}+qq_1\frac{(x-b)^2}{(b-a)^2}+I_1=$$
$$pp_1\frac{x-a}{b-a}+qq_1\frac{x-b}{b-a}+I_1, \quad (3)$$

оскільки $(x-a)^2=(x-a)(x-b)+(x-a)(b-a)$, а тому $(x-a)^2+I_1=(x-a)(b-a)+I_1$. Аналогічно $(x-b)^2+I_1=(x-b)(b-a)+I_1$. Рівності (2), (3) якраз і означають, що φ зберігає множення.

Приклад 35. Доведіть, що факторкільця $\mathbb{Z}[x]/(x^2-2)$ і $\mathbb{Z}[x]/(x^2-3)$ не ізоморфні.

Позначимо $I_1=(x^2-2)$, $I_2=(x^2-3)$. Міркуватимемо від супротивного. Нехай $\varphi:\mathbb{Z}[x]/(x^2-2)\to\mathbb{Z}[x]/(x^2-3)$ — ізоморфізм. Оскільки $\varphi(1+I_1)=1+I_2$, то $\varphi(2+I_1)=\varphi((1+I_1)+(1+I_1))=\varphi(1+I_1)+\varphi(1+I_1)=(1+I_2)+(1+I_2)=2+I_2$. В $\mathbb{Z}[x]/(x^2-2)$ є елемент, квадрат якого дорівнює $2+I_1$: це $x+I_1$ (дійсно: $(x+I_1)^2=x^2+I_1=2+(x^2-2)+I_1=2+I_1$). Нехай $\varphi(x+I_1)=ax+b+I_2$ $(a,b\in\mathbb{Z})$. Тоді

$$2+I_2=\varphi((x+I_1)^2)=(ax+b+I_2)^2=a^2x^2+2abx+b^2+I_2=$$
$$a^2(x^2-3)+3a^2+b^2+2abx+I_2=2abx+(3a^2+b^2)+I_2,$$

звідки $2+I_2=2abx+(3a^2+b^2)+I_2$. Ця рівність означає, що $2ab=0$ і $3a^2+b^2=2$. Але, очевидно, що жодна пара цілих чисел a,b не задовільняє останнє рівняння. Отримали суперечність. Отже, ізоморфізм між заданими кільцями встановити не можна.

Ідея, на які базувалися наші міркування, така: в першому факторкільці є елемент, квадрат якого дорівнює двійці, а у другому такого елемента немає. З іншого боку, елемент, в квадраті рівний двійці при ізоморфізмі мусить переходити в елемент з такою ж властивістю. Отже, ізоморфізм побудувати неможливо.

Приклад 36. Нехай $I=\{f\in C[0,1]:\ f(0)=f(1)=0\}$. Довести, що $C[0,1]/I\simeq\mathbb{R}\times\mathbb{R}$.

Визначимо відображення $C[0,1]\to\mathbb{R}\times\mathbb{R}$ для довільної функції $f\in C[0,1]$ поклавши $\varphi(f)=(f(0),f(1))$. Згідно основної теореми про

гомоморфізм кілець досить перевірити, що φ — гомоморфізм і $Ker\varphi = I$,$Im\varphi = \mathbb{R} \times \mathbb{R}$.

Спочатку пересвідчимось, що φ зберігає додавання і множення:

$$\varphi(f+g) = ((f+g)(0),(f+g)(1)) = (f(0)+g(0), f(1)+g(1)) = \\ (f(0),f(1)) + (g(0),g(1)) = \varphi(f) + \varphi(g);$$

$$\varphi(fg) = ((fg)(0),(fg)(1)) = (f(0)g(0), f(1)g(1)) = \\ (f(0),f(1))(g(0),g(1)) = \varphi(f)\varphi(g).$$

Тепер покажемо, що $Ker\varphi = I$:

$$f \in Ker\varphi \Leftrightarrow \varphi(f) = (0,0) \Leftrightarrow (f(0),f(1)) = (0,0) \Leftrightarrow \\ f(0) = f(1) = 0 \Leftrightarrow f \in I.$$

Лишилось показати, що $Im\varphi = \mathbb{R}\times\mathbb{R}$. Для цього зауважимо, що для будь-якої пари $(a,b) \in \mathbb{R} \times \mathbb{R}$ $(a,b) = \varphi(a + (b-a)x)$.

Задачі

4.1 Навести приклад таких кілець з одиницями R і S, а також гомоморфізму $\varphi : R \to S$, що образ одиниці кільця R не є одиницею кільця S.

4.2 Знайти всі гомоморфізми кілець:
а) $\mathbb{Z} \to 2\mathbb{Z}$; б) $2\mathbb{Z} \to 2\mathbb{Z}$; в) $2\mathbb{Z} \to 3\mathbb{Z}$; г) $\mathbb{Z} \to M_2(\mathbb{Z}_2)$.

4.3 Для заданого кільця K і його ідеала I описати елементи факторкільця K/I, побудуйте таблички додавання і множення у факторкільці, з'ясуйте, чи є ідеал I простим у кожному з наступних випадків:

а) $K = \mathbb{Z}_{12}, I = (4)$;

б) $K = \mathbb{Z}_{20}, I = (5)$;

в) $K = \mathbb{Z}_6 \times \mathbb{Z}_4, I = ((4,2))$;

г) $K = \mathbb{Z}[i\sqrt{3}], I = (1 + i\sqrt{3})$.

4.4 Знайти кількість елементів факторкільця K/I, якщо

а) $K = \mathbb{Z}_5[x], I = (x^2)$;

б) $K = \mathbb{Z}_m[x], I = (x^k)$;

в) $K = \mathbb{Z}_6[x, y], I = (x^5, y^7)$;

г) $K = \mathbb{Z}_m[x, y], I = (x^k, y^l)$;

д) $K = \mathbb{Z}_m[x, y], I = (x^k, xy, y^l)$;

е) $K = \mathbb{Z}_8[x, y], I = (6, x^5, y^7)$;

ж) $K = \mathbb{Z}_{16} \times \mathbb{Z}_{15}, I = ((2, 5))$;

з) $K = \mathbb{Z}_{18} \times \mathbb{Z}_{30}, I = ((8, 25))$;

к) $K = \mathbb{Z}_m \times \mathbb{Z}_n, I = ((k, l))$;

4.5 Нехай $f_1(x) = x^2 + 1$, $f_2(x) = x^2$, $f_3(x) = x^2 + 2$, $f_4(x) = x^2 + x + 1$, $f_5(x) = x^2 + x$, $f_6(x) = x^2 + 2x + 1$, $f_7(x) = x^2 + 2x$, $f_8(x) = x^2 + x + 2$, $f_9(x) = x^2 + 2x + 2 \in \mathbb{Z}_3[x]$ (це повний список унітарних многочленів степеня 2 над $\mathbb{Z}_3$). Для кожного i, $1 \leq i \leq 9$, через K_i позначимо факторкільце $\mathbb{Z}_3[x]/(f_i)$. Для кожного i $(1 \leq i \leq 9)$ описати елементи факторкільця K_i, виписати таблички додавання та множення в K_i; розбити множину $\{K_i,\ 1 \leq i \leq 9\}$ на класи попарно ізоморфних кілець. З'ясувати, які з $\{K_i\}$ є полями.

4.6 Довести, що $\mathbb{R}[x]/(x^2 - 5x + 4) \simeq \mathbb{R}^2$.

4.7 Довести, що а) $\mathbb{R}[x]/(x^2 + x + 1) \simeq \mathbb{C}$;

б) $\mathbb{R}[x]/(f(x)) \simeq \mathbb{C}$, де $f(x)$ — незвідний над $\mathbb{R}$ многочлен степеня 2.

4.8 Нехай $K = \mathbb{R}[x], I = (x^3)$. Довести, що елемент $a + bx + cx^2 + (x^3) \in K/I$ є оборотним тоді й тільки тоді, коли $a \neq 0$.

