Київський університет імені Тараса Шевченка

Ю.А.ДРОЗД

ТЕОРІЯ ГАЛУА

Навчальний посібник
для студентів механіко-математичного факультету

Київ
Редакційно-видавничий центр
"Київський університет"
1997

УДК 512.4
Дрозд Ю.А. Теорія Галуа: Навчальний посібник для студентів механіко-математичного факультету. – К.: РВЦ "Київський університет", 1997. – 35 с.

На грунті теорем про гомоморфізми полів викладено основи теорії Галуа, включаючи критерії розв' язності рівнянь у радикалах.

Розраховано на студентів спеціальності "математика".

Рецензенти: В.В.Кириченко, д-р фіз.-мат. наук,
Я.П.Сисак, д-р фіз.-мат. наук

Затверджено Радою
механіко-математичного факультету
12 жовтня 1997 року

ISBN 966-594-022-8

Передмова

Теорія Галуа була одним із перших розділів сучасної алгебри і досі займає чільне місце в підготовці фахівців-математиків у всьому світі. Відповідні традиції існували і в радянських університетах; досить згадати класичний курс алгебри [**9**]. На жаль, з незрозумілих причин у повоєнні радянські часи теорія Галуа поступово зникла з університетських програм, що, звичайно, негативно вплинуло на рівень математичної освіти. Зараз становище починає виправлятися, але бракує сучасних підручників з цієї теорії (книга Сушкевича давно стала бібліографічною рідкістю, та й не зовсім відповідає нинішній математичній мові). Книги [**1**] та [**8**] також не є дуже розповсюдженими і не зовсім узгоджуються з університетськими програмами, а виклад теорії Галуа в таких книгах, як [**3**], [**4**] або [**7**], хоча й здійснений на високому рівні, дається зовсім в іншому науковому і методичному контексті.

Цей посібник має на меті закрити згадану прогалину і дати сучасний виклад терії Галуа, який ґрунтується на існуючій програмі алгебричних курсів університетів та педагогічних інститутів і органічно вписується у відповідну дидактичну систему. За основний підручник для посилань на "стандартні" факти із загального курсу обрано книгу [**6**], як найбільш уживану, хоча її можна з успіхом замінити, наприклад, на [**10**].

Автор намагався, по-перше, звести до розумного мінімуму базові принципи, на яких ґрунтується виклад, а по-друге, зробити його таким, що дозволяв би порівняно легко перейти до узагальнень. Тут у першу чергу малася на увазі теорія Галуа лінійних диференціальних рівнянь ("теорія Пікара-Вессіо" [**5**]), яка відіграє все більшу роль. Тому було обрано дві основні теореми, з яких подальша теорія розвивається більш-менш формально. Це – теорема про продовження (теорема 1.1), яка дозволяє будувати гомоморфізми (зокрема, автоморфізми) полів, та теорема про незалежність (теорема 1.2), яка обмежує їхню кількість. Сподіваюся, читач зможе переконатися, що, дійсно, все наступне виводиться з цих принципів порівняно логічно і нескладно. Звичайно, конкретні умови викладання можуть вимагати окремих спрощень чи скорочень. Наприклад, при розгляді теореми 4.8 можна обмежитись випадком кільця цілих чисел (який лише і використовується надалі) і т. ін.

У посібнику виклад доведено до детального розгляду задачі про розв'язування рівнянь у радикалах, включаючи загальний

критерій Галуа такої розв'язності, теорему Руффіні–Абеля про нерозв'язність "загального рівняння" ступеня $n > 4$ і приклади конкретних рівнянь, нерозв'язних у радикалах. Також (менш детально, оскільки це істотно простіше) розглянуто питання про розв'язування рівнянь (зокрема, рівнянь поділу кола) у квадратних радикалах. Зважаючи на велике значення цих питань для елементарної математики, треба визнати, що, наприклад, для підготовки *викладачів* математики будь-якого рівня їхній розгляд є цілком необхідним.

До посібника включено досить велику кількість вправ. Вони носять, переважно, не технічний характер, а спрямовані на вироблення у читача відповідної інтуїції та навичок доведень і досліджень у цій галузі. До вправ, які видавалися більш складними, додано вказівки, подекуди досить детальні. Читачу слід, по можливості, розв'язувати всі вправи у перебігу їхньої появи в тексті, тим більше, що результати деяких з них надалі використовуються в доведеннях.

1. Теореми про гомоморфізми полів

ТЕОРЕМА 1.1 (теорема про продовження). *Нехай* L *– розширення поля* K, φ *– гомоморфізм поля* K *в деяке поле* K'. *Тоді існує розширення* L' *поля* K' *і такий гомоморфізм* $\psi : \mathsf{L} \to \mathsf{L}'$, *що* $\psi(a) = \varphi(a)$ *для всіх* $a \in \mathsf{K}$.

Гомоморфізм ψ зветься *продовженням* φ на розширення L.

ДОВЕДЕННЯ. Ми обмежимось випадком, коли розширення L поля K є *скінченно-породженим*, тобто $\mathsf{L} = \mathsf{K}(\alpha_1, \alpha_2, \ldots, \alpha_n)$. Для нескінченно-породжених розширень доведення є цілком аналогічним, але потребує деякої теоретико-множинної техніки: або трансфінітної індукції, або леми Цорна, або ще якогось аналогічного твердження. У цих лекціях ми розглядатимемо лише скінченно-породжені розширення.

Отже, нехай $\mathsf{L} = \mathsf{K}(\alpha_1, \alpha_2, \ldots, \alpha_n)$. Доведення вестимо індукцією за кількістю породжуючих елементів n. Нехай спочатку $n = 1$, тобто $\mathsf{L} = \mathsf{K}(\alpha)$. Якщо елемент α є трансцендентним над K, то $\mathsf{L} \simeq \mathsf{K}(x)$ (полю раціональних дробів) і можна покласти $\mathsf{L}' = \mathsf{K}'(x)$ та

$$\psi\left(\frac{f(x)}{g(x)}\right) = \frac{(\varphi f)(x)}{(\varphi g)(x)}.$$

Тут і надалі для довільного многочлена $f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n$ ми позначаємо $(\varphi f)(x) = \varphi(a_0)x^n + \varphi(a_1)x^{n-1} + \cdots + \varphi(a_n)$.

Нехай тепер елемент α є алгебричним над K і $p(x)$ – його мінімальний многочлен. Тоді $\mathsf{L} \simeq \mathsf{K}[x]/(p(x))$ (див. [**6**, с.420]). Нехай $q(x)$ – якийсь незвідний множник многочлена $(\varphi p)(x)$ над полем K'. Розглянемо розширення L' поля K', в якому многочлен $q(x)$ має корінь β (див. [**6**, с.276]). Тоді визначено гомоморфізм $\mathsf{K}[x] \to \mathsf{L}'$, який переводить $f(x)$ в $(\varphi f)(\beta)$. Оскільки $(\varphi p)(\beta) = 0$, його ядро збігається з ідеалом $(p(x))$. Отже, ми одержуємо шуканий гомоморфізм $\mathsf{L} \to \mathsf{L}'$.

Обґрунтування "кроку індукції" залишаємо читачеві як вправу. □

ТЕОРЕМА 1.2 (теорема про незалежність). *Нехай* $\varphi_1, \varphi_2, \ldots, \varphi_n$ *– попарно різні гомоморфізми довільної групи* G *до мультиплікативної групи* K^* *деякого поля* K. *Тоді* $\varphi_1, \varphi_2, \ldots, \varphi_n$ *є лінійно незалежними як функції, себто, для довільних елементів* $c_1, c_2, \ldots, c_n$ *поля* K, *з яких принаймні один – ненульовий, знайдеться такий елемент* $g \in \mathsf{G}$, *для якого* $\sum_{i=1}^{n} c_i\varphi_i(g) \neq 0$.

ДОВЕДЕННЯ. Скористаємося індукцією за n. При $n = 1$ твердження тривіальне, оскільки $\varphi_1(g) \neq 0$. Припустимо, що теорема є вірною для довільних $n-1$ гомоморфізмів, але знайдуться такі елементи $c_1, c_2, \ldots, c_n \in \mathsf{K}$, принаймні один з яких ненульовий. що $\sum_{i=1}^{n} c_i\varphi_i(g) = 0$ для всіх $g \in \mathsf{G}$. Вважатимемо, що $c_1 \neq 0$. Оскільки $\varphi_1 \neq \varphi_n$, знайдеться елемент $h \in \mathsf{G}$, для якого $\varphi_1(h) \neq \varphi_n(h)$. Скористаємося рівностями:

$$\sum_{i=1}^{n} c_i\varphi_i(h)\varphi_i(g) = \sum_{i=1}^{n} \varphi_i(hg) = 0 \quad \text{для всіх } g \in \mathsf{G}$$

та

$$\sum_{i=1}^{n} c_i\varphi_n(h)\varphi_i(g) = \varphi_n(h)\sum_{i=1}^{n} \varphi_i(g) = 0\,.$$

Віднімаючи з першої рівності другу, одержуємо:

$$\sum_{i=1}^{n-1} c_i[\varphi_i(h) - \varphi_n(h)]\varphi_i(g) = 0 \quad \text{для всіх } g \in \mathsf{G},$$

що неможливо, за припущенням індукції, бо $c_1[\varphi_1(h) - \varphi_n(h)] \neq 0$. □

НАСЛІДОК 1.3. *Нехай* $\varphi_1, \varphi_2, \ldots, \varphi_n$ *– попарно різні гомоморфізми поля* L *у поле* M, $\mathsf{K} = \{\, a \in \mathsf{L} \mid \varphi_i(a) = \varphi_j(a)$ *для всіх* $i, j \,\}$. *Тоді* $[\mathsf{L} : \mathsf{K}] \geq n$.

ДОВЕДЕННЯ. Припустимо, що $[\mathsf{L} : \mathsf{K}] = m < n$ і $\{\theta_1, \theta_2 \ldots \theta_m\}$ – база L над K. Розглянемо в арифметичному лінійному просторі M^m вектори $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n$, де $\mathbf{v}_i = (\varphi_i(\theta_1), \varphi_i(\theta_2), \ldots, \varphi_i(\theta_m))$. Ці вектори лінійно залежні, оскільки $m < n$, . Отже, знайдуться такі елементи $c_1, c_2, \ldots, c_n \in \mathsf{M}$, не всі рівні нулю, що $\sum_{i=1}^{n} c_i\varphi_i(\theta_k) = 0$ для всіх номерів $k = 1, 2, \ldots, m$. Нехай γ – довільний елемент поля L. Розкладемо його за базою: $\gamma = \sum_{k=1}^{m} a_k\theta_k$, де $a_k \in \mathsf{K}$, і позначимо $b_k = \varphi_i(a_k)$ (за означенням підполя K це значення не залежить від номера i). Тоді

$$\sum_{i=1}^{n} c_i\varphi_i(\gamma) = \sum_{i=1}^{n} c_i \sum_{k=1}^{m} b_k\varphi_i(\theta_k) = \sum_{k=1}^{m} b_k \sum_{i=1}^{n} c_i\varphi_i(\theta_k) = 0\,.$$

Але це протирічить теоремі 1.2, оскільки $\varphi_1, \varphi_2, \ldots, \varphi_n$ є, зокрема, різними гомоморфізмами $\mathsf{L}^* \to \mathsf{M}^*$. □

НАСЛІДОК 1.4. *Нехай* L *– розширення поля* K, $\mathsf{Aut}\,(\mathsf{L}/\mathsf{K})$ *– множина таких автоморфізмів* σ *поля* L, *що* $\sigma(a) = a$ *для всіх* $a \in \mathsf{K}$. *Тоді* $|\mathsf{Aut}\,(\mathsf{L}/\mathsf{K})| \leq [\mathsf{L} : \mathsf{K}]$.

