Міністерство освіти і науки України

Житомирський державний університет імені Івана Франка

ЕЛЕМЕНТИ АЛГЕБРИ І ТЕОРІЇ ГАЛУА

Навчально-методичний посібник

Житомир

2025

УДК 512:378.22(072)
Е 46

Рекомендовано до друку Вченою радою
Житомирського державного університету імені Івана Франка
(протокол № 21 від 31 жовтня 2025 року)

Рецензенти:

Валерій ЖУРАВЛЬОВ – доктор фізико-математичних наук, професор, завідувач кафедри вищої та прикладної математики Поліського національного університету.

Олександр ПРИЛИПКО – кандидат фізико-математичних наук, доцент, доцент кафедри інженерії програмного забезпечення Державного університету «Житомирська політехніка».

Василь МИХАЙЛЕНКО – доктор фізико-математичних наук, професор, професор кафедри алгебри та геометрії Житомирського державного університету імені Івана Франка.

Елементи алгебри і теорії Галуа: Навчально-методичний посібник / Укладачі Погоруй А. О., Фонарюк О. В. Житомир: Вид-во ЖДУ імені Івана Франка, 2025. 81 с.

У навчально-методичному посібнику подано курс лекцій з додаткових розділів алгебри, що охоплює базові поняття загальної алгебри та основи теорії Галуа. Посібник призначений для здобувачів вищої освіти фізико-математичних факультетів, а також аспірантів, викладачів, науковців і докторантів. Викладений матеріал може бути використаний у навчальному процесі як на заняттях, так і при самостійному вивченні здобувачами курсу алгебри та теорії Галуа.

УДК 512:378.22(072)

Зміст

ПЕРЕДМОВА

Навчальний посібник написано на основі лекцій з курсу «Додаткові розділи алгебри», які автори читають для здобувачів фізико-математичного факультету ЖДУ імені Івана Франка. У ньому розглядаються деякі базові поняття і твердження загальної алгебри та наводиться короткий виклад теорії Галуа.

У першому розділі посібника вивчається поняття алгебраїчної структури і розглядаються приклади деяких алгебраїчних структур з однією бінарною операцією: півгрупа, моноїд, квазігрупа, група та структури з двома бінарними операціями: кільця, поля. Наводяться такі базові поняття теорії груп: гомоморфізм та ізоморфізм груп, підгрупа, циклічна група, суміжні класи, терема Лагранжа, тощо. Розглядаються важливі приклади кілець та їх основних понять: ідемпотент, нільпотент, ідеал, дільник нуля та інші. Також вивчаються різні поля – скінченні та нескінченні і їх розширення алгебраїчні та трансцендентні.

Другий розділ посібника присвячений теорії Галуа. Вивчаються основи теорії Галуа та її застосування до розв’язаності поліноміальних рівнянь у радикалах на прикладі рівняння п’ятого степеню, корені якого не виражаються у радикалах через коефіцієнти многочлена. Розглядаються застосування ідей теорії Галуа для обґрунтування можливості (неможливості) побудов за допомогою циркуля та лінійки.

Посібник можна використовувати у навчальному процесі для підготовки бакалаврів та магістрів як аудиторно, так і при самостійному вивченні здобувачами курсу алгебри та теорії Галуа.

І БАЗОВІ ПОНЯТТЯ АЛГЕБРИ

ЛЕКЦІЯ 1. АЛГЕБРАЇЧНІ ОПЕРАЦІЇ. АЛГЕБРАЇЧНІ СТРУКТУРИ

Нехай $X \neq \emptyset$ деяка множина. Через X^n будемо позначати декартовий добуток множини X на себе n разів, тобто $X^n = \underbrace{X \times X \times \ldots \times X}_{n}$, де $n \in \mathbb{Z}_+ = \mathbb{N} \cup \{0\}$.

Означення 1.1. *Відображення $f: X^n \to X$ називається n-арною алгебраїчною операцією на X.*

Зауваження 1.1. Надалі під n-арною операцією будемо мати на увазі саме внутрішню n-арну операцію, тобто, коли результат операції має ту ж природу, що і множники. Наприклад, векторний добуток векторів. Скалярний же добуток векторів не є внутрішньою бінарною операцією, оскільки у цьому випадку результат добутку векторів є скаляр, а не вектор.

Домовимось також надалі використовувати такі позначення : $\mathbb{Z}^* = \mathbb{Z}\backslash\{0\}$, $\mathbb{Q}^* = \mathbb{Q}\backslash\{0\}$, $\mathbb{R}^* = \mathbb{R}\backslash\{0\}$, $\mathbb{C}^* = \mathbb{C}\backslash\{0\}$.

Приклади

1. Якщо $n = 2$, то операція називається бінарною. Це одна з найбільш вживаних в математиці операцій і такими є, наприклад, множення та додавання на множині дійсних чисел.
2. При $n = 1$ операція називається унарною і до таких операцій належить, наприклад, існування протилежного числа $(-n)$ для $n \in \mathbb{Z}$ чи оберненого r^{-1} для $r \in \mathbb{R}^*$.
3. Прикладами 0-арної операції є існування нейтрального елементу при додаванні дійсних чисел (нуль) та при їх множенні (одиниця).
4. При $n = 3$ операцію називають тернарною і в якості прикладу можна навести подвійний векторний добуток $[\boldsymbol{a}, [\boldsymbol{b}, \boldsymbol{c}]]$ векторів простору $\boldsymbol{a}$, $\boldsymbol{b}$, $\boldsymbol{c}$.

Із означення випливає, що бінарна операцію двох елементів $x, y \in X$ позначається як $f(x, y)$, але частіше у загальних випадках для бінарних операцій використовуються символи *, °. Також, щоб підкреслити близькість операції до адитивних властивостей іноді використовується символ $+$, а для близькості до мультиплікативних властивостей використовується символ $\times$ та вживається відповідно адитивна та мультиплікативна термінологія.

Означення 1.2. *Алгебраїчною структурою називається непорожня множина X з довільною кількістю внутрішніх операцій довільної арності*.

Будемо позначати алгебраїчні структури у вигляді упорядкованого набору $(X, f, g, h, \dots)$, де $f, g, h, \dots$ – внутрішні операції.

Приклади

1. $(\mathbb{Z}, +)$ – алгебраїчна структура з операцією додавання на множині цілих чисел.
2. $(\mathbb{R}, -, \times)$ – алгебраїчна структура з операціями віднімання та множення на множині дійсних чисел.
3. $(\mathbb{N}, +, \uparrow)$ – алгебраїчна структура з операціями додавання та піднесення до степеню на множині натуральних чисел.

Вправа 1.1. Навести власні приклади алгебраїчних структур.

Означення 1.3. *Бінарна операція * на множині X називається*

1. *<u>Комутативною</u>, якщо* $\forall x, y \in X$,

$$x * y = y * x.$$

2. *<u>Асоціативною</u>, якщо* $\forall x, y \in X$,

$$x * (y * z) = (x * y) * z.$$

Означення 1.4. *Елемент $e_r \in X$ називається правим нейтральним елементом бінарної операції * якщо* $\forall x \in X$,

$$x * e_r = x.$$

Елемент $e_l \in X$ називається лівим нейтральним елементом бінарної операції $*$ якщо $\forall x \in X$,

$$e_l * x = x.$$

Елемент $e \in X$ називається нейтральним елементом бінарної операції $*$ якщо $\forall x \in X$,

$$x * e = e * x = x.$$

В адитивній термінології нейтральний елемент називають *нулем* операції, а в мультиплікативній *одиницею* операції.

Твердження 1.1. *Якщо існують правий нейтральний $e_r \in X$ та лівий нейтральний $e_l \in X$ елементи операції $*$, то існує нейтральний елемент $e \in X$ цієї операції, причому*

$$e_r = e_l = e.$$

Доведення. Дійсно, із означення правого і лівого елементів випливає

$$e_l = e_l * e_r = e_r.$$

Звідки випливає, що e_r (чи e_l) є нейтральним елементом операції $*$.

Означення 1.5. *Нехай e – нейтральний елемент відносно операції $*$. Елемент $x_r^{-1} \in X$ називається правим симетричним елементом до елемента $x \in X$, якщо*

$$x * x_r^{-1} = e.$$

Елемент $x_l^{-1} \in X$ називається лівим симетричним елементом до елемента $x \in X$, якщо

$$x_l^{-1} * x = e.$$

Одночасно правий і лівий симетричний елемент $x^{-1} \in X$ до елемента $x \in X$ називається симетричним елементом до x, тобто

$$x * x^{-1} = x^{-1} * x = e.$$

В адитивній термінології симетричний елемент називається протилежним, а у мультиплікативній обернений елемент.

Твердження 1.2. *Нехай $*$ асоціативна операція на X і існують правий симетричний елемент $x_r^{-1} \in X$ та лівий симетричний елемент $x_l^{-1} \in X$ до $x \in X$. Тоді існує єдиний симетричний до x елемент x^{-1}, причому*

$$x_r^{-1} = x_l^{-1} = x^{-1}.$$

Доведення. Із означення 4 випливає, що

$$x * x_r^{-1} = e = x_l^{-1} * x.$$

Помноживши рівність $x * x_r^{-1} = e$ зліва на x_l^{-1} отримаємо

$$x_l^{-1} * (x * x_r^{-1}) = x_l^{-1} * e = x_l^{-1}.$$

З іншого боку, використовуючи асоціативність, маємо

$$x_l^{-1} * (x * x_r^{-1}) = (x_l^{-1} * x) * x_r^{-1} = e * x_r^{-1} = x_r^{-1},$$

тобто $x_r^{-1} = x_l^{-1}$. Звідки випливає єдиність x_r^{-1} та x_l^{-1}. Дійсно, якщо припустити існування ще одного правого симетричного елемента $\tilde{x}_r^{-1}$ до x, то має виконуватись рівність $\tilde{x}_r^{-1} = x_l^{-1}$, а, отже, $\tilde{x}_r^{-1} = x_r^{-1}$. Аналогічно для лівого симетричного елемента.

Отже, існує і єдиний симетричний до x *елемент* x^{-1}: $x^{-1} = x_r^{-1}$ (або $x^{-1} = x_l^{-1}$).

Приклади

1. В алгебраїчній структурі $(\mathbb{R}, -)$ 0 – тільки правий нейтральний елемент.

2. В алгебраїчній структурі векторів простору із векторним добутком не існує ні правого, ні лівого нейтрального елемента.
3. В алгебраїчній структурі $(2^X, \cup)$ $\emptyset$ – нейтральний елемент, але для жодного $2^X \ni A \neq \emptyset$ не існує симетричного.

ОСНОВНІ АЛГЕБРАЇЧНІ СТРУКТУРИ З БІНАРНОЮ ОПЕРАЦІЄЮ

Означення 1.6. *Алгебраїчна структура* $(X, *)$ *називається* <u>*оперативом*</u>*, якщо* $\forall x, y \in X,\ x * y \in X$.

Приклади

1. $(\mathbb{Z}, +)$, $(\mathbb{Q}, \times)$, $(\mathbb{R}, -)$ – оперативи.
2. $(\mathbb{Z}, -)$ – оператив, тоді як $(\mathbb{N}, -)$ не оператив, оскільки, наприклад, $3 - 5 = -2 \notin \mathbb{N}$.
3. $(\mathbb{Q}^*, :)$ – оператив, а $(\mathbb{Z}^*, :)$ не оператив, оскільки, наприклад, $\frac{1}{2} \notin \mathbb{Z}^*$.

Півгрупи

Означення 1.7. *Оператив* $(X, *)$ *з асоціативною операцією* $*$ *називається* <u>*півгрупою*</u>.

Приклади

1. $(\mathbb{N}, +)$, $(\mathbb{N}, \cdot)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, \cdot)$ – півгрупи.
2. Нехай $M_{n\times n}$ – квадратні дійсні матриці розмірності n із звичайною операцією добутку $\cdot$ цих матриць, тоді $(M_{n\times n}, \cdot)$ – півгрупа.
3. Множина перехідних ймовірностей марковського процесу на вимірному просторі утворюють півгрупу (наслідок рівняння Чепмена-Колмогорова).
4. Алгебраїчна структура векторів простору із векторним добутком не є півгрупою оскільки векторний добуток не асоціативний.

Моноїди

Означення 1.8. *Півгрупа* $(X,*)$ *яка містить нейтральний елемент* e *відносно операції* $*$ *називається моноїдом.*

Позначається $(X,*,e)$.

Приклади

1. $(\mathbb{N},\cdot,1)$, $(\mathbb{Q},+,0)$, $(\mathbb{R},\cdot)$, $(2^X,\cup,\emptyset)$, $(2^X,\cap,X)$ – моноїди.
2. $(\mathbb{N},+)$ – не моноїд, оскільки не містить нейтрального елемента 0, але є півгрупою.
3. $(\mathbb{N},\text{НСК},1)$, де НСК – це найменше спільне кратне, є моноїдом.

Вправа 1.2. Навести власні приклади моноїдів та півгруп, що не є моноїдами.

ЛЕКЦІЯ 2. **ГРУПИ**

Групи та деякі їх базові властивості

Означення 2.1. *Групою називається моноїд* $(X,*,e)$*, кожен елемент якого має симетричний, тобто* $\forall x \in X$ *існує* $x^{-1} \in X$.

Як правило для позначення груп на місці X використовують символ G.

Повне описання групи як математичної структури має вигляд: $(G,e,inv,*)$, де G – множина елементів групи, e – це 0-арна операція, яка позначає існування нейтрального елемента e групи, inv – це 1-арна операція взяття симетричного елемента, тобто $inv\colon G \to G$, $inv(x) = x^{-1}$, $*$ це – бінарна операція групи.

Для спрощення запису для позначення групи $(G,e,inv,*)$ будемо використовувати позначення $(G,*,e)$. Через $|G|$ позначають кількість елементів групи, яке називається порядком групи. Група $(G,*,e)$ з комутативною операцією $*$ називається абелевою. Часто для підкреслювання близькості

бінарної операції групи до операції додавання (множення) групу називають адитивною (мультиплікативною).

Приклади

1. $(\mathbb{Z}, +)$ – група нескінченна (адитивна, абелева).
2. $(\mathbb{R}^*, \cdot)$ – група нескінченна (мультиплікативна, абелева).
3. $(2^X, \Delta)$, де Δ операція симетричної різниці, – абелева група.
4. $(\{+1, -1\}, \cdot)$ – скінченна група 2-го порядку (мультиплікативна, абелева).
5. $(GL_{n\times n}(\mathbb{R}), \cdot)$ (де $GL_{n\times n}(\mathbb{R})$ – множина невироджених дійсних матриць розміру $n \times n$) – група (мультиплікативна, некомутативна при $n > 1$).
6. Множина комплексних чисел з модулем одиниця і операцією множення комплексних чисел – мультиплікативна абелева група.
7. Група поворотів правильного n-кутника навколо його центру, яка складається із елементів: $R_{\frac{360}{n}k}$, $k = 0,1, \dots, n-1$, де R_α – поворот -кутника на α градусів з операцією «композиція поворотів». Легко бачити, що $e = R_0$ – нейтральний елемент цієї групи. Позначається через C_n.
8. Діедральна (діедрична) група – це група симетрій правильного n-кутника, у якій, крім поворотів навколо центру n-кутника, розглядаються відображення відносно осей симетрії цього n-кутника. Позначається через D_{2n} оскільки містить $2n$ елементів (або у книгах з геометрії через D_n).

Вправа 2.1. Переконатись, що у прикладі 3 $(2^X, \Delta)$ є група (вказати нейтральний елемент, симетричний елемент до $A \in 2^X$, перевірити, що операція Δ асоціативна).

Вправа 2.2. Описати елементи діедральної групи правильного трикутника та виписати таблицю множення цих елементів (таблицю Келі).

Вправа 2.3. Нехай $(G,*,e)$ – група, $a,b \in G$. Показати, що

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

Теорема 2.1. Алгебраїчна структура $(G,*)$ є групою тоді і тільки тоді, коли виконуються умови:

1. Операція $*$ є асоціативною,
2. $\forall a,b \in G$ існують єдиний елемент $g \in G$ та єдиний елемент $h \in G$ такі, що $a*g = b$ та $h*b = a$.

Доведення. Необхідність випливає із означення групи. Дійсно, помножимо рівняння $a*g = b$ зліва на a^{-1} отримаємо $g = a^{-1}*b$. Аналогічно, помножимо рівняння $h*b = a$ справа на b^{-1} отримаємо $h = a*b^{-1}$. Тобто, g та h, які задовольняють умову 2, існують і єдині.

Достатність. Покажемо, що за умов теореми існує нейтральний елемент. Дійсно, для $\forall x \in G$ існує єдина пара елементів $g_0, h_0 \in G$ така, що $x*g_0 = x$ та $h_0 * x = x$.

Далі, із 2 випливає, що $\forall y \in G$ існує k таке, що $k*x = y$. Отже, з урахуванням умови 1, маємо

$$y*g_0 = (k*x)*g_0 = k*(x*g_0) = k*x = y.$$

Тобто, g_0 є правим нейтральним елементом алгебраїчної структури $(G,*)$. Аналогічно доводиться, що h_0 – лівий нейтральний елемент, а значить за твердженням 1.1 $g_0 = h_0 = e$ – нейтральний елемент.

Для довільного a, із рівняння $a*g = e$ (тут у якості b взято нейтральний елемент e) отримуємо, що $g = a_r^{-1}$. Аналогічно, покладаючи $b = a$ та $a = e$ у рівнянні $h*b = a$ отримуємо $h = a_l^{-1}$. Звідки за твердженням 1.2 $a^{-1} = a_r^{-1} = a_l^{-1}$.

Отже, $(G,*)$ є групою.

Наслідок 2.1. Із теореми 1 випливає правило скорочення у групі, тобто, якщо $a*g_1 = a*g_2$, то $g_1 = g_2$ і, якщо $h_1*b = h_2*b$, то $h_1 = h_2$.

Вправа 2.4. Довести наслідок 2.1.

Гомоморфізм груп

Означення 2.2. *Нехай* $(G_1,*)$ *та* $(G_2,\circ)$ *- групи. Гомоморфізмом групи* $(G_1,*)$ *у групу* $(G_2,\circ)$ *називається відображення* $\varphi: G_1 \to G_2$, *для якого виконується властивість* $\forall x, y \in G_1$

$$\varphi(x * y) = \varphi(x) \circ \varphi(y).$$

Приклади

1. Розглянемо відображення $\varphi: GL_{n\times n}(\mathbb{R}) \to \mathbb{R}^*$, при якому $\forall A \in GL_{n\times n}(\mathbb{R})$, $\varphi(A) = det(A)$. Оскільки $\forall A, B \in GL_{n\times n}(\mathbb{R})$ $\varphi(AB) = det(AB) = det(A)det(B)$, то φ – гомоморфізм.
2. Нехай $(G,*)$ – група. Покладемо $\forall g \in G$ $\varphi(g) = 0$. Очевидно, що φ є гомоморфізм групи $(G,*)$ у групу $(\mathbb{Z},+)$ (або у групу $(\mathbb{Q},+)$, або у групу $(\mathbb{R},+)$).

Означення 2.3. *Нехай* φ *– гомоморфізмом групи* $(G_1,*,i)$ *у групу* $(G_2,\circ,e)$. *Ядро гомоморфізму* φ *— це підмножина всіх елементів* G_1, *що відображаються в нейтральний елемент* e *групи* $(G_2,\circ,e)$*:*

$$\ker\varphi = \{x \in G_1 | \varphi(x) = e\}.$$

Легко бачити, що $\ker\varphi \neq \emptyset$ оскільки нейтральний елемент i групи $(G_1,*,i)$ належить до ядра, тобто $\varphi(i) = e$.

Дійсно, $\forall x \in G_1$ $\varphi(x) = \varphi(x * i) = \varphi(x) \circ \varphi(i)$, звідки $\varphi(i) = e$.

Означення 2.3. *Ізоморфізмом* φ *групи* $(G_1,*)$ *на групу* $(G_2,\circ)$ *називається бієктивний гомоморфізм, тобто гомоморфізм, для якого виконується умови:*

1. *якщо* $x \neq y$ *то* $\varphi(x) \neq \varphi(y)$,
2. $\varphi(G_1) = G_2$.

Якщо групи $(G_1,*)$ та $(G_2,\circ)$ – ізоморфні то позначають $(G_1,*) \cong (G_2,\circ)$.

Означення 2.4. *Ізоморфізмом φ групи $(G,*)$ у себе, тобто бієктивний гомоморфізм $\varphi: G \to G$, $\varphi(x * y) = \varphi(x) \circ \varphi(y)$, $\forall x, y \in G$, називається автоморфізмом.*

Частинним випадком автоморфізму є *внутрішній* автоморфізм, коли $\exists h \in G$ такий, що $\forall x \in G$

$$\varphi(x) = h * x * h^{-1}.$$

Будь-який не внутрішній автоморфізм називається *зовнішнім*. Звичайно, внутрішній автоморфізм актуальний тільки для некомутативних груп.

Приклади

1. Функція $\varphi(x) = e^x$ є ізоморфізмом адитивної групи $(\mathbb{R}, +, 0)$ на мультиплікативну групу $(\mathbb{R}_{>0}, \cdot, 1)$. Дійсно,
$$e^{x+y} = e^x \cdot e^y.$$
2. Функція $\varphi(x) = \ln x$ є ізоморфізмом групи $(\mathbb{R}_{>0}, \cdot, 1)$ на групу $(\mathbb{R}, +, 0)$. Дійсно,
$$\ln(x \cdot y) = \ln x + \ln y.$$
3. Функція $\varphi(a + bi) = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$ є ізоморфізмом групи $(\mathbb{C}, \cdot, 0)$, де $\mathbb{C}$ – комплексні числа, на групу матриць $\left\{\begin{pmatrix} a & -b \\ b & a \end{pmatrix}, +, \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}\right\}$, де $a, b \in \mathbb{R}$, а $+$ – операція додавання матриць.
4. Функція $\varphi(a + bi) = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$ є ізоморфізмом групи $(\mathbb{C}, \cdot, 1)$, де $\mathbb{C}$ – комплексні числа, на групу матриць $\left\{\begin{pmatrix} a & -b \\ b & a \end{pmatrix}, \times, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right\}$, де $a, b \in \mathbb{R}$, а $\times$ – операція множення матриць.

