Державний вищий навчальний заклад
“ Запорізький національний університет ”
Міністерство освіти і науки України

І.Г. Величко
А.І. Зінченко

ТЕОРІЯ КІЛЕЦЬ

Навчально-методичний посібник
для студентів IV курсу математичного факультету

Затверджено
вченою радою ЗНУ
протокол № від

Запоріжжя
2010

УДК 512.55
ББК 22.144

Величко І.Г. Зінченко А.І. Теорія кілець: Навчально-методичний посібник для студентів IV курсу математичного факультету. – Запоріжжя: ЗНУ, 2010. – с.

Навчально-методичний посібник містить означення, приклади розв'язання задач та задачі для самостійного розв'язку по курсу "Теорія кілець".

Призначений для студентів IV курсу математичного факультету денного та заочного відділень.

Рецензент
зав. кафедри алгебри і геометрії ЗНУ
д.фіз.-мат. наук, проф. *А.К. Приварников*
Відповідальний за випуск *І.Г.Величко*

ЗМІСТ

1. ВСТУП

Курс теорії кілець є невід'ємною складовою частиною підготовки фахівця в області алгебри. Йому передує вивчення загального курсу «алгебра і теорія чисел» і курсу за вибором студента «теорія груп». Знання, отримані в результаті опрацювання теоретичного і практичного матеріалу курсу, будуть корисними при опануванні наступного алгебраїчного курсу «Теорія полів».

Одним з важливих прикладів кілець є множина цілих чисел з операціями додавання і множення. Використання цього факту дозволяє узагальнити деякі результати, отримані в теорії чисел. Майже всі результати, які стосуються многочленів та матриць, знайомі студентам з курсів алгебри і лінійної алгебри, можна сформулювати в термінах кілець.

З методичної точки зору вивчення курсу «Теорія кілець» також є дуже важливим для студентів-математиків. Одною з основних вимог до сучасного математика є вміння проводити математичні перетворення в рамках заданої аксіоматики. Розвитку цього вміння сприяє розв'язання алгебраїчних задач, і зокрема, задач, пов'язаних з алгебраїчними структурами. Майже всі задачі, наведені в цьому посібнику, для розв'язання окрім знання аксіоматики потребують творчого мислення.

Там, де самостійне розв'язання задач може визвати труднощі, наведені вказівки. Для найбільш складних задач наведені розв'язки.

1. Означення кільця. Приклади кілець.

Кільце $(K,+,\cdot)$ - це множина K, на якій задано дві бінарні алгебраїчні операції: додавання $(+)$ і добутку $(\cdot)$ і виконуються наступні аксіоми.

0.1) $\forall a,b\in K$ $\quad a+b\in K$ (алгебраїчність операції додавання)

0.2) $\forall a,b\in K$ $\quad a\cdot b\in K$ (алгебраїчність операції добутку)

1) $\forall a,b,c\in K$ $\quad a+(b+c)=(a+b)+c$ (асоціативність додавання)

2) $\exists q\in K\ \ \forall a\in K$ $\quad a+q=a$ (існування нейтрального елемента відносно додавання).

3) $\forall a\in K\ \ \exists b\in K$ $\quad a+b=q$ (існування протилежного елемента).

4) $\forall a,b\in K$ $\quad a+b=b+a$ (комутативність додавання).

5.1) $\forall a,b,c\in K$ $\quad a\cdot(b+c)=a\cdot b+a\cdot c$ (ліва дистрибутивність)

5.2) $\forall a,b,c\in K$ $\quad (a+b)\cdot c=a\cdot c+b\cdot c$ (права дистрибутивність).

Аксіоми 0.1 та 1-4 означають, що множина K є комутативною групою відносно операції додавання. Нейтральний елемент відносно додавання зазвичай називають нульовим. Елемент, протилежний елементу a позначають “$-a$”. Вираз $a-b$ є скорочений запис виразу $a+(-b)$. Для зручності в подальшому при записі добутку елементів знак $\cdot$ будемо опускати.

В кільці можуть виконуватися і додаткові аксіоми, і в цьому разі кільця мають спеціальну назву.

6) $\forall a,b,c\in K$ $\quad a(bc)=(ab)c$ (асоціативність добутку). Відповідні кільця називають ***асоціативними***.

7) $\forall a,b\in K$ $\quad ab=ba$ (комутативність добутку). Відповідні кільця називають ***комутативними***.

8) $\exists e\in K\ \ \forall a\in K$ $\quad ae=ea=a$ (існування нейтрального елемента відносно добутку). Нейтральний елемент відносно добутку називають одиницею кільця а відповідні кільця - ***кільцями з одиницею***.

9) $\forall a\neq q\ \ \exists b$ $\quad ab=ba=e$ (оберненість ненульових елементів). Елемент, обернений до елемента a позначають a^{-1}.

В подальшому, якщо не зазначено протилежне, під терміном кільце будемо розуміти асоціативне кільце.

В некомутативних кільцях розрізняють ліву та праву одиниці (права одиниця – це такий елемент e, що $\forall a \quad ea = a$).

У разі, якщо на множині $(K,+,\cdot)$ виконуються аксіоми 0-9, то матимемо таку алгебраїчну структуру як ***поле***. Іншими словами поле – це асоціативне комутативне кільце з 1, в якому кожний ненульовий елемент має обернений.

Вправи

1.1. Заповнити таблицю

Множина	0	1	2	3	4	5	6	7	8	9	Висновок

В якості множин розглянути $N, Z, Q, R, C, M_2(Z), M_2(R), R[x], 3Z, Z_3, Z_6$ з природним чином заданими операціями додавання і добутку. Тут $M_2(Z)$ та $M_2(R)$ - множини квадратних матриць другого порядку відповідно з цілими та дійсними елементами, $R[x]$- множина поліномів з дійсними коефіцієнтами, $3Z$ - множина цілих чисел, кратних трьом, Z_m - множина лишків по модулю m.

К відповідних клітинках таблиці потрібно поставити знак “+” якщо аксіома виконується та знак “–” в противному випадку.

1.2. Довести, що множина $M = \left\{ \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} a, b \in Z \right\}$ є кільцем.

1.3. A - деяка множина, B - сукупність всіх підмножин множини A. На множині B задамо операцію додавання і добутку наступним чином:

$$X + Y = (X \cup Y) \setminus (X \cap Y) \text{ та } X \cdot Y = X \cap Y .$$

Довести, що $(B,+,\cdot)$ є кільце з 1.

1.4 Кільце, для якого виконуються всі аксіоми 0-9 за виключенням аксіоми 7, називають ***тілом***. Кватерніони – це множина елементів вигляду $z = x + iy + jz + kt$, де x, y, z, t - дійсні числа. Складаються кватерніони покомпонентно. При обчисленні добутку користуються співвідношеннями $i^2 = j^2 = k^2 = -1$, $ij = k,\ ji = -k$, $jk = i, kj = -i$, $ki = j, ik = -j$. Довести що множина кватерніонов є тілом.

Приклади розв'язання задач

1.1. Розглянемо множину $Z_6 = \{0,1,2,3,4,5\}$. Додавання та добуток елементів задаються наступними таблицями

+	**0**	**1**	**2**	**3**	**4**	**5**
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

.	**0**	**1**	**2**	**3**	**4**	**5**
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	6	2	4
3	0	3	6	3	6	3
4	0	4	2	6	4	2
5	0	5	4	3	2	1

Перевіримо аксіоми кільця.

Так як всі елементи таблиці належать множені Z_6, то це означає, що нульова аксіома (яка складається з двох: 0.1 та 0.2) виконується.

Аксіома 1 виконується. Для перевірки цього потрібно взяти всілякі впорядковані трійки елементів з Z_6 та перевірити аксіому.

Наприклад, для трійки 3,4,1 маємо

3+(4+1)=3+5=2, (3+4)+1=1+1=2, 2=2.

Або можна скористатися наступним міркуванням: так як числа $a+(b+c)$ та $(a+b)+c$ співпадають, то вони мають однакові остачі при діленні на будь яке натуральне число, в тому числі і на 6.

Аксіома 2 виконується. Нейтральним елементом відносно додавання є елемент 0.

Аксіома 3 виконується. В кожному рядку таблиці для додавання нульовий елемент зустрічається рівно по одному разу, а це означає, що для кожного елементу є протилежний.

Аксіома 4 виконується. Таблиця для суми є симетричною відносно головної діагоналі, а це і означає, що додавання комутативне.

Аксіома 5 виконується. Довести цей факт можна так само, як і аксіому 2.

Аксіома 6 виконується. Доведення аналогічне доведенню аксіоми 2.

Аксіома 7 виконується. Таблиця для добутку є симетричною відносно головної діагоналі, а це і означає, що множення комутативне

Аксіома 8 виконується. Нейтральним елементом відносно множення є елемент 1.

Аксіома 9 не виконується. Так як в рядках таблиці множення, які відповідають елементам 2,3,4, немає одиниць, то ці елементи не мають обернених.

Отже можна зробити висновок, що множина Z_6 з природним чином заданими операціями додавання і добутку є асоціативне комутативне кільце з одиницею, але не є полем.

2. Наслідки із аксіом кільця

2.1. Довести, що права дистрибутивність є наслідком комутативності множення і лівої дистрибутивності.

2.2. Довести, що для будь якого кільця мають місце наступні твердження:

а) $\forall x \quad xq = qx = q$.

