

## Теорема на Bezout. Полиномиални кодове върху равнинни криви.

ОПРЕДЕЛЕНИЕ 10.1. *Множеството*

$$Z(f) = \{[x : y : z] \in \mathbb{P}^2(\bar{k}) \mid f(x, y, z) = 0\}$$

на нулите на (евентуално разложим) хомогенен полином  $f(x, y, z) \in \bar{k}[x, y, z]$  в двумерното проективно пространство  $\mathbb{P}^2(\bar{k})$  се нарича проективна равнинна крива.

Степента на проективна равнинна крива  $Z(f) \subset \mathbb{P}^2(\bar{k})$  се определя като общата степен на хомогенния полином  $f(x, y, z)$ ,  $\deg Z(f) = \deg(f)$ .

Ще докажем Слаба форма на Теоремата на Bezout с помощта на резултанта на два полинома на една променлива. Да напомним, че за полиноми

$$f(t) = a_0 t^n + a_1 t^{n-1} + \dots + a_{n-1} t + a_n = a_0 \prod_{i=1}^n (t - \alpha_i),$$

$$g(t) = b_0 t^m + b_1 t^{m-1} + \dots + b_{m-1} t + b_m = b_0 \prod_{j=1}^m (t - \beta_j)$$

с коефициенти от поле  $K$ , резултантата се определя като

$$R(f, g) = a_0^m b_0^n \prod_{i=1}^n \prod_{j=1}^m (\alpha_i - \beta_j).$$

Непосредствено се вижда, че

$$R(f, g) = a_0^m \prod_{i=1}^n \left[ b_0 \prod_{j=1}^m (\alpha_i - \beta_j) \right] = a_0^m \prod_{i=1}^n g(\alpha_i)$$

и  $R(f, g) = 0$  за  $f(t) \not\equiv 0_K$ ,  $g(t) \not\equiv 0_K$  точно когато  $f$  и  $g$  имат общ корен. Дискриминантата на  $f(t)$  се определя като

$$D(f) := a_0^{2n-2} \prod_{n \geq i > j \geq 1} (\alpha_i - \alpha_j)^2$$

ЛЕМА 10.2. Нека  $f(t), g(t) \in K[t]$  са полиноми на една променлива  $t$  с коефициенти от поле  $K$ , а  $P$  е простото подполе на  $K$ . Тогава дискриминантата  $D(f) \in P[a_0, \dots, a_n]$  на  $f(t)$  е полином на коефициентите на  $f(t)$ , резултантата  $R(f, g) \in P[a_0, \dots, a_n, b_0, \dots, b_m]$  на  $f$  и  $g$  е полином на коефициентите на  $f$  и  $g$ .

**Доказателство:** Нека  $\sigma_1, \dots, \sigma_n$  са елементарните симетрични полиноми на  $\alpha_1, \dots, \alpha_n$ , а  $\tau_1, \dots, \tau_m$  са елементарните симетрични полиноми на  $\beta_1, \dots, \beta_m$ . Непосредствено се вижда, че  $\prod_{n \geq i > j \leq 1} (\alpha_i - \alpha_j)^2$  е симетричен полином на  $\alpha_1, \dots, \alpha_n$ ,

откъдето и полином  $\prod_{n \geq i > j \geq 1} (\alpha_i - \alpha_j)^2 \in P[\sigma_1, \dots, \sigma_n]$  на елементарните симетрични полиноми  $\sigma_1, \dots, \sigma_n$  на  $\alpha_1, \dots, \alpha_n$  с коефициенти от  $P$ . От формулите на Виет  $\sigma_i = (-1)^i \frac{a_i}{a_0}$  за  $1 \leq i \leq n$  получаваме, че

$$\prod_{n \geq i > j \leq 1} (\alpha_i - \alpha_j)^2 \in P \left[ \frac{a_1}{a_0}, \dots, \frac{a_n}{a_0} \right].$$

Съгласно алгоритъма за представяне на симетричен полином на  $\alpha_1, \dots, \alpha_n$  като полином на  $\sigma_1, \dots, \sigma_n$ , мономите на  $\prod_{n \geq i > j \leq 1} (\alpha_i - \alpha_j)^2$  са от вида

$$\mu = \left( \frac{a_1}{a_0} \right)^{k_1 - k_2} \left( \frac{a_2}{a_0} \right)^{k_2 - k_3} \dots \left( \frac{a_{n-1}}{a_0} \right)^{k_{n-1} - k_n} \left( \frac{a_n}{a_0} \right)^{k_n}$$

