Глава 6

Рационални и затворени точки върху проективни алгебрични множества

1. $\mathbb{F}_q$-рационални и $\mathbb{F}_q$-затворени точки на проективното пространство $\mathbb{P}^n(\overline{\mathbb{F}_q})$

Определение 6.1. *Множеството* $\mathbb{P}^n(\overline{k}) = \left(\overline{k}^{n+1} \setminus \{(0,\ldots,0)\}\right)/\overline{k^*}$ *на правите през началото* $(0,0) \in \overline{k}^{n+1}$ *в афинното пространство* $\overline{k}^{n+1}$ *се нарича n-мерно проективно пространство.*

Точките $a \in \mathbb{P}^n(\overline{k})$ представляват класове на пропорционалност на

$$(a_0, a_1, \ldots, a_n) \in \overline{k}^{n+1} \setminus \{(0,\ldots,0)\},$$

които ще бележим с $a = [a_0 : a_1 : \ldots : a_n]$. Компонентите $a_0, \ldots, a_n$ се наричат хомогенни координати на a и са определени с точност до ненулев множител от $\overline{k}$.
Проективното пространство $\mathbb{P}^n(\overline{k}) = \cup_{i=0}^n U_i$ се покрива от стандартните афинни подмножества

$$U_i = \{x = [x_0 : \ldots : x_i : \ldots : x_n] \in \mathbb{P}^n(\overline{k}) \quad | \quad x_i \neq 0\}.$$

Изображенията

$$\varphi_i : U_i \longrightarrow \overline{k}^n,$$

$$\varphi_i([x_0 : \ldots : x_i : \ldots : x_n]) = \left(\frac{x_0}{x_i}, \ldots, \frac{x_{i-1}}{x_i}, \frac{x_{i+1}}{x_i}, \ldots, \frac{x_n}{x_i}\right)$$

са взаимно еднозначни.

Определение 6.2. *Точките $x \in \mathbb{P}^n(\overline{k})$, които имат представяне от вида $x = [x_0 : \ldots : x_n]$ с $x_i \in k$ за $\forall 0 \leq i \leq n$ се наричат k-рационални.*

Точката $x \in \mathbb{P}^n(\overline{k})$ е k-рационална точно когато има представяне от вида $x = [a_0 : \ldots : a_{i-1} : 1 : a_{i+1} : \ldots : a_n]$ с $(a_0, \ldots, a_{i-1}, a_{i+1}, \ldots, a_n) \in k^n$.

Лема 6.3. *Броят на $\mathbb{F}_q$-рационалните точки $\mathbb{P}^n(\mathbb{F}_q)$ на проективното пространство $\mathbb{P}^n(\overline{\mathbb{F}_q})$ е*

$$|\mathbb{P}^n(\mathbb{F}_q)| = \frac{q^{n+1}-1}{q-1}.$$

Доказателство: Множеството $\mathbb{F}_q^{n+1} \setminus \{(0,\ldots,0)\}$ има $q^{n+1}-1$ елемента. Всяка $\mathbb{F}_q^*$-орбита върху $\mathbb{F}_q^{n+1} \setminus \{(0,\ldots,0)\}$ се състои от $q-1$ точки и броят на $\mathbb{F}_q^*$-орбитите върху $\mathbb{F}_q^{n+1} \setminus \{(0,\ldots,0)\}$ е $\frac{q^{n+1}-1}{q-1} = |\mathbb{P}^n(\mathbb{F}_q)|$, Q.E.D.

Лема 6.4. *Абсолютната група на Galois $Gal(\overline{k}/k)$ на съвършено поле k действа върху проективното пространство $\mathbb{P}^n(\overline{k})$.*
Фиксираните точки на $Gal(\overline{k}/k)$ върху $\mathbb{P}^n(\overline{k})$ са точно k-рационалните,

$$\mathbb{P}^n(\overline{k})^{Gal(\overline{k}/k)} = \mathbb{P}^n(k).$$

Доказателство: Действието на $Gal(\overline{k}/k)$ върху афинното пространство $\overline{k}^{n+1}$ се ограничава до действие на $Gal(\overline{k}/k)$ върху $\overline{k}^{n+1} \setminus \{(0,\dots 0)\}$. По-точно, за $\forall \varphi \in Gal(\overline{k}/k)$ и за $\forall (x_0,\dots,x_n) \in \overline{k}^{n+1} \setminus \{(0,\dots,0)\}$ с $x_i \neq 0$ имаме $\varphi(x_i) \neq 0$ съгласно $\varphi(0) = 0$ и взаимната еднозначност на φ. Следователно $\varphi(x_0,\dots,x_n) = (\varphi(x_0),\dots,\varphi(x_n)) \in \overline{k}^{n+1} \setminus \{(0,\dots 0)\}$. Ако $(x_0,x_1,\dots,x_n) \in \overline{k}^{n+1} \setminus \{(0,\dots,0)\}$ и $(\lambda x_0, \lambda x_1,\dots,\lambda x_n) \in \overline{k}^{n+1} \setminus \{(0,\dots,0)\}$ с $\lambda \in \overline{k}^*$ са точки от една и съща $\overline{k}^*$-орбита, то за $\forall \varphi \in Gal(\overline{k}/k)$ е изпълнено

$$\varphi(\lambda x_0,\dots,\lambda x_n) = (\varphi(\lambda)\varphi(x_0),\dots,\varphi(\lambda)\varphi(x_n))$$

с $\varphi(\lambda) \in \overline{k}^*$, така че $\varphi(x_0,\dots,x_n)$ и $\varphi(\lambda x_0,\dots,\lambda x_n)$ са от една и съща $\overline{k}^*$-орбита. По този начин, действието на $Gal(\overline{k}/k)$ върху $\overline{k}^{n+1} \setminus \{(0,\dots,0)\}$ индуцира коректно зададено действие на $Gal(\overline{k}/k)$ върху множеството $\mathbb{P}^n(\overline{k})$ на $\overline{k}^*$-орбитите върху $\overline{k}^{n+1} \setminus \{(0,\dots,0)\}$.
Непосредствено се проверява, че $\varphi_i : U_i \to \overline{k}$ са еквивариантни относно действието на абсолютната група на Galois $Gal(\overline{k}/k)$. По-точно, $\varphi\varphi_i(a) = \varphi_i\varphi(a)$ за всяка точка $a \in U_i$. Точката $a = [a_0 : a_1 : \dots : a_n] \in \mathbb{P}^n(\overline{k})$ с $a_i \neq 0$ е неподвижна под действие на $Gal(\overline{k}/k)$ тогава и само тогава, когато $\varphi_i(a) = \left(\frac{a_0}{a_i},\dots,\frac{a_{i-1}}{a_i},\frac{a_{i+1}}{a_i},\dots,\frac{a_n}{a_i}\right) \in \overline{k}^n$ е неподвижна точка на $Gal(\overline{k}/k)$ за някое $0 \leq i \leq n$ с $a_i \neq 0$. Последното е еквивалентно на k-рационалност на $\varphi_i(a)$, а оттам и на a, Q.E.D.

Определение 6.5. *Орбитите $P = Orb_{Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)}(a)$ на $a \in \mathbb{P}^n(\overline{\mathbb{F}_q})$ под действие на абсолютната група на Galois $Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ на крайно поле $\mathbb{F}_q$ се наричат $\mathbb{F}_q$-затворени точки на $\mathbb{P}^n(\overline{\mathbb{F}_q})$.*
Елементите на $\mathbb{F}_q$-затворена точка върху $\mathbb{P}^n(\overline{\mathbb{F}_q})$се наричат $\mathbb{F}_q$-спрегнати.

Разсъжденията от доказателството на Лема 6.4 доказват следната

Лема 6.6. *Ако a е точка от стандартното афинно подмножество $U_i \subset \mathbb{P}^n(\overline{\mathbb{F}_q})$, то $\mathbb{F}_q$-затворената точка $Orb_{Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)}(a) \subset U_i$ се съдържа изцяло в U_i и се изобразява изоморфно върху $\mathbb{F}_q$-затворената точка*

$$\varphi_i Orb_{Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)}(a) = Orb_{Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)}\varphi_i(a) \subset \overline{\mathbb{F}_q}^n$$

на афинното пространство $\overline{\mathbb{F}_q}^n$.