б) Якщо $a + x = a + y$, то $x = y$.

в) При заданих a, b рівняння $a + x = b$ має єдиний розв'язок $x = (-a) + b$.

г) $\forall a, b \qquad (-a)(-b) = ab$.

д) $\forall a, b \qquad (-a)b = a(-b) = -(ab)$

2.3. Довести, що якщо в кільці є одиниця, то вона одна.

Вказівка. Припустити, що в кільці дві одиниці, та знайти їх добуток.

2.4. Навести приклади кілець спеціального вигляду, які мають декілька лівих одиниць. Те ж завдання для правих одиниць.

Вказівка. Розглянути в кільці M *із вправи 1.2 матриці вигляду* $\begin{pmatrix} 1 & 0 \\ x & 0 \end{pmatrix}$ *і перевірити, що всі вони є лівими одиницями.*

В якості кільця, яке містить декілька правих одиниць, розглянути кільце $M' = \left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \middle| a, b \in Z \right\}$.

2.5. Навести приклад кільця з одиницею, в якому є необоротні елементи, які мають однобічні обернені.

2.6. Довести, що оборотні елементі комутативного кільця (тобто ті елементи, які мають обернений) створюють групу відносно множення.

2.7. Нехай K - асоціативне кільце з одиницею e. Довести що з оберненості елементу $e - ab$ випливає оберненість елемента $e - ba$.

2.2. а) Відповідно до аксіоми 2 маємо, що $x+q=x$. Помножимо цю рівність зліва (нагадаємо, що кільце не обов'язково комутативне, тому обов'язково вказувати, з якої сторони виконується множення) на елемент x. Матимемо $x(x+q)=x^2$. Звідки, після використання дистрибутивності виливає, що

$$x^2+xq=x^2.$$

Відповідно до аксіоми 3 існує елемент, протилежний елементу x^2. Додамо його до обох частин цієї рівності (так як додавання є комутативним, то не потрібно пояснювати, з якої сторони ми його додаємо).

$$x^2+xq+\left(-x^2\right)=x^2+\left(-x^2\right).$$

Скориставшись комутативністю та асоціативністю додавання (аксіоми 1 та 4) запишемо

$$\left(x^2+\left(-x^2\right)\right)+xq=x^2+\left(-x^2\right).$$

Згідно аксіомі 3 сума будь якого елемента та протилежного йому дорівнює нульовому елементу, а отже

$$q+xq=q\ .$$

Застосувавши до лівої частини отриманої тотожності аксіому 2, матимемо, що

$$xq=q\ ,$$

що й потрібно було довести.

2.7. Позначимо через c елемент, обернений до елементу $e-ab$. Тоді $(e-ab)c=c-abc=e$ і $c(e-ab)=c-cab=e$, звідки випливає, що

$$abc=c-e \qquad \text{(а)}$$

та

$$cab=c-e. \qquad \text{(б)}$$

Потрібно довести, що існує елемент d такий, що

$$(e-ba)d=e, \qquad \text{(в)}$$

та

$$d(e-ba)=e \qquad \text{(г)}$$

Почнемо з (в). Для того, щоб явно отримати елемент e в правій частині цієї рівності, елемент d будемо шукати у вигляді

$$d = e + x . \tag{д}$$

Тоді

$$(e - ba)d = (e - ba)(e + x) = e - ba + x - bax = e .$$

Для того, щоб було виконане остання рівність, елемент x повинен задовольняти рівнянню

$$(e - ba)x = ba . \tag{е}$$

Для того, щоб використати формулу (а), обчислимо вираз

$$(e - ba)bc = bc - b(abc) = bc - b(c - e) = bc - bc + be = b .$$

Отримане співвідношення $(e - ba)bc = b$ помножимо справа на елемент a:

$$(e - ba)bca = ba . \tag{є}$$

Порівняємо (е) та (є). Як бачимо, $x = bca$, а отже, згідно (д) маємо, що

$$d = e + bca . \tag{ж}$$

Доведемо, що знайдене d задовольняє не тільки (в), але й (г).

$$d(e - ba) = (e + bca)(e - ba) = e + bca - ba - bcaba = e + b(c - e - cab)a =$$

$$= e + bqa = e + q = e.$$

Таким чином ми довели, що елемент $e + bca$ є оберненим до елементу $e - ba$.

3. Нільпотенти та ідемпотенти. Дільники нуля.

Елемент x кільця K називається ***нільпотентом***, якщо $\exists n \in N$, таке, що $x^n = q$. Елемент x кільця K називається ***ідемпотентом***, якщо $x^2 = x$.

Елемент $a \neq q$ кільця K називається ***дільником нуля***, якщо існує $b \neq 0$, такий що $ab = 0$. Кільце K називається ***областю цілісності***, якщо в ньому немає дільників нуля.

Іншими словами, кільце K називається областю цілісності, якщо з рівності $ab = q$ випливає, що $a = q$ або $b = q$.

3.1. Привести приклади нільпотента, ідемпотента, дільника нуля. *Вказівка. Розгляньте кільце* $M_2(Z)$.

3.2. Довести, що поле є областю цілісності.

3.3. Довести, що в полі є тільки два ідемпотента і тільки один нільпотент.

3.4. Довести, що якщо x - нільпотент кільця з одиницею, то елементи $e + x$ та $e - x$ мають обернені.

3.5. З'ясуйте, чи є дільники нуля в кільцях Z_6, Z_8, Z_9, Z_{10}. При яких m кільце Z_m є областю цілісності.

Вказівка. Доведіть, що кільце Z_m містить нільпотентні елементи тоді і тільки тоді, коли m не свободо від квадратів (тобто коли m ділиться на квадрат деякого простого числа).

3.6. Довести, що якщо x - ідемпотент кільця з одиницею, то елемент $y = e - x$ також є ідемпотентом, та x, y - дільники нуля. *Вказівка. Довести, що* $xy = q$.

3.7. В кільці K кожен елемент є ідемпотентом. Довести, що кільце K комутативне.

3.8. Довести, що елемент, який має обернений, не може бути дільником нуля.

3.9. K - область цілісності, $a \neq q$, $ab = ac$. Довести, що $b = c$. (Це означає, що в полі можна скорочувати рівність на ненульовий елемент).

3.10. Довести, що будь яке скінчене комутативне кільце з 1 без дільників нуля є полем.

3.11. Нехай K - кільце з одиницею без дільників нуля. Довести, що всякий елемент в K, який має однобічний обернений елемент, оборотний.

Приклади розв'язання задач

3.6. Кожен елемент кільця є ідемпотентом. Це означає, що $\forall x \quad x^2 = x$. Потрібно довести, що $\forall a, b \quad ab = ba$.

Перший спосіб.

Візьмемо два довільних елемента c та d, та покладемо $c + d = x$. Тоді

$$c + d = (c + d)^2 = (c + d)(c + d) = c^2 + cd + dc + d^2 = c + cd + dc + d,$$

а отже $\forall c, d$

$$cd + dc = q \tag{а}$$

Аналогічно

$$c - d = (c - d)^2 = (c - d)(c - d) = c^2 - cd - dc + d^2 = c - cd - dc + d,$$

а отже $\forall c, d$

$$cd + dc = d + d \tag{б}$$

Порівняв (а) та (б) маємо, що $\forall d$ має місце тотожність

$$d + d = 0 \tag{в}$$

Поклав в (а) $c = a, d = b$ отримаємо, що $ab + ba = q$. Додамо до обох частин доданок ba:

$$ab + ba + ba = ba \tag{г}$$

Поклавши в (в) $d = ba$, маємо, що $ba + ba = q$. З урахуванням цього співвідношення (г) спроститься і набуде вигляду $ab = ba$, що й потрібно було довести.

Другий спосіб.

$$a+b=(a+b)^2=a^2+ab+ba+b^2=a+ab+ba+b,$$

а отже

$$ab+ba=q \tag{а}$$

Помножимо рівність (а) зліва на ab та отримаємо, що

$$q=(ab)q=(ab)(ab+ba)=abab+abba=(ab)^2+ab^2a=ab+aba \tag{б}$$

Помножимо рівність (а) справа на ba та отримаємо, що

$$q=q(ab)=(ab+ba)(ba)=abba+baba=ab^2a+(ba)^2=aba+ba. \tag{в}$$

З рівностей (б) та (в) випливає, що

$$ab+aba=q=aba+ba,$$

а, отже

$$ab=ba,$$

$ab=ba$, що й потрібно було довести.

3.10 Потрібно довести, що будь який ненульовий елемент має обернений.

Нехай K - скінчене кільце. Позначимо через K^* множину всіх ненульових елементів кільця K, тобто $K^*=\{e,b_1,b_2,...,b_n\}$. Візьмемо ненульовий елемент $a\in K$ і розглянемо множину

$$aK^*=\{ae,ab_1,ab_2,...,ab_n\}.$$

Якщо припустити, що множина aK^* містить однакові елементи, то $ab_k=ab_m$ для деяких $k\neq m$ (можна вважати, що $e=b_0$), а отже

$$a(b_k-b_m)=q\ .$$

Так як K - область цілісності, то $b_k-b_m=q$, що неможливо, бо це різні елементи. Те, що множина aK^* не містить нульових елементів випливає з того, що K є областю цілісності.