4.9 З'ясувати, чи буде полем факторкільце $\mathbb{Z}_5[x]/(f(x))$ у кожному з наступних випадків:

а) $f(x) = x^2 + 1$;

б) $f(x) = x^2 + 4x + 1$;

в) $f(x) = x^3 + x + 1$;

г) $f(x) = x^3 + 4x + 4$.

4.10 Розбити наступну множину кілець на класи попарно ізоморфних: $K_1 = \mathbb{C}[x,y]/(x-y,\ xy-1)$, $K_2 = \mathbb{C}[x]/((x-1)^2)$, $K_3 = \mathbb{C}[x,y]$, $K_4 = \mathbb{C}[x]/(x^2)$.

4.11 Чи ізоморфні факторкільця $\mathbb{R}[x]/(x^2+x+1)$ і $\mathbb{R}[x]/(2x^2-3x+3)$

4.12 Довести, що для будь-якого цілого $n > 1$ факторкільце $\mathbb{Z}[x]/(n)$ ізоморфне кільцю $\mathbb{Z}_n[x]$.

4.13 Визначити, якому з кілець $\mathbb{Z}_m$ ізоморфне кожне з наступних факторкілець K/I:

а) $K = \mathbb{Z}[i], I = (3+i)$;

б) $K = \mathbb{Z}[i], I = (3-2i)$;

в) $K = \mathbb{Z}[i\sqrt{3}], I = (1+3i\sqrt{3})$;

г) $K = \mathbb{Z}[\sqrt{5}], I = (7-3\sqrt{5})$;

4.14 Довести, що

а) $\mathbb{Z}_7[x]/(x^2+5) \simeq \mathbb{Z}_7 \times \mathbb{Z}_7$;

б) $\mathbb{Z}_5[x]/(x^2+1) \simeq \mathbb{Z}_5 \times \mathbb{Z}_5$.

4.15 У кожному з наступних випадків Довести, що $\mathbb{R}[x,y]/I \simeq \mathbb{R}[x]$:

а) $I = (y)$;

б) $I = (x^2-y)$;

в) $I = (x)$;

г) $I = (x-y^2)$.

4.16 Нехай F — поле і $n \in \mathbb{N}$. Через I позначимо головний ідеал, породжений x^n, кільця $F[x]$, а через J - головний ідеал, породжений x^n, кільця $F[[x]]$. Довести, що $F[x]/I \simeq F[[x]]/J$.

4.17 Довести, що

а) $\mathbb{Z}[\frac{1}{7}]/(10) \simeq \mathbb{Z}_{10}$;

б) $\mathbb{Z}[\frac{1}{10}]/(7) \simeq \mathbb{Z}_7$.

в) Чи правда, що $\mathbb{Z}[\frac{1}{6}]/(3) \simeq \mathbb{Z}_3$?

4.18 Нехай $I = \{f \in C[0,5] :\ f(x) = 0, 4 \le x \le 5\}$. Довести, що $C[0,5]/I \simeq C[4,5]$.

4.19 Нехай $I = \{f \in C[0,1] :\ f(1) = 0\}$. Довести, що $C[0,1]/I \simeq \mathbb{R}$.

5 Подільність, розкладні і нерозкладні елементи

Нехай R — це деяка область цілісності.

Означення 9. Кажуть, що елемент $b \in R$ ділиться на елемент $a \in R$ (відповідно, елемент a є дільником елемента b), якщо існує такий елемент $c \in R$ що $b = ac$.

Записують це так: $a|b$. Основні властивості відношення подільності в області цілісності R такі:

Твердження 9. 1) Якщо $a|b$ і $b|c$, то $a|c$;
2) Якщо $a|b$ і $a|c$, то $a|(b + c)$;
3) Якщо $a|b$, то $a|bc$ для довільного $c \in R$.

Елементи $a, b \in R$ називаються асоційованими, якщо $a|b$ і $b|a$. Відношення асоційованості є відношенням еквівалентності на множині ненульових елементів R.

Твердження 10. Елементи a, b області цілісності R є асоційованими тоді й лише тоді, коли знайдеться такий оборотний елемент $c \in R$ що $a = bc$.

Зокрема, в кільці цілих чисел $\mathbb{Z}$ асоційованими є ті і лише ті числа, які відрізняються лише знаком, а в кільці $F[x]$ многочленів над полем F — ті та тільки ті многочлени, які відрізняються на ненульовий множник з F. Тобто кожен ненульовий многочлен цього кільця є асоційованим з єдиним унітарним многочленом.

Означення 10. Необоротний елемент $a \neq 0$ області цілісності R називається розкладним, якщо існують такі необоротні елементи $b, c \in R$, що $a = bc$. Якщо ж такого розкладу не існує, то елемент a називається нерозкладним (або простим).

Нерозкладні елементи кільця $\mathbb{Z}$ називаються простими числами, а нерозкладні елементи кільця $F[x]$ — незвідними над F многочленами.

Таким чином, кожен ненульовий елемент області цілісності є елементом одного з трьох типів: оборотним, розкладним або нерозкладним.

Приклади розв'язування задач

Приклад 37. Довести, що у кільці $\mathbb{Z}[\sqrt{2}]$ елемент $5 + 2\sqrt{2}$ є дільником елемента $6 - \sqrt{2}$.

Перший спосіб. За означенням, $5+2\sqrt{2}$ ділить $6-\sqrt{2}$, якщо знайдеться такий елемент $x+y\sqrt{2}\in\mathbb{Z}[\sqrt{2}]$, що $(5+2\sqrt{2})(x+y\sqrt{2})=6-\sqrt{2}$. Розкривши дужки, отримаємо: $5x+4y+(2x+5y)\sqrt{2}=6-\sqrt{2}$, звідки $5x-4y=6$ і $2x+5y=-1$. Отримана система рівнянь має розв'язок в цілих числах $x=2$, $y=-1$. Тому $(5+2\sqrt{2})(2-\sqrt{2})=6-\sqrt{2}$. Таким чином, $5+2\sqrt{2}$ є дільником елемента $6-\sqrt{2}$ у кільці $\mathbb{Z}[\sqrt{2}]$.

Другий спосіб. Кільце $\mathbb{Z}[\sqrt{2}]$ є підкільцем поля $\mathbb{R}$. Оскільки у полі всякий ненульовий елемент ділить всякий інший елемент, то знайдеться (єдине) дійсне число z, таке, що $(5+2\sqrt{2})z=6-\sqrt{2}$. Звідси знайдемо z:

$$z=\frac{6-\sqrt{2}}{5+2\sqrt{2}}=\frac{(6-\sqrt{2})(5-2\sqrt{2})}{25-8}=2-\sqrt{2}\in\mathbb{Z}[\sqrt{2}]$$

(для спрощення виразу для z ми домножили чисельник і знаменник дробу $\frac{6-\sqrt{2}}{5+2\sqrt{2}}$ на $5-2\sqrt{2}$, маючи на меті позбутися від ірраціональності у знаменнику). Отже, в $\mathbb{Z}[\sqrt{2}]$ виконується рівність $(5+2\sqrt{2})(2-\sqrt{2})=6-\sqrt{2}$, і $5+2\sqrt{2}$ є дільником $6-\sqrt{2}$.

Приклад 38. В кільці $\mathbb{Z}[i]$ знайти всі елементи, асоційовані з елементом $3+5i$.

Елемент $a+bi\in\mathbb{Z}[i]$ буде асоційованим з $3+5i$ тоді й лише тоді, коли $a+bi=(3+5i)u$, де u — дільник одиниці. Із приклада 18 нам відомий список дільників одиниці: це $1,-1,i,-i$. Таким чином, асоційованими з $3+5i$ є такі елементи: $3+5i,-3-5i,3i-5,-3i+5$.

Приклад 39. У кільці $\mathbb{Z}_5[x]$ знайдіть всі елементи, асоційовані з $f(x)=x^3+4x^2+3x+2$.