Вправа 2.3. Навести свої приклади гомоморфізмів та ізоморфізмів та автоморфізмів.

Квазігрупи

Латинський квадрат n-го порядку – це таблиця $L = (l_{ij})$ розміру $n \times n$, заповнена n елементами множини M таким чином, що в кожному рядку і в кожному стовпці таблиці кожен елемент з M зустрічається рівно один раз.

Означення 2.4. *Квазігрупою називається оператив* $(X,*)$, *такий що* $\forall a, b \in X$, *існує єдиний* $x \in X$ *такий, що* $a * x = b$ *та існує єдиний* $y \in X$ *такий, що* $y * a = b$.

Будь-латинський квадрат є таблицею множення (таблицею Келі) квазігрупи.

Зауваження 2.1. Слід відзначити, що означення квазігрупи не передбачає існування нейтрального елементу.

Приклади

1. $(\mathbb{Z}, -)$, $(\mathbb{R}^*, :)$ – квазігрупи без нейтрального елементу (існує тільки правий нейтральний елемент).
2. $(2^X, \Delta)$ – квазігрупа з нейтральним елементом $\emptyset$.

Вправа 2.4. Переконайтесь, що $(2^X, \Delta)$ – квазігрупа.

Вправа 2.5. Наведіть свої приклади квазігруп, у яких не існує нейтрольного елементу.

Твердження 2.1. *Якщо* $(X,*)$ *– півгрупа і квазігрупа, то* $(X,*)$ *– група.*

Доведення. Нехай $x \in X$, тоді за означенням 2.4 існує і єдиний $e \in X$ такий, що $e * x = x$. Звідки $(x * e) * x = x * (e * x) = x * x$. Позначимо $a = x * x$. Із єдності розв'язку

$$(x * e) * x = a = x * x$$

випливає, що $x * e = x$.

Аналогічно, для $\forall y \in X$, маємо $(y * e) * x = y * (e * x) = y * x$. Позначимо $b = y * x$. Із єдності розв'язку $(y * e) * x = b = y * x$. Звідки $y * e = y$.

Отже, e – нейтральний елемент. Залишилось довести існування оберненого для кожного елемента множини X.

Розглянемо довільне $a \in X$. Рівняння $a * x = e$ має розв'язок $x = a_r^{-1}$, а рівняння $x * a = e$ має розв'язок $x = a_l^{-1}$. Звідки, з урахуванням асоціативності $a_r^{-1} = a_l^{-1} = a^{-1}$.

Отже, $\forall a \in X$ існує обернений a^{-1}.

ЛЕКЦІЯ 3. **ПІДГРУПА. СИМЕТРИЧНА ГРУПА. ЦИКЛІЧНІ ГРУПИ**

Означення 3.1. *Підгрупою групи* $(G,*)$ *називається група* $(H,*)$ *щодо тої ж операції* $*$*, де* $H \subset G$.

Позначається $H < G$.

Очевидно, що кожна група $(G,*,e)$ в якості півгрупи має $(e,*,e)$, тобто групу, яка складається тільки з нейтрального елементу e.

Приклади

1. $(\mathbb{R}_{>0},\cdot)$ – підгрупа групи $(\mathbb{R}^*,\cdot)$;
2. $(\mathbb{P},+,0)$ ($\mathbb{P}$ – множина парних цілих чисел) є підгрупа групи $(\mathbb{Z},+,0)$.

Вправа 3.1. Навести свої приклади підгруп.

Теорема 3.1. *Нехай* $H \subset G$ *– непорожня підмножина, де* $(G,*,e)$ *– група.* Для того, щоб $(H,*)$ була б підгрупою групи $(G,*,e)$, необхідно і достатньо, щоб:

1. $\forall x,y \in H, x * y \in H$;
2. $\forall x \in H, x^{-1} \in H$.

Доведення. Необхідність очевидна.

Достатність. Асоціативність $*$ випливає із того, що $(G,*,e)$ – група. Оскільки $\forall x \in H, e = x * x^{-1} \in H$. Отже, $(H,*,e)$ – група, а, значить, півгрупа групи $(G,*,e)$.

Симетрична група

Нехай M – скінченна множина, що містить n елементів. Для спрощення викладок припустимо, що $M = \{1,2,\dots,n\}$. Перестановкою (або підстановкою) множини M називається довільна бієкція $\varphi: M \to M$.

Очевидно, що існує $n!$ перестановок множини M. Нехай φ та ψ перестановки множини M.

Множенням або композицією перестановок φ та ψ називається перетворення $\varphi \circ \psi: M \to M$ таке, що $\forall k \in M$

$$\varphi \circ \psi(k) = \varphi\big(\psi(k)\big).$$

Твердження 3.1. *Множенням перестановок φ та ψ множини M є перестановкою множини M.*

Доведення. Покажемо, що $\varphi \circ \psi$ є ін'єкцією. Дійсно, якщо $k, l \in M$ і $k \neq l$, то $\psi(k) \neq \psi(l)$, звідки $\varphi\big(\psi(k)\big) \neq \varphi\big(\psi(l)\big)$, тобто $\varphi \circ \psi$ інєкцієя.

Залишилось довести, що $\varphi \circ \psi$ сюр'єкція. Нехай $m \in M$, тоді, оскільки ψ бієкція існує $l \in M$ таке, що $\psi(l) = m$. Аналогічно існує $k \in M$ таке, що $\varphi(k) = l$. Звідки випливає, що $\varphi\big(\psi(k)\big) = m$ і, отже, $\varphi \circ \psi$ є бієкцією, тобто перестановкою множини M.

Означення 3.1. *Множенням $\circ$ перестановок φ* та *ψ називається перестановка $\varphi \circ \psi: M \to M$.*

Особливе місце займає тотожна перестановка ε, яка кожен елемент множини M переводить в самого себе, тобто $\forall k \in M\ \varepsilon(k) = k$. Легко бачити, що для довільної перестановки φ множини M має місце

$$\varphi \circ \varepsilon = \varepsilon \circ \varphi = \varphi.$$

Отже, ε – нейтральний елемент операції $\circ$.

Із математичного аналізу добре відомо, що бієкція має обернене відображення, яке також є бієкцією. Припустимо, що перестановка φ множини M задається

формулою $\varphi(k) = i_k$, $k = 1, \dots, n$. Оберненою перестановкою до перестановки φ називається перестановка

$$\varphi^{-1}(i_k) = k.$$

Неважко переконатись, що

$$\varphi \circ \varphi^{-1} = \varphi^{-1} \circ \varphi = \varepsilon.$$

Вправа 3.1. Довести, що операція композиція перестановок асоціативна та некомутативна.

Позначимо через $S(M)$ – множину усіх перестановок скінченної множини M.

Означення 3.2. *Симетричною групою (або групою підстановок (перестановок)) називається група* $(S(M), \circ, \varepsilon)$.

У випадку, коли $|M| = n$, симетричну групу позначають через S_n.

Якщо n невелике, елементи групи S_n зручно зображати у вигляді таблиць. Наприклад, при $n = 3$

$$\varepsilon = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \varphi_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \varphi_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \varphi_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix},$$

$$\varphi_4 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 1 \end{pmatrix}, \varphi_5 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}.$$

Для довільного випадку підстановка $\varphi(k) = i_k$, $k = 1, \dots, n$ записується так

$$\varphi = \begin{pmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix}.$$

Для запису оберненої до φ підстановки φ^{-1} у вигляді таблиці спочатку записуємо

$$\varphi^{-1} = \begin{pmatrix} i_1 & i_2 & \dots & i_n \\ 1 & 2 & \dots & n \end{pmatrix},$$

а далі впорядковуємо верхній рядок у порядку зростання і переписуємо відповідно елементи нижнього рядка. Переконайтесь, що так виписана φ^{-1} дійсно має властивості оберненого елемента.

Крім табличного зображення, при записі підстановок зручно користуватись розкладанням на цикли. Циклом довжиною k називається підстановка, при повторенні якої щонайменше k разів кожен з її символів переходить у себе. Цикл φ довжиною k такий , що $\varphi(i_m) = i_{m+1}, m < k$, $\varphi(i_k) = i_1$, а для всіх $i \in M\backslash\{i_1, \dots, i_k\}$: $\varphi(i) = i$, записується так

$$(i_1 \quad i_2 \quad \dots \quad i_k).$$

Відзначимо, що такий запис циклу не єдиний, наприклад, легко бачити, що

$$(i_1 \quad i_2 \quad \dots \quad i_k) = (i_k \quad i_1 \quad \dots \quad i_{k-1}).$$

Зокрема, підстановка $\varphi = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ є циклом довжиною 3. Такий цикл зображується у вигляді аналогічних записів

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (1 \quad 2 \quad 3) = (3 \quad 1 \quad 2) = (2 \quad 3 \quad 1)$$

Твердження 3.2. *Будь-яка підстановка розкладається у добуток циклів, що не перетинаються.*

Доведення. Нехай $\varphi \in S(M)$.

Якщо для деякого $i_1 \in M$, $\varphi(i_1) = i_2$ і при цьому $i_2 = i_1$, то маємо цикл (i_1) довжиною 1.

Якщо ж $i_2 \neq i_1$, але $\varphi(i_2) = i_3 = i_1$, то маємо цикл (i_1, i_2) довжиною 2.

Якщо $i_3 \neq i_1$, але $\varphi(i_3) = i_4 = i_1$, то маємо цикл (i_1, i_2, i_3) довжиною 3.

Оскільки $|M| = n \in \mathbb{N}$, то продовжуючи цю процедуру за якогось $k \leq n$ ми вперше отримаємо $\varphi(i_k) = i_1$ і матимем цикл $(i_1 \quad i_2 \quad \dots \quad i_k)$ довжиною k. Далі беремо елемент, який не потрапив у цей цикл і, застосовуючи ті ж

міркування, отримаємо зображення підстановки φ у вигляді добутку циклів, які не мають спільних елементів.

Приклад

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix} = (1 \quad 2 \quad 3)(4 \quad 5).$$

Відзначимо, що добуток незалежних циклів (циклів, які не перетинаються) комутативний, наприклад,

$$(1 \quad 2 \quad 3)(4 \quad 5) = (4 \quad 5)(1 \quad 2 \quad 3).$$

Вправа 3.2. Переконайтесь, що у загальному випадку добуток незалежних циклів комутативний.

Підстановка, при якій рівно два числа переходять одне в інше, а всі інші не змінюються називається транспозицією. Легко переконатись, що транспозиція – це цикл довжиною 2.

Будь-який цикл може бути зображений у вигляді добутку транспозицій причому не єдиним чином. Наприклад,

$$\begin{aligned}(i_1 \quad i_2 \quad \dots \quad i_k) &= (i_{k-1}i_k)(i_{k-2}i_{k-1}) \dots (i_3 i_2)(i_1 i_2) \\ &= (i_1 i_2)(i_1 i_3) \dots (i_1 i_{n-1})(i_1 i_n) = (i_1 i_n)(i_2 i_n) \dots (i_{n-1} i_n).\end{aligned} \tag{3.1}$$

Твердження 3.3. *Будь-яка підстановка розкладається у добуток транспозицій.*

Доведення. Це твердження є наслідком рівності (3.1) та твердження 3.2

Розглянемо приклад зображення підстановки у вигляді добутку транспозицій:

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = (1 \quad 3)(1 \quad 2) = (2 \quad 3)(1 \quad 3).$$

При усіх розкладах підстановки у вигляді добутку транспозицій парність числа цих транспозицій є однією і тою ж, і ця парність називається парністю підстановки.

Вправа 3.3. Довести, що $D_6 \cong S_3$, тобто діедральна група трикутника (див. вправу 2.2) ізоморфна симетричній групі S_3.

Теорема Келі

Нехай A – деяка непорожня множина. Аналогічно тому, як було показано для випадку симетричної групи, можна показати, що множина $\mathrm{Aut}(A)$ усіх бієктивних відображень множини A у себе є групою відносно операції композиції $\circ$ відображень, тобто $\forall f, g \in \mathrm{Aut}(A), \forall a \in A\ (f \circ g)(a) = f\big(g(a)\big)$. Нейтральним елементом цієї групи є тотожнє відображення id_A множини A в себе. Очевидно, що якщо $A = \{1,2, \dots, n\}$, то $\mathrm{Aut}(A) = S_n$.

Теорема 3.2 (Келі). *Нехай* $(G,*,e)$ *– група. Тоді* $(G,*,e)$ *ізоморфна деякій підгрупі групи* $(\mathrm{Aut}(G),\circ,\mathrm{id}_G)$.

Доведення. Зафіксуємо довільне $g \in G$ і нехай відображення $\psi_g: G \to G$ таке, що $\psi_g(x) = g * x$, $\forall x \in G$. Доведемо, що ψ_g є автоморфізмом на G (тобто $\psi_g \in \mathrm{Aut}(G)$). Спочатку покажемо, що ψ_g – сюр'єкція. Дійсно, для будь-якого $y \in G$ при $x = g^{-1} * y \ \in G$ маємо $\psi_g(x) = g * (g^{-1} * y\ ) = y$.

Тепер покажемо, що ψ_g – ін'єкція. Нехай $x_1, x_2 \in G$ і при цьому $x_1 \neq x_2$, тоді, якби $\psi_g(x_1) \neq \psi_g(x_1)$ тому, що в протилежному випадку ми мали б рівність $g * x_1 = g * x_2$ звідки $x_1 = x_2$, що суперечить припущенню.

Отже, $\psi_g: G \to G$ – бієкція, а, значить автоморфізм. Звідки

$$H = \{\psi_g | g \in G\} \subset \mathrm{Aut}(G).$$

Тепер визначимо

$$\varphi: G \to H: g \overset{\varphi}{\to} \psi_g.$$

Очевидно, що $\varphi: G \to H$ бієкція, оскільки різним $g_1, g_2 \in G$ відповідають різні ψ_{g_1}, ψ_{g_2} і φ – сюр'єкція за визначенням. Покажемо, що φ гомоморфізмом. Дійсно, $\forall x \in G, g_1, g_2 \in G$ маємо

$$\varphi(g_2 * g_1)(x) = \psi_{g_2 g_1}(x) = (g_2 * g_1) * x = g_2 * (g_1 * x) = \psi_{g_2}(x)\left(\psi_{g_1}(x)\right)$$
$$= \left(\psi_{g_2} \circ \psi_{g_1}\right)(x) = \left(\varphi(g_2) \circ \varphi(g_1)\right)(x).$$

Отже, $\varphi(g_2 * g_1) = \varphi(g_2) \circ \varphi(g_1)$, тобто $\varphi: G \to H$ – ізоморфізм.

Циклічні групи

Нехай $(G,*,e)$ – група, а $g \in G$ деякий її елемент. Через $g^n, n \in \mathbb{N}$ будемо позначати елемент $\underbrace{g * g * \ldots * g}_{n \text{ разів}}$, а через g^{-n} – елемент, симетричний до g^n.

Вправа 3.4. Показати, що $g^{-n} = \underbrace{g^{-1} * g^{-1} * \ldots * g^{-1}}_{n \text{ разів}}$.

Підмножину елементів G, що складається із $g^0 = e, g, g^{-1}, g^2, g^{-2}, \ldots$ позначимо через $\langle g \rangle$. Структура $(\langle g \rangle,*,e)$ є підгрупою групи $(G,*,e)$.

Дійсно, якщо $g^l, g^m \in \langle g \rangle$, то $g^l * g^m = g^{l+m} \in \langle g \rangle$, а із $g^m \in \langle g \rangle$ випливає $g^{-m} \in \langle g \rangle$.

При цьому група $(\langle g \rangle,\circ,e)$ називається породженою твірним елементом g, а її порядок *порядком* елемента g.

Означення 3.2. *Група $(G,*,e)$ називається циклічною, якщо існує $g \in G$ такий, що $\langle g \rangle = G$, тобто $G = \{g^n | n \in \mathbb{Z}\}$.*

Іншими словами, *група називається циклічною, якщо вона збігається з однією із своїх циклічних підгруп.*

Вправа 3.5. Нехай $(G,*,e)$ – циклічна група, довести, що вона абелева.

Зауваження. У наведеному вище означенні циклічної групи було використано мультиплікативну термінологію. В адитивній термінології циклічна група, породжена елементом g записується так:

$$G = \langle g \rangle = \{ng | n \in \mathbb{Z}\}.$$

Приклади

1. $(\mathbb{Z}, +, 0)$ – циклічна адитивна група нескінченного порядку;
2. Нехай $(G, *, e)$ – група, причому $G = e$. Тоді $(G, *, e)$ циклічна група порядку 1.
3. Множина комплексних коренів n-го степеню із 1: $e^{\frac{2\pi k}{n}}$, $k = 0,1, \dots, n-1$ з операцією множення комплексних чисел – циклічна група порядку n.

Вправа 3.6. Навести власні приклади циклічних груп та вказати їх твірні елементи.

ЛЕКЦІЯ 4. СУМІЖНІ КЛАСИ. ТЕОРЕМА ЛАГРАНЖА

Означення 4.1. *Якщо $(H, *, e)$ – підгупа групи $(G, *, e)$, то правими суміжними класами суміжності за підгрупою H називаються множини*

$$Hg = \{h * g | h \in H\}, \qquad g \in G.$$

Відповідно лівими суміжними класами суміжності за підгрупою H називаються множини

$$gH = \{g * h | h \in H\}, \qquad g \in G.$$

Будь-який елемент суміжного класу (правого чи лівого) називається представником цього класу.

Твердження 4.1. *Нехай a і b представники правого суміжного класу Hg, тобто $a \in Hg$ і $b \in Hg$. Тоді $a * b^{-1} \in H$.*

Доведення. Оскільки $a \in Hg$, то $\exists h_1 \in H$, такий що $a = h_1 * g$. Аналогічно $\exists h_2 \in H$, такий що $b = h_2 * g$. Звідки

$$a * b^{-1} = (h_1 * g) * (g^{-1} * h_2^{-1}) = h_1 * h_2^{-1} \in H.$$

Вправа 4.1. Довести, що коли a і b представники лівого суміжного класу gH, тобто $a \in gH$ і $b \in gH$, то $a^{-1} * b \in H$.

На групі $(G,*,e)$ введемо відношення $\sim_R$ пов'язане з підгрупою $(H,*,e)$ для правого суміжного класу Hg:

$$a \sim_R b \Leftrightarrow a * b^{-1} \in H$$

та для лівого суміжного класу gH:

$$a \sim_L b \Leftrightarrow a^{-1} * b \in H.$$

Вправа 4.2. Довести, що відношення $\sim_R$ та $\sim_L$ є відношеннями еквівалентності на G, а, отже, розбивають G на класи еквівалентності, що не перетинаються.

Твердження 4.2. *Класи еквівалентності відношення $\sim_R$ є правими класами суміжності за підгрупою H.*

Доведення. Дійсно, якщо $a \sim_R b$, то $a * b^{-1} \in H$, тобто $\exists h \in H$ таке, що $h = a * b^{-1}$ або $a = h * b$. Звідки $a \in Hb$ і, оскільки $b = e * b$, то $b \in Hb$.

Вправа 4.3. Нехай $H_1, H_2, \dots, H_n$ – класи еквівалентності відношення $\sim_L$. Показати, що якщо $a_i \in H_i$, $i = 1,2, \dots, n$, то $H_i = a_i H$, тобто класи еквівалентності відношення $\sim_L$ є лівими класами суміжності за підгрупою H. А також, що коли $H_1, H_2, \dots, H_n$ – класи еквівалентності відношення $\sim_R$, тоді, якщо $a_i \in H_i$, $i = 1,2, \dots, n$, то $H_i = H a_i$.

Теорема 4.1. *Нехай група $(G,*)$ — скінченна, тобто $|G| < +\infty$. Тоді*

I. *Якщо $H, H_1, H_2, \dots, H_n$ – класи еквівалентності відношення $\sim_L$ і $a_i \in H_i$, $i = 1,2, \dots, n$,* то

$$G = H \sqcup a_1 H \sqcup a_2 H \sqcup \dots \sqcup a_n H,$$

де знак $\sqcup$ *означає об'єднання множин, які не перетинаються.*

II. Якщо $H, H_1, H_{2,\dots}, H_n$ *– класи еквівалентності відношення* $\sim_R$ *і* $a_i \in H_i$, $i = 1,2, \dots, n$, то

$$G = H \sqcup Ha_1 \sqcup Ha_2 \sqcup \dots \sqcup Ha_n.$$

Доведення. Покажемо, що справедлива частина I. Дійсно, із того, що

$$G = H \sqcup H_1 \sqcup H_2 \sqcup \dots \sqcup H_n$$

та вправи 4.3 ($H_i = a_i H, i = 1, \dots, n$) випливає доведення теореми. Частина II доводиться аналогічно.

Твердження 4.2. *Будь-який клас суміжності* (*правий чи лівий*) *за підгрупою* H *містить* $|H|$ *елементів.*

Доведення. Для будь-якого представника g правого класу суміжності Hg за підгрупою H відображення $f: H \ni h \xrightarrow{f} h * g \in Hg$ є бієктивним (взаємно однозначним відображенням H на всю множину Hg). Дійсно, для всіх $h_1, h_2 \in Hg$ таких, що $h_1 \neq h_2$ маємо, що $h_1 * g \neq h_2 * g$. Крім цього, із означення правого класу суміжності Hg випливає, що f відображає H на всю множину Hg. Отже, H та Hg мають однакову потужність, тобто $|Hg| = |H|$.

Для лівого класу суміжності gH твердження доводиться аналогічно.

Теорема 4.2 (Лагранж). *Для будь-якої скінченної групи* $(G,*)$ *її порядок* $|G|$ *ділиться на порядок* $|H|$ *підгрупи* $(H,*)$ *цієї групи.*

Доведення. Нехай $|G| = k$, а $|H| = m$. Тоді, за твердженням 4.2, будь-який суміжний клас (правий чи лівий) містить рівно m. Якщо таких класів l, то за теоремою 4.1, $k = ml$.

Якщо група комутативна, то очевидно, що її праві та ліві класи суміжності збігаються. Для некомутативних груп у загальному випадку такі об'єкти відрізняються.

