Міністерство освіти та науки України
Ужгородський національний університет

П. М. Гудивок,
О. А. Кирилюк, Є. Я. Погоріляк,
О. А. Тилищак, Н. В. Юрченко

ПРАКТИКУМ З АЛГЕБРИ І ТЕОРІЇ ЧИСЕЛ

Ужгород 2008

УДК 512.8

Практикум з алгебри і теорії чисел / Гудивок П. М., Кирилюк О. А., Погоріляк Є. Я., Тилищак О. А., Юрченко Н. В. – Ужгород: Видавництво УжНУ «Говерла», 2008. – 64 с.

У навчальному посібнику подано теоретичний матеріал без доведень, розв'язки типових задач, задачі для самостійного розв'язування з тем абстрактної алгебри: «Групи», «Кільця», «Поля», «Модулі», «Цілі алгебраїчні числа», «Алгебри», «Зображення скінченних груп».

Посібник призначений для студентів математичних факультетів університетів.

Рецензенти: доктор фізико-математичних наук, професор *А. А. Бовді*
кандидат фізико-математичних наук, доцент *В. П. Рудько*
кандидат фізико-математичних наук, доцент *І. В. Шапочка*

Рекомендовано до друку Редакційно-видавничою радою університету, протокол № від 2008 р.

ISBN

Зміст

Передмова

В діючій програмі курсу «Алгебра і теорія чисел» для студентів-математиків велика увага приділяється вивченню алгебраїчних структур (група, кільце, поле) і їх застосуванню в теорії чисел. Цей розділ протягом ряду років студентам математичного факультету Ужгородського національного університету автори викладали в такій послідовності: основні поняття теорії груп (група, підгрупа, фактор-група), гомоморфізми груп, циклічні групи, прямий добуток груп, скінченні абелеві групи, основні поняття теорії кілець (кільце, ідеал, поле, фактор-кільце), гомоморфізми кілець, поле відношень, кільця головних ідеалів, евклідові і факторіальні кільця, кільце класів лишків, конгруенції, алгебраїчні та скінченні розширення полів, прості розширення полів, скінченні поля, модулі, цілі алгебраїчні числа, алгебри над полем, про зображення скінченних груп над полями.

Така послідовність викладу матеріалу дає можливість застосувати теорію груп і кілець до теорії чисел.

Мета даного посібника — допомогти студентам в засвоєнні досить важкого розділу курсу алгебри «Елементи теорії груп та кілець». До кожної теми подаються теоретичний матеріал (без доведення), зразки розв'язування прикладів і вправи для самостійної роботи. В кінці розробки наводиться список рекомендованої літератури. Найбільш повно необхідний теоретичний матеріал викладений в підручнику: А. И. Кострикин «Введение в алгебру», Москва, 1977.

§1. Групи. Підгрупи

Нехай M і N — непорожні множини. Множина всіх впорядкованих пар (x, y) $(x \in M,\ y \in N)$ називається *декартовим добутком* множин M і N. Позначається цей добуток символом $M \times N$.

Бінарною алгебраїчною операцією на множині M називається відображення f множини $M \times M$ в множину M. Отже, бінарна алгебраїчна операція f на множині M — це деяке правило, за яким кожній впорядкованій парі (a, b) $(a, b \in M)$ ставиться у відповідність певний елемент $f(a, b)$ з множини M. Будемо $f(a, b)$ позначати так:

$$f(a, b) = a \cdot b = ab.$$

У такому позначенні f називається множенням, а ab — *добутком* елементів a і b. Інколи позначають $f(a, b) = a + b$. У цьому випадку f називається додаванням, а $a + b$ — *сумою* елементів a і b.

Непорожня множина G, на якій задана бінарна алгебраїчна операція множення, називається *групою*, якщо виконуються умови:

1) алгебраїчна операція асоціативна, тобто для довільних елементів a, b, $c \in G$ справедлива рівність $(ab)c = a(bc)$;
2) існує *одиничний елемент*, тобто існує такий елемент e множини G, що для довільного елемента $a \in G$ справедливі рівності: $ae = ea = a$;
3) для всякого елемента $a \in G$ існує *обернений елемент* a^{-1} із множини G, тобто такий елемент, що $aa^{-1} = a^{-1}a = e$.

Якщо для довільних елементів a, b групи G виконується рівність $ab = ba$, то група G називається *абелевою*.

Якщо множина G скінченна, то група G називається *скінченною*, а число елементів множини G називається *порядком групи* G і позначається $|G|$.

Нехай G — група, a — деякий елемент групи G. Позначимо

$$a^n = \underbrace{a \cdot a \ldots a}_{n \text{ раз}} \qquad (n \in \mathbb{N}).$$

За означенням $a^0 = e$, $a^{-n} = (a^n)^{-1}$ $(n \in \mathbb{N})$. Якщо для довільного натурального числа n $a^n \neq e$, то a називається *елементом нескінченного порядку*. Нехай n — найменше з натуральних чисел m таких, що $a^m = e$. Тоді число n називають *порядком елемента* a.

Група G називається *періодичною*, якщо кожен її елемент є елементом скінченного порядку. Група, всі елементи якої, окрім одиничного, є нескінченного порядку, називається *групою без кручення*.

Нехай G — група. Непорожня підмножина H групи G називається *підгрупою* групи G, якщо відносно алгебраїчної операції, заданої на G, H є групою.

Непорожня підмножина H групи G є підгрупою групи G тоді і тільки тоді, коли для довільних елементів a і b із H виконуються такі умови:

$$1)\ ab \in H; \qquad 2)\ a^{-1} \in H. \tag{1}$$

Нехай H — підгрупа групи G, a — фіксований елемент групи G. Позначимо через aH множину $\{ah | h \in H\}$. Підмножина $aH \subset G$ називається *лівим суміжним класом* групи G за підгрупою H, а елемент a — *представником* цього суміжного класу. Аналогічно множина $Ha = \{ha | h \in H\}$ називається *правим суміжним класом* групи G за підгрупою H. Легко перевірити, що два одноіменні (ліві або праві) суміжні класи групи G за підгрупою H або суміщаються, або не перетинаються.

Підгрупа H групи G називається *нормальною підгрупою* (позначають $H \triangleleft G$), якщо для довільного елемента $a \in G$ виконується рівність $aH = Ha$. Ця умова еквівалентна умові: $a^{-1}Ha = H$ для будь-якого елемента a групи G, де $a^{-1}Ha = \{a^{-1}ha | h \in H\}$.

Підгрупа H групи G є нормальною підгрупою тоді і тільки тоді, коли для довільного елемента a групи G

$$a^{-1}Ha \subset H. \tag{2}$$

Теорема Лагранжа. *Нехай G — скінченна група, H — підгрупа групи G. Тоді порядок підгрупи H ділить порядок групи G.*

П р и к л а д и

1. *Показати, що множина цілих раціональних чисел $\mathbb{Z}$ з операцією додавання є групою і знайти хоча б одну нескінченну підгрупу цієї групи.*

Розв'язання. Очевидно, операція додавання цілих раціональних чисел є бінарною алгебраїчною операцією на множині $\mathbb{Z}$. Добре відомо, що ця операція асоціативна: $(a + b) + c = a + (b + c)$ для довільних $a, b, c \in \mathbb{Z}$. Роль одиничного елемента буде відігравати число 0, оскільки $0 + a = a + 0 = a$ для довільного $a \in \mathbb{Z}$. Оберненим елементом до елемента $a \in \mathbb{Z}$ буде $-a \in \mathbb{Z}$, бо $a + (-a) = (-a) + a = 0$ для довільного $a \in \mathbb{Z}$. Говорять також, що $-a$ є *протилежним* елементом до елемента a. Отже, множина $\mathbb{Z}$ з операцією додавання є групою. Цю групу будемо позначати $\mathbb{Z}^+$ і називати *адитивною групою цілих чисел.*

Зауважимо, що група $\mathbb{Z}^+$ є абелевою групою, оскільки для довільних $a, b \in \mathbb{Z}^+$ виконується рівність $a + b = b + a$. Група $\mathbb{Z}^+$ — нескінченна

група без кручення, бо якщо $a \in \mathbb{Z}^+$ $(a \neq 0)$ і $n \in \mathbb{N}$, то $na \neq 0$, тобто a — елемент нескінченного порядку.

Розглянемо підмножину $(m\mathbb{Z})^+$ множини цілих чисел, що складається з чисел кратних деякому цілому числу m. Легко перевірити, що виконуються умови (1), а саме: для довільних ma, $mb \in (m\mathbb{Z})^+$

$$ma + mb = m(a + b) \in (m\mathbb{Z})^+, \quad -ma = m(-a) \in (m\mathbb{Z})^+.$$

Отже, $(m\mathbb{Z})^+$ — нескінченна підгрупа групи $\mathbb{Z}^+$.

2. *Показати, що множина всіх підстановок степеня n з операцією множення є групою, а множина всіх парних підстановок степеня n є нормальною підгрупою цієї групи.*

Розв'язання. Позначимо через S_n сукупність всіх підстановок степеня n, тобто сукупність всіх взаємно однозначних відображень множини $M = \{1, 2, \ldots, n\}$ на себе:

$$S_n = \left\{ \begin{pmatrix} 1 & 2 & \ldots & n \\ \alpha_1 & \alpha_2 & \ldots & \alpha_n \end{pmatrix} | \alpha_i \in M, i = 1, 2, \ldots, n \right\}.$$

Добутком двох підстановок φ і ψ із множини S_n називається така підстановка $\delta \in S_n$, що $\delta(u) = \varphi(\psi(u))$ $(u \in M)$. Наприклад

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}.$$

Легко перевірити, що ця операція асоціативна, а одиничним елементом є одинична підстановка (тотожне відображення). Оберненою підстановкою для підстановки

$$\begin{pmatrix} 1 & 2 & \ldots & n \\ \alpha_1 & \alpha_2 & \ldots & \alpha_n \end{pmatrix}$$

є підстановка

$$\begin{pmatrix} \alpha_1 & \alpha_2 & \ldots & \alpha_n \\ 1 & 2 & \ldots & n \end{pmatrix}.$$

Таким чином, множина S_n всіх підстановок степеня n з операцією множення є групою. Цю групу називають *симетричною групою* n-го степеня. S_n — скінченна група порядку $|S_n| = n!$.

Множина всіх парних підстановок степеня n є підгрупою групи S_n. Ця підгрупа позначається через A_n і називається *знакозмінною групою* степеня n. Очевидно, порядок підгрупи A_n при $n > 1$ дорівнює $\frac{n!}{2}$. Звідси випливає, що є точно два ліві (праві) суміжні класи A_n і B_n групи S_n за підгрупою A_n. Очевидно, B_n складається із всіх непарних підстановок

степеня n. Значить, A_n є нормальною підгрупою групи S_n. При $n = 1$ $A_n = S_n$ і також $A_n \lhd S_n$.

3. *Нехай $\mathbb{C}$ — множина всіх комплексних чисел. Показати, що множина $GL(n,\mathbb{C})$ всіх невироджених $n \times n$-матриць з комплексними елементами відносно операції множення матриць є групою. Довести, що множина $SL(n,\mathbb{C}) = \{A \in GL(n,\mathbb{C}) \mid \det A = 1\}$ є нормальною підгрупою групи $GL(n,\mathbb{C})$.*

Розв'язання. Відомо, що добуток двох невироджених комплексних $n \times n$-матриць є знову невироджена комплексна $n \times n$-матриця. Операція множення матриць асоціативна, роль одиничного елемента відіграє одинична матриця E і якщо $A \in GL(n,\mathbb{C})$, то $A^{-1} \in GL(n,\mathbb{C})$. Отже, множина $GL(n,\mathbb{C})$ з операцією множення матриць є групою. Ця група називається *повною лінійною групою* степеня n над $\mathbb{C}$. Оскільки операція множення матриць не є комутативною, то, очевидно, група $GL(n,\mathbb{C})$ $(n > 1)$ — неабелева. Зрозуміло, що група $GL(n,\mathbb{C})$ — нескінченна.

Множина $SL(n,\mathbb{C})$ є підгрупою групи $GL(n,\mathbb{C})$, що неважко показати, перевіривши умови (1). Група $SL(n,\mathbb{C})$ називається *спеціальною лінійною групою* степеня n над $\mathbb{C}$. Покажемо, що $SL(n,\mathbb{C})$ є нормальною підгрупою групи $GL(n,\mathbb{C})$. Для довільних матриць $A \in GL(n,\mathbb{C})$, $B \in SL(n,\mathbb{C})$ має місце включення $A^{-1}BA \in SL(n,\mathbb{C})$, бо

$$\det(A^{-1}BA) = \det(A^{-1}) \cdot \det B \cdot \det A = (\det A)^{-1} \cdot \det B \cdot \det A = \det B = 1.$$

Тоді на основі (2), $SL(n,\mathbb{C}) \lhd GL(n,\mathbb{C})$.

Аналогічно визначаються групи $GL(n,\mathbb{Q})$ і $GL(n,\mathbb{R})$, де $\mathbb{Q}$ — множина всіх раціональних чисел, $\mathbb{R}$ — множина всіх дійсних чисел. Групи $\mathbb{C}^* = GL(1,\mathbb{C})$, $\mathbb{R}^* = GL(1,\mathbb{R})$ і $\mathbb{Q}^* = GL(1,\mathbb{Q})$ називаються *мультиплікативними групами* відповідно комплексних, дійсних і раціональних чисел.

Вправи

1. Вияснити, які з вказаних числових множин з заданими операціями будуть групами:

а) множина всіх дійсних чисел з операцією додавання;
б) множина комплексних чисел з заданим аргументом φ відносно операції множення;
в) множина всіх додатних раціональних чисел з операцією множення;
г) множина степенів даного дійсного числа $a \neq 0$ з цілими показниками відносно операції множення;

д) множина U_n всіх комплексних коренів з одиниці фіксованого степеня n відносно операції множення;
е) множина ненульових комплексних чисел з модулями, які не перевищують фіксоване число r, відносно операції множення.

2. Перевірити, які із вказаних нижче сукупностей відображень множини $M = \{1, 2, \ldots, n\}$ в себе утворюють групу відносно множення:

а) множина всіх відображень;
б) множина всіх відображень M на M;
в) множина всіх взаємно однозначних відображень;
г) множина всіх парних перестановок;
д) множина всіх непарних перестановок;
е) множина всіх транспозицій;
є) множина $\{e, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\}$.

3. Вияснити, які із вказаних множин $n \times n$-матриць з елементами із множини $\mathbb{R}$ дійсних чисел утворюють групу:

а) множина симетричних матриць відносно операції множення;
б) множина матриць з фіксованим детермінантом d відносно операції множення;
в) множина невироджених матриць відносно операції додавання;
г) множина невироджених матриць відносно операції множення;
д) множина діагональних матриць відносно операції додавання;
е) множина діагональних матриць відносно операції множення;
є) множина ортогональних матриць відносно операції множення;
ж) множина ненульових матриць вигляду

$$\begin{pmatrix} x & y \\ -y & x \end{pmatrix} \qquad (x, y \in \mathbb{R})$$

відносно операції множення;
з) множина матриць

$$\left\{ \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \pm \begin{pmatrix} i & 0 \\ 0 & i \end{pmatrix}, \pm \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \pm \begin{pmatrix} 0 & i \\ -i & 0 \end{pmatrix} \right\}$$

$(i^2 = -1)$ відносно операції множення.

4. Знайти порядок елемента групи:

а) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix} \in S_5$, б) $-\frac{\sqrt{3}}{2} + \frac{1}{2}i \in \mathbb{C}^*$,

в) $\begin{pmatrix} 0 & i \\ 1 & 0 \end{pmatrix} \in GL(2, \mathbb{C})$, г) $\frac{1}{\sqrt{2}} - \frac{1}{\sqrt{2}}i \in \mathbb{C}^*$,

д) $\begin{pmatrix} -1 & a \\ 0 & 1 \end{pmatrix} \in GL(2, \mathbb{R})$, е) $\begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} \in GL(2, \mathbb{Q})$,

є) $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in GL(2, \mathbb{Z})$, ж) $i \in \mathbb{C}^*$.

5. Знайти всі підгрупи симетричної групи S_3. Вияснити, які з них будуть нормальними.

6. *Центром* групи G називається множина $\mathcal{Z}(G) = \{a \in G | ag = ga \ (g \in G)\}$. Довести, що центр групи G — нормальна підгрупа групи G.

7. Показати, що елементи ab та ba в довільній групі G $(a, b \in G)$ мають однакові порядки.

8. Довести, що переріз двох нормальних підгруп групи G є нормальною підгрупою групи G.

9. Нехай A і B — нормальні підгрупи групи G такі, що $A \cap B = \{e\}$. Довести, що $xy = yx$ для довільних елементів $x \in A$ та $y \in B$.

10. Нехай всі елементи групи, крім одиниці, мають порядок 2. Довести, що група абелева.

11. Нехай G — скінченна група порядку $2n$ і H — підгрупа групи G порядку n. Показати, що H — нормальна підгрупа групи G.

§2. Фактор-групи

Нехай G — довільна група. *Добутком* підмножин A і B групи G називається підмножина $A \cdot B = \{xy \,|\, x \in A,\ y \in B\}$. Розглянемо множину всіх суміжних класів групи G за нормальною підгрупою H (немає потреби говорити про ліві чи праві класи, оскільки H — нормальна підгрупа і тому ці класи суміщаються): $\{aH \,|\, a \in G\}$. Очевидно, $aH = \{a\} \cdot H$ для довільного елемента $a \in G$. Тоді $aH \cdot bH = a(Hb)H = a(bH)H = (ab)(H \cdot H) = abH$.

Отже, добутком двох суміжних класів aH і bH є суміжний клас $(ab)H$:

$$aH \cdot bH = (ab)H. \tag{1}$$

Легко перевірити, що множина $\{aH \,|\, a \in G\}$ з введеною операцією мно-

ження (1) є групою. Одиничним елементом цієї групи є суміжний клас $eH = H$ (e — одиничний елемент групи G). Оберненим елементом до суміжного класу aH є суміжний клас $a^{-1}H$. Так визначена група називається *фактор-групою* групи G за підгрупою H і позначається G/H.

Якщо G — скінченна група, то порядок фактор-групи G/H визначається за формулою $|G/H| = \frac{|G|}{|H|}$.

П р и к л а д и

1. *Знайти фактор-групу мультиплікативної групи комплексних чисел $\mathbb{C}^*$ за підгрупою $H = \{z \in \mathbb{C}^* \,|\, |z| = 1\}$.*

Розв'язання. Оскільки $\mathbb{C}^*$ — абелева група, а всяка підгрупа абелевої групи є нормальною підгрупою цієї групи, то H — нормальна підгрупа групи $\mathbb{C}^*$. Розглянемо деякий суміжний клас aH із представником $a \in$ $\in \mathbb{C}^*$. Тоді для довільного елемента $g = ah \in aH$, де $h \in H$, $|g| = |ah| =$ $= |a||h| = |a|$. З іншого боку для довільного елемента g групи $\mathbb{C}^*$ такого, що $|g| = |a|$, має місце включення $g \in aH$. Останнє випливає з того, що $|ga^{-1}| = |g||a|^{-1} = 1$. А, отже, $ga^{-1} \in H$. Таким чином, суміжний клас aH групи $\mathbb{C}^*$ за підгрупою H із представником a складається з усіх комплексних чисел, модуль яких дорівнює модулю числа a, тобто з усіх точок комплексної площини, розташованих на колі $K(0, |a|)$ з центром в точці 0 і радіусом $|a|$. Добутком суміжних класів $aH = K(0, |a|)$ і $bH =$ $= K(0, |b|)$ буде суміжний клас $abH = K(0, |ab|)$ ($a, b \in \mathbb{C}^*$). Із попередніх міркувань відразу випливає, що $aH \neq bH$ тоді і тільки тоді, коли $|a| \neq$ $\neq |b|$. Тому група $\mathbb{C}^*/H$, очевидно, нескінченна.

