Київський національний університет імені Тараса Шевченка
Механіко-математичний факультет

Євгенія Кочубінська

Лекції зі скінченних полів

Навчальний посібник

для студентів механіко – математичного факультету

Київ 2023

Кочубінська Є.А. Лекції зі скінченних полів. Навчальний посібник для студентів механіко – математичного факультету. – К., 2023.–131 с.

Рецензенти: д-р фіз.-мат. наук, проф. Д.А.Номіровський
канд. фіз.-мат. наук, доц. Д.О. Іваненко

Рекомендовано до друку вченою радою механіко-математичного факультету (Протокол №11 від 20 квітня 2023 року)

Світлій пам’яті Сергія Адамовича Овсієнка

Зміст

Вступ

Теорія скінченних полів почала неявно формуватися ще у роботах Гаусса та Галуа. Протягом останніх декад інтерес до скінченних полів значно зріс у великій мірі у зв'язку із застосуваннями до криптографії та теорії кодування. Проте, на жаль, цьому цікавому об'єкту не приділяють достатньої уваги у стандартному курсі алгебри. Навчальний посібник базується на спецкурсі, який автор читала студентам механіко-математичного факультету. Сподіваюся, що він стане у нагоді тим студентам, які хочуть трохи глибше познайомитися з предметом. Припускається, що читач знайомий з курсами лінійної алгебри і алгебри та теорії чисел, що читалися на першому та другому курсах.

Частина I

Будова скінченних полів

Розділ 1

Короткі відомості з теорії полів

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 нейтральним елементом 1 (цю групу називають мультиплікативною групою поля);
- додавання та множення пов'язані дистрибутивними законами: для довільних $a, b, c \in F$

$$a(b + c) = ab + ac.$$

Якщо поле складається зі скінченної кількості елементів, то поле називається *скінченним*.

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. Позначимо через $P(F)$ просте підполе поля F. Нехай $\operatorname{char} F = 0$, тоді всі елементи $n \cdot 1$, $n \in \mathbb{Z}$, є різними та утворюють підкільце поля F, яке ізоморфне $\mathbb{Z}$. Множина

$$Q(F) = \left\{ \frac{m \cdot 1}{n \cdot 1} \mid m, n \in \mathbb{Z}, n \neq 0 \right\}$$

є підполем поля F, яке ізоморфне $\mathbb{Q}$. Будь-яке підполе F має містити 1 та 0, а тому має містити і $Q(F)$.Отже, $(Q(F) \subset P(F)$. Оскільки $Q(F)$ є підполе F, то $P(F) \subset Q(F)$. □

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 $\mathbb{F} \to \mathbb{F}\colon a \mapsto a^p$ — 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 ненульового 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 інший 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 $f'(x) = qx^{q-1} - 1 = -1 \neq 0$ є 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

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

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 дільників 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 $l_1 \geqslant \ldots \geqslant l_t$, …, $j_1 \geqslant \ldots \geqslant j_r$.

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 $|A| = \operatorname{Exp} A$. 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 $|G| = \operatorname{Exp}(G)$. Нехай $|G| = n$, $\operatorname{Exp}(G) = k$. 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. $\square$

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, $\mathbb{F}_q(\zeta) = \mathbb{F}_r$. $\square$

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 $\alpha + 1$.

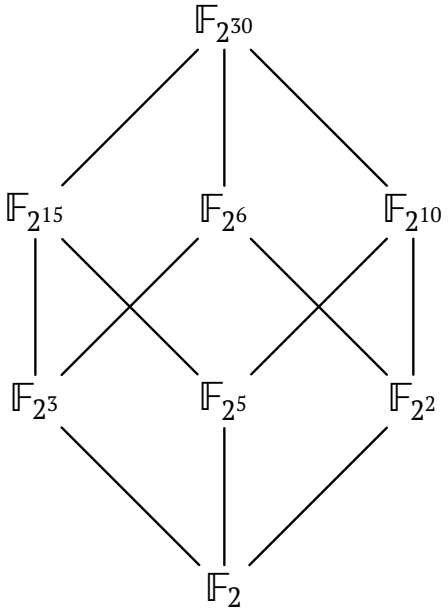
2. Розглянемо скінченне поле $\mathbb{F}_9 = \mathbb{F}_3(\beta)$, де β — корінь незвідного над $\mathbb{F}_3$ многочлена $x^2 + 1 = 0$. У цьому випадку β не є примітивним елементом поля $\mathbb{F}_9$, бо $\beta^4 = 1$, отже, не породжує поле $\mathbb{F}_9$.

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 кореням 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 Мебіуса 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 дільники 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 $\mathbb{F}_2$.

За теоремою 3.12 маємо

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

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 многочленів над полем $\mathbb{F}_2$ a) степеня 4; b) степеня 12.

Обчислимо добутки, використовуючи теорему 3.14:

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

$$\begin{aligned}I(2,12)&=\prod_{d|12}(x^{2^d}-x)^{\mu\left(\frac{12}{d}\right)}=\\&=(x^{4096}-x)^{\mu(1)}(x^{64}-x)^{\mu(2)}\times\\&\times(x^{16}-x)^{\mu(3)}(x^8-x)^{\mu(4)}(x^4-x)^{\mu(6)}(x^2-x)^{\mu(12)}=\\&=(x^{4096}-x)^1(x^{64}-x)^{-1}(x^{16}-x)^{-1}(x^8-x)^0(x^4-x)^1(x^2-x)^0=\\&=\frac{(x^{4096}-x)(x^4-x)}{(x^{64}-x)(x^{16}-x)}.\end{aligned}$$ □

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 α, α^q, $\alpha^{q^2}, \ldots, \alpha^{q^{d-1}}$, кожний з 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

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

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 $\alpha \in E$

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

□

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*

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

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

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

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

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

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

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

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

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

Доведення. Властивість а) випливає з означення норми.

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

Властивість а) означає, що відображення $\mathrm{N}_{\mathrm{F/K}}$ є гомоморфізмом мультиплікативної групи F^* в мультиплікативну групу K^*. Оскільки елементами ядра гомоморфізму $\mathrm{N}_{\mathrm{F/K}}$ 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, з урахуванням леми 2.3, виконуються рівності

$$\mathrm{N}_{\mathrm{F/K}}(\alpha^q) = (\mathrm{N}_{\mathrm{F/K}}(\alpha))^q = \mathrm{N}_{\mathrm{F/K}}(\alpha). \quad \square$$

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 $\alpha \in E$

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

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 $\{\beta_1, \ldots, \beta_m\}$ нази-*

ваються 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 коефіцієнти $c_1, c_2, c_3 \in \mathbb{F}_2$ визначаються рівностями

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

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

5.2 Теорема про нормальний базис

До найбільш важливих типів базисів поля F над підполем K належать поліноміальний та нормальний базиси. *Поліноміальний базис* $\{1, \alpha, \alpha^2, \dots \alpha^{m-1}\}$ — 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 $\left\{\alpha, \alpha^q, \dots, \alpha^{q^{m-1}}\right\}$, 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 множина 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

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

З пункту 4 леми 5.3 випливає, що коли покласти $v = v_1 + v_2 + \cdots + v_s$, 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 $\left\{\alpha, \alpha^2, 1 + \alpha + \alpha^2\right\}$ — 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

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

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 $\operatorname{Tr}_{F/K}(\alpha_i\alpha_j)$. 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* $\mathrm{Tr}_{\mathrm{F/K}}(\alpha_i\beta_j)$*;*

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

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

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

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

Означення 6.4. *Нехай b та 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 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 фактор-кільце $\mathbb{F}_p[x]/(f)$.

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 $\varphi(8)/(\operatorname{ord}_8 3) = 4/2 = 2$ 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 $f(x)=a_0+a_1x+\ldots+a_{n-1}x^{n-1}+x^n$ — 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

Теорема Веддербарна

Цей розділ стоїть трохи осторонь. Він не пов'язний з іншими розділами та не впливає на подальший виклад, але цей факт настільки красивий, що вартує бути наведеним. Відомий угорський математик Пал Ердеш називав Книгою місце, де Бог зберігає найкращі математичні доведення. Переказують, що в одній зі своїх лекцій він сказав: "Вірити в Бога необов'язково, але варто вірити в Книгу". Математики Мартін Айгнер та Гюнтер Ціглер 1998 року написали книгу "Доведення з Книги. Найкращі доведення з часів Евкліда і до наших днів" [4], яку присвятили Палу Ердешу. Зокрема, Книга містить теорему Веддербарна, яке стверджує, що кожне скінченне кільце з діленням є полем. Нагадаю, що кільце з діленням — це кільце з одиницею, у якому кожний ненульовий елемент є оборотним [1]. Отже, поле — це комутативне кільце з діленням. Існують різні доведення теореми Веддербарна (див., наприклад, [2, Теорема 2.55]), але я наведу доведення саме з Книги.

Перш ніж доводити теорему, пригадаємо деякі факти з теорії груп. Детальний виклад можна знайти, наприклад, в [1] або будь-якому іншому підручнику з теорії груп. Нехай G — група. *Центром* групи G називається множина

$$Z(G) = \{a \in G \mid ag = ga \; \forall g \in G\}$$

[1] Замість кільця з діленням часто вживають термін *тіло*.

всіх тих елементів групи G, яку комутують з усіма елементами групи G. *Централізатором* множини A у групі G називається множина

$$Z(A) = \{g \in G \mid ag = ga \; \forall a \in A\}$$

всіх тих елементів групи G, яку комутують з усіма елементами множини A.

Нормалізатором підмножини $A \subset$ у групі G називається множина

$$N(A) = \left\{g \in G \mid g^{-1}Ag = A\right\}.$$

Якщо $A = \{a\}$, то $Z(A) = N(A)$, бо $ga = ag \Leftrightarrow g^{-1}ag = a$.

Клас спряженості елемента $a \in G$ — це множина

$$C(a) = \left\{x^{-1}ax \mid x \in G\right\}$$

всіх елементів групи G, спряжених з елементом a.

Теорема 8.1 (Формула класів)**.** *Нехай $C_1, \ldots, C_k$ — всі неодноелементні класи спряженості групи G. Виберемо у кожному класі C_i представник a_i. Тоді*

$$|G| = |Z(G)| + \sum_{i=1}^{k} |C_i|.$$

Теорема 8.2. *Для довільного елемента a скінченної групи G*

$$|C(a)| = \frac{|G|}{|N(a)|} = \frac{|G|}{|Z(a)|}.$$

Лема 8.3. *Нехай R — кільце з діленням. Централізатор*

$$C_a = \{r \in R \mid ra = ar\}$$

довільного елемента $a \in R$ є підкільцем з діленням.

Доведення. Очевидно, що централізатор C_a елемента $a \in R$ містить 0 та 1. Для довільних $r, s \in C_a$ виконується

$$(r-s)a = ra - sa = ar - as = a(r-s),$$
$$(rs)a = r(sa) = r(as) = (ra)s = (ar)s = a(rs),$$

що дає $r - s \in C_a$, $rs \in C_a$, тобто C_a — підкільце кільця R.

Нехай $r \in C_a$ — довільний ненульовий елемент. Тоді

$$r^{-1}a = r^{-1}arr^{-1} = r^{-1}rar^{-1} = ar^{-1},$$

звідки $r^{-1} \in C_a$. Отже, C_a — підкільце з діленням. □

Центром $Z(R)$ кільця R називається множина всіх таких елементів кільця, які комутують з усіма елементами кільця, тобто

$$Z(R) = \bigcap_{a \in R} C_a.$$

З означення центру та леми 8.3 випливає, що центр кільця з діленням є комутативним кільцем з діленням, тобто полем.

Теорема 8.4 (Веддербарн)**.** *Кожне скінченне кільце з діленням є полем.*

Доведення. Нехай R — скінченне кільце з діленням. Тоді його центр Z є скінченним полем. Нехай $|Z| = q$.

Ми можемо розглядати кільце R та централізатор C_a елемента $a \in R$ як векторні простори над Z. Тоді $|R| = q^n$, де n — це розмірність R як векторного простору над Z, а $|C_a| = q^{n_a}$ для деякого належним чином обраного $n_a \in \mathbb{N}$.

Припустимо, що R не є полем. Це означає, що для деякого $a \in R$ централізатор C_a не збігається з усім кільцем R, тобто $n_a < n$, зокрема, $n > 1$, а також, що $Z \neq R$.

Розглянемо множину всіх різних класів спряженості у мультиплікативній групі R^* кільця R. За припущенням центр Z не збігається з усім кільцем R, а тому і для мультиплікативної

групи її центр $Z(R^*)$ не збігається з усією групою R^*. Як відомо, елемент групи належить центру тоді і лише тоді, коли його клас спряженості містить більше одного елемента, тому серед усіх класів спряженості групи R^* буде принаймні один, які містить принаймні 2 елементи. Оскільки R — кільце з діленням, то $|R^*| = |R| - 1 = q^n - 1$, $|Z(R^*)| = |Z| - 1 = q - 1$. Позначимо $C_a^* = C_a \setminus \{0\}$, тоді $|C_a^*| = q^{n_a} - 1$. Позначимо через $C(a_1), \ldots, C(a_k)$ всі різні неодноелементні класи спряженості групи R^* та запишемо формулу класів

$$|R^*| = |Z(R^*)| + \sum_{i=1}^{k} |C(a_i)| = |Z(R^*)| + \sum_{i=1}^{k} \frac{|R^*|}{|C_{a_i}^*|}.$$

Звідси маємо

$$q^n - 1 = q - 1 + \sum_{i=1}^{k} \frac{q^n - 1}{q^{n_i} - 1}. \tag{8.1}$$

З цієї рівності випливає, що $1 < \frac{q^n-1}{q^{n_i}-1}$ для всіх i.

Покажемо тепер, що з подільності $q^{n_i} - 1 \mid q^n - 1$ випливає подільність $n_i \mid n$. Розділимо з остачею n на n_i:

$$n = bn_i + r, \text{ де } 0 \neq r < n_i.$$

Враховуючи, що $q^{n_i} - 1 \mid q^n - 1$, отримаємо

$$q^{n_i} - 1 \mid (q^{bn_i+r} - 1) - (q^{n_i} - 1) = q^{n_i}(q^{(b-1)n_i+r} - 1).$$

Оскільки q^{n_i} та $q^{n_i} - 1$ взаємно прості, то $q^{n_i} - 1 \mid q^{(b-1)n_i+r} - 1$. Міркуючи таким чином і далі, прийдемо до того, що

$$q^{n_i} - 1 \mid q^r - 1,$$

де $0 \leqslant r < n_i$, а це можливо лише при $r = 0$. Отже, $n_i \mid n$. Підсумовуючи, отримаємо, що

$$n_i \mid n \text{ для всіх } i. \tag{8.2}$$

Згадаємо тепер про кругові многочлени (див. розділ 6). За теоремою 6.2

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

Причому коефіцієнти многочлена $Q_d(x)$ є цілими, більше того, вони дорівнюють ± 1.

Нехай $n_i \mid n$ — одне з чисел, що з'являється в (8.1). Тоді

$$x^n - 1 = \prod_{d|n} Q_d(x) = (x^{n_i} - 1)Q_n(x) \prod_{d|n, d\nmid n_i, d\neq n} Q_d(x).$$

Звідси маємо наступні відношення подільностіу кільці $\mathbb{Z}$:

$$Q_n(q) \mid q^n - 1 \text{ та } Q_n(q) \Big| \frac{q^n - 1}{q^{n_i} - 1}. \tag{8.3}$$

Оскільки (8.3) виконується для всіх i, то з формули класів (8.1) випливає

$$Q_n(q) \mid q - 1.$$

Покажемо, що це неможливо. Як вже відомо, $Q_n(x) = \prod(x - \zeta)$, де ζ пробігає всю множину примітивних коренів n-го степеня з 1. Нехай $\zeta_0 = a + bi$ — це один з цих коренів. За припущенням $Z \neq R$, тому $n > 1$. Тоді $\zeta_0 \neq 1$, з чого випливає, що $Re\,\zeta_0 = a < 1$. Враховуючи, що $|\zeta_0|^2 = a^2 + b^2 = 1$, обчислимо норму комплексного числа $q - \zeta_0$:

$$\begin{aligned} |q - \zeta_0|^2 = |q - a - bi|^2 &= (q - a)^2 + b^2 = \\ &= q^2 - 2aq + a^2 + b^2 = q^2 - 2aq + 1 > \\ &> q^2 - 2q + 1 (\text{ бо } a < 1) = \\ &= (q - 1)^2. \end{aligned}$$

Таким чином, $|q - \zeta_0| > q - 1$ виконується для всіх примітивних коренів n-го степеня з 1. На Рис.8.1 наведено геометричну ілюстрацію.

