

Афинни алгебрични множества. Теорема на Hilbert за базиса. Теорема на Hilbert за нулите.

Навсякъде в този въпрос ще считаме, че k е съвършено поле. По определение това означава, че всяко крайно разширение $F \supset k$ е сепараabelно. 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 сепараabelно и нормално. Алгебричната обвивка $\bar{k}$ на съвършено поле k съвпада със сепараabelната обвивка k^{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 $a \in E^{\text{Gal}(\bar{k}/k)} = E^{\text{Gal}(E/k)} = k$.

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

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

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: Нека θ е примитивен елемент на крайното сепарабельно разширение $\mathbb{F}_q(a_1, \dots, a_n) \supseteq \mathbb{F}_q$, а $\varphi \in \text{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ е произволен автоморфизъм на $\overline{\mathbb{F}_q}$, фиксиращ точките от $\mathbb{F}_q$. Тогава

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

Достатъчно е да докажем съпадението на степените

$$[\mathbb{F}_q(\theta) : \mathbb{F}_q] = [\mathbb{F}_q(\varphi(\theta)) : \mathbb{F}_q], \quad (4.1)$$

за да твърдим съпадението на полетата $\mathbb{F}(\theta) = \mathbb{F}_q(\varphi(\theta))$, защото за всяко естествено число n съществува единствено разширение $\mathbb{F}_{q^n}$ на $\mathbb{F}_q$ от степен n . Ако $f_\theta(x) \in \mathbb{F}_q[x] \setminus \mathbb{F}_q$ е минималният полином на θ над $\mathbb{F}_q$, то степента $[\mathbb{F}_q(\theta) : \mathbb{F}_q] = \deg(f_\theta)$. Образът $\varphi(\theta)$ на θ под действие на $\varphi \in \text{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ е корен на $f_\theta(x)$. Съгласно своята неразложимост над $\mathbb{F}_q$, полиномът $f_\theta(x) \in \mathbb{F}_q[x] \setminus \mathbb{F}_q$ е минимален полином на $\varphi(\theta)$ над $\mathbb{F}_q$ и $[\mathbb{F}_q(\varphi(\theta)) : \mathbb{F}_q] = \deg(f_\theta)$. Оттук следват (4.1) и $\mathbb{F}_q(\varphi(a_1), \dots, \varphi(a_n)) = \mathbb{F}_q(\varphi(\theta)) = \mathbb{F}_q(\theta) = \mathbb{F}_q(a_1, \dots, a_n)$, 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 Φ_{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: За $\forall 1 \leq i \leq n$ нека m_i е минималното естествено число, за което $\mathbb{F}_{q^{m_i}}$ съдържа a_i . Тогава най-малкото общо кратно $m = \text{LCM}(m_1, \dots, m_n)$ е минималното естествено число, за което $\mathbb{F}_{q^m}$ съдържа всички компоненти $a_1, \dots, a_n$ на a . Ограничението

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

така че орбитата $\text{Orb}_{\text{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)}(a) = \text{Orb}_{\text{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)}(a) = \text{Orb}_{\langle \Phi_q|_{\mathbb{F}_{q^m}} \rangle}(a)$. Твърдим, че стабилизаторът на a в $\langle \Phi_q|_{\mathbb{F}_{q^m}} \rangle$ е тривиален, $\text{Stab}_{\langle \Phi_q|_{\mathbb{F}_{q^m}} \rangle}(a) = \{Id_{\mathbb{F}_{q^m}}\}$, защото допускането $\Phi_{q^r}(a) = a$ за някое $1 \leq r \leq m-1$ означава съществуване на естествено число $r < m$ с $a_1, \dots, a_n \in \mathbb{F}_{q^r}$. Броят на елементите в орбитата

$$|P| = |\text{Orb}_{\text{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)}(a)| = |\text{Orb}_{\langle \Phi_q|_{\mathbb{F}_{q^m}} \rangle}(a)| = [\langle \Phi_q|_{\mathbb{F}_{q^m}} \rangle : \{Id_{\mathbb{F}_{q^m}}\}] = m$$

съвпада с индекса на стабилизатора m . Това доказва (i) и (ii).

Условиата $a_i \in \mathbb{F}_{q^{m_i}}$ са еквивалентни на $\Phi_{q^{m_i}}(a_i) = a_i$, така че $a \in \mathbb{F}_{q^m}$ е равносилно на $\Phi_{q^m}(a) = a$. Следователно минималното естествено число m , за

което $\mathbb{F}_{q^m}$ съдържа $a_1, \dots, a_n$ е и минималното естествено число с $\Phi_{q^m}(a) = a$. Това установява верността на (iii).

За (iv) да отбележим, че ако $m = \deg \text{Orb}_{\text{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)}(a)$, то дефиниционното поле $\mathbb{F}_q(a_1, \dots, a_n) \subseteq \mathbb{F}_{q^m}$. Допускането $\mathbb{F}_q(a_1, \dots, a_n) = \mathbb{F}_{q^k}$ за някой естествен делител $k < m$ на m води до противоречие с определението за степен на $\mathbb{F}_q$ -затворена точка, защото тогава $k \in \mathbb{N}$, $k < m$ има свойството $\mathbb{F}_{q^k} \ni a_1, \dots, a_n$, Q.E.D.

ЗАДАЧА 4.6. (i) Да се докаже, че:

(а) произволен пораждащ α_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 α_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 $\mathbb{F}_2$.

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 естественият най-голям общ делител на m и r . Тогава P се разлага в непресичащо се обединение

$$P = \cup_{j=1}^d P_j \quad (4.2)$$

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 напомним, че $\overline{\mathbb{F}_{q^r}} = \overline{\mathbb{F}_q}$. По определение, $\text{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_{q^r})$ е подгрупа на $\text{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$, така че $\mathbb{F}_{q^r}$ -затворената точка $P_1 = \text{Orb}_{\text{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)}(a)$ е подмножество на $\mathbb{F}_q$ -затворената точка $P = \text{Orb}_{\text{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)}(a)$. Степента на P_1 е равна на степента $[\mathbb{F}_{q^r}(a_1, \dots, a_n) : \mathbb{F}_{q^r}]$ на дефиниционното поле $\mathbb{F}_{q^r}(a_1, \dots, a_n)$ на $a = (a_1, \dots, a_n)$ над $\mathbb{F}_{q^r}$. Полето $\mathbb{F}_{q^r}(a_1, \dots, a_n)$ е минималното разширение на $\mathbb{F}_q$, съдържащо $\mathbb{F}_{q^r}$ и $\mathbb{F}_q(a_1, \dots, a_n) = \mathbb{F}_{q^m}$. По-точно, $\mathbb{F}_{q^r}(a_1, \dots, a_n) = \mathbb{F}_{q^\mu}$ за естественото най-малко общо кратно $\mu = \text{LCM}(m, r) = \frac{mr}{d}$ на m и r . Следователно

$$\deg(P_1) = [\mathbb{F}_{q^r}(a_1, \dots, a_n) : \mathbb{F}_{q^r}] = [\mathbb{F}_{q^{\frac{mr}{d}}} : \mathbb{F}_{q^r}] = \frac{m}{d}$$

и $P = \text{Orb}_{\text{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)}(a)$ се разлага в непресичащо се обединение на d на брой $\mathbb{F}_{q^r}$ -затворени точки от степен $\frac{m}{d}$.

В частност, P_j са $\mathbb{F}_{q^r}$ -рационални точки тогава и само тогава, когато $\deg(P_j) = \frac{m}{d} = 1$ и m дели r , Q.E.D.

Като непосредствено следствие от предишното твърдение получаваме, че ако $P_1, \dots, P_k$ са краен брой различни $\mathbb{F}_q$ -затворени точки със степени $\deg(P_j) = m_j \in \mathbb{N}$, $m = \text{LCM}(m_1, \dots, m_k)$ е естественото най-малко общо кратно на степените им, а $r \in \mathbb{N}$ е естествено число, кратно на m , то непресичащото се обединение $P_1 \cup \dots \cup P_k$ се разбива в $m_1 + \dots + m_k$ на брой $\mathbb{F}_{q^r}$ -рационални точки.

Ако $\{P_k\}_{k=1}^\infty$ е безкрайна редица от различни $\mathbb{F}_q$ -затворени точки P_k с неограничена редица от степени $\{m_k = \deg(P_k)\}_{k=1}^\infty$, то не съществува крайно разширение $\mathbb{F}_{q^s}$ на $\mathbb{F}_q$, над което $\cup_{k=1}^\infty P_k$ се разлага в обединение на $\mathbb{F}_{q^s}$ -рационални точки. Причина за това е несъществуването на естествено число $s \in \mathbb{N}$, което да дели всички елементи на неограничената редица $\{m_k\}_{k=1}^\infty$.