ЛЕКЦІЯ 5. **ФАКТОРГРУПА. РОЗВ'ЯЗУВАНА ГРУПА**

Означення 5.1. *Якщо* $(H,*)$ *підгрупа групи* $(G,*)$ *така, що праві і ліві суміжні класи за підгрупою* H *збігаються, тобто* $Hg = gH$ *для всіх* $g \in G$*, то* $(H,*)$ *називається нормальним дільником групи* $(G,*)$.

Позначається $H \lhd G$.

Твердження 5.1. *Підгрупа* $(H,*)$ *є нормальним дільником групи* $(G,*)$ *тоді і тільки тоді, коли* $\forall g \in G$ *та* $\forall h \in H$ *маємо*

$$g^{-1}hg \in H.$$

Зауваження 5.1. Для скорочення запису, як і при множенні чисел знак $*$ між символами опускаємо, тобто hg – це $h * g$.

Доведення. Достатність. Нехай $\forall g \in G \ \ та \ \ \forall h \in H \ \ g^{-1}hg \in H$. Звідси випливає, що $hg \in gH$. З іншого боку, $hg \in Hg$ і оскільки це виконується для $\forall h \in H$, то для фіксованого $g \in G$, $Hg = gH$. Далі, оскільки з попереднього $Hg = gH$ для будь-якого $g \in G$, то $(H,*)$ – нормальний дільник $(G,*)$.

Необхідність. Нехай підгрупа $(H,*)$ є нормальним дільником групи $(G,*)$. Тоді $Hg = gH$ для всіх $g \in G$. Звідки $\forall g \in G$ та $\forall h \in H$ існує $h_1 \in H$ таке, що $hg = gh_1$, тобто $g^{-1}hg = h_1 \in H$. Отже, $\forall g \in G$ та $\forall h \in H$ маємо $g^{-1}hg \in H$.

Нехай $(H,*)$ є нормальним дільником групи $(G,*)$. На класах суміжності g_1H та g_2H введемо операцію g_1Hg_2H, яка є множиною всіх добутків елементів із g_1H на елементи g_2H, тобто

$$g_1Hg_2H := \{xy | x \in g_1H, y \in g_2H\}. \qquad (5.1)$$

Оскільки $(H,*)$ – нормальний дільник, то неважко переконатись, що

$$(g_1H)(g_2H) = g_1g_2H.$$

Дійсно,

$$g_1h_1g_2h_2 = g_1(g_2g_2^{-1})h_1g_2h_2 = g_1g_2(g_2^{-1}h_1g_2)h_2 = g_1g_2h_1'h_2 = g_1g_2h,$$

де $g_2^{-1}h_1g_2 = h_1' \in H$.

Враховуючи це, неважко переконатись, що операція $g_1H * g_2H$ є груповою, тобто вона асоціативна, в якості нейтрального елементу виступає множина H та для будь-якого gH існує обернений $g^{-1}H$.

Означення 5.2. *Множина класів суміжності gH за нормальним дільником $(H,*)$ групи $(G,*)$ з операцією (5.1) називається фактор-групою.*

Позначається G/H.

Означення 5.3. *Відображення $\varphi: G \to G/H$ таке, що $\varphi(g) = gH$, $\forall g \in G$ є гомоморфізмом, який називається канонічним.*

Легко бачити, що ядро цього канонічного гомоморфізму є група H.

Позначимо через e – групу $(e,*,e)$, тобто групу, яка складається тільки з нейтрального елементу e, а через G_i – групи $(G_i,*,e)$, які є підгрупами групи $(G,*,e)$.

Означення 5.4. *Група $(G,*)$ називається розв'язуваною, якщо існує скінченна зростаюча послідовність $e = G_0 \lhd G_1 \lhd \cdots \lhd G_k = G$, де*

1. *G_{i-1} – нормальна підгрупа групи G_i, $i = 1, \dots, k$;*
2. *Фактор групи G_i/G_{i-1} – абелеві, $i = 1, \dots, k$.*

ЛЕКЦІЯ 6. **КІЛЬЦЕ. ПРИКЛАДИ КІЛЕЦЬ**

Означення 6.1. *Множина $\mathcal{R} \neq \emptyset$ називається кільцем, якщо на ній визначені дві операції: додавання $+: \mathcal{R} \times \mathcal{R} \to \mathcal{R}$ та множення $\circ: \mathcal{R} \times \mathcal{R} \to \mathcal{R}$, причому $(\mathcal{R}, +)$ – абелева група, тобто*

a) $\forall x, y \in \mathcal{R},\ x + y = y + x$;

b) $\forall x, y, z \in \mathcal{R},\ (x + y) + z = x + (y + z)$;

c) $\exists 0 \in \mathcal{R}: \forall x \in \mathcal{R},\ x + 0 = x$;

d) $\forall x \in \mathcal{R}\ \exists(-x) \in \mathcal{R}:,\ x + (-x) = 0$;

і, крім цього, виконуються операції дистрибутивності:

$$x \circ (y + z) = x \circ y + x \circ z;$$

$$(x + y) \circ z = x \circ z + y \circ z.$$

Елемент 0 називається нейтральним елементом за додаванням (або нулем), а елемент $(-x)$ називається протилежним елементом до x.

Кільце позначається так: $(\mathcal{R}, +, \circ)$, або просто через $\mathcal{R}$, якщо операції додавання і множення на $\mathcal{R}$ не потребують уточнення.

Якщо множення $\circ$ асоціативне, тобто $x \circ (y \circ z) = (x \circ y) \circ z$, то кільце $(\mathcal{R}, +, \circ)$ називається *асоціативним*.

Твердження 6.1. $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ *– кільце, яке називається кільцем лишків за модулем* $n \in \mathbb{Z}$.

Доведення випливає із властивостей a) – f) операцій додавання і множення на $\mathbb{Z}/n\mathbb{Z}$ (див. Лекція 3).

Приклади

1. $(\mathbb{Z}, +, \cdot)$ – асоціативне кільце цілих чисел.
2. $(\mathbb{P}, +, \cdot)$ – асоціативне кільце парних чисел.
3. $(\mathbb{R}, +, \cdot)$ – асоціативне кільце дійсних чисел.
4. $(2^X, \Delta, \cap)$, (де операція симетричної різниці Δ виступає в якості додавання, а перетин $\cap$ – в якості множення) –Булеве кільце.
5. $(M_{n\times n}(\mathbb{R}), +, \cdot)$ (де $M_{n\times n}(\mathbb{R})$ – множина дійсних матриць розміру $n \times n$) – асоціативне кільце матриць.
6. Кільце чисел $\left(\mathbb{Z}\left[\frac{1}{2}\right], +, \cdot\right)$, де $\mathbb{Z}\left[\frac{1}{2}\right] = \left\{\frac{n}{2^m}, m, n \in \mathbb{N}\right\}$.
7. Кільце подвійних чисел $\{a + b\boldsymbol{e} | a, b \in \mathbb{R}, \boldsymbol{e}^2 = 1\}$. Додавання покоординатне, а множення має вигляд:

$$(a + b\boldsymbol{e})(c + d\boldsymbol{e}) = ac + bd + (ad + bc)\boldsymbol{e}.$$

8. $(V, +, \times)$ (V – множина векторів простору з операціями додавання та векторного добутку) – неасоціативне кільце, оскільки у загальному випадку

$$(\vec{a} \times \vec{b}) \times \vec{c} \neq \vec{a} \times (\vec{b} \times \vec{c}).$$

9. Кільце дуальних чисел $\{a + b\boldsymbol{\varepsilon} | a, b \in \mathbb{R}, \boldsymbol{\varepsilon}^2 = 0\}$. Додавання по координатне, а множення має вигляд: $(a + b\boldsymbol{\varepsilon})(c + d\boldsymbol{\varepsilon}) = ac + (ad + bc)\boldsymbol{\varepsilon}$.

10. Кільце функцій $f: \mathbb{R} \to \mathbb{R}$ з поточковим додаванням і множенням.

11. $\mathbb{Z}/n\mathbb{Z}$ ($\mathbb{Z}_n$) – кільце класів лишків за модулем n. $\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \dots, \overline{n-1}\}$, де $\bar{k} = \{k + mn | \, m \in \mathbb{N}\}$. $\bar{k} + \bar{l} = \overline{k+l}$, $\bar{k} \cdot \bar{l} = \overline{kl}$.

12. Нехай $(\mathcal{R}, +, \cdot)$ комутативне асоціативне кільце. Через $\mathcal{R}[x]$ позначають кільце многочленів $a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$, де $a_i \in \mathcal{R}$, із звичайними операціями додавання і множення многочленів.

Означення 6.2. *Якщо в кільці існує елемент* $1 \in \mathcal{R}$, *такий що* $\forall x \in \mathcal{R}$,

$$x \circ 1 = x = 1 \circ x,$$

тоді $(\mathcal{R}, +, \circ)$ *називається кільцем з одиницею*, *а* 1 *– нейтральним елементом або одиницею за множенням.*

Означення 6.3. *Якщо множення* $\circ$ *комутативне, то* $(\mathcal{R}, +, \circ)$ *називається комутативним кільцем*.

Як правило, під комутативним кільцем розуміють комутативне асоціативне кільце з одиницею.

Вправа 6.1. Які із наведених вище прикладів кілець є кільцями з одиницею?

Кілець нескінченно багато*

Цей пункт може бути пропущеним, якщо невідомі такі поняття як *потужність* множини, *зліченність*, *континуум*.

Постає питання: кількість кілець скінченна чи нескінченна? Відповідь – кілець нескінченно багато причому потужність множини кілець не менш ніж континуальна.

Нехай $S \subset \mathbb{P} = \{2,3,5,7, \dots\}$ підмножина множини простих чисел. Розглянемо множину:

$$R_S = \left\{ \frac{m}{\prod_{p \in S} p^{l_p}} \mid m \in \mathbb{Z}, l_p \in \mathbb{N}_0 \right\}.$$

Легко перевірити, що $(R_S, +, \cdot)$ (тут " $+$ " , " $\cdot$ " – відповідно операції додавання і множення дійсних чисел) є кільцем.

Звідки випливає, що кілець існує нескінченно багато, а саме, кількість підмножин натуральних чисел (континуум)

$$|\mathbb{P}| = |\mathbb{N}| = \aleph_0$$

$$\left|2^{\mathbb{P}}\right| = \aleph_1 = c.$$

Пряма сума кілець

Означення 6.4. *Нехай* $(R, +, \circ)$, $(S, \boxplus, *)$ *два кільця. Прямою сумою цих кілець називається кільце* $(R \oplus S, +, \cdot)$, *де* $R \oplus S = \{(x, y) | x \in R, y \in S\}$, *на якій задані операції:*

$$(x_1, y_1) + (x_2, y_2) = (x_1 + x_2, y_1 \boxplus y_2),$$

$$(x_1, y_1) \cdot (x_2, y_2) = (x_1 \circ x_2, y_1 * y_2).$$

Неважко переконатись, що нейтральним елементом операції додавання є

$$0_{R \oplus S} = (0_R, 0_S),$$

а нейтральним елементом операції множення є

$$1_{R \oplus S} = (1_R, 1_S).$$

Вправа 6.2. Перевірити, що $(R \oplus S, +, \cdot)$ є кільцем.

Означення 6.5. *Нехай* $(R,+,\cdot)$ *кільце. Протилежним кільцем називається кільце* $(R^0,+,\circ)$*, де* $R^0 = R$*, а операція* $\circ$ *визначається так:*

$$x \circ y = y \cdot x.$$

Вправа 6.3. Навести приклади кілець, протилежні кільця до яких відрізняються від самих кілець.

Приєднання одиниці

Нехай $(R,+,\cdot)$ – кільце без одиниці. Розглянемо множину $\mathbb{Z} \times R$:

$$\mathbb{Z} \times R = \{(x,y) | x \in \mathbb{Z}, y \in R\}.$$

На множині $\mathbb{Z} \times R$ введемо операції додавання і множення:

$$(m,x) + (n,y) = (m+n, x+y),$$

$$(m,x) \cdot (n,y) = (mn, nx + my + x \cdot y).$$

Тут $mx = \underbrace{x + x + \cdots + x}_{m}$, $0x = \mathbf{0}$, $\mathbf{0} \in R$, $m\mathbf{0} = \mathbf{0}$, $(-1)x = -x$, $(-2)x = 2(-x)$.

Легко переконатись, що структура $(\mathbb{Z} \times R,+,\cdot)$ є кільцем, причому у такому кільці одиниця це $(1,\mathbf{0})$. Дійсно,

$$(m,x) \cdot (1,\mathbf{0}) = (m, 1x + m \cdot \mathbf{0} + x \cdot \mathbf{0}) = (m,x),$$

$$(1,\mathbf{0}) \cdot (n,y) = (n, n \cdot \mathbf{0} + 1y + \mathbf{0} \cdot y) = (n,y).$$

Означення 6.6. *Кільце* $(L,+,\otimes)$ *називається кільцем Лі, якщо для множення виконуються умови:*

1. $\forall x \in L,\ \ x \otimes x = 0,$
2. $\forall x,y,z \in L$

$$(x \otimes y) \otimes z + (y \otimes z) \otimes x + (z \otimes x) \otimes y = 0. \qquad (6.1)$$

Співвідношення (6.1) називається *тотожністю Якобі*.

Із умови 1 випливає, що $\forall x, y \in L, x \otimes y = -y \otimes x$.

ЛЕКЦІЯ 7. **ПІДКІЛЬЦЕ. ОБЛАСТЬ ЦІЛІСНОСТІ.**

Підкільце. Критерій підкільця

Нехай $(\mathcal{R}, +, \cdot)$ – кільце.

Означення 7.1. *Підкільцем кільця* $(\mathcal{R}, +, \cdot)$ *називається кільце* $(\mathcal{R}_1, +, \cdot)$, для якого $\mathcal{R}_1 \subset \mathcal{R}$, *а операції додавання та множення такі ж як у кільця* $(\mathcal{R}, +, \cdot)$.

Позначається $(\mathcal{R}_1, +, \cdot) \subset (\mathcal{R}, +, \cdot)$.

Теорема 7.1. (Критерій підкільця) *Нехай* $\emptyset \neq \mathcal{R}_1 \subset \mathcal{R}$. *Для того, щоб* $(\mathcal{R}_1, +, \cdot)$ *було підкільцем кільця* $(\mathcal{R}, +, \cdot)$ *необхідно і достатньо виконання умов*:

1) $\forall a, b \in \mathcal{R}_1 \Rightarrow a + b \in \mathcal{R}_1$,
2) $\forall a \in \mathcal{R}_1 \Rightarrow -a \in \mathcal{R}_1$,
3) $\forall a, b \in \mathcal{R}_1 \Rightarrow a \cdot b \in \mathcal{R}_1$.

Доведення. Необхідність випливає із означення кільця.

Достатність. З урахуванням умов 1), 2), легко переконатись, що $0 \in \mathcal{R}_1$ оскільки $0 = a + (-a) \in \mathcal{R}_1$. Асоціативність та комутативність додавання в $(\mathcal{R}_1, +)$ є наслідком асоціативності та комутативності додавання в $(\mathcal{R}, +)$. Отже, $(\mathcal{R}_1, +)$ – абелева група.

Дистрибутивність множення відносно додавання в $(\mathcal{R}_1, +, \cdot)$ є наслідком дистрибутивності в $(\mathcal{R}, +, \cdot)$.

Вправа 7.1. Довести, що умови 1) – 3) критерія підкільця можна замінити двома умовами:

1) $\forall a, b \in \mathcal{R}_1 \Rightarrow a - b \in \mathcal{R}_1$,
2) $\forall a, b \in \mathcal{R}_1 \Rightarrow a \cdot b \in \mathcal{R}_1$.

Приклади

1. Кільце раціональних чисел є підкільцем кільця дійсних чисел, а воно підкільце кільця комплексних чисел: $(\mathbb{Q}, +, \cdot) \subset (\mathbb{R}, +, \cdot)$.
2. Парні числа $2\mathbb{Z}$ є підкільцем кільця $\mathbb{Z}$, але без 1

$$(2\mathbb{Z}, +, \cdot) \subset (\mathbb{Z}, +, \cdot).$$

3. $\forall n \in \mathbb{N}$ $(n\mathbb{Z}, +, \cdot)$ є підкільцем кільця $(\mathbb{Z}, +, \cdot)$. Дійсно,

$$\forall m_1, m_2 \in \mathbb{Z}, \qquad m_1 n, m_2 n \in n\mathbb{Z},$$

$$m_1 n - m_2 n = (m_1 - m_2)n \in n\mathbb{Z},$$

$$m_1 n m_2 n = \big((m_1 m_2)n\big)n \in n\mathbb{Z}.$$

Вправа 7.2. Чи існують підкільця кільця $(\mathbb{Z}, +, \cdot)$, які відмінні від підкілець виду $(n\mathbb{Z}, +, \cdot)$?

Дільники нуля. Оборотні елементи

Нехай $(R, +, \cdot)$ кільце.

Означення 7.2. *Ненульовий елемент $a \in R$ називається правим (лівим) дільником нуля, якщо існує ненульовий елемент $b \in R$ такий, що $ba = 0$ ($ab = 0$). Елемент, який є одночасно правим і лівим дільником нуля називається дільником нуля.*

Означення 7.3. *Елемент $a \in R$ називається нільпотентом, якщо існує $n \in \mathbb{N}$ таке, що $a^n = 0$.*

Вправа 7.3. Довести, що нільпотент $a \neq 0$ є дільником нуля.

Означення 7.4. *Асоціативне комутативне кільце з одиницею, яке не містить дільників нуля називається областю цілісності.*

Приклади

1. $(\mathbb{Z}, +, \cdot)$,

2. $\mathbb{Z}[\sqrt{2}] = \{n + m\sqrt{2} \mid n, m \in \mathbb{Z}\}$,
3. $(\mathbb{Q}, +, \cdot)$,
4. $\mathbb{Z}/p\mathbb{Z}$, де p – просте число.

Означення 7.5. *Елемент $a \in R$ називається оборотним в кільці $(R, +, \cdot)$ з одиницею 1, якщо існує $a^{-1} \in R$ такий, що*

$$a \cdot a^{-1} = 1 = a^{-1} \cdot a.$$

Елемент a^{-1} називається оберненим до a.

Множину всіх оборотних елементів кільця $(R, +, \cdot)$ позначають R^*.

Теорема 7.2. *В асоціативному кільці $(R, +, \cdot)$ з одиницею 1 оборотний елемент не може бути ні правим, ні лівим дільником нуля.*

Доведення. Нехай $a \in R$ – оборотний і a^{-1} – обернений до a. Якщо припустити, що при цьому a, наприклад, правий дільник нуля, тобто, існує ненульовий елемент $b \in R$ такий, що $ba = 0$. Тоді

$$0 = 0 \cdot a^{-1} = (b \cdot a) \cdot a^{-1} = b \cdot (a \cdot a^{-1}) = b \cdot 1 = b,$$

що суперечить умові $b \neq 0$. Для лівого елемента нуля доведення аналогічне.

Зауважимо, що умова відсутності дільників нуля у кільці з одиницею не гарантує оберненість усіх ненульових елементів кільця. Наприклад, кільце $(\mathbb{Z}, +, \cdot)$ не містить дільників нуля, але крім 1 та -1, всі інші елементи цього кільця необоротні.

Закони скорочення в кільці $(R, +, \cdot)$:

$$\forall a, b, x \in R, \quad x \neq 0, \quad a \cdot x = b \cdot x \Leftrightarrow a = b, \quad \text{(праве скорочення)};$$

$$\forall a, b, x \in R, \quad x \neq 0, \quad x \cdot a = x \cdot b \Leftrightarrow a = b, \quad \text{(ліве скорочення)}.$$

Теорема 7.3. *У будь-якому кільці $(R, +, \cdot)$ праве і ліве скорочення виконується тоді і тільки тоді, коли це кільце не містить дільників нуля.*

Доведення. Необхідність випливає із того, що якщо $x \neq 0$ і $a \cdot x = b \cdot x$, то $(a - b) \cdot x = 0$ і, за умови, що $(R, +, \cdot)$ не містить дільників нуля, маємо $a - b = 0$, тобто $a = b$.

Якщо ж виконуються закони скорочення і $a \neq 0$, $b \neq 0$, $a \cdot b = 0$, то

$$0 = a \cdot b = a \cdot 0 \Rightarrow b = 0,$$

що суперечить умові $b \neq 0$.

Означення 7.6. *Булеве кільце – це асоціативне кільце:* $(\mathcal{R}, +, \circ)$*, таке що* $\forall x \in \mathcal{R}$, $x \circ x = x$.

Твердження 7.1. *Нехай* $(\mathcal{R}, +, \circ)$ - булеве кільце, тоді

1. $\forall\, x, y \in \mathcal{R},\ \ x \circ y = y \circ x$;
2. $\forall\, x \in \mathcal{R},\ \ x + x = 0$.

Доведення. Із означення випливає, що $(x + y) \circ (x + y) = x + y$, звідки

$$x \circ y + y \circ x = 0.$$

Підставивши $y = x$, отримаємо $x + x = 0$.

Далі, оскільки $x \circ y + y \circ x = 0$ та $x \circ y + x \circ y = 0$, то $x \circ y = y \circ x$.

Якщо у множині 2^X, $X \neq \emptyset$, в якості суми множин A і B взяти симетричну різницю $A + B \stackrel{\text{def}}{=} (A \setminus B) \cup (B \setminus A)$, а в якості добутку перетин $A \times B \stackrel{\text{def}}{=} A \cap B$, то отримаємо булеве кільце.

Інший приклад булевого кільця $\mathbb{Z}/2\mathbb{Z}$ $(\mathbb{Z}_2)$ – кільце класів лишків за модулем 2.

Пряма сума кілець

Нехай R, S два кільця

$$R \oplus S = \{(x, y) | x \in R, y \in S\},$$

$$(x_1, y_1) + (x_2, y_2) = (x_1 + x_2, y_1 + y_2),$$

$$(x_1, y_1) \cdot (x_2, y_2) = (x_1 \cdot x_2, y_1 \cdot y_2),$$

$$0_{R \oplus S} = (0_R, 0_S),$$

$$1_{R\oplus S} = (1_R, 1_S).$$

Протилежне кільце

Нехай $(R, +,\cdot)$ – кільце. Розглянемо множину з операціями $(R^o, +,\circ)$,

де $R^o = R$, $+$ така ж операція, як і в $(R, +,\cdot)$, а

$$x \circ y = y \cdot x.$$

Вправа 7.4. Переконайтесь, що $(R^o, +,\circ)$ також є кільцем.