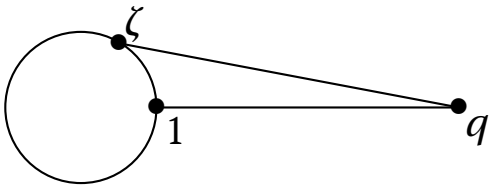


Рис. 8.1: $|q - \zeta| > |q - 1|$

Звідси випливає

$$|Q_n(q)| = \prod_{\zeta} |q - \zeta| > q - 1,$$

що означає, що $Q_n(q)$ не може бути дільником $q - 1$. Маємо суперечність. Отже, $n = 1$, а тому $R = Z$. Таким чином, R — комутативне кільце з діленням, тобто поле. Теорему доведено. □

Розділ 9

Порядки многочленів та примітивні многочлени

Лема 9.1. *Якщо $f \in \mathbb{F}_q[x]$ — многочлен степеня m, який задовольняє умови $f(0) \neq 0$, то існує натуральне число $e \leqslant q^m - 1$, для якого двочлен $x^e - 1$ ділиться на многочлен $f(x)$.*

Доведення. Факторкільце $R = \mathbb{F}_q[x]/(f)$ містить $q^m - 1$ ненульових елементів. Оскільки кожний з q^m класів суміжності $x^j + (f)$, $j = 0, 1, \ldots, q^m - 1$, є ненульовим елементом елементом факторкільця R, то повинні існувати такі цілі числа r та s, $0 \leqslant r < s \leqslant q^m - 1$, що $x^s \equiv x^r \pmod{f(x)}$. Оскільки многочлени x та $f(x)$ взаємно прості, то $x^{s-r} \equiv 1 \pmod{f(x)}$. Звідси випливає, що $x^{s-r} - 1$ ділиться на f, А $0 < s - r \leqslant q^m - 1$. □

Означення 9.1. *Нехай $f \in \mathbb{F}_q[x]$ — ненульовий многочлен. Якщо $f(0) \neq 0$, то найменше натуральне число e, для якого многочлен $f(x)$ ділить $x^e - 1$, називається* порядком *многочлена $f(x)$. Позначається* $\operatorname{ord}(f)$. *Якщо ж $f(0) = 0$, то многочлен $f(x)$ однозначно зображується у вигляді $f(x) = x^h g(x)$, де $h \in \mathbb{N}$, $g \in \mathbb{F}_q[x]$, $g(0) \neq 0$, і у цьому випадку* $\operatorname{ord}(f)$ *визначається як* $\operatorname{ord}(g)$.

Приклад 9.2. Нехай $f(x) = x^2 + x + 1 \in \mathbb{F}_2[x]$. Тоді $\operatorname{ord}(f) = 3$, бо f ділить $x^3 - 1$. □

Теорема 9.3. *Нехай $f \in \mathbb{F}_q[x]$ — незвідний многочлен степеня m, який задовольняє умову $f(0) \neq 0$. Порядок цього многочлена збігається з порядком довільного кореня цього многочлена у групі $\mathbb{F}^*_{q^m}$.*

Доведення. Поле $\mathbb{F}_{q^m}$ є полем розкладу многочлена f над полем $\mathbb{F}_q$. Всі корені многочлена f мають один і той самий порядок у групі $\mathbb{F}_{q^m}*$.

Нехай $\alpha \in \mathbb{F}^*_{q^m}$ — який-небудь корінь многочлена f. Рівність $\alpha^e = 1$ виконується тоді і лише тоді, коли многочлен $f(x)$ ділить $x^e - 1$. Твердження теореми випливає тепер з означення $\operatorname{ord}(f)$ та порядку елемента α в групі $\mathbb{F}^*_{q^m}$. □

Наслідок 9.4. *Якщо $f \in \mathbb{F}_q[x]$ — незвідний многочлен степеня m над полем $\mathbb{F}_q$, то його порядок ділить число $q^m - 1$.*

Доведення. Якщо $f(x) = cx$, де $c \in \mathbb{F}^*_q$, то $\operatorname{ord}(f) = 1$. В іншому разі результат випливає з теореми 9.3 та того факту, що $|\mathbb{F}^*_{q^m}| = q^m - 1$. □

Теорема 9.5. *Число унітарних незвідних многочленів з $\mathbb{F}_q[x]$ степеня m порядку e і дорівнює*

- *$\varphi(e)/m$, якщо $e \geqslant 2$, а m — показник, якому належить число q за модулем e, тобто $m = \operatorname{ord}_e(q)$;*
- *2, якщо $m = e = 1$;*
- *0 в усіх інших випадках.*

Зокрема, ступінь незвідного многочлена з $\mathbb{F}_q[x]$ порядку e повинен збігатися з показником, якому належить числу q за модулем e.

Доведення. Нехай $f(x) \in \mathbb{F}_q[x]$ — незвідний многочлен, причому $f(0) \neq 0$. Тоді за теоремою 9.3 $\operatorname{ord}(f) = e$ тоді і лише тоді,

коли всі корені многочлена $f(x)$ є первісними коренями степеня e з одиниці над полем $\mathbb{F}_q$, тобто коли многочлен f ділить круговий многочлен Q_e.

З властивостей кругового многочлена випливає, що всі незвідні дільники многочлена Q_e мають один і той самий степінь, який дорівнює найменшому натуральному числу m, для якого $q^m \equiv 1 \pmod{e}$. Кількість таких дільників дорівнює $\varphi(e)/m$. Для $m = e = 1$ потрібно ще врахувати многочлена $f(x) = x$. □

Лема 9.6. *Нехай c — натуральне число, нехай $f \in \mathbb{F}_q[x]$, $f(0) \neq 0$. Многочлен f ділить многочлен $x^c - 1$ тоді і лише тоді, коли* $\operatorname{ord}(f)$ *ділить число c.*

Доведення. Достатність. Якщо число $e = \operatorname{ord}(f)$ ділить c, то многочлен $f(x)$ ділить $x^e - 1$, а $x^e - 1$ ділить $x^c - 1$.

Необхідність. Нехай $e = \operatorname{ord}(f)$, нехай $f(x) \mid x^e - 1$. За означенням порядку многочлена $c \geqslant e$. Розділимо c на e з остачею

$$c = me + r, \quad \text{де } m \in \mathbb{N},\ 0 \leqslant r < e.$$

Тоді

$$x^c - 1 = (x^{me} - 1)x^r + (x^r - 1).$$

Оскільки многочлен $f(x)$ ділить $x^{me} - 1$ та $x^c - 1$, то $f(x)$ ділить $x^r - 1$, а це можливо лише при $r = 0$. Отже, число e ділить число c. □

Наслідок 9.7. *Якщо $e_1, e_2 \in \mathbb{N}$, то в $\mathbb{F}_q[x]$ НСД$(x^{e_1} - 1, x^{e_2} - 1) = x^d - 1$, де $d =$ НСД(e_1, e_2).*

Доведення. Нехай $f(x)$ — унітарний НСД многочленів $x^{e_1} - 1$ та $x^{e_2} - 1$, $d = \text{НСД}(e_1, e_2)$. Оскільки $x^d - 1$ — спільний дільник цих многочленів, то $x^d - 1$ ділить $f(x)$. З іншого боку, оскільки $f(x)$ ділить $x^{e_1} - 1$ та $x^{e_2} - 1$, то за лемою 9.6 порядок многочлена $f(x)$ ділить e_1 та e_2. Отже, $\operatorname{ord}(f)$ ділить d, а тому за лемою 9.6 многочлен $f(x)$ ділить $x^d - 1$. Таким чином, $f(x) = x^d - 1$. □

Теорема 9.8. *Нехай $n \in \mathbb{N}$, $g(x)$ — незвідний многочлен над скінченним полем характеристики p, такий, що $g(0) \neq 0$. Тоді для многочлена вигляду $f = g^n$*

$$\operatorname{ord}(f) = \operatorname{ord}(g^n) = p^t \operatorname{ord}(g),$$

де t — найменше ціле число, для якого $p^t \geqslant n$.

Доведення. Нехай $e = \operatorname{ord}(g)$, $c = \operatorname{ord}(f)$. З подільності $x^c - 1$ на $f(x)$ випливає подільність $x^c - 1$ на $g(x)$. Тому з леми 9.6 випливає, що $e \mid c$.

Многочлен $g(x)$ ділить $x^e - 1$, тому $f(x)$ ділить $(x^e - 1)^n$, а отже, ділить і многочлен $(x^e - 1)^{p^t} = x^{ep^t} - 1$. Таким чином, згідно з лемою 9.6 число c ділить число ep^t. Отже, число c є числом вигляду $c = ep^s$, де $0 \leqslant s \leqslant t$.

За наслідком 9.4 з теореми 9.3 число e не ділиться на p. Тому всі корені многочлена $x^e - 1$ є простими. Звідси випливає, що всі корені многочлена $x^{ep^s} - 1 = (x^e - 1)^{p^s}$ мають кратність p^s. Оскільки многочлен $f(x) = (g(x))^n$ ділить $x^{ep^s} - 1$, то порівнявши кратності коренів, отримаємо, що $p^s \geqslant n$, так що $s \geqslant t$. Таким чином, $s = t$ та $c = ep^t$. □

Приклад 9.9. Знайдемо порядок многочлена

$$g(x) = (x^2 + x + 1)^3 = (f(x))^3 \in \mathbb{F}_2[x].$$

За прикладом 9.2 $\operatorname{ord}(g) = 3$. Найменше t, таке, що $2^t \geqslant 3$ — це $t = 2$. Отже, $\operatorname{ord}(g) = 2^2 \cdot 3 = 12$. □

Теорема 9.10. *Нехай $g_1, \ldots, g_k$ — попарно взаємно прості ненульові многочлени над скінченним полем $\mathbb{F}_q$, нехай $f = g_1 \ldots g_k$. Тоді*

$$\operatorname{ord}(f) = \operatorname{ord}(g_1 \ldots g_k) = НСК(\operatorname{ord}(g_1), \ldots, \operatorname{ord}(g_k)).$$

Доведення. Для доведення досить розглянути випадок, коли $g_i(0) \neq 0$, $i = 1, \ldots, k$. Покладемо

$$e = \operatorname{ord}(f),\ e_i = \operatorname{ord}(g_i), \quad i = 1, \ldots, k.$$

Нехай $c = \text{НСК}(e_1, \ldots, e_k)$. Тоді кожний многочлен $g_i(x)$, $1 \leqslant i \leqslant k$, ділить двочлен $x^{e_i} - 1$, а тому ділить $x^c - 1$. Оскільки многочлени $g_1, \ldots, g_k$ — попарно взаємно прості, то многочлен $f(x) = g_1(x) \ldots g_k(x)$ ділить $x^c - 1$. Враховуючи лему 9.6, маємо, що e ділить c. З іншого боку, $f(x)$ ділить $x^e - 1$, а тому кожний многочлен $g_i(x)$, $1 \leqslant i \leqslant k$, ділить $x^e - 1$. Знов застосувавши лему 9.6, одержимо, що кожне з чисел e_i, $1 \leqslant i \leqslant k$, ділить e, а тому c ділить e. Отже, $c = e$. □

З теорем 9.8 та 9.10 випливає теорема.

Теорема 9.11. *Нехай $\mathbb{F}_q$ — скінченне поле характеристики p. Якщо $f = a f_1^{n_1} f_2^{n_2} \ldots f_k^{n_k}$, $a \in \mathbb{F}_q^*$, — канонічний розклад у кільці $\mathbb{F}_q[x]$ многочлена $f(x) \in \mathbb{F}_q[x]$, $f(0) \neq 0$, то*

$$\operatorname{ord}(f) = p^t \mathit{НСК}\big(\operatorname{ord}(f_1, \operatorname{ord}(f_2), \ldots, \operatorname{ord}(f_k)\big),$$

де t — найменше ціле число, для якого $p^t \geqslant \max n_1, \ldots, n_k$.

Приклад 9.12. Знайдемо порядок многочлена

$$f(x) = (x^2 + x + 1)^3 (x^3 + x + 1) \in \mathbb{F}_2[x].$$

З прикладу 9.9 $\operatorname{ord}(x^2+x+1)^3 = 12$. Очевидно, $\operatorname{ord}(x^3+x+1) \neq 1$, а оскільки $\operatorname{ord}(x^3+x+1)$ має ділити $2^3-1 = 7$, то $\operatorname{ord}(x^3+x+1) = 7$. Таким чином, $\operatorname{ord}(f) = \text{НСК}(7, 12) = 84$. Зауважимо, що $\deg(f) = 9$, а $84 \nmid 2^9 - 1$. Отже, наслідок 9.4 з теореми 9.3 не справджується для звідних многочленів. □

Приклад 9.13 (Обчислення порядків)**.** Одним з методів знаходження порядку незвідного многочлена $f \in \mathbb{F}_q[x]$, який

задовольняє умову $f(0) \neq 0$, базується на тому факті, що порядок e многочлена f є найменшим таким натуральним числом, що

$$x^e \equiv 1 \pmod{f(x)}.$$

За наслідком 9.4 число e ділить $q^m - 1$, де m — степінь многочлена f. Припустимо, що $q^m > 2$. Розкладемо це число на прості співмножники:

$$q^m - 1 = \prod_{j=1}^{s} p_j^{r_j}.$$

Для кожного j, $1 \leqslant j \leq s$, знайдемо лишки одночленів $x^{(q^m-1)/p_j}$ за модулем $f(x)$. Зазвичай це робиться шляхом перемноження належним чином обраного набору лишків за модулем $f(x)$ степенів $x, x^q, x^{q^2}, \ldots, x^{q^{m-1}}$ змінної x. Якщо виявиться, що $x^{(q^{m-1})/p_j} \neq 1 \pmod{f(x)}$, то число e ділиться на $p_j^{r_j}$, а якщо $x^{(q^{m-1})/p_j} = 1 \pmod{f(x)}$, то число e не ділиться на $p_j^{r_j}$. В останньому випадку, ми з'ясовуємо, чи буде число e ділитися на $p_j^{r_j-1}, p_j^{r_j-2}, \ldots, p_j$, обчислюючи відповідно лишки за модулем $f(x)$ наступних степенів змінної x:

$$x^{(q^{m-1})/p_j^2},\ x^{(q^{m-1})/p_j^3},\ \ldots,\ x^{(q^{m-1})/p_j^{r_j}}.$$

Такий підрахунок проводиться для кожного простого дільника p_j числа $q^m - 1$, в результаті знаходиться число $e = \operatorname{ord}(f)$.

Ключовим у використанні цього метода є розклад числа $q^m - 1$ на прості множники. Існують великі таблиці для розкладу чисел такого вигляду, особливо для випадку $q = 2$.

Розглянемо незвідний многочлен $f(x) = x^3 + 2x + 1 \in \mathbb{F}_3[x]$. Знайдемо його порядок методом, описаним вище методом.

У нас $q = 3$, $m = 3$. Нехай $e = \operatorname{ord}(f)$. За наслідком 9.4 $e \mid 3^3 - 1 = 26$. Розкладемо число 26 на прості множники $26 = 2 \cdot 13$. Покладемо $p_1 = 2$, $r_1 = 1$, $p_2 = 13$, $r_2 = 1$.

($j = 1$) Обчислимо $x^{26/13} = x^2 \neq 1 \pmod f$. Отже, $2 \mid e$.

($j = 2$) Обчислимо $x^{26/2} = x^{13} = x \cdot x^3 \cdot x^9 \equiv x(x+1)(x+2) = x(x^2+2) \equiv x^3 + 2x \equiv 2x + x + 2 \equiv\neq 1 \pmod f$. Отже, $13 \mid e$.

