Глава 1

Начални сведения за кодове и крайни полета

1. Основни понятия за кодове - минимално разстояние, пораждаща и проверочна матрица, дуален код, граница на Singleton

Кодовете са схеми за предаване на информация, които позволяват коригирането на определен брой грешки, възникнали от шума по канала за предаване. Математически, кодовете са крайни множества от думи C с фиксирана дължина n, които могат да се възстановяват еднозначно при смущение на не повече от t символа. Азбуката на тези думи е най-често крайно поле $\mathbb{F}_q$ с q елемента. Ако C е линейно пространство над $\mathbb{F}_q$, казваме, че C е линеен код.

Определение 1.1. *Разстоянието на Hamming $d(x,y)$ между $x, y \in \mathbb{F}_q^n$ е броят на различните компоненти $x_i \neq y_i$ за $1 \leq i \leq n$.*

Лема 1.2. *Разстоянието на Hamming $d : \mathbb{F}_q^n \times \mathbb{F}_q^n \to \{0, 1, \ldots, n\}$ е метрика.*

Доказателство: Ясно е, че $d(x,y) \geq 0$ с равенство $d(x,y) = 0$ точно когато $x = y$. Освен това $d(x,y) = d(y,x)$. Остава да се провери неравенството на триъгълника $d(x^{(1)}, x^{(3)}) \leq d(x^{(1)}, x^{(2)}) + d(x^{(2)}, x^{(3)})$ за произволни $x^{(1)}, x^{(2)}, x^{(3)} \in \mathbb{F}_q^n$. Да означим

$$I_{ij} = \{1 \leq k \leq n \ \mid \ x_k^{(i)} \neq x_k^{(j)}\} \quad \text{за всички} \quad 1 \leq i < j \leq 3.$$

С допускане на противното проверяваме, че $I_{13} \subseteq I_{12} \cup I_{23}$. Следователно

$$d(x^{(1)}, x^{(3)}) = |I_{13}| \leq |I_{12}| + |I_{23}| = d(x^{(1)}, x^{(2)}) + d(x^{(2)}, x^{(3)})$$

и $d : \mathbb{F}_q^n \times \mathbb{F}_q^n \to \{0, 1, \ldots, n\}$ е метрика, Q.E.D.

Определение 1.3. *Минималното разстояние $d(C)$ на код $C \subset \mathbb{F}_q^n$ е най-малкото разстояние между две различни думи на C.*

При фиксирана дължина n и минимално разстояние $d(C)$ се търсят кодове $C \subset \mathbb{F}_q^n$ с възможно най-голям брой думи $|C|$ или с възможно най-висока ефективност при предаване на информация.
При фиксирана дължина n и брой на думите $|C|$ се максимизира минималното разстояние $d = d(C)$. Причина за това е еднозначността на декодиране при не повече от $\left[\frac{d-1}{2}\right]$ грешни символа в процеса на предаване на информация. (Да напомним, че $\left[\frac{d-1}{2}\right]$ означава цялата част на $\frac{d-1}{2}$ или най-голямото цяло число, ненадминаващо $\frac{d-1}{2}$.) Нека

$$B_n(x, r) = \{y \in \mathbb{F}_q^n \ \mid \ d(x,y) \leq r\}$$

е затвореното кълбо с център x и радиус r в $\mathbb{F}_q^n$ относно разстоянието на Hamming. Ако $C \subset \mathbb{F}_q^n$ е код с минимално разстояние $d = d(C)$, твърдим, че кълбата $B_n\left(x, \left[\frac{d-1}{2}\right]\right)$ с центрове $x \in C$ не се пресичат две по две. В противен случай, за различни $x, y \in C$ и $z \in B_n\left(x, \left[\frac{d-1}{2}\right]\right) \cap B_n\left(y, \left[\frac{d-1}{2}\right]\right)$, неравенството на триъгълника дава

$$d \leq d(x,y) \leq d(x,z) + d(y,z) \leq 2\left[\frac{d-1}{2}\right] < d.$$

Ако C е не само подмножество, но и линейно подпространство на $\mathbb{F}_q^n$, то броят на думите в C е q^k, където k е размерността на C над $\mathbb{F}_q$. В такъв случай казваме, че думите $x = (x_1, \ldots, x_n) \in C$ от кода имат k информационни и $n - k$ проверочни символа. Определяме минималното тегло $w(C)$ на C като най-малкият брой ненулеви компоненти в ненулева дума от C. За линейни кодове $w(C) = d(C)$. По-точно, ако $d(C) = d(x, y)$, то $d(C) = w(x - y) \geq w(C)$. В сила е и обратното неравенство $w(C) = w(z) = d(z, \mathbb{O}) \geq d(C)$, откъдето $w(C) = d(C)$.

Пример 1.4. *Да разгледаме* 1*-мерния код* $C = \{(0,0,0), (1,1,1)\} \subset \mathbb{F}_2^3$ *с дължина* 3*. Неговото минимално разстояние е* 3*, така че декодирането е еднозначно при смущение на не повече от* $\left[\frac{3-1}{2}\right] = 1$ *символ. Понеже всяка дума от* $\mathbb{F}_2^3$ *има поне два равни символа и е на разстояние* ≤ 1 *от кодова дума, от всяка получена дума* $\forall x \in \mathbb{F}_2^3$ *можем да възстановим еднозначно кодовата дума* $c \in C$*, от която е възникнала.*

Определение 1.5. *Ако* $g^{(i)} = (g_{i1}, \ldots, g_{in})$*,* $1 \leq i \leq k$ *е базис на линейния код* $C \subset \mathbb{F}_q^n$ *над* $\mathbb{F}_q$*, то матрицата* $G = (g_{ij})_{i=1}^{k}{}_{j=1}^{n} \in (\mathbb{F}_q)_{k \times n}$*, образувана по редове от* $g^{(1)}, \ldots, g^{(k)}$ *се нарича пораждаща матрица на* C*.*

Определение 1.6. *Ако* $H \in M_{m,n}(\mathbb{F}_q)$ *е матрица с* m *реда,* n *стълба и елементи от крайното поле* $\mathbb{F}_q$*, а* $C \subset \mathbb{F}_q^n$ *е пространството от решения на хомогенната система линейни уравнения* $Hx^t = \mathbb{O}$*, то* H *се нарича проверочна матрица на* C*.*

Ако $\dim_{\mathbb{F}_q}(C) = k$, то H е от ранг $\mathrm{rk}H = n - k$. Следователно H има $m \geq n - k$ реда. Без ограничение на общността можем да изпуснем зависимите уравнения и да считаме, че H има $m = n - k$ реда.
В $\mathbb{F}_q$-линейното пространство $\mathbb{F}_q^n$ въвеждаме вътрешно произведение

$$\langle x, y \rangle = x_1 y_1 + x_2 y_2 + \ldots + x_n y_n \quad \text{за} \quad x, y \in \mathbb{F}_q^n.$$

Непосредствено се вижда, че вътрешното произведение е симетрична билинейна билинейна форма с максимален ранг n.

Определение 1.7. *Нека* $C \subset \mathbb{F}_q$ *е код. Ортогоналното допълнение*

$$\{x \in \mathbb{F}_q^n \mid \langle x, c \rangle = 0 \quad \textit{за} \quad \forall c \in C\}$$

на C *относно* $\langle\ ,\ \rangle$ *се нарича дуален код на* C *и се бележи с* $C^\perp$*.*

Ако $C \subset \mathbb{R}^n$ е $\mathbb{R}$-линейно подпространство на $\mathbb{R}^n$, то $\mathbb{R}^n = C \oplus C^\perp$ се разлага в директна сума на C и $C^\perp$, т.е. $\mathbb{R}^n = C + C^\perp$ и $C \cap C^\perp = \{0^n\}$. За $\mathbb{F}_q$-линейни подпространства $C \subset \mathbb{F}_q^n$ това не винаги е вярно. Като пример да разгледаме едномерното подпространство $C = \{(0,0,0), (1,1,0)\}$ на $\mathbb{F}_2^3$ над $\mathbb{F}_2$. По определение,

$$C^\perp = \{(x_1, x_2, x_3) \in \mathbb{F}_2^3 \mid x_1 + x_2 = 0\} = \{(x_1, x_1, x_3) \in \mathbb{F}_2^3 \mid x_1, x_3 \in \mathbb{F}_2\}.$$

Да забележим, че $\dim_{\mathbb{F}_2} C^\perp = 2$ и $C^\perp \supseteq C$, така че $C + C^\perp = C^\perp \subsetneq \mathbb{F}_2^3$ и $C \cap C^\perp = C \neq \{0^3\}$.
Ако $G \in M_{k,n}(\mathbb{F}_q)$ е пораждаща матрица на кода $C \subset \mathbb{F}_q^n$, то пространството от решения на хомогенната линейна система $Gx = 0_{k \times 1}$ съвпада с $C^\perp$ и G е проверочна матрица на $C^\perp$. Още повече,

$$\dim C + \dim C^\perp = \mathrm{rk}G + \dim C^\perp = n.$$

Да отбележим, че $C \subseteq (C^\perp)^\perp$, защото за $\forall c \in C$ и за $\forall c' \in C^\perp$ е изпълнено $\langle c, c' \rangle = 0$. Съгласно $\dim C = n - \dim C^\perp = \dim(C^\perp)^\perp$ имаме съвпадение

$$C = (C^\perp)^\perp.$$

Ако G е проверочна матрица на $C^\perp$, то линейната обвивка на вектор-редовете на G се съдържа, а оттам и съвпада с $(C^\perp)^\perp = C$, защото $\mathrm{rk}G = n - \dim C^\perp = \dim C$. С това проверихме, че $G \in M_{k,n}(\mathbb{F}_q)$ е пораждаща матрица на C точно когато е проверочна матрица на $C^\perp$. Вземайки предвид $(C^\perp)^\perp = C$ получаваме, че H е пораждаща матрица на $C^\perp$ точно когато е проверочна матрица на C.

