Г.М.КУДРЯВЦЕВА

ПОЛЯ.
ПРИКЛАДИ І ЗАДАЧІ

Київський Національний Університет імені Тараса
Шевченка

Г.М.КУДРЯВЦЕВА

ПОЛЯ.
ПРИКЛАДИ І ЗАДАЧІ

Навчальний посібник

Київ — 2005

Даний посібник укладено на основі практичних занять, які автор веде на механіко–математичному факультеті Київського національного університету імені Тараса Шевченка. Може бути використаний усіма, хто вивчає теорію полів, зокрема студентами математичних спеціальностей університетів.

Укладач: Г.М.Кудрявцева, канд. фіз.-мат. наук

Рецензенти: В.М.Бондаренко, д-р фіз.-мат. наук
В.В.Плахотник, канд. фіз.-мат. наук, доцент

Затверджено до друку Вченою Радою
механіко–математичного факультету
Київського національного університету
імені Тараса Шевченка
(*протокол №12 від 30 червня 2005 року*)

Зміст

Передмова

Даний посібник укладено на основі матеріалів практичних занять з нормативного курсу алгебри і теорії чисел, які автор веде на механіко–математичному факультеті Київського національного університету імені Тараса Шевченка. В цьому курсі основи теорії полів розглядають, як правило, протягом другої половини четвертого семестру. Посібником охоплюється весь матеріал з теорії полів (включаючи теорію Галуа), який входить до навчальної програми курсу алгебри і теорії чисел. Для найкращого оволодіння матеріалом посібника необхідним є знайомство з основами теорії груп, кілець, елементарної теорії чисел, математичного аналізу та теоретико–множинною технікою.

Розділи посібника складаються з трьох частин. На початку кожного з них наводяться необхідні теоретичні відомості. Далі розглядаються приклади розв'язування типових задач, причому деякі з них використовуються при розв'язуванні інших задач. Третю частину кожного розділу складають задачі для самостійного розв'язування, що дозволяє розглядати цей посібник і як задачник.

Кожен розділ може бути основою одного або двох практичних занять. Для розгляду на такому занятті рекомендується використовувати як приклади, наведені в посібнику, так і задачі для самостійного розв'язування. Для домашнього завдання задачі слід підбирати саме з третьої частини кожного розділу.

В кінці наводиться список рекомендованої літератури. Він містить зокрема збірники задач, а також посібники, за якими можна вивчати як основи теорії полів, так і її подальші розділи.

Позначення

$|A|$ — потужність множини A;

(a, b) —- найбільший спільний дільник цілих чисел a і b;

$\mathrm{Aut}K$ — група автоморфізмів поля K;

$\mathbb{C}$ — поле комплексних чисел;

C_n — циклічна група порядку n;

$\mathrm{char}F$ — характеристика поля F;

$\deg f(x)$ — степінь многочлена $f(x)$;

$\det A$ — визначник матриці A;

$(F, +, \cdot, 0, 1)$ — поле F з діями додавання $+$, множення $\cdot$ та нейтральними елементами 0 для додавання і 1 для множення;

$F(\alpha)$ — просте розширення поля F за допомогою елемента α, тобто найменше поле, яке містить F і α;

$F(\alpha_1, \ldots, \alpha_n)$ — розширення поля F за допомогою елементів $\alpha_1, \ldots, \alpha_n$, тобто найменше поле, яке містить F і $\alpha_1, \ldots, \alpha_n$;

$F[x_1, \ldots, x_n]$ — кільце многочленів від змінних $x_1, \ldots, x_n$ над полем F;

$F(x_1, \ldots, x_n)$ — поле раціональних функцій від змінних $x_1, \ldots, x_n$ над полем F;

$F[x]/(f(x))$ — факторкільце кільця многочленів $F[x]$ за головним ідеалом, породженим $f(x) \in F[x]$.

$[F : P]$ — степінь розширення $F \supset P$;

$m_\alpha(x)$ — мінімальний многочлен елемента α;

$M_n(F)$ — кільце матриць порядку n над полем F;

$\binom{n}{k}$ — біноміальний коефіцієнт, дорівнює кількості (невпорядкованих) n- елементних підмножин у k- елементній множині;

$\mathbb{Q}$ — поле раціональних чисел;

$\mathbb{Q}(\alpha)$ — див. $F(\alpha)$;

$\overline{z}$ — спряжене до комплексного числа z;

$|z|$ — модуль комплексного числа z;

$\mathbb{Z}$ — кільце цілих чисел;

$\mathbb{Z}_p$ — поле класів лишків за простим модулем p;

$\mathbb{Z}_n^*$ — мультиплікативна група оборотних класів лишків за модулем числа n.

1 Означення, характеристика та ізоморфізм полів

Означення 1. *Полем називається комутативне кільце з одиницею, в якому будь-який ненульовий елемент оборотний.*

Іншими словами, непорожня множина F із визначеними на ній двома бінарними операціями $+$ та $*$, що називаються відповідно *додаванням* та *множенням*, називається *полем*, якщо відносно операції додавання F є абелевою групою, нейтральний елемент якої називається *нульовим елементом* і як правило позначається символом 0, відносно операції множення $F \setminus \{0\}$ також є алебелевою групою. Крім того, додавання і множення пов'язані дистрибутивним законом: $a \cdot (b + c) = a \cdot b + a \cdot c$ для будь-яких $a, b, c \in F$. Зауважимо, що із означення одразу випливає, що будь-яке поле містить щонайменше два елементи: нульовий елемент і *одиничний елемент* — нейтральний елемент для множення, який як правило позначається символом 1. Прикладами числових полів є $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Q}(\sqrt{2})$, нечислових - поле $\mathbb{Z}_p$ класів лишків за простим модулем p.

Підмножина поля називається *підполем*, якщо вона замкнена відносно операцій додавання і множення, визначених на початковому полі, а також відносно взяття протилежного та оберненого елементів. Якщо для полів F, P виконується $F \supset P$, причому P є підполем F, то F називають розширенням поля P. Скрізь у посібнику позначення "$F \supset P$"означатиме, що поле F є розширенням поля P (причому символ " $\supset$ " позначає *нестроге* включення).

Нехай $F \supset P$ — розширення і $\alpha_1, \ldots, \alpha_n \in F$. Позначимо через M множину полів, які містять $\alpha_1, \ldots, \alpha_n$, а також одночасно є розширеннями P і підполями F. Множина M є непорожною, оскільки $F \in M$. Позначимо $P(\alpha_1, \ldots, \alpha_n) = \cap_{L \in M} L$. Очевидно, що $P(\alpha_1, \ldots, \alpha_n)$ є полем і, отже, є найменшим за включенням елементом множини M. Щойно визначене поле $P(\alpha_1, \ldots, \alpha_n)$ часто називають *полем, отриманим із P приєднанням елементів $\alpha_1, \ldots, \alpha_n$.*

Поле, яке не містить власних підполів, називається *простим.*

Теорема 1. *1. Кожне поле містить єдине просте підполе.*

2. Поля $\{\mathbb{Z}_p : p \text{ просте}\}$, $\mathbb{Q}$ і лише вони є простими.

Із сформульованої теореми випливає коректність наступного означення.

Означення 2. *Кажуть, що поле F має характеристику p (p — просте число), якщо F містить поле $\mathbb{Z}_p$, і характеристику 0, якщо F містить поле $\mathbb{Q}$.*

Характеристика поля F позначається $\mathrm{char}F$. Із означення характеристики випливає, що $\mathrm{char}F = p$ тоді й лише тоді, коли $\underbrace{1 + \ldots 1}_{p} = 0$, і $\mathrm{char}F = 0$ тоді й лише тоді, коли $\underbrace{1 + \ldots 1}_{n} \neq 0$ для будь-якого натурального числа n.

Нехай F, P — поля. *Гомоморфізмом* називається таке відображення $\varphi : F \to P$ що для будь-яких $a, b \in F$ виконуються рівності

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

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

Ізоморфізмом називається бієктивний гомоморфізм.

Означення 3. *Поля F та P називаються ізоморфними, якщо існує ізоморфізм $\varphi : F \to P$.*

Зауважимо, що при гомоморфізмі нульовий елемент переходить в нульовий елемент, а одиничний елемент — в одниничний. *Автоморфізмом* поля F називається будь-який ізоморфізм $\varphi : F \to F$.

Приклади розв'язування задач

Приклад 1. *Визначити, які з наступних множин є полями відносно дій додавання та множення дійсних чисел*

a) $A = \{a + b\sqrt{2} : \ a, b \in \mathbb{Q}\}$;

b) $B = \{a + b\sqrt[3]{2} : \ a, b \in \mathbb{Q}\}$;

c) $C = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} : \ a, b, c \in \mathbb{Q}\}$.

Оскільки A, B, C є підмножинами поля $\mathbb{R}$, то асоціативність та комутативність додавання і множення, а також дистрибутивний закон автоматично виконуються для елементів множин A, B, C. Кожна із заданих множин містить 0 та 1 - нейтральні елементи для додавання і множення в $\mathbb{R}$, отже 0 та 1 виконують ролі нейтральних елементів для додавання та множення для кожної із даних множин. Крім цього, очевидно, що

всі три множини замкнені відносно додавання та взяття протилежного елемента. Нам лишається дослідити A, B, C на замкненість відносно множення та на оборотність всіх ненульових елементів.

a) A замкнена відносно множення, оскільки для $(a+b\sqrt{2})$ і $(c+d\sqrt{2})$ із A маємо:

$$(a+b\sqrt{2})(c+d\sqrt{2}) = (ac+2bd)+(ad+bc)\sqrt{2} \in A.$$

Далі, візьмемо ненульвий елемент $(a+b\sqrt{2}) \in A$.

$$\frac{1}{a+b\sqrt{2}} = \frac{a-b\sqrt{2}}{a^2-2b^2} = \frac{a}{a^2-2b^2} - \frac{b}{a^2-2b^2}\sqrt{2}$$

(відзначимо, що $a^2-2b^2 \neq 0$ для $a, b \in \mathbb{Q}$, оскільки $\sqrt{2} \notin \mathbb{Q}$). Отже, $(a+b\sqrt{2})^{-1} = \frac{a}{a^2-2b^2} - \frac{b}{a^2-2b^2}\sqrt{2}$. Таким чином, кожен ненульовий елемент із A є оборотним, а отже, A є полем.

Покажемо, що $A = \mathbb{Q}(\sqrt{2})$, тобто, що A є найменшим полем, яке містить $\mathbb{Q}$ і $\sqrt{2}$. Справді, нехай деяке поле P містить $\mathbb{Q}$ і $\sqrt{2}$. Тоді зокрема, $1, \sqrt{2} \in P$, що тягне $a+b\sqrt{2} \in P$ для будь-яких раціональних a і b. Таким чином, $P \supset A$.

b) Намагаючись довести замкненість відносно множення аналогічно попередньому пункну візьмемо два довільних елементи $(a+b\sqrt[3]{2})$ і $(c+d\sqrt[3]{2})$ із A, перемножаючи які отримаємо:

$$(a+b\sqrt[3]{2})(c+d\sqrt[3]{2}) = ac+(bc+ad)\sqrt[3]{2}+bd\sqrt[3]{4}.$$

Доведемо, що $\sqrt[3]{4} \notin B$ (цього достатньо, щоб стверджувати, що B не замкнена відносно множення, позаяк $\sqrt[3]{4} = \sqrt[3]{2}\sqrt[3]{2}$). Від супротивного, припустимо, що $\sqrt[3]{4} = e+f\sqrt[3]{2}$ для деяких $e, f \in \mathbb{Q}$. Тоді $\sqrt[3]{2}$ є коренем многочлена $x^2-fx-e \in \mathbb{Q}[x]$. Але, з іншого боку, $\sqrt[3]{2}$ є коренем незвідного над $\mathbb{Q}$ (в силу ознаки Айзенштайна) многочлена x^3-2. Поділивши x^3-2 на x^2-fx-e з остачею, отримаємо

$$x^3-2 = f(x)(x^2-fx-e)+r(x), \tag{1}$$

де остача $r(x) \in \mathbb{Q}[x]$ — ненульовий многочлен степеня не вище 1. Підставляючи в (1) $x = \sqrt[3]{2}$, отримаємо $r(\sqrt[3]{2}) = 0$, що неможливо: якщо $\deg r(x) = 0$, то $r(x)$ взагалі не має коренів, якщо ж $\deg r(x) = 1$, то $r(x)$ має раціональний корінь. Отримана суперечність означає, що множина B не замкнена відносно множення, тому не є полем.

c) Так само, як у пункті а), перевіряється, що множина C є замкненою відносно множення. Лишається перевірити, чи кожен ненульовий елемент із C є оборотним. Для цього розглянемо довільний ненульовий елемент $\alpha = a+b\sqrt[3]{2}+c\sqrt[3]{4} \in C$. Покладемо $f(x) = cx^2+bx+a$. Оскільки x^3-2 є незвідним над $\mathbb{Q}$, то НСД$(x^3-2, f(x)) = 1$. Тому знайдуться $p(x), q(x) \in \mathbb{Q}[x]$, такі, що

$$1 = p(x)(x^3-2) + q(x)(cx^2+bx+a).$$

Звідси при $x = \sqrt[3]{2}$ отримаємо $1 = q(\sqrt[3]{2}) \cdot \alpha$. Таким чином, $\alpha^{-1} = q(\sqrt[3]{2})$. Оскільки, очевидно, $q(\sqrt[3]{2}) \in C$, то α є оборотним в C, звідки випливає, що C є полем. Так само, як і у пункті а), встановлюється, що $C = \mathbb{Q}(\sqrt[3]{2})$.

Приклад 2. *Перевірити, чи утворює поле відносно звичайних матричних операцій множина матриць вигляду* $M_p^n = \left\{ \begin{pmatrix} x & y \\ ny & x \end{pmatrix} : x, y \in \mathbb{Z}_p \right\}$, *де* n *— фіксований елемент із* $\mathbb{Z}_p$, *для* $p = 2, 3, 5, 7$.

Оскільки $M_n^p \subset M_2(\mathbb{Z}_p)$, і $M_2(\mathbb{Z}_p)$ є кільцем з одиницею, то M_n^p буде полем в тому й лише тому разі, коли M_n^p замкнена відносно додавання матриць і взяття протилежної матриці, замкнена відносно множення, крім того, довільні дві матриці із M_n^p комутують і кожна ненульова матриця оборотна.

Замкненість відносно додавання і взяття протилежної матриці випливають безпосередньо із визначення M_n^p. Нехай $A = \begin{pmatrix} x & y \\ ny & x \end{pmatrix}$, $B = \begin{pmatrix} u & v \\ nv & u \end{pmatrix} \in M_n^p$. Тоді

$$A \cdot B = B \cdot A = \begin{pmatrix} xu+nyv & xv+yu \\ nvx+nuy & nvy+xu \end{pmatrix} \in M_n^p$$

.

Отже, M_n^p замкнена відносно множення матриць і будь-які дві матриці із M_n^p перестановочні.

Припустимо, що $A = \begin{pmatrix} x & y \\ ny & x \end{pmatrix} \in M_n^p$ — оборотна в $M_n(\mathbb{Z}_p)$. Тоді $d = \det A = x^2 - ny^2 \neq 0$ і $A^{-1} = \begin{pmatrix} xd^{-1} & -yd^{-1} \\ -nyd^{-1} & xd^{-1} \end{pmatrix} \in M_n^p$.

Лишилось дослідити, при яких цілих n кожна ненульова матриця із M_n^p є оборотною, тобто при яких цілих n нерівність $x^2 - ny^2 \neq 0$ виконується для будь-яких одночасно не рівних нулю $x, y \in \mathbb{Z}_p$.

Нехай $y = 0$. Тоді $d = x^2 \neq 0$, оскільки $x \neq 0$ і в полі $\mathbb{Z}_p$ відсутні дільники нуля. Нехай тепер $y \neq 0$. Виконання нерівності $x^2 - ny^2 \neq 0$ для всіх $x \in \mathbb{Z}_p$, $y \in \mathbb{Z}_p \setminus \{0\}$ еквівалентне виконанню нерівності $\left(\frac{x}{y}\right)^2 - n \neq 0$ для всіх $x \in \mathbb{Z}_p$, $y \in \mathbb{Z}_p \setminus \{0\}$, що в свою чергу рівносильно виконанню нерівності $z^2 - n \neq 0$ для всіх $z \in \mathbb{Z}_p$ (в силу того, що $\left\{\frac{x}{y} : x \in \mathbb{Z}_p, y \in \mathbb{Z}_p \setminus \{0\}\right\} = \mathbb{Z}_p$).

