ЛЕКЦИЯ 9
ДЕЛИМОСТ НА ПОЛИНОМИ

Определение. *Нека K е комутативен пръстен и $f(x), g(x) \in K[x]$. Казваме, че $f(x)$ се дели на $g(x)$ (или $g(x)$ дели $f(x)$), ако съществува $h(x) \in K[x]$, такъв че $f(x) = g(x).h(x)$.*

Равенството $0 = g(x).0$ означава, че нулевият полином се дели на всеки друг полином. Тъй като от $f(x) = 0.g(x)$ следва, че $f(x) = 0$, то нулевият полином дели само себи си.

Твърдение 1. *Нека K е комутативен пръстен и $f(x)$, $f_1(x)$, ..., $f_s(x) \in K[x]$. Ако $f(x)$ дели всеки от полиномите $f_1(x)$, ..., $f_s(x)$, тогава $f(x)$ дели и $f_1(x).g_1(x)+\cdots+f_s(x).g_s(x)$, където $g_1(x)$, ..., $g_s(x)$ са произволни полиноми от $K[x]$.*

Доказателство:

От $f(x)$ дели $f_i(x)$ имаме, че съществува полином $f_i^*(x)$, така че $f_i(x) = f_i^*(x).f(x)$, $i = 1, \ldots, s$.

Следователно

$$f_1(x).g_1(x) + \cdots + f_s(x).g_s(x) =$$
$$f_1^*(x).f(x).g_1(x) + \cdots + f_s^*(x).f(x).g_s(x) =$$
$$f(x)\big(f_1^*(x).g_1(x) + \cdots + f_s^*(x).g_s(x)\big)$$

и $f(x)$ дели $f_1(x).g_1(x) + \cdots + f_s(x).g_s(x)$.

Твърдение 2. *Нека K е комутативен пръстен с единица. За всяко естествено число n и всяко $\alpha \in K$ полиномът $x^n - \alpha^n$ се дели на $x - \alpha$.*

Доказателство:

$$(x-\alpha)(x^{n-1} + \alpha^1 x^{n-2} + \alpha^2 x^{n-3} + \cdots + \alpha^{n-2}x + \alpha^{n-1}) =$$
$$= x^n + \alpha x^{n-1} + \alpha^2 x^{n-2} + \cdots + \alpha^{n-2}x^2 + \alpha^{n-1}x -$$

$$-\alpha x^{n-1} - \alpha^2 x^{n-2} - \cdots - \alpha^{n-2}x^2 - \alpha^{n-1}x - \alpha^n = x^n - \alpha^n.$$

Следователно $x^n - \alpha^n$ се дели на $x - \alpha$.

Теорема 1. *Нека K е комутативен пръстен с единица и $f(x) \in K[x]$. За всяко $\alpha \in K$ съществува $g(x) \in K[x]$, такъв че $f(x) = (x-\alpha)g(x)+f(\alpha)$.*

Доказателство:

Нека

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n.$$

Тогава

$$f(\alpha) = a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_n\alpha^n$$

и

$$f(x) - f(\alpha) = a_1(x-\alpha) + a_2(x^2-\alpha^2) + \cdots + a_n(x^n - \alpha^n).$$

Съгласно Твърдение 2 имаме, че всяко събираемо в дясната част на последното равенство се дели на $(x-\alpha)$. От Твърдение 1 следва, че $(x-\alpha)$ дели $f(x)-f(\alpha)$, т. е. $f(x)-f(\alpha) = (x-\alpha)g(x)$ и $f(x) = (x-\alpha)g(x)+f(\alpha)$.

Следствие 1. *Нека K е комутативен пръстен с единица и $f(x)$ е полином с коефициенти от този пръстен. Елементът $\alpha \in K$ е корен на $f(x)$ тогава и само тогава, когато $x - \alpha$ дели $f(x)$.*

Доказателство:

1) Нека α е корен на $f(x)$, т. е. $f(\alpha) = 0$. От Теорема 1 имаме $f(x) = (x-\alpha)g(x) + f(\alpha) = (x-\alpha)g(x)$ и следователно $(x-\alpha)$ дели $f(x)$.

2) Нека $(x-\alpha)$ дели $f(x)$. Тогава $f(x) = (x-\alpha)g(\alpha)$. Следователно $f(\alpha) = (\alpha-\alpha)g(x) = 0$ и α е корен на $f(x)$.

Следствие 2. *Нека K е комутативен пръстен с единица, в който няма делители на нулата. Тогава броят на различните корени на всеки ненулев полином от $K[x]$ в пръстена K не е по-голям от степента на $f(x)$.*

Доказателство:

Нека $f(x) \in K[x]$ и е ненулев.