Очевидно, $\mathsf{Aut}\,(\mathsf{L}/\mathsf{K})$ є підгрупою в групі $\mathsf{Aut}\,\mathsf{L}$ всіх автоморфізмів поля L. Вона зветься *групою автоморфізмів розширення* L *поля* K.

Для довільної підгрупи $\mathsf{G} \subseteq \mathsf{Aut}\,\mathsf{L}$ позначимо

$$\mathsf{L}^{\mathsf{G}} = \{\, a \in \mathsf{L} \mid \sigma(a) = a \text{ для всіх } \sigma \in \mathsf{G} \,\}\,.$$

Підполе L^{G} зветься *полем інваріантів групи* G.

ТЕОРЕМА 1.5. $[\mathsf{L} : \mathsf{L}^{\mathsf{G}}] = |\mathsf{G}|$.

ДОВЕДЕННЯ. Позначимо $n = |\mathsf{G}|$, $\mathsf{K} = \mathsf{L}^{\mathsf{G}}$. За наслідком 1.4, $[\mathsf{L} : \mathsf{K}] \geq n$. Залишається перевірити, що коли $\theta_1, \theta_2, \ldots, \theta_m \in \mathsf{L}$ і $m > n$, то елементи $\theta_1, \theta_2, \ldots, \theta_m$ лінійно залежні над K.

Нехай $\mathsf{G} = \{\, \sigma_1, \sigma_2, \ldots, \sigma_n \,\}$. Розглянемо у просторі L^n вектори

$$\mathbf{v}_i = (\sigma_1^{-1}(\theta_i), \sigma_2^{-1}(\theta_i), \ldots, \sigma_n^{-1}(\theta_i)) \quad (i = 1, 2, \ldots, m)\,.$$

Вони лінійно залежні, тобто знайдуться елементи $c_1, c_2, \ldots, c_m \in \mathsf{L}$, не всі рівні нулю, такі що $\sum_{i=1}^{m} c_i\sigma_k^{-1}(\theta_i) = 0$ для всіх $k = 1, 2, \ldots, n$. Нехай, наприклад, $c_1 \neq 0$. Тоді, домножуючи останню рівність на елементи з поля L, можна зробити c_1 довільним елементом цього поля. Підберемо його так, щоб $\sum_{k=1}^{n} \sigma_k(c_1) \neq 0$ (це можна зробити за теоремою 1.2).Застосовуючи до рівності $\sum_{i=1}^{m} c_i\sigma_k^{-1}(\theta_i) = 0$ автоморфізм σ_k, одержимо $\sum_{i=1}^{m} \sigma_k(c_i)\theta_i = 0$. Беручи суму цих рівностей за всіма k, отримуємо співвідношення $\sum_{i=1}^{m} a_i\theta_i = 0$, де $a_i = \sum_{k=1}^{n} \sigma_k(c_i)$ (зокрема, $a_1 \neq 0$). Але легко перевірити, що тоді $\sigma(a_i) = a_i$ для всіх $\sigma \in \mathsf{G}$, тобто $a_i \in \mathsf{K}$ і елементи $\theta_1, \theta_2, \ldots, \theta_m$ дійсно є лінійно залежними над K. □

ВПРАВА 1.6. *Нехай* K *– скінченне поле з* q *елементами,* L *– його розширення ступеня* n*. Доведіть, що* $\mathrm{Aut}(\mathsf{L}/\mathsf{K})$ *– циклічна група порядку* n *з твірним* ϕ*, де* $\phi(\alpha) = \alpha^q$ *для всіх* $\alpha \in \mathsf{L}$ *("автоморфізм Фробеніуса").*

ВКАЗІВКИ: (i) Оскільки $q = l^m$, де $l = \mathrm{char}\,\mathsf{K}$ [**6**, с. 428], то ϕ – гомоморфізм. Завдяки скінченності L, він є тоді автоморфізмом, причому якщо $\alpha \in \mathsf{K}^*$, то $\alpha^{q-1} = 1$, звідки випливає, що $\phi \in \mathrm{Aut}(\mathsf{L}/\mathsf{K})$.

(ii) Оскільки $|\mathsf{L}| = q^n$, то $\phi^n = 1$. Навпаки, якщо $0 < k < n$, то $\phi^k \neq 1$, оскільки рівняння $x^{q^k} = x$ має щонайбільше q^k розв'язків.

(iii) Для завершення доведення залишається скористатися наслідком 1.4.

2. Сепарабельні та нормальні розширення

Незвідний многочлен $p(x) \in \mathsf{K}[x]$ зветься *сепарабельним*, якщо $p'(x) \neq 0$. Оскільки $\deg p'(x) < \deg p(x)$, звідси випливає, що тоді $(p, p') = 1$, отже, довільний корінь α многочлена $p(x)$ (у якомусь розширенні поля K) є простим. Навпаки, якщо $p(x)$ має простий корінь в якомусь розширенні поля K, то $p'(\alpha) \neq 0$, отже, многочлен $p(x)$ є сепарабельним.

Довільний многочлен $f(x) \in \mathsf{K}[x]$ зветься *сепарабельним*, якщо такими є всі його незвідні множники.

Алгебричний елемент α деякого розширення поля K зветься *сепарабельним*, якщо сепарабельним є його мінімальний многочлен (тобто α є його простим коренем). Очевидно, елемент є сепарабельним тоді і лише тоді, коли він є коренем якогось сепарабельного многочлена.

Алгебричне розширення, всі елементи якого сепарабельні, зветься *сепарабельним розширенням*.

ТЕОРЕМА 2.1 (теорема про сепарабельні розширення). *Нехай* L *– скінченне розширення поля* K *ступеня* n*. Наступні умови є еквівалентними:*

1. L *– сепарабельне розширення;*
2. $\mathsf{L} = \mathsf{K}(\alpha_1, \alpha_2, \ldots, \alpha_m)$*, де всі елементи* α_i *є сепарабельними.*
3. *Для довільного гомоморфізму* $\varphi : \mathsf{K} \to \mathsf{K}'$ *існує таке розширення* L' *поля* K'*, що* φ *має* n *різних продовжень до гомоморфізмів* $\mathsf{L} \to \mathsf{L}'$*.*

4. *Існує розширення* M *поля* K*, для якого знайдуться* n *різних гомоморфізмів* $\varphi_1, \varphi_2, \ldots, \varphi_n : \mathsf{L} \to \mathsf{M}$*, таких що* $\varphi_i(a) = a$ *для всіх номерів* i *та всіх елементів* $a \in \mathsf{K}$*.*

ДОВЕДЕННЯ. 1⇒2 тривіально.

3⇒4 одержимо, взявши за φ тотжне відображення $\mathsf{K} \to \mathsf{L}$.

4⇒1. Припустимо, що якийсь елемент $\alpha \in \mathsf{L}$ є несепарабельним над K. Позначимо $p(x)$ його мінімальний многочлен, $d = \deg p(x)$ і $\mathsf{P} = \mathsf{K}(\alpha)$. При довільному гомоморфізмі $\psi : \mathsf{P} \to \mathsf{M}$, який залишає на місці всі елементи з K, α переходить у корінь многочлена $p(x)$, причому знання $\psi(\alpha)$ повністю визначає ψ. Оскільки $p(x)$ має кратні корені, загальна кількість цих коренів, а тому й гомоморфізмів $\mathsf{P} \to \mathsf{M}$ менша від d. Але $[\mathsf{L} : \mathsf{P}] = [\mathsf{L} : \mathsf{K}]/[\mathsf{P} : \mathsf{K}] = n/d$. За наслідком 1.3 кожен гомоморфізм $\psi : \mathsf{P} \to \mathsf{M}$ має не більше за n/d продовжень до гомоморфізмів $\mathsf{L} \to \mathsf{M}$. Отже, всього одержуємо менш ніж $d \cdot n/d = n$ різних гомоморфізмів $\mathsf{L} \to \mathsf{M}$, що протирічить умові 3.

2⇒3 доведемо індукцією за m. Нехай спочатку $m = 1$, тобто $\mathsf{L} = \mathsf{K}(\alpha)$, де елемент α є сепарабельним. Позначимо $p(x)$ його мінімальний многочлен. Тоді $\deg p(x) = [\mathsf{L} : \mathsf{K}] = n$. Розглянемо многочлен $q(x) = (\varphi p)(x) \in \mathsf{K}[x]$. Нехай L' – його поле розкладу. Оскільки $(p, p') = 1$, то й $(q, q') = 1$, отже, $q(x)$ має в L' n різних коренів $\beta_1, \beta_2, \ldots, \beta_n$. Тоді так само, як у доведенні теореми 1.1, можна побудувати гомоморфізми $\varphi_i : \mathsf{L} \to \mathsf{L}'$, такі що $\varphi_i(\alpha) = \varphi(a)$ при $a \in \mathsf{K}$ і $\varphi_i(\alpha) = \beta_i$ при $i = 1, 2, \ldots, n$, що й треба.

Обгрунтування кроку індукції ми залишаємо читачеві як вправу. ВКАЗІВКА: Спочатку продовжіть φ на поле $\mathsf{P} = \mathsf{K}[\alpha_1, \alpha_2, \ldots, \alpha_{m-1}]$ і скористайтеся формулою $[\mathsf{L} : \mathsf{K}] = [\mathsf{L} : \mathsf{P}] = [\mathsf{P} : \mathsf{K}]$ [**6**, с. 421]. Перевірте, що α_m є сепарабельним над P. □

Поле K зветься *досконалим*, якщо всі незвідні многочлени над ним (або, що те саме, всі його алгебричні розширення) є сепарабельними.

ТЕОРЕМА 2.2. *Поле характеристики* 0 *завжди досконале. Поле* K *характеристики* $l > 0$ *є досконалим тоді і лише тоді, коли для довільного елемента* $a \in \mathsf{K}$ *знайдеться такий елемент* $b \in \mathsf{K}$*, що* $a = b^l$*.*

ДОВЕДЕННЯ. Твердження про поля характеристики 0 тривіальне. Нехай далі $\mathrm{char}\,\mathsf{K} = l > 0$. Очевидно, що $p'(x) = 0$ тоді і

лише тоді, коли $p(x)$ має вигляд:

$$p(x) = a_0x^{ml} + a_1x^{(m-1)l} + \cdots + a_{m-1}x^l + a_m\,.$$

Якщо $a_i = b_i^l$, де $b_i \in \mathsf{K}$, то $p(x) = q(x)^l$, де

$$q(x) = b_0x^m + b_1x^{m-1} + \cdots + b_{m-1}x + b_m \in \mathsf{K}[x]\,,$$

отже, $p(x)$ є звідним.

Навпаки, припустимо, що рівняння $x^l = a$ не має розв'язків у полі K. Доведемо, що тоді многочлен $x^l - a$ є незвідним над K. Дійсно, нехай θ – його корінь у деякому розширенні поля K. Тоді, очевидно, $x^l - a = (x-\theta)^l$, тому довільний власний дільник цього многочлена має вигляд $(x-\theta)^m$, де $m < l$. Але $(x-\theta)^m = x^m - m\theta x^{m-1} + \cdots + (-1)^m\theta^m$, а $m\theta \notin \mathsf{K}$. Отже, дійсно, $x^l - a$ – незвідний, причому $(x^l-a)' = 0$, тобто поле K недосконале. □

ВПРАВА 2.3. 1. *Доведіть, що кожне скінченне поле є досконалим.*

2. *Нехай* P *– довільне поле характеристики* $l > 0$. *Доведіть, що поле раціональних функцій* $\mathsf{P}(x)$ *– недосконале.*

ВПРАВА 2.4. *Доведіть, що коли елемент* α *з розширення* L *поля* K *є сепарабельним і не належить* K, *то знайдуться таке розширення* $\mathsf{M} \supseteq \mathsf{L}$ *і такий гомоморфізм* $\varphi : \mathsf{L} \to \mathsf{M}$, *що* $\varphi(a) = a$ *для всіх* $a \in \mathsf{K}$, *але* $\varphi(\alpha) \neq \alpha$.

