Конспект лекцій зі спецкурсу “Скінченні поля”

Кочубінська Є.А.

2018

Зміст

Розділ 1

Короткі відомості з теорії полів

Базове припущення. *Студент знайомий з курсами лінійної алгебри і алгебри та теорії чисел, що читалися на першому та другому курсах.*

1.1 Характеристика поля

Поле F — це непорожня множина, на якій визначено дві бінарні дії $+$ та $\cdot$, що називаються *додаванням* та *множенням*, відповідно, яка містить два виділені елементи 1 та 0, $1 \neq 0$, і задовольняє умови

- $(F, +)$ — абелева група з нейтральним елементом 0;
- $F^* = (F \setminus \{0\}, \cdot)$ — абелева група з нейтральний елементом 1 (цю групу називають мультиплікативною групою поля);
- додавання та множення пов'язані дистрибутивними законами.

Нехай F — поле. Підмножина K поля F, яка сама є полем відносно заданих на F операцій, називається його *підполем*. У цьому випадку поле F називається *розширенням* поля K. Якщо $K \neq F$, то K називається *власним підполем* поля F.

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

Приклад 1.1. Простими полями є поля $\mathbb{Z}_p$ та $\mathbb{Q}$.

Перетин всіх підполів поля F є, очевидно, підполем поля F, яке називається *простим підполем* поля F.

Означення 1.1. *Найменше таке* $k \in \mathbb{N}$*, що*

$$\underbrace{1 + 1 + \ldots + 1}_{k} = 0,$$

називається характеристикою поля. Позначається $\operatorname{char} F$*. Якщо такого* k *не існує, то вважають, що* $\operatorname{char} F = 0$.

Твердження 1.1. *Характеристика поля є або простим числом, або 0. Характеристика скінченного поля завжди є простим числом.*

Доведення. Припустимо, що F — поле, характеристикою якого є складене число, нехай це число $n = kl$, де $k, l < n$. Тоді

$$n \cdot 1 = (kl) \cdot 1 = (k \cdot 1)(l \cdot 1) = .0$$

Оскільки в полі немає дільників нуля, то $k \cdot 1 = 0$ або $l \cdot 1 = 0$, що суперечить означенню характеристики поля.

Припустимо, що F — скінченне поле. Тоді в послідовності

$$0,\ 1,\ 1+1,\ 1+1+1,\ \ldots$$

деякі члени повинні повторюватись. Нехай для деяких $r > s$ $r \cdot 1 = s \cdot 1$. Тоді $(r-s) \cdot 1 = 0$. Отже, поле F має скінченну характеристику. □

Теорема 1.2. *1. Якщо характеристика поля F дорівнює простому числу p, то просте підполе поля F ізоморфне полю $\mathbb{Z}_p$.*

2. Якщо характеристика поля F дорівнює 0, то просте підполе поля F ізоморфне полю раціональних чисел $\mathbb{Q}$.

Доведення. 1. Нехай P — просте підполе поля F.

Нехай $\operatorname{char} F = p$. Тоді можемо визначити відображення

$$\Theta : \mathbb{Z}_p \to F$$

за правилом

$$\overline{r} \mapsto r \cdot 1, \quad (r = 0,\ 1,\ , \ldots, p-1).$$

Легко перевірити, що відображення Θ є ізоморфізмом між $\mathbb{Z}_p$ та $\operatorname{Im}\Theta$. Кожне підполе F містить елемент 1, а тому містить і $r \cdot 1 = \underbrace{1+1+\ldots+1}_{r}$.

Отже, поле $\operatorname{Im}\Theta$ міститься в кожному підполі поля F, а тому є його простим підполем:

$$P = \operatorname{Im}\Theta \simeq \mathbb{Z}_p.$$

Ізоморфізм Θ є єдиним, бо

$$\Theta(1) = 1 \Rightarrow \Theta(r) = \Theta(1+\ldots+1) = \Theta(1)+\ldots\Theta(1) = r \cdot 1.$$

2. Вправа. □

Наслідок 1.3. *Поле $\mathbb{Z}_p$ є єдиним полем, що складається з p елементів.*

Надалі єдине поле з p елементів позначатимемо $\mathbb{F}_p$.

Вправа 1.1. Якщо $\operatorname{char}\mathbb{F} = p$, то

1) $(a+b)^p = a^p + b^p$;

2) $(a+b)^{p^n} = a^{p^n} + b^{p^n}$ для всіх $n \geqslant 1$.

Отже, відображення $\mathbb{F} \longrightarrow \mathbb{F}$: $a \mapsto a^p$ — це гомоморфізм, який називається *ендоморфізмом Фробеніуса*. Якщо поле $\mathbb{F}$ скінченне, то це відображення буде автоморфізмом, який називається *автоморфізмом Фробеніуса*.

1.2 Розширення полів

У цьому підрозділі зібрано відомості про розширення полів, яку будуть потрібні для подальшого викладу.

Нехай K — підполе поля L, S — підмножина L. Перетин всіх підполів, що містять S, очевидно, є найменшим підполем L, яке містить K та S. Називатимемо його підполем поля L, породженим K та S (або породженим множиною S над K). Позначатимемо $K(S)$. Ясно, що $K(S)$ є розширенням поля K.

Якщо $S = \{\alpha_1, \alpha_2, \ldots, \alpha_k\}$, то писатимемо $F(\alpha_1, \alpha_2, \ldots, \alpha_k)$ для $F(S)$. Якщо множина S складається з одного елемента, то говорять, що $F(S)$ є простим розширенням поля F.

Очевидно, що поле L ми можемо розглядати як векторний простір над полем K. Позначимо $[L : K]$ — розмірність L як векторного простору над K. Ця розмірність називається *степенем розширення* L над K. Розширення називається скінченним, якщо $[L : K] < \infty$.

Теорема 1.4 (про башту розширень)**.** *Якщо L — скінченне розширення поля K, а M — скінченне розширення поля L, тоді M —скінченне розширення поля K, причому*

$$[M : K] = [M : L][L : K].$$

Нехай K — поле, L — розширення поля K. Елемент $\alpha \in L$ називається *алгебраїчним* над полем K, якщо α є коренем деякого многочлена $f(x) \in K[x]$. Розширення L поля K називається *алгебраїчним*, якщо всі елементи поля L є алгебраїчними над полем K.

Теорема 1.5. *Кожне скінченне розширення є алгебраїчним.*

Означення 1.2. *Нехай $L \supset K$ — розширення, $\alpha \in L$ — алгебраїчний над K елемент. Мінімальним многочленом елемента α над полем K називається унітарний многочлен $m_\alpha(x) \in K[x]$ найменшого степеня, який анулює α, тобто $m_\alpha(\alpha) = 0$.*

Вправа 1.2. 1. Мінімальний многочлен елемента α ділить довільний анулюючий многочлен елемента α.

2. Мінімальний многочлен незвідний.

3. Мінімальний многочлен визначений однозначно.

Вправа 1.3. Многочлен $f(x) \in K[x]$ є мінімальним для елемента $\alpha \in L$, $L \supset K$, якщо виконується один з наборів умов

1) f — унітарний многочлен найменшого степеня, який анулює α;

2) f — унітарний, $f(\alpha) = 0$ і f ділить будь–який інщий анулюючий многочлен елемента α;

3) f — унітарний, незвідний та $f(\alpha) = 0$.

Теорема 1.6 (про будову простих алгебраїчних розширень)**.** *Нехай $K \subset K(\alpha)$ — просте алгебраїчне розширення, $m_\alpha(x)$ — мінімальний многочлен елемента α. Тоді*

1) $K(\alpha) \simeq K[x]/(m_\alpha(x))$*, зокрема*

$$K(\alpha) = \left\{a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_{n-1}\alpha^{n-1} \mid a_i \in K\right\};$$

2) $[K(\alpha) : K] = \deg m_\alpha$*;*

3) $\left\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\right\}$ *є базисом $K(\alpha)$ над K.*

Приклад 1.7. Теорема 1.6 дає один зі способів побудови скінченного поля.

Розглянемо многочлен $f(x) = x^2 + x + 1 \in \mathbb{F}_2[x]$. Легко перевірити, що він незвідний над полем $\mathbb{F}_2$. Тоді факторкільце $\mathbb{F}_2[x]/(f)$ є полем. Його елементами є класи суміжності $\{(f), 1 + (f), x + (f), x + 1 + (f)\}$.

Опишемо тепер елементи цього поля дещо інакше. Нехай α — корінь многочлена $f(x) = x^2 + x + 1 \in \mathbb{F}_2[x]$ у деякому розширенні поля $\mathbb{F}_2$, тобто $\alpha^2 + \alpha + 1 = 0$. Многочлен f є мінімальним для елемента α. Тоді $\mathbb{F}_2(\alpha) = \{0, 1, \alpha, \alpha + 1\}$ — просте алгебраїчне розширення поля $\mathbb{F}_2$. Базисом розширення $\mathbb{F}_2(\alpha)$ є $\{1, \alpha\}$, степінь розширення дорівнює $[\mathbb{F}_2(\alpha) : \mathbb{F}_2] = 2$. □

Означення 1.3. *Підполе L поля $\mathbb{C}$ називається полем розкладу многочлена $f(x) \in K[x]$, якщо $L \supset K$ та*

1) *f розкладається над L у добуток лінійних множників;*

2) *якщо $K \subset L' \subset L$ та f розкладається над L', то $L' = L$.*

Теорема 1.8 (Існування та єдиність поля розкладу)**.** *Якщо K — деяке поле та f — многочлен з $K[x]$, то існує поле розкладу многочлена f над полем K. Будь-які два поля розкладу многочлена f над K ізоморфні та відповідний ізоморфізм не змінює елементи поля K і здійснює деяку перестановку коренів многочлена.*

Розділ 2

Характеризація скінченних полів

Лема 2.1. *Нехай F — скінченне поле, яке містить підполе K з q елементів. Тоді F складається з q^m елементів, де $m = [F : K]$.*

Доведення. Оскільки F — скінченне поле, то його можна розглядати як скінченновимірний векторний простір над полем K. Нехай його розмірність над K дорівнює m, а $b_1, b_2, \ldots, b_m$ — базис F над K. Тоді кожний елемент $b \in F$ єдиним чином зображується у вигляді

$$b = k_1 b_1 + k_2 b_2 + \ldots k_m b_m,$$

де $k_1, k_2, \ldots, k_m \in K$. □

Теорема 2.2. *Нехай F — скінченне поле. Тоді воно складається з p^n елементів, де просте число p є характеристикою поля F, а $n \in \mathbb{N}$ є степенем поля F над його простим підполем.*

Доведення. Оскільки F — скінченне, то $\operatorname{char} F = p$, де p — деяке просте число. Тому просте підполе поля F ізоморфне полю $\mathbb{F}_p$, а, отже, містить p елементів. З леми 2.1 випливає, що $|F| = p^n$. □

Лема 2.3. *Якщо F — скінченне поле з q елементів, то для кожного $a \in F$ виконується $a^q = a$.*

Доведення. Оскільки F — поле, то його мультиплікативна група F^* складається з $q - 1$ елементів. Тому для довільного $a \in F^*$ має місце рівність $a^{q-1} = 1$. Оскільки $0^q = 0$, то маємо твердження леми. □

Лема 2.4. *Якщо F — скінченне поле з q елементів, K — підполе поля F, то многочлен $x^q - x \in K[x]$ розкладається над F наступним чином:*

$$x^q - x = \prod_{a \in F} (x - a),$$

та F є полем розкладу многочлена $x^q - x$ над полем K.

Доведення. Оскільки многочлен $x^q - x$ має степінь q, то він має щонайбільше q коренів у полі F. З леми 2.3 нам відомі ці корені: ними є всі елементи поля F. Таким чином, многочлен $x^q - x$ розкладається над F вказаним способом і не може розкладатися над жодним меншим полем. □

Теорема 2.5 (існування та єдиність скінченних полів)**.** *Для кожного простого числа p та кожного натурального числа n існує скінченне поле з p^n елементів. Кожне скінченне поле з $q = p^n$ елементів ізоморфне полю розкладу многочлена $x^q - x$ над полем $\mathbb{F}_p$.*

Доведення. Існування. Нехай $q = p^n$. Розглянемо многочлен $f(x) = x^q - x$ над полем $\mathbb{F}_p$. Нехай F — це поле розкладу многочлена $f(x)$ над $\mathbb{F}_p$. Похідна $f'(x) = qx^{q-1} - 1 = -1 \neq 0$ сталим многочленом з $\mathbb{F}_p$, а тому не має спільних коренів з $f(x)$. Отже, многочлен $x^q - x$ має q різних коренів в полі F.

Покладемо

$$S = \{a \in F \mid a^q - a = 0\}.$$

Множина S має властивості:

1) S містить 0 та 1;

2) якщо $a, b \in S$, то $(a-b)^q = a^q - b^q = a - b$, звідки $a - b \in S$;

3) для $a, b \in S$, $b \neq 0$, маємо $(ab^{-1})^q = a^q b^{-q} = ab^{-1}$, отже, $ab^{-1} \in S$.

Таким чином, множина S є полем.

З іншого боку, многочлен $x^q - x$ повинен цілком розкладатися в S, оскільки S містить всі його корені. Таким чином, $S = F$, а оскільки S складається з q елементів, то F є скінченним полем з q елементів.

Єдиність. Нехай F — скінченне поле, яке складається з $q = p^n$ елементів. Тоді $\operatorname{char} F = p$, а тому F містить в якості підполя $\mathbb{F}_p$. З леми 2.4 випливає, що F є полем розкладу многочлена $x^q - x$ над полем $\mathbb{F}_p$. Твердження теореми випливає тепер з єдиності поля розкладу многочлена. □

Ця теорема дає змогу говорити про цілком визначене скінченне поле з q елементів (або *поле Галуа* з q елементів). Позначатимемо його надалі через $\mathbb{F}_q$. Зауважимо, що поширеним є також позначення $GF(q)$.

Наслідок 2.6. *Скінченні поля, які складаються з однакової кількості елементів, ізоморфні.*

Теорема 2.7 (про скінченні підгрупи мультиплікативної групи поля)**.** *Кожна скінченна підгрупа мультиплікативної групи поля є циклічною.*

Перш ніж доводити теорему 2.7, нагадаємо поняття експоненти групи та її властивості.

Означення 2.1. *Експонентою групи G називається найменше таке число $n \in \mathbb{N}$, що $g^n = 1$ для всіх $g \in G$.*

Позначатимемо експоненту групи через $\mathrm{Exp}(G)$.

Приклад 2.8. 1. Експонента скінченної циклічної групи C_n порядку n дорівнює n.

2. Експонента діедральної групи $\mathcal{D}_4$ дорівнює 8.

3. Експонента симетричної групи $\mathcal{S}_3$ степеня 3 дорівнює 6.