За означенням, многочлен $g(x)\in\mathbb{Z}_5[x]$ буде асоційованим з $f(x)$ тоді й лише тоді, коли $f(x)|g(x)$ і $g(x)|f(x)$. Оскільки $f(x)|g(x)$, і $deg(f(x))=3$, то $deg(g(x))\leq 3$. Але ж і $g(x)|f(x)$. Тому $deg(g(x))=3$. Часткою двох многочленів третього степеня є многочлен нульового степеня, тобто ненульовий елемент поля $\mathbb{Z}_5$. Отже, є 4 можливості:

1. $g(x)=f(x)=x^3+4x^2+3x+2$.
2. $g(x)=2f(x)=2x^3+3x^2+x+4$.
3. $g(x)=3f(x)=3x^3+2x^2+4x+1$.
4. $g(x)=4f(x)=4x^3+x^2+2x+3$.

Зауваження. Можна було міркувати інакше: так, як у попередньому прикладі, зауваживши, що оборотними елементами кільця $\mathbb{Z}_5[x]$ є многочлени нульового степеня і лише вони.

Приклад 40. Довести, що елемент 10 кільця $\mathbb{Z}[\frac{1}{6}]$ є нерозкладним елементом.

Припустимо, що $10 = xy$, x, y — необоротні елементи кільця $\mathbb{Z}[\frac{1}{6}]$. Звідси і з того, що $x = \frac{a}{6^k}$, $y = \frac{b}{6^l}$ для деяких $a, b \in \mathbb{Z}$, $k, l \in \mathbb{N}$, випливає, що $10 \cdot 6^{k+l} = ab$. Із цієї рівності випливає, що ab ділиться на 5, тому a ділиться на 5 або b ділиться на 5. Нехай, скажімо, a ділиться на 5, тобто $a = 5a_1$, $a_1 \in \mathbb{Z}$. Тоді $2 \cdot 6^{k+l} = a_1 b$, звідки a_1 і b є оборотними елементами в $\mathbb{Z}[\frac{1}{6}]$ (дійсно, a_1, b — цілі числа, простими дільниками яких можуть бути лише 2 і 3, звідки $\frac{1}{a_1}, \frac{1}{b} \in \mathbb{Z}[\frac{1}{6}]$). Тому елемент $y = \frac{b}{6^l}$ — теж оборотний елемент кільця $\mathbb{Z}[\frac{1}{6}]$, що суперечить початковому припущенню. Аналогічно, розглядаючи випадок, коли b ділиться на 5, отримаємо, що x — оборотний елемент, що також суперечить початковому припущенню. Таким чином, встановлено, що 10 є нерозкладним елементом кільця $\mathbb{Z}[\frac{1}{6}]$.

Приклад 41. Нехай B — кільце функцій із задачі 1.4. Довести, що функція $id(x) = x \in B$ не має розкладу на добуток нерозкладних множників у кільці B.

Спочатку зробимо таке зауваження: якщо $f(x) = a_1 x^{b_1} + \cdots + a_n x^{b_n}$, $g(x) = c_1 x^{d_1} + \cdots + c_m x^{d_m}$ і $n > 1$ або $m > 1$, то добуток $f(x)g(x)$ є сумою принаймі двох доданків: $a_1 c_1 x^{b_1+d_1}$ і $a_n c_m x^{b_n+d_m}$. Очевидно, аналогічне зауваження справедливе для добутку будь-якої іншої кількості функцій. Тому всякий розклад функції $id(x)$ на множники у кільці B має вигляд $id(x) = x = t_1 x^{\omega_1} \cdot \cdots \cdot t_r x^{\omega_r}$. Звідси $t_1 \cdot \cdots \cdot t_r = 1$ і $\omega_1 + \cdots + \omega_r = 1$. Розглянемо довільний співмножник $t_k x^{\omega_k}$ у нашому розкладі ($k \in \{1, \ldots, r\}$). Якщо $\omega_k = 0$, то $t_k x^{\omega_k}$ — оборотний в B елемент. Якщо ж $\omega_k > 0$, то з рівності $t_k x^{\omega_k} = t_k x^{\frac{\omega_k}{2}} \cdot x^{\frac{\omega_k}{2}}$ випливає, що $t_k x^{\omega_k}$ — розкладний елемент. Отже, розкладу функції $id(x)$ на нерозкладні множники кільця B не існує.

Задачі

5.1 Перевірити, чи є елемент $1+i \in \mathbb{Z}[i]$ дільником кожного з наступних елементів:

а) 2;

б) $5 + 2i$;

в) $7 - i$;

г) $1 + 6i$.

5.2 У кільці $\mathbb{Z}[i\sqrt{7}]$ знайти всі елементи, асоційовані із данним елементом:

а) 6;

б) $1 - i\sqrt{7}$.

5.3 Знайти унітарний многочлен, асоційований із заданим многочленом кільця $\mathbb{Z}_7[x]$:

а) $4x^2 + 6x + 5$;

б) $2x^5 + 4x + 2$;

в) $5x^4 + 2x^2 + 3x + 1$.

5.4 У кільці $\mathbb{Z}[i\sqrt{5}]$ знайти всі дільники елемента $13 + 2i\sqrt{5}$.

5.5 У кільці $\mathbb{Z}[i\sqrt{3}]$ знайти всі дільники данного елемента:

а) $5 + i\sqrt{3}$;

б) $4 - 5i\sqrt{3}$;

в) 3.

5.6 Нехай K — область цілісності і $a, b \in K$. Довести, що

а) a ділить b тоді й лише тоді, коли $aK \subseteq bK$;

б) a і b асоційовані тоді й лише тоді, коли $aK = bK$.

5.7 Довести, що асоційовані елементи є одночасно або оборотними, або розкладними, або нерозкладними.

5.8 Довести, що якщо a — нерозкладний елемент кільця A, всі ідеали якого є головними, то ідеал (a) кільця A — максимальний.

5.9 Визначити, елементом якого типу (оборотним, розкладним, нерозкладним) є кожен з наступних елементів кільця $\mathbb{Z}[\frac{1}{2}]$:

а) 4; б) 9; в) $\frac{15}{8}$;

г) $\frac{3}{4}$; д) $\frac{14}{32}$ е)44.

5.10 Визначити, елементом якого типу (оборотним, розкладним, нерозкладним) є кожен з наступних елементів кільця $\mathbb{Z}[\frac{1}{10}]$:

а) 20; б) 18; в) $\frac{77}{5}$;

г) $\frac{3}{8}$; д) $\frac{1}{25}$ е)$\frac{13}{80}$.

5.11 Визначити, чи буде данне число розкладним елементом кільця $\mathbb{Z}[i\sqrt{5}]$:

а) 10; б)$7 + i\sqrt{5}$;

в) $2 + 3i\sqrt{5}$; г) $5 + 4i\sqrt{5}$.

5.12 Визначити, чи даний многочлен розкладний у кільці $\mathbb{R}[x, y]$:

а) $x^5 + xy^4 + x^4y + y^5$;

б) $x + y^2$;

в) $x^4 + y^4$;

г) $x^8 - y^6$.

5.13 Нехай F — поле. Довести, що якщо многочлени $f, g \in F[x_1, \ldots, x_n]$ не мають спільного дільника степеня ≥ 1, то многочлен

$$x_{n+1}f + g \in F[x_1, \ldots, x_{n+1}]$$

не є розкладним елементом кільця $F[x_1, \ldots, x_{n+1}]$.

5.14 Нехай A, B — області цілісності, причому A є підкільцем B і $a \in A$. Довести або спростувати наступні твердження:

а) якщо a розкладний в A, то він розкладний і в B;

б) якщо a розкладний в B, то він розкладний і в A;

в) якщо a нерозкладний в A, то він нерозкладний і в B;

г) якщо a нерозкладний в B, то він нерозкладний і в A.

6 Факторіальні кільця

Нехай R — це деяка область цілісності.