Ми довели, що кожна з множини K^* та aK^* містить всі ненульові елементи кільця K, а отже ці множини співпадають. Це означає, що в множині aK^* є елемент $e\in K^*$ або, що теж саме,

$$\exists k,\quad ab_k=e.$$

Таким чином елемент a має обернений.

4. Підкольця.

Підмножина M кільця $K(+,\cdot)$, яка сама є кільцем відносно тих же операцій + та $\cdot$, називається ***підкільцем***. Цей факт будемо записувати у вигляді $M < K$.

Центр кільця K - це підмножина, яка складається із всіх елементів $a \in K$, таких що $\forall x \in K \quad ax = xa$.

4.1. Довести теорему (критерій підкільця): підмножина M кільця K буде підкільцем тоді і тільки тоді, коли виконуються дві наступні аксіоми.

а) $\forall a,b \in M \qquad a-b \in M$

б) $\forall a,b \in M \qquad ab \in M$

Вказівка. Якщо M - підмножина кільця K, то аксіоми 1, 4 та 5 виконуються автоматично. Для перевірки того, що $M < K$, потрібно перевірити лише аксіоми 0, 2 та 3.

4.2. Довести, що множина $M = \left\{ \begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix} \middle| y \in Z \right\}$ не є підкільцем кільця $M_2(Z)$, а множина $H = \left\{ \begin{pmatrix} x & y \\ -y & x \end{pmatrix} \middle| x, y \in Z \right\}$ є комутативним підкільцем кільця $M_2(Z)$.

4.3. Довести, що множина $M = \left\{ \begin{pmatrix} a & b \\ 2b & a \end{pmatrix} \middle| a,b \in Q \right\}$ є полем. З'ясувати, чи для яких цілих n множина $\left\{ \begin{pmatrix} a & b \\ nb & a \end{pmatrix} \middle| a,b \in Q \right\}$ буде полем?

4.4. Знайти всі підкільця кілець Z_3, Z_4, Z_6.

Вказівка. Скористатися тим, що підкільце є підгрупою кільця, якщо їх розглядати як адитивні групи і теоремою Лагранжа про те, що порядок групи ділиться на порядок її підгрупи.

4.5. Нехай K - просте кільце. Довести, що кільце $M_2(K)$ також є простим.

4.6. Довести, що центр кільця є підкільцем.

4.7. Знайти центр кільця $M_2(Z)$.

Приклади розв'язання задач

4.3 Для того, щоб довести, що M є кільцем, можна перевірити аксіоми кільця. Простіше перевірити, що M є підкільцем кільця $M_2(Q)$, а отже і кільцем. Скористаємося результатами вправи 4.1, і перевіримо виконання критерію підкільця

$$\begin{pmatrix} a & b \\ 2b & a \end{pmatrix} - \begin{pmatrix} c & d \\ 2d & c \end{pmatrix} = \begin{pmatrix} a-c & b-d \\ 2(b-d) & a-c \end{pmatrix} \in M,$$

$$\begin{pmatrix} a & b \\ 2b & a \end{pmatrix} \begin{pmatrix} c & d \\ 2d & c \end{pmatrix} = \begin{pmatrix} ac+2bd & ab+bc \\ 2(bc+ad) & 2bd+ac \end{pmatrix} \in M.$$

Ми скористались тим фактом, що якщо $a,b,c,d \in Q$, то

$$a-c, b-d, ac+2bd, ad+bc \in Q.$$

Асоціативність множення елементів M випливає з асоціативності множення матриць.

Перевіримо комутативність:

$$\begin{pmatrix} a & b \\ 2b & a \end{pmatrix} \begin{pmatrix} c & d \\ 2d & c \end{pmatrix} = \begin{pmatrix} ac+2bd & ab+bc \\ 2(bc+ad) & 2bd+ac \end{pmatrix},$$

$$\begin{pmatrix} c & d \\ 2d & c \end{pmatrix} \begin{pmatrix} a & b \\ 2b & a \end{pmatrix} = \begin{pmatrix} ac+2bd & ab+bc \\ 2(bc+ad) & 2bd+ac \end{pmatrix}.$$

Праві частини цих рівностей співпадають, а отже співпадають і ліві, а отже, множення комутативне.

Одиницею кільця M є матриця $E = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

Перевіримо оберненість ненульових елементів. Для ненульової матриці $A=\begin{pmatrix} a & b \\ 2b & a \end{pmatrix}$ існує обернена, якщо $|A| = a^2 - 2b^2 \neq 0$, і в цьому разі $A^{-1} = \frac{1}{a^2-2b^2}\begin{pmatrix} a & -b \\ -2b & a \end{pmatrix}$.

Якщо $|A| = a^2 - 2b^2 = 0$, то $2 = \frac{a^2}{b^2}$, а отже $\frac{a}{b} = \sqrt{2}$, а цього буте не може, так як за означенням a, b - раціональні, а їх відношення $\sqrt{2}$ - ірраціональне. Таким чином, будь який ненульовий елемент кільця M має обернений, а отже M - поле.

5. Ідеали. Головні ідеали.

Підкільце J називається ***лівим ідеалом*** кільця K, якщо

$$\forall j \in J\ \forall x \in K \quad xj \in J\ .$$

Коротко ця умова записується у вигляді $KJ \subset J$. Аналогічно, умовою $JK \subset J$ визначається ***правий ідеал*** кільця K. Для комутативних кілець любою з цих умов визначається поняття ***ідеалу***. Ідеал, який є одночасно лівим та правим, називається ***двостороннім ідеалом***. В комутативному кільці поняття лівого, правого та двостороннього ідеалів співпадають, тому їх називають ***ідеалами***.

Якщо $a_1, a_2, ..., a_m$ є елементами комутативного кільця K, то множина $\left\langle a_1, a_2, ..., a_m \right\rangle = \left\{ \sum\limits_{i=1}^{m} a_i x_i \middle| x_i \in K \right\}$ буде ідеалом. Говорять, що цей ідеал породжений елементами $a_1, a_2, ..., a_m$. Ідеал, породжений одним елементом, називається ***головним ідеалом***.

Добуток ідеалів I та J - це множина $IJ = \sum\limits_{k} i_k j_k\ ,\ i_k \in I, j_k \in J$.

Сумою ідеалів J, I кільця K називають множину $J + I = \left\{ j + i \middle| j \in J, i \in I \right\}$

5.1. Довести теорему (критерій ідеалу): підмножина J кільця K буде лівим ідеалом тоді і тільки тоді, коли виконуються дві наступні аксіоми.

б) $\forall a, b \in J \qquad a - b \in J$

а) $\forall j \in J\ \forall b \in K \qquad jb \in J$

Сформулювати подобну теорему для правого ідеалу та для ідеалу.

5.2. Довести, що в кільці $A = \left\{ \begin{pmatrix} a & b \\ b & a \end{pmatrix} \middle| a, b \in Z \right\}$ множина $J = \left\{ \begin{pmatrix} a & a \\ a & a \end{pmatrix} \middle| a \in Z \right\}$ є ідеалом.

5.3. Довести, що множина $\langle a_1, a_2, ..., a_m \rangle = \left\{ \sum_{i=1}^{m} a_i x_i \middle| x_i \in K \right\}$ є ідеалом.

5.4. Навести приклади ідеалів в кільцях Z, $R[x]$.

5.5. Довести, що множина $M = \left\{ \begin{pmatrix} x & y \\ 0 & x \end{pmatrix} \middle| x, y \in Z \right\}$ є підкільцем кільця $M_2(Z)$ і таким чином є кільцем. Описати всі ідеали кільця M.

5.6. В кільці $M_2(Z)$ навести приклад лівого ідеалу, який не є правим ідеалом.

5.7. Знайти всі двосторонні ідеали в кільці $M_2(Z)$.

5.7. З'ясувати, чи утворюють ідеал необоротні елементи кільця Z_{16}? А кільця Z_{24}? При яких n необоротні елементи кільця Z_n утворюють ідеал.

Вказівка. Довести, що необоротні елементі кільця Z_m утворюють тоді і тільки тоді, коли m є степеню простого числа

5.8. Довести, що перетин ідеалів є ідеалом.

5.9. Довести, що в комутативному кільці добуток ідеалів-ідеал.

5.10. Довести, що сума ідеалів – ідеал.

5.11. Довести, що для довільних ідеалів в комутативному кільці має місце включення $JI \subset (J \cap I)$.

5.12. Нехай J, I_1, I_2 - ідеали кільця з одиницею K. Довести, що якщо $J + I_1 = K$ та $J + I_2 = K$, то $J + I_1 I_2 = K = J + (I_1 \cap I_2)$.

5.13 Довести, що Z - кільце головних ідеалів.

5.14. Довести, що $R[x]$ - кільце головних ідеалів.

5.15. Розглянемо кільце $K = \{x + iy\sqrt{3} \mid x, y \in Z\}$. Довести, що

1) $I = \{3a + ib\sqrt{3} \mid a, b \in Z\}$ - головний ідеал кільця K;

2) $J = \{2a + b + ib\sqrt{3} \mid a, b \in Z\}$ - неголовний ідеал кільця K.