Лема 1.8. *(i) Нека $H \in M_{n-k,n}(\mathbb{F}_q)$ е проверочна матрица на линеен код $C \subset \mathbb{F}_q^n$. В такъв случай, C има минимално разстояние d тогава и само тогава, когато произволни $d-1$ стълба на H са линейно независими и съществуват d линейно зависими стълба на H.*
(ii) Граница на Singleton: *Ако $C \subset \mathbb{F}_q^n$ е линеен код с дължина n, размерност $\dim C = k$ и минимално разстояние d, то $k + d \leq n + 1$.*

Доказателство: (i) Линейната система уравнения $Hx^t = \mathbb{O}$ има решение c с тегло $w = w(c)$ тогава и само тогава, когато w стълба на H изпълняват линейна зависимост, чиито всички коефициенти са ненулеви. Минималното разстояние d на линеен код C е минималното естествено число, за което съществува ненулева дума на C с тегло d.
(ii) Ако $C \subset \mathbb{F}_q^n$ е линеен код с размерност k, то произволна проверочна матрица H на C е от ранг $n-k$. Следователно произволни $n-k+1$ стълба на H са линейно зависими и $d \leq n-k+1$.
Ето втори начин за доказване на границата на Singleton. Ако линейният код $C \subset \mathbb{F}_q^n$ има минимално разстояние d, то координатното подпространство $W = \mathbb{F}_q^{d-1} \times \{(0^{n-d+1}\} \subset \mathbb{F}_q^{d-1} \times \mathbb{F}_q^{n-d+1}$ има тривиално сечение $W \cap C = \{0^n\} \subset \mathbb{F}_q^n$ с кода C. По теоремата за размерност на сума и сечение,

$$k + (d-1) = \dim C + \dim W = \dim(C+W) + \dim(C \cap W) = \dim(C+W) \leq n,$$

Q.E.D.

Определение 1.9. *Линейният код C с дължина n, размерност k и минимално разстояние d се нарича максимално отделим (Maximum Distance Separable or MDS-code), ако параметрите му изпълняват единната граница с равенство, $k + d = n + 1$.*

Линеен код $C \subset \mathbb{F}_q^n$ е максимално отделим точно когато е в общо положение спрямо координатните оси в $\mathbb{F}_q^n$.

Пример 1.10. (Кодове на Reed-Solomon) *За произволно крайно поле $\mathbb{F}_q$ с q елемента и произволни естествени числа $k \leq n \leq q$ нека*

$$\mathbb{F}_q[x]^{(k)} := \{f(x) \in \mathbb{F}_q[x] \quad | \quad \deg(f) \leq k-1\}$$

е k-мерното линейно пространство на полиномите на x от степен не по-голяма от $k-1$ с коефициенти от $\mathbb{F}_q$, а $a_1, \ldots, a_n \in \mathbb{F}_q$ са различни точки. Разглеждаме остойностяващото изображение

$$\mathcal{E} : \mathbb{F}_q[x]^{(k)} \longrightarrow \mathbb{F}_q^n,$$

$$\mathcal{E}(f) = (f(a_1), \ldots, f(a_n)) \quad за \quad \forall f \in \mathbb{F}_q[x]^{(k)}.$$

Непосредствено се проверява, че $\mathcal{E}$ е $\mathbb{F}_q$-линейно влагане, защото полином $f \in \mathbb{F}_q[x]^{(k)}$ от степен $\deg(f) \leq k-1$ може да има най-много $k-1$ различни корена. Образът $C := \mathrm{im}\mathcal{E} = \mathcal{E}(\mathbb{F}_q[x]^{(k)})$ на $\mathcal{E}$ е линеен код с дължина n и размерност k, който се нарича код на Reed-Solomon. Всяка ненулева дума $\mathcal{E}(f) \in C \setminus \{0^n\}$ има най-много $k-1$ нулеви компоненти, откъдето най-малко $n-k+1$ ненулеви координати. Комбинирайки с границата на Singleton $d \leq n+1-k$ получаваме, че минималното разстояние на кода C е $d = n+1-k$. Следователно кодът $C = \mathcal{E}(\mathbb{F}_q[x]^{(k)}) \subset \mathbb{F}_q^n$ на Reed-Solomon е максимално отделим.

Алгебро-геометричните кодове са пространства от стойности на функции върху краен брой точки $P_1, \ldots, P_n$ от крива X. Техните дуални кодове $C^\perp$ се състоят от резидуумите на подходящи диференциални форми в същите точки $P_1, \ldots, P_n$. В настоящия въпрос ще скицираме конструкцията на C и $C^\perp$, без да уточняваме свойствата на използваните функции и диференциални форми. Точка P от крива X е $\mathbb{F}_q$-рационална, ако се представя чрез наредена m-торка $P = (x_1, \ldots, x_m)$ с елементи $x_i \in \mathbb{F}_q$. Произволна гладка крива X има крайно множество $X(\mathbb{F}_q)$ от $\mathbb{F}_q$-рационални точки. Избираме подмножество $D = \{P_1, \ldots, P_n\} \not\subseteq X(\mathbb{F}_q)$ с n елемента. Разглеждаме крайномерни линейни пространства V_ν над $\mathbb{F}_q$, съставени от функции $f : D \to \mathbb{F}_q$, които се анулират върху най-много $\nu < n$ от точките $P_1, \ldots, P_n$. Остойностяващото изображение

$$\mathcal{E}_D : V_\nu \longrightarrow \mathbb{F}_q^n,$$

$$\mathcal{E}_D(f) = (f(P_1), \ldots, f(P_n)) \quad \text{за} \quad \forall f \in V_\nu$$

е $\mathbb{F}_q$-линейно влагане и образът $C_{D,\nu} = \mathcal{E}_D(V_\nu)$ е $\mathbb{F}_q$-линейно подпространство на $\mathbb{F}_q^n$ с размерност $k = \dim_{\mathbb{F}_q}(C_{D,\nu}) = \dim_{\mathbb{F}_q}(V_\nu)$. Ако $C_{D,\nu}$ има минимално разстояние d и $u = (f(P_1), \ldots, f(P_n)) \in C_{D,\nu}$ е дума с тегло d, то $f \in V_\nu$ се анулира точно в $n - d$ точки от D и $n - d \leq \nu$, съгласно определението на V_ν. Оттук $d \geq n - \nu$.

2. Алгебрични разширения на полета

Определение 1.11. *Ако $F \supset K$ е разширение на полета (т.е. K е подполе на поле F) и $a_1, \ldots, a_m \in F$, то полето $K(a_1, \ldots, a_m)$, съставено от рационалните функции*

$$\frac{f(a_1, \ldots, a_m)}{g(a_1, \ldots, a_m)}$$

или частните на полиномите $f(x_1, \ldots, x_m), g(x_1, \ldots, x_m) \in K[x_1, \ldots, x_m]$, $g(a_1, \ldots, a_m) \neq 0$ на $a_1, \ldots, a_m$ с коефициенти от K се нарича разширение на K чрез $a_1, \ldots, a_m$.
Разширенията от вида $K(a_1, \ldots, a_m) \supset K$ се наричат крайнопородени. Казваме, че $K(a_1)$ е просто разширение на K чрез a_1.

Определение 1.12. *Нека K е подполе на поле F. Елементът $\alpha \in F$ е алгебричен над K, ако съществува полином $f(x) \in K[x] \setminus K$ с корен α, $f(\alpha) = 0$.*

Твърдение 1.13. *Нека K е подполе на поле F, $\alpha \in F$ е алгебричен над K елемент на F, а $f(x) \in K[x] \setminus K$ е полином от минимална степен $\deg(f) = d$ със старши коефициент 1 и корен α, $f(\alpha) = 0$. Тогава:*
(i) множеството

$$I(\alpha) := \{g(x) \in K[x] \;\mid\; g(\alpha) = 0\}$$

на полиномите от $K[x]$ с корен α съвпада с главния идеал $\langle f(x)\rangle \triangleleft K[x]$, породен от $f(x)$;
(ii) $f(x) \in K[x]$ е неразложим над K;
(iii) ако $h(x) \in K[x]$ е полином от минимална степен $\deg(h) = d$ със старши коефициент 1 и $h(\alpha) = 0$, то $h(x) \equiv f(x)$ съвпадат като полиноми (т.е. $f(x)$ и $h(x)$ имат едни и същи коефициенти пред равните степени на x);
(iv) простото алгебрично разширение $K(\alpha)$ на K чрез α съвпада с пръстена

$$K[\alpha] = \{g(\alpha) \;\mid\; g(x) \in K[x]\}$$

на полиномите на α с коефициенти от K;

(v) полето $K(\alpha)$ е линейно пространство над полето K с размерност $\dim_K K(\alpha) = d$.

