

M. Brašar, Uvod v algebro, osnutek
in novega
učbenika

$(S, \cdot)$ $\cdot$ je binarna operacija na S

namesto $\cdot(a, b)$ pišemo $a \cdot b$

$$S \times S \rightarrow S$$

$\mathbb{Z}$ z operacijama seštevanja in množenja

$A \subseteq \mathbb{Z}$ je zaprta za operacijo $\cdot$ če
 $a, b \in A \Rightarrow a \cdot b \in A$

$$|S| = n$$

Koliko je binarnih operacij

$$n^{nn} = n^{n^2}$$

- je asociativna če

$$\forall a, b, c \in S. (a \cdot b) \cdot c = a \cdot (b \cdot c)$$

Pokaži da $a_1 \cdot \dots \cdot a_n$ neodvisen od oklepajev

Vsplošnem: indukcija

$$\text{Vemo } (a \cdot b) \cdot c = a \cdot (b \cdot c) \text{ za } n=3$$

Trditev drži za $3 \leq k \leq n$ faktorjev

$$n \geq 4$$

Poglejmo si zadjo uporabo operacije

$$\underbrace{(a_1 \cdot \dots \cdot a_l)}_{\substack{\text{postavljen} \\ \text{oklepaji} \\ \text{notri}}} \cdot \underbrace{(a_{l+1} \cdot \dots \cdot a_n)}_{\substack{\text{postavljen} \\ \text{oklepaji notri}}$$

$$1 \leq l \leq n-1$$

Recimo da je $(a_1 \cdot \dots \cdot a_l)$ dolženo v

$a_1(a_2(\dots \cdot a_l))$ in tudi drugi oklepi.

$$\underline{\underline{(a_1(\dots (a_l(a_{l+1}(a_{l+2} \dots a_n))))}} = a_1 \cdot (a_2(a_3 \dots a_n))$$

Polgrupa je množica z asociativno binarno operacijo $(S, \cdot)$

Monad je polgrupa z enoto
 $1 \cdot s = s \cdot 1 = s$ za $\forall s \in S$
(enota mora biti obojestranska)

Element $t \in S$ je levi inverz za s , če
drži $t \cdot s = 1$

Če je l levi inverz za s in
 r desni inverz za s sta enaka

$$ls = 1 = sr$$

$$l = l \cdot 1 = l \cdot (s \cdot r) = (l \cdot s) \cdot r = 1 \cdot r = r$$

Posledica: če ima s inverz, potem je
inverz en sam

Naj bo S končen monoid

Predpostavimo da je $s \in S$ obrnljiv z leve

Dokeži da je S obrnljiv

Vemo: $ts = 1$ za nek $t \in S$

$s, s, s^2, s^3, \dots$ v tem zaporedju so ponavljanje

$$s^n = s^{n+m} \quad m \geq 1$$

$$t^2 \cdot s^2 = \underbrace{t \cdot t \cdot s}_1 s = ts = 1$$

$$\forall n. t^n s^n = 1$$

$$t^n s^n = 1$$

$$t^n s^{n+m} = 1$$

$$(t^n \cdot s^n) \cdot s^m = 1$$

$$1 \cdot s^m = 1$$

$$s^m = 1$$

$$s \cdot (s^{m-1}) = 1$$

s^{m-1} je desni inverz



Navedi primer monoida S in
elementa $s \in S$, ki ima lev: inverz, nima
pa desnega

Navedi vsaj dva ~~trivijalna~~ lažna ~~inverza~~ inverza

Označimo $F(X) = \{f: X \rightarrow X\}$

$F(\mathbb{N})$

$f: n \mapsto 2n$ injektivna, ni surjektivna

$$g = \begin{cases} 2n \mapsto n \\ 2n+1 \mapsto n \end{cases} \quad h = \begin{cases} 2n \mapsto n \\ 2n+1 \mapsto 0 \end{cases}$$

$$f \circ g(x) = f(g(x)) = f(n) = 2n = x \quad \checkmark$$

$$h \circ f(x) = h(2x)$$

ni desnega levega
lažna inverza

$$f: n \mapsto 2n+2$$

Naj bo $(S, \cdot)$ monoid. Ali sta elementa $x, y \in S$ desni in levi inverz, če ~~ne~~, je desni in levi član

a) $x \cdot y \cdot x$

b) $x \cdot y$

a) $x \cdot y \cdot x \cdot f = f \cdot x \cdot y \cdot x = 1$

$x (y \cdot x \cdot f) = (f \cdot x \cdot y) x = 1$

desni in levi inverz

$y \cdot x \cdot f = f \cdot x \cdot y$

$x \cdot y \cdot x \cdot f = x \cdot f \cdot x \cdot y = 1 = f \cdot x \cdot y \cdot x$

$(x \cdot f \cdot x) y = y (f \cdot x \cdot f) = 1$

b) $x \cdot y \cdot f = f \cdot x \cdot y = 1$

Protiprimer

$g: n \mapsto 2n \quad f \circ g = id$

$f: 2n \mapsto n$
 $2n+1 \mapsto 0$

Grupa $(G, \cdot)$ je

1. monoid (asociativnost, enota)

2. $\forall g \in G. \exists g^{-1} \in G. g \cdot g^{-1} = g^{-1} \cdot g = 1$

G grupa, $a, b \in G$

$\forall a, b \in G. ax=b$ in $xa=b$ enolično rešljivi

$a^{-1} / ax=b$

$$x = a^{-1}b$$

$xa=b / a^{-1}$ dve različni enačbi

$$x = ba^{-1}$$

Obratno: Naj bo $(S, \cdot)$ polgrupa

z deljenjem (torej $\forall a, b \in S$ sta enačbi

$ax=b$ in $xa=b$ sta rešljivi)

Pokaži da je S grupa

$ax=b$ vzamemo $b=1$

$ax=1$ $xa=1$

$x=a^{-1}$ a ima levi in desni trej je
obnjljiv. Zp. (jubena

Torej ima inverz

Ampak ni nujno da ima S enoto

Moramo pokazati da ima S enoto

$b=a$

$ax=a$ $xa=a$

$x=1_a$ desna enota

$\forall b: b \cdot 1_a = b$

$b \cdot a = ba \cdot 1_a$

$1_a = x b = by$

$b = z \cdot 1_a = 1_a z$

$$a \circ x = b$$

$$y \circ a = b$$

za $b = a$ je eneka režijski

$$a \circ x = a$$

$$y \circ a = a$$

$x \dots$ desni inverz a

$y \dots$ levi inverz a

$$b = t \circ a \quad b = x \circ a \text{ imerizirani}$$

$$b \circ 1_a = t \circ a \circ 1_a = t \circ a = b$$

1_a je desna enota

$$b = a \circ t \quad \text{ker } b = a \circ x \text{ režijski}$$

$$y \text{ je } 1_a$$

$$1_a \circ b = 1_a \circ a \circ t = a \circ t = b$$

Dokaz: dajmo vsake grupe s štirimi elementi zabeležiti

$$G = \{1, a, b, c\} \quad a \neq b \neq c \neq 1$$

$$\text{Recimo da } ab \neq ba \quad a, b \in G$$

- 1) $ab = 1$ b je desni inverz za a ter je a levi inverz za b torej $ba = 1$
- 2) $ab = a$ $b = 1$ ~~$\times$~~
- 3) $ab = b$ $a = 1$ ~~$\times$~~
- 4) $ab = c$

enako velja za ba

$$\text{torej } ba = c = ab \quad \times$$

Trditelj: $\forall$ grupi: $xy=1$ sled $yx=1$,
 le v abelovi grupi iz
 $xyz=1$ sled: $zyx=1$

$$a) xy=1 \Leftrightarrow y=x^{-1} \Leftrightarrow xy=1$$

$$b) xyz=1 \Rightarrow x^{-1} \cancel{xy} = yz \Rightarrow yzx^{-1} = 1 \\ \Rightarrow zyx^{-1} = 1$$

6 ni abelova, ampak
 $xyz=1 \not\Rightarrow zyx=1$

$$(1\ 2)(2\ 3)(1\ 2\ 3) = (1\ 3\ 2)$$

$$(1\ 2\ 3)(2\ 3)(1\ 2) = \text{id}$$

Dokazi da kjer velja v grupi

a) $\forall x. x^2 = 1$ abelova

b) ~~Enostan~~ $x^2 = a$ je rešiva v vsaki grupi

c) A_3 je res $x^2 = a$ v vsaki grupi največ 2 rešitvi:

d) ~~da~~ A_4 je res $x^2 = ax$ le eno rešitev

d) $x^2 = ax \quad /x^{-1}$
 $x = a$ ima rešitev

a)

$$a, b \in G$$

$$a^2 \circ b^2 = 1$$

$$a \circ b = c$$

$$a \circ (a \circ b) \circ b = 1$$

$$(a \circ b) \circ (a \circ b) = 1$$

$$a \circ (b \circ a) \circ b = 1$$

$$a \circ (a \circ b) \circ b = a \circ (b \circ a) \circ b$$

$$a \circ b = b \circ a \quad \checkmark$$

b) A_4 je $x^2 = a$ rešiva vedno

$$(\mathbb{Z}, +) \quad 2x = a$$

$$2 \cdot 3 = 6$$

$$2x = 3 \quad \text{ni rešitve v } \mathbb{Z}$$

c) $x^2 = a$ največ dve rešitvi?

D_{2n} je grupa rotacij

Vseko zcaljenje za $n \geq 2$ je protiprimer

$\mathbb{Z}_2 \oplus \mathbb{Z}_2$ je tudi protiprimer

Simetrična grupa S_n

$\Pi \in S_n$ je soda oz liha če je produkt sode mnoge transpozicij

$\Pi \in S_n$ zapisano kot produkt disjunktivnih cikla

$$\Pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 4 & 5 & 1 & 2 & 7 & 6 \end{pmatrix}$$

$$(1 \ 3 \ 5 \ 2 \ 4) (6 \ 7)$$

$$(1 \ n)(1 \ n-1) \dots (1 \ 3)(1 \ 2) = \\ = (1 \ 2 \ 3, \dots, n)$$

$$\text{sgn}(\Pi) = (-1)^k \quad k \dots \text{st transpozicij}$$

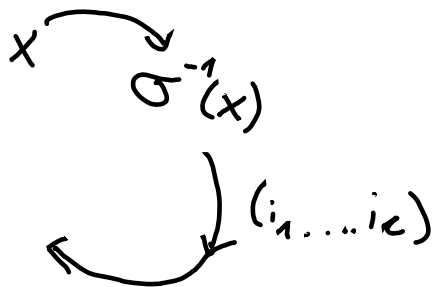
$$\text{če je } \sigma \text{ n-cikel} \Rightarrow \text{sgn}(\sigma) = (-1)^{n-1}$$

Naj bo $\sigma \in S_n$

Potem $\forall k$ -cikla $(i_1, \dots, i_k) \in S_n$

Velja $\underbrace{\sigma(i_1, \dots, i_k) \sigma^{-1}}_{\text{konjugiranje cikla}} = (\sigma(i_1) \dots \sigma(i_k))$

$x \in \{1, \dots, n\}$



$$\begin{aligned} x = \sigma(i_1) \quad & \sigma(i_1, \dots, i_k) \sigma^{-1}(\sigma(i_1)) = \\ & = \sigma(i_1, \dots, i_k) i_1 = \\ & = \sigma(i_2) \end{aligned}$$

Torej se ~~sig~~ $\sigma(i_1) \mapsto \sigma(i_2)$

Torej $(\sigma(i_1) \dots \sigma(i_k))$

Definicija: Permutaciji $\sigma, \sigma' \in S_n$ imata
enako zgradbo disjunktih ciklov
če sta σ in σ' produkta disjunktih
ciklov istih dolžin $k_1, \dots, k_s$ $k_1 \leq k_2 \leq \dots \leq k_s$

npr:

$(123)(456)(78)$ in $(428)(81)(637)$

Dokaži da sta σ in σ' konjugirani:

$\Leftrightarrow$ imata enako ~~sig~~ $\rightarrow$ $\rightarrow$ $\rightarrow$

$$\Rightarrow \sigma' = \pi \sigma \pi^{-1} \text{ za nek } \pi$$

$$\sigma = (i_1 \dots i_k) (\dots) (\dots)$$

$$\sigma' = \pi \sigma \pi^{-1} = (\pi(i_1) \dots \pi(i_k)) (\dots) (\dots)$$

Vidimo da so ~~skl~~: enako dolgi

$\Leftarrow$ Rečimo da

$$\sigma = (i_1 \dots i_k) (j_1 \dots j_k) (\dots)$$

$$\sigma' = (I_1 \dots I_{k_1}) (\dots) \dots$$

Definirajmo π da velja

$$\pi: i_j \mapsto I_j \text{ za } \forall j$$

$$\sigma' = (\pi(i_1) \dots \pi(i_k)) (\dots)$$

$$\text{Vemo torej da } \sigma' = \pi (i_1 \dots i_k) (\dots) \dots \pi^{-1}$$

$$\sigma' = \pi \sigma \pi^{-1}$$

Poišči vse permutacije π , ki komutirajo
z $(1\ 2)$

$$\pi(1\ 2) = \pi(\underline{2\ 1})$$

$$\text{za } n \geq 2$$

$$\pi(1\ 2) = \pi(1\ 2)\pi$$

$$\pi(1\ 2)\pi^{-1} = (1\ 2) = (\pi(1)\ \pi(2))$$

$$\pi(1) = 1 \quad \pi(2) = 2$$

$$\text{ali } \pi(1) = 2 \quad \pi(2) = 1$$

$$\pi_1 = (1\ 2)\sigma$$

$$\pi_2 = \sigma$$

kjer σ ima različne
točke v 1, 2

koliko jih je?

$$2 \cdot (n-2)!$$

$$\{\pi \in S_n; \pi(1\ 2) = (1\ 2)\pi\} = C((1\ 2))$$

centralizator elementa $(1, 2)$

$$C((1\ 2)) = S_2 \oplus S_{n-2}$$

$$\{1, 2\} \quad \{3, \dots, n\}$$

direktna vsota permutacijskih grup

Pokaži, da lahko $\forall \pi \in S_n$ zapišemo kot produkt transpozicij oblike

$$(k, k+1) \text{ kjer}$$

$$1 \leq k \leq n-1$$

$$\pi = (i_1 i_2)(i_3 i_4) \dots \dots \dots (i_{n-1} i_n)$$

Transpozicijo (i_1, i_2) zapišemo preko transpozicij

$$(1 \ 3) = (12)(2 \ 3)(12)$$

$$(1 \ 4) = (12)(2 \ 3)(3 \ 4)(23)(1 \ 2)$$

$$(i \ j)$$

$$j-i > 1$$

$$(i \ j) = (i \ i+1) \dots (i \ j) \dots (i \ j+1)$$

Transpozicije $(k \ k+1)$ generirajo simetrično grupo

3. poglavje

H, K konen: podgrupi grupe G

Pokaži $|HK| = \frac{|H||K|}{|H \cap K|}$

$$HK = \{h \cdot k; h \in H, k \in K\} = \bigcup_{h \in H} hK$$

$$|hK| = |K|$$

Recimo da imamo modsekov

$$|HK| = m|K|$$

$$h_1 K = h_2 K \Leftrightarrow h_2^{-1} h_1 \in K \Leftrightarrow$$

$$h_2^{-1} h_1 \in K \cap H$$

$$H \cap K \leq H$$

koliko je odsekov $h(H \cap K)$

$$[H : H \cap K] = \frac{|H|}{|H \cap K|} = m$$

$$|HK| = m|K| = \frac{|H| \cdot |K|}{|H \cap K|}$$

Naj bo G končna grupa in $H \leq G$

Pokaži da $\exists a, b \in G. a \notin H, b \notin H, ab \notin H \Leftrightarrow$

$$\Leftrightarrow \frac{2|H| < |G|}{\swarrow}$$

$$2 < \frac{|G|}{|H|} \Leftrightarrow [G:H] \geq 2$$

$\mathcal{F}$. odsekov G po H je vsaj 3

$\Rightarrow$ Recimo da $\exists a, b \in H. a \notin H. b \notin H. ab \notin H$

Prvi odsek je gotovo H

$$eH \Leftrightarrow aH \Leftrightarrow a \in H \quad \times \quad aH \text{ je odsek}$$

$$aH = bH = abH$$

$$aH = abH \Leftrightarrow eH = bH \quad \times$$

Torej manj kot tri razlike

$\Leftarrow$ imamo vsaj tri odseke

$$aH \neq bH \neq H$$

$$b^{-1} \notin H$$

$$a \notin H \quad b^{-1} \notin H \quad \text{in} \quad b^{-1}a \notin H$$

$$a^{-1}H = aH$$

$$a^{-1}k = a^{-1}h$$

$$a^2 = hk^{-1}$$

ciklične grupe

$$\mathbb{Z}_{12} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\} = \langle 1 \rangle$$

red: 0 12 6 4 3 12 2 12 3 4 6 12

Lagrangeev izrek

Red podgrupe deli red grupe

Pokaži: $\mathbb{Z}_n$ vsebuje podgrupo reda k
 $\Leftrightarrow k|n$

taka grupa je ena sama

$$n = k \cdot l$$

$$\langle l \rangle = \{0, l, 2l, \dots, (k-1)l\}$$

Zakaj ni druge podgrupe reda k

$$H < \mathbb{Z}_n \text{ reda } k$$

$$H = \{ \underset{0}{\sum} h_1, \dots, h_k \}$$

$$\text{red}(h_i) | k$$

$$t \in \mathbb{Z}_n, \text{red } t | k \Leftrightarrow tk = 0 \quad \forall \mathbb{Z}_n$$

$$t \text{ o } e_j \quad n | tk$$

$$k \cdot l | tk$$

$$l | t$$

$$t \in \langle l \rangle$$

$$\text{To o } e_j \quad h_i \in \langle l \rangle \quad \text{To o } e_j \quad H = \langle l \rangle$$

Pokaži da je podgrupa ciklične grupe ciklična

$$G = \langle a \rangle$$

1) $\mathbb{Z} = \langle 1 \rangle$ a ima neskončen red

$$2) G = \langle a \rangle ; a^n = 1$$
$$\{1, a, a^2, \dots, a^{n-1}\}$$

$$G = \mathbb{R}_n$$

Podgrupe v $\mathbb{Z}$:

$$\mathbb{Z}, \{0\}, 2\mathbb{Z}, 3\mathbb{Z}, \dots, n\mathbb{Z}$$

$\mathbb{Z}$ nima drugih podgrup $H < \mathbb{Z}$

$$H \neq \{0\}$$

$n > 0$ in n najmanjši pozitiven element H

$$\text{Pokažimo } H = n\mathbb{Z}$$

$$\text{ker } n \in H \Rightarrow n\mathbb{Z} \subseteq H$$

$$k \in H. \quad n|k$$

$d = D(n, k)$ največji skupni delitelj

$$d < n$$

$$d = \alpha n + \beta k$$
$$\alpha \in \mathbb{Z} \quad \beta \in \mathbb{Z}$$

$$d \in H \quad \times$$

Določí red od $k \in \mathbb{Z}_n$

$$0 \leq k \leq n-1$$

$$\begin{array}{ll} \text{red}(0) = 1 & \text{red}(k) \stackrel{r}{=} \text{je najmanjše} \\ \text{red}(1) = n & \text{tako št. da } n \mid rk \end{array}$$

$$g = D(n, k)$$

$$n = g\alpha$$

$$k = g\beta$$

$$g\alpha \mid r g\beta$$

$$D(\alpha, \beta) = 1$$

$$\alpha \mid r\beta$$

$$r = \alpha$$

$$\alpha = \frac{n}{g} = \frac{n}{D(n, k)}$$

Kdaj $k \in \mathbb{Z}_n$ generira $\mathbb{Z}_n$?

Ko sta n, k tuja

$\mathbb{Z}_2 \oplus \mathbb{Z}_3$ ge ciklione

$\mathbb{Z}_2 \oplus \mathbb{Z}_2$ ni ciklione, ker

$(1,1)$ generira celo grupo ^{ima} ^{elementa} reda 4

$$(1,1) = (1,1)$$

$$2(1,1) = (0,2)$$

$$3(1,1) = (1,0)$$

$$4(1,1) = (0,1)$$

$$5(1,1) = (1,2)$$

$$6(1,1) = (0,0)$$

DN: Kde je $\mathbb{Z}_n \oplus \mathbb{Z}_x$ c.kl.ora

Naj bo G neskončna grupa.

Pokaži, da ima G neskončno mnogo podgrup

1) Če ima G element neskončnega reda, potem
ima G podgrupo $H \cong \mathbb{Z}$ in ima neskončno podgrup

2. G nima elementa neskončnega reda

$\langle 1 \rangle$ je podgrupa (enota) je končna

$a \in G - \langle 1 \rangle$

$\langle a \rangle$ je končna

in tako lahko nadaljujemo

2. način

$\forall a \in G \langle a \rangle$

$G = \bigcup_{g \in G} \langle g \rangle$ recimo da je končno mnogo

Potem bi bila G končna unija končnih množic $\times$

Pokaži:

1) $\text{red}(a) = \text{red}(a^{-1})$

2) $\text{red}(a) = \text{red}(bab^{-1})$

3) $\text{red}(ab) = \text{red}(ba)$

4) A: imate u ti grupi: elementi

$a^{-1}b^{-1}$ in $a^{-1}b$ enak red kot ab

1) Recimo da $a^r = 1$ ~~red kleno~~

$a^r = 1$

2) $\forall r \in \mathbb{N}, a^r \neq 1$

$(a^{-1})^r = a^{-r} = (a^r)^{-1} = 1^{-1} = 1$ $(a^{-1})^r \neq 1$

$\text{red}(a^{-1}) \leq \text{red}(a)$

ker: simetrija je to enako

2) $a^r = 1 \quad (bab^{-1})^r =$

$bab^{-1} \cdot bab^{-1} \cdot \dots \cdot bab^{-1} = ba^r b^{-1} =$

$b1b^{-1} = bb^{-1} = 1$

$(bab^{-1})^r = 1 \quad b^{-1} / ba^r b^{-1} = 1 \quad /b$

$a^r = b^{-1}b = 1 \quad \checkmark$

3) $\text{red}(ab) = \text{red}(ba)$

$(ab)^r = 1$

~~$(ba)^r = 1$~~

$ba^{r-1} = a^{-1}b^{-1}$

$abab \dots ab = a(ba)^{r-1}b = 1$

$(ba)^r = bab a \dots ba = (ba)^{r-1}ba =$

$= a^{-1}b^{-1}ba = 1 \quad \checkmark$

$a^{-1}b^{-1} \quad a^{-1}b$ enak red kot ab

$(ab)^{-1} = b^{-1}a^{-1}$

$\text{red}(ab) = \text{red}(ab)^{-1} = \text{red}(b^{-1}a^{-1}) =$

$= \text{red}(a^{-1}b^{-1}) \quad \checkmark$

$\text{red } a^{-1}b \quad (a^{-1}b)^n = (ab)^r$

$\{0, 1, 2\} \mathbb{Z}_3$

$a=2 \quad b=1$

$a+b=0 \quad \text{red}(a+b)=0$

$\text{red}(2-1) = \text{red}(1) = 3$

2^{n-1}

n^2 vseh možnosti, $\frac{n!}{2!}$ lahko zavrže

1, 3 in greš same vase. Večje področje.

Pokaži da je grupa

$(\mathbb{R}^*, \cdot)$ generirane z intervalom

$$A = [2, -1]$$

G je generirane z $A \subseteq G$

da vsak $g \in G$ zapišemo

$$g: a_1^{e_1} \dots a_n^{e_n}$$

$$g = a_1^{\pm 1} a_2^{\pm 1} a_3^{\pm 1} \dots a_n^{\pm 1}$$

$$a_i \in A, e_i = \pm 1$$

$$x, y \in A^2 \Leftrightarrow = [1, 4]$$

$$A^3 = [-8, -1]$$

$$A^{-1} = [-1, -\frac{1}{2}]$$

$$A^{2n} = [1, 2^{2n}]$$

$$A^{-2} = [\frac{1}{4}, 1]$$

$$A^{2n+1} = [-2^{2n-1}, -1]$$

$$A^{-2n} = [\frac{1}{2^{2n}}, 1]$$

$$A^{-2n+1} = [-1, -\frac{1}{2^{2n-1}}]$$

$$a \in \mathbb{R}^*$$

$$\exists n \in \mathbb{N}. k$$

" .