Означення 11. Кажуть, що необоротний елемент $a \neq 0$ області цілісності R однозначно розкладається на нерозкладні множники, якщо
1) його можна подати як добуток нерозкладних елементів;
2) з рівностей

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

де $p_1, p_2, \dots, p_n, q_1, q_2, \dots, q_m$ — нерозкладні елементи, маємо, що $n = m$ і після перестановки множників елементи p_1 і q_1, p_2 і $q_2, \dots$, p_n і q_n є асоційованими.

Зауважимо, що кожен нерозкладний елемент також має однозначний розклад на нерозкладні множники і в його розкладі є лише один множник.

Означення 12. Область цілісності називається факторіальним кільцем (або кільцем з однозначним розкладом), якщо у ньому кожен ненульовий необоротний елемент має однозначний розклад на нерозкладні множники.

Факторіальними є зокрема кільце цілих чисел $\mathbb{Z}$ і кільце многочленів $F[x_1, \dots, x_n]$ від n змінних над полем F.

Теорема 2. Область цілісності R є факторіальним кільцем тоді й лише тоді, коли для довільного нерозкладного елемента $a \in R$ такого, що $a|bc$, маємо $a|b$ або $a|c$.

Найбільшим спільним дільником елементів $a, b \in R$ (скорочено будемо писати НСД(a, b)) назвемо такий елемент $d \in R$, що
1) $d|a$ і $d|b$;
2) для кожного $c \in R$ такого, що $c|a$ і $c|b$, маємо $c|d$.

Найменшим спільним кратним елементів $a, b \in R$ (скорочено пишемо НСК(a, b)) назвемо такий елемент $D \in R$, що
1) $a|D$ і $b|D$;
2) для кожного $C \in R$ такого, що $a|C$ і $b|C$, маємо $D|C$.

Цілком аналогічно визначаються найбільший спільний дільник і найменше спільне кратне довільної сукупності елементів з R.

Не для кожних двох елементів $a, b \in R$ існують найбільший спільний дільник і найменше спільне кратне. При цьому має місце

Твердження 11. Два найбільші спільні дільники елементів $a, b \in R$ є асоційованими і елемент, асоційований з НСД(a, b), сам є НСД(a, b).

Тобто якщо найбільший спільний дільник елементів $a, b \in R$ існує, то він визначений однозначно з точністю до асоційованості. Аналогічне твердження має місце і для найменшого спільного кратного.

Елементи $a, b \in R$ називаються взаємно простими, якщо НСД$(a, b) = 1$.

Твердження 12. У факторіальному кільці будь-які два ненульові елементи мають найбільший спільний дільник і найменше спільне кратне.

Приклади розв'язування задач

Приклад 42. Визначити, чи елемент 10 кільця $\mathbb{Z}[i\sqrt{6}]$ має однозначний розклад на нерозкладні множники.

Нехай $a+bi\sqrt{6}$ — дільник 10 в $\mathbb{Z}[i\sqrt{6}]$. Тоді знайдеться такий елемент $c + di\sqrt{6} \in \mathbb{Z}[i\sqrt{6}]$, що $10 = (a + bi\sqrt{6})(c + di\sqrt{6})$. Обчислимо і прирівняємо норми елементів із останньої рівності: $100 = (a^2 + 6b^2)(c^2 + 6d^2)$. Звідси $a^2 + 6b^2 \in \mathbb{N}$ $(a, b \in \mathbb{Z})$— дільник числа 100, тобто одне з чисел $1, 2, 4, 5, 10, 20, 25, 50, 100$. Розглянемо випадки:

1. $a^2 + 6b^2 = 1$. Тоді $b = 0$, a дорівнює 1 або -1, відповідно $a + bi$ дорівнює 1 або -1.

2. $a^2 + 6b^2 = 2$. Це рівняння не має розв'язків в цілих числах.

3. $a^2 + 6b^2 = 4$. Тоді $b = 0$, a дорівнює 2 або -2, відповідно $a + bi$ дорівнює 2 або -2.

4. $a^2 + 6b^2 = 5$. Це рівняння не має розв'язків у цілих числах.

5. $a^2 + 6b^2 = 10$. Маємо 4 розв'язки: $a = 2$ і $b = 1$, $a = 2$ і $b = -1$, $a = -2$ і $b = 1$, $a = -2$ і $b = -1$. Відповідно для $a + bi$ маємо 4 варіанти: $2 + i$, $2 - i$, $-2 + i$, $-2 - i$.

6. $a^2 + 6b^2 = 20$. Тоді $c^2 + 5d^2 = 5$. Немає цілочисельних розв'язків.

7. $a^2 + 6b^2 = 25$. Тоді $b = 0$, a дорівнює 5 або -5, відповідно $a + bi$ дорівнює 5 або -5.

8. $a^2 + 6b^2 = 50$. Тоді $c^2 + 6d^2 = 2$. Немає цілочисельних розв'язків.

9. $a^2 + 6b^2 = 100$. Тоді $b = 0$, a дорівнює 10 або -10, відповідно $a + bi$ дорівнює 10 або -10.

Таким чином, ми знайшли всі дільники числа $10 \in \mathbb{Z}[i\sqrt{6}]$, і бачимо, що, наприклад,

$$10 = 2 \cdot 5 = (2 + i\sqrt{6})(2 - i\sqrt{6})$$

(звичайно, вказані два розклади досить легко можна було вгадати спочатку, не прибігаючи до пошуку всіх дільників числа 10.)

Тепер пересвідчимось, що $2, 5, 2+i\sqrt{6}, 2-i\sqrt{6}$ — нерозкладні елементи кільця $\mathbb{Z}[i\sqrt{6}]$. Якщо $a+bi$ ділить $2+i\sqrt{6}$, то $a+bi$ також ділить і 10. Всі дільники десятки ми вже знайшли, для кожного з них неважко перевірити, чи ділить він $2+i\sqrt{6}$, в результаті отримуємо список дільників $2+i\sqrt{6}$: 1, -1, $-2-i\sqrt{6}$ і сам $2+i\sqrt{6}$. Ці дільники — невласні, отже, $2+i\sqrt{6} \in \mathbb{Z}[i\sqrt{6}]$ — нерозкладний елемент. Нерозкладність елементів $2, 5, 2-i\sqrt{6}$ встановлюється аналогічно. Таким чином, вказані два розклади числа 10 є розкладами на нерозкладні множники.

Крім цього, очевидно, що число 2 не асоційоване ні з $2+i\sqrt{6}$, ані з $2-i\sqrt{6}$ (2 асоційоване лише з -2, внаслідок задачі 2.3). Отже, доведено, що в кільці $\mathbb{Z}[i\sqrt{6}]$ елемент 10 не має однозначного розкладу на нерозкладні множники.

Приклад 43. Користуючись факторіальністю кільця $\mathbb{Z}[i]$, знайти кількість дільників елемента $z = 210 - 30i$ цього кільця.

Подамо число z у вигляді $z = u \cdot a_1^{k_1} \cdot \dots \cdot a_m^{k_m}$, де u — оборотний елемент, $m \in \mathbb{N}$, $a_1, \dots, a_m$ — попарно неасоційовані нерозкладні елементи кільця $\mathbb{Z}[i]$. Оскільки $\mathbb{Z}[i]$ — факторіальне кільце, то кожен дільник z однозначно подається у вигляді $v \cdot a_1^{l_1} \cdot \dots \cdot a_m^{l_m}$, де v — оборотний елемент і $0 \le l_i \le k_i$ для $i = 1, \dots, m$. Звідси випливає, що кількість дільників z дорівнює $4(k_1+1)\dots(k_m+1)$ (4 способи вибрати v, k_i+1 спосіб вибрати l_i для $i = 1, \dots, m$).