Лема 2.9. 1. *Експонента скінченної групи не перевищує її порядок.*

2. *У скінченній абелевій групі експонента дорівнює найменшому спільному кратному порядків її елементів.*

3. *Скінченна абелева група — циклічна тоді і лише тоді, коли її експонента дорівнює порядку.*

Доведення. Пункти 1 та 2 леми випливають з теореми Лагранжа.

3. Нехай порядок абелевої групи A дорівнює n. За основною теоремою про скінченні абелеві групи A ізоморфна прямому добутку своїх примарних підгруп

$$A \cong C_{p_1^{l_1}} \times \ldots \times C_{p_1^{l_t}} \times \ldots \times C_{p_s^{j_1}} \times \ldots \times C_{p_s^{j_r}},$$

де $p_1, p_2, \ldots, p_s$ — це список всіх різних простих дільники числа n, а $p_1^{l_1+\ldots+l_t} \cdot \ldots \cdot p_s^{j_1+\ldots+j_r} = n$. Не обмежуючи загальності, можемо вважати, що $l_1 \geqslant \ldots \geqslant l_t, \ldots, j_1 \geqslant \ldots \geqslant j_r$.

За пунктом 2 експонента групи A дорівнює добутку $p_1^{l_1} \ldots p_s^{j_1}$. Отже, $\mathrm{Exp}(G) = |G|$ тоді і тільки тоді, коли $t = \ldots = r = 1$.

Нагадаємо, що $C_{mk} \cong C_m \times C_k$ тоді і лише тоді, коли $(m, k) = 1$

Необхідність. Нехай A — циклічна група. Припустимо, що $t \geqslant 2$. У цьому випадку циклічна група A містить нециклічну підгрупу. Отже, отримали суперечність.

Достатність. Нехай $|A| = \mathrm{Exp}\, A$. У цьому випадку $t = \ldots = r = 1$, а тому

$$C_{p_1^{l_1}} \times \ldots \times C_{p_s^{j_1}} \cong C_{p_1^{l_1} \ldots p_s^{j_1}}. \quad \square$$

Доведення теореми 2.7. Нехай F^* — мультиплікативна підгрупа поля F, G — її скінченна підгрупа. Покажемо, що $|G| = \mathrm{Exp}(G)$. Нехай $|G| = n$, $\mathrm{Exp}(G) = k$. Очевидно, що $k \leqslant n$. За означенням експоненти кожний елемент $g \in G$ є коренем рівняння $x^k - 1 = 0$. Кількість коренів рівняння не перевищує його степінь, тому $n \leqslant k$. Таким чином, $k = n$, і за лемою 2.9 група G є циклічною. □

Наслідок 2.10 (Теорема про мультиплікативну підгрупу скінченного поля)**.** *Мультиплікативна група $\mathbb{F}_q^*$ довільного скінченного поля $\mathbb{F}_q$ є циклічною.*

Означення 2.2. *Твірний елемент мультиплікативної групи скінченного поля називається примітивним елементом поля.*

Теорема 2.11. *Нехай $\mathbb{F}_q$ — скінченне поле, $\mathbb{F}_r$ — його скінченне розширення. Тоді $\mathbb{F}_r$ є простим алгебраїчним розширенням поля $\mathbb{F}_q$, причому в якості твірного елемента цього простого розширення можна брати будь-який примітивний елемент поля $\mathbb{F}_r$.*

Доведення. Нехай ζ — довільний примітивний елемент поля $\mathbb{F}_r$. Тоді очевидно, що $\mathbb{F}_q(\zeta) \subset \mathbb{F}_r$. З іншого боку, поле $\mathbb{F}_q(\zeta)$ містить 0 та всі степені елемента ζ, а, отже, всі елементи поля $\mathbb{F}_r$. Таким чином, $\mathbb{F}_q(\zeta) = \mathbb{F}_r$. □

Наслідок 2.12. *Для кожного скінченного поля $\mathbb{F}_q$ і кожного $n \in \mathbb{N}$ в кільці $\mathbb{F}_q[x]$ існує незвідний многочлен степеня n.*

Доведення. Нехай $\mathbb{F}_r$ — розширення поля $\mathbb{F}_q$ порядку q^n, отже, степінь розширення $[\mathbb{F}_r : \mathbb{F}_q] = n$. За теоремою 2.11, існує такий елемент $\zeta \in \mathbb{F}_r$, що $\mathbb{F}_r = \mathbb{F}_q(\zeta)$. З властивостей мінімального многочлена маємо, що мінімальний многочлен ζ над $\mathbb{F}_q$ є незвідним многочленом в $\mathbb{F}_q[x]$ степеня n. □

Приклад 2.13. 1. Розглянемо скінченне поле $\mathbb{F}_4 = \mathbb{F}_2(\alpha)$, де α — корінь незвідного над $\mathbb{F}_2$ многочлена $x^2 + x + 1$, тобто $\alpha^2 + \alpha + 1 = 0$. Тоді елементи α та $\alpha + 1$ є примітивними елементами поля $\mathbb{F}_4$. Дійсно, $\alpha^2 = \alpha^2 + \alpha + 1 + \alpha + 1 = \alpha + 1$, $\alpha^3 = 1$. Аналогічна перевірка для $\alpha + 1$.

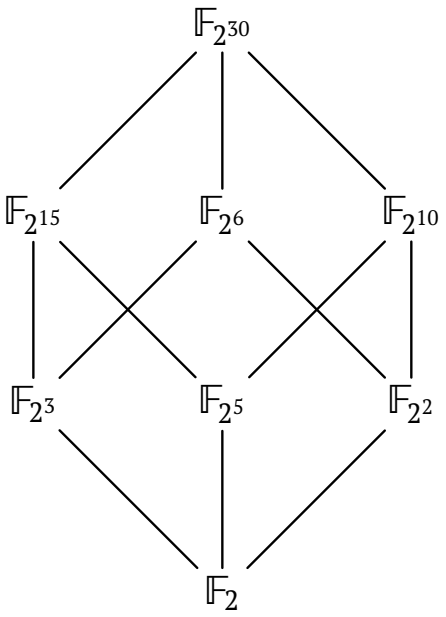
2. Розглянемо скінченне поле $\mathbb{F}_9 = \mathbb{F}_3(\beta)$, де β — корінь незвідного над $\mathbb{F}_3$ многочлена $x^2 + 1 = 0$. У цьому випадку β не є примітивним елементом поля $\mathbb{F}_9$, бо $\beta^4 = 1$, отже, не породжує поле $\mathbb{F}_9$.

Теорема 2.14 (критерій підполя)**.** *Нехай $\mathbb{F}_q$ — скінченне поле з $q = p^n$ елементів (p — просте число). Тоді кожне підполе поля $\mathbb{F}_q$ має порядок p^m, де m є додатним дільником числа n. Навпаки, якщо m — додатний дільник числа n, то існує рівно одне підполе поля $\mathbb{F}_q$, що складається з p^m елементів.*

Доведення. Зрозуміло, що будь-яке підполе поля $\mathbb{F}_q$ має порядок p^m для деякого $m \in \mathbb{N}$, $m \leqslant n$. З леми 2.1 випливає, що число $q = p^n$ повинно бути степенем числа p^m, отже, m обов'язково ділить n.

Навпаки, якщо m — додатний дільник числа n, то $(p^m - 1)|(p^n - 1)$. Отже, многочлен $x^{p^m-1} - 1$ ділить многочлен $x^{p^n-1} - 1$ в $\mathbb{F}_p[x]$. Таким чином, $x^{p^m} - x$ ділить многочлен $x^{p^n} - x$ в $\mathbb{F}_p[x]$. Звідси випливає, що кожний корінь многочлена $x^{p^m} - x$ є коренем многочлена $x^q - x$, а тому належить полю $\mathbb{F}_q$. Тому поле $\mathbb{F}_q$ повинно містити в якості підполя поле розкладу многочлена $x^{p^m} - x$ над $\mathbb{F}_p$. З доведення теореми 2.5 випливає, що таке поле розкладу має порядок p^m. Якби поле $\mathbb{F}_q$ містило два різних підполя порядку p^m, то ці два підполя містили б у сукупності більше за p^m коренів многочлена $x^{p^m} - x$ в полі $\mathbb{F}_q$, що неможливо. □

Приклад 2.15. Зобразимо діаграму підполів поля $\mathbb{F}_{2^{30}}$:



Розділ 3

Незвідні многочлени над скінченними полями

3.1 Корені незвідних многочленів

Лема 3.1. *Нехай $f(x) \in \mathbb{F}_q[x]$ — незвідний многочлен над скінченним полем $\mathbb{F}_q$ і нехай α — корінь $f(x)$ в деякому розширенні поля $\mathbb{F}_q$. Тоді для многочлена $h(x) \in \mathbb{F}_q[x]$ рівність $h(\alpha) = 0$ виконується тоді і лише тоді, коли $f(x)$ ділить $h(x)$.*

Доведення. Нехай a — старший коефіцієнт многочлена $f(x)$. Покладемо $g(x) = a^{-1}f(x)$. Тоді $g(x)$ — нормований незвідний многочлен з $\mathbb{F}_q[x]$, причому $g(\alpha) = 0$. Звідси випливає, що $g(x)$ — мінімальний многочлен елемента α над $\mathbb{F}_q$. □

Лема 3.2. *Нехай $f \in \mathbb{F}_q[x]$ — незвідний многочлен степеня m над полем $\mathbb{F}_q$. Тоді $f(x)$ ділить многочлен $x^{q^n} - x$ тоді і лише тоді, коли m ділить n.*

Доведення. Необхідність. Припустимо, що многочлен $f(x)$ ділить $x^{q^n} - x$. Нехай α — деякий корінь многочлена $f(x)$ полі розкладу цього многочлена над $\mathbb{F}_q$. Тоді $\alpha^{q^n} = \alpha$, що дає $\alpha \in \mathbb{F}_{q^n}$. Отже, просте розширення $\mathbb{F}_q(\alpha)$ поля $\mathbb{F}_q$ є підполем поля $\mathbb{F}_{q^n}$. Оскільки $[\mathbb{F}_q(\alpha) : \mathbb{F}_q] = m$ і $[\mathbb{F}_{q^n}(\alpha) : \mathbb{F}_q] = n$, то з теореми 1.4 (про башту розширень) випливає, що m ділить n.

Достатність. Якщо m ділить n, то з теореми 2.14 випливає, що поле $\mathbb{F}_{q^n}$ містить $\mathbb{F}_{q^m}$ в якості підполя. Якщо α — деякий корінь многочлена $f(x)$ у полі розкладу цього многочлена над $\mathbb{F}_q$, то $[\mathbb{F}_q(\alpha) : \mathbb{F}_q] = m$, так що $\mathbb{F}_q(\alpha) = \mathbb{F}_{q^m}$. Отже, $\alpha \in \mathbb{F}_{q^n}$, тому $\alpha^{q^n} = \alpha$. Таким чином, α — корінь многочлена $x^{q^n} - x \in \mathbb{F}_q[x]$. З леми 3.1 випливає, що $f(x)$ ділить $x^{q^n} - x$. □

Тепер ми можемо описати множину коренів незвідного многочлена.

Теорема 3.3. *Якщо $f \in \mathbb{F}_q(x)$ — незвідний многочлен степеня m, то в полі $\mathbb{F}_{q^m}$ міститься будь-який корінь α многочлена f. Більше того, всі корені*

многочлена f є простими, ними є m різних елементів поля $\mathbb{F}_{q^m}$:

$$\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{m-1}}.$$

Доведення. Нехай α є коренем многочлена $f(x)$ у полі розкладу цього многочлена над $\mathbb{F}_q$. Тоді з властивостей мінімального многочлена випливає, що $[\mathbb{F}_q(\alpha) : \mathbb{F}_q] = m$. Отже, $\mathbb{F}_q(\alpha) = \mathbb{F}_{q^m}$, зокрема, $\alpha \in \mathbb{F}_{q^m}$.

Доведемо тепер, що коли $\beta \in \mathbb{F}_{q^m}$ — корінь деякого многочлена f, то β^q — теж корінь цього многочлена. Нехай f записаний у вигляді

$$f(x) = a_m x^m + \ldots + a_1 x + a_0,$$

$a_i \in \mathbb{F}_q$, $0 \leqslant i \leqslant m$. Врахувавши лему 2.3 одержимо

$$\begin{aligned} f(\beta^q) &= a_m \beta^{qm} + \ldots + a_1 \beta^q + a_0 = \\ &= a_m^q \beta^{qm} + \ldots + a_1^q \beta^q + a_0^q = \\ &= (a_m \beta^m + \ldots + a_1 \beta + a_0)^q = f(\beta)^q = 0. \end{aligned}$$

Звідси маємо, що елементи $\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{m-1}}$ є коренями многочлена f. Лишилося довести, що ці елементи різні. Припустимо зворотне. Тоді $\alpha^{q^j} = \alpha^{q^k}$ для деяких цілих j і k, $0 \leqslant j < k \leqslant m-1$. Піднісши цю рівність до степеня q^{m-k}, одержимо

$$\alpha^{q^{m-k+j}} = \alpha^{q^m} = \alpha.$$

Тоді з леми 3.1 випливає, що $f(x)$ ділить $x^{q^{m-k+j}} - x$, а за лемою 3.2 це можливо лише у випадку, коли число m ділить $m - k + j$. Оскільки $0 < m - k + j < m$, то приходимо до суперечності. □

Наслідок 3.4. *Якщо $f \in \mathbb{F}_q[x]$ — незвідний многочлен степеня m, то його полем розкладу над полем $\mathbb{F}_q$ є $\mathbb{F}_{q^m}$.*

Доведення. З теореми 3.3 випливає, що многочлен f цілком розкладається в полі $\mathbb{F}_{q^m}$. При цьому для деякого кореня α многочлена f маємо рівність $\mathbb{F}_q(\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{m-1}}) = \mathbb{F}_q(\alpha)$. Але з доведення теореми 3.3 випливає, що $\mathbb{F}_q(\alpha) = \mathbb{F}_{q^m}$. □

Наслідок 3.5. *Поля розкладу будь-яких двох незвідних многочленів одного і того самого степеня з кільця $\mathbb{F}_q[x]$ ізоморфні.*

Пізніше побачимо, що елементи α^i, які з'являються у доведення цієї теореми, виникають досить часто у теорії полів.