1) Določiti red podgrupe $\leftarrow$ množice generirane z A
 $GL_n(\mathbb{C})$ generirane z matrikama

$$A = \begin{bmatrix} i & 0 \\ 0 & 1 \end{bmatrix} \quad B = \begin{bmatrix} 1 & 0 \\ 0 & \frac{2\pi i}{e^3} \end{bmatrix}$$

2) Opisati podgrupo grupe $GL_2(\mathbb{C})$
 generirane z $A = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$

$$B = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

$$1) \quad A^2 = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix} \quad A^3 = \begin{bmatrix} -i & 0 \\ 0 & 1 \end{bmatrix} \quad A^4 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

$$\text{red}(\{A\}) = 4$$

$$A^{-1} = A^3$$

$$B^3 = 1$$

$$B^{-1} = B^2$$

$$A^k B^m = A^s B^n$$

$$A^{k-s} B^{m-n} = 1$$

Katero iz naslednjih množic so
kolobarji: za običajno seštevanje in
množenje

a) $\left\{ \frac{m}{2n+1} : m, n \in \mathbb{Z} \right\}$

b) $\left\{ \frac{2n+1}{m} : m, n \in \mathbb{Z}, m \neq 0 \right\}$

c) $\{ m+n\sqrt{2} : m, n \in \mathbb{Z} \}$

f) $\{ p+q\sqrt{2} : p, q \in \mathbb{Q} \}$

komutativno ✓ vse

$$\frac{m}{2n+1} + \frac{k}{2c+1} = \frac{m(2c+1) + k(2n+1)}{(2n+1)(2c+1)} =$$

$$= \frac{\dots}{2(2nc+n+c)+1} \quad \checkmark$$

$$\frac{m}{2n+1} \cdot \frac{k}{2c+1} = \frac{mk}{2(2nc+n+c)+1} \quad \checkmark$$

$$\frac{1}{2 \cdot 0 + 1} = 1 \quad \checkmark$$

b) $\frac{\frac{2n+1}{m}}{\frac{2k+1}{c}} = \frac{2nc+c+2km+m}{m \cdot c} = \frac{2n+c}{m} \quad \checkmark$

$$m+n\sqrt{2} + k+c\sqrt{2} = \quad \checkmark$$

$$(m+n\sqrt{2})(k+c\sqrt{2}) = 0+0\sqrt{2} = 0 \quad \checkmark$$

$$= mk + 2cn + \sqrt{2}(nk+mc) \quad \checkmark$$

$$1+0\sqrt{2} = 1 \quad \checkmark$$

X -množica $\mathcal{P}(X)$... potenčna množica

$$A, B \subseteq X$$

$$A+B = (A-B) \cup (B-A)$$

$$A \cdot B = A \cap B$$

a) Pokaži, da je $(\mathcal{P}(X), +, \cdot)$ kolobar

$$\text{Velja: } A^2 = A \text{ za } \forall A$$

$\nwarrow$ idempotent
($\mathcal{P}(X)$ je boolov kolobar, ker je $\forall A \in \mathcal{P}(X)$
idempotent ($A^2 = A$))

b) Pokaži, da je $\forall$ boolov kolobar komutativen
in ima karakteristiko 2.

$$(a+a=0 \text{ za } \forall a)$$

a) notranje operacije očitno

$$A+B = (A-B) \cup (B-A) = (B-A) \cup (A-B) = B+A$$

$$A+\emptyset = (A-\emptyset) \cup (\emptyset-A) = A \cup \emptyset = A \quad \checkmark$$

$$A+A = (A-A) \cup (A-A) = \emptyset \cup \emptyset = \emptyset$$

$$A \cdot X = A \cap X = A$$

$$A(B+C) = A \cap ((B-C) \cup (C-B)) =$$

$$= (A \cap (B-C)) \cup (A \cap (C-B))$$

$$= (A \cap B - A \cap C) \cup (A \cap C - A \cap B) =$$

$$(A \cap B) + (A \cap C) = AB + AC$$

b) Rečimo $a^2 = a$ za $\forall a$ dokaži $a+a=0$
komutativnost

$$(ab)^2 = ab \cdot ab$$

$$(A+B)^2 = A^2 + AB + BA + B^2 =$$

$$A + AB + BA + B = A + B$$

$$AB + BA = 0$$

$$B = A$$

$$AA + AA = 0$$

$$A + A = 0$$

$$AB = -BA$$

$$-BA = BA$$

$$AB = BA$$

idempotent: $X^2 = X$

nilpotent: $X^n = 0$ za nek n

Najbo $A \in M_n(\mathbb{R})$ matrica oblike
 $\begin{bmatrix} c_1 a_1 & c_1 a_2 & \dots & c_1 a_n \\ c_2 a_1 & c_2 a_2 & \dots & c_2 a_n \\ \vdots & \vdots & \ddots & \vdots \\ c_n a_1 & c_n a_2 & \dots & c_n a_n \end{bmatrix}$
 negovec ex. Pokazi da $A^2 = \lambda A$ za nek λ
 Pokazi kak idempotent, ki ni diagonalna
 in ni ~~zaga~~ nilpotent, ki ni tridna

$$A = \begin{bmatrix} c_1 a_1 & c_1 a_2 & \dots & c_1 a_n \\ c_2 a_1 & c_2 a_2 & \dots & c_2 a_n \\ \vdots & \vdots & \ddots & \vdots \\ c_n a_1 & c_n a_2 & \dots & c_n a_n \end{bmatrix} =$$

$$= \begin{bmatrix} c_1 \\ \vdots \\ c_n \end{bmatrix} \cdot [a_1 \dots a_n]$$

$$A^2 = \begin{bmatrix} c_1 \\ \vdots \\ c_n \end{bmatrix} \underbrace{[a_1 \dots a_n] \begin{bmatrix} c_1 \\ \vdots \\ c_n \end{bmatrix}}_{\lambda \in \mathbb{R}} [a_1 \dots a_n]$$

$$= \lambda A$$

$$a_1 c_1 + a_2 c_2 = 1$$

$$1 \cdot 3 + (-2) \cdot 1 = 1$$

$$\begin{bmatrix} 3 \\ 1 \end{bmatrix} [1 \ -2] = \begin{bmatrix} 3 & -6 \\ 1 & -2 \end{bmatrix} = A$$

$$A^2 = \begin{bmatrix} 3 & -6 \\ 1 & -2 \end{bmatrix} \cdot \begin{bmatrix} 3 & -6 \\ 1 & -2 \end{bmatrix} = \begin{bmatrix} 3 & -6 \\ 1 & -2 \end{bmatrix} \quad \checkmark$$

$$c_1 a_1 + a_2 c_2 = 0$$

$$1 \cdot 2 + 2(-1) = 0$$

$$A = \begin{bmatrix} 2 \\ -1 \end{bmatrix} [1 \ 2] = \begin{bmatrix} 2 & 4 \\ -1 & -2 \end{bmatrix}$$

$$A^2 = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

1) x nilpotent kolobirja ~~k~~
 ~~p~~ $\Rightarrow$ da je element $1-x$ obrnljiv

2) $x, y \in K$. $1-xy$ je obrnljiv $\Leftrightarrow 1-yx$ je obrnljiv

1) $x^n = 0$

$$\frac{1}{1-x} = \sum_{n=0}^{\infty} x^n = \sum_{\substack{i=1 \\ \text{inverz}}}^n x^{n_i} =$$

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

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

$$1 - x^n = 1$$

$1-xy$ je obrnljiv $\Rightarrow 1-yx$ je obrnljiv

$$\frac{1}{1-xy} = \sum_{k=0}^{\infty} (xy)^k = 1 + xy + xyxy + \dots$$

$$= 1 + xy + x(yx)y + x(yx)^2y + \dots =$$

$$= 1 + x \left(\underbrace{1 + yx + (yx)^2 + \dots}_{\frac{1}{1-yx}} \right) y$$

$\frac{1}{1-xy}$ je obrnljiv

$$(1-yx) \left(1 + y(1-xy)^{-1}x \right) =$$

$$= (1-yx) + (1-yx)y(1-xy)^{-1}x =$$

$$= (1-yx) + (y(1-xy)^{-1})x - yxy(1-xy)^{-1}x$$

$$= 1 - yx \left(1 + y(1-xy)^{-1}x \right)$$

$$= 1 - y \left(1 + (1-xy)^{-1} - xy(1-xy)^{-1} \right) x =$$

$$= 1 - y \left((1-xy)(1-xy)^{-1} \right) x =$$

$$= 1 - y1x = 1 - yx$$

Algebra nad poljem

$(A, \cdot, +)$ - kolobar

A je vektorski prostor nad F

$$\forall \alpha \in F \quad u, v \in A$$

$$(\alpha u)v = \alpha(uv) = u(\alpha v)$$

Nej bo A končno razsežna algebra

Dokazi:

- Vsek nen ničlen element je bodisi delitelj nič, bodisi obrnljiv
- če ima $a \in A$ levi ali desni inverz je obrnljiv
- če je A obseg je vsaka algebra podobseg

Namig: če je A n -razsežna $\Rightarrow 1, a, \dots, a^{n-1}$ lin odvisni

- ~~Nej bo~~ Naj bo n tak da $a^0, 1, \dots, a^{n-1}$ lin neodvisni in a^n je l. odvisen

$$\lambda_0 + \lambda_1 a + \dots + \lambda_n a^n = 0 \quad \text{z } \lambda_1, \dots, \lambda_n \neq 0$$

gotovo $\lambda_n \neq 0$

$$\lambda_0 \neq 0 \Rightarrow$$

$$1 + \frac{\lambda_1}{\lambda_0} a + \dots + \frac{\lambda_n}{\lambda_0} a^n = 0$$

$$1 + a \left(\frac{\lambda_1}{\lambda_0} + \dots + \frac{\lambda_n}{\lambda_0} a^{n-1} \right) = 0$$

$$a \left(-\frac{\lambda_1}{\lambda_0} - \dots - \frac{\lambda_n}{\lambda_0} a^{n-1} \right) = 1$$

a je obrnljiv

$$\lambda_0 = 0 \Rightarrow$$

$$a \underbrace{(\lambda_1 + \dots + \lambda_n a^{n-1})}_{\neq 0 \text{ (ker } \lambda_n \neq 0)} = 0$$

Torej je a delitelj nič

b) ~~1~~ a ima levi inverz

$$ba=1$$

$$b / \alpha_0 + \alpha_1 a + \dots + \alpha_n a^n = 0$$

$$\alpha_0 b + \alpha_1 ba + \dots + \alpha_n ba^n = 0$$

$$\downarrow / \alpha_0 b + \underbrace{\alpha_1 + \dots + \alpha_n a^{n-1}}_{\text{lin kombinacija}} = 0$$

$$\alpha_0 b^n + \alpha_1 b^{n-1} + \alpha_2 b^{n-2} + \dots + \alpha_n = 0$$

$\alpha_n \neq 0$ po predpostavki.

~~ba~~ $\Rightarrow$ b je obratno prejšnji teži

njegov inverz

$$b^{-1} = \beta_0 + \beta_1 b + \dots + \beta_n b^n$$

$$ba=1 \quad xb=1$$

$$x=a$$

$$\cancel{ba=a} \quad ab=1$$

c) A je $\mathcal{L}_B$
 B podalgebra

Naj $b \in B$; $b \neq 0$: Dokaż: $b^{-1} \in B$

$$b^{-1} = \beta_0 + \underbrace{\beta_1 b}_{\in B} + \dots + \underbrace{\beta_{n-1} b^{n-1}}_{\in B}$$

X množica

$\mathcal{P}: \{ \{x\}^c \mid x \in X \}$ podbaza topologije
končnih komplementov
 $\mathcal{P}_X = \{x\}^c$

$$U \in \mathcal{T}_{KK}$$

$$U = \{a_1, \dots, a_n\}^c$$

$$U = \bigcap_{i=1}^n \mathcal{P}_i$$



$$\mathcal{T}_{KK} \subseteq \mathcal{P}$$

$$\mathcal{P}_X + \mathcal{P}_Y = X \text{ je pokrivenje}$$

$$\mathcal{P} \subseteq \mathcal{T}_{KK}$$

očito

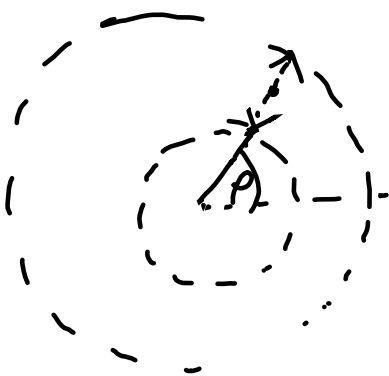
4.6

$$\{(x, y) \in \mathbb{R}^2 ; 1 < x^2 + y^2 < 4\}$$

homeomorfien netivia

Produkt topologisch prosterar

$$(A, \mathcal{T}_A) \times (B, \mathcal{T}_B)$$



$$ae^{p_i} \xrightarrow{1 < a < 4} (f(a), g(p))$$

4.8.

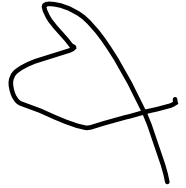
$$(-\infty, 0) \cup [0, \infty) \rightarrow \mathbb{R}$$

$$\text{in}_1(X) \rightarrow X$$

$$\text{in}_2(X) \rightarrow X$$

surj ✓

inj ✓



wezmast:

$$f^*(a, b) = \begin{cases} \text{in}_1^*(a, 0) \cup \text{in}_2^*([0, b]) & \text{if } a < 0 < b \\ \text{in}_1^*(a, b) & \text{if } a, b < 0 \\ \text{in}_2^*(a, b) & \text{if } a, b \geq 0 \end{cases}$$

✓
✓
✓

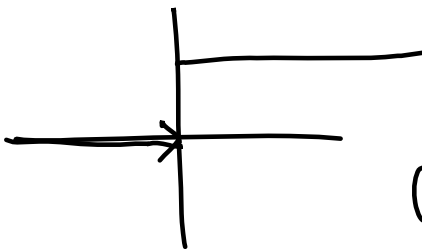
Homeomorfizem?

N: (en je poveren drugi ni

inverz ni wizen

$$\text{in}_2([0, 1]) \mapsto [0, 1]$$

b)



Heaviside funkcija
je zveza

4.9
 V_A подпространство $(X, \mathcal{T}_{\kappa\kappa})$ имеем $\mathcal{T}_{\kappa\kappa}$

$$\mathcal{T}_A = \{ U \cap A ; U \in \mathcal{T}_{\kappa\kappa} \}$$

$$U = \{ a_1, \dots, a_n \}^c \cap A =$$



то A компактен $\dots$ ∞ ∞ ∞

то A некомпактен:

4.10.)

$$N_{dis} \xrightarrow{i} R_{eu}$$

Vseke preslikave iz diskretne topologije
je zvezna

$$i_*(\{n\}) = \{n\} = (n - \frac{1}{2}, n + \frac{1}{2}) \cap \mathbb{N} \quad \checkmark$$

ali slike odprte množice v odprte?

$$i_*(\{1\}) = \{1\} \quad \text{ker } i \text{ ni odprta}$$

Vseke slike so zaprte, ker je
vsaka zaprta množica slike v zaprto

NTSE: naslednje trditve so ekvivalentne

- f je odprta vložitev
- f je odprta zvezna injekcija
- f je vložitev in $f_*(A)$ je odprta

b) $\mathbb{Q} \longrightarrow \mathbb{R}$

$$i_*(\{q\}) = \{q\} \quad n: \text{odprto } \vee \quad \mathbb{Q} = \text{ak}$$

$$\Rightarrow i_m: U \hookrightarrow B_U$$

$\eta \checkmark$

zverzet disk $\rightarrow$ nedisk $\checkmark$

$$i^2 = j^2 = k^2 = -1$$

kwaternioniska
grupe

$$\begin{array}{ll} ij = k & ji = -k \\ jk = i & kj = -i \\ ki = j & ik = -j \end{array}$$

$$\mathbb{H} = \underbrace{\{\alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k \mid \alpha_i \in \mathbb{R}\}}_h$$

$$\bar{h} = \alpha_0 - \alpha_1 i - \alpha_2 j - \alpha_3 k$$

$$h \cdot \bar{h} = \alpha_0^2 + \alpha_1^2 + \alpha_2^2 + \alpha_3^2 = \|h\|^2$$

$$h^{-1} = \frac{\bar{h}}{\|h\|} \quad h \neq 0$$

1) Za katere $h \in H$ je resljiva enačba
 $ix - xi = h$

Poišči vse resitve enačbe $ix - xi = h$

2) Poišči vse resitve enačbe $x^2 - 1 \in H$

3) Pokaži, da za $\forall$ kvaternion dostaja
 $\alpha, \beta \in \mathbb{R}$ da je $h^2 + \alpha h + \beta = 0$

4) Naj bo $h \in H \setminus \mathbb{R}$. Pokaži da je

$$\overline{h}h = 0 \iff \exists x \in H \setminus \mathbb{R} \quad hx \neq xh \quad h^2x = xh^2$$

$$3) h \in H \exists \alpha, \beta \in \mathbb{R}$$

$$h^2 + \alpha h + \beta = 0$$

$$\forall \mathbb{C}: \quad \begin{array}{l} \alpha = -(h + \bar{h}) \\ \beta = h \cdot \bar{h} \end{array} \quad \left. \vphantom{\begin{array}{l} \alpha = -(h + \bar{h}) \\ \beta = h \cdot \bar{h} \end{array}} \right\} \text{vietau izteik}$$

Reins da

$$h^2 - \underbrace{(h + \bar{h})h}_{\in \mathbb{R}} + \underbrace{h \cdot \bar{h}}_{\in \mathbb{R}} = 0$$

$$h^2 - h^2 - \bar{h}h + h \cdot \bar{h} = 0$$

$$h \cdot \bar{h} = \bar{h}h$$

$$\begin{array}{c} \parallel \\ \|h\|^2 = \parallel \bar{h} \|^2 \\ \parallel \\ \|h\|^2 \end{array} \quad \begin{array}{l} \text{Nesdi} \\ \text{d in } \mathbb{R} \end{array}$$



$$4) h \in \mathcal{H} - \mathbb{R}$$

$$h + \bar{h} = 0 \Leftrightarrow \nexists x \exists x. \quad h x \neq x h \\ h^2 x = x h^2$$

$$\Rightarrow h^2 + \alpha h + \beta = 0 \\ -(\underbrace{h + \bar{h}}_{\parallel h \parallel^2}) \quad \parallel h \parallel^2$$

$$h^2 = -\parallel h \parallel^2$$

$$h^2 x = -\parallel h \parallel^2 x = x(-\parallel h \parallel^2) = x h^2 \quad \checkmark$$

Isceemo x, k ne komutirato

$$h = \alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k \quad \text{baze } b \text{ s } \alpha_2 \neq 0$$

$$h i = \alpha_0 j - \alpha_1 + \alpha_2 k - \alpha_3 j$$

$$i h = \alpha_0 i - \alpha_1 - \alpha_2 k + \alpha_3 j$$

$$\alpha_2 k = -\alpha_2 k$$

$$\alpha_2 = 0 \quad \times$$

$$\Leftarrow h x \neq x h$$

$$h^2 x = x h^2 \quad h^2 = -\alpha h + \beta$$

$$\text{Recimo da } \alpha = -(h + \bar{h}) \neq 0 \\ (-\alpha h + \beta) x = x (-\alpha h + \beta)$$

$$-\alpha h x + \beta x = -x \alpha h + x \beta$$

$$\alpha h x = \alpha x h$$

$$h x = \alpha x \quad \times$$

$$\text{Torej } \alpha = 0$$

$$-(h + \bar{h}) = 0$$

$$h + \bar{h} = 0$$

~~7~~

6) Podkolebar generiran z 3: $v \in \mathbb{C}$
 7) $5-6i$ in $2+5i$

6): Zaprto od z sestevanje

$$n3i; \quad n \in \mathbb{Z}$$

$$1 \rightarrow \mathbb{Z} \subseteq \mathbb{C}$$

$$n+k3i; \quad n, k \in \mathbb{Z}$$

$$(n+k3i)^c$$

$$(3i)^2 = -9 \in \mathbb{Z} \quad \checkmark$$

$$A = \{n+k3i; n, k \in \mathbb{Z}\}$$

Torej je podkolebar

7)

$$n(5-6i) = n5 - n6i$$

$$k(2+5i) = 2k + k5i \quad \in \mathbb{C}$$

$$\mathbb{Z} \subseteq \mathbb{C}$$

$$(6i)^c, (5i)^c$$

$$(6i)^2 = -36 \quad (5i)^2 = -25 \in \mathbb{Z} \quad \checkmark$$

$$A = \{n(5-6i); n \in \mathbb{Z}\} \cup \{n(2+5i); n \in \mathbb{Z}\}$$

$$5-6i \quad 2+5i$$

$$\mathbb{Z} \subseteq K \text{ ker } 1 \in K$$

$$-6i \in K \Rightarrow \{n6i\} \subseteq K$$

$$15i \in K \Rightarrow \{n5i\} \subseteq K$$

$$5-6i \in A \quad 3i \in K$$

$$2+5i \in A \quad A \subseteq K$$

$$\text{in } A \text{ je koliko, to je } A \supseteq K$$

$$\text{To je } A = K$$

8) Daloči podalgebra algebre

$M_2(\mathbb{R})$ generirano z metriko

$$A = \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix} \quad B = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$$

$$\begin{bmatrix} n & n \\ 0 & 0 \end{bmatrix} \in K \quad \begin{bmatrix} 0 & 0 \\ 0 & n \end{bmatrix} \in K$$

$$\begin{bmatrix} n & n \\ 0 & k \end{bmatrix} \in K$$

$$\begin{bmatrix} n & 0 \\ 0 & n \end{bmatrix} \stackrel{\leftarrow \text{enke}}{\in K}$$

$$\Rightarrow \begin{bmatrix} 0 & n \\ 0 & 0 \end{bmatrix} \in K \quad \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \in K$$

$$\text{Produkti: } \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \begin{bmatrix} n & k \\ c & l \end{bmatrix} = \begin{bmatrix} an & ak+bl \\ 0 & cl \end{bmatrix} \checkmark$$

1. $\mathbb{R}[x]$ lahko obravnavamo kot aditivno grupo, kolobar, realni vektorski prostor ali pa ne realno algebro

Opisi podgrupo, podkolobar, podprostor in podalgebro $\mathbb{R}[x]$ generirano s polinomi s x^2 in $2x^3$

$$G = \{ nx^2 + 2kx^3 ; n, k \in \mathbb{Z} \}$$

G je grupa

zaprtest za seštevanje in invertiranje

$$\begin{aligned} nx^2 + 2kx^3 - ix^2 - 2jx^3 &= \\ &= (n-i)x^2 + 2(k-j)x^3 \end{aligned}$$

$\Rightarrow G$ je najmanjša grupa, ki vsebuje to

$$K = \{ 0, 1, x^2, x^3, 2x^3, 2x^2, x^2 + 2x^3, \dots \}$$

$$K = \{ \alpha_0 + \alpha_2 x^2 + 2\alpha_3 x^3 + \alpha_4 x^4 + 2\alpha_5 x^5 + \dots ; \alpha_i \in \mathbb{R} \}$$

Ali je kolobar?

- $\cdot$ -podgrupa je
- enota vsebuje
- enota

- zaprtest za množenje ✓

(ker pri lihih potencah je sode kot lihe potence, in pri lihi je 2 torej je pri lihih 2

Brez α_1
ker smo mnogi α_i
niso 0

podprostor (seštevanje + množenje s skalarjem)

$$P = \{ \alpha x^2 + \beta \cdot 2x^3 \} \quad \alpha, \beta \in \mathbb{R} \Rightarrow$$

$$P = \{ \alpha x^2 + \beta x^3 ; \alpha, \beta \in \mathbb{R} \}$$

podalgebra

podkolobar + množenje s skalarjem
 $\alpha k \quad \alpha \in \mathbb{R}$

$$\{ \alpha_0 + \alpha_2 x^2 + 2\alpha_3 x^3 + \dots ; \alpha_0, \alpha_2 \in \mathbb{R} \}$$

$$= \mathbb{R}[x] - \text{lin} \{ x \}$$

je res najmanjša zaradi zaprtesti

5. poglavje

$\varphi: G \longrightarrow H$ je homomorfizem grup,
če φ ohranja operacijo
 $\varphi(gh) = \varphi(g)\varphi(h)$

izomorfizem = homomorfizem + bijekcija
automorfizem = izomorfizem vase

Naj bo $p: G \rightarrow H$ homomorfizem in $a \in G$ ima končen red.