Определение 6.7. *Дефиниционното поле на точка $a = [a_0 : \dots : a_n] \in \mathbb{P}^n(\overline{\mathbb{F}_q})$ се определя като разширението $\mathbb{F}_q\left(\frac{a_0}{a_i},\dots,\frac{a_{i-1}}{a_i},\frac{a_{i+1}}{a_i},\dots,\frac{a_n}{a_i}\right)$ на $\mathbb{F}_q$ за някое $a_i \neq 0$.*

Лема 6.8. *Дефиниционното поле $\mathbb{F}_q\left(\frac{a_0}{a_i},\dots,\frac{a_{i-1}}{a_i},\frac{a_{i+1}}{a_i},\dots,\frac{a_n}{a_i}\right)$ на точка $a = [a_0 : \dots : a_n] \in \mathbb{P}^n(\overline{\mathbb{F}_q})$ над $\mathbb{F}_q$ не зависи от избора на $a_i \neq 0$.*

Доказателство: Достатъчно е да проверим, че ако $a_0 \neq 0$ и $a_1 \neq 0$, то

$$\mathbb{F}_q\left(\frac{a_1}{a_0},\ \frac{a_i}{a_0}\ \Big|\ 2 \leq i \leq n\right) = \mathbb{F}_q\left(\frac{a_0}{a_1},\ \frac{a_i}{a_1}\ \Big|\ 2 \leq i \leq n\right). \tag{6.1}$$

За целта, полагаме

$$c = \frac{a_1}{a_0}$$

и свеждаме (6.1) към

$$\mathbb{F}_q\left(c,\ \frac{a_i}{a_0}\ \Big|\ 2 \leq i \leq n\right) = \mathbb{F}_q\left(c^{-1},\ c^{-1}\frac{a_i}{a_0}\ \Big|\ 2 \leq i \leq n\right) \tag{6.2}$$

От $c^{-1} \in \mathbb{F}_q\left(c, \ \frac{a_i}{a_0} \ \Big| \ 2 \leq i \leq n\right)$ и $c^{-1}\frac{a_i}{a_0} \in \mathbb{F}_q\left(c, \frac{a_i}{a_0} \ \Big| \ 2 \leq i \leq n\right)$ следва

$$\mathbb{F}_q\left(c^{-1}, \ \ c^{-1}\frac{a_i}{a_0} \ \ \Big| \ \ 2 \leq i \leq n\right) \subseteq \mathbb{F}_q\left(c, \ \ \frac{a_i}{a_0} \ \ \Big| \ \ 2 \leq i \leq n\right).$$

От друга страна, $c \in \mathbb{F}_q\left(c^{-1}, \ \ c^{-1}\frac{a_i}{a_0} \ \ \Big| \ \ 2 \leq i \leq n\right)$ и

$$\frac{a_i}{a_0} = c\left(c^{-1}\frac{a_i}{a_0}\right) \in \mathbb{F}_q\left(c^{-1}, \ \ c^{-1}\frac{a_i}{a_0} \ \ \Big| \ \ 2 \leq i \leq n\right)$$

дават $\mathbb{F}_q\left(c, \ \ \frac{a_i}{a_0} \ \ \Big| \ \ 2 \leq i \leq n\right) \subseteq \mathbb{F}_q\left(c^{-1}, \ \ c^{-1}\frac{a_i}{a_0} \ \ \Big| \ \ 2 \leq i \leq n\right)$. Това доказва (6.2), Q.E.D.

От Лема 6.8 и Лема-Определение 4.4 следва, че дефиниционното поле на точка $a \in \mathbb{P}^n(\overline{\mathbb{F}_q})$ съвпада с дефиниционното поле на $\sigma(a) \in \mathbb{P}^n(\overline{\mathbb{F}_q})$ за произволен автоморфизъм $\sigma \in Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$. Това дава възможност да определим дефиниционното поле на $\mathbb{F}_q$-затворена точка върху $\mathbb{P}^n(\overline{\mathbb{F}_q})$ над $\mathbb{F}_q$ като дефиниционното поле на произволен неин елемент над $\mathbb{F}_q$.

Комбинирайки Лема 6.8 с Твърдение-Определение 4.5 получаваме следващото

Следствие-Определение 6.9. *(i) Всяка $\mathbb{F}_q$-затворена точка*

$$P = Orb_{Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)}(a),$$

$a \in \mathbb{P}^n(\overline{\mathbb{F}_q})$ е крайно множество.

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

(ii) Степента на $\mathbb{F}_q$-затворена точка $P = Orb_{Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)}(a)$ върху проективното пространство $\mathbb{P}^n(\overline{\mathbb{F}_q})$ е минималното естествено $m \in \mathbb{N}$, за което има представяне $a = [a_0 : \ldots : a_n] \in \mathbb{P}^n(\overline{\mathbb{F}_q})$ с $a_0, \ldots, a_n \in \mathbb{F}_{q^m}$.

(iii) Степента на $\mathbb{F}_q$-затворена точка $P = Orb_{Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)}(a)$ върху $\mathbb{P}^n(\overline{\mathbb{F}_q})$ е минималното естествено число m, за което автоморфизмът на Frobenius Φ_{q^m} оставя на място a, $\Phi_{q^m}(a) = a$.

(iv) Степента на $\mathbb{F}_q$-затворена точка $P = Orb_{Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)}(a)$ върху $\mathbb{P}^n(\overline{\mathbb{F}_q})$ съвпада със степента $\left[\mathbb{F}_q\left(\frac{a_0}{a_i}, \ldots, \frac{a_{i-1}}{a_i}, \frac{a_{i+1}}{a_i}, \ldots, \frac{a_n}{a_i}\right) : \mathbb{F}_q\right]$ на дефиниционното поле на $a \in \mathbb{P}^n(\overline{\mathbb{F}_q})$ над $\mathbb{F}_q$.

Задача 6.10. *В означенията от Задача 4.6 да се намерят $\mathbb{F}_2$-затворените точки*

$$S = Orb_{Gal(\overline{\mathbb{F}_2}/\mathbb{F}_2)}[\alpha_4 : \alpha_4^2 : \alpha_8], \quad T = Orb_{Gal(\overline{\mathbb{F}_2}/\mathbb{F}_2)}[\alpha_4 - \alpha_8 : \alpha_8 : 1 + \alpha_4]$$

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

Лема 6.8 и Твърдение 4.7 дават следното

Следствие 6.11. *Ако $P = Orb_{Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)}(a)$, $a \in \mathbb{P}^n(\overline{\mathbb{F}_q})$ е $\mathbb{F}_q$-затворена точка върху $\mathbb{F}^n(\overline{\mathbb{F}_q})$, r е естествено число, $d = GCD(m, r)$ е най-големият общ делител на m и r, то*

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

се разлага в непресичащо се обединение от d на брой $\mathbb{F}_{q^r}$-затворени точки P_j от степен $\deg(P_j) = \frac{m}{d}$.

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

ЗАДАЧА 6.12. *В означенията от задача 4.6 да се разложат $\mathbb{F}_2$-затворените точки*

$$S = Orb_{Gal(\overline{\mathbb{F}_2}/\mathbb{F}_2)}[\alpha_4 : \alpha_4^2 : \alpha_8], \quad T = Orb_{Gal(\overline{\mathbb{F}_2}/\mathbb{F}_2)}[\alpha_4 - \alpha_8 : \alpha_8 : 1 + \alpha_4]$$

в непресичащо се обадинение на $\mathbb{F}_{2^r}$-затворени точки за $r = 2, 3, 6$.

2. $\mathbb{F}_q$-рационални и $\mathbb{F}_q$-затворени точки за проективни алгебрични множества

ОПРЕДЕЛЕНИЕ 6.13. *За произволна фамилия $S \subseteq \overline{k}[x_0, x_1, \dots, x_n]_h$ от хомогенни полиноми множеството*

$$Z(S) = \{a = [a_0 : \dots : a_n] \in \mathbb{P}^n(\overline{k}) \quad | \quad f(a) = 0 \quad \text{за всеки} \quad f \in S\}$$

на нулите на хомогенните полиноми от S в $\mathbb{P}^n(\overline{k})$ се нарича проективно алгебрично множество.