ЗАДАЧА 4.8. В означенията от задача 4.6 да се разложат $\mathbb{F}_2$ -затворените точки $P, Q, R \in \mathbb{F}_2^2$ 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 $d = \text{GCD}(m, r) \in \mathbb{N}$ 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 $f(x) \in \mathbb{F}_q[x]$.

Наистина, ако $f(x) = \prod_{i=1}^m (x - a_i) \in \mathbb{F}_q[x] \setminus \mathbb{F}_q$ е неразложим над $\mathbb{F}_q$, то за всяко $1 \leq i \leq m$, $\mathbb{F}_q$ -затворената точка $P_i = \text{Orb}_{\text{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)}(a_i) \subseteq \{a_1, \dots, a_m\}$ се съдържа в множеството на корените на $f(x) = 0$, защото произволен елемент $\varphi \in \text{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ изобразява a_i в корен на минималния полином $f(x)$ на a_i над $\mathbb{F}_q$. Дефиниционното поле на a_i над $\mathbb{F}_q$ е от степен $[\mathbb{F}_q(a_i) : \mathbb{F}_q] = \deg(f) = m$, така че $\mathbb{F}_q$ -затворената точка P_i е от степен $\deg(P_i) = [\mathbb{F}_q(a_i) : \mathbb{F}_q] = m$ и $P_i = \{a_1, \dots, a_m\}$ съвпада с множеството на корените на $f(x) = 0$.

Обратно, нека $P = \text{Orb}_{\text{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)}(a) = \{a, a^q, \dots, a^{q^{m-1}}\}$ е $\mathbb{F}_q$ -затворена точка на $\overline{\mathbb{F}_q}$ от степен m . Тогава полиномът

$$g(x) = \prod_{j=0}^{m-1} (x - a^{q^j})$$

с корени $a, a^q, \dots, a^{q^{m-1}} \in \mathbb{F}_q(a) = \mathbb{F}_{q^m}$ има коефициенти от $\mathbb{F}_{q^m}$. Автоморфизмът на Frobenius $\Phi_q : \mathbb{F}_{q^m} \rightarrow \mathbb{F}_{q^m}$, $\Phi_q(\alpha) = \alpha^q$ действа като пермутация в множеството $\{a, a^q, \dots, a^{q^{m-1}}\}$ на корените на $g(x)$ и стабилизира коефициентите на $g(x)$, които с точност до знак са елементарните симетрични полиноми на $a, a^q, \dots, a^{q^{m-1}}$. Следователно $g(x) \in (\mathbb{F}_{q^m})^{\text{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)}[x] = \mathbb{F}_q[x]$ е с коефициенти от $\mathbb{F}_q$. Твърдим, че полиномът $g(x) \in \mathbb{F}_q[x]$ е неразложим над $\mathbb{F}_q$. Допускаме обратното и разлагаме $g(x) = g_1(x) \dots g_k(x)$ в произведение от неразложими над $\mathbb{F}_q$ множители $g_i(x) \in \mathbb{F}_q[x] \setminus \mathbb{F}_q$. Докажем, че множеството на корените на произволен неразложим над $\mathbb{F}_q$ множител $g_j(x) \in \mathbb{F}_q[x] \setminus \mathbb{F}_q$ на $g(x)$ е $\mathbb{F}_q$ -затворена точка P_j . Оттук следва, че $P = P_j$, защото P_j е $\text{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ -орбита, съдържаща се в $\text{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ -орбитата P . Сега $\deg(g_j) = \deg(P_j) = \deg(P) = m = \deg(g)$ е противоречие, доказващо неразложимостта на $g(x) \in \mathbb{F}_q[x] \setminus \mathbb{F}_q$ 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 $\mathbb{F}_{2^{2012}}$?

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 $\bar{k}^n$ 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 $Z(S)$.

Действието на елемент $\varphi \in \text{Gal}(\bar{k}/k)$ върху коефициентите на полином $f(x) \in \bar{k}[x_1, \dots, x_n]$ задава действие на $\text{Gal}(\bar{k}/k)$ върху $\bar{k}[x_1, \dots, x_n]$,

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

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

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

$$\begin{aligned} \varphi(f(a_1, \dots, a_n)) &= \varphi \left(\sum_{i=(i_1, \dots, i_n)} c_i a_1^{i_1} \dots a_n^{i_n} \right) = \\ &= \sum_{i=(i_1, \dots, i_n)} \varphi(c_i) \varphi(a_1)^{i_1} \dots \varphi(a_n)^{i_n} = \varphi(f)(\varphi(a)). \end{aligned}$$

ЛЕМА-ОПРЕДЕЛЕНИЕ 4.12. Нека $Z(S)/\mathbb{F}_q$ е афинно алгебрично множество, определено над $\mathbb{F}_q$, $a \in Z(S)$. Тогава $\mathbb{F}_q$ -затворената точка $P = \text{Orb}_{\text{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q)}(a)$ върху $\bar{\mathbb{F}}_q^n$, породена от a се съдържа изцяло в $Z(S)$ и се нарича $\mathbb{F}_q$ -затворена точка на $Z(S)$.

Доказателство: Полиномите $f(x_1, \dots, x_n) \in S$, определящи $Z(S)$ са с коефициенти от $\mathbb{F}_q$, така че за произволен автоморфизъм $\varphi \in \text{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q)$ е в сила

$$f(\varphi(a)) = \varphi(f)(\varphi(a)) = \varphi(f(a)) = \varphi(0) = 0.$$

Следователно $\varphi(a) \in Z(S)$ и P се съдържа в $Z(S)$, Q.E.D.

ПРИМЕР 4.13. 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 4.14. 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 $Y(\mathbb{F}_4) = Y(\mathbb{F}_2)$.

ЛЕМА 4.15. (i) Афинното алгебрично множество $Z(0) = \bar{k}^n$, зададено от тъждествено нулевия полином съвпада с цялото афинно пространство $\bar{k}^n$.
(ii) Афинното алгебрично множество $Z(\bar{k}[x_1, \dots, x_n]) = \emptyset$, зададено от целия полиномиален пръстен $\bar{k}[x_1, \dots, x_n]$ е празното множество.
(iii) Ако $S \subseteq T \subseteq \bar{k}[x_1, \dots, x_n]$, то $Z(S) \supseteq Z(T)$.
(iv) Ако $I(S) = \langle S \rangle$ е идеалът в $\bar{k}[x_1, \dots, x_n]$, породен от S , то $Z(S) = Z(I(S))$.
(v) Ако $S \subset T \subseteq \bar{k}[x_1, \dots, x_n]$, то $Z(S) \supsetneq Z(T)$.
(vi) За произволни подмножества $S_i \subset \bar{k}[x_1, \dots, x_n]$ е в сила $Z(\cup_i S_i) = \cap_i Z(S_i)$.
(vii) Ако S, T са подмножества на $\bar{k}[x_1, \dots, x_n]$ и $ST = \{fg \mid f \in S, g \in T\}$, то $Z(ST) = Z(S) \cup Z(T)$.

Доказателство: (iii) Ако $a \in Z(T)$, то за $\forall f \in S \subseteq T$ е в сила $f(a) = 0$, така че $a \in Z(S)$.

(iv) Ако $a \in Z(S)$, $f_1, \dots, f_m \in S$ и $f = \sum_{i=1}^m f_i g_i \in I(S)$, то $f(a) = 0$ и $a \in Z(I(S))$.

Това доказва, че $Z(S) \subseteq Z(I(S))$. От $S \subseteq I(S)$ получаваме $Z(I(S)) \subseteq Z(S)$ и $Z(S) = Z(I(S))$.

(v) За $\forall a \in Z(T)$ и $\forall f \in S \subset T$ е изпълнено $f(a) = 0$, така че $a \in Z(S)$.

(vi) От $\cup_{i \in I} S_i \supseteq S_i$ следва $Z(\cup_{i \in I} S_i) \subseteq Z(S_i)$ за всички $i \in I$ и $Z(\cup_i S_i) \subseteq \cap_i Z(S_i)$. Обратно, ако $a \in \cap_i Z(S_i)$, то $a \in Z(S_i)$ за $\forall i$. Произволен полином $f \in \cup_i S_i$ принадлежи на някое S_i и се анулира в a . Следователно $a \in Z(\cup_i S_i)$ и $\cap_i Z(S_i) \subseteq Z(\cup_i S_i)$.

(vii) Ако $a \in Z(ST) \setminus Z(S)$, то съществува полином $f \in S$ с $f(a) \neq 0$. За всяко $g \in T$ полиномът $fg \in ST$ се анулира в a , $0 = (fg)(a) = f(a)g(a)$. Следователно $g(a) = 0$ и $a \in Z(T)$. Това установява включването $Z(ST) \subseteq Z(S) \cup Z(T)$. Обратно, от $I(ST) \subseteq I(S)$ следва, че $Z(ST) = Z(I(ST)) \supseteq Z(I(S)) = Z(S)$. Аналогично, $Z(ST) \supseteq Z(T)$ и $Z(ST) \supseteq Z(S) \cup Z(T)$, Q.E.D.