Pokaži, da $\text{red}(p(a)) \mid \text{red}(a)$
 Če je p vložitev (monomorfizem) sta reda enaka.

$$a^n = 1$$

$$p(a^n) = p(1) = 1$$

$$\text{"}$$

$$(p(a))^n \text{ torej } \text{red}(p(a)) \mid n$$

Recimo da je vložitev

Recimo da je injektivna

$$\text{red}(p(a)) = k$$

$$\text{red } a = k \cdot t = n$$

$$a^{k \cdot t} = 1$$

$$p(a^{k \cdot t}) = 1 \quad |\ker p| = 1$$

torej je to edini element z lastnostjo

$$p(x) = 1$$

$$p(a^t)$$

$$p(a^t) = p(a)^k = 1$$

$$a^k = 1$$

$$\text{torej } t = n \quad k = n$$

Nekj ba G grupa in $a \in G$. Pokazi:

1) $\exists \varphi: \mathbb{Z} \rightarrow G$. $\varphi(1) = a$

2) $\exists \varphi: \mathbb{Z}_n \rightarrow G$, da je $\varphi(1) = a$
 $\Leftrightarrow a^n = 1$

3) Noben: izmed grup $(\mathbb{R}^+, \cdot)$, $(\mathbb{R}^*, \cdot)$
in $(\mathbb{C}^*, \cdot)$

$$\varphi(1) = \cancel{a} a$$

$$\varphi(i) = a^i$$

$$\varphi(1+1) = a a = a^2$$

$$\varphi(n) = \varphi(n-1) + \varphi(1) = \varphi(n-1) \cdot a = a^n$$

Predpostavimo $\varphi(n-1) = a^{n-1}$

$\mathbb{Z}_n \rightarrow G$
2) $\varphi(1) = a \Leftrightarrow a^n = 1$

$$\varphi(i) = a^i \Rightarrow$$

$$\varphi(n) = \varphi(0) = 1$$
$$\parallel a^n$$

$$\Leftrightarrow a^n = 1$$

$$a^n = 1 = \varphi(0) = \varphi(n)$$

$$a^n = \varphi(n) = \varphi(1)^n$$

$$(\mathbb{R}^+, \cdot) \not\cong (\mathbb{R}^*, \cdot)$$

$\uparrow$
 $\mathbb{R} - \{0\}$

Resumo de teste isomorfismos

$$\text{red}(a) = n \quad a^n = 1$$

vs: elementos raízes $\{1, -1\}$ imagem nenhuma
 $\vee \mathbb{R}^*$

$$\text{red}(-1) = 2$$

• red elemento se chama n , então
 $\vee \mathbb{R}^+$ n: elemento rede 2

$$\mathbb{Z}_n \subset \mathbb{Z}^*$$

$|a| \neq 1 \Rightarrow$ não tem nenhuma rede

Por fim claram $\text{red} \in \mathbb{N} - \{1, 2\}$

$$i^4 = 1 \quad \text{red}(i) = 4$$

$$\text{Dodano } \mathbb{Z}_6 \not\cong S_3$$

$\uparrow$
 comutativo

$\uparrow$
 elemento inverso

4) Pojasni zakaj endomorfizem
algebre $M_2(\mathbb{R})$ ne more preoblikovati
matrice E_{11} v E_{12} pri čem je
endomorfizem ϕ , da je $\phi(E_{11}) = E_{12}$,

5) Naj bo A ~~matrica~~ ~~matrica~~ ~~matrica~~

$$A = \left\{ \begin{bmatrix} a & b & d \\ 0 & a & c \\ 0 & 0 & a \end{bmatrix} \mid a, b, c, d \in \mathbb{R} \right\}$$

$$A' = \left\{ \begin{bmatrix} a & 0 & 0 \\ b & a & 0 \\ d & c & a \end{bmatrix} \mid a, b, c, d \in \mathbb{R} \right\}$$

Preveri, da sta A in A' izomorfni in

$A \cong A'$. Pokaži, da A ni izomorfna
algebri $M_2(\mathbb{R})$

G

E_{11} je idempotent

Rečnaden je

$$P(E_{11}) = P(E_{11} \cdot E_{11}) = P(E_{11})$$

$$E_{12} \cdot E_{12} \neq 1 \cdot E_{12}$$

$$P(E_{11}) = E_{22}$$

$$P(E_{22}) = E_{11} \text{ zbog idempotentnosti}$$

$$P(E_{12}) =$$

$$\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \quad \text{u ovom primaru}$$

$$\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$$

$$\pi = (12)$$

$$E_{11} \cdot E_{12} = E_{12}$$

$$E_{21} \cdot E_{11} = 0$$

$$P(E_{ij} \cdot E_{kl}) = P(E_{ij}) P(E_{kl})$$

$$\delta_{\pi(j)\pi(k)}$$

$$H < G$$

H je cdivka

$$\forall g \in G \quad gH = Hg \Leftrightarrow gHg^{-1} \in H$$

$$D_8 \quad H_1 = \langle r \rangle$$

$$H_2 = \langle z \rangle$$

$$H_1 \trianglelefteq D_8$$

(kerina indeks 2)

$$[D_8 : H_1] = 2$$

$$(8 : 4 = 2)$$

$$[D_8 : H_2] = 4$$

$$rH_2 = H_2r$$

.....

$$r\{1, z\} = \{r, rz\}$$

$$\{1, z\} \cdot r = \{r, zr\}$$

$$= \{r, r^3z\}$$



$\neq$

Torej H_2 ni cdivka

Podobno v D_{2n}

$H \triangleleft G$ G/H ... kvocientna grupa
 $\downarrow$ množica vseh odsekov

$$g_1 H \cdot g_2 H = (g_1 g_2) H$$

$$(g_1 H)^{-1} = g_1^{-1} H$$

$$\text{enda: } H = 1 \cdot H$$

Naj bo G teka grupa, da je $G/Z(G)$ ciklična

Dokazi da je G abelove grupa

$$(Z(G) = \{g \in G, gh = hg \ \forall h \in G\})$$

$$\text{Naj bo } G/Z(G) = \langle a \rangle$$

$$G/Z(G) = g \cdot Z(G)$$

$$\{ Z(G), aZ(G), a^2Z(G), \dots, \}$$

$\forall$ element lahko zapisemo kot $a^k z$, kjer

$$a^k z \cdot a^n \cdot c = a^k (z a^n) c = \quad z \in Z(G)$$

$$= a^k (a^n z) c = a^{k+n} z \cdot c =$$

$$\in \frac{G}{Z(G)}$$

$$= a^{n+k} \cdot c \cdot z = a^n (a^k c) z = (a^n c) (a^k z)$$

② Naj bo $|G| = 55$. Pokaži

a) $\forall$ prava podgrupa G je ciklična

b) G je bodisi Abelova bodisi $Z(G) = \{1\}$

a) red podgrupe deli red G

red podgrupe je 11 ali 5 ali 1
↓ ciklone ↓ $\{1\}$

$\mathbb{Z}_p$ je ciklična grupa p do izomorfizma
natanko.

Ta je ciklična

b) Denimo da je G ⁿⁱ Abelova. Potem $Z(G) = \{1\}$

Po prvi nalogi kvocient $G/Z(G)$ ni cikličen

Recimo da center ni trivialen

$|Z(G)|$ je lahko 5 ali 1

Potem j $|G/Z(G)| \neq 1$ ali 5

in taka grupa je ciklična, torej *

③ Pojasi, da lahko s3 zamanjamo
s produktom dveh prostev
Ali lahko tudi z 8?

Če imamo $p \cdot q$ ($p \neq q$) potem podobno kot a)
če imamo red p^2 , potem podobno kot pri 2b)

~~$Z(D_8)$~~ $Z(D_8) = \{1, r^2\}$
in D_8 ni abelova

$Z(Q) = \{\pm 1\}$ in Q ni abelova
↑
kvaternionске
 $\{\pm i, \pm j, \pm k, \pm 1\}$

$\{1, r, r^2, r^3\}$
grupa reda 4, ki ni ciklična

N : ciklična, ker nima elementa reda 4

1. izrek o izomorfizmu

$f: G \longrightarrow H$ epimorfizem

Potem velja: $\ker f \triangleleft G$

$$G/\ker f \cong H$$

Naj bo G grupa vseh nekonstantnih
linearnih funkcij

$$G = \{ax+b; a, b \in \mathbb{R}\} \text{ operacija kompozicije}$$

$a \neq 0$

$$(ax+b)(cx+d) = a(cx+d)+b = acx + ad+b$$

enota: x

inverzi

$$ac=1 \quad c=a^{-1}$$

$$ad+b=0 \quad d = -\frac{b}{a} = -ba^{-1}$$

$$a^{-1}x - ba^{-1} \text{ je inverz}$$

$$\text{Označimo } \mathbb{N} = \{x+b; b \in \mathbb{R}\}$$

4) Pokazi, da je $\mathbb{N}$ edinka in $\mathbb{N}/\mathbb{N} \cong \mathbb{R}^*$

$$5) \mathbb{C}^*/\mathbb{R}^* \cong \mathbb{T}$$

$$6) \mathbb{R}^*/\mathbb{R}^+$$

$$\textcircled{4} \quad p: G \longrightarrow \mathbb{R}^*$$

$$p(ax+b) = a$$

p ist homomorphism

$$p((ax+b)(cx+d)) = p(acx+...) = ac$$

$$= p(ax+b) p(cx+d)$$

$$\ker p: p(ax+b) = 1$$

$$\{x+b; b \in \mathbb{R}\}$$

surjektiv: $N = \ker p \triangleleft G$

$$a \in \mathbb{R} \quad p(ax+0) = a$$

$$\textcircled{5} \quad p: \mathbb{C}^* \longrightarrow \mathbb{T} = \{z \in \mathbb{C} \mid |z|=1\}$$

$$p: a e^{i\alpha} \longmapsto e^{i\alpha}$$

surjektiv: $\checkmark$

$$p(z) = \frac{z}{|z|}$$

$$p(a e^{i\alpha} \cdot b e^{i\beta}) = p(ab e^{i(\alpha+\beta)}) =$$

$$= e^{i(\alpha+\beta)} = e^{i\alpha} \cdot e^{i\beta} = p(e^{i\alpha}) \cdot p(e^{i\beta})$$

$$\ker p: e^{i\alpha} = 1$$

$$\alpha = 2\pi k \quad k \in \mathbb{Z}$$

$$\{a e^{i 2\pi k} = a : a \in \mathbb{R}^+\} = \mathbb{R}^+$$

$$G/\mathbb{R}^+ = \mathbb{T}$$

$$\textcircled{6} \quad \frac{\mathbb{R}^*}{\mathbb{R}^+}$$

$$p: \mathbb{R}^* \longrightarrow \{ -1, 1 \}$$

$$p(\mathbb{R}^+) = 1$$

$$p(a) \longmapsto \frac{a}{|a|}$$

$$\ker p = \mathbb{R}^+$$

$$\text{homomorphism: } p(a \cdot b) = \frac{ab}{|ab|} = \frac{a}{|a|} \cdot \frac{b}{|b|}$$

$$= p(a) \cdot p(b) \quad \checkmark$$

surjektiv: $\frac{1}{1} = 1$

$$p(1) = 1 \quad p(-1) = \frac{-1}{|-1|} = -1$$

⑦ Kateri znari je izomorfna grupa U_n / SU_n

⑧ netrivialna podgrupa N grupe T
da je $\pi/N \cong \pi$

⑨ $\mathbb{R}/\mathbb{Z}$

$$U_n = \{ A \in M_n(\mathbb{C}) : A A^H = I \}$$

$$p: U_n \rightarrow \pi$$

$$A \mapsto \det A$$

$$p(A \cdot B) = \det(A \cdot B) = \det A \cdot \det B$$

surjektivnost

$$a = e^{i\varphi} \quad A = \begin{bmatrix} e^{i\varphi} & & 0 \\ & 1 & \\ 0 & & \ddots \\ & & & 1 \end{bmatrix}$$

$$\ker p = \{ A \in U_n : \det A = 1 \} = SU_n$$

$$\textcircled{8} \quad \pi/N = \pi$$

$$p: e^{i\varphi} \mapsto e^{i2\varphi} \quad \text{je homomorfizem}$$

$$\ker p: e^{i2\varphi} = 1 \quad 2\varphi = 0 + 2\pi k \quad 0 + \pi k \quad \ker p = \{1, -1\}$$

$$\textcircled{9} \quad \mathbb{R}/\mathbb{Z} \rightarrow [0, 1)$$

$$\begin{array}{ccc} a, a_1, a_2, \dots & \xrightarrow{\quad} & 0, a_1, \dots \\ n & \xrightarrow{\quad} & e^{i2n\pi} \end{array}$$

$$\begin{array}{ccc} x & \xrightarrow{\quad} & e^{i2x\pi} \\ \mathbb{R}/\mathbb{Z} & \xrightarrow{\quad} & \pi \end{array}$$

$$p(x+y) = e^{i(x+y)} = e^{ix} e^{iy} = p(x) p(y) \quad \checkmark$$

$$\ker p: e^{ix2\pi} = 1$$

$$x2\pi = 2\pi k \quad k \in \mathbb{Z}$$

$$x = k, k \in \mathbb{Z}$$

$$\ker p = \mathbb{Z}$$

Pokaži, da je center enostavnega
kelobnega polja

rebrno komutativnost in drži, vendar

$Z(K)$ je kelobar in je komutativna

$a \in Z(K)$ a komutira z vsim

$$ab = ba \quad \text{za}$$

generiramo aK ideal

$aK = \{a \cdot k \mid k \in K\}$ je ideal

$$a(k+t) = a \cdot k + a \cdot t \quad \checkmark$$

$a \in aK$ torej je aK nenicelni

$\Rightarrow aK = K$ (ker je K enostaven)

$$\exists b. ab = 1 \Rightarrow ba = 1$$

Pokažimo da je $\underline{b} \in Z(K)$

$$k \in K$$

$$k = (ab)k = k(ab) = a(kb)$$

$$bk = b(akb) = kb$$

za poljuben k

$$\Rightarrow p r_1 I = I_1$$

$$a - c \in I_1 \quad a, c \in I_1$$

eneb za I_3

K_1, K_2 kloba in obliki $I_1 \times I_2$ $I_1 \triangleleft K_1$ $I_2 \triangleleft K_2$

$$I_1 \times I_2 = \{(a, b) ; a k_1 = k_1 a ; b k_2 = k_2 b\}$$

aditivna podgrupa

Nej bo $I \triangleleft K_1 \times K_2$

$$(a, b)(c, d) = (ac, bd) = (ca, db) \\ \in I \quad \in K \quad - (cd)(b, a)$$

Torej $a \in I_1$ z nek ideal in
 $b \in I_2$ ker komutirata z vsakim
 elementom

Čeprav se sestavljajo:

$$(a, b)(c, d) \in I$$

$$(a, b) - (c, d) = (a - c, b - d) \in I$$

Opomba: Za grupe oblike to ne
 velja

$$\mathbb{Z}_2 \oplus \mathbb{Z}_2$$

$$\{(0, 0), (1, 1)\} \text{ nima oblike}$$

$$H_1 \oplus H_2$$

$$H_1 \triangleleft \mathbb{Z}_2 \oplus \mathbb{Z}_2 \quad H_2 \triangleleft \mathbb{Z}_2$$

5)

ideali idly $R \times R \times R$
 nZ so ideali tu ni maksimalni
 ker v prostoru neskonco

R idealov nima (razen $R, 0$)

Fig $R \times R$ ^{reducibilni} nima idealov

Fig $(R \times R) \times R$ ^{reducibilni} nima idealov

$$\{0\} \times \{0\} \times \{0\}$$

$$\{0\} \times \{0\} \times R$$

$$\{0\} \times R \times R$$

$$R \times R \times R$$

$$\{0\} \times R \times \{0\}$$

$$R \times \{0\} \times \{0\}$$

$$R \times \{0\} \times R$$

$$R \times R \times \{0\}$$

maximalen

$(g(x)) \dots$ glavn: kolobara $F[x]$

$$(g(x)) = \{ g(x)h(x) \mid h(x) \in F[x] \}$$

Presek in vsota ^{in produkt} idealov (x^2+x) in (x^2-x)
 kolobara $R[x]$ I J

$$I+J = \{ x+y \mid x \in I, y \in J \}$$

$$I+J = \{ \sum_{i=1}^n x_i + y_i \mid x_i \in I, y_i \in J \}$$

① $I \cap J$

$$x(x^2+1) \quad x(x-1)$$

večkratke: preverim drugo in drugo so
 večkratke

$$x(x+1)(x-1)$$

$$I \cdot J = \{ h(x) \cdot (x^2+x) \cdot g(x)(x^2-x) \}$$

$$I \cdot J = \{ h(x)(x^2+x)(x^2-x)g(x) \} \quad I \cdot J \subseteq ((x^2+x)(x^2-x))$$

$$\text{p.j.} \quad h(x)(x^2+x)(x^2-x) \in I \cdot J$$

$I+J$

$$v \geq \quad \begin{matrix} I = (8) \\ J = (6) \end{matrix} \quad I+J = (2)$$

$$I+J = (x)$$

$$I+J \subseteq (x)$$

$$h(x)x(x+1) + g(x)x(x-1) =$$

$$(h(x)(x+1) + g(x)(x-1))x \quad \checkmark$$

$$(x) \subseteq I+J$$

ker je prazen $x \in I+J$

$$\frac{1}{2}(x^2+x) - \frac{1}{2}(x^2-x) = \frac{1}{2}(0+2x) = x$$

$\in I \qquad \in J$

1) Ali ima $\mathbb{C}[x] / (x^2+1)$ delitelje nič

$$\textcircled{b} -11- \quad \mathbb{R}[x] / (x^2+1) \quad -1-$$

6) Ali je izomorfizem $\mathbb{R}[x] / (x^2-1)$?

$$I = (x^2+1) \quad (f(x)) \dots \text{glevni ideal} \\ = \{ p(x) \cdot f(x) ; f(x) \in \mathbb{R}[x] \}$$

odsek: imajo oblik $f(x)+I$

$$f(x)+I = g(x)+I \Leftrightarrow f(x)-g(x) \in I$$

$$h(x) = \underbrace{f(x) \cdot p(x)}_{\in I} + r(x)$$

$$h(x) - r(x) \in I$$

$$h(x)+I = r(x)+I$$

→ stopajmo manjša od 2 (ker x^2+1)

Vseh odsek ima oblik

$$ax+b+I$$

$$(ax+b) - (cx+d) = (a-c)x + (b-d)$$

$$a=c \quad b=d$$

(ker mora biti
vedno več od x^2+1)

$$(ax+b+I)(cx+d+I) = I$$

$$(ax+b)(cx+d)+I = I$$

$$\begin{matrix} a=1 & c=1 \\ b=i & d=-i \end{matrix}$$

→

$$(x+i)(x-i) = x^2+1 \in I \quad \checkmark$$

Torej sta $(x+i)+I$ in $(x-i)+I$ delitelja nič

2) v $\mathbb{R}[x] / (x^2+1)$ ni deliteljev nič

3) Ali je izomorfizem klobazju? Ne ker
ima ta delitelje nič, tisti pa ne

$$(x-1)(x+1) = x^2-1 \in I$$

③ Naj bodo $I_1, \dots, I_s$ ideali: kolobarje K in velja $I_i + I_j = K$ za $\forall i \neq j$

Definirajmo $f: K \rightarrow \frac{K}{I_1} \times \frac{K}{I_2} \times \dots \times \frac{K}{I_s}$

$$f(a) = (a + I_1, \dots, a + I_s)$$

Pokaži da je f epimorfizem in $\ker f = I_1 \cap \dots \cap I_s$

$$\begin{aligned} f(a+b) &= ((a+b) + I_1, \dots, (a+b) + I_s) = \\ &= (a + I_1 + b + I_1, \dots, a + I_s + b + I_s) = \\ &= (a + I_1, \dots, a + I_s) + (b + I_1, \dots, b + I_s) \quad \checkmark \end{aligned}$$

$$f(ab) = (ab + I_1, \dots, ab + I_s) = f(a) \cdot f(b)$$

$$f(1) = (1 + I_1, \dots, 1 + I_s) =$$

surjektivnost

$(a + I_1, \dots, a + I_s)$ poljuben element

$$a_i - a \in I_i \quad \forall i$$

Davaj, je potrebno da $\exists a_i$ da $(0, \dots, a_i + I_i, \dots, 0)$ leži v $\ker f$. Preverimo, da $(0, \dots, 1 + I_i, \dots, 0)$ leži v $\ker f$

$$a \in I_j \quad i \neq j$$

$$\forall i \quad I_i + I_j = K \quad \forall i \neq j$$

$$1 = a_1 = a_2 + b_2 = a_3 + b_3 = \dots = a_s + b_s \quad \begin{matrix} a_i \in I_i \\ b_i \in I_i \end{matrix}$$

$$1 = (a_2 + b_2) \cdot \dots \cdot (a_s + b_s) =$$

$$a_2 a_3 \dots a_s + \dots + \underbrace{b_2 b_3 \dots b_s}_{\text{cdim del ki nima nobene delilnice iz } I_1}$$

$$1 + I_1 = b_2 b_3 \dots b_s + I_1$$

$$f(b_2 \dots b_s) = (1 + I_1, \dots, 0 + I_2, \dots, 0 + I_s)$$

$$A \in \ker f \Leftrightarrow a \in I_1 \cap I_2 \cap \dots \cap I_s$$

$$\text{torej } a \in I_1 \cap I_2 \cap I_s \dots$$

④ Kitajski izrek o ostankih)

Naj, bodo $n_1, \dots, n_s$ parna tuja
cela števila. Potem da za
p-jubne cela števila $a_1, \dots, a_s \exists$ celo
število a , za katero drži

$$a \equiv a_i \pmod{n_i} \text{ za } \forall i$$

Ker če je $b \equiv a \pmod{n_i} \Rightarrow n_i \mid (a-b)$

Poišči ~~$x \in \mathbb{Z}$ da velja~~

$x \in \mathbb{Z}$ da velja

$$x \equiv 2 \pmod{3}$$

$$x \equiv 1 \pmod{4}$$

$$x \equiv 3 \pmod{7}$$

$x = 17$ je en
rešitev

Naj bo C kolektor vse konvergentnih
realnih zaporedij

in C_0 množica vseh zaporedij z limito 0

Pokaži da je C_0 maksimalni ideal C
in ~~kvocient kolektor~~ $C/C_0 \cong$

⑥ Pokaži, da je kelobar

$\mathbb{R}[x]/(x^2)$ izomorfen kelobarju vseh
 2×2 matrik oblike $\begin{bmatrix} a & b \\ 0 & a \end{bmatrix}$ $a, b \in \mathbb{R}$

Poišči take ideale I in J kelobarja

$K = \left\{ \begin{bmatrix} m & k \\ 0 & n \end{bmatrix} \mid m, n, k \in \mathbb{Z} \right\}$ da je

$$|\frac{K}{I}| = |\frac{K}{J}| = 4 \text{ in } K/I \cong K/J$$

$$\mathbb{R}[x] \rightarrow K$$

$$\ker p = (x^2)$$

$$p(a_0 + a_1 x + a_2 x^2 + \dots + a_n x^n) = \begin{bmatrix} a_0 & a_1 \\ 0 & a_0 \end{bmatrix}$$

