Міністерство освіти і науки України

Прикарпатський національний університет
імені Василя Стефаника

Володимир Гаврилків

Елементи теорії груп та теорії кілець

Навчальний посібник
для студентів спеціальностей
“Математика”, “Статистика”,
“Середня освіта(математика)”

Івано-Франківськ

2024

УДК 512.5
ББК 22.144
Г 12

Гаврилків В.М. Елементи теорії груп та теорії кілець: навчальний посібник. Вид. друге, доповн. / В.М. Гаврилків. — Івано-Франківськ: Голіней, 2024. — 152 с.

У навчальному посібнику у вигляді курсу з 15 лекцій викладено основи теорії груп та теорії кілець. Наведено велику кількість ілюстративних прикладів, які пояснюють і розширюють теоретичний матеріал. Кожна лекція супроводжується вправами для самостійного розв'язування.

Для студентів спеціальностей "Математика", "Статистика" та "Середня освіта(математика)" закладів вищої освіти.

Рекомендовано Вченою радою факультету математики та інформатики як навчальний посібник для студентів спеціальностей "Математика", "Статистика" та "Середня освіта(математика)".

Рецензенти: доктор фізико-математичних наук, професор
Артемович Орест Дем'янович, професор факультету прикладної математики Сілезької Політехніки (Польща);
доктор фізико-математичних наук, старший науковий співробітник
Любашенко Володимир Васильович, провідний науковий співробітник Інституту математики НАН України.

Зміст

Передмова 4

Розділ I. Елементи теорії груп 5
Лекція 1. Означення групи. Підгрупи 5
Лекція 2. Симетрична група та її підгрупи 18
Лекція 3. Порядок елемента групи. Циклічні підгрупи 28
Лекція 4. Розбиття групи за підгрупою. Теорема Лагранжа 35
Лекція 5. Нормальні підгрупи. Факторгрупи 42
Лекція 6. Морфізми груп. Теорема Келі 50
Лекція 7. Дія групи на множині. Центр групи 61
Лекція 8. Комутант групи. Розв'язні групи 70
Лекція 9. Прямі добутки груп 78
Лекція 10. Теореми Силова та їх застосування 86

Розділ II. Елементи теорії кілець 99
Лекція 1. Основні означення. Класи кілець 99
Лекція 2. Гомоморфізми та ідеали кілець 108
Лекція 3. Евклідові кільця. Подільність 119
Лекція 4. Конгруенції в кільці цілих чисел. Теорема Ейлера 128
Лекція 5. Конгруенції з одним невідомим. Теорема Вільсона 137

Список літератури 149

Предметний покажчик 150

Передмова

На початку минулого століття алгебра утвердилася як теоретико-множинна, аксіоматична наука, для якої основним об'єктом вивчення є алгебраїчні операції, що виконуються над елементами довільної природи. Відомо, наскільки значним, а іноді і вирішальним був подальший вплив сучасної алгебри на розвиток багатьох галузей математики, з яких насамперед слід виділити топологію і функціональний аналіз. Різноманітні алгебраїчні структури виникають практично у всіх математичних курсах, включно з прикладними. Останні посилюють актуальність вивчення алгебри з огляду на всепроникні цифрові технології та стрімкий розвиток комп'ютерних наук. Навчальний посібник присвячено класичним алгебраїчним структурам, які студенти опановують на молодших курсах університетської підготовки. Його метою є ознайомлення читача з основами теорії груп та теорії кілець.

Загальновизнано, що найкращий спосіб вивчення математики ґрунтується на розв'язуванні прикладів і практичних задач. Практичний підхід до викладення матеріалу не тільки допомагає вивчити методи та інструменти для розв'язання задач, а й зміцнює розуміння основних понять. Книзі притаманний послідовний опис теорії з великою кількістю ілюстративних прикладів. Вона містить близько 500 вправ, які пояснюють і розширюють теоретичний матеріал.

У навчальний посібник включено лекції з теорії груп та теорії кілець, які автор читає у курсі алгебри та теорії чисел для студентів спеціальностей "Математика", "Статистика" та "Середня освіта(математика)" на факультеті математики та інформатики Прикарпатського національного університету імені Василя Стефаника. Посібник складається з 15 лекцій, поділених на два розділи. У першому розділі розглянуто основи теорії груп. Другий розділ містить виклад основних понять і фактів, пов'язаних з кільцями. Важливі поняття та теореми проілюстровано численними прикладами. Кожну лекцію доповнено ретельно підібраними вправами, які є основою для проведення практичного заняття з даної теми, а також можуть бути використані при складанні аудиторних і домашніх контрольних робіт. Посібник може використовуватись також як довідник, чому сприяє детальний предметний покажчик.

Розділ I

Елементи теорії груп

Лекція 1. Означення групи. Підгрупи

Бінарною операцією, заданою на множині X, називається відображення $* : X \times X \to X$, де $X \times X$ – множина всіх впорядкованих пар елементів з X. Для спрощення запису образ $*(a, b) \in X$ елемента $(a, b) \in X \times X$ позначатимемо через $a * b$ і називатемемо *добутком* елементів a і b.

Бінарна операція $*$ на множині X називається *асоціативною*, якщо $a * (b * c) = (a * b) * c$ для всіх $a, b, c \in X$. Пара $(S, *)$, де S – множина, а $*$ – асоціативна бінарна опрерація на S, називається *напівгрупою*. Якщо з контексту зрозуміло про яку операцію $*$ на множині S йде мова, то замість $a * b$ писатимемо ab, а замість $(S, *)$ – S.

Приклад 1.1. Розглянемо множину $\mathbb{N}$ натуральних чисел і арифметичні бінарні операції $+, -, \cdot$. Оскільки $a+b, a \cdot b \in \mathbb{N}$ для будь-яких $a, b \in \mathbb{N}$, то операції $+$ і $\cdot$ є заданими на множині $\mathbb{N}$. Проте різниця -1 натуральних чисел 1 і 2 не є натуральним числом, а отже, операція $-$ не є заданою на множині $\mathbb{N}$.

Оскільки $a + (b + c) = (a + b) + c$ і $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ для будь-яких $a, b, c \in \mathbb{N}$, то пари $(\mathbb{N}, +)$ і $(\mathbb{N}, \cdot)$ є напівгрупами.

Якщо $a * b = b * a$ для всіх $a, b \in X$, то бінарна операція $*$ називається *комутативною* на X.

Приклад 1.2. Бінарна операція $*$, задана на множині $\mathbb{Z}$ правилом $a * b = -(a + b)$, є комутативною, але не є асоціативною. Дійсно,

$$a * b = -(a + b) = -(b + a) = b * a,$$

$$a * (b * c) = a * (-(b + c)) = -(a - (b + c)) = -a + b + c,$$

$$(a * b) * c = (-(a + b)) * c = -(-(a + b) + c) = a + b - c.$$

Таким чином, пара $(\mathbb{Z}, *)$ не є напівгрупою.

Твердження 1.1.

У напівгрупі S результат застосування операції до декількох елементів не залежить від способу розстановки дужок.

Доведення. Нехай $a_1, a_2, \ldots, a_n \in S$. Не міняючи порядку слідування елементів, можна різними способами знаходити добуток цих елементів. Для $n \leqslant 4$ можна утворити наступні добутки:

$n = 1$ a_1;
$n = 2$ a_1a_2;
$n = 3$ $(a_1a_2)a_3, a_1(a_2a_3)$;
$n = 4$ $((a_1a_2)a_3)a_4, (a_1(a_2a_3))a_4, a_1((a_2a_3)a_4), a_1(a_2(a_3a_4)), (a_1a_2)(a_3a_4)$.

Оскільки бінарна операція є асоціативною, то $(a_1a_2)a_3 = a_1(a_2a_3)$. Для $n = 4$, використовуючи асоціативність, легко перевірити, що всі п'ять добутків співпадають.

Продовжимо доведення індукцією за $n \in \mathbb{N}$. Вважаємо, що для кількості елементів $< n$ твердження вірне. Потрібно довести, що

$$(a_1 \ldots a_k)(a_{k+1} \ldots a_n) = (a_1 \ldots a_s)(a_{s+1} \ldots a_n)$$

для будь яких $k, s \in \{1, \ldots, n-1\}$.

За припущенням індукції всередині дужок добутки визначаються однозначно. Не обмежуючи загальності можна вважати, що $k > s$. Тоді

$$(a_1 \ldots a_k)(a_{k+1} \ldots a_n) = ((a_1 \ldots a_s)(a_{s+1} \ldots a_k))(a_{k+1} \ldots a_n) =$$
$$(a_1 \ldots a_s)((a_{s+1} \ldots a_k)(a_{k+1} \ldots a_n)) = (a_1 \ldots a_s)(a_{s+1} \ldots a_n).$$

□

У випадку $a_1 = a_2 = \ldots a_n = a$ добуток $a_1 * a_2 * \ldots * a_n$ позначається через a^n і називається *n-м степенем елемента a*. З твердження 1.1 випливає, що виконуються звичайні правила піднесення до степеня, а саме, $a^m * a^n = a^{m+n}$, $(a^m)^n = a^{mn}$ для всіх $m, n \in \mathbb{N}$.

Елемент e напівгрупи $(S, *)$ називається *лівою* (*правою*) *одиницею*, якщо $e * a = a$ $(a * e = a)$ для всіх $a \in S$. Елемент $e \in S$ називається *одиницею*, якщо e є як лівою, так і правою одиницею напівгрупи S.

Напівгрупа, яка містить одиницю, називається *моноїдом*. Зауважимо, що $f = e*f = e$ для кожної лівої одиниці e і правої одиниці f напівгрупи S. Звідси випливає, що моноїд містить єдину одиницю. Якщо e – одиниця моноїда M, то домовимося, що $a^0 = e$ для кожного елемента $a \in M$.

Елемент $e \in S$ називається *ідемпотентом*, якщо $e * e = e$. Зрозуміло, що одиниця напівгрупи є ідемпотентом.

Приклад 1.3. У напівгрупі $(\mathbb{Z}, \cdot)$ рівняння $x^2 = x$ має два розв'язки 0 і 1, які є ідемпотентами. Оскільки $a \cdot 1 = 1 \cdot a = a$ для кожного $a \in \mathbb{Z}$, то число 1 є одиницею моноїда $(\mathbb{Z}, \cdot)$.

Елемент a моноїда $(M, *)$ називається *оборотним зліва* (*справа*), якщо існує такий елемент $b \in M$, що $b * a = e$ ($a * b = e$). Якщо $a * b = e$, то елемент a називається *лівим оберненим* до елемента b, а b – *правим оберненим* до a. Елемент, оборотний як зліва, так і справа, називається *оборотним*.

Приклад 1.4. У моноїді $(\mathbb{R}, \cdot)$ для кожного дійсного числа $a \neq 0$ рівняння $a \cdot x = 1$ і $x \cdot a = 1$ мають єдиний розв'язок $x = \frac{1}{a} \in \mathbb{R}$, а тому всі елементи $a \neq 0$ є оборотними. Рівняння $0 \cdot x = 1$ і $x \cdot 0 = 1$ розв'язків не мають, а отже, 0 не є оборотним.

Напівгрупа G називається *групою*, якщо

1) G містить ліву одиницю, тобто існує $e \in G$, що $e * a = a$ для кожного $a \in G$;
2) кожен елемент $a \in G$ є оборотним зліва, тобто для кожного $a \in G$ існує $x \in G$, що $x * a = e$.

Нехай G – група, x – лівий обернений до елемента $a \in G$. З аксіом 1), 2) випливає, що $x * (a * x) = (x * a) * x = e * x = x$. Якщо рівність $x * (a * x) = x$ домножити зліва на лівий обернений до x, то отримаємо, що $e * a * x = e$, звідки $a * x = e$. Таким чином, в групі G кожен лівий обернений до елемента a є також і правим оберненим. Оскільки $a * e = a * x * a = e * a = a$, то кожна ліва одиниця є одночасно і правою одиницею групи G.

Нехай b_1 і b_2 – обернені елементи до елемента a групи G, тоді

$$b_1 = b_1 * e = b_1 * (a * b_2) = (b_1 * a) * b_2 = e * b_2 = b_2.$$

Таким чином, для кожного елемента a групи G існує єдиний обернений елемент, який позначимо через a^{-1}. Зрозуміло, що $(a^{-1})^{-1} = a$. Оскільки

$$(a * b) * (b^{-1} * a^{-1}) = a * (b * b^{-1}) * a^{-1} = a * a^{-1} = e,$$

то $(a * b)^{-1} = b^{-1} * a^{-1}$ для кожних $a, b \in G$.

Приклад 1.5. Покажемо, що пара $(\mathbb{Z}, *)$, де $a * b = a + b - 2024$ є групою.

1) Оскільки $a * b = a + b - 2024 \in \mathbb{Z}$ для кожних $a, b \in \mathbb{Z}$, то бінарна операція $*$ є заданою на множині $\mathbb{Z}$.

2) З рівностей $a * (b * c) = a * (b + c - 2024) = a + (b + c - 2024) - 2024 = a + b + c - 4048 = (a + b - 2024) + c - 2024 = (a * b) + c - 2024 = (a * b) * c$ випливає, що операція $*$ є асоціативною, а тому пара $(\mathbb{Z}, *)$ – напівгрупа.

3) Припустимо, що напівгрупа містить ліву одиницю e. Тоді $e*a=a$ для кожного $a\in\mathbb{Z}$. Звідки $e+a-2024=a$ і $e=2024$.

4) Для кожного елемента $a\in\mathbb{Z}$ розглянемо рівняння $x*a=e$, яке має вигляд $x+a-2024=2024$. Оскільки дане рівняння має розв'язок $x=4048-a\in\mathbb{Z}$, то кожен елемент $a\in\mathbb{Z}$ є оборотним зліва.

Таким чином, пара $(\mathbb{Z},*)$ є групою.

Приклад 1.6. Доведемо, що пара $(G,\circ)$, де

$$G=(\mathbb{Q}\backslash\{0\})\times\mathbb{Q},\quad (a_1,b_1)\circ(a_2,b_2)=(a_1a_2,a_1b_2+b_1),$$

є групою.

1) Якщо $(a_1,b_1),(a_2,b_2)\in G$, то $a_1\neq 0$ і $a_2\neq 0$, звідки $a_1a_2\neq 0$ і $(a_1,b_1)\circ(a_2,b_2)=(a_1a_2,a_1b_2+b_1)\in G$.

2) З рівностей $(a_1,b_1)\circ[(a_2,b_2)\circ(a_3,b_3)]=(a_1,b_1)\circ(a_2a_3,a_2b_3+b_2)=(a_1a_2a_3,a_1(a_2b_3+b_2)+b_1)=(a_1a_2a_3,a_1a_2b_3+a_1b_2+b_1)$ та $[(a_1,b_1)\circ(a_2,b_2)]\circ(a_3,b_3)=(a_1a_2,a_1b_2+b_1)\circ(a_3,b_3)=(a_1a_2a_3,a_1a_2b_3+a_1b_2+b_1)$ випливає, що пара $(G,\circ)$ є напівгрупою.

3) Припустимо, що напівгрупа містить ліву одиницю $e=(x_1,x_2)$. Тоді $e\circ a=a$ для кожного $a=(a_1,a_2)\in G$. Звідки $(x_1,x_2)\circ(a_1,a_2)=(a_1,a_2)$, а отже, $(x_1a_1,x_1a_2+x_2)=(a_1,a_2)$. Таким чином, $x_1a_1=a_1$ і $x_1a_2+x_2=a_2$, а тому $e=(x_1,x_2)=(1,0)\in G$.

4) Для кожного елемента $a=(a_1,a_2)\in G$ розглянемо рівняння $x*a=e$. Нехай $x=(x_1,x_2)$. Тоді рівняння набуде вигляду $(x_1,x_2)\circ(a_1,a_2)=(1,0)$. Звідки $x_1a_1=1$ і $x_1a_2+x_2=0$, а отже, $(x_1,x_2)=(\frac{1}{a_1},-\frac{a_2}{a_1})\in G$.

Таким чином, кожен елемент $a\in G$ має лівий обернений, а тому пара $(G,\circ)$ є групою.

Група G називається *абелевою*, якщо всі її елементи *комутують*, в тому сенсі, що $a*b=b*a$ для кожних $a,b\in G$. Таким чином, група з прикладу 1.5 є абелевою, а з прикладу 1.6 не є абелевою.

Приклад 1.7. Матричні групи.

Через $M(n,\mathbb{R})$ позначається множина всіх квадратних $n\times n$-матриць з дійсними елементами. Зрозуміло, що $M(n,\mathbb{R})$ з операцією множення матриць є моноїдом з одиницею E. Оскільки тільки невироджені матриці мають оберенені, то $M(n,\mathbb{R})$ не є групою.

Нехай $GL(n,\mathbb{R})=\{A\in M(n,\mathbb{R})\mid \det A\neq 0\}$. Тоді $GL(n,\mathbb{R})$ – група, яку називають *повною* або *загальною лінійною групою степеня n над* $\mathbb{R}$.

$SL(n,\mathbb{R}) = \{A \in GL(n,\mathbb{R}) \mid \det A = 1\}$ – група, яка називається *спеціальною лінійною групою степеня n над $\mathbb{R}$.*

Визначимо від'ємні цілі степені елемента a групи G як обернені до додатних степенів, тобто покладемо $a^{-n} := (a^n)^{-1}$ для всіх $n \in \mathbb{N}$.

Твердження 1.2.

$(a^s)^{-1} = (a^{-1})^s = a^{-s}$ для кожного елемента a групи G і кожного $s \in \mathbb{Z}$.

Доведення. Нехай $s > 0$.

Тоді $a^{-s} = (a^s)^{-1} = (\underbrace{a \dots a}_{s})^{-1} = \underbrace{a^{-1} \dots a^{-1}}_{s} = (a^{-1})^s$.

Якщо $s = 0$, то $(a^s)^{-1} = e = (a^{-1})^s = a^{-s}$.

Нехай $s < 0$. Тоді

$$(a^s)^{-1} = ((a^{-1})^{|s|})^{-1} = ((a^{|s|})^{-1})^{-1} = a^{|s|} = a^{-s} \quad \text{і}$$
$$(a^{-1})^s = (a^{-1})^{-|s|} = ((a^{-1})^{|s|})^{-1} = ((a^{|s|})^{-1})^{-1} = a^{|s|} = a^{-s}.$$

□

Твердження 1.3.

Для кожного елемента a групи G і будь-яких $s,t \in \mathbb{Z}$ мають місце рівності:

$$a^s a^t = a^{s+t}, \quad (a^s)^t = a^{st}.$$

Доведення. Для натуральних показників ці рівності отримано раніше. Якщо один з показників дорівнює нулю, то очевидно, що рівності також виконуються.

Нехай $s < 0$ і $t < 0$. Тоді

$$a^s a^t = a^{-|s|} a^{-|t|} = (a^{-1})^{|s|} (a^{-1})^{|t|} = (a^{-1})^{|s|+|t|} = a^{s+t};$$
$$(a^s)^t = (a^{-|s|})^t = ((a^{|s|})^{-1})^t = (a^{|s|})^{-t} = (a^{|s|})^{|t|} = a^{|s||t|} = a^{st}.$$

Якщо $s < 0$ і $t > 0$, то

$$a^s a^t = a^{-|s|} a^t = \underbrace{a^{-1} \dots a^{-1}}_{|s|} \underbrace{a \dots a}_{t} = a^{t-|s|} \text{ (або } (a^{-1})^{|s|-t} \text{ при } |s| \geqslant t) = a^{t+s};$$

$$(a^s)^t = \underbrace{a^s \dots a^s}_{t} = \underbrace{a^{-1} \dots a^{-1}}_{|s|} \dots \underbrace{a^{-1} \dots a^{-1}}_{|s|} = (a^{-1})^{|s|t} = a^{st}.$$

Випадок $s > 0$ і $t < 0$ перевіряється аналогічно. □

Непорожня множина X з визначеною на ній операцією $*$ називається *квазігрупою*, якщо для кожних $a, b \in X$ система рівнянь $a * x = b$ і $y * a = b$ має єдиний розв'язок $(x, y) \in X \times X$.

Приклад 1.8. У прикладі 1.2 показано, що бінарна операція $*$, задана на множині $\mathbb{Z}$ правилом $a * b = -(a + b)$, не є асоціативною. Отже, пара $(\mathbb{Z}, *)$ не є групою. Для кожних $a, b \in X$ розглянемо рівняння $a * x = b$ і $y * a = b$, які записуються у вигляді $-(a+x) = b$ і $-(y+a) = b$ відповідно. Дані рівняння мають єдиний розв'язок $x = y = -a - b \in \mathbb{Z}$, а тому пара $(\mathbb{Z}, *)$ є квазігрупою.

Характеризаційна теорема 1.1.

Напівгрупа G є групою тоді і тільки тоді, коли вона є квазігрупою.

Доведення. Якщо G є групою, то пара $(x, y) = (a^{-1}b, ba^{-1}) \in G \times G$ є єдиним розв'язком системи рівнянь $ax = b$ і $ya = b$. Дійсно, якщо $ax_1 = b = ax_2$, то домноживши рівності зліва на a^{-1} отримаємо, що $x_1 = a^{-1}b = x_2$. Аналогічно для другого рівняння.

Нехай напівгрупа G є квазігрупою. Спершу доведемо існування лівої одиниці. Нехай $c \in G$ – довільний елемент. За означенням квазігрупи існує елемент e_c, для якого $e_c c = c$. Для довільного елемента $a \in G$ знайдемо розв'язок x_c рівняння $cx = a$. Далі маємо, що $e_c a = e_c(cx_c) = (e_c c)x_c = cx_c = a$, тобто $e = e_c$ – ліва одиниця напівгрупи G. Але тоді для кожного $a \in G$ розв'язок рівняння $ya = e$ є лівим оберненим елементом до елемента a. □

Якщо $M \subset G$, $a \in G$, то через $a * M$ та $M * a$ позначимо множини $\{a * m \mid m \in M\}$ та $\{m * a \mid m \in M\}$ відповідно.

Зрозуміло, що для множини G з визначеною на ній операцією $*$, умова $a * G = G = G * a$ для кожного елемента $a \in G$ рівносильна тому, що для кожних $a, b \in G$ система рівнянь $a*x = b$ і $y*a = b$ має розв'язок $(x, y) \in G \times G$. Оскільки в другому абзаці доведення характеризаційної теореми 1.1 єдиність розв'язку системи не використовується, то з теореми 1.1 випливає наступна

Характеризаційна теорема 1.2.

Напівгрупа $(G, *)$ є групою тоді і лише тоді, коли $a * G = G = G * a$ для кожного елемента $a \in G$.

Якщо G – група, то потужність $|G|$ множини G називається *порядком* групи G. Якщо порядок скінченний, то група G називається *скінченною*. У цьому випадку її можна задати за допомогою таблиці множення, яка називається

таблицею Келі групи G. Таблиця Келі є квадратною матрицею, елементи якої належать групі G, а рядки і стовпці позначені елементами групи G. На перетині рядка, позначеного елементом $a \in G$, і стовпця, позначеного елементом $b \in G$, міститься їх добуток $a * b$.

Якщо операція $*$ є асоціативною на множині M, то з характеризаційної теореми 1.2 випливає, що матриця з елементами множини M є таблицею Келі групи тоді і лише тоді, коли кожен рядок і кожен стовпець матриці складається з усіх елементів множини M.

Приклад 1.9. Розглянемо множину $Q_8 = \{1, -1, i, -i, j, -j, k, -k\}$. Таблиця множення її елементів є наступною:

$*$	1	-1	i	$-i$	j	$-j$	k	$-k$
1	1	-1	i	$-i$	j	$-j$	k	$-k$
-1	-1	1	$-i$	i	$-j$	j	$-k$	k
i	i	$-i$	-1	1	k	$-k$	$-j$	j
$-i$	$-i$	i	1	-1	$-k$	k	j	$-j$
j	j	$-j$	$-k$	k	-1	1	i	$-i$
$-j$	$-j$	j	k	$-k$	1	-1	$-i$	i
k	k	$-k$	j	$-j$	$-i$	i	-1	1
$-k$	$-k$	k	$-j$	j	i	$-i$	1	-1

Перевіримо асоціативність операції $*$ на множині $\{i, j, k\}$:

$$
\begin{aligned}
&i * (j * k) = i * i = -1 = k * k = (i * j) * k,\\
&i * (k * j) = i * (-i) = 1 = -j * j = (i * k) * j,\\
&j * (k * i) = j * j = -1 = i * i = (j * k) * i,\\
&j * (i * k) = j * (-j) = 1 = -k * k = (j * i) * k,\\
&k * (i * j) = k * k = -1 = j * j = (k * i) * j,\\
&k * (j * i) = k * (-k) = 1 = -i * i = (k * j) * i.
\end{aligned}
$$

Далі, використовуючи ті факти, що елемент -1 комутує з усіма елементами множини Q_8 і $-a = -1 * a$ для всіх $a \in \{1, i, j, k\}$, легко перевірити асоціативність операції $*$ на множині Q_8.

Кожен рядок і кожен стовпець містить всі елементи множини Q_8, а тому $(Q_8, *)$ є групою. Оскільки $ij = k \neq -k = ji$, то вона є неабелевою групою порядку 8.

Група Q_8 називається *групою кватерніонів*.

Серед непорожніх підмножин групи G деякі можуть також бути групами. Непорожня підмножина H групи G називається *підгрупою*, якщо H є групою

відносно тієї ж операції, яка визначена на G. Якщо H – підгрупа групи G, то будемо записувати $H < G$.

Зауважимо, що кожна група G містить одиничну підгрупу $\{e\}$ і підгрупу G. Ці підгрупи називаються *тривіальними підгрупами. Власною підгрупою* групи G називається підгрупа $H \neq G$.

Твердження 1.4 (Критерій підгрупи).

Непорожня підмножина H групи G є підгрупою групи G тоді і лише тоді, коли $hk, h_G^{-1} \in H$ для всіх $h, k \in H$.

Доведення. Якщо H підгрупа групи G, то за означення групи $hk \in H$ для кожних $h, k \in H$. Нехай e і f – одиниці груп G і H відповідно. Тоді $ef = f = ff$. Домноживши справа рівність $ef = ff$ на елемент $f^{-1} \in G$, отримаємо, що $ee = fe$, тобто $f = e$. Оскільки H – група, то для кожного $h \in H$ існує обернений h^{-1} в групі H, для якого $h^{-1}h = hh^{-1} = f = e$. А це означає, що елемент h^{-1} є оберненим до елемента $h \in H$ в групі G.

Нехай $hk, h^{-1} \in H$ для всіх $h, k \in H$. Оскільки асоціативність виконується для всіх елементів групи G і $hk \in H$ для кожних $h, k \in H$, то H є напівгрупою. Елемент h^{-1}, обернений до елемента h в групі G, належить H, а тому $h^{-1}h \in H$. Оскільки $e = h^{-1}h$, то e – одиниця групи H. □

Приклад 1.10. Розглянемо групу $(\mathbb{R}, +)$. Оскільки $a + b, -a \in \mathbb{Z}$ для будь-яких цілих чисел a і b, то $\mathbb{Z}$ є підгрупою групи $\mathbb{R}$. Проте для натурального числа 1 обернений до нього в групі $\mathbb{R}$ елемент -1 не належить $\mathbb{N}$, а тому $\mathbb{N}$ не є підгрупою групи $\mathbb{R}$.

З характеризаційної теореми 1.2 випливає

Твердження 1.5 (Критерій підгрупи).

Непорожня підмножина H групи G є підгрупою групи G тоді і лише тоді, коли $aH = H = Ha$ для кожного $a \in H$.

Твердження 1.6.

Перетин довільної непорожньої сім'ї підгруп групи G є підгрупою.

Доведення. Нехай $K = \bigcap_{i \in I} H_i$, де H_i – підгрупа групи G для кожного $i \in I$, I – непорожня множина індексів. Якщо $a, b \in K$, то $a, b \in H_i$

для кожного $i \in I$. Оскільки H_i – підгрупи, то $ab, a^{-1} \in H_i$ для кожного $i \in I$, звідки $ab, a^{-1} \in K$. Таким чином, K – підгрупа групи G за твердженням 1.4. □

Нехай A – непорожня підмножина групи G. Перетин всіх підгруп групи G, які містять підмножину A, називається *підгрупою, породженою множиною* A, і позначається $\langle A \rangle$. Таким чином,

$$\langle A \rangle = \bigcap_{A \subset H < G} H.$$

Позначимо через A^{-1} множину всіх обернених елементів до елементів множини A, тобто $A^{-1} = \{a^{-1} \mid a \in A\}$.

Твердження 1.7.

Нехай A – непорожня підмножина групи G. Тоді підгрупа $\langle A \rangle$, породжена множиною A, складається з усіх скінченних добутків елементів з A і обернених до них елементів, тобто

$$\langle A \rangle = \{a_1 \cdot \ldots \cdot a_n \mid a_i \in A \cup A^{-1}, n \in \mathbb{N}\}.$$

Доведення. Нехай

$$K = \{a_1 \cdot \ldots \cdot a_n \mid a_i \in A \cup A^{-1}, n \in \mathbb{N}\}$$

і $a, b \in K$. Тоді

$$a = a_1 \cdot \ldots \cdot a_n, b = b_1 \cdot \ldots \cdot b_k, \quad a_i, b_i \in A \cup A^{-1}, \quad n, k \in \mathbb{N}.$$

Тому $ab = a_1 \cdot \ldots \cdot a_n b_1 \cdot \ldots \cdot b_k$ також є скінченним добутком елементів множини $A \cup A^{-1}$. Крім того,

$$a^{-1} = (a_1 \cdot \ldots \cdot a_n)^{-1} = a_n^{-1} \cdot \ldots \cdot a_1^{-1} \in K,$$

бо $a_i^{-1} \in A \cup A^{-1}$. Таким чином, K є підгрупою групи G і $K \supset A$, а отже, $K \supset \langle A \rangle$.

Якщо H – довільна підгрупа і $H \supset A$, то $H \supset A^{-1}$, а тому $H \supset K$ за твердженням 1.4, звідки

$$\langle A \rangle = \bigcap_{A \subset H < G} H \supset K.$$

Таким чином, $K = \langle A \rangle$. □

Якщо $\langle A \rangle = G$, то множина A називається *множиною твірних* групи G, а її елементи – *твірними елементами*. Рівність $a_1 \ldots a_n = e$, де $a_i \in A \cup A^{-1}$, називатимемо *співвідношенням*, що зв'язує в групі G елементи множини A.

Якщо M – така множина співвідношень, що будь-який елемент групи G можна отримати з елементів твірної множини A, використовуючи тільки співвідношення множини M, то множину M називатимемо *множиною визначальних співвідношень* групи G. У цьому випадку будемо казати, що *група G є заданою за допомогою множини твірних A і множини визначальних співвідношень M*, та записувати $G = \langle A \mid M \rangle$. Для спрощення запису замість множин A і M часто пишуть їх елементи. Множина твірних A групи G називається *мінімальною*, якщо для кожного $a \in A$ множина $A \backslash \{a\}$ вже не є множиною твірних групи G.

Група, яка не має нетривіальних визначальних співвідношень, називається *вільною*.

Приклад 1.11. Нехай група G є заданою за допомогою множини твірних і множини визначальних співвідношень:

$$G = \langle a, b \mid a^{2025} = b^2 = e,\ ab = ba^2 \rangle.$$

Спершу знайдемо всі елементи даної групи. Використавши визначальні співвідношення, отримаємо:

$$a = ae = ab^2 = (ab)b = (ba^2)b = (ba)(ab) =$$
$$= (ba)(ba^2) = b(ab)a^2 = b(ba^2)a^2 = b^2a^4 = a^4,$$

звідки $a^3 = e$.

Неважко перевірити, що e, a, a^2, b, ab, a^2b – попарно різні елементи групи G. Крім того,

$$a^2b = a(ab) = a(ba^2) = (ab)a^2 = (ba^2)a^2 = ba^4 = ba.$$

Користуючись отриманими рівностями, побудуємо таблицю Келі:

$*$	e	a	a^2	b	ab	a^2b
e	e	a	a^2	b	ab	a^2b
a	a	a^2	e	ab	a^2b	b
a^2	a^2	e	a	a^2b	b	ab
b	b	a^2b	ab	e	a^2	a
ab	ab	b	a^2b	a	e	a^2
a^2b	a^2b	ab	b	a^2	a	e

Таким чином, група G є неабелевою групою порядку 6.

Рекомендована література : [**2**, с. 12–16, 19–30], [**9**, с. 66–79], [**13**, с. 11–17], [**14**, с. 1–8], [**15**, с. 35–53].

Вправи до лекції 1.

1.1. Показати, що пара $(\mathbb{N}, *)$, де $a * b = b$, є напівгрупою. Чи є вона моноїдом? Скільки лівих і правих одиниць містить дана напівгрупа?

1.2. Знайти всі оборотні елементи моноїда $(\mathbb{Z}, \cdot)$.

1.3. Довести, що множина всіх цілих чисел, які діляться на 3, з операцією додаваня є абелевою групою.

1.4. З'ясувати, чи утворює напівгрупу, моноїд, квазігрупу або групу пара $(\mathbb{Q}, *)$, де

а) $a * b = a + b + 5$;
б) $a * b = \frac{ab}{4}$;
в) $a * b = a - b$;
г) $a * b = \frac{a+b}{2}$.

1.5. Які з вказаних множин квадратних матриць з дійсними елементами утворюють групу:

а) множина симетричних матриць відносно додавання;
б) множина симетричних матриць відносно множення;
в) множина матриць із фіксованим визначником d відносно множення;
г) множина діагональних матриць відносно додавання;
д) множина діагональних матриць відносно множення;
е) множина верхніх трикутних матриць відносно множення.

1.6. Довести, що множина $\mathbb{Q}\backslash\{1\}$ з бінарною операцією $a * b = ab - a - b + 2$ утворює групу.

1.7. З'ясувати, чи є групою дійсний інтервал $(-2, +\infty)$ з бінарною операцією $*$, якщо

$$a * b = ab + 2(a + b + 1).$$

1.8. Довести, що множина $(0, 1) \cup (1, +\infty)$ з бінарною операцією $*$ є групою, якщо $a * b = a^{\ln b}$. Чи є ця група абелевою?

1.9. Довести, що пара $(\mathbb{Z}, *)$, де $m * n = (-1)^n m + n$, є групою.

1.10. Довести, що множина $G = [0, 1)$ із бінарною операцією $*$, де $a * b$ дорівнює дробовій частині числа $a + b$, утворює групу.

1.11. Довести, що пара $(\mathbb{R}\backslash\{0\} \times \mathbb{Z}, *)$, де $(a, m) * (b, n) = (ab, m+n)$, є групою.

1.12. На множині $\mathbb{R}^2$ задано операцію

$$(a, b) * (c, d) = (ac - 2bd, ad + bc).$$

З'ясувати, чи множина $\mathbb{R}^2\backslash\{(0, 0)\}$ є групою відносно операції $*$.

1.13. З'ясувати, чи утворює напівгрупу, моноїд, квазігрупу або групу множина $\mathcal{P}(X)$ всіх підмножин множини X з операцією $*$, якщо

а) $A * B = A \cap B$; б) $A * B = A \backslash B$; в) $A * B = A \triangle B$.

1.14. Довести, що множина матриць вигляду

$$\begin{pmatrix} a & 0 \\ -b & a \end{pmatrix},$$

де a і b – довільні ненульові дійсні числа, є групою відносно операції множення матриць.

1.15. Чи утворює групу множина ненульових комплексних чисел з модулем, який не перевищує фіксованого числа $r > 0$, відносно операції множення?

1.16. Навести приклад неабелевої групи, всі власні підгрупи якої є абелевими.

1.17. Нехай всі елементи групи G є ідемпотентами. Довести, що $|G| = 1$.

1.18. Нехай H і K – підгрупи групи G. Чи завжди $H \cup K$ є підгрупою групи G?

1.19. Показати, що кожна група містить єдиний ідемпотент.

1.20. Довести, що група G є абелевою тоді і лише тоді, коли для будь-яких її елементів a і b має місце рівність $(ab)^2 = a^2b^2$.

1.21. Нехай $(G, *)$ – група. Довести, що G є групою відносно операції $\circ$, де $a \circ b = b * a$.

1.22. З'ясувати, чи утворює групу множина $M = \{e, a, b, c, d\}$ з операцією $*$, заданою наступною таблицею Келі:

$*$	e	a	b	c	d
e	e	a	b	c	d
a	a	b	d	e	c
b	b	c	a	d	e
c	c	d	e	a	b
d	d	e	c	b	a

1.23. На множині $M = \{0, 1, 2, 3, 4, 5, 6, 7\}$ визначено бінарну операцію $*$, для якої виконуються наступні властивості:

а) $m * n \leqslant m + n$ для кожних $m, n \in M$;
б) $m * m = 0$ для кожного $m \in M$.

Побудувати таблицю Келі групи $(M, *)$.

1.24. Для множини $\mathbb{Z}$ з операцією $m * n = \left\lfloor \frac{m}{2} \right\rfloor + \left\lfloor \frac{n}{2} \right\rfloor$ показати, що мають місце рівності $a * \mathbb{Z} = \mathbb{Z} = \mathbb{Z} * a$ для кожного $a \in \mathbb{Z}$, але алгебраїчна структура $(\mathbb{Z}, *)$ не є квазігрупою. Нагадаємо, що $\lfloor x \rfloor = \max\{n \in \mathbb{Z} : n \leqslant x\}$ для $x \in \mathbb{R}$.

1.25. Нехай Q – скінченна непорожня множина з бінарною операцією $*$. Довести, що $(Q, *)$ є квазігрупою тоді і лише тоді, коли $Q * a = Q = a * Q$ для кожного $a \in Q$.

1.26. З'ясувати, чи є підгрупами групи $(\mathbb{R}\backslash\{0\}, \cdot)$ наступні підмножини:

а) $\mathbb{Q}\backslash\{0\}$;
б) $\mathbb{Z}\backslash\{0\}$;
в) $\{-1, 1\}$;
г) $\{-1, 1, -2, 2\}$;
д) $\mathbb{R}\backslash(-\infty, 0]$;
е) $\mathbb{R}\backslash\mathbb{Q}$.

1.27. Довести, що наступні підмножини є підгрупами групи $(\mathbb{C}\backslash\{0\}, \cdot)$:

а) $\{1, -1\}$;
б) $\{1, -1, i, -i\}$;
в) $C_n = \{z \in \mathbb{C} \ : \ z^n = 1\}$;
г) $\mathbb{T} = \{z \in \mathbb{C} \ : \ |z| = 1\}$.

1.28. Довести, що для кожного $k \in \mathbb{Z}$ підмножини $k\mathbb{Z}$ і $\{0, 2k + 1\}$ є підгрупами групи $(\mathbb{Z}, *)$, де $m * n = (-1)^n m + n$.

1.29. Довести, що підмножина $H \subset \mathbb{Z}$ є підгрупою групи $(\mathbb{Z}, +)$ тоді й лише тоді, коли $a - b \in H$ для кожних $a, b \in H$.

1.30. Нехай H – підгрупа групи G. Довести, що $g^{-1}Hg$ є підгрупою групи G для кожного $g \in G$.

1.31. Довести, що множина H всіх раціональних чисел, які можна подати у вигляді частки двох непарних чисел, є підгрупою групи $(\mathbb{Q}\backslash\{0\}, \cdot)$.

1.32. Показати, що підмножини $\{0, 2\}$ і $(1, +\infty)$ є підгрупами групи $\mathbb{R}\backslash\{1\}$ з бінарною операцією $a * b = ab - a - b + 2$.

1.33. Нехай a і b – взаємно обернені елементи групи G. Довести, що для кожного $n \in \mathbb{Z}$ елементи a^n і b^n також є взаємно оберненими в групі G.

1.34. Навести приклад скінченної неабелевої групи G, яка містить таку підгрупу $H_0 \neq \{e\}$, що $H_0 \subset H$ для кожної підгрупи $H \neq \{e\}$ групи G.

1.35. Побудувати таблицю Келі групи G, заданої за допомогою множини твірних і множини визначальних співвідношень:

$$G = \langle a, b \mid a^5 = b^2 = e, \ ab = ba^2 \rangle.$$

1.36. Знайти підгрупу $\langle A \rangle$ групи Q_8, породжену множиною $A = \{-1, i\}$. Показати, що група кватерніонів задається наступним чином:

$$Q_8 = \langle i, j \mid i^2 = j^2, \ ji = ij^3 \rangle.$$

1.37. Показати, що множина простих чисел є множиною твірних групи додатніх раціональних чисел з операцією множення.

1.38. Довести, що група не може бути подана у вигляді об'єднання двох своїх власних підгруп.

Лекція 2. Симетрична група та її підгрупи

Нехай X – довільна множина. Бієктивне відображення $s : X \to X$ називається *підстановкою* множини X. Через S_X позначимо множину всіх підстановок множини X. Визначимо композицію $s \circ t$ підстановок s і t як послідовну дію відображень t і s, тобто наступним чином:

$$s \circ t(x) = s(t(x)) \text{ для кожного } x \in X.$$

Теорема 2.1.

Множина S_X з операцією $\circ$ утворює групу.

Доведення. Нехай $s, t \in S_X$. Покажемо, що $s \circ t$ також є підстановкою множини X. Якщо $s \circ t(x_1) = s \circ t(x_2)$, то за означенням композиції $s(t(x_1)) = s(t(x_2))$. Оскільки відображення $s : X \to X$ є ін'єктивним, то з рівності $s(t(x_1)) = s(t(x_2))$ випливає, що $t(x_1) = t(x_2)$. А тоді з ін'єктивності $t : X \to X$ маємо, що $x_1 = x_2$. Таким чином, відображення $s \circ t$ є ін'єктивним. Оскільки відображення $s : X \to X$ є сюр'єктивним, то для кожного $z \in X$ існує $y \in X$, що $s(y) = z$. З сюр'єктивності $t : X \to X$ випливає, що $y = t(x)$ для деякого $x \in X$. Тоді $s \circ t(x) = s(t(x)) = s(y) = z$, і відображення $s \circ t$ є сюр'єктивним. Таким чином, $s \circ t \in S_X$, тобто композиція $\circ$ є бінарною операцією, заданою на множині S_X.

Оскільки

$$s \circ (t \circ r)(x) = s((t \circ r)(x)) = s(t(r(x))) = s \circ t(r(x)) = (s \circ t) \circ r(x)$$

для будь-яких $s, t, r \in S_X$ і будь-якого $x \in X$, то S_X є напівгрупою.

Розглянемо тотожне відображення $id_X : X \to X$, $id_X(x) = x$ для кожного $x \in X$. Очевидно, що дане відображення є підстановкою множини X. Для кожного $s : X \to X$ маємо, що $id_X \circ s(x) = id_X(s(x)) = s(x)$ для кожного $x \in X$. А тому підстановка id_X є лівою одиницею напівгрупи S_X.

Оскільки відображення $s : X \to X$ є бієкцією, то для кожного $y \in X$ існує єдиний елемент $x \in X$, що $y = s(x)$. Визначимо відображення $s^{-1} : X \to X$, поклавши $s^{-1}(y) = x$. За побудовою дане відображення є підстановкою і

$$s^{-1} \circ s(x) = s^{-1}(s(x)) = s^{-1}(y) = x = id_X(x) \text{ для кожного } x \in X,$$

а тому $s^{-1} \circ s = id_X$, тобто s^{-1} є лівим оберненим елементом до елемента $s \in S_X$. □

Групу S_X всіх підстановок множини X називають *симетричною групою* на множині X.

Якщо X – скінченна множина потужності n, то будемо вживати позначення S_n замість S_X. Крім того, не обмежуючи загальності, можна вважати, що $X = \{1, 2, \ldots, n\}$. У цьому випадку кожній підстановці s можна взаємно однозначно поставити у відповідність матрицю

$$s = \begin{pmatrix} 1 & 2 & \ldots & n \\ s(1) & s(2) & \ldots & s(n) \end{pmatrix}$$

Кількість таких матриць дорівнює кількості перестановок елементів другого рядка – $n!$. Таким чином, група S_n має порядок $n!$.

Позначення, які ми вживали до цього часу для підстановок, є досить громіздкими. Для спрощення запису підстановок введемо поняття циклу.

Підстановка $s : X \to X$ називається *циклом* довжини k, якщо існують такі елементи $a_1, a_2, \ldots, a_k \in X$, що

$$s(a_1) = a_2,\ s(a_2) = a_3, \ldots, s(a_{k-1}) = a_k,\ s(a_k) = a_1,$$

і $s(x) = x$ для всіх інших елементів $x \in X$. Для циклу вживатимемо позначення $(a_1 a_2 \ldots a_k)$.

Приклад 2.1. Підстановка

$$s = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 3 & 5 & 1 & 4 & 2 \end{pmatrix} = (162354)$$

є циклом довжини 6, а підстановка

$$t = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 4 & 2 & 3 & 5 & 6 \end{pmatrix} = (243)$$

– цикл довжини 3.

Цикли є "будівельними блоками" для підстановок. Зрозуміло, що кожна скінченна підстановка складається з скінченної кількості циклів. Цикли довжини 1 в записі підстановки опускатимемо. Тотожну підстановку id_X позначатимемо через (1).

Приклад 2.2. Підстановка

$$s = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 1 & 3 & 6 & 5 \end{pmatrix} = (1243)(56)$$

складається з цикла довжини 2 і цикла довжини 4.

Приклад 2.3. Знайдемо добуток циклів $s = (1352)$ і $t = (256)$. Оскільки для підстановки s:

$$1 \overset{s}{\mapsto} 3,\ 3 \overset{s}{\mapsto} 5,\ 5 \overset{s}{\mapsto} 2,\ 2 \overset{s}{\mapsto} 1,\ 4 \overset{s}{\mapsto} 4,\ 6 \overset{s}{\mapsto} 6,$$

а для підстановки t:

$$2 \overset{t}{\mapsto} 5,\ 5 \overset{t}{\mapsto} 6,\ 6 \overset{t}{\mapsto} 2,\ 1 \overset{t}{\mapsto} 1,\ 3 \overset{t}{\mapsto} 3,\ 4 \overset{t}{\mapsto} 4,$$

то враховуючи, що в добутку $s \circ t$ спочатку діє t, а потім s, для підстановки $s \circ t$ маємо:

$$1 \overset{t}{\mapsto} 1 \overset{s}{\mapsto} 3,\ 3 \overset{t}{\mapsto} 3 \overset{s}{\mapsto} 5,\ 5 \overset{t}{\mapsto} 6 \overset{s}{\mapsto} 6,\ 6 \overset{t}{\mapsto} 2 \overset{s}{\mapsto} 1,\ 2 \overset{t}{\mapsto} 5 \overset{s}{\mapsto} 2,\ 4 \overset{t}{\mapsto} 4 \overset{s}{\mapsto} 4,$$

а отже,

$s \circ t = (1356)$. Якщо $r = (1634)$, то $s \circ r = (1652)(34)$.

Цикл довжини 2 називається *транспозицією*. Оскільки

$$(a_1 a_2 \dots a_n) = (a_1 a_n)(a_1 a_{n-1}) \dots (a_1 a_3)(a_1 a_2),$$

то має місце наступне

Твердження 2.1.

Кожну підстановку скінченної множини, що містить принаймні 2 елементи, можна подати у вигляді добутку транспозицій.

Твердження 2.2.

Якщо одиниця id_X записана у вигляді добутку r транспозицій:

$$id_X = s_1 s_2 \dots s_r,$$

то r є парним числом.

Доведення. Скористаємось методом математичної індукції. Транспозиція не може бути одиницею (1), а тому $r > 1$. Якщо $r = 2$, то твердження вірне. Нехай $r > 2$. У цьому випадку для добутку $s_{r-1}s_r$ останніх двох транспозицій виконується одна з рівностей:

$$1)\ (ab)(ab) = id_X$$
$$2)\ (bc)(ab) = (ac)(bc)$$
$$3)\ (cd)(ab) = (ab)(cd)$$
$$4)\ (ac)(ab) = (ab)(bc),$$

де a, b, c і d різні елементи множини X.

В першому випадку добуток двох останніх транспозицій є одиницею групи, а тому $id_X = s_1 s_2 \dots s_{r-2}$. За припущенням математичної індукції число $r - 2$ є парним, а тому r також є парним.

У кожному з наступних випадків можна замінити $s_{r-1}s_r$ на праву частину відповідної рівності, щоб отримати новий добуток r транспозицій. В новому добутку останнє входження елемента a міститься в передостанній транспозиції. Продовжимо даний процес для $s_{r-2}s_{r-1}$. Аналогічно отримаємо або добуток $r-2$ транспозицій, або новий добуток r транспозицій, в якому останнє входження елемента a міститься в $r-2$ транспозиції. Продовжуючи аналогічно, отримаємо, що або останнє входження елемента a є в першій транспозиції, або в добутку r транспозицій є дві послідовні однакові транспозиції, які в добутку дають id_X. В першому випадку у добутку всіх транспозицій елемент a не переходить в a, а тому добуток транспозицій не може дорівнювати одиниці id_X. Отже, залишається тільки другий випадок. Але тоді, викинувши дві послідовні однакові транспозиції і використавши припущення математичної індукції, отримаємо, що $r-2$, а отже, і r – парні числа. □

Теорема 2.2.

Якщо підстановка s записана у вигляді добутку парної кількості транспозицій, то довільне інше подання s у вигляді добутку транспозицій також містить парну кількість транспозицій. Аналогічно, якщо підстановка s записана у вигляді добутку непарної кількості транспозицій, то довільне інше подання s у вигляді добутку транспозицій також містить непарну кількість транспозицій.

Доведення. Нехай

$$s = t_1 \dots t_m = r_1 \dots r_k,$$

де m є парним числом. Оскільки

$$s^{-1} = (t_1 \dots t_m)^{-1} = t_m^{-1} \dots t_1^{-1} = t_m \dots t_1, \text{ то}$$

$$id_X = st_m \dots t_1 = r_1 \dots r_k t_m \dots t_1,$$

а тому k також є парним за твердженням 2.2.

Випадок, коли підстановка s записана у вигляді добутку непарної кількості транспозицій, доводиться аналогічно. □

З теореми 2.2 випливає коректність наступних означень.

Підстановка s називається *парною*, якщо вона може бути записана у вигляді добутку парної кількості транспозицій.

Підстановка s називається *непарною*, якщо s може бути записана у вигляді добутку непарної кількості транспозицій.

Приклад 2.4. Тотожна підстановка (1) є парною, бо вона задається добутком, в якому немає транспозицій (0 транспозицій). Підстановка $(12345) = (15)(14)(13)(12)$ є парною, а підстановка $(1234) = (14)(13)(12)$ – непарна.

Через A_n позначимо множину всіх парних підстановок скінченної множини X потужності $|X| = n$.

Твердження 2.3.

Підмножина A_n є підгрупою симетричної групи S_n.

Доведення. Якщо обидві підстановки $s, t \in A_n$ записані у вигляді добутку парної кількості транспозицій, то $s \circ t$ також є добутком парної кількості транспозицій, а тому $s \circ t \in A_n$. Якщо $s = t_1 \dots t_m \in A_n$, то m – парне, а тому

$$s^{-1} = (t_1 \dots t_m)^{-1} = t_m^{-1} \dots t_1^{-1} = t_m \dots t_1 \in A_n.$$

□

Група A_n називається *знакозмінною групою* на множині X.

Приклад 2.5. Знайдемо всі елементи знакозмінної групи A_4. Оскільки кожен цикл $(a_1a_2a_3)$ є добутком двох транспозицій $(a_1a_2a_3) = (a_1a_3)(a_1a_2)$, то A_4 містить всі цикли довжини 3, а також підстановки виду $(a_1a_2)(a_3a_4)$. Всі цикли (a_1a_2) довжини 2 і $(a_1a_2a_3a_4) = (a_1a_4)(a_1a_3)(a_1a_2)$ довжини 4 є добутками непарної кількості транспозицій, а тому групі A_4 не належать. Таким чином,

$A_4 = \{(1), (123), (132), (124), (142), (134), (143), (234), (243), (12)(34), (13)(24), (14)(23)\}$.

Знакозмінна група A_4 містить 12 елементів. Це не випадково.

Твердження 2.4.

Кількість парних підстановок групи S_n, де $n \geqslant 2$, дорівнює кількості непарних підстановок. Тому порядок групи A_n дорівнює $\frac{n!}{2}$.

Доведення. Позначимо через B_n множину непарних підстановок групи S_n. Нехай s – довільна транспозиція.

Визначимо відображення

$$\psi : A_n \to B_n, \quad \psi(t) = s \circ t.$$

Нехай $\psi(t_1) = \psi(t_2)$. Тоді $s \circ t_1 = s \circ t_2$, а отже, $t_1 = s^{-1} \circ s \circ t_2 = t_2$, і відображення ψ є ін'єктивним.

