

Групи є одним з основних і історично перших типів алгебраїчних структур. Теорія груп вивчає загальні властивості операцій, що найчастіше зустрічаються в математиці (зокрема, таких як додавання чисел та векторів, множення біективних відображень множини та ін.). Поняття групи з'явилось в математиці при вивченні підстановок (тобто біективних відображень скінченної множини в себе) у зв'язку з проблемою розв'язання алгебраїчних рівнянь в радикалах. У роботах Н.-Х. Абеля (1824) та Е. Галуа (1830) були виявлені глибокі зв'язки між властивостями групи підстановок та властивостями алгебраїчних рівнянь.

У 1870 р. з'явилася книга К. Жордана “Трактат про підстановки”, де був підведенний підсумок попередніх досліджень групи підстановок. В цей же час К. Жордан один з перших почав вивчати і нескінченні групи.

Ще одним джерелом виникнення поняття групи є геометрія. У середині XIX ст. поряд з евклідовою геометрією з'явилось багато інших геометрій: геометрія Лобачевського, проективна геометрія та інші. Виникла потреба вивчення різних геометрій та зв'язків між ними з єдиної точки зору. Ця єдина точка зору була сформульована Ф. Клейном у його “Ерлангенській програмі” у 1872 р., де було запропоновано розглядати геометрію як науку про ті властивості елементів простору, що залишаються незмінними при дії певної групи перетворень (тобто біективних відображень) простору в себе. Так, зокрема, евклідову геометрію можна трактувати як науку про інварінти групи ортогональних перетворень (див. ч.ІІ).

Нарешті, велика роль у виникненні та розвитку теорії груп належить теорії чисел. Зокрема, досить згадати, що класи лишків за $\text{mod } n$ утворюють групу відносно операції додавання і це було одним із перших прикладів загального поняття, яке тепер називають факторгрупою.

З початку XIX ст. теорія груп стає самостійною математичною дисципліною, яка вивчає довільні множини з алгебраїчною операцією, що задовільняє аксіоми групи. Основною задачею теорії груп є опис (класифікація) з точністю до ізоморфізму всіх можливих груп.

1 Групи та їх ізоморфізми

1.1 Огляд деяких теоретико-групових понять та прикладів груп

Нагадаємо, що *групою* називають множину G з асоціативною алгебраїчною операцією, якщо для цієї операції існує нейтральний елемент e і для кожного елемента $g \in G$ існує обернений g^{-1} . Якщо групова операція на

множині G комутативна, то G називають *абельовою* (*комутативною*) групою.

Відображення $f: G_1 \rightarrow G_2$ називають *гомоморфізмом* груп G_1 і G_2 , якщо $f(ab) = f(a)f(b)$ для довільних $a, b \in G_1$. Біективний гомоморфізм називається *ізоморфізмом*.

Підмножина H групи G є *підгрупою*, якщо H сама є групою відносно тієї ж операції, що і G . Важливими підгрупами будь-якої групи G є її циклічні підгрупи. *Циклічна підгрупа* (g) групи G , породжена елементом $g \in G$, — це підгрупа, що складається з усіх цілих степенів елемента g : $(g) = \{g^n \mid n \in \mathbb{Z}\}$. Група є циклічною, якщо вона збігається з однією зі своїх циклічних підгруп.

Ми знаємо, що кожна нескінчена циклічна група ізоморфна групі \mathbb{Z} цілих чисел, кожна скінчена циклічна група ізоморфна групі \mathbb{C}_n — коренів n -го степеня з 1.

Підгрупу H групи G називають *нормальнюю* і пишуть $H \triangleleft G$, якщо ліві суміжні класи за підгрупою H збігаються з правими, тобто для кожного $g \in G$ вірна рівність $gH = Hg$.

Очевидно, кожна підгрупа абелевої групи G є її нормальнюю підгрупою. Якщо G неабельова група, то в ній можуть існувати як нормальні так і підгрупи, які не є такими.

Якщо H нормальна підгрупа групи G , то на множині суміжних класів G/H можна ввести алгебраїчну операцію $g_1H \cdot g_2H = g_1g_2H$, відносно якої G/H виявляється групою. Це *факторгрупа* групи G за підгрупою H .

Відображення $f: G \rightarrow G/H$, для якого $f(g) = gH$ є гомоморфізмом груп, називають *канонічним гомоморфізмом*.

Нехай $f: G_1 \rightarrow G_2$ — гомоморфізм груп. Тоді його образ $\text{Im}f = \{b \in G_2 \mid \exists a \in G_1 \quad f(a) = b\}$ є підгрупою групи G_2 , ядро $\text{Ker}f = \{a \in G_1 \mid f(a) = e\}$ (тут e — нейтральний елемент групи G_2) є нормальнюю підгрупою групи G_1 . З іншого боку, кожна нормальнна підгрупа H групи G є ядром канонічного гомоморфізму $G \rightarrow G/H$. Тому нормальні підгрупи можна характеризувати, як ядра гомоморфізмів груп.

Групи поділяють на скінченні та нескінченні, абелеві та не абелеві. Важливим класом груп є скінченно породжені абелеві групи. Структура скінченно породжених абелевих груп була описана раніше (див. част. II, Розд. ?, теор. ?).

Важливе значення має вивчення класів груп, що мають деяку додаткову структуру, узгоджену з груповою операцією, наприклад, топологічна група — це група, на якій задана топологія, відносно якої групова операція неперервна, алгебраїчна група — це група, множина якої складається з точок афінного або проективного простору, що задовольняють деякій

системі алгебраїчних рівнянь, групова операція задається за допомогою раціональних функцій або многочленів.

Завершимо цей п. оглядом деяких прикладів груп.

1). Множини $n\mathbb{Z}$, \mathbb{Z} , \mathbb{Q} , \mathbb{R} , \mathbb{C} — це нескінчені абелеві групи відносно звичайної операції додавання чисел.

2) Множини $\mathbb{Q} \setminus \{0\}$, $\mathbb{R} \setminus \{0\}$, $\mathbb{C} \setminus \{0\}$ ненульових раціональних, дійсних і комплексних чисел є комутативними групами відносно звичайного множення. Ці групи позначають \mathbb{Q}^* , \mathbb{R}^* , \mathbb{C}^* відповідно.

3) Для числової множини $A \subset \mathbb{R}$ нехай $A_{>0}$ означає множину додатних елементів в A . Якщо A — яка-небудь підгрупа групи \mathbb{R}^* , то $A_{>0}$ теж підгруп групи \mathbb{R}^* .

4) $\mathbb{C}_n = \{z \in \mathbb{C} \mid z^n = 1\}$, $\bigcup_{n \in \mathbb{N}} \mathbb{C}_n$, $\mathcal{U} = \{z \in \mathbb{C} \mid |z| = 1\}$ — групи відносно множення комплексних чисел.

5) Множина S_n підстановок n елементів і, більш загально, множина $\text{Aut } A$ всіх біективних відображень множини A в себе є групами відносно множення відображень. Ці групи некомутативні, якщо множина A має більше, ніж 2 елементи.

6) Множина $\text{GL}_n(P)$ — невироджених матриць n -го порядку з елементами з поля P , множина $O_n(\mathbb{R})$ — ортогональних матриць, $U_n(\mathbb{C})$ — унітарних матриць, $\text{SL}_n(P) = \{A \in \text{GL}_n(P) \mid \det A = 1\}$ є групами відносно множення матриць. Групи $\text{GL}_n(P)$ та $\text{SL}_n(P)$ називають, відповідно, *повною лінійною групою* та *спеціальною лінійною групою* над полем P .

7) У прикладах 1), 2), 4) кожна з груп, у наведених там ланцюжках є підгрупою кожної наступної групи. У прикладі 6 група $\text{SL}_n(P)$ є нормальнюю підгрупою групи $\text{GL}_n(P)$, Оскільки вона є ядром гомоморфізму $f: \text{GL}_n(P) \rightarrow P$, де $f(A) = \det A$.

1.2 Теорема Келі

Ми знаємо (див. приклад 5 п. 1.1), що множина $\text{Aut } A$ всіх біективних відображень множини A в себе є групою відносно операції добутку відображень. Виявляється, що підгрупами цих груп $\text{Aut } A$ вичерпуються всі групи.

Теорема 1. *Нехай G — будь-яка група. Тоді G ізоморфна деякій підгрупі групи $\text{Aut } G$.*

Доведення. Розглянемо відображення $F: G \rightarrow \text{Aut } G$, для якого $F(g)(x) = gx$ для кожного $x \in G$. Відображення F означене коректно, тобто $F(g)$

є біективним відображенням множини G , бо для нього існує обернене відображення $(F(g))^{-1} = f(g^{-1})$. Справді,

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

Отже, $F(g^{-1})F(g) = 1_G$. Так само показуємо, що $F(g)F(g^{-1}) = 1_G$.

Відображення F — ін'єктивне, бо коли $g_1 \neq g_2$, то й $F(g_1) \neq F(g_2)$ тому, що $F(g_1)(e) = g_1$, $F(g_2)(x) = g_2$ (e — нейтральний елемент групи G). Перевіримо, що F — гомоморфізм груп. Маємо, $F(g_1g_2)(x) = (g_1g_2)x = g_1(g_2x) = F(g_1)(F(g_2)(x)) = F(g_1)F(g_2)(x)$. Отже, $F(g_1g_2) = F(g_1)F(g_2)$.

Звідси випливає, що F є біективним гомоморфізмом групи G на підгрупу $\text{Im } F$ групи $\text{Aut } G$ (пригадаємо, що образ гомоморфізму є підгрупою). \square

Наслідок 2. *Кожна скінчена група з n елементами ізоморфна підгрупі групи S_n .*

Для позначення, що групи G_1 і G_2 ізоморфні, пишемо $G_1 \simeq G_2$.

1.3 Прямий добуток груп

Нехай G_1 і G_2 — дві групи. Розглянемо декартовий добуток $G_1 \times G_2 = \{(g_1, g_2) \mid g_1 \in G_1, g_2 \in G_2\}$. Введемо на множині $G_1 \times G_2$ алгебраїчну операцію покомпонентного множення: $(g_1, g_2)(g'_1, g'_2) = (g_1g'_1, g_2g'_2)$, де $g_i g'_i$ — добуток елементів групи G_i , $i = 1, 2$. Легко пересвідчитися в тому, що відносно цієї операції $G_1 \times G_2$ є групою. Пропонуємо зробити це самостійно. Цю групу називають *зовнішнім прямим добутком* груп G_1 і G_2 .

Виділимо в групі $G_1 \times G_2$ дві підмножини: $A = \{(a, e_2) \mid a \in G_1\}$ та $B = \{(e_1, b) \mid b \in G_2\}$, де e_1, e_2 — відповідно, нейтральні елементи груп G_1 та G_2 .

Твердження 3. а) A і B є нормальними підгрупами групи $G = G_1 \times G_2$;
б) $A \cap B = \{e_1, e_2\}$ — нейтральний елемент групи G ;
в) $\forall a \in A \forall b \in B \quad ab = ba$.

Доведення. а) Нехай $(a, e_1), (a', e_2) \in A$. $(a, e_2)(a', e_2) = (aa', e_2) \in A$ і $(a, e_2)^{-1} = (a^{-1}, e_2) \in A$. Тому A — підгрупа групи G . Так само перевіряємо, що і B підгрупа.

Розглянемо довільні елементи $(g_1, g_2) \in G$, $(a, e_2) \in A$. Тоді

$$(g_1, g_2)(a, e_2)(g_1, g_2)^{-1} = (g_1ag_1^{-1}, e_2) \in A.$$

Це означає, що $(g_1, g_2)A(g_1, g_2)^{-1} \subset A$ бо $(g_1, g_2)A \subset A(g_1, g_2)$. Аналогічно: $(g_1, g_2)A \supset A(g_1, g_2)$. Тому $A \triangleleft G$ і, аналогічно, $B \triangleleft G$.

в) Нехай $a = (g_1, e_2)$, $b = (e_1, g_2)$. Тоді $ab = (g_1, g_2) = ba$. \square

За допомогою операції прямого добутку груп з даних груп можна будувати нові групи. Але більш важливою є обернена задача: у даній групі G знайти такі підгрупи A і B , щоб група G була ізоморфна (зовнішньому) прямому добутку груп, ізоморфних групам A і B . У цьому випадку вивчення групи G зводиться до вивчення, як правило, більш простих груп A і B . Зауважимо, що у випадку абелевих груп прямі добутки скінченного числа груп називають *прямими сумами*. Вже було доведено, що кожна скінченно породжена абелева група ізоморфна прямій сумі цикліческих груп.

Означення 4. Група G є внутрішнім прямим добутком двох своїх підгруп A і B , якщо ці підгрупи мають такі властивості:

- 1) $AB = \{ab \mid a \in A, b \in B\} = G$;
- 2) $A \triangleleft G$ і $B \triangleleft G$;
- 3) $A \cap B = \{e\}$ — нейтральний елемент групи G .

Приклади.

1) Розглянемо в цикліческій групі $\mathbb{Z}/6\mathbb{Z}$ підгрупи $A = \{\bar{0}, \bar{3}\}$ і $B = \{\bar{0}, \bar{2}, \bar{4}\}$. Оскільки $\bar{3} + \bar{4} = \bar{1}$, то $A + B = \mathbb{Z}/6\mathbb{Z}$. Крім цього, $A \cap B = \{\bar{0}\}$, друга умова з попереднього означення виконується автоматично. Отже, $\mathbb{Z}/6\mathbb{Z}$ є (внутрішньою) прямою сумою підгруп A і B .

2) Група $\mathbb{Z}/8\mathbb{Z}$ не розкладається в пряму суму своїх нетривіальних підгруп. Справді, всі її нетривіальні підгрупи такі: $\{\bar{0}, \bar{2}, \bar{4}, \bar{6}\}$ і $\{\bar{0}, \bar{4}\}$. Вони мають перетин $\{\bar{0}, \bar{4}\} \neq \{\bar{0}\}$.

3) Група \mathbb{C}^* розкладається у прямий добуток своїх підгруп $\mathbb{R}_{>0}$ і $\mathcal{U} = \{z \in \mathbb{C} \mid |z| = 1\}$.

4) Група S_3 не розкладається в прямий добуток нетривіальних підгруп, бо єдиною нормальнюю підгрупою в S_3 є група A_3 , що складається з парних підстановок.

Наступне твердження показує, що з точністю до ізоморфізму поняття внутрішнього і зовнішнього прямого добутку збігаються.

Теорема 5. Якщо група G розкладається у внутрішній прямий добуток своїх підгруп A і B , то:

- a) для кожного $a \in A$ і кожного $b \in B$ $ab = ba$;
- б) G ізоморфна зовнішньому прямому добутку $A \times B$.

Доведення. а) Розглянемо елемент $aba^{-1}b^{-1} \in G$. З умови $B \triangleleft G$ маємо $(aba^{-1})b^{-1} \in B$, а з умови $A \triangleleft G$ випливає $a(ba^{-1}b^{-1}) \in A$. Отже, $aba^{-1}b^{-1} \in A \cap B = \{e\}$. Тому $aba^{-1}b^{-1} = e$ і $ab = ba$.

б) Розглянемо відображення $\varphi: A \times B \rightarrow G$, де $\varphi(a, b) = ab$. Перш за все, з умови 1 означення внутрішнього прямого добутку випливає, що φ сюр'єктивне відображення. Перевіряємо, що воно ін'єктивне: якщо $ab = a_1b_1$, де $a, a_1 \in A$ і $b, b_1 \in B$, то $a_1^{-1}a = b_1b^{-1} \in A \cap B$. Тому $a_1^{-1}a = b_1b^{-1} = e$ і $a = a_1$, $b = b_1$. Залишається переконатися, що φ гомоморфізм. Маємо

$$\begin{aligned}\varphi((a_1, b_1)(a_2, b_2)) &= \varphi(a_1a_2, b_1b_2) = a_1a_2b_1b_2 = \\ &= a_1b_1a_2b_2 = \varphi((a_1, b_1))\varphi((a_2, b_2));\end{aligned}$$

тут третя рівність випливає з твердження а). \square

Поняття прямого добутку можна узагальнити на випадок родини груп $\{G_i\}_{i \in I}$.

Означення 6. Прямим добутком родини груп G_i називають декартовий добуток $\prod_{i \in I} G_i$ множин G_i , тобто множину всіх відображень $f: I \rightarrow \bigcup_{i \in I} G_i$ таких, що $f(i) \in G_i$ для кожного $i \in I$ разом з операцією “покомпонентного множення”

$$(f \circ g)(i) = f(i)g(i).$$

Пропонуємо читачеві самостійно переконатися в тому, що прямий добуток довільної родини груп є групою.

1.4 Прямі добутки та короткі точні послідовності гомоморфізмів

Більша частина цього п. присвячена прямим добуткам абелевих груп. Прямий добуток скінченної множини абелевих груп називають *прямою сумою* і позначають $\bigoplus_{i=1}^n A_i$, бо $A \oplus B$ у випадку двох груп.

Означення 7. Короткою точникою послідовністю груп називається пара гомоморфізмів груп $f: A \rightarrow G$, $g: G \rightarrow B$ з властивостями $\text{Ker } f = 0$, $\text{Im } f = \text{Ker } g$, $\text{Im } g = B$.

Коротку точну послідовність прийнято записувати у вигляді

$$0 \longrightarrow A \longrightarrow G \longrightarrow B \longrightarrow 0. \quad (1.4.1)$$

Приклади.

Розглянемо будь-який гомоморфізм груп $f: G \rightarrow G'$, Якщо $A = \text{Kerg}$, $B = \text{Img}$, то одержуємо коротку точну послідовність

$$0 \longrightarrow A \xrightarrow{i} G \xrightarrow{f} B \longrightarrow 0, \quad (1.4.2)$$

де i — вкладення, тобто $i(a) = a$ для кожного $a \in A$.

Наведемо декілька конкретних прикладів послідовностей такого вигляду.

а) Нехай $G = \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ і $g: \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \rightarrow \mathbb{Z}/2\mathbb{Z}$ — гомоморфізм, для якого $g((\bar{a}, \bar{b})) = \bar{b}$. Ядро цього гомоморфізму є підгрупою $\{(\bar{0}, \bar{0}), (\bar{1}, \bar{0})\}$, ізоморфною $\mathbb{Z}/2\mathbb{Z}$, і ми одержуємо коротку точну послідовність

$$0 \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow 0. \quad (1.4.3)$$

б) Нехай $G = \mathbb{Z}/4\mathbb{Z}$ і $g: \mathbb{Z}/4\mathbb{Z} \rightarrow \mathbb{Z}/4\mathbb{Z}$ — гомоморфізм, для якого $g(\bar{a}) = 2\bar{a}$. Тоді $\text{Img} \simeq \mathbb{Z}/2\mathbb{Z}$, $\text{Kerg} \simeq \{\bar{0}, \bar{2}\} \simeq \mathbb{Z}/2\mathbb{Z}$, і ми одержуємо точну послідовність

$$0 \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow \mathbb{Z}/4\mathbb{Z} \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow 0. \quad (1.4.4)$$

в) Нехай $G = S_3$ — група підстановок на множині з трьох елементів. Розглянемо гомоморфізм $g: S_3 \rightarrow \mathbb{Z}/2\mathbb{Z}$, що ставить у відповідність $\bar{0}$ парним підстановкам і $\bar{1}$ непарним. Тут $\text{Kerg} = A_3 \simeq \mathbb{Z}/3\mathbb{Z}$ і точна послідовність (1.4.1) у цьому випадку має вигляд

$$0 \longrightarrow \mathbb{Z}/3\mathbb{Z} \longrightarrow S_3 \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow 0. \quad (1.4.5)$$

Проаналізуємо докладніше коротку точну послідовність (1.4.5). $S_3 = \{e, a, a^2, b, ab, a^2b\}$, де a — тричленний цикл, b — як-небудь транспозиція. Тоді, враховуючи ізоморфізми $A = A_3 \approx \mathbb{Z}/3\mathbb{Z}$ і $B = \{e, b\} \approx \mathbb{Z}/2\mathbb{Z}$, точна послідовність (1.4.5) має вигляд

$$0 \longrightarrow A \longrightarrow S_3 \longrightarrow B \longrightarrow 0. \quad (1.4.6)$$

Ясно, що тут $AB = \{xy \mid x \in A, y \in B\} = S_3$, A — нормальна підгрупа в S_3 і $A \cap B = \{e\}$, тобто S_3 є “майже прямим добутком” груп A і B . S_3 не є прямим добутком A і B , бо не вистачає однієї умови, саме, B не є нормальнюю підгрупою в S_3 .

Означення 8. Група G називається *напівпрямим добутком* групи A на групу B , якщо

- 1) $G = AB = \{xy \mid x \in A, y \in B\}$;
- 2) A — нормальна підгрупа групи G ;
- 3) $A \cap B = \{e\}$ — нейтральний елемент групи G .

Напівпрямий добуток групи A на групу B позначають $A \times B$.

Отже, аналіз груп, що входять у точну послідовність (1.4.6), показує, що S_3 напівпрямий добуток своїх підгруп A і B . Зрозуміло, що прямий добуток груп є частковим випадком напівпрямого добутку. Ці поняття різні, бо, наприклад, прямий добуток циклічної групи третього порядку на циклічну групу другого порядку є циклічною групою шостого порядку.

Зауваження 9. Якщо група G є середнім членом точної послідовності (1.4.1), то кажуть, що група G є розширенням групи A з допомогою групи B . Вивчення розширень груп має важливе значення як для теорії груп, так і для її застосувань. Теорія розширень груп була одним з джерел виникнення одного з дуже важливих для сучасної математики розділів алгебри — гомологічної алгебри.

Точні послідовності (1.4.3) і (1.4.5) показують, що розширення груп можуть виникати з прямих або напівпрямих добутків груп (такі розширення називають *розділеннями*). Але, як показує точна послідовність (1.4.4), розширення не зобов'язане бути прямим (півпрямим) добутком: група $\mathbb{Z}/4\mathbb{Z}$ не розкладається в нетривіальний прямий добуток.

Зауважимо, що у випадку абелевої групи G поняття півпрямого добутку збігається з поняттям прямої суми.

Вияснимо, за яких умов група G ізоморфна напівпрямому добутку $A \times B$ групи A на групу B . Для цього введемо ще одне означення.

Означення 10. Кажуть, що коротка точна послідовність груп

$$0 \longrightarrow A \xrightarrow{i} G \xrightarrow{\pi} B \longrightarrow 0 \tag{1.4.7}$$

розділюється, якщо існує гомоморфізм $j: B \rightarrow G$ такий, що $\pi \circ j = 1_B$.

Далі ін'єктивні гомоморфізми ми називатимемо *мономорфізмами*, сюр'єктивні — *епіморфізмами*.

Теорема 11. Група G ізоморфна напівпрямому добутку $A \times B$ тоді й лише тоді, коли існує коротка точна послідовність груп (1.4.7), що розщеплюється.

Доведення. \Rightarrow . Нехай $G \simeq A \times B = AB$. Розглянемо відображення $i: A \rightarrow AB$, $i(a) = a$ та $\pi: AB \rightarrow B$, $\pi(ab) = b$, де $a \in A$, $b \in B$. Відображення i , очевидно, є мономорфізмом.

Перевіримо, що π — епіморфізм. Оскільки $A \triangleleft G = AB$, то для $a_1, a_2 \in A$, $b_1, b_2 \in B$ маємо $a_1 b_1 a_2 b_2 = a_1 b_1 a_2 b_1^{-1} b_1 b_2 = a_3 b_1 b_2$, де $a_3 \in A$. Тому $\pi((a_1 b_1)(a_2 b_2)) = \pi(a_3(b_1 b_2)) = b_1 b_2 = \pi(a_1 b_1)\pi(a_2 b_2)$ і, отже, π — гомоморфізм. Очевидно, що π є епіморфізмом.

Приймемо для $b \in B$ $j(b) = b = eb$. Ясно, що j гомоморфізм і $\pi \circ j = 1_B$.

\Leftarrow . Навпаки, нехай існує коротка точна послідовність вигляду (1.4.7), що розщеплюється. Оскільки, $\pi \circ j = 1_B$, то j мономорфізм і його образ B' є підгрупою групи G , $B' \simeq B$. Так само мономорфізм i відображає ізоморфно групу A на підгрупу A' групи G . Нехай $g \in G$ довільний елемент групи G . Знайдеться елемент $b \in B$, для якого $\pi(g) = b = (\pi \circ j)(b) = \pi(j(b)) = \pi(b')$, де $b' \in B'$. Звідси $\pi(b')\pi(g)^{-1} = \pi(b'g^{-1}) = e$, отже, $b'g^{-1} \in \text{Ker } \pi$. Але $\text{Ker } \pi = \text{Im } i$, тому існує $a' \in A'$, що $b'g^{-1} = a'$. Звідси $g = (a')^{-1}b' \in A'B'$, і ми бачимо, що $G = A'B'$. Далі, $A' \triangleleft G$, бо $A' = \text{Ker } \pi$. Залишається довести, що $A' \cap B' = \{e\}$. Нехай $x' \in A' \cap B'$. Тоді $\pi(x') = e$, бо $x' \in A'$ і $\pi(x') = (\pi \circ j)(x) = x$, де x прообраз елемента x' відносно гомоморфізму j . Отже, $x = e$, Оскільки j мономорфізм, то $\bar{x}' = e$. \square

Означення 12. Скажемо, що точна послідовність (1.4.7) *розщеплюється зліва*, якщо існує гомоморфізм $\rho: G \rightarrow A$ такий, що $\rho i = 1_A$.

Теорема 13. Група G ізоморфна прямому добутку груп A і B тоді і тільки тоді, коли існує коротка точна послідовність груп (1.4.7), що розщеплюється зліва.

Доведення. \Rightarrow . За теоремою (5) можна вважати, що $G = A \times B$. Розглянемо відображення $\rho: A \times B \rightarrow A$, де $\rho((a, b)) = a$. Очевидно, ρ епіморфізм. Крім цього, розглянемо гомоморфізми $i: A \rightarrow A \times B$, $i(a) = (a, e)$ та $\pi: A \times B \rightarrow B$, $\pi((a, b)) = b$. Ясно, що $\rho \circ i = 1_A$ і послідовність

$$0 \longrightarrow A \xrightarrow{i} A \times B \xrightarrow{\pi} B \longrightarrow 0$$

точна.

\Leftarrow . Припустимо, що існує точна послідовність вигляду (1.4.7), яка розщеплюється зліва, тобто маємо точну послідовність груп

$$0 \longrightarrow A \xrightarrow{i} G \xrightarrow{\pi} B \longrightarrow 0, \quad G \xrightarrow{\rho} A$$

разом з гомоморфізмом ρ , для якого $\rho \circ i = 1_A$.

Позначимо $A' = \text{Im}i$, $B' = \text{Ker}\rho$. Нехай $g \in G$, $a = \rho(g) \in A$. Тоді $\rho(g) = \rho(i(a))$, тобто $\rho(g^{-1}i(a)) = e$ і $g^{-1}i(a) = b' \in B'$. Звідси $g = i(a)(b')^{-1} \in A'B'$. A' і B' — це ядра гомоморфізмів π і ρ , тому $A' \triangleleft G$ і $B' \triangleleft G$. Доведемо, що $B' \simeq B$. Оскільки $G = A'B'$ і $A' = \text{Im}i = \text{Ker}\pi$, то π відображає сюр'ективно B' на B . Якщо для деякого $b' \in B'$ $\pi(b') = e$, то $b' = i(a)$ для деякого $a \in A$. Тому $\rho(b') = \rho(i(a)) = a = e$, тому і $b' = i(e) = e$. Звідси випливає, що π ізоморфізм групи B' на групу B . Нарешті, якщо $g \in A' \cap B'$, то існує $a \in A$, для якого $g = i(a)$ і $e = \rho(g) = \rho(i(a)) = a$. Тому $g = i(e) = e$, отже, $A' \cap B' = \{e\}$. \square

З попереднього випливає, що у випадку абелевої групи G маємо таку теорему.

Теорема 14. Для абелевої групи G наступні твердження еквівалентні:

- 1) G ізоморфна прямій сумі груп A і B ;
- 2) існує точна послідовність (1.4.7) абелевих груп, що розщеплюється зліва;
- 3) існує точна послідовність (1.4.7), що розщеплюється.

Доведення. Зауважимо, що коли абелева група G є напівпрямим добутком двох підгруп, то G автоматично є прямою сумою цих підгруп. Тому з теореми (11) випливає еквівалентність 1) \Leftrightarrow 3). Еквівалентність 1) \Leftrightarrow 2) випливає з теореми (13). \square

Зауваження 15. 1) Для неабелевих груп з твердження 3 теореми (14) не випливає твердження 2. Справді, якби це не було так, то послідовність (1.4.6), яка розщеплюється, розщеплювалася б зліва, тому некомутативна група S_3 була б прямим добутком двох абелевих груп, що приводить до суперечності.

2) Зрозуміло, що точна послідовність (1.4.4) не розщеплюється. Загальніше, будь-яка коротка точна послідовність, середнім членом якої є циклічна група порядку p^n , де p просте число, не розщеплюється.

2 Теореми про гомоморфізми груп

2.1 Гомоморфізми та підгрупи

Нехай $f: G_1 \rightarrow G_2$ — гомоморфізм груп. Ми вже знаємо, що $\text{Im}f$ є підгрупою групи G_2 , $\text{Ker}f$ — нормальні підгрупи групи G_1 . Ці факти є частковими випадками наступного твердження.

Твердження 16. гомоморфізми груп мають такі властивості:

- 1) образи $f(H)$ підгруп H групи G_1 є підгрупами групи G_2 ;
- 2) прообрази $f^{-1}(H')$ підгруп H' групи G_2 є підгрупами групи G_1 ;
- 3) прообрази нормальніх підгруп групи G_2 є нормальними підгрупами групи G_1 ;
- 4) якщо гомоморфізм $f: G_1 \rightarrow G_2$ сюр'єктивний, то образ $f(H)$ нормальної підгрупи H групи G_1 є нормальною підгрупою групи G_2 .

Доведення. 1) Ця властивість, по-суті, означає, що образ групи при гомоморфізмі є підгрупою, це ми вже доводили.

2) Якщо $a, b \in f^{-1}(H')$, то $f(ab) = f(a)f(b) \in H'$, отже, $ab \in f^{-1}(H')$. Крім цього, $f(a^{-1}) = f(a)^{-1} \in H'$, тобто $a^{-1} \in f^{-1}(H')$. За критерієм підгрупи це означає, що $f^{-1}(H')$ підгрупа.

3) Нехай $a \in f^{-1}(H')$, g — довільний елемент групи G_1 . Зауважимо, що $f(gag^{-1}) = f(g)f(a)f(g)^{-1} \in H'$, бо $H' \triangleleft G_2$. Тому $gag^{-1} \in f^{-1}(H')$, це означає, що $H \triangleleft G_1$.

4) Нехай $a' \in f(H)$, g' — довільний елемент групи G_2 . Існують $a \in H$, $g \in G_1$ такі, що $a' = f(a)$, $g' = f(g)$. Звідси $g'a'g'^{-1} = f(g)f(a)f(g)^{-1} = f(gag^{-1}) \in f(H)$, бо $gag^{-1} \in H$. Звідси випливає, що $f(H) \triangleleft G_2$. \square

Наслідок 17. Нехай H — нормальна підгрупа групи G , $f: G \rightarrow G/H$ — канонічний гомоморфізм. гомоморфізм f визначає біективну відповідність між підгрупами A групи G з властивістю $H \subset A$ та підгрупами фактор-групи G/H , причому нормальним підгрупам групи G відповідають нормальні підгрупи фактор-групи G/H і навпаки.

Доведення. Якщо A — підгрупа групи G , $A \supset H$, то $f(A)$ — підгрупа групи G/H з властивістю 1) з попереднього твердження.

Нехай A і B — різні підгрупи групи G , $A \subset H$, $B \subset H$. Припустимо, що $a \in A$, $a \notin B$. Якщо $f(a) \in f(B)$, то $f(a) = f(b)$ для деякого $b \in B$. Звідси $f(b^{-1}a) = e$, тобто $b^{-1}a \in H \subset B$ і $a \in B$. Одержано суперечність показує, що $f(A) \neq f(B)$, тобто різним підгрупам $A \subset G$ таким, що $H \subset A$ відповідають різні підгрупи в G/H . Очевидно, ця відповідність сюр'єктивна. Нарешті, з властивості 4) твердження маємо, що нормальним підгрупам групи G відповідають нормальні підгрупи групи G/H , і навпаки за властивістю 3). \square

Зauważення 18. Якщо гомоморфізм $f: G_1 \rightarrow G_2$ не сюр'єктивний, то образ нормальній підгрупи не обов'язково є нормальнюю підгрупою, наприклад:

$$G_1 = S_3, \quad G_2 = S_4, \quad f(\sigma) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ \sigma(1) & \sigma(2) & \sigma(3) & 4 \end{pmatrix}$$

для $\sigma \in S_3$. Тоді $A_3 \triangleleft S_3$, ле $f(A_3)$ не є нормальнюю підгрупою в S_4 . Наприклад,

$$(1, 4)(1, 2, 3)(1, 4) = (2, 3, 4) \notin f(S_3).$$

2.2 Основні теореми про гомоморфізми та їх застосування

Теорема 19. *Кожний гомоморфізм груп $f: G_1 \rightarrow G_2$ визначає ізоморфізм $\bar{f}: G_1/\text{Ker } f \simeq \text{Im } f$, $\bar{f}(\bar{a}) = f(a)$, де $\bar{a} = a\text{Ker } f$ — суміжний клас групи G_1 з представником a за нормальнюю підгрупою $\text{Ker } f$.*

Ми вже доводили цю теорему (див. част. I, Е). Вона суттєво використовується у доведенні інших теорем про гомоморфізми, тому її називають *основною*.

Наведені нижче приклади ілюструють, як основна теорема про гомоморфізми груп може бути використана для обчислення факторгруп.

Приклади.

1) Розглянемо гомоморфізм $f: \mathbb{C}^* \rightarrow \mathbb{R}_{>0}^*$ мультиплікативної групи комплексних чисел у мультиплікативну групу додатних дійсних чисел, такий що $f(z) = |z|$. Цей гомоморфізм сюр'ективний. Підгрупа $\mathcal{U} = \{z \in \mathbb{C}^* \mid |z| = 1\}$ є його ядром. Отже, $\mathbb{C}^*/\mathcal{U} \simeq \mathbb{R}_{>0}$.

2) Нехай P — поле і $\text{GL}_n(P)$ — повна лінійна група над полем P . Ядром гомоморфізму $f: \text{GL}_n(P) \rightarrow P^*$, де $f(A) = \det A$ є спеціальна лінійна група $\text{SL}_n(P)$. Звідси одержуємо, що $\text{GL}_n(P)/\text{SL}_n(P) \simeq P^*$.

3) Розглянемо множини $\text{T}_n(P) = \{[a_{ij}] \in \text{GL}_n(P) \mid a_{ij} = 0$ для $i > j\}$ — невироджених верхніх трикутних матриць з елементами поля P , $\text{UT}_n(P) = \{[a_{ij}] \in \text{T}_n(P) \mid a_{ij} = 1, 1 \leq i \leq n\}$ — верхніх трикутних матриць, всі діагональні елементи яких дорівнюють 1 та $\text{D}_n(P) = \{[a_{ij}] \in \text{GL}_n(P) \mid a_{ij} = 0$ для $i \neq j\}$ — діагональних матриць. Всі ці множини є групами відносно множення матриць. Відображення $f: \text{T}_n(P) \rightarrow \text{D}_n(P)$,

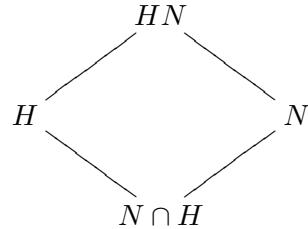
$$f \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ 0 & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & a_{nn} \end{pmatrix} = \begin{pmatrix} a_{11} & 0 & \dots & 0 \\ 0 & a_{22} & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & a_{nn} \end{pmatrix}$$

є гомоморфізмом груп і $\text{Ker } f = \text{UT}_n(P)$. Тому $\text{T}_n(P)/\text{UT}_n(P) \simeq \text{D}_n(P)$.

2.3 Дві теореми про ізоморфізми

Теорема 20. Нехай H — підгрупа групи G , N — нормальнна підгрупа групи G . Тоді $H \cap N$ — нормальнна підгрупа групи H і факторгрупа $H/H \cap N$ ізоморфна фактор-групі HN/N .

Доведення. Формулювання цієї теореми легко запам'ятати, якщо зобразити всі підгрупи, які беруть участь у її формулюванні, у вигляді “вершин паралелограма”:



Для доведення теореми розглянемо канонічний гомоморфізм $f: G \rightarrow G/N$. Розглянемо відображення f тільки на підгрупі H . Одержаніся гомоморфізм $f': H \rightarrow G/N$. Маємо $\text{Im}f' = \{hN \mid h \in H\} = HN/N$, $\text{Ker}f' = \{h \in H \mid hN = N\} = H \cap N$. З основної теореми про гомоморфізм одержуємо $H/\text{Ker}f' \simeq \text{Im}f'$, тобто $H/H \cap N \simeq HN/N$. \square

Теорема 21. Нехай M і N — нормальні підгрупи групи G і $M \subset N$.
Тоді

$$G/M/N/M \simeq G/N.$$

Доведення. Побудуємо відображення $f: G/M \rightarrow G/N$, де $f(gM) = gN$. Перш за все, зауважимо, що f — коректно означене відображення. Справді, якщо $g_1M = g_2M$, то $g_2^{-1}g_1 \in M \subset N$, тому $g_1N = g_2N$. Зовсім просто перевірити, що f — гомоморфізм: $f(g_1Mg_2M) = f(g_1g_2M) = g_1g_2N = g_1Ng_2N = f(g_1M)f(g_2M)$. Сюр'ективність гомоморфізму f очевидна з його означення. Знайдемо $\text{Ker}f$: $\text{Ker}f = \{gM \mid gN = N\} = \{gM \mid g \in N\} = N/M$. Звідси, застосовуючи основну теорему про гомоморфізм, одержуємо $G/M/\text{Ker}f = G/M/N/M \simeq G/N$, що й потрібно було довести. \square

Наведемо два прості приклади застосувань доведених теорем.

1) Нехай H — підгрупа групи S_n і нехай H містить хоч одну непарну підстановку. Тоді індекс підгрупи парних підстановок в групі H дорівнює 2. Справді, розглянемо групу A_n — підгрупу парних підстановок

в S_n . Тоді $HA_n = \{fa \mid h \in H, a \in A_n\}$ — підгрупа в групі S_n . Для того, щоб це перевірити, скористаємося тим, що $A_n \triangleleft S_n$. Для $h_1, h_2 \in H$, $a_1, a_2 \in A_n$ маємо $h_1 a_1 h_2 a_2 = h_1 h_2 a_3 a_2 \in HA_n$, де $a_3 \in A_n$ і $(h_1 a_1)^{-1} = a_1^{-1} h_1^{-1} = h_1^{-1} a_4$, $a_4 \in A_n$ (тут ми використали той факт, що $hA_n = A_n h$, тобто нормальність підгрупи A_n в S_n). Тепер за першою теоремою про ізоморфізм $HA_n/A_n \simeq H/H \cap A_n$. Але в нашому випадку $HA_n = S_n$. Звідси $(S_n : A_n) = (H : H \cap A_n) = 2$.

2) Якщо m і n — додатні натуральні числа, то $\mathbb{Z}/mn\mathbb{Z}/m\mathbb{Z}/mn\mathbb{Z} \simeq \mathbb{Z}/m\mathbb{Z}$.

3 Дія групи на множині

3.1 Означення та приклади

Означення 22. *Дією групи G на множині M* називають відображення $G \times M \rightarrow M$ з декартового добутку множин G і M у множину M , яке впорядкованій парі $(g, m) \in G \times M$ ставить у відповідність елемент ${}^g m \in M$, якщо це відображення має такі дві властивості:

- 1) ${}^{g_1 g_2} m = {}^{g_1}({}^{g_2} m)$;
- 2) ${}^e m = m$.

Тут g_1, g_2 — довільні елементи групи G , e — нейтральний елемент G , m — довільний елемент множини M .

Приклади.

1) Якщо $M = G$, і відображення $G \times G \rightarrow G$ є груповою операцією в G , то властивості 1), 2) з означення 22 зводяться до асоціативності множення та властивості нейтрального елемента: ${}^{g_1 g_2} m = (g_1 g_2)m = g_1(g_2 m) = {}^{g_1}(g_2 m)$, ${}^e m = em = m$. У цьому випадку кажуть, що група G діє на собі зсувами. Зафіксувавши елемент $g \in G$, одержуємо відображення $T_g: G \rightarrow G$, де $T_g(x) = gx$. Відображення T_g має обернене $(T_g)^{-1} = T_{g^{-1}}$, тому воно біективне. Далі, $T_{g_1} \circ T_{g_2} = T_{g_1 g_2}$, тобто співставлення $g \mapsto T_g$ є гомоморфізмом групи G в групу всіх біективних відображень множини G в себе. Ми вже зустрічалися з цією ситуацією у п. 1.2 при доведенні теореми Келі.

2) Група G діє зсувами не лише на множині всіх своїх елементів, але і на деяких інших своїх підмножинах. Зокрема, нехай H — підгрупа групи G , не обов'язково нормальні, $M = \{gH \mid g \in G\}$ — множина лівих суміжних класів групи G з підгрупою H . Відображення $G \times M \rightarrow M$,

$(g_1, gH) \mapsto g_1gH$ є дією групи G на множині M . Якщо $H \triangleleft G$, то G діє на факторгрупі G/H .

3) Нехай знову $G = M$. Розглянемо відображення *спряження*: $G \times G \rightarrow G$, $(g, m) \mapsto {}^g m = gmg^{-1}$. Маємо ${}^{g_1g_2}m = (g_1g_2)m(g_1g_2)^{-1} = g_1(g_2mg_2^{-1})g_1^{-1} = {}^{g_1}(g_2m)$ і ${}^e m = eme^{-1} = m$, тобто спряження є дією групи G на множині своїх елементів.

4) Якщо зафіксувати деякий елемент $g \in G$, то спряження визначає бієктивне відображення $C_g: G \rightarrow G$, $C_g(x) = gxg^{-1}$, $C_g^{-1} = C_{g^{-1}}$. У прикладі 3) ми перевірили рівність $C_{g_1g_2} = C_{g_1} \circ C_{g_2}$. Ця рівність означає, що співставлення $g \mapsto C_g$ є гомоморфізмом групи G у групу всіх бієктивних відображень множини G в себе. Відображення C_g є не лише автоморфізмом множини G , ле і автоморфізмом групи G , тобто воно зберігає групову операцію. Справді, $C_g(xy) = gxyg^{-1} = gxg^{-1}gyg^{-1} = C_g(x)C_g(y)$. Автоморфізмами C_g називають *внутрішніми автоморфізмами групи* G .

Нехай H — підгрупа групи G , $g \in G$. Множина $gHg^{-1} = \{ghg^{-1} \mid h \in H\}$ є теж, як легко переконатися, підгрупою групи G . Тому G діє спряженнями на множині своїх підгруп.

4) Нехай \mathbb{R}^n — числовий n -вимірний векторний простір, $G = \mathrm{GL}_n(\mathbb{R})$ — повна лінійна група. Група G діє на \mathbb{R}^n за правилом $(A, x) \mapsto Ax$ — добуток матриць A і x . Так само на \mathbb{R}^n діють інші класичні матричні групи, зокрема, $\mathrm{SL}_n(\mathbb{R})$ та $\mathrm{O}_n(\mathbb{R})$.

3.2 Стабілізатори та орбіти

Означення 23. Нехай група G діє на множині M і нехай m — деякий фіксований елемент множини M . *Стабілізатором* $\mathrm{St}(m)$ елемента m називають множину

$$\mathrm{St}(m) = \{g \in G \mid {}^g m = m\}.$$

Використовуючи критерій підгрупи, легко переконатися в тому, що стабілізатори є підгрупами групи G : якщо $g_1, g_2 \in \mathrm{St}(m)$, то ${}^{g_1g_2}m = {}^{g_1}({}^{g_2}m) = {}^{g_1}m = m$, тобто $g_1g_2 \in \mathrm{St}(m)$; $m = {}^e m = {}^{g_1^{-1}}{}^{g_1}m = {}^{g_1^{-1}}m$, ${}^{g_1^{-1}}m = m$, значить і $g_1^{-1} \in \mathrm{St}(m)$.

Приклади.

1) Нехай група G діє на собі спряженнями. Стабілізатор елемента $a \in G$ є підгрупою, що складається з елементів $g \in G$, для яких $gag^{-1} = a$, тобто $ga = ag$. Отже, стабілізатор елемента a складається з

усіх елементів групи G , що комутують з a ; його називають *централізатором* елемента a . Перетин централізаторів всіх елементів називають *центром групи* G ; це підгрупа елементів групи G , що комутують з усіма елементами групи G .

2) Нехай тепер група G діє спряженнями на множині своїх підгруп. Стабілізатор підгрупи H є підгрупою тих елементів $g \in G$, для яких $gHg^{-1} = H$. Ясно, що це найбільша підгрупа групи G , для якої H є її нормальнюю підгрупою; цю підгрупу називають *нормалізатором* підгрупи H .

Означення 24. Якщо група G діє на множині M , то *орбітою* елемента $m \in M$ називають множину $\mathcal{O}(m) = \{^g m \mid g \in G\}$.

Приклади.

1) Нехай $G = \left\{ \begin{pmatrix} \cos \varphi & \sin \varphi \\ -\sin \varphi & \cos \varphi \end{pmatrix} \mid \varphi \in \mathbb{R} \right\}$ — група всіх поворотів площини \mathbb{R}^2 . Група G діє на \mathbb{R}^2 так, як це означено в прикладі 5 п. 3.1. Орбітами тут є точка $(0, 0)$ та концентричні кола з центром у цій точці.

2) Розглянемо деяку підстановку $\varphi \in S_n$ і циклічну підгрупу $G = (\varphi)$, породжену цією підстановкою. Група G діє на множині $M = \{1, 2, \dots, n\}$ за правилом $(\varphi^k, x) \mapsto \varphi^k(x)$. Для цієї дії орбіти $\{i_1, i_2, \dots, i_m\}$ перебувають у біективній відповідності з циклами, в добуток яких розкладається підстановка φ (враховуючи одночленні цикли).

Твердження 25. Різні орбіти не мають спільних елементів.

Доведення. Потрібно довести, що коли $\mathcal{O}(m_1) \cap \mathcal{O}(m_2) \neq \emptyset$, то $\mathcal{O}(m_1) = \mathcal{O}(m_2)$. Якщо $m_0 \in \mathcal{O}(m_1) \cap \mathcal{O}(m_2)$, то існують $g_1, g_2 \in G$ такі, що $m_0 = {}^{g_1} m_1 = {}^{g_2} m_2$. Нехай $t \in \mathcal{O}(m_1)$. Тоді $t = {}^g m_1$ для деякого $g \in G$ і $t = {}^g m_1 = {}^{g g_1^{-1}} {}^{g_1} m_1 = {}^{g g_1^{-1}} {}^{g_2} m_2 \in \mathcal{O}(m_2)$. Звідси $\mathcal{O}(m_1) \subset \mathcal{O}(m_2)$.

Так само доводимо, що $\mathcal{O}(m_2) \subset \mathcal{O}(m_1)$, отже, $\mathcal{O}(m_1) = \mathcal{O}(m_2)$. \square

Твердження 26. $\text{St}({}^g m) = g^{-1} \text{St}(m)g$, тобто стабілізатори різних елементів одної орбіти спряженні.

Доведення. Починаємо з рівності $\text{St}({}^g m)g = {}^g m$. Звідси одержуємо, що $g^{-1} \text{St}({}^g m)g \subset \text{St}(m)$. Так само з рівності $\text{St}(m)g^{-1} {}^g m = {}^{g^{-1}} {}^g m$, тобто з рівності $g \text{St}(m)g^{-1} {}^g m = {}^g m$, випливає рівність $g \text{St}(m)g^{-1} \subset \text{St}({}^g m)$ або $\text{St}(m) \subset g^{-1} \text{St}({}^g m)g$. \square

Припустимо, що група G діє на скінченній множині M . Тоді кожна орбіта складається зі скінченої кількості елементів. Кількість елементів орбіти $\mathcal{O}(m)$ назовемо її довжиною і позначимо $|\mathcal{O}(m)|$.

Твердження 27. Якщо група G діє на скінченній множині, то довжина кожної орбіти $\mathcal{O}(m)$ дорівнює індексу стабілізатора $\text{St}(m)$ в групі G , тобто $|\mathcal{O}(m)| = (G : \text{St}(m))$.

Доведення. Якщо ${}^{g_1}m = {}^{g_2}m$, то $g_1^{-1}g_2 \in \text{St}(m)$, тобто $g_2 \in g_1\text{St}(m)$. Навпаки, ${}^{g_1}m \neq {}^{g_2}m$ тоді і тільки тоді, коли $g_2 \notin g_1\text{St}(m)$, тобто коли g_1 і g_2 лежать в різних суміжних класах групи G за підгрупою $\text{St}(m)$. Інакше кажучи, різні елементи орбіти перебувають у біективній відповідності з різними суміжними класами за підгрупою $\text{St}(m)$. Це й означає, що $|\mathcal{O}(m)| = (G : \text{St}(m))$. \square

3.3 Формула класів

У попередньому п. було доведено, що коли група G діє на множині M , то різні орбіти попарно не перетинаються. Якщо множина M скінчена, то позначимо через $|M|$ кількість її елементів. Нехай m_i — представники всіх різних орбіт, $i \in \mathcal{I}$, $\text{St}(m_i)$ — стабілізатори елементів m_i .

Теорема 28.

$$|M| = \sum_{i \in \mathcal{I}} (G : \text{St}(m_i)), \quad (3.3.1)$$

тобто кількість елементів множини M дорівнює сумі індексів стабілізаторів елементів m_i .

Доведення. За твердженням 25 різні орбіти утворюють покриття множини M . Тому $|M| = \sum_{i \in \mathcal{I}} |\mathcal{O}(m_i)|$, а за твердженням 27 маємо рівність $|\mathcal{O}(m_i)| = (G : \text{St}(m_i))$. Звідси й випливає формула (3.3.1). \square

Формулу (3.3.1) називають *формулою класів*.

3.4 Центр p -групи

Означення 29. Нехай p -просте число. Скінченна група, порядок якої є степенем числа p , називається *p -групою*.

Зауважимо, що існують некомутативні p -групи. Наприклад, множина матриць вигляду $\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}$, де a, b, c пробігають скінченне поле з p елементів, є некомутативною p -групою порядку p^3 .

Теорема 30. *Кожна нетривіальна p -група G має нетривіальний центр.*

Доведення. Нехай G діє на собі спряженнями. Якщо елемент $g \in G$ належить до центру групи G , то орбіта цього елемента є одноелементною підмножиною $\{g\}$. В іншому випадку, довжина орбіти є більшою від одиниці і дорівнює індексу централізатора $(G : \text{St}(g))$. З теореми Лагранжа випливає, що цей індекс є числом, що ділиться на p . Тому формула класів дає

$$|G| = |Z| + \sum_{i \in I} (G : \text{St}(g_i)), \quad (3.4.1)$$

де g_i — представники орбіт, що мають більше, ніж один елемент, $|Z|$ — порядок центру Z групи G . $|Z| \geq 1$, бо нейтральний елемент групи G , очевидно, лежить в центрі. Оскільки $|G|$ і $(G : \text{St}(g_i))$ діляться на p , то з (3.4.1) випливає, що і $|Z|$ ділиться на p , тобто центр містить більше ніж один елемент. \square

4 Теореми Силова

За теоремою Лагранжа порядок скінченної групи ділиться на порядок кожної своєї підгрупи. Звідси постає питання пошуку для кожного дільника m порядку n групи G підгрупи порядку m . В загальному випадку відповідь на це питання негативна, про що свідчить приклад групи парних підстановок A_4 порядку 12, в якій немає підгруп порядку 6. У випадку абелевих груп частковою позитивною відповіддю є наступне тверження.

Твердження 31. *Якщо просте число p ділить порядок абелевої групи G , то в ній існує елемент порядку p .*

Доведення. Проведемо доведення індукцією за порядком групи G . База індукції очевидна: якщо G — група простого порядку p , то, за наслідком з теореми Лагранжа, порядок кожного елемента $a \in G$, $a \neq e$ дорівнює p . Проводячи індуктивний крок, можна вважати, що в групі G існує власна нетривіальна підгрупа. Справді, якщо в G немає власних нетривіальних підгруп, то вона циклічна. Досить взяти $g \in G$, $g \neq e$ і група буде збігатися з циклічною групою, породженою елементом g . Підгрупи циклічних груп відомі; якщо циклічна група має порядок mn , то досить взяти породжуючий елемент в степені m і породити ним підгрупу — отримаємо власну нетривіальну підгрупу.

Нехай H — нетривіальна підгрупа групи G . Якщо порядок H не ділиться на p , то порядок фактор-групи G/H ділиться на p , значить у

фактор-групі G/H існує елемент gH порядку p . Для його прообразу g при канонічному гомоморфізмі $G \rightarrow G/H$ маємо $g^p = h \in H$. Звідси випливає, що g має порядок pt , де t — порядок h . Тоді елемент g^m має порядок p . \square

У загальному випадку відповідь на питання про існування підгруп певних порядків, які є дільниками порядку групи, дають теореми Силова.

Нехай $|G| = p^n m$, де p — просте число, m — натуральне число, взаємно просте з p . Підгрупу $P \subset G$ порядку $|P| = p^n$ (якщо така існує) назовемо *силовською p -підгрупою* групи G .

Теорема 32 (перша теорема Силова). *Силовські p -підгрупи існують.*

Доведення. Проведемо доведення індукцією за порядком групи G . Нехай $|G| = p^k m$, де $(m, p) = 1$. База індукції — випадок $|G| = p$ — очевидна. Можливі два випадки:

- 1) порядок центру $Z(G)$ ділиться на p ;
- 2) порядок центру $Z(G)$ не ділиться на p .

Якщо порядок центру $Z(G)$ ділиться на p , то, в силу твердження 31, в $Z(G)$ знайдеться підгрупа H порядку p . Вона, як і довільна підгрупа центру, нормальна в G . Порядок факторгрупи G/H , за теоремою Лагранжа, ділиться на p^{k-1} , тому, за припущенням індукції, в G/H існує підгрупа порядку p^{k-1} . Нехай K — її повний прообраз при канонічному гомоморфізмі $G \rightarrow G/H$; тоді $H \subseteq K$, бо H — повний прообраз одиниці. Порядок K/H дорівнює p^{k-1} , порядок H дорівнює p , отже, порядок K дорівнює p^k .

У випадку, коли p не ділить порядок центру $Z(G)$, розглянемо дію спряження групи G на множині $M = G$, тобто $(g, x) = x^g = g^{-1}xg$. При такій дії одноелементні орбіти — це елементи з $Z(G)$, іх ми виділимо окремо і отримаємо таке розбиття групи G :

$$G = Z(G) \cup \mathcal{O}(x_1) \cup \cdots \cup \mathcal{O}(x_n),$$

де $\mathcal{O}(x_i)$ — різні орбіти, для яких $|\mathcal{O}(x_i)| > 1$. Оскільки p не ділить порядок $Z(G)$, то в силу формули класів $|G| = |Z(G)| + |\mathcal{O}(x_1)| + \cdots + |\mathcal{O}(x_n)|$, знайдеться таке i , що довжина орбіти $\mathcal{O}(x_i)$ не ділиться на p . Але довжина орбіти $\mathcal{O}(x_i)$ дорівнює індексу в G централізатора $\text{St}(x_i)$, значить, за теоремою Лагранжа, порядок $\text{St}(x_i)$ ділиться на p^k . Оскільки порядок $\text{St}(x_i)$ строго менший від порядку групи G (індекс $\text{St}(x_i)$ більший ніж 1, бо $|\mathcal{O}(x_i)| > 1$), то до $\text{St}(x_i)$ можна застосувати індуктивне

припущення, і в $\text{St}(x_i)$, значить і в G , знайдеться підгрупа порядку p^k .

□

Звідси, як наслідок, отримуємо теорему Коші.

Наслідок 33 (теорема Коші). *Якщо порядок скінченної групи ділиться на p , то в ній існує елемент порядку p .*

Доведення. Розглянемо силовську p -підгрупу H групи G . $H \in p$ -підгрупою, тому, за теоремою 30 вона має нетривіальний центр $Z(H)$. Оскільки $Z(H)$ — абельова p -група, то за твердженням 31 в ній існує елемент порядку p . □

Дві інші теореми Силова дають нам опис силовських підгруп.