~~$$a_1: \begin{bmatrix} a_1 & a_0 \\ 0 & a_1 \end{bmatrix}$$~~

$$\begin{aligned} & p(a_0 + a_1 x + \dots + a_n x^n) \cdot (b_0 + b_1 x + \dots + b_n x^n) = \\ & = p(a_0 b_0 + x(a_0 b_1 + b_0 a_1) + \dots) = \end{aligned}$$

$$\begin{bmatrix} a_0 b_0 & a_0 b_1 + b_0 a_1 \\ & a_0 b_0 \end{bmatrix}$$

$$\begin{bmatrix} a_0 & a_1 \\ 0 & a_0 \end{bmatrix} \begin{bmatrix} b_0 & b_1 \\ 0 & b_0 \end{bmatrix} = \begin{bmatrix} a_0 b_0 & a_1 b_0 + a_0 b_1 \\ 0 & a_0 b_0 \end{bmatrix} \checkmark$$

zastave: a_0 b_1 + b_0 a_1

$$\text{surjektivnost } \begin{bmatrix} a & b \\ 0 & a \end{bmatrix} = p(a + bx) \checkmark$$

$$\ker p: \begin{bmatrix} 0 & 0 \\ c & 0 \end{bmatrix} = p(0 + 0 + x^2 \frac{c}{1}) =$$

$$p(1) = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \checkmark$$

$$\begin{bmatrix} m & k \\ 0 & n \end{bmatrix} \quad m, k, n \in \mathbb{Z}$$

$$\frac{K}{I} \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$$

$$p\left(\begin{bmatrix} m & k \\ 0 & n \end{bmatrix}\right) = (\cancel{m}, \cancel{n}) \quad (m \pmod{2}, n \pmod{2})$$

$$p\left(\begin{bmatrix} m & k \\ 0 & n \end{bmatrix} \begin{bmatrix} a & b \\ 0 & c \end{bmatrix}\right) = p\left(\begin{bmatrix} m & k & \dots & \dots \\ 0 & n & c \end{bmatrix}\right) =$$

$$(\underbrace{mk}_{\text{odd}}, \underbrace{nc}_{\text{odd}}) = (\underbrace{m}_{\text{odd}}, \underbrace{n}_{\text{odd}}) \cdot (\underbrace{a}_{\text{odd}}, \underbrace{c}_{\text{odd}})$$

$$\ker p: \begin{bmatrix} 0 + \mathbb{Z}_2 & k \\ 0 & 0 + \mathbb{Z}_2 \end{bmatrix} = (0, 0) \quad \checkmark$$

$$p\left(\begin{bmatrix} m & k \\ 0 & n \end{bmatrix}\right) = m \pmod{4}$$

$$\ker p = \begin{bmatrix} \mathbb{Z}_4 & \mathbb{Z} \\ 0 & n \end{bmatrix}$$

$$K, H \leq G$$

$$H \trianglelefteq G \text{ in } K \trianglelefteq H$$

$$K \trianglelefteq H \trianglelefteq G$$

$$A_i, j \in K \leq G$$

$$G = A_4 = \{ 1, (1,2)(3,4), (13)(2,4), \dots \}$$

Podgrupa $N \trianglelefteq G$ je karakteristična, če
 $\varphi(N) \subseteq N$ za $\forall \varphi \in \text{Aut}(G)$

karakteristična grupa je edinka

Pokaži:

- a) $\{1, -1, i, -i\}$ je edinka, ni pa karakteristična
- b) $\forall G \neq \{1\}$. $G \times \{1\} \triangleleft G \times G$ ni pa karakteristična podgrupa
- c) $Z(G)$ je karakteristična podgrupa
- d) $K \leq^{\text{kr}} G$ $H \leq^{\text{kr}} G$ potem je $KH \leq^{\text{kr}} G$

① $G \dots p$ -grupa

$H \dots 2$ -grupa

$p \neq 2$ prostevili

G in H sta ciklični; $\Leftrightarrow G \oplus H$ ciklična

$$\Rightarrow \begin{array}{ll} |G| = p^k & G \cong \mathbb{Z}_{p^k} \\ |H| = 2^n & H \cong \mathbb{Z}_{2^n} \end{array}$$

$$G \oplus H \cong \mathbb{Z}_{p^k} \oplus \mathbb{Z}_{2^n} = \mathbb{Z}_{p^k \cdot 2^n}$$

ker sta p^k in 2^n tuji

$\Leftarrow G \oplus H$ ciklična, torej je abelova

$\Rightarrow G$ in H sta tudi abelovi

$$|G \oplus H| = p^s \cdot 2^t \quad \begin{array}{c} G' \\ \hline \end{array} \quad \begin{array}{c} H' \\ \hline \end{array}$$

$$G \oplus H \cong \underbrace{\mathbb{Z}_{p^{a_1}} \oplus \dots \oplus \mathbb{Z}_{p^{a_k}}}_{G'} \oplus \underbrace{\mathbb{Z}_{2^{b_1}} \oplus \dots \oplus \mathbb{Z}_{2^{b_l}}}_{H'}$$

$$G \oplus H \ni a \quad \text{red } a = p^s \cdot 2^t$$

$$G' \ni a'_s \quad \text{red } a'_s = s \quad \wedge \quad H' \ni a'_t \quad \text{red } a'_t = t$$

tudi enoličnost razvoja $G \oplus H$

zaključimo da $G \cong G'$ in $H \cong H'$

② Pokaži: končna abelova grupa je ciklična $\Leftrightarrow \forall p \in \mathbb{P}. p \mid |G| \Rightarrow$
 G vsebuje $n-1$ elementov reda p

$(\Rightarrow) G$ je ciklična $G = \langle a \rangle$
 $|G| = n$

$$G = \mathbb{Z}_{p_1^{\alpha_1}} \oplus \dots \mathbb{Z}_{p_1^{\alpha_k}} \oplus \dots \oplus \mathbb{Z}_{p_s^{\beta_1}} \oplus \dots \oplus \mathbb{Z}_{p_s^{\beta_m}}$$

G je ciklična $\Leftrightarrow k=1, \dots, m=1$

$$G \cong \mathbb{Z}_{p_1^{\alpha_1}} \oplus \mathbb{Z}_{p_2^{\alpha_2}} \oplus \dots \mathbb{Z}_{p_s^{\alpha_s}}$$

$$|G| = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_s^{\alpha_s}$$

$(a_1, 0, \dots, 0)$ ima red p_1

BŠZS: $p = p_1$

Dokažimo: G ima $p-1$ elementov reda p

$\forall \mathbb{Z}_{p^{\alpha}}$ element reda p :

$$p^{\alpha-1}, 2 \cdot p^{\alpha-1}, \dots, (p-1)p^{\alpha-1}$$

$$\Rightarrow p-1 \text{ elementov reda } p$$

$(\Leftarrow)$

$$G = \mathbb{Z}_{p_1^{\alpha_1}} \oplus \dots \mathbb{Z}_{p_1^{\alpha_k}} \oplus \dots \oplus \mathbb{Z}_{p_s^{\beta_1}} \oplus \dots$$

ker je končna abelova grupa

$\rightarrow p-1$ elementov reda p

Pokaži: morajo biti $k=1$

Rečimo da $k \neq 1$

$$\mathbb{Z}_{p_1^{\alpha_1}} \oplus \dots \mathbb{Z}_{p_1^{\alpha_k}}$$

$\uparrow$
 $p^{\alpha_1-1}, 2p^{\alpha_1-1}, \dots, (p-1)p^{\alpha_1-1}$ imajo red p
 $\rightarrow p^{\alpha_k-1}, \dots, (p-1)p^{\alpha_k-1}$ imajo red p

Torej ima vsaj $2(p-1)$ elementov reda p

Torej $k=1$ torej za vse $\times$

$$\text{Torej je } G = \mathbb{Z}_{p_1^{\alpha_1}} \oplus \dots \oplus \mathbb{Z}_{p_s^{\alpha_s}}$$

Torej je ciklična

③ Naj bo G končna abelova grupa
in $|G|=n$. Pokaži $\forall m, m|n$.

G ima podgrupo reda m

④ Naj bo $G = A_n$. Pokaži da G nima
podgrupe reda 6

Rečimo da $|G|=200$ abelova

Pokaži: G ima podgrupo reda 20

$$\begin{array}{r|l} 200 & 2 \\ 100 & 2 \\ 50 & 2 \\ 25 & 5 \\ 5 & 5 \end{array}$$

$$200 = 2^3 \cdot 5^2$$

$$20 = 2^2 \cdot 5$$

$$G = \underbrace{G_1}_{\text{red } 8} \oplus \underbrace{G_2}_{\text{red } 25}$$

$$H = \underbrace{H_1}_{\text{red } 4} \oplus \underbrace{H_2}_{\text{red } 5}$$

Dovolj je pokazati: G_1 ima podgrupo

H_1 reda 4 in G_2 ima podgrupo H_2 reda 5

vs možnosti:

$$G_1 = \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \rightsquigarrow (\{0\}, \mathbb{Z}_2, \mathbb{Z}_2)$$

$$G_1 = \mathbb{Z}_4 \oplus \mathbb{Z}_2 \rightsquigarrow (\mathbb{Z}_4, \{0\})$$

$$G_1 = \mathbb{Z}_8 \rightsquigarrow 2 \cdot \mathbb{Z}_8$$

Podobno za G_2

Naj bo m m/n poljuben

$$G = \mathbb{Z}_{p_1^{\alpha_1}} \oplus \dots \mathbb{Z}_{p_1^{\alpha_k}} \oplus \dots \oplus \mathbb{Z}_{p_s^{\alpha_1}} \oplus \dots \mathbb{Z}_{p_s^{\alpha_m}}$$

$$m = p_{i_1}^{j_1} \dots p_{i_c}^{j_c}$$

B SZS: $p_{i_1} \dots p_{i_c} = p_1 \dots p_c$

$\mathbb{Z}_{p^{\alpha}}$ ima podgrupo $\mathbb{Z}_{p^j}$ $j \leq \alpha$

$$\mathbb{Z}_{p^{\alpha}} = \mathbb{Z}_{p^{\alpha_1}} \oplus \mathbb{Z}_{p^{\alpha_2}} \oplus \dots \mathbb{Z}_{p^{\alpha_k}}$$

$$p^{\alpha_1 + \alpha_2 + \dots + \alpha_k} = p^{\alpha}$$

$$\Rightarrow \alpha_1 + \alpha_2 + \dots + \alpha_k = \alpha$$

pa velikosti

Naj bo $a = p^{\alpha-j}$

Potem je

$$p^{\alpha-j} \mathbb{Z}_{p^{\alpha_1}} \oplus \mathbb{Z}_{p^{\alpha_2}} \oplus \dots \mathbb{Z}_{p^{\alpha_k}}$$

reda

$$p^j$$

$$= \alpha_1 - \alpha + j + \alpha_2 + \dots + \alpha_k = \alpha - \alpha + j = j$$

2. naci 1 za (4)

$H \subset A_4$ podgrupa reda 6

imamo 2 možnosti

1) $H \cong S_3$

2) $H \cong C_6$ ne, ker bi morali imeti A_4 element reda 6

1) $S_3 = \{ (1,2), (2,3), (1,3), (1,2,3), (1,3,2), 1 \}$

$\Rightarrow H = \{ \underbrace{(12)(34)}_A, \underbrace{(13)(24)}_B, \underbrace{(14)(23)}_C \}$

1) $\{A, B, C, 1\}$ je $\subset A_4$, 2 3 cikle, 1²

2) $(1,2)(2,3) \neq (2,3)(1,2)$

ampak $ab = ba \quad ac = ca \quad bc = cb$

$H=6$ in
nima
podgrupe sklenj

⑤ Pokaži da je podgrupa

$B = \langle (1,1), (1,3) \rangle$ grupe $\mathbb{Z} \oplus \mathbb{Z}$

izomorfna grupi $\mathbb{Z} \oplus \mathbb{Z}$

in da je

$$(\mathbb{Z} \oplus \mathbb{Z})/B \cong \mathbb{Z}_2$$

$$\mathbb{Z} \oplus \mathbb{Z} = \langle (1,0), (0,1) \rangle$$

$$(1,3) - (1,1) = (0,2)$$

$$(1,1) - (0,2) = (1,-1)$$

$$(1,1) + (1,-1) = (2,0)$$

$$2\mathbb{Z} \cong \mathbb{Z}$$

$$2\mathbb{Z} \oplus 2\mathbb{Z} = \langle (2,0), (0,2) \rangle$$

$$\cong \langle \mathbb{Z} + \mathbb{Z} \rangle$$

$$\mathbb{Z} \oplus \mathbb{Z} \rightarrow B$$

$$p(1,0) \mapsto (1,1)$$

p si razbiri:

$$p(0,1) \mapsto (1,3)$$

do homomorfizma

$$p(\alpha \cdot (1,0) + \beta \cdot (0,1)) = \alpha(1,1) + \beta(1,3)$$

$$p(\alpha + \beta, \alpha + 3\beta) = (\alpha + \beta, \alpha + 3\beta)$$

$$(\alpha, \alpha) + (\beta, 3\beta) \checkmark$$

p je injektiven

$$p(\alpha, \beta) = (0,0)$$

$$(\alpha + \beta, \alpha + 3\beta) = (0,0)$$

$$\alpha + \beta = 0 \quad \alpha = -\beta$$

$$\alpha + 3\beta = 0$$

$$2\beta = 0$$

$$\beta = 0 \Rightarrow \alpha = 0$$

$\sum_{i=1}^n u_i$

$$\mathbb{Z} \oplus \mathbb{Z}/B \cong \mathbb{Z}_2$$

$$\ker p = B$$

$$p(\alpha, \beta) = (\alpha + \beta) \mod 2$$

je homomorfizem

$$p(1,1) = 0$$

$$p(1,0) = 1$$

$$\ker p = \{ (\alpha, \beta) \mid \alpha + \beta \mod 2 = 0 \}$$

$$C = \{ (\alpha, \beta) \mid \alpha + \beta \mod 2 = 0 \}$$

$$C = B$$

$$B \subseteq C$$

$$\alpha(1,1) + \beta(1,3) =$$

$$(\alpha + \beta, 3\alpha + \beta)$$

$$\alpha + 3\alpha + \beta + \beta = 4\alpha + 2\beta \text{ je sob}$$

$$C \subseteq B$$

$$(a+b) = 2c$$

$$(a,b) \in C \text{ pojava } a+b = 2c$$

$$a = \alpha + \beta$$

$$b = \alpha + 3\beta$$

$$\alpha - b = 2\beta$$

$$\beta = \frac{b-a}{2} \in \mathbb{Z}$$

$$\alpha = a - \frac{b-a}{2} \in \mathbb{Z}$$

obzira reku

⑥ Ponovimo:

elementa σ in $\pi \in S_n$ sta konjugirana
($\sigma: \alpha \pi \alpha^{-1}$ za nek $\alpha \in S_n$)

$\Leftrightarrow \sigma$ in π imata enako ciklično
strukturo (enake št enake dolge cikle)

Cilj: Konjugirani razredi v A_n

Naj bo $\sigma \in A_n$ in $C(\sigma)$ centralizator
 σ v S_n . Pokaži:

1) $C(\sigma) \subseteq A_n \Rightarrow$ konjugirani razred
 σ v S_n razpade na 2 enako
velike razrede v A_n

2) $C(\sigma) \not\subseteq A_n \Rightarrow$ konjugirani razred
 σ v S_n sovpada z razredom σ v A_n

Primeri:

1) id

2) $(12)(34), (14)(23), (13)(24)$
razred v S_4

3) $(123), (132), (124), (142), (134), (143)$
 $(234), (243)$
v A_4 v S_4

1) id

2) $(12)(34), (14)(23), (13)(24)$ je
en razred, ker je liho število

3) Iz predavanj sledi: moč razrede
deli red grupe

Ta razred razpade na 2

Opis konjugirane sheme razrede v S_n in A_n

V A_n imamo k razrede

(id, produkt dveh disjunktih ciklov, ...)

v S_n je

1) id

2) en dvacikel

3) dva dvacikla

4) en tricikel

5) k cikel

② Opisi konjugiranih razred grup
 Q in D_8

"Us bi podvojil število nalog in jo
dal naslednjemu"
- bar

$$Q = \{1, -1, i, -i, j, -j, k, -k\}$$

$$Z(Q) = \{1, -1\} \Rightarrow \{1\}, \{-1\} \text{ sta konjugirani razredi}$$

i : Vemo: moč orbite je enaka indeksu centralizatorja

$$C(i) = \{\pm 1, \pm i\}, \text{ ker imamo že 4 elemente}$$

Torej orbita i je ima 2 elementa

$$|Q \cdot i| = [Q : C(i)] = 2$$

$$i = 1 \cdot i \cdot 1^{-1} \in Q, \quad i \in Q \cdot i$$

$$j \cdot i \cdot j^{-1} = -ijj^{-1} = -i$$

$$\text{Torej } -i \in Q \cdot i \quad Q \cdot i = \{i, -i\}$$

Podobno za vse ostale j in k

$$\text{Torej } Q \cdot j = \{j, -j\} \quad Q \cdot k = \{k, -k\}$$

$$D_8 = \{id, r, r^2, r^3, z, zr, zr^2, zr^3\}$$

$$Z(D_8) = \{id, r^2\} \Rightarrow \{id\}, \{r^2\} \text{ sta razreda}$$

$C(r) = \{id, r, r^2, r^3\}$ to so vsi ker se
bi bila še kaj več bi moralo
biti 8, ampak r ni v centru, torej
ima največ 4

$$\Rightarrow |D_8 \cdot r| = 2$$

$$D_8 \cdot r = \{r, r^3\}$$

$$zr z^{-1} = z z r^3 = r^3$$

$$C(z) = \{id, z, r^2, zr^2\}$$

$$|D_8 \cdot z| = 2$$

$$D_8 \cdot z = \{z, zr^2\}$$

$$r^{-1} z \cdot r = r^3 \cdot r^3 z = r^2 z = zr^2$$

Ostaneta zr in zr^3 ne moreta biti sama
ker če bi bila sama bi bila v centru
 $D_8 \cdot zr = \{zr, zr^3\}$

6) Naj bo $g = (1\ 6\ 9)(2\ 10)(3\ 4\ 5 \rightarrow 8)$
 opišite orbite in stabilizatorje za $\alpha \in S_{10}$
 karavne delovanje grupe $G = \langle g \rangle$ na
 množico $X = \{1, \dots, 10\}$

$$t_j \quad h \cdot x = h(x)$$

$$(4) \quad G \leq GL_n(\mathbb{R})$$

G deluje na $V = \mathbb{R}^n$

za $A \in G$ in $v \in V$

$$A \cdot v = Av$$

Opis orbite tega delovanja, če

a) $G = GL_n(\mathbb{R})$

b) $G = O_n(\mathbb{R})$

c) $G =$ je iz diagonalnih matrik v $GL_n(\mathbb{R})$

d) G je sestavljena iz vseh zgornje trikotnih
obrnjenih matrik

v točkah a) in d) poišči stabilizator vektorja

$$v = \begin{bmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{bmatrix}$$

a) $A \cdot 0 = 0$ za $\forall A \in GL_n(\mathbb{R})$

1) $\{0\}$

Naj bosta v in w nen nična vektorja

Dopolnimo v in w do vsake svoje baze

n. obstoje prehodne matrike da zloži

$$v \quad v \quad w$$

Torej druga orbita je vse ostalo

b) $\{0\}$ orbita

množenje z ortogonalnim ~~o~~ obratne
dolžine tvoj

če sta u in v v isti orbiti morata
imeti isto orbito

namiramo u in v in ju dopolnimo
do ortonormirane baze. ~~to~~

Obstaja prehodna ortogonalna matrika

in preslikava $\frac{u}{\|u\|}$ v $\frac{v}{\|v\|}$ tvoj skalar:

$$u \cdot v = \|u\| \|v\| \cos \angle(u, v) \quad \|u\| = \|v\|$$

$\Rightarrow u$ in v sta v isti orbiti

$\Rightarrow$ ista norma

c) $G = \text{diag}$ n -th matrix

Nej bo $v = \begin{bmatrix} v_1 \\ \vdots \\ v_n \end{bmatrix}$ $A = \begin{bmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_n \end{bmatrix}$

$$A \cdot v = \begin{bmatrix} \lambda_1 v_1 \\ \vdots \\ \lambda_n v_n \end{bmatrix} \text{ torej}$$

ničle so ne istih velikosti kot v
 2^n

d) $\begin{bmatrix} a_{11} & a_{12} \\ 0 & a_{22} \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} x a_{11} + a_{12} y \\ a_{22} y \end{bmatrix}$

$$y = 0 \Rightarrow A y \cdot (y) = 0 \quad \begin{bmatrix} a \in \mathbb{R} \\ 0 \end{bmatrix}$$

$$y \neq 0 \Rightarrow \begin{bmatrix} b \in \mathbb{R} \\ a \in \mathbb{R} \end{bmatrix}$$

dve orbiti:

Podoben se več dimenzij

1) zadnjih $k \neq 0 \Rightarrow \{ \text{vse} \text{ zadnjih } k \text{ } 0 \}$

2) Torej so $n+1$ bit

Burinskaya lemma

$$G \curvearrowright X$$

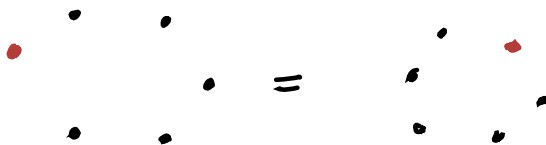
$$\# \text{ orbit: } \frac{1}{|G|} \sum_{g \in G} |g^x|$$

$$g^x = \{x \in X : gx = x\}$$

6 koral in različnih barv

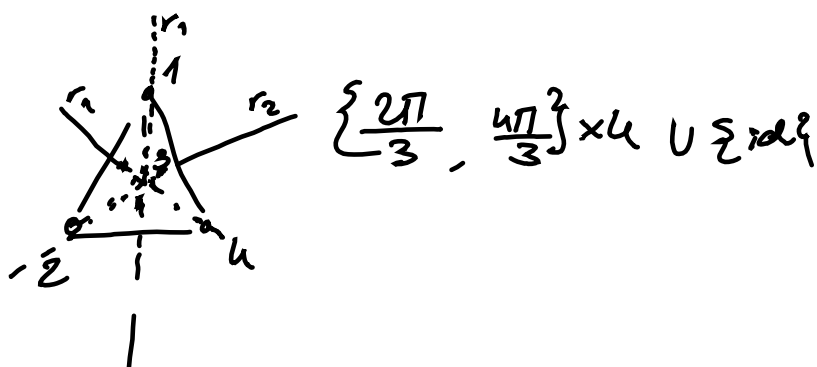
Poišči število ogrlic, ki jih lahko sestavimo.

(ogrlica sta enaki če se do eno prestavi
v drugo z rotacijo ali zrcaljenjem)



③ Na koliko načinov se da pobarvati
lice pravilnega tetraedra z rdečo
modro in zeleno tako da je natanko
eno lice modro

④ Na koliko načinov se da pobarvati
robove pravilnega tetraedra
z rdečo in modro



$$r_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix} = (2 \ 4 \ 3)$$

$$r_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix} = (1 \ 3 \ 4)$$

$$r_1 \cdot r_2 = (2 \ 4 \ 3)(1 \ 3 \ 4) = (1 \ 2 \ 4) = r_3$$

$$z_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} = (1 \ 3)(2 \ 4)$$

$$z_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} = (1 \ 2)(3 \ 4)$$

$$z_3 = (1 \ 4)(2 \ 3)$$

$$A_4$$

$$S_4 \supseteq G \supseteq A_4$$

$$G \neq A_4 \Rightarrow G = S_4 \text{ ker pa ne velja}$$

g	$ G $ neg. ~~točk~~
1 id	$4 \cdot 2^3$
8 $(i \ j \ k)$	$1 \cdot 2$
3 $(ij)(kl)$	0

$$\frac{1}{12} (4 \cdot 2^3 + 8 \cdot 2) = \frac{2}{3} (4 + 2) = 4$$

Izrek: Sylawa

$$|G| = t \cdot p^s \quad p \nmid t \quad p \dots \text{primeslo}$$

p -podgrupa Sylawa je podgrupa moči p^s

$n_p \dots$ število p -podgrup Sylawa

$$n_p \equiv 1 \pmod{p}$$

$$n_p \mid |G|$$

$$n_p \mid t$$

Dokaz: $n_p \mid t$

$$n_p \mid t \cdot p^s$$

$$(n_p, p) = 1$$

$$(n_p, p^s) = 1 \Rightarrow n_p \mid t$$

⑤ Pokaži da ima S_4 4 3-podgrupe Sylowa

⑥ Pokaži da je vsaka 2-podgrupa Sylowa S_4 izomorfna D_8

Navedi vse 2-podgrupe Sylowa in dajmo še nekaj katerih se da ne, pa ne!

$$|S_4| = 24 = 3 \cdot 2^3$$

3 podgrupe Sylowa ma moč 3

2-podgrupa Sylowa ma moč 2

$$n_3 \mid 8 \quad n_3 \equiv 1 \pmod{3}$$

$$n_3 = \{1, 4\}$$

$$n_2 \mid 3$$

$$n_2 \equiv 1 \pmod{2}$$

$$n_2 = \{1, 3\}$$

Velja: $n_p = 1 \Leftrightarrow p$ -podgrupa ~~edinstvena~~ Sylowa
 $J \subset \text{ed. nke}$

$$P_1 = \langle (1, 2, 3) \rangle$$

$$P_2 = \langle (2, 4, 2) \rangle$$

$$P_3 = \langle (1, 3, 4) \rangle \Rightarrow n_3 = 4$$

$$P_4 = \langle (2, 3, 4) \rangle$$

za n_2 :

$$H_1 = \{ (1, 2, 3, 4), (1, 3)(2, 4), (1, 4, 3, 2), \\ (1, 2)(3, 4), (1, 4)(2, 3), (1, 3)(2, 4), \text{id} \}$$

H_1 je 2-podgrupa Sylowa S_4

$$H_2 = \{ (1, 1, 3, 2, 4), (1, 2)(3, 4), (1, 4, 2, 3), (1, 3)(2, 4), \\ (1, 4)(2, 3), (1, 2)(3, 4) \}$$

(vse smo konjugirali z $(2, 3)$)

Dalje: H_3 in element ki konjugira H_1 in H_2

Pomembna uporaba izreka izreka Sylowa: iskanje enost. grup. (Nima drugih edinst.)