с  $k_1 \geq k_2 \geq \dots \geq k_{n-1} \geq k_n \geq 0$ . Тук  $k_1$  не надминава максималната степен  $2n-2$ , в която  $\alpha_1$  участва в моном на  $\prod_{n \geq i > j \geq 1} (\alpha_i - \alpha_j)^2$ . Следователно мономите на  $D(f) = a_0^{2n-2} \prod_{n \geq i > j \geq 1} (\alpha_i - \alpha_j)^2$  са от вида

$$a_0^{2n-2} \mu = a_0^{2n-2-k_1} a_1^{k_1-k_2} a_2^{k_2-k_3} \dots a_{n-1}^{k_{n-1}-k_n} a_n^{k_n}$$

с  $2n-2 \geq k_1 \geq k_2 \geq \dots \geq k_{n-1} \geq k_n \geq 0$ , така че  $a_0^{2n-2} \mu \in P[a_0, a_1, \dots, a_n]$  и  $D(f) \in P[a_0, a_1, \dots, a_n]$ .

Полиномът  $\prod_{i=1}^n \prod_{j=1}^m (\alpha_i - \beta_j)$  от степен  $m$  относно  $\alpha_i$  и от степен  $n$  относно  $\beta_j$  е симетричен полином на  $\alpha_1, \dots, \alpha_n$  и симетричен полином на  $\beta_1, \dots, \beta_m$ . Следователно

$$\prod_{i=1}^n \prod_{j=1}^m (\alpha_i - \beta_j) \in P[\sigma_1, \dots, \sigma_n, \tau_1, \dots, \tau_m] = P \left[ \frac{a_1}{a_0}, \dots, \frac{a_n}{a_0}, \frac{b_1}{b_0}, \dots, \frac{b_m}{b_0} \right],$$

съгласно основната теорема за симетричните полиноми и формулите на Виет  $\sigma_i = (-1)^i \frac{a_i}{a_0}$  за  $1 \leq i \leq n$ ,  $\tau_j = (-1)^j \frac{b_j}{b_0}$  за  $1 \leq j \leq m$ . Мономите на

$$\prod_{i=1}^n \prod_{j=1}^m (\alpha_i - \beta_j)$$

са от вида

$$\nu = \left( \frac{a_1}{a_0} \right)^{k_1 - k_2} \dots \left( \frac{a_{n-1}}{a_0} \right)^{k_{n-1} - k_n} \left( \frac{a_n}{a_0} \right)^{k_n} \left( \frac{b_1}{b_0} \right)_{l_1 - l_2} \dots \left( \frac{b_{m-1}}{b_0} \right)^{l_{m-1} - l_m} \left( \frac{b_m}{b_0} \right)^{l_m}$$

за  $m \geq k_1 \geq k_2 \geq \dots \geq k_{n-1} \geq k_n \geq 0$ ,  $n \geq l_1 \geq l_2 \geq \dots \geq l_{m-1} \geq l_m \geq 0$ .

Следователно мономите на  $R(f, g) = a_0^m b_0^n \prod_{i=1}^n \prod_{j=1}^m (\alpha_i - \beta_j)$  са от вида

$$a_0^m b_0^n \nu = a_0^{m-k_1} a_1^{k_1-k_2} \dots a_{n-1}^{k_{n-1}-k_n} a_n^{k_n} b_0^{n-l_1} b_1^{l_1-l_2} \dots b_{m-1}^{l_{m-1}-l_m} b_m^{l_m} \in P[a_0, a_1, \dots, a_n, b_0, b_1, \dots, b_m]$$

и  $R(f, g) \in P[a_0, a_1, \dots, a_n, b_0, b_1, \dots, b_m]$ , Q.E.D.

