

M. Bršsar, Uvod v algebro, osnutki  
Inovaze  
učbenika

$(S, \circ)$  • je binarna operacija na S

namesto  $\circ(a,b)$  pišemo  $a \circ b$   
 $S \times S \rightarrow S$

$\mathbb{Z}$  z operacijima sestavljanja in množenja

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

$$|S| = n$$

Koliko je binarnih operacija

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

- je asociativna če

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

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

V splošnem: indukcija

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

Treba dokazati za  $3 \leq k \leq n$  faktorjev

$n \geq 4$

Poglejmo si zadjo uporabo operacije

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

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

Rečimo da je  $(a_1 \cdot \dots \cdot a_l)$  oblikovan v  $a_1(a_2(\dots \cdot a_l)))$  in tudi drugačno oblikovan

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

$$a_1 \cdot (a_2(a_3 \cdot \dots \cdot a_n))$$

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

Monoid je polgrupa z enoto

$$1 \cdot s = s \cdot 1 = s \quad \forall s \in S$$

(enota mora biti obojestranska)

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

če je  $l$  lev: inverz za  $S$  in  
 $r$  desn: inverz za  $s$  sta enake

$$ls = 1 = sr$$

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

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

Naj bo  $S$  končen monoid

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

Dokaži da je  $S$  obrnljiv

Vemo:  $f s = 1$  za nek  $t \in S$

$s^0, s, s^2, s^3, \dots$  v tem zaporedju so ponavljanja

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

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

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

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

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

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

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

$$s^m = 1$$

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

$s^{m-1}$  je desni inverz

Navedi prime monoide  $\mathbb{S}$  in  
elemente  $SES$ , k-ima lev: inverz, nema  
pa desnege

Navedi vrednost u razloženje lva: ~~inverz~~ inverz

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

$\mathcal{F}(\mathbb{N})$

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

$$g \begin{cases} 2n \mapsto n \\ 2n+1 \mapsto n \end{cases}$$

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

$$\stackrel{\text{def}}{=} f \circ g(x) = f(g(x)) = x \quad \checkmark$$

$h \circ f(x) = x$   $n$ : desnega konste  
lva rezultira lva

$f: n \mapsto 2n+2$

Naj bo \$(S, \cdot)\$ monoid. A1; sta elemente \$x, y \in S\$ dobjiv, ce ~~nu~~, je dobjiv element

$$a) x \cdot y \cdot x$$

$$b) x \cdot y$$

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

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

deshi in levi inverz

$$\underbrace{y \cdot x \cdot f} = f \cdot x \cdot y$$

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

$$(x + x)y = y \cdot \underbrace{f \cdot x}_{y \cdot x \cdot f} = 1$$

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

Pratipomer

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

$$f: 2n \mapsto n$$

$$2n+1 \mapsto 0$$

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,  $a, b \in G$

$$\forall a, b \in G. ax = b \text{ in } xa = b \text{ enotno resljivi}$$

$$\tilde{a}^{-1} / ax = b \qquad xa = b / \tilde{a}^{-1} \begin{matrix} \text{due} \\ \text{razlioni} \end{matrix} \\ x = \tilde{a}^{-1}b \qquad \qquad \qquad x = b\tilde{a}^{-1} \begin{matrix} \text{enotno} \\ \text{resljivo} \end{matrix}$$

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

z deljenjem (torej  $\forall a, b \in S$ . sta enotni  
 $ax = b$  in  $xa = b$  sta resljivi)

Pokaži da je  $S$  grupa

$$ax = b \quad \text{vezemo } b = 1$$

$$ax = 1 \quad xa = 1$$

$x = \tilde{a}^{-1}$  a ima levi in desni trejje  
obnljiv. Zapišemo na  
trejje ima mrež

Ampak n: nej ne da ima  $S$  enoto

Moramo pokazati da ima  $S$  enoto

$$b = a$$

$$ax = a \quad xa = a$$

$$x = 1_a \quad \underline{\text{desna enota}}$$

$$\forall b : \underline{b \cdot 1_a = b}$$

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

$$1_a = x b = by$$

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

$$a \circ x = b$$
$$y \circ a = b$$

$$x \circ b = a$$
$$y \circ a = a$$

jje enecte regiiv  
X... desr: invza  
Y... lev: inv er a

$$b = t \circ a$$
$$b = x \circ a$$

inverzert

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

1je desna enote

$$b = a \circ t$$
$$\ker b = a \circ x$$

regiiv

$$y \circ l_a$$

$$l_a \circ b = l_a \circ a \circ t = a \circ t = b$$

Dokazi: da je vaške grupe s članki  
elementi Abelove

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

$$\text{Recimo da } ab \neq ba \in G$$

1)  $ab = 1$        $b$  je devojni inverz za  $a$  torej je inverz

2)  $ab = a$        $b = a^{-1}$  ~~je~~ torej  $b = a$

3)  $ab = b / b^{-1}$        $a = 1$  ~~je~~

4)  $ab = c$

enako velja za  $ba$

torej  $ba = c = ab$  ~~je~~

Tidlitter: V ~~grup~~<sup>tz</sup>  $x_y = 1$  sled  $yx = 1$ ,

le vælvelige grup: tz

$xyz = 1$  sled:  $zyx = 1$

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

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

4) G n; vælvelige, ampak

$$xyz = 1 \quad \cancel{zyx = 1}$$

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

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

Dokazi da liger vsele v grapi

a)  $\exists x. x^2 = 1$  akcelova

b) Ali je  $x^2 = a$  rešljive v vsaki grapi?

c) Ali je res  $x^2 = a$  v vsaki grapi: najvec 2 rešitv:

d) Ali je res  $x^2 = ax$  le eno rešitev

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

a)

$$a, b \in G$$

$$a^2 \circ b^2 = 1 \quad a \circ b = c$$
$$a \circ (a \circ b) \circ b = 1 \quad (a \circ b) \circ (a \circ b) = 1$$
$$a \circ (b \circ a) \circ b = 1$$

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

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

b) Ali je  $x^2 = a$  rešljive vedno

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

$$2 \cdot 3 = 3$$

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

c)  $x^2 = a$  najvec dve rešitvi?

$D_{2n}$  je grapa rotacij

Vseko zapisovanje za  $n \geq 2$  je pravipomer

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

## Simetrične grupe $S_n$

$\Pi \in S_n$  je sada oz. lih a če je produkt  
soda mnoge transpozicij

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

$$\Pi = \left( \begin{smallmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 4 & 0 & 5 & 1 & 2 & 7 \end{smallmatrix} \right)$$

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

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

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

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

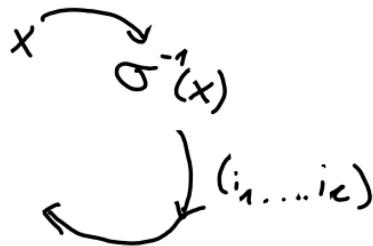
$$\text{če je } \sigma \text{ } n\text{-cikel} \Rightarrow \text{sgn}(\sigma) = (-1)^{n-1}$$

Naj bo  $\sigma \in S_n$ ,

Potem  $\forall k\text{-cikel } (i_1, \dots, i_k) \in S_n$

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

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



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

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

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

Definicija: Permutaciji  $\sigma, \sigma' \in S_n$  imata

enako zgradbo disjunktnih ciklov  
če sta  $\sigma$  in  $\sigma'$  produkta disjunktnih  
ciklov istih dolžin  $k_1, \dots, k_s$   $k_1 \leq k_2 \leq \dots \leq k_s$

np:

$$(1\ 2\ 3)(4\ 5\ 6)(7\ 8) \text{ in } (4\ 2\ 8)(8\ 1)(6\ 3\ 7)$$

Dokaz je sto  $\sigma$  i  $\sigma'$  konjugiran:

$\Leftrightarrow$  imete enako  $\text{arg} \rightarrow \sigma' = \sigma$

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

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

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

Vidimo da se ovi enoti delje

$\Leftarrow$  Recamo da

$$\begin{aligned}\sigma &= (i_1 \dots i_k) (j_1 \dots j_l) (\dots) \\ \sigma' &= (I_1 \dots I_{k'}) (\dots) \dots\end{aligned}$$

Deklinirajmo  $\pi$  de velja

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

$$\sigma' = (\pi(i_1), \dots, \pi(i_{k'})) (\dots)$$

$$\text{Vemotrag: } \sigma' = \pi(i_1 \dots i_{k'}) (\dots) \dots \pi^{-1}$$

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

Počišći sve permutacije  $\pi$ , ki kontinjuiraju  
 $\tau = (1 \ 2)$

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

za  $n \geq 2$

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

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

$$\pi(1) = 1$$

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

$$\pi(1) = 2 \quad \pi(2) = \cancel{1}$$

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

$$\pi_2 = \circ \quad \text{kojer } \circ \text{ ima nejedne}\text{ take v } 1, 2$$

Kako jo hje?