ПРИМЕР 4.16. 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 множества $Z(\langle f \rangle) = Z(f)$ на корените на f . Вземайки предвид, че $Z(f)$ се състои от $\deg(f) \in \mathbb{N}$ точки, стигаме до извода, че афинните алгебрични подмножества на афинната права $\bar{k}$ са $\emptyset$, $\bar{k}$ и крайните подмножества.

1. Ньотерови пръстени. Теорема на Hilbert за базиса

ТВЪРДЕНИЕ 4.17. Комутативният пръстен с единица R е ньотеров тогава и само тогава, когато всяка ненамаляваща редица от идеали

$$I_1 \subseteq I_2 \subseteq \dots \subseteq I_n \subseteq I_{n+1} \subseteq \dots \quad (4.3)$$

се стабилизира след краен брой стъпки.

В частност, ако R е ньотеров пръстен, то всяко пораждащо подмножество S на идеал $\langle S \rangle \triangleleft R$ има крайно пораждащо подмножество $\{s_1, \dots, s_n\} \subseteq S$, $\langle S \rangle = \langle s_1, \dots, s_n \rangle$.

Доказателство: Нека R е ньотеров пръстен и (4.3) е ненамаляваща редица от идеали. Твърдим, че $I := \cup_{s=1}^{\infty} I_s$ е идеал в R . Наистина, за произволни $a, b \in I$ съществуват $p, q \in \mathbb{N}$, така че $a \in I_p$, $b \in I_q$. Ако $n := \max(p, q)$, то $a, b \in I_n$ и $a - b \in I_n \triangleleft R$. За $\forall a \in I_p$ и $\forall r \in R$, имаме $ar \in I_p \subseteq I$, така че I е идеал в R . По определението за ньотеровост, идеалът $I = \langle a_1, \dots, a_k \rangle = Ra_1 + \dots + Ra_k$

е крайнопороден. Ако $a_j \in I_{n_j}$ и $n := \max(n_1, \dots, n_k)$, то за всяко $m \geq n$ е в сила $I \subseteq I_n \subseteq I_m \subseteq I$. Следователно $I = I_n = I_{n+1} = \dots$ и редицата (4.3) се стабилизира след краен брой стъпки.

Ще докажем, че ако всяка ненамаляваща редица от идеали 4.3 се стабилизира след краен брой стъпки, то всяко множество $S \subseteq R$ има крайно подмножество $\{s_1, \dots, s_n\} \subseteq S$, така че $\langle S \rangle = \langle s_1, \dots, s_n \rangle$. Оттук следва, че условието за стабилизация на ненамаляващите редици от идеали е достатъчно за нютеровостта на пръстена. Освен това, ако R е нютеров пръстен то всяко пораждащо множество на идеал има крайно пораждащо подмножество, защото стабилизацията на ненамаляващите редици от идеали е необходимо условие за нютеровост.

С допускане на противното, нека $S \subseteq R$ е такова подмножество, че идеалът $I = \langle S \rangle$ няма крайна пораждаща система $\{s_1, \dots, s_n\} \subseteq S$. Тогава избираме $\sigma_1 \in S$. С индукция по $n \in \mathbb{N}$, ако $\sigma_1, \dots, \sigma_n \in S$ са такива, че $\sigma_i \in S \setminus \langle \sigma_1, \dots, \sigma_{i-1} \rangle$ за $\forall 2 \leq i \leq n$, то съществува $\sigma_{n+1} \in S \setminus \langle \sigma_1, \dots, \sigma_n \rangle$. В противен случай, от $S \subseteq I_n := \langle \sigma_1, \dots, \sigma_n \rangle$ следва $\langle S \rangle \subseteq I_n$, защото I_n е затворено относно събиране на свои елементи и умножение с елементи на R . Комбинирайки с $I_n \subseteq \langle S \rangle$ получаваме $I = I_n$, така че крайното подмножество $\{\sigma_1, \dots, \sigma_n\} \subseteq S$ поражда I . Това противоречи на допускането и доказва съществуването на безкрайна редица $\{\sigma_n\}_{n=1}^\infty \subseteq S$, изпълняваща условието $\sigma_n \in S \setminus I_{n-1} := \langle \sigma_1, \dots, \sigma_{n-1} \rangle$ за $\forall n \geq 2$. Безкрайната редица от идеали $I_{n-1} \subsetneq I_n$ е строго растяща. Това противоречи на предположението за стабилизация на ненамаляващите редици от идеали и доказва твърдението, Q.E.D.

ТВЪРДЕНИЕ 4.18. *Ако R е нютерова комутативна област с единица, то пръстенът $R[x]$ на полиномите на една променлива x с коефициенти от R е също нютерова комутативна област с единица.*

Доказателство: Ако R е комутативна област с единица, а $LM(f)$ е старшият моном на нетъждествено нулев полином $f(x) \in R[x] \setminus \{0\}$, то Лемата за старшия еднороден на произведение на полиноми на една променлива гласи, че $LM(fg) = LM(f)LM(g)$ за произволни $f(x), g(x) \in R[x] \setminus \{0\}$. Оттук следва, че пръстенът $R[x]$ на полиномите на една променлива x с коефициенти от комутативна област с единица R е комутативна област с единица. Остава да проверим, че всеки идеал в $R[x]$ е крайно породен.

Допускаме противното и разглеждаме идеал $I \triangleleft R[x]$, който не е крайно породен. Избираме $f_1 \in I \setminus \{0\}$ от минимална степен. С индукция по броя на избраните полиноми, ако сме фиксирали $f_1, \dots, f_{j-1} \in I$, то вземаме $f_j \in I \setminus \langle f_1, \dots, f_{j-1} \rangle$ от минимална степен. По този начин получаваме безкрайна редица от полиноми $f_1, \dots, f_j, \dots$. Разглеждаме идеала $J \triangleleft R$, породен от старшите коефициенти $LC(f)$ на $\forall f \in I \setminus \{0\}$. Пръстенът R е нютеров, така че J е крайно породен идеал или съществува $j \in \mathbb{N}$, така че $J = \langle LC(f_1), \dots, LC(f_j) \rangle$. Тогава $L(f_{j+1}) \in J$ има представяне

$$LC(f_{j+1}) = \sum_{i=1}^j r_i LC(f_i)$$

чрез подходящи $r_i \in R$. Съгласно избора на f_i от минимална степен имаме $\deg(f_{j+1}) \geq \deg(f_i)$ за $\forall 1 \leq i \leq j$. Полиномът

$$f'_{j+1} = f_{j+1} - \sum_{i=1}^j r_i x^{\deg(f_{j+1}) - \deg(f_i)} f_i,$$

е от степен $\deg(f'_{j+1}) < \deg(f_{j+1})$, защото старшите мономи

$$LM(r_i x^{\deg(f_{j+1}) - \deg(f_i)} f_i) = r_i x^{\deg(f_{j+1}) - \deg(f_i)} LM(f_i)$$

по Лемата за старшия едночлен на произведение на полиноми с коефициенти от комутативна област с единица R и старшите коефициенти

$$LC(r_i x^{\deg(f_{j+1}) - \deg(f_i)} f_i) = r_i LC(f_i).$$

Съгласно избора на $f_{j+1} \in I \setminus \langle f_1, \dots, f_j \rangle$ от минимална степен, $f'_{j+1} \in \langle f_1, \dots, f_j \rangle$.

В резултат, $f_{j+1} = f'_{j+1} + \sum_{i=1}^j r_i x^{\deg(f_{j+1}) - \deg(f_i)} f_i \in \langle f_1, \dots, f_j \rangle$, което е противоречие, доказващо нютеровостта на $R[x]$, Q.E.D.

Като непосредствено следствие от предишното твърдени получаваме следната

ТЕОРЕМА 9. (Теорема на Hilbert за базиса) *Пръстенът на полиномите $k[x_1, \dots, x_n]$ на няколко променливи с коефициенти от поле k е нютерова област с единица.*

ЗАДАЧА 4.19. *За произволен идеал $I \triangleleft k[x, y]$ да означим с $J(I) \triangleleft k[x]$ идеала, породен от старшите коефициенти $LC_y(f) \in k[x]$ на $f(x, y) \in I$, разгледани като полиноми на y с коефициенти от $k[x]$. Ако $J(I) = \langle a(x) \rangle$ се поражда от $a(x) \in k[x]$ и $f(x, y) \in I$ е полином от степен $\deg_y f(x, y) = d$ относно y със старши коефициент $LC_y(f) = a(x)$, да се докаже, че съществува пораждаща система $f(x, y), f_1(x, y), \dots, f_m(x, y) \in k[x, y]$ на $I = \langle f(x, y), f_1(x, y), \dots, f_m(x, y) \rangle$ с $\deg_y f_i(x, y) \leq d$ за всички $1 \leq i \leq m$.*

Упътване: Изберете $I = \langle f(x, y), f_1(x, y), \dots, f_m(x, y) \rangle$ така, че за всеки индекс $1 \leq i \leq m$ полиномът $f_i(x, y)$ е от минимална степен с условието $f_i(x, y) \in I \setminus \langle f(x, y), f_1(x, y), \dots, f_{i-1}(x, y) \rangle$.