Для нашого числа z маємо:

$$z = 2\cdot 3\cdot 5\cdot (7-i) = (1+i)\cdot(1-i)\cdot 3\cdot(2+i)\cdot(2-i)\cdot(1-i)\cdot(2-i)\cdot(1+2i) = 3\cdot(1+i)\cdot(1-i)^2\cdot(2+i)\cdot(2-i)^2\cdot(1+2i).$$

Співмножники 3, $1+i$, $1-i$, $2+i$, $2-i$, $1+2i$ — нерозкладні, однак $1+i = i(1-i)$, $1+2i = i(2-i)$. Враховуючи ці рівності, отримаємо розклад $z = -3(1-i)^3(2+i)(2-i)^3$, в якому множники 3, $1-i$, $2+i$, $2-i$ нерозкладні і попарно неасоційовані. Отже, кількість дільників z дорівнює $4 \cdot 2 \cdot 4 \cdot 2 \cdot 4 = 256$.

Приклад 44. Визначити, чи існує в кільці $\mathbb{Z}[i\sqrt{6}]$ НСД елементів $2 + 16i\sqrt{6}$ і $8 + i\sqrt{6}$. Якщо так, знайди НСД вказаних чисел.

Спочатку знайдемо всі дільники одного із заданих чисел (метод знаходження всіх дільників елемента із $\mathbb{Z}[i\sqrt{6}]$ вказаний в прикладі 42).

Після цього перевіряємо, які із отриманих дільників першого числа ділять також і друге. В результаті отримаємо повний список спільних дільників двох заданих чисел.

Для наших числових даних знаходимо, що дільниками числа $8+i\sqrt{6}$ в $\mathbb{Z}[i\sqrt{6}]$ є числа 1, -1, $8+i\sqrt{6}$, $-8-i\sqrt{6}$, $1+i\sqrt{6}$, $-1-i\sqrt{6}$, $2-i\sqrt{6}$, $-2+i\sqrt{6}$.

Очевидно, що 1 і -1 ділять $2+16i\sqrt{6}$. Далі,

$$\frac{2+16i\sqrt{6}}{8+i\sqrt{6}} = \left(\frac{8}{5}+\frac{9}{5}i\sqrt{6}\right) \notin \mathbb{Z}[i\sqrt{6}];$$

$$\frac{2+16i\sqrt{6}}{1+i\sqrt{6}} = \left(14+2i\sqrt{6}\right) \in \mathbb{Z}[i\sqrt{6}];$$

$$\frac{2+16i\sqrt{6}}{2-i\sqrt{6}} = \left(\frac{46}{3}+\frac{17}{5}i\sqrt{6}\right) \notin \mathbb{Z}[i\sqrt{6}].$$

Таким чином, маємо список спільних дільників наших чисел: 1, -1, $1+i\sqrt{6}$, $1-i\sqrt{6}$. Оскільки кожен із цих чотирьох дільників ділить $1+i\sqrt{6}$, то НСД даних чисел існує і (з точністю до асоційованості) дорівнює $1+i\sqrt{6}$.

Приклад 45. Визначити, чи існує в кільці $\mathbb{Z}[i\sqrt{3}]$ НСД елементів 4 і $2-2i\sqrt{3}$.

Міркуючи, як і в попередньому прикладі, знаходимо всі спільні дільники даних чисел. Це числа 1, -1, 2, -2, $1+i\sqrt{3}$, $-1-i\sqrt{3}$, $1-i\sqrt{3}$, $-1+i\sqrt{3}$.

Жодне з чисел 1, -1, $1+i\sqrt{3}$, $-1-i\sqrt{3}$, $1-i\sqrt{3}$, $-1+i\sqrt{3}$ не є НСД даних чисел, бо вони не діляться на 2. Крім цього 2 і -2 також не будуть НСД даних чисел, оскільки 2 і -2 не діляться на $1+i\sqrt{3}$.

Отже, в кільці $\mathbb{Z}[i\sqrt{3}]$ не існує НСД елементів 4 і $2-2i\sqrt{3}$.

Приклад 46. Нехай a, b — ненульові елементи кільця K. Довести, що якщо існує НСК(a,b), то існує НСД(a,b), і НСК$(a,b)\cdot$НСД$(a,b) \sim a\cdot b$.

Покладемо $w =$НСК(a,b), $d = \frac{ab}{w}$. Нам треба показати, що НСД$(a,b) = d$ (відзначимо, що $d \in K$, оскільки із $a|ab$, $b|ab$ випливає $w|ab$). Оскільки $a = d\frac{w}{b}$, $b = d\frac{w}{a}$ (звичайно, $\frac{w}{d}$, $\frac{w}{a} \in K$), то $d|a, d|b$. Тепер візьмемо довільний елемент $d' \in K$, такий, що $d'|a$ і $d'|b$.. Ми маємо пересвідчитись, що $d'|d$. В силу вибору елемента d' для деяких $a', b' \in K$ виконуються рівності $a = a'd'$, $b = b'd'$. Зрозуміло, що $a|a'b'd'$ і $b|a'b'd'$.

Звідси, враховуючи, що $w = \text{НСК}(a,b)$, випливає, що $w|a'b'd'$. Остання подільність рівносильна такій: $\frac{ab}{d}|a'b'd'$, звідки $ab|a'b'd'd$, що еквівалентно $a'd'b'd'|a'b'd'd$. Отже, $d'|d$, що і треба було довести.

Приклад 47. Нехай a, b — ненульові елементи кільця K і існує $\text{НСД}(a,b)$. Чи випливає звідси, що існує $\text{НСК}(a,b)$?

Розглянемо елементи $a = 2$ і $b = 1 + i\sqrt{3}$ кільця $\mathbb{Z}[i\sqrt{3}]$. Легко перевіряється, що $\text{НСД}(a,b) = 1$. Припустимо, що існує $\text{НСК}(a,b)$. Тоді, використовуючи результат попереднього прикладу, бачимо, що повинна виконуватись рівність $\text{НСК}(a,b)\cdot\text{НСД}(a,b) \sim a \cdot b$. Для наших чисел ця рівність перепишеться так: $\text{НСК}(a,b) = 2(1 + i\sqrt{3})$. Тоді $2(1 + i\sqrt{3})$ мусить ділити будь-яке спільне кратне наших чисел. Але це не так: 4 — спільне кратне a і b, але $2(1 + i\sqrt{3})$ не ділить 4. Отримана суперечність означає, що $\text{НСК}(a,b)$ не існує.

Задачі

6.1 Визначити, чи має даний елемент кільця $\mathbb{Z}[i\sqrt{3}]$ однозначний розклад на нерозкладні множники:

а) 4; б) $8 + 3i\sqrt{3}$;

в) $5 + i\sqrt{3}$; г)$2 - 2i\sqrt{3}$.

6.2 Визначити, чи має даний елемент кільця $\mathbb{Z}[i\sqrt{5}]$ однозначний розклад на нерозкладні множники:

а) 9; б) $1 + 4i\sqrt{5}$;

в) $5 - 2i\sqrt{5}$; г) $3 - 3i\sqrt{5}$.

6.3 Нехай K — поле. Довести, що підкільце $K[x^2, x^3]$ кільця $K[x]$ є факторіальним кільцем.

6.4 Обчислити кількість дільників кожного з наступних елементів кільця $\mathbb{Z}[i]$:

а) 32; б) $40 + 40i$; в) $60 + 30i$;

г) $52 + 156i$; д) 60; е) $600 - 200i$.

6.5 Довести, що якщо $d_1 = \text{НСД}(a,b,c)$, $d_2 = \text{НСД}(a,b)$, то $d_1 = \text{НСД}(d_2,c)$.

6.6 Довести, що якщо $d_1 = \text{НСД}(a,b,c,d)$, $d_2 = \text{НСД}(a,b)$, $d_3 = \text{НСД}(c,d)$, то $d_1 = \text{НСД}(d_2,d_3)$.

6.7 Довести, що якщо $D_1 = \text{НСК}(a,b,c,d)$, $D_2 = \text{НСК}(a,b)$, $D_3 = \text{НСК}(c,d)$, то $D_1 = \text{НСК}(D_2, D_3)$.

6.8 Довести, що якщо $d_1 = \text{НСД}(a,b)$, $d_2 = \text{НСД}(a, a+b)$, то d_1 і d_2 асоційовані.

