Глава 1

# Въпрос 1: Полиноми и афинни пространства

Най-общо казано, афинно алгебрично многообразие е множеството от решения на система полиномиални уравнения. Идеалът на афинно алгебрично многообразие се определя като множеството на полиномите, анулиращи се във всички точки на това многообразие. Алгебричната геометрия изучава връзките между алгебричните многообразия и техните идеали. Настоящият курс по изчислителна алгебрична геометрия предлага конкретен конструктивен подход към предмета, характерен за епохата на възникването му през XIX век. Да напомним някои определения, които ще са ни нужни по-нататък.

Определение 1.1. *Непразното множество $R$ се нарича пръстен, ако в $R$ са определени две операции - събиране и умножение,*

$$R \times R \longrightarrow R, \qquad R \times R \longrightarrow,$$
$$(a, b) \mapsto a + b, \qquad (a, b) \mapsto ab,$$

*изпълняващи свойствата:*
*(i) асоциативност на събирането*

$$(a + b) + c = a + (b + c) \quad \text{за } \forall a, b, c \in R;$$

*(ii) комутативност на събирането*

$$a + b = b + a \quad \text{за } \forall a, b \in R;$$

*(iii) съществуване на нулев елемент $0 \in R$, така че $a + 0 = a$ за $\forall a \in R$;*
*(iv) съществуване на противоположен елемент $-a \in R$ за $\forall a \in R$, така че $a + (-a) = 0$;*
*(v) асоциативност на умножението*

$$(ab)c = a(bc) \quad \text{за } \forall a, b, c \in R;$$

*(vi) дистрибутивни закони за събирането и умножението*

$$a(b + c) = ab + ac \quad \text{за } \forall a, b, c \in R,$$
$$(a + b)c = ac + bc \quad \text{за } \forall a, b, c \in R.$$

Определение 1.2. *Казваме, че $R$ е комутативен пръстен с единица, ако $R$ е пръстен, в който $ab = ba$ за $\forall a, b \in R$ и съществува $1 \in R$, така че $a1 = a$ за $\forall a \in R$.*

Определение 1.3. *Поле $k$ е комутативен пръстен с единица, в който всеки нулев елемент $0 \neq a \in k$ има обратен $a^{-1} \in k$, така че $aa^{-1} = 1$.*

А сега да преминем към изучаването на полиномите с коефициенти от поле.

Определение 1.4. *Нулевите степени на променливите $x_1, \ldots, x_n$ ще считаме, че са равни на единицата 1 на полето $k$. За произволно естествено $m$ и $1 \leq i \leq n$, $x_i^m$ е произведението на $m$ екземпляра на $x_i$ със себе си. Произведенията от вида*

$$x^\alpha = x_1^{\alpha_1} \ldots x_n^{\alpha_n}$$

*с неотрицателни цели степени $\alpha_i$ се наричат мономи на $x_1, \ldots, x_n$.*

Определение 1.5. *Полином $f(x_1, \ldots, x_n)$ на $x_1, \ldots, x_n$ с коефициенти от поле $k$ е крайна линейна комбинация*

$$f(x_1, \ldots, x_n) = \sum_{\alpha \in A} a_\alpha x^\alpha$$

*с коефициенти $a_\alpha \in k$. Полиномите $f(x_1, \ldots, x_n) = \sum_{\alpha \in A} a_\alpha x^\alpha$ и $g(x_1, \ldots, x_n) = \sum_{\beta \in B} b_\beta x^\beta$ са равни, ако за всяка наредена $n$-торка $\alpha = (\alpha_1, \ldots, a_n)$ от неотрицателни цели числа $\alpha_i$, коефициентите $a_\alpha = \beta_\alpha$ на $x^\alpha$ в $f(x_1, \ldots, x_n)$ и $g(x_1, \ldots, x_n)$ са равни.*
*Множеството на полиномите $f(x_1, \ldots, x_n)$ на $x_1, \ldots, x_n$ с коефициенти от $k$ ще бележим с $k[x_1, \ldots, x_n]$.*

