IPMVFMF2025-02-28

$x^p - x \quad \vee \mathbb{Z}_p[x]$

vsi $a \in \mathbb{Z}_p$ so ničle $x^p - x$.

$\Rightarrow \quad x^p - x = x(x-1)(x-2)\cdots(x-(p-1))$

izrek o deljenju: let p in q polinoma $\in K[x]$, K polje (komutativen obseg).

potem $\exists$ polinoma t in $r \in K[x] \ni: p = tq + r$, pri čemer velja $\deg(r) < \deg(q)$, polinoma t in r sta enolično določena

---

Posledica: a ničla polinoma $p \iff$
$\exists k \in K[x] \ni: p = (x-a)k$.

Dokaz: ($\Rightarrow$): vemo: obstaja razcep

$p = (x-a)k + r$, $r \in K$

a ničla $\Rightarrow \quad p(a) = \underbrace{(a-a)}_{0} \cdot k(a) + r \to r = 0$

$p(a) = 0$

($\Leftarrow$) očitno

N

let F polje in $p \in F[x]$ polinom stopnje $n \geq 1$.
pokaži, da ima p največ n ničel.

indukcija po n: ničla obstaja:

BAZA: $n=1$: $p(x)=ax+b=0 \Leftrightarrow x_0 = a^{-1}(-b)$

preverit: je treba, da noben drug element ni ničla.

naj bo $x_1 \neq$ tak, da $x_0 \neq x_1$:

trdimo, da ni ničla.

PODRAA $p(x_1)=0=ax_1+b$

$ax_1+b = ax_0+b$

$x_1 = x_0$ ✗

KORAK: $n \to n+1$:

$p(x) = a_{n+1}x^{n+1} + a_n x^n + \cdots + a_1 x + a_0$

Potrebujemo: želimo, da ima $p(x)$ vsaj $n+1$ ničel.

I.P.: polinom n-te stopnje ima največ n ničel.

Če $p(x)$ ima vsaj ničle, smo trditev dokazali. Če ima ničlo x_0, velja

$p(x_0)=0 \Rightarrow p(x) = (x-x_0)t(x)$

in $\deg(t) = n \xrightarrow{I.P.} t$ ima največ n ničel.

Preverimo še, da je vsaka ničla p, ki ni x_0, nujno ničla polinoma t.

$x_1 \neq x_0$: $p(x_1) = (x_1 - x_0)\,t(x_1)$

$\neq 0$

$\Longrightarrow \quad k(x_1) = 0$ (ker lahko delimo z $x_1 - x_0$)

sklep: p ima največ n-tl ničel

N: poišči polinom $p \in R[x]$ stopnje n z več kot n ničlami. R je kolobar, ne nujno obseg.

$R = \mathbb{Z}_6 \qquad 2 \cdot 3 = 0$

$p(x) = 2x$ stopnja 1

ničle: $0, 3$

kaj pa tak z vodilnim koef 1?:

$(x-3)(x-2) = x^2 - 5x + 6 = x^2 + x$

stopnja: 2

ničle: $2, 3, 0, 5$

Če želimo sklepati, da ima polinom stopnje n največ n ničel, mora biti kolobar dovolj lep — recimo polje

Definicija: polinom $a(x) = a_n x^n + \dots + a_0 \in \mathbb{Z}[x]$ je primitivan $\Leftrightarrow \gcd\{a_0, \dots, a_n\} = 1$

Napomena: Produkt primitivnih polinoma je primitivan!

$$a(x) = a_n x^n + \dots + a_0 \quad \text{primitivan}$$
$$b(x) = b_m x^m + \dots + b_0$$
$$(ab)(x) = a_n b_m x^{n+m} + (a_{n-1} b_m + a_n b_{m-1}) x^{n+m-1} + \dots + (a_0 b_1 + b_0 a_1) x + a_0 b_0$$

Izberimo p praštevilo in dokažimo, da ne deli vsakega koeficienta c.

Izberimo najmanjša indeksa i, j, da p ne deli a_i in p ne deli b_j.

Če skušamo gnide pravi definirajmo

$a_k := 0$ za $k < 0$

$b_k := 0$ za $k > m$

$c_k := 0$ za $k > n+m$

Domnevamo p ne deli $c_{i+j} =$

$= \underbrace{a_0 b_{i+j} + a_1 b_{i+j-1} + \dots +}\ a_i b_j \ \underbrace{+ \dots + a_{i+j} b_0}$

delfiv: s p zavedi $\neq$ | ni deljivo s p | delfiv s p zavedi $\neq$ *

torej p ne deli c_{i+j}. □

Komentar: Hp potrebilo smo posebej, da p ne deli nekega člena $c_k \Rightarrow$
p ne deli $\gcd(c_0, \dots, c_{n+m})$

Def.: polinom $p \in K[x]$ je razcepen $\Leftrightarrow$ lahko ga faktoriziramo v $p = p_1 p_2$, kjer sta p_1, p_2 konstantna.

Def: ireducibilen polinom $p \in K[x]$ je nerazcepen $\Leftrightarrow$ ni razcepen.

Dokaži Gaussovo lemo:
$p \in \mathbb{Z}[x]$ je razcepen v $\mathbb{Z}[x] \Leftrightarrow$ je razcepen v $\mathbb{Q}[x]$.

($\Rightarrow$) trivialno

($\Leftarrow$) Let $p(x) \in \mathbb{Z}[x]$ razcepen v

$\mathbb{Q}[x]$, torej $p(x) = q(x)r(x)$,

$q, r \in \mathbb{Q}[x]$

izberemo lcm vseh imenovalcev za

q in r

$\downarrow \quad \downarrow$

$c_1 \quad c_2$

$$\Rightarrow c_1 c_2 p(x) = \underbrace{c_1 q(x)}_{q'(x)} \underbrace{c_2 r(x)}_{r'(x)}$$

opazimo, da q' in $r' \in \mathbb{Z}[x]$

iz q' in r' in p izpostavimo

njihove GCD-je (vsakega posebej)

$q'(x) = a \cdot q''(x) \qquad r'(x) = b \cdot r''(x)$

$p(x) = d \cdot p''(x)$

opazimo, da so q'', r'' in p'' primitivni.

$$c_1 c_2 d \underbrace{p''}_{\text{primitiven}} = a b \underbrace{q'' r''}_{\text{primitiven}}$$

opazimo, da smo izpostavili gcd iz polinoma na levi / desni strani $\Rightarrow p'' = \pm q'' r''$

$$P = q'' r''$$

$$\pm q'' \cdot d$$