СЛЕДСТВИЕ 4.20. *Всяко афинно многообразие $V \subset \bar{k}^n$ е множество на нулите $V = Z(f_1, \dots, f_m)$ на краен брой полиноми*

$$f_1(x_1, \dots, x_n), \dots, f_m(x_1, \dots, x_n) \in \bar{k}[x_1, \dots, x_n].$$

Доказателство: Нека $S \subseteq \bar{k}[x_1, \dots, x_n]$ е множество от полиноми, а $V = Z(S) \subseteq \bar{k}^n$ е афинното алгебрично многообразие на нулите на S . Тогава $V = Z(I(S))$ съвпада с множеството на нулите на идеала $I(S) \triangleleft \bar{k}[x_1, \dots, x_n]$, породен от S . Съгласно Теорема 9 на Hilbert за базиса, съществуват полиноми $f_1, \dots, f_m \in \bar{k}[x_1, \dots, x_n]$, които пораждат идеала $I(S) = \langle f_1, \dots, f_m \rangle$. В резултат, $V = Z(I(S)) = Z(f_1, \dots, f_m)$ се задава като множеството на нулите на краен брой полиноми, Q.E.D.

ЛЕМА 4.21. *Ако $\varphi : R \rightarrow S$ е хомоморфизъм на комутативни пръстени с единица и R е нютеров пръстен, то образът $Im(\varphi) := \{\varphi(r) \mid r \in R\}$ на φ е нютеров пръстен.*

Доказателство: Трябва да докажем, че произволен идеал $I \triangleleft Im(\varphi)$ е крайнопороден. За целта използваме, че пълният праобраз

$$\varphi^{-1}(I) := \{r \in R \mid \varphi(r) \in I\}$$

е идеал в R . Наистина, за $\forall a, b \in \varphi^{-1}(I)$ и $r \in R$ е в сила $a - b, ar \in \varphi^{-1}(I)$ съгласно $\varphi(a - b) = \varphi(a) - \varphi(b) \in I$ и $\varphi(ar) = \varphi(a)\varphi(r) \in I$ за $\varphi(a), \varphi(b) \in I$.

Доколкото пръстенът R е нютеров, идеалът $\varphi^{-1}(I) \triangleleft R$ е крайнопороден, т.е. съществуват $r_1, \dots, r_n \in \varphi^{-1}(I)$, така че

$$\varphi^{-1}(I) = \langle r_1, \dots, r_n \rangle = \left\{ \sum_{i=1}^n r_i s_i \mid s_i \in R, 1 \leq i \leq n \right\}.$$

Твърдим, че

$$I = \langle \varphi(r_1), \dots, \varphi(r_n) \rangle = \left\{ \sum_{i=1}^n \varphi(r_i) \varphi(s_i) \mid s_i \in R, 1 \leq i \leq n \right\}$$

се поражда от $\varphi(r_1), \dots, \varphi(r_n)$ като идеал в пръстена $Im(\varphi) = \{\varphi(s) \mid s \in R\}$. Наистина, всеки елемент на $I \triangleleft Im(\varphi)$ е от вида $\varphi(r)$ за някое $r \in R$. По определението на $\varphi^{-1}(I)$ имаме $r \in \varphi^{-1}(I)$, така че $r = \sum_{i=1}^n r_i s_i$ за подходящи $s_1, \dots, s_n \in R$. Следователно $\varphi(r) = \sum_{i=1}^n \varphi(r_i) \varphi(s_i) \in \langle \varphi(r_1), \dots, \varphi(r_n) \rangle$, така че идеалът $I = \langle \varphi(r_1), \dots, \varphi(r_n) \rangle$ е крайнопороден и пръстенът $Im(\varphi)$ е нютеров, Q.E.D.

СЛЕДСТВИЕ 4.22. *Ако R е нютеров комутативен пръстен с единица, то всяка крайнопородена R -алгебра $S = R[a_1, \dots, a_n]$ е също нютеров комутативен пръстен с единица.*

Доказателство: Нека $\pi_A : R[x_1, \dots, x_n] \rightarrow S = R[a_1, \dots, a_n]$ е естественят епиморфизъм, отговарящ на пораждащата система $a_1, \dots, a_n$ на $S = R[a_1, \dots, a_n]$. Полиномиалният пръстен $R[x_1, \dots, x_n]$ е нютеров комутативен пръстен с единица. Прилагайки Лема 4.21 получаваме, че $Im(\pi_A) = R[a_1, \dots, a_n] = S$ е нютеров комутативен пръстен с единица, Q.E.D.

ЗАДАЧА 4.23. *Да се докаже, че ако R е комутативен пръстен с единица и пръстенът на полиномите $R[x]$ на x с коефициенти от R е нютеров, то R е нютеров пръстен.*

Упътване: Допуснете противното и разгледайте безкрайна строго растяща редица

$$I_1 \subsetneq I_2 \subsetneq \dots \subsetneq I_s \subsetneq I_{s+1} \subsetneq \dots$$

от идеали I_s в R . Ако $J_s = I_s R[x]$ са идеалите в $R[x]$, породени от I_s , то ненамаляващата редица

$$J_1 \subseteq J_2 \subseteq \dots \subseteq J_s \subseteq J_{s+1} \subseteq \dots$$

от идеали в нютеровия пръстен $R[x]$ се стабилизира след краен брой стъпки, $J_n = J_{n+1} = \dots$ за някое $n \in \mathbb{N}$. Произволен елемент $\beta \in I_{n+1} \setminus I_n$ принадлежи на идеала $I_{n+1} R[x] = J_{n+1} = J_n = I_n R[x]$ в $R[x]$, така че съществуват елементи $\alpha_1, \dots, \alpha_m \in I_n$ и полиноми $g_1(x), \dots, g_m(x) \in R[x]$ с $\beta = \sum_{i=1}^m \alpha_i g_i(x)$. В частност, $\beta = \sum_{i=1}^m \alpha_i g_i(0) \in I_n \triangleleft R$, което противоречи на избора на β и доказва нютеровостта на R .

2. Крайно породени модули и алгебри над нютеров пръстен

ЛЕМА 4.24. *Ако R е нютеров комутативен пръстен с единица, а M е крайно породен R -модул, то всеки R -подмодул N на M е крайно породен над R .*

Доказателство: С индукция по броя n на пораждащите $\mu_1, \dots, \mu_n$ на $M = R\mu_1 + \dots + R\mu_n$, ако $M = R\mu_1$, то за произволен R -подмодул N на $M = R\mu_1$ множеството

$$C_N = \{r \in R \mid r\mu_1 \in N\}$$

на коефициентите на елементите на N е идеал в R . Пръстенът R е нютеров, така че съществуват краен брой пораждащи $r_1, \dots, r_l$ на $C_N = \langle r_1, \dots, r_l \rangle = Rr_1 + \dots + Rr_l$. Тогава $N = Rr_1\mu_1 + \dots + Rr_l\mu_1$ е крайно породен R -модул. За произволно естествено число n да разгледаме естествения хомоморфизъм на R -модули

$$\begin{aligned} \pi_n : M = R\mu_1 + \dots + R\mu_n &\longrightarrow M/R\mu_n, \\ \pi_n \left(\sum_{i=1}^n r_i \mu_i \right) &= \sum_{i=1}^{n-1} r_i \mu_i + R\mu_n \end{aligned}$$

с ядро $\ker(\pi_n) = R\mu_n$ и образ

$$\operatorname{im}(\pi_n) = M/R\mu_n = R(\mu_1 + R\mu_n) + \dots + R(\mu_{n-1} + R\mu_n),$$

който е породен от $\mu_1 + R\mu_n, \dots, \mu_{n-1} + R\mu_n$ като R -модул. За произволен R -подмодул N на M , хомоморфизмът π_n се ограничава до епиморфизъм

$$\pi_n : N \longrightarrow (N + R\mu_n)/R\mu_n.$$

По индукционно предположение, подмодулът $(N + R\mu_n)/R\mu_n$ на $(n-1)$ -породения R -модул $M/R\mu_n$ е крайно породен, т.е.