Якщо $t \in B_n$, то $s^{-1} \circ t = st \in A_n$ і $\psi(s^{-1} \circ t) = s \circ s^{-1} \circ t = t$, а отже, відображення ψ – сюр'єктивне.

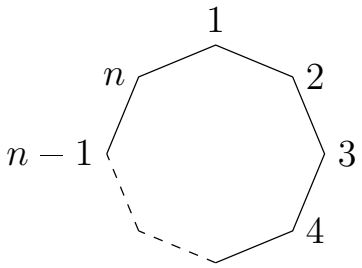
Таким чином, відображення ψ є бієкцією. □

Вивчимо будову деяких підгруп симетричної групи, які часто зустрічаються в геометрії.

Розглянемо групу $\mathrm{Isom}(\mathbb{R}^2) \subset S_{\mathbb{R}^2}$ рухів (бієктивних відображень, що зберігають відстані) евклідової площини $\mathbb{R}^2$. Якщо F – довільна фігура на площині, то множина тих рухів s, які залишають нерухомою фігуру F, тобто $s(F) = F$, є підгрупою групи $\mathrm{Isom}(\mathbb{R}^2)$. Дана підгрупа називається *групою симетрій* фігури F.

Нехай F – правильний n-кутник. Тоді кожен рух, який залишає нерухомим даний многокутник, індукує бієктивне відображення на множині вершин правильного n-кутника, і множина D_n таких бієктивних відображень вершин є підгрупою симетричної групи S_n.

Занумеруємо вершини правильного n-кутника числами $1, 2, \ldots, n$:



Зауважимо, що є n можливостей для заміни вершини з номером 1. Якщо вершину 1 замінено на вершину k, то вершину 2 можна замінити або вершиною $k+1$, або $k-1$. Далі заміна визначається однозначно. Таким чином, є $2n$ різних бієктивних відображень множини вершин правильного n-кутника, при яких n-кутник "накладається" на себе.

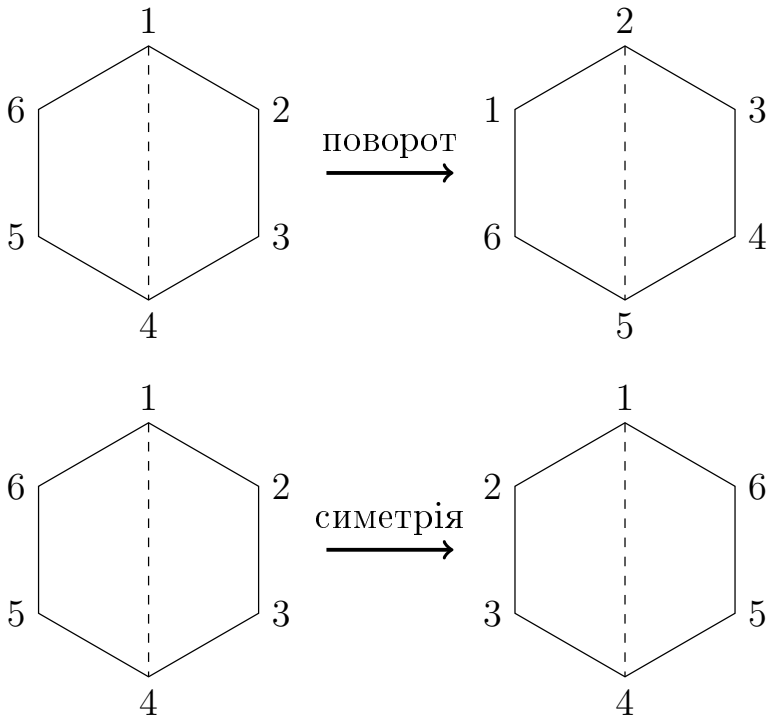
Група D_n називається *діедральною групою порядку* $2n$.

Теорема 2.3.

Діедральна група D_n, $n \geqslant 3$, порядку $2n$, складається з усіх добутків двох елементів r і s, для яких виконуються рівності $r^n = e$, $s^2 = e$, $srs = r^{-1}$, тобто

$$D_n = \langle r, s \mid r^n = e,\ s^2 = e,\ srs = r^{-1} \rangle.$$

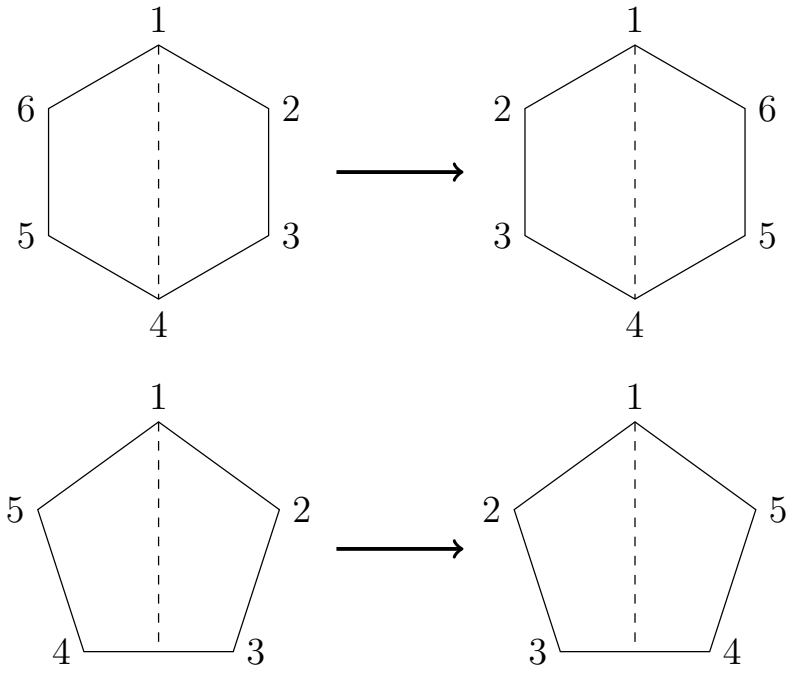
Доведення. Позначимо через e бієктивне відображення, яке залишає нерухомими всі вершини правильного n-кутника. Очевидно, що e – одиниця групи D_n. Елементами групи D_n є повороти і симетрії.



Всього є n різних поворотів:

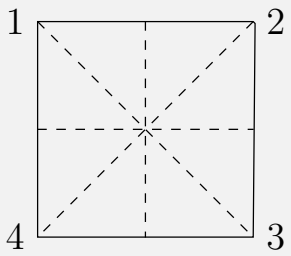
$$e,\ \frac{360^\circ}{n},\ 2\cdot\frac{360^\circ}{n},\dots,(n-1)\cdot\frac{360^\circ}{n}.$$

Позначимо через r поворот на кут $\frac{360^\circ}{n}$. Поворот r породжує всі інші повороти, а саме $r^k = k\cdot\frac{360^\circ}{n}$. Позначимо n симетрій через $s_1, s_2, \dots, s_n$, де s_k – симетрія, яка залишає нерухомою вершину з номером k. Всього є два типи симетрій, які залежать від парності числа n. Якщо n парне, то при симетрії дві вершини залишаються нерухомими, якщо ж n непарне, то – одна.



В обох випадках порядок елемента s_k дорівнює 2. Покладемо $s = s_1$. Тоді $s^2 = e$ і $r^n = e$. Якщо бієктивне відображення t многокутника на себе замінює вершину 1 вершиною k, то вершину 2 воно може замінити або вершиною $k+1$, або $k-1$. Якщо вершину 2 замінено вершиною $k+1$, то $t = r^{k-1}$; якщо ж – вершиною $k-1$, то $t = r^{k-1}s$. Таким чином, елементи r і s породжують групу D_n, тобто D_n складається з усіх скінченних добутків елементів r і s. Крім того, очевидно, що $srs = r^{-1}$. □

Приклад 2.6. Група D_4 симетрій квадрата містить 8 елементів. Занумеруємо вершини квадрата числами $1, 2, 3, 4$:



Тоді повороти задаються циклами:

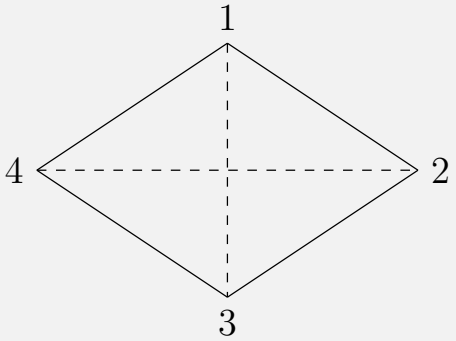
$$r = (1432), \quad r^2 = (13)(24), \quad r^3 = (1234), \quad r^4 = e,$$

а симетрії: $s_1 = (24)$, $s_2 = (13)$.

Інші два елементи мають вигляд:

$$rs_1 = (14)(23), \quad r^3 s_2 = (12)(34).$$

Приклад 2.7. Розглянемо групу симетрій ромба. Занумеруємо вершини ромба числами $1, 2, 3, 4$:



Позначимо через a симетрію, яка залишає нерухомими вершини 1 і 3, а через b – симетрію, що залишає нерухомими вершини 2 і 4. Тоді $a = (24)$, $b = (13)$. Звідки $a^2 = b^2 = e$ і $ab = ba = (13)(24)$. Таким чином, група симетрій ромба є абелевою групою порядку 4.

Нехай $c = ab$. Тоді таблиця Келі має наступний вигляд:

$*$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Група симетрій ромба називається 4-*групою Клейна* і позначається V_4. Таким чином,

$$V_4 = \langle a, b \mid a^2 = b^2 = e, ab = ba \rangle.$$

Рекомендована література : [**9**, с. 24–32, 84–88], [**11**, с. 27–30], [**12**, с. 23–33], [**15**, с. 74–91].

Вправи до лекції 2.

2.1. Чи є відображення $f : \mathbb{R} \to \mathbb{R}$, $f(x) = x^3 + 3x^2 + 3x$, підстановкою на множині $\mathbb{R}$?

2.2. Записати наступні підстановки за допомогою циклів:

а) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 1 & 2 \end{pmatrix}$; б) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 3 & 5 & 1 \end{pmatrix}$; в) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 2 & 1 & 4 \end{pmatrix}$.

2.3. Обчислити добутки циклів:

а) $(1345)(234)$; б) $(1254)(13)(25)$;
в) $(1254)^{100}$; г) $(135)^{-3}$;
д) $(12)(23)(34)(45)(56)$; е) $(12)(13)(15)(14)(13)(12)$.

2.4. Подати наступні підстановки у вигляді добутку транспозицій та з'ясувати, чи є вони парними.

а) (16345); б) $(36)(1254)$;
в) $(17254)(154632)$; г) $(1234)(354)(123)$.

2.5. Побудувати таблиці Келі для груп S_3 і D_4. Знайти всі їх підгрупи.

2.6. Нехай G – група, $a \in G$. З'ясувати, чи є відображення $s : G \to G$ елементом симетричної групи S_G:

а) $s(g) = g^{-1}$; б) $s(g) = aga^{-1}$; в) $s(g) = ag$.

2.7. У групі S_5 розв'язати рівняння $(124) \circ x \circ (13) = (245)$.

2.8. Довести, що множина всіх бієкцій $f : \mathbb{R} \to \mathbb{R}$, $f(0) = 0$, $f(2024) = 2024$, є підгрупою групи $S_{\mathbb{R}}$.

2.9. Виписати всі елементи наступних множин:

а) $\{s \in S_4 \mid s(1) = 3\}$; б) $\{s \in S_4 \mid s(2) = 2\}$;
в) $\{s \in S_4 \mid s(1) = 3 \text{ і } s(2) = 2\}$.

Чи є дані множини підгрупами групи S_4?

2.10. Довести, що кожен цикл парної (непарної) довжини є непарною (парною) підстановкою.

2.11. Показати, що кожен елемент симетричної групи S_n можна подати у вигляді скінченного добутку наступних транспозицій:

а) $(12), (13), \ldots, (1n)$; б) $(12), (23), \ldots, (n-1, n)$.

2.12. Знайти всі степені циклу $(123456) \in S_6$.

2.13. Нехай $s = (143)(125)$, $t = (243)$. Довести, що підстановка $(t^{-1} \circ s \circ t)^{2024}$ є циклом довжини 5.

2.14. Довести, що $(12 \ldots n)^{-1} = (1n \ldots 32)$.

2.15. Знайти всі елементи знакозмінної групи A_5.

2.16. Знайти всі мінімальні множини твірних групи S_3.

2.17. Задати групу S_3 за допомогою мінімальної множини твірних і множини визначальних співвідношень.

2.18. З'ясувати, при яких $n \in \mathbb{N}$ групи S_n, A_n і D_n є абелевими.

2.19. Довести, що множина всіх циклів довжини 3 є множиною твірних групи A_n.

2.20. Скільки різних 2–елементних множин твірних має група A_4?

2.21. Побудувати таблицю Келі для групи симетрій прямокутника.

2.22. Знайти кількість тих підстановок із групи S_9, які комутують із підстановкою $s = (123456789)$.

2.23. У групі S_4 знайти підгрупи H_1 і H_2, задані одноелементними множинами твірних $\{(1243)\}$ і $\{(1342)\}$ відповідно. Чи є $H_1 \cap H_2$ абелевою підгрупою групи S_4?

2.24. Нехай підстановка групи S_n записана у вигляді добутку m незалежних циклів, включаючи цикли довжини 1. Різниця $n - m$ називається *декрементом* підстановки. Довести, що парність підстановки співпадає з парністю її декремента.

2.25. Довести, що множина $\mathrm{Aff}(\mathbb{R})$ всіх афінних відображень $f : \mathbb{R} \to \mathbb{R}$, $f(x) = ax + b$, де $a, b \in \mathbb{R}$, $a \neq 0$, є підгрупою симетричної групи $S_{\mathbb{R}}$.

2.26. Показати, що множина $\mathrm{Aff}^+(\mathbb{R})$ всіх афінних відображень вигляду $f(x) = ax + b$, де $a > 0$, є підгрупою групи $\mathrm{Aff}(\mathbb{R})$.

2.27. Довести, що множина $\mathrm{Shift}(\mathbb{R})$ всіх зсувів $r_b(x) = x + b$ є підгрупою групи $\mathrm{Aff}^+(\mathbb{R})$.

2.28. Показати, що множина всіх гомотетій $f(x) = ax$, $a \neq 0$, є підгрупою групи $\mathrm{Aff}(\mathbb{R})$.

2.29. Довести, що всі дробово-лінійні функції вигляду

$$f(x) = \frac{ax + b}{cx + d},$$

де $a, b, c, d \in \mathbb{R}$, $ad \neq bc$, утворюють групу відносно операції композиції функцій. Чи є дана група підгрупою групи $S_{\mathbb{R}}$?

2.30. Довести, що кожна підгрупа $G < S_n$, яка містить непарну підстановку, обов'язково містить підгрупу порядку $|G|/2$.

2.31. Довести, що для кожної підгрупи H симетричної групи S_n, або всі підстановки в H є парними, або рівно половина підстановок є парними.

Лекція 3. Порядок елемента групи. Циклічні підгрупи

Зафіксуємо елемент a групи G. Перетин всіх підгруп групи G, які містять елемент a, називається *циклічною підгрупою, породженою елементом* a, і позначається $\langle a \rangle$. Таким чином,

$$\langle a \rangle = \bigcap_{a \in H < G} H.$$

З твердження 1.7 у випадку $A = \{a\}$ випливає наступна

Теорема 3.1.

Циклічна підгрупа $\langle a \rangle$, породжена елементом a, складається з усіх цілих степенів елемента a, тобто $\langle a \rangle = \{a^m \mid m \in \mathbb{Z}\}$.

Згідно з твердженням 1.3 для будь-яких $m, n \in \mathbb{Z}$ мають місце рівності $a^m a^n = a^{m+n} = a^{n+m} = a^n a^m$, а тому група $\langle a \rangle$ є абелевою.

Для елемента $a \in G$ можливі наступні два випадки.

1. Усі степені елемента a є різними, тобто $a^m \neq a^n$ для цілих $m \neq n$. У цьому випадку кажуть, що елемент a має *нескінченний порядок*.

2. Серед степенів елемента a є рівні, тобто $a^m = a^n$ для деяких різних $m, n \in \mathbb{Z}$. Тоді $|m-n| \in \mathbb{N}$ і $a^{|m-n|} = e$, тобто існують натуральні степені елемента a, які дорівнюють одиниці групи G. Найменше натуральне число n, для якого $a^n = e$, називається *порядком елемента* a і позначається $|a|$.

Приклад 3.1. Знайдемо порядки елементів

$$A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 3 \\ 0 & 1 \end{pmatrix}$$

групи $GL(2, \mathbb{R})$.

Оскільки $A^2 = -E$, $A^3 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, $A^4 = E$, то $|A| = 4$.

Якщо $n \in \mathbb{N}$, то $B^n = \begin{pmatrix} 1 & 3n \\ 0 & 1 \end{pmatrix}$, а отже, B має нескінченний порядок.

Очевидно, що в кожній групі одиниця e має порядок 1. Інших елементів порядку 1 в групі немає.

Приклад 3.2. Покажемо, що група G парного порядку містить елемент порядку 2. Нехай $|G| = n$ – парне число. Якщо елемент $a \in G$ дорівнює своєму оберненому, тобто $a = a^{-1}$, то $a^2 = e$. Припустимо, що серед елементів групи G немає елементів другого порядку. Тоді лише одиничний елемент e є оберненим до себе. Отже, усі інші $n-1$ елементів розбиваються на пари елементів, обернених один до одного. Але це неможливо, оскільки число $n-1$ є непарним.

Елементи a і b групи G називаються *спряженими в групі* G, якщо $b = g^{-1}ag$ для деякого $g \in G$.

Приклад 3.3. Спряжені елементи мають однаковий порядок. Дійсно,

$$b^n = (g^{-1}ag)(g^{-1}ag)\dots(g^{-1}ag) = g^{-1}a^n g.$$

Якщо $b^n = e$, то $a^n = gb^n g^{-1} = gg^{-1} = e$. Якщо $a^n = e$, то $b^n = g^{-1}eg = e$. Таким чином, $a^n = e$ тоді і лише тоді, коли $b^n = e$, а отже, порядки елементів a і b рівні.

Група G називається *періодичною*, якщо всі її елементи мають скінченний порядок. Зрозуміло, що кожна скінченна група є періодичною. Існують нескінченні періодичні групи як завгодно великих порядків.

Приклад 3.4. Для довільної множини X група $\mathcal{P}(X)$ всіх підмножин множини X з операцією симетричної різниці є періодичною. Дійсно, одиницею даної групи є порожня множина $\varnothing$ і $A^2 = A \triangle A = \varnothing$ для кожної множини $A \in \mathcal{P}(X)$.

Якщо єдиним елементом скінченного порядку є одиничний, то група G називається *групою без кручень*.

Теорема 3.2.

Нехай елемент $a \in G$ має скінченний порядок n. Тоді порядок циклічної підгрупи $\langle a \rangle$ дорівнює n і $\langle a \rangle = \{e, a, a^2, \ldots, a^{n-1}\}$. Причому $a^m = e$ тоді і лише тоді, коли m ділиться на n.

Доведення. За теоремою 3.1 циклічна підгрупа $\langle a \rangle = \{a^m \mid m \in \mathbb{Z}\}$ складається з усіх цілих степенів елемента a. Довільне ціле число m можна подати у вигляді

$$m = nq + r, \quad 0 \leqslant r < n.$$

Тому

$$a^m = a^{nq+r} = a^{nq}a^r = (a^n)^q a^r = a^r, \text{ звідки } \langle a \rangle \subset \{e, a, a^2, \ldots, a^{n-1}\}.$$

Протилежне включення є очевидним, а тому $\langle a \rangle = \{e, a, a^2, \ldots, a^{n-1}\}$. У цьому випадку підгрупа $\langle a \rangle$ має порядок n. Дійсно, якби $a^k = a^s$ при $0 \leqslant k < s < n$, то $a^{s-k} = e$ і $1 \leqslant s - k < n$, що суперечить мінімальності n.

Оскільки $a^m = a^r$, то $a^m = e$ тільки при $r = 0$, тобто коли m ділиться на n. □

Група G називається *циклічною*, якщо існує такий елемент $a \in G$, що $\langle a \rangle = G$. Якщо елемент a має нескінченний порядок, то всі елементи групи G є попарно різними, і G – *нескінченна циклічна група*:

$$G = \{\ldots, a^{-m}, \ldots, a^{-1}, a^0 = e, a, \ldots, a^m, \ldots\}.$$

Зрозуміло, що кожна нескінченна циклічна група є групою без кручень і кожна її неодинична підгрупа є нескінченною. Нескінченна циклічна група є прикладом вільної групи з одним твірним елементом.

Приклад 3.5. У групі $(\mathbb{Z}, +)$ підгрупа $\langle a \rangle$, породжена цілим числом a, складається з усіх кратних числа a, тобто $\langle a \rangle = \{ma \mid m \in \mathbb{Z}\}$. Оскільки $\langle 1 \rangle = \{m1 \mid m \in \mathbb{Z}\} = \mathbb{Z}$, то $(\mathbb{Z}, +)$ – нескінченна циклічна група. Очевидно, що $\langle -1 \rangle = \mathbb{Z}$ і $\langle a \rangle \neq \mathbb{Z}$ для кожного цілого $a \notin \{-1, 1\}$.

Якщо елемент a має скінченний порядок n, то $G = \langle a \rangle = \{e, a, a^2, \ldots, a^{n-1}\}$ за теоремою 3.2, тобто група G складається з n елементів. У цьому випадку G – *скінченна циклічна група порядку* n.

Приклад 3.6. Для кожного натурального числа n група $(\mathbb{C}\backslash\{0\}, \cdot)$ містить n різних коренів степеня n з одиниці, які обчислюються за допомогою наступної формули:

$$\xi_k = \cos\frac{2\pi k}{n} + i\sin\frac{2\pi k}{n},\ k \in \{0, 1, \ldots, n-1\}.$$

Оскільки

$$\xi_k = \cos\frac{2\pi k}{n} + i\sin\frac{2\pi k}{n} = (\cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n})^k = \xi_1^k,$$

то множина $C_n = \{z \in \mathbb{C} \mid z^n = 1\}$ всіх коренів степеня n з одиниці є циклічною групою $\langle \xi_1 \rangle$ порядку n, породженою елементом ξ_1.

Теорема 3.3.

Кожна підгрупа циклічної групи є циклічною.

Доведення. Нехай H – довільна підгрупа циклічної групи $G = \langle a \rangle$. Тоді $e \in H$ і якщо інших елементів підгрупа H не містить, то $H = \langle e \rangle$.

Нехай $a^t \in H, a^t \neq e$. Тоді $a^{-t} \in H$ і можна обрати в H елемент a^m з найменшим натуральним показником m. Якщо a^n – довільний елемент підгрупи H, то

$$n = mq + r,\quad 0 \leqslant r < m \quad \text{і}$$

$$a^r = a^{n-mq} = a^n a^{-mq} = a^n((a^m)^q)^{-1} \in H.$$

З мінімальності m випливає, що $r = 0$ і n ділиться на m. Таким чином, $H \subset \langle a^m \rangle$. Оскільки H – підгрупа, то $\langle a^m \rangle \subset H$, а отже, $H = \langle a^m \rangle$. □

Твердження 3.1.

Якщо $|a| = n$, *то* $|a^m| = \frac{n}{(n,m)}$.

Доведення. Нехай $n = dn_1$, $m = dm_1$, де $d = (n, m)$. Тоді $(n_1, m_1) = 1$. Якщо $(a^m)^t = e$, то $a^{mt} = e$, а тому $mt = dm_1 t$ ділиться на $n = dn_1$ за теоремою 3.2. Оскільки $(n_1, m_1) = 1$, то t ділиться на n_1. А тоді з рівностей

$$(a^m)^{n_1} = a^{dm_1 n_1} = a^{nm_1} = (a^n)^{m_1} = e$$

випливає, що $|a^m| = n_1 = \frac{n}{d} = \frac{n}{(n,m)}$. □

Наслідок 3.1.

Елемент a^k є твірним елементом циклічної групи $\langle a \rangle$ порядку n тоді і лише тоді, коли $(n, k) = 1$.

Нагадаємо, що функція Ейлера $\varphi : \mathbb{N} \to \mathbb{N}$ ставить у відповідність кожному натуральному числу n кількість натуральних чисел, які взаємно прості з n і не перевищують n. Таким чином, кількість твірних елементів циклічної групи порядку n дорівнює $\varphi(n)$.

Приклад 3.7. Порядок елемента ξ_{24} циклічної групи C_{60} дорівнює

$$|\xi_{24}| = |\xi_1^{24}| = \frac{60}{(60, 24)} = 5.$$

Приклад 3.8. Твірними елементами групи C_8 є ξ_1, $\xi_1^3 = \xi_3$, $\xi_1^5 = \xi_5$ і $\xi_1^7 = \xi_7$.

Твердження 3.2.

У скінченній циклічній групі порядку n для кожного натурального дільника d числа n існує єдина підгрупа порядку d.

Доведення. Нехай $G = \langle a \rangle$ – скінченна циклічна група порядку n, d – натуральний дільник числа n. За твердженням 3.1 елемент $a^{\frac{n}{d}}$ має порядок d, а тому циклічна підгрупа $\langle a^{\frac{n}{d}} \rangle$ має порядок d. Нехай $M = \langle a^m \rangle$ – довільна підгрупа порядку d. За теоремою 3.2 з рівності $a^{md} = e$ випливає, що md ділиться на n, а тому m ділиться на $\frac{n}{d}$. Тоді маємо, що $a^m \in \langle a^{\frac{n}{d}} \rangle$, а отже, $\langle a^m \rangle \subset \langle a^{\frac{n}{d}} \rangle$. Оскільки $|\langle a^m \rangle| = d = |\langle a^{\frac{n}{d}} \rangle|$, то $\langle a^m \rangle = \langle a^{\frac{n}{d}} \rangle$. □

Нагадаємо, що функція $\tau : \mathbb{N} \to \mathbb{N}$ ставить у відповідність кожному натуральному числу n кількість його натуральних дільників. Таким чином, кількість різних підгруп циклічної групи порядку n дорівнює $\tau(n)$.

Твердження 3.3.

Нехай елементи a і b групи G комутують. Якщо $|a| = n$, $|b| = m$ і $(m, n) = 1$, то $|ab| = nm$.

Доведення. Нехай $t = |ab|$. Тоді $(ab)^t = e$. Оскільки елементи a і b комутують, то $(ab)^t = a^t b^t$, а отже, елементи a^t і b^t – взаємно обернені. Легко перевірити, що взаємно обернені елементи мають однаковий порядок, а тому $|a^t| = |b^t|$. За твердженням 3.1 порядки елементів a^t і b^t є дільниками n і m відповідно. Оскільки $(n, m) = 1$, то $|a^t| = |b^t| = 1$, звідки $a^t = b^t = e$. Тоді t ділиться на n і t ділиться на m, а отже, t ділиться на nm. З мінімальності t випливає, що $t = nm$. □

Рекомендована література : [**2**, с. 30–32, 35–36], [**9**, с. 79–81], [**12**, с. 54–61], [**15**, с. 57–72], [**16**, с. 12–14].

Вправи до лекції 3.

3.1. Знайти циклічну підгрупу групи S_5, породжену елементом a, якщо

а) $a = (123)$; б) $a = (1324)$; в) $a = (123)(45)$.

3.2. Знайти порядки наступних елементів групи $(\mathbb{C}\backslash\{0\}, \cdot)$:

а) i; б) $\frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}$; в) $i + 1$.

3.3. Скільки різних циклічних підгруп містить група A_4?

3.4. Відомо, що кожна власна підгрупа групи G є циклічною. Чи обов'язково група G є циклічною?

3.5. Знайти всі підгрупи циклічної групи C_{12}.

3.6. З'ясувати, чи є множина $\mathbb{Z}$ з операцією $n * m = n + (-1)^n m$ циклічною групою.

3.7. Скількома способами можна обрати твірний елемент у циклічній групі порядку 120?

3.8. Скільки різних підгруп містить циклічна група порядку 120?

3.9. Нехай G – група, $a, b, c \in G$. Довести, що

а) $|a^{-1}| = |a|$; б) $|ab| = |ba|$;
в) $|abc| = |bca| = |cab|$.

3.10. Нехай G – група, $a, b \in G$, $|a| = 2$, $|b| = 5$. Знайти $|aba|$.

3.11. Довести, що в групі S_n кожен цикл довжини $k \leqslant n$ має порядок k.

3.12. Знайти порядки всіх елементів групи $(\mathbb{Z}, *)$, де $m * n = (-1)^n m + n$. Показати, що множина всіх елементів скінченного порядку не є підгрупою даної групи.

3.13. Довести, що підмножина $\mathrm{Tor}\,(G)$ всіх елементів скінченного порядку абелевої групи G є підгрупою групи G. Група $\mathrm{Tor}\,(G)$ називається *підгрупою кручення* абелевої групи G.

3.14. Знайти підгрупу кручення групи $[0, 1)$ із бінарною операцією $*$, де $a * b$ дорівнює дробовій частині числа $a + b$.

3.15. Знайти кількість елементів порядку 12 групи $(\mathbb{C}\backslash\{0\}, \cdot)$.

3.16. Нехай G – група, $a, b \in G$, $|a| = 5$ і $a^3 b = ba^3$. Довести, що $ab = ba$.

3.17. Нехай G – група, $a, b \in G$, $|a| = 5$, $|b| = 9$ і $a^4 b^8 ab = e$. Знайти $|ab|$.

3.18. Нехай g – неодиничний елемент групи G, який комутує тільки з e і g. Знайти порядок елемента g.

3.19. Показати, що кожна скінченна група містить непарну кількість елементів g, для яких $g^3 = e$.

3.20. Довести, що в будь-якій скінченній групі для кожного натурального числа $n > 2$ кількість елементів порядку n є парною.

3.21. Нехай g – такий елемент групи G, що $g^2 \neq e$ і $g^6 = e$. Довести, що $g^4 \neq e$ і $g^5 \neq e$. Що можна сказати про порядок елемента g?

3.22. Знайти кількість елементів порядку 2 у циклічній групі G, якщо:

а) $|G|$ – непарне число; б) $|G|$ – парне число.

3.23. Нехай g – такий неодиничний елемент групи G, що елементи g^6 і g^7 є взаємно оберненими. Знайти $|g|$.

3.24. Нехай a і b мають порядки 15 і 16 відповідно в групі G. Знайти порядок підгрупи $\langle a \rangle \cap \langle b \rangle$.

3.25. Нехай a – елемент групи G. Знайти твірний елемент підгрупи $\langle a^n \rangle \cap \langle a^m \rangle$.

3.26. Знайти усі розв'язки рівняння $x^6 = e$ і всі елементи порядку 6 в циклічній групі C_{120}.

3.27. Яким може бути порядок циклічної групи, якщо твірний елемент у ній можна обрати рівно 10 способами?

3.28. Відомо, що деяка група містить 4 елементи, один з яких має порядок 4. Який порядок мають решту елементів групи і скільки підгруп має ця група?

3.29. Показати, що підгрупа H групи $(\mathbb{Q}, +)$, породжена множиною $A = \{\frac{1}{2}, \frac{1}{3}\}$, є циклічною.

3.30. Знайти добуток усіх елементів циклічної групи $G = \langle a \rangle$ порядку n.

3.31. Нехай G – скінченна абелева група, $A = \{a \in G \mid a^2 = e\}$. Довести, що $\prod_{g \in G} g = \prod_{a \in A} a = c$, де c – деякий елемент множини A. Чи є A підгрупою групи G?

3.32. Довести, що група G є абелевою за умови, що $a^2 = e$ для кожного $a \in G$.

3.33. Довести, що підмножина H періодичної групи G є підгрупою тоді і лише тоді, коли $ab \in H$ для будь-яких елементів $a, b \in H$.

3.34. Довести, що група $\mathrm{Aff}(\mathbb{R})$ не містить елементів скінченного порядку, більшого ніж 2.

3.35. Нехай $|g| = nm$, де $(m, n) = 1$. Довести, що $g = ab = ba$ для деяких елементів a і b групи G, де $|a| = n$, $|b| = m$.

Лекція 4. Розбиття групи за підгрупою. Теорема Лагранжа

Сім'я $\mathcal{D}$ підмножин множини X називається *розбиттям* X, якщо:

1) всі елементи $\mathcal{D}$ непорожні;
2) об'єднання $\cup\mathcal{D}$ рівне X;
3) якщо елементи F і G сім'ї $\mathcal{D}$ мають непорожній перетин, то $F = G$.

Для кожного відношення еквівалентності $\rho \subset X \times X$ існує єдине розбиття $\mathcal{D}$ множини X, для якого $(x, y) \in \rho$ тоді і лише тоді, коли x та y потрапляють в один елемент сім'ї $\mathcal{D}$. Елемент шуканого розбиття $\mathcal{D}$, який містить $x \in X$, складається з усіх елементів $y \in X$, для яких $(x, y) \in \rho$. Цей елемент називається *класом еквівалентності* x (відносно відношення ρ) і позначається $[x]$ або $\overline{x}$. Таким чином, $\mathcal{D} = \{\overline{x} : x \in X\}$.

Нехай G – група, а H – довільна її підгрупа. Розглянемо наступне бінарне відношення $\rho_l \subset G \times G$:

$$(a, b) \in \rho_l \Leftrightarrow a^{-1}b \in H.$$

Відношення ρ_l є відношенням еквівалентності. Дійсно:

1) *Рефлексивність.* Для кожного $a \in G$ виконано $a^{-1}a = e \in H$, а тому $(a, a) \in \rho_l$.
2) *Симетричність.* Нехай $(a, b) \in \rho_l$. Тоді $a^{-1}b \in H$. Оскільки H є підгрупою, то $b^{-1}a = (a^{-1}b)^{-1} \in H$, звідки $(b, a) \in \rho_l$.
3) *Транзитивність.* Нехай $(a, b), (b, c) \in \rho_l$. Тоді $a^{-1}b, b^{-1}c \in H$. Звідси $a^{-1}c = (a^{-1}b)(b^{-1}c) \in H$, а тому $(a, c) \in \rho_l$.

Отже, відношення ρ_l задає деяке розбиття групи G. Клас еквівалентності, який містить елемент a, має вигляд:

$$\overline{a} = \{g \in G : (a, g) \in \rho_l\} = \{g \in G : a^{-1}g \in H\} = \{g \in G : g \in aH\} = aH.$$

Утворене розбиття називатимемо *лівостороннім розбиттям групи G за підгрупою H*, а клас еквівалентності $\overline{a}$ – *лівим суміжним класом групи G за підгрупою H, породженим елементом a*. Таким чином,

$$G = \bigcup_{g \in G} gH.$$

Позначимо через $(G : H)$ множину всіх лівих суміжних класів групи G за підгрупою H. Потужність множини лівих суміжних класів називається *індексом підгрупи H в групі G* і позначається $|G : H|$.

Приклад 4.1. Якщо $H = \{e\}$, то лівий суміжний клас, породжений елементом a є одноелементним: $\overline{a} = aH = a\{e\} = \{a\}$. Таким чином, лівостороннє розбиття групи G за підгрупою H складається з усіх одноелементних підмножин групи G, тобто

$$G = \bigcup_{g \in G} \{g\}.$$

У цьому випадку індекс підгрупи H в групі G дорівнює $|G|$, тобто $|G : H| = |G|$.

Якщо $H = G$, то $aH = aG = G$ для кожного $a \in G$, а тому лівосторонній розклад групи G за підгрупою H містить єдиний елемент – групу G. Таким чином, $|G : H| = 1$.

Аналогічним чином легко перевірити, що бінарне відношення $\rho_r \subset G \times G$:

$$(a, b) \in \rho_r \Leftrightarrow ba^{-1} \in H,$$

є відношенням еквівалентності. Клас еквівалентності $\overline{a}$ співпадає з підмножиною Ha групи G і називається *правим суміжним класом групи G за підгрупою H, породженим елементом a*. Розбиття, породжене відношенням ρ_r, називатимемо *правостороннім розбиттям групи G за підгрупою H*. Таким

чином,

$$G = \bigcup_{g \in G} Hg.$$

Приклад 4.2. Для кожного елемента g групи S_3 знайдемо ліві і праві суміжні класи за підгрупою $H = \{(1), (12)\}$, породжені g:

g	gH	Hg
(1)	$\{(1), (12)\}$	$\{(1), (12)\}$
(12)	$\{(1), (12)\}$	$\{(1), (12)\}$
(13)	$\{(13), (123)\}$	$\{(13), (132)\}$
(23)	$\{(23), (132)\}$	$\{(23), (123)\}$
(123)	$\{(13), (123)\}$	$\{(23), (123)\}$
(132)	$\{(23), (132)\}$	$\{(13), (132)\}$

Таким чином,

$$G = \bigcup_{g \in G} gH = \{(1), (12)\} \cup \{(13), (123)\} \cup \{(23), (132)\}$$

і

$$G = \bigcup_{g \in G} Hg = \{(1), (12)\} \cup \{(13), (132)\} \cup \{(23), (123)\}$$

З таблиці видно, що $(13)H \neq H(13)$, тобто лівий і правий суміжний класи, породжені однаковими елементами, можуть не співпадати. Група S_3 містить три різних лівих і три різних правих суміжних класів за підгрупою H. Тому індекс підгрупи H в групі S_3 дорівнює 3.

Твердження 4.1.

Кількість лівих суміжних класів групи G за підгрупою H дорівнює кількості правих суміжних класів.

Доведення. Оскільки H підгрупа групи G, то $h^{-1} \in H$ для кожного $h \in H$, тобто $H^{-1} \subset H$. Тоді з рівності $h = (h^{-1})^{-1}$ випливає, що $H^{-1} = H$. Розглянемо відображення ψ з множини лівих суміжних класів у множину правих суміжних класів:

$$\psi(gH) = (gH)^{-1} = H^{-1}g^{-1} = Hg^{-1}.$$

Якщо $\psi(g_1H) = \psi(g_2H)$, то $(g_1H)^{-1} = (g_2H)^{-1}$, звідки $g_1H = g_2H$, а тому відображення ψ є ін'єктивним. Для кожного правого суміжного класу Hg існує такий лівий суміжний клас $g^{-1}H$, що $\psi(g^{-1}H) = H(g^{-1})^{-1} = Hg$, а отже, ψ – сюр'єктивне відображення. Таким чином,

відображення ψ є бієкцією множини лівих суміжних класів на множину правих суміжних класів групи G за підгрупою H. □

Зауваження 4.1.

Нехай H – підгрупа групи G.

1. *Підгрупа H завжди є лівим і правим суміжним класом. Дійсно, $H = eH = He$.*
2. *Оскільки $g = ge = eg$, то $g \in gH \cap Hg$ для кожного $g \in G$.*
3. *Якщо G – абелева група, то $gH = Hg$ для кожного $g \in G$, тобто лівий і правий суміжний класи, які містять елемент g, співпадають.*

Приклад 4.3. Знайдемо ліві і праві суміжні класи групи $(\mathbb{Z}, +)$ за підгрупою $5\mathbb{Z}$. Оскільки група $\mathbb{Z}$ є абелевою, то ліві і праві суміжні класи, породжені однаковими елементами, співпадають. Суміжні класи мають вигляд $k + 5\mathbb{Z}$, де $k \in \mathbb{Z}$. Тоді

$$\begin{aligned}
\overline{0} &= 5\mathbb{Z} = \{\ldots, -15, -10, -5, 0, 5, 10, 15, \ldots\},\\
\overline{1} &= 1 + 5\mathbb{Z} = \{\ldots, -14, -9, -4, 1, 6, 11, 16, \ldots\},\\
\overline{2} &= 2 + 5\mathbb{Z} = \{\ldots, -13, -8, -3, 2, 7, 12, 17, \ldots\},\\
\overline{3} &= 3 + 5\mathbb{Z} = \{\ldots, -12, -7, -2, 3, 8, 13, 18, \ldots\},\\
\overline{4} &= 4 + 5\mathbb{Z} = \{\ldots, -11, -6, -1, 4, 9, 14, 19, \ldots\}.
\end{aligned}$$

Легко бачити, що $\mathbb{Z} = \overline{0} \cup \overline{1} \cup \overline{2} \cup \overline{3} \cup \overline{4}$, а тому є 5 різних суміжних класів групи $\mathbb{Z}$ за підгрупою $5\mathbb{Z}$.

Теорема 4.1 (Теорема Лагранжа).

Якщо H – підгрупа скінченної групи G, то

$$|G| = |H| \cdot |G : H|.$$

Зокрема порядок скінченної групи ділиться на порядок кожної її підгрупи.

Доведення. Розглянемо лівостороннє розбиття групи G за підгрупою H. Одним з лівих суміжних класів є підгрупа $H = eH$. Нехай gH – довільний лівий суміжний клас.

Розглянемо відображення

$$l_g : H \to gH, \quad l_g(h) = gh.$$

Якщо $l_g(h_1) = l_g(h_2)$, то $gh_1 = gh_2$, а тому $h_1 = h_2$, і відображення l_g є ін'єкцією. Оскільки $g^{-1}a \in H$ для кожного $a \in gH$ і $l_g(g^{-1}a) = a$, то l_g – сюр'єкція. Таким чином, l_g – бієкція.

Отже, потужність кожного лівого суміжного класу дорівнює порядку підгрупи H. Оскільки скінченна група містить скінченну кількість лівих суміжних класів і дані класи попарно не перетинаються, то $|G| = |H| \cdot m$, де m – кількість лівих суміжних класів. Таким чином,

$$|G| = |H| \cdot |G : H|,$$

і порядок групи G ділиться на порядок підгрупи H. □

Наслідок 4.1.

Порядок кожного елемента скінченної групи G ділить порядок групи G.

Доведення. Порядок елемента $a \in G$ дорівнює порядку циклічної підгрупи $\langle a \rangle$, породженої даним елементом, а тому за теоремою Лагранжа $|a| = |\langle a \rangle|$ ділить $|G|$. □

Наслідок 4.2.

Якщо порядком групи G є просте число p, то G – циклічна група.

Доведення. Нехай a – довільний неодиничний елемент групи G. За теоремою Лагранжа порядок циклічної підгрупи $\langle a \rangle$, породженої елементом a, ділить $|G| = p$. Оскільки $a \neq e$, то $|\langle a \rangle| = p$, а тому група G співпадає з циклічною підгрупою $\langle a \rangle$. □

Нехай A і B – підмножини групи G. Покладемо $AB = \{ab \mid a \in A, b \in B\}$.

Якщо H – підгрупа групи G, то $HH \subset H = eH \subset HH$, звідки $HH = H$. Тоді за індукцією $H^n = \underbrace{H \dots H}_{n} = H$ для кожного $n \in \mathbb{N}$.

Добуток HK двох підгруп H і K групи G не обов'язково є підгрупою групи G.

Приклад 4.4. Розглянемо підгрупи $H = \{(1), (12)\}$ і $K = \{(1), (13)\}$ групи S_3. Добуток підгруп H і K дорівнює:

$$HK = \{(1), (12), (13), (132)\}.$$

Підмножина HK не є підгрупою групи S_3, бо $(13)(12) = (123) \notin HK$. Аналогічно $KH = \{(1), (12), (13), (123)\}$ не є підгрупою групи S_3.

Твердження 4.2.

Добутки HK та KH двох підгруп H і K групи G є підгрупами групи G тоді і лише тоді, коли H і K є переставними, тобто $HK = KH$.

Доведення. Нехай HK та KH є підгрупами групи G і $h \in H$, $k \in K$. Тоді

$$kh = ((kh)^{-1})^{-1} = (h^{-1}k^{-1})^{-1} \in HK, \text{ а тому } KH \subset HK.$$

Аналогічно

$$hk = ((hk)^{-1})^{-1} = (k^{-1}h^{-1})^{-1} \in KH.$$

Звідки $HK \subset KH$, а отже, $HK = KH$.

Навпаки, нехай $HK = KH$ і $h_1, h_2 \in H, k_1, k_2 \in K$. Тоді $k_1h_2 = h_3k_3$ для деяких $h_3 \in H, k_3 \in K$. Тому

$$(h_1k_1)(h_2k_2) = h_1(k_1h_2)k_2 = h_1h_3k_3k_2 \in HK \quad i$$

$$(h_1k_1)^{-1} = k_1^{-1}h_1^{-1} \in KH = HK.$$

Таким чином, $HK = KH$ – підгрупа групи G. □

Рекомендована література : [**2**, с. 39–43], [**9**, с. 90–98], [**13**, с. 20–25], [**15**, с. 92–99].

Вправи до лекції 4.

4.1. Знайти лівостороннє розбиття групи Q_8 за підгрупою $H = \{-1, 1\}$.

4.2. Знайти суміжні класи групи $(3\mathbb{Z}, +)$ за підгрупою $15\mathbb{Z}$.

4.3. Знайти лівостороннє та правостороннє розбиття групи A_4 за підгрупою $H = \{(1), (123), (132)\}$. Порівняти їх.

4.4. Описати суміжні класи групи $(\mathbb{C}\backslash\{0\}, \cdot)$ за підгрупою H, якщо

а) $H = \mathbb{R}\backslash\{0\}$; б) $H = \mathbb{R}_+$; в) $H = \{z \in \mathbb{C} \ : \ |z| = 1\}$.

4.5. Знайти лівостороннє та правостороннє розбиття групи $GL(n, \mathbb{R})$ за підгрупою $SL(n, \mathbb{R})$. Чому дорівнює індекс підгрупи $SL(n, \mathbb{R})$ в групі $GL(n, \mathbb{R})$?

4.6. З'ясувати, чи є лівим або правим суміжним класом по деякій підгрупі групи S_5 підмножина A:

а) $A = \{(234), (1234)\}$; б) $A = \{(12), (123), (1234)\}$.

4.7. Знайти суміжні класи циклічної групи C_{12} за всіма її підгрупами.

4.8. Знайти всі підгрупи індекса 2 групи Q_8.

4.9. Описати суміжні класи групи $(\mathbb{C}, +)$ за підгрупою $H = \{a+ib \mid a, b \in \mathbb{Z}\}$.

4.10. Описати суміжні класи групи векторів площини, які виходять з початку координат, з операцією додавання векторів за підгрупою векторів, що лежать на осі абсцис.

4.11. Знайти індекс підгрупи A_n в групі S_n.

4.12. Знайти ліві і праві суміжні класи групи S_n за підгрупою S_{n-1}.

4.13. Показати, що підгрупа $\mathbb{Z}$ має нескінченний індекс в групі $(\mathbb{Q}, +)$

4.14. Навести приклад скінченної групи, у якої індекси всіх власних неодиничних підгруп: а) попарно різні; б) однакові.

4.15. Навести приклад нескінченної групи, у якої індекси власних неодиничних підгруп: а) попарно різні; б) однакові.

4.16. Наступна таблиця є таблицею Келі деякої групи. Заповнити її порожні клітинки.

$*$	e	a	b	c	d
e	e				
a		b			e
b		c	d	e	
c		d		a	b
d					

4.17. Нехай скінченна група G містить елемент a порядку 6 та елемент b порядку 14. Яке мінімальне значення $|G|$?

4.18. Нехай H – підгрупа групи G, $a, b \in G$ Чи з рівності $aH = bH$ випливає рівність $a^2H = b^2H$? Відповідь обгрунтуйте.

4.19. Нехай $|G : H| = 2$. Довести, що $ab \in H$ для кожних $a, b \in G \backslash H$.

4.20. Нехай p – просте число. Підгрупи яких порядків містить діедральна група D_p порядку $2p$?

4.21. Знайти кількість елементів порядку p групи порядку p, де p – просте число.

4.22. Нехай p, q – прості числа, G – група порядку pq. Довести, що всі власні підгрупи групи G є циклічними.

4.23. Нехай порядок скінченої групи G дорівнює n. Довести, що $a^n = e$ для кожного $a \in G$.

4.24. Нехай G – група непарного порядку. Довести, що для кожного $a \in G$ існує такий елемент $b \in G$, що $a = b^2$.

4.25. Нехай G – група непарного порядку з одиницею e. Довести, що рівняння $x^2 = e$ має єдиний розв'язок. Далі, для кожного $g \in G\backslash\{e\}$ довести, що рівняння $x^2 = g$ має єдиний розв'язок.

4.26. Нехай G – група, H – довільна її підгрупа. Довести або спростувати твердження: відображення $f : \{gH \mid g \in G\} \to \{Hg \mid g \in G\}$, $f(gH) = Hg$, є бієкцією.

4.27. Нехай G – група порядку 10, та $x, y \in G$ – різні елементи порядку 2. Нехай $H = \langle x, y\rangle$. Яким може бути порядок підгрупи H? Чи можуть елементи x та y комутувати?

4.28. Довести, що підмножина A групи G є лівим суміжним класом за деякою підгрупою тоді і лише тоді, коли вона є правим суміжним класом за деякою (можливо іншою) підгрупою.

4.29. Довести, що непорожня підмножина A групи G є суміжним класом за деякою підгрупою тоді і лише тоді, коли $gA^{-1}A = A$ для деякого $g \in G$.

4.30. Нехай $g_1, \ldots, g_n$ – представники різних лівих суміжних класів групи G за підгрупою H. Довести, що $g_1^{-1}, \ldots, g_n^{-1}$ – представники різних правих суміжних класів G за H.

4.31. Нехай m і k – взаємно прості натуральні числа. Довести, що абелева група G порядку mk є циклічною тоді і лише тоді, коли G містить елемент порядку m і елемент порядку k.

4.32. Довести, що множина $\mathcal{P}(G)$ всіх підмножин групи G з операцією множення підмножин є моноїдом. Знайти всі його оборотні елементи.

4.33. Підмножина A групи G називається *самозачепленою*, якщо $gA \cap A \neq \varnothing$ для кожного $g \in G$. Довести, що множина A є самозачепленою тоді і лише тоді, коли $AA^{-1} = G$.

Лекція 5. Нормальні підгрупи. Факторгрупи

Підгрупа H називається *нормальною* або *інваріантною підгрупою* групи G, якщо лівостороннє та правостороннє розбиття групи G за підгрупою H співпадають, тобто

$$\{gH \mid g \in G\} = \{Hg \mid g \in G\}.$$

Якщо H є нормальною підгрупою групи G, то будемо записувати $H \lhd G$ або $G \rhd H$. Нормальні підгрупи також називають *нормальними дільниками* групи.

Приклад 5.1. Розглянемо підгрупу $H = \{(1), (123), (132)\}$ групи S_3.

Оскільки $(12)H = \{(12), (23), (13)\}$ і

$$G = \{(1), (123), (132)\} \cup \{(12), (23), (13)\},$$

то множина лівих суміжних класів має вигляд:

$$\{\{(1), (123), (132)\}, \{(12), (23), (13)\}\}.$$

Оскільки $H(12) = \{(12), (13), (23)\}$ і

$$G = \{(1), (123), (132)\} \cup \{(12), (23), (13)\},$$

то множина правих суміжних класів має вигляд:

$$\{\{(1), (123), (132)\}, \{(12), (23), (13)\}\}.$$

Таким чином, правостороннє і лівостороннє розбиття групи S_3 за підгрупою H співпадають, а тому H – нормальна підгрупа групи S_3.

Оскільки $g \in gH \cap Hg$, то H є нормальною підгрупою групи G тоді і лише тоді, коли $gH = Hg$ для кожного $g \in G$.

Приклад 5.2. Розглянемо підгрупу $H = \{(1), (13)\}$ групи S_3.

Оскільки $(12)H = \{(12), (132)\}$, а $H(12) = \{(12), (123)\}$, то $(12)H \neq H(12)$. Таким чином, H не є нормальною підгрупою групи S_3.

Очевидно, що будь-яка підгрупа абелевої групи є нормальною.

Для нормальності підгрупи H в групі G досить вимагати виконання тільки одного з включень:

$$\forall g \in G \ (\ gH \subset Hg\ ) \quad \text{або} \quad \forall g \in G \ (\ Hg \subset gH\ ).$$

Дійсно, якщо $gH \subset Hg$ для кожного $g \in G$, то і $g^{-1}H \subset Hg^{-1}$ для $g^{-1} \in G$, звідки, домноживши отримане включення на g зліва і справа, отримаємо $Hg \subset gH$. Аналогічно у другому випадку.