3.2 Функція Мебіуса та незвідні многочлени

Теорема 3.6. *Для довільних скінченного поля $\mathbb{F}_q$ та натурального числа n добуток всіх унітарних незвідних многочленів над $\mathbb{F}_q$, степінь яких ділить n, дорівнює $x^{q^n} - x$.*

Доведення. За лемою 3.2 незвідними унітарними многочленами над $\mathbb{F}_q$, які з'являються в канонічному розкладі $g(x) = x^{q^n} - x$, є в точності ті, степені яких ділять n. Оскільки $g' = -1$, то g не має кратних коренів в своєму полі розкладу над $\mathbb{F}_q$. Таким чином, кожний незвідний унітарний многочлен над $\mathbb{F}_q$, степінь якого ділить n, з'являється рівно один раз в канонічному розкладі g над $\mathbb{F}_q$. □

Приклад 3.7. Візьмемо $q = n = 2$. Незвідними унітарними многочленами над $\mathbb{F}_2$, степінь яких ділить 2, є x, $x+1$, x^2+x+1. Неважко перевірити, що $x(x+1)(x^2+x+1) = x^4 + x = x^4 - x$. □

Наслідок 3.8. *Якщо $N_q(d)$ — це кількість унітарних незвідних многочленів в $\mathbb{F}_q[x]$ степеня d, тоді*

$$q^n = \sum_{d|n} dN_q(d) \quad \text{для всіх } n \in \mathbb{N},$$

сума береться по всім додатним дільникам n.

Доведення випливає з теореми 3.3 шляхом порівняння степеня многочлена $g = x^{q^n} - x$ з загальним степенем розкладу g. □.

Цей наслідок дає змогу вивести явну формулу для знаходження числа незвідних унітарних многочленів заданого степеня над полем $\mathbb{F}_q$.

Означення 3.1. *Функція Мебіуса μ — це функція на множині натуральних чисел, яка задається правилом*

$$\mu(n) = \begin{cases} 1, & \text{якщо } n = 1 \\ (-1)^k, & \text{якщо } n \text{ добуток } k \text{ різних простих} \\ 0, & \text{якщо } n \text{ ділиться на квадрат простого числа.} \end{cases}$$

Приклад 3.9. $\mu(5) = -1$, $\mu(35) = 1$, $\mu(25) = 0$. □

Лема 3.10. *Для $n \in \mathbb{N}$ функція Мьобіуса задовольняє рівність*

$$\sum_{d|n} \mu(d) = \begin{cases} 1, & \text{якщо } n = 1 \\ 0, & \text{якщо } n > 1 \end{cases}.$$

Доведення. Для $n = 1$ твердження очевидне.

Для $n > 1$ досить розглянути випадки, коли для додатних дільників d числа n $\mu(d) \neq 0$, а саме: такі d, для яких $d = 1$ або d є добутком різних простих чисел. Якщо $p_1, p_2, \ldots, p_k$ — різні прості дільника числа n, то

$$\sum_{d|n} \mu(d) = \mu(1) + \sum_{i=1}^{k} \mu(p_i) + \sum_{1 \leqslant i_1 < i_2 \leqslant k} \mu(p_{i1} p_{i2}) + \ldots + p_1 p_2 \ldots p_k =$$
$$= 1 + \binom{k}{1}(-1) + \binom{k}{2}(-1)^2 + \ldots + \binom{k}{k}(-1)^k = (1 + (-1))^k = 0.$$

□

Теорема 3.11 (формула обернення Мебіуса)**.** ***Адитивна версія.*** *Нехай G — абелева група з адитивною дією. Нехай h та H — дві функції з множини натуральних чисел в групу G. Тоді*

$$H(n) = \sum_{d|n} h(d) \text{ для всіх } n \in \mathbb{N} \tag{3.1}$$

тоді і лише тоді, коли

$$h(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) H(d) = \sum_{d|n} \mu(d) H\left(\frac{n}{d}\right) \text{ для всіх } n \in \mathbb{N}. \tag{3.2}$$

Мультиплікативна версія. *Нехай G — абелева група з мультиплікативною дією. Нехай h та H — дві функції з множини натуральних чисел в групу G. Тоді*

$$H(n) = \prod_{d|n} h(d) \text{ для всіх } n \in \mathbb{N} \tag{3.3}$$

тоді і лише тоді, коли

$$h(n) = \prod_{d|n} H\,(d)^{\mu\left(\frac{n}{d}\right)} = \prod_{d|n} H\left(\frac{n}{d}\right)^{\mu(d)} \text{ для всіх } n \in \mathbb{N}. \tag{3.4}$$

Доведення. Адитивна версія. Доведемо в один бік. Припустимо, що має місце перша рівність. Тоді

$$\sum_{d|n} \mu\left(\frac{n}{d}\right) H(d) = \sum_{d|n} \mu(d) H\left(\frac{n}{d}\right) = \sum_{d|n} \mu(d) \sum_{c|\frac{n}{d}} h(c) =$$
$$= \sum_{c|n} \sum_{d|\frac{n}{c}} \mu(d) h(c) = \sum_{c|n} h(c) \sum_{d|\frac{n}{c}} \mu(d) = h(n).$$

□

Теорема 3.12. *Кількість $N_q(n)$ незвідних унітарних многочленів в $\mathbb{F}_q[x]$ степеня n дорівнює*

$$N_q(n) = \frac{1}{n}\sum_{d|n}\mu\left(\frac{n}{d}\right)q^d = \frac{1}{n}\sum_{d|n}\mu(d)\,q^{\frac{n}{d}}.$$

Доведення. Застосуємо адитивну версію формули обернення Мебіуса до групи $G = (\mathbb{Z}, +)$. Покладемо $h(n) = nN_q(n)$ та $H(n) = q^n$ для всіх $n \in \mathbb{N}$. За наслідком 3.8 рівність (3.1) виконується, з чого випливає твердження теореми. □

Приклад 3.13. Знайти кількість незвідних унітарних многочленів степеня 12 над полем $\mathbb{F}_{12}$.

За теоремою 3.12 маємо

$$\begin{aligned}
N_2(12) &= \frac{1}{12}\sum_{d|12}\mu\left(\frac{12}{d}\right)q^d = \\
&= \frac{1}{12}\left(2^{12}\mu(1) + 2^6\mu(2) + 2^4\mu(3) + 2^3\mu(4) + v\,\mu(6) + 2\mu(12)\right) = \\
&= \frac{1}{12}\left(1\cdot 2^{12} + (-1)\cdot 2^6 + (-1)\cdot 2^4 + 0\cdot 2^3 + 1\cdot 2^2 + 0\cdot 2\right) = \\
&= \frac{1}{12}(4096 - 64 - 16 + 4) = 335. \quad \square
\end{aligned}$$

Теорема 3.14. *Добуток $I(q, n; x)$ всіх незвідних над $\mathbb{F}_q$ многочленів степеня n дорівнює*

$$I(q, n; x) = \prod_{d|n}\left(x^{q^d} - x\right)^{\mu\left(\frac{n}{d}\right)} = \prod_{d|n}(x^{q^{\frac{n}{d}}} - x)^{\mu(d)}.$$

Доведення. За теоремою 3.6

$$x^{q^n} - x = \prod_{d|n} I(q, d; x).$$

Застосуємо формулу обернення Мебіуса до мультиплікативної групи всіх ненульових раціональних функцій над $\mathbb{F}_q$. Поклавши $h(n) = I(q, n; x)$ та $H(n) = x^{q^n} - x$, одержимо потрібну формулу. □

Приклад 3.15. Знайти добуток незвідних унітарних незвідних многочленів над полем $\mathbb{F}_2$ a) степеня 4; b) степеня 12.

Обчислимо добутки, використовуючи теорему 3.14:

$$I(2,4) = (x^{16}-x)^{\mu(1)}(x^4-x)^{\mu(2)}(x^2-x)^{\mu(4)} = (x^{16}-x)^1(x^4-x)^{-1}(x^2-x)^0 =$$
$$= \frac{x^{15}-1}{x^3-1} = x^{12}+x^9+x^6+x^3+1;$$

$$I(2,12) = \prod_{d|12}(x^{2^d}-x)^{\mu\left(\frac{12}{d}\right)} =$$
$$= (x^{4096}-x)^{\mu(1)}(x^{64}-x)^{\mu(2)}(x^{16}-x)^{\mu(3)}(x^8-x)^{\mu(4)}(x^4-x)^{\mu(6)}(x^2-x)^{\mu(12)} =$$
$$= (x^{4096}-x)^1(x^{64}-x)^{-1}(x^{16}-x)^{-1}(x^8-x)^0(x^4-x)^1(x^2-x)^0 =$$
$$= \frac{(x^{4096}-x)(x^4-x)}{(x^{64}-x)(x^{16}-x)}. \quad \square$$

Розділ 4

Сліди та норми

4.1 Автоморфізми та спряжені елементи

Означення 4.1. *Нехай $\mathbb{F}_{q^m}$ — розширення поля $\mathbb{F}_q$, нехай $\alpha \in \mathbb{F}_{q^m}$. Тоді елементи*

$$\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{m-1}}$$

називаються спряженими з елементом α відносно поля $\mathbb{F}_q$.

Зауваження 4.1. 1. Спряжені з $\alpha \in \mathbb{F}_{q^m}$ відносно поля $\mathbb{F}_q$ елементи різні тоді і лише тоді, коли степінь мінімального многочлена $m_\alpha(x)$ дорівнює m.

2. В іншому разі, степінь d мінімального многочлена $m_\alpha(x)$ над $\mathbb{F}_q$ є власним дільником числа m, і тоді серед спряжених з α відносно поля $\mathbb{F}_q$ різними будуть лише елементи $\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{d-1}}$, кожний яких повторюється в ряду спряжених m/d разів.

Теорема 4.1. *Елементи, які спряжені з елементом $\alpha \in \mathbb{F}_q^*$ відносно довільного підполя $\mathbb{F}_q$, мають один і той самий порядок в групі $\mathbb{F}_q^*$.*

Доведення. У кожній циклічній групі $\langle a \rangle$ порядку n елемент a^k породжує підгрупу порядку $\frac{n}{(k,n)}$. Крім того, кожний степінь характеристики поля $\mathbb{F}_q$ взаємно простий з порядком $q-1$ групи $\mathbb{F}_q^*$. □

Наслідок 4.2. *Якщо α — примітивний елемент поля $\mathbb{F}_q$, то примітивними також будуть і всі спряжені з ним відносно будь-якого підполя елементи.*

Приклад 4.3. Нехай $\alpha \in \mathbb{F}_{16}$ — корінь многочлена $f(x) = x^4+x+1 \in \mathbb{F}_2[x]$. Тоді спряженими з α відносно поля $\mathbb{F}_2$ будуть елементи

$$\alpha,\ \alpha^2,\ \alpha^4 = \alpha + 1,\ \alpha^8 = \alpha^2 + 1,$$

кожний з яких є примітивним елементом поля $\mathbb{F}_{16}$. Спряженими з α відносно поля $\mathbb{F}_4$ є лише елементи α та $\alpha^4 = \alpha + 1$. □

Теорема 4.4 (про автоморфізми скінченного поля)**.** *Різними автоморфізмами поля $\mathbb{F}_{q^m}$ над $\mathbb{F}_q$ є відображення*

$$\sigma_0, \sigma_1, \ldots, \sigma_{m-1},$$

які визначаються умовами

$$\sigma_j(\alpha) = \alpha^{q^j},$$

де $\alpha \in \mathbb{F}_{q^m}$, $0 \leqslant j \leqslant m-1$, і лише вони.

Доведення. Доведемо спочатку, що кожне відображення σ_j, $0 \leqslant j \leqslant m-1$, є автоморфізмом.

Для кожного відображення σ_j та довільних $\alpha, \beta \in \mathbb{F}_{q^m}$, очевидно, виконуються рівності

$$\sigma_j(\alpha\beta) = \sigma_j(\alpha)\sigma_j(\beta) \quad \text{та} \quad \sigma_j(\alpha+\beta) = \sigma_j(\alpha) + \sigma_j(\beta).$$

Отже, σ_j є гомоморфізмом поля $\mathbb{F}_{q^m}$.

Крім того, $\sigma_j(\alpha) = 0$ тоді і лише тоді, коли $\alpha = 0$, отже, σ_j є мономорфізмом. Оскільки $\mathbb{F}_{q^m}$ — скінченна множина, то σ_j є епіморфізмом. Таким чином, відображення σ_j автоморфізмом поля $\mathbb{F}_{q^m}$.

За лемою 2.3 $\sigma_j(a) = a$ для всіх $a \in \mathbb{F}_q$. Таким чином, кожне σ_j є автоморфізмом поля $\mathbb{F}_{q^m}$ над $\mathbb{F}_q$. При цьому відображення $\sigma_0, \sigma_1, \ldots, \sigma_{m-1}$ різні, бо переводять фіксований елемент поля $\mathbb{F}_{q^m}$ в різні елементи.

Припустимо тепер, що σ — довільний автоморфізм поля $\mathbb{F}_{q^m}$ над $\mathbb{F}_q$. Покажемо, що це насправді автоморфізм σ_j для деякого $0 \leqslant j \leqslant m-1$.

Нехай β — деякий примітивний елемент поля $\mathbb{F}_{q^m}$,

$$f(x) = x^m + a_{m-1}x^{m-1} + \ldots + a_0 \in \mathbb{F}_q[x]$$

— його мінімальний многочлен над $\mathbb{F}_q$. Тоді

$$0 = \sigma(\beta^m + a_{m-1}\beta^{m-1} + \ldots + a_0) = \sigma(\beta)^m + a_{m-1}\sigma(\beta)^{m-1} + \ldots + a_0,$$

тому елемент $\sigma(\beta) \in \mathbb{F}_{q^m}$ також є коренем многочлена f. З теореми 3.3 випливає, що

$$\sigma(\beta) = \beta^{q^j}$$

для деякого j, $0 \leqslant j \leqslant m-1$.

Оскільки σ — гомоморфізм, то для довільного $\alpha \in \mathbb{F}_{q^m}$ отримаємо

$$\sigma(\alpha) = \alpha^{q^j},$$

бо будь-який елемент $\alpha \neq 0$ можна зобразити степенем елемента β. □

Отже, всі спряжені до $\alpha \in \mathbb{F}_{q^m}$ можна одержати, діючи на α автоморфізмами поля $\mathbb{F}_{q^m}$ над $\mathbb{F}_q$.

Зауваження 4.2. Автоморфізми поля $\mathbb{F}_{q^m}$ над полем $\mathbb{F}_q$ утворюють групу відносно композиції відображень, яка називається *групою Галуа* та позначається $Gal(\mathbb{F}_{q^m}/\mathbb{F}_q)$. За теоремою 4.4 ця група є циклічною порядку m з твірним елементом σ_1.

4.2 Сліди та норми

Нехай $F = \mathbb{F}_{q^m}$, $K = \mathbb{F}_q$. Нагадаємо, що поле F можна розглядати як векторний простір над полем K. Тоді розмірність F над K дорівнює m. Якщо $\{\alpha_1, \ldots, \alpha_m\}$ — базис поля F (як векторного простору) над K, то кожний елемент $\alpha \in F$ єдиним чином можна зобразити у вигляді лінійної комбінації

$$\alpha = c_1\alpha_1 + c_2\alpha_2 + \ldots + c_m\alpha_m,\ c_j \in K,\ 1 \leqslant j \leqslant m.$$

Введемо важливу функцію з F в K, яка, як доведемо пізніше, є лінійною.