Отже, $e = 26$.

Зауваження. В обчисленнях використали, що $x^3 \equiv x + 3 \pmod f$, а тоді $x^3 = (x+2)^2 = x^3+8 = x^3+2 \equiv x+1 \pmod f$. □

Приклад 9.14. Розглянемо незвідний многочлен $f(x) = x^4 + x^3+x^2+2x+2 \in \mathbb{F}_3[x]$. Знайдемо його порядок описаним вище методом.

У нас $q = 3$, $m = 4$. Нехай $e = \operatorname{ord}(f)$. За наслідком 9.4 $e \mid 3^4 - 1 = 80$. Розкладемо число 80 на прості множники $80 = 2^4 \cdot 5$. Покладемо $p_1 = 2$, $r_1 = 4$, $p_2 = 5$, $r_2 = 1$.

($j = 1$) Обчислимо $x^{40} \pmod f$. Для цього врахуємо, що $x^{40} = x^{27} \cdot x^9 \cdot x^3 \cdot x$. Далі обчислимо покроково:

$$x^9 \equiv 2x^3 + x^2 + 2 \pmod f$$
$$x^{27} \equiv 2x^2 + 2x \pmod f$$
$$x^{40} \equiv (2x^2 + 2x) \cdot (2x^3 + x^2 + 2) \cdot x^3 \cdot x \equiv (2x^3 + x + 2) \cdot x^3 \cdot x$$
$$\equiv (2x^3 + 2x^2 + 2x + 1) \cdot x \equiv 2 \not\equiv 1 \pmod f.$$

Отже, $40 \mid e$.

($j = 2$) Обчислимо $x^{16} \pmod f$. Для цього врахуємо, що $x^{16} = x^9 \cdot x^3 \cdot x^3 \cdot x$. Далі обчислимо покроково:

$$x^9 \equiv 2x^3 + x^2 + 2 \pmod f$$
$$x^{16} \equiv (2x^3 + x^2 + 2) \cdot x^3 \cdot x^3 \cdot x \equiv (2x^2 + x + 2) \cdot x^3 \cdot x \equiv$$
$$\equiv (x^3 + x + 2) \cdot x \equiv 2x^3 + 1 \not\equiv 1 \pmod f.$$

Отже, $16 \mid e$.

З умов $e \mid 80$, $40 \mid e$ та $16 \mid e$ маємо, що $e = 80$. □

Зауважимо, що отримані результати узгоджуються з теоремою 9.20 ($x^{40} \equiv 2 \pmod{f(x)}$).

Існує зв'язок між порядками деяких многочленів, які можна одержати одне з одного простими алгебраїчними перетвореннями.

Нехай дано многочлен

$$f(x) = a_n x^n + a_{n-1}^{n-1} + \ldots + a_1 x + a_0 \in \mathbb{F}_q[x],$$

де $a_n \neq 0$. Тоді двоїстий до нього многочлен визначається так:

$$f^*(x)x^n f(\frac{1}{x}) = a_o x^n + a_1^{n-1} + \ldots + a_{n-1} + a_n.$$

Теорема 9.15. *Нехай f — ненульовий многочлен з $\mathbb{F}_q[x]$, f^* — двоїстий до нього многочлен. Тоді* $\mathrm{ord}(f) = \mathrm{ord}(f^*)$.

Існує також зв'язок між порядками многолченів $f(x)$ та $f(-x)$. Оскільки для полів $\mathbb{F}_{2^m}$ $f(-x) = f(x)$, то досить розглянути лише поля непарної характеристики.

Теорема 9.16. *Нехай q — непарне, нехай $f(x) \in \mathbb{F}_q[x]$ — многочлен додатного степеня, такий, що $f(0) \neq 0$, нехай $e = \mathrm{ord}(f(x))$, $e' = \mathrm{ord}(f(-x))$. Тоді $e' = e$, якщо e ділиться на 4; і $e' = 2e$, якщо e — непарне. Якщо ж $e = 2h$, де h — непарне, то $e' = e/2$ у випадку, коли всі незвідні дільники многочлена f мають парний порядок, і $e' = e$ у протилежному випадку.*

9.1 Примітивні многочлени.

Означення 9.2. *Многочлен $f \in \mathbb{F}_q[x]$ степеня $m \geqslant 1$ називається примітивним многочленом над полем $\mathbb{F}_q$, якщо він є мінімальним многочленом над $\mathbb{F}_q$ деякого примітивного елемента розширення $\mathbb{F}_{q^m}$ поля $\mathbb{F}_q$.*

Таким чином, примітивний многочлен над $\mathbb{F}_q$ степеня m — це многочлен, який задовольняє умови:

- $f(x)$ — нормований;
- $f(x)$ — незвідний над $\mathbb{F}_q$;
- $f(x)$ має корінь $\alpha \in \mathbb{F}_{q^m}$, який є твірним мультиплікативної групи $\mathbb{F}_{q^m}^*$ поля $\mathbb{F}_{q^m}$.

Теорема 9.17. *Многочлен $f \in \mathbb{F}_q[x]$ степеня m є примітивним многочленом над $\mathbb{F}_q$ тоді і лише тоді, коли $f(x)$ — нормований многочлен, такий, що $f(0) \neq 0$ та* $\operatorname{ord}(f) = q^m - 1$.

Доведення. Необхідність. Якщо f — примітивний многочлен над $\mathbb{F}_q$, то він є нормованим многочленом, який задовольняє умову $f(0) \neq 0$. Оскільки f — незвідний над $\mathbb{F}_q$, то з теореми 9.3 та того факту, що його коренем є примітивний елемент розширення $\mathbb{F}_{q^m}$ поля $\mathbb{F}_q$, випливає, що $\operatorname{ord}(f) = q^m - 1$.

Достатність. З умови $\operatorname{ord}(f) = q^m - 1$ випливає, що $m \geqslant 1$. Покажемо, що f незвідний над $\mathbb{F}_q$. Припустимо, що він є звідним над $\mathbb{F}_q$. Тоді або f є степенем деякого незвідного многочлена, або його можна подати у вигляді добутку двох взаємно простих многочленів додатного степеня. У першому випадку нехай $f = g^b$, де многочлен $g \in \mathbb{F}_q[x]$ — незвідний над $\mathbb{F}_q$, $g(0) \neq 0$, $b \geqslant 2$. Тоді за теоремою 9.8 порядок многочлена повинен ділитися на характеристику поля $\mathbb{F}_q$, але $q^m - 1$ не ділиться на неї, отже, приходимо до суперечності. У другому випадку нехай $f = g_1 g_2$, де g_1, g_2 — взаємно прості многочлени з $\mathbb{F}_q[x]$ додатних степенів m_1 та m_2 відповідно. Якщо $e_i = \operatorname{ord}(g_i)$, $i = 1, 2$, то за теоремою 9.10 маємо $\operatorname{ord}(f) < e_1 e_2$. Крім того за лемою 9.1 $e_i \leqslant q_i^m - 1$, $i = 1, 2$, так що

$$\operatorname{ord}(f) \leqslant (q^{m_1} - 1)(q^{m_2} - 1) < q^{m_1+m_2} - 1 = q^m - 1,$$

і знов приходимо до суперечності. Отже, многочлен f незвідний над $\mathbb{F}_q$, а тоді з теореми 9.3 та нормованості f маємо, що f — примітивний многочлен над $\mathbb{F}_q$. □

Зауважимо, що вимога $f(0) \neq 0$ знадобилася лише для того, щоб виключити випадок незвідного многочлена $f(x) = x$ в $\mathbb{F}_2$.

Приклад 9.18. Незвідний многочлен $f(x) = x^4+x^3+x^2+2x+2 \in \mathbb{F}_3[x]$ є примітивним, бо $\operatorname{ord}(f) = 3^4 - 1$. □

Лема 9.19. *Нехай $f \in \mathbb{F}_q[x]$ — многочлен додатного степеня, який задовольняє умову $f(0) \neq 0$. Нехай $r \in \mathbb{N}$ — найменше таке число, для якого $x^r \equiv a \pmod{f(x)}$, де $a \in \mathbb{F}_q^*$ однозначно визначений. Тоді $\operatorname{ord}(f) = hr$, де h — порядок елемента a в $\mathbb{F}_q^*$.*

Доведення. Покладемо $e = \operatorname{ord}(f)$. Оскільки $x^e \equiv 1 \pmod{f(x)}$, то отримаємо, що $e \geqslant r$. Тому можемо записати $e = sr + t$, де $s \in \mathbb{N}$, $0 \leqslant t < r$. Тоді

$$1 \equiv x^e \equiv x^{sr+t} =\equiv a^s x^t \pmod{f(x)}, \tag{9.1}$$

так що $x^t = a^{-s} \pmod{f(x)}$, а тому з визначення числа r одержимо, що $t = 0$. З порівняння (9.1) тоді видно, що $a^s \equiv 1 \pmod{f(x)}$, тобто $a^s = 1$, а тому $s \geqslant h$ та $e \geqslant hr$. З іншого боку, $x^{hr} \equiv a^h \equiv 1 \pmod{f(x)}$, так що $hr \geqslant e$. Отже, $e = hr$. □

Теорема 9.20. *Нормований многочлен $f \in \mathbb{F}_q[x]$ степеня $m \geqslant 2$ є примітивним многочленом над полем $\mathbb{F}_q$ тоді і лише тоді, коли $(-1)^m f(0)$ — примітивний елемент над $\mathbb{F}_q$ і найменшим натуральним числом r, для якого $x^r \equiv a \pmod{f(x)}$ для деякого $a \in \mathbb{F}_q$, є*

$$r = \frac{q^m - 1}{q - 1}.$$

Якщо $f(x)$ — примітивний многочлена над $\mathbb{F}_q$, то має місце порівняння

$$x^r \equiv (-1)^m f(0) \pmod{f(x)}.$$

Доведення. Необхідність. Якщо многочлен f примітивний над полем $\mathbb{F}_q$, то f має корінь $\alpha \in \mathbb{F}_{q^m}$, який є примітивним елементом поля $\mathbb{F}_{q^m}$. Обчислимо норму $\mathrm{N}_{\mathrm{F/K}}(\alpha)$, $F = \mathbb{F}_{q^m}$, $K = \mathbb{F}_q$.

За означенням $\mathrm{N}_{\mathrm{F/K}}(\alpha) = \alpha^{\frac{q^m-1}{q-1}}$. З іншого боку, норма елемента дорівнює вільному члену характеристичного многочлена елемента α, тому $\mathrm{N}_{\mathrm{F/K}}(\alpha) = (-1)^m f(0)$. Отже, маємо рівність

$$(-1)^m f(0) = \alpha^{\frac{q^m-1}{q-1}}. \tag{9.2}$$

З неї випливає, що порядок елемента $(-1)^m f(0)$ в групі $\mathbb{F}_q^*$ дорівнює $q-1$, тобто $(-1)^m f(0)$ — примітивний елемент поля $\mathbb{F}_q$.

Оскільки f — мінімальний многочлен елемента α над полем $\mathbb{F}_q$, то з властивостей мінімального многочлена та рівності (9.2) випливає, що

$$x^{\frac{q^m-1}{q-1}} \equiv (-1)^m f(0) \pmod{f(x)},$$

так що $r \leqslant \frac{q^m-1}{q-1}$. Але з теореми 9.17 та леми 9.19 випливає, що $q^m - 1 = \mathrm{ord}(f) \leqslant (q-1)r$, так що $r \geqslant \frac{(q^m-1)}{q-1}$. Отже, $r = \frac{(q^m-1)}{q-1}$.

Достатність. Припустимо, що умови теореми виконуються. З рівності $r = \frac{(q^m-1)}{q-1}$ та леми 9.19 тоді випливає, що числа $\mathrm{ord}(f)$ та q взаємно прості. З теореми 9.10 випливає, що многочлен f розкладається в добуток $f = f_1 f_2 \dots f_k$ нормованих незвідних над $\mathbb{F}_q$ многочленів $f_1, f_2, \dots, f_k$. Якщо $m_i = \deg(f_i)$, то $\mathrm{ord}(f_i)$ ділить $q^{m_i} - 1$, $1 \leqslant i \leqslant k$ (наслідок 1 з теореми 1). Оскільки $q^{m_i} - 1$ ділить число

$$d = \frac{(q^{m_1}-1)\dots(q^{m_k}-1)}{(q-1)^{k-1}},$$

то число $\mathrm{ord}(f_i)$ ділить $x^d - 1$ для $1 \leqslant i \leqslant k$. З леми 2 з попередньої лекції випливає, що $f_i(x)$ ділить $x^d - 1$ для $1 \leqslant i \leqslant k$, так що многочлен $f(x)$ ділить $x^d - 1$. Якщо $k \geqslant 2$, то

$$d < \frac{q^{m_1+\dots+m_k} - 1}{q-1} = \frac{q^m - 1}{q-1} = r,$$

що суперечить визначенню числа r. Таким чином, $k = 1$ і многочлен f є незвідним над $\mathbb{F}_q$.

Якщо $\beta \in \mathbb{F}_{q^m}$ — корінь многочлена f, то з міркувань, подібних до тих, які привели до (9.2), прийдемо до $\beta^r = (-1)^m f(0)$, так що $x^r \equiv (-1)^m f(0) \pmod{f(x)}$. Оскільки порядок елемента $(-1)^m f(0)$ в групі $\mathbb{F}_q^*$ дорівнює $q-1$, то з леми 9.19 випливає, що $\operatorname{ord}(f) = q^m - 1$, так що за теоремою 9.17 f є примітивним многочленом над $\mathbb{F}_q$. □

Розділ 10

Побудова незвідних многоленів

Теорема 10.1. *Нехай $I(q, n; x)$ позначає добуток всіх незвідних нормованих многочленів степеня n з кільця $\mathbb{F}_q[x]$. Тоді для $n > 1$ має місце формула*

$$I(q, n; x) = \prod_{\substack{m \mid q^n - 1 \\ \operatorname{ord}_m(q) = n}} Q_m(x). \tag{10.1}$$

Доведення. Для $n > 1$ нехай S — множина елементів поля $\mathbb{F}_{q^n}$, які мають степінь n на полем $\mathbb{F}_q$. Тоді кожний елемент $\alpha \in S$ має мінімальний многочлен степеня n над $\mathbb{F}_q$, а тому є коренем многочлена $I(q, n; x)$. З іншого боку, якщо β — корінь многочлена $I(q, n; x)$, то він одночасно є коренем деякого нормованого незвідного многочлена степеня n з $\mathbb{F}_q[x]$, а це означає, що $\beta \in S$.Тому

$$I(q, n; x) = \prod_{\alpha \in S} (x - \alpha).$$

Якщо $\alpha \in S$, то $\alpha \in \mathbb{F}_{q^n}^*$, отже, порядок елемента α в цій мультиплікативній групі ділить число $q^n - 1$.

Зауважимо, що елемент $\gamma \in \mathbb{F}_{q^n}^*$ є елементом деякого власного підполя $\mathbb{F}_{q^d}$ поля $\mathbb{F}_{q^n}$ тоді і лише тоді, коли $\gamma^{q^d} = \gamma$, тобто якщо $\operatorname{ord}(\gamma) \mid q^d - 1$. Тому порядок m елемента α з S повинен бути таким, щоб n було найменшим таким натуральним

числом, що $q^n \equiv 1 \pmod{m}$. Нехай m — додатний дільник числа $q^n - 1$ з такою властивістю. Позначимо S_m — множина елементів порядку m з S. Тоді S буде об'єднаннями множин S_m, що не перетинаються, так що можна записати

$$I(q, n; x) = \prod_m \prod_{\alpha \in S_m} (x - \alpha).$$

Множина S_m складається з усіх елементів групи $\mathbb{F}_{q^n}^*$, які мають порядок m. Іншими словами, S_m — це множина первісних коренів m-го степеня з одиниці над $\mathbb{F}_q$. Тоді з означення кругового многочлена випливає, що

$$\prod_{\alpha \in S} (x - \alpha) = Q_m(x).$$

□

Приклад 10.2. Знайдемо всі нормовані незвідні многочлени степеня 4 над полем $\mathbb{F}_2$. З рівності (10.1) випливає, що $I(2, 4; x) = Q_5(x)Q_{15}(x)$. (Дільниками числа $2^4 - 1 = 15$ є 1, 3, 5, 15. Серед них умові, що $n = 4$ є мультиплікативним порядком $q = 2$ за модулем m задовольняють лише $m = 5, 15$.)