Доказателство: (i) Включването $\langle f(x)\rangle = \{f(x)h(x) \mid h(x) \in K[x]\} \subseteq I(\alpha)$ следва непосредствено от $f(\alpha)h(\alpha) = 0h(\alpha) = 0$. За обратното включване $I(\alpha) \subseteq \langle f(x)\rangle$ да разгледаме произволен полином $g(x) \in I(\alpha)$ и да го разделим на $f(x)$ с частно $q(x) \in K[x]$ и остатък $r(x) \in K[x]$, $\deg(r) < d = \deg(f)$. Заместваики $x = \alpha$ в $g(x) = f(x)q(x) + r(x)$ получаваме $r(\alpha) = 0$. Съгласно избора на $f(x) \in K[x] \setminus K$ от минимална степен с корен α, оттук следва $r(x) \equiv 0$. В резултат, $g(x) = f(x)q(x) \in \langle f(x)\rangle$ и $I(\alpha) = \langle f(\alpha)\rangle$.
(ii) Нека $f(x) = f_1(x)f_2(x)$ е същинско разлагане на $f(x)$ над K, т.е. $f_i(x) \in K[x]$ са от степени $0 < \deg(f_i) < \deg(f) = d$. Тогава от $0 = f(\alpha) = f_1(\alpha)f_2(\alpha)$ с $f_i(\alpha) \in F$ следва $f_j(\alpha) = 0$ за някое $j \in \{1, 2\}$, защото полето F няма делители на нулата. Ако $b_j \in K^*$ е старшият коефициент на $f_j(x) \in K[x] \setminus K$, то $b_j^{-1}f_j(x) \in K[x]\setminus K$ е полином от степен $\deg(b_0^{-1}f_j(x)) = \deg(f_j(x)) < \deg(f) = d$ със старши коефициент 1 и корен α, което противоречи на избора на $f(x)$ и доказва неразложимостта на $f(x)$ над K.
(iii) Ако $h(x) \in K[x] \setminus K$ е полином от минимална степен $\deg(h) = \deg(f) = d$ със старши коефициент 1 и корен α, то $g(x) := f(x) - h(x) \in K[x]$ е полином от степен $\deg(g) < d$ с корен α. Съгласно избора на $f(x)$ оттук следва, че $g(x) \equiv 0$ или $f(x) \equiv h(x)$.
(iv) Всеки полином $g(\alpha)$ на α с коефициенти от K може да се разглежда като рационална функция $\frac{g(\alpha)}{1_K} \in K(\alpha)$. Затова $K[\alpha] \subseteq K(\alpha)$. Трябва да докажем, че за произволни $g(\alpha), h(\alpha) \in K[\alpha]$ с $h(\alpha) \neq 0$ съществува полином $t(\alpha) \in K[\alpha]$, така че $\frac{g(\alpha)}{h(\alpha)} = t(\alpha)$. По-точно, полиномите $f(x)$ и $h(x)$ са взаимно прости, защото неразложимият над K полином $f(x)$ не дели $h(x)$. Съгласно тъждеството на Безу съществуват $u(x), v(x) \in K[x]$, така че $f(x)u(x) + h(x)v(x) = 1$. Заместваики $x = \alpha$ получаваме $h(\alpha)v(\alpha) = 1$ или

$$\frac{1}{h(\alpha)} = v(\alpha).$$

В резултат,

$$\frac{g(\alpha)}{h(\alpha)} = g(\alpha)v(\alpha) =: t(\alpha) \in K[\alpha]$$

и $K(\alpha) \subseteq K[\alpha]$.
(v) Полето $K(\alpha)$ е линейно пространство над своето подполе K. Ако

$$f(x) = x^d + c_{d-1}x^{d-1} + \ldots + c_1x + c_0 \in K[x], \quad \text{то}$$

$$\alpha^d = \sum_{i=0}^{d-1}(-c_i)\alpha \in K\alpha^{d-1} + K\alpha^{d-2} + \ldots + K\alpha + K = l_K(1, \alpha, \ldots, \alpha^{d-1}).$$

С индукция по $m \geq d$ установяваме, че $\alpha^m \in l_K(1, \alpha, \ldots, a^{d-1})$ е от K-линейната обвивка на мономите $1, \alpha, \ldots, \alpha^{d-1}$. По-точно, ако $\alpha^{m-1} = \sum\limits_{i=0}^{d-1} k_i\alpha^i$, то

$$\alpha^m = \alpha.\alpha^{m-1} = k_{d-1}\alpha^d + \sum_{i=0}^{d-2} k_i\alpha^{i+1} =$$

$$= k_{d-1}\left[\sum_{i=0}^{d-1}(-c_i)\alpha^i\right] + \sum_{j=1}^{d-1} k_{j-1}\alpha^j = -k_{d-1}c_0 + \sum_{i=1}^{d-1}(k_{i-1} - c_ik_{d-1})\alpha^i.$$

Следователно

$$K[\alpha] = l_K(1, \alpha, \ldots, \alpha^{d-1}, \alpha^d, \ldots) = \sum_{i=0}^{\infty} K\alpha^i \subseteq l_K(1, \alpha, \ldots, \alpha^{d-1}) \subseteq K[\alpha]$$

или $K[\alpha] = l_K(1, \alpha, \ldots, \alpha^{d-1})$ е K-линейната обвивка на $1, \alpha, \ldots, \alpha^{d-1}$. Тези мономи са линейно независими, защото в противен случай α е корен на полином $g(x) \in K[x] \setminus K$ от степен $\deg(g) \leq d-1 < d$. Следователно $K(\alpha) = K[\alpha]$ има базис $1, \alpha, \ldots, \alpha^{d-1}$ над K и $\dim_K K(\alpha) = d$, Q.E.D.

Определение 1.14. *Разширението $F \supset K$ е алгебрично, ако всеки елемент $a \in F$ е алгебричен над K.*

Определение 1.15. *Полето F е крайно разширение на полето K, ако F е крайномерно линейно пространство над K.*
Ако $F \supset K$ е крайно разширение, то размерността на F над K се нарича степен на F над K и се бележи с $[F : K] = \dim_K F$.

Ако $F \supset K$ и $E \supset F$ са крайни разширения, то $E \supset K$ е крайно разширение и

$$[E : K] = [E : F][F : K].$$

Това е непосредствено следствие на факта, че ако $e_1, \ldots e_n$ е базис на E над F и $f_1, \ldots, f_m$ е базис на F над K, то $\{e_i f_j \mid 1 \leq i \leq n, \ \ 1 \leq j \leq m\}$ е базис на E над K.

Определение 1.16. *Ако K е подполе на поле F, а $\alpha \in F$ е алгебричен над K, то единственият полином $f(x) \in K[x] \setminus \{0\}$ от минимална степен $d \in \mathbb{N}$ със старши коефициент 1 и $f_\alpha(\alpha) = 0$ се нарича минимален полином на α над K. Степента $[K(\alpha) : K] = d = \deg(f_\alpha(x))$ на простото алгебрично разширение $K(\alpha)$ над K се нарича степен на алгебричност на α над K.*

Нека $\alpha \in F$ има минимален полином $f(x) = x^d + \sum_{i=0}^{d-1} c_i x^i \in K[x]$ над K. В доказателството на Твърдение 1.13 (v) установихме, че простото алгебрично разширение

$$K(\alpha) = K[\alpha] = l_K(1, \alpha, \ldots, \alpha^{d-1}) = K[\alpha]^{(d)}$$

на K съвпада с K-линейното пространство на полиномите на α от степен $\leq d-1$ с коефициенти от K. Събирането и изваждането в $K[\alpha]^{(d)}$ се свежда до събиране и изваждане на коефициентите на α^i,

$$\left(\sum_{i=0}^{d-1} a_i \alpha^i\right) \pm \left(\sum_{i=0}^{d-1} b_i \alpha^i\right) = \sum_{i=0}^{d-1} (a_i \pm b_i)\alpha^i.$$

Умножението

$$\left(\sum_{i=0}^{d-1} a_i \alpha^i\right)\left(\sum_{j=0}^{d-1} b_j \alpha^j\right) = \sum_{i=0}^{2(d-1)} \left(\sum_{s=0}^{i} a_s b_{i-1}\right)\alpha^i \in K[\alpha]$$

започва с умножение на полиноми на α. Както в доказателството на Твърдение 1.13 (v), изразяваме последователно $\alpha^d, \alpha^{d+1}, \ldots, \alpha^{2(d-1)} \in K^{(d)}[\alpha]$ като полиноми на α от степени $\leq d-1$ с коефициенти от K, използвайки минималния полином $\alpha^d = \sum_{i=0}^{d-1} (-c_i)\alpha^i$ на α над K. Делението на $g(\alpha) = \sum_{i=0}^{d-1} a_i \alpha^i$ с $h(\alpha) = \sum_{i=0}^{d-1} b_i \alpha^i \neq 0$ повтаря разсъжденията от доказателството на Твърдение 1.13(iv). По-точно, по алгоритъма на Евклид намираме полиноми $u(x), v(x) \in K[x]$, изпълняващи тъждеството на Безу $f(x)u(x) + h(x)v(x) = 1$. Частното

$\frac{g(\alpha)}{h(\alpha)} = g(\alpha)v(\alpha) \in K[\alpha]$ е полином на α с коефициенти от K. Редуцираме мономите α^i с $i \geq d$ до полиноми на α от степени $\leq d-1$ с коефициенти от K и получаваме $\frac{g(\alpha)}{h(\alpha)} \in K[\alpha]^{(d)}$.