Отже, для знаходження потрібних значень n потрібно виписати квадрати всіх елементів із $\mathbb{Z}_p$ для кожного конкрентного p і взяті ті n, які серед виписаних квадратів не зустрілися.

1) $p = 2$. $0^2 = 0, 1^2 = 1$. Всі елементи із $\mathbb{Z}_2$ є квадратами певних елементів із $\mathbb{Z}_2$. Отже, при жодному $n \in Z_2$ M_n^2 не є полем.

2) $p = 3$. $0^2 = 0$, $1^2 = 1$, $2^2 = 1$. В списку квадратів не зустрівся лише елемент 2, тому M_n^3 є полем тоді й лише тоді, коли $n = 2$.

3) $p = 5$. $0^2 = 0$, $1^2 = 1$, $2^2 = 4$, $3^2 = 4$, $4^2 = 1$. В списку квадратів не зустрілися елементи $2, 3$, тому M_n^5 є полем тоді й лише тоді, коли $n = 2, 3$.

4) $p = 7$. $0^2 = 0$, $1^2 = 1$, $2^2 = 4$, $3^2 = 2$, $4^2 = 2$, $5^2 = 4$, $6^2 = 1$. В списку квадратів не зустрілися елементи $3, 5, 6$, тому M_n^7 є полем тоді й лише тоді, коли $n = 3, 5, 6$.

Зауважимо, що із розв'язання задачі випливає, що M_n^p є полем для тих і лише тих n, для яких порівняння $x^2 \equiv n (\mathrm{mod}\, p)$ не має розв'язків. Такі n називаються *квадратичними нелишками за модулем* p.

Приклад 3. *Нехай K — поле характеристики p, і для деяких $a, b \in K$ виконується рівність $a^p = b^p$. Довести, що $a = b$.*

За формулою бінома Ньютона маємо

$$(a - b)^p = \sum_{k=0}^{p} \binom{p}{k} a^k b^{p-k} (-1)^{p-k} \tag{2}$$

Покажемо, що $\binom{p}{k}$ ділиться на p при $1 \leq k \leq p - 1$. Дійсно, $\binom{p}{k} = \frac{p!}{k!(p-k)!}$ — ціле число. Знаменник на p не ділиться, а чисельник ділиться, тому при скороченні дробу скорочення на p не відбудеться, і ціле $\binom{p}{k}$ ділиться на p. Звідси, враховуючи, що $p = \underbrace{1 + \cdots + 1}_{p} = 0$ у полі

характеристики p, випливає, що рівність (2) набуде вигляду $(a-b)^p = b^p(-1)^p + a^p$. Якщо p непарне, то у правій частині матимемо 0, а тому $(a-b)^p = 0$, звідки, враховуючи відсутність дільників нуля в K, $a = b$. Лишилося розглянути випадок $p = 2$. Тоді $0 = a^2 - b^2 = (a-b)(a+b)$. Знову беручи до уваги відсутність в K дільників нуля, отримаємо $a = b$ або $a = -b$. Але у полі характеристики 2 виконується $1 + 1 = 0$, звідки $1 = -1$, а тому $-b = b$. Отже, і в цьому випадку отримуємо $a = b$.

Приклад 4. *Довести, що*

a) *поля* $\mathbb{Q}(\sqrt{3})$ *і* $\mathbb{Q}(\sqrt{6})$ *не ізоморфні;*

b) *поля* $\mathbb{Q}(\sqrt{3})$ *і* $\mathbb{Q}(\sqrt{12})$ *ізоморфні.*

a) Припустимо, що $\varphi : \mathbb{Q}(\sqrt{3}) \to \mathbb{Q}(\sqrt{6})$ — ізоморфізм. Оскільки $\varphi(1) = 1$, то $\varphi(3) = \varphi(1+1+1) = \varphi(1) + \varphi(1) + \varphi(1) = 1 + 1 + 1 = 3$. Нехай $\varphi(\sqrt{3}) = a + b\sqrt{6}$. Тоді

$$\varphi(3) = \varphi((\sqrt{3})^2) = (\varphi(\sqrt{3}))^2 = (a + b\sqrt{6})^2 = a^2 + 6b^2 + 2ab\sqrt{6},$$

звідки $\begin{cases} a^2 + 6b^2 = 3 \\ 2ab = 0 \end{cases}$. Із другої рівності випливає, що хоча б одне із чисел a, b повинно дорівнювати нулю. Але тоді, очевидно, що перше рівняння не має раціональних розв'язків. Таким чином неможливо знайти раціональні a, b такі, що $\varphi(\sqrt{3}) = a + b\sqrt{6}$. Отже, ізоморфізму між $\mathbb{Q}(\sqrt{3})$ і $\mathbb{Q}(\sqrt{6})$ не існує.

b) Оскільки $\sqrt{12} = 2\sqrt{3}$, то $\mathbb{Q}(\sqrt{12}) \subseteq \mathbb{Q}(\sqrt{3})$. Аналогічно, $\sqrt{3} = \frac{1}{2}\sqrt{12}$ тягне $\mathbb{Q}(\sqrt{3}) \subseteq \mathbb{Q}(\sqrt{12})$. Отже, $\mathbb{Q}(\sqrt{12}) = \mathbb{Q}(\sqrt{3})$, а тому тотожне відображення $a + b\sqrt{3} \mapsto a + \frac{b}{2}\sqrt{12}$ є ізоморфізмом $\mathbb{Q}(\sqrt{3}) \to \mathbb{Q}(\sqrt{12})$.

Приклад 5. *Довести, що поля* $\mathbb{Q}$ *і* $\mathbb{R}$ *не мають автоморфізмів, відмінних від тотожних.*

Нехай $\varphi : \mathbb{Q} \to \mathbb{Q}$ — автоморфізм. Оскільки $\varphi(1) = 1$, то для будь-якого цілого n повинно бути $\varphi(n) = n$, звідки для будь-яких цілих m, n, $n \neq 0$, повинно бути $\varphi(\frac{m}{n}) = \frac{\varphi(m)}{\varphi(n)} = \frac{m}{n}$. Отже, φ — тотожний автоморфізм.

Нехай тепер $\varphi : \mathbb{R} \to \mathbb{R}$ — автоморфізм. Міркуючи, як і у випадку поля $\mathbb{Q}$, приходимо до висновку, що $\varphi(a) = a$ для будь-якого раціонального a. Припустимо, що $a \in \mathbb{R}$ — додатне. Тоді $\varphi(a) = \varphi((\sqrt{a})^2) = (\varphi(\sqrt{a}))^2$, звідки $\varphi(a)$ — квадрат дійсного числа, а тому $\varphi(a)$ є додатним. Якщо

тепер $a > b$, то $a - b > 0$, звідки $\varphi(a) - \varphi(b) = \varphi(a - b) > 0$. Таким чином, $a > b$ тягне $\varphi(a) > \varphi(b)$, тобто φ — монотонно зростає на $\mathbb{R}$.

Припустимо, що $\varphi(a) \neq a$ для $a \in \mathbb{R}$. Можливі 2 випадки: $\varphi(a) > a$ або $\varphi(a) < a$. Нехай спочатку, $\varphi(a) > a$. Візьмемо $\alpha \in \mathbb{Q}$ таке, що $a < \alpha < \varphi(a)$ (таке α існує, оскільки a можна як завгодно точно наблизити раціональним числом). Звідси, враховуючи монотонність φ, отримуємо $\varphi(a) < \varphi(\alpha) = \alpha < \varphi(a)$. Супепечність. Міркуючи аналогічно, приходимо до суперечності і у випадку $\varphi(a) < a$. Таким чином, $\varphi(a) = a$, $a \in \mathbb{R}$, тобто φ є тотожним автоморфізмом.

Задачі

1.1 Які з наступних числових множин є полями відносно звичайних дій додавання і множення:

a) $\mathbb{Z}$;

b) $\{0, 1\}$;

c) $\{a + b\sqrt[3]{3} : a, b \in \mathbb{Q}\}$;

d) $\{a + b\sqrt[3]{3} + c\sqrt[3]{9} : a, b, c \in \mathbb{Q}\}$;

e) $\{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} : a, b, c, d \in \mathbb{Q}\}$;

f) $\{z \in \mathbb{C} : |z| \leq 1\}$?

1.2 Довести, що множина $M_n = \left\{ \begin{pmatrix} x & y \\ ny & x \end{pmatrix} : x, y \in \mathbb{Q} \right\}$, $n \in \mathbb{Z}$, утворює поле відносно звичайних матричних операцій тоді й лише тоді, коли n не є квадратом цілого числа. Довести, що в останньому випадку, поле M_n ізоморфне полю $\mathbb{Q}(\sqrt{n})$.

1.3 Нехай $(F, +, \cdot, 0, 1)$ — поле. Чи буде полем множина $F^2 = \{(a, b) : a, b \in F\}$ з діями $(a, b) \oplus (c, d) = (a + c, b + d)$, $(a, b) * (c, d) = (a \cdot c, b \cdot d)$, нульовим елементом $(0, 0)$ та одиничним $(1, 1)$?

1.4 Знайти всі підполя поля $\mathbb{Q}(\sqrt{a})$, $a \in \mathbb{Q}$.

1.5 Довести, що поля $\mathbb{Q}(\sqrt{a})$ і $\mathbb{Q}(\sqrt{b})$, $b \neq 0$, ізоморфні тоді й лише тоді, коли $\frac{a}{b}$ є квадратом раціонального числа.

1.6 Знайти характеристику поля, в якому $(1 + 1 + 1 + 1 + 1)^2 = (1 + 1)^5$.

1.7 Довести, що характеристика скінченного поля відмінна від нуля.

1.8 Довести, що потужність скінченного поля є степенем простого числа — характеристики цього поля.

1.9 Нехай $L \supset K$, де L — скінченне поле характеристики p. Довести, що $\mathrm{char}K = p$.

1.10 Навести приклад поля потужності

a) 4; b) 8; c) 9.

1.11 Нехай P — поле характеристики p. Довести, що для довільних $a, b \in P$ і $n \in \mathbb{N}$ справедливі рівності:

a) $(a+b)^{p^n} = a^{p^n} + b^{p^n}$; b) $(a-b)^{p^n} = a^{p^n} - b^{p^n}$.

1.12 Довести, що у полі потужності n виконується тотожність $x^n = x$.

1.13 Довести, що для комплексного числа z, яке не є дійсним, поле $\mathbb{R}(z)$ збігається з $\mathbb{C}$.

1.14 У полі $\mathbb{Q}(\sqrt{2})$ розв'язати наступні рівняння:

a) $x^2 + (4 - 2\sqrt{2})x + 3 - 2\sqrt{2} = 0$;

b) $x^2 - x - 3 = 0$;

c) $x^2 + x - 7 + 6\sqrt{2} = 0$.

1.15 У кожному з полів $\mathbb{Z}_3$ та $\mathbb{Z}_7$ розв'язати систему рівнянь

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

1.16 Довести, що факторкільце $\mathbb{Z}_2[x]/(x^3 + x + 1)$ є полем. Позначимо через $\overline{f(x)}$ клас еквівалентності за ідеалом $(x^3 + x + 1)$, що містить $f(x)$. У заданому полі розв'язати рівняння:

a) $t^2 + \overline{x^2 + x + 1} = 0$; b) $t^2 + t + \overline{x^2 + 1} = 0$.

1.17 Нехай $\varphi : P \to F$ — гомоморфізм полів, причому $\varphi(a) \neq 0$ для деякого ненульового $a \in P$. Довести, що φ — ін'єктивний.

1.18 Довести, що факторкількільце $\mathbb{Z}_3[x]/(x^3+2x+2)$ є полем та знайдіть усі автоморфізми цього поля.

1.19 Знайти всі автоморфізми поля $\mathbb{C}$, при яких кожне дійсне число переходить в себе.

1.20 Довести, що для будь-якого автоморфізму φ поля F множина елементів, нерухомих відносно φ, є підполем.

1.21 Довести, що у полі $\mathbb{Z}_p$ виконуються рівності:

a) $\sum_{k=1}^{p-1} k^{-1} = 0$, $p > 2$;

b) $\sum_{k=1}^{\frac{p-1}{2}} k^{-2} = 0$, $p > 3$.

2 Розширення полів

Нехай $P \supset F$ — розширення полів.

Означення 4. Степенем розширення $P \supset F$ *називається розмірність* P *як векторного простору над полем* F, базисом P *над* F *називають базис векторного простору* P *над полем* F.

Степінь розширення $P \supset F$ позначається $[P : F]$.

Означення 5. *Розширення* $P \supset F$ *називається* скінченним, *якщо* $[P : F] < \infty$, *і* нескінченним *в противному разі.*

Для обчислення степенів розширень часто буває корисною наступна теорема про вежу розширень.

Теорема 2. *Нехай* P, F, K *— поля, причому* $P \supset F \supset K$.

1) $[P : K] < \infty \Leftrightarrow [P : F] < \infty$ *і* $[F : K] < \infty$.

2) Якщо $[P : K] < \infty$, *то* $[P : K] = [P : F] \cdot [F : K]$.

3) Нехай $a_1, \ldots, a_m$ *— базис* P *над* F, $b_1, \ldots, b_n$ *— базис* F *над* K. *Тоді* $\{a_i b_j\}_{1 \le i \le m, 1 \le j \le n}$ *— базис* P *над* K.

Означення 6. *Елемент* $\alpha \in P$ *називається* алгебраїчним *над* F, *якщо знайдеться многочлен* $f(x) \in F[x]$, *такий, що* $f(\alpha) = 0$ *(такі многочлени називаються анулюючими для* α*). Елемент* $\alpha \in P$, *який не є алгебраїчним над* F, *називається* трансцендентним *над* F.

Мінімальним многочленом алгебраїчного над F елемента α називається унітарний анулюючий многочлен найменшого степеня. Мінімальний многочлен елемента α часто позначається $m_\alpha(x)$. *Степенем* α *над* F називається степінь многочлена $m_\alpha(x)$.

Означення 7. *Розширення* $P \supset F$ *називається алгебраїчним, якщо будь-який елемент* $\alpha \in P$ *є алгебраїчним над* F. *Якщо ж існує елемент* $\alpha \in P$, *трансцендентний над* F, *то розширення* $P \supset F$ *називається трансцендентним.*

Теорема 3. *Довільне скінченне розширення є алгебраїчним.*

Алгебраїчні і трансцендентні елементи розширення $\mathbb{C} \supset \mathbb{Q}$ називаються відповідно алгебраїчними і трансцендентними числами. Прикладами алгебраїчних і трансцендентних чисел є відповідно $\sqrt[5]{3}$, $i + \sqrt{2}$ і e, π, $\sqrt{2}^{\sqrt{3}}$. Множина алгебраїних чисел утворює поле, яке має зліченну потужність. Із цього факту, зокрема, випливає, що трансцендентних чисел континуум багато.

Алгебраїчне число u називається *цілим алгебраїчним*, якщо існує унітарний многочлен з цілими коефіцієнтами, коренем якого є u. Якщо u — ціле алгебраїчне число, то мінімальний многочлен елемента u має цілі коефіцієнти.

Означення 8. *Якщо $P = F(\alpha)$ для деякого $\alpha \in P$, то поле P називається* простим розширенням поля F за допомогою елемента $\alpha \in P$. *Просте розширення $F(\alpha) \supset F$ називається* простим алгебраїчним розширенням *або* простим трансцендентним розширенням *в залежності від того, є α алгебраїчним чи трансцендентним над F елементом.*

Наступні дві теореми відомі відповідно як теореми про будову простих алгебраїчних та простих трансцендентних розширень.

Теорема 4. *Нехай $F(\alpha) \supset F$ — просте алгебраїчне розширення і $m_\alpha(x) \in F[x]$ — мінімальний многочлен елемента α. Позначимо $n = \deg m_\alpha(x)$. Тоді*

1) $[F(\alpha) : F] = n$, зокрема $F(\alpha) \supset F$ — скінченне розширення.