2. *Знайти фактор-групу адитивної групи цілих чисел $\mathbb{Z}^+$ за підгрупою $(m\mathbb{Z})^+$, де $m > 1$.*

Розв'язання. Множина $\mathbb{Z}^+/(m\mathbb{Z})^+$ складається з елементів: $\mathbb{Z}^+/(m\mathbb{Z})^+ = \{(m\mathbb{Z})^+, 1+(m\mathbb{Z})^+, \ldots, (m-1)+(m\mathbb{Z})^+\}$. Дійсно, довільне ціле число n можна представити у вигляді $n = mq + r$, де $0 \leq r < m$ (за алгоритмом ділення). Тоді

$$n + (m\mathbb{Z})^+ = (r + mq) + (m\mathbb{Z})^+ = r + (m\mathbb{Z})^+.$$

Далі, якщо $0 \leq i < j \leq m - 1$, то $j - i \notin (m\mathbb{Z})^+$, а, отже, $i + (m\mathbb{Z})^+ \neq$ $\neq j + (m\mathbb{Z})^+$. Додаються суміжні класи за таким правилом

$$(a + (m\mathbb{Z})^+) + (b + (m\mathbb{Z})^+) = (a + b) + (m\mathbb{Z})^+.$$

Таким чином, $\mathbb{Z}^+/(m\mathbb{Z})^+$ — група порядку m. Наприклад, при $m = 3$ маємо групу

$$\mathbb{Z}^+/(3\mathbb{Z})^+ = \{(3\mathbb{Z})^+, 1 + (3\mathbb{Z})^+, 2 + (3\mathbb{Z})^+\}$$

і таблиця додавання елементів цієї групи виглядає так:

$+$	$(3\mathbb{Z})^+$	$1+(3\mathbb{Z})^+$	$2+(3\mathbb{Z})^+$
$(3\mathbb{Z})^+$	$(3\mathbb{Z})^+$	$1+(3\mathbb{Z})^+$	$2+(3\mathbb{Z})^+$
$1+(3\mathbb{Z})^+$	$1+(3\mathbb{Z})^+$	$2+(3\mathbb{Z})^+$	$(3\mathbb{Z})^+$
$2+(3\mathbb{Z})^+$	$2+(3\mathbb{Z})^+$	$(3\mathbb{Z})^+$	$1+(3\mathbb{Z})^+$

Фактор-групу $\mathbb{Z}^+/(m\mathbb{Z})^+$ позначають через $\mathbb{Z}_m^+$ і називають *групою класів лишків* за модулем m.

Вправи

1. Нехай H — підгрупа групи G. Довести, що:

а) два елементи a, b групи G тоді і тільки тоді належать одному лівому суміжному класу групи G за підгрупою H, коли $a^{-1}b \in H$;
б) між елементами двох суміжних класів групи G за підгрупою H існує взаємно однозначна відповідність.

2. Знайти фактор-групу G/H у таких випадках:

а) G — мультиплікативна група комплексних коренів четвертого степеня з одиниці, H — підгрупа коренів другого степеня з одиниці;
б) $G = GL(n, \mathbb{C})$ — повна лінійна група над $\mathbb{C}$,
$H = SL(n, \mathbb{C})$ — спеціальна лінійна група над $\mathbb{C}$;
в) $G = S_n$ — симетрична група, $H = A_n$ — знакозмінна група;
г) $G = \mathbb{C}^+$ — адитивна група комплексних чисел, $H = \mathbb{R}^+$ — адитивна група дійсних чисел;
д) $G = \mathbb{C}^*$ — мультиплікативна група комплексних чисел,
$H = \mathbb{R}^*$ — мультиплікативна група дійсних чисел;
е) $G = \mathbb{R}^*$, $H = \mathbb{R}_+^*$, де $\mathbb{R}_+^*$ — мультиплікативна група додатних дійсних чисел;
є) $G = (4\mathbb{Z})^+$, $H = (12\mathbb{Z})^+$.

3. Довести, що фактор-група абелевої групи за довільною підгрупою — абелева група.

4. Довести, що у фактор-групі $\mathbb{Q}^+/\mathbb{Z}^+$ кожен елемент має скінченний порядок.

5. Нехай $\overline{S}$ — підгрупа фактор-групи G/H. Довести, що підмножина S групи G, що є об'єднанням всіх суміжних класів, які входять в $\overline{S}$, є підгрупою групи G, що містить H. Причому, якщо $\overline{S} \triangleleft G/H$, то $S \triangleleft G$.

§3. Гомоморфізми груп

Відображення f групи G_1 в групу G_2 називається *гомоморфним*, якщо для довільних елементів a і b групи G_1 справедлива рівність $f(ab) = f(a)f(b)$. Відображення f називається відображенням групи G_1 *на* групу G_2, якщо довільний елемент b групи G_2 є образом деякого елемента a групи G_1, тобто існує елемент $a \in G_1$ такий, що $f(a) = b$. Гомоморфне відображення групи G_1 на групу G_2 називається *ізоморфним*, якщо воно взаємно однозначне. Групи G_1 та G_2 називаються *ізоморфними*, якщо існує ізоморфне відображення групи G_1 на групу G_2. Це записують так: $G_1 \cong G_2$.

При гомоморфному відображенні $f : G_1 \to G_2$ образом одиничного елемента групи G_1 є одиничний елемент групи G_2, а образом оберненого елемента до елемента $a \in G_1$ — обернений до образу $f(a)$ цього елемента, тобто $f(a^{-1}) = f(a)^{-1}$ $(a \in G_1)$. Для всякої підгрупи H_1 групи G_1 образ $f(H_1) = \{f(a) \mid a \in H_1\}$ є підгрупою групи G_2. Множина $\operatorname{Im} f = f(G_1)$ називається *образом* гомоморфного відображення f.

Ядром гомоморфного відображення $f : G_1 \to G_2$ називається множина $\{a \in G_1 \mid f(a) = e_2\}$, де e_2 — одиничний елемент групи G_2. Ядро гомоморфізму f позначають через $\operatorname{Ker} f$.

Основна теорема про гомоморфізми груп. *Нехай f — гомоморфне відображення групи G_1 на групу G_2 і $H = \operatorname{Ker} f$ — ядро гомоморфного відображення f. Тоді H — нормальна підгрупа групи G_1 і фактор-група G/H ізоморфна групі G_2.*

Теорема Келі. *Нехай G — скінченна група порядку n. Тоді група G ізоморфна деякій підгрупі симетричної групи S_n.*

Ізоморфне відображення групи G на групу G називається *автоморфізмом*. Наприклад, відображення $f : g \to g^{-1}$ $(g \in G)$ є автоморфізмом абелевої групи G.

П р и к л а д и

1. *Показати, що фактор-група $GL(n, \mathbb{C})/SL(n, \mathbb{C})$ ізоморфна групі $\mathbb{C}^*$.*

Розв'язання. Побудуємо відображення $f : GL(n, \mathbb{C}) \to \mathbb{C}^*$ за таким правилом: матриці $A \in GL(n, \mathbb{C})$ поставимо у відповідність її детермінант $\det A$. Тоді

$$f(AB) = det(AB) = \det A \cdot \det B = f(A) \cdot f(B) \quad (A, B \in GL(n, \mathbb{C})).$$

Отже, f — гомоморфне відображення групи $GL(n, \mathbb{C})$ в групу $\mathbb{C}^*$. Крім того, f є відображенням на групу $\mathbb{C}^*$, оскільки для довільного елемента

$\alpha \in \mathbb{C}^*$ існує матриця, наприклад

$$A = \begin{pmatrix} \alpha & 0 & 0 & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 1 \end{pmatrix},$$

така, що $f(A) = \alpha$ і $A \in GL(n, \mathbb{C})$. Зрозуміло, що $\operatorname{Ker} f = SL(n, \mathbb{C})$. Тому із основної теореми про гомоморфізми груп випливає, що

$$GL(n, \mathbb{C})/SL(n, \mathbb{C}) \cong \mathbb{C}^*.$$

2. *Довести ізоморфізм мультиплікативної групи додатних дійсних чисел $\mathbb{R}_+^*$ та адитивної групи дійсних чисел $\mathbb{R}^+$.*

Розв'язання. Побудуємо відображення $f : \mathbb{R}_+^* \to \mathbb{R}^+$ за таким правилом: $f(a) = \lg a$ $(a \in \mathbb{R}_+^*)$. Оскільки

$$\lg(ab) = \lg a + \lg b \quad (a, b \in \mathbb{R}_+^*),$$

то відображення f є гомоморфним. Добре відомо, що логарифм задає відображення множини $\mathbb{R}_+^*$ на множину $\mathbb{R}^+$. Далі, оскільки рівняння $\lg x = 0$ має єдиний розв'язок $x = 1$, то $\operatorname{Ker} f = \{1\}$. Тому із основної теореми про гомоморфізми груп одержуємо, що $\mathbb{R}_+^*/\{1\} \cong \mathbb{R}^+$. А звідси одразу випливає, що $\mathbb{R}_+^* \cong \mathbb{R}^+$.

В п р а в и

1. Нехай C_n — група комплексних коренів степеня n з одиниці. Визначити, скільки існує гомоморфізмів груп: а) C_2 в C_4; б) C_6 в C_3; в) C_5 в C_5; г) C_3 в C_5.

2. Чи є відображення $f : \mathbb{C}^* \to \mathbb{R}^*$ гомоморфним, якщо: а) $f(z) = |z|$; б) $f(z) = 2|z|$; в) $f(z) = |z|^{-1}$; г) $f(z) = |z|^2$; д) $f(z) = 1 + |z|$; е) $f(z) = 1$ (z — довільний елемент групи $\mathbb{C}^*$).

3. Для яких груп G відображення $f : G \to G$, що задане правилом а) $f(x) = x^2$; б) $f(x) = x^{-1}$ є гомоморфним? При якій умові ці відображення є автоморфізмами групи G?

4. Довести, що в кожному з наведених випадків відображення є гомоморфним. Знайти ядро та образ цього гомоморфізма:

а) адитивна група комплексних чисел $\mathbb{C}^+$ відображена в адитивну групу дійсних чисел $\mathbb{R}^+$ так, що кожному комплексному числу записаному в алгебраїчній формі поставлений у відповідність коефіцієнт при i: $a + bi \to b$;

б) мультиплікативна група комплексних чисел $\mathbb{C}^*$ відображена в групу комплексних чисел з модулем, рівним 1, так, що кожному комплексному числу поставлено у відповідність комплексне число з тим же аргументом, але з модулем рівним 1:

$$r(\cos\varphi + i\sin\varphi) \to \cos\varphi + i\sin\varphi;$$

в) група $\mathbb{C}^*$ відображена в мультиплікативну групу додатних дійсних чисел так, що кожному комплексному числу поставлений у відповідність його модуль: $a + bi \to \sqrt{a^2 + b^2}$.

5. Довести, що групи $(5\mathbb{Z})^+$ (адитивна група цілих чисел, кратних 5) і $(2\mathbb{Z})^+$ (адитивна група цілих чисел, кратних числу 2) ізоморфні.

6. Описати всі можливі гомоморфізми групи $\mathbb{Z}^+$ в групу $\mathbb{Z}^+$.

7. Перевірити, чи будуть ізоморфними дві групи четвертого порядку: $C_4 = \{e, a, a^2, a^3 | a^4 = e\}$, $V = \{e, b, c, bc | b^2 = e, c^2 = e, bc = cb\}$.

8. Довести, що гомоморфний образ абелевої групи є абелевою групою.

9. Нехай f — гомоморфізм групи G_1 в групу G_2 заданий за правилом $f(a) = e_2$ для будь-якого елемента $a \in G_1$, де e_2 — одиниця групи G_2. Так визначений гомоморфізм називається *тривіальним*. Побудувати нетривіальний гомоморфізм групи $\mathbb{C}^*$ в групу $\mathbb{R}^*$.

10. Нехай G — група і H — нормальна підгрупа групи G. Показати, що існує група $\overline{G}$ і гомоморфізм $f : G \to \overline{G}$ такий, що $\operatorname{Ker} f = H$.

11. Довести, що для довільної групи G:

а) множина всіх автоморфізмів групи G є групою;

б) відображення $\sigma : x \to a^{-1}xa$, де a — фіксований елемент групи G є автоморфізмом групи G (внутрішнім автоморфізмом);

в) множина всіх внутрішніх автоморфізмів групи G є групою.

§4. Циклічні групи

Група G називається *циклічною* групою, якщо вона складається з степенів одного з своїх елементів a, тобто $G = \{a^n \mid n \in \mathbb{Z}\}$ (a — фіксований елемент групи G). Елемент a називається в цьому випадку *твірним елементом* групи G, а група G позначається так $G = \langle a \rangle$.

Якщо для довільних цілих чисел n та m $a^n \neq a^m$ при $n \neq m$, то група $G = \langle a \rangle$ є нескінченною циклічною групою. Прикладом нескінченної циклічної групи є адитивна група цілих чисел.

Якщо ж знайдуться різні цілі числа n та m такі, що $a^n = a^m$, то група $G = \langle a \rangle$ буде скінченною групою порядку t, де t — порядок елемента a в

групі G, тобто $G = \{e, a, a^2, \ldots, a^{t-1}\}$. Прикладом скінченної циклічної групи порядку n служить мультиплікативна група комплексних коренів n-го степеня з одиниці — всі ці корені є степенями одного з них, а саме первісного кореня.

Циклічна група має такі властивості:

1. Всяка нескінченна циклічна група G ізоморфна адитивній групі цілих чисел $\mathbb{Z}^+$.
2. Всяка циклічна група порядку n ізоморфна групі $\mathbb{Z}_n^+$.
3. Всяка підгрупа циклічної групи — циклічна.
4. Всяка підгрупа H скінченної циклічної групи $G = \langle a \rangle$ порядку n породжується елементом a^s, де s — дільник числа n, і є циклічною групою порядку t, причому $n = st$.
5. У циклічної групи порядку n є стільки підгруп, скільки є дільників у числа n.

П р и к л а д и

1. *Показати, що група простого порядку завжди циклічна.*

Розв'язання. Нехай G — група простого порядку p, e — одиничний елемент групи G. Нехай a — елемент групи G, відмінний від e. Розглянемо циклічну підгрупу групи G, породжену елементом a, тобто $H = \langle a \rangle$. За теоремою Лагранжа $|H|$ ділить p. Враховуючи, що p — просте число і те, що $H \neq \langle e \rangle$, маємо $|H| = p$. Тоді $H = G$ і, отже, G — циклічна група.

2. *Виписати всі підгрупи групи* $\mathbb{Z}_{18}^+$.

Розв'язання. Група $\mathbb{Z}_{18}^+ = \{(18\mathbb{Z})^+, 1 + (18\mathbb{Z})^+, \ldots, 17 + (18\mathbb{Z})^+\}$ є циклічною групою порядку 18. Твірним елементом цієї групи є, наприклад, $1 + (18\mathbb{Z})^+$, оскільки $n + (18\mathbb{Z})^+ = n(1 + (18\mathbb{Z})^+)$ $(n = 0, 1, \ldots, 17)$. Тоді на основі властивості 3 циклічних груп маємо, що всяка підгрупа групи $\mathbb{Z}_{18}^+$ є циклічною і їх стільки, скільки дільників у числа 18. А саме є підгрупи порядків: 1, 2, 3, 6, 9, 18. Випишемо їх:

$$G_1 = \langle (18\mathbb{Z})^+ \rangle,\ G_2 = \langle 9 + (18\mathbb{Z})^+ \rangle,\ G_3 = \langle 6 + (18\mathbb{Z})^+ \rangle,$$
$$G_6 = \langle 3 + (18\mathbb{Z})^+ \rangle,\ G_9 = \langle 2 + (18\mathbb{Z})^+ \rangle,\ G_{18} = \mathbb{Z}_{18}^+ = \langle 1 + (18\mathbb{Z})^+ \rangle.$$

Тут $|G_i| = i \quad (i = 1, 2, 3, 6, 9, 18)$.

В п р а в и

1. Довести, що задані групи є циклічними і знайти їх твірні елементи:

а) група $(n\mathbb{Z})^+$ цілих чисел, кратних даному натуральному числу n, відносно операції додавання;

б) група комплексних коренів n-го степеня з одиниці відносно операції множення;

в) група обертання правильного n-кутника.

2. Знайти порядок циклічної підгрупи групи $GL(2,\mathbb{R})$, породженої матрицею:

а) $\begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}$; б) $\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$; в) $\begin{pmatrix} \frac{1}{2} & 0 \\ 1 & \frac{1}{2} \end{pmatrix}$; г) $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$.

3. Довести, що циклічна група порядку p^n містить підгрупу порядку p^m для довільного $m \in \{0, 1\ , 2, \ldots, n\}$ (p — просте число).

4. Знайти всі підгрупи циклічної групи порядку:

а) 12; б) 15; в) 24; г) p; д) p^2; е) p^n.

5. Нехай $C_n = \langle a | a^n = e \rangle$ — циклічна група порядку n і $b = a^k$ ($k \in \mathbb{N}$). Довести, що:

а) елемент b тоді і тільки тоді буде твірним елементом групи C_n, коли n і k — взаємно прості числа;

б) порядок елемента b дорівнює $\frac{n}{d}$, де d — найбільший спільний дільник чисел k і n.

6. В циклічній групі $\langle a \rangle$ порядку n знайти всі елементи g, що задовольняють умові $g^k = e$ і всі елементи порядку k, якщо:

а) $n = 24$, $k = 6$; б) $n = 100$, $k = 20$; в) $n = 360$, $k = 7$.

7. Нехай G — скінченна група і a — елемент групи G. Довести, що $G = \langle a \rangle$ тоді і тільки тоді, коли $|G|$ дорівнює порядку елемента a.

8. Знайти фактор-групу циклічної групи G порядку n за підгрупою порядку t, якщо:

а) $n = 8$, $t = 2$; б) $n = 15$, $t = 3$; в) $n = p^2$, $t = p$ (p — просте число).

9. Довести, що група H тоді і тільки тоді є гомоморфним образом скінченної циклічної групи G, коли H також циклічна і її порядок ділить порядок групи G.

10. Нехай $G = \langle a \rangle$ — нескінченна циклічна група, H — довільна група. Довести, що для довільного елемента $b \in H$ існує одне і тільки одне гомоморфне відображення $f : G \to H$ таке, що $f(a) = b$.

11. Знайти всі гомоморфні відображення:

а) групи $C_{18} = \langle a | a^{18} = e \rangle$ в себе;

б) групи $C_{12} = \langle a | a^{12} = e \rangle$ в групу $C_{16} = \langle b | b^{16} = e \rangle$;
в) групи $C_{18} = \langle a | a^{18} = e \rangle$ на себе;
г) групи $C_{20} = \langle a | a^{20} = e \rangle$ в групу $C_{12} = \langle b | b^{12} = e \rangle$.

12. Знайти в групі $\mathbb{C}^*$ циклічні підгрупи порядку:
а) 2; б) 3; в) 4; г) n.

13. Знайти всі автоморфізми циклічної групи порядку:
а) 3; б) 4; в) 12; г) 15; д) 20.

§5. Прямий добуток груп

Нехай задано групи G_1, G_2, ..., G_n. Позначимо через G множину всіх впорядкованих n-ок вигляду $(g_1, g_2, \ldots, g_n)$, де $g_i \in G_i$ $(i = 1, 2, \ldots, n)$. Два елементи $x = (g_1, g_2, \ldots, g_n)$ і $y = (h_1, h_2, \ldots, h_n)$ групи G будемо вважати рівними тоді і тільки тоді, коли $g_i = h_i$ $(i = 1, 2, \ldots, n)$. Задамо операцію множення елементів множини G в такий спосіб:

$$x \cdot y = (g_1 h_1, g_2 h_2, \ldots, g_n h_n).$$

Легко перевірити, що тоді G — група, причому одиничним елементом групи G буде елемент $e = (e_1, e_2, \ldots, e_n)$, де e_i — одиничний елемент групи G_i $(i = 1, 2, \ldots, n)$. Оберненим до елемента x буде елемент $x^{-1} = (g_1^{-1}, g_2^{-1}, \ldots, g_n^{-1})$. Так визначена група G називається *зовнішнім прямим добутком* груп G_1, G_2, ..., G_n. Позначатимемо зовнішній добуток груп G_1, G_2, ..., G_n так: $G = G_1 \dot{\times} G_2 \dot{\times} \cdots \dot{\times} G_n$.

Якщо групи G_1, G_2, ..., G_n задані адитивно, то в цьому випадку групу G називають *зовнішньою прямою сумою* груп G_1, G_2, ..., G_n і позначають так: $G = G_1 \dot{+} G_2 \dot{+} \cdots \dot{+} G_n$.

Нехай G — група і G_1, G_2, ..., G_n — підгрупи групи G $(n \geq 2)$. Будемо говорити, що G є *внутрішнім прямим добутком n підгруп* G_1, G_2, ..., G_n, якщо виконуються такі умови:

1) $G_i \triangleleft G$ $(i = 1, 2, \ldots, n)$;
2) $G = G_1 \cdot G_2 \ldots G_n$;
3) $(G_1 \cdot G_2 \ldots G_i) \cap G_{i+1} = \{e\}$ $(i = 1, 2, \ldots, n-1)$.

Позначають внутрішній прямий добуток груп G_1, G_2, ..., G_n так: $G = G_1 \times G_2 \times \cdots \times G_n$.

Якщо група G задано адитивно, то кажуть, що група G є *внутрішньою прямою сумою підгруп* G_1, G_2, ..., G_n і позначають $G = G_1 \oplus G_2 \oplus \oplus \cdots \oplus G_n$.

Теорема. *Група G є внутрішнім прямим добутком підгруп G_1, G_2, ..., G_n тоді і тільки тоді, коли виконуються такі умови:* 1) $a_i a_j = a_j a_i$

($a_i \in G_i$, $a_j \in G_j$, $i \neq j$; $i, j = 1, \ldots, n$); 2) *кожний елемент* a *групи* G *однозначно представляється у вигляді* $a = a_1 a_2 \ldots a_n$ ($a_i \in G_i$; $i = 1, 2, \ldots, n$).