Твърдение 1.17. *Следните условия са еквивалентни за разширението $F \supset K$:*
(i) $[F : K] = n < \infty$;
(ii) $F = K(a_1, \dots a_m) \supset K$ е крайно породено и алгебрично над K;
(iii) $F = K(a_1, \dots, a_m) \supset K$ е крайно породено разширение на K чрез алгебрични над K елементи $a_1, \dots, a_m$.

Доказателство: $(i) \Rightarrow (ii)$ Ако $[F : K] = n$, то за $\forall a \in F$ мономите $1, a, \dots, a^n \in F$ са линейно зависими над K и a е алгебричен над K. Това означава, че разширението $F \supset K$ е алгебрично. За произволен базис $f_1, \dots, f_n$ на F над K е в сила

$$F = Kf_1 + \dots + Kf_n \subseteq K(f_1, \dots, f_n) \subseteq F,$$

откъдето $F = K(f_1, \dots, f_n)$ е крайнопородено разширение на K.
Импликацията $(ii) \Rightarrow (iii)$ следва от определението за алгебрично разширение $F \supset K$.
$(iii) \Rightarrow (i)$ Нека $f = K(a_1, \dots, a_m)$ и a_i са алгебрични над K елементи с минимални полиноми $f_i(x) \in K[x] \setminus K$ от степени $\deg(f_i) = d_i \in \mathbb{N}$ за $\forall 1 \leq i \leq n$. Тогава редицата от разширения

$$K \subset K(a_1) \subset \dots \subset K(a_1, \dots, a_{i-1}) \subset K(a_1, \dots, a_{i-1}, a_i) \subset \dots \subset K(a_1, \dots, a_m)$$

дава равенството на степените

$$[K(a_1, \dots, a_m) : K] = \prod_{i=1}^{m} [K(a_1, \dots, a_{i-1}, a_i) : K(a_1, \dots, a_{i-1})].$$

Елементите a_i са алгебрични над $K(a_1, \dots, a_{i-1})$ в качеството си на корени на полиномите $f_i(x) \in K(a_1, \dots, a_{i-1})[x] \setminus K(a_1, \dots, a_{i-1})$. Минималните полиноми $g_i(x) \in K(a_1, \dots, a_{i-1})[x] \setminus K(a_1, \dots, a_{i-1})$ на a_i над $K(a_1, \dots, a_{i-1})$ делят $f_i(x)$, така че $[K(a_1, \dots, a_{i-1}, a_i) : K(a_1, \dots, a_{i-1})] = \deg(g_i) \leq \deg(f_i) = [K(a_i) : K]$ и $[K(a_1, \dots, a_m) : K] \leq \prod_{i=1}^{m} [K(a_i) : K] < \infty$, Q.E.D.
Съществуват алгебрични разширения $E \supset K$, които не са крайни. Такива полета E са безкрайно породени над K.

3. Поле на разлагане на полином

Лема 1.18. *Ако полиномът $p(x) \in K[x] \setminus K$ с коефициенти от поле K е неразложим над K, то фактор-пръстенът*

$$F_1 = K[x]/\langle p\rangle \left(K + \langle p\rangle/\langle p\rangle\right)[x+\langle p\rangle] \simeq \left(K/K \cap \langle p\rangle\right)[x+\langle p\rangle] = K[x+\langle p\rangle] = K(x+\langle p\rangle$$

на $K[x]$ по главния идеал $\langle p\rangle$, породен от p е разширението на полето K чрез корена $x + \langle p\rangle$ на $p(x)$.

Тази лема се изучава в задължителния курс по Висша алгебра или Алгебра 2. Ще напомним накратко идеята за доказателство. Преди всичко, F_1 е комутативен пръстен с единица. Произволен представител $g(x) \in K[x]$ на ненулев елемент $g(x) + \langle p\rangle \neq \langle p\rangle$ е взаимно прост с $p(x)$, защото $p(x)$ е неразложим над K и $p(x)$ не дели $g(x)$. Съгласно тъждеството на Безу съществуват $u(x), v(x) \in K[x]$, така че $g(x)u(x) + p(x)v(x) = 1$. В резултат, $(g(x) + \langle p\rangle)(u(x) + \langle p\rangle) = 1 + \langle p\rangle$ и $(g(x) + \langle p\rangle)^{-1} = u(x) + \langle p\rangle \in F_1$ е обратният на $g(x) + \langle p\rangle$.

Лема 1.19. *За произволен полином $f(x) \in K[x] \setminus K$ съществува разширение $F \supset K$, над което $f(x)$ се разлага в линейни множители.*

Полиномът $f(x)$ се разлага в произведение $f(x) = p_1(x)^{a_1} \dots p_m(x)^{a_m}$ на неразложими над K множители $p_i(x) \in K[x]$ в естествени степени a_i. Факторпръстенът $F_1 = K[x]/\langle p_1 \rangle$ е разширение на K, в което $p_1(x)$ има корен $\alpha_1 = x + \langle p_1 \rangle$. Полиномът $f(x) \in K[x] \subseteq F_1[x]$ с корен $\alpha_1 \in F_1$ се разлага над F_1 в произведение

$$f(x) = (x - \alpha_1) f_1(x)$$

с $f_1(x) \in F_1[x]$ от степен $\deg(f_1) = \deg(f) - 1$. С индукция по степента $\deg(f)$ на $f(x) \in K[x] \setminus K$, ако $f_1(x) = \prod_{i=2}^{\deg(f)} (x - \alpha_i)$ за $\alpha_2, \dots, \alpha_{\deg(f)}$ от подходящо разширение $F \supseteq F_1$, то

$$(x) = \prod_{i=1}^{\deg(f)} (x - \alpha_i)$$

се разлага в линейни множители над F.

Определение 1.20. *Ако полиномът $f(x) \in K[x] \setminus K$ има корени $\alpha_1, \dots, \alpha_n$ в подходящо разширение $F \supseteq K$, то крайно породеното разширение*

$$K \subseteq K(\alpha_1, \dots, \alpha_n) \subseteq F$$

се нарича поле на разлагане на $f(x)$ над K.

Твърдение 1.21. *Нека $K(\alpha_1, \dots, \alpha_n)$ и $K(\alpha'_1, \dots, \alpha'_n)$ са полета на разлагане на $f(x)$ над K. Тогава съществува изоморфизъм на пръстени*

$$\varphi : K(\alpha_1, \dots, \alpha_n) \longrightarrow K(\alpha'_1, \dots \alpha'_n),$$

който се огранича̧ва до тъждественото изображение на K.

Идея за доказателство: Първо ще установим, че тъждественото влагане $\varphi : K \to K(\alpha'_1, \dots, \alpha'_n)$ се продължава до хомоморфизъм на пръстени $\varphi : K(\alpha_1, \dots, \alpha_n) \to K(\alpha'_1, \dots, \alpha'_n)$ на алгебричното разширение $K(\alpha_1, \dots, \alpha_n)$ на K. За да приложим Лемата на Цорн да разгледаме фамилията $\{(F_\nu, \varphi_\nu)\}_{\nu \in S}$ от полета $K \subset F_\nu \subseteq K(\alpha_1, \dots, \alpha_n)$, за които съществуват хомоморфизми на пръстени $\varphi_\nu : F_\nu \to K(\alpha'_1, \dots, \alpha'_n)$, продължаващи $\varphi_\nu|_K = \mathrm{Id}_K$. Въвеждаме частична наредба $(F_\nu, \varphi_\nu) \geq (F_\mu, \varphi_\mu)$, ако F_μ е подполе на F_ν и $\varphi_\nu|_{F_\mu} = \varphi_\mu$. Тогава всяко линейно наредено подмножество $\{(F_i, \varphi_i)\}_{i \in I} \subseteq \{(F_\nu, \varphi_\nu)\}_{\nu \in S}$ има горна граница $(F_\infty = \cup_{i \in I} F_i, \varphi_\infty)$ с $\varphi_\infty|_{F_i} = \varphi_i$ за $\forall i \in I$. Причина за това е, че за произволни $a, b \in F_\infty$ с $a \in F_i$, $b \in F_j \setminus \{0\}$ е в сила $a, b \in F_{\max(i,j)}$, а оттам и $a - b, \frac{a}{b} \in F_{\max(i,j)} \subseteq F_\infty$. Това доказва, че F_∞ е подполе на $K(\alpha_1, \dots, \alpha_n)$, съдържащо K. Хомоморфизмът $\varphi_\infty : F_\infty \to K(\alpha'_1, \dots, \alpha'_n)$ е коректно определен, защото за произволни $i \neq j$ от I е в сила условие за съгласуваност $\varphi_{\max(i,j)}|_{F_{\min(i,j)}} = \varphi_{\min(i,j)}$, заложено в определението на въведената частична наредба. Прилагаме Лемата на Цорн и получаваме съществуването на максимален елемент (E, φ_E) в разглежданата фамилия.
Ако $E \subsetneq K(\alpha_1, \dots, \alpha_n)$ е собствено подполе то съществува корен α_n на $f(x)$ извън E и простото алгебрично разширение $E(\alpha_n) = E[\alpha_n]$ е от степен $[E(\alpha_n) : E] = d > 1$. Изображението

$$\varphi : E[\alpha_n] \longrightarrow K(\alpha'_1, \dots, \alpha'_n),$$

$$\varphi\left(\sum_{i=0}^{d-1} c_i \alpha_n^i\right) = \sum_{i=0}^{d-1} \varphi_E(c_i)(\alpha'_n)^i \quad \text{за} \quad \forall c_i \in E$$

е хомоморфизъм на пръстени, продължаващ $\varphi_E : E \to K(\alpha'_1, \dots, \alpha'_n)$. Това противоречи на максималността на (E, φ_E) и доказва, че $E = K(\alpha_1, \dots, \alpha_n)$.