Ако $f(x_0, \dots, x_n) \in \overline{k}[x_0, \dots, x_n]$ е хомогенен полином от степен d, то за $\forall a = [a_0 : \dots : a_i : \dots : a_n] \in \mathbb{P}^n(\overline{k})$ и $\forall \lambda \in \overline{k}^*$ е в сила $f(\lambda a_0, \lambda a_n) = \lambda^d f(a_0, \dots, a_n)$. Следователно $f(a_0, \dots, a_n) = 0$ тогава и само тогава, когато $f(\lambda a_0, \dots, \lambda a_n) = 0$ или произволен хомогенен полином $f(x_0, \dots, x_n)$ се анулира в $(a_0, \dots, a_n)$ точно когато се анулира във всички точки $(\lambda a_0, \dots, \lambda a_n) \in \overline{k}^{n+1} \setminus \{(0, \dots, 0)\}$, пропорционални на $(a_0, \dots, a_n)$. По този начин, анулирането на хомогенен полином $f(x_0, \dots, x_n)$ в точка $a \in \mathbb{P}^n(\overline{k})$ е коректно определено като анулиране на $f(x_0, \dots, x_n)$ във всички повдигания на a до точки на $\overline{k}^{n+1} \setminus \{(0, \dots, 0)\}$. Нехомогенен полином $g(x_0, \dots, x_n) \in \overline{k}[x_1, \dots, x_n]$ може да се анулира в някои точки от $\overline{k}^*$-орбита и да не се анулира в други точки от същата орбита. Например $g(x_0, x_1) = x_0 - 1$ се анулира в $(1, 1) \in \overline{k}^2 \setminus \{(0, 0)\}$, но не се анулира в точките $(\lambda, \lambda) \in Orb_{\overline{k}^*}(1, 1) \subset \overline{k}^2 \setminus \{(0, 0)\}$ с $\lambda \in \overline{k}^* \setminus \{1\}$. Затова не можем да определим нулите на $g(x_0, x_1) = x_0 - 1$ върху $\mathbb{P}^1(\overline{k})$.
Ако k е съвършено поле, то абсолютната група на Galois $Gal(\overline{k}/k)$ действа върху множеството $\overline{k}[x_0, \dots, x_n]_h$ на хомогенните полиноми с коефициенти от алгебричната обвивка $\overline{k}$ и фиксираните точки за това действие са хомогенните полиноми $k[x_0, \dots, x_n]_h$ с коефициенти от k.

ОПРЕДЕЛЕНИЕ 6.14. *Ако $S \subseteq k[x_1, \dots, x_n]_h$ се състои от хомогенни полиноми с коефициенти от k, то проективното алгебрично множество $Z(S)/k$ е определено над k.*
Ако $Z(S)/k$ е проективно алгебрично множество, определено над k, то сечението

$$Z(S)(k) := Z(S) \cap \mathbb{P}^n(k)$$

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

Непосредствено се вижда, че ако k е съвършено поле, то $Gal(\overline{k}/k)$ действа върху всяко проективно алгебрично множество $Z(S)$, определено над k. При това, $Gal(\overline{k}/k)$-фиксираните точки на това действие са точно k-рационалните,

$$Z(S)^{Gal(\overline{k}/k)} = Z(S)(k).$$

Нека $Z(S)/\mathbb{F}_q$ е проективно алгебрично множество, определено над $\mathbb{F}_q$ и $a \in Z(S)$. Тогава $\mathbb{F}_q$-затворената точка $P = Orb_{Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)}(a)$ върху $\mathbb{P}^n(\overline{\mathbb{F}_q})$, породена от a се съдържа изцяло в $Z(S)$ и се нарича $\mathbb{F}_q$-затворена точка на $Z(S)$.

ОПРЕДЕЛЕНИЕ 6.15. *Идеалът $I \triangleleft k[x_1, \dots, x_n]$ е хомогенен, ако се поражда от хомогенни полиноми.*

Определение 6.16. *Хомогенният идеал $I_h(Z(S)) \triangleleft \overline{k}[x_0, \dots, x_n]$, породен от хомогенните полиноми $f(x_0, \dots, x_n) \in \overline{k}[x_0, \dots, x_n]_h$, анулиращи се върху $Z(S)$ се нарича хомогенен идеал на проективното алгебрично множество $Z(S) \subseteq \mathbb{P}^n(\overline{k})$.*

Лема 6.17. *Идеалът $I \triangleleft k[x_1, \dots, x_n]$ е хомогенен тогава и само тогава, когато за всеки елемент $f = \sum\limits_{i=0}^{m} f^{[i]}$ на I хомогенните компоненти $f^{[i]}$ на f от степен i принадлежат на I.*

Доказателство: Ако идеалът $I = \langle f_1, \dots, f_s \rangle$ се поражда от хомогенни полиноми $f_1, \dots, f_s \in F[x_1, \dots, x_n]$, то произволен елемент на I е от вида

$$f = \sum_{j=1}^{s} g_j f_j.$$

Ако $\deg(f_j) = d_j$, то хомогенните компоненти

$$f^{[d]} = \sum_{j=1}^{s} g_j^{[d-d_j]} f_j$$

принадлежат на I.
Обратно, нека $I = \langle g_1, \dots, g_l \rangle$ се поражда от полиномите $g_1, \dots, g_l \in F[x_1, \dots, x_n]$. По предположение, всички хомогенни компоненти $g_i^{[j]}$ на $g_i = \sum\limits_{j=0}^{d_i} g_i^{[j]}$ принадлежат на I, така че идеалът

$$J = \langle g_i^{[j]} \ \mid \ 0 \leq j \leq d_i, \ \ 1 \leq i \leq l \rangle$$

се съдържа в идеала I. От друга страна, $I \subseteq J$, защото за произволни полиноми $h_1, \dots, h_l \in k[x_1, \dots, x_n]$ е в сила $\sum\limits_{i=1}^{l} g_i h_i = \sum\limits_{i=1}^{l} \sum\limits_{j=0}^{d_i} g_i^{[j]} h_i \in J$. Следователно $I = J$ се поражда от хомогенните полиноми $g_i^{[j]}$ и I е хомогенен идеал, Q.E.D.

Лема 6.18. *Ако I е хомогенен идеал в $k[x_0, \dots, x_n]$, то идеалът I е прост тогава и само тогава, когато за произволни хомогенни полиноми*

$$f(x_0, \dots, x_n), g(x_0, \dots, x_n) \in k[x_0, \dots, x_n]$$

с $f(x_0, \dots, x_n) g(x_0, \dots, x_n) \in I$ е в сила $f(x_0, \dots, x_n) \in I$ или $g(x_0, \dots, x_n) \in I$.

Доказателство: Необходимостта на условието следва от определението за прост идеал. Да допуснем, че за произволни хомогенни полиноми $f(x_0, \dots, x_n)$, $g(x_0, \dots, x_n) \in k[x_0, \dots, x_n]$ с $fg \in I$ следва $f \in I$ или $g \in I$, но идеалът I не е прост. Тогава съществуват полиноми $F, G \in k[x_0, \dots, x_n]$ с $FG \in I$, $F \notin I$, $G \notin I$. Ако

$$F = \sum_{i=0}^{m} F^{[i]} \quad \text{и} \quad G = \sum_{j=0}^{n} G^{[j]}$$

са разлаганията на F и G в сума от хомогенни компоненти, без ограничение на общността можем да предполагаме, че $F^{[m]} \notin I$, $G^{[n]} \notin I$. В противен случай, $F_1 := F - F^{[m]}$ има произведение $F_1 G = FG - F^{[m]} G \in I$ и можем да разглеждаме F_1 и G вместо F и G. Хомогенната компонента от максимална степен

$$(FG)^{[m+n]} = \left[\left(\sum_{i=0}^{m} F^{[i]} \right) \left(\sum_{j=0}^{n} G^{[j]} \right) \right]^{[m+n]} = F^{[m]} G^{[n]} \in I$$

принадлежни на I, защото $FG \in I$ и I е хомогенен идеал. По предположение, от $F^{[m]}G^{[n]} \in I$ следва $F^{[m]} \in I$ или $G^{[n]} \in I$. Противоречието доказва твърдението, Q.E.D.

Сега ще разгледаме някои свойства на проективните алгебрични множества и операциите с тях.

Лема 6.19. *(i) Ако $S \subseteq \overline{k}[x_0, \ldots, x_n]_h$ е множество от хомогенни полиноми, то проективното алгебрично множество $Z(S) = Z(\langle S\rangle_h)$, определено от S съвпада с проективното алгебрично множество, определено от хомогенните полиноми на идеала $\langle S\rangle$, породен от S.*

(ii) Ако $S \subseteq T \subseteq \overline{k}[x_0, \ldots, x_n]_h$ са множества от хомогенни полиноми, то съответните им проективни алгебрични множества $Z(S) \supseteq Z(T)$ изпълняват обратното включване.