Приклади розв'язання задач

5.12. Рівність $J + I_m = K$ ($m = 1,2$) означає наступне:

$$\forall x \in K \quad \exists\, y_m \in J, z_m \in I_m, \text{ такі, що } x = y_m + z_m.$$

Візьмемо довільний елемент $x \in K$ і, скориставшись умовою задачі, запишемо $x = y_1 + z_1, 1 = y_2 + z_2$. З урахуванням цього матимемо

$$x = x \cdot 1 = (y_1 + z_1)(y_2 + z_2) = y_1 y_2 + y_1 z_2 + y_2 z_1 + z_1 z_2.$$

Так як y_1 та y_2 належать ідеалу J, то і елемент $y = y_1 y_2 + y_1 z_2 + y_2 z_1$ також належить J. Елемент $z = z_1 z_2 \in I_1 I_2$, а, отже, $x = y + z \in J + I_1 I_2$.

Ми довели, що $\forall x \in K \quad x \in J + I_1 I_2$, звідки випливає включення $K \subset J + I_1 I_2$. Обернене включення $J + I_1 I_2 \subset K$ тривіальне. Таким чином $J + I_1 I_2 = K$.

5.13. Доведемо що Z - кільце головних ідеалів. Нехай M - ненульовий ідеал Z. Позначимо через a мінімальний додатній елемент множини M. Доведемо, що $M = \langle a \rangle$.

Так як $a \in M$, а M є ідеалом, то $\forall x \in Z \quad ax \in Z \Rightarrow \langle a \rangle = aZ \subset M$.

Той факт, що $M \subset \langle a \rangle$ будемо доводити методом від супротивного. Нехай існує $b \in M \setminus \langle a \rangle$. Тоді поділимо число b на число a з остачею:

$$b = aq + r, \; 0 \le r < a.$$

Оскільки $b \notin \langle a \rangle$, то b не ділиться на a. Звідси випливає, що остача $r \neq 0$.

Елемент $b \in M$ і $aq \in M$, оскільки $a \in M$, а M є ідеалом. Таким чином ми знайшли додатне число $r = b - aq$, яке належить M і менше за a, а це суперечить вибору a.

З включень $\langle a \rangle \subset M$ та $M \subset \langle a \rangle$ випливає, що $M = \langle a \rangle$. Таким чином ідеал M породжений одним елементом, і отже є головним.

5.15. Доведемо, що $I = \langle i\sqrt{3} \rangle$.

Візьмемо довільний елемент кільця і помножимо його на $i\sqrt{3}$:

$(x + iy\sqrt{3})i\sqrt{3} = -3y + 3ix\sqrt{3} \in I$, а це означає, що $\langle i\sqrt{3} \rangle \subset I$.

Візьмемо довільний елемент із I та запишемо його у вигляді добутку елементу кільця на $i\sqrt{3}$:

$$3a + ib\sqrt{3} = (b - ia\sqrt{3})i\sqrt{3}.$$

Це означає, що $I \subset \langle i\sqrt{3} \rangle$. Отже ми можемо зробити висновок, що ідеал $I = \langle i\sqrt{3} \rangle$ - головний.

Доведемо, що $J = \{2a + b + ib\sqrt{3} \mid a, b \in Z\}$ - неголовний ідеал кільця K. Припустимо супротивне, що $\exists \alpha \in J$, таке, що $J = \langle \alpha \rangle$. Тоді $\forall z \in J\ \exists t \in K \quad z = \alpha\, t$.

Нехай $\alpha = 2a + b + ib\sqrt{3}$, $z = 2c + d + id\sqrt{3}$, $t = x + iy\sqrt{3}$.
Обчислимо

$$\alpha\ t = (2a + b + ib\sqrt{3})(x + iy\sqrt{3}) = 2ax + bx - 3by + i\sqrt{3}(2ay + by + bx) =$$
$$= z = 2c + d + id\sqrt{3}.$$

Таким чином, повинні існувати такі цілі числа a, b, щоб система рівнянь відносно x, y

$$\begin{cases} x(2a + b) - 3by = 2c + d, \\ xb + y(2a + b) = d \end{cases}$$

повинна мати цілі розв'язки при довільних цілих c, d.

Розв'язок цієї системи можна знайти за формулами Крамера

$$\Delta = \begin{vmatrix} 2a+b & -3b \\ b & 2a+b \end{vmatrix} = (2a+b)^2 + 3b^2 ,$$

$$\Delta_x = \begin{vmatrix} 2c+d & -3b \\ d & 2a+b \end{vmatrix} = (2a+b)(2c+d) + 3bd ,$$

$$\Delta_y = \begin{vmatrix} 2a+b & 2c+d \\ b & d \end{vmatrix} = (2a+b)d - (2c+d)b = 2(ad-bc),$$

$$x = \frac{(2a+b)(2c+d)+3bd}{(2a+b)^2+3b^2}, \quad y = \frac{2(ad-bc)}{(2a+b)^2+3b^2} .$$

Покладемо $c=1, d=0$ і знайдемо, що $y = \dfrac{-2b}{(2a+b)^2+3b^2}$.

Оскільки для цілого $b \neq 0$ маємо, що

$$0 < |-2b| < 3b^2 \le \left|(2a+b)^2 + 3b^2\right| ,$$

то в цьому випадку $0 < |y| < 1$, а це суперечить тому, що y – ціле.

Отже $b=0$ і маємо $x = \dfrac{2a(2c+d)}{4a^2}$, $y = \dfrac{2ad}{4a^2} = \dfrac{d}{2a}$. При $d=1$ число y не буде цілим. Отже, при будь-якому виборі цілих числа a,b, можна обрати такі цілі c,d, щоб x,y, які знайдені з системе

$$\begin{cases} x(2a+b) - 3by = 2c+d, \\ xb + y(2a+b) = d \end{cases}$$

не будуть цілими, а це означає, що ідеал J не породжується одним елементом, а, отже, він не є головним.

6. Фактор - кільця

Будемо вважати що K - комутативне кільце. Нехай J - ідеал кільця K. Розіб'ємо множину K на так звані суміжні класи за ідеалом J. Елементи x та y належать одному класу тоді і тільки тоді, коли $x-y\in J$. Через $\bar{x}$ позначимо клас, якому належить елемент x. На множині класів введемо операції $+$ та $\cdot$ наступним чином:

$$\bar{x}+\bar{y}=\overline{x+y},\ \bar{x}\cdot\bar{y}=\overline{xy}.$$

Множина суміжник класів із введеними операціями буде утворювати кільце, яке називається фактор кільцем K по ідеалу J та позначається K/J.

6.1. Довести, що два суміжних класи або не перетинаються, або повність співпадають.

6.2. Довести, що якщо кільце скінчене, то всі суміжні класи мають однакову кількість елементів.

6.3. Довести, що операції додавання та множення на множині суміжних класів вводяться коректно і результат операції не залежить від вибору елементів із класів а залежить лише від самих класів. Тобто потрібно довести, що якщо $\bar{x}=\bar{y}$ та $\bar{z}=\bar{t}$, то $\overline{x+z}=\overline{y+t}$ та $\overline{xz}=\overline{yt}$.

6.4. Знайти всі елементи фактор-кілець $Z/2Z, Z/3Z, Z/4Z$ та виписати для них таблиці додавання і добутку.

6.5. В кільці $Z_6=\{\bar{0},\bar{1},\bar{2},\bar{3},\bar{4},\bar{5}\}$ задані дві підмножини $M=\{\bar{0},\bar{2},\bar{4}\}$ та $T=\{\bar{0},\bar{3}\}$. Довести, що ці підмножини є ідеалами. Описати кільця Z_6/M та Z_6/T.

6.6. Знайти всі суміжні класи в кільці $A = \left\{ \begin{pmatrix} a & b \\ b & a \end{pmatrix} \middle| a, b \in Z \right\}$ по ідеалу $J = \left\{ \begin{pmatrix} a & a \\ a & a \end{pmatrix} \middle| a \in Z \right\}$. Записати таблиці додавання і добутку.

6.7. Довести, що множина всіх многочленів від змінної x з цілими коефіцієнтами, які при $x = 0$ приймають значення 0, утворюють ідеал в кільці всіх многочленів від змінної x з цілими коефіцієнтами $Z[x]$. Знайти суміжні класи по цьому ідеалу.

6.8. Довести, що множина дільників нуля в фактор-кільці $Z / p^k Z$, де p - просте число, є ідеалом.

6.9. Нехай $Z[i] = \{x + iy | x, y \in Z, i^2 = -1\}$ - кільце цілих гаусових чисел, $J = 2Z[i] = \{x + iy | x, y \in 2Z\}$. Описати елементи фактор-кільця $Z[i]/J$ і побудувати таблиці додавання та множення.

6.10. Нехай K - кільце з одиницею, J - ідеал в K. Довести, що фактор кільце K/J також е кільцем з одиницею.

6.11. Відомо що кільце K є областю цілісності. Чи можна стверджувати, що кільце K/J також обов'язково буде областю цілісності?

Вказівка. Розглянути приклад, наведений у вправі 6.9.

Приклади розв'язання задач

6.1. Нехай A та B - два суміжні класи за ідеалом J. Припустимо, що ці класи перетинаються, тобто $\exists x \in A \cap B$. Нехай y - довільний елемент із A. Оскільки елементи x та y належать одному класу A, то, за означенням, їх різниця $x - y \in J$.

З іншого боку, оскільки $x \in B$ та $x - y \in J$, то, за означенням, $y \in B$. Таким чином $A \subset B$. Аналогічно доводиться протилежне включення $B \subset A$, а, отже, якщо ці класи перетинаються, то вони співпадають.