Нетъждествено нулевият хомоморфизъм $\varphi : K(\alpha_1, \ldots, \alpha_n) \to K(\alpha'_1, \ldots, \alpha'_n)$ е влагане, защото $K(\alpha_1, \ldots, \alpha_n)$ е поле.
Твърдим, че $K(\alpha_1, \ldots, \alpha_{i-1}, \alpha_i) = K(\alpha_1, \ldots, \alpha_{i-1})(\alpha_i)$ за всяко $1 \leq i \leq n$. Наистина, произволни $f, g \in K[\alpha_1, \ldots, \alpha_{i-1}, \alpha_i]$ с $g(\alpha_1, \ldots, \alpha_i) \neq 0$ могат да се разглеждат като полиноми $f, g \in K[\alpha_1, \ldots, \alpha_{i-1}][\alpha_i] \subseteq K(\alpha_1, \ldots, \alpha_{i-1})[\alpha_i]$ на α_i с коефициенти от полето $K(\alpha_1, \ldots, \alpha_{i-1})$. Следователно $\frac{f(\alpha_1,\ldots,\alpha_i)}{g(\alpha_1,\ldots,\alpha_i)} \in K(\alpha_1, \ldots, \alpha_{i-1})(\alpha_i)$ и $K(\alpha_1, \ldots, \alpha_{i-1}, \alpha_i) \subseteq K(\alpha_1, \ldots, \alpha_{i-1})(\alpha_i)$. Обратно,

$$K(\alpha_1, \ldots, \alpha_{i-1})(\alpha_i) \subseteq K(\alpha_1, \ldots, \alpha_{i-1}, \alpha_i),$$

защото $K(\alpha_1, \ldots, \alpha_{i-1}) \subset K(\alpha_1, \ldots, \alpha_{i-1}, \alpha_i)$, $\alpha_i \in K(\alpha_1, \ldots, \alpha_{i-1}, \alpha_i)$ и полето $K(\alpha_1, \ldots, \alpha_{i-1}, \alpha_i)$ е затворено относно събиране, изваждане, умножение и деление с ненулев елемент.
Ако $\alpha, \ldots, \alpha_n$ са алгебрични над K, то разширението

$$K(\alpha_1, \ldots, \alpha_n) = K[\alpha_1, \ldots, \alpha_n]$$

на K чрез $\alpha_1, \ldots, \alpha_n$ се изчерпва от полиномите на $\alpha_1, \ldots, \alpha_n$ с коефициенти от K. С индукция по $1 \leq i \leq n$ ще проверим, че $K(\alpha_1, \ldots, \alpha_i) = K[\alpha_1, \ldots, \alpha_i]$. Съгласно Твърдение 1.13 (iv), $K(\alpha_1) = K[\alpha_1]$ да алгебричния над K елемент α_1. Допускането $K(\alpha_1, \ldots, \alpha_{i-1}) = K[\alpha_1, \ldots, \alpha_i]$ води до

$$K(\alpha_1, \ldots, \alpha_{i-1}, \alpha_i) = K(\alpha_1, \ldots, \alpha_{i-1})(\alpha) = K[\alpha_1, \ldots, \alpha_{i-1}](\alpha_i).$$

Алгебричният над K елемент α_i е алгебричен и над $K(\alpha_1, \ldots, \alpha_{i-1})$, така че $K[\alpha_1, \ldots, \alpha_{i-1}](\alpha_i) = K[\alpha_1, \ldots, \alpha_{i-1}][\alpha_i] = K[\alpha_1, \ldots, \alpha_{i-1}, \alpha_i]$.
Образът $\mathrm{im}\varphi = \varphi(K(\alpha_1, \ldots, \alpha_n)) = \varphi(K[\alpha_1, \ldots, \alpha_n])$ е подпръстен на полето $K(\alpha'_1, \ldots, \alpha'_n) = K[\alpha'_1, \ldots, \alpha'_n]$, съдържащ полето K. Достатъчно е да проверим, че $\alpha'_1, \ldots, \alpha'_n \in \mathrm{im}\varphi$, за да получим, че $K[\alpha'_1, \ldots, \alpha'_n]$ се съдържа и съвпада с $\mathrm{im}\varphi$. Това ще докаже, че $\varphi : K(\alpha_1, \ldots, \alpha_n) \to K(\alpha'_1, \ldots, \alpha'_n)$ е изоморфизъм на пръстени. За произволно $1 \leq i \leq n$ действаме с φ върху $f(\alpha_i) = 0_K$ и получаваме $f(\varphi(\alpha_i)) = 0_K$. Следователно $\varphi(\alpha_i) \in K(\alpha'_1, \ldots, \alpha'_n)$ е корен на $f(x)$ и съвпада с някое α'_j. С други думи, φ се ограничава до изображение

$$\varphi : \{\alpha_1, \ldots, \alpha_n\} \longrightarrow \{\alpha'_1, \ldots, \alpha'_n\}.$$

Нека $\alpha_1, \ldots, \alpha_m$ са различните корени на $f(x)$ от $K(\alpha_1, \ldots, \alpha_n)$, а $\alpha'_1, \ldots, \alpha'_\mu$ са различните корени на $f(x)$ от $K(\alpha'_1, \ldots, \alpha'_n)$. Тогава φ се ограничава до изображение

$$\varphi : \{\alpha_1, \ldots, \alpha_m\} \longrightarrow \{\alpha'_1, \ldots, \alpha'_\mu\},$$

чийто образ има m елемента, съгласно взаимната еднозначност на φ върху своя образ. В резултат, $m \leq \mu$. Повтаряме горните разглеждания след замяна на ролите на $K(\alpha_1, \ldots, \alpha_n)$ и $K(\alpha'_1, \ldots, \alpha'_n)$, за да получим $\mu \leq m$. Следователно $\mu = m$ и изображението $\varphi : \{\alpha_1, \ldots, \alpha_m\} \to \{\alpha'_1, \ldots, \alpha'_m\}$ е взаимно еднозначно. В частност, $\alpha'_1, \ldots, \alpha'_m \in \mathrm{im}\varphi$, откъдето $\alpha'_1, \ldots, \alpha'_n \in \mathrm{im}\varphi$, Q.E.D.

4. Класификация на крайните полета и техните подполета

Лема 1.22. *Ако k е поле с q елемента, то простото подполе на k е полето от остатъци $\mathbb{F}_p$ при деление с някакво просто число p и ако $[k : \mathbb{F}_p] = \dim_{\mathbb{F}_p}(k) = n$, то k има $q = p^n$ елемента.*

Доказателство: Ако допуснем, че простото подполе P на $\mathbb{F}_q$ не е изоморфно на $\mathbb{F}_p$ за просто p, то $P \simeq \mathbb{Q}$ е изоморфно на полето на рационалните числа и е безкрайно множество. Това противоречи на крайността на k и доказва, че $P \simeq \mathbb{F}_p$ за някое просто p.
Полето k е линейно пространство над простото си подполе $P \simeq \mathbb{F}_p$. По-точно, за произволни $a, b \in k$ и $\lambda \in P$ имаме коректно определени $a+b \in k$ и $\lambda a \in k$. Освен

това, $(k,+)$ е абелева група. Дистрибутивният закон за събиране и умножение в k се ограничава до дистрибутивните закони над скаларен и векторен множител. Асоциативността на умножението в k дава $(\lambda\mu)a = \lambda(\mu a)$ за $\forall\lambda,\mu \in P$, $\forall a \in k$. Накрая, $1a = a$ за единизата 1 на P и k и за всеки елемент $a \in k$.
Ако допуснем, че полето k е безкрайномерно линеейно пространство над P, то за всяко естествено число N съществуват N линейно независими над P вектора $a_1, \ldots, a_N \in k$. За $N > |k|$ получаваме противоречие и доказваме, че k е крайномерно линейно пространство над $P \simeq \mathbb{F}_p$. Ако размерността на k над $\mathbb{F}_p$ е $[k : \mathbb{F}_p] = n$, то линейното пространство k над $\mathbb{F}_p$ е изоморфно на пространството $\mathbb{F}_p^n$ на наредените n-торки с елементи от $\mathbb{F}_p$ и броят на елементите му е

$$q = |k| = |\mathbb{F}_p^n| = p^n,$$

Q.E.D.