(iii) Ако $M \subseteq N \subseteq \mathbb{P}^n(\overline{k})$ са подмножества на проективното пространство $\mathbb{P}^n(\overline{k})$, то хомогенните им идеали $I_h(N) \subseteq I_h(M) \lhd \overline{k}[x_0, \ldots, x_n]$ изпълняват противоположното включване.

(iv) Ако $S_\alpha \subseteq \overline{k}[x_0, \ldots, x_n]_h$, $\alpha \in A$ са множества от хомогенни полиноми, то

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

Доказателство: Свойствата (ii) и (iii) са ясни.

(i) От $S \subseteq \langle S\rangle_h$ следва $Z(\langle S\rangle_h) \subseteq Z(S)$. За обратното включване $Z(S) \subseteq Z(\langle S\rangle_h)$ избираме точка $a \in Z(S)$ и хомогенен полином $f = \sum_{i=1}^{l} f_i g_i \in \langle S\rangle_h$, който се представя чрез краен брой хомогенни полиноми $f_i \in S$ и някакви полиноми $g_i \in \overline{k}[x_0, \ldots, x_n]$. Сега $f(a) = \sum_{i=1}^{l} f_i(a) g_i(a) = 0.g_1(a) + \ldots + 0.g_l(a) = 0$ показва, че $a \in Z(\langle S\rangle_h)$ и $Z(S) = Z(\langle S\rangle_h)$.

(iv) От включванията $S_\alpha \subseteq \cup_{\alpha \in A} S_\alpha \subseteq \overline{k}[x_0, \ldots, x_n]_h$ за $\forall \alpha \in A$ получаваме обратните включвания $Z(S_\alpha) \supseteq Z(\cup_{\alpha \in A} S_\alpha)$, откъдето $\cap_{\alpha \in A} Z(S_\alpha) \supseteq Z(\cup_{\alpha \in A} S_\alpha)$. За да проверим $\cap_{\alpha \in A} Z(S_\alpha) \subseteq Z(\cup_{\alpha \in A} S_\alpha)$ избираме точка $a \in \cap_{\alpha \in A} Z(S_\alpha)$ и полином $f \in \cup_{\alpha \in A} S_\alpha$. Ако $f \in S_{\alpha_0}$, то $f(a) = 0$ съгласно $a \in Z(S_{\alpha_0})$ и $a \in Z(\cup_{\alpha \in A} S_\alpha)$. Това доказва $\cap_{\alpha \in A} Z(S_\alpha) \subseteq Z(\cup_{\alpha \in A} S_\alpha)$ и

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

Q.E.D.

Твърдение 6.20. *(i) Ако $I_1, \ldots, I_m$ са хомогенни идеали в $\overline{k}[x_0, \ldots, x_n]$, то*

$$Z((I_1 \ldots I_m)_h) = Z((I_1)_h) \cup \ldots \cup Z((I_m)_h).$$

(ii) Ако $S_1, \ldots, S_m \subseteq \overline{k}[x_0, \ldots, x_n]_h$ са множества от хомогенни полиноми, то произведението им

$$S_1 \ldots S_m = \{f_1 \ldots f_m \mid f_j \in S_j, \quad 1 \leq j \leq m\} \subseteq \overline{k}[x_0, \ldots, x_n]_h$$

се състои от хомогенни полиноми и

$$Z(S_1 \ldots S_m) = Z(S_1) \cup \ldots \cup Z(S_m).$$

Доказателство: (i) От включването на идеали $I_1 \ldots I_m \subseteq I_j$ следва включването $(I_1 \ldots I_m)_h \subseteq (I_j)_h$ на хомогенните им елементи и обратното включване $Z((I_j)_h) \subseteq Z((I_1 \ldots I_m)_h)$ на съответните проективни алгебрични множества за $\forall 1 \leq j \leq m$. Следователно $Z((I_1)_h) \cup \ldots \cup Z((I_m)_h) \subseteq ((I_1 \ldots I_m)_h)$. Да допуснем, че обратното включване не е изпълнено. Тогава съществува точка $a \in Z((I_1 \ldots I_m)_h) \setminus (\cup_{j=1}^m Z((I_j)_h))$. Съгласно $a \notin Z((I_j)_h)$ за $\forall 1 \leq j \leq m$ съществуват хомогенни полиноми $f_j \in (I_j)_h$ с $f_j(a) \neq 0$. Но тогава $f_1 \ldots f_m \in (I_1 \ldots I_m)_h$ е хомогенен полином от $I_1 \ldots I_m$ с $(f_1 \ldots f_m)(a) = f_1(a) \ldots f_m(a) \neq 0$, защото в полето $\overline{k}$ няма делители на нулата. Това противоречи на $a \in Z((I_1 \dots I_m)_h)$ и доказва $Z((I_1 \dots I_m)_h) \subseteq Z((I_1)_h) \cup \dots \cup Z((I_m)_h)$, а оттам и

$$Z((I_1 \dots I_m)_h) = Z((I_1)_h) \cup \dots \cup Z((I_m)_h),$$

Q.E.D.

3. Топология на Зариски върху проективно алгебрично множество

Множеството $\mathcal{Z} = \{Z(S)\}_{S \subseteq \overline{k}[x_0,\dots,x_n]_h}$ е фамилия от затворени подмножества на $\mathbb{P}^n(\overline{k})$, защото $\emptyset = Z(\overline{k}[x_0,\dots,x_n]) \in \mathcal{Z}$, $\mathbb{P}^n(\overline{k}) = Z(0) \in \mathcal{Z}$, $\cap_{\alpha\in A} Z(S_\alpha) = Z(\cup_{\alpha\in A} S_\alpha) \in \mathcal{Z}$ за $S_\alpha \subseteq \overline{k}[x_0,\dots,x_n]_h$, $\alpha \in A$ и $Z(S_1) \cup \dots \cup Z(S_m) = Z(S_1 \dots S_m) \in \mathcal{Z}$ за $S_j \subseteq \overline{k}[x_0,\dots,x_n]_h$, $1 \leq j \leq m$.

Определение 6.21. *Топологията върху $\mathbb{P}^n(\overline{k})$ със затворени подмножества $\mathcal{Z} = \{Z(S)\}_{S \subseteq \overline{k}[x_0,\dots,x_n]_h}$ се нарича топология на Зариски върху $\mathbb{P}^n(\overline{k})$.*

За произволно множество $S_o \subseteq \overline{k}[x_0,\dots,x_n]_h$ от хомогенни полиноми, топологията върху $Z(S_o)$, индуцирана от топологията на Зариски върху $\mathbb{P}^n(\overline{k})$ се нарича топология на Зариски върху $Z(S_o)$. Затворените подмножества на топологията на Зариски върху проективно алгебрично множество $Z(S_o)$ са

$$\{Z(S) \cap Z(S_o)\}_{S \subseteq \overline{k}[x_0,\dots,x_n]_h} = \{Z(S \cup S_o)\}_{S \subseteq \overline{k}[x_0,\dots,x_n]_h} = \{Z(T)\}_{S_o \subseteq T \subseteq \overline{k}[x_0,\dots,x_n]_h}.$$

Определение 6.22. *Проективната обвивка $\overline{W}$ на подмножество $W \subset \mathbb{P}^n(\overline{k})$ е сечението $\overline{W} = \cap_{F \supseteq W} F$ на всички Зариски затворени подмножества $F \subseteq \mathbb{P}^n(\overline{k})$, съдържащи W.*

Лема 6.23. *Проективната обвивка $\overline{M}$ на подмножество $M \subseteq \mathbb{P}^n(\overline{k})$ е равна на*

$$\overline{M} = Z(I_h(M)_h).$$

В частност, ако M е проективно алгебрични множество, то $M = V_{\mathbb{P}^n}(I_h(M)_h)$.

