# Тема 28 - Алгебра

Полиноми на една променлива. Теорема за деление на полиноми с частно и остатък. Схема на Хорнер. НОД - тъждество на Безу и алгоритъм на Евклид - Корени на полином и зависимости м/у корените и коефициентите на полинома

## 1. Полиноми на една променлива

Дефиниция (полином с коефициенти над поле): Нека $F$ е произволно поле. Дефинираме множеството $F[x] = \{ f = (a_0, a_1, \ldots, a_n, 0, 0, \ldots) \mid a_i \in F \}$, т.е $F[x]$ е съвкупността от всички безкрайни редици, които имат краен брой ненулеви елементи от $F$. Елементите (редиците) на така дефинираното множество $F[x]$ ще наричаме полиноми.

Нека $f = (a_0, a_1, \ldots, a_n, \ldots) \in F[x]$ и $g = (b_0, b_1, \ldots, b_n, \ldots) \in F[x]$. Въвеждаме следните две бинарни операции в $F[x]$:

а) събиране: $f + g = (a_0 + b_0, a_1 + b_1, \ldots, a_s + b_s, a_{s+1}, \ldots) \in F[x]$

б) умножение: $f \times g = (c_0, c_1, \ldots, c_k, \ldots) \in F[x]$, където $c_k = \sum_{k=ij} a_i b_j$

$\rightarrow f + g = (a_0 + b_0, a_1 + b_1, \ldots, a_s + b_s, a_{s+1}, \ldots, a_n, 0, \ldots) \in F[x]$

Числото $n$ наричаме степен на полинома $f$ и означаваме $\deg(f) = n$. Полиномите от нулева степен наричаме константни полиноми. Те са от вида $f = a \in F[x]$. По дефиниция нулевият полином има степен $\deg(0) = -\infty$.

Дефиниция (степен на полином). Степента на ненулев полином на една променлива е равна на най-високата степен на променлива с ненулев коефициент. За

степените на полиномите f и g от F[x] са в сила следните две свойства:

а) $\deg(f+g) \leq \max(\deg(f), \deg(g))$

б) Ако F е област, то $\deg(f \cdot g) = \deg(f) + \deg(g)$ и F област $\Rightarrow$ F[x] също е област. Област означава, че няма делители на 0.

Д-во:

Събиране: Ако $\deg(f) \neq \deg(g)$ то степента на сумата ще е равна на по-голямата от двете степени.
Ако $\deg(f) = \deg(g)$, то степента на сумата ще е по-малка от $\deg(f)$ само ако коефициентите на най-високата степен се неутрализират, в противен случай степента е равна на $\deg(f) = \deg(g)$

Произведение: Най-високата степен в произведението $f \cdot g$ се получава от произведението на най-високите степени на двата полинома, т.е
$(a_n x^n) \cdot (b_m x^m) = a_n b_m x^{(n+m)}$

Пример за полиноми:

$P(x) = 5x^5 + 3x^2 + 4x + 3$

$Q(x) = 6x^4 + 3x^3 + 2x^2 + 5x + 1$

$\deg(P) = 5$ ; $\deg(Q) = 4$

$P(x) + Q(x) = 5x^5 + 6x^4 + 3x^3 + (3+2)x^2 + (4+5)x + (1+3)$
$= 5x^5 + 6x^4 + 3x^3 + 5x^2 + 9x + 4$

$P(x) \cdot Q(x) = 5x^5 \cdot 6x^4 + 5x^5 \cdot 3x^3 + 5x^5 \cdot 2x^2 + 5x^5 \cdot 5x + 5x^5 \cdot 1 +$
$3x^2 \cdot 6x^4 + 3x^2 \cdot 3x^3 + \ldots + 3 \cdot 1 =$
$= 30x^9 + 15x^8 + 10x^7 + 25x^6 + 5x^5 + 18x^6 + 9x^5 + \ldots + 3$

# 1. Полиноми на 1 променлива

$x = (0, 1, 0, \dots)$, $1 \in F$

$x^2 = (0, 1, 0, \dots)(0, 1, 0, \dots) = (0, 0, 1, 0, \dots)$

$x^3 = (0, 1, 0, \dots)(0, 0, 1, 0, \dots) = (0, 0, 0, 1, 0, \dots)$

$x^n = (0, 0, \dots, \underbrace{1}_{n+1\text{-място}}, 0 \dots)$

$a = (a, 0 \dots)$, $x = (0, 1, 0 \dots)$

$ax = (0, a, 0, \dots)$

$ax^2 = (0, 0, a, \dots)$

$f(a_0, a_1, \dots, a_n, 0, \dots) = (a_0, 0 \dots) + (0, a_1, 0, \dots) + \dots + (0, 0 \dots, a_n, 0, \dots) = a_0 + a_1 x + a_2 x^2 + \dots + a_n x^n$