6.9. Елементи $z_1 = x_1 + iy_1$ та $z_2 = x_2 + iy_2$ належать одному класу тоді і тільки тоді, коли $z_1 - z_2 = (x_1 - x_2) + (y_1 - y_2)i \in 2Z[i]$, тобто коли обидва числа $x_1 - x_2$ та $y_1 - y_2$ є одночасно парними. Остання умова еквівалентна тому, що числа x_1 та x_2 однакової парності і числа y_1 та y_2 також однакової парності.

Таким чином, класи еквівалентності будуть наступними

$$A = \overline{0} = \overline{0 + 0i} = \{a + bi \mid a, b - \textit{парні}\},$$

$$B = \overline{1} = \overline{1 + 0i} = \{a + bi \mid a - \textit{непарне}, b - \textit{парне}\},$$

$$C = \overline{i} = \overline{0 + 1i} = \{a + bi \mid a - \textit{парне}, b - \textit{непарне}\},$$

$$D = \overline{1 + i} = \overline{1 + 1i} = \{a + bi \mid a - \textit{непарне}, b - \textit{непарне}\}.$$

Покажемо, як обчислювати елементи таблиць додавання і множення. Знайдемо суму $\overline{1 + i} + \overline{1} = \overline{(1 + i) + 1} = \overline{2 + i} = \overline{i}$. Остання рівність має місце тому що $2 + i \in B = \overline{i}$.

Знайдемо добуток $\overline{1 + i} \cdot \overline{1 + i} = \overline{(1 + i)(1 + i)} = \overline{2i} = \overline{0}$. Остання рівність має місце тому що $2i \in A = \overline{0}$. Аналогічним чином обчислюються інші елементи таблиць.

Звернемо увагу, що квадрат ненульового елементу $\overline{1 + i}$ фактор-кільця $Z[i]/J$ дорівнює нульовому елементу $\overline{0}$ цього фактор-кільця.

7. Ізоморфізми та гомоморфізми кілець.

Нехай $(K,+,\cdot)$ та $(L,\oplus,\mathbf{o})$ кільця. ***Гомоморфізмом*** називається відображення $f:K\to L$, яке зберігає операції, тобто задовільне наступним умовам:

а) $\forall x,y\in K \quad f(x+y)=f(x)\oplus f(y)$

б) $\forall x,y\in K \quad f(x\cdot y)=f(x)\mathbf{o}\, f(y)$

Ядро гомоморфізму це множина елементів кільця K, які це відображення переводить в нульовий елемент кільця M.

$$Ker\ f=\{x\in K \mid f(x)=q_M\}.$$

Образ гомоморфізму це множина елементів кільця M, які мають прообрази.

$$\operatorname{Im} f=\{y\in L \mid \exists x\in K,\ f(x)=y\}$$

Якщо $\operatorname{Im} f=L$ то гомоморфізм називають ***сюр'єктивним гомоморфізмом*** або ***епіморфізмом***.

Ізоморфізм – це бієктивний гомоморфізм. Кільця називаються ***ізоморфними***, якщо між ними можна встановити ізоморфізм. Ізоморфні кільця з точки зору алгебри однакові і відрізняються лише позначеннями. Якщо кільця K та L ізоморфні, то пишуть, що $K\cong L$.

7.1. Довести, що гомоморфізм $f:K\to L$ є ізоморфізмом тоді і тільки тоді, коли одночасно виконуються дві умови

а) $Ker\ f=\{q_K\}$

б) $\operatorname{Im} f=L$.

7.2. Нехай $A=\left\{\begin{pmatrix} a & b\\ b & a\end{pmatrix}\middle| a,b\in Z\right\}$. Довести, що відображення $f:A\to Z$, яке задається наступним чином: $f:\begin{pmatrix} a & b\\ b & a\end{pmatrix}\to a-b$ є гомоморфізмом. Знайти образ і ядро цього гомоморфізму. Чи буде цей гомоморфізм ізоморфізмом?

7.3. Довести, що відображення $f:Z[x]\to R$, $f:g(x)\to g(0)$ є гомоморфізмом. Знайти образ і ядро цього гомоморфізму.

7.4. Довести, що кільця $A=\left\{\begin{pmatrix} a & 3b \\ b & a \end{pmatrix} \middle| a,b\in Z\right\}$ та $B=\left\{a+b\sqrt{3} \middle| a,b\in Z\right\}$ ізоморфні. В якості ізоморфізму розглянути відображення $f:A\to B$, яке задається наступним чином: $f:\begin{pmatrix} a & 3b \\ b & a \end{pmatrix}\to a+b\sqrt{3}$.

7.5. Довести, що кільце цілих гаусових чисел $Z[i]=\left\{x+iy \middle| x,y\in Z, i^2=-1\right\}$ ізоморфно кільцю $A=\left\{\begin{pmatrix} a & -b \\ b & a \end{pmatrix} \middle| a,b\in Z\right\}$.

7.6. Довести, що кільця $Z/4Z$ та $Z[i]/2Z[i]$ не ізоморфні, хоча мають однакову кількість елементів.

7.7. Нехай $f:K\to L$ - гомоморфізм. Довести, що

а) $f(a-b)=f(a)-f(b)$

б) $f(0)=0$

в) $f(-a)=-f(a)$

г) $f(e_K)=e_M$. Тут e - одиничний елемент в відповідному кільці.

7.8. Довести, що ядро гомоморфізму $f:K\to L$ є ідеалом K.

7.9. Довести, що образ гомоморфізму $f:K\to L$ є підкільцем кільця L.

7.10. $f:K\to L$ - гомоморфізм. Довести, що $\operatorname{Im} f\cong K/Ker\ f$.

7.11. Покажіть на прикладі, що гомоморфний образ області цілісності не завжди є областю цілісності.

7.5. Відображення $f : Z[i] \to A$ задамо наступним природним чином: $f(x+iy)=\begin{pmatrix} x & -y \\ y & x \end{pmatrix}$. Зрозуміло, що відображення f є бієкцією між множинами $Z[i]$ та A. Перевіримо, чи зберігає воно операції множення і додавання. Позначимо $z_k = x_k + iy_x$, тоді $f(z_k)=\begin{pmatrix} x_k & -y_k \\ y_k & x_k \end{pmatrix}$.

$$f(z_1+z_2)= f((x_1+x_2)+i(y_1+y_2))=\begin{pmatrix} x_1+x_2 & -y_1-y_2 \\ y_1+y_2 & x_1+x_2 \end{pmatrix},$$

$$f(z_1)+ f(z_2)=\begin{pmatrix} x_1 & -y_1 \\ y_1 & x_1 \end{pmatrix}+\begin{pmatrix} x_2 & -y_2 \\ y_2 & x_2 \end{pmatrix}=\begin{pmatrix} x_1+x_2 & -y_1-y_2 \\ y_1+y_2 & x_1+x_2 \end{pmatrix}.$$

Як бачимо, рівність $f(z_1+z_2)= f(z_1)+ f(z_2)$ завжди виконується.

$$f(z_1z_2)= f(x_1x_2-y_1y_2+i(x_1y_2+x_2y_1))=$$

$$=\begin{pmatrix} x_1x_2-y_1y_2 & -x_1y_2-x_2y_1 \\ x_1y_2+x_2y_1 & x_1x_2-y_1y_2 \end{pmatrix},$$

$$f(z_1)f(z_2)=\begin{pmatrix} x_1 & -y_1 \\ y_1 & x_1 \end{pmatrix}\begin{pmatrix} x_2 & -y_2 \\ y_2 & x_2 \end{pmatrix}=\begin{pmatrix} x_1x_2-y_1y_2 & -x_1y_2-x_2y_1 \\ x_1y_2+x_2y_1 & x_1x_2-y_1y_2 \end{pmatrix}.$$

Як бачимо, рівність $f(z_1z_2)= f(z_1)\circ f(z_2)$ завжди виконується. Таким чином ми довели, що відображення f є ізоморфізмом, і це означає, що кільця $Z[i]$ та A ізоморфні.

7.8. Нехай $x, y\in Ker\, f$. Це означає що $f(x)= f(y)=q$, де q - нульовий елемент кільця L. Перевіримо критерій ідеалу (вправа 5.1).

За означенням гомоморфізму $f(x-y)= f(x)- f(y)=q-q=q$, отже $x-y\in Ker\, f$.

Нехай $z\in K$. За означенням гомоморфізму $f(z\cdot x)= f(z)\circ f(x)= f(z)\circ q=q$, і, аналогічно $f(x\cdot z)=q$. Таким чином $\forall z\in K$ $\forall x\in Ker\, f$ $x\cdot z\in Ker\, f$ та $z\cdot x\in Ker\, f$. Критерій двостороннього ідеалу виконується, а це означає, що ядро гомоморфізму є ідеалом.

8. Додаткові відомості про ідеали

Кільце називається ***простим***, якщо воно не містить двосторонніх ідеалів, відмінних від нульового ідеалу і самого кільця.

Ідеал називають ***максимальним***, якщо будь-який ідеал, який строго містить цій ідеал, співпадає із усім кільцем.

Ідеал комутативного кільця називається ***простим***, якщо фактор-кільце по цьому є областю цілісності.

Ідеал I комутативного кільця K називається ***примарним***, якщо з умов $ab \in J$ та $a \notin J$ випливає, що $\exists n \in N$, $b^n \in I$.