Домноживши рівність $Hg = gH$ на g^{-1} зліва отримаємо, що H є нормальною підгрупою групи G тоді і лише тоді, коли $g^{-1}Hg = H$ для кожного $g \in G$. З останньої рівності випливає, що $H \lhd G$ тоді і лише тоді, коли разом з кожним з своїм елеменом підгрупа H містить усі спряжені з ним елементи у групі G:

$$H \lhd G \ \Leftrightarrow\ \forall h \in H\ \forall g \in G \ (\ g^{-1}hg \in H\ ).$$

Приклад 5.3. З'ясуємо, при яких $k \in \mathbb{N}\backslash\{1\}$ підмножини $k\mathbb{Z} = \{ka \mid a \in \mathbb{Z}\}$ є нормальними підгрупами групи $(\mathbb{Z}, *)$, де $m * n = (-1)^n m + n$.

Спершу зауважимо, що одиницею групи $(\mathbb{Z}, *)$ є число 0, а оберненим до елемента $a \in \mathbb{Z}$ є елемент $a^{-1} = (-1)^{a-1}a$.

Якщо $s, t \in k\mathbb{Z}$, то $s = ka$ і $t = kb$ для деяких $a, b \in \mathbb{Z}$. Тоді

$$s * t = (ka) * (kb) = (-1)^{kb}ka + kb = k((-1)^{kb}a + b) \in k\mathbb{Z}$$

і

$$s^{-1} = (ka)^{-1} = (-1)^{ka-1}ka = k((-1)^{ka-1}a) \in k\mathbb{Z}.$$

Тому для кожного $k \in \mathbb{N}$ підмножини $k\mathbb{Z}$ є підгрупами групи $(\mathbb{Z}, *)$.

Нехай n і a – довільні цілі числа. Тоді

$$n^{-1} * (ka) * n = ((-1)^{n-1}n) * (ka) * n = ((-1)^{ka}(-1)^{n-1}n + ka) * n =$$
$$= (-1)^n((-1)^{ka+n-1}n + ka) + n = (-1)^{ka-1}n + (-1)^n ka + n =$$
$$= ((-1)^{ka-1} + 1)n + k((-1)^n a).$$

Якщо k є парним числом, то $ka - 1$ є непарним, а тому

$$n^{-1} * (ka) * n = k((-1)^n a) \in k\mathbb{Z}$$

для кожних $n, a \in \mathbb{Z}$. Таким чином, у цьому випадку $k\mathbb{Z}$ є нормальною підгрупою групи $(\mathbb{Z}, *)$.

Якщо $k > 1$ є непарним числом, то поклавши $a = 1$, $n = k - 1$, отримаємо

$$n^{-1} * (ka) * n = ((-1)^{k-1} + 1)(k - 1) + (-1)^{k-1}k = 3k - 2 \notin k\mathbb{Z}.$$

Тому в цьому випадку $k\mathbb{Z}$ не є нормальними підгрупами групи $(\mathbb{Z}, *)$.

Приклад 5.4. Нехай циклічна підгрупа C групи G є нормальною підгрупою групи G. Покажемо, що кожна підгрупа H групи C є нормальною підгрупою групи G. Дійсно, нехай a – твірний елемент групи C. Оскільки $C \lhd G$, то $g^{-1}ag \in C$ для кожного $g \in G$, а тому $g^{-1}ag = a^k$ для деякого $k \in \mathbb{Z}$. Підгрупа H є циклічною за теоремою 3.3 і породжується a^n для деякого $n \in \mathbb{Z}$. Тоді $g^{-1}(a^n)^t g = (g^{-1}ag)^{nt} = a^{knt} = (a^n)^{kt} \in H$ для кожних $g \in G$, $t \in \mathbb{Z}$, а тому $H \lhd G$.

Твердження 5.1.

Якщо K і H – підгрупи групи G, причому $H \lhd G$, то KH також є підгрупою групи G.

Доведення. Оскільки $H \lhd G$, то $gH = Hg$ для кожного $g \in G$. Зокрема $gH = Hg$ для кожного $g \in K$, тобто $KH = HK$. Тоді за твердженням 4.2 добуток $KH = HK$ є підгрупою групи G. □

Твердження 5.2.

Добуток скінченної кількості нормальних підгруп групи G є нормальною підгрупою групи G.

Доведення. Нехай $H_1, \ldots, H_k$ – нормальні підгрупи групи G. З попереднього твердження випливає, що $H_1 \cdot \ldots \cdot H_k$ є підгрупою групи G. Оскільки для кожного $g \in G$:

$$g(H_1H_2 \cdot \ldots \cdot H_k) = H_1gH_2 \cdot \ldots \cdot H_k = \ldots = H_1H_2 \cdot \ldots \cdot gH_k = (H_1H_2 \cdot \ldots \cdot H_k)g,$$

то $H_1 \cdot \ldots \cdot H_k \lhd G$. □

У кожній групі G тривіальні підгрупи (одинична підгрупа $\{e\}$ і сама група G) є нормальними підгрупами. Неодинична група G називається *простою*, якщо вона не містить нетривіальних нормальних підгруп. Групу порядку 1 не відносять до простих груп.

Теорема 5.1.

Неодинична абелева група G є простою тоді і лише тоді, коли G є циклічною групою простого порядку p.

Доведення. Нехай G – абелева проста група. Тоді $|G| \geqslant 2$. Якщо a – неодиничний елемент групи G, то циклічна підгрупа $\langle a \rangle$ є нормальною, а тому $\langle a \rangle = G$. Група G не може бути нескінченною, бо тоді вона б містила нетривіальну нормальну підгрупу $\langle a^2 \rangle$.

Нехай $G = \langle a \rangle$ – скінченна циклічна підгрупа порядку n і p – простий дільник n. Елемент a^p має порядок $|a^p| = \frac{n}{(n,p)} = \frac{n}{p}$, а тому циклічна підгрупа $\langle a^p \rangle$ є власною ($\neq G$) нормальною підгрупою групи G. Це можливо лише у випадку $\langle a^p \rangle = \{e\}$, тобто коли $n = p$ – просте число.

Навпаки, якщо $|G| = p$, то за наслідком 4.2 з теореми Лагранжа група G є циклічною, кожна неодинична підгрупа якої має порядок p, а тому співпадає з G. Таким чином, G – проста група. □

Існують неабелеві прості групи. Наприклад, знакозмінна група A_n є неабелевою простою групою для кожного $n > 4$.

Нехай H – нормальна підгрупа групи G, тоді для кожного $g \in G$ лівий суміжний клас gH співпадає з правим суміжним класом Hg, а тому для спрощення називатимемо їх суміжними класами.

Теорема 5.2.

Множина $(G : H)$ суміжних класів групи G за нормальною підгрупою H з операцією множення підмножин у групі є групою.

Доведення. Нехай $\overline{a}, \overline{b} \in (G : H)$. Тоді

$$\overline{a} \cdot \overline{b} = (aH)(bH) = a(Hb)H = abHH = abH = \overline{ab} \in (G : H),$$

а отже, операція є заданою на множині $(G : H)$.

Для кожних $\overline{a}, \overline{b}, \overline{c} \in (G : H)$ маємо:

$$\overline{a} \cdot (\overline{b} \cdot \overline{c}) = \overline{a} \cdot \overline{bc} = \overline{a(bc)} = \overline{(ab)c} = \overline{ab} \cdot \overline{c} = (\overline{a} \cdot \overline{b}) \cdot \overline{c},$$

а тому операція множення суміжних класів є асоціативною.

Оскільки для кожного $\overline{a} \in (G : H)$ мають місце рівності $\overline{e} \cdot \overline{a} = \overline{ea} = \overline{a}$ і $\overline{a^{-1}} \cdot \overline{a} = \overline{a^{-1}a} = \overline{e}$, то $\overline{e}$ є лівою одиницею напівгрупи $(G : H)$ і кожен суміжний клас $\overline{a}$ має лівий обернений $\overline{a^{-1}} \in (G : H)$.

Таким чином, $(G : H)$ – група. □

Група всіх суміжних класів групи G за нормальною підгрупою H називається *факторгрупою* групи G за підгрупою H і позначається G/H.

З теореми Лагранжа випливає, що для скінченної групи G і кожної її нормальної підгрупи H має місце рівність $|G| = |H| \cdot |G/H|$. Зокрема порядок скінченної групи ділиться на порядок кожної її факторгрупи. Порядок факторгрупи G/H дорівнює індексу підгрупи H в групі G.

Твердження 5.3.

Кожна факторгрупа G/H циклічної групи G є циклічною.

Доведення. Нехай $G = \langle a \rangle$ – циклічна група, породжена елементом a, і $\overline{g}$ – довільний елемент факторгрупи G/H. Оскільки G – циклічна група, то $g = a^k$ для деякого $k \in \mathbb{Z}$. Тоді

$$\overline{g} = gH = a^k H = a^k H^k = (aH)^k = \overline{a}^k.$$

Таким чином, G/H – циклічна група, породжена елементом $\overline{a}$. □

Приклад 5.5. Побудуємо таблицю Келі факторгрупи групи $(\mathbb{Z}, +)$ за підгрупою $4\mathbb{Z}$.

Оскільки група $(\mathbb{Z}, +)$ є абелевою, то підгрупа $4\mathbb{Z}$ є нормальною.

Суміжні класи мають вигляд $k + 4\mathbb{Z}$, де $k \in \mathbb{Z}$. Тоді

$$\overline{0} = 4\mathbb{Z} = \{\ldots, -12, -8, -4, 0, 4, 8, 12, \ldots\},$$
$$\overline{1} = 1 + 4\mathbb{Z} = \{\ldots, -11, -7, -3, 1, 5, 9, 13, \ldots\},$$
$$\overline{2} = 2 + 4\mathbb{Z} = \{\ldots, -10, -6, -2, 2, 6, 10, 14, \ldots\},$$
$$\overline{3} = 3 + 4\mathbb{Z} = \{\ldots, -9, -5, -1, 3, 7, 11, 15, \ldots\}.$$

Легко бачити, що $\mathbb{Z} = \overline{0} \cup \overline{1} \cup \overline{2} \cup \overline{3}$, а тому є 4 різних суміжних класи групи $\mathbb{Z}$ за підгрупою $4\mathbb{Z}$.

Використовуючи формулу $\overline{m}+\overline{n}=\overline{m+n}$ і замінюючи при потребі елемент $m+n$ на найменше невід'ємне число класу $\overline{m+n}$, отримаємо наступну таблицю Келі факторгрупи $\mathbb{Z}/4\mathbb{Z}$:

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{0}$	$\overline{1}$	$\overline{2}$

З таблиці Келі видно, що факторгрупа $\mathbb{Z}/4\mathbb{Z}$ є циклічною групою порядку 4, породженою елементом $\overline{1}$.

Для кожного натурального числа $k\geqslant 2$ факторгрупу $\mathbb{Z}/k\mathbb{Z}$ групи $(\mathbb{Z},+)$ позначають через $\mathbb{Z}_k$. Група $\mathbb{Z}_k=\{\overline{0},\overline{1},\ldots,\overline{k-1}\}$ є циклічною групою порядку k, породженою елементом $\overline{1}$.

Приклад 5.6. Побудуємо таблицю Келі факторгрупи групи $(\mathbb{Z},*)$ за нормальною підгрупою $4\mathbb{Z}$, де $m*n=(-1)^n m+n$.

Суміжні класи мають вигляд:

$k*4\mathbb{Z}=\{k*(4a)\mid a\in\mathbb{Z}\}=\{(-1)^{4a}k+4a\mid a\in\mathbb{Z}\}=\{k+4a\mid a\in\mathbb{Z}\}=k+4\mathbb{Z}$,

де $k\in\mathbb{Z}$. Таким чином, суміжні класи такі ж, як і в попередньому прикладі.

Використовуючи формулу $\overline{m}*\overline{n}=\overline{m*n}=\overline{(-1)^n m+n}$ і замінюючи при потребі елемент $m*n$ на найменше невід'ємне число класу $\overline{m*n}$, отримаємо наступну таблицю Келі факторгрупи $\mathbb{Z}/4\mathbb{Z}$:

$*$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{1}$	$\overline{1}$	$\overline{0}$	$\overline{3}$	$\overline{2}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{2}$	$\overline{1}$	$\overline{0}$

З таблиці Келі видно, що факторгрупа $\mathbb{Z}/4\mathbb{Z}$ є абелевою групою порядку 4. Дана група не є циклічною. Всі неодиничні елементи факторгрупи $\mathbb{Z}/4\mathbb{Z}$ мають порядок 2. Таким чином, будова $\mathbb{Z}/4\mathbb{Z}$ така ж, як і у групи Клейна V_4.

Крім того, зауважимо, що $\mathbb{Z}/4\mathbb{Z} = \{\overline{0}, \overline{1}\} * \{\overline{0}, \overline{2}\}$. Отже, група $\mathbb{Z}/4\mathbb{Z}$ є добутком двох своїх нормальних підгруп порядку 2, перетин яких співпадає з одиничною підгрупою.

Твердження 5.4.

Кожна підгрупа H індекса 2 є нормальною підгрупою групи G.

Доведення. Оскільки $|G : H| = 2$, то лівостороннє і правостороннє розбиття групи G за підгрупою H містять по 2 елементи. Оберемо $g \notin H$, тоді $H \cup gH = G = H \cup Hg$, звідки випливає, що $gH = Hg$, а тому $\{H, gH\} = \{H, Hg\}$, і H – нормальна підгрупа групи G. □

Приклад 5.7. Покажемо, що кожна підгрупа неабелевої групи Q_8 є нормальною. Оскільки $|Q_8| = 8$, то за теоремою Лагранжа порядок кожної підгрупи групи Q_8 належить множині $\{1, 2, 4, 8\}$. Зрозуміло, що тривіальні підгрупи порядків 1 і 8 є нормальними. Підгрупи порядку 4 мають індекс 2 у групі Q_8, а тому за попереднім твердженням є нормальними. Елемент -1 є єдиним елементом порядку 2 групи кватерніонів, а тому група Q_8 містить єдину підгрупу $\{1, -1\}$ порядку 2. Дана підгрупа є нормальною, бо $g\{1, -1\} = \{g, -g\} = \{1, -1\}g$ для кожного $g \in Q_8$.

Рекомендована література : [**2**, с. 43–54, 76–79], [**4**, с. 31–36], [**9**, с. 98–103], [**15**, с. 155–161], [**16**, с. 14–17].

Вправи до лекції 5.

5.1. Знайти ліві та праві суміжні класи групи S_3 за підгрупою $H = \{(1), (23)\}$. З'ясувати, чи група H є нормальною підгрупою групи S_3.

5.2. З'ясувати, чи підгрупа $H = \langle(123)\rangle = \{(1), (123), (132)\}$ є нормальною підгрупою групи A_4.

5.3. Навести приклад неабелевої групи G і нормальної підгрупи $H \lhd G$, що G/H і H – абелеві групи.

5.4. Показати, що підгрупа $H = \{(1), (12)(34), (13)(24), (14)(23)\}$ є нормальною і абелевою підгрупою групи A_4. Знайти нормальну підгрупу групи H, яка не є нормальною підгрупою групи A_4. Звідси вивести, що бінарне відношення "бути нормальною" не є транзитивним.

5.5. З'ясувати, для яких $k \in \mathbb{Z}$ підмножини $\{0, 2k + 1\}$ є нормальними підгрупами групи $(\mathbb{Z}, *)$, де $m * n = (-1)^n m + n$.

5.6. Довести, що $A_n \lhd S_n$.

5.7. Показати, що група $SL(n,\mathbb{R})$ є нормальною підгрупою групи $GL(n,\mathbb{R})$. Охарактеризувати суміжні класи групи $GL(n,\mathbb{R})$ за підгрупою $SL(n,\mathbb{R})$.

5.8. Показати, що діедральна група D_4 містить нормальну підгрупу H порядку 2. Побудувати таблицю Келі факторгрупи G/H. З'ясувати, чи є G/H циклічною. Побудувати таку бієкцію $\psi : G/H \to V_4$, що при заміні в таблиці Келі для G/H усіх елементів групи G/H їх образами в групі Клейна V_4, отримаємо таблицю Келі групи V_4.

5.9. Довести, що множина $\mathrm{Shift}\,(\mathbb{R})$ всіх зсувів вигляду $r_b(x) = x + b$ є нормальною підгрупою групи $\mathrm{Aff}\,(\mathbb{R})$ всіх афінних відображень $f : \mathbb{R} \to \mathbb{R}$, $f(x) = ax + b$, де $a, b \in \mathbb{R}$, $a \neq 0$, з операцією композиції відображень.

5.10. Чи є нормальною підгрупою групи $GL(n,\mathbb{R})$ підмножина діагональних (верхньотрикутних) матриць з ненульовими діагональними елементами?

5.11. Нехай $H = \{a \in G \mid a^{-1} = a\}$ є підгрупою групи G. Довести, що H є нормальною підгрупою групи G.

5.12. Описати факторгрупу групи $(\mathbb{R}, +)$ за підгрупою $\mathbb{Z}$.

5.13. Побудувати таблицю Келі факторгрупи групи $(\mathbb{R}\backslash\{0\}, \cdot)$ за підгрупою $(0, +\infty)$.

5.14. Побудувати таблицю Келі групи $3\mathbb{Z}$ за підгрупою $18\mathbb{Z}$.

5.15. У факторгрупі $\mathbb{Q}/\mathbb{Z}$ знайти порядок і найменший додатній представник суміжного класу:

а) $\overline{20,3}$; б) $\overline{2,37}$; в) $\overline{-3,25}$.

5.16. Скласти таблиці Келі всіх факторгруп циклічної групи C_8.

5.17. Описати факторгрупу групи $(\mathbb{C}\backslash\{0\}, \cdot)$ за підгрупою $\mathbb{T} = \{z \in \mathbb{C} : |z| = 1\}$.

5.18. Побудувати таблицю Келі факторгрупи групи $(\mathbb{Z}, *)$, де $m*n = (-1)^n m + n$, за підгрупою $6\mathbb{Z}$. Порівняти її будову з будовами груп S_3 та D_3.

5.19. Описати факторгрупу групи $(\mathbb{Q}\backslash\{0\}, \cdot)$ за підгрупою H всіх раціональних чисел, які можна подати у вигляді частки двох непарних чисел.

5.20. Показати, що кожна факторгрупа G/H абелевої групи G є абелевою.

5.21. Довести, що для $n \geqslant 3$ група S_n не містить нормальної підгрупи порядку 2.

5.22. Нехай $G = \langle a \rangle$ – циклічна група порядку n. Чому дорівнює порядок факторгрупи $G/\langle a^k \rangle$?

5.23. Довести, що $\mathbb{Q}/\mathbb{Z}$ – періодична група, яка містить єдину підгрупу порядку n для кожного $n \in \mathbb{N}$. І кожна така підгрупа – циклічна.

5.24. Нехай K – підгрупа групи G, $H \lhd G$. Довести, що $H \cap K \lhd K$.

5.25. Нехай H – підгрупа групи G. Довести, що

$$\bigcap_{g \in G} g^{-1} H g \lhd G.$$

5.26. Довести, що перетин довільної непорожньої сім'ї нормальних підгруп групи G є нормальною підгрупою групи G.

5.27. Нехай H – нормальна підгрупа групи G і $|G/H| = n < \infty$. Довести, що $g^n \in H$ для кожного $g \in G$.

5.28. Нехай $H \lhd G$. Довести, що з періодичності груп H і G/H випливає періодичність групи G.

5.29. Довести, що якщо H – єдина підгрупа порядку n групи G, то $H \lhd G$. Вивести звідси, що група G не є простою, якщо для деякого $n \in \mathbb{N}$ вона містить єдину нетривіальну підгрупу порядку n.

5.30. Нехай H – така підгрупа групи G, що добуток кожних двох правих суміжних класів знову є правим суміжним класом. Довести, що $H \lhd G$.

5.31. Нехай G – група, $(ab)^n = a^n b^n$ для деякого $n \in \mathbb{N}\backslash\{1\}$ і кожних $a, b \in G$. Довести, що $H_n = \{g^n \mid g \in G\}$ є нормальною підгрупою групи G.

5.32. Нехай H – підгрупа групи G і для кожних $a, b \in G$ з $Ha \neq Hb$ випливає, що $aH \neq bH$. Довести, що $H \lhd G$.

5.33. Довести, що підгрупа H групи G є нормальною тоді і лише тоді, коли разом з добутком ab елементів a і b групи G вона також містить добутки квадратів a^2b^2 цих елементів.

5.34. Нехай H – підгрупа групи G, N – нормальна підгрупа групи G, та $(|G : H|, |N|) = 1$. Довести, що N є підгрупою групи H.

Лекція 6. Морфізми груп. Теорема Келі

Нехай $(G, *)$ і $(G', \circ)$ – групи. Відображення $\varphi : G \to G'$ називається *гомоморфізмом* групи $(G, *)$ в групу $(G', \circ)$, якщо

$$\varphi(a * b) = \varphi(a) \circ \varphi(b)$$

для будь-яких $a, b \in G$.

Ядром гомоморфізму $\varphi : G \to G'$ називається множина всіх елементів групи $(G, *)$, які відображаються в одиничний елемент e' групи $(G', \circ)$, і позначається $\operatorname{Ker}\varphi$, тобто

$$\operatorname{Ker}\varphi = \{g \in G \mid \varphi(g) = e'\}.$$

Образ $\varphi(G) = \{\varphi(g) \mid g \in G\}$ гомоморфізму $\varphi : G \to G'$ позначають через $\operatorname{Im}\varphi$.

Приклад 6.1. Нехай e' – одиниця групи $(G', \circ)$. Відображення $\varphi : G \to G'$, $\varphi(g) = e'$ для кожного $g \in G$, є гомоморфізмом, бо

$$\varphi(a * b) = e' = e' \circ e' = \varphi(a) \circ \varphi(b) \quad \text{для всіх } a, b \in G.$$

Даний гомоморфізм називатимемо *тривіальним* гомоморфізмом групи $(G, *)$ в групу $(G', \circ)$. Очевидно, що $\operatorname{Ker}\varphi = G$, $\operatorname{Im}\varphi = \{e'\}$.

Твердження 6.1.

Нехай $\varphi : G \to G'$ – гомоморфізм групи $(G, *)$ в групу $(G', \circ)$. Тоді:

1) *одиниця e групи $(G, *)$ відображається в одиницю e' групи $(G', \circ)$, тобто $\varphi(e) = e'$;*
2) *обернений елемент a^{-1} до елемента $a \in G$ відображається в обернений $\varphi(a)^{-1}$ до елемента $\varphi(a) \in G'$, тобто $\varphi(a^{-1}) = \varphi(a)^{-1}$ для кожного $a \in G$;*
3) *образ $\operatorname{Im}\varphi$ гомоморфізму φ є підгрупою групи $(G', \circ)$;*
4) *ядро гомоморфізму є нормальною підгрупою групи $(G, *)$, тобто $\operatorname{Ker}\varphi \lhd G$.*

Доведення. 1) Згідно з означенням гомоморфізму

$$\varphi(e) \circ \varphi(e) = \varphi(e * e) = \varphi(e) = \varphi(e) \circ e'.$$

Домноживши дані рівності зліва на $\varphi(e)^{-1}$, отримаємо $\varphi(e) = e'$.

2) Оскільки $e = a^{-1} * a$, то

$$e' = \varphi(e) = \varphi(a^{-1} * a) = \varphi(a^{-1}) \circ \varphi(a),$$

тобто $\varphi(a^{-1}) = \varphi(a)^{-1}$.

3) Якщо $a', b' \in \operatorname{Im}\varphi$, то існують такі елементи $a, b \in G$, що $\varphi(a) = a'$, $\varphi(b) = b'$. Оскільки $(G, *)$ – група, то $a * b, a^{-1} \in G$. Тоді

$$a' \circ b' = \varphi(a) \circ \varphi(b) = \varphi(a * b) \in \operatorname{Im}\varphi,$$

і

$$(a')^{-1} = \varphi(a)^{-1} = \varphi(a^{-1}) \in \operatorname{Im}\varphi,$$

тобто $\operatorname{Im}\varphi$ – підгрупа групи $(G', \circ)$.

4) Нехай $a, b \in \operatorname{Ker}\varphi$, тобто $\varphi(a) = \varphi(b) = e'$. Тоді

$$\varphi(a * b) = \varphi(a) \circ \varphi(b) = e' \circ e' = e', \quad \text{звідки } a * b \in \operatorname{Ker}\varphi.$$

Оскільки

$$\varphi(a^{-1}) = \varphi(a)^{-1} = e'^{-1} = e', \quad \text{то } a^{-1} \in \operatorname{Ker}\varphi.$$

Отже, $\operatorname{Ker}\varphi$ – підгрупа групи $(G, *)$.

Для кожних $g \in G, a \in \operatorname{Ker}\varphi$ маємо:

$$\varphi(g^{-1} * a * g) = \varphi(g^{-1}) \circ \varphi(a) \circ \varphi(g) =$$
$$= \varphi(g)^{-1} \circ e' \circ \varphi(g) = \varphi(g)^{-1} \circ \varphi(g) = e'.$$

Таким чином, $g^{-1} * a * g \in \operatorname{Ker}\varphi$, а тому $\operatorname{Ker}\varphi$ – нормальна підгрупа групи $(G, *)$.

□

Приклад 6.2. Знайдемо всі гомоморфізми, які діють з циклічної групи $\langle a \rangle = \{e, a, \ldots, a^5\}$ порядку 6 у циклічну групу $\langle b \rangle = \{e', b, \ldots, b^8\}$ порядку 9.

Нехай $\varphi : \langle a \rangle \to \langle b \rangle$ – гомоморфізм і $\varphi(a) = b^m$, де $m \in \{0, 1, \ldots, 8\}$. Тоді

$$\varphi(a^k) = \varphi(a \cdot \ldots \cdot a) = \varphi(a) \cdot \ldots \cdot \varphi(a) = (\varphi(a))^k = (b^m)^k = b^{mk}$$

для кожного $k \in \mathbb{Z}$.

Зокрема при $k = 6$ маємо:

$$b^{6m} = \varphi(a^6) = \varphi(e) = e'.$$

Оскільки $|b| = 9$, то $6m$ ділиться на 9, звідки $2m$ ділиться на 3. З $(2, 3) = 1$ випливає, що m ділиться на 3, а тому $m \in \{0, 3, 6\}$.

Таким чином, маємо 3 гомоморфізми:

$$\varphi_1 : a^k \mapsto b^{0k} = e', \quad \varphi_2 : a^k \mapsto b^{3k}, \quad \varphi_3 : a^k \mapsto b^{6k}.$$

Враховуючи, що $b^{9+i} = b^i$, задамо їх у вигляді наступної таблиці:

x	$\varphi_1(x)$	$\varphi_2(x)$	$\varphi_3(x)$
e	e'	e'	e'
a	e'	b^3	b^6
a^2	e'	b^6	b^3
a^3	e'	e'	e'
a^4	e'	b^3	b^6
a^5	e'	b^6	b^3

З таблиці знаходимо:

$$\operatorname{Ker}\varphi_1 = \langle a\rangle, \quad \operatorname{Ker}\varphi_2 = \operatorname{Ker}\varphi_3 = \{e, a^3\},$$
$$\operatorname{Im}\varphi_1 = \{e'\}, \quad \operatorname{Im}\varphi_2 = \operatorname{Im}\varphi_3 = \{e', b^3, b^6\}.$$

Якщо $\varphi : G \to G'$ – гомоморфізм групи $(G, *)$ в групу $(G', \circ)$, то підгрупу $\operatorname{Im}\varphi = \varphi(G)$ групи $(G', \circ)$ називають *зображенням* групи $(G, *)$ в групі $(G', \circ)$. Зображенням групи групи $(G, *)$ в групу $(G', \circ)$ називають також і гомоморфізм $\varphi : G \to G'$. Зображення називається *точним*, якщо $\varphi : G \to G'$ – ін'єкція. Гомоморфізм $\varphi : G \to GL(n, F)$ називається *лінійним зображенням* групи $(G, *)$ в групі $GL(n, F)$.

Твердження 6.2.

Якщо $\varphi : G \to G'$ – гомоморфізм групи $(G, *)$ в групу $(G', \circ)$, a – елемент скінченного порядку групи $(G, *)$, то $|\varphi(a)|$ є дільником $|a|$.

Доведення. Нехай $|a| = n$, $|\varphi(a)| = m$. За означенням гомоморфізму $\varphi(a)^n = \varphi(a^n) = \varphi(e) = e'$. Тоді m є дільником n за теоремою 3.2. □

Гомоморфізм $\varphi : G \to G'$ називається *мономорфізмом*, якщо $\operatorname{Ker}\varphi = \{e\}$. З означення ядра випливає, що гомоморфізм φ є мономорфізмом тоді і лише тоді, коли φ є ін'єкцією.

Якщо $\operatorname{Im}\varphi = G'$, то гомоморфізм $\varphi : G \to G'$ називається *епіморфізмом*. Зрозуміло, що в цьому випадку φ – сюр'єкція.

Гомоморфізм $\varphi : G \to G'$, який є одночасно мономорфізмом і епіморфізмом, називається *ізоморфізмом*, а групи $(G, *)$ і $(G', \circ)$ – *ізоморфними*. У цьому випадку пишемо $(G, *) \cong (G', \circ)$. Гомоморфізм $\varphi : G \to G'$ є ізоморфізмом тоді і лише тоді, коли відображення φ є бієкцією. Ізоморфні групи мають однакову будову, а тому в теорії груп вони не розрізняються. Одним з основних завдань теорії груп є класифікація груп з точністю до ізоморфізму.

Якщо $\varphi : G \to G'$ – мономорфізм, то група $(G, *)$ – ізоморфна підгрупі $\operatorname{Im}\varphi$ групи G'. Тому мономорфізм $\varphi : G \to G'$ називають також *вкладенням* групи $(G, *)$ в групу $(G', \circ)$.

Приклад 6.3. Розглянемо групи $(\mathbb{R}, +)$ і $(\mathbb{R}_+, \cdot)$, де $\mathbb{R}_+ = \{x \in \mathbb{R} \mid x > 0\}$. Відображення $\psi : \mathbb{R} \to \mathbb{R}_+$, $\varphi(x) = 2^x$, є гомоморфізмом. Дійсно,

$$\psi(x + y) = 2^{x+y} = 2^x 2^y = \psi(x)\psi(y)$$

для кожних $x, y \in \mathbb{R}$.

Крім того, для кожного $y \in \mathbb{R}_+$ дійсне число $x = \log_2 y$ відображається в y:

$$\psi(x) = \psi(\log_2 y) = 2^{\log_2 y} = y.$$

Отже, ψ – епіморфізм. Якщо $\psi(x) = \psi(y)$, то $2^x = 2^y$, звідки $x = y$. Тому ψ – мономорфізм.

Таким чином, відображення $\psi : \mathbb{R} \to \mathbb{R}_+$ є ізоморфізмом, а групи $(\mathbb{R}, +)$ і $(\mathbb{R}_+, \cdot)$ – ізоморфні.

Гомоморфізм $\varphi : G \to G$ називається *ендоморфізмом* групи $(G, *)$. Множину всіх ендоморфізмів групи $(G, *)$ позначають через $\mathrm{End}\,(G)$.

Бієктивний ендоморфізм $\varphi : G \to G$ називається *автоморфізмом* групи $(G, *)$. Через $\mathrm{Aut}\,(G)$ позначають множину всіх автоморфізмів групи $(G, *)$.

Приклад 6.4. Покажемо, що для кожного елемента a групи $(G, *)$ відображення

$$\psi_a : G \to G, \quad \psi_a(x) = a^{-1} * x * a$$

є автоморфізмом. Дійсно,

$$\psi_a(x * y) = a^{-1} * x * y * a = a^{-1} * x * a * a^{-1} * y * a = \psi_a(x) * \psi_a(y)$$

для кожних $x, y \in G$.

Якщо $\psi_a(x) = \psi_a(y)$, то $a^{-1} * x * a = a^{-1} * y * a$, звідки $x = y$, і ψ_a – ін'єкція. Для кожного $y \in G$ елемент $x = a * y * a^{-1}$ відображається в y, а тому ψ_a – сюр'єкція.

Таким чином, відображення ψ_a – автоморфізм групи G.

Автоморфізм $\psi_a : G \to G, \quad \psi_a(x) = a^{-1} * x * a$, називається *внутрішнім автоморфізмом* групи $(G, *)$, породженим елементом $a \in G$. Множину всіх внутрішніх автоморфізмів групи $(G, *)$ позначають через $\mathrm{Inn}\,(G)$.

Твердження 6.3.

Кожна нескінченна циклічна група є ізоморфною групі $(\mathbb{Z}, +)$.

Доведення. Нехай $G = \langle a \rangle$ – нескінченна циклічна група, породжена елементом a. Розглянемо відображення

$$\psi : \mathbb{Z} \to G, \quad \psi(n) = a^n.$$

Для кожних $m, k \in \mathbb{Z}$ маємо:

$$\psi(m + k) = a^{m+k} = a^m a^k = \psi(m)\psi(k).$$

Тому ψ – гомоморфізм.

Оскільки кожен елемент $g \in G$ є степенем елемента a, то $g = a^n$ для деякого $n \in \mathbb{Z}$. Звідки $\psi(n) = a^n = g$, а тому ψ є епіморфізмом. З означення нескінченної циклічної групи випливає, що $a^k \neq a^m$ при $k \neq m$, а тому ψ – мономорфізм. □

Твердження 6.4.

Кожна скінченна циклічна група порядку n є ізоморфною групі

$$C_n = \{z \in \mathbb{C} \mid z^n = 1\}$$

комплексних коренів n-го степеня з 1.

Доведення. Нехай $G = \langle a \rangle = \{e, a, \ldots, a^{n-1}\}$ – скінченна циклічна група порядку n, породжена елементом a. Нагадаємо, що комплексні корені n-го степеня з 1 мають вигляд:

$$\xi_k = \cos\frac{2\pi k}{n} + i\sin\frac{2\pi k}{n}, \quad \text{де } k \in \{0, 1, \ldots, n-1\}.$$

Зауважимо, що $\xi_{n+i} = \xi_i$ і $a^{n+i} = a^i$ для кожного $i \in \mathbb{Z}$. Розглянемо відображення

$$\psi : C_n \to G, \quad \psi(\xi_k) = a^k.$$

Для кожних $\xi_m, \xi_k \in C_n$ маємо:

$$\psi(\xi_m\xi_k) = \psi(\xi_{m+k}) = a^{m+k} = a^m a^k = \psi(\xi_m)\psi(\xi_k).$$

Тому ψ – гомоморфізм.

Нехай $\psi(\xi_m) = \psi(\xi_k)$, де $m, k \in \{0, 1, \ldots, n-1\}$. Тоді $a^m = a^k$. Звідси випливає, що

$$a^{m-k} = a^{k-m} = e \quad i \quad |m-k| < n.$$

Оскільки a – елемент порядку n, то $m - k = 0$, а отже, $\xi_m = \xi_k$. Очевидно, що відображення ψ є епіморфізмом, а тому ψ – ізоморфізм груп C_n і G. □

Нехай $(G, *)$ – група, H – її нормальна підгрупа. Розглянемо відображення

$$\pi : G \to G/H, \quad \pi(g) = \overline{g}.$$

Оскільки

$$\pi(a * b) = \overline{a * b} = \overline{a} * \overline{b} = \pi(a) * \pi(b)$$

для кожних $a, b \in G$, то відображення π є гомоморфізмом.

Гомоморфізм $\pi : G \to G/H$ називається *природнім* гомоморфізмом групи G на факторгрупу G/H. Очевидно, що $\operatorname{Ker}\pi = H$.

Теорема 6.1 (Основна теорема про гомоморфізми для груп).

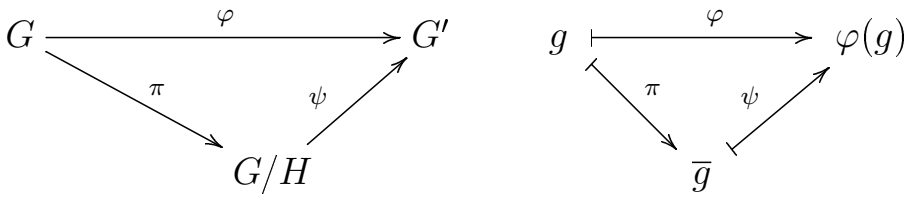
Якщо $\varphi : G \to G'$ – гомоморфізм групи $(G, *)$ в групу $(G', \circ)$, то факторгрупа групи G за ядром $\operatorname{Ker}\varphi$ ізоморфна образу $\operatorname{Im}\varphi$, тобто $G/\operatorname{Ker}\varphi \cong \operatorname{Im}\varphi$. Зокрема, якщо $\varphi : G \to G'$ – епіморфізм, то $G/\operatorname{Ker}\varphi \cong G'$.

Доведення. Оскільки за твердженням 6.1(4) ядро $H = \operatorname{Ker}\varphi$ є нормальною підгрупою групи G, то факторгрупа G/H існує. Поставимо у відповідність елементу $\overline{g} = g * H$, де $g \in G$, факторгрупи G/H елемент $\varphi(g)$ підгрупи $\operatorname{Im}\varphi = \varphi(G)$ групи G', тобто визначимо відповідність

$$\psi : G/H \to \operatorname{Im}\varphi \subset G', \quad \psi(\overline{g}) = \varphi(g).$$

Оскільки $\overline{g} = \pi(g)$, де $\pi : G \to G/H$ – природній гомоморфізм, то для кожного $g \in G$ маємо $\psi(\pi(g)) = \varphi(g)$, тобто $\psi \circ \pi = \varphi$.

Зобразимо визначену відповідність діаграмами:



Якщо $a \in \overline{g}$, то $a = g * h$ для деякого $h \in H$, а тому

$$\varphi(a) = \varphi(g * h) = \varphi(g) \circ \varphi(h) = \varphi(g) \circ e' = \varphi(g).$$

Таким чином, відповідність ψ не залежить від вибору представника суміжного класу і кожному елементу $\overline{g} \in G/H$ ставиться у відповідність єдиний елемент $\varphi(g) \in \operatorname{Im}\varphi$, тобто ψ є відображенням групи G/H в групу $\operatorname{Im}\varphi$.

Оскільки

$$\psi(\overline{a} * \overline{b}) = \psi(\overline{a * b}) = \varphi(a * b) = \varphi(a) \circ \varphi(b) = \psi(\overline{a}) \circ \psi(\overline{b}),$$

то ψ – гомоморфізм.

Якщо $\varphi(a)$ – довільний елемент образу $\operatorname{Im}\varphi$, то $\varphi(a) = \psi(\overline{a})$, тобто ψ – сюр'єкція.

Якщо $\psi(\overline{a}) = \psi(\overline{b})$, то $\varphi(a) = \varphi(b)$. Тоді $\varphi(a^{-1} * b) = e'$, а тому $a^{-1} * b \in \operatorname{Ker}\varphi = H$, звідки $\overline{a} = \overline{b}$. Таким чином, ψ – ін'єкція, а отже, ψ – ізоморфізм груп G/H і $\operatorname{Im}\varphi$. □

Приклад 6.5. Покажемо, що факторгрупа групи $(\mathbb{R}\backslash\{0\}, \cdot)$ за підгрупою $H = \{-1, 1\}$ є ізоморфною групі $(\mathbb{R}_+, \cdot)$. Розглянемо відображення

$$\varphi : \mathbb{R}\backslash\{0\} \to \mathbb{R}_+, \quad \varphi(x) = |x|.$$

Оскільки

$$\varphi(xy) = |xy| = |x| \cdot |y| = \varphi(x)\varphi(y) \quad \text{і} \quad \operatorname{Im}\varphi = \mathbb{R}_+,$$

то відображення φ є епіморфізмом з ядром

$$\operatorname{Ker}\varphi = \{x \in \mathbb{R} \mid \varphi(x) = 1\} = \{x \in \mathbb{R} \mid |x| = 1\} = \{-1, 1\}.$$

За теоремою 6.1 факторгрупа групи $(\mathbb{R}\backslash\{0\}, \cdot)$ за підгрупою $\operatorname{Ker}\varphi = \{-1, 1\} = H$ є ізоморфною групі $\operatorname{Im}\varphi = \mathbb{R}_+$.

Приклад 6.6. Покажемо, що не існує епіморфізму $\varphi : S_3 \to C_3$. Дійсно, якби такий епіморфізм існував, то $S_3/\operatorname{Ker}\varphi \cong C_3$. За теоремою Лагранжа $|\operatorname{Ker}\varphi| = \frac{|S_3|}{|C_3|} = \frac{6}{3} = 2$. Отже, $\operatorname{Ker}\varphi$ – нормальна підгрупа порядку 2 групи S_3. Однак група S_3 не містить нормальних підгруп порядку 2.

Нехай $(G, *)$ – група. Для кожного $a \in G$ відображення

$$l_a : G \to G, \quad l_a(g) = a * g$$

називатимемо *лівим зсувом* на елемент a.

Теорема 6.2 (Теорема Келі).

Кожна група $(G, *)$ ізоморфна деякій підгрупі симетричної групи S_G.

Доведення. Спершу покажемо, що для кожного $a \in G$ відображення l_a є підстановкою на множині G, тобто – бієктивним відображенням. Якщо $l_a(g_1) = l_a(g_2)$, то $a * g_1 = a * g_2$, звідки, домноживши на a^{-1} зліва, отримаємо $g_1 = g_2$. Отже, $l_a : G \to G$ – ін'єкція. Для кожного $g \in G$ елемент $h = a^{-1} * g \in G$ відображається в g:

$$l_a(h) = l_a(a^{-1} * g) = a * a^{-1} * g = g,$$

а тому $l_a : G \to G$ – сюр'єкція. Таким чином, $l_a : G \to G$ є підстановкою, тобто $l_a \in S_G$.

Визначимо відображення

$$\psi : G \to S_G, \quad \psi(a) = l_a.$$

Покажемо, що $l_a \circ l_b = l_{a*b}$ для кожних $a, b \in G$. Дійсно, для кожного $g \in G$ маємо:

$$l_a \circ l_b(g) = l_a(l_b(g)) = l_a(b * g) = a * (b * g) = (a * b) * g = l_{a*b}(g).$$

Оскільки

$$\psi(a * b) = l_{a*b} = l_a \circ l_b = \psi(a) \circ \psi(b),$$

то ψ – гомоморфізм.

Якщо $a \neq b$, то $l_a(e) = a \neq b = l_b(e)$. Отже, $l_a \neq l_b$, а тому ψ – мономорфізм.

Таким чином, група $(G, *)$ є ізоморфною підгрупі

$$\operatorname{Im}\psi = \psi(G) = \{\ l_a \mid a \in G\ \}$$

групи S_G. □

Приклад 6.7. Побудуємо вкладення групи Клейна

$$V_4 = \langle a, b \mid a^2 = b^2 = e, ab = ba \rangle$$

в групу S_4. Покладемо $c = ab$. Користуючись доведенням теореми Келі, отримаємо:

$$\psi(e) = l_e = \begin{pmatrix} e & a & b & c \\ ee & ea & eb & ec \end{pmatrix} = \begin{pmatrix} e & a & b & c \\ e & a & b & c \end{pmatrix} = (e),$$

$$\psi(a) = l_a = \begin{pmatrix} e & a & b & c \\ ae & aa & ab & ac \end{pmatrix} = \begin{pmatrix} e & a & b & c \\ a & e & c & b \end{pmatrix} = (ea)(bc),$$

$$\psi(b) = l_b = \begin{pmatrix} e & a & b & c \\ be & ba & bb & bc \end{pmatrix} = \begin{pmatrix} e & a & b & c \\ b & c & e & a \end{pmatrix} = (eb)(ac),$$

$$\psi(c) = l_c = \begin{pmatrix} e & a & b & c \\ ce & ca & cb & cc \end{pmatrix} = \begin{pmatrix} e & a & b & c \\ c & b & a & e \end{pmatrix} = (ec)(ab).$$

Занумерувавши елементи e, a, b, c числами $1, 2, 3, 4$ відповідно, отримаємо, що група V_4 ізоморфна підгрупі

$$H = \{(1), (12)(34), (13)(24), (14)(23)\}$$

групи S_4.

Рекомендована література : [**2**, с. 32–34, 37–39, 62–64], [**9**, с. 106–112], [**11**, с. 12–14], [**12**, с. 97–100], [**13**, с. 36–41], [**15**, с. 141-146, 165–174].

Вправи до лекції 6.

6.1. З'ясувати, чи є гомоморфізмом групи $(\mathbb{Z}, +)$ у себе відображення:

а) $\varphi(n) = 4n$; б) $\varphi(n) = 3n + 2$; в) $\varphi(n) = n^2$.

6.2. Показати, що відображення, задане формулою $\psi(x) = 5 \ln x$, є ізоморфізмом групи $(\mathbb{R}_+, \cdot)$ в групу $(\mathbb{R}, +)$.

6.3. Довести, що відображення

$$f : \mathbb{R} \times \mathbb{R} \to \mathbb{R}, \quad f(x, y) = x + y,$$

є гомоморфізмом групи $(\mathbb{R} \times \mathbb{R}, +)$, де $(a, b) + (c, d) = (a + c, b + d)$, в групу $(\mathbb{R}, +)$. Зобразити його ядро та прообрази геометрично.

6.4. Показати, що відображення

$$\varphi : \mathbb{R} \to \mathbb{C}\backslash\{0\}, \quad \varphi(\theta) = \cos\theta + i \sin\theta,$$

є гомоморфізмом груп $(\mathbb{R}, +)$ та $(\mathbb{C}\backslash\{0\}, \cdot)$. Довести, що його ядро ізоморфне $(\mathbb{Z}, +)$.

6.5. Побудувати всі гомоморфізми з циклічної групи C_{12} у циклічну групу C_{15}. Знайти їх ядра та образи.

6.6. Довести, що групи $4\mathbb{Z}/12\mathbb{Z}$ і $3\mathbb{Z}/9\mathbb{Z}$ – ізоморфні.

6.7. Побудувати точне лінійне зображення групи C_4 в групі $GL(2, \mathbb{C})$.

6.8. Показати, що відображення $\varphi(x) = x^2 + 1$ є гомоморфізмом групи $(\mathbb{Q}\backslash\{0\}, \cdot)$ в групу $\mathbb{Q}\backslash\{1\}$ з бінарною операцією $a * b = ab - a - b + 2$.

6.9. Показати, що відображення $\varphi(x) = 3^x - 2$ є ізоморфізмом групи $(\mathbb{R}, +)$ в групу $(-2, +\infty)$ з бінарною операцією $*$, де $a * b = ab + 2(a + b + 1)$.

6.10. Довести, що для кожного $\alpha \in \mathbb{R}$ група $(\alpha, +\infty)$ з операцією $x * y = (x - \alpha)(y - \alpha) + \alpha$ ізоморфна групі $(\mathbb{R}, +)$.

6.11. Довести, що гомоморфізм $\psi : G \to G'$ є ізоморфізмом тоді і лише тоді, коли існує таке відображення $\phi : G' \to G$, що $\psi \circ \phi = \mathrm{Id}_{G'}$ і $\phi \circ \psi = \mathrm{Id}_G$.

6.12. Нехай $\psi : G \to G'$ – ізоморфізм, $a, b \in G$. Довести:

- $|a| = |\psi(a)|$;
- $ab = ba$ тоді і лише тоді, коли $\psi(a)\psi(b) = \psi(b)\psi(a)$.

6.13. Показати, що дві скінченні групи G і G' є ізоморфними тоді і лише тоді, коли існує така бієкція $\psi : G \to G'$, що при заміні в таблиці Келі групи G всіх елементів їх образами в групі G', отримаємо таблицю Келі групи G'.

6.14. Довести, що група S_3 є ізоморфною групі $(\{0, 1, 2, 3, 4, 5\}, *)$, де $a * b$ – остача від ділення $a + (-1)^a b$ на 6.

6.15. Довести, що для кожного $n \in \mathbb{N}$ факторгрупа $\mathbb{Z}/2n\mathbb{Z}$ групи $(\mathbb{Z}, *)$, де $a * b = (-1)^b a + b$, за підгрупою $2n\mathbb{Z}$ є ізоморфною діедральній групі D_n.

6.16. Нехай $G = (\mathbb{C}\backslash\{0\}, \cdot)$. Довести, що відображення φ є ендоморфізмом. Знайти його образ і ядро. Використовуючи доведення основної теореми про гомоморфізми, побудувати ізоморфізм $\psi : G/\mathrm{Ker}\,\varphi \to \mathrm{Im}\,\varphi$, якщо:

а) $\varphi(z) = |z|$; б) $\varphi(z) = \frac{z}{|z|}$; в) $\varphi(z) = \frac{\overline{z}}{z}$.

6.17. Використовуючи основну теорему про гомоморфізми, показати, що факторгрупа S_n/A_n ізоморфна підгрупі $\{-1, 1\}$ групи $(\mathbb{R}\backslash\{0\}, \cdot)$.

6.18. Довести, що $GL(n, \mathbb{R})/SL(n, \mathbb{R}) \cong (\mathbb{R}\backslash\{0\}, \cdot)$.

6.19. Довести, що факторгрупа групи $(\mathbb{Q}_+, \cdot)$ за підгрупою H всіх додатніх раціональних чисел, які можна подати у вигляді частки двох непарних чисел, є ізоморфною групі $(\mathbb{Z}, +)$.

6.20. Показати, що відображення

$$\varphi : \mathbb{R} \to \mathbb{T} = \{z \in \mathbb{C} \ : \ |z| = 1\}, \quad \varphi(x) = e^{2\pi x i} = \cos(2\pi x) + i \sin(2\pi x)$$

є епіморфізмом групи $(\mathbb{R}, +)$ на групу $(\mathbb{T}, \cdot)$. Вивести звідси, що $\mathbb{R}/\mathbb{Z} \cong \mathbb{T}$.

6.21. Показати, що група $(\mathbb{Q}_+, \cdot)$ не є ізоморфною групі $(\mathbb{Q}, +)$.

6.22. Довести, що множина $\mathrm{End}\,(G)$ з операцією композиції є моноїдом, але не є групою.

6.23. Довести, що множина $\mathrm{Aut}\,(G)$ є підгрупою симетричної групи S_G.

6.24. Довести, що $\mathrm{Inn}\,(G) \lhd \mathrm{Aut}\,(G)$.

6.25. Показати, що відображення $\psi : \mathbb{C}\backslash\{0\} \to \mathbb{C}\backslash\{0\}$, $\psi(a + ib) = a - ib$, є автоморфізмом групи $(\mathbb{C}\backslash\{0\}, \cdot)$.

6.26. Довести, що відображення $\psi : G \to G$, $\psi(g) = g^{-1}$, є автоморфізмом абелевої групи G.

6.27. Нехай G – абелева група порядку n, $(n, m) = 1$, $m \in \mathbb{N}$. Довести, що відображення $\varphi : g \mapsto g^m$ є автоморфізмом групи G.

6.28. Знайти моноїд ендоморфізмів та групу автоморфізмів циклічної групи порядку n.

6.29. За яких умов на групу G відображення $\varphi : G \to G$, $\varphi : g \mapsto g^2$, є гомоморфізмом?

6.30. Побудувати вкладення групи Q_8 в групу S_8.

6.31. Довести, що не існує нетривіального гомоморфізму з групи порядку 5 в групу порядку 6.

6.32. З'ясувати, на які з груп C_2, C_4 і V_4 існують епіморфізми з групи Q_8.

6.33. З'ясувати, чи існує епіморфізм $\varphi : A_4 \to V_4$.

6.34. Довести, що не існує нетривіальних гомоморфізмів $\varphi : \mathbb{Q} \to \mathbb{Z}$.

6.35. *Короткою точною послідовністю* називається така послідовність

$$\{e\} \to A \xrightarrow{f} B \xrightarrow{g} C \to \{e\}$$

груп та гомоморфізмів, що образ кожного гомоморфізму збігається з ядром наступного гомоморфізму. Довести, що

а) $f : A \to B$ – мономорфізм; б) $g : B \to C$ – епіморфізм;
в) $B/f(A) \cong C$.

6.36. Нехай $\varphi : G \to G'$ – гомоморфізм групи G в групу G', $H \lhd G$. Довести, що $\varphi(H) \lhd \operatorname{Im}\varphi$.

6.37. Нехай $\varphi : G \to G'$ – гомоморфізм, H' – підгрупа групи G'. Довести, що $H = \varphi^{-1}(H')$ є підгрупою групи G, і якщо $H' \lhd G'$, то $H \lhd G$. Вивести звідси, що $\operatorname{Ker}\varphi \lhd G$.

6.38. Нехай $H \lhd G$. Довести, що для кожної підгрупи K групи G відображення

$$\varphi : KH/H \to K/(H \cap K), \quad \varphi : aH \mapsto a(K \cap H)$$

є ізоморфізмом.