ВКАЗІВКА: Унаслідок теореми 1.1 можна вважати, що $\mathsf{L} = \mathsf{K}[\alpha]$. Тоді можна взяти за M *поле розкладу* (над L) мінімального многочлена елемента α над полем K.

Нагадаємо, що розширення L поля K зветься *полем розкладу* многочлена $f(x) \in \mathsf{K}[x]$, якщо в ньому $f(x) = \prod_{i=1}^m (x-\alpha_i)$, причому $\mathsf{L} = \mathsf{K}(\alpha_1, \alpha_2, \ldots, \alpha_m)$.

ТЕОРЕМА 2.5. *Нехай* L *– скінченне розширення поля* K. *Наступні умови є рівносильними:*

1. L *– поле розкладу деякого многочлена* $f(x) \in \mathsf{K}[x]$.
2. $\varphi(\mathsf{L}) \subseteq \mathsf{L}$ *для довільного розширення* $\mathsf{M} \supseteq \mathsf{L}$ *і довільного гомоморфізму* $\varphi : \mathsf{L} \to \mathsf{M}$, *такого що* $\varphi(a) = a$ *для всіх* $a \in \mathsf{K}$.
3. *Якщо незвідний над полем* K *многочлен* $p(x)$ *має корінь в* L, *то він розкладається в* L *на лінійні множники.*

ДОВЕДЕННЯ. 1⇒2 випливає з того, що φ переводить кожен корінь $p(x)$ знов-таки в корінь $p(x)$.

2⇒3. Нехай $\alpha \in \mathsf{L}$ і $p(\alpha) = 0$. Розглянемо поле розкладу L' многочлена $p(x)$ над полем L і довільний корінь $\beta \in \mathsf{L}$ многочлена $p(x)$. Тоді існує гомоморфізм $\psi : \mathsf{K}(\alpha) \to \mathsf{L}(\beta)$, який переводить α в β. За теоремою 1.1 його можна продовжити до гомоморфізму φ поля L в деяке поле $\mathsf{M} \supseteq \mathsf{L}(\beta)$. Оскільки $\varphi(\mathsf{L}) \subseteq \mathsf{L}$, то, зокрема, $\beta = \varphi(\alpha) \in \mathsf{L}$. Отже, $p(x)$ розкладається в L на лінійні множники.

3⇒1. Якщо $\mathsf{L} = \mathsf{K}(\alpha_1, \alpha_2, \ldots, \alpha_m)$ і $p_i(x) \in \mathsf{K}[x]$ – мінімальний многочлен елемента α_i, то $p_i(x)$ розкладається в L на лінійні множники, а тому L – поле розкладу многочлена $f(x) = \prod_{i=1}^m p_i(x)$. □

Розширення L поля K, яке задовольняє рівносильним умовам теореми 2.5, зветься *нормальним*. Зауважимо, що для *скінченних* розширень з підрахунку розмірностей випливає, що в умові 2 цієї теореми насправді $\varphi(\mathsf{L}) = \mathsf{L}$.

Розширення L поля K назвемо *розширенням Галуа*, якщо виконано умову $\mathsf{L}^{\mathsf{Aut}(\mathsf{L}/\mathsf{K})} = \mathsf{K}$, тобто для довільного елемента $\alpha \in \mathsf{L} \setminus \mathsf{K}$ знайдеться такий автоморфізм σ цього розширення, що $\sigma(\alpha) \neq \alpha$. Групу автоморфізмів розширення Галуа звуть *групою Галуа* цього розширення.

ТЕОРЕМА 2.6. *Нехай* L *– розширення поля* K. *Наступні умови рівносильні:*

1. L *– скінченне розширення Галуа.*
2. $\mathsf{K} = \mathsf{L}^{\mathsf{G}}$ *для деякої скінченної підгрупи* $\mathsf{G} \subseteq \mathsf{Aut}(\mathsf{L})$.
3. *Це розширення скінченне і* $|\mathsf{Aut}(\mathsf{L}/\mathsf{K})| = [\mathsf{L} : \mathsf{K}]$.
4. L *– поле розкладу деякого сепарабельного многочлена* $f(x) \in \mathsf{K}[x]$.
5. L *– скінченне нормальне сепарабельне розширення.*

ДОВЕДЕННЯ. 1⇒2. Зважуючи на наслідок 1.4, можна покласти $\mathsf{G} = \mathsf{Aut}(\mathsf{L}/\mathsf{K})$.

2⇒3 випливає з теореми 1.5 і наслідку 1.4.

3⇒4. З умови 4 теореми 2.1 випливає, що L є сепарабельним (досить покласти $\mathsf{M} = \mathsf{L}$). Далі, для довільного $\mathsf{M} \supseteq \mathsf{L}$, за наслідком 1.3 існує щонайбільше $[\mathsf{L} : \mathsf{K}]$ гомоморфізмів $\varphi : \mathsf{L} \to \mathsf{M}$, таких що $\varphi(a) = a$ при $a \in \mathsf{K}$. Але кожен автоморфізм $\sigma \in$

$\mathrm{Aut}(\mathsf{L}/\mathsf{K})$, звичайно, можна розглядати як гомоморфізм $\mathsf{L} \to \mathsf{M}$ з такою властивістю. Отже, це *всі* такі гомоморфізми, тобто виконується умова 2 теореми 2.5 і L є нормальним.

4⇔5 за теоремами 2.1 і 2.5.

4⇒1. За вправою 2.4 для довільного $\alpha \in \mathsf{L} \setminus \mathsf{K}$ існує таке розширення $\mathsf{M} \supseteq \mathsf{L}$ і такий гомоморфізм $\varphi : \mathsf{L} \to \mathsf{M}$, що $\varphi(a) = a$ при $a \in \mathsf{K}$, але $\varphi(\alpha) \neq \alpha$. Але за умовою 2 теореми 2.5 $\varphi(\mathsf{L}) \subseteq \mathsf{L}$. Отже, $\varphi \in \mathrm{Aut}(\mathsf{L}/\mathsf{K})$ і $\alpha \neq \mathsf{L}^{\mathrm{Aut}(\mathsf{L}/\mathsf{K})}$. □

НАСЛІДОК 2.7. *Нехай* L *– скінченне розширення Галуа поля* K, P *– проміжне підполе, тобто* $\mathsf{K} \subseteq \mathsf{P} \subseteq \mathsf{L}$. *Тоді* L *– розширення Галуа поля* P.

ДОВЕДЕННЯ. Дійсно, якщо L – поле розкладу над K сепарабельного многочлена $f(x) \in \mathsf{K}[x]$, то воно є полем розкладу того ж самого многочлена над P. Але очевидно, що цей многочлен залишається сепарабельним і над P. □

ВПРАВА 2.8. *Нехай* L *– скінченне розширення Галуа поля* K, P *– проміжне підполе. Тоді для довільного гомоморфізму* $\varphi : \mathsf{P} \to \mathsf{M}$, *де* $\mathsf{M} \supseteq \mathsf{L}$, *який залишає на місці всі елементи поля* K, $\varphi(\mathsf{P}) \subseteq \mathsf{L}$ *і* φ *продовжується до автоморфізму поля* L.

ВКАЗІВКА: Скористайтеся теоремами 1.1 і 2.5.

3. Теорія Галуа скінченних розширень

Нехай L – деяке розширення поля K, $\mathsf{G} = \mathrm{Aut}(\mathsf{L}/\mathsf{K})$. Для кожної підмножини $X \subseteq \mathsf{G}$ позначимо

$$\mathsf{L}^X = \{\alpha \in \mathsf{L} \mid \sigma(\alpha) = \alpha \text{ для всіх } \sigma \in X\}.$$

Відповідно для кожної підмножини $Y \subseteq \mathsf{L}$ позначимо

$$\mathsf{G}^Y = \{\sigma \in \mathsf{G} \mid \sigma(\alpha) = \alpha \text{ для всіх } \alpha \in Y\}.$$

Очевидно, L^X – проміжне підполе, а G^Y – підгрупа групи G, причому $X \subseteq \mathsf{G}^{\mathsf{L}^X}$ і $Y \subseteq \mathsf{L}^{\mathsf{G}^Y}$.

ТЕОРЕМА 3.1 (Основна теорема теорії Галуа, ОТТГ). *Якщо* L *– скінченне розширення Галуа поля* K *з групою Галуа* G, *то* $\mathsf{H} = \mathsf{G}^{\mathsf{L}^{\mathsf{H}}}$ *для довільної підгрупи* $\mathsf{H} \subseteq \mathsf{G}$ *і* $\mathsf{P} = \mathsf{L}^{\mathsf{G}^{\mathsf{P}}}$ *для довільного проміжного підполя* $\mathsf{P} \subseteq \mathsf{L}$.

Отже, пара відображень $\mathsf{P} \mapsto \mathsf{G}^{\mathsf{P}}$ та $\mathsf{H} \mapsto \mathsf{L}^{\mathsf{H}}$ встановлює взаємно однозначну відповідність між проміжними підполями скінченного розширення Галуа і підгрупами його групи Галуа. Цю відповідність звуть *відповідністю Галуа*.

ДОВЕДЕННЯ. Оскільки $\mathsf{G}^{\mathsf{P}} = \mathrm{Aut}(\mathsf{L}/\mathsf{P})$, то рівність $\mathsf{L}^{\mathsf{G}^{\mathsf{P}}}$ випливає з наслідку 2.7. Далі, за теоремою 1.5 і наслідком 1.4, $|\mathsf{G}^{\mathsf{L}^{\mathsf{H}}}| \leq [\mathsf{L} : \mathsf{L}^{\mathsf{H}}] = \mathsf{H}$ і, оскільки $\mathsf{H} \subseteq \mathsf{G}^{\mathsf{L}^{\mathsf{H}}}$, маємо також $\mathsf{H} = \mathsf{G}^{\mathsf{L}^{\mathsf{H}}}$. □

Нагадаємо, що підмножини X та $\sigma X \sigma^{-1}$, де $\sigma \in \mathsf{G}$, звуться *спряженими в групі* G. Підмножини $Y \subseteq \mathsf{L}$ та $\sigma(Y)$, де $\sigma \in \mathrm{Aut}(\mathsf{L}/\mathsf{K})$ будемо звати *спряженими в розширенні* L поля K.

ЛЕМА 3.2 (формула спряженості). *Для довільного розширення* L *поля* K *і довільного елемента* $\sigma \in \mathsf{G} = \mathrm{Aut}(\mathsf{L}/\mathsf{K})$ *мають місце рівності:*

$$\mathsf{L}^{\sigma X \sigma^{-1}} = \sigma(\mathsf{L}^X) \quad і \quad \mathsf{G}^{\sigma(Y)} = \sigma \mathsf{G}^Y \sigma^{-1}.$$

Зауважимо, що тут розширення не вважається розширенням Галуа, ані навіть скінченним чи алгебричним.

ДОВЕДЕННЯ. Нехай $\tau \in X$, $\alpha \in \mathsf{L}^X$. Тоді

$$(\sigma\tau\sigma^{-1})(\sigma(\alpha)) = \sigma\tau(\alpha) = \sigma(\alpha), \text{ тобто } \sigma(\alpha) \in \mathsf{L}^{\sigma X \sigma^{-1}}.$$

Отже, $\sigma(\mathsf{L}^X) \subseteq \mathsf{L}^{\sigma X \sigma^{-1}}$. Навпаки, якщо $\beta \in \mathsf{L}^{\sigma X \sigma^{-1}}$, то

$$\tau(\sigma^{-1}\beta) = \sigma^{-1}(\sigma\tau\sigma^{-1})(\beta) = \sigma^{-1}(\beta),$$

тобто $\sigma^{-1}(\beta) \in \mathsf{L}^X$ і $\beta \in \sigma(\mathsf{L}^X)$. Отже, $\mathsf{L}^{\sigma X \sigma^{-1}} \subseteq \sigma(\mathsf{L}^X)$ і першу рівність доведено. Доведення другої (цілком аналогічне) ми залишаємо як вправу читачеві. □

Зокрема, відповідність Галуа переводить спряжені підгрупи у спряжені підполя і навпаки.