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

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

centralizator elementa  $(1, 2)$

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

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

dveletri u svakoj permutacijskoj grupi

Pokaži da lahko  $\pi \in S_n$  zapisemo kot produkt transpozicij oblike

$(k, k+n)$  kjer

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

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

Transpozicijo  $(i_1, i_2)$  zapisemo preko transpoziciji:

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

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

$$(i \ j)$$

$$j-i > 1$$

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

Transpozicije  $(k \ k+n)$  generirajo simetrično grupe

### 3. pooglajje

$H, K$  konen: podgrupi grupe  $G$

$$\text{Po kesi } |HK| = \frac{|H||K|}{|H \cap K|}$$

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

$$|hK| = |K|$$

Recimo da imamo m odsekov

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

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

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

$$H \cap K \leq H$$

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 grupe in  $H \leq G$

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

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

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

št. odsekov  $G$  po  $H$  je večji 3

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

Prvi odsek je gttovo  $H$

$$eH \Leftrightarrow aH \Leftrightarrow a \in H \quad \text{ali je oddel}$$

$$aH = bH = abH$$

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

Torej manj tri oddelki

$\Leftarrow$  imamo večji tri oddelki

$$aH \neq bH \neq H$$

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

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

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

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

$$a^2 = h k^{-1}$$

## Ciklične grupe

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

red: 0 1 2 6 4 3 12 2 12 3 4 6 12

## Lagrangeov izrek

Red podgrupe deli red grupe

Pokazi:  $\mathbb{Z}_n$  vsebuje podgrupo reda  $k$

$$\Leftrightarrow k|n$$

takške grupe je ena samo

$$n = k \cdot l$$

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

zakej n; druge podgrupe reda  $k$

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

$$H = \sum_{i=0}^k h_i, \dots, h_k \}$$

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

$$t \in \mathbb{Z}_n \text{ . red } t/k \Leftrightarrow tk = 0 \vee \mathbb{Z}_n$$

$$\text{torej } n/tk$$

$$k \cdot l/tk$$

$$l/t$$

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

$$\text{Torej } h_i \in \langle l \rangle \quad \text{Torej } H = \langle l \rangle$$

Pokazi 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  $\mathbb{Z}$ :

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

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

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

$\exists n > 0$  in  $n$  najmanjši pozitiven element  $H$

$$\text{Pokažimo } H = n\mathbb{Z}$$

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

$$k \in H, nk$$

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

$$d = \alpha n + \beta k \quad d < n$$
$$\in H \quad \in H$$

$$d \in H \neq$$

Doloci red od  $k \in \mathbb{Z}_n$

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

$$\begin{aligned} \text{red}(0) &= 1 & \text{red}(k) &= r \\ \text{red}(1) &= n & \text{je najmanje} \\ & & \text{takoto s.t. da } n | rk \end{aligned}$$

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

$$\begin{array}{l} n = g\alpha \\ k = g\beta \end{array} \quad g\alpha | r g\beta$$

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

$$\alpha | r\beta$$

$$r = \alpha$$

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

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

Ko sta  $n, k$  tega?

$\mathbb{Z}_2 \oplus \mathbb{Z}_3$       je ciklične  
 $\mathbb{Z}_2 \oplus \mathbb{Z}_2$       ni ciklične, ker  
 (1,1) generira celo grpo      reda 4

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

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

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

$$k(1,1) = (0,1)$$

$$S(1,1) = (1, 2)$$

$$G(1,1) = (0\ 0)$$

DN: Kde je  $Z_n \oplus Z_k$  akkorad

Naj bo  $G$  neskončna grupa.

Potem, da ima  $G$  neskončno mnogo podgrup

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

2) Če nima elementov neskončne reda

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

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

$\langle a \rangle$  je končna

in tako lahko nedajujemo

2. način

$\forall g \in G \quad \langle g \rangle$

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

Potem bi bila  $G$  končna unija končnih mnogic \*

Pokazi:

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

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

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

4) Al: imat u t grup: elemente

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

1) Recimo da je  $\cancel{\text{red}} \cancel{\text{kot}}$   $\overset{\text{red koren}}{\cancel{\text{kot}}}$

$$a^r = 1$$

$$2) \forall r, a^r \neq 1$$

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

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

črudi simetrije jeto enakost

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

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

$$b1 \cdot b^{-1} = bb^{-1} = 0$$

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

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

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

$$(ab)^r = 1 \quad \cancel{(ab)}^r = 1$$

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

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

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

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

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

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

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

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

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

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

$$a = 2 \quad b = 1$$

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

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

$\binom{n^2}{2}$  vseh možnosti.  $\binom{n^2}{2}$  lahko zavrsti  
1, 2 in 3 in greb same vase. Vecje podnebje.

Pokazi kako je grupa

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

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

---

G je generirana z  $A \subseteq G$

da vsak  $g \in G$  izjema

$$g: a_1^{e_1} \cdots a_n^{e_n} \quad g = a_1^{\pm 1} a_2^{\pm 1} a_3^{\pm 1} \cdots a_n^{\pm 1}$$

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

$$xy \in A^2 \quad A = [1, 4]$$

$$A^3 = [-8, -1] \quad A^{-1} = [-1, -\frac{1}{2}]$$

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

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

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

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

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

" "

1) Dolaci red podgrupe  $\leftarrow$  moć grupe generirane z A

$GL_n(\mathbb{C})$  generirane z metrikom

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

2) Opsiđi podgrupa 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 needed nij; h mnacic so  
kolobarj: za obicajno sestavljanje in  
mnocenje

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

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

c)  $\left\{ m+n\sqrt{2} \quad m, n \in \mathbb{Z} \right\}$

f)  $\left\{ p+q\sqrt{2} ; p, q \in \mathbb{Q} \right\}$

kernetekivno ✓ vse

$$\frac{m}{2n+1} + \frac{k}{2c+1} = \frac{m(2c+1) + k(2n+1)}{(2n+1)(2c+1)} = 0 \quad \checkmark$$

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

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

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

c)  $\frac{2n+1}{m} + \frac{2k+1}{c} = \frac{2nc+c+2km+m}{m.c} = \frac{2n+c+2km+m}{m.c} = \frac{2n+c}{m.c}$

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

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

$$= \cancel{mkt2cn} + \sqrt{2}(nk+mk) \quad \checkmark$$

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

$X$ -množica  $P(X)$  ... potencije množice

$$A, B \subseteq X$$

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

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

a) Pokazi, da je  $(P(X), +, \cdot)$  kolobar

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

$(P(X)$  je boolev kolobar, ker je  $\forall A \in P(X)$  idempotent ( $A^2 = A$ ))

b) Pokazi, da je  $\forall$  boolev kolobar komutativen in ima karakteristiko 2.  
 $(a+a=0 \text{ za } \forall a)$

c) notranje operacije oddite

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

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

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

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

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

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

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

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

b) Recimo  $a^2 = a$  za  $\forall a$  dokazi  $a+a=0$  komutativnes +

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

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

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

$$AB+BA = 0$$

$$B=A$$

$$AA+AA=0$$

$$A+A=0$$

$$AB = -BA$$

$$-BA = BA$$

$$AB = BA$$

idempotent:  $x^2 = x$

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

Najbo  $A \in M_n(\mathbb{R})$  metriken negativer negativer eig. Pötzl da  $A^2 = \lambda A$  zende  
 Poiszi bek dempotent, k*i*n: diagonal in ~~zugehörig~~<sup>k*i*n:</sup> patent, k*i*n: tridiagonale

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

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

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

$$c_1 a_1 + c_2 a_2 = 1$$

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

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

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

$$c_1 a_1 + c_2 a_2 = 0$$

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

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

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



1)  $x$  nilpotent keleber ja  $K$

rekursiv do je element  $1-x$  abrljiv

2)  $x, y \in K$ .  $1-xy$  je abrljiv  $\Leftrightarrow$   $\frac{1-yx}{1-xy}$  je abrljiv

3)  $x^n = 0$

$$\frac{1}{1-x} = \sum_{n=0}^{\infty} x^n = \underbrace{\sum_{i=0}^n x^{*i}}_{\text{inver } z} =$$
$$(1-x)(1+x+x^2+\dots+x^n) = 1$$

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

$$1 \cancel{x^n} = 1$$

\

$1-xy$  je abrljiv  $\Leftrightarrow \frac{1-yx}{1-xy}$  je abrljiv

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

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

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

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

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

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

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

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

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

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

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

# Algebra nad poljem

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

A je vektorski prostor nad F

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

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

Naj bo A končna razsežna algebra

Dokaz:

- Vsek neničlen element je bodisi delitelj niza, bodisi obrnjiv
- če ima  $a \in A$  levi ali desni inverz je obrnjiv
- če je 1 obseg je vsake algebra podobseg

Namig: Če je A n-razsežna  $\Rightarrow 1, a, \dots, a^n$  lin. neodvisni

a) ~~Naj~~ naj bo n tako da so

$1, \dots, a^{n-1}$  lin. neodvisni in  $a^n$  jeli...  
je

$$\lambda_0 + \lambda_1 a_1 + \dots + \lambda_n a_n = 0 \quad \cancel{\lambda_1, \dots, \lambda_n \neq 0}$$

potem  $\lambda_n \neq 0$

$$\lambda_n \neq 0 \Rightarrow$$

$$1 + \frac{\lambda_1}{\lambda_n} a_1 + \dots + \frac{\lambda_{n-1}}{\lambda_n} a_{n-1} = 0$$

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

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

a je obrnjiv

$$\lambda_0 = 0 \Rightarrow$$

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

Torej je a delitelj niza

b) By a me levi inverz

$$ba = 1$$

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

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

$$\hookrightarrow / \underbrace{\alpha_0 b + \alpha_1 + \dots + \alpha_n a^{n-1}}_{\text{in redvizi}} = 0$$

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

$\alpha_n \neq 0$  po predpostavke.