2) $F(\alpha) \simeq F[x]/(m_\alpha(x))$, зокрема $F(\alpha) = \{a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} : a_i \in F,\ 0 \le i \le n-1\}$.

3) Базисом $F(\alpha)$ над F є $\{1, \alpha, \ldots, \alpha^{n-1}\}$.

Теорема 5. *Нехай $F(\alpha) \supset F$ — просте трансцендентне розширення розширення. Тоді*

1) $F(\alpha) \supset F$ — нескінченне розширення.

2) $F(\alpha) = \{\frac{f(\alpha)}{g(\alpha)} : f, g \in F[x], g \neq 0\}$;

3) $F(\alpha) \simeq F(x)$.

Приклади розв'язування задач

Приклад 6. *Довести, що* $[F(\alpha) : F] = 1 \Leftrightarrow F = F(\alpha)$.

Враховуючи очевидне включення $F(\alpha) \supset F$, достатньо довести лише зворотне включення $F(\alpha) \subset F$. Оскільки $[F(\alpha) : F] = \deg m_\alpha(x)$, то рівність $[F(\alpha) : F] = 1$ еквівалентна існуваню многочлена $ax + b \in F[x]$ $(a \neq 0)$, такого, що $a\alpha + b = 0$. Остання рівність еквівалентна тому, що $\alpha = -\frac{b}{a} \in F$, звідки $F(\alpha) \subset F$.

Приклад 7. *Довести, що розширення* $\mathbb{Q}(\alpha)$ *поля* $\mathbb{Q}$ *є алгебраїчним, знайти степінь розширення* $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ *та мінімальний многочлен* $m_\alpha(x)$ *елемента* α *для* $\alpha = 1 + \sqrt{2} + \sqrt{3}$.

Для того, щоб пересвідчитись, що α — алгебраїчний над $\mathbb{Q}$, побудуємо многочлен $f(x) \in \mathbb{Q}[x]$, який анулює α. Після піднесення рівності $\alpha - 1 = \sqrt{2} + \sqrt{3}$ до квадрату, отримаємо $(\alpha - 1)^2 - 5 = 2\sqrt{6}$, звідки після повторного піднесення до квадрату $((\alpha - 1)^2 - 5)^2 = 24$. Таким чином, $f(\alpha) = 0$ для $f(x) = ((x - 1)^2 - 5)^2 - 24 = x^4 - 4x^3 - 4x^2 + 16x - 8$. Далі можна міркувати по-різному.

Перший спосіб. Покажемо, що побудований многочлен $f(x)$ є незвідним над $\mathbb{Q}$. Стандартний спосіб доведення незвідності многочлена над $\mathbb{Q}$ — застосування ознаки Айзенштайна — для многочлена $f(x)$ не працює.

Незвідність многочлена $f(x)$ встановимо в наступний спосіб. Помічаємо спочатку, що

$$f(x) = (x - 1 + \sqrt{2} + \sqrt{3}) \cdot (x - 1 - \sqrt{2} + \sqrt{3}) \cdot (x - 1 + \sqrt{2} - \sqrt{3}) \cdot (x - 1 - \sqrt{2} - \sqrt{3}). \quad (3)$$

Цей розклад і однозначність розкладу на незвідні множинки над $\mathbb{R}$ тягнуть відсутність у $f(x)$ раціональних коренів. Якщо б попри відсутності раціональних коренів $f(x)$ був звідним над $\mathbb{Q}$, то він би мав дільник степеня 2 над $\mathbb{Q}$. Внаслідок однозначності розкладу на незвідні множники цей дільник був би добутком якихось двох із вказаних в (3) лінійних множників. Перебір шести випадків показує, що жоден із таких многочленів не є многочленом над $\mathbb{Q}$.

Таким чином, $f(x)$ є незвідним над $\mathbb{Q}$, а тому $m_\alpha(x) = f(x)$. Оскільки $[\mathbb{Q}(\alpha) : \mathbb{Q}] = \deg m_\alpha(x)$, то $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$.

Другий спосіб. Застосуємо теорему про вежу розширень для доведення рівності $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$. Спочатку покажемо, що

$$\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(1+\sqrt{2}+\sqrt{3}). \tag{4}$$

Перше включення очевидне. Покладемо $a = 1+\sqrt{2}+\sqrt{3}$. Для того, щоб показати, що $\mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(a)$, достатньо встановити, що $\sqrt{2} \in \mathbb{Q}(a)$. Оскільки

$$\sqrt{6} = \frac{(a-1)^2 - 5}{2} \in \mathbb{Q}(a),$$

то $b = \sqrt{6}(a-1) = 2\sqrt{3} + 3\sqrt{2} \in \mathbb{Q}(a)$, звідки $\sqrt{2} = b - 2(a-1) \in \mathbb{Q}(a)$. Отже, $\sqrt{2} \in \mathbb{Q}(a)$.

Зауважимо, що обидва включення у вежі (4) строгі, оскільки $\sqrt{2} \notin \mathbb{Q}$, $\sqrt{3}+\sqrt{2} \notin \mathbb{Q}(\sqrt{2})$. Тому, враховуючи приклад 6, $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] \geq 2$ і $[\mathbb{Q}(1+\sqrt{2}+\sqrt{3}) : \mathbb{Q}(\sqrt{2})] \geq 2$. Отже, за теоремою про вежу розширень

$$[\mathbb{Q}(1+\sqrt{2}+\sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(1+\sqrt{2}+\sqrt{3}) : \mathbb{Q}(\sqrt{2})] \cdot [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] \geq 2 \cdot 2 = 4.$$

Але з іншого боку $[\mathbb{Q}(1+\sqrt{2}+\sqrt{3}) : \mathbb{Q}] = \deg(m_\alpha(x)) \leq \deg(f(x)) = 4$. Таким чином, $[\mathbb{Q}(1+\sqrt{2}+\sqrt{3}) : \mathbb{Q}] = 4$, звідки $m_\alpha(x) = f(x)$.

Зауваження. Те, що число $1+\sqrt{2}+\sqrt{3}$ є алгебраїчним випливає ще й з того факту, що множина алгебраїчних чисел є полем і алгебраїчності чисел $\sqrt{2}$ та $\sqrt{3}$.

Приклад 8. *Нехай u — корінь многочлена $x^3 + 3x^2 - 9x + 6 \in \mathbb{Q}[x]$. Подати елемент $\frac{u^2}{u^2+2u-11}$ у вигляді лінійної комбінації $1, u, u^2$.*

На першому етапі позбудемось від многочлена від u в знаменнику. Многочлен $f(x) = x^3 + 3x^2 - 9x + 6$ є незвідним за ознакою Айзенштайна для $p = 3$. Тому $f(x)$ і $g(x) = x^2 + 2x - 11$ взаємно прості. За допомогою алгоритму Евкліда знайдемо $s(x), t(x) \in \mathbb{Q}[x]$, такі, що $f(x)s(x) + g(x)t(x) = 1$:

$$f(x) = g(x)(x+1) + 17, \text{ звідки } 1 = \frac{1}{17}f(x) - \frac{x+1}{17}g(x).$$

Підставивши в останню рівність $x = u$ і врахувавши $f(u) = 0$, отримуємо

$$1 = -\frac{u+1}{17}g(u), \text{ звідки } \frac{1}{g(u)} = -\frac{u+1}{17}.$$

Таким чином,

$$\frac{u^2}{u^2+2u-11} = -\frac{1}{17}u^2(u+1) = -\frac{1}{17}(u^3+u^2).$$

На другому етапі поділимо $x^3 + x^2$ на $f(x)$ з остачею:

$$x^3 + x^2 = (x^3 + 3x^2 - 9x + 6) + (-2x^2 + 9x - 6).$$

Підставивши в останню рівність $x = u$ і врахувавши $f(u) = 0$, отримуємо

$$u^3 + u^2 = -2u^2 + 9u - 6. \text{ Отже, } \frac{u^2}{u^2 + 2u - 11} = -2u^2 + 9u - 6.$$

Приклад 9. *Довести, що для раціонального q числа* $\sin(q\pi)$ *і* $\cos(q\pi)$ *алгебраїчні.*

Розглянемо комплексне число $z = \cos(q\pi) + i\sin(q\pi)$. Виберемо таке $n \in \mathbb{N}$, що $nq \in 2\mathbb{Z}$. Тоді, використовуючи формулу Муавра і періодичність з періодом 2π функцій sin і cos, отримуємо:

$$z^n = \cos(nq\pi) + i\sin(nq\pi) = \cos 0 + i\sin 0 = 1,$$

звідки, зокрема, випливає, що z є алгебраїчним. Оскільки $\overline{z}^n = \overline{z^n} = 1$, то $\overline{z} = \cos(q\pi) - i\sin(q\pi)$ також є алгебраїчним. Звідси і із того, що множина алгебраїчних чисел є полем, випливає, що

$$\cos(q\pi) = \frac{1}{2}(z + \overline{z}) \text{ і } \cos(q\pi) = \frac{1}{2i}(z - \overline{z})$$

є алгебраїчними.

Відзначимо, що обчислюючи z^n за формулою бінома Ньютона та прирівнюючи отриману дійсну частину до одиниці, неважко отримати анулюючий многочлен для $\cos(q\pi)$. Справді,

$$z^n = (\cos(q\pi) + i\sin(q\pi))^n = \sum_{k=0}^{n} \binom{n}{k} i^k (\sin(q\pi))^k (\cos(q\pi))^{n-k} =$$
$$\sum_{k=0}^{[n/2]} \binom{n}{2k} (-1)^k (\sin(q\pi))^{2k} (\cos(q\pi))^{n-2k} +$$
$$i \cdot \sum_{k=0}^{[(n-1)/2]} \binom{n}{2k+1} (-1)^k (\sin(q\pi))^{2k+1} (\cos(q\pi))^{n-(2k+1)}.$$

Покладемо $y = \cos(q\pi)$. Тоді $\sin^2(q\pi) = 1 - y^2$. Тому $\cos(q\pi)$ є коренем многочлена

$$f(x) = \sum_{k=0}^{[n/2]} \binom{n}{2k} (-1)^k (1-x^2)^k (x)^{n-2k} - 1.$$

Приклад 10. *Знайти базис та вказати степінь над* $\mathbb{Q}$ *поля* $\mathbb{Q}(\varepsilon, \sqrt[3]{3})$, $\varepsilon = \cos\frac{\pi}{3} + i\sin\frac{\pi}{3}$.

Очевидно, $\mathbb{Q}(\varepsilon, \sqrt[3]{3}) \supset \mathbb{Q}(\sqrt[3]{3}) \supset \mathbb{Q}$. Знайдемо степінь та базис кожного із розширень $\mathbb{Q}(\varepsilon, \sqrt[3]{3}) \supset \mathbb{Q}(\sqrt[3]{3})$ і $\mathbb{Q}(\sqrt[3]{3}) \supset \mathbb{Q}$.

Зрозуміло, що $\mathbb{Q}(\varepsilon, \sqrt[3]{3}) \neq \mathbb{Q}(\sqrt[3]{3})$. Тому, беручи до уваги, що ε є коренем многочлена $x^2 - x + 1 \in \mathbb{Q}(\sqrt[3]{3})[x]$, маємо $[\mathbb{Q}(\varepsilon, \sqrt[3]{3}) : \mathbb{Q}(\sqrt[3]{3})] = 2$. За теоремою 4 елементи $1, \varepsilon$ утворюють базис $\mathbb{Q}(\varepsilon, \sqrt[3]{3})$ над $\mathbb{Q}(\sqrt[3]{3})$. Далі, $[\mathbb{Q}(\sqrt[3]{3}) : \mathbb{Q}] = 3$, оскільки $\sqrt[3]{3}$ є коренем незвідного (за ознакою Айзенштайна) над $\mathbb{Q}$ многочлена $x^3 - 3$. За теоремою 4 елементи $1, \sqrt[3]{3}, \sqrt[3]{9}$ утворюють базис $\mathbb{Q}(\sqrt[3]{3})$ над $\mathbb{Q}$.

За теоремою про вежу розширень (теорема 2)

$$[\mathbb{Q}(\varepsilon, \sqrt[3]{3}) : \mathbb{Q}] = [\mathbb{Q}(\varepsilon, \sqrt[3]{3}) : \mathbb{Q}(\sqrt[3]{3})] \cdot [\mathbb{Q}(\sqrt[3]{3}) : \mathbb{Q}] = 2 \cdot 3 = 6.$$

Знаючи базиси розширень на кожній з ланок вежі, за теоремою 2 знаходимо базис $\mathbb{Q}(\varepsilon, \sqrt[3]{3})$ над $\mathbb{Q}$: це $1, \sqrt[3]{3}, \sqrt[3]{9}, \varepsilon, \varepsilon\sqrt[3]{3}, \varepsilon\sqrt[3]{9}$.

Приклад 11. *Нехай* $[F : P]$ *— просте число. Довести, що для будь-якого* $a \in F \setminus P$ *виконується* $F = P(a)$.

Нехай $a \in F \setminus P$. Оскільки $F \supset P(a) \supset P$, то $p = [F : P] = [F : P(a)] \cdot [P(a) : P]$ за теоремою 2. Те, що $a \in F \setminus P$, тягне $[P(a) : P] > 1$ (див. приклад 6). Але дільник простого числа p, відмінний від 1, мусить збігатися з p, тому $[P(a) : P] = p$. За означенням степеня розширення F і $P(a)$ — p-вимірні векторні простори над полем P, причому $F \supset P(a)$. Але тоді довільний базис $P(a)$ над P також слугуватиме базисом F над P. Звідси випливає, що $F = P(a)$.

Приклад 12. *Для довільного поля* K *розглянемо поле раціональних функцій* $K(x, y)$ *і його підполе* $L = K(x^2 + x + 1)$. *Визначити підполе* $M \subset K(x, y)$ *елементів, алгебраїчних над* L. *Знайти* $[M : L]$.

Елемент x є алгебраїчним над L степеня не вище 2, оскільки він анулюється многочленом $t^2 + t - (x^2 + x) \in L[t]$. Оскільки крім цього $x \notin L$,

то $[L(x) : L] = 2$. Позаяк $L(x) \supset L$ — скінченне розширення, то воно алгебраїчне, звідки $L(x) \subset M$. З іншого боку, жодна раціональна фукнкція, істотно залежна від y, не може бути елементом, алгебраїчним над L, оскільки інакше б y був би коренем певного многочлена з коефіцієнтами із L, що тягнуло б алгебраїчну залежність елементів x і y. Але із визначення $K(x, y)$ випливає, що x, y алгебраїчно незалежні: $\frac{f(x,y)}{g(x,y)} = 0 \Leftrightarrow f(x, y) = 0$. Отримана суперечність означає, що $M \subset L(x)$. Таким чином, $M = L(x)$.

Приклад 13. *Довести, що* $y = \sqrt{x}\left(\sqrt[3]{\frac{1}{x}} - 1\right)$ *є алгебраїчним над* $K(x)$ *і знайти його степінь.*

Знайдемо мінімальний многочлен для y. Оскільки $y = \sqrt[6]{x} - \sqrt{x}$, то $y + \sqrt{x} = \sqrt[6]{x}$. Після піднесення цієї рівності до третього степеня, отримуємо: $y^3 + 3xy + 3y^2\sqrt{x} + x\sqrt{x} = \sqrt{x}$. Перенесемо доданки, що містять $\sqrt{x}$, у правий бік, винесемо $\sqrt{x}$ за дужки і отримаємо: $y^3+3xy = \sqrt{x}(-3y^2 + 1 - x)$. Підносячи отриману рівність до квадрату і зводячи подібні при степенях y, отримуємо: $y^6-3xy^4+(3x^2+6x)y^2-x^3+2x^2-x = 0$. Звідси випливає, що елемент y є коренем многочлена

$$f(t) = t^6 - 3xt^4 + (3x^2 + 6x)t^2 - (x^3 - 2x^2 + x) \in K(x)[t].$$

Отриманий многочлен має коефіцієнти із $K[x]$, всі коефіцієнти, крім старшого, діляться на незвідний многочлен x, але вільний член не ділиться на x^2. Тому за ознакою Айзенштайна даний многочлен є незвідним над $K[x]$, звідки в силу леми Гауса, він є незвідним і над $K(x)$. Таким чином, $f(t)$ — мінімальний многочлен для y, звідки випливає, що степінь y над $K(x)$ дорівнює $\deg f(t) = 6$.

