IRMV FMF 2025-03-07

Ugotovi, ali sta dana polinoma nerazcepna v $\mathbb{Q}[x]$.

a) $p(x) = x^4 + 4$

$x^4 = -4$

$x^2 = \pm 2i$

$x_{1,2} = \sqrt{2i}$

$x_{3,4} = \sqrt{-2i}$

$w^2 = 2i \quad x = 0 \quad y = 2 \quad r = 2$

$r^2 e^{i\varphi 2} = 2e^{i\frac{\pi}{2}}$

$x_{1,2} = \pm\sqrt{2}\, e^{i\frac{\pi}{4}} = \pm(1+i)$

$x_{3,4} = \pm(1-i)$

razcep nad $\mathbb{C}$: $(x-(1+i))(x-(-1-i))(x-(1-i))(x-(-1+i)) =$

$= (x^2-(1-i)x-(1+i)x+(1-i)(1+i))(x^2-x(-1-i)$
$-x(-1+i)+(-1-i)(-1+i)) =$

$= (x^2-2x+2)(x^2+2x+2)$

LAŽJE: $x^4+4 = \underbrace{x^4+4x^2+4}_{(x^2+2)^2} \underbrace{-4x^2}_{(2x)^2} =$

$(x^2+2)^2 - (2x)^2$

razlika kvadratov!

$= (x^2-2x+2)(x^2+2x+2)$

identiteta Sophie Germain

b) $p(x) = x^4 - 2x^3 + x + 1$

„rational root test" (izrek o racionalnih ničli)

let $p(x) = a_k x^k + \dots + a_0 \quad a_i \in \mathbb{Z}$.

kdaj je lahko $\frac{m}{n}$ $(\gcd(m,n)=1)$ ničla?

$$0 = a_k \left(\frac{m}{n}\right)^k + \dots + a_1 \frac{m}{n} + a_0 \quad / \cdot n^k$$

$$0 = a_k m^k + a_{k-1} m^{k-1} n + \dots + a_1 m n^{k-1} + a_0 n^k$$

opazimo, da mora n deliti $a_k m^k$ in
da mora m deliti $a_0 n^k$.

ker sta m in n tuji, mora n deliti a_k in
m deliti a_0.

torej $\frac{m}{n}$ je ničla $\Rightarrow m | a_0$ in $n | a_k$.

v našem primeru je $a_k = 1$ in $a_0 = 1$,
torej sta kandidata ± 1:
$p(1) = 1 \neq 0 \quad p(-1) = 3 \neq 0 \Rightarrow$ racionalnih ničel ni.

$\Longrightarrow p(x)$ nima linearnih faktorjev.

ali $\exists$ razcep na ~~kvadratne faktorje~~?

če tak razcep $\exists$, po gaussovi lemi $\exists$ že
v $\mathbb{Z}[x]$, BSS vodilna koeficienta v
razcepu sta 1.

PODRAA $p(x)=(x^2+ax+b)(x^2+cx+d)=$

$$= x^4+cx^3+dx^2+ax^3+acx^2+adx+bx^2+bcx+bd=$$

$$= x^4+x^3(c+a)+x^2(ac+b+d)+x(ad+bc)+bd$$

Primerjamo koeficiente

	če $b=d=1$:	če $b=d=-1$
$a+c=-2$		$-a-c=1 \Rightarrow a+c=-1$
$ac+b+d=0$	$a+c=1$	$a+c=-2$
$ad+bc=1$	$a+c=-2$	$\times$
$bd=1$	$\times$	

tak razcep $\nexists \Rightarrow p(x)$ ni razcepna v $\mathbb{Q}[x]$.

Trditev: eisensteinov kriterij

let $a(x)=a_nx^n+\dots+a_1x+a_0 \in \mathbb{Z}[x]$

tak, da $\exists p$ praštevilo $\ni: p|a_0 \wedge p|a_1 \wedge \dots \wedge p|a_{n-1}$
$\wedge\ p\nmid a_n \wedge p^2 \nmid a_0$.

potem je a nerazcepen nad $\mathbb{Q}[x]$.

Dokaz: PODRAA razcep obstaja.