Лекція 7. Дія групи на множині. Центр групи

Нехай X – множина, G – група. У цій лекції розглядатимемо відображення, які кожній парі елементів $g \in G$ і $x \in X$ ставлять у відповідність елемент $y \in X$. Іншими словами, мова буде йти про відображення $\circ : G \times X \to X$. Для спрощення запису образ $\circ(g, x) \in X$ пари $(g, x) \in G \times X$ позначатимемо через $g \circ x$. Якщо з контексту зрозуміло про яку операцію $\circ$ йде мова, то замість $g \circ x$ писатимемо gx.

Дією групи $(G, *)$ *на множині* X називається відображення $\circ : G \times X \to X$, для якого виконано наступні умови:

1) $e \circ x = x$ для кожного $x \in X$;
2) $(g * h) \circ x = g \circ (h \circ x)$ для кожних $g, h \in G$, $x \in X$.

Розглянемо бінарне відношення

$$\rho \subset X \times X, \quad (x, y) \in \rho \;\Leftrightarrow\; \exists g \in G\ (y = g \circ x).$$

Дане відношення є відношенням еквівалентності. Дійсно:

1) *Рефлексивність*. Для кожного $x \in X$ виконано $x = e \circ x$, а тому $(x, x) \in \rho$.
2) *Симетричність*. Нехай $(x, y) \in \rho$. Тоді $y = g \circ x$ для деякого $g \in G$. Тоді $g^{-1} \circ y = g^{-1} \circ (g \circ x) = (g^{-1} * g) \circ x = e \circ x = x$, а тому $(y, x) \in \rho$.

3) *Транзитивність.* Нехай $(x,y),(y,z)\in\rho$. Тоді $y=h\circ x$ і $z=g\circ y$ для деяких $h,g\in G$. Звідси $z=g\circ(h\circ x)=(g*h)\circ x$, а тому $(x,z)\in\rho$.

Отже, відношення ρ задає деяке розбиття множини X.

Клас еквівалентності $G\circ x=\{g\circ x\mid g\in G\}$ елемента $x\in X$ називається *орбітою, породженою елементом* x. Таким чином, під дією групи G множина X розбивається на попарно неперетинні орбіти. Потужність орбіти $G\circ x$ називатимемо також *довжиною орбіти елемента* x.

Дія групи G на множині X називається *транзитивною*, якщо всі елементи множини X належать одній орбіті при цій дії. В цьому випадку множину X називають *однорідним G-простором*. Дія групи G на множині X називається *вільною*, якщо $g\circ x\neq h\circ x$ для будь-яких різних $g,h\in G$ і довільного $x\in X$.

Якщо група G діє на множині X, то *стабілізатором елемента* $x\in X$ називається множина $St(x)$ всіх елементів групи G, які не змінюють x, тобто

$$St(x)=\{g\in G\mid g\circ x=x\}.$$

Твердження 7.1.

Стабілізатор $St(x)$ кожного елемента $x\in X$ є підгрупою групи G.

Доведення. Нехай $g,h\in St(x)$. Тоді $g\circ x=x$ і $h\circ x=x$, звідки

$$(g*h)\circ x=g\circ(h\circ x)=g\circ x=x$$

і

$$g^{-1}\circ x=g^{-1}\circ(g\circ x)=(g^{-1}*g)\circ x=e\circ x=x.$$

Таким чином, $g*h,g^{-1}\in St(x)$, а тому $St(x)$ – підгрупа групи G. □

Зрозуміло, що дія групи G на множині X є вільною тоді і лише тоді, коли стабілізатор кожного елемента $x\in X$ є одиничною підгрупою групи G.

Зауважимо, що у загальному випадку $St(x)$ не є нормальною підгрупою групи G.

Приклад 7.1. Нехай $X=\{-2,-\sqrt{2},0,\sqrt{2},2\}$, $\mathbb{Z}$ – група цілих чисел з операцією додавання. Розглянемо відображення

$$\circ:\mathbb{Z}\times X\to X,\quad n\circ x=(-1)^n x.$$

Оскільки $0\circ x=(-1)^0x=x$ і

$$n\circ(m\circ x)=n\circ((-1)^m x)=(-1)^n(-1)^m x=(-1)^{n+m}x=(n+m)\circ x$$

для кожних $n,m\in\mathbb{Z}$, $x\in X$, то $\circ:\mathbb{Z}\times X\to X$ – дія групи $\mathbb{Z}$ на множині X.

Орбітою елемента $x \in X$ є множина

$$\mathbb{Z} \circ x = \{(-1)^n x \mid n \in \mathbb{Z}\} = \{-x, x\}.$$

Таким чином, під дією групи $\mathbb{Z}$ множина X розіб'ється на три орбіти:

$$\{-2, 2\}, \quad \{-\sqrt{2}, \sqrt{2}\} \quad \text{і} \quad \{0\}.$$

Стабілізатором елемента $x \in X$ є підгрупа

$$St(x) = \{n \in \mathbb{Z} \mid n \circ x = x\} = \{n \in \mathbb{Z} \mid (-1)^n x = x\} \subset \mathbb{Z}.$$

Таким чином, $St(0) = \mathbb{Z}$ і $St(x) = 2\mathbb{Z}$ для кожного $x \in X \backslash \{0\}$. Розглянута дія не є ні транзитивною, ні вільною.

Приклад 7.2. Якщо X – довільна множина і G – підгрупа симетричної групи S_X, то G діє на множині X за правилом $\circ : (s, x) \mapsto s(x)$ для кожних $s \in G$, $x \in X$. Визначену дію називатимемо *природньою*. Нехай $G = S_X$. Тоді для кожного $x \in X$ транспозиція $(ax) \in S_X$ переводить $a \in X$ в x, звідки $G \circ a = X$. Таким чином, дія групи S_X на множині X є транзитивною, а множина X є однорідним S_X-простором.

Приклад 7.3. Нехай X – множина точок площини, G – група всіх векторів площини з операцією додавання векторів. Дію вектора на точку визначимо як паралельне перенесення точки на відповідний вектор. Будь-яку зафіксовану точку $x \in X$ всі вектори площини перенесуть у кожну точку площини. Таким чином, орбіта кожної точки співпадає з множиною всіх точок площини, тобто дія групи векторів на множині точок площини є транзитивною, а множина X є однорідним G-простором.

Твердження 7.2.

Нехай $\circ : G \times X \to X$ – дія групи G на множині X. Тоді для кожного елемента $x \in X$ довжина орбіти $G \circ x$ дорівнює індексу стабілізатора елемента x в групі G, тобто $|G \circ x| = |G : St(x)|$.

Доведення. Визначимо відповідність

$$\psi : G \circ x \to (G : St(x)), \quad \psi(g \circ x) = gSt(x),$$

де $(G : St(x))$ – множина лівих суміжних класів групи G за підгрупою $St(x)$.

Якщо $g\circ x = h\circ x$, то $(h^{-1}g)\circ x = x$, тобто $h^{-1}g \in St(x)$. Звідси випливає, що $g \in hSt(x)$, а тому $gSt(x) = hSt(x)$. Таким чином, ψ – (однозначне) відображення. Очевидно, що дане відображення є сюр'єктивним. Покажемо, що воно є ін'єктивним. Нехай $\psi(g\circ x) = \psi(h\circ x)$, тобто $gSt(x) = hSt(x)$. Тоді $h^{-1}g \in St(x)$. Звідси випливає, що $(h^{-1}g)\circ x = x$, а тому $g\circ x = h\circ x$. □

З попереднього твердження і теореми Лагранжа випливає наступний

Наслідок 7.1.

Якщо група G – скінченна, то $|G| = |G\circ x|\cdot|St(x)|$ для кожного $x \in X$. Зокрема довжина кожної орбіти є дільником порядку скінченної групи.

Якщо X – скінченна множина і $X = G\circ x_1 \sqcup \ldots \sqcup G\circ x_k$ – розбиття множини X на k орбіт відносно дії $\circ : G\times X \to X$, то

$$|X| = \sum_{i=1}^{k} |G\circ x_i| = \sum_{i=1}^{k} |G : St(x_i)|.$$

Розглянемо деякі важливі дії групи на множині.

1) Нехай G – група і $\mathcal{P}(G)$ – множина всіх її підмножин. Розглянемо відображення

$$\circ : G\times\mathcal{P}(G) \to \mathcal{P}(G), \quad g\circ A = gAg^{-1}.$$

Оскільки

$$e\circ A = eAe^{-1} = A$$

і

$$(gh)\circ A = (gh)A(gh)^{-1} = g(hAh^{-1})g^{-1} = g(h\circ A)g^{-1} = g\circ(h\circ A),$$

то $\circ : G\times\mathcal{P}(G) \to \mathcal{P}(G)$ – дія групи G на множині $\mathcal{P}(G)$.

Орбіта $G\circ A = \{gAg^{-1} \mid g \in G\}$ є сім'єю всіх підмножин групи G, спряжених з множиною A. Найцікавішим є випадок, коли множина є підгрупою H групи G, а орбіта – множиною всіх спряжених з H підгруп.

Стабілізатор підмножини A також позначається через

$$N(A) = \{g \in G \mid gAg^{-1} = A\} = \{g \in G \mid gA = Ag\}$$

і називається *нормалізатором* підмножини A в групі G. Зауважимо, що якщо H – підгрупа групи G, то H – підгрупа групи $N(H)$. Зрозуміло, що підгрупа H є нормальною підгрупою групи G тоді і лише тоді, коли $N(H) = G$.

З наслідку 7.1 випливає, що у випадку скінченної групи G кількість різних підмножин, спряжених з множиною A, дорівнює $|G : N(A)|$. Зокрема кількість різних підмножин, спряжених з множиною A, є дільником порядку групи G.

2) Нехай група G діє на множині $X = G$ спряженням елементів:

$$\circ : G\times G \to G, \quad g\circ a = gag^{-1}.$$

Орбіта $G \circ a = \{gag^{-1} \mid g \in G\}$ є класом $K(a)$ всіх елементів групи G, спряжених з елементом a.

Стабілізатор елемента a також позначається через

$$C(a) = \{g \in G \mid gag^{-1} = a\} = \{g \in G \mid ga = ag\}$$

і називається *централізатором* елемента a в групі G.

Приклад 7.4. Знайдемо клас спряжених елементів і централізатор елемента (12) симетричної групи S_3.

$(1)(12)(1)^{-1} = (12)$, $(12)(12)(12)^{-1} = (12)$,
$(13)(12)(13)^{-1} = (123)(13) = (23)$, $(23)(12)(23)^{-1} = (132)(23) = (13)$,
$(123)(12)(123)^{-1} = (13)(132) = (23)$, $(132)(12)(132)^{-1} = (23)(123) = (13)$.

Отже, $K(12) = \{(12), (13), (23)\}$.

$$(1)(12) = (12) = (12)(1),\ (12)(12) = (1),$$
$$(12)(13) = (132) \neq (123) = (13)(12),$$
$$(12)(23) = (123) \neq (132) = (23)(12),$$
$$(12)(123) = (23) \neq (13) = (123)(12),$$
$$(12)(132) = (13) \neq (23) = (132)(12).$$

Таким чином, $C(12) = \{(1), (12)\}$.

З наслідку 7.1 випливає, що у випадку скінченної групи G кількість різних елементів, спряжених з елементом $a \in G$, дорівнює $|G : C(a)|$. Зокрема кількість різних елементів, спряжених з a, є дільником порядку групи G.

Приклад 7.5. Нехай G – група порядку 36, $a \in G$ і $|a| = 6$. З'ясуємо, чи може кількість елементів, спряжених із a в групі G, дорівнювати 12.

Оскільки циклічна підгрупа $\langle a \rangle$ є абелевою, то централізатор $C(a)$ елемента a містить не менше $6 = |\langle a \rangle|$ елементів. Тоді для кількості k різних елементів, спряжених з a, маємо:

$$k = |G : C(a)| = \frac{|G|}{|C(a)|} \leqslant \frac{36}{6} = 6.$$

Таким чином, $k \neq 12$.

Зауважимо, що $C(a)$ – підгрупа групи G за твердженням 7.1.

Централізатором підмножини A групи G називається підгрупа

$$C(A) = \bigcap_{a \in A} C(a) = \{g \in G \mid \forall a \in A\ ga = ag\}.$$

Централізатор групи G називається *центром* групи G і позначається через $Z(G)$. Таким чином,

$$Z(G) = \{g \in G \mid \forall a \in G\ ga = ag\}.$$

Оскільки $gZ(G) = Z(G)g$ для кожного $g \in G$, то центр групи G є нормальною підгрупою групи G. Зрозуміло, що група G є абелевою тоді і лише тоді, коли $Z(G) = G$.

Приклад 7.6. Нехай група G містить єдиний елемент a порядку 2. Покажемо, що $a \in Z(G)$.

Дійсно, оскільки спряжені елементи мають однакові порядки, то елемент a спряжений тільки сам із собою. Це означає, що $gag^{-1} = a$ для всіх $g \in G$, тобто $ag = ga$ для будь-якого $g \in G$.

Група G називається *p-групою*, якщо $|G| = p^n$, де p – просте число, $n \in \mathbb{N}$.

Теорема 7.1.

Кожна p-група має неодиничний центр.

Доведення. Нехай $|G| = p^n$, де p – просте число, $n \in \mathbb{N}$. Розглянемо дію спряження групи G на G:

$$\circ : G \times G \to G, \quad \circ : (g, a) \mapsto gag^{-1}.$$

Відносно цієї дії група G розбивається на класи спряжених елементів, потужності яких є дільниками $|G| = p^n$. Якщо клас елемента a є одноточковим, тобто $\{g^{-1}ag : g \in G\} = \{a\}$, то $ga = ag$ для кожного $g \in G$, а отже, $a \in Z(G)$. Зрозуміло, що клас кожного елемента центра є одноточковим, а тому $Z(G)$ співпадає з об'єднанням одноточкових класів. Таким чином, отримуємо розбиття

$$G = Z(G) \sqcup K(g_1) \sqcup \ldots \sqcup K(g_s),$$

де $|K(g_i)| = p^{k_i}$ і $k_i \in \mathbb{N}$ для кожного $i \in \{1, \ldots, s\}$. Тоді

$$|G| = |Z(G)| + |K(g_1)| + \ldots + |K(g_s)|.$$

Таким чином,

$$|Z(G)| = p^n - (p^{k_1} + \ldots + p^{k_s}),$$

а отже, $|Z(G)|$ ділиться на p. □

Приклад 7.7. Знайдемо центр групи кватерніонів Q_8.

Оскільки $1x = x = x1$, $(-1)x = -x = x(-1)$ для кожного $x \in Q_8$ і

$$ij = 1 \neq -1 = ji,$$
$$(-i)k = j \neq -j = k(-i),$$
$$(-j)(-k) = i \neq -i = (-k)(-j),$$

то $Z(Q_8) = \{1, -1\}$.

Твердження 7.3.

Кожна група порядку p^2, де p – просте число, є абелевою.

Доведення. Оскільки центр $Z(G)$ групи G є неодиничним згідно з теоремою 7.1, то $|Z(G)| \in \{p, p^2\}$. Припустимо, що група G не абелева, тобто $|Z(G)| = p$. Оскільки $Z(G)$ є нормальною підгрупою групи G, то за теоремою Лагранжа порядок факторгрупи $|G/Z(G)| = p$. Отже, група $G/Z(G)$ є циклічною, породженою деяким елементом $aZ(G) \in G/Z(G)$, $a \in G$. Звідси випливає, що $gZ(G) = (aZ(G))^k = a^kZ(G)$ для кожного $g \in G$. Таким чином, кожен елемент $g \in G$ можна подати у вигляді $g = a^kz$, де $k \in \mathbb{Z}$, $z \in Z(G)$. Тоді для будь-яких елементів $g_1, g_2 \in G$, $g_1 = a^{k_1}z_1$, $g_2 = a^{k_2}z_2$ маємо:

$$g_1g_2 = (a^{k_1}z_1)(a^{k_2}z_2) = a^{k_1}a^{k_2}z_1z_2 = a^{k_2}a^{k_1}z_2z_1 = a^{k_2}z_2a^{k_1}z_1 = g_2g_1.$$

Отримана суперечність доводить твердження. □

Рекомендована література : [**2**, с. 79–88, 57–60], [**9**, с. 103–105], [**12**, с. 41–45, 49–53, 112–132], [**15**, с. 209–225].

Вправи до лекції 7.

7.1. Довести, що відображення $\circ : G \times G \to G$ є дією та описати орбіти і стабілізатори, якщо

а) $g \circ a = ga$, б) $g \circ a = ag^{-1}$.

7.2. Визначимо дію групи $(\mathbb{R}, +)$ на дійсній площині $\mathbb{R}^2$ як поворот точки $M \in \mathbb{R}^2$ на кут $\alpha \in \mathbb{R}$ навколо точки O проти годинникової стрілки. Описати геометрично орбіти та знайти стабілізатори цієї дії.

7.3. Знайти орбіти та стабілізатори природньої дії підгрупи $H = \langle (123), (34) \rangle$ групи S_5 на множині $\{1, 2, 3, 4, 5\}$.

7.4. Довести, що відображення, яке кожній парі $\alpha \in \mathbb{R}$, $\overrightarrow{v} \in E^2$ ставить вектор, отриманий з $\overrightarrow{v}$ поворотом на кут α, задає дію групи $(\mathbb{R}, +)$ на E^2 – множині векторів площини. Описати орбіти і стабілізатори.

7.5. Довести, що відображення, яке кожній парі $\alpha \in \mathbb{R}_+$, $\overrightarrow{v} \in E^2$ ставить вектор $\alpha\overrightarrow{v}$, задає дію групи $(\mathbb{R}_+, \cdot)$ на множині E^2. Описати орбіти і стабілізатори.

7.6. Знайти централізатор елемента $A = \begin{pmatrix} 3 & 0 \\ 0 & 5 \end{pmatrix}$ групи $GL(2, \mathbb{R})$.

7.7. Знайти всі класи спряжених елементів груп Q_8 та D_4.

7.8. Знайти нормалізатор та централізатор циклічної підгрупи $\langle i \rangle$ групи Q_8.

7.9. Знайти централізатор підгрупи $H = \{(1), (123), (132)\}$ в групі S_3.

7.10. Знайти нормалізатор підгрупи $H = \{(1), (123), (132)\}$ в групі A_4. Чи є підгрупа H нормальною?

7.11. Знайти $Z(G)$, якщо

а) $G = S_3$, б) $G = A_4$, в) $G = GL(n, \mathbb{R})$.

7.12. Знайти центр групи матриць наступного вигляду з операцією множення матриць:

$$A = \begin{pmatrix} 1 & 0 & 0 \\ a & 1 & 0 \\ b & c & 1 \end{pmatrix}, \text{ де } a, b, c \in \mathbb{Q}.$$

7.13. В групі $\mathbb{Z}$ з операцією $m * n = (-1)^n m + n$ знайти:

а) централізатор та клас спряжених елементів числа 2;
б) централізатор та нормалізатор підгрупи $4\mathbb{Z}$;
в) центр групи.

7.14. Довести, що кожна дія групи порядку 25 на 2024-елементній множині має принаймні чотири одноелементні орбіти.

7.15. Нехай G – група порядку 101, $g \in G$. Знайти $|C(g)|$.

7.16. Нехай g – елемент порядку n скінченної групи G. Довести, що $|C(g)|$ ділиться на n.

7.17. Нехай G – група порядку 21, $a \in G$, $|a| = 7$ і $a \notin Z(G)$. Знайти кількість елементів групи G, спряжених з елементом a.

7.18. Нехай H – нормальна підгрупа групи G порядку 2. Довести, що H міститься в центрі групи G.

7.19. Нехай x та y – елементи групи G, $xy = z \in Z(G)$. Показати, що елементи x та y комутують.

7.20. Довести, що $\psi(Z(G)) = Z(G)$ для кожного автоморфізму групи G.

7.21. Описати скінченні групи, які мають рівно два класи спряжених елементів.

7.22. Довести, що кожна нормальна підгрупа H групи G є об'єднанням деякої кількості класів спряжених елементів групи G.

7.23. Нехай K – клас спряжених елементів групи G. Довести, що для кожного натурального числа n множина $\{g^n \mid g \in K\}$ також буде класом спряжених елементів групи G.

7.24. Довести, що кожна підгрупа центру групи є нормальною.

7.25. Довести, що

а) якщо H і K – спряжені підгрупи скінченної групи G і $K \subset H$, то $K = H$;

б) підгрупи $H = \left\{ \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \;\middle|\; n \in \mathbb{Z} \right\}$ і $K = \left\{ \begin{pmatrix} 1 & 2n \\ 0 & 1 \end{pmatrix} \;\middle|\; n \in \mathbb{Z} \right\}$ – спряжені в групі $GL(2, \mathbb{R})$ і $K \subsetneq H$.

7.26. Довести, що в періодичній групі жодна підгрупа не може бути спряжена з своєю власною підгрупою.

7.27. Нехай група S_n діє на множині $X = \{1, \ldots, n\}$ за правилом $s \circ x = s(x)$ для кожних $s \in S_n$, $x \in X$. Показати, що відображення $s(i, j) = (s(i), s(j))$ визначає дію дію групи S_n на множині $X \times X$. Знайти орбіти цієї дії.

7.28. Нехай група S_3 діє на векторному просторі $\Omega = \mathbb{R}^3$:

$$\sigma \circ (x_1, x_2, x_3) = (\varphi(\sigma)x_{\sigma(1)}, \varphi(\sigma)x_{\sigma(2)}, \varphi(\sigma)x_{\sigma(3)}),$$

де $\varphi : S_3 \to \{\pm 1\}$, $\varphi(\sigma) = \begin{cases} 1, & \text{якщо } \sigma \text{ є парною підстановкою,} \\ -1, & \text{якщо } \sigma \text{ є непарною підстановкою.} \end{cases}$

Розглянемо декілька прикладів цієї групової дії: якщо $\sigma = (13)$, то $\sigma \circ (1, 4, -2) = (2, -4, -1)$, а якщо $\tau = (123)$, то $\tau \circ (3, 0, 2) = (0, 2, 3)$.

а) Нехай $x = (1, 4, 0) \in \mathbb{R}^3$. Знайти стабілізатор вектора x відносно цієї дії групи S_3 на $\mathbb{R}^3$. Скільки векторів містить орбіта вектора x?

б) Знайдіть те саме для векторів $x = (1, 1, -1)$ та $x = (0, 0, 0)$.

в) Якими можуть бути потужності орбіт для цієї дії групи S_3 на $\mathbb{R}^3$?

г) Які підгрупи групи S_3 можуть бути стабілізаторами $St(x)$ вектора $x \in \mathbb{R}^3$?

7.29. Нехай $\circ : G \times X \to X$ – дія групи G на множині X і $Y \subset X$. Показати, що множина $G_Y = \{g \in G \mid g \circ Y = Y\}$ є підгрупою групи G. Довести, що $G_{X \setminus Y} = G_Y$.

7.30. Нехай $\circ : G \times X \to X$ – дія групи G на множині X. Підмножина $Y \subset X$ називається *G-інваріантною*, якщо $g \circ y \in Y$ для кожних $g \in G$, $y \in Y$. Довести, що підмножина $Y \subset X$ є G-інваріантною тоді і лише тоді, коли Y є об'єднанням G-орбіт.

7.31. *Ядром* дії $\circ : G \times X \to X$ називається множина $\{g \in G \mid \forall x \in X\ g \circ x = x\}$. Довести, що ядро дії є підгрупою групи G.

7.32. Нехай $\circ : G \times X \to X$ – дія групи G на множині X. Довести, що відображення

$$\varphi : G \to S_X, \quad \varphi : g \mapsto l_g, \quad l_g(x) = g \circ x,$$

є гомоморфізмом. Знайти його ядро.

7.33. Нехай G – група і $X = \{\alpha \mid \alpha : G \to \mathbb{R}\}$. Довести, що відображення

$$\circ : G \times X \to X, \quad (g \circ \alpha)(x) = \alpha(gx)$$

є дією. Чи є дана дія вільною?

7.34. Нехай H – підгрупа групи G і $(G : H)$ – множина лівих суміжних класів розбиття групи G за підгрупою H Довести, що відображення

$$\circ : G \times (G : H) \to (G : H), \quad g \circ (xH) = (gx)H$$

є транзитивною дією. Знайти ядро цієї дії.

7.35. Нехай $\circ : G \times X \to X$ – дія групи G на множині X. Довести, що $St(g \circ x) = gSt(x)g^{-1}$ для кожних $g \in G$, $x \in X$.

7.36. Довести, що якщо факторгрупа $G/Z(G)$ є циклічною, то група G є абелевою.

7.37. Довести, що якщо G неабелева і $|G| = p^3$, то $|Z(G)| = p$ (p — просте число).

7.38. Знайти кількість класів спряжених елементів і кількість елементів у кожному класі для неабелевої групи порядку p^3 (p — просте число).

7.39. З точністю до ізоморфізму описати всі групи порядку 4.

Лекція 8. Комутант групи. Розв'язні групи

В абелевій групі кожні два елементи переставні між собою. Якщо група неабелева, то в ній існують непереставні елементи, тобто такі елементи a і b, що $ab \neq ba$. Тому природньо розглянути елемент x, для якого $ab = bax$, тобто $x = a^{-1}b^{-1}ab$.

Комутатором елементів a і b називають елемент $a^{-1}b^{-1}ab$, який позначають $[a, b]$. Зрозуміло, що $ab = ba[a, b]$. Таким чином, елементи a і b є переставними тоді і лише тоді, коли $[a, b] = e$ – одиниця групи.

Множина G', яка складається з всеможливих скінченних добутків комутаторів елементів групи G, називається *комутантом* або *похідною* групи G.

Зрозуміло, що група G є абелевою тоді і лише тоді, коли $G' = \{e\}$.

Теорема 8.1.

Комутант G' є нормальною підгрупою групи G.

Доведення. Зрозуміло, що $e \in G'$ і добуток двох елементів з G' належить G'.

Оскільки

$$[a,b]^{-1} = (a^{-1}b^{-1}ab)^{-1} = b^{-1}a^{-1}ba = [b,a] \in G',$$

і кожен елемент $u \in G'$ є добутком $u = u_1 \cdot \ldots \cdot u_m$ скінченної кількості комутаторів u_i, то

$$u^{-1} = (u_1 \cdot \ldots \cdot u_m)^{-1} = u_m^{-1} \cdot \ldots \cdot u_1^{-1} \in G'.$$

Таким чином, G' – підгрупа групи G.

Для кожного $g \in G$ маємо

$$g[a,b]g^{-1} = ga^{-1}b^{-1}abg^{-1} = ga^{-1}g^{-1}gb^{-1}g^{-1}gag^{-1}gbg^{-1} =$$
$$= (gag^{-1})^{-1}(gbg^{-1})^{-1}gag^{-1}gbg^{-1} = [gag^{-1}, gbg^{-1}] \in G'.$$

Тоді для кожного елемента $u \in G'$, який є добутком $u = u_1 \cdot \ldots \cdot u_m$ скінченної кількості комутаторів u_i, отримуємо

$$gug^{-1} = gu_1u_2 \cdot \ldots \cdot u_mg^{-1} = (gu_1g^{-1})(gu_2g^{-1}) \cdot \ldots \cdot (gu_mg^{-1}) \in G'.$$

Таким чином, $G' \lhd G$. □

Твердження 8.1.

Кожна підгрупа H групи G, яка містить комутант G' групи G, є нормальною в групі G.

Доведення. Нехай $H \supset G'$ і $h \in H$, $g \in G$. Тоді

$$g^{-1}hg = (hh^{-1})(g^{-1}hg) = h(h^{-1}g^{-1}hg) = h[h,g] \in H.$$

Оскільки підгрупа H разом з кожним своїм елементом містить всі спряжені до нього в групі G, то H – нормальна підгрупа групи G. □

Твердження 8.2.

Факторгрупа G/G' – абелева.

Доведення. Нехай $\overline{a}, \overline{b} \in G/G'$. Тоді

$$[\overline{a}, \overline{b}] = [aG', bG'] = (aG')^{-1}(bG')^{-1}(aG')(bG') =$$
$$= G'a^{-1}G'b^{-1}aG'bG' = a^{-1}b^{-1}abG' = [a, b]G' = G' = \overline{e}.$$

Оскільки комутатор довільних двох елементів групи G/G' дорівнює одиниці $\overline{e}$, то G/G' – абелева група. □

Оскільки комутант G' групи G є її підгрупою, то в ній можна теж розглянути комутант $(G')'$ і т.д.

Таким чином, вважаючи $G^{(0)} = G$, для кожного $k \in \mathbb{N}$ визначимо k-ту похідну групи G за правилом:

$$G^{(k)} = (G^{(k-1)})'.$$

Зауважимо, що $G^{(k)} \lhd G^{(k-1)}$ і $G^{(k-1)}/G^{(k)}$ – абелева група для кожного $k \in \mathbb{N}$.

Група G називається *розв'язною*, якщо $G^{(n)} = \{e\}$ для деякого $n \in \mathbb{N} \cup \{0\}$. Найменше число n з такою властивістю називається *ступенем розв'язності* групи G. Очевидно, що ступінь розв'язності групи G дорівнює 1 тоді і лише тоді, коли група G є абелевою.

Приклад 8.1. У групі $\mathbb{Z}$ з операцією $m * n = (-1)^n m + n$ знайдемо комутатори всіх елементів, комутант групи та з'ясуємо, чи є дана група розв'язною.

Одиницею групи $\mathbb{Z}$ є число 0, обернений до елемента $n \in \mathbb{Z}$ дорівнює $(-1)^{n-1}n$.

Нехай $m, n \in \mathbb{Z}$. Знайдемо комутатор $[m, n]$ елементів m і n (в обчисленнях будемо враховувати, що $(-1)^{-a} = (-1)^a$):

$$[m, n] = m^{-1} * n^{-1} * m * n = ((-1)^{m-1}m) * ((-1)^{n-1}n) * m * n =$$
$$= ((-1)^{(-1)^{n-1}n}(-1)^{m-1}m + (-1)^{n-1}n) * ((-1)^n m + n)) =$$
$$= ((-1)^{n+m-1}m + (-1)^{n-1}n) * ((-1)^n m + n) =$$
$$= (-1)^{(-1)^n m+n}((-1)^{n+m-1}m + (-1)^{n-1}n) + (-1)^n m + n =$$
$$= -m + (-1)^{m-1}n + (-1)^n m + n = ((-1)^n - 1)m + ((-1)^{m-1} + 1)n.$$

Проаналізуємо комутатор

$$[m, n] = ((-1)^n - 1)m + ((-1)^{m-1} + 1)n$$

в залежності від парності чисел m і n:

- якщо $m = 2k$, $n = 2s$, де $k, s \in \mathbb{Z}$, то $[m, n] = 0$;
- якщо $m = 2k$, $n = 2s + 1$, де $k, s \in \mathbb{Z}$, то $[m, n] = -4k$;

- якщо $m = 2k+1$, $n = 2s$, де $k, s \in \mathbb{Z}$, то $[m, n] = 4s$;
- якщо $m = 2k+1$, $n = 2s+1$, де $k, s \in \mathbb{Z}$, то $[m, n] = -2(2k+1) + 2(2s+1) = 4(s-k)$.

З отриманих рівностей для комутаторів випливає, що комутант групи $\mathbb{Z}$ співпадає з підгрупою цілих чисел, кратних 4, тобто $\mathbb{Z}' = 4\mathbb{Z}$.

Оскільки $2\mathbb{Z} \supset 4\mathbb{Z} = \mathbb{Z}'$, то з твердження 8.1 випливає, що $2\mathbb{Z} \lhd \mathbb{Z}$. Крім того, комутатор довільних двох елементів групи $2\mathbb{Z}$ дорівнює 0, а тому $2\mathbb{Z}$ – абелева підгрупа групи $\mathbb{Z}$.

У прикладі 5.6 показано, що факторгрупа $\mathbb{Z}/\mathbb{Z}' = \mathbb{Z}/4\mathbb{Z}$ є ізоморфною групі Клейна V_4, а тому є абелевою групою порядку 4.

Оскільки $[m, n] = 0$ для парних m і n, то група $4\mathbb{Z}$ є абелевою і $(4\mathbb{Z})' = \{0\}$.

Таким чином, $\mathbb{Z}'' = (\mathbb{Z}')' = (4\mathbb{Z})' = \{0\}$, а тому $(\mathbb{Z}, *)$ – розв'язна група ступеня 2.

Ланцюжок підгруп

$$G = H_0 > H_1 > \ldots > H_{n-1} > H_n = \{e\}.$$

називається *рядом* довжини n групи G.

Ряд називається *нормальним*, якщо $H_i \lhd G$, і *субнормальним*, якщо $H_i \lhd H_{i-1}$ для кожного $i \in \{1, \ldots, n\}$. Факторгрупи H_{i-1}/H_i називаються *факторами* ряду.

Лема 8.1.

Якщо $H \lhd G$ і G/H – абелева група, то $H \supset G'$.

Доведення. Досить довести, що $[a, b] \in H$ для кожних $a, b \in G$. Оскільки факторгрупа G/H – абелева, то комутатор довільних її елементів одиничний, тобто $[aH, bH] = H$. Але тоді з рівності $[aH, bH] = [a, b]H$ випливає, що $[a, b]H = H$, тобто $[a, b] \in HH^{-1} = H$. □

Характеризаційна теорема 8.1.

Група G є розв'язною тоді і лише тоді, коли вона володіє субнормальним рядом з абелевими факторами.

Доведення. Нехай G – розв'язна група. Тоді $G^{(n)} = \{e\}$ для деякого $n \in \mathbb{N}$. З доведеного вище випливає, що ряд

$$G \rhd G' \rhd \ldots \rhd G^{(n-1)} \rhd G^{(n)} = \{e\}$$

є субнормальним рядом з абелевими факторами.

Навпаки, нехай група G володіє субнормальним рядом з абелевими факторами:

$$G = H_0 \rhd H_1 \rhd \ldots \rhd H_{n-1} \rhd H_n = \{e\}.$$

Скористаємось методом математичної індукції. Оскільки $H_1 \lhd H_0 = G$ і $G/H_1 = H_0/H_1$ – абелева група, то $H_1 \supset G'$ за лемою 8.1.

Нехай $H_{k-1} \supset G^{(k-1)}$. Доведемо, що $H_k \supset G^{(k)}$. Оскільки $H_k \lhd H_{k-1}$ і H_{k-1}/H_k – абелева, то $H_k \supset H'_{k-1}$ за лемою 8.1. З включення $H_{k-1} \supset G^{(k-1)}$ випливає, що $H'_{k-1} \supset G^{(k)}$. Звідки $H_k \supset G^{(k)}$.

Таким чином, $\{e\} = H_n \supset G^{(n)}$, і G – розв'язна група. □

Приклад 8.2. Покажемо, що група S_3 є розв'язною. Циклічна підгрупа $H_1 = \langle(123)\rangle = \{(1), (123), (132)\}$ має індекс 2 в групі S_3, а тому $H_1 \lhd S_3$. Порядок факторгрупи S_3/H_1 дорівнює 2, а тому $S_3/H_1 = \{H_1, S_3 \backslash H_1\} = \{\overline{(1)}, \overline{(12)}\}$ – абелева група.

Покладемо $H_2 = \{(1)\}$. Тоді $H_2 \lhd H_1$ і $H_1/H_2 \cong H_1$ – циклічна, а отже, абелева. Таким чином, ми побудували субнормальний ряд з абелевими факторами:

$$S_3 = H_0 \rhd H_1 \rhd H_2 = \{(1)\}.$$

Оскільки група S_3 не є абелевою, то за характеризаційною теоремою 8.1 група S_3 є розв'язною ступеня 2.

Лема 8.2.

Нехай $H \lhd G$. Елемент g групи G можна подати у вигляді $g = xh$, де $x \in G^{(k)}$, $h \in H$, тоді і лише тоді, коли $[g] = gH \in (G/H)^{(k)}$, тобто для кожного $k \in \mathbb{N} \cup \{0\}$ має місце рівність

$$G^{(k)}H/H = (G/H)^{(k)}.$$

Доведення. Дійсно, вважаючи $G^{(0)} = G$, бачимо, що для $k = 0$ лема вірна.

Припустимо, що лема вірна для $k-1$. Доведемо для k. Якщо u – комутатор в групі $G^{(k-1)}$, то $u = a^{-1}b^{-1}ab$ для деяких $a, b \in G^{(k-1)}$. Тоді $[u] = [a]^{-1}[b]^{-1}[a][b]$. З індуктивного припущення випливає, що $[a], [b] \in (G/H)^{(k-1)}$, тобто $[u]$ – комутатор в групі $(G/H)^{(k-1)}$.

Нехай $g = xh$, де $x \in G^{(k)}$, $h \in H$. Тоді $g = u_1 \cdot \ldots \cdot u_m h$, де u_i – комутатори в групі $G^{(k-1)}$. З доведеного випливає, що $[u_i]$ – комутатори в групі $(G/H)^{(k-1)}$, а тому

$$[g] = [u_1] \cdot \ldots \cdot [u_m] \in ((G/H)^{(k-1)})' = (G/H)^{(k)}.$$

Нехай $[g] \in (G/H)^{(k)}$. Тоді $[g] = [u_1]\cdot\ldots\cdot[u_m]$, де $[u_i] = [a_i]^{-1}[b_i]^{-1}[a_i][b_i]$ для деяких $[a_i], [b_i] \in (G/H)^{(k-1)}$. За індуктивним припущенням $a_i = c_i h_i$ і $b_i = d_i s_i$ для деяких $c_i, d_i \in G^{(k-1)}$, $h_i, s_i \in H$. Зауважимо, що $v_i = c_i^{-1}d_i^{-1}c_i d_i \in G^{(k)}$. З другого боку, для деякого $z \in H$ маємо

$$u_i = (c_i h_i)^{-1}(d_i s_i)^{-1}(c_i h_i)(d_i s_i)z = h_i^{-1}c_i^{-1}s_i^{-1}d_i^{-1}c_i h_i d_i s_i z.$$

Тоді

$$[u_i] = [c_i^{-1}][d_i^{-1}][c_i][d_i] = [v_i], \quad i \in \{1, \ldots, m\},$$

а отже,

$$[g] = [u_1]\cdot\ldots\cdot[u_m] = [v_1]\cdot\ldots\cdot[v_m] = [v_1\cdot\ldots\cdot v_m].$$

Таким чином, $g = v_1\cdot\ldots\cdot v_m h$ для деякого $h \in H$, а тому $v_1\cdot\ldots\cdot v_m \in G^{(k)}$. □

Теорема 8.2.

Нехай $H \lhd G$. Група G є розв'язною тоді і лише тоді, коли розв'язними є група H і факторгрупа G/H.

Доведення. Нехай G – розв'язна група. Тоді $G^{(n)} = \{e\}$ для деякого $n \in \mathbb{N}$. Оскільки $H^{(i)} \subset G^{(i)}$ для кожного $i \in \mathbb{N}$, то $H^{(n)} = \{e\}$, і підгрупа H – розв'язна.

Якщо $[g] \in (G/H)^{(n)}$, то за лемою 8.2 має місце рівність $g = xh$, де $x \in G^{(n)} = \{e\}$, $h \in H$. Тоді $g = h \in H$ і $[g] = [e]$. Таким чином, $(G/H)^{(n)} = \{[e]\}$, а тому G/H – розв'язна група.

Навпаки, нехай група H і факторгрупа G/H є розв'язними. Тоді $(G/H)^{(k)} = \{[e]\}$ і $H^{(t)} = \{e\}$ для деяких $k, t \in \mathbb{N}$. Якщо $x \in G^{(k)}$, то $[x] \in (G/H)^{(k)} = \{[e]\}$ за лемою 8.2, тобто $x \in H$. Отже, $G^{(k)} \subset H$, звідки

$$G^{(k+t)} = (G^{(k)})^{(t)} \subset H^{(t)} = \{e\}.$$

Таким чином, G – розв'язна група. □

Теорема 8.3.

Кожна p-група є розв'язною.

Доведення. Нехай $|G| = p^n$, де p – просте число, $n \in \mathbb{N}$. За теоремою 7.1 кожна p-група має неодиничний центр. Тоді за теоремою Лагранжа $|G|$ ділиться на $|Z(G)|$, тобто $|Z(G)| \geqslant p$.

Доведемо твердження індукцією за n. Група G порядку p – абелева, а тому є розв'язною.

Припустимо, що всі p-групи порядків менше $|G|$ є розв'язними. Доведемо розв'язність групи G. Оскільки $Z(G) \lhd G$, то факторгрупа $G/Z(G)$ існує. Якщо $Z(G) = G$, то G – абелева група, а тому є розв'язною. Якщо $Z(G) \neq G$, то $|Z(G)| < |G|$ і $|G/Z(G)| < |G|$, а тому за індуктивним припущення групи $Z(G)$ і $G/Z(G)$ є розв'язними. Але тоді за теоремою 8.2 група G – розв'язна. □

Приклад 8.3. Кожна група порядку 1375, яка містить єдину підгрупу порядку 125, є розв'язною. Дійсно, нехай H – підгрупа порядку 125. Тоді $g^{-1}Hg$ також є підгрупою порядку 125 для кожного $g \in G$. З єдиності H випливає, що $g^{-1}Hg = H$ для кожного $g \in G$, а тому H – нормальна в G. За теоремою Лагранжа факторгрупа G/H має порядок 11 і є циклічною, а отже, абелевою. Оскільки $|H| = 5^3$, то за теоремою 8.3 група H є розв'язною.

Таким чином, за теоремою 8.2 група G – розв'язна.

Рекомендована література : [**2**, с. 74–76, 114–117], [**9**, с. 105–106], [**11**, с. 31–34], [**15**, с. 201–207].

Вправи до лекції 8.

8.1. У групі S_3 знайти наступні комутатори:

а) $[(12),(13)]$, б) $[(123),(23)]$, в) $[(123),(132)]$.

8.2. У групі $GL(2,\mathbb{R})$ знайти комутатор матриць

$$A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad \text{і} \quad B = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}.$$

8.3. Довести, що для довільних елементів a, b і c групи G мають місце рівності:

а) $[a,bc] = [a,c](c^{-1}[a,b]c)$; б) $[ab,c] = (b^{-1}[a,c]b)[b,c]$.

8.4. З'ясувати, які з наступних рівностей виконуються для кожних елементів a, b і c групи S_3:

а) $[[a,b],c] = (1)$; б) $[a^2,b^2] = (1)$.

8.5. Нехай a і b – елементи групи G, $a^2 = e$. Довести, що $[[a,b],a] = [b,a]^2$.

8.6. Нехай комутатор $[a,b]$ елементів a і b групи G комутує з a. Довести, що $[a,b]^n = [a^n,b]$ для кожного $n \in \mathbb{Z}$.

8.7. Довести, що елементи a^2 і b комутують тоді і лише тоді, коли

$$[a,b][[a,b],a][a,b] = e.$$

8.8. Знайти комутант групи Q_8. Показати, що група Q_8 є розв'язною та знайти її ступінь розв'язності.

8.9. Довести, що A_4 і S_4 – розв'язні групи.

8.10. Показати, що комутатор довільних двох підстановок групи S_n є парною підстановкою. Знайти комутатор двох транспозицій.

8.11. Довести, що $S_n' = A_n$.

8.12. Довести, що проста група є розв'язною тоді і лише тоді, коли вона є циклічною групою.

8.13. Довести, що групи A_n і S_n при $n \geqslant 5$ не є розв'язними.

8.14. Знайти похідну групи D_n.

8.15. Показати, що діедральні групи є розв'язними ступеня 2.

8.16. Довести, що кожна група порядку 1323, яка містить нормальну підгрупу порядку 27, є розв'язною.

8.17. Довести, що кожна група порядку 216, яка містить єдину підгрупу порядку 8, є розв'язною.

8.18. Відомо, що в групі G порядку 1225 кількість підгруп, спряжених з підгрупою H порядку 49, не перевищує 4. Довести, що G – розв'язна група.

8.19. Описати комутант групи $\mathrm{Aff}(\mathbb{R})$. Чи є група $\mathrm{Aff}(\mathbb{R})$ розв'язною?

8.20. Навести приклад субнормального ряду, який не є нормальним.

8.21. Побудувати ряд найбільшої довжини циклічної групи C_{24}.

8.22. Довести, що група є розв'язною тоді і лише тоді, коли вона володіє нормальним рядом з абелевими факторами.

8.23. Нехай H і K – нормальні підгрупи групи G. Довести, що $[h,k] \in H \cap K$ для кожних $h \in H$, $k \in K$.

8.24. Нехай H і K – нормальні підгрупи групи G, $H \cap K = \{e\}$. Довести, що $hk = kh$ для кожних $h \in H$, $k \in K$.

8.25. Нехай елементи a і b групи G переставні зі своїм комутатором. Довести, що

$$(ab)^n = a^n b^n [b,a]^{\frac{(n-1)n}{2}} \text{ для кожного } n \in \mathbb{N}.$$

8.26. Нехай $\varphi : G \to H$ – епіморфізм груп G і H. Довести, що $\varphi(G') = H'$.

8.27. Нехай $\varphi : G \to H$ – епіморфізм груп G і H. Довести, що якщо G є розв'язною, то H також є розв'язною.

8.28. Нехай G – скінченна група, $|G'| = 2$. Довести, що $G' \subset Z(G)$.

8.29. Довести, що комутант G' неодиничної скінченної p–групи G завжди відмінний від групи G.

8.30. Нехай G – неабелева група порядку p^3, де p – просте число. Довести, що $G' = Z(G)$.

Лекція 9. Прямі добутки груп

Нехай задано n груп: $(G_1, *_1), (G_2, *_2), \ldots, (G_n, *_n)$. На декартовому добутку $G_1 \times G_2 \times \ldots \times G_n$ задамо операцію $\circ$ наступним чином:

$$(a_1, a_2, \ldots, a_n) \circ (b_1, b_2, \ldots b_n) = (a_1 *_1 b_1, a_2 *_2 b_2, \ldots, a_n *_n b_n).$$

Теорема 9.1.

Декартів добуток $G_1 \times G_2 \times \ldots \times G_n$ з операцією $\circ$ є групою.

Доведення. Нехай $(a_1, \ldots, a_n), (b_1, \ldots, b_n), (c_1, \ldots, c_n) \in G_1 \times \ldots \times G_n$. Тоді

$$(a_1, \ldots, a_n) \circ ((b_1, \ldots, b_n) \circ (c_1, \ldots, c_n)) = (a_1, \ldots, a_n) \circ (b_1 *_1 c_1, \ldots, b_n *_n c_n) =$$
$$= (a_1 *_1 (b_1 *_1 c_1), \ldots, a_n *_n (b_n *_n c_n)) = ((a_1 *_1 b_1) *_1 c_1, \ldots, (a_n *_n b_n) *_n c_n) =$$
$$= (a_1 *_1 b_1, \ldots, a_n *_n b_n) \circ (c_1, \ldots, c_n) = ((a_1, \ldots, a_n) \circ (b_1, \ldots, b_n)) \circ (c_1, \ldots, c_n)$$

Нехай e_i – одиниця групи G_i, де $i \in \{1, \ldots, n\}$.

Тоді для кожного $(a_1, \ldots, a_n) \in G_1 \times \ldots \times G_n$ маємо:

$$(e_1, \ldots, e_n) \circ (a_1, \ldots, a_n) = (e_1 *_1 a_1, \ldots, e_n *_n a_n) = (a_1, \ldots, a_n).$$

Отже, $(e_1, \ldots, e_n)$ – ліва одиниця напівгрупи $G_1 \times \ldots \times G_n$.

Для кожного елемента $(a_1, \ldots, a_n) \in G_1 \times \ldots \times G_n$ мають місце рівності:

$$(a_1^{-1}, \ldots, a_n^{-1}) \circ (a_1, \ldots, a_n) = (a_1^{-1} *_1 a_1, \ldots, a_n^{-1} *_n a_n) = (e_1, \ldots, e_n).$$

Таким чином, $(a_1^{-1}, \ldots, a_n^{-1})$ – лівий обернений елемент до елемента $(a_1, \ldots, a_n)$, а тому $(G_1 \times \ldots \times G_n, \circ)$ – група. □

Група $G_1 \times G_2 \times \ldots \times G_n$ з операцією покомпонентного множення $\circ$ називається *зовнішнім прямим добутком* груп $G_1, G_2, \ldots, G_n$.

Приклад 9.1. Утворимо зовнішній прямий добуток групи $\mathbb{Q}_+$ додатніх раціональних чисел і циклічної групи $C_2 = \{1, -1\}$. Елементами групи $\mathbb{Q}_+ \times C_2$ є всі пари чисел виду $(r, 1)$ і $(r, -1)$, де r – додатнє раціональне число. Очевидно, що відображення

$$\psi : \ \mathbb{Q}_+ \times C_2 \to \mathbb{Q}\backslash\{0\}, \quad \psi : (r, 1) \mapsto r, \ \psi : (r, -1) \mapsto -r$$

є ізоморфізмом групи $\mathbb{Q}_+ \times C_2$ і групи ненульових раціональних чисел з операцією множення.

Твердження 9.1.

Нехай $G_1 \times \ldots \times G_n$ – зовнішній прямий добуток груп $G_1, \ldots, G_n$, $G_i^\star = \{(e_1, \ldots, e_{i-1}, g, e_{i+1}, \ldots, e_n) \mid g \in G_i\}$, де $i \in \{1, \ldots, n\}$. Тоді:

1) *$G_i^\star$ є нормальною підгрупою групи $G_1 \times \ldots \times G_n$, ізоморфною групі G_i, де $i \in \{1, \ldots, n\}$;*
2) *$G_i^\star \cap (\prod_{j \neq i} G_j^\star) = \{(e_1, \ldots, e_n)\}$ для кожного $i \in \{1, \ldots, n\}$;*
3) *$G_1^\star \circ \ldots \circ G_n^\star = G_1 \times \ldots \times G_n$.*

Доведення. 1) Оскільки

$$(e_1, \ldots, g, \ldots, e_n) \circ (e_1, \ldots, g', \ldots, e_n) = (e_1, \ldots, g *_i g', \ldots, e_n) \in G_i^\star$$

і

$$(e_1, \ldots, g, \ldots, e_n)^{-1} = (e_1, \ldots, g^{-1}, \ldots, e_n) \in G_i^\star$$

для кожних

$$(e_1, \ldots, g, \ldots, e_n), (e_1, \ldots, g', \ldots, e_n) \in G_i^\star,$$

то $G_i^\star$ – підгрупа групи $G_1 \times \ldots \times G_n$.

Для кожних $(a_1, \ldots, a_i, \ldots a_n) \in G_1 \times \ldots \times G_n$, $(e_1, \ldots, g, \ldots, e_n) \in G_i^\star$ маємо:

$$\begin{gathered}(a_1^{-1}, \ldots, a_i^{-1}, \ldots, a_n^{-1}) \circ (e_1, \ldots, g, \ldots, e_n) \circ (a_1, \ldots, a_i, \ldots, a_n) = \\ = (a_1^{-1} *_1 e_1 *_1 a_1, \ldots, a_i^{-1} *_i g *_i a_i, \ldots, a_n^{-1} *_n e_n *_n a_n) = \\ = (e_1, \ldots, a_i^{-1} *_i g *_i a_i, \ldots, e_n) \in G_i^\star.\end{gathered}$$

Таким чином, $G_i^\star \lhd G_1 \times \ldots \times G_n$.

Легко перевірити, що для кожного $i \in \{1, \ldots, n\}$ відображення $\psi_i : G_i \to G_i^\star$, $\psi(g) = (e_1, \ldots, e_{i-1}, g, e_{i+1}, \ldots, e_n)$, є ізоморфізмом.

Пункт 2) є очевидним.

3) Кожен елемент $(a_1, a_2, \ldots, a_n) \in G_1 \times G_2 \times \ldots \times G_n$ можна подати у вигляді

$$(a_1, a_2, \ldots, a_n) = (a_1, e_2, \ldots, e_n) \circ (e_1, a_2, \ldots, e_n) \circ \ldots \circ (e_1, e_2, \ldots, a_n).$$

Отже, $(a_1, a_2, \ldots, a_n) \in G_1^\star \circ G_2^\star \circ \ldots \circ G_n^\star$, а тому

$$G_1^\star \circ G_2^\star \circ \ldots \circ G_n^\star = G_1 \times G_2 \times \ldots \times G_n.$$

□

Поширимо поняття добутку груп на випадок довільної (зокрема, нескінченної) кількості груп. Для цього спершу пригадаємо, як вводиться декартів добуток довільної сім'ї множин.