Доказателство: По определение, $\overline{M} = \cap_{M \subseteq Z} Z$ е сечението на Зариски затворените подмножества $Z \subset \mathbb{P}^n(\overline{k})$, съдържащи M. Да забележим, че

$$M \subseteq Z(I_h(M)_h),$$

защото всеки хомогенен елемент f на $I_h(M)$ е хомогенен полином, анулиращ се във всички точки на M. В качеството си на Зариски затворено подмножество на $\mathbb{P}^n(\overline{k})$, съдържащо M, $Z(I_h(M)_h)$ участва в сечението $\cap_{M \subseteq Z} Z = \overline{M}$ и го съдържа.
За обратното вкрючване $Z(I_h(M)_h) \subseteq \overline{M}$ е достатъчно да проверим, че

$$Z(I_h(M)_h) \subseteq Z$$

за всяко Зариски затворено подмножество $M \subseteq Z = Z(S_o) \subseteq \mathbb{P}^n(\overline{k})$, зададено с множество S_o от хомогенни полиноми. Наистина, от $M \subseteq Z(S_o) = Z$ следва $I_h(M) \supseteq I_h(Z(S_o)) \supseteq S_o$, а оттам и $I_h(M)_h \supseteq I_h(Z(S_o))_h \supseteq S_o$. Това е достатъчно за $Z(I_h(M)_h) \subseteq Z(S_o) = Z$ и доказва $Z(I_h(M)_h) \subseteq_{Z \supseteq M} Z = \overline{M}$, Q.E.D.

Задача 6.24. *Нека*

$$\left| \begin{array}{llllll} f_1(x_0,\dots,x_n) & = a_{1,0}x_0 & +a_{1,1}x_1 & +\dots & +a_{1,n}x_n & = 0 \\ \dots & \dots & \dots & \dots & \dots & \\ f_m(x_0,\dots,x_n) & = a_{m,0}x_0 & a_{m,1}x_1 & +\dots & +a_{m,n}x_n & = 0 \end{array} \right.$$

е хомогенна система линейни уравнения с коефициенти $a_{i,j} \in k$, $b_0, \dots b_{n-r} \in k^{n+1}$ е фундаментална система решения, а $X \subseteq \mathbb{P}^n(k)$ е проективно алгебрично множество . Да се докаже, че

$$\varphi : Z(f_1,\dots,f_m) = \Pi(l_k(b_0,\dots b_{n-r}) \setminus \{(0,\dots 0)\} \longrightarrow \mathbb{P}^{n-r}(k),$$

$$\varphi\Pi\left(\sum_{i=0}^{n-r} y_i b_i\right) = [y_0 : \ldots : y_{n-r}]$$

е взаимно еднозначно изображение, което изобразява $X \cap Z(f_1, \ldots, f_m)$ в проективно алгебрично подмножество на $\mathbb{P}^{n-r}(k)$.

Упътване: Използвайте компонентите на векторите $b_0, \ldots, b_{n-r} \in k^{n+1}$, за да изразите хомогенните координати $x_0, \ldots, x_n$ на точките

$$x = [x_0 : \ldots : x_n] \in Z(f_1, \ldots, f_m)$$

чрез координатите $y_0, \ldots, y_{n-r}$ на $\Pi^{-1}(x) \in k^{n+1}$ спрямо $b_0, \ldots, b_{n-r}$.
По определение, за $\forall [x_0 : \ldots : x_n] \in \mathbb{P}^n(k)$ съществува $0 \leq i \leq n$, така че $x_i \neq 0$. Ако $U_i = \{x \in \mathbb{P}^n(k) \ \mid \ x_i \neq 0\}$, то $\mathbb{P}^n(k)$ се разлага в обединение

$$\mathbb{P}^n(k) = U_0 \cup \ldots \cup U_n.$$

Допълненията

$$H_i = \mathbb{P}^n(k) \setminus U_i = \{x \in \mathbb{P}^n(k) \ \mid \ x_i = 0\} \simeq \mathbb{P}^{n-1}(k)$$

са проективни хиперравнини, така че U_i са Зариски отворени подмножества на $\mathbb{P}^n(k)$.
Следващото твърдение установява, че отворените подмножества $U_i \subset \mathbb{P}^n(k)$ са изоморфни на n-мерното афинно пространство k^n по такъв начин, че топологията на Зариски върху U_i, наследена от $\mathbb{P}^n(k)$ съвпада с топологията на Зариски върху k^n.

Твърдение 6.25. *За $\forall 0 \leq i \leq n$ изображението*

$$\varphi_i : U_i = \{x \in \mathbb{P}^n(\overline{k}) \ \mid \ x_i \neq 0\} \longrightarrow \overline{k}^n,$$

$$\varphi_i([x_0 : \ldots : x_{i-1} : x_i : x_{i+1} : \ldots : x_n]) = \left(\frac{x_0}{x_i}, \ldots, \frac{x_{i-1}}{x_i}, \frac{x_{i+1}}{x_i}, \ldots, \frac{x_n}{x_i}\right)$$

е хомеоморфизъм относно топологията върху U_i, индуцирана от топологията на Зариски върху $\mathbb{P}^n(\overline{k})$ и топологията на Зариски върху $\overline{k}^{n+1}$.
Изображението φ_i се нарича афинен координатен хомеоморфизъм на U_i.

Доказателство: Вече споменахме, че изображението φ_i е взаимно еднозначно. Остава да проверим, че $\varphi_i : U_i \to \overline{k}^n$ и $\varphi_i^{-1} : \overline{k}^n \to U_i$ са непрекъснати изображения относно съответните топологии на Зариски. По определение, изображение $f : X \to Y$ на топологични пространства е непрекъснато, ако всяка отвореноо подмножсето $U \subseteq Y$ се издърпва до отворено подмножество $f^{-1}(U)$. Твърдим, че $f^{-1}(Y \setminus U) = X \setminus f^{-1}(U)$. Наистина, ако $a \in f^{-1}(Y \setminus U)$, то $a \in X$ и $f(a) \in Y \setminus U$, откъдего $f(a) \notin U$ и $a \notin f^{-1}(U)$. Обратно, ако $a \in X \setminus f^{-1}(U)$, то $f(a) \notin U$, откъдето $f(a) \in Y \setminus U$ и $a \in f^{-1}(Y \setminus U)$. Следователно изображението $f : X \to Y$ издърпва отворените подмножества $U \subseteq Y$ в отворени подмножества $f^{-1}(U)$ точно когато f издърпва затворените подмножества $Y \setminus U \subseteq Y$ в затворени подмножества $f^{-1}(Y \setminus U) = X \setminus f^{-1}(U) \subseteq X$. Затова е достатъчно да проверим, че за произволно подмножество $T \subseteq \overline{k}\left[\frac{x_0}{x_i}, \ldots, \frac{x_{i-1}}{x_i}, \frac{x_{i+1}}{x_i}, \ldots, \frac{x_n}{x_i}\right]$, афинното алгебрично множество $Z(T) \subseteq \overline{k}^n$ се издърпва в Зариски затворено подмножество $\varphi_i^{-1} Z(T) \subseteq U_i$ и за произволно подмножество $S \subseteq \overline{k}[x_0, \ldots, x_n]_h$ с непразно сечение $Z(S) \cap U_i \neq \emptyset$ на проективното алгебрично множество $Z(S) \subseteq \mathbb{P}^n(\overline{k})$ със стандартното афинно алгебрично множество $U_i \subset \mathbb{P}^n(\overline{k})$, праобразът $(\varphi_i^{-1})^{-1}(Z(S) \cap U_i) = \varphi_i(Z(S) \cap U_i) \subseteq \overline{k}^n$ е Зариски затворен в $\overline{k}^n$.

За целта въвеждаме i-тата дехомогенизация $f_{[i]}$ на хомогенен полином $f \in \overline{k}[x_0, \ldots, x_n]_h$ от степен d като

$$f_{[i]}\left(\frac{x_0}{x_i}, \ldots, \frac{x_{i-1}}{x_i}, \frac{x_{i+1}}{x_i}, \ldots, \frac{x_n}{x_i}\right) := x_i^{-d} f(x_0, \ldots, x_n)$$

и забелязваме, че $f_{[i]}$ е полином на $\frac{x_0}{x_i}, \ldots, \frac{x_{i-1}}{x_i}, \frac{x_{i+1}}{x_i}, \ldots, \frac{x_n}{x_i}$ от обща степен $\leq d$. Обратно, за произволен полином $g \in \overline{k}\left[\frac{x_0}{x_i}, \ldots, \frac{x_{i-1}}{x_i}, \frac{x_{i+1}}{x_i}, \ldots, \frac{x_n}{x_i}\right]$ от обща степен d определяме i-тата хомогенизация като

$$g^{[i]}(x_0, \ldots, x_n) := x_i^d g\left(\frac{x_0}{x_i}, \ldots, \frac{x_{i-1}}{x_i}, \frac{x_{i+1}}{x_i}, \ldots, \frac{x_n}{x_i}\right)$$