Теорема 34 (друга теорема Силова). *Нехай P і P_1 — довільні дві силовські p -підгрупи групи G . Тоді вони є спряженими, тобто знайдеться елемент $g \in G$, для якого $P_1 = gPg^{-1}$.*

Доведення. Визначимо дію групи P_1 на множині лівих суміжних класів $G/P = \bigcup_i g_i P$ як відображення: $(p_1, gP) \mapsto p_1 g P$ для довільних $p_1 \in P$, $g \in G$. За твердженням 27, довжина довільної орбіти ділить порядок групи P_1 , який дорівнює p^k . Нагадаємо, що $|G| = p^k m$, де m — ціле число, взаємно просте з p . Тоді

$$m = \frac{p^k m}{p^k} = \frac{|G|}{|P|} = p^{k_1} + p^{k_2} + \dots,$$

де p^{k_1}, p^{k_2}, \dots — довжини орбіт. Оскільки числа m і p взаємно прості, то хоча б одна з орбіт має довжину $p^{k_i} = 1$, тобто $P_1 \cdot gP = gP$ для деякого елемента $g \in G$. Звідси $P_1 \cdot gPg^{-1} = gPg^{-1}$, тому $P_1 \subset gPg^{-1}$. Оскільки P_1 — силовська p -підгрупа, то порядки груп P_1 і P однакові і скінченні, і з включення $P_1 \subset gPg^{-1}$ випливає, що $P_1 = gPg^{-1}$, що й потрібно довести. □

Теорема 35 (третя теорема Силова). *Кількість N_p силовських p -підгруп групи G конгруентна з 1 за модулем числа p .*

Доведення. Нехай P — силовська p -підгрупа, M — множина всіх силовських p -підгруп. Нехай група P діє спряженнями на множині M , тобто $(p, S) \mapsto p^{-1}Sp$ для довільного $p \in P$ і довільної силовської підгрупи S . Які можуть бути орбіти при цій дії? Існує орбіта, яка складається з одного елемента, Оскільки $p^{-1}Pp = P$ для всіх $p \in P$. Довжина кожної

іншої орбіти дорівнює індексу стабілізатора в P , і тому є степенем простого числа p . Тоді $|M| = 1 + p^{k_1} + \dots + p^{k_s}$, де $k_1 \geq 1, \dots, k_s \geq 1$. Звідси й випливає, що $N_p \equiv 1 \pmod{p}$. \square

5 Розв'язні групи

Означення 36. Група G називається *розв'язною*, якщо існує послідовність її підгруп $G_0 = G, G_1, G_2, \dots, G_k = \{e\}$, для якої виконуються умови:

- 1) $G_k \subset G_{k-1} \subset \dots \subset G_1 \subset G_0$,
- 2) G_i — нормальнa підгрупа в G_{i-1} ,
- 3) фактор-групи G_{i-1}/G_i — абелеві ($i = 1, 2, \dots, k$).

Прикладом розв'язної групи може служити довільна абелева група, а також група S_3 . Єдиною нормальнou підгрупою групи S_3 є група парних підстановок A_3 . Розглянемо послідовність $S_3 \supset A_3 \supset \{e\}$ і фактор-групи $S_3/A_3, A_3/\{e\}$. Група S_3/A_3 є групою другого порядку, отже абелевою. Група $A_3/\{e\}$ ізоморфна групі A_3 , яка породжується підстановкою $(\begin{smallmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{smallmatrix})$, тобто є циклічною, і отже, абелевою.

Перевіримо, що група S_4 — теж розв'язна. Для цього розглянемо таку послідовність її підгруп: $S_4 \supset A_4 \supset H \supset \{e\}$, де A_4 — підгрупа парних підстановок і $H = \{e, (1, 2)(3, 4), (1, 3)(2, 4), (1, 4)(2, 3)\}$ — підгрупа Клейна. $A_4 \triangleleft S_4$, бо A_4 має індекс 2 в S_4 . Підгрупа H є нормальнou підгрупою в A_4 . Справді, нехай $a \in A_4, h \in H$. Тоді $(aha^{-1})^2 = ah^2a^{-1} = aa^{-1} = e$. Тому $aha^{-1} \in H$, бо всі елементи з $A_4 \setminus H$ є потрійними циклами, отже, мають порядок 3. Нарешті, група H — абелева, факторгрупи S_4/A_4 та A_4/H є групами, відповідно, 2-го та 3-го порядків — тому вони циклічні і, отже, бельові.

Твердження 37. *Кожна p -група розв'язна.*

Доведення. Нехай G — p -група. Оскільки центр p -групи нетривіальний, то можливі випадки: $Z(G) = G$, тобто G абелева, а, значить, розв'язна, бо $\{e\} \neq Z(G) \subset G$. У другому випадку можна побудувати фактор-групу $\bar{G} = G/H_1$, де через H_1 ми позначили центр $Z(G)$. Вона знову є p -групою і має нетривіальний центр $Z(\bar{G}) = H_2/H_1$. Продовжуючи так міркувати, ми отримаємо зростаючу послідовність підгруп

$$\{e\} \triangleleft H_1 \triangleleft H_2 \triangleleft \dots \quad (5.0.2)$$

Група G — скінчена, тому послідовність (5.0.2) повинна через скінченне число кроків обірватися рівністю $H_n = G$. Всі факторгрупи H_k/H_{k-1} є абелевими, отже група G розв'язна. \square

Покажемо, що група S_n при $n \geq 5$ нерозв'язна. Спочатку доведемо одну властивість групи S_n .

Твердження 38. *Нехай G — деяка підгрупа групи S_n , $n \geq 5$, в яку входять всі потрійні цикли, H — нормальнна підгрупа групи G і факторгрупа G/H — абельова. Тоді в H також входять всі потрійні цикли.*

Доведення. Нехай f — канонічний гомоморфізм $G \rightarrow G/H$, при якому кожному елементу $g \in G$ відповідає клас gH , і нехай (a, b, c) — деякий потрійний цикл. Приймемо $x = (d, b, a)$, $y = (a, l, c)$ і розглянемо елемент $x^{-1}y^{-1}xy$. Маємо

$$f(x^{-1}y^{-1}xy) = f(x^{-1})f(y^{-1})f(x)f(y) = (f(x))^{-1}f(x)(f(y))^{-1}f(y) = e',$$

де e' — нейтральний елемент групи G/H (слід зауважити, що тут ми використовуємо той факт, що G/H абельова). Отже, $x^{-1}y^{-1}xy \in H$. З іншого боку, кожен потрійний цикл (a, b, c) можна записати у вигляді $x^{-1}y^{-1}xy$, як показує рівність $x^{-1}y^{-1}xy = (a, b, d)(c, l, a)(d, b, a)(a, l, c) = (a, b, c)$. \square

Твердження 39. *Груп S_n при $n \geq 5$ нерозв'язна.*

Доведення. Нехай ми маємо послідовність нормальних підгруп $G_0 = S_n \supset G_1 \supset \dots \supset G_k = \{e\}$, для якої факторгрупи G_{i-1}/G_i абелеві. Оскільки групі S_n належать всі потрійні цикли, то за попереднім твердженням вони повинні належати кожній групі G_i . Але тоді група G_k не може бути тривіальною. \square

Теорема 40. *Довільна підгрупа розв'язної групи розв'язна.*

Доведення. Нехай G розв'язна група, тобто для G існує такий ланцюжок підгруп $G = G_0 \supset G_1 \supset G_2 \supset \dots \supset G_n = \{e\}$, що G_i нормальнна підгрупа в G_{i-1} і факторгрупи G_{i-1}/G_i абелеві, $i = 1, 2, \dots, n$. Якщо H довільна підгрупа групи G , то приймемо $H_i = H \cap G_i$. Тоді

$$H_{i-1} \cap G_i = H_{i-1} \cap G_{i-1} \cap G_i = H_{i-1} \cap G_i = H_i. \quad (5.0.3)$$

Оскільки G_i нормальнна підгрупа в G_{i-1} , то H_i нормальнна в H_{i-1} . Тепер, використовуючи теорему 20 та (5.0.3), отримуємо

$$H_{i-1}/H_i = H_{i-1}/H_{i-1} \cap G_i \simeq H_{i-1}G_i/G_i \subset H_{i-1}G_{i-1}/G_i = G_{i-1}/G_i,$$

тобто H_{i-1}/H_i є підгрупою абелевої групи G_{i-1}/G_i , а тому абелево. Отже, для підгрупи H існує ланцюжок підгруп

$$H = H_0 \supset H_1 \supset H_2 \supset \dots \supset H_n = \{e\},$$

де H_i нормальна підгрупа в H_{i-1} і факторгрупи H_{i-1}/H_i абелеві. Тому група H розв'язна. \square

Теорема 41. *Гомоморфний образ розв'язної групи є розв'язною групою.*

Доведення. Нехай G розв'язна група і G_i підгрупи відповідного ланцюжка підгруп. Нехай f — гомоморфізм і $f(G) = G'$. Переконаємося, що $G'_i = f(G_i)$ утворюють ланцюжок нормальних підгруп для групи G' . За твердженням 16, 4) G'_i є нормальною підгрупою групи G'_{i-1} . Легко переконатися, що гомоморфізм $f: G_{i-1} \rightarrow G'_{i-1}$ породжує гомоморфізм G_{i-1}/G_i на G'_{i-1}/G'_i , $\bar{f}(aG_i) = f(a)G'_i$. Група G_{i-1}/G_i абелева, Оскільки гомоморфний образ бельової групи є абелевою групою, тому отримуємо, що G'_{i-1}/G'_i абелева група і це завершує доведення. \square

Наслідок 42. *Кожна факторгрупа розв'язної групи є розв'язною групою.*

Теорема 43. *Нехай G скінчена розв'язна група. Існує послідовність підгруп*

$$G = G_0 \supset G_1 \supset G_2 \supset \cdots \supset G_n \supset \{e\},$$

де $G_{i-1} \triangleright G_i$, i факторгрупи G_{i-1}/G_i циклічні.

Доведення. Для групи G існує послідовність підгруп $G = G_0 \supset G_1 \supset G_2 \supset \cdots \supset G_n = \{e\}$ з властивістю $G_i \triangleleft G_{i-1}$ і з абелевими факторгрупами $\overline{H}_{i-1} = G_{i-1}/G_i$, $1 \leq i \leq k$. \overline{H}_{i-1} — скінчена абелева група, тому вона є прямою сумою циклічних підгруп $K_1 \oplus \cdots \oplus K_m$. Розглянемо ланцюжок підгруп групи \overline{H}_{i-1} :

$$\overline{H}_{i-1} = \overline{H}_{i-1,1} \supset \overline{H}_{i-1,2} \supset \cdots \supset \overline{H}_{i-1,m} \supset \{e\}, \quad (5.0.4)$$

де $\overline{H}_{i-1,j} = K_j \oplus \cdots \oplus K_m$, $1 \leq j \leq m$.

З теореми 20 про ізоморфізми груп випливає, що фактор-групи

$$\begin{aligned} \overline{H}_{i-1,j}/\overline{H}_{i-1,j+1} &= K_j \oplus (K_{j+1} \oplus \cdots \oplus K_m)/K_{j+1} \oplus \cdots \oplus K_m \simeq \\ &\simeq K_j/K_j \cap (K_{j+1} \oplus \cdots \oplus K_m) = K_j/\{e\} = K_j \end{aligned}$$

є циклічними групами. За ланцюжком підгруп (5.0.4) будуємо ланцюжок підгруп групи G_{i-1} :

$$G_{i-1} = G_{i-1,1} \supset G_{i-1,2} \supset \cdots \supset G_{i-1,m} \supset G_i, \quad (5.0.5)$$

де $G_{i-1,j}$, $1 \leq j \leq m$ — прообраз підгрупи $H_{i-1,j}$ відносно канонічного гомоморфізму $\bar{f}: G_{i-1} \rightarrow G_{i-1}/G_i$. За твердженням 16, 4), $G_{i-1,j+1}$ є

нормальною підгрупою групи $G_{i-1,j}$. Тепер, використовуючи теорему 21 про ізоморфізми груп, маємо:

$$G_{i-1,j}/G_{i-1,j+1} \simeq G_{i-1,j}/G_i/G_{i-1,j}/G_i \simeq \overline{H}_{i-1,j}/\overline{H}_{i-1,j+1} \simeq K_j.$$

Ми довели, що між групами G_{i-1} та G_i можна вставити скінченну кількість підгруп так, що одержиться нормальний ланцюжок підгруп (5.0.5) з циклічними факторгрупами $G_{i-1,j}/G_{i-1,j+1}$. Зробивши це для всіх i , $1 \leq i \leq k-1$, одержимо ланцюжок підгруп, про який іде мова у формульованні теореми. \square

Вправи

1. Довести, що множина з двох елементів e, a із законом композиції $ee = e, ea = ae = a, aa = e$ є групою.
2. Нехай p — просте число. Довести, що множина \mathbb{C}_{p^∞} всіх коренів рівнянь $x^{p^n} = 1, n = 1, 2, \dots$ над полем комплексних чисел з операцією звичайного множення, є нескінченною абелевою групою (група \mathbb{C}_{p^∞} називається *квазіциклическою групою*).
3. Довести, що підгрупами $\mathbb{C}_{p^n}, n = 1, 2, \dots$, вичерпуються всі власні підгрупи квазіциклическої групи \mathbb{C}_{p^∞} .
4. Довести, що група S_4 має, крім тривіальних, лише наступні нормальні підгрупи:
 - a) підгрупу парних підстановок A_4 ;
 - б) “четверну групу Клейна U_4 ”, яка складається з підстановок: (1), (12)(34), (13)(24), (14)(23).
5. Довести, що факторгрупа S_4/U_4 ізоморфна групі S_3 (U_4 — “четверна група Клейна”).
6. Довести, що коли підгрупи H, K цикліческої групи G задовольняють умову $G/H \simeq G/K$, то $H = K$.
7. Довести, що кожна підгрупа і кожна факторгрупа цикліческої групи циклічна.
8. Довести, що підгрупа $M = \{X \in \mathrm{GL}_n(\mathbb{R}) \mid \det X > 0\}$ нормальна в $\mathrm{GL}_n(\mathbb{R})$.

9. Навести приклад групи G і її підгруп H, K , для яких $H \triangleleft K, K \triangleleft G$, але H не є нормальнюю підгрупою в G .
10. Довести, що потрійні цикли $(123), (124), \dots, (12n)$ при $n > 2$ породжують групу парних підстановок A_n .
11. Довести, що група $\mathrm{SL}_n(\mathbb{Z})$ породжується матрицями вигляду $E + E_{ij}$, $(i \neq j)$, де E одинична матриця порядку n , E_{ij} — матриця порядку n , яка на місці (i, j) містить одиницю, а на інших місцях нулі.
12. Довести, що абелльова група є простою лише тоді, коли вона циклічна і має простий порядок.
13. Показати, що $\mathrm{Aut}S_3 \cong S_3$.
14. Довести, що група матриць вигляду $\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$, $a \neq 0$, відносно звичайного множення над довільним числовим полем має тривіальний центр.
15. Довести, що існує лише дві неізоморфні групи порядку 6: циклічна група \mathbb{Z}_6 і симетрична група S_3 .
16. Довести, що група парних підстановок A_4 не містить підгруп порядку 6.
17. Довести, що група порядку 196 містить нормальну силовську p -підгрупу.
18. Нехай група G має порядок pq (p, q різні прості числа і $p < q$), причому силовська p -підгрупа єдина. Довести, що тоді G циклічна група порядку pq .
19. Знайти з точністю до ізоморфізму всі групи порядку 15 (див. задачу 18).
20. Знайти з точністю до ізоморфізму всі абелльові групи порядку 72.
21. Довести, що довільна абелльова група порядку n , де n не ділиться на квадрат жодного простого числа, ізоморфна групі комплексних коренів n -го степеня з одиницею.

6 Основні поняття теорії кілець

6.1 Означення та найпростіші наслідки з аксіом

Означення 44. Абелльова група $(R, +)$ називається *кільцем*, якщо на ній визначена операція множення, яка зв'язана з додаванням дистрибутивним законом:

$$(a+b)c = ac + bc \text{ і } a(b+c) = ab + ac \text{ для всіх } a, b, c \in R.$$

Якщо $(R, +, \cdot)$ — кільце, то $(R, +)$ називають *адитивною групою* кільця R , а (R, \cdot) — *мультиплікативним групoidом*. Операції в кільці називають, відповідно, додаванням і множенням. Якщо множення асоціативне, тобто $a(bc) = (ab)c$ для всіх $a, b, c \in R$, то кільце $(R, +, \cdot)$ називають *асоціативним*. Якщо $ab = ba$ для всіх $a, b, c \in R$, то кільце R називається *комутативним*.

З означення кільця випливає, що в R існує єдиний нейтральний відносно додавання елемент 0 . З іншого боку, в $(R, +, \cdot)$ може не бути нейтрального елемента відносно множення. Наприклад, множина всіх парних цілих чисел є кільцем відносно звичайних операцій додавання і множення і в ньому, очевидно, немає нейтрального відносно множення елемента. Кільце, в якому існує нейтральний елемент відносно множення (його називають *одиничним елементом* і позначають 1), називається *кільцем з 1*. Якщо в кільці існує одиничний елемент 1 , то він єдиний: маємо $1' = 1' \cdot 1'' = 1''$, якщо $1'$ і $1''$ — два одиничні елементи.

Оскільки кільце є абелльовою групою відносно додавання, то в ньому вірні всі безпосередні наслідки з аксіом групи, а саме, єдиність 0 і протилежного елемента, закон скорочення, рівність $-(-a) = a$, однозначна розв'язність рівняння $a + x = b$ і т.п.

Наступне твердження є списком тих найпростіших властивостей кільця, що безпосередньо випливають з аксіом.

- Твердження 45.**
- 1) $a(b - c) = ab - ac$, $(b - c)a = ba - ca$;
 - 2) $(\sum_{i=1}^n a_i) \left(\sum_{j=1}^m b_j \right) = \sum_{i=1, j=1}^{m, n} a_i b_j$;
 - 3) $a^n \cdot a^m = a^{n+m}$; $(a^n)^m = a^{nm}$, де $a^n = \underbrace{a \dots a}_n$, $a^0 = 1$;
 - 4) $n(ab) = a \cdot nb = na \cdot b$;
 - 5) $0 \cdot a = a \cdot 0 = 0$;
 - 6) $a(-b) = (-a)b = -(ab)$;
 - 7) $(-a)(-b) = ab$
- (тут a, b, c, a_i, b_j — довільні елементи кільця R , $m, n \in \mathbb{Z}$).

Доведення. Властивості 1)–4) пропонуємо довести самостійно.

5) $0 \cdot a = (0 + 0)a = 0 \cdot a + 0 \cdot a$. Звідси $0 + 0 \cdot a = 0 \cdot a + 0 \cdot a$, властивість $0 \cdot a = 0$ випливає із закону скорочення для груп. Так само $a \cdot 0 = 0$.

6) $a(-b) + ab = a(-b + b) = a \cdot 0 = 0$ за властивістю 5). Звідси $a(-b) = -ab$. Аналогічно доводимо, що $(-a)b = -ab$.

7) $(-a)(-b) + (-a)b = -a(-b + b) = -a \cdot 0 = 0$. Використовуючи 6), одержуємо, що $(-a)(-b) = ab$. \square

Означення 46. Елемент e кільця R назовемо *їдемпотентом*, якщо $e^2 = e$. Якщо a і b — ненульові елементи кільця R і $ab = 0$, то a і b називають *дільниками нуля*: a — лівий дільник нуля, а b — правий дільник нуля у випадку некомутативного кільця. Якщо $ab = 1$, то a і b називають *дільниками одиниці* (або *одиницями*) кільця R . Очевидно, що дільники нуля не можуть бути дільниками одиниці і навпаки. Ненульовий елемент кільця, який не є дільником нуля, називають *регулярним* елементом.

Очевидно, що 0 і 1 є ідемпотентами, назовемо їх тривіальними ідемпотентами.

Твердження 47. В кільці без дільників нуля кожен ідемпотент тривіальний.

Доведення. Нехай $e \in R$ — ідемпотент, $e \neq 0$ і $a \in R$. Тоді $e(a - ea) = ea - ea = 0$, звідси $a = ea$. Так само показуємо, що $ae = a$. Отже, $e = 1$. \square

Зауважимо, що в кільці з дільниками нуля можуть бути нетривіальні ідемпотенти. Наприклад, елементи $\bar{5}$ і $\bar{6}$ кільця $\mathbb{Z}/10\mathbb{Z}$ є ідемпотентами.

Мультиплікативний моноїд (R, \cdot) асоціативного кільця з 1 в загальному випадку не є групою. Однак існують кільця, в яких ненульові елементи утворюють групу відносно множення. Такі кільця називають *тілами*. Комутативне тіло називають *полем*.

Підмножину R_1 кільця R , яка сама є кільцем відносно тих самих операцій, що і R , називають *підкільцем* кільця R . Пропонуємо читачеві самостійно довести таке твердження.

Твердження 48. Непорожня підмножина R_1 кільця R є підкільцем тоді і тільки тоді, коли виконуються умови:

- a) якщо $a, b \in R_1$, то $a + b \in R_1$ і $ab \in R_1$;
- б) якщо $a \in R_1$, то $-a \in R_1$.

Одноелементну множину $\{0\}$ і все кільце R називають тривіальними підкільцями кільця R .

Відзначимо, що у випадку комутативних кілець з одиницею аксіома комутативності додавання є наслідком інших аксіом кільця. Справді, $0 = a + b + (-b - a) = a + b + (-1)(b + a)$. Звідси випливає $b + a = 0 + (b + a) = a + b + (-1 + 1)(b + a) = a + b + 0(b + a) = a + b$.

Якщо R — кільце без одиниці, то комутативність додавання не можна вивести з інших аксіом. Щоб переконатися в цьому, візьмемо довільну некомутативну групу R , групову операцію в R назовемо додаванням, і означимо на R нульове множення, тобто для довільних $a, b \in R$ за означенням $ab = 0$, де 0 — нейтральний елемент групи R . Зрозуміло, що R задовільняє всі аксіоми кільця, крім комутативності додавання.

Будь-яку абелеву групу $(A, +)$ можна вважати кільцем, задавши в A нульове множення. Таке кільце називають *нульовим*.

Відзначимо, що ми обмежуємо себе вивченням асоціативних кілець, тому далі термін кільце означатиме асоціативне кільце.

6.2 Приклади кілець і тіл

a) Числові кільця. Множини $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ із звичайними операціями додавання і множення є кільцями. Очевидно, що всі ці кільця є кільцями з одиницею. Кільця $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ є полями, кільце \mathbb{Z} не є полем. Множина $2\mathbb{Z}$ всіх парних чисел є кільцем без одиниці. У ланцюжку включень $2\mathbb{Z} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ кожне кільце є підкільцем всіх кілець, у які воно включено.

Якщо R — будь-яке підкільце поля комплексних чисел \mathbb{C} , то назовемо R *числовим кільцем*. Нехай R — числове кільце і $\alpha \in \mathbb{C}$. Тоді множина $R[\alpha] = \{a_0 + a_1\alpha + \cdots + a_n\alpha^n \mid a_i \in R\}$ — теж числове кільце відносно звичайних операцій додавання і множення.

б) Кільця матриць. Нехай R — будь-яке кільце. Множина $M_n(R)$ квадратних матриць n -го порядку з елементами з кільця R є кільцем відносно звичайних операцій додавання та множення матриць: для $[a_{ij}], [b_{ij}] \in M_n(R)$

$$[a_{ij}] + [b_{ij}] = [a_{ij} + b_{ij}], \quad [a_{ij}] \cdot [b_{ij}] = \left[\sum_{k=1}^n a_{ik}b_{kj} \right].$$

Зокрема, можна розглядати кільця матриць n -го порядку, елементами яких є матриці m -го порядку: $M_n(M_m(R))$.

Кільця матриць $M_n(R)$ є некомутативними кільцями, навіть якщо кільце R комутативне. В кільцях матриць є багато дільників нуля і нетривіальних ідемпотентів. Наприклад, $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \in M_2(\mathbb{Z})$ є дільником нуля і ідемпотентом. Зауважимо, що підмножина матриць $A = \left\{ \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \mid a \in \mathbb{Z} \right\}$ є підкільцем кільця $M_n(\mathbb{Z})$. Одиничним елементом кільця A є матриця $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$, одиничним елементом кільця $M_n(\mathbb{Z})$ є одинична матриця $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. Це показує, що одиниця підкільца може не бути одиницею кільца.

в) Кільця многочленів. Якщо R — будь-яке кільце, то можна побудувати кільце $R[X]$ многочленів з коефіцієнтами з кільця R . Кільце многочленів $R[X]$ комутативне, якщо R комутативне, і без дільників нуля, якщо R без дільників нуля. Зокрема, всі кільця $\mathbb{Z}[X]$, $\mathbb{Z}[X_1, \dots, X_n]$ (або, більш загально, $R[X]$, $R[X_1, \dots, X_n]$, де R — будь-яке числове кільце) є комутативними кільцями з 1 і без дільників нуля.

г) Кільця формальних степеневих рядів. Нехай R — довільне кільце. Розглянемо множину $R[[X]] = \{(a_0, a_1, \dots, a_n, \dots) \mid a_i \in R\}$ всіх нескінченних послідовностей елементів кільця \mathbb{R} . Введемо позначення: $(a_0, a_1, \dots, a_n, \dots) = \sum_{n=0}^{\infty} a_n X^n$. Означимо на $R[[X]]$ дві операції:

$$\begin{aligned} \sum_{n=0}^{\infty} a_n X^n + \sum_{n=0}^{\infty} b_n X^n &= \sum_{n=0}^{\infty} (a_n + b_n) X^n \\ \left(\sum_{n=0}^{\infty} a_n X^n \right) \cdot \left(\sum_{n=0}^{\infty} b_n X^n \right) &= \sum_{n=0}^{\infty} \left(\sum_{i+j=n} a_i b_j \right) X^n. \end{aligned}$$

Так само, як і у випадку многочленів перевіряємо, що $R[[X]]$ — кільце відносно цих операцій.

д) Кільця функцій. Нехай R — довільне кільце. Розглянемо множину $R^M \stackrel{\text{df}}{=} \{f: M \rightarrow R\}$ — всіх відображення з M у R . Означимо на цій множині R^M дві операції додавання і множення: для $f, g \in R^M$

$$(f + g)(m) = f(m) + g(m), \quad (f \cdot g)(m) = f(m)g(m).$$

Легко перевірити, що R^M є кільцем відносно цих операцій. Якщо R — кільце з 1, то і R^M — кільце з 1 (одиничний елемент кільця R^M — це відображення $\tilde{1}: M \rightarrow R$, для якого $\tilde{1}(m) = 1$, де 1 — одиничний елемент кільця R).

Зокрема, кільцями є множини $F_{(a,b)}$ (множина всіх дійсних функцій, визначених на інтервалі (a, b)), а їх підкільцями — $C_{(a,b)}$ (множина всіх неперервних функцій на (a, b)), $C_{(a,b)}^{(n)}$ (множина всіх n разів неперервно диференційованих функцій) і т.п.

е) Приклад бульового кільця. *Бульовим кільцем* називають кільце, в якому всі елементи є ідемпотентами. Нехай M — довільна множина, 2^M — множина всіх підмножин множини M . Розглянемо на множині 2^M операції додавання і множення:

$$A + B \stackrel{\text{df}}{=} (A \cup B) \setminus (A \cap B), \quad A \cdot B \stackrel{\text{df}}{=} A \cap B.$$

Роль нуля тут відіграє порожня множина, а роль одиниці — вся множина M . Рівність $A + A = (A \cup A) \setminus (A \cap A) = \emptyset$ показує, що $-A = A$, звідси $2A = \emptyset$. Очевидно, що $A^2 = A \cap A = A$. Отже, 2^M є бульовим кільцем (пропонуємо читачеві самостійно перевірити, що 2^M є кільцем відносно визначених вище операцій).

е) Приклад некомутативного тіла (тіло кватерніонів). Розглянемо множину \mathbb{H} , елементи якої назовемо *кватерніонами*

$$H = \left\{ \begin{pmatrix} u & v \\ -\bar{v} & \bar{u} \end{pmatrix} \mid u, v \in \mathbb{C} \right\} \subset M_2(\mathbb{C}),$$

де $\overline{(\cdot)}$ означає комплексне спряження. З рівностей

$$\begin{aligned} \begin{pmatrix} u & v \\ -\bar{v} & \bar{u} \end{pmatrix} + \begin{pmatrix} z & t \\ -\bar{t} & \bar{z} \end{pmatrix} &= \begin{pmatrix} u+z & v+t \\ -\overline{(v+t)} & \overline{(u+z)} \end{pmatrix}, \\ - \begin{pmatrix} u & v \\ -\bar{v} & \bar{u} \end{pmatrix} &= \begin{pmatrix} -u & -v \\ -\overline{(-v)} & -\bar{u} \end{pmatrix}, \\ \begin{pmatrix} u & v \\ -\bar{v} & \bar{u} \end{pmatrix} \cdot \begin{pmatrix} z & t \\ -\bar{t} & \bar{z} \end{pmatrix} &= \begin{pmatrix} uz - v\bar{t} & ut + v\bar{z} \\ -\overline{(ut + v\bar{z})} & \overline{uz - v\bar{t}} \end{pmatrix} \end{aligned}$$

згідно твердження 48 випливає, що \mathbb{H} — підкільце кільця $M_2(\mathbb{C})$. Переонаємося, що кожна ненульова матриця з кільця \mathbb{H} має обернену, що знову належить до \mathbb{H} .

Для цього зауважимо, що коли $u = a + bi$ і $v = c + di$, то $u\bar{u} + v = a^2 + b^2 + c^2 + d^2$. Тому з $(\begin{smallmatrix} u & v \\ -\bar{v} & \bar{u} \end{smallmatrix}) \neq (\begin{smallmatrix} 0 & 0 \\ 0 & 0 \end{smallmatrix})$ випливає $u\bar{u} + v\bar{v} \neq 0$. Тепер

$$\begin{pmatrix} u & v \\ -\bar{v} & \bar{u} \end{pmatrix} \frac{1}{u\bar{u} + v\bar{v}} \begin{pmatrix} \bar{u} & -v \\ \bar{v} & u \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \frac{1}{u\bar{u} + v\bar{v}} \begin{pmatrix} \bar{u} & -v \\ \bar{v} & u \end{pmatrix} \begin{pmatrix} u & v \\ -\bar{v} & \bar{u} \end{pmatrix},$$

тобто

$$\frac{1}{u\bar{u} + v\bar{v}} \begin{pmatrix} \bar{u} & -v \\ \bar{v} & u \end{pmatrix} = \begin{pmatrix} u & v \\ -\bar{v} & \bar{u} \end{pmatrix}^{-1}.$$

Отже, \mathbb{H} — тіло, воно некомутативне, бо, наприклад, $(\begin{smallmatrix} i & 0 \\ 0 & -i \end{smallmatrix})(\begin{smallmatrix} 0 & i \\ i & 0 \end{smallmatrix}) \neq (\begin{smallmatrix} 0 & i \\ i & 0 \end{smallmatrix})(\begin{smallmatrix} i & 0 \\ 0 & -i \end{smallmatrix})$.

Ототожнимо поле дійсних чисел \mathbb{R} з підкільцем матриць у \mathbb{H} вигляду $(\begin{smallmatrix} a & 0 \\ 0 & a \end{smallmatrix})$ за допомогою відображення $a \mapsto (\begin{smallmatrix} a & 0 \\ 0 & a \end{smallmatrix})$. Зрозуміло, що це відображення суму (добуток) дійсних чисел переводить у суму (добуток) відповідних їм матриць. Введемо позначення

$$\mathbf{id} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \mathbf{i} = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \quad \mathbf{j} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad \mathbf{k} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

У цих позначеннях маємо, враховуючи ототожнення $a = (\begin{smallmatrix} a & 0 \\ 0 & a \end{smallmatrix})$, $(\begin{smallmatrix} u & v \\ -v & u \end{smallmatrix}) = a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}$, де $u = a + bi$, $v = c + di$. Безпосереднім обчисленням перевіряється, що

$$\begin{aligned} \mathbf{i}^2 &= \mathbf{j}^2 = \mathbf{k}^2 = -1, \\ \mathbf{ij} &= \mathbf{k}, \quad \mathbf{ji} = -\mathbf{k}, \quad \mathbf{jk} = \mathbf{i}, \quad \mathbf{kj} = -\mathbf{i}, \quad \mathbf{ki} = \mathbf{j}, \quad \mathbf{ik} = -\mathbf{j}. \end{aligned} \tag{6.2.1}$$

Кватерніон $\bar{x} = a - bi - cj - dk$ називають *спряженим* до кватерніона $x = a + bi + cj + dk$. Перемножаючи кватерніони x і \bar{x} , з врахуванням властивостей (6.2.1), або, що легше, використовуючи матричний запис кватерніонів, одержуємо $x\bar{x} = \bar{x}x = a^2 + b^2 + c^2 + d^2$. Добуток $\bar{x}x$ позначають $N(x)$ і називають *нормою* кватерніона x . Можна перевірити, що $N(xy) = N(x)N(y)$. Крім того, ясно, що для ненульового кватерніона x маемо $x \cdot \frac{\bar{x}}{N(x)} = \frac{\bar{x}}{N(x)} \cdot x = 1$, отже, $x^{-1} = \frac{\bar{x}}{N(x)}$.

ж) Скручені ряди Лорана. Множина скручених рядів Лорана служить ще одним прикладом некомутативного тіла. Розглянемо відображення $\sigma: \mathbb{C} \rightarrow \mathbb{C}$, для якого $\sigma(x) = \bar{x}$ ((\cdot) означає комплексне спряження, $\sigma^t = \underbrace{\sigma \circ \dots \circ \sigma}_{t \text{разів}}$, де \circ означає добуток відображень); зрозуміло,

що

$$\sigma^t(x) = \begin{cases} x, & t \text{ — парне,} \\ \bar{x}, & t \text{ — непарне.} \end{cases}$$

Розглянемо множину $\mathbb{C}((x, \tau))$ всіх формальних рядів $\sum_{k \geq n} x^k a_k$, де $n \in \mathbb{Z}$, $a_k \in \mathbb{C}$ для всіх $k \geq n$. Рівність рядів визначається за правилом $\sum_{k \geq n} x^k a_k = \sum_{k \geq m} x^k b_k$, якщо $a_k = b_k$ для всіх $k \geq \min\{m, n\}$ і $a_k = 0$ для $n \leq k < \min\{m, n\}$, а також $b_k = 0$ для $m \leq k < \min\{m, n\}$ (якщо $m < n$). Таким чином, для довільної скінченної множини елементів $\mathbb{C}((x, \tau))$ можна вважати, що їх записи починаються з одного і того ж n . Додавання рядів означимо покомпонентно:

$$\sum_{k \geq n} x^k a_k + \sum_{k \geq n} x^k b_k = \sum_{k \geq n} x^k (a_k + b_k).$$

Множення рядів означимо, виходячи з умови $(x^k a)(x^t b) = x^{k+t} \sigma^t(a)b$ і тоді

$$\sum_{k \geq n} x^k a_k \cdot \sum_{k \geq m} x^k b_k = \sum_{k \geq m} x^k c_k,$$

де $c_k = \sum_{i+j=k} \sigma^j(a_i)b_j$. Безпосередня перевірка показує, що $\mathbb{C}((x, \tau))$ відносно введених операцій додавання і множення є тілом, яке називають *тілом скрученых рядів Лорана*. (Пропонуємо читачеві перевірити це в якості вправи.)

з) Приклад неасоціативного кільця. Множина 3-вимірних векторів з дійсними координатами із звичайним додаванням та векторним множенням в якості добутку.

6.3 Гомоморфізми та ізоморфізми

Нехай $\{R, +, \cdot\}$ — кільце і $\{S, +, \cdot\}$ — алгебраїчна структура з двома бінарними алгебраїчними операціями (“додавання” і “множення”). Відображення $\phi: R \rightarrow S$ назовемо *гомоморфізмом*, якщо

$$\phi(a + b) = \phi(a) + \phi(b), \quad \phi(a \cdot b) = \phi(a) \cdot \phi(b)$$

для довільних $a, b \in R$. ϕR назовемо гомоморфним образом кільця R відносно гомоморфізму ϕ .

Твердження 49. *Гомоморфний образ кільця є кільцем.*

Доведення твердження очевидне в силу того факту, що гомоморфний образ напівгрупи (групи) є знову напівгрупою (групою). Оскільки гомоморфний образ моноїда є знову моноїдом, то очевидно, що коли R має одиницю, то її відповідає одиниця кільця ϕR . Якщо R — комутативне кільце, то ϕR — теж комутативне кільце. Зазначимо, що коли R — кільце без дільників нуля, то ϕR не обов'язково є кільцем без дільників нуля і навпаки — кільце R може мати дільники нуля, а ϕR може їх не мати.

Одним з прикладів гомоморфізму є відображення кільця діагональних матриць другого порядку над полем дійсних чисел в поле дійсних чисел, заданий умовою: $\phi \left(\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \right) = a$.

Біективний гомоморфізм кілець назовемо *ізоморфізмом*, і той факт, що між кільцями $\{R, +, \cdot\}$ і $\{S, +, \cdot\}$ існує ізоморфізм, позначимо $R \cong S$.

Нехай R і S — кільца і ϕ — гомоморфізм R в S . Якщо $\phi R = S$, тоді ϕ називається *епіморфізмом* кільця R в S . Гомоморфізм ϕ кільця R в кільце S назовемо *мономорфізмом*, якщо ϕ — ін'єктивне відображення.

6.4 Вкладення кільця в кільце з одиницею

Для довільного кільця R існує кільце з одиницею R^1 і мономорфізм ϕ кільця R в R^1 . Кільце R^1 визначимо, як множину пар (a, m) , де $a \in R$, $m \in \mathbb{Z}$, а операцію означимо наступним чином:

$$(a, n) + (b, m) = (a + b, n + m), \quad (a, n) \cdot (b, m) = (ab + ma + nb, nm).$$

Стандартна перевірка, зробити яку пропонуємо читачеві в якості вправи, показує, що відносно введених операцій додавання і множення R^1 є кільцем з одиницею (одиницею є пара $(0, 1)$). Мономорфізм ϕ означається так: $\phi(a) = (a, 0)$ для довільного $a \in R$.

6.5 Прямі добутки та прямі суми кілець

Нехай \mathcal{I} — довільна множина, $\{R_i\}_{i \in \mathcal{I}}$ — родина кілець. *Зовнішнім прямим добутком* кілець R_i називають множину всіх відображень

$$f: \mathcal{I} \rightarrow \bigcup_{i \in \mathcal{I}} R_i$$

з множини \mathcal{I} в об'єднання множин R_i таких, що $f(i) \in R_i$. Прямий добуток кілець позначають $\prod_{i \in \mathcal{I}} R_i$. На множині $\prod_{i \in \mathcal{I}} R_i$ визначають операції додавання і множення:

$$(f + g)(i) \stackrel{\text{df}}{=} f(i) + g(i), \quad (f \cdot g)(i) \stackrel{\text{df}}{=} f(i)g(i).$$

Легко перевірити, що $\prod_{i \in \mathcal{I}} R_i$ є кільцем відносно цих операцій. Познавши $f(i) = f_i \in R_i$, елементи прямого добутку можна ототожнити з нескінченною рядками (\dots, f_i, \dots) . З означення операцій в прямому добутку випливає, що такі рядки додаються і перемножуються покомпонентно:

$$\begin{aligned} (\dots, f_i, \dots) + (\dots, g_i, \dots) &= (\dots, f_i + g_i, \dots), \\ (\dots, f_i, \dots) \cdot (\dots, g_i, \dots) &= (\dots, f_i g_i, \dots). \end{aligned}$$

Підкільце S кільця $R = \prod_{i \in \mathcal{I}} R_i$, що складається з усіх таких рядків, у яких майже всі елементи дорівнюють нулеві називається *прямою (зовнішньою) сумою* кілець R_i .

Якщо множина \mathcal{I} скінчена, то поняття прямого добутку та прямої суми збігаються: в обох випадках це множина

$$\{(a_1, a_2, \dots, a_n) \mid a_i \in R_i, 1 \leq i \leq n\}$$

з покомпонентними додаванням і множенням. Пряма сума (прямий добуток) кілець R_1, \dots, R_n позначається $R_1 \oplus \dots \oplus R_n$,

Зауважимо, що прямі добутки і прямі суми зв'язані з ідемпотентами. Так кільце \mathbb{Z} не має нетривіальних ідемпотентів, але в прямій сумі $\mathbb{Z} \oplus \mathbb{Z}$ є нетривіальні ідемпотенти $(1, 0)$ і $(0, 1)$.

Навпаки, вірне таке твердження.

Твердження 50. Якщо в комутативному кільці з 1 існує нетривіальний ідемпотент, то R розкладається в пряму суму підкілець.

Доведення. Нехай e — нетривіальний ідемпотент. Розглянемо підмножину $eR = \{ea \mid a \in R\}$. Маємо $ea + eb = e(a + b)$, $ea \cdot eb = e^2ab = eab$ і $-ea = e(-a)$. Тому з критерію підкільця (тврдження 48) випливає, що eR — підкільце. Далі, $(1 - e)^2 = 1 - 2e + e^2 = 1 - 2e + e = 1 - e$, отже, $1 - e$ — теж ідемпотент і за доведеним $(1 - e)R$ — теж підкільце кільця R . З рівності $1 = e + (1 - e)$ випливає, що для кожного елемента $a \in R$ маємо $a = ea + (1 - e)a$.

Розглянемо відображення $\phi: R \rightarrow eR \oplus (1 - e)R$, $\phi(a) = (ea, (1 - e)a)$. Очевидно, ϕ сюр'єктивне. Якщо $\phi(a) = \phi(b)$, то $ea = eb$ і $a - ea = b - eb$, звідки $a = b$. Отже, ϕ ін'єктивне, а тому бієктивне.

Переконаємося, нарешті, що ϕ переводить суму (добуток) елементів в суму (добуток) їх образів: $\phi(a + b) = (ea + b, (1 - e)(a + b)) = (ea, (1 - e)a) + (eb, (1 - e)b) = \phi(a) + \phi(b)$ і $\phi(ab) = (eab, (1 - e)ab) = (e^2ab, (1 - e)^2ab) = (ea, (1 - e)a) \cdot (eb, (1 - e)b) = \phi(a)\phi(b)$. Це означає, що кільце R отожнюється (точніше кажучи, ізоморфне) з прямою сумою кілець eR та $(1 - e)R$. \square

7 Ідеали та фактор кільця

7.1 Означення ідеалів. Головні та скінченно породжені ідеали

Нехай R довільне кільце. Серед підкілець особливу роль грають підкільця, які називаються ідеалами: їх роль аналогічна ролі нормальних підгруп в теорії груп.

Означення 51. Непорожня підмножина I кільця R називається *правим (лівим) ідеалом*, якщо вона задовольняє умовам:

- $i_1 - i_2 \in I$ для довільних $i_1, i_2 \in I$;
- $ir \in I$ ($ri \in I$) для довільних $i \in I, r \in R$.

Аналогично, непорожня підмножина I кільця R називається *лівим ідеалом*, якщо:

а) $i_1 - i_2 \in I$ для довільних $i_1, i_2 \in I$;

б) $ri \in I$ для довільних $i \in I, r \in R$.

Непорожню підмножину I кільця R , яка є одночасно лівим і правим ідеалом R , назовемо *двобічним ідеалом* кільця R , або скорочено *ідеалом Кільця R* . У випадку комутативного кільця ці три поняття (правий (лівий) ідеал та ідеал), очевидно, зводяться до одного.

Кожен (лівий, правий) ідеал кільця R є, очевидно, підкільцем в R .

Твердження 52. *Кожниий (лівий, правий) ідеал кільця R є його підкільцем.*

Доведення. Якщо I , наприклад, лівий ідеал і $a, b \in I$, то $0 = a - a \in I$, отже, $-b = 0 - b \in I$, тому $a + b \in I$; $ab \in I$ за означенням ідеалу. Отже, I задовільняє умовам критерію підкільця (тврдження 48). \square

Зauważення 53. Обернене твердження невірне: \mathbb{Z} є підкільцем поля \mathbb{Q} , але \mathbb{Z} не є ідеалом в \mathbb{Q} .

Приклади. Ясно, що тривіальні підкільця (а саме $\{0\}$ і R) кільця R є завжди ідеалами (тривіальними ідеалами) кільця R . Ідеал I кільця називається *нетривіальним*, якщо $I \neq (0)$ і $I \neq R$. Ідеалом кільця цілих чисел є, наприклад, кільце парних чисел. Діагональні матриці другого порядку з дійсними елементами утворюють підкільце, але не ідеал, в кільці матриць другого порядку над полем дійсних чисел. Серед прикладів ідеалів особливу роль відіграють ідеали, породжені елементом, а саме: правим ідеалом, породженим елементом $a \in R$ називається множина $(a)_r = \{ar + na \mid r \in R, n \in \mathbb{Z}\}$. Аналогічно означається лівий ідеал, породжений елементом a , $(a)_l = \{ra + na \mid r \in R, n \in \mathbb{Z}\}$. Легко переконатися, що множина $(a)_r$ справді є правим ідеалом: $r_1a + n_1a - (r_2a + n_2a) = (r_1 - r_2)a + (n_1 - n_2)a \in (a)_l$ і якщо $s \in R$, то $(ar + na)s = a(rs) + n(as) \in (a)_l$. Правий ідеал $(a)_r$ ї, очевидно, найменшим правим ідеалом, який містить a , а тому $(a)_r$ можна визначити як перетин всіх правих ідеалів, що містять елемент a .

Якщо кільце R є кільцем з одиницею, то $ar + na = ar + n1 \cdot a = a(r + n \cdot 1) = ar'$, де $r' \in R$. Тобто у цьому випадку $(a)_r = aR = \{ar \mid r \in R\}$.

Правий ідеал, породжений одним елементом a , називається *головним правим ідеалом*. Аналогічно означають *головний лівий ідеал*.

Знайдемо всі ідеали кільця цілих чисел. В силу наведених вище міркувань, ідеалами в \mathbb{Z} є головні ідеали $a\mathbb{Z}$, де $a \in \mathbb{Z}$. Оскільки ідеал — це підгрупа відносно операції додавання, а всі підгрупи циклічної групи циклічні, то правильне і обернене твердження, тобто ідеалами $a\mathbb{Z}$ вичерпуються всі ідеали кільця \mathbb{Z} .

Не слід думати, що в кільцях є лише головні ідеали. Так, наприклад, в кільці многочленів $P[X, Y]$ від двох змінних X, Y над полем P , ідеал I , який складається з многочленів без вільного члена, не є головним. Якби I був головним, то він складався б з усіх многочленів, які діляться на деякий фіксований многочлен f_0 . Значить, на нього діляться многочлени X і Y , але у них спільними дільниками є лише константи, яких в I немає.

У кільці $M_n(\mathbb{R})$, $n > 1$, підмножина матриць з нульовим i -им рядком є правим (але не лівим) ідеалом. Так само, підмножина матриць з нульовим j -им стовпчиком є лівим (але не правим) ідеалом.

Означення 54. Правим ідеалом $(a_1, \dots, a_m)_r$ кільця R , породженим елементами a_1, \dots, a_m , називають сукупність всіх сум

$$\sum_{i=1}^m a_i r_i + \sum_{j=1}^m n_j a_j,$$

де $r_i \in R$, $n_j \in \mathbb{Z}$. У випадку кільця з одиницею цей правий ідеал є множиною $\{\sum_{i=1}^m a_i r_i \mid r_i \in R\}$ і позначається $a_1 R + \dots + a_m R$. Він є перетином всіх правих ідеалів, які містять елементи a_1, a_2, \dots, a_m . Цей ідеал називається *скінченнопородженим правим ідеалом*, породженим елементами a_1, a_2, \dots, a_m . Так само означаються скінченнопороджені ліві ідеали.

7.2 Ідеали в полі

Нехай R — комутативне кільце з одиницею.

Твердження 55. Якщо в ідеалі I кільця R є обертовні елементи, то $I = R$.

Доведення. Якщо ідеал I містить елемент a , для якого існує такий елемент b , що $ab = 1$, то $1 \in I$, і для довільного $r \in R$ маємо $r = r \cdot 1 \in I$, тобто $R \subset I$, отже, $I = R$. \square

Твердження 56. Комутативне кільце з одиницею є полем тоді і тільки тоді, коли всі його ідеали тривіальні.

Доведення. Необхідність очевидна в силу твердження 55. Навпаки, нехай всі ідеали кільця R тривіальні, тоді для довільного ненульового елемента a ідеал aR співпадає з R . Звідси $1 \in aR$, тобто існує таке b , що $1 = ab$, що й потрібно було довести. \square

7.3 Фактор-кільця

Нехай I — ідеал в кільці R . За твердженням 52 I — підкільце в R , зокрема, I — підгрупа адитивної групи кільця R . Під розбиттям кільця R за ідеалом I ми розуміємо розбиття адитивної групи R на суміжні класи $\bar{a} \stackrel{\text{df}}{=} a + I$.

Якщо $R = \bigcup(a + I)$ — розбиття кільця R на суміжні класи за ідеалом I , то це розбиття узгоджене з операціями і на фактор-множині операції можна задати так:

$$(a + I) + (b + I) = (a + b) + I, \quad (a + I)(b + I) = ab + I,$$

або, позначивши $a + I \stackrel{\text{df}}{=} \bar{a}$,

$$\bar{a} + \bar{b} = \overline{a + b}, \quad \bar{a} \cdot \bar{b} = \overline{ab}. \quad (7.3.1)$$

Легко перевірити, що фактор-множина множини R , елементами якої є суміжні класи $\bar{a} = a + I$ є кільцем відносно операцій (7.3.1). Це кільце називають *фактор-кільцем* кільця R за ідеалом I і позначають R/I .

Дуже важливими прикладами фактор-кілець є кільця класів лишків, які вивчалися в курсі алгебри і теорії чисел (І семестр). Зокрема, у І семестрі було доведено, що кільце $\mathbb{Z}/n\mathbb{Z}$ є полем тоді й лише тоді, коли n — просте число. Наведемо ще один варіант доведення цього факту. Якщо p — просте число, то з наслідку до теореми Лагранжа випливає, що група $\mathbb{Z}/p\mathbb{Z}$ має лише тривіальні підгрупи, отже, кільце $\mathbb{Z}/p\mathbb{Z}$ має лише тривіальні ідеали, тому за твердженням 56 $\mathbb{Z}/p\mathbb{Z}$ є полем. Навпаки, якщо p не просте число, то $p = p_1 p_2$, де $p_1 < p$, $p_2 < p$. Звідси $\bar{0} = \bar{p} = \bar{p}_1 \cdot \bar{p}_2$, де $\bar{p}_1 \neq 0$ і $\bar{p}_2 \neq 0$. Отже, в $\mathbb{Z}/p\mathbb{Z}$ існують дільники нуля і тому воно не може бути полем.

Зауважимо, що коли R комутативне кільце, то і всі фактор-кільця R/I кільця R комутативні. Якщо R кільце з 1, то і фактор-кільце R/I має одиничний елемент $\bar{1} = 1 + I$. Але, якщо R кільце без дільників нуля, то, як видно з попереднього абзацу, фактор-кільце кільця R може мати дільники нуля.

7.4 Теореми про гомоморфізм

Фактор-кільця та ідеали тісно пов'язані з гомоморфізмами кілець. Перш за все, якщо I — ідеал кільця R , то визначене природне відображення

$$\phi: K \rightarrow K/I, \quad (7.4.1)$$

для якого $\phi(a) = a + I = \bar{a}$. Дуже легка перевірка показує, що ϕ — гомоморфізм. Справді, використовуючи означення (7.3.1) операцій у фактор-кільці, маємо $\phi(a + b) = \overline{a + b} = \bar{a} + \bar{b} = \phi(a) + \phi(b)$ і $\phi(ab) = \overline{ab} = \bar{a} \cdot \bar{b} = \phi(a)\phi(b)$. Гомоморфізм (7.4.1) називають *канонічним* або *природним* гомоморфізмом.

Нехай тепер $f: R_1 \rightarrow R_2$ — гомоморфізм кілець. Ми вже знаємо (тврдження 49), що $\text{Im } f$ — підкільце кільця R_2 . Множину $\text{Ker } f = \{a \in R \mid f(a) = 0\}$ називають *ядром гомоморфізму*.

Твердження 57. $\text{Ker } f$ — ідеал кільця R_1 .

Доведення. Якщо $a, b \in \text{Ker } f$, то $f(a - b) = f(a) - f(b) = 0 - 0 = 0$, отже, $a - b \in \text{Ker } f$. Нехай r — довільний елемент кільця R_1 . Тоді $\phi(ar) = \phi(a)\phi(r) = 0 \cdot \phi(r) = 0 = \phi(r) \cdot 0 = \phi(r)\phi(a) = \phi(ra)$. Отже, $\text{Ker } \phi$ — ідеал. \square

Твердження 58. Гомоморфізм кілець $f: R_1 \rightarrow R_2$ є мономорфізмом тоді і тільки тоді, коли $\text{Ker } \phi = 0$.

Доведення. Якщо f — мономорфізм, то оскільки $f(0) = 0$, повинно бути $f(a) \neq 0$ для $a \neq 0$. Навпаки, якщо $\text{Ker } f = 0$ і $f(a) = f(b)$, то $f(a - b) = 0$, отже $a - b \in \text{Ker } f$, тому $a - b = 0$, тобто $a = b$. \square

Зауважимо, що фактор-кільце R/I є образом кільця R при канонічному гомоморфізмі ϕ , а ядро канонічного гомоморфізму збігається з ідеалом I . Отже, кожний ідеал є ядром деякого гомоморфізму (а саме, канонічного). Покажемо тепер, що кожний гомоморфний образ кільця є, по суті, деяким фактор-кільцем, тобто фактор-кільцями кільця R вичерпуються всі гомоморфні образи кільця R .

Теорема 59. Нехай $f: R \rightarrow R'$ — гомоморфізм кілець. Тоді існує ізоморфізм кілець

$$\bar{f}: R/\text{Ker } f \cong \text{Im } f.$$

Доведення. Означимо \bar{f} так: $\bar{f}(\bar{a}) = f(a)$. По-перше, \bar{f} коректно означене відображення, бо якщо $\bar{a}_1 = \bar{a}_2$, то $a_1 - a_2 \in \text{Ker } f$, отже, $0 = f(a_1 - a_2) = f(a_1) - f(a_2)$ і $f(a_1) = f(a_2)$, тобто $\bar{f}(\bar{a}_1) = \bar{f}(\bar{a}_2)$.

По-друге, \bar{f} — гомоморфізм: $\bar{f}(\bar{a} + \bar{b}) = \bar{f}(\overline{a+b}) = f(a+b) = f(a) + f(b) = \bar{f}(\bar{a}) + \bar{f}(\bar{b})$, і така сама перевірка для добутку.

І по-третє, \bar{f} — біективне відображення. Справді, сюр'ективність \bar{f} випливає з його означення. Знайдемо $\text{Ker } \bar{f}$: $\text{Ker } \bar{f} = \{\bar{a} \mid \bar{f}(\bar{a}) = 0\} = \{\bar{a} \mid f(a) = 0\} = \{\bar{0}\}$, тому з твердження 58 випливає, що \bar{f} — мономорфізм. Теорему доведено. \square

Наслідок 60. Нехай $I_1 \subset I_2$ — ідеали кільця R . Тоді I_1 — ідеал кільця I_2 , I_2/I_1 — ідеал кільця R/I_1 і існує ізоморфізм $R/I_1/I_2/I_1 \cong R/I_2$.

Доведення. Легко бачити, що I_1 — ідеал кільця I_2 . Розглянемо відображення фактор-кілець $g: R/I_1 \rightarrow R/I_2$, $g(a+I_1) = a+I_2$. Легко переконатися в тому, що g — коректно означений сюр'ективний гомоморфізм. Знайдемо ядро гомоморфізму g :

$$\text{Kerg} = \{a+I_1 \mid a+I_2 = I_2\} = \{a+I_1 \mid a \in I_2\} = I_2/I_1.$$

За твердженням 57 $\text{Kerg} = I_2/I_1$ — ідеал кільця R/I_1 , за теоремою 59 $R/I_1/\text{Kerg} \cong \text{Img} = R/I_2$. \square

7.5 Основні операції над ідеалами

Означення 61. Нехай I_1 та I_2 — ідеали кільця R . Означимо їх перетин, суму та добуток:

$I_1 \cap I_2$ — перетин множин I_1 та I_2 ,

$I_1 + I_2 \stackrel{\text{df}}{=} \{a+b \mid a \in I_1, b \in I_2\}$,

$I_1 I_2 \stackrel{\text{df}}{=} \{\sum_{i=1}^n a_i b_i \mid a_i \in I_1, b_i \in I_2, n \in \mathbb{N}\}$ — множина всіх скінчених сум, доданками яких є добутки елементів з ідеалів I_1 та I_2 .

Твердження 62. Якщо I_1 та I_2 — ідеали кільця R , то $I_1 \cap I_2$, $I_1 + I_2$, $I_1 I_2$ — теж ідеали кільця R .