Нехай $X_1, X_2, \ldots, X_n$ – довільні множини. Добуток $X_1 \times X_2 \times \ldots \times X_n$ складається з наборів $(x_1, x_2, \ldots, x_n)$, індексованих числами $1, 2, \ldots, n$. Кожен такий набір можна вважати функцією, яка індексу 1 зіставляє значення x_1, індексу 2 – значення $x_2, \ldots$, індексу n – значення x_n. Нагадаємо, що послідовність $x = (x_1, x_2, \ldots)$ елементів множини X ми вважаємо відображенням $x : \mathbb{N} \to X$, а члени $x_1, x_2, \ldots$ – значеннями $x(1), x(2)$, і т.д. Взагалі, довільний набір елементів x_α з множини X, індексований елементами α з деякої індексної множини $\mathcal{A}$, можна вважати функцією $x : \mathcal{A} \to X$. Таким чином, приходимо до наступного означення.

(*Декартів*) *добуток* $\prod_{\alpha\in\mathcal{A}} X_\alpha$ сім'ї множин $X_\alpha, \alpha \in \mathcal{A}$, – це множина всіх таких функцій $x : \mathcal{A} \to \bigcup_{\alpha\in\mathcal{A}} X_\alpha$, що $x(\alpha) \in X_\alpha$ для кожного $\alpha \in \mathcal{A}$.

Замість $x(\alpha)$ пишемо x_α, а всю функцію (елемент добутку) записуємо $x = (x_\alpha)_{\alpha\in\mathcal{A}}$, уявляючи набором *координат* – елементів x_α з індексами $\alpha \in \mathcal{A}$.

Нехай $\{(G_\alpha, *_\alpha) \mid \alpha \in \mathcal{A}\}$ – сім'я груп. Введемо на добутку $\prod_{\alpha\in\mathcal{A}} G_\alpha$ операцію $\circ$ наступним чином

$$((x_\alpha)_{\alpha\in\mathcal{A}}) \circ ((y_\alpha)_{\alpha\in\mathcal{A}}) = (x_\alpha *_\alpha y_\alpha)_{\alpha\in\mathcal{A}}.$$

Легко перевірити, що множина $\prod_{\alpha\in\mathcal{A}} G_\alpha$ з операцією $\circ$ є групою з одиницею $(e_\alpha)_{\alpha\in\mathcal{A}}$, де e_α – одиниця групи G_α.

Група $\prod_{\alpha\in\mathcal{A}} G_\alpha$ з операцією покомпонентного множення $\circ$ називається *прямим добутком* сім'ї груп $\{G_\alpha \mid \alpha \in \mathcal{A}\}$.

Якщо всі групи $G_\alpha, \alpha \in \mathcal{A}$, рівні деякій групі G, то прямий добуток називається *степенем групи* G і позначається $G^{\mathcal{A}}$. Якщо потужність множини індексів $\mathcal{A}$ рівна τ, а склад $\mathcal{A}$ несуттєвий, то для $G^{\mathcal{A}}$ вживають позначення G^τ. Зрозуміло, що при $\mathcal{A} = \{1, 2, \ldots, n\}$ отримуємо *n-й степінь* G^n з елементами $(g_1, g_2, \ldots, g_n)$, де $g_i \in G$. Степінь $G^{\mathbb{N}}$ звичайно позначають через G^ω і називають *зліченним степенем групи* G. Елементи G^ω – це послідовності вигляду $(g_1, g_2, \ldots)$ з членами з групи G.

Приклад 9.2. Покажемо, що група $\mathcal{P}(\mathbb{N})$ всіх підмножин множини $\mathbb{N}$ з операцією симетричної різниці множин є ізоморфною зліченному степеню циклічної групи $C_2 = \{1, -1\}$.

Розглянемо відображення

$$\psi : \mathcal{P}(\mathbb{N}) \to (C_2)^\omega, \quad \psi(A) = (a_1, a_2, \ldots, a_k, \ldots), \text{ де } a_i = \begin{cases} 1, i \notin A \\ -1, i \in A \end{cases}$$

Покажемо, що відображення ψ – ізоморфізм. Нехай

$$\psi(A) = (a_1, a_2, \ldots, a_k, \ldots), \quad \psi(B) = (b_1, b_2, \ldots, b_k, \ldots),$$
$$\psi(A \triangle B) = (c_1, c_2, \ldots, c_k, \ldots),$$
$$\text{де } A \triangle B = (A \cup B)\backslash(A \cap B) = (A\backslash B) \cup (B\backslash A).$$

Оскільки $a_i, b_i \in \{-1, 1\}$ для кожного $i \in \mathbb{N}$, то можливі наступні чотири випадки:

а) якщо $(a_i, b_i) = (1, 1)$, то $i \notin A \cup B$, звідки $i \notin A \triangle B$ і $c_i = 1$;
б) якщо $(a_i, b_i) = (-1, -1)$, то $i \in A \cap B$, звідки $i \notin A \triangle B$ і $c_i = 1$;
в) якщо $(a_i, b_i) = (1, -1)$, то $i \in B\backslash A$, звідки $i \in A \triangle B$ і $c_i = -1$;
г) якщо $(a_i, b_i) = (-1, 1)$, то $i \in A\backslash B$, звідки $i \in A \triangle B$ і $c_i = -1$.

У всіх випадках бачимо, що $c_i = a_i b_i$. Звідси слідує, що

$$\psi(A \triangle B) = (c_1, c_2, \ldots, c_k, \ldots) = (a_1 b_1, a_2 b_2, \ldots, a_k b_k, \ldots) =$$
$$= (a_1, a_2, \ldots, a_k, \ldots) \circ (b_1, b_2, \ldots, b_k, \ldots) = \psi(A) \circ \psi(B).$$

Отже, ψ – ізоморфізм.

Якщо $\psi(A) = \psi(B)$, то $(a_1, a_2, \ldots, a_k, \ldots) = (b_1, b_2, \ldots, b_k, \ldots)$. Тоді $a_i = b_i$ для кожного $i \in \mathbb{N}$, звідки $A = B$, а отже, ψ – ін'єкція. Прообраз елемента $(a_1, a_2, \ldots, a_k, \ldots) \in (C_2)^\omega$ містить множину $A = \{i \in \mathbb{N} \mid a_i = -1\}$, а тому ψ – сюр'єкція.

Таким чином, групи $\mathcal{P}(\mathbb{N})$ і $(C_2)^\omega$ – ізоморфні.

Цілком аналогічно можна показати, що $\mathcal{P}(X) \cong (C_2)^\tau$ для кожної множини X потужності τ.

Прямою сумою сім'ї груп $\{G_\alpha \mid \alpha \in \mathcal{A}\}$ називається підгрупа

$$\left\{(g_\alpha)_{\alpha\in\mathcal{A}} \in \prod_{\alpha\in\mathcal{A}} G_\alpha \;\middle|\; \{\alpha \mid g_\alpha \neq e_\alpha\} \text{ – скінченна}\right\}$$

прямого добутку $\prod_{\alpha\in\mathcal{A}} G_\alpha$ і позначається $\bigoplus_{\alpha\in\mathcal{A}} G_\alpha$.

Приклад 9.3. Розглянемо підгрупу $\mathcal{P}_{<\omega}(\mathbb{N}) = \{A \subset \mathbb{N} \mid A \text{ – скінченна}\}$ групи $\mathcal{P}(\mathbb{N})$. Образ підгрупи $\mathcal{P}_{<\omega}(\mathbb{N})$ при ізоморфізмі ψ з прикладу 9.2 рівний підгрупі тих послідовностей з $(C_2)^\omega$, які містять скінченну кількість -1. Таким чином, група $\mathcal{P}_{<\omega}(\mathbb{N})$ є ізоморфною прямій сумі зліченної кількості груп C_2.

Зрозуміло, що у випадку скінченної індексної множини $\mathcal{A}$, поняття прямого добутку і прямої суми співпадають.

Теорема 9.2.

Нехай G – група і $H_1, H_2, \ldots, H_n$ – такі її підгрупи, для яких виконано наступні умови:

1) $H_i \lhd G$ *для кожного* $i \in \{1, \ldots, n\}$;
2) $H_i \cap (\prod_{j \neq i} H_j) = \{e\}$ *для кожного* $i \in \{1, \ldots, n\}$;
3) $H_1 \cdot H_2 \cdot \ldots \cdot H_n = G$.

Тоді $G \cong H_1 \times H_2 \times \ldots \times H_n$.

Доведення. Нехай $a \in H_i$, $b \in H_j$ при $i \neq j$. Тоді з умови 1) випливає, що

$$[a, b] = a^{-1}(b^{-1}ab) = (a^{-1}b^{-1}a)b \in H_i \cap H_j = \{e\},$$

звідки $ab = ba$. Розглянемо відображення

$$\psi : H_1 \times H_2 \times \ldots \times H_n \to G, \quad \psi(h_1, h_2, \ldots, h_n) = h_1 \cdot h_2 \cdot \ldots \cdot h_n.$$

Оскільки елементи h_i і h_j комутують, то

$$\begin{gathered}\psi((h_1, h_2, \ldots, h_n) \circ (h'_1, h'_2, \ldots, h'_n)) = \psi(h_1h'_1, h_2h'_2, \ldots, h_nh'_n) = \\ = h_1h'_1h_2h'_2 \cdot \ldots \cdot h_nh'_n = (h_1h_2 \ldots h_n)(h'_1h'_2 \ldots h'_n) = \\ = \psi(h_1, h_2, \ldots, h_n)\psi(h'_1, h'_2, \ldots, h'_n).\end{gathered}$$

Отже, відображення ψ – гомоморфізм.

Нехай $\psi(h_1, h_2, \ldots, h_n) = \psi(h'_1, h'_2, \ldots, h'_n)$. Тоді $h_1h_2 \ldots h_n = h'_1h'_2 \ldots h'_n$, звідки $(h'_1)^{-1}h_1 = h'_2 \ldots h'_nh_n^{-1} \ldots h_2^{-1}$. Якщо h_i і h'_j комутують, то h_i і $(h'_j)^{-1}$ комутують, а отже, $(h'_1)^{-1}h_1 = h'_2h_2^{-1} \ldots h'_nh_n^{-1} \in H_1 \cap (H_2 \cdot \ldots \cdot H_n) = \{e\}$, звідки $h_1 = h'_1$. Аналогічно $h_i = h'_i$ для кожного $i \in \{1, \ldots, n\}$. Таким чином, $(h_1, h_2, \ldots, h_n) = (h'_1, h'_2, \ldots, h'_n)$, і гомоморфізм ψ є мономорфізмом.

З умови 3) випливає, що кожен елемент $g \in G$ можна подати у вигляді $g = h_1h_2 \ldots h_n$, де $h_i \in H_i$ для кожного $i \in \{1, \ldots, n\}$. Тоді $\psi(h_1, h_2, \ldots, h_n) = h_1h_2 \ldots h_n = g$, а тому ψ – епіморфізм. □

Теорема 9.2 обгрунтовує коректність наступного означення.

Група G називається *внутрішнім прямим добутком* підгруп $H_1, H_2, \ldots, H_n$, якщо виконуються наступні умови:

1) $H_i \lhd G$ для кожного $i \in \{1, \ldots, n\}$;
2) $H_i \cap (\prod_{j \neq i} H_j) = \{e\}$ для кожного $i \in \{1, \ldots, n\}$;
3) $H_1 \cdot H_2 \cdot \ldots \cdot H_n = G$.

Приклад 9.4. Розглянемо групу Клейна

$$V_4 = \langle a, b \mid a^2 = b^2 = e, ab = ba \rangle.$$

Нехай $H_1 = \langle a \rangle = \{e, a\}$, $H_2 = \langle b \rangle = \{e, b\}$. Оскільки V_4 – абелева, то $H_1 \lhd G$ і $H_2 \lhd G$. Крім того, $H_1 \cap H_2 = \{e\}$ і $H_1 H_2 = \{e, a\}\{e, b\} = \{e, a, b, ab\} = V_4$.

Таким чином, $V_4 \cong H_1 \times H_2 \cong C_2 \times C_2$.

Приклад 9.5. Опишемо з точністю до ізоморфізму всі абелеві групи G порядку 8.

Якщо група G містить елемент порядку порядку 8, то вона ізоморфна циклічній групі C_8. В іншому випадку за наслідком 4.1 з теореми Лагранжа всі неодиничні елементи групи G мають порядок 2 або 4.

Нехай усі неодиничні елементи групи G мають порядок 2, і a – один із них. Оберемо довільно $b \notin \{e, a\}$, $c \notin \{e, a, b, ab\}$ і розглянемо підгрупи $H_1 = \{e, a\}$, $H_2 = \{e, b\}$, $H_3 = \{e, c\}$. Оскільки $H_1 \cap H_2 = \{e\}$, то $|H_1 H_2| = 4$. Аналогічно з $H_1 H_2 \cap H_3 = \{e\}$ слідує, що $|H_1 H_2 H_3| = 8$, а отже, $H_1 H_2 H_3 = G$ і для підгруп H_1, H_2, H_3 виконуються всі умови з означення внутрішнього прямого добутку. Таким чином,

$$G \cong H_1 \times H_2 \times H_3 \cong C_2 \times C_2 \times C_2 = (C_2)^3.$$

Якщо група G містить елемент a порядку 4, то $G = \{e, a, a^2, a^3\} \sqcup b\{e, a, a^2, a^3\}$ для деякого $b \notin \langle a \rangle$. Якщо $|b| = 4$, то з $b^2 \in \langle a \rangle$ і $|b^2| = 2$ випливає, що $b^2 = a^2$. Тоді $(ba)^2 = b^2 a^2 = a^4 = e$, тобто $|ba| = 2$. Таким чином, множина $G \backslash \langle a \rangle$ містить елемент c порядку 2. Для підгруп $H_1 = \langle a \rangle$ і $H_2 = \langle c \rangle$ виконуються всі умови з означення внутрішнього прямого добутку, а тому

$$G \cong H_1 \times H_2 \cong C_4 \times C_2.$$

Таким чином, з точністю до ізоморфізму існує три абелеві групи порядку 8:

$$C_8, \quad C_4 \times C_2, \quad (C_2)^3.$$

Кажуть, що група G є *напівпрямим добутком* своїх підгруп H_1 і H_2, якщо виконуються наступні умови:

1) $H_1 \lhd G$;
2) $H_1 \cap H_2 = \{e\}$;
3) $H_1 \cdot H_2 = G$.

Напівпрямий добуток груп H_1 і H_2 позначається $H_1 \rtimes H_2$ або $H_1 \leftthreetimes H_2$. Також використовують позначення $H_2 \ltimes H_1$ та $H_2 \rightthreetimes H_1$.

Приклад 9.6. Розглянемо симетричну групу

$$S_3 = \{(1), (12), (13), (23), (123), (132)\}.$$

Єдиною нетривіальною нормальною підгрупою групи S_3 є підгрупа

$$H_1 = \langle (123) \rangle = \{(1), (123), (132)\}.$$

Отже, групу S_3 не можна подати у вигляді внутрішнього прямого добутку своїх нетривіальних підгруп.

Нехай $H_2 = \langle (12) \rangle = \{(1), (12)\}$. Тоді $H_1 \cap H_2 = \{(1)\}$ і

$$H_1 H_2 = \{(1), (123), (132)\}\{(1), (12)\} =$$

$$= \{(1), (123), (132), (12), (13), (23)\} = S_3.$$

Таким чином, $S_3 = H_1 \leftthreetimes H_2 \cong C_3 \leftthreetimes C_2$.

Рекомендована література : [**2**, с. 96–103], [**10**, с. 105–107], [**11**, с. 21–23], [**12**, с. 152–180], [**15**, с. 146–154], [**16**, с. 20–24, 27–28] .

Вправи до лекції 9.

9.1. Побудувати таблицю Келі зовнішнього прямого добутку груп V_4 та C_3.

9.2. Подати циклічну групу C_6 у вигляді внутрішнього прямого добутку власних підгруп.

9.3. Подати групу $(\mathbb{C}\backslash\{0\}, \cdot)$ у вигляді внутрішнього прямого добутку нетривіальних підгруп.

9.4. Подати групу A_4 у вигляді внутрішнього прямого або напівпрямого добутку власних підгруп.

9.5. Чи можна групу Q_8 подати у вигляді внутрішнього прямого або напівпрямого добутку власних підгруп?

9.6. Довести, що $D_n \cong C_n \leftthreetimes C_2$.

9.7. Подати групу $\mathrm{Aff}(\mathbb{R})$ всіх афінних відображень на $\mathbb{R}$ як внутрішній напівпрямий добуток нетривіальних підгруп.

9.8. Довести нерозкладність у прямий добуток нетривіальних підгруп групи $(\mathbb{Z}, +)$.

9.9. Чи можна групу $\mathbb{Z}$ з операцією $m * n = (-1)^n m + n$ подати у вигляді внутрішнього прямого або напівпрямого добутку нетривіальних підгруп?

9.10. Довести, що $(\{2^n 3^m \mid n, m \in \mathbb{Z}\}, \cdot) \cong (\mathbb{Z}, +) \times (\mathbb{Z}, +)$.

9.11. Довести, що група $C_2 \times C_2$ ізоморфна групі $(\{0, 1, 2, 3\}, *)$, де $a * b$ – остача від ділення $a + (-1)^a b$ на 4.

9.12. Знайти всі підгрупи групи $C_3 \times C_3$.

9.13. Нехай $G = C_4 \times C_4$ і $H = \langle (1,-1),(-1,1) \rangle$. Знайти порядок факторгрупи G/H.

9.14. Нехай G – група. Довести, що $D = \{(g,g) \mid g \in G\}$ є підгрупою групи $G \times G$, ізоморфною групі G. Підгрупа D називається *діагональною підгрупою* групи $G \times G$.

9.15. Довести, що $D = \{(g,g) \mid g \in S_3\}$ не є нормальною підгрупою групи $S_3 \times S_3$.

9.16. Нехай G – група, $D = \{(g,g) \mid g \in G\}$ – діагональна підгрупа групи $G \times G$. Довести, що група G є абелевою тоді і лише тоді, коли $D \lhd G \times G$.

9.17. Нехай G – абелева група, $D = \{(g,g) \mid g \in G\}$ – діагональна підгрупа групи $G \times G$. Використовуючи основну теорему про гомоморфізми, довести ізоморфізм $(G \times G)/D \cong G$.

9.18. Нехай $G = \langle a \rangle \times \langle b \rangle$, де $|a| = \infty$, $|b| = 7$. Який порядок елемента ab?

9.19. Скільки елементів порядку $2, 4, 5$ і 6 в групі $C_2 \times C_3 \times C_4$?

9.20. Знайти максимальний порядок елементів групи $S_3 \times S_8$.

9.21. Довести, що $S_3 \times C_2 \cong D_6$.

9.22. Знайти з точністю до ізоморфізму всі абелеві групи порядку 12.

9.23. Показати, що з точністю до ізоморфізму існує єдина абелева група порядку pq, де p і q – прості числа.

9.24. Знайти з точністю до ізоморфізму всі абелеві групи порядку pq^2, де p і q – прості числа.

9.25. Нехай $(n,m) = 1$. Довести, що $C_{nm} \cong C_n \times C_m$.

9.26. Нехай $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s}$, де $p_1, p_2, \dots, p_s$ – різні прості числа. Довести, що

$$C_n \cong C_{p_1^{\alpha_1}} \times C_{p_2^{\alpha_2}} \times \dots \times C_{p_s^{\alpha_s}}.$$

9.27. Нехай елементи $g \in G$ і $h \in H$ мають скінченні порядки n і m відповідно. Довести, що порядок $(g,h) \in G \times H$ дорівнює найбільшому спільному дільнику чисел n і m.

9.28. Нехай $G = H_1 \times H_2$. Довести, що $G/H_1 \cong H_2$.

9.29. Довести, що $(G_1 \times G_2) \times G_3 \cong G_1 \times (G_2 \times G_3) \cong G_1 \times G_2 \times G_3$.

9.30. Нехай $H_1 \lhd G_1$ і $H_2 \lhd G_2$. Довести, що $H_1 \times H_2 \lhd G_1 \times G_2$ і $(G_1 \times G_2)/(H_1 \times H_2) \cong (G_1/H_1) \times (G_2/H_2)$.

9.31. Нехай $G = H_1 \times H_2$. Довести, що кожен елемент $g \in G$ єдиним способом подається у вигляді $g = h_1 h_2$, де $h_1 \in H_1$, $h_2 \in H_2$.

9.32. Показати, що група додатніх раціональних чисел з операцією множення подається у вигляді прямого добутку зліченної множини нескінченних циклічних груп, породжених простими числами. Вивести звідси, що $(\mathbb{Q}_+, \cdot) \cong (\mathbb{Z}, +)^\omega$.

9.33. Подати групу ненульових раціональних чисел з операцією множення у вигляді добутку циклічних груп.

9.34. Довести, що центр прямого добутку рівний прямому добутку центрів співмножників.

9.35. Довести, що циклічна група порядку p^n, де p – просте число, не розкладається в прямий добуток власних підгруп.

9.36. Нехай H і K – групи і $\varphi : K \to \operatorname{Aut} H$ – гомоморфізм. Довести, що декартів добуток $H \times K$ з операцією $(h_1, k_1)(h_2, k_2) = ([\varphi(k_2^{-1})(h_1)]h_2, k_1 k_2)$ є групою, яка є напівпрямим добутком $H \leftthreetimes K$ груп H і K.

Лекція 10. Теореми Силова та їх застосування

Згідно теореми Лагранжа порядок скінченної групи ділиться на порядок кожної своєї підгрупи. Обернене твердження не вірне, тобто в скінченній групі G може і не бути підгрупи порядку, який є дільником $|G|$. Розглянемо наступний приклад.

Приклад 10.1. Покажемо, що знакозмінна група A_4 порядку 12 не містить підгрупи порядку 6. З точністю до ізоморфізму існує дві групи порядку 6: циклічна C_6 і симетрична S_3. Порядок будь-якої підстановки на 4-елементній множині не перевищує 4, а тому група A_4 не містить елемента порядку 6, а отже, і циклічної підгрупи порядку 6. Неможливим є і випадок симетричної групи S_3, оскільки S_3 містить непереставні елементи порядку 2, зокрема (12) та (13): $(12) \circ (13) = (132) \neq (123) = (13) \circ (12)$, в той час як в A_4 всі елементи порядку 2 комутують. Дійсно, A_4 містить три елементи порядку 2: (12)(34), (13)(24) і (14)(23), які є елементами абелевої підгрупи групи A_4, ізоморфної групі Клейна V_4.

Однак у деяких випадках обернена теорема до теореми Лагранжа має місце. Розглянемо один з таких важливих випадків.

Нагадаємо, що групу H називають *p-групою*, якщо $|H| = p^k$, де p — просте число, $k \in \mathbb{N}$. Кажемо, що p-підгрупа H групи G є *силовською p-підгрупою*, якщо її порядок p^k є найбільшим степенем числа p, який ділить $|G|$.

Приклад 10.2. Підгрупа $H = \{(1), (12)(34), (13)(24), (14)(23)\}$ є силовською 2-підгрупою знакозмінної групи A_4 порядку $|A_4| = 2^2 \cdot 3$, а підгрупа $K = \{(1), (12)(34)\}$ є 2-підгрупою групи A_4, але не силовською.

Наступні результати, опубліковані норвезьким математиком П.Л. Силовим у 1872 році, за своєю фундаментальністю і різноманітністю застосувань порівнювані з теоремою Лагранжа.

Спершу доведемо необхідну лему.

Лема 10.1 (Лема Коші).

Якщо просте число p є дільником порядку абелевої групи G, то вона містить підгрупу порядку p.

Доведення. Доведемо методом математичної індукції за порядком групи G. Якщо $|G| = p$ – просте число, то лема очевидна. Нехай $n > 1$, і лема має місце для всіх груп G порядку $|G| < n$. Доведемо для $|G| = n$. Достатньо довести, що G містить елемент порядку p. Оберемо довільний елемент $a \in G \backslash \{e\}$. Якщо $m = |a|$ ділиться на p, то елемент a^k має порядок p, де $k = \frac{m}{p}$. Дійсно, $|a^k| = \frac{m}{(m,k)} = p$. Нехай m не ділиться на p, тобто $(m, p) = 1$. Розглянемо циклічну підгрупу $H = \langle a \rangle$ і факторгрупу G/H. Оскільки $|G/H| = \frac{n}{m}$ ділиться на p і $|G/H| < n$, то за припущенням індукції G/H містить елемент $\overline{b} = bH$ порядку p. Оскільки елемент $b \in G$ належить до прообразу елемента $\overline{b} \in G/H$ при природному гомоморфізмі $\pi : G \to G/H$, то згідно з твердженням 6.2 отримуємо, що $|b|$ ділиться на $|\overline{b}| = p$, тобто $|b| = pt$, $t \in \mathbb{N}$. Але тоді $|b^t| = \frac{pt}{(pt,t)} = p$. Лему доведено. □

Теорема 10.1 (Перша теорема Силова).

Якщо $|G| = p^k \cdot m$, де p – просте число, то група G містить підгрупу H порядку $|H| = p^k$. Зокрема силовські p-підгрупи існують.

Доведення. Доведемо методом математичної індукції за порядком групи G. Якщо $|G| = p$ – просте число, то теорема очевидна. Нехай $n > 1$, і теорема має місце для всіх груп G порядку $|G| < n$. Доведемо для $|G| = n$. При проведенні індуктивного кроку розглянемо два випадки.

1. Порядок центру $Z(G)$ групи G ділиться на p. Оскільки $Z(G)$ є абелевою групою, то за лемою 10.1 група $Z(G)$ містить підгрупу A порядку p. Вона, як і кожна підгрупа центру, є нормальною в групі G. За теоремою Лагранжа порядок факторгрупи G/A ділиться на p^{k-1}. Оскільки $|G/A| = p^{k-1} \cdot m < n$, то за припущенням математичної індукції G/A містить p-підгрупу B порядку $|B| = p^{k-1}$. Позначимо через H повний прообраз групи B при природньому гомоморфізмі $\pi : G \to G/A$. Тоді H є групою, що містить підгрупу A, яка є прообразом одиниці групи B, $A = \mathrm{Ker}\,\pi$. Оскільки звуження π_H природнього гомоморфізму π на підгрупу $H \subset G$ є епіморфізмом $\pi_H : H \to B$, то за основною теоремою про гомоморфізми для груп група B є ізоморфною факторгрупі $H/\mathrm{Ker}\,\pi_H = H/A$. За теоремою Лагранжа $|H| = |B| \cdot |A| = p^k$, а отже, H – шукана p-підгрупа групи G.

2. Порядок центру $Z(G)$ групи G не ділиться на p. Розглянемо дію спряження групи G на G:

$$\circ : G \times G \to G, \quad \circ : (g, a) \mapsto gag^{-1}.$$

Відносно цієї дії група G розбивається на класи спряжених елементів. Якщо клас елемента a є одноточковим, тобто $\{gag^{-1} : g \in G\} = \{a\}$, то $ga = ag$ для кожного $g \in G$, а отже, $a \in Z(G)$. Зрозуміло, що клас кожного елемента центра є одноточковим, а тому $Z(G)$ співпадає з об'єднанням одноточкових класів. Таким чином, отримуємо розбиття

$$G = Z(G) \sqcup K(g_1) \sqcup \ldots \sqcup K(g_s),$$

де $|K(g_i)| \geqslant 2$ для кожного $i \in \{1, \ldots, s\}$. Звідки

$$|G| = |Z(G)| + |K(g_1)| + \ldots + |K(g_s)|.$$

Оскільки $|Z(G)|$ не ділиться на p, а $|G|$ ділиться на p, то $|K(g_t)|$ не ділиться на p для деякого $t \in \{1, \ldots, s\}$. Але $|K(g_t)|$ дорівнює індексу $|G : C(g_t)|$ централізатора $C(g_t)$ елемента g_t в групі G. З того, що

$$p^k \cdot m = |G| = |G : C(g_t)| \cdot |C(g_t)|$$

і $|G : C(g_t)| = |K(g_t)|$ не ділиться на p випливає, що $|C(g_t)|$ ділиться на p^k. Оскільки $|G : C(g_t)| = |K(g_t)| \geqslant 2$, то $|C(g_t)| < |G|$, а тому за припущенням математичної індукції $C(g_t)$ містить підгрупу порядку p^k групи G. □

Теорема 10.2 (Друга теорема Силова).

Нехай H і P – будь-які дві силовські p-підгрупи групи G. Тоді $H = aPa^{-1}$ для деякого елемента $a \in G$. Іншими словами, всі силовські p-підгрупи спряжені в групі G.

Доведення. Нехай $|G| = p^k \cdot m$, де p – просте число, $(p, m) = 1$. Визначимо дію групи H на множині $(G : P) = \{gP \mid g \in G\}$ лівих суміжних класів групи G за підгрупою P:

$$\circ : H \times (G : P) \to (G : P), \quad \circ : (h, gP) \mapsto (hg)P.$$

Відносно цієї дії множина $(G : P)$ розбивається на орбіти, довжини яких ділять порядок $|H| = p^k$ групи H. Таким чином,

$$m = \frac{p^k \cdot m}{p^k} = \frac{|G|}{|P|} = |G : P| = p^{n_1} + \ldots + p^{n_s},$$

де $p^{n_1}, \ldots, p^{n_s}$ – довжини орбіт.

Оскільки $(m, p) = 1$, то принаймні одна орбіта має довжину $p^{n_t} = 1$. Нехай ця орбіта містить елемент $aP \in (G : P)$, де $a \in G$. Тоді $H(aP) = aP$, а тому $H(aPa^{-1}) = aPa^{-1}$. З того, що aPa^{-1} є групою випливає, що $H \subset aPa^{-1}$. Оскільки $|H| = |P| = |aPa^{-1}|$, то $H = aPa^{-1}$. □

Теорема 10.3 (Третя теорема Силова).

Для кількості s_p силовських p-підгруп групи G має місце конгруенція $s_p \equiv 1 (\mathrm{mod}\ p)$ та рівність $s_p = |G : N(P)|$, де P – довільна силовська p-підгрупа групи G.

Доведення. Нехай $|G| = p^k \cdot m$, де p – просте число, $(p, m) = 1$. Позначимо через $\mathcal{S}_p$ - сім'ю всіх силовських p-підгруп групи G. Тоді $P \in \mathcal{S}_p$. Оскільки за теоремою 10.2 всі силовські p-підгрупи спряжені в групі G, то відносно дії

$$\circ : G \times \mathcal{S}_p \to \mathcal{S}_p, \quad \circ : (g, K) \mapsto gKg^{-1}$$

множина $\mathcal{S}_p$ є однорідним G-простором (містить тільки одну орбіту). Отже, $|\mathcal{S}_p|$ дорівнює індексу нормалізатора $N(P)$ в групі G. Таким чином, $s_p = |\mathcal{S}_p| = |G : N(P)|$.

Розглянемо дію групи P на множині $\mathcal{S}_p$:

$$\circ : P \times \mathcal{S}_p \to \mathcal{S}_p, \quad \circ : (g, K) \mapsto gKg^{-1}.$$

Відносно заданої дії множина $\mathcal{S}_p$ розбивається на орбіти, довжини яких є дільниками порядку $|P| = p^k$ групи P. Спершу опишемо всі одноелементні орбіти відносно цієї дії. Нехай $\{H\}$ – одноелементна орбіта, тоді $g^{-1}Hg = H$ для кожного $g \in P$. Звідки випливає, що $P \subset N(H)$. Оскільки $H \subset N(H)$, то P і H – силовські p-підгрупи нормалізатора $N(H)$ групи H. За теоремою 10.2 маємо, що $P = aHa^{-1}$ для деякого $a \in N(H)$. Оскільки $H = aHa^{-1} = P$, то $\{P\}$ – єдина одноелементна орбіта, а тому решта орбіт мають довжину p^r при $r \geqslant 1$. Таким чином,

$$s_p = |\mathcal{S}_p| = |\{P\}| + |\mathcal{O}(K_1)| + \ldots + |\mathcal{O}(K_n)| = 1 + p^{k_1} + \ldots + p^{k_n} = 1 + pt,\ t \in \mathbb{Z}.$$

Звідки слідує конгруенція $s_p \equiv 1 (\mathrm{mod}\ p)$. □

Зауваження 10.1.

Нехай P – силовська p-підгрупа групи G, де $|G| = p^k \cdot m$, $(p, m) = 1$. Оскільки P є підгрупою групи $N(P)$, то за теоремою Лагранжа $|N(P)|$ ділиться на $|P|$. Тоді з рівності $s_p = |G : N(P)| = \frac{|G|}{|N(P)|}$ випливає, що кількість s_p силовських p-підгруп групи G потрібно шукати серед дільників числа $m = \frac{|G|}{p^k}$.

Твердження 10.1.

Силовська p-підгрупа P є нормальною підгрупою групи G тоді і лише тоді, коли $s_p = 1$.

Доведення. Дійсно, група P є нормальною в G тоді і лише тоді, коли $N(P) = G$, що в свою чергу рівносильно рівності $s_p = |G : N(P)| = 1$. □

Приклад 10.3. Покажемо, що кожна група G порядку 70 містить підгрупу порядку 10.

Оскільки згідно з зауваженням 10.1 кількість s_5 силовських 5-підгруп групи G є дільником $\frac{|G|}{5} = 14$ і $s_5 \equiv 1 (\mathrm{mod}\ 5)$, то $s_5 \in \{1, 2, 7, 14\} \cap \{1, 6, 11, 16, \ldots\} = \{1\}$. Таким чином, існує єдина силовська 5-підгрупа H порядку 5, а тому за твердженням 10.1 вона є нормальною в G. За теоремою 10.1 група G містить підгрупу K порядку 2. Оскільки підгрупа H нормальна, то HK є підгрупою групи G згідно з твердженням 5.1. З $(|H|, |K|) = (5, 2) = 1$ та наслідку 4.1 з теореми Лагранжа випливає, що $H \cap K = \{e\}$, а тому $|HK| = |H| \cdot |K| = 10$.

Приклад 10.4. Покажемо, що кожна група G порядку 140 містить підгрупу індекса 2.

Оскільки згідно з зауваженням 10.1 кількість s_5 силовських 5-підгруп групи G є дільником $\frac{|G|}{5} = 28$ і $s_5 \equiv 1 (\mathrm{mod}\ 5)$, то $s_5 \in \{1, 2, 4, 7, 14, 28\} \cap \{1, 6, 11, 16, 21, 26, 31, \ldots\} = \{1\}$. Таким чином, існує єдина силовська 5-підгрупа H_1 порядку 5, а тому за твердженням 10.1 вона є нормальною в G. Аналогічно s_7 є дільником $\frac{|G|}{7} = 20$ і $s_7 \equiv 1 (\mathrm{mod}\ 7)$, а отже, $s_7 = 1$. Тому група G містить нормальну силовську 7-підгрупу H_2 порядку 7. Згідно з твердженням 5.2 добуток $H = H_1 H_2$ двох нормальних підгруп H_1 та H_2 є нормальною підгрупою групи G. З $(|H_1|, |H_2|) = (5, 7) = 1$ та

наслідку 4.1 з теореми Лагранжа випливає, що $H_1 \cap H_2 = \{e\}$, а тому $|H| = |H_1| \cdot |H_2| = 35$. За теоремою 10.1 група G містить підгрупу K порядку 2. Оскільки підгрупа H нормальна, то $T = HK$ є підгрупою групи G згідно з твердженням 5.1, і $|T| = |H| \cdot |K| = 70$. Таким чином, індекс підгрупи T в групі G дорівнює $\frac{|G|}{|T|} = 2$.

Приклад 10.5. Покажемо, що кожна група G порядку 33 є циклічною.

Знайдемо кількість s_3 силовських 3-підгруп та кількість s_{11} силовських 11-підгруп групи G. Згідно з зауваженням 10.1 число s_3 є дільником $\frac{|G|}{3} = 11$ і за теоремою 10.3 має місце конгруенція $s_3 \equiv 1 (\mathrm{mod}\ 3)$. Тоді $s_3 \in \{1, 11\} \cap \{1, 4, 7, 10, 13, \ldots\} = \{1\}$. Отже, $s_3 = 1$, а тому за твердженням 10.1 силовська 3-підгрупа H_1 порядку $|H_1| = 3$ є нормальною підгрупою групи G. Аналогічно s_{11} є дільником 3 і $s_{11} \equiv 1 (\mathrm{mod}\ 11)$, а отже, $s_{11} = 1$. Тому група G містить нормальну силовську 11-підгрупу H_2 порядку $|H_2| = 11$. Оскільки за наслідком 4.1 з теореми Лагранжа всі неодиничні елементи групи H_1 мають порядок 3, а всі неодиничні елементи групи H_2 порядок 11, то $H_1 \cap H_2 = \{e\}$. Звідси слідує, що $|H_1H_2| = |H_1| \cdot |H_2| = 33$, а тому $H_1H_2 = G$. Таким чином, група G є внутрішнім прямим добутком нормальних підгруп H_1 і H_2. Оскільки групи H_1 і H_2 мають простий порядок, то вони є циклічними, а тому група $G \cong C_3 \times C_{11}$ є абелевою.

Нехай $H_1 = \langle a \rangle$, $H_2 = \langle b \rangle$. Покажемо, що елемент $c = ab = ba$ має порядок $3 \cdot 11 = 33$. За наслідком 4.1 з теореми Лагранжа $|c| \in \{1, 3, 11, 33\}$. Якби $|c| = 1$, то $ab = e$, звідки $|a| = |b|$, і отримуємо суперечність. Якщо б $|c| = 3$, то $e = (ab)^3 = a^3b^3 = b^3$, що суперечить $|b| = 11$. Аналогічно у випадку $|c| = 11$ отримаємо $a^{11} = e$, звідки $e = a^2(a^3)^3 = a^2e = a^2$ – суперечність з $|a| = 3$. Таким чином, $|c| = 33$, а тому породжена елементом c циклічна підгрупа співпадає з групою G. Отже, G – циклічна група.

Приклад 10.6. Знайдемо кількість елементів порядку 7 простої групи G порядку 168.

Спершу відшукаємо кількість силовських 7-підгруп групи G порядку $|G| = 168 = 2^3 \cdot 3 \cdot 7$. Як відомо s_7 є дільником $\frac{168}{7} = 24$ і $s_7 \equiv 1 (\mathrm{mod}\ 7)$. Отже, $s_7 \in \{1, 2, 3, 4, 6, 8, 12, 24\} \cap \{1, 8, 15, 22, 29, \ldots\} = \{1, 8\}$. Оскільки група G проста, то вона не містить власних нормальних підгруп, а тому

$s_7 \neq 1$ згідно з твердженням 10.1. Таким чином, група G містить 8 підгруп порядку 7. За наслідком 4.1 з теореми Лагранжа кожен неодиничний елемент підгрупи порядку 7 має порядок 7. Отже, кожна підгрупа порядку 7 містить 6 елементів порядку 7. Дві різні підгрупи порядку 7 мають тривіальний перетин (бо інакше спільний неодиничний елемент мав би порядок 7 і породжував би їх обох, а тому вони б збігалися). Таким чином, кількість елементів порядку 7 дорівнює $8 \cdot 6 = 48$.

Твердження 10.2.

Нехай група G має порядок $|G| = p^2q$, де p і q – різні прості числа. Тоді G містить нормальну силовську p-підгрупу або нормальну силовську q-підгрупу.

Доведення. Припустимо супротивне, тоді за твердженням 10.1 отримаємо нерівності $s_p > 1$ і $s_q > 1$. Силовські q-підгрупи мають порядок q, а тому є циклічними і породжуються будь-яким своїм неодиничним елементом. Таким чином, кожен елемент порядку q породжує силовську q-підгрупу. Оскільки єдиними дільниками q є 1 і q, то дві різні силовські q-підгрупи мають тривіальний перетин. Звідси випливає, що кількість елементів порядку q групи G дорівнює $s_q(q-1)$. Згідно з зауваженням 10.1 число s_q ділить p^2, а тому $s_q \in \{p, p^2\}$.

Якщо $s_q = p^2$, то кількість елементів, порядком яких не є число q дорівнює $p^2q - p^2(q-1) = p^2$. Оскільки силовська p-підгрупа має порядок p^2 і не може містити елементів порядку q, то вона містить всі p^2 елементів, які не мають порядку q. Звідси випливає, що інших силовських p-підгруп немає, тобто $s_p = 1$ – суперечність.

Нехай $s_q = p$. Тоді $p = s_q \equiv 1 (\mathrm{mod}\ q)$, а отже $p > q$. Оскільки s_p ділить q, то $s_p = q$. Звідки $q \equiv 1 (\mathrm{mod}\ p)$, а отже, $q > p$. Таким чином, початкове припущення не вірне і група G містить нормальну силовську p-підгрупу або нормальну силовську q-підгрупу. □

Скінченна група G називається *нільпотентною*, якщо всі її силовські підгрупи є нормальними. Зрозуміло, що кожна група порядку p^n, де p – просте число, є нільпотентною.

Далі опишемо з точністю до ізоморфізму всі групи порядків p, p^2 і pq, де p, q – прості числа.

Якщо порядок групи G дорівнює p, то за наслідком 4.1 з теореми Лагранжа кожен неодиничний елемент групи G має порядок p, а тому G є циклічною групою, породженою будь-яким неодиничним елементом. Таким чином, з твердження 6.4 випливає наступне

Твердження 10.3.

З точністю до ізоморфізму існує єдина група простого порядку p – циклічна C_p.

Перейдемо до опису всіх груп G порядку p^2. Згідно з наслідком з теореми Лагранжа порядок кожного неодиничного елемента групи G належить множині $\{p, p^2\}$.

Якщо група G містить елемент порядку p^2, то вона є циклічною групою, породженою даним елементом. Таким чином, в цьому випадку група G ізоморфна циклічній групі C_{p^2} порядку p^2.

Нехай кожен неодиничний елемент групи G має порядок p. Оберемо довільні елементи $a \in G\backslash\{e\}$ і $b \in G\backslash\langle a\rangle$. Перетин циклічних підгруп $\langle a\rangle$ і $\langle b\rangle$ дорівнює $\{e\}$, бо якби $\langle a\rangle \cap \langle b\rangle$ містив деякий неодиничний елемент, то породжена ним підгрупа порядку p співпадала би як з $\langle a\rangle$, так і з $\langle b\rangle$. Оскільки згідно з твердженням 7.3 група G є абелевою, то $\langle a\rangle$ і $\langle b\rangle$ – нормальні в G підгрупи. Крім того, $\langle a\rangle \cdot \langle b\rangle = G$. Отже, $G \cong \langle a\rangle \times \langle b\rangle \cong C_p \times C_p$.

Таким чином, отримуємо наступне

Твердження 10.4.

Якщо p – просте число, то з точністю до ізоморфізму існує дві групи порядку p^2 – C_{p^2} і $C_p \times C_p$.

Приклад 10.7. Покажемо, що кожна група G порядку 36 не є простою.

Згідно з зауваженням 10.1 кількість s_3 силовських 3-підгруп групи G є дільником $\frac{|G|}{9} = 4$ і $s_3 \equiv 1 (\mathrm{mod}\ 3)$ за теоремою 10.3, а тому $s_3 \in \{1, 4\}$. Якщо $s_3 = 1$, то за твердженням 10.1 силовська 3-підгрупа є нормальною. Нехай G містить 4 різні силовські 3-підгрупи порядку 9 і H, K – довільні дві з них. Оскільки $|H| = |K| = 9$, то за твердженням 7.3 дані групи є абелевими, а тому їх підгрупа $H \cap K$ є нормальною як в K, так і в H. З того, що $H \neq K$ і теореми Лагранжа випливає, що $|H \cap K| \in \{1, 3\}$. Якби $|H \cap K| = 1$, то $|HK| = |H||K| = 81 > 36 = |G|$, а тому $|H \cap K| = 3$. Оскільки $H \cap K$ є нормальною в H і K, то нормалізатор $N(H \cap K)$ підгрупи $H \cap K$ в групі G містить обидві групи H і K. Тоді з рівності $|H \cap K| = 3$ випливає, що $|N(H \cap K)| \geqslant 15$. Оскільки група $N(H \cap K) \subset G$ містить підгрупу H, то за теоремою Лагранжа $|G| = 36$ ділиться на $|N(H \cap K)|$ і $|N(H \cap K)|$ ділиться на $|H| = 9$. Таким чином, $|N(H \cap K)| \in \{18, 36\}$. Якщо $|N(H \cap K)| = 18$, то підгрупа $N(H \cap K)$ індекса 2 є нормальною в G. У випадку $|N(H \cap K)| = 36$ маємо $G = N(H \cap K)$, а тому $H \cap K$ є нормальною підгрупою групи G.

Приклад 10.8. Доведемо, що кожна група G порядку 75950, яка містить підгрупу індекса 2, є розв'язною.

Нехай H – підгрупа індекса 2 в групі G порядку $|G| = 2 \cdot 5^2 \cdot 7^2 \cdot 31$. Тоді $|H| = \frac{|G|}{2} = 5^2 \cdot 7^2 \cdot 31$. Кожна підгрупа індекса 2 є нормальною і факторгрупа G/H має порядок 2, тому є циклічною, а отже, абелевою.

Оскільки s_{31} є дільником $\frac{|H|}{31} = 5^2 7^2$ і $s_{31} \equiv 1 (\mathrm{mod}\ 31)$, то

$$s_{31} \in \{1, 5, 7, 25, 35, 49, 175, 245, 1225\}.$$

Серед даних чисел тільки для 1 виконується конгруенція, а тому $s_{31} = 1$, і група H містить нормальну силовську 31-підгрупу K.

Покажемо, що факторгрупа H/K є абелевою. Легко перевірити, що кожна група порядку $5^2 \cdot 7^2$, зокрема і H/K, містить нормальну силовську 5-підгрупу H_1 порядку 25 і нормальну силовську 7-підгрупу H_2 порядку 49. Оскільки за наслідком з теореми Лагранжа всі неодиничні елементи групи H_1 мають порядок 5 або 25, а всі неодиничні елементи групи H_2 порядок 7 або 49, то $H_1 \cap H_2 = \{e\}$. Звідси слідує, що $|H_1 \cdot H_2| = |H_1| \cdot |H_2| = 1225$, а тому $H/K \cong H_1 \times H_2$. За твердженням 7.3 групи H_1 і H_2 є абелевими, а тому група H/K також є абелевою.

Тривіальна підгрупа $\{e\}$ є нормальною в кожній групі, зокрема в групі K. Крім того, факторгрупа $K/\{e\} \cong K$ простого порядку 31 є циклічною, а тому – абелева.

Таким чином, ми побудували нормальний ряд

$$G \rhd H \rhd K \rhd \{e\}$$

з абелевими факторгрупами G/H, H/K та $K/\{e\}$. Отже, група G є розв'язною.

Розглянемо групу G порядку $|G| = pq$, де p, q – прості числа, $p < q$.

Згідно з теоремою 10.3 і зауваженням 10.1 для кількості s_q силовських q-підгруп має місце конгруенція $s_q \equiv 1 (\mathrm{mod}\ q)$ і s_q є дільником $\frac{|G|}{q} = p$. Оскільки при $t \geqslant 1$ маємо $p < q < 1 + qt$, то $s_q = 1$. Отже, за твердженням 10.1 силовська q-підгрупа Q порядку $|Q| = q$ є нормальною підгрупою групи G.

Кількість s_p силовських p-підгруп є дільником $\frac{|G|}{p} = q$, а отже, $s_p = 1$ або $s_p = q$. Крім того, має місце конгруенція $s_p \equiv 1 (\mathrm{mod}\ p)$. Якщо $s_p = 1$ (це гарантовано буде виконуватися у випадку, коли p не є дільником $q - 1$), то силовська p-підгрупа P порядку p є нормальною в G. Нехай $a \in Q \backslash \{e\}$ і $b \in P \backslash \{e\}$, а тому $|a| = q$ і $|b| = p$. Тоді $Q = \langle a \rangle$, $P = \langle b \rangle$. З різних порядків неодиничних елементів груп Q і P випливає, що $Q \cap P = \{e\}$. Крім того, $\langle a \rangle \cdot \langle b \rangle = G$, а отже, $G \cong \langle a \rangle \times \langle b \rangle \cong C_q \times C_p$ – абелева група. Легко перевірити, що елемент $c = ab = ba$ має порядок pq, а тому $G = \langle c \rangle$. Таким чином, у випадку $s_p = 1$ група G є циклічною, і $G \cong C_q \times C_p \cong C_{pq}$. Якщо ж $s_p = q$, то

за твердженням 10.1 група P не є нормальною підгрупою групи G. Оскільки група $Q = \langle a \rangle$ є нормальною, то $b^{-1}ab = a^r$ для деякого $r \in \{1, \dots, q-1\}$. Якщо $r = 1$, то група G є абелевою. Нехай $r \neq 1$. Тоді $a^{ri} = (b^{-1}ab)^i = b^{-1}a^ib$ для кожного $i \in \mathbb{Z}$, зокрема $b^{-1}a^rb = a^{r^2}$, звідки випливає, що $b^{-2}ab^2 = b^{-1}a^rb = a^{r^2}$, а отже, $b^{-s}ab^s = a^{r^s}$ для кожного $s \in \mathbb{Z}$. Таким чином, при $s = p$ маємо $a = b^{-p}ab^p = a^{r^p}$, звідки $a^{r^p-1} = e$. Оскільки $|a| = q$, то $r^p - 1$ ділиться на q, а отже, $r^p \equiv 1 (\mathrm{mod}\ q)$. Крім того, одержуємо формулу множення

$$(b^xa^y)(b^za^t) = b^x(a^yb^z)a^t = b^x(b^za^{yr^z})a^t = b^{x+z}a^{yr^z+t}, \text{ де } x, y, z, t \in \mathbb{Z}.$$

Легко перевірити, що якщо $q - 1$ ділиться на p, $r^p \equiv 1 (\mathrm{mod}\ q)$ і $r \in \{2, \dots, q-1\}$, то дана формула визначає неабелеву групу порядку pq, породжену елементами a і b. За малою теоремою Ферма конгруенція $r^{q-1} \equiv 1 (\mathrm{mod}\ q)$ має $q - 1$ розв'язків, які утворюють циклічну мультиплікативну групу порядку $q - 1$. Розв'язки конгруенції $r^p \equiv 1 (\mathrm{mod}\ q)$ утворюють циклічну підгрупу порядку p, а тому ті з них, які відмінні від $1 + q\mathbb{Z}$ мають вигляд $r+q\mathbb{Z}, r^2+q\mathbb{Z}, \dots, r^{p-1}+q\mathbb{Z}$, де $r+q\mathbb{Z}$ – один з таких розв'язків. Всі ці розв'язки визначають одну і ту ж групу порядку pq, оскільки заміна твірного b на b^j веде до заміни r на r^j.

Оскільки $Q \lhd G$, $Q \cap P = \{e\}$ і $Q \cdot P = G$, то в цьому випадку група G є напівпрямим добутком $Q \rtimes P \cong C_q \rtimes C_p$ груп Q і P.

Таким чином, отримуємо наступне

Твердження 10.5.

Нехай p, q прості числа, $p < q$. Якщо $q - 1$ не ділиться на p, то з точністю до ізоморфізму існує єдина група порядку pq: циклічна C_{pq}; а коли $q - 1$ ділиться на p, то – дві: циклічна C_{pq} і неабелева

$$G = \langle a, b \mid a^q = b^p = e, ab = ba^r \rangle,$$

де $r^p \equiv 1 (\mathrm{mod}\ q)$ і $r \in \{2, \dots, q-1\}$.

Приклад 10.9. Опишемо всі неабелеві групи G порядку 8. Група G не містить елемента порядку 8, бо інакше вона була б циклічною. Якщо всі її елементи порядку 2, то $ba = a^2bab^2 = a(ab)^2b = ab$, а тому G – абелева група. Таким чином, група G містить елемент a порядку 4. Нехай $b \notin \langle a \rangle = H$, тоді $G = H \sqcup bH$ і $b^2 \in H$. Якщо $b^2 \in \{a, a^3\}$, то b є елементом порядку 8, і G – циклічна група. Отже, $b^2 \in \{e, a^2\}$. Оскільки H є нормальною підгрупою групи G, то $b^{-1}ab \in H$. З того, що $b^{-1}ab$ є елементом порядку 4 випливає $b^{-1}ab \in \{a, a^3\}$. Якщо $b^{-1}ab = a$, то G є абелевою групою, а тому $b^{-1}ab = a^3$. Отже, з точністю до ізоморфізму є дві неабелеві групи G порядку 8:

$D_4 = \langle a, b \mid a^4 = b^2 = e, b^{-1}ab = a^3 \rangle$, $Q_8 = \langle a, b \mid a^4 = e, b^2 = a^2, b^{-1}ab = a^3 \rangle$.