Кільце $(R^o, +,\circ)$ називається протилежним до $(R, +,\cdot)$.

ЛЕКЦІЯ 8. **ІДЕАЛИ. ФАКТОР КІЛЬЦЕ**

Означення 8.1. *Підкільце I кільця $(R, +,\cdot)$ називається лівим ідеалом, якщо $\forall a \in I$, $\forall r \in R$ маємо $r \cdot a \in I$ $(RI \subset I)$. Аналогічно підкільце I кільця $(R, +,\cdot)$ називається правим ідеалом, якщо $\forall a \in I$, $\forall r \in R$ маємо $a \cdot r \in I$ $(IR \subset I)$.*

Підкільце I кільця $(R, +,\cdot)$ називається ідеалом, якщо I – лівий і правий ідеал одночасно.

Очевидно, що саме кільце $(R, +,\cdot)$ та нульове кільце $(0, +,\cdot)$ є ідеалами в $(R, +,\cdot)$, які називають тривіальними. Звичайно, інтерес становлять нетривіальні або власні ідеали кільця.

Твердження 8.1. *Непорожня множина $I \subset R$ є ідеалом тоді і тільки тоді, коли*

1. $\forall a, b \in I, a - b \in I;$
2. $\forall a \in I, \forall r \in R, r \cdot a \in I$ *і* $a \cdot r \in I.$

Доведення є прямим наслідком вправи 7.1.

Приклади

1. $n\mathbb{Z}$, де $n \in \mathbb{N}$ є ідеалом кільця $(\mathbb{Z}, +, \cdot)$.
2. Нехай $\mathbb{R}[x]$ – кільце многочленів над дійсними числами. Многочлени, які діляться на деякий ненульовий многочлен $p(x) \in \mathbb{R}[x]$ є ідеалом.

Твердження 8.2. *Перетин довільної кількості ідеалів деякого кільця є ідеалом.*

Доведення. Нехай I_α, $\alpha \in \mathrm{A}$ – набір ідеалів кільця $(R, +, \cdot)$. Розглянемо перетин цих ідеалів $I = \bigcap_{\alpha \in \mathrm{A}} I_\alpha$.

Нехай маємо довільні $a, b \in I$ та $r \in R$. Тоді $a, b \in I_\alpha$ та $a \cdot r \in I_\alpha$ для всіх $\alpha \in \mathrm{A}$. Звідки $a - b \in I$ та $a \cdot r \in I$, для $\forall a, b \in I$ та $\forall r \in R$. Отже, за твердженням 8.2 I – ідеал кільця $(R, +, \cdot)$.

Означення 8.2. *Нехай $(R, +, \cdot)$ – кільце і $S \subset R$. Ідеал(S) , який є перетином ідеалів кільця $(R, +, \cdot)$, що містять S*

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

називається ідеалом, породженим множиною S.

Легко бачити, що (S) є найменшим ідеалом, який містить S.

Якщо S – одноелементна множина, що складається з одного елемента a, то ідеал (S) позначають (a) і називають *головним ідеалом*, породженим елементом a. Якщо $(R, +, \cdot)$ – комутативне кільце, то неважко переконатись, що головний ідеал, породженим елементом a має вигляд

$$(a) = \{ar : r \in R\}.$$

Операції над ідеалами

Нехай I та J ідеали кільця $(R, +, \cdot)$.

Означення 8.3. *Сумою ідеалів I* та *J називається множина*

$$I + J = \{a + b : a \in I, b \in J\}.$$

Добутком ідеалів I та J *називається множина*

$$IJ = \left\{ \sum_{k=1}^{n} a_k b_k : a_k \in I, b_k \in J, \ \ n \in \mathbb{N} \right\}.$$

Твердження 8.3. *Нехай* I_k, $k = 1, \dots, n$ *– набір ідеалів кільця* $(R, +, \cdot)$. *Тоді*

1) $\sum_{k=1}^{n} I_k$ *та* $\prod_{k=1}^{n} I_k$ *– ідеали;*
2) *добуток ідеалів асоціативний;*
3) *добуток ідеалів дистрибутивний.*

Доведення. Досить показати, що 1) виконується для $n = 2$. Для доведення застосуємо твердження 8.1.

Нехай $a_1, a_2 \in I$, $b_1, b_2 \in J$. Тоді $a_1 + b_1 - (a_2 + b_2) = (a_1 - a_2) + (b_1 - b_2) \in I + J$. Далі, $\forall r \in R, r(a_1 + b_1) = ra_1 + rb_1 \in I + J$ та $(a_1 + b_1)r = a_1 r + b_1 r \in I + J$. Отже, $I + J$ – ідеал.

Нехай $a_1, .., a_n, a_1', .., a_n' \in I$, $b_1, \dots, b_n, b_1', \dots, b_n' \in J$. Тоді

$$\sum_{k=1}^{n} a_k b_k - \sum_{k=1}^{n} a_k' b_k' = \sum_{k=1}^{n} a_k b_k + \sum_{k=1}^{n} (-a_k') b_k' \in IJ;$$

$$r\left(\sum_{k=1}^{n} a_k b_k \right) = \sum_{k=1}^{n} (r a_k) b_k \in IJ;$$

$$\left(\sum_{k=1}^{n} a_k b_k \right) r = \sum_{k=1}^{n} a_k (b_k r) \in IJ.$$

Аналогічно доводяться пункти 2) та 3).

Означення 8.4. *Ідеал* I *кільця* $(R, +, \cdot)$ *називається максимальним, якщо* $I \neq R$ *і, якщо* J *ідеал кільця* $(R, +, \cdot)$ *такий, що* $I \subset J \subset R$, *то* $I = J$ *або* $J = R$.

Гомоморфізм. Ізоморфізм. Автоморфізм кілець

Нехай $(R,+,\cdot)$, $(S,\oplus,\circ)$ – кільця.

Означення 8.5. *Відображення $\varphi: R \to S$ називається* ***гомоморфізмом****, якщо $\forall a,b \in R$ має місце*

$$\varphi(a+b) = \varphi(a) \oplus \varphi(b);$$

$$\varphi(a \cdot b) = \varphi(a) \circ \varphi(b).$$

Означення 8.6. *Якщо гомоморфізм $\varphi: R \to S$ є взаємно однозначним відображенням, то φ називається* ***ізоморфізмом****.*
Ізоморфізм $\varphi: R \to R$ кільця R на себе називається ***автоморфізмом****.*

Означення 8.7. *Ядром гомоморфізму $\varphi: R \to S$ називається множина*

$$ker(\varphi) = \{r \in R | \varphi(r) = 0\}.$$

Образом гомоморфізму φ називається множина

$$Im(\varphi) = \{s \in S | \exists r \in R: \varphi(r) = s\}.$$

Твердження 8.4. *Нехай $\varphi: R \to S$ – гомоморфізм кілець $(R,+,\cdot)$ та $(S,\oplus,\circ)$.*

Тоді

1) $ker(\varphi)$ *– ідеал в* $(R,+,\cdot)$*;*
2) $Im(\varphi)$ *– підкільце* $(S,\oplus,\circ)$.

Доведення. 1). Нехай $a_1, a_2 \in ker(\varphi)$. Тоді $\varphi(a_1) = 0$, $\varphi(a_2) = 0$, звідки $\varphi(a_1 - a_2) = 0$ і, отже, $a_1 - a_2 \in ker(\varphi)$. Нехай $a \in ker(\varphi)$, $r \in R$. Тоді $\varphi(a \cdot r) = \varphi(a) \circ \varphi(r) = 0 \circ \varphi(r) = 0$. З урахуванням твердження 8.1 $ker(\varphi)$ – ідеал.

2) Нехай $s_1, s_2 \in Im(\varphi)$. Тоді $\exists r_1, r_2 \in R$: $\varphi(r_1) = s_1$, $\varphi(r_2) = s_2$. Звідки

$$\varphi(r_1 - r_2) = \varphi(r_1) - \varphi(r_2) = s_1 - s_2 \in Im(\varphi),$$

$$\varphi(r_1 \cdot r_2) = \varphi(r_1) \circ \varphi(r_2) = s_1 \circ s_2 \in Im(\varphi).$$

Отже, $Im(\varphi)$ – підкільце.

Факторкільце

Нехай $(R,+,\cdot)$ – кільце, $S \subset R$, $a \in R$. Записом $a+S$ позначається множина

$$a+S \coloneqq \{a+b : b \in S\}.$$

Нехай I ідеал кільця $(R,+,\cdot)$. Розглянемо множину $R/I = \{a+I : a \in R\}$, на якій введені такі операції додавання та множення:

$$(a+I) \oplus (b+I) := a+b+I,$$

$$(a+I) \circ (b+I) := a \cdot b + I.$$

Із означення операції додавання $\oplus$ випливає, що у якості нейтрального елемента по $\oplus$ (або нуля) виступає ідеал I, оскільки $(a+I) \oplus I = a+I$. Звідси випливає, що $a+I = a'+I$, якщо існує $i \in I$ таке, що $a' = a+i$.

Теорема 8.1. $(R/I, \oplus, \circ)$ *– кільце, яке називають фактор кільцем кільця* $(R,+,\cdot)$ *за ідеалом* I.

Доведення. Доведемо коректність додавання і множення.

Дійсно, нехай $a+I = a'+I$ і $b+I = b'+I$. Це означає, що існують $i, j \in I$ такі, що $a' = a+i$, $b' = b+j$. Звідки, з урахуванням того, що $i+j+I = I$, маємо

$$(a'+I) \oplus (b'+I) = (a+i+I) \oplus (b+j+I) = a+i+b+j+I = a+b+I$$
$$= (a+I) \oplus (b+I).$$

Далі, неважко переконатись, що $a \cdot i + b \cdot j + i \cdot j \in I$. Звідки

$$(a'+I) \circ (b'+I) = (a+i+I) \circ (b+j+I) = a \cdot b + a \cdot i + b \cdot j + i \cdot j + I$$
$$= a \cdot b + I = (a+I) \circ (b+I).$$

Властивості кільця для додавання $\oplus$ і дистрибутивність множення відносно додавання перевірте самостійно.

Приклади

1. Кільце $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ є фактор кільцем кільця $(\mathbb{Z}, +, \cdot)$ за ідеалом $n\mathbb{Z}$, де $n \in \mathbb{N}$.
2. Кільце $\left(\mathbb{Q}[\sqrt{2}], +, \cdot\right)$, де $\mathbb{Q}[\sqrt{2}] = \{r + s\sqrt{2} \mid r, s \in \mathbb{Q}\}$ містить ідеал $I(\sqrt{2}) = \{s\sqrt{2} \mid s \in \mathbb{Q}\}$. Легко переконатись, що фактор кільце $\left(\mathbb{Q}[\sqrt{2}]/I(\sqrt{2}), +, \cdot\right)$ ізоморфне кільцю раціональних чисел $(\mathbb{Q}, +, \cdot)$.

ЛЕКЦІЯ 9. **ПОЛЕ. ПОЛЕ КОМПЛЕКСНИХ ЧИСЕЛ**

Означення 9.1. *Кільце з одиницею називають кільцем з діленням, якщо в ньому виконується умова* $\forall x \in \mathcal{R}$*:* $x \neq 0$*,* $\exists x^{-1}$ *такий, що* $x \circ x^{-1} = 1 = x^{-1} \circ x$.

Означення 9.2. *Асоціативне кільце з діленням називають тілом (англійською skew field).*

Означення 9.3. *Комутативне тіло називається полем (англійською field).*

Приклади

1) Поле дійсних чисел $(\mathbb{R}, +, \cdot)$;

2) Поле раціональних чисел $(\mathbb{Q}, +, \cdot)$;

3) Поле комплексних чисел $(\mathbb{C}, +, \cdot)$;

4) Тіло кватерніонів $(\mathbb{H}, +, \cdot)$.

5) Кільце з діленням $(\mathbb{O}, +, \cdot)$, де $\mathbb{O}$ – октоніони.

5) Поле Галуа $\mathbb{Z}/p\mathbb{Z}$ $(\mathbb{Z}_p)$ – поле класів лишків за модулем p, де p – просте число.

6) Поле $\left(\mathbb{Q}[\sqrt{2}], +, \cdot\right)$, де $\mathbb{Q}[\sqrt{2}] = \{x + y\sqrt{2} \mid x, y \in \mathbb{Q}\}$

Вправа 9.1. Переконайтесь, що $\left(\mathbb{Q}[\sqrt{2}], +, \cdot\right)$ – поле.

Комплексні числа

Через i будемо позначати уявну одиницю, яка символізує один із розв'язків рівняння $x^2 + 1 = 0$ або по іншому $i^2 = -1$.

Означення 9.4. *Комплексним числом називається вираз* $x + yi$, *де* $x, y \in \mathbb{R}$.

Означення 9.5. *Множина комплексних чисел позначається через*

$$\mathbb{C} = \{z: z = x + yi\ , x, y \in \mathbb{R}\},$$

При цьому $x = Re(z)$ називається дійсною частиною, а $y = Im(z)$ – уявною частиною комплексного числа z, а запис $z = x + yi$ називається *алгебраїчною формою запису* комплексного числа z.

Операції над комплексними числами

Числа $z_1 = x_1 + y_1 i$ та $z_2 = x_2 + y_2 i$ рівні тоді і тільки тоді, коли $x_1 = x_2$ та $y_1 = y_2$.

Додавання (віднімання): $z_1 \pm z_2 = x_1 \pm x_2 + (y_1 \pm y_2)i$.

Множення: $z_1 z_2 = x_1 x_2 - y_1 y_2 + (x_1 y_2 + x_2 y_1)i$.

Формальне означення комплексних чисел

Комплексне число $z = x + yi$ розглядається як пара дійсних чисел $\binom{x}{y}$.

Операції задаються так:

Додавання: $\binom{x_1}{y_1} + \binom{x_2}{y_2} = \binom{x_1 + x_2}{y_1 + y_2}$,

Множення: $\binom{x_1}{y_1} \cdot \binom{x_2}{y_2} = \binom{x_1 x_2 - y_1 y_2}{x_1 y_2 + x_2 y_1}$.

Перевага формального означення комплексних чисел у тому, що не потрібно вводити уявне число $i = \sqrt{-1}$, при цьому дійсне число x задається парою $\binom{x}{0}$, а чисто уявне число iy – парою $\binom{0}{y}$, зокрема $i = \binom{0}{1}$. Легко переконатись, що

$$i^2 = \begin{pmatrix}0\\1\end{pmatrix} \cdot \begin{pmatrix}0\\1\end{pmatrix} = \begin{pmatrix}-1\\0\end{pmatrix}, \qquad \begin{pmatrix}0\\y\end{pmatrix} = \begin{pmatrix}0\\1\end{pmatrix} \cdot \begin{pmatrix}y\\0\end{pmatrix} = iy.$$

Ділення комплексних чисел

Означення 9.6. *Комплексне число $\bar{z} = x - yi$ називається спряженим до $z = x + yi$.*

Легко бачити, що $z\bar{z} = x^2 + y^2 = \bar{z}z$. Звідси для $z_1 = x_1 + y_1 i$, $z_2 = x_2 + y_2 i \neq 0$, маємо

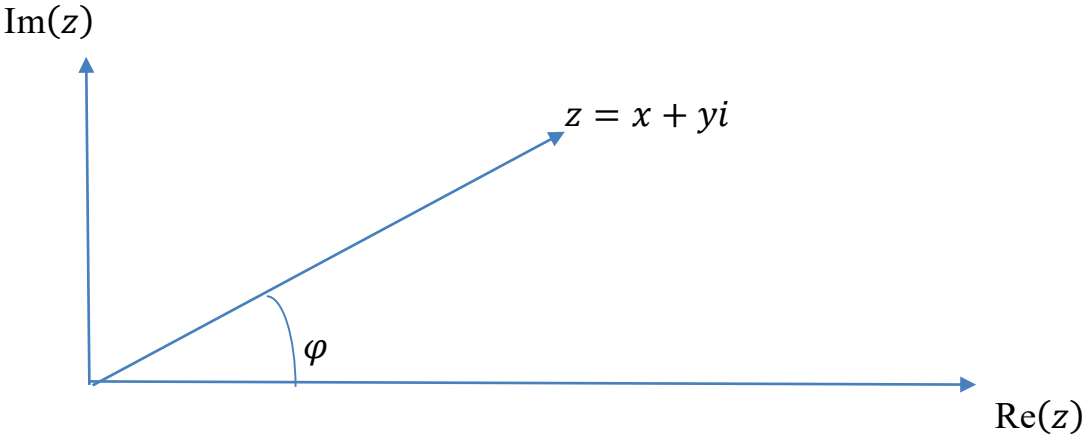
$$\frac{z_1}{z_2} = \frac{x_1 + y_1 i}{x_2 + y_2 i}\frac{\overline{z_1}}{\overline{z_2}} = \frac{x_1x_2 + y_1y_2 - (x_1y_2 - x_2y_1)i}{x_2^2 + y_2^2} = \frac{x_1x_2 + y_1y_2}{x_2^2 + y_2^2} - \frac{x_1y_2 - x_2y_1}{x_2^2 + y_2^2}\, i.$$

Зауваження 9.1. Операція ділення на ненульові комплексні числа разом з тим, що $(\mathbb{C}, +, \cdot)$ є комутативним кільцем свідчить, що $(\mathbb{C}, +, \cdot)$ – поле.

Зауваження 9.1. Операція ділення на ненульові комплексні числа разом з тим, що $(\mathbb{C}, +, \cdot)$ є комутативним кільцем свідчить, що $(\mathbb{C}, +, \cdot)$ – поле.

Геометричне зображення комплексних чисел

Комплексне число $z = x + yi$ може розглядатись як вектор на площині з ортогональним базисом $\{1, i\}$. Тому можна здійснювати перехід від прямокутної системи координат (x, y) до полярної $(|z|, \varphi)$, де $|z| = \sqrt{x^2 + y^2}$ – модуль комплексного числа z, а $\varphi = Arg(z)$ – аргумент z.



$Arg(z)$ визначається з точністю до періоду 2π, тобто $Arg(z) = \varphi + 2\pi k$, $k \in \mathbb{Z}$. Для однозначності вводиться поняття головного значення аргументу числа z: $\varphi = arg(z) \in]-\pi, \pi]$ (у деяких підручниках $arg(z) \in [0,2\pi[$).

Обчислення $arg(z)$ залежить від квадранту системи координат, у якому знаходиться число z:

1. Якщо $z \in I$ або $z \in IV$, то

$$arg(z) = \arctan\frac{y}{x};$$

2. Якщо $z \in II$, то

$$arg(z) = \pi + \arctan\frac{y}{x};$$

3. Якщо $z \in III$, то

$$arg(z) = -\pi + \arctan\frac{y}{x}.$$

Формула переходу від полярної системи $(|z|, \varphi)$ координат до декартової (x, y):

$$\begin{cases} x = |z|\cos\varphi \\ y = |z|\sin\varphi \end{cases}$$

Тригонометрична форма запису комплексного числа

$$z = |z|(\cos\varphi + i\sin\varphi).$$

Цією формою зручно користуватись при обчисленні добутку чи ділення комплексних чисел, а також при піднесенні комплексного числа до степеню та взяття кореня.

Нехай для $z_1 = |z_1|(\cos\varphi_1 + i\sin\varphi_1)$, $z_2 = |z_2|(\cos\varphi_2 + i\sin\varphi_2)$. Тоді

$$z_1 z_2 = |z_1||z_2|(\cos\varphi_1 + i\sin\varphi_1)(\cos\varphi_2 + i\sin\varphi_2)$$
$$= |z_1||z_2|\big(\cos\varphi_1\cos\varphi_2 - \sin\varphi_1\sin\varphi_2$$
$$+ i(\cos\varphi_1\sin\varphi_2 + \cos\varphi_2\sin\varphi_1)\big)$$
$$= |z_1||z_2|(\cos(\varphi_1 + \varphi_2) + i\sin(\varphi_1 + \varphi_2)).$$

Аналогічно показується, що

$$\frac{z_1}{z_2} = \frac{|z_1|}{|z_2|}(\cos(\varphi_1 - \varphi_2) + i\sin(\varphi_1 - \varphi_2)).$$

Піднесення до степеню

Використовуючи формулу добутку комплексних чисел, легко бачити, що для $n \in \mathbb{N}$

$$z^n = |z|^n(\cos n\varphi + i\sin n\varphi).$$

Корінь з комплексного числа

Означення 9.7. *Коренем степеню $n \in \mathbb{N}$ комплексного числа z називається комплексне число v таке, що $v^n = z$.*

Нехай $z = |z|(\cos\varphi + i\sin\varphi)$, а $v = |v|(\cos\alpha + i\sin\alpha)$. Тоді

$$v^n = |v|^n(\cos n\alpha + i\sin n\alpha) = |z|(\cos\varphi + i\sin\varphi).$$

Звідки маємо співвідношення

$$|v| = \sqrt[n]{|z|},$$

$$n\alpha = \varphi + 2\pi k,\ k \in \mathbb{Z}.$$

Отже, маємо рівно n різних значень для α (з точністю до періоду 2π):

$$\alpha = \frac{\varphi + 2\pi k}{n},\ k = 0,1,\dots,n-1.$$

Приклад. Легко переконатись, що $\sqrt[n]{1} = \{1, \omega, \omega^2, \dots, \omega^{n-1}\}$, тобто містить n чисел, де $\omega = \left(\cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}\right)$, $n \in \mathbb{N}$.

Показникова форма запису комплексного числа

Формула Ойлера $e^{i\varphi} = \cos\varphi + i\sin\varphi$. Доведення цієї формули здійснюється шляхом розкладу функцій e^{-ix}, $\cos x$ та $\sin x$ у ряди Тейлора. Звідки випливає показникова форма запису

$$z = |z|e^{i\varphi}.$$

ЛЕКЦІЯ 10. **КІЛЬЦЕ МНОГОЧЛЕНІВ**

Нехай $(\mathbb{K}, +, \cdot)$ – комутативне кільце з одиницею 1.

