

## Рационални и затворени точки на афинни алгебрични множества

Навсякъде в този въпрос ще считаме, че  $k$  е съвършено поле. По определение това означава, че всяко крайно разширение  $F \supset k$  е сепарабелно. Като пример да споменем, че всяко поле  $k$  с характеристика  $\text{char}(k) = 0$  е съвършено, защото произволен неразложим над  $k$  полином  $f(x) \in k[x] \setminus k$  няма кратни корени. Докажем, че и всяко крайно поле  $k = \mathbb{F}_q$  е съвършено, защото произволно крайно разширение  $\mathbb{F}_{q^m} \supset \mathbb{F}_q$  на  $\mathbb{F}_q$  е сепарабелно и нормално. Алгебричната обвивка  $\bar{k}$  на съвършено поле  $k$  съвпада със сепарабелната обвивка  $k^{\text{sep}}$ . Множеството  $\bar{k}^{\text{Gal}(\bar{k}/k)} = k$  на фиксирани точки на абсолютната група на Galois  $\text{Gal}(k^{\text{sep}}/k) = \text{Gal}(\bar{k}/k)$  се изчерпва с  $k$ . По-точно, нека  $a \in \bar{k}^{\text{Gal}(\bar{k}/k)}$  има минимален полином  $f_a(x) \in k[x] \setminus k$  над  $k$ . Полето на разлагане  $E = k(a = a_1, \dots, a_m) \supseteq k$ ,  $m \leq \deg(f_a)$  на  $f_a(x)$  над  $k$  е крайно разширение на Galois на  $k$ , съдържащо  $a$ . Ограничението  $\text{Gal}(\bar{k}/k)|_E$  на абсолютната група на Galois върху  $E$  съвпада с групата на Galois  $\text{Gal}(E/k)$  на  $E$  над  $k$ . Съгласно Лема 2.11, фиксирани точки  $E^{\text{Gal}(E/k)} = k$  на групата на Galois на  $E$  над  $k$  се изчерпват с  $k$ , така че  $a \in E^{\text{Gal}(\bar{k}/k)} = E^{\text{Gal}(E/k)} = k$ .

### 1. $\mathbb{F}_q$ -рационални и $\mathbb{F}_q$ -затворени точки на афинно пространство

**ОПРЕДЕЛЕНИЕ 4.1.** Ако  $\bar{k}$  е алгебричната обвивка на съвършено поле  $k$ , а  $n$  е естествено число, то множеството  $\bar{k}^n$  на наредените  $n$ -торки  $a = (a_1, \dots, a_n)$  с компоненти  $a_i \in \bar{k}$  се нарича  $n$ -мерно афинно пространство над полето  $\bar{k}$ .

Елементите  $a = (a_1, \dots, a_n)$  на  $k^n$  се наричат  $k$ -рационални точки.

Абсолютната група на Galois  $\text{Gal}(\bar{k}/k)$  действа покомпонентно върху  $\bar{k}^n$  по правилото

$$\varphi(a_1, \dots, a_n) = (\varphi(a_1), \dots, \varphi(a_n)) \quad \text{за } \forall \varphi \in \text{Gal}(\bar{k}/k), \forall a_i \in \bar{k}.$$

Оттук следва, че  $\text{Gal}(\bar{k}/k)$ -фиксираните точки на афинното пространство  $\bar{k}^n$  са

$$(\bar{k}^n)^{\text{Gal}(\bar{k}/k)} = k^n.$$

По-точно, ако  $a = (a_1, \dots, a_n) \in (\bar{k}^n)^{\text{Gal}(\bar{k}/k)}$ , то  $\varphi(a_i) = a_i$  за всички  $1 \leq i \leq n$  и  $a_i \in k$  за всички  $1 \leq i \leq n$ .

**ОПРЕДЕЛЕНИЕ 4.2.** Ако  $a \in \overline{\mathbb{F}_q}^n$ , то  $\text{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ -орбитата  $P = \text{Orb}_{\text{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)}(a)$  на  $a$  се нарича  $\mathbb{F}_q$ -затворена точка.

Елементите на  $\mathbb{F}_q$ -затворена точка се наричат  $\mathbb{F}_q$ -спрегнати.

**ОПРЕДЕЛЕНИЕ 4.3.** Дефиниционното поле на точка  $a \in \overline{\mathbb{F}_q}^n$  над  $\mathbb{F}_q$  е разширението  $\mathbb{F}_q(a_1, \dots, a_n) \supseteq \mathbb{F}_q$  на  $\mathbb{F}_q$  чрез компонентите  $a_1, \dots, a_n \in \overline{\mathbb{F}_q}$  на  $a = (a_1, \dots, a_n)$ .

ЛЕМА-ОПРЕДЕЛЕНИЕ 4.4. *Дефиниционното поле на точка*

$$a = (a_1, \dots, a_n) \in \overline{\mathbb{F}_q}^n$$

над  $\mathbb{F}_q$  съвпада с дефиниционното поле на нейния образ

$$\varphi(a) = (\varphi(a_1), \dots, \varphi(a_n)) \in \overline{\mathbb{F}_q}^n$$

под действие на произволен автоморфизъм  $\varphi \in \text{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$  над  $\mathbb{F}_q$ .

Определяме дефиниционното поле на  $\mathbb{F}_q$ -затворена точка над  $\mathbb{F}_q$  като дефиниционното поле  $\mathbb{F}_q(a_1, \dots, a_n)$  на произволен неин елемент над  $\mathbb{F}_q$ .

**Доказателство:** Да забележим, че за произволен елемент  $\varphi \in \text{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$  полето

$$\mathbb{F}_q(\varphi(a_1), \dots, \varphi(a_n)) = \varphi(\mathbb{F}_q(a_1, \dots, a_n)) = \varphi(L)$$

е образът на  $L = \mathbb{F}_q(a_1, \dots, a_n)$  под действие на  $\varphi$ . Крайното разширение  $L \supseteq \mathbb{F}_q$  на крайното поле  $\mathbb{F}_q$  е сепарабельно и нормално, т.е. разширение на Galois. Ограничението  $\varphi|_L$  на  $\varphi \in \text{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$  върху  $L$  принадлежи на групата на Galois  $\text{Gal}(L/\mathbb{F}_q)$  и  $\varphi(L) = L$ , Q.E.D.

ТВЪРДЕНИЕ-ОПРЕДЕЛЕНИЕ 4.5. (i) *Всяка  $\mathbb{F}_q$ -затворена точка*

$$P = \text{Orb}_{\text{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)}(a), \quad a \in \overline{\mathbb{F}_q}^n$$

е крайно множество.

Броят на елементите на  $\mathbb{F}_q$ -затворена точка  $P$  се нарича степен на  $P$  и се бележи с  $\deg(P)$ .

(ii) *Степента на  $\mathbb{F}_q$ -затворена точка  $P = \text{Orb}_{\text{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)}(a)$ ,  $a = (a_1, \dots, a_n) \in \overline{\mathbb{F}_q}^n$  е минималното естествено число  $m$ , за което  $\mathbb{F}_{q^m}$  съдържа компонентите  $a_1, \dots, a_n$  на  $a$ .*

(iii) *Степента на  $\mathbb{F}_q$ -затворена точка  $P = \text{Orb}_{\text{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)}(a)$ ,  $a = (a_1, \dots, a_n) \in \overline{\mathbb{F}_q}^n$  е минималното естествено число  $m$ , за което автоморфизмът на Frobenius  $\Phi_{q^m}$  оставя на място  $a$ ,  $\Phi_{q^m}(a) = a$ .*

(iv) *Степента  $m$  на  $\mathbb{F}_q$ -затворена точка  $P = \text{Orb}_{\text{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)}(a)$ ,  $a = (a_1, \dots, a_n) \in \overline{\mathbb{F}_q}^n$  съвпада със степента  $[\mathbb{F}_q(a_1, \dots, a_n) : \mathbb{F}_q]$  на дефиниционното поле на  $P$  над  $\mathbb{F}_q$ .*

**Доказателство:** Нека  $m$  е минималното естествено число, за което  $\mathbb{F}_{q^m}$  съдържа всички компоненти  $a_1, \dots, a_n$  на точката  $a = (a_1, \dots, a_n)$ . Докажем, че  $\mathbb{F}_{q^m} \supseteq \mathbb{F}_q$  е крайно разширение на Galois, така че ограничението

$$\text{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)|_{\mathbb{F}_{q^m}} = \text{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q) = \langle \Phi_q \rangle \simeq (\mathbb{Z}_m, +)$$

на абсолютната група на Galois на  $\mathbb{F}_q$  върху  $\mathbb{F}_{q^m}$  съвпада с групата на Galois на  $\mathbb{F}_{q^m}$  относно  $\mathbb{F}_q$ . Оттук,  $\mathbb{F}_q$ -затворената точка

$$\text{Orb}_{\text{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)}(a) = \text{Orb}_{\text{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)}(a) = \{a, \Phi_q(a), \dots, \Phi_{q^{m-1}}(a)\}$$

съвпада с орбитата на точката  $a$  под действие на цикличната група от ред  $m$ , породена от автоморфизма на Frobenius  $\Phi_q$ , действащ по правилото  $\Phi_q(x) = (x_1^q, \dots, x_n^q)$  за  $\forall x \in \overline{\mathbb{F}_q}^n$ . Това доказва, че  $\mathbb{F}_q$ -затворената точка  $\text{orb}_{\text{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)}(a)$  е крайно множество. Броят на елементите на  $\text{Orb}_{\text{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)}(a)$  е равен на  $m$ , защото в противен случай съществува  $0 \leq j \leq m-1$  с  $\Phi_{q^j}(a) = a$ . Следователно всички компоненти  $a_i$  на  $a$  са корени на полинома  $x^{q^j} - x = 0$  за  $\forall 1 \leq i \leq n$  и  $a_1, \dots, a_n \in \mathbb{F}_{q^j}$ . Това противоречи на избора на  $m$  и доказва, че  $|\text{Orb}_{\text{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)}(a)| = m$ . Междувременно докажем, че степента  $m$  на  $\mathbb{F}_q$ -затворената точка съвпада с минималното естествено число, за което  $\Phi_{q^m}(a) = a$ .