Використовуючи раніше отримані результати, у наступній таблиці подамо повну класифікацію з точністю до ізоморфізму груп G порядку $|G| \leqslant 10$:

порядок	кількість	абелеві	неабелеві
1	1	C_1	–
2	1	C_2	–
3	1	C_3	–
4	2	$C_4, V_4 \cong C_2 \times C_2$	–
5	1	C_5	–
6	2	C_6	$S_3 \cong D_3 \cong C_3 \rtimes C_2$
7	1	C_7	–
8	5	$C_8, C_4 \times C_2, C_2 \times C_2 \times C_2$	$Q_8, D_4 \cong C_4 \rtimes C_2$
9	2	$C_9, C_3 \times C_3$	–
10	2	C_{10}	$D_5 \cong C_5 \rtimes C_2$

Рекомендована література : [**2**, с. 92–96], [**11**, с. 23–26], [**12**, с. 139–149], [**13**, с. 54–64], [**15**, с. 227–238].

Вправи до лекції 10.

10.1. Виписати всі силовські 2-підгрупи і 3-підгрупи груп S_3 і A_4.

10.2. Для кожної пари (H, P) силовських 2-підгруп групи S_3 знайти такий елемент $a \in S_3$, що $H = aPa^{-1}$.

10.3. Знайти порядки всіх силовських підгруп симетричної групи S_{20}.

10.4. Знайти порядок силовської p–підгрупи групи S_{p^k}.

10.5. Нехай G – абелева група порядку n, і просте число p є дільником n. Довести, що група G містить єдину силовську p-підгрупу. Знайти силовську 2-підгрупу та силовську 3-підгрупу циклічної групи C_{24}.

10.6. Скільки силовських 7-підгруп і 11-підгруп містить група порядку 4235?

10.7. Скільки підгруп порядку 5 містить знакозмінна група A_5?

10.8. Довести, що не існує простих груп порядків 350, 196, 200.

10.9. Скільки елементів порядку 5 містить група порядку 255, яка не має нормальних підгруп порядку 5?

10.10. Скільки різних силовських 3-підгруп і силовських 5-підгруп в неабелевій групі порядку 225?

10.11. Показати, що всі групи порядків 15, 101, 143 та 2431 є циклічними.

10.12. Довести, що всі силовські підгрупи групи порядку 11025 є абелевими.

10.13. Довести, що кожна група порядку 5929 є абелевою.

10.14. Показати, що кожна група порядку 385 містить нормальну підгрупу порядку 77.

10.15. Довести, що група G порядку 715 містить підгрупи всіх порядків, які є дільниками 715.

10.16. Довести, що кожна група порядку 30 містить підгрупу індекса 2.

10.17. Показати, що групи порядків 56 і 80 містять нормальні силовські підгрупи.

10.18. Нехай G – група порядку 48. Показати, що перетин кожних двох різних силовських 2-підгруп групи G має порядок 8.

10.19. Довести, що всі групи порядків 1815 і 1474 є розв'язними.

10.20. Чи існують нерозв'язні групи порядку 27783?

10.21. З'ясувати, чи є група S_3 нільпотентною.

10.22. Показати, що кожна група порядку 1225 – нільпотентна.

10.23. Довести, що кожна нільпотентна група є розв'язною.

10.24. Довести, що $(G, \circ)$, де

$$G = (\mathbb{Z}_3 \backslash \{0\}) \times \mathbb{Z}_3, \quad (a_1, b_1) \circ (a_2, b_2) = (a_1 a_2, a_1 b_2 + b_1),$$

є групою, ізоморфною симетричній групі S_3.

10.25. В групі $(G, \circ)$ знайти неабелеву підгрупу порядку 21, якщо

$$G = (\mathbb{Z}_7 \backslash \{0\}) \times \mathbb{Z}_7, \quad (a_1, b_1) \circ (a_2, b_2) = (a_1 a_2, a_1 b_2 + b_1).$$

10.26. Нехай p, q – прості числа і $q - 1$ ділиться на p. Довести, що група $(G, \circ)$, де

$$G = (\mathbb{Z}_q \backslash \{0\}) \times \mathbb{Z}_q, \quad (a_1, b_1) \circ (a_2, b_2) = (a_1 a_2, a_1 b_2 + b_1),$$

містить неабелеву підгрупу порядку pq.

10.27. Знайти всі нормальні підгрупи діедральної групи D_p порядку $2p$, де p – просте число.

10.28. Довести, що якщо $|G| = p^2 q^2 \neq 36$ (де p і q – прості числа), то G містить нормальну силовську підгрупу.

10.29. Довести, що скінченна група G розкладається в прямий добуток своїх силовських підгруп тоді й лише тоді, коли вона для кожного простого дільника p свого порядку містить єдину силовську p–підгрупу.

10.30. Довести, що всі групи порядків $p^2 q$ та $2pq$, де p, q – прості числа, є розв'язними.

10.31. Нехай H – нормальна підгрупа скінченної групи G, P – силовська p-підгрупа групи H. Довести, що $G = N(P)H$.

10.32. Довести, що якщо підгрупа K скінченої групи G містить нормалізатор деякої силовської підгрупи, то $N(K) = K$.

Розділ II

Елементи теорії кілець

Лекція 1. Основні означення. Класи кілець

Трійка $(R, \dotplus, \odot)$, де R – множина, $\dotplus : R \times R \to R$, $\odot : R \times R \to R$ – бінарні операції, називається *кільцем*, якщо виконуються наступні умови:

1) $(R, \dotplus)$ – абелева група;
2) $(R, \odot)$ – напівгрупа;
3) для кожних $a, b, c \in R$ мають місце рівності

$$a \odot (b \dotplus c) = (a \odot b) \dotplus (a \odot c),$$

$$(a \dotplus b) \odot c = (a \odot c) \dotplus (b \odot c).$$

Для спрощення запису надалі вважатимемо, що бінарна операція $\odot$ має вищий пріоритет, ніж $\dotplus$. Якщо з контексту зрозуміло, про які бінарні операції йде мова, то замість $(R, \dotplus, \odot)$ писатимемо R.

Приклад 1.1. Нехай $(G, \dotplus)$ – абелева група з одиницею e. Визначимо бінарну операцію $\odot : G \times G \to G$ поклавши $a \odot b = e$ для кожних $a, b \in G$. Тоді $(G, \dotplus, \odot)$ – кільце. Дійсно,

$$a \odot (b \odot c) = a \odot e = e = e \odot c = (a \odot b) \odot c,$$

$$a \odot (b \dotplus c) = e = e \dotplus e = (a \odot b) \dotplus (a \odot c),$$

$$(a \dotplus b) \odot c = e = e \dotplus e = (a \odot c) \dotplus (b \odot c).$$

Приклад 1.2. Більшість відомих нам числових множин з операціями додавання і множення є кільцями: $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$. Трійка $(\mathbb{N}, +, \cdot)$ не є кільцем, оскільки $(\mathbb{N}, +)$ не є групою.

Якщо $(R, \dotplus, \odot)$ – кільце, то потужність $|R|$ множини R називається *порядком* кільця. Кільце скінченного порядку називатимемо *скінченним*.

Одиницю групи $(R, \dotplus)$ називатимемо *нулем кільця* $(R, \dotplus, \odot)$ і позначатимемо θ. Обернений елемент до елемента a групи $(R, \dotplus)$ називатимемо *протилежним елементом до* a і позначатимемо $\ominus a$. Домовимося також через $a \ominus b$ позначати елемент $a \dotplus (\ominus b)$.

Твердження 1.1.

Нехай $(R, \dotplus, \odot)$ *– кільце. Тоді для кожних* $a, b \in R$ *мають місце рівності:*

1) $a \odot \theta = \theta \odot a = \theta$;
2) $\ominus(a \odot b) = (\ominus a) \odot b = a \odot (\ominus b)$.

Доведення. 1) Оскільки

$$\theta \dotplus a \odot \theta = a \odot \theta = a \odot (\theta \dotplus \theta) = a \odot \theta \dotplus a \odot \theta \quad \text{і}$$
$$\theta \dotplus \theta \odot a = \theta \odot a = (\theta \dotplus \theta) \odot a = \theta \odot a \dotplus \theta \odot a,$$

то $a \odot \theta = \theta = \theta \odot a$.

2) З рівностей

$$a \odot b \dotplus (\ominus a) \odot b = (a \ominus a) \odot b = \theta \odot b = \theta \quad \text{і}$$
$$a \odot b \dotplus a \odot (\ominus b) = a \odot (b \ominus b) = a \odot \theta = \theta$$

випливає, що $\ominus(a \odot b) = (\ominus a) \odot b = a \odot (\ominus b)$. □

Кільце $(R, \dotplus, \odot)$ називається *комутативним*, якщо $a \odot b = b \odot a$ для кожних $a, b \in R$. Якщо $(R, \odot)$ – моноїд з одиницею e, то кільце $(R, \dotplus, \odot)$ називається *кільцем з одиницею*, а елемент e – *одиницею кільця*.

Приклад 1.3. Нехай R – кільце, $n \in \mathbb{N}$. Позначимо через $M(n, R)$ множину всіх $n \times n$-матриць з елементами з кільця R. Множина $M(n, R)$ з операціями додавання і множення матриць є кільцем з одиницею. Якщо $R \neq \{\theta\}$ і $n \geqslant 2$, то кільце $M(n, R)$ не є комутативним.

Елемент a кільця $(R, \dotplus, \odot)$ називається *ідемпотентом*, якщо $a \odot a = a$.

Приклад 1.4. Якщо R – кільце з одиницею e, то в кільці $M(2, R)$ для кожного $a \in R$ матриця $\begin{pmatrix} e & a \\ \theta & \theta \end{pmatrix}$ є ідемпотентом, оскільки

$$\begin{pmatrix} e & a \\ \theta & \theta \end{pmatrix} \begin{pmatrix} e & a \\ \theta & \theta \end{pmatrix} = \begin{pmatrix} e & a \\ \theta & \theta \end{pmatrix}.$$

Елемент $a \neq \theta$ комутативного кільця $(R, \dotplus, \odot)$ називається *дільником нуля*, якщо $a \odot b = \theta$ для деякого $b \in R$, $b \neq \theta$.

Приклад 1.5. У кільці $M(2,R)$ матриці $\begin{pmatrix} a & \theta \\ \theta & \theta \end{pmatrix}$ і $\begin{pmatrix} \theta & \theta \\ \theta & b \end{pmatrix}$, де $a,b \in R\backslash\{\theta\}$, є дільниками нуля, оскільки

$$\begin{pmatrix} a & \theta \\ \theta & \theta \end{pmatrix}\begin{pmatrix} \theta & \theta \\ \theta & b \end{pmatrix} = \begin{pmatrix} \theta & \theta \\ \theta & \theta \end{pmatrix} \text{ і } \begin{pmatrix} \theta & \theta \\ \theta & b \end{pmatrix}\begin{pmatrix} a & \theta \\ \theta & \theta \end{pmatrix} = \begin{pmatrix} \theta & \theta \\ \theta & \theta \end{pmatrix}.$$

Якщо $R=\{\theta\}$, то кільце R називатимемо *тривіальним*, в іншому випадку – *нетривіальним*.

Нетривіальне комутативне кільце з одиницею називається *цілісним кільцем* або *областю цілісності*, якщо воно не містить дільників нуля, тобто з рівності $a\odot b=\theta$ випливає, що $a=\theta$ або $b=\theta$.

Твердження 1.2.

Нехай $(R,\dotplus,\odot)$ – нетривіальне комутативне кільце з одиницею. Кільце R є цілісним тоді і лише тоді, коли для кожного $a\in R\backslash\{\theta\}$ лівий зсув

$$l_a : R\to R,\quad l_a(x)=a\odot x,$$

є ін'єктивним відображенням.

Доведення. Нехай R – цілісне кільце і $a\neq\theta$. Якщо $l_a(x)=l_a(y)$, то $a\odot x=a\odot y$, а тому $a\odot(x\ominus y)=\theta$. Оскільки $a\neq\theta$ і R – цілісне кільце, то $x\ominus y=\theta$, звідки $x=y$. Отже, l_a – ін'єктивне відображення.

Нехай кільце R не є цілісним. Тоді існують такі елементи $a,b\in R$, $a\neq\theta$, $b\neq\theta$, що $a\odot b=\theta$. Оскільки $l_a(\theta)=a\odot\theta=\theta=a\odot b=l_a(b)$, то відображення l_a не є ін'єктивним. □

Кільце $(R,\dotplus,\odot)$ з одиницею $e\neq\theta$ називається *тілом*, якщо $(R\backslash\{\theta\},\odot)$ є групою, тобто для кожного $a\in R$, $a\neq\theta$, існує $a^{-1}\in R$, що $a\odot a^{-1}=a^{-1}\odot a=e$. Комутативне тіло називається *полем*.

Кожне поле $(F,\dotplus,\odot)$ є цілісним кільцем. Дійсно, якщо $a,b\in F$, $a\odot b=\theta$ і $a\neq\theta$, то існує $a^{-1}\in R$, що $a\odot a^{-1}=a^{-1}\odot a=e$. Але тоді $b=e\odot b=a^{-1}\odot a\odot b=a^{-1}\odot\theta=\theta$.

Приклад 1.6. Кільця $(\mathbb{Q},+,\cdot)$, $(\mathbb{R},+,\cdot)$, $(\mathbb{C},+,\cdot)$ є полями, а $(\mathbb{Z},+,\cdot)$ – цілісне кільце, яке не є полем.

Твердження 1.3.

Кожне скінченне цілісне кільце є полем.

Доведення. Нехай $(R, \dotplus, \odot)$ – скінченне цілісне кільце. Тоді R – комутативне кільце з одиницею e. Нехай $a \in R$, $a \neq \theta$. За твердженням 1.2 відображення $l_a : R \to R$, $l_a(x) = a \odot x$, є ін'єктивним. Оскільки кільце R є скінченним, то l_a – сюр'єктивне відображення. Тоді для одиниці $e \in R$ існує такий $x \in R$, що $l_a(x) = e$, звідки $a \odot x = e$ і $x = a^{-1}$. Таким чином, для кожного ненульового елемента a кільця R існує обернений $a^{-1} \in R$, а тому R – поле. □

Нехай $(R, \dotplus, \odot)$ – кільце з одиницею e. Позначимо через R^* множину всіх оборотних елементів моноїда $(R, \odot)$. Якщо a і b – оборотні елементи, то $(a \odot b)^{-1} = b^{-1} \odot a^{-1}$ і $(a^{-1})^{-1} = a$, а тому R^* – група, яка називається *групою дільників одиниці* кільця R.

Приклад 1.7. У кільці $(\mathbb{Z}, +, \cdot)$ з рівності $ab = 1$ випливає, що $a = b = 1$ або $a = b = -1$, а тому $\mathbb{Z}^* = \{1, -1\}$.

Зрозуміло, що комутативне кільце F з одиницею є полем тоді і лише тоді, коли $F^* = F \backslash \{\theta\}$.

Серед непорожніх підмножин кільця R деякі можуть також бути кільцями. Підмножина K кільця R називається *підкільцем*, якщо K є кільцем відносно тих же операцій, які визначені на R. Зауважимо, що кожне кільце R містить нульове підкільце $\{\theta\}$ і підкільце R. Ці підкільця називаються *тривіальними підкільцями. Власним підкільцем* кільця R називається підкільце $K \neq R$.

З твердження 1.4 розділу I випливає наступне

Твердження 1.4 (Критерій підкільця).

Непорожня підмножина K кільця $(R, \dotplus, \odot)$ є підкільцем кільця R тоді і лише тоді, коли $a \ominus b, a \odot b \in K$ для всіх $a, b \in K$.

Приклад 1.8. Розглянемо кільце $(\mathbb{R}, +, \cdot)$. Оскільки $a - b, ab \in \mathbb{Z}$ для будь-яких цілих чисел a і b, то $\mathbb{Z}$ є підкільцем кільця $\mathbb{R}$. Проте для натурального числа $1 \in \mathbb{N}$ протилежний до нього в кільці $\mathbb{R}$ елемент -1 не є натуральним числом, а тому $\mathbb{N}$ не є підкільцем кільця $\mathbb{R}$.

Твердження 1.5.

Перетин довільної непорожньої сім'ї підкілець кільця R є підкільцем кільця R.

Доведення. Нехай $K = \bigcap_{i\in I} R_i$, де R_i – підкільце кільця R для кожного $i \in I$, I – непорожня множина індексів. Якщо $a, b \in K$, то $a, b \in R_i$ для кожного $i \in I$, а тому $a \ominus b, a \odot b \in R_i$, звідки $a \ominus b, a \odot b \in K$. Таким чином, K – підкільце кільця R за твердженням 1.4. □

Нехай A – непорожня підмножина кільця R. Перетин всіх підкілець кільця R, які містять підмножину A, називається *підкільцем, породженим множиною* A, і позначається $\langle A\rangle$. Якщо K – підкільце кільця R і $a \in R\backslash K$, то будемо казати, що підкільце $K' = \langle K \cup \{a\}\rangle$ *отримане приєднанням до* K *елемента* a, і записувати $K' = K[a]$.

Приклад 1.9. Кільце $\mathbb{Z}$ цілих чисел є підкільцем кільця $\mathbb{C}$ комплексних чисел. Кільце $\mathbb{Z}[i]$ співпадає з множиною $\{a + bi \mid a, b \in \mathbb{Z}\}$, що не складно перевірити, враховуючи рівність $i^2 = -1$. Кільце $\mathbb{Z}[i]$ називається *кільцем цілих гаусових чисел.*

Підполем P поля F називається підкільце в F, яке також є полем. У цьому випадку поле F називають *розширенням* поля P. З означення випливає, що одиниця і нуль поля F містяться також у P і є для P одиницею і нулем. Якщо розглянути в F перетин P' усіх підполів, які містять P і деякий елемент $a \in F\backslash P$, то P' є *мінімальним полем, що містить множину* $P \cup \{a\}$. У цьому випадку кажуть, що розширення P' поля P *отримане приєднанням до* P *елемента* a і записують $P' = P(a)$.

Приклад 1.10. Поле $\mathbb{Q}$ раціональних чисел є підполем поля $\mathbb{R}$ дійсних чисел, а $\mathbb{R}$ – розширення поля $\mathbb{Q}$. Поле $\mathbb{Q}(\sqrt{3})$ співпадає з множиною $\{a + b\sqrt{3} \mid a, b \in \mathbb{Q}\}$, що не складно перевірити, враховуючи рівності

$$(\sqrt{3})^2 = 3 \quad \text{і} \quad \frac{1}{a + b\sqrt{3}} = \frac{a}{a^2 - 3b^2} - \frac{b}{a^2 - 3b^2}\sqrt{3}$$

для $a + b\sqrt{3} \neq 0$.

Нехай $(R, \dotplus, \odot)$ – кільце. Для кожних $n \in \mathbb{N}$, $r \in R$ покладемо

$$n \cdot r = \underbrace{r \dotplus r \dotplus \ldots \dotplus r}_{n}.$$

Якщо існує таке натуральне число n, що для кожного $r \in R$ виконується рівність $n \cdot r = \theta$, то найменше m з таких чисел n називається *характеристикою кільця* R, а саме кільце R називається кільцем (*додатньої*) *характеристики* m. Якщо такого натурального n не існує, то кільце R називається *кільцем характеристики нуль*. Через $\operatorname{char} R$ позначимо характеристику кільця R.

Зрозуміло, що $\operatorname{char} R = 1$ тоді і лише тоді, коли $R = \{\theta\}$.

Якщо $(R, \dotplus, \odot)$ – скінченне кільце порядку n, то за теоремою Лагранжа порядок $|r|$ кожного елемента r абелевої групи $(R, \dotplus)$ є дільником n. Зауважимо, що замість позначення r^k, яке використовувалося для запису степеня елемента r в теорії груп, вживаємо позначення $k \cdot r$. Оскільки θ – одиниця абелевої групи $(R, \dotplus)$, то $|r| \cdot r = \theta$ для кожного $r \in R$. Звідси випливає, що характеристика кільця R дорівнює найменшому спільному кратному порядків всіх елементів абелевої групи $(R, \dotplus)$ і не перевищує n. Зокрема, якщо група $(R, \dotplus)$ є циклічною, то характеристика кільця $(R, \dotplus, \odot)$ дорівнює $|R|$.

Приклад 1.11. Нескінченні числові кільця $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ і $(\mathbb{C}, +, \cdot)$ мають характеристику нуль.

Приклад 1.12. Розглянемо циклічну групу $C_2 = \{-1, 1\}$ з операцією множення і її зліченний степінь $(C_2)^\omega$ з операцією покомпонентного множення $\circ$. Тоді $e = (1, 1, \ldots, 1, \ldots)$ – одиниця групи $(C_2)^\omega$. Визначимо бінарну операцію $\odot$ на $(C_2)^\omega$, поклавши $a \odot b = e$ для кожних $a, b \in (C_2)^\omega$. Тоді $((C_2)^\omega, \circ, \odot)$ – кільце. Оскільки порядок кожного неодиничного елемента групи $((C_2)^\omega, \circ)$ дорівнює 2, то характеристика кільця $((C_2)^\omega, \circ, \odot)$ також дорівнює 2. Побудоване кільце є прикладом нескінченного кільця додатньої характеристики.

Твердження 1.6.

Якщо цілісне кільце $(R, \dotplus, \odot)$ має додатню характеристику p, то p – просте число.

Доведення. Нехай e – одиниця кільця $(R, \dotplus, \odot)$. Оскільки цілісне кільце містить ненульовий елемент, то $\operatorname{char} R \geqslant 2$. Якщо p – складене число, то $p = km$, де $k, m \in \{2, \ldots, p-1\}$. Тоді

$$\theta = p \cdot e = (km) \cdot e = (k \cdot e) \odot (m \cdot e).$$

Оскільки кільце R є цілісним, то $k \cdot e = \theta$ або $m \cdot e = \theta$.

Таким чином,

$$k \cdot r = k \cdot (e \odot r) = (k \cdot e) \odot r = \theta \odot r = \theta \quad \text{для всіх } r \in R$$

або

$$m \cdot r = m \cdot (e \odot r) = (m \cdot e) \odot r = \theta \odot r = \theta \quad \text{для всіх } r \in R,$$

що суперечить мінімальності p з означення характеристики. □

Теорема 1.1.

Характеристика скінченного поля $(F, \dotplus, \odot)$ є простим числом.

Доведення. Оскільки поле є цілісним кільцем і містить щонайменше два елементи – нуль θ і одиницю $e \neq \theta$, то враховуючи твердження 1.6, достатньо довести, що скінченне поле має додатню характеристику. Розглянемо в полі F елементи

$$e, \quad 2 \cdot e, \quad 3 \cdot e, \ldots, \quad n \cdot e, \ldots .$$

Оскільки поле F містить скінченну кількість різних елементів, то існують такі числа $k, m \in \mathbb{N}$, $k < m$, що $k \cdot e = m \cdot e$. Тоді $(m-k) \cdot e = \theta$ і $m - k > 0$. Таким чином,

$$(m-k) \cdot r = (m-k) \cdot (e \odot r) = ((m-k) \cdot e) \odot r = \theta \odot r = \theta \quad \text{для всіх } r \in R,$$

а тому F має додатню характеристику. □

Рекомендована література : [**3**, с. 6–19], [**5**, с. 5–20], [**8**, с. 5–22], [**9**, с. 112–124], [**12**, с. 223–239], [**15**, с. 239–245].

Вправи до лекції 1.

1.1. Показати, що множина матриць вигляду

$$\begin{pmatrix} a & b \\ 0 & a \end{pmatrix}, \quad \text{де } a, b \in \mathbb{Z},$$

з операціями додавання і множення матриць утворює комутативне кільце з одиницею. Знайти ідемпотенти та оборотні елементи.

1.2. З'ясувати, чи утворює кільце множина

$$R = \left\{ \frac{a + b\sqrt{5}i}{2} \;\middle|\; a, b - \text{цілі числа однакової парності} \right\}$$

відносно операцій додавання і множення комплексних чисел.

1.3. Знайти всі дільники нуля та ідемпотенти в кільці матриць вигляду

$$\begin{pmatrix} a & b \\ 2b & a \end{pmatrix}, \quad \text{де } a, b \in \mathbb{R}.$$

1.4. Нехай $(G, \dotplus)$ – абелева група. З'ясувати, чи трійка $(G, \dotplus, \odot)$ є кільцем, де $a \odot b = b$ для кожних $a, b \in G$.

1.5. Показати, що множина матриць вигляду

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}, \quad \text{де } a, b, c \in \mathbb{R},$$

є підкільцем кільця $M(2, \mathbb{R})$.

1.6. З'ясувати, чи є підкільцем поля $(\mathbb{R}, +, \cdot)$ множина $K = \{a + b\sqrt[3]{5} \mid a, b \in \mathbb{Q}\}$.

1.7. Довести, що підмножина

$$\mathbb{Q}(\sqrt[3]{2}) = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} \mid a, b, c \in \mathbb{Q}\}$$

є підполем поля дійсних чисел.

1.8. Знайти елемент, обернений до елемента $1 - \sqrt[3]{2} + 2\sqrt[3]{4}$ в полі $\mathbb{Q}(\sqrt[3]{2})$.

1.9. Довести, що кільце $\mathbb{Z}[\sqrt{2}]$ містить нескінченну кількість оборотних елементів.

1.10. Показати, що оборотний елемент кільця з одиницею не може бути дільником нуля.

1.11. Довести, що кожне цілісне кільце містить рівно два ідемпотенти – нуль і одиницю кільця.

1.12. Довести, що для кожної множини X трійка $(\mathcal{P}(X), \triangle, \cap)$, де $\mathcal{P}(X)$ – множина всіх підмножин множини X, є комутативним кільцем з одиницею. Знайти оборотні елементи, дільники нуля та ідемпотенти. Охарактеризувати множини X, для яких $(\mathcal{P}(X), \triangle, \cap)$ – поле.

1.13. Охарактеризувати множини X, для яких $(\mathcal{P}(X), \triangle, \cup)$ – кільце.

1.14. Знайти характеристику кільця $(\mathcal{P}(X), \triangle, \cap)$.

1.15. Нехай u – оборотний елемент кільця $(R, \dotplus, \odot)$ з одиницею. Довести, що елемент $\ominus u$ також є оборотним.

1.16. *Центром* кільця $(R, \dotplus, \odot)$ називається множина

$$Z(R) = \{a \in R \mid a \odot r = r \odot a \ \text{ для всіх } r \in R\}.$$

Довести, що $Z(R)$ – комутативне підкільце кільця R.

1.17. Нехай R – кільце, в якому $e = \theta$. Довести, що $R = \{\theta\}$.

1.18. Нехай $(R, \dotplus, \odot)$ і $(S, \oplus, \circledast)$ – кільця. На декартовому добутку $R \times S$ визначимо операції $\star$ і $\circ$ наступним чином:

$$(r, s) \star (r', s') = (r \dotplus r', s \oplus s'), \quad (r, s) \circ (r', s') = (r \odot r', s \circledast s').$$

Довести, що $(R \times S, \star, \circ)$ – кільце.

1.19. Довести, що $\triangle_R = \{(r, r) \mid r \in R\}$ є підкільцем кільця $R \times R$.

1.20. Кільце $(R, \dotplus, \odot)$ називається *булевим*, якщо $r \odot r = r$ для кожного $r \in R$. Довести, що $r \dotplus r = \theta$ для кожного $r \in R$.

1.21. Довести, що кожне булеве кільце є комутативним.

1.22. Довести, що булеве кільце з одиницею, яке містить більше двох елементів, не є цілісним.

1.23. Довести, що непорожня скінченна підмножина K є підкільцем кільця $(R, \dotplus, \odot)$ тоді і лише тоді, коли $a \dotplus b \in K$ і $a \odot b \in K$ для будь-яких $a, b \in K$.

1.24. Елемент x кільця $(R, \dotplus, \odot)$ називається *нільпотентним*, якщо $x^n = 0$ для деякого $n \in \mathbb{N}$. Довести, що $1 - x$ є оборотним елементом для кожного нільпотентного елемента $x \in R$.

1.25. Нехай $(R, \dotplus, \odot)$ є таким кільцем, що $(a \dotplus a^2) \odot b = b \odot (a \dotplus a^2)$ для всіх $a, b \in R$. Довести, що

а) $x^2 \odot y = y \odot x^2$ для всіх $x, y \in R$;

б) $(R, \dotplus, \odot)$ є комутативним кільцем.

1.26. У множині $\mathbb{H}$ виразів $a + bi + cj + dk$, де $i^2 = j^2 = k^2 = -1$, $ij = k, ji = -k, jk = i, kj = -i, ki = j, ik = -j$, $a, b, c, d \in \mathbb{R}$, введено бінарні операції $\dotplus$ і $\odot$:

$$(a_1 + b_1 i + c_1 j + d_1 k) \dotplus (a_2 + b_2 i + c_2 j + d_2 k) = (a_1 + a_2) + (b_1 + b_2) i + (c_1 + c_2) j + (d_1 + d_2) k$$

$$(a_1 + b_1 i + c_1 j + d_1 k) \odot (a_2 + b_2 i + c_2 j + d_2 k) = (a_1 a_2 - b_1 b_2 - c_1 c_2 - d_1 d_2) +$$

$$+ (a_1 b_2 + b_1 a_2 + d_1 c_2 - c_1 d_2) i + (a_1 c_2 + c_1 a_2 - b_1 d_2 + d_1 b_2) j + (a_1 d_2 + d_1 a_2 + b_1 c_2 - c_1 b_2) k.$$

Довести, що $(\mathbb{H}, \dotplus, \odot)$ – некомутативне тіло. Тіло $\mathbb{H}$ називається тілом *кватерніонів*.

1.27. Нехай $(R, \dotplus, \odot)$ – кільце, X – довільна непорожня множина. Довести, що множина всіх функцій $f : X \to R$ є кільцем відносно операцій

$$(f \oplus g)(x) = f(x) \dotplus g(x), \quad (f \cdot g)(x) = f(x) \odot g(x).$$

1.28. Довести, що в кільці всіх функцій $f : [0, 1] \to \mathbb{R}$ оборотними елементами є такі функції f, що $f(x) \neq 0$ для кожного $x \in [0, 1]$. Показати, що відмінні від нуля кільця необоротні елементи є дільниками нуля.

1.29. З'ясувати, чи є підкільцем кільця всіх функцій $f : [0,1] \to \mathbb{R}$ підмножина всіх функцій $g : [0,1] \to \mathbb{R}$, де $g(x) = 0$ для кожного $x \in \mathbb{Q} \cap [0,1]$.

1.30. Нехай $(\mathbb{R}, +, \cdot)$ – кільце дійсних чисел, $X = [a,b]$ – замкнений інтервал в $\mathbb{R}$. Довести, що множина $C_{[a,b]}$ всіх неперервних функцій $f : X \to \mathbb{R}$ є кільцем з одиницею відносно операцій

$$(f \dotplus g)(x) = f(x) + g(x), \quad (f \cdot g)(x) = f(x)g(x).$$

1.31. Показати, що функція $f : [0,1] \to \mathbb{R}$, $f(x) = x - \frac{1}{2}$ не є ні оборотним елементом, ні дільником нуля в кільці $C_{[0,1]}$ всіх неперервних функцій $f : [0,1] \to \mathbb{R}$. Чи містить дільники нуля кільце $C_{[0,1]}$?

1.32. Нехай $(R, \dotplus, \odot)$ – комутативне кільце простої характеристики p. Довести, що

$$(a \dotplus b)^{p^n} = a^{p^n} \dotplus b^{p^n}, \quad (a \ominus b)^{p^n} = a^{p^n} \ominus b^{p^n}$$

для всіх $a, b \in R$, $n \in \mathbb{N}$.

Лекція 2. Гомоморфізми та ідеали кілець

Нехай $(R, \dotplus, \odot)$ і $(R', \dotplus, \circledast)$ – кільця. Відображення $\varphi : R \to R'$ називається *гомоморфізмом* кільця R в кільце R', якщо

$$\varphi(a \dotplus b) = \varphi(a) \dotplus \varphi(b),$$
$$\varphi(a \odot b) = \varphi(a) \circledast \varphi(b)$$

для будь-яких $a, b \in R$.

Ядром гомоморфізму $\varphi : R \to R'$ називається множина всіх елементів кільця R, які відображаються в нуль θ' кільця R' і позначається $\operatorname{Ker}\varphi$, тобто

$$\operatorname{Ker}\varphi = \{r \in R \mid \varphi(r) = \theta'\}.$$

Образ $\varphi(R) = \{\varphi(r) \mid r \in R\}$ гомоморфізму $\varphi : R \to R'$ позначають через $\operatorname{Im}\varphi$.

З твердження 6.1 розділу I випливає наступне

Твердження 2.1.

Образ $\operatorname{Im}\varphi$ *гомоморфізму* $\varphi : R \to R'$ *є підкільцем кільця* R'.

Гомоморфізм $\varphi : R \to R'$ називається *мономорфізмом*, якщо $\operatorname{Ker}\varphi = \{\theta\}$. Легко перевірити, що гомоморфізм φ є мономорфізмом тоді і лише тоді, коли відображення φ є ін'єкцією.

Якщо $\operatorname{Im}\varphi = R'$, то гомоморфізм $\varphi : R \to R'$ називається *епіморфізмом*. Зрозуміло, що в цьому випадку φ – сюр'єкція.

Гомоморфізм $\varphi : R \to R'$, який є одночасно мономорфізмом і епіморфізмом, називається *ізоморфізмом*, а кільця R і R' – *ізоморфними*. У цьому

випадку пишемо $R \cong R'$. Гомоморфізм $\varphi : R \to R'$ є ізоморфізмом тоді і лише тоді, коли відображення φ є бієкцією. Ізоморфні кільця мають однакову будову, а тому в теорії кілець вони не розрізняються.

Приклад 2.1. Розглянемо кільця $M(2,\mathbb{Q})$ і $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$. Визначимо відображення

$$\varphi : \mathbb{Q}[\sqrt{2}] \to M(2,\mathbb{Q}), \quad \varphi(a + b\sqrt{2}) = \begin{pmatrix} a & b \\ 2b & a \end{pmatrix}.$$

Оскільки

$$\varphi((a_1 + b_1\sqrt{2}) + (a_2 + b_2\sqrt{2})) = \varphi((a_1 + a_2) + (b_1 + b_2)\sqrt{2}) =$$
$$= \begin{pmatrix} a_1 + a_2 & b_1 + b_2 \\ 2(b_1 + b_2) & a_1 + a_2 \end{pmatrix} = \begin{pmatrix} a_1 & b_1 \\ 2b_1 & a_1 \end{pmatrix} + \begin{pmatrix} a_2 & b_2 \\ 2b_2 & a_2 \end{pmatrix} =$$
$$= \varphi(a_1 + b_1\sqrt{2}) + \varphi(a_2 + b_2\sqrt{2})$$

і

$$\varphi((a_1 + b_1\sqrt{2})(a_2 + b_2\sqrt{2})) = \varphi((a_1a_2 + 2b_1b_2) + (a_1b_2 + b_1a_2)\sqrt{2}) =$$
$$= \begin{pmatrix} a_1a_2 + 2b_1b_2 & a_1b_2 + b_1a_2 \\ 2(a_1b_2 + b_1a_2) & a_1a_2 + 2b_1b_2 \end{pmatrix} = \begin{pmatrix} a_1 & b_1 \\ 2b_1 & a_1 \end{pmatrix} \begin{pmatrix} a_2 & b_2 \\ 2b_2 & a_2 \end{pmatrix} =$$
$$= \varphi(a_1 + b_1\sqrt{2})\varphi(a_2 + b_2\sqrt{2}),$$

то φ – гомоморфізм. Очевидно, що φ є мономорфізмом, але не є епіморфізмом кільця $\mathbb{Q}[\sqrt{2}]$ в кільце $M(2,\mathbb{Q})$.

Проте кільця $\mathbb{Q}[\sqrt{2}]$ і $\left\{ \begin{pmatrix} a & b \\ 2b & a \end{pmatrix} \;\middle|\; a, b \in \mathbb{Q} \right\}$ – ізоморфні.

У теорії груп нормальні підгрупи групи відігравали дуже важливу роль. У теорії кілець аналогом нормальних підгруп є спеціальні підкільця кілець, які називаються ідеалами.

Підкільце I кільця $(R, \dotplus, \odot)$ називається *лівим* (*правим*) *ідеалом кільця* R, якщо $R \odot I \subset I$ $(I \odot R \subset I)$, тобто $r \odot a \in I$ $(a \odot r \in I)$ для кожних $r \in R, a \in I$. Підкільце I кільця R називається *ідеалом кільця* R, якщо воно є лівим і правим ідеалом одночасно. Зрозуміло, що в комутативному кільці поняття лівого ідеалу, правого ідеалу та ідеалу співпадають.

Кожне кільце R містить ідеали $\{\theta\}$ і R, які називатимемо *тривіальними ідеалами*. *Власним ідеалом* кільця R називається ідеал $I \neq R$.

Приклад 2.2. Нехай $(\mathbb{Q}, +, \cdot)$ – кільце раціональних чисел. Тоді підмножина $\mathbb{Z}$ є підкільцем кільця Q, але не є ідеалом. Дійсно, $1 \in \mathbb{Z}$, $\frac{1}{2} \in \mathbb{Q}$, але $1 \cdot \frac{1}{2} = \frac{1}{2} \notin \mathbb{Z}$.

Приклад 2.3. Нехай $(R, \dotplus, \odot)$ – кільце, $a \in R$. Підмножина $R \odot a$ є лівим ідеалом кільця R. Дійсно, якщо $r_1 \odot a, r_2 \odot a \in R \odot a$, то $(r_1 \odot a) \ominus (r_2 \odot a) = (r_1 \ominus r_2) \odot a \in R \odot a$, а також $s \odot (r \odot a) = (s \odot r) \odot a \in R \odot a$ для кожних $r \odot a \in R \odot a$, $s \in R$. Аналогічно підмножина $a \odot R$ є правим ідеалом кільця R.

Зауважимо, що елемент $a \in R$ може не належати множинам $R \odot a$, $a \odot R$: у кільці $(2\mathbb{Z}, +, \cdot)$ ідеал $2(2\mathbb{Z}) = 4\mathbb{Z}$ не містить числа 2.

Нехай $(R, \dotplus, \odot)$ – комутативне кільце. Тоді найменшим ідеалом, який містить елемент $a \in R$, є ідеал

$$\langle a \rangle = \{r \odot a \dotplus n \cdot a \mid r \in R, n \in \mathbb{Z}\}.$$

Ідеал $\langle a \rangle$ комутативного кільця R називається *головним ідеалом, породженим елементом* $a \in R$. Якщо R – комутативне кільце з одиницею, то $\langle a \rangle = R \odot a = a \odot R$.

Ідеал I комутативного кільця R називається *головним*, якщо $I = \langle a \rangle$ для деякого $a \in R$. Якщо кожен ідеал цілісного кільця R є головним, то R називається *кільцем головних ідеалів*.

Кожне поле $(F, \dotplus, \odot)$ є кільцем головних ідеалів. Дійсно, якщо ідеал $I \neq \{\theta\} = \langle \theta \rangle$, то ненульовий елемент $r \in I$ має обернений r^{-1} в полі F. Тоді $e = r^{-1} \odot r \in r^{-1} \odot I \subset I$, звідки $r = e \odot r \in I \odot r \subset I$ для кожного $r \in F$. Таким чином, $I = F = \langle e \rangle$.

Якщо I – ідеал кільця $(R, \dotplus, \odot)$, то I є нормальною підгрупою абелевої групи $(R, \dotplus)$. Тому можна розглядати факторгрупу групи $(R, \dotplus)$ за підгрупою I, яка також є абелевою. Елементами R/I є суміжні класи вигляду $\overline{r} = r \dotplus I$. Крім того, $\overline{r} \dotplus \overline{s} = \overline{r \dotplus s}$.

Теорема 2.1.

Нехай I – ідеал кільця $(R, \dotplus, \odot)$. Факторгрупа групи $(R, \dotplus)$ за підгрупою I є кільцем з операцією

$$(r \dotplus I) \odot (s \dotplus I) = r \odot s \dotplus I.$$

Доведення. Розглянемо довільні два елементи $\overline{r} = r \dotplus I$ та $\overline{s} = s \dotplus I$ множини R/I. Покажемо, що добуток $\overline{r} \odot \overline{s}$ не залежить від вибору представників класів $\overline{r}$ і $\overline{s}$. Нехай $r' \in \overline{r}$, $s' \in \overline{s}$, тоді $r' = r \dotplus a$, $s' = s \dotplus b$ для

деяких $a, b \in I$. Тоді

$$r' \odot s' = (r \dotplus a) \odot (s \dotplus b) = r \odot s \dotplus r \odot b \dotplus a \odot s \dotplus a \odot b.$$

Оскільки I – ідеал, то $r \odot b \dotplus a \odot s \dotplus a \odot b \in I$, а тому $r' \odot s' \in r \odot s \dotplus I$. Таким чином, операція $\overline{r} \odot \overline{s} = \overline{r \odot s}$ є коректно визначеною на R/I.

З рівностей

$$(\overline{r} \odot \overline{s}) \odot \overline{t} = \overline{r \odot s} \odot \overline{t} = \overline{(r \odot s) \odot t} = \overline{r \odot (s \odot t)} = \overline{r} \odot \overline{s \odot t} = \overline{r} \odot (\overline{s} \odot \overline{t}),$$

$$\overline{r} \odot (\overline{s} \dotplus \overline{t}) = \overline{r} \odot \overline{s \dotplus t} = \overline{r \odot (s \dotplus t)} = \overline{r \odot s \dotplus r \odot t} = \overline{r \odot s} \dotplus \overline{r \odot t} = \overline{r} \odot \overline{s} \dotplus \overline{r} \odot \overline{t},$$

$$(\overline{r} \dotplus \overline{s}) \odot \overline{t} = \overline{r \dotplus s} \odot \overline{t} = \overline{(r \dotplus s) \odot t} = \overline{r \odot t \dotplus s \odot t} = \overline{r \odot t} \dotplus \overline{s \odot t} = \overline{r} \odot \overline{t} \dotplus \overline{s} \odot \overline{t}$$

випливає, що $(R/I, \dotplus, \odot)$ – кільце. □

Кільце $(R/I, \dotplus, \odot)$ називається *факторкільцем кільця R за ідеалом I*. Елементи кільця R/I називатимемо *класами лишків кільця R за модулем ідеалу I*. Елементи a і b кільця R називатимемо *конгруентними за модулем I* та записувати $a \equiv b (\mathrm{mod}\, I)$, якщо $a \ominus b \in I$, тобто коли вони належать одному класу лишків кільця R за модулем ідеалу I.

Приклад 2.4. Розглянемо у кільці цілих чисел $(\mathbb{Z}, +, \cdot)$ головні ідеали $\langle m \rangle = m\mathbb{Z}$, породжені натуральними числами m. Через $\mathbb{Z}_m$ позначимо факторкільце $\mathbb{Z}/\langle m \rangle$. Елементи кільця $\mathbb{Z}_m$ мають вигляд:

$$\overline{a} = a + \langle m \rangle = a + m\mathbb{Z} = \{a + mt \mid t \in \mathbb{Z}\}.$$

Кільце $\mathbb{Z}_m$ містить m різних елементів: $\overline{0}, \overline{1}, \ldots, \overline{m-1}$.

Приклад 2.5. Таблиці Келі кільця $\mathbb{Z}_6$ мають вигляд:

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{5}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{0}$	$\overline{2}$	$\overline{4}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{2}$	$\overline{0}$	$\overline{4}$	$\overline{2}$
$\overline{5}$	$\overline{0}$	$\overline{5}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Аналізуючи таблицю Келі множення елементів кільця $\mathbb{Z}_6$, бачимо, що $\mathbb{Z}_6^* = \{\overline{1}, \overline{5}\}$ – група дільників одиниці; елементи $\overline{2}, \overline{3}, \overline{4}$ – дільники нуля; а $\overline{0}, \overline{1}, \overline{3}, \overline{4}$ – ідемпотенти.

Теорема 2.2.

Факторкільце $\mathbb{Z}_p$ кільця $\mathbb{Z}$ за головним ідеалом, породженим простим числом p, є полем.

Доведення. Згідно з твердженням 1.3 достатньо показати, що $\mathbb{Z}_p$ є цілісним кільцем. Зрозуміло, що $\mathbb{Z}_p$ – комутативне кільце з одиницею $\overline{1}$. Нехай $\overline{a}, \overline{b} \in \mathbb{Z}_p$ і $\overline{a} \cdot \overline{b} = \overline{0}$. Тоді $\overline{ab} = \overline{0} = p\mathbb{Z}$, а тому ab ділиться на p. Оскільки p – просте число, то a ділиться на p або b ділиться на p, тобто $a \in p\mathbb{Z}$ або $b \in p\mathbb{Z}$. Таким чином, $\overline{a} = \overline{0}$ або $\overline{b} = \overline{0}$, а тому $\mathbb{Z}_p$ – цілісне кільце. □

Нехай $(R, \dotplus, \odot)$ – кільце, I – його ідеал. Розглянемо відображення

$$\pi : R \to R/I, \quad \pi(r) = \overline{r}.$$

Оскільки

$$\pi(r \dotplus s) = \overline{r \dotplus s} = \overline{r} \dotplus \overline{s} = \pi(r) \dotplus \pi(s),$$
$$\pi(r \odot s) = \overline{r \odot s} = \overline{r} \odot \overline{s} = \pi(r) \odot \pi(s)$$

для кожних $r, s \in R$, то відображення π є гомоморфізмом.

Гомоморфізм $\pi : R \to R/I$ називається *природнім* гомоморфізмом кільця R на факторкільце R/I. Очевидно, що $\operatorname{Ker}\pi = I$.

Твердження 2.2.

Нехай $(R, \dotplus, \odot)$ і $(R', \oplus, \circledast)$ – кільця. Ядро $\operatorname{Ker}\varphi$ кожного гомоморфізму $\varphi : R \to R'$ є ідеалом кільця R.

Доведення. З теорії груп відомо, що $\operatorname{Ker}\varphi$ є підгрупою абелевої групи $(R, \dotplus)$ (див. твердження 6.1 розділу I). Нехай $r \in R$, $a \in \operatorname{Ker}\varphi$. Тоді $r \odot a, a \odot r \in \operatorname{Ker}\varphi$. Дійсно,

$$\varphi(r \odot a) = \varphi(r) \circledast \varphi(a) = \varphi(r) \circledast 0' = 0'$$

і

$$\varphi(a \odot r) = \varphi(a) \circledast \varphi(r) = 0' \circledast \varphi(r) = 0'.$$

□

Теорема 2.3 (Основна теорема про гомоморфізми для кілець).

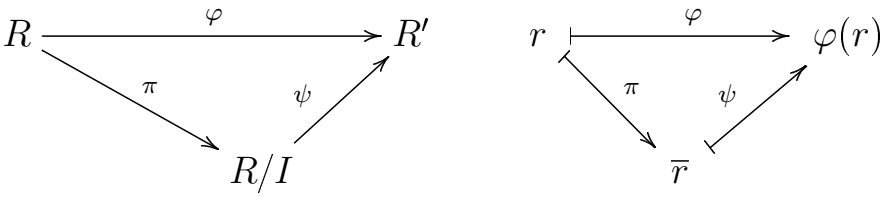
Якщо $\varphi : R \to R'$ – гомоморфізм кілець $(R, \dotplus, \odot)$ і $(R', \oplus, \circledast)$, то факторкільце кільця R за ядром $\operatorname{Ker}\varphi$ ізоморфне образу $\operatorname{Im}\varphi$, тобто $R/\operatorname{Ker}\varphi \cong \operatorname{Im}\varphi$. Зокрема, якщо $\varphi : R \to R'$ – епіморфізм, то $R/\operatorname{Ker}\varphi \cong R'$.

Доведення. Оскільки за твердженням 2.2 ядро $I = \operatorname{Ker}\varphi$ є ідеалом кільця R, то факторкільце R/I існує. Поставимо у відповідність елементу $\overline{r} = r \dotplus I$, де $r \in R$, факторкільця R/I елемент $\varphi(r)$ підкільця $\operatorname{Im}\varphi = \varphi(R)$ кільця R', тобто визначимо відповідність

$$\psi : R/I \to \operatorname{Im}\varphi \subset R', \quad \psi(\overline{r}) = \varphi(r).$$

Оскільки $\overline{r} = \pi(r)$, де $\pi : R \to R/I$ – природній гомоморфізм, то для кожного $r \in R$ маємо $\psi(\pi(r)) = \varphi(r)$, тобто $\psi \circ \pi = \varphi$.

Зобразимо визначену відповідність діаграмами:



Якщо $r' \in \overline{r}$, то $r' = r \dotplus a$ для деякого $a \in I$, а тому

$$\varphi(r') = \varphi(r \dotplus a) = \varphi(r) \oplus \varphi(a) = \varphi(r) \oplus \theta' = \varphi(r).$$

Таким чином, відповідність ψ не залежить від вибору представника класу, а тому кожному елементу $\overline{r} \in R/I$ ставиться у відповідність єдиний елемент $\varphi(r) \in \operatorname{Im}\varphi$, тобто ψ є відображенням кільця R/I в кільце $\operatorname{Im}\varphi$.

Оскільки

$$\psi(\overline{r} \dotplus \overline{s}) = \psi(\overline{r \dotplus s}) = \varphi(r \dotplus s) = \varphi(r) \oplus \varphi(s) = \psi(\overline{r}) \oplus \psi(\overline{s}),$$
$$\psi(\overline{r} \odot \overline{s}) = \psi(\overline{r \odot s}) = \varphi(r \odot s) = \varphi(r) \circledast \varphi(s) = \psi(\overline{r}) \circledast \psi(\overline{s}),$$

то ψ – гомоморфізм.

Якщо $\varphi(r)$ – довільний елемент образу $\operatorname{Im}\varphi$, то $\varphi(r) = \psi(\overline{r})$, тобто ψ – сюр'єкція.

Якщо $\psi(\overline{r}) = \psi(\overline{s})$, то $\varphi(r) = \varphi(s)$, звідки $\varphi(r \ominus s) = \theta'$. Отже, $r \ominus s \in \operatorname{Ker}\varphi = I$, тобто $\overline{r} = \overline{s}$. Таким чином, ψ – ін'єкція, а тому ψ – ізоморфізм кілець R/I і $\operatorname{Im}\varphi$. □

Характеризаційна теорема 2.1.

Поле $(F, \dotplus, \odot)$ є полем простої характеристики p тоді і лише тоді, коли воно містить підполе, ізоморфне полю $\mathbb{Z}_p$.

Доведення. Нехай $(F, \dotplus, \odot)$ – поле характеристики p, e – одиниця поля F. Розглянемо відображення

$$\varphi : \mathbb{Z} \to F, \quad \varphi(n) = n \cdot e = \underbrace{e \dotplus e \dotplus \ldots \dotplus e}_{n}.$$

Відображення φ – гомоморфізм, дійсно

$$\varphi(n+m) = (n+m)\cdot e = n\cdot e \dotplus m\cdot e = \varphi(n)\dotplus\varphi(m),$$

$$\varphi(nm) = (nm)\cdot e = n\cdot e \odot m\cdot e = \varphi(n)\odot\varphi(m).$$

Оскільки p – характеристика поля F, то

$$\operatorname{Ker}\varphi = \{n\in\mathbb{Z} \mid \varphi(n)=\theta\} = \{n\in\mathbb{Z} \mid n\cdot e=\theta\} = p\mathbb{Z} = \langle p\rangle.$$

Тоді $\operatorname{Im}\varphi \cong \mathbb{Z}/\langle p\rangle = \mathbb{Z}_p$ за теоремою 2.3.

Нехай поле $(F, \dotplus, \odot)$ містить підполе P, ізоморфне полю $\mathbb{Z}_p$ при ізоморфізмі $\psi : \mathbb{Z}_p \to P$. Якщо e – одиниця поля F, то $e\in P$, а тому

$$p\cdot e = \underbrace{e\dotplus\ldots\dotplus e}_{p} = \underbrace{\psi(\overline{1})\dotplus\ldots\dotplus\psi(\overline{1})}_{p} = \psi(\underbrace{\overline{1}+\ldots+\overline{1}}_{p}) = \psi(\overline{0}) = \theta.$$

Тоді для кожного $r\in F$ маємо

$$p\cdot r = p\cdot(e\odot r) = (p\cdot e)\odot r = \theta\odot r = \theta.$$

Таким чином, $\operatorname{char} F = p$. □

Наслідок 2.1.

Кожне скінченне поле має порядок p^n, де p – просте число, $n\in\mathbb{N}$.