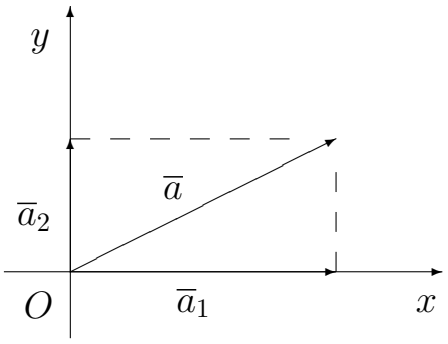
Нехай $G = G_1 \dot{\times} G_2$ — зовнішній прямий добуток груп G_1 та G_2. Розглянемо такі підгрупи групи G:

$$\overline{G}_1 = \{(g_1, e_2) | g_1 \in G_1\}, \qquad \overline{G}_2 = \{(e_1, g_2) | g_2 \in G_2\},$$

де e_i — одиничний елемент групи G_i ($i = 1, 2$). Неважко показати тоді за означенням внутрішнього прямого добутку підгруп, що $G = \overline{G}_1 \times \overline{G}_2$, тобто G є внутрішнім прямим добутком підгруп $\overline{G}_1$ та $\overline{G}_2$. При цьому група $\overline{G}_1$ ізоморфна групі G_1, а група $\overline{G}_2$ — групі G_2.

П р и к л а д и

1. *Нехай* G *— група векторів на площині відносно операції додавання,* G_1 *— підгрупа векторів, що лежать на осі* Ox*;* G_2 *— підгрупа векторів, що лежать на осі* Oy*. Показати, що* $G = G_1 \oplus G_2$.



Мал. 1

Розв'язання. Добре відомо, що для довільних векторів $\overline{a}_1 \in G_1$ і $\overline{a}_2 \in G_2$ справедлива рівність $\overline{a}_1 + \overline{a}_2 = \overline{a}_2 + \overline{a}_1$. Крім того, всякий вектор $\overline{a}$ однозначно розкладається в суму векторів з підгруп G_1 та G_2: $\overline{a} = \overline{a}_1 + \overline{a}_2$, де $\overline{a}_1$ — проекція вектора $\overline{a}$ на вісь Ox, а $\overline{a}_2$ — проекція вектора $\overline{a}$ на вісь Oy. Отже, з теореми 1 випливає, що $G = G_1 \oplus G_2$.

2. *Довести, що група* $G = \mathbb{Z}_p^+ \dot{+} \mathbb{Z}_p^+$ *не є циклічною групою* (p *— просте число*).

Розв'язання. За означенням зовнішньої прямої суми груп всякий елемент групи G є парою (a, b), де $a, b \in \mathbb{Z}_p^+$. Доведемо, що G не є циклічною групою методом від супротивного. Тобто, припустимо протилежне, що G — циклічна група і (a_0, b_0) — твірний елемент цієї групи. Тоді порядок цього елемента дорівнює порядку групи і, отже, дорівнює p^2. З іншого боку $p(a_0, b_0) = (pa_0, pb_0) = (0, 0)$. Одержане протиріччя доводить розглядуване твердження.

3. *Нехай* $G = G_1 \times G_2$ *— прямий розклад групи* G*. Довести, що фактор-група* G/G_1 *ізоморфна групі* G_2.

Розв'язання. На основі теореми 1 довільний елемент a групи G однозначно розкладається у добуток $a = a_1 a_2$ ($a_1 \in G_1$, $a_2 \in G_2$). Побудуємо

відображення $f : G \to G_2$ за таким правилом: $f(a) = a_2$. Це відображення є гомоморфним, бо для довільних елементів a, $b \in G$

$$f(ab) = f([a_1a_2][b_1b_2]) = f([a_1b_1][a_2b_2]) = a_2b_2 = f(a)f(b),$$

де $b = b_1b_2$ ($b_1 \in G_1$, $b_2 \in G_2$). Відображення f є відображенням «на», оскільки довільний елемент a групи G_2 є образом елемента a групи G. Далі, неважко показати, що $\operatorname{Ker} f = G_1$. За основною теоремою про гомоморфізми груп одержуємо, що $G/G_1 \cong G_2$.

В п р а в и

1. Знайти порядок групи $\mathbb{Z}_m^+ \dot{+} \mathbb{Z}_n^+$.

2. Нехай G_i — скінченна група порядку n_i ($i = 1, 2$). Знайти порядок групи $G = G_1 \dot{\times} G_2$.

3. Довести, що зовнішній прямий добуток двох абелевих груп є абелева група.

4. Чи будуть групи а) $\mathbb{Z}_2^+ \dot{+} \mathbb{Z}_3^+$; б) $\mathbb{Z}_2^+ \dot{+} \mathbb{Z}_4^+$; в) $\mathbb{Z}_9^+ \dot{+} \mathbb{Z}_6^+$; г) $\mathbb{Z}_m^+ \dot{+} \mathbb{Z}_n^+$ циклічними?

5. Довести, що група векторів n-вимірного дійсного лінійного простору відносно операції додавання є прямою сумою n підгруп векторів одновимірних підпросторів.

6. Довести, що адитивна група комплексних чисел $\mathbb{C}^+$ є прямою сумою підгруп дійсних і уявних чисел.

7. Довести, що мультиплікативна група дійсних чисел є прямим добутком підгруп додатних чисел і чисел, за модулем рівних одиниці.

8. Нехай G — група. Підгрупи $\{e\}$ та G, де e — одиниця групи G, називаються *тривіальним підгрупами* групи G. Довести, що групи $\mathbb{Z}^+$ та $\mathbb{Q}^+$ не розкладаються в пряму суму нетривіальних підгруп.

9. Нехай A — *прямий множник* групи G, тобто існує така підгрупа B групи G, що $G = A \times B$. Довести, що всяка нормальна підгрупа C підгрупи A буде нормальною підгрупою і в групі G.

§6. Абелеві групи

Група G називається *абелевою* (*комутативною*), якщо для довільних елементів a і b групи G справедлива рівність $ab = ba$. Нехай P — множина всіх елементів скінченного порядку абелевої групи G. Множина P є підгрупою групи G і ця група називається *періодичною частиною* групи G.

Група H називається *p-групою* (p — просте число), якщо порядок кожного елемента групи H є степенем числа p. Якщо H — скінченна p-група, то її порядок дорівнює p^n для деякого $n \in \mathbb{N} \cup \{0\}$.

Лема 1. *Скінченна циклічна p-група не розкладається в прямий добуток нетривіальних циклічних підгруп.*

Теорема 1. *Нехай G — скінченна абелева p-група порядку $|G| > 1$. Тоді група G однозначно з точністю до ізоморфізму розкладається в прямий добуток циклічних p-підгруп.*

Однозначний розклад з точністю до ізоморфізму означає наступне: нехай

$$G = G_1 \times G_2 \times \cdots \times G_q \quad (|G_i| > 1,\ i = 1, \ldots, q), \tag{1}$$

$$G = \overline{G}_1 \times \overline{G}_2 \times \cdots \times \overline{G}_r \quad (|\overline{G}_j| > 1,\ j = 1, \ldots, r) \tag{2}$$

— два розклади абелевої p-групи в прямий добуток циклічних p-підгруп; тоді $q = r$ і $G_i \cong \overline{G}_{\sigma(i)}$ $(i = 1, \ldots, q)$ для деякої підстановки $\sigma \in S_q$.

Нехай далі має місце розклад (1), де G_i — циклічна група порядку $|G_i| = p^{n_i}$ $(i = 1, 2, \ldots, q)$. Тоді

$$|G| = |G_1| \cdot |G_2| \ldots |G_q| = p^{n_1} \cdot p^{n_2} \ldots p^{n_q} = p^{n_1 + n_2 + \cdots + n_q}.$$

Числа p^{n_1}, p^{n_2}, …, p^{n_q} називаються *інваріантами групи G*. У випадку, коли має місце розклад (1), говорять, що G є *абелевою p-групою типу* $(p^{n_1}, p^{n_2}, \ldots, p^{n_q})$.

Скінченна абелева p-група однозначно з точністю до ізоморфізму визначається своїми інваріантами. Число всіх неізоморфних абелевих p-груп порядку p^m $(m \in \mathbb{N})$ дорівнює числу різних розкладів числа m в суму такого вигляду:

$$m = n_1 + n_2 + \cdots + n_q \qquad (n_1 \geq n_2 \geq \ldots \geq n_q \geq 1;\ q \in \mathbb{N}). \tag{3}$$

Розкладу (3) відповідає абелева p-група типу $(p^{n_1}, p^{n_2}, \ldots, p^{n_q})$. Різним розкладам вигляду (3) відповідають неізоморфні абелеві p-групи порядку p^m.

Теорема 2. *Нехай G — скінченна абелева група порядку $n = p_1^{s_1} p_2^{s_2} \cdots p_r^{s_r}$ (p_1, p_2, …, p_r — попарно різні прості числа, $s_i \in \mathbb{N}$; $i = 1, 2, \ldots, r$). Тоді має місце розклад $G = G_1 \times G_2 \times \cdots \times G_r$, де G_i — абелева p_i-підгрупа порядку $p_i^{s_i}$ $(i = 1, \ldots, r)$.*

Теорема 3 (Основна теорема про скінченні абелеві групи)**.** *Нехай G — скінченна абелева група порядку $n = p_1^{s_1} p_2^{s_2} \ldots p_r^{s_r}$ (p_1, p_2, …, p_r — попарно різні прості числа, $s_i \in \mathbb{N}$; $i = 1, \ldots, r$). Тоді G однозначно з*

точністю до ізоморфізму розкладається в прямий добуток циклічних p_i-підгруп ($i \in \{1, \ldots, r\}$).

Нехай m_i — число неізоморфних абелевих груп порядку $p_i^{s_i}$ ($i = 1, \ldots, r$), тоді число всіх неізомофних груп порядку $n = p_1^{s_1} \ldots p_r^{s_r}$ дорівнює $m_1 \ldots m_r$.

П р и к л а д и

1. *Виписати з точністю до ізоморфізму всі абелеві 2-групи порядку 8.*

Розв'язання. Оскільки $8 = 2^3$, то для знаходження всіх неізоморфних абелевих 2-груп порядку 2^3 потрібно знайти всі різні розклади числа 3 у суму вигляду (3). Очевидно,

$$3 = 3, \qquad 3 = 2 + 1, \qquad 3 = 1 + 1 + 1$$

— всі необхідні нам розклади. Таким чином, існує три неізоморфні абелеві 2-групи порядку 8, а саме

$$\begin{aligned} 3 = 3 &\to G_1 = \langle a_1 \rangle \quad (a_1^{2^3} = e); \\ 3 = 2 + 1 &\to G_2 = \langle a_2 \rangle \times \langle b_2 \rangle \quad (a_2^{2^2} = e,\ b_2^2 = e); \\ 3 = 1 + 1 + 1 &\to G_3 = \langle a_3 \rangle \times \langle b_3 \rangle \times \langle c_3 \rangle \quad (a_3^2 = e,\ b_3^2 = e,\ c_3^2 = e). \end{aligned}$$

2. *Виписати всі з точністю до ізоморфізму абелеві групи порядку 12.*

Розв'язання. Нехай G — абелева група порядку 12. Оскільки $12 = 2^2 \cdot 3$, то $G = H_1 \times H_2$, де H_1 — абелева група порядку $2^2 = 4$, а H_2 — абелева група порядку 3. Оскільки неізоморфних абелевих груп четвертого порядку є дві:

$$H_1^{(1)} = \langle a \rangle \quad (a^4 = e); \qquad H_1^{(2)} = \langle b \rangle \times \langle c \rangle \quad (a^2 = e,\ c^2 = e),$$

а неізоморфних абелевих груп третього порядку є одна $H_2 = \langle d \rangle$ $(d^3 = e)$, то є дві неізоморфні абелеві групи порядку дванадцять, а саме

$$G_1 = \langle a \rangle \times \langle d \rangle \quad (a^4 = e,\ d^3 = e);$$

$$G_2 = \langle b \rangle \times \langle c \rangle \times \langle d \rangle \quad (b^2 = e,\ c^2 = e,\ d^3 = e).$$

3. *Виявнити, чи ізоморфні групи $G_1 = \mathbb{Z}_{12}^+ \dot{+} \mathbb{Z}_{72}^+$ та $G_2 = \mathbb{Z}_{18}^+ \dot{+} \mathbb{Z}_{48}^+$?*

Розв'язання. Нехай $m = p_1^{k_1} \cdot p_2^{k_2}$, де p_1, p_2 — різні прості числа. Тоді за теоремою 3 група $\mathbb{Z}_m^+$ ізоморфна групі $\mathbb{Z}_{m_1}^+ \dot{+} \mathbb{Z}_{m_2}^+$, де $m_i = p_i^{k_i}$ $(i = 1, 2)$. Оскільки $\mathbb{Z}_m^+$ — циклічна група, то $\mathbb{Z}_{m_i}^+$ — циклічна p_i-підгрупа групи $\mathbb{Z}_m^+$

($i = 1, 2$). Тому кожна з груп $\mathbb{Z}_{m_i}^+$ ($i = 1, 2$) далі не розкладається в пряму суму. Тоді

$$\mathbb{Z}_{12}^+ \cong \mathbb{Z}_3^+ \dot{+} \mathbb{Z}_4^+, \quad \mathbb{Z}_{72}^+ \cong \mathbb{Z}_8^+ \dot{+} \mathbb{Z}_9^+, \quad \mathbb{Z}_{18}^+ \cong \mathbb{Z}_2^+ \dot{+} \mathbb{Z}_9^+, \quad \mathbb{Z}_{48}^+ \cong \mathbb{Z}_3^+ \dot{+} \mathbb{Z}_{16}^+.$$

Остаточний розклад груп G_1 та G_2 такий:

$$G_1 \cong \mathbb{Z}_3^+ \dot{+} \mathbb{Z}_4^+ \dot{+} \mathbb{Z}_8^+ \dot{+} \mathbb{Z}_9^+, \quad G_2 \cong \mathbb{Z}_2^+ \dot{+} \mathbb{Z}_9^+ \dot{+} \mathbb{Z}_3^+ \dot{+} \mathbb{Z}_{16}^+.$$

Отже, в силу теореми 3 ці групи не ізоморфні.

В п р а в и

1. Знайти періодичну частину групи $\mathbb{R}^*$.

2. Знайти фактор-групу групи $\mathbb{Q}^*$ за її періодичною частиною.

3. Розкласти циклічну групу порядку m у прямий добуток своїх підгруп, якщо: а) $m = 30$; б) $m = 27$; в) $m = 72$; г) $m = 125$.

4. Скільки є неізоморфних абелевих груп прядку: а) 16; б) 108?

5. Описати з точністю до ізоморфізму всі абелеві групи порядків: а) 4; б) 15; в) 36; г) 100; д) 72.

6. Чи ізоморфні групи:

а) $G_1 = \mathbb{Z}_{12}^+ \dot{+} \mathbb{Z}_{20}^+$, $G_2 = \mathbb{Z}_{16}^+ \dot{+} \mathbb{Z}_{15}^+$, $G_3 = \mathbb{Z}_4^+ \dot{+} \mathbb{Z}_{60}^+$;

б) $H_1 = C_{10} \dot{\times} C_{15} \dot{\times} C_{14}$, $H_2 = C_{25} \dot{\times} C_4 \dot{\times} C_{21}$, $H_3 = C_6 \dot{\times} C_{35} \dot{\times} C_{10}$?

Чи є серед них циклічні групи?

7. Довести, що скінченна абелева група порядку n, де n не ділиться на квадрат цілого числа більшого за одиницю, є циклічною.

8. Нехай A, B, C — скінченні абелеві групи і $A \dot{+} C \cong B \dot{+} C$. Довести, що $A \cong B$.

9. Довести, що група порядку p^2 (p — просте число) є абелевою.

10. Скільки підгруп

а) порядків 2 і 6 в нециклічній абелевій групі порядку 12;

б) порядків 3 і 6 в нециклічній абелевій групі порядку 18?

§7. Кільця. Ідеали

Непорожня множина K, на якій задані дві бінарні алгебраїчні операції (будемо їх називати додаванням і множенням), називається *кільцем* (асоціативним), якщо виконуються такі умови:

1) множина K відносно операції додавання є абелевою групою;
2) для довільних елементів a, b, $c \in K$ справедлива рівність $(ab)c = a(bc)$;
3) для довільних елементів a, b, $c \in K$ справедливі рівності $a(b+c) = ab + ac$, $(a+b)c = ac + bc$.

Множини $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ відносно звичайних операцій додавання і множення є кільцями.

Кільце K називається *комутативним*, якщо $ab = ba$ для довільних елементів a, $b \in K$. Очевидно, кільця $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ — комутативні. Прикладом некомутативного кільця є кільце квадратних $n \times n$-матриць з елементами з комутативного кільця P ($n > 1$, $P \neq \{0\}$). Будемо позначати це кільце через $P_{n\times n}$.

Нехай $K \neq \{0\}$. Якщо існує такий елемент $e \in K$, що $ae = ea = a$ для всякого $a \in K$, то елемент e називається *одиничним елементом* або *одиницею* кільця K. У цьому випадку говорять, що K — *кільце з одиницею*. Кільця $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ — це кільця з одиницею. Прикладом кільця без одиниці є кільце $2\mathbb{Z}$ цілих парних чисел.

Нехай K — кільце з одиницею e. Елемент $a \in K$ називається *оборотним*, якщо існує такий елемент $b \in K$, що $ab = ba = e$. Тоді елемент b позначають через a^{-1} і називають *оберненим* до елемента a. Множина всіх оборотних елементів кільця K відносно операції множення утворює групу, яка називається *мультиплікативною групою кільця* K. Будемо позначати її через K^*.

Комутативне кільце з одиницею називають *полем*, якщо $K^* = K \setminus \{0\}$. Прикладом полів є кільця $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$. Кільце $\mathbb{Z}$ не є полем, оскільки $\mathbb{Z}^* = \{-1, 1\} \neq \mathbb{Z} \setminus \{0\}$.

Елементи a, $b \in K$ називаються *дільниками нуля* у кільці K, якщо $a \neq 0$, $b \neq 0$, а $ab = 0$. Якщо у комутативному кільці K немає дільників нуля, то таке кільце називається *областю цілісності*. Прикладом області цілісності є кільце $\mathbb{Z}$, а також довільне поле. Наведемо приклади дільників нуля у кільці $P_{2\times 2}$, де P — комутативне кільце з одиницею. Нехай

$$a = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \qquad b = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}.$$

Очевидно, $a \neq 0$ і $b \neq 0$, а їх добуток $ab = 0$.

Непорожня підмножина $S \subset K$ називається *підкільцем* кільця K, якщо відносно операцій додавання і множення, заданих в K, множина S є кільцем. Так, $\mathbb{Z}$ — підкільце кілець $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$; $\mathbb{Q}$ — підкільце кілець $\mathbb{R}$, $\mathbb{C}$; $\mathbb{R}$ — підкільце кільця $\mathbb{C}$.

Підкільце V комутативного кільця K називається *ідеалом* кільця K, якщо для довільних елементів $a \in K$ та $u \in V$ добуток au є елементом підкільця V, тобто $au \in V$.

Непорожня підмножина S комутативного кільця K є ідеалом кільця K тоді і тільки тоді, коли виконуються умови:

1) для довільних елементів a, $b \in S$ різниця $a - b$ є елементом підмножини S, тобто $a - b \in S$;
2) для довільних елементів $a \in K$, $b \in S$ добуток ab є елементом підмножини S, тобто $ab \in S$.

П р и к л а д и

1. *Нехай p — деяке просте число. Раціональне число $\frac{m}{n}$ називається p-цілим, якщо його знаменник n взаємно простий з p. Довести, що множина I_p всіх p-цілих чисел утворює кільце відносно операцій додавання і множення раціональних чисел. Знайти мультиплікативну групу цього кільця.*

Розв'язання. Сума і добуток двох раціональних чисел $\frac{m_1}{n_1}$ та $\frac{m_2}{n_2}$, що належать множині I_p, є знову раціональним числом, що міститься в I_p, бо добуток $n_1 n_2$ не ділиться на p. Очевидно, $0 \in I_p$ та для довільного числа $\frac{m}{n} \in I_p$ протилежне до нього число $-\frac{m}{n}$ також міститься в I_p. Умови асоціативності для операцій додавання та множення, умови комутативності для операцій додавання та множення і умови дистрибутивності виконуються для елементів із I_p, бо I_p — підмножина поля $\mathbb{Q}$. Отже, I_p — комутативне кільце. Очевидно, I_p — кільце з одиницею. Проте I_p не є полем, бо, наприклад, число p не є оборотним в кільці I_p.

Мультиплікативною групою кільця I_p є підмножина $A = \{\frac{m}{n} \in I_p | m \neq \neq 0,\ (m, p) = 1\}$. Дійсно, для довільного числа $\frac{m}{n} \in A$ число $\frac{n}{m}$ міститься в I_p і є оберненим до нього. З іншого боку, якщо $\frac{m}{n} \in I_p^*$, то $\left(\frac{m}{n}\right)^{-1} = \frac{n}{m} \in \in I_p$, і тому $(m, p) = 1$.