Задачі

2.1 Визначити, чи є розширення $\mathbb{Q}(\alpha)$ поля $\mathbb{Q}$ є алгебраїчним. Якщо так, знайти $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ та $m_\alpha(x)$:

a) $\sqrt[4]{5} + \sqrt{5}$;

b) $\sqrt{\pi} + 1$;

c) $\sqrt[6]{3} + \sqrt{3}$;

d) $1+\sqrt{2}+\cdots+\sqrt{2^{n-1}}$.

2.2 Знайти мінімальний многочлен елемента α над полем F, якщо

a) $\alpha = 3+2i$, $F=\mathbb{R}$;

b) $\alpha = 3+2i$, $F=\mathbb{C}$;

c) $\alpha = 1+\sqrt{3}$, $F=\mathbb{Q}$;

d) $\alpha = 1+\sqrt{3}$, $F=\mathbb{Q}(\sqrt{2}+\sqrt{3})$.

2.3 Нехай u — корінь многочлена $x^3+3x^2-9x+6 \in \mathbb{Q}[x]$. Подати наступні елементи поля $\mathbb{Q}(u)$ у вигляді лінійної комбінації $1, u, u^2$:

$$u^5; \quad u^4+u; \quad \frac{1}{u}; \quad \frac{u^4+3u+1}{u^2+2u-11}.$$

2.4 Довести, що розщирення $\mathbb{R} \supset \mathbb{Q}$ є нескінченним.

2.5 Довести, що $\mathbb{Q}(\pi) \simeq \mathbb{Q}(x)$.

2.6 Довести, що будь-яке скінченне розширення поля $\mathbb{R}$ ізоморфне $\mathbb{R}$ або $\mathbb{C}$.

2.7 Довести, що комплексне число z є алгебраїчним тоді й лише тоді, коли $\overline{z}$ є алгебраїчним.

2.8 Довести, що дійсні числа a і b алгебраїчні тоді й лише тоді, коли комплексне число $z=a+bi$ алгебраїчне.

2.9 Визначити, які з наступних чисел є цілими алгебраїчними:

$$\sqrt{2}; \quad \sqrt{2}+\sqrt{3}; \quad \frac{2+\sqrt{5}}{2}; \quad \frac{\sqrt{5}+\sqrt{13}}{2}; \quad \sqrt{\frac{3-i\sqrt{3}}{2}}.$$

2.10 Нехай a — алгебраїчне число. Довести, що знайдеться натуральне n, таке, що na — ціле алгебраїчне число.

2.11 Нехай d — ціле безквадратне число (тобто d не ділиться на квадрат цілого числа $a>1$). Знайти всі алгебраїчні елементи поля $\mathbb{Q}(\sqrt{d})$. Відповідь: $a+b\sqrt{d}$, де a,b — цілі, при $d \equiv 2 (\mathrm{mod}\, 4)$ або $d \equiv 3 (\mathrm{mod}\, 4)$; $\frac{a+b\sqrt{d}}{2}$, де a,b — цілі числа однакової парності, при $d \equiv 1 (\mathrm{mod}\, 4)$.

2.12 Довести, що розширення $P(\alpha_1, \ldots, \alpha_n) \supset P$, де $\alpha_1, \ldots, \alpha_n$ — алгебраїчні над P, є скінченним.

2.13 Довести, що відношення "бути алгебраїчним розширенням"є транзитивним, тобто, якщо $P \supset F$, $F \supset K$ — алгебраїчні розширення, то $P \supset K$ — також алгебраїчне розширення.

2.14 Знайти степені наступних розширень поля $\mathbb{Q}$:

a) $\mathbb{Q}(1 + \sqrt{5})$;
b) $\mathbb{Q}(\sqrt[3]{2} + 2\sqrt[3]{4})$;
c) $\mathbb{Q}\left(\frac{\sqrt{2}}{\sqrt[3]{2}}\right)$;
d) $\mathbb{Q}(\sqrt{2} + i)$;
e) $\mathbb{Q}(\sqrt[105]{9})$.

2.15 Знайти базиси та вказати степінь над $\mathbb{Q}$ наступних полів:

a) $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{6})$;
b) $\mathbb{Q}(\varepsilon)$, $\varepsilon = \frac{-1+i\sqrt{3}}{2}$;
c) $\mathbb{Q}(\varepsilon)$, $\varepsilon = \cos\frac{2\pi}{p} + i\sin\frac{2\pi}{p}$, p — просте число;
d) $\mathbb{Q}(\sqrt{3}, \sqrt[3]{3})$;
e) $\mathbb{Q}(\sqrt{3}, i)$.

2.16 Навести приклад алгебраїчних над полем F елементів a і b степенів відповідно r і q $(p \neq q)$, таких, що $[F(a, b) : F] < rq$.

2.17 Довести, що для алгебраїчних над полем F елементів a і b степенів відповідно r і q, де $(p, q) = 1$, виконується рівність $[F(a, b) : F] = rq$.

2.18 Нехай $F \subset P$, $a, b \in P$ — алгебраїчні над F елементи степенів відповідно p і q, де p, q — прості числа, причому $p > q$ і $b^p \notin F$. Довести, що ab — алгебраїчний над F степеня pq.

2.19 Навести приклад алгебраїчних чисел a і b степенів відповідно 2 і 3, таких, що ab має степінь:

a) 3; b) 6.

2.20 Нехай $\operatorname{char} P \neq 2$ і $[F : P] = 2$. Довести, що знайдеться елемент $a \in F$, такий, що $F = P(a)$ і $a^2 \in P$. Чи лишиться це твердження справедливим, якщо $\operatorname{char} P = 2$?

2.21 Нехай a — алгебраїчний над F елемент непарного степеня. Довести, що $F(a) = F(a^2)$.

2.22 Нехай a — алгебраїчний над F елемент і $K(a) = K(a^2)$. Чи випливає звідси, що a має непарний степінь над F?

2.23 Довести, що розширення простого степеня не має проміжних підполів, тобто якщо $[F : K] = p$ — просте число і $F \supset P \supset K$, то $F = P$ або $P = K$.

2.24 Для довільного поля K розглянемо поле раціональних функцій $K(x, y)$ і його підполе $L = K(x^2 + x + 10)$. Визначити, які з наступних елементів є алгебраїчними над L:

a) x;

b) $x + y$;

c) $\dfrac{1}{x+1}$;

d) $\dfrac{x}{y}$;

e) $\dfrac{x+y}{x-y}$.

2.25 Знайти степінь розширення $L \subset M$, якщо

a) $L = K(x^2)$, $M = K(x)$;

b) $L = K\left(x - \dfrac{1}{x}\right)$;

c) $L = K\left(x^2 + \dfrac{1}{x^2}\right), M = K(x)$;

d) $L = K(x^2, y^2), M = K(x, y)$.

2.26 Довести, що даний елемент є алгебраїчним над $K(x)$ і знайти його степінь у кожному з наступних випадків:

a) $\sqrt{x} + \sqrt{\dfrac{1}{x}}$;

b) $\sqrt[3]{\dfrac{1}{x+1}}$.

2.27 Довести, що якщо $[K : L] = n$, то $[K(x) : L(x)] = n$.

2.28 Довести, що якщо $a \in K(x)$ — елемент, алгебраїчний над K, то $a \in K$.

2.29 Нехай $a_0x^n + \cdots + a_n \in K[x]$, $a_0 \neq 0$. Довести, що $[K(x) : K(a_0x^n + \cdots + a_n)] = n$.

3 Поля розкладу многочленів, нормальні розширення

Нехай $f(x) \in K[x]$ — незвідний над полем K многочлен. Наступна теорема відома як *теорема про символічне приєднання Кронекера.*

Теорема 6. *Існує розширення поля K, в якому многочлен $f(x)$ має корінь.*

Доведення теореми Кронекера є конструктивним: шуканим розширенням буде, наприклад, поле $K[x]/(f(x))$: в цьому полі $f(x)$ має коренем елемент $\overline{x} = x + (f(x))$.

Із теореми Кронекера випливає, що для довільного многочлена $f(x) \in K[x]$ знайдеться розширення поля K, яке містить всі корені многочлена $f(x)$, тобто таке розширення поля K, над яким $f(x)$ розкладається на лінійні множники.

Означення 9. *Найменше розширення K, яке містить всі корені $f(x)$, називається* полем розкладу $f(x)$.

Відомо, що поле розкладу многочлена визначене однозначно із точністю до ізоморфізму. Якщо $\alpha_1, \ldots, \alpha_n$ — всі корені $f(x)$, то поле розкладу $f(x)$ збігається з полем $K(\alpha_1, \ldots, \alpha_n)$.

Означення 10. *Розширення $F \supset K$ називається* нормальним*, якщо F є полем розкладу деякого многочлена $f(x) \in K[x]$.*

Теорема 7. *Нехай $F \supset K$ — скінченне розширення. Наступні умови еквівалентні.*

1. *$F \supset K$ — нормальне розширення.*
2. *Для будь-якого гомоморфізму полів $\varphi : F \to P$, тотожного на K (тобто $\varphi(a) = a$ для всіх $a \in K$), виконується $\varphi(F) = F$.*
3. *Якщо незвідний многочлен $f(x) \in K[x]$ має корінь в F, то цей многочлен розкладається над F на лінійні множники.*

Приклади розв'язування задач

Приклад 14. *Знайти розширення поля $\mathbb{Q}$, яке є полем розкладу многочлена $x^3 - 2$, а також степінь цього розширення над $\mathbb{Q}$.*

Позначимо шукане поле через F. За означенням, F — найменше поле, що містить поле $\mathbb{Q}$ і всі корені даного многочлена, тобто $F = \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3)$, де $\alpha_1, \alpha_2, \alpha_3$ — корені $x^3 - 2$.

Нехай $\varepsilon_1 = \cos\frac{2\pi}{3} + i\sin\frac{2\pi}{3}$ — первісний корінь степеня 3 з одиниці. Тоді коренями многочлена $x^3 - 2$ є

$$\beta_0 = \sqrt[3]{2}, \beta_1 = \sqrt[3]{2}\varepsilon_1, \beta_2 = \sqrt[3]{2}\varepsilon_1^2. \tag{5}$$

Отже, $F = \mathbb{Q}(\beta_0, \beta_1, \beta_2)$.

Оскільки $\varepsilon_1 = \frac{\beta_2}{\beta_1} \in F$, $\sqrt[3]{2} = \beta_0 \in F$, то $\mathbb{Q}(\sqrt[3]{2}, \varepsilon_1) \subset F$. З іншого боку, із рівностей (5) випливає, що β_0, β_1, $\beta_2 \in \mathbb{Q}(\sqrt[3]{2}, \varepsilon_1)$, звідки $F \subset \mathbb{Q}(\sqrt[3]{2}, \varepsilon_1)$. Таким чином, $F = \mathbb{Q}(\sqrt[3]{2}, \varepsilon_1)$. Очевидно, що

$$F \supset \mathbb{Q}(\sqrt[3]{2}) \supset \mathbb{Q}. \tag{6}$$

Оскільки $F = \mathbb{Q}(\sqrt[3]{2})(\varepsilon_1)$, причому ε_1 є коренем многочлена $x^2 + x + 1$, незвідного над $\mathbb{Q}(\sqrt[3]{2})$, то $[F : \mathbb{Q}(\sqrt[3]{2})] = 2$. Крім цього, $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$, позаяк $\sqrt[3]{2}$ є коренем многочлена $x^3 - 2$, незвідного над $\mathbb{Q}$. Застосовуючи до (6) теорему про вежу розширень (теорема 2), отримуємо

$$[F : \mathbb{Q}] = [F : \mathbb{Q}(\sqrt[3]{2})] \cdot [\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 2 \cdot 3 = 6.$$

Приклад 15. *Знайти степінь над $\mathbb{Q}$ поля розкладу многочлена $x^n - 1$, $n \in \mathbb{N}$.*

Зрозуміло, що шукане поле має вигляд $\Gamma_n = \mathbb{Q}(\varepsilon)$, де ε — деякий первісний корінь степеня n із 1. Позначимо через P_n множину потужності $|P_n| = \varphi(n)$ всіх первісних коренів степеня n із 1 (де φ — функція Ойлера). Оскільки підгрупи групи $G = \langle\varepsilon\rangle$ коренів n-го степеня із 1 знаходяться у бієктивній відповідності із дільниками числа n і кожен корінь n-го степеня з 1 є первісним коренем степеня d з 1 для деякого дільника d числа n, то множина всіх коренев n-го степеня з 1 є диз'юнктним об'єднанням множин P_d, де d пробігає множину дільників числа n.

Круговим многочленом, що відповідає полю Γ_n, називається многочлен

$$\Phi_n(x) = \prod_{\theta \in P_n} (x - \theta)$$

степеня $\varphi(n)$. Із наведених міркувань щодо множини P_n випливає, що

$$x^n - 1 = \prod_{k=0}^{n-1} (x - \varepsilon^k) = \prod_{d|n} \left(\prod_{\theta \in P_d} (x - \theta) \right) = \prod_{d|n} \Phi_d(x).$$

Покажемо, що $\Phi_n(x) \in \mathbb{Z}[x]$, застосовуючи індукцію за n. Для $n = 1$ маємо: $\Phi_1(x) = x - 1$. Припустимо, що $n \geq 2$ і $\Phi_k(x) \in \mathbb{Z}[x]$ для всіх $k < n$. Покладемо

$$g(x) = \prod_{d|n, d<n} \Phi_d(x).$$

Очевидно, $g(x)$ — унітарний многочлен. Крім цього, за припущенням $g(x)$ має цілі коефіцієнти. Застосовуючи алгоритм ділення з остачею, ми отримуємо однозначно визначені $q(x), r(x) \in \mathbb{Z}[x]$, такі, що $x^n - 1 = q(x)g(x) + r(x)$, причому $\deg r(x) < \deg g(x)$. Але $x^n - 1 = \Phi_n(x)g(x)$ в $\mathbb{Q}[x]$. Отже, $\Phi_n(x) = q(x) \in \mathbb{Z}[x]$.

Тепер покажемо, що $\Phi_n(x)$ незвідний над $\mathbb{Q}$. Позначимо через $m(x)$ унітарний мінімальний многочлен елемента ε над $\mathbb{Q}$. Нехай p — просте число, $p < n$ і $(p, n) = 1$. Покажемо спочатку, що ε^p також є коренем $m(x)$. Для цього позначимо через $f(x)$ — унітарний мінімальний многочлен елемента ε^p над $\mathbb{Q}$ і покажемо, що насправді $f(x) = m(x)$. Міркуватимемо від супротивного. Припустимо, що $m(x) \neq g(x)$. Оскільки $x^n - 1$ ділиться також на $m(x)$, і на $g(x)$, то $x^n - 1$ ділиться і на найменше спільне кратне $m(x)$ і $g(x)$, яке, враховуючи незвідність обох цих многочленів, дорівнює їхньому добутку $m(x)g(x)$. Отже,

$$x^n - 1 = m(x)g(x)h(x), \tag{7}$$

причому внаслідок леми Гауса $h(x) \in \mathbb{Z}[x]$. Далі, многочлен $f(x^p)$ має ε своїм коренем, тому ділиться на $m(x)$: $f(x^p) = m(x)k(x)$, де знов-таки внаслідок леми Гауса $k(x) \in \mathbb{Z}[x]$.

Розглянемо многочлен $f(x^p)(\mathrm{mod}\, p)$. Зрозуміло, що $f(x^p) \ (\mathrm{mod}\, p) = (f(x))^p \ (\mathrm{mod}\, p)$. Враховуючи це, матимемо

$$(f(x))^p(\mathrm{mod}\, p) = m(x)(\mathrm{mod}\, p) \cdot k(x)(\mathrm{mod}\, p).$$

Нехай $t(x) \in \mathbb{Z}_p[x]$ — незвідний многочлен, що ділить $m(x)(\mathrm{mod}\, p)$. Тоді $t(x)$ ділить і $(f(x))^p(\mathrm{mod}\, p)$, а отже і $f(x)(\mathrm{mod}\, p)$. Переходячи тепер у (7) до модуля p, отримуємо:

$$(x^n - 1)(\mathrm{mod}\, p) = m(x)(\mathrm{mod}\, p) \cdot g(x)(\mathrm{mod}\, p) \cdot h(x)(\mathrm{mod}\, p).$$

Оскільки права частина останньої рівності ділиться на $t^2(x)$, то її ліва частина також повинна ділитися на $t^2(x)$. Тобто, і многочлен $(x^n - 1)(\mathrm{mod}\, p)$, і його похідна $((x^n - 1)(\mathrm{mod}\, p))' = (nx^{n-1})(\mathrm{mod}\, p)$ повинні ділитися на $t(x)$. А це суперечить очевидній взаємній простоті многочлена $(x^n - 1)(\mathrm{mod}\, p)$ і його похідної. Отже, ми довели, що для довільного простого $p < n$, такого, що $(p, n) = 1$, елемент ε^p є коренем $m(x)$.