ТЕОРЕМА 3.3 (критерій нормальності). *Нехай* L *– скінченне розширення Галуа поля* K *з групою Галуа* G, P *– його проміжне підполе.* P *є нормальним (тобто розширенням Галуа) тоді і лише тоді, коли відповідна підгрупа* $\mathsf{H} = \mathsf{G}^{\mathsf{P}}$ *є нормальною в* G. *У цьому разі* $\mathrm{Aut}(\mathsf{P}/\mathsf{K}) \simeq \mathsf{G}/\mathsf{H}$.

Доведення. Якщо розширення P нормальне, то за теоремою 2.5 (умова 2) $\sigma(\mathsf{P}) = \mathsf{P}$ для довільного $\sigma \in \mathsf{G}$. Тоді за лемою 3.2 $\sigma\mathsf{H}\sigma^{-1} = \mathsf{H}$, тобто H – нормальна підгрупа. Навпаки, нехай підгрупа H є нормальною. За ОТТГ і лемою 3.2 $\sigma(\mathsf{P}) = \mathsf{L}^{\sigma\mathsf{H}\sigma^{-1}} = \mathsf{L}^{\mathsf{H}} = \mathsf{P}$ для всіх $\sigma \in \mathsf{G}$. Обмежуючи кожен автоморфізм на підполе P, одержимо гомоморфізм груп $f : \mathsf{G} \to \mathsf{Aut}(\mathsf{P}/\mathsf{H})$. Очевидно, $\ker f = \mathsf{H}$. За теоремою про гомоморфізм [**6**, с. 312] $\operatorname{Im} f \simeq \mathsf{G}/\mathsf{H}$, зокрема,

$$|\operatorname{Im} f| = (\mathsf{G} : \mathsf{H}) = \frac{|\mathsf{G}|}{|\mathsf{H}|} = \frac{[\mathsf{L} : \mathsf{K}]}{[\mathsf{L} : \mathsf{P}]} = [\mathsf{P} : \mathsf{K}].$$

Зважуючи на наслідок 1.4, маємо, що $\operatorname{Im} f = \mathsf{Aut}(\mathsf{P} : \mathsf{K})$. За теоремою 2.6 (умова 3) P є нормальним розширенням і його група Галуа ізоморфна G/H. □

Поле L зветься *композитом* своїх підполів L_1 і L_2, якщо воно ними породжується, тобто в ньому немає власних підполів, які б містили і L_1 і L_2. У такому разі пишуть $\mathsf{L} = \mathsf{L}_1\mathsf{L}_2$.

Теорема 3.4 (теорема про трансляцію). *Нехай L – скінченне розширення Галуа поля K, з групою Галуа G, K' – довільне розширення K і L' – деякий композит L та K'. Тоді L' – скінченне розширення Галуа поля K', причому* $\mathsf{Aut}(\mathsf{L}'/\mathsf{K}') \simeq \mathsf{G}^{\mathsf{K}'\cap\mathsf{L}}$.

Доведення. За теоремою 2.6 L – поле розкладу деякого сепарабельного многочлена $f(x)$ над полем K. Але тоді L' є полем розкладу того ж многочлена над полем K', отже, є також розширенням Галуа цього поля. Крім того, якщо $\sigma \in \mathsf{Aut}(\mathsf{L}'/\mathsf{K}')$, то $\sigma(\mathsf{L}) = \mathsf{L}$ (за умовою 2 теореми 2.5). Якщо обмеження σ на L є тотожним відображенням, то підполе L'^{σ} містить і K' і L, звідки $\mathsf{L}'^{\sigma} = \mathsf{L}'$, тобто $\sigma = 1$. Отже, обмежуючи кожен автоморфізм σ на підполе L, одержимо занурення груп Галуа $f : \mathsf{Aut}(\mathsf{L}'/\mathsf{K}') \to \mathsf{G}$. Обчислимо його образ H. Якщо $\alpha \in \mathsf{L}^{\mathsf{H}}$, то $\sigma(\alpha) = \alpha$ для всіх $\sigma \in \mathsf{Aut}(\mathsf{L}'/\mathsf{K}')$, звідки за теоремою 2.6 (умова 1) $\alpha \in \mathsf{K}'$. Оскільки, очевидно, $\mathsf{K}' \cap \mathsf{L} \subseteq \mathsf{L}^{\mathsf{H}}$, маємо, що $\mathsf{L}^{\mathsf{H}} = \mathsf{K}' \cap \mathsf{L}$ і за ОТТГ $\mathsf{H} = \mathsf{G}^{\mathsf{K}'\cap\mathsf{L}}$. □

З ОТТГ випливає, зокрема, що скінченне розширення Галуа має лише скінченну кількість проміжних підполів. Зауважимо, що скінченне сепарабельне розширення завжди можна вкласти у

скінченне розширення Галуа. Дійсно, нехай $\mathsf{L} = \mathsf{K}(\alpha_1, \alpha_2, \ldots, \alpha_m)$, де кожен елемент α_i є коренем сепарабельного многочлена $p_i(x) \in \mathsf{K}[x]$. Тоді L міститься у полі розкладу сепарабельного многочлена $f(x) = \prod_{i=1}^{m} p_i(x)$.

Наслідок 3.5. *Кожне сепарабельне розширення має лише скінченну кількість проміжних підполів.*

Теорема 3.6 (теорема про примітивний елемент). *Якщо L – сепарабельне розширення поля K, то знайдеться такий елемент $\theta \in \mathsf{L}$, що $\mathsf{L} = \mathsf{K}(\theta)$.*
(Такий елемент зветься *примітивним елементом* розширення L.)

Доведення. Якщо поле K скінченне, то і L скінченне. Тоді його мультиплікативна група циклічна [**6**, с. 429] і за θ можна взяти твірний цієї групи. Тому надалі вважатимемо поле K нескінченним. За наслідком 3.5 L має лише скінченне число власних проміжних підполів: $\mathsf{L}_1, \mathsf{L}_2, \ldots, \mathsf{L}_m$. Ясно, що досить вибрати елемент θ так, щоб він не належав об'єднанню $\bigcup_{i=1}^{m} \mathsf{L}_i$. Отже, твердження теореми безпосередньо випливає з наступної простої леми, доведення якої ми залишаємо читачеві:

Лема 3.7. *Якщо V – векторний простір над нескінченним полем, $U_1, U_2, \ldots, U_m$ – його власні підпростори, то $\bigcup_{i=1}^{m} U_i \neq V$.*

□

Нехай L – поле розкладу деякого многочлена $f(x) \in \mathsf{K}[x]$. Припустимо, що L має примітивний елемент θ (наприклад, многочлен $f(x)$ сепарабельний) і $p(x)$ – мінімальний многочлен елемента θ. Тоді $p(x)$ зветься *резольвентою Галуа* многочлена $f(x)$ (над полем K).

Вправа 3.8. *Доведіть, що резольвента Галуа многочлена $f(x)$ – це такий многочлен $p(x)$, який задовольняє наступні вимоги:*

1. *$p(x)$ незвідний.*
2. *Кожен корінь многочлена $p(x)$ раціонально виражається через елементи поля K і якийсь один (а тоді, звичайно, через будь-який) з цих коренів.*
(Многочлен з цією властивістю зветься *нормальним*.)

3. *Кожен корінь многочлена $f(x)$ раціонально виражається через елементи поля K і корені многочлена $f(x)$ і навпаки. кожен корінь многочлена $p(x)$ раціонально виражається через елементи поля K і корені многочлена $p(x)$.*
(Такі два многочлени звуться *еквівалентними за Чирнгаусом.*)

ТЕОРЕМА 3.9 (теорема про мінімальний многочлен). *Нехай L – розширення Ґалуа поля K (не обов'язково скінченне) з групою Ґалуа G, $\alpha \in \mathsf{L}$ – алгебричний над K елемент і $p(x)$ – його мінімальний многочлен над K. Тоді індекс $m = (\mathsf{G} : \mathsf{G}^\alpha)$ є скінченним і якщо $\tau_1, \tau_2, \ldots, \tau_m$ – представники всіх суміжних класів групи G за підгрупою G^α, то $p(x) = \prod_{i=1}^m (x - \tau_i(\alpha))$.*

ДОВЕДЕННЯ. Легко перевірити, що $\sigma(\alpha) = \sigma'(\alpha)$ тоді і лише тоді, коли $\sigma\mathsf{G}^\alpha = \sigma'\mathsf{G}^\alpha$. Оскільки $\sigma(\alpha)$ – знов корінь многочлена $p(x)$, звідси випливає, що $m < \infty$ і $p(x)$ ділиться на многочлен $g(x) = \prod_{i=1}^m (x - \tau_i(\alpha))$. Але для довільного $\sigma \in \mathsf{G}$ елементи $\sigma\tau_1, \sigma\tau_2, \ldots \sigma\tau_n$ також лежать у різних суміжних класах за підгрупою G^α. Тому елементи $\sigma\tau_i(\alpha)$ – це ті самі елементи $\tau_i(\alpha)$, лише записані в іншому порядку. Звідси випливає, що

$$(\sigma g)(x) = \prod_{i=1}^m (x - \sigma\tau_i(\alpha)) = \prod_{i=1}^m (x - \tau_i(\alpha)) = g(x).$$

Оскільки $\mathsf{L}^\mathsf{G} = \mathsf{K}$, то $g(x) \in \mathsf{K}[x]$. З мінімальності $p(x)$ одержуємо, що $p(x) = g(x)$. □

ВПРАВА 3.10. *Нехай L – розширення Ґалуа поля K (не обов'язково скінченне) з групою Ґалуа G, $p(x)$ – незвідний многочлен над полем K, $q(x)$ – його незвідний множник над полем L і $\mathsf{H} = \{\sigma \in \mathsf{G} \mid (\sigma q)(x) = q(x)\}$. Тоді $m = (\mathsf{G} : \mathsf{H}) < \infty$ і якщо $\tau_1, \tau_2, \ldots, \tau_m$ – представники всіх суміжних класів G за підгрупою H, то $p(x) = \prod_{i=1}^m (\tau_i q)(x)$ (ясно, що всі ці многочлени також незвідні над L).*

ВПРАВА 3.11. *Нехай $\mathsf{L} = \mathsf{L}_1\mathsf{L}_2$, де L_i $(i = 1, 2)$ – скінченне розширення Ґалуа поля K з групою Ґалуа G_i. Доведіть,*

що L – також скінченне розширення Ґалуа, а його група Ґалуа G ізоморфна підгрупі в $\mathsf{G}_1 \times \mathsf{G}_2$, яка складається з усіх таких пар (σ_1, σ_2), що обмеження σ_1 і σ_2 на $\mathsf{L}_1 \cap \mathsf{L}_2$ збігаються.

ВКАЗІВКА: Протиставляючи елементу $\sigma \in \mathsf{G}$ пару (σ_1, σ_2), де σ_i – обмеження σ на L_i, одержимо занурення G у вказану підгрупу. Для доведення їхньої збіжності можна скористатися теоремою 3.4.

ВПРАВА 3.12. *Нехай K – досконале поле, L – його квадратичне розширення (тобто $(\mathsf{L} : \mathsf{K}) = 2$), причому:*

1. *Кожен многочлен непарного ступеня над полем K має корінь в K.*
2. *Довільне квадратне рівняння над L має корінь в L.*

Доведіть, що поле L є алгебрично замкненим. Поклавши $\mathsf{K} = \mathbb{R}$. виведіть звідси "Основну теорему алгебри".