От  $a_1, \dots, a_n \in \mathbb{F}_{q^m}$  и  $\mathbb{F}_q \subseteq \mathbb{F}_{q^m}$  следва, че дефиниционното поле  $\mathbb{F}_q(a_1, \dots, a_n)$  на  $a$  над  $\mathbb{F}_q$  се съдържа в  $\mathbb{F}_{q^m}$ . Ако  $\mathbb{F}_q(a_1, \dots, a_n) = \mathbb{F}_{q^s} \subseteq \mathbb{F}_{q^m}$ , то  $s$  дели  $m$  и  $s \leq m$ . Съгласно минималността на  $m$  имаме  $s = m$  и  $\mathbb{F}_q(a_1, \dots, a_n) = \mathbb{F}_{q^s} = \mathbb{F}_{q^m}$ , Q.E.D.

**ЗАДАЧА 4.6.** (i) Да се докаже, че:

(a) произволен пораждащ  $\alpha_4$  на  $\mathbb{F}_4^*$  има минимален полином  $x^2 + x + 1 \in \mathbb{F}_2[x]$  над  $\mathbb{F}_2$ , така че  $\mathbb{F}_4 = \{a + b\alpha_4 \mid a, b \in \mathbb{F}_2\}$ ;

(б) произволен пораждащ  $\alpha_8$  на  $\mathbb{F}_8^*$  има минимален полином  $x^3 + x + 1 \in \mathbb{F}_2[x]$  или  $x^3 + x^2 + 1 \in \mathbb{F}_2[x]$  над  $\mathbb{F}_2$ , така че  $\mathbb{F}_8 = \{a + b\alpha_8 + c\alpha_8^2 \mid a, b, c \in \mathbb{F}_2\}$ .

(ii) За  $\alpha_8^2 = \alpha_8 + 1$  да се намерят  $\mathbb{F}_2$ -затворените точки

$$P = \text{Orb}_{\text{Gal}(\overline{\mathbb{F}_2}/\mathbb{F}_2)}(0, \alpha_4), \quad Q = \text{Orb}_{\text{Gal}(\overline{\mathbb{F}_2}/\mathbb{F}_2)}(1, \alpha_8), \quad R = \text{Orb}_{\text{Gal}(\overline{\mathbb{F}_2}/\mathbb{F}_2)}(\alpha_4, \alpha_8)$$

върху  $\overline{\mathbb{F}_2}^{-2}$ , техните степени и дефиниционни полета над  $\mathbb{F}_2$ .

## 2. Разлагане на $\mathbb{F}_q$ -затворени точки над разширения на $\mathbb{F}_q$

**ТВЪРДЕНИЕ 4.7.** Нека  $P = \text{Orb}_{\text{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)}(a)$ ,  $a = (a_1, \dots, a_n) \in \overline{\mathbb{F}_q}^n$  е  $\mathbb{F}_q$ -затворена точка от степен  $m \in \mathbb{N}$ ,  $r$  е естествено число, а  $d = \text{GCD}(m, r) \in \mathbb{N}$  е естественният най-голям общ делител на  $m$  и  $r$ . Тогава  $P$  се разлага в непресичащо се обединение

$$P = \cup_{j=1}^d P_j \tag{4.1}$$

на  $d$  на брой  $\mathbb{F}_{q^r}$ -затворени точки  $P_j$  със степени  $\deg(P_j) = \frac{m}{d}$ .

В частност,  $P = \cup_{j=1}^m P_j$  се разлага в непресичащо се обединение на  $m$  на брой  $\mathbb{F}_{q^r}$ -рационални точки точно когато  $m$  дели  $r$ .

**Доказателство:** Да отбележим, че алгебричната обвивка  $\overline{\mathbb{F}_{q^r}} = \overline{\mathbb{F}_q}$  на  $\mathbb{F}_{q^r}$  съвпада с алгебричната обвивка на  $\mathbb{F}_q$ . От една страна, всеки елемент  $\alpha \in \overline{\mathbb{F}_q}$  е алгебричен над  $\mathbb{F}_q$ . Следователно  $\alpha$  е алгебричен над  $\mathbb{F}_{q^r}$  и  $\alpha \in \overline{\mathbb{F}_{q^r}}$ . Това доказва, че  $\overline{\mathbb{F}_q} \subseteq \overline{\mathbb{F}_{q^r}}$ . От друга страна,  $\overline{\mathbb{F}_{q^r}} = \cup_{s=1}^{\infty} \mathbb{F}_{q^{rs}} \subseteq \cup_{t=1}^{\infty} \mathbb{F}_{q^t} \subseteq \overline{\mathbb{F}_q}$ , откъдето

$$\overline{\mathbb{F}_{q^r}} = \overline{\mathbb{F}_q}.$$

Абсолютната група на Galois  $\text{Gal}(\overline{\mathbb{F}_{q^r}}/\mathbb{F}_{q^r}) = \text{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$  на  $\mathbb{F}_{q^r}$  е подгрупа на абсолютната група на Galois  $\text{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$  на  $\mathbb{F}_q$  и  $\mathbb{F}_{q^r}$ -затворената точка  $\text{Orb}_{\text{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_{q^r})}(a)$  се съдържа в  $\mathbb{F}_q$ -затворената точка  $\text{Orb}_{\text{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)}(a)$ . Съгласно Твърдение-Определение 4.5 (iv), степента

$$|\text{Orb}_{\text{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_{q^r})}(a)| = [\mathbb{F}_{q^r}(a_1, \dots, a_n) : \mathbb{F}_{q^r}]$$

на  $\mathbb{F}_{q^r}$ -затворената точка, породена от  $a \in \overline{\mathbb{F}_q}^n$  съвпада със степента на дефиниционното поле на  $a$  над  $\mathbb{F}_{q^r}$  спрямо  $\mathbb{F}_{q^r}$ . Твърдим, че  $\mathbb{F}_{q^r}(a_1, \dots, a_n) = \mathbb{F}_{q^\mu}$  за естественото най-малко общо кратно  $\mu = \text{LCM}(m, r) \in \mathbb{N}$  на  $m$  и  $r$ . Наистина,  $\mathbb{F}_{q^r} \subseteq \mathbb{F}_{q^\mu}$ , защото  $r$  дели  $\mu$ . От това, че  $m$  дели  $\mu$  получаваме включването  $\mathbb{F}_q(a_1, \dots, a_n) = \mathbb{F}_{q^m} \subseteq \mathbb{F}_{q^\mu}$ . Следователно  $\mathbb{F}_{q^r}(a_1, \dots, a_n) \subseteq \mathbb{F}_{q^\mu}$ . Ако  $\mathbb{F}_{q^r}(a_1, \dots, a_n) = \mathbb{F}_{q^s}$  за някое естествено  $s$ , то  $s$  дели  $\mu$  съгласно включването  $\mathbb{F}_{q^s} \subseteq \mathbb{F}_{q^\mu}$ . От друга страна,  $\mathbb{F}_{q^r} \subseteq \mathbb{F}_{q^r}(a_1, \dots, a_n) = \mathbb{F}_{q^s}$  и

$$\mathbb{F}_{q^m} = \mathbb{F}_q(a_1, \dots, a_n) \subseteq \mathbb{F}_{q^r}(a_1, \dots, a_n) = \mathbb{F}_{q^s}$$

изискват  $r$  да дели  $s$  и  $m$  да дели  $s$ . Оттук,  $s$  е общо кратно на  $r$  и  $m$ , така че най-малкото общо кратно  $\mu$  на  $r$  и  $m$  дели  $s$ . Естествените числа  $s$  и  $\mu$  съвпадат, защото  $s$  дели  $\mu$  и  $\mu$  дели  $s$ . В резултат,

$$|\text{Orb}_{\text{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)}(a)| = [\mathbb{F}_{q^\mu} : \mathbb{F}_{q^r}] = \frac{\mu}{r} = \frac{m}{d}$$

за естествения най-голям общ делител  $d = GCD(m, r)$  на  $m$  и  $r$ . Това доказва, че произволна  $\mathbb{F}_q$ -затворена точка  $Orb_{Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)}(a)$  от степен  $m$  се разлага в непресичащо се обединение на  $d$  на брой  $\mathbb{F}_{q^r}$ -затворени точки от степен  $\frac{m}{d}$ . В частност,  $Orb_{Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)}(a)$  се разлага в обединение на  $m$  на брой  $\mathbb{F}_{q^r}$ -рационални точки точно когато  $d = m$ . Последното е в сила тогава и само тогава, когато  $m$  дели  $r$ , Q.E.D.

Нека  $\{P_k\}_{k=1}^{\infty}$  е безкрайна редица от различни  $\mathbb{F}_q$ -затворени точки  $P_k$  с ограничени степени  $m_k \leq m$  за всички  $k \in \mathbb{N}$  и някое  $m \in \mathbb{N}$ . Тогава за всяко общо кратно  $r \in \mathbb{N}$  на числата  $1, 2, \dots, m$ , непресичащото се обединение  $\cup_{k=1}^{\infty} P_k$  се разлага в непресичащо се обединение на  $\mathbb{F}_{q^r}$ -рационални точки.