ЛЕМА 10.3. Нека

$$f(t) = a_0 t^n + a_1 t^{n-1} + \dots + a_{n-1} t + a_n \quad u$$

$$g(t) = b_0 t^m + b_1 t^{m-1} + \dots + b_{m-1} t + b_m$$



$\det(L)$  по адюнгирани количества относно  $(m+n)$ -ти стълб,  $(m+n-1)$ -ви стълб, ...  $(m+1)$ -ви стълб в първоначалната номерация на стълбовете и т.н. Получаваме

$$\begin{aligned} & (-1)^{mn} a_0^m \left[ \prod_{i=1}^n g(\alpha_i) \right] (-1)^{\frac{n(n-1)}{2}} \prod_{1 \leq j < i \leq n} (\alpha_i - \alpha_j) = \\ & = \det(M) (-1)^{mn} (-1)^{\frac{n(n-1)}{2}} \prod_{1 \leq j < i \leq n} (\alpha_i - \alpha_j). \end{aligned}$$

Резултантата  $R(f, g) = a_0^m \prod_{i=1}^n g(\alpha_i)$ , защото  $g(\alpha_i) = b_0 \prod_{j=1}^m (\alpha_i - \beta_j)$ . След почленно умножение с  $(-1)^{mn} (-1)^{\frac{n(n-1)}{2}} a_0^{2n-2} \prod_{1 \leq j < i \leq n} (\alpha_i - \alpha_j)$  имаме

$$R(f, g)D(f) = \det(M)D(f) \quad (10.1)$$

за дискриминантата  $D(f)$  на  $f(t)$ .

Достатъчно е да докажем, че  $D(f) \in P[a_0, \dots, a_n]$  не се анулира тъждествено като полином на  $a_0, \dots, a_n$  с коефициенти от простото подполе  $P$  на  $K$ , за да получим  $R(f, g) = \det(M)$ . Да допуснем, че  $D(f) \equiv 0$  се анулира тъждествено като полином на  $a_0, \dots, a_n$ . Тогава всеки полином  $f(t) \in K[t]$  има кратен корен или  $\forall f(t) \in K[t]$  има общ корен с формалната си производна  $f'(t) \in K[t]$ . Ако характеристиката  $\text{char}(K) = 0$  или  $\text{char}(K) = p$  не дели степента  $\deg(f) = n$ , то  $f(t) = t^n + 1$  и  $f'(t) = nt^{n-1}$  нямат общ корен. В случая на степен  $\deg(f) = n$ , кратна на характеристиката  $\text{char}(K) = p$  полиномът  $f(t) = t^n + t + 1 \in K[t]$  и формалната му производна  $f'(t) = 1$  нямат общи корени. Полученото противоречие доказва, че  $D(f) \neq 0 \in P[a_0, \dots, a_n]$  и  $R(f, g) = \det(M)$ , Q.E.D. Теоремата на Bezout за проективни равнинни криви  $Z(f) \subset \mathbb{P}^2(\bar{k})$  и  $Z(g) \subset \mathbb{P}^2(\bar{k})$  гласи, че ако сечението  $Z(f) \cap Z(g)$  е крайно, то броят на точките в него е равен на произведението на степените на  $Z(f)$  и  $Z(g)$ , т.е.

$$|Z(f) \cap Z(g)| = \deg Z(f) \deg Z(g).$$

Ние ще докажем и използваме

**ТВЪРДЕНИЕ 10.4.** (Слаб вариант на Теоремата на Bezout) *Ако  $Z(f) \subset \mathbb{P}^2(\bar{k})$  и  $Z(g) \subset \mathbb{P}^2(\bar{k})$  са проективни равнинни криви с крайно сечение  $Z(f) \cap Z(g)$ , то*

$$|Z(f) \cap Z(g)| \leq \deg Z(f) \deg Z(g).$$

**Доказателство:** Разглеждаме проекцията

$$\Pi : \mathbb{P}^2(\bar{k}) \dashrightarrow \mathbb{P}^1(\bar{k}),$$

$$\Pi([x : y : z]) = [x : y],$$

която е определена върху  $\mathbb{P}^2(\bar{k}) \setminus \{[0 : 0 : 1]\}$ . За всяка точка  $[x_o : y_o] \in \mathbb{P}^1(\bar{k})$  слят

$$\Pi^{-1}[x_o : y_o] = \{[x : y : z] \in \mathbb{P}^2(\bar{k}) \mid x_o y - x y_o = 0\}$$

е проективизацията на равнината

$$\{(x, y, z) \in \bar{k}^3 \mid x_o y - x y_o = 0\} \simeq \bar{k}^2$$

през началото в  $\bar{k}^3$ , така че  $\Pi^{-1}[x_o : y_o] \simeq \mathbb{P}^1(\bar{k})$  е проективна права.