ВКАЗІВКИ: (i) Досить перевірити, що коли $\mathsf{M} \supseteq \mathsf{L}$ – скінченне розширення Ґалуа поля K, то $\mathsf{M} = \mathsf{L}$. Нехай $\mathsf{G} = \mathsf{Aut}(\mathsf{M}/\mathsf{K})$, H – її силовська 2-підгрупа (див. [**6**, с. 333]). З умови 1 виведіть, що $\mathsf{M}^\mathsf{H} = \mathsf{K}$, тобто $\mathsf{H} = \mathsf{G}$.

(ii) Отже, $|\mathsf{G}^\mathsf{L}| = 2^m$. Якщо $m > 0$, в G є підгрупа F індекса 2 (див. [**6**, с. 334]). Тоді $[\mathsf{M}^\mathsf{F} : \mathsf{L}] = 2$, що неможливо внаслідок умови 2.

4. Обчислення груп Ґалуа

Почнемо з деяких прикладів. Нагадаємо, що *первісним коренем ступеня n з одиниці* зветься такий елемент $\zeta = \sqrt[n]{1}$, що $\zeta^n = 1$, але $\zeta^m \neq 1$ при $0 < m < n$. Зауважимо, що це можливо лише коли n не ділиться на характеристику l поля: якщо $n = ln$, то з $\zeta^n = 1$ випливає, що $\zeta^m = 1$.

ВПРАВА 4.1. *Припустимо, що поле K містить первісний корінь ступеня n з одиниці, а $\mathsf{L} = \mathsf{K}(\theta)$, де $\theta^n = a \in \mathsf{K}$* (будемо писати $\theta = \sqrt[n]{a}$). *Доведіть, що L розширення Ґалуа, його група Ґалуа G циклічна, її порядок ділить n, причому $|\mathsf{G}| = n$ тоді і лише тоді, коли многочлен $x^n - a$ є незвідним над K.*

ВКАЗІВКИ: (i) Усі корені многочлена $x^n - a$ – це $\theta, \zeta\theta, \zeta^2\theta, \ldots, \zeta^{n-1}\theta$, де $\zeta = \sqrt[n]{1}$. Звідси випливає нормальність L.

(ii) Якщо $\sigma \in \mathsf{G}$, то $\sigma(\theta) = \zeta^m\theta$, де $0 \le m < n$, причому знання m повністю визначає σ. Перевірте, що відображення $\sigma \mapsto m$ є зануренням G до групи лишків $\mathbb{Z}_n$ за модулем n.

(iii) Для завершення доведення скористайтеся тим, що довільна підгрупа в $\mathbb{Z}_n$ є циклічною [**6**, с. 167], а $|\mathsf{G}| = \deg p(x)$, де $p(x)$ – мінімальний многочлен елемента θ.

Нехай знову n не ділиться на характеристику поля K, а L – поле розкладу (над K) многочлена $x^n - 1$ (або, що те саме, кругового многочлена $\Phi_n(x)$, див. [**6**, с. 434]). За теоремою 2.6 воно є розширенням Галуа.

ВПРАВА 4.2. *Доведіть, що група Галуа* $\mathsf{G} = \mathsf{Aut}(\mathsf{L}/\mathsf{K})$ *абелева, її порядок ділить* $\phi(n)$, *де* ϕ *– функція Ейлера* [**6**, с. 433], *причому* $|\mathsf{G}| = \phi(n)$ *тоді і лише тоді, коли многочлен* $\Phi_n(x)$ *є незвідним над полем* K.

ВКАЗІВКИ: (i) Усі корені многочлена $x^n - 1$ є простими, тому вони утворюють підгрупу порядка n в мультиплікативній групі поля L. Ця підгрупа циклічна [**6**, с. 430], отже, $\mathsf{L} = \mathsf{K}(\zeta)$, де $\zeta = \sqrt[n]{1}$.

(ii) Якщо $\sigma \in \mathsf{G}$, то $\sigma(\zeta) = \zeta^m$, де $0 < m < n$ і $(m, n) = 1$, причому знання m повністю визначає σ. Перевірте, що $\sigma \mapsto m$ задає занурення G у групу $\mathbb{Z}_n^*$ обертовних елементів кільця лишків за модулем n.

ВПРАВА 4.3. *Нехай знов* n *не ділиться на характеристику поля* K, *а* L *– поле розкладу многочлена* $x^n - a$, *де* $a \in \mathsf{K}$. *Доведіть, що його група Галуа* G *ізоморфна підгрупі групи* T_n *матриць вигляду*

$$\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}, \qquad \text{де } a \in \mathbb{Z}_n^*,\ b \in \mathbb{Z}_n$$

(операція – звичайне множення матриць).

ВКАЗІВКА: Перевірте, що $\mathsf{L} = \mathsf{K}(\theta, \zeta)$, де $\theta = \sqrt[n]{a}$, $\zeta = \sqrt[n]{1}$, причому якщо $\sigma \in \mathsf{G}$, то $\sigma(\zeta) = \zeta^a$, де $a \in \mathbb{Z}_n^*$, а $\sigma(\theta) = \zeta^b\theta$, де $b \in \mathbb{Z}_n$.

ВПРАВА 4.4. *Нехай* L *– поле розкладу многочлена* $x^4 - 2$ *над полем* $\mathbb{Q}$ *раціональних чисел (він є незвідним за критерієм Ейзенштейна* [**6**, с. 231]). *Обчисліть його групу Галуа* G *і знайдіть усі підполя в* L.

ВКАЗІВКИ: (i) Перевірте, що $\mathsf{L} = \mathbb{Q}(\theta, i)$, де $\theta = \sqrt[4]{2}$, $i = \sqrt{-1}$, причому $[\mathsf{L} : \mathbb{Q}] = 8$ і базу L утворюють числа

$$\{1, \theta, \theta^2, \theta^3, i, i\theta, i\theta^2, i\theta^3\}.$$

Отже, в позначеннях вправи 4.3 $\mathsf{G} \simeq \mathsf{T}_4$. Позначимо

$$\sigma = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad \tau = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Тоді $\mathsf{G} = \langle \sigma, \tau \mid \sigma^4 = \tau^2 = 1,\ \tau\sigma = \sigma^3\tau \rangle$.

(ii) Перевірте, що G містить 6 циклічних підгруп:

$$\mathsf{C}_b = \langle \sigma^b\tau \rangle\ (b = 0, 1, 2, 3) \text{ та } \mathsf{D}_b = \langle \sigma^b \rangle\ (b = 0, 1).$$

і 2 нециклічні підгрупи:

$$\mathsf{H}_b = \langle \sigma^2, \sigma^b\tau \mid b = 0, 1 \rangle.$$

(iii) Очевидно, $\mathsf{L}^{\langle\sigma\rangle} = \mathbb{Q}(i)$ і $\mathsf{L}^{\langle\tau\rangle} = \mathbb{Q}(\theta)$. Оскільки $\sigma^2\tau = \sigma\tau\sigma^{-1}$, поле $\mathsf{L}^{\langle\sigma^2\tau\rangle}$ знаходиться за лемою 3.2. Далі, $\sigma(\theta^2) = -\theta^2$, звідки $\sigma^2(\theta^2) = \theta^2$ і $\mathsf{L}^{\mathsf{H}_0} = \mathbb{Q}(\theta^2) = \mathbb{Q}(\sqrt{2})$. Тепер легко перевірити, що $\mathsf{L}^{\langle\sigma^2\rangle} = \mathbb{Q}(\sqrt{2}, i)$.

(iv) Обчислимо $\mathsf{L}^{\langle\sigma\tau\rangle}$. Зауважимо, що $\sigma\tau(i) = i$, а $\sigma\tau(\theta) = i\theta$. Звідси випливає, що коли

$$\alpha = x_1 + x_2\theta + x_3\theta^2 + x_4\theta^3 + x_5 i + x_6 i\theta + x_7 i\theta^2 + x_8 i\theta^3,$$

то рівність $\sigma\tau(\alpha) = \alpha$ рівносильна системі лінійних рівнянь: $x_2 = x_6$, $x_3 = 0$, $x_4 = -x_8$, $x_5 = 0$. Звідси знаходимо базу $\mathsf{L}^{\langle\sigma\tau\rangle}$: $\{1, \theta + i\theta, i\theta^2, \theta^3 - i\theta^3\}$. Оскільки $(\theta + i\theta)^2 = 2i\theta^2$, а $(\theta + i\theta)^3 = -2(\theta^3 - i\theta^3)$, маємо, що $\mathsf{L}^{\langle\sigma\tau\rangle} = \mathbb{Q}(\theta + i\theta) = \mathbb{Q}(\sqrt[4]{-2})$. Поле $\mathsf{L}^{\langle\sigma^3\tau\rangle}$ тепер знаходиться за лемою 3.2. Нарешті, легко перевіряється, що $\mathsf{L}^{\mathsf{H}_1} = \mathbb{Q}(i\theta^2) = \mathbb{Q}(\sqrt{-2})$.

Розглянемо тепер деякі загальні результати про групи Галуа.

ТЕОРЕМА 4.5. *Нехай* $\mathsf{K} = \mathsf{F}(t_1, t_2, \ldots, t_n)$ *– поле раціональних функцій від* n *змінних над полем* F,

$$f(x) = x^n + t_1x^{n-1} + t_2x^{n-2} + \cdots + t_{n-1}x + t_n$$

(*"загальний многочлен ступеня n над полем F"*), L – *поле розкладу* $f(x)$ *над* K. *Тоді* $\mathsf{Aut}(\mathsf{L}/\mathsf{K}) \simeq \mathfrak{S}_n$ (*симетрична група ступеня* n). *Зокрема,* $[\mathsf{L} : \mathsf{K}] = n!$.

Доведення. Позначимо $\xi_1, \xi_2, \ldots, \xi_n$ корені многочлена $f(x)$ у полі L. Тоді $\mathsf{L} = \mathsf{K}(\xi_1, \xi_2, \ldots, \xi_n) = \mathsf{F}(\xi_1, \xi_2, \ldots, \xi_n)$, оскільки за формулами Вієта $t_i = (-1)^i s_i(\xi_1, \xi_2, \ldots, \xi_n)$, де s_i – елементарні симетричні многочлени від n змінних. Далі, якщо $g(x_1, x_2, \ldots, x_n)$ – ненульовий многочлен з $\mathsf{F}(\xi_1, \xi_2, \ldots, \xi_n)$, то $g(\xi_1, \xi_2, \ldots, \xi_n) \neq 0$: інакше, виразивши многочлен $\prod_{\sigma \in \mathfrak{S}_n} g(x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(n)})$ через елементарні симетричні і підставивши в нього ξ_i, ми одержали б рівність вигляду $h(t_1, t_2, \ldots, t_n) = 0$, що неможливо. Отже, L також є полем раціональних функцій від n змінних $\xi_1, \xi_2, \ldots, \xi_n$ над полем F. Тому можна означити занурення $\mathfrak{S}_n \to \mathsf{Aut}(\mathsf{L}/\mathsf{K})$: підстановці σ відповідає автоморфізм, який переводить кожне ξ_i у $\xi_{\sigma(i)}$ (ясно, що при цьому t_i лишаються нерухомими). Але й навпаки, довільний автоморфізм лише переставляє корені ξ_i многочлена $f(x)$. Отже, $\mathsf{Aut}(\mathsf{L}/\mathsf{K}) \simeq \mathfrak{S}_n$. □

Якщо $f(x) \in \mathsf{K}[x]$ – сепарабельний многочлен, L – його поле розкладу, то група $\mathsf{G} = \mathsf{Aut}(\mathsf{L}/\mathsf{K})$ зветься *групою Галуа* многочлена $f(x)$ (або рівняння $f(x) = 0$). Отже, ми довели, що група Галуа загального многочлена (або загального рівняння) ступеня n над довільним полем F є повною симетричною групою ступеня n.