Ако безкрайната редица  $\{P_k\}_{k=1}^{\infty}$  от различни  $\mathbb{F}_q$ -затворени точки има неограничено растяща редица от степени  $\{m_k\}_{k=1}^{\infty} \subset \mathbb{N}$ , то  $\cup_{k=1}^{\infty} P_k$  не се разлага в непресичащо се обединение на  $\mathbb{F}_{q^r}$ -рационални точки за нито едно крайно разширение  $\mathbb{F}_{q^r}$  на  $\mathbb{F}_q$ . В противен случай би трябвало да съществува естествено число  $r$ , което е кратно на  $m_k$  за  $\forall k \in \mathbb{N}$ . За  $m_k > r$  получаваме противоречие, което доказва, че  $\cup_{k=1}^{\infty} P_k$  не се разлага в обединение на  $\mathbb{F}_{q^r}$ -рационални точки за нито едно  $r \in \mathbb{N}$ .

**ЗАДАЧА 4.8.** В означенията от задача 4.6 да се разложат  $\mathbb{F}_2$ -затворените точки  $P, Q, R \subset \overline{\mathbb{F}_2}^2$  в непресичащо се обединение от  $\mathbb{F}_{2^r}$ -затворени точки за  $r = 4, 6, 7$ .

**СЛЕДСТВИЕ 4.9.** Нека  $f(x) \in \mathbb{F}_q[x]$  е неразложим над  $\mathbb{F}_q$  полином от степен  $\deg(f) = m$ ,  $r \in \mathbb{N}$  е произволно естествено число, а  $d = GCD(m, r) \in \mathbb{N}$  е естественият най-голям общ делител на  $m$  и  $r$ . Тогава  $f(x) \in \mathbb{F}_{q^r}[x]$  се разлага в произведение  $f(x) = f_1(x) \dots f_d(x)$  на  $d$  на брой неразложими над  $\mathbb{F}_{q^r}$  полиноми  $f_j(x) \in \mathbb{F}_{q^r}[x]$  от степен  $\deg(f_j) = \frac{m}{d}$ .

**Доказателство:** Достатъчно е да проверим, че  $\mathbb{F}_q$ -затворените точки на  $\overline{\mathbb{F}_q}$  са точно множествата на корените на неразложимите над  $\mathbb{F}_q$  полиноми  $f(x) \in \mathbb{F}_q[x]$ .

Нека

$$f(x) = \prod_{i=1}^m (x - \alpha_i) \in \mathbb{F}_q[x]$$

е неразложим над  $\mathbb{F}_q$  полином с корени  $\alpha_1, \dots, \alpha_m$  от подходящо разширение на  $\mathbb{F}_q$ . Тогава  $f(\alpha_1) = 0$  и за всяко  $\varphi \in Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$  имаме  $0 = \varphi(0) = \varphi(f(\alpha_1)) = f(\varphi(\alpha_1))$ , защото коефициентите на  $f$  остават на място под действие на  $\varphi$ . Следователно  $\mathbb{F}_q$ -затворената точка

$$Orb_{Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)}(\alpha_1) \subseteq \{\alpha_1, \dots, \alpha_m\}$$

се съдържа в множеството на корените на  $f(x)$ . Съгласно Твърдение-Определение 4.5 (iv), степента  $|Orb_{Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)}(\alpha_1)| = [\mathbb{F}_q(\alpha_1) : \mathbb{F}_q]$  на  $Orb_{Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)}(\alpha_1)$  съвпада със степента на дефиниционното поле  $\mathbb{F}_q(\alpha_1)$  на  $\alpha_1$  над  $\mathbb{F}_q$  относно  $\mathbb{F}_q$ . Нееразложимият над  $\mathbb{F}_q$  полином  $f(x) \in \mathbb{F}_q[x]$  със старши коефициент 1 и корен  $\alpha_1$  е минималният полином на  $\alpha_1$  над  $\mathbb{F}_q$ , така че

$$[\mathbb{F}_q(\alpha_1) : \mathbb{F}_q] = \deg_{\mathbb{F}_q} \alpha_1 = \deg f = m$$

и  $\mathbb{F}_q$ -затворената точка  $Orb_{Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)}(\alpha_1)$  от степен  $m$  съвпада с множеството на корените  $\{\alpha_1, \dots, \alpha_m\}$  на  $f$ .

Обратно, нека  $Orb_{Gal(\overline{\mathbb{F}}_q/\mathbb{F}_q)}(\alpha) = \{\alpha, \Phi(\alpha), \dots, \Phi^{q^m-1}(\alpha)\}$  е  $\mathbb{F}_q$ -затворена точка от степен  $m$ , съдържаща се в афинната права  $\overline{\mathbb{F}}_q$ . Разглеждаме полинома

$$g(x) = \prod_{i=0}^{m-1} (x - \Phi_{q^i}(\alpha)).$$

Автоморфизмът на Frobenius  $\Phi_q$  действа върху корените  $\alpha, \Phi_q(\alpha), \dots, \Phi_{q^{m-1}}(\alpha)$  на  $g(x)$  и запазва коефициентите на този полином. Следователно  $g(x) \in \mathbb{F}_q[x]$ . Нека  $f(x) \in \mathbb{F}_q$  е неразложимият над  $\mathbb{F}_q$  множител на  $g(x)$  с корен  $\alpha$  и старши коефициент 1. Тогава  $\mathbb{F}_q$ -затворената точка  $Orb_{Gal(\overline{\mathbb{F}}_q/\mathbb{F}_q)}(\alpha)$  съвпада с множеството на корените на  $f(x)$ . Отгук,  $f(x) \in \mathbb{F}_q[x]$  и  $g(x) \in \mathbb{F}_q[x]$  са полиноми с едни и същи корени и старши коефициент 1, така че  $f(x) \equiv g(x)$  съвпадат като полиноми на една променлива. Това доказва неразложимостта на  $g(x) \in \mathbb{F}_q[x]$  над  $\mathbb{F}_q$ , Q.E.D.

**ЗАДАЧА 4.10.** *Да се докаже, че:*

(i) *за всяко естествено число  $k$  полиномът  $x^2 + x + 1 \in \mathbb{F}_2[x]$  е неразложим над  $\mathbb{F}_{2^{2k-1}}$  и се разлага в линейни множители над  $\mathbb{F}_{2^{2k}}$ .*

(ii) *за всяко естествено число  $k$  полиномите  $x^3 + x + 1 \in \mathbb{F}_2[x]$  и  $x^3 + x^2 + 1 \in \mathbb{F}_2[x]$  се разлагат в линейни множители над  $\mathbb{F}_{2^{3k}}$ .*

*Неразложим ли е полиномът  $x^3 + x + 1 \in \mathbb{F}_2[x]$  над полето  $\mathbb{F}_{2^{2011}}$ ? А над  $\mathbb{F}_{2^{2012}}$ ?*

### 3. $\mathbb{F}_q$ -рационални и $\mathbb{F}_q$ -затворени точки на афинни алгебрични множества, определени над $\mathbb{F}_q$

Сега ще въведем афинните алгебрични множество и ще разгледаме някои операции с тях.

**ОПРЕДЕЛЕНИЕ 4.11.** *Ако  $S \subseteq \overline{k}[x_1, \dots, x_n]$  е множество от полиноми на  $x_1, \dots, x_n$  с коефициенти от  $\overline{k}$ , то множеството на нулите*

$$Z(S) = \{a \in \overline{k}^n \mid f(a) = 0 \text{ за } \forall f \in S\}$$

*на  $S$  в афинното пространство  $\overline{k}^n$  се нарича афинно алгебрично множество. Ако  $S \subseteq k[x_1, \dots, x_n]$  е множество от полиноми с коефициенти от  $k$ , казваме, че афинното алгебрично множество  $Z(S)$  е определено над  $k$  и записваме  $Z(S)/k$ .*

*Ако  $Z(S)/k$  е афинно алгебрично множество, определено над  $k$ , то сечението*

$$Z(S) \cap k^n = Z(S)(k)$$

*се нарича множество на  $k$ -рационалните точки на  $Z(S)$ .*

Нека  $k$  е съвършено поле. Действието на елемент  $\varphi \in Gal(\overline{k}/k)$  върху коефициентите на полином  $f(x) \in \overline{k}[x_1, \dots, x_n]$  задава действие на  $Gal(\overline{k}/k)$  върху  $\overline{k}[x_1, \dots, x_n]$ ,

$$\varphi \left( \sum_{i=(i_1, \dots, i_n)} a_i x_1^{i_1} \dots x_n^{i_n} \right) = \sum_{i=(i_1, \dots, i_n)} \varphi(a_i) x_1^{i_1} \dots x_n^{i_n} \in \overline{k}[x_1, \dots, x_n].$$

Полиномът  $f(x_1, \dots, x_n) \in \overline{k}[x_1, \dots, x_n]$  остава на място под действие на групата на Galois  $Gal(\overline{k}/k)$  тогава и само тогава, когато  $f(x_1, \dots, x_n) \in k[x_1, \dots, x_n]$  е с коефициенти от  $k$ .