Покажемо нарешті, що всі первісні корені степеня n із 1 є коренями $m(x)$. Нехай ε^s — первісний корінь степеня n із 1, де $s = p_1 \dots p_r$, причому p_i, $1 \le i \le r$, — прості числа, взаємно прості з n (не обов'язково попарно різні). За доведеним вище ε^{p_1} буде коренем многочлена $m(x)$. Але тоді знов-таки за доведеним вище $\varepsilon^{p_1 p_2} = (\varepsilon^{p_1})^{p_2}$ також буде коренем $m(x)$. Повторюючи це міркування потрібну кількість разів, бачимо, що і ε^s теж буде коренем $m(x)$.

Отже, ми довели, що кожен корінь $\Phi_n(x)$ є також коренем $m(x)$. Звідси, враховуючи, що $\Phi_n(x)$ не має кратних коренів, отримуємо рівність $m(x) = \Phi_n(x)$. Зокрема, $\Phi_n(x)$ є незвідним над $\mathbb{Q}$ і тому степінь поля розкладу $x^n - 1$ над $\mathbb{Q}$ дорівнює $\varphi(n)$.

Приклад 16. *Знайти поле розкладу многочлена $x^2 + 1$ над $\mathbb{Z}_3$.*

Розглянемо поле $F = \mathbb{Z}_3/(x^2+1) = \{\overline{0}, \overline{1}, \overline{2}, \overline{x}, \overline{x+1}, \overline{x+2}, \overline{2x}, \overline{2x+1}, \overline{2x+2}\}$, де через $\overline{ax+b}$ ми позначаємо елемент $ax+b+(x^2+1)$ поля F. В полі F многочлен x^2+1 має корінь — це $\overline{x}$. За теоремою 4 $F \simeq \mathbb{Z}_3(\overline{x})$. Будемо вважати, що $\mathbb{Z}_3 = \{\overline{0}, \overline{1}, \overline{2}\}$, і тому $F = \mathbb{Z}_3(\overline{x}) = \mathbb{Z}_3(\overline{x}, \overline{2x})$. Але легко бачити, що $\overline{2x}$ є другим коренем x^2+1 (оскільки $\overline{2x}^2 + 1 = \overline{x}^2 + 1 = \overline{x^2+1} = \overline{0}$). Отже, за означенням полем розкладу x^2+1 над $\mathbb{Z}_3$ є поле $\mathbb{Z}_3(\overline{x}, \overline{2x}) = F$.

Приклад 17. *Нехай $f(x) \in F[x]$ — незвідний многочлен, P — таке розширення поля F, що $[P : F]$ і $\deg f(x)$ взаємно прості. Довести, що $f(x)$ є незвідним над P.*

Нехай $\deg f(x) = n$, $[P : F] = k$ і $(n, k) = 1$. Припустимо, що $f(x) = f_1(x) \cdot \dots \cdot f_r(x)$ в $P[x]$, причому для всіх i, $1 \le i \le r$, многочлен $f_i(x) \in P[x]$ — незвідний в кільці $P[x]$. За теоремою Кронекера (теорема 6) в деякому розширенні поля F многочлен f має корінь, який позначимо a_1. Очевидно, a_1 буде також коренем деякого з многочленів $f_i(x)$, наприклад $f_1(x)$. За теоремою 4 $[F(a_1) : F] = n$. З іншого боку, $F \subset P \subset P(a_1)$, звідки $[P(a_1) : F] = [P(a_1) : P] \cdot [P : F] = sk$, де $s = \deg f_1$. Оскільки $F \subset F(a_1) \subset P(a_1)$ то число $[P(a_1) : F] = sk$ ділиться на n. Звідси із урахуванням взаємної простоти n і k отримуємо, що s ділиться на n. Однак оскільки

$$n = \deg f(x) = \sum_{i=1}^{r} \deg f_i(x) = s + \sum_{i=2}^{r} \deg f_i(x),$$

то $n = s$ і $\deg f_2(x) = \dots = \deg f_r(x) = 0$. А це означає, що $f(x)$ є незвідним над P.

Приклад 18. *Довести, що розширення* $\mathbb{Q}(\sqrt[3]{2}) \supset \mathbb{Q}$ *не є нормальним.*

Від супротивного, припустимо, $\mathbb{Q}(\sqrt[3]{2}) \supset \mathbb{Q}$ — нормальне розширення. Розглянемо многочлен $f(x) = x^3 - 2 \in \mathbb{Q}[x]$. Він незвідний над $\mathbb{Q}$ внаслідок ознаки Айзенштайна і має корінь в $\mathbb{Q}(\sqrt[3]{2})$. Тому за теоремою 7 всі корені $f(x)$ мусять лежати в $\mathbb{Q}(\sqrt[3]{2})$. Отже, повинно бути $\beta_1 = \sqrt[3]{2}\cdot(\cos\frac{2\pi}{3} + i\sin\frac{2\pi}{3}) \in \mathbb{Q}(\sqrt[3]{2})$, і $\beta_2 = \sqrt[3]{2}\cdot(\cos\frac{4\pi}{3} + i\sin\frac{4\pi}{3}) \in \mathbb{Q}(\sqrt[3]{2})$, звідки $\frac{1}{\sqrt[3]{2}}(\beta_1 - \beta_2) = i\sqrt{3} \in \mathbb{Q}(\sqrt[3]{2})$, а тому $i \in \mathbb{Q}(\sqrt[3]{2})$, зокрема, i є дійсним числом. Суперечність. Таким чином, дане розширення не є нормальним.

Приклад 19. *Визначити, чи є нормальним розширення* $\mathbb{Q}(x^2) \subset \mathbb{Q}(x)$.

Зауважимо, що многочлен $t^2 - x^2 \in \mathbb{Q}(x^2)[t]$ є анулюючим для x^2. Оскільки, очевидно, $x \notin \mathbb{Q}(x^2)$, то мінімальний многочлен для x над $\mathbb{Q}(x^2)$ повинен мати принаймі другий степінь. Тому $t^2 - x^2$ є мінімальним многочленом для x. Оскільки $(-x)$ (другий корінь цього многочлена) також лежить в $\mathbb{Q}(x)$, то за теоремою 7 дане розширення є нормальним.

Приклад 20. *Визначити, чи є нормальним розширення* $\mathbb{Z}_3(x^3) \subset \mathbb{Z}_3(x)$.

Розглянемо многочлен $f(t) = t^3 - x^3 \in \mathbb{Z}_3(x^3)[t]$. Даний многочлен має коренем $x \in \mathbb{Z}_3(x)$. Крім того, $f(t)$ розпадається на лінійні множники $f(t) = (t - x)^3$ над полем $\mathbb{Z}_3(x)$. Якщо $F \supset \mathbb{Z}_3(x^3)$ — найменше розширення $\mathbb{Z}_3(x^3)$, над яким $f(t)$ розпадається на лінійні множники, то $F \ni x$, звідки $F \supset \mathbb{Z}_3(x)$. Таким чином, $\mathbb{Z}_3(x)$ є полем розкладу многочлена $f(t) \in \mathbb{Z}_3(x^3)[t]$, що за означенням тягне нормальність заданого розширення.

Приклад 21. *Довести, що кожне розширення степеня* 2 *є нормальним.*

Нехай $L \supset K$ — розширення степеня 2 і $a \in L \setminus K$. Тоді $L = K(a)$ за доведеним у прикладі 11. Розширення $K(a) \supset K$ алгебраїчне, оскільки воно скінченне. Із теореми 4 про будову простих алгебраїчних розширень випливає, що a є коренем певного многочлена $f(x)$ степеня 2, незвідного над K. Але тоді над полем L маємо: $f(x) = (x - a)g(x)$, де $\deg g(x) = 1$. Тому $f(x)$ розкладається над L на лінійні множники. Оскільки довільне поле F, таке, що $L \supset F \supset K$, яке не дорівнює L, збігається з K, то L є найменшим полем, над яким $f(x)$ розкладається на лінійні множники, тобто полем розкладу $f(x)$. Отже, за означенням $L \supset K$ — нормальне розширення.

Приклад 22. *Довести, що поле розкладу многочлена* $x^{p^n} - x \in \mathbb{Z}_p[x]$ *має потужність* p^n.

Нехай $f(x) = x^{p^n} - x \in \mathbb{Z}_p[x]$. Оскільки $f'(x) = -1$, то $(f(x), f'(x)) = 1$, звідки випливає, що $f(x)$ не має кратних коренів. Позначимо через $F \supset \mathbb{Z}_p$ — поле розкладу $f(x)$, і через $A = \{\alpha_1, \ldots, \alpha_{p^n}\}$ — множину коренів $f(x)$. Зрозуміло, що $A \subset F$. Покажемо, що A є полем. Нехай $\alpha, \beta \in A$. Оскільки F має характеристику p, використовуючи результат задачі 1.11, маємо: $(\alpha + \beta)^{p^n} = \alpha^{p^n} + \beta^{p^n} = \alpha + \beta$, звідки $\alpha + \beta \in A$. Аналогічно, $\alpha - \beta \in A$. Крім того, $(\alpha\beta)^{p^n} = \alpha^{p^n}\beta^{p^n} = \alpha\beta$, звідки $\alpha\beta \in A$. Нарешті, якщо $\alpha \neq 0$, то $(\alpha^{-1})^{p^n} = (\alpha^{p^n})^{-1} = \alpha^{-1}$, звідки $\alpha^{-1} \in A$. Ми показали, що A є підмножиною поля F, замкненою відносно додавання, віднімання, множення та взяття оберненого елемента. Це означає, що A є полем. Враховуючи те, що A містить всі корені $f(x)$, приходимо до висновку, що A є полем розкладу $f(x)$, тобто $A = F$.

Приклад 23. *Нехай* $K \subset L$ *і* L *— скінченне поле. Довести, що* L *є нормальним розширенням поля* K.

Відомо (див., зокрема, задачу 1.8), що потужність скінченного поля є степенем простого числа — характеристики цього поля. Нехай $|L| = p^n$, де $p = \mathrm{char}L$. Тоді за попереднім прикладом, враховуючи, що з точністю до ізоморфізму існує лише одне поле потужності p^n і єдиність поля розкладу, можна вважати, що L є полем розкладу многочлена $f(x) = x^{p^n} - x \in \mathbb{Z}_p[x]$. Оскільки $L \supset K \supset \mathbb{Z}_p$ (див. задачу 1.9), то $f(x)$ можна розглядати як многочлен над K, а тому L є полем розкладу многочлена $f(x) \in K[x]$, що за означенням тягне нормальність даного розширення.

Приклад 24. *Нехай* K *— поле,* $a \in K$ *і* p *— просте число. Довести, що многочлен* $x^p - a$ *або є незвідним, або має корінь в* K.

Припустимо, що многочлен $x^p - a$ є звідним над K: $x^p - a = f(x)g(x)$. Над своїм полем розкладу $x^p - a$ розкладається на множники в наступний спосіб:

$$x^p - a = (x - \theta)(x - \varepsilon\theta)\ldots(x - \varepsilon^{p-1}\theta),$$

де ε — первісний корінь степеня p із одиниці і θ — такий елемент, що $\theta^p = a$. Отже, множник $f(x)$ повинен бути добутком множників вигляду $x - \varepsilon^t\theta$, звідки вільний член многочлена $f(x)$ дорівнює $b = \lambda\theta^s$ або $-b = -\lambda\theta^s$, де λ — корінь степеня p із 1 і $0 < s < p$. Відзначимо, що

$b^p = \theta^{ps} = a^s$. Оскільки $(p, s) = 1$, то знайдуться цілі числа c, d, такі, що $cs + dp = 1$. Але тоді

$$a = a^{cs}a^{dp} = b^{pc}a^{dp} = (b^c a^d)^p,$$

звідки випливає, що елемент $b^c a^d \in K$ є коренем многочлена $x^p - a$, що і треба було довести.

Задачі

3.1 Знайти розширення поля $\mathbb{Q}$, яке є полем розкладу многочлена $f(x)$, а також степінь цього розширення, якщо

a) $f(x) = x^2 - 2$;

b) $f(x) = x^4 - 2$;

c) $f(x) = x^4 + 2$;

d) $f(x) = x^4 + x^2 + 1$;

e) $f(x) = x^p - 1$, p — просте;

f) $f(x) = x^p - a$, $a \in \mathbb{Q}$, a не є p-им степенем в $\mathbb{Q}$, p — просте.

3.2 Знайти поле розкладу многочлена $x^3 + x - 1$ над $\mathbb{Z}_5$.

3.3 Знайти поле розкладу многочлена $x^3 + x + 1$ над $\mathbb{Z}_2$.

3.4 Знайти базиси і степінь над $\mathbb{Q}$ поля розкладу многочлена

a) $(x^2 - 2)(x^2 - 5)$;

b) $x^4 - x^2 + 1$;

c) $x^3 - 2$;

d) $x^4 - 7$.

3.5 Визначити, які з наступних розширень поля $\mathbb{Q}$ є нормальними:

a) $\mathbb{Q}(\sqrt{2})$; b) $\mathbb{Q}(i, \sqrt{2})$; c) $\mathbb{Q}(\sqrt[4]{2})$; d) $\mathbb{Q}(\sqrt[3]{2}, i)$;

e) $\mathbb{Q}(\sqrt{2}, \sqrt{3})$; f) $\mathbb{Q}(\sqrt[4]{2}, i)$; g) $\mathbb{Q}(\sqrt[6]{3}, i)$; h) $\mathbb{Q}(\sqrt[6]{2}, i)$.

3.6 Знайти найменше нормальне розширення поля $\mathbb{Q}$, яке містить задане поле:

a) $\mathbb{Q}(\sqrt{2})$; b) $\mathbb{Q}(\sqrt[3]{2})$; c) $\mathbb{Q}(\sqrt[4]{2})$.

3.7 Визначити, які з наступних розширень є нормальними:

a) $\mathbb{Q}(x^3) \subset \mathbb{Q}(x)$; b) $\mathbb{C}(x^3) \subset \mathbb{C}(x)$; c) $\mathbb{C}(x^n) \subset \mathbb{C}(x)$.

3.8 Визначити, які з наступних розширень є нормальними:

a) $\mathbb{Z}_3(x^2) \subset \mathbb{Z}_3(x)$; b) $\mathbb{Z}_3(x^4) \subset \mathbb{Z}_3(x)$.

3.9 Вказати найменше поле, що містить $\mathbb{Q}(x)$, яке є нормальним розширенням поля

a) $\mathbb{Q}(x^3)$; b) $\mathbb{Q}(x^4)$; c) $\mathbb{Q}(x^n)$, $n \in \mathbb{N}$.

3.10 Нехай ε_n є первісним коренем степеня n з одиниці. Довести, що $\mathbb{Q}(\varepsilon_n) \supset \mathbb{Q}$ є нормальним розширенням.

3.11 Нехай L, M — скінченні розширення поля K, причому $K \subset L \subset M$. Довести або спростувати кожне з наступних тверджень:

a) якщо M — нормальне розширення поля K, то M — нормальне розширення поля L;

b) якщо M — нормальне розширення поля L і L — нормальне розширення поля K, то M — нормальне розширення поля K;

c) якщо M — нормальне розширення поля K, то L — нормальне розширення поля K.

3.12 Нехай $L \supset \mathbb{Q}$ — скінченне нормальне розширення непарного степеня. Довести, що тоді $L \subset \mathbb{R}$.

3.13 Нехай K — поле, $a \in K$, $n \in \mathbb{N}$ і многочлен $x^n - 1$ розкладається над K на лінійні множники. Довести, що многочлен $x^n - a$ або є незвідним над K, або для деякого дільника d числа n многочлен $x^d - a$ має корінь в K.