$\Leftrightarrow b$  je obanjiv poprejšnji teček

njen inverz

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

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

$$\cancel{b = a}$$
$$x = a$$
$$ab = 1 \quad \text{ok}$$

c) A je closed

B je closed

Naj  $b \in B$ ;  $b \neq 0$ : Dále  $\exists b^{-1} \in \underline{B}$

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

$X$  mnogoščice

$P: \{ \{x\}^c \mid x \in X \}$  podbase topologije  
končnih komplementov

$$P_X = \{X\}^c$$

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

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

$$U = \bigcap_{i=1}^n P_i$$



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

$$P_X + P_Y = X \text{ je potrjeno} \quad P \subseteq \mathcal{T}_{kk}$$

ocitno

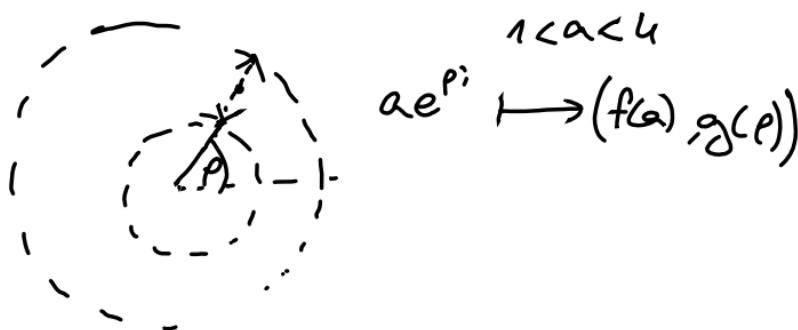
(4.5)

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

homeomorfen metriken

Produkt topologisch prosterav

$$(A, \tau_A) \times (B, \tau_B)$$



(4.8)

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

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

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

surj ✓

inj ✓



zweimal:

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

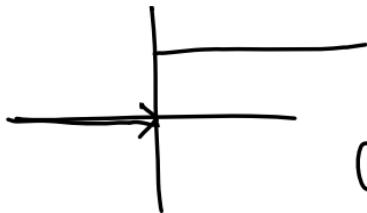
Homeomorfismen?

N:  $\{\text{en } j\}$  posieren drüg  $n_i$

invert  $n_i$ : zweimal

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

b)



Heaviside funktion

je zweimal

4.5  
V\_A padfester ( $X, \mathcal{T}_{kk}$ ) iste  $\mathcal{T}_{kk}$

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

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



z. B. kanten ... oder

z. A. neukanten:

(4.10.)

$$\mathbb{N}_{\geq 3} \xrightarrow{i} \mathbb{R}_{\text{cke}}$$

Vseka preslikava iz diskrete topologije  
je zvezna

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

Ali sl. ka odprt množico v odprte?

$$i^*(\{1\}) = \{1\} \text{ st. rej; ni odprt}$$

Vseka sl. ka bo zgr. k, ker je

vseka odprt množica sl. ka v zgr. b

NTSE: nedelje trdite so ekvivalentne

- $f$  je odprt vložitev

- $f$  je odprt zvezna injekcija

- $f$  je vložitev in  $f^*(A)$  je odprt

$$b) \quad Q \rightarrow R$$

$$i^*(\{g_j\}) = \{g_j\} \quad n: \text{adgets} \vee Q = ak$$

$\Rightarrow$  imm. visible

if ✓

wereest disk  $\rightarrow$  redish ✓

$$i^2 = j^2 = k^2 = -1 \quad \text{Kawernionsche}$$

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

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

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

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

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

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

Pošči vse reslike enačbe  $ix - xi = h$

2) Pošči vse reslike enačbe  $x^2 - 1 \in H$

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

4) Našlo, da  $h \in H \cap \mathbb{R}$ . Dokaži da je  
 ~~$h\bar{h} = h + \bar{h} = 0 \Leftrightarrow \exists x \in H \quad h \neq xh \quad h^2x = xh^2$~~

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

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

$\forall C:$   $\alpha = -(\bar{h}h)$  } viator izrek  
 $\beta = h \cdot \bar{h}$

Reimo de

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

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

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

$$\begin{aligned} \|h\|^2 &= \|\bar{h}\|^2 && \text{Ne sadi zme} \\ \|\bar{h}\|^2 & && \alpha \text{ in } \mathbb{C} \end{aligned}$$



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

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

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

$$-(h + \bar{h}) \quad ||h||^2$$

$$h^2 = -||h||^2$$

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

Scanno  $x, h$  ne komutieren

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

bereits  $\alpha_2 \neq 0$

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

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

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

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

$\Leftarrow h x \neq x h$

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

Rechts raus da  $\alpha = -(h + \bar{h}) \neq 0$

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

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

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

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

Trej  $\alpha = 0$

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

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

6) Podkolebær generiran  $\geq 3$ :  $V \oplus C$   
 $7)$   $5 - 6i \in 2 + 5i$

6): Zerstörte Zerlegung

$$n3; n \in \mathbb{Z}$$

$$1 \oplus \rightarrow \mathbb{Z} \oplus k$$

$$n+k3; n, k \in \mathbb{Z}$$

$$(n+k3)^c$$

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

$$A = \{n+k3; n, k \in \mathbb{Z}\}$$

Trej je podkolebær

④

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

$$k(2+5i) = 2k + k5i \in k$$

$$\mathbb{Z} \subseteq k$$

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

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

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

$$5-6: 2+5;$$

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

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

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

$$\begin{matrix} 5-6 \in A & 3 \in K \\ 2+5 \in A & A \subseteq K \end{matrix}$$

in  $A$  de kelerler, tarej  $A \supseteq K$

Tarej  $A = K$

8) Dolaci podalgebra algebre

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

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

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

$$\begin{bmatrix} n & n \\ 0 & n \end{bmatrix} \subseteq K$$

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

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

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, reallni vektorski prostor ali pa ne realna algebra

Opisi podgrupa, podkolobar, podprostор in podalgebra  $\mathbb{R}[x]$  generirana s polinomoma s  $x^2$  in  $2x^3$

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

G je grupe

zaprtest in seštevanje in množenje

$$nx^2 + 2kx^3 - ix^2 - jx^3 =$$

$$= (n-i)x^2 + 2(k-j)x^3$$

$\Rightarrow G$  je neprazna grupa, ki ustreza to ✓

$$K = \{ 0, 1, x^{2m}, x^{3k}, x^{2k}, 2x^3, 2x^{2m+1}, kx^2 + m2x^2, \dots \}$$

$$K = \{ \alpha_0 + \alpha_1 x^2 + 2\alpha_3 x^3 + \alpha_4 x^4 + 2\alpha_5 x^5 + \dots ; \alpha_i \in \mathbb{R} \}$$

Ali je kolobar?

Brez  $\alpha_1$ , ker ona množi  $\alpha_0$  niso 0

- podgrupa je

- enota vsebuje

- enota

- zaprtest in množenje ✓

(ker pri linih potencah je

sode kot lini potence, in pari

lini je 2 ter je jo podeljena 2

podprostор (seštevanje + množenje sklepjeno)

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

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

Podalgebra

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

$$\{ \alpha_0 + \alpha_1 x^2 + 2\alpha_3 x^3 + \dots ; \alpha_0, \alpha_1 \in \mathbb{R} \}$$

$$= \mathbb{R}[x] - \text{lin} \{ x^3 \}$$

je res neprazna in zade zaprta

## 5. poglavlje

$\varphi: G \longrightarrow H$  je homomorfizem grup,  
če je  $\varphi$  obdržala operacijo  
 $\varphi(g \cdot h) = \varphi(g) \varphi(h)$

izomorfizem = homomorfizem + bijekcija  
automorfizem = izomorfizem vase

Neg bo  $\rho: G \rightarrow H$  homomorfismen in  
 $a \in G$  ina koren red.

Potenci, de red( $\rho(a)$ ) | red(a)  
če je  $\rho$  vložitev (monomorfizem) sta  
reda enake.

$$a^n = 1$$

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

"

$$(\rho(a))^n \text{ tarej red}(\rho(a)) \text{ in}$$

Resimo de je vložitev

Resimo de je nizvedben

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

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

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

$$\rho(a^{kt}) = 1 \quad |\ker \rho| = 1$$

torej je to edin. element za kategorij

$$\rho(1) = 1$$

$$\rho(a^t)$$

$$\rho(a^t) = \rho(a)^t = 1$$

$$\cancel{\star \exists} \quad a^k = 1$$

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

Nach  $\alpha$  G agruppe in  $a \in G$ . Pokazij:

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

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

3) Noten: zma gruppe  $(\mathbb{R}^+, \cdot)$ ,  $(\mathbb{R}^*, \cdot)$   
in  $(\mathbb{C}^*, \cdot)$

$$\rho(1) = \cancel{\text{def}} a$$

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

$\rho(1+1) = a \cdot a = a^2$

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

Predprodukto  $\rho(n-1) = a^{n-1}$   $\square$

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

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

$$\begin{aligned} \rho(n) &= \rho(0) = 1 \\ &\Downarrow a^n \end{aligned}$$

$$\Leftarrow a^n = 1$$

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

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

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

↑  
 $\mathbb{R} - \{0\}$

Regrame de date: ieron faza

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

Vsi elementi vor fi ~~cate~~ <sup>$\in \{1, -1\}$</sup>  impreuna red  
 $\vee \mathbb{R}^{\neq}$

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

- red elementelor se obinu, astfel
- v  $\mathbb{R}^+$  nu elemente red 2

$$z \in \mathbb{C}^*$$

$|z| \neq 1 \Rightarrow$  impreuna red

Pagini de clasa red  $\in \{1, -1, 2\}$

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

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

↑                      ↑  
 cantică              relație într-un

4) Pojavi: zakej endemorfizam  
 algebre  $M_2(\mathbb{R})$  ne more preštet:  
 matrice  $E_{11} \cup E_{12}$  pač  
 endemorfizam prelaze  $\rho(E_{11}), \rho(E_{12})$

5) Nej bo A ~~matematik~~

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

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

Prever: deska A in A' k-nasežni: in  
 $A \cong A'$ . Podeli: da A ni izomorfna  
 algebri  $M_2(\mathbb{R})$

G

$E_{11}$  je idempotent

Reineader je

$$\rho(E_{11}) = \rho(E_{11} \cdot E_{11}) = \cancel{\rho(E_{11})}$$

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



$$\rho(E_{22}) = E_{22}$$

$\rho(E_{22}) = E_{22}$  wird idempotentrest

$$\rho(E_{12}) =$$

$$\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \quad \begin{matrix} \text{v uskem} \\ \text{primera} \end{matrix}$$

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

$$\pi = (12)$$

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

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

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

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

$H < G$

$H$  je edinke

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

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

$$H_2 = \langle z \rangle$$

$$H_1 \triangleleft D_8$$

(kerime indeks 2)

$$([D_8 : H_1] = 2)$$

$$[D_8 : H_2] = 4$$

$$(8 : 4 = 2)$$

$$rH_2 = H_2 r$$

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

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

$$\xrightarrow{\quad} \quad \xleftarrow{\quad}$$

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

Ter ej  $H_2$  ni edinke

Podobno u  $D_{2n}$

$H \triangleleft G$        $G/H$  ... kvocientna grupa  
 ↓ množica vseh odsečkov

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

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

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

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

Dokazi da je  $G$  abelova grupa

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

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

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

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

Vsi elementi lahko zapisemo kot  $a^k z$ , kjer

$$a^k z \cdot a^n c = a^k (za^n) c = \underset{z \in Z(G)}{=}$$

$$= a^k (a^n z) c = a^{k+n} z \cdot c = \underset{\in G}{\underset{\in Z(G)}}{=}$$

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

② Nej bo  $|G| = 55$ . Pokaži

a) t preva podgrupe  $G$  je ciklična

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

c) red podgrupe deli red  $G$

red podgrupe je 11 ali 5, ali 1

$\mathbb{Z}_5$  je edina grupa p do izomorfizma  
nastanljena.