Доведення. Доведемо, що добуток $I_1 I_2$ є ідеалом. Очевидно, що сума двох елементів $\sum_{i=1}^n a_i b_i$ та $\sum_{i=1}^{n'} a'_i b'_i$ є знову елементом з $I_1 I_2$. Далі, якщо $c \in R$, то $c(\sum_{i=1}^n a_i b_i) = \sum_{i=1}^n c(a_i)b_i \in I_1 I_2$, бо $c a_i \in I_1$. Так само і $(\sum_{i=1}^n a_i b_i)c \in I_1 I_2$.

Пропонуємо читачеві самостійно переконатися в тому, що $I_1 \cap I_2$ та $I_1 + I_2$ є ідеалами. \square

7.6 Прості і максимальні ідеали

Означення 63. Ідеал P комутативного кільця R називають простим, якщо з умов $a \notin P$ і $b \notin P$ випливає, що $ab \notin P$ (або, що рівносильно, з $ab \in P$ випливає $a \in P$ або $b \in P$).

Твердження 64. Власний ідеал P комутативного кільця R є простим тоді і тільки тоді, коли R/P – кільце без дільників нуля.

Доведення. Нехай P – простий ідеал, а R/P – кільце з дільниками нуля, тобто існують елементи $\bar{a} \neq \bar{0}$, $\bar{b} \neq \bar{0}$, $\bar{a}, \bar{b} \in R/P$, що $\bar{a} \cdot \bar{b} = \bar{0}$. Враховуючи означення фактор-кільця, бачимо, що умови $\bar{a} \neq \bar{0}$, $\bar{b} \neq \bar{0}$ означають не що інше, як $a \notin P$, $b \notin P$. А умова $\bar{a} \cdot \bar{b} = \bar{0}$, означає, що $ab \in P$. Звідси бачимо, що в R існують елементи $a \notin P$, $b \notin P$ такі, що $ab \in P$, що суперечить простоті ідеалу P .

Навпаки, нехай R/P – кільце без дільників нуля і $ab \in P$, тобто $\bar{a} \cdot \bar{b} = \bar{0}$ в R/P . Звідси $\bar{a} = \bar{0}$ або $\bar{b} = \bar{0}$, тобто $a \in P$ або $b \in P$. \square

Приклад. Якщо p – просте число, то $p\mathbb{Z}$ є простим ідеалом в кільці \mathbb{Z} .

Означення 65. Ідеал M комутативного кільця R називається *максимальним*, якщо якщо він не міститься в жодному власному ідеалі кільця R .

Твердження 66. Коєсен відмінний від R максимальний ідеал M комутативного кільця з одиницею є простим і кільце R/M є полем. Навпаки, якщо R/M поле, то M максимальний ідеал.

Доведення. Нехай M – максимальний ідеал комутативного кільця R з одиницею. Нехай $a \notin M$, розглянемо ідеал $M + aR$. Очевидно $M \subset M + aR$, а тому що $a \notin M$, то $M \neq M + aR$. З максимальності M випливає, що $M + aR = R$. Тому існують елементи $m \in M$, $r \in R$, що $m + ar = 1$. Очевидно, що $r \notin M$, бо у протилежному випадку $M = R$. Застосовуючи природний гомоморфізм з R в R/M , маємо $\bar{m} + \bar{a} \cdot \bar{r} = \bar{1}$. Звідси $\bar{a} \cdot \bar{r} = \bar{1}$; отже, показано, що для довільного ненульового елемента $\bar{a} \in R/M$ існує $\bar{r} \in R/M$, що $\bar{a} \cdot \bar{r} = \bar{1}$, тобто R/M поле. З твердження 64 випливає, що M простий ідеал в R .

Навпаки, якщо R/M – поле, P – власний ідеал, який містить M , і $a \in P \setminus M$, то рівняння $\bar{a} \cdot \bar{x} = \bar{1}$ має розв'язок в R/M . Це означає, що існують $r \in R$ і $m \in M$ такі, що $1 = ar - m \in P$. Тому $P = R$. Твердження доведено. \square

Однак не кожен простий ідеал є максимальним, зокрема, в кільці цілих чисел ідеал (0) є простим, але не максимальним, бо він міститься в кожному власному ідеалі $n\mathbb{Z}$ кільця \mathbb{Z} . Покажемо, що в довільному кільці з одиницею існують максимальні ідеали.

Теорема 67 (Крулля). *В кожному кільці з одиницею існують максимальні ідеали.*

Доведення. Множина A всіх власних ідеалів кільця R є частково впорядкованою відносно звичайного теоретико-множинного включення ідеалів. Нехай $\{I_\alpha\}_{\alpha \in \Lambda}$ — довільна лінійно впорядкована підмножина множини A . Розглянемо $I = \bigcup_{\alpha \in \Lambda} I_\alpha$. Очевидно, що I — ідеал в R . $I \neq R$, бо у протилежному випадку існує $\alpha \in \Lambda$, що $1 \in I_\alpha$, тобто $I_\alpha = R$, що суперечить виборові ідеалів I_α . Отже, множина A є індуктивною. За лемою Цорна в A існує максимальний елемент, який, очевидно, є максимальним ідеалом. Це завершує доведення теореми. \square

7.7 Теорема Коена

В деяких класах кілець структура простих ідеалів цілком визначає структуру всіх ідеалів кільця. Як ілюстрацію, наведемо дві теореми Коена.

Теорема 68 (перша теорема Коена). *Комутативне кільце з одиницею є кільцем, в якому кожний ідеал головний тоді і тільки тоді, коли кожний його простий ідеал головний.*

Доведення. Нехай в кільці R існують ідеали, які не є головними і нехай F — множина таких ідеалів. Доведемо, що F — індуктивна за включенням, тобто, якщо $\{I_\alpha\}_{\alpha \in \Lambda}$ — лінійно впорядкована за включенням множина елементів із F , то $I = \bigcup_{\alpha \in \Lambda} I_\alpha \in F$. Якби це було не так, тобто $I = aR$ — головний ідеал, то існував би такий індекс $\alpha \in \Lambda$, що $a \in I_\alpha$, а значить $aR \subset I_\alpha$. Але $I_\alpha \subset I$, тому $aR = I_\alpha$, що неможливо, бо $I_\alpha \in F$. Згідно леми Цорна існує максимальний елемент N в F . Оскільки $N \in F$, то N — не головний ідеал. Покажемо, що N простий ідеал в R . Якщо б це не було не так, то в R існували б елементи $a \notin N$, $b \notin N$, що $ab \in N$. З максимальності N із $N \subset N + aR$, $N \neq N + aR$, випливає, що ідеал $N + aR = cR$ — головний. Нехай $K = \{r \mid rc \in N\}$. Очевидно, що K — ідеал в R , причому $b \in K$ і $N \subset K$, $N \neq K$. Звідси $K = dR$. Твердимо, що тоді $N = cdR$. В силу означення K маємо $dc \in N$, а значить $cdR \subset N$. Оскільки $N \subset cR$, то для довільного $m \in N$ маємо $m = cx$, $x \in R$. Оскільки $m \in N$, то $x \in K$, тобто $x = dy$, $y \in R$. Отже, $N = cdR$, що неможливо, бо $N \in F$. Отримана суперечність показує, що N — простий

ідеал кільця R , що неможливо, бо в R всі прості ідеали головні. Теорему доведено. \square

Теорема 69 (Друга теорема Коена). У комутативному кільці з одиницею коєсен ідеал є скінченнопородженим тоді й лише тоді, коли коєсен простий ідеал є скінченнопородженим.

Доведення. Нехай в кільці R існують ідеали, які не є скінченнопородженими і нехай F — множина таких ідеалів. Так само, як і в доведенні першої теореми Коена, показуємо існування максимальних в F ідеалів. Нехай N — довільний максимальний в F ідеал. Покажемо, що N — простий ідеал. Якщо б це було не так, то в R існували б такі елементи $a \notin N$, $b \notin N$, що $ab \in N$. В силу означення N і того, що $b \notin N$ б ідеал $N + bR$ скінченнопороджений, тобто $N + bR = \sum_{i=1}^k (n_i + br_i)R$, де $n_i \in N$. Множина $J = \{x \mid bx \in N\}$ є ідеалом в R . Крім цього $N \subset J$ і $N \neq J$, бо $a \in J$ і $a \notin N$. Тому $J = \sum_{i=1}^t s_i R$.

Оскільки $N \subset N + bR$, то для довільного $m \in N$ маємо

$$m = \sum_{i=1}^k (n_i + br_i)x_i = \sum_{i=1}^k n_i x_i + b \sum_{i=1}^k r_i x_i.$$

Звідси $m - \sum_{i=1}^k n_i x_i = b \sum_{i=1}^k r_i x_i \in N$, тобто $\sum_{i=1}^k r_i x_i \in J$. Оскільки $J = \sum_{i=1}^t s_i R$, то $\sum_{i=1}^k r_i x_i = \sum_{i=1}^t s_i y_i$ для деяких $y_i \in R$ ($i = 1, 2, \dots, t$). Отже, $m = \sum_{i=1}^k n_i x_i + b \sum_{i=1}^t s_i y_i$. Оскільки m — довільний елемент N , то ми маємо включення $N \subset \sum_{i=1}^k n_i R + \sum_{i=1}^t b s_i R$. За означенням ідеалу J , маємо $s_i \in J$ ($i = 1, \dots, t$), тобто $b s_i \in N$ для довільного $i = 1, \dots, t$. Звідси $\sum_{i=1}^t b s_i R \subset N$. Оскільки $n_i \in N$ ($i = 1, \dots, k$), то $\sum_{i=1}^k n_i R \subset N$. Отже, $\sum_{i=1}^k n_i R + \sum_{i=1}^t b s_i R \subset N$, тобто $N = \sum_{i=1}^k n_i R + \sum_{i=1}^t b s_i R$, що суперечить тому, що $N \in F$. Оскільки в R довільний простий ідеал є скінченнопородженим, то з попередніх міркувань випливає, що множина F порожня, тобто всі ідеали кільця R є скінченнопородженими, що доводить теорему. \square

8 Вкладення кілець в поля. Локалізація та класичне кільце дробів

Оскільки тіло є кільцем без дільників нуля, то зрозуміло, що довільне підкільце поля є теж кільцем без дільників нуля. У частині ??, Розділ ?? було побудоване (для довільного комутативного кільця R з 1 і

без дільників нуля) поле дробів $Q(R)$ кільця R . Поле $Q(R)$ будується з кільця R так само як поле раціональних чисел \mathbb{Q} будується з кільця цілих чисел \mathbb{Z} : поле $Q(R)$ складається з дробів, тобто елементів вигляду $\frac{n}{m}$, де $n, m \in \mathbb{Z}$, $m \neq 0$, причому $\frac{n_1}{m_1} = \frac{n_2}{m_2}$ рівні тоді і тільки тоді, коли $n_1 m_2 = n_2 m_1$ (точніше кажучи, дроби $\frac{n}{m}$ — це суміжні класи фактормноожини $R \times R \setminus \{0\} / \sim$, де $(n_1, m_1) \sim (n_2, m_2)$, якщо $n_1 m_2 = n_2 m_1$). Операції додавання і множення в $Q(R)$ задаються звичайними правилами:

$$\frac{n_1}{m_1} + \frac{n_2}{m_2} = \frac{n_1 m_2 + n_2 m_1}{m_1 m_2}, \quad \frac{n_1}{m_1} \cdot \frac{n_2}{m_2} = \frac{n_1 n_2}{m_1 m_2}.$$

Наша мета тепер — узагальнити цю конструкцію на випадок довільного кільця з 1 (не обов'язково без дільників нуля).

Крім цього, як ми побачимо, схожа конструкція дозволяє вважати задане комутативне кільце підкільцем деякого кільця з єдиним максимальним ідеалом.

8.1 Кільце дробів: єдиність

Нехай R — комутативне кільце з одиницею. Непорожня підмноожина S кільця R називається *мультиплікативно замкненою*, якщо:

- a) для довільних $s_1, s_2 \in S$ завжди $s_1 s_2 \in S$;
- b) $1 \in S$.

Прикладом мультиплікативно замкненої мноожини може служити мноожина всіх регулярних елементів кільця R .

Означення 70. Означимо кільце дробів для R відносно мультиплікативно замкненої мноожини S , як кільце RS^{-1} разом з кільцевим гомоморфізмом $\phi: R \rightarrow RS^{-1}$, що задовольняє умовам:

- 1) $\phi(S)$ — оборотний елемент для довільного $s \in S$;
- 2) довільний елемент RS^{-1} має вигляд $\phi(a)\phi(s)^{-1}$, де $s \in S$, $a \in R$;
- 3) $\phi(a) = 0$ тоді і тільки тоді, коли $as = 0$ для деякого $s \in S$.

Наперед не ясно, чи кільце RS^{-1} існує, а якщо існує, то чи воно визначене однозначно кільцем R та мноожиною S . Відповідь на друге питання дає наступне твердження.

Твердження 71. Якщо кільце дробів RS^{-1} існує, то воно задовольняє наступній універсальній умові: для довільного кільцевого гомоморфізму $\psi: R \rightarrow K$ такого, що $\psi(s)$ є оборотним елементом в K для кожного $s \in S$, існує єдиний гомоморфізм $\sigma: RS^{-1} \rightarrow K$ такий, що $\sigma\phi = \psi$.

Доведення. Означимо σ так: $\sigma(\phi(a)\phi(s)^{-1}) = \psi(a)\psi(s)^{-1}$. Відображення σ коректно означене. Справді, нехай $\phi(a)\phi(s)^{-1} = \phi(b)\phi(t)^{-1}$, де $a, b \in R$, $s, t \in S$. Тоді $\phi(a) = \phi(b)\phi(t)^{-1}\phi(s) = \phi(b)(\phi(t)^{-1}\phi(s)) = \phi(b)\phi(s)\phi(u)^{-1}$ для деяких $c \in R$, $u \in S$, що можливо згідно умови 2). Звідси отримуємо $\phi(a)\phi(u) = \phi(b)\phi(s)$ і $\phi(s)\phi(u) = \phi(t)\phi(s)$.

З умови 3 означення 70 одержимо $aуз = bcz$ і $sуз' = tcz'$ для деяких $z, z' \in S$. Оскільки $\psi(z)$ і $\psi(z')$ оборотні в K , то $\psi(a)\psi(u) = \psi(b)\psi(s)$ і $\psi(s)\psi(u) = \psi(t)\psi(s)$. Звідси $\psi(a) = \psi(b)\psi(s)\psi(u)^{-1}$ і $\psi(a)\psi(s)^{-1} = \psi(b)\psi(s)\psi(u)^{-1}\psi(s)^{-1}$, а також $\psi(s) = \psi(t)\psi(s)\psi(u)^{-1}$, $\psi(t)^{-1}\psi(s) = \psi(s)\psi(u)^{-1}$, $\psi(t)^{-1} = \psi(s)\psi(u)^{-1}\psi(s)^{-1}$. Отже, $\psi(a)\psi(s)^{-1} = \psi(b)\psi(t)^{-1}$. Очевидно, що σ гомоморфізм і $\sigma\phi = \psi$, причому σ визначений днозначно. Твердження доведене. \square

Як наслідок отримаємо теорему:

Теорема 72. *Кільце дробів RS^{-1} визначається умовами 1)–3) означення 70 однозначно з точністю до ізоморфізму.*

Доведення. Якщо K_1 і K_2 — два кільця дробів відносно мультиплікативної множини S і $\phi_1: R \rightarrow K_1$, $\phi_2: R \rightarrow K_2$ — відповідні гомоморфізми, то за твердженням 71 існує єдина пара гомоморфізмів $\sigma_1: K_1 \rightarrow K_2$ і $\sigma_2: K_2 \rightarrow K_1$, для яких $\sigma_1\phi_1 = \phi_2$ і $\sigma_2\phi_2 = \phi_1$. Звідси $\sigma_1\sigma_2\phi_2 = \phi_1$. Знову з твердження 71 випливає, що $\sigma_1\sigma_2 = 1_{K_2}$. Так само, $\sigma_2\sigma_1 = 1_{K_1}$, отже, σ_1 і σ_2 взаємно обернені ізоморфізми. \square

8.2 Існування кілець дробів

Теорема 73. *Нехай R — комутативне кільце з одиницею, а S — мультиплікативно замкнена множина в R . Існує кільце дробів RS^{-1} і воно має вигляд $R \times S / \sim$, де \sim — відношення еквівалентності, визначене наступним способом: $(a, s) \sim (a', s')$, якщо існує таке $t \in R$, що $(as' - a's)t = 0$.*

Доведення. Вказане відношення є відношенням еквівалентності. Справді, очевидно, що воно рефлексивне і симетричне. Воно також транзитивне, бо якщо $(a's - as')t = 0$ і $(a''s' - a's'')t' = 0$, то $(a''s - as'')tt's' = 0$ і $tt's' \in S$. Нехай \bar{R} фактор-множина множини $R \times S$ відносно введеного відношення еквівалентності. Для довільної пари $(a, s) \in R \times S$ позначимо через $\frac{a}{s}$ суміжний клас множини \bar{R} з представником (a, s) .

Наділимо множину \bar{R} структурою кільця. Нехай $x = \frac{a}{s}$ і $y = \frac{b}{t}$ — два елементи множини \bar{R} . Елементи $(at + bs)/ts$ і ab/st залежать тільки від x

і y . Справді, якщо $x = \frac{a'}{s'}$, то існує елемент $r \in S$, що $(as' - a's)r = 0$. Звідси $((at + sb)s't - (a't - bs')st)r = 0$ і $(abs't - a'b)r = 0$. Безпосередня перевірка показує, що операції

$$\frac{a}{s} + \frac{b}{t} = \frac{at + bs}{st}, \quad \frac{a}{s} \cdot \frac{b}{t} = \frac{ab}{st}$$

визначають на \bar{R} структуру комутативного кільця з нульовим елементом $\frac{0}{1}$ і одиницею $\frac{1}{1}$.

Відображення $h: R \rightarrow \bar{R}$, $h(a) = \frac{a}{1}$ є очевидно гомоморфізмом кілець і образ $\frac{s}{1}$ кожного елемента $s \in S$ має в \bar{R} обернений $\frac{1}{s}$. Очевидно, що гомоморфізм h задоволяє умови 1)–3). Теорему доведено. \square

Особливий інтерес становить випадок, коли розглянути множину S_{reg} всіх регулярних елементів кільця R . Очевидно, що S_{reg} мультиплікативно замкнена. Кільце дробів RS_{reg}^{-1} називають *класичним кільцем дробів* і позначають, як правило, $Q_{\text{Cl}}(R)$.

8.3 Локалізація

Якщо P — простий ідеал комутативного кільця R , то множина $R \setminus P$ мультиплікативно замкнена і кільце RS^{-1} позначають через R_P . Відмітимо, що R_P є комутативним кільцем з єдиним максимальним ідеалом $PR_P = \{\frac{p}{s} \mid p \in P, s \in R \setminus P\}$. Справді, якщо $a \notin P$, то $a \in R \setminus P$, а значить $\frac{a}{1}$ оборотний елемент в R_P . Отже, необоротними елементами в R_P є лише елементи $\frac{p}{s}$, де $p \in P$, $s \in R \setminus P$. Оскільки P — простий ідеал, то різниця таких елементів є елементом такого ж вигляду. Отже, ці елементи утворюють ідеал, який, очевидно, є максимальним.

Кільце R_P називають *локалізацією* кільця R за простим ідеалом P .

Комутативне кільце з одиницею з єдиним максимальним ідеалом називають *локальним кільцем*. Ми бачимо, що локалізація комутативного кільця за простим ідеалом є локальним кільцем.

9 Деякі класи кілець з умовами на їх ідеали

9.1 Нетерові та артінові кільца

Як правило, яке-небудь більш-менш задовільне описання того чи іншого класу кілець вдається отримати лише при умові, коли той чи інший ланцюг ідеалів обривається, тобто при певних умовах скінченності. Toчніше, скажемо, що зростаюча послідовність ідеалів $I_1 \subset I_2 \subset \dots \subset I_n \subset$

обривається, якщо існує номер m , такий що $I_m = I_{m+i}$ для довільного i . Скажемо, що спадна послідовність ідеалів $I_1 \supset I_2 \supset \dots \supset I_n \supset \dots$ обривається, якщо існує номер m , такий що $I_m = I_{m+i}$ для довільного i . Комутативне кільце називається *нетеровим*, якщо довільна зростаюча послідовність його ідеалів обривається. Комутативне кільце називається *артіновим*, якщо довільна спадна послідовність його ідеалів обривається. Очевидно, що довільне скінченне кільце (тобто, кільце з скінченною кількістю елементів) є артіновим і нетеровим.

Твердження 74. *Комутативне кільце з одиницею R є нетеровим тоді і тільки тоді, коли кожний його ідеал є скінченнопородженим.*

Доведення. Нехай R — нетерове кільце, I — довільний його ідеал. Якщо існує елемент $a_1 \in I$ з $I = a_1R$, то доведення очевидне. В протилежному випадку існують елементи $a_1, a_2 \in I$, такі що $a_2 \notin a_1R$. Розглянемо ідеал $a_1R + a_2R$; очевидно, що $a_1R \subset a_1R + a_2R$, причому $a_1R \neq a_1R + a_2R$. Якщо $a_1R + a_2R = I$, то все доведено. В протилежному випадку, існує елемент $a_3 \in I$, для якого $a_3 \notin a_1R + a_2R$. В результаті отримуємо ланцюжок ідеалів

$$a_1R \subset a_1R + a_2R \subset a_1R + a_2R + a_3R.$$

Продовжуючи цей процес і враховуючи нетеровість кільця, отримаємо, що існує такий номер n , що $I = a_1R + \dots + a_nR$, тобто I — скінченно породжений ідеал.

Нехай в кільці R довільний ідеал є скінченно породженим, а $I_1 \subset \dots \subset I_n \subset \dots$ — довільний зростаючий ланцюг ідеалів R . Нехай $I = \bigcup I_i$. Очевидно, що I — ідеал в R , тоді $I = a_1R + \dots + a_nR$. Оскільки $a_j \in I$, $j = 1, 2, \dots, n$, то існує ідеал I_j , для якого $a_j \in I_j$. Оскільки ідеали I_j утворюють ланцюг, існує номер m , що $a_1, \dots, a_n \in I_m$, тоді $a_1R + \dots + a_nR \subset I_m$. В силу визначення ідеалу I , маємо $I_m = a_1R + \dots + a_nR$, тобто наш ланцюг ідеалів стабілізується. Твердження доведено. \square

За доведеним твердженням комутативне кільце головних ідеалів є нетеровим. Кільце цілих чисел є нетеровим кільцем, але воно не є артіновим. Прикладом нескінченно спадного ланцюга ідеалів в \mathbb{Z} є ланцюг ідеалів $2\mathbb{Z} \supset 4\mathbb{Z} \supset \dots \supset 2^n\mathbb{Z} \supset \dots$. Проте відомо, що довільне артінове кільце з одиницею є нетеровим (див. [?, Розділ 8]). Прикладом артінового кільця без одиниці, яке не є нетеровим, є кільце з нульовим множенням, адитивною групою якого є квазіциклична група типу p^∞ , де p — просте число, а саме, група, яка є об'єднанням зростаючої послідовності цикліческих підгруп $\langle c_1 \rangle \subset \langle c_2 \rangle \subset \dots \subset \langle c_n \rangle \subset \dots$, де $pc_1 = 0$ і $pc_n = c_{n-1}$, якщо

$n > 1$. Очевидно, що ідеалами в цьому кільці є підгрупи $\langle c_i \rangle$, і довільний спадний ланцюг ідеалів обривається на скінченному кроці, а довільний зростаючий ланцюг не обривається.

9.2 Теорема Гільберта про базу

Теорема Гільберта про базу дозволяє будувати нові класи нетерових кілець за допомогою відомих.

Теорема 75 (Гільберта про базу). *Кільце многочленів над комутативним нетеровим кільцем з одиницею є нетеровим.*

Доведення. Нехай I — ідеал кільця $R[x]$. Для довільного натурального n позначимо через I_n множину елементів $r \in R$, для яких існує многочлен в I з старшим коефіцієнтом rx^n . Легко перевірити, що I_n — ідеал в R і що $I_n \subset I_{n+1}$. Ланцюжок $I_1 \subset I_2 \subset \dots$ обривається на деякому номері n_0 . Нехай $\{a_i\}$ — скінчена множина елементів в кільці R , які породжують ідеал I_i ($i \leq n_0$), і нехай f_{ij} — многочлени в I з старшими коефіцієнтами a_{ij} . Переконаємося, що многочлени f_{n_0j} породжують I .

Якщо в I існують многочлени, які не можна записати як комбінацію f_{ij} , то виберемо серед них многочлен найменшого степеня, наприклад, $g(x) = bx^m + \dots$, тоді $b \in I_m$, і якщо $m \leq n_0$, то в силу визначення ідеала I_{n_0} можна записати $b = \sum_j a_{n_0j} b_j$. Многочлен $g(x) - \sum_j f_{n_0j}(x) b_j$ є многочленом меншого степеня, ніж m . Індукція за степенем дає нам можливість записати його у вигляді комбінації f_{n_0j} , а значить $g(x)$ можна записати у вигляді комбінації f_{n_0j} . Отримана суперечність показує, що многочлени f_{n_0j} породжують I .

Якщо $m > n_0$, то $b = \sum a_{n_0j} b_j$ і, провівши аналогічні міркування для многочлена $g(x) - \sum_j f_{n_0j}(x) x^{m-n_0} b_j$, отримаємо доведення теореми. \square

Як наслідок отримуємо:

Теорема 76. *Кільце многочленів від n змінних над комутативним нетеровим кільцем з одиницею нетерове.*

Не слід думати, що всі комутативні кільця з одиницею є нетеровими. Наприклад, кільце многочленів $R = P[x_1, \dots, x_n, \dots]$ від нескінченної множини змінних над полем P не задовільняє обом умовам артіновості і нетеровості: з одного боку $x_1R \subset x_1R + x_2R \subset \dots$, а з іншого боку $x_iR \supset x_i^2R \supset x_i^3R \supset \dots$

За другою теоремою Коена для того, щоб комутативне кільце з одиницею було нетеровим кільцем, необхідно і досить, щоб довільний простий ідеал кільця був скінченно породженим.

9.3 Топологія Зариського

Мета цього пункту — звернути увагу на те, що теорема Гільберта про базу має застосування до вивчення систем поліноміальних рівнянь.

Означення 77. Нехай K — поле. *Замкненою множиною* в

$$K^n = \underbrace{K \times \cdots \times K}_n$$

називають множину $A \subset K^n$, що складається з елементів $(x_1, \dots, x_n) \in K^n$, які є спільними розв'язками системи рівнянь

$$\begin{cases} f_1(X_1, \dots, X_n) = 0, \\ \dots \dots \dots \\ f_m(X_1, \dots, X_n) = 0. \end{cases} \quad (9.3.1)$$

Доповнення $U = K^n \setminus A$ до замкненої множини A називають *відкритою множиною*.

Твердження 78. 1) Порожня підмножина $\emptyset \subset K^n$ і вся множина K^n є замкненими;

2) Об'єднання скінченної родини замкнених множин є замкненою множиною;

3) Перетин довільної родини замкнених множин є замкненою множиною.

Доведення. 1) Порожня множина є множиною розв'язків рівняння $1 = 0$, а вся множина K^n є множиною розв'язків рівняння $0 = 0$.

2) Досить розглянути випадок об'єднання двох замкнених множин. Якщо замкнена множина A визначена системою рівнянь (9.3.1), замкнена множина B — системою рівнянь

$$\begin{cases} g_1(X_1, \dots, X_n) = 0, \\ \dots \dots \dots \\ g_l(X_1, \dots, X_n) = 0. \end{cases}$$

то множина $A \cup B$ є множиною спільних розв'язків системи ml рівнянь

$$f_i(X_1, \dots, X_n) \cdot g_j(X_1, \dots, X_n) = 0, \quad 1 \leq i \leq m, \quad 1 \leq j \leq l.$$

3) Нехай $\{A_i\}_{i \in I}$ — родина замкнених множин в K^n , і нехай множина A_i визначена системою рівнянь

$$f_{j_i}(X_1, \dots, X_n) = 0, \quad 1 \leq j_i \leq m_i. \quad (9.3.2)$$

Перетин $\bigcap_{i \in J} A_i$ є множиною тих елементів $(x_1, \dots, x_n) \in K^n$, що задовільняють всі системи (9.3.2). Легко зрозуміти, що перетин $\bigcap_{i \in I} A_i$ складається з елементів $(x_1, \dots, x_n) \in K^n$, в яких перетворюються в нуль всі многочлени з ідеалу I , породженого всіма многочленами систем (9.3.2). Оскільки кільце $K[X_1, \dots, X_n]$ нетерове, то цей ідеал I скінченно породжений, наприклад, многочленами $h_1(X_1, \dots, X_n), \dots, h_k(X_1, \dots, X_n)$. Звідси випливає, що $(x_1, \dots, x_n) \in \bigcap_{i \in I} A_i$ тоді і тільки тоді, коли (x_1, \dots, x_n) є розв'язком систем рівнянь

$$\begin{cases} h_1(X_1, \dots, X_n) = 0, \\ \dots \dots \dots \\ h_k(X_1, \dots, X_n) = 0, \end{cases}$$

тобто $\bigcap_{i \in I} A_i$ є замкненою множиною. \square

Наслідок 79. 1) Порожня підмножина $\emptyset \subset K^n$ і вся множина K^n є відкритими множинами;

2) Перетин скінченної родини відкритих множин — відкрита множина;

3) Об'єднання довільної родини відкритих множин є відкритою множиною.

Доведення. 1) безпосередньо випливає з означення та властивості 1) з попереднього твердження.

2) Нехай U_1, U_2 — відкриті множини. Тоді $U_1 = K^n \setminus A_1$, $U_2 = K^n \setminus A_2$, де A_1 і A_2 — замкнені множини. $U_1 \cap U_2 = (K^n \setminus A_1) \cap (K^n \setminus A_2) = K^n \setminus (A_1 \cup A_2)$ — відкрита множина, бо вона є доповненням замкненої множини $A_1 \cup A_2$.

3) Якщо $\{U_i\}_{i \in I}$ — родина відкритих множин, то $U_i = K^n \setminus A_i$, де A_i — замкнені множини. Звідси маємо $\bigcup_{i \in I} U_i = \bigcup_{i \in I} (K^n \setminus A_i) = K^n \setminus (\bigcap_{i \in I} A_i)$ — відкрита множина, бо $\bigcap_{i \in I} A_i$ — замкнена множина. \square

З доведеного наслідку випливає, що відкриті множини задають топологію на множині K^n . Цю топологію називають *топологією Зариського*.

9.4 Кільця Безу

Найближчим класом кілець до комутативних кілець головних ідеалів, які, взагалі кажучи, не є нетеровими кільцями, є кільця Безу.

Комутативне кільце з одиницею називається *кільцем Безу*, якщо кожний скінченнопороджений ідеал цього кільця є головним. Очевидними прикладами кілець Безу є кільця головних ідеалів.

Твердження 80. *Комутативне нетерове кільце Безу є кільцем головних ідеалів.*

Доведення очевидне в силу того, що в даному кільці довільний ідеал є скінченнопородженим, а значить головним.

Наведемо приклад комутативного кільця Безу без дільників нуля, яке не є кільцем головних ідеалів. Позначимо через R кільце степеневих рядів над полем раціональних чисел з вільним цілим членом, тобто $R = \{z_0 + q_1x + \dots + q_nx^n + \dots \mid z_0 \in \mathbb{Z}, q_i \in \mathbb{Q}\}$. Очевидно, що ряди вигляду $1 + q_1x + \dots + q_nx^n + \dots$, де q_i — довільні раціональні числа, є оборотними елементами в R . Справді, якщо позначити через $u = q_1x + \dots + q_nx^n + \dots$, тоді даний ряд має вигляд $1 + u$ і оберненим до нього є ряд $1 - u + u^2 - u^3 + \dots + (-1)^n u^n + \dots$. Якщо для ряду $f \in R$ позначити через $a_{n(f)}$ перший відмінний від нуля його коефіцієнт, тоді, згідно сказаного вище, f можна подати у вигляді $f = a_{n(f)}x^{n(f)}u$, де $u \in U$.

Нехай f, g — довільні ненульові елементи R . Можливі випадки:

- 1) $n(f) = n(g) = 0$;
- 2) $n(f) > n(g)$ або $n(g) > n(f)$;
- 3) $n(f) = n(g) \neq 0$.

Якщо $n(f) = n(g) = 0$, то $f = a_0u_f$, $g = b_0u_g$, де $a_0, b_0 \in \mathbb{Z}$, $u_f, u_g \in U$. Тоді $fR + gR = dR$, де $d\mathbb{Z} = a_0\mathbb{Z} + b_0\mathbb{Z}$. Нехай $n(f) > n(g)$ і $f = a_{n(f)}x^{n(f)}u_f$, $b_{n(g)}x^{n(g)}u_g$, де $u_f, u_g \in U$. Тоді $f = b_{n(g)}x^{n(g)}u_g \cdot \frac{a_{n(f)}}{b_{n(g)}}x^{n(f)-n(g)}u_fu_g^{-1}$. Тобто $fR \subset gR$. Звідси $fR + gR = gR$. Якщо ж $k = n(f) = n(g) \neq 0$, то $f = \frac{m}{n}x^k u_f$, $g = \frac{p}{q}x^k u_g$, де $m, n, p, q \in \mathbb{Z}$, $u_f, u_g \in U$. Тоді очевидно, що $fR + gR = \frac{d}{nq}x^k R$, де $d\mathbb{Z} = mq\mathbb{Z} + np\mathbb{Z}$. Отже, R — кільце Безу.

З іншого боку, R не є кільцем головних ідеалів, оскільки воно не є факторіальним. Справді, елемент x має безліч простих дільників p , $x = p \cdot \frac{1}{p}x$ для довільного простого числа $p \in \mathbb{Z}$.

9.5 Кільця нормування

Ще одним прикладом комутативного кільца Безу є комутативні кільця нормування. Комутативне кільце з одиницею R , називається *кільцем нормування*, якщо для довільних елементів $a, b \in R$ виконується $a|b$, або $b|a$.

Твердження 81. *Комутативне кільце з одиницею є кільцем нормування тоді і тільки тоді, коли множина його ідеалів є лінійно впорядкована за включенням.*

Доведення. Нехай R — кільце нормування, а I, J — його ідеали. Припустимо, що існують елементи $i \in I, j \in J$ такі, що $i \notin J$ і $j \notin I$. Тоді $i|j$, або $j|i$. Якщо $i|j$, то $iR \supset jR$ і тому $j \in I$, якщо ж $j|i$, то $jR \supset iR$ і $i \in J$. Отже, таких двох елементів немає, а значить $J \supset I$ або $I \supset J$. Якщо ж множина ідеалів кільця R є лінійно впорядкованаю, то для довільних елементів a і $b \in R$ маємо $aR \supset bR$, або $bR \supset aR$, а це означає, що $a|b$ або $b|a$, що і потрібно довести. \square

Твердження 82. *Комутативне кільце з одиницею R є кільцем нормування тоді і лише тоді, коли R — кільце Безу з єдиним максимальним ідеалом.*

Доведення. Нехай R — кільце нормування, тоді для довільних елементів $a, b \in R$ маємо $aR + bR = \begin{cases} bR, & \text{якщо } a|b, \\ aR, & \text{якщо } b|a. \end{cases}$ Звідси отримуємо, використовуючи індукцію за кількістю твірних скінченнопороджених ідеалів, що R — кільце Безу. Припустимо, що в R існують два різні максимальні ідеали M_1, M_2 . Тоді $M_1 + M_2 = R$, звідси $m_1 + m_2 = 1$, де $m_1 \in M_1$, $m_2 \in M_2$. Оскільки R — кільце нормування, то $m_1|m_2$, або $m_2|m_1$, що можливо лише у випадку, коли $m_1 \in U$, або $m_2 \in U$, що неможливо, бо ідеали M_1 і M_2 власні.

Нехай тепер R — локальне кільце Безу (тобто кільце Безу з єдиним максимальним ідеалом), і нехай $a, b \in R \setminus \{0\}$. Розглянемо ідеал $aR + bR = dR$. Маємо $a = da_0, b = db_0, au + bv = d$, де $u, v, a_0, b_0 \in R$. Тоді $d(1 - a_0u - b_0v) = 0$. Якщо M — єдиний максимальний ідеал кільця R , то $m \in M$ тоді і тільки тоді, коли $m \notin U$. Справді, оскільки M — власний ідеал, то M не містить жодної одиниці кільця. Якби в R існував необоротний елемент n , причому $n \notin M$, то існував би такий максимальний ідеал N , що $n \in N$. Але ж R — локальне кільце, тому це неможливо. Якщо $a_0 \in M$ і $b_0 \in M$, то $1 - a_0u - b_0v \notin M$, а значить $d = 0$, оскільки $d(1 - a_0u - b_0v) = 0$ і $1 - a_0u - b_0v$ — оборотний елемент R . Але $d \neq 0$, бо $a \neq 0$ і $b \neq 0$. Отримана суперечність показує, що $a_0 \notin M$ або $b_0 \notin M$. Якщо $a_0 \notin M$, то $a_0 \in U$, тому $a|d$, а тоді $a|b$. Так само, якщо $b_0 \notin M$, тоді $b|a$, тобто R — кільце нормування. \square

Прикладами кілець нормування можуть служити кільця $\mathbb{Z}/p^n\mathbb{Z}$, де p просте число, а також локалізація кільця многочленів за будь-яким максимальним ідеалом кільця $P[x]$. Кільце $P[[x]]$ формальних степеневих рядів над полем P так само є кільцем нормування.

9.6 Регулярні кільця

Ще одну серію прикладів комутативних кілець Безу дають регулярні кільця. Кільце з одиницею називається *регулярним*, якщо рівняння $ax = a$ має розв'язок в R для довільного $a \in R$. Взагалі кажучи, дає означення діється для некомутативних кілець без одиниці, але ми обмежимося лише комутативними регулярними кільцями. Очевидними прикладами регулярних кілець є поля і бульові кільця.

Твердження 83. *Нехай R — комутативне кільце з одиницею. Тоді наступні твердження еквівалентні:*

- 1) R регулярне;
- 2) кожний головний ідеал кільца R породжується ідемпотентом;
- 3) кожний скінченнопороджений ідеал кільца R є головним і породжується ідемпотентом.

Доведення. Доведення проводимо за схемою $1) \Rightarrow 2) \Rightarrow 3) \Rightarrow 1)$.

$1) \Rightarrow 2)$ Нехай R — регулярне кільце, і $a \in R$. Тоді існує $x \in R$, що $ax = a$. Звідси маємо $axa = ax$ і $aR \supset axR \supset axaR = aR$, тобто ax — ідемпотент в R , такий що $axR = aR$.

$2) \Rightarrow 3)$ Нехай в R довільний головний ідеал породжується ідемпотентом. Покажемо, що ідеал $aR + bR$ є головним для довільних $a, b \in R$. $aR = eR$ для деякого ідемпотента $e \in R$, і оскільки $b - eb \in aR + bR$, бачимо, що $aR + bR = eR + (b - eb)R$. Тоді існує ідемпотент $f \in R$ такий, що $fR = (b - eb)R$; зазначимо, що $ef = 0$. Крім того $g = f - fe$ — ідемпотент і $eg = 0$. Оскільки $fg = g$ і $gf = f$, то $gR \supset fgR \supset fgfR = f^2R = fR$, тому $gR = fR = (b - eb)R$, звідси $aR + bR = eR + gR$. А так як $eg = 0$, то для $u, v \in R$ маємо $eu + gv = (e + g)(eu + gv)$, тому $aR + bR = (e + g)R$.

$3) \Rightarrow 1)$ Нехай в R довільний скінченнопороджений ідеал породжується ідемпотентом, тоді для довільного $a \in R$ існує ідемпотент $e \in R$ такий, що $eR = aR$. Тоді $e = ax$, $a = ey$, де $x, y \in R$, звідси $a = ea = axa$. \square

10 Вправи

1. Довести дистрибутивність законів віднімання для кільця.
2. Навести приклад алгебраичної структури з двома бінарними алгебраїчними операціями “+” і “·”, яка має всі аксіоми кільца без аксіоми лівої дистрибутивності ($a(b + c) = ab + ac$).
3. Показати, що оборотний елемент кільца не є дільником нуля.

4. Вияснити, чи обов'язково сума дільників нуля є дільником нуля?
Чи вірно це для оборотних елементів?
5. Навести приклад неасоціативного кільця, яке було б комутативним.
6. Показати, що всі комплексні числа, які є коренями многочленів з цілим коефіцієнтом і старшим коефіцієнтом, що дорівнює 1, утворюють підкільце поля комплексних чисел. Це підкільце носить назву *кільце цілих алгебраочних чисел*.
7. Показати, що множина $\mathcal{L}_f(M)$ всіх скінчених підмножин множини M є підкільцем кільця $\mathcal{L}(M)$ і $\mathcal{L}_f(M)$ має одиницю тоді і тільки тоді, коли M — скінчена.
8. Показати, що: а) в бульовому кільці для довільного $a \in R$ $a+a=0$;
б) бульове кільце комутативне.
9. Показати, що в кільці \mathbb{Z}_m довільний елемент є дільником нуля або дільником одиниці.
10. Розіб'ємо множину \mathbb{Q} на класи за ознакою: до одного класу належать числа з однаковою дробовою частиною. Перевірити, чи це розбиття узгоджене з операціями додавання і множення.
11. Показати, що серед факторкілець довільного комутативного кільця з одиницею завжди можна знайти поля.
12. Довести, що в кільці \mathbb{Z} ідеал, породжений числами m і n , збігається з ідеалом, породженим найбільшим спільним дільником чисел m і n . Показати, що в \mathbb{Z} ідеали $a\mathbb{Z}$ і $(-a)\mathbb{Z}$ співпадають.
13. Показати, що $\mathbb{R}[x]/(x^2 + 1) \cong \mathbb{C}$.
14. Показати, що $\mathbb{Z}[x]/(2, x^2 + x + 1)$ — поле з чотирьох елементів.
15. Знайти всі дільники нуля кільця $\mathbb{Z}[x]/(x^8 - 16)$.
16. Показати, що для довільного кільця R з одиницею і для кожного натурального числа n $R_n[x] \cong (R[x])_n$.
17. Нехай I — ідеал кільця R . Показати, що $R_n/I_n \cong (R/I)_n$ для довільного натурального числа n .

18. Показати, що відображення

$$a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k} \mapsto \begin{pmatrix} a & b & c & d \\ -b & a & -d & c \\ -c & d & a & -b \\ -d & -c & b & a \end{pmatrix}$$

ї мономорфізмом тіла кватерніонів в кільце $M_n(\mathbb{R})$.

19. Нехай R — комутативне кільце, а I і J — ідеали в R . Показати, що $I + J$, $I \cap J$ — ідеали в R . Навести приклад, коли $lUpJ$ не є ідеалом.
20. Нехай R — комутативне кільце з одиницею. Навести приклад кільця R без дільників нуля, що R/I — кільце без дільників нуля. Навести приклад, коли R/I — кільце без дільників нуля, а R — кільце з дільниками нуля.
21. Нехай S — нетривіальне комутативне кільце, а R — поле. Показати, що довільний гомоморфізм $f: S \rightarrow R$ є мономорфізмом. Чи вірне обернене твердження? Чи можна визначити таким чином довільне поле.
22. Нехай R — комутативне кільце з одиницею без дільників нуля. Показати, що $U(R[x]) = U$.
23. Нехай R — комутативне кільце з одиницею і K — підкільце $Q_{\text{reg}}(K)$, яке містить R . Показати, що $Q_{\text{reg}} = Q_{\text{reg}}(K)$.
24. Нехай R — комутативне кільце з одиницею, для якого довільний власний гомоморфний образ є кільцем головних ідеалів. Показати, що тоді довільний ідеал R є скінченнопородженим.
25. Навести приклад комутативного кільця R з дільниками нуля, такого що R_p — кільце без дільників нуля для довільного простого ідеалу P .
26. Нехай R — комутативне кільце з одиницею без дільників нуля, для якого довільний власний гомоморфний образ є кільцем головних ідеалів. Показати, що в R довільний власний ідеал є добутком простих ідеалів (такі кільця носять назву Дедекіндовых).
27. Показати, що в кільці цілих алгебраочних чисел немає ні атомів, ні простих елементів.

28. Нехай P — поле і $R = P[x, y, z]/(x^2 - yz)$. Нехай $f: P[x, y, z] \rightarrow R$ — природній гомоморфізм. Показати, що $f(x)$ — атом, який не є простим елементом в R .
29. Показати, що в комутативній області Безу довільний атомає простим елементом.
30. Нехай R — комутативне кільце з одиницею без дільників нуля і з скінченим числом максимальних ідеалів. Припустимо, що R_M — факторіальна область для довільного максимального ідеалу M . Показати, що R — факторіальна область.
31. Показати, що кільце формальних степеневих рядів над довільним полемає факторіальним.
32. Нехай R — факторіальна область і p — простий елемент R . Показати, що довільний елемент із $R[[x]]$ з вільним членом p є атомом в $R[[x]]$.
33. Нехай R — комутативне кільце з одиницею без дільників нуля, а S мультиплікативно замкнена множина в R . Показати, якщо R факторіальна, то R_S факторіальна. Навести приклад, коли R_S факторіальна, а R такою не є.
34. Показати, що комутативне кільце без дільників нуля R з одиницею є факторіальним тоді і тільки тоді, коли в R перетин довільних двох головних ідеалів є головним ідеалом і коли R задовільняє умові обриву зростаючих ланцюгів головних ідеалів.
35. Показати, що комутативне кільце без дільників нуля R з одиницею є факторіальним тоді і тільки тоді, коли довільний ненульовий простий ідеал R містить простий елемент.
36. Показати, що якщо R — факторіальна область, то такою є $R[[x]]$.
37. Нехай R — область головних ідеалів з скінченим числом максимальних ідеалів. Показати, що R евклідове.
38. Нехай I — ідеал в $\mathbb{Z}[[x]]$, який породжений x . Довести, що всякий простий ідеал I є головним, але не кожний ідеал I є головним.
39. Нехай R — комутативне кільце з одиницею без дільників нуля і S — мультиплікативно замкнена множина в R . Показати, якщо R — евклідова область, то R_S теж евклідова.

40. Нехай R — евклідова область відносно відображення ϕ . Означимо на M_n відображення $|A| = \phi(\det A)$. Показати, що для довільних матриць $A, B \in M_n$, де $|A| \neq 0$ існують матриці $P, Q \in M_n$ такі, що $B = AQ + P$, де $0 < |P| < |A|$, або $P = 0$.
41. Нехай R — евклідова область відносно відображення ϕ . Показати, що для кожного $x \neq 0$ існує одиниця u така, що $\phi(x) \geq \phi(u)$.
42. Показати, що кільце дійсних функцій, неперервних на $[0, 1]$, не є ні артіновим, ні нетеровим.
43. Довести, що артінове кільце без дільників нуля є полем.
44. Довести, що фактор-кільце нетерового (артінового) кільця є нетеровим (артіновим).
45. Означимо відображення $h: R[[x]] \rightarrow R$ наступним чином $h(f(x)) = f(0)$. Показати, що h — гомоморфізм кілець. Якщо R — кільце з одиницею і якщо P — простий ідеал $R[[x]]$, показати, що P скінченнопороджений тоді і тільки тоді, коли $h(P)$ скінченнопороджений. item Показати, що $R[[x]]$ нетерове тоді і тільки тоді, коли R нетерове з одиницею.
46. Нехай R комутативне кільце з одиницею і I_1, I_2, \dots, I_n — ідеали в R такі, що $I_1 \cap I_2 \cap \dots \cap I_n = \{0\}$ і кожне фактор-кільце R/I_j нетерове. Показати, що R нетерове.
47. Показати, що довільна локалізація R_S комутативного нетерового кільця з одиницею є нетеровим кільцем.
48. Нехай I — ідеал комутативного кільця R з одиницею такий, що довільний простий ідеал, який містить I , є скінченнопородженим. Показати, що довільний ідеал кільця R , який містить I , є скінченнопородженим.
49. Нехай R — комутативне нетерове кільце з одиницею. Показати, що R регулярне тоді і тільки тоді, коли $R[[x]]$ регулярне.
50. Показати, що кільце дійсних неперервних на $[0, 1]$ функцій є регулярним.
51. Нехай R — область Безу, а S — мультиплікативно замкнена множина в R . Показати, що R_S — область Безу.

52. Нехай R — комутативне кільце Безу, а P — простий ідеал. Показати, що R_p — кільце нормування.
53. Нехай R — комутативне кільце з одиницею без дільників нуля і з скінченим числом максимальних ідеалів. Припустимо, що для довільного максимального ідеалу M кільця R R_M є кільцем нормування. Показати, що R — область Безу.
54. Нехай R — комутативне кільце без дільників нуля з одиницею таке, що R_M — кільце нормування для довільного максимального ідеалу M кільця R (такі кільця називають Прюфера). Показати, що в R довільний скінченнопороджений ненульовий простий ідеал є максимальним.
55. Нехай R — область Прюфера, а S — мультиплікативно замкнена множина в R . Показати, що R_S — область Прюфера.
56. Нехай R — область нормування, а S — мультиплікативно замкнена множина. Показати, що R_S — область нормування.
57. Нехай R — комутативне кільце з одиницею. Нехай S — множина всіх многочленів в $R[x]$ таких, що їх коефіцієнти породжують R (тобто, примітивних многочленів). Нехай $T = R[x]S^{-1}$. Показати:
- 1) якщо R — кільце нормування, то T — кільце нормування;
 - 2) якщо R — область Прюфера, то T — область Прюфера;
 - 3) якщо R — область Дедекінда, то T — область головних ідеалів.
58. Показати, що комутативне кільце з одиницею є регулярним тоді і тільки тоді, коли для довільного максимального ідеалу M кільця R кільце R_M є полем.
59. Показати, що комутативне кільце з одиницею є регулярним тоді і тільки тоді, коли всі прості ідеали R є максимальними і в R не існує ненульових нільпотентних елементів (тобто елементів $a \in R \setminus \{0\}$ таких, що $a^n = 0$ для довільного $n \in \mathbb{N}$).
60. Показати, що комутативне кільце з одиницею є регулярним тоді і тільки тоді, коли 1) R/P — регулярне для довільного простого ідеалу P ; 2) всі ідеали R є ідемпотентами (тобто $I^2 = I$ для довільного ідеалу I кільця R).

61. Нехай R — комутативне регулярне кільце, а x — елемент, який не лежить в квадраті довільного максимального ідеалу. Показати, що R/xR регулярне.
62. Нехай R — комутативне кільце з одиницею і з єдиним максимальним ідеалом, який є головним. Показати: 1) якщо R — кільце без дільників нуля, тоді R — область головних ідеалів; 2) якщо R — кільце з дільниками нуля, тоді довільний ідеал R є степенем максимального.
63. Показати, що комутативне регулярне кільце з єдиним максимальним ідеаломає кільцем без дільників нуля.

11 Розширення

11.1 Просте підполе. Характеристика поля

Означення 84. Якщо K — підполе поля L (тобто K є полем відносно тих же операцій, що і L), то поле L називають *розширенням поля* K і позначають L/K . Наприклад, поле комплексних чисел \mathbb{C} є розширенням поля дійсних чисел \mathbb{R} , поля \mathbb{R} і \mathbb{C} є розширеннями поля раціональних чисел \mathbb{Q} .

Означення 85. Два поля K_1 і K_2 називають *ізоморфними*, якщо існує біективне відображення $f: K_1 \rightarrow K_2$, що є гомоморфізмом кілець, тобто $f(a+b) = f(a) + f(b)$ і $f(ab) = f(a)f(b)$.

Нехай $\{K_i\}_{i \in \mathcal{I}}$ — родина підполів поля K . Тоді перетин $\bigcap_{i \in \mathcal{I}} K_i$ — теж підполе поля K .

Означення 86. *Простим підполем* поля K називають перетин всіх підполів поля K .

Твердження 87. *Кожне просте підполе ізоморфне або полю раціональних чисел \mathbb{Q} або полю $\mathbb{Z}/p\mathbb{Z}$, де p — просте число.*

Доведення. Розглянемо відображення $f: \mathbb{Z} \rightarrow K$, де $f(n) = n1$, 1 — одиничний елемент поля K . Легко перевірити, що f — гомоморфізм кілець: $f(m+n) = (m+n) \cdot 1 = m \cdot 1 + n \cdot 1 = f(m) + f(n)$, $f(mn) = (mn) \cdot 1 = m(n \cdot 1) = (m \cdot 1)(n \cdot 1) = f(m)f(n)$. Образ гомоморфізму f є підкільцем поля K , і за теоремою про гомоморфізм маємо

$$\text{Im } f \simeq \mathbb{Z}/\text{Ker } f,$$

де $\text{Ker } f$ — ідеал у евклідовому кільці \mathbb{Z} , тому $\text{Ker } f = n\mathbb{Z}$, де $n \in \mathbb{N}$.

Якщо $n = 0$, то $\text{Im } f \simeq \mathbb{Z}$. Звідси випливає, що поле K містить також підполе, ізоморфне полю \mathbb{Q} . Якщо $n = p \neq 0$, то $\text{Im } f \simeq \mathbb{Z}/p\mathbb{Z}$. Оскільки в полі немає дільників нуля, то p тут просте число, і $\mathbb{Z}/p\mathbb{Z}$ — поле. Залишається зауважити, що ні поле \mathbb{Q} , ні поле $\mathbb{Z}/p\mathbb{Z}$ не містять власних підполів. \square

Означення 88. Поле K має *характеристику* θ , якщо з рівності $n \cdot 1 = 0$ випливає $n = 0$, де 1 — одиничний елемент поля K . У цьому випадку поле K містить в якості простого під поля поле, ізоморфне полю \mathbb{Q} . Якщо просте підполе поля K ізоморфне полю $\mathbb{Z}/p\mathbb{Z}$, то кажуть, що K має *характеристику* p . У цьому випадку просте число p є найменшим натуральним числом, що має властивість $p \cdot 1 = 0$. Характеристику поля K позначають $\text{ch } K$.

11.2 Скінченнопороджені та прості розширення

Нехай L/K — розширення поля K , M — деяка підмножина поля L .

Означення 89. Найменше підполе $K(M)$ поля L , що містить як поле K , так і множину M (тобто, перетин всіх підполів поля L з цими властивостями) називають *розширенням поля K з допомогою приєднання множини M* .

Якщо множина M складається лише з одного елемента, $M = \{\alpha\}$, то поле $K(\alpha)$ утворене приєднанням елемента α до поля K називають *простим розширенням поля K* . Якщо $M = \{\alpha_1, \dots, \alpha_n\}$ — скінченна множини, то поле $K(M) = K(\alpha_1, \dots, \alpha_n)$ називають *скінченнопородженим розширенням поля K* .

Твердження 90.

$$\begin{aligned} K(\alpha_1, \alpha_2, \dots, \alpha_n) &= K(\alpha_1)(\alpha_2) \dots (\alpha_n) = \\ &= \left\{ \frac{f(\alpha_1, \dots, \alpha_n)}{g(\alpha_1, \dots, \alpha_n)} \mid f(X_1, \dots, X_n), g(X_1, \dots, X_n) \in K[X_1, \dots, X_n], \right. \\ &\quad \left. g(X_1, \dots, X_n) \neq 0 \right\}. \end{aligned}$$

Доведення. За означенням $K(\alpha_1, \dots, \alpha_n)$ є найменшим підполем поля L , що містить елементи K і $\alpha_1, \dots, \alpha_n$. Таке підполе необхідно містить і всі елементи вигляду $f(\alpha_1, \dots, \alpha_n)$, де $f(X_1, \dots, X_n)$ — многочлен з коефіцієнтами з поля K , тому містить і всі елементи вигляду $\frac{f(\alpha_1, \dots, \alpha_n)}{g(\alpha_1, \dots, \alpha_n)}$, де $f, g \in K[X_1, \dots, X_n]$, $g(\alpha_1, \dots, \alpha_n) \neq 0$, які, очевидно, утворюють підполе поля L . \square

11.3 Алгебраїчні та трансцендентні елементи

Означення 91. Нехай L/K — розширення полів. Елемент $\alpha \in L$ називають *алгебраїчним* над K , якщо існує многочлен $f(X) \in K[X]$ з властивістю $f(\alpha) = 0$. В іншому випадку α називають *трансцендентним* над K .

Теорема 92. а) Якщо α — алгебраїчний над полем K , то існує $n \in \mathbb{N}$ таке, що

$$K(\alpha) = \{a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} \mid a_i \in K\},$$

причому кожний елемент з поля $K(\alpha)$ записується у вигляді $a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}$ однозначно.

б) Якщо α трансцендентний над K , то поле

$$K(\alpha) = \left\{ \frac{f(\alpha)}{g(\alpha)} \mid f(X), g(X) \in K[X], g(X) \neq 0 \right\}$$

ізоморфне полю $K(X)$ — полю дробів кільця $K[X]$.