Теорема 1. *За всяко просто число p и за всяко естествено число n съществува единствено с точност до изоморфизъм поле $\mathbb{F}_q$ с $q = p^n$ елемента, което е поле на разлагане на полинома $x^q - x$ над простото подполе $\mathbb{F}_p$ на $\mathbb{F}_q$ и се изчерпва с кореният на $x^q - x$.*

Доказателство: Да напомним, че в поле с проста характеристика p е в сила биномната формула

$$(a \pm b)^p = a^p \pm b^p,$$

защото биномните коефициенти

$$\binom{p}{i} = \frac{p(p-1)\ldots(p-i+1)}{1.2\ldots i}$$

с $1 \le i \le p-1$ се делят на p. С индукция по $k \in \mathbb{N}$, оттук следва, че

$$(a \pm b)^{p^k} = a^{p^k} \pm b^{p^k}.$$

Нека $\mathbb{F}_p(\alpha_1, \ldots, \alpha_q)$ е полето на разлагане на $x^q - x$ над $\mathbb{F}_p$, а $R = \{\alpha_1, \ldots, \alpha_q\} \subseteq \mathbb{F}_p(\alpha_1, \ldots, \alpha_q)$ е подмножеството на корените на $x^q - x = 0$ от $\mathbb{F}_p(\alpha_1, \ldots, \alpha_q)$. За произволни $\alpha, \beta \in R$, $\beta \neq 0$ са в сила

$$(\alpha - \beta)^q = \alpha^q - \beta^q = \alpha - \beta \quad \text{и} \quad \left(\frac{\alpha}{\beta}\right)^q = \frac{\alpha^q}{\beta^q} = \frac{\alpha}{\beta}.$$

Следователно R е подполе на $\mathbb{F}_p(\alpha_1, \ldots, \alpha_q)$. Твърдим, че множеството R се състои от q различни елемента. Наистина, формалната производна $(x^q - x)' = qx^{q-1} - 1 = -1$ няма общ корен с $x^q - x$, така че $x^q - x$ няма кратни корени и $\alpha_1, \ldots, \alpha_q$ са две по две различни.
За да докажем съвпадението $\mathbb{F}_p(\alpha_1, \ldots, \alpha_q) = R$ да отбележим очевидното вкрючване $R \subseteq \mathbb{F}_p(\alpha_1, \ldots, \alpha_q)$. Твърдим, че полето $R = \{\alpha_1, \ldots, \alpha_q\}$ съдържа простото поле $\mathbb{F}_p$ с p елемента. За целта използваме, че за всяко $a \in \mathbb{F}_p$ е в сила $a^p = a$. С индукция по $1 \le i \le n$ проверяваме, че $a^{p^i} = a$. Поточно, $a^{p^i} = (a^{p^{i-1}})^p = a^p = a$. Подполето R на $\mathbb{F}_p(\alpha_1, \ldots, \alpha_q)$ съдържа простото подполе $\mathbb{F}_p$ и елементите $\alpha_1, \ldots, \alpha_q$. Следователно $R \supseteq \mathbb{F}_p(\alpha_1, \ldots, \alpha_q)$ и $R = \mathbb{F}_p(\alpha_1, \ldots, \alpha_q)$. В резултат, $\mathbb{F}_p(\alpha_1, \ldots, \alpha_q) = \{\alpha_1, \ldots, \alpha_q)$ е поле с q елемента.
Остава да докажем, че произволно поле k с $q = p^n$ елемента е изоморфно на $\mathbb{F}_p(\alpha_1, \ldots, \alpha_q) = R$. За целта е достатъчно да установим, че k е поле на разлагане на $x^q - x$ над $\mathbb{F}_p$. Наистина, произволен ненулев елемент β на поле k с q елемента изпълнява равенството $\beta^{q-1} = 1_k$, защото редът на $\beta \in k^*$ дели реда $q-1$ на мултипликативната група k^* на k. Умножавайки почленно с β получаваме, че всички елементи $\gamma \in k$ са корени на полинома $x^q - x \in \mathbb{F}_p[x]$ с коефициенти от простото подполе $\mathbb{F}_p$ на k. С други думи, съществува поле на разлагане

$\mathbb{F}_p(\alpha'_1,\ldots,\alpha'_q)$ на x^q-x над $\mathbb{F}_p$, така че $k\subseteq\{\alpha'_1,\ldots,\alpha'_q\}=\mathbb{F}_p(\alpha'_1,\ldots,\alpha'_q)$. Понеже k има q елемента, оттук следва $k=\{\alpha'_1,\ldots,\alpha'_q\}\simeq\mathbb{F}_p(\alpha_1,\ldots,\alpha_q)$, Q.E.D.

Следствие 1.23. *Полето $\mathbb{F}_{q^m}$ е подполе на $\mathbb{F}_{q^n}$ тогава и само тогава, когато m дели n.*

Доказателство: Нека m дели n или $n=mk$ за някое $k\in\mathbb{N}$. Тогава всеки елемент $\alpha\in\mathbb{F}_{q^m}$ изпълнява равенството $\alpha^{q^m}=\alpha$. Чрез повдигане в степен q^m получаваме $\alpha^{q^{2m}}=\left(\alpha^{q^m}\right)^{q^m}=\alpha^{q^m}=\alpha$. С индукция по $i\in\mathbb{N}$ оттук следва $\alpha^{q^{im}}=\alpha$. В частност, $\alpha^{q^n}=\alpha^{q^{km}}=\alpha$ и $\alpha\in\mathbb{F}_{q^n}$, $\mathbb{F}_{q^m}\subseteq\mathbb{F}_{q^n}$.
Обратно, ако $\mathbb{F}_{q^m}$ е подполе на $\mathbb{F}_{q^n}$, то веригата $\mathbb{F}_q\subseteq\mathbb{F}_{q^m}\subseteq\mathbb{F}_{q^n}$ от крайни разширения има степени

$$n=[\mathbb{F}_{q^n}:\mathbb{F}_q]=[\mathbb{F}_{q^n}:\mathbb{F}_{q^m}][\mathbb{F}_{q^m}:\mathbb{F}_q]=[\mathbb{F}_{q^n}:\mathbb{F}_{q^m}]m.$$

Следователно m дели n и $[\mathbb{F}_{q^n}:\mathbb{F}_{q^m}]=\frac{n}{m}$, Q.E.D.

5. Структурна теорема за крайно породените абелеви групи. Цикличност на мултипликативната група на крайно поле.

Ще изведем цикличността на мултипликативната група $\mathbb{F}_q^*$ на крайно поле $\mathbb{F}_q$ от структурната теорема за крайно породените абелеви групи. Същият резултат се получава и от факта, че за произволни $a,b\in\mathbb{F}_q^*$ съществува елемент $c\in\mathbb{F}_q^*$, чийто ред е най-малкото общо кратно на редовете на a и b.
Да напомним еквивалентността на понятията абелева група $(G,+)$ и $\mathbb{Z}$-модул G (т.е. линейно пространство G над $\mathbb{Z}$). От една страна, всеки модул е абелева група относно събирането. Всяка абелева група има естествено зададено умножение с $z\in\mathbb{Z}$. По-точно, $0g=0_G$ за $0\in\mathbb{Z}$, $\forall g\in G$ и неутралния елемент $0_G\in(G,+)$. Ако $n\in\mathbb{N}$ и $g\in G$, то $ng=g+\ldots+g$ е n-кратната сума на g със себе си, а $(-n)g=-(ng)$ е противоположният елемент на $ng\in G$.
Ако анулаторът $\mathrm{Ann}(g)=\{z\in\mathbb{Z}\ \mid\ zg=0\}$ на $g\in G$ не е нулев, то $\mathrm{Ann}(g)$ е идеал в $\mathbb{Z}$ и $\mathrm{Ann}(g)=n\mathbb{Z}$ за някое естествено $n\in\mathbb{N}$. Тогава $\psi:\mathbb{Z}\longrightarrow\mathbb{Z}g$, $\psi(z)=zg$ е епиморфизъм на $\mathbb{Z}$-модули с ядро $\ker\psi=\mathrm{Ann}(g)$, така че главният $\mathbb{Z}$-модул $\mathbb{Z}g\simeq\mathbb{Z}/n\mathbb{Z}=\mathbb{Z}_n$ е изоморфен на адитивната група $(\mathbb{Z}_n,+)$ на остатъците при деление с n.

Теорема 2. *За всяка крайно породена абелева група G съществуват естествени $d_1,\ldots,d_t$ и неотрицателно цяло r, така че*

$$G\simeq\mathbb{Z}_{d_1}\times\mathbb{Z}_{d_2}\times\ldots\times\mathbb{Z}_{d_t}\times\mathbb{Z}^r$$

и d_i дели d_{i+1} за всички $1\leq i\leq t-1$. (Ако $G\simeq\mathbb{Z}^r$, то казваме, че G е свободна абелева група от ранг r.)