$$(N + R\mu_n)/R\mu_n = R(\nu_1 + R\mu_n) + \dots + R(\nu_m + R\mu_n)$$

за някакви елементи $\nu_1, \dots, \nu_m \in N$. От друга страна, R -подмодулът $N \cap R\mu_n$ на $R\mu_n$ е крайно породен или

$$N \cap R\mu_n = R\lambda_1 + \dots + R\lambda_l$$

за подходящи $\lambda_1, \dots, \lambda_l \in N \cap R\mu_n$. Твърдим, че

$$N = R\lambda_1 + \dots + R\lambda_l + R\nu_1 + \dots + R\nu_m \quad (4.4)$$

се поражда от $\lambda_1, \dots, \lambda_l, \nu_1, \dots, \nu_m \in N$ като R -модул. Включването

$$R\lambda_1 + \dots + R\lambda_l + R\nu_1 + \dots + R\nu_m \subseteq N$$

следва от $\lambda_j, \nu_i \in N$. Всеки елемент $x \in N$ се изобразява в

$$\pi_n(x) = \sum_{i=1}^m r_i(\nu_i + R\mu_n)$$

под действие на π_n , така че $x_o := x - \sum_{i=1}^m r_i\nu_i \in N$ попада в ядрото $\ker(\pi_n) \cap N =$

$N \cap R\mu_n$. Следователно $x_o = \sum_{j=1}^l s_j\lambda_j$ за подходящи $s_j \in R$ и

$$x = \sum_{j=1}^l s_j\lambda_j + \sum_{i=1}^m r_i\nu_i.$$

Това доказва 4.4, Q.E.D.

ЗАДАЧА 4.25. Нека k е поле, а $M = k[x]\mu_1 + k[x]\mu_2$ е $k[x]$ -модул с два пораждащи μ_1 и μ_2 . Да се докаже, че всеки $k[x]$ -подмодул N на M има два пораждащи.

ОПРЕДЕЛЕНИЕ 4.26. Ако R и S са комутативни пръстени с единица, S е R -модул и

$$r(s_1s_2) = (rs_1)s_2 \quad \text{за} \quad \forall s_1, s_2 \in S, \quad \forall r \in R,$$

то казваме, че S е R -алгебра.

ПРИМЕР 4.27. Пръстенът $R[x_1, \dots, x_n]$ на полиномите на $x_1, \dots, x_n$ с коефициенти от комутативен пръстен с единица R е R -алгебра.

ОПРЕДЕЛЕНИЕ 4.28. Комутативният пръстен с единица S е крайнопородена алгебра над комутативния пръстен с единица R , ако съществуват елементи $a_1, \dots, a_n \in S$, така че

$$S = R[a_1, \dots, a_n] = \{f(a_1, \dots, a_n) \mid f \in R[x_1, \dots, x_n]\}$$

се състои от полиномите на $a_1, \dots, a_n$ с коефициенти от R .

ЛЕМА 4.29. *Нека R е нютерова комутативна област с единица, $R[a_1, \dots, a_n]$ е крайно породена R -алгебра, а S е такъв подпръстен на $R[a_1, \dots, a_n]$, съдържащ R , че $R[a_1, \dots, a_n]$ е крайно породен S -модул. Тогава S е крайно породена R -алгебра.*

Доказателство: Нека

$$R[a_1, \dots, a_n] = Sb_1 + \dots + Sb_m.$$

Без ограничение на общостта ще считаме, че $b_m = 1_R$, присъединявайки единицата на R към пораждащата система на $R[a_1, \dots, a_n]$ като S -модул. От $a_p \in R[a_1, \dots, a_n]$ за $\forall 1 \leq p \leq n$ следва съществуването на $\alpha_{p1}, \dots, \alpha_{pm} \in S$, така че

$$a_p = \sum_{q=1}^m \alpha_{pq} b_q.$$

От друга страна, за произволни $1 \leq i, j \leq m$ елементите $b_i, b_j \in R[a_1, \dots, a_n]$ имат произведение $b_i b_j \in R[a_1, \dots, a_n]$, така че

$$b_i b_j = \sum_{q=1}^m \alpha_{ijq} b_q$$

за подходящи $\alpha_{ijq} \in S$. Да разгледаме подпръстена

$$S_o := R[\alpha_{pq}, \alpha_{ijq} \mid 1 \leq p \leq n, \quad 1 \leq i, j, q \leq m]$$

на S , съдържащ R . Съгласно Твърдение 4.18, пръстенът S_o е нютерова комутативна област с единица, като крайно породена алгебра над нютеровата комутативна област с единица R . Твърдим, че

$$R[a_1, \dots, a_n] = S_o b_1 + \dots + S_o b_m.$$

Модулът $M_o := S_o b_1 + \dots + S_o b_m$ над пръстена S_o е подгрупа на адитивната група $(R[a_1, \dots, a_n], +)$, защото $(S_o, +)$ е подгрупа на $(S, +)$ и $(S, +)$ е подгрупа на $(R[a_1, \dots, a_n], +)$. Съгласно $b_i b_j = \sum_{q=1}^m \alpha_{ijq} b_q \in M_o$, за $\forall 1 \leq i, j \leq m$, S_o -модулът M_o е подпръстен на $R[a_1, \dots, a_n]$. От друга страна, R е подпръстен на S_o и $S_o = S_o b_m$ е подпръстен на M_o , така че R е подпръстен на M_o . Вземайки предвид $a_p = \sum_{q=1}^m \alpha_{pq} b_q \in M_o$ за $\forall 1 \leq p \leq n$ получаваме, че $R[a_1, \dots, a_n]$ се съдържа, а оттам и съвпада с M_o , $R[a_1, \dots, a_n] = M_o$.

По построение, S_o е подпръстен на S , така че S е S_o -модул. Пръстенът S_o е нютеров, а пръстенът S е S_o -подмодул на крайно породения S_o -модул $R[a_1, \dots, a_n]$, така че

$$S = S_o \sigma_1 + \dots + S_o \sigma_l$$

е крайно породен S_o -модул, съгласно Лема 4.24. От една страна,

$$S = S_o \sigma_1 + \dots + S_o \sigma_l \subseteq S_o[\sigma_1, \dots, \sigma_l].$$

От друга страна,

$$S_o[\sigma_1, \dots, \sigma_l] \subseteq S,$$

защото S_o е подпръстен на S , $\sigma_1, \dots, \sigma_l \in S$ и S е затворено относно умножение и събиране на свои елементи. Следователно

$$\begin{aligned} S &= S_o[\sigma_1, \dots, \sigma_l] = R[\alpha_{pq}, \alpha_{ijq} \mid 1 \leq p \leq n, \quad 1 \leq i, j, q \leq m][\sigma_r \mid 1 \leq r \leq l] = \\ &= R[\alpha_{pq}, \alpha_{ijq}, \sigma_r \mid 1 \leq p \leq n, \quad 1 \leq i, j, q \leq m, \quad 1 \leq r \leq l] \end{aligned}$$

е крайно породена R -алгебра, Q.E.D.

ЛЕМА 4.30. *Ако k е безкрайно поле и разширението $L \supset k$ е крайно породена k -алгебра, $L = k[a_1, \dots, a_n]$, то $a_1, \dots, a_n$ са алгебрични над k .
В частност, L е крайно разширение на k .*

Доказателство: Полето от частни $k(a_1, \dots, a_n)$ на $L = k[a_1, \dots, a_n]$ се съдържа, а оттам и съвпада с полето L . Да допуснем, че някой пораждащ a_i на L над k не е алгебричен над k и да изберем максимално трансцендентно (т.е. алгебрично независимо) подмножество $a_1, \dots, a_m$ на $a_1, \dots, a_n$. Тогава за $\forall m+1 \leq i \leq n$ съществува нетъждествено нулев полином $h_i(y_1, \dots, y_m, y_i) \in k[y_1, \dots, y_m, y_i]$ с $h_i(a_1, \dots, a_m, a_i) = 0$, зависещ от y_i .