2. *Показати, що множина $m\mathbb{Z}$ всіх цілих чисел, кратних фіксованому натуральному числу m, є ідеалом кільця $\mathbb{Z}$.*

Розв'язання. Оскільки $m\mathbb{Z} \subset \mathbb{Z}$, то досить показати, що різниця двох довільних елементів із $m\mathbb{Z}$ є також елементом із $m\mathbb{Z}$ і, що добуток довільного елемента кільця $\mathbb{Z}$ на елемент із $m\mathbb{Z}$ є елементом із $m\mathbb{Z}$. Ці умови виконуються, оскільки для довільних елементів $mz_i \in m\mathbb{Z}$ $(i = = 1, 2)$ і $z \in \mathbb{Z}$

$$mz_1 - mz_2 = m(z_1 - z_2) \in m\mathbb{Z}, \qquad z(mz_1) = m(zz_1) \in m\mathbb{Z}.$$

Отже, $m\mathbb{Z}$ — ідеал кільця $\mathbb{Z}$.

3. *Нехай $\mathbb{C}[x]$ — множина всіх многочленів від однієї невідомої x з комплексними коефіцієнтами. Показати, що $\mathbb{C}[x]$ є кільцем відносно операції додавання і множення многочленів. Довести, що множина всіх многочленів, вільний член яких дорівнює нулеві, є ідеалом кільця $\mathbb{C}[x]$.*

Розв'язання. Нехай

$$f(x) = a_n x^n + \cdots + a_1 x + a_0 \quad (a_i \in \mathbb{C};\ i = 0, 1, \ldots, n;\ n \in \mathbb{N} \cup \{0\}),$$

$$g(x) = b_m x^m + \cdots + b_1 x + b_0 \quad (b_j \in \mathbb{C};\ j = 0, 1, \ldots, m;\ m \in \mathbb{N} \cup \{0\})$$

— довільні многочлени із $\mathbb{C}[x]$ відповідно степенів n і m. Припустимо, не зменшуючи загальності, що $n \geq m$. Тоді за означеннями суми та добутку многочленів

$$f(x) + g(x) = c_n x^n + \cdots + c_1 x + c_0 \in \mathbb{C}[x],$$

$$f(x)g(x) = d_{n+m} x^{n+m} + \cdots + d_1 x + d_0 \in \mathbb{C}[x],$$

де $c_i = a_i + b_i$ $(i = 0, \ldots, n;\ b_j = 0,\ j = m+1, \ldots, n)$, а $d_k = \sum_{i+j=k} a_i b_j$ $(k = 0, \ldots, n+m)$. Отже, додавання та множення многочленів є бінарними алгебраїчними операціями.

Використовуючи добре відомі властивості дій додавання і множення многочленів, неважко показати, що відносно цих операцій $\mathbb{C}[x]$ є комутативним кільцем з одиницею. Роль одиниці відіграє многочлен $f(x) = 1$.

Множина всіх многочленів із $\mathbb{C}[x]$, вільний член яких дорівнює нулеві, суміщаються з множиною $x\mathbb{C}[x]$ тих многочленів, які діляться на x. Якщо многочлени $f_1(x)$ та $f_2(x)$ діляться на x, то і їх різниця $f_1(x) - f_2(x)$ ділиться на x; якщо многочлен $f(x) \in \mathbb{C}[x]$ ділиться на x, а $g(x)$ — довільний многочлен із $\mathbb{C}[x]$, то добуток $f(x)g(x)$ також ділиться на x. Отже, $x\mathbb{C}[x]$ — ідеал кільця $\mathbb{C}[x]$.

В п р а в и

1. Вияснити, які з вказаних множин будуть кільцями (полями):

а) множина $\mathbb{Z}[i] = \{a + bi \in \mathbb{C} \mid a, b \in \mathbb{Z}\}$ *цілих гаусових чисел* відносно звичайних операцій додавання і множення комплексних чисел;

б) множина многочленів з дійсними коефіцієнтами відносно звичайних операцій додавання і множення многочленів;

в) множина $\mathbb{Z}[\sqrt{p}] = \{a + b\sqrt{p} \in \mathbb{R} \mid a, b \in \mathbb{Z}\}$ відносно звичайних операцій додавання і множення дійсних чисел;

г) множина $C_{[-1;1]}$ всіх неперервних на відрізку $[-1;\ 1]$ функцій $f : [-1,\ 1] \to \mathbb{R}$ відносно звичайних операцій додавання і множення функцій;

д) множина дійсних ортогональних матриць порядку n відносно операцій додавання і множення матриць;

е) множина дійсних матриць порядку $n \geq 2$, у яких два останні рядки — нульові, відносно операцій додавання і множення матриць;

є) множина дійсних симетричних матриць порядку n відносно операцій додавання і множення матриць.

2. Нехай n — дане натуральне число. Раціональне число називається *n-цілим*, якщо його знаменник взаємно простий з n. Довести, що множина n-цілих чисел є підкільцем кільця $\mathbb{Q}$.

3. Показати, що в кільці з одиницею існує тільки одна одиниця.

4. Показати, що якщо кільце містить не більше трьох елементів, то воно комутативне.

5. Довести, що скінченна область цілісності з одиницею є полем.

6. Довести комутативність довільного кільця, в якому кожний елемент x задовольняє рівнянню $x^2 = x$.

7. Нехай a — дільник нуля в кільці K з одиницею. Довести, що $a \notin K^*$.

8. Довести, що в кільці $\mathbb{C}[x]$ немає дільників нуля.

9. Навести приклади дільників нуля в кільці матриць третього порядку над полем раціональних чисел.

10. Перевірити, чи буде множина V ідеалом в кільці K, якщо:

а) $K = \mathbb{R}[x]$, $V = \mathbb{R}[x^3]$;

б) $K = \mathbb{R}[x]$, $V = x^3\mathbb{R}[x] = \{x^3 f(x) \mid f(x) \in \mathbb{R}[x]\}$;

в) $K = \mathbb{Z}[x]$, V — множина многочленів, у яких старший коефіцієнт ділиться на 2;

г) $K = \mathbb{Z}[i]$, $V = 2K$.

11. Вияснити, чи будуть наведені множини підкільцями або ідеалами у вказаних кільцях:

а) множина $\mathbb{Z}$ у кільці $\mathbb{Z}[x]$ цілочислових многочленів;

б) множина $\mathbb{N}$ у кільці $\mathbb{Z}$;

в) множина $\mathbb{Z}$ у кільці $\mathbb{Z}[i]$;

г) множина $T = \{x(1+i) \mid x \in \mathbb{Z}[i]\}$ у кільці $\mathbb{Z}[i]$;

д) множина $\mathbb{Z}[x]$ у кільці $\mathbb{Q}[x]$.

12. Довести, що перетин двох ідеалів комутативного кільця є ідеалом цього кільця.

13. Показати, що в полі є тільки *тривіальні ідеали* (тобто нульовий і саме поле).

14. Нехай K — комутативне кільце з одиницею 1 і V — ідеал в K. Довести, що $V = K$ тоді і тільки тоді, коли $1 \in V$.

§8. Фактор-кільця

Нехай K — комутативне кільце, V — ідеал кільця K. Нехай a деякий елемент кільця K. Множина $a+V = \{a+v \,|\, v \in V\}$ називається *суміжним класом* кільця K за ідеалом V або *класом лишків за модулем* V, а елемент a — *представником* цього суміжного класу. Перетворимо множину $K/V = \{a + V \mid a \in K\}$ всіх суміжних класів кільця K за ідеалом V у кільце, покладаючи

$$(a + V) + (b + V) = (a + b) + V \quad (a + V,\ b + B \in K/V),$$

$$(a + V)(b + V) = ab + V \quad (a + V,\ b + B \in K/V).$$

Легко показати, що сума і добуток суміжних класів не залежить від вибору представників суміжних класів. Множина K/V відносно визначених операцій додавання та множення суміжних класів є кільцем. Це кільце називається *фактор-кільцем* кільця K за ідеалом V. Нулем кільця K/V є суміжний клас $V = 0 + V$. Кільце $\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z}$ ($m \in \mathbb{N}$) називається *кільцем класів лишків за модулем* m.

П р и к л а д и

1. *Нехай m — довільне натуральне число. Знайти елементи кільця $\mathbb{Z}_m$ класів лишків за модулем m. Показати, що коли m не є простим числом, то $\mathbb{Z}_m$ не є полем.*

Розв'язання. Нагадаємо, що фактор-група $\mathbb{Z}^+/(m\mathbb{Z})^+$ складається з таких елементів: $(m\mathbb{Z})^+$, $1+(m\mathbb{Z})^+$, $\ldots$, $(m-1)+(m\mathbb{Z})^+$. Отже, фактор-кільце $\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z}$ складається із таких m елементів:

$$\mathbb{Z}_m = \{m\mathbb{Z},\ 1 + m\mathbb{Z},\ 2 + m\mathbb{Z},\ \ldots,\ (m-1) + m\mathbb{Z}\}.$$

Очевидно,

$$(a + m\mathbb{Z}) + (b + m\mathbb{Z}) = c + m\mathbb{Z},$$

$$(a + m\mathbb{Z})(b + m\mathbb{Z}) = d + m\mathbb{Z},$$

де c, d — відповідно остача від ділення $a + b$ та ab на m (a, $b \in \{0, 1, 2, \ldots, m-1\}$). Одиницею кільця $\mathbb{Z}_m$ є суміжний клас $1 + m\mathbb{Z}$.

Якщо m — непросте число, тоді кільце $\mathbb{Z}_m$ не є полем, оскільки містить дільники нуля, які, як відомо, не є оборотними елементами. Дійсно, нехай $m = m_1 \cdot m_2$ ($m_i \in \mathbb{N}$, $m_i > 1$; $i = 1, 2$). Тоді $m_i + m\mathbb{Z} \neq m\mathbb{Z}$ ($i = 1, 2$) і

$$(m_1 + m\mathbb{Z})(m_2 + m\mathbb{Z}) = m_1 \cdot m_2 + m\mathbb{Z} = m\mathbb{Z}.$$

2. *Показати, що фактор-кільце* $\mathbb{C}[x]/x\mathbb{C}[x]$ *є полем.*

Розв'язання. Оскільки будь-який многочлен $f(x) \in \mathbb{C}[x]$ однозначно представляється у вигляді $f(x) = xg(x) + a$ ($g(x) \in \mathbb{C}[x]$, $a \in \mathbb{C}$), то $f(x) + x\mathbb{C}[x] = a + x\mathbb{C}[x]$. Тому

$$\mathbb{C}[x]/x\mathbb{C}[x] = \{a + x\mathbb{C}[x] \mid a \in \mathbb{C}\},$$

причому, очевидно,

$$(a + x\mathbb{C}[x]) + (b + x\mathbb{C}[x]) = (a + b) + x\mathbb{C}[x],$$

$$(a + x\mathbb{C}[x])(b + x\mathbb{C}[x]) = ab + x\mathbb{C}[x]$$

для довільних елементів a, $b \in \mathbb{C}$. Одиницею кільця $\mathbb{C}[x]/x\mathbb{C}[x]$ є суміжний клас $1 + x\mathbb{C}[x]$. А елемент $a^{-1} + x\mathbb{C}[x]$ є оберненим до ненульового елемента $a + x\mathbb{C}[x]$. Таким чином, фактор-кільце $\mathbb{C}[x]/x\mathbb{C}[x]$ є полем.

В п р а в и

1. Нехай K — комутативне кільце з одиницею 1 і V — ідеал цього кільця. Показати, що фактор-кільце K/V також має одиницю.

2. Знайти всі елементи фактор-кілець: а) $\mathbb{Z}_5$; б) $\mathbb{Z}_6$; в) $\mathbb{R}[x]/x\mathbb{R}[x]$; г)$\mathbb{R}[x]/(x+1)\mathbb{R}[x]$; д) $\mathbb{Z}[i]/2\mathbb{Z}[i]$.

3. Знайти суміжні класи кільця $\mathbb{R}[x]$ за ідеалом $V = (x^2 - 1)\mathbb{R}[x]$. Чи буде фактор-кільце $\mathbb{R}[x]/V$ містити дільники нуля?

4. Ненульовий елемент u кільця K називається *нільпотентним*, якщо $u^n = 0$ для деякого натурального числа n. Показати, що кільце $\mathbb{Z}_m$ класів лишків за модулем $m \in \mathbb{N}$ містить нільпотентні елементи тільки тоді, коли m ділиться на квадрат натурального числа більшого за одиницю.

5. Довести, що фактор-кільце $\mathbb{Z}[i]/3\mathbb{Z}[i]$ є полем з дев'яти елементів.

6. Довести, що фактор-кільце $\mathbb{Z}[i]/2\mathbb{Z}[i]$ не є полем.

§9. Гомоморфізми кілець

Нехай задано кільця K і K'. Відображення $f : K \to K'$ називається *гомоморфним*, якщо для довільних елементів a і b кільця K виконуються такі дві умови:

1) $f(a+b) = f(a) + f(b)$;
2) $f(ab) = f(a)f(b)$.

Відображення кільця K на кільце K' називається *ізоморфним*, якщо воно гомоморфне і взаємно однозначне. Кільця K та K' називаються *ізоморфними*, якщо існує ізоморфне відображення кільця K на кільце K'. Це записують так: $K \cong K'$. Ізоморфне відображення кільця K на кільце K називається *автоморфізмом*.

Ядром гомоморфного відображення f кільця K в кільце K' називається множина $\{a \in K \mid f(a) = 0'\}$, де $0'$ — нуль кільця K'. Ядро гомоморфізму f позначають через $\operatorname{Ker} f$.

Основна теорема про гомоморфізми кілець. *Нехай K та K' — комутативні кільця і f — гомоморфне відображення кільця K на кільце K'. Тоді ядро $\operatorname{Ker} f$ гомоморфного відображення f є ідеалом кільця K і фактор-кільце $K/\operatorname{Ker} f$ ізоморфне кільцю K'.*

П р и к л а д и

1. *Показати, що відображення $f : \mathbb{Z} \to \mathbb{Z}_m$, визначене за правилом $f(a) = a + m\mathbb{Z}$ $(a \in \mathbb{Z})$, є гомоморфним відображенням кільця $\mathbb{Z}$ на кільце $\mathbb{Z}_m$.*

Розв'язання. Очевидно, для довільних елементів a, $b \in \mathbb{Z}$

$$f(a+b) = (a+b) + m\mathbb{Z} = (a + m\mathbb{Z}) + (b + m\mathbb{Z}) = f(a) + f(b),$$

$$f(ab) = ab + m\mathbb{Z} = (a + m\mathbb{Z})(b + m\mathbb{Z}) = f(a)f(b).$$

Таким чином, відображення f є гомоморфним.

Відображення f є відображенням «на», оскільки довільний суміжний клас $a + m\mathbb{Z} \in \mathbb{Z}_m$ є образом елемента $a \in \mathbb{Z}$.

2. *Описати всі автоморфізми кільця $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ цілих гаусових чисел.*

Розв'язання. Нехай f — довільний автоморфізм кільця $\mathbb{Z}[i]$. Тоді f є гомоморфне відображення кільця $\mathbb{Z}[i]$ на кільце $\mathbb{Z}[i]$ і за властивостями гомоморфізму кілець $f(0) = 0$ і $f(1) = 1$, $f(-l) = -f(l)$, де 0 та 1 — відповідно нуль та одиниця кільця $\mathbb{Z}[i]$, l — довільний елемент кільця $\mathbb{Z}[i]$. Більше того, для довільного натурального числа m $f(m) = m$. Дійсно,

$$f(m) = f(m \cdot 1) = f(\underbrace{1 + 1 + \cdots + 1}_{m \text{ раз}}) =$$

$$= \underbrace{f(1) + f(1) + \cdots + f(1)}_{m \text{ раз}} = m \cdot f(1) = m \cdot 1 = m.$$

Тому і для довільного цілого числа n $f(n) = n$.

Тоді образом довільного елемента $a+bi$ $(a, b \in \mathbb{Z})$ кільця $\mathbb{Z}[i]$ є елемент

$$f(a + bi) = f(a) + f(bi) = f(a) + f(b)f(i) = a + bf(i).$$

Таким чином, для знаходження образу довільного елемента кільця $\mathbb{Z}[i]$ досить знати образ елемента i цього кільця. Оскільки $i^2 = -1$, то

$$-1 = f(-1) = f(i^2) = f(i)^2.$$

Звідси $f(i) = \pm i$. Отже, всякий автоморфізм f кільця $\mathbb{Z}[i]$ повинен задовольняти або умові $f(a+bi) = a+bi$ $(a,\ b \in \mathbb{Z})$, або умові $f(a+bi) = a-bi$ $(a,\ b \in \mathbb{Z})$. З іншого боку відображення $f_1 : \mathbb{Z}[i] \to \mathbb{Z}[i]$, що задається за правилом $f_1(a + bi) = a + bi$ $(a,\ b \in \mathbb{Z})$, є тотожнім відображенням і, очевидно, є автоморфізмом кільця $\mathbb{Z}[i]$. Неважко перевірити, що і відображення $f_2 : \mathbb{Z}[i] \to \mathbb{Z}[i]$, що задається за правилом $f_2(a + bi) = a - bi$ $(a,\ b \in \mathbb{Z})$ також є автоморфізмом кільця $\mathbb{Z}[i]$.

Таким чином, всі автоморфізми кільця $\mathbb{Z}[i]$ вичерпуються двома відображеннями: тотожнім відображенням f_1, а також відображенням $f_2 : a + bi \to a - bi$ $(a,\ b \in \mathbb{Z})$.

Вправи

1. Чи буде відображення $f : x \to 2x$ гомоморфним відображенням кільця $\mathbb{Z}$ в кільце $\mathbb{Z}$?

2. Чи буде відображення $\varphi : \mathbb{R}[x] \to \mathbb{R}$, що задається за правилом $\varphi(g(x)) = g(0)$ $(g(x) \in \mathbb{R}[x])$, гомоморфним відображенням кільця $K = \mathbb{R}[x]$ в поле $\mathbb{R}$? Якщо буде, то знайти ядро $\operatorname{Ker}\varphi$ та *образ* $\operatorname{Im}\varphi = \varphi(K) = \{\varphi(a) \mid a \in K\}$ цього гомоморфного відображення.

3. Нехай K_1 та K_2 — кільця з одиницею. Довести, що при гомоморфному відображенні кільця K_1 на кільце K_2 одиничний елемент кільця K_1 відображається в одиничний елемент кільця K_2, а мультиплікативна група K_1^* відображається в мультиплікативну групу K_2^*.

4. Нехай K — довільне кільце з одиницею e. Довести, що відображення $\varphi : \mathbb{Z} \to K$, для якого $\varphi(n) = ne$ $(n \in \mathbb{Z})$, є гомоморфним відображенням кільця $\mathbb{Z}$ в кільце K. Знайти образ цього гомоморфного відображення.

5. Нехай

$$A = \left\{ \begin{pmatrix} a & b \\ 2b & a \end{pmatrix} \mid a, b \in \mathbb{Q} \right\}, \qquad \mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}.$$

Показати, що A та $\mathbb{Q}(\sqrt{2})$ є підкільцями відповідно кілець $\mathbb{Q}_{2\times 2}$ та $\mathbb{R}$. Довести, що кільця A та $\mathbb{Q}(\sqrt{2})$ — ізоморфні. Перевірити, чи є полем кільце $\mathbb{Q}(\sqrt{2})$.

6. Чи будуть ізоморфними кільця $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$ та $\mathbb{Z}[\sqrt{3}] = \{m + n\sqrt{3} \mid m, n \in \mathbb{Z}\}$?

7. Знайти всі автоморфізми поля $\mathbb{C}$ комплексних чисел, що залишають незмінними дійсні числа, тобто такі автоморфізми φ поля $\mathbb{C}$, що для всіх $a \in \mathbb{R}$ $\varphi(a) = a$.

8. Чи можна поле $\mathbb{Q}$ раціональних чисел гомоморфно відобразити а) на кільце $\mathbb{Z}$ цілих чисел; б) в кільце $\mathbb{Z}$ цілих чисел?

9. Описати всі *ендоморфізми* (гомоморфізми в себе) а) кільця $\mathbb{Z}$ цілих чисел; б) поля $\mathbb{Q}$ раціональних чисел.

10. Довести, що при гомоморфному відображенні f кільця K_1 на кільце K_2 образом ідеала V_1 кільця K_1 є деякий ідеал V_2 кільця K_2.

§10. Поля. Поле відношень

Нехай P — поле, e — одиниця поля P. Якщо $ne \neq 0$ для довільного натурального числа n, тоді кажуть, що поле P має *характеристику нуль*. Припустимо, що існує натуральне число m таке, що $me = 0$. Тоді найменше натуральне число p таке, що $pe = 0$, називається *характеристикою поля* P. Характеристика поля або дорівнює нулю, або є простим числом.