Припустимо, що многочлен $f(x)$ не має кратних коренів (це не знижує загальності, оскільки від кратних множників можна звільнитися добре відомою процедурою). Якщо $\alpha_1, \alpha_2, \ldots, \alpha_n$ – всі корені $f(x)$, то кожен автоморфізм з G лише переставляє ці корені. Отже, маємо природне занурення $\mathsf{G} \to \mathfrak{S}_n$. Надалі ми будемо ототожнювати автоморфізми $\sigma \in \mathsf{G}$ з відповідними перестановками коренів.

Вправа 4.6. *Доведіть, що многочлен* $f(x)$ *є незвідним тоді і лише тоді, коли група* G *є* транзитивною, *тобто для кожної пари індексів* i, j *знайдеться такий автоморфізм* σ, *що* $\sigma(\alpha_i) = \alpha_j$.

Вказівка: Скористайтеся ізоморфізмом $\mathsf{K}(\alpha_i) \simeq \mathsf{K}(\alpha_j)$ і вправою 2.8.

Нехай знову $f(x) \in \mathsf{K}[x]$ – сепарабельний многочлен без кратних коренів. L – його поле розкладу і G – його група Галуа, ототожнена, як вище, з деякою групою перестановок його коренів $\alpha_1, \alpha_2, \ldots, \alpha_n$, так що $\sigma(\alpha_i) = \alpha_{\sigma(i)}$. Розглянемо поля раціональних функцій від n змінних, відповідно, над K і L: $\mathsf{K}' = \mathsf{K}(t_1, t_2, \ldots, t_n)$ і $\mathsf{L}' = \mathsf{L}(t_1, t_2, \ldots, t_n)$. Ясно, що $\mathsf{K}' \cap \mathsf{L} = \mathsf{K}$. Тоді за теоремою 3.4 $\mathsf{Aut}(\mathsf{L}'/\mathsf{K}') \simeq \mathsf{G}$. З іншого боку, $\mathfrak{S}_n$ діє на L' перестановками змінних. Автоморфізм поля sL', який відповідає підстановці σ при цій дії, позначимо σ_t. Отже, $\sigma_t(g)(t_1, t_2, \ldots, t_n) = g(t_{\sigma(1)}, t_{\sigma(2)}, \ldots, t_{\sigma(n)})$. Покладемо

$$\theta = \sum_{i=1}^{n} \alpha_i t_i \quad \text{і} \quad F(x) = \prod_{\sigma \in \mathfrak{S}_n} (x - \sigma_t(\theta)).$$

Теорема 4.7. $F(x) \in \mathsf{K}'[x]$ *і якщо* $p(x)$ – *якийсь його незвідний множник у* $\mathsf{K}'[x]$, *то група* G *спряжена у* $\mathfrak{S}_n$ *з підгрупою*

$$\mathsf{G}_p = \{\, \sigma \in \mathfrak{S}_n \mid (\sigma_t p)(x) = p(x) \,\}.$$

Доведення. Якщо $\sigma \in \mathsf{G}$, то

$$\sigma(\theta) = \sum_{i=1}^{n} \alpha_{\sigma(i)} t_i = \sum_{i=1}^{n} \alpha_i t_{\sigma^{-1}(i)} = \sigma_t^{-1}(\theta).$$

Аналогічно, $\sigma\tau_t(\theta) = (\tau\sigma^{-1})_t(\theta)$. Тому $(\sigma F)(x) = F(x)$, тобто $F(x) \in \mathsf{K}'[x]$. Крім того, з рівності $\sigma(\theta) = \theta$ випливає, що $\sigma = 1$, отже, $\mathsf{L}' = \mathsf{K}'(\theta)$.

Позначимо $\mathsf{P} = \{\, \gamma \in \mathsf{K}' \mid \sigma_t(\gamma) = \gamma \text{ для всіх } \sigma \in \mathfrak{S}_n \,\}$. За теоремою 2.6, K' є розширенням Галуа поля P. Легко збагнути, що $F(x) \in \mathsf{P}[x]$ і є незвідним многочленом над P. Згідно з вправою 3.10 кожен незвідний множник $F(x)$ над K' має вигляд $(\tau_t p)(x)$ для деякого $\tau \in \mathfrak{S}_n$. Але, як і в лемі 3.2, легко перевірити, що $\mathsf{G}_{\tau_t p} = \tau \mathsf{G} \tau^{-1}$. Тому за $p(x)$ можна взяти *довільний* незвідний множник многочлена $F(x)$, зокрема, той, коренем якого є θ. Тому можна вважати, що $p(x)$ – мінімальний многочлен елемента θ над полем K'. За теоремою 3.9 $\{\, \sigma(\theta) \mid \sigma \in \mathsf{G} \,\}$ – це всі корені $p(x)$. Але, очевидно, $\sigma_t(\theta)$ – це корінь $(\sigma_t p)(x)$. Отже,

якщо $\sigma \in \mathsf{G}$, то $\sigma(\theta)$ – це корінь многочлена $(\sigma_i^{-1}p)(x)$ і, оскільки різні незвідні многочлени не можуть мати спільних коренів, $(\sigma_i^{-1}p)(x) = p(x)$, тобто $\sigma_i \in \mathsf{G}_p$. Навпаки, якщо $\sigma_i \in \mathsf{G}_p$, то $p(\sigma_i(\theta)) = 0$, звідки $\sigma_i(\theta) = \tau(\theta) = \tau_i^{-1}(\theta)$ для деякого $\tau \in \mathsf{G}$. Оскільки всі α_i різні, звідси маємо, що $\sigma = \tau^{-1} \in \mathsf{G}$. □

Одержаний результат застосуємо в такій ситуації. Нехай A – факторіальне кільце (тобто кільце з однозначним розкладом на незвідні множники [**6**, с. 221]), K – його поле часток, π – незвідний елемент кільця A, $\overline{\mathsf{A}} = \mathsf{A}/(\pi)$ і $\overline{\mathsf{K}}$ – поле часток кільця $\overline{\mathsf{A}}$. Для довільного многочлена $f(x) \in \mathsf{A}[x]$ позначимо $\overline{f}(x)$ многочлен з $\overline{\mathsf{A}}[x]$, який одержується з $f(x)$ заміною всіх коефіцієнтів їхніми лишками за модулем π.

ТЕОРЕМА 4.8. *Припустимо, що старший коефіцієнт многочлена $f(x)$ дорівнює 1 і обидва многочлени $f(x)$ та $\overline{f}(x)$ не мають кратних коренів. Тоді група Галуа $\overline{\mathsf{G}}$ многочлена $\overline{f}(x)$ спряжена в $\mathfrak{S}_n$ (де $n = \deg f(x)$) з деякою підгрупою групи Галуа G многочлена $f(x)$.*

ДОВЕДЕННЯ. Будемо дотримуватись позначень з доведення попередньої теореми. Очевидно, $F(x) \in A[x, t_1, t_2, \ldots, t_n]$, а многочлен $\overline{F}(x)$, який будується в той самий спосіб за многочленом $\overline{f}(x)$, належить $\overline{\mathsf{A}}[x, t_1, t_2, \ldots, t_n]$ і також одержується з $F(x)$ заміною коефіцієнтів на лишки за модулем π. Розкладемо $F(x)$ на незвідні множники в кільці $\mathsf{A}[x, t_1, t_2, \ldots, t_n]$: $F(x) = p_1(x)p_2(x)\ldots p_k(x)$. Відомо, що многочлени $p_i(x)$ залишаються незвідними і в кільці $\mathsf{K}'[x]$ [**6**, с. 442]. За теоремою 4.7 G можна ототожнити з $\{\sigma \in \mathfrak{S}_n \,|\, (\sigma_i p_1)(x) = p_1(x)\}$. Але $\overline{F}(x) = \overline{p}_1(x)\overline{p}_2(x)\ldots\overline{p}_k(x)$, а $\overline{\mathsf{G}}$ спряжена з підгрупою $\mathsf{G}_q = \{\sigma \in \mathfrak{S}_n \,|\, (\sigma_i q)(x) = q(x)\}$, де $q(x)$ – якийсь незвідний множних $\overline{p}_1(x)$. За побудовою ні $F(x)$, ані $\overline{F}(x)$ не мають кратних множників. Тому, якщо $\sigma \in \mathsf{G}_q$, то $(\sigma_i p_1)(x) = p_1(x)$: інакше було б $(\sigma_i p_1)(x) = p_i(x)$ для якогось $i > 1$, а тоді $q(x)$ був би спільним множником $\overline{p}_1(x)$ і $\overline{p}_i(x)$, тобто, кратним множником $\overline{F}(x)$. Отже, $\mathsf{G}_q \subseteq \mathsf{G}$, що й треба було довести. □

Цей метод зручно застосовувати до многочленів з цілими коефіцієнтами. Зокрема, з них можна одержати наступні результати, які будуть згодом використані, коли ми вивчатимемо розв'язність рівнянь у радикалах.

ВПРАВА 4.9. *Доведіть, що група Галуа G многочлена $f(x) = x^5 - x - 1$ над полем раціональних чисел збігається з повною симетричною групою $\mathfrak{S}_5$.*

ВКАЗІВКИ: (i) $f(x) \equiv (x^3 + x + 1)(x^2 + x + 1)(\mod 2)$, де обидва співмножники є незвідними. Тому з теореми 4.8 випливає, що G містить перестановку вигляду $\sigma = (ij)(klm)$, де всі індекси різні, а тоді й транспозицію $(ij) = \sigma^3$.

(ii) За модулем 3 многочлен $f(x)$ є незвідним, звідки випливає, що його група Галуа за цим модулем є циклічною (вправа 1.6) і транзитивною (вправа 4.6), отже, породжується циклом довжини 5. Тому можна вважати, що $\mathsf{G} \ni (1, 2, 3, 4, 5)$.

(iii) Залишається перевірити, що $\langle (i, j), (1, 2, 3, 4, 5) \rangle = \mathfrak{S}_5$.

ВПРАВА 4.10. *Доведіть, що, для довільного n, існує незвідний многочлен $f(x) \in \mathbb{Q}[x]$, група Галуа якого збігається з $\mathfrak{S}_n$.*

ВКАЗІВКИ: (i) Над полем лишків $\mathbb{Z}_p$ існують незвідні многочлени довільного ступеня [**6**, с. 429]. Тому можна побудувати такі многочлени ступеня n з цілими коефіцієнтами і старшим коефіцієнтом 1:

$f_2(x)$, незвідний за модулем 2;

$f_3(x)$, який за модулем 3 має незвідний множник ступеня $n - 1$;

$f_5(x)$, який за модулем 5 має незвідний квадратичний множник і незвідний множник ступеня або $n-2$, якщо n непарне, або $n - 3$, якщо n парне.

(ii) Покладіть $f(x) = 10f_3(x) + 6f_5(x) - 15f_2(x)$. Тоді його група Галуа G містить цикл довжини n, цикл довжини $n-1$ і транспозицію.

(iii) Виведіть звідси, що $\mathsf{G} = \mathfrak{S}_n$.

5. Розв'язність рівнянь у радикалах

У цьому розділі (крім кількох останніх вправ) ми вважатимемо, що всі поля мають характеристику 0.

Простим радикальним розширенням поля K звуть розширення вигляду $\mathsf{K}(\sqrt[n]{a})$, де многочлен $x^n - a$ є незвідним над K. Розширення L звуть *радикальним*, якщо існує ланцюг проміжних підполів

$$\mathsf{K} = \mathsf{P}_0 \subset \mathsf{P}_1 \subset \mathsf{P}_2 \subset \ldots \subset \mathsf{P}_m = \mathsf{L},$$

в якому кожне P_i $(i = 1, 2, \ldots, m)$ є простим радикальним розширенням P_{i-1}. Кажуть, що рівняння $f(x) = 0$ є *розв'язним у радикалах*, якщо поле розкладу многочлена $f(x)$ можна вкласти в деяке радикальне розширення[1]. Зауважимо, що з означення безпосередньо випливає, що рівняння $f(x) = 0$ є розв'язним у радикалах тоді і лише тоді, коли таким є рівняння $p(x) = 0$, де $p(x)$ – резольвента Галуа многочлена $f(x)$.