$a(x)=b(x)c(x)$ $\quad \deg(b)+\deg(c)=\deg(a) \quad \deg(b),\deg(c)\geq 1$

$b(x)=b_kx^k+\dots+b_0 \quad c(x)=c_mx^m+\dots+c_0$

$m+k=n$

oglejmo si koeficiente $a_0=b_0\cdot c_0$.

pogoj $p|a_0 \wedge p^2\nmid a_0$ zagotavlja, da je natanko
eden izmed $\{b_0,c_0\}$ deljiv s p.
BSS $p|b_0 \wedge p\nmid c_0$.

$$a_1 = c_0 b_1 + c_1 \underbrace{b_0}_{p \nmid}$$

$\underbrace{\qquad}_{p \nmid}$

$\underbrace{\qquad}_{p \mid}$

$\underbrace{\quad}_{p \nmid} \Rightarrow p \mid b_1$

dogovori za
$j > k: \; b_j = 0$

$l > m: \; c_l = 0$

$$a_2 = c_0 b_2 + c_1 b_1 + c_2 b_0 \Rightarrow p \mid b_2$$

postopek ponavljamo...

$$a_{n-1} = c_0 b_{n-1} + c_1 b_{n-2} + \dots + c_{n-1} b_0 \Rightarrow p \mid b_{n-1}$$

$$a_n = \underbrace{c_0 \cancel{b_n}}_{0} + \dots + \underbrace{c_1 b_{n-1} + \dots + c_n b_0}_{\text{vsi deljivi s } p}$$

$$\Rightarrow p \mid a_n \quad \cancel{\longrightarrow}$$

b) $\forall n \in \mathbb{N}$ konstruiraj nerazcepen polinom stopnje n nad $\mathbb{Q}$.

$$x^n + 2x^{n-1} + \dots + 2x + 2$$

(izpolnjuje eisensteinov kriterij za $p=2$)

Še en primer: $x^n + 2$

N

Dokaži, da je $q(x) = x^{p-1} + x^{p-2} + \dots + x + 1$ nerazcepen v $\mathbb{Q}[x]$ za vsako praštevilo p.

TRIK:

$$1 + q + \dots + q^{n-1} = S$$
$$q + q^2 + \dots + q^n = qS$$
$$\Rightarrow S - qS = 1 - q^n$$
$$\Rightarrow S = \frac{1-q^n}{1-q}$$

ta argument deluje, ker tolobar polinomov lahko vložimo v obseg ulomkov, ki je v tem primeru ravno obseg $\mathbb{Q}(x)$ vseh racionalnih funkcij v x.

$$q(x) = \sum_{i=0}^{p-1} x^i = \frac{1-x^p}{1-x} = \frac{x^p - 1}{x-1} = \frac{(t+1)^p - 1}{t} =$$

$t = x-1 \quad x = t+1$

$$= \frac{\binom{p}{0} t^p + \binom{p}{1} t^{p-1} + \dots + \cancel{\binom{p}{p} - 1}}{t} =$$

$$= \binom{p}{0} t^{p-1} + \binom{p}{1} t^{p-2} + \dots + \binom{p}{p-1} t^0$$

ta polinom zadošča pogojem eisensteinovega kriterija za $p = p$, torej ni razcepen. $\square$

N

poišči vse nerazcepne polinome stopnje največ 3 v $\mathbb{Z}_2[x]$.

z bruteforce najdemo nerazcepne:

stopnje 1: $x, x+1$

2: x^2+x+1

3: x^3+x+1, x^3+x^2+1

opomba: če ima polinom stopnje 3 razcep, je edina možnost, da razpade na kvadraten in linearen faktor

in s tem ničlo.

opomba: nerazcepne polinome je v splošnem težko najti, obstaja pa vsaj eden vsake stopnje $n \geq 1$.

število nerazcepnih polinomov stopnje n nad $\mathbb{Z}_p$ lahko izračunamo s pomočjo Möbiusove fje:

$$\mu(n) = \begin{cases} 1; & n=1 \\ 0; & n \text{ deljiv s kvadratom nekega praštevila} \\ (-1)^k; & n \text{ produkt } k \text{ različnih praštevil} \end{cases}$$

izrek (gauss): št. nerazc. pol. st. n v $\mathbb{Z}_p[x]$ je

$$N_p(n) = \frac{p-1}{n} \sum_{d \mid n} \mu\left(\frac{n}{d}\right) p^d.$$