Нехай K — область цілісності з одиницею 1. Позначимо через K' множину всіх таких впорядкованих пар (a, b) $(a, b \in K)$, що $b \neq 0$:

$$K' = \{(a, b) \mid a, b \in K;\ b \neq 0\}.$$

Пари (a, b) та (c, d) будемо вважати еквівалентними, якщо $ad = bc$. Множина K' розбивається на класи еквівалентних пар, які між собою не перетинаються. Позначимо через $\frac{a}{b}$ клас еквівалентних пар із представником (a, b). Множину всіх таких класів позначимо через $\widetilde{K}$. Очевидно, $\frac{a}{b} = \frac{c}{d}$ тоді і тільки тоді, коли $ad = bc$. Задамо на множині $\widetilde{K}$ операції додавання та множення:

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}, \quad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd} \quad \left(\frac{a}{b},\ \frac{c}{d} \in \widetilde{K}\right).$$

Відносно заданих операцій множина $\widetilde{K}$ є полем. Нульом поля $\widetilde{K}$ є елемент $\frac{0}{1}$, а одиницею — елемент $\frac{1}{1}$. Оберненим до ненульового елемента $\frac{a}{b}$ є елемент $\frac{b}{a}$. Так визначене поле $\widetilde{K}$ називається *полем відношень* (*полем*

часток) кільця K. Множина $\{\frac{a}{1} | a \in K\}$ є підкільцем поля $\widetilde{K}$, яке ізоморфне кільцю K. Очевидно, поле $\mathbb{Q}$ раціональних чисел є полем відношень кільця $\mathbb{Z}$ цілих чисел.

П р и к л а д и

1. *Показати, що кільце $\mathbb{Z}_p$ класів лишків за модулем p, де p — просте число, є полем характеристики p.*

Розв'язання. Покажемо спочатку, що $\mathbb{Z}_p$ є полем. Оскільки $\mathbb{Z}_p$ є комутативним кільцем з одиницею $e = 1 + p\mathbb{Z}$, то досить показати, що для всякого ненульового елемента $s + p\mathbb{Z}$ ($s \in \{1, 2, \ldots, p-1\}$) в $\mathbb{Z}_p$ знайдеться обернений елемент. Так як $(s, p) = 1$, то в кільці $\mathbb{Z}$ існують такі елементи u і v, що $us + vp = 1$. Тоді

$$1 + p\mathbb{Z} = (us + vp) + p\mathbb{Z} = us + p\mathbb{Z} = (u + p\mathbb{Z})(s + p\mathbb{Z}).$$

Тобто елемент $u + p\mathbb{Z}$ є оберненим до елемента $s + p\mathbb{Z}$. Отже, $\mathbb{Z}_p$ — поле.

Оскільки $p(1 + p\mathbb{Z}) = p\mathbb{Z}$ (нагадаємо, що суміжний клас $p\mathbb{Z}$ є нульовим елементом поля $\mathbb{Z}_p$) і p — найменше серед натуральних чисел, що задовольняють цій умові, то характеристика поля $\mathbb{Z}_p$ дорівнює p.

2. *Розв'язати систему рівнянь*

$$\begin{cases} x + \overline{2}z = \overline{1}, \\ y + \overline{2}z = \overline{2}, \\ \overline{2}x + z = \overline{1} \end{cases}$$

в полі $\mathbb{Z}_5$ ($\overline{a} = a + 5\mathbb{Z}$, $a \in \mathbb{Z}$).

Розв'язання. Додавши до третього рівняння перше рівняння системи, помножене на $\overline{3}$, одержимо систему

$$\begin{cases} x + \overline{2}z = \overline{1}, \\ y + \overline{2}z = \overline{2}, \\ \overline{2}z = \overline{4}. \end{cases}$$

Визначивши з останнього рівняння отриманої системи невідому z і підставивши її значення у перші два рівняння системи, отримаємо

$$\begin{cases} x = \overline{1} - \overline{4} = \overline{-3} = \overline{2}, \\ y = \overline{2} - \overline{4} = \overline{-2} = \overline{3}, \\ z = \overline{2}. \end{cases}$$

Отже, $(\overline{2}, \overline{3}, \overline{2})$ є розв'язком даної в умові завдання системи.

В п р а в и

1. Нехай p — просте число, P — поле характеристики p. Довести, що для довільних елементів x, $y \in P$

$$(x+y)^{p^m} = x^{p^m} + y^{p^m} \qquad (m \in \mathbb{N}).$$

2. Знайти всі розв'язки рівняння $x^p - 1 = 0$ в полі характеристики $p > 0$.

3. Розв'язати систему рівнянь

$$\begin{cases} x + \overline{2}z = \overline{1}, \\ y + \overline{2}z = \overline{2}, \\ \overline{2}x + z = \overline{1} \end{cases}$$

в полі $\mathbb{Z}_3$ ($\overline{a} = a + 3\mathbb{Z}$, $a \in \mathbb{Z}$).

4. Розв'язати систему рівнянь

$$\begin{cases} \overline{3}x + y + \overline{2}z = \overline{1}, \\ x + \overline{2}y + \overline{3}z = \overline{1}, \\ \overline{4}x + \overline{3}y + \overline{2}z = \overline{1} \end{cases}$$

в полі $\mathbb{Z}_5$ ($\overline{a} = a + 5\mathbb{Z}$, $a \in \mathbb{Z}$).

5. Знайти всі автоморфізми поля $\mathbb{Q}(\sqrt{2})$.

6. Знайти поле відношень кільця а) $\mathbb{R}[x]$, б) $\mathbb{Z}[\sqrt{2}]$, в) $\mathbb{Z}[x]$.

7. Нехай F_1, F_2 — поля відношень областей цілісності K_1, K_2 відповідно. Довести, що довільний ізоморфізм $\varphi : K_1 \to K_2$ продовжується, причому єдино можливим способом, до ізоморфізму $\psi : F_1 \to F_2$.

8. Довести, що поля $\mathbb{Q}$ та $\mathbb{R}$ не мають автоморфізмів, відмінних від тотожнього.

§11. Кільця головних ідеалів. Евклідові кільця

Нехай K — комутативне кільце з одиницею, M — довільна підмножина кільця K. Очевидно, множина всіх елементів вигляду $x_1m_1 + x_2m_2 + \dots + x_sm_s$ ($x_i \in K$, $m_i \in M$; $i = 1, \dots, s$) утворює ідеал кільця K, який позначають через $\langle M \rangle$ і називають ідеалом кільця K, *породженим* множиною M. Якщо M — скінченна множина і $M = \{u_1, \dots, u_n\}$, то $\langle M \rangle$ записують у вигляді $\langle u_1, \dots, u_n \rangle$. Якщо множина M складається з одного елемента a, то в цьому випадку ідеал $I = \langle a \rangle$ називається *головним* ідеалом кільця K. Тоді $I = \{xa \mid x \in K\} = Ka$.

Комутативне кільце K з одиницею, в якому кожен ідеал головний, будемо називати *кільцем головних ідеалів*, а область цілісності з одиницею, в якій кожен ідеал головний, — *областю головних ідеалів*.

Нехай K — область цілісності з одиницею. Кільце K називається *евклідовим*, якщо існує таке відображення $\delta : K \setminus \{0\} \to \mathbb{N} \cup \{0\}$, яке задовольняє умовам:

1) для довільних ненульових елементів a, $b \in K$ $\delta(ab) \geq \delta(a)$;
2) для довільних елементів a, $b \in K$ $(a \neq 0)$ існують такі елементи q, $r \in K$, що $b = aq + r$, де $r = 0$ або $\delta(r) < \delta(a)$.

Теорема 1. *Всяке евклідове кільце є областю головних ідеалів.*

П р и к л а д и

1. *Показати, що кільце $\mathbb{Z}$ — евклідове.*

Розв'язання. Розглянемо відображення $\delta : \mathbb{Z} \setminus \{0\} \to \mathbb{N} \cup \{0\}$, що визначається за правилом $\delta(m) = |m|$ $(m \in \mathbb{Z})$. Тоді

$$\delta(mn) = |mn| = |m| \cdot |n| \geq |m| = \delta(m) \qquad (m, n \in \mathbb{Z} \setminus \{0\}).$$

За алгоритмом ділення в $\mathbb{Z}$ для довільних елементів m, $n \in \mathbb{Z}$ $(n \neq 0)$ існують елементи q, $r \in \mathbb{Z}$ такі, що $m = nq + r$, $0 \leqslant r < |b|$. Зрозуміло, що $r = 0$ або $\delta(r) = |r| < |n| = \delta(n)$. Отже, $\mathbb{Z}$ — евклідове кільце.

2. *Показати, що $\mathbb{Z}[i]$ є евклідовим кільцем.*

Розв'язання. Очевидно, $\mathbb{Z}[i]$ є областю цілісності з одиницею. Визначимо відображення $\delta : \mathbb{Z}[i] \setminus \{0\} \to \mathbb{N} \cup \{0\}$ в такий спосіб:

$$\delta(a) = |a|^2 = m^2 + n^2 \qquad (a = m + ni;\ m, n \in \mathbb{Z}).$$

Тоді $\delta(ab) = |ab|^2 = |a|^2|b|^2 = \delta(a)\delta(b) \geq \delta(a)$ $(a, b \in \mathbb{Z}[i] \setminus \{0\})$. Таким чином, умова 1) із означення евклідового кільця виконується.

Нехай $a = m + ni$, $b = s + ti \in \mathbb{Z}[i]$ $(m, n, s, t \in \mathbb{Z})$ і $b \neq 0$. Тоді a, $b \in \mathbb{C}$ і

$$\frac{a}{b} = \frac{m + ni}{s + ti} = \frac{ms + nt}{s^2 + t^2} + \frac{ns - mt}{s^2 + t^2} i = m_1 + n_1 i \qquad (m_1, n_1 \in \mathbb{Q}).$$

Візьмемо найближчі до m_1, n_1 цілі числа відповідно m' і n' такі, що $m_1 = m' + r_1$, $n_1 = n' + r_2$ $(|r_1| \leq \frac{1}{2}$, $|r_2| \leq \frac{1}{2})$. Тоді

$$a = b[(m' + r_1) + (n' + r_2)i] = bq + r,$$

де $q = m' + n'i$, а $r = b(r_1 + r_2 i)$. Очевидно, $q \in \mathbb{Z}[i]$. Звідси випливає, що і $r = a - bq \in \mathbb{Z}[i]$. Нарешті, якщо $r \neq 0$, то

$$\delta(r) = |r|^2 = |b|^2 |r_1^2 + r_2^2| \leq \delta(b) \left(\frac{1}{4} + \frac{1}{4} \right) = \frac{1}{2} \delta(b) < \delta(b).$$

Таким чином, $\delta(r) < \delta(b)$ при $r \neq 0$. Отже, і властивість 2) із означення евклідового кільця виконується. Тобто $\mathbb{Z}[i]$ — евклідове кільце.

В п р а в и

1. Знайти всі елементи головного ідеалу $\langle a \rangle$ кільця K, якщо:
а) $K = \mathbb{Z}_{12}$, $a = 10 + 12\mathbb{Z}$; б) $K = \mathbb{Z}_{10}$; $a = 5 + 10\mathbb{Z}$.

2. Знайти фактор-кільце кільця K за головним ідеалом, породженим елементом a, якщо: а) $K = \mathbb{Z}_{12}$, $a = 10 + 12\mathbb{Z}$; б) $K = \mathbb{Z}_{24}$, $a = 15 + 24\mathbb{Z}$; в) $K = \mathbb{R}[x]$, $a = x^2 - 1$; г) $K = \mathbb{Z}[i]$, $a = 2$; д) $K = \mathbb{R}[x]$, $a = x$. Які з одержаних фактор-кілець будуть містити дільники нуля?

3. В кільці $\mathbb{Z}$ задані ідеали $2\mathbb{Z}$ та $3\mathbb{Z}$. Знайти $2\mathbb{Z} \cap 3\mathbb{Z}$, $2\mathbb{Z} + 3\mathbb{Z}$ та $(2\mathbb{Z})(3\mathbb{Z})$.

4. Показати, що $m\mathbb{Z} + n\mathbb{Z} = \text{НСД}(m, n)\mathbb{Z}$; $m\mathbb{Z} \cap n\mathbb{Z} = \text{НСК}(m, n)\mathbb{Z}$.

5. Нехай K — комутативне кільце з одиницею. Довести, що головний ідеал $V = \langle a \rangle$ $(a \in K)$ кільця K тоді і тільки тоді відмінний від K, коли a — необоротний елемент в K.

6. Нехай K — область цілісності з одиницею. Довести, що ідеали $V = \langle a \rangle$ і $U = \langle b \rangle$ кільця K тоді і тільки тоді суміщаються, коли $a = b\varepsilon$, де $\varepsilon \in K^*$.

7. В кільці $\mathbb{Z}$ знайти ідеал, породжений елементами 2 і 3.

8. Довести, що якщо в комутативному кільці K з одиницею немає нетривіальних ідеалів, то K є полем.

9. Фактор-кільце K/I комутативного кільця K з одиницею за ідеалом I є полем тоді і тільки тоді, коли ідеал I є *максимальний*, тобто $I \neq K$ і не існує ідеалу V кільця K, $I \subset V$, $I \neq V$, $V \neq K$.

10. Показати, що ідеал $V = \langle 2, x \rangle$ не є головним ідеалом кільця $\mathbb{Z}[x]$.

11. Показати, що кільце $P[x]$ поліномів від однієї невідомої x над довільним полем P є евклідовим кільцем.

12. Довести, що кільце I_p p-цілих раціональних чисел є евклідовим кільцем.

13. Нехай K — область цілісності з одиницею, L — підкільце кільця K, що містить одиницю кільця K. Які з тверджень істинні:

а) якщо K — область головних ідеалів, то L — область головних ідеалів;

б) якщо K — евклідове кільце, то L — евклідове кільце?

§12. Факторіальні кільця

Нехай K — область цілісності з одиницею, K^* — мультиплікативна група кільця K. Нехай a — деякий ненульовий і необоротний елемент кільця K, тобто $a \neq 0$ і $a \notin K^*$. Елемент a називається *простим*, якщо його не можна представити у вигляді добутку двох необортних елементів кільця K, тобто $a \neq bc$ (b, $c \notin K^*$). В протилежному випадку елемент a називається *непростим*.

Теорема 1. *Нехай K — область головних ідеалів, a — ненульовий елемент кільця K. Фактор-кільце $K/\langle a\rangle$ є полем тоді і тільки тоді, коли a — простий елемент.*

Будемо говорити, що в області цілісності з одиницею K має місце розклад на прості множники, якщо довільний ненульовий та необоротний елемент $a \in K$ представляється у вигляді добутку простих елементів, тобто $a = a_1 a_2 \dots a_t$ (a_i — простий елемент кільця K; $i = 1, \dots, t$). Кажуть, що в кільці K має місце однозначний розклад на прості множники, якщо:

1) в кільці K має місце розклад на прості множники;
2) для будь-яких двох представлень елемента $u \in K$ у вигляді добутку простих елементів кільця K, тобто $u = a_1 a_2 \dots a_t$ і $u = b_1 b_2 \dots b_s$ (a_i, b_j — прості елементи кільця K, $i = 1, \dots, t$; $j = 1, \dots, s$), $t = s$, $a_i = b_{\sigma(i)}\varepsilon_i$ для деякої підстановки σ степеня t і оборотного елемента $\varepsilon_i \in K^*$ ($i = 1, \dots, t$).

Область цілісності з одиницею, в якій має місце однозначний розклад на прості множники, називається *факторіальним кільцем*.

Теорема 2. *Всяка область головних ідеалів є факторіальним кільцем.*

Нехай E — клас евклідових кілець, Γ — клас областей головних ідеалів, Φ — клас факторіальних кілець. Тоді $E \subset \Gamma \subset \Phi$ (можна показати, що включення строгі).

Прикладом факторіального кільця, що не є областю головних ідеалів, є кільце $F[x, y]$ поліномів від двох невідомих x і y над полем F.

П р и к л а д и

1. *З'ясувати, чи фактор-кільце $\mathbb{R}[x]/(x^2+1)\mathbb{R}[x]$ є полем.*

Розв'язання. Поліном $\psi(x) = x^2 + 1$ є незвідним поліномом над полем дійсних чисел $\mathbb{R}$, а, отже, є простим елементом кільця $\mathbb{R}[x]$. За теоремою 1 задане фактор-кільце є полем.

2. *Показати, що кільце $\mathbb{Z}[\sqrt{-3}]$ не є факторіальним.*

Розв'язання. Знайдемо спочатку мультиплікативну групу K^* кільця $K = \mathbb{Z}[\sqrt{-3}]$. Нехай $u = a + b\sqrt{-3} \in \mathbb{Z}[\sqrt{-3}]$ $(a, b \in \mathbb{Z})$. Позначимо $N(u) = u \cdot \overline{u}$, де $\overline{u} = a - b\sqrt{-3}$. Очевидно, $N(u) = a^2 + 3b^2$. Далі вважаємо, що $u \in K^*$. Тоді існує таке число $v \in K$, що $uv = 1$. Звідси випливає, що $N(u)N(v) = N(uv) = N(1) = 1$. Отже, $N(u) = a^2 + 3b^2 = 1$. Ця рівність має місце тільки тоді, коли $b = 0$ і $a = \pm 1$. Таким чином, $K^* = \{\pm 1\}$.

Покажемо далі, що кільце $K = \mathbb{Z}[\sqrt{-3}]$ не є факторіальним. Легко бачити, що $4 = 2 \cdot 2 = (1 + \sqrt{-3})(1 - \sqrt{-3})$. Числа 2 і $1 \pm \sqrt{-3}$ є простими елементами кільця K. Дійсно, якщо, наприклад, $1 + \sqrt{-3}$ є непростим елементом кільця K, то $1 + \sqrt{-3} = u_1 \cdot u_2$, де $u_i \notin K^*$ $(i = 1, 2)$. Тоді

$$N(u_1)N(u_2) = N(u_1u_2) = N(1 + \sqrt{-3}) = 4.$$

Отже, $N(u_1) = 2$. З іншого боку, якщо $u_1 = a_1 + b_1\sqrt{-3}$ $(a_1,\ b_1 \in \mathbb{Z})$, то $N(u_1) = a_1^2 + 3b_1^2$. Звідси $a_1^2 + 3b_1^2 = 2$, що неможливо. Одержане протиріччя показує, що $1 + \sqrt{-3}$ — простий елемент кільця K. Аналогічно показується, що 2 і $1 - \sqrt{-3}$ є простими елементами кільця K. Нарешті, можна довести, що $1 + \sqrt{-3} \neq 2\theta$ для довільного $\theta \in K^*$. Таким чином, ми показали, що в кільці K число 4 розкладається на прості множники двома суттєво різними способами: $4 = 2 \cdot 2 = (1 + \sqrt{-3})(1 - \sqrt{-3})$. Отже, кільце $K = \mathbb{Z}[\sqrt{-3}]$ не є факторіальним.

В п р а в и

1. Знайти прості елементи в кільцях $\mathbb{C}[x]$ та $\mathbb{R}[x]$.

2. Розкласти елемент $x^2 + 1$ у добуток простих елементів у кільці $\mathbb{C}[x]$ та у кільці $\mathbb{R}[x]$.

3. Довести, що в кільці $\mathbb{Z}[i]$ цілих гаусових чисел елементи 2, 5 не є простими.

4. Чи будуть елементи $x^2 + 2$, $x^2 - 2$, $x^2 + 1$ простими в кільці $\mathbb{Q}[x]$?

5. Розкласти у добуток простих елементів елементи $x^3 + 1$, $x^2 + x + 1$, $x^2 + 1$ кільця $\mathbb{Z}_2[x]$.

6. Довести, що в довільному факторіальному кільці існують найбільший спільний дільник та найменше спільне кратне двох (або декількох) елементів.

7. Вияснити, чи будуть факторіальними кільця $\mathbb{Z}_5$, $\mathbb{Z}_6$, $\mathbb{Z}_8$?

8. Показати, що кільце $\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$ не є факторіальним.

9. Знайти мультиплікативну групу кільця $\mathbb{Z}[i]$.

10. Показати, що кільце $\mathbb{Z}[\sqrt{-2}] = \{a + b\sqrt{-2} \mid a, b \in \mathbb{Z}\}$ — евклідове, поклавши $\delta(a + b\sqrt{-2}) = a^2 + 2b^2$.

11. Нехай K — факторіальне кільце, L — підкільце кільця K, що містить одиницю кільця K. Чи буде L також факторіальним кільцем?

12. Перевірити, чи є фактор-кільця полями:
$\mathbb{Q}[x]/(x^2-2)\mathbb{Q}[x]$; $\mathbb{C}[x]/(x^2+1)\mathbb{C}[x]$; $\mathbb{R}[x]/x\mathbb{R}[x]$; $\mathbb{Z}_2[x]/(x^2+1)\mathbb{Z}_2[x]$.

§13. Мультиплікативна група кільця класів лишків

Нехай $K_1, \ldots, K_n$ — задані кільця, $K = K_1 \times \cdots \times K_n$ — декартовий добуток множин $K_1, \ldots, K_n$. Перетворимо множину K в кільце, визначивши операції додавання і множення в K в такий спосіб:

$$(x_1, \ldots, x_n) + (y_1, \ldots, y_n) = (x_1 + y_1, \ldots, x_n + y_n),$$

$$(x_1, \ldots, x_n) \cdot (y_1, \ldots, y_n) = (x_1 y_1, \ldots, x_n y_n),$$

де $x_i, y_i \in K_i$ $(i = 1, \ldots, n)$. Так визначене кільце K називається *зовнішньою прямою сумою* кілець $K_1, \ldots, K_n$ і позначається через $K_1 \dot{+} \cdots \dot{+} K_n$.