Степента на моном $x^\alpha = x_1^{\alpha_1} \ldots x_n^{\alpha_n}$ е

$$\deg(x^\alpha) = \alpha_1 + \ldots + \alpha_n.$$

Степента на полином $f = \sum_{\alpha \in A} a_\alpha x^\alpha$ се определя като

$$\deg(f) = \max\{\deg(x^\alpha) \,|\, \alpha \in A, a_\alpha \neq 0\}.$$

Лема 1.6. *За поризволни полиноми $f = \sum_{\alpha \in A} a_\alpha x^\alpha$ и $g = \sum_{\beta \in B} b_\beta x^\beta$ да положим $b_\alpha = 0$ за всички $\alpha \in A \setminus B$ и $a_\alpha = 0$ за всички $\alpha \in B \setminus A$. Да определим събиране*

$$f + g = \sum_{\alpha \in A \cup B} (a_\alpha + b_\alpha) x^\alpha$$

*и умножение*

$$fg = \sum_{\alpha \in A} \sum_{\beta \in B} a_\alpha b_\beta x^{\alpha+\beta},$$

*където $x^{\alpha+\beta} = x_1^{\alpha_1+\beta_1} \ldots x_n^{\alpha_n+\beta_n}$. Тогава $k[x_1, \ldots, x_n]$ е комутативен пръстен с единица относно така зададените операции.*

Доказателството на тази лема се привежда в редовния курс по алгебра и се извършва чрез проверка на аксиомите. Нулевият елемент на $k[x_1, \ldots, x_n]$ е така нареченият нулев полином, чиито всички коефициенти са нулеви.
А сега да преминем към

Определение 1.7. *Множеството*

$$k^n = \{(a_1, \ldots, a_n) \,|\, a_i \in k,\, 1 \leq i \leq n\}$$

*на наредените $n$-торки елементи от поле $k$ ще наричаме $n$-мерно афинно пространство над $k$.*

Всеки полином $f \in k[x_1, \ldots, x_n]$ определя функция

$$f : k^n \longrightarrow k,$$

$$f(a_1, \ldots, a_n) = \sum_{\alpha \in A} a_\alpha a_1^{\alpha_1} \ldots a_n^{\alpha_n}.$$

Ако $f(x_1, \ldots, x_n) = \sum_{\alpha \in A} a_\alpha x^\alpha$ е нулевият полином, т.е. $a_\alpha = 0$ за $\forall \alpha \in A$, то функцията $f : k^n \to k$ се анулира тъждествено върху $k^n$. Обратното не винаги е вярно. Например, полиномът $f(x) = x^2 - x = x(x-1)$ с коефициенти от полето $\mathbb{Z}_2$ на остатъците при деление с 2 не е тъждествено нулев, но функцията

$$f(x) = x(x-1) : \mathbb{Z}_2 \longrightarrow \mathbb{Z}_2$$

се анулира тъждествено върху $\mathbb{Z}_2 = \{0(\mathrm{mod}2), 0(\mathrm{mod}2)\}$. В сила е следното

Твърдение 1.8. *Нека $k$ е безкрайно поле, а $f \in k[x_1, \ldots, x_n]$ е полином на $x_1, \ldots, x_n$ с коефициенти от $k$. В такъв случай, $f$ е тъждествено нулевият полином тогава и само тогава, когато $f : k^n \to k$ е тъждествено нулевата функция върху $k^n$.*

**Доказателство:** Трябва да докажем, че ако $f(a_1,\dots,a_n)=0\in k$ за всички $\forall(a_1,\dots,a_n)\in k^n$, то $f(x_1,\dots,x_n)\in k[x_1,\dots,x_n]$ е тъждествено нулевият полином. Ще приложим индукция по броя $n$ на променливите $x_1,\dots,x_n$.
За $n=1$ всеки полином $f(x_1)$ от степен $N=\deg(f)\geq 0$ има най-много $N$ различни корена, така че анулирането на $f$ във всички $a\in k$ изисква $f$ да е тъждествено нулевият полином. По-подробно, ако $\deg(f)=0$, то $f$ е ненулева константа от полето $k$ и няма корени. С индукция по степента $d=\deg(f)$, ако $f(x)=0$ няма корени в $k$, то в частност, корените на $f(x)=0$ са най-много $d$. Ако $a_0\in k$ е корен на $f(x)$, то при деление на $f(x)$ с $x-a_0$ получаваме $f(x)=(x-a_0)f_1(x)$ за подходящ полином $f_1(x)\in k[x]$ и нулев остатък. От $d=\deg(f)=\deg(x-a_0)+\deg(f_1)=1+\deg(f_1)$ следва, че $\deg(f_1)=d-1$. По индукционно предположение, $f_1(x)=0$ има най-много $d-1$ корена $a_1,\dots,a_s\in k$, $s\leq d-1$. Доколкото всеки корен на $f(x)=(x-a_0)f_1(x)=0$ е равен на $a_0$ или е корен на $f_1(x)=0$, корените $a_0,a_1,\dots,a_s\in k$ на $f(x)=0$ се оказват най-много $d$.
Да допуснем, че сме доказали твърдението за полиноми на $n-1$ порменливи и да разгледаме полином $f(x_1,\dots,x_n)\in k[x_1,\dots,x_n]$, който се анулира във всички $(a_1,\dots,a_n)\in k^n$. Представяме