Ta je ciklične

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

Po prvi: nalogi kvocientni cikličen

Recimo da centar ni trivialan

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

Potem je  $|G/Z(G)| = 11$  ali 5

in teke grupe je ciklične, kraj \*

③ Pojasni, da lahko sč znameno  
s produktom tudi preštevi  
A: lahko fudi z 8?

če imamo p·q ( $p \neq q$ ) potem podobno kot 26)  
če imamo red  $p^2$ , potem podobno kot pri 26)

$$\mathcal{Z}(D_8) \quad \mathcal{Z}(D_8) = \{1, r^2\}$$

in  $D_8$  n: abelova

$$\mathcal{Z}(Q) = \{\pm 1\} \quad \text{in } Q \text{ n: abelova}$$

↑  
kvaternionske

$$\{\pm i, \pm j, \pm k, \pm 1\}$$

$$\{1, r, r^2, r^3\}$$

grupa reda 4, k: n: ciklična

N: ciklične, ker nima elementa reda 4

## 1. izrek o izomorfizmu

$f: G \rightarrow H$  epimorfizem

Potem velja:  $\ker f \triangleleft G$

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

Naj bo  $G$  grupa vseh nekonstantnih linearnih funkcij

$G = \{ax+b ; a, b \in \mathbb{R}\}$  operacija kompozitum  
 $a \neq 0$

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

enota:  $X$

inverz:

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

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

$$a^{-1}x + b a^{-1} \quad \text{je inverz}$$

Oznadimo  $\mathcal{N} = \{x+b ; b \in \mathbb{R}\}$

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

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

⑥  $\mathbb{R}^*/\mathbb{R}^+$

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

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

$f$  ist homomorfisch

$$f((ax+b)(cx+d)) = f(acx + \dots) = ac$$

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

$$\ker f: \quad f(ax+b) = 1$$

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

$$\text{surjektiv} \Leftrightarrow \ker f \triangleleft G$$

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

\textcircled{5}

$$f: \mathbb{C}^* \longrightarrow T = \{z \in \mathbb{C} \mid |z|=1\}$$

$$f(ae^{i\alpha}) \mapsto e^{i\alpha} \quad \rho(z) = \frac{z}{|z|}$$

$$f(ae^{i\alpha} \cdot e^{i\beta}) = f(ab e^{i(\alpha+\beta)}) =$$

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

$$\ker f: \quad f(e^{i\alpha}) = 1$$

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

$$\{ae^{i2\pi k}; a \in \mathbb{R}^+\} = \mathbb{R}^+$$

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

$$\textcircled{6} \quad \frac{\mathbb{R}^*}{\mathbb{R}^+} \quad f: \mathbb{R}^* \longrightarrow ? \quad \{-1, 1\}$$

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

$$f(a) \rightarrow \frac{a}{|a|}$$

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

$$\text{homomorfisch: } f(a \cdot b) = f\left(\frac{ab}{|ab|}\right) = \frac{a}{|a|} \cdot \frac{b}{|b|} = f(a) \cdot f(b)$$

$$\text{surjektiv: } \frac{1}{1} = 1 \quad \frac{-1}{-1} = -1$$

④ Keterznanje je izomorfija grupe  $\frac{U_n}{SU_n}$

⑤ reaktivna podgrupa  $N$  grupe  $\pi$   
de jo  $\pi/N \cong \pi$

⑥  $? \cong \mathbb{R}/\mathbb{Z}$

$$U_n = \{ A A^H = I \}$$

$$\rho: U_n \rightarrow \pi$$

$$A \mapsto \det A$$

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

Surjektivnost

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

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

⑦  $\frac{\pi}{N} = \pi$

$$\rho: e^{ip} \mapsto e^{i2p} \quad \text{je homometrična}$$

$$\ker \rho: e^{i2p} = 1 \quad \text{je } 2p = 0 + 2\pi k \quad 0 + 2\pi k \quad \ker \rho = \{ 1, -1 \}$$

⑧  $\mathbb{R}/\mathbb{Z} \rightarrow [0, 1)$

$$\alpha, \alpha_1, \alpha_2, \dots \xrightarrow{n} 0, \alpha_1, \dots$$

$$x \xrightarrow{} e^{i2\pi x}$$

$$\mathbb{R}/\mathbb{Z} \xrightarrow{} \pi$$

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

$$\ker \rho = e^{ix2\pi} = 1$$

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

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

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

Pokazi, da je center eneskrivega  
kotlobega polje

rabimo konifikacijo in drugi vogl

$Z(k)$  je kotlobar in je konfikativ

$a \in Z(k)$  a konfiktira z vsemi

$$ab = b \cdot a \quad , k_a$$

generiramo ak ideal

$$ak = \{ak, k \in k\} \text{ je ideal}$$

$$ak + at = a(k+t) \quad \checkmark$$

$a \in ak$  torej je ak neničeln;

$$\Rightarrow ak = k \quad (\text{kjer je } k \text{ eneskriv})$$

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

Pokazi, da je b  $\in Z(g)$

$$k \in k$$

$$k = (ab)k = k(bb) = akb$$

$$bk = bakk = kb$$

z poljuben  $k$

$$\Rightarrow pr_1 I \not= I_1$$

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

enako za  $I_2$

$I_1, I_2$  kolo  $\mathbb{Z}_1$  i  $\mathbb{Z}_2$  oblike  $I_1 \times I_2$   $I_1 \triangleleft I_1 \times I_2$   
 $I_2 \triangleleft I_1 \times I_2$

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

aditivne podgrupe

Naj bo  $I \triangleleft \mathbb{Z} \times \mathbb{Z}$

$$(a, b)(c, d) = (ac, bd) = (ca, db)$$
$$\in I \quad \in \mathbb{Z} \quad - (c, d)(b, a)$$

Torej  $a \in I_1$ , zerek ideal in  
 $b \in I_2$  ker bo amotrate z usklj.  
elementom

Cerkeat se sestavijo:

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

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

Opomba: Za grupe odlike to ne

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

$$\cdot \{(0, 0), (1, 1)\}$$
 nima oblike  
 $H_1 \oplus H_2$

$$H_1 \triangleleft \mathbb{Z}_2 \text{ in } H_2 \triangleleft \mathbb{Z}_2$$

⑤

ideal:  $R \times R \times R$   
 n.zf so ideal: Tu m: meistheg  
 (her ab prosteril) negativ

$R$ : ideal or  $n.m.$  (son  $R, \emptyset$ )  
 $\exists e$ :  $R \times R$  negativ  
 $\exists g$ :  $(R \times R) \times R$   $n.m.$  ideal or  
 rezipient  $n.m.$  ideal

$$\{\circ\} \times \{\circ\} \times \{\circ\}$$

"

$$\{\circ\} \times \{\circ\} \times R$$

$$\{\circ\} \times R \times R$$

$$R \times R \times R$$

$$\{\circ\} \times R \times \{\circ\}$$

$$R \times \{\circ\} \times \{\circ\}$$

$$R \times \{\circ\} \times R$$

$$R \times R \times \{\circ\}$$

nabringen

$(g(x)) \dots$  gern: halbenge  $F[x]$

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

Präsent in weiter ideal  $(x^2+x)$ : in  $(x^2-x)$   
halbenge  $R[x]$       "      "

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

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

$$\textcircled{1} \quad I \cap J$$

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

Vektoren: gege. in drückt es  
vektoriell

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

$$I \cdot J \quad h(x) \cdot (x^2+x) \\ g(x) \cdot (x^2-x)$$

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

$$\text{Rechnen } h(x)(x^2+x)(x^2-x) \in I \cdot J$$

$$I+J$$

$$v \not\in \quad \begin{matrix} I = (x) \\ J = (x) \end{matrix} \quad I+J = (2)$$

$$\overline{\quad} \quad I+J = (x)$$

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

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

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

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

$$\text{denn je polynom } x \in I+J$$

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

① A1: imo  $\frac{\mathbb{R}[x]}{(x^2+1)}$  delitej nica

$$\textcircled{1} \quad -\text{II}- \quad \frac{\mathbb{R}[x]}{x^2+1} \quad -\text{II}-$$

② A1: je izomorf  $\frac{\mathbb{R}[x]}{x^2-1}$ ?

$$I = (x^2+1) \quad \begin{aligned} f(x) & \dots \text{glevn: ideal} \\ & = \{ p(x) \cdot f(x) : f(x) \in \mathbb{R}[x] \} \end{aligned}$$