Полето $L_o = k(a_1, \dots, a_m)$ на рационалните функции на $a_1, \dots, a_m$ с коефициенти от k е подполе на $k(a_1, \dots, a_n) = L$, съдържащо k . Полиномите

$$h_i(a_1, \dots, a_m, y_i) \in k[a_1, \dots, a_m][y_i] \subseteq L_o[y_i]$$

с корени a_i не се анулират тъждествено съгласно алгебричната независимост на $a_1, \dots, a_m$. По този начин, всички a_i за $m+1 \leq i \leq n$ се оказват алгебрични над L_o . От една страна имаме влагания на пръстени

$$L = k[a_1, \dots, a_n] \subseteq k[a_1, \dots, a_m][a_{m+1}, \dots, a_n] \subseteq L_o[a_{m+1}, \dots, a_n].$$

От друга страна, $L_o[a_{m+1}, \dots, a_n]$ е подпръстен на L , защото L_o е подполе на L , $a_{m+1}, \dots, a_n \in L$ и полето L е затворено относно умножение и събиране на свои елементи. Следователно $L = L_o[a_{m+1}, \dots, a_n]$ е крайно породена L_o -алгебра. Поради алгебричността на $a_{m+1}, \dots, a_n$ над L_o , степента $[L : L_o] < \infty$ е крайна и L е крайно породен L_o -модул. Прилагаме Лема 4.29 към нютеровата област с единица k , крайно породената k -алгебра $L = k[a_1, \dots, a_n]$ и подпръстена L_o на L , съдържащ k . Понеже L е крайномерно линейно пространство над L_o , полето

$$L_o = k \left[\frac{f_1(a_1, \dots, a_m)}{g_1(a_1, \dots, a_m)}, \dots, \frac{f_t(a_1, \dots, a_m)}{g_t(a_1, \dots, a_m)} \right]$$

е крайно породена k -алгебра за някакви полиноми $f_i(x_1, \dots, x_m), g_i(x_1, \dots, x_m) \in k[x_1, \dots, x_m]$, $g_i(a_1, \dots, a_m) \neq 0$. Всеки елемент $\lambda \in k$ е различен от a_m , защото a_m е алгебрично независимо над k . Оттук $\frac{1}{a_m - \lambda} \in L_o$ и съществуват неотрицателни цели $d_1, \dots, d_t$, както и полином $F_\lambda(x_1, \dots, x_m) \in k[x_1, \dots, x_m]$, за които

$$\frac{1}{a_m - \lambda} = \frac{F_\lambda(a_1, \dots, a_m)}{g_1(a_1, \dots, a_m)^{d_1} \dots g_t(a_1, \dots, a_m)^{d_t}}$$

Последното равенство е еквивалентно на

$$(a_m - \lambda)F_\lambda(a_1, \dots, a_m) = g_1(a_1, \dots, a_m)^{d_1} \dots g_t(a_1, \dots, a_m)^{d_t}.$$

Съгласно алгебричната независимост на a_m над $k(a_1, \dots, a_{m-1})$, получаваме равенството на полиноми

$$(x_m - \lambda)F_\lambda(a_1, \dots, a_{m-1}, x_m) = g_1(a_1, \dots, a_{m-1}, x_m)^{d_1} \dots g_t(a_1, \dots, a_{m-1}, x_m)^{d_t}$$

на променливата x_m с коефициенти от $k(a_1, \dots, a_{m-1})$. Множеството на корените на дясната страна е крайно и представлява обединението на корените на $g_i(a_1, \dots, a_{m-1}, x_m)$ за всички $1 \leq i \leq t$. Но всяко $x_m = \lambda \in k$ е корен на лявата страна, така че безкрайността на k води до противоречие, доказващо алгебричността на всяко a_i над k , Q.E.D.

ЗАДАЧА 4.31. *Да се докаже, че ако поле F е крайно породена $\mathbb{Z}$ -алгебра $F = \mathbb{Z}[a_1, \dots, a_n]$, то F е крайно поле.*

Упътване: Ако P е простото подполе на F , то $F = P[a_1, \dots, a_n]$ е крайно породена P -алгебра. Приложете Твърдение 4.30, за да получите, че F е крайномерно линейно пространство над P .

Ако допуснем, че F е безкрайно поле, то $P \simeq \mathbb{Q}$ е изоморфно на полето на рационалните числа. Приложете Твърдение 4.29 към ньотеровата комутативна област с единица $\mathbb{Z}$, крайно породената $\mathbb{Z}$ -алгебра $F = \mathbb{Z}[a_1, \dots, a_n]$ и подпръстена $P \simeq \mathbb{Q}$ на F , съдържащ $\mathbb{Z}$, за да получите противоречие.

ЛЕМА 4.32. *Ако F е алгебрично затворено поле, то всеки максимален идеал $\mathfrak{M}$ в $F[x_1, \dots, x_n]$ е от вида $\mathfrak{M} = \langle x_1 - a_1, \dots, x_n - a_n \rangle$ за някакви $a_1, \dots, a_n \in F$ и представлява идеала на полиномите, анулиращи се в точка $a = (a_1, \dots, a_n) \in F^n$.*

Доказателство: Всяко алгебрично затворено поле F е безкрайно. По-точно, ако $\text{char}(F) = 0$, то простото подполе на F е изоморфно на безкрайното поле $\mathbb{Q}$ на рационалните числа и $F \supset \mathbb{Q}$ е безкрайно поле. Ако $\text{char}(F) = p$ е просто число, то простото подполе на F е изоморфно на $\mathbb{F}_p$. Всеки елемент α на алгебричната обвивка $\overline{\mathbb{F}_p} = \cup_{m=1}^{\infty} \mathbb{F}_{p^m}$ на $\mathbb{F}_p$ е алгебричен над F и принадлежи на F . Следователно F съдържа безкрайното поле $\overline{\mathbb{F}_p} = \cup_{m=1}^{\infty} \mathbb{F}_{p^m}$ и $|F| = \infty$.
Фактор-пръстенът

$$L = F[x_1, \dots, x_n]/\mathfrak{M} = [(F + \mathfrak{M})/\mathfrak{M}] [x_1 + \mathfrak{M}, \dots, x_n + \mathfrak{M}]$$

е разширение на полето

$$(F + \mathfrak{M})/\mathfrak{M} \simeq F/(F \cap \mathfrak{M}) = F,$$

което в същото време е крайно породена алгебра над $(F + \mathfrak{M})/\mathfrak{M}$. Съгласно Лема 4.30, елементите $x_1 + \mathfrak{M}, \dots, x_n + \mathfrak{M}$ са алгебрични над $(F + \mathfrak{M})/\mathfrak{M} \simeq F$. Вземайки предвид алгебричната затвореност на F , стигаме до извода, че $x_i + \mathfrak{M} \in (F + \mathfrak{M})/\mathfrak{M}$ за $\forall 1 \leq i \leq n$. С други думи, съществуват $a_i \in F$ с $x_i + \mathfrak{M} = a_i + \mathfrak{M}$ или $x_i - a_i \in \mathfrak{M}$ за $\forall 1 \leq i \leq n$. Следователно идеалът $\mathfrak{M}_o := \langle x_1 - a_1, \dots, x_n - a_n \rangle \triangleleft F[x_1, \dots, x_n]$ се съдържа в максималния идеал $\mathfrak{M} \triangleleft F[x_1, \dots, x_n]$. Всеки елемент на фактор-пръстена $F[x_1, \dots, x_n]/\mathfrak{M}_o$ е от вида

$$f(x_1, \dots, x_n) + \mathfrak{M}_o = f(a_1, \dots, a_n) + \mathfrak{M}_o \in (F + \mathfrak{M}_o)/\mathfrak{M}_o,$$

така че

$$F[x_1, \dots, x_n]/\mathfrak{M}_o = (F + \mathfrak{M}_o)/\mathfrak{M}_o \simeq F/(F \cap \mathfrak{M}_o) = F$$

е поле. Следователно идеалът $\mathfrak{M}_o \triangleleft F[x_1, \dots, x_n]$ е максимален и съвпада с $\mathfrak{M} \supset \mathfrak{M}_o$, съгласно $\mathfrak{M} \neq F[x_1, \dots, x_n]$, Q.E.D.

Ако допуснем, че съществува $f(x_1, \dots, x_n) \in \mathfrak{M} \setminus \mathfrak{M}_o$, то $\mathfrak{M}_o \neq f(x_1, \dots, x_n) + \mathfrak{M}_o = f(a_1, \dots, a_n) + \mathfrak{M}_o$, съгласно $x_i - a_i \in \mathfrak{M}_o$. Оттук, $f(a_1, \dots, a_n) \in F^* \cap \mathfrak{M}$ и $\mathfrak{M} = F[x_1, \dots, x_n]$. Противоречието доказва, че $\mathfrak{M} = \mathfrak{M}_o$, Q.E.D.

ЗАДАЧА 4.33. *Нека k е поле с алгебрична обвивка $\bar{k}$, а $p(x) \in k[x]$ е неразложим над k полином от степен $\deg(p) = d \geq 2$ без кратни корени. Да се докаже, че фактор-пръстенът $k[x]/\langle p(x) \rangle$ е разширение на k от степен d , а идеалът $\langle p(x) \rangle \triangleleft k[x]$ на $\bar{k}[x]$, породен от $p(x)$ е произведение на d максимални идеала, отговарящи на точки от $\bar{k}$.*

ЗАДАЧА 4.34. *Нека k е поле, I е собствен идеал в пръстена $k[x_1, \dots, x_n]$ на полиномите на $x_1, \dots, x_n$ с коефициенти от k . Да се докаже, че съществува крайно разширение $F \supseteq k$ и елементи $a_1, \dots, a_n$ на полето F , такива че $f(a_1, \dots, a_n) = 0$ за $\forall f \in I$.*

Упътване: Изберете максимален идеал $\mathfrak{M}$ в $k[x_1, \dots, x_n]$, съдържащ I . Разгледайте полето $F = k[x_1, \dots, x_n]/\mathfrak{M}$ и елементите $a_i = x_i + \mathfrak{M}$ за $\forall 1 \leq i \leq n$.