3.14 Довести, що у попередній задачі вимога про розкладність многочлена $x^n - 1$ над K на лінійні множники є істотною.

4 Сепарабельні елементи і розширення

Незвідний многочлен $f(x) \in K[x]$ називається *сепарабельним*, якщо $f(x)$ не має кратних коренів (зауважимо, що із незвідності $f(x)$ випливає, що всі його корені не належать K). Многочлен $g(x) \in K[x]$ називається *сепарабельним*, якщо кожен його незвідний дільник є сепарабельним.

Нехай $F \supset K$ — розширення полів.

Означення 11. *Елемент $a \in F$ називається* сепарабельним *над K, якщо a є коренем певного сепарабельного многочлена над K, тобто якщо мінімальний многочлен елемента a не має кратних коренів. Розширення $F \supset K$ називається* сепарабельним*, якщо кожен його елемент є сепарабельним.*

Зауважимо, що із означення безпосередньо випливає, що сепарабельне розширення є алгебраїчним.

Означення 12. *Поле K називається* досконалим*, якщо кожне його алгебраїчне розширення є сепарабельним.*

Теорема 8. *Нехай F — скінченне сепарабельне розширення поля K. Тоді знайдеться елемент $\theta \in L$, такий, що $F = K(\theta)$.*

Елемент θ, зазначений у теоремі 8, називається *примітивним елементом* розширення $F \supset K$, а сама теорема 8 часто називається *теоремою про примітивний елемент.*

Зазначимо, що у випадку нескінченного поля K шукати примітивний елемент розширення можна в наступний спосіб.

Нехай спочатку $L = K(\alpha, \beta)$. Через $f(x)$ і $g(x)$ позначимо мінімальні многочлени елементів α і β відповідно. Нехай $\alpha = \alpha_1, \ldots, \alpha_n$ — всі корені $f(x)$, $\beta = \beta_1, \ldots, \beta_m$ — усі корені $g(x)$. Покладемо $d_{ij} = \frac{\beta_i - \beta_1}{\alpha_j - \alpha_1}$, $1 \leq i \leq m$, $2 \leq j \leq n$. Візьмемо будь-який елемент $c \in K$, відмінний від кожного з d_{ij}. Тоді за примітивний елемент даного розширення можна взяти $\theta = \beta + c\alpha$.

Припустимо, що ми вміємо шукати примітивний елемент розширення поля K, одержаного приєднанням менш ніж n елементів, $n \geq 2$, і нехай маємо розширення $K(\alpha_1, \ldots, \alpha_n)$. Позначимо через θ примітивний елемент розширення $K(\alpha_1, \ldots, \alpha_{n-1})$. Тоді

$$K(\alpha_1, \ldots, \alpha_n) = K(\alpha_1, \ldots, \alpha_{n-1})(\alpha_n) = K(\theta, \alpha_n),$$

і наша задача зводиться до відшукання примітивного елемента розширення, отриманого приєднанням двох елементів.

Приклади розв'язування задач

Приклад 25. *Довести, що елемент a, алгебраїчний над полем K, не є сепарабельним тоді й лише тоді, коли похідна мінімального многочлена елемента a є нульовим многочленом.*

Нехай a не є сепарабельним і $m'_a(x)$ не є тотожним нулем. Тоді із незвідності $m_a(x)$ і $\deg m'_a(x) < \deg m_a(x)$ випливає, що $(m_a(x), m'_a(x))=1$. Але ж $m_a(x)$ має деякий корінь α кратності не нижче 2. Тому α є також і коренем $m'_\alpha(x)$, звідки $(x-\alpha)$ — спільний дільник $m_a(x)$ і $m'_\alpha(x)$ всупереч їх взаємній простоті.

Навпаки, нехай $m'_a(x)$ є нульовим многочленом. Тоді будь-який корінь $m_a(x)$ є також і коренем похідної, звідки $m_a(x)$ має кратні корені, а отже є несепарабельним многочленом. Тому і елемент a не є сепарабельним.

Приклад 26. *Нехай* $\mathrm{char}K = 0$. *Довести, що K є досконалим, тобто що кожен алгебраїчний над K елемент є сепарабельним.*

Достатньо показати, що будь-який незвідний над K многочлен є сепарабельним. Нехай $f \in K[x]$ — незвідний многочлен. Позначимо $n = \deg f$. Оскільки $\mathrm{char}K = 0$, похідна f' многочлена f має степінь $n-1$ і відмінний від нуля старший коефіцієнт, а отже є ненульовим многочленом. Тепер потрібне твердження випливає із попереднього прикладу.

Приклад 27. *Нехай* $\mathrm{char}K = p \neq 0$. *Довести, що алгебраїчний над K елемент a є несепарабельним тоді й лише тоді, коли його мінімальний многочлен $f(x)$ дорівнює $g(x^p)$ для певного $g(x) \in K[x]$.*

Враховуючи приклад 25, досить показати, що похідна мінімального многочлена $f(x)$ елемента a є нульовим многочленом тоді й лише тоді, коли $f(x) = g(x^p)$ для певного $g(x) \in K[x]$. Нехай $f(x) = \sum_{i=o}^{n} x^i a_{n-i}$. Тоді $f'(x) = \sum_{i=1}^{n} x^{i-1} \cdot i a_i$. Умова $f'(x) \equiv 0$ рівносильна тому, що $i \cdot a_i = 0$ для всіх i, $1 \leq i \leq n$. Це, в свою чергу, еквіваленте тому, що для кожного i, $1 \leq i \leq n$ або $i = pk_i = 0(\mathrm{mod}\, p)$, або ж $a_i = 0$, тобто тому, що

$$f(x) = \sum_{i=o}^{n} x^i a_{n-i} = \sum_{0 \leq i \leq n, a_i \neq 0} x^i a_{n-i} = \sum_{0 \leq i \leq n, a_i \neq 0} (x^p)^{k_i} a_{n-i}$$

є многочленом від x^p.

Приклад 28. *Нехай* $\mathrm{char}K = p \neq 0$. *Довести, що елемент* a, *алгебраїчний над* K, *є сепарабельним тоді й лише тоді, коли* $K(a) = K(a^p)$.

Припустимо, що a — сепарабельний елемент і позначимо через $f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n$ мінімальний многочлен елемента a. За прикладом 25 $f'(x)$ не є нульовим многочленом.

Розглянемо многочлен $g(x) = a_0^p x^p + \cdots + a_n^p$ і покажемо, що він є незвідним. Дійсно, якщо б $g(x) = t(x)s(x)$ і $\deg t(x), \deg s(x) < n$, то тоді б

$$g(x^p) = (f(x)^p = t(x^p)s(x^p).$$

Звідси, враховуючи незвідність $f(x)$, випливає, що $t(x^p) = (f(x))^m$ для певного m, $1 \leq m < p$. Але тоді

$$t'(x^p) = m(f(x))^{m-1} \cdot f'(x),$$

що тягне $f'(x) \equiv 0$. Отрмана суперечність доводить, що $g(x)$ є незвідним. Оскільки, крім цього,

$$g(a^p) = a_0^p a^{np} + \cdots + a_n^p = ((f(a))^p,$$

то $g(x)$ є мінімальним многочленом для a^p. Звідси випливає, що $[K(a^p) : K] = n$. Але ж за умовою $[K(a) : K] = n$ і крім цього, маємо очевидні включення $K(a) \supset K(a^p) \supset K$. Тому $K(a^p) = K(a)$.

Нехай тепер $K(a^p) = K(a)$. Припустимо, від супротивного, що a — несепарабельний. Тоді для мінімального многочлена $f(x)$ елемента a маємо $f(x) = g(x^p)$ для певного $g(x) \in K[x]$ (див. приклад 27). Але тоді $\deg f(x) = p \cdot \deg g(x)$, зокрема $\deg g(x) < \deg f(x)$. Оскільки $g(x)$ анулює a^p, то $[K(a^p) : K] \leq \deg g(x)$. Але тоді

$$[K(a) : K] = \deg f(x) > \deg g(x) \geq [K(a^p) : K],$$

всупереч $K(a^p) = K(a)$. Отримана суперечність доводить, що a є сепарабельним.

Приклад 29. *Навести приклад поля* K *і елемента* a, *що є алгебраїчним, але не є сепарабельним над* K.

Нехай $L = \mathbb{Z}_p(x)$, $K = \mathbb{Z}_p(x^p)$. Оскільки $x^p \in L$, то $K \subset L$. Елемент $x \in L$ є алгебраїчним над K, оскільки многочлен $f(y) = y^p - x^p \in K[y]$ його анулює. Але оскільки

$$K(x) = L \neq K = K(x^p),$$

то із прикладу 28 випливає, що x не є сепарабельним над K.

Приклад 30. *Знайти примітивний елемент розширення* $\mathbb{Q} \subset \mathbb{Q}(i, \sqrt{2})$.

Перший спосіб. Скористаємось алгоритмом для відшукання примітивного елемента. Спочатку виписуємо мінімальні многочлени елементів i і $\sqrt{2}$: це x^2+1 і x^2-2 відповідно. Тоді $d_{12} = \frac{i-i}{\sqrt{2}+\sqrt{2}} = 0$, $d_{22} = \frac{i+i}{\sqrt{2}+\sqrt{2}} = \frac{i}{\sqrt{2}} \notin \mathbb{Q}$. Отже, за елемент c можна вибрати будь-яке ненульове раціональне число. Тоді кожен з елемнетів $\theta_c = i + c\sqrt{2}$, $c \in \mathbb{Q} \setminus \{0\}$, буде примітивним елементом даного розширення.

Другий спосіб. Покажемо, що за примітивний елемент можна взяти $i + \sqrt{2}$. Для цього встановимо рівність $\mathbb{Q}(i, \sqrt{2}) = \mathbb{Q}(i + \sqrt{2})$.

Включення $\mathbb{Q}(i + \sqrt{2}) \subset \mathbb{Q}(i, \sqrt{2})$ очевидне (оскільки $\mathbb{Q} \subset \mathbb{Q}(i, \sqrt{2})$, $i + \sqrt{2} \in \mathbb{Q}(i, \sqrt{2})$). Для встановлення зворотного включення $\mathbb{Q}(i, \sqrt{2}) \subset \mathbb{Q}(i + \sqrt{2})$ достатньо показати, що $i, \sqrt{2} \in \mathbb{Q}(i + \sqrt{2})$. Позначимо $\alpha = i + \sqrt{2}$. Тоді $-3\alpha^{-1} = i - \sqrt{2} \in \mathbb{Q}(i + \sqrt{2})$, звідки $i = \frac{\alpha - 3\alpha^{-1}}{2}$, $\sqrt{2} = \frac{\alpha + 3\alpha^{-1}}{2} \in \mathbb{Q}(i + \sqrt{2})$.

Задачі

4.1 Довести, що будь-який многочлен над полем характеристики 0 є сепарабельним.

4.2 Довести, що у випадку скінченного поля K кожний алгебраїчний над K елемент є сепарабельним.

4.3 Довести, що корені многочлена $x^n - 1 \in K[x]$ є сепарабельними елементами над полем K.

4.4 Нехай $\mathrm{char} k = p$ і $f(x) \in K[x]$ — незвідний многочлен. Довести, що над полем розкладу $f(x) = ((x - a_1) \dots (x - a_m))^{p^e}$, де e — ціле невід'ємне число і $a_i \neq a_j$ при $i \neq j$.

4.5 Знайти примітивний елемент розширення

a) $\mathbb{Q}(\sqrt{2}, \sqrt{3}) \supset \mathbb{Q}$;

b) $\mathbb{Q}(\sqrt{2} - i, \sqrt{3} - i) \supset \mathbb{Q}$;

c) $\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) \supset \mathbb{Q}$;

d) $\mathbb{Q}(\sqrt{2} + \sqrt{3}, \sqrt{2} + i, \sqrt{3} - i) \supset \mathbb{Q}$.

4.6 Навести приклад таких елементів a, b, алгебраїчних над $\mathbb{Q}$, що $\mathbb{Q}(a,b) \neq \mathbb{Q}(a+b)$. Вкажіть таке d, що $\mathbb{Q}(a,b) = \mathbb{Q}(a+db)$.

4.7 Нехай K — поле, характеристика якого відмінна від 2, $L = K(x^2, y^2)$, $M = K(x,y)$. Довести, що знайдеться такий елемент $c \in M$, що $M = L(c)$.

4.8 Нехай $\mathrm{char}K = 2$, $L = K(x^2, y^2)$, $M = K(x,y)$. Довести, що не існує такого елемента $c \in M$, що $M = L(c)$.

4.9 Нехай p — просте число. Навести приклад поля характеристики p і скінченного розширення цього поля, для якого не існує примітивного елемента.

4.10 Довести, що розширення $\mathbb{Z}_p(x^p, y^p) \subset \mathbb{Z}_p(x,y)$ має нескінченно багато проміжних підполів.

5 Автоморфізми полів, основна теорема теорії Галуа

У цьому розділі всі розширення вважаються скінченними.

Означення 13. *Розширення $L \supset K$ називається розширенням Галуа, якщо це розширення є нормальним і сепарабельним.*

Для розширення $L \supset K$ позначимо

$$\mathrm{Aut}(L|K) = \{\varphi \in \mathrm{Aut}L : \ \varphi(x) = x \, \forall x \in K\}.$$

Очевидно, що $\mathrm{Aut}(L|K)$ є групою. У випадку, коли $L \supset K$ — розширення Галуа, ця група називається *групою Галуа* даного розширення.

Теорема 9. *Для розширення $L \supset K$ наступні умови еквівалентні.*

1. *$L \supset K$ є розширенням Галуа;*
2. *Для довільного елемента $a \in L \setminus K$ знайдеться такий автоморфізм $\sigma \in \mathrm{Aut}(L|K)$, що $\sigma(a) \neq a$;*
3. *$|\mathrm{Aut}(L|K)| = [L : K]$;*
4. *L є полем розкладу деякого сепарабельного над K многочлена.*

Зауважимо, що розширення поля характеристики 0 є розширенням Галуа тоді й лише тоді, коли воно є нормальним. Це випливає із теореми 9 і досконалості полів нульової характеристики.

Нехай $L \supset K$ — розширення Галуа з групою Галуа $G = \mathrm{Aut}(L|K)$. Для підмножини $X \subset G$ позначимо

$$L^X = \{l \in L : \varphi(l) = l \, \forall \varphi \in X\}.$$

Зрозуміло, що L^X є полем, причому $L \supset L^X \supset K$, це поле називається *полем нерухомих точок* множини автоморфізмів X.

Нехай тепер $L \supset Y \supset K$, де Y — деяка множина (не обов'язково поле). Позначимо

$$G^Y = \{g \in G : \ g(y) = y \, \forall \, y \in Y\}.$$

Очевидно, G^Y є підгрупою групи G. У випадку, коли Y є підполем L, розширення $L \supset Y$ є розширенням Галуа, а група G^Y збігається із групою $\mathrm{Aut}(L|Y)$.

Наступна теорема відома як *основна теорема теорії Галуа* (або скорочено *ОТТГ*).

Теорема 10. *Нехай $L \supset K$ — розширення Галуа з групою Галуа G. Позначимо через $\mathcal{A}$ множину підгруп групи G, через $\mathcal{B}$ — множину підполів L, що містять K. Визначимо відображення $\varphi : \mathcal{A} \to \mathcal{B}$ і $\psi : \mathcal{B} \to \mathcal{A}$ правилами:*

$$\varphi(H) = L^H \ \forall\, H \in \mathcal{A}, \quad \psi(P) = G^P \ \forall\, P \in \mathcal{B}.$$

Тоді φ і ψ є взаємно оберненими бієкціями, що обертають включення, тобто:

1) $\varphi(\psi(P)) = L^{G^P} = P$ для всіх $P \in \mathcal{B}$;

2) $\psi(\varphi(H)) = G^{L^H} = H$ для всіх $H \in \mathcal{A}$;

3) $P_1 \supset P_2$ тоді й лише тоді, коли $G^{P_1} \subset G^{P_2}\ \forall\, P_1, P_2 \in \mathcal{B}$;

4) $H_1 \supset H_2$ тоді й лише тоді, коли $L^{H_1} \subset L^{H_2}\ \forall\, H_1, H_2 \in \mathcal{A}$.