Нагадаємо [6, с. 318],[11, § 9.2], що група G зветься *розв'язною*, якщо $\mathsf{G}^{(k)} = 1$ для деякого номера k, де $\mathsf{G}^{(k)}$ – k-а *похідна група* групи G, тобто $\mathsf{G}^{(1)} = \mathsf{G}'$ (комутант G) і $\mathsf{G}^{(k+1)} = \mathsf{G}^{(k)\prime}$ для кожного k.

Нам будуть потрібні наступні прості властивості розв'язних груп, доведення яких можна знайти в будь-якому підручнику з теорії груп (див. напр. [11, § 9.2]):

1. Підгрупи і фактор-групи розв'язних груп знов є розв'язними.
2. Якщо H – нормальна підгрупа G, причому групи H та G/H розв'язні, то група G також розв'язна.
3. Скінченна група G є розв'язною тоді і лише тоді, коли в ній є ланцюг підгруп $\mathsf{G} = \mathsf{H}_0 \supset \mathsf{H}_1 \supset \mathsf{H}_2 \supset \ldots \supset \mathsf{H}_m = 1$, такий що кожна підгрупа H_i $(i = 1, 2, \ldots, m)$ є нормальною в H_{i-1} з циклічною фактор-групою $\mathsf{H}_{i-1}/\mathsf{H}_i$.

Теорема 5.1 (Теорема Лагранжа). *Припустимо, що поле K містить первісний корінь ζ ступеня n з одиниці, а L – його розширення Галуа, група Галуа G якого є циклічною порядку n. Тоді L є простм радикальним розширенням поля K.*

Доведення. Позначимо σ твірний групи G і виберемо елемент $\alpha \in \mathsf{L}$ так, щоб

$$\theta = \alpha + \zeta\sigma(\alpha) + \zeta^2\sigma^2(\alpha) + \cdots + \zeta^{n-1}\sigma^{n-1}(\alpha) \neq 0$$

[1]Ми побачимо далі (вправа 5.9), що звідси, взагалі кажучи, *не випливає*, що саме поле розкладу є радикальним.

(це можливо за теоремою 1.2). Тоді легко впевнитись, що $\sigma(\theta) = \zeta^{-1}\theta$, звідки $\sigma^m(\theta) = \zeta^m\theta \neq \theta$ при $0 < m < n$. Отже, $\mathsf{G}^\theta = 1$ і за ОТТГ $\mathsf{K}(\theta) = \mathsf{L}$. Але $\sigma(\theta^n) = \zeta^{-n}\theta^n = \theta^n$, тобто $\theta^n = a \in \mathsf{K}$. Оскільки $n = [\mathsf{L} : \mathsf{K}]$ дорівнює ступеню мінімального многочлена твірного θ, цей мінімальний многочлен має збігатися з $x^n - a$, отже, останній є незвідним. □

Наслідок 5.2. *Нехай знову $\mathsf{K} \ni \zeta = \sqrt[n]{1}$ і L – нормальне розширення поля K ступеня n. Воно є радикальним тоді і лише тоді, коли його група Галуа G є розв'язною.*

Доведення. Припустимо, що група G є розв'язною. Тоді в ній є ланцюг підгруп $\mathsf{G} = \mathsf{H}_0 \supset \mathsf{H}_1 \supset \ldots \supset \mathsf{H}_m = 1$, в якому кожна наступна підгрупа є нормальною в попередній і всі фактор-групи $\mathsf{G}_i = \mathsf{H}_i/\mathsf{H}_{i-1}$ циклічні. Зауважимо, що $n_i = |\mathsf{G}_i|$ ділить n, отже, K містить також первісні корені всіх ступенів n_i з одиниці. Позначимо $\mathsf{P}_i = \mathsf{L}^{\mathsf{H}_i}$. З ОТТГ і теореми 2.7 випливає, що P_i є нормальним розширенням P_{i-1} з групою Галуа G_i. За теоремою Лагранжа це розширення є простим радикальним, а тому L є радикальним розширенням поля K. Доведення оберненого твердження (практично таке саме, лише із заміною теореми Лагранжа на вправу 4.1) ми залишаємо як вправу читачеві. □

Теорема 5.3. *Рівняння $x^n - 1 = 0$ завжди є розв'язним у радикалах.*

Доведення. Позначимо $\mathsf{L} = \mathsf{K}(\sqrt[n]{1})$ (це є поле розкладу $x^n - 1$) і застосуємо індукцію за n. Якщо $n = 1$ (або $n = 2$), то $\mathsf{L} = \mathsf{K}$ і доводити нема чого. Припустимо, що твердження теореми є вірним для всіх $m < n$. Тоді, зокрема, поле $\mathsf{K}(\sqrt[\phi(n)]{1})$, де ϕ – функція Ейлера, можна вкласти у радикальне розширення M. З теореми 1.1 випливає, що M можна вважати вкладеним у деяке розширення L' поля L. З вправи 4.2 та наслідку 5.2 тоді випливає, що розширення $\mathsf{LM} = \mathsf{M}(\sqrt[n]{1})$ поля M є радикальним. Але тоді, очевидно, LM є радикальним роззширенням поля K, яке містить L. □

Теорема 5.4 (Критерій Галуа). *Рівняння $f(x) = 0$ є розв'язним у радикалах тоді і лише тоді, коли його група Галуа є розв'язною.*

Іншими словами, скінченне розширення Галуа L поля K можна вкласти у радикальне розширення тоді і лише тоді, коли група Галуа $\mathsf{G} = \mathsf{Aut}(\mathsf{L}/\mathsf{K})$ є розв'язною. Зауважимо ще, що, коли K

містить первісний корінь ступеня $n = [\mathsf{L} : \mathsf{K}]$ з одиниці, з наслідку 5.2 випливає, що в цьому випадку вже само L є радикальним розширенням. Проте в загальному випадку це, взагалі кажучи, не так (див. вправу 5.9 нижче).

Доведення. Нехай група G є розв'язною. Покладемо $\mathsf{K}' = \mathsf{K}(\sqrt[n]{1})$, де $n = [\mathsf{L} : \mathsf{K}] = |\mathsf{G}|$. За теоремою 5.3, поле K' можна вкласти у радикальне розширення P поля K. Більш того, завдяки теоремі 1.1 можна вважати, що P міститься в деякому розширенні поля L. Розглянемо тоді композит $\mathsf{L}' = \mathsf{LP}$. За теоремою 3.4 він є розширенням Галуа поля P з групою Галуа $\mathsf{G}^{\mathsf{L}\cap\mathsf{P}}$. Остання є розв'язною як підгрупа розв'язної групи G. Отже, за наслідком 5.2 поле L', а тому й L, можна занурити в радикальне розширення поля P, яке, звісно, буде й радикальним розширенням поля K.

Навпаки, нехай K міститься в радикальному розширенні M поля K. Тоді існує ланцюг проміжних підполів

$$\mathsf{K} = \mathsf{P}_0 \subset \mathsf{P}_1 \subset \mathsf{P}_2 \subset \ldots \subset \mathsf{P}_m = \mathsf{M},$$

в якому кожне P_i $(0 < i \leq m)$ – просте радикальне розширення P_{i-1}. Припустимо спочатку, що K містить первісний корінь з одиниці ступеня $N = [\mathsf{M} : \mathsf{K}]$, а тому й первісні корені з одиниці всіх ступенів $n_i = [\mathsf{P}_i : \mathsf{P}_{i-1}]$. Розв'язність групи G в цьому випадку доведемо індукцією за m.

Якщо $m = 1$, то внаслідок вправи 4.1 M є розширенням Галуа з циклічною групою Галуа F. Але тоді за теоремою 3.3 $\mathsf{G} \simeq \mathsf{F}/\mathsf{H}$, де $\mathsf{H} = \mathsf{F}^{\mathsf{L}}$, отже, G також є циклічною.

Припустимо, що твердження теореми є вірним для ланцюгів довжини $m - 1$. Розглянемо в M підполе $\mathsf{L}' = \mathsf{P}_1\mathsf{L}$. За теоремою 3.4 воно є розширенням Галуа поля P_1 з групою Галуа $\mathsf{H} = \mathsf{G}^{\mathsf{P}_1\cap\mathsf{L}}$. Але P_1 – розширення Галуа K з циклічною групою Галуа (вправа 4.1), отже, за теоремою 3.3 $\mathsf{P}_1 \cap \mathsf{L}$ – також розширення Галуа K з циклічною групою Галуа F. Застосувавши знову теорему 3.3, маємо, що H – нормальна підгрупа в G, причому $\mathsf{G}/\mathsf{H} \simeq \mathsf{F}$. Оскільки H є розв'язною за припущенням індукції, розв'язною є і вся група G (див. властивість 2 розв'язних груп, цитовану вище).

Нехай тепер K – довільне поле. Позначимо $\mathsf{K}' = \mathsf{K}(\sqrt[N]{1})$, $\mathsf{L}' = \mathsf{L}(\sqrt[N]{1}) = \mathsf{K}'\mathsf{L}$. За теоремою 3.4, L' – розширення Галуа

K' з групою Галуа $\mathsf{H} = \mathsf{G}^{\mathsf{K}'\cap\mathsf{L}}$. Але K' – розширення Галуа K з абелевою групою Галуа (див. вправу 4.2), звідки, як і вище, випливає, що H – нормальна підгрупа в G і фактор-група G/H абелева. Внаслідок властивості 2 розв'язних груп, наведеній вище, достатньо довести розв'язність групи H. Але L' міститься в розширенні $\mathsf{M}' = \mathsf{M}(\sqrt[N]{1})$ поля K'. Розглянемо в ньому ланцюг підполів

$$\mathsf{K}' = \mathsf{P}'_0 \subset \mathsf{P}'_1 \subset \mathsf{P}'_2 \subset \ldots \subset \mathsf{P}'_m = \mathsf{M}',$$

де $\mathsf{P}'_i = \mathsf{P}(\sqrt[N]{1})$. Кожне P'_i одержується з P'_{i-1} приєднанням кореня деякого многочлена $x^{n_i} - \alpha_i$. Тому з вправи 4.1 і теореми Лагранжа випливає, що P'_i є простим радикальним розширенням P'_{i-1}, ступінь якого ділить n_i, тобто, M' – радикальне розширення поля K', ступінь якого ділить N. Тоді з доведеного вище випливає, що група H є розв'язною, що і треба було довести. □

Нагадаємо (див. [6, с. 320]), що симетрична група $\mathfrak{S}_n$ при $n \geq 5$ не є розв'язною. Тому з теорем 5.4 і 4.5, а також вправи 4.10 випливають наступні результати.

Наслідок 5.5 (Теорема Руффіні–Абеля). *Загальне алгебричне рівняння ступеня $n \geq 5$ над довільним полем не є розв'язним у радикалах.*

Наслідок 5.6. *Для довільного $n \geq 5$ існують рівняння над полем раціональних чисел, які не є розв'язними в радикалах.*

Для *незвідних* многочленів означення розв'язності в радикалах можна дещо послабити, спираючись на наступне твердження.

Вправа 5.7. *Довільне радикальне розширення можна вкласти в радикальне розширення Галуа.*

Вказівка: Якщо L_1 і L_2 – два радикальні розширення, які містяться в деякому розширенні M, то їхній композит $\mathsf{L}_1\mathsf{L}_2$ також є радикальним розширенням.