$F[x] = \{ f = a_0 + a_1 x + a_2 x^2 + \dots + a_n x^n \mid a_i \in F, n \in \mathbb{N} \}$

$g = b_0 + b_1 x + b_2 x^2 + \dots + b_s x^s$ Б.О.О $n \geq s$

$f + g = (a_0 + b_0) + (a_1 + b_1) x + \dots + (a_s + b_s) x^s + a_{s+1} x^{s+1} + \dots + a_n x^n$

$f \cdot g = c_0 + c_1 x + c_2 x^2 + \dots + c_k x^k$

$c_k = \sum_{i+j=k} a_i b_j$

$f = a_0 + a_1 x + a_2 x^2 + \dots + a_n x^n$

$g = b_0 + b_1 x + b_2 x^2 + \dots + b_s x^s$

$f = g$, ако $n = s$ и $a_i = b_i$, $i = \overline{0, n}$

$f$ - полином на променливата $x$

$a_0$ - свободен член/коефициент

$a_i$ - коефициенти, $i = \overline{1, n-1}$

$a_n$ - старши коефициент

$n$ - степен на полинома $f$, бележим: $\deg f = n$

$f = a \in F$ - константен полином, $\deg f = 0$, $a \neq 0$

$f = 0 \in F$, $\deg 0 = -\infty$

Нека $b \in F$ и $f(b)$ = $f = a_0 + a_1 x + a_2 x^2 + \dots + a_n x^n \in F[x]$, тогава

$f(b) = a_0 + a_1 b + a_2 b^2 + \dots + a_n b^n$ наричаме с-ст на полинома $f$ в $b$.

Тук нагоре правим следната Уговорка:
F е числово поле и

$$F[x] = \{ f = a_0 x^n + a_1 x^{n-1} + \dots + a_{n-1} x + a_n \mid a_i \in F \}$$

$\deg f = n$, $a_0$ = старши коефициент, $a_i$ - коефициент, $a_n$ - свободен член

$F[x]$ е комутативен пръстен с 1 (цяла област).

2. Теорема за деление с частно и остатък (теорема 1)
Нека $F$ е поле. Нека $f, g \in F[x]$, $g \neq 0$.
Тогава съществуват единствени $q, r \in F[x]$ такива, че $f = q.g + r$, $\deg(r) < \deg(g)$. Казваме, че $q$ е частно, а $r$ е остатък при делението на $f$ с $g$.

Доказателство:
Съществуване. Нека $\deg(f) = n$, $f = a_0x^n + a_1x^{n-1} + \dots + a_n$, $a_0 \neq 0$, и $\deg(g) = m$. $g = b_0x^m + b_1x^{m-1} + \dots + b_m$, $b^0 \neq 0$.
Ще направим доказателство с индукция по $n$.
1) $\deg(f) < \deg(g)$. Тогава $f = 0 \cdot g + f \Rightarrow q = 0, r = f$
Тогава $\deg(r) = \deg(f) < \deg(g)$ ✓
2) $\deg(g) = 0 \Rightarrow g = a \in F$. Тогава $f = g \cdot \frac{f}{g} = g \cdot \frac{f}{a}$

и следователно $q = \frac{f}{a}$ и $r = 0$

Така отново $\deg(r) < \deg(g)$ $(-\infty < 0)$
3) $\deg(f) > \deg(g)$ и $\deg(g) \neq 0$. Да разглеждаме $Q = \frac{a_0}{b_0} x^{n-m}$. Ако вземем $Q.g$, то това е полином със старши ~~коефициент~~ член $a_0x^n$, т.е. съвпада със старшия член на $f$.
Сега нека $f_1 = f - Q.g$. Следователно за построението $f_1$ е вярно, че $\deg(f_1) < \deg(f) = n$. Съгласно индуктивно предположение, всеки полином от степен строго по-малка от $n$ може да се представи във вида $f' = q'.g + r'$, за някакви $q', r' \in F[x]$, такива че $\deg(r') < \deg(g)$. Тогава $f_1 = q_1.g + r_1$. ~~и сега~~
Сега можем да заместим: $f = f_1 - Q.g =$
$q_1.g - Q.g + r_1 = (q_1 - Q)g + r_1$ и сега чрез полагане $q = q_1 - Q$ и $r = r_1$ получаваме, че

$f = q \cdot g + r$, където
$\deg(r) = \deg(r') < \deg(g)$. Така показваме, че
$q$ и $r \in F[x]$ съществуват

Единственост: Нека $f = q_1 \cdot g + r_1 = q_2 \cdot g + r_2$.
Нека $q_1 \neq q_2$ и $r_1 \neq r_2$. Тогава
$(q_1 - q_2) \cdot g = r_2 - r_1$
$\deg((q_1 - q_2) \cdot g) = \deg(q_1 - q_2) + \deg(g) \geq \deg(g)$
$\deg(r_2 - r_1) \leq \deg(r_2) < \deg(g)$ по условие
$\Rightarrow \deg((q_1 - q_2) \cdot g) > \deg(r_2 - r_1)$, което е противоречие. □