Доказателството ще направим по индукция относно $n = \text{ст.}\,(f(x))$.

База: $n = 0$. В тази ситуация $f(x) = a_0$, $a_0 \neq 0$ и твърдението е очевидно, понеже $f(x)$ няма корени.

Нека $n \geq 1$. Ако $f(x)$ няма корени в K, тогава твърдението е очевидно. Нека $f(x)$ има корен $\alpha \in K$. Тогава $f(x) = (x-\alpha)g(x)$, където $g(x) \in K[x]$ и ст. $g(x) = n-1$.

Допускаме, че $f(x)$ освен α има друг корен β, $\beta \neq \alpha$. Тогава $f(\beta) = (\beta-\alpha)g(\beta)$ Понеже $\beta - \alpha \neq 0$ и в K няма делители на нулата, следва

$g(\beta) = 0$. И така всеки корен на полинома $f(x)$ в K, който е различен от α е корен на $g(x)$. Съгласно индуктивната хипотеза броят на различните корени на полинома $g(x)$ не са повече от $n-1$. Следователно броят на различните корени на $f(x)$ в K не е повече от n.

Забележка. *Ако в основния пръстен има делители на нулата, тогава някои полиноми могат да имат повече корени отколкото е тяхната степен.*

Пример. *Разглеждаме пръстена на квадратните матрици от втори ред над* $\mathbb{R}$. *Полиномът* $X^2 - E$ *има очевидно следните четири корена*

$$X_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad X_2 = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \quad X_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad X_4 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$$

Теорема 2. *Нека* K *е комутативен пръстен с единица, в който няма делители на нулата и* $|K| = \infty$. *Нека* $f(x)$, $g(x) \in K[x]$ *и* $f(\alpha) = g(\alpha)$, *за всяко* $\alpha \in K$. *Тогава* $f(x)$ *и* $g(x)$ *са равни в алгебричен смисъл.*

Доказателство:

Допускаме, че $f(x)$ и $g(x)$ не са равни в алгебричен смисъл. Това означава, че коефициентите им пред някоя от степените на x са различни. Следователно полиномът $h(x) = f(x) - g(x)$ има ненулев коефициент и поради това h(x) е ненулев полином. Нека ст. $h(x) = n$. Избираме α_1, $\ldots$, $\alpha_{n+1} \in K$, такива че $\alpha_i \neq \alpha_j$, $i \neq j$. Този избор е възможен, защото $|K| = \infty$. От условието имаме

$$h(\alpha_i) = f(\alpha_i) - g(\alpha_i) = 0, \quad i = 1, \ldots, n+1$$

И така, полиномът $h(x)$ има повече корени от колкото е неговата степен, което противоречи на Следствие 2.

Определение. *Нека* F *е поле и* $a, b \in F$, $b \neq 0$. *Дробта* $\dfrac{a}{b}$ *се дефинира с равенството*

$$\frac{a}{b} \stackrel{\text{def}}{=} a.b^{-1}.$$

Теорема 3. *Нека* F *е поле и* $\alpha_1, \ldots, \alpha_n \in F$, $\alpha_i \neq \alpha_j$, $i \neq j$. *За произволни елементи* $y_1, \ldots, y_n \in F$ *съществува и то единствен полином* $f(x) \in F[x]$, *такъв че* ст. $f(x) \leqq n-1$ *и* $f(\alpha_i) = y_i$, $i = 1, \ldots, n$.

Доказателство:

Трябва да определим коефициентите $a_0, a_1, \ldots, a_{n-1}$ на полинома

$$f(x) = a_0 + a_1 x + \cdots + a_{n-1} x^{n-1}.$$

От условието имаме

$$\begin{aligned}
f(\alpha_1) &= a_0 + a_1\alpha_1 + \cdots + a_{n-1}\alpha_1^{n-1} = y_1 \\
f(\alpha_2) &= a_0 + a_1\alpha_2 + \cdots + a_{n-1}\alpha_2^{n-1} = y_2 \\
&\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\
f(\alpha_n) &= a_0 + a_1\alpha_n + \cdots + a_{n-1}\alpha_n^{n-1} = y_n
\end{aligned}$$

Можем да разглеждаме тези равенства като линейна система относно a_0, a_1, $\ldots$, a_{n-1}, която е квадратна. Детерминантата на тази система е

$$\begin{vmatrix} 1 & \alpha_1 & \alpha_1^2 & \ldots & \alpha_1^{n-1} \\ 1 & \alpha_2 & \alpha_2^2 & \ldots & \alpha_2^{n-1} \\ & \cdots\cdots\cdots\cdots & & & \\ 1 & \alpha_n & \alpha_n^2 & \ldots & \alpha_n^{n-1} \end{vmatrix} = \prod_{1\le i<j\le n} (\alpha_i - \alpha_j).$$

Тъй като $\alpha_i - \alpha_j \neq 0$ и в полето няма делители на нулата, тази детерминанта е различна от нула. Получената линейна система е Крамерова и тя има единствено решение, което може да се намери например по формулите на Крамер. Понеже α_1, $\ldots$, α_n, y_1, y_2, $\ldots y_n \in F$, коефициентите на тази система са елементи на F. Следователно решението ѝ също принадлежи на F. С това доказахме, че търсеният полином $f(x) \in F[x]$ съществува и е единствен. Изчисляването на коефициентите чрез фолмулите на Крамер не е целесъобразно.

