Глава 1

Мотивация

Ще нахвърлим накратко някои факти от теория на кодирането и криптографията, които мотивират нашите разглеждания в областта на алгебричната геометрия.

Ако A е крайно множество, то означаваме с A^n множеството на наредените n-торки $(a_1, \ldots, a_n)$ с елементи a_i от A. Всяко подмножество C на A^n се нарича код с дължина n над азбуката A. Обикновено A е крайно поле или краен пръстен. В приложението към настоящия въпрос напомняме класификацията на крайните полета и техните подполета. Ако $A = \mathbb{F}_q$ е крайно поле с $q = p^m$ елемента за някое просто число p и C е подпространство на пространството $\mathbb{F}_q^n$ на наредените n-торки с елементи от $\mathbb{F}_q$, то C се нарича линеен код. Ние ще се занимаваме предимно с линейни кодове над крайни полета. Ако $C \subset \mathbb{F}_q^n$ е линеен код, то размерността k на C се определя като размерността на пространството C над полето $\mathbb{F}_q$. Линейните кодове $C \subset \mathbb{F}_q^n$ с размерност k имат $\mathrm{card}(C) = q^k$ елемента или $k = \log_q(\mathrm{card}(C))$.

За произволно крайно множество A и произволно естествено n, разстоянието на Hamming $d(x, y)$ от $x = (x_1, \ldots, x_n) \in A^n$ до $y = (y_1, \ldots, y_n) \in A^n$ е броят на различните компоненти $x_i \neq y_i$ за $1 \leq i \leq n$.

Лема 1.1. *За произволно крайно множество A и произволно естествено n, разстоянието на Hamming $d : A^n \times A^n \to \{0, 1, \ldots, n\}$ е метрика в A^n.*

Доказателство: Преди всичко, $d(x, y) = d(y, x)$. Твърдим, че за произволни $x, y, z \in A^n$ е в сила неравенството на триъгълника $d(x, z) \leq d(x, y) + d(y, z)$. За целта, нека

$$I = \{1 \leq i \leq n \,|\, x_i \neq y_i\},\ J = \{1 \leq i \leq n \,|\, \leq y_i \neq z_i\} \text{ и } K = \{1 \leq i \leq n \,|\, x_i \neq z_i\}.$$

За всяко $i \in \{1, \ldots, n\} \setminus (I \cup J)$ е изпълнено $x_i = y_i$ и $y_i = z_i$, откъдето $x_i = z_i$. Следователно $K \subseteq I \cup J$ и

$$d(x, z) = \mathrm{card}(K) \leq \mathrm{card}(I) + \mathrm{card}(J) = d(x, y) + d(y, z).$$

Накрая, $d(x, y) \geq 0$ за $\forall x, y \in A^n$ с равенство $d(x, y) = 0$ тогава и само тогава, когато $x_i = y_i$ за $\forall 1 \leq i \leq n$ или $x = y$, Q.E.D.

Минималното разстояние на код $C \subset A^n$ се определя като

$$d_{\min}(C) = \min\{d(x, y) \,|\, x, y \in C,\ x \neq y\}.$$

За крайно поле $A = \mathbb{F}_q$ и $0^n = (0_{\mathbb{F}_q}, \ldots, 0_{\mathbb{F}_q}) \in \mathbb{F}_q^n$, определяме теглото на Hamming като $\mathrm{wt}(x) = d(x, 0^n)$ за $\forall x \in \mathbb{F}_q^n$. Нека

$$\mathrm{wt}_{\min}(C) = \min\{\mathrm{wt}(x) \,|\, x \in C,\ x \neq 0^n\}$$

е минималното тегло на Hamming. За линеен код $C \subset \mathbb{F}_q^n$ твърдим, че минималното разстояние $d_{\min}(C)$ съвпада с минималното тегло $\mathrm{wt}_{\min}(C)$. Наистина, Декартовият квадрат $C \times C$ е крайно множество и $d_{\min}(C)$ се достига върху някакви $y, z \in C$, $y \neq z$. Понеже $y_i \neq z_i$ точно когато $y_i - z_i \neq 0$, имаме $d(y, z) = \mathrm{wt}(y - z)$ и $d_{\min}(C) \geq \mathrm{wt}_{\min}(C)$. От друга страна,

$$\{\mathrm{wt}(x) \,|\, x \in C,\ x \neq 0^n\} \subset \{d(x, y) \,|\, x, y \in C,\ x \neq y\},$$