Ако  $f(x_1, \dots, x_n) \in \overline{k}[x_1, \dots, x_n]$ ,  $a = (a_1, \dots, a_n) \in \overline{k}^n$  и  $\varphi \in Gal(\overline{k}/k)$ , то

$$\varphi(f(a_1, \dots, a_n)) = \varphi \left( \sum_{i=(i_1, \dots, i_n)} c_i a_1^{i_1} \dots a_n^{i_n} \right) =$$

$$= \sum_{i=(i_1, \dots, i_n)} \varphi(c_i) \varphi(a_1)^{i_1} \dots \varphi(a_n)^{i_n} = \varphi(f)(\varphi(a)).$$

Нека  $k$  е съвършено поле, а  $Z(S)/k$  е афинно алгебрично множество, определено над  $k$ . Тогава абсолютната група на Galois  $Gal(\bar{k}/k)$  действа върху  $Z(S)$  и фиксираните точки за това действие са  $k$ -рационалните. Наистина, за всяко  $a \in Z(S)$  и всяко  $\varphi \in Gal(\bar{k}/k)$  имаме  $\varphi(a) \in Z(S)$ , защото произволен полином  $f \in S \subset k[x_1, \dots, x_n]$  има нулева стойност  $f(a) = 0$  в  $a$ , откъдето  $0 = \varphi(f(a)) = f(\varphi(a))$ . Точката  $a \in Z(S)$  остава на място под действие на  $Gal(\bar{k}/k)$  точно когато  $a \in k^n$ .

Оттук следва, че ако  $Z(S)/\mathbb{F}_q$  е афинно алгебрично множество, определено над  $\mathbb{F}_q$  и  $a \in Z(S)$ , то  $\mathbb{F}_q$ -затворената точка  $P = Orb_{Gal(\bar{\mathbb{F}}_q/\mathbb{F}_q)}(a)$  върху  $\bar{\mathbb{F}}_q^n$ , породена от  $a$  се съдържа изцяло в  $Z(S)$ . Затова казваме, че  $P = Orb_{Gal(\bar{\mathbb{F}}_q/\mathbb{F}_q)}(a)$  е  $\mathbb{F}_q$ -затворена точка на  $Z(S)$ .

**ПРИМЕР 4.12.** За произволен полином  $f(x) \in \mathbb{F}_2[x]$ , афинното алгебрично множество

$$X = \{(x, y) \in \bar{\mathbb{F}}_2^2 \mid y = f(x)\}$$

е афинна крива, определена над  $\mathbb{F}_2$  и изоморфна на  $\bar{\mathbb{F}}_2$ . За всяко естествено число  $n$ ,  $\mathbb{F}_2^n$ -рационалните точки  $X(\mathbb{F}_2^n) = \{(x, f(x)) \mid x \in \mathbb{F}_2^n\} \simeq \mathbb{F}_2^n$ .

**ПРИМЕР 4.13.** Множеството

$$Y = \{(x, y) \in \bar{\mathbb{F}}_2^2 \mid y^2 + y = x^3 + x\}$$

е афинна алгебрична крива, определена над  $\mathbb{F}_2$ . Тя има  $\mathbb{F}_2$ -рационални точки  $Y(\mathbb{F}_2) = \mathbb{F}_2^2$  и  $\mathbb{F}_4$ -рационални точки  $Y(\mathbb{F}_4) = Y(\mathbb{F}_2) = \mathbb{F}_2^2$ .

Ако  $a, b \in \mathbb{F}_2$ , то  $b^2 + b = 2b = 0$ ,  $a^3 + a = 2a = 0$ , така че  $b^2 + b = a^3 + a$  и  $\forall (a, b) \in \mathbb{F}_2^2$  е  $\mathbb{F}_2$ -рационална точка на  $Y$ . Твърдим, че не съществуват  $\mathbb{F}_4$ -рационални точки на  $Y$ , които не са  $\mathbb{F}_2$ -рационални. Наистина, ако  $(x, y) \in Y(\mathbb{F}_4)$  и  $x = 0$ , то решенията на  $y^2 + y = y(y+1) = 0$  съвпадат с  $\mathbb{F}_2$ . Ако  $(x, y) \in Y(\mathbb{F}_4)$  и  $x \in \mathbb{F}_4^*$ , то  $x^3 = 1$  и  $1 + x = x^3 + x = y^2 + y = \text{Tr}_{\mathbb{F}_4/\mathbb{F}_2}(y) \in \mathbb{F}_2$ . Следователно  $x = 1 \in \mathbb{F}_2$  и решенията на  $y^2 + y = 0$  съставят  $\mathbb{F}_2$ , така че отново  $(x, y) \in Y(\mathbb{F}_2)$ . Това доказва, че  $Y(\mathbb{F}_4) = Y(\mathbb{F}_2)$ .

Продължаваме с някои елементарни свойства на афинните алгебрични множества:

**ЛЕМА 4.14.** За произволно подмножество  $S \subseteq \bar{k}[x_1, \dots, x_n]$  да означим с  $Z(S) \subseteq \bar{k}^n$  афинното алгебрично множество, определено от  $S$ . Тогава:

(i)  $Z(0) = \bar{k}^n$ .

(ii)  $Z(\bar{k}[x_1, \dots, x_n]) = \emptyset$ .

(iii)  $Z(S) = Z(\langle S \rangle)$  за идеала  $\langle S \rangle \triangleleft \bar{k}[x_1, \dots, x_n]$ , породен от  $S \subseteq \bar{k}[x_1, \dots, x_n]$ .

**Доказателство:** (i) Тъждествено нулевият полином  $0 \in \bar{k}[x_1, \dots, x_n]$  се анулира във всяка точка  $a = (a_1, \dots, a_n) \in \bar{k}^n$ .

(ii) Елементите на мултипликативната група  $\bar{k}^*$  на полето  $\bar{k}$  не се анулират в нито една точка на афинното пространство  $\bar{k}^n$ .

(iii) Ако  $a \in Z(S) \subset \bar{k}^n$ , то за произволен полином  $f = \sum_{i=1}^m f_i g_i \in \langle S \rangle$  с  $f_i \in S$ ,

$$g_i \in \bar{k}[x_1, \dots, x_n] \text{ е в сила } f(a) = \sum_{i=1}^m f_i(a) g_i(a) = \sum_{i=1}^m 0 \cdot g_i(a) = 0. \text{ Следователно}$$

$$Z(S) \subset Z(\langle S \rangle).$$

За  $a \in Z(\langle S \rangle)$  и  $f \in S \subset \langle S \rangle$  имаме  $f(a) = 0$ , така че  $Z(\langle S \rangle) \subseteq Z(S)$  и  $Z(S) = Z(\langle S \rangle)$ , Q.E.D.

**ЛЕМА-ОПРЕДЕЛЕНИЕ 4.15.** *За произволно подмножество  $Z \subseteq \bar{k}^n$  на афинното пространство  $\bar{k}^n$ , множеството на полиномите*

$$I(Z) := \{f \in \bar{k}[x_1, \dots, x_n] \mid f(a_1, \dots, a_n) = 0 \text{ за } \forall a = (a_1, \dots, a_n) \in Z\},$$

*които се анулират във всяка точка на  $Z$  е идеал в  $\bar{k}[x_1, \dots, x_n]$ , наречен идеал на множеството  $Z$  над  $\bar{k}$ .*

*За произволно подмножество  $Z \subseteq \bar{k}^n$  можем да разгледаме и идеала*

$$I_k(Z) := \{f \in k[x_1, \dots, x_n] \mid f(a_1, \dots, a_n) = 0 \text{ за } \forall a = (a_1, \dots, a_n) \in Z\}$$

*на  $Z$  над  $k$ .*

Следващата лема доказва, че съответствието между подмножества от полиноми  $S \subset k[x_1, \dots, x_n]$  и афинните алгебрични множества  $Z(S) \subseteq \bar{k}^n$ , определени от тях обръща включванията

**ЛЕМА 4.16.** *Съответствието между множества от полиноми и афинни алгебрични множества обръща включванията. По-точно:*

(i) *ако  $S \subset T \subseteq \bar{k}[x_1, \dots, x_n]$ , то  $Z(S) \supseteq Z(T)$ ;*

(ii) *ако  $Z \subset W \subseteq \bar{k}^n$ , то  $I(Z) \supseteq I(W)$ .*

**Доказателство:** (i) За  $\forall a \in Z(T) \subseteq \bar{k}^n$  и  $\forall f \in S \subset T$  е изпълнено  $f(a) = 0$ , така че  $a \in Z(S)$ .

(ii) Ако  $f \in I(W)$ , то за всяка точка  $a \in Z \subset W$  е в сила  $f(a) = 0$ . Следователно  $f \in I(Z)$ , Q.E.D.

**ПРИМЕР 4.17.** *Афинните алгебрични подмножества на правата  $\bar{k}$  са  $\emptyset$ ,  $\bar{k}$  и крайните подмножества.*

Да напомним, че идеалите в пръстена  $\bar{k}[x]$  на полиномите на една променлива  $x$  с коефициенти от  $\bar{k}$  са  $\bar{k}[x]$ ,  $0$  и главните идеали  $\langle f(x) \rangle$ , породени от полиноми  $f(x) \in \bar{k}[x] \setminus \bar{k}$ . Следователно афинните алгебрични подмножества на  $\bar{k}$  са  $Z(\bar{k}[x]) = \emptyset$ ,  $Z(0) = \bar{k}$  и множествата  $Z(\langle f \rangle) = Z(f)$  на корените на  $f$ . Вземайки предвид, че  $Z(f)$  се състои от  $\deg(f) \in \mathbb{N}$  точки, броени с кратности, стигаме до извода, че афинните алгебрични подмножества на афинната права  $\bar{k}$  са  $\emptyset$ ,  $\bar{k}$  и крайните подмножества.