6.9 Довести, що якщо $d = \text{НСД}(a,b)$ і $a = da'$, $b = db'$, то елементи a' і b' взаємно прості.

6.10 Визначити, чи існує в кільці $\mathbb{Z}[i\sqrt{3}]$ НСД наступних пар елементів. Якщо так, знайдіть НСД:

а) $14, 1 + 4i\sqrt{3}$;

б) $7 + i\sqrt{3}$, $9 + 5i\sqrt{3}$;

в) $2 - 2i\sqrt{3}$, $2 + 2i\sqrt{3}$;

г) $3 + 2i\sqrt{3}$, $5 + i\sqrt{3}$.

6.11 Визначити, чи існує в кільці $\mathbb{Z}[i\sqrt{5}]$ НСД наступних пар елементів. Якщо так, знайдіть НСД:

а) $9, 4 + 2i\sqrt{5}$;

б) $4 + 6i\sqrt{5}$, $5 - 3i\sqrt{5}$;

в) $7 - i\sqrt{5}$, $16 + i\sqrt{5}$;

г) 6, $3 + 3i\sqrt{5}$.

6.12 Визначити, чи для даних $a, b, c \in \mathbb{Z}[i\sqrt{5}]$ виконується рівність

$$\text{НСД}(ca, cb) = c \cdot \text{НСД}(a,b) :$$

а) $a = 3, b = 2i\sqrt{5}, c = 3$;

б) $a = 2, b = 1 + i\sqrt{5}, c = 1 - i\sqrt{5}$.

6.13 Нехай $a, b, c,$ — ненульові елементи кільця K. Довести, що з існування $\text{НСК}(a,b)$ випливає існування $\text{НСК}(ca, cb)$ і виконується рівність $\text{НСК}(ca, cb) = c \cdot \text{НСК}(a,b)$.

6.14 Нехай $\varphi : K_1 \to K_2$ — ізоморфізм областей цілісності і нехай $a, b, d \in K_1$. Довести, що із $d = \text{НСД}(a,b)$ випливає, що $\varphi(d) = \text{НСД}(\varphi(a), \varphi(b))$.

7 Евклідові кільця

Нехай R — це деяка область цілісності.

Означення 13. Кільце R називається евклідовим, якщо існує функція

$$N : R \setminus \{0\} \to \mathbb{N} \cup \{0\}$$

така, що виконуються умови:
1) для довільних $a, b \in R$ маємо $N(ab) \geq N(a)$;
2) для довільних $a, b \in R$, $b \neq 0$ існують елементи $q, r \in R$, для яких

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

При цьому про умову 2) кажуть як про умову, що дає можливість ділення з остачею на ненульові елементи кільця. Елементи q і r останньої рівності називаються відповідно неповною часткою і остачею від ділення a на b.

Функцію N з означення евклідового кільця називають евклідовою нормою на R.

Найвідомішими прикладами евклідових кілець є:

1. кільце цілих чисел $\mathbb{Z}$ з евклідовою нормою $N(a) = |a|$, $a \in \mathbb{Z}, a \neq 0$;
2. кільце многочленів $F[x]$ над полем F з евклідовою нормою $N(f(x)) = \deg f(x)$, $f(x) \in \mathbb{Z}, f(x) \not\equiv 0$;
3. кільце цілих гаусових чисел $\mathbb{Z}[i]$ з евклідовою нормою $N(a + bi) = a^2 + b^2$, $a + bi \in \mathbb{Z}[i], a + bi \neq 0$.

Кожне евклідове кільце є факторіальним, а тому для довільних ненульових елементів евклідового кільця існує їх найбільший спільний дільник. Більше того, його можна знайти, використовуючи наступну процедуру, відому під назвою алгоритм Евкліда. Нехай задано ненульові елементи a, b евклідового кільця R з евклідовою нормою N. Не обмежуючи загальності, можна вважати, що $N(a) \geq N(b)$. Ділимо з остачею a на b. Одержуємо рівність

$$a = bq_1 + r_1, \text{ де } r_1 = 0 \text{ або } N(r_1) < N(b).$$

Якщо $r_1 = 0$, то НСД$(a, b) = b$. Якщо ж $r_1 \neq 0$, то ділимо з остачею b на r_1:

$$b = r_1 q_2 + r_2, \text{ де } r_2 = 0 \text{ або } N(r_2) < N(r_1).$$

Знову, якщо $r_2 = 0$, то НСД$(a, b) = r_1$. Інакше ділимо з остачею r_1 на r_2 і т.д. Оскільки $N(b) > N(r_1) > N(r_2) > \ldots$, то за скінченне число кроків ми одержимо остачу, рівну 0. Тоді найбільшим спільним дільником елементів a і b буде остання ненульова остача. Крім того, послідовно виражаючи її через попередні, можна отримати лінійний вираз для найбільшого спільного дільника елементів a, b, тобто подати його у вигляді суми $l_1a + l_2b$ для деяких елементів $l_1, l_2 \in R$.

Означення 14. Область цілісності, в якій кожен ідеал є головним, називається кільцем головних ідеалів.

Має місце

Теорема 3. 1) Кожне евклідове кільце є кільцем головних ідеалів.
2) Кожне кільце головних ідеалів є факторіальним.

Це означає, що, зокрема, кільцями головних ідеалів є кільце цілих чисел $\mathbb{Z}$, кільце многочленів $F[x]$ над полем F, кільце цілих гаусових чисел $\mathbb{Z}[i]$.

Зауважимо, що твердження, обернені до тверджень теореми 3, є неправильними.

Приклади розв'язування задач

Приклад 48. За допомогою алгоритма Евкліда в кільці $\mathbb{Z}_7[x]$ обчислити НСД(f, g), якщо $f(x) = x^4 + 2x^2 + x + 2$, $g(x) = x^3 + 5x + 3$. Многочлен НСД(f, g) подати у вигляді НСД$(f, g) = hf + kg$, де $h, k \in \mathbb{Z}_7[x]$.

Оскільки $\deg(f) > \deg(g)$, то спочатку ділимо з остачею f на g. Отримаємо:

$$x^4 + 2x^2 + x + 2 = (x^3 + 5x + 3)x + (4x^2 + 5x + 2). \tag{4}$$

Тепер ділимо з остачею g на $4x^2 + 5x + 2$:

$$x^3 + 5x + 3 = (4x^2 + 5x + 2)(2x + 1) + (3x + 1). \tag{5}$$

Наступний крок:

$$4x^2 + 5x + 2 = (3x + 1)(6x + 2).$$

Ми бачимо, що відбулося ділення без остачі, тому припиняємо процес ділення: НСД(f, g) — це остання ненульова остача, тобто будь-який многочлен, асоційований із $(3x + 1)$.

Тепер, користуючись рівностями 4 і 5, знайдемо лінійний вираз для НСД(f, g).

$$3x + 1 = (x^3 + 5x + 3) + (4x^2 + 5x + 2) \cdot (5x + 6) =$$
$$(x^3 + 5x + 3) + ((x^4 + 2x^2 + x + 2) + (x^3 + 5x + 3) \cdot 6x) \cdot (5x + 6) =$$
$$(x^4 + 2x^2 + x + 2) \cdot (5x + 6) + (x^3 + 5x + 3) \cdot (2x^2 + x + 1).$$

Приклад 49. Нехай $K = \mathbb{Z}_5[x]$, $I = ((x^3 + 4x^2 + x + 3))$. Користуючись алгоритмом Евкліда, обчислити $((x^2 + 2x + 4) + I)^{-1}$ у факторкільці K/I.

