Делимост на полиноми

Определение:
Нека K *е комутативен пръстен и* f(x), g(x) ∈ K[x]. *Казваме, че* f(x) *се дели на* g(x)*(или* g(x) *дели* f(x)*), ако съществува* h(x) ∈ 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) ⇒ f(x) = 0 то нулевият полином дели само себи си

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

Д-во:
От f(x) дели $f_1(x) \Rightarrow f_1(x) = \tilde{f}_1(x).f(x)$
:
От f(x) дели $f_s(x) \Rightarrow f_s(x) = \tilde{f}_s(x).f(x)$
Следователно
$f_1(x).g_1(x) + \ldots + f_s(x).g_s(x) = \tilde{f}_1(x).f(x).g_1(x) + \ldots + \tilde{f}_s(x).f(x)g_s(x) = f(x)(\tilde{f}_1(x).g(x) + \ldots + \tilde{f}_s(x)g_s(x))$
⇒ f(x) дели $f_1(x).g_1(x) + \ldots + f_s(x).g_s(x)$□

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

Д-во:
$(x - \alpha)(x^{n-1} + x^{n-2}\alpha^1 + x^{n-3}\alpha^2 + \ldots + x\alpha^{n-2} + \alpha^{n-1}) =$
$= x^n + x^{n-1}\alpha + x^{n-2}\alpha^2 + \ldots + x^2\alpha^{n-2} + x\alpha^{n-1} - x^{n-1}\alpha - x^{n-2}\alpha^2 - \ldots - x^2\alpha^{n-2} - x\alpha^{n-1} - \alpha^n = x^n - \alpha^n$
$\Rightarrow x^n - \alpha^n$ се дели на (x - α)

Теорема:
Нека K *е комутативен пръстен с единица и* f(x) ∈ K[x]. *За всяко* α ∈ K *съществува* g(x) ∈ K[x]*, такъв, че* f(x) = (x - α)g(x) + f(α).

Д-во:
$f(x) = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n$
$f(\alpha) = a_0 + a_1\alpha + a_2\alpha^2 + \ldots + a_n\alpha^n$
$f(x) - f(\alpha) = a_1(x - \alpha) + a_2(x^2 - \alpha^2) + \ldots + a_n(x^n - \alpha^n)$
Съгласно Твърдение 2 имаме, че всяко събираемо в дясната част на последното равенство се дели на (x-α)
От Твърдение 1 следва, че (x - α) дели f(x) - f(α), т.е. f(x) - f(α) = (x - α)g(x)
⇒ f(x) = (x - α)g(x) + f(α)

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

Д-во:
1) Нека α е корен на f(x), т.е. f(α) = 0
От теорема1 ⇒ f(x) = (x - α)g(x) + f(α) = (x - α) g(x) ⇒ (x - α) дели f(x)
2) Нека (x - α) дели f(x), тогава f(x) = (x - α) g(α)
⇒ f(α) = (α - α) g(α) = 0 ⇒ 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 *е не по-голям от степента на* f(x).

Д-во:
Нека $f(x) \in K[x]$ и е ненулев.
Доказателството ще направим по индукция относно n = ст(f(x)),
База: $n = 0 \Rightarrow f(x) = a_0$, $a_0 \neq 0$ и е ясно, че f(x) няма корени.
База: $n = 1 \Rightarrow f(x) = a_0 + a_1x$, $a_0 \neq 0$
Ако f(x) няма корени, тогава твърдението е вярно. Нека f(x) има корен $\alpha \in K$, т.е. $a_0 + a_1 \alpha = 0$
Допускаме, че $\beta \in K$ също е корен на f(x), т.е. $a_0 + a_1\beta = 0$
$\Rightarrow a_1(\alpha - \beta) = 0$
a_1 не е нула и в K няма делители на нулата, следователно $\alpha - \beta = 0 \Leftrightarrow \alpha = \beta$
$\Rightarrow$ f(x) има не повече от един корен
Нека $n \geq 2$.
Ако f(x) няма корени, тогава твърдението е вярно
Нека f(x) има корен $\alpha \in K$. Тогава $f(x) = (x - \alpha)g(x)$, където $g(x) \in K[x]$
ст $f(x) = n \Rightarrow$ 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 $\Rightarrow g(\beta) = 0$
И така всеки корен на полинома f(x), който е различен от α е корен на g(x). От индуктивната хипотеза броят на различните корени на полинома g(x) не са повече от n – 1. Следователно броят на различните корени на f(x) не е повече от n.

Забележка:
Ако в пръстена има делители на нулата, тогава някои полеоми могат да имат повече корени отколкото е тяхната степен.