така че $d_{\min}(C) \leq \mathrm{wt}_{\min}(C)$ и $d_{\min}(C) = \mathrm{wt}_{\min}(C)$.
Ако $C \subset \mathbb{F}_q^n$ е линеен код с дължина n, размерност k и минимално разстояние d, то можем да считаме, че всеки елемент $x = (x_1, \ldots, x_n) \in C$ има k информационни символа и $n - k$ проверочни символа. Затова бихме искали k да е сравнително голямо спрямо n, така че да не предаваме твърде много несъществени символи и кодирането да е ефикасно.
От друга страна, бихме искали да имаме сравнително голямо минимално разстояние d, защото ако при предаване на кодирана информация са сгрешени най-много $\left[\frac{d-1}{2}\right]$ символа, то получената дума се декодира еднозначно. По-точно, нека $B_t(x) = \{y \in A^n \mid d(x, y) \leq t\}$ е затвореното кълбо с център $x \in A^n$ и радиус $t \in \mathbb{N}$. Тогава за произволни $x, y \in C$, $x \neq y$, кълбата $B_{\left[\frac{d-1}{2}\right]}(x)$ и $B_{\left[\frac{d-1}{2}\right]}(y)$ не се пресичат в A^n. В противен случай, за всяко $z \in B_{\left[\frac{d-1}{2}\right]}(x) \cap B_{\left[\frac{d-1}{2}\right]}(y)$ неравенството на триъгълника дава $d(x, y) \leq d(x, z) + d(y, z) \leq 2\left[\frac{d-1}{2}\right] < d$, което противоречи на $d \leq d(x, y)$ по определението за минимално разстояние d. По този начин, всяка предадена дума се съдържа в единствено кълбо $B_{\left[\frac{d-1}{2}\right]}(x)$ с център в C и се заменя еднозначно с x. С други думи, кодовете с минимално разстояние d поправят най-много $\left[\frac{d-1}{2}\right]$ грешки и затова търсим кодове със сравинтелно голямо d за фиксирани n и k.
Линейните кодове $C \subset \mathbb{F}_q^n$ с дължина n, размерност k и минимално разстояние d ще наричаме накратко $[n, k, d]_q$-кодове. За да се убедим, че всеки линеен код $C \subset \mathbb{F}_q^n$ е множество от стойности, да напомним някои сведения за линейните функционали върху крайномерно пространство V. Ако V е линейно пространство над поле F, то F-линейните изображения $\alpha : V \to F$ се наричат линейни функционали върху V. Линейните функционали α и β върху V се събират поточково, $(\alpha + \beta)(v) = \alpha(v) + \beta(v)$ за $\forall v \in V$. За произволно $\lambda \in F$ и произволен линеен функционал α определяме $\lambda\alpha : V \to F$ по правилото $(\lambda\alpha)(v) = \lambda\alpha(v)$ за $\forall v \in V$. Непосредствено се проверява, че $\alpha + \beta : V \to F$ и $\lambda\alpha : V \to F$ са линейни функционали. По-точно, $(\alpha+\beta)(v_1+v_2) = \alpha(v_1+v_2)+\beta(v_1+v_2) = [\alpha(v_1)+\alpha(v_2)]+[\beta(v_1)+\beta(v_2)] = [\alpha(v_1)+\beta(v_1)]+[\alpha(v_2)+\beta(v_2)] = (\alpha+\beta)(v_1)+(\alpha+\beta)(v_2)$ и $(\alpha+\beta)(\mu v_1) = \alpha(\mu v_1)+\beta(\mu v_1) = \mu\alpha(v_1)+\mu\beta(v_1) = \mu[\alpha(v_1)+\beta(v_1)] = \mu(\alpha+\beta)(v_1)$ за $\forall v_1, v_2 \in V, \forall \mu \in F$. Аналогично, $(\lambda\alpha)(v_1+v_2) = \lambda\alpha(v_1+v_2) = \lambda(\alpha(v_1)+\alpha(v_2)) = \lambda\alpha(v_1)+\lambda\alpha(v_2) = (\lambda\alpha)(v_1)+(\lambda\alpha)(v_2)$ и $(\lambda\alpha)(\mu v_1) = \lambda\alpha(\mu v_1) = \lambda\mu\alpha(v_1) = \mu[\lambda\alpha(v_1)] = \mu(\lambda\alpha)(v_1)$ за $\forall v_1, v_2 \in V$, $\forall \mu \in F$. С така определените събиране и умножение с $\lambda \in F$, множеството V^* на линейните функционали върху V образува линейно пространство над F, наречено дуално пространство на V. Верността на аксиомите за линейно пространство във V^* се свежда до съответните свойства на събирането и умножението в F, чрез остойностяване на линейните функционали във фиксиран вектор. За асоциативността на събирането е достатъчно да отбележим, че $[(\alpha+\beta)+\gamma](v) = (\alpha+\beta)(v)+\gamma(v) = (\alpha(v)+\beta(v))+\gamma(v) = \alpha(v)+(\beta(v)+\gamma(v)) = \alpha(v)+(\beta+\gamma)(v) = [\alpha+(\beta+\gamma)](v)$ във всяко $v \in V$. Комутативността на събирането във V^* следва от $(\alpha+\beta)(v) = \alpha(v)+\beta(v) = \beta(v)+\alpha(v) = (\beta+\alpha)(v)$ за $\forall v \in V$. Нулевият функционал $\mathcal{O} : V \to k$ има нулева стойност $\mathcal{O}(v) = 0 \in F$ за $\forall v \in V$. Тогава за $\forall \alpha \in V^*$ е изпълнено $(\alpha+\mathcal{O})(v) = \alpha(v)+\mathcal{O}(v) = \alpha(v)+0 = \alpha(v)$ в произволен вектор $v \in V$, откъдето $\alpha + \mathcal{O} = \alpha$. Всеки линеен функционал $\alpha : V \to F$ има противоположен $(-\alpha) : V \to k$, така че $(-\alpha)(v) = -\alpha(v)$ за $\forall v \in V$. Тогава $[\alpha + (-\alpha)](v) = \alpha(v) + (-\alpha)(v) = \alpha(v) + [-\alpha(v)] = 0$ за $\forall v \in V$, така че $\alpha + (-\alpha) = \mathcal{O}$. За произволни $\lambda, \mu \in F$ и $\alpha \in V^*$ е в сила дистрибутивният закон над скаларен множител, $(\lambda + \mu)\alpha = \lambda\alpha + \mu\alpha$, съгласно $[(\lambda+\mu)\alpha](v) = (\lambda+\mu)\alpha(v) = \lambda\alpha(v)+\mu\alpha(v) = (\lambda\alpha)(v)+(\mu\alpha)(v) = (\lambda\alpha+\mu\alpha)(v)$ за $\forall v \in V$. Дистрибутивният закон над векторен множител $\lambda(\alpha+\beta) = \lambda\alpha+\lambda\beta$

за $\lambda \in F$ и $\alpha, \beta \in V^*$ следва от $[\lambda(\alpha+\beta)](v) = \lambda[(\alpha+\beta)(v)] = \lambda[\alpha(v)+\beta(v)] = \lambda\alpha(v)+\lambda\beta(v) = (\lambda\alpha)(v)+(\lambda\beta)(v) = (\lambda\alpha+\lambda\beta)(v)$ във всяко $v \in V$. За произволни $\lambda, \mu \in F$ и $\alpha \in V^*$ от $[(\lambda\mu)\alpha](v) = (\lambda\mu)\alpha(v) = \lambda[\mu\alpha(v)] = \mu[\lambda\alpha(v)] = \lambda[(\mu\alpha)(v)] = \mu[(\lambda\alpha)(v)] = [\lambda(\mu\alpha)](v) = [\mu(\lambda\alpha)](v)$ за $\forall v \in V$. Накрая, $(1_F.\alpha)(v) = 1_F.\alpha(v) = \alpha(v)$ за всяко $v \in V$ доказва $1_F\alpha = \alpha$ за $\forall\alpha \in V^*$. С това проверихме, че V^* е линейно пространство над F.
Дуалното порстранство V^* на крайномерно пространство V е изоморфно на V. Това е съдържанието на следното

Твърдение 1.2. *Ако $e_1, \ldots, e_n$ е базис на линейното пространство V над поле F, то съществува еднозначно определен дуален базис $\varepsilon^1, \ldots, \varepsilon^n$ на V^*, така че*

$$\varepsilon^i(e_j) = \delta_{ij} = \begin{cases} 1_F & \text{за } i = j \\ 0_F & \text{за } i \neq j. \end{cases}$$

Изображението

$$\varphi_V : V \longrightarrow V^*,$$
$$\varphi_V\left(\sum_{i=1}^n x_i e_i\right) = \sum_{i=1}^n x_i\varepsilon^i$$

е линеен изоморфизъм, а оттам и

$$\varphi_{V^*}\varphi_V : V \to (V^*)^*$$

е линеен изоморфизъм. Ще отъждествяваме V с $(V^*)^*$ посредством съответствието

$$v \mapsto (w^* \mapsto v(w^*) = w^*(v)) \quad \text{за } \forall v \in V, \quad \forall w^* \in V^*.$$