Нехай $L \supset K$ — розширення Галуа з групою Галуа G і H — підгрупа G. Тоді розширення $L \supset L^H$ буде розширенням Галуа, причому $[L : L^H] = |H|$. Розширення $L^H \supset K$ буде, очевидно, сепарабельним, але взагалі кажучи, не буде нормальним. Наступну теорему часто називають *критерієм нормальності*.

Теорема 11. *$L^H \supset K$ є нормальним тоді й лише тоді, коли H є нормальною підгрупою в G. У випадку, коли $H \lhd G$, групи $\mathrm{Aut}(L^H | K)$ і G/H ізоморфні, причому будь-який автоморфізм із $\mathrm{Aut}(L^H | K)$ є обмеженням на L^H деякого автоморфізму із G.*

Приклади розв'язування задач

Приклад 31. *Нехай $L \supset K$ — розширення і $f(x) \in K[x]$ — многочлен, про який відомо, що його корінь a лежить в L. Довести, що $\sigma(a)$ є коренем $f(x)$ для довільного $\sigma \in \mathrm{Aut}(L|K)$.*

Нехай $f(x) = a_0x^n + \cdots + a_n$. Візьмемо $\sigma \in \mathrm{Aut}(L|K)$. Подіємо на ліву і праву частини рівності $0 = a_0a^n + \cdots + a_n$ автоморфізмом σ. Отримаємо:

$$0 = \sigma(0) = \sigma(a_0a^n + \cdots + a_{n-1}a + a_n) =$$
$$\sigma(a_0)\sigma(a^n) + \cdots + \sigma(a_{n-1})\sigma(a) + \sigma(a_n) = a_0\sigma(a)^n + \cdots + a_{n-1}\sigma(a) + a_n.$$

Це означає, що $\sigma(a)$ також є коренем $f(x)$.

Приклад 32. *Нехай L — поле розкладу многочлена $x^m - 1$ над $\mathbb{Q}$. Довести, що $L \supset \mathbb{Q}$ — розширення Галуа і $\mathrm{Aut}(L|\,\mathbb{Q}) \simeq \mathbb{Z}_m^*$.*

Позначимо через θ — первісний корінь степеня m з одиниці. Коренями многочлена $x^m - 1$ є θ^k при $0 \le k \le m-1$. Тому поле розкладу даного многочлена над $\mathbb{Q}$ збігається з $\mathbb{Q}(\theta)$, що тягне нормальність розширення.

Таким чином, $L \supset \mathbb{Q}$ — розширення Галуа. Тепер використаємо той факт, що мінімальний многочлен для θ над $\mathbb{Q}$ має степінь $\varphi(m)$ (див. розв'язання прикладу 15). Тому $[L : \mathbb{Q}] = \varphi(m)$, що тягне рівність $|\mathrm{Aut}(L|\,\mathbb{Q})| = \varphi(m)$.

Нехай $\sigma \in \mathrm{Aut}(L|\,\mathbb{Q})$. Внаслідок попереднього прикладу $(\sigma(\theta))^m = 1$. Покажемо, що $\sigma(\theta)$ — первісний корінь степеня m з одиниці. Припустимо, що $(\sigma(\theta))^d = 1$ для певного $d < m$. Тоді

$$\theta^d = (\sigma^{-1}(\sigma(\theta))^d = \sigma^{-1}(\sigma(\theta)^d) = \sigma^{-1}(1) = 1,$$

всупереч тому, що θ — первісний. Отже, під дією σ елемент θ може переходити лише в θ^k, де $(k, m) = 1$. З іншого боку, із теореми 4 про будову простих алгебраїчних розширень випливає, що $1, \theta, \ldots, \theta^{\varphi(m)-1}$ — базис L над $\mathbb{Q}$. Тому для $\sigma \in \mathrm{Aut}(L|\,\mathbb{Q})$ значення $\sigma(x)$ для всіх $x \in L$ визначаються значенням $\sigma(\theta)$. Із сказаного, враховуючи, що $|\mathrm{Aut}(L|\,\mathbb{Q})| = \varphi(m)$, випливає, що

$$\mathrm{Aut}(L|\,\mathbb{Q}) = \{\sigma_k : 1 \le k \le m, (k, m) = 1, \text{ де } \sigma_k(\theta) = \theta^k\}.$$

Визначимо бієкцію $\tau : \mathrm{Aut}(L|\,\mathbb{Q}) \to \mathbb{Z}_m^*$ правилом: $\sigma_k \mapsto k$. Нехай $t, s \in \mathbb{Z}_m^*$. Тоді

$$\sigma_{ts}(\theta^i) = \theta^{its} = (\theta^{ti})^s = \sigma_s(\sigma_t(\theta^i)),$$

$0 \le i \le m-1$. Звідси випливає, що $\sigma_{ts}(x) = \sigma_s(\sigma_t(x))$ для всіх $x \in L$. Таким чином, τ — ізоморфізм, отже, $\mathrm{Aut}(L|\,\mathbb{Q}) \simeq \mathbb{Z}_m^*$.

Приклад 33. *Визначити всі автоморфізми поля розкладу многочлена $f(x) = x^4 - 2 \in \mathbb{Q}[x]$.*

Нехай L — поле розкладу $f(x)$. Оскільки поле $\mathbb{Q}$ не має автоморфізмів, відмінних від тотожного (див. приклад 5), то група G автоморфізмів поля L збігається із $\mathrm{Aut}(L|\,\mathbb{Q})$. Позаяк над полем характеристики 0 будь-який многочлен є сепарабельним (див задачу 4.1), то $L \supset \mathbb{Q}$ є розширенням Галуа.

За теоремою 9 $|G| = [L : \mathbb{Q}]$. Для того, щоб обчислити $[L : \mathbb{Q}]$, спочатку зауважимо, що $L = \mathbb{Q}(i, \sqrt[4]{2})$, після чого запишемо таку вежу розширень:

$$L \supset \mathbb{Q}(\sqrt[4]{2}) \supset \mathbb{Q}.$$

Розширення $L = (\mathbb{Q}(\sqrt[4]{2}))(i) \supset \mathbb{Q}(\sqrt[4]{2})$ є простим алгебраїчним, тому його степінь дорівнює степеню мінімального многочлена x^2+1 елемента i, звідки $[L : \mathbb{Q}(\sqrt[4]{2})]=2$. Базисом L над $\mathbb{Q}(\sqrt[4]{2})$ є, наприклад $\{1, i\}$.

Аналогічно, $[\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}]$ дорівнює степеню мінімального многочлена для $\sqrt[4]{2}$ над $\mathbb{Q}$. Оскільки цим многочленом є $x^4 - 2$, то $[\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] = 4$. Базисом $\mathbb{Q}(\sqrt[4]{2})$ над $\mathbb{Q}$ є $\{1, \sqrt[4]{2}, \sqrt[4]{4}, \sqrt[4]{8}\}$ (будова базиса простого алгебраїчного розширення описана в теоремі 26).

За теоремою про вежу розширень

$$|G| = [L : \mathbb{Q}] = [L : \mathbb{Q}(\sqrt[4]{2})][\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] = 2 \cdot 4 = 8.$$

Згідно з пуктом 3 теореми 2 множина $\{1, \sqrt[4]{2}, \sqrt[4]{4}, \sqrt[4]{8}, i, i\sqrt[4]{2}, i\sqrt[4]{4}, i\sqrt[4]{8}\}$ є базисом L над $\mathbb{Q}$.

Нехай $\sigma \in \mathrm{Aut}(L|\,\mathbb{Q})$. Оскільки $\sqrt[4]{2}$ — корінь многочлена $x^4-2 \in \mathbb{Q}[x]$, то за прикладом 31 $\sigma(\sqrt[4]{2})$ також є коренем цього є многочлена. Тому $\sigma(\sqrt[4]{2})$ мусить бути одним із чисел $\sqrt[4]{2}, i\sqrt[4]{2}, -\sqrt[4]{2}, -i\sqrt[4]{2}$. Аналогічно, оскільки i — корінь многочлена $x^2+1 \in \mathbb{Q}[x]$, то $\sigma(i)$ мусить збігатися з i або з $-i$. Із вигляду базису L над $\mathbb{Q}$ випливає, що значеннями $\sigma(\sqrt[4]{2})$ і $\sigma(i)$ однозначно визначаються значення σ на усіх базисних елементах, а отже, і значення σ на всіх елементах із L. Таким чином, група $\mathrm{Aut}(L|\mathbb{Q})$ налічує не більше $4 \cdot 2 = 8$ автоморфізмів. Напочатку розв'язання було встановлено, що $|\mathrm{Aut}(L|\mathbb{Q})| = 8$. Тому будь-яке відображення σ, для якого $\sigma(\sqrt[4]{2})$ — це один з елементів $\sqrt[4]{2}, i\sqrt[4]{2}, -\sqrt[4]{2}, -i\sqrt[4]{2}$ і $\sigma(i)$ — один з елементів $i, -i$, однозначно продовжується до $\sigma \in \mathrm{Aut}(L|\,\mathbb{Q})$.

Всі елементи із $\mathrm{Aut}(L|\,\mathbb{Q})$ наведено у наступній таблиці.

	σ_1	σ_2	σ_3	σ_4	σ_5	σ_6	σ_7	σ_8
i	i	i	i	i	$-i$	$-i$	$-i$	$-i$
$\sqrt[4]{2}$	$\sqrt[4]{2}$	$i\sqrt[4]{2}$	$-\sqrt[4]{2}$	$-i\sqrt[4]{2}$	$\sqrt[4]{2}$	$i\sqrt[4]{2}$	$-\sqrt[4]{2}$	$-i\sqrt[4]{2}$

Приклад 34. *Визначити всі підгрупи групи автоморфізмів поля* $\mathbb{Q}(\sqrt{2}, \sqrt{3})$. *Для кожної із підгруп визначити поле нерухомих точок.*

Нехай $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Очевидно, L є полем розкладу многочлена $(x^2 - 2)(x^2 - 3) \in \mathbb{Q}[x]$. Тому $L \supset \mathbb{Q}$ — розширення Галуа. Крім цього $\mathrm{Aut}L = \mathrm{Aut}(L|\,\mathbb{Q})$ (працюють ті самі аргументи, що і у попередньому прикладі).

Оскільки

$$\mathbb{Q}(\sqrt{2},\sqrt{3}) \supset \mathbb{Q}(\sqrt{3}) \supset \mathbb{Q}$$

і на кожному етапі степінь розширення дорівнює 2, то $[L : \mathbb{Q}] = 4$. Враховуючи, що $\{1, \sqrt{2}\}$ — базис L над $\mathbb{Q}(\sqrt{3})$ і $\{1, \sqrt{3}\}$ — базис $\mathbb{Q}(\sqrt{3})$ над $\mathbb{Q}$, отримуємо що базисом L над $\mathbb{Q}$ є множина $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$. Із пункта 3 теореми 9 випливає, що $|\mathrm{Aut}(L|\,\mathbb{Q})| = 4$. Якщо $\sigma \in \mathrm{Aut}(L|\,\mathbb{Q})$, то σ однозначно визначається значеннями $\sigma(\sqrt{2})$ і $\sigma(\sqrt{3})$, але $\sigma(\sqrt{2})$ може дорівнювати лише $\sqrt{2}$ або $-\sqrt{2}$, а $\sigma(\sqrt{3})$ може дорівнювати лише $\sqrt{3}$ або $-\sqrt{3}$ (див. приклад 31). Оскільки група $\mathrm{Aut}(L|\,\mathbb{Q})$ налічує рівно 4 елементи, то будь-яке відображення σ, визначене на $\sqrt{2}$ і $\sqrt{3}$, так, що $\sigma(\sqrt{2})$ — корінь $x^2 - 2$, $\sigma(\sqrt{3})$ — корінь $x^2 - 3$, продовжується до автоморфізма із $\mathrm{Aut}(L|\,\mathbb{Q})$.

Наведемо всі елементи із $\mathrm{Aut}(L|\,\mathbb{Q})$ у наступній таблиці.

	σ_1	σ_2	σ_3	σ_4
1	1	1	1	1
$\sqrt{2}$	$\sqrt{2}$	$\sqrt{2}$	$-\sqrt{2}$	$-\sqrt{2}$
$\sqrt{3}$	$\sqrt{3}$	$-\sqrt{3}$	$\sqrt{3}$	$-\sqrt{3}$
$\sqrt{6}$	$\sqrt{6}$	$-\sqrt{6}$	$-\sqrt{6}$	$\sqrt{6}$

Із таблиці бачимо, що всі автоморфізми, крім тотожного, мають другий порядок. Це означає, що $\mathrm{Aut}(L|\,\mathbb{Q}) \simeq C_2 \times C_2$, де C_2 — циклічна група другого порядку. Тому $\mathrm{Aut}(L|\,\mathbb{Q})$ має рівно 5 підгруп, серед яких дві невласні: $G = \mathrm{Aut}(L|\,\mathbb{Q})$ і $G_1 = \{\sigma_1\}$ і три підгрупи другого порядку: $G_2 = \{\sigma_2, \sigma_1\}$, $G_3 = \{\sigma_3, \sigma_1\}$, $G_4 = \{\sigma_4, \sigma_1\}$.

Перейдемо до визначення полів нерухомих точок для кожної із підгруп. Оскільки $G = \mathrm{Aut}(L|\,\mathbb{Q})$ — найбільша за включенням підгрупа у $\mathrm{Aut}(L|\,\mathbb{Q})$, то за ОТТГ їй відповідає найменше за включенням проміжне підполе — поле $\mathbb{Q}$. Аналогічно, оскільки $\{\sigma_1\}$ — найменша за включенням підгрупа, то їй відповідає найбільше за включенням проміжне підполе — поле L.

Розглянемо підгрупу $G_2 = \{\sigma_2, \sigma_1\}$. За ОТТГ цій підгрупі відповідає проміжне поле

$$L^{G_2} = \{x \in L :\ \sigma_1(x) = x \text{ і } \sigma_2(x) = x\} = \{x \in L :\ \sigma_2(x) = x\}$$

(оскільки σ_1 — тотожний автоморфізм, то $\sigma_1(x) = x$ для всіх $x \in L$, тому система рівностей $\sigma_1(x) = x$ і $\sigma_2(x) = x$ рівносильна одній рівності $\sigma_2(x) = x$).

Нехай x — довільний елемент поля L. Подамо його у вигляді лінійної комбінації базисних елементів: $x = x_1 + x_2\sqrt{2} + x_3\sqrt{3} + x_4\sqrt{6}$, $x_1, x_2, x_3, x_4 \in \mathbb{Q}$. Якщо $x \in L^{G_2}$, то $\sigma_2(x) = x$, тобто

$$x_1 + x_2\sqrt{2} - x_3\sqrt{3} - x_4\sqrt{6} = \sigma_2(x) = x = x_1 + x_2\sqrt{2} + x_3\sqrt{3} + x_4\sqrt{6}.$$

Прирівнюючи коефіцієнти при однакових базисних елементах, отримуємо: $x_1 = x_1$, $x_2 = x_2$, $x_3 = x_4 = 0$. Отже, $x = x_1 + x_2\sqrt{2}$. Тому $L^{G_2} \subset \mathbb{Q}(\sqrt{2})$.

Оскільки $\sigma_2(\sqrt{2}) = \sqrt{2}$, то $\sigma_2(x) = x$ для всіх $x \in \mathbb{Q}(\sqrt{2})$, звідки $L^{G_2} \supset \mathbb{Q}(\sqrt{2})$. Таким чином $L^{G_2} = \mathbb{Q}(\sqrt{2})$.

Аналогічно встановлюється, що $L^{G_3} = \mathbb{Q}(\sqrt{3})$ і $L^{G_4} = \mathbb{Q}(\sqrt{6})$.

Приклад 35. *Навести приклад числового поля L, група автоморфізмів якого була б ізоморфна циклічній групі порядку* 5.