Доведення. Розглянемо гомоморфізм $\phi: K[X] \rightarrow K(\alpha)$, який кожному многочлену $f(X) \in K[X]$ ставить у відповідність значення цього многочлена при $X = \alpha$ (гомоморфізм підстановки). Можливі два випадки для ядра цього гомоморфізму, що відповідають твердженням а) і б) з формулювання теореми: а) $\text{Ker } \phi \neq 0$, б) $\text{Ker } \phi = 0$.

У випадку а) $\text{Ker } \phi$ є ненульовим ідеалом кільця $K[X]$. Всі ідеали в $K[X]$ головні, тому $\text{Ker } \phi = (p(X))$. Підкільце $\text{Im } \phi \simeq K[X]/(p(X))$ є областю цілісності, тому многочлен $p(X)$ — незвідний. Звідси випливає, що фактор-кільце $K[X]/(p(X))$ є полем. Справді, досить переконатися, що кожний ненульовий елемент $\bar{f} = f(X) + (p(X))$ має обернений. $\bar{f} \neq \bar{0}$ означає, що $p(X) \nmid f(X)$, звідси випливає, що $p(X)$ і $f(X)$ — взаємно прості. За наслідком з алгоритму Евкліда існують многочлени $u(X)$ та $v(X)$ такі, що $u(X)f(X) + v(X)p(X) = 1$. Переходячи до суміжних класів, одержуємо з останнього рівності $\bar{u} \cdot \bar{f} + \bar{v} \cdot \bar{p} = \bar{u} \cdot \bar{f} = \bar{1}$, тобто \bar{f} має обернений. Звідси одержуємо, що $\text{Im } \phi = K(\alpha) = K[\alpha]$. Нехай $f(\alpha) \in K[\alpha]$, де $f(X) \in K[X]$. Розділимо $f(X)$ на $p(X)$ з остачею:

$$f(X) = p(X)d(X) + r(X),$$

де $\deg r(X) < n = \deg p(X)$. Звідси одержуємо

$$f(\alpha) = p(\alpha)d(\alpha) + r(\alpha) = r(\alpha) = a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1},$$

де $a_i \in K$. Для завершення доведення твердження а) теореми залишилось довести однозначність. Якщо $a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} = a'_0 + a'_1\alpha + \cdots + a'_{n-1}\alpha^{n-1}$, то α є коренем многочлена $p_1(X) = (a_0 - a'_0) + (a_1 - a'_1)X + \cdots + (a_{n-1} - a'_{n-1})X^{n-1}$. Якщо $p_1(X) \neq 0$, то $p_1(X)$ і $p(X)$ взаємно прості, Оскільки $p(X)$ незвідний. Тому з наслідку з алгоритму Евкліда випливає, що існують многочлени $a(X), b(X) \in K[X]$ такі, що

$$a(X)p_1(X) + b(X)p(X) = 1.$$

Підставимо сюди $X = \alpha$, одержимо $0 = 1$. Одержані суперечності означає, що $p_1(X) = 0$, отже, $a_0 = a'_0, \dots, a_{n-1} = a'_{n-1}$ і твердження а) теореми доведено.

б) Тут $\text{Im}\phi = K[\alpha] \simeq K[X]$, тому поле $K(\alpha)$ ізоморфне полю $K(X)$ — полю дробів кільця $K[X]$. \square

Приклади. 1) $\sqrt[3]{2}$ є коренем незвідного над полем \mathbb{Q} многочлена $X^3 - 2$. Отже,

$$\mathbb{Q}(\sqrt[3]{2}) = \{a_0 + a_1\sqrt[3]{2} + a_2\sqrt[4]{4} \mid a_0, a_1, a_2 \in \mathbb{Q}\}.$$

2) Ми знаємо що $\alpha = \sum_{n=0}^{\infty} 10^{-n!}$ трансцендентне дійсне число. Тому $\mathbb{Q}(\alpha) \simeq \mathbb{Q}(X)$.

Означення 93. Якщо елемент $\alpha \in L$ — алгебраїчний над полем K , то *мінімальним многочленом елемента* α називають многочлен $p(X)$, який задовольняє такі три умови:

- 1) $p(\alpha) = 0$;
- 2) $\forall f(X) \in K[X] \quad f(\alpha) = 0 \Rightarrow \deg f(X) \geq \deg p(X)$;
- 3) старший коефіцієнт многочлена $p(X)$ дорівнює 1.

Зauważення 94. Мінімальний многочлен алгебраїчного елемента α є незвідним і однозначно визначається елементом α .

11.4 Скінченні розширення

Нехай L/K — розширення поля K . Тоді $L \in K$ — лінійним простором.

Означення 95. розширення L/K називають *скінченним*, якщо простір L — скінченновимірний, в іншому випадку L/K називають *нескінченним розширенням*. Розмірність $\dim_K L$ лінійного простору L називають *степенем розширення* L/K і позначають $[L : K]$: $[L : K] = \dim_K L$.

Твердження 96. Нехай $K \subset L \subset M$ — башта полів. Якщо два з трьох розширень L/M , M/L , M/K скінченні, то й третє розширення скінченне і справедлива рівність

$$[M : K] = [M : L] \cdot [L : K]. \quad (11.4.1)$$

Доведення. Припустимо, що $[L : K] < \infty$ і $[M : L] < \infty$. Нехай $\alpha_1, \dots, \alpha_n$ — база K -лінійного простору L , і β_1, \dots, β_m — база L -лінійного простору M . Перевіримо, що елементи $\alpha_i\beta_j$, $1 \leq i \leq n$, $1 \leq j \leq m$ складають бу K -лінійного простору M . І m елементів $\alpha_i\beta_j$ лінійно незалежні над K : якщо $\sum_{i,j} a_{ij}\alpha_i\beta_j = 0$, де $a_{ij} \in K$, то $\sum_{j=1}^m (\sum_{i=1}^n a_{ij}\alpha_i)\beta_j = 0 \Rightarrow \sum_i a_{ij}\alpha_i = 0$, Оскільки β_1, \dots, β_m — база $M/L \Rightarrow a_{ij} = 0$, Оскільки $\alpha_1, \dots, \alpha_n$ — база L/K .

З іншого боку, елементи $\alpha_i\beta_j$ утворюють систему твірних розширення M/K . Справді, якщо $\xi \in M$, то $\xi = \sum_{j=1}^m \gamma_j \beta_j$ з $\gamma_j \in L$. Оскільки $\alpha_1, \dots, \alpha_n$ — база L/K , то $\gamma_j = \sum_{i=1}^n a_{ij}\alpha_i$ і $\xi = \sum_{j=1}^m \sum_{i=1}^n a_{ij}\alpha_i\beta_j$.

Якщо $[M : K] < \infty$, то $[M : L] < \infty$ і $[L : K] < \infty$ і рівність (11.4.1) доводимо як в попередньому випадку. \square

Означення 97. розширення L/K називають *алгебраїчним*, якщо кожен елемент $\alpha \in L$ є алгебраїчним над полем K .

Твердження 98. Кожне скінченне розширення L/K є алгебраїчним.

Доведення. Нехай $[L : K] = n$ і $\alpha \in L$. $n+1$ елементів $1, \alpha, \dots, \alpha^n$ є лінійно залежними. Тому існують елементи $a_0, a_1, \dots, a_n \in K$, що не всі дорівнюють 0, і такі, що $a_0 + a_1\alpha + \dots + a_n\alpha^n = 0$. Отже, α є коренем многочлена $a_0 + a_1X + \dots + a_nX^n \in K[X]$. \square

Зауважимо, що обернене твердження невірне (див. вправу 10), але вірне таке твердження.

Твердження 99. Нехай $\alpha_1, \dots, \alpha_n$ — алгебраїчні над полем K елементи. Тоді $K(\alpha_1, \dots, \alpha_n)$ — скінченне розширення поля K .

Доведення. З твердження а) теореми 92 випливає, що всі розширення $K(\alpha_i)/K$ скінченні і $[K(\alpha_i) : K]$ дорівнює степеню мінімального многочлена елемента α_i . Нехай $[K(\alpha_i) : K] = n_i$. Розглянемо башту

$$K \subset K(\alpha_1) \subset K(\alpha_1, \alpha_2) \subset \dots \subset K(\alpha_1, \dots, \alpha_n).$$

З твердження 96 одержуємо

$$\begin{aligned}[K(\alpha_1, \dots, \alpha_n) : K] &= [K(\alpha_1, \dots, \alpha_n) : K(\alpha_1, \dots, \alpha_{n-1})] \cdots [K(\alpha_1) : K] \leq \\ &\leq [K(\alpha_n) : K] \cdots [K(\alpha_1) : K] = n_1 \cdots n_k < \infty.\end{aligned}$$

□

11.5 Теорема Кронекера-Артіна

Теорема 100. *Нехай K — поле, $f(X)$ — многочлен з коефіцієнтами з поля K , $f(X) \in K[X]$, $\deg f(X) = n \geq 1$. Існує розширення L/K , в якому многочлен $f(X)$ має корінь, тобто $f(\alpha) = 0$ для деякого $\alpha \in L$.*

Доведення. Досить розглянути випадок, коли многочлен $f(X)$ незвідний, Оскільки корінь незвідного множника многочлена є коренем самого многочлена. У цьому випадку фактор-кільце $K[X]/(f(X))$ є полем (це показано в доведенні теореми 92). Візьмемо $L = K[X]/(f(X))$. Нехай $\bar{X} \in L$ — суміжний клас з представником X . Елементи з L вигляду $\bar{a} = a + (f(X))$, де $a \in K$, утворюють підполе поля L , ізоморфне полю K . Ототожнюючи за допомогою цього ізоморфізму елементи $a \in K$ із суміжними класами $\bar{a} \in L$, маємо $f(\bar{X}) = a_0 + a_1\bar{X} + \cdots + a_n\bar{X}^n = \bar{a}_0 + \bar{a}_1\bar{X} + \cdots + \bar{a}_n\bar{X} = \bar{a}_0 + a_1X + \cdots + a_nX^n = \bar{f}(X) = \bar{0}$, тобто $\alpha = \bar{X}$ — корінь многочлен $f(X)$. □

Наслідок 101. *Нехай $f_1(X), \dots, f_m(X) \in K[X]$, $\deg f_i(X) \geq 1$, $1 \leq i \leq m$, тоді існує розширення L/K , в якому кожний многочлен $f_i(X)$ має корінь α_i .*

Доведення. З теореми випливає, що існує розширення L_1/K і $\alpha_1 \in L_1$, що є коренем многочлен $f_1(X)$: $f_1(\alpha_1) = 0$. Так само існує розширення L_2/L_1 , в якому многочлен $f_2(X)$ з коефіцієнтами в полі L_1 (тому, що $K \subset L_1$) має корінь α_2 : $f_2(\alpha_2) = 0$. І так далі, існує башта розширень

$$K \subset L_1 \subset L_2 \subset \cdots \subset L_m$$

така, що многочлен $f_k(X)$ має корінь $\alpha_k \in L_k$, $1 \leq k \leq m$. В розширенні L_m/K кожний многочлен f_1, \dots, f_m має корінь. □

12 Гомоморфізми (вкладення) полів

12.1 Гомоморфізми та їх продовження

Означення 102. Відображення $\sigma: K_1 \rightarrow K_2$ називають *гомоморфізмом поля* K_1 в поле K_2 , якщо

$$\sigma(a + b) = \sigma(a) + \sigma(b), \quad \sigma(ab) = \sigma(a)\sigma(b), \quad \sigma(0) = 0, \quad \sigma(1) = 1.$$

Зauważення 103. Кожний гомоморфізм полів є вкладенням, тобто має нульове ядро. Це випливає з того, що ядро будь-якого гомоморфізму кільце $\sigma: K_1 \rightarrow K_2$ є ідеалом кільця K_1 . Оскільки K_1 — поле, то в K_1 немає нетривіальних ідеалів. Звідси, і з умови $f(1) = 1$, випливає, що $\text{Ker } \sigma = 0$. Тому у випадку полів вживають слово *вкладення* замість слова *гомоморфізм*. Кожне вкладення полів $\sigma: K_1 \rightarrow K_2$ визначає ізоморфізм $\sigma: K_1 \xrightarrow{\sim} \sigma(K_1)$ поля K_1 на його образ $\sigma(K_1)$ в полі K_2 .

Приклад. Розглянемо поле $\mathbb{Q}(\sqrt[4]{2})$ і гомоморфізм $\sigma: \mathbb{Q}(\sqrt[4]{2}) \rightarrow \mathbb{C}$ такий, що $\sigma(a) = a$ для кожного $a \in \mathbb{Q}$ і $\sigma(\sqrt[4]{2}) = i\sqrt[4]{2}$, тобто

$$\sigma(a_0 + a_1\sqrt[4]{2} + a_2(\sqrt[4]{2})^2 + a_3(\sqrt[4]{2})^3) = a_0 + a_1i\sqrt[4]{2} + a_2(i\sqrt[4]{2})^2 + a_3(i\sqrt[4]{2})^3,$$

де $a_0, a_1, a_2, a_3 \in \mathbb{Q}$. Відображення σ є гомоморфізмом: його можна розкласти в додаток трьох гомоморфізмів

$$\mathbb{Q}(\sqrt[4]{2}) \xrightarrow{\sim} \mathbb{Q}[X]/(X^4 - 2) \xrightarrow{\sim} \mathbb{Q}(i\sqrt[4]{2}) \rightarrow \mathbb{C},$$

$$\sqrt[4]{2} \mapsto \bar{X} \mapsto i\sqrt[4]{2} \mapsto i\sqrt[4]{2}.$$

Гомоморфізм σ є вкладенням поля $\mathbb{Q}(\sqrt[4]{2})$ в поле \mathbb{C} , і його образом є поле $\mathbb{Q}(i\sqrt[4]{2})$.

Означення 104. Нехай $\sigma: K_1 \rightarrow K_2$ вкладення полів. Вкладення полів $\tau: L_1 \rightarrow L_2$ називають *продовженням вкладення* σ , якщо поле L_1 є розширенням поля K_1 , L_2 — розширенням K_2 , і $\tau(a) = \sigma(a)$ для кожного $a \in K_1$.

Якщо τ є продовженням σ , то це записують у вигляді комутативної діаграми гомоморфізмів, що на мал. 1 (тут $\tau i_1 = i_2 \sigma$, $i_1(a) = a$ для всіх $a \in K_1$, $i_2(a) = a$ для всіх $a \in K_2$).

Нехай $f(x) = a_0 + a_1X + \cdots + a_nX^n$ — многочлен з коефіцієнтами з поля K_1 , $\sigma: K_1 \rightarrow K_2$ — вкладення поля K_1 у поле K_2 , $\tau: L_1 \rightarrow L_2$ — продовження σ . Справедливе наступне

Твердження 105. Якщо $\alpha \in L_1$ — корінь многочлена $f(X) \in K_1[X]$, то $\tau(\alpha)$ — корінь многочлена

$$f^\sigma(X) = \sigma(a_0) + \sigma(a_1)X + \cdots + \sigma(a_n)X^n \in K_2[X].$$

$$\begin{array}{ccc} K_1 & \xrightarrow{\sigma} & K_2 \\ i_1 \downarrow & & \downarrow i_1 \\ L_1 & \xrightarrow{\tau} & L_2 \end{array}$$

Рис. 1:

Доведення. Маємо рівність в полі L_1

$$a_0 + a_1\alpha + \cdots + a_n\alpha^n = 0.$$

Подіємо на цю рівність гомоморфізмом τ :

$$\tau(a_0) + \tau(a_1)\tau(\alpha) + \cdots + \tau(a_n)(\tau(\alpha))^n = \sigma(a_0) + \sigma(a_1)\tau(\alpha) + \cdots + \sigma(a_n)\tau(\alpha)^n = 0.$$

□

Наслідок 106. Нехай $\tau: L_1 \rightarrow L_2$ — продовження одніичноого вкладення $id: K_1 \rightarrow K_1$. Тоді τ переводить кожний корінь α многочлена $f(X) \in K_1[X]$, що міститься в полі L_1 , в корінь цього ж многочлена в полі L_2 .

12.2 Теореми про продовження гомоморфізмів

Теорема 107. Нехай L_1 — скінченнопороджене розширення поля K_1 , σ — вкладення поля K_1 в деяке поле K_2 . Тоді існує розширення L_2 поля K_2 і продовження $\tau: L_1 \rightarrow L_2$ вкладення σ .

Доведення. $L = K(\alpha_1, \dots, \alpha_n)$. Міркуючи за індукцією, можна вважати, що $L = K(\alpha)$. Якщо α — трансцендентний над K_0 , то покладемо $L_2 = K_2(X)$ — поле раціональних функцій від X над полем K_2 , а вкладення τ означимо так:

$$\tau\left(\frac{a_0 + a_1\alpha + \cdots + a_k\alpha^k}{b_0 + b_1\alpha + \cdots + b_m\alpha^m}\right) = \frac{\sigma(a_0) + \sigma(a_1)X + \cdots + \sigma(a_k)X^k}{\sigma(b_0) + \sigma(b_1)X + \cdots + \sigma(b_m)X^m}.$$

Якщо ж α — алгебраїчний над K_1 , то нехай $p(X) = c_3 + c_1X + \cdots + c_mX^m$ — мінімальний многочлен для α над K_1 . Теорема Кронекера-Артіна стверджує, що існує розширення L поля K_2 , в якому многочлен $p^\sigma(X) = \sigma(c_0) + \sigma(c_1)X + \cdots + \sigma(c_m)X^m \in K_2[X]$ має корінь $\alpha' \in L$. Розглянемо поле $L_2 = K_2(\alpha')$ і гомоморфізм $\tau: L_1 \rightarrow L_2$ такий, що $\tau(a) = \sigma(a)$ для всіх $a \in K_1$ і $\tau(\alpha) = \alpha'$, тобто $\tau(a_0 + a_1\alpha + \cdots + a_{s-1}\alpha^{s-1}) = \sigma(a_0) + \sigma(a_1)\alpha' + \cdots + \sigma(a_{s-1})\alpha'^{s-1}$. Вкладення τ і є шуканим продовженням вкладення σ . □

12.3 Лема Артіна про лінійну незалежність характерів

Означення 108. Нехай G — група, K — поле. *Характером групи G в полі K* називають гомоморфізм $\sigma: G \rightarrow K^*$ групи G в мультиплікативну групу поля K .

Приклади

1) Якщо $G = \mathbb{Z}/n\mathbb{Z}$, то кожний характер цієї групи $\sigma: \mathbb{Z}/n\mathbb{Z} \rightarrow \mathbb{C}^*$ в полі комплексних чисел \mathbb{C} цілком визначається значенням $\sigma(\bar{1}) \in \mathbb{C}$. Маємо $1 = \sigma(\bar{0}) = \sigma(n \cdot \bar{1}) = \sigma(\bar{1})^n$, тобто $\sigma(\bar{1})$ є коренем n -го степеня з 1. Звідси випливає, що існує n різних характерів $\sigma_1, \dots, \sigma_n: \mathbb{Z}/n\mathbb{Z} \rightarrow \mathbb{C}^*$, де $\sigma_k(\bar{1}) = \cos \frac{2\pi k}{n} + i \sin \frac{2\pi k}{n}$, $1 \leq k \leq n$.

2) Якщо $\sigma: L \rightarrow M$ — вкладення полів, то σ можна розглядати як характер мультиплікативної групи L^* в полі M .

Наступна лема про характери груп буде використана якраз у випадку вкладень полів. У її формулуванні вираз $\alpha_1\sigma_1 + \dots + \alpha_n\sigma_n$, де $\sigma_1, \dots, \sigma_n$ — характери групи G в полі K , а $\alpha_1, \dots, \alpha_n \in K$ означає функцію, визначену на G із значеннями в полі K .

Лема 109 (Артін). *Нехай G — група, K — поле, $\sigma_1, \dots, \sigma_n: G \rightarrow K^*$ — різні характери групи G в полі K . Тоді $\sigma_1, \dots, \sigma_n$ — лінійно незалежні над K , тобто якщо $\alpha_1\sigma_1 + \dots + \alpha_n\sigma_n = 0$, де $\alpha_1, \dots, \alpha_n \in K$, то $\alpha_1 = \dots = \alpha = 0$.*

Доведення. Міркуємо за індукцією. Якщо $n = 1$, то з рівності $\alpha_1\sigma_1 = 0$ випливає рівність в полі K $\alpha_1\sigma(g) = 0$, де $g \in G$. Оскільки $\sigma_1(g) \in K^*$, то $\alpha_1 = 0$. Припустимо, що твердження леми справедливе для $n - 1$ різних характерів. Якщо ми маємо n різних характерів і для деяких $\alpha_1, \dots, \alpha_n \in K$

$$\alpha_1\sigma_1 + \dots + \alpha_n\sigma_n = 0, \quad (12.3.1)$$

то для кожного $g \in G$ одержується рівність

$$\alpha_1\sigma_1(g) + \dots + \alpha_n\sigma_n(g) = 0. \quad (12.3.2)$$

Оскільки характери $\sigma_1, \dots, \sigma_n$ — різні, то існує елемент $g' \in G$, для якого $\sigma_1(g') \neq \sigma_n(g')$. Підставивши в (12.3.2) $g'g$ замість g , одержуємо

$$\alpha_1\sigma_1(g')\sigma_1(g) + \dots + \alpha_{n-1}\sigma_{n-1}(g')\sigma_{n-1}(g) + \alpha_n\sigma_n(g')\sigma_n(g) = 0. \quad (12.3.3)$$

Домножимо рівність (12.3.2) на $\sigma_n(g')$:

$$\alpha_1\sigma_n(g')\sigma_1(g) + \dots + \alpha_{n-1}\sigma_n(g')\sigma_{n-1}(g) + \alpha_n\sigma_n(g')\sigma_n(g) = 0. \quad (12.3.4)$$

Віднімемо почленно (12.3.3) і (12.3.4), одержимо

$$\alpha_1(\sigma_1(g') - \sigma_n(g'))\sigma_1(g) + \cdots + \alpha_{n-1}(\sigma_{n-1}(g') - \sigma_n(g'))\sigma_{n-1}(g) = 0.$$

За припущенням індукції звідси випливає, що $\alpha_i(\sigma_i(g') - \sigma_n(g')) = 0$ для всіх i , $1 \leq i \leq n-1$. Зокрема, $\alpha_1(\sigma_1(g') - \sigma_n(g')) = 0$, тому $\alpha_1 = 0$ за вибором елемента g' . Підставимо $\alpha_1 = 0$ в (12.3.1), одержимо

$$\alpha_2\sigma_2 + \cdots + \alpha_n\sigma_n = 0,$$

а звідси маємо $\alpha_2 = \cdots = \alpha_n = 0$ за припущенням індукції. \square

12.4 Теорема про кількість вкладень

Теорема 110. *Нехай L/K – скінченне розширення, $[L : K] = n$, $\sigma_1, \dots, \sigma_m$ – різні вкладення поля L у поле M такі, що $\sigma_i(a) = \sigma_j(a)$ для всіх $a \in K$ і всіх i, j , $1 \leq i, j \leq m$. Тоді $m \leq n$.*

Доведення. Доводимо від супротивного. Припустимо, що $m > n$. Нехай u_1, \dots, u_n – база L/K . m векторів

$$\begin{aligned} v_1 &= (\sigma_1(u_1), \dots, \sigma_1(u_n)), \\ &\dots \\ v_m &= (\sigma_m(u_1), \dots, \sigma_m(u_n)) \end{aligned}$$

простору M^n є лінійно залежними над M . Це означає, що існують $\lambda_1, \dots, \lambda_m \in M$, які не всі дорівнюють 0, і $\sum_{k=1}^m \lambda_k \sigma_k(u_i) = 0$ для всіх i , $1 \leq i \leq n$.

Кожний елемент $\alpha \in L$ можна записати у вигляді $\alpha = \sum_{i=1}^n a_i u_i$, де $a_i \in K$. Маємо

$$\left(\sum_{k=1}^m \lambda_k \sigma_k \right) (\alpha) = \sum_{k=1}^m \lambda_k \sigma_k \left(\sum_{i=1}^n a_i u_i \right) = \sum_{k=1}^m \sum_{i=1}^n \lambda_k \sigma_k(a_i) \sigma_k(u_i).$$

За умовами теореми $\sigma_k(a_i)$ не залежить від k , позначимо $\sigma_k(a_i) = b_i$ і підставимо це в останню суму:

$$\left(\sum_{k=1}^m \lambda_k \sigma_k \right) (\alpha) = \sum_{k=1}^m \sum_{i=1}^n \lambda_k b_i \sigma_k(u_i) = \sum_{i=1}^n b_i \left(\sum_{k=1}^m \lambda_k \sigma_k(u_i) \right) = 0.$$

Отже, $\sum_{k=1}^m \lambda_k \sigma_k = 0$ і не всі $\lambda_1, \dots, \lambda_m$ дорівнюють нулю. Це суперечить лемі Артіна. \square

Наслідок 111. *Нехай L/K – скінченне розширення, $[L : K] = n$, $\sigma_1, \dots, \sigma_m$ – різні вкладення поля L у поле M такі, що $\sigma_i(a) = a$ для всіх $a \in K$ і всіх i , $1 \leq i \leq m$. Тоді $m \leq n$.*

13 Алгебраїчно замкнені поля

Поле L називають *алгебраїчно замкненим*, якщо кожний многочлен $f(X) \in L[X]$ степеня ≥ 1 має корінь в полі L .

Метою цього параграфа є доведення теореми про те, що для кожного поля K існує розширення L/K алгебраїчне над K і алгебраїчно замкнене. розширення L/K з такими властивостями називають *алгебраїчним замиканням* поля K . Для побудови алгебраїчного замикання буде використаний метод Артіна, викладений у книзі С. Ленга [?].

Нам необхідно ввести в розгляд кільце многочленів від нескінченної кількості змінних.

13.1 Кільце многочленів $K[S]$

Нехай K довільне кільце, S множина (можливо нескінчена), елементи якої позначаємо $X_s, s \in S$. Кожній скінченний підмножині $\{X_{i_1}, \dots, X_{i_n}\} \subset S$ поставимо у відповідність кільце многочленів $K[X_{i_1}, \dots, X_{i_n}]$ від n змінних. Через $K[S]$ позначимо об'єднання всіх $K[X_{i_1}, \dots, X_{i_n}]$, для всіх скінчених підмножин $\{X_{i_1}, \dots, X_{i_n}\}$ множини S . $K[S]$ складається з многочленів, кожний многочлен з $K[S]$ залежить лише від скінченої кількості змінних, але різні многочлени залежать, взагалі кажучи, від різних змінних. Якщо маємо два многочлени $f, g \in K[S]$ і f залежить від змінних із скінченої підмножини $S_1 \subset S$, g — від змінних із скінченої підмножини $S_2 \subset S$, то можна вважати, що f і g залежать від змінних з множини $S_1 \cup S_2$. Очевидно, що $K[S]$ є кільцем відносно звичайних операцій додавання та множення многочленів.

У доведенні теореми про існування алгебраїчно замкнених розширень даного поля K ми використаємо кільце многочленів $K[S]$ з коефіцієнтами з поля K .

13.2 Теорема про існування алгебраїчно замкнених розширень

Теорема 112. Для кожного поля K існує алгебраїчно замкнене розширення E/K .

Доведення. Нехай S — множина всіх многочленів степеня ≥ 1 з коефіцієнтами з поля K . Поставимо у відповідність кожному такому многочлену $f(X) \in K[X]$ символ $X_f \in S$. Одержано взаємно однозначну відповідність множини многочленів степеня ≥ 1 і множини символів X_f . Розглянемо ідеал \mathcal{I} в кільці $K[X]$, породжений многочленом $f(X_f)$.

\mathcal{I} складається з усіх многочленів вигляду

$$g_{f_1}(X_{i_1}, \dots, X_{i_{k_1}})f_1(X_{f_1}) + \dots + g_{f_r}(X_{j_1}, \dots, X_{j_{k_r}})f_r(X_{f_r}).$$

Переконаємось в тому, що $\mathcal{I} \neq K[S]$. Якби це було не так, то ми одержали б для деяких $g_{f_1}, \dots, g_{f_r} \in K[S]$

$$g_{f_1} \cdot f_1(X_{f_1}) + \dots + g_{f_r} \cdot f_r(X_{f_r}) = 1. \quad (13.2.1)$$

Застосуємо наслідок з теореми Кронекера-Артіна: існує розширення L/K , в якому кожний многочлен f_i має корінь α_i . Підставивши в (13.2.1) α_i замість X_{f_i} і 0 замість інших змінних, що туди входять, одержимо $0 = 1$. Ця суперечність показує, що \mathcal{I} — власний ідеал кільця $K[S]$. Тому існує максимальний ідеал \mathcal{M} , $\mathcal{I} \subset \mathcal{M}$. Фактор-кільце $L_1 = K[S]/\mathcal{M}$ є полем і його можна вважати розширенням поля K (ототожнюючи, як звичайно, $\alpha \in K$ і суміжний клас $\bar{\alpha} = \alpha + \mathcal{M} \in L_1$).

Якщо $f(X) \in K[X]$, $\deg f(X) \geq 1$, то $f(X) \in \mathcal{M}$ і ми маємо $\bar{0} = \overline{f(X)} = a_0 + a_1 \bar{X} + \dots + a_n \bar{X}^n$, тобто $f(X)$ має корінь \bar{X} в L_1 .

Так само будуємо розширення L_2/L_1 , в якому кожний многочлен з коефіцієнтами з L_1 має корінь в L_2 . Продовжуючи цей процес, одержуємо нескінченну башту розширень

$$K = L_0 \subset L_1 \subset L_2 \subset \dots \subset L_m \subset \dots \quad (13.2.2)$$

з властивістю, що кожен многочлен з коефіцієнтами з поля L_i має корінь в полі L_{i+1} . Позначимо через E об'єднання всіх полів L_i , $0 \leq i < \infty$. Якщо $\alpha, \beta \in E$, то існує $i \geq 1$, що $\alpha, \beta \in L_i$ і ми беремо суму $\alpha + \beta$ тадобуток $\alpha\beta$ елементів α і β в полі L_i . Очевидно, так визначені операції задовільняють всі аксіоми поля, тому E поле.

Перевіримо, що E алгебраїчно замкнене. Нехай $f(X) = a_0 + a_1 X + \dots + a_n X^n \in E[X]$. Кожен коефіцієнт a_k належить деякому полю L_{i_k} , тому всі коефіцієнти належать полю L_i , де $i = \max\{i_0, \dots, i_n\}$. З побудовою башти (13.2.2) многочлен $f(X)$ має корінь $\alpha \in L_{i+1} \subset E$. \square

14 Алгебраїчне замикання

Означення 113. Поле \overline{K} називають *алгебраїчним замиканням поля K* , якщо воно є алгебраїчним і алгебраїчно замкненим розширенням поля K .

Теорема 114. Для кожного поля K існує алгебраїчне замикання \overline{K} поля K .

Доведення. Позначимо \overline{K} множину всіх алгебраїчних над K елементів з алгебраїчно замкненого розширення E/K , існування якого стверджується у попередній теоремі. Доведемо, що \overline{K} — поле. Нехай $\alpha, \beta \in \overline{K}$. Тоді $K(\alpha, \beta)$ — скінченне розширення поля K , це випливає з твердження 99, отже, $K(\alpha, \beta)$ — алгебраїчне над K з твердженням 98. Тому $\alpha + \beta, \alpha \cdot \beta \in \overline{K}$ і \overline{K} замкнене відносно операцій додавання та множення. Очевидно, \overline{K} є полем відносно цих операцій.

Покажемо, що \overline{K} алгебраїчно замкнене поле. Нехай $f(X) \in \overline{K}[X]$, $f(X) = a_0 + a_1 X + \cdots + a_n X^n$, де всі a_i алгебраїчні над K , $n \geq 1$ і α — корінь многочлен $f(X)$. Тоді $\alpha \in E$ — алгебраїчний над $K(a_0, \dots, a_n)$. Маємо, знову використовуючи твердження 99,

$$[K(\alpha, a_0, \dots, a_n) : K(a_0, \dots, a_n)] < \infty \text{ і } [K(a_0, \dots, a_n) : K] < \infty,$$

тому з твердження 98 випливає, що α — алгебраїчний над K , тобто $\alpha \in \overline{K}$. \square

15 “Єдиність” алгебраїчного замикання

Означення 115. розширення L_1 і L_2 поля K називають *еквівалентними* над полем K , якщо існує ізоморфізм $\sigma: L_1 \rightarrow L_2$, який продовжує однійничий автоморфізм поля K , тобто $\sigma(a) = a$ для всіх $a \in K$.

Ми доведемо, що коли \overline{K}_1 і \overline{K}_2 — алгебраїчні замикання поля K , то вони еквівалентні над K . Це випливатиме з наступної теореми.

Теорема 116. Нехай K — поле, L/K — алгебраїчне розширення, $\sigma: K \rightarrow E$ — вкладення поля K в алгебраїчно замкнене поле E . Тоді існує продовження $\tau: L \rightarrow E$ вкладення σ . Якщо поле E алгебраїчне над σK , а поле L — алгебраїчно замкнене, то вкладення τ є ізоморфізмом полів L і E .

Доведення. Розглянемо множину S пар (M, λ) , де M — підполе поля L , $\lambda: M \rightarrow E$ — продовження вкладення $\sigma: K \rightarrow E$. Множина S — непорожня: вона містить елемент (K, σ) . Означимо на множині S порядок. Вважаємо, що $(M_1, \lambda_1) \leq (M_2, \lambda_2)$, якщо $M_1 \subset M_2$ і λ_2 продовження вкладення λ_1 . Якщо $\{(M_i, \lambda_i)\}$ лінійно впорядкована підмножина множини S , то $(\bigcup M_i, \tau)$, де τ дорівнює λ_i на M_i є максимальним елементом лінійно впорядкованої множини $\{(M_i, \lambda_i)\}$. Тому можна застосувати лему Цорна, і в множині S існує максимальний елемент (N, τ) . Перевіримо, що $N = L$. Якщо $N \subsetneq L$, то існує $\alpha \in L$, $\alpha \notin N$ і α — алгебраїчний над N

(тому, що L — алгебраїчне над K). З теореми ?? про продовження гомоморфізмів випливає, що існує продовження $\tau': N(\alpha) \rightarrow E$ вкладення $\tau: N \rightarrow E$, тобто (N, τ) не є максимальним елементом множини S . Тому $N = L$ і перше твердження теореми доведене.

Якщо L алгебраїчно замкнене, E алгебраїчне над σK , то τL — підполе поля E , τL — алгебраїчне над σK . Отже, E і τL — алгебраїчні замикання поля σK , $\tau L \subset E$. Звідси випливає, що $E = \tau L$ і теорему доведено. \square

Наслідок 117. *Нехай \bar{K}_1 і \bar{K}_2 — алгебраїчні замикання поля K . Тоді вони еквівалентні над K .*

Доведення. Теорема стверджує, що існує продовження $\tau: \bar{K}_1 \rightarrow \bar{K}_2$ однічного автоморфізму $\sigma = id: K \rightarrow K$ і це продовження є ізоморфізмом полів \bar{K}_1 і \bar{K}_2 . \square

16 Поле розкладу многочлена

Означення 118. Полем розкладу многочлен $f(X) \in K[X]$ називають найменше розширення (в з д ному алгебраїчному замиканні \bar{K} поля K), в якому многочлен $f(X)$ розкладається на лінійні множники.

Приклади.

- 1) $\mathbb{Q}(\sqrt{5})$ — поле розкладу многочлен $X^2 - X - 1 \in \mathbb{Q}[X]$;
- 2) \mathbb{C} — поле розкладу многочлен $X^2 + 1 \in \mathbb{R}[X]$, ле поле \mathbb{C} не є полем розкладу многочлен $X^2 + 1 \in \mathbb{Q}(X)$. Полем розкладу ост нього многочлен є поле $\mathbb{Q}(i)$.

Теорема 119. Для кожного многочлен $f(X) \in K[X]$ існує поле розкладу цього многочлена. Поле розкладу визначається многочленом $f(X)$ однозначно з точністю до еквівалентності.

Доведення. Якщо $f(X) \in K[X]$, то за теоремою Кронекера-Артіна існує розширення K_1 поля K , у якому многочлен $f(X)$ має корінь α_1 . З теореми Безу про корені многочлена випливає, що в кільці $K_1[X]$ вірна рівність $f(X) = (X - \alpha_1)f_1(X)$. Так само, існує розширення K_2/K_1 , у якому многочлен $f_1(X)$ має корінь α_2 . І так далі, через не більше, ніж $n = \deg f$ кроків, ми одержимо розширення L поля K , у якому многочлен $f(X)$ розкладається на лінійні множники: $f(X) = (X - \alpha_1)f(X) =$

$(X - \alpha_1)(X - \alpha_2)f_2(X) = \dots = (X - \alpha_1)\dots(X - \alpha_n)a_n$, де a_n — старший коефіцієнт многочлен $f(X)$.

Зауважимо, що коли якимось способом побудоване розширення L , у якому многочлен $f(X)$ розкладається на лінійні множники, $f(X) = (X - \alpha_1)\dots(X - \alpha_n)a_n$, то полем розкладу є підполе $K(\alpha_1, \dots, \alpha_n)$ поля L , що одержується приєднанням до поля K всіх коренів многочлен $f(X)$.

Поле розкладу $K(\alpha_1, \dots, \alpha_n)$ можна одержати ще таким способом. Розглянемо яке-небудь алгебраїчне замикання \bar{K} поля K . У полі \bar{K} многочлен $f(X)$ розкладається на лінійні множники і поле розкладу можна одержати як в попередньому абзаці.

Доведемо єдиність (з точністю до еквівалентності) поля розкладу. Нехай $K_1 = K(\alpha_1, \dots, \alpha_n)$ і $K_2 = K(\beta_1, \dots, \beta_n)$ дві поля розкладу. Розглянемо алгебраїчні замикання \bar{K}_1 і \bar{K}_2 полів K_1 і K_2 . \bar{K}_1 і \bar{K}_2 — алгебраїчні замикання поля K , тому вони еквівалентні: існує ізоморфізм $\tau: \bar{K}_1 \rightarrow \bar{K}_2$, для якого $\tau(a) = a$ для всіх $a \in K$. Вияснимо як τ діє на корені многочлена $f(X)$. Якщо α_i — корінь многочлена $f(X) = a_0 + a_1X + \dots + a_nX^n \in K[X]$, то $a_0 + a_1\alpha_i + \dots + a_n\alpha_i^n = 0$, звідси $a_0 + a_1\tau(\alpha_i) + \dots + a_n\tau(\alpha_i)^n = 0$, тобто $\tau(\alpha_i)$ є одним з коренів многочлен $f(X)$ у полі \bar{K}_2 . Отже, $\tau(\alpha_i) = \beta_j$ для деякого j , $1 \leq j \leq n$. Оскільки τ ін'єктивне відображення, то τ переводить різні корені множини $\{\alpha_1, \dots, \alpha_n\}$ у різні корені множини $\{\beta_1, \dots, \beta_n\}$, тобто τ є еквівалентністю полів $K(\alpha_1, \dots, \alpha_n)$ та $K(\beta_1, \dots, \beta_n)$. \square

17 Поле раціональних функцій

У цьому параграфі ми розглянемо поле раціональних функцій з точки зору розширень полів. Поле раціональних функцій $K(X)$ над полем K — це, за означенням, поле дробів кільця многочленів $K[X]$. Це поле можна трактувати також як поле, одержане з поля K приєднанням елемента $X \in K[X]$. Елемент X є трансцендентним над K , це випливає з означення многочленів.

17.1 Підполя поля $K(X)$

Поле $K(X)$ складається з елементів вигляду $\alpha = \frac{f(X)}{g(X)}$, де $f(X), g(X) \in K[X]$. Елементи $\alpha \in K$ будемо називати *константами*, всі елементи поля $K(X)$ будемо називати *раціональними функціями*. У записі $\alpha = \frac{f(X)}{g(X)}$ раціональної функції, то многочлени $f(X)$ і $g(X)$ вважатимемо взаємно простими. Введемо *степінь* раціональної функції α : $\deg \alpha =$

$\max\{\deg f, \deg g\}$.

Теорема 120. Нехай $\alpha \in K(X)$, $\alpha \notin K$, $\deg \alpha = n \geq 1$. Тоді α трансцендентний над полем K елемент, X алгебраїчний над $K(\alpha)$ і $[K(X) : K(\alpha)] = n$.

Доведення. Доведемо спочатку, що елемент X алгебраїчний над $K(\alpha)$. Для цього розглянемо многочлен $\alpha g(X) - f(X) \in K(\alpha)[X]$. $g(X)$ є ненульовим многочленом, нехай b_k — який-небудь його ненульовий коефіцієнт. Тоді $b_k \alpha - a_k$ ненульовий коефіцієнт многочлена $\alpha g(X) - f(X)$ (тут a_k і b_k — коефіцієнти при X^k многочленів $f(X), g(X) \in K(\alpha)[X]$). Це означає, що X — алгебраїчний над $K(\alpha)$.

Доведемо, що α — трансцендентний над K . Якби це було не так, то α був би коренем деякого незвідного многочлен степеня m , тоді з теоремою 92 $[K(\alpha) : K] = m$, тому $[K(X) : K] = [K(X) : K(\alpha)] \cdot [K(\alpha) : K] \leq mn$. Звідси випливало б, що X алгебраїчний над K . Одержані суперечність.

Тепер доведемо, що $[K(X) : K(\alpha)] = n$. Для цього досить показати, що многочлен $\alpha g(Y) - f(Y)$ незвідний над $K(\alpha)$. Якби це було не так, то цей многочлен розкладався б на множники в кільці $K[\alpha, Y]$ і один з цих множників не залежав би від α , бо наш многочлен має степінь 1 за α . Тому ми мали б у кільці $K[\alpha, Y]$

$$\alpha g(Y) + f(Y) = h(Y) (\alpha g_1(Y) + f_1(Y)).$$

Але звідси випливає, що многочлени $f(Y)$ і $g(Y)$ мають спільний множник $h(Y)$, а вони в нас взаємно прості. Одержані суперечність показує, що $\alpha g(Y) + f(Y)$ незвідний, отже, X є коренем незвідного многочлен степеня n з коефіцієнтами з поля $K(\alpha)$ і з теореми 92 випливає, що $[K(X) : K(\alpha)] = n$. \square

17.2 Теорема Люрота

Теорема 121. Коєсне підполе поля раціональних функцій, що складається не лише з констант, ізоморфне полю раціональних функцій.

Доведення. Нехай ми маємо підполе M : $K \subsetneq M \subset K(X)$. Нехай $\alpha \in M$, $\alpha \notin K$. Розглянемо поле $K(\alpha)$. Маємо $K(\alpha) \subset M \subset K(X)$. За попередньою теоремою 120 $[K(X) : K(\alpha)] < \infty$, тому і $[K(X) : M] < \infty$. Скінченне розширення є алгебраїчним, отже, X алгебраїчний над M . Нехай X є коренем незвідного многочлена $\tilde{f}(T)$ степеня n з коефіцієнтами з поля M :

$$\tilde{f}(T) = T^n + a_{n-1}T^{n-1} + \cdots + a_0. \quad (17.2.1)$$

Коефіцієнти a_i многочлена (17.2.1) є деякими раціональними функціями від X . Домножимо многочлен (17.2.1) на спільний знаменник коефіцієнтів a_i , а тоді розділимо одержаний многочлен з коефіцієнтами з $K[X]$ на найбільший спільний дільник коефіцієнтів. Одержано многочлен

$$f(X, T) = b_n(X)T^n + b_{n-1}(X)T^{n-1} + \cdots + b_0(X).$$

Нехай m — степінь многочлена $f(X, T)$ за X .

Коефіцієнти $a_i(X) = \frac{b_i(X)}{b_n(X)}$ не можуть бути всі незалежними від X , бо тоді X був би алгебраїчним над K . Позначимо через α будь-який з коефіцієнтів a_i , що залежить від X : $\alpha = \frac{b_i(X)}{b_n(X)}$. Запишемо цей дріб у нескоротному вигляді $\alpha = \frac{g(X)}{h(X)}$. Маємо $\deg g(X) \leq m$ і $\deg h(X) \leq m$. Многочлен $g(T) - \alpha h(T) \in M[T]$ ненульовий і має корінь $T = X$, тому цей многочлен ділиться на $\tilde{f}(T)$ в кільці $M[T]$

$$g(T) - \alpha h(T) = \tilde{f}(T)p(T).$$

Підставимо $\alpha = \frac{g(X)}{h(X)}$ і домножимо на $h(X)$. Одержано

$$h(X)g(T) - g(X)h(T) = f(X, T)q(X, T), \quad (17.2.2)$$

де $q(X, T)$ — многочлен від T з коефіцієнтами з $K[X]$. Порівнюючи степені по X у лівій і правій частині рівності (17.2.2), одержуємо, що многочлен $q(X, T)$ не залежить від X , тому (використовуючи симетрію відносно X і T у (17.2.2) зліва) він не залежить і від T . Тому $q(X, T) = q_0 \in K$ і ми маємо

$$h(X)g(T) - g(X)h(T) = q_0 \cdot f(X, T).$$

Звідси випливає, що степені многочлена $f(X, T)$ за X і за T одинакові: $m = n$. Крім цього, обов'язково $\deg g = n$ оскільки $\deg h = n$. Отже, $\deg \alpha = n$. Розглянемо башту полів

$$K \subset K(\alpha) \subset M \subset K(X).$$

Маємо, використовуючи теорему 120,

$$n = [K(X) : K(\alpha)] = [K(X) : M] \cdot [M : K(\alpha)] = n \cdot [M : k(\alpha)].$$

Звідси випливає, що $[M : K(\alpha)] = 1$, тому $M = K(\alpha)$. Але α трансцендентний елемент, і тому з теореми 92 випливає, що $K(\alpha) \simeq K(X)$. \square

18 Скінченні поля

18.1 Кількість елементів скінченного поля

Скінченне поле з q елементів прийнято позначати \mathbb{F}_q . Простим підполем поля \mathbb{F}_q може бути лише поле $\mathbb{Z}/p\mathbb{Z}$. У такому випадку характеристика поля \mathbb{F}_q дорівнює p , де p просте число.

Твердження 122. Поле \mathbb{F}_q складається з p^n елементів, де $p = \text{char}\mathbb{F}_q$, n — додатне натуральне число.

Доведення. Поле \mathbb{F}_q є розширенням свого простого під поля $\mathbb{Z}/p\mathbb{Z}$. Отже, \mathbb{F}_q — скінченновимірний лінійний простір над полем $\mathbb{Z}/p\mathbb{Z}$. Якщо e_1, \dots, e_n — база $\mathbb{Z}/p\mathbb{Z}$ -простору \mathbb{F}_q , то кожен елемент з \mathbb{F}_q однозначно записується у вигляді лінійної комбінації $\alpha_1 e_1 + \dots + \alpha_n e_n$, де $\alpha_i \in \mathbb{Z}/p\mathbb{Z}$. Всього існує p^n таких лінійних комбінацій. Тому $q = p^n$. \square

Приклад. Поле з p^n елементів можна одержати з допомогою приєднання до поля $\mathbb{Z}/p\mathbb{Z}$ кореня α незвідного над $\mathbb{Z}/p\mathbb{Z}$ многочлен степеня n . Наприклад, поле з 8 елементів може бути побудоване за допомогою приєднання до поля $\mathbb{Z}/2\mathbb{Z}$ кореня многочлена $X^3 + X + 1 \in \mathbb{Z}/2\mathbb{Z}[X]$. Многочлен $X^3 + X + 1$ незвідний над $\mathbb{Z}/2\mathbb{Z}$ тому, що він не має коренів в $\mathbb{Z}/2\mathbb{Z}$, якби він був звідний, то в його розкладі на незвідні множники знайшовся б лінійний множник і многочлен мав би корінь у $\mathbb{Z}/2\mathbb{Z}$.

Нехай α — корінь многочлен $X^2 + X + 1$. Будемо вважати, що α є елементом алгебраїчного замикання $\overline{\mathbb{Z}/2\mathbb{Z}}$ поля $\mathbb{Z}/2\mathbb{Z}$. Використовуючи теорему 120 п. 17.1, маємо

$$\begin{aligned} \mathbb{Z}/2\mathbb{Z}(\alpha) &= \{a_0 + a_1\alpha + a_2\alpha^2 \mid a_i \in \mathbb{Z}/2\mathbb{Z}\} = \\ &= \{0, 1, \alpha, 1 + \alpha, \alpha^2, 1 + \alpha^2, \alpha + \alpha^2, 1 + \alpha + \alpha^2\}. \end{aligned}$$

Мультиплікативна група поля $\mathbb{Z}/2\mathbb{Z}(\alpha)$ складається з 7 елементів, тому вона циклічна і будь-який елемент, відмінний від 1, є її твірним. Зокрема, α — твірний елемент цієї групи. Знайдемо всі степені α , використовуючи в обчисленнях тотожність $\alpha^3 = \alpha + 1$, яка означає, що α корінь многочлен $X^3 + X + 1$.

n	1	2	3	4	5	6	7
α^n	α	α^2	$\alpha + 1$	$\alpha^2 + \alpha$	$\alpha^2 + \alpha + 1$	$\alpha^2 + 1$	1

У цьому прикладі ми зробили висновок про циклічність мультиплікативної групи поля $\mathbb{Z}/2\mathbb{Z}(\alpha)$, використовуючи той факт, що вона складається з 7 (7 просте число!) елементів.

Але мультиплікативна група поля з 9 елементів складається з 8 елементів, і в цьому випадку її циклічність неочевидна. Зрештою ми вже доводили, що *мультиплікативна група довільного скінченного поля є циклічною* (див. “Алгебра і теорія чисел”).

18.2 \mathbb{F}_q — поле розкладу многочлена $X^q - X$

Нехай L/K — розширення полів. Біективний гомоморфізм $\sigma: L \rightarrow L$ такий, що $\sigma(a) = a$ для всіх $a \in K$, називають *автоморфізмом поля* L над полем K .

Лема 123. Якщо \mathbb{F}_q — скінченне поле, що складається з $q = p^n$ елементів, то для кожного i , $1 \leq i \leq n$ відображення $\sigma^i: \mathbb{F}_q \rightarrow \mathbb{F}_q$, $\sigma^i(\alpha) = \alpha^{p^i}$ є автоморфізмом поля \mathbb{F}_q над \mathbb{F}_p . Всі ці n автоморфізмів є різними і не існує інших автоморфізмів поля \mathbb{F}_q .

Доведення. Доведемо спочатку, що $\sigma^1 = \sigma$ є автоморфізмом. Для цього зауважимо, що для простого числа p у формулі бінома Ньютона

$$(\alpha + \beta)^p = \alpha^p + \sum_{k=1}^{p-1} C_p^k \alpha^{p-k} \beta^k + \beta^p \quad (18.2.1)$$

всі біноміальні коефіцієнти $C_p^k = \frac{p!}{k!(p-k)!}$ діляться на p . Тому якщо $\alpha, \beta \in \mathbb{F}_{p^n}$, то з (18.2.1) одержуємо $(\alpha + \beta)^p = \alpha^p + \beta^p$. Крім цього, очевидно, $(\alpha\beta)^p = \alpha^p\beta^p$. Це означає, що $\sigma: L \rightarrow L$ є гомоморфізмом.

Покажемо, що σ ін'єктивне відображення: якщо $\sigma(\alpha) = \sigma(\beta)$, тобто $\alpha^p = \beta^p$, то $\alpha^p - \beta^p = (\alpha - \beta)^p = 0$, звідси $\alpha = \beta$. Нарешті, використаємо той факт, що ін'єктивне відображення скінченної множини в себе є сюр'єктивним. Отже, σ — автоморфізм. далі, σ^i є добутком автоморфізму σ на себе i разів, тому σ^i — теж автоморфізм. Для доведення, що автоморфізми $\sigma, \sigma^2, \dots, \sigma^n$ — різні, перевіримо, що коли α — твірний елемент циклічної групи $\mathbb{F}_{p^n}^*$, то $\sigma(\alpha), \sigma^2(\alpha), \dots, \sigma^n(\alpha)$ всі різні. Якби $\sigma^i(\alpha) = \sigma^j(\alpha)$ для $1 \leq i < j \leq n$, то $\sigma^{j-i}(\alpha) = \alpha$, тобто $\alpha^{p^{j-i}} - \alpha = 0$, звідки $\alpha^{p^{j-i}-1} = 1$. Ми одержали, що порядок α не більший, ніж $p^{j-i} - 1 < p^n - 1$. Це суперечить теоремі про те, що порядок скінченної циклічної групи дорівнює порядку її твірної.

Нарешті, той факт, що не існує інших автоморфізмів поля \mathbb{F}_q випливає з наслідку 111, де потрібно взяти $K = \mathbb{F}_p$, $L = \mathbb{F}_{p^n}$. \square

Зауваження 124. Для кожного $\alpha \in \mathbb{F}_q$, $\sigma^n(\alpha) - \alpha = \alpha^{p^n} - \alpha = \alpha(\alpha^{p^n-1} - 1) = 0$, бо для ненульового α маємо $\alpha^{p^n-1} = 1$ за наслідком з теореми Лагранжа, а для $\alpha = 0$ це очевидно. Отже, $\sigma^n(\alpha) = \alpha$ і $\sigma^n = 1_{\mathbb{F}_q}$.

Доведемо тепер, що для кожного $q = p^n$ існує єдине з точністю до еквівалентності скінченнє поле, що складається з q елементів. Інакше кажучи, для кожного додатного натурального n існує єдине розширення степеня n поля \mathbb{F}_p і так само існує єдине розширення степеня m поля \mathbb{F}_{p^n} для кожного m . Це випливає з такої теореми.

Теорема 125. Поле \mathbb{F}_{p^n} є полем розкладу многочлен

$$X^{p^n} - X \tag{18.2.2}$$

з коефіцієнтами з поля \mathbb{F}_p .

Доведення. Нехай K — поле розкладу многочлен (18.2.2). Відомо (теорема 119), що поле розкладу многочлен однозначно з точністю до еквівалентності визначається цим многочленом. Покажемо, що кожен елемент поля \mathbb{F}_{p^n} є коренем многочлена (18.2.2). Для 0 це очевидно. Якщо $\alpha \neq 0$, то $\alpha \in \mathbb{F}_{p^n}^*$. За наслідком з теореми Лагранжа маємо, що $\alpha^{p^n-1} = 1$ бо $\alpha^{p^n} - \alpha = 0$, тобто α корінь многочлена (18.2.2). Звідси $\mathbb{F}_q \subset K$. Тепер перевіримо, що множина M коренів многочлена (18.2.2) є полем з q елементів. Нехай $\alpha, \beta \in M$. Тоді з леми 123, зокрема, випливає, що $(\alpha + \beta)^{p^n} = \alpha^{p^n} + \beta^{p^n}$. Далі, $\alpha^{p^n} + \beta^{p^n} = \alpha + \beta$, Оскільки α і β — корені многочлена (18.2.2). Звідси одержуємо, що $(\alpha + \beta)^{p^n} = \alpha + \beta$, тобто $\alpha + \beta \in M$. Так само $(\alpha\beta)^{p^n} = \alpha\beta$, тобто $\alpha\beta \in M$. Отже, множина M замкнена відносно операцій додавання і множення. Звідси випливає, що множина M є підполем поля розкладу K , Оскільки поле розкладу є найменшим полем, що містить всі корені многочлена, то $M = K$. Тому $\mathbb{F}_q = K$. \square

Наслідок 126. Для кожного $n \in \mathbb{N}$ існує єдине розширення поля \mathbb{F}_p степеня n .

Доведення. Це розширення є полем розкладу многочлен $X^{p^n} - X \in \mathbb{F}_p[X]$. \square

Наслідок 127. Для кожного $m \in \mathbb{N}$ існує єдине розширення поля \mathbb{F}_q степеня m , де $q = p^n$.

Доведення. Маємо башту розширень

$$\mathbb{F}_p \subset \mathbb{F}_q \subset \mathbb{F}_{q^m} = \mathbb{F}_{p^{mn}}.$$

Тут $\mathbb{F}_{p^{mn}}$ поле розкладу многочлена $X^{p^{mn}} - X$, друге включення випливає з того, що многочлен $X^{p^n} - X$ ділить многочлен $X^{p^{mn}} - X$.