Доказателство: Доколкото $e_1, \ldots, e_n$ е базис на V, за всяко $1 \leq i \leq n$ съществува единствен линеен функционал $\varepsilon^i : V \to F$, трансформиращ e_j в $\varepsilon^i(e_j) = \delta_{ij}$. Това се дължи на факта, че всеки вектор $v \in V$ има еднозначно определени координати $x_1, \ldots, x_n \in k$, така че $v = \sum\limits_{j=1}^n x_j e_j$. Определяме $\varepsilon^i(v) = x_i$ и проверяваме, че така зададеното изображение е линейно. По-точно,

$$\varepsilon^i\left(\sum_{j=1}^n x_j e_j + \sum_{k=1}^n y_k e_k\right) = \varepsilon^i\left(\sum_{j=1}^n (x_j+y_j)e_j\right) =$$

$$x_i + y_i = \varepsilon^i\left(\sum_{j=1}^n x_j e_j\right) + \varepsilon^i\left(\sum_{k=1}^n y_k e_k\right),$$

$$\varepsilon^i\left(\lambda\left(\sum_{j=1}^n x_j e_j\right)\right) = \varepsilon^i\left(\sum_{j=1}^n (\lambda x_j)e_j\right) = \lambda x_i = \lambda\varepsilon^i\left(\sum_{j=1}^n x_j e_j\right).$$

За произволен линеен функционал $\eta^i : V \to F$ с $\eta^i(e_j) = \delta_{ij}$ следва, че

$$\eta^i\left(\sum_{j=1}^n x_j e_j\right) = \sum_{j=1}^n x_j\eta^i(e_j) = \sum_{j=1}^n x_j\varepsilon^i(e_j) = \varepsilon^i\left(\sum_{j=1}^n x_j e_j\right),$$

откъдето $\eta^i \equiv \varepsilon^i$.
Твърдим, че така построените линейни функционали $\varepsilon^1, \ldots, \varepsilon^n \in V^*$ образуват базис на V^*. Наистина, ако $\sum\limits_{i=1}^n \lambda\varepsilon^i = \mathcal{O} \in V^*$, то за произволно $1 \leq j \leq n$ е в сила $\lambda_j = \lambda_j.1_F = \sum\limits_{i=1}^n \lambda_i\varepsilon^i(e_j) = \left(\sum\limits_{i=1}^n \lambda_i\varepsilon^i\right)(e_j) = \mathcal{O}(e_j) = 0_V \in V$. Следователно

$\varepsilon^1, \ldots, \varepsilon^n$ са линейно независими. Произволен линеен функционал $\varepsilon : V \to F$ се представя като линейна комбинация $\varepsilon = \sum\limits_{i=1}^{n} \varepsilon(e_i)\varepsilon^i$ съгласно

$$\varepsilon\left(\sum_{j=1}^{n} x_j e_j\right) = \sum_{j=1}^{n} x_j \varepsilon(e_j) = \sum_{i=1}^{n}\sum_{j=1}^{n} \varepsilon(e_i) x_j \varepsilon^i(e_j) =$$

$$\sum_{i=1}^{n} \varepsilon(e_i)\varepsilon^i\left(\sum_{j=1}^{n} x_j e_j\right) = \left(\sum_{i=1}^{n} \varepsilon(e_i)\varepsilon^i\right)\left(\sum_{j=1}^{n} x_j e_j\right).$$

По този начин, линейната обвивка на $\varepsilon^1, \ldots, \varepsilon^n$ съвпада с V^* и $\varepsilon^1, \ldots, \varepsilon^n$ е базис на V^*.

Накрая да отбележим, че изображението

$$\varphi_V : V \longrightarrow V^*,$$

$$\varphi_V\left(\sum_{i=1}^{n} x_i e_i\right) = \sum_{i=1}^{n} x_i \varepsilon^i$$

е коректно определено и взаимно-еднозначно, защото $e_1, \ldots, e_n$ е базис на V, а $\varepsilon^1, \ldots, \varepsilon^n$ е базис на V^*. Съгласно

$$\varphi_V\left(\sum_{i=1}^{n} x_i e_i + \sum_{j=1}^{n} y_j e_j\right) = \varphi_V\left(\sum_{i=1}^{n} (x_i + y_i) e_i\right) = \sum_{i=1}^{n} (x_i + y_i)\varepsilon^i =$$

$$\sum_{i=1}^{n} x_i \varepsilon^i + \sum_{j=1}^{n} y_j \varepsilon^j = \varphi_V\left(\sum_{i=1}^{n} x_i e_i\right) + \varphi_V\left(\sum_{j=1}^{n} y_j e_j\right) \quad \text{и}$$

$$\varphi_V\left(\lambda\left(\sum_{i=1}^{n} x_i e_i\right)\right) = \varphi_V\left(\sum_{i=1}^{n} (\lambda x_i) e_i\right) = \sum_{i=1}^{n} (\lambda x_i)\varepsilon^i = \lambda\left(\sum_{i=1}^{n} x_i \varepsilon^i\right) = \lambda\varphi_V\left(\sum_{i=1}^{n} x_i e_i\right),$$

изображението φ_V е линеен изоморфизъм, Q.E.D.

Хиперравнина в n-мерно линейно пространство V е $(n-1)$-мерно подпространство $H \subset V$. Твърдим, че че за всяка хиперравнина $H \subset V$ съществува ненулев линеен функционал $\alpha : V \to$, така че $H = H_\alpha = \{v \in V \mid \alpha(v) = 0\}$. Наистина, всеки избор на базис $e_1, \ldots, e_n$ на V задава координатен линеен изоморфизъм $\psi : V \to {}^n$, $\psi\left(\sum\limits_{i=1}^{n} x_i e_i\right) = (x_1, \ldots, x_n)$. Образът $H_o = \psi(H) \subset F^n$ на $H \subset V$ е хиперравнина в F^n. Следователно съществуват $a_1, \ldots, a_n \in F$, с $a_{i_o} \neq 0_F$ за някое $1 \leq i_o \leq n$, така че $(n-1)$-мерното подпространство $H_o \subset F^n$ съвпада с пространството от решения на хомогенното линейно уравнение $\sum\limits_{i=1}^{n} a_i x_i = 0$. По този начин, $H = \left\{v = \sum\limits_{i=1}^{n} x_i e_i \mid \sum\limits_{i=1}^{n} a_i x_i = 0\right\}$. Ако $\varepsilon^1, \ldots, \varepsilon^n \in V^*$ е дуалният базис на $e_1, \ldots, e_n \in V$, то $\sum\limits_{i=1}^{n} a_i x_i = \sum\limits_{i=1}^{n} a_i \varepsilon^i\left(\sum\limits_{j=1}^{n} x_j e_j\right)$. Следователно $\alpha = \sum\limits_{i=1}^{n} a_i \varepsilon^i \in V^*$ с $a_{i_o} \neq 0$ е ненулев линеен функционал, задаващ хиперравнината

$$H = H_\alpha = \{v \in V \mid \alpha(v) = 0\}.$$

Произволен линеен код $C \subset \mathbb{F}_q^n$ се реализира като множеството на образите на n точки под действие на k-мерно пространство от линейни функционали.