3. Теорема на Hilbert за нулите

ЛЕМА-ОПРЕДЕЛЕНИЕ 4.35. Нека R е комутативен пръстен с единица R , а I е идеал в R . Тогава множеството

$$r(I) = \{x \in R \mid x^n \in I \text{ за някое } n \in \mathbb{N}\}$$

е идеал в R , съдържащ I и се нарича радикал на идеала I .

В частност, радикалът $\mathfrak{N} = r(\{0\})$ на нулевия идеал $\{0\} \triangleleft R$ е идеал в R , който се нарича нил-радикал на R . Съгласно

$$\mathfrak{N} = \{x \in R \mid x^n = 0 \text{ за някое } n \in \mathbb{N}\},$$

нил-радикалът се състои от нилпотентните елементи на R .

Доказателство: Ако $x, y \in r(I)$, то съществуват $m, n \in \mathbb{N}$, така че $x^m \in I$ и $y^n \in I$. В резултат,

$$\begin{aligned} (x - y)^{m+n-1} &= \sum_{i=0}^{n-1} (-1)^i \binom{m+n-1}{i} x^{m+n-1-i} y^i + \\ &+ \sum_{i=n}^{m+n-1} (-1)^i \binom{m+n-1}{i} x^{m+n-i} y^i \in I, \end{aligned}$$

защото $x^{m+n-1-i} \in I$ за $0 \leq i \leq n-1$ и $y^i \in I$ за $n \leq i \leq m+n-1$. Следователно $x - y \in r(I)$ и $(r(I), +)$ е подгрупа на $(R, +)$.

За произволно $x \in r(I)$ с $x^m \in I$ за някое $m \in \mathbb{N}$ и произволно $r \in R$ е в сила $rx \in r(I)$, съгласно $(rx)^m = r^m x^m \in I \triangleleft R$. Следователно $r(I)$ е идеал в R .

Непосредствено се вижда, че всеки елемент на I се съдържа в $r(I)$, Q.E.D.

ТВЪРДЕНИЕ 4.36. Ако R е комутативен пръстен с единица, то нил-радикалът

$$\mathfrak{N} = \cap_{\mathfrak{p} \triangleleft R} \mathfrak{p}$$

на R съвпада със сечението на всички прости идеали $\mathfrak{p} \triangleleft R$.

Радикалът

$$r(I) = \cap_{I \subseteq \mathfrak{p} \triangleleft R} \mathfrak{p}$$

на произволен идеал $I \triangleleft R$ съвпада със сечението на простите идеали $\mathfrak{p}$ в R , съдържащи I .

Доказателство: Ако $x \in \mathfrak{N}$, то съществува $n \in \mathbb{N}$, така че $x^n = 0$ принадлежи на всеки прост идеал $\mathfrak{p}$ в R . Оттук $x \in \mathfrak{p}$ и нил-радикалът $\mathfrak{N} \subseteq \cap_{\mathfrak{p} \triangleleft R} \mathfrak{p}$ се съдържа в сечението на простите идеали $\mathfrak{p}$ в R .

Обратното включване $\cap_{\mathfrak{p} \triangleleft R} \mathfrak{p} \subseteq \mathfrak{N}$ е еквивалентно на включването

$$R \setminus \mathfrak{N} \subseteq R \setminus (\cap_{\mathfrak{p} \triangleleft R} \mathfrak{p})$$

на съответните допълнения. За произволен елемент $x \in R \setminus \mathfrak{N}$ разглеждаме множеството

$$\Sigma_x := \{J \triangleleft R \mid x \notin r(J)\}$$

на идеалите J в R , чиито радикали $r(J) \triangleleft R$ не съдържат x . Множеството $\Sigma_x \neq \emptyset$ не е празно, защото нулевият идеал $\{0\} \in \Sigma_x$. Произволно линейно наредено подмножество $\{J_\alpha\}_{\alpha \in A} \subseteq \Sigma_x$ има горна граница $J_\infty := \cup_{\alpha \in A} J_\alpha$. Както в доказателството на Лема ?? проверяваме, че J_∞ е идеал в R . Ако $x \in r(J_\infty)$, то $x^n \in J_\infty$ за някое $n \in \mathbb{N}$. Следователно $x^n \in J_\alpha$ за някое $\alpha \in A$ и $x \in r(J_\alpha)$, противно на избора на $J_\alpha \in \Sigma_x$. Следователно $x \notin r(J_\infty)$ и $J_\infty \in \Sigma_x$. Ясно е, че $J_\infty \supseteq J_\alpha$ за $\forall \alpha \in A$. Съгласно Лемата на Zorn, Σ_x има максимален елемент J . Достатъчно е да докажем, че идеалът J е прост, за да получим съвпадението $\mathfrak{N} = \cap_{\mathfrak{p} \triangleleft R} \mathfrak{p}$ на нил-радикала $\mathfrak{N}$ със сечението на простите идеали в R .

Ако идеалът $J \triangleleft R$ не е прост, то съществуват $a, b \in R \setminus J$ с $ab \in J$. Тогава идеалите $J_1 := J + \langle a \rangle \supsetneq J$ и $J_2 := J + \langle b \rangle \supsetneq J$ не принадлежат на Σ_x заради максималността на $J \in \Sigma_x$. Следователно съществуват $m, n \in \mathbb{N}$ с $x^m = \alpha + ar_1 \in J_1$, $x^n = \beta + br_2 \in J_2$ за някои $\alpha, \beta \in J$, $r_1, r_2 \in R$. Оттук, $x^{m+n} = (\alpha\beta + \alpha br_2 + \beta ar_1) + abr_1r_2 \in J$ и $x \in r(J)$, противно на избора на $J \in \Sigma_x$. Това доказва, че идеалът J е прост и $\mathfrak{N} = \bigcap_{\mathfrak{p} \triangleleft R} \mathfrak{p}$.

Идеалите $\bar{J}$ в R/I са от вида J/I за някакъв идеал $J \triangleleft R$, съдържащ I . Наистина, ако $I \subseteq J \triangleleft R$, то $\bar{J} = J/I \triangleleft R/I$. За произволен идеал $\bar{J} \triangleleft R/I$, множеството

$$J := \{x \in R \mid x + I \in \bar{J}\}$$

е идеал в R , съдържащ I и $J/I = \{x + I \mid x \in J\} = \bar{J}$. По-точно, ако $x, y \in J$, то $(x + I) - (y + I) = x - y + I \in \bar{J} \triangleleft R/I$, така че $x - y \in J$ и $(J, +)$ е подгрупа на $(R, +)$. За $\forall x \in J$ и $\forall r \in R$ имаме $(r + I)(x + I) = rx + I \in \bar{J} \triangleleft R/I$, откъдето $rx \in J$ и $J \triangleleft R$ е идеал в R . За $\forall x \in I$ е в сила $x + I = I \in \bar{J}$, защото нулевият елемент I на R/I принадлежи на всеки идеал $\bar{J} \triangleleft R/I$. Съвпадението $J/I = \bar{J}$ е непосредствено следствие от определението на J .

Фактор-пръстенът $(R/I)/\bar{J} \simeq R/J$ на идеал $\bar{J} \triangleleft R/I$ съвпада с фактор-пръстена R/J по неговото повдигане $J \triangleleft R$. По-точно, изображението

$$\varphi : R/I \longrightarrow R/J,$$

$$\varphi(r + I) = r + J \quad \text{за} \quad \forall r \in R$$

е коректно определен епиморфизъм на пръстени, съгласно $I \subseteq J$. Ядрото на φ е $\ker(\varphi) = J/I = \bar{J}$ и индуцираното изображение

$$\bar{\varphi} : (R/I)/\bar{J} \longrightarrow R/J,$$

$$\bar{\varphi}((r + I) + \bar{J}) = r + J \quad \text{за} \quad \forall r \in R$$

е коректно определен изоморфизъм на пръстени, съгласно Теоремата за хомоморфизмите.

Идеалът $\bar{J} \triangleleft R/I$ е прост тогава и само тогава, когато повдигането му $J \triangleleft R$ е прост идеал. Еквивалентно, фактор-пръстенът $(R/I)/\bar{J}$ е област на цялост точно когато R/J е област на цялост.