Розглянемо многочлен $f(x) = x^{11} - 1 \in \mathbb{Q}[x]$. Позначимо $L = \mathbb{Q}(\theta)$, де $\theta = \cos\frac{2\pi}{11} + i\sin\frac{2\pi}{11}$ — первісний корінь степеня 11 з 1, поле розкладу цього многочлена. Із прикладу 32 випливає, що $\mathrm{Aut}(L|\,\mathbb{Q}) \simeq \mathbb{Z}_{11}^*$. Група $\mathbb{Z}_{11}^*$ циклічна як мультиплікативна група скінченного поля і має порядок $\varphi(11) = 10$. Автоморфізм σ_2, визначений правилом $\theta \mapsto \theta^2$ має у групі $\mathrm{Aut}(L|\,\mathbb{Q})$ порядок 10, звідки $\mathrm{Aut}(L|\,\mathbb{Q}) = \{\sigma_2, \sigma_2^2, \ldots, \sigma_2^{10} = e\}$, де через e позначено тотожний автоморфізм поля L.

Розглянемо підгрупу $H = \{\sigma_2^5, e\}$. Для проміжного поля L^H маємо: $[L : L^H] = |H| = 2$, а тому $[L^H : \mathbb{Q}] = 5$. Оскільки $H \lhd G$, то $L^H \supset \mathbb{Q}$ — розширення Галуа і $\mathrm{Aut}(L^H|\,\mathbb{Q}) \simeq G/H \simeq C_5$ за критерієм нормальності (теорема 11).

Визначимо, які елементи із L належать до L^H. За означенням,

$$L^H = \{x \in L : \sigma_2^5(x) = x \text{ і } e(x) = x\} = \{x \in L : \sigma_2^5(x) = x\}.$$

Внаслідок теореми 4 про будову простих алгебраїчних розширень множина $\{1, \theta, \ldots, \theta^9\}$ є базисом L над $\mathbb{Q}$. Крім цього, оскільки $x^{11} - 1 = (x-1)g(x)$, де $g(x) = x^{10} + \cdots + 1$ — мінімальний многочлен для θ, то $\theta^{-1} = \theta^{10} = -(1 + \theta + \cdots + \theta^9)$.

Нехай $x = \sum_{i=0}^{9} x_i\theta^i \in L^H$. Це є еквівалентним тому, що $x = \sigma_2^5(x)$. Оскільки

$$\sigma_2^5(\theta) = (\sigma_2(\theta))^5 = \theta^{10} = \theta^{-1},$$

то

$$\sigma_2^5(x) = \sum_{i=0}^{9} x_i\theta^{-i} = \sum_{i=0}^{9} x_i\theta^{11-i} =$$
$$x_0 + x_1(-1-\theta-\cdots-\theta^9) + x_2\theta^9 + x_3\theta^8 + \cdots + x_9\theta^2 =$$
$$(x_0 - x_1) - x_1\theta + (x_9 - x_1)\theta^2 + \cdots + (x_2 - x_1)\theta^9.$$

Прирівняємо коефіцієнти при однакових базисних векторах елементів x і $\sigma_2^5(x)$. Отримуємо: $x_0 = x_0$, $x_1 = 0$, $x_2 = x_9$, $x_3 = x_8$, $x_4 = x_7$, $x_5 = x_6$.

Таким чином, $x \in L^H$ тоді й лише тоді, коли

$$x = x_0 + x_2(\theta^2 + \theta^{-2}) + x_3(\theta^3 + \theta^{-3}) + x_4(\theta^4 + \theta^{-4}) + x_5(\theta^5 + \theta^{-5}).$$

Легко бачити, що $\theta^2 + \theta^{-2} = (\theta + \theta^{-1})^2 - 2 \in \mathbb{Q}(\theta + \theta^{-1})$. Аналогічно встановлюється, що $\theta^3 + \theta^{-3}$, $\theta^4 + \theta^{-4}$, $\theta^5 + \theta^{-5} \in \mathbb{Q}(\theta + \theta^{-1})$. Тому $L^H \subset \mathbb{Q}(\theta + \theta^{-1})$.

Далі, оскільки $\sigma_2^5(\theta + \theta^{-1}) = \theta^{10} + \theta^{-10} = \theta^{-1} + \theta$, то $\theta + \theta^{-1} \in L^H$, звідки $L^H \supset \mathbb{Q}(\theta + \theta^{-1})$. Таким чином, $L^H = \mathbb{Q}(\theta + \theta^{-1}) = \mathbb{Q}(\cos\frac{2\pi}{11})$.

Отже, розширення $\mathbb{Q}(\cos\frac{2\pi}{11}) \supset \mathbb{Q}$ є розширенням Галуа, причому $\mathrm{Aut}(\mathbb{Q}(\cos\frac{2\pi}{11})|\,\mathbb{Q}) = \mathrm{Aut}(\mathbb{Q}(\cos\frac{2\pi}{11})) \simeq C_5$.

Приклад 36. *Довести, що існує рівно один автоморфізм f поля $K(x)$, сталий на K, при якому $x \mapsto \frac{1}{x}$. Визначити поле нерухомих точок цього автоморфізма.*

Безпосередня перевірка показує, що відображення $\tau : K(x) \to K(x)$, визначене правилом $f(x) \mapsto f(\frac{1}{x})$ є автоморфізмом поля $K(x)$. Якщо ψ — автоморфізм $K(x)$, такий, що $\psi(x) = \frac{1}{x}$, то тоді $\psi(x^n) = \left(\frac{1}{x}\right)^n$ для всіх $n \geq 0$. Але тоді $\psi(f(x)) = \tau(f(x))$ для довільної раціональної функції $f(x) \in K(x)$.

Нехай $L \subset K(x)$ — поле нерухомих точок τ. Оскільки $\tau(x - \frac{1}{x}) = -\frac{1}{x} + x$, то $x - \frac{1}{x} \in L$. Тому $K\left(x - \frac{1}{x}\right) \subset L$. З іншого боку, $L \neq K(x)$, позаяк, наприклад, $x \notin L$. Але $\left[K(x) : K\left(x - \frac{1}{x}\right)\right] = 2$ (див. задачу 2.25b)). Оскільки, крім цього,

$$K\left(x - \frac{1}{x}\right) \subset L \subset K(x),$$

то $L = K\left(x - \frac{1}{x}\right)$.

Приклад 37. *Проілюструвати основну теорему теорії Галуа на прикладі розширення* $\mathbb{Q}\left(x^2+\frac{1}{x^2}\right) \subset \mathbb{Q}(x)$.

Спочатку покажемо, що дане розширення є розширенням Галуа. Оскільки характеристика полів нульова, досить довести нормальність.

Розглянемо $f(t) = t^4 - t^2(x^2+\frac{1}{x^2}) + 1 \in \left(\mathbb{Q}\left(x^2+\frac{1}{x^2}\right)\right)[t]$. Коренями цього многочлена є $x, -x, \frac{1}{x}, -\frac{1}{x}$. Тому $\mathbb{Q}(x)$ є полем розкладу $f(t)$, що тягне нормальність нашого розширення.

Покладемо $G = \mathrm{Aut}\left(\mathbb{Q}(x)|\mathbb{Q}\left(x^2+\frac{1}{x^2}\right)\right)$. Оскільки $f(t)$ анулює x, то $[\mathbb{Q}(x) : \mathbb{Q}\left(x^2+\frac{1}{x^2}\right)] \leq \deg f(t) = 4$. З іншого боку, оскільки

$$\mathbb{Q}\left(x^2+\frac{1}{x^2}\right) \subset \mathbb{Q}\left(x+\frac{1}{x}\right) \subset \mathbb{Q}(x),$$

причому обидва включення строгі, то $[\mathbb{Q}(x) : \mathbb{Q}\left(x^2+\frac{1}{x^2}\right)] \geq 4$. Таким чином, $|G| = 4$.

Легко бачити, що відображення $\sigma_1, \sigma_2, \sigma_3, \sigma_4$, де $\sigma_1(f(x)) = f(x)$, $\sigma_2(f(x)) = f(-x)$, $\sigma_3(f(x)) = f(\frac{1}{x})$, $\sigma_4(f(x)) = f(-\frac{1}{x})$, $f(x) \in \mathbb{Q}(x)$, є автоморфізмами $\mathbb{Q}(x)$, тотожними на $\mathbb{Q}\left(x^2+\frac{1}{x^2}\right)$, тому належать до G. Отримуємо, що $G = \{\sigma_1, \sigma_2, \sigma_3, \sigma_4\}$. Оскільки $\sigma_2, \sigma_3, \sigma_4$ мають другий порядкок, а σ_1 є тотожним автоморфізмом, то $G \simeq C_2 \times C_2$.

Група G має 5 підгруп: $H_0 = G$, $H_1 = \{\sigma_1\}$ і три двоелементні підгрупи $H_2 = \{\sigma_1, \sigma_2\}$, $H_3 = \{\sigma_1, \sigma_3\}$, $H_4 = \{\sigma_1, \sigma_4\}$. Позначимо через $L_i = (\mathbb{Q}(x))^{H_i}$, $0 \leq i \leq 4$, відповідне проміжне підполе.

За ОТТГ $L_0 = \mathbb{Q}\left(x^2+\frac{1}{x^2}\right)$, $L_1 = \mathbb{Q}(x)$. Далі,

$$L_2 = \{g \in \mathbb{Q}(x) : g(-x) = g(x)\} = \mathbb{Q}(x^2);$$

$$L_3 = \{g \in \mathbb{Q}(x) : g\left(\frac{1}{x}\right) = g(x)\} = \mathbb{Q}\left(x+\frac{1}{x}\right);$$

$$L_4 = \{g \in \mathbb{Q}(x) : g\left(-\frac{1}{x}\right) = g(x)\} = \mathbb{Q}\left(x-\frac{1}{x}\right).$$

Пояснимо, наприклад, останню рівність. Оскільки $x - \frac{1}{x}$ не змінюється при підстановці $-\frac{1}{x}$ замість x, то $\mathbb{Q}\left(x-\frac{1}{x}\right) \subset L_4$. Із ОТТГ випливає, що $[\mathbb{Q}(x) : L_4] = |H_4| = 2$. Але з іншого, боку, $[\mathbb{Q}(x) : \mathbb{Q}\left(x-\frac{1}{x}\right)] = 2$, звідки $L_4 = \mathbb{Q}\left(x-\frac{1}{x}\right)$.

Задачі

5.1 Знайти всі автоморфізми поля

a) $\mathbb{Q}(\sqrt{2})$; b) $\mathbb{Q}(\sqrt[3]{2})$; c)$\mathbb{Q}(\sqrt[4]{2})$; d) $\mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{5})$.

5.2 Довести, що поле дійсних чисел не є розширенням Галуа жодного власного підполя.

5.3 Визначити поле нерухомих точок групи автоморфізмів поля

a) $\mathbb{Q}(\sqrt{2})$; b) $\mathbb{Q}(\sqrt[4]{2})$.

5.4 Визначити всі підгрупи групи автоморфізмів поля $\mathbb{Q}(\sqrt[3]{2},\varepsilon)$, де $\varepsilon = \frac{-1+i\sqrt{3}}{2}$. Для кожної із підгруп вказати поле нерухомих точок.

5.5 Проілюструвати основну теорему теорії Галуа на прикладі розширення $L \supset \mathbb{Q}$, де L — поле розкладу многочлена

a) x^4+x^2-6; b)x^3-3; c)x^4-5.

5.6 Навести приклад такого числового поля L, група автоморфізмів якого була б ізоморфна

a) циклічній групі порядку 2;

b) циклічній групі порядку 4;

c) четверній групі Кляйна;

d) циклічній групі порядку 6;

e) нециклічній групі порядку 6;

f) циклічній групі порядку 3;

5.7 Довести що група Галуа розширення $\mathbb{Q}(\varepsilon_p) \supset \mathbb{Q}$, де ε_p є первісним коренем степеня p з 1, p — просте, є циклічною.

5.8 Знайти групу Галуа розширення $\mathbb{Q}(\varepsilon_m) \supset \mathbb{Q}$, де ε_m є первісним коренем з одиниці степеня

a) 12; b) 15; c) 16.

5.9 Нехай ε_m — первісний корінь з одиниці степеня m. Проілюструвати основну теорему теорії Галуа на прикладі розширення $\mathbb{Q}(\varepsilon_m) \supset \mathbb{Q}$ для

a) $m=5$; b) $m=7$; c) $m=9$.

5.10 Довести, що група Галуа поля розкладу многочлена $x^m - a \in \mathbb{Q}[x]$ над $\mathbb{Q}$ ізоморфна групі T_m матриць вигляду $\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$, де $a \in \mathbb{Z}_m^*$, $b \in \mathbb{Z}_m$ (групова операція — звичайне множення матриць).

5.11 Довести, що існує рівно один автоморфізм f поля $K(x)$ при якому

a) $x \mapsto x$; b) $x \mapsto -x$; c) $x \mapsto -\frac{1}{x}$.

Визначити поле нерухомих точок зазначеного автоморфізма.

5.12 Довести, що існує рівно один автоморфізм f поля $K(x, y)$ при якому

a) $x \mapsto x$, $y \mapsto y$; b) $x \mapsto -x$ $y \mapsto y$; c) $x \mapsto -x$, $y \mapsto -y$.

Визначити поле нерухомих точок зазначеного автоморфізма.

5.13 Проілюструвати основну теорему теорії Галуа на прикладі наступного розширення $K(x^2, y^2) \subset K(x, y)$.

5.14 Довести, що для кожного многочлена $ax + b \in \mathbb{Q}[x]$, $a \neq 0$, існує рівно один автоморфізм поля $\mathbb{Q}(x)$, при якому образом x є $ax + b$. Знайти поле нерухомих точок автоморфізма

a) $x \mapsto -x$; b) $x \mapsto 2x$; c) $x \mapsto x + 1$.

Визначити поле нерухомих точок для сукупності даних трьох автоморфізмів.

5.15 У кожному з випадків визначити групу $\mathrm{Aut}(\mathbb{Z}_3(x)|K)$ розширення $\mathbb{Z}_3(x) \supset K$ і встановити, чи є це розширення розширенням Галуа:

a) $K = \mathbb{Z}_3(x^2)$; b)$K = \mathbb{Z}_3(x^3)$; c)$K = Z_3(x^4)$.

5.16 Довести, що існує єдиний автоморфізм поля $\mathbb{Z}_3(x)$, при якому $x \mapsto x + 1$. Знайти поле нерухомих точок цього автоморфізма.

5.17 Проілюструвати основну теорему теорії Галуа на прикладі розширення $\mathbb{Z}_3(x^6 + x^4 + x^2) \subset \mathbb{Z}_3(x)$.

5.18 Нехай K є полем характеристики 2. Яке з наступних розширень є розширенням Галуа:

a) $K(x^2 + x) \subset K(x)$; b)$K(x^2 + x) \subset K(x)$

5.19 Довести, що довільне розширення $K \subset L$, де поля K і L скінченні, є розширенням Галуа і група Галуа цього розширення є циклічною.

Література

[1] M. Bryński, J. Jurkiewicz *Zbiór zadań z algebry.* Warszawa: PWN, 1981.

[2] J. Rutkowski *Algebra abstrakcyjna w zadaniach.* Warszawa: PWN, 2000.

[3] *Сборник задач по алгебре* под редакцией А.И.Кострикина. М.: Физматлит, 2001.

[4] Г.М. Кудрявцева, А.С. Олійник *Кільця. Приклади і задачі.* К.: ВПЦ Київський університет, 2005.

[5] О.О.Безущак, О.Г.Ганюшкін *Елементи теорії чисел.* К.: ВПЦ Київський університет, 2003.

[6] О.Г.Ганюшкін, О.О.Безущак *Завдання до практичних занять з алгебри і теорії чисел (теорія груп).* К.: ВПЦ Київський університет, 2004.

[7] О.Г.Ганюшкін, О.О.Безущак *Теорія груп.* К.: ВПЦ Київський університет, 2005.

[8] Ю.А. Дрозд *Теорія Галуа.* К.: ВПЦ Київський університет, 1997.

[9] А.И.Кострикин *Введение в алгебру.* М.: Наука , 1977.

[10] Е.Артін *Теорія Галуа.* К.: Радянська школа, 1963.

[11] М.М. Постников *Теория Галуа.* М.: Физматгиз, 1963.

[12] Б.Л. ван дер Варден *Алгебра.* М.: Наука, 1976.

[13] С. Ленг *Алгебра.* М.: Мир, 1968

[14] Р. Лидл, Г. Нидеррайтер *Конечные поля.* Т. 1,2, М.: Мир, 1988.