**ЛЕМА 4.18.** (i) *Ако  $S_\alpha \subseteq k[x_1, \dots, x_n]$ ,  $\alpha \in A$  са множества от полиноми, то афинното алгебрично множество*

$$Z(\cup_{\alpha \in A} S_\alpha) = \cap_{\alpha \in A} Z(S_\alpha).$$

(ii) *Ако  $I_\alpha$ ,  $\alpha \in A$  са идеали в  $k[x_1, \dots, x_n]$ , то*

$$Z\left(\sum_{\alpha \in A} I_\alpha\right) = \cap_{\alpha \in A} Z(I_\alpha).$$

(iii) *Ако  $Z_\alpha \subseteq \bar{k}^n$ ,  $\alpha \in A$  са подмножества на афинното пространство  $\bar{k}^n$ , то идеалът на обединението им е*

$$I(\cup_{\alpha \in A} Z_\alpha) = \cap_{\alpha \in A} I(Z_\alpha).$$

**Доказателство:** (i) От  $S_\alpha \subseteq \cup_{\alpha \in A} S_\alpha$  следва  $Z(\cup_{\alpha \in A} S_\alpha) \subseteq Z(S_\alpha)$  за всяко  $\alpha \in A$ . В резултат,  $Z(\cup_{\alpha \in A} S_\alpha) \subseteq \cap_{\alpha \in A} Z(S_\alpha)$ . Обратно, ако  $a \in \cap_{\alpha \in A} Z(S_\alpha)$  и  $f \in \cup_{\alpha \in A} S_\alpha$ , то  $f \in S_\alpha$  за някое  $\alpha \in A$  и  $f(a) = 0$ . Това доказва включването  $\cap_{\alpha \in A} Z(S_\alpha) \subseteq Z(\cup_{\alpha \in A} S_\alpha)$ .

(ii) От  $I_\alpha \subseteq \sum_{\alpha \in A} I_\alpha$  получаваме  $Z\left(\sum_{\alpha \in A} I_\alpha\right) \subseteq Z(I_\alpha)$  за  $\forall \alpha \in A$ . Това доказва, че  $Z\left(\sum_{\alpha \in A} I_\alpha\right) \subseteq \cap_{\alpha \in A} Z(I_\alpha)$ . Обратно, за произволна точка  $a \in \cap_{\alpha \in A} Z(I_\alpha)$

и произволен полином  $f = \sum_{i=1}^k f_{\alpha_i} \in \sum_{\alpha \in A} I_{\alpha}$  с  $f_{\alpha_i} \in I_{\alpha_i}$ ,  $\alpha_i \in A$  имаме  $f(a) = \sum_{i=1}^k f_{\alpha_i}(a) = 0 + \dots + 0 = 0$ , защото  $a \in V(I_{\alpha_i})$  за  $\forall 1 \leq i \leq k$ . Оттук  $\cap_{\alpha \in A} Z(I_{\alpha}) \subseteq Z\left(\sum_{\alpha \in A} I_{\alpha}\right)$ .

(iii) Възоснова на Лема 4.16 (ii), от  $Z_{\alpha} \subseteq \cup_{\alpha \in A} Z_{\alpha}$  следва  $I(\cup_{\alpha \in A} Z_{\alpha}) \subseteq I(Z_{\alpha})$  за всяко  $\alpha \in A$ , така че  $I(\cup_{\alpha \in A} Z_{\alpha}) \subseteq \cap_{\alpha \in A} I(Z_{\alpha})$ . За произволна точка  $a \in \cup_{\alpha \in A} Z_{\alpha}$  съществува индекс  $\alpha_o \in A$  с  $a \in Z_{\alpha_o}$ . Следователно полиномите  $f \in \cap_{\alpha \in A} I(Z_{\alpha}) \subseteq I(Z_{\alpha_o})$  се анулират в  $a$  и  $\cap_{\alpha \in A} I(Z_{\alpha}) \subseteq I(\cup_{\alpha \in A} Z_{\alpha})$ , Q.E.D.

ЛЕМА 4.19. (i) Ако  $I_j \triangleleft \bar{k}[x_1, \dots, x_n]$  са идеали в  $k[x_1, \dots, x_n]$ , то произведението им определя афинното алгебрично множество

$$Z(I_1 \dots I_m) = \cup_{j=1}^m Z(I_j).$$

(ii) Произведението  $S_1 S_2 \dots S_m := \{f_1 \dots f_m \mid f_j \in S_j\}$  на произволни подмножества от полиноми  $S_j \subseteq \bar{k}[x_1, \dots, x_n]$  определя афинното алгебрично множество

$$Z(S_1 S_2 \dots S_m) = \cup_{j=1}^m Z(S_j);$$

(iii) Ако  $I_j \triangleleft \bar{k}[x_1, \dots, x_n]$  са идеали в  $\bar{k}[x_1, \dots, x_n]$ , то сечението им определя афинното алгебрично множество

$$Z(I_1 \cap \dots \cap I_m) = Z(I_1) \cup \dots \cup Z(I_m).$$

**Доказателство:** (i) Прилагайки Лема 4.16 (i), от  $I_1 \dots I_j \dots I_m \subseteq I_j$  получаваме обратното включване  $Z(I_1 \dots I_j \dots I_m) \supseteq Z(I_j)$  за  $\forall 1 \leq j \leq m$ . Това доказва включването  $Z(I_1 \dots I_m) \supseteq \cup_{j=1}^m Z(I_j)$ .

Да допуснем, че съществува точка  $a \in Z(I_1 \dots I_m) \setminus (\cup_{j=1}^m Z(I_j))$ . Тогава за всяко  $1 \leq j \leq m$  можем да изберем полином  $f_j \in I_j$  с  $f_j(a) \neq 0$ , така че  $(f_1 \dots f_j \dots f_m)(a) = f_1(a) \dots f_j(a) \dots f_m(a) \neq 0$ . Съгласно  $f_1 \dots f_j \dots f_m \in I_1 \dots I_m$ , това противоречи на  $a \in Z(I_1 \dots I_m)$  и доказва, че  $Z(I_1 \dots I_m) = \cup_{j=1}^m Z(I_j)$ .

(ii) Първо ще проверим съвпадението на идеалите

$$\langle S_1 \dots S_m \rangle = \langle S_1 \rangle \dots \langle S_m \rangle.$$

Всеки елемент  $g \in \langle S_1 \dots S_m \rangle$  е крайна сума на полиноми от вида  $f_1 \dots f_m h$  с  $f_j \in S_j$ ,  $1 \leq j \leq m$ ,  $h \in \bar{k}[x_1, \dots, x_n]$ . От  $f_j \in \langle S_j \rangle$  за  $1 \leq j \leq m$  и  $f_m h \in \langle S_m \rangle$  следва, че  $f_1 \dots f_m h \in \langle S_1 \rangle \dots \langle S_m \rangle$ , откъдето  $g \in \langle S_1 \rangle \dots \langle S_m \rangle$ . Обратно, всеки елемент  $p \in \langle S_1 \rangle \dots \langle S_m \rangle$  е крайна сума на полиноми от вида  $p_1 \dots p_m$  с  $p_j \in \langle S_j \rangle$ ,  $1 \leq j \leq m$ . От своя страна, всяко  $p_j$  е крайна сума на  $f_{j,s_j} q_{j,s_j}$  с  $f_{j,s_j} \in S_j$ ,  $q_{j,s_j} \in \bar{k}[x_1, \dots, x_n]$ ,  $s_j \in \mathbb{N}$ . Следователно  $p$  е крайна сума на полиноми от вида  $r_{s_1, \dots, s_m} = (f_{1,s_1} q_{1,s_1}) \dots (f_{m,s_m} q_{m,s_m}) = f_{1,s_1} \dots f_{m,s_m} (q_{1,s_1} \dots q_{m,s_m})$ . Съгласно  $f_{1,s_1} \dots f_{m,s_m} \in S_1 \dots S_m$  имаме  $r_{s_1, \dots, s_m} \in \langle S_1 \dots S_m \rangle$ , откъдето  $p \in \langle S_1 \dots S_m \rangle$ . Това доказва  $\langle S_1 \rangle \dots \langle S_m \rangle \subseteq \langle S_1 \dots S_m \rangle$ .

Прилагайки доказаното условие (i) към идеалите  $I_j = \langle S_j \rangle$ , получаваме, че

$$Z(\langle S_1 \rangle \dots \langle S_m \rangle) = \cup_{j=1}^m Z(\langle S_j \rangle).$$

Съгласно  $\langle S_1 \rangle \dots \langle S_m \rangle = \langle S_1 \dots S_m \rangle$  имаме

$$Z(\langle S_1 \dots S_m \rangle) = \cup_{j=1}^m Z(\langle S_j \rangle).$$

Прилагаме Лема 4.14 (iii) и получаваме равенствата  $Z(\langle S_1 \dots S_m \rangle) = Z(S_1 \dots S_m)$  и  $Z(\langle S_j \rangle) = Z(S_j)$ , откъдето  $Z(S_1 \dots S_m) = \cup_{j=1}^m Z(S_j)$ .



(iii) От  $I_1 \dots I_m \subseteq I_1 \cap \dots \cap I_m \subseteq I_j$  следва  $Z(I_j) \subseteq Z(I_1 \cap \dots \cap I_m) \subseteq Z(I_1 \dots I_m)$  за  $\forall 1 \leq j \leq m$ , съгласно Лема 4.16 (i). Следователно

$$Z(I_j) \cup \dots \cup Z(I_m) \subseteq Z(I_1 \cap \dots \cap I_m) \subseteq Z(I_1 \dots I_m).$$

Комбинирайки с доказаното условие (i) получаваме (iii), Q.E.D.