Комутативне кільце називається ***ньотеровим***, якщо всяка строго зростаюча послідовність ідеалів є скінченою.

Комутативне кільце називають ***артіновим***, якщо всяка строго спадаюча послідовність ідеалів є скінченою.

8.1. Довести, що максимальний ідеал є простим.

8.2. Довести, що фактор-кільце по максимальному ідеалу є полем. Якщо фактор-кільце по ідеалу є полем, то цей ідеал максимальний

8.3. Довести, що артіново кільце з одиницею, яке не містить ідемпотентів, відмінних від нуля та одиниці, є тілом.

8.4. Довести, що якщо $K[x]$ - ньотерово кільце, то K також ньотерово.

8.5. Довести, що кільце Z ньотерово.

8.6. Нехай K - комутативне кільце з одиницею. Радикал $\sqrt{J}$ ідеалу J задається так: $\sqrt{J} = \{a \in K, \exists n \in N, a^n \in J\}$. Довести, що якщо P - примарний ідеал, тоді $\sqrt{P}$ - найменший простий ідеал, якій містить P .

8.7. Нехай K - комутативне кільце з одиницею. Довести, що ідеал J максимален в K тоді і тільки тоді, коли фактор-кільце K/J - поле.

8.8. Довести, що поле – це просте кільце.

8.9. Довести, що ідеал $A = \left\langle x^2, 2x \right\rangle$ в кільці $Z[x]$ не є примарним.

Приклади розв'язання задач

8.5. Нехай дана строго зростаюча послідовність ідеалів в Z:

$$J_1 < J_2 < J_3 < \ldots$$

Так, як Z є кільцем головних ідеалів, то кожен з ідеалів J_k породжений одним елементом, тобто $J_k = \langle a_k \rangle$. Таким чином маємо, що $\langle a_1 \rangle < \langle a_2 \rangle < \langle a_3 \rangle < \ldots$.

Умова $\langle a \rangle < \langle b \rangle$ еквівалентна тому, що $a\mathrm{M}b$. Так як послідовність строго зростаюча, то $\langle a \rangle \neq \langle b \rangle$, а це означає, що $a \neq b$, і значить $|a| > |b|$.

Отже задана строго зростаюча послідовність ідеалів в Z $J_1 < J_2 < J_3 < \ldots$ породжує послідовність цілих чисел $a_1, a_2, a_3, \ldots$, таких що $|a_1| > |a_2| > |a_3| > \ldots$. Оскільки модуль цілого числа є невід'ємним цілим числом, то така послідовність може містити лише скінчену кількість елементів. А це означає, що в Z всяка строго зростаюча послідовність ідеалів є скінченою, а отже Z є ньотеровим.

9. Класифікація елементів в кільці.

Вважаємо, що a, b, c, p, u є ненульовими елементами КОМУТАТИВНОГО КІЛЬЦЯ З ОДИНИЦЕЮ, який є ОБЛАСТЬ ЦІЛІСНОСТІ. Говорять, що ***елемент*** b ***ділить елемент*** a (позначається $b|a$) якщо існує елемент c такий, що $a = bc$. Елемент u називають ***одиничним***, якщо від ділить одиницю кільця. Елементи a та b називають ***асоційованими***, якщо для деякого одиничного елемента u має місце рівняння $a = bu$. Неодиничний елемент p називається ***незвідним***, якщо p ділиться тільки на одиничні елементи та на елементи, які асоційовані з p. Неодиничний ненульовий елемент p називається ***простим***, якщо з того, що $p|ab$ випливає, що $p|a$ або $p|b$.

9.1. Довести, що $b|a$ тоді і тільки тоді, коли $(a) \subset (b)$.

9.2. Довести, що елемент u одиничний тоді і тільки тоді, коли $(u) = K$.

9.3. Довести, що елементи a та b асоційовані тоді і тільки тоді, коли $(a) = (b)$.

9.4. Довести, що простота елемента p еквівалентна тому факту, що якщо $ab \in (p)$, то $a \in (p)$ або $b \in (p)$.

9.5. Сформулювати в термінах ідеалів поняття незвідного елементу.

9.6. Довести, що в кільці Z має місце рівність ідеалів $(a, b) = (d)$, де $d = НОД(a, b)$. Узагальнити цей факт на кільце головних ідеалів.

9.7. Довести, що в кільці Z рівність $(a, b) = Z$ має місце тоді і тільки тоді, коли елементи a та b є взаємно-простими.

9.8. Довести, що в довільному кільці, яке є комутативною областю цілісності з одиницею, кожен простий елемент є незвідним.

9.9. Довести, що в області головних ідеалів кожен незвідний елемент є простим.

9.10. Довести, що якщо $a \neq q$ кільця K і ідеал (a) є простим в K, то елемент a є незвідним.

9.11. Довести, що відношення асоційованості елементів є відношенням еквівалентності.

9.12. Довести, що елементи 2 ,$3, 1+i\sqrt{5}, 1-i\sqrt{5}$ незвідні в кільці $K = \{a+bi\sqrt{5} \mid a,b \in Z\} = Z[\sqrt{-5}]$.

Приклади розв'язання задач

9.8. Нехай p - довільний простий елемент кільця, і p ділиться на c. Потрібно довести, що елемент c або одиничний, або асоційований з p.

Вираз p ділиться на c е означає, що існує елемент a, такий що $p = ca$, і, отже $p \mid ca$. Із простоти елемента p випливає, що $p \mid a$ або $p \mid c$.

Якщо $p \mid a$, то $a = pu$ для деякого елементу u. В цьому випадку $p = ca = puc$ (ми скористалися тим, що кільце комутативне). Отже $p - puc = p(e - uc) = 0$, і оскільки $p \neq q$, а кільце – область цілісності, то $uc = e$, а це означає, що c є одиничним елементом.

Якщо $p \mid c$, то $c = pv = cav$. Звідси робимо висновок, що $av = e$ і що a та v - одиничні елементи. Таким чином елемент p можна отримати, якщо помножити елемент c на одиничний елемент a. А це означає, що елемент c асоційований з елементом p.

9.12. Представимо елемент 2 у вигляді добутку двох елементів із кільця K: $2 = u \cdot v$. Числа $\bar{u}$ та $\bar{v}$ також належать K, і $\bar{u}\bar{v} = 2$ (риска означає комплексне спряження). Маємо, що $u\bar{u}v\bar{v} = 4$.

Для будь якого ненульового $u = x + y\sqrt{-5} \in K$ число $u\bar{u} = x^2 + 5y^2$ буде натуральним, і воно не може дорівнювати 2. З урахуванням цього факту та рівності $u\bar{u}v\bar{v} = 4$ робимо висновок, що або $u\bar{u} = 1, v\bar{v} = 4$, або $u\bar{u} = 4, v\bar{v} = 1$. В будь-якому разі один з елементів u або v буде одиничним, і інший – асоційований з елементом 2. Це означає, що елемент 2 є незвідним.

Для елементу 3 доведення аналогічне.

Якщо $1 + i\sqrt{5} = uv$, то $u\bar{u}v\bar{v} = \left(1 + i\sqrt{5}\right)\left(1 - i\sqrt{5}\right) = 6$. Число $u\bar{u} = x^2 + 5y^2$ при цілих x, y не може приймати значення 2 та 3, отже або $u\bar{u} = 1, v\bar{v} = 6$, або $u\bar{u} = 6, v\bar{v} = 1$. В будь-якому разі один з елементів u або v буде одиничним, і інший – асоційований з елементом $1 + i\sqrt{5}$. Це означає, що елемент $1 + i\sqrt{5}$ є незвідним.

Для елементу $1 - i\sqrt{5}$ доведення аналогічне.

10. Факторіальні кільця. Евклідові кільця.

Зафіксуємо множину S - набор простих (або,як синонім, незвідних) елементів кільця головних ідеалів K, який задовольняє двом умовам:

1) Кожний простий елемент із K асоційований з деяким елементом із S.

2) Ніякі два елемента із S не асоційовані між собою.

Говорять, що ненульовий елемент $a \in K$ ***однозначно розкладається на добуток незвідних множників*** якщо в K існує одиничний елемент u і елементи $p_i \in S$, $i = \overline{1,r}$, такі, що $a = u \prod_{k=1}^{r} p_k$, причому для двох таких розкладів незвідні елементи можуть розрізнятися лише порядком в добутку.

Кільце називається ***факторіальним***, якщо воно є областю цілісності і кожний ненульовий елемент єдиним образом розкладається в добуток незвідних елементів.

Кільце називають ***евклідовим***, якщо в ньому можна виконувати ділення з остачею. Точніше якщо існує така функція $d : K \setminus q \to N$, така, що $\forall a, b \in K \setminus q \quad \exists q, r \in K$, такі що $a = bq + r$ та $r = q$ або $d(r) < d(b)$.

10.1. Довести, що евклідове кільце є кільцем головних ідеалів.

10.2. Довести, що в евклідовому кільці простота елемента p еквівалентна максимальності ідеалу (p).

10.3. Довести, що кільце головних ідеалів є ньотеровим.

10.4. Довести, що кожен ненульовий елемент із кільця головних ідеалів K, який не є одиничним елементом, ділиться на незвідний елемент.