Enestavna grupa: nima prvih edist

$$|A_5| = 60$$

A_5 je enestavna

⑦ Pokaži da ^{poljubna} grupa reda n ni enestavna

če:

a) $n = 88$

b) $n = 30$

c) $n = 48$

d) $n = 36$

a) $n = 88 = 2^3 \cdot 11$

$$p_1 = 11 \rightarrow n_{11} = 1 \pmod{11}$$

$$n_{11} | 8 \Rightarrow n_{11} = 1$$

$\Rightarrow$ ker je edine j edinke

b) $n = 30 = 2 \cdot 3 \cdot 5$

$$p_1 = 2 \quad n_2 = 1 \pmod{2}$$

$$n_2 \nmid 15$$

$$n_2 \in \{1, 3, 5\}$$

$$p_3 = 5$$

$$n_5 = 1 \pmod{5}$$

$$n_5 | 6$$

$$n_5 \in \{1, 6\}$$

Recimo da imamo 6 podgrup reda 5

Njihov preseček je samo id

Grej j 24 elementov reda 5

če $n_3 = 10$

Vsej 20 elementov reda 3

$$26 + 24 > 30$$

ali: $n_3 = 1$ ali: $n_5 = 1$

① $H < G$ grupa

$$N_G(H) = \{g \in G : gHg^{-1} = H\} \quad (H \trianglelefteq G \Rightarrow G = N_G(H))$$

$$C_G(H) = \{g \in G : ghg^{-1} = h \text{ za } \forall h \in H\}$$

$$\begin{array}{c} \Updownarrow \\ \text{Pohleži:} \quad gh = hg \end{array}$$

$$N_G(H)/C_G(H) \text{ izomorfna } \text{Aut}(H)$$

$$\text{odnos: } C_G(H) \leq N_G(H)$$

$$p: N_G(H) \longrightarrow \text{Aut}(H)$$

$$g \longmapsto p_g \quad (p_g(h) = ghg^{-1})$$

$$p_{g_1} \circ p_{g_2} = p_{g_1 g_2} \quad \text{odnos}$$

$$\ker p = \{g \in N_G(H), p(g) = 1\} = \underset{\text{id}_H}{\{g \in N_G(H), ghg^{-1} = h\}}$$

$$\{g \in N_G(H) : ghg^{-1} = h\} = C_G(H)$$

$$\frac{N_G(H)}{C_G(H)} \cong \text{im } p \leq \text{Aut}(H)$$

② Najbo $G = \mathbb{H}^*$ (neničeln kvaternioni)

$$H = \{1, -1, i, -i\} < G$$

Dalocí $N_G(H), C_G(H)$ in pdeži:

$$\frac{N_G(H)}{C_G(H)} \cong \mathbb{Z}_2 \cong \text{Aut}(H)$$

$$g^1 g e^1 H$$

$$g(-1)g^{-1} = -1 \in H$$

$$N_G(H) = \{g \in G; g; g^{-1} \in H\}$$

$$g i g^{-1} = 1$$

$$g i = 1 g$$

$$i = 1 \quad *$$

$$g i g^{-1} = i$$

$$g i = i g$$

Torej iščemo centralizatorja

$$g = a + bi + cj + dk$$

$$g i = i g \Leftrightarrow g = a + bi$$

$$g i g^{-1} = -i$$

$$g i = -i g$$

$$a i - b - c j - d k = (a i - b + c j + d k)$$

$$a i - b = -a i + b$$

$$2a i = 2b$$

$$a i = b$$

$$a = b = 0$$

$$g = c k + d j$$

$$g i g^{-1} = i \Rightarrow$$

$$g(-i)g^{-1} = -i$$

$$N_G(H) = \{a + bi; a, b \in \mathbb{R}, a^2 + b^2 \neq 0\} \cup$$

$$\{c j + d k; c, d \in \mathbb{R}, c^2 + d^2 \neq 0\}$$

$$C_G(H) = \{a + bi; a, b \in \mathbb{R}, a^2 + b^2 \neq 0\}$$

$$\text{Aut}(H)$$

$$H \cong \mathbb{Z}_4 \quad H = \langle i \rangle$$

$$\text{Aut}(H) = \{id_H; (i \mapsto -i)\} \quad (\text{zaradi dvojnega reda})$$

$$\text{Aut}(H) \cong \mathbb{Z}_2$$

$$\text{def: } \varphi: N_G(H) \rightarrow \text{Aut}(H)$$

$$g \mapsto (h \mapsto g h g^{-1})$$

$$\text{Ker } \varphi: g \mapsto id_H \Rightarrow h = g h g^{-1} \quad \forall h$$

$$\Leftrightarrow g \in C_G(H)$$

$$\text{za } g = c j + d k$$

$$\text{pden } g \mapsto (i \mapsto (-i))$$

ker ni v centralizatorju, torej ostane

ker ostane

3) Pokaži da grupa reda 48 ne more biti enostavna

4) -||- reda 36 ne more biti enostavna

$$48 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 3 = 2^4 \cdot 3$$

2 podgrupa Sylava ima red 16

3-podgrupa Sylava ima red 3

$n_2 \dots$ št 2-podgrup

$$n_2 \equiv 1 \pmod{2} \quad n_2 \mid 3$$

$$n_2 \in \{1, 3\}$$

če $n_2 = 1$ bi pomenilo da je einka, torej grupa ni enostavna

Recimo da je $n_2 = 3$ torej so 3 take podgrupe

Naj bosta H, K dve podgrupi

$$|H \cap K| = \{1, 2, 4, 8, 16\}$$

$$|HK| = \frac{|H| \cdot |K|}{|H \cap K|} = \frac{16 \cdot 16}{|H \cap K|} \leq 48$$

$$|H \cap K| \geq \frac{16}{3}$$

$$|H \cap K| = 8$$

$$N_G(H \cap K) \leq G$$

$$\frac{H \cap K \triangle H}{H \cap K \triangle K} \Rightarrow H \triangle K$$

$$h x h^{-1} \in H \cap K \Rightarrow h \in N_G(H \cap K)$$

$$H \subseteq N_G(H \cap K)$$

$$K \subseteq N_G(H \cap K)$$

$$|N_G(H \cap K)| \geq |H| + |K| - |H \cap K| = 24$$

$$\text{torej } |N_G(H \cap K)| \in \{24, 48\}$$

Ne sme biti 24, ker polj bi bila edinka (ker indeks 2)

če $|N_G(H \cap K)|$ cele grupe je $H \cap K$ edinka v G

(5) Naj bo G končna grupa $H < G$
 $[G:H] = m$

Pokaži: $|G| \nmid m!$ G ne more biti enostavna

Primeri: —————

$m=3$:

H je indeksa 3

$\Rightarrow G$ ne more biti ciklost

$$|G| = 48$$

H 2-podgrupe Sylow

$$[G:H] = 3$$

G ne more biti enostavna

$$G \cdot H \cong \{gH \mid g \in H\}$$

$$|G \cdot H| = m$$

G deluje na množici odsekov

$$g \cdot hH = ghH$$

(Delovanje je $\rho: G \rightarrow \text{Sym}(G \cdot H)$)

$$\rho: g \mapsto \rho_g(hH) = ghH$$

ρ je homomorfizem

$$G/\ker \rho \cong \text{im } \rho \subseteq \text{Sym}(G \cdot H)$$

$$\ker \rho \triangleleft G$$

$$\ker \rho \notin \{1, G\}$$

$$|\text{im } \rho| \mid m! \leftarrow |G \cdot H| = m$$

||

$$|G/\ker \rho| \quad G = |\text{im } \rho| \cdot |\ker \rho|$$

$$\text{če } |\ker \rho| = 1 \Rightarrow |G| \nmid m! \quad *$$

$$\text{če } |\ker \rho| = |G| \Leftrightarrow$$

$$\rho_g(hH) = hH$$

$$g \neq 1 \Rightarrow \rho_g = \begin{pmatrix} H & h_1H & \dots \\ & gH & \end{pmatrix}$$

$$g \notin H \Rightarrow gH \neq H$$

$$\Rightarrow \rho_g \neq \text{id}$$

$$|G| = 3 \cdot 2^k \quad k \geq 2$$

G ni enostavna

2-podgrupa Sylowa je reda 2^k in
je indeksa 3

H je 2-podgrupa Sylowa

$$[G:H] = 3$$

$$m=3$$

$$k \geq 2 \Rightarrow |G| \geq 12 \Rightarrow |G| \nmid 6!$$

⑦ Naj bo $|G| = 2m$; m liho

Pokaži, da ima G podgrupo indeksa 2 in
zato ne more biti enostavna

izreki Sylowa razdeljujejo:

1. deljeno grupo reda m

$$\text{1. deljeno } f: G \rightarrow \mathbb{Z}_2 \text{ surj} \\ \Rightarrow \ker f \triangleleft G \quad [G: \ker f] = 2$$

$$\text{Cauchy} \Rightarrow \exists a \in G: a^2 = 1$$

$$G \curvearrowright G \text{ s konj. a.t. } \varphi_g(h) = gh$$

$$f: G \rightarrow \text{Sym}(G)$$

$$f(g) = \rho_g \quad \rho_g(h) = gh$$

$$\rho_a(h) = ah \quad \text{Al: je lahko } ah = h \\ \varphi_a(ah) = h$$

$$\Leftrightarrow a = 1 \quad * \text{ ker } a \text{ red } 2$$

ρ_a je produkt transpozicij (zamenjuje dva elementa) in nima negativnih točk $\Rightarrow$ je produkt m transpozicij

$$\text{sgn}(\rho_a) = -1$$

$$G \xrightarrow{f} \text{Sym}(G) \xrightarrow{\text{sgn}} \{1, -1\}$$

kompozitum homomorfizmov

sgn je surjektivna ker id in ρ_a
oblikata 1 oz. -1 razl.

$$\Rightarrow \ker f \triangleleft G \quad [G: \ker f] = 2$$

⑧ p -präst

Koliko različnih p -podgrup Sylowa ima S_p

⑨ Koliko p -podgrup Sylowa ima A_5 če

a) $p=2$

b) $p=3$

c) $p=5$

$$|S_p| = p! = p(p-1)!$$

p podgrupe Sylowa ima red p

$$n_p \equiv 1 \pmod{p} \quad n_p | (p-1)!$$

p podgrupe Sylowa je $\cong \mathbb{Z}_p$

S_p ima $(p-1)!$ p -ciklov

$$\Rightarrow \frac{(p-1)!}{(p-1)} = (p-2)$$

p -podgrupe
Sylowa

Komutatorska grupa rešljive grupe

G , Grupa $A, B \subseteq G$

Označimo $Z[A, B]$ podgenerirano Z

$$[a, b] = a^{-1}b^{-1}ab \text{ gdje } a \in A, b \in B$$

$Z G$ označimo $[G, G]$ - komutatorska podgrupa grupe G

1) Naj bo $H < G$ Pokaži, da je $H \triangleleft G \iff [H, G] \subseteq H$

2) Pokaži, da je $G' \triangleleft G$ in G/G' abelova

3) Naj bo H cinka in G/H abelova.
Pokaži $G' \subseteq H$

$$H \triangleleft G \iff [h, g] \in H \quad \forall g \in G, \forall h \in H$$

$$H \triangleleft G \iff ghg^{-1} \in H \quad \forall g \in G \iff ghg^{-1} \in H \quad \forall g \in G, \forall h \in H$$

($\Rightarrow$)

$$\begin{array}{c} h^{-1}g^{-1}hg \in H \\ \uparrow \quad \underbrace{\hspace{1cm}}_{\in H} \\ \in H \end{array}$$

$$(\Leftarrow) h^{-1}g^{-1}hg \in H$$

$$2) G' \triangleleft G \iff \forall g \in G \quad h \in G' \quad ghg^{-1} \in G'$$

Dovolj je pokazati za generator

$$[a, b] = a^{-1}b^{-1}ab$$

$$g[a, b]g^{-1} \in G'$$

$$ga^{-1}b^{-1}abg^{-1} = [gag^{-1}, gbg^{-1}]$$

$$gag^{-1}g^{-1}g^{-1}b^{-1}gg^{-1}gg^{-1}bg^{-1} =$$

$$[gag^{-1}, gbg^{-1}] \quad \text{to je u. od}$$

$$\text{malih } [gag^{-1}, gbg^{-1}]$$

③

$H \trianglelefteq G$ in G/H abelove

Dovolj pokazati $\forall a, b \in G. [a, b] \in H$

Vemo $\forall a, b \in G. (ab)H = (ba)H \Leftrightarrow$

$$(b^{-1}a^{-1}ba) \in H$$

$$\Rightarrow [b, a] \in H \quad \blacksquare$$

6) Poišči komutatorske podgrupe

a) A_4

b) Q

c) S_n , $n \geq 3$

a) $D_{2,n}$ $n \geq 3$

a) $K = \{ \text{id}, (12)(34), (13)(24), (14)(23) \} \trianglelefteq A_4$

$|A_4/K| = 3 \Rightarrow A_4/K$ je abelove

Pa nalogi $3 \Rightarrow G' \subseteq K$

$G' = \{1\} \Leftrightarrow G$ abelove

Torej $A_4' \neq \{1\} \Rightarrow$ je reda 2 ali 4

Piszs $(12)(34) \in A_4' \Rightarrow A_4' = K$

$g(12)(34)g^{-1} \in A_4'$

$g = (132) \Rightarrow$
 $(31)(24) \in A_4'$

$$b) Q = \{ \pm 1, \pm i, \pm j, \pm k \}$$

$$H_i = \{ \pm 1, \pm i \} \quad |G/H| = 2 \Rightarrow j \in \text{abelova}$$

$$\Rightarrow Q' \leq H \quad \Downarrow \quad H \triangleleft G$$

$$\text{Podobno } Q' \leq H_j \Rightarrow Q' = \{ \pm 1 \}$$

$$c) S_n \quad n \geq 3$$

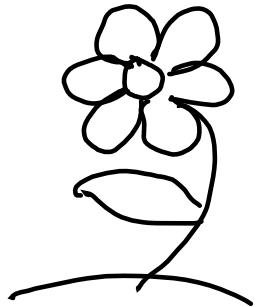
$$|S_3| = 6$$

A_3 je edinka

S_3/A_3 je abelova

$$\Rightarrow S_3' \subseteq A_3$$

$$\text{Podobno } S_n \subseteq A_n$$



$$(a, b)(a, d)(a, b)(a, d) = (a \ b \ d)$$

$$(a \ b \ d) = [(a, b), (a, d)] \in S_n' \Rightarrow A_n \subseteq S_n'$$

① koliko elementov reda 7 je v osnovni grupi reda 168

J

$$\begin{array}{r|l} 168 & 2 \\ 84 & 2 \\ 42 & 2 \\ 21 & 3 \\ 7 & 7 \end{array}$$

$$168 = 2^3 \cdot 3 \cdot 7$$

Obstaja 7-podgrupe Sylowa
in je izomorfna $\mathbb{Z}_7$ ki ima
7 elementov reda 7

$$n_7 \equiv 1 \pmod{7} \quad n_7 \mid 2^3 \cdot 3$$

$$n_7 \in \{1, 8\}$$

$n_7 = 1 \Leftrightarrow H$ je edinka. ~~X~~ (ker enota
 $\Rightarrow n_7 = 8$. sele jo se biki v enoti

$$8 \cdot 6 + 1 = 49$$

49 elementov reda 7

② Pokaži da je 2-podgrupa $SL_2(\mathbb{Z}_3)$ izomorfna grupi Q i nije ciklika

$$|SL_2(\mathbb{Z}_3)| = \frac{|GL_2|}{2} = 24 = 2^3 \cdot 3$$

$GL_2: \begin{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} & \begin{bmatrix} 1 \\ 1 \end{bmatrix} \end{bmatrix} \quad |GL_2| = 48$
 $\downarrow \qquad \qquad \downarrow$
 $3 \cdot 3 - 1 = 8 \qquad 3 - 3$

$n_2 | 3 \quad n_2 \equiv 1 \pmod{2} \quad \text{tj: } GL_2 \rightarrow \{\pm 1, \pm i\}$
 $\Rightarrow n_2 = \{1, 3\}$
 $A \mapsto \det A$
 $\ker \rho = \mathbb{Z}_2$

~~2-podgrupa Sylowa je ciklika~~

~~ima red 8~~

$n_3 | 8 \quad n_3 \equiv 1 \pmod{3}$
 $\text{tj } n_3 \in \{1, 4\}$

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^n = \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix} \quad \text{ima red 3}$$

$$\left\{ \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix} \right\} \text{ je 3 podgrupe Sylowa}$$

$$\left\{ \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 2 & 1 \end{bmatrix} \right\} \text{ je 3 podgrupa Sylowa}$$

to je njih je 4

$$4 \cdot 2 = 8 \quad \text{elementa reda 3}$$

$$\text{red } A = 3 \Rightarrow \text{red } (I - A) = 6$$

Taj najdemo se 8 elementa reda 6

Ostane nam se 8 elementa

to je oblik a i ne podgrupe Sylowa, jer n: plaća se veći

$$Q = \{\pm 1, \pm i, \pm j, \pm k\}$$

$I, -I$ i se 6 drugih elementa

$$ij = k \quad i^2 = j^2 = k^2 = -1$$

$$A = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} = \begin{bmatrix} 2 & 3 \\ 3 & 2 \end{bmatrix} = \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix} = -I$$

$$B = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} = -I$$

imamo $A, -A, B, -B$

$$C = AB = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 3 & 2 \\ 1 & 3 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

③ Pokaži, da je grupa reda $8p$; $p \neq 2$ rešljiva

Rešljiva:

$$G = G_0 > G_1 > G_2 \dots > G_n = \{1\}$$

$$G_i \triangleleft G_{i+1} \quad G_{i+1}/G_i \text{ abelove}$$

ekvivalentno

$$G > G' > G'' \dots > G^{(n)} > \dots$$

$$\exists n \in \mathbb{N} \text{ da je } G^{(n)} = \{1\}$$

Dejstvo: Naj bo $H \triangleleft G$ in H in G/H rešljivi
 $\Rightarrow G$ je rešljiva

$$|G| = 8p = 2^3 \cdot p$$

$$p = 2 \Rightarrow |G| = 2^4$$

iz predavanj vem, da so grupe p^n rešljive

ker: $Z(G) \neq \{1\}$ za končne grupe

$$|Z(G)| = p^k$$

$$a \in Z(G) \text{ reda } p$$

$$\langle a \rangle \cong C_p \leq Z(G)$$

$$\langle a \rangle \triangleleft G$$

$$|G/\langle a \rangle| = p^{n-1}$$

indukcija
 torej je G rešljiva

$$p \neq 2 \Rightarrow 8p = 2^3 \cdot p$$

2-podgrupa solva reda 8

~~p-podgrupa~~ solva reda p

$$n_p \mid 8 \quad n_p \equiv 1 \pmod{p}$$

$$n_p \in \{1\} \text{ za } p > 7 \text{ in } p = 5$$

$\Rightarrow$ p-podgr. solva je cirkla

$$H \cong C_p \text{ je rešljiva}$$

$$|G/H| = 8 = p^n \text{ je rešljiva}$$

$$p = 3 \Rightarrow$$

$$n_3 \in \{1, 4\}$$

$$n_3 = 4 \Rightarrow$$

$$\text{red } G = 24$$

8 elementov reda 3 niso v ~~8~~ $2p$ -podgr.

$$n_2 \in \{1, 3\}$$

$$n_2 \Rightarrow 1 \quad n_2 \text{ je edinka reda 8}$$

$$|G/H_2| = 3 \text{ rešljiva}$$

$$n_2 \Rightarrow 3 \text{ reda 8}$$

~~8 elementov~~ ~~reda 3~~ prosta ni

trivialna

ker red 3 elementov

$$H_1 \cap H_2 \in \{2, 4\}$$



Polinom vs polinomska funkcija

$$f(x) = x^2 + x \in \mathbb{Z}_2[x] \quad \text{polinomska funkcija}$$

$$g(x) = 0 \in \mathbb{Z}_2[x]$$

$$h(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$$

Dva polinoma sta enake če imata enake koeficiente

Polinom definira polinomske funkcije

$$\tilde{f}(x) = \tilde{g}(x) \quad \text{ker} \quad \tilde{f}(0) = \tilde{g}(0) \quad \text{in} \quad \tilde{f}(1) = \tilde{g}(1)$$

④ Določí kvadratni polinom iz $\mathbb{Z}_6[X]$ ki mu pripada ničelna polinomska funkcija