Доказателство: Всяка крайно породена абелева група G има представяне с пораждащи $x_1,\ldots,x_g$ и съотношения $\sum\limits_{j=1}^{g}a_{ij}x_j=0$, $1\leq i\leq s$, където a_{ij} са цели числа. Без ограничение на общността считаме, че системата пораждащи е минимална. Образуваме матрицата $A=(a_{ij})_{1\leq i\leq s,\ \ 1\leq j\leq g}\in M_{s,g}(\mathbb{Z})$ и забелязваме, че групата G не се променя под действие на следните елементарни преобразувания върху съотношенията на G или редовете на A :
(i) умножение на j-ти ред със $z\in\mathbb{Z}$ и прибавяне към i-ти ред;
(ii) умножение на ред с (-1);
(iii) транспозиция или размяна на два реда.
От друга страна, следните операции върху пораждащите $x_1,\ldots,x_g$ на G или стълбовете на A не променят G:
(iv) замяна на x_j с x_j+zx_i, където $z\in\mathbb{Z}$;

(v) замяна на x_i с $-x_i$;
(vi) транспозиция на x_i с x_j.
В множеството на ненулевите елементи на матриците, получени от A чрез операциите (i)-(vi) избираме цяло число d_1 с минимална абсолютна стойност. След евентуална замяна на d_1 с $-d_1$, последвана от разместване на редовете и стълбовете на съответната матрица A, считаме, че $d_1 \in \mathbb{N}$ и се намира в първи ред и първи стълб. Съгласно минималността на d_1, всички други елементи от първи ред и първи стълб на A се делят на d_1 и можем да ги анулираме с подходящи елементарни преобразувания. По-точно, ако $a_{1i} = d_1 q_{1i} + r_{1i}$ е делението на $a_{1i} \in \mathbb{Z}$ с $d_1 \in \mathbb{N}$ с частно q_{1i} и остатък $r_{1i} \in \mathbb{Z}$, $0 \leq r_{1i} \leq d_1 - 1$, то умножаваме първия стълб с $(-q_{1i})$ и го прибавяме към i-ти стълб, за да получим r_{1i} на място $(1, i)$. Допускането $r_{1i} \neq 0$ води до противоречие с минималността на $|d_1|$. По този начин достигаме до

$$A = \begin{pmatrix} d_1 & 0 & \dots & 0 \\ 0 & a_{22} & \dots & a_{2g} \\ \dots & \dots & \dots & \dots \\ 0 & a_{s2} & \dots & a_{sg} \end{pmatrix} \in \mathbb{Z}_{r \times g} \tag{1.1}$$

Твърдим, че d_1 дели всички елементи a_{ij} с $2 \leq i \leq s$, $2 \leq j \leq g$ от тази матрица. Например, ако $a_{ij} = d_1 q_{ij} + r_{ij}$ е делението на $a_{ij} \in \mathbb{Z}$ с $i \geq 2$, $j \geq 2$ на d_1 с частно $q_{ij} \in \mathbb{Z}$ и остатък $r_{ij} \in \mathbb{Z}$, $0 \leq r_{ij} \leq d_1 - 1$, то прибавяме първи стълб към j-ти стълб, умножаваме първи ред с $(-q_{ij})$ и прибавяме към i-ти ред. Това води до поява на r_{ij} на място (i, j). Допускането $r_{ij} > 0$ противоречи на избора на $d_1 \in \mathbb{Z} \setminus \{0\}$ с минимална абсолютна стойност $|d_1|$ и доказва, че d_1 дели a_{ij} за всички $2 \leq i \leq r$, $2 \leq j \leq g$. В резултат, d_1 се оказва най-голям общ делител на елементите на матрицата (1.1). Понеже операциите (i)-(vi) не променят най-големия общ делител d на елементите на първоначалната матрица A, оттук следва, че $d = d_1$. Към матрицата с $r-1$ реда и $g-1$ стълба, получена от (1.1) след премахване на първи ред и първи стълб, прилагаме аналогични разсъждения, докато сведем A към вида

$$A = \begin{pmatrix} d_1 & 0 & \dots & 0 & 0 & \dots & 0 \\ 0 & d_2 & \dots & 0 & 0 & \dots & 0 \\ 0 & 0 & \dots & d_t & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 0 & 0 & \dots & 0 \end{pmatrix}.$$

Премахваме нулевите редове, защото те не налагат съществени съотношения и разпознаваме $\mathbb{Z}$-модула $\mathbb{Z}_{d_1} \times \ldots \times \mathbb{Z}_{d_t} \times \mathbb{Z}^r$ с $r = g - t$, отговарящ на такава матрица от коефициенти на съотношенията, Q.E.D.
В частност, ако G е крайна абелева група, то $G \simeq \mathbb{Z}_{d_1} \times \ldots \times \mathbb{Z}_{d_t}$ и d_i делят d_t за всички $1 \leq i \leq t$. Следователно всеки елемент $g = (g_1, \ldots, g_t) \in G$ изпълнява равенството $g^{d_t} = e_G$, където e_G е неутралният елемент на G.

Твърдение 1.24. *Мултипликативната група $\mathbb{F}_q^*$ на крайно поле $\mathbb{F}_q$ е циклична.*

Доказателство: Да допуснем, че мултипликативната група $\mathbb{F}_q^*$ е изоморфна на директно произведение $\mathbb{Z}_{d_1} \times \ldots \times \mathbb{Z}_{d_{t-1}} \times \mathbb{Z}_{d_t}$ с $t \geq 2$ множителя и $d_i \geq 2$ делящи d_{i+1} за всички $1 \leq i \leq t-1$. Тогава $\mathbb{F}_q^*$ се състои от корени на полинома $f(x) = x^{d_t} - 1_{\mathbb{F}_p} \in \mathbb{F}_p[x]$ с коефициенти от простото подполе $\mathbb{F}_p$ на $\mathbb{F}_q$. Понеже $f(x)$ има най-много d_t корена в кое и да е разширение на $\mathbb{F}_p$, оттук следва неравенството $d_1 \ldots d_{t-1} d_t = |\mathbb{F}_q^*| \leq d_t$. В резултат, $d_1 \ldots d_{t-1} \leq 1$ за

естествените числа $d_i \geq 2$ е противоречие, доказващо изоморфизма на групи $\mathbb{F}_q^* \simeq (\mathbb{Z}_{q-1}, +)$, Q.E.D.

6. Циклотомични полиноми и аритметика в крайно поле

Елементите от ред n в мултипликативната група $\mathbb{C}^*$ на полето $\mathbb{C}$ на комплексните числа се наричат примитивни корени на единицата. Това са числата $\omega_n^k = \cos\left(\frac{2k\pi}{n}\right) + i\sin\left(\frac{2k\pi}{n}\right)$, където k пробягва мултипликативната група $\mathbb{Z}_n^*$ на остатъците при деление с n. Ако $n = p_1^{a_1} \dots p_s^{a_s}$ е разлагането на $n \in \mathbb{N}$ в прости множители p_i, то редът на $\mathbb{Z}_n^*$ или броят на взаимно простите с n остатъци при деление с n е равен на функцията на Euler

$$\varphi(n) = p_1^{a_1-1}(p_1 - 1) \dots p_s^{a_s-1}(p_s - 1).$$

Полиномът

$$C_n(x) := \prod_{k \in \mathbb{Z}_n^*} (x - \omega_n^k)$$

със старши коефициент 1, чиито корени са примитивните n-ти корени на единицата се нарича n-ти циклотомичен полином. Ясно е, че

$$C_n(x) = \frac{x^n - 1}{\prod\limits_{m/n, m<n} C_m(x)},$$

където m пробягва естествените делители m на n, които са строго по-малки от n. С индукция по n оттук следва, че $C_n(x)$ е полином с цели коефициенти, защото частното на полиноми с цели коефициенти и старши коефициенти 1 е полином с цели коефициенти и старши коефициент 1. Ако

$$C_n(x) = x^{\varphi(n)} + a_{\varphi(n)-1}x^{\varphi(n)-1} + \ldots + a_1 x + a_0 \in \mathbb{Z}[x],$$

то за всяко естествено число N редукцията на $C_n(x)$ по модул N е полиномът

$$C_n(\mathrm{mod}N) := x^{\varphi(n)} + \ldots + [a_1(\mathrm{mod}N)]x + [a_0(\mathrm{mod}N)] \in \mathbb{Z}_N[x],$$

чиито коефицинети са съответните остатъци при деление с N.

Следствие 1.25. *Ако α е пораждащ на мултипликативната група $\mathbb{F}_{p^n}^*$ на крайно поле $\mathbb{F}_{p^n}$, то*

$$\mathbb{F}_{p^n} = \mathbb{F}_p(\alpha) = \mathbb{F}_p[\alpha]$$

се поражда от α над простото си подполе $\mathbb{F}_p$.
Минималният полином $f(x) \in \mathbb{F}_p[x] \setminus \mathbb{F}_p$ на α над $\mathbb{F}_p$ е от степен n.
Полиномът $f(x)$ дели редукцията $C_{p^n-1}(x)(\mathrm{mod}p) \in \mathbb{F}_p[x]$ на циклотомичния полином $C_{p^n-1}(x) \in \mathbb{Z}[x]$ по модул p.
Ако $C_{p^n-1}(x)(\mathrm{mod}p) = f_1(x) \dots f_k(x)$ е разлагането на $C_{p^n-1}(x)(\mathrm{mod}p)$ в неразложими над $\mathbb{F}_p$ множители $f_i(x) \in \mathbb{F}_p[x]$ със страши коефициенти 1, то $\deg(f_i) = n$ за всяко $1 \leq i \leq k$.