Справді, якщо $\alpha \in \mathbb{F}_{p^n}$, то $\alpha^{p^n} = \alpha$. Звідси, $(\alpha^{p^n})^{p^n} = \alpha^{p^{2n}} = \alpha^{p^n} = \alpha$, і т.д., $\alpha^{p^{mn}} = \alpha$, тобто кожний корінь многочлена $X^{p^n} - X$ є коренем многочлена $X^{p^{mn}} - X$. \square

18.3 Підполя скінченного поля

Теорема 128. *Нехай \mathbb{F}_{p^m} та \mathbb{F}_{p^n} два скінчені поля. Тоді \mathbb{F}_{p^m} є підполем поля \mathbb{F}_{p^n} тоді і тільки тоді, коли $m|n$.*

Доведення. Якщо \mathbb{F}_{p^m} підполе поля \mathbb{F}_{p^n} , то \mathbb{F}_{p^n} скінченне розширення поля \mathbb{F}_{p^m} . Нехай $d = [\mathbb{F}_{p^n} : \mathbb{F}_{p^m}]$. Тоді $p^n = (p^m)^d$, Оскільки кожний елемент $\alpha \in \mathbb{F}_{p^n}$ однозначно записується у вигляді лінійної комбінації $a_1e_1 + \dots + a_de_d$, де e_1, \dots, e_d база \mathbb{F}_{p^n} над \mathbb{F}_{p^m} і коефіцієнти a_1, \dots, a_d незалежно один від одного можуть набувати p^m значень. Тому $n = md$.

Навпаки, якщо $n = md$, то \mathbb{F}_{p^m} поле розкладу многочлена $X^{p^m} - X$, \mathbb{F}_{p^n} поле розкладу многочлена $X^{p^{md}} - X$. Включення $\mathbb{F}_{p^m} \subset \mathbb{F}_{p^n}$ випливає з подільності $X^{p^m} - X | X^{p^{md}} - X$ (див. доведення наслідку 127). \square

Приклад. Поле $\mathbb{F}_{2^{30}}$ має такі підполя: $\mathbb{F}_2, \mathbb{F}_{2^2}, \mathbb{F}_{2^3}, \mathbb{F}_{2^5}, \mathbb{F}_{2^6}, \mathbb{F}_{2^{10}}, \mathbb{F}_{2^{15}}, \mathbb{F}_{2^{30}}$.

18.4 Незвідні многочлени над полем \mathbb{F}_q

Теорема 129. а) Для кожного натурального n , $n \geq 1$, існує незвідний многочлен $f(X) \in \mathbb{F}_q[X]$ степеня n .

б) В результаті приєднання до \mathbb{F}_q коренів двох різних незвідних над \mathbb{F}_q многочленів степеня n одержуються однакові розширення.

в) Якщо α — корінь незвідного многочлен $f(X) = a_0 + a_1X + \dots + a_nX^n \in \mathbb{F}_q[X]$, то $\alpha, \alpha^q, \dots, \alpha^{q^{n-1}}$ — всі його різні корені.

Доведення. а) Нехай \mathbb{F}_{q^n} — розширення поля \mathbb{F}_q степеня n . Розглянемо твірний елемент γ циклічної групи $\mathbb{F}_{q^n}^*$. Якщо $p(X) \in \mathbb{F}_q[X]$ — мінімальний многочлен елемента γ , то $p(X)$ незвідний. Далі, очевидно, $[\mathbb{F}_{q^n} : \mathbb{F}_q] = n$, тому $\deg p(X) = n$.

б) Одержано розширення \mathbb{F}_{q^n} , що є полями розкладу многочлена $X^{q^n} - X \in \mathbb{F}_p[X]$.

в) Піднесемо тотожність $a_0 + a_1\alpha + \dots + a_n\alpha^n = 0$ до степеня q^i . Використавши лему 123 та рівності $a_i^q = a_i$, $0 \leq i \leq n$, які вірні тому що

$a_i \in \mathbb{F}_q$, одержуємо

$$a_0 + a_1 \alpha^{q^i} + \cdots + a_n (\alpha^{q^i})^n = 0.$$

Це означає, що α^{q^i} корені нашого многочлена. Доведемо, що корені $\alpha, \alpha^q, \dots, \alpha^{q^{n-1}}$ всі різні. Для цього потрібно використати той факт, що коли α корінь незвідного многочлен $f(X)$ і $g(\alpha) = 0$ для многочлен $g(X)$, то $f(X)|g(X)$. Справді, розділимо $g(X)$ на $f(X)$ з остачею: $g(X) = f(X)d(X) + r(X)$. Звідси $r(\alpha) = 0$, тому $r(X) = 0$, бо в іншому випадку ми одержали б, що найбільший спільний дільник многочленів $f(X)$ і $r(X)$ не дорівнює 1, що суперечить незвідності многочлена $f(X)$.

Тепер, якби серед коренів $\alpha, \alpha^q, \dots, \alpha^{q^{n-1}}$ були одинакові, наприклад, $\alpha^{q^i} = \alpha^{q^j}$, $0 \leq i < j \leq n - 1$, то підносячи обидві частини останньої рівності до степеня q^{n-j} , ми одержали б $\alpha^{q^{n-j+i}} = \alpha^{q^n} = \alpha$. Це означає, що α є коренем многочлена $X^{q^s} - X$, де $s = n - j + i < n$. З доведеного випливає, що многочлен $f(X) \in \mathbb{F}_q[X]$ ділить многочлен $X^{q^s} - X \in \mathbb{F}_q[X]$. Тому поле розкладу многочлен $f(X)$ міститься у полі розкладу многочлена $X^{q^s} - X$. Але поле розкладу $f(X)$ містить не менше, як q^n елементів, а поле розкладу $X^{q^s} - X$ містить q^s елементів. Звідси випливає, що $q^n \leq q^s$ бо $n \leq s$. Одержанна суперечність завершує доведення. \square

Приклад. Над полем \mathbb{F}_2 многочлени $X^3 + X + 1$ та $X^3 + X^2 + 1$ незвідні. Тому приєднавши до \mathbb{F}_2 корінь одного з цих многочленів одержимо поле \mathbb{F}_8 .

Вправи

- Нехай $\alpha = \sqrt[3]{2}$, $j = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$. Показати, що $\mathbb{Q}(\alpha) \simeq \mathbb{Q}(j\alpha) \simeq \mathbb{Q}(j^2\alpha)$ і $\mathbb{Q}(\alpha, j\alpha) = \mathbb{Q}(\alpha, \sqrt{-3})$. Знайти $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}]$ та $[\mathbb{Q}(\sqrt[3]{2}, \sqrt{-3}) : \mathbb{Q}]$.
- Що можна сказати про степінь над \mathbb{Q} підполя поля \mathbb{C} , породженого радикалом раціонального числа, тобто про $[\mathbb{Q}(\sqrt[n]{\frac{a}{b}}) : \mathbb{Q}]$, де $a, b \in \mathbb{Q}$? Навести приклади.
- Нехай X — змінна. Показати, що $1, X$ — база розширення $\mathbb{Q}(X)/\mathbb{Q}(X^2)$ та розширення $\mathbb{Q}(X)/\mathbb{Q}(X^2 + X)$. Описати поле $\mathbb{Q}(X^2) \cap \mathbb{Q}(X^2 + X)$.

4. Розглянемо множину всіх розширень поля K , що містяться в даному полі L . Показати, що це гратка (тобто частково впорядкована множина, у якій для кожних двох її елементів існують точна верхня і точна нижня грані), де точною верхнею грани розширень K_1/K і K_2/K є їх композит K_1K_2 , тобто найменше підполе в L , що містить $K_1 \cup K_2$, точною нижньою грани є перетин $K_1 \cap K_2$.

Припустимо, що $[L : K] < \infty$.

- a) Довести, що $[K_1K_2 : K] \leq [K_1 : K] \cdot [K_2 : K]$.
 б) Якщо одне з чисел $[K_1 : K]$ або $[K_2 : K]$ дорівнює 2, то довести, що

$$[K_1K_2 : K] = [K_1 : K] \cdot [K_2 : K] \Leftrightarrow K_1 \cap K_2 = K.$$

Чи вірно це у всіх випадках? Розглянути випадки, коли K_1 та K_2 породжені над \mathbb{Q} числами: 1) $i, \sqrt{2}$; 2) $\sqrt[3]{2}, \sqrt[3]{3}$; 3) $-\frac{1}{2} + \frac{\sqrt{-3}}{2}, \sqrt[3]{2}$.

5. Показати, що елемент α — алгебраїчний над полем \mathbb{Q} і обчислити у вигляді многочлен від α обернені до $\alpha + 1$ та $\alpha^3 + 1$, якщо: а) $\alpha = \sqrt{2} + \sqrt{3}$; б) $\alpha = 1 + \sqrt[4]{2}$; в) $\alpha = \frac{1}{1+\sqrt{2}}$; г) α — корінь многочлен $X^3 - X - 1$; д) α — корінь многочлен $X^2 + iX + 2$.
6. Якщо L — скінченне розширення поля K , то кожне кільце A таке, що $K \subset A \subset L$ є полем.
7. Довести, що якщо L/M і M/K — алгебраїчні розширення, то L/K також алгебраїчне розширення і навпаки.
8. Нехай L/K — скінченне розширення поля K , x — елемент алгебраїчний над K . Чи залишається база L/K базою $L(x)/K(x)$?
9. Довести, що існують дійсні трансцендентні числа над \mathbb{Q} . Вказівка: показати, що алгебраїчне замикання поля \mathbb{Q} є зліченою множиною.
10. Нехай $K_n = \mathbb{Q}(\sqrt[2^n]{2})$, $n = 1, 2, \dots$, $L = \bigcup_{n=1}^{\infty} K_n$. Довести, що L/\mathbb{Q} — нескінченне алгебраїчне розширення.
11. Нехай L — підполе простого розширення $K(\alpha)$, $K \subset L \subset K(\alpha)$. Довести, що мінімальний многочлен елемент α над L ділить мінімальний многочлен елемент α над K . Показати, що поле L породжується коефіцієнтами мінімального многочленадля α над L . Вивести звідси, що існує лише скінчені кількість проміжних між K та $K(\alpha)$ полів.

12. Якщо K_1 та K_2 — проміжні між K та L поля і $[K_1 : K]$ та $[K_2 : K]$ взаємно прості, то довести, що $K_1 \cap K_2 = K$.
13. Довести, що для нескінченного поля K з того, що для скінченно-го розширення L/K існує тільки скінченна кількість проміжних між K та L полів, випливає, що L/K — просте розширення.
14. Нехай $L = \mathbb{F}_2(X, Y)$ — поле раціональних функцій від двох змінних над \mathbb{F}_2 . Показати, що його степінь над $K = \mathbb{F}_2(X^2, Y^2)$ дорівнює 4 і що квадрат кожного елемента поля L належить K . Довести, що розширення L/K не є простим, вказавши нескінченну множину проміжних полів.
15. Нехай L — поле розкладу многочлен $f(X) \in K[X]$, $\deg f(X) = n$. Показати, що $[L : K] \leq n!$. Знайти степінь над \mathbb{Q} полів розкладу многочленів $X^3 - 2$ та $X^4 - 2$.
16. Чи може скінченне розширення поля \mathbb{Q} містити нескінченну кількість коренів з 1?
17. Для поля K , що містить корені n -го степеня з 1, знайти елементи $a, b \in K$ такі, що многочлени $X^n - a$ та $X^n - b$ мають одне і те ж поле розкладу. Довести, що існування цілого m , $(m, n) = 1$ з властивістю $\sqrt[n]{a^m b^{-1}} \in K$ є необхідною і достатньою умовою для цього.
18. Нехай $K(x)$ — поле раціональних функцій від X з коефіцієнтами з поля K . $\alpha \in K(x)$. Довести, що $K(\alpha) = K(x)$ тоді і тільки тоді, коли $\alpha = \frac{ax+b}{cx+d}$, де $a, b, c, d \in K$ і $a \neq 0$ або $c \neq 0$.
19. Довести, що всі автоморфізми поля раціональних функцій $K(x)$ над полем K мають вигляд $\sigma(x) = \frac{ax+b}{cx+d}$, де $a, b, c, d \in K$, $ad - bc \neq 0$ і $\sigma(a) = a$ для всіх $a \in K$.
20. Нехай $m \in \mathbb{N}$. Довести, що

$$\sum_{x \in \mathbb{F}_q} x^m = \begin{cases} -1, & \text{якщо } m \geq 1 \text{ і } q - 1 \mid m, \\ 0, & \text{в інших випадках} \end{cases}$$

(вважаємо тут, що $x^0 = 1$ для всіх $x \in \mathbb{F}_q$).

21. (теорема Шевальє-Варнінга). Нехай

$$f_i(X_1, X_2, \dots, X_n) \in \mathbb{F}_q[X_1, \dots, X_n], \quad 1 \leq i \leq k,$$

і нехай

$$\{(c_1, \dots, c_n) \in \mathbb{F}_q^n \mid f_i(c_1, \dots, c_n) = 0, 1 \leq i \leq k\}.$$

Довести, що $N \equiv 0 \pmod{p}$, де $p = \text{char}\mathbb{F}_q$. Вказівка: розглянути многочлен $f = \prod_{i=1}^k (1 - f_i^{q-1})$. Довести, що

$$N \equiv \sum_{x_1, \dots, x_n \in \mathbb{F}_q^n} f(x_1, \dots, x_n) \equiv 0 \pmod{p},$$

використавши задачу 20.

22. Довести, що кожна скінченна підгрупа мультиплікативної групи K^* довільного поля K є циклічною.
23. Довести, що многочлени $X^2 + 1$ та $X^2 + X + 4$ незвідні над полем \mathbb{F}_{11} . Вивести звідси, що фактор-кільця $\mathbb{F}_{11}[X]/(X^2 + 1)$ і $\mathbb{F}_{11}[X]/(X^2 + X + 4)$ є полями і ці поля ізоморфні.
24. Знайти який-небудь твірний елемент мультиплікативної групи поля: а) \mathbb{F}_4 , б) \mathbb{F}_7 , в) \mathbb{F}_{25} , г) \mathbb{F}_{27} .
25. Довести, що для кожного елемента $\alpha \in \mathbb{F}_q$ існує лише один елемент $\beta \in \mathbb{F}_q$ з властивістю $\beta^p = \alpha$.
26. Довести, що коли $\text{char}\mathbb{F}_q \neq 2$, то елемент $\alpha \in \mathbb{F}_q^*$ має в \mathbb{F}_q квадратний корінь тоді і тільки тоді, коли $\alpha^{\frac{q-1}{2}} = 1$.
27. Довести, що для заданого натурального числа k елемент $\alpha \in \mathbb{F}_q^*$ є k -им степенем деякого елемента з поля \mathbb{F}_q тоді і тільки тоді, коли $\alpha^{\frac{q-1}{d}} = 1$, де $d = (q-1, k)$.
28. Довести, що для заданого $k \in \mathbb{N}$ кожен елемент поля \mathbb{F}_q є k -тим степенем деякого елемента з цього поля тоді і тільки тоді, коли $(q-1, k) = 1$.
29. Нехай $k \in \mathbb{N}$, $k|q-1$ і $a \in \mathbb{F}_q$, причому рівняння $x^k = a$ не має розв'язків в \mathbb{F}_q . Довести, що це рівняння має розв'язки в \mathbb{F}_{q^m} , якщо $k|m$. Довести, що якщо k — просте число, то справедливе і обернене твердження.
30. Показати, що для $a \in \mathbb{F}_q$ і $n \in \mathbb{N}$, $n \neq 0$ многочлен $X^{q^n} - X + na$ ділиться на $X^q - X + a$ в кільці $\mathbb{F}_q[X]$.

31. Довести, що кожний квадратний многочлен з $\mathbb{F}_q[X]$ має корінь в $\mathbb{F}_{q^2}[X]$.

Теорія Галуа виникла із задачі про розв'язування в радикалах алгебраїчних рівнянь. Загальновідома формула для розв'язування квадратного рівняння була встановлена ще у далеку давнину. Методи розв'язування рівнянь 3-го та 4-го степенів були знайдені в XVI ст. Протягом трьох наступних століть без особливого успіху проводились пошуки формул для розв'язування рівнянь 5-го і вищих степенів. Нарешті, в 1824 р. Н.Х. Абелль довів, що загальне алгебраїчне рівняння степеня $n \geq 5$ у радикалах не розв'язується. Тому постало питання про необхідні та достатні умови, яким повинні задовольняти коефіцієнти рівняння, щоб воно розв'язувалося в радикалах, тобто могло бути зведене до ланцюжка двочленних рівнянь вигляду $x^n - a = 0$. Відповідь не це питання була знайдена Е. Галуа у 1832 р.

Ідеї Галуа мали вирішальний вплив на розвиток алгебри протягом цілого століття. Незважаючи на те, що теорія Галуа інтенсивно розвивалася і узагальнювалася у багатьох напрямках, дотепер залишилося багато нерозв'язаних задач цієї теорії. Наприклад, невідомо чи для кожної скінченної групи G існує рівняння над полем раціональних чисел \mathbb{Q} , що має цю групу в якості своєї групи Галуа.

19 Розширення Галуа

19.1 Теорема про простоту сепара贝尔но породжених розширень

Нгадаємо, що розширення L/K називають *простим*, якщо $L = K(\alpha)$ для деякого $\alpha \in L$. Цей елемент α називають *примітивним елементом* простого розширення L/K .

Приклад. Покажемо, що поле розкладу L многочлена $X^3 + pX + q \in \mathbb{Q}[X]$ є простим. Маємо $L = \mathbb{Q}(a, b, c)$, де a, b, c — корені нашого многочлена. Оскільки $a+b+c=0$, то $L = \mathbb{Q}(a, b)$. Очевидно, що $\mathbb{Q}(a, b) = \mathbb{Q}(a, b, c) \supset \mathbb{Q}(b - c)$. Покажемо, що і $\mathbb{Q}(b - c) \supset \mathbb{Q}(a, b)$. Маємо

$$(b - c)^2 = (b + c)^2 - 4bc = a^2 - 4bc = a^2 + \frac{4q}{a} = \frac{-pa + 3q}{a} = -p + \frac{3q}{a}.$$

Звідси $a \in \mathbb{Q}(b - c)$. Тому $\mathbb{Q}(b - c) = \mathbb{Q}(a, b - c) = \mathbb{Q}(a, b + c, b - c) \supset \mathbb{Q}(a, b)$.

Означення 130. алгебраїчний елемент $\alpha \in L/K$ називають *сепараційним* над K , якщо мінімальний многочлен елемента α над K не має кратних коренів.

Приклади.

1) Якщо $\text{char} K = 0$, то кожний алгебраїчний над K елемент є сепараційним над K . Справді, в цьому випадку похідна мінімального многочлена для α є завжди ненульовим многочленом. Оскільки мінімальний многочлен незвідний, то не існує спільних коренів многочленів $f(X)$ і $f(X)'$. Отже, мінімальний многочлен для α не має кратних коренів.

2) Нехай $K = \mathbb{F}_2(X)$ — поле раціональних функцій від X з коефіцієнтами з поля \mathbb{F}_2 . Приєднаємо до K корінь многочлена $Y^2 - X \in \mathbb{F}_2[X]$. Позначимо цей корінь \sqrt{X} . Тоді $(Y^2 - X)' = 2Y = 0$ — похідна многочлена $Y^2 - X$ є нульовим многочленом. Це означає, що \sqrt{X} є двократним коренем незвідного над $\mathbb{F}_2(X)$ многочлена $Y^2 - X$.

Теорема 131. Нехай $L = K(\alpha_1, \dots, \alpha_n)$ — скінченно породжене алгебраїчне розширення поля K , причому елементи $\alpha_1, \dots, \alpha_n$ сепараційні. Тоді розширення L просте.

Доведення. Припустимо спочатку, що поле K нескінченне. Міркуючи за індукцією, досить знайти елемент γ в полі $K(\alpha, \beta)$, де α, β сепараційні над K , такий, що $K(\gamma) = K(\alpha, \beta)$. Нехай $p_\alpha[X]$ та $p_\beta[X]$ мінімальні многочлени над K відповідно для елементів α та β . Вважаємо, що $\deg p_\alpha = r$, $\deg p_\beta = s$. Нехай $\alpha_1, \alpha_2, \dots, \alpha_r$ — всі корені многочлен p_α , $\beta_1, \beta_2, \dots, \beta_s$ — всі корені многочлен p_β . Будемо шукати елемент γ у вигляді $\gamma = \alpha + t\beta$, де $t \in K$. Виберемо t так, щоб елементи $\alpha_i + t\beta_j$ були попарно різними для всіх i, j , $1 \leq i \leq r$, $1 \leq j \leq s$. Такий вибір можливий: потрібно взяти $t \in K$ з властивістю $t \neq \frac{\alpha_{i'} - \alpha_i}{\beta_{j'} - \beta_j}$ для всіх i, i', j, j' , $1 \leq i, i' \leq r$, $1 \leq j, j' \leq s$. Таке t існує, Оскільки поле K нескінченне.

Тепер, для так вибраного t , одержуємо, що β єдиний спільний корінь многочленів $p_\beta(X)$ та $p_\alpha(\gamma - tX)$. Це означає, що многочлен $X - \beta$ є найбільшим спільним дільником многочленів $p_\beta(X)$ та $p_\alpha(\gamma - tX)$. З алгоритму Евклід знаходження найбільшого спільного дільника випливає, що $X - \beta \in K(\gamma)[X]$. Зокрема, $\beta \in K(\gamma)$. Звідси випливає, що і $\alpha \in K(\gamma)$, тому $K(\gamma) = K(\alpha, \beta)$.

Нехай тепер K — скінченне поле з q елементів, L — скінченне розширення поля K , $[L : K] = m$. Тоді $L = \mathbb{F}_{q^m}$. Ми знаємо, що мультиплікативна група $\mathbb{F}_{q^m}^*$ є циклічною, вона породжується деяким елементом $\alpha \in L$. Тоді $L = K(\alpha)$. \square

19.2 Теореми про сепарабельні розширення

Означення 132. алгебраїчне розширення L/K називають *сепарабельним*, якщо кожний елемент $\alpha \in L$ є сепарабельним над K , тобто є коренем сепарабельного многочлена. Многочлен $f(X) \in K[X]$ називають *сепарабельним*, якщо він не має кратних коренів.

Теорема 133. Нехай L/K скінченне розширення, $[L : K] = n$. Тоді наступні твердження еквівалентні:

- 1) L/K — сепарабельне;
- 2) $L = K(\alpha)$, де α — сепарабельний над K ;
- 3) якщо $\sigma: K \rightarrow K'$ — вкладення, то існує розширення L' поля K' і n продовжень $\sigma_1, \dots, \sigma_n$ вкладення σ до вкладень $\sigma_i: L \rightarrow L'$.

Доведення. 1) \Rightarrow 2). Скінченне розширення L/K є, очевидно, скінченно породженим: $L = K(u_1, \dots, u_n)$, де u_1, \dots, u_n — база K -лінійного простору L . З теореми 131 про простоту сепарабельно породжених розширень випливає, що L породжується над K одним елементом, тобто $L = K(\alpha)$.

2) \Rightarrow 3). Нехай $p(X) = a_0 + a_1X + \dots + a_nX^n$ — мінімальний многочлен елемента α . Тоді $\deg p = n$. Візьмемо в якості L' поле розкладу многочлен $p^\sigma(X) = \sigma(a_0) + \sigma(a_1)X + \dots + \sigma(a_n)X^n \in K'[X]$. Многочлен $p^\sigma(X)$ — сепарабельний, Оскільки з $p(X)' \neq 0$ випливає $p^\sigma(X)' \neq 0$. Тому в L' многочлен $p^\sigma(X)$ має n різних коренів $\beta_1, \beta_2, \dots, \beta_n$. n гомоморфізмів $\sigma_1, \dots, \sigma_n: L \rightarrow L'$ таких, що $\sigma_i(a) = \sigma(a)$ для $a \in K$ і $\sigma_i(\alpha) = \beta_i$, $1 \leq i \leq n$, і є шуканими продовженнями вкладення σ .

3) \Rightarrow 1). Нехай $\gamma \in L$, $q(X)$ — мінімальний многочлен для γ над K і $M = K(\gamma)$. Якщо γ — несепарабельний елемент, то многочлен $q(X)$ має кратні корені. Кожне продовження одиничного гомоморфізму $1_K: K \rightarrow K$ до вкладення $\sigma: M \rightarrow M'$ поля M в поле M' повинне переводити γ в корінь многочлена $q(X)$. Тому існує менше, ніж $m = [M : K] = \deg q(X)$ таких продовжень. Застосовуючи теорему 110 про кількість вкладень, одержуємо, що для кожного вкладення $\sigma: M \rightarrow M'$ існує не більше, ніж $[L : M]$ продовжень цього вкладення до вкладень $\tau: L \rightarrow L'$. В результаті існує менше, ніж $n = [L : K] = [L : M] \cdot [M : K]$ продовжень 1_K до вкладень $\sigma: L \rightarrow L'$. \square

19.3 Теореми про поле розкладу

Теорема 134. Для скінченного розширення L/K еквівалентні такі умови:

- 1) L — поле розкладу деякого многочлен $f(X) \in K[X]$;

2) якщо $\sigma: L \rightarrow L'$ — вкладення і $\sigma(a) = a$ для кожного $a \in K$, то $\sigma(L) = L$;

3) будь-який незвідний многочлен $p(X) \in K[X]$, що має корінь в L , розкладається в L на лінійні множники.

Доведення. 1) \Rightarrow 2) Нехай $L = K(\alpha_1, \dots, \alpha_n)$, де α_i — корені многочлена $f(X)$. З того, що $\sigma(a) = a$ для всіх $a \in K$ випливає $\sigma(K(\alpha_1, \dots, \alpha_n)) = K(\sigma(\alpha_1), \dots, \sigma(\alpha_n)) = K(\alpha_{i_1}, \dots, \alpha_{i_n})$, де $\alpha_{i_1}, \dots, \alpha_{i_n}$ — деяка перестановка коренів $\alpha_1, \dots, \alpha_n$. Тому $\sigma(L) = L$.

2) \Rightarrow 3) Якщо $\alpha \in L$ корінь незвідного многочлен $p(X) \in K[X]$, і β інший корінь цього ж многочлена, то маємо гомоморфізм $K(\alpha) \rightarrow K(\beta)$, який α відображає у β , а всі елементи з поля K залишають незмінними. За теоремою ?? про продовження гомоморфізмів цей гомоморфізм може бути продовжений до вкладення $\sigma: L \rightarrow L'$. Маємо $\sigma(L) = L$, отже, $\beta = \sigma(\alpha) \in L$, тому всі корені многочлен $p(X)$ містяться в L і $p(X)$ розкладається в L на лінійні множники.

3) \Rightarrow 1) розширення L/K — скінченнопороджене, оскільки воно скінченне. $L = K(\gamma_1, \dots, \gamma_m)$. Нехай $p_i(X)$ мінімальний многочлен для γ_i над K , $p(X) = \prod_{i=1}^m p_i(X)$. Тоді поле L є полем розкладу многочлена $p(X)$. \square

19.4 Відповідності Галуа

Для розширення L/K позначимо $\text{Aut}(L/K)$ — множину всіх автоморфізмів поля L над K . Інакше кажучи, $\text{Aut}(L/K)$ складається з усіх біективних відображень $\sigma: L \rightarrow L$, що є гомоморфізмами полів і мають властивість $\sigma(a) = a$ для всіх $a \in K$.

Твердження 135. $\text{Aut}(L/K)$ — група відносно звичайного множення автоморфізмів.

Доведення. $\text{Aut}(L/K)$ є підмножиною $\text{Aut}L$ — групи всіх біективних відображень з L в L . Доведемо, що $\text{Aut}(L/K)$ група. Для цього досить перевірити для цієї підмножини умови критерію підгрупи. Маємо для

$u, v, u', v' \in L; \sigma, \sigma_1, \sigma_2 \in \text{Aut}(L/K); \sigma(u') = u, \sigma(v') = v$:

$$\begin{aligned} (\sigma_1\sigma_2)(u \stackrel{+}{\cdot} v) &= \sigma_1 \left(\sigma_2(u \stackrel{+}{\cdot} v) \right) = \sigma_1 \left(\sigma_2(u) \stackrel{+}{\cdot} \sigma_2(v) \right) = (\sigma_1\sigma_2)(u) \stackrel{+}{\cdot} \sigma_1\sigma_2)(v), \\ \sigma^{-1}(u \stackrel{+}{\cdot} v) &= \sigma^{-1} \left(\sigma(u') \stackrel{+}{\cdot} \sigma(v') \right) = \\ &= (\sigma^{-1}\sigma)(u') \stackrel{+}{\cdot} (\sigma^{-1}\sigma)(v') = u' \stackrel{+}{\cdot} v' = \sigma^{-1}(u) \stackrel{+}{\cdot} \sigma^{-1}(v), \\ (\sigma_1\sigma_2)(a) &= \sigma_1(\sigma_2(a)) = \sigma_1(a) = a, \\ \sigma^{-1}(a) &= a. \end{aligned}$$

Тут знак $\stackrel{+}{\cdot}$ використано в тому розумінні, що виписані рівності вірні як для додавання, так і для множення. \square

Введемо позначення:

$$L^H = \{\alpha \in L \mid \sigma(\alpha) = \alpha \text{ для всіх } \sigma \in H\},$$

де L/K — розширення поля K , а H — підгрупа групи $\text{Aut}(L/K)$.

Твердження 136. L^H — підполе поля L , що містить поле K : $K \subset L^H \subset L$.

Доведення. Досить перевірити, що L^H — замкнене відносно операцій додавання і множення та переходу до обернених елементів. Маємо для $\sigma \in H, u, v \in L^H$:

$$\begin{aligned} \sigma(u \stackrel{+}{\cdot} v) &= \sigma(u) \stackrel{+}{\cdot} \sigma(v) = u \stackrel{+}{\cdot} v, \quad \sigma(-u) = -\sigma(u) = -u, \\ \sigma(u^{-1}) &= \sigma(u)^{-1} = u^{-1}. \end{aligned}$$

Введемо позначення:

$$G^M = \{\sigma \in G \mid \sigma(\alpha) = \alpha \text{ для всіх } \alpha \in M\},$$

де $G = \text{Aut}(L/K)$, M — підполе поля L , що містить поле K , тобто $K \subset M \subset L$. \square

Твердження 137. G^M є підгрупою групи G .

Доведення. Доведення цього твердження, по-суті, повторює прості і нудні обчислення, використані у кінці доведення твердження 135. Тому пропонуємо це доведення в якості вправи. \square

Означення 138. Нехай L/K розширення полів, $G = \text{Aut}(L/K)$. Якщо H підгрупа групи G , то за твердженням 136 їй ставиться у відповідність підполе L^H поля L ; якщо M підполе поля L , то з твердженням 137 йому ставиться у відповідність підгрупа G^M групи G . Ці відповідності називають *відповідностями Галуа*.

Твердження 139. a) Відповідності Галуа обертають включення, тобто:

$$H_1 \subset H_2 \Leftrightarrow L^{H_1} \supset L^{H_2},$$

$$M_1 \subset M_2 \Leftrightarrow G^{M_1} \supset G^{M_2}.$$

$$b) H \subset G^{L^H} \text{ i } M \subset L^{G^M}.$$

Доведення. Все це безпосередньо випливає з означень. Обмежимося доведенням частини б). Якщо $\sigma \in H$, то для кожного $\alpha \in L^H$ $\sigma(\alpha) = \alpha$, отже, $\sigma \in G^{L^H}$. Якщо $\alpha \in M$, то для кожного $\sigma \in G^M$ $\sigma(\alpha) = \alpha$, отже, $\alpha \in L^{G^M}$. \square

19.5 Нерівність $[L : L^H] \leq |H|$

Нехай L/K — скінченне розширення, $G = \text{Aut}(L/K)$. З наслідку 111 теореми про кількість вкладень випливає, що група G скінчена. Нехай H підгрупа групи G і $|H|$ порядок підгрупи H .

Теорема 140. $[L : L^H] \leq |H|$.

Доведення. Міркуємо від супротивного: нехай $|H| = m$ і $[L : L^H] > m$. Ми одержимо суперечність, якщо доведемо, що для $n > m$ кожна система елементів $u_1, \dots, u_n \in L$ є лінійно залежною над L^H . Нехай $H = \{\sigma_1, \dots, \sigma_m\}$. Розглянемо в просторі L^m систему векторів

$$v_1 = (\sigma_1^{-1}(u_1), \dots, \sigma_m^{-1}(u_1)),$$

.....

$$v_n = (\sigma_1^{-1}(u_n), \dots, \sigma_m^{-1}(u_n)).$$

-і вектори лінійно залежні в L^m , тобто існують такі скаляри $\lambda_1, \dots, \lambda_n \in L$, які не всі дорівнюють 0, що $\sum_{i=1}^n \lambda_i v_i = 0$. Звідси маємо

$$\sum_{i=1}^n \lambda_i \sigma_j^{-1}(u_i) = 0 \tag{19.5.1}$$

для всіх j , $1 \leq j \leq m$.

Не зменшуючи загальності, можна вважати, що $\lambda_1 \neq 0$, тоді, домножуючи рівності (19.5.1) на будь-який елемент з поля L , можна вважати λ_1 будь-яким елементом поля L . Виберемо λ_1 так, щоб $\sum_{j=1}^m \sigma_j(\lambda_1) \neq 0$. Можливість такого вибору випливає з леми Артіна (лема 109) про лінійну незалежність характерів.

Тепер подіємо на j -у рівність (19.5.1) автоморфізмом σ_j і додамо результати. Отримаємо: $\sum_{j=1}^m \sum_{i=1}^n \sigma_j(\lambda_i) u_i = 0$ бо $\sum_{i=1}^n \left(\sum_{j=1}^m \sigma_j(\lambda_i) \right) u_i = 0$. Тут $\sum_{j=1}^m \sigma_j(\lambda_i) \in L^H$, Оскільки для $\sigma \in H$ елементи $\sum_{j=1}^m \sigma_j(\lambda_i)$ та $\sum_{j=1}^m \sigma_j(\lambda_i)$ відрізняються лише перестановкою доданків. Крім того, як було зазначено раніше, $\sum_{j=1}^m \sigma_j(\lambda_1) \neq 0$. Це означає, що вектори v_1, \dots, v_n є лінійно залежними над L^H . \square

19.6 Теореми про нормальні розширення

Означення 141. розширення L/K називають *нормальним*, якщо $L^{\text{Aut}(L/K)} = K$. Інакше кажучи, розширення L/K нормальнє, якщо для кожного елемента $\alpha \in L$, $\alpha \notin K$ існує автоморфізм $\sigma \in \text{Aut}(L/K)$ для якого $\sigma(\alpha) \neq \alpha$.

Приклади.

1) Нехай $L = \mathbb{Q}(\sqrt{2})$. $\text{Aut}(L/\mathbb{Q}) = \{1, \sigma\}$, де $\sigma(a + b\sqrt{2}) = a - b\sqrt{2}$. Звідси

$$L^{\text{Aut}(L/\mathbb{Q})} = \{a + b\sqrt{2} \mid a + b\sqrt{2} = a - b\sqrt{2}; a, b \in \mathbb{Q}\} = \mathbb{Q}.$$

Отже, $\mathbb{Q}(\sqrt{2})$ нормальнє розширення поля \mathbb{Q} .

2) Нехай $L = \mathbb{Q}(\sqrt[4]{2})$. Якщо $\sigma \in \text{Aut}(L/\mathbb{Q})$, то $\sigma(\sqrt[4]{2}) = \sqrt[4]{2}$ бо $\sigma(\sqrt[4]{2}) = -\sqrt[4]{2}$. Звідси випливає, що елемент $\alpha = a_0 + a_1\sqrt[4]{2} + a_2\sqrt[4]{4} + a_3\sqrt[4]{8}$ міститься в $L^{\text{Aut}(L/\mathbb{Q})}$ тоді і тільки тоді, коли

$$a_0 - a_1\sqrt[4]{2} + a_2\sqrt[4]{4} - a_3\sqrt[4]{8} = a_0 + a_1\sqrt[4]{2} + a_2\sqrt[4]{4} + a_3\sqrt[4]{8},$$

тобто тоді і тільки тоді, коли $\alpha = a_0 + a_2\sqrt[4]{4} = a_0 + a_2\sqrt{2}$. Тому в цьому випадку $L^{\text{Aut}(L/\mathbb{Q})} = \mathbb{Q}(\sqrt{2}) \supsetneqq \mathbb{Q}$ і розширення $\mathbb{Q}(\sqrt[4]{2})$ не є нормальним.

Теорема 142. Для скінченного сепарабельного розширення L/K еквівалентні такі умови:

- 1) L/K нормальнє розширення;
- 2) $|\text{Aut}(L/K)| = [L : K]$;
- 3) L поле розкладу сепарабельного многочлен $f(X) \in K[X]$.

Доведення. 1) \Rightarrow 2). Візьмемо в теоремі 140 $H = \text{Aut}(L/K)$. Одержано

$$[L : L^{\text{Aut}(L/K)}] = [L : K] \leq |\text{Aut}(L/K)|.$$

Протилежна нерівність $[L : K] \geq |\text{Aut}(L/K)|$ випливає з наслідку 111 теореми 110 про кількість вкладень.

2) \Rightarrow 3). Щойно згаданий наслідок 111 стверджує, що існує не більше, ніж $[L : K]$ продовжень одиничного гомоморфізму поля K до вкладень $\sigma: L \rightarrow L'$. Але з 2) випливає, що для кожного такого вкладення σ маємо $\sigma(L) = L$. Залишається застосувати теорему 134 про поле розкладу.

3) \Rightarrow 1). Нехай $\alpha \in L \setminus K$ і нехай $p(X)$ мінімальний многочлен для α над K , і α' корінь многочлена $p(X)$ відмінний від α . Тоді $\alpha' \in L$ за теоремою 134 про поле розкладу. Ізоморфізм $\sigma: K(\alpha) \rightarrow K(\alpha')$, $\sigma(\alpha) = \alpha'$, $\sigma(a) = a$ для всіх $a \in K$ продовжується до автоморфізму $\tau \in \text{Aut}(L/K)$, для якого $\tau(\alpha) \neq \alpha$. \square

19.7 Група Галуа

Означення 143. Нормальне і сепарабельне розширення L/K називають *розширенням Галуа*. Для розширення Галуа L/K групу $\text{Aut}(L/K)$ називають *групою Галуа* і позначають $\text{Gal}(L/K)$. *Групою Галуа сепарабельного многочлена* $f(X) \in K[X]$ називають групу Галуа поля розкладу цього многочлена, цю групу позначають G_f .

Твердження 144. *Група Галуа многочлена* $f(X) \in K[X]$, $\deg f(X) = n$, *изоморфна деякій підгрупі групи підстановок* S_n .

Доведення. Доведення цього простого і важливого факту ґрунтуються на зауваженні, що кожен автоморфізм $\sigma \in G_f$ переводить корінь α многочлена f у корінь $\sigma(\alpha)$ цього ж многочлена: якщо $a_0 + a_1\alpha + \dots + a_n\alpha^n = 0$, то $\sigma(a_0 + a_1\alpha + \dots + a_n\alpha^n) = a_0 + a_1\sigma(\alpha) + \dots + a_n\sigma(\alpha)^n = 0$, Оскільки $\sigma(a_i) = a_i$, $0 \leq i \leq n$. Розглянувши обмеження автоморфізму σ на множину коренів $\{\alpha_1, \dots, \alpha_n\}$ многочлен $f(X)$, одержимо підстановку

$$\begin{pmatrix} \alpha_1, & \alpha_2, & \dots, & \alpha_n \\ \alpha_{i_1}, & \alpha_{i_2}, & \dots, & \alpha_{i_n} \end{pmatrix}, \quad (19.7.1)$$

де $\alpha_{i_k} = \sigma(\alpha_k)$.

Нехай автоморфізму $\tau \in G_f$ відповідає підстановка

$$\begin{pmatrix} \alpha_{i_1}, & \alpha_{i_2}, & \dots, & \alpha_{i_n} \\ \alpha_{j_1}, & \alpha_{j_2}, & \dots, & \alpha_{j_n} \end{pmatrix}. \quad (19.7.2)$$

Добутку $\tau\sigma$ автоморфізмів σ і τ відповідає підстановка

$$\begin{pmatrix} \alpha_1, & \alpha_2, & \dots, & \alpha_n \\ \alpha_{j_1}, & \alpha_{j_2}, & \dots, & \alpha_{j_n} \end{pmatrix},$$

тобто добуток підстановок (19.7.1) і (19.7.2). маємо, отже, гомоморфізм $G_f \rightarrow S_n$. Очевидно, цей гомоморфізм ін'єктивний, тобто різним автоморфізмам поля розкладу відповідають різні підстановки.

Отже, група G_f ізоморфна деякій підгрупі групи S_n . \square

Приклади.

1) Поле \mathbb{C} є полем розкладу многочлен $X^2 + 1 \in \mathbb{R}[X]$. $[\mathbb{C} : \mathbb{R}] = 2$. Отже, $\text{Gal}(\mathbb{C}/\mathbb{R}) \simeq C_2$ — циклічна група другого порядку. Нетривіальний елемент $\sigma \in \text{Gal}(\mathbb{C}/\mathbb{R})$ діє так: $\sigma(x + iy) = x - iy$.

2) Нехай $f(X) = X^2 + pX + q \in \mathbb{Q}[X]$ незвідний над \mathbb{Q} многочлен. Якщо L поле розкладу многочлена $f(X)$, то $L = \mathbb{Q}(\sqrt{p^2 - 4q})$, $[L : \mathbb{Q}] = 2$ і $G_f \simeq C_2$.

3) Розглянемо поле L розкладу многочлена $f(X) = X^4 + X^2 + 1 \in \mathbb{Q}[X]$. Легко переконатися, що коренями цього многочлена є $j, j^2, -j, -j^2$, де $j = -\frac{1}{2} + \frac{\sqrt{-3}}{2}$. Отже, $L = \mathbb{Q}(j) = \mathbb{Q}(\sqrt{-3})$, $[L : \mathbb{Q}] = 2$ і $G_f \simeq C_2$.

4) Група Галуа многочлена третього степеня.

Розглянемо поле розкладу многочлен $X^3 + a_1X^2 + a_2X + a_3 \in K[X]$. Будемо вважати, що $\text{char}K \neq 2, 3$; тоді заміна $X' = X - \frac{a_1}{3}$ показує, що досить розглянути многочлен $f(X) = X^3 + pX + q \in K[X]$. Вже було показано (див. приклад в п. 19.1), що $K(a, b, c) = K(a-b)$, де a, b, c корені многочлена $f(X)$. Попробуємо знайти многочлен $g(X)$, коренями якого є різниці коренів многочлен $f(X)$, тобто $\pm(a-b), \pm(b-c), \pm(a-c)$. Для цього досить знайти многочлен від $Y = X^2$ з коренями $(a-b)^2, (b-c)^2, (a-c)^2$. Маємо $(a-b)^2 = (a+b)^2 - 4ab = c^2 + \frac{4q}{c}$. Але $c^3 = -pc - q$, тому $(a-b)^2 = \frac{c^3+4q}{c} = -p + \frac{3q}{c}$. Звідси випливає, що многочлен з коренями $(a-b)^2$ одержиться, якщо замінити X в $X^3 + pX + q$ на Y , де $Y = -p + \frac{3q}{X}$, тобто $X = \frac{3q}{Y+p}$. Звідси маємо рівняння для Y : $\frac{27q^3}{(Y+p)^3} + \frac{3pq}{Y+p} + q = 0$ оскільки $(Y+p)^3 + 3p(Y+p)^2 + 27q^2 = 0$, тобто $Y(Y+3p)^2 + 4p^3 + 27q^2 = 0$.

Зокрема, з формулами Вієта одержуємо, що $(a-b)^2(b-c)^2(a-c)^2 = -4p^3 - 27q^2 = \Delta$ — дискримінант многочлена $f(X)$. Очевидно, $\Delta = 0$ тоді і тільки тоді, коли многочлен $f(X)$ має кратний корінь. Різниці коренів многочлен $f(X)$ є коренями многочлена $g(X) = X^2(X^2 + 3p)^2 - \Delta$.

Група Галуа незвідного многочлена $X^3 + pX + q$ ізоморфна або A_3 або S_3 (переконайтесь у тому, що вона не може бути групою порядку 2).

Все залежить від того, чи многочлен $g(X)$ незвідний. Якщо він незвідний, то поле розкладу має степінь 6 над K і група Галуа ізоморфна S_3 . Якщо $g(X)$ звідний, то група Галуа поля $K(a, b, c) = K(a - b)$ ізоморфна групі A_3 .

Покажемо, що $g(X)$ незвідний тоді і тільки тоді, коли $\sqrt{\Delta} = (a - b)(b - c)(a - c) \notin K$. Якщо $\sqrt{\Delta} \in K$, то

$$g(X) = \left(X(X^2 + 3p) + \sqrt{\Delta} \right) \left(X(X^2 + 3p) - \sqrt{\Delta} \right).$$

Навпаки, якщо $g(X)$ звідний над K , то він обов'язково має незвідний множник степеня 3. Приймемо $g(X) = r(X)s(X)$, $\deg(r(X)) = 3$. З рівності $r(X)s(X) = r(-X)s(-X)$ випливає, що $r(X)$ ділить $r(-X)$ оскільки $s(-X)$. Вважаючи, що всі старші коефіцієнти дорівнюють 1, маємо $r(X) = -s(-X)$ бо $r(X) = -r(-X)$.

Якщо $r(X) = -r(-X)$, то $r(0) = 0$, отже, $g(0) = 0$ і $\Delta = 0$, що неможливо (f не має крім коренів). залишається випадок $r(X) = -s(-X)$, звідки $\sqrt{\Delta} = r(0) \in K$.

Підсумовуючи результати цих обчислень, маємо

$$\text{Gal}(L/K) \simeq \begin{cases} A_3, & \sqrt{\Delta} \in K, \\ S_3, & \sqrt{\Delta} \notin K. \end{cases}$$

20 Основна теорема теорії Галуа та її наслідки

20.1 Основна теорема теорії Галуа

Нехай L/K — скінченне розширення Галуа з групою Галуа $G = \text{Gal}(L/K)$. Відповідності Галуа — це два відображення. Одне з них відображає множину підполів поля L , що містять поле K , у множину підгруп групи G за правилом

$$M \mapsto G^M = \{\sigma \in G \mid \sigma(\alpha) = \alpha \ \forall \alpha \in M\},$$

а інше відображає множину підгруп групи G у множину підполів поля L за правилом

$$H \mapsto L^H = \{\alpha \in L \mid \sigma(\alpha) = \alpha \ \forall \sigma \in H\}.$$

Основна теорема теорії Галуа стверджує, що ці відображення є взаємно оберненими.

Теорема 145 (Основна теорема теорії Галуа). *Нехай L/K скінченне розширення Галуа. Відповідності Галуа є взаємно оберненими біективними відображеннями множини підгруп групи $G = \text{Gal}(L/K)$ і множини підполів M поля L , що містять поле K .*

Доведення. У нас все готове для того, щоб доведення цієї теореми було коротким. Потрібно довести, що $L^{G^M} = M$ і $G^{L^H} = H$. Включення $M \subset L^{G^M}$ та $H \subset G^{L^H}$ безпосередньо випливають з означення (див., також, твердження 139). Доведемо, що фактично вірні рівності $L^{G^M} = M$ та $G^{L^H} = H$.

$L^{G^M} = M$. Маємо $K \subset M \subset L$, розширення L/K нормальнє і сепарабельне. З теореми про нормальні розширення випливає, що L поле розкладу деякого сепарабельного многочлена з коефіцієнтами з поля K . Оскільки $K \subset M$, то очевидно, що L поле розкладу сепарабельного многочлена з коефіцієнтами з поля M . Тому L/M — розширення Галуа і зрозуміло, що $G^M = \text{Aut}(L/M)$. Тепер з нормальності розширення L/M одержуємо $L^{G^M} = L^{\text{Aut}(L/M)} = M$.

$G^{L^H} = H$. Маємо $|G^{L^H}| \leq [L : L^H] \leq |H|$, де перша нерівність випливає з теореми 110 про кількість вкладень, а друга нерівність це теорема 140. Отже, $|G^{L^H}| \leq |H|$, а Оскільки H є підгрупою скінченної групи G^{L^H} , то остання нерівність можлива лише тоді, коли $H = G^{L^H}$. \square

Наслідок 146. Якщо L/K скінченне розширення Галуа, то існує лише скінченна кількість підполів M поля L таких, що $K \subset M \subset L$.

Доведення. Це випливає з того, що $G = \text{Gal}(L/K)$ скінченна група порядку $[L : K]$, тому в G існує лише скінченна кількість підгруп. \square

20.2 Теорема про спряженість

Нехай L/K — розширення Галуа, M — підполе в L , $K \subset M \subset L$ і $\sigma \in G = \text{Gal}(L/K)$. Позначимо

$$\sigma(M) = \{\sigma\alpha \mid \alpha \in L\} \subset L.$$

Для підгрупи H групи G позначимо

$$\sigma H \sigma^{-1} = \{\sigma\tau\sigma^{-1} \mid \tau \in H\}.$$

Легко пересвідчитися в тому, що $\sigma(M)$ підполе поля L , $K \subset \sigma(M) \subset L$ і $\sigma H \sigma^{-1}$ підгрупа групи G .

Теорема 147. Нехай L/K розширення Галуа і нехай за відповідністю Галуа підполю M , $K \subset M \subset L$, відповідає підгрупа H групи $G = \text{Gal}(L/K)$. Тоді підполю σM відповідає підгрупа $\sigma H\sigma^{-1}$, тобто при відповідностях Галуа спряженим під полям відповідають спряжені підгрупи.

Доведення. Потрібно довести, що $L^{\sigma H\sigma^{-1}} = \sigma M$, якщо $L^H = M$. Для цього перевіримо, що $L^{\sigma H\sigma^{-1}} \subset \sigma M$ і $\sigma M \subset L^{\sigma H\sigma^{-1}}$.

$L^{\sigma H\sigma^{-1}} \subset \sigma M$. Якщо $\alpha \in L^{\sigma H\sigma^{-1}}$, то для кожного $\tau \in H$ $\sigma\tau\sigma^{-1}(\alpha) = \alpha$, $\tau\sigma^{-1}(\alpha) = \sigma^{-1}(\alpha)$. Звідси $\sigma^{-1}(\alpha) = \beta \in M$, $\alpha = \sigma(\beta) \in \sigma M$.

$\sigma M \subset L^{\sigma H\sigma^{-1}}$. Нехай $\alpha = \sigma\beta \in \sigma M$, $\beta \in M$. Тоді для кожного $\tau \in H$ маємо $\sigma\tau\sigma^{-1}(\alpha) = \sigma\tau\sigma^{-1}\sigma(\beta) = \sigma\tau(\beta) = \alpha$, тобто $\alpha \in L^{\sigma H\sigma^{-1}}$. \square

20.3 Теорема про нормальність

Теорема про нормальність дає відповідь на запитання, при яких умовах підполе розширення Галуа саме є розширенням Галуа. Перед тим, як формулювати цю теорему, зробимо декілька зауважень про сепарабельність та нормальність для башти полів.

Нехай $K \subset M \subset L$ башта скінчених розширень поля K . розширення L/K сепарабельне тоді і тільки тоді, коли L/M і M/K сепарабельні. Справді, якщо L/K — сепарабельне, то (Оскільки $M \subset L$) кожен елемент поля M сепарабельний над K і (Оскільки $K \subset M$) кожний елемент поля L є коренем сепарабельного многочлен з коефіцієнтами з поля M .

Навпаки, якщо M/K і L/M — сепарабельні, то за теоремою 133 про сепарабельні розширення існує $[M : K]$ продовжень однічного гомоморфізму 1_K до вкладень $M \rightarrow M'$, і для кожного вкладення $\sigma: M \rightarrow M'$ існує $[L : M]$ продовження σ до вкладень $\sigma: L \rightarrow L'$. Разом існує $[L : K]$ продовження 1_K , тому L/K сепарабельне за теоремою про сепарабельні розширення.

Для нормальних розширень ситуація не така приемна. Зокрема, підрозширення нормального розширення вже не обов'язково є нормальним розширенням. Наприклад, $K = \mathbb{Q} \subset M = \mathbb{Q}(\sqrt[4]{2}) \subset L = \mathbb{Q}(i, \sqrt[4]{2})$. Поле L/K є полем розкладу многочлена $X^4 - 2 \in \mathbb{Q}[X]$, отже, L/K нормальнє розширення. Але, як відомо (згадайте приклад з п. 19.6) розширення M/K не є нормальним.

Теорема 148. Нехай L/K скінченне розширення Галуа з групою Галуа $G = \text{Gal}(L/K)$, M підполе поля L , $K \subset M \subset L$. розширення M/K нормальнє тоді і тільки тоді, коли відповідна полю M за основною

теоремою теорії Галуа підгрупа H є нормальнюю в G . У цьому випадку $\text{Gal}(M/K) \simeq G/H$.

Доведення. Якщо M/K — нормальнє розширення, то можна означити гомоморфізм

$$F: \text{Gal}(L/K) \rightarrow \text{Gal}(M/K),$$

$F(\sigma) = \sigma|_M$ обмеження автоморфізму σ на поле M . Взагалі, можна лише стверджувати, що $\sigma|_M$ — вкладення поля M у поле L , але, Оскільки M/K нормальне, то за теоремою 142 воно є полем розкладу многочленів з коефіцієнтами з поля K , тоді за теоремою 134 про поле розкладу $\sigma|_M(M) = M$. Тому F коректно означене відображення і, очевидно, що F гомоморфізм груп.

F сюр'єктивний гомоморфізм, що випливає з теореми про продовження гомоморфізмів (п. ??, розд. ??): кожен автоморфізм поля M може бути продовжений до автоморфізму поля L (тут використовуємо нормальність розширень M/K та L/K). Обчислимо $\text{Ker } F$. $\text{Ker } F = \{\sigma \in G \mid \sigma(\alpha) = \alpha \forall \alpha \in M\} = H$. Отже, з одного боку, H — нормальнна підгрупа, оскільки H є ядром гомоморфізму груп, з іншого боку $G/H \simeq \text{Im } F = \text{Gal}(M/K)$ за теоремою про гомоморфізм.

Залиється довести, що коли H нормальнна підгрупа групи G , то $M = L^H$ нормальнє розширення поля K . Нехай σ вкладення M в L . Тоді σ продовжується до автоморфізму поля L над K за теоремою про продовження гомоморфізмів та за нормальністю L/K . Тепер з теореми про спряженість маємо $\sigma(M) = L^{\sigma H \sigma^{-1}} = L^H = M$. Отже, σ автоморфізм поля M і M/K нормальнє розширення за теоремами 134 та 142. \square

20.4 Теорема про трансляцію

Пригадаємо, що для двох підполів K_1 і K_2 поля L композитом $K_1 K_2$ пілів K_1 і K_2 називають найменше підполе поля L , що містить K_1 і K_2 .

Теорема 149. *Нехай L/K — скінченне розширення Галуа, K' — розширення поля K і $L' = LK'$ — композит полів L і K' (вважаємо, що всі ці поля є під полями деякого поля E). Тоді L'/K' розширення Галуа і $\text{Gal}(L'/K') \simeq \text{Gal}(L/K)^{K' \cap L}$.*

Доведення. Оскільки L/K поле розкладу сепарабельного многочлена над K (тому, що L/K розширення Галуа), то L'/K' поле розкладу цього ж многочлена над K' , отже, L'/K' розширення Галуа. Нехай $\sigma \in \text{Gal}(L'/K')$. Тоді обмеження $\sigma|_L$ -автоморфізму σ на поле L є K -автоморфізмом поля L , а відображення $F(\sigma) = \sigma|_L$ є, очевидно, гомоморфізмом груп $\text{Gal}(L'/K')$ та $\text{Gal}(L/K)$. Обчислимо $\text{Ker } F$. Якщо $\sigma \in \text{Ker } F$,

то $\sigma|_L = 1_L$. Тоді $\sigma = 1_{L'}$, бо $L' = LK'$, і σ залишає незмінними елементи з K' . Отже, $\text{Ker } F = \{1_{L'}\}$. Тому $\text{Gal}(L'/K') \simeq \text{Im } F$. Тепер $L^{\text{Im } F} = K' \cap L$ і $\text{Im } F = \text{Gal}(L/K)^{K' \cap L}$, що й потрібно було довести. \square

20.5 алгебраїчна замкненість поля \mathbb{C}

Доведемо, що поле комплексних чисел \mathbb{C} алгебраїчно замкнене. Цей факт випливає з наступної теореми.

Теорема 150. *Нехай K поле характеристики 0, а L його розширення степеня 2. Припустимо, що виконуються такі умови:*

- a) *коежен многочлен непарного степеня з коефіцієнтами з поля K має корінь у полі K ;*
- b) *для коєзного $\alpha \in L$ многочлен $X^2 - \alpha$ має корінь у полі L .*

Тоді поле L алгебраїчно замкнене.

Доведення. Перш за все зауважимо, що з умови б) випливає, що кожний квадратний тричлен $X^2 + pX + q \in L[X]$ має корінь в L . Оскільки його корені обчислюються з формулою $x_{1,2} = \frac{-p \pm \sqrt{p^2 - 4q}}{2}$.