⑤ Naj bo F -polje. Pokaži da sta naslednje pogoji ekvivalentna

a) F je končno

b) obstajata različna polinoma

$f(x), g(x) \in F[X]$ z enako pripadajočo polinomske funkcije

④ $x(x-1)(x-2)(x-3) \in \mathbb{Z}_6[X]$

x	x^2	$2x$
0	0	0
1	1	2
2	0	0
3	1	2

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

⑤ F je končno polje

$$F = \{a_1, a_2, \dots, a_n\}$$

uredimo: $(x-a_1)(x-a_2) \dots (x-a_n)$
ima ničelno polinomske funkcije

b) $\Rightarrow$ a)

$$\tilde{p}(x) = \tilde{f}(x) \quad \text{Rešimo da } n \geq k$$

$$a_n x^n + \dots + a_0 = b_n x^k + \dots + b_0$$

$$a_n x^n + \dots + a_{k+1} x^k + (a_k - b_k) x^k + \dots + (a_0 - b_0) = 0$$

$(f-g)x$ je ničelna polinomska funkcija

Vemo: $f(x) \in F[x] \wedge f(a) = 0 \Rightarrow (x-a) | f(x)$

$$(f-g)(x) = (x-a) \cdot k \quad \forall a \in F$$

$$\text{st}(f-g) = d$$

verujemo $(a_1, \dots, a_{d+1})$

~~$(f-g) \neq 0$~~ $(x-a_i) | (f-g)$ za vsa a_i

$$\text{torej } (f-g)(x) = (x-a_1) \dots (x-a_{d+1})$$

stopnja $\geq d+1$

$n-1$ ba F polje $\mathbb{D}$ v

nekonečnem polnem $\mathbb{D}[X]$ v

n razločnih elementih iz F doseže enako vrednost pomeni da obstaja $a \in F$

v $a_1, \dots, a_n$ doseže a

$$f(a_1) = \dots = f(a_n) = a$$

razg - 2

opazimo: $f(x) = (x-a_1) \dots (x-a_n)$

in torej $a_1, \dots, a_n$

teži $f(x) = (x-a_1) \dots (x-a_n) = (x-a)^n$

ker $f(x) = (x-a)^n$

① Razstavi na nerazcepne faktorje nad $\mathbb{R}$

a) $x^5 - 81x$

b) $x^5 + 81x$

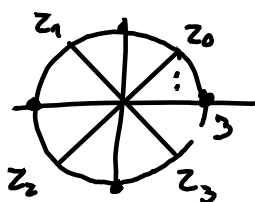
Vsek polinom st ≥ 3 je razcepen

a) $x(x^4 - 81) = x(x^2 - 9)(x^2 + 9) =$

$= x(x-3)(x+3)(x^2+9)$

b) $x(x^4 + 81) =$

$x^4 = -81$



$x^4 + 81 = (x - z_0)(x - z_1)(x - z_2)(x - z_3)$

$= (x^2 + 2ax + (a^2 + b^2))(x^2 + 2cx + (c^2 + d^2))$

$a = \frac{\sqrt{2}}{2} \cdot 3 \quad b = \frac{\sqrt{2}}{2} \cdot 3$

$(x - (a + bi))(x - (a - bi)) = x^2 - 2ax + a^2 + b^2$

$x(x^4 + 81) = x(x^2 + 3\sqrt{2}x + 9)(x^2 - 3\sqrt{2}x + 9)$

(2) Pokaż, że $f(x)$ nie rozkłada się nad $\mathbb{Q}$:

a) $f(x) = 7x^6 + 30x^3 - 6x^2 + 60$

b) $f(x) = \frac{2}{7}x^5 - \frac{7}{2}x^2 - x + 2$

Eisenstein test

$p \in \mathbb{P}$. $f(x) = a_n x^n + \dots + a_1 x + a_0$ $a_i \in \mathbb{Z}$

$p \mid a_{n-1}, \dots, a_0$ $p \nmid a_n$ $p^2 \nmid a_0$

$\Rightarrow f(x)$ nie rozkłada się nad $\mathbb{Q}$

a) $7x^2 + 30x^3 - 6x^2 + 60$

$p = 3 \Rightarrow$ nie rozkłada się nad $\mathbb{Q}$

b) $14f(x) = 4x^5 - 49x^2 - 14x + 28$

$p = 7 \Rightarrow f(x)$ nie rozkłada się nad $\mathbb{Q}$

$f(x)$ nie rozkłada się $\Leftrightarrow 14f(x)$ nie rozkłada się

③

$$f(x) = x^n + 1$$

Pokaži da je $f(x)$ nerazcepen nad $\mathbb{Q}$

$$\Leftrightarrow n = 2^k \quad k \geq 1$$

$$(\Rightarrow) n=2 \quad x^2+1 \text{ nerazcepen}$$

$$n=3 \quad x^3+1 = (x+1)(x^2 - x + 1)$$

$$n=5 \quad x^5+1 = (x+1)(\dots)$$

↑
velja za katere koli lihe n

Recimo da ni oblike 2^k

torej $n = 2^k \cdot l$ l ... liho število

$l \geq 3$

$$x^6+1 = x^{2 \cdot 3}+1 = (x^2)^3+1 = (x^2+1)(x^4-x^2+1)$$

$$x^{2^k l}+1 = (x^{2^k})^l+1 = (x^{2^k}+1)(\dots)$$

$$\Leftarrow x^2+1 \quad \checkmark$$

$$x^4+1$$

če Eisensteinov kriterij ne deluje za $f(x)$,
lahko poskusimo za $f(x+1)$

$$f(x+1) = (x+1)^n + 1 = x^n + nx^{n-1} + \dots + nx + 2$$

$$p=2$$

torej ni razcepen

ker $f(x+1)$ nerazcepen $\Leftrightarrow f(x)$ ni razcepen

$$f(x+1) = (x+1)^{2^k} + 1 = \sum_{i=0}^{2^k} \binom{2^k}{i} x^i + 1 =$$

$$= x^{2^k} + \sum_{i=0}^{2^k-1} \binom{2^k}{i} x^i + 2$$

↑ $\binom{2^k}{i}$ je sod za $1 \leq i \leq 2^k-1$

Poltem velja kriterij za $p=2$

$$f(x+1) = (x+1)^{2^{k+1}} + 1 =$$

$$\left((x+1)^{2^k} \right)^2 + 1 =$$

po indukciji p deli 2^k

$$= \left(x^{2^k} + \underbrace{\text{sodi}}_{\text{sodi}} + 1 \right)^2 + 1 =$$

$$= x^{2^{k+1}} + \underbrace{\text{sodi}}_{\text{sodi}} + 2$$

④ $\mathbb{Z}_2 \quad \forall n=2,3,4,5,6$

zapiši polinom $f_n(x) = x^n + 1$

kot produkt nerazcepnih polinomov nad $\mathbb{Z}_2$

⑤ Polinom $f(x) = x^4 + 2$ zapiši kot produkt
neraz. nad $\mathbb{Z}_3$

⑥ $f(x) = x^4 - 2x^3 - 2x + 4$ zapiši kot produkt
nerazc. nad $\mathbb{Z}_7$

$f(x)$ ima faktor $(x-b) \Leftrightarrow f(b) = 0$

$x^2 + x + 1$ je cdin: nerazcepní v $\mathbb{Z}_2[x]$
glej 2

$$f(x) = x^4 + 2$$

Imamo 2 možnosti: razstavimo na 2 faktorja

→ linearni faktor +

$$f(1) = 0$$

$$f(x) = (x-1)(\dots)$$

$$(x^4 + 2) : (x-1) = (x^4 + 2)(x+2)$$

$$x^4 + 2 = (x^2 + 1)(x-1)(x+1)$$

⑥

$$f(x) = x^4 - 2x^3 - 2x + 4 =$$

$$= x^3(x-2) - 2(x-2) =$$

$$= (x^3 - 2)(x - 2)$$

iscanemo $x^3 = 2$ za nek $x \in \mathbb{Z}_7$

0	0	0
1	1	1
2	8	1
3	27	-1
-3	-27	1
-2		-1
-1		-1

$\Rightarrow x^3 - 2 \nexists$
nerazcepen

kako določimo razcepnost nad $\mathbb{Q}$

- 1) Eisensteinov test za $f(x)$
- 2) $\leadsto f'(x+1)$
- 3) $\leadsto$ prevod na polinom nad $\mathbb{Z}_p$

⑦ Naj bodo $a_0, \dots, a_n \in \mathbb{Z}$ in $p \in \mathbb{P}$
 $p \nmid a_n$

Če je polinom $a_n x^n + \dots + a_1 x + a_0$ razcepen nad $\mathbb{Q}$
je $a_n(\text{mod } p)x^n + \dots + a_1(\text{mod } p)x + a_0(\text{mod } p)$
razcepen nad $\mathbb{Z}_p$

Posledično: Če je $a_n(\text{mod } p)x^n + \dots + a_0(\text{mod } p)$
nerazcepen nad $\mathbb{Z}_p$ je $a_n x^n + \dots + a_0$
nerazcepen nad $\mathbb{Q}$

$\Rightarrow$ Po predpostavki: je $p(x)$ razcepen nad $\mathbb{Q}$

$$p(x) = g(x) \cdot k(x) \quad g, k \text{ nekonst}$$

$$= (b_m x^m + \dots + b_0)(c_l x^l + \dots + c_0)$$

$$m+l=n$$

$$a_n = b_m \cdot c_l$$

$$\Rightarrow p \nmid b_m, c_l$$

$$\mathbb{Z} \rightarrow \mathbb{Z}_p$$

$$n \mapsto n \text{ mod } p$$

$$\ker f = p\mathbb{Z}$$

surjektivni:
homomorfizem
kelobezjev

$$\underbrace{\mathbb{Z}[x] \xrightarrow{f(x)} \mathbb{Z}_p[x]}_{\text{f(x) mod p}} \\ a_n x^n + \dots + a_0 \mapsto (a_n \text{ mod } p)x^n + \dots + (a_0 \text{ mod } p)$$

DN: to je homomorfizem kelobezjev

$$p(x) \text{ mod } p = (g(x) \text{ mod } p)(k(x) \text{ mod } p)$$

ker b_m in c_l nista deljiva s p

toraj se stopnje ohranjata

a, b, c liha števila $\Rightarrow p(x) = ax^4 + bx + c$ nerazcepen nad $\mathbb{Q}$

$p(x) = 7x^5 + 3x^2 + 1$ nerazcepen nad $\mathbb{Q}$

$$p(x) = x^5 + x^2 + 1 \pmod{2}$$

$$p(0) = 1$$

$$p(1) = 1$$

Če bi bil razcepen je eden od faktorjev

$$x^2 + x + 1$$

$$(x^5 + x^2 + 1) : (x^2 + x + 1) = x^3 - x^2$$

$$\begin{array}{r} -x^3 - x^4 - x^3 \\ \hline \end{array}$$

$$\begin{array}{r} -x^4 - x^3 + x^2 + 1 \\ \hline \end{array}$$

$$\begin{array}{r} +x^4 + x^3 + x^2 \\ \hline \end{array}$$

je ostrek

$1 \neq 0$ ni deljiv $\Rightarrow$ ni razcepen

$$p(x) = 36x^3 + 7x + 6$$

$$p(x) = x^3 + 2x + 1 \pmod{5}$$

$$p(0) = 1$$

$$p(1) = 4$$

$$p(2) = 3$$

$$p(-1) = 3$$

$$p(3) = 4$$

nime nical $\Rightarrow$ ni vazegher

(4) $a_1, \dots, a_n$ različna cela števila

Pokaži da je $p(x) = (x-a_1) \dots (x-a_n) - 1$
nerazcepen nad $\mathbb{Q}$

Recimo da je razcepen

$$p(x) = g(x) \cdot r(x) \quad \text{st}(g(x)) + \text{st}(r(x)) = \text{st}(p(x))$$

BŠZS vodi in člen $g(x) \neq 1$

$$\forall i \in [n]. \quad p(a_i) = -1 \Rightarrow p(a_i) r(a_i) = -1$$

g in r imata cele koeficiente

$$g(a_i) = \pm 1 \quad r(a_i) = \mp 1$$

$\forall i$:

$$\text{I } g(a_i) = 1, r(a_i) = -1$$

$$\text{II } g(a_i) = -1, r(a_i) = 1$$

BŠZS. I ali II velja v večini plovci ^{ali celo} (recimo I)

$$\text{st}(g) \leq \frac{n}{2} \quad \text{BŠZS}$$

$$g(x) - 1 \text{ ima } 0$$

$$g(x) - 1 \text{ ima } > \frac{n}{2} \text{ ničel } \rightarrow \text{ne}$$

$$\Rightarrow \text{st}(g(x)) = \frac{n}{2} \quad \text{in } \text{st}(r(x)) = \frac{n}{2}$$

$$g(x) = b_k x^k + \dots + b_0 \quad r(x) = c_k x^k + \dots + c_0$$

$$\text{st}(g(x) - r(x)) \leq \frac{n}{2} - 1$$

Recimo da I velja za $a_1, \dots, a_{\frac{n}{2}}$

in II velja za $a_{\frac{n}{2}+1}, \dots, a_n$

$g(x) - 1$ ima ničle za $a_1, \dots, a_{\frac{n}{2}}$

$r(x) - 1$ ima ničle za $a_{\frac{n}{2}+1}, \dots, a_n$

$$\begin{aligned} (g(x) - 1)(r(x) - 1) &= g(x)r(x) - r(x) - g(x) + 1 = \\ &= \underbrace{g(x)r(x)}_{-1} - (g(x) + r(x)) \text{ ima } a_1, \dots, a_n \text{ ničel} \end{aligned}$$

~~preveč ničel~~

$a_1, \dots, a_n$ različne cele števila

Pokaži da je

$p(x) = (x-a_1)^2 \dots (x-a_n)^2 + 1$ nerazcepljen nad $\mathbb{Q}$

Recimo da je $\exists r, g \in \mathbb{Z}[X]$ takol
 $p(x) = r(x) \cdot g(x)$

$$p(a_i) = 1$$

$$\forall i \Rightarrow r(a_i) \cdot g(a_i) = 1$$

$$r(a_i) = g(a_i) = \pm 1$$

$p(x) > 0 \forall x \Rightarrow p(x)$ nima ničel $\Rightarrow$
 $r(x)$ in $g(x)$ nima ničel

$$r(a_i) = 1 \text{ in } r(a_j) = -1 \quad \times$$

ker je urezen $\Rightarrow$

$$(\forall a_i : r(a_i) = 1) \vee (\forall a_i : r(a_i) = -1) \\ \Rightarrow \text{!} g(a_i)$$

B SZS $r(a_i) = g(a_i) = 1 \quad \forall i$

$$r(x) - 1 \text{ ima } \geq n \text{ ničel} \Rightarrow \text{st}(r(x)) \geq n \\ \text{--- ! ---} \text{st}(g(x)) \geq$$

$$\Rightarrow \text{st}(r(x)) = \text{st}(g(x)) = n$$

$$\text{st}(p(x)) = \text{st}(r(x)) + \text{st}(g(x)) = 2n$$

$$r(a_i) - g(a_i) = 0 \Rightarrow$$

$$\text{st}(g(x) - r(x)) \geq n \quad a_i = 0$$

$$\Rightarrow \text{g(x) = r(x)} \quad r(x) = g(x)$$

$$\Rightarrow p(x) = r^2(x)$$

$$p(x) = \underbrace{(x-a_1) \dots (x-a_n)}_{A(x)}^2 + 1 = r^2(x)$$

$$A^2(x) - r^2(x) = -1$$

$$(r(x) - A(x))(r(x) + A(x)) = 1$$

$\Rightarrow r(x) - A(x)$ je konstanten in
 $A(x) + r(x)$ je konstanten

$\times$ ker ima $A(x)$ stopnjo

Razširitve polj

E, F polj:

$E \subseteq F$ $[F:E]$ stopnja razširitve
 $\downarrow$
 $\dim F$ kot vektorskega polja nad E

$a \in F$

$E(a)$ - razširitev F s pomočjo A

$\downarrow$ najmanjše podpolje F , ki vsebuje E in a

npr: $\mathbb{Q}(\sqrt{2}) \supseteq \mathbb{Q}$

"

$$\{a + b\sqrt{2} ; a, b \in \mathbb{Q}\}$$

$$[E(a): E] = \text{st}(\min; \max; \text{polinom } a \text{ v } E) \\ \text{st}(m_a(x)) \quad m_a x \in E[x]$$

Če imamo $E \subseteq F \subseteq G$ zaporedje razširitev,

$$\text{če } [G:E] = m, [G:F] = k, [F:E] = n \Rightarrow m = kn$$

$$E \subseteq F \quad a \in F$$

$$E(a) = E \iff [E(a):E] = 1$$

$(\Rightarrow)$ minimalni polinom $x - a \in E$

$(\Leftarrow)$ Baza $E(a)$ nad E je $\{1\}$

$$a = \underset{\in E}{\alpha} \cdot 1 \in E$$

①

Pokażi $\mathbb{R}(a) = \mathbb{C} \iff a \in \mathbb{C} - \mathbb{R}$

$\Rightarrow$ Reczmo że $a \in \mathbb{R}$

potem $\mathbb{R}(a) = \mathbb{R}$

$\Leftarrow a \in \mathbb{C} - \mathbb{R}$

$$\mathbb{R} \subseteq \mathbb{R}(a) \subseteq \mathbb{C} \quad [\mathbb{C} : \mathbb{R}] = 2$$

$$\text{cozto } \mathbb{R} \neq \mathbb{R}(a) \Rightarrow [\mathbb{R}(a) : \mathbb{R}] \geq 2$$

$$\Rightarrow [\mathbb{R}(a) : \mathbb{R}] = 2 \Rightarrow \overset{\curvearrowright}{[\mathbb{R}(a) : \mathbb{C}] = 1}$$

$$\Rightarrow \mathbb{C} = \mathbb{R}(a)$$

Nej bo $[E:F] = 12$

Pojasni zakaj elementiz E ne more biti algebraičen stopnje 8 nad F

α je alg. nad stopnjo k nad F če

$$[F(\alpha):F] = k$$

$\Leftrightarrow$ min polinom $m_\alpha(x) \in F[x]$ ima stopnjo k

$$[E:F] = 12$$

$$\underbrace{F \subseteq F(\alpha) \subseteq E}_{\substack{8 \\ 12}}$$

$$8 \cdot k = 12$$

$$k = \frac{3}{2} \notin \mathbb{Z} \quad *$$

Primer:

$$\mathbb{Q}(\sqrt[12]{2})$$

$x^{12} - 2$ je minimalni polinom po Eisensteinovem kriteriju

$$\sqrt[4]{2} = \alpha^3 \in \mathbb{Q}(\sqrt[12]{2})$$

$$\underbrace{\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[4]{2}) \subseteq \mathbb{Q}(\sqrt[12]{2})}_{\substack{4 \quad 3 \\ 12}}$$

Naj bo n liho število

4.4

$$\forall a \in \mathbb{Q} (\sqrt[n]{a}) \in \mathbb{Q} \text{ velja } a^2 \notin \mathbb{Q}$$

...

② Naj bo $[E:F] = p$ ~~primo~~ število
 $\exists \exists F$

p -poti v elementiz E/F je alg. stopnja
 p nad F

$$F \subseteq F(a) \subseteq E \quad \text{zanka}$$

$\underbrace{\hspace{1cm}}_{\geq 2r} \quad \underbrace{\hspace{1cm}}_k$
 $\underbrace{\hspace{2cm}}_p$

$$p = r \cdot k \Rightarrow r = 1 \vee k = 1$$

$$\Rightarrow k = 1$$

$$\Rightarrow r = p$$

③ koliko je $[\mathbb{Q}(\sqrt[3]{3-\sqrt{7}}) : \mathbb{Q}]$?

koliko je $[\mathbb{Q}(3-5\sqrt[3]{7} + 4\sqrt[3]{49}) : \mathbb{Q}]$?

$$a^2 = 9 - 6\sqrt{7} + 7$$

$$(x^2 - 6x)(a) = 16 - 6\sqrt{7} - 18 + 6\sqrt{7} = -2$$

$$p(x) = x^2 - 6x + 2$$

↑ nezrečen, po
Eisensteinu

stopnja razreditve = 2

2. način

$$[\mathbb{Q}(\sqrt{7}) : \mathbb{Q}] = 2 \quad a \in \mathbb{Q}(\sqrt{7})$$

$$\Rightarrow \mathbb{Q} \subseteq \mathbb{Q}(a) \subseteq \mathbb{Q}(\sqrt{7})$$

$$\underbrace{\qquad\qquad\qquad}_{r \neq 1} \qquad \underbrace{\qquad\qquad\qquad}_2$$

$$\Rightarrow r = 2$$

$$[\mathbb{Q}(3-5\sqrt[3]{7} + 4\sqrt[3]{49})$$

Vemo $[\mathbb{Q}(\sqrt[3]{7}) : \mathbb{Q}] = 3$ ker $x^3 - 7$ ni razložen

$$b \in \mathbb{Q}(\sqrt[3]{7})$$

$$\mathbb{Q} \subseteq \mathbb{Q}(b) \subseteq \mathbb{Q}(\sqrt[3]{7})$$

$$\underbrace{\qquad\qquad\qquad}_{b \notin \mathbb{Q}} \Rightarrow r \neq 1 \Rightarrow r = 3$$

$$b \in \mathbb{Q} \quad 3-5\sqrt[3]{7} + 4\sqrt[3]{49} = \alpha$$

$$4x^2 - 5x + 3 - \alpha \text{ anihilira } \sqrt[3]{7}$$

Amorfo $x^3 - 7$ tudi anihilira in ni deljiv $\times$

Nasprotuje linearni neodvisnosti

(Baza: 1, $\sqrt[3]{7}$, $\sqrt[3]{49}$)

$$p(x) = 3 - 5x + 4x^2$$

$$D(p(x), x^3 - 7) = 1$$

$$\alpha(x)p(x) + \beta(x)(x^3 - 7) = 1$$

$$x = \sqrt[3]{7}$$

$$b^{-1} = \alpha(\sqrt[3]{7})$$

⑤ Koliko je $[\mathbb{Q}(\underbrace{\sqrt[3]{3+\sqrt{3}}}_a) : \mathbb{Q}]$

$$a^6 = (3+\sqrt{3})^2 = 9 + 6\sqrt{3} + 3 = 12 + 6\sqrt{3}$$

$$a^3 = 3 + \sqrt{3}$$

$$a^6 - 6a^3 = 12 - 18 + 6\sqrt{3} - 6\sqrt{3} = -6$$

$$a^6 - 6\sqrt{3} + 6 \quad P_0 \text{ Eisenstein}$$

$$\Rightarrow [\mathbb{Q}(\sqrt[3]{3+\sqrt{3}}) : \mathbb{Q}]$$

a, b algebraični:

$$\text{pokaži: } [F(a, b) : F] = [F(a) : F] \cdot [F(b) : F]$$

$$\underbrace{F \subseteq F(a)}_m \subseteq \underbrace{F(a, b)}_k$$

$$\underbrace{F \subseteq F(b)}_n \subseteq \underbrace{F(a, b)}_c$$

če sta si
maji

$$F(a, b) = mk = nc$$

$$\Rightarrow m \mid [F(a, b) : F] \wedge n \mid [F(a, b) : F]$$

$$\Rightarrow mn \mid [F(a, b) : F]$$

$$[F(b) : F] = n \Rightarrow \exists p(x) \in F[x], p(b) = 0$$

in je nerazločljiva

$$p(x) \in F[x]$$

$$\Rightarrow p(x) \in F(a)[x]$$

$$p(b) = 0$$

$$\Rightarrow [F(a, b) : F(a)] \leq n \Rightarrow k \leq n \Rightarrow$$

$$[F(a, b) : F] = mk \leq m \cdot n \Rightarrow = mn$$

⑦ ~~11/10~~

$$[\mathbb{Q}(\sqrt{3}, \sqrt[3]{5}) : \mathbb{Q}] = ?$$

$$2 \cdot 3 = 6$$

$$(8) [\mathbb{Q}(\sqrt{3} + \sqrt[3]{5}) : \mathbb{Q}] = ?$$

6) Pokaži da je

$$[\mathbb{Q}(\sqrt{3}, i) : \mathbb{Q}] = 4$$

Pokaži, da je $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{3}, i)$

komentar

izrek o primitivnem elementu

$$\mathbb{Q}(\sqrt{3}, \sqrt[3]{5}) = \mathbb{Q}(\sqrt{3} + \sqrt[3]{5})$$

$$[\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2 \quad [\mathbb{Q}(i) : \mathbb{Q}] = 2$$

① Pdezi: $F(a^k, a^l) = F(a^d)$; $d = (k, l)$

② $[\mathbb{Q}(\sqrt[4]{2}, \sqrt[3]{2}) : \mathbb{Q}]$ in $[\mathbb{Q}(\sqrt[4]{2}, \sqrt[6]{2}) : \mathbb{Q}]$

$$\begin{aligned} k &= d \cdot \alpha & a^k &= a^{d\alpha} = (a^d)^\alpha \\ l &= d \cdot \beta & a^l &= a^{d\beta} = (a^d)^\beta \end{aligned}$$

$$F(a^k, a^l) \subseteq F(a^d)$$

Davetj je pdezi da $a^d \in F(a^k, a^l)$

$$d = mk + nl \quad m, n \in \mathbb{Z}$$

$$a^d = a^{mk+nl} = (a^k)^m \cdot (a^l)^n \in F(a^k, a^l)$$

② $\mathbb{Q}(\sqrt[4]{2}, \sqrt[3]{2}) = \mathbb{Q}(2^{\frac{1}{6}})$

$$2^{\frac{1}{2}}, 2^{\frac{1}{3}} = 2^{\frac{1}{6} \cdot 3}, 2^{\frac{1}{6} \cdot 2}$$

$$[\mathbb{Q}(2^{\frac{1}{6}}) : \mathbb{Q}] = 6$$

ker $x^6 - 2$ minimalni polinom
in je ireducibilan po Eisensteinu

$$\mathbb{Q}(\sqrt[4]{2}, \sqrt[6]{2}) = \mathbb{Q}(\sqrt[12]{2})$$

$$2^{\frac{1}{4}} = 2^{\frac{3}{12}} \quad [\dots] = 12$$

$$2^{\frac{1}{6}} = 2^{\frac{2}{12}} \quad \text{ker } x^{12} - 2 \text{ ireducibilan po Eisensteinu}$$

③ Koliko je $[\mathbb{Q}(\sqrt{2} + 3\sqrt{2}) : \mathbb{Q}]$ in
 $[\mathbb{Q}(\sqrt{2} + 4\sqrt{2}) : \mathbb{Q}]$?