Интерполационна формула на Лагранж

Разглеждаме полинома

$$f(x) = \frac{(x-\alpha_2)\ldots(x-\alpha_n)}{(\alpha_1-\alpha_2)\ldots(\alpha_1-\alpha_n)}y_1 + \\ \frac{(x-\alpha_1)(x-\alpha_3)\ldots(x-\alpha_n)}{(\alpha_2-\alpha_1)(\alpha_2-\alpha_3)\ldots(\alpha_2-\alpha_n)}y_2 + \cdots + \frac{(x-\alpha_1)\ldots(x-\alpha_{n-1})}{(\alpha_n-\alpha_1)\ldots(\alpha_n-\alpha_{n-1})}y_n$$

Ясно е, че степента на този полином не е по-голяма от $n-1$. Понеже α_1, $\ldots$, α_n, y_1, y_2, $\ldots y_n \in F$, имаме $f(x) \in F[x]$. Очевидно е, че

$$\begin{aligned}
f(\alpha_1) &= y_1 + 0 + \cdots + 0 = y_1 \\
f(\alpha_2) &= 0 + y_2 + \cdots + 0 = y_2 \\
&\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\
f(\alpha_n) &= 0 + 0 + \cdots + y_n = y_n
\end{aligned}$$

Поради това $f(x)$ е търсеният в Теорема 3 полином. Този начин за получаване на полинома $f(x)$ се нарича *Интерполационна формула на Лагранж.*

Правило на Хорнер

Нека K е комутативен пръстен с единица и $f(x) = a_0 + a_1x + \cdots + a_nx^n \in K[x]$, $a_n \neq 0$, $n \geqq 1$. Ако $\alpha \in K$ трябва да пресметнем $f(\alpha) =?$. Съгласно Теорема 1

$$f(x) = (x - \alpha)g(x) + f(\alpha), \text{ където ст. } g(x) = n - 1.$$

Нека $g(x) = b_0 + b_1x + \cdots + b_{n-1}x^{n-1}$. Тогава

$$f(x) = (x - \alpha)(b_0 + b_1x + \cdots + b_{n-1}x^{n-1}) + f(\alpha) =$$
$$\underbrace{(f(\alpha) - \alpha b_0)}_{\shortparallel\, a_0} + \underbrace{(b_0 - \alpha b_1)}_{\shortparallel\, a_1} x + \underbrace{(b_1 - \alpha b_2)}_{\shortparallel\, a_2} x^2 + \cdots + \underbrace{(b_{n-2} - \alpha b_{n-1})}_{\shortparallel\, a_{n-1}} x^{n-1} + \underbrace{b_{n-1}}_{\shortparallel\, a_n} x^n$$

Приравнявайки коефициентите пред съответните степени на x, получаваме равенствата

$$\begin{array}{r|l} x^n & a_n = b_{n-1} \\ x^{n-1} & a_{n-1} = b_{n-2} - \alpha b_{n-1} \\ \cdots & \cdots\cdots\cdots\cdots\cdots \\ x^1 & a_1 = b_0 - \alpha b_1 \\ x^0 & a_0 = f(\alpha) - \alpha b_0 \end{array} \quad \Rightarrow \quad \begin{cases} b_{n-1} = a_n \\ b_{n-2} = a_{n-1} + \alpha b_{n-1} \\ \cdots\cdots\cdots\cdots\cdots \\ b_0 = a_1 + \alpha b_1 \\ f(\alpha) = a_0 + \alpha b_0 \end{cases} \qquad (*)$$

Равенствата (*) се наричат *правило на Хорнер*. Движейки се отгоре надолу, от тези равенства последователно пресмятаме коефициентите b_{n-1}, $\ldots$, b_0 и най-накрая $f(\alpha)$. Броят на умноженията при пресмятането на $f(\alpha)$ по този начин е n. При непосредственото пресмятане на $f(\alpha)$ умноженията са $\dfrac{n(n+1)}{2}$. Следователно пресмятането на $f(\alpha)$ по правилото на Хорнер е по икономично.