Означення 4.2. *Слід* $\mathrm{Tr}_{F/K}(\alpha)$ *елемента* $\alpha \in F$ *над полем* K *визначається рівністю*

$$\mathrm{Tr}_{F/K}(\alpha) = \alpha + \alpha^q + \alpha^{q^2} + \ldots + \alpha^{q^{m-1}}.$$

Якщо K *— просте підполе, то* $\mathrm{Tr}_{F/K}(\alpha)$ *називається абсолютним слідом і позначається просто* $\mathrm{Tr}_F(\alpha)$.

Корисним буває визначати слід і з іншого погляду.

Означення 4.3. *Нехай* $\alpha \in F$ *та* $f(x) \in K[x]$ *— мінімальний многочлен* α *над* K*, його степінь* d *є дільником* $m = [F : K]$*. Тоді* $g(x) = f^{m/d}(x) \in K[x]$ *називається характеристичним многочленом елемента* α *над полем* K.

За теоремою 3.3 коренями многочлена $f(x)$ є $\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{d-1}}$. За зауваженням 4.1 коренями многочлена $g(x)$ є спряжені до α відносно K елементи. Звідси

$$g(x) = x^m + a_{m-1}x^{m-1} + \ldots + a_0 = (x-\alpha)(x-\alpha^q)\ldots(x-\alpha^{q^{m-1}}). \quad (4.1)$$

Порівняння коефіцієнтів дає

$$\mathrm{Tr}_{F/K}(\alpha) = -a_{m-1}.$$

Зокрема, це означає, що слід $\mathrm{Tr}_{F/K}(\alpha)$ завжди є елементом поля K.

Теорема 4.5 (Властивості сліду)**.** *Нехай* $K = \mathbb{F}_q$, $F = \mathbb{F}_{q^m}$. *Тоді функція сліду* $\mathrm{Tr}_{F/K}$ *має наступні властивості*

а) $\mathrm{Tr}_{F/K}(\alpha + \beta) = \mathrm{Tr}_{F/K}(\alpha) + \mathrm{Tr}_{F/K}(\beta)$ *для всіх* $\alpha, \beta \in F$;

б) $\mathrm{Tr}_{F/K}(c\alpha) = c\,\mathrm{Tr}_{F/K}(\alpha)$ *для всіх* $c \in K$, $\alpha \in F$;

в) $\mathrm{Tr}_{F/K}$ *є лінійним відображенням з* F *на* K, *де* F *та* K *розглядаються як векторні простори над полем* K;

г) $\mathrm{Tr}_{F/K}(a) = ma$ *для всіх* $a \in K$;

д) $\mathrm{Tr}_{F/K}(\alpha^q) = \mathrm{Tr}_{F/K}(\alpha)$ *для всіх* $\alpha \in F$.

Доведення. а) Враховуючи вправу 1.1 і лему 2.3, для $\alpha, \beta \in F$ маємо

$$\begin{aligned}\mathrm{Tr}_{F/K}(\alpha + \beta) &= (\alpha + \beta) + (\alpha + \beta)^q + \ldots + (\alpha + \beta)^{q^{m-1}} = \\ &= \alpha + \beta + \alpha^q + \beta^q + \ldots + \alpha^{q^{m-1}} + \beta^{q^{m-1}} = \mathrm{Tr}_{F/K}(\alpha) + \mathrm{Tr}_{F/K}(\beta).\end{aligned}$$

б) За лемою 2.3 для $c \in K$ $c^{q^j} = c$ для всіх $j \geqslant 1$. Тому для $\alpha \in F$

$$\begin{aligned}\mathrm{Tr}_{F/K}(c\alpha) &= c\alpha + c^q\alpha^q + \ldots + c^{q^{m-1}}\alpha^{q^{m-1}} = \\ &= c\alpha + c\alpha^q + \ldots + c\alpha^{q^{m-1}} = c\,\mathrm{Tr}_{F/K}(\alpha).\end{aligned}$$

в) З властивостей а) та б) з урахуванням того, що $\mathrm{Tr}_{F/K}(\alpha) \in K$ для всіх $\alpha \in F$, випливає, що $\mathrm{Tr}_{F/K}$ є лінійним відображенням з F в K. Лишається довести, що це відображення “на”. З огляду на б), для цього потрібно довести існування такого елемента $\alpha \in F$, що $\mathrm{Tr}_{F/K}(\alpha) \neq 0$. Ясно, що $\mathrm{Tr}_{F/K}(\alpha) = 0$ тоді і лише тоді, коли α є коренем многочлена

$$x^{q^{m-1}} + \ldots + x^q + x \in K[x]$$

у полі F. Але оскільки цей многочлен може мати не більше, ніж q^{m-1} коренів в F, а поле F складається з q^m елементів, то потрібний нам елемент в полі F існує.

г) Ця рівність випливає з означення сліду та леми 2.3.

д) За лемою 2.3 для $\alpha \in F$ маємо $\alpha^{q^m} = \alpha$. Тоді

$$\mathrm{Tr}_{F/K}(\alpha^q) = \alpha^q + \alpha^{q^2} + \ldots + \alpha^{q^m} = \mathrm{Tr}_{F/K}(\alpha). \quad \square$$

Функція сліду не лише сама є лінійним відображенням з F на K, але може бути використана для опису *всіх* лінійних відображень з F в K. Цей опис має ту перевагу, що він не залежить від вибору базиса.

Теорема 4.6. *Нехай F — скінченне розширення поля K (обидва поля розглядаються як векторний простір над K). Тоді лінійними відображеннями з F в K є відображення L_β, $\beta \in F$, які визначаються умовою*

$$L_\beta(\alpha) = \mathrm{Tr}_{F/K}(\beta\alpha) \text{ для всіх } \alpha \in F,$$

і лише вони. При цьому якщо β та γ— різні елементи поля F, то $L_\beta \neq L_\gamma$.

Доведення. Кожне відображення L_β є лінійним з F в K (за пунктом в) теореми 4.5). При цьому, якщо $\beta, \gamma \in F$, $\beta \neq \gamma$, то

$$L_\beta - L_\gamma = \mathrm{Tr}_{F/K}(\beta\alpha) - \mathrm{Tr}_{F/K}(\gamma\alpha) = \mathrm{Tr}_{F/K}((\beta-\gamma)\alpha) \neq 0$$

для належним чином обраного елемента $\alpha \in F$, бо $\mathrm{Tr}_{F/K}$ відображає F *на* K. Тому відображення L_β та L_γ різні.

Покажемо, що відображення L_β дають всі лінійні відображення з поля F у поле K. Якщо $K = \mathbb{F}_q$ і $F = \mathbb{F}_{q^m}$, то легко пересвідчитися, що всього можна одержати q^m різних лінійних відображень L_β з F в K.

З іншого боку, обравши деякий базис $\{\alpha_1, \ldots, \alpha_m\}$ векторного простору F над полем K, можна одержати будь-яке лінійне відображення з F в K, відображаючи базисні елементи α_j, $j = 1, \ldots, m$, у довільні елементи поля K. Це можна зробити q^m різними способами. Отже, всі лінійні відображення з F в K вичерпуються відображеннями L_β, $\beta \in F$. □

Теорема 4.7. *Нехай F — скінченне розширення поля $K = \mathbb{F}_q$. Тоді для $\alpha \in F$ рівність $\mathrm{Tr}_{F/K}(\alpha) = 0$ виконується тоді і лише тоді, коли має місце рівність $\alpha = \beta^q - \beta$ для деякого елемента $\beta \in F$.*

Доведення. Достатність очевидна внаслідок теореми 4.5 д).

Необхідність. Припустимо, що $\alpha \in F = \mathbb{F}_{q^m}$ — такий елемент, що $\mathrm{Tr}_{F/K}(\alpha) = 0$, β — корінь многочлена $x^q - x - \alpha$ у деякому розширенні поля F. Тоді $\beta^q - \beta = \alpha$ та

$$\begin{aligned} 0 = \mathrm{Tr}_{F/K}(\alpha) &= \alpha + \alpha^q + \ldots + \alpha^{q^{m-1}} = \\ &= (\beta^q - \beta) + (\beta^q - \beta)^q + \ldots + (\beta^q - \beta)^{q^{m-1}} = \\ &= (\beta^q - \beta) + (\beta^{q^2} - \beta^q) + \ldots + (\beta^{q^m} - \beta^{q^{m-1}}) = \beta^{q^m} - \beta, \end{aligned}$$

отже, $\beta \in F$. □

Теорема 4.8 (транзитивність сліду)**.** *Нехай K — скінченне поле, F — скінченне розширення поля K і E — скінченне розширення поля F. Тоді для всіх $\alpha \in E$ має місце рівність*

$$\mathrm{Tr}_{E/K}(\alpha) = \mathrm{Tr}_{F/K}(\mathrm{Tr}_{E/F}(\alpha)).$$

Доведення. Нехай $K = \mathbb{F}_q$, $[F : K] = m$, $[E : F] = n$, тоді за теоремою 1.4 (про башту розширень) $[E : K] = mn$. Тоді для $\alpha \in E$

$$\mathrm{Tr}_{F/K}(\mathrm{Tr}_{E/F}(\alpha)) = \sum_{i=0}^{m-1} (\mathrm{Tr}_{E/F}(\alpha))^{q^i} = \sum_{i=0}^{m-1} \left(\sum_{j=0}^{n-1} \alpha^{q^{jm}} \right)^{q^i} =$$

$$= \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} \alpha^{q^{jm+i}} = \sum_{k=0}^{mn-1} (a^{q^k}) = \mathrm{Tr}_{E/K}(\alpha).$$

□

Розглянемо ще одну функцію зі скінченного поля в його підполе.

Означення 4.4. *Нехай $f = \mathbb{F}_{q^m}$, $K = \mathbb{F}_q$. Для $\alpha \in F$ норма елемента α над полем K визначається рівністю*

$$\mathrm{N_{F/K}}(\alpha) = \alpha \cdot \alpha^q \cdot \ldots \cdot \alpha^{q^{m-1}} = \alpha^{(q^m-1)/(q-1)}.$$

Так само як і у випадку сліду, на норму можна подивитися з іншого погляду. Порівнюючи у рівності (4.1) постійні члени, одержимо

$$\mathrm{N_{F/K}}(\alpha) = (-1)^m a_0.$$

Зокрема, маємо, що норма $\mathrm{N_{F/K}}(\alpha)$ завжди є елементом поля K.

Теорема 4.9 (Властивості норми)**.** *Нехай $K = \mathbb{F}_q$, $F = \mathbb{F}_{q^m}$. Тоді функція норми $\mathrm{N_{F/K}}$ має наступні властивості:*

а) $\mathrm{N_{F/K}}(\alpha\beta) = \mathrm{N_{F/K}}(\alpha)\,\mathrm{N_{F/K}}(\beta)$ *для всіх $\alpha, \beta \in F$;*

б) $\mathrm{N_{F/K}}$ *відображає F на K і F^* на K^*;*

в) $\mathrm{N_{F/K}}(a) = a^m$ *для всіх $a \in K$;*

г) $\mathrm{N_{F/K}}(\alpha^q) = \mathrm{N_{F/K}}(\alpha)$ *для всіх $\alpha \in F$.*

Доведення. Властивість а) випливає з означення норми.

б) Ми вже зауважили, що функція $\mathrm{N_{F/K}}$ відображає F в K. Оскільки $\mathrm{N_{F/K}}(\alpha) = 0$ тоді і лише тоді, коли $\alpha = 0$, то $\mathrm{N_{F/K}}$ відображає F^* в K^*.

Властивість а) означає, що відображення $\mathrm{N_{F/K}}$ є гомоморфізмом мультиплікативної групи F^* в мультиплікативну групу K^*. Оскільки елементами ядра гомоморфізму $\mathrm{N_{F/K}}$ є корені многочлена $x^{(q^m-1)/(q-1)} - 1 \in K[x]$, які належать полю F, і лише вони, то порядок d цього ядра задовольняє нерівність $d \leqslant (q^m - 1)/(q - 1)$. За теоремою про гомоморфізм для груп

образ відображення $\mathrm{N}_{\mathrm{F/K}}$ має порядок $(q^m - 1)/d \geqslant q - 1 = |K^*|$. Отже, $\mathrm{N}_{\mathrm{F/K}}$ відображає F^* на K^*, а, отже, F на K.

в) Ця властивість випливає з означення норми та того факту, що всі елементи, які спряжені з $a \in K$ відносно поля K, дорівнюють a.

г) За властивістю а) має місце рівність $\mathrm{N}_{\mathrm{F/K}}(\alpha^q) = (\mathrm{N}_{\mathrm{F/K}}(\alpha))^q$. Для довільного $\alpha \in F$ вірно, що $\mathrm{N}_{\mathrm{F/K}}(\alpha) \in K$. Тому, врахувавши лему 2.3, $\mathrm{N}_{\mathrm{F/K}}(\alpha^q) = (\mathrm{N}_{\mathrm{F/K}}(\alpha))^q = \mathrm{N}_{\mathrm{F/K}}(\alpha)$ виконуються рівності. □

Теорема 4.10 (транзитивність норми)**.** *Нехай K — скінченне поле, F — скінченне розширення поля K, E — скінченне розширення поля F. Тоді для всіх $\alpha \in E$*

$$\mathrm{N}_{E/K}(\alpha) = \mathrm{N}_{F/K}(\mathrm{N}_{E/F}(\alpha)).$$

Доведення. Нехай $[F : K] = m$, $[E : F] = n$. Тоді для всіх $\alpha \in E$

$$\mathrm{N}_{F/K}(\mathrm{N}_{E/F}(\alpha)) = \mathrm{N}_{\mathrm{F/K}}(\alpha^{(q^{mn}-1)/(q^m-1)}) = \left(\alpha^{(q^{mn}-1)/(q^m-1)}\right)^{(q^m-1)/(q-1)} =$$
$$= \alpha^{(q^{mn}-1)/(q-1)} = \mathrm{N}_{E/K}.$$ □

Розділ 5

Базиси. Нормальний базис. Теорема про нормальний базис

5.1 Дуальний базис

Нехай $\{\alpha_1, \ldots, \alpha_m\}$ — базис скінченного поля F над деяким підполем K. Тоді кожний елемент $\alpha \in F$ єдиним чином зображується у вигляді

$$\alpha = c_1(\alpha)\alpha_1 + \ldots + c_m(\alpha)\alpha_m. \tag{5.1}$$

Природним чином виникає питання, як обчислити коефіцієнти $c_j(\alpha)$, $1 \leqslant j \leqslant m$. Відображення $c_j : \alpha \mapsto c_j(\alpha)$ є лінійним з F в K. За теоремою 4.6 існує такий елемент β_j, що $c_j(\alpha) = \mathrm{Tr}_{F/K}(\beta_j\alpha)$ для всіх $\alpha \in F$. Поклавши $\alpha = \alpha_i$, $1 \leqslant i \leqslant m$, побачимо, що $\mathrm{Tr}_{F/K}(\beta_j\alpha_i)$ дорівнює 0 при $i \neq j$ та 1 при $i = j$. Крім того, $\{\beta_1, \ldots, \beta_m\}$ теж є базисом F над K. Дійсно, якщо

$$d_1\beta_1 + \ldots + d_m\beta_m = 0 \text{ при } d_i \in K, \quad 1 \leqslant i \leqslant m,$$

то, множачи на фіксоване α_i та застосовуючи функцію $\mathrm{Tr}_{F/K}$, одержимо, що $d_i = 0$.