и забелязваме, че $g^{[i]}$ е хомогенен полином на $x_0, \ldots, x_n$ от степен d. Произволен хомогенен полином $f \in \overline{k}[x_0, \ldots, x_n]$ се анулира в точка $a \in U_i$ тогава и само тогава, когато i-тата му дехомогенизация $f_{[i]}$ се анулира в $a_{[i]}$, съгласно $f_{[i]}(a_{[i]}) = a_i^{-\deg(f)} f(a_0, \ldots, a_n)$. За произволно крайно множество $S \subset \overline{k}[x_0, \ldots, x_n]_h$ от хомогенни полиноми означаваме с $S_{[i]}$ множеството на i-тите дехомогенизации на елементите на S получаваме,че $\varphi_i(Z(S) \cap U_i) = Z(S_{[i]})$. Обратно, полином $g \in \overline{k}\left[\frac{x_0}{x_i}, \ldots, \frac{x_{i-1}}{x_i}, \frac{x_{i+1}}{x_i}, \ldots, \frac{x_n}{x_i}\right]$ се анулира в $a_{[i]}$ точно когато i-тата му хомогенизация се анулира в a, защото $g^{[i]}(a) = a_i^{\deg(g)} g(a_{[i]})$. Ако $T \subset \overline{k}\left[\frac{x_0}{x_i}, \ldots, \frac{x_{i-1}}{x_i}, \frac{x_{i+1}}{x_i}, \ldots, \frac{x_n}{x_i}\right]$ е крайно множество от полиноми и $T^{[i]}$ е множеството на i-тите хомогенизации на елементите на T, то $\varphi_i^{-1} Z(T) = Z(T^{[i]}) \cap U_i$, Q.E.D.

Задача 6.26. *Нека*

$$\varphi_0 : U_0 = \{x \in \mathbb{P}^2(k) \mid x_0 \neq 0\} \longrightarrow k^2,$$

$$\varphi_0([x_0 : x_1 : x_2]) = \left(\frac{x_1}{x_0}, \frac{x_2}{x_0}\right)$$

е афинният координатен хомеоморфизъм на U_0, *а*

$$C = \left\{(y_1, y_2) \in k^2 \;\middle|\; y_2^2 = \sum_{i=0}^{2m+1} a_i y_1^i\right\}$$

е афинна крива, $a_i \in k$, $a_{2m+1} \neq 0$, $m \in \mathbb{N}$. *Да се докаже, че Зариски затворената обвивка* $\overline{\varphi_0^{-1}(C)}$ *на* $\varphi_0^{-1}(C) \subset U_0$ *в* $\mathbb{P}^2(k)$ *се получава от* $\varphi_0^{-1}(C)$ *чрез присъединяване на единствена точка* $\infty \in \mathbb{P}^2(k)$ *и да се намери точката* ∞.

Задача 6.27. *Нека*

$$\varphi_0 : U_0 = \{x \in \mathbb{P}^3(k) \mid x_0 \neq 0\} \longrightarrow k^3,$$

$$\varphi_0([x_0 : x_1 : x_2 : x_3]) = \left(\frac{x_1}{x_0}, \frac{x_2}{x_0}, \frac{x_3}{x_0}\right)$$

е афинният координатен хомеоморфизъм на U_0, *а*

$$X = \{(y_1, y_2, y_3) \in k^3 \mid y_1^3 y_2 - y_1 y_2^3 - y_1^3 - 2y_1 y_2 = 0\}$$

е афинна повърхнина. Да се докаже, че Зариски затворената обвивка

$$\overline{\varphi_0^{-1}(X)} = \varphi_0^{-1}(X) \cup H_1 \ldots \cup H_4$$

на $\varphi_0^{-1}(X) \subset U_0$ *в* $\mathbb{P}^3(k)$ *се получава от* $\varphi_0^{-1}(X)$ *чрез присъединяване на четири проективни хиперравнини* $H_i \simeq \mathbb{P}^2(k)$ *и да се намерят уравнения на* $H_1, \ldots, H_4$.

ПРИМЕР 6.28. *Зариски затворените подмножества на проективната права $\mathbb{P}^1(\overline{k})$ са $\emptyset$, $\mathbb{P}^1(\overline{k})$ и крайните подмножества*

Наистина, ако $Z \subseteq \mathbb{P}^n(\overline{k})$ е Зариски затворено подмножсетво, то

$$Z = (Z \cap U_0) \cup (Z \setminus U_0)$$

с $Z \setminus U_0 \subseteq \mathbb{P}^1(\overline{k}) \setminus U_0 = \{[0:1]\}$. Сечението $Z \cap U_0$ се изобразява в Зариски затворено подмножество $\varphi_0(Z \cap U_0) \subseteq \overline{k}$, така че $\varphi_0(Z \cap U_0) = \emptyset, \overline{k}$ или $\varphi_0(Z \cap U_0)$ е крайно множество. В резултат, $Z = \emptyset, U_0, \mathbb{P}^1(\overline{k}$ или Z е крайно множество. Трябва да докажем, че $Z \neq U_0$. В противен случай, прилагаме горните разглеждания към $Z = (Z \cap U_1) \cup (Z \setminus U_1)$ с единствен проблем при $Z = U_1$. Но допускането $U_0 = Z = U_1$ води до противоречие поради $U_0 \neq U_1$ и доказва, че Зариски затворените подмножества на $\mathbb{P}^1(\overline{k})$ са $\emptyset, \mathbb{P}^1(\overline{k})$ и крайните множества.

4. Едновременна неприводимост на афинно алгебрично множество и проективната му обвивка

ОПРЕДЕЛЕНИЕ 6.29. *Проективните алгебрични множества, които са неприводими относно топологията на Зариски се наричат проективни алгебрични многообразия.*

ТВЪРДЕНИЕ 6.30. *Проективното алгебрично множество $Z = Z(S) \subseteq \mathbb{P}^n(\overline{k})$ с $S \subseteq \overline{k}[x_0, \dots, x_n]_h$ е проективно многообразие тогава и само тогава, когато хомогенният идеал $I_h(Z) \triangleleft \overline{k}[x_0, \dots, x_n]$ е прост.*

Доказателство: Да допуснем, че $Z = Z(S) \subseteq \mathbb{P}^n(\overline{k})$ е неприводимо проективно алгебрично множество, чийто хомогенен идеал $I_h(Z) \triangleleft \overline{k}[x_0, \dots, x_n]$ не е прост. Съгласно Лема 6.18, съществуват хомогенни полиноми $f(x_0, \dots, x_n)$ и $g(x_0, \dots, x_n)$ от $k[x_0, \dots, x_n]_h \setminus I_h(X)$ с $fg \in I_h(Z)_h$. Твърдим, че

$$Z_1 := Z(f) \not\supseteq Z(I_h(Z)_h) = Z, \quad Z_2 := Z(g) \not\supseteq Z(I_h(Z)_h) = Z,$$

защото предположението $Z_1 \supseteq Z$ води до $f|_Z = 0$, откъдето $f \in I_h(X)$, противно на избора на $f \notin I_h(X)$. От друга страна, $Z(fg) \supseteq Z(I_h(Z)_h) = Z$, така че

$$Z = Z(fg) \cap Z = (Z(f) \cup Z(g)) \cap Z = (Z_1 \cap Z) \cup (Z_2 \cap Z).$$

Подмножествата $Z_1 \cap Z$ и $Z_2 \cap Z$ на Z са затворени и различни от Z съгласно $Z \not\subseteq Z_1$, $Z \not\subseteq Z_2$. Това противоречи на неприводимостта на Z и доказва простотата на хомогенния идеал на неприводимо проективно алгебрично множество.
Обратно, нека $Z \subseteq \mathbb{P}^n(\overline{k})$ е проективно алгебрично множество с прост хомогенен идеал $I_h(Z) \triangleleft \overline{k}[x_0, \dots, x_n]$ и $Z = Z_1 \cup Z_2$ за Зариски затворени $Z_i \subsetneq Z$. Тогава

$$I_h(Z) = I_h(Z_1 \cup Z_2) = I_h(Z_1) \cap I_h(Z_2)$$

и $I_h(Z_i) \supsetneq I_h(Z)$ за $1 \leq i \leq 2$. По-точно, от $Z_i \subseteq Z$ следва $I_h(Z_i) \supseteq I_h(Z)$ и предположението $I_h(Z_i) = I_h(Z)$ води до $Z_i = Z(I_h(Z_i)_h) = Z(I_h(Z)_h) = Z$, което противоречи на допускането за приводимост на Z. От $I_h(Z_i) \supsetneq I_h(Z)$ следва $I_h(Z_i)_h \supsetneq I_h(Z)_h$. По-точно, включването $I_h(Z_i)_h \supseteq I_h(Z)_h$ е ясно. Допускането $I_h(Z_i)_h = I_h(Z)_h$ води до съвпадение $I_h(Z_i) = I_h(Z)$, защото хомогенните идеали $I_h(Z_i)$ и $I_h(Z)$ се пораждат от хомогенните си елементи. Избираме хомогенни полиноми $f_i \in I_h(Z_i)_h \setminus I_h(Z)_h$ и забелязваме, че $f_1 f_2 \in I_h(Z_i)_h \cap I_h(Z_2)_h = I_h(Z)_h$. Това противоречи на простотата на идеала $I_h(Z)$ и доказва неприводимостта на проективните алгебрични множества Z с прост хомогенен идеал $I_h(Z)$, Q.E.D.