10.5. Довести, що кожен ненульовий елемент із кільця головних ідеалів K, який не є одиничним елементом, можна представити у вигляді добутку незвідних елементів

10.6. Нехай a - деякий ненульовий елемент кільця головних ідеалів K, а p - деякий простий елемент K. Довести, що існує таке $n \in N \cup \{0\}$, що $p^n \big| a$, а p^{n+1} не ділиться на a.

Будемо вважати таке n значенням функції $ord_p(a)$.

10.7. Довести, що якщо $a, b \neq 0$, то $ord_p(ab) = ord_p(a) \cdot ord_p(b)$.

10.8. Довести теорему: якщо кільце головних ідеалів є областю цілісності, то воно факторіальне.

10.9. Довести, що кільце $Z[i]$ факторіальне.

10.10. Довести, що кільце $R[x]$ факторіальне.

10.11. Довести, що кільце $Z\left[\sqrt{-5}\right]$ не факторіально.

Вказівка: Скористайтеся результатами вправи 9.12. Представте елемент 6 двома способами у вигляді незвідних елементів.

10.12. Довести, що ненульовий елемент p факторіального кільця K є простим тоді і тільки тоді, коли K/pK є областю цілісності.

Приклади розв'язання задач

10.1. Нехай I є ідеалом в евклідовому кільці K. Серед чисел $\{d(x) \mid x \in I\}$ оберемо найменше натуральне число a і знайдемо такий елемент $y \in I$, що $d(y) = a$. Доведемо, що $I = \langle a \rangle$. Оскільки $a \in I$, то включення $\langle a \rangle \subset I$ очевидно. Осталось довести, що $I \subset \langle a \rangle$.

Припустимо супротивне, що $\exists z \in I \setminus \langle a \rangle$, тобто такий елемент z із ідеалу, який не ділиться на a. Оскільки K - евклідова область, то $\exists q, r \in K$, такі що $z = qa + r$, де $0 < d(r) < d(a)$.

Елемент $z \in I$, елемент $a \in I$, і, оскільки I - ідеал, то і елемент $r = z - aq \in I$. Таким чином ми в I знайшли такий елемент z, що $0 < d(z) < d(a)$, що суперечить вибору a. Отже ідеал I є головним.

11. Кільце цілих гаусових чисел.

Раніше було доведено, що $Z[i]$ є факторіальним кільцем. В цьому розділі доводиться теорема про представлення натурального числа у вигляді суми двох квадратів цілих чисел. В цьому розділі p означатиме непарне просте число.

11.1. Довести, що можливі два випадки: або p - простий елемент в $Z[i]$, або $p=(a+ib)(a-ib)$, де a, b - прості елементи в $Z[i]$.

11.2. Довести, що елемент 2 не є простим в $Z[i]$.

11.3. Довести, що якщо p не є простим в $Z[i]$, то $p \equiv 1(\mathrm{mod}\, 4)$.

11.4.

а) Для простого числа $p=4k+1$ покладемо $t=(2k)!$.Довести, що $t \equiv \dfrac{(p-1)!}{((p-1)/2)!}(\mathrm{mod}\, p)$.

б) Довести, що $t^2+1 \equiv 0(\mathrm{mod}\, p)$.

в) Припустити, що p є простим елементом в $Z[i]$, і довести, що існують такі цілі числа a, b, що $t+i=p(a+ib)$ або $t-i=p(a+ib)$.

в) Довести, що якщо просте число $p \equiv 1(\mathrm{mod}\, 4)$, то p не є простим в $Z[i]$ і p можна представити у вигляді $p=m^2+n^2$, $m,n \in Z$.

11.5. Довести, що просте число p буде простим в $Z[i]$ тоді і тільки тоді, коли $p \equiv 3(\mathrm{mod}\, 4)$.

11.6. Нехай число t є сумою квадратів двох цілих чисел: $t=m^2+n^2$, таких що $НСД(m,n)=1$ і непарне проте число p є його дільником. Довести, що $p \equiv 1(\mathrm{mod}\, 4)$.

11.7. Довести, що натуральне число t можна представити у вигляді суми квадратів двох цілих чисел тоді і тільки тоді, коли в канонічний розклад числа t кожен простий дільник вигляду $4k+3$ входить в парному ступені.

11.8. Без посилань на попередню теорему та не використовуючи метод перебору довести, що діофантове рівняння $x^2 + y^2 = 19$ не має розв'язків.

11.9. Розглянути числа від 40 до 60. З'ясувати, які з чисел можна розкласти на суму двох квадратів та записати відповідні розклади.

11.10. Розв'язати рівняння $x^2 + y^2 = 346$ в цілих числах.

Приклади розв'язання задач

11.8. Оскільки 19 - непарне число, то одне з чисел, (наприклад x) є парним, а інше (відповідно y) є непарним. Таким чином $x = 2k$, $x^2 = 4k \equiv 0 \pmod 4$.

$$y = 2k + 1,\ y^2 = 4k^2 + 4k + 1 \equiv 1 \pmod 4.$$

$$x^2 + y^2 \equiv 0 + 1 \equiv 1 \pmod 4,$$

$$19 \equiv 3 \pmod 4.$$

Оскільки $x^2 + y^2 \not\equiv 19 \pmod 4$, то рівність $x^2 + y^2 = 19$ не може виконуватися ні при яких цілих x та y.

12. Китайська теорема об остачах.

Говорять, що елементи a,b кільця головних ідеалів K ***порівняні по ідеалу*** J якщо $a-b\in K$, Цей факт записують наступним чином $a\equiv b\,(J)$

12.1. Довести, що відношення порівнянності по фіксованому ідеалу є відношенням еквівалентності, і відповідні класи співпадають с суміжними класами відносно ідеалу.

12.2. Довести, що якщо елементи кільця є взаємно простими, тобто $(a,b)=K$, то існують такі елементи $u,v\in K$, що $au+bv=e$.

12.3. Довести, що якщо $НСД(b,a_1)=1$ та $НСД(b,a_2)=1$, то $НСД(b,a_1a_2)=1$. Узагальнити цей факт для довільного набору цілих чисел $a_1,a_2,...,a_n$.

12.4. Нехай $a_1,a_2,...,a_n$ - набір попарно взаємно простих цілих чисел. Довести, що якщо ціле число m ділиться на кожне з чисел $a_1,a_2,...,a_n$, то воно ділиться на число $a_1a_2...a_n$.

12.5. Довести китайську теорему об остачах. Нехай $m_1,m_2,...,m_k$ набор попарно взаємно простих натуральних чисел. Довести, що система порівнянь

$$\begin{cases} x\equiv a_1(\operatorname{mod} m_1), \\ x\equiv a_2(\operatorname{mod} m_2), \\ \\ x\equiv a_k(\operatorname{mod} m_k) \end{cases}$$

має розв'язок при будь-якому наборі $a_1,a_2,...,a_k$, і будь-які два розв'язки відрізняються не величину, кратну $m_1m_2...m_k$.

12.6. Узагальнити цю теорему на довільне кільце головних ідеалів.

12.7. Розв'язати системи порівнянь в кільці Z:

$$\begin{cases} x \equiv 3 \pmod 5, \\ x \equiv 2 \pmod 4, \\ x \equiv 1 \pmod 7 \end{cases} \qquad \begin{cases} x \equiv a_1 \pmod 5, \\ x \equiv a_2 \pmod 4, \\ x \equiv a_k \pmod 7 \end{cases} \qquad \begin{cases} x \equiv 0 \pmod 3, \\ x \equiv 1 \pmod 5, \\ x \equiv 3 \pmod 7 \end{cases}$$

12.8. Розв’язати системи порівнянь в кільці $R[x]$:

$$\begin{cases} f(x) \equiv 1 \pmod{x+1}, \\ f(x) \equiv 2 + x \pmod{x^2+1}, \\ f(x) \equiv x^2 - x \pmod{x^3} \end{cases} \qquad \begin{cases} f(x) \equiv 2 \pmod{x+1}, \\ f(x) \equiv 1 - x \pmod{x^2+1}, \\ f(x) \equiv x^2 + 2 \pmod{x^3+1} \end{cases}$$

Приклади розв’язання задач

12.5. Введемо в розгляд числа $M_i = \prod\limits_{\substack{j=\overline{1,k}, \\ j \neq i}} m_i$. Оскільки при $i \neq j$ $НСД(m_i, m_j) = 1$, то $НСД(m_i, M_i) = 1$. Найбільший спільний дільник чисел можна представити у вигляді лінійної комбінації цих чисел, а це означає, що $\exists u_i, v_i \in Z \quad u_i M_i + v_i m_i = 1$.

Позначимо $A_i = u_i M_i = 1 - v_i m_i$.

Установимо такі властивості:

$$A_i = 1 - v_i m_i \equiv 1 \pmod{m_i},$$

$$A_i = u_i M_i \equiv 0 \pmod{m_j} \text{ при } j \neq i,$$

які можна записати у вигляді однієї формули:

$$A_i \equiv d_{ij} \pmod{m_j}, \text{ де } d_{ij} \text{ - символ Кронекера.}$$

Розглянемо число $x = \sum\limits_{j=1}^{k} a_j A_j$ і покажемо, що воно задовільне заданій системі порівнянь: $x = \sum\limits_{j=1}^{k} a_j A_j \equiv \sum\limits_{j=1}^{k} a_j d_{ij} \equiv a_i \pmod{m_i}$.