Означення 5.1. *Нехай K — скінченне поле і F — його скінченне розширення. Тоді два базиси $\{\alpha_1, \ldots, \alpha_m\}$ та $\{\beta_1, \ldots, \beta_m\}$ називаються дуальними , якщо для $1 \leqslant i, j \leqslant m$*

$$\mathrm{Tr}_{F/K}(\alpha_i\beta_j) = \begin{cases} 0, & \text{якщо } i \neq j; \\ 1, & \text{якщо } i = j. \end{cases}$$

Зі сказаного вище випливає, що для довільного базиса $\{\alpha_1, \ldots, \alpha_m\}$ поля F над полем K завжди існує деякий дуальний базис $\{\beta_1, \ldots, \beta_m\}$. Дійсно, дуальний базис для базису $\{\alpha_1, \ldots, \alpha_m\}$ визначається однозначно, оскільки з означення видно, що коефіцієнти $c_j(\alpha)$, $1 \leqslant j \leqslant m$, в (5.1) для всіх $\alpha \in F$ задаються рівністю $c_j(\alpha) = \mathrm{Tr}_{F/K}(\beta_j\alpha)$, і за теоремою 4.6 елемент $\beta_j \in F$ однозначно визначається лінійним відображенням c_j.

Приклад 5.1. Нехай $\alpha \in \mathbb{F}_8$ — корінь незвідного многочлена $x^3 + x^2 + 1 \in \mathbb{F}_2[x]$. Тоді

$$\left\{\alpha, \alpha^2, 1 + \alpha + \alpha^2\right\}$$

є базисом поля $\mathbb{F}_8$ над $\mathbb{F}_2$. Базис $\left\{\alpha, \alpha^2, 1 + \alpha + \alpha^2\right\}$ є дуальним до цього базису. Базис, який дуальний сам до себе, називається *автодуальним* базисом. Елемент $\alpha^6 \in \mathbb{F}_8$ можна єдиним чином подати у вигляді

$$\alpha^6 = c_1\alpha + c_2\alpha^2 + c_3(1 + \alpha + \alpha^2),$$

де кофіцієнти $c_1.c_2, c_3 \in \mathbb{F}_2$ визначаються рівностями

$$\begin{aligned} c_1 &= \mathrm{Tr}_{\mathrm{F/K}}(\alpha \cdot \alpha^6) = 1, \\ c_2 &= \mathrm{Tr}_{\mathrm{F/K}}(\alpha^2\alpha^6) = 1, \\ c_3 &= \mathrm{Tr}_{\mathrm{F/K}}((1 + \alpha + \alpha^2)\alpha^6) = 0, \end{aligned}$$

отже, $\alpha^6 = \alpha + \alpha^2$. □

5.2 Теорема про нормальний базис

До найбільш важливих типів базисів F над K належать поліноміальний та нормальний базиси. *Поліноміальний базис* $\left\{1, \alpha, \alpha^2, \ldots \alpha^{m-1}\right\}$ — це базис, утворений степенями твірного елемента поля F (як скінченного розширення поля K). В якості α часто береться примітивний елемент поля F. Нехай $K = \mathbb{F}_q$, $F = \mathbb{F}_{q^m}$. Тоді базис поля F над K вигляду $\left\{\alpha, \alpha^q, \ldots, \alpha^{q^{m-1}}\right\}$, який складається з належним чином обраного елемента $\alpha \in F$ і спряжених з ним відносно поля K елементів, називається *нормальним базисом* поля F над K.

Приклад 5.2. Нехай $\alpha \in \mathbb{F}_8$ — корінь незвідного многочлена $x^3 + x^2 + 1 \in \mathbb{F}_2[x]$. Тоді $\left\{\alpha, \alpha^2, 1 + \alpha + \alpha^2\right\}$ — нормальний базис поля $\mathbb{F}_8$ над $\mathbb{F}_2$, бо $\alpha^4 = 1 + \alpha + \alpha^2$. □

Перш ніж доводити теорему про нормальний базис наведемо результати з лінійної алгебри, які, проте, виходять за межі стандартного курсу.

Нехай $T : V \to V$ — лінійне перетворення скінченновимірного векторного простору над полем F. Нехай $m(x)$ — мінімальний многочлен T.

Можна розширити поняття мінімального многочлена наступним чином. Припустимо, що $v \in V$. Розглянемо множину многочленів

$$I(v) = \{f(x) \mid f(T)v = 0\}.$$

Очевидно, що ця множину є ідеалом у кільці $F[x]$. Відомо, що це кільце є кільцем головних ідеалів. Нехай многочлен $m_v(x)$ породжує ідеал $I(v)$. Наведемо основні властивості многочлена m_v.

Лема 5.3. *1. $m_v(x) \mid m(x)$ для всіх $v \in V$.*

2. $m(x) = НСК_{v\in V}(m_v(x))$.

3. Якщо $u = f(T)v$ для деякого многочлена $f(x)$, то $m_u(x) \mid m_v(x)$.

4. Якщо $u, v \in V$ та $(m_u(x), m_v(x)) = 1$, то $m_{u+v}(x) = m_u(x)m_v(x)$.

Доведення. 1. Оскільки $m(T) = 0$, то $m(T)v = 0$ для всіх v. Тому $m_v(x) \mid m(x)$ для всіх $v \in V$.

2. З доведеного вище випливає, що многочлен $f(x) = \text{НСК}_{v\in V}(m_v(x))$ визначений та $f(x) \mid m(x)$. Але $f(T)v = 0$ для всіх $v \in V$, тому $f(T) = 0$. Отже, $f(x) = m(x)$.

3. Маємо рівності

$$m_v(T)u = m_v(T)f(T)v = f(T)m_v(T)v = 0.$$

Отже, $m_u(x) \mid m_v(x)$.

4. Зауважимо, що $m_{u+v}(x) \mid m_u(x)m_v(x)$. Розглянемо вектор $w = m_u(T)(u + v) = m_u(T)v$. Покладемо $f(x) = m_w(x)$. Тоді $0 = f(T)w = f(T)m_u(T)v$, а тому $m_v(x) \mid f(x)m_u(x)$. Оскільки $m_u(x)$ та $m_v(x)$ взаємно прості, то $m_v(x) \mid f(x)$. З іншого боку, за пунктом 3 $f(x) \mid m_{u+v}(x)$. Отже, $m_v(x) \mid m_{u+v}(x)$. Аналогічно доводиться, що $m_u(x) \mid m_{u+v}(x)$. Оскільки $m_u(x)$ та $m_v(x)$ взаємно прості, то $m_u(x)m_v(x) \mid m_{u+v}(x)$. Отже, $m_u(x)m_v(x) = m_{u+v}(x)$. □

Лема 5.4 (про циклічний вектор)**.** *Нехай V — скінченновимірний векторний простір над полем F. Для довільного лінійного оператора у просторі V існує такий вектор v, що $m(x) = m_v(x)$. Такий вектор v називається* циклічним.

Доведення. Нехай $m(x) = p_1^{k_1}(x)m_2^{k_2}(x)\dots p_s^{k_s}(x)$ — канонічний розклад мінімального многочлена $m(x)$.

З пункту 2 леми 5.3 випливає, що для кожного i, $1 \leqslant i \leqslant s$, знайдеться такий вектор u_i, мінімальний многочлен якого ділиться на $p_i(x)^{k_i}$. Запишемо $m_{u_i}(x) = p_i(x)^{k_i}f_i(x)$.

Тоді для вектора $v_i = f_i(T)u_i$ мінімальним многочленом буде $p_i(x)^{k_i}$. Очевидно, що

$$\text{НСД}(m_{v_1}, m_{v_2}, \dots, m_{v_s}) = 1.$$

З пункту 4 леми 5.3 випливає, що коли покласти $v = v_1 + v_2 + \dots + v_s$, то $m_v = m(x)$. □

Теорема 5.5 (про нормальний базис)**.** *У скінченному полі $F = \mathbb{F}_{p^n}$ існує такий елемент α, що спряжені з ним елементи*

$$\alpha, \alpha^p, \ldots, \alpha^{p^{n-1}}$$

утворюють базис поля F над його простим підполем $\mathbb{F}_p$.

Доведення. Розглянемо відображення

$$\sigma : F \to F : \alpha \mapsto \alpha^p.$$

Це відображення, очевидно, є лінійним, тому можна застосувати лему 5.4.

Мінімальним многочленом σ є $m(x) = x^n - 1$. Очевидно, що σ задовольняє рівняння $m(x) = 0$. Припустимо, що σ анулюється многочленом

$$a_d\sigma^d + a_{d-1}\sigma^{d-1} + \ldots + a_0$$

меншого степеня $d < n$. Тоді кожний елемент $\alpha \in F$ задовольняє рівняння

$$a_d x^{p^d} + a_{d-1}x^{p^{d-1}} + \ldots + a_0 = 0.$$

Цей многочлен має щонайбільше p^d коренів у полі F. Таким чином, існують елементи поля, які не є його коренями.

Відповідно до леми 5.4 ми можемо знайти циклічний вектор $\alpha \in F$ оператора σ, мінімальним многочленом якого є $x^n - 1$. З цього, зокрема, випливає, що $\alpha, \sigma(\alpha), \ldots, \sigma^{n-1}(\alpha)$ лінійно незалежні, а тому утворюють базис поля F над $\mathbb{F}_p$. □

Теорема 5.6 (про примітивний нормальний базис)**.** *Для кожного скінченного поля F існує нормальний базис цього поля над його простим підполем, який складається з примітивних елементів поля F.*

Приклад 5.7. Нехай $\alpha \in \mathbb{F}_8$ — корінь незвідного многочлена $x^3 + x^2 + 1 \in \mathbb{F}_2[x]$. Тоді $\{\alpha, \alpha^2, 1 + \alpha + \alpha^2\}$ — примітивний нормальний базис поля $\mathbb{F}_8$ над $\mathbb{F}_2$, бо $|\mathbb{F}_8^*| = 7$, а тому кожний неодиничний елемент є твірним. □

5.3 Характеризація базисів

Означення 5.2. *Нехай K — скінченне поле, F — його скінченне розширення степеня m. Дискримінантом $\Delta_{F/K}(\alpha_1, \ldots, \alpha_m)$ елементів $\alpha_1, \ldots, \alpha_m$ називається визначник порядку m вигляду*

$$\Delta_{F/K}(\alpha_1, \ldots, \alpha_m) = \begin{vmatrix} \mathrm{Tr}_{F/K}(\alpha_1\alpha_1) & \mathrm{Tr}_{F/K}(\alpha_1\alpha_2) & \ldots & \mathrm{Tr}_{F/K}(\alpha_1\alpha_m) \\ \mathrm{Tr}_{F/K}(\alpha_2\alpha_1) & \mathrm{Tr}_{F/K}(\alpha_2\alpha_2) & \ldots & \mathrm{Tr}_{F/K}(\alpha_2\alpha_m) \\ \vdots & \vdots & \ddots & \vdots \\ \mathrm{Tr}_{F/K}(\alpha_m\alpha_1) & \mathrm{Tr}_{F/K}(\alpha_m\alpha_2) & \ldots & \mathrm{Tr}_{F/K}(\alpha_m\alpha_m) \end{vmatrix}$$

З означення випливає, що дискримінант $\Delta_{F/K}(\alpha_1, \ldots, \alpha_m)$ є елементом поля K.

Теорема 5.8 (про характеризацію базису)**.** *Нехай K — скінченне поле, F — його розширення степеня m. Елементи $\{\alpha_1, \ldots, \alpha_m\}$ поля F утворюють його базис над полем K тоді і лише тоді, коли $\Delta_{F/K}(\alpha_1, \ldots, \alpha_m) \neq 0$.*

Доведення. Необхідність. Нехай $\{\alpha_1, \ldots, \alpha_m\}$ — базис поля F над K. Доведемо, що рядки визначника $\Delta_{F/K}(\alpha_1, \ldots, \alpha_m)$ лінійно незалежні. Це означатиме, що $\Delta_{F/K}(\alpha_1, \ldots, \alpha_m) \neq 0$.

Припустимо, що

$$c_1 \mathrm{Tr}_{F/K}(\alpha_1\alpha_j) + c_2 \mathrm{Tr}_{F/K}(\alpha_2\alpha_j) + \ldots + c_m \mathrm{Tr}_{F/K}(\alpha_m\alpha_j) = 0,$$

де $c_1, \ldots, c_m \in K$.

Тоді якщо $\beta = c_1\alpha_1 + c_2\alpha_2 + \ldots + c_m\alpha_m$, то $\mathrm{Tr}_{F/K}(\beta\alpha_j) = 0$ для $1 \leqslant j \leqslant m$, а оскільки елементи $\alpha_1, \alpha_2, \ldots, \alpha_m$ породжують весь простір F, то це означає, що $\mathrm{Tr}_{F/K}(\beta\alpha) = 0$ для всіх $\alpha \in F$.

Це можливо лише при $\beta = 0$, тобто $c_1\alpha_1 + c_2\alpha_2 + \ldots + c_m\alpha_m = 0$, а це означає, що $c_1 = c_2 = \ldots = c_m = 0$.

Достатність. Припустимо, що $\Delta_{F/K}(\alpha_1, \ldots, \alpha_m) \neq 0$ та

$$c_1\alpha_1 + c_2\alpha_2 + \ldots + c_m\alpha_m = 0$$

для деяких $c_1, \ldots, c_m \in K$. Тоді

$$c_1\alpha_1\alpha_j + c_2\alpha_2\alpha_j + \ldots + c_m\alpha_m\alpha_j = 0 \text{ для } 1 \leqslant j \leqslant m$$

і, застосовуючи функцію сліду, одержимо

$$c_1 \mathrm{Tr}_{F/K}(\alpha_1\alpha_j) + c_2 \mathrm{Tr}_{F/K}(\alpha_2\alpha_j) + \ldots + c_m \mathrm{Tr}_{F/K}(\alpha_m\alpha_j) = 0 \text{ для } 1 \leqslant j \leqslant m.$$

Оскільки рядки визначника $\Delta_{F/K}(\alpha_1, \ldots, \alpha_m)$ лінійно незалежні, то $c_1 = c_2 = \ldots = c_m = 0$. Тому елементи $\alpha_1, \alpha_2, \ldots, \alpha_m$ — лінійно незалежні над полем K. □

Можна розглядати і інший визначник, який використовується для тих самих цілей, що і дискримінант, але його елементами є елементи розширення F поля $K = \mathbb{F}_q$. Для елементів $\alpha_1, \alpha_2, \ldots, \alpha_m$ поля F розглянемо матрицю $A = (a_{ij})_{m\times m}$, де $a_{ij} = \alpha_j^{q^{i-1}}$. Неважко перевірити, що в матриці $B = A^T A$ на місці (i, j) стоїть елемент $\mathrm{Tr}_{\mathrm{F/K}}(\alpha_i\alpha_j)$. Перейшовши до визначників, одержимо

$$\Delta_{F/K}(\alpha_1, \ldots, \alpha_m) = \det(A)^2.$$

Таким чином, маємо наслідок.