Нехай $f(X) \in L[X]$ незвідний многочлен, і M' його поле розкладу над L . розширення L/K і M'/L скінчені і сепарабельні, отже, (це вже було обґрунтоване в п. 20.3) розширення M'/K скінченне і сепарабельне. За теоремою 131 про простоту скінченних сепарабельних розширень існує $\alpha \in M'$ з властивістю $M' = K(\alpha)$. Приєднаємо до M' всі корені мінімального многочлен для α над K . Одержано башту розширень $K \subset L \subset M' \subset M$, де M/K скінченне розширення Галуа.

Нехай $G = \text{Gal}(M/K)$ і H силовська 2-підгрупа групи G . Розглянемо відповідне підгрупі H , за основною теоремою теорії Галуа, підполе M^H . Маємо

$$K \subset M^H \subset M,$$

де $[M : M^H] = |H| = 2^n$, і $[M^H : K] = 2k + 1$ для деякого $k \in \mathbb{N}$. Звідси випливає, що $[M^H : K] = 1$, оскільки якщо $\gamma \in M^H$ і $p(X)$ мінімальний многочлен для γ , то $[K(\gamma) : K] = \deg p(X)$ непарне число, тому $p(X)$ має корінь в K , отже, $\deg p(X) = 1$ і $\gamma \in K$.

Ми одержали, що $M^H = K$, отже, $[M : K] = [M : L] \cdot [L : K] = 2^{m+1}$, де $[M : L] = 2^m$. Доведемо, що $m = 0$.

Якщо $m = 1$, то $[M : L] = 2$ і $M = L(\alpha)$, де α корінь незвідного многочлена степеня 2. Але з умови б) випливає, що не існує незвідних многочленів степеня 2 над L . Отже, припущення, що $m = 1$ веде до суперечності.

Якщо $m > 1$, то в групі $\text{Gal}(L/M)$, що має порядок 2^m існує підгрупа H_1 порядку 2^{m-1} (існування такої підгрупи випливає з теоретико-групової леми нижче).

Нехай M_1 відповідне підгрупі H_1 підполе поля M . Маємо

$$L \subset M_1 \subset M,$$

де $[M : M_1] = 2^{m-1}$, отже, $[M_1 : L] = 2$, але раніше вже було показано, що це веде до суперечності.

Остаточно маемо $m = 0$, тобто $[M : L] = 1$, отже, $M = L$ і $f(X)$ має в полі L корінь.

Таким чином, наша теорема буде доведеною, якщо ми доведемо таке твердження.

Лема 151. *Нехай p просте число, G — p -група порядку p^m . Тоді для кожного k , $0 \leq k \leq m$, в G існує підгрупа порядку p^k .*

Доведення. Міркуємо за індукцією. Якщо $m = 1$, то доводити нічого. Припустимо, що лема доведена для всіх p -груп порядків менших, ніж p^m , і розглянемо p -групу G порядку p^m . Відомо, що група G має нетривіальний центр C , який теж є p -групою. Підгрупа C має елементи порядку p , отже, і підгрупи порядку p : якщо $a \in C$, то порядок елемента a дорівнює p^s , де $s \leq m$ за наслідком з теореми Лагранжа. Якщо $s > 1$, то елемент $a^{p^{s-1}}$ має порядок p .

Нехай $H \subset C$ підгрупа порядку p групи G , H нормальна підгрупа, Оскільки вона міститься в центрі. Розглянемо фактор-групу G/H і канонічний гомоморфізм $f: G \rightarrow G/H$. маємо $|G/H| = p^{m-1}$ і за припущенням індукції для кожного $k \leq m$ в G/H існує підгрупа \tilde{G} порядку p^{k-1} . Прообраз $f^{-1}(\tilde{G})$ є підгрупою групи G порядку p^k . Лему доведено. \square

Наслідок 152. *Поле \mathbb{C} алгебраїчно замкнене.*

Доведення. Досить перевірити, що поля \mathbb{R} і \mathbb{C} задовольняють умови з формулування теореми. $\mathbb{C} = \mathbb{R}(i)$, тому $[\mathbb{C} : \mathbb{R}] = 2$. Кожен многочлен непарного степеня з дійсними коефіцієнтами має дійсний корінь. Справді, Оскільки для такого многочлене $f(X)$ маємо $\lim_{X \rightarrow -\infty} f(X) = -\infty$ і

$\lim_{X \rightarrow +\infty} f(X) = +\infty$, то існує інтервал дійсної осі, на кінцях якого неперервна функція $f(X)$ приймає значення різних знаків. З теореми, яку в курсі математичного аналізу називають теоремою Коші про проміжне

значення, випливає, що існує $\alpha \in \mathbb{R}$ з властивістю $f(\alpha) = 0$, тобто многочлен $f(X)$ має дійсний корінь.

Для перевірки умови б) теореми досить зауважити, що з кожного комплексного числа добувається квадратний корінь. Цей факт добре відомий з I семестру, але для повноти нагадаємо його. Якщо $\alpha = a + bi$, то $\sqrt{\alpha}$ знаходимо з рівності $(x + iy)^2 = a + bi$, яка рівносильна системі рівнянь

$$\begin{cases} x^2 - y^2 = a, \\ 2xy = b. \end{cases}$$

Розв'язуючи цю систему, одержимо

$$x^2 = \frac{a + \sqrt{a^2 + b^2}}{2}, \quad y^2 = \frac{-a + \sqrt{a^2 + b^2}}{2}.$$

Одержані вирази для x^2 та y^2 невід'ємні, тому можна знайти x і y . Знаки в x та y беремо так, щоб $2xy = b$. \square

Приклади.

1) Нехай L поле розкладу многочлена $(X^2 - 2)(X^3 - 3) \in \mathbb{Q}[X]$. Якщо перенумерувати корені $\sqrt{2}, -\sqrt{2}, \sqrt{3}, -\sqrt{3}$ цього многочлена числами 1, 2, 3, 4, то $\text{Gal}(L/K) = \{1, (1, 2), (3, 4), (1, 2)(3, 4)\} \cong C_2 \times C_2$. Ця група має три власні циклічні підгрупи $\{1, (1, 2)\}$, $\{1, (3, 4)\}$ та $\{1, (1, 2)(3, 4)\}$. Відповідні цим підгрупам за відповідністю Галуа під поля є такими: $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{3})$ та $\mathbb{Q}(\sqrt{6})$.

2) *Формули Кардано* для многочлена 3-го степеня. Нехай K поле. Припустимо, що $\text{char } K \neq 2, 3$ і що $\sqrt{-3} \in K$, приєднавши, якщо потрібно до K корінь многочлена $X^2 + 3$. Позначимо через L поле розкладу незвідного многочлена $f(X) = X^3 + pX + q \in K[X]$, і через $a, b, c \in L$ корені $f(X)$, $j = -\frac{1}{2} + \frac{\sqrt{-3}}{2}$.

Розглянемо елементи $x_1 = a + bj + cj^2$ і $x_2 = a + cj + bj^2$. Якщо подіяти на елементи a, b, c групою S_3 і назвати образи елементів x_1 та x_2 спряженими до x_1 , то множина шести спряжених до x_1 елементів є такою:

$$\{x_1, jx_1, j^2x_1, x_2, jx_2, j^2x_2\}. \quad (20.5.1)$$

Зазначимо, що

$$\begin{aligned} x_1x_2 &= (a + bj + cj^2)(a + cj + bj^2) = \\ &= (a^2 + b^2 + c^2) + (ab + ac + bc)(j + j^2) = \\ &= a^2 + b^2 + c^2 - (ab + ac + bc) = (a + b + c)^2 - 3(ab + ac + bc) = -3p, \end{aligned}$$

Оскільки $a + b + c = 0$.

Якщо елементи множини (20.5.1) піднести до кубу, то серед кубів залишиться тільки два різних: x_1^3 та x_2^3 . Звідси випливає, що $[K(x_1^3) : K] = 2$ і що x_1^3 є коренем многочлена 2-го степеня над K . Щоб знайти цей многочлен, зауважимо, що зі зроблених обчислень випливає $x_1^3 x_2^3 = -27p^3$. Крім цього, $x_1^3 + x_2^3 = (x_1 + x_2)^3 - 3x_1 x_2 (x_1 + x_2) = (2a - b - c)^3 + 9p(2a - b - c) = (3a)^3 + 27ap = 27(a^3 + ap) = -27q$.

Отже, x_1^3 та x_2^3 є коренями многочлена $X^2 + 27qX - 27p^3$. Звідси

$$x_1 = \sqrt[3]{\frac{-27q + \sqrt{27(4p^3 + 27q^2)}}{2}}, \quad x_2 = \sqrt[3]{\frac{-27q - \sqrt{27(4p^3 + 27q^2)}}{2}},$$

де кубічні корені у виразах для x_1 та x_2 вибрані так, щоб $x_1 x_2 = -3p$. Тепер для коренів a, b, c многочлена $X^3 + pX + q$ маємо систему рівнянь

$$\begin{cases} a + b + c = 0, \\ a + bj + cj^2 = x_1, \\ a + bj^2 + cj = x_2, \end{cases}$$

розв'язавши яку, матимемо формулі для коренів a, b, c . Зокрема, додавши почленно рівняння нашої системи і використавши, що $j^3 = 1$ (тобто $1 + j + j^2 = 0$), одержимо

$$3a = x_1 + x_2$$

60

$$a = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}.$$

Вправа. Припустимо, що $G = \text{Gal}(L/K) \simeq S_3$. Тоді G має 6 підгруп. Спробуйте вказати відповідні цим підгрупам підполі поля L .

20.6 Група Галуа загального многочлена

Наведемо приклад розширення Галуа L/K з групою Галуа S_n . Нехай K поле, t_1, \dots, t_n алгебраїчно незалежні над K , інакше кажучи, поле $K(t_1, \dots, t_n)$ ізоморфне полю рациональних функцій від n змінних з коефіцієнтами з поля K . Нехай $s_1 = t_1 + \dots + t_n, s_2 = t_1 t_2 + \dots + t_{n-1} t_n, \dots, s_n = t_1 \dots t_n$. Це елементарні симетричні многочлени від t_1, \dots, t_n . З теореми про симетричні многочлени випливає, що s_1, \dots, s_n алгебраїчно незалежні над K і що кожен симетричний многочлен є многочленом

від елементарних симетричних многочленів. Формули Вієта показують, що поле $K(t_1, \dots, t_n)$ є полем розкладу многочлена $f(X) = \prod_{i=1}^n (X - t_i)$, коефіцієнтами якого є (з точністю до знаків) s_1, \dots, s_n . Тому поле $K(t_1, \dots, t_n)$ є полем розкладу многочлена $f(X) \in K(s_1, \dots, s_n)[X]$. Крім цього,

$$\text{Gal}(K(t_1, \dots, t_n)/K(s_1, \dots, s_n)) \simeq S_n.$$

Многочлен $f(X) = \prod_{i=1}^n (X - t_i)$, де t_1, \dots, t_n алгебраїчно незалежні над K називають *загальним многочленом степеня n*. Бачимо, що група Галуа загального многочлена над полем $K(s_1, \dots, s_n)$ ізоморфна групі S_n .

20.7 Формули Кардано для многочлена 4-го степеня

Нехай K деяке поле, $\text{char } K \neq 2, 3$. Розглянемо загальний многочлен 4-го степеня $f(T) = T^4 + s_1T^3 + s_2T^2 + s_3T + s_4$. Після заміни $T = X - \frac{s_1}{4}$ одержимо многочлен, що не містить одночлен з X^3 : $f(X) = X^4 + aX^2 + bX + c$. Нехай x_1, x_2, x_3, x_4 корені многочлена $f(X)$ і $L = K(a, b, c)(x_1, x_2, x_3, x_4)$ його поле розкладу. Розглянемо елемент $\alpha = x_1x_2 + x_3x_4 \in L$. Група Галуа многочлена $f(X)$ ізоморфна групі S_4 . Підгрупа групи S_4 , що залишає елемент α інваріантним, складається з восьми підстановок: $1, (1, 2), (3, 4), (1, 2)(3, 4), (1, 3)(2, 4), (1, 4)(2, 3), (1, 3, 2, 4), (1, 4, 2, 3)$.

Звідси випливає, що α має лише $24 : 8 = 3$ різних образів при дії групи S_4 на α (орбіта α складається з трьох елементів): α, β і γ . $\alpha = x_1x_2 + x_3x_4, \beta = x_2x_3 + x_1x_4, \gamma = x_1x_3 + x_2x_4$.

Отже, α корінь многочлена 3-го степеня над полем $K(a, b, c)$. Для того, щоб знайти цей многочлен, обчислимо елементарні симетричні многочлени від α, β і γ .

$$\begin{aligned} \alpha + \beta + \gamma &= \sum_{i < j} x_i x_j = a, \\ \alpha\beta + \beta\gamma + \gamma\alpha &= \\ \gamma &= (\sum x_i)(\sum_{i < j < k} x_i x_j x_k) - 4x_1 x_2 x_3 x_4 = -4c, \\ \alpha\beta\gamma &= x_1 x_2 x_3 x_4 (\sum x_i)^2 + (\sum_{i < j < k} x_i x_j x_k)^2 - 4x_1 x_2 x_3 x_4 (\sum_{i < j} x_i x_j) = -4ac + b^2. \end{aligned}$$

Отже, α, β і γ корені многочлен

$$X^3 - aX^2 - 4cX + 4ac - b^2. \quad (20.7.1)$$

Покажемо, що x_1, x_2, x_3, x_4 виражаються через α, β і γ . Маємо

$$\begin{cases} (x_1 + x_3)(x_2 + x_4) = \alpha + \beta, \\ (x_1 + x_3) + (x_2 + x_4) = 0. \end{cases}$$

Звідси $x_1 + x_3 = \sqrt{-\alpha - \beta} = \sqrt{\gamma - a}$, $x_2 + x_4 = -\sqrt{-\alpha - \beta} = -\sqrt{\gamma - a}$.
Аналогічно $x_1 + x_4 = \sqrt{\beta - a}$, $x_2 + x_3 = -\sqrt{\beta - a}$, $x_1 + x_2 = \sqrt{\alpha - a}$,
 $x_3 + x_4 = -\sqrt{\alpha - a}$.

Звідси маємо

$$\begin{aligned} 3x_1 + x_2 + x_3 + x_4 &= 2x_1 = \sqrt{\alpha - a} + \sqrt{\beta - a} + \sqrt{\beta - a}, \\ 3x_2 + x_1 + x_3 + x_4 &= 2x_2 = \sqrt{\alpha - a} - \sqrt{\beta - a} - \sqrt{\beta - a}, \\ 3x_3 + x_1 + x_2 + x_4 &= 2x_3 = -\sqrt{\alpha - a} - \sqrt{\beta - a} + \sqrt{\gamma - a}, \\ 3x_4 + x_1 + x_2 + x_3 &= 2x_4 = -\sqrt{\alpha - a} + \sqrt{\beta - a} - \sqrt{\gamma - a}, \end{aligned}$$

де α, β, γ корені многочлен (20.7.1). Це є *формули Кардано для многочлена 4-го степеня*.

21 Розв'язність рівнянь у радикалах

21.1 Група Галуа многочлена $X^n - 1$

Елемент α поля K називають *коренем з 1*, якщо $\alpha^n = 1$. Множина всіх коренів з 1 в полі K утворює підгрупу мультиплікативної групи поля K . Кожна скінчenna підгрупа мультиплікативної групи будь-якого поля є циклічною. Це доводиться з допомогою таких же міркувань як ті, що були використані для доведення циклічності мультиплікативної групи скінченного поля. Якщо група коренів n -го степеня з 1 поля K містить всі корені многочлена $X^n - 1$ (їх буде n , якщо $\text{char}K \nmid n$), то ця циклічна група складається з n' елементів, де $n = p^k n'$, $p = \text{char}K$, $(n', p) = 1$. Її твірна має порядок n' і називається *первісним коренем n -го степеня з 1*. Якщо $\text{char}K \mid n$, то $n = n'$.

Так само, як і у випадку комплексних коренів з 1, доводимо, що коли ξ первісний корінь n -го степеня з 1, то ξ^k первісний корінь тоді і тільки тоді, коли $(k, n) = 1$.

Твердження 153. *Нехай $\text{char}K \nmid n$; L поле розкладу многочлена $X^n - 1 \in K[X]$. Тоді L/K розширення Галуа і $\text{Gal}(L/K)$ ізоморфна підгрупі групи $(\mathbb{Z}/n\mathbb{Z})^*$.*

Доведення. При наших припущеннях, L – поле розкладу сепарабельного многочлена, отже, розширення Галуа. Нехай ξ первісний корінь n -го степеня з 1. Якщо $\xi \in K$, то $L = K$ і $\text{Gal}(L/K) = \{1\}$. Якщо $\xi \notin K$, $\sigma \in \text{Gal}(L/K)$, то $\sigma(\xi)$ теж корінь многочлен $X^n - 1$ і $\sigma(\xi)$ має такий же порядок як і ξ . Тому $\sigma(\xi) = \xi^k$, де $(k, n) = 1$: елементи групи Галуа переводять первісні корені з 1 в первісні корені. Розглянемо відображення F : $\text{Gal}(L/K) \rightarrow (\mathbb{Z}/n\mathbb{Z})^*$, де $F(\sigma) = \bar{k} \Leftrightarrow \sigma(\xi) = \xi^k$. Якщо $\sigma, \tau \in \text{Gal}(L/K)$ і $f(\tau) = \bar{l}$, то $F(\sigma\tau) = \bar{k}\bar{l}$, Оскільки $(\sigma\tau)(\xi) = \sigma(\tau(\xi)) = \sigma(\xi^l) = \sigma(\xi)^l = \xi^{kl}$. Отже, F гомоморфізм. $\text{Ker } F = \{\sigma \mid \sigma(\xi) = \xi\} = \{id\}$. З теореми про гомоморфізм випливає, що $\text{Gal}(L/K) \simeq \text{Im } F \subset (\mathbb{Z}/n\mathbb{Z})^*$. \square

21.2 Циклічні розширення

Означення 154. Скінченне розширення Галуа L/K називають *циклічним*, якщо його група $\text{Gal}(L/K)$ циклічна.

Приклади.

1) Група Галуа поля розкладу многочлена $X^2 - 2 \in \mathbb{Q}[X]$ циклічна група 2-го порядку. При деяких обмеженнях ми доведемо, що будь-яке циклічне розширення поля K є полем розкладу деякого многочлен $X^n - a$.

2) Перевіримо, що будь-яке скінченне розширення поля \mathbb{F}_q є циклічним розширенням Галуа. Нехай L/\mathbb{F}_q розширення степеня n . Ми вже знаємо з п. 18.2, що $L = \mathbb{F}_{q^n}$ – поле розкладу многочлен $X^{q^n} - X$. Похідна цього многочлена дорівнює $-1 \neq 0$, отже, L/\mathbb{F}_q розширення Галуа. Відображення $\sigma: L \rightarrow L$, $\sigma(\alpha) = \alpha^q$ є автоморфізмом поля L , причому автоморфізми $\sigma, \sigma^2, \dots, \sigma^{n-1}, \sigma^n$ всі різні і залишають незмінними елементи з поля \mathbb{F}_q . Той факт, що ці автоморфізми всі різні випливає з того, що для твірного елемента α мультиплікативної групи $\mathbb{F}_{q^n}^*$ елементи $\alpha^q, \alpha^{q^2}, \dots, \alpha^{q^n}$ всі різні (це було доведено в п. 18.2). Вони залишають незмінними всі елементи поля \mathbb{F}_q , оскільки кожний елемент $\beta \in \mathbb{F}_q$ є коренем рівняння $X^q - X = 0$. Ми маємо $n = [\mathbb{F}_{q^n} : \mathbb{F}_q]$ автоморфізмів $\sigma, \sigma^2, \dots, \sigma^n = id$ поля \mathbb{F}_{q^n} над полем \mathbb{F}_q . Але з теореми про кількість вкладень (див. наслідок 111) випливає, що вони вичерпують всю групу $\text{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$, тому ця група циклічна, породжена автоморфізмом σ .

Теорема 155. Нехай K поле, $\text{char } K \nmid n$. Притустимо, що первісний корінь n -го степеня з 1 належить до K .

a) Якщо L/K циклічне розширення степеня n , то існує елемент $\theta \in L$, для якого $L = K(\theta)$ і θ є коренем многочлена $X^n - a$, де $a \in K$.

б) Навпаки, якщо $a \in K$, і θ деякий корінь многочлену $X^n - a$, то $K(\theta)/K$ – циклічне розширення, $[K(\theta) : K] = d$, $d|n$ і $\theta^d \in K$. Якщо, зокрема, $X^n - a$ незвідний над K , то $d = n$.

Доведення. а) Нехай $\xi \in K$ первісний корінь n -го степеня з 1, σ твірна групи $\text{Gal}(L/K)$. З леми Артіна про лінійну незалежність характерів (п. 12.3, Розд. ??) випливає, що існує елемент $\alpha \in L$, для якого

$$\theta = \alpha + \xi\sigma(\alpha) + \cdots + \xi^{n-1}\sigma^{n-1}(\alpha) \neq 0.$$

Маємо

$$\begin{aligned} \sigma(\theta) &= \sigma(\alpha) + \xi\sigma^2(\alpha) + \cdots + \xi^{n-1}\sigma^n(\alpha) = \\ &= \xi^{-1}\alpha + \xi^{-1}\xi\sigma(\alpha) + \xi^{-1}\xi^2\sigma^2(\alpha) + \cdots + \xi^{-1}\xi^{n-1}\sigma^{n-1}(\alpha) = \xi^{-1}\theta. \end{aligned}$$

Звідси $\sigma(\theta^n) = \sigma(\theta)^n = (\xi^{-1}\theta)^n = \theta^n$. Автоморфізм σ залиш є незмінним θ^n , отже, кожний автоморфізм σ^i , $1 \leq i \leq n$, теж залишає незмінним θ^n , тоді $\theta^n = a \in K$ і θ є коренем многочлена $X^n - a$.

Доведемо, що $L = K(\theta)$. Оскільки ξ первісний корінь n -го степеня з 1, то елементи $\theta, \sigma(\theta) = \xi\theta, \sigma^2(\theta) = \xi^2\theta, \dots, \sigma^{n-1}(\theta) = \xi^{n-1}\theta$ всі різні. Тому маємо

$$n = [L : K] \geq [K(\theta) : K] \geq |\text{Aut}(K(\theta)/K)| = n,$$

і звідси випливає, що $K(\theta) = L$.

б) Якщо $\theta \in L$ корінь многочлена $X^n - a \in K[X]$, то $\xi^i\theta$ теж корінь цього многочлена для всіх i , $0 \leq i \leq n-1$. Отже, $K(\theta)$ поле розкладу многочлену $X^n - a$, тому $K(\theta)/K$ розширення Галуа. Якщо $\sigma \in \text{Gal}(K(\theta)/K)$, то $\sigma(\theta) = \xi^i\theta$ для деякого i , $0 \leq i \leq n-1$. Означимо відображення $F: \text{Gal}(L/K) \rightarrow \mathbb{Z}/n\mathbb{Z}$ так: $F(\sigma) = \bar{i} \Leftrightarrow \sigma(\theta) = \xi^i\theta$.

F гомоморфізм груп, Оскільки, якщо $F(\tau) = \bar{j}$, то $(\sigma\tau)(\theta) = \sigma(\tau(\theta)) = \sigma(\xi^j\theta) = \xi^j\sigma(\theta) = \xi^{i+j}\theta$, тому $F(\sigma\tau) = \overline{i+j} = \bar{i} + \bar{j} = F(\sigma) + F(\tau)$. F , очевидно, ін'єктивний гомоморфізм. Тому $\text{Gal}(K(\theta)/K)$ ізоморфна підгрупі групи $\mathbb{Z}/n\mathbb{Z}$. Звідси випливає, що $\text{Gal}(K(\theta)/K)$ циклічна група порядку d , де $d|n$. Нехай тепер σ твірна групи $\text{Gal}(K(\theta)/K)$. Тоді $\sigma(\theta) = \eta\theta$, де η первісний корінь степеня d з 1. Звідси випливає, що σ залишає незмінним елемент θ^d . $\sigma(\theta^d) = \sigma(\theta)^d = (\eta\theta)^d = \eta^d \cdot \theta^d = \theta^d$. Тому θ^d залишається незмінним при дії всіх елементів групи $\text{Gal}(K(\theta)/K)$, отже, $\theta^d \in K$. \square

21.3 Радикальні та напівабельові розширення

Відтепер і до кінця цього параграфа вважаємо, що характеристика поля K дорівнює 0. Таке обмеження пов'язане з тим, що нам доведеться розглядати розширення Галуа типу $K(\alpha)/K$, де α корінь многочлена $X^n - a \in K[X]$, ми дослідили в попередньому пункті такі розширення лише при обмеженні $\text{char } K \nmid n$. Зауважимо, що результати, аналогічні тим, які ми доведемо, справедливі для полів будь-якої характеристики. Ми обмежуємося розглядом полів характеристики 0 лише для спрощення доведень і формулювань.

Означення 156. розширення L/K називають *простим радикальним розширенням* поля K , якщо $L = K(\alpha)$, де α корінь многочлена $X^n - a \in K[X]$. розширення L/K називають *радикальним розширенням* поля K , якщо існує башта полів

$$K = K_0 \subset K_1 \subset \cdots \subset K_m = L,$$

де K_i/K_{i-1} просте радикальне розширення для всіх i , $1 \leq i \leq m$.

Приклад. Формули Кардано (див. пп. 20.5 і 20.7) показують, що полі розкладу многочленів $X^3 + pX + q$ та $X^4 + aX^2 + bX + c$ є радикальними розширеннями полів $K(p, q)$ та $K(a, b, c)$ відповідно.

Означення 157. розширення L/K називають *напівабельовим*, якщо існує башта $K = K_0 \subset K_1 \subset K_2 \subset \cdots \subset K_m = L$, де K_i/K_{i-1} розширення Галуа абелевою групою Галуа.

Лема 158. *Будь-яке радикальне розширення L/K можна вклсти в напівабельове розширення.*

Доведення. Нехай L/K — радикальне розширення і

$$K = K_0 \subset K_1 \subset K_2 \subset \cdots \subset K_m = L$$

відповідна йому башта простих радикальних розширень: $K_i = K_{i-1}(\alpha_i)$, де α_i корінь многочлена $X^{n_i} - a_i \in K_{i-1}[X]$. Приєднаємо до поля K первісний корінь ξ n -го степеня з 1, де n найменше спільне кратне всіх n_i і розглянемо башту

$$K = K_0 \subset K_0(\xi) \subset K_1(\xi) \subset K_2(\xi) \subset \cdots \subset K_m(\xi) = L(\xi).$$

розширення $K(\xi)/K$ має абелеву групу Галуа: вона ізоморфна підгрупі групи $(\mathbb{Z}/n\mathbb{Z})^*$ з твердженням 153. Далі, кожне поле $K_{i-1}(\xi)$ містить

всі корені степеня n_i з 1, тому за теоремою 155 $\text{Gal}(K_i(\xi)/K_{i-1}(\xi))$ є циклічною групою. Отже, $L(\xi)$ напівабельове розширення поля K і $L \subset L(\xi)$. \square

Лема 159. *Нехай L_1 і L_2 напівабельові розширення поля K , які є підполями деякого розширення L/K . Тоді поле L_1L_2 — композит полів L_1 і L_2 також є напівабельовим розширенням поля K .*

Доведення. За припущенням леми існують дві башти полів

$$\begin{aligned} K &= K_0 \subset K_1 \subset K_2 \subset \cdots \subset K_m = L_1, \\ K' &= K'_0 \subset K'_1 \subset K'_2 \subset \cdots \subset K'_{m'} = L_2, \end{aligned}$$

де K_i/K_{i-1} та K'_i/K'_{i-1} розширення Галуа з абелевими групами Галуа. Утворимо таку башту

$$K = K_0 \subset K_1 \subset \cdots \subset K_m = L_1K'_0 \subset L_1K'_1 \subset \cdots \subset L_1K'_{m'} = L_1L_2.$$

З теореми про трансляцію (п. 20.4) випливає, що $L_1K'_i/L_1K'_{i-1}$ є розширенням Галуа з групою Галуа $\text{Gal}(L_1K'_i/L_1K'_{i-1})$, яка ізоморфна $\text{Gal}(K'_i/K'_{i-1})^{K'_i \cap L_1}$ — підгрупі абелевої групи $\text{Gal}(K'_i/K'_{i-1})$ для всіх i , $1 \leq i \leq m'$. Тому L_1L_2 напівабельове розширення поля K . \square

Лема 160. *Кожне напівабельове розширення можна вклсти у нормальне напівабельове розширення.*

Доведення. Нехай L напівабельове розширення поля K . Оскільки L/K скінченне сепарабельне розширення, то з теореми 131 про простоту випливає, що $L = K(\beta)$. Якщо приєднати до L всі корені мінімального многочлена елемента β над K , то одержимо нормальнє розширення E поля K . Нехай L_1, L_2, \dots, L_r образи поля L при всіх автоморфізмах поля E над K . Переконаємося у тому, що всі розширення L_1, L_2, \dots, L_r напівабельові. Нехай σL одне з розширень L_1, L_2, \dots, L_r , де $\sigma \in \text{Gal}(E/K)$. Для поля L існує башта

$$K = K_0 \subset K_1 \subset K_2 \subset \cdots \subset K_m = L,$$

де $H_i = \text{Gal}(K_i/K_{i-1})$ абелеві групи для всіх i , $1 \leq i \leq m$.

Розглянемо таку башту

$$K = \sigma K = \sigma K_0 \subset \sigma K_1 \subset \cdots \subset \sigma K_m = \sigma L.$$

Автоморфізму $\tau \in H_i$ відповідає автоморфізм $\sigma\tau\sigma^{-1}$ поля σK_i над σK_{i-1} . Тому розширення $\sigma K_i/\sigma K_{i-1}$ є розширенням Галуа з абелевою групою Галуа $\sigma H\sigma^{-1}$, отже, розширення σL напівabelьове.

За лемою 159 композит $M = L_1 L_2 \dots L_r$ є напівabelьовим розширенням. Залиється довести, що M нормальне розширення поля K . Для цього досить показати, що для кожного автоморфізму σ поля E над K $\sigma M = M$ (порівняйте теореми про нормальні розширення та про поле розкладу). Але M і σM відрізняються лише перестановкою множників L_1, L_2, \dots, L_r у композиті $L_1 L_2 \dots L_r$. Отже, $\sigma M = M$. \square

Лема 161. *Група Галуа нормальногоп напівabelьового розширення M/K є розв'язною.*

Доведення. Існує башта розширень $K = K_0 \subset K_1 \subset K_2 \subset \dots \subset K_{m-1} \subset K_m = M$, де K_i/K_{i-1} розширення Галуа з абелевою групою Галуа. Розглянемо відповідний за основною теоремою теорії Галуа ланцюжок підгруп групи $G = \text{Gal}(M/K)$:

$$G = G_0 \supset G_1 \supset \dots \supset G_{m-1} \supset G_m = \{e\},$$

де $G_i = G^{K_i} = \{\sigma \in G \mid \sigma(\alpha) = \alpha \quad \forall \alpha \in K_i\}$. Для кожного i , $0 \leq i \leq m$, поле M є розширенням Галуа поля K_i з групою Галуа G_i .

Розглянемо башту полів

$$K_{i-1} \subset K_i \subset M.$$

K_i/K_{i-1} розширення Галуа; за теоремою 148 група G_i є нормальнюю підгрупою групи G_{i-1} і фактор-група $G_{i-1}/G_i \simeq \text{Gal}(K_i/K_{i-1})$ абельова. Тому група G розв'язна. \square

21.4 Розв'язність рівнянь у радикалах

Означення 162. Нехай $f(X) \in K[X]$ незвідний над полем K многочлен. Рівняння $f(X) = 0$ називають *розв'язним у радикалах*, якщо існує радикальне розширення L поля K , в якому $f(X)$ має корінь.

Теорема 163. *Нехай $f(X) \in K[X]$ незвідний над полем K многочлен, E поле розкладу многочлена $f(X)$ з групою Галуа $G = \text{Gal}(E/K)$. Рівняння $f(X) = 0$ тоді і тільки тоді розв'язне в радикалах, коли група G розв'язна. У цьому випадку існує таке радикальне розширення поля K , в якому $f(X)$ розкладається на лінійні множники.*

Доведення. \implies . Нехай існує радикальне розширення L поля K , в якому многочлен $f(X)$ має корінь. За лемами 158 і 160 поле L можна вклсти в напівабельове нормальнє розширення M поля K . З теореми про нормальні розширення випливає, що $f(X)$ розкладається на лінійні множники в полі M , отже, поле розкладу E многочлен $f(X)$ є підполем поля M , тому з теореми 148 про нормальність одержуємо, що $\text{Gal}(E/K) = \text{Gal}(M/K)/\text{Gal}(M/E)$. Ми одержуємо, що $G = \text{Gal}(E/K)$ є фактор-групою розв'язної за лемою 161 групи $\text{Gal}(M/K)$, отже, є розв'язною групою.

\Leftarrow . Нехай група G розв'язна, $n = |G|$. Приєднаємо до поля K першій корінь ξ n -го степеня 1, $K' = K(\xi)$ — радикальне розширення поля K . Поле $E' = EK'$ є полем розкладу многочлена $f(X)$ над полем K' . З теореми про трансляцію одержуємо, що $G' = \text{Gal}(E'/K') = \text{Gal}(E/K)^{K' \cap E}$ підгрупа розв'язної групи $\text{Gal}(E/K)$, отже, розв'язна група. Розглянемо

$$G' = G'_0 \triangleright G'_1 \triangleright G'_2 \triangleright \cdots \triangleright G'_s = \{e\}$$

ланцюжок нормальніх підгруп з циклічними фактор-групами G'_i/G'_{i+1} , $0 \leq i \leq s-1$ і відповідну цьому ланцюгу з основною теоремою теорії Галуа башту полів

$$K' = K'_0 \subset K'_1 \subset \cdots \subset K'_s = E,$$

де $K'_i = E'^{G'_i}$, E'/K'_i розширення Галуа з групою Галуа G'_i . K'_i/K'_{i-1} циклічне розширення, тому за теоремою 155 про циклічні розширення $K'_i = K'_{i-1}(\theta_i)$, де θ_i корінь многочлена $X^{n_i} - a_i \in K_{i-1}[X]$. Отже, E' — радикальне розширення поля K' , а тому і радикальне розширення поля K . Оскільки K'/K радикальне. Отже, E' радикальне розширення поля K , в якому многочлен $f(X)$ розкладається на лінійні множники.

□

Наслідок 164 (Абель). *Нехай $f(X)$ загальний многочлен (див. приклад з п. 20.6) степеня n над полем K характеристики 0. Якщо $n \geq 5$, то рівняння $f(X) = 0$ не розв'язне в радикалах.*

Доведення. Ми вже знаємо, що група Галуа загального многочлена степеня n ізоморфна групі S_n . Але група S_n нерозв'язна при $n \geq 5$. Тому загальне рівняння в цьому випадку нерозв'язне в радикалах. □

21.5 Приклади нерозв'язних рівнянь степеня ≥ 5

Побудуємо приклади многочленів степеня $n \geq 5$ з раціональними коефіцієнтами, група Галуа яких ізоморфна групі S_n . Для цього використаємо

один результат про групу S_n .

Лема 165. S_n породжується циклами $(1, 2, \dots, n)$ та $(1, 2)$.

Доведення. Маємо

$$\begin{aligned}(1, 2, \dots, n)(1, 2)(1, 2, \dots, n)^{-1} &= (2, 3), \\(1, 2, \dots, n)(2, 3)(1, 2, \dots, n)^{-1} &= (3, 4), \\&\dots \\(1, 2, \dots, n)(n-2, n-1)(1, 2, \dots, n)^{-1} &= (n-1, n).\end{aligned}$$

Далі, $(1, 2)(2, 3)(1, 2) = (1, 3)$, $(1, 3)(3, 4)(1, 3) = (1, 4)$, ..., $(1, n-1)(n-1, n)(1, n-1) = (1, n)$, отже підгрупа, породжена циклами $(1, 2, \dots, n)$ та $(1, 2)$ містить всі транспозиції вигляду $(1, k)$, де $k \in \{2, \dots, n\}$. Але звідси випливає, що ця підгрупа містить всі транспозиції: $(1, k)(1, l)(1, k) = (k, l)$, де $1 < k, l \leq n$. Лема випливає з того, що S_n породжується транспозиціями. \square

Нехай $f(X) \in \mathbb{Q}[X]$ незвідний многочлен простого степеня p , що має два комплексно спряжені корені і $p-2$ дійсних коренів. Тоді в групі Галуа його поля розкладу L існує автоморфізм, який відповідає транспозиції комплексно спряжених коренів.

Крім цього, якщо α будь-який корінь многочлен $f(X)$, то $[\mathbb{Q}(\alpha) : \mathbb{Q}] = p$, отже $p|[L : \mathbb{Q}]$, але $[L : \mathbb{Q}] = |\text{Gal}(L/\mathbb{Q})|$. Оскільки p просте, то в $\text{Gal}(L/\mathbb{Q})$ існує елемент порядку p , підстановка порядку p в S_p необхідно є циклом. Це означає, що група Галуа поля розкладу многочлен $f(X)$ ізоморфна підгрупі групи S_p , яка містить цикл довжини p і цикл довжини 2. Нумеруючи підходящим способом корені многочлен $f(X)$, можна вважати, що ця підгрупа містить транспозицію $(1, 2)$ і якийсь цикл $\sigma = (i_1, \dots, i_p)$. Деякий степінь циклу σ переводить 1 в 2. Тому, знову беручи до уваги, що p просте і нумеруючи відповідним чином корені, одержуємо, що згадана підгрупа групи S_p містить цикл $(1, 2, 3, \dots, p)$. З леми випливає, що ця підгрупа є вся група S_p .

Наведемо конкретний приклад многочлен з групою Галуа S_5 . Достати вказати незвідний многочлен п'ятого степеня з раціональними коефіцієнтами, графік якого перетинає вісь абсцис три рази. Наприклад, $f(X) = X^5 - 4X - 2$. Справді, цей многочлен незвідний за критерієм Ейзенштейна і має три дійсних корені. Щоб переконатися в останньому твердженні, зауважимо, що $f'(X) = 5X^4 - 4$ має два дійсні корені: $\pm\sqrt[4]{2/\sqrt{5}}$ ($\sqrt[4]{2/\sqrt{5}} < 1$). Крім того, $p(-1) = 1$, $p(0) = -2$ і ескіз графіка $f(X)$ має такий вигляд

Отже, рівняння $X^5 - 4X^4 - 2 = 0$ нерозв'язне в радикалах.

Зауважимо, що у вправах 32 - 40, які ми запозичили з основного тексту книги Е. Артіна “Теорія Галуа”, обґрунтovується ще один метод побудови многочленів над полем \mathbb{Q} з нерозв'язною групою Галуа.

22 Геометричні побудови на площині

22.1 Конструктивні точки

Маємо площину, деяку підмножину M_0 на площині, а також лінійку та циркуль. Будемо вважати, що площаина ототожнюється з полем комплексних чисел \mathbb{C} , отже, $M_0 \subset \mathbb{C}$, де M_0 деяка підмножина множини комплексних чисел.

Означення 166. Виходячи з множини M_0 , побудуємо множину M_1 , додавши до множини M_0 усі точки комплексної площини, які є:

- 1) перетинами прямих, кожна з яких містить хоч би дві точки множини M_0 ;
- 2) перетинами кіл з центрами у точках з M_0 і радіусами, що дорівнюють відстані між двома точками з множини M_0 ;
- 3) перетинами прямих родини 1), кіл родини 2) та прямих і кіл родин 1) і 2).

Далі будуємо множину M_2 , виходячи із вже побудованої M_1 . Застосовуючи аналогічний процес, крок за кроком, одержимо множину M_n для всіх натуральних $n \in \mathbb{N}$. Множину $M = \bigcup_{n \in \mathbb{N}} M_n$ назовемо множиною *K₀-конструктивних точок* площини. У випадку, коли $M_0 = \{0, 1\}$, відповідну множину M називають множиною *конструктивних точок* площини.

Вважають, що завжди $\{0, 1\} \subset M_0$.

Першим простим фактом про множину M є така теорема.

Теорема 167. *Підмножини M M₀-конструктивних точок поля \mathbb{C} є підполем поля \mathbb{C} , замкненим відносно комплексного спряження та добування квадратних коренів.*

kern1in
kern1.1in

Рис. 2:

Доведення. Використовуючи означення множини M конструктивних точок, ми можемо побудувати середину відрізка, кінцями якого є точки з M , перпендикуляр до цього відрізка, що проходить через його середину, а також пряму паралельну прямій родини 1) з означення множини M , яка проходить через точку множини M , та бісектрису кута, утвореного двома прямими родини 1). Оскільки $\{0, 1\} \subset M_0 \subset M$, то можна за допомогою циркуля та лінійки побудувати на площині координатні осі Ox та Oy , а також усі числа вигляду $a + bi$, де $a, b \in \mathbb{Q}$.

Покажемо, що множина M M_0 -конструктивних точок є підполем поля \mathbb{C} . Нехай $z_1, z_2 \in M$. Тоді зрозуміло, що $z_1 + z_2 \in M$ (див. мал. 2))

Перевіримо, що $z_1 z_2 \in M$. Справді $|z_1 z_2|$ будується так (див. мал. 2 б)):

- а) “переносимо” z_2 на вісь Ox з допомогою циркуля;
- б) проводимо через точку $|z_2|$ пряму l_1 , паралельну прямій $1z_1$;
- в) для точки z_3 , що є перетином прямих l_1 та Oz_1 маємо $|z_3| = |z_1||z_2|$.

Отже, точка $z_1 z_2$ лежать на тій же дузі кола з центром у точці , що і точка z_3 , $i \arg z_1 z_2 = \arg z_1 + \arg z_2$.

Якщо $z \in M$, то $\bar{z}, \Re z, \Im z, |z|, -z$ та z^{-1} для $z \neq 0$ теж всі належать до M . Побудову елемента z^{-1} ілюструє мал. 2 в).

Із сказаного вище випливає, що M поле, замкнене відносно спряження. Залиється показати, що коли $z \in M$, то $\pm\sqrt{z} \in M$. $\pm\sqrt{z}$ розміщені на бісектрисі кута, утвореного дійсною напівпрямою та напівпрямою, що з’єднує O і z . Їх спільний модуль одержується за допомогою кола, кінцями діаметра якого є точки z та $-z/|z|$ (див. мал. 2 г)). \square

22.2 Необхідна і достатня умови конструктивності

Нехай M_0 деяка підмножина поля комплексних чисел \mathbb{C} . Приєднаємо множину M_0 до поля \mathbb{Q} . Одержано поле $\mathbb{Q}(M_0)$ — перетин усіх підполів поля \mathbb{C} , що містять як \mathbb{Q} так і M_0 . Це найменше підполе поля \mathbb{C} , яке містить множину M_0 .

Твердження 168. Якщо число $z \in \mathbb{C}$ є M_0 -конструктивним, то мінімальний многочлен для z над $\mathbb{Q}(M_0)$ має степінь 2^k , де $k \in \mathbb{N}$.

Доведення. Конструктивна точка z є результатом побудови скінченної послідовності точок $z_1, \dots, z_l, \dots, z_m = z$, де кожна точка z_l одержується з точок поля $\mathbb{Q}(M_0, z_1, \dots, z_{l-1})$ за правилами 2) або 3) з означення 166. Розглянемо випадок, коли точка $z_l = x + iy$ одержується за правилом 3). У цьому випадку x та y є розв'язками системи рівнянь

$$\begin{cases} (x - x_1)^2 + (y - y_1)^2 = r_1^2, \\ (x - x_2)^2 + (y - y_2)^2 = r_2^2, \end{cases}$$

де $x_1, y_1, x_2, y_2, r_1, r_2 \in \mathbb{Q}(M_0, z_1, \dots, z_{l-1})$.

Віднявши почленно ці рівняння і виразивши одну невідому через інші, одержимо, що x та y є коренями квадратного рівняння. Звідси випливає, що $z_l \in \mathbb{Q}(M_0, z_1, \dots, z_{l-1})(\sqrt{\alpha_{l-1}})$, де $\alpha_{l-1} \in \mathbb{Q}(M_0, z_1, \dots, z_{l-1})$.

Таким чином, щоб дізнатися, що число $z \in \mathbb{C}$ є M_0 -конструктивним, потрібно переконатися, що існує скінчenna башта розширень $\mathbb{Q}(M_0) = K_0 \subset K_1 \subset \dots \subset K_m$ з властивостями:

- a) $z \in K_m$;
- б) для кожного i , $0 \leq i \leq m-1$ $P_{i+1} = P_i(\alpha_i)$, де $\alpha_i^2 \in P_i$.

Зрозуміло, що $[K_m : K_0] = 2^m$ і $K_0 \subset K_0(z) \subset K_m$. Звідси випливає, що $[K_0(z) : K_0]$ є степенем 2, отже, мінімальний многочлен для z над K_0 має степінь 2^k для деякого $k \in \mathbb{N}$. \square

22.3 Приклади

1) *Розглянемо три знамениті античні задачі: про квадратуру круга, подвоєння куба та трисекцію кута.*

Перевіримо, що числа π , $\sqrt[3]{2}$ та $\cos 20^\circ$ неконструктивні. Що стосується числа π , то відомо, що π трансцендентне, кожне конструктивне число є алгебраїчним над \mathbb{Q} . $\sqrt[3]{2}$ неконструктивне, бо мінімальний многочлен $X^3 - 2 \in \mathbb{Q}[X]$ числа $\sqrt[3]{2}$ має степінь 3. Залишається показати, що $\cos 20^\circ$ неконструктивне число. Оскільки, $\cos 3\alpha = 4\cos^3 \alpha - 3\cos \alpha$, то кут в 60° можна розділити на 3 за допомогою циркуля та лінійки тоді і тільки тоді, коли мінімальний многочлен для $\cos 20^\circ$ має степінь 2^k , але Оскільки цей мінімальний многочлен є многочленом $4X^3 - 3X - \frac{1}{2}$ (в чому легко переконатися, спробувавши знайти його раціональні корені), то це неможливо. Отже, $\cos 20^\circ$ неконструктивне число.

2) *Побудова правильного п'ятикутника.*

Для того, щоб побудувати правильний п'ятикутник, потрібно побудувати комплексне число $\xi = e^{2\pi i/5} = \cos \frac{2\pi}{5} + i \sin \frac{2\pi}{5}$. Груп Галуа поля $\mathbb{Q}(\xi)$ циклічна, має порядок 4 і породжена автоморфізмом σ , для якого $\sigma(\xi) = \xi^2$ (згадайте п. 21.1).

Розглянемо підполе L поля $\mathbb{Q}(\xi)$, що відповідає підгрупі $\{1, \sigma^2\}$. L породжується над \mathbb{Q} будь-яким елементом α , $\alpha \notin \mathbb{Q}$, де $\sigma^2(\alpha) = \alpha$. В якості α можна взяти $\alpha = \xi + \sigma^2(\xi) = \xi + \xi^4 = 2 \cos \frac{2\pi}{5}$. Маємо $\sigma(\alpha) = \sigma(\xi) + \sigma(\xi^4) = \xi^2 + \xi^8 = \xi^2 + \xi^3$, отже, $\sigma(\alpha) + \alpha = -1$ і $\sigma(\alpha)\alpha = \xi^3 + \xi^4 + \xi^6 + \xi^7 = \xi + \xi^2 + \xi^3 + \xi^4 = -1$. Значить, α і $\sigma(\alpha)$ є коренями многочлена $X^2 + X - 1$. Звідси одержуємо, що $\cos \frac{2\pi}{5} = \frac{-1 + \sqrt{5}}{4}$ і побудова правильного п'ятикутника, вписаного в коло радіуса 1 зводиться до побудови цього числа.

3) *Правильний семикутник не можна побудувати за допомогою циркуля та лінійки.* Справді, для цього потрібно було б побудувати число $\xi_7 = e^{\frac{2\pi i}{7}}$. Маємо $[\mathbb{Q}(\xi_7) : \mathbb{Q}] = 6$ тому, що незвідний многочлен для ξ_7 над \mathbb{Q} є $1 + X + X^2 + X^3 + X^4 + X^5 + X^6$, 6 не є степенем двійки, отже, ξ_7 не можна побудувати за допомогою циркуля та лінійки.

4) *Побудова правильного 17-кутника* можлива тому, що поле K розкладу мінімального многочлен $\Phi_{17}(X) = \sum_{i=0}^{16} x^i$ для $\xi_{17} = e^{\frac{2\pi i}{17}}$ над \mathbb{Q} є розширенням Галуа, група Галуа якого ізоморфна групі $(\mathbb{Z}/17\mathbb{Z})^*$, яка є циклічною групою порядку 16, породженою, наприклад, елементом $3 \in (\mathbb{Z}/17\mathbb{Z})^*$. Отже, твірною групи $\text{Gal}(K/\mathbb{Q})$ є автоморфізм σ , для якого $\sigma(\xi_{17}) = \xi_{17}^3$. В цій групі існує ланцюжок підгруп

$$G = (\sigma) \supset (\sigma^2) \supset (\sigma^4) \supset (\sigma^8) \supset \{e\}$$

з циклічним фактор-групами порядку 2. За основною теоремою теорії Галуа цьому ланцюжку підгруп відповідає башта розширень

$$\mathbb{Q} = K_0 \subset K_1 \subset K_2 \subset K_3 \subset K_4 = K,$$

де $[K_i : K_{i-1}] = 2$. Звідси випливає, що число ξ_{17} можна одержати за допомогою послідовного приєднання квадратних радикалів, отже, правильний 17-кутник можна побудувати за допомогою циркуля та лінійки.

Вправи.

- Показати, що $\mathbb{Q}(\sqrt[4]{2}, i)$ поле розкладу многочлен $X^4 - 2$ над \mathbb{Q} . Перевірити, що $[\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}] = 8$. Знайти групу Галуа многочлена $X^4 - 2$ та всі її підгрупи. Вказати відповідні цим підгрупам підполія.
- Кажуть, що скінченне розширення Галуа L/K має *нормальну базу*, якщо існує елемент $\alpha \in L$ такий, що множина всіх спряжених до нього (тобто множина $\sigma_1\alpha, \sigma_2\alpha, \dots, \sigma_n\alpha$, де $\{\sigma_1, \sigma_2, \dots, \sigma_n\} = \text{Gal}(L/K)$) утворює базу L/K . Знайти нормальні бази для розширень $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{2} + \sqrt{3})$, $\mathbb{Q}(i, \sqrt[3]{2})$.

3. Нехай група Галуа скінченного розширення Галуа L/K ізоморфна підгрупі групи S_n , що містить підстановки одного з таких типів:
 - а) всі транспозиції,
 - б) всі транспозиції, що переводять даний елемент у будь-який інший,
 - в) одну транспозицію і один циклово-переставу n .

Довести, що в цих випадках $\text{Gal}(L/K) \simeq S_n$.

4. Нехай $f(X), g(X) \in K[X]$ і $f(X)|g(X)$. Нехай G_f та G_g групи Галуа многочленів $f(X)$ та $g(X)$. Довести, що існує сюр'ективний гомоморфізм $G_g \rightarrow G_f$. Яке його ядро?
5. Підгрупу $G \subset S_n$ називають *транзитивною*, якщо для довільних $i, j \in \{1, \dots, n\}$ існує $\sigma \in G$, такий, що $\sigma(i) = j$. Довести, що група Галуа сепараційного многочлена є транзитивною тоді і тільки тоді, коли цей многочлен незвідний.
6. Дослідити групи Галуа многочленів $X^3 + 2X + 1$, $X^4 + X^2 + X + 1 \in \mathbb{Q}[X]$.
7. Що можна сказати про групу Галуа парного многочлена (тобто многочлена від X^2)?
8. *Поле поділу круга.* Нехай ξ_n первісний корінь n -го степеня з 1 над полем \mathbb{Q} . Показати, що $L = \mathbb{Q}(\xi_n)$ є полем розкладу многочлену $X^n - 1 \in \mathbb{Q}[X]$ і $\text{Gal}(L/\mathbb{Q}) \simeq (\mathbb{Z}/n\mathbb{Z})^*$.

Вказівка. Ми знаємо, що $\text{Gal}(L/\mathbb{Q})$ ізоморфна підгрупі групи $(\mathbb{Z}/n\mathbb{Z})^*$. Тому досить перевірити, що всі первісні корені n -го степеня з 1 є коренями мінімального многочлена для ξ_n .

9. Показати, що група Галуа многочлена $X^p - 1 \in \mathbb{Q}[X]$ ізоморфна групі коренів $p - 1$ -го степеня з 1, якщо p просте число.
10. Описати групи Галуа полів поділу круга степенів 4, 6, 9, 10.
11. У полі розкладу L многочлен $X^3 + 3X + 1 \in \mathbb{Q}[X]$ візьмемо в якості примітивного елемент різницю двох коренів цього многочлена. Показати, що мінімальним многочленом для цього елемента є многочлен $X^3 - 9X + 9$. Вивести звідси, що $\text{Gal}(L/K) \simeq C_3$.

12. Нехай $K(x)$ поле розкладу деякого многочлен над K , $y \in K(x)$. Припустимо, що поле $K(y)$ містить всі спряжені до y (див. вправу 2). Довести, що $\text{Gal}(K(y)/K)$ є гомоморфним образом групи $\text{Gal}(K(x)/K)$.
13. Вивчити групи Галуа многочленів $X^4 - 5X + 6$, $X^4 + X^2 + 1$, $X^4 + 1$, $X^3 + X - 2X - 1$, $X^4 - 2 \in \mathbb{Q}[X]$.
14. *Резольвентою Галуа* многочлена $f(X) \in K[X]$ називають довільний мінімальний многочлен примітивного елемента поля розкладу многочлена f . Показати, що степінь резольвенти дорівнює порядку групи Галуа многочлена f і що резольвента має ту ж групу Галуа, що і многочлен. Знайти резольвенти Галуа для многочленів $X^2 - 2$, $X^4 + 2$, $X^3 + X^2 + X + 1$, $X^3 + pX + q \in \mathbb{Q}[X]$.
15. Многочлен $f(X) \in K[X]$ називають *нормальним*, якщо він незвідний і один з його коренів породжує його поле розкладу. Довести, що такі властивості еквівалентні:
- а) $f(X)$ нормальний;
 - б) всі корені многочлен $f(X)$ є примітивними елементами поля розкладу;
 - в) всі корені многочлена $f(X)$ раціонально виражаються через один з них;
 - г) степінь кожної резольвенти Галуа (див. вправу 14) многочлена $f(X)$ дорівнює степеню многочлена $f(X)$.
16. Перевірити такі властивості для многочлена $f(X) \in K[X]$:
- а) кожний незвідний многочлен степеня 2 є нормальним;
 - б) незвідний многочлен степеня 3 є нормальним тоді і тільки тоді, коли $\sqrt[3]{\Delta} \in K$, де Δ — дискримінант многочлена $f(X)$;
 - в) для простого числа p незвідний многочлен $X^p - a \in K[X]$ є нормальним тоді і тільки тоді, коли поле K містить всі корені p -го степеня з 1;
 - г) якщо група Галуа незвідного многочлена $f(X)$ є циклічною, то $f(X)$ нормальним;
 - д) якщо група Галуа незвідного многочлена $f(X)$ є абелевою, то цей многочлен нормальний.

Вказівка. Питання зводиться до доведення, що група Галуа незвідного многочлена транзитивна (див. вправу 5) і що транзитивна абелевова підгрупа групи S_n обов'язково має порядок n . Щоб довести це, доводять, що для кожного i , $1 \leq i \leq n$, існує єдиний елемент $\sigma \in G$ з властивістю $\sigma(1) = i$.

17. Дослідити на нормальності многочлени $X^3 + X^2 + X + 1$, $X^4 - 5X^2 + 6$, $X^4 - a$, $X^4 + aX + b \in \mathbb{Q}[x]$.
18. Довести, що кожна скінчenna група є групою Галуа деякого розширення L/K .
19. Довести, що для нормальних сепарабельних розширень K_1/K та K_2/K вірна рівність $[K_1 K_2 : K][K_1 \cap K_2 : K] = [K_1 : K][K_2 : K]$. Показати, використовуючи поля $K_1 = \mathbb{Q}(\sqrt[3]{2})$ та $K_2 = \mathbb{Q}(\sqrt{-3}, \sqrt[3]{2})$, що це невірно без умови нормальності обох розширень K_1/K та K_2/K .

Вказівка. Довести спочатку, що

$$\text{Gal}(K_1 K_2 / K_1 \cap K_2) = \text{Gal}(K_1 / K_1 \cap K_2) \times \text{Gal}(K_2 / K_1 \cap K_2).$$

20. Нехай L/K скінчне розширення Галуа і $x \in L$. Трив x *слід* x є сумою всіх спряжених до x і $N(x)$ *норма* x є добутком всіх спряжених до x (див. вправу 2). Довести, що коли $\text{Gal}(L/K)$ циклічна група, породжена елементом σ , то $\text{Tr}(x - \sigma(x)) = 0$ і $N(x/\sigma(x)) = 1$. Навпаки, якщо $\text{Tr}y = 0$, то існує $x \in L$, то $y = x - \sigma(x)$, якщо $N(y) = 1$, то існує $x \in L$ з властивістю $y = x/\sigma(x)$.