За теоремою 6.7 (ii) многочлен $Q_n(x)$ розкладається в добуток $\varphi(n)/d$ незвідних нормованих многочленів степеня d, де d — найменше таке натуральне число, що $q^n \equiv 1 \pmod{n}$. Тому $Q_5 = x^4 + x^3 + x^2 + x + 1$ є незвідним в $\mathbb{F}_2$, бо $\varphi(5) = 4$, $d = 4$. Круговий многочлен $Q_{15}(x)$ розкладається в добуток $\varphi(15)/4 = 2$ незвідних многочленів степеня 4. Оскільки $Q_5(x+1) = x^4 + x^3 + 1$ — незвідний многочлен над $\mathbb{F}_2$, то він повинен ділити $Q_{15}(x)$, отже,

$$Q_{15}(x) = x^8 + x^7 + x^5 + x^4 + x^3 + x + 1 = \left(x^4 + x + 1\right)\left(x^4 + x^3 + 1\right).$$

Тому незвідними над $\mathbb{F}_2$ многочленами 4-го степеня є $x^4 + x^3 + x^2 + x + 1$, $x^4 + x + 1$ та $x^4 + x^3 + 1$. □

Теорема 10.3. *Нехай f — незвідний многочлен над $\mathbb{F}_q$ степеня n і $k \in \mathbb{N}$. Тоді в кільці $\mathbb{F}_{q^k}$ многочлен f розкладається в добуток на d незвідних співмножників одного і того самого степеня n/d, де $d = НСД\,(k, n)$.*

Доведення. Випадок $f(0) = 0$ є тривіальним. Припустимо, що $f(0) \neq 0$. Нехай g — незвідний дільник многочлена f з $\mathbb{F}_{q^k}$. Якщо $\operatorname{ord}(f) = e$, то і $\operatorname{ord}(g) = e$, бо корені многочлена g є в той самий час і коренями f. Мультиплікативний порядок числа q за модулем e дорівнює n. Степінь многочлена g дорівнює мультиплікативному порядку q^k за модулем e. Степені q^j, $j = 0, 1, \ldots$, які розглядаються за модулем e, утворюють циклічну групу порядку n. Отже, мультиплікативний порядок числа q^k за модулем e дорівнює n/d, а тому і степінь многочлена g дорівнює n/d. □

Наслідок 10.4. *Незвідний над полем $\mathbb{F}_q$ многочлен степеня n лишається незвідним над розширенням $\mathbb{F}_{q^k}$ цього поля тоді і лише тоді, коли числа n та k взаємно прості.*

Лема 10.5. *Нехай $s \geqslant 2$ та $e \geqslant 2$ — взаємно прості цілі числа, і нехай m — мультиплікативний порядок числа s за модулем e. Нехай $t \geqslant 2$ — ціле число, прості дільники якого ділять число e, але не ділять $(s^m - 1)/e$. І нехай $s^m \equiv 1 \pmod 4$, коли $t \equiv 0 \pmod 4$. Тоді мультиплікативний порядок числа s за модулем et дорівнює mt.*

Теорема 10.6. *Нехай $f_1(x), \ldots, f_N(x)$ — всі різні нормовані незвідні многочлени з $\mathbb{F}_q[x]$ степеня m і порядку e, і нехай $t \geqslant 2$ — деяке ціле число, прості дільники якого ділять e, але не ділять $(q^m - 1)/e$. Нехай $q^m \equiv 1 \pmod 4$, якщо $t \equiv 0 \pmod 4$. Тоді $f_1(x^t), \ldots, f_N(x^t)$ — всі різні нормовані незвідні многочлени з $\mathbb{F}_q[x]$ степеня mt порядку et.*

Доведення. З умови теореми випливає, що $e \geqslant 2$. За теоремою 9.5 нормований незвідний многочлен степеня m і порядку $e \geqslant 2$ існує лише тоді, коли m є мультиплікативним порядком q за модулем e. В цьому випадку $N = \varphi(e)/m$. За лемою 10.5 мультиплікативний порядок числа q за модулем et дорівнює mt. Тоді з рівності $\varphi(et)/mt = \varphi(e)/m$ випливає, що кількість нормованих незвідних многочленів степеня mt і порядку et в кільці $\mathbb{F}_q[x]$ теж дорівнює N.

Тому лишилося показати, що кожний з многочленів $f_j(x^t)$, $1 \leqslant j \leqslant N$, є незвідним над $\mathbb{F}_q$ і має порядок et. Оскільки корені кожного многочлена $f_j(x)$ є первісними коренями степеня e з одиниці над $\mathbb{F}_q$ (теорема **??**), то f_j ділить круговий многочлен $Q_e(x)$ над $\mathbb{F}_q$. Але тоді многочлен $f_j(x^t)$ ділить $Q_e(x^t)$, а тому $Q_e(x^t) = Q_{et}(x)$ (бо для всіх $m \in \mathbb{N}$ кратних простому числу p виконується $Q_{mp}(x) = Q_m(x^p)$. Довести!) Таким чином $f_j(x^t)$ ділить $Q_{et}(x)$. За теоремою 6.7 (ii) степінь кожного незвідного дільника многочлена $Q_{et}(x)$ в $\mathbb{F}_q[x]$ дорівнює мультиплікативному порядку q за модулем et. Цей порядок дорівнює mt. Оскільки многочлен $f_j(x^t)$ має степінь mt, то

він незвідний в кільці $\mathbb{F}_q[x]$. Крім того, оскільки $f_j(x^t)$ ділить $Q_{et}(x)$, то порядок многочлена $f_j(x^t)$ дорівнює et. □

Приклад 10.7. Незвідними многочленами степеня $m = 4$ і порядку $e = 15$ в кільці $\mathbb{F}_2[x]$ є $x^4 + x + 1$ та $x^4 + x^3 + 1$.

Число $t = 3$ задовольняє умови теореми ($t|15$, але $t \nmid (2^4 - 1)/15$. Тому незвідними многочленами в $\mathbb{F}_2[x]$ степеня $mt = 12$ та порядку $et = 45$ є $x^{12} + x^3 + 1$ та $x^{12} + x^9 + 1$. □

Випадок $t \equiv 0 \pmod 4$ та $q^m \equiv 3 \pmod 4$ не охоплюється теоремою 10.6. Тут повинно бути $q \equiv 3 \pmod 4$ і непарне m.

Теорема 10.8. *Нехай $f_1(x), \ldots, f_N(x)$ — всі різні нормовані незвідні многочлени з $\mathbb{F}_q[x]$ непарного степеня m і порядку e. Нехай $q = 2^a u - 1$ і $t = 2^b v$, де a і $b \geqslant 2$ — цілі, u, v — непарні числа і при цьому всі прості дільники числа t ділять e, але не ділять $(q^m - 1)/e$. Нехай k — найменше з чисел a і b. Тоді кожен з многочленів $f_j(x^t)$ розкладається в добуток 2^{k-1} нормованих незвідних многочленів $g_{ij}(x)$ з $\mathbb{F}_q[x]$ степеня $mt2^{1-k}$. Вказаними $2^{k-1}N$ многочленами $g_{ij}(x)$ вичерпуються всі різні нормовані незвідні многочлени з $\mathbb{F}_q[x]$ степеня $mt2^{1-k}$ і порядку et.*

Покажемо тепер, як з даного незвідного многочлена порядку e можна одержати всі незвідні многочлени, порядки яких ділять e. Оскільки в їх число обов'язково увійде $g(x) = x$, то будемо розглядати лише ті многочлени g, для яких $g(0) \neq 0$.

Нехай f — нормований незвідний многочлен з $\mathbb{F}_q[x]$ степеня m і порядку e, такий, що $f(0) \neq 0$. Нехай $\alpha \in \mathbb{F}_{q^m}$ — деякий корінь многочлена f, і для кожного $t \in \mathbb{N}$ нехай $g_t \in \mathbb{F}_q[x]$ — мінімальний многочлен елемента α^t над $\mathbb{F}_q$.

Нехай $T = \{t_1, t_2, \ldots, t_n\}$ — множина таких натуральних чисел, що для кожного $t \in \mathbb{N}$ існує однозначно визначений індекс i, $1 \leqslant i \leqslant n$, такий, що $t \equiv t_i q^b \pmod e$ для деякого цілого числа $b \geqslant 0$. Таку множину T можна побудувати, наприклад, таким чином. Покладемо $t_1 = 1$, і, коли вже побудовано

$t_1, \ldots, t_{j-1}$, нехай t_j буде найменшим натуральним числом, для якого $t_j \not\equiv t_i q^b \pmod{e}$ при $1 \leqslant i < j$ і всіх цілих $b \geqslant 0$. Ця процедура закінчиться через скінченну кількість кроків.

Теорема 10.9. *Многочленами $g_{t_1}, g_{t_2}, \ldots, g_{t_n}$ вичерпуються всі різні нормовані незвідні многолчени з $\mathbb{F}_q[x]$, порядки яких ділять число e, а постійні члени відмінні від 0.*

Доведення. Кожний многочлен g_{t_i} за означенням є нормованим та незвідним в кільці $\mathbb{F}_q[x]$ та задовольняє умову $g_{t_i}(0) \neq 0$. Крім того, оскільки многочлен g_{t_i} має корінь α^{t_i}, порядок якого в групі $\mathbb{F}_{q^m}^*$ ділить порядок елемента α, то $\operatorname{ord}(g_{t_i})$ ділить e.

Нехай g — довільний нормований незвідний многочлен з $\mathbb{F}_q[x]$ порядку d, який ділить e, такий, що $g(0) \neq 0$. Якщо β — який-небудь корінь многочлена g, то з рівності $\beta^d = 1$ випливає, що $\beta^e = 1$, так що β — корінь степеня e з одиниці над $\mathbb{F}_q$. Оскільки α — первісний корінь степеня e з одиниці над $\mathbb{F}_q$, то за теоремою 6.1 (i) маємо, що $\beta = \alpha^t$ для деякого $t \in \mathbb{N}$. Тоді з визначення множини T випливає, що $t \equiv t_i q^b \pmod{e}$ при деякому цілому i, $1 \leqslant i \leqslant n$, і цілому $b \geqslant 0$. Тому $\beta = \alpha^t = (\alpha^{t_i})^{q^b}$, так що β — корінь многочлена g_{t_i} (теорема 3.3). А оскільки g — мінімальний многочлен елемента β над $\mathbb{F}_q$, то з теореми 10.14 (iii) випливає, що $g = g_{t_i}$.

Лишилося довести, що многочлени g_{t_i}, $1 \leqslant i \leqslant n$, різні. Припустимо, що $g_{t_i} = g_{t_j}$ при $i \neq j$. Тоді α^{t_i} та α^{t_j} — корені многочлена g_{t_i}, так що $\alpha^{t_j} = (\alpha^{t_i})^{q^b}$ для деякого $b \geqslant 0$. Звідси випливає, що $t_j \equiv t_i q^b \pmod{e}$, але оскільки крім того, $t_j \equiv t_j q^o \pmod{e}$, то ми одержимо суперечність з визначенням множини T. □

Мінімальний многочлен g_t елемента $\alpha^t \in \mathbb{F}_{q^m}$ над $\mathbb{F}_q$ зазвичай обчислюють за допомогою характеристичного многочлена f_t цього елемента над $\mathbb{F}_q$. Відомо, що $f_t = g_t^r$, де $r = m/k$, k —

степінь многочлена g_t. Оскільки g_t — незвідний над $\mathbb{F}_q$, то число k є мультиплікативним порядком q за модулем $d = \operatorname{ord}(g_t)$. Отже, число d дорівнює порядку елемента α^t в групі $\mathbb{F}_{q^m}^*$, п цей порядок дорівнює $e/(t,e)$. Отже, можна знайти числа d, k, r.

Теорема 10.10. *Нехай f — нормований незвідний многочлен степеня m з $\mathbb{F}_q[x]$. Нехай $\alpha \in \mathbb{F}_{q^m}$ — деякий корінь цього многочлена, і для $t \in \mathbb{N}$ нехай f_t — характеристичний многочлен елемента $\alpha^t \in \mathbb{F}_{q^m}$ над $\mathbb{F}_q$. Тоді*

$$f_t(x^t) = (-1)^{m(t+1)} \prod_{j=1}^{t} f(\omega_j),$$

де $\omega_1, \omega_2, \ldots, \omega_t$ — корені степеня t з одиниці над $\mathbb{F}_q$ з урахуванням їхніх кратностей.

Доведення. Нехай $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_m$ — всі корені многочлена f. Тоді $\alpha_1^t, \alpha_2^t, \ldots, \alpha_m^t$ — корені многочлена f_t з урахуванням їх кратностей. Тому

$$f_t(x^t) = \prod_{i=1}^{m}(x^t - \alpha_i^t) = \prod_{i=1}^{m}\prod_{j=1}^{t}(x - \alpha_i\omega_j) = \prod_{i=1}^{m}\prod_{j=1}^{t}\omega_j(\omega_j^{-1}x - \alpha_i).$$

Порівнявши коефіцієнти в рівності

$$x^t - 1 = \prod_{j=1}^{t}(x - \omega_j),$$

одержимо, що

$$\prod_{j=1}^{t}\omega_j = (-1)^{t+1},$$

так що

$$f_t(x^t) = (-1)^{m(t+1)} \prod_{j=1}^{t} \prod_{i=1}^{m} (\omega_j^{-1} x - \alpha_i) =$$
$$= (-1)^{m(t+1)} \prod_{j=1}^{t} \prod_{i=1}^{m} f(\omega_j^{-1} x) =$$
$$= (-1)^{m(t+1)} \prod_{j=1}^{t} \prod_{i=1}^{m} f(\omega_j x),$$

бо $\omega_1^{-1}, \omega_2^{-1}, \ldots, \omega_t^{-1}$ пробігають в точності всі корені степеня t з одиниці над полем $\mathbb{F}_q$. □

Приклад 10.11. Розглянемо незвідний $f(x) = x^4+x+1 \in \mathbb{F}_2[x]$. Обчислимо f_3. Коренями 3-го степеня з 1 над $\mathbb{F}_2$ є 1, ω, ω^2, де ω — корінь многочлена $x^2 + x + 1$, який належить полю $\mathbb{F}_4$. Тоді

$$f_3(x^3) = (-1)^{16} f(x) f(\omega x) f(\omega^2 x) =$$
$$= (x^4 + x + 1)(\omega x^4 + \omega x + 1)(\omega^2 x^4 + \omega^2 x + 1) =$$
$$= x^{12} + x^9 + x^6 + x^3 + 1.$$

Отже, $f_3(x) = x^4 + x^3 + ^2 + x + 1$. □

Приклад 10.12. Інший спосіб відшукання характеристичного многочлена f_t елемента α^t базується на теорії матриць. Нехай

$$f(x) = x^m + a_{m-1}x^{m-1} + \ldots + a_1 x + a_0,$$

нехай A — його супутня матриця:

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

Тоді f характеристичним многочленом матриці A. Для кожного $t \in \mathbb{N}$ многочлен f_t є характеристичним многочленом для t-го степеня A^t матриці A. Таким чином, обчислюючи степені матриці A, можна одержати многочлени f_t.

Нехай $f(x) = x^4 + x + 1 \in \mathbb{F}_2[x]$. Обчислимо f_3. Супровідною матрицею многочлена f є матриця

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

Тоді

$$A^3 = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 \end{pmatrix}.$$

Характеристичним многочленом матриці A^3 є $x^4 + x^3 + x^2 + x + 1$.