Множеството $\mathcal{P} = \{P_1, \ldots, P_n\}$ от n точки $P_1, \ldots, P_n$ в k-мерно линейно пространство V се нарича $[n, k, d]_q$-система, ако $d = n - \max\limits_{\alpha \in V^* \setminus \{\mathcal{O}\}} \mathrm{card}(\mathcal{P} \cap H_\alpha) \geq 1$.
Условието $\max_{\alpha \in V^* \setminus \{\mathcal{O}\}} \mathrm{card}(\mathcal{P} \cap H_\alpha) < \mathrm{card}(\mathcal{P}) = n$ означава, че $\mathcal{P}$ не се съдържа в нито една хиперравнина $H_\alpha \subset V$.
Линейното изображение $\psi : V \to W$ се нарича влагане, ако $\psi : V \to Im(\psi)$ е взаимно-еднозначно върху образа си $Im(\psi) = \{\psi(v) \,|\, v \in V\}$. Доколкото $\psi(v_1) = \psi(v_2)$ е равносилно с $\psi(v_1 - v_2) = \psi(v_1) + [-\psi(v_2)] = 0_W$, линейното изображение $\psi : V \to W$ е влагане тогава и само тогава, когато когато ядрото му $Ker(\psi) := \{v \in V \,|\, \psi(v) = 0_W\}$ е тривиално, $Ker(\psi) = \{0_V\}$.

Лема 1.3. *Ако $\mathcal{P} = \{P_1, \ldots, P_n\} \subset V$ е $[n, k, d]_q$-система, то остойностяващото изображение*

$$\mathcal{E}_{\mathcal{P},V^*} : V^* \longrightarrow \mathbb{F}_q^n,$$

$$\mathcal{E}_{\mathcal{P},V^*}(\alpha) = (\alpha(P_1), \ldots, \alpha(P_n)) \quad \textit{за} \quad \forall \alpha \in V^*$$

е линейно влагане и образът му $C := Im\,(\mathcal{E}_{\mathcal{P},V^*})$ е $[n, k, d]_q$-код.

Доказателство: Преди всичко, изображението $\mathcal{E}_{\mathcal{P},V^*}$ на дуалното пространство V^* на V е линейно, защото

$$\mathcal{E}_{\mathcal{P},V^*}(\alpha+\beta) = ((\alpha+\beta)(P_1), \ldots, (\alpha+\beta)(P_n)) = (\alpha(P_1)+\beta(P_1), \ldots, \alpha(P_n)+\beta(P_n)) =$$

$$(\alpha(P_1), \ldots, \alpha(P_n)) + (\beta(P_1), \ldots, \beta(P_n)) = \mathcal{E}_{\mathcal{P},V^*}(\alpha) + \mathcal{E}_{\mathcal{P},V^*}(\beta) \text{ и}$$

$$\mathcal{E}_{\mathcal{P},V^*}(\lambda\alpha) = ((\lambda\alpha)(P_1), \ldots, (\lambda\alpha)(P_n)) = (\lambda\alpha(P_1), \ldots, \lambda\alpha(P_n)) =$$

$$\lambda(\alpha(P_1), \ldots, \alpha(P_n)) = \lambda\mathcal{E}_{\mathcal{P},V^*}(\alpha)$$

за произволни $\alpha, \beta \in V^*$ и произволно $\lambda \in \mathbb{F}_q$. Освен това, ако $\mathcal{E}_{\mathcal{P},V^*}(\alpha) = (\alpha(P_1), \ldots, \alpha(P_n)) = 0^n_{\mathbb{F}_q}$ за ненулев линеен функционал $\alpha \in V^*$, то точките $P_1, \ldots, P_n$ принадлежат на хиперравнината $H_\alpha = \{v \in V \,|\, \alpha(v) = 0\}$. Това противоречи на $d = n - \max\limits_{\alpha \in V^* \setminus \{\mathcal{O}\}} \mathrm{card}(\mathcal{P} \cap H_\alpha) \geq 1$ и доказва, че $Ker\,(\mathcal{E}_{\mathcal{P},V^*}) = 0_{V^*}$. С други думи, остойностяващото изображение $\mathcal{E}_{\mathcal{P},V^*} : V^* \to \mathbb{F}_q^n$ е влагане. Образът му $C := Im\,(\mathcal{E}_{\mathcal{P},V^*})$ е линейно подпространство на $\mathbb{F}_q^n$, съгласно $\mathcal{E}_{\mathcal{P},V^*}(\alpha) + \mathcal{E}_{\mathcal{P},V^*}(\beta) = \mathcal{E}_{\mathcal{P},V^*}(\alpha + \beta)$ и $\lambda\mathcal{E}_{\mathcal{P},V^*}(\alpha) = \mathcal{E}_{\mathcal{P},V^*}(\lambda\alpha)$ за $\forall \alpha, \beta \in V^*$, $\forall \lambda \in \mathbb{F}_q$. Линейният код $C \subset \mathbb{F}_q^n$ има дължина n в качеството си на подпространство на $\mathbb{F}_q^n$. Наличието на линеен изоморфизъм $\mathcal{E}_{\mathcal{P},V^*} : V^* \to C$ гарантира равенството на размерностите $\dim(C) = \dim(V^*) = \dim(V) = k$. Остава да докажем, че минималното разстояние на C е d. Еквивалентно, минималното тегло на C е d или всяка ненулева кодова дума $(\alpha(P_1), \ldots, \alpha(P_n)) \in C$ има най-много $n - d$ нулеви компоненти. Условието $\alpha(P_i) = 0$ е равносилно на $P_i \in H_\alpha = \{v \in V \,|\, \alpha(v) = 0\}$, така че минималното разстояние на C е d тогава и само тогава, когато $\max\limits_{\alpha \in V^* \setminus \{\mathcal{O}\}} \mathrm{card}(\mathcal{P} \cap H_\alpha) = n - d$, Q.E.D.
Две $[n, k, d]_q$-системи $\mathcal{P} \subset V$ и $\mathcal{P}_1 \subset V_1$ са еквивалентни, ако съществува линеен изоморфизъм $\psi : V \to V_1$ с $\psi(\mathcal{P}) = \mathcal{P}_1$. Това съотношение е релация на еквивалентност, защото $\mathrm{Id}_V : V \to V$ с $\mathrm{Id}_V(\mathcal{P}) = \mathcal{P}$ осъществява еквивалентност на произволна $[n, k, d]_q$-система $\mathcal{P} \subset V$ със себе си. Ако линейният изоморфизъм $\psi : V \to V_1$ с $\psi(\mathcal{P}) = \mathcal{P}_1$ задава еквивалентност на $[n, k, d]_q$-система $\mathcal{P} \subset V$ с $[n, k, d]_q$-система $\mathcal{P}_1 \subset V_1$, то $\psi^{-1} : V_1 \to V$ с $\psi^{-1}(\mathcal{P}_1) = \mathcal{P}$ определя еквивалентност на $\mathcal{P}_1 \subset V_1$ с $\mathcal{P} \subset V$. Накрая, ако линейните изоморфизми $\psi : V \to V_1$ и $\theta : V_1 \to V_2$ с $\psi(\mathcal{P}) = \mathcal{P}_1$ и $\theta(\mathcal{P}_1) = \mathcal{P}_2$ реализират еквивалентности на $\mathcal{P}$ с $\mathcal{P}_1$ и на $\mathcal{P}_1$ с $\mathcal{P}_2$, то линейният изоморфизъм $\theta\psi : V \to V_2$ с $\theta\psi(\mathcal{P}) = \mathcal{P}_2$ задава еквивалентност на $\mathcal{P}$ с $\mathcal{P}_2$. По този начин, множеството на $[n, k, d]_q$-системите се разбива в непресичащо се обединение от класове на еквивалентност. Еквивалентността на $[n, k, d]_q$-системи $\mathcal{P}$ и $\mathcal{P}_1$ ще бележим с $\mathcal{P} \sim \mathcal{P}_1$.