ТВЪРДИМ, че съществува такава координатна система в  $\bar{k}^3$ , спрямо която сечението  $Z(f) \cap Z(g) \subseteq \mathbb{P}^2(\bar{k}) \setminus \{[0 : 0 : 1]\}$  се съдържа в дефиниционната област на  $\Pi$  и ограничението  $\Pi : Z(f) \cap Z(g) \rightarrow \Pi(Z(f) \cap Z(g))$  е взаимно еднозначно върху образа си. За целта разглеждаме правите през началото  $l_i = \{(\lambda p_i, \lambda q_i, \lambda r_i) \mid \lambda \in \bar{k}\}$ ,  $1 \leq i \leq n$ , до които се повдигат точките от



Следователно  $R_z(f, g)(x, y) \in \bar{k}[x, y]$  е хомогенен полином от степен

$$\begin{aligned} \Delta &= \delta(s+l) + \frac{(s+l-1)(s+l)}{2} - (m-l)l - \frac{(l-1)l}{2} - (n-s)s - \frac{(s-1)s}{2} = \\ &= ms + nl - sl \leq mn, \end{aligned}$$

защото  $(m-l)(n-s) \geq 0$ , Q.E.D.

Равенството  $|Z(f) \cap Z(g)| = \deg(f) \deg(g)$  за крайно сечение  $Z(f) \cap Z(h)$  се извежда от неравенствата

$$|Z(f) \cap Z(h)| = \sum_{p \in Z(f) \cap Z(g)} \dim_{\bar{k}} \mathcal{O}_p / \langle f, g \rangle_p \leq \dim_{\bar{k}} \bar{k}[x, y] / \langle f, g \rangle \leq \deg(f) \deg(g),$$

които после се доказват че са изпълнени като равенства.

Сега ще построим полиномиални кодове върху афинни равнинни криви над крайни полета. Ще пресметнем размерностите на тези кодове и ще оценим отдолу минималните им разстояния.

Нека  $Z(h) = \{(x, y) \in \bar{\mathbb{F}}_q^2 \mid h(x, y) = 0\}$  е афинна равнинна крива, зададена чрез неразложим над  $\bar{\mathbb{F}}_q$  (необезателно хомогенен) полином  $h(x, y) \in \mathbb{F}_q[x, y]$  от обща степен  $m$ . Да означим с  $U_l$  множеството на полиномите от  $\mathbb{F}_q[x, y]$  с обща степен  $\leq l$ . Тогава  $U_l$  е  $\frac{(l+1)(l+2)}{2}$ -мерно линейно пространство над  $\mathbb{F}_q$ , защото мономите  $x^s y^{i-s}$  с  $0 \leq s \leq i$ ,  $0 \leq i \leq l$  образуват  $\mathbb{F}_q$ -базис на  $U_l$  и техният брой е  $\sum_{i=0}^l (i+1) = \frac{(l+1)(l+2)}{2}$ . Избираме  $n$  различни  $\mathbb{F}_q$ -рационални точки  $P_1, \dots, P_n \in Z(h)(\mathbb{F}_q)$  за някое естествено  $n > ml$  и разглеждаме остойносттаващото изображение

$$\mathcal{E} : U_l \longrightarrow \mathbb{F}_q^n,$$

$$\mathcal{E}(f) = (f(P_1), \dots, f(P_n)).$$

Ядрото  $\ker \mathcal{E} = \{g \in U_l \mid g(P_i) = 0, 1 \leq i \leq n\}$  се състои от онези полиноми  $g \in U_l$ , за които  $P_1, \dots, P_n \in Z(g) \cap Z(h)$ . Ако сечението  $Z(g) \cap Z(h)$  е крайно, то броят на точките в него е

$$n = |\{P_1, \dots, P_n\}| \leq |Z(g) \cap Z(h)| \leq lm,$$

което противоречи на избора на  $n > lm$ . Следователно  $Z(g) \cap Z(h)$  е крива за всички  $g \in U_l \setminus \{0\}$ . От  $Z(g) \cap Z(h) \subseteq Z(h)$  е неприводимостта на  $Z(h)$  получаваме  $Z(g) \cap Z(h) = Z(h)$ , откъдето  $Z(h) \subseteq Z(g)$ . Следователно идеалите  $r(\langle h \rangle) = IZ(h) \supseteq IZ(g)$  изпълняват противоположното включване. Неразложимият над  $\bar{\mathbb{F}}_q$  полином  $h$  поражда прост идеал  $\langle h \rangle$ , така че  $r(\langle h \rangle) = \langle h \rangle$ . Оттук,  $g \in IZ(g) \subseteq \langle h \rangle$ . Обратно, ако  $g \in \langle h \rangle$ , то  $g(P_i) = 0$  за  $\forall P_i \in Z(h)$  и  $g \in \ker \mathcal{E}$ . С това доказахме, че

$$\ker \mathcal{E} = \langle h \rangle \cap U_l = \{hf \mid \deg(hf) \leq l\} = \{hf \mid \deg f \leq l-m\} \simeq U_{l-m} \quad \text{за } l \geq m$$

и  $\ker \mathcal{E} = \{0\}$  за  $l < m$ .