□

Приклад 10.13. З'ясуємо, які з многочленів f_t є незвідними в кільці $\mathbb{F}_q$. З зауваження перед теоремою 10.10 випливає, що характеристичний многочлен f_t елемента $\alpha^t \in \mathbb{F}_{q^m}$ над $\mathbb{F}_q$ є незвідним в $\mathbb{F}_q[x]$ тоді і лише тоді, коли він збігається з мінімальним многочленом g_t елемента α^t над $\mathbb{F}_q$, тобто коли $\deg(g_t) = m$, а для цього необхідно і достатньо, щоб число m було мультиплікативним порядком q за модулем $d = e/(t, e)$.

Розглянемо, наприклад, випадок $q = 2$, $m = 6$, $e = 21$. З'ясуємо, коли многочлени f_t є звідними. Оскільки мультиплікативний порядок числа q за модулем деякого дільника числа e, повинен бути дільником числа m, то, крім m, можливі порядки — це $k = 1, 2, 3$. Для них $q^k = 1, 3, 7$, тому порівняння $q^k \equiv 1 \pmod{d}$ виконується лише для $d = 1, 3, 7$. Таким чином, многочлен f_t є звідним в кільці $\mathbb{F}_2[x]$ у випадках, коли

$(t, 21) = 3, 7, 21$. Оскільки досить розглянути лише ті значення t, для яких $1 \leqslant t \leqslant 21$, то одержимо, що многочлен f_t є звідним в кільці $\mathbb{F}_2[x]$ для всіх значень t зі вказаного проміжку, за винятком $t = 3, 6, 7, 9, 12, 14, 15, 18, 21$.

Якщо в якості f взяти примітивний многочлен над $\mathbb{F}_q$, тобто вважати $e = q^m - 1$, то степені елемента α будуть пробігати всі ненульові елементи поля $\mathbb{F}_{q^m}$. Тому описаний вище методі можна застосовувати для обчислення мінімальних многочленів над $\mathbb{F}_q$ всіх елементів мультиплікативної групи поля $\mathbb{F}^*_{q^m}$. □

Незвідні многочлени часто виникають як мінімальні многочлени елементів деякого розширення поля. Зберемо найбільш корисні факти про мінімальні многочлени.

Теорема 10.14 (Властивості мінімальних многоленів)**.** *Нехай α — деякий елемент з розширення $\mathbb{F}_{q^m}$ поля $\mathbb{F}_q$, нехай d — степінь елемента α над $\mathbb{F}_q$, а $g \in \mathbb{F}_q[x]$ — мінімальний многочлен елемента α над $\mathbb{F}_q$. Тоді*

а) *Многочлен g є незвідним над $\mathbb{F}_q$, його степінь d ділить число m.*

б) *Многочлен $f \in \mathbb{F}_q[x]$ задовольняє умову $f(\alpha) = 0$ тоді і лише тоді, коли f ділить g.*

в) *Якщо f — нормований незвідний многочлен з $\mathbb{F}_q[x]$, такий, що $f(\alpha) = 0$, то $f = g$.*

г) *$g(x)$ ділить многочлени $x^{q^d} - x$ та $x^{q^m} - x$.*

д) *Коренями многочлена $g(x)$ є елементи $\alpha, \alpha^q, \ldots, \alpha^{q^{d-1}}$, причому $g(x)$ — мінімальний многочлен над $\mathbb{F}_q$ кожного з цих елементів.*

е) *Якщо $\alpha \neq 0$, то порядок многочлена g дорівнює порядку елемента α в мультиплікативній групі $\mathbb{F}^*_{q^m}$ поля $\mathbb{F}_{q^m}$.*

ж) *g є примітивним многочленом над полем $\mathbb{F}_q$ тоді і лише тоді, коли порядок елемента α в групі $\mathbb{F}_{q^m}^*$ дорівнює $q^d - 1$.*

Приклад 10.15. [Прямий метод знаходження мінімальних многочленів] Нехай $\theta \in \mathbb{F}_{16}$ — корінь незвідного многочлена $x^4 + x + 1 \in \mathbb{F}_2[x]$. θ є твірним елементом поля $\mathbb{F}_{2^6}$ як простого розширення поля $\mathbb{F}_2$, так що $\{1, \theta, \theta^2, \theta^3\}$ — базис $\mathbb{F}_{2^4}$ над $\mathbb{F}_2$.

Нехай $\beta = \theta^2 + \theta^3$. Знайдемо мінімальний многочлен для β.

1. Виразимо $\beta^0, \beta^1, \beta^2, \beta^4, \beta^4$ через базисні елементи:

$$\begin{aligned}\beta^0 &= 1\\ \beta^1 &= \theta^3 + \theta^2,\\ \beta^2 &= \theta^3 + \theta^2 + \theta + 1\\ \beta^3 &= \theta^3\\ \beta^4 &= \theta^3 + \theta\end{aligned}$$

Нехай для $1 \leqslant i \leqslant m + 1 = 5 \quad \beta^{i-1} = \sum_{j=1}^{m} b_{ij}\theta^{j-1}$.

2. Запишемо многочлен g у вигляді $g(x) = c_m x^m + \ldots + c_1 x + c_0 = c_4 x^4 + c_3 x^3 + c_2 x^2 + c_1 x + c_0$. Нам потрібно, щоб многочлен g був нормованим многочленом найменшого степеня, який задовольняє умови $g(\beta) = 0$. Ця умова $g(\beta) = c_4\beta^4 + c_3\beta^3 + c_2\beta^2 + c_1\beta + c_0 = 0$ приводить до однорідної СЛР:

$$\sum_{i=1}^{m+1} c_{i-1} b_{ij}, \quad j = 1, 2, \ldots, m$$

з невідомими $c_0, c_1, \ldots, c_m$. Отже, матимемо

$$\begin{aligned} c_0 + c_2 &= 0\\ c_2 + c_4 &= 0\\ c_1 + c_2 &= 0\\ c_1 + c_2 + c_3 + c_4 &= 0\end{aligned} \tag{10.2}$$

3. Матрицею цієї ОСЛР є матриця

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

   Її ранг дорівнює $r = 4$. Отже, розмірність простору розв'язків дорівнює $s = m + 1 - r = 1$.

4. Якщо $s = 1$, то покладемо $c_m = 1$. Якщо $s > 1$, то покладемо $c_m = c_{m-1} = \ldots = c_{m-s+2} = 0$, а $c_{m-s+1} = 1$. Виразимо серез них решту розв'язків системи.

   В нашому випадку $s = 1$, тому $c_4 = 1$. Решту коефіцієнтів знайдемо з системи (10.2): $c_0 = c_1 = c_2 = c_3 = 1$. Отже, мінімальним многочленом елемента β над $\mathbb{F}_2$ є $g(x) = x^4 + x^3 + x^2 + x + 1$.

□

Приклад 10.16. Ще один метод знаходження мінімальних многочленів полягає в наступному. Якщо потрібно знайти мінімальний многочлен g елемента $\beta \in \mathbb{F}_{q^m}$ над $\mathbb{F}_q$, то обчислюємо степені $\beta, \beta^q, \beta^{q^2}, \ldots$ доки не одержимо найменше $d \in \mathbb{N}$, для якого $\beta^{q^d} = \beta$. Це d є степенем многочлена g, а сам g задається формулою

$$g(x) = (x - \beta)(x - \beta^q) \ldots (x - \beta^{q^{d-1}}).$$

Елементи $\beta, \beta^q, \beta^{q^2}, \ldots, \beta^{q^{d-1}}$ є різними спряженими з β елементами відносно поля $\mathbb{F}_q$, а g — мінімальний многочлен над $\mathbb{F}_q$ будь-якого з цих елементів.

Знайдемо мінімальні многочлени над $\mathbb{F}_2$ для всіх елементів поля $\mathbb{F}_8$. Нехай $\theta \in \mathbb{F}_8$ — корінь примітивного многочлена $x^3 + x + 1$ над $\mathbb{F}_2$.

Побудуємо для поля $\mathbb{F}_8$ таблицю індексів

i	0	1	2	3	4	5	6
θ^i	1	θ	θ^2	$1+\theta$	$\theta+\theta^2$	$1+\theta+\theta^2$	$1+\theta^2$

Тепер знайдемо мінімальні многочлени для всіх елементів β поля $\mathbb{F}_q$:
$\beta = 0$: $g_1(x) = x$.
$\beta = 1$: $g_2(x) = x + 1$.
$\beta = \theta$: різними спряженими з β елементами відносно $\mathbb{F}_2$ є $\theta, \theta^2, \theta^4$, мінімальний многочлен кожного з них дорівнює

$$g_3(x) = (x-\theta)(x-\theta^2)(x-\theta^4) = x^3 + x + 1$$

$\beta = \theta^3$: різними спряженими з β елементами відносно $\mathbb{F}_2$ є $\theta^3, \theta^6, \theta^{12} = \theta^5$, мінімальний многочлен кожного з них дорівнює

$$g_4(x) = (x-\theta^3)(x-\theta^6)(x-\theta^5) = x^3 + x^2 + 1.$$

Важливою задачею є знаходження примітивних многочленів.

Один з підходів базується на тому факті, що добуток всіх примітивних многочленів степеня m над $\mathbb{F}_q$ дорівнює круговому многочлену Q_e, де $e = q^m - 1$. Тому всі примітивні многочлени над $\mathbb{F}_q$ степеня m можна знайти, розкладаючи круговий многочлен Q_e.

Інший підхід полягає в побудові деякого примітивного елемента поля $\mathbb{F}_{q^m}$, для якого потім обчислюється мінімальний многочлен, який і є примітивним. Для знаходження примітивного елемента поля $\mathbb{F}_{q^m}$ беруть порядок цього елемента $q^m - 1$, розкладають на множники $q^m - 1 = h_1 \cdot \ldots \cdot h_k$. Для кожного h_i, $1 \leqslant k \leqslant k$, можна знайти елемент $\alpha_i \in \mathbb{F}^*_{q^m}$ порядку h_i, тоді елемент $\alpha = \alpha_i \ldots \alpha_k$ має порядок $q^m - 1$.

Приклад 10.17 (Знаходження примітивних многочленів)**.** Знайдемо примітивний многочлен степеня 6 над $\mathbb{F}_2$. Оскільки

$2^6 - 1 = 9 \cdot 7$, то побудуємо спочатку два елементи групи $\mathbb{F}_{64}^*$ порядків 9 і 7. Знайдемо 9-круговий многочлен

$$Q_9(x) = \prod_{d|9} (x^{\frac{9}{d}} - 1)^{\mu(d)} = (x-1)^{\mu(9)}(x^3-1)^{\mu(3)}(x^9-1)^{\mu(1)} =$$
$$= \frac{x^9 - 1}{x^3 - 1} = x^6 + x^3 + 1.$$

Оскільки $\operatorname{ord}_9 2 = 6$, то круговий многочлен Q_9 є незвідним над $\mathbb{F}_2$.

Нехай θ — корінь цього многочлена. Його порядок в групі $\mathbb{F}_{64}^*$ дорівнює 9, причому $\mathbb{F}_{64} = \mathbb{F}_2(\theta)$. Елемент $\alpha \in \mathbb{F}_{64}^*$ порядку 7 задовольняє рівність $\alpha^8 = \alpha$. Можемо записати

$$\alpha = \sum_{i=0}^{5} a_i \theta^i = \alpha^8 = \left(\sum_{i=0}^{5} a_i \theta^i \right)^8 = \sum_{i=0}^{5} a_i \theta^{8i} =$$
$$= a_0 + a_1\theta^8 + a_2\theta^7 + a_3\theta^6 + a_4\theta^5 + a_5\theta^4 =$$
$$= a_0 + a_1(\theta^5 + \theta^2) + a_2(\theta^4 + \theta) + a_3(\theta^3 + 1) + a_4\theta^5 + a_5\theta^4 =$$
$$= (a_0 + a_3) + a_2\theta + a_1\theta^2 + a_3\theta^3 + (a_2 + a_5)\theta^4 + (a_1 + a_4)\theta^5.$$

Прирівнявши коефіцієнти, отримаємо $a_1 = a_2$, $a_3 = 0$, $a_4 = a_2 + a_5$. Обираючи $a_0 = a_3 = a_4 = 0$, $a_1 = a_2 = a_5 = 1$, отримаємо, що $\alpha = \theta + \theta^2 + \theta^5$ є елементом порядку 7. Таким чином, елемент $\zeta = \alpha\theta = 1 + \theta^2$ є примітивним елементом поля $\mathbb{F}_{64}$. Мінімальний многочлен елемента ζ над $\mathbb{F}_2$ тоді дорівнює

$$g(x) = (x - \zeta)(x - \zeta^2)(x - \zeta^4)(x - \zeta^8)(x - \zeta^{16})(x - \zeta^{32}) =$$
$$= x^6 + x^4 + x^3 + x + 1.$$

Цю саму відповідь можна одержати, застосувавши спосіб, описаний у прикладі 10.15. □

Якщо примітивний многочлен g степеня m над $\mathbb{F}_q$ відомий, то решту примітивних многочленів над $\mathbb{F}_q$ можна одержати,

розглядаючи деякий корінь θ многочлена g в полі $\mathbb{F}_{q^m}$ і знаходячи мінімальні многочлени над $\mathbb{F}_q$ для всіх елементів вигляду θ^t, де θ пробігає всі натуральні взаємно прості з $q^m - 1$ числа, які не перевищують $q^m - 1$.

Приклад 10.18. Знайти над полем $\mathbb{F}_2$ всі незвідні многочлени порядку $e = 21$ степеня $m = 6$. Нехай $\theta \in \mathbb{F}_{64}$ — корінь примітивного многочлена $x^6+x^4+x^3+x+1$, тоді кожний елемент поля $\mathbb{F}_{64}$ можна подати у вигляді елемента θ. Кількість таких многочленів дорівнює $\varphi(e)/m = \varphi(21)/6 = 2$. Оскільки порядок многочлена дорівнює порядку його кореня, то потрібно знайти мінімальні многочлени елементів порядку 21. Елементами порядку 21 є θ^k для $k = 3, 6, 12, 15, 24, 30, 33, 39, 48, 51, 57, 60$.

Мінімальні многочлени для спряжених елементів θ^3, θ^6, θ^{12}, θ^{24}, θ^{48}, $\theta^{96} = \theta^{33}$ однакові, і кожен з них дорівнює:

$$g(x) = (x - \theta^3)(x - \theta^6)(x - \theta^{12})(x - \theta^{24})(x - \theta^{48})(x - \theta^{33}) = \\ = x^6 + x^5 + x^4 + x^2 + 1.$$

Мінімальні многочлени для спряжених елементів θ^{15}, θ^{30}, θ^{60}, θ^{57}, θ^{51}, θ^{39} однакові, і кожен з них дорівнює:

$$g(x) = (x - \theta^{15})(x - \theta^{30})(x - \theta^{60})(x - \theta^{57})(x - \theta^{51})(x - \theta^{39}) = \\ = x^6 + x^4 + x^2 + x + 1. \quad \square$$

Розділ 11

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. Якщо $\deg g = k$, то $k \leqslant n/2$ і 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 11.1 (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 11.1. 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 11.2 (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:

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

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

Крок 3. Обчислити a^m за формулою

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

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

Теорема 11.2. *Алгоритм 11.1 вимагає* $O\left(n^3 \operatorname{length}(q)\right)$ *дій у полі* $\mathbb{F}_q$.

Доведення. Розглянемо одну ітерацію з основного циклу алгоритму 11.1. Якщо використовувати алгоритм 11.2, 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 11.3. *Нехай* $N_q(n)$ *— це кількість унітарних незвідних многочленів степеня* n *над полем* $\mathbb{F}_q$. *Тоді для всіх* $n \geqslant 1$

$$\frac{q^n}{2n} \leqslant N_q(n) \leqslant \frac{q^n}{n}, \tag{11.1}$$

та

$$N_q(n) = \frac{q^n}{n} + O\left(\frac{q^{n/2}}{n}\right). \tag{11.2}$$

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

$$q^n = \sum_{d|n} dN_q(d), \tag{11.3}$$

сума береться по всім додатним дільникам числа n. Усі доданки у правій частини (11.3) додатні, $nN_q(n)$ — один з цих доданків, тому $q^n \geqslant nN_q(n)$. Звідси випливає права частина нерівності (11.1). 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 11.3. *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 11.1 перевірити, чи він незвідний

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

Теорема 11.4. *Алгоритм 11.3 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 11.3 середня кількість ітерацій алгоритму 11.3 дорівнює $O(n)$. За теоремою 11.2 алгоритм 11.3 потребує $O(n^3 \operatorname{length}(q))$ дій у полі $\mathbb{F}_q$. Звідси маємо твердження теореми. Друга частина твердження очевидна. □

Частина II

Застосування скінченних полів

Розділ 12

Дискретний логарифм

Задача дискретного логарифмування. Нехай дано просте число p, твірний елемент α групи $\mathbb{Z}_p^*$ та елемент $\beta \in \mathbb{Z}_p^*$. Знайти таке ціле число x, $0 \leqslant x \leqslant p-2$, що $\alpha^x \equiv \beta \pmod{p}$.