#### 4. Топология на Зариски.

ОПРЕДЕЛЕНИЕ 4.20. Топология върху множество  $X$  е фамилия

$\mathcal{U} = \{U_\alpha\}_{\alpha \in A}$  от подмножества, така че

(i)  $X \in \mathcal{U}$ ,  $\emptyset \in \mathcal{U}$ ;

(ii)  $\cup_{\alpha \in \Sigma} U_\alpha \in \mathcal{U}$  за произволни подмножества  $\Sigma \subseteq A$ ;

(iii)  $U_{\alpha_1} \cap \dots \cap U_{\alpha_k} \in \mathcal{U}$  за произволни крайни подмножества  $\{\alpha_1, \dots, \alpha_k\} \subseteq A$ . Подмножествата  $U_\alpha \in \mathcal{U}$  се наричат отворени, а допълненията им  $Z_\alpha = X \setminus U_\alpha$  са затворени.

Множество  $X$ , снабдено с топология  $\mathcal{U} = \{U_\alpha\}_{\alpha \in A}$  се нарича топологично пространство.

Топология върху  $X$  може да се зададе с фамилия  $\mathcal{Z} = \{Z_\alpha\}_{\alpha \in A}$  от затворени подмножества, така че

(i)  $\emptyset \in \mathcal{Z}$ ,  $X \in \mathcal{Z}$ ;

(ii)  $\cap_{\alpha \in \Sigma} Z_\alpha \in \mathcal{Z}$  за  $\forall \Sigma \subseteq A$ ;

(iii)  $Z_{\alpha_1} \cup \dots \cup Z_{\alpha_k} \in \mathcal{Z}$  за  $\forall \{\alpha_1, \dots, \alpha_k\} \subseteq A$ .

Твърдим, че когато  $S$  пробягва подмножествата на  $\bar{k}[x_1, \dots, x_n]$ , афините алгебрични множества  $Z(S) \subseteq \bar{k}^n$  образуват фамилия от затворени подмножества на афинното пространство  $\bar{k}^n$ . Това следва от Лема 4.14 (i), (ii), Лема 4.18 (ii) и Лема 4.19 (ii).

ОПРЕДЕЛЕНИЕ 4.21. Топологията върху  $\bar{k}^n$ , чиито затворени подмножества  $\mathcal{Z} = \{V(S)\}_{S \subseteq \bar{k}[x_1, \dots, x_n]}$  са афинните алгебрични множества  $Z(S) \subseteq \bar{k}^n$  за произволни  $S \subseteq \bar{k}[x_1, \dots, x_n]$  се нарича топология на Зариски върху  $\bar{k}^n$ .

ОПРЕДЕЛЕНИЕ 4.22. Затворената обвивка  $\bar{M}$  на подмножество  $M$  на топологично пространство  $X$  е сечението

$$\bar{M} = \cap_{Z \supseteq M} Z$$

на всички затворени подмножества  $Z \subseteq X$ , съдържащи  $M$ .

Затворената обвивка  $\bar{M}$  на  $M$  е минималното затворено подмножество на  $X$ , съдържащо  $M$ . Да отбележим, че подмножеството  $M$  е затворено тогава и само тогава, когато  $M = \bar{M}$ .

ЛЕМА 4.23. Ако  $M \subseteq \bar{k}^n$  е подмножество на афинното пространство  $\bar{k}^n$ , то Зариски затворената обвивка

$$\bar{M} = ZI(M)$$

съпада с афинното многообразие на идеала  $I(M) \triangleleft \bar{k}[x_1, \dots, x_n]$  на  $M$ .

В частност, ако  $X \subseteq \bar{k}^n$  е афинно алгебрично множество, то  $X = ZI(X)$ .

**Доказателство:** По определение, всеки полином  $f \in I(M)$  се анулира върху  $M$ , така че  $M \subseteq ZI(M)$ . Следователно затвореното множество  $ZI(M)$  участва в сечението  $\cap_{Z \supseteq M} Z = \bar{M}$  и го съдържа,  $ZI(M) \supseteq \bar{M}$ .

За обратното включване  $ZI(M) \subseteq \bar{M} = \cap_{Z \supseteq M} Z$  е достатъчно да проверим, че  $ZI(M) \subseteq Z$  за всяко Зариски затворено подмножество  $Z \subseteq \bar{k}^n$ , съдържащо  $M$ . По определение,  $Z = Z(S)$  за някакво множество от полиноми  $S \subseteq \bar{k}[x_1, \dots, x_n]$ . Условието  $M \subseteq Z(S)$  означава анулиране на всички полиноми  $f \in S$  в точките

$a \in M$ ,  $f(a) = 0$ . Следователно  $S \subseteq I(M)$ , откъдето  $Z = Z(S) \supseteq ZI(M)$  съгласно Лема 4.16 (i), Q.E.D.

**ЗАДАЧА 4.24.** Да се докаже, че  $\mathbb{Z}^n$  не е афинно алгебрично подмножество на  $\mathbb{C}^n$ .

**Упътване:** Използвайте, че произволен полином  $f \in I(\mathbb{Z}^n) \setminus \{0\}$  има представяне

$$f(x_1, \dots, x_{n-1}, x_n) = \sum_{i=0}^d c_i(x_1, \dots, x_{n-1})x_n^i \in \mathbb{C}[x_1, \dots, x_{n-1}][x_n]$$

с коефициенти  $c_i(x_1, \dots, x_{n-1}) \in I(\mathbb{Z}^{n-1}) \triangleleft \mathbb{C}[x_1, \dots, x_{n-1}]$ , за да изведете, че идеалът  $I(\mathbb{Z}^n) = 0$ . Следователно  $\mathbb{Z}^n \not\subseteq ZI(\mathbb{Z}^n) = \mathbb{C}^n$  не е Зариски затворено подмножество.

**ЛЕМА-ОПРЕДЕЛЕНИЕ 4.25.** Нека  $M$  е затворено подмножество на топологично пространство  $X$  с фамилия от затворени подмножества  $\mathcal{Z} = \{Z_\alpha\}_{\alpha \in A}$ . Тогава  $\mathcal{Z} \cap M := \{Z_\alpha \cap M\}_{\alpha \in A}$  е фамилия от затворени подмножества на  $M$  и топологията върху  $M$  със затворени подмножества  $\mathcal{Z} \cap M$  се нарича индуцирана от топологията върху  $X$ .

В частност, топологията на Зариски върху афинното пространство  $\bar{k}^n$  индуцира топология на Зариски върху произволно афинно алгебрично подмножество  $X \subseteq \bar{k}^n$  с фамилия от затворени подмножества  $\{X \cap Z(S)\}_{S \subseteq \bar{k}[x_1, \dots, x_n]}$ .

**Доказателство:** От  $\emptyset, X \in \mathcal{Z}$  следва  $\emptyset \cap M = \emptyset, X \cap M = M \in \mathcal{Z} \cap M$ . За произволно подмножество  $A_o \subseteq A$  имаме

$$\bigcap_{\alpha \in A_o} (Z_\alpha \cap M) = (\bigcap_{\alpha \in A_o} Z_\alpha) \cap M \in \mathcal{Z} \cap M.$$

Достатъчно е да проверим, че

$$(Z_{\alpha_1} \cap M) \cup \dots \cup (Z_{\alpha_m} \cap M) = (Z_{\alpha_1} \cup \dots \cup Z_{\alpha_m}) \cap M,$$

за да твърдим, че  $(Z_{\alpha_1} \cap M) \cup \dots \cup (Z_{\alpha_m} \cap M) \in \mathcal{Z} \cap M$  и  $\mathcal{Z} \cap M$  образува фамилия от затворени подмножества на  $M$ . Наистина, от

$$Z_{\alpha_j} \cap M \subseteq (Z_{\alpha_1} \cup \dots \cup Z_{\alpha_m}) \cap M$$

следва  $(Z_{\alpha_1} \cap M) \cup \dots \cup (Z_{\alpha_m} \cap M) \subseteq (Z_{\alpha_1} \cup \dots \cup Z_{\alpha_m}) \cap M$ . Обратно, ако  $z \in (Z_{\alpha_1} \cup \dots \cup Z_{\alpha_m}) \cap M$ , то съществува  $1 \leq j \leq m$ , така че  $z \in Z_{\alpha_j} \cap M$  и  $(Z_{\alpha_1} \cup \dots \cup Z_{\alpha_m}) \cap M \subseteq (Z_{\alpha_1} \cap M) \cup \dots \cup (Z_{\alpha_m} \cap M)$ , Q.E.D.

**ОПРЕДЕЛЕНИЕ 4.26.** База  $\mathcal{B} = \{U_\beta\}_{\beta \in B}$  на топология  $\mathcal{U} = \{U_\alpha\}_{\alpha \in A}$  е подфамилия  $\mathcal{B} \subset \mathcal{U}$  от отворени подмножества, така че всяко отворено множество  $U_\alpha \in \mathcal{U}$  може да се представи като обединение  $U_\alpha = \bigcup_{\beta \in \Sigma(\alpha)} U_\beta$  на множества  $U_\beta$  от базата, индексирани с подмножество  $\Sigma(\alpha)$  на  $B$ , зависещо от  $\alpha$ .

**ОПРЕДЕЛЕНИЕ 4.27.** За произволни полиноми  $f$  извън идеала  $I(X)$  на афинно алгебрично множество  $X$ , подмножествата

$$U_f = \{x \in X \mid f(x) \neq 0\}$$

се наричат главни Зариски отворени подмножества на  $X$ .