Условието  $\ker \mathcal{E} = \langle h \rangle \cap U_l$  може да се докаже и чрез използване на свойствата на резултантата на два полинома. Ако резултантата  $R_y(h, g) = 0 \in \bar{k}$  на  $h$  и  $g$  относно  $y$  се анулира тъждествено като полином на  $x$ , то  $h(x, y)$  и  $g(x, y)$  имат общ делител, зависещ от  $y$ . Поради неразложимостта на  $h \in \bar{k}[x, y]$ , този общ делител съвпада е  $h$  с точност до мултипликативна константа от  $\bar{k}^*$  и  $g \in \langle h \rangle$ . Ако  $R_y(h, g) \in \bar{k}[x] \setminus \{0\}$ , то  $R_y(h, g) = 0$  има краен брой корени  $\alpha_1, \dots, \alpha_m$ . Проекцията  $\Pi_2 : \bar{k}^2 \rightarrow \bar{k}$ ,  $\Pi_2(x, y) = x$  изобразява безкрайното множество  $Z(h) \cap Z(g)$  в крайното множество  $Z_1(R_y(h, g)) = \{\alpha_1, \dots, \alpha_m\}$ , така че поне един слой  $\Pi_2^{-1}(\alpha_i) = \{y \in \bar{k} \mid g(\alpha_i, y) = h(\alpha_i, y) = 0\}$  е безкраен. След трансляция по оста  $Ox$  можем да считаме, че  $\alpha_i = 0$ . Сега от  $g(0, y) = h(0, y) \equiv 0 \in \bar{k}[y]$  следва, че  $g(x, y)$  и  $h(x, y)$  се делят на  $x$ . Поради неразложимостта на

$h$  имаме  $h = ax$  за някое  $a \in \bar{k}^*$  и  $h$  дели  $g$ . С други думи,  $g \in \langle h \rangle$  и в този случай.

Образът  $C = \mathcal{E}(U_l)$  на  $U_l$  под действие на  $\mathcal{E}$  е  $\mathbb{F}_q$ -линеен код с дължина  $n$  и размерност

$$\dim C = \dim U_l - \dim \ker \mathcal{E} = \begin{cases} \binom{l+2}{2} - \binom{l-m+2}{2} & \text{за } l \geq m, \\ \binom{l+2}{2} & \text{за } l < m. \end{cases}$$

Твърдим, че минималното разстояние  $d$  на  $C$  е  $d \geq n - lm$ . За целта използваме съпадението на  $d$  с минималното тегло  $w$  на  $C$ . Ненулева дума  $c = (g(P_1), \dots, g(P_n)) \in C$  има нулева компонента  $g(P_i) = 0$  точно когато  $P_i \in Z(g) \cap Z(h)$ . Съгласно  $c \neq (0, \dots, 0)$  сечението  $Z(g) \cap Z(h)$  е крайно и броят на точките в него е  $|Z(g) \cap Z(h)| \leq lm$ . Следователно кодова дума  $c \in C \setminus \{(0, \dots, 0)\}$  има най-много  $lm$  нулеви компоненти или поне  $n - ml$  ненулеви компоненти. С други думи,  $d = w \geq n - ml$ .