Узагальнена задача дискретного логарифмування. Нехай дано скінченну циклічну групу G порядку n, твірний елемент α групи G, елемент $\beta \in G$. Знайти таке ціле число x, $0 \leqslant x \leqslant n-1$, що $\alpha^x \equiv \beta$.

Число x називається *дискретним логарифмом* β з основою α.

Приклад 12.1. Візьмемо групу $G = \mathbb{Z}_{11}^* = \langle 2 \rangle$. Тоді дискретний логарифм числа 7 з основою 2 дорівнює 7.

Зауваження 12.1. Нехай α та γ — два різних твірних циклічної групи G порядку n, нехай $\beta \in G$. Нехай $x = \log_\alpha \beta$, $y = \log_\gamma \beta$, $z = \log_\alpha \gamma$. Тоді $\alpha^x = \beta = \alpha^y = (\alpha^z)^y$, звідки $x = zy \pmod{n}$ та

$$\log_\gamma \beta = (\log_\alpha \beta)(\log_\alpha \gamma)^{-1} \pmod{n}.$$

Це означає, що будь-який алгоритм, який обчислює логарифми з основою α, можна використати для обчислення логарифму з будь-якою іншою основою γ. Отже, *складність задачі дискретного логарифмування не залежить від вибору твірного групи G.*

12.1 Алгоритми розв'язування задачі дискретного логарифмування

Повний перебір. Найбільш очевидний алгоритм розв'язування узагальненої задачі дискретного логарифмування — це послідовно обчислювати

$$\alpha^0, \alpha^1, \alpha^2, \ldots,$$

доки не одержимо β. Цей метод вимагає $O(n)$ множень, де n — це порядок α, а тому неефективний, коли n велике (наприклад, у криптографічних інтересах).

Метод Шенкса (Baby-step giant-step). Це фундаментальний алгоритм розв'язування задачі дискретного логарфимування. Він застосовний до будь–якої скінченної циклічної групи.

Нехай $m = [\sqrt{n}] + 1$, де n — це порядок елемента α. Алгоритм Шенкса базується на наступному спостереженні. Якщо $\beta = \alpha^x$, тоді можна записати $x = im + j$, де $0 \leqslant i, j < m$. Отже, $\alpha^x = \alpha^{im}\alpha^j$, з чого випливає $\beta(\alpha^{-m})^i = \alpha^j$. Це передбачає наступний алгоритм обчислення x.

Алгоритм Шенкса.

Дано: твірний α циклічної групи G порядку n та елемент $\beta \in G$.

Знайти: дискретний логарифм $x = \log_\alpha \beta$.

1. Покласти $m = [\sqrt{n}] + 1$.
2. Побудувати таблицю зі входженнями (j, α^j) для $0 \leqslant j < m$. Впорядкувати цю таблицю за другою компонентою.
3. Обчислити α^{-m} та покласти $\gamma = \beta$.
4. Для i від 0 до $m - 1$ зробити наступне:
    a) Перевірити, чи не є γ другою компонентою деякого елемента з таблиці.

б) Якщо $\gamma = \alpha^j$, то покласти $x = im + j$.

в) Покласти $\gamma = \gamma \cdot \alpha^{-m}$.

Оцінимо кількість дій, потрібних для роботи алгоритму Шенксак. Для побудови таблиці потрібно $O(\sqrt{n})$ множень та $O(\sqrt{n} \ln n)$ порівнянь для сортування. Маючи вже побудовану таблицю, для кроку 4 нам потрібно $O(\sqrt{n})$ множень та $O(\sqrt{n})$ переглядів таблиці. За припущення, що групове множення вимагає більше часу, ніж $\ln n$ порівнянь, то час роботи алгоритму можна оцінити наступним чином.

Факт 12.1. *Алгоритм Шенкса вимагає $O(\sqrt{n})$ групових множень.*

Приклад 12.2. Нехай $p = 113$, $\alpha = 3$ — твірний $\mathbb{Z}_{113}^*$. Обчислимо $\log_3 32$.

1. Покладемо $m = [\sqrt{112}] + 1 = 11$.

2. Побудуємо таблицю з елементів (j, α^j) для $j = 0, 1, 2, \ldots$.

j	0	1	2	3	4	5	6	7	8	9	10
$3^j \pmod{113}$	1	3	9	27	81	17	51	40	7	21	63

та відсортуємо за другою компонентою:

j	0	1	8	2	5	9	3	7	6	10	4
$3^j \pmod{113}$	1	3	7	9	17	21	27	40	51	63	81

3. Обчислюємо в групі $\mathbb{Z}_{113}^*$ спочатку $\alpha^{-1} = 3^{-1} = 38$, а потім $\alpha^{-m} = 3^{-113} = 58$.

4. Далі обчислюємо $\gamma = \beta\alpha^{-mi} \pmod{113}$ для $i = 0, 1, 2, \ldots$ до тих пір, доки не одержимо значення з другого рядка таблиці:

i	0	1	2	3	4	5
$\gamma = 32 \cdot 58^i \pmod{113}$	32	48	72	108	49	17

Оскільки $\beta\alpha^{-5m} = \alpha^5$, то $\beta = \alpha^{60}$. Отже, $\log_3 32 = 60$.

12.2 Алгоритм Діффі–Хелмана обчислення спільного таємного значення

Цей алгоритм дає змогу двом віддаленим абонентам мережі встановити спільне таємне значення шляхом обміну нетаємними повідомленнями. Це спільне таємне значення може потім використовуватися для обчислення спільного сесійного таємного ключа в алгоритмах симетричного шифрування.

Процес встановлення спільного таємного значення.

Перед початком роботи абоненти A та B узгоджують скінченну циклічну групу G порядку n та її твірний елемент g. Після цього виконують наступні дії.

Абонент A

- обирає випадкове ціле число x, $0 \leqslant x < n$;
- обчислює в групі G елемент $X = g^x$;
- надсилає елемент $X = g^x$ групи G абоненту B.

Абонент B

- обирає випадкове ціле число y, $0 \leqslant y < n$;
- обчислює в групі G елемент $Y = g^y$;
- надсилає елемент $Y = g^y$ групи G абоненту A.

Після цього абонент A обчислює Y^x, а абонент B обчислює X^y. Таким чином абоненти A і B обчислили спільне таємне значення, бо

$$Y^x = g^{yx} = g^{xy} = X^y.$$

Задача Діффі–Хелмана. *Нехай g — твірний скінченної циклічної групи. Знаючи g, g^x та g^y, знайти g^{xy}.*

Припущення Діффі–Хелмана. *Складність обчислення g^{xy} за g, g^x та g^y надзвичайно висока.*

Складність розв'язання задачі Діффі–Хелмана забезпечує надійність алгоритму Діффі-Хелмана встановлення спільного таємного значення.

Припущення Діффі–Хелмана апріорі не слабше за припущення про надзвичайну складність задачі дискретного логарифмування в скінченній групі. Якби можна було легко обчислювати дискретні логарифми, то припущення Діффі–Хелмана було б невірним. Є думка, що справедливим є і обернене твердження, проте поки це питання лишається відкритим. Іншими словами, поки ще ніхто не запропонував алгоритм одержання g^{xy} з g^x та g^y без використання x та y. Проте цілком можливо, що такий спосіб існує.

Розділ 13

Елементи теорії кодування

13.1 Поняття коду

Нехай X — це скінченна множина символів ($|X| = q > 1$), яку називатимемо *алфавітом*, нехай n — натуральне число. *Словом* довжиною n над алфавітом X називається послідовність $a_1a_2 \dots a_n$ з n символів, де $a_1, a_2, \dots, a_n \in X$. *Код* C довжиною n — це підмножина множини X^n всіх слів довжиною n, за умови, що $|C| > 1$. Елементи множини C називаються *кодовими словами*.

Означення 13.1. *Нехай $v = v_1 \dots v_n$, $w = w_1 \dots w_n$ — слова довжиною n. Відстанню Хеммінга $d(v, w)$ від слова v до слова w називається кількість координат, в яких словах v та w відрізняються:*

$$d(v, w) = |\{i \mid 1 \leqslant i \leqslant n, v_i \neq w_i\}|.$$

При передачі повідомлення зашумленим каналом зв'язку деякі символи можуть бути змінені. Відстань Хеммінга між словом, що передавалося, та словом, що було одержане, вказує на кількість помилок.

Твердження 13.1. *1. Для довільних слів v та w $d(v, w) \geqslant 0$ та $d(v, w) = 0$ тоді і лише тоді, коли $v = w$.*

2. *Для довільних слів v та w* $\quad d(v,w) = d(w,v)$.

3. (*Нерівність трикутника.*) *Для довільних слів u, v, w*

$$d(u,w) \leqslant d(u,v) + d(v,w).$$

З твердження 13.1 випливає, що відстань Хеммінга задає метрику на множині слів над алфавітом X.

Означення 13.2. *Нехай $e \in \mathbb{N}$. Кажуть, що код C довжиною n виправляє e помилок, якщо для довільного слова w довжиною n існує щонайбільше одне кодове слово c, таке, що $d(w,c) \leqslant e$.*

Назва "коди, що виправляють помилки" пояснюється наступним чином. Припустимо, що код C — це код, що виправляє e помилок, і ми знаємо, що при передачі одного слова може трапитися не більше, ніж e помилок. Тоді ці помилки можуть бути виправлені. Якщо c — це слово, що передавалось, а w — це слово, яке було одержане, то за припущенням $d(c,w) \leqslant e$. Оскільки код C виправляє e помилок, то будь–яке інше кодове слово c' задовольняє нерівність $(c',w) > e$. Отже, c — це кодове слово, як найближче до передаваного слова, а тому декодування є правильним.

Означення 13.3. *Найменшою відстанню коду C називається найменша відстань між двома різними словами цього коду.*

Найменшу відстань коду C позначатимемо $d_{\min}C$.

Теорема 13.1. *Код C виправляє e помилок тоді і лише тоді, коли*

$$d_{\min}C \geqslant 2e + 1.$$

Доведення. Необхідність. Нехай код C виправляє e помилок. Припустимо, що $d_{\min}C = d \leqslant 2e$. Покладемо $f = [d/2]$, тоді $f \leqslant e$ та $e - f \leqslant e$. З умови випливає, що знайдуться два кодові слова c_1 та c_2, відстань між якими дорівнює $d(c_1,c_2) = d$. Це

означає, що перейти від слова c_1 до слова c_2 можна шляхом зміни d координат. Будемо змінювати координати по одній. Нехай w — це слово, яке одержане з c_1 після f замін. Тоді $d(c_1, w) = f \leqslant e$, $d(c_2, w) = d - f \leqslant e$. Отже, існують два кодові слова, які знаходяться на відстані не більшій за e від слова w. Таким чином, код C не є кодом, що виправляє e помилок.

Достатність. Припустимо, що код C не є кодом, що виправляє e помилок. Тоді існують слово w та два кодових слова c_1 та c_2, які знаходяться на відстані не більшій за e від слова w, тобто $d(c_1, w) \leqslant e$ та $d(c_2, w) \leqslant e$. З твердження 13.1 випливає, що $d(c_1, c_2) \leqslant e + e = 2e$. Отже, маємо суперечність з умовою $d_{\min} C \geqslant 2e + 1$. □

Теорема 13.2. *Нехай C — код довжиною n над алфавітом з q символів, d — мінімальна відстань коду. Тоді*

1. *(границя Хеммінга) якщо $d \geqslant 2e + 1$, то*

$$|C| \leqslant q^n / \sum_{i=0}^{e} \binom{n}{i} (q-1)^i;$$

2. *(границя Сінглтона)*

$$|C| \leqslant q^{n-d+1}.$$

Доведення. (а) Нехай c — кодове слово. Лишаємо читачеві в якості вправи перевірити, шо кількість слів w, які задовольняють нерівність $d(c, w) \leqslant e$, дорівнює

$$\sum_{i=0}^{e} \binom{n}{i} (q-1)^i.$$

Можна дивитися на ці слова як на “сфери” радіуса e, центром яких є кодове слово c. Якщо ми зробимо це для всіх кодових

слів, то знайдені слова не будуть накладатися, бо, за припущенням, код C виправляє e помилок, то немає жодного слова, яке б знаходилось на відстані, що не перевищує e, від двох або більше слів. Геометрично це означає, що сфери упаковані у просторі без накладань. Отже, загальна кількість шуканих слів дорівнює

$$|C| \cdot \sum_{i=0}^{e} \binom{n}{i} (q-1)^i,$$

але це число не може перевищувати загальної кількості q^n слів довжиною n над алфавітом q.

(b) В усіх кодових словах візьмемо лише перші $n-d+1$ координат. Покажемо, що всі ці початки різні. Дійсно, припустимо, що перші $n-d+1$ координат деяких різних слів c_1 та c_2 однакові, але тоді вони можуть відрізнятися не більше ніж в останніх $n-(n-d+1) = d-1$ координатах. Отже, $d(c_1, c_2) \leqslant d-1$, що суперечить припущенню. Таким чином, кількість кодових слів не може перевищувати загальну кількість початків, яка дорівнює q^{n-d+1}. □

Коди, які досягають границю Хеммінга, називаються *досконалими*. Коди, які досягають границю Сінглтона, називаються *роздільними кодами з максимальною відстанню*.

Приклад 13.3. Кодом з повтореннями називається код, у якому всі кодові слова мають вигляд $aa\ldots a$, $a \in X$, $|X| = q$. Такий код складається з q слів, і його мінімальна відстань дорівнює довжині n. Якщо $d = n$, то за пунктом (b) теореми 13.2 $|C| \leqslant q^{n-n+1} = q$, тобто код з повтореннями досягає границі Сінглтона. Якщо $q = 2$, а $n = 2e+1$, то цей код досягаю також і границі Хеммінга.

13.2 Лінійні коди

Формалізуємо процеси кодування та декодування. Нехай S — це множина повідомлень, X — алфавіт, що складається з q символів, C — код довжиною n над алфавітом X. Тоді відображення кодування — це ін'єктивне відображення

$$\epsilon : S \to C.$$

Відображення декодування — це відображення

$$\delta : X^n \to C.$$

Хоча жодних формальних вимог не висувається, як правило, припускають, що кодове слово декодується в найближче слово, тобто $\delta(w)$ — це слово, яке якомога ближче до слова w.

Візьмемо в якості алфавіту X скінченне поле $\mathbb{F}_q$ і надалі всі кодові слова розглядатимемо над таким алфавітом. Доволі часто коди розглядають над полем $\mathbb{F}_2$, у таких випадках говорять про бінарний алфавіт, а коди над алфавітом $\mathbb{F}_2$ називають *бінарними* кодами.

Означення 13.4. *Лінійним кодом довжиною n та розмірністю k, або скорочено лінійним (n, k) – кодом, називається k–вимірний підпростір векторного простору $\mathbb{F}_q^n$.*

Означення 13.5. *Вагою* $\mathrm{wt}(w)$ *слова w називається кількість ненульових координат слова w. Мінімальною вагою кода називається найменша вага серед усіх кодових слів.*

Твердження 13.2. *Мінімальна вага та мінімальна відстань лінійного коду однакові.*

Доведення. Пропонуємо читачеві довести це твердження самостійно. □

З цього твердження вже випливають певні переваги лінійних кодів. Наприклад, замість того, щоб порівнювати усі пари кодових слів, щоб знайти мінімальну відстань, досить переглянути усі кодові слова та знайти мінімальну вагу. Якщо передавалося слово c, а одержане було слово w, то $c = w + x$, де вага слова x дорівнює кількості помилок, що трапилися при передачі повідомлення.