Нехай $h(x) \in \mathbb{Z}_5[x]$. Зауважимо, що рівність $(h(x) + I) \cdot ((x^2 + 2x + 4) + I) = 1 + I$ виконується у факторкільці K/I тоді й лише тоді, коли в $\mathbb{Z}_5[x]$ для деякого $k(x) \in \mathbb{Z}_5[x]$ виконується рівність

$$h(x) \cdot (x^2 + 2x + 4) + k(x) \cdot (x^3 + 4x^2 + x + 3) = 1.$$

За допомогою алгоритма Евкліда знаходимо НСД$(x^2 + 2x + 4, x^3 + 4x^2+x+3)$ в K і його лінійний вираз: НСД$(x^2+2x+4, x^3+4x^2+x+3) = 1$,

$$1 = (x^2 + 2x + 4) \cdot (3x^2 + 2x + 1) + (x^3 + 4x^2 + x + 3) \cdot (2x + 4).$$

Отже, $h(x) = 3x^2 + 2x + 1$. Таким чином, у факторкільці маємо: $((x^2 + 2x + 4) + I)^{-1} = (3x^2 + 2x + 1) + I$.

Приклад 50. За допомогою алгоритма Евкліда в кільці $\mathbb{Z}[i]$ обчислити НСД чисел $4 + 18i$ і $23 + i$.

Спочатку визначимо, в якого із данних чисел більша норма: $N(4 + 18i) = 4^2 + 18^2 = 340$, $N(23 + i) = 23^2 + 1^2 = 530$. Ділимо $23 + i$ (бо норма цього числа більша) на $4 + 18i$ у полі $\mathbb{C}$:

$$\frac{23 + i}{4 + 18i} = \frac{1}{340}(23 + i)(4 - 18i) = \frac{11}{34} - \frac{41}{34}i.$$

Найближчими цілими числами до $\frac{11}{34}$ і $-\frac{41}{34}$ є відповідно 0 і -1. Тому покладемо неповну частку (в $\mathbb{Z}[i]$) при діленні $23 + i$ на $4 + 18i$ рівною $0 + (-1)i = -i$, після чого обчислимо остачу r_1 із рівності $23 + i = (4+18i)(-i)+r_1$. Отримаємо $r_1 = 5+5i$. Отже, перша рівність в ланцюгу рівностей алгоритма Евкліда буде такою:

$$23 + i = (4 + 18i)(-i) + (5 + 5i).$$

Зауважимо, що $N(5+5i) = 50 < 340 = N(4+18i)$. Наступним кроком ділимо (в $\mathbb{C}$) $4 + 18i$ на $5 + 5i$:

$$\frac{4 + 18i}{5 + 5i} = \frac{1}{10}(4 + 18i)(1 - i) = \frac{22}{10} + \frac{4}{10}i \approx 2 + i.$$

Тому друга рівність в нашому ланцюгу рівностей буде наступною:

$$4 + 18i = (5 + 5i)(2 + i) + r_2.$$

Звідси знаходимо r_2 : $r_2 = -1 + 3i$. Відзначимо, що $N(r_2) < N(r_1)$. Наступним кроком ділимо в $\mathbb{C}$ r_1 на r_2 :

$$\frac{5 + 5i}{-1 + 3i} = \frac{1}{10}(5 + 5i)(-1 - 3i) = 1 - 2i.$$

Отже, $5 + 5i = (-1 + 3i)(1 - 2i) + 0$. Таким чином, остання ненульова остача — це r_2, і НСД$(4 + 18i, 23 + i) = -1 + 3i$.

Приклад 51. Довести, що ідеал I кільця головних ідеалів R є простим тоді й лише тоді, коли він є максимальним.

Те, що із максимальності ідеала I випливає його простота, є наслідком тверджень 7, 8. Припустимо, $I = (p)$ простий, і $(p) \subseteq (a)$ для деякого необоротного $a \in R$ (зауважимо, що необоротність a рівносильна тому, що $(a) \neq R$). Звідси випливає, що $p \in (a)$, тобто $p = ka$ для деякого $k \in R$. Остання рівність і простота p тягнуть, що k мусить бути оборотним. Отже, a і p є асоційованими, звідки випливає, що $(p) = (a)$. Таким чином, (p) є максимальним.

Приклад 52. Довести, що

а) факторкільце $\mathbb{Z}[i]/(2)$ не є полем;

б) факторкільце $\mathbb{Z}[i]/(3)$ є полем з 9 елементів;

в) факторкільце $\mathbb{Z}[i]/(n)$ $(n \geq 2)$ є полем тоді й лише тоді, коли n — просте число, що не дорівнює сумі квадратів двох цілих чисел.

Випадки а) і б) випливають із в). За твердженням 8 факторкільце $\mathbb{Z}[i]/(n)$ є полем тоді й лише тоді, коли ідеал (n) є максимальним. Оскільки кільце $\mathbb{Z}[i]$ — евклідове, то воно є кільцем головних ідеалів. Звідси, враховуючи попередній приклад, випливає, що факторкільце

$\mathbb{Z}[i]/(n)$ є полем тоді й лише тоді, коли ідеал (n) є простим. В свою чергу, ідеал (n) є простим тоді й лише тоді, коли елемент n є простим в $\mathbb{Z}[i]$. Таким чином, нам треба показати, що n є простим в $\mathbb{Z}[i]$ тоді й лише тоді, коли n — просте число, що не дорівнює сумі квадратів двох цілих чисел.

Нехай спочатку n є простим в $\mathbb{Z}[i]$. Тоді, очевищно, що ціле число n також повинно бути простим. Якщо б $n = a^2 + b^2$ для деяких цілих a і b, то тоді б в $\mathbb{Z}[i]$ $n = (a + bi)(a - bi)$. Тому n — просте число, що не дорівнює сумі квадратів двох цілих чисел.

Навпаки, нехай n — просте число, що не дорівнює сумі квадратів двох цілих чисел. Припустимо, що n — не простий елемент в $\mathbb{Z}[i]$ і $n = z_1 z_2$ — нетривіальний розклад на множники. З останньої рівності випливає відповідна рівнівть для норм (тобто квадраиів модулів) елементів: $n^2 = N(z_1)N(z_2)$. Оскільки за припущенням z_1, z_2 — необоротні в $\mathbb{Z}[i]$ і ціле число n просте, то повинно бути $N(z_1) = N(z_2) = n$. Звідси випливає, що $n = a^2 + b^2$, $z_1 = a + bi$. Отримана суперечність завершує доведення.

Приклад 53. Довести, що кільце $\mathbb{Z}[x]$ многочленів з цілими коефіцієнтами не є кільцем головних ідеалів.

Зауважимо, що задане кільце є областю цілісності і тому для доведення вкажемо ідеал цього кільця, який не є головним. Нехай I — це множина всіх многочленів з цього кільця з парним вільним членом. Очевидно, I є ідеалом. Припустимо, що цей ідеал є головним, тобто $I = (s(x))$ для деякого $s(x) \in \mathbb{Z}[x]$. Оскільки $2 \in I$, то існує такий многочлен $t(x)$, що $2 = s(x)t(x)$. Це означає, що степені многочленів $s(x)$ і $t(x)$ рівні 0, тобто кожен з них тотожно дорівнює деякому ненульовому цілому числу. А саме, можливі лише випадки, коли $s(x) \equiv \pm 1$ або $s(x) \equiv \pm 2$. Але якщо $s(x) \equiv \pm 1$, то $I = (s(x)) = \mathbb{Z}[x]$. Якщо ж $s(x) \equiv \pm 2$, то $I = (s(x))$ складається з многочленів з парними коефіцієнтами. Обидва випадки суперечать вибору I. Таким чином, ідеал I не є головним, а кільце $\mathbb{Z}[x]$ не є кільцем головних ідеалів

Задачі

7.1 За допомогою алгоритма Евкліда обчислити НСД наступних пар елементів кільця $\mathbb{Z}$:

а) $2352, 268$; б) $15088, 4554$;

в) $2159, 221$; г) $29049, 2047$;

д) $13699, 1349$; е) $21567, 5005$.

7.2 За допомогою алгоритма Евкліда для кільця $\mathbb{Z}$ обчислити обернений для заданого елемента кільця $\mathbb{Z}_{1734}$:

а) 343; б) 185; в) 637; г) 1633.