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

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

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

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

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

steje manja od 2

Vsek delek imo oblik

$$ax+b+I$$

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

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

(ker mora bidi  
sečatih od  $x^2+1$ )

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

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

$$\begin{array}{ll} a=1 & c=1 \\ b=i & d=-i \end{array} \quad \rightarrow$$

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

Torej ste  $(x+i)^{+I}$  in  $(x-i)^{+I}$  delitej nica

② v  $\frac{\mathbb{R}[x]}{(x^2+1)}$  ni delitej nica

③ A1: je izomorf kolabaju? Ne ker imo ~~ne~~ te delitej nica, tisti pa ne

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

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

Definirajmo  $\varphi: K \rightarrow \frac{K}{I_1} \times \frac{K}{I_2} \times \dots \times \frac{K}{I_s}$   
 $\varphi(a) = a + I_1, \dots, a + I_s)$

Početek de je  $\varphi$  epimorfizem in  $\ker \varphi = I_1 \cap \dots \cap I_s$

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

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

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

surjektivnost

$(a_1+I_1, \dots, a_s+I_s)$  poljuben element

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

Dovolj je pokazati da  $\exists a_i$  de  $(0, \dots, a_i, \dots, 0)$   
lest vimp. Pravzaprav da  $(0, \dots, 1+I_i, \dots, 0)$   
lest rdeči

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

$$\text{vegn } I_i + I_j = K \text{ za } i \neq j$$

$$1 = a_1 + b_1 = a_2 + b_2 = a_3 + b_3 = \dots a_s + b_s \quad \begin{matrix} a_i \in I_i \\ b_i \in I_j \end{matrix}$$

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

$$a_2 a_3 \dots a_s + \dots + \underbrace{b_2 b_3 \dots b_s}_{\substack{\text{dim del k. niz} \\ \text{natr. redi: } i \in I_i}}$$

dim del k. niz  
natr. redi:  $i \in I_i$

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

$$\varphi(\underbrace{b_2 \dots b_s}_{\in I_2 \dots I_s}) = (1+I_1,$$

$a \in I_1 \cap I_2 \cap I_3 \dots$

Torec  $a \in I_1 \cap I_2 \cap I_3 \cap \dots$

(4) (mitajši iz en o ostankih)

Naj bodo  $n_1, \dots, n_s$  pravna tve  
cela števila. Potem je za  
pravljene cele številke  $a_1, \dots, a_s$   $\exists$  celo  
število  $a$ , za katere velja

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

$$\text{Ako je } b \equiv a \pmod{n_i} \Rightarrow n_1, \dots, n_s \mid (a-b)$$

Poisci ~~preklici~~

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

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

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

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

$x = 17$  je en

ravnatelj

Naj bo c katalizor vse konvergentnih  
realističnih reakcij;

"in Co množice vseh reakcij  $\geq$  limita 0

Poleti da je Co maksimalni ideal C  
in ~~katalizator~~  $\%_{Co} =$

## ⑥ Pokekzi; de je kelobor

$\mathbb{R}[x] / (x^2)$  izomorfen kelobargu ush  
 $2 \times 2$  metrike oblik  $\begin{bmatrix} a & b \\ 0 & a \end{bmatrix}$   $a, b \in \mathbb{R}$

Poisə take ideala  $I$  in  $J$  kelobargu

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

$$\left| \frac{k}{I} \right| = \left| \frac{k}{J} \right| = q \text{ in } k_I = k_J$$

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

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

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

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

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

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

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

Sektoranje: osire

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

$$\ker \rho: \begin{bmatrix} a & b \\ 0 & a \end{bmatrix} = \rho(0 + 0 + x^2 \underbrace{(0, 1)}_{n}) =$$

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

I

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

$$\frac{\mathbb{Z}}{I} \cong \mathbb{Z}_2 \times \mathbb{Z}_2$$

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

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

$$(ma, mb) = (m, n) \cdot (a, c)$$

~~and hence~~  $m \pmod 2$   $a \pmod 2$   $n \pmod 2$   $c \pmod 2$ .

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

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

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

$K, H \subset G$

$H \triangleleft G \Leftrightarrow K \triangleleft H$

$K \triangleleft H \triangleleft G$

All  $\sigma \in K \triangleleft G$

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

Podgrupa  $\overset{N \leq G}{\text{je}}$  karakteristicka,  $\Leftrightarrow$   
 $\varphi(N) \subseteq N \quad \forall \varphi \in \text{Aut}(G)$

Karakteristicka grupe je edinice

Pokazi:

- $\{1, -1, i, -i\}$  je edinice, ni pa karakteristicka
- $\forall G \neq \{1\} \quad G \times \{1\} \triangleleft G \times G$  n: pa karakteristicka podgrupe
- $Z(G)$  je karakteristicka podgrupe
- $K \overset{\text{ker}}{\leq} G \quad H \overset{\text{ker}}{\leq} G$  potem je  $K \overset{\text{ker}}{\leq} G$

①  $G \dots p\text{-grupa}$   
 $H \dots g\text{-grupa}$        $p \neq 2$  pravilenji

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

$$\Rightarrow |G| = p^k \quad G \cong \mathbb{Z}_{p^k}$$

$$|H| = 2^n \quad H \cong \mathbb{Z}_{2^n}$$

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

ker sta  $p^k$  in  $2^n$  "taji":

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

$\Rightarrow G$  in  $H$  sta tudi abelovi

$$|G \oplus H| = p^s \cdot 2^t$$

$$G \oplus H \cong \underbrace{\mathbb{Z}_{p^{s_1}} \oplus \dots \oplus \mathbb{Z}_{p^{s_k}}} \oplus \underbrace{\mathbb{Z}_{2^{t_1}} \oplus \dots \oplus \mathbb{Z}_{2^{t_m}}}$$

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

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

teradi enolomasti ravno  $G \oplus H$

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

② Pokazi: končna abelova grupe je ciklična  $\Leftrightarrow \forall p \in P, p \mid |G| \Rightarrow G$  vsebuje  $n-1$  elementov reda  $p$

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

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

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

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

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

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

Bšz:  $p = p_1$

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

V  $\mathbb{Z}_p^\alpha$  element reda  $p$ :

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

$\Rightarrow p-1$  elementov reda  $p$

■

$(\Leftarrow)$

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

ker je končna abelova grupe

$\rightarrow p-1$  elementov reda  $p$

Pokazi morajo da je  $k=1$

Reimo da  $k \neq 1$

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

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

Torej ima večjo  $2/p$  elementov reda  $p$

Torej  $k=1$  torej  $\Leftrightarrow \text{vse } \times$

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

Torej je ciklične

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

$G$  ima podgrubo reda  $m$

---

④ Naj bo  $G = A_4$ . Pokaži da  $G$  nima  
podgrupe reda 6

---

Rečimo da  $|G|=200$  abelova

Pokaži:  $G$  ima podgrubo reda 20

$$\begin{array}{c} 200 \\ 100 \\ 50 \\ 25 \\ 5 \end{array} \Big| \begin{array}{c} 2 \\ 2 \\ 2 \\ 5 \\ 5 \end{array}$$

$$200 = 2^3 \cdot 5^2 \quad 20 = 2^2 \cdot 5$$

$$G = \underbrace{G_1}_{\text{red } 8} \oplus \underbrace{G_2}_{\text{red } 25} \quad H = \underbrace{H_1}_{\text{red } 4} \oplus \underbrace{H_2}_{\text{red } 5}$$

Dovolj je pokazati:  $G_1$  ima podgrubo  $H_1$  reda 4 in  $G_2$  ima podgrubo  $H_2$  reda 5

Vse možnosti:

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

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

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

Podgrubo za  $G_2$

Naj bo m m/n poljuben

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

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

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

$$\mathbb{Z}_{p^{\alpha}} \text{ ima podgrubo } \mathbb{Z}_{p^j} \quad j \leq \alpha$$

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

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

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

$p^\alpha$  velikost

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

Potenje

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

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

2. nach  $\alpha(4)$

$H \subset A_4$  paragrafe red o 6

rimano 2 monasti

$$1) H \cong S_3$$

$$2) H \cong C_6 \quad \text{ne, ker } L; \text{ marab inoltre } A_4 \\ \text{element reda 6}$$

$$\begin{aligned} 1) \quad S_3 &= \{ (1, 2), (2, 3), (1, 3), (1, 2, 3), (1, 3, 2), 1 \} \\ \Rightarrow H &= \overbrace{\{ (12)(34), (13)(24), (14)(23) \}}^A, \overbrace{\{ }}^B, \overbrace{\{ }}^C \end{aligned}$$

$$1) \quad \overset{A}{\{ A, B, C, 1 \}} \subset A_4 \quad , 2 \text{ 3cicle, 1 } \overset{?}{\circ}$$

$$2) \quad (1, 2)(2, 3) \neq (2, 3)(1, 2) \quad \cancel{H = 6} : n \\ \text{- ampiat } ab = ba \quad ac = ca \quad bc = cb$$

## ⑤ Pokazi da je podgrupa

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

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

in de je

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

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

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

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

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

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

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

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

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

$$\varphi(1,0) \mapsto (1,1) \quad \varphi \text{ si razgradi}$$

$$\varphi(0,1) \mapsto (1,3) \quad \text{do homomorfizma}$$

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

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

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

$\varphi$  je injektiven

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

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

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

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

$$2\beta = 0 \quad \beta = 0 \quad \alpha = 0$$

$C$

$$B \subseteq C$$

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

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

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

$$C \subseteq B$$

$$\cancel{(\alpha + \beta) = 2c}$$

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

$$a = \alpha + \beta$$

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

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

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

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

obzadja rešku

## ⑥ Ponavimo:

element  $\sigma$  in  $\Pi \in S_n$  sta konjugirana  
( $\sigma: \alpha \Pi \alpha^{-1} = \text{nek } \alpha \in S_n$ )

$\Leftrightarrow \sigma$  in  $\Pi$  imata enako cikločno strukturo (enako št. enakodolžih ciklov)

Cilj: Konjugiranosti razred:  $v A_n$

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

- 1)  $C(\sigma) \subseteq A_n \Rightarrow$  konjugiranosti razred  $\sigma \in S_n$  razpade na 2 enake velike razrede  $v A_n$
- 2)  $C(\sigma) \not\subseteq A_n \Rightarrow$  konjugiranosti razred  $\sigma \in S_n$  se razpade z razredom  $\sigma \in A_n$

Primer:

- 1) id
- 2)  $(12)(34), (14)(23), (13)(24)$   
razred  $v S_4$
- 3)  $(123), (132), (124), (142), (134), (143)$   
 $(234), (243)$   
 $v S_4$

$v A_4$ :

1) |id|

2)  $(12)(34), (14)(23), (13)(24)$  je en razred, ker je lahko sterego

3) Iz predavanj, sledi: moč razrede deli red grupe

Ta razred razpade na 2

Opiši konjugira no sime razrede v  $S_n$  in  $A_n$

$\vee A_n$  imamo 4 razrede

(id., produkt dveh disjunktnih zikelov, ...)