Через $\mathbb{K}[x]$ позначимо множину многочленів з коефіцієнтами із кільця $\mathbb{K}$:

$$\mathbb{K}[x] = \{a_0 + a_1x + \cdots + a_{n-1}x^{n-1} + a_nx^n |\, n \in \mathbb{N}, a_k \in \mathbb{K}\}.$$

Означення 10.1. *Степенем многочлена* $0 \not\equiv f(x) = a_0 + a_1x + \cdots + a_nx^n$ *називається величина* $\deg(f) = \max\{k \in \mathbb{N}: a_k \neq 0\}$. *Старшим коефіцієнтом ненульового многочлена* $f(x)$ *називається число* $\mathrm{coef}(f) = a_n$, *де* $n = \deg(f)$.

Многочлен $f(x) \equiv 0$, у якого всі коефіцієнти нулі, будемо називати нульовим і позначати $\theta(x)$. Степенем нульового многочлена покладемо рівним мінус нескінченності $\deg(\theta) = -\infty$, причому вважаємо, що $\forall a \in \mathbb{K}$

$$\max(a, -\infty) = a\,, a + -\infty = -\infty.$$

Означення 10.2. *Многочлени* $f, g \in \mathbb{K}[x]$ *називаються рівними, якщо* $\deg(f) = \deg(g)$ *і*

$$a_k = b_k, \qquad k = 0,1,2, \dots$$

Операції в $\mathbb{K}[x]$

Нехай

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n \text{ та } g(x) = b_0 + b_1 x + \cdots + b_m x^m$$

Тоді

$$f(x) + g(x) = a_0 + b_0 + (a_1 + b_1)x + \cdots,$$

$$f(x) \cdot g(x) = \sum_k c_k x^k,$$

де $c_k = \sum_{i=0}^{k} a_i \, b_{k-i}$.

Твердження 10.1. $\forall f, g \in \mathbb{K}[x]$

1. $\deg(f + g) \leq \max\big(\deg(f), \deg(g)\big)$,
2. $\deg(f \cdot g) \leq \deg(f) + \deg(g)$, причому $\deg(f \cdot g) < \deg(f) + \deg(g) \Leftrightarrow \operatorname{coef}(f)\operatorname{coef}(g) = 0$.
3. Якщо $\mathbb{K}$ – область цілісності, то $\deg(f \cdot g) = \deg(f) + \deg(g)$, $\operatorname{coef}(f)\operatorname{coef}(g) = \operatorname{coef}(f \cdot g)$.

Вправа 10.1. Довести твердження 10.1.

Теорема 10.1. $(\mathbb{K}[x], +, \cdot)$ – *комутативне кільце з одиницею. Якщо* $(\mathbb{K}, +, \cdot)$ *область цілісності, то* $(\mathbb{K}[x], +, \cdot)$ – *область цілісності, причому* $(\mathbb{K}, +, \cdot)$ *підкільце кільця* $(\mathbb{K}[x], +, \cdot)$.

Доведення. Операції над многочленами зводяться до операцій над елементами кільця $(\mathbb{K}, +, \cdot)$. Безпосередньо перевіряється, що ці операції задовольняють означення асоціативного комутативного кільця з одиницею, тобто $\forall f, g \in \mathbb{K}[x]$

1. $f + g = g + f$;
2. $f + \theta = f$;
3. $f + (-f) = \theta,\ -f(x) = (-1) \cdot f(x)$;

4. $f + (g + h) = (f + g) + h$;
5. $f \cdot g = g \cdot f$;
6. $f \cdot (g + h) = f \cdot h + g \cdot h$;
7. $f \cdot (g \cdot h) = (f \cdot g) \cdot h$.

Нехай $(\mathbb{K}, +, \cdot)$ – область цілісності. Тоді, якщо $f \cdot g = \theta$, то

$$\deg(f \cdot g) = \deg(\theta) + \deg(g) = -\infty,$$

але $\deg(f \cdot g) = \deg(f) + \deg(g)$ і, якщо $f \neq \theta$ та $g \neq \theta$, то $\deg(f \cdot g) \geq 0$. Отримали суперечність. Отже, або $f = \theta$, або $g = \theta$, тобто немає дільників нуля.

Ділення многочленів

Нехай $\mathbb{F}$ поле. Розглянемо кільце многочленів над $\mathbb{F}$: $(\mathbb{F}[x], +, \cdot)$, що є областю цілісності многочленів, оскільки поле – область цілісності. Для стислості кільце $(\mathbb{F}[x], +, \cdot)$ надалі будемо позначати через $\mathbb{F}[x]$.

Означення 10.3. *Многочлен $f \in \mathbb{F}[x]$ ділиться на многочлен $g \in \mathbb{F}[x]$, якщо існує многочлен $h \in \mathbb{F}[x]$ такий, що*

$$f = g \cdot h. \tag{10.1}$$

Наприклад, $f(x) = x^3 - 1$, $g(x) = x^2 + x + 1$,

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

Теорема 10.2 (Ділення з остачею) *Для довільних многочленів $f, g \in \mathbb{F}[x]$, $g \neq \theta$ існує єдина пара многочленів $q, r \in \mathbb{F}[x]$ така, що*

$$f = g \cdot q + r, \tag{10.2}$$

де $\deg(r) < \deg(g)$ *або* $r = \theta$.

Многочлен q називається неповна частка, а r – остача.

Доведення. Спочатку доведемо існування многочленів $q, r \in \mathbb{F}[x]$ Якщо $f(x) = c \in \mathbb{F}$, $\theta \neq g \in \mathbb{F}[x]$, то, якщо $\deg(g) \geq 1$, то

$$f = g \cdot \theta + c.$$

Якщо $\deg(g) = 0$, тобто $g = k \in \mathbb{F}$, причому $k \neq 0$. Тоді $\exists l \in \mathbb{F}$ таке, що

$$c = kl.$$

За індукцією припустимо, що для будь-якого многочлену $f \in \mathbb{F}[x]$ з $\deg(f) < n$, $n \in \mathbb{N}$ ділення з остачею виконується.

Покажемо, що ділення з остачею виконується і для $\deg(f) = n$. Дійсно, якщо $\deg(g) > n$, то

$$f = g \cdot \theta + f, \qquad \deg(f) = n < \deg(g)$$

Тепер припустимо, що $\deg(g) \leq \deg(f)$. Нехай

$f(x) = a_0 + a_1 x + \cdots + a_n x^n$, $g(x) = b_0 + b_1 x + \cdots + b_m x^m$, де $m \leq n$.

Розглянемо многочлен

$$p(x) = f(x) - \frac{a_n}{b_m} x^{n-m} g(x) = a_n x^n - \frac{a_n}{b_m} x^{n-m} b_m x^m - \cdots$$

Звідки видно, що $\deg(p) < n$. За припущенням індукції існують $q, r \in \mathbb{F}[x]$ такі, що $p = g \cdot q + r$, *де* $\deg(r) < \deg(g)$. Отже,

$$f(x) - \frac{a_n}{b_m} x^{n-m} g(x) = g(x) \cdot q(x) + r(x).$$

Тобто

$$f(x) = g(x) \cdot \left(\frac{a_n}{b_m} x^{n-m} + q(x) \right) + r(x), \qquad \deg(r) < \deg(g).$$

Доведемо єдиність: припустимо, що існують $q_1, r_1 \in \mathbb{F}[x]$ та $q_2, r_2 \in \mathbb{F}[x]$ такі, що $q_1 \neq q_2$ та

$$f = g \cdot q_1 + r_1, \qquad \deg(r_1) < \deg(g),$$

$$f = g \cdot q_2 + r_2, \qquad \deg(r_2) < \deg(g).$$

Звідки

$$0 = g \cdot (q_1 - q_2) + r_1 - r_2.$$

Оскільки $\deg(r_1 - r_2) \leq \deg(r_1)$, то

$$\deg(r_1 - r_2) < \deg(g).$$

Далі, враховуючи властивість степеню $\deg(f \cdot g) = \deg(f) + \deg(g)$ для многочленів над полем та те, що $\deg(q_1 - q_2) \geq 0$, маємо

$$\deg\big(g \cdot (q_1 - q_2)\big) = \deg(g) + \deg(q_1 - q_2) \geq \deg(g) > \deg(r_1 - r_2).$$

Але із того, що $g \cdot (q_1 - q_2) = r_2 - r_1$ випливає, що $\deg\big(g \cdot (q_1 - q_2)\big) = \deg(r_2 - r_1) = \deg(r_1 - r_2)$.

Суперечність виникла із припущення існування двох різних пар $q_1, r_1 \in \mathbb{F}[x]$ та $q_2, r_2 \in \mathbb{F}[x]$, які задовольняють (10.2).

ЛЕКЦІЯ 11. **НАЙБІЛЬШИЙ СПІЛЬНИЙ ДІЛЬНИК МНОГОЧЛЕНІВ**

Означення 11.1. *Спільний дільник двох многочленів $f, g \in \mathbb{F}[x]$, який ділиться на будь-який інший спільний дільник цих многочленів, називається їх найбільшим спільним дільником* (НСД).

Позначається $\text{НСД}(f, g)$.

НСД многочленів визначається однозначно з точністю до сталого множника (оскільки, якщо $d(x) = \text{НСД}(f, g)$, то й $c \cdot d(x) = \text{НСД}(f, g)$, $c \neq 0$.

Многочлени $f(x)$ та $g(x)$ називаються взаємно простими, якщо кожний їхній спільний дільник є ненульовою константою, тобто $\text{НСД}(f, g) = c \neq 0$.

Аналогічно алгоритму Евкліда для знаходження НДС двох цілих чисел, алгоритм Евкліда застосовується для знаходження НДС двох многочленів $f, g \in \mathbb{F}[x]$:

$$f(x) = g(x) \cdot q_1(x) + r_1(x), \qquad \deg(r_1) < \deg(g),$$

$$g(x) = r_1(x) \cdot q_2(x) + r_2(x), \qquad \deg(r_2) < \deg(r_1),$$

$$r_1(x) = r_2(x) \cdot q_2(x) + r_3(x), \qquad \deg(r_3) < \deg(r_2),$$

$$- - - - - - - - - - - - -$$

$$r_{s-1}(x) = r_s(x) \cdot q_s(x) + r_{s+1}(x), \qquad \deg(r_{s+1}) < \deg(r_s),$$

$$r_s(x) = r_{s+1}(x) \cdot q_{s+2}(x).$$

Теорема 11.1. $r_{s+1}(x) = \text{НСД}(f, g)$.

Доведення теореми аналогічне доведенню теореми 2.1 для цілих чисел.

Аналогічно доводиться лінійне зображення $d(x) = \text{НСД}(f, g)$, тобто існують многочлени $u, v \in \mathbb{F}[x]$ такі, що

$$f(x) \cdot u(x) + g(x) \cdot v(x) = d(x). \qquad (11.1)$$

При цьому, якщо $\deg(g) > 0$ і $\deg(f) > 0$, то $\deg(u) < \deg(g)$, $\deg(v) < \deg(f)$. Доведемо це від супротивного, припустимо, що $\deg(u) \geq \deg(g)$. Тоді існують $q, r \in \mathbb{F}[x]$ такі, що

$$u(x) = g(x) \cdot q(x) + r(x), \qquad \deg(r) < \deg(g).$$

Підставляючи в (11.1), маємо

$$f(x) \cdot r(x) + g(x) \cdot [v(x) + f(x) \cdot q(x)] = d(x).$$

Множник $r(x)$, що стоїть при $f(x)$ має степінь менший степені $g(x)$. Степінь многочлена в квадратних дужках, що стоїть при $g(x)$, у свою чергу менший

степеню $f(x)$. Дійсно, якби цей степінь був не менший степеню $f(x)$, то вираз $g(x) \cdot [v(x) + f(x) \cdot q(x)]$ мав би степінь більший степеню $f(x) \cdot r(x)$ і тоді степінь $d(x)$ був би більший або рівний степеню $f(x) \cdot g(x)$, що неможливо з урахуванням зроблених припущень ($\deg(g) > 0$ і $\deg(f) > 0$).

Наслідок 11.1. *Многочлени $f, g \in \mathbb{F}[x]$ взаємно прості тоді і тільки тоді, якщо існують многочлени $u, v \in \mathbb{F}[x]$ такі, що*

$$f(x) \cdot u(x) + g(x) \cdot v(x) = 1.$$

Означення 11.2. *Елемент $x_0 \in \mathbb{F}$ називається коренем многочлена $f \in \mathbb{F}[x]$, якщо $f(x_0) = 0$.*

Теорема 11.2 (Безу). *Елемент $x_0 \in \mathbb{F}$ є коренем многочлена $f \in \mathbb{F}[x]$ тоді і тільки тоді, коли многочлен f ділиться на $x - x_0$.*

Доведення. Поділимо з остачею f ділиться на $x - x_0$:

$$f(x) = (x - x_0) \cdot q(x) + r(x).$$

Оскільки $\deg(r) < \deg(x - x_0) = 1$, то $r(x) = r$ – константа. Отже,

$$f(x_0) = r.$$

Звідки, якщо x_0 – корінь, то $f(x_0) = 0 = r$, тобто $f(x)$ ділиться на $x - x_0$. Нехай $f(x)$ ділиться на $x - x_0$, тобто $f(x) = (x - x_0) \cdot q(x)$. Звідки $f(x_0) = 0$.

На практиці часто потрібно доводити незвідність многочлена над полем раціональних чисел (тобто неможливість розкладання у добуток двох многочленів над $\mathbb{Q}$ із степенями більших нуля), для цього корисно знати критерій Ейзенштейна, який є ознакою незвідності многочлена над $\mathbb{Q}$.

Спочатку доведемо допоміжні леми:

Лема 11.1. *Нехай $g(x), h(x) \in \mathbb{Z}[x]$ і $f(x) = g(x)h(x)$. Нехай просте число p ділить всі коефіцієнти $f(x)$. Тоді p ділить всі коефіцієнти $g(x)$ або p ділить всі коефіцієнти $h(x)$.*

Доведення. Нехай $f(x) = a_0 + a_1x + \cdots + a_nx^n$, $g(x) = b_0 + b_1x + \cdots + b_mx^m$, $h(x) = c_0 + c_1x + \cdots + c_lx^l$. Припустимо, що p не ділить всі коефіцієнти $g(x)$ і p не ділить всі коефіцієнти $h(x)$. Позначимо

$$\beta = \min\{k \in \{0,1,\dots,m\} | p \nmid b_k\},$$

$$\gamma = \min\{k \in \{0,1,\dots,m\} | p \nmid c_k\}.$$

Тоді

$$a_{\beta\gamma} = b_\beta c_\gamma + b_{\beta-1}c_{\gamma+1} + \cdots + b_0c_{\gamma+\beta} + b_{\beta+1}c_{\gamma-1} + \cdots + b_{\gamma+\beta}c_0, \qquad (11.2)$$

де припускається, що якщо індекс виходить за свої допустимі межі, то вважається, що коефіцієнт з таким індексом дорівнює нулеві, наприклад, $b_{-1} = 0$, $c_{m+1} = 0$ і т. д.

Оскільки $p \nmid b_\beta c_\gamma$, але $p | b_{\beta-1}c_{\gamma+1}$, …, $p | b_{\beta+1}c_{\gamma-1}$,…, $p | b_{\gamma+\beta}c_0$, тобто p ділить всі інші доданки правої частини (11.2), крім $b_\beta c_\gamma$, то $p \nmid a_{\beta\gamma}$.

Лема 11.2 (Гаусс) *Нехай $f(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1} + a_nx^n$, де коефіцієнти $a_k \in \mathbb{Z}$, $k = 0,1,\dots,n$. Тоді, якщо многочлен $f(x)$ – незвідний над $\mathbb{Z}$, то він незвідний і над полем $\mathbb{Q}$.*

Доведення. Припустимо, що $f(x)$ розкладається на добуток многочленів ненульових степенів $g(x), h(x) \in \mathbb{Q}[x]$. Покажемо, що тоді існують $G(x), H(x) \in \mathbb{Z}[x]$ такі, що $f(x) = G(x)H(x)$.

Очевидно, що існують $b, c \in \mathbb{N}$ такі, що $bg(x), ch(x) \in \mathbb{Z}[x]$. Покладемо $a = bc$, $G_0(x) = bg(x)$, $H_0(x) = ch(x)$. Тоді

$$af(x) = G_0(x)H_0(x).$$

Якщо $a = 1$, то покладемо $G(x) = G_0(x)$, $H(x) = H_0(x)$ і лема доведена. Якщо ж $a > 1$, то існує просте число p_1 таке, що $a = p_1a_1$ для деякого додатного a_1. Тоді за лемою 11.1 p_1 ділить всі коефіцієнти $G_0(x)$, або p_1 ділить всі коефіцієнти $H_0(x)$.

Якщо p_1 ділить всі коефіцієнти $G_0(x)$, то покладемо $G(x) = G_1(x) = \frac{G_0(x)}{p_1}$, якщо ж p_1 ділить всі коефіцієнти $H_0(x)$, то покладемо $H(x) = H_1(x) = \frac{H_0(x)}{p_1}$. І тоді

$$a_1 f(x) = G(x)H(x).$$

Далі, якщо $a_1 > 1$, то існує просте число p_2 таке, що $a_1 = p_2 a_2$ для деякого додатного a_2.

Аналогічно попередньому одержуємо:

$$a_2 f(x) = G(x)H(x).$$

Продовжимо цей процес і, оскільки додатні $a > a_1 > a_2 > \cdots$, то на якомусь кроці k одержимо $a_k = 1$ і, отже,

$$f(x) = G(x)H(x), \qquad G(x), H(x) \in \mathbb{Z}[x].$$

Теорема 11.3 (Критерій Ейзенштейна). *Нехай $f(x) = a_0 + a_1 x + \cdots + a_n x^n$, де коефіцієнти $a_k \in \mathbb{Z}$, $k = 0,1,\dots,n$ такі, що існує просте число p для якого виконуються умови:*

1. $p | a_k$, $k = 0,1,\dots,n-1$, $p \nmid a_n$;
2. $p^2 \nmid a_0$.

Тоді $f(x)$ – незвідний над полем $\mathbb{Q}$.

Доведення. Нехай $f(x) = g(x)h(x)$, де $g, h \in \mathbb{Q}[x]$. З урахуванням леми Гауса, досить розглянути випадок $f(x) = g(x)h(x)$, де $g(x) = b_0 + b_1 x + \cdots + b_m x^m$, $h(x) = c_0 + c_1 x + \cdots + c_l x^l$, $b_i, c_j \in \mathbb{Z}$, $i = 0,1,\dots,m$, $j = 0,1,\dots,l$.

Звідки $a_0 = b_0 c_0$ і, отже, або $p | b_0$, або $p | c_0$, але не одночасно, оскільки $p^2 \nmid a_0$.

Нехай $p | b_0$ і $p \nmid c_0$. Очевидно, що не всі коефіцієнти g діляться на p інакше на p ділились би всі коефіцієнти f. Нехай i найменший індекс такий, що $p \nmid b_i$. Але

$$a_i = b_i c_0 + b_{i-1} c_1 + \cdots + b_0 c_i$$

і, оскільки $p | a_i$ (зауважимо, що $i < n$) та $p | b_j$ для всіх $j < i$, то $p | b_i c_0$, що суперечить припущенню $p \nmid c_0$ і $p \nmid b_i$.

ЛЕКЦІЯ 12. **ВЛАСТИВОСТІ КОРЕНІВ МНОГОЧЛЕНА. ОСНОВНА ТЕОРЕМА АЛГЕБРИ**

Раціональні корені многочлена з цілими числами

Теорема 12.1. *Нехай* $x_0 = \frac{p}{q}$, $p \in \mathbb{Z}$, $q \in \mathbb{N}$ *нескоротний дріб – корінь многочлена*

$$a_0 + a_1 x + \cdots + a_n x^n = 0,$$

де $a_k \in \mathbb{Z}$. *Тоді* $a_0 \vdots p$, $a_n \vdots q$.

Доведення. Помноживши на q^n рівність

$$a_0 + a_1 \frac{p}{q} + a_2 \left(\frac{p}{q}\right)^2 \ldots + a_n \left(\frac{p}{q}\right)^n = 0,$$

маємо

$$a_0 q^n + \underline{a_1 p q^{n-1} + \cdots + a_1 q p^{n-1} + a_n p^n} = 0.$$

Оскільки підкреслена знизу частина виразу ділиться на p, а q і p – взаємно прості, то a_0 ділиться на p. Аналогічно, підкреслена зверху частина виразу

$$\overline{a_0 q^n + a_1 p q^{n-1} + \cdots + a_1 q p^{n-1}} + a_n p^n = 0.$$

ділиться на q, отже, a_n ділиться на q, оскільки q і p – взаємно прості.

Теорема 12.2 (Вієта). *Нехай* $\mathbb{F}$ *– поле і* $x_1, x_2, \ldots, x_n \in \mathbb{F}$ *– корені (серед них можуть бути однакові, тобто кратні) многочлена* $f(x) = a_0 + a_1 x + \cdots + a_{n-1} x^{n-1} + x^n$, *де* $a_k \in \mathbb{F}$. *Тоді*

$$f(x) = (x - x_1) \cdot (x - x_2) \cdot \ldots \cdot (x - x_n) \qquad (12.1)$$

і мають місце співвідношення, які називають формулами Вієта:

$$a_{n-1} = -(x_1 + x_2 + \cdots + x_n);$$

$$a_{n-2} = x_1x_2 + x_1x_3 + \cdots x_1x_n + x_2x_3 + \cdots + x_{n-1}x_n;$$

$$a_{n-3} = -(x_1x_2x_3 + x_1x_2x_4 + \cdots + x_{n-2}x_{n-1}x_n);$$

$$- - - - - - - - - - - - - - - -$$

$$a_0 = (-1)^n x_1x_2 \ldots x_n.$$

Доведення. Формула (12.1) є прямим наслідком теореми 11.2 (Безу). Дійсно, оскільки x_1 корінь $f(x)$, то існує многочлен $q(x) \in \mathbb{F}[x]$ такий, що

$$f(x) = (x - x_1) \cdot q_1(x).$$

Далі, многочлен $q(x)$ у свою чергу має корінь x_2 і тоді існує многочлен $q_2(x) \in \mathbb{F}[x]$ такий, що $q_1(x) = (x - x_2) \cdot q_2(x)$, тобто

$$f(x) = (x - x_1) \cdot (x - x_2) \cdot q_2(x).$$

Продовжуємо цей процес поки вичерпаємо всі корені.