3 (Схема на Хорнер - директно следствие от теорема 1
Нека $f \in F[x]$, $f = a_0 x^n + a_1 x^{n-1} + \dots + a_n$, $a_0 \neq 0$,
$g = (x - \alpha) \in F[x]$. Нека $f = q \cdot g + r$ (съгласно теорема 1)
и $\deg(r) < \deg(g) = \deg(x - \alpha) = 1 \Rightarrow r = a$ - константа,
$r \in F$ и $q$ има вида $q = b_0 x^{n-1} + b_1 x^{n-2} + \dots + b_{n-1}$.
Схема на Хорнер помага за намирането на
корени на полиноми - ако $r = 0$, казваме, че $\alpha$ е
корен. Така представяме $f$ по следния начин:
$f = (x - \alpha) \cdot (b_0 x^{n-1} + b_1 x^{n-2} + \dots + b_{n-1}) + r = a_0 x^n + a_1 x^{n-1} + \dots + a_n$
Където: $b_0 = a_0$
$b_1 = a_1 + \alpha b_0$
$b_2 = a_2 + \alpha b_1$
$\vdots$
$b_i = a_i + \alpha b_{i-1}$
$\vdots$
$b_{n-1} = a_{n-1} + \alpha b_{n-2}$
$r = a_n + \alpha b_{n-1}$

| | $a_0$ | $a_1$ | $a_2$ | $\dots$ | $a_{n-1}$ | $a_n$ |
|---|---|---|---|---|---|---|
| $\alpha$ | $b_0$ | $b_1$ | $b_2$ | $b$ | $b_{n-1}$ | $r$ |

4. Най-голям общ делител на полином с коеф. от поле.
Нека F е поле. Нека $f, g \in F[x]$, $g \neq 0$. Най-голям общ делител (НОД) на полиномите f и g наричаме полинома $d(x) \in F[x]$, за който е изпълнено, че:
1) d дели f ($d \mid f$) и d дели g ($d \mid g$)
2) Ако $d_1$ дели f и $d_1$ дели g, то $d_1$ дели d
В този случай казваме, че d е НОД на f и g и бележим $d = (f, g)$

Твърдение за съществуване на НОД: Всеки два полинома $f, g \in F[x]$, $g \neq 0$ притежават НОД
Доказателство: Нека I е идеалът на пръстена F[x], породен от f и g. Тогава $I = \{uf + v.g \mid u, v \in F[x]\}$. По условие $g \neq 0 \Rightarrow I \neq \{0\}$. Използваме твърдението, че в полето F[x] всички идеали са главни. Следователно $I = \langle d \rangle$. Ще покажем, че $d = (f, g)$.
1) $f, g \in I \Rightarrow f = f_1 . d$, $g = g_1 . d$ за някакви $f_1, g_1 \in F[x]$. Това обаче означава, че $d \mid f$ и $d \mid g$.
2) $d \in I \Rightarrow d = u . f + v . g$, за някакви $u, v \in F[x]$. Сега нека $d_1 \mid f$ и $d_1 \mid g$. Това от свойство 5 следва, че $d_1 \mid uf + vg$ за всякакви $u, v \in F[x]$. Следователно $d_1 \mid d$
От 1), 2) следва, че d е НОД на f и g, т. е $d = (f, g)$
$d = (f, g)$ е определен с точност до ненулева константа

Твърдение на Безу: Нека $f, g \in F[x]$, $g \neq 0$. Тогава $\exists u, v \in F[x]$ такива, че $uf + v.g = d$, където $d = (f, g)$. В частност, ако f и g са взаимно прости, то $uf + v.g = 1 = d$. Вярно е и обратното, ако съществуват u и v, такива, че $uf + vg = 1$, то f и g са взаимно прости.

Алгоритъм на Евклид - взимайки дадените на входа на алгоритъма две числа a и b, проверяваме дали b е равно на 0. Ако да, числото a е търсеният

Най-голям общ делител. Ако не, повтаряме процеса, като използваме за входни данни b и остатъка получен при деленето на a и b. Аналогично можем да приложим този алгоритъм за полиноми вместо числа.

Нека $f \neq 0$, $g \neq 0 \in F[x]$ ; $(f,g) = ?$

$f = g \cdot q_1 + r_1$, $\deg(g) > \deg(r_1)$ (1)

ако $r_1 \neq 0$ $g = r_1 \cdot q_2 + r_2$, $\deg(r_1) > \deg(r_2)$ (2)

ако $r_2 \neq 0$ $r_1 = r_2 \cdot q_3 + r_3$, $\deg(r_2) > \deg(r_3)$ (3)

$\vdots$ краен брой $\deg(r_i) \leq \deg(r_{i-1})$

$r_{k-1} = r_k \cdot q_{k+1} + 0$ (4)

$\Rightarrow$ Последният ненулев остатък $r_k$ е НОД на $f$ и $g$.