$\vee S_n$  je

1) id

2) en dvackel

3) dva dvackela

4) en triakel

5) kvakel

② Opis konjugiranosti razred grup  
Q in  $D_8$

"Je b; podvojil število nalog in jo  
del naslednjema"

-bar

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

$Z(Q) = \{1, -1\} \Rightarrow \{1\}, \{-1\}$  sta konjugirane razrede

i: Vemo: moč orbite je enaka indeksu centralizatorja

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

Torej orbita i je imenovana z elementoma

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

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

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

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

Podobno za vse ostale j in k

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

$$D_8 = \{ \text{id}, r, r^2, r^3, z, zr, zr^2, zr^3 \}$$

$$Z(D_8) = \{ \text{id}, r^2 \} \Rightarrow \{ \text{id} \}, \{ r^2 \} \text{ sta razvede}$$

$C(r) = \{ \text{id}, r, r^2, r^3 \}$  to so vse ker je  
 b: bila se koju vse b: morebiti  
 b:iti 8, ampers r ni u centru, ter je  
 ima na jvečjih

$$\Rightarrow |D_8 \cdot r| = 2$$

$$D_8 \cdot r = \{ r, r^3 \}$$

$$zr z^{-1} = zzr^3 = r^3$$

$$C(z) = \{ \text{id}, z, z^2, zr^2 \}$$

$$|D_8 \cdot z| = 2$$

$$D_8 \cdot z = \{ z, zr^2 \}$$

$$r^{-1} z \cdot r = r^3 \cdot r^3 z = r^2 z = zr^2$$

Ostanka  $zr$  in  $zr^3$  nemoreba biti same  
 ker ce bila sama bi bila u centru

$$D_8 \cdot zr = \{ zr, zr^3 \}$$

⑥ Maj bo  $g = (1 \ 6 \ 9)(2 \ 10)(3 \ 4 \ 5 \xrightarrow{8})$   
Opisi orbiti in stabilizatorje  $\subset S_{10}$   
narevne delovanje grupe  $\overset{G}{\cong} \langle g \rangle$  na  
množici  $X = \{1, \dots, 10\}$

$$t_j \quad h \cdot x = h(x)$$

④  $G \leq GL_n(\mathbb{R})$

$G$  deluje na  $V = \mathbb{R}^n$

za  $A \in G$  in  $v \in V$

$$A \cdot v = Av$$

Opis orbit 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 obveznih matrik

V tačkah a in d) posesi stabilizator vseh pogojih

$$v = \begin{bmatrix} 1 \\ \vdots \\ 1 \end{bmatrix}$$

a)  $A \cdot 0 = 0 \quad \forall A \in GL_n(\mathbb{R})$

1)  $\{0\}$

Naj bosta  $v$  in  $w$  neenake vektorje

Dopolnilo  $v$  in  $w$  do vseh svojih baze  
n. obsteja prehodna matrika da zlik

$$v \quad v \quad w$$

Torej druga orbita je vse ostalo

b)  $\{0\}$  orbit

množenje z ortogonalnim  $\Rightarrow$  ohrange dolžino terg

če sta v in u v risti orbiti merite  
meriti isto orbito

normiramo  $u$  in  $v$  in jih dopolnimo  
do ortognanirane baze. Toda  
obstaja prehodna ortogonalna matrika

in presek  $\frac{u}{\|u\|} \times \frac{v}{\|v\|}$  terj skalar faktor:  
 $u \cdot v + \text{ber } \|u\| = \|v\|$

$\Rightarrow u$  in  $v$  sta oziroma or. si.

$\Leftrightarrow$  množenje z matriko

c)  $G = \text{diag in the matrix}$

Nerij bo  $v = \begin{bmatrix} v_1 \\ \vdots \\ v_n \end{bmatrix}$   $A = \begin{bmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_n \end{bmatrix}$

$$A \cdot v = \begin{bmatrix} \lambda_1 v_1 \\ \vdots \\ \ddots \\ \lambda_n v_n \end{bmatrix} \text{ tang}$$

wie se na isch moestik dat  $v$

$z^n$

d)

$$\begin{bmatrix} a_{11} & a_{12} \\ 0 & a_{22} \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} x a_{11} + a_{12} y \\ a_{22} y \end{bmatrix}$$

$$y=0 \Rightarrow A y \cdot (x) = 0 \quad \begin{bmatrix} a \in \mathbb{R} \\ 0 \end{bmatrix}$$

$$y \neq 0 \Rightarrow \begin{bmatrix} b \in \mathbb{R} \\ a \in \mathbb{R} \end{bmatrix}$$

dearbit:

Probabilo se vec dimenzij

1) zadnjih  $k \neq 0 \Rightarrow \{ \text{Wijfors zadnjih } k \neq 0 \}$

2) Tang je  $n^{\text{th}}$  arb bit

Burnside's lemma

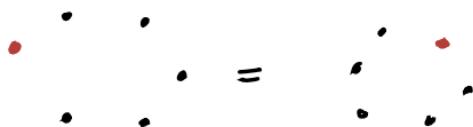
$$G \curvearrowright X$$

$$\text{# orbit: } \frac{1}{|G|} \sum_{g \in G} |g^x|$$

$$g^x = \{x \in X : gx = x\}$$

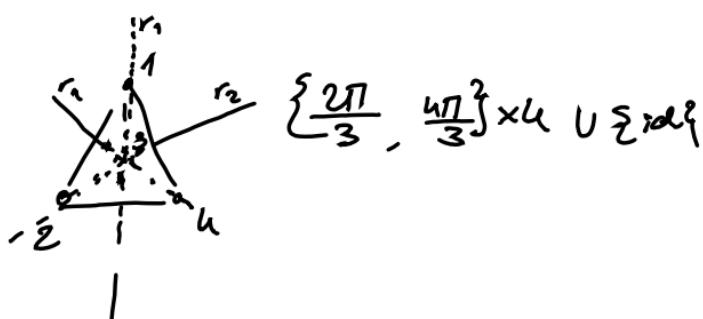
6 korak n različnih barv

Poisci število ogljic, ki jih lahko sestavimo.  
(ogljiči sta enaki če se do ene prestavita  
v drug z rotacijo ali zrcaljenjem)



③ Na koliko načinov se da pobarvati lice pravilnega tetraedra z rdečo madro in zeleno tako da je netekno eno lice madro

④ Na koliko načinov se da pobarvati robove pravilnega tetraedra z rdečo in zeleno



$$r_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix} = (2\ 4\ 3)$$

$$r_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix} = (1\ 3\ 4)$$

$$r_1 \cdot r_2 = (2\ 4\ 3)(1\ 3\ 4) = (1\ 2\ 4) = r_3$$

$$z_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} = (1\ 3)(2\ 4)$$

$$z_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} = (1\ 2)(3\ 4)$$

$$z_3 = (1\ 4)(2\ 3)$$

$A_u$

$S_u \supseteq G \supseteq A_u$

$G \neq A_u \Rightarrow G = S_u$  ker pa ne velja

$\emptyset$ $id$ $(: j k)$ $(i j) / (k l)$	Čet neg took $4 \cdot 2^3$ $1 \cdot 2$ $0$
---	---

$$\frac{1}{12} (4 \cdot 2^3 + 8 \cdot 2) = \frac{2}{3} (4 + 2) = 4$$

Izrek: Sylowa

$$|G| = t \cdot p^s \quad p \nmid t \quad p \text{ ... prostovl}$$

$p$ -podgrupa Sylowa je podgrupa mod  $p^s$

$n_p$  ... število  $p$ -podgrup Sylowa

$$n_p \equiv 1 \pmod{p}$$

$$n_p \mid |G|$$

$$n_p \mid t$$

$$\text{Dokaz: } n_p \mid t$$

$$n_p \mid t \cdot p^s$$

$$(n_p, p) = 1$$

$$(n_p, p^s) = 1 \Rightarrow n_p \mid t$$

⑤ Pokaz de imo  $S_4$  a 3-podgrupe Sylowa

⑥ Pokaz de jo vrake 2-podgrupe Sylowa  $S_4$  izomorfne  $D_8$

Naved vse 2-podgrupe Sylowa in amente so ena jo katerih so dene podgrupe!