13. Різні задачі

Характеристикою кільця K (позначають $char\,K$) називають таке натуральне число n, що для будь-якого $a\in K$ має місце рівність $\underbrace{a+a+\cdot\cdot\cdot+a}_{n\ раз}=0$. Якщо такого n не існує, то вважають характеристику кільця рівною нулю.

13.1. Навести приклад кілець, яке має характеристику 3 та 4.

13.2. Довести, що характеристика поля є або нулем, або простим числом.

13.3. Якщо K - кільце, то $K[x]$ - множина всіх многочленів від змінної x. Довести, що $K[x]$ - кільце.

13.4. В кільці $K=Z\left[\sqrt{-5}\right]=\{a+bi\,|\,a,b\in Z\}$ знайти всі оборотні елементи.

13.5. Нехай K - комутативне кільце з одиницею. Довести, що многочлен $f(x)=\sum\limits_{k=1}^{n}a_kx^k\in K[x]$ тоді і тільки тоді, коли елемент a_0 має обернений в K, а елементи $a_1,a_2,...,a_n$ - нільпотенти.

13.6. Фактор-кільце $R[x]/(f(x))$ буде полем тоді і тільки тоді, коли многочлен $f(x)$ незвідний над полем R.

13.7. Довести, що $J=\{f(x)\in Z[x]\,|\,f(x)\,\vdots\,6\ \forall x\in Z\}$ - ідеал кільця $Z[x]$. Знайти характеристику кільця $Z[x]/J$

13.8. Описати всі скінчені ненульові асоціативні комутативні кільця(можливо без одиниці), в яких добуток всіх ненульових елементів дорівнює елементу, відмінному від нуля та одиниці. (Задача з олімпіади Московського державного університету 2009р.)

13.9. Навести приклади неголовних ідеалів в кільці $R[x,y]$.

СПИСОК РЕКОМЕНДОВАНОЇ ЛІТЕРАТУРИ

1. К. Айерленд, М. Роузен. Классическое введение в современную теорию чисел. – М.: Мир, 1987
2. Б.Л. Ван дер Варден. Алгебра. - М.: Наука, 1976
3. Завало С. Т. Курс алгебры. - К.: Вища школа, 1985
4. Завало С.Т., Костарчук В.Н., Хацет Б.И. Алгебра и теория чисел. Ч.1 - К.: Вища школа, 1997; Ч.2 - К.: Вища школа, 1980
5. Кострикин А.И. Введение в алгебру. - М.: Наука, 1977
6. Кострикин А.И. Сборник задач по алгебре. М.: Наука, 1987; М.: Факториал, 1995
7. Куликов Л. Я. Алгебра и теория чисел. - М.: Высшая школа, 1979
8. Курош А.Г. Курс высшей алгебры. – М.: Наука, 1975
9. Лельчук М.П., Полевченко И.И., Радьков А.М., Чеботаревский Б.Д. Практические занятия по алгебре и теории чисел. - Минск: Вышейшая школа, 1986
10. Ленг С. Алгебра. - М.: Мир, 1968
11. Проскуряков И. В. Сборник задач по линейной алгебре. – М.: Наука, 1974
12. Фаддеев Д. К. Лекции по алгебре. - М.:Наука, 1987 Фаддеев Д. К., Соминский И. С. Сборник задач по высшей алгебре. – М.: Наука, 1977; СПб.: "Лань", 1999
13. Шнеперман Л.Б. Курс алгебры и теории чисел в задачах и упражнениях. Ч.2. - Минск: Вышейшая школа, 1987
14. Шнеперман Л.Б. Сборник задач по алгебре и теории чисел. - Минск: Вышейшая школа, 1982
15. Бородін О.І., Потьомкін Л.В., Сліпенко А.К. Основні поняття сучасної алгебри. - К.: Рад.школа, 1983
16. О.В. Мельников, В.Н. Ремесленников, В.А. Романьков и др.; Под общ. ред. Л.А. Скорнякова. Общая алгебра. Т.1. - М.: Наука, 1990
17. Скорняков Л.А. Элементы алгебры. М.: Наука, 1986 .
18. Фрид Э. Элементарное введение в абстрактную алгебру. - М.: Мир, 1979

ТЕРМІНОЛОГІЧНИЙ СЛОВНИК

Артінове кільце - комутативне кільце, в якому всяка строго спадаюча послідовність ідеалів є скінченою.

Асоціативне кільце – кільце, в якому має місце асоціативність множення.

Асоційовані елементи – два такі елементи кільця, що один із них е добутком іншого елементу на одиничний елемент.

Головний ідеал - ідеал, породжений одним елементом.

Гомоморфізм - відображення одного кільця на друге, яке зберігає операції додавання та множення.

Дільник нуля – такий ненульовий елемент кільця, для якого існує ненульовий елемент, такий що їх добуток є нульовим елементом.

Добуток ідеалів - множина, елементи якої можна записати у вигляді суми. Кожен елемент суми є добутком двох елементів, взятих з кожного з цих ідеалів.

Евклідове кільце – кільце, в якому можна виконувати ділення з остачею.

Ідеал кільця (***двосторонній ідеал)*** – підкільце яке є одночасно і лівим і правим ідеалом.

Ідемпотент - елемент кільця, квадрат якого дорівнює самому цьому елементу

Ізоморфізм –гомоморфізм, який є бієкціею.

Ізоморфні кільця - кільця між яким можна встановити ізоморфізм. Ізоморфні кільця з точки зору алгебри однакові і відрізняються лише позначеннями.

Кільце - множина, на якій задано дві бінарні алгебраїчні операції: додавання і добутку і виконуються ряд аксіом.

Комутативне кільце - кільце, в якому має місце комутативність множення

Ліва одиниця –елемент e, такий що $\forall a \quad ae = a$.

Лівий ідеал кільця - підкільце, яке має наступну властивість: добуток елементу кільця на елемент ідеалу обов'язково належить ідеалу.

Максимальний ідеал – ідеал, який має наступну властивість: будь-який ідеал, який строго містить цій ідеал, співпадає із усім кільцем.

Незвідний елемент - неодиничний елемент кільця, який ділиться тільки на одиничні елементи та на елементи, які асоційовані з ним.

Нільпотент – елемент кільця, деяка степінь котрого є нульовим елементом.

Нульовий елемент – елемент q, такий що $\forall a \quad a+q=q+a$.

Ньотерово кільце - комутативне кільце, в якому всяка строго зростаюча послідовність ідеалів є скінченою

Область цілісності – кільце, в якому немає дільників нуля.

Область головних ідеалів – кільце, в якому кожний ідеал є головним.

Образ гомоморфізму це множина елементів кільця, які мають прообрази.

Одиниця кільця –елемент e, такий що $\forall a \quad ae=ea=a$ ..

Одиничний елемент **–** елемент кільця, який ділить одиницю кільця.

Підкільце – підмножина кільця, яка сама є кільцем відносно тих же операцій.

Поле –асоціативне комутативне кільце з 1, в якому кожний ненульовий елемент має обернений.

Права одиниця –елемент e, такий що $\forall a \quad ea=a$.

Правий ідеал кільця **-** підкільце, яке має наступну властивість: добуток елементу ідеалу на елемент кільця обов'язково належить ідеалу.

Примарний ідеал - ідеал комутативного кільця, який має наступну властивість: якщо добуток двох елементів кільця належить цьому ідеалу, то деяка степінь одного з множників обов'язково належить цьому ідеалу.

Простий елемент - неодиничний ненульовий елемент, який має наступну властивість: якщо добуток двох елементів ділиться на цей елемент, то обов'язково хоча б один із дільників ділиться на цей елемент.

Простий ідеал - ідеал комутативного кільця, фактор-кільце по якому є областю цілісності.

Просте кільце – кільце, яке не містить двосторонніх ідеалів, відмінних від нульового ідеалу і самого кільця.

Радикал ідеалу – це множина всіх таких елементів кільця, які задовольняють наступній умові: деякий натуральний степінь елементу належить заданому ідеалу.

Сума ідеалів – множина, елементи якої можна записати у вигляді суми двох елементів, взятих з кожного з цих ідеалів.

Суміжний клас за ідеалом – максимальна підмножина елементів кільця, яка має наступну властивість: різниця будь яких двох елементів цієї підмножини належить заданому ідеалу.

Фактор кільце по ідеалу – кільце, елементами якого є суміжні класи за заданим ідеалом.

Факторіальне кільце – кільце, яке є областю цілісності і кожний ненульовий елемент цього кільця єдиним образом розкладається в добуток незвідних елементів.

Характеристика кільця – таке натуральне число n, що якщо будь який елемент скласти сам з собою n разів, то отримаємо нульовий елемент. Якщо такого числа не існує, то вважають, що характеристика числа дорівнює нулю.

Центр кільця – це підмножина, яка складається із всіх таких елементів, які комутують зі всіма елементами кільця.

Ядро гомоморфізму це множина елементів кільця, які це відображення переводить в нульовий елемент.

Навчальне видання

(українською мовою)

Величко Ігор Георгійович
Зінченко Андрій Іванович

Теорія кілець

Навчально-методичний посібник
для студентів IV курсу математичного факультету

Рецензент д.ф.-м.н., проф. *А.К. Приварников*
Відповідальний за випуск *І.Г. Величко*
Коректор *А.Г. Кривохата*