Природним чином виникає запитання, як описати лінійний код. Оскільки лінійний код C — це підпростір простору $\mathbb{F}_q^n$, то в ньому можна обрати базис, що складатиметься з k слів довжиною n. Утворимо матрицю G, рядками якої будуть слова, що відповідають цим базисним векторам. Ця матриця називається *твірною матрицею* коду C.

Кожне кодове слово можна єдиним чином записати у вигляді

$$c = x_1 g_1 + \cdots + x_k g_k, \text{ де } g_1, \ldots, g_k \text{ — рядки матриці } G.$$

Якщо позначити $x = x_1 \ldots x_k \in \mathbb{F}_q^k$, то більш коротко можна записати $c = xG$. Таким чином, якщо множина S повідомлень, які мають бути передані, це множина $\mathbb{F}_q^k$ всіх слів довжиною k, тоді відображення ϵ кодування — це просто лінійне відображення

$$x \mapsto x\,G : \quad \mathbb{F}_q^k \to \mathbb{F}_q^n.$$

Це відображення є ін'єктивним, а його образом є код C.

З курсу лінійної алгебри відомо, що коли до рядків матриці G застосувати елементарні перетворення, то векторний простір, що породжується рядками матриці, не зміниться. Таким чином, матриця, одержана в результаті елементарних перетворень, буде твірною матрицею лінійного коду C. Зрозуміло, що за допомогою елементарних перетворень матрицю можна

звести до вигляду

$$(I \quad A) = \begin{pmatrix} 1 & 0 & \dots & 0 & a_{11} & \dots & a_{1,n-k} \\ 0 & 1 & \dots & 0 & a_{21} & \dots & a_{2,n-k} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 & a_{k1} & \dots & a_{k,n-k} \end{pmatrix},$$

де I позначає одиничну, а A деяку матрицю. Тому за потреби ми можемо вважати, що твірна матриця коду записана у вигляді $(I\ A)$. Цей вигляд називатимемо *стандартною* матрицею коду. Легко переконатися, що коли матриця G записана у стандартному вигляді, то відображення кодування задається правилом

$$x \mapsto x\,G = (x \quad xA).$$

У цьому випадку перші k символів кодового слова — це в точності повідомлення, яке передавалося. Ці перші k символів називаються *інформаційними символами*, а решта $n - k$ символів називаються *перевірочними символами*. Неважко зрозуміти, що коли код заданий стандартною матрицею, то процеси кодування та декодування стають надзвичайно простими.

Приклад 13.4. Розглянемо код над полем $\mathbb{F}_2$, який заданий твірною матрицею

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

Як бачимо, матриця G — це записана у стандартній формі матриця бінарного коду розмірності 4 довжиною 7. Якщо виписати всі 16 кодових слів, то побачимо, що мінімальна вага коду дорівнює 3, тобто цей код може виправляти одну помилку. При

кодуванні слова $x_1x_2x_3x_4$ одержимо кодове слово $x_1x_2\ldots x_7$, де

$$x_5 = x_2 + x_3 + x_4,$$
$$x_6 = x_1 + x_3 + x_4,$$
$$x_7 = x_1 + x_2 + x_4.$$

Зауважимо, що цей код досягає границі Хеммінга. Дійсно

$$|C| = 16 = \frac{2^7}{(1 + 7(2-1))}.$$

Це означає, що кулі радіуса 1 покривають весь простір $\mathbb{F}_2^7$, отже, кожне слово знаходиться на відстані 0 або 1 рівно від одного кодового слова. Тому декодування ми можемо здійснити наступним чином: взяти одержане слово, передивитися всі 16 кодових слів, обрати серед них те, яке збігається з даним словом або відрізняється щонайбільше на один символ та взяти перші чотири символи цього кодового слова.

Зрозуміло, що описаний метод декодування важко назвати ефективним. Розглянемо далі більш ефективний спосіб, так зване *декодування за допомогою синдрому*.

Для цього дамо дещо інакше означення лінійного коду. Пригадаємо з курсу лінійної алгебри, що з кожним лінійним відображенням можна пов'язати образ та ядро. Попереднє означення прив'язувалося до образу лінійного відображення.

З боку теорії кодування є серйозні причини звернутися до ядра відображення кодування. Повідомлення приходить у вигляді

кодове слово + помилка.

Наша мета — прибрати помилку та відновити кодове слово. Нам невідомо, який символ був змінений у процесі передачі повідомлення, але ми знаємо, з якого простору обирається кодове слово. Тому розглянемо такий спосіб декодування. Спершу приберемо кодове слово, щоб віднайти помилку, а потім

одержимо кодове слово, віднявши помилку від одержаного слова. Тому природно, що ми хочемо мати таке лінійне відображення f, яке відображає кожне кодове слово в нульове слово, але є ін'єктивним на множині всіх можливих помилок, тобто

$$f(\text{кодове слово+помилка}) = f(\text{кодове слово}) + f(\text{помилка}) = f(\text{помилка}).$$

Пов'яжемо з кодом ще одну матрицю.

Означення 13.6. *Нехай C — лінійний код довжиною n та розмірністю k над алфавітом X.* Перевірочною матрицею *коду називається матриця H розміру $(n-k) \times n$ з властивістю, що для слова $w \in X^n$ виконується*

$$wH^T = 0 \Leftrightarrow w \in C.$$

Слово wH^T називається *синдромом* слова w.

Твердження 13.3. *Нехай H — перевірочна матриця лінійного коду, який виправляє e помилок. Нехай w_1, w_2 — довільні слова, вага яких не перевищує e. Тоді синдроми слів w_1 та w_2 однакові тоді і лише тоді, коли $w_1 = w_2$.*

Доведення. Якщо $w_1H = w_2H$, то $(w_1 - w_2)H = 0$, а тому $w_1 - w_2 \in C$. Але вага слова $w_1 - w_2$ щонайбільше $2e$, в той час як мінімальна вага коду C щонайменше $2e + 1$. Отже, $w_1 - w_2 = 0$. □

Приклад 13.5. Розглянемо матрицю

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

Ця матриця є перевірочною матрицею для коду з прикладу 13.4. У цьому легко переконатися, обчисливши добуток GH^T. Зверніть увагу, що i–й стовпчик — це двійкове зображення i.

Оскільки цей код виправляє 1 помилку, то множина всіх помилок складається з нульового слова 0 та слів e_i, в яких на i–му місці стоїть 1, а решта 0, для $i = 1, \ldots, 7$. Синдромом нульового є 0, а синдромом помилки e_i є i–й стовпчик матриці H.

Процес декодування тепер виглядає наступним чином. Маючи слово w, потрібно обчислити його синдром wH. Якщо він дорівнює 0, то помилок не відбулося. Якщо синдром — це двійкове зображення i, то це означає, що помилка відбулася в i–й позиції.

Припустимо, що ми хочемо передати слово $w = 1001$. Відповідне йому кодове слово — це $c = 1001100$. Припустимо, що у другій позиції відбулася помилка та у процесі передачі було одержане слово $c' = 1101100$. Його синдром дорівнює $c'H = (001)^T$, а це другий стовпчик матриці H. Тому ми виправляємо кодове слово c' на 1001100 і одержуємо вихідне повідомлення 1001.

Якщо ж трапилося дві помилки, то правильне декодування стає неможливим. Припустимо, що при передачі відбулося дві помилки, наприклад, у позиціях 2 та 3, і було одержане кодове слово $c'' = 1111100$. Синдром цього слова дорівнює $(001)^T$, тобто помилка відбулася у першій позиції. Після виправлення одержимо кодове слово 0111100, візьмемо перші чотири символи 0111, що дасть, на жаль, неправильне повідомлення.

Декодування за допомогою синдрому можна використовувати для довільного лінійного коду, хоча в деяких випадках це не найбільш ефективний спосіб. Мінімальну вагу коду можна знайти за його перевірочною матрицею.

Твердження 13.4. *Нехай C — лінійний код з перевірочною матрицею H. Тоді мінімальна вага коду C не менша за δ тоді і лише тоді, коли довільні $\delta - 1$ стовпців матриці H лінійно незалежні.*

Доведення. Нехай $h_1, \ldots, h_n$ — стовпці перевірочної матриці

H. Тоді $c_1 \dots c_n$ є кодовим словом тоді і лише тоді, коли

$$c_1 h_1 + \cdots + c_n h_n = 0.$$

З цього випливає, що кодові слова ваги f відповідають відношенню лінійної залежності на множині з f стовпців. Мінімальна вага дорівнює мінімальній кількості лінійно залежних стовпців. □

Використання поняття перевірочної матриці дає змогу легко ввести важливий клас кодів, а саме кодів Хеммінга. Нехай k — деяке фіксоване натуральне число, $F = \mathbb{F}_q$ — скінченна поле, F^k — k–вимірний векторний простір всіх стовпців вимірністю k. Позначимо $X = F^k \setminus \{0\}$. Тоді $|X| = q^k - 1$.

На множині X введемо відношення еквівалентності за правилом: два елементи множини X еквівалентні тоді і лише тоді, коли один з них пропорційний іншому. Зрозуміло, що кожний клас еквівалентності складається з $q - 1$ елементів, а кількість класів еквівалентності дорівнює

$$n = \frac{q^k - 1}{q - 1}.$$

Нехай Y — множина представників класів еквівалентності, тобто вона складається з ненульових векторів, взятих по одному з кожного класу суміжності. Нехай H — матриця розміру $k \times n$, стовпцями якої є елементи множини Y. Лінійний код (n, k)-код, перевірочною матрицею якого є матриця H, називається *q-арним кодом Хеммінга*. Код з прикладу 13.4 є бінарним $(7, 4)$ – кодом Хеммінга, це випливає з прикладу 13.5.

Твердження 13.5. *Коди Хеммінга є досконалими кодами, які виправляють одну помилку, тобто вони досягають границі Хеммінга.*

Доведення. За побудовою всі стовпці перевірочної матриці коду Хеммінга є ненульовими і жодні два непропорційні. Таким чином, довільні два стовпці цієї матриці лінійно незалежні. Отже, за твердженням 13.4 мінімальна вага цього коду щонайменше 3, а тому він є кодом, що виправляє одну помилку.

Оскільки

$$|C| = q^{n-k} = \frac{q^n}{1 + n(q-1)},$$

то цей код досягає границі Хеммінга. □

Природним чином виникає питання, як за твірною матрицею коду знайти його перевірочну матрицю.

Твердження 13.6. *Нехай G та H — це матриці розмірів $k \times n$ та $(n-k) \times n$ відповідно над скінченним полем F, рядки яких є лінійно незалежними. Тоді G та H є відповідно твірною та перевірочною матрицею одного й того самого коду тоді і лише тоді, коли $GH^\top = 0$.*

Якщо твірна матриця записана у стандартній формі $G = (I \quad A)$, то перевірочна матриця має вигляд $H = (-A \quad I)$.

Доведення. Розмірність коду C як векторного простору дорівнює k. Розмірність ортогонального доповнення C' до простору, породженого рядками матриці H, теж дорівнює k. Отже, умова $GH^\top = 0$ еквівалентна припущенню, що кожний рядок G належить C', тобто $C \subset C'$. Таким чином, $C = C'$.

Другу частину твердження залишаємо читачеві в якості вправи. □

Зауважимо наостанок, що твірна та перевірочна матриці коду C є відповідно перевірочною та твірною матрицями деякого коду $C^\perp$. Такий код $C^\perp$ називається *дуальним*, або *ортогональним*,кодом до коду C. З погляду лінійної алгебри дуальний код $C^\perp$ є ортогональним доповнення до коду C.

13.3 Циклічні коди

Означення 13.7. *Нехай C — лінійний код довжиною n над полем F. Код C називається* циклічним*, якщо для довільного слова*

$$w = a_0 a_1 \dots a_{n-1} \in C$$

його циклічний зсув $a_{n-1}a_0 \dots a_{n-2}$ теж належить коду C.

З кожним словом $w = a_0 a_1 \dots a_{n-1} \in C$ можна пов'язати многочлен $w(x) = a_0 + a_1 x + \dots + a_{n-1}x^{n-1} \in F[x]$.

Нехай I — це ідеал в кільці $F[x]$, породжений многочленом $x^n - 1$, та нехай R — це факторкільце $F[x]/R$. Кожний клас суміжності з R можна однозначно подати у вигляді $f(x) + I$, де $f(x)$ — це многочлен з $F[x]$ степеня не більшого за $n - 1$. Отже, існує природна бієкція між множиною $R = F[x]/I$ та множиною F^n всіх слів довжиною n.

Твердження 13.7. *Код C довжиною n є циклічним кодом тоді і лише тоді, коли відповідні елементи кільця R утворюють ідеали.*

Доведення. Покажемо спершу, що множення на x у факторкільці R відповідає циклічному зсуву для коду C. Розглянемо слово $w = a_0 a_1 \dots a_{n-1}$. Йому відповідає многочлен $a_0 + a_1 x + \dots a_{n-1}x^{n-1}$. Помноживши на x, матимемо $a_0 x + a_1 x^2 + \dots a_{n-1}x^n$. Оскільки x^n та 1 належать одному класу суміжності за ідеалом I, то маємо рівність класів суміжності

$$a_0 x + a_1 x^2 + \dots a_{n-1}x^n + I = a_{n-1} + a_0 x + \dots + a_{n-2}x^{n-1} + I,$$

а многочлен $a_{n-1} + a_0 x + \dots a_{n-2}x^{n-1}$ відповідає слову $a_{n-1}a_0 \dots a_{n-2}$, яке є циклічним зсувом слова w.

Таким чином, якщо множина C є ідеалом, то вона замкнена відносно додавання та множення на скаляр (тобто є лінійним кодом), а також відносно множення на x (тобто замкнена відносно циклічного зсуву, а тому є циклічним кодом).

Навпаки, припустимо, що код C циклічний. Тоді він замкнений відносно додавання та множення на довільний скаляр або x. Поєднуючи ці дві дії, можемо побудувати будь-який многочлен. Отже, множина C замкнена відносно множення на довільний многочлен, а тому є ідеалом. □

Нагадаємо, що коли R — комутативне кільце з одиницею, в якому кожний ідеал є головним, то ця властивість зберігається для довільного факторкільця кільця R.

Твердження 13.8. *Кожний ідеал факторкільця $R = F[x]/(x^n - 1)$ породжується класом $g(x) + (x^n - 1)$, де $g(x)$ — унітарний дільник многочлена $x^n - 1$. Для кожного ідеалу існує єдиний такий многочлен.*

Доведення. Нехай ідеал I кільця $F[x]/(x^n - 1)$ породжується класом $f(x) + \left(x^n - 1\right)$. Нехай $g(x)$ — це унітарний найбільший спільний дільник многочленів $f(x)$ та $x^n - 1$. Тоді g ділить f, а тому (g) містить f. З іншого боку, з розширеного алгоритму Евкліда маємо рівність

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

Перейшовши до факторкільця R матимемо рівність класів суміжності

$$g(x) + \left(x^n - 1\right) = a(x)f(x) + \left(x^n - 1\right).$$

Отже, f ділить g, а тому (f) містить (g). Таким чином, $I = (g)$, де многочлен g — унітарний дільник многочлена $x^n - 1$. Єдиність такого многочлена випливає з другої теореми про гомоморфізм для кілець. □

Многочлен $g(x)$ називається *твірним многочленом* циклічного коду, який відповідає ідеалу $(g(x))$.

З цього твердження випливає, що для побудови всіх циклічних кодів довжиною n, ми повинні розкласти многочлен

$x^n - 1$ у добуток незвідних над полем F многочленів, перерахувати всі дільники $x^n - 1$ та для кожного дільника побудувати відповідний йому ідеал факторкільця R.

Наступна теорема дає спосіб за твірним многочленом циклічного коду виписати твірну та перевірочну матриці коду.