Вказівка. Для елемента $z \in L$ з властивістю $\text{Tr}(z) \neq 0$ (такий елемент z існує за лемою Артіна) розглянути елемент

$$\begin{aligned} x &= (y\sigma(z) + (y + \sigma(y))\sigma^2(z) + \cdots + \\ &\quad + (y + \sigma(y) + \cdots + \sigma^{n-2}(y))\sigma^{n-1}(z)\frac{1}{\text{Tr}(z)}. \end{aligned}$$

У випадку норми розглянути елемент

$$x = z + y\sigma(z) + y\sigma(y)\sigma^2(z) + \cdots + y\sigma(y)\dots\sigma^{n-2}(y)\sigma^{n-1}(z),$$

де $z \in L$ вибраний так, щоб

$$z + y\sigma(z) + y\sigma(y)\sigma^2(z) + \cdots + y\sigma(y)\dots\sigma^{n-2}(y)\sigma^{n-1}(z) \neq 0$$

(тут знову потрібно застосувати лему Артіна).

Твердження вправи 20 є важливими в теорії полів фактами. Вони відомі під назвою *адитивної та мультиплікативної теореми 90 Гільберта*.

21. Використовуючи вправу 20 довести, що коли L/K розширення Галуа з циклічною групою Галуа і первісний корінь ξ_n n -го степеня з 1 лежить в K , то L/K просте радикальне розширення.

Вказівка. Дослідити норму ξ_n .

22. Якщо L/K нормальнє сепарабельне розширення, то пишемо $K \triangleleft L$, і якщо H нормальні підгрупа групи G , то пишемо $H \triangleleft G$. Нехай $K \triangleleft L_1, K \triangleleft L_2$ (L_1 та L_2 є підполями деякого поля L). Довести, що $K \triangleleft L_1 \cap L_2, K \triangleleft L_1L_2$ і $\text{Gal}(L_1L_2/K) \subset \text{Gal}(L_1/K) \times \text{Gal}(L_2/K)$. Останні включення перетворюються у рівність, якщо $L_1 \cap L_2 = K$. Чи є остання умова необхідною?
23. Нехай $K \triangleleft L$ і $K \subset M$ (поля M і L є підполями деякого поля N). Довести, що $M \triangleleft ML, \text{Gal}(ML/M) = \text{Gal}(L/L \cap M), L \cap M \triangleleft L, |\text{Gal}(ML/M)| \mid [L : K]$. Розглянути приклад $L = \mathbb{Q}(\sqrt{-3}, \sqrt[3]{2})$ і $M = \mathbb{Q}(\sqrt[3]{2})$, щоб переконатися, що ці твердження можуть бути невірними, якщо розширення M/K не є нормальним.
24. Нехай L поле розкладу сепарабельного многочлен $f(X) \in K[X]$ і $\theta \in L$. Тоді

$$|\text{Gal}(L/K)| / |\text{Gal}(L/K(\theta))| = [K(\theta) : K].$$

25. В умовах попередньої вправи довести, що коли $\theta_1, \theta_2 \in L$, то

$$\text{Gal}(L/K(\theta_1, \theta_2)) = \text{Gal}(L/K(\theta_1)) \cap \text{Gal}(L/K(\theta_2)).$$

26. В умовах вправи 24 довести, що коли $K(\theta)$ містить всі спряжені до θ , то

$$\text{Gal}(L/K(\theta)) \triangleleft \text{Gal}(L/K) \text{ і } \text{Gal}(K(\theta)/K) \simeq \text{Gal}(L/K)/\text{Gal}(L/K(\theta)).$$

27. Нехай K_i поле розкладу многочлен $f_i(X) \in K[X], i = 1, 2$. Довести, що:

- a) $\text{Gal}(K_1K_2/K_2) \triangleleft \text{Gal}(K_1/K)$;
- б) $\text{Gal}(K_1K_2/K_2) \simeq \text{Gal}(K_1/K_1 \cap K_2)$;
- в) $\text{Gal}(K_1 \cap K_2/K) \simeq \text{Gal}(K_1/K)/\text{Gal}(K_1/K_1 \cap K_2)$.

28. Нехай $K(\theta)$ розширення Галуа поля K . Описати розширення L/K , що задовільняють умову $\text{Gal}(K(\theta)/K) = \text{Gal}(L(\theta)/L)$.
29. Довести, що коли многочлен $f(X) \in K[X]$ незвідний і $K \triangleleft L$, то всі прості множники многочлена $f(X)$ в кільці $L[X]$ мають один і той же степінь. Що відбувається, якщо не вважати, що $K \triangleleft L$?
30. Довести, що коли група G транзитивна (див. вправу 5) підгрупа групи S_n , де n просте число і H нормальнa підгрупа групи G , то H транзитивна підгрупа або $H = \{e\}$.
- Вказівки.* Використовуючи вправу 17, можна вважати, що $G = \text{Gal}(L/K)$. Якщо L поле розкладу многочлен $f(X) \in K[X]$ і $\alpha_1, \dots, \alpha_n$ корені $f(X)$, то $L = K(\alpha_1, \dots, \alpha_n)$.
- a) Перевірте, що з транзитивності групи G випливає незвідність многочлена $f(X)$ і навпаки.
- b) Нормальний підгрупі $H \triangleleft G$ відповідає нормальне розширення M/K . Розглянути розклад многочлена $f(X)$ на незвідні множники $f(X) = f_1(X) \dots f_r(X)$ в кільці $M[X]$. Кожен α_i є коренем лише одного многочлена $f_j(X)$, і в цьому випадку для $\sigma \in G$, $\sigma(\alpha_i)$ є коренем многочлен $\sigma(f_j(X))$. Далі, $\sigma(f_j(X))$ один з многочленів $f_1(X), \dots, f_r(X)$. Звідси випливає, що всі $f_1(X), \dots, f_r(X)$ мають один і той же степінь. Вивести звідси, що області транзитивності групи H мають одинакову довжину. Звідси випливає, що H транзитивна група або $H = \{e\}$.
31. Нехай K поле і $f(X) \in K[X]$ незвідний многочлен простого степеня n , група Галуа якого розв'язна і

$$G = G_0 \triangleright G_1 \triangleright \cdots \triangleright G_m \triangleright G_{m+1} = \{e\}$$

ланцюжок нормальних підгруп, причому G_m циклічна. Перевірити, що G_m транзитивна група порядку n .

32. Якщо G транзитивна циклічна підгрупа простого порядку n деякої групи підстановок S_n , σ твірна групи G , то при належній нумерації можна вважати, що $\sigma(i) = \sigma^i(1) = i + 1$, числа $1, \dots, n$ можна ототожнити з елементами скінченного поля $\mathbb{Z}/n\mathbb{Z}$. Отже, елементи σ^i транзитивної циклічної групи простого порядку n визначають підстановку σ^i поля $\mathbb{Z}/n\mathbb{Z}$ таку, що $\sigma^i(x) = x + i$.

Якщо $a, b \in \mathbb{Z}/n\mathbb{Z}$, причому $a \neq 0$, то функція $x \mapsto ax + b$ є підстановкою множини $\mathbb{Z}/n\mathbb{Z}$. Групу E підстановок множини $\mathbb{Z}/n\mathbb{Z}$ називають *лінійною*, якщо кожна підстановка τ цієї групи має вигляд $\tau(x) = ax + b$, $a, b \in \mathbb{Z}/n\mathbb{Z}$, $a \neq 0$, причому підстановка $\sigma(x) = x + 1$ належить E .

Показати, що коли τ є елементом лінійної групи E , то порядок елемента τ дорівнює n тоді і тільки, коли $\tau(x) = x + i$, тобто коли $a = 1$.

33. Нехай H підгрупа групи S_n , де n просте число і $N \triangleleft H$, причому N лінійна група. Тоді і H лінійна група.

Вказівка. Нехай $\sigma(x) = x + 1$. Тоді $\sigma \in N$. Якщо $\tau \in H$, то $\tau\sigma\tau^{-1} \in N$. З вправи 32 випливає, що $\tau(y + x) = \tau(y) + ix$ і $\tau(x) = ix + b$.

34. Довести, що коли група Галуа незвідного многочлена простого степеня розв'язна, то вона лінійна.

Вказівка. Використати вправу 33.

35. Довести, що лінійна група підстановок поля $\mathbb{Z}/n\mathbb{Z}$ має не більше, ніж $(n - 1)n$ елементів.

36. Довести, що кожна лінійна група розв'язна.

Вказівка. Нехай N циклічна підгрупа лінійної групи H , N породжена елементом σ , $\sigma(x) = x + 1$. Показати, що $N \triangleleft H$ і H/N абелева група.

37. Довести, що кожна нетотожна підстановка лінійної групи не має двох нерухомих точок.

38. Довести, що якщо рівняння $f(X) = 0$, де $f(X) \in K[X]$ незвідний многочлен простого степеня n , розв'язне, то його поле розкладу породжується будь-якими двома його коренями.

Вказівка. Розглянути поле $M = K(\alpha, \beta)$, де α, β дійсні корені многочлен $f(X)$. За основною теоремою теорії Галуа полю M відповідає підгрупа H . Вона розв'язна. Залишається використати вправи 34 та 37.

39. Довести, що коли незвідний многочлен простого степеня $f(X) \in \mathbb{Q}[X]$ має два дійсні корені α і β і якщо він розв'язний в радикалах, то всі корені $f(X)$ дійсні.

Вказівка. Припустити, що існує комплексний корінь γ і розглянути автоморфізм σ поля розкладу, для якого $\sigma(\alpha) = \alpha$, $\sigma(\beta) = \beta$, $\sigma(\gamma) = \bar{\gamma}$ комплексно спряжений до γ і використати вправи 34 і 37.

40. Довести, що незвідний многочлен простого степеня $n \geq 5$ над \mathbb{Q} нерозв'язний в радикалах тоді і тільки тоді, коли він має точно три дійсних корені.

Вказівка. Використати вправу 39.

41. Довести, що коли правильний p -кутник, де p просте число, можна побудувати за допомогою циркуля та лінійки, то $p - 1 = 2^k$, де $k \in \mathbb{N}$. Перевірити, що коли натуральне число m має непарний простий множник, то $1 + 2^m$ не просте. Вивести звідси, що коли правильний p -кутник можна побудувати за допомогою циркуля та лінійки, то $p = 1 + 2^{2^n}$.
42. Довести, що коли m і n взаємно прості, то правильний mn -кутник можна побудувати за допомогою циркуля і лінійки тоді і тільки тоді, коли можна побудувати правильний m -кутник і правильний n -кутник.
43. Довести, що правильний p^n -кутник ($n > 1$, p просте) можна побудувати за допомогою циркуля та лінійки тоді і тільки тоді, коли $p = 2$.
44. Правильний n -кутник можна побудувати за допомогою циркуля та лінійки тоді і тільки тоді, коли розклад числа n на прості множники має вигляд $n = 2^n p_1 \dots p_s$, де $p_i = 2^{2^{n_i}} + 1$, $n, n_i \in \mathbb{N}$ і p_1, \dots, p_s різні прості числа такого вигляду.
45. Довести, що комплексне число є конструктивним тоді і тільки тоді, коли воно належить нормальному розширенню K/\mathbb{Q} з $[K : \mathbb{Q}] = 2^n$.
46. Дослідити можливість трисекції кута 72° .

p-адичні числа

Поняття числа є одним з найбільш важливих у математиці. Програма середньої школи дає загальне уявлення про натуральні, раціональні і дійсні числа та про властивості алгебраїчних операцій на цих числових множинах. Вже з перших кроків у вивченні алгебри чи геометрії у вищій школі вважаються відомими всі ці числові системи, незважаючи на те, що дійсне число є досить складним математичним об'єктом. Досить сказати, що весь математичний аналіз є, по-суті, науковою про дійсні числа.

Вивчення математичного аналізу розпочинається, як правило, з формульовання аксіом дійсних чисел. Однією з прийнятих систем аксіом є така: множина дійсних чисел \mathbb{R} це *впорядковане поле*¹

Зауважимо, що впорядковане поле K є лінійно впорядкованим, K містить поле раціональних чисел \mathbb{Q} в якості впорядкованого під поля (див. вправу 1), яке має ще такі дві властивості:

- a) *аксіома Архімеда*: $\forall a \in \mathbb{R}, \exists n > \mathbb{N}, n > a$;
- b) *аксіома повноти*: кожна фундаментальна послідовність дійсних чисел має границю в \mathbb{R} .

Аксіома повноти не є очевидною аксіомою, але вона є вирішальною для побудови математичного аналізу. Інколи замість аксіоми повноти формулюють якусь іншу, наприклад, аксіому точної верхньої грані чи аксіому про вкладені відрізки і тоді твердження аксіоми повноти одержується як одна з перших теорем математичного аналізу.

Зауважимо, що всі аксіоми дійсних чисел, за винятком аксіоми повноти, вірні і для поля раціональних чисел \mathbb{Q} . Наша мета — вивчити ще одну важливу числову систему, яку тепер широко використовують в теорії чисел і яку називають полем p -адичних чисел. Ми одержимо p -адичні числа з раціональних, використовуючи побудову, яка дає і дійсні числа. Для того, щоб це зробити, нам доведеться спочатку описати метод Кантора побудови поля дійсних чисел.

23 Поле дійсних чисел

Історично поле дійсних чисел виникло в результаті розширень числових систем: від натуральних чисел до додатних дробів та цілих чисел, далі до раціональних чисел і, нарешті, до дійсних чисел. Нам потрібно вказати множину, яка задовольняє аксіомам, що наведені у вступі. Цей параграф, присвячений короткому опису як можна одержати цю множину.

23.1 Натуральні числа

Множину натуральних чисел вводять як множину \mathbb{N} , що задовольняє таким аксіомам:

¹Поле K називають *впорядкованим*, якщо для його елементів визначена властивість бути додатним (позначають $a > 0$), яка задовольняє такі властивості:

1. Для кожного $a \in K$ виконується одна і тільки одна з трьох можливостей: $a = 0$, $a > 0$, $a < 0$.
2. Якщо $a > 0$ і $b > 0$, то $a + b > 0$ і $ab > 0$.

1) існує ін'єктивне відображення $f: \mathbb{N} \rightarrow \mathbb{N}$, яке ставить у відповідність кожному $a \in \mathbb{N}$ елемент $f(a) \stackrel{\text{df}}{=} a'$. a' називають *наступним* за a числом;

2) існує елемент $0 \in \mathbb{N}$, який не є наступним для жодного $a \in \mathbb{N}$, тобто $0 \notin \text{Im } f$;

3) якщо S підмножина множини \mathbb{N} , для якої $0 \in S$, і для кожного $a \in S$ маємо $a' \in S$, то $S = \mathbb{N}$.

Аксіоми 1), 2), 3) називають *аксіомами Пеано*.

Аксіому 3) називають *аксіомою індукції*. На ній ґрунтуються метод математичної індукції.

Щоб задати множину натуральних чисел, досить вказати будь-яку множину, що задовольняє аксіомам 1), 2), 3). Таку множину можна побудувати, виходячи з порожньої множини \emptyset :

$$\begin{aligned}\emptyset &\stackrel{\text{df}}{=} 0, & \{\emptyset\} &\stackrel{\text{df}}{=} 1 = 0', & \{\emptyset, \{\emptyset\}\} &\stackrel{\text{df}}{=} 2 = 1', & \{\{\emptyset, \{\emptyset\}\}, \{\emptyset, \{\emptyset\}\}\} &\stackrel{\text{df}}{=} 3 = 2', \\ && && \{\{\emptyset, \{\emptyset\}\}, \{\{\emptyset, \{\emptyset\}\}\}, \{\{\emptyset, \{\emptyset\}\}, \{\emptyset, \{\emptyset\}\}\}\} &\stackrel{\text{df}}{=} 4 = 3', \dots.\end{aligned}$$

Тут $n' = n \cup \{n\}$, $n \in n'$ і $n \subset n'$. Легко пересвідчитись, що так побудована множина $\{0, 1, 2, \dots\}$ задовольняє аксіоми Пеано.

На множині \mathbb{N} розглядають дві операції додавання і множення, які визначають “за індукцією”.

Означення 169. а) Для $a, b \in \mathbb{N}$ $a + 0 = a$ і $a + b' = (a + b)'$.
б) Для $a, b \in \mathbb{N}$ $a \cdot 0 = 0$ і $ab' = ab + a$.

Елемент $0'$ позначають 1. Доводять, що $a' = a + 1$, а також, що відносно додавання та множення множина \mathbb{N} є комутативном моноїдом і множення дистрибутивне відносно додавання (див. вправу 2).

Множина \mathbb{N} є цілком впорядкованою множиною відносно такого відношення порядку: $a \leq b$, якщо існує c , що $a + c = b$. Ще, звичайно, потрібно довести і ми пропонуємо цю вправу читачеві.

Перефразовуючи афоризм Кронекера, можна сказати, що Бог створив натуральні числа з \emptyset , а все інше справа рук людини.

23.2 Кільце цілих чисел

Побудуємо кільце цілих чисел. Для цього розглянемо на множині впорядкованих пар натуральних чисел, тобто на множині $\mathbb{N} \times \mathbb{N}$, таке бінарне відношення:

$$(a, b) \sim (a_1, b_1) \Leftrightarrow a + b_1 = a_1 + b.$$

Відношення \sim , очевидно, симетричне і рефлексивне. Легко перевірити, що воно транзитивне. Якщо $a + b_1 = a_1 + b$ і $a_1 + b_2 = a_2 + b_1$, то $a + b_1 + a_1 + b_2 = a_1 + b + a_2 + b_1$, звідси $a + b_2 = a_2 + b$.

Отже, маємо фактор-множину $\mathbb{Z} = \mathbb{N} \times \mathbb{N} / \sim$, елементами множини \mathbb{Z} є суміжні класи множини $\mathbb{N} \times \mathbb{N}$ відносно нашого відношення еквівалентності. Суміжний клас з представником $(a, b) \in \mathbb{N}^2$ далі позначатимемо $(a - b)$ або $a - b$.

Означимо на \mathbb{Z} операції додавання і множення:

$$(a - b) + (c - d) = a + c - (b + d), \quad (23.2.1)$$

$$(a - b)(c - d) = ac + bd - (ad + bc). \quad (23.2.2)$$

Переконаємося в тому, що ці операції означені коректно, тобто результати додавання і множення не залежать від вибору представників в суміжних класах. Обмежимося перевіркою лише коректності множення, а коректність додавання читач легко перевірить самостійно в якості вправи.

Якщо $c - d = c_1 - d_1$, то

$$(a - b)(c_1 - d_1) = ac_1 - bd_1 - (ad_1 + bc_1). \quad (23.2.3)$$

Порівнюючи це з (23.2.2), одержимо

$$\begin{aligned} ac + bd + ad_1 + bc_1 &= a(c + d_1) + b(d + c_1), \\ ac_1 + bd_1 + ad + bc &= a(c_1 + d) + b(d_1 + c). \end{aligned}$$

Тому $ac + bd + ad_1 + bc_1 = ac_1 + bd_1 + ad + bc$, Оскільки $c + d_1 = c_1 + d$, а це означає, що добуток (23.2.3) дорівнює добутку (23.2.2). Коректність множення доведено.

Проста перевірка (з використанням того факту, що множина \mathbb{N} натуральних чисел є моноїдом відносно додавання і відносно множення) показує (вправа 3), що множина \mathbb{Z} є областю відносно визначених рівностями (23.2.1) та (23.2.2) операцій. Зауважимо лише, що $0 = a_a = 0 - 0$, $1 = 1 - 0$, $-(a - b) = b - a$.

Вкладемо тепер множину \mathbb{N} у множину \mathbb{Z} за допомогою ін'єктивного відображення $f: \mathbb{N} \rightarrow \mathbb{Z}$

$$f(a) = a - 0. \quad (23.2.4)$$

При такому вкладенні додаванню та множенню натуральних чисел відповідає додавання та множення цілих чисел, означене за допомогою рівностей (23.2.1) і (23.2.2).

Кожне ціле число $a - b$ можна записати у вигляді $a - b = (a - 0) + (0 - b)$. Доданок $a - 0$ ототожнимо з натуральним числом a за допомогою відображення (23.2.4), а доданок $0 - b$ позначимо $-b$. Числа вигляду $-b$ назвемо *від'ємними числами*. Отже, кожне ціле число є сумою натурального числа і від'ємного числа.

Множина \mathbb{Z} є лінійно впорядкованою множиною відносно такого відношення порядку:

$$\dots < -3 < -2 < -1 < 0 < 1 < 2 < 3 < \dots,$$

тобто для $m, n \in \mathbb{Z}$ $m \leq n$ тоді і тільки тоді, коли $n - m \in \mathbb{N}$ згідно ототожнення (23.2.4).

Пропонуємо довести самостійно такі властивості:

$$m \leq n \Rightarrow m + p \leq n + p, \quad (23.2.5)$$

$$m \leq n, 0 \leq p \Rightarrow mp \leq np, \quad (23.2.6)$$

$$m \leq n, p \leq 0 \Rightarrow mp \geq np, \quad (23.2.7)$$

$$m \geq 0, n \geq 0 \Rightarrow m + n \geq 0, mn \geq 0 \quad (23.2.8)$$

де $m, n, p \in \mathbb{Z}$.

23.3 Поле раціональних чисел

Ми вже знаємо, що кожну область K можна вкласти в поле дробів $Q(K)$. Легко переконатися в тому, що для натуральних чисел m і n $mn = 0 \Leftrightarrow m = 0$ або $n = 0$ і вивести звідси, що кільце \mathbb{Z} не має дільників нуля. Тому кільце \mathbb{Z} можна вкласти в поле дробів $Q(\mathbb{Z})$, яке позначають \mathbb{Q} і називають *полем раціональних чисел*. Якщо раціональне число записане у вигляді дробу $a = \frac{m}{n}$, де $m, n \in \mathbb{Z}$, $n \neq 0$, то домовимося вважати, що $n > 0$.

Введемо на множині \mathbb{Q} відношення порядку: якщо $a_1 = \frac{m_1}{n_1}$, $a_2 = \frac{m_2}{n_2}$, то $a_1 \leq a_2$ означає $m_1n_2 < n_1m_2$.

Можна довести (ми пропонуємо це в якості ще однієї вправи), що множина \mathbb{Q} є лінійно впорядкованою множиною, яка має властивості (23.2.5), (23.2.6), (23.2.7) і (23.2.8), а поле \mathbb{Q} є впорядкованим полем.

Означення 170. *Абсолютною величиною* $|a|$ *раціонального числа* a називають $\max\{a, -a\}$.

Твердження 171. 1) $|a| \geq 0$, $|a| = 0 \Leftrightarrow a = 0$,

$$2) |ab| = |a||b|,$$

$$3) |a + b| \leq |a| + |b|.$$

Доведення. Властивості 1) і 2) очевидні. Нерівність 3) доводимо так. Якщо $a \geq 0$ і $b \geq 0$, то $a + b = |a + b| = |a| + |b|$. Якщо $a \leq 0$ і $b \leq 0$, то $|a + b| = -(a + b) = -a - b = |a| + |b|$. Якщо $a \geq 0$, а $b < 0$, то $|a + b| = \mathbb{F}|a| - |b| \leq \mathbb{F}|a| + |b| = |a| + |b|$. \square

Означення 172. Відображення $\phi: \mathbb{Q} \rightarrow \mathbb{Q}$ називають *нормуванням поля* \mathbb{Q} із значеннями в \mathbb{Q} , якщо ϕ має такі 3 властивості:

- 1) $\phi(a) \geq 0$, $\phi(a) = 0 \Leftrightarrow a = 0$,
- 2) $\phi(ab) = \phi(a)\phi(b)$,
- 3) $\phi(a + b) \leq \phi(a) + \phi(b)$.

Отже, бачимо, що абсолютна величина $|a|$ є нормуванням.

Тепер переконаємося, що існують і інші нормування поля \mathbb{Q} .

Означення 173. Нехай p просте число. Якщо $a \in \mathbb{Q}$, $a \neq 0$, то існує єдине $k \in \mathbb{Z}$, для якого $a = p^k \frac{m}{n}$, де m і n взаємно прості з p . Означимо

$$|a|_p = p^{-k} \text{ і } |0|_p = 0.$$

і назовемо $|a|_p$ *p-адичною нормою числа a*.

Твердження 174. *p-адична норма є нормуванням поля* \mathbb{Q} *зі значеннями в* \mathbb{Q} .

Доведення. Властивість 1) з означення 172 очевидна. Властивість 2) доводиться дуже просто: якщо $a = p^k \frac{m}{n}$, $b = p^l \frac{m_1}{n_1}$, то $|ab|_p = \mathbb{F}|p^{k+l} \frac{mm_1}{nn_1}| = p^{-k-l} = |a|_p \cdot |b|_p$.

Що стосується 3), то ми доведемо навіть сильнішу нерівність $|a+b|_p \leq \max\{|a|_p, |b|_p\}$. Нехай, наприклад, $k \leq l$. Тоді $|a+b|_p = \mathbb{F}|p^k \frac{m}{n} + p^l \frac{m_1}{n_1}|_p = \mathbb{F}|p^k \frac{m+p^{l-k}m_1}{n n_1}|_p = \mathbb{F}|p^{k+s} \frac{m_2}{n n_1}|_p$, де $s \geq 0$, m_2 і nn_1 взаємно прості з p . Отже, $|a+b|_p = p^{-k} \cdot p^{-s} \leq p^{-k} = \max\{|a|_p, |b|_p\} \leq |a|_p + |b|_p$. \square

Означення 175. Нормування ϕ поля \mathbb{Q} називають *неархімедовим*, якщо воно має властивості 1) і 2) з означення 172 і властивість

$$3') \quad \phi(a + b) \leq \max\{\phi(a), \phi(b)\}.$$

З доведення твердження 174 випливає, що кожне *p-адичне нормування* є неархімедовим. Абсолютну величину називають ще *архімедовим нормуванням поля* \mathbb{Q} .

Пізніше ми доведемо (див. теорему Островського), що абсолютна величина та *p-адичні нормування* вичерпують, по-суті, всі можливі нормування поля раціональних чисел \mathbb{Q} . Всі ці нормування зв'язані між

собою за допомогою так званої формулі добутку, яку ми доводимо у твердженні 176.

Для одноманітності позначень введемо символ ∞ і позначимо абсолютну величину числа $a \in \mathbb{Q}$ символом $|a|_\infty$. Нехай S множина, що є об'єднанням множини всіх простих чисел P і символу ∞ : $S = P \cup \{\infty\}$. Вірне таке

Твердження 176 (формула добутку). Якщо $a \in \mathbb{Q}$, $a \neq 0$, то

$$\prod_{p \in S} |a|_p = 1.$$

Доведення. Для $a = 1$ формула очевидна. Якщо $a \neq 1$, то запишемо a у вигляді

$$a = \pm p_1^{k_1} \cdot p_t^{k_t},$$

де $t \leq 0$, $k_1, \dots, k_t \in \mathbb{Z} \setminus \{0\}$, p_1, \dots, p_t різні прості числа, що входять в розклад чисельника або знаменника числа a в добуток простих чисел.

Маємо

$$\prod_{p \in S} |a|_p = |a|_\infty \cdot |a|_{p_1} \cdots |a|_{p_t} = p_1^{k_1} \cdots p_t^{k_t} \cdot p_1^{-k_1} \cdots p_t^{-k_t} = 1.$$

□

23.4 Послідовності раціональних чисел

Означення 177. Послідовністю $\{a_n\}$ елементів поля K називають відображення $f: \mathbb{N} \rightarrow K$, де $a_n = f(n)$.

Поняття послідовності дійсних чисел добре відоме з аналізу. Але з точки зору, прийнятої в цьому параграфі (в якому ми зайняті побудовою числових систем, починаючи з множини натуральних чисел \mathbb{N}), ми, поки-що, не маємо у своїму розпорядженні поля дійсних чисел \mathbb{R} , а маємо лише поле \mathbb{Q} разом з множиною нормувань поля \mathbb{Q} , серед яких одне архімедове нормування $|\cdot|_\infty$, що є звичайною абсолютною величиною, і нескінчена множина неархімедових нормувань $|\cdot|_p$, по одному для кожного простого числа p . Тому тепер ми розглядаємо лише послідовності раціональних чисел, але у всіх означеннях символ $|a|$ буде означати не лише абсолютну величину числа $a \in \mathbb{Q}$, але й будь-яку p -адичну норму числа a .

Означення 178. Послідовність раціональних чисел $\{a_n\}$ називають *обмеженою*, якщо існує раціональне число $M > 0$ таке, що $|a_n| < M$ для всіх $n \in \mathbb{N}$. Послідовність раціональних чисел $\{a_n\}$ називають *збіжною* до раціонального числа a (записують це $\lim_{n \rightarrow \infty} a_n = a$), якщо

$$\forall \varepsilon \in \mathbb{Q}, \exists n_0 \in \mathbb{N} \quad n > n_0 \Rightarrow |a_n - a| < \varepsilon. \quad (23.4.1)$$

Збіжну послідовність $\{a_n\}$ називають *0-послідовністю*, якщо $\lim_{n \rightarrow \infty} a_n = 0$.

Послідовність раціональних чисел $\{a_n\}$ називають *фундаментальною*, якщо $\lim_{n,m \rightarrow \infty} |a_n - a_m| = 0$, тобто

$$\forall \varepsilon \in \mathbb{Q}, \exists n_0 \in \mathbb{N} \quad (n > n_0 \wedge m > n_0) \Rightarrow |a_n - a_m| < \varepsilon. \quad (23.4.2)$$

Приклади. 1) Послідовність $\mathbb{F}_{\{\frac{1}{2^n}\}}$ обмежена, а послідовність $\{n\}$ необмежена, якщо $\|\cdot\| = \|\cdot\|_\infty$, але послідовність $\{n\}$ обмежена, якщо $\|\cdot\| = \|\cdot\|_p$, де p просте число, Оскільки $|n|_p = p^{-k} \leq 1$, де p^k найбільша степінь p , що ділить n . Послідовність $\mathbb{F}_{\{\frac{1}{2^n}\}}$ необмежена, якщо $\|\cdot\| = \|\cdot\|_2$.

2) Якщо $\|\cdot\| = \|\cdot\|_\infty$, то $\lim_{n \rightarrow \infty} \frac{n^2+2}{3n^2+5} = \frac{1}{3}$, а послідовність $\{(-1)^n\}$ не є збіжною. Якщо $\|\cdot\| = \|\cdot\|_5$, то $\lim_{n \rightarrow \infty} 5^n = 0$, тобто послідовність $\{5^n\}$ збігається у цьому випадку до 0.

3) $\mathbb{F}_{\{\frac{1}{n+1}\}}$ 0-послідовність, якщо $\|\cdot\| = \|\cdot\|_\infty$, $\{n2^n\}$ 0-послідовність, якщо $\|\cdot\| = \|\cdot\|_2$.

Твердження 179. Якщо нормування $\|\cdot\|$ неархімедове (тобто p -адичне), то послідовність $\{a_n\}$ є фундаментальною тоді і тільки тоді, коли

$$\forall \varepsilon \in \mathbb{Q}, \exists n_0 \in \mathbb{N} \quad n > n_0 \Rightarrow |a_n - a_{n+1}| < \varepsilon. \quad (23.4.3)$$

Доведення. Досить показати, що у випадку неархімедового нормування з умови (23.4.3) випливає умова (23.4.2). Нехай, наприклад, $m > n$. Маємо, використовуючи неархімедовість нормування $\|\cdot\|$,

$$\begin{aligned} |a_n - a_m| &\leq |(a_n - a_{n+1}) + (a_{n+1} - a_{n+2}) + \cdots + (a_{m-1} - a_m)| \leq \\ &\leq \max_k \{|a_k - a_{k+1}|\} < \varepsilon. \end{aligned}$$

□

Твердження 180. а) Коєсна збіжна послідовність фундаментальна.
б) Коєсна фундаментальна послідовність обмежена.

Доведення. Міркування такі ж, як і ті, що застосовуються в курсі математичного аналізу для послідовностей дійсних чисел.

а) Використовуючи (23.4.1), одержуємо для $n > n_0$, $m > n_0$:

$$|a_n - a_m| = |a_n - a + a - a_m| \leq |a_n - a| + |a - a_m| < 2\varepsilon.$$

б) Зауважимо, що з нерівності трикутника $|a + b| \leq |a| + |b|$ випливають нерівності

$$|a| - |b| \leq \mathbb{F}|a| - |b| \leq |a \pm b| \leq |a| + |b|. \quad (23.4.4)$$

Нехай $\{a_n\}$ фундаментальна послідовність. Тоді існує $n_0 \in \mathbb{N}$ з властивістю $|a_n - a_{n_0+1}| < 1$ для всіх $n > n_0$. Звідси одержуємо, використовуючи (23.4.4), $|a_n| < 1 + |a_{n_0+1}|$. Тоді $|a_n| < 1 + M$ для всіх $n \in \mathbb{N}$, якщо $M = \max\{|a_0|, \dots, |a_{n_0+1}|\}$. \square

Приклади. 1) Кожна збіжна послідовність з попередніх прикладів є фундаментальною.

2) Послідовність $1+p, 1+p^2, \dots, 1+p^n, \dots$ є фундаментальною, якщо $|| = ||_p$.

Зауваження 181. Якщо послідовність збіжна, то вона має лише одну границю, тобто з рівностей $\lim_{n \rightarrow \infty} a_n = a$ і $\lim_{n \rightarrow \infty} a_n = b$ випливає, що $a = b$. Доведіть це самостійно.

23.5 Поповнення поля \mathbb{Q}

Тепер наша мета — побудувати для поля \mathbb{Q} і нормування $||_p$, де p просте число або $p = \infty$, поле \mathbb{Q}_p , в якому (як виявиться пізніше) кожна фундаментальна послідовність відносно нормування $||_p$ є збіжною. Якщо $p = \infty$, то в результаті ми отримаємо поле дійсних чисел, $\mathbb{Q}_\infty = \mathbb{R}$. Якщо p просте число, то відповідне поле \mathbb{Q}_p називають *полем p -адичних чисел*.

Розглянемо для цього множину Φ_p всіх фундаментальних послідовностей поля раціональних чисел. Індекс p тут означає, що ми розглядаємо одне з нормувань $||_p$ поля \mathbb{Q} , не виключаючи і випадок, коли $p = \infty$.

Введемо на множині Φ_p операції додавання і множення: якщо $\{a_n\}$, $\{b_n\} \in \Phi_p$, то

$$\{\alpha_n\} + \{\beta_n\} = \{\alpha_n + \beta_n\}, \quad \{\alpha\} \cdot \{\beta_n\} = \{\alpha_n \beta_n\}.$$

Теорема 182. Сума і добуток двох фундаментальних послідовностей є фундаментальними послідовностями. Множина всіх фундаментальних послідовностей Φ_p є комутативною областю цілісності. Множина \mathcal{I}_p всіх 0-послідовностей кільця Φ_p є ідеалом і фактор-кільце $\mathbb{Q}_p = \Phi_p/\mathcal{I}_p$ є полем, \mathbb{Q}_p розширення поля \mathbb{Q} .

Доведення. Перш за все потрібно перевірити, що сума і добуток фундаментальних послідовностей є знову фундаментальними послідовностями. Маємо

$$|(a_n + b_n) - (a_m + b_m)| \leq |a_n - a_m| + |b_n - b_m| < 2\varepsilon,$$

де $n > n_0$, $m > n_0$, а n_0 вибране так, що $|a_n - a_m| < \varepsilon$ і $|b_n - b_m| < \varepsilon$. Це означає, що $\{a_n + b_n\}$ фундаментальна послідовність.

Тепер використаємо той факт, що фундаментальна послідовність обмежена. Нехай $M \in \mathbb{Q}$ таке, що $|a_n| < M$ і $|b_n| < M$ для всіх $n \in \mathbb{N}$. Тоді

$$\begin{aligned} |a_n b_n - a_m b_m| &= |a_n b_n - a_n b_m + a_n b_m - a_m b_m| \leq \\ &\leq |a_n||b_n - b_m| + |b_m||a_n - a_m| < 2\varepsilon M, \end{aligned}$$

тобто $\lim_{n,m \rightarrow \infty} |a_n b_n - a_m b_m| = 0$ і послідовність $\{a_n b_n\}$ фундаментальна.

Легко зрозуміти, що множина Φ_p є комутативним кільцем з 1 відносно визначених вище операцій. Зауважимо лише, що нейтральними елементами для додавання та множення є “сталі” послідовності $\{0\}$ та $\{1\}$.

Перевіримо, що множина \mathcal{I}_p всіх 0-послідовностей є ідеалом кільця Φ_p . Якщо $\lim_{n \rightarrow \infty} a_n = 0$ і $\lim_{n \rightarrow \infty} b_n = 0$, то $\lim_{n \rightarrow \infty} (a_n + b_n) = 0$, бо $|a_n + b_n| \leq |a_n| + |b_n| < 2\varepsilon$ для $n \in \mathbb{N}$ таких, що $|a_n| < \varepsilon$ і $|b_n| < \varepsilon$. Далі, якщо $\lim_{n \rightarrow \infty} a_n = 0$ і $\{c_n\} \in \Phi_p$, то існує $M \in \mathbb{Q}$, $M > 0$ з властивістю $|c_n| < M$ для всіх $n \in \mathbb{N}$ за твердженням 1806). Тому з $|a_n| < \varepsilon$ випливає $|a_n c_n| = |c_n||a_n| \leq M|a_n| < M\varepsilon$ для досить великих n , тобто $\{a_n c_n\} \in \mathcal{I}_p$, а тому $\mathcal{C}\mathcal{I}_p$ ідеал кільця Φ_p .

Фактор-кільце $\mathbb{Q}_p = \Phi_p/\mathcal{I}_p$ є полем. Справді, нехай $\overline{\{a_n\}} = \{a_n\} + \mathcal{C}\mathcal{I}_p$ ненульовий елемент з \mathbb{Q}_p . Це означає, що фундаментальна послідовність $\{a_n\}$ не належить \mathcal{I}_p . З фундаментальності $\{a_n\}$ маємо: $\forall \varepsilon > 0, \exists n_0 \in \mathbb{N}$ з властивістю $m > n_0 \wedge n > n_0 \Rightarrow |a_m - a_n| < \frac{\varepsilon}{2}$. Але, Оскільки, $\{a_n\} \notin \mathcal{I}_p$, то існує n_1 , $n_1 > n_0$ і $|a_{n_1}| > \varepsilon$. Звідси одержуємо для $n > n_0$

$$\varepsilon < |a_{n_1}| = |a_n + a_{n_1} - a_n| \leq |a_n| + |a_{n_1} - a_n| \leq |a_n| + \frac{\varepsilon}{2}$$

або $|a_n| > \frac{\varepsilon}{2}$ для всіх $n > n_0$.

Розглянемо послідовність $\{d_n\}$, де $d_n = 1$ для $n \leq n_0$ і $d_n = a_n^{-1}$ для $n > n_0$. Маємо $|d_n - d_m| = \left| \frac{1}{a_n} - \frac{1}{a_m} \right| = |a_n^{-1}a_m^{-1}| |a_n - a_m| \leq \frac{4}{\varepsilon^2} |a_n - a_m| \xrightarrow[m,n \rightarrow \infty]{} 0$ (тут ε фіксоване), отже, $\{d_n\} \in \Phi_p$. Крім цього, $a_n d_n = 1$ для $n > n_0$, а це означає, що $\{\overline{d_n}\} = \{\overline{a_n}\}^{-1}$ в \mathbb{Q}_p .

Нарешті, ототожнимо кожний елемент $a \in \mathbb{Q}$ з класом “сталої” послідовності. Для цього розглянемо відображення $\phi: \mathbb{Q} \rightarrow \mathbb{Q}_p$, $\phi(a) = \{\bar{a}\} = \{a\} + \mathcal{I}_p$. ϕ є ін'єктивним гомоморфізмом поля \mathbb{Q} в поле \mathbb{Q}_p , тому, ототожнивши \mathbb{Q} з його образом $\phi(\mathbb{Q})$ можна вважати, що \mathbb{Q}_p є розширенням поля \mathbb{Q} . \square

Означення 183. Поля \mathbb{Q}_p , побудовані в процесі доведення теореми називають *поповненнями поля \mathbb{Q} відносно нормувань $|\cdot|_p$* .

23.6 Абсолютна величина в полі \mathbb{Q}_∞

Означимо у полі \mathbb{Q}_∞ відношення порядку. Надалі елементи поля \mathbb{Q}_∞ позначатимемо $\alpha, \beta, \dots, \alpha_1, \alpha_2, \dots$.

Лема 184. Якщо $\alpha \in \mathbb{Q}_\infty$, $\alpha \neq 0$ і α зображеній фундаментальною послідовністю $\{a_n\}$, то існує $n_1 \in \mathbb{N}$ такий, що для всіх $n > n_1$ числа a_n всі додатні або всі від'ємні.

Доведення. В процесі доведення теореми 182 ми бачили, що існує $n_0 \in \mathbb{N}$ з властивістю $|a_n| > \frac{\varepsilon}{2}$ для деякого $\varepsilon > 0$ і всіх $n > n_0$. Оскільки $\{a_n\}$ фундаментальна послідовність, то існує $n'_0 \in \mathbb{N}$, що з $m > n'_0$, $n > n'_0$ випливає $|a_m - a_n| < \varepsilon$. Нехай $n_1 = \max\{n_0, n'_0\}$. Якби для $m > n_1$ і $n > n_1$ числа a_m і a_n мали різні знаки, то ми одержали б $|a_m - a_n| = |a_m| + |a_n| > \varepsilon$. Суперечність. \square

З доведеного випливає, що можна дати таке

Означення 185. Нехай $\alpha \in \mathbb{Q}_\infty$, $\alpha \neq 0$. Скажемо, що $\alpha > 0$, якщо $a_n > 0$ для всіх досить великих n і $\alpha < 0$, якщо $a_n < 0$ для всіх досить великих n . Тут $\{a_n\}$ будь-яка фундаментальна послідовність, що належить суміжному класу α .

Зрозуміло, що це означення коректне, тобто не залежить від вибору представника $\{a_n\}$ в класі α . Все ж запропонуємо читачеві довести це.

Означення 186. Для $\alpha, \beta \in \mathbb{Q}_\infty$ скажемо, що $\alpha > \beta$, якщо $\alpha - \beta > 0$ і $\alpha - \beta \geq 0$, якщо $\alpha - \beta > 0$ або $\alpha = \beta$.

Твердження 187. 1) $\alpha < \beta$ або $\alpha = \beta$ або $\beta < \alpha$,

- 2) $\alpha \leq \beta \Rightarrow \alpha + \gamma \leq \beta + \gamma$,
- 3) $\alpha \leq \beta, \gamma \geq 0 \Rightarrow \alpha\gamma \leq \beta\gamma$,
- 4) $\alpha \geq 0, \beta \geq 0 \Rightarrow \alpha\beta \geq 0$.
- 5) \mathbb{Q}_∞ впорядковане поле.

Доведення нескладне і ми його пропускаємо.

Означення 188. Для $\alpha \in \mathbb{Q}_\infty$ з представником $\{a_n\}$ назовемо *абсолютною величиною* $|\alpha|$ клас з представником $\mathbb{F}_{\{|\alpha|\}}$.

Це означення коректне, бо з фундаментальності послідовності $\{a_n\}$ випливає фундаментальність послідовності $\{|a_n|\}$ в силу нерівності $||a_m| - |a_n|| \leq |a_n - a_m|$. З означення, отже, випливає, що $|\alpha| \in \mathbb{Q}_\infty$ і $|\alpha| = \max\{\alpha, -\alpha\}$ відносно означеного вище відношення порядку.

Твердження 189. Абсолютна величина $||$ має такі властивості:

- 1) $|\alpha| \geq 0, |\alpha| = 0 \Leftrightarrow \alpha = 0$;
- 2) $|\alpha\beta| = |\alpha||\beta|$;
- 3) $|\alpha + \beta| \leq |\alpha| + |\beta|$.

Інакше кажучи, абсолютна величина $||$ є нормуванням поля \mathbb{Q}_∞ зі значеннями в \mathbb{Q}_∞ .

Доведення. 1) безпосередньо випливає з означення за лемою 184.

2) теж випливає з означення абсолютної величини, з означення множення в полі \mathbb{Q}_∞ та з відповідної властивості абсолютної величини в полі \mathbb{Q} .

Доведення 3) зводиться до доведення нерівності $|\alpha| + |\beta| - |\alpha + \beta| \geq 0$. Якщо $\{a_n\}$ і $\{b_n\}$ фундаментальні послідовності, що зображають α і β , то за означенням остання нерівність рівносильна нерівностям раціональних чисел $|a_n| + |b_n| - |a_n + b_n| \geq 0$ для всіх досить великих n . Але ці нерівності вірні навіть для всіх n за відповідною властивістю абсолютної величини в полі \mathbb{Q} . \square

Зauważення 190. Якщо $a \in \mathbb{Q}$, то представником a в \mathbb{Q}_∞ є стала послідовність $\{a_n\}$, а представником $|a|$ є стала послідовність $\mathbb{F}_{\{|\alpha|\}}$. Тому можна вважати, що абсолютна величина в полі \mathbb{Q}_∞ для раціональних чисел дорівнює абсолютної величині в полі \mathbb{Q} .

Завершимо цей п. одним дуже простим і важливим твердженням.

Твердження 191. Поле \mathbb{Q}_∞ задоволяє аксіому Архімеда.

Доведення. Оскільки \mathbb{Q} є підполем поля \mathbb{Q}_∞ , то $\mathbb{N} \subset \mathbb{Q}_\infty$. Нехай $\alpha \in \mathbb{Q}_\infty$. Розглянемо $|\alpha| \in \mathbb{Q}_\infty$. $|\alpha|$ зображеній фундаментальною послідовністю $\mathbb{F}_{\{|a_n|\}}$, яка обмежена за твердженням 180. Тому існує $M \in \mathbb{Q}$ з властивістю $M > |a_n|$, отже, $M \geq |\alpha|$. $M = \frac{a}{b}$ з $a, b \in \mathbb{N}$, $b > 0$. Розділимо a на b з остачею. Одержано $M = \frac{bd+r}{b} < d + 1$. Тому для $n = d + 1$ матимемо $n > |\alpha| \geq \alpha$, що й потрібно було довести. \square

23.7 Повнота поля \mathbb{Q}_∞

Теорема 192. Поле \mathbb{Q}_∞ повне, тобто кожна фундаментальна послідовність $\{a_n\}$ з елементів поля \mathbb{Q}_∞ є збіжною.

Доведення. Нехай $\{\alpha_n\}$ фундаментальна послідовність в \mathbb{Q}_∞ . Нагадаємо, що всі α_n є суміжними класами, що складаються з фундаментальних послідовностей раціональних чисел. Нехай послідовність раціональних чисел $\{a_{nm}\}$ є представником класу α_n . Складемо з усіх послідовностей $\{a_{nm}\}$ “діагональну послідовність” $\{a_{nn}\}$. Переконаємося, що $\{a_{nn}\}$ фундаментальна послідовність раціональних чисел. З фундаментальноті полідовності $\{\alpha_n\}$ випливає, що для кожного $\varepsilon \in \mathbb{Q}_\infty$, $\varepsilon > 0$,

$$|\alpha_n - \alpha_m| < \varepsilon$$

для досить великих m і n , що, в свою чергу, означає, що

$$|a_{nk} - a_{mk}| < \varepsilon. \quad (23.7.1)$$

З фундаментальності послідовності $\{a_{nm}\}$ одержуємо, що для кожного $\varepsilon \in \mathbb{Q}_\infty$, $\varepsilon > 0$ вірна нерівність

$$|a_{nl} - a_{ns}| < \varepsilon \quad (23.7.2)$$

для досить великих n і s . З (23.7.1) і (23.7.2) маємо

$$|a_{mm} - a_{nn}| = |a_{mm} - a_{mn} + a_{mn} - a_{nn}| \leq |a_{mm} - a_{mn}| + |a_{mn} - a_{nn}| < 2\varepsilon$$

для досить великих m і n . Це означає, що послідовність $\{a_{nn}\}$ фундаментальна.

Нехай α елемент поля \mathbb{Q}_∞ з представником $\{a_{nn}\}$. Покажемо, що $\lim_{n \rightarrow \infty} \alpha_n = \alpha$. Для цього досить показати, що $\lim_{n,m \rightarrow \infty} |a_{nm} - a_{mm}| = 0$, але це випливає з (23.7.1). \square

23.8 Щільність \mathbb{Q} в \mathbb{Q}_∞

Теорема 193. *Кожний елемент $\alpha \in \mathbb{Q}_\infty$ є границею послідовності раціональних чисел.*

Доведення. Нехай α має своїм представником фундаментальну послідовність $\{a_n\}$, де $a_n \in \mathbb{Q}$. Тоді елемент $\alpha - a_n$ має представником послідовність $a_m - a_n$ (де n фіксоване, а $m \in \mathbb{N}$). З фундаментальності $\{a_n\}$ одержуємо, що $\lim_{m,n \rightarrow \infty} |a_n - a_m| = 0$, а це й означає, що $\lim_{n \rightarrow \infty} a_n = \alpha$. \square

23.9 Поле дійсних чисел

Ми побудували впорядковане поле \mathbb{Q}_∞ , яке є розширенням поля \mathbb{Q} , задовільняє аксіому Архімеда і аксіому повноти. У вступі до цього параграфа було сказано, що ці властивості є якраз аксіомами поля дійсних чисел \mathbb{R} . Отже, ми можемо стверджувати, що побудоване поле \mathbb{Q}_∞ є полем дійсних чисел. Наведений спосіб побудови поля \mathbb{R} належить Кантору. Зауважимо, що існують і інші методи побудови поля дійсних чисел. Два найвідоміших серед них це метод перерізів Дедекінда та метод Вейєрштраса, у якому дійсні числа є нескінченними десятковими дробами.

Після побудови поля \mathbb{R} будь-яким з цих способів виникають два питання. Перше з них — питання єдності і відповідь на це питання така: \mathbb{R} визначається своїми аксіомами однозначно з точністю до топологічного ізоморфізму над \mathbb{Q} (тобто ізоморфізму полів, що переводить фундаментальні послідовності у фундаментальні послідовності і залишає всі раціональні числа незмінними). Пропонуємо читачеві довести це самостійно (див. вправу 6 і вказівку до неї).

Друге питання — це питання про несуперечливість, тобто, по-суті, питання про існування дійсних чисел. Це питання значно складніше, воно зводиться до віри в те, що аксіоми теорії множин та аксіоми арифметики (аксіоми Пеано), які використовуються при побудові поля \mathbb{R} , не можуть привести до суперечності. Це є одне свідчення того, що дійсні числа є досить складним об'єктом.

На завершення цього параграфа покажемо як дійсні числа (тобто класи еквівалентних фундаментальних послідовностей раціональних чисел) можна записувати у вигляді нескінчених десяткових дробів.

Теорема 194. *a) Для кожного дійсного числа α , $0 \leq \alpha < 1$, існує послідовність $\{d_n\}$ раціональних чисел, що належить класу α і має вигляд*

$$d_0 = 0; d_1 = 0, c_1; d_2 = 0, c_1 c_2; \dots; d_n = 0, c_1 c_2 \dots c_n; \dots,$$

де $c_i \in \{0, 1, 2, \dots, 9\}$. Тому α можна ототожнити з нескінченим десятковим дробом

$$\alpha = 0, c_1 c_2 \dots c_n \dots$$

б) Кожне дійсне число α можна ототожнити з нескінченим десятковим дробом

$$\alpha = \pm 10^{-m}(0, c_1 c_2 \dots c_n \dots).$$

Доведення. а) Якщо $\alpha = 0$, то покладемо $\alpha = 0,00\dots$ Нехай $\alpha > 0$. З впорядкованості поля \mathbb{R} одержуємо, що існує $c_1 \in \{0, 1, 2, \dots, 9\}$ з властивістю $\frac{c_1}{10} \leq \alpha < \frac{c_1+1}{10}$. Звідси $c_1 \leq 10\alpha < c_1 + 1$, тому так само існує $c_2 \in \{0, 1, 2, \dots, 9\}$, для якого $c_1 + \frac{c_2}{10} \leq 10\alpha < c_1 + \frac{c_2+1}{10}$ або $0, c_1 c_2 \leq \alpha < 0, c_1 c_2 + 10^{-2}$. За індукцією одержуємо, що існують $c_1, c_2, \dots, c_n \in \{0, 1, \dots, 9\}$, для яких

$$0, c_1 c_2 \dots c_n \leq \alpha < 0, c_1 c_2 \dots c_n + 10^{-n}.$$

Для послідовності $d_n = 0, c_1 c_2 \dots c_n$ маємо $|\alpha - d_n| < 10^{-n}$, тому $\lim_{n \rightarrow \infty} d_n = \alpha$, отже, послідовність d_n належить класу α . Це дозволяє записати $\alpha = 0, c_1 c_2 \dots c_n \dots$

б) Досить довести це твердження для випадку $\alpha > 0$. В іншому випадку розглядається число $-\alpha$. За аксіомою Архімеда існує натуральне число n з властивістю $\alpha < n$. Якщо $10^m \geq n$, то $\frac{\alpha}{10^m} < 1$. Звідси за доведеним $\frac{\alpha}{10^m} = 0, c_1 c_2 \dots c_n \dots$, тому $\alpha = 10^m(0, c_1 c_2 \dots c_n \dots)$. \square

Підсумуємо. В цьому параграфі ми побудували поле дійсних чисел \mathbb{R} як поповнення поля раціональних чисел відносно абсолютної величини. Більш глибоке вивчення поля \mathbb{R} є предметом математичного аналізу. Враховуючи це, ми вважатимемо відомими елементарні властивості деяких функцій від дійсного аргумента (таких як a^x , x^a , $\log_a x$, де $a \in \mathbb{R}$), що будуть використані в параграфі 3. Крім поля \mathbb{R} , ми маємо ще нескінченну кількість полів \mathbb{Q}_p поповнень поля \mathbb{Q} відносно p -адичних нормувань. Їх вивченю присвячений наступний параграф.

24 Теорема Островського

24.1 Еквівалентні нормування

Ми вже мали справу з нормуваннями поля раціональних чисел (абсолютна величина та p -адичні нормування) та їх продовженнями до нормувань поля дійсних чисел та полів p -адичних чисел. Всі ці нормування були частковими випадками наступного загального поняття.

Означення 195. Нормуванням поля K називають відображення $||: K \rightarrow \mathbb{R}$, що має такі властивості:

- 1) $|\alpha| \geq 0$, $|\alpha| = 0 \Leftrightarrow \alpha = 0$,
- 2) $|\alpha\beta| = |\alpha| \cdot |\beta|$,
- 3) $|\alpha + \beta| \leq |\alpha| + |\beta|$.

Якщо разом з властивостями 1), 2) нормування $||$ має властивість
3') $|\alpha + \beta| \leq \max\{|\alpha|, |\beta|\}$,

то таке нормування називають *неархімедовим*.

Пригадаємо, що поля дійсних та p -адичних чисел є поповненнями поля раціональних чисел відносно абсолютної величини або відносно одного з p -адичних нормувань. З теореми Островського, якій присвячено цей параграф, випливає, що інших поповнень поля раціональних чисел не має.

Для формулювання теореми Островського нам потрібне поняття еквівалентних нормувань.

Означення 196. Нехай $||_1$ і $||_2$ два нормування поля K із значеннями в \mathbb{R} . Нормування $||_2$ називають *еквівалентним* нормуванню $||_1$, якщо існує $\rho \in \mathbb{R}$, $\rho > 0$, таке, що $|a|_2 = |a|_1^\rho$ для кожного $a \in K$.

Твердження 197. Якщо $||: K \rightarrow \mathbb{R}$ нормування і $||_1: K \rightarrow \mathbb{R}$ відображення, таке, що існує $\rho \in \mathbb{R}$, $0 < \rho < 1$, і $|a|_1 = |a|^\rho$ для всіх $a \in K$, то $||_1$ нормування поля K , причому $||_1$ неархімедове для будь-якого $\rho > 0$, якщо $||$ неархімедове.

Доведення. Нам потрібно перевірити, що відображення $||_1^\rho$ задовольняє властивості 1), 2), 3) з означення нормування. Для властивостей 1), 2) це очевидно. Властивість 3) випливає з такого міркування. Якщо $\beta = 0$, то нерівність 3) має вигляд $|\alpha| \leq |\alpha|$ і доводити нічого.