Лема 1.4. *Ако $\mathcal{P} \subset V$ и $\mathcal{P}_1 \subset V_1$ са еквивалентни $[n,k,d]_q$-системи с остойностяващи изображения $\mathcal{E}_{\mathcal{P},V^*} : V^* \to \mathbb{F}_q^n$ и $\mathcal{E}_{\mathcal{P}_1,V_1^*} : V_1^* \to \mathbb{F}_q^n$, то съответните им $[n,k,d]_q$-кодове $C = Im\left(\mathcal{E}_{\mathcal{P},V^*}\right)$ и $C_1 = Im\left(\mathcal{E}_{\mathcal{P}_1,V_1^*}\right)$ съвпадат.*

Доказателство: Нека $\psi : V \to V_1$ е линейният изоморфизъм с $\psi(\mathcal{P}) = \mathcal{P}_1$, осъществяващ еквивалентността на $\mathcal{P}$ с $\mathcal{P}_1$. Твърдим, че дуалното изображение

$$\psi^* : V_1^* \longrightarrow V^*,$$

$$\psi^*(\alpha_1) := \alpha_1\psi \quad \text{за} \quad \forall \alpha_1 \in V_1^*$$

е линеен изоморфизъм. Наистина, от $\psi^*(\alpha_1+\beta_1) = (\alpha_1+\beta_1)\psi = \alpha_1\psi + \beta_1\psi = \psi^*(\alpha_1)+\psi^*(\beta_1)$ и $\psi^*(\lambda\alpha_1) = (\lambda\alpha_1)\psi = \lambda(\alpha_1\psi) = \lambda\psi^*(\alpha_1)$ за произволни $\alpha_1, \beta_1 \in V_1^*$ и $\lambda \in \mathbb{F}_q$ следва линейността на $\psi^* : V_1^* \to V^*$. Освен това, ψ^* е взаимнооднозначно, съгласно $(\psi^{-1})^*\psi^* = \mathrm{Id}_{V_1^*}$ и $\psi^*(\psi^{-1})^* = \mathrm{Id}_{V^*}$. Оттук

$$\mathcal{E}_{\mathcal{P}_1,V_1^*}(\alpha_1) = (\alpha_1(\psi(P_1)), \ldots, \alpha_1(\psi(P_n)) =$$

$$(\psi^*(\alpha_1)(P_1), \ldots, \psi^*(\alpha_1)(P_n)) = \mathcal{E}_{\mathcal{P},V^*}(\psi^*(\alpha_1)).$$

С това установихме, че $Im\left(\mathcal{E}_{\mathcal{P}_1,V_1^*}\right) = Im\left(\mathcal{E}_{\mathcal{P},V^*}\right)$, Q.E.D.
За да докажем, че всеки линеен $[n,k,d]_q$-код $C \subset \mathbb{F}_q^n$ се индуцира от $[n,k,d]_q$-система, да отбележим, че координатните изображения

$$\kappa^j : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q,$$

$$\kappa^j(a_1, \ldots, a_j, \ldots, a_n) = a_j \quad \text{за} \quad \forall 1 \le j \le n$$

са линейни функционали върху $\mathbb{F}_q^n$. Ограниченията $\kappa_C^j : C \to \mathbb{F}_q$ върху подпространството C на $\mathbb{F}_q^n$ са линейни функционали върху C, т.е. $\kappa_C^1, \ldots, \kappa_C^n \in C^*$.

Лема 1.5. *Ако $C \subset \mathbb{F}_q^n$ е линеен $[n,k,d]_q$-код, то множеството $\mathcal{P}(C) := \{\kappa_C^1, \ldots, \kappa_C^n\} \subset C^*$ е $[n,k,d]_q$-система и остойностяващото изображение*

$$\mathcal{E}_{\mathcal{P}(C),C} : C = (C^*)^* \longrightarrow \mathbb{F}_q^n$$

има образ $Im\left(\mathcal{E}_{\mathcal{P}(C),C}\right) = C$.

Доказателство: Произволна кодова дума $c = (c_1, \ldots, c_n) \in C$ остава на място под действие на остойностяващото изображение

$$\mathcal{E}_{\mathcal{P}(C),C}(c) = (c(\kappa_C^1), \ldots, c(\kappa_C^n)) = (\kappa_C^1(c), \ldots, \kappa_C^n(c)) = (c_1, \ldots, c_n),$$

така че $Im\left(\mathcal{E}_{\mathcal{P}(C),C}\right) = C$. По определение, $\mathcal{P}(C)$ е множество от n точки в k-мерното пространство $C^* \simeq C$. Хиперравнините в C^* са от вида

$$H_c = \{\alpha \in C^* \,|\, c(\alpha) = \alpha(c) = 0\}$$

за някое ненулево $c \in (C^*)^* = C$. Следователно

$$\mathcal{P}(C) \cap H_c = \{\kappa_C^j \,|\, c\left(\kappa_C^j\right) = \kappa_C^j(c) = c_j = 0\}$$

и $\max\limits_{H_c} \mathrm{card}(\mathcal{P}(C) \cap H_c)$ е максималният брой на нулевите компоненти на ненулева дума $c \in C \setminus \{0^n\}$. По предположение, C има минимално разстояние d. Следователно C има минимално тегло d или максималният брой на ненулевите компоненти на ненулева дума $c \in C$ е $n-d$. Следователно $\max\limits_{c \in C\setminus\{0^n\}} \mathrm{card}(\mathcal{P}(C) \cap H_c) = n-d$ и $\mathcal{P}(C)$ е $[n,k,d]_q$-система, Q.E.D.
Сега сме готови да докажем следното

Твърдение 1.6. *Линейните $[n,k,d]_q$-кодове са във взаимно-еднозначно съответствие с класовете на еквивалентност на $[n,k,d]_q$-системите.*