Теорема 13.6. *Нехай $g(x)$ — твірний многочлен циклічного коду C та*

$$g(x) = a_{n-k}x^{n-k} + a_{n-k-1}x^{n-k-1} + \cdots + a_0, \quad a_{n-k} = 1.$$

Нехай $x^n - 1 = g(x)h(x)$, де

$$h(x) = b_k x^k + b_{k-1}x^{k-1} + \cdots + b_0, \quad b_k = 1.$$

Тоді твірна матриця G та перевірочна матриця H мають вигляд

$$G = \begin{pmatrix} a_0 & a_1 & \dots & a_{n-k} & 0 & \dots & 0 \\ 0 & a_0 & a_1 & \dots & a_{n-k} & \dots & 0 \\ \vdots & \ddots & \vdots & \ddots & \vdots & \ddots & \vdots \\ 0 & \dots & 0 & a_0 & a_1 & \dots & a_{n-k} \end{pmatrix},$$

$$H = \begin{pmatrix} b_k & b_{k-1} & \dots & a_0 & 0 & \dots & 0 \\ 0 & b_k & b_{k-1} & \dots & b_0 & \dots & 0 \\ \vdots & \ddots & \vdots & \ddots & \vdots & \ddots & \vdots \\ 0 & \dots & 0 & b_k & b_{k-1} & \dots & b_0 \end{pmatrix}.$$

Доведення. Рядки матриці G відповідають многочленам $g(x)$, $xg(x), \dots, x^{k-1}g(x)$, отже, всі вони належать C. Візьмемо деяке слово $w \in C$, що відповідає многочлену $f(x)g(x) \pmod{x^n-1}$. Розділимо многочлен $f(x)$ на $h(x)$ з остачею:

$$f(x) = h(x)q(x) + r(x), \quad \text{де } r = 0 \text{ або } \deg r(x) < \deg k.$$

Тоді

$$f(x)g(x) = (x^n - 1)q(x) + r(x)g(x).$$

Звідси випливає, що

$$f(x)g(x) \equiv r(x)g(x) \pmod{x^n - 1},$$

а добуток $r(x)g(x)$ є лінійною комбінацією многочленів $x^i g(x)$, де $i < k$. Отже, слово w є лінійною комбінацією рядків матриці G. Звідси випливає, що код C є векторним простором, натягнутим на систему векторів–рядків матриці G.

На місці (i, j) матриці G стоїть елемент a_{j-i}, причому $a_l = 0$, якщо l не належить відрізку $[0, n-k]$. З подібним обмеженням на місці (i, j) стоїть елемент b_{k-j+i}. З правила множення матриць випливає, що на місці (i, j) матриці $GH^\top$ стоїть елемент

$$\sum_l a_{l-i} b_{k-l+j} = \sum_m a_m b_{k-i+j-m}.$$

Цей елемент є $(k - i + j)$-м коефіцієнтом добутку gh. Для $1 \leqslant i \leqslant k$ та $1 \leqslant j \leqslant n - k$ виконується

$$k - k + 1 = 1 \leqslant k - i + j \leqslant k - 1 + (n - k) = n - 1.$$

Але $g(x)h(x) = x^n - 1$ і всі відповідні коефіцієнти дорівнюють 0. Отже, $GH^\top = 0$ і за твердженням 13.6 матриця H є перевірочною матрицею коду C. □

З цієї теореми, зокрема, випливає, що $\dim C = k = n - \deg g(x)$.

Приклад 13.7. Опишемо всі бінарні циклічні коди довжиною 7. Маємо розклад

$$x^7 - 1 = (x - 1)(x^3 + x + 1)(x^3 + x^2 + 1).$$

Отже, існує 8 різних циклічних кодів, що відповідають дільникам $x^7 - 1$. Опишемо декілька кодів, решту залишимо читачеві як вправу.

- $g(x) = 1$. Цей код породжується словом 1000000 та його циклічними зсувами, а, отже, збігається з усім простором $\mathbb{F}_2^7$.
- $g(x) = x - 1$. Цей код породжується словом 1100000 та його циклічними зсувами та складається з усіх слів з парними вагами. Розмірність цього коду дорівнює 6, а мінімальна вага дорівнює 2.
- $g(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$. Цей код є кодом з повтореннями, який породжений словом 1111111.
- $g(x) = x^7 + 1$. Це взагалі не є кодом, бо ця множина містить лише нульовий вектор, а код за означенням повинен містити принаймні два кодових слова.

13.4 Коди БЧХ

У попередніх розділах ми побачили, як можна будувати коди заданих довжини та розмірності. Ця задача є доволі простою, проте задача відшукання мінімальної відстані вже є набагато складнішою. Звісно, зручно було б мати конструкцію, яка б дозволяла за наперед заданими довжиною n та мінімальною відстанню d знайти код довжиною n та мінімальною відстанню щонайменше d.

Конструкція кодів з такими властивостями була запропонована незалежно Хоквінгемом у 1959 р. та Боузом і Чоудхурі у 1960 р. Коди з такою властивістю називаються *кодами БЧХ*. Властивості цих кодів залежать від властивостей скінченних полів.

Коди, які ми будемо будувати, — це циклічні коди довжиною n над полем $\mathbb{F}_q$, де n та q — взаємно прості. Також у нас є наперед задане число $\delta \in \mathbb{N}$. Нижче ми визначимо код БЧХ довжиною n та заданою мінімальною відстанню δ.

Нехай e — це мультиплікативний порядок q за модулем n. Нехай a — первісний корінь степеня n з одиниці в $\mathbb{F}_{q^e}$. Нехай $\mathbb{F}_{q^e} = \mathbb{F}_q(\alpha)$. Тоді кожний елемент поля $\mathbb{F}_{q^e}$ можна однозначно подати у вигляді

$$c_0 + c_1\alpha + \cdots + c_{e-1}\alpha^{e-1}.$$

Кожному такому многочлену можна зіставити набір

$$(c_0 c_1 \ldots c_{e-1}).$$

З технічних міркувань будемо використовувати стовпцеве зображення $(c_0 c_1 \ldots c_{e-1})^\top$. Вибір елемента α несуттєвий, тому можемо взяти $\alpha = a$.

Означення 13.8. Кодом БЧХ довжиною n та конструктивною відстанню δ *називається код, перевірочна матриця якого має вигляд:*

$$H = \begin{pmatrix} 1 & a & a^2 & \ldots & a^{n-1} \\ 1 & a^2 & a^4 & \ldots & a^{2(n-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & a^{\delta-1} & a^{2(\delta-1)} & \ldots & a^{(\delta-1)(n-1)} \end{pmatrix}.$$

Кожний елемент матриці H належить полю $\mathbb{F}_{q^e}$, а тому вона є матрицею розміру $e \times 1$ над полем $\mathbb{F}_q$. Таким чином, матриця H є матрицею розміру $e(\delta - 1) \times n$ над полем $\mathbb{F}_q$.

Теорема 13.8. *Мінімальна відстань коду БЧХ довжиною n та конструктивною відстанню δ дорівнює щонайменше δ, а його розмірність не менша за $n - e(\delta - 1)$.*

Доведення. Щоб показати, що мінімальна відстань коду не менша за δ, необхідно і достатньо довести, що довільні $\delta - 1$ стовпців перевірочної матриці лінійно незалежні.

Розглянемо визначник матриці, складеної зі стовпців з номерами $m_1, m_2, \ldots, m_{\delta-1}$ матриці H як матриці над полем $\mathbb{F}_{q^e}$:

$$\begin{pmatrix} a^{m_1} & \dots & a^{m_{\delta-1}} \\ \vdots & \ddots & \vdots \\ a^{m_1(\delta-1)} & \dots & a^{m_{\delta-1}(\delta-1)} \end{pmatrix}.$$

Винісши з i–го стовпця, $i = 1, \dots, \delta - 1$, множник $a^{m_i} \neq 0$, одержимо визначник Вандермонда $V(a^{m_1}, \dots, a^{m_{\delta-1}})$, який не дорівнює 0, бо всі $a^{m_1}, \dots, a^{m_{\delta-1}}$ різні. Отже, обрані стовпці лінійно незалежні над полем $\mathbb{F}_{q^e}$, а тому лінійно незалежні і над меншим полем.

Розмірність коду дорівнює $n - \operatorname{rank} H$. А ранг перевірочної матриці H не більший за кількість стовпців, яка дорівнює $e(\delta - 1)$. □

Теорема 13.9. *Коди БЧХ є циклічними.*

Доведення. Будь–якому слову $w = c_0 c_1 \dots c_{n-1}$ відповідає многочлен $f(x) = c_0 + c_1 x + \dots + c_{n-1} x^{n-1}$. Умова належності слова w коду БЧХ може бути записана наступним чином

$$f(a^i) = c_0 + c_1 a^i + \dots + c_{n-1} a^{i(n-1)} = 0,$$

для $i = 1, 2, \dots, \delta - 1$.

Нехай $g(x)$ — це найменше спільне кратне мінімальних многочленів елементів $a, a^2, \dots, a^{\delta-1}$ над полем $\mathbb{F}_q$. Тоді слово, що відповідає $f(x)$ належить коду БЧХ тоді і лише тоді, коли $f(x)$ ділиться на $g(x)$. Більше того, корені $g(x)$ є коренями n–го степеня з одиниці, отже, $g(x)$ ділить $x^n - 1$. Таким чином, коди БЧХ є циклічними кодами з твірним многочленом $g(x)$. □

Важливим частковим випадком кодів БЧХ є випадок, коли $n = q - 1$. Коди з такою властивістю називаються *кодами Ріда–Соломона*. У цьому випадку $\operatorname{ord}_n q = 1$, тому відповідно до теореми 13.8 для коду C Ріда–Соломона одержимо $\dim C \geqslant n - \delta + 1$. З іншого боку, якщо справжня мінімальна відстань

дорівнює d, то $\delta \leqslant d$ і границя Сінглтона дасть $|C| \leqslant q^{n-d+1}$, звідки $\dim(C) \leqslant n - d + 1$. Підсумувавши, одержимо

$$n - d + 1 \leqslant n - \delta + 1 \leqslant \dim(C) \leqslant n - d + 1,$$

що дає $\dim(C) = n - d + 1$. Отже, маємо таку властивість кодів Ріда–Соломона:

Твердження 13.9. *Мінімальна відстань коду Ріда–Соломона з конструктивною відстанню δ дорівнює δ, а розмірність дорівнює $n - \delta + 1$. Отже, коди Ріда–Соломона є роздільними кодами з максимальною відстанню.*

Розділ 14

Застосування до комбінаторики

14.1 Латинські квадрати

Означення 14.1. *Таблиця*

$$L = (a_{ij}) = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{pmatrix}$$

називається латинським квадратом порядку n, якщо кожний рядок і кожний стовпчик цієї таблиці містять рівно по одному разу кожний елемент з заданої n-елементної множини.

Приклад 14.1. Латинський квадрат порядку 3:

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \\ 2 & 3 & 1 \end{pmatrix} \quad \square$$

Теорема 14.2. *Для довільного $n \in \mathbb{N}$ існує латинський квадрат порядку n.*

Доведення. Розглянемо таблицю (a_{ij}), де $a_{ij} \equiv i + j \pmod{n}$, $1 \leqslant a_{ij} \leqslant n$. Тоді з рівності $a_{ij} = a_{ik}$ випливає, що $i + j \equiv i + k$

$(\mathrm{mod}\ n)$, тобто $j \equiv k\ (\mathrm{mod}\ n)$, що дає $j = k$, бо $1 \leqslant i, j, k \leqslant n$. Аналогічно з рівності $a_{ij} =_{kj}$ випливає, що $i = k$. Таким чином, елементи кожного рядка і кожного стовпця всі різні. □

Означення 14.2. *Два латинських квадрата (a_{ij}) та (b_{ij}) називаються порядку n називаються попарно ортогональними, якщо всі n^2 впорядкованих пар (a_{ij}, b_{ij}) різні*

Приклад 14.3. Латинські квадрати

$$L_1 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \\ 2 & 3 & 1 \end{pmatrix} \text{ та } L_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{pmatrix}$$

попарно ортогональні. Відповідними їм парами є

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

Отже, латинські квадрати L_1 та L_2 дійсно ортогональні. □

Використовуючи існування скінченних полів порядку q, можна показати, що коли $n = q$ і є степенем простого числа, то існує $q - 1$ попарно ортогональних латинських квадратів порядку q.

Теорема 14.4. *Нехай $a_0 = 0, a_1, \ldots, a_{q-1}$ — елементи поля $\mathbb{F}_q$. Тоді таблиці вигляду*

$$L_k = \begin{pmatrix} a_0 & a_1 & \ldots & a_{q-1} \\ a_k a_1 & a_k a_1 + a_1 & \ldots & a_k a_1 + a_{q-1} \\ a_k a_2 & a_k a_2 + a_1 & \ldots & a_k a_2 + a_{q-1} \\ \vdots & \vdots & \ddots & \vdots \\ a_k a_{q-1} & a_k a_{q-1} + a_1 & \ldots & a_k a_{q-1} + a_{q-1} \end{pmatrix}, \quad k = 1, \ldots, q-1,$$

утворюють множину з $q-1$ попарно ортогональних латинських квадратів порядку q.

Доведення. Очевидно, що кожна таблиця вигляду L_k є латинським квадратом.

Нехай $a_{ij}^{(k)} = a_k a_{i-1} + a_{j-1}$ — це (i,j)-й елемент латинського квадрата L_k. Якщо $k \neq m$, то припустимо, що для деяких $1 \leqslant i, j, g, h \leqslant q$

$$(a_{ij}^{(k)}, a_{ij}^{(m)}) = (a_{gh}^{(k)}, a_{gh}^{(m)}).$$

Тоді

$$(a_k a_{i-1} + a_{j-1}, a_m a_{i-1} + a_{j-1}) = (a_k a_{g-1} + a_{h-1}, a_m a_{g-1} + a_{h-1}),$$

звідки

$$a_k(a_{i-1} - a_{g-1}) = a_{h-1} - a_{j-1}, \quad a_m(a_{i-1} - a_{g-1}) = a_{h-1} - a_{j-1}.$$

Оскільки $a_k \neq a_m$, то отримаємо, що $a_{i-1} = a_{g-1}$, $a_{h-1} = a_{j-1}$. Отже, $i = g$, $j = h$. Таким чином, всі впорядковані пари однаково розташованих елементів L_k та L_m є різними, тобто латинські квадрати L_k та L_m ортогональні. □

Приклад 14.5. Над полем $\mathbb{F}_5$ можна побудувати 4 попарно ортогональних латинських квадратів. Перерахуємо їх:

$$L_1 = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 & 0 \\ 2 & 3 & 4 & 0 & 1 \\ 3 & 4 & 0 & 1 & 2 \\ 4 & 0 & 1 & 2 & 3 \end{pmatrix}, \quad L_2 = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 0 & 1 \\ 4 & 0 & 1 & 2 & 3 \\ 1 & 2 & 3 & 4 & 0 \\ 3 & 4 & 0 & 1 & 2 \end{pmatrix},$$

$$L_3 = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 \\ 3 & 4 & 0 & 1 & 2 \\ 1 & 2 & 3 & 4 & 0 \\ 4 & 0 & 1 & 2 & 3 \\ 2 & 3 & 4 & 0 & 1 \end{pmatrix}, \quad L_4 = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 \\ 4 & 0 & 1 & 2 & 3 \\ 3 & 4 & 0 & 1 & 2 \\ 2 & 3 & 4 & 0 & 1 \\ 1 & 2 & 3 & 4 & 0 \end{pmatrix}.$$

Бібліографія

[1] Безущак О.О., Ганюшкін О.Г. Теорія груп: Навчальний посібник для студентів механіко-математичного факультету. – К.: ВПЦ “Київський університет”, 2005.

[2] Lidl R., Niederreiter H. Finite Fields. – Addison-Wesley Publishing Company, Advanced Book Program/World Science Division, 1983.

[3] Menezes A., Blake I. Applications of Finite Fields. – Kluwer international series in engineering and computer science: Communications and information theory The Springer International Series in Engineering and Computer Science, 1993.

[4] Aigner M., Ziegler G. (2009). Proofs from THE BOOK. – Berlin, New York: Springer-Verlag, 2009.