Припустимо, що $|\alpha| \leq |\beta|$, $\beta \neq 0$. Тоді

$$\begin{aligned} |\alpha + \beta|^\rho &= |\beta|^\rho \left| 1 + \frac{\alpha}{\beta} \right|^\rho \leq |\beta|^\rho \left| 1 + \frac{|\alpha|}{|\beta|} \right|^\rho \leq \\ &\leq |\beta|^\rho \left(1 + \frac{|\alpha|}{|\beta|} \right) \leq |\beta|^\rho \left| 1 + \left(\frac{|\alpha|}{|\beta|} \right)^\rho \right| = |\alpha|^\rho + |\beta|^\rho. \end{aligned}$$

Якщо $||$ неархімедове, то $|\alpha + \beta| \leq \max\{|\alpha|, |\beta|\}$. Звідси, очевидно, випливає $|\alpha + \beta|^\rho \leq \max\{|\alpha|^\rho, |\beta|^\rho\}$. \square

З доведеного твердження випливає, що коли $||$ будь-яке нормування поля раціональних чисел і $0 < \rho < 1$ ($\rho > 0$ у випадку неархімедового нормування), то $||^\rho$ теж нормування поля \mathbb{Q} . Зауважимо, що коли

ми маємо фундаментальну або збіжну послідовність раціональних чисел відносно нормування $\|\cdot\|$, то вона залишається фундаментальною або збіжною і відносно $\|\cdot|^p$. З цього зауваження випливає просте, але важливе

Твердження 198. Якщо нормування $\|\cdot\|_1$ і $\|\cdot\|_2$ поля K еквівалентні, то поповнення відносно цих нормувань одинакові.

25 Поле \mathbb{Q}_p

25.1 Нормування поля \mathbb{Q}_p

Покажемо, що p -адичне нормування $\|\cdot\|_p$ поля \mathbb{Q} (див. означення 173 та твердження 174) можна продовжити до нормування поля \mathbb{Q}_p . Спочатку доведемо дві прості леми.

Лема 199. Якщо $a, b \in \mathbb{Q}$, $|a|_p \neq |b|_p$, то $|a + b|_p = \max\{|a|_p, |b|_p\}$.

Доведення. Нехай $a = p^k \frac{r}{s}$, $b = p^l \frac{r_1}{s_1}$, де r, s, r_1, s_1 взаємно прості з p і нехай $|a|_p < |b|_p$, тобто $k > l$. Маємо

$$|a + b|_p = \left| p^k \frac{r}{s} + p^l \frac{r_1}{s_1} \right|_p = \left| p^l \right|_p \frac{p^{k-l} rs_1 + sr_1}{ss_1} = p^{-l} = |b|_p,$$

Оскільки ss_1 та $p^{k-l}rs_1 + sr_1$ взаємно прості з p . □

Лема 200. Нехай $\{a_n\}$ фундаментальна відносно p -адичного нормування $\|\cdot\|_p$ послідовність раціональних чисел, яка не є 0-послідовністю. Тоді існує $n_0 \in \mathbb{N}$ таке, що $|a_n|_p = |a_m|_p$ для всіх $n > n_0$, $m > n_0$.

Доведення. Оскільки $\{a_n\}$ не 0-послідовністю, то існує $\varepsilon \in \mathbb{Q}$, $\varepsilon > 0$ таке, що для кожного n_0 знайдеться $n > n_0$ з властивістю $|a_n|_p > \varepsilon$. З фундаментальності $\{a_n\}$ випливає, що для вказаного ε знайдеться n_0 , для якого з нерівностей $m > n_0$, $n > n_0$ випливає нерівність $|a_m - a_n|_p < \varepsilon$. Використовуючи лему 199, маємо

$$|a_m|_p = |a_n + a_m - a_n|_p = \max\{|a_n|_p, |a_m - a_n|_p\} = |a_n|_p,$$

де $m > n_0$ і $n > n_0$. □

З леми 200 випливає, що для фундаментальної послідовності раціональних чисел $\{a_n\}$ послідовність $\{|a_n|_p\}$ стабілізується, тобто $\{|a_n|_p\}$ стає сталою для досить великих n , якщо $\lim_{n \rightarrow \infty} a_n \neq 0$. Якщо ж $\lim_{n \rightarrow \infty} a_n =$

0, то і $\lim_{n \rightarrow \infty} |a_n|_p = 0$. В кожному випадку існує границя $\lim_{n \rightarrow \infty} |a_n|_p$. Отже, p -адичне нормування поля раціональних чисел можна продовжити до нормування поля p -адичних чисел.

Означення 201. Якщо $\alpha \in \mathbb{Q}_p$ і $\{a_n\}$ — фундаментальна послідовність раціональних чисел, що є представником числа α , то за означенням

$$|\alpha|_p = \lim_{n \rightarrow \infty} |a_n|_p.$$

Нормування $|\cdot|_p$ задовольняє всі умови з означення нормування, тобто

- 1) $|\alpha|_p \geq 0$, $|\alpha|_p = 0 \Leftrightarrow \alpha = 0$,
- 2) $|\alpha\beta|_p = |\alpha|_p \cdot |\beta|_p$,
- 3) $|\alpha + \beta|_p \leq \max \{|\alpha|_p, |\beta|_p\} \leq |\alpha|_p + |\beta|_p$.

Справді, властивість 1) безпосередньо випливає з означення. Властивість 2) є наслідком того факту, що границя добутку дорівнює добутку границь. Якщо $\alpha = 0$ або $\beta = 0$, то властивість 3) очевидна. В іншому випадку всі послідовності $\{|(a_n + b_n)|_p\}$, $\{|a_n|_p\}$ та $\mathbb{F}_{\{b_n\}} \{b_n\}$ стабілізуються для досить великих n . Тому нерівність 3) випливає з нерівності

$$|a_n + b_n|_p \leq \max \{|a_n|_p, |b_n|_p\}.$$

25.2 Повнота поля \mathbb{Q}_p та щільність \mathbb{Q} а \mathbb{Q}_p

Для всіх полів \mathbb{Q}_p , як і для поля \mathbb{R} , вірні такі теореми.

Теорема 202 (про повноту \mathbb{Q}_p). *Поле \mathbb{Q}_p повне, тобто кожна фундаментальна послідовність $\{\alpha_n\}$ з елементами з \mathbb{Q}_p є збіжною.*

Теорема 203 (про щільність). *Поле \mathbb{Q}_p щільне в \mathbb{Q}_p , тобто кожне p -адичне число є границею послідовності раціональних чисел.*

Доведення. Доведення дослівно повторюють доведення теорем 192 та 193 з п. 23.7 про повноту та щільність для поля $\mathbb{R} = \mathbb{Q}_\infty$. Рекомендуємо читачеві просто переписати ці доведення, замінюючи абсолютну величину $|\cdot|$ на p -адичне нормування $|\cdot|_p$. \square

25.3 Канонічні зображення p -адичних чисел

Ми означили дійсні і p -адичні числа як класи еквівалентних фундаментальних послідовностей раціональних чисел. При такому підході єдина відмінність між дійсними та p -адичними числами полягає в тому, що для

побулови поля \mathbb{R} використовується абсолютна величина в полі \mathbb{Q} , а для побудови поля \mathbb{Q}_p p -адичне нормування.

З такими числами – класами важко працювати, тому корисно в кожному класі вибрати зручні представники і працювати з представниками. Так у випадку скінченного поля $\mathbb{Z}/p\mathbb{Z}$, елементами якого теж є суміжні класи, правда значно простішої природи, ми вибираємо представники $0, 1, \dots, p-1$ всіх різних суміжних класів і працюємо з $\bar{0}, \bar{1}, \dots, \bar{p-1}$.

Для випадку поля дійсних чисел ми вже показали в п. 23.9, що кожне $\alpha \in \mathbb{R}$ зображається нескінченим десятковим дробом

$$\pm 10^m(0, c_1 c_2 \dots c_n \dots),$$

де $c_i \in \{0, 1, \dots, 9\}$, інакше кажучи, в класі α існує послідовність раціональних чисел вигляду

$$\{\pm 10^m(0, c_1 c_2 \dots c_n)\}.$$

Наша мета тепер вказати аналогічне зображення для p -адичних чисел.

Теорема 204. *Нехай $\alpha \in \mathbb{Q}_p$, $|\alpha|_p = p^{-m}$. В класі α існує едина фундаментальна послідовність раціональних чисел*

$$\{p^m(a_0 + a_1 p + \dots + a_n p^n)\}, \quad (25.3.1)$$

де $a_0, a_1, \dots, a_n \in \{0, 1, \dots, p-1\}$, $a_0 \neq 0$, $m \in \mathbb{Z}$.

Інакше кажучи, кожне ненульове p -адичне число зображається у вигляді нескінченного ряду

$$p^m(a_0 + a_1 p + \dots + a_n p^n + \dots), \quad (25.3.2)$$

де послідовність (25.3.1) є послідовністю часткових сума ряду (25.3.2).

Для доведення теореми нам потрібна

Лема 205. *Для кожного простого числа p , кожного ненульового раціонального числа $\frac{r}{s}$ з $(s, p) = 1$ і кожного натурального числа n існує ціле число c , $0 \leq c < p^n$, що має властивість $|c - \frac{r}{s}|_p \leq p^{-n}$.*

Доведення. Оскільки $(s, p) = 1$, то конгруенція $sx \equiv r \pmod{p^n}$ має єдиний розв'язок. Отже, існує c , $0 \leq c < p^n$, $sc - r = p^n t$, де $t \in \mathbb{Z}$. Звідси $|c - \frac{r}{s}|_p = |\frac{cs-r}{s}|_p = |\frac{p^n t}{s}|_p \leq p^{-n}$, що й потрібно було довести. \square

Тепер повернімось до доведення теореми 204.

Доведення. Нехай, спочатку, $|\alpha|_p \leq 1$. Тоді в класі α можна вибрати послідовність $\{b_n\}$ з властивістю $|b_n|_p \leq 1$, а в силу фундаментальності послідовності $\{b_n\}$ у ній можна вибрати підпослідовність $\{b_{i_n}\}$ з властивістю

$$|b_{i_n} - b_{i_{n-1}}|_p < p^{-n}.$$

Перепозначивши b_{i_n} знову на b_n , одержуємо, що існує послідовність $\{b_n\}$ представник класу α з властивостями

$$|b_n - b_{n-1}| < p^{-n}, \quad (25.3.3)$$

$$|b_n|_p \leq 1. \quad (25.3.4)$$

Нехай $b_n = \frac{r_n}{s_n}$, де $r_n, s_n \in \mathbb{Z}$. З (25.3.4) випливає, що можна вважати $(s_n, p) = 1$. Тоді з леми 205 одержуємо, що існує єдине ціле c_n , яке її розв'язком конгруенції $s_n x \equiv r_n \pmod{p^{n+1}}$, $0 \leq c_n < p^{n+1}$ таке, що

$$|b_n - c_n|_p < p^{-n-1}. \quad (25.3.5)$$

Нерівність (25.3.5) означає, що послідовності $\{b_n\}$ та $\{c_n\}$ еквівалентні, тобто $\{c_n\}$ є представником класу α . Зауважимо, що з нерівності $0 \leq c_n < p^{n+1}$ випливає, що ціле число c_n можна записати у вигляді

$$c_n = a_0 + a_1 p + \cdots + a_n p^n, \quad (25.3.6)$$

де $a_0, \dots, a_n \in \{0, 1, \dots, p-1\}$, a_0, \dots, a_n однозначно визначаються числом c_n , яке, в свою чергу, однозначно визначається умовою (25.3.5) та умовою $0 \leq c_n < p^{n+1}$. Крім цього маємо, використовуючи нерівності (25.3.3) і (25.3.5),

$$\begin{aligned} |c_n - c_{n-1}|_p &= |c_n - b_n + b_n - b_{n-1} + b_{n-1} - c_{n-1}| \leq \\ &\leq \max \{|c_n - b_n|_p, |b_n - b_{n-1}|_p, |b_{n-1} - c_{n-1}|_p\} \leq \\ &\leq \max \{p^{-n-1}, p^{-n}, p^{-n}\} = p^{-n}, \end{aligned}$$

тобто

$$c_n \equiv c_{n-1} \pmod{p^n}. \quad (25.3.7)$$

З конгруенції (25.3.7) випливає, що коли $c_n = a_0 + a_1 p + \cdots + a_n p^n$, то $c_{n+1} = c_n + a_{n+1} p^{n+1}$, де $a_{n+1} \in \{0, 1, \dots, p-1\}$.

Разом все це означає, що послідовність цілих чисел $\{c_n\}$, що є представником p -адичного числа α , можна інтерпретувати як послідовність часткових сум такого ряду

$$a_0 + a_1 p + \cdots + a_n p^n + \dots, \quad (25.3.8)$$

причому послідовність $a_0, a_1, \dots, a_n, \dots$, $0 \leq a_i < p$, однозначно визначається числом α . З умови $|\alpha|_p = p^{-m} \leq 1$ випливає, що $a_0 = \dots = a_{m-1} = 0$ і ряд (25.3.8) набуває вигляду $p^m(a_m + a_{m+1}p + \dots + a_{m+n}p^n + \dots)$. Замінивши в цьому виразі a_m на a_0, \dots, a_{m+n} на a_n і т.д., одержуємо (25.3.2).

Залишившися випадок $|\alpha|_p > 1$. Нехай $p^m = |\alpha|_p > 1$. Тоді $|p^{-m}\alpha|_p = 1$, і за доведенням $p^{-m}\alpha$ є границею послідовності часткових сум ряду

$$a_0 + a_1p + \dots + a_np^n + \dots,$$

де $a_0 \neq 0$. Тому α є границею послідовності часткових сум ряду

$$p^m(a_0 + a_1p + \dots + a_np^n + \dots).$$

□

Використовуючи зображення p -адичних чисел у вигляді рядів (25.3.2), над ними можна виконувати операцію додавання та множення за тим же принципом, що і додавання та множення дійсних чисел. Щоб проілюструвати це, наведемо приклади на додавання. Нехай $\alpha = 5^{-2} + 2 \cdot 5^{-1} + 1 + 2 \cdot 5 + 3 \cdot 5^2 + \dots$ і $\beta = 3 \cdot 5^{-1} + 3 + 4 \cdot 5 + 2 \cdot 5^2 + \dots$ два 5-адичні числа. Маємо

$$\begin{aligned} & 5^{-2} + 2 \cdot 5^{-1} + 1 + 2 \cdot 5 + 3 \cdot 5^2 + \dots \\ & + \\ & \frac{3 \cdot 5^{-1} + 3 + 4 \cdot 5 + 2 \cdot 5^2 + \dots}{5^{-2} + 5 \cdot 5^{-1} + 4 + 6 \cdot 5 + 5 \cdot 5^2 + \dots =} \\ & = 5^{-2} + 1 + 4 + 1 \cdot 5 + 6 \cdot 5^2 + \dots = \\ & = 5^{-2} + 2 \cdot 5 + 1 \cdot 5^2 + \dots \end{aligned}$$

$$\alpha + \beta = 5^{-2} + 5^{-2} + 2 \cdot 5 + 1 \cdot 5^2 + \dots.$$

25.4 Арифметика поля \mathbb{Q}_p

У початковому розумінні арифметика це наука про натуральні (цілі) числа, зокрема, про властивості подільності цих чисел. Тому, коли в якому-небудь полі розглядають підкільце цього поля і вивчають дільники одиниці, прості елементи, розклад на прості множники та інші поняття такого типу, то кажуть, що вивчають арифметику цього поля.

В цьому п. ми виділиммо в полі p -адичних чисел \mathbb{Q}_p підкільце \mathbb{Z}_p , яке назовемо кільцем цілих p -адичних чисел, і вивчимо арифметику цього кільця.

Означення 206. Число $\alpha \in \mathbb{Q}_p$ називають *цілим p-адичним числом*, якщо $|\alpha|_p \leq 1$. Множину всіх цілих p -адичних чисел позначають $= \mathbb{Z}_p$.

Введемо поняття p -показника p -адичного числа α .

Означення 207. Нехай $\alpha \in \mathbb{Q}_p$, $\alpha \neq 0$. Якщо $|\alpha|_p = p^{-m}$, то m називають *p-показником числа α* і пишуть $m = v_p(\alpha)$. За означенням $v_p(0) = \infty$.

Очевидно, що $m = v_p(\alpha) \iff |\alpha|_p = p^{-m}$.

У термінах p -показника означення 206 можна переформулювати так.

Означення 208. Число $\alpha \in \mathbb{Q}_p$ називають *цілим p-адичним числом*, якщо $v_p(\alpha) \geq 0$.

Твердження 209. \mathbb{Z}_p підкільце поля \mathbb{Q}_p . Поле \mathbb{Q}_p є полем дробів кільця \mathbb{Q}_p .

Доведення. З властивостей

$$|\alpha|_p \leq 1, \quad |\beta|_p \leq 1 \implies |\alpha\beta|_p \leq 1 \text{ і } |\alpha + \beta|_p \leq \max \mathbb{F} \{ |\alpha|_p, |\beta|_p \} \leq 1$$

випливає, що \mathbb{Z}_p замкнене відносно операцій додавання та множення. Звідси легко випливає, що \mathbb{Z}_p підкільце.

Очевидно, поле дробів кільця \mathbb{Z}_p міститься в \mathbb{Q}_p . Навпаки, якщо $\alpha \in \mathbb{Q}_p$, $v_p(\alpha) = m$, то $v_p(p^{-m}\alpha) = 0$, тобто $\beta = p^{-m}\alpha \in \mathbb{Z}_p$ і $\alpha = \frac{\beta}{p^m}$, звідси бачимо, що α належить полю дробів кільця \mathbb{Z}_p . \square

Тепер знайдемо одиниці кільця \mathbb{Z}_p .

Твердження 210. Елемент $u \in \mathbb{Z}_p$ є одиницею кільця \mathbb{Z}_p тоді і тільки тоді, коли $|u|_p = 1$.

Доведення. Якщо $u|1$, то існує $v \in \mathbb{Z}_p$, $uv = 1$. Звідси $|u|_p \cdot |v|_p = 1$ і $|u|_p \leq 1$, $|v|_p \leq 1$, а тому $|u|_p = 1$.

Навпаки, нехай $|u|_p = 1$. Для u існує обернений v у полі \mathbb{Q}_p . Отже, $uv = 1$, $|uv|_p = |uv|_p = |u|_p \cdot |v|_p = 1$, звідси $|v|_p = 1$, тому $v \in \mathbb{Z}_p$. \square

Наслідок 211. Коjsne ненульове p -адичне число α однозначно записується у вигляді $\alpha = p^m u$, де $m = v_p(\alpha) \in \mathbb{Z}$, $u \in \mathbb{Z}_p$, $u|1$.

Доведення. Якщо $\alpha = p^m u = p^n v$, де $u|1$, $v|1$, то $m = n = v_p(\alpha)$. Звідси $p^n(u - v) = 0$ і тому $u = v$. \square

Наслідок 212. У кільці цілих p -адичних чисел \mathbb{Z}_p існує єдиний з точністю до дільників одиниці простий елемент. Це просте число p .

Доведення. Нехай q простий елементакільце \mathbb{Z}_p . З наслідку 211 маємо $q = p^m u$, де $u|1$, а $m = v_p(\alpha) \in \mathbb{N}$, оскільки в даному випадку $\alpha \in \mathbb{Z}_p$. Тому, обов'язково $m = 1$, отже, $q = pu$, що і стверджує наслідок 212. \square

Наслідок 213. *Кільце \mathbb{Z}_p факторіальне.*

Доведення. Якщо $\alpha \in \mathbb{Z}_p$, $\alpha \neq 0$, то за наслідком 211 α однозначно записується у вигляді $\alpha = p^m u$, де p простий елемент, $m \geq 0$, $u|1$. \square

Бачимо, що арифметика в кільці \mathbb{Z}_p дуже проста: існує єдиний простий елемент і кожний елементакільця \mathbb{Z}_p є добутком деякого степеня цього простого елемента p і дільника одиниці.

Наслідок 214. *Якщо $\alpha, \beta \in \mathbb{Z}_p$, то $\alpha|\beta$ тоді і тільки тоді, коли $v_p(\alpha) \leq v_p(\beta)$.*

Доведення. Нехай $\alpha = p^m u$, $\beta = p^n v$. Якщо $\alpha|\beta$, то $\beta = \alpha\gamma$, де $\gamma = p^r w$. Тут u, v, w дільники 1. Звідси $p^n v = p^{m+r} u w$, отже, $m \leq n$. Навпаки, якщо $n \leq m$, то для елемента $\gamma = p^{n-m} u^{-1} v$, одержуємо $\beta = \alpha\gamma$. \square

Твердження 215. *Кожний ненульовий ідеал кільця \mathbb{Z}_p має вигляд $p^n \mathbb{Z}_p$, отже, є головним. Фактор кільце $\mathbb{Z}_p / p^n \mathbb{Z}_p$ скінченне і складається з p^n елементів і в кожному суміжному класі цього кільця існує представник вигляду*

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

де $a_i \in \{0, 1, \dots, p-1\}$.

Доведення. Нехай I ненульовий ідеал, $n = \min_{\alpha \in I} \{v_p(\alpha)\}$. Тоді кожний елемент $\alpha \in I$ має вигляд $\alpha = p^m u$, де $m \geq n$, $u|1$. Це ѹ означає, що I головний ідеал, породжений елементом p^n .

З теореми 204 випливає, що кожне ціле p -адичне число зображається у вигляді нескінченного ряду $p^m(a_0 + a_1 p + \cdots + a_n p^n + \dots)$, де (у нашому випадку) $m \geq 0$, $a_i \in \{0, 1, \dots, p-1\}$. Отже, якщо не вимагати, щоб $a_0 \neq 0$, то бачимо, що кожне ціле p -адичне число може бути зображене у вигляді ряду

$$a_0 + a_1 p + \cdots + a_n p^n + \dots \tag{25.4.1}$$

Образом елемента (25.4.1) при канонічному гомоморфізмі $\mathbb{Z}_p \rightarrow \mathbb{Z}_p / p^n \mathbb{Z}_p$ є суміжний клас з представником

$$a_0 + a_1 p + \cdots + a_{n-1} p^{n-1}, \tag{25.4.2}$$

який теж можна трактувати як ряд вигляду (25.4.1) з $a_n = a_{n+1} = \dots = 0$.

Очевидно, різні числа вигляду (25.4.2) визначають різні елементи кільця $\mathbb{Z}_p/p^n\mathbb{Z}_p$. Оскільки $a_i \in \{0, 1, \dots, p-1\}$, то існує p^n чисел вигляду (25.4.2), і це завершує доведення. \square

25.5 Локальна компактність поля \mathbb{Q}_p

Означення 216. Поле K з нормуванням $||$ називають *локально компактним*, якщо кожна обмежена послідовність $\{\alpha_n\}$ елементів поля K містить збіжну підпослідовність.

В курсі математичного аналізу доводять, що поле дійсних чисел є локально компактним.

Теорема 217. Поле \mathbb{Q}_p локально компактне.

Доведення. Доведемо спочатку, що з кожної послідовності цілих p -адичних чисел можна вибрати збіжну підпослідовність. Нехай $\{\alpha_n\}$ послідовність цілих p -адичних чисел. З твердження 215 одержуємо, що $\mathbb{Z}_p/p\mathbb{Z}_p$ складається з p елементів, тому існує ціле число d_0 , $0 \leq d_0 < p$, і існує підпослідовність $\{\alpha_n^{(0)}\}$ послідовності $\{\alpha_n\}$ з властивістю

$$p|\alpha_n^{(0)} - d_0. \quad (25.5.1)$$

Далі, за твердженням 215, фактор-кільце $\mathbb{Z}_p/p^2\mathbb{Z}_p$ скінченне, тому так само існує ціле число d_1 , $0 \leq d_1 < p^2$ і підпослідовність $\{\alpha_n^{(1)}\}$ послідовності $\{\alpha_n^{(0)}\}$ з властивістю

$$p^2|\alpha_n^{(1)} - d_1. \quad (25.5.2)$$

З (25.5.1) і (25.5.2) маємо $p|(d_1 - \alpha_n^{(1)}) + (\alpha_n^{(1)} - d_0)$, тобто $p|d_1 - d_0$. Припустимо, що ми вже знайшли цілі числа d_0, d_1, \dots, d_{k-1} і підпослідовності $\{\alpha_n^{(0)}\} \supset \{\alpha_n^{(1)}\} \supset \dots \supset \{\alpha_n^{(k-1)}\}$ з властивостями

$$p^{i+1}|(\alpha_n^{(i)} - d_i), \quad (25.5.3)$$

$$p^i|d_i - d_{i-1} \quad (25.5.4)$$

для $1 \leq i \leq k-1$.

Оскільки $\mathbb{Z}_p/p^k\mathbb{Z}_p$ скінченне, то існує d_k , $0 \leq d_k < p^k$ і підпослідовність $\{\alpha_n^{(k)}\}$ послідовності $\{\alpha_n^{(k-1)}\}$ такі, що

$$p^{k+1}|(\alpha_n^{(k)} - d_k), \quad (25.5.5)$$

$$p^k|d_k - d_{k-1}. \quad (25.5.6)$$

Для доведення (25.5.6), зауважимо, що з (25.5.3) при $i = k - 1$ і з (25.5.5) випливає $p^k | ((d_k - \alpha_n^{(k)}) + (\alpha_n^{(k)} - d_{k-1}))$, тобто (25.5.6).

Таким чином, за індукцією ми маємо послідовність цілих чисел $d_0, d_1, \dots, d_n, \dots$ з властивістю $p^n | d_{n-1} - d_n$, тобто $|d_n - d_{n-1}| \leq p^{-n}$. Оскільки нормування $\|\cdot\|_p$ неархімедове, то це означає, що послідовність $\{d_n\}$ фундаментальна і, отже, визначає деяке ціле p -адичне число α .

Складемо тепер з усіх послідовностей $\{\alpha_n^{(k)}\}$ “діагональну” послідовність $\alpha_n^{(n)}$. Маємо

$$|\alpha_n^{(n)} - \alpha|_p = |\alpha_n^{(n)} - d_n + d_n - \alpha|_p \leq \max \left\{ |\alpha_n^{(n)} - d_n|, |d_n - \alpha| \right\} \xrightarrow{n \rightarrow \infty} 0,$$

отже, $\lim_{n \rightarrow \infty} \alpha_n^{(n)} = \alpha$ і ми виділили збіжну підпослідовність $\{\alpha_n^{(n)}\}$ послідовності $\{\alpha_n\}$.

Нехай тепер $\{\alpha_n\}$ довільна обмежена послідовність p -адичних чисел. Тоді існує $m \in \mathbb{Z}$, що послідовність $\{p^m \alpha_n\}$ є послідовністю цілих p -адичних чисел (якщо $|\alpha_n|_p \leq M$ для всіх $n \in \mathbb{N}$, то виберемо m так, щою $p^m \geq M$). За доведеним існує збіжна підпослідовність $\{p^m \alpha_{i_n}\}$ послідовності $\{p^m \alpha_n\}$. Отже, підпослідовність $\{\alpha_{i_n}\}$ є збіжною підпослідовністю послідовності $\{\alpha_n\}$. Теорему доведено. \square

25.6 алгебраїчні рівняння над \mathbb{Z}_p

Ми будемо розглядати многочлени $f(X_1, \dots, X_m) \in \mathbb{Z}_p[X_1, \dots, X_m]$ з цілими p -адичними коефіцієнтами. Оскільки кільце цілих чисел \mathbb{Z} є підкільцем кільця \mathbb{Z}_p , то кожен многочлен з цілими коефіцієнтами будемо вважати і многочленом з цілими p -адичними коефіцієнтами для кожного простого числа p .

Впорядковану послідовність p -адичних чисел $\alpha_1, \dots, \alpha_m$ таку, що $f(\alpha_1, \dots, \alpha_m) = 0$ в полі \mathbb{Q}_p будемо називати p -адичним розв'язком рівняння

$$f(X_1, \dots, X_m) = 0. \quad (25.6.1)$$

Нас будуть цікавити розв'язки рівнянь (25.6.1) в цілих p -адичних числах. У цьому випадку ми можемо вважати, що всі коефіцієнти многочлена $f(X_1, \dots, X_n)$ є рядами (тобто границями часткових сум таких рядів) вигляду

$$a_0 + a_1 + \dots + a_n p^n + \dots, \quad (25.6.2)$$

де $a_i \in \{0, 1, \dots, p-1\}$ і, аналогічно, цілі p -адичні розв'язки $(\alpha_1, \dots, \alpha_m)$ є такими, що кожне α_i зображається рядом вигляду (25.6.2).

Теорема 218. Якщо $f(X_1, \dots, X_m) \in \mathbb{Z}_p[X_1, \dots, X_m]$, то рівняння

$$f(X_1, \dots, X_m) = 0$$

має розв'язок в цілих p -адичних числах тоді і тільки тоді, коли конгруенція

$$f(X_1, \dots, X_m) \equiv 0 \pmod{p^n} \quad (25.6.3)$$

має розв'язок (c_{1n}, \dots, c_{mn}) , $c_{ij} \in \mathbb{Z}$ для всіх натуральних n .

Доведення. Якщо рівняння $f(X_1, \dots, X_n) = 0$ має розв'язок в цілих p -адичних числах, то для деяких $c_1, \dots, c_m \in \mathbb{Z}_p$ маємо

$$f(c_1, \dots, c_m) = 0.$$

Застосуємо до цієї рівності канонічний гомоморфізм $\mathbb{Z}_p \rightarrow \mathbb{Z}_p/p^n\mathbb{Z}_p$. Одержано

$$f(\bar{c}_1, \dots, \bar{c}_m) = 0$$

в $\mathbb{Z}_p/p^n\mathbb{Z}_p$, де можна вважати, що представники класів $\bar{c}_1, \dots, \bar{c}_m$ є ціліми числами вигляду

$$a_0 + a_1 p + \dots + a_{n-1} p^{n-1}.$$

Все це і означає, що конгруенція (25.6.3) має розв'язок в цілих числах.

Нехай, навпаки, всі конгруенції (25.6.3) мають розв'язок $(c_n^{(1)}, \dots, c_n^{(m)})$ в цілих числах. Всі послідовності цілих чисел $\{c_n^{(i)}\}$, $1 \leq i \leq m$, є обмеженими послідовностями цілих p -адичних чисел, Оскільки кожне ціле число є цілим p -адичним числом.

Застосовуючи теорему про локальну компактність поля \mathbb{Q}_p ми можемо вибрати збіжну підпослідовність $\{c_{n_1}^{(1)}\}$ послідовності $\{c_n^{(1)}\}$, далі вибираємо збіжну підпослідовність $\{c_{n_2}^{(2)}\}$ послідовності $\{c_n^{(2)}\}$ і т.д., вибираємо збіжну підпослідовність $\{c_{n_m}^{(m)}\}$ послідовності $\{c_n^{(m)}\}$. Тоді всі послідовності $\{c_{n_1}^{(1)}\}, \dots, \{c_{n_m}^{(m)}\}$ є збіжними. Нехай $\alpha_i = \lim_{n_m \rightarrow \infty} c_{n_m}^{(i)}$.

Оскільки многочлени з $\mathbb{Q}_p[X_1, \dots, X_m]$ є неперервними функціями з \mathbb{Q}_p^m в \mathbb{Q}_p (це доводиться так само, як і факт, що многочлени з $\mathbb{R}[X_1, \dots, X_m]$ є неперервними функціями з \mathbb{R}^m в \mathbb{R} : пропонуємо доведення в якості вправи), то з

$$f(c_{n_m}^{(1)}, \dots, c_{n_m}^{(1)}) \equiv 0 \pmod{p^{n_m}}$$

випливає

$$f(\alpha_1, \dots, \alpha_m) = \lim_{n_m \rightarrow \infty} f(c_{n_m}^{(1)}, \dots, c_{n_m}^{(1)}) = 0,$$

що й потрібно було довести. \square

З доведеної теореми випливає, що існування розв'язку в цілих p -адичних числах рівняння $f(X_1, \dots, X_m) = 0$, де $f(X_1, \dots, X_n)$ многочлен з цілими коефіцієнтами, рівносильне існуванню розв'язків конгруенцій

$$f(X_1, \dots, X_m) \equiv 0 \pmod{p^n}$$

для всіх натуральних n , тобто нескінченної сім'о конгруенцій. В наступному п. ми покажемо, що при деяких простих умовах на многочлен f існування цілого p -адичного розв'язку рівняння $f = 0$ рівносильне існуванню розв'язку одної-єдиної конгруенції, тобто питання про існування цілого розв'язку рівняння $f = 0$ може бути ефективно розв'язане за скінченне число кроків.

Нехай тепер $f(X_1, \dots, X_m) \in \mathbb{Z}_p[X_1, \dots, X_m]$ однорідний многочлен степеня k . У цьому випадку рівняння $f = 0$ має нульовий розв'язок. Вияснимо при яких умовах це рівняння має ненульовий розв'язок.

Теорема 219. Рівняння

$$f(X_1, \dots, X_n) = 0, \quad (25.6.4)$$

де f однорідний многочлен степеня k з цілими p -адичними коефіцієнтами, має ненульовий розв'язок тоді і тільки тоді, коли для кожного натурального n конгруенція

$$f(X_1, \dots, X_n) \equiv 0 \pmod{p^n}, \quad (25.6.5)$$

має розв'язок (c_{1n}, \dots, c_{nm}) в цілих числах, де не всі числа серед c_{1n}, \dots, c_{nm} діляться на p .

Доведення. Нехай $\alpha_1 = p^{r_1}u_1, \dots, \alpha_m = p^{r_m}u_m$, де u_1, \dots, u_m дільники 1, ненульовий розв'язок рівняння (25.6.4) в цілих p -адичних числах і нехай $r = \min\{r_1, \dots, r_m\}$. Тоді $\beta_1 = p^{r_1-r}u_1, \dots, \beta_m = p^{r_m-r}u_m$ теж розв'язок рівняння (25.6.4), причому хоч одне з чисел β_1, \dots, β_m є p -адичною одиницею. Припустимо, що це β_1 . Тоді в канонічному зображенні (25.6.2) для β_1 маємо $\alpha_0 \not\equiv 0 \pmod{p}$ і β_1 є границею послідовності цілих чисел $\{d_n\}$ з властивістю $d_n \not\equiv 0 \pmod{p}$. Звідси випливає, що конгруенція (25.6.4) має розв'язок (c_{1n}, \dots, c_{mn}) в цілих числах, де $c_{1n} = d_n$ не ділиться на p . Навпаки, якщо для кожного $n \in \mathbb{N}$ конгруенція (25.6.5) має розв'язок (c_{1n}, \dots, c_{mn}) , де не всі c_{1n}, \dots, c_{mn} діляться на p , то існує j , $1 \leq j \leq m$, що c_{jn} не ділиться на p для нескінченної кількості значень n . Припустимо, і це не зменшує загальності, що $j = 1$. Виберемо підпослідовність $\{c_{1n_k}\}$ послідовності $\{c_{1n}\}$ з властивістю $p \nmid c_{1n_k}$. Виходячи з послідовностей $\{c_{1n_k}\}, \dots, \{c_{mn_k}\}$, як і в теоремі 218 знаходимо розв'язок $\{\alpha_1, \dots, \alpha_m\}$ рівняння (25.6.4) в цілих p -адичних числах. Зрозуміло, що $p \nmid \alpha_1$, тому $\alpha_1 \neq 0$. \square

25.7 Лема Гензеля

Теорема 220. *Нехай $f(X) \in \mathbb{Z}_p[X]$ многочлен з цілими p -адичними коефіцієнтами. Припустимо, що існує ціле p -адичне число, для якого*

$$\begin{aligned} f(a_0) &\equiv 0 \pmod{p^{2\delta+1}}, \\ f'(a_0) &\equiv 0 \pmod{p^\delta}, \\ f''(a_0) &\not\equiv 0 \pmod{p^{\delta+1}}, \end{aligned}$$

де $\delta \geq 0$, $f'(X)$ похідна многочлена $f(X)$.

Тоді існує ціле p -адичне число α , таке, що $f(\alpha) = 0$ і $\alpha \equiv a_0 \pmod{p}$.

Доведення. Методом математичної індукції ми покажемо, що послідовність p -адичних чисел $\{\alpha_n\}$, визначена рекурентною формулою

$$\alpha_n = \alpha_{n-1} - \frac{f(\alpha_{n-1})}{f'(\alpha_{n-1})}, \quad (25.7.1)$$

ї фундаментальною послідовністю цілих p -адичних чисел і, якщо $\alpha = \lim \alpha_n$, то $f(\alpha) = 0$.

Доведемо, що послідовність, визначена формулою (25.7.1) має такі властивості

$$f(\alpha_n) \equiv 0 \pmod{p^{2\delta+n+1}}, \quad (25.7.2)$$

$$f'(\alpha_n) \equiv 0 \pmod{p^\delta}, \quad (25.7.3)$$

$$f''(\alpha_n) \not\equiv 0 \pmod{p^{\delta+1}}, \quad (25.7.4)$$

$$\alpha_n \equiv \alpha_{n-1} \pmod{p^{\delta+n}}. \quad (25.7.5)$$

Для $n = 0$ ці властивості (25.7.2) – (25.7.4) перетворюються в умови теореми, а про властивість (25.7.5) тут мови немає. Припустимо, що $n > 0$ і властивості (25.7.2) – (25.7.5) доведені для всіх α_m з $m < n$.

Розкладемо многочлен $f(X)$ за формулою Тейлора

$$f(X) = f(c) + (X - c) \frac{f'(c)}{1} + (X - c)^2 \frac{f''(c)}{2!} + \dots \quad (25.7.6)$$

і підставимо в (25.7.6) $c = \alpha_{n-1}$, $X = \alpha_n$. Одержано

$$f(\alpha_n) = \frac{1}{2} \left(\frac{f(\alpha_{n-1})}{f'(\alpha_{n-1})} \right)^2 f''(\alpha_{n-1}) + \dots .$$

Використовуючи (25.7.2) і (25.7.3) для $n - 1$ замість n , одержуємо

$$f(\alpha_n) \equiv 0 \pmod{p^{4\delta+2n-2\delta}} \equiv 0 \pmod{p^{2\delta+2n}} \equiv 0 \pmod{p^{2\delta+n+1}},$$

тобто властивість (25.7.2) доведена для всіх n .

$$\alpha_n - \alpha_{n-1} = -\frac{f(\alpha_{n-1})}{f'(\alpha_{n-1})} \equiv 0 \pmod{p^{2\delta+n-\delta}} \equiv 0 \pmod{p^{\delta+n}}$$

це властивість (25.7.5).

Звідси випливає, що $f'(\alpha_n) \equiv f'(\alpha_{n-1}) \pmod{p^{\delta+n}}$ і, зокрема, $f'(\alpha_n) \equiv 0 \pmod{p^\delta}$, $f'(\alpha_n) \not\equiv 0 \pmod{p^{\delta+1}}$, тобто всі властивості (25.7.2) – (25.7.5) доведені.

З (25.7.5) випливає фундаментальність послідовності $\{\alpha_n\}$. Переходячи в (25.7.2) до границі, одержуємо $f(\alpha) = 0$, де $\alpha = \lim_{n \rightarrow \infty} \alpha_n$, $\alpha \equiv \alpha_0 \pmod{p}$. \square

Доведену теорему називають ще *лемою Гензеля або р-адичною лемою Ньютона*. Остання назва пояснюється тим, що рекурентна формула (25.7.1) для послідовності $\{\alpha_n\}$ має такий самий вигляд, як і формула Ньютона

$$\alpha_n = \alpha_{n-1} - \frac{f(\alpha_{n-1})}{f'(\alpha_{n-1})}$$

для обчислення послідовних наближень кореня многочлена $f(X) \in \mathbb{R}[X]$ з дійсними коефіцієнтами (див., наприклад, Бахвалов Н.С., Численные методы, 2 изд., М., 1975).

Наслідок 221. *Нехай $f(X_1, \dots, X_m) \in \mathbb{Z}_p[X_1, \dots, X_m]$ многочлен з цілими р-адичними коефіцієнтами. Припустимо, що існують цілі р-адичні числа $\alpha_0^{(1)}, \dots, \alpha_0^{(m)}$ з властивостями*

$$\begin{aligned} f(\alpha_0^{(1)}, \dots, \alpha_0^{(m)}) &\equiv 0 \pmod{p^{2\delta+1}}, \\ \frac{df}{dX_{i_0}}(\alpha_0^{(1)}, \dots, \alpha_0^{(m)}) &\equiv 0 \pmod{p^\delta}, \\ \frac{df}{dX_{i_0}}(\alpha_0^{(1)}, \dots, \alpha_0^{(m)}) &\not\equiv 0 \pmod{p^{\delta+1}}, \end{aligned}$$

де $\delta \geq 0$, $1 \leq i_0 \leq m$. Тоді існують цілі р-адичні числа $\alpha^{(1)}, \dots, \alpha^{(m)}$, такі, що $f(\alpha^{(1)}, \dots, \alpha^{(m)}) = 0$ і $\alpha^{(i)} \equiv \alpha_0^{(i)} \pmod{p}$, $1 \leq i \leq m$.

Доведення. Розглянемо многочлен

$$f(\alpha_0^{(1)}, \dots, \alpha_0^{(i_0-1)}, X, \alpha_0^{(i_0+1)}, \dots, \alpha_0^{(m)}) = h(X).$$

За теоремою 220 існує $\alpha^{(i_0)} \equiv \alpha_0^{(i_0)} \pmod{p}$, для якого $h(\alpha^{(i_0)}) = 0$. Візьмемо $\alpha^{(k)} = \alpha_0^k$ для $k \neq i_0$. Тоді $\alpha^{(1)}, \dots, \alpha^{(m)}$ є шуканим розв'язком рівняння $f(X_1, \dots, X_n) = 0$. \square

Наслідок 222. Нехай $f(X) \in \mathbb{Z}_p[X]$ многочлен з цілими p -адичними коефіцієнтами. Припустимо, що існує ціле p -адичне число α_0 , для якого

$$\begin{aligned} f(\alpha_0) &\equiv 0 \pmod{p}, \\ f'(\alpha_0) &\not\equiv 0 \pmod{p}. \end{aligned}$$

Тоді існує ціле p -адичне число α , таке, що $f(\alpha) = 0$ і $\alpha \equiv \alpha_0 \pmod{p}$.

Доведення. Цей наслідок частковий випадок теореми при $\delta = 0$. \square

Приклад. Використаємо наслідок 222 для обчислення декількох перших членів послідовності натуральних чисел, що збігається до $\sqrt{3}$ в \mathbb{Q}_{11} .

Розглянемо рівняння $X^2 - 3 = 0$, де $X^2 - 3 \in \mathbb{Z}_{11}[X]$. $\alpha_0 = 5$ є розв'язком конгруенції $X^2 - 3 \equiv 0 \pmod{11}$ і не є розв'язком конгруенції $2X \equiv 0 \pmod{11}$, отже, задовольняє умови наслідку 222. Обчислимо $\alpha_1 = \left(\alpha_0 - \frac{f(\alpha_0)}{f'(\alpha_0)} \right) \pmod{11^2}$, де $f(X) = X^2 - 3$. Маємо

$$\begin{aligned} \alpha_1 &= \left(5 - \frac{2 \cdot 11}{10} \right) \pmod{11^2} \equiv (5 + 2 \cdot 11) \pmod{11^2}, \\ \alpha_2 &= \left(27 - \frac{6 \cdot 11^2}{2 \cdot 27} \right) \pmod{11^3} \equiv (27 + 6 \cdot 11^2) \\ &\quad \pmod{11^3} \equiv (5 + 2 \cdot 11 + 6 \cdot 11^2) \pmod{11^3}. \end{aligned}$$

Отже, початок канонічного зображення одного із коренів рівняння $X^3 - 3 = 0$ в \mathbb{Z}_{11} має такий вигляд

$$5 + 2 \cdot 11 + 6 \cdot 11^2 + \dots$$

Зауважимо, що рівняння $X^3 - 3 = 0$ має ще один корінь β , для якого $\beta \equiv 6 \pmod{11}$.

У цьому прикладі обчислення можна проводити і іншим способом. Запишемо

$$(a_0 + a_1 11 + a_2 11^2 + \dots)^2 = 3$$

і спробуємо знайти $a_0, a_1, a_2, \dots \in \{0, 1, \dots, 10\}$ так, щоб була справедливою остання рівність. Ця рівність означає, що $a_0^2 \equiv 3 \pmod{11}$. Звідси $a_0 = 5$ або $a_0 = 6 \pmod{11}$, і далі, якщо $a_0 = 5$:

$$25 + 2 \cdot 5a_1 \cdot 11 \equiv 3 \pmod{11^2}. \text{ Тому } 10a_1 \equiv -2 \pmod{11}.$$

$$\text{Звідси } a_1 = 2, a_0 + a_1 11 = 27.$$

$$27^2 + 2 \cdot 27a_2 \cdot 11^2 \equiv 3 \pmod{11^3}. \text{ Тому } 54a_2 \equiv -6 \pmod{11}.$$

$$\text{Звідси } a_2 \equiv 6 \pmod{11}$$

і т.д. Бачимо, що одержується такий же результат, як і раніше.

25.8 Теорема Острівського

Зауважимо, що серед нормувань кожного поля K із значеннями в полі \mathbb{R} є одне, так зване, тривіальне нормування, для якого $|0| = 0$ і $|\alpha| = 1$ для кожного $\alpha \in K$, $\alpha \neq 0$.

Якщо ми спробуємо побудувати поповнення поля \mathbb{Q} відносно тривіального нормування, то прийдемо знову до поля \mathbb{Q} . Оскільки фундаментальними послідовностями у цьому випадку є послідовності $\{a_n\}$, які починаючи з деякого натурального n стають постійними, тобто $a_n = a_{n+1} = \dots$.

Теорема 223 (теорема Острівського). *Кожне нетривіальне нормування поля \mathbb{Q} еквівалентне одному з p -адичних нормувань $||_p$ або звичайній абсолютної величині $||_\infty = ||$.*

Доведення. Нехай $||$ нетривіальне нормування поля \mathbb{Q} . Зафіксуємо $a \in \mathbb{N}$, $a > 1$. Якщо $b \in \mathbb{N}$, $b > 0$, то b можна записати у вигляді

$$b = b_0 + b_1 a + \dots + b_{m-1} a^{m-1} + b_m a^m,$$

де $0 \leq b_j < a$, $0 \leq j \leq m$, $b_m \neq 0$. Тут $b \geq a^m$, тому $\lg b \geq m \lg a$ і $m \leq \frac{\lg b}{\lg a}$. Використовуючи властивість 3) з означення нормування (тобто нерівність трикутника), одержуємо

$$|b| \leq |b_0| + |b_1||a| + \dots + |b_{m-1}||a^{m-1}| + |b_m||a^m| \leq M(1 + |a| + \dots + |a|^m), \quad (25.8.1)$$

де $M = \max \mathbb{F}\{|1|, |2|, \dots, |a-1|\}$.

Якщо $|a| \leq 1$, то $1 + |a| + \dots + |a|^m \leq m + 1 \leq \frac{\lg b}{\lg a} + 1$. Якщо $|a| > 1$, то $1 + |a| + \dots + |a|^m \leq (m+1)|a|^m \leq \left(\frac{\lg b}{\lg a} + 1\right) |a|^{\frac{\lg b}{\lg a}}$.

Підставимо це у нерівність (25.8.1):

$$|b| \leq M \left(\frac{\lg b}{\lg a} + 1 \right) \max \left\{ 1, |a|^{\frac{\lg b}{\lg a}} \right\}.$$

Підставимо в цю нерівність $b = c^n$:

$$|c|^n \leq M \left(\frac{n \lg c}{\lg a} + 1 \right) \max \left\{ 1, |a|^{\frac{n \lg c}{\lg a}} \right\}.$$

Звідси $\lim_{n \rightarrow \infty} \sqrt[n]{|c|^n} \leq \max \mathbb{F}\{1, |a|^{\frac{\lg c}{\lg a}}\} \lim_{n \rightarrow \infty} \sqrt[n]{M} \lim_{n \rightarrow \infty} \sqrt[n]{\frac{n \lg c}{\lg a} + 1}$ або

$$|c| \leq \max \left\{ 1, |a|^{\frac{\lg c}{\lg a}} \right\}. \quad (25.8.2)$$

Розглянемо два випадки.

1) Існує натуральне число c з властивістю $|c| > 1$. Підставимо таке c у (25.8.2). Одержано

$$|c| \leq |a|^{\frac{\lg c}{\lg a}}. \quad (25.8.3)$$

Звідси випливає, що $|a| > 1$ для кожного $a > 1$. Далі, з (25.8.3) маємо

$$|c|^{\frac{1}{\lg c}} \leq |a|^{\frac{1}{\lg a}},$$

і, міняючи ролями a і c ,

$$|a|^{\frac{1}{\lg a}} \leq |c|^{\frac{1}{\lg c}},$$

тобто

$$|a|^{\frac{1}{\lg a}} = |c|^{\frac{1}{\lg c}}. \quad (25.8.4)$$

Оскільки $|a| > 1$, то існує $\alpha \in \mathbb{R}$, $\alpha > 0$, що $|a| = |a|_\infty^\alpha$. Тоді з (25.8.4) маємо

$$|c| = |a|^{\frac{\lg c}{\lg a}} = \mathbb{F} |a^{\frac{\lg c}{\lg a}}|_\infty^\alpha = \mathbb{F} |c^{\log_c a^{\frac{\lg c}{\lg a}}}|_\infty^\alpha = \mathbb{F} |c^{\frac{\lg a}{\lg c} \cdot \frac{\lg c}{\lg a}}|_\infty^\alpha = |c|_\infty^\alpha.$$

Це означає, що наше нормування еквівалентне абсолютної величині на множині \mathbb{N} . Звідси випливає, що воно еквівалентне абсолютної величині і на множині \mathbb{Q} .

2) $|c| \leq 1$ для всіх ненульових натуральних чисел c .

Оскільки нормування $||$ нетривіальне, то існує просте число p з властивістю $|p| < 1$, оскільки в іншому випадку, беручи до уваги властивість 2) з означення нормування, ми одержали б, що $|c| = 1$ для всіх натуральних чисел c , а звідси легко випливає, що нормування $||$ тривіальне.

Існує лише одне просте число з властивістю $|p| < 1$, бо якби існувало ще одне просте число q , для якого $|q| < 1$, то ми одержали для деякого натурального n

$$|q|^n < \frac{1}{2} \quad \text{i} \quad |p|^n < \frac{1}{2}.$$

Але q^n і p^n взаємно прости, тому існують такі цілі u, v , що $up^n + vq^n = 1$.

Звідси

$$1 = |1| = |up^n + vq^n| \leq |u||p^n| + |v||q^n| < \frac{1}{2} + \frac{1}{2} = 1,$$

і ми приходимо до суперечності.

Нехай $|p| = \rho$, де $0 < \rho < 1$, $x = p^{v_p(x)} \frac{a}{b}$ раціональне число і $v_p(x)$ p -показник числа x (див. п.25.4). Тоді

$$|x| = |p|^{v_p(x)} \frac{|a|}{|b|} = |p|^{v_p(x)} = \rho^{v_p(x)}.$$

Бачимо, що наше нормування $\| \cdot \|$ еквівалентне p -адичному нормуванню $\| \cdot \|_p$, для якого $|x|_p = \left(\frac{1}{p}\right)^{v_p(x)}$. \square

Вправи.

1. Нехай K впорядковане поле (див. вступ до розділу 22.3). Довести, що
 - a) K лінійно впорядкована множина;
 - б) $\forall a \in K \setminus \{0\} \quad a^2 > 0$;
 - в) $\text{char } K = 0$ і K містить підполе, ізоморфне полю раціональних чисел \mathbb{Q} .
2. Довести, що додавання та множення натуральних чисел, означені в п. 23.1, мають такі властивості:
 - а) $a + (b + c) = (a + b) + c$;
 - б) $a' = a + 1 = 1 + a$, де $1 = 0'$;
 - в) $a + b = b + a$;
 - г) $0 \cdot a = 1, \quad 1 \cdot a = a \cdot 1 = a$;
 - д) $(a + b)c = ac + bc$;
 - е) $ab = ba$;
 - ж) $(ab)c = a(bc)$.
3. Довести, що означена в п. 23.2 множина цілих чисел \mathbb{Z} є областю цілісності.
4. Довести, що поле раціональних чисел \mathbb{Q} є впорядкованим полем лише відносно одного відношення порядку (тобто звичайного).
5. Довести, що в полі комплексних чисел \mathbb{C} не можна ввести таке відношення порядку, відносно якого воно було б впорядкованим.

Вказівка. Розглянути випадок $i > 0$ та $i < 0$.

6. Нехай \mathbb{R}_1 та \mathbb{R}_2 два впорядкованих поля, що задовольняють аксіомі Архімеда та аксіомі повноти. Довести, що існує ізоморфізм $\varphi: \mathbb{R}_1 \rightarrow \mathbb{R}_2$ над \mathbb{Q} (тобто $\varphi(a) = a$ для всіх $a \in \mathbb{Q}$).

Вказівка. \mathbb{Q} щільне в \mathbb{R}_1 і в \mathbb{R}_2 . Поставимо у відповідність елементу $x \in \mathbb{R}_1$ елемент $y = \varphi(x) \in \mathbb{R}_2$, якщо x і y є границями тих самих послідовностей раціональних чисел.

7. Для довільного нормування $\|\cdot\|$ поля K довести неперервність операцій додавання, множення та знаходження оберненого елемента. Довести, що многочлен $f(X) \in K[X]$ визначає неперервну функцію з K в \mathbb{R} .
8. Довести, що нормування $\|\cdot\|$ поля K неархімедове тоді і тільки тоді, коли $|n \cdot 1| \leq 1$, де 1 у виразі $n \cdot 1$ означає одиничний елемент поля K , а 1 у правій частині нерівності означає дійсне число 1 .
9. Довести, що два еквівалентних нормування поля K є одночасно архімедові або одночасно неархімедові.
10. Довести, що два p -адичні нормування $\|\cdot\|_{p_1}$ та $\|\cdot\|_{p_2}$ нееквівалентні, якщо p_1 і p_2 різні прості числа.
11. Нехай $x \in \mathbb{Q}$ і $|x|_p \leq 1$ для всіх простих p . Довести, що $x \in \mathbb{Z}$.
12. Довести, що кожне нормування скінченного поля тривіальне (тобто $|0| = 0$ і $|a| = 1$ для всіх $a \neq 0$).
13. Довести, що кожне нормування поля характеристики p є неархімедовим.
14. Довести, що канонічне зображення числа $a \in \mathbb{Q}_p$ обривається (тобто $a_i = 0$ для всіх i , що більші від деякого натурального числа n) тоді і тільки тоді, коли a додатне раціональне число, знаменник якого є степенем p .
15. Довести, що канонічне зображення числа $a \in \mathbb{Q}_p$ починаючи з деякого номера періодичне (тобто існує n , що $a_{i+r} = a_i$ для деякого r і всіх $i > n$).
16. Знайти канонічні зображення чисел: а) -8 в \mathbb{Q}_7 ; б) $-\frac{1}{6}$ в \mathbb{Q}_7 ; в) $-\frac{3}{10}$ в \mathbb{Q}_{11} .
17. Знайти канонічні зображення з 4-ма знаками для
 - а) $(1 + 2 \cdot 3 + 1 \cdot 3^2 + 2 \cdot 3^3 + \dots)(1 + 3 + 3^2 + 3^3 + \dots)$;
 - б) $(2 + 3 \cdot 5 + 4 \cdot 5^2 + 2 \cdot 5^3 + \dots)$;
 - в) $\sqrt{3}$ в \mathbb{Q}_{13} .
18. Для яких p можна добути квадратний корінь з -1 в \mathbb{Q}_p ?
19. Довести, що ряд $1 + p + p^2 + p^3 + \dots$ збігається до $(1 - p)^{-1}$ в \mathbb{Q}_p .

20. Довести, що коли $(m, p) = 1$, то кожний дільник одиниці $u \in \mathbb{Z}_p$ такий, що $u \equiv 1 \pmod{p}$ є m -тим степенем в \mathbb{Z}_p .
21. Показати, що рівняння $3X^3 + 4Y^3 + 5Z^3 = 0$ має розв'язок в цілих p -адичних числах, що не всі діляться на p , для $p = 2, 3, 5, 7$.
- Вказівка.* Використати лему Гензеля.
22. Нехай K поле і $K(X)$ полі рациональних функцій над K . Кожну ненульову рациональну функцію $a \in K(X)$ можна виразити вигляді $a = X^m \frac{f(X)}{g(X)}$, де $f(X), g(X) \in K[X]$, $f(0) \neq 0$, $g(0) \neq 0$. Нехай $\rho \in \mathbb{R}$, $0 < \rho < 1$. Довести, що функція

$$|a| = \rho^m, \quad |0| = 0$$

ї нормуванням поля K .

23. В умовах попередньої задачі довести, що поповнення поля $K(X)$ ізоморфне полю

$$K((X)) = \left\{ \sum_{i=m}^{\infty} \alpha_i X^i \mid m \in \mathbb{Z}, \alpha_i \in K \right\}$$

формальних степеневих рядів зі звичайними операціями над рядами.

24. Добути $\sqrt{1+X}$ в $K((X))$.