**ЗАДАЧА 10.5.** Да се докаже, че полиномът  $f(x, y) = x^3 + x - y^2 \in \overline{\mathbb{F}_9}[x, y]$  е неразложим. Да се намерят  $\mathbb{F}_9$ -рационалните точки  $P_1, \dots, P_n \in V(\mathbb{F}_9)$  на неприводимата афинна равнинна крива

$$V = \{(x, y) \in \overline{\mathbb{F}_9}^{-2} \mid y^2 = x^3 + x\}.$$

Да се пресметнат размерността и минималното разстояние на  $\mathbb{F}_9$ -линейния код  $C = \text{im}(\mathcal{E})$ , където

$$\mathcal{E}: U_1 = \{g(x, y) = a_0 + a_1x + a_2y \mid a_i \in \mathbb{F}_9\} \longrightarrow \mathbb{F}_9^n,$$

$$\mathcal{E}(g) = (g(P_1), \dots, g(P_n)).$$

**Решение:** Да допуснем, че  $f(x, y) = g(x, y)h(x, y)$  с  $g, h \in \overline{\mathbb{F}_9}[x, y]$  е разложим. Ако  $h$  не зависи от  $x$  и  $y_i \in \overline{\mathbb{F}_9}$  е корен на  $h(y) = 0$ , то

$$f(x, y_i) = x^3 + x - y_i^2 \equiv 0 \in \overline{\mathbb{F}_9}[x]$$

е противоречие. Следователно  $g(x, y)$  и  $h(x, y)$  имат ненулеви степен

$$1 \leq \deg_x g, \deg_x h \leq \deg_x f = 3$$

относно  $x$ . Съгласно  $\deg_x g + \deg_x h = \deg_x f = 3$ , можем да предполагаем, че  $\deg_x g = 1$  и  $\deg_x h = 2$  след евентуална размяна между  $g$  и  $h$ . С други думи,

$$x^3 + x - y^2 = f(x, y) = g(x, y)h(x, y) = [a(y)x + b(y)][p(y)x^2 + q(y)x + r(y)] \quad (10.2)$$

за някакви полиноми  $a, b, p, q, r \in \overline{\mathbb{F}_9}[y]$ . Сравнявайки коефициентите на  $x^3$  в (10.2) получаваме  $a(y)p(y) \equiv 1 \in \overline{\mathbb{F}_9}[y]$ , откъдето  $a, p \in \overline{\mathbb{F}_9}^*$ ,  $p = a^{-1}$ . След умножение на  $g(x, y)$  с  $a^{-1} \in \overline{\mathbb{F}_9}$  и на  $h(x, y)$  с  $a \in \overline{\mathbb{F}_9}$  можем да считаме, че  $a(y) \equiv p(y) \equiv 1 \in \overline{\mathbb{F}_9}[y]$ . Сравняването на коефициентите на  $x^2$ ,  $x$  и  $1$  в (10.2) дава

$$b(y) + q(y) \equiv 0 \in \overline{\mathbb{F}_9}[y], \quad b(y)q(y) + r(y) \equiv 1 \in \overline{\mathbb{F}_9}[y], \quad b(y)r(y) \equiv -y^2 \in \overline{\mathbb{F}_9}[y].$$

Следователно

$$q(y) \equiv -b(y), \quad r(y) \equiv 1 + b^2(y), \quad b^3(y) + b(y) \equiv -y^2 \in \overline{\mathbb{F}_9}[y].$$

От последното равенство получаваме, че  $\deg b(y) = s \geq 1$ , откъдето  $\deg b^3(y) = 3s > s = \deg b(y)$ . Сега  $\deg(b^3(y) + b(y)) = 3s = 2 = \deg(-y^2)$  е противоречие, доказващо неразложимостта на  $f(x, y) \in \overline{\mathbb{F}_9}[x, y]$ .

Нека  $\mathbb{F}_9 = \{a + b\alpha \mid a, b \in \mathbb{F}_3\}$  за порождащия  $\alpha$  на  $\mathbb{F}_9^*$  с  $\alpha^2 = \alpha + 1$ . Вземайки предвид  $\text{Gal}(\mathbb{F}_9/\mathbb{F}_3) = \langle \Phi_3 \rangle \simeq (\mathbb{Z}_2, +)$  с  $\Phi_3(x) = x^3$ , представяме уравнението на  $V$  във вида

$$y^2 = \text{Tr}_{\mathbb{F}_9/\mathbb{F}_3}(x).$$

За  $\forall(x, y) \in V(\mathbb{F}_9)$  имаме  $y^2 = \text{Tr}_{\mathbb{F}_3}^{\mathbb{F}_9}(x) \in \mathbb{F}_3$ . Затова решенията на  $y^2 = x^3 + x$  са точно решенията на системите

$$\begin{cases} y^2 = a \\ x^3 + x = a \end{cases} \quad \text{за } \forall a \in \mathbb{F}_3.$$