Да забележим, че нил-радикалът на R/I е

$$\begin{aligned} \mathfrak{N}(R/I) &= \{r + I \in R/I \mid (r + I)^n = I \text{ за някое } n \in \mathbb{N}\} = \\ &= \{r + I \in R/I \mid r^n \in I \text{ за някое } n \in \mathbb{N}\} = r(I)/I. \end{aligned}$$

Вземайки предвид, че $\mathfrak{N}(R/I)$ е сечението на простите идеали $\bar{\mathfrak{p}} \triangleleft R/I$, получаваме, че

$$r(I)/I = \bigcap_{\bar{\mathfrak{p}} \triangleleft R/I} \bar{\mathfrak{p}} = \bigcap_{I \subseteq \mathfrak{p} \triangleleft R} (\mathfrak{p}/I) = (\bigcap_{I \subseteq \mathfrak{p} \triangleleft R} \mathfrak{p})/I$$

е факторът на сечението $\bigcap_{I \subseteq \mathfrak{p} \triangleleft R} \mathfrak{p}$ на простите идеали $\mathfrak{p}$ в R , съдържащи I .

Твърдим, че

$$r(I) = \bigcap_{I \subseteq \mathfrak{p} \triangleleft R} \mathfrak{p}.$$

По-общо, ако J_1 и J_2 са идеали в R , съдържащи идеала I и факторите $J_1/I = J_2/I$ съвпадат, то и идеалите $J_1 = J_2$ съвпадат. Наистина, за всяко $x_1 \in J_1$ съществува $x_2 \in J_2$, така че $x_1 + I = x_2 + I$. Тогава $x = x_1 - x_2 \in I \subseteq J_2$, така че $x_1 = x + x_2 \in J_2$ и $J_1 \subseteq J_2$. Аналогично проверяваме, че $J_2 \subseteq J_1$, откъдето $J_1 = J_2$, Q.E.D.

ТЕОРЕМА 10. (Теорема на Hilbert за нулите) Нека k е алгебрично затворено поле, I е идеал в $k[x_1, \dots, x_n]$,

$$V(I) = \{a = (a_1, \dots, a_n) \in k^n \mid f(a_1, \dots, a_n) = 0 \text{ за } \forall f \in I\}$$

е афинното алгебрично множество, определено от I , а

$$IV(I) = \{g \in k[x_1, \dots, x_n] \mid g(a_1, \dots, a_n) = 0 \text{ за } \forall a = (a_1, \dots, a_n) \in V(I)\}$$

е идеалът на $V(I)$ в $k[x_1, \dots, x_n]$. Тогава

$$IV(I) = r(I)$$

за радикала $r(I) \triangleleft k[x_1, \dots, x_n]$ на I .

Доказателство: Включването $r(I) \subseteq IV(I)$ е тривиално, защото ако $f^m \in I$ за полином $f \in k[x_1, \dots, x_n]$ и $m \in \mathbb{N}$, то $f^m(a_1, \dots, a_n) = 0$ за всяка точка $(a_1, \dots, a_n) \in V(I)$. Поради липсата на делители на нулата в полето k , оттук следва $f(a_1, \dots, a_n) = 0$, така че $f \in IV(I)$.

Обратното включване $IV(I) \subseteq r(I)$ е еквивалентно на включването

$$k[x_1, \dots, x_n] \setminus r(I) \subseteq k[x_1, \dots, x_n] \setminus IV(I)$$

на съответните допълнения. Ако $f(x_1, \dots, x_n) \in k[x_1, \dots, x_n] \setminus r(I)$, то съгласно Твърждение 4.36 съществува прост идеал $\mathfrak{p} \triangleleft k[x_1, \dots, x_n]$, съдържащ I , така че $f(x_1, \dots, x_n) \notin \mathfrak{p}$. Фактор-пръстенът

$$R_1 := k[x_1, \dots, x_n]/\mathfrak{p} = (k + \mathfrak{p})/\mathfrak{p}[x_1 + \mathfrak{p}, \dots, x_n + \mathfrak{p}]$$

е област на цялост и се влага в поле от частни Q_1 . Понеже $f + \mathfrak{p} \neq \mathfrak{p}$ е ненулев елемент на R_1 , съществува $(f + \mathfrak{p})^{-1} = \frac{1}{f + \mathfrak{p}} \in Q_1$ и можем да разгледаме подпръстена

$$R_2 = R_1 \left[\frac{1}{f + \mathfrak{p}} \right] \simeq (k + \mathfrak{p})/\mathfrak{p} \left[x_1 + \mathfrak{p}, \dots, x_n + \mathfrak{p}, \frac{1}{f + \mathfrak{p}} \right]$$

на Q_1 , който е крайно породена k -алгебра. Произволен максимален идеал $\mathfrak{M}$ на R_2 не съдържа $f + \mathfrak{p}$, защото $f + \mathfrak{p} \in R_2^*$ е обратим в R_2 . Полето

$$R_2/\mathfrak{M} \simeq (k + \mathfrak{M})/\mathfrak{M} \left[x_1 + \mathfrak{M}, \dots, x_n + \mathfrak{M}, \frac{1}{f + \mathfrak{p}} + \mathfrak{M} \right]$$

е изоморфно на алгебрично затвореното поле k . Следователно съществуват $a_1, \dots, a_n, a_0 \in k$, така че $x_i + \mathfrak{M} = a_i + \mathfrak{M}$ за $\forall 1 \leq i \leq n$ и $f + \mathfrak{M} = a_0 + \mathfrak{M} \neq \mathfrak{M}$. Ако $g \in I \subseteq \mathfrak{p}$, то $g + \mathfrak{p} = \mathfrak{p}$ е нулевият елемент на R_1 и R_2 , така че

$$g + \mathfrak{M} = g(x_1 + \mathfrak{M}, \dots, x_n + \mathfrak{M}) = g(a_1 + \mathfrak{M}, \dots, a_n + \mathfrak{M}) = g(a_1, \dots, a_n) + \mathfrak{M} = \mathfrak{M}$$

е нулевият елемент на $R_2/\mathfrak{M}$. Следователно $g(a_1, \dots, a_n) \in k \cap \mathfrak{M} = \{0\}$ и точката $(a_1, \dots, a_n) \in V(I)$ се съдържа в нулите на идеала I . Ако допуснем, че $f \in IV(I)$, то $f(a_1, \dots, a_n) = 0$. В резултат,

$$a_0 + \mathfrak{M} = f + \mathfrak{M} = f(x_1 + \mathfrak{M}, \dots, x_n + \mathfrak{M}) = f(a_1, \dots, a_n) + \mathfrak{M} = \mathfrak{M}.$$

Противоречието доказва, че $f \notin IV(I)$. С други думи, $k[x_1, \dots, x_n] \setminus r(I)$ се съдържа в $k[x_1, \dots, x_n] \setminus IV(I)$, откъдето $IV(I) \subseteq r(I)$ и $IV(I) = r(I)$, Q.E.D.

ОПРЕДЕЛЕНИЕ 4.37. Идеалът I на комутативен пръстен с единица R се нарича радикален, ако съвпада с радикала си $r(I) = I$.

Непосредствено се вижда, че радикалът $r(I)$ на произволен идеал I в комутативен пръстен с единица R е радикален идеал. По-точно, ако $x^n \in r(I)$ за някое $n \in \mathbb{N}$, то съществува $m \in \mathbb{N}$, така че $(x^n)^m = x^{mn} \in I$. Следователно $x \in r(I)$ и $r(r(I)) = r(I)$.

ЗАДАЧА 4.38. Да се докаже, че:

- (i) всеки прост идеал $\mathfrak{p}$ в комутативен пръстен с единица R е радикален;
- (ii) всеки максимален идеал $\mathfrak{M}$ в комутативен пръстен с единица R е радикален;
- (iii) идеалът $I(X) = \{f(x_1, \dots, x_n) \in k[x_1, \dots, x_n] \mid f(a) = 0 \text{ за } \forall a \in X\}$ на подмножество $X \subseteq k^n$ на афинно пространство k^n над поле k е радикален.

Упътване: За (ii) използвайте, че всяко поле е комутативна област с единица, така че всеки максимален идеал в комутативен пръстен с единица R е прост идеал.

ЗАДАЧА 4.39. (Слаба форма на Теоремата на Hilbert за нулите) *Да се докаже, че ако k е алгебрично затворено поле, а I е идеал в $k[x_1, \dots, x_n]$ с празно множество на нулите $V(I) = \emptyset$, то $I = k[x_1, \dots, x_n]$ съвпада с целия полиномиален пръстен $k[x_1, \dots, x_n]$.*

Упътване: Допуснете, че $I \subsetneq k[x_1, \dots, x_n]$ и изберете максимален идеал $\mathfrak{M}$ в $k[x_1, \dots, x_n]$, съдържащ I . Тогава $\mathfrak{M} = \langle x_1 - a_1, \dots, x_n - a_n \rangle$ за някои $a_1, \dots, a_n \in k$ и афинното алгебрично множество $\emptyset = V(I) \supseteq V(\mathfrak{M}) = \{(a_1, \dots, a_n)\}$.