$r_k = (f,g)$

Доказателство: Ако тръгнем отзад-напред получаваме:

(4) $\Rightarrow r_k \mid r_{k-1}$ ... (1) $\Rightarrow r_k \mid f$ и $r_k \mid g$

Обратно, ако $d_1 \mid f$ и $d_1 \mid g$, тръгваме отпред-назад и получаваме: (1) $d_1 \mid f$, $d_2 \mid g$, ..., (4) $\Rightarrow d_1 \mid r_k$ ✓

5. Корени на полиноми

Нека $F$ е поле и $F \leq K$ - разширение на полето $F$.

Нека $f \in F[x]$, $\alpha \in K$, то $\alpha$ е корен на $f$, ако $f(\alpha) = 0$.

$f(\alpha) = 0 \iff f = (x-\alpha) \cdot q$, $q \in K[x]$

6. Принцип за сравняване на коефициенти: Нека $F$ е област. Нека $g_1, g_2 \in F[x]$ и $\deg(g_1) \leq n$, $\deg(g_2) \leq n$. Нека съществуват $n+1$ два по два различни елемента $\alpha_1, \alpha_2, \ldots, \alpha_{n+1}$ от $F$, такива че $g_1(\alpha_i) = g_2(\alpha_i)$ за $i = \overline{1, n+1}$. Тогава $g_1 = g_2$

Виет: Зависимостите м/у коефициентите и корените на един полином

Нека $F$ е поле, $n \in \mathbb{Z}_{\geq 0}$ и

$f = a_0x^n + a_1x^{n-1} + \dots + a_n \in F[x]$ и

$\alpha_1, \alpha_2, \dots, \alpha_n$ всички корени на $f$ в $K \supseteq F$, $\dim_F K = \overline{1,n}$

$\Rightarrow f = a_0x^n + a_1x^{n-1} + \dots + a_n = a_0(x-\alpha_1)\cdot(x-\alpha_2)\dots(x-\alpha_n)$

Ако разкрием скобите и сравним директно коефициентите пред различните степени на $x$ отляво и отдясно, то

с уе получим зависимостите м/у корените $\alpha_1, \dots, \alpha_n$ на $f$ коефициентите му пред различните степени на $x$.

Тези зависимости са известни като формули на Виет:

$\binom{n}{1}$ $\alpha_1 + \alpha_2 + \dots + \alpha_n = -\frac{a_1}{a_0}$

$\binom{n}{2}$ $\alpha_1\alpha_2 + \alpha_1\alpha_3 + \dots + \alpha_{n-1}\alpha_n = \frac{a_2}{a_0}$

$\vdots$

$\binom{n}{i}$ $\alpha_1\alpha_2\dots\alpha_i + \dots + \alpha_{n-i+1}\dots\alpha_{n-1}\alpha_n = \frac{(-1)^i a_i}{a_0}$

$\binom{n}{n}$ $\alpha_1\alpha_2\dots\alpha_n = (-1)^n \frac{a_n}{a_0}$

$\Rightarrow$ броят на обединенията

Общо формулите на Виет могат да се представят като

$$\sum_{1 \leq i_1 < i_2 < \dots < i_k \leq n} \alpha_{i_1}\alpha_{i_2}\dots\alpha_{i_k} = (-1)^k \frac{a_k}{a_0}$$

, където броят на обединенията в сумата е числа от биномния коефициент $\binom{n}{k} = \frac{n!}{k!(n-k)!}$

Пример:

$ax^3 + bx^2 + cx + d$

$\beta_1 = \alpha_1 + \alpha_2 + \alpha_3 = -\frac{b}{a}$

$\beta_2 = \alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3 = \frac{c}{a}$

$\beta_3 = \alpha_1\alpha_2\alpha_3 = -\frac{d}{a}$

$ax^4 + bx^3 + cx^2 + dx + m$

$\beta_1 = \alpha_1 + \alpha_2 + \alpha_3 + \alpha_4 = -\frac{b}{a}$

$\beta_2 = \alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_1\alpha_4 + \alpha_2\alpha_3 + \alpha_2\alpha_4 + \alpha_3\alpha_4 =$

$\beta_3 = \alpha_1\alpha_2\alpha_3 + \alpha_1\alpha_2\alpha_4 + \alpha_1\alpha_3\alpha_4 + \alpha_2\alpha_3\alpha_4 = -\frac{c}{a}$

$\beta_4 = \alpha_1\alpha_2\alpha_3\alpha_4 = \frac{m}{a}$