④ Koliko je $[\mathbb{Q}(\sqrt[6]{2}) : \mathbb{Q}(\sqrt{2})]$

Koliko je

$$[Q(\sqrt[6]{3}, i) : Q(\sqrt{3}, i)]$$

$$\mathbb{Q}(\sqrt[6]{3}, i) \cong \mathbb{Q}(\sqrt[6]{3}, i) \xrightarrow{F}$$

$$\sqrt{3} + i = 3^{\frac{1}{2}} + i = 3^{\frac{3}{6}} + i = (\sqrt[6]{3})^3 + i \in F$$

$$\mathbb{Q}(\sqrt{3} + i) = \mathbb{Q}(\sqrt{3}, i)$$

✓

$$2 \quad a = \sqrt{3} + i$$

$$j = a - \sqrt{3}$$

$$-1 = a^2 - a2\sqrt{3} + 3$$

$$a^2\sqrt{3} = a^2 + 4$$

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{3}, i) \subseteq \mathbb{Q}(\sqrt[6]{3}, i)$$

$$\underbrace{\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{3})}_{\text{normal}} \subseteq \underbrace{\mathbb{Q}(\sqrt{3}, i)}_{\text{normal}} \subseteq \mathbb{Q}(\sqrt{3}, i)$$

$$\underbrace{2 \quad 2}_{4}$$

$$\underbrace{O(\mathbb{Q}(i))}_2 \subset \underbrace{O(\sqrt{3}i)}_6$$



$$\Rightarrow \mathbb{Q}(\sqrt[3]{3}, i) : \mathbb{Q}(\sqrt[3]{3} + i) = 3$$

6) Pokazi da $\mathbb{Q}(\sqrt{3}) \neq \mathbb{Q}(\sqrt{2})$

7) Neg bode $a_1, \dots, a_n$ algeb. nad F

Pokezi

$$[F(a_1, \dots, a_n) : F] \leq [F(a_1) : F] \dots [F(a_n) : F]$$

6) Neg bo $f: \mathbb{Q}(\sqrt{2}) \rightarrow \mathbb{Q}(\sqrt{3})$ izomorfizem

$$f(1) = 1 \quad \wedge \quad f(0) = 0$$

$$f(2) = 2 \quad \text{ker} \quad 1+1=2 \quad f(1)+f(1)=2$$

$$f(n) = n \quad \forall n \in \mathbb{Z} \quad f(n^{-1}) = f(n)^{-1} = n^{-1}$$

$$f\left(\frac{m}{n}\right) = f(m \cdot n^{-1}) = f(m) \cdot f(n^{-1}) = m \cdot n^{-1}$$

$\leadsto f$ ahrenja racionalne stavila

$$f(a+b\sqrt{2}) = a+b f(\sqrt{2})$$

$$f(\sqrt{2}) = \alpha + \beta\sqrt{3}$$

$$f(2) = \alpha^2 + 2\alpha\beta\sqrt{3} + 3\beta^2 = 2$$

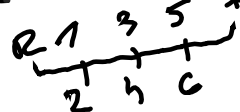
$$\underbrace{2\alpha\beta\sqrt{3}}_{\in \mathbb{Q}} = \underbrace{2\alpha^2 - 3\beta^2}_{\in \mathbb{Q}}$$

$$\Rightarrow \alpha = 0 \vee \beta = 0$$

$$\beta = 0 \Rightarrow \alpha^2 = 2 \quad \alpha \notin \mathbb{Q} \quad *$$

$$\alpha = 0 \Rightarrow 3\beta^2 = 2 \Rightarrow \beta = \sqrt{\frac{2}{3}} \notin \mathbb{Q}$$

1. y_i 
 Aig
 To je racionalno, racionalnih, ampak ne bi tedaj



⑦

$n=2$:

$$\underline{F(a, b) \leq F(a) \cdot F(b)}$$

$$[F(a, b) : F] \leq \underbrace{[F(a) : F]}_k \cdot \underbrace{[F(b) : F]}_m$$

$$\underbrace{F \leq F(a)}_k \leq \underbrace{F(a) \leq F(a, b)}$$

Vemo: $[F : F(b)] = m \Rightarrow \exists p(x)$ nerazcep $p \in F[x]$
 $p(b) = 0$ $\text{st}(p(x)) = m$

$$p(x) \in F(a)[x]$$

$p(x)$ je morda razcepen

Torej minimalni polinom $\text{st} \leq m$

Podobno za več njev

- ⑧ Naj bodo $a_1, \dots, a_n$ algebraični: stopnje 2
 Pokaži da stopnje razširitve

$$[F(a_1, \dots, a_n) : F] = 2^k \text{ za nek } k \leq n$$

- ⑨ Za racionalna prostora $p_1, \dots, p_n$

$$[\mathbb{Q}(p_1, \dots, p_n) : \mathbb{Q}] = 2^k$$

$$\underbrace{F \subseteq F(a_1)}_2 \subseteq \underbrace{F(a_1, a_2)}_{\leq 2} \subseteq \underbrace{F(a_1, a_2, a_3)}_{\leq 2} \subseteq \dots \subseteq F(a_1, \dots, a_n)$$

$\Rightarrow$ Vseko imamo izbira 1 ali 2

Recimo da je $k \geq 2 \Rightarrow$

$$[F(a_1, \dots, a_n) : F] = 2^k \quad k \leq n$$

- ⑩ Dokazati moramo za $\forall p$

$x^2 - p$ ni razcepni v $\mathbb{Q}(g_1, \dots, g_n)$ $\in \mathbb{P}$

$$\mathbb{Q} \subseteq \underbrace{\mathbb{Q}(\sqrt{2})}_F \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3}) \subseteq \dots$$

$$\text{Vemo: } F(\sqrt{a}, \sqrt{b}) \supseteq F$$

$$\sqrt{a}, \sqrt{b}, \sqrt{ab} \notin F$$

$$\underbrace{F \subseteq F(\sqrt{a})}_2 \subseteq \underbrace{F(\sqrt{a}, \sqrt{b})}_?$$

$$F \subseteq F(\sqrt{b}) \subseteq F(\sqrt{a}, \sqrt{b})$$

$$\sqrt{b} = \alpha + \beta\sqrt{a} \quad \alpha, \beta \in F$$

$$b = \alpha^2 + 2\alpha\beta\sqrt{a} + \beta^2 a$$

$$2\alpha\beta\sqrt{a} = b - \alpha^2 - \beta^2 a$$

$$\text{če } \alpha\beta \neq 0 \Rightarrow \sqrt{a} \in F$$

$$\Rightarrow \alpha\beta = 0$$

$$\alpha = 0 \Rightarrow b = \beta^2 a$$

$\Rightarrow a_1, \dots, a_n \in F_{\text{extension}} \text{ nicht}$

18.4

$$h(x) := \gcd(f(x), f'(x))$$

$$h(x) = \alpha(x) f(x) + \beta(x) \cdot f'(x) \in F[x]$$

$$h(x) \neq 1 \Rightarrow$$

$$(x-b) \mid h(x) \in E[x]$$

$$\Rightarrow \text{node: } (x-b) \mid (f(x), f'(x))$$

$$\underline{b} \text{ ist eine Nullstelle von } f$$

$$f(x) = (x-b)r(x)$$

$$f'(x) = r(x) + (x-b)r'(x)$$

$$\Rightarrow (x-b) \mid r(x) \Rightarrow$$

$$(x-b)^2 \mid f(x)$$

$\Leftarrow$

$f(x) f'(x) \text{ teilt}$

$$1 = \alpha(x) \cdot f(x) + \beta(x) f'(x) \in F[x]$$

$$\exists a \in E \text{ da } (x-a)^2 \mid f(x)$$

$$f(x) = (x-a)^2 k(x)$$

$$f'(x) = 2(x-a)k(x) + k'(x)(x-a)^2$$

$$\Rightarrow 1 = 0 \text{ wegen } x=a$$

② Naj bo F polje karakteristike 0
in $F \subseteq E$ E/F

Pokaži: $a \in E$ je k -kratna ničla $f(x) \iff$
 $\iff f(a) = f'(a) = \dots = f^{(k-1)}(a) = 0$
in $f^{(k)}(a) \neq 0$

a je k -kratna ničla $f(x)$ če
 $(x-a)^k \mid f(x)$ in $(x-a)^{k+1} \nmid f(x)$

$$f(x) = f(a) + \frac{f'(a)}{1!}(x-a) + \frac{f''(a)}{2!}(x-a)^2 + \dots$$

(lahko ker char $F = 0$)

$\Rightarrow$ predpostavimo a k -kratna ničla

$$f(x) = f(a) + \dots + \frac{(x-a)^{k-1}}{(k-1)!} f^{(k-1)}(a) + (x-a)^k h(x)$$

$$f(a) = 0$$

x
resolj; den.

$$(x-a) \dots (x-a)^k \text{ so linearne resolj.}$$

$$\Rightarrow f(a) = \frac{f'(a)}{1!} = \dots = \frac{f^{(k-1)}(a)}{(k-1)!} = 0$$

$\Rightarrow$

$\neq$

$$f(a) = 0 \dots f^{(k-1)}(a) = 0$$

$$f^{(k)}(a) \neq 0$$

$\dots$

Opomba. $f(x)$ razcepi (le 1) $f(x)$, $f(x)/f(x)$

$$\text{st } (f'(x)) < f(x)$$

$$\Rightarrow ((f(x), f'(x)) \neq 1 \Leftrightarrow f'(x) \equiv 0)$$

③ Pojasni zakaj $\mathbb{Q}(\sqrt{2})$ je razpadno polje vsakega izmed polinoma

$$x^2 - 2$$

$$3x^3 - 6x$$

$$x^4 - 3x^2 + 2$$

Razpadno polje $f(x)$ je najmanjša razširitev E polja F , da $f(x)$ razpade nad E na linearne faktorje

$\alpha_1, \dots, \alpha_k$ vse nicle $f(x)$

$$E = F(\alpha_1, \dots, \alpha_k)$$

$$f(x) = x^2 - 2 \quad \text{nicle: } \sqrt{2}, -\sqrt{2}$$

$$\Rightarrow (x - \sqrt{2})(x + \sqrt{2})$$

$$\mathbb{Q}(\sqrt{2}, -\sqrt{2}) = \mathbb{Q}(\sqrt{2})$$

$$p(x) = 3x^3 - 6x = 3x(x^2 - 2) = 3x(x - \sqrt{2})(x + \sqrt{2})$$

$$\Rightarrow \mathbb{Q}(0, \sqrt{2}, -\sqrt{2}) = \mathbb{Q}(\sqrt{2})$$

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

$$(x - \sqrt{2})(x + \sqrt{2})(x - 1)(x + 1)$$

$$\rightarrow \mathbb{Q}(\sqrt{2})$$

④ Pokaži zakaj je $\mathbb{Q}(\sqrt{2}, \sqrt{3})$
razpadno polje polnoma

$$x^4 - 5x^2 + 6 \in \mathbb{Q}[x]$$

$$f_A = (x^2 - 2)(x^2 - 3) = (x - \sqrt{2})(x + \sqrt{2})(x - \sqrt{3})(x + \sqrt{3})$$

$$E = \mathbb{Q}(\sqrt{2}, -\sqrt{2}, \sqrt{3}, \sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$$

⑤ Označimo

$\omega = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$ primitivni 3. koren iz enote

Pokaži: $\mathbb{Q}(\sqrt[3]{2}, \omega)$ dobimo razpadno polje
polinoma $x^3 - 2 \in \mathbb{Q}[x]$

Poišči stopnjo razpadnega polja nad $\mathbb{Q}$

$$x^3 - 2 = (x - \sqrt[3]{2})(x^2 + \sqrt[3]{2}x + 2)$$

$$\mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2) = \mathbb{Q}(\sqrt[3]{2}, \omega)$$

$$\leq \checkmark$$

$$2 \quad \omega = \frac{\sqrt[3]{2}\omega}{\sqrt[3]{2}}$$

$$\mathbb{Q} \subseteq \mathbb{Q}(\omega)$$

stopnja:

$$\underbrace{\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2})}_3 \subseteq \underbrace{\mathbb{Q}(\sqrt[3]{2}, \omega)}_{\leq 2 \neq 1} \Rightarrow 6$$

$$\left(\omega + \frac{1}{2}\right)^2 = \left(i\frac{\sqrt{3}}{2}\right)^2 = -\frac{3}{2}$$

$$\text{pod: } \left(x + \frac{1}{2}\right)^2$$

G) Pokazi

a) $Q(\cdot)$ je razpredno poje polinom

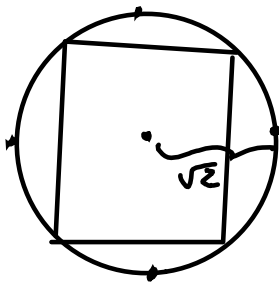
$$X^4 + 4 \in \mathbb{Q}[X]$$

b) $\mathbb{Q}(\sqrt[4]{2}, i)$ je razpadno polje, polnane

$$x^4 + 2 \in \mathbb{Q}[x]$$

c) $\mathbb{Q}(\sqrt{2}, i)$ ~~verfuehrt~~ ~~sch~~ $X^4 + 1 \in \mathbb{Q}[X]$

$$a) \quad x^{4-k} = \frac{2}{a} \prod_{i=1}^4 (x - x_i) = \frac{2}{a} (x - 1)(x - (-1))(x - i)(x - (-i))$$



$$x^4 = -4$$

$$\sqrt{2} \frac{\sqrt{2}}{2} (1+i) \cdot \sqrt{2} \frac{\sqrt{2}}{2} (-1+i)$$

$$\sqrt{2} \frac{\sqrt{2}}{2} (-1-i) \sqrt{2} \frac{\sqrt{2}}{2} (1-i)$$

Reziprokno pajaie: $Q(i, -j) = Q(j)$

b) $x^4 + 2$



$x^4 = -2$

$4\sqrt{2}$

$$x^4 + 2 = \sqrt[4]{2} \frac{\sqrt{2}}{2} (1+i) = \frac{\sqrt[4]{2}}{\sqrt[4]{4}} = \frac{1}{\sqrt[4]{2}}$$

$$x^{4+2} = (x - \frac{1}{\sqrt{2}}(1+i)) (x - \frac{1}{\sqrt{2}}(1-i)) \dots$$

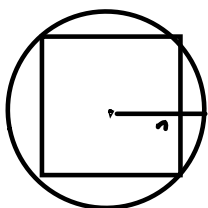
$$\mathbb{Q} \left(\frac{1}{4\sqrt{2}} (1+i), \dots \right)$$

$$j: \frac{1}{4\sqrt{2}}(1+i) - \frac{1}{4\sqrt{2}}(-1+i) = \frac{1}{4\sqrt{2}}(2i).$$

$$\frac{1}{4\sqrt{2}} = \frac{1}{4\sqrt{2}} ((1+i) + (1-i)) = \frac{2}{4\sqrt{2}}$$

$$\Rightarrow \sqrt[4]{2} \quad \sqrt[4]{2}$$

$$c) \quad x^{4+1} = (x^{\frac{\sqrt{2}}{2} + i})^{\alpha} (x^{-\frac{\sqrt{2}}{2} + i})^{\beta} (x^{\frac{\sqrt{2}}{2} + i})^{\gamma} (x^{-\frac{\sqrt{2}}{2} + i})^{\delta}$$



5 ✓

$$\sqrt{2}: \alpha + \beta = \frac{\sqrt{2}}{2} (2) = \sqrt{2}$$

$$i: \frac{\sqrt{2}}{2}(\alpha + \gamma) = \frac{\sqrt{2}}{2}(2i) \cdot \frac{\sqrt{2}}{2} = i$$

$$f(x) \in F[x] \quad \text{st} (f(x)) = n$$

E - razpadno polje $f(x)$

$$\text{pokaži } [E:F] \leq n!$$

in $n \mid [E:F]$ če $f(x)$ nerazcepen

$$X^3 - 2, [E:F] \leq 6$$

$$3 \mid [E:F]$$

$$E = F(a_1, \dots, a_k) \quad a_i \text{ niče} \quad k \leq n$$

$$F \subseteq F(a_1) \subseteq \dots \subseteq F(a_k) \leq n!$$

$$\underbrace{\leq n \quad \leq (n-1) \quad \dots \quad 1}$$

↑ ker smo ano niče že uveljavili
stopnje minimalnega polnoma

$$f(x) = (x - a_1) g(x) \text{ nad } F(a_1)$$

$$\text{st} g(x) = n-1$$

$$\text{če ni razcepen} \Rightarrow \text{st } F \subseteq F(a_1) \leq n$$

teme 15 minut

←

Denimo da F ni algebrsko zaprta

$\exists f(x)$ ki nima ničle v F

Naj bo a ta ničla. $F(a)$ naj bo razširitev

$$a \in F(a) \Rightarrow F(a) \neq F$$

$$\text{f.m. stopnje } n \Rightarrow [F(a):F] \leq n$$

ker je končno

③

Naj bo $E \supsetneq \mathbb{R}$ koreno razširitev realnih števil

Pokaži da je $E \cong \mathbb{C}$

Na tabl:

4.)

Oglejmo si polinom

$$f(x) = x^2 + x + 1 \in \mathbb{Z}_2[x]$$

je nerazcepen nad $\mathbb{Z}_2[x]$

$$\mathbb{Z}_2[x]$$

$$F = \mathbb{Z}_2[x] / (x^2 + x + 1) \quad I = (x^2 + x + 1)$$

$x^2 + x + 1$ je maksimalen ideal (ker je polinom nerazcepen)

($(x^2 + x)$ ni maksimalen ker $x^2 + x = x(x+1)$ Trej $(x) \supseteq (x^2 + x)$
 večkratnik: x
 $x+1$
 $x^2 + x + 1$
 $x^2 + x$
 $x^2 + x + 1$

elementi tega polja so $p(x) + I$

$$p(x) + I = q(x) + I \Leftrightarrow p(x) - q(x) \in I$$

st $(p(x)) \geq 2$

$$p(x) = \underbrace{\alpha(x) \cdot (x^2 + x + 1)}_{\in I} + q(x)$$

$$\Rightarrow F = \mathbb{Z}_2[x] / (x^2 + x + 1) = \{0 + I, 1 + I, x + I, x + 1 + I\}$$

$$= \{0, 1, \bar{x}, \bar{x} + 1\} \cong \mathbb{Z}_2$$

$\bar{x}$ je nida $x^2 + x + 1$ nad F

$$\begin{aligned} \bar{x}^2 + \bar{x} + 1 &= (x + I)^2 + (x + I) + 1 + I = \\ &= (x^2 + x + 1) + I = I = 0 + I \end{aligned}$$

+	0	1	$\bar{x}$	$\bar{x} + 1$
0	0	1	$\bar{x}$	$\bar{x} + 1$
1	1	0	$\bar{x} + 1$	$\bar{x}$
$\bar{x}$	$\bar{x}$	$\bar{x} + 1$	0	1
$\bar{x} + 1$	$\bar{x} + 1$	$\bar{x}$	1	0

•	0	1	$\bar{x}$	$\bar{x} + 1$
0	0	0	0	0
1	0	1	$\bar{x}$	$\bar{x} + 1$
$\bar{x}$	0	$\bar{x}$	$\bar{x} + 1$	1
$\bar{x} + 1$	0	$\bar{x} + 1$	1	$\bar{x}$

$$\bar{x}^2 + 2\bar{x} + 1$$

$$\bar{x} \cdot \bar{x} = x^2 + I$$

$$\begin{aligned} x^2 : (x^2 + x + 1) &= 1 \\ -x^2 - x - 1 & \\ \hline -x - 1 & \\ x + 1 & \end{aligned} \quad \begin{aligned} x^2 + 1 \\ \hline x + 1 = x \end{aligned}$$

Pokaži da je F (prava strana)

Razpadna polje $x^2+x+1 \in \mathbb{Z}_2[x]$

$\bar{x}$ je nicle

Najti mereno vse nicle

Možnosti $\bar{x}$ in $\bar{x}+1$

$$f(\bar{x}+1) = \bar{x} + \bar{x} + 1 + 1 = 0$$

Podoben je stopnja 2, torej ima največ dve
nicli $\Rightarrow$ našli smo vse nicle $\Rightarrow$

$\mathbb{Z}_2(\bar{x}, \bar{x}+1)$ je razpadno polje

//

$$\mathbb{Z}_2(\bar{x}) = F \quad \text{po definiciji } F$$

Naj bo $g(x) \in \mathbb{Z}_p[x]$ nerazcepen stopnje n
 pri čemer da $\underbrace{GF(p^n)}_{\substack{\text{končno polje} \\ \text{s } p^n \text{ elementi}}} = \frac{\mathbb{Z}_p[x]}{(g(x))}$

2) pokaži $g(x) \mid x^{p^n} - x$

$GF(p^n)$ je razpadno polje $x^{p^n} - x$

$$x^{p^n} - x = \prod_{a \in GF(p^n)} (x - a)$$

Primer:

$$GF(2^2) = \{1, 0, a, a+1\}$$

$$a = \bar{x}$$

$$x^4 - x = x \cdot (x-1) \underbrace{(x-a)(x-(a+1))}_{x^2+x+1} \text{ nad } F$$

$$x^4 - x = x(x-1)(x^2+x+1) \text{ nad } \mathbb{Z}_2$$

1)

elementy F so oblike: $p(x) + I$
 $\deg(p(x)) < n$

$$a_0 + a_1 x + \dots + a_{n-1} x^{n-1} + I$$

$$\text{so elementi } \Rightarrow |F| = p^n$$

$$\text{Po teoriji: } F \cong GF(p^n)$$

□

$$2) \quad \bar{x} \text{ je ničla } \frac{\text{ker}}{Y} g(x+I) = g(x) + I = I = 0$$

$$x^{p^n} - x = \prod_{a \in F} (x - a)$$

$$\bar{x} \text{ je ničla v } F, \text{ ~~ker~~ od } g(x) \text{ in } x^{p^n} - x$$

če $g(x) \nmid x^{p^n} - x$ potem sta si tuji

$$\exists k(x), l(x) \in \mathbb{Z}_p[x] \text{ da } g(x)k(x) + l(x) \cdot (x^{p^n} - x) = 1$$

verifikiramo $\bar{x}$

$$\underbrace{g(\bar{x})}_{0} k(\bar{x}) + l(\bar{x}) (\underbrace{\bar{x}^{p^n} - \bar{x}}_0) = 1$$

$$0 = 1 \quad \times$$

Pokazi

$$a) GF(8) = \mathbb{Z}_2[x] / (x^3 + x + 1)$$

$$b) GF(9) = \mathbb{Z}_3[x] / (x^2 + 1)$$

$$c) GF(16) = \mathbb{Z}_2[x] / (x^4 + x + 1)$$

7) Poišči, kdo $x^8 - x$ kot produkt polinomov iz $\mathbb{Z}_2[x]$

$GF(8)$ je razpadno polje $x^8 - x$
 vse sledi iz prejšnje naloge, samo
 nerazcepnost moramo preveriti

a) $x^3 + x + 1$ če je razcepen ima ničlo

$$0: 0 + 0 + 1 = 1$$

$$1: 1 + 1 + 1 = 1 \quad \text{ne j n ničlen}$$

$$I = x^3 + x + 1$$

$$f(x) + I = \overline{f(x)}$$

$$(\overline{x^2 + 1})^{-1}$$

$$(x^2 + 1, x^3 + x + 1) = 1 \quad \in I$$

$$1 = s(x)(x^2 + 1) + t(x)(x^3 + x + 1) \in \mathbb{Z}_2[x]$$

$$\forall \mathbb{Z}_2[x] / I \quad 1 = \overline{s(x)} \cdot \overline{x^2 + 1}$$

c) Vemo od prej da je nerazcepen
 poiščimo inverz

20

$$x^8 - x = x(x^7 - 1) = x(x-1)(x^6 + \dots + 1)$$

$$2.4) \mid x^{p^n} - x$$

3 razcepi (ker je $n=3$)
vemo iz a. razloga

$$(x^6 + x^5 + x^4 + x^3 + x^2 + x + 1) : (x^3 + x + 1) = x^2 + x^2$$

$$\begin{array}{r} x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 \\ - (x^3 + x + 1) \cdot x^3 \\ \hline x^5 + x^4 + x^2 + x + 1 \\ - (x^3 + x + 1) \cdot x^2 \\ \hline x^5 + x^4 - x^2 + x + 1 \\ - (x^3 + x + 1) \cdot x^2 \\ \hline x^4 - x^3 - x^2 + x + 1 \end{array}$$

Ker ima $x^8 - x$ 8 različne ničle in se
e delitelj je še ena ničla
 ~~x^3~~

$$x^8 - x = x(x-1)(x^3 + x + 1)(x^3 + x^2 + 1)$$

9,5
Naj bo $[L:K] = 2$. Pokaži da je $L \supseteq K$ normalna

Vzemimo nek polinom stopnje 2

$$(x-a)(x-b) = x^2 - x(a+b) + ab$$

Recimo da $a \in K$ $b \in L-K$

$a+b$ mora biti nad K
 $d = ab$ mora biti nad K

$$b = a - c \in K \quad \text{---}$$

Kdaj je razširitev normalna?