$$|S_4| = 24 = 3 \cdot 2^3$$

3 podgrupe Sylowa ma mod 3

2-podgrupa Sylowa ma mod 2

$$n_3 | 8 \quad n_3 \equiv 1 \pmod{3}$$

$$n_3 = \{1, 4\}$$

$$n_2 | 3$$

$$n_2 \equiv 1 \pmod{2}$$

$$n_2 = \{1, 3\}$$

Vedja:  $n_p=1 \Leftrightarrow p$ -podgrupa ~~z Sylowa~~  $\subset S_4$

$$P_1 = \langle (1, 2, 3) \rangle$$

$$P_2 = \langle (2 \ 4 \ 2) \rangle$$

$$P_3 = \langle (1 \ 2 \ 4) \rangle \Rightarrow n_3 = 4$$

$$P_4 = \langle (2 \ 3 \ 4) \rangle$$

za  $n_2$ :

$$\Pi_1 = \{(1, 2, 3, 4), (1 \ 3)(2 \ 4), (1 \ 4 \ 3 \ 2), (1 \ 2)(3 \ 4), (1 \ 4)(2 \ 3), (1 \ 3)(2 \ 4), \text{id}\}$$

To jo 2 podgrape Sylowa s

$$\Pi_2 = \{(1 \ 3 \ 2 \ 4), (1 \ 2)(3 \ 4), (1 \ 4 \ 2 \ 3), (1 \ 3)(2 \ 4), (1 \ 4)(2 \ 3), (1 \ 2)(3 \ 4)\}$$

(vse smo konjugatni z  $(2, 3)$ )

DNL =  $H_3$ : in element ki konjugata  $H_1$  in  $H_2$

Pomembne uporabe izkhan izkhan Sylowa: iskanje enost. grpa. (Nima drugih edink)

Enestava na grupa: nima previh edinst

$$|A_5| = 60$$

$A_5$  je enostavna

valjuba

⑦ Pokaži, da <sup>valjuba</sup> grupe reda  $n$  nima enostavn

če:

a)  $n = 88$

b)  $n = 30$

c)  $n = 48$

d)  $n = 36$

a)  $n = 88 = 2^3 \cdot 11$

$$p_1 = 11 \rightarrow n_{11} = 1 \bmod 11$$

$$n_{11} \mid 8 \Rightarrow n_{11} = 1$$

$\Rightarrow$  ker je edinejo edinstva

b)  $n = 30 = 2 \cdot 3 \cdot 5$

$$p_1 = 2 \quad n_2 = 1 \bmod 2$$

$$n_2 \mid 15$$

$$n_2 \in \{1, 3, 5\}$$

$$p_3 = 5$$

$$n_5 = 1 \bmod 5$$

$$n_5 \mid 6$$

$$n_5 \in \{1, 6\}$$

Rečimo da imamo 6 podgrup reda 5

Njihov prosti jih sene so id

Torej je  $2k$  elementov rede 5

če  $n_3 = 10$

Vsega 20 elementov rede  $\geq 3$

$$20 + 2k > 30$$

a1:  $n_3 = 1$  a1:  $n_5 = 1$

①  $H \subset G$  One case

$$N_G(H) = \{g \in G : ghg^{-1} = h \} \quad (\stackrel{H \trianglelefteq G}{\stackrel{\Rightarrow}{G = N_G(H)}})$$

$$C_G(H) = \{g \in G : ghg^{-1} = h \text{ for all } h \in H\}$$

↑  
Pohere:  $gh = hg$

$N_G(H)/C_G(H)$  isomorphic  $\text{Aut}(H)$

ocimo:  $C_G(H) \leq N_G(H)$

$\varphi: N_G(H) \rightarrow \text{Aut}(H)$

$$g \mapsto \varphi_g \quad (\varphi_g(h) = ghg^{-1})$$

$$\varphi_{g_1} \circ \varphi_{g_2} = \varphi_{g_1 \cdot g_2} \quad \text{also}$$

$$\ker \varphi = \{g \in N_G(H), \varphi(g) = 1\} =$$

$\overset{''}{\text{id}}_H$

$$\{g \in N_G(H) : ghg^{-1} = g\} = C_G(H)$$

$$\frac{N_G(H)}{C_G(H)} \cong \text{im } \varphi \leq \text{Aut}(H)$$

② Nacho  $G = \mathbb{H}^*$  (renzielen Quaternionen)

$$H = \{1, -1, i, -i\} \subset G$$

Daloci  $N_G(H), C_G(H)$  in pokazi:

$$\frac{N_G(H)}{C_G(H)} \cong \mathbb{Z}_2 \cong \text{Aut}(H)$$

$$g_1 g_2^{-1} H$$

$$g(-1) g^{-1} = -1 \in H$$

$$N_G(H) = \{g \in G; g^{-1} H g \}$$

$$g_i g_i^{-1} = 1$$

$$\begin{matrix} g_i = 1 \\ i=1 \end{matrix} *$$

$$g_i g_i^{-1} = 1$$

$g_i = ig$  Torej sčemo centralizatorja

$$g = a + bi + cj + dk$$

$$g_i = ig \Leftrightarrow g = a + b$$

$$g_i g_i^{-1} = 1$$

$$g_i = -ig$$

$$a_i - b_i - c_i - d_i = (a_i - b_i + c_i + d_i)$$

$$\text{Ker } a_i - b_i = -a_i + b_i$$

$$2a_i = 2b_i$$

$$a_i = b_i \quad \cancel{\Rightarrow} \quad a = b = 0$$

$$g = ck + dj$$

$$g_i g_i^{-1} = 1 \Rightarrow$$

$$g(-i) g^{-1} = -1$$

$$N_G(H) = \{a + bi; a, b \in \mathbb{R}, a^2 + b^2 \neq 0\} \cup$$

$$\{cj + dk; c, d \in \mathbb{R}, c^2 + d^2 \neq 0\}$$

$$C_G(H) = \{a + bi; a, b \in \mathbb{R}, a^2 + b^2 \neq 0\}$$

$\text{Aut}(H)$

$$H \cong \mathbb{Z}_4 \quad H = \langle i \rangle$$

$$\text{Aut}(H) = \{id_H; (i \mapsto -i)\} \quad (\text{zarej dveje parne redovi})$$

$$\text{Aut}(H) \cong \mathbb{Z}_2$$

$$\text{def: } f: N_G(H) \rightarrow \text{Aut}(H)$$

$$g \mapsto (h \mapsto ghg^{-1})$$

$$\text{za } g = c + di \Rightarrow h = ghg^{-1} = h$$

$$\Leftrightarrow g \in C_G(H)$$

$$\text{za } g = c + di$$

$$\text{potem } g \mapsto (i \mapsto -i)$$

ker  $n: v \in \text{centralizatorju, torej potisk}$

ker ostane

3) Potenci de grupa reda 48 ne more biti enostavne

4) -||- reda 36 ne more biti enostavne

$$48 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 3 = 2^4 \cdot 3$$

2-podgrupa Sylava ima red 16

3-podgrupa Sylava ima red 3

$n_2 \dots \leq 2$ -podgrup

$$n_2 \equiv 1 \pmod{2} \quad n_2 \mid 3$$

$$n_2 \in \{1, 3\}$$

če  $n_2 = 1$  bo zvezdilo da je enaka, tretjega grupe n: enostavne

če pa je  $n_2 = 3$  tretje so 3 tek vrednosti

Naj bo sta  $H, K$  dve podgrupe:

$$|H \cap K| = \{1, 2, 4, 8, 16\}$$

$$|HK| = \frac{k^{48}}{|H \cap K|} = \frac{16 \cdot 16}{|H \cap K|} \leq 48$$

$$|H \cap K| \geq \frac{16}{3}$$

$$|H \cap K| = 8$$

$$N_G(H \cap K) \leq G$$

$$\begin{matrix} H \cap K \triangleleft H \\ H \cap K \triangleleft K \end{matrix} \Rightarrow H \subseteq N_G(H \cap K)$$

$$H \subseteq N_G(H \cap K)$$

$$K \subseteq N_G(H \cap K)$$

$$|N_G(H \cap K)| \geq |H| + |K| - |H \cap K| = 24$$

$$\text{torej } |N_G(H \cap K)| \in \{24, 48\}$$

Nesme biti 24, ker pa je, ki bila edenka (ker indeks 2)

če  $|N_G(H \cap K)|$  cele grupe je  $\frac{|H \cap K|}{|G|}$  edenka

(5) Nej bo  $G$  končna grupa  $H \subset G$   
 $[G:H] = m$

Pokaži:  $|G| \nmid m!$   $G$  ne more biti enastavna

Primeri: — — — — —

Mož: 3:

$H$  je indeksa 3

$\Rightarrow G$  ne morebiti enakost

$$|G| = 48$$

$H$  2-podgrupe Sylava

$$[G:H] = 3$$

$G$  ne more biti  
enastavne

— — — — —

$$G \cdot H \cong gH \quad ; \quad g \in H$$

$$|G \cdot H| = m$$

$G$  deluje na mnogici odsekov

$$g \cdot hH = ghH$$

(Delovanje je  $\rho: G \rightarrow \text{Sym}(G \cdot H)$ )

$$\rho: g \mapsto \rho_g(hH) = ghH$$

$\rho_g$  je homomorfizem

$$\frac{G}{\ker \rho} \cong \text{im } \rho \subseteq \text{Sym}(G \cdot H)$$

$\ker \rho \triangleleft G$

$$\ker \rho \not\subseteq \{e_G\}$$

-----

$$|\text{im } \rho| \mid m! \quad \leftarrow |G \cdot H| = m$$

||

$$|\frac{G}{\ker \rho}| \quad G = |\text{im } \rho| \cdot |\ker \rho|$$

$$\text{če } |\ker \rho| = 1 \Rightarrow |G| \nmid m! \quad *$$

$$\text{če } |\ker \rho| = \frac{G}{\ker \rho} \Leftrightarrow$$

$$\rho_g(hH) = hH$$

$$g \neq 1 \Rightarrow \rho_g = \begin{pmatrix} H & h_1H & h_2H & \dots \\ & gH & & \end{pmatrix}$$