Наслідок 5.9. *Елементи $\{\alpha_1, \alpha_2, \ldots, \alpha_m\}$ поля $\mathbb{F}_{q^m}$ утворюють базис цього поля над полем $\mathbb{F}_q$ тоді і ліше тоді, коли*

$$\det(A) = \begin{vmatrix} \alpha_1 & \alpha_2 & \ldots & \alpha_m \\ \alpha_1^q & \alpha_2^q & \ldots & \alpha_m^q \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{q^{m-1}} & \alpha_2^{q^{m-1}} & \ldots & \alpha_m^{q^{m-1}} \end{vmatrix} \neq 0.$$

Лема 5.10. *Нехай F — довільне поле. Для довільних елементів $a_0, a_1, \ldots, a_{m-1}$ поля F матриця-циркулянт*

$$c[a_0, a_1, \ldots, a_{m-1}] = \begin{pmatrix} a_0 & a_1 & a_2 & \ldots & a_{m-1} \\ a_{m-1} & a_0 & a_1 & \ldots & a_{m-2} \\ a_{m-2} & a_{m-1} & a_0 & \ldots & a_{m-3} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_1 & a_2 & a_3 & \ldots & a_0 \end{pmatrix}$$

невироджена тоді і лише тоді, коли многочлени $a_{m-1}x^{m-1} + \ldots + a_1x + a_0$ та $x^m - 1$ взаємно прості.

Доведення. Нехай A — це квадратна матриця порядку m вигляду

$$A = \begin{pmatrix} 0 & 1 & 0 & \ldots & 0 & 0 \\ 0 & 0 & 1 & \ldots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & 0 & 1 \\ 1 & 0 & 0 & \ldots & 0 & 0 \end{pmatrix}.$$

Покладемо $f(x) = a_{m-1}x^{m-1} + \ldots + a_1x + a_0$. Легко переконатися, що

$$c[a_0, a_1, \ldots, a_{m-1}] = \sum_{i=0}^{m-1} a_i A^i = f(A).$$

Зауважимо, що мінімальним многочленом матриці A є $x^m - 1$.

Припустимо, що $f(x)$ та $x^m - 1$ взаємно прості. Тоді знайдуться такі многочлени $a(x)$ та $b(x)$, що

$$a(x)f(x) + b(x)(x^m - 1) = 1.$$

Тоді $a(A)f(A) = I_m$, де I_m позначає одиничну матрицю порядку m. Звідси випливає, що $f(A)$ невироджена.

Припустимо тепер, що $(f(x), x^m - 1) = d(x) \neq 1$. Нехай $f(x) = d(x)f_1(x)$, $x^m - 1 = d(x)h(x)$. Оскільки $\deg(h(x)) < m$, то $h(A) \neq 0$. Оскільки $A^m - 1 = d(A)h(A) = 0$, то $d(A)$ вироджена. Таким чином $f(A) = d(A)f_1(A)$ теж вироджена.

Отже, $f(A)$ невироджена тоді і лише тоді, коли $(f(x), x^m - 1) = 1$. □

Теорема 5.11 (про характеризацію нормального базису)**.** *Елемент $\alpha \in F$ породжує нормальний базис поля $\mathbb{F}_{q^m}$ над полем $\mathbb{F}_q$, тоді і лише тоді, коли многочлени $x^m - 1$ та $\alpha^{q^{m-1}}x^{m-1} + \alpha^{q^{m-2}}x^{m-2} + \ldots + \alpha^q x + \alpha$ з кільця $\mathbb{F}_{q^m}[x]$ взаємно прості.*

Доведення. Зауважимо, що елемент $\alpha \in \mathbb{F}_{q^m}$ породжує нормальний базис над полем $\mathbb{F}_q$ тоді лише тоді, коли елементи $\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{m-1}}$ лінійно незалежні над $\mathbb{F}_q$. За наслідком 5.9 ці елементи лінійно незалежні тоді і лише тоді, коли матриця

$$A = \begin{pmatrix} \alpha & \alpha^q & \alpha^{q^2} & \ldots & \alpha^{q^{m-1}} \\ \alpha^q & \alpha^{q^2} & \alpha^{q^3} & \ldots & \alpha \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \alpha^{q^{m-1}} & \alpha & \alpha^q & \ldots & \alpha^{q^{m-2}} \end{pmatrix}$$

невироджена. Помітимо, що коли переписати рядки матриці A у зворотному порядку, починаючи з другого, то одержимо матрицю-циркулянт $c[\alpha, \alpha^q, \ldots, \alpha^{q^{m-1}}]$, яка невироджена тоді і лише тоді, коли матриця A невироджена. За лемою 5.10 матриця $c[\alpha, \alpha^q, \ldots, \alpha^{q^{m-1}}]$ невироджена тоді і лише тоді, коли многочлени $x^m - 1$ та $\alpha^{q^{m-1}}x^{m-1} + \alpha^{q^{m-2}}x^{m-2} + \ldots + \alpha^q x + \alpha$ взаємно прості. □

Теорема 5.12. *Нехай $\alpha \in \mathbb{F}_{q^m}$, $\alpha_i = \alpha^{q^i}$ та $t_i = \mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha_0\alpha_i)$, $0 \leqslant i \leqslant m-1$. Тоді α породжує нормальний базис поля $\mathbb{F}_{q^m}$ над полем $\mathbb{F}_q$ тоді і лише тоді, коли многочлен $g(x) = t_{m-1}x^{m-1} + \ldots + t_1 x + t_0 \in \mathbb{F}_q[x]$ та $x^m - 1$ взаємно прості.*

Доведення. За теоремою 5.8 елементи $\alpha_0, \alpha_1, \ldots, \alpha_{m-1}$ утворюють базис тоді і лише тоді, коли $\Delta(\alpha_0, \alpha_1, \ldots, \alpha_{m-1}) \neq 0$. Оскільки $\mathrm{Tr}(\alpha_i\alpha_{i+j}) = \mathrm{Tr}(\alpha_0\alpha_i)$, то

$$\Delta(\alpha_0, \alpha_1, \ldots, \alpha_{m-1}) = \begin{vmatrix} t_0 & t_1 & t_2 & \ldots & t_{m-1} \\ t_{m-1} & t_0 & t_1 & \ldots & t_{m-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ t_1 & t_2 & t_3 & \ldots & t_0 \end{vmatrix}.$$

За лемою 5.10 $\Delta(\alpha_0, \alpha_1, \ldots, \alpha_{m-1}) \neq 0$ тоді і лише тоді, коли $x^m - 1$ та $g(x)$ взаємно прості. □

Теорема 5.13. *Базис, дуальний до нормального, є нормальним.*

Доведення. Нехай $\left\{\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{m-1}}\right\}$ — нормальний базис поля $\mathbb{F}_{q^m}$ над полем $\mathbb{F}_q$, $\{\beta_1, \beta_2, \ldots, \beta_m\}$ — дуальний до нього базис. Розглянемо матриці

$$A = \begin{pmatrix} \alpha & \alpha^q & \alpha^{q^2} & \ldots & \alpha^{q^{m-1}} \\ \alpha^q & \alpha^{q^2} & \alpha^{q^3} & \ldots & \alpha \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \alpha^{q^{m-1}} & \alpha & \alpha^q & \ldots & \alpha^{q^{m-2}} \end{pmatrix} \text{ та } B = \begin{pmatrix} \beta_1 & \beta_2 & \ldots & \beta_m \\ \beta_1^q & \beta_2^q & \ldots & \beta_m^q \\ \vdots & \vdots & \ddots & \vdots \\ \beta_1^{q^{m-1}} & \beta_2^{q^{m-1}} & \ldots & \beta_m^{q^{m-1}} \end{pmatrix}.$$

За означенням дуального базису $AB = I_m$, а тому і $BA = I_m$. Матриця A симетрична, тому $(AB)^T = B^T A^T = B^T A = I_m$.

З рівностей $BA = I_m = B^T A$ отримуємо, що $B^T = B$. Звідси випливає, що $\beta_i = \beta_1^{q^{i-1}}$. Отже, базис $\{\beta_1, \beta_2, \ldots, \beta_m\}$ є нормальним. □

Теорема 5.14 (про обчислення дуального базису)**.** *Нехай K — скінченне поле, F — його скінченне розширення. Нехай $\{\alpha_1, \alpha_2, \ldots, \alpha_m\}$ — базис F над K. Нехай матриця $A = (a_{ij})_{m\times m}$, де $a_{ij} = \mathrm{Tr}_{F/K}(\alpha_i\alpha_j)$. Нехай матриця $B = (b_{jk}) \in \mathrm{M}_{m\times s}(F)$ і $\beta_k = \sum_{j=1}^m b_{jk}\alpha_j$. Тоді*

а) *у добутку матриць AB на місці (i, j) стоїть $\mathrm{Tr}_{F/K}(\alpha_i\beta_j)$;*

б) *для матриці $B = A^{-1}$ базис $\{\beta_1, \beta_2, \ldots, \beta_m\}$ є дуальним до базису $\{\alpha_1, \alpha_2, \ldots, \alpha_m\}$.*

Доведення. Пункт а) випливає з правила множення матриць.

б) За теоремою 5.8 матриця A є оборотною. Врахувавши це та правило множення матриць, одержуємо пункт б). □

Розділ 6

Корені з одиниці та кругові многочлени

Дослідимо поле розкладу многочлена $x^n - 1$ над довільним полем K, де $n \in \mathbb{N}$.

Означення 6.1. *Для $n \in \mathbb{N}$ поле розкладу многочлена $x^n - 1$ над довільним полем K називається n–круговим (або n–циклотомічним) полем над K і позначається $K^{(n)}$. Корені многочлена $x^n - 1$ з поля K називаються коренями n-го степеня з одиниці над K, множину цих коренів позначимо $E^{(n)}$.*

Теорема 6.1. *Нехай $n \in \mathbb{N}$, K — поле характеристики p (можливо $p = 0$). Тоді*

а) *Якщо $p \nmid n$, то множина $E^{(n)}$ є циклічною підгрупою порядку n мультиплікативної групи поля $K^{(n)}$.*

б) *Якщо $p \mid n$ та $n = mp^e$, де $m, e \in \mathbb{N}$ і $p \nmid m$, то $K^{(n)} = K^{(m)}$, $E^{(n)} = E^{(m)}$ і коренями многочлена $x^n - 1$ в полі $K^{(n)}$ є m елементів множини $E^{(m)}$, кожний з яких має кратність p^e.*

Доведення. а) Випадок $n = 1$ тривіальний.

Нехай $n \geqslant 2$. Многочлен $x^n - 1$ та його похідна nx^{n-1} не мають спільних коренів, бо nx^{n-1} має єдиний корінь 0 в полі $K^{(n)}$. Отже, многочлен $x^n - 1$ не може мати кратних коренів, тому множина $E^{(n)}$ складається з n елементів.

Якщо $\zeta, \eta \in E^{(n)}$, то $(\zeta\eta^{-1})^n = \zeta^n(\eta^n)^{-1} = 1$, так що $\zeta\eta^{n-1} \in E^{(n)}$. Отже, $E^{(n)}$ — мультиплікативна група.

За теоремою 2.7 скінченна підгрупа мультиплікативної групи поля є циклічною.

б) Цей пункт випливає з пункту а) та рівності

$$x^n - 1 = x^{mp^e} - 1 = (x^m - 1)^{p^e}. \quad \square$$

Означення 6.2. *Нехай K — поле характеристики p, n — натуральне число, яке не ділиться на p. Тоді твірний елемент циклічної групи $E^{(n)}$ називається первісним (або примітивним) коренем n-го степеня з одиниці над полем K.*

Група $E^{(n)}$ має $\varphi(n)$ твірних елементів, тобто існує $\varphi(n)$ примітивних коренів з одиниці над полем K. Якщо ζ — один з них, тоді множина всіх примітивних коренів з одиниці над полем K описується таким чином

$$\{\zeta^s \mid 1 \leqslant s \leqslant n, (n,s) = 1\}.$$

Означення 6.3. *Нехай K — поле характеристики p, n — натуральне число, яке не ділиться на p, і ζ — первісний корінь n-го степеня з одиниці над полем K. Тоді многочлен*

$$Q_n(x) = \prod_{\substack{s=1 \\ (s,n)=1}}^{n} (x - \zeta^s)$$

називається n-круговим (або n-циклотомічним) многочленом над полем K.

Очевидно, що $\deg Q_n(x) = \varphi(n)$, а коефіцієнти належать n-круговому полю над K. Насправді вони належать простому підполю поля K.

Теорема 6.2. *Нехай K — поле характеристики p, n — натуральне число, яке не ділиться на p. Тоді*

а) $x^n - 1 = \prod_{d|n} Q_d(x)$;

б) *коефіцієнти n-кругового многочлена $Q_n(x)$ належать простому підполю поля K, або кільцю $\mathbb{Z}$, якщо $p = 0$.*

Доведення. а) Кожний корінь n-го степеня з одиниці над полем K є первісним коренем d-го степеня з одиниці рівно для одного натурального дільника d числа n. А саме: якщо ζ^s — довільний корінь n-го степеня з одиниці над K (де ζ — деякий первісний корінь n-го степеня над полем K), то вказане число d дорівнює $\frac{n}{(s,n)}$, тобто d — порядок елемента ζ^s в групі $E^{(n)}$. Оскільки

$$x^n - 1 = \prod_{s=1}^{n} (x - \zeta^s),$$

то формулу в пункті а) можна одержати, зібравши ті множники $(x - \zeta^s)$, для яких ζ^s є первісним коренем з одиниці d-го степеня з одиниці над полем K (для кожного додатного дільника d числа n.)