Доведення. Нехай $(F, \dotplus, \odot)$ – скінченне поле. Згідно з теоремою 1.1 характеристика поля F дорівнює деякому простому числу p. За характеризаційною теоремою 2.1 поле F містить підполе $\mathbb{Z}_p$, а тому F можна розглядати як лінійний простір над полем $\mathbb{Z}_p$. Нехай $(e_1, e_2, \ldots, e_n)$ – база даного лінійного простору. Тоді кожен елемент з F має єдине зображення вигляду

$$a_1\odot e_1 \dotplus a_2\odot e_2 \dotplus \ldots \dotplus a_n\odot e_n, \quad \text{де } a_i\in\mathbb{Z}_p, \quad i\in\{1,\ldots,n\}.$$

Оскільки кожен елемент a_i можна обрати p способами з множини $\mathbb{Z}_p$, то за комбінаторним правилом множення кількість елементів поля F дорівнює $\underbrace{p\cdot p\cdot\ldots\cdot p}_{n} = p^n$. □

Характеризаційна теорема 2.2.

Поле $(F, \dotplus, \odot)$ є полем характеристики нуль тоді і лише тоді, коли воно містить підполе, ізоморфне полю $\mathbb{Q}$ раціональних чисел.

Доведення. Нехай $(F, \dotplus, \odot)$ – поле характеристики нуль, e – одиниця поля F. Знайдемо ядро гомоморфізму $\varphi : \mathbb{Z}\to F, \quad \varphi(n) = n\cdot e$.

$$\operatorname{Ker}\varphi = \{n\in\mathbb{Z} \mid \varphi(n)=\theta\} = \{n\in\mathbb{Z} \mid n\cdot e=\theta\} = \{0\}.$$

Тоді φ є мономорфізмом і поле F містить підкільце $\operatorname{Im}\varphi$, ізоморфне кільцю цілих чисел $\mathbb{Z}$. Оскільки F – поле, то $\frac{a}{b} := ab^{-1} \in F$ для кожних $a, b \in \operatorname{Im}\varphi$, $b \neq 0$. Звідси випливає, що F містить підполе, ізоморфне полю $\mathbb{Q}$ раціональних чисел.

Нехай поле $(F, \dotplus, \odot)$ містить підполе P, ізоморфне полю $\mathbb{Q}$. Якщо e – одиниця поля F, то $e \in P$, а тому з $n \cdot e = \theta$ випливає, що $n = 0$. Таким чином, $\operatorname{char} F = 0$. □

Власний ідеал M кільця $(R, \dotplus, \odot)$ називається *максимальним*, якщо для кожного ідеалу I кільця R з включень $M \subset I \subset R$ випливає, що $I = M$ або $I = R$.

Характеризаційна теорема 2.3.

Нехай $(R, \dotplus, \odot)$ – комутативне кільце з одиницею, M – ідеал кільця R. Ідеал M є максимальним тоді і лише тоді, коли R/M – поле.

Доведення. Нехай M – максимальний ідеал кільця $(R, \dotplus, \odot)$. Оскільки кільце R є комутативним кільцем з одиницею e, то R/M – комутативне кільце з одиницею $\overline{e} = e \dotplus M$. Покажемо, що кожен ненульовий елемент $\overline{a} \in R/M$ має обернений. Оскільки $\overline{a} \neq \overline{\theta} = M$, то $a \notin M$.

Покладемо $I = \{r \odot a \dotplus m \mid r \in R, m \in M\}$ і покажемо, що I – ідеал кільця R. Якщо $r_1 \odot a \dotplus m_1$ та $r_2 \odot a \dotplus m_2$ – елементи множини I, то

$$(r_1 \odot a \dotplus m_1) \ominus (r_2 \odot a \dotplus m_2) = (r_1 \ominus r_2) \odot a \dotplus (m_1 \ominus m_2) \in I.$$

Крім того, $r \odot I \subset I$ для кожного $r \in R$.

Оскільки M – максимальний ідеал і $I \supsetneq M$, то $I = R$. Тоді $e = a \odot b \dotplus m$ для деяких $b \in R$, $m \in M$. Таким чином,

$$\overline{a} \odot \overline{b} = \overline{a \odot b} = a \odot b \dotplus M = e \ominus m \dotplus M = e \dotplus M = \overline{e} \quad \text{і} \quad (\overline{a})^{-1} = \overline{b}.$$

Нехай M – ідеал кільця R і R/M – поле. Оскільки R/M – поле, то воно містить не менше двох елементів: $\overline{\theta} = M$ і $\overline{e} = e \dotplus M$. Звідси випливає, що M – власний ідеал кільця R. Нехай I – ідеал кільця R і $I \supsetneq M$. Оберемо елемент $a \in I \backslash M$. Тоді $\overline{a} \neq M = \overline{\theta}$, а тому $\overline{a} \odot \overline{b} = \overline{e}$ для деякого $\overline{b} \in R/M$. Отже, $a \odot b \dotplus M = e \dotplus M$, тобто $a \odot b \dotplus m_1 = e \dotplus m_2$ для деяких $m_1, m_2 \in M$. Таким чином, $e = a \odot b \dotplus m_1 \ominus m_2 \in I$, а тому $r = e \odot r \in I$ для кожного $r \in R$. Отже, $I = R$. □

Власний ідеал P кільця $(R, \dotplus, \odot)$ називається *простим*, якщо для кожних $a, b \in R$ з належності $a \odot b \in P$ випливає, що $a \in P$ або $b \in P$.

Характеризаційна теорема 2.4.

Нехай $(R, \dotplus, \odot)$ – комутативне кільце з одиницею, P – власний ідеал кільця R. Ідеал P є простим тоді і лише тоді, коли R/P – цілісне кільце.

Доведення. Нехай P – простий ідеал кільця $(R, \dotplus, \odot)$ і $\overline{a} \odot \overline{b} = \overline{\theta}$. Тоді $a \odot b \dotplus P = P$, а отже, $a \odot b \in P$. Якщо $a \notin P$, то $b \in P$ за означенням простого ідеалу. Але тоді $\overline{b} = P = \overline{\theta}$, і R/P – цілісне кільце.

Нехай P – ідеал кільця R, R/P – цілісне кільце і $a \odot b \in P$. Тоді $\overline{a} \odot \overline{b} = \overline{a \odot b} = P = \overline{\theta}$. Звідси випливає, що $\overline{a} = \overline{\theta}$ або $\overline{b} = \overline{\theta}$ за означенням цілісного кільця. Таким чином, $a \in P$ або $b \in P$, а тому P – простий ідеал. □

Оскільки кожне поле є цілісним кільцем, то з характеризаційних теорем 2.3 і 2.4 випливає наступне

Твердження 2.3.

Кожен максимальний ідеал комутативного кільця з одиницею є простим.

Приклад 2.6. Якщо p – просте натуральне число, то за теоремою 2.2 факторкільце $\mathbb{Z}/\langle p \rangle$ є полем. Тоді з характеризаційних теорем 2.3 і 2.4 випливає, що головний ідеал $\langle p \rangle$ є максимальним і простим. Якщо ж m – складене натуральне число, то факторкільце $\mathbb{Z}/\langle m \rangle$ містить дільники нуля, а тому не є цілісним кільцем і, зокрема, полем. У цьому випадку головний ідеал $\langle m \rangle$ не є ні максимальним, ні простим.

Рекомендована література : [**3**, с. 19–36], [**5**, с. 20–36], [**8**, с. 23–39, 45–50], [**9**, с. 124–136], [**12**, с. 239–260], [**15**, с. 246–252].

Вправи до лекції 2.

2.1. З'ясувати, чи є відображення $f : \mathbb{Z} \to \mathbb{Z}$, $f(n) = 3n$, гомоморфізмом кільця $(\mathbb{Z}, +, \cdot)$ в себе.

2.2. Довести, що відображення $\psi : \mathbb{C} \to \mathbb{C}$, $\psi(a + bi) = a - bi$, є автоморфізмом поля $(\mathbb{C}, +, \cdot)$.

2.3. Нехай

$$R = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \;\middle|\; a, b, c \in \mathbb{Z} \right\}.$$

Довести, що відображення

$$\varphi : R \to \mathbb{Z} \times \mathbb{Z}, \quad \varphi \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} = (a, c),$$

є епіморфізмом. Знайти його ядро.

2.4. Довести, що кільця $\mathbb{Q}[\sqrt{3}i]$ та

$$R = \left\{ \begin{pmatrix} a & -3b \\ b & a \end{pmatrix} \;\middle|\; a, b \in \mathbb{Q} \right\}$$

є ізоморфними.

2.5. Нехай φ – відображення кільця $R = \left\{ \begin{pmatrix} a & b \\ b & a \end{pmatrix} \;\middle|\; a, b \in \mathbb{Z} \right\}$ на кільце $\mathbb{Z}$ цілих чисел, причому $\varphi \begin{pmatrix} a & b \\ b & a \end{pmatrix} = a - b$. Довести, що φ – гомоморфізм, і знайти його ядро.

2.6. Довести, що множина матриць вигляду

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix}, \quad \text{де } a, b \in \mathbb{R},$$

з операціями додавання і множення матриць утворює поле, ізоморфне полю комплексних чисел.

2.7. Нехай $C_{[a,b]}$ – кільце неперервних дійснозначних функцій на відрізку $[a, b]$. Довести, що для кожного $\alpha \in [a, b]$ відображення

$$\varphi_\alpha : C_{[a,b]} \to \mathbb{R}, \quad \varphi_\alpha(f) = f(\alpha),$$

є гомоморфізмом.

2.8. Чи є лівим ідеалом або правим ідеалом кільця $M(2, \mathbb{Z})$ підмножина матриць вигляду

$$\begin{pmatrix} m & 0 \\ n & 0 \end{pmatrix}, \quad \text{де } m, n \in \mathbb{Z}?$$

2.9. З'ясувати, які з наступних підмножин є ідеалами кільця $\mathbb{Z} \times \mathbb{Z}$:

а) $\{(a, a) \mid a \in \mathbb{Z}\}$; б) $\{(2a, 0) \mid a \in \mathbb{Z}\}$; в) $\{(a, -a) \mid a \in \mathbb{Z}\}$.

2.10. Знайти всі дільники нуля, оборотні елементи та ідемпотенти в кільці $\mathbb{Z}_{12}$.

2.11. Знайти характеристику кільця $\mathbb{Z}_m$.

2.12. Довести, що підмножина $P = \{\overline{0}, \overline{2}, \overline{4}, \overline{6}, \overline{8}, \overline{10}\}$ є простим ідеалом кільця $\mathbb{Z}_{12}$.

2.13. Знайти всі ідеали кільця $\mathbb{Z}_{15}$. Які з цих ідеалів є простими або максимальними?

2.14. Довести, що $\langle 2 - \sqrt{3} \rangle = \mathbb{Z}[\sqrt{3}]$.

2.15. Нехай I – ідеал кільця R. Довести, що

$$[R : I] = \{x \in R \mid rx \in I \text{ для всіх } r \in R\}$$

є іделом кільця R, який містить ідеал I.

2.16. У кільці $(\mathcal{P}(\mathbb{N}), \triangle, \cap)$ навести приклад ідеалу, який не є головним.

2.17. Охарактеризувати множини X, для яких $(\mathcal{P}(X), \triangle, \cap)$ – кільце головних ідеалів.

2.18. Довести, що в кільці $\mathbb{Z}$ при $m \geqslant 1$ $a \equiv b (\mathrm{mod} \langle m \rangle)$ тоді і лише тоді, коли $a - b$ ділиться на m.

2.19. Побудувати таблиці Келі факторкільця $\mathbb{Z}[i]/\langle 3i \rangle$. Знайти його характеристику.

2.20. Знайти всі дільники нуля, ідемпотенти та оборотні елементи в факторкільці $\mathbb{Z}[\sqrt{3}]/\langle 2 \rangle$.

2.21. Довести, що нетривіальне комутативне кільце з одиницею, яке не має нетривіальних ідеалів, є полем.

2.22. Нехай M – ідеал кільця R. Довести, що якщо всі ненульові елементи множини $R \backslash M$ оборотні, то M – єдиний максимальний ідеал кільця R.

2.23. Нехай R – кільце всіх неперервних функцій $f : [0, 1] \to \mathbb{R}$,

$$I = \{f \in R \mid f(1/3) = f(1/2) = 0\}.$$

Довести, що I – ідеал кільця R, який не є простим.

2.24. Нехай R – комутативне кільце з одиницею, P – простий ідеал в R, який не містить дільників нуля. Довести, що R – цілісне кільце.

2.25. Довести, що в булевому кільці кожен простий ідеал є максимальним.

2.26. Нехай K – підкільце кільця R, I – ідеал кільця R. Довести, що $K \cap I$ – ідеал кільця K.

2.27. Довести, що кожен нетривіальний ідеал кільця $\mathbb{Z}[i]$ містить натуральне число.

2.28. У кільці цілих чисел навести приклад простого ідеалу, який не є максимальним.

2.29. Довести, що в кільці $\mathbb{Z} \times \mathbb{Z}$ максимальні ідеали мають вигляд $p\mathbb{Z} \times \mathbb{Z}$ або $\mathbb{Z} \times p\mathbb{Z}$ для деякого простого p.

2.30. Нехай $\varphi : R \to S$ – епіморфізм кілець. Довести, що образ центру кільця R міститься в центрі кільця S.

2.31. Довести, що з точністю до ізоморфізму існує два кільця простого порядку p.

Лекція 3. Евклідові кільця. Подільність

Нехай $(R, \dotplus, \odot)$ – цілісне кільце. Довільна функція

$$\delta : R \to \mathbb{N} \cup \{0\}, \text{ для якої } \delta(\theta) = 0,$$

називається *нормою цілісного кільця* R. Якщо $\delta(a) > 0$ при $a \neq \theta$, то кажемо, що норма δ є *додатньою*.

Цілісне кільце $(R, \dotplus, \odot)$ називається *евклідовим*, якщо існує така норма $\delta : R \to \mathbb{N} \cup \{0\}$, що для будь-яких $a, b \in R$, $b \neq \theta$, існують елементи $q, r \in R$, для яких

$$a = b \odot q \dotplus r, \quad \text{де } r = \theta \text{ або } \delta(r) < \delta(b).$$

Елемент q називається *неповною часткою*, а елемент r – *остачею від ділення* a *на* b.

Приклад 3.1. Кожне поле $(F, \dotplus, \odot)$ є евклідовим кільцем з нормою $\delta(a) = 0$ для кожного $a \in F$. Дійсно, якщо $a, b \in F$, $b \neq \theta$, то поклавши $q = b^{-1} \odot a$, отримаємо, що $a = bq + \theta$.

Твердження 3.1.

Кільце $(\mathbb{Z}, +, \cdot)$ *є евклідовим.*

Доведення. Визначимо додатню норму δ на кільці $(\mathbb{Z}, +, \cdot)$, поклавши $\delta(a) = |a|$.

Нехай $a, b \in \mathbb{Z}$, $b \neq 0$.

Розглянемо спершу випадок $b > 0$. Оскільки напіввідкриті інтервали

$$[nb, (n+1)b), \ n \in \mathbb{Z}$$

утворюють розбиття дійсної прямої $\mathbb{R}$, то a належить одному з них, скажімо

$$a \in [qb, (q+1)b) \text{ для деякого } q \in \mathbb{Z}.$$

Покладемо $r = a - bq$. Тоді $a = bq + r$ і $0 \leqslant r < b = |b| = \delta(b)$.

Якщо $b<0$, то $-b>0$, а тому за попередніми міркуваннями

$$a=(-b)q+r,\quad \text{де } q\in\mathbb{Z}\ \text{ і }\ 0\leqslant r<|-b|=|b|.$$

Звідси $a=b(-q)+r$, де $-q\in\mathbb{Z}$ і $0\leqslant r<|b|=\delta(b)$. □

Твердження 3.2.

Кільце цілих гаусових чисел $(\mathbb{Z}[i],+,\cdot)$ є евклідовим.

Доведення. Нагадаємо, що кільце цілих гаусових чисел

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

є підкільцем поля $\mathbb{C}$ комплексних чисел.

Спершу покажемо, що $(\mathbb{Z}[i],+,\cdot)$ – цілісне кільце. Дійсно, дане кільце є комутативним з одиницею $1=1+0i$.

Якщо $(a+bi)(c+di)=0+0i$, то $|(a+bi)(c+di)|=0$, звідки

$$(a^2+b^2)(c^2+d^2)=|a+bi|^2|c+di|^2=|(a+bi)(c+di)|^2=0.$$

Тоді $a^2+b^2=0$ або $c^2+d^2=0$, а отже, $a=b=0$ або $c=d=0$. Таким чином, $a+bi=0+0i$ або $c+di=0+0i$, а тому $\mathbb{Z}[i]$ – цілісне кільце.

Визначимо додатню норму δ на кільці $(\mathbb{Z}[i],+,\cdot)$, поклавши

$$\delta(m+ni)=|m+ni|^2=m^2+n^2.$$

Зауважимо, що для кожних $\alpha,\beta\in\mathbb{C}$:

$$\delta(\alpha\beta)=|\alpha\beta|^2=(|\alpha||\beta|)^2=|\alpha|^2|\beta|^2=\delta(\alpha)\delta(\beta).$$

Нехай $a,b\in\mathbb{Z}[i]$, $b\neq 0$. Тоді $\frac{a}{b}\in\mathbb{C}$, а тому $\frac{a}{b}=\alpha+\beta i$, де $\alpha,\beta\in\mathbb{Q}$. Оберемо "найближчі" до α і β такі цілі числа k і s, що $\alpha=k+\rho$, $\beta=s+\mu$, $|\rho|\leqslant\frac{1}{2}$, $|\mu|\leqslant\frac{1}{2}$. Тоді

$$a=b((k+\rho)+(s+\mu)i)=b(k+si)+b(\rho+\mu i).$$

Покладемо $q=k+si\in\mathbb{Z}[i]$, $r=a-bq=b(\rho+\mu i)$. Оскільки $a,b,q\in\mathbb{Z}[i]$, то $r\in\mathbb{Z}[i]$.

Тоді $a=bq+r$, де $r=0+0i$, якщо $\rho=\mu=0$, і

$$\delta(r)=\delta(b(\rho+\mu i))=\delta(b)\delta(\rho+\mu i)=\delta(b)(\rho^2+\mu^2)\leqslant\delta(b)\Big(\frac{1}{4}+\frac{1}{4}\Big)=\frac{1}{2}\delta(b)<\delta(b)$$

Таким чином, $\mathbb{Z}[i]$ – евклідове кільце. □

Твердження 3.3.

Кожне евклідове кільце є кільцем головних ідеалів.

Доведення. Нехай I – ідеал евклідового кільця $(R, \dotplus, \odot)$. Якщо $I = \{\theta\}$, то $I = \langle\theta\rangle$ – головний ідеал. В іншому випадку оберемо в ідеалі I ненульовий елемент d з найменшою нормою $\delta(d)$. Оскільки $d \in I$, то $\langle d\rangle \subset I$.

Нехай a – довільний елемент ідеалу I. Оскільки R – евклідове кільце, то існують такі елементи $q, r \in R$, що $a = d \odot q \dotplus r$, де $r = \theta$ або $\delta(r) < \delta(d)$. Оскільки $a, d \in I$, то $r = a \ominus d \odot q \in I$. З мінімальності норми елемента d в ідеалі I випливає, що $r = \theta$, а тому $a = d \odot q \in d \odot R = \langle d\rangle$. Таким чином, $I = \langle d\rangle$ – головний ідеал. □

Надалі $(R, \dotplus, \odot)$ – комутативне кільце з одиницею e. Кажемо, що елемент $a \in R$ *ділиться на елемент* $b \in R$ *в кільці* R або елемент $b \in R$ *є дільником елемента* $a \in R$, якщо $a = b \odot c$ для деякого $c \in R$. Якщо елемент a ділиться на елемент b, то $a = b \odot c \in b \odot R = \langle b\rangle$, звідки $\langle a\rangle \subset \langle b\rangle$. Зрозуміло, що і навпаки: якщо $\langle a\rangle \subset \langle b\rangle$, то a ділиться на b. Дільники одиниці – це оборотні елементи кільця R. Нагадаємо, що оборотні елементи утворюють підгрупу напівгрупи $(R, \odot)$, яку ми домовилися позначати R^*.

Твердження 3.4.

Нехай $(R, \dotplus, \odot)$ – комутативне кільце з одиницею. Елемент $r \in R$ є оборотним тоді і лише тоді, коли $\langle r\rangle = R$.

Доведення. Якщо елемент r є оборотним, то $e = r^{-1} \odot r \in R \odot r = \langle r\rangle$. Але тоді $s = s \odot e \in s \odot \langle r\rangle \subset \langle r\rangle$ для кожного $s \in R$, а отже, $\langle r\rangle = R$.

Нехай $R = \langle r\rangle = r \odot R$. Оскільки R – комутативне кільце з одиницею e, то $e = r \odot a = a \odot r$ для деякого $a \in R$. Таким чином, r – оборотний елемент. □

Елементи a і b кільця R називаються *асоційованими*, якщо існує такий оборотний елемент $f \in R^*$, що $a = b \odot f$. Оскільки відношення ρ

$$a \rho b \quad \Leftrightarrow \quad a \text{ і } b \text{ – асоційовані елементи}$$

є відношенням еквівалентності, то кільце R розбивається на класи асоційованих елементів. Позначимо через $[r]$ клас асоційованих з елементом $r \in R$ елементів.

Твердження 3.5.

Нехай $(R, \dotplus, \odot)$ – цілісне кільце. Елементи a і b є асоційованими тоді і лише тоді, коли $\langle a\rangle = \langle b\rangle$.

Доведення. Якщо елементи a і b асоційовані, то що $a = b \odot f$ для деякого $f \in R^*$, звідки $b = a \odot f^{-1}$. Оскільки a ділиться на b і b ділиться на a, то $\langle a \rangle \subset \langle b \rangle$ і $\langle b \rangle \subset \langle a \rangle$, звідки $\langle a \rangle = \langle b \rangle$.

Нехай $\langle a \rangle = \langle b \rangle$. Якщо $a = \theta$, то $\langle b \rangle = \langle a \rangle = \{\theta\}$, звідки $b = \theta$. Тоді $b \odot e = \theta \odot e = \theta = a$, а тому елементи a і b – асоційовані. Нехай $a \neq \theta$. З рівності $\langle a \rangle = \langle b \rangle$ випливає, що a є дільником b і b є дільником a, звідки $a = b \odot c$ і $b = a \odot d$ для деяких $c, d \in R$. Тоді $a = b \odot c = a \odot d \odot c$, звідки $a \odot (e \ominus d \odot c) = \theta$. Оскільки кільце R цілісне і $a \neq \theta$, то $d \odot c = e$. Таким чином, елементи c і d – оборотні, а тому a і b – асоційовані. □

Приклад 3.2. У кільці $(\mathbb{Z}, +, \cdot)$ з рівності $ab = 1$ випливає, що $a = b = 1$ або $a = b = -1$. Отже, кільце $\mathbb{Z}$ містить два оборотні елементи, а тому $\mathbb{Z}^* = \{-1, 1\}$. Таким чином, для кожного $a \in \mathbb{Z}$ клас $[a]$ асоційованих з a елементів дорівнює $\{-a, a\}$.

Приклад 3.3. Нехай $a + bi$ – оборотний елемент у кільці $(\mathbb{Z}[i], +, \cdot)$. Тоді з рівності $(a + bi)(c + di) = 1 + 0i$ випливає, що $|(a + bi)(c + di)| = (a^2 + b^2)(c^2 + d^2) = 1$. Звідки $a^2 + b^2 = 1$, і $(a, b) \in \{(1, 0), (-1, 0), (0, 1), (0, -1)\}$. Таким чином, $\mathbb{Z}[i]^* = \{1, -1, i, -i\}$. Для кожного $a+bi \in \mathbb{Z}[i]$ клас $[a+bi]$ асоційованих з $a + bi$ елементів дорівнює $(a + bi)\mathbb{Z}[i]^* = \{a + bi, -a - bi, -b + ai, b - ai\}$.

З твердження 3.5 випливає, що кожному головному ідеалу $\langle r \rangle$ цілісного кільця R взаємно однозначно відповідає клас $[r]$ асоційованих з r елементів.

Елемент $c \in R$ називається *простим елементом кільця* R, якщо він не є оборотним елементом і не має інших дільників, крім асоційованих з ним елементів і оборотних елементів.

Приклад 3.4. Ціле число 2 є простим елементом кільця $(\mathbb{Z}, +, \cdot)$, але не є простим елементом кільця $(\mathbb{Z}[i], +, \cdot)$, оскільки $2 = (1 + i)(1 - i)$.

Теорема 3.1.

Нехай $(R, \dotplus, \odot)$ – кільце головних ідеалів. Елемент $c \in R$ є простим елементом кільця R тоді і лише тоді, коли факторкільце $R/\langle c \rangle$ є полем.

Доведення. Якщо c – оборотний елемент, то $\langle c \rangle = R$ за твердженням 3.4 і факторкільце $R/\langle c \rangle$ має порядок 1, а тому не може бути полем.

Якщо c – не оборотний і не простий елемент, то c має деякий дільник $a \in R$, який не є асоційованим з c і не є оборотним елементом. Нехай $c = a \odot b$, де $b \in R$. Тоді $\langle c \rangle \subset \langle a \rangle$ і $\langle c \rangle \neq \langle a \rangle$ за твердженням 3.5. Оскільки a не є оборотним, то $\langle a \rangle \subsetneq R$ за твердженням 3.4. Таким чином, ідеал $\langle c \rangle$ не є максимальним, а тому факторкільце $R/\langle c \rangle$ не є полем за характеризаційною теоремою 2.3.

Нехай c – простий елемент кільця R. Оскільки c не є оборотним, то $\langle c \rangle \neq R$. Нехай $I \supset \langle c \rangle$ – ідеал кільця R. Оскільки R – кільце головних ідеалів, то $I = \langle a \rangle$ для деякого $a \in R$. Отже, $c \in \langle a \rangle$ і a – дільник елемента c. Тому a – або оборотний елемент, або асоційований з c елемент. Таким чином, $I = R$ або $I = \langle c \rangle$ за твердженнями 3.4 і 3.5. Звідси випливає, що $\langle c \rangle$ – максимальний ідеал, а тому факторкільце $R/\langle c \rangle$ є полем за характеризаційною теоремою 2.3. □

Приклад 3.5. Простими елементами кільця $(\mathbb{Z}, +, \cdot)$ є числа p і $-p$, де p – просте натуральне число. Оскільки $(\mathbb{Z}, +, \cdot)$ є кільцем головних ідеалів за твердженнями 3.1 і 3.3, то факторкільце $\mathbb{Z}/I$ є полем тоді і лише тоді, коли $I = \langle p \rangle = \langle -p \rangle$, де p – просте число.

Приклад 3.6. Число 3 є простим елементом кільця цілих гаусових чисел $\mathbb{Z}[i]$. Дійсно, якщо $3 = (a + bi)(c + di)$, де $a, b, c, d \in \mathbb{Z}$, то $(a^2 + b^2)(c^2 + d^2) = 9$, звідки $a^2 + b^2 = 1$, $a^2 + b^2 = 3$ або $a^2 + b^2 = 9$. Оскільки рівняння $a^2 + b^2 = 3$ не має розв'язків у цілих числах, то $(a, b) \in \{(1, 0), (-1, 0), (0, 1), (0, -1)\}$ або $(a, b) \in \{(3, 0), (-3, 0), (0, 3), (0, -3)\}$, а тому $a + bi$ – оборотний елемент або асоційований з 3 елемент.

Оскільки $\mathbb{Z}[i]$ – кільце головних ідеалів за твердженнями 3.2 і 3.3, то за теоремою 3.1 факторкільце

$$\mathbb{Z}[i]/\langle 3 \rangle = \{\overline{0}, \overline{1}, \overline{2}, \overline{i}, \overline{1+i}, \overline{2+i}, \overline{2i}, \overline{1+2i}, \overline{2+2i}\}$$

є полем порядку 9. Згідно з твердженнями 2.3 і 2.3 ідеал $\langle 3 \rangle$ є максимальним і простим в кільці $\mathbb{Z}[i]$.

Ненульовий елемент d кільця R називається *найбільшим спільним дільником елементів* $a, b \in R$ (одночасно не рівних нулю кільця), якщо виконуються наступні умови:

1) d є дільником елементів a і b;
2) d ділиться на будь-який інший спільний дільник елементів a і b.

Через (a, b) позначимо найбільший спільний дільник елементів a і b. Якщо (a, b) є оборотним елементом кільця R, то елементи a і b називаються *взаємно простими*.

Нехай $(R, \dotplus, \odot)$ – кільце головних ідеалів. Два ненульових елемента a і b породжують ідеал $\langle a, b\rangle = \{r \odot a \dotplus s \odot b \mid r, s \in R\}$, який також є головним, тобто породжується деяким елементом $d \in R$. Отже, $d = r \odot a \dotplus s \odot b$ для деяких $r, s \in R$, звідки випливає, що d ділиться на кожен спільний дільник елементів a і b. Оскільки $\langle a\rangle \subset \langle d\rangle$ і $\langle b\rangle \subset \langle d\rangle$, то d є дільником елементів a і b, а тому є їх найбільшим спільним дільником. Якщо d' – асоційований з d елемент, то $\langle d'\rangle = \langle d\rangle$ за твердженням 3.5, а тому d' також є найбільшим спільним дільником елементів a і b. Таким чином, в кільці головних ідеалів будь-які два (одночасно не рівні нулю кільця) елементи мають найбільший спільний дільник, який визначається з точністю до асоційованих елементів (можна вважати, що найбільший спільний дільник є класом асоційованих елементів).

Зауваження 3.1.

Більш формально в кільці головних ідеалів слід би було розглядати поняття найбільшого спільного дільника головних ідеалів або класів асоційованості. Проте такий підхід є складнішим для розуміння і засвоєння.

Твердження 3.6.

Нехай $(R, \dotplus, \odot)$ – кільце головних ідеалів. Якщо елементи $a, b, q, r \in R$ зв'язані співвідношенням $a = b \odot q \dotplus r$, то $(a, b) = (b, r)$ з точністю до асоційованості.

Доведення. З рівності $a = b \odot q \dotplus r$ випливає, що кожен спільний дільник елементів b і r є дільником елемента a. І навпаки, з рівності $r = a \ominus b \odot q$ випливає, що кожен спільний дільник елементів a і b є дільником елемента r. Таким чином, множина спільних дільників елементів a і b співпадає з множиною спільних дільників елементів b і r. А тому $(a, b) = (b, r)$ з точністю до асоційованості. □

Для знаходження найбільшого спільного дільника двох елементів евклідового кільця $(R, \dotplus, \odot)$ використовують простий метод, названий *алгоритмом Евкліда.*

Нехай $a, b \in R$, $b \neq \theta$. Тоді

$$\begin{aligned}
&a = b \odot q_0 \dotplus r_1 && \delta(r_1) < \delta(b)\\
&b = r_1 \odot q_1 \dotplus r_2 && \delta(r_2) < \delta(r_1)\\
&r_1 = r_2 \odot q_2 \dotplus r_3 && \delta(r_3) < \delta(r_2)\\
&\ldots\ldots\ldots\ldots && \ldots\ldots\ldots\\
&r_{n-2} = r_{n-1} \odot q_{n-1} \dotplus r_n && \delta(r_n) < \delta(r_{n-1})\\
&r_{n-1} = r_n \odot q_n
\end{aligned}$$

Тут r_n – остання ненульова остача. Така остача r_n існує, оскільки послідовність $\delta(b) > \delta(r_1) > \ldots > \delta(r_n)$ є спадною послідовністю невід'ємних цілих чисел, а тому не може бути нескінченною.

Тоді за твердженням 3.6 маємо:

$$(a, b) = (b, r_1) = (r_1, r_2) = \ldots = (r_{n-1}, r_n) = (r_n, \theta) = r_n.$$

Таким чином, найбільший спільний дільник двох елементів евклідового кільця дорівнює останній ненульовій остачі алгоритму Евкліда для цих елементів.

Приклад 3.7. Використовуючи алгоритм Евкліда, знайдемо найбільший спільний дільник елементів $6 - 17i$ та $18 + i$ евклідового кільця $\mathbb{Z}[i]$ цілих гаусових чисел. Для відшукання неповних часток і остач в процесі ділення використовуватимемо метод, описаний при доведенні твердження 3.2:

$$\frac{6 - 17i}{18 + i} = \frac{(6 - 17i)(18 - i)}{(18 + i)(18 - i)} = \frac{91 - 312i}{325} = -i + \left(\frac{91}{325} + \frac{13}{325}i\right)$$

Нагадаємо, що в останній рівності числа $\alpha = \frac{91}{325}$ і $\beta = -\frac{312}{325}$ записані у вигляді

$$\alpha = k + \rho,\ \beta = s + \mu, \quad \text{де } k, s \in \mathbb{Z}, \quad |\rho| \leqslant \frac{1}{2},\ |\mu| \leqslant \frac{1}{2}.$$

Тоді

$6 - 17i = (18 + i)(-i) + (5 + i)$, причому $\delta(5 + i) = 26 < 325 = \delta(18 + i)$.

Отже, $5 + i$ – перша остача.

$$\frac{18 + i}{5 + i} = \frac{(18 + i)(5 - i)}{(5 + i)(5 - i)} = \frac{91 - 13i}{26} = \frac{7 - i}{2} = 3 + \left(\frac{1}{2} - \frac{1}{2}i\right)$$

Звідси

$18 + i = (5 + i) \cdot 3 + (3 - 2i)$, причому $\delta(3 - 2i) = 13 < 26 = \delta(5 + i)$.

Таким чином, $3 - 2i$ – друга остача.

$$\frac{5+i}{3-2i} = \frac{(5+i)(3+2i)}{(3-2i)(3+2i)} = \frac{13+13i}{13} = 1+i.$$

Отже,

$$5+i = (3-2i)(1+i) + (0+0i),$$

а тому третя остача дорівнює нулю кільця $\mathbb{Z}[i]$.

Згідно з алгоритмом Евкліда, найбільший спільний дільник елементів $6-17i$ та $18+i$ з точністю до асоційованості дорівнює останній ненульовій остачі $3-2i$.

Більш формально, $([6-17i],[18+i]) = [3-2i]$ або $(\langle 6-17i\rangle, \langle 18+i\rangle) = \langle 3-2i\rangle$.

Ненульовий елемент d кільця R називається *найменшим спільним кратним елементів* $a, b \in R\backslash\{0\}$, якщо виконуються наступні умови:

1) d ділиться на елементи a і b;
2) d є дільником всіх елементів, які діляться на a і b.

Аналогічно, як і найбільший спільний дільник, у кільці головних ідеалів найменше спільне кратне визначається з точністю до асоційованих елементів. **Рекомендована література** : [**3**, с. 41–60], [**5**, с. 36–48], [**8**, с. 40–44, 51–58], [**9**, с. 159–177], [**12**, с. 270–294].

Вправи до лекції 3.

3.1. Показати, що елементи $2+3\sqrt{7}$ і $1-2\sqrt{7}$ є дільниками елемента $40+\sqrt{7}$ в кільці $\mathbb{Z}[\sqrt{7}]$.

3.2. З'ясувати, чи ділиться елемент $3+4i$ на $2-5i$ у кільці $\mathbb{Z}[i]$ цілих гаусових чисел.

3.3. Довести, що елемент $12-3\sqrt[3]{2}-7\sqrt[3]{4}$ ділиться на $1+2\sqrt[3]{2}-3\sqrt[3]{4}$ в кільці

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

3.4. Довести, що кільце $\mathbb{Z}[\sqrt{3}]$ містить нескінченну кількість дільників одиниці.

3.5. З'ясувати, чи елементи $5+\sqrt{3}$ та $7-3\sqrt{3}$ є асоційованими в кільці $\mathbb{Z}[\sqrt{3}]$.

3.6. Знайти клас асоційованих з $3-7i$ елементів у кільці $\mathbb{Z}[i]$.

3.7. Показати, що кожен клас $[r]$ асоційованих елементів з елементом $r \neq 0$ у кільці $\mathbb{Z}[\sqrt{2}]$ містить нескінченну кількість елементів.

3.8. Показати, що число 13 є простим елементом кільця $\mathbb{Z}$, але не є простим елементом його розширення $\mathbb{Z}[\sqrt{3}]$.

3.9. Довести, що прості натуральні числа 5, 13, 17 не є простими цілими гаусовими числами.

3.10. Показати, що ціле гаусове число є простим, якщо його норма є простим натуральним числом.

3.11. Довести, що норма простого цілого гаусового числа є або простим натуральним числом, або квадратом простого натурального числа.

3.12. Довести, що усі прості натуральні числа, які при діленні на 4 дають остачу 3, є простими цілими гаусовими числами.

3.13. Показати, що числа 2 та $1+\sqrt{3}i$ є простими елементами кільця $\mathbb{Z}[\sqrt{3}i]$.

3.14. Знайти всі прості елементи кільця $(\mathcal{P}(X), \triangle, \cap)$, якщо $X = \{1, 2, 3, 4\}$.

3.15. Знайти потужність множини простих елементів кільця $(\mathcal{P}(X), \triangle, \cap)$ для кожної множини X.

3.16. З'ясувати, чи в кільці всіх функцій $f : [0, 1] \to \mathbb{R}$ функції $f_1(x) = x$ і $f_2(x) = 1 - x$ є асоційованими елементами.

3.17. Показати, що головні ідеали $\langle 7\rangle$ та $\langle 3 + 2i\rangle$ є простими в кільці $\mathbb{Z}[i]$.

3.18. З'ясувати, чи головні ідеали $\langle 5\rangle$ та $\langle 7\rangle$ є максимальними в кільці $\mathbb{Z}[\sqrt{2}i]$.

3.19. Довести, що факторкільце $\mathbb{Z}[i]/\langle 3i\rangle$ є полем, і побудувати таблиці Келі додавання і множення його елементів.

3.20. З'ясувати, чи факторкільце $\mathbb{Z}[\sqrt{7}]/\langle 40 + \sqrt{7}\rangle$ є цілісним.

3.21. Використовуючи алгоритм Евкліда, знайти найбільший спільний дільник цілих чисел -396 та 780.

3.22. Знайти найбільший спільний дільник цілих гаусових чисел $10 - 37i$ та $14 - 5i$.

3.23. Довести, що кільця $\mathbb{Z}[\sqrt{d}]$, де $d \in \{2, 3\}$, є евклідовими з нормою $\delta(a + b\sqrt{d}) = |a^2 - db^2|$, $a, b \in \mathbb{Z}$.

3.24. Знайти найбільший спільний дільник чисел $22+5\sqrt{2}$ і $2-4\sqrt{2}$ у кільці $\mathbb{Z}[\sqrt{2}]$.

3.25. Довести, що кільце $\mathbb{Z}[\sqrt{2}i]$ є евклідовими з нормою $\delta(a + b\sqrt{2}i) = a^2 + 2b^2$, $a, b \in \mathbb{Z}$.

3.26. З'ясувати, чи елементи $3 + 4\sqrt{2}i$ та $5 - 7\sqrt{2}i$ є взаємно простими елементами кільця $\mathbb{Z}[\sqrt{2}i]$.

3.27. Знайти твірний елемент головного ідеалу $\langle 47 - 13i, 53 + 56i\rangle$ кільця цілих гаусових чисел.

3.28. Показати, що число 4 неоднозначно розкладається в добуток простих елементів у кільці $\mathbb{Z}[\sqrt{3}i]$.

3.29. Подати елемент $1+7i \in \mathbb{Z}[i]$ у вигляді добутку простих елементів.

3.30. Довести, що факторкільце $\mathbb{Z}[i]/I$ є скінченним для кожного ненульового ідеалу I кільця $\mathbb{Z}[i]$.

Лекція 4. Конгруенції в кільці цілих чисел. Теорема Ейлера

У цій лекції детально вивчаються будова і властивості факторкілець кільця цілих чисел $(\mathbb{Z}, +, \cdot)$. За твердженнями 3.1 і 3.3 кільце цілих чисел є кільцем головних ідеалів, тобто кожен ідеал I є головним в тому сенсі, що $I = \langle m \rangle = m\mathbb{Z}$ для деякого $m \in \mathbb{Z}$. Якщо $m \in \{0, 1\}$, то $\langle 0 \rangle = \{0\}$ і $\langle 1 \rangle = \mathbb{Z}$ – тривіальні ідеали кільця $\mathbb{Z}$. Крім того, $\langle -m \rangle = \langle m \rangle$. Тому надалі розглядатимемо факторкільця $\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z}$ для натуральних $m \geqslant 2$. Нагадаємо, що елементи кільця $\mathbb{Z}_m$ називаються класами лишків за модулем ідеалу $\langle m \rangle$ і позначаються $[a]_m = a + m\mathbb{Z} = \{a + mt \mid t \in \mathbb{Z}\}$. Для спрощення клас $[a]_m$ називатимемо *класом лишків за модулем m, породженим елементом a*. Елементи a і b одного класу лишків називаємо *конгруентними на модулем m* і записуємо $a \equiv b (\mathrm{mod}\, m)$. Таким чином, $a \equiv b (\mathrm{mod}\, m)$ тоді і лише тоді, коли $b \in [a]_m = \{a + mt \mid t \in \mathbb{Z}\}$, тобто $b = a + mt$ для деякого $t \in \mathbb{Z}$. Остання рівність рівносильна тому, що $b - a$ ділиться на m в кільці $\mathbb{Z}$.

Зауважимо також, що з теореми 2.2 випливає, що кільце $\mathbb{Z}_m$ є полем тоді і лише тоді, коли m – просте число.

Згідно з теоремою про ділення з остачею кожному цілому числу a відповідає певна остача r від ділення a на m :

$$a = mq + r, \quad 0 \leqslant r < m.$$

Характеризаційна теорема 4.1.

Для того, щоб цілі числа a і b були конгруентні за модулем m, необхідно і достатньо, щоб при діленні на m вони давали однакові остачі.

Доведення. Нехай $a \equiv b (\mathrm{mod}\, m)$ і числу a відповідає остача r від ділення a на m: $a = mq + r, \quad 0 \leqslant r < m$. Тоді $b = a + mt$ для деякого $t \in \mathbb{Z}$, звідки $b = mq + r + mt = m(q + t) + r$.

Якщо $a = mq + r$ і $b = ms + r$, то $b - a = m(s - q)$, тобто $b - a$ ділиться на m, а тому $a \equiv b (\mathrm{mod}\, m)$. □

Оскільки при діленні цілих чисел на деяке натуральне число m можна одержати тільки m різних остач (а саме: $0, 1, 2, ..., m - 1$), то кільце цілих

чисел розбивається на m класів лишків за модулем m:

$$\mathbb{Z} = [0]_m \sqcup [1]_m \sqcup \ldots \sqcup [m-1]_m.$$

Твердження 4.1.

Кожен клас лишків $[a]_m$ за модулем m розбивається на $d \in \mathbb{N}$ класів лишків за модулем dm, а саме:

$$[a]_{dm}, [a+m]_{dm}, [a+2m]_{dm}, \ldots, [a+(d-1)m]_{dm}.$$

Доведення. У класі $[a]_m$ містяться всі числа x, конгруентні з a за модулем m, тобто числа $x = a + mt$, де $t \in \mathbb{Z}$. Цей клас містить, зокрема, d таких чисел:

$$x_0 = a, x_1 = a + m, x_2 = a + 2m, ..., x_{d-1} = a + (d-1)m.$$

За модулем dm ці числа не конгруентні, бо різниця будь-яких з них не ділиться на dm, оскільки модуль різниці є меншим за число dm. Отже, за модулем dm числа x_i, $i \in \{0, \ldots, d-1\}$, належать різним класам.

З іншого боку, будь-яке число $x = a + mt$ з класу $[a]_m$ конгруентне за модулем dm з одним із чисел x_i, $i \in \{0, \ldots, d-1\}$. Дійсно, нехай число t при діленні на d дає остачу p: $t = ds + p$, $0 \leqslant p < d$. Тоді числа $x = a + mt \in [a]_m$ і $x_p = a + mp$ конгруентні за модулем dm:

$$x - x_p = (a + mt) - (a + mp) = m(t - p) = m(ds) = (md)s.$$

Таким чином, отримано розбиття:

$$[a]_m = [a]_{dm} \sqcup [a+m]_{dm} \sqcup [a+2m]_{dm} \sqcup \ldots \sqcup [a+(d-1)m]_{dm}.$$

□

Розглянемо деякі властивості конгруенцій. Якщо $a \equiv b (\mathrm{mod}\, m)$ і $c \equiv d (\mathrm{mod}\, m)$, то $[a]_m = [b]_m$ і $[c]_m = [d]_m$. Тоді за означенням суми, різниці і добутку класів лишків маємо, що $[a+c]_m = [b+d]_m$, $[a-c]_m = [b-d]_m$ і $[ac]_m = [bd]_m$, звідки $a+c \equiv b+d (\mathrm{mod}\, m)$, $a-c \equiv b-d (\mathrm{mod}\, m)$ і $ac \equiv bd (\mathrm{mod}\, m)$. Таким чином, конгруенції за одним модулем можна почленно додавати, віднімати, множити, а отже, і підносити до натурального степеня. Звідси випливає, що якщо у виразі $\sum a_{i_1}^{n_1} a_{i_2}^{n_2} \cdot \ldots \cdot a_{i_s}^{n_s}$ всі числа $a_{i_1}, a_{i_2}, \ldots, a_{i_s}$ замінити на конгруентні їм за модулем m числа $b_{i_1}, b_{i_2}, \ldots, b_{i_s}$ відповідно, то новий вираз $\sum b_{i_1}^{n_1} b_{i_2}^{n_2} \cdot \ldots \cdot b_{i_s}^{n_s}$ буде конгруентний за модулем m до заданого.

Твердження 4.2.

Для конгруенцій мають місце наступні властивості:

1) *обидві частини конгруенції можна ділити на їх спільний дільник, взаємно простий з модулем;*
2) *обидві частини конгруенції і модуль можна множити на те саме натуральне число;*
3) *обидві частини конгруенції і модуль можна ділити на їх спільний натуральний дільник;*
4) *якщо конгруенція має місце за кількома модулями, то вона має місце і за модулем, який дорівнює НСК цих модулів;*
5) *якщо одна частина конгруенції і модуль діляться на деяке ціле число, то й друга частина конгруенції ділиться на це число;*
6) *якщо* $a \equiv b(\mathrm{mod}\, m)$, *то* $(a, m) = (b, m)$.

Доведення.

1) Нехай $a \equiv b(\mathrm{mod}\, m)$, d – дільник чисел a і b, $(d, m) = 1$. Тоді $a = a_1 d$, $b = b_1 d$. Оскільки $a - b = d(a_1 - b_1)$ ділиться на m і $(d, m) = 1$, то $a_1 - b_1$ ділиться на m, а отже, $a_1 \equiv b_1(\mathrm{mod}\, m)$.
2) Якщо $a \equiv b(\mathrm{mod}\, m)$, то $a = b + mt$ для деякого $t \in \mathbb{Z}$. Тоді $ak = bk + (mk)t$, звідки $ak = bk(\mathrm{mod}\, mk)$.
3) Якщо $ak = bk(\mathrm{mod}\, mk)$, то $ak = bk + (mk)t$ для деякого $t \in \mathbb{Z}$. Тоді $a = b + mt$, звідки $a \equiv b(\mathrm{mod}\, m)$.
4) Нехай
$$\begin{aligned} a &\equiv b(\mathrm{mod}\, m_1) \\ a &\equiv b(\mathrm{mod}\, m_2) \\ &\cdots\cdots\cdots\cdots \\ a &\equiv b(\mathrm{mod}\, m_k) \end{aligned} .$$
Тоді $a - b$ ділиться на $m_1, m_2, \ldots, m_k$, звідки $a - b$ ділиться і на $m = [m_1, m_2, \ldots, m_k]$ – НСК чисел $m_1, m_2, \ldots, m_k$. Отже, $a - b = mt$, тобто $a \equiv b(\mathrm{mod}\, m)$.
5) Нехай $a \equiv b(\mathrm{mod}\, m)$. Тоді $a = b + mt$ для деякого $t \in \mathbb{Z}$. Якщо числа b і m діляться на d, тобто $b = db_1$ і $m = dm_1$, то $a = b + mt = d(b_1 + m_1 t)$ ділиться на d. Аналогічно для $b = a - mt$.
6) З попереднього пункту випливає, що множина спільних дільників чисел a і m збігається з множиною спільних дільників чисел b і m, а тому збігаються також і найбільші спільні дільники, тобто $(a, m) = (b, m)$.

□

Оскільки конгруентні числа при діленні на натуральне число m дають однакові остачі, то конгруенції можна використовувати для виведення ознак подільності.

Твердження 4.3.

Натуральне число n ділиться на 11 тоді і лише тоді, коли різниця суми його цифр, які стоять на парних позиціях, і суми цифр, які стоять на непарних позиціях, ділиться на 11.

Доведення. Запишемо число n у вигляді:

$$n = a_0 + a_1 10 + a_2 10^2 + \ldots + a_m 10^m,$$

де a_i – цифри числа n, $a_i \in \{0, 1, \ldots, 9\}$.

Оскільки $10^k \equiv (-1)^k (\mathrm{mod}\, 11)$, то

$$n = a_0 + a_1 10 + a_2 10^2 + \ldots, + a_m 10^m \equiv a_0 - a_1 + a_2 - a_3 + \ldots + (-1)^m a_m (\mathrm{mod}\, 11) \equiv$$
$$\equiv (a_0 + a_2 + \ldots) - (a_1 + a_3 + \ldots) (\mathrm{mod}\, 11).$$

Звідси і випливає твердження. □

У кожному класі $[a]_m$ лишків за модулем m можна обрати *найменший невід'ємний лишок (ННЛ)* – остачу від ділення a на m, і *абсолютно найменший лишок (АНЛ)* – лишок, модуль якого менший від модулів усіх лишків класу $[a]_m$.

Приклад 4.1. У класі $[3]_7 = \{\ldots, -25, -18, -11, -4, 3, 10, 17, 24, \ldots\}$ найменшим невід'ємним лишком є число 3, і абсолютно найменшим лишком – також число 3, оскільки його модуль менший від модулів всіх інших лишків даного класу. У цьому випадку ННЛ і АНЛ збігаються. А у класі $[6]_7 = \{\ldots, -22, -15, -8, -1, 6, 13, 20, \ldots\}$ число 6 є ННЛ, проте АНЛ є число -1.

Множина чисел, утворена з m лишків, узятих по одному з кожного класу лишків за модулем m, називається *повною системою лишків (ПСЛ) за модулем m*.

Приклад 4.2. При $m = 5$ ПСЛ є такі множини чисел:

$P_1 = \{0, 1, 2, 3, 4\}$ – складається з найменших невід'ємних лишків усіх класів;

$P_2 = \{-2, -1, 0, 1, 2\}$ – складається з абсолютно найменших лишків;

$P_3 = \{-7, -1, 25, 1, 12\}$ – складається з довільних п'яти чисел, взятих по одному з кожного класу.

За твердженням 4.2(6) усі числа класу $[a]_m$ мають однаковий НСД з модулем m: якщо $a \equiv b (\mathrm{mod}\, m)$, то $(a, m) = (b, m)$. Тому коректним є наступне означення.

Найбільшим спільним дільником класу $[a]_m$ називається найбільший спільний дільник чисел a і m. Якщо $(a, m) = 1$, то клас $[a]_m$ називається *взаємно простим з модулем.*

Множина лишків, узятих по одному з кожного класу лишків, взаємно простого з модулем m, називається *зведеною системою лишків (ЗСЛ) за модулем* m.

Приклад 4.3. Множини $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ і $\{1, 3, 7, 9\}$ є ПСЛ та ЗСЛ за модулем 10 відповідно. Класи $[1]_{10}, [3]_{10}, [7]_{10}, [9]_{10}$ є взаємно простими з модулем.

Нагадаємо, що функцією Ейлера $\varphi : \mathbb{N} \to \mathbb{N}$ називається функція, значення $\varphi(m)$ якої дорівнює кількості натуральних чисел, які не перевищують m і взаємно прості з m. Таким чином, кількість чисел, які утворюють ЗСЛ за модулем m, дорівнює $\varphi(m)$.

Твердження 4.4.

Якщо множина P є ПСЛ (ЗСЛ) за модулем m і $a \in \mathbb{Z}$, $(a, m) = 1$, то множина $aP = \{ax \mid x \in P\}$ також є ПСЛ (ЗСЛ) за модулем m.

Доведення. Нехай $x, x' \in P$. Якщо $ax \equiv ax' (\mathrm{mod}\, m)$ і $(a, m) = 1$, то $x \equiv x' (\mathrm{mod}\, m)$, за твердженням 4.2(1). Отже, елементи множини aP попарно неконгруентні за модулем m. Таким чином, якщо P – ПСЛ за модулем m, то aP також є ПСЛ за модулем m.