Пример:
K е пръстен на квадратните матрици от втори ред.

Полиномът $X^2 - E$ има очевидно следните четири корена

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

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.*

Д-во:
Допускаме, че f(x) и g(x) не са равни в алгебричен смисъл. Това означава, че някой от коефициентите пред съответните степени са различни. Следователно полинома h(x) = f(x)-g(x) има ненулев коефициент и поради това h(x) е ненулев полином. Нека ст.h(x) = n. Избираме $\alpha_1, \ldots, \alpha_{n+1} \in K$ такива, че $\alpha_i \neq \alpha_j$, $i \neq j$. Този избор е възможен, защото $|K| = \infty$. От условието имаме

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

И така, полиномът h(x) има повече корени от колкото е негвата степен, което е противоречие□

Определение:
Нека F *е поле и* $a, b \in F, b \neq 0$.
$\frac{a}{b} =^{def} a.b^{-1}$

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) *такъв, че* ст. $f(x) \leq n-1$ *и* $f(\alpha_i) = y_i$, $i = 1, \ldots, n$

Д-во:
Търсим полинома

$$f(x) = a_0 + a_1x + \ldots + a_{n-1}x^{n-1},$$

От условието имаме
$f(\alpha_1) = a_0 + a_1\alpha_1 + \ldots + a_{n-1}\alpha_1^{n-1} = y_1$
$f(\alpha_2) = a_0 + a_1\alpha_2 + \ldots + a_{n-1}\alpha_2^{n-1} = y_2$
:
$f(\alpha_n) = a_0 + a_1\alpha_n + \ldots + a_{n-1}\alpha_n^{n-1} = y_n$
Тези равенства можем да ги разглеждаме като линейна система относно $a_0, a_1, \ldots, a_{n-1}$, която е квадратна. Детерминантата на тази система е

$$\begin{vmatrix} 1 & \alpha_1 & \ldots & \alpha_1^{n-1} \\ 1 & \alpha_2 & \ldots & \alpha_2^{n-1} \\ \ldots & \ldots & \ldots & \ldots \\ 1 & \alpha_n & \ldots & \alpha_n^{n-1} \end{vmatrix} = \prod_{1 \leq i < j \leq n}(\alpha_i - \alpha_j), \ \alpha_i - \alpha_j \neq 0$$

Тъй като 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. С това доказахме, че полиномът f(x) съществува и е единствен. Изчисляването на коефициентите чрез фолмулите на Крамер не е целесъобразно.

Интерполационна формула на Лагранж

Разглеждаме полинома

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

Ясно е, че степента на този полином не е по-голяма от n-1. Очевидно е, че

$$f(\alpha_1) = y_1 + 0 + \ldots + 0 = y_1$$
$$f(\alpha_2) = 0 + y_2 + \ldots + 0 = y_2$$
:
$$f(\alpha_n) = 0 + 0 + \ldots + y_n = y_n$$

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

Правило на Хорнер

Нека К е комутативен пръстен с единица и $f(x) = a_0 + a_1x + \ldots + a_nx^n \in K[x]$. Ако $\alpha \in K$ трябва да пресметнем $f(\alpha) = ?$. Съгласно Теоремата

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

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

$$f(x) = (x - \alpha)(b0 + b_1x + \ldots + b_{n-1}x^{n-1}) + f(\alpha) =$$
$$= \underset{\|a_0}{(f(\alpha) - \alpha b_0)} + \underset{\|a_1}{(b_0 - \alpha b_1)}x + \underset{\|a_2}{(b_1 - \alpha b_2)}x^2 + \ldots + \underset{\|a_{n-1}}{(b_{n-2} - \alpha b_{n-1})}x^{n-1} + \underset{\|a_n}{b_{n-1}x^n}$$

По този начин получаваме равенствата

$$\begin{cases} a_n = b_{n-1} \\ an-1 = bn-2 - \alpha bn-1 \\ : \\ a_1 = b_0 - \alpha b_1 \\ a_0 = f(\alpha) - \alpha b_0 \end{cases} \Rightarrow \begin{cases} b_{n-1} = a_n \\ b_{n-2} = a_{n-1} + \alpha b_{n-1} \\ : \\ b_0 = a_1 + \alpha b_1 \\ f(\alpha) = a_0 + \alpha b_0 \end{cases} \quad (*)$$

Равенствата (*) се наричат *правило на Хорнер.* От тези равенства последователно пресмятаме коефициентите b_{n-1}, ... , 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 $n(n+1)/2$
Следователно пресмятането на $f(\alpha)$ по правилото на Хорнер е по икономично.