• L je razpadno polje $f(x) \in K[x]$

• če $f(x) \in K[x]$ nerazc in ima ničlo v L ,
razpade nad L

Doloci ali je naslednja razširitev
polja $\mathbb{Q}$ normalna

Koristna
naloge

a) $\mathbb{Q}(\sqrt{2}, i)$

b) $\mathbb{Q}(\sqrt[4]{2})$

c) $\mathbb{Q}(\sqrt[3]{2}, i)$

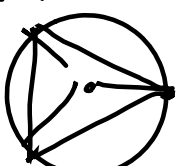
a) $f_A = (x^2 - \sqrt{2})(x+1)$

$$\mathbb{Q}(\sqrt{2}, -\sqrt{2}, i, -i) = \mathbb{Q}(\sqrt{2}, i)$$

b) $g_A = x^4 - 2 = (x - \sqrt[4]{2})(x + \sqrt[4]{2})(x - i\sqrt[4]{2})(x + i\sqrt[4]{2})$

$\mathbb{Q}$ razcepi v $\mathbb{Q}$, ima n:le v $\sqrt[4]{2}$ v L
in ima kompleksne n:le $\Rightarrow$
ne razpade na linearne faktorje $\Rightarrow$
razširitev ni normalna

c) $h_A = (x^3 - 2)(x+1) =$

 $(x - \sqrt[3]{2})(x - (\frac{1}{2} + \frac{\sqrt{3}}{2}i)\sqrt[3]{2})(x - (\frac{1}{2} - \frac{\sqrt{3}}{2}i)\sqrt[3]{2})$

↓

$\frac{\sqrt{2}}{2} + \frac{\sqrt{6}}{2}i, \frac{\sqrt{2}}{2} - \frac{\sqrt{6}}{2}i, \frac{\sqrt{2}}{2} + \frac{\sqrt{6}}{2}i, \frac{\sqrt{2}}{2} - \frac{\sqrt{6}}{2}i$

ker n: $\sqrt{3}$ potem
leži v

Baza F nad $\mathbb{Q}$

$$\{1, \sqrt[3]{2}, \sqrt[3]{4}, i, i\sqrt[3]{2}, i\sqrt[3]{4}\}$$

Reimo da $\sqrt{3} \in F \Rightarrow$

$$\sqrt{3} \in \mathbb{Q}(\sqrt[3]{2})$$

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{3}) \subseteq \mathbb{Q}(\sqrt[3]{2})$$

1
2
3

2/3
✗

Al: f razširitev $\mathbb{Z}_3(x^3) \subseteq \mathbb{Z}_3(x)$ normalna

$\mathbb{Z}_3(x)$ - polje racionalnih funkcij nad $\mathbb{Z}_3$
od spr. x

$$\frac{x^3 + x^6}{2x^3 - 1} \in \mathbb{Z}_3(x^3) \subseteq \mathbb{Z}_3(x)$$

$$f(t) \in \mathbb{Z}_3(x^3)[t]$$

$$f(t) = t^2 + \frac{x^3 + 1}{x^6}t + \frac{x^3 + 1}{x^3 + x^6}$$

$$\mathbb{Z}_3(x) = \mathbb{Z}_3(x^3)(x)$$

$$f(t) = t^3 - x^3 \in \mathbb{Z}_3(x^3)[t]$$

$$f(x) = 0$$

$$[\mathbb{Z}_3(x) : \mathbb{Z}_3(x^3)] \leq 3$$

$$f(t) = t^3 - x^3 = (t - x)^3$$

nima ničle v $\mathbb{Z}_3(x^3)$ in je
nerazcepen

$$\rightarrow = 1 \text{ ali } 3 \text{ (ker ne more biti 2)} \\ \text{in } \neq 1 \Rightarrow = 3$$

$\mathbb{Z}_3(x)$ je razpadno polje za

$$f(x) = t^3 - x^3 \Rightarrow \text{to je normalna razširitev}$$

$$\mathbb{Z}_3(x^3)(x) = \mathbb{Z}_3(x^3, x) = \mathbb{Z}_3(x)$$

④ Poišči primitivni element razšir.

a) $\mathbb{Q}(\sqrt{2}, \sqrt{3}) \supseteq \mathbb{Q}$

b) $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}) \supseteq \mathbb{Q}$

⑤ Poišči, pona a, b alg., nerez. in

$\mathbb{Q}(a, b) \neq \mathbb{Q}(a+b)$

Navedi $\alpha \in \mathbb{Q}$ da $\mathbb{Q}(a, b) = \mathbb{Q}(a, \alpha b)$

izpeljava

$\mathbb{Q}(\alpha, \beta) = \mathbb{Q}(\beta + c\alpha)$, kjer $c \in \mathbb{Q}$,

$c \neq c_{ij} = \frac{\beta_i - \beta_1}{\alpha_j - \alpha_1} \quad j \neq 1$

kjer so $\beta = \beta_1 \dots \beta_n$ so ničle minimalnega polinoma za β in $\alpha = \alpha_1 \dots \alpha_m$ ničle minimalnega polinoma za α

a) $\mathbb{Q}(\sqrt{2}, \sqrt{3})$

$p(x) = x^2 - 2 \quad f(x) = x^2 - 3$

ničle: $\sqrt{2}, -\sqrt{2} \quad \sqrt{3}, -\sqrt{3}$

$C = \left\{ 0, \frac{-2\sqrt{3}}{2\sqrt{2}} \right\} = \left\{ 0, \frac{\sqrt{3}}{\sqrt{2}} \right\}$

Možni primitivni elementi $\mathbb{Q} - C = \mathbb{Q} - \{0\}$
(konstanta pri vsakem ki je v merodelnem $\sqrt{3} + c\sqrt{2}$)

b) $\mathbb{Q}(\sqrt[4]{2} + \sqrt{3}, \sqrt{5})$

$p(x) = x^2 - 5 \quad f(x) =$

$\beta_1 = \sqrt{5} \quad \beta_2 = -\sqrt{5}$

$\mathbb{Q}(\sqrt{2}, \sqrt{3}) \supseteq \mathbb{Q}$

4 Galoisova razširitev (normalna, končna, separabilna)

$\sigma \in \text{Aut}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}) = \text{Gal}(E/\mathbb{Q})$

$\sigma(1) = 1$

$\sigma\left(\frac{p}{q}\right) = \frac{p}{q}$ za $\forall \frac{p}{q} \in \mathbb{Q}$ (ker ohranja deljenije in sestevnje)

$\sigma \in \text{Gal}(E/\mathbb{Q})$

$\sigma(\sqrt{2}) = \pm\sqrt{2}$

$\sigma(\sqrt{3}) = \pm\sqrt{3}$

≤ 4 avtomorfizmov

vemo moč razširitve $= 4 = |\text{Gal}(E/\mathbb{Q})|$

$\Rightarrow$ vse te možnosti so avtomorfizmi

$\sigma(2+\sqrt{3}) = \sigma(2) + \sigma(\sqrt{3})$ je oblike $\pm\sqrt{2} \pm \sqrt{3}$

f naj bo minimalni polinom za $\alpha = \sqrt{2} + \sqrt{3}$

$f(\alpha) = 0$

$\sigma(f(\alpha)) = 0$ ničle $f(x)$:

$f(\sigma(\alpha)) = 0 \quad \sqrt{2} + \sqrt{3}, -\sqrt{2} + \sqrt{3}$

$\sqrt{2} - \sqrt{3}, -\sqrt{2} - \sqrt{3}$

Ker obstaja avtomorfizem ki slika $\sqrt{2} + \sqrt{3}$ v eno od teh ničel.

lahko bi bilo tudi več ničel, ampak je minimalni polinom stopnje 4

$c \neq \frac{\alpha_i - \alpha}{\beta_j - \beta} = \frac{\alpha_i - \alpha}{-2\sqrt{5}}$

$C = \left\{ 0, \frac{\sqrt{2}}{\sqrt{5}}, \frac{\sqrt{3}}{\sqrt{5}}, \frac{\sqrt{2} + \sqrt{3}}{\sqrt{5}} \right\}$

$\mathbb{Q} - C = \mathbb{Q} - \{0\}$

$\alpha + \beta$ je primitiven

$\sqrt{2} + \sqrt{3} + \sqrt{5}$ je primitiven

⑤

$\mathbb{Q}(a, b) \neq \mathbb{Q}(a+b) \quad \mathbb{Q}(\sqrt{2}, -\sqrt{2}) = \mathbb{Q}(0)$

keje k_0

$a = \sqrt{2} - \sqrt{3}$

$\mathbb{Q}(a) \neq \mathbb{Q}(b) ?$

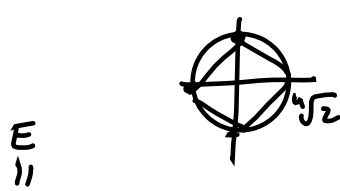
$b = \sqrt{3}$

$\mathbb{Q}(\sqrt{2} - \sqrt{3}, \sqrt{3}) \neq \mathbb{Q}(\sqrt{2})$

$\alpha_2 = \sqrt{2} + \sqrt{3}$

$\frac{\alpha_2 - \alpha}{\beta_2 - \beta_1} = \frac{2\sqrt{3}}{-2\sqrt{3}} = -1$

$$f(x) = x^4 - 2 = (x - \sqrt[4]{2})(x + \sqrt[4]{2})(x + i\sqrt[4]{2})(x - i\sqrt[4]{2})$$



$$\mathbb{Q}(\sqrt[4]{2}, i) \supseteq \mathbb{Q}(\sqrt[4]{2}) \supseteq \mathbb{Q}$$

$\underbrace{\hspace{1.5cm}}_2 \quad \underbrace{\hspace{1.5cm}}_4$
 $\underbrace{\hspace{3.5cm}}_8$

Ali je to razširitev galoisova? Ja

1) $\text{Gal}(E/\mathbb{Q}) = \text{Aut}(E)$ ← ker so racionalna števila

2) $\text{Gal}(\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}) = ? = \text{Aut}(\mathbb{Q}(\sqrt[4]{2}))$ negibna

$$\text{Gal}(F/K) = \{ \sigma \in \text{Aut}(F); \sigma(k) = k \forall k \in K \}$$

ko je ne delni. $\mathbb{Q}$ je Gal = Aut

2) i) $\sqrt[4]{2} \mapsto \sqrt[4]{2}$ $x^4 - 2 = (x - \sqrt[4]{2})(x + \sqrt[4]{2})(x^2 + \sqrt{2})$

ii) $\sqrt[4]{2} \mapsto -\sqrt[4]{2}$ Štela je deljena z enim $\Rightarrow$ 2 možnosti

Base $\{1, \sqrt[4]{2}, \sqrt[4]{4}, \sqrt[4]{8}\}$

u bistvu se ne vemo da to obstaja, da je avtomatično!

$$\sigma: \sqrt[4]{2} \mapsto -\sqrt[4]{2}$$

$$\sigma(\sqrt[4]{4}) = \sigma(\sqrt[4]{2})\sigma(\sqrt[4]{2}) = \sqrt[4]{4}$$

$$\sigma(\sqrt[4]{8}) = \sigma(\sqrt[4]{4})\sigma(\sqrt[4]{2}) = -\sqrt[4]{8}$$

Preveriti moramo: $\sigma(ab) = \sigma(a)\sigma(b)$

$$a, b \in \{1, \sqrt[4]{2}, \sqrt[4]{4}, \sqrt[4]{8}\}$$

$$\alpha = \sqrt[4]{2}$$

$$\sigma(\alpha^k \alpha^m) = \sigma(\alpha^{k+m}) = (-1)^{k+m} \alpha^{k+m}$$

$$|\text{Gal}(\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q})| = 2 \neq 4$$

$\Rightarrow$ ni galoisova ← št min polinoma

1) $\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q}$ je normalna ker je razpadno polje polinoma
 št razširitve = $|\text{Gal}(\text{razširitev})|$

$$f(x) = x^4 - 2$$

$$r_1, r_2, r_3, r_4 \text{ ničle}$$

1) $G = \text{Gal}(\dots) \leq S_n$ ← Galoisova grupa z n ničlami: je vedno

2) G deluje tranzitivno na $\{r_1, \dots, r_n\}$ podgrupa S_n ima eno orbito ki je vse

$$\forall i, j. \exists \sigma \in G. \sigma(r_i) = \sigma(r_j)$$

ker ima orbito velja, da je moč vsaj 4 (v splošnem vsaj 2) (ker katero koli ničlo lahko preslikamo v katero koli ničlo)

Vemo da je grupa D_8

Vemo $D_8 \leq S_n$ ker je grupa simetrije, je vsake druge podgrupa množice S_n izmatna v S_n

id $r_1 + r_3 = 0$ opazimo da to velja med ničlami
 $r_2 + r_4 = 0$

$$\{r_1, r_3\} \rightarrow \{r_1, r_3\}$$

$$\rightarrow \{r_2, r_4\}$$

$$\left\{ \begin{array}{l} r_1, r_3 \mapsto r_1, r_3 \\ r_2, r_4 \mapsto r_2, r_4 \end{array} \right\} \quad 2 \cdot 2 \text{ možnosti}$$

$$\left\{ \begin{array}{l} r_1, r_3 \mapsto r_2, r_4 \\ r_2, r_4 \mapsto r_1, r_3 \end{array} \right\} \quad 2 \cdot 2 \text{ možnosti}$$

$\Rightarrow$ 8 kandidatov.

ker je to maksimalna število so to vse možnosti

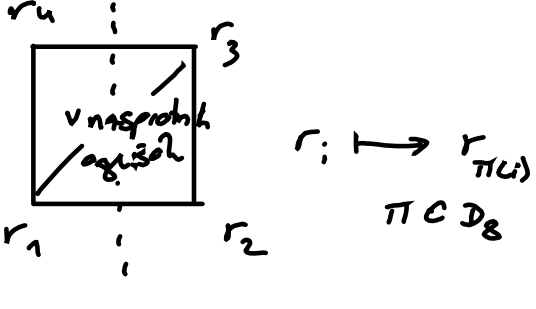
$$\sigma_1: r_1 \mapsto r_2$$

$$r_3 \mapsto r_4$$

$$r_2 \mapsto r_1$$

$$r_4 \mapsto r_3$$

Vemo da je simetrija



Definirali smo ne ničel, preveriti moramo na bazi

$$r_1 \mapsto r_2 \quad \sqrt[4]{2} \mapsto \sqrt[4]{2} \quad \sigma(a) = ia$$

$$r_2 \mapsto r_3 \quad ia \mapsto -a \quad \sigma(ia) = -a$$

$$\sigma(i)\sigma(a)$$

$$-a = \sigma(i) \cdot ia \quad / a^{-1}$$

$$-1 = \sigma(i) \cdot i \quad / i^{-1}$$

$$i = \sigma(i) \quad / i^{-1}$$

$$L_1 = \mathbb{Q}(i)$$

$$L_2 = \mathbb{Q}(\sqrt{2})$$

$$L_3 = \mathbb{Q}(i\sqrt{2})$$

$$[E:L] = [E:L_2] = [E:L_3] = 4$$

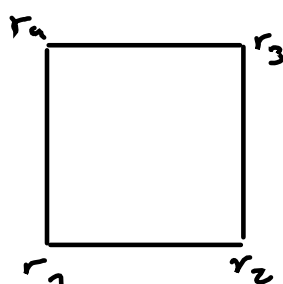
$$\text{paži: } \text{Gal}(E/L_1), \text{Gal}(E/L_2) \text{ in } \text{Gal}(E/L_3)$$

$$\begin{array}{c} \mathbb{Q} \subseteq L_1 \subseteq \mathbb{Q}(\sqrt{2}, i) \\ \underbrace{\hspace{10em}} \\ \text{Gal} \\ \Rightarrow \underbrace{\hspace{3em}} \underbrace{\hspace{3em}} \\ \quad ? \quad \text{Gal} \end{array}$$

$$\text{Vemo: } |\text{Gal}(E/L_1)| = [E:L_1]$$

$$\begin{array}{c} \mathbb{Q} \subseteq L_1 \subseteq \mathbb{Q}(\sqrt{2}, i) \\ \underbrace{\hspace{3em}} \\ 2 \\ \underbrace{\hspace{10em}} \\ 8 \\ \underbrace{\hspace{3em}} \\ 4 \end{array}$$

$$\text{Gal}(E/L_1) \cong ? \leq D_8$$



← n:če iz prejšnje velja

Podgrupe reda 4?

$$1) \underbrace{\{id, r_1, r_2, r_3\}}_{G_1} \cong C_4$$

$$2) \underbrace{\{id, r_1^2, r_2, r_2^2\}}_{G_2} \cong K_4 = \mathbb{Z}_2 \oplus \mathbb{Z}_2$$

$$3) \underbrace{\{1, (r_2, r_4), (r_1, r_3), (r_1, r_3)(r_2, r_4)\}}_{G_3} \cong K_4$$

$$E^{G_1} = \{e \in E : \sigma(e) = e \forall \sigma \in G_1\}$$

zaključimo od teh grup so realne tečke $i, \sqrt{2}$ in $i\sqrt{2}$

$$G_1: \sqrt[4]{2} \rightarrow i\sqrt[4]{2} \rightarrow -\sqrt[4]{2} \rightarrow -i\sqrt[4]{2}$$

$$\text{Gal}(E/L_1): \sigma(i) = i$$

$$\begin{array}{l} \{r_1, r_3\} \rightarrow \{r_1, r_3\} \\ \quad \searrow \{r_2, r_4\} \end{array}$$

$$\begin{array}{l} r_1 = \sqrt[4]{2} \\ r_2 = i\sqrt[4]{2} \\ r_3 = -\sqrt[4]{2} \\ r_4 = -i\sqrt[4]{2} \end{array}$$

$$r_1 \mapsto r_2 \mapsto r_3 \mapsto r_4 \mapsto r_1$$

$$\sigma(i) = \frac{\sigma(r_2)}{\sigma(r_1)} \quad \text{ker } i = \frac{r_2}{r_1}$$

$$\sigma(i) = \frac{r_3}{r_2} = \frac{-\sqrt[4]{2}}{i\sqrt[4]{2}} = \frac{-1}{i} = i$$

$$L_2$$

$$r_1 r_3 = -\sqrt{2}$$

$$r_2 r_4 = -\sqrt{2}$$

$$(r_1 r_4)(r_2 r_3)(\sqrt{2}) = -\sqrt{2}$$

...delo mame

$$\text{ne Alesina} \Rightarrow L_2 \sim G_3 \\ L_3 \sim L_2$$

$$G \triangleleft (E/L_1)$$

$$E = L_1$$

$$\{e \in E: \sigma(e) = e, \forall \sigma \in G \triangleleft (E/L_1)\} = Q(;) \quad C_n$$

Vemo : je notri:
in st nad $\emptyset$ robi bits 2 $\Rightarrow Q(2)$

$$[E:L_1] = 4 \Rightarrow L_1:Q = 2$$

$$f(x) = x^4 + bx^2 + c \in \mathbb{Q}[x]$$

$$\text{nick: } y = x^2: y^2 + by + c$$

$$\text{nick: } \pm \alpha \quad \pm \beta$$

$$\sigma(\pm \alpha) \in \{\pm \alpha\} \cup \{\pm \beta\}$$

$$\text{poderia ser } \sigma(\pm \beta)$$

$$|G| \leq 8$$

$$G \leq D_8$$

$$\begin{aligned} &\text{se usarmos nick racional } \Rightarrow \\ &E = \mathbb{Q} \Rightarrow G = \{id\} \end{aligned}$$

$$\gamma = \alpha\beta \quad \leftarrow \text{niczy}$$

$$\gamma^2 \in \mathbb{Q} \quad \gamma^2 = \alpha^2\beta^2 = c$$

$$f(x) = (x^2 - \alpha^2)(x^2 - \beta^2) =$$

γ jest niepodzielne $x^2 - c$

$$\sigma(\gamma) = \pm \gamma$$

orbita γ $|G \cdot \gamma| = [G : G_\gamma]$ $\swarrow$ stabilizator
kaj jest $\text{st}(\gamma)$

id

$$\alpha \mapsto \beta \Rightarrow \beta \mapsto \alpha$$

$$\alpha \mapsto -\beta \Rightarrow \beta \mapsto -\alpha$$

produkt lech dach

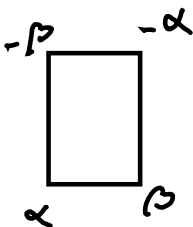
$$G_\gamma = K_u \cap G \quad \leftarrow \text{istnieje drugie } K_u$$

$$1) \text{ Czy } \gamma \in \mathbb{Q} \Rightarrow \sigma(\gamma) = \gamma$$

$$|G \cdot \gamma| = 1 \Rightarrow |G| = |G \cap K_u| \Rightarrow G \subseteq K_u$$

2)

$$\sigma \in G_{\alpha^2} \Rightarrow \sigma(\alpha) = \pm \alpha \quad \sigma(\beta) = \pm \beta$$



zaczynając z ujemne

$$\langle z, r^2 \rangle = K_u$$

$$|G_{\alpha^2}| = [G : G_{\alpha^2}]$$

$$\parallel$$

$$1 \Leftrightarrow \alpha^2 \in \mathbb{Q}$$

podobnie tutaj $G \subseteq K_u$

3) Kde j $G \subseteq C_u$?

$$\delta = \alpha^3\beta - \beta^3\alpha \quad C_u \text{ stabilizuje } G_\delta \subseteq C_u$$

$$|G_\delta| = 1 \Leftrightarrow \delta \in \mathbb{Q} \Leftrightarrow G \subseteq C_u$$

$$\delta^2 = \alpha^4\beta^2(\alpha^2 - \beta^2)^2 = c(\alpha^2 - \beta^2)^2$$

$$D = b^2 - 4c = (\alpha^2 - \beta^2)^2 \quad \leftarrow \text{razem}$$

$$\delta^2 = c(b^2 - 4c) \in \mathbb{Q}$$

nic nie
wadrat

$X^4 + 4X^2 + 2$ je nerazcepljen

polj nerazcepljen $\Rightarrow$ Gal deluje tranzitivno

$$D = 16 - 8 = 8$$

$c \cdot D = 16$ je popolnkvadrat

$$\Rightarrow Gal \subseteq C_4 \Rightarrow Gal = C_4$$

Naj bo $f(x) \in \mathbb{Q}[x]$ nerazc. pol. 3

ki ima eno realno ničlo

potem $G(f) \cong S_3$

$a \in \mathbb{R}$ nida

3 nide $\Rightarrow$

$$G \subseteq S_3$$

$$\mathbb{Q} \subseteq \mathbb{Q}(a) \subseteq E$$

$$\underbrace{\hspace{1cm}}_3 \quad \underbrace{\hspace{1cm}}_2$$

$$|G| = 6$$

$$\Rightarrow G \cong S_3$$

$f(x) = x^3 + ax^2 + bx + c \in \mathbb{Q}[x]$ nerazcepen

$$x_{1,2} = \frac{-b \pm \sqrt{D}}{2} \text{ za kvadratne}$$

$$(x_1 - x_2)^2 = D$$

$$D = ((x_1 - x_2)(x_1 - x_3)(x_2 - x_3))^2 \dots \text{diskrimi-}$$

nanten simetrični polinom od x_1, x_2, x_3 . kubične enačbe

za x_1, x_2, x_3 nide f(x)

$$\rightarrow g(x_1, x_2, x_3) = g(x_{\sigma(1)}, x_{\sigma(2)}, x_{\sigma(3)})$$

Osnovni izrek o sim. polinomih

vseh simetričnih polinomov se da izraziti

$$x_1 + x_2 + x_3$$

preko osnovnih

$$x_1 x_2 + x_1 x_3 + x_2 x_3$$

sim. polinomov

$$x_1 x_2 x_3$$

$$D = 18abc + a^2b^2 - 4b^3 - 4a^3c - 27c^2$$

$$\text{če } \sqrt{D} \in \mathbb{Q} \Rightarrow \sqrt{D} \rightarrow \sqrt{D}$$

$$f(x) = x^3 - 2$$

$$D = -108$$

n: kwadrat
rac. sterile

$\Rightarrow$

$$G \cong S_3$$

$$f(x) = x^3 - 4x + 2$$

$$D = 208$$

3 realne i 1 ciekie apak $G \cong S_3$

$$g(x) = x^3 - 3x + 1 \quad \text{nerazgen}$$

$$D = 81$$

kwadrat realnys

sterile

$$\Rightarrow G \cong C_3$$

$$f(x) \in \mathbb{Q}[x]$$

nerazc pol. st. 5

G vsebuje 5-cikel

$$|G \cdot x_1| = 5 = [G : G_{x_1}] = 5$$

$$5 \mid |G|$$

$$\exists \sigma \text{ reda } 5 \text{ v } G \leq S_5$$

σ je 5-cikel

$$\sigma = (x_1, x_2, x_3, x_4, x_5)$$

$$\sigma^2 = (x_1, x_3, x_5, x_2, x_4)$$

S_5 je generirano s (12345)