Доказателство: Съгласно Лема 1.3 и Лема 1.4, всеки клас на еквивалентност на $[n,k,d]_q$-системи $\mathcal{P} \subset V$ определя линеен $[n,k,d]_q$-код $C = Im\,(\mathcal{E}_{\mathcal{P},V^*})$. От Лема 1.5 знаем, че произволен линеен $[n,k,d]_q$-код $C \subset \mathbb{F}_q^n$ отговаря на $[n,k,d]_q$-система $\mathcal{P}(C) = \{\kappa_C^1, \ldots, \kappa_C^n\} \subset C^*$, така че $Im\left(\mathcal{E}_{\mathcal{P}(C),C}\right) = C$. Остава да проверим, че ако $C = Im\,(\mathcal{E}_{\mathcal{P},V^*})$, то $\mathcal{P}(C) = \mathcal{P}$. Преди всичко да напомним, че остойностяващото изображение $\mathcal{E}_{\mathcal{P},V^*} : V^* \to C$, $\mathcal{E}_{\mathcal{P},V^*}(\alpha) = (\alpha(P_1), \ldots, \alpha(P_n))$ е линеен изоморфизъм. Дуалното изображение $\mathcal{E}^*_{\mathcal{P},V^*} : C^* \to (V^*)^* = V$ е също линеен изоморфизъм. Това позволява отъждествяването на C^* с V и разглеждането на точките $P_1, \ldots, P_n$ като линейни функционали върху $C = Im\,(\mathcal{E}_{\mathcal{P},V^*})$. По-точно, $\alpha(P_j) = P_j\mathcal{E}_{\mathcal{P},V^*}(\alpha) = P_j(\alpha(P_1), \ldots, \alpha(P_n))$ за $\forall \alpha \in V^*$. От друга страна, $\kappa_C^j\mathcal{E}_{\mathcal{P},V^*}(\alpha) = \kappa_C^j(\alpha(P_1), \ldots, \alpha(P_n)) = \alpha(P_j)$, така че $P_j = \kappa_C^j$ за $\forall 1 \leq j \leq n$. Това доказва съвпадението $\mathcal{P} = \mathcal{P}(C)$ и взаимната еднозначност на съответствието между линейните $[n,k,d]_q$-кодове и класовете на еквивалентност на $[n,k,d]_q$-системите, Q.E.D.

Класически пример за алгебро-геометричен код от стойности със сравнително ефективни параметри е така наречената L-конструкция. Дивизор D върху алгебрична крива X е крайна сума $D = \sum m_i P_i$ от точки P_i с цели коефициенти $m_i \in \mathbb{Z}$. Ако всички m_i са неотрицателни, то дивизорът D се нарича ефективен. Дивизорът на рационална функция $f \in \mathbb{F}_q(X)$ се определя като разликата $(f) = (f)_0 - (f)_\infty$ на множеството $(f)_0$ на нулите и множеството $(f)_\infty$ на полюсите на f, броени с техните кратности. Да разгледаме пространството $L(D) = \{f \in \mathbb{F}_q(X) \,|\, (f) + D \geq 0\}$ на рационалните функции върху X, чиито полюси се съдържат в ефективния дивизор $D \subset X$ и множество $\mathcal{P} = \{P_1, \ldots, P_n\}$ от n точки P_i върху X с координати от $\mathbb{F}_q$. Образът $C = Im\left(\mathcal{E}_{\mathcal{P},L(D)}\right)$ на остойностяващото изображение

$$\mathcal{E}_{\mathcal{P},L(D)} : L(D) \longrightarrow \mathbb{F}_q^n,$$

$$\mathcal{E}_{\mathcal{P},L(D)}(f) = (f(P_1), \ldots, f(P_n)) \quad \text{за} \quad \forall f \in L(D)$$

е линеен код с дължина n. Ако $\forall f \in L(D)$ има най-много $m < n$ нули върху точките $X(\mathbb{F}_q)$ на X с координати от $\mathbb{F}_q$, то $\mathcal{E}_{\mathcal{P},L(D)}$ е линейно влагане и C е $[n, \dim L(D), d]_q$-код с минимално разстояние $d \geq n - m$. Последната оценка отдолу гарантира еднозначно декодиране, когато при предаване на информация са смутени не повече от $\left[\frac{n-m-1}{2}\right]$ символа. От Теоремата на Риман-Рох следва, че $\dim L(D) \geq \deg(D) - g + 1$, където $\deg(D) = \deg\left(\sum m_i P_i\right) = \sum m_i$ е степента на D, а g е родът на X. По този начин, L-конструкцията дава поне $\deg(D) - g + 1$ информационни символа и кодирането е сравнително ефикасно. Алгебричната геометрия и, по-специално, елиптичните криви $E(\mathbb{F}_q)$ над крайно поле $\mathbb{F}_q$ се използват в асиметричната криптография. Това се основава на структурата на абелева група върху $E(\mathbb{F}_q)$. Да напомним, че редът r на елемент $G \in E(\mathbb{F}_q)$ е минималното естествено число r с $G^r = e$, където e е неутралният елемент на $E(\mathbb{F})$. Цикличната подгрупа $\langle G \rangle = \{G^n \,|\, n \in \mathbb{Z}\} \subseteq E(\mathbb{F}_q)$ е от ред r и индекс $h = [E(\mathbb{F}_q) : \langle G \rangle] = \frac{\mathrm{card}(E(\mathbb{F}_q))}{r}$. (Индексът h се определя като броя на съседните класове на $E(\mathbb{F}_q)$ относно $\langle G \rangle$.) Генераторът на ключове избира полето $\mathbb{F}_q$, уравнението на елиптичната крива $E(\mathbb{F}_q)$ над $\mathbb{F}_q$ и елемент $G \in E(\mathbb{F}_q)$ от прост ред r, така че съответната циклична подгрупа $\langle G \rangle \subseteq E(\mathbb{F}_q)$ да е със сравинтелно малък индекс $h = [E(\mathbb{F}_q) : \langle G \rangle]$. За случайно цяло число $0 \leq x \leq r - 1$, той пресмята $G_1 = G^x$ и публикува публично G, G_1 и r. При изпращане на съобщение $M \in E(\mathbb{F}_q)$ към генератора на ключове се избира случайно цяло число $0 \leq y \leq r - 1$ и се предават елементите $c_1 = G^y$ и $c_2 = MG_1^y$ на $E(\mathbb{F}_q)$. В резултат, генераторът на съобщенията пресмята $c_2\,(c_1^x)^{-1} = M$. Описаната криптографска система е толкова по-надеждна , колкото по-трудно

може да се отгатне цялото число x по зададени G и $G_1 = G^x$. Тази задача се нарича проблем за дискретния логаритъм.
Последната част на материала се отнася до така наречените базиси на Грьобнер. Нека I е ненулев идеал в пръстена $F[x_1, \ldots, x_n]$ на полиномите на $x_1, \ldots, x_n$ с коефициенти от поле F. Съгласно Теоремата на Хилберт за базиса, идеалът I е крайноопроден, т.е. съществуват краен брой полиноми $f_1, \ldots, f_m \in I$, така че

$$I = \langle f_1, \ldots, f_m \rangle = \left\{ \sum_{i=1}^{m} f_i g_i \;\middle|\; g_i \in F[x_1, \ldots, x_n] \right\}.$$