**ЛЕМА 4.28.** Фамилията  $\{U_f\}_{f \notin I(X)}$  от главни отворени подмножества  $U_f = \{a \in X \mid f(a) \neq 0\}$  на афинно алгебрично множество  $X \subseteq \bar{k}^n$  образува база на топологията на Зариски върху  $X$ .

**Доказателство:** Всяко Зариски отворено подмножество на  $X$  е от вида

$$\begin{aligned} X \setminus Z(S) &= \{a \in X \mid f(a) \neq 0 \text{ за някой полином } f \in S \setminus I(X)\} = \\ &= \cup_{f \in S \setminus I(X)} \{a \in X \mid f(a) \neq 0\} = \cup_{f \in S \setminus I(X)} U_f, \end{aligned}$$

Q.E.D.

Всяко Зариски отворено подмножество на афинно алгебрично множество  $Z(S_0)$  е от вида

$$Z(S_0) \setminus Z(S) = \{a \in Z(S_0) \mid f(a) \neq 0 \text{ за някакъв полином } f \in S \setminus IZ(S_0)\} = \cup_{f \in S \setminus IZ(S_0)} U_f,$$

Q.E.D.

## 5. Неприводимост

**ОПРЕДЕЛЕНИЕ 4.29.** *Непразното подмножество  $M$  на топологично пространство  $X$  е неприводимо, ако за всяко разлагане  $M = M_1 \cup M_2$  в обединение на затворени подмножества  $M_i \subseteq M$  относно индуцираната от  $X$  топология върху  $M$  е в сила  $M = M_1$  или  $M = M_2$ .*

**ОПРЕДЕЛЕНИЕ 4.30.** *Афинните алгебрични множества, които са неприводими относно топологията на Зариски се наричат афинни алгебрични многообразия.*

**ЛЕМА 4.31.** *Афинно алгебрично множество  $Z(S) \subseteq \bar{k}^n$  е афинно многообразие тогава и само тогава, когато идеалът  $I(Z(S)) \triangleleft \bar{k}[x_1, \dots, x_n]$  е прост.*

**Доказателство:** Да допуснем, че  $X = Z(S) \subseteq \bar{k}^n$  е афинно алгебрично многообразие, чийто идеал  $I(X) \triangleleft \bar{k}[x_1, \dots, x_n]$  не е прост. Тогава съществуват полиноми  $f, g \in \bar{k}[x_1, \dots, x_n] \setminus I(X)$  с  $fg \in I(X)$ . Съгласно Лема 4.23 имаме  $X = ZI(X)$ . Твърдим, че  $Z(f) \not\supseteq ZI(X) = X$  и  $Z(g) \not\supseteq ZI(X) = X$ , защото предположението  $Z(f) \supseteq X$  води до  $f|_X = 0$ , откъдето  $f \in I(X)$ , противно на избора на  $f \notin I(X)$ . От друга страна,  $Z(fg) \supseteq ZI(X) = X$ , съгласно Лема 4.16(i). Прилагаме Лема 4.19(ii) и получаваме

$$X = Z(fg) \cap X = [Z(f) \cup Z(g)] \cap X = [Z(f) \cap X] \cup [Z(g) \cap X].$$

Подмножествата  $Z(f) \cap X$  и  $Z(g) \cap X$  на  $X$  са затворени и различни от  $X$  съгласно  $X \not\subseteq Z(f)$ ,  $X \not\subseteq Z(g)$ . Това противоречи на неприводимостта на  $X$  и доказва простотата на идеала на неприводимо афинно алгебрично множество. Обратно, нека  $X = Z(S) \subseteq \bar{k}^n$  е афинно алгебрично множество с прост идеал  $I(X) \triangleleft \bar{k}[x_1, \dots, x_n]$  и  $X = Z_1 \cup Z_2$  за затворени  $Z_i \subsetneq X$ . Тогава

$$I(X) = I(Z_1 \cup Z_2) = I(Z_1) \cap I(Z_2)$$

съгласно Лема 4.18(iii). Въз основа на Лема 4.16(ii), от  $Z_i \subseteq X$  следва  $I(Z_i) \supseteq I(X)$ . Допускането  $I(X) = I(Z_i)$  и прилагането на Лема 4.23 водят до  $X = ZI(X) = ZI(Z_i) = Z_i$ , противно на предположението  $Z_i \subsetneq X$ . Това доказва  $I(Z_i) \not\supseteq I(X)$  за  $1 \leq i \leq 2$ . Избираме полиноми  $f_i \in I(Z_i) \setminus I(X)$  и забелязваме, че

$$f_1 f_2 \in I(Z_1) I(Z_2) \subseteq I(Z_i) \cap I(Z_2) = I(X).$$

Това противоречи на простотата на идеала  $I(X)$  и доказва неприводимостта на афинните алгебрични множества  $X = Z(S)$  с прост идеал  $I(X)$ , Q.E.D.

**ЗАДАЧА 4.32.** *Да се докаже, че ако  $k$  е безкрайно поле, то*

$$X = \{(x, x) \in \bar{k}^2 \mid x \neq 1\}$$

*не е афинно алгебрично подмножество на  $\bar{k}^2$ .*

**Упътване:** Използвайте, че  $X$  е непразно собствено подмножество на кривата  $Z(x_1 - x_2) \subset \bar{k}^2$ .

**ОПРЕДЕЛЕНИЕ 4.33.** Подмножеството  $M$  на топологично пространство  $X$  е навсякъде гъсто, ако затворената обвивка  $\bar{M} = X$  съвпада с  $X$ .

Например, подмножеството  $M$  на афинно многообразие  $X$  е Зариски навсякъде гъсто тогава и само тогава, когато  $ZI(M) = X$ .

**ОПРЕДЕЛЕНИЕ 4.34.** Околност  $V_p$  на точка  $p$  от топологично пространство  $X$  е подмножество  $V_p \subset X$ , което съдържа  $p$  заедно с някакво отворено множество  $U_p \subseteq V_p$ .

**ЛЕМА 4.35.** Подмножеството  $M$  на топологично пространство  $X$  е навсякъде гъсто тогава и само тогава, когато за всяка точка  $p \in X$  и за всяка околност  $V_p$  на  $p$  е в сила  $M \cap V_p \neq \emptyset$ .

**Доказателство:** Да допуснем, че  $\bar{M} = X$ , но съществува околност  $V_p$  на  $p$ , която не пресича  $M$ . Ако  $U_p$  е отворено множество с  $p \in U_p \subseteq V_p$ , то  $U_p \cap M = \emptyset$ . Следователно  $Z_p := X \setminus U_p$  е затворено подмножество на  $X$ , съдържащо  $M$ , а оттам и затворената обвивка  $\bar{M} = \bigcap_{Z \supseteq M} Z$ , която е сечението на затворените подмножества  $X \supseteq Z \supseteq M$ . Оттук  $Z_p = \bar{M} = X$  и  $U_p = X \setminus Z_p = \emptyset$ , противно на  $p \in U_p$ . С това установихме, че ако  $M$  е навсякъде гъсто, то  $M$  пресича всички околности на точки от  $X$ .

Обратно, нека  $M \cap V_p \neq \emptyset$  за произволна околност  $V_p$  на точка  $p \in X$ . Ако затворената обвивка  $\bar{M}$  е собствено затворено подмножество на  $X$ , то  $U := X \setminus \bar{M}$  е непразно отворено подмножество. Разглеждаме  $U$  като околност  $V_q = U$  на всяка своя точка  $q \in U$  и получаваме, че  $M \cap V_q = M \cap (X \setminus \bar{M}) \neq \emptyset$ , което противоречи на  $M \subseteq \bar{M}$ . Следователно  $\bar{M} = X$  и  $M$  е навсякъде гъсто в  $X$ , Q.E.D.

**ТВЪРДЕНИЕ 4.36.** Следните условия са еквивалентни за подмножеството  $M$  на топологичното пространство  $X$ :

- (i)  $M$  е неприводимо;
- (ii) всеки две непразни подмножества на  $M$ , които са отворени относно индуцираната от  $X$  топология върху  $M$  имат непразно сечение;
- (iii) всяко непразно подмножество на  $M$ , което е отворено относно индуцираната от  $X$  топология върху  $M$  е навсякъде гъсто в  $M$ .

**Доказателство:** (i)  $\Rightarrow$  (ii) Отворените подмножества на топологията върху  $M$ , индуцирана от топологията върху  $X$  са от вида  $U \cap M$  за отворени  $U \subseteq X$ . Ако допуснем, че  $M$  е неприводимо и съществуват отворени подмножества  $U, V \subseteq X$  с  $U \cap M \neq \emptyset$ ,  $V \cap M \neq \emptyset$  и  $(U \cap M) \cap (V \cap M) = (U \cap V) \cap M = \emptyset$ , то  $M = M \setminus (U \cap V) = (M \setminus U) \cup (M \setminus V)$ . По определение,  $M \setminus U$  и  $M \setminus V$  са затворени подмножества на  $M$ , така че  $M = M \setminus U$  или  $M = M \setminus V$ , съгласно неприводимостта на  $M$ . Това противоречи на  $U \cap M \neq \emptyset$ ,  $V \cap M \neq \emptyset$  и доказва, че произволни непразни отворени подмножества на неприводимо подмножество  $M \subseteq X$  имат непразно сечение.