б) Індукція по n. Твердження, очевидно, є справедливим для $Q_1(x) = x - 1$. Нехай $n > 1$ і припустимо, що воно є вірним для всіх $Q_d(x)$, де $1 \leqslant d < n$. За пунктом (а))

$$Q_n(x) = \frac{x^n - 1}{\prod_{d|n, d<n} Q_d(x)}.$$

За припущенням індукції, у знаменнику стоїть многочлен, коефіцієнти якого належать простому підполю поля K (або $\mathbb{Z}$, якщо $\operatorname{char} K = 0$). Розділивши чисельник на знаменник, одержимо твердження пункту б). □

Приклад 6.3. Нехай $n = 3$, K — довільне поле, для якого $\operatorname{char} K \neq 3$, нехай ζ — примітивний кубічний корінь над K. Тоді

$$Q_3(x) = (x - \zeta)(x - \zeta^2) = x^2 - (\zeta + \zeta^2)x + \zeta^3 = x^2 + x + 1.$$

□

Приклад 6.4. Нехай r — просте і $k \in \mathbb{N}$. Тоді

$$Q_{r^k} = 1 + x^{r^{k-1}} + x^{2r^{k-1}} + \ldots + ^{(r-1)r^{k-1}},$$

оскільки за теоремою 6.2

$$Q_{r^k} = \frac{x^{r^k} - 1}{Q_1(x)Q_r(x)\ldots Q_{r^{k-1}}} = \frac{x^{r^k} - 1}{x^{r^{k-1}} - 1}.$$

При $k = 1$ маємо

$$Q_r(x) = 1 + x + x^2 + \ldots + x^{r-1}.$$

□

Використовуючи формулу обернення Мебіуса, можна одержати явну формулу для n-го кругового многочлена $Q_n(x)$ для довільного $n \in \mathbb{N}$.

Теорема 6.5. *Нехай K — поле характеристики p, n — натуральне число, яке не ділиться на p. Тоді n-й круговий многочлен має вигляд*

$$Q_n(x) = \prod_{d|n} \left(x^d - 1\right)^{\mu\left(\frac{n}{d}\right)} = \prod_{d|n} \left(x^{\frac{n}{d}} - 1\right)^{\mu(d)}.$$

Доведення. Застосуємо формулу обернення Мьобіуса до мультиплікативної групи G ненульових раціональних функцій над K. Покладемо $h(n) = Q_n(x)$, $H(n) = x^n - 1$ для всіх $n \in \mathbb{N}$. За теоремою 6.2 рівність $H(n) = \prod_{d|n} h(d)$ виконується, тому за формулою обернення Мьобіуса маємо

$$Q_n(x) = h(n) = \prod_{d|n} H(d)^{\mu\left(\frac{n}{d}\right)} = \prod_{d|n} (x^d - 1)^{\mu\left(\frac{n}{d}\right)}.$$

□

Приклад 6.6. Нехай $n = 12$, K — деяке поле, над яким визначений $Q_{12}(x)$. Тоді

$$Q_{12}(x) = \prod_{d|12}(x^{\frac{12}{d}} - 1)^{\mu(d)}$$
$$= (x^{12} - 1)^{\mu(1)}(x^6 - 1)^{\mu(2)}(x^4 - 1)^{\mu(3)}(x^3 - 1)^{\mu(4)}(x^2 - 1)^{\mu(6)}(x - 1)^{\mu(12)} =$$
$$= \frac{(x^{12} - 1)(x^2 - 1)}{(x^6 - 1)(x^4 - 1)} = x^4 - x^2 + 1.$$

□

Означення 6.4. *Нехай b, n — взаємно прості натуральні числа. Найменше таке $k \in \mathbb{N}$, що $b^k \equiv 1 \pmod{n}$ називається мультиплікативним порядком b за модулем n, позначається* $\mathrm{ord}_n(b)$.

Теорема 6.7. *Кругове поле $K^{(n)}$ є простим алгебраїчним розширенням поля K. Більше того, якщо $K = \mathbb{F}_q$ та $(q, n) = 1$, а $d = \mathrm{ord}_n(q)$, тоді*

- *Q_n розкладається у добуток $\varphi(n)/d$ різних унітарних незвідних многочленів з $K[x]$ одного і того самого степеня d;*
- *$K^{(n)}$ є полем розкладу довільного такого незвідного дільника над полем K;*
- *$[K^{(n)} : K] = d$.*

Доведення. Якщо існує примітивний корінь ζ з одиниці n-го степеня над K, то $K^{(n)} = K(\zeta)$. В іншому разі, K — поле простої характеристики p, яка ділить число n, і ми потрапляємо в ситуацію теореми 6.1 б). Тоді $K^{(n)} = K^{(m)}$, де $n = mp^e$, $(m, p) = 1$. Отже, знов $K^{(n)} = K(\zeta)$, бо існує первісний корінь m-го степеня з одиниці ζ над K.

Нехай $K = \mathbb{F}_q$, припустимо, що $(q, n) = 1$, таким чином примітивний корінь з одиниці степеня n над полем $\mathbb{F}_q$ існує. Нехай η — один з них. Тоді

$$\eta \in \mathbb{F}_{q^k} \Leftrightarrow \eta^{q^k} = \eta \Leftrightarrow q^k \equiv 1 \pmod{n}.$$

Найменше натуральне число, для якого це виконується, це $k = d$, отже, $\eta \in \mathbb{F}_{q^d}$, але не в довільному власному підполі. Таким чином, мінімальний многочлен для η має степінь d. Оскільки η — довільний корінь $Q_n(x)$, то твердження теореми має місце, бо ми можемо послідовно ділити на мінімальні многочлени коренів многочлена $Q_n(x)$. □

Приклад 6.8. Нехай $K = \mathbb{F}_{11}$, $n = 12$. З попереднього прикладу маємо, що $Q_{12}(x) = x^4 - x^2 + 1 \in \mathbb{F}_{11}[x]$. Опишемо $K^{(12)}$.

- Оскільки $12 \nmid (11-1)$, але $12 \mid (11^2-1)$, то $d = \mathrm{ord}_{12}(11) = 2$.
- Таким чином, $Q_{12}(x)$ розкладається в добуток $\varphi(12)/2 = 4/2 = 2$ унітарних квадратних незвідних над $\mathbb{F}_{11}$ многочленів. Круговим полем є $K^{(12)} = \mathbb{F}_{121}$.
- Неважко перевірити, що розклад $Q_{12}(x)$ на множники має вигляд

$$Q_{12} = (x^2 + 5x + 1)(x^2 - 5x + 1).$$

□

Теорема 6.9. *Скінченне поле $\mathbb{F}_q$ є $(q-1)$-круговим полем над будь-яким зі своїх підполів.*

Доведення. Многочлен $x^{q-1} - 1$ цілком розкладається на множники в полі $\mathbb{F}_q$, бо його коренями є як раз всі ненульові елементи поля $\mathbb{F}_q$. З іншого боку, зрозуміло, що цей многочлен не може цілком розкладатися на множники в жодному іншому власному підполі поля $\mathbb{F}_q$. Отже, $\mathbb{F}_q$ є полем розкладу многочлена $x^{q-1} - 1$ над довільним зі своїх підполів. □

Розділ 7

Зображення елементів скінченного поля

Розглянемо три способи зображення елементів скінченного поля.

Перший спосіб. Поле $\mathbb{F}_q$, де $q = p^n$, є простим алгебраїчним розширенням поля $\mathbb{F}_p$. Дійсно, якщо f — незвідний многочлен степеня n над полем $\mathbb{F}_p$, то кожний корінь цього α цього многочлена належить полю $\mathbb{F}_{p^n} = \mathbb{F}_q$, а тому $\mathbb{F}_q = \mathbb{F}_p(\alpha)$. Отже, кожний елемент поля $\mathbb{F}_q$ можна однозначно подати у вигляді значень деякого многочлена з $\mathbb{F}_p[x]$ степеня, не більшого за $n-1$, при $x = \alpha$. Можна також розглядати поле $\mathbb{F}_q$ як факторкільце $\mathbb{F}_p[x]/(f)$.

Приклад 7.1. Зобразимо у такий спосіб елементи поля $\mathbb{F}_9$. Для цього розглянемо поле $\mathbb{F}_9$ як просте алгебраїчне розширення степеня 2 над полем $\mathbb{F}_3$, яке одержується приєднанням кореня α деякого незвідного квадратного многочлена над $\mathbb{F}_3$. Візьмемо в якості такого незвідного многочлена многочлен $f(x) = x^2 + 1 \in \mathbb{F}_3$. Тоді $f(\alpha) = \alpha^2 + 1 = 0$ в $\mathbb{F}_9$. Звідси

$$\mathbb{F}_9 = \{a\alpha + b \mid a, b \in \mathbb{F}_3\} = \{0, 1, 2, \alpha, 1+\alpha, 2+\alpha, 2\alpha, 1+2\alpha, 2+2\alpha\}.$$

При такому зображенні дії виконуються за подвійним модулем: за модулем простого числа p та за модулем незвідного многочлена f. Наприклад,

$$(2+\alpha) + (1+\alpha) = 3 + 2\alpha = 2\alpha,$$

$$(2+\alpha)(1+\alpha) = \alpha^2 + 3\alpha + 2 = \alpha^2 + 1 + 1 = 1. \quad \square$$

Другий спосіб використовує теореми 6.7 та 6.9. Оскільки $\mathbb{F}_q = \mathbb{F}_{p^n}$ є $(q-1)$-круговим полем над $\mathbb{F}_p$, то можемо побудувати його наступним чином:

- Знайти розклад $(q-1)$-кругового многочлена $Q_{q-1} \in \mathbb{F}_p[x]$ в добуток незвідних многочленів в $\mathbb{F}_p[x]$, всі степені яких однакові.
- Корінь α кожного з цих дільників є первісним коренем $(q-1)$-го степеня з одиниці над $\mathbb{F}_p$, а тому є примітивним елементом поля $\mathbb{F}_q$.

- Для такого α ми маємо

$$\mathbb{F}_q = \left\{0, \alpha, \alpha^2, \ldots, \alpha^{q-2}, \alpha^{q-1} = 1\right\}.$$

Приклад 7.2. Розглянемо знов поле $\mathbb{F}_9$.

- Зрозуміло, що $\mathbb{F}_9 = \mathbb{F}_3^{(8)}$.
- Знайдемо $Q_8(x)$:

$$Q_8(x) = \frac{x^{2^3} - 1}{x^{2^2} - 1} = x^4 + 1 \in \mathbb{F}_3[x].$$

  Його розкладом в добуток незвідних в $\mathbb{F}_3[x]$ є

$$Q_8(x) = (x^2 + x + 2)(x^2 + 2x + 2).$$

  Маємо $\varphi(8)/(\mathrm{ord}_8\, 3) = 4/2 = 2$ незвідних квадратних многочленів.

- Нехай ζ — корінь многочлена $x^2 + x + 2$. Тоді ζ є первісним коренем з одиниці степеня 8 над полем $\mathbb{F}_3$. Отже,

$$\mathbb{F}_9 = \left\{0, \zeta, \zeta^2, \ldots, \zeta^7, \zeta^8 = 1\right\}. \quad \square$$

Природним чином виникає запитання, яким чином це зображення елементів поля $\mathbb{F}_9$ пов'язане з попереднім.

Приклад 7.3. Розглянемо многочлен $f(x) = x^2 + 1 \in \mathbb{F}_3[x]$, він є незвідним над полем $\mathbb{F}_3$. Отже, ми можемо побудувати поле $\mathbb{F}_9$ шляхом приєднання кореня α многочлена $f(x) = x^2+1$ до поля $\mathbb{F}_3$. Тоді $f(\alpha) = \alpha^2+1 = 0$ в $\mathbb{F}_9$ і

$$\mathbb{F}_9 = \{0, 1, 2, \alpha, 1 + \alpha, 2 + \alpha, 2\alpha, 1 + 2\alpha, 2 + 2\alpha\}.$$

Помітимо, що елемент $\zeta = \alpha + 1$ є коренем многочлена $x^2 + x + 2 \in \mathbb{F}_3[x]$. Отже, елементи в двох зображеннях поля $\mathbb{F}_9$ пов'язані так:

i	1	2	3	4	5	6	7	8
ζ^i	$1 + \alpha$	2α	$1 + 2\alpha$	2	$2 + 2\alpha$	α	$2 + \alpha$	1

$\square$

Зображення елементів скінченного поля таким способом дає зручний спосіб знаходження добутку елементів. Дійсно,

$$\zeta^3 \cdot \zeta^6 = \zeta^9 = \zeta.$$

Проте цей спосіб не дуже зручний для виконання дії додавання. Для спрощення дії додавання будуються так звані таблиці додавання одиниці. Нас цікавить, чому дорівнюватиме показник j у рівності $\zeta^i + 1 = \zeta^j$ для всіх $i = 1, \ldots, 8 \cup \{-\infty\}$ (за домовленістю вважається, що $0 = \zeta^{-\infty}$). Складемо таблицю, для побудови якої використаємо вже знайдені зображення елементів поля $\mathbb{F}_9$:

i	1	2	3	4	5	6	7	8	$-\infty$
ζ^i	$1+\alpha$	2α	$1+2\alpha$	2	$2+2\alpha$	α	$2+\alpha$	1	0
ζ^i+1	$2+\alpha$	$1+2\alpha$	$2+2\alpha$	0	2α	$1+\alpha$	α	2	1
$\zeta^j = \zeta^i+1$	ζ^7	ζ^3	ζ^5	$\zeta^{-\infty}$	ζ^2	ζ	ζ^6	ζ^4	ζ^8
j	7	3	5	$-\infty$	2	1	6	4	8

Насправді нас цікавлять лише перший та останній рядки цієї таблиці, бо нам потрібно знати лише показники степенів.

Тепер цю таблицю зручно використовувати для "перетворення" дії додавання на дію множення. Наприклад,

$$\zeta^6 + \zeta^3 = \zeta^3(\zeta^3 + 1) = \zeta^3 \cdot \zeta^5 = \zeta^8 = 1.$$

Третій спосіб зображення елементів скінченного поля $\mathbb{F}_q$ використовує матриці. Нехай $f(x) = a_0 + a_1 x + \ldots + a_{n-1}x^{n-1} + x^n$ — унітарний многочлен степеня n над деяким полем. Його *супутньою матрицею* називається наступна квадратна матриця порядку n:

$$A = \begin{pmatrix} 0 & 0 & 0 & \ldots & 0 & -a_0 \\ 1 & 0 & 0 & \ldots & 0 & -a_1 \\ 0 & 1 & 0 & \ldots & 0 & -a_2 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & 1 & -a_{n-1} \end{pmatrix}$$

Матриця A задовольняє рівняння $f(A) = 0$. Отже, якщо A — супутня матриця унітарного незвідного многочлена f степеня n над простим скінченним полем $\mathbb{F}_p$, то $f(A) = \mathbf{0}$. Тому матриця A може грати роль "кореня" многочлена f. Звідси випливає, що елементи поля $\mathbb{F}_{p^n}$ зображаються всіма можливими многочленами над $\mathbb{F}_p$ від матриці A степенів, менших за n.