Нехай m — довільне натуральне число більше одиниці. Позначимо через $\varphi(m)$ кількість натуральних чисел, менших за m і взаємно простих з m. Вважатимемо, що $\varphi(1) = 1$. Відображення $\varphi : \mathbb{N} \to \mathbb{N}$, визначене за правилом $\varphi : m \to \varphi(m)$ називається *функцією Ейлера*. Розкладемо довільне натуральне число m у добуток степенів різних простих чисел: $m = p_1^{n_1} p_2^{n_2} \ldots p_s^{n_s}$ ($p_1, \ldots, p_s$ — різні прості числа, $n_1, \ldots, n_s \in \mathbb{N}$). Тоді

$$\varphi(m) = (p_1^{n_1} - p_1^{n_1-1})(p_2^{n_2} - p_2^{n_2-1}) \ldots (p_s^{n_s} - p_s^{n_s-1}).$$

Теорема 1. *Нехай* $m = p_1^{n_1} p_2^{n_2} \ldots p_s^{n_s}$ ($p_1, \ldots, p_s$ — *різні прості числа*, $n_1, \ldots, n_s \in \mathbb{N}$), $\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z}$, $\mathbb{Z}_m^*$ — *мультиплікативна група кільця* $\mathbb{Z}_m$. *Тоді*

$$\mathbb{Z}_m \cong \mathbb{Z}_{p_1^{n_1}} \dot{+} \cdots \dot{+} \mathbb{Z}_{p_s^{n_s}}, \quad \mathbb{Z}_m^* \cong \mathbb{Z}_{p_1^{n_1}}^* \dot{\times} \cdots \dot{\times} \mathbb{Z}_{p_s^{n_s}}^*, \quad |\mathbb{Z}_m^*| = \varphi(m).$$

Відмітимо, що $\mathbb{Z}_m^* = \{a + m\mathbb{Z} \mid 1 \le m < a,\ (a,m) = 1\}$, де (u,v) — найбільший спільний дільник чисел $u,\ v \in \mathbb{Z}$.

Теорема 2. *Нехай p — непарне просте число. Тоді мультиплікативна група $\mathbb{Z}_{p^n}^*$ $(n \in \mathbb{N})$ є циклічною групою. Група $\mathbb{Z}_{2^n}^*$ при $n = 1, 2$ — циклічна, а при $n > 2$ є абелевою групою типу $(2, 2^{n-2})$, а саме $\mathbb{Z}_{2^n}^* = \langle -1 + 2^n\mathbb{Z}\rangle \times \langle 5 + 2^n\mathbb{Z}\rangle$.*

П р и к л а д и

1. *Скільки є цілих чисел, менших за 500, взаємно простих з числом 500.*

Розв'язання. Очевидно, $500 = 2^2 \cdot 5^3$. Тоді

$$\varphi(500) = (2^2 - 2^1)(5^3 - 5^2) = 200.$$

2. *Описати будову мультиплікативної групи кільця $\mathbb{Z}_{36}$.*

Розв'язання. Оскільки $36 = 2^2 \cdot 3^2$, то за теоремою 1 $\mathbb{Z}_{36}^* \cong \mathbb{Z}_{2^2}^* \dot{\times} \mathbb{Z}_{3^2}^*$, де $\mathbb{Z}_{2^2}^*$ — циклічна група порядку $\varphi(2^2) = 2$, а $\mathbb{Z}_{3^2}^*$ — циклічна група порядку $\varphi(3^2) = 6$. Отже, група $\mathbb{Z}_{36}^*$ — це прямий добуток циклічної групи другого порядку на циклічну групу шостого порядку. Знайдемо твірні елементи груп $\mathbb{Z}_4^*$ та $\mathbb{Z}_9^*$. Очевидно, $\mathbb{Z}_4^* = \langle -1 + 4\mathbb{Z}\rangle$. Покажемо далі, що $\mathbb{Z}_9^* = \langle 2 + 9\mathbb{Z}\rangle$. Оскільки $|\mathbb{Z}_9^*| = 6$, то за теоремою Лагранжа досить перевірити, що порядок елемента $2+9\mathbb{Z}$ не дорівнює 2 і 3. Дійсно,

$$(2 + 9\mathbb{Z})^2 = 4 + 9\mathbb{Z} \ne 1 + 9\mathbb{Z}, \quad (2 + 9\mathbb{Z})^3 = 8 + 9\mathbb{Z} \ne 1 + 9\mathbb{Z}.$$

Таким чином, $\mathbb{Z}_{36}^* \cong \langle -1 + 4\mathbb{Z}\rangle \dot{\times} \langle 2 + 9\mathbb{Z}\rangle$.

В п р а в и

1. Обчислити $\varphi(m)$, якщо m дорівнює: а) 24; б) 96; в) 100; г) 45.

2. Довести, що для довільних взаємно простих натуральних чисел m та n $\varphi(mn) = \varphi(m)\varphi(n)$.

3. Показати, що група $\mathbb{Z}_n^*$ $(n > 1)$ — циклічна тоді і тільки тоді, коли $n \in \{2, 4, p^m, 2p^m\}$ (p — непарне просте число, $m \in \mathbb{N}$).

4. Нехай $m = p^r$ (p — непарне просте число, $r \in \mathbb{N}$), $c = \varphi(m) = p_1^{r_1} \dots p_k^{r_k}$ ($p_1, \dots, p_k$ — різні прості числа, $r_1, \dots, r_k \in \mathbb{N}$). Довести твердження: елемент $a + m\mathbb{Z}$, де $(a,m) = 1$, буде твірним елементом циклічної групи $\mathbb{Z}_m^*$ тоді і тільки тоді, коли m не задовольняє ні одній із конгруенцій

$$a^{\frac{c}{p_i}} \equiv 1 \pmod m \quad (i = 1, \dots, k).$$

5. Знайти твірні елементи циклічної групи $\mathbb{Z}_m^*$, якщо а) $m = 11$; б) $m = 19$; в) $m = 25$; г) $m = 17$.

6. Описати мультиплікативну групу кільця класів лишків $\mathbb{Z}_m$ при а) $m = 39$; б) $m = 27$; в) $m = 72$; г) $m = 360$.

§14. Конгруенції

Нехай K — комутативне кільце з одиницею і V — нетривіальний ідеал кільця K. Елементи $a \in K$ і $b \in K$ називаються *конгруентними* за модулем V, якщо $a - b \in V$. Це записують так: $a \equiv b \pmod{V}$. Цей запис означає, що $a - b + V = V$. Що в свою чергу еквівалентно умові $a + V = b + V$, тобто a і b є елементами одного і того ж суміжного класу кільця K за ідеалом V.

Надалі будемо вважати, що $K = \mathbb{Z}$. Тоді $V = m\mathbb{Z}$ для деякого натурального числа m ($m > 1$). Якщо елементи a, $b \in \mathbb{Z}$ конгруентні за ідеалом V, тобто $a + m\mathbb{Z} = b + m\mathbb{Z}$, то кажуть, що цілі числа a і b конгруентні за модулем m і записують це так: $a \equiv b \pmod{m}$. Очевидно, $a \equiv b \pmod{m}$ тоді і тільки тоді, коли $a - b = km$ для деякого цілого числа k.

Властивості конгруенцій:

1. $a \equiv a \pmod{m}$.
2. Якщо $a \equiv b \pmod{m}$, то $b \equiv a \pmod{m}$.
3. Якщо $a \equiv b \pmod{m}$, $b \equiv c \pmod{m}$, то $a \equiv c \pmod{m}$.
4. Якщо $a \equiv b \pmod{m}$, $c \equiv d \pmod{m}$, то $a \pm c \equiv b \pm d \pmod{m}$, $ac \equiv bd \pmod{m}$.
5. Якщо $ac \equiv bc \pmod{m}$ і $(|c|, m) = 1$, то $a \equiv b \pmod{m}$.

Теорема Ейлера. *Нехай m — довільне натуральне число більше 1, a — довільне ціле число таке, що $(|a|, m) = 1$. Тоді*

$$a^{\varphi(m)} \equiv 1 \pmod{m}. \tag{1}$$

Мала теорема Ферма. *Нехай p — просте число і a — довільне ціле число. Тоді $a^p \equiv a \pmod{p}$.*

Нехай $f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n \in \mathbb{Z}[x]$ ($a_i \in \mathbb{Z}$; $i = 0, 1, \ldots, n$), де $a_0 \not\equiv 0 \pmod{m}$. Вираз вигляду

$$f(x) \equiv 0 \pmod{m} \tag{2}$$

називають *конгруенцією n-го степеня за модулем m*.

Нехай для $x_0 \in \mathbb{Z}$ справедлива конгруенція $f(x_0) \equiv 0 \pmod{m}$. Тоді $f(x_1) \equiv 0 \pmod{m}$ для довільного $x_1 \in x_0 + m\mathbb{Z}$. Клас $x_0 + m\mathbb{Z}$ називається *розв'язком конгруенції* (2). Очевидно, конгруенція (2) не може мати більше ніж m різних розв'язків.

Розглянемо конгруенцію першого степеня:

$$ax \equiv b \pmod{m} \quad (a, b \in \mathbb{Z},\ m > 1). \tag{3}$$

Якщо $(|a|, m) = 1$, то конгруенція (3) має єдиний розв'язок:

$$x \equiv a^{\varphi(m)-1} b \pmod{m}. \tag{4}$$

Якщо $(|a|, m) = d > 1$, то конгруенція (3) має розв'язок тоді і тільки тоді, коли d ділить b.

Нехай $(|a|, m) = d > 1$ і d ділить b. Тобто $a = a_1 d$, $b = b_1 d$, $m = m_1 d$, де $(|a_1|, m_1) = 1$ $(a_1, b_1, m_1 \in \mathbb{Z})$. Тоді конгрунція $a_1 x \equiv b_1 \pmod{m}$ має єдиний розв'язок $x_0 + m_1\mathbb{Z}$. А конгруенція (3) у даному випадку буде мати точно d різних розв'язків:

$$x_0 + i\frac{m}{d} + m\mathbb{Z} \quad (i = 0, 1, \ldots, d-1). \tag{5}$$

П р и к л а д и

1. *Знайти найменший додатній лишок числа* 5^{100} *за модулем* 17.

Розв'язання. Оскільки $(5, 17) = 1$, то можна скористатися теоремою Ейлера: $5^{\varphi(17)} \equiv 1 \pmod{17}$. Очевидно, $\varphi(17) = 16$. Тобто $5^{16} \equiv 1 \pmod{17}$. Тоді

$$5^{100} = 5^{16 \cdot 6 + 4} = (5^{16})^6 \cdot 5^4 \equiv 5^4 \equiv 13 \pmod{17}.$$

2. *Розв'язати конгруенцію першого степеня* $5x \equiv 2 \pmod{36}$.

Розв'язання. У нас задана конгруенція вигляду (3), причому $(5, 36) = 1$. Тоді за формулою (4) конгруенція має єдиний розв'язок $x \equiv 5^{\varphi(36)-1} \cdot 2 \pmod{36}$. Як відомо

$$\varphi(36) = \varphi(2^2 \cdot 3^2) = (2^2 - 2)(3^2 - 3) = 2 \cdot 6 = 12.$$

Залишається знайти найменший додатній лишок числа $5^{11} \cdot 2$ за модулем 36:

$$5^{11} \cdot 2 = 5^{3 \cdot 3 + 2} \cdot 2 = (5^3)^3 \cdot 5^2 \cdot 2 \equiv 17^3 \cdot 14 \equiv 22 \pmod{36}.$$

Отже, $22 + 36\mathbb{Z}$ — єдиний розв'язок конгруенції.

3. *Розв'язати конгруенцію першого степеня* $9x \equiv 6 \pmod{15}$.

Розв'язання. Оскільки $(9, 15) = 3$ і 3 ділить 6, то дана конгруенція має точно три розв'язки. Знайдемо їх. Конгруенція $3x \equiv 2 \pmod{5}$ має розв'язок $4 + 5\mathbb{Z}$. Тоді на основі (5) конгруенція $9x \equiv 6 \pmod{15}$ має розв'язки: $4 + 15\mathbb{Z}$, $9 + 15\mathbb{Z}$, $14 + 15\mathbb{Z}$.

В п р а в и

1. Знайти остачу від ділення числа 2000^{2000} на число 7.

2. Знайти найменший додатній лишок числа 3^{1000} за модулем 13.

3. Розв'язати такі лінійні конгруенції:

а) $2x \equiv 5 \pmod{9}$; б) $5x \equiv 3 \pmod{7}$; в) $4x \equiv 2 \pmod{7}$;

г) $7x \equiv 1 \pmod{9}$; д) $25x \equiv 7 \pmod{49}$; е) $4x \equiv 9 \pmod{15}$.

4. Скільки розв'язків мають такі конгруенції першого степеня:

а) $3x \equiv 7 \pmod{9}$; б) $3x \equiv 10 \pmod{12}$; в) $17x \equiv 40 \pmod{51}$.

5. Знайти всі розв'язки конгруенцій першого степеня:

а) $15x \equiv 21 \pmod{33}$; б) $3x \equiv 9 \pmod{12}$; в) $25x \equiv 40 \pmod{55}$.

6. Розв'язати конгруенції другого степеня:

а) $x^2 \equiv -1 \pmod{13}$; б) $x^2 \equiv -1 \pmod{11}$; в) $x^2 \equiv 2 \pmod{31}$.

7. Довести, що конгруенція другого степеня $x^2 + 1 \equiv 0 \pmod{p}$ не має розв'язків при $p \equiv 3 \pmod{4}$.

8. Довести, що $(p-1)! \equiv -1 \pmod{p}$, якщо p — просте число.

9. Довести, що конгруенція $a_0x^n + a_1x^{n-1} + \cdots + a_n \equiv 0 \pmod{p}$ степеня n за простим модулем p має не більш як n розв'язків.

10. Знайти ознаку подільності цілих чисел на n для всіх $n \leq 11$.

11. Розв'язати в цілих раціональних числах рівняння з двома невідомими:

а) $53x + 32y = 1$; б) $64x + 28y = 12$; в) $63x + 99y = 3$.

§15. Алгебраїчні та скінченні розширення полів

Якщо поле P міститься в полі F, то кажуть, що поле F є *розширенням* поля P а поле P є *підполем* поля F.

Нехай поле F — розширення поля P ($P \subset F$). Елемент $\alpha \in F$ називається *алгебраїчним* над полем P, якщо α є коренем деякого ненульо-

вого полінома $f(x)$ з коефіцієнтами із поля P. Число $\alpha \in \mathbb{C}$ називається *алгебраїчним числом*, якщо воно є алгебраїчним елементом над полем $\mathbb{Q}$ раціональних чисел. Число $\beta \in \mathbb{C}$ називається *трансцендентним*, якщо воно не є алгебраїчним числом. Розширення F поля P називається *алгебраїчним*, якщо всякий елемент $\alpha \in F$ є алгебраїчним елементом над полем P.

Поле F називається *скінченним* розширенням поля P ($P \subset F$), якщо поле F є скінченно вимірним лінійним простором над полем P. Розмірність цього простору називається *степенем* поля F над полем P і позначається через $(F : P)$.

Теорема 1. *Всяке скінченне розширення даного поля є алгебраїчним.*

Теорема 2. *Нехай P, F, S — поля, що задовольняють таким умовам: $P \subset F \subset S$; $(F : P) = m$; $(S : F) = n$. Тоді S — скінченне розширення поля P степеня $(S : P) = mn$.*

Поле P називається *алгебраїчно замкнутим*, якщо будь-який многочлен $f(x)$ степеня $n \in \mathbb{N}$ з коефіцієнтами з поля P розкладається над полем P на лінійні множники, тобто

$$f(x) = a(x - \xi_1)(x - \xi_2) \dots (x - \xi_n) \quad (a, \xi_1, \dots, \xi_n \in P).$$

Кожне поле P міститься в деякому алгебраїчно замкнутому полі.

П р и к л а д и

1. *Показати, що $\frac{-1+i\sqrt{3}}{2}$ є алгебраїчним числом.*

Розв'язання. За означенням алгебраїчного числа досить показати, що число $\alpha = \frac{-1+i\sqrt{3}}{2}$ є коренем деякого ненульового многочлена $f(x)$ з коефіцієнтами з поля $\mathbb{Q}$ раціональних чисел. В якості многочлена $f(x)$ можемо взяти, наприклад, многочлен $(x-\alpha)(x-\overline{\alpha})$, де $\overline{\alpha}$ — число, комплексно спряжене до α. Тобто

$$f(x) = \left(x - \frac{-1 + i\sqrt{3}}{2}\right)\left(x - \frac{-1 - i\sqrt{3}}{2}\right) = x^2 + x + 1.$$

2. *Нехай F — розширення поля $\mathbb{Z}_p$ і $(F : \mathbb{Z}_p) = n$. Показати, що поле F складається із p^n елементів.*

Розв'язання. Із умови $(F : \mathbb{Z}_p) = n$ випливає, що в полі F існують n елементів $u_1, \dots, u_n$, які утворюють базис лінійного простору F над полем $\mathbb{Z}_p$. Отже, довільний елемент u поля F однозначно представляється у вигляді:

$$u = \alpha_1 u_1 + \dots + \alpha_n u_n \quad (\alpha_1, \dots, \alpha_n \in \mathbb{Z}_p).$$

Враховуючи, що поле $\mathbb{Z}_p$ складається з p елементів, одержуємо, що в полі F є точно p^n елементів.

В п р а в и

1. Нехай F — розширення поля $\mathbb{Q}$ степеня 2. Довести, що довільний елемент $\alpha \in F$ є коренем деякого многочлена над полем $\mathbb{Q}$, степінь якого не перевищує 2.

2. Чи будуть алгебраїчними числа: а) $1 - i$; б) $\frac{-1+\sqrt{-15}}{2}$; в) $2 + \sqrt[3]{3}$?

3. Показати, що якщо F є алгебраїчним розширенням поля $\mathbb{R}$, то F суміщається з $\mathbb{R}$ або $\mathbb{C}$.

4. Чи можуть бути поля $\mathbb{Q}(\sqrt{2}) = \{a+b\sqrt{2} | a, b \in \mathbb{Q}\}$ і $\mathbb{Q}$ ізоморфними?

5. Чи буде поле $\mathbb{Q}(\sqrt{2})$ алгебраїчно замкнутим?

6. Показати, що якщо одне із комплексних чисел α і $\sqrt{\alpha}$ є трансцендентним, то і друге число буде також трансцендентним.

§16. Прості розширення полів

Нехай F — розширення поля P ($P \subset F$), а M — довільна непорожня підмножина поля F. Позначимо через $P(M)$ переріз всіх таких полів, що містять поле P, множину M і містяться в полі F. Очевидно, $P(M)$ — мінімальне підполе поля F, що містить множину M і поле P. Говорять, що $P(M)$ одержано із поля P *приєднанням* множини M. Якщо M — скінченна множина і $M = \{u_1, \ldots, u_n\}$, то $P(M)$ записують у вигляді $P(u_1, \ldots, u_n)$. Якщо множина M складається з одного елемента θ, то поле $P(\theta)$ називається *простим* розширенням поля P.

Теорема 1. *Нехай F — розширення поля P, $\theta \in F$ — алгебраїчний елемент над полем P. Нехай $f(x)$ — незвідний поліном з коефіцієнтами з поля P степеня n, коренем якого є θ. Тоді $P(\theta) \cong P[x]/f(x)P[x]$, причому $(P(\theta) : P) = n$ і кожний елемент u поля $P(\theta)$ однозначно представляється у вигляді*

$$u = a_0 \cdot 1 + a_1\theta + \cdots + a_{n-1}\theta^{n-1} \quad (a_0, \ldots, a_{n-1} \in P).$$

Теорема 2. *Нехай K — поле характеристики 0, $K(u_1, u_2, \ldots, u_n)$ — розширення поля K, де u_1, u_2, …, u_n — алгебраїчні елементи над K. Для деякого алгебраїчного елемента θ над полем K*

$$K(u_1, u_2, \ldots, u_n) = K(\theta).$$

П р и к л а д и

1. *Знайти степінь поля* $\mathbb{Q}(\varepsilon)$ *над полем* $\mathbb{Q}$, *де* ε — *первісний корінь третього степеня із одиниці.*

Розв'язання. Очевидно, ε є коренем полінома $x^3-1=(x-1)\times(x^2+$ $+x+1)$. Звідси одержуємо, що ε є коренем незвідного над $\mathbb{Q}$ полінома $f(x)=x^2+x+1$. Тоді за теоремою 1 $\mathbb{Q}(\varepsilon)\cong\mathbb{Q}[x]/f(x)\mathbb{Q}[x]$ і, отже, $(\mathbb{Q}(\varepsilon):\mathbb{Q})=2$. Тому довільний елемент $u\in\mathbb{Q}(\varepsilon)$ має вигляд: $u=\alpha+\beta\varepsilon$ (α, $\beta\in\mathbb{Q}$).