Перемножуючи дужки у правій частині (12.1) і прирівнюючи коефіцієнти при однакових степенях змінної x, одержимо формули Вієта.

Якщо головний коефіцієнт a_n многочлена $f(x)$ не дорівнює одиниці, то неважко переконатись, що формули Вієта запишуться з тою різницею, що у лівих частинах замість a_k потрібно поставити $\frac{a_k}{a_n}$, $k = 1, \ldots, n-1$.

Основна теорема алгебри

Теорема 12.3 (Основна теорема алгебри комплексних чисел). *Нехай $f(x) \in \mathbb{C}[x]$, тоді існує $x_0 \in \mathbb{C}$ такий, що $f(x_0) = 0$. Іншими словами, будь-який многочлен з комплексними коефіцієнтами має хоча б один корінь у полі комплексних чисел.*

Теорему приймаємо без доведення. Одне із найпростіших доведень теореми 12.3 здійснюється в курсі комплексного аналізу за допомогою теореми Ліувілля.

Наслідок 12.1. *Будь-який многочлен* $f(x) \in \mathbb{C}[x]$ *степені* $n \geq 1$ *має рівно* n *коренів з урахуванням кратності.*

Наслідок 12.2. *Будь-який многочлен* $f(x) \in \mathbb{C}[x]$ *степені* $n \geq 1$ ($f(x) = a_0 + a_1 x + \cdots + a_n x^n$) *розкладається в добуток* n *лінійних множників:*

$$f(x) = a_n(x - x_1) \cdot (x - x_2) \cdot \ldots \cdot (x - x_n), \qquad (12.2)$$

причому цей розклад єдиний.

Доведення. Коефіцієнт a_n присутній у розкладі $f(x)$ з тієї причини, що після розкриття дужок у правій частині при x^n має бути коефіцієнт a_n, тобто $\text{coef}(f) = a_n$. Покажемо єдиність розкладу (12.2): припустимо, що існує інший розклад многочлена

$$f(x) = a_n(x - y_1) \cdot (x - y_2) \cdot \ldots \cdot (x - y_n) \qquad (12.3)$$

Із (12.2) та (12.3) випливає, що

$$(x - x_1) \cdot (x - x_2) \cdot \ldots \cdot (x - x_n) = (x - y_1) \cdot (x - y_2) \cdot \ldots \cdot (x - y_n). \quad (12.4)$$

Якби якийсь корінь x_k у лівій частині (12.4) був відмінний від усіх коренів y_l, $l = 1, \ldots, n$ у правій частині (12.4), то, підставляючи його у (12.4) ми отримали б зліва нуль, а справа число, відмінне від нуля. Аналогічно для якби якийсь корінь y_l у правій частині (12.4) не збігався з жодним x_i, $i = 1, \ldots, n$ у лівій частині (12.4). Отже, будь-який x_k рівний деякому y_l і навпаки.

Звідси ще не випливає єдиність розкладу (12.2), оскільки аргументи вище не заперечують, що якійсь однакові корені справа і зліва в (12.4) можуть мати різну кратність. Покажемо, що це також не можливо. Дійсно, припустимо, що кратність якогось кореня, наприклад x_1 зліва більша ніж справа, а саме $(x - x_1)^l$ знаходиться зліва і $(x - x_1)^m$ знаходиться справа при цьому $l > m$. Тоді, скоротивши праву і ліву частини (12.2) на $(x - x_1)^m$ отримаємо рівність, де справа немає множника $(x - x_1)$, а зліва є множник $(x - x_1)^{l-m}$, що не можливо згідно вищеописаних аргументів.

Лема 12.1. *Якщо многочлени* $f, g \in \mathbb{C}[x]$ *такі, що* $\deg(g) \leq n$, $\deg(f) \leq n$, *мають рівні значенні у більш ніж* n *різних точках, то* $f(x) = g(x)$.

Доведення. Розглянемо многочлен $f(x) - g(x)$. За припущеннями леми він має більш ніж n коренів і при цьому його степінь не більший n, а це можливо, коли $\forall x \in \mathbb{C}$, $f(x) - g(x) = 0$.

Отже, многочлен степені не більше n однозначно визначається своїми значеннями у $(n+1)$ різних точках.

Інтерполяційна формула Лагранжа

Припустимо, що перед нами стоїть задача побудови многочлена степені не вище n, який при різних значеннях змінної $x_1, x_2, \dots, x_{n+1}$ приймають відповідні значення $c_1, c_2, \dots, c_{n+1}$. Такий многочлен f визначається формулою

$$f(x) = \sum_{k=1}^{n+1} \frac{c_k(x - x_1) \dots (x - x_{k-1})(x - x_{k+1}) \dots (x - x_{n+1})}{(x_k - x_1) \dots (x_k - x_{k-1})(x_k - x_{k+1}) \dots (x_k - x_{n+1})}.$$

Дійсно, безпосередньою підстановкою неважко переконатись, що $f(x_k) = c_k$, $k = 1, \dots, n+1$.

ЛЕКЦІЯ 13. **РОЗШИРЕННЯ КІЛЕЦЬ І ПОЛІВ**

Означення 13.1. *Якщо кільце* $(\mathcal{R}_1, +, \cdot)$ *є підкільцем кільця* $(\mathcal{R}, +, \cdot)$, *то* $(\mathcal{R}, +, \cdot)$ *називається розширенням кільця* $(\mathcal{R}_1, +, \cdot)$. *Якщо* $(\mathcal{R}_1, +, \cdot)$ та $(\mathcal{R}, +, \cdot)$ – *поля, то* $(\mathcal{R}, +, \cdot)$ *називається розширенням поля* $(\mathcal{R}_1, +, \cdot)$.

Через $\mathcal{R}/\mathcal{R}_1$ позначається розширенням кільця (поля) $(\mathcal{R}_1, +, \cdot)$ до кільця (поля) $(\mathcal{R}, +, \cdot)$.

Приклади

1. Кільце $(\mathbb{Z}[i],+,\cdot)$, $(\mathbb{Z}[i]=\{n+mi\,,n,m\in\mathbb{Z}\}$ – множина гауссових чисел) є розширенням кільця $(\mathbb{Z},+,\cdot)$.
2. $\mathbb{Z}[\omega]=\{n+m\omega\,|n,m\in\ \mathbb{Z}\}$, де $\omega=\left(\cos\frac{2\pi}{3}+i\sin\frac{2\pi}{3}\right)$ – множина чисел Ейзенштейна. $(\mathbb{Z}[\omega],+,\cdot)$ – розширення кільця $(\mathbb{Z},+,\cdot)$.
3. Поле комплексних чисел $(\mathbb{C},+,\cdot)$ є розширенням поля дійсних чисел $(\mathbb{R},+,\cdot)$.

Лінійний простір

Означення 13.2. *Лінійним (або векторним) простором над полем* $\mathbb{F}$ *називається непорожня множина* L *з операціями додавання* $+$ *та множення на елементи поля* $\mathbb{F}$*, які задовольняють умови* $\forall a,b,c\in L,\ \forall\lambda,\mu\in\mathbb{F}$*:*

I. $a+b=b+a$;
II. $(a+b)+c=a+(b+c)$;
III. $\exists 0\in L\colon a+0=a$;
IV. $\exists(-a)\in L\colon a+(-a)=0$;
V. $1a=a$;
VI. $\lambda(\mu a)=(\lambda\mu)a$;
VII. $\lambda(a+b)=\lambda a+\lambda b$;
VIII. $(\lambda+\mu)a=\lambda a+\mu a$.

Елементи лінійного простору L будемо називати векторами.

Базис і розмірність векторного простору

Означення 13.4. *Систему векторів* $a_1,a_2,\dots,a_n$ *лінійного простору* L *називають лінійно незалежною, якщо з рівності*

$$\lambda_1a_1+\lambda_2a_2+\cdots+\lambda_na_n=0$$

випливає, що

$$\lambda_1=\lambda_2=\cdots=\lambda_n=0,$$

де $\lambda_1,\lambda_2,\dots,\lambda_n$ *– елементи поля* $\mathbb{F}$.

Якщо ж існує набір $\{\lambda_1, \lambda_2, \dots, \lambda_n\} \subset \mathbb{F}$*, не всі з яких дорівнюють нулю і*

$$\lambda_1 a_1 + \lambda_2 a_2 + \cdots + \lambda_n a_n = 0,$$

то систему векторів $a_1, a_2, \dots, a_n$ *називають лінійно незалежною.*

Означення 13.5. *Базисом лінійного простору L називають лінійно незалежну систему з найбільш можливою кількістю векторів. Вектори, що утворюють базис лінійного простору, називаються базисними, а кількість векторів базису називають вимірністю L і позначають* $\dim(L)$.

Легко перевірити, що будь яке розширення $\mathbb{E}/\mathbb{F}$ поля $(\mathbb{F}, +, \cdot)$ до поля $(\mathbb{P}, +, \cdot)$ є векторним простором $\mathbb{E}$ над полем $\mathbb{F}$. Розмірність цього векторного простору позначається $[\mathbb{E}: \mathbb{F}]$.

Означення 13.6. *Розширення* $\mathbb{E}/\mathbb{F}$ *називається скінченним, якщо векторний простір* $\mathbb{E}$ *над полем* $\mathbb{F}$ *є скінченновимірним, тобто* $[\mathbb{E}: \mathbb{F}] < \infty$*. У протилежному випадку розширення* $\mathbb{E}/\mathbb{F}$ *називається нескінченним. Розмірність* $[\mathbb{E}: \mathbb{F}]$ *простору* $\mathbb{E}/\mathbb{F}$ *називають* ***степенем розширення****.*

По іншому, розширення $(\mathbb{E}, +, \cdot)$ поля $(\mathbb{F}, +, \cdot)$ є скінченним, якщо існують елементи $a_0, a_1, \dots, a_n \in \mathbb{E}$ такі, що кожен елемент $b \in \mathbb{E}$ єдиним чином зображується у вигляді

$$b = \beta_0 a_0 + \beta_1 a_1 + \cdots + \beta_n a_n,$$

де $\beta_k \in \mathbb{F}$, $k = 0,1,2, \dots, n$.

Приклади

1) Поле $\left(\mathbb{Q}\left(\sqrt{2}\right), +, \cdot\right)$, де $\mathbb{Q}\left(\sqrt{2}\right) = \left\{x + y\sqrt{2} \,|x, y \in \mathbb{Q}\right\}$ є скінченим розширенням поля $\mathbb{Q}$, оскільки $\left[\mathbb{Q}\left(\sqrt{2}\right): \mathbb{Q}\right] = 2$.
2) Поле комплексних чисел $(\mathbb{C}, +, \cdot)$ є скінченим розширенням поля дійсних чисел $(\mathbb{R}, +, \cdot)$, оскільки $\mathbb{C} = \mathbb{R}(i) = \{x + yi \,|x, y \in \mathbb{R}\}$ і $[\mathbb{C}: \mathbb{R}] = 2$.
3) Поле дійсних чисел $(\mathbb{R}, +, \cdot)$ є нескінченним розширенням поля раціональних чисел $(\mathbb{Q}, +, \cdot)$.

4) Поле гауссових чисел $(\mathbb{Q}(i), +, \cdot)$, де $\mathbb{Q}(i) = \{x + yi \,|x, y \in \mathbb{Q}\}$ є скінченим розширенням поля $\mathbb{Q}$

Означення 13.4. *Нехай* $(\mathbb{F}, +, \cdot)$, $(\mathbb{F}_1, +, \cdot)$, $(\mathbb{F}_2, +, \cdot)$, … , $(\mathbb{F}_n, +, \cdot)$ *– поля. Тоді співвідношення* $\mathbb{F} \subset \mathbb{F}_1 \subset \mathbb{F}_2 \subset \cdots \subset \mathbb{F}_n$ *називають вежею полів. Вежа полів може бути нескінченною.*

Лема 13.1. *Для вежі полів* $\mathbb{F} \subset \mathbb{P} \subset \mathbb{H}$ *має місце*

$$[\mathbb{P}: \mathbb{F}] = [\mathbb{H}: \mathbb{P}][\mathbb{P}: \mathbb{F}].$$

Доведення. Нехай $\boldsymbol{E}$ – базис в $\mathbb{P}/\mathbb{F}$, а $\boldsymbol{B}$ – базис в $\mathbb{H}/\mathbb{P}$. Тоді множина $\{x \cdot y \,|x \in \boldsymbol{E}, y \in \boldsymbol{B}\} \subset \mathbb{P}$ – базис в $\mathbb{P}$.

Нехай $\mathbb{P}/\mathbb{F}$ – деяке розширення поля $\mathbb{F}$, а $a_1, \dots, a_n \in \mathbb{P}$, $n \in \mathbb{N}$ – довільні елементи поля $\mathbb{P}$, які не містяться в $\mathbb{F}$.

Означення 13.5. *Найменше поле, яке містить одночасно* $\mathbb{F}$ *і* $a_1, \dots, a_n$ *називається скінченно породженим розширенням, породженим скінченною кількістю елементів* $a_1, \dots, a_n$.

Розширення поля $\mathbb{F}$, породжене числами $a_1, \dots, a_n$ позначається через $\mathbb{F}(a_1, \dots, a_n)$.

Якщо $n = 1$ розширення називають простим.

ІІ ОСНОВИ ТЕОРІЇ ГАЛУА

ЛЕКЦІЯ 14. **АЛГЕБРАЇЧНІ РОЗШИРЕННЯ ПОЛІВ**

Означення 14.1. *Число* a *називається алгебраїчним над полем* $(\mathbb{F}, +, \cdot)$, *якщо* a *є коренем деякого ненульового многочлена з коефіцієнтами із* $\mathbb{F}$. *Неалгебраїчні числа називаються* ***трансцендентними***.

Наприклад, $\sqrt{2}$ є алгебраїчним над полем раціональних чисел $\mathbb{Q}$, оскільки $\sqrt{2}$ є коренем рівняння $x^2 - 2 = 0$, а числа π та e– алгебраїчні над полем дійсних чисел $\mathbb{R}$, але трансцендентні над полем $\mathbb{Q}$.

Якщо будь-яке алгебраїчне число над полем $(\mathbb{F}, +, \cdot)$ належить $\mathbb{F}$, то поле називається *алгебраїчно замкнутим*.

Із основної теореми алгебри комплексних чисел випливає, що поле комплексних чисел є алгебраїчно замкнутим.

Означення 14.2. *Розширення* $(\mathbb{E}, +, \cdot)$ *поля* $(\mathbb{F}, +, \cdot)$ *називається* ***алгебраїчно породженим***, *якщо існують алгебраїчні над полем* $\mathbb{F}$ *числа* $a_1, \dots, a_n$ *такі, що* $\mathbb{E} = \mathbb{F}(a_1, a_2, \dots, a_n)$. *Якщо* $n = 1$, *то* $\mathbb{E} = \mathbb{F}(a_1)$ *називається простим алгебраїчним розширенням.*

Означення 14.3. *Розширення* $(\mathbb{E}, +, \cdot)$ *поля* $(\mathbb{F}, +, \cdot)$ *називається* ***складово алгебраїчним розширенням***, *якщо існує такий ланцюжок підполів*

$$\mathbb{F} = L_1 \subset L_2 \subset \cdots \subset L_r = \mathbb{E},$$

що для довільного $k = 2, \dots, r$ *поле* L_k *є простим алгебраїчним розширенням поля* L_{k-1}.

Означення 14.4. *Розширення* $(\mathbb{E}, +, \cdot)$ *поля* $(\mathbb{F}, +, \cdot)$ *називається* ***алгебраїчним***, *якщо будь-який елемент поля* $\mathbb{E}$ *є алгебраїчним над полем* $\mathbb{F}$.

Алгебраїчність скінченних розширень

Теорема 14.1. *Будь-яке скінченне розширення є алгебраїчним.*

Доведення. Нехай $\mathbb{E}/\mathbb{F}$ – скінченне розширення і $[\mathbb{E}:\mathbb{F}] = n \in \mathbb{N}$. Для довільного $b \in \mathbb{E}$ вектори $1, b, \ldots, b^n$ – лінійно залежні як $n+1$ вектор в n-вимірному просторі. Отже, існують числа $\beta_0, \beta_1, \ldots, \beta_n$ такі, що

$$\beta_0 + \beta_1 b + \cdots + \beta_n b^n = 0.$$

Тобто b – є алгебраїчним числом як корінь многочлена $\beta_0 + \beta_1 x + \cdots + \beta_n x^n$.

Наслідок 14.1. *Із доведення теореми випливає, що при* $[\mathbb{E}:\mathbb{F}] = n$*, якщо* $b \in \mathbb{E}$ *є коренем многочлена* $p(x) \in \mathbb{F}[x]$*, то* $\deg(p) \leq n$.

Наслідок 14.2. *Поле дійсних чисел не є скінченним розширенням поля раціональних чисел, оскільки, як уже відзначалось, числа* π *та* e *– неалгебраїчні, тобто трансцендентні над* $\mathbb{Q}$ (*приймається без доведення*).

Означення 14.5. *Розширення, що містить трансцендентні елементи називається трансцендентним розширенням.*

Очевидно, що поле дійсних чисел є трансцендентним розширенням раціональних чисел.

Означення 14.6. *Мінімальним многочленом для алгебраїчного числа* α *над полем* $\mathbb{F}$ *називається многочлен, старший коефіцієнт якого дорівнює одиниці поля, а його степінь мінімальна із усіх многочленів з коефіцієнтами із* $\mathbb{F}$*, для яких* α *є коренем.*

Мінімальний многочлен фіксованого алгебраїчного числа будемо позначати через $I(x)$.

ЛЕКЦІЯ 15. **ПРОБЛЕМИ ПОБУДОВИ ЦИРКУЛЕМ І ЛІНІЙКОЮ**

Теорема 15.1. *Просте алгебраїчне розширення* $\mathbb{E} = \mathbb{F}[\alpha]$ *поля* $\mathbb{F}$ *має розмірність, що дорівнює степеню мінімального многочлена* $I(x)$ *для* α.

Доведення. Нехай $\deg(I) = n$, $I(x) = b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1} + \alpha^n$. Очевидно, що елементи 1, α,…, α^{n-1} є лінійно незалежними над полем $\mathbb{F}$, інакше існував би многочлен степені $n-1$, для якого α є коренем, що суперечить припущенню $\deg(I) = n$.

Позначимо через $\mathbb{F}_{n-1}[x]$ многочлени степені не вищої $n-1$ з коефіцієнтами із поля $\mathbb{F}$. Покажемо, що виразами $p(\alpha) = c_0 + c_1\alpha + \cdots + c_{n-1}\alpha^{n-1}$, $p \in \mathbb{F}_{n-1}[x]$, однозначно описуються всі елементи поля $\mathbb{P}$. Нехай $p, q \in \mathbb{F}_{n-1}[x]$, тоді очевидно, що $p \pm q \in \mathbb{F}_{n-1}[x]$.

Покажемо, що $p(\alpha)q(\alpha) = d(\alpha)$, де $d \in \mathbb{F}_{n-1}[x]$. При перемноженні вирізів $p(\alpha)q(\alpha)$ може з'явитися доданок, який містить α^k, де $n \le k \le 2n-2$. Із $I(\alpha) = 0$ випливає $\alpha^n = -b_0 - b_1\alpha - \cdots - b_{n-1}\alpha^{n-1}$, тому ми можемо понизити степінь α^k, якщо $n \le k$, наприклад, якщо $k = 2n-2$ (тобто k приймає максимальне значення), то

$$\alpha^{2n-2} = \alpha^{n-2}\alpha^n = -b_0\alpha^{n-2} - b_1\alpha^{n-1} - \cdots - b_{n-1}\alpha^{2n-3}.$$

Продовжуючи підставляти $-b_0 - b_1\alpha - \cdots - b_{n-1}\alpha^{n-1}$ замість α^n можна досягнути щоб у виразі $p(\alpha)q(\alpha)$ максимальний степінь α був $n-1$.

Покажемо, що якщо $p = c_0 + c_1x + \cdots + c_{n-1}x^{n-1}$ не нульовий многочлен, то $1/p(\alpha) = g(\alpha)$, де $g \in \mathbb{F}_{n-1}[x]$. Найбільший спільний дільник многочленів $p(x)$ та $I(x)$ є константа, інакше $I(x)$ розкладався в добуток многочленів степенів менших ніж n, один із яких має корінь α, що суперечить мінімальності многочлена $I(x)$ для α. Звідси із співвідношення (11.1) випливає, що існують многочлени $u(x)$ та $v(x)$, $u, v \in \mathbb{F}_{n-1}[x]$ такі, що

$$I(x)u(x) + p(x)v(x) = 1.$$

Підставляючи $x = \alpha$ з урахуванням $I(\alpha) = 0$, маємо

$$p(\alpha)v(\alpha) = 1.$$

Отже,

$$v(\alpha) = 1/p(\alpha) = \frac{1}{c_0 + c_1\alpha + \cdots + c_{n-1}\alpha^{n-1}}.$$

Звідки безпосередньо випливає, що якщо $q(x)$ не нульовий многочлен, то

$$\frac{p(\alpha)}{q(\alpha)} = d(\alpha), \qquad d(x) \in \mathbb{F}_{n-1}[x].$$

Отже, вирази $p(\alpha) = c_0 + c_1\alpha + \cdots + c_{n-1}\alpha^{n-1}$, $p \in \mathbb{F}_{n-1}[x]$ з операціями додавання і множення із поля $\mathbb{F}$ утворюють мінімальне поле, яке містить $\mathbb{F}$ (покласти у виразі нулю всі коефіцієнти крім c_0) і містить α, тобто збігається з розширенням $\mathbb{E} = \mathbb{F}[\alpha]$.