Старшите мономи $LT(f)$ на ненулевите полиноми $f \in I$ относно лексикографската наредба пораждат идеала $LT(I)$ на старшите мономи на I. Ще докажем, че съществуват полиноми $g_1, \ldots, g_k \in I$, така че $LT(I)$ се поражда от $LT(g_1), \ldots, LT(g_k)$ и I се поражда от $g_1, \ldots, g_k$. Такива полиноми $g_1, \ldots, g_k \in I$ образуват базис на Грьобнер на I. Базисите на Грьобнер на ненулев полиномиален идеал $I \lhd F[x_1, \ldots, x_n]$ служат за изучаване на алгебричното многообразие $V(I) \subset F^n$, отговарящо на I. По-точно, ако G е базис на Грьобнер на I и $I_j := I \cap F[x_{j+1}, \ldots, x_n]$ е j-тият елиминационен идеал, то $G_j := G \cap F[x_{j+1}, \ldots, x_n]$ е базис на Грьобнер на I_j. По този начин, елиминационните многообразия $V_{n-j}(I_j) \subset F^{n-j}$ съвпадат с $V_{n-j}(G_j) \subset F^{n-j}$. Проекциите $\mathrm{pr}_{n-j} : V_{n-j+1}(G_{j-1}) \to V_{n-j}(G_j)$ върху последните $n-j$ компоненти са сюрективни изображения с едномерни или крайни слоеве и определят структурата на $V(I)$ посредством редицата

$$V(I) = V(G) \to V_{n-1}(G_1) \to \ldots \to V_{n-j+1}(G_{j-1}) \to V_{n-j}(G_j) \to \ldots \to V_1(G_{n-1}).$$

Приложение:
Класификация на крайните полета и техните подполета

Да напомним, че поле F е с характеристика $\mathrm{char}(F) = 0$, ако за всяко естествено число $n \in \mathbb{N}$ е в сила $n1_F \neq 0_F$. В такъв случай, F съдържа подполе, изоморфно на полето $\mathbb{Q}$ на рационалните числа. Рационалните числа са безброй много, така че крайно поле F не може да е с $\mathrm{char}(F) = 0$. С други думи, за всяко крайно поле F съществува естествено число $m \in \mathbb{N}$, така че $m1_F = 0_F$. Минималното m с това свойство е просто число p, поради липсата на делители на нулата в F. Казваме, че F има характеристика p и записваме $\mathrm{char}(F) = p$. Всяко поле F с $\mathrm{char}(F) = p$ съдържа подполе F_o, изоморфно на полето $\mathbb{Z}_p$ от остатъци при деление с p. Всяко крайно поле F с $\mathrm{char}(F) = p$ е крайномерно линейно пространство над своето просто подполе $F_o \simeq \mathbb{Z}_p$. Затова броят на елементите на крайно поле F е естествена степен p^n, $n \in \mathbb{N}$ на характеристиката p.

Твърдение 1.7. *За всяко просто число p и за всяко естествено число n съществува единствено с точност до изоморфизъм поле $\mathbb{F}_{p^n}$ с p^n елемента.*

Доказателство: Нека F_1 е разширение на $\mathbb{Z}_p$, съдържащо всички корени на полинома $f(x) = x^{p^n} - x \in \mathbb{Z}_p[x]$. Формалната производна $f'(x) = p^n x - 1 = -1 \in \mathbb{Z}_p[x]$ не се анулира никога, така че $f(x) = 0$ има p^n различни корена $\alpha_1, \ldots, \alpha_{p^n}$. Твърдим, че $F_o = \{\alpha_1, \alpha_2, \ldots \alpha_{p^n}\}$ е поле. За целта е достатъчно да

проверим, че F_o е подполе на F_1. Наистина, за произволни $1 \leq i, j, k \leq p^n$, $\alpha_k \neq 0_{F_1}$ е в сила $(\alpha_i - \alpha_j)^{p^n} = \alpha_i^{p^n} + (-1)^{p^n}\alpha_j^{p^n} = \alpha_i - \alpha_j$ и $(\alpha_i\alpha_k^{-1})^{p^n} = \alpha_i^{p^n}(\alpha_k^{p^n})^{-1} = \alpha_i\alpha_k^{-1}$, така че $\alpha_i - \alpha_j, \alpha_i\alpha_k^{-1} \in k_o$. Това установява съществуването на поле F_o с p^n елемента, за произволно просто p и естествено n.
Ако F е поле с p^n елемента, то характеристиката $\mathrm{char}(F) = p$. Мултипликативната група $F^* = F \setminus \{0_F\}$ е от ред $p^n - 1$, така че редът на всеки елемент $\alpha \in F^*$ дели $p^n - 1$ и $\alpha^{p^n-1} = 1_F$. Чрез почленно умножение с α получаваме $\alpha^{p^n} = \alpha$ за $\forall \alpha \in F^*$. Ясно е, че 0_F е също корен на $f(x) = x^{p^n} - x \in \mathbb{Z}_p[x]$, така че F е множеството на корените на $f(x) = 0$ в подходящо разширение на $\mathbb{Z}_p$. По този начин, F_o и F са минимални разширения на $\mathbb{Z}_p$, в които полиномът $f(x)$ се разлага на линейни множители. С други думи, F_o и F са полета на разлагане на $f(x)$ над $\mathbb{Z}_p$. Известно е, че полето на разлагане е единствено с точност до изоморфизъм, откъдето и полето с p^n елемента е единствено с точност до изоморфизъм, Q.E.D.
За да докажем цикличността на произволна крайна подгрупа G на мултипликативната група k^* на поле k ни е нужна следната

Лема 1.8. *Нека G е абелева група, $a \in G$ е от ред r, $b \in G$ е от ред s. Тогава съществува елемент $c \in G$, чийто ред е най-малкото общо кратно $[r, s]$ на r и s.*