Доказателство: От $\mathbb{F}_{p^n} = \{0, \alpha, \dots, \alpha^{p^n-2}, \alpha^{p^n-1} = 1\}$ е ясно, че $\mathbb{F}_{p^n} = \mathbb{F}_p(\alpha)$. Степента

$$n = [\mathbb{F}_{p^n} : \mathbb{F}_p] = [\mathbb{F}_p(\alpha) : \mathbb{F}_p] = \deg(f)$$

съгласно Твърдение 1.13 (v).
Достатъчно е да проверим, че $C_{p^n-1}(\mathrm{mod}p)$ се анулира в α, за да приложим Твърдение 1.13 (i) и да получим, че полиномът $C_{p^n-1}(\mathrm{mod}p) \in \langle f(x) \rangle$. Понеже $\alpha \in \mathbb{F}_{p^n}^*$ е от ред $p^n - 1$, за всеки делител m на $p^n - 1$, по-малък от $p^n - 1$ имаме $C_m(\mathrm{mod}p)(\alpha) \in \mathbb{F}_{p^n}^*$, а $\alpha^{p^n-1} - 1_{\mathbb{F}_{p^n}} = 0_{\mathbb{F}_{p^n}}$. Следователно

$$C_{p^n-1}(\mathrm{mod}p)(\alpha) = \frac{\alpha^{p^n-1} - 1_{\mathbb{F}_{p^n}}}{\prod\limits_{m/p^n-1, m<p^n-1} C_m(\mathrm{mod}p)(\alpha)} = 0_{\mathbb{F}_{p^n}}$$

и минималният полином $f(x) \in \mathbb{F}_p[x] \setminus \mathbb{F}_p$ на α над $\mathbb{F}_p$ дели полинома

$$C_{p^n-1}(\mathrm{mod}p)(x) \in \mathbb{F}_p[x].$$

За да докажем, че всеки неразложим над $\mathbb{F}_p$ множител $f_i(x)$ на $C_{p^n-1}(x)(\mathrm{mod}p)$ е от степен n, забелязваме, че всеки корен α на $C_{p^n-1}(x)(\mathrm{mod}p)$ в подходящо разширение $E \supset \mathbb{F}_p$ е елемент $\alpha \in E^*$ от ред p^n-1 на мултипликативната група E^* на E. Наистина, от

$$\left[\prod_{m/p^n-1, m<p^n-1} C_m(x)(\mathrm{mod}p)\right] C_{p^n-1}(x)(\mathrm{mod}p) = (x^{p^n-1}-1)(\mathrm{mod}p) \in \mathbb{F}_p[x]$$

следва, че α е корен на $(x^{p^n-1}-1)(\mathrm{mod}p)$. Следователно редът r на $\alpha \in E^*$ дели p^n-1. Ако допуснем, че $r < p^n-1$, то α е корен както на

$$\prod_{m/p^n-1, m<p^n-1} C_m(x)(\mathrm{mod}p),$$

така и на $C_{p^n-1}(x)(\mathrm{mod}p)$. Оттук, α е кратен корен на $(x^{p^n-1}-1)(\mathrm{mod}p)$ и трябва да анулира формалната производна $(p^n-1)x^{p^n-2}(\mathrm{mod}p) = -x^{p^n-2}(\mathrm{mod}p)$ на $(x^{p^n-1}-1)(\mathrm{mod}p)$. Противоречието доказва, че $\alpha \in E^*$ е от ред p^n-1.
За произволен неразложим над $\mathbb{F}_p$ множител $f_i(x) \in \mathbb{F}_p[x]$ на $C_{p^n-1}(\mathrm{mod}p)$ със стапши коефициент 1 да изберем корен α на $f_i(x)$ в подходящо разширение $F \supset \mathbb{F}_p$. Тогава $f_i(x)$ съвпада с минималния полином на α над $\mathbb{F}_p$ поради анулирането си в α, неразложимостта си над $\mathbb{F}_p$ и това, че има старши коефициент 1. Следователно $\deg(f_i) = [\mathbb{F}_p(\alpha) : \mathbb{F}_p]$. Нека $\langle\alpha\rangle$ е цикличната подгрупа на E^*, породена от α. Съгласно $\langle\alpha\rangle \cup \{0\} \subseteq \mathbb{F}_p(\alpha)$, полето $\mathbb{F}_p(\alpha)$ има поне $|\mathbb{F}_p(\alpha)| \geq p^n$ елемента. От дурга страна, $\mathbb{F}_p(\alpha) \subseteq \mathbb{F}_{p^n}$, защото $\mathbb{F}_p \subset \mathbb{F}_{p^n}$ и $\alpha^{p^n} = \alpha$. Следователно $|\mathbb{F}_p(\alpha)| \leq p^n$ и $|\mathbb{F}_p(\alpha)| = p^n$. Това доказва, че $\mathbb{F}_p(\alpha) = \mathbb{F}_{p^n}$ и $\deg(f_i) = [\mathbb{F}_{p^n} : \mathbb{F}_p] = n$, Q.E.D.
За да извършваме аритметични действия (събиране, изваждане, умножение и деление с ненулев елемент) в крайно поле $\mathbb{F}_{p^n}$ разлагаме редукцията

$$C_{p^n-1}(x)(\mathrm{mod}\, p) = f_1(x) \ldots f_k(x)$$

на циклотомичния полином $C_{p^n-1}(x) \in \mathbb{Z}[x]$ в произведение на неразложими над $\mathbb{F}_p$ множители $f_i(x) \in \mathbb{F}_p[x]$ със старши коефициенти 1. Избираме множител

$$f_i(x) = x^n + c_{n-1}x^{n-1} + \ldots + c_1x + c_0 \in \mathbb{F}_p,$$

корен α на $f_i(x)$ в подходящо разширение на $\mathbb{F}_p$ и отъждествяваме полето $\mathbb{F}_{p^n} = \mathbb{F}_p(\alpha)$ с разширението на $\mathbb{F}_p$ чрез α. Понеже α е алгебричен над $\mathbb{F}_p$ от степен n, полето $\mathbb{F}_p(\alpha) = \mathbb{F}_p[\alpha] = \mathbb{F}_p[\alpha]^{(n)}$ се състои от полиноми на α от степен, не по-голяма от $n-1$ със коефициенти от полето $\mathbb{F}_p$ на остатъците при деление с простото число p. Събирането, изваждането, умножението и делението с ненулев елемент в $\mathbb{F}_p(\alpha)$ са описани след Определение 1.16.

Задача 1.26. *Нека α е пораждащ на мултипликативната група $\mathbb{F}_9^*$ на полето $\mathbb{F}_9$ с 9 елемента. Да се докаже, че минималният полином на α над $\mathbb{F}_3$ е $x^2-x-1=0$ или $x^2+x-1=0$.*

В следващите задачи фиксираме $\mathbb{F}_9 = \mathbb{F}_3(\alpha) = \mathbb{F}_3[\alpha]$ с $\alpha^2 = \alpha + 1$.

Задача 1.27. *За произволно естествено $1 \leq \nu \leq 8$ да разгледаме линейното пространство $V_\nu = \mathbb{F}_9^{(\nu+1)}[x]$ на полиномите на трансцендентна над $\mathbb{F}_9$*

променлива x от степен $\leq \nu$ с коефициенти от $\mathbb{F}_9$. Фиксираме $\mathbb{F}_9 = \mathbb{F}_3(\alpha)$ с $\alpha^2 = \alpha + 1$, точките

$$p_1 = \overline{0} \in \mathbb{F}_3 \subset \mathbb{F}_9, \quad p_2 = \overline{1} \in \mathbb{F}_3 \subset \mathbb{F}_9, \quad p_3 = -\overline{1} \in \mathbb{F}_3 \subset \mathbb{F}_9,$$
$$p_4 = \alpha \in \mathbb{F}_9, \quad p_5 = \alpha + \overline{1} \in \mathbb{F}_9, \quad p_6 = \alpha - \overline{1} \in \mathbb{F}_9,$$
$$p_7 = -\alpha \in \mathbb{F}_9, \quad p_8 = -\alpha + \overline{1} \in \mathbb{F}_9, \quad p_9 = -\alpha - \overline{1} \in \mathbb{F}_9.$$

и $D = \{p_1, \ldots, p_9\}$. Разглеждаме остойностяващото изображение

$$\mathcal{E}_D : V_\nu = \mathbb{F}_9^{(\nu+1)}[x] \longrightarrow \mathbb{F}_9^9,$$
$$\mathcal{E}_D\left(\sum_{i=0}^{\nu} a_i x^i\right) = \left(\sum_{i=0}^{\nu} a_i p_1^i, \ldots, \sum_{i=0}^{\nu} a_i p_9^i\right).$$

(а) Да се провери, че $\mathcal{E}$ е $\mathbb{F}_9$-линейно изображение.
(б) Да се намери размерността на образа $C_{D,\nu} = \mathcal{E}(V_\nu)$.
(в) Да се докаже, че $C_{D,3}$ е максимално отделим код, без да се използва наготово Пример 1.10.

Дуалният код $C_{D,\nu}^*$ на $C_{D,\nu}$ има дължина $n^* = n$ и размерност

$$k^* = \dim_{\mathbb{F}_q}(C_{D,\nu}^*) = n - k.$$

Използвайте наготово съществуването на $\mathbb{F}_q$-линеен изоморфизъм

$$C_{D,\nu}^* \simeq \mathcal{E}_D(V_{n-2-\nu}) = C_{D,n-2-\nu}.$$

Тогава минималното разстояние d^* на $C_{n,\nu}^*$ изпълнява неравенството

$$d^* \geq \nu + 2.$$

Задача 1.28. *Нека $C_{D,3}$ е линейният код от Задача 1.27.*
(а) Да се намерят размерността k^* и минималното разстояние d^* на дуалния код $C_{D,3}^*$ на $C_{D,3}$.
(б) Да се установи дали $C_{D,3}^*$ е максимално отделим код.
(в) Да се провери, че думата $c = (\overline{1}, \ldots, \overline{1}) \in \mathbb{F}_9^9$ принадлежи на кода $C_{D,3}^*$.

Упътване: (в) Използвайте, че всяка пораждаща матрица на $C_{D,3}$ е проверочна матрица на $C_{D,3}^*$. Приложете формулите на Нютон за полинома $x^9 - x = 0$.