Побудови циркулем та лінійкою

1. Будь-який відрізок, що має дожину $a \in \mathbb{N}$;
2. Будь-який відрізок дожини $a = m/n$, де $m, n \in \mathbb{N}$;
3. $\sqrt{ab}$, якщо задані відрізки a, b. Зокрема можна побудувати $\sqrt{a}$;
4. ab, якщо задані відрізки a, b. Зокрема можна побудувати a^2;
5. a/b, якщо задані відрізки a, b.

Вправа 15.1. Переконатись у справедливості тверджень 1-5.

Отже, за допомогою циркуля і лінійки можна побудувати відрізки довжини яких є елементами множини чисел, що є розширенням поля раціональних чисел $\mathbb{Q}$, яка крім раціональних чисел містить усі лінійні комбінації з раціональними коефіцієнтами від парних коренів додатних раціональних чисел. Неважко переконатись, що таке розширення є полем, яке будемо позначати через $\mathbb{Q}\left(\sqrt[2^n]{\cdot}\right)$, $n \in \mathbb{N}$.

Вправа 15.2. Довести, що $\mathbb{Q}\left(\sqrt[2^n]{\cdot}\right)$ є полем.

Лема 15.1. *За допомогою циркуля і лінійки можна побудувати тільки відрізки довжини d, де $d \in \mathbb{Q}\left(\sqrt[2^n]{\cdot}\right)$.*

Доведення. Нехай OXY декартова система координат. Відкладемо на осях OX та OY відрізки довжин α_k та β_k відповідно, де $\alpha_k, \beta_k \in \mathbb{Q}\left(\sqrt[2^n]{\cdot}\right)$, $k = 1,2$,

тобто одержимо дві точки на площині $O_1(\alpha_1, \beta_1)$ та $O_2(\alpha_2, \beta_2)$. Покажемо, що за допомогою циркуля неможливо побудувати точку, хоча б одна координата якої не належить $\mathbb{Q}\left(\sqrt[2^n]{\cdot}\right)$. Нехай $S(O_1, r_1)$ та $S(O_2, r_2)$ два кола з центрами $O_k(\alpha_k, \beta_k)$ і радіусами r_k, $k = 1{,}2$ відповідно, де $r_k \in \mathbb{Q}\left(\sqrt[2^n]{\cdot}\right)$. Якщо ці кола перетинаються, то координати точок перетину задовольняють систему рівнянь

$$\begin{cases} (x-\alpha_1)^2 + (y-\beta_1)^2 = r_1^2 \\ (x-\alpha_2)^2 + (y-\beta_2)^2 = r_2^2 \end{cases} \tag{14.1}$$

Віднімемо від першого рівняння друге рівняння системи (14.1), маємо

$$2(\alpha_2 - \alpha_1)x + 2(\beta_2 - \beta_1)y + \alpha_1^2 + \beta_1^2 - \alpha_2^2 - \beta_2^2 + r_2^2 - r_1^2 = 0.$$

Звідки випливає, що

$$y = Ax + B,$$

де $A, B \in \mathbb{Q}\left(\sqrt[2^n]{\cdot}\right)$, або $x = Ay + B$, якщо $\beta_2 = \beta_1$.

Підставляючи $y = Ax + B$ (або $x = Ay + B$) в одне із рівнянь системи (14.1), ми одержимо квадратне рівняння відносно y (або x) з коефіцієнтами із $\mathbb{Q}\left(\sqrt[2^n]{\cdot}\right)$. Але розв'язок такого квадратного рівняння є число із поля $\mathbb{Q}\left(\sqrt[2^n]{\cdot}\right)$, оскільки при знаходженні кореня квадратного рівняння ми використовуємо операції додавання, віднімання, множення і ділення та взяття квадратного кореня над числами A, B, то одержимо число, що належить полю $\mathbb{Q}\left(\sqrt[2^n]{\cdot}\right)$. А якщо $y \in \mathbb{Q}\left(\sqrt[2^n]{\cdot}\right)$ (чи $x \in \mathbb{Q}\left(\sqrt[2^n]{\cdot}\right)$), то і $x \in \mathbb{Q}\left(\sqrt[2^n]{\cdot}\right)$ (чи $y \in \mathbb{Q}\left(\sqrt[2^n]{\cdot}\right)$), що випливає із співвідношення $y = Ax + B$ (або $x = Ay + B$), де $A, B \in \mathbb{Q}\left(\sqrt[2^n]{\cdot}\right)$.

Очевидно, що якщо крім циркуля застосувати лінійку, то побудовані точки також будуть мати координати із $\mathbb{Q}\left(\sqrt[2^n]{\cdot}\right)$, оскільки пряма $y = Ax + B$ (або $x = Ay + B$), що проходить через точки з координатами із $\mathbb{Q}\left(\sqrt[2^n]{\cdot}\right)$має коефіцієнти $A, B \in \mathbb{Q}\left(\sqrt[2^n]{\cdot}\right)$.

Можна також скористатися теоремою Мора-Маскероні, яка стверджує: що можна побудувати за допомогою циркуля з лінійкою, можна побудувати за допомогою одного циркуля, тобто інших точок при побудові циркуля і лінійки ми не одержимо.

Неможливість подвоєння куба

Нехай об'єм куба дорівнює одиниці і за допомогою циркуля та лінійки потрібно побудувати куб вдвічі більшого об'єму. Очевидно, що для розв'язку такої задачі потрібно побудувати відрізок довжиною $\sqrt[3]{2}$.

Розглянемо вежу полів $\mathbb{Q} = \mathbb{F}_0 \subset \mathbb{F}_1 \subset \cdots \subset \mathbb{F}_{k-1} \subset \mathbb{F}_k$, таку, що $[\mathbb{F}_i : \mathbb{F}_{i-1}] = 2$, $i = 1, \dots, k$, тобто, поле $\mathbb{F}_i$ одержуємо розширенням поля $\mathbb{F}_{i-1}$, додаючи один елемент q, який є квадратним коренем із якогось додатного елемента поля $\mathbb{F}_{i-1}$, причому $q \notin \mathbb{F}_{i-1}$. (Очевидно, що відрізок довжиною q завжди можна побудувати за допомогою циркуля і лінійки). Зрозуміло, що довжина будь-якого відрізка, який можна побудувати за допомогою циркуля та лінійки лежить у полі таких веж при достатньо великому $k \in \mathbb{N}$. Припустимо, що можна побудувати $\sqrt[3]{2}$ за допомогою циркуля та лінійки.

Розглянемо поле $\mathbb{Q}(\sqrt[3]{2})$. Тоді $\mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{F}_k$ для досить великого $k \in \mathbb{N}$. Тоді, з урахуванням того, що $[\mathbb{F}_k : \mathbb{Q}(\sqrt[3]{2})] = 3$, із леми 13.1 та теореми 14.2 випливає

$$2^k = [\mathbb{F}_k : \mathbb{Q}] = [\mathbb{F}_k : \mathbb{Q}(\sqrt[3]{2})] \cdot [\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3 \cdot [\mathbb{F}_k : \mathbb{Q}(\sqrt[3]{2})],$$

де $[\mathbb{F}_k : \mathbb{Q}(\sqrt[3]{2})] \in \mathbb{N}$, що неможливо.

Неможливість трисекції кута

Кут $\alpha = 30°$ не можна розділити на три рівні частини за допомогою циркулі і лінійки, тобто побудувати кут $10°$, оскільки $\alpha = \sin 10°$ задовольняє кубічне рівняння над полем раціональних чисел

$$4\alpha^3 - 3\alpha + \frac{1}{2} = 0,$$

де $4\alpha^3 - 3\alpha + \frac{1}{2}$ – незвідний многочлен над полем раціональних чисел (переконайтесь!). Тобто мінімальний многочлен $I(x)$ для α має степінь 3.

Вправа 15.3. Довести неможливість квадратури кола, тобто неможливо за допомогою циркуля та лінійки побудувати квадрат, рівновеликий за площею до заданого круга.

ЛЕКЦІЯ 16. **ПОЛЕ АЛГЕБРАЇЧНИХ ЧИСЕЛ**

Означення 16.1. *Підмножина* $\mathbb{A}$ *комплексних чисел називається множиною алгебраїчних чисел, якщо будь-яке* $x \in \mathbb{A}$ *є коренем ненульового многочлена* $f(x) = a_0 + a_1x + \cdots + a_nx^n$ *над полем раціональних чисел, тобто є розв'язком рівняння*

$$a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 = 0, \qquad (15.1)$$

де $a_k \in \mathbb{Q}$, $a_n \neq 0$, $n \in \mathbb{N}$.

Наприклад, будь-яке раціональне число r є алгебраїчним, оскільки це число – розв'язок рівняння

$$x - r = 0.$$

Інший приклад: i, $-i$ є алгебраїчними числами, оскільки вони розв'язки рівняння

$$x^2 + 1 = 0.$$

Будь-яке неалгебраїчне комплексне число називається *трансцендентним*.

Твердження 16.1. *Якщо* $t \in \mathbb{A}$, *то* $-t \in \mathbb{A}$.

Доведення. Дійсно, якщо $t \in \mathbb{A}$, то існує многочлен $a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$, де $a_k \in \mathbb{Q}$, $a_n \neq 0$, $n \in \mathbb{N}$ такий, що t є його корінь, тобто

$$a_nt^n + a_{n-1}t^{n-1} + \cdots + a_1t + a_0 = 0.$$

Якщо n парне, то легко бачити, що $-t$ задовольняє рівняння

$$a_nx^n - a_{n-1}x^{n-1} + a_{n-2}t^{n-2} - \cdots + a_2x^2 - a_1x + a_0 = 0.$$

Отже, $-t$ є також алгебраїчним числом.

Вправа 16.1. Розглянути випадок, коли $n \in \mathbb{N}$ непарне.

Вправа 16.2. Довести, що якщо $t, s \in \mathbb{A}$, то $t + s \in \mathbb{A}$, $t \cdot s \in \mathbb{A}$, а коли $s \neq 0$, то $\frac{t}{s} \in \mathbb{A}$. Тобто $(\mathbb{A}, +, \cdot)$ є полем, яке називається *полем алгебраїчних чисел*.

Зауваження. Якщо не удалось самостійно виконати вправу 15.2, то нижче наводиться теорема 15.1, яка дає відповідь на вправу 15.2.

Вправа 16.3. Довести, що не існує підполя поля раціональних чисел $\mathbb{Q}$, яке не збігається з самим полем $\mathbb{Q}$, тобто не існує власного підполя $\mathbb{Q}$.

Теорема 16.1. *Множина алгебраїчних чисел* $\mathbb{A}$ *є полем.*

Доведення. Нехай $t, s \in \mathbb{A}$. Розглянемо розширення поля раціональних чисел: $\mathbb{Q}(t)$ та $\mathbb{Q}(t, s) = \big(\mathbb{Q}(t)\big)(s)$. Оскільки t алгебраїчне число, то $[\mathbb{Q}(t): \mathbb{Q}] < \infty$. З тих же міркувань $[\mathbb{Q}(s): \mathbb{Q}] < \infty$. Але очевидно, що $[\mathbb{Q}(t, s): \mathbb{Q}(t)] \leq [\mathbb{Q}(s): \mathbb{Q}]$ оскільки найменший степінь многочлена над $\mathbb{Q}$ для якого s корінь не більший степеня многочлена над $\mathbb{Q}(t)$ для якого s корінь. Тоді, із леми 13.1 випливає, що

$$[\mathbb{Q}(t, s): \mathbb{Q}] = [\mathbb{Q}(t, s): \mathbb{Q}(t)] \cdot [\mathbb{Q}(t): \mathbb{Q}] \leq [\mathbb{Q}(s): \mathbb{Q}] \cdot [\mathbb{Q}(t): \mathbb{Q}] < \infty.$$

Оскільки $\mathbb{Q}(t, s)$ – поле, то $t \pm s \in \mathbb{Q}(t, s)$, $t \cdot s \in \mathbb{Q}(t, s)$, при $s \neq 0$, $\frac{t}{s} \in \mathbb{Q}(t, s)$, а це означає, що існують многочлени скінченного степеню над $\mathbb{Q}$ для яких ці значення є коренями, тобто $t \pm s \in \mathbb{A}$, $t \cdot s \in \mathbb{A}$, при $s \neq 0$, $\frac{t}{s} \in \mathbb{A}$.

Теорема 16.2. *Поле алгебраїчних чисел* $\mathbb{A}$ *є алгебраїчно замкнутим.*

Доведення. Розглянемо многочлен над полем $\mathbb{A}$ степені $n \in \mathbb{N}$, тобто

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0,$$

де $a_k \in \mathbb{A}$, $k = 0,1, \ldots, n$, $a_n \neq 0$.

Нехай α є коренем цього многочлена. Покажемо, що α – алгебраїчне число, тобто $\alpha \in \mathbb{A}$. Розглянемо таку вежу розширень полів:

$$\mathbb{Q} \subset \mathbb{Q}(a_0) \subset \mathbb{Q}(a_0, a_1) \subset \cdots \subset \mathbb{Q}(a_0, a_1, \ldots, a_n) \subset \mathbb{Q}(a_0, a_1, \ldots, a_n, \alpha).$$

Оскільки $a_k,\ k = 0,1, \dots, n$ – алгебраїчні, то на кожному кроці розмірність розширення скінченна

$$[\mathbb{Q}(a_0, a_1, \dots, a_k): \mathbb{Q}(a_0, a_1, \dots, a_{k-1})] < \infty.$$

Крім цього, $[\mathbb{Q}(a_0, a_1, \dots, a_n, \alpha): \mathbb{Q}(a_0, a_1, \dots, a_n)] < \infty$ оскільки α – корінь многочлена і коефіцієнтами із поля $\mathbb{Q}(a_0, a_1, \dots, a_n)$, тобто $\mathbb{Q}(a_0, a_1, \dots, a_n, \alpha)$ є алгебраїчним розширенням поля $\mathbb{Q}(a_0, a_1, \dots, a_n)$.

З урахуванням леми 13.1, розмірність розширення $\mathbb{Q}(a_0, a_1, \dots, a_n, \alpha)$ над $\mathbb{Q}$ є скінченною, тобто послідовність $1, \alpha, \alpha^2, \dots, \alpha^N$ є лінійно залежною над $\mathbb{Q}$ для деякого скінченного $N \in \mathbb{N}$, а, отже, α є коренем деякого многочлена N-го степеня з раціональними коефіцієнтами і, значить, α – алгебраїчне число.

Далі, скрізь, де не зазначено протилежне, ми розглядаємо поля характеристики нуль.

Теорема 16.3. (Про примітивний елемент) *Нехай* $\mathbb{E}$ *є скінченним розширенням поля* $\mathbb{F}$*, тобто* $[\mathbb{E}: \mathbb{F}] = n \in \mathbb{N}$*. Тоді* $\exists \gamma \in \mathbb{E}: \mathbb{E} = \mathbb{F}(\gamma)$.

Доведення. Оскільки $\mathbb{E}$ – скінченне розширення, то $\exists \alpha, \beta, \lambda_1, \dots, \lambda_{n-2} \in \mathbb{E}$:

$$\mathbb{F} \subset \mathbb{F}(\alpha) \subset \mathbb{F}(\alpha, \beta) \subset \cdots \subset \mathbb{F}(\alpha, \beta, \lambda_1, \dots, \lambda_{n-2}) = \mathbb{E}.$$

Досить показати, що $\exists \gamma \in \mathbb{E}$:

$$\mathbb{F} \subset \mathbb{F}(\alpha) \subset \mathbb{F}(\alpha, \beta) = \mathbb{F}(\gamma).$$

Очевидно, що α і β – алгебраїчні числа, а, отже, існують їх мінімальні многочлени з коефіцієнтами із поля $\mathbb{F}$ такі, що

$$f(x) = (x - \alpha)(x - \alpha_1) \dots (x - \alpha_r),$$

$$g(x) = (x - \beta)(x - \beta_1) \dots (x - \beta_s).$$

Доведемо існування $\theta \in \mathbb{F}$ такого, що $\alpha_i + \theta\beta_j \neq \alpha_l + \theta\beta_m$, якщо $i \neq l$ або $j \neq m, i, l = 0,1, \dots, r, j, m = 0,1, \dots, s$, де $\alpha_0 = \alpha, \beta_0 = \beta$. Оскільки всіх різних α_i,

β_j, є $(r+1)\cdot(s+1)$ пар, а $\mathbb{F}$ – поле характеристики нуль, то, очевидно, що таке θ існує. Покладемо $\gamma = \alpha + \theta\beta$.

Легко бачити, що $\mathbb{F} \subset \mathbb{F}[\gamma] \subset \mathbb{E}$, оскільки $\gamma = \alpha + \theta\beta \in \mathbb{F}(\alpha, \beta) = \mathbb{E}$.

Розглянемо многочлен:

$$p(x) = f(\gamma - \theta x) = a_0 + a_1(\gamma - \theta x) + a_2(\gamma - \theta x)^2 + \cdots = b_0 + b_1 x + b_2 x^2 + \cdots$$

де $b_k \in \mathbb{F}[\gamma]$, тобто $p(x) \in \mathbb{F}[\gamma][x]$.

Многочлени $p(x)$ та $g(x)$ мають спільний корінь β, дійсно,

$$p(\beta) = f(\gamma - \theta\beta) = f(\alpha) = 0,$$

а $g(\beta) = 0$ за побудовою.

Оскільки $\alpha_i + \theta\beta_j$ різні при різних i та j, то більше спільних коренів $p(x)$ та $g(x)$ не мають. Дійсно, крім β многочлен $g(x)$ має корені β_j, $j = 1, \ldots, s$, але тоді

$\gamma - \theta\beta_j = \alpha_i$, для якихось i та j, тобто $\gamma = \alpha_i + \theta\beta_j$, що неможливо, оскільки тоді $\alpha_i + \theta\beta_j = \gamma = \alpha + \theta\beta$.

Отже, $\text{НСД}\big(p(x), g(x)\big) = x - \beta$. Тоді за формулою (11.1) існують многочлени $u(x), v(x) \in \mathbb{F}(\gamma)[x]$ такі, що

$$\mathbb{F}(\gamma)[x] \ni f(x)\cdot u(x) + g(x)\cdot v(x) = x - \beta.$$

Звідки $\beta \in \mathbb{F}(\gamma)$. З урахуванням того, що $\alpha \in \mathbb{F}(\gamma)$ випливає, що $\mathbb{F}(\gamma) = \mathbb{F}(\alpha, \beta)$.

ЛЕКЦІЯ 17. **ГРУПА ГАЛУА. ОСНОВНА ТЕОРЕМА ТЕОРІЇ ГАЛУА**

Група Галуа та її базові властивості

Означення 17.1. *Нехай поле* $\mathbb{E}$ *є розширенням поля* $\mathbb{F}$. *Групою автоморфізмів розширення* $\mathbb{E}/\mathbb{F}$ *називається сукупність всіх автоморфізмів* $\varphi: \mathbb{E} \to \mathbb{E}$ *таких, що* $\forall a \in \mathbb{F}$

$$\varphi(a) = a.$$

Позначається $\mathrm{Aut}(\mathbb{P}/\mathbb{F})$.

Вправа 17.1. Переконатись, що $\mathrm{Aut}(\mathbb{E}/\mathbb{F})$ з операцією композиції автоморфізмів справді є групою.

Означення 17.2. *Нехай поле* $\mathbb{E}$ *є алгебраїчним розширенням поля* $\mathbb{F}$. *Групою Галуа* $\mathbb{E}/\mathbb{F}$ *називається така група автоморфізмів розширення* $\mathbb{E}/\mathbb{F}$, *що кількість елементів (автоморфізмів) цієї групи дорівнює степеню розширення* $\mathbb{E}/\mathbb{F}$, *тобто*

$$|\mathrm{Aut}(\mathbb{E}/\mathbb{F})| = [\mathbb{E}: \mathbb{F}].$$

Позначається $\mathrm{Gal}(\mathbb{E}/\mathbb{F})$.

Нехай многочлен $f \in \mathbb{F}[x]$ розкладається у полі $\mathbb{E}$ на добуток многочленів першого степеню:

$$f(x) = (x - \alpha_1)(x - \alpha_2) \dots (x - \alpha_k) \in \mathbb{E}[x], \qquad (17.1)$$

де $\alpha_i \neq \alpha_j$, якщо $i \neq j$, тобто $f(x)$ не має кратних коренів.

Розширення $\mathbb{E}$ поля $\mathbb{F}$ називається полем розкладу многочлена $f \in \mathbb{F}[x]$, якщо у ньому $f(x) = (x - \alpha_1)(x - \alpha_2) \dots (x - \alpha_k)$ причому $\mathbb{E} = \mathbb{F}(\alpha_1, \alpha_2, \dots, \alpha_k)$.

Приклад. Для многочлена $x^2 + 1 \in \mathbb{R}[x]$ полем розкладу є поле комплексних чисел $\mathbb{C}$.

Означення 17.3. *Алгебраїчне розширення* $\mathbb{E}/\mathbb{F}$ *називається* ***нормальним****, якщо будь-який незвідний над* $\mathbb{F}$ *многочлен, що має хоча б один корінь в* $\mathbb{E}$ *розкладається в* $\mathbb{E}$ *на лінійні множники.*

Означення 17.4. *Алгебраїчне розширення* $\mathbb{E}/\mathbb{F}$ *називається* ***сепарабельним****, якщо будь-який елемент розширення є коренем многочлена, який не має кратних коренів у своєму полі розкладу.*

Означення 17.5. *Нормальне і сепаребельне алгебраїчне розширення* $\mathbb{E}/\mathbb{F}$ *називається розширенням Галуа*.

Означення 17.6. *Групою Галуа многочлена* f *називається група Галуа* $\mathbb{E}/\mathbb{F}$*, де* $\mathbb{E}$ *мінімальне поле, у якому виконується* (17.1).

Група Галуа многочлена $f \in \mathbb{F}[x]$ не міняє коефіцієнти многочлена, оскільки вони належать $\mathbb{F}$, а тільки перемішує його корені α_i, $i = 1, \dots, k$.