Приклад 7.4. Нехай задано многочлен $f(x) = x^2 + 1 \in \mathbb{F}_3[x]$. Супутньою матрицею цього многочлена є матриця

$$A = \begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix}.$$

Отже, поле $\mathbb{F}_9$ можна подати так:

$$\mathbb{F}_9 = \{\mathbf{0}, I, A, 2I, I + A, 2I + A, 2A, I + 2A, 2I + 2A\}\,, \text{ де}$$

$$\mathbf{0} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, 2I = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}, A = \begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix}, I + A = \begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix},$$

$$2I + A = \begin{pmatrix} 2 & 2 \\ 1 & 2 \end{pmatrix}, 2A = \begin{pmatrix} 0 & 1 \\ 2 & 0 \end{pmatrix}, I + 2A = \begin{pmatrix} 1 & 1 \\ 2 & 1 \end{pmatrix}, 2I + 2A = \begin{pmatrix} 2 & 1 \\ 2 & 2 \end{pmatrix}.$$

Якщо поле $\mathbb{F}_9$ задане таким чином, то обчислення в цьому полі здійснюються за звичайними правилами алгебри матриць. Наприклад,

$$(2I + A)(I + 2A) + (2A) = \begin{pmatrix} 2 & 2 \\ 1 & 2 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 2 & 1 \end{pmatrix} + \begin{pmatrix} 0 & 1 \\ 2 & 0 \end{pmatrix} =$$

$$= \begin{pmatrix} 0 & 1 \\ 2 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 1 \\ 2 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix} = A. \quad \square$$

Аналогічним чином, метод, заснований на розкладі кругового многочлена Q_{q-1} на незвідні множники в $\mathbb{F}_p[x]$, також можна пристосувати для зображення елементів поля $\mathbb{F}_q$ матрицями.

Приклад 7.5. Нехай $h(x) = x^2 + x + 2 \in \mathbb{F}_3[x]$ — незвідний дільник кругового многочлена $Q_8(x) \in \mathbb{F}_3[x]$. Супутньою матрицею многочлена h є матриця

$$C = \begin{pmatrix} 0 & 1 \\ 1 & 2 \end{pmatrix}.$$

Поле $\mathbb{F}_9$ може бути зображено наступним чином

$$\mathbb{F}_9 = \left\{\mathbf{0}, C, C^2, C^3, C^4, C^5, C^6, C^7, C^8\right\},$$

де

$$\mathbf{0} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \quad C = \begin{pmatrix} 0 & 1 \\ 1 & 2 \end{pmatrix}, \quad C^2 = \begin{pmatrix} 1 & 2 \\ 2 & 2 \end{pmatrix},$$

$$C^3 = \begin{pmatrix} 2 & 2 \\ 2 & 0 \end{pmatrix}, \quad C^4 = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}, \quad C^5 = \begin{pmatrix} 0 & 2 \\ 2 & 1 \end{pmatrix},$$

$$C^6 = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}, \quad C^7 = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \quad C^8 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Обчислення здійснюються за правилами алгебри матриць. Наприклад,

$$C^2 + C = \begin{pmatrix} 1 & 2 \\ 2 & 2 \end{pmatrix} + \begin{pmatrix} 0 & 1 \\ 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = C^8. \quad \square$$

Розділ 8

Алгоритми побудови незвідних многочленів та скінченних полів

Почнемо з ефективного алгоритму, що дозволяє з'ясувати, чи є заданий многочлен незвідним. Як відомо, якщо многочлен $f(x)$ незвідний над $\mathbb{F}_q$, то факторкільце $\mathbb{F}_q[x]/(f(x))$ є полем. Тому зв'язок між побудовою скінченних полів та незвідними многочленами є цілком природним.

Нехай $f(x) \in \mathbb{F}_q[x]$ — незвідний многочлен степеня $n > 0$.

Нагадаємо, що за теоремою 3.6 для кожного $k \in \mathbb{N}$ добуток всіх унітарних незвідних многочленів над $\mathbb{F}_q$, степінь яких ділить k, дорівнює

$$x^{q^k} - x.$$

Таким чином, НСД$(x^q - x, f)$ — це добуток всіх різних унітарних лінійних дільників многочлена f. Якщо f не має лінійних дільників, то НСД$(x^{q^2} - x, f)$ — це добуток всіх різних унітарних квадратних незвідних дільників многочлена f. І так далі. Отже, якщо f — звідний многочлен, то він повинен ділитися на деякий незвідний многочлен степеня щонайбільше $n/2$.

Нехай g — незвідний дільник многочлена f найменшого можливого степеня. Нехай $\deg g = k$, тоді $k \leqslant n/2$ та НСД$(x^{q^k} - x, f) \neq 1$. Навпаки, якщо f — незвідний, то НСД$(x^{q^k} - x, f) = 1$ для всіх натуральних k, які не перевищують $n/2$.

Таким чином, щоб з'ясувати, чи є многочлен f незвідним, досить перевірити, чи НСД$(x^{q^k} - x, f) = 1$ для всіх $1 \leqslant k \leqslant n/2$. Якщо ця умова виконується, то можемо зробити висновок, що многочлен f незвідний. У протилежному випадку зробити висновок, що многочлен звідний.

Для спрощення обчислень врахуємо, що коли $h \equiv x^{q^k} \pmod f$, то НСД$(x - h, f) =$ НСД$(x^{q^k} - x, f)$.

З наведених міркувань випливає наступний алгоритм.

Алгоритм 8.1 (перевірка незвідності многочлена)**.** *Дано*: многочлен $f \in \mathbb{F}_q[x]$ степеня $n > 0$.

Потрібно: з'ясувати, чи $f(x)$ незвідний над $\mathbb{F}_q$.

Для цього потрібно зробити наступне:

- покласти $h := x \pmod f$
- для k від 1 до $[n/2]$ обчислювати
  - $h := h^q \pmod f$
  - якщо НСД$(x - h, f) \neq 1$, то результатом є "f — *звідний*"
- *Результат:* "f — *незвідний*" □

Перш ніж оцінювати час роботи наведеного алгоритму, наведемо деякі факти з теорії складності. Під довжиною числа розумітимемо кількість знаків у двійковому записі цього числа. Неважко переконатися, що довжина числа n дорівнює

$$\text{length}(n) = 1 + [\log_2 n] = 1 + \left[\frac{\ln n}{\ln 2}\right] = O(\ln n).$$

Швидке піднесення до степеня. У прикладних задачах часто виникає потреба знайти великий степінь натурального числа за модулем деякого натурального числа N.

Припустимо, що потрібно обчислити a^m. Можна діяти прямолінійно, послідовно множачи на a:

$$a_1 \equiv a \pmod N, a_2 = a_1 \cdot a \pmod N, a_3 = a_2 \cdot a \pmod N, \ldots,$$

Звісно, таким чином ми коли–небудь одержимо відповідь, але для достатньо великих m, скажімо $m = 2^{1024}$, час роботи може оцінюватися мільярдами років. Інша ідея полягає у зображенні показника степеня у бінарній системі числення та наступного обчислення порядку $\log_2 m$ квадратів числа a та приблизно такої самої кількості множень. Проілюструємо цю ідею прикладом.

Приклад 8.1. Для обчислення 3^{100} шляхом послідовного множення на 3 потрібно 99 дій. А можна діяти таким чином. Зобразимо спершу число 100 у вигляді суми степенів 2:

$$100 = 2^6 + 2^5 + 2^2.$$

Після цього обчислимо

$$3^2, \quad 3^4 = (3^2)^2, \quad 3^8 = (3^4)^2, \quad 3^{16} = (3^8), \quad 3^{32} = (3^{16})^2, \quad 3^{64} = (3^{32})^2,$$

остаточно підрахуємо

$$3^{100} = 3^{64} \cdot 3^{32} \cdot 3^4.$$

Отже, для обчислення 3^{100} нам знадобилося лише 8 множень. □

Опишемо алгоритм швидкого піднесення до степеня формально.

Алгоритм 8.2 (швидке піднесення до степеня)**.** *Дано:* $a \in \mathbb{N}$, $m \in \mathbb{N}$, $N \in \mathbb{N}$.

Обчислити: $a^m \pmod N$.

Крок 1. Зобразити m у вигляді суми степенів 2:

$$m = m_0 + m_1 \cdot 2 + m_2 \cdot 2^2 + \ldots + m_k \cdot 2^k, \qquad m_0, \ldots, m_k \in \{0, 1\},$$

можемо припускати, що $m_k = 1$.

Крок 2. Обчислити a^{2^j} для $0 \leqslant j \leqslant k$ шляхом послідовного піднесення до квадрату:

$$\begin{aligned} b_0 &= a \\ b_1 &= b_0^2 = a^2 \\ b_2 &= b_1^2 = a^{2^2} \\ b_3 &= b_2^2 = a^{2^3} \\ &\vdots \\ b_k &= b_{k-1}^2 = a^{2^k}. \end{aligned}$$

Оскільки кожне число b_j є квадратом попереднього, то потрібно виконати k піднесень до квадрату.

Крок 3. Обчислити a^m за формулою

$$\begin{aligned} a^m &= a^{m_0 + m_1 \cdot 2 + m_2 \cdot 2^2 + \ldots + m_k \cdot 2^k} \\ &= a^{m_0} \cdot (a^2)^{m_1} \cdot (a^{2^2})^{m_2} \cdot (a^{2^3})^{m_3} \cdot \ldots (a^{2^k})^{m_k} \\ &= b_0^{m_0} \cdot b_1^{m_1} \cdot b_2^{m_2} \cdot b_3^{m_3} \ldots b_k^{m_k}. \end{aligned}$$

Враховуючи, що $b_0, b_1, b_2, b_3, \ldots, b_k$ були обчислені на попередньому кроці, то цей крок вимагає щонайбільше k множень.

Таким чином, цей алгоритм потребую щонайбільше $2k$ множень для обчислення a^m. Оскільки $m \leqslant 2^k$, то нам потрібно не більше, ніж $\log_2 m$ дій множення. Отже, при такому піднесенні до степеня кількість дій може бути оцінена як $O(\text{length}(m))$. □

Цей алгоритм можна застосовувати і для піднесення до степеня m многочлена за модулем іншого многочлена. Кількість дій у цьому випадку буде оцінюватися як $O(\text{length}(m))$.

Вправа 8.1. Покажіть, що найбільший спільний дільник двох многочленів степенів k_1 та k_2 відповідно можна знайти за $O(k_1 k_2)$ дій.

Теорема 8.2. *Алгоритм 8.1 вимагає* $O\left(n^3 \operatorname{length}(q)\right)$ *дій у полі* $\mathbb{F}_q$.

Доведення. Розглянемо одну ітерацію з основного циклу алгоритму 8.1. Якщо використовувати алгоритм 8.2, то піднесення многочлена h до степеня q за модулем многочлена f вимагає $O\left(\operatorname{length}(q)\right)$ множень. Отже, всього потрібно $O\left(n^2 \operatorname{length}(q)\right)$ дій в $\mathbb{F}_q$. Обчислення найбільшого спільного дільника вимагає $O(n^2)$ дій в $\mathbb{F}_q$. Підсумовуючи, отримуємо, що виконання однієї ітерації циклу потребує $O\left(n^2 \operatorname{length}(q)\right)$ дій у полі $\mathbb{F}_q$.Таким чином, алгоритм загалом вимагає $O\left(n^3 \operatorname{length}(q)\right)$ дій в $\mathbb{F}_q$. □

Зауважимо, що кожна дія у полі $\mathbb{F}_q$ потребує $O\left(\operatorname{length}(q)^2\right)$ елементарних дій. Отже, загальний час роботи $O\left(n^3 \operatorname{length}(q)^3\right)$ дій в $\mathbb{F}_q$. Отже, наведений алгоритм є поліноміальним.

Розглянемо тепер задачу побудови незвідного многочлена заданого степеня $n > 0$. Наведений спосіб ілюструватиме підхід, який можна охарактеризувати як “будуй та доводь”. Ідея полягає в тому, що спочатку будується многочлен наперед заданого степеня з випадковими коефіцієнтами з вказаного поля, а потім перевіряється, чи є цей многочлен незвідним.

Теорема 8.3. *Нехай* $N_q(n)$ *— це кількість унітарних незвідних многочленів степеня* n *над полем* $\mathbb{F}_q$. *Тоді для всіх* $n \geqslant 1$

$$\frac{q^n}{2n} \leqslant N_q(n) \leqslant \frac{q^n}{n}, \tag{8.1}$$

та

$$N_q(n) = \frac{q^n}{n} + O\left(\frac{q^{n/2}}{n}\right). \tag{8.2}$$

Доведення. Нагадаємо, що для всіх $n \in \mathbb{N}$ справджується рівність

$$q^n = \sum_{d|n} d N_q(d), \tag{8.3}$$

сума береться по всім додатним дільникам числа n. Усі доданки у правій частини (8.3) додатні, $nN_q(n)$ — один з цих доданків, тому $q^n \geqslant nN_q(n)$. Звідси випливає права частина нерівності (8.1). Оскільки ця нерівність виконується для всіх $n \in \mathbb{N}$, то маємо

$$nN_q(n) = q^n - \sum_{\substack{d|n \\ d<n}} dN_q(d) \geqslant q^n - \sum_{\substack{d|n \\ d<n}} q^d \geqslant q^n - \sum_{d=1}^{[n/2]} q^d.$$

Покладемо

$$S(q,n) = \sum_{d=1}^{[n/2]} q^d = \frac{q}{q-1}\left(q^{[n/2]} - 1\right).$$

Отже, $nN_q(n) \geqslant q^n - S(q,n)$. Неважко переконатися, що $S(q,n) = O\left(q^{n/2}\right)$. Лишилося довести, що $S(q,n) \leqslant \frac{q^n}{2}$. Безпосередніми обчисленнями можна перевірити, що ця нерівність правильна для $n = 1, 2, 3$. Для $n \geqslant 4$ маємо

$$S(q,n) \leqslant q^{n/2} + 1 \leqslant q^{n-1} \leqslant \frac{q^n}{2}.$$

□

Алгоритм 8.3. *Дано*: натуральне число n.

Потрібно: побудувати унітарний незвідний многочлен $f(x) \in \mathbb{F}_q[x]$ степеня n.

Для цього потрібно повторювати наступні кроки, поки не одержимо незвідний многочлен:

- випадковим чином обрати $c_0, c_1, \ldots, c_{n-1}$
- покласти $f := x^n + \sum_{i=0}^{n-1} c_i x^i$
- за алгоритмом 8.1 перевірити, чи він незвідний

Результат: унітарний незвідний многочлен $f(x) \in \mathbb{F}_q[x]$ степеня n.

Теорема 8.4. *Алгоритм 8.3 вимагає в середньому $O(n^4 \operatorname{length}(q))$ дій у полі $\mathbb{F}_q$. Результат рівномірно розподілений на множині всіх унітарних незвідних многочленів степеня n.*

Доведення. В силу теореми 8.3 середня кількість ітерацій алгоритму 8.3 дорівнює $O(n)$. За теоремою 8.2 алгоритм 8.3 потребує $O(n^3 \operatorname{length}(q))$ дій у полі $\mathbb{F}_q$. Звідси маємо твердження теореми. Друга частина твердження очевидна. □