(ii)  $\Rightarrow$  (i) Да предположим, че произволни непразни отворени подмножества на  $M$  имат непразно сечение, но  $M \subseteq X$  не е неприводимо. Тогава съществуват затворени подмножества  $Z_1, Z_2 \subseteq X$  с  $Z_1 \cap M \subsetneq M$ ,  $Z_2 \cap M \subsetneq M$  и  $M = (Z_1 \cap M) \cup (Z_2 \cap M) = (Z_1 \cup Z_2) \cap M$ . Оттук,  $M \subseteq Z_1 \cup Z_2$  и

$$\emptyset = M \setminus (Z_1 \cup Z_2) = (M \setminus Z_1) \cap (M \setminus Z_2)$$

за отворените подмножества  $M \setminus Z_1 \subseteq M$ ,  $M \setminus Z_2 \subseteq M$ . Условието  $Z_j \cap M \subsetneq M$ ,  $1 \leq j \leq 2$  гарантират, че  $M \setminus Z_j \neq \emptyset$  и водят до противоречие с предположение

(ii). Това доказва неприводимостта на произволно подмножество  $M \subseteq X$ , чиито непразни отворени подмножества имат непразно сечение.

(ii)  $\Rightarrow$  (iii) Съгласно Лема 4.35, достатъчно е да проверим, че за всяко отворено подмножество  $U \subseteq X$  с  $U \cap M \neq \emptyset$  и за всяка околност  $V_p \subseteq M$  на точка  $p \in M$  е в сила  $(U \cap M) \cap V_p \neq \emptyset$ . Наистина, от определението за околност  $V_p$  на точка  $p \in M$  следва съществуването на отворено подмножество  $p \in U_p \subseteq X$ , така че  $p \in U_p \cap M \subseteq V_p$ . Сега  $U \cap M \neq \emptyset$  и  $U_p \cap M \neq \emptyset$  са отворени подмножества на  $M$  и имат непразно сечение  $\emptyset \neq (U \cap M) \cap (U_p \cap M) \subseteq (U \cap M) \cap V_p$  по предположение (ii). Това доказва, че  $U \cap M$  е навсякъде гъсто в  $M$ .

(iii)  $\Rightarrow$  (ii) За произволни отворени  $U, V \subseteq X$  с  $U \cap M \neq \emptyset$ ,  $V \cap M \neq \emptyset$  можем да разглеждаме отвореното подмножество  $V \cap M \subseteq M$  като околност на всяка своя точка  $p \in V \cap M$ . Съгласно Лема 4.35, навсякъде гъстото подмножество  $\emptyset \neq U \cap M \subseteq M$  има непразно сечение  $(U \cap M) \cap (V \cap M) \neq \emptyset$ , Q.E.D.

**ОПРЕДЕЛЕНИЕ 4.37.** *Топологията  $\mathcal{U} = \{U_\alpha\}_{\alpha \in A}$  върху  $X$  се нарича Хаусдорфова, ако произволни различни точки  $x, y \in X$  имат непресичащи се околности  $W_x, W_y$ .*

Съгласно Твърдение 4.36, индуцираната топология върху неприводимо подмножество  $M$  на топологично пространство  $X$  не е Хаусдорфова. В частност, топологията на Зариски върху афинно алгебрично многообразие  $X \subseteq \bar{k}$  не е Хаусдорфова.

## 6. Афинен координатен пръстен

**ОПРЕДЕЛЕНИЕ 4.38.** *Ако  $Z \subset \bar{k}^n$  е афинно алгебрично множество с идеал  $I(Z) \triangleleft k[x_1, \dots, x_n]$ , то фактор-пръстенът*

$$\bar{k}[Z] = \bar{k}[x_1, \dots, x_n]/I(Z)$$

*се нарича афинен координатен пръстен на  $Z$ .*

*Ако  $Z/k \subset \bar{k}^n$  е афинно алгебрично множество, определено над  $k$ , то фактор-пръстенът*

$$k[Z] = k[x_1, \dots, x_n]/I_k(Z) \quad \text{с} \quad I(Z)_k = I(Z) \cap k[x_1, \dots, x_n]$$

*се нарича афинен координатен пръстен на  $Z$  над  $k$ .*

Афинното алгебрично множество  $Z$  е афинно многообразие тогава и само тогава, когато афинният координатен пръстен  $\bar{k}[Z]$  е област на цялост. Ако афинното алгебрично множество  $Z/k$ , определено над  $k$  е абсолютно неприводимо, то  $\bar{k}[Z]$  и  $k[Z]$  са области на цялост. Може  $k[Z]$  да е област на цялост, а  $\bar{k}[Z]$  да има делители на нулата.

**ЗАДАЧА 4.39.** *Да се докаже, че афинното алгебрично множество*

$$V = Z(x^2 + y^2) \subset \bar{\mathbb{F}}_3^{-2}$$

*е приводимо, въпреки, че идеалът му  $I_{\bar{\mathbb{F}}_3}(V) = (x^2 + y^2)\mathbb{F}_3[x, y]$  над  $\mathbb{F}_3$  е прост.*

**Упътване:** Разложете  $x^2 + y^2 \in \mathbb{F}_3[x, y] \subset \bar{\mathbb{F}}_3[x, y]$  над  $\bar{\mathbb{F}}_3$  като намерите полиноми  $f_j(x, y) \in \mathbb{F}_9[x, y]$  с

$$x^2 + y^2 = f_1(x, y)f_2(x, y). \quad (4.2)$$

Степента на  $x^2 + y^2$  спрямо  $y$  е 2, така че търсим

$$f_j(x, y) = a_j(x)y + b_j(x) \in \mathbb{F}_9[x][y]$$

за подходящи полиноми  $a_j(x), b_j(x) \in \mathbb{F}_9[x]$ . Сравняването на коефициентите на  $y^2, y, 1$  в (4.2) дава  $a_j \in \bar{\mathbb{F}}_3^*$  и  $b_j(x) = \alpha_j x \in \bar{\mathbb{F}}_3[x]$ . Без ограничение на общността можем да считаме, че  $a_1 = a_2 = 1$ , така че  $\alpha_2 = \alpha_1^{-1} = -\alpha_1 \in \bar{\mathbb{F}}_3^*$ .

Докажете, че уравнението  $\alpha_1^2 = -1$  няма решение в  $\mathbb{F}_3$  и има решение в  $\mathbb{F}_9$ . Следователно идеалът  $I(V)_{\mathbb{F}_3} \triangleleft \mathbb{F}_3[x, y]$  е прост, а  $I(V)_{\mathbb{F}_9} \triangleleft \mathbb{F}_9[x, y]$  не е прост.

**ТВЪРДЕНИЕ 4.40.** *Афинният координатен пръстен  $\bar{k}[Z]$  на афинно алгебрично множество  $Z$  е крайномерен над полето  $\bar{k}$  тогава и само тогава, когато  $Z = \{p_1, \dots, p_r\}$  е крайно множество.*

**Доказателство:** Ако  $Z = \{p_1, \dots, p_r\}$  е крайно множество от точки  $p_i = (p_{i1}, \dots, p_{in}) \in \bar{k}^n$ , образуваме полиномите

$$g_j(x_j) = \prod_{i=1}^r (x_j - p_{ij}),$$

чиито корени са  $j$ -тите координати на точките от  $Z$ . Тогава  $g_1(x_1), \dots, g_n(x_n) \in I(Z)$ ,  $\deg(g_j) = r$ , така че за всяко  $m_j \geq r + 1$  е в сила

$$x_j^{m_j} + I(Z) \in l_{\bar{k}}(1 + I(Z), x_j + I(Z), \dots, x_j^{r-1} + I(Z)).$$

Следователно

$$\bar{k}[Z] = l_{\bar{k}}(x_1^{i_1} \dots x_n^{i_n} + I(Z) \mid 0 \leq i_j \leq r - 1, \quad 1 \leq j \leq n)$$

е крайномерно линейно пространство над  $\bar{k}$ .

Нека  $\dim_{\bar{k}} \bar{k}[Z] = d$ . Избираме крайно подмножество  $Z_0 = \{p_1, \dots, p_r\}$  на  $Z$ . Полагаме  $Z_i = Z_0 \setminus \{p_i\}$  за  $\forall 1 \leq i \leq r$  и забелязваме, че  $I(Z_i) \supsetneq I(Z_0)$ , защото  $I(Z_i) = I(Z_0)$  води до  $Z_i = ZI(Z_i) = ZI(Z_0) = Z_0$ . Избираме полиноми  $f_i \in I(Z_i) \setminus I(Z_0)$  за  $\forall 1 \leq i \leq r$ . Твърдим, че  $f_1 + I(Z), \dots, f_r + I(Z) \in \bar{k}[Z]$  са линейно независими над  $\bar{k}$ . В противен случай, за някое  $i \in \{1, \dots, r\}$  съществуват  $\lambda_s \in \bar{k}$  за  $\forall s \in \{1, \dots, r\} \setminus \{i\}$ , така че

$$f_i + I(Z) = \sum_{s \neq i} \lambda_s (f_s + I(Z)).$$

Дясната страна на това равенство се анулира в  $p_i$ , защото  $p_i \in Z_s$  за  $\forall s \neq i$  и  $f_s + I(Z) \subset I(Z_s)$  съгласно  $Z_s \subset Z_0 \subseteq Z$ . Лявата страна  $f_i + I(Z)$  не се анулира в  $p_i$ , защото всеки полином от  $I(Z)$  се анулира в  $p_i \in Z$ , а  $f_i \in I(Z_i) \setminus I(Z_0)$  не се анулира в  $p_i$ . Противоречието доказва линейната независимост на елементите  $f_1 + I(Z), \dots, f_r + I(Z) \in \bar{k}[Z]$  над  $\bar{k}$ , така че

$$\dim_{\bar{k}} \bar{k}[Z] = d \geq r$$

и  $Z$  има най-много  $d = \dim_{\bar{k}} \bar{k}[Z]$  елемента, Q.E.D.