Доказателство: За взаимно прости r и s ще докажем, че $c = ab \in G$ е от ред $[r, s] = rs$. По-точно, ако c е от ред t, то $e_G = c^{ts} = a^{ts}(b^s)^t = a^{st}$ изисква r да дели ts. Поради взаимната простота на r и s, оттук получаваме, че r дели t. Аналогично, от $e_G = c^{tr} = (a^r)^t b^{tr} = b^{tr}$ следва, че s дели tr, а оттам и t. Щом взаимно простите r и s делят t, то и произведението им rs дели t. От друга страна, $c^{rs} = (a^r)^s(b^s)^r = e_G$, така че t дели rs. Следователно $t = rs$.
В общия случай, нека $\{p_1, \ldots, p_m\}$ е обединението на простите делители на r и s, така че $r = p_1^{\alpha_1} \ldots p_m^{\alpha_m}$, $s = p_1^{\beta_1} \ldots p_m^{\beta_m}$ за подходящи $\alpha_i, \beta_j \in \mathbb{N} \cup \{0\}$. Полагайки $\gamma_i = \max(\alpha_i, \beta_i)$, изразяваме най-малкото общо кратно във вида $[r, s] = p_1^{\gamma_1} \ldots p_m^{\gamma_m}$. Ако $\gamma_i = \alpha_i$ и $\rho_i = \frac{r}{p_i^{\alpha_i}}$, то $c_i = a^{\rho_i}$ е елемент от ред $\frac{r}{(r,\rho_i)} = \frac{r}{\rho_i} = p_i^{\alpha_i}$, където (r, ρ_i) е най-големият общ делител на r и ρ_i. Аналогично, за $\gamma_i = \beta_i$ и $\sigma_i = \frac{s}{p_i^{\beta_i}}$ елементът $c_i = b^{\sigma_i} \in G$ е от ред $\frac{s}{(s,\sigma_i)} = \frac{s}{\sigma_i}p_i^{\beta_i}$. По този начин установяваме съществуването на $c_1, \ldots, c_m \in G$ от редове $p_1^{\gamma_1}, \ldots, p_m^{\gamma_m}$. С индукция по $1 \leq i \leq m$ доказваме, че $c_1 \ldots c_i \in G$ е елемент от ред $p_1^{\gamma_1} \ldots p_i^{\gamma_i}$, вземайки предвид взаимната простота на $p_1^{\gamma_1} \ldots p_{i-1}^{\gamma_{i-1}}$ и $p_i^{\gamma_i}$ за $2 \leq i \leq m$, Q.E.D.

Твърдение 1.9. *Всяка крайна подгрупа G на мултипликативната група F^* на поле F е циклична.*
В частност, мултипликативната група $\mathbb{F}_{p^n}^*$ на крайно поле $\mathbb{F}_{p^n}$ е циклична.

Доказателство: В крайната група G избираме елемент $\alpha \in G$ от максимален ред r. Ще докажем, че $G = \langle\alpha\rangle$ е цикличната група, породена от α. За целта да отбележим, че редът s на произволен елемент $\beta \in G$ дели r. В противен случай, най-големият общ делител $(r, s) < s$, така че най-малкото общо кратно $[r, s] = \frac{rs}{(r,s)} > r$. Съгласно Лема 1.8, съществува елемент $\gamma \in G$ от ред $[r, s]$. Това противоречи на максималността на r и доказва, че редът s на β дели реда r на α. В резултат, $\beta^r = e_G$ за неутралния елемент e_G на G и G се състои от корени на полинома $g(x) = x^r - 1 \in k[x]$. Броят на тези корени не надминава r, така че G има най-много r елемента. От друга страна, $e_G, \alpha, \ldots, \alpha^{r-1}$ са r различни елемента на G, така че $G = \{e_G, \alpha, \ldots, \alpha^{r-1}\} = \langle\alpha\rangle$ е циклична група от ред r, Q.E.D.

Лема 1.10. *Ако $G = \langle\alpha\rangle$ е циклична група от ред r, то за всеки естествен делител s на r съществува единствена подгрупа $G_s = \langle\alpha^{\frac{r}{s}}\rangle$ на G от ред s, която съвпада с корените на уравнението $x^s = e_G$ в G.*

Доказателство: Елементът $\alpha^{\frac{r}{s}} \in G$ е от ред $\left[r : \left(r, \frac{r}{s}\right)\right] = r : \left(\frac{r}{s}\right) = s$, така че $G_s = \langle\alpha^{\frac{r}{s}}\rangle$ е циклична подгрупа на G от ред s.
За да докажем единствеността на G_s, характеризирайки тази подгрупа като множеството на корените на $x^s = e_G$ в G, да напомним съществуването на групов изоморфизъм $\varphi : G \to \mathbb{C}_r$ в мултипликативната група

$$\mathbb{C}_r = \langle\omega_r\rangle = \left\{\omega_r^k \,|\, 0 \leq k \leq r-1\right\}$$

на r-тите корени на единицата, породена от $\omega_r = \cos\left(\frac{2\pi}{r}\right) + i\sin\left(\frac{2\pi}{r}\right)$. Произволна подгрупа $H_s \subset G$ от ред s се изобразява в подгрупа $F_s = \varphi(H_s) \subset \mathbb{C}_r$ от ред s. Понеже редът на $f \in F_s$ дели реда s на F_s, подгрупата F_s се състои от корени на уравнението $x^s = 1$ в $\mathbb{C}$. Уравнението $x^s = 1$ има най-много s комплексни корена, така че F_s съвпада с корените на $x^s = 1$ в $\mathbb{C}$. Груповият изоморфизъм φ^{-1} е съгласуван с умножението и трансформира комплексното число $1 \in \mathbb{C}_r$ в неутралния елемент $e_G \in G$, оттук следва, че H_s се състои от корените на $x^s = e_G$ в G и съвпада с $G_s = \langle\alpha^{\frac{r}{s}}\rangle$, Q.E.D.

Твърдение 1.11. *(i) За всеки естествен делител m на $n \in \mathbb{N}$ съществува единствено подполе на $\mathbb{F}_{p^n}$, изоморфно на $\mathbb{F}_{p^m}$.*
(ii) Всяко подполе на $\mathbb{F}_{p^n}$ е изоморфно на $\mathbb{F}_{p^m}$ за някакъв естествен делител m на n.

Доказателство: (i) Мултипликативната група $\mathbb{F}_{p^n}^* = \langle\alpha\rangle$ е циклична от ред $p^n - 1$. Ако $n = mk$ за някои естествени m и k, то

$$p^n - 1 = (p^m)^k - 1 = (p^m - 1)\left(p^{m(k-1)} + p^{m(k-2)} + \ldots + p^{2m} + p^m + 1\right).$$

Ако означим $l = p^{m(k-1)} + p^{m(k-2)} + \ldots + p^m + 1$, то $\langle\alpha^l\rangle$ е циклична подгрупа на $\mathbb{F}_{p^n}^*$ от ред $p^m - 1$, която съвпада с корените на $x^{p^m-1} = 1_{\mathbb{F}_{p^n}}$ в $\mathbb{F}_{p^n}$. Следователно $F = \langle\alpha^l\rangle \cup \{0_{\mathbb{F}_{p^n}}\}$ съвпада с множеството на корените $f(x) = x^{p^m} - x \in \mathbb{Z}_p[x]$ в $\mathbb{F}_{p^n}$ и представлява поле, изоморфно на $\mathbb{F}_{p^m}$.
(ii) Ако F е подполе на $\mathbb{F}_{p^n}$, то $\mathbb{F}_{p^n}$ е линейно пространство над F с някаква крайна размерност k. Тогава $\mathbb{F}_{p^n} \simeq F^k$ и $p^n = \mathrm{card}(\mathbb{F}_{p^n}) = \mathrm{card}(F)^k$, откъдето $\mathrm{card}(F) = p^{\frac{n}{k}}$. По този начин, $\frac{n}{k} = m \in \mathbb{N}$ и F е поле с p^m елемента. Всички полета F с p^m елемента са изоморфни на $\mathbb{F}_{p^m}$, Q.E.D.