Наслідок 5.8. *Якщо $p(x)$ – незвідний многочлен, то рівняння $p(x) = 0$ є розв'язним у радикалах тоді і лише тоді, коли воно має принаймні один розв'язок у деякому радикальному розширенні.*

Вправа 5.9. *Вкладіть поле $\mathbb{Q}(\sqrt[7]{1})$ у радикальне розширення поля $\mathbb{Q}$. Переконайтесь, що само L не є радикальним розширенням.*

ВКАЗІВКА: Група Галуа цього розширення є циклічною порядка 6, тому вона має лише дві нетривіальні підгрупи: порядків 2 і 3.

Розглянемо, нарешті, важливе для елементарної геометрії питання про розв'язність рівнянь у *квадратних радикалах*. Кажуть, що рівняння $f(x)=0$ є *розв'язним у квадратних радикалах*, якщо існує ланцюг полів

$$\mathsf{K}=\mathsf{P}_0\subset\mathsf{P}_1\subset\mathsf{P}_2\subset\ldots\subset\mathsf{P}_m=\mathsf{L},$$

такий що L містить поле розкладу многочлена $f(x)$ і $[\mathsf{P}_i:\mathsf{P}_{i-1}]=2$ для кожного $i=1,2,\ldots,m$. Очевидно, в цьому випадку P_i – квадратичне розширення P_{i-1}, тобто $\mathsf{P}_i=\mathsf{P}_{i-1}(\sqrt{\alpha_i})$ для деякого $\alpha_i\in\mathsf{P}_{i-1}$. Тому розширення L в цьому випадку зветься *квадратично-радикальним*.

ВПРАВА 5.10. *Доведіть, що рівняння є розв'язним у квадратних радикалах тоді і лише тоді, коли його група Галуа* G *є 2-групою, тобто* $|\mathsf{G}|=2^k$ *для деякого* k.

ВКАЗІВКИ: (i) Ступінь квадратично-радикального розширення є завжди 2^m для деякого m, тому, якщо поле розкладу вкладається у квадратично-радикальне, то $|\mathsf{G}|=2^k$.

(ii) Якщо $|\mathsf{G}|=2^k$, то в G є ланцюг підгруп

$$\mathsf{G}=\mathsf{G}_0\supset\mathsf{G}_1\supset\mathsf{G}_2\supset\ldots\supset\mathsf{G}_k=1,$$

де $|\mathsf{G}_i|=2^{k-i}$ (див. [**6**, с. 334]). Тому G_i – підгрупа індексу 2 в G_{i-1}, отже, нормальна (див. [**6**, с. 171]). Тоді за L можна прийняти поле розкладу $f(x)$, а за P_i – поле $\mathsf{L}^{\mathsf{G}_i}$.

Зауважимо, що з наміченого доведення випливає, зокрема, що довільне розширення Галуа ступеня 2^k є насправді квадратично-радикальним.

ВПРАВА 5.11. *Доведіть аналогічно вправі 5.7, що довільне квадратично-радикальне розширення можна вкласти у деяке квадратично-радикальне розширення Галуа. Виведіть з цього, що коли* L *є квадратично-радикальним розширенням, то будь-яке його проміжне підполе* P *також є квадратично-радикальним.*

ВКАЗІВКА (до другої частини): L можна вважати розширенням Галуа з групою Галуа G порядку 2^k. Тоді, якщо $\mathsf{H}=\mathsf{G}^{\mathsf{P}}$,

причому $|\mathsf{H}|=2^l$, то з [**11**, с. 55] випливає, що існує ланцюг підгруп

$$\mathsf{G}=\mathsf{G}_0\supset\mathsf{G}_1\supset\mathsf{G}_2\supset\ldots\supset\mathsf{G}_{k-l}=\mathsf{H},$$

в якому $(\mathsf{G}_{i-1}:\mathsf{G}_i)=2$ для всіх $i>0$. Тепер доведення завершується так само, як і в попередній вправі.

НАСЛІДОК 5.12. *Нехай* $p(x)$ *– незвідний многочлен над полем* K, α *– його корінь в якомусь розширенні поля* K. *Рівняння* $p(x)=0$ *є розв'язним у квадратних радикалах тоді і лише тоді, коли* $\mathsf{K}(\alpha)$ *є квадратично-радикальним розширенням* K.

Зокрема, якщо $\deg p(x)$ не є ступенем двійки, вказане рівняння не є розв'язним у квадратних радикалах.

ВПРАВА 5.13 (критерій Гаусса). *Доведіть, що рівняння* $x^n-1=0$ *є розв'язним у квадратних радикалах над полем раціональних чисел тоді і лише тоді, коли* $n=2^m l_1 l_2\ldots l_k$, *де* $l_1,l_2,\ldots,l_k$ *– попарно різні прості числа вигляду* $2^{2^r}+1$ *("прості числа Ферма").*

Геометрично це означає, що лише в цьому випадку правильний n-кутник можна побудувати циркулем та лінійкою.

ВКАЗІВКА: Скористайтеся тим, що многочлен поділу кола $\Phi_n(x)$ є незвідним над полем раціональних чисел (див. [**6**, с. 207]) і формулою для функції Ейлера $\phi(x)$.

Для полів характеристики $l>0$ питання про розв'язність рівнянь у радикалах треба дещо переформулювати, оскільки просте радикальне розширення $\mathsf{K}(\sqrt[l]{a})$ тут є несепарабельним. Для того, щоб зберегти аналогію з випадком характеристики 0, звичайно трохи збільшують клас "простих розширень". Саме, назвемо *простим* l*-розширенням* поля K характеристики $l>0$ поле $\mathsf{K}(\theta)$, де $\theta^l=\theta+a$, причому $a\in\mathsf{K}$, а $\theta\notin\mathsf{K}$. Розширення L назвемо *квазірадикальним*, якщо в ньому існує ланцюг проміжних підполів

$$\mathsf{K}=\mathsf{P}_0\subset\mathsf{P}_1\subset\mathsf{P}_2\subset\ldots\subset\mathsf{P}_m=\mathsf{L},$$

в якому кожне P_i $(i>0)$ є або простим радикальним, або простим l-розширенням поля P_{i-1}. Будемо тепер називати рівняння $f(x)=0$ *квазірозв'язним у радикалах*, якщо поле розкладу многочлена $f(x)$ можна занурити у квазірадикальне розширення

поля K. Наступний цикл вправ показує, що при такому означенні мають місце всі результати, аналогічні тим, які ми довели для полів характеристики 0. В усіх цих вправах вважається, що поля мають характеристику $l > 0$.

ВПРАВА 5.14. 1. *Доведіть, що коли θ – корінь многочлена $x^l - x - a$, то* всі *його корені – це $\theta, \theta+1, \theta+2, \ldots, \theta+l-1$. Зокрема, якщо цей многочлен не має коренів у полі K, то він незвідний над цим полем.*

2. *Доведіть, що просте l-розширення є розширенням Галуа, група Галуа якого – циклічна порядку l.*

3. *Доведіть, що й навпаки, кожне розширення Галуа, група Галуа якого – циклічна порядку l є простим l-розширенням.*
   ВКАЗІВКА: Розгляньте L як лінійний простір над K, а відображення $S : \alpha \mapsto \sigma(\alpha) - \alpha$, де σ – твірний групи Галуа, як лінійне перетворення цього простору. Очевидно, $S^l = 0$, причому $\ker S = \mathsf{K}$ – одновимірний підпростір. Тому жорданова нормальна форма перетворення S складається з однієї клітини Жордана. З цього випливає, що $\operatorname{Im} S = \ker S$. Зокрема, в полі L є такий елемент θ, що $\sigma(\theta) - \theta = 1$. Тоді легко переконатися, що $\theta^l - \theta \in \mathsf{K}$.

4. *Доведіть, що рівняння $f(x) = 0$ із* сепарабельним *многочленом $f(x)$ є квазірозв'язним у радикалах тоді і лише тоді, коли його група Галуа є розв'язною.*
   (Доведення практично повторює доведення теореми 5.4.)

Випадок несепарабельних рівнянь потребує деяких додаткових понять.

ВПРАВА 5.15. *Нехай L – скінченне розширення поля K. Доведіть еквівалентність наступних умов:*

1. *Це розширення нормальне і не має нетотожних автоморфізмів.*
2. *Кожен елемент з $\mathsf{L} \setminus \mathsf{K}$ є несепарабельним над K.*
3. $\mathsf{L} = \mathsf{K}(\alpha_1, \alpha_2, \ldots, \alpha_m)$, *де $\alpha_i^{l^k} \in \mathsf{K}$ для деякого показника k і всіх номерів i.*
4. *Знайдеться такий показник k, що $\alpha^{l^k} \in \mathsf{K}$ для всіх $\alpha \in \mathsf{K}$.*

Розширення, які задовольняють ці умови, звуться *чисто несепарабельними*. Відповідно, елемент α зветься *чисто несепарабельним* (над K), якщо $\alpha^{l^k} \in \mathsf{K}$ для деякого k.

ВКАЗІВКИ. 1⇒2: Скористайтеся вправою 2.4.

2⇒3: Якщо α – корінь незвідного многочлена $x^{nl} + a_1 x^{(n-1)l} + a_2 x^{(n-2)l} + \cdots + a_n$ і $a_{n-i} \neq 0$ для деякого i, яке не ділиться на l, то α^l – сепарабельний елемент.

3⇒4: Відображення $\alpha \mapsto \alpha^{l^k}$ є автоморфізмом поля L, який відображає підполе K в себе.

4⇒1 випливає з того, що $x^{l^k} - \alpha^{l^k} = (x - \alpha)^{l^k}$.

Очевидно, всі чисто несепарабельні розширення є радикальними.

ВПРАВА 5.16. 1. *Нехай L – довільне скінченне розширення поля K. Доведіть, що множина L_0 всіх його чисто несепарабельних елементів є підполем, причому L – сепарабельне розширення поля L_0. Підполе L_0 зветься* чисто несепарабельною частиною *розширення L.*

2. *Нехай розширення L нормальне і $\mathsf{G} = \operatorname{Aut}(\mathsf{L}/\mathsf{K})$. Доведіть, що $\mathsf{L}_0 = \mathsf{L}^{\mathsf{G}}$. Зокрема, L є розширенням Галуа поля L_0.*

3. *Нехай L – поле розкладу многочлена $f(x)$ над полем K. Доведіть, що рівняння $f(x) = 0$ є квазірозв'язним у радикалах тоді і лише тоді, коли група $\operatorname{Aut}(\mathsf{L}/\mathsf{K})$ є розв'язною.*

Алфавітний покажчик

Бібліографія

[1] [А] Артін Е. *Теорія Галуа.* – К., 1963.
[2] [Б] Бурбаки Б. *Алгебра: Многочлены и поля. Упорядоченные группы.* – М., 1965.
[3] [В] Ван дер Варден Б.Л. *Алгебра.* – М., 1976.
[4] [ДК] Дрозд Ю. А., Кириченко В. В. *Конечномерные алгебры.* – К., 1980.
[5] [Ка] Капланский И. *Введение в дифференциальную алгебру.* – М., 1959.
[6] [Ко] Кострикин А И. *Введение в алгебру.* – М., 1977.
[7] [Л] Ленг С. *Алгебра.* – М., 1968.
[8] [П] Постников М. М. *Теория Галуа.* – М., 1963.
[9] [С] Сушкевич А. К. *Основы высшей алгебры.* – М.; Л., 1932.
[10] [Ф] Фаддеев Д. К. *Лекции по алгебре.* – М., 1984.
[11] [Х] Холл М. *Теория групп.* – М., 1962.

Зміст

Навчальне видання

Юрій Анатолійович Дрозд

Теорія Галуа

Навчальний посібник
для студентів механіко-математичного факультету

Редактор Л.Л.Воронцова
Молодший редактор Н.Ю.Мельничук