2. *Нехай* F *є квадратичним розширенням поля* $\mathbb{Q}$, *тобто* $(F:\mathbb{Q})=2$ ($F\subset\mathbb{C}$). *Показати, що* $F=\mathbb{Q}(\sqrt{d})$, *де* d — *деяке ціле число* ($d\neq 0$, $d\neq 1$), *що не ділиться на квадрат натурального числа відмінного від одиниці.*

Розв'язання. Із вправи 1 §11 випливає, що існує таке число $\theta\in F$, що θ є коренем незвідного над полем $\mathbb{Q}$ полінома $f(x)=x^2+\alpha x+\beta$ (α, $\beta\in\mathbb{Q}$). Внаслідок теореми 1 $(\mathbb{Q}(\theta):\mathbb{Q})=2$ і $\mathbb{Q}\subset\mathbb{Q}(\theta)\subset F$. Звідси і із теореми 2 §11 випливає, що $F=\mathbb{Q}(\theta)$. Очевидно,

$$f(x)=\left(x+\frac{\alpha}{2}\right)^2+\beta-\frac{\alpha^2}{4}=y^2-d_1,$$

де $d_1=\frac{\alpha^2}{4}-\beta$, $y=x+\frac{\alpha}{2}$. Оскільки $\left(\theta+\frac{\alpha}{2}\right)^2-d_1=f(\theta)=0$, то $\left(\theta+\frac{\alpha}{2}\right)^2=d_1$, причому d_1 не є квадратом раціонального числа. Тому

$$\mathbb{Q}(\theta)=\mathbb{Q}(\theta+\frac{\alpha}{2})=\mathbb{Q}(\sqrt{d_1}).$$

Далі, очевидно, раціональне число d_1 можна представити у вигляді добутку квадрата деякого раціонального числа m та цілого числа d ($d\neq 0$, $d\neq 1$), що не ділиться на квадрат натурального числа відмінного від одиниці, тобто $d_1=m^2d$. Тоді

$$\mathbb{Q}(\sqrt{d_1})=\mathbb{Q}(m\sqrt{d})=\mathbb{Q}(\sqrt{d}).$$

Отже, $F=\mathbb{Q}(\sqrt{d})$, де $d\in\mathbb{Z}$, ($d\neq 0$, $d\neq 1$) й d не ділиться на квадрат натурального числа відмінного від одиниці.

В п р а в и

1. Знайти степінь поля $\mathbb{Q}(\sqrt{2})$ над полем $\mathbb{Q}$.

2. Нехай квадратний тричлен $f(x)$ з дійсними коефіцієнтами має від'ємний дискримінант. Показати, що фактор-кільце $\mathbb{R}[x]/f(x)\mathbb{R}[x]$ є полем, яке ізоморфне полю $\mathbb{C}$.

3. Нехай $\mathbb{Q}(\sqrt{d})$ і $\mathbb{Q}(\sqrt{d'})$ — квадратичні поля (d, d' — вільні від квадратів цілі раціональні числа). Довести, що $\mathbb{Q}(\sqrt{d}) = \mathbb{Q}(\sqrt{d'})$ тоді і тільки тоді, коли $d = d'$.

4. Показати, що $\mathbb{Q}(\varepsilon, i) = \mathbb{Q}(\varepsilon i)$ ($\varepsilon^3 = 1$, $\varepsilon \neq 1$, $i^2 = -1$).

5. Показати, що $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$.

6. Довести, що $\mathbb{Q}(\sqrt{3}, i) = \mathbb{Q}(\xi)$, де $i^2 = -1$, ξ — первісний корінь степеня 12 із одиниці.

§17. Скінченні поля

Поле F називається *скінченним*, якщо воно складається з скінченного числа елементів. Прикладом скінченного поля є поле $\mathbb{Z}_p$ (p — просте ціле раціональне число).

Теорема 1. *Для кожного простого числа p і кожного натурального числа n існує з точністю до ізоморфізму точно одне поле F_{p^n} з числом елементів p^n. Мультиплікативна група поля F_{p^n} є циклічною групою порядку $p^n - 1$.*

Теорема 2. *Всяке скінченне поле F_{p^n} ізоморфне фактор-кільцю $\mathbb{Z}_p[x]/f(x)\mathbb{Z}_p[x]$, де $f(x)$ — деякий незвідний поліном над $\mathbb{Z}_p$ степеня n.*

П р и к л а д и

1. *Побудувати поле із 4 елементів.*

Розв'язання. Розглянемо фактор-кільце

$$T = \mathbb{Z}_2[x]/(x^2 + x + 1)\mathbb{Z}_2[x].$$

Оскільки $\overline{0} = 2\mathbb{Z}$, $\overline{1} = 1 + 2\mathbb{Z}$ не є коренями полінома $f(x) = x^2 + x + \overline{1}$, то $f(x)$ незвідний поліном над $\mathbb{Z}_2$. Звідси та із теореми 3 §13 випливає, що T є полем. Тоді за теоремою 1 §6 $T \cong \mathbb{Z}_2(\theta)$, де $f(\theta) = \overline{0}$. Отже, $\mathbb{Z}_2(\theta) = \{\alpha + \beta\theta \mid \alpha, \beta \in \mathbb{Z}_2\}$. Таким чином, поле $\mathbb{Z}_2(\theta)$ складається із 4 елементів: $\overline{0}$, $\overline{1}$, θ, $\overline{1} + \theta$.

Легко бачити, що $\mathbb{Z}_2(\theta)^* = \langle\theta\rangle$.

В п р а в и

1. Побудувати поле з 9 елементів.

2. Нехай поле P є розширенням поля $\mathbb{Z}_p$ і містить p^m елементів. Довести, що всі елементи поля P задовольняють рівнянню $x^{p^m} - x = 0$.

3. Чи має рівняння: а) $x^2 = \overline{5}$; б) $x^7 = \overline{7}$; в) $x^3 = \overline{a}$ розв'язки в полі $\mathbb{Z}_{11}$ ($\overline{b} = b + 11\mathbb{Z}$, $b \in \mathbb{Z}$).

4. Знайти порядок елемента $\overline{2} = 2 + p\mathbb{Z}$ в мультиплікативній групі поля $\mathbb{Z}_p$ для $p = 3, 5, 7, 11$. В яких із цих груп $\overline{2}$ є твірним елементом?

5. Знайти твірні елементи в мультиплікативній групі поля: а) $\mathbb{Z}_7$; б) $\mathbb{Z}_{11}$.

6. Знайти незвідні многочлени степенів менших за п'ять над полем $\mathbb{Z}_2$.

7. Знайти всі незвідні многочлени степеня 2 над полем $\mathbb{Z}_3$.

8. Довести, що всяке скінченне розширення скінченного поля є простим.

9. Довести, що в полі F_q (поле із q елементів) має місце розклад

$$x^q - x = \prod_{a \in F_q} (x - a).$$

10. Довести, що всяке скінченне поле характеристики p містить разом з кожним із своїх елементів a рівно один корінь p-го степеня із a.

11. Нехай F_r і F_q — скінченні поля. Довести, що поле F_r ізоморфне деякому підполю поля F_q тоді і тільки тоді, коли $q = r^m$ для деякого натурального числа m.

12. Довести, що для всякого натурального числа n існує многочлен степеня n, незвідний над полем F_q.

§18. Модулі

Нехай K — кільце з одиницею 1, M — адитивно записана абелева група. Нехай задане відображення $\varphi : K \times M \to M$, тобто таке відображення φ, яке кожній впорядкованій парі (α, x) $(\alpha \in K, x \in M)$ ставиться у відповідність певний елемент $\varphi(\alpha, x)$ з групи M. Будемо $\varphi(\alpha, x)$ позначати так: $\varphi(\alpha, x) = \alpha \cdot x = \alpha x$. Елемент αx групи M називається *добутком* елемента α кільця K на елемент x модуля M. Група M називається лівим *K-модулем*, якщо виконуються умови:

1) $\alpha(x + y) = \alpha x + \alpha y$;
2) $(\alpha + \beta)x = \alpha x + \beta x$;
3) $(\alpha\beta)x = \alpha(\beta x)$;
4) $1x = x$

для довільних $\alpha, \beta \in K$ та $x, y \in M$.

Надалі лівий K-модуль будемо називати просто K-модулем. Очевидно, довільний лінійний простір над полем F буде F-модулем.

Підмодулем K-модуля M називається підгрупа V адитивної групи M така, що $\alpha v \in V$ для довільних елементів $\alpha \in K$, $v \in V$.

Нехай S — непорожня підмножина K-модуля M. Позначимо через $\langle S\rangle$ підмножину в M, що складається із всіх елементів вигляду:

$$\alpha_1 x_1 + \cdots + \alpha_r x_r \quad (\alpha_i \in K,\ x_i \in S;\ i = 1,\ \ldots,\ r).$$

Неважко показати, що множина $\langle S\rangle$ є підмодулем K-модуля M. Цей підмодуль називається підмодулем K-модуля M, *породженим* множиною S, а множина S — множиною *твірних елементів* цього підмодуля. K-модуль M називається *скінченно породженим*, якщо існує така скінченна підмножина S із M, що $M = \langle S\rangle$. K-модуль M називається *циклічним*, якщо він породжується одним елементом. K-модуль M будемо називати *вільним K-модулем рангу n*, якщо існує така підмножина $\{u_1,\ \ldots,\ u_n\}$ елементів із M, що довільний елемент $m \in M$ однозначно представляється у вигляді:

$$m = \alpha_1 u_1 + \cdots + \alpha_n u_n \quad (\alpha_i \in K,\ i = 1,\ \ldots,\ n).$$

Якщо K — комутативне кільце, то ранг вільного K-модуля визначається однозначно.

Нехай V — підмодуль K-модуля M і M/V — фактор-група адитивної абелевої групи M за підгрупою V. Добуток елементів кільця K на елементи цієї групи задамо в такий спосіб:

$$\alpha(m + V) = \alpha m + V \quad (\alpha \in K,\ m \in M).$$

Тоді фактор-група M/V буде K-модулем і цей модуль будемо називати *фактор-модулем* модуля M за підмодулем V.

Відображення f K-модуля M в K-модуль M' називається *гомоморфним*, якщо $f(a+b) = f(a)+f(b)$ і $f(\gamma a) = \gamma f(a)$ для довільних елементів $a,\ b \in M$ і $\gamma \in K$. Гомоморфне відображення K-модуля M на K-модуль M' називається *ізоморфним*, якщо воно взаємно однозначне. K-модулі M та M' називаються *ізоморфними*, якщо існує ізоморфне відображення групи K-модуля M на K-модуль M'. Це записують так: $M \cong M'$.

Очевидно, підмножина $\operatorname{Ker} f = \{m \in M \mid f(m) = 0\}$, яка називається *ядром* гомоморфізму f, є підмодулем K-модуля M.

Теорема 1. *Нехай M і M' — K-модулі і f — гомоморфне відображення K-модуля M на K-модуль M'. Тоді $M/\operatorname{Ker} f \cong M'$.*

Нехай $M_1,\ \ldots,\ M_r$ $(r \in \mathbb{N})$ — K-модулі і $M = M_1 \dot{+} \cdots \dot{+} M_r$ — зовнішня пряма сума адитивних абелевих груп $M_1, \ldots, M_r$. Перетворимо M в K-модуль, покладаючи $\lambda(m_1, \ldots, m_r) = (\lambda m_1, \ldots, \lambda m_r)$, де $\lambda \in$ $\in K$, $m_i \in M_i$ $(i = 1, \ldots, r)$. Так визначений K-модуль M називається *зовнішньою прямою сумою* K-модулів $M_1,\ \ldots,\ M_r$.

K-модуль T називається *внутрішньою прямою сумою* своїх підмодулів $T_1, \ldots, T_r$ ($r \in \mathbb{N}$), якщо кожний елемент $t \in T$ однозначно представляється у вигляді: $t = t_1 + \cdots + t_r$ ($t_i \in T_i$, $i = 1, \ldots, r$). У цьому випадку будемо вживати позначення $T = T_1 \oplus \cdots \oplus T_r$.

Аналогічно як у випадку груп, установлюється зв'язок між зовнішньою і внутрішньою прямими сумами K-модулів.

П р и к л а д и

1. *Перетворити довільне кільце K з одиницею в K-модуль.*

Розв'язання. Відображення $K \times K \to K$ задамо в такий спосіб: $(\alpha, x) \to \alpha \cdot x$ (α, $x \in K$). Легко перевірити, що тоді виконуються умови 1)–4) в означенні K-модуля. Очевидно, K-модуль K є скінченно породженим. Він породжується одиницею кільця K.

2. *Показати, що $\mathbb{Z}$-модуль $\mathbb{Q}$ не є скінченно породженим $\mathbb{Z}$-модулем.*

Розв'язання. Припустимо, що $\mathbb{Q}$ — скінченно породжений $\mathbb{Z}$модуль. Тоді знайдуться такі раціональні числа $u_i = \frac{\alpha_i}{\beta_i}$ ($\alpha_i \in \mathbb{Z}$, $\beta_i \in \mathbb{N}$; $i = 1, \ldots, n$), що довільне раціональне число u представляється у вигляді

$$u = \lambda_1 u_1 + \cdots + \lambda_n u_n \quad (\lambda_i \in \mathbb{Z};\ i = 1, \ldots, n).$$

Отже,

$$u = \frac{\alpha}{\beta_1 \ldots \beta_n} \tag{1}$$

для деякого цілого числа α. Очевидно, число $u_0 = \frac{\alpha}{\beta_1 \ldots \beta_n + 1}$ у вигляді (1) не представляється. Таким чином, $\mathbb{Q}$ не є скінченно породженим $\mathbb{Z}$-модулем.

В п р а в и

1. Показати, що кільце $P[x]$ многочленів від невідомої x над полем P є P-модулем. Чи буде цей модуль скінченно породженим?

2. Показати, що довільна адитивна абелева група є $\mathbb{Z}$-модулем.

3. Показати, що ідеал комутативного кільця K з одиницею є K-модулем.

4. Чи можна стверджувати, що елементи $2, 3 \in \mathbb{Z}$ є системою твірних елементів $\mathbb{Z}$-модуля $\mathbb{Z}$.

5. Довести, що якщо комутативне кільце з одиницею розглянути як модуль над собою, то підмодулі цього модуля суміщаються з ідеалами кільця K.

6. Нехай K — кільце з одиницею і V — підмодуль K-модуля M. Довести, що якщо K-модуль V і фактор-модуль K/V — скінченно породжені K-модулі, то і M теж скінченно породжений K-модуль.

7. Нехай K — кільце з одиницею і K-модуль M є внутрішньою прямою сумою підмодулів M_1 і M_2. Показати, що якщо V_i — підмодуль модуля M_i $(i = 1, 2)$, то $V_1 + V_2 = V_1 \oplus V_2$.

8. Нехай K — кільце з одиницею, M — K-модуль. Довести, що якщо $M = M_1 \oplus M_2$, то $M/M_1 \cong M_2$.

9. Нехай K — кільце головних ідеалів. Довести, що будь-який підмодуль циклічного K-модуля є також циклічним K-модулем.

§19. Цілі алгебраїчні числа

Нехай $\mathbb{C}$ — поле комплексних чисел. Число $u \in \mathbb{C}$ називається *цілим алгебраїчним* числом, якщо u є коренем деякого многочлена $f(x)$ вигляду: $f(x) = x^n + \alpha_1 x^{n-1} + \cdots + \alpha_n \quad (\alpha_i \in \mathbb{Z},\ i = 1, \ldots, n)$.

Теорема 1. *Нехай α — алгебраїчне число. Тоді $\alpha = \frac{\beta}{n}$, де n — ціле раціональне число $(n \neq 0)$, β — ціле алгебраїчне число.*

Лема 1. *Нехай K — підкільце поля $\mathbb{C}$, яке є скінченно породженим $\mathbb{Z}$-модулем. Тоді довільний елемент кільця K є цілим алгебраїчним числом.*

Теорема 2. *Нехай F — розширення поля раціональних чисел і $F \subset \subset \mathbb{C}$. Множина всіх цілих алгебраїчних чисел поля F є кільцем.*

Теорема 3. *Нехай $F = \mathbb{Q}(\sqrt{d})$, де d — ненульове ціле число $(d \neq 1)$, яке не ділиться на квадрат простого числа. Якщо $d \equiv 2 \pmod 4$ або $d \equiv 3 \pmod 4$, то довільне ціле алгебраїчне число із поля $\mathbb{Q}(\sqrt{d})$ має вигляд: $a + b\sqrt{d}$ $(a, b \in \mathbb{Z})$. При $d \equiv 1 \pmod 4$ цілі алгебраїчні числа із поля $\mathbb{Q}(\sqrt{d})$ мають вигляд: $a + b\omega$ $(a, b \in \mathbb{Z})$, де $\omega = \frac{1+\sqrt{d}}{2}$.*

П р и к л а д и

1. *Довести, що число $\sqrt[5]{2} + \sqrt[7]{3}$ є цілим алгебраїчним числом.*

Розв'язання. Оскільки $\sqrt[5]{2}$ є коренем многочлена $x^5 - 2$, а $\sqrt[7]{3}$ — коренем многочлена $x^7 - 3$, то числа $\sqrt[5]{2}$ та $\sqrt[7]{3}$ є цілими алгебраїчними числами. На основі теореми 2 сума цілих алгебраїчних чисел є цілим алгебраїчним числом. Тому число $\sqrt[5]{2} + \sqrt[7]{3}$ є цілим алгебраїчним числом.

2. *Показати, що $u = \frac{-1+\sqrt{d}}{2}$ є цілим алгебраїчним числом, якщо $d \in \mathbb{Z}$ і $d \equiv 1 \pmod 4$.*

Розв'язання. Нехай $u' = \frac{-1-\sqrt{d}}{2}$. Тоді $u + u' = -1$, $uu' = \frac{1-d}{4}$. Із умови $d \equiv 1 \pmod 4$ випливає, що $uu' \in \mathbb{Z}$. Отже, u є коренем полінома $(x - u)(x - u') = x^2 + x + \frac{1-d}{4} \in \mathbb{Z}[x]$. Таким чином, u — ціле алгебраїчне число.

3. *Знайти мультиплікативну групу кільця K всіх цілих алгебраїчних чисел поля $\mathbb{Q}(i)$ $(i^2 = -1)$.*

Розв'язання. В силу теореми 3 $K = \mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$. Нехай $u = a + bi$ — елемент мультиплікативної групи K^*. Тоді існує елемент $v \in K^*$ такий, що $uv = 1$. Звідси одержуємо, що $|uv| = |u||v| = 1$, де $|z|$ — модуль комплексного числа z. Отже, $|u|^2|v|^2 = 1$. Значить, $|u|^2 = a^2+b^2 = 1$. Ця рівність має місце тоді і тільки тоді, коли $(a, b) = (\pm 1, 0)$ або $(a, b) = (0, \pm 1)$. Таким чином, $u = \pm 1$ або $u = \pm i$, тобто $K^* = \mathbb{Z}[i]^* = \{1, -1, i, -i\}$.

Вправи

1. Перевірити, чи будуть цілими алгебраїчними числа:
а) $2\sqrt[5]{7}$; б) $\sqrt{3}\sqrt[3]{4}$; в) $\frac{7}{\sqrt{2}-\sqrt{3}}$; г) $\frac{\sqrt{7}}{2-\sqrt{5}}$.

2. Довести, що раціональне число α є цілим алгебраїчним числом тоді і тільки тоді, коли α є цілим числом.

3. Знайти кільце цілих алгебраїчних чисел квадратичного поля: а) $\mathbb{Q}(\sqrt{-3})$; б) $\mathbb{Q}(\sqrt{19})$.

4. Показати, що кільце всіх цілих алгебраїчних чисел поля $\mathbb{Q}(\sqrt{-13})$ не є факторіальним.

§20. Алгебри

Нехай A — кільце, яке є також лінійним простором над полем F. Якщо для довільних елементів a, $b \in A$ і $\lambda \in F$

$$\lambda(ab) = (\lambda a)b = a(\lambda b),$$

то кільце A називається *алгеброю* над полем F. Якщо алгебра A над полем F є скінченно вимірним лінійним простором над цим же полем, то алгебра A називається *скінченно вимірною алгеброю над полем F*. Розмірність лінійного простору A над полем F називається *розмірністю* алгебри A і позначається через $\dim_F A$.

Можна показати, що множина $F_{n\times n}$ всіх матриць порядку n над полем F відносно звичайних операцій додавання і множення матриць та операції множення елемента поля F на матрицю є алгеброю розмірності n^2.

Підалгеброю алгебри A називається підкільце B кільця A, яке є підпростором лінійного простору A над полем F.

Відображення f алгебри A над полем F в алгебру A' над полем F

називається *гомоморфним*, якщо

$$f(a+b)=f(a)+f(b),\quad f(ab)=f(a)f(b),\quad f(\lambda a)=\lambda f(a)$$

для довільних елементів a, $b\in A$ і $\lambda\in F$. Гомоморфне відображення алгебри A над полем F на алгебру A' над полем F називається *ізоморфним*, якщо воно взаємно однозначне. Алгебри A та A' над полем F називаються *ізоморфними*, якщо існує ізоморфне відображення алгебри A на алгебру A'. Це записують так: $A\cong A'$.