ЛЕМА 6.31. *Нека Z е неприводимо затворено подмножество на топологично пространство X, а $U \subseteq X$ е отворено подмножество с непразно сечение $Z \cap U \neq \emptyset$. Тогава $Z \cap U$ е отворено, навсякъде гъсто в Z и неприводимо подмножество на X.*

Доказателство: Подмножеството $Z \cap U \subseteq Z$ е отворено съгласно определението на индуцираната от X топология върху Z.
За произволни подмножества $A, B \subseteq X$ на топологичното пространство X твърдим, че $\overline{A \cup B} = \overline{A} \cup \overline{B}$. От една страна,

$$\overline{A} \cup \overline{B} = (\cap_{Z_1 \supseteq A} Z_1) \cup (\cap_{Z_2 \supseteq B} Z_2) = \cap_{Z_1 \supseteq A} \cap_{Z_2 \supseteq B} \ (Z_1 \cup Z_2)$$

се съдържа в $\overline{A \cup B} = \cap_{Z \supseteq A \cup B} Z$, защото всяко затворено подмножество $Z \subseteq X$ с $Z \supseteq A \cup B$ може да се представи като $Z = Z \cup Z$ с $Z \supseteq A$, $Z \supseteq B$ и участва в сечението $\cap_{Z_1 \supseteq A} \cap_{Z_2 \supseteq B} \ (Z_1 \cup Z_2) = \overline{A \cup B}$. Обратно, произволни затворени $Z_1, Z_2 \subseteq X$ с $Z_1 \supseteq A$, $Z_2 \supseteq B$ имат затворено обединение $Z_1 \cup Z_2 \supseteq A \cup B$, така че $Z_1 \cup Z_2$ участва в сечението $\cap_{Z \subseteq A \cup B} Z = \overline{A \cup B}$ и $\overline{A \cup B} \subseteq \overline{A} \cup \overline{B}$. Това доказва $\overline{A \cup B} = \overline{A} \cup \overline{B}$.
За гъстотата на $Z \cap U$ в Z разглеждаме разлагането

$$Z = (Z \cap U) \cup (Z \setminus U).$$

Затворената обвивка

$$Z = \overline{Z} = \overline{(Z \cap U) \cup (Z \setminus U)} = \overline{(Z \cap U)} \cup \overline{(Z \setminus U)} = \overline{(Z \cap U)} \cup (Z \setminus U),$$

съгласно затовреността на Z и $Z \setminus U$. Неприводимостта на Z изисква $Z = \overline{Z \cap U}$, защото допускането $Z = Z \setminus U$ противоречи на $Z \cap U \neq \emptyset$. Това доказва, че $Z \cap U$ е навсякъде гъсто в Z.
За неприводимостта на $Z \cap U$ да допуснем, че $Z \cap U = V_1 \cup V_2$ за някакви затворени подмножества $V_j \subseteq Z \cap U$. По определение,

$$V_j = Z'_j \cap (Z \cap U) = (Z'_j \cap Z) \cap U = Z_j \cap U$$

за някакви затворени $Z'_j \subseteq X$ и $Z_j := Z'_j \cap Z \subseteq X$. Затворената обвивка

$$Z = \overline{Z \cap U} = \overline{(Z_1 \cap U) \cup (Z_2 \cap U)} = \overline{(Z_1 \cap U)} \cup \overline{(Z_2 \cap U)} = Z_1 \cup Z_2,$$

съгласно гъстотата на $Z \cap U$ в Z и на $Z_j \cap U$ в Z_j (при $Z_j \cap U \neq \emptyset$). Неприводимостта на Z изисква $Z = Z_1$ или $Z = Z_2$, откъдето $Z \cap U = Z_1 \cap U$ или $Z \cap U = Z_2 \cap U$ и $Z \cap U$ е неприводимо подмножество на X, Q.E.D.

ТВЪРДЕНИЕ 6.32. *(i) Ако $W \subseteq \overline{k}^n \simeq U_i \subset \mathbb{P}^n(\overline{k})$ е афинно многообразие, то проективната обвивка $\overline{W} \subseteq \mathbb{P}^n(\overline{k})$ е проективно многообразие.*
(ii) Ако афинното многообразие W/k е определено над полето k, то проективната обвивка $\overline{W}/k$ е определена над k.
(iii) Ако $V \subseteq \mathbb{P}^n(\overline{k})$ е проективно алгебрично многообразие,

$$U_i = \{x = [x_0 : \ldots : x_n] \in \mathbb{P}^n(\overline{k}) \quad | \quad x_i \neq 0\}$$

е стандартно афинно отворено подмножество на $\mathbb{P}^n(\overline{k})$ и сечението $V \cap U_i \neq \emptyset$ не е празно, то $V \cap U_i \subseteq U_i \simeq \overline{k}^n$ е афинно алгебрично многообразие.
(iv) Ако V/k е проективно алгебрично многообразие, определено над k и пресичащо стандартното афинно отворено подмножество U_i на $\mathbb{P}^n(\overline{k})$, то $V \cap U_i \subseteq U_i \simeq \overline{k}^n$ е афинно алгебрично многообразие, определено над k.

Доказателство: (i) Нека $\overline{W} = Z_1 \cup Z_2$ е разлагане на проективната обвивка $\overline{W} \subseteq \mathbb{P}^n(\overline{k})$ в обединение на затворени подмножества $Z_j \subseteq \overline{W}$. Тогава сечението

$$W = \overline{W} \cap U_i = (Z_1 \cup Z_2) \cap U_i = (Z_1 \cap U_i) \cup (Z_2 \cap U_i)$$

се представя като обединение на Зариски затворени $Z_j \cap U_i \subseteq U_i$, $1 \leq j \leq 2$. Неприводимото афинно алгебрично множество W съвпада с някое от Зариски затворените подмножества $Z_j \cap U_i \subseteq U_i$. Оттук, проективната обвивка

$$\overline{W} = \overline{Z_j \cap U_i} = Z_j,$$

съгласно гъстотата на $Z_j \cap U_i$ в Z_j. Това доказва неприводимостта на $\overline{W}$.
(ii) Ако $W = Z(T) \subseteq \overline{k}^n \simeq U_i$ е непирводимо алгебрично множество, определено от полиноми $T \subseteq k\left[\frac{x_0}{x_i}, \ldots, \frac{x_{i-1}}{x_i}, \frac{x_{i+1}}{x_i}, \ldots, \frac{x_n}{x_i}\right]$, то проективната обвивка $\overline{W} = Z(T^{[i]})$ се определя от множеството $T^{[i]} \subseteq k[x_0, \ldots, x_n]_h$ на i-тите хомогенизации на полиномите от T и $\overline{W}$ е неприводимо проективно алгебрично множество, определено над k.
(iii) Ако $V \subseteq \mathbb{P}^n(\overline{k})$ е неприводимо проективно алгебрично множество с $V \cap U_i \neq \emptyset$ за някое стандартно афинно отворено подмножсетво $U_i \subset \mathbb{P}^n(\overline{k})$, то $V \cap U_i$ е неприводимо съгласно Лема 6.31. По определението за индуцирана топология, $V \cap U_i$ е затворено подмножество на $U_i \simeq \overline{k}^n$.
(iv) Ако $V = Z(S)$ с $S \subseteq k[x_0, \ldots, x_n]_h$ е неприводимо проективно алгебрично монжество, определено над k и $V \cap U_i \neq \emptyset$, то $V \cap U_i = Z(S_{[i]}) \subseteq \overline{k}^n \simeq U_i$ е неприводимо афинно алгебрично множество, определено от множеството $S_{[i]} \subseteq k\left[\frac{x_0}{x_i}, \ldots, \frac{x_{i-1}}{x_i}, \frac{x_{i+1}}{x_i}, \ldots, \frac{x_n}{x_0}\right]$ на i-тите дехомогенизации на полиномите от S. В частност, $V \cap U_i$ е определено над k, Q.E.D.