Ако  $\text{Tr}_{\mathbb{F}_3}^{\mathbb{F}_9}(x) = 0$ , то  $x \in \{0, \pm(\alpha + 1)\} = \ker \text{Tr}_{\mathbb{F}_3}^{\mathbb{F}_9}$  и  $y = 0$ . Забелязваме, че  $x = -1 \in \mathbb{F}_3$  е решение на  $x^3 + x = 1$ . Съгласно линейността на следата, всички решения на  $\text{Tr}_{\mathbb{F}_3}^{\mathbb{F}_9}(x) = 1$  са  $-1 + \ker \text{Tr}_{\mathbb{F}_3}^{\mathbb{F}_9} = \{-1, \alpha, 1 - \alpha\}$ . От друга страна,  $y^2 = 1$  има решения  $y = \pm 1$ . Аналогично,  $x_2 = 1$  е решение на  $x^3 + x = -1$ . Всички решения на това уравнение са  $1 + \ker \text{Tr}_{\mathbb{F}_3}^{\mathbb{F}_9} = \{1, -\alpha, -1 + \alpha\}$ . Вече пресметнахме, че корените на  $y^2 = -1$  в  $\mathbb{F}_9$  са  $y \in \{\pm(1 + \alpha)\}$ . Следователно  $\mathbb{F}_9$ -рационалните точки на  $V$  са:

$$\begin{aligned} P_1 &= (0, 0), & P_2 &= (\alpha + 1, 0), & P_3 &= (-\alpha - 1, 0), \\ P_4 &= (-1, 1), & P_5 &= (\alpha, 1), & P_6 &= (1 - \alpha, 1), \\ P_7 &= (-1, -1), & P_8 &= (\alpha, -1), & P_9 &= (1 - \alpha, -1), \\ P_{10} &= (1, 1 + \alpha), & P_{11} &= (-\alpha, 1 + \alpha), & P_{12} &= (-1 + \alpha, 1 + \alpha), \\ P_{13} &= (1, -1 - \alpha), & P_{14} &= (-\alpha, -1 - \alpha), & P_{15} &= (-1 + \alpha, -1 - \alpha). \end{aligned}$$

Остойносттащото изображение  $\mathcal{E} : U_1 \rightarrow \mathbb{F}_9^{15}$ ,  $\mathcal{E}(f) = (f(P_1), \dots, f(P_{15}))$  е влагане, защото неразложимият над  $\overline{\mathbb{F}_9}$  полином  $y^2 - x^3 - x$  е от степен  $m = 3$ , строго по-голяма от степента  $l = 1$  на полиномите в които замества с  $P_i$ . Следователно  $C = \mathcal{E}(U_1) \subset \mathbb{F}_9^{15}$  е  $\mathbb{F}_9$ -линеен код с дължина  $n = 15$  и размерност  $\dim C = \dim U_1 = \binom{1+2}{2} = \binom{3}{2} = 3$ . Горните разглеждания доказват, че минималното разстояние  $d \geq n - ml = 15 - 3 \cdot 1 = 12$ . Достатъчно е да забележим съществуването на дума

$\mathcal{E}(y) = (0, 0, 0, 1, 1, 1, -1, -1, -1, 1 + \alpha, 1 + \alpha, 1 + \alpha, -1 - \alpha, -1 - \alpha, -1 - \alpha) \in C$  с тегло 12, за да стигнем до извода, че минималното разстояние на  $C$  е  $d = 12$ .

**Задача 10.6.** *Да се докаже, че полиномът  $f(x, y) = x^3 + x - y^4 \in \overline{\mathbb{F}_9}[x, y]$  е неразложим. Да се намерят  $\mathbb{F}_9$ -рационалните точки  $P_1, \dots, P_n \in V(\mathbb{F}_9)$  на неприводимата афинна равнинна крива*

$$V = \{(x, y) \in \overline{\mathbb{F}_9}^2 \mid y^4 = x^3 + x\}.$$

*Да се пресметнат размерността и минималното разстояние на  $\mathbb{F}_9$ -линейния код  $C = \text{im}(\mathcal{E})$ , където*

$$\begin{aligned} \mathcal{E} : U_1 &= \{g(x, y) = a_0 + a_1x + a_2y \mid a_i \in \mathbb{F}_9\} \longrightarrow \mathbb{F}_9^n, \\ \mathcal{E}(g) &= (g(P_1), \dots, g(P_n)). \end{aligned}$$