$$f(x_1,\dots,x_n)=\sum_{i=0}^{N} g_i(x_1,\dots,x_{n-1})x_n^i$$

като полином на $x_n$, чиито коефициенти $g_i(x_1,\dots,x_n)\in k[x_1,\dots,x_{n-1}]$ са полиноми на $x_1,\dots,x_{n-1}$ с коефициенти от $k$. За всяко фиксирано $(a_1,\dots,a_{n-1})\in k^{n-1}$ полиномът

$$f(a_1,\dots,a_{n-1},x_n)=\sum_{i=0}^{N} g_i(a_1,\dots,a_{n-1})x_n^i\in k[x_n]$$

на една променлива $x_n$ се анулира във всички $x_n=a_n\in k$. Както вече отбелязахме, $f(a_1,\dots,a_{n-1},x_n)$ трябва да се анулира тъждествено като полином на $x_n$. Това означава анулиране на коефициентите $g_i(a_1,\dots,a_{n-1})=0$ за всички $1\leq i\leq N$. Прилагайки това разсъждение за всички $(a_1,\dots,a_{n-1})\in k^{n-1}$ получаваме, че всички $g_i: k^{n-1}\to k$ задават тъждествено нулевата функция. По индукционно предположение оттук следва анулирането на всички $g_i(x_1,\dots,x_{n-1}\in k[x_1,\dots,x_{n-1}]$ като полиноми на $x_1,\dots,x_{n-1}$ с коефициенти от $k$. Това е достатъчно за анулирането на $f=\sum_{i=0}^{N} g_i(x_1,\dots,x_{n-1})x_n^i$ като полином на $x_1,\dots,x_n$ с коефициенти от $k$, Q.E.D.
Прилагайки горното твърдение към разликата на полиноми $f,g\in k[x_1,\dots,x_n]$ получаваме следното

Следствие 1.9. *Нека $k$ е безкрайно поле, а $f(x_1,\dots,x_n)$ и $g(x_1,\dots,x_n)$ са полиноми на $x_1,\dots,x_n$ с коефициенти от $k$. В такъв случай $f(x_1,\dots,x_n)$ и $g(x_1,\dots,x_n)$ съвпадат като полиноми на $x_1,\dots,x_n$ с коефициенти от $k$ тогава и само тогава, когато $f:k^n\to k$ и $g:k^n\to k$ съвпадат като функции.*

## Задачи

Задача 1.10. *Нека $\mathbb{Z}_2$ е полето от остатъци при деление с 2. Да се докаже, че всеки от полиномите $g_{ij}(x_1,\dots,x_n)=x_1\dots x_n(x_i+x_j)$ с $1\leq i<j\leq n$ задава тъждествено нулевата функция $g_{ij}:\mathbb{Z}_2^n\to\mathbb{Z}_2$ без да съвпада с тъждествено нулевия полином.*

Задача 1.11. *Нека $f(x_1,\dots,x_n)=\sum_{\alpha\in A} a_\alpha x^\alpha$ е полином на $x_1,\dots,x_n$ с коефициенти от полето $\mathbb{C}$ на комплексните числа, $M$ е неотрицателно цяло*

*число със свойството* $M \geq \alpha_i$ *за всички* $\alpha = (\alpha_1, \ldots, \alpha_n) \in A$, $1 \leq i \leq n$, *а*

$$\mathbb{N}^n_{M+1} = \{(z_1, \ldots, z_n) \,|\, z_i \in \mathbb{N}, 1 \leq z_i \leq M+1,\ 1 \leq i \leq n\}.$$

*Да се докаже, че ако функцията*

$$f : \mathbb{C}^n \longrightarrow \mathbb{C},$$
$$(a_1, \ldots, a_n) \mapsto f(a_1, \ldots, a_n)$$

*се анулира във всички точки от* $\mathbb{N}^n_{M+1}$, *то* $f(x_1, \ldots, x_n)$ *съвпада с тъждествено нулевия полином.*