IPMV+MF 2025-05-16

V

Izračunaj stopnjo in bazo razširitve $\mathbb{Q}(e^{\frac{2\pi i}{n}})$ nad $\mathbb{Q}$, kjer je $n \in \mathbb{P}$.

izračunati moramo stopnjo min. polinoma števila $a = e^{\frac{2\pi i}{n}}$. $a^n = 1$ $g(a) = 0$. ali je g minimalni polinom?

$g(x) = x^n - 1$: g je razcepen $\rightarrow$ ni ireducibilen polinom

$$x^n - 1 = (x-1)\underbrace{(x^{n-1} + x^{n-2} + \dots + 1)}_{p(x)}$$

in a je ravno ničla $p(x)$.

$p(x)$ je polinom najnižje stopnje, ki ima a.

spomnimo se: po eisensteinu je $p(x)$ ireducibilen (če $n \in \mathbb{P}$)

$$\left[\mathbb{Q}(e^{\frac{2\pi i}{n}} : \mathbb{Q}\right] \Rightarrow p(x) \text{ je min pol. št. } a$$

$\Rightarrow$ stopnja je $n-1$ baza: $1, a, \dots, a^{n-2}$

Opomba: obsegi $\mathbb{Q}(e^{\frac{2\pi i}{n}})$ so zelo pomembni v kriptografiji (imenujejo se ciklotomski obsegi)

Opazimo: $\cos\frac{2\pi}{n}, \sin\frac{2\pi}{n} \in \mathbb{Q}(e^{\frac{2\pi i}{n}})$

Opomba: Ko n ni manjše praštevilo, je stopnja $[\mathbb{Q}(e^{\frac{2\pi i}{n}}) : \mathbb{Q}]$ enaka $\varphi(n)$ (Eulerjeva f-a).

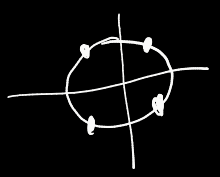
spomnimo se: razpadni obseg polinoma $p \in \mathbb{Q}[x]$ je najmanjši obseg F, $\mathbb{Q} \leq F \leq \mathbb{C}$, ki vsebuje vse ničle polinoma p.

N

Poišči razpadna obsega naslednjih polinomov:

a) $p(x) = x^4 + 1 \in \mathbb{Q}[x]$

ničle: $x^4 = -1$ $\quad x = e^{\frac{\pi i}{4}(1+2k)}$ $\quad k \in \{0,1,2,3\}$



$x_1 = \frac{\sqrt{2}}{2}(1+i)$

$x_2 = \dots$

$\mathbb{Q}(e^{\frac{\pi i}{4}})$ vsebuje 1. ničlo.

$x_0 = e^{\frac{i\pi}{4}}$ $\quad x_1 = (e^{\frac{i\pi}{4}})^3$ $\quad x_2 = (e^{\frac{i\pi}{4}})^5$ $\quad x_3 = (e^{\frac{i\pi}{4}})^7$

<u>Opazimo:</u> Vse ničle so potence x_0

$f = \mathbb{Q}(e^{\frac{i\pi}{8}})$ je razpadni obseg celega polinoma

<u>$\varphi(8) = 4$</u> je stopnja razširitve.

enačenja ffja. alternativno opazimo, da je

$x^4 + 1$ nerazcepen, torej je minimalni polinom za $e^{\frac{i\pi}{4}}$

<u>Opazka:</u> $\mathbb{Q}(e^{\frac{\pi i}{4}}) = \mathbb{Q}(\sqrt{2}, i)$

b) $p(x) = x^3 - 3 \in \mathbb{Q}[x]$ $\quad f = ?$

$x^3 - 3 = 0$

$x^3 = 3$

$x 3 = 3(\cos(0) + i\sin(0))$

$x = 3^3 e^{\frac{2k\pi i}{3}}$ $\quad k \in \{0,1,2\}$

$x_0 = \sqrt[3]{3}$ $\quad x_1 = \sqrt[3]{3}\, e^{\frac{2\pi i}{3}}$ $\quad x_2 = \sqrt[3]{3}\, e^{\frac{4\pi i}{3}}$

oglejmo si: $F_1 = \mathbb{Q}(\sqrt[3]{3})$. ali F_1 vsebuje tudi ost. dve niti? neg $\mathbb{Q}(\sqrt[3]{3}) \subseteq \mathbb{R}$, toda $\operatorname{Im} x_1 \neq 0$.

$$F_2 = \mathbb{Q}\left(\sqrt[3]{3}, e^{\frac{2\pi i}{3}}\right)$$. opazimo, da

F_2 vsebuje vse 3 niste in je po konstrukciji najmanjši tak razširitev obseg polinoma p.

izračunajmo še stopnjo razširitve F_2 nad $\mathbb{Q}$.

produktna formula:

$$[F_2 : \mathbb{Q}] = [F_2 : F_1] \cdot [F_1 : \mathbb{Q}] = 6$$

$$\varphi(3) = 2 \qquad 3, \text{ saj je } p \text{ minimalni polinom števila } \sqrt[3]{3}.$$

ker je ciklotomska razširitev (glej 1. vaja teh vaj).

alt. naloga za doma: min. pol.: $x^2 + x + 1$

Opomba: razširitve obsegov lahko študiramo tudi nad drugimi obsegi, ne le nad $\mathbb{Q}$.

razširitve končnih obsegov so tako up. pomembne za študij polinomov $q \in \mathbb{Z}_p[x]$. razpadni obseg f takega polinoma je neka razširitev $\mathbb{Z}_p$.