Теорема 1. *Всяка алгебра A над полем F з одиницею розмірності n ізоморфна деякій підалгебрі алгебри $F_{n\times n}$.*

Нехай $\mathbb{H}$ — чотирьохвимірний лінійний простір над полем дійсних чисел $\mathbb{R}$. Позначимо через e, i, j, k базис простору $\mathbb{H}$ над полем $\mathbb{R}$. Перетворимо лінійний простір $\mathbb{H}$ в алгебру над полем $\mathbb{R}$, задавши операцію множення базисних елементів в такий спосіб, як вказано в таблиці.

$\cdot$	e	i	j	k
e	e	i	j	k
i	i	$-e$	k	$-j$
j	j	$-k$	$-e$	i
k	k	j	$-i$	$-e$

Ця алгебра називається *алгеброю кватерніонів*. Елемент $\overline{u}=\alpha_1 e-\alpha_2 i-$ $-\alpha_3 j-\alpha_4 k$ називається *спряженим* до елемента $u=\alpha_1 e+\alpha_2 i+\alpha_3 j+\alpha_4 k$ ($\alpha_i\in\mathbb{R}$; $i=1,2,3,4$). Якщо $u\neq 0$, то

$$u^{-1}=(\alpha_1^2+\alpha_2^2+\alpha_3^2+\alpha_4^2)^{-1}\overline{u}.$$

Отже, алгебра $\mathbb{H}$ є тілом.

Теорема 1. *Нехай A — скінченно вимірна алгебра з одиницею над алгебраїчно замкнутим полем F. Якщо алгебра A є тілом, то вона ізоморфна полю F.*

Теорема Фробеніуса. *Нехай A — скінченно вимірна алгебра з одиницею над полем $\mathbb{R}$ дійсних чисел. Якщо алгебра A є тілом, то вона ізоморфна одній із таких алгебр: $\mathbb{R}$, $\mathbb{C}$, $\mathbb{H}$.*

П р и к л а д и

1. *Нехай F — довільне поле, $F[x]$ — кільце многочленів від однієї невідомої x з коефіцієнтами з поля F. Показати, що $F[x]$ є нескінченно вимірною алгеброю над полем F.*

Розв'язання. Очевидно, $F[x]$ є алгеброю над полем F. Припустимо, що $F[x]$ — скінченно вимірна алгебра над полем F. Тоді знайдуться такі

многочлени $f_i(x) \in F[x]$, $(i = 1, \ldots, n)$, що довільний многочлени $f(x) \in$ $\in F[x]$ представляється у вигляді

$$f(x) = \lambda_1 f_1(x) + \cdots + \lambda_n f_n(x) \quad (\lambda_i \in F;\ i = 1, \ldots, n). \tag{1}$$

Не зменшуючи загальності будемо вважати, що $f_i(x) \neq 0$, $(i = 1, \ldots, n)$. Нехай m — найбільша степінь многочленів $f_i(x)$, $(i = 1, \ldots, n)$. Очевидно, многочлен $f_0 = x^{m+1} \in F[x]$ у вигляді (1) не представляється. Таким чином, $F[x]$ не є скінченно вимірною алгеброю над полем F.

2. *Нехай F — поле, $F_{n\times n}$ — множина всіх матриць порядку n над полем F. Показати, що $F_{n\times n}$ є алгеброю розмірності n^2 над полем F.*

Розв'язання. Очевидно, відносно операцій додавання і множення матриць, та операції множення елемента поля F на матрицю множина $F_{n\times n}$ є алгеброю над полем F. Покажемо, що розмірність цієї алгебри над полем F дорівнює n^2. Дійсно, легко перевірити лінійну незалежність системи матриць $\{e_{ij} \mid i, j = 1, \ldots, n\}$ над полем F, де e_{ij} $(i, j = 1, \ldots, n)$ — це матриця порядку n, в якій на перетині i-ого рядка та j-ого стовпця стоїть 1, а всі інші елементи дорівнюють нулю. Всяка матриця $a = ||\alpha_{ij}|| \in F_{n\times n}$ однозначно представляється у вигляді $a = \sum_{i,j=1}^{n} \alpha_{ij} e_{ij}$. Отже, $\dim_F F_{n\times n} = n^2$.

В п р а в и

1. Показати, що поле $\mathbb{C} = \mathbb{R}(i)$ $(i^2 = -1)$ комплексних чисел є алгеброю розмірності 2 над полем $\mathbb{R}$.

2. Знайти в алгебрі кватерніонів $\mathbb{H}$ обернені елементи до таких елементів: а) $1 + i + j$; б) $i + j$; в) $2 - i - j$; г) $1 - k$.

3. Розв'язати в алгебрі кватерніонів $\mathbb{H}$ рівняння: а) $x^2 = -1$; б) $(1 + j)x = j - k$; в) $(i + j + k)x = 1 - k$.

4. Нехай A — алгебра над полем $\mathbb{C}$ комплексних чисел з базисом e, i, j, k і з такою ж таблицею множення, як і в алгебрі кватерніонів. Знайти в алгебрі A дільники нуля.

5. Знайти розмірність алгебри $T(n, \mathbb{R})$ всіх верхніх трикутних матриць порядку $n \geq 2$ над полем $\mathbb{R}$.

6. Показати, що множина діагональних матриць порядку n над полем $\mathbb{R}$ є алгеброю над $\mathbb{R}$. Знайти розмірність цієї алгебри.

7. Довести, що множина матриць вигляду

$$\begin{pmatrix} a + bi & c + di \\ -c + di & a - bi \end{pmatrix} \quad (a, d, c, d \in \mathbb{R};\ i^2 = -1)$$

є алгеброю над полем $\mathbb{R}$ розмірності 4. Показати, що ця алгебра ізоморфна алгебрі кватерніонів $\mathbb{H}$.

§21. Про зображення груп

Нехай G — група, F — поле, $GL(n,F)$ — повна лінійна група степеня n над полем F. Гомоморфізм Δ групи G в групу $GL(n,F)$ називається *матричним F-зображенням степеня n* групи G. Матричні F-зображення Δ і Γ степеня n групи G називаються *F-еквівалентними*, якщо існує така матриця $C \in GL(n,F)$, що $C^{-1}\Delta(g)C = \Gamma(g)$ для довільного елемента $g \in G$. Матричне F-зображення степеня n групи G називається *звідним* над полем F, якщо воно F-еквівалентне зображенню Γ вигляду:

$$\Gamma : g \to \Gamma(g) = \begin{pmatrix} \Gamma_1(g) & T(g) \\ 0 & \Gamma_2(g) \end{pmatrix} \quad (g \in G),$$

де Γ_i — матричне F-зображення степеня n_i групи G ($n_i < n$, $i = 1, 2$). В протилежному випадку зображення Δ називається *незвідним* над полем F. Матричне F-зображення Δ групи G називається *цілком звідним* над полем F, якщо воно F-еквівалентне зображенню Γ вигляду:

$$\Gamma : g \to \Gamma(g) = \begin{pmatrix} \Gamma_1(g) & & \mathbf{0} \\ & \ddots & \\ \mathbf{0} & & \Gamma_r(g) \end{pmatrix} \quad (g \in G),$$

де Γ_i $(i = 1, \ldots, r)$ — незвідне матричне F-зображення групи G.

Теорема Машке. *Нехай G — скінченна група порядку $|G|$, F — поле характеристики $p \geq 0$. Якщо p не ділить $|G|$, то довільне матричне F-зображення групи G цілком звідне над полем F.*

Нехай $\mathbb{C}$ — поле комплексних чисел і G — скінченна група. Тоді степінь незвідного матричного $\mathbb{C}$-зображення групи G ділить порядок групи G. Якщо G — абелева група, то всі незвідні матричні $\mathbb{C}$-зображення групи G мають степінь 1 і число нееквівалентних незвідних $\mathbb{C}$-зображень групи G дорівнює порядку групи G.

Нехай M — n-вимірний лінійний простір над полем F, $GL(M)$ — група всіх оборотних лінійних операторів простору M. Відмітимо, що групи $GL(M)$ і $GL(n,F)$ ізоморфні. Гомоморфізм Φ групи G в групу $GL(M)$ називається *зображенням групи G лінійними операторами* простору M. Будемо говорити, що зображення Φ реалізується в просторі M.

Зображення $\Phi : g \to \Phi_g$ і $\Phi' : g \to \Phi'_g$ групи G, які реалізуються відповідно в просторах M і M' над полем F, називаються *еквівалентними*,

якщо існує такий ізоморфізм φ простору M на M', що $\varphi\Phi_g = \Phi'_g\varphi$ для довільного елемента $g \in G$.

Нехай M — лінійний простір над полем F, в якому реалізується зображення Φ групи G. Підпростір T простору M називається *G-підпростором* простору M, якщо $\Phi_g(m) \in T$ для довільних елементів $g \in G$ і $m \in T$. Зображення $\Phi : G \to GL(M)$ групи G називається *незвідним*, якщо простір M містить тільки тривіальні G-підпростори $\{0\}$ і M.

Існує тісний зв'язок між матричними F-зображеннями групи G і зображеннями групи G лінійними операторами. Якщо вибрати фіксований базис в n-вимірному лінійному просторі M над полем F, то зображенню $\Phi : G \to GL(M)$ буде відповідати певне матричне зображення $\widetilde{\Phi} : G \to GL(n, F)$. Зображення Φ групи G незвідне тоді і тільки тоді, коли відповідне йому матричне зображення $\widetilde{\Phi}$ групи G незвідне над полем F.

П р и к л а д и

1. *Знайти всі незвідні матричні $\mathbb{C}$-зображення циклічної групи $G = \langle a \rangle$ порядку n.*

Розв'язання. Як відомо, незвідні матричні $\mathbb{C}$-зображення групи $G = \langle a \rangle$ мають степінь один. Далі, відображення $\Delta : G \to GL(1, \mathbb{C})$ є зображенням тоді і тільки тоді, коли $\Delta(a^l) = \lambda^l$ $(l = 0, 1, \ldots, n-1)$, де $\lambda^n = 1$ $(\lambda \in \mathbb{C}^*)$. Отже, всі незвідні нееквівалентні $\mathbb{C}$-зображення групи G вичерпуються такими зображеннями: $\Delta_j : a \to \varepsilon^j$ $(j = 0, 1, \ldots, n-1)$, де ε — первісний корінь степеня n із одиниці.

2. *Знайти всі незвідні матричні $\mathbb{C}$-зображення абелевої групи $G = G_1 \times G_2$, де $G_i = \langle a_i \rangle$ — циклічна група порядку n_i $(i = 1, 2)$.*

Розв'язання. Як відомо, кожне незвідне матричне $\mathbb{C}$-зображення Γ групи G має степінь 1. Звідси і із прикладу 1 випливає, що Γ має вигляд:

$$\Gamma = \Gamma_{ij} : a_1 \to \Gamma_{ij}(a_1) = \varepsilon_1^i, \quad a_2 \to \Gamma_{ij}(a_2) = \varepsilon_2^j,$$

де $i \in \{0, 1, \ldots, n_1 - 1\}$; $j \in \{0, 1, \ldots, n_2 - 1\}$; ε_r — первісний корінь степеня n_r з одиниці $(r = 1, 2)$. Неважко показати, що зображення Γ_{ij} і Γ_{kl} $(i, k \in \{0, \ldots, n_1 - 1\}$; $j, l \in \{0, \ldots, n_2 - 1\})$ $\mathbb{C}$-еквівалентні тоді і тільки тоді, коли $i = k$, $j = l$.

3. *Показати, що скінченна група G порядку n має точне матричне $\mathbb{C}$-зображення Γ степеня n, тобто таке $\mathbb{C}$-зображення Γ, що* $\operatorname{Ker}\Gamma = \{e\}$ *(e — одиничний елемент групи G).*

Розв'язання. Нехай g_1, g_2, …, g_n — всі елементи групи G і M — n-вимірний лінійний простір над полем $\mathbb{C}$ з базисом g_1, g_2, …, g_n. Позна-

чимо через Γ'_g $(g \in G)$ лінійний оператор простору M, який визначається в такий спосіб:

$$\Gamma'_g(g_i) = g \cdot g_i \quad (i = 1, \ldots, n), \quad \Gamma'_g\left(\sum_{i=1}^{n} \alpha_i g_i\right) = \sum_{i=1}^{n} \alpha_i \Gamma'_g(g_i), \quad (\alpha_i \in \mathbb{C}).$$

Нехай Γ_g — матриця лінійного оператора Γ'_g в базисі $g_1, \ldots, g_n$. Неважко показати, що відображення $\Gamma : g \to \Gamma_g$ $(g \in G)$ є матричним $\mathbb{C}$-зображенням степеня n групи G. Покажемо, що це зображення є точним. Нехай $g \in \operatorname{Ker}\Gamma$. Тоді $\Gamma'_g(g_i) = g_i$ $(i = 1, \ldots, n)$. Тому $g \cdot g_i = g_i$ $(i = 1, \ldots, n)$. Отже, $g = e$, тобто $\operatorname{Ker}\Gamma = \{e\}$.

4. *Показати, що скінченна неабелева група має принаймні одне незвідне матричне $\mathbb{C}$-зображення степеня $m > 1$.*

Розв'язання. Нехай G — скінченна неабелева група порядку n. Із прикладу 3 випливає, що група G має точне матричне $\mathbb{C}$-зображення Γ степеня n. Припустимо, що всі незвідні матричні $\mathbb{C}$-зображення групи G мають степінь 1. Тоді за теоремою Машке зображення Γ $\mathbb{C}$-еквівалентне зображенню Γ' вигляду:

$$\Gamma' : \ g \to \Gamma'(g) = \begin{pmatrix} \alpha_1(g) & & 0 \\ & \ddots & \\ 0 & & \alpha_n(g) \end{pmatrix} \quad \begin{pmatrix} \alpha_i(g) \in \mathbb{C}^*; \ g \in G; \\ i = 1, \ldots, n \end{pmatrix}.$$

Звідси випливає, що група $\overline{G} = \{\Gamma'(g) \mid g \in G\}$ є абелевою групою. З іншого боку, враховуючи, що зображення Γ' — точне, маємо, що $G \cong \overline{G}$. Ми одержали протиріччя, оскільки група G — неабелева. Отже, не всі незвідні матричні $\mathbb{C}$-зображення неабелевої скінченної групи G мають степінь 1.

5. *Нехай $G = \mathbb{Z}^+$. Показати, що відображення*

$$\Gamma : n \to \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \quad (n \in G)$$

є матричним $\mathbb{C}$-зображенням групи G і це зображення не є цілком звідним над полем $\mathbb{C}$.

Розв'язання. Нехай n і m — довільні елементи групи G. Тоді

$$\Gamma(n+m) = \begin{pmatrix} 1 & n+m \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix} = \Gamma(n) \cdot \Gamma(m).$$

Отже, відображення Γ є $\mathbb{C}$-зображенням групи G. Покажемо, що це зображення не є цілком звідним над полем $\mathbb{C}$. Припустимо, що зображення

Γ — цілком звідне зображення над полем $\mathbb{C}$. Тоді воно $\mathbb{C}$-еквівалентне зображенню Γ' вигляду:

$$\Gamma' : n \to \begin{pmatrix} \alpha(n) & 0 \\ 0 & \beta(n) \end{pmatrix} \quad (\alpha(n), \beta(n) \in \mathbb{C}^*,\ n \in G).$$

Значить, існує така матриця $C \in GL(2, \mathbb{C})$, що $C^{-1}\Gamma(n)C = \Gamma'(n)$ для довільного елемента $n \in G$. Тоді матриці

$$\Gamma(1) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix},\ \Gamma'(1) = \begin{pmatrix} \alpha(1) & 0 \\ 0 & \beta(1) \end{pmatrix}$$

подібні над полем $\mathbb{C}$. Ці матриці є нормальними формами Жордана, які є різними з точністю до порядку розташування клітинок Жордана. Отже, матриці $\Gamma(1)$, $\Gamma'(1)$ не є подібними. Одержане протиріччя показує, що зображення Γ не є цілком звідним над полем $\mathbb{C}$.

В п р а в и

1. Показати, що циклічна 2-група порядку 2^n $(n > 1)$ має незвідне матричне $\mathbb{Q}$-зображення степеня 2.

2. Знайти всі незвідні матричні $\mathbb{C}$-зображення всіх абелевих груп порядку 12.

3. Довести, що якщо скінченна абелева група G має точне незвідне матричне $\mathbb{C}$-зображення, то G — циклічна група.

4. Показати, що точне матричне $\mathbb{C}$-зображення другого степеня скінченної неабелевої групи є незвідним.

5. Показати, що група S_3 всіх підстановок 3-го степеня має точне матричне $\mathbb{C}$-зображення степеня 3.

6. Нехай F_p — поле характеристики p $(p > 0)$. Довести, що всяке незвідне матричне F_p-зображення Γ циклічної p-групи G має вигляд: $\Gamma : g \to 1$ $(g \in G)$.

7. Нехай F_p — поле характеристики $p > 0$ і $H = \langle a \rangle$ — циклічна група порядку p. Показати, що матричне F_p-зображення

$$\Gamma : a \to \Gamma(a) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

групи $H = \langle a \rangle$ не є цілком звідним над полем F_p.

8. Нехай V — n-вимірний векторний простір над полем F з базисом $e_1, \ldots, e_n$. Задамо відображення $\Phi : S_n \to GL(V)$, за правилом

$\Phi : \ \sigma \to \Phi_\sigma$ ($\sigma \in S_n$, $\Phi_\sigma \in GL(V)$), де $\Phi_\sigma(e_i) = e_{\sigma(i)}$ ($i = 1, \ldots, n$). Довести, що Φ — зображення групи S_n лінійними операторами простору V.

Література

1. *Ван дер Варден Б.Л.* Алгебра. – М.: Наука, 1979.
2. *Виноградов И.М.* Основы теории чисел. – М.: Наука, 1981.
3. *Дрозд Ю.А., Кириченко В.В.* Конечномерные алгебры. – К.: Вища школа, 1980.
4. *Завало С.Т.* Курс алгебри. – К.: Вища школа, 1985.
5. *Калужнин Л.А.* Введение в общую алгебру. – М.: Наука, 1973.
6. *Каргаполов М.И., Мерзляков Ю.И.* Основы теории групп. – М.: Наука, 1982.
7. *Кострикин А.И.* Введение в алгебру. – М.: Наука, 1977.
8. *Курош А.Г.* Курс высшей алгебры. – М.: Наука, 1971.
9. *Скорняков Л.А.* Элементы общей алгебры. – М.: Наука, 1983.
10. *Фаддеев Д.К.* Лекции по алгебре. – М.: Наука, 1984.
11. *Проскуряков И.В.* Сборник задач по линейной алгебре. – М.: Наука, 1974.
12. *Фаддеев Д.К., Соминский И.С.* Сборник задач по высшей алгебре. – М.: Наука, 1977.
13. Сборник задач по алгебре / Под редакцией Кострикина А.И. – М.: Наука, 1987.

Предметний показчик

Позначення

$\mathbb{N}$ — множина всіх натуральних чисел,
$\mathbb{Z}$ — множина всіх цілих чисел,
$\mathbb{Q}$ — множина всіх раціональних чисел,
$\mathbb{R}$ — множина всіх дійсних чисел,
$\mathbb{C}$ — множина всіх комплексних чисел,
$f : M_1 \to M_2$ — відображення f множини M_1 в множину M_2,
$f(M_1)$ — образ відображення f,
$|G|$ — порядок групи G,
$H \lhd G$ — H нормальна підгрупа групи G,
G/H — фактор-група групи G за підгрупою H,
$G_1 \dot{\times} G_2$ — зовнішній прямий добуток груп G_1 і G_2,
$G_1 \dot{+} G_2$ — зовнішня пряма сума груп G_1 і G_2,
$G = G_1 \times G_2$ — внутрішній прямий добуток підгруп G_1 і G_2 групи G,
$G = G_1 \oplus G_2$ — внутрішня пряма сума підгруп G_1 і G_2 групи G,
S_n — симетрична група степеня n,
A_n — знакозмінна група степеня n,
$GL(n, F)$ — повна лінійна група степеня n над полем F,
$SL(n, F)$ — спеціальна лінійна група степеня n над полем F,
$\det A$ — детермінант матриці A,
K^+ — адитивна група кільця K,
K^* — мультиплікативна група кільця K з одиницею,
K/V — фактор-кільце комутативного кільця K за ідеалом V,
$K[x]$ — кільце поліномів від однієї невідомої x над комутативним кільцем K з одиницею,
$\mathbb{Z}_m$ — кільце класів лишків за модулем m,
$K_{n\times n}$ — кільце всіх матриць порядку n з елементами із комутативного кільця K,
$F(\theta)$ — просте розширення поля F,
$A \cup B$ — об'єднання множин A і B,
$A \cap B$ — переріз множин A і B,
$A \setminus B$ — різниця множин A і B.

ГУДИВОК Петро Михайлович
КИРИЛЮК Олександр Антонович
ПОГОРІЛЯК Євгенія Яківна
ТИЛИЩАК Олександр Андрійович
ЮРЧЕНКО Наталія Василівна

ПРАКТИКУМ З АЛГЕБРИ І ТЕОРІЇ ЧИСЕЛ