Нехай P – ЗСЛ за модулем m, $x \in P$. Тоді $(x, m) = 1$. Оскільки $(a, m) = 1$, то $(ax, m) = 1$. Звідси випливає, що aP також є ЗСЛ за модулем m. □

Зауваження 4.1.

Якщо число x є лишком ПСЛ (ЗСЛ) за модулем m, тобто належить класу $[x]_m$, то добуток ax хоч і належатиме до ПСЛ (ЗСЛ) за модулем m, але може міститися в іншому класі. Тільки в тому випадку, коли $a = km + 1$, добуток $ax = (km + 1)x = kmx + x \equiv x (\mathrm{mod}\, m)$ належить тому ж класу $[x]_m$.

Приклад 4.4. Оберемо з класів лишків $[1]_8, [3]_8, [5]_8, [7]_8$ ЗСЛ $\{1, 3, 5, 7\}$ за модулем 8. Якщо $a = 11$, то добутки ax є числами $11, 33, 55, 77$, які належать відповідно класам $[3]_8, [1]_8, [7]_8, [5]_8$.

Теорема 4.1 (Теорема Ейлера).

Якщо m – натуральне число і $m \geqslant 2$, $(a, m) = 1$, то

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

Доведення. Нехай числа

$$x_1, x_2, \ldots, x_{\varphi(m)}$$

утворюють ЗСЛ найменших невід'ємних лишків (ННЛ) за модулем m. Тоді за твердженням 4.4 при $(a, m) = 1$ числа $ax_1, ax_2, \ldots, ax_{\varphi(m)}$ теж утворюють ЗСЛ за модулем m. Ці числа належать деяким класам, взаємно простим з модулем m. Їх можна замінити ННЛ

$$\bar{x}_1, \bar{x}_2, ..., \bar{x}_{\varphi(m)}$$

з тих же класів, до яких вони належать. Вважаючи, що

$$\begin{gathered} ax_1 \equiv \bar{x}_1 (\mathrm{mod}\ m) \\ ax_2 \equiv \bar{x}_2 (\mathrm{mod}\ m) \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots, \\ ax_{\varphi(m)} \equiv \bar{x}_{\varphi(m)} (\mathrm{mod}\ m) \end{gathered}$$

перемножимо ці $\varphi(m)$ конгруенцій. Отримаємо

$$a^{\varphi(m)} x_1 x_2 \cdot \ldots \cdot x_{\varphi(m)} \equiv \bar{x}_1 \bar{x}_2 \cdot \ldots \cdot \bar{x}_{\varphi(m)} (\mathrm{mod}\, m).$$

Оскільки $\{x_1, x_2, \ldots, x_{\varphi(m)}\} = \{\bar{x}_1, \bar{x}_2, \ldots, \bar{x}_{\varphi(m)}\}$, то, поділивши на добуток елементів цієї множини обидві частини конгруенції за твердженням 4.2(1), одержимо:

$$a^{\varphi(m)} \equiv 1 (\mathrm{mod}\, m),$$

що й треба було довести. □

Теорема 4.2 (Мала теорема Ферма).

Якщо число p – просте і $(a,p)=1$, то

$$a^{p-1}\equiv 1(\mathrm{mod}\, p).$$

Доведення. Мала теорема Ферма є наслідком теореми Ейлера: оскільки $\varphi(p)=p-1$, то $a^{p-1}\equiv 1(\mathrm{mod}\, p)$. □

Наслідок 4.1.

Якщо p – просте число, то для будь-якого цілого числа a має місце конгруенція

$$a^{p}\equiv a(\mathrm{mod}\, p).$$

Доведення. Якщо $(a,p)=1$, то $a^{p-1}\equiv 1(\mathrm{mod}\, p)$ за теоремою 4.2. Помноживши обидві частини конгруенції на a, одержимо $a^{p}\equiv a(\mathrm{mod}\ p)$. Якщо $(a,p)\neq 1$, то $(a,p)=p$, бо p – просте число. Тоді a ділиться на p, а отже, і

$$a^{p}-a=a(a^{p-1}-1)$$

також ділиться на p. Таким чином,

$$a^{p}-a\equiv 0(\mathrm{mod}\, p)\ \text{ або }\ a^{p}\equiv a(\mathrm{mod}\, p),$$

що й треба було довести. □

Приклад 4.5. Знайдемо остачу від ділення числа 42^{50} на 17.

Оскільки 17 – просте число і $(42,17)=1$, то за малою теоремою Ферма

$$42^{16}\equiv 1(\mathrm{mod}\, 17).$$

Піднесемо до куба обидві частини конгруенції:

$$42^{48}\equiv 1(\mathrm{mod}\, 17).$$

Крім того,

$$42\equiv 8(\mathrm{mod}\, 17),\quad a\quad 42^{2}\equiv 8^{2}(\mathrm{mod}\, 17)\equiv 64(\mathrm{mod}\, 17)\equiv 13(\mathrm{mod}\, 17).$$

Далі отримуємо:

$$42^{50}\equiv 42^{48}42^{2}(\mathrm{mod}\, 17)\equiv 13(\mathrm{mod}\, 17).$$

Отже, остача дорівнює 13.

Рекомендована література : [**1**, с. 115–146], [**3**, с. 37–41], [**5**, с. 48–55], [**6**, с. 72–86], [**9**, с. 194–206], [**15**, с. 253–262].

Вправи до лекції 4.

4.1. Чи конгруентні числа 89, 199 і 335 з числом 27 за модулем 11?

4.2. З'ясувати, чи мають місце конгруенції $5^{2016} \equiv 2016 (\mathrm{mod}\ 25)$, $7^{119} \equiv 3 (\mathrm{mod}\ 243)$.

4.3. Охарактеризувати конгруенціями цілі числа n, якщо:

а) n – непарне число;

б) n має вигляд $8k-3$, $k \in \mathbb{Z}$.

4.4. Показати, що для кожного непарного натурального числа n має місце конгруенція $n^2 \equiv 1 (\mathrm{mod}\ 8)$.

4.5. Довести, що задані рівняння не мають розв'язків у натуральних числах:

а) $26^x + 36^y = 59^z$;

б) $2^x + 5^y = 19^z$.

4.6. Нехай $a \equiv 3 (\mathrm{mod}\ 4)$. Показати, що $\frac{a+1}{4}$ є цілим числом.

4.7. Знайти дві останні цифри чисел 2^{999} і 605^{2016}.

4.8. Знайти остачу від ділення

а) $2^{100} + 5^{200}$ на 30;

б) $13^{1054} - 38 \cdot 16^{285} + 37^{17}$ на 15.

4.9. Знайти останню цифру числа $(\ldots(((7^7)^7)^7)^{\cdots})^7$ – піднесення до степеня виконується 2016 раз.

4.10. Вивести ознаки подільності на 2, 3, 5 і 9.

4.11. Знайти остачу від ділення 111111110888888895 на 9.

4.12. Знайти остачу від ділення 121311510848583895 на 11.

4.13. Вивести ознаки подільності на 7 і 13.

4.14. Нехай натуральне число a має зображення $d_k d_{k-1} \ldots d_2 d_1 d_0$ у десятковій системі числення. Через $S(a)$ позначимо суму 3-цифрових блоків числа a, розбиваючи число a на блоки справа наліво. Наприклад, якщо $a = 5987654321$, то $a = \underline{005}\ \underline{987}\ \underline{654}\ \underline{321}$ і $S(a) = 5 + 987 + 654 + 321 + 1967$. Довести, що натуральне число a ділиться на 37 тоді і лише тоді, коли $S(a)$ ділиться на 37. Що зміниться, якщо 37 замінити на 27?

4.15. З'ясувати, чи є ПСЛ за модулем m множина:

а) $\{33, -20, 24, 54, -21, -30, 37, -17\}$, якщо $m = 8$;

б) $\{17, -23, 28, -50, -40, -31\}$, якщо $m = 6$.

4.16. З'ясувати, чи є ЗСЛ за модулем m множина:

а) $\{19, -1, 33, -19\}$, якщо $m = 8$;
б) $\{13, -13, 29, -29\}$, якщо $m = 10$.

4.17. Побудувати ПСЛ за модулем 7, яка складається з:

а) від'ємних чисел;
б) непарних чисел;
в) парних чисел;
г) простих чисел.

4.18. Нехай P – ПСЛ за модулем 10. Показати, що $S = \{x^5 \mid x \in P\}$ також є ПСЛ за модулем 10.

4.19. Показати, що $P_a = \{6a - 1, 6a + 1\}$ є ЗСЛ за модулем 6 для кожного $a \in \mathbb{Z}$.

4.20. Користуючись теоремою Ейлера, знайти остачу від ділення:

а) 7^{2016} на 12; б) 109^{345} на 14; в) 353^{160} на 75.

4.21. Для кожного $a \in \mathbb{Z}$ знайти остачу від ділення a^{2016} на 27.

4.22. Для кожного простого числа p знайти остачу від ділення 2^{p-2} на p.

4.23. Показати, що $a^{297} - a^3$ ділиться на 343 для кожного $a \in \mathbb{Z}$.

4.24. Довести, що коли $79a + 10b + c \equiv 0 (\mathrm{mod}\ 21)$, то $a - 2b + 4c \equiv 0 (\mathrm{mod}\ 21)$, де $a, b, c \in \mathbb{Z}$.

4.25. Довести, що $1^{2k+1} + 2^{2k+1} + 3^{2k+1} + \ldots + (p-1)^{2k+1} \equiv 0 (\mathrm{mod}\ p)$, де p – просте число, $p > 2$.

4.26. Показати, що для кожного непарного натурального числа n має місце конгруенція

$$1 + 2 + \ldots + (n-1) \equiv 0 (\mathrm{mod}\ n).$$

Чи це твердження вірне для парного натурального числа?

4.27. Методом математичної індукції довести, що для кожного $n \in \mathbb{N}$ має місце конгруенція $5^n \equiv 1 + 4n (\mathrm{mod}\ 16)$.

4.28. З'ясувати, для яких натуральних чисел n має місце конгруенція

$$1^2 + 2^2 + \ldots + (n-1)^2 \equiv 0 (\mathrm{mod}\ n).$$

4.29. Для натурального числа n через $D(n)$ позначимо останню цифру десяткового запису числа n. Наприклад, $D(4) = 4$, $D(35) = 5$ та $D(237) = 7$. Знайти всі елементи, які належать множині

$$S = \{D(19^m + \sum_{k=1}^{m} k!) \mid m \in \mathbb{N}\}.$$

4.30. Нехай a_0 та a_1 – цілі числа. Для натурального числа $n \geqslant 2$ визначимо $a_n = a_{n-1} + a_{n-2}$. Довести, що з конгруенцій $a_2 \equiv 6a_0 (\mathrm{mod}\ 19)$ та $a_3 \equiv 6a_1 (\mathrm{mod}\ 19)$ випливає конгруенція $a_{n+2} \equiv 6a_n (\mathrm{mod}\ 19)$ для кожного цілого невід'ємного числа n. Скільки пар (a_0, a_1) цілих чисел, для яких $0 \leqslant a_0 < 19$ та $0 \leqslant a_1 < 19$, задовольняють умови $a_2 \equiv 6a_0 (\mathrm{mod}\ 19)$ та $a_3 \equiv 6a_1 (\mathrm{mod}\ 19)$?

Лекція 5. Конгруенції з одним невідомим. Теорема Вільсона

Конгруенціями з одним невідомим за модулем m називаються конгруенції виду

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0 \equiv 0 (\mathrm{mod}\, m),$$

де в лівій частині є многочлен з цілими коефіцієнтами.

Якщо a_n не ділиться на модуль m, то ціле невід'ємне число n називають *степенем конгруенції*. У випадку, коли a_n ділиться на m, старший член $a_n x^n \equiv 0 (\mathrm{mod}\, m)$ і його можна відкинути.

Якщо $a \equiv b (\mathrm{mod}\, m)$, то

$$a_n b^n + a_{n-1} b^{n-1} + \ldots + a_1 b + a_0 \equiv a_n a^n + a_{n-1} a^{n-1} + \ldots + a_1 a + a_0 (\mathrm{mod}\, m),$$

а тому коректним є наступне означення.

Розв'язком конгруенції $f(x) \equiv 0 (\mathrm{mod}\, m)$ називається клас лишків за модулем m, кожне число якого задовольняє цю конгруенцію. Оскільки класів лишків за даним модулем m є m, то конгруенція може мати лише скінченну кількість розв'язків, або й не мати їх зовсім.

Приклад 5.1. Конгруенція $4x \equiv 1 (\mathrm{mod}\, 10)$ не має розв'язків, бо із неї випливає рівність $4x = 1 + 10t$, яка є неможливою, оскільки для довільних $x, t \in \mathbb{Z}$ ліва частина – парне число, а права – непарне.

Щоб знайти розв'язки конгруенції, досить замість невідомого x підставити в конгруенцію числа з різних класів лишків за модулем m. Для цього можна перебрати ПСЛ із найменших невід'ємних лишків, а ще краще – ПСЛ із абсолютно найменших лишків.

Приклад 5.2. Розв'яжемо конгруенцію $x^3 + 14x + 1 \equiv 0 (\mathrm{mod}\, 7)$. Знайдемо ПСЛ із найменших невід'ємних лишків за модулем 7: $\{0, 1, 2, 3, 4, 5, 6\}$. Підставимо лишки у конгруенцію. Бачимо, що числа 3, 5 і 6 задовольняють конгруенцію. Отже, розв'язками є класи лишків: $[3]_7$, $[5]_7$ і $[6]_7$.

Конгруенції називаються *рівносильними*, якщо множини їх розв'язків збігаються.

Конгруенції розв'язують за допомогою побудови більш простих конгруенцій, рівносильних заданим. З означення і властивостей конгруенцій випливає, що наступні дії не змінюють множину розв'язків конгруенції:

1) додавання до обох частин конгруенції будь-якого многочлена $g(x)$ з цілими коефіцієнтами;
2) додавання до однієї частини конгруенції многочлена з коефіцієнтами, кратними модулю;
3) заміна кожного коефіцієнта конгруентним йому за даним модулем числом;
4) множення обох частин конгруенції на число, взаємно просте з модулем;
5) ділення обох частин конгруенції на їх цілий дільник, взаємно простий з модулем;
6) множення обох частин конгруенції і модуля на те саме натуральне число;
7) ділення обох частин конгруенції і модуля на їх спільний натуральний дільник.

Приклад 5.3. Конгруенцію $14x^3 + 10x^2 - 21x - 3 \equiv 0(\mathrm{mod}\,7)$ можна спростити так:

1) відкинемо многочлен $14x^3 - 21x$, бо його коефіцієнти кратні модулю: $10x^2 - 3 \equiv 0(\mathrm{mod}\,7)$;

2) замінимо число 10 конгруентним йому за модулем 7 числом 3: $3x^2 - 3 \equiv 0(\mathrm{mod}\,7)$;

3) Оскільки $(3, 7) = 1$, то поділимо на 3 ліву і праву частини конгруенції: $x^2 - 1 \equiv 0(\mathrm{mod}\,7)$.

Конгруенція $x^2-1 \equiv 0(\mathrm{mod}\,7)$ рівносильна конгруенції $(x-1)(x+1) \equiv 0(\mathrm{mod}\,7)$, з якої випливає, що добуток $(x-1)(x+1)$ ділиться на просте число 7. Тоді $(x-1)$ або $(x+1)$ ділиться на 7, тобто $x-1 \equiv 0(\mathrm{mod}\,7)$ або $x+1 \equiv 0(\mathrm{mod}\,7)$. Таким чином, розв'язками конгруенції є класи лишків $[1]_7$ і $[6]_7$.

Конгруенції I-го степеня мають вигляд

$$a_1x + a_0 \equiv 0(\mathrm{mod}\,m).$$

Якщо перенести вільний член в праву частину конгруенції і змінити позначення коефіцієнтів, то дістанемо

$$ax \equiv b(\mathrm{mod}\,m).$$

Твердження 5.1.

Якщо $(a, m) = 1$, то конгруенція $ax \equiv b(\mathrm{mod}\,m)$ має єдиний розв'язок.

Доведення. Якщо P – ПСЛ за модулем m, то aP також є ПСЛ за модулем m згідно з твердженням 4.4. Тоді існує єдиний елемент $ai \in aP$, який конгруентний з b за модулем m, для деякого $i \in P$. Отже, клас лишків $[i]_m$ і є єдиним розв'язком конгруенції. □

Твердження 5.2.

Якщо $(a, m) = d > 1$ і b не ділиться на d, то конгруенція $ax \equiv b (\mathrm{mod}\, m)$ не має розв'язків.

Доведення. Припустимо супротивне. Нехай $ax_0 \equiv b (\mathrm{mod}\ m)$ для деякого $x_0 \in \mathbb{Z}$. Тоді $ax_0 = b + mt$, де $t \in \mathbb{Z}$. Але така рівність неможлива, якщо a і m діляться на d, а b не ділиться на d. Отже, припущення невірне. □

Твердження 5.3.

Якщо $(a, m) = d > 1$ і b ділиться на d, то конгруенція $ax \equiv b (\mathrm{mod}\, m)$ має d розв'язків.

Доведення. Нехай $a = a_1 d, \quad b = b_1 d, \quad m = m_1 d$. Поділимо обидві частини конгруенції і модуль на d і дістанемо рівносильну їй конгруенцію $a_1 x \equiv b_1 (\mathrm{mod}\ m_1)$. Оскільки $(a_1, m_1) = 1$, то ця конгруенція за твердженням 5.1 має єдиний розв'язок – клас лишків $[i]_{m_1}$. Однак за твердженням 4.1 цей клас лишків розбивається на d класів лишків за модулем $dm_1 = m$. Таким чином, конгруенція $ax \equiv b (\mathrm{mod}\, m)$ має d розв'язків:

$$[i]_m, [i + m_1]_m, \ldots, [i + (d-1)m_1]_m.$$

□

Конгруенції I-го степеня можна розв'язувати різними методами. Розглянемо найбільш вживані з них.

1) Підстановка в конгруенцію чисел ПСЛ. Цей спосіб використовується при невеликих модулях. При великих модулях підстановку лишків ПСЛ проводять на заключному етапі побудови рівносильних конгруенцій.
2) Зведення конгруенцій I-го степеня до рівносильної їй конгруенції з коефіцієнтом при x, рівним одиниці, використовуючи дії 1) – 7), описані вище.

Приклад 5.4. Конгруенція $11x \equiv 7(\mathrm{mod}\ 17)$ має єдиний розв'язок, бо $(11, 17) = 1$. Віднявши від правої частини число $51 = 3 \cdot 17$, отримаємо конгруенцію $11x \equiv -44(\mathrm{mod}\ 17)$. Оскільки $(11, 17) = 1$, то поділимо обидві частини конгруенції на 11: $x \equiv -4(\mathrm{mod}\ 17)$. Отже, розв'язком конгруенції є клас $[-4]_{17} = [13]_{17}$.

3) Метод Ейлера. Нехай задано конгруенцію $ax \equiv b(\mathrm{mod}\ m)$, $(a, m) = 1$. За твердженням 5.1 ця конгруенція має один розв'язок. За теоремою Ейлера $a^{\varphi(m)} \equiv 1(\mathrm{mod}\ m)$. Тому $a^{\varphi(m)}b \equiv b(\mathrm{mod}\ m)$, звідки $a(a^{\varphi(m)-1}b) \equiv b(\mathrm{mod}\ m)$. Таким чином, $x \equiv a^{\varphi(m)-1} \cdot b(\mathrm{mod}\ m)$.

Приклад 5.5. Розв'язати конгруенцію $10x \equiv 6(\mathrm{mod}\ 16)$.

Оскільки $(10, 16) = 2$ і 6 ділиться на 2, то конгруенція має два розв'язки. Поділимо обидві частини конгруенції і модуль на 2. Для розв'язування отриманої конгруенції $5x \equiv 3(\mathrm{mod}\ 8)$ можна застосувати метод Ейлера. Оскільки $\varphi(8) = 4$, то $x \equiv 5^{\varphi(8)-1} \cdot 3(\mathrm{mod}\ 8) = 5^3 \cdot 3(\mathrm{mod}\ 8) = 125 \cdot 3(\mathrm{mod}\ 8) \equiv 5 \cdot 3(\mathrm{mod}\ 8) = 15(\mathrm{mod}\ 8) \equiv 7(\mathrm{mod}\ 8)$. Оскільки $[7]_8 = [7]_{16} \sqcup [15]_{16}$, то класи $[7]_{16}$ і $[15]_{16}$ є розв'язками конгруенції $10x \equiv 6(\mathrm{mod}\ 16)$.

4) Розв'язування конгруенцій за допомогою ланцюгових дробів.

Нехай задано конгруенцію $ax \equiv b(\mathrm{mod}\ m)$, де $(a, m) = 1$. Розкладемо $\frac{m}{a}$ в ланцюговий дріб. Якщо $\frac{P_{n-1}}{Q_{n-1}}$ і $\frac{P_n}{Q_n} = \frac{m}{a}$ є передостанній і останній підхідні дроби, то

$$P_nQ_{n-1} - P_{n-1}Q_n = (-1)^{n-1}, \text{звідки} \quad mQ_{n-1} - P_{n-1}a = (-1)^{n-1}.$$

Враховуючи, що перший член кратний модулю m, отримаємо:

$$-P_{n-1}a \equiv (-1)^{n-1}(\mathrm{mod}\ m) \quad \text{або} \quad a(-1)^nP_{n-1} \equiv 1(\mathrm{mod}\ m).$$

Таким чином,

$$a(-1)^nP_{n-1}b \equiv b(\mathrm{mod}\ m), \text{ звідки } x \equiv (-1)^nP_{n-1}b(\mathrm{mod}\ m).$$

Приклад 5.6. Розв'язати конгруенцію

$$123x \equiv 15(\mathrm{mod}\ 435).$$

Оскільки $(a, m) = (123, 435) = 3$ і 15 ділиться 3, то конгруенція має три розв'язки. Поділимо обидві частини конгруенції і модуль на 3. Одержимо рівносильну конгруенцію:

$$41x \equiv 5(\mathrm{mod}\ 145).$$

Розкладемо число $\frac{m}{a} = \frac{145}{41}$ в ланцюговий дріб за алгоритмом Евкліда: $145 = 41 \cdot 3 + 22,\ 41 = 22 \cdot 1 + 19,\ 22 = 19 \cdot 1 + 3,\ 19 = 3 \cdot 6 + 1,\ 3 = 1 \cdot 3.$

Неповними частками є числа 3,1,1,6,3. Тут $n = 4$. Обчислимо P_3 за наступною схемою, використовуючи формулу $P_k = q_k P_{k-1} + P_{k-2}$:

k	-1	0	1	2	3	4
q_k		3	1	1	6	3
P_k	1	3	4	7	46	145

Отже, чисельник передостаннього підхідного дробу $P_3 = 46$. Тому маємо:

$$x \equiv (-1)^4 \cdot 46 \cdot 5 (\mathrm{mod}\ 145) \equiv 85 (\mathrm{mod}\ 145).$$

Таким чином, клас лишків $[85]_{145}$ є розв'язком конгруенції $41x \equiv 5 (\mathrm{mod}\ 145)$. Але при модулі 435 цей клас лишків розбивається на три класи: $[85]_{435}, [85 + 145]_{435}, [85 + 2 \cdot 145]_{435}$, тобто $[85]_{435}, [230]_{435}, [375]_{435}$ – розв'язки конгруенції $123x \equiv 15 (\mathrm{mod}\ 435)$.

Опишемо групу $\mathbb{Z}_m^*$ дільників одиниці кільця $\mathbb{Z}_m$. Нехай $[a]_m$ – оборотний елемент моноїда $(\mathbb{Z}_m, \cdot)$. Тоді $[a]_m[x]_m = [1]_m$ для деякого $[x]_m \in \mathbb{Z}_m$. Остання рівність рівносильна конгруенції $ax \equiv 1 (\mathrm{mod}\ m)$, яка за твердженнями 5.1 і 5.2 має розв'язок тоді лише тоді, коли $(a, m) = 1$. Звідси випливає, що елемент $[a]_m \in \mathbb{Z}_m$ є оборотним тоді і лише тоді, коли $(a, m) = 1$. Таким чином, порядок групи $\mathbb{Z}_m^*$ дорівнює $\varphi(m)$. За наслідком 4.1 з теореми Лагранжа порядок кожного елемента скінченої групи є дільником порядку групи. Зокрема $([a]_m)^{\varphi(m)} = [1]_m$ для $(a, m) = 1$. Таким чином, $a^{\varphi(m)} \equiv 1 (\mathrm{mod}\ m)$, тобто отримано інше доведення теореми Ейлера.

Якщо $(a, m) = 1$, то порядок елемента $[a]_m$ групи $\mathbb{Z}_m^*$ називають *показником числа a за модулем m*. З наслідку 4.1 з теореми Лагранжа випливає, що показник числа a за модулем m є дільником $\varphi(m)$. Ціле число a називається *первісним коренем за модулем m*, якщо $[a]_m$ – твірний елемент групи $\mathbb{Z}_m^*$, тобто порядок $[a]_m$ дорівнює $\varphi(m)$.

Далі ми дамо характеризацію простих чисел, яка називається "Теоремою Вільсона", хоча вперше її доведення було отримане Лагранжем.

Характеризаційна теорема 5.1 (Теорема Вільсона).

Натуральне число p є простим тоді і лише тоді, коли

$$(p - 1)! \equiv -1 (\mathrm{mod}\ p).$$

Доведення. Якщо $p = 2$, то теорема є очевидною. Тому надалі вважаємо, що просте число $p > 2$, зокрема воно є непарним.

Спершу припустимо, що p – просте число, і доведемо, що $(p-1)! \equiv -1(\mathrm{mod}\ p)$. Нехай $a \in \{1, 2, \ldots, p-1\}$. Тоді конгруенція $ax \equiv 1(\mathrm{mod}\ p)$ за твердженням 5.1 має єдиний розв'язок $[a']_p$, де $a' \in \{1, 2, \ldots, p-1\}$. Якщо $a = a'$, то $a^2 \equiv 1(\mathrm{mod}\ p)$, звідки $a^2 - 1 = (a-1)(a+1)$ ділиться на p. Тоді $(a-1)$ або $(a+1)$ ділиться на p, а отже, $a \in \{1, p-1\}$. Таким чином, множина $\{2, 3, \ldots, p-2\}$ розбивається на пари елементів, які належать різним взаємно оберненим класам-елементам групи $\mathbb{Z}_p^*$. Звідси випливає, що

$$2 \cdot 3 \cdot \ldots \cdot (p-2) \equiv 1(\mathrm{mod}\ p).$$

Помноживши обидві частини отриманої конгруенції на $p-1$, отримуємо $(p-1)! \equiv p-1(\mathrm{mod}\ p) \equiv -1(\mathrm{mod}\ p)$.

Нехай $(p-1)! \equiv -1(\mathrm{mod}\ p)$. Доведемо, що тоді p – просте число. Припустимо, що число $p \geqslant 4$ є складеним. Нехай q – простий дільник p. Тоді $q < p$, а отже, $(p-1)!$ ділиться на q. Оскільки за умовою $(p-1)!+1$ ділиться на p, то $(p-1)! + 1$ ділиться на q. Отримуємо протиріччя, оскільки просте число не може ділити одночасно числа a і $a+1$, бо тоді воно б і ділило число $1 = (a+1) - a$. □

Розглянемо системи конгруенцій першого степеня. Нехай задано наступну систему:

$$\begin{cases} a_1 x \equiv b_1(\mathrm{mod}\ n_1) \\ a_2 x \equiv b_2(\mathrm{mod}\ n_2) \\ \ldots\ldots\ldots\ldots\ldots \\ a_k x \equiv b_k(\mathrm{mod}\ n_k) \end{cases}$$

Якщо b_i не ділиться на (a_i, n_i) для деякого $i \in \{1, \ldots, k\}$, то i-та конгруенція, а отже, і вся система не мають розв'язків. В іншому випадку, поділивши на (a_i, n_i) обидві частини i-ї конгруенції та модуль для кожного $i \in \{1, \ldots, k\}$, отримаємо наступну систему:

$$\begin{cases} a_1' x \equiv b_1'(\mathrm{mod}\ m_1), \quad (a_1',\, m_1) = 1 \\ a_2' x \equiv b_2'(\mathrm{mod}\ m_2), \quad (a_2',\, m_2) = 1 \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ a_k' x \equiv b_k'(\mathrm{mod}\ m_k), \quad (a_k',\, m_k) = 1 \end{cases}$$

Розв'язавши кожну конгруенцію окремо, отримаємо рівносильну систему:

$$\begin{cases} x \equiv c_1(\mathrm{mod}\ m_1) \\ x \equiv c_2(\mathrm{mod}\ m_2) \\ \ldots\ldots\ldots\ldots \\ x \equiv c_k(\mathrm{mod}\ m_k) \end{cases}$$

Таким чином, досить вміти розв'язувати останню систему конгруенцій.

Твердження 5.4.

Якщо система

$$\begin{cases} x \equiv c_1 (\mathrm{mod}\ m_1) \\ x \equiv c_2 (\mathrm{mod}\ m_2) \\ \dots\dots\dots\dots\dots \\ x \equiv c_k (\mathrm{mod}\ m_k) \end{cases}$$

має хоча б один розв'язок, то вона має єдиний розв'язок за модулем m, що дорівнює НСК чисел $m_1, m_2, \dots, m_k$.

Доведення. Дійсно, нехай a і b – представники класів-розв'язків системи конгруенцій. Тоді $a \equiv c_i (\mathrm{mod}\ m_i)$ і $b \equiv c_i (\mathrm{mod}\ m_i)$ для кожного $i \in \{1, \dots, k\}$. Отже, $a \equiv b (\mathrm{mod}\ m_i)$, тобто $a - b$ ділиться на m_i для кожного $i \in \{1, \dots, k\}$, а тому $a - b$ ділиться і на $m = [m_1, m_2, ..., m_k]$. Таким чином, $a \equiv b (\mathrm{mod}\ m)$, а тому $[a]_m = [b]_m$. □

Теорема 5.1 (Китайська теорема про лишки).

Якщо $m_1, m_2, ..., m_k$ – попарно взаємно прості числа, то єдиним розв'язком за модулем $m = m_1 \cdot m_2 \cdot \dots \cdot m_k$ системи конгруенцій є $[a]_m$, де $a = M_1 y_1 c_1 + \dots + M_k y_k c_k$, причому числа M_i і y_i визначаються з умов:

$$M_i = \frac{m_1 m_2 \cdot \dots \cdot m_k}{m_i}, \qquad M_i y_i \equiv 1 (\mathrm{mod}\ m_i).$$

Доведення. Дійсно, підставляючи значення a в i-ту конгруенцію $x \equiv c_i (\mathrm{mod}\ m_i)$ системи і беручи до уваги, що всі M_j при $j \neq i$ діляться на m_i, і конгруенція

$$M_i y_i \equiv 1 (\mathrm{mod}\ m_i), \quad (M_i, m_i) = 1$$

з невідомим y_i має єдиний розв'язок, одержимо: $a \equiv M_i y_i c_i \equiv c_i (\mathrm{mod}\ m_i)$. Таким чином, a задовольняє будь-яку конгруенцію системи, а отже, і всю систему. Тим самим показано, що $[a]_m$ і є тим єдиним розв'язком системи за модулем $m = m_1 \cdot m_2 \cdot \dots \cdot m_k$, бо НСК взаємно простих чисел дорівнює їхньому добутку. □

Приклад 5.7. Розв'яжемо систему:

$$\begin{cases} x \equiv 15(\mathrm{mod}\ 17) \\ x \equiv 11(\mathrm{mod}\ 13) \\ x \equiv 3(\mathrm{mod}\ 10) \end{cases}$$

Модулі є попарно взаємно простими, а тому можна використатити китайську теорему про лишки.

$$M = 17 \cdot 13 \cdot 10 = 2210,$$

$$M_1 = \frac{2210}{17} = 130, \quad M_2 = \frac{2210}{13} = 170, \quad M_3 = \frac{2210}{10} = 221.$$

$$130y_1 \equiv 1(\mathrm{mod}\ 17) \ \ (\Rightarrow) \ \ -6y_1 \equiv 18(\mathrm{mod}\ 17) \ \ (\Rightarrow) \ \ y_1 \equiv -3(\mathrm{mod}\ 17)$$

$$170y_2 \equiv 1(\mathrm{mod}\ 13) \quad (\Rightarrow) \quad y_2 \equiv 1(\mathrm{mod}\ 13)$$

$$221y_3 \equiv 1(\mathrm{mod}\ 10) \quad (\Rightarrow) \quad y_3 \equiv 1(\mathrm{mod}\ 10)$$

Отже,

$$a = 130 \cdot (-3) \cdot 15 + 170 \cdot 1 \cdot 11 + 221 \cdot 1 \cdot 3 = -3317,$$

а тому клас лишків $[-3317]_{2210} = [1103]_{2210}$ – єдиний розв'язок системи.

5.1. Зауваження. Перший зафіксований приклад на використання китайської теореми про лишки з'явився у китайській математичній праці Сун-цзи Суан Чіна кінця третього або початку четвертого століття. Формулюється задача наступним чином:

"*У нас є кілька речей, але ми не знаємо точно, скільки саме. Якщо порахувати їх трійками, то у нас залишиться дві речі. Якщо порахувати речі п'ятірками, то у залишку отримаємо три речі. Якщо порахувати їх сімками, у нас залишиться дві речі. Скільки всього є речей?*"

У загальному випадку, коли модулі $m_1, m_2, \ldots, m_k$ можуть і не бути попарно взаємно простими, систему розв'язують наступним чином. З першої конгруенції системи випливає, що всі значення x, які її задовольняють, мають вигляд $x = c_1 + m_1 t_1$, де t_1 пробігає всі цілі числа. Щоб обрати з них ті значення x, які задовольняють і другу конгруенцію, визначимо t_1 з наступної умови:

$$c_1 + m_1 t_1 \equiv c_2(\mathrm{mod}\ m_2) \quad \text{або} \quad m_1 t_1 \equiv c_2 - c_1(\mathrm{mod}\ m_2).$$

Ця конгруенція I-го степеня з невідомою t_1 має розв'язки, якщо $c_2 - c_1$ ділиться на (m_1, m_2), бо інакше остання конгруенція не має розв'язків, а отже, і вся система також не має розв'язків. Нехай $c_2 - c_1$ ділиться на (m_1, m_2). Розв'язуючи цю конгруенцію, отримаємо:

$$t_1 \equiv t_1'(\mathrm{mod}\ \frac{m_2}{(m_1, m_2)}).$$

Тоді множина всіх значень t_1, що задовольняють другу конгруенцію, задається з допомогою формули:

$$t_1 \equiv t_1' + \frac{m_2}{(m_1, m_2)} t_2,$$

де t_2 пробігає всі цілі числа. Звідси

$$x = c_1 + m_1 t_1' + \frac{m_1 m_2}{(m_1, m_2)} t_2 = y_2 + [m_1, m_2] t_2,$$

де $y_2 = c_1 + m_1 t_1'$ задовольняє перші дві конгруенції. Далі аналогічно з отриманих чисел обираємо ті, які задовольняють ще й третю конгруенцію. Відтак знову, або прийдемо до конгруенції відносно t_2, яка не має розв'язків, або знайдемо, що значення

$$x = y_3 + [m_1, m_2, m_3] t_3,\ t_3 \in \mathbb{Z}, \quad \text{або} \quad x \equiv y_3 (\text{mod}\ [m_1, m_2, m_3])$$

задовольняють перші три конгруенції. І так далі. Якщо така система має розв'язки, то знайдемо єдиний її розв'язок за модулем $[m_1, m_2, ..., m_k]$.

Приклад 5.8. Розв'яжемо систему:

$$\begin{cases} x \equiv 2 (\text{mod}\ 15) \\ x \equiv 7 (\text{mod}\ 20) \\ x \equiv 12 (\text{mod}\ 35) \end{cases}$$

Підставимо $x = 2 + 15t_1$ у другу конгруенцію системи:

$$\begin{gathered} 2 + 15t_1 \equiv 7 (\text{mod}\ 20) \\ 15t_1 \equiv 5 (\text{mod}\ 20) \\ 3t_1 \equiv 1 (\text{mod}\ 4) \\ t_1 \equiv 3 (\text{mod}\ 4) \\ t_1 = 3 + 4t_2 \end{gathered}$$

Підставимо $x = 2 + 15t_1 = 2 + 15(3 + 4t_2) = 47 + 60t_2$ у третю конгруенцію системи:

$$\begin{gathered} 47 + 60t_2 \equiv 12 (\text{mod}\ 35) \\ 60t_2 \equiv -35 (\text{mod}\ 35) \\ 25t_2 \equiv 0 (\text{mod}\ 35) \\ 5t_2 \equiv 0 (\text{mod}\ 7) \\ t_2 \equiv 0 (\text{mod}\ 7) \\ t_2 = 7t_3 \end{gathered}$$

Таким чином, $x = 47 + 60t_2 = 47 + 420t_3$, а отже, $[47]_{420}$ – розв'язок системи конгруенцій.

Рекомендована література : [**1**, с. 147–161], [**6**, с. 86–115], [**9**, с. 194–206], [**12**, с. 265–269], [**15**, с. 253–262].

Вправи до лекції 5.

5.1. З'ясувати, скільки розв'язків мають конгруенції:

а) $4x \equiv 20(\mathrm{mod}\ 9)$; б) $6x \equiv 9(\mathrm{mod}\ 8)$; в) $8x \equiv 12(\mathrm{mod}\ 4)$.

5.2. Розв'язати конгруенції, підставляючи числа з ПСЛ:

а) $4x \equiv 10(\mathrm{mod}\ 6)$; б) $4x \equiv 9(\mathrm{mod}\ 6)$; в) $4x^3 \equiv 9(\mathrm{mod}\ 4)$.

5.3. Розв'язати конгруенції методом рівносильних перетворень:

а) $7x \equiv 3(\mathrm{mod}\ 13)$; б) $16x \equiv 5(\mathrm{mod}\ 23)$; в) $32x \equiv 7(\mathrm{mod}\ 51)$.

5.4. Розв'язати конгруенції методом Ейлера:

а) $7x \equiv 3(\mathrm{mod}\ 13)$; б) $16x \equiv 9(\mathrm{mod}\ 23)$; в) $64x \equiv 6(\mathrm{mod}\ 30)$.

5.5. Розв'язати конгруенції методом ланцюгових дробів:

а) $32x \equiv 182(\mathrm{mod}\ 119)$; б) $365x \equiv 50(\mathrm{mod}\ 395)$.

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

а) $3x + 4y = 13$; б) $12x + 8y = 17$; в) $91x - 28y = 35$.

5.7. Для перевезення зерна є мішки по 60 і 80 кг. Скільки таких мішків потрібно для перевезення 440 кг зерна?

5.8. Розв'язати систему конгруенцій

$$\begin{cases} x \equiv 5(\mathrm{mod}\ 7) \\ x \equiv 3(\mathrm{mod}\ 4), \end{cases}$$

використовуючи китайську теорему про лишки.

5.9. Розв'язати наступну систему конгруенцій двома методами:

$$\begin{cases} 2x \equiv 3(\mathrm{mod}\ 5) \\ 7x \equiv 5(\mathrm{mod}\ 9) \end{cases}$$

5.10. Знайти всі розв'язки за модулем 300 системи конгруенцій:

$$\begin{cases} 3x \equiv 1(\mathrm{mod}\ 20) \\ 2x \equiv 3(\mathrm{mod}\ 15) \end{cases}$$

5.11. Розв'язати системи конгруенцій:

а) $\begin{cases} x \equiv 12(\mathrm{mod}\ 3) \\ x \equiv 34(\mathrm{mod}\ 4) \\ x \equiv 21(\mathrm{mod}\ 5) \end{cases}$ б) $\begin{cases} x \equiv 5(\mathrm{mod}\ 4) \\ x \equiv 7(\mathrm{mod}\ 6) \\ x \equiv 12(\mathrm{mod}\ 9) \end{cases}$

5.12. Розв'язати системи конгруенцій:

а) $\begin{cases} 4x \equiv 40(\mathrm{mod}\ 3) \\ 9x \equiv 34(\mathrm{mod}\ 4) \\ 16x \equiv 21(\mathrm{mod}\ 5) \end{cases}$ б) $\begin{cases} 7x \equiv 3(\mathrm{mod}\ 11) \\ 3x \equiv 2(\mathrm{mod}\ 5) \\ 15x \equiv 5(\mathrm{mod}\ 35) \end{cases}$

в) $\begin{cases} 4x \equiv 10(\mathrm{mod}\ 9) \\ 12x \equiv -4(\mathrm{mod}\ 7) \\ 4x \equiv 5(\mathrm{mod}\ 12) \end{cases}$ г) $\begin{cases} 36x \equiv 12(\mathrm{mod}\ 3) \\ 41x \equiv 34(\mathrm{mod}\ 12) \\ 87x \equiv 16(\mathrm{mod}\ 9) \end{cases}$

5.13. Розв'яжіть 1700-річну задачу Сун-цзи Суан Чіна, сформульовану в кінці п'ятої лекції.

5.14. На шляху до пункту здачі яєць у вантажівку фермера потрапляє метеорит і знищує всю його продукцію. Для того, щоб подати страховий позов, він повинен знати, скільки яєць було розбито. Він пам'ятає, що коли він рахував яйця парами, то в кінці залишилося 1 яйце, коли рахував трійками, то у залишку було 2 яйця, коли рахував четвірками, залишилося 1 яйце, і коли він підрахував їх п'ятірками, також залишилося 1 яйце, але коли порахував яйця сімками, то в залишку не було жодного яйця. Яка найменша кількість яєць була у вантажівці?

5.15. Три конвеєрні стрічки на фабриці подають шоколадні батончики: перша – кожні 8 секунд, друга – кожні 9 секунд, причому перша подача на другу стрічку відбувається через 2 секунди після старту, а третя – кожні 11 секунд, перша подача через 3 секунди після старту. Знайдіть найменший момент часу, коли всі три стрічки одночасно подадуть батончики, та визначте, через скільки секунд цей збіг повториться вдруге.

5.16. З'ясувати, при яких значеннях $a \in \mathbb{Z}$ має розв'язки система:

$$\begin{cases} 6x \equiv a(\mathrm{mod}\ 4) \\ 3x \equiv 4(\mathrm{mod}\ 10) \end{cases}$$

5.17. Знайти хоча б одне значення $m \in \mathbb{N}$, при якому несумісною є система:

$$\begin{cases} x \equiv 9(\mathrm{mod}\ 6) \\ x \equiv 7(\mathrm{mod}\ m) \end{cases}$$

5.18. Скласти таблицю Келі групи $\mathbb{Z}_8^*$.

5.19. Знайти обернені елементи до $[13]_{21}, [20]_{21} \in \mathbb{Z}_{21}^*$.

5.20. Знайти порядки всіх елементів групи $\mathbb{Z}_{12}^*$.

5.21. Знайти показники всіх цілих чисел за модулем 11. Описати первісні корені за модулем 11.

5.22. Скільки точок з цілими координатами лежать на прямій $9x-11y+6 = 0$ між прямими $x = -150$ та $x = 100$?

5.23. Скільки точок з цілими координатами лежать на прямій $4x - 15y = 7$ між прямими $y = 0$ та $y = 2016$?

5.24. Через скільки точок з цілими координатами проходять сторони трикутника з вершинами $A(2, 3)$, $B(7, 8)$ та $C(13, 5)$?

5.25. Розв'язати конгруенцію $x^2 - 1 \equiv 0 (\mathrm{mod}\ 35)$.

5.26. Довести, що для кожного непарного простого числа p конгруенція $x^2 + 1 \equiv 0 (\mathrm{mod}\ p)$ має розв'язок тоді і лише тоді, коли конгруенція $x^2 + 1 \equiv 0 (\mathrm{mod}\ p^2)$ має розв'язок.

5.27. Довести, що для складеного числа $n > 4$ виконується конгруенція $(n - 1)! \equiv 0 (\mathrm{mod}\ n)$.

5.28. Довести, що для кожного простого числа $p > 2$ має місце конгруенція $2(p - 3)! \equiv -1 (\mathrm{mod}\ p)$.

5.29. Доведіть, що для непарного простого числа p має місце конгруенція:

$$\prod_{k=1}^{\frac{p-1}{2}} k^2 \equiv (-1)^{\frac{p+1}{2}} (\mathrm{mod}\ p).$$

5.30. Нехай I та J такі ідеали кільця R, що $I + J = R$. Довести, що

а) для кожних $r, s \in R$ система конгруенцій

$$\begin{cases} x \equiv r (\mathrm{mod}\ I) \\ x \equiv s (\mathrm{mod}\ J) \end{cases}$$

має розв'язок;

б) довільні два розв'язки системи конгруентні за модулем ідеалу $I \cap J$;

в) $R/(I \cap J) \cong (R/I) \times (R/J)$.

Список літератури

1. Безущак О.О. *Елементи теорії чисел* / О.О. Безущак, О.Г. Ганюшкін. – К.: ВПЦ "Київський університет", 2003. – 202 с.
2. Безущак О.О. *Теорія груп: Навчальний посібник для студентів механіко-математичного факультету* / О.О. Безущак, О.Г. Ганюшкін. – К.: ВПЦ "Київський університет", 2005. – 123 с.
3. Бондаренко Є.В. *Теорія кілець* / Є.В. Бондаренко. – К.: ВПЦ "Київський університет", 2012. – 64 с.
4. Ганюшкін О.Г. *Завдання до практичних занять з алгебри і теорії чисел (теорія груп)* / О.Г. Ганюшкін, О.О. Безущак. – К.: ВПЦ "Київський університет", 2007. – 103 с.
5. Головащук Н.С. *Збірник задач з теорії кілець* / Н.С. Головащук, Є.А. Кочубінська, С.А. Овсієнко. – К.: ВПЦ "Київський університет", 2013. – 86 с.
6. Завало С.Т. *Алгебра і теорія чисел. Практикум. Частина 2* / С.Т. Завало, С.С. Левищенко та ін. – Київ: Вища школа, 1986. – 264 с.
7. Калашнікова Н.В. *Елементи алгебри та їх застосування в криптографії: посібник* / Н.В. Калашнікова. – Дніпропетровськ: РВВ ДНУ, 2015. – 40 с.
8. Кудрявцева Г.М. *Кільця. Приклади і задачі* / Г.М. Кудрявцева, А.С. Олійник. – К.: ВПЦ "Київський університет", 2005. – 60 с.
9. Курдаченко Л.А. *Вибрані розділи алгебри та теорії чисел* / Л.А. Курдаченко, В.В. Кириченко, М.М. Семко. – К.: ІМ НАНУ, 2005. – 208 с.
10. Никифорчин О.Р. *Елементи загальної топології* / О.Р. Никифорчин. – Івано-Франківськ: Голіней, 2015. – 240 с.
11. Тилищак О.А. *Елементи теорії груп* / О.А. Тилищак. – Вид. УжНУ "Голверла", 2009. – 40 с.
12. Dummit D.S. *Abstract Algebra* / David S. Dummit, Richard M. Foote. – Wiley Intern. Ed., Chichester: Wiley, 2004. – 932 p.
13. Hall M. *The Theory of Groups* / M. Hall. – American Mathematical Soc., 1999. – 434 p.
14. Howie J.M. *Fundamentals of semigroup theory* / J.M. Howie. – New York: Oxford University Press, 1995. – 351 p.
15. Judson T.W. *Abstract Algebra: Theory and Applications* / Thomas W. Judson. – An open-source textbook available at http://abstract.ups.edu, 2012. – 428 p.
16. Robinson D.J.S. *A course in the theory of groups* / Derek J.S. Robinson. – 2nd ed. – Springer-Verlag New York, 1995. – 499 p.

Предметний покажчик

A_n, 22
C_n, 17, 31
D_n, 23
$GL(n, \mathbb{R})$, 8
$M(n, \mathbb{R})$, 8
$SL(n, \mathbb{R})$, 9
S_X, 18
$\mathrm{Aff}\,(\mathbb{R})$, 28
$\mathrm{Aff}^+(\mathbb{R})$, 28
$\mathrm{Im}\,\varphi$, 51, 109
$\mathrm{Ker}\,\varphi$, 51, 109
$\mathrm{Shift}\,(\mathbb{R})$, 28
$\mathrm{Tor}\,(G)$, 34
$\mathbb{T}$, 17
$\mathbb{Z}[i]$, 104
$\mathrm{Aut}\,(G)$, 54
$\mathrm{End}\,(G)$, 54
$\mathrm{Inn}\,(G)$, 54
$\mathrm{Isom}\,(\mathbb{R}^n)$, 23
$\mathrm{char}\,R$, 105
p-група, 66
  силовська, 87

ідеал, 110
  власний, 110
  головний, 111
  лівий, 110
  максимальний, 116
  правий, 110
  простий, 116
  тривіальний, 110
ідемпотент, 6, 101
ізоморфізм, 53, 109

АНЛ, 132

ЗСЛ, 133

ННЛ, 132

ПСЛ, 132

автоморфізм, 54
  внутрішній, 54
алгоритм Евкліда, 125

бінарна операція, 5
  асоціативна, 5
  комутативна, 5

визначальні співвідношення, 14
вкладення, 54

гомоморфізм, 51, 109
  природній, 56, 113
  тривіальний, 51
гомоморфізму
  образ, 51, 109
  ядро, 51, 109
група, 7
  ізоморфна, 53
  Клейна, 26
  абелева, 8
  без кручень, 30
  вільна, 14
  діедральна, 23
  дільників одиниці кільця, 103
  загальна лінійна, 8
  знакозмінна, 22
  кватерніонів, 11
  нільпотентна, 93
  періодична, 29
  проста, 45
  розв'язна, 72
  симетрій, 23
    ромба, 26
  симетрична, 18
  спеціальна лінійна, 9
  циклічна, 30

дільник нуля, 101
дія групи, 61
  вільна, 62
  природня, 63
  транзитивна, 62
декремент підстановки, 27
довжина орбіти, 62

елемент
  нільпотентний, 108
  простий, 123
  протилежний, 100
  твірний, 13
елементи
  асоційовані, 122
  комутують, 8
  спряжені, 29
ендоморфізм, 54
епіморфізм, 53, 109

зображення, 53
  лінійне, 53
  точне, 53

кільце, 100
  ізоморфне, 109
  булеве, 108
  головних ідеалів, 111
  евклідове, 120
  з одиницею, 101
  комутативне, 101
  нетривіальне, 102
  скінченне, 100
  тривіальне, 102
  функцій, 108
    неперервних, 109
  цілісне, 102
  цілих гаусових чисел, 104
квазігрупа, 10
клас лишків, 112
композиція, 18
комутант групи, 71
комутатор, 71
конгруентні елементи, 112

лівий зсув, 57

множина твірних, 13
  мінімальна, 14
моноїд, 6
мономорфізм, 53, 109

найбільший спільний дільник, 124
найменше спільне кратне, 127
напівгрупа, 5
напівпрямий добуток, 84
неповна частка, 120
норма, 120
  додатня, 120
нормалізатор, 64
нормальний дільник, 43
нуль кільця, 100

обернений елемент
  лівий, 7
  правий, 7
область цілісності, 102
оборотний елемент, 7
  зліва, 7
  справа, 7
одиниця, 6
  кільця, 101
  ліва, 6
  права, 6
однорідний простір, 62
орбіта, 62
остача, 120

підгрупа, 11
  інваріантна, 43
  власна, 12
  діагональна, 85
  кручення, 34
  нормальна, 43
  породжена множиною, 13
  тривіальна, 12
  циклічна, 28
підкільце, 103
  власне, 103
  породжене множиною, 104
  тривіальне, 103
підполе, 104

підстановка, 18
  непарна, 21
  парна, 21
первісний корінь, 142
показник числа, 142
поле, 102
порядок
  групи, 10
  елемента, 29
  кільця, 100
похідна групи, 71
пряма сума, 82
прямий добуток
  внутрішній, 83
  зовнішній, 79

рівносильні конгруенції, 138
розбиття, 35
  лівостороннє, 36
  правостороннє, 37
розв'язок конгруенції, 138
розширення поля, 104
ряд, 73
  нормальний, 74
  субнормальний, 74

самозачеплена множина, 42
стабілізатор, 62
степінь групи, 81
  зліченний, 81
степінь конгруенції, 138
ступінь розв'язності, 72
суміжний клас
  лівий, 36
  правий, 37

тіло, 102
  кватерніонів, 108
таблиця Келі, 10
транспозиція, 20

факторгрупа, 46
фактори ряду, 74
факторкільце, 112

характеристика кільця, 105
  додатня, 105
  нуль, 105

центр
  групи, 66
  кільця, 107
централізатор
  елемента, 65
  підмножини, 66
цикл, 19