Приклад. Розглянемо групу автоморфізмів розширення $\mathbb{Q}[\sqrt[3]{2}]/\mathbb{Q}$. Оскільки многочлен $x^3 - 2 = (x - \sqrt[3]{2})(x - \sqrt[3]{2}\omega)(x - \sqrt[3]{2}\omega^2)$, де $\omega = \left(\cos\frac{2\pi}{3} + i\sin\frac{2\pi}{3}\right)$ а $\sqrt[3]{2}\omega \notin \mathbb{Q}[\sqrt[3]{2}]$, то група автоморфізмів розширення $\mathbb{Q}[\sqrt[3]{2}]/\mathbb{Q}$ – не група Галуа.

Пояснимо цей факт іншими словами: нехай φ: $\mathbb{Q}[\sqrt[3]{2}] \to \mathbb{Q}[\sqrt[3]{2}]$ автоморфізм розширення $\mathbb{Q}[\sqrt[3]{2}]/\mathbb{Q}$. Нагадаємо, що $\varphi(q) = q, \forall q \in \mathbb{Q}$. Позначимо $\beta = \varphi(\sqrt[3]{2})$. Тоді, за властивістю ізоморфізму $\varphi(a^n) = (\varphi(a))^n$, $n \in \mathbb{N}$, отже,

$$\beta^3 - 2 = \left(\varphi(\sqrt[3]{2})\right)^3 - 2 = \varphi\left((\sqrt[3]{2})^3\right) - 2 = \varphi(2) - 2 = 0.$$

Тобто β є коренем многочлена $x^3 - 2$, коренем якого є й $\sqrt[3]{2}$. Отже, автоморфізм φ може тільки переводити корені $x^3 - 2$ в інші корені $x^3 - 2$. Але коренями многочлена $x^3 - 2$ є $\sqrt[3]{2}$, $\sqrt[3]{2}\omega$, $\sqrt[3]{2}\omega^2$, причому $\sqrt[3]{2}\omega$ та $\sqrt[3]{2}\omega^2$ не дійсні. Тому автоморфізм φ може тільки залишити $\sqrt[3]{2}$ на місці, тобто ніяких нетривіальних автоморфізмів розширення $\mathbb{Q}[\sqrt[3]{2}]/\mathbb{Q}$ не існує, при цьому $[\mathbb{Q}[\sqrt[3]{2}]: \mathbb{Q}] = 3$, що не відповідає означенню 17.6 групи Галуа.

Якщо ж розглянути розширення $\mathbb{Q}\left[\sqrt[3]{2}, \sqrt[3]{2}\omega\right]$, то група автоморфізмів $\mathbb{Q}\left[\sqrt[3]{2}, \sqrt[3]{2}\omega\right]/\mathbb{Q}$ є групою Галуа. (Переконайтесь!)

Очевидно, що $\mathbb{E}$ для якого виконується (15.2) є наступим алгебраїчним розширенням поля $\mathbb{F}$:

$$\mathbb{E} = \mathbb{F}[\alpha_1, \alpha_2, \dots, \alpha_k].$$

Нехай $[\mathbb{E}: \mathbb{F}] = r$. Із теореми про примітивний елемент випливає, що $\exists \gamma \in \mathbb{E}$, що $\mathbb{E} = \mathbb{F}[\gamma]$, причому 1, γ, γ^2,…, γ^{r-1} – лінійно незалежні, тобто утворюють базис $\mathbb{E}/\mathbb{F}$. (Чому?). Нехай многочлен $I(x) \in \mathbb{F}[x]$, $I(x) = b_0 + b_1 x + \cdots + b_{n-1}x^{r-1} + x^r$ є мінімальним для γ. Крім γ многочлен $I(x)$ має ще $r-1$ корінь γ_2,…, γ_r. Розглянемо можливі автоморфізми φ_i, $i = 1, \dots, r$ розширення $\mathbb{E}/\mathbb{F}$:

$$\varphi_1(\gamma) = \gamma,$$

$$\varphi_2(\gamma) = \gamma_2,$$

$$- - - - -$$

$$\varphi_r(\gamma) = \gamma_r.$$

Більше автоморфізмів не існує. Дійсно, якби існував ще один автоморфізм φ_{r+1}, тоді б $\exists i \in \{1,2, \dots, r\}$, для якого $\varphi_{r+1}(\gamma) = \gamma_i = \varphi_i(\gamma)$, а, отже,

$$\varphi_{r+1}(\gamma^k) = \left(\varphi_{r+1}(\gamma)\right)^k = \gamma_i^k = \left(\varphi_i(\gamma)\right)^k = \varphi_i(\gamma^k), k = 1,2, \dots, r-1.$$

Тобто, з урахуванням того, що при довільному автоморфізмі φ, $\varphi(1) = 1$, базис 1, γ, γ^2,…, γ^{r-1} переходить у базис 1, γ_i, ..., γ_i^{r-1}, як при автоморфізмі φ_i так і при автоморфізмі φ_{r+1}, а це означає, що $\forall a \in \mathbb{P}$ $\varphi_{r+1}(a) = \varphi_i(a)$. Дійсно, нехай $a = a_0 + a_1\gamma + \cdots + a_{r-1}\gamma^{r-1}$, $a_l \in \mathbb{F}$, тоді

$$\begin{aligned}\varphi_{r+1}(a) &= a_0 + a_1\varphi_{r+1}(\gamma) + \cdots + a_{r-1}\varphi_{r+1}(\gamma^{r-1}) \\ &= a_0 + a_1\varphi_i(\gamma) + \cdots + a_{r-1}\varphi_i(\gamma^{r-1}) = \varphi_i(a).\end{aligned}$$

Основна теорема теорії Галуа

Лема 17.1. *Нехай* $\mathbb{F} \subset \mathbb{L}$ *– розширення поля причому* $\mathbb{L}/\mathbb{F}$ *– розширення Галуа з групою Галуа* $\mathrm{Gal}(\mathbb{L}/\mathbb{F})$. *Нехай* $\mathbb{E}$ *– розширення поля* $\mathbb{F}$*, причому* $\mathbb{F} \subset \mathbb{E} \subset \mathbb{L}$. *Тоді* $\mathbb{L}/\mathbb{E}$ – розширення Галуа і $\mathrm{Gal}(\mathbb{L}/\mathbb{E})$ *є підгрупою* $\mathrm{Gal}(\mathbb{L}/\mathbb{F})$.

Доведення. Оскільки $\mathbb{F} \subset \mathbb{E}$, то очевидно, що $\mathrm{Aut}(\mathbb{L}/\mathbb{E})$ є підгрупою $\mathrm{Gal}(\mathbb{L}/\mathbb{F})$. Залишається показати, що $\mathbb{L}/\mathbb{E}$ – нормальне і сепарабельне, тобто розширення Галуа. Оскільки $\mathbb{L}/\mathbb{F}$ – розширення Галуа, то $\mathbb{L}$ є полем розкладу для будь-якого многочлена $f \in \mathbb{F}[x]$, тобто поле $\mathbb{L}$ є множиною алгебраїчних чисел над полем $\mathbb{F}$ (див. означення 14.1). Аналогічно доведенню алгебраїчної замкнутості $\mathbb{A}$ в теоремі 16.2 доводиться алгебраїчна замкнутість $\mathbb{L}$, а, отже, з урахуванням $\mathbb{E} \subset \mathbb{L}$, поле $\mathbb{L}$ є полем розкладу для будь-якого многочлена $f \in \mathbb{E}[x]$, тобто $\mathbb{L}/\mathbb{E}$ – нормальне розширення. Покажемо сепарабельність розширення $\mathbb{L}/\mathbb{E}$. Дійсно, нехай $f_\alpha \in \mathbb{E}[x]$ – мінімальний многочлен $\alpha \in \mathbb{L}$ над полем $\mathbb{E}$, а $g_\alpha \in \mathbb{F}[x]$ – мінімальний многочлен α над полем $\mathbb{F}$, тоді g_α ділиться на f_α в $\mathbb{L}[x]$. Оскільки $\mathbb{L}/\mathbb{F}$ сепарабельне, то g_α не має кратних коренів, а, отже, і f_α не має кратних коренів.

Теорема 17.1. Нехай $\mathbb{E}/\mathbb{F}$ та $\mathbb{L}/\mathbb{F}$ – розширення Галуа, де $\mathbb{F} \subset \mathbb{E} \subset \mathbb{L}$. Тоді $\mathrm{Gal}(\mathbb{L}/\mathbb{E}) \lhd \mathrm{Gal}(\mathbb{L}/\mathbb{F})$, тобто $\forall h \in \mathrm{Gal}(\mathbb{L}/\mathbb{E})$, $\forall g \in \mathrm{Gal}(\mathbb{L}/\mathbb{F})$ виконується $g^{-1}hg \in \mathrm{Gal}(\mathbb{L}/\mathbb{E})$.

Доведення. Із умов теореми 16.1 із леми 16.1 випливає, що $\mathbb{L}/\mathbb{E}$ – розширення Галуа. Нехай $g \in \mathrm{Gal}(\mathbb{L}/\mathbb{F})$ і $h \in \mathrm{Gal}(\mathbb{L}/\mathbb{E})$, покажемо, що $\forall x \in \mathbb{E}$ має місце $g^{-1}hg(x) = x$. Із $h \in \mathrm{Gal}(\mathbb{L}/\mathbb{E})$ випливає, що $h(y) = y$ для будь-якого $y \in \mathbb{E}$. Покажемо, що якщо $g \in \mathrm{Gal}(\mathbb{L}/\mathbb{F})$, то $g(x) \in \mathbb{E}$ для всіх $x \in \mathbb{E}$. Враховуючи означення 17.2, маємо

$$|\mathrm{Gal}(\mathbb{L}/\mathbb{F})| = [\mathbb{L}\colon \mathbb{F}],\ |\mathrm{Gal}(\mathbb{L}/\mathbb{E})| = [\mathbb{L}\colon \mathbb{E}],\ |\mathrm{Gal}(\mathbb{E}/\mathbb{F})| = [\mathbb{E}\colon \mathbb{F}].$$

Із леми 13.1 випливає, що

$$[\mathbb{L}\colon \mathbb{F}] = [\mathbb{L}\colon \mathbb{E}][\mathbb{E}\colon \mathbb{F}].$$

Отже, група $\mathrm{Gal}(\mathbb{L}/\mathbb{F})$ складається із композиції автоморфізмів групи $\mathrm{Gal}(\mathbb{L}/\mathbb{E})$ і автоморфізми групи $\mathrm{Gal}(\mathbb{E}/\mathbb{F})$, але автоморфізми групи $\mathrm{Gal}(\mathbb{L}/\mathbb{E})$ діють як тотожні на $\mathbb{E}$, а автоморфізми групи $\mathrm{Gal}(\mathbb{E}/\mathbb{F})$ на виходять за межі поля $\mathbb{E}$, тобто, якщо $x \in \mathbb{E}$, то $g(x) \in \mathbb{E}$ для всіх $x \in \mathbb{E}$ при $g \in \mathrm{Gal}(\mathbb{L}/\mathbb{F})$. Отже, $h\big(g(x)\big) = g(x)$, і, нарешті

$$g^{-1}hg(x) = g^{-1}g(x) = x.$$

Звідси випливає, що $g^{-1}hg \in \mathrm{Gal}(\mathbb{L}/\mathbb{E})$.

Наслідок 17.1. *Фактор-група* $\mathrm{Gal}(\mathbb{L}/\mathbb{F})/\mathrm{Gal}(\mathbb{L}/\mathbb{E})$ *ізоморфна групі* $\mathrm{Gal}(\mathbb{E}/\mathbb{F})$*, тобто*

$$\mathrm{Gal}(\mathbb{L}/\mathbb{F})/\mathrm{Gal}(\mathbb{L}/\mathbb{E}) \simeq \mathrm{Gal}(\mathbb{E}/\mathbb{F}).$$

ЛЕКЦІЯ 18. **НЕРОЗВ'ЯЗУВАНІСТЬ РІВНЯННЯ П'ЯТОГО СТЕПЕНЮ В РАДИКАЛАХ**

Нехай маємо поліноміальне рівняння

$$a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0, \qquad a_k \in \mathbb{Q}, k = 1,2,\dots,n\,.$$

Розв'язати це рівняння у радикалах означає представити формулу, яка місить скінченну кількість операцій додавання/віднімання, множення/ділення та взяття коренів довільних натуральних степенів над коефіцієнтами $a_k, k = 1,2,\dots,n$. Ці операції можна занумерувати послідовністю: №1, №2, …, №m. Оскільки коефіцієнти $a_k \in \mathbb{Q}, k = 1,2,\dots$, то почнемо із поля $\mathbb{Q}$ і, якщо операція №1 здійснюється в результаті додавання/віднімання, множення/ділення, то, очевидно, поле не розширюється, а якщо в результаті взяття кореня l_1 ступеня, такого, що цей результат дає число $\sqrt[l_1]{q_1}$, яке не міститься в $\mathbb{Q}$, то одержуємо розширення $\mathbb{Q}\big(\sqrt[l_1]{q_1}\big)$. Аналогічно розширюємо поле $\mathbb{Q}\big(\sqrt[l_2]{q_2}\big)$, якщо в результаті операції взяття кореня l_2 ступеня, такого, що цей результат дає число $\sqrt[l_2]{q_2}$, яке

не містить поле $\mathbb{Q}(\sqrt[l_1]{q_1})$, то одержуємо розширення $\mathbb{Q}(\sqrt[l_1]{q_1})(\sqrt[l_2]{q_2})$. Якщо враховувати тільки ті операції, які розширюють попередні поля, то в результаті ми одержимо поле $\mathbb{Q}(\sqrt[l_1]{q_1})(\sqrt[l_2]{q_2})\dots(\sqrt[l_m]{q_m})$. Послідовність таких розширень будемо називати вежею раціональних розширень.

Як показано в прикладі лекції 17 група автоморфізмів розширення $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ – не є групою Галуа. Тому замість розширень $\mathbb{Q}(\sqrt[l]{q})$ будемо розглядати розширення $\mathbb{Q}(x^l - q)$, яке включає всі комплексні корені із q та степені цих коренів до $l-1$ включно. Неважко переконатись, що розширення $\mathbb{Q}(x^{l_1} - q_1)\dots(x^{l_{i+1}} - q_{i+1})/\mathbb{Q}$ є розширенням Галуа.

Теорія Галуа стверджує, що починаючи з п'ятого ступеня існують многочлени, корені яких не належать вежі раціональних розширень.

Розглянемо многочлен

$$p(x) = x^5 - 4x - 2.$$

За допомогою критерія Ейзенштейна легко переконатись, що $p(x)$ незвідний над полем раціональних чисел. Многочлен $p'(x) = 5x^4 - 4$ має два дійсні корені $\pm\sqrt[4]{\frac{5}{4}}$, причому в точці $-\sqrt[4]{\frac{5}{4}}$ графік $p(x)$ має локальний максимум, а в $\sqrt[4]{\frac{5}{4}}$ – локальний мінімум. Оскільки $p(x) \to -\infty$ при $x \to -\infty$, $p(-1) = 1$, $p(1) = -5$ та $p(x) \to +\infty$ при $x \to +\infty$, то легко бачити, що $p(x)$ має три різні дійсні корені, які позначимо x_1, x_2, x_3 та два комплексно спряжені корені x_4, x_5.

Розглянемо розширення $\mathbb{Q}(x_1, x_2, x_3, x_4, x_5)$ поля $\mathbb{Q}$ коренями рівняння $p(x) = 0$. Опишемо всі автоморфізми групи $\mathrm{Aut}(\mathbb{Q}(x_1, x_2, x_3, x_4, x_5)/\mathbb{Q})$.

По-перше, одним із таких автоморфізмів є комплексне спряження площини, яке переставляє x_4 та x_5, тобто підстановка $(45) \in \mathrm{Aut}(\mathbb{Q}(x_1, x_2, x_3, x_4, x_5)/\mathbb{Q})$.

Покажемо, що кількість атоморфізмів $\mathrm{Aut}(\mathbb{Q}(x_1, x_2, x_3, x_4, x_5)/\mathbb{Q})$ збігається з кількістю групи підстановок S_5, тобто дорівнює $|S_5| = 5! = 120$.

Із незвідності многочлена $x^5 - 4x - 2$ над $\mathbb{Q}$ випливає, що прості алгебраїчні розширення $\mathbb{Q}(x_1)$, $\mathbb{Q}(x_2)$, $\mathbb{Q}(x_3)$, $\mathbb{Q}(x_4)$, $\mathbb{Q}(x_5)$ ізоморфні між собою.

Дійсно, $\mathbb{Q}(x_1)$ – це всі вирази $q_0 + q_1x_1 + q_2x_1^2 + q_3x_1^3 + q_4x_1^4$, $q_k \in \mathbb{Q}$ (Див. доведення теореми 15.1). Заміною x_1 на x_2 у цих виразах одержимо $\mathbb{Q}(x_2)$ і так далі.

Далі, для спрощення викладок корінь x_k ототожнюємо з його номером k.

Означення 18.1. *Класом елемента* $k \in \{1,2,3,4,5\}$ *називається множина елементів* $i \in \{1,2,3,4,5\}$ *таких, що* $(ki) \in \mathrm{Aut}(\mathbb{Q}(x_1, x_2, x_3, x_4, x_5)/\mathbb{Q})$.

Клас елемента 4 містить 5, оскільки $(45) \in \mathrm{Aut}(\mathbb{Q}(x_1, x_2, x_3, x_4, x_5)/\mathbb{Q})$. Дійсно, у цьому випадку автоморфізмом є комплексне спряження.

Твердження 18.2. *Відношення* (ki) *елементів* k, i *є відношенням еквівалентності.*

Доведення. Для цього досить показати транзитивність, оскільки рефлексивність і симетричність очевидні. Спочатку розглянемо частинний випадок – якщо справедливе відношення (15), то має місце (14) оскільки виконується крім (45). Дійсно,

$$(45)(51)(45) = (14).$$

Загальний випадок: нехай виконується (ki) та (ij), тоді має місце (jk):

$$(ji)(ik)(ji) = (jk).$$

Тобто транзитивність виконується і, отже, відношення еквівалентності (ki) розбиває множину $\{1,2,3,4,5\}$ на класи еквівалентності.

Покажемо, що всі класи мають однакову кількість елементів і, з урахуванням того, що ця кількість елементів має ділити 5, маємо, що це один клас.

Візьмемо елементи 1 та 4. Розглянемо підстановку $\varphi_{1\to4}$, яка переводить 1 в 4, а інші елементи якось переставляє, і нехай підстановка $\varphi_{4\to1}$ – обернена до $\varphi_{1\to4}$. Покажемо, що підстановка $\varphi_{4\to1}(45)\varphi_{1\to4} = (1i)$, де i це елемент у який

переходить 5 при підстановці $\varphi_{4\to1}$. Очевидно, що при $\varphi_{4\to1}(45)\varphi_{1\to4}$ елемент 1 переходить в i. Оскільки $\varphi_{1\to4}$ обернена до $\varphi_{4\to1}$, то вона переводить i у 5, отже, легко бачити, що i переходить в 5, а 5 при перестановці (45) переходить із i в 4. Інші елементи при $\varphi_{4\to1}(45)\varphi_{1\to4}$ залишаються на місці, оскільки 2 і 3 при обернених підстановках $\varphi_{1\to4}$ та $\varphi_{4\to1}$ залишаються на місці. Залишається 5 якому залишається перейти тільки в себе (більше немає куди). Якщо в класі $\{45\}$ є ще якийсь елемент l, тобто маємо клас $\{45l\}$, то аналогічно показується, що і в класі $\{1i\}$ є ще якийсь елемент j. Аналогічно для інших класів, отже, всі класи рівні між собою і це є один клас $\{1,2,3,4,5\}$.

Оскільки будь-яка підстановка зображується у вигляді добутку транспозицій, то $\mathrm{Aut}(\mathbb{Q}(x_1,x_2,x_3,x_4,x_5)/\mathbb{Q})$ складається з усіх підстановок групи S_5, тобто містить 120 автоморфізмів.

Позначимо через A_5 підмножину парних підстановок S_5.

Вправа 18.1. Переконатись, що A_5 з операцією композиції є групою.

Твердження 18.3. *A_5 – нормальна підгрупа групи S_5.*

Доведення. Неважко переконатись, що для будь-якої підстановки $\varphi \in S_5$ парність φ та φ^{-1} одна і та ж. Тому, якщо $\psi \in A_5$, тобто ψ – парна, то підстановка $\varphi^{-1}\circ\psi\circ\varphi$ також парна, отже, $\varphi^{-1}\circ\psi\circ\varphi \in A_5$.

Твердження 18.4. *Не існує жодної нормальної підгрупи A_5, тобто A_5 – проста.*

Доведення. В групі S_5 існують цикли довжини 2, їх умовно позначимо (ab), довжини 3 – (abc), довжини 4 – $(abcd)$, довжини 5 – $(abcde)$ і комбінації циклів: $(ab)\circ(cd)$ та $(abc)\circ(de)$. Із них парні, тобто належать A_5, такі: (abc), $(abcde)$, $(ab)\circ(cd)$. Цикли $(abcde)$ та $(abced)$ не переводяться один в інший в групі A_5, оскільки переводяться транспозицією.

Кількість циклів (abc) дорівнює $2\mathrm{C}_5^3 = 20$. Кількість довжини 5 дорівнює $4! = 24$ із них 12 виду $(abcde)$ та 12 виду $(abced)$. Нарешті, кількість композицій виду $(ab)\circ(cd)$ дорівнює $\frac{5}{2}\mathrm{C}_4^2 = 15$.

Нормальна підгрупа або містить один із таких циклів цілком, або не містить жодного. Отже,

$$60 = 20c_1 + 15c_2 + 12c_3 + 12c_4,$$

де $c_i \in \{0,1\}$.

Безпосереднім перебором легко переконатись, що таких c_i, $i = 1,2,3,4$ не існує.

Література

1. Бондаренко Є. В. Теорія кілець. К.: ВПЦ “Київський університет”, 2012.
2. Гаврилків В. М. Елементи теорії груп та теорії кілець: навчальний посібник. Івано-Франківськ: Голіней, 2016. 148 с.
3. Пилипів В. М., Заторський Р. А., Ліщинський І. І. Кільце поліномів: навчально-методичний посібник. Івано-Франківськ: Плай, 2014. 100 с.
4. Дрозд Ю. А. Теорія Галуа: навчальний посібник для студентів механіко-математичного факультету. Київ: Київський університет, 1997. 31 с.