7.3 За допомогою алгоритма Евкліда обчислити НСД многочленів $f, g \in \mathbb{Z}_7[x]$, а також знайти лінійний вираз НСД$(f, g) = hf + kg$, $h, k \in \mathbb{Z}_7[x]$:

а) $f = x^4 + 5x^3 + 2x + 6$, $g = x^3 + 4x^2 + 4x + 5$;

б) $f = x^4 + x^2 + 6x + 3$, $g = x^4 + x^3 + 5x + 1$.

7.4 За допомогою алгоритма Евкліда для кільця $\mathbb{Z}_5[x]$ обчислити у факторкільці $\mathbb{Z}_5[x]/I$, $I = (x^3+x+1)$, обернені до наступних елементів:

а) $(x^2 + 4x + 1) + I$; б) $(2x^2 + 4x + 3) + I$;

в) $(4x^2 + 4x + 2) + I$; г) $(4x^2 + 3x + 3) + I$.

7.5 За допомогою алгоритма Евкліда обчислити НСД наступних пар елементів кільця $\mathbb{Z}[i]$:

а) $7 - i, 5 + 9i$; б) $6 + 7i, 1 - 8i$;

в) $19 + 9i, 11 - 3i$; г) $5 + 5i, 13 + 3i$;

д) $4 - 2i, 9 + 3i$; е) $5 + 12i, 7 - 2i$.

7.6 Доведіть, що функція $N : \mathbb{Z}[i\sqrt{2}] \to \mathbb{N} \cup 0$, визначена правилом $N(a + bi\sqrt{2}) = a^2 + 2b^2$, є евклідовою нормою.

7.7 За допомогою алгоритма Евкліда обчислити НСД наступних пар елементів кільця $\mathbb{Z}[i\sqrt{2}]$:

а) $5 + i\sqrt{2}, 9$; б) $7 - 4i\sqrt{2}, 17 - 2i\sqrt{2}$;

в) $5 + 6i\sqrt{2}, 4 - i\sqrt{2}$; г) $9 + 9i\sqrt{2}, 13 - 10i\sqrt{2}$.

7.8 Довести, що функція $N : \mathbb{Z}[\sqrt{3}] \to \mathbb{N} \cup \{0\}$, визначена правилом $N(a + b\sqrt{3}) = |a^2 - 3b^2|$, є евклідовою нормою.

7.9 За допомогою алгоритма Евкліда обчислити НСД наступних пар елементів кільця $\mathbb{Z}[\sqrt{3}]$:

а) $7 + 5\sqrt{3}, 14 - 3\sqrt{3}$; б) $25 + 3\sqrt{3}, 1 + 13\sqrt{3}$;

в) $8 + \sqrt{3}, 6 - 3\sqrt{3}$; г) $16 - i\sqrt{3}, 2 + 4\sqrt{3}$.

7.10 Нехай K — евклідове кільце і N — евклідова норма на K. Довести, що елемент $a \in K$ є оборотним тоді й тільки тоді, коли $N(a) = N(1)$.

7.11 Довести, що кільце $\mathbb{Z}[i\sqrt{3}]$ не є евклідовим.

7.12 Довести, що область цілісності R є евклідовим кільцем тоді й лише тоді, коли існує функція $N : R/\{0\} \to \mathbb{N} \cup 0$, для якої виконується лише умова 2) з означення 13.

7.13 При яких n кільце $\mathbb{Z}_n$ є кільцем головних ідеалів?

7.14 Довести, що кільце $\mathbb{F}[x, y]$ ($\mathbb{F}$ — поле) не є кільцем головних ідеалів.

7.15 Довести, що у підкільці кільця многочленів $\mathbb{F}[x]$ ($\mathbb{F}$ — поле), яке складається з усіх многочленів з нульовим коефіцієнтом при x, ідеал, породжений x^2 та x^3, не є головним.

7.16 Нехай R — кільце головних ідеалів. Довести, що для довільної матриці $A \in M_n(R)$ існують оборотні елементи U, V кільця $M_n(R)$ такі, що добуток UAV є діагональною матрицею $diag(d_1, d_2, \ldots, d_k, 0, \ldots, 0)$, причому $d_1|d_2| \ldots |d_k$.

7.17 Підкільце A кільця $\mathbb{C}$ називається майже евклідовим, якщо модулі всіх його елементів цілі і для довільних елементів $a, b \in A$, $b \neq 0$, таких, що a не ділиться на b, знайдуться елементи $c, d \in A$, для яких виконуються нерівності

$$0 < |ac - bd|^2 < |b|^2.$$

Довести, що кожне майже евклідове кільце є кільцем головних ідеалів.

Далі наводиться низка задач, присвячена прикладу кільця головних ідеалів, яке не є евклідовими. Розглядається кільце $A = \mathbb{Z}[\theta]$, де $\theta = \frac{1+i\sqrt{19}}{2}$.

7.18 Показати, що кільце A рівне кільцю A_{-19} з прикладу 10.

7.19 Перевірити наступні рівності:

a) $\bar{\theta} = 1 - \theta$;

b) $\theta\bar{\theta} = 5$;

c) $\theta^2 = \theta - 5$;

d) $\theta(a+b\theta) = -5b + (a+b)\theta$ для довільного $a+b\theta \in A$;

e) $|a+b\theta|^2 = a^2 + ab + 5b^2$ для довільного $a+b\theta \in A$.

7.20 Довести, що $A^* = \{1, -1\}$.

7.21 Довести, що елементи $\pm 2, \pm 3$ нерозкладні в A. (Вказівка: Якщо $2 = (a+b\theta)(c+d\theta)$, то $4 = |a+b\theta|^2|c+d\theta|^2$.)

7.22 Довести, що кільце A не є евклідовим. (Вказівка: Припустити, що на A існує евклідова норма. Показати, що мінімальне значення норми серед ненульових необоротних елементів A може мати лише один з елементів $\pm 2, \pm 3$. Поділивши θ на кожен з них з остачею, отримати суперечність.)

7.23 Нехай $a+b\theta \in \mathbb{Q}[\theta] \setminus \mathbb{Z}[\theta]$. У кожному з наступних випадків вказати такі $c, d \in A$, що $0 < |(a+b\theta)c - d|^2 < 1$:

a) $b \in \mathbb{Z}$;

b) $a \in \mathbb{Z}$, $5b \notin \mathbb{Z}$;

c) $a \in \mathbb{Z}$, $5b \in \mathbb{Z}$;

d) $a, b \notin \mathbb{Z}$, $2a, 2b \in \mathbb{Z}$;

e) $2a, 2b \notin \mathbb{Z}$;

f) $2a \in \mathbb{Z}$, $a, 2b \notin \mathbb{Z}$;

g) $2b \in \mathbb{Z}$, $2a, b \notin \mathbb{Z}$.

7.24 Довести, що кільце A є майже евклідовим, а отже кільцем головних ідеалів.

7.25 Довести, що кільце $B = \mathbb{Z}[\omega]$, де $\omega = \frac{1+i\sqrt{23}}{2}$ не є евклідовим. Чи буде воно кільцем головних ідеалів?

Література

[1] J.Rutkowski Algebra abstrakcyjna w zadaniach. Warszawa:PWN, 2000.

[2] Сборник задач по алгебре (под редакцией А.И.Кострикина) М.:Физматлит, 2001.

[3] О.О.Безущак, О.Г.Ганюшкін Елементи теорії чисел. К.:ВПЦ Київський університет, 2003.

[4] О.Г.Ганюшкін, О.О.Безущак Завдання до практичних занять з алгебри і теорії чисел (теорія груп). К.:ВПЦ Київський університет, 2004.

[5] А.И.Кострикин Введение в алгебру. М.:Наука , 1977.

[6] N.M. Gubareni, V.V.Kirichenko. Rings and Modules. Czestochowa, 2001.

[7] М.Атья, И.Макдональд Введение в коммутативную алгебру. М.:Мир, 1972.

[8] Н.Джекобсон Теория колец. М.:Из-во иностранной литературы, 1947.

[9] И.Херстейн Некоммутативные кольца. М.:Мир, 1972.