Задача 6.33. *Да се намери проективната обвивка $\overline{W}$ на афинното многообразие*

$$W = \{(x, y) \in \overline{\mathbb{F}_5}^2 \mid y^2 = x^3 + x\} \subset \overline{\mathbb{F}_5}^2.$$

Всеки неразложим хомогенен полином $f \in k[x_0, \ldots, x_n]$ поражда прост идеал $\langle f \rangle \triangleleft k[x_0, \ldots, x_n]$. Следващият пример илюстрира съществуването на неразложими хомогенни полиноми $f, g \in k[x_0, \ldots, x_n]$, за които идеалът $\langle f, g \rangle$ не е прост.
От простотата на нулевия хомогенен идеал в областта $\overline{k}[x_0, \ldots, x_n]$ следва неприводимостта на проективното пространство $\mathbb{P}^n(\overline{k})$.

Задача 6.34. *Да се докаже, че проективните алгебрични множества*

$$X = \left\{ [x_0 : x_1 : x_2] \in \mathbb{P}^2(\mathbb{C}) \;\middle|\; x_2^2 x_0^{2n-1} + \sum_{i=0}^{2n+1} a_i x_1^i x_0^{2n+1-i} = 0 \right\}$$

и

$$X = \left\{ [x_0 : x_1 : x_2] \in \mathbb{P}^2(\mathbb{C}) \;\middle|\; x_2^3 x_0^{3n-2} + \sum_{i=0}^{3n+1} a_i x_1^i x_0^{3n+1-i} = 0 \right\}$$

са неприводими.

5. Разлагане на алгебрично множество в крайно обединение на неприводими компоненти

Твърдение-Определение 6.35. *Произволно афинно или проективно алгебрично множество X се представя като крайно обединение*

$$X = X_1 \cup \ldots \cup X_m$$

на краен брой афинни или проективни многообразия $X_i \subseteq X$, които се наричат неприводими компоненти на X.

Доказателство: Да допуснем противното и да изберем алгебрично множество X, което не може да се представи като крайно обединение на неприводими афинни алгебрични подмножества. Тогава X не е неприводимо, така че може да се представи като обединение $X = X_1 \cup X_1'$ на собствени алгебрични подмножества $X_1 \subsetneq X$ и $X_1' \subsetneq X$. Поне едното от X_1 или X_1' не е крайно обединение от неприводими алгебрични подмножества, защото в противен случай X ще се окаже крайно обединение от неприводими алгебрични множества. За определеност да предположим, че X_1 не е крайно обединение на неприводими алгебрични множества. Повтаряйки горното разсъждение получаваме представяне $X_1 = X_2 \cup X_2'$ в обединение на собствени алгебрични подмножества $X_2 \subsetneq X_1$ и $X_2' \subsetneq X_1$, така че X_2 не се представя като крайно обединение от неприводими алгебрични множества. Продължавайки по същия начин построяваме безкрайна строго намаляваща редица

$$X \supsetneq X_1 \supsetneq X_2 \supsetneq \ldots \supsetneq X_m \supsetneq X_{m+1} \supsetneq \ldots$$

от Зариски затворени подмножества на $\overline{k}^n$. Съответната редица от идеали

$$I(X) \subsetneq I(X_1) \subsetneq I(X_2) \subsetneq \ldots \subsetneq I(X_m) \subsetneq I(X_m) \subsetneq \ldots$$

или хомогенни идеали

$$I_h(X) \subsetneq I_h(X_1) \subsetneq I_h(X_2) \subsetneq \ldots \subsetneq I_h(X_m) \subsetneq I_h(X_m) \subsetneq \ldots$$

нараства строго. Наистина, съвпадението $I(X_m) = I(X_{m+1})$ или, съответно, $I_h(X_m) = I_h(X_{m+1})$ води до $X_m = ZI(X_m) = ZI(X_{m+1}) = X_{m+1}$, съответно, $X_m = Z(I_h(X_m)_h) = Z(I_h(X_{m+1})_h) = X_{m+1}$ за Зариски затворените X_m, X_{m+1}. Пръстенът $\overline{k}[x_1, \ldots, x_n]$, съответно, $\overline{k}[x_0, \ldots, x_n]$ е ньотеров и не съдържа строго растящи редици от идеали. Противоречието доказва, че всяко афинно или проективно алгебрично множество има разлагане в крайно обединение на афинни, съответно, проективни многообразия, Q.E.D.
За да имаме единственост на разлагането на алгебрично множество в крайно обединение на неприводими компоненти, трябва да се ограничим с така наречените несъкратими разлагания.

Определение 6.36. *Разлагането $X = X_1 \cup \ldots \cup X_m$ на афинно афинно или проективно алгебрично множество X в крайно обединение от неприводими алгебрични подмножества $X_i \subseteq X$ се нарича несъкратимо, ако $X_i \not\subseteq X_j$ за всички $i \neq j$.*

Твърдение 6.37. *Всяко афинно или проективно алгебрично множество X има несъкратимо разлагане $X = X_1 \cup \ldots \cup X_m$ в крайно обединение от неприводими афинни, съответно, проективни алгебрични подмножества $X_i \subseteq X$. Всеки две несъкратими разлагания $X = X_1 \cup \ldots \cup X_m = Y_1 \cup \ldots \cup Y_l$ в крайни обединения от неприводими афинни алгебрични подмножества $X_i \subseteq X$ или $Y_j \subseteq X$ съвпадат, т.е. $m = l$ и съществува пермутация $j \in Sym_m$, така че $X_i = Y_{j(i)}$ за всички $1 \leq i \leq m$.*

Доказателство: Ако $X = X_1 \cup \ldots \cup X_s$ е произволно разлагане на афинно или проективно алгебрично множество X в крайно обединение от неприводими компоненти X_i, то за всяка двойка индекси $1 \leq i \neq j \leq s$ с $X_i \subseteq X_j$ изпускаме X_i и отново получаваме разлагане на X в крайно обединение от неприводими алгебрични подмножества. Двойките индекси $1 \leq i \neq j \leq s$ са краен брой, така че след евентуално изпускане на краен брой X_i получаваме несъкратимо разлагане $X = X_1 \cup \ldots \cup X_m$, $m \leq s$ в обединение на краен брой неприводими алгебрични подмножества X_j.

Нека $X = X_1 \cup \ldots \cup X_m$ и $X = Y_1 \cup \ldots \cup Y_l$ са две несъкратими разлагания на X в обединение от неприводими алгебрични подмножества X_i или Y_j. Тогава

$$X_i = X_i \cap X = X_i \cap (Y_1 \cup \ldots \cup Y_{l-1} \cup Y_l) = (X_i \cap Y_1) \cup \ldots \cup (X_i \cap Y_{l-1}) \cup (X_i \cap Y_l). \quad (6.3)$$

Поради неприводимостта на X_i и затвореността на $X_i \cap Y_j$ имаме $X_i = X_i \cap Y_{j(i)}$, а оттам и $X_i \subseteq Y_{j(i)}$ за някое $1 \leq j(i) \leq l$. Разменяме ролите на двете разлагания и с аналогични разглеждания и получаваме съществуването на индекс $1 \leq k(j(i)) \leq m$ с $Y_{j(i)} \subseteq X_{k(j(i))}$. В резултат, $X_i \subseteq X_{k(j(i))}$. Съгласно несъкратимостта на разлагането $X = X_1 \cup \ldots \cup X_m$, оттук следва $k(j(i)) = i$ и $X_i = Y_{j(i)}$.

Различните помежду си неприводими алгебрични множества $X_1, \ldots, X_m$ съвпадат съответно с различните помежду си неприводими алгебрични множества $Y_{j(1)}, \ldots, Y_{j(m)}$, така че $m \leq l$. Аналогични разсъждения след размяна на ролите на двете разлагания дават $l \leq m$, откъдето $l = m$. Още повече, множествата $X_1, \ldots, X_m$ съвпадат съответно с множествата $Y_{j(1)}, \ldots, Y_{j(m)}$, получени от $Y_1, \ldots, Y_m$ чрез прилагане на пермутацията $j \in Sym(m)$, Q.E.D.