[TOPOLOGIJA]

spomnimo se: na $\mathbb{R}^n$ imamo normo

$\|x\| = \|(x_1, \dots, x_n)\| = \sqrt{x_1^2 + \dots + x_n^2}$ in razdaljo oz. metriko:

$d(x,y) = \|x-y\|$

spomnimo se: odprta krogla s središčem v $a \in \mathbb{R}^n$ in radijem $r > 0$ je

$$K(a,r) = \{ x \in \mathbb{R}^n ; \|x-a\| < r \}$$

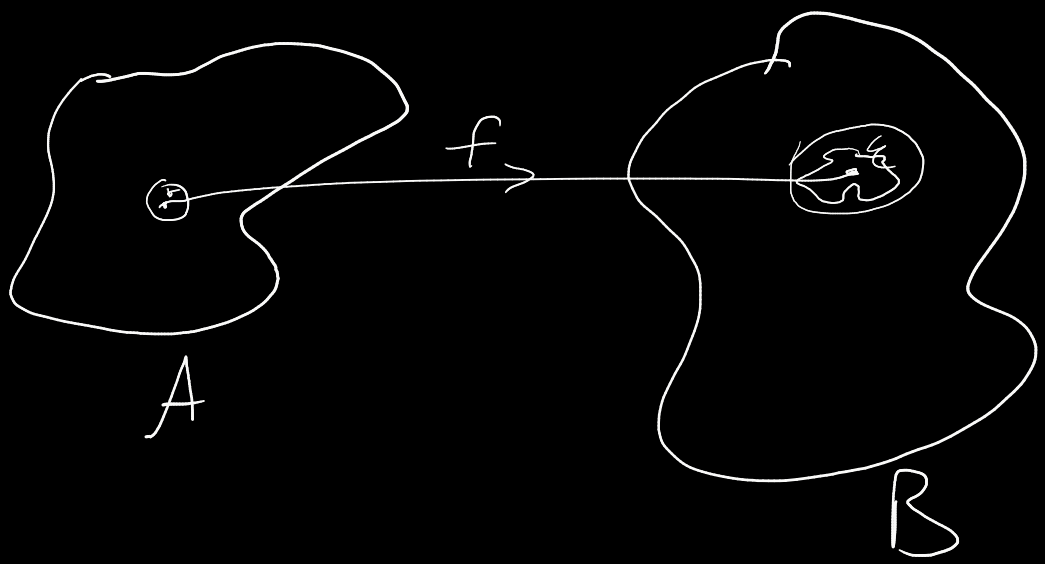
zaprta krogla: $\bar{K}(a,r) = \dots \leq \dots$

Def: Let $A \subseteq \mathbb{R}^n$ in $B \subseteq \mathbb{R}^m$ podmnožici. $f: A \to B$ je zvezna v $a \in A$, če velja $\forall \varepsilon > 0 \exists \gamma > 0 \forall x \in A$:

$$\|x-a\| < \gamma \Rightarrow \|f(x)-f(a)\| < \varepsilon$$

$\S\S$ $\quad$ $\S\S$

$x \in K(a,r)$ $\quad$ $f(x) \in K(f(a), \varepsilon)$



Def: Fja $f: A \to B$ je zvezna, če je zvezna v vseh točkah $a \in A$.

spomnimo se: odprta krogla v A:

$$K_A(a, \dots) = \{ x \in A : \|x-a\| < r \}$$

*Množica $U \subseteq A$ je odprta, če za vsak $a \in U$ obstaja odprta krogla $K(a, r)$: $a \in K(a, r) \subseteq U$

nauk: pojem krogle je odvisen od tega, v katerem prostoru smo.

ekvivalentno definiciji *: $U \subseteq A$ je odprta, če je unija neke družine odp. krogel v A.

opazimo: $f: A \to B$ je zvezna $\Leftrightarrow$ praslika vsake odprte $U \subseteq B$ je odprta $U \subseteq A$.

Def: $f: A \to B$ je homeomorfizem, če je zvezna bijekcija z zveznim inverzom

Def: $A \approx B$ ZOB A homeomorfna $B \Leftrightarrow$ $\exists f: A \to B$ homeomorfizem

pomni: topolog ne razlikuje med homeomorfnimi prostori. TOPOLOGY JOKE

N: ugotovi, ali so dani intervali homeomorfni.

a.) $(0,1) \approx (a, \infty)$

...

naslednjič sem jaz na vrsti