$$g \notin H \Rightarrow gH \neq H$$

$$\Rightarrow \rho_g \neq \text{id}$$

$$|G|=3 \cdot 2^k \quad k \geq 2$$

$G$  n: enostavna

2-podgrupa Sylova je reda  $2^k$  in  
je indeksa 3

$H$  je 2-podgrupa Sylova

$$[G:H] = 3$$

$$m=3$$

$$k \geq 2 \Rightarrow |G| \geq 12 \Rightarrow |G| \nmid G!$$

⑦ Naj bo  $|G|=2m$ ; m l:ho

Potem, da ima G podgrubo indeksa 2 inato ne more biti enostavna

iz reki sybva redenje n:

l:čemo grpo reda m

l:čemo  $f: G \rightarrow \mathbb{Z}_2$  surj

$$\Rightarrow \ker f \trianglelefteq G \quad [G : \ker f] = 2$$

Cauchy  $\Rightarrow \exists a \in G; a^2 = 1$

$G \cong G$  s konij ali  $\varphi_g(h) = g^h$

$\varphi: G \rightarrow \text{Sym}(G)$

$$\varphi(g) = \varphi_g \quad \varphi_g(h) = g^h$$

$$\varphi_a(h) = ah$$

Ali: je lahko  $ah = h$

$$\varphi_a(ah) = h$$

$$\Leftrightarrow a=1 \quad \text{ker } \varphi \text{ red 2}$$

$\varphi_a$  je produkt transpozicij (zamenjuje dva elementa) in nima negativnih tacok  $\Rightarrow$  je produkt m transpozicij

$$\text{sgn}(\varphi_a) = -1$$

$$G \xrightarrow{\varphi} \text{Sym}(G) \xrightarrow{\text{sgn}} \{-1, 1\}$$

kompozitum homomorfizmov

sgn je surjektivna ker id in  $\varphi_a$  sklene v 1 oz -1 res.

$$\Rightarrow \ker \varphi \trianglelefteq G \quad [G : \ker \varphi] = 2$$

⑧  $p$ -prast

Koliko radionicih  $p$ -podgrup Sylowa

ima  $S_p$

⑨ Koliko  $p$ -podgrup Sylowa ima  $A_5$  ee

a)  $p=2$

b)  $p=3$

c)  $p=5$

---

$$|S_p| = p! = p(p-1)!$$

$p$  podgrupe Sylowa imaju red  $p$

$$n_p \equiv 1 \pmod{p} \quad n_p | (p-1)!$$

$p$  podgrupe Sylowa  $\cong Z_p$

$S_p$  imaju  $(p-1)!$   $p$ -ciklova

$$\Rightarrow \frac{(p-1)!}{(p-1)} = (p-2) \quad \begin{matrix} p\text{-podgrupe} \\ \text{Sylowa} \end{matrix}$$

# Komutatorske grupe resljive grupe

$G, \text{Grupa } A, B \subseteq G$

oznacimo  $[A, B]$  podgrupu rano  $z$

$$[a, b] = a^{-1}b^{-1}ab \text{ kjer } a \in A, b \in B$$

$\in G'$  oznacimo  $[G, G]$  - komutatorska podgrupa grupe  $G$

1) Naj bo  $h \in G$  Poteri de je  $H \trianglelefteq G \Leftrightarrow [H, G] \subseteq H$

2) Poteri de je  $G$ 's  $G$  in  $G/G'$  zveljavne

3) Naj bo  $h$  edinka in  $G/H$  zveljavna.  
Poteri  $G' \subseteq H$

$$H \trianglelefteq G \Leftrightarrow [h, g] \in H \quad \forall g \in G, \forall h \in H$$

$$H \trianglelefteq G \Leftrightarrow ghg^{-1} \in H \quad \forall g \in G \Leftrightarrow ghg^{-1} \in H, \forall g \in G, \forall h \in H$$

( $\Rightarrow$ )

$$\underbrace{h^{-1}g^{-1}hg}_{\in H} \in H$$

$$(\Leftarrow) h^{-1}g^{-1}hg \in H$$

$$2) G' \trianglelefteq G \Leftrightarrow \underbrace{\forall g \in G} \quad \underbrace{h \in G'} \quad \underbrace{ghg^{-1} \in G'}$$

Dovolj je potrebiti za generator

$$h = a^{-1}b^{-1}ab = [a, b]$$

$$\underbrace{g[a, b]}_{\in G'} \underbrace{g^{-1}}_{\in G}$$

$$g a^{-1} b^{-1} a b g^{-1} = \underbrace{[gag^{-1}, gab^{-1}]}_{\cancel{gag^{-1}bab^{-1}}}$$

$$\underbrace{g a^{-1} g g^{-1} b^{-1} g g^{-1}}_{\cancel{gag^{-1}bab^{-1}}} \underbrace{a g^{-1} b g^{-1}}_{\cancel{bab^{-1}g^{-1}}} =$$

$$[gag^{-1}, gab^{-1}] \rightarrow \text{je u. d.}$$

male pot.

$$[gag^{-1}, gbg^{-1}]$$

③

$H \triangleleft G$  in  $G/H$  abelovac

Dovolj pokazati  $\forall a, b \in G. [a, b] \in H$

Vemo  $\forall a, b \in G. (ab)H = (ba)H \iff$

$$(b^{-1}a^{-1}ba) \in H$$

$$\Rightarrow [b, a] \in H \blacksquare$$

① Poisci konutatorcke podgrupe

- a)  $A_4$
- b)  $Q$
- c)  $S_n, n \geq 3$
- d)  $D_{2,n} n \geq 3$

$$\text{a)} K = \{ \text{id}, (12)(3,4), (13)(2,4), (14)(2,3) \} \trianglelefteq A_4$$

$$|A_4/K| = 3 \Rightarrow A_4/K \text{ je abelova}$$

$$\text{Po nalogi 3} \Rightarrow G' \leq K$$

$$G' = \{1\} \Leftrightarrow G \text{ abelova}$$

$$\text{Toreg } A_4' \neq \{1\} \Rightarrow \text{je reda 2 ali 4}$$

$$\text{BESVS } (12)(34) \in A_4' \Rightarrow A_4' = K$$

$$g(12)(34)g^{-1} \in A_4$$

$$g = (132) \Rightarrow (31)(24) \in A_4$$

$$b) Q = \{ \pm 1, \pm i, \pm j, \pm k \}$$

$$H = \{ 1, \pm i \} \quad |G/H| = 2 \Rightarrow j \in \text{abelove} \\ \Rightarrow Q' \leq H \quad \Downarrow \quad H \triangleleft G$$

$$\text{Padobrno } Q' \leq H_j \quad \Rightarrow Q' = \{ \pm j \}$$

$$c) S_n \quad n \geq 3$$

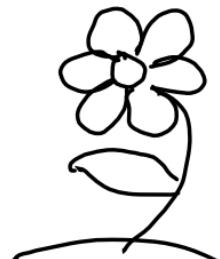
$$|S_3| = 6$$

$$A_3 \quad j \in \text{edinke}$$

$$S_3 / A_3 \quad je \text{ abelove}$$

$$\Rightarrow S_3' \subseteq A_3$$

$$\text{Padobrno } S_n \subseteq A_n$$



$$(a,b)(a,d)(a,b)(a,d) = (a \ b \ d)$$

$$(a \ b \ d) = [(a,b), (ad)] \in S_n' \Rightarrow A_n \subseteq S_n'$$

① Koliko elementov reda 7 je v proststevni  
grupi reda 168

J

---

$$168 \mid 2$$

$$168 = 2^3 \cdot 3 \cdot 7$$

$$84 \mid 2$$

$$42 \mid 2$$

Obstaja 7-podgrupa Sylowa

$$21 \mid 3$$

in je izomorfne  $\mathbb{Z}_7$  k. imo

$$7 \mid 1$$

7 elementov reda 7

$$n_7 \equiv 1 \pmod{7} \quad n_7 \mid 2^3 \cdot 3$$

$$n_7 \in \{1, 8\}$$

$$n_7 = 1 \Leftrightarrow H \text{ je edinka. } \times \text{ (ker enotam)}$$

$$\Rightarrow n_7 = 8. \text{ selevjo se lahko vredi}$$

$$8 \cdot 6 + 1 = 49$$

$$49 \text{ elementov reda 7}$$

② Pokaz de je  $\mathbb{Z}$ -podgrupi  $SL_2(\mathbb{Z}_3)$   
izomorfne grupi  $\mathbb{Q}$  in je edink

$$|SL_2(\mathbb{Z}_3)| =$$

$$= \frac{|GL_2|}{2} = 24 = 2^3 \cdot 3 \quad GL_2: \begin{bmatrix} [\cdot] & [\cdot] \\ [1] & [1] \end{bmatrix} \quad |GL_2| = 48$$

$\left\{ \begin{array}{c} \downarrow \\ 3 \cdot 3 - 1 = 8 \end{array} \right\} \quad \left\{ \begin{array}{c} \downarrow \\ 3 \cdot 3 = 9 \end{array} \right\}$

$$n_2 \mid 3 \quad n_2 \equiv 1 \pmod{2}$$

$$\rightarrow n_2 = \{1, 3\}$$

$$\text{def: } GL_2 \rightarrow \{-1, 1\}$$

$$A \mapsto \det A$$

$$\ker \varphi = \text{SL}_2$$

~~2 podgrupe sistema je edinka~~

ime red 8

$$n_3 \mid 8 \quad n_3 \equiv 1 \pmod{3}$$

$$\text{def } n_3 \in \{1, 4\}$$

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^n = \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix} \quad \text{ime red 3}$$

$\left\{ \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix} \right\} \text{je 3 podgrupe sistema}$

$\left\{ \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 2 & 1 \end{bmatrix} \right\} \text{je 3 podgrupe sistema}$

Torej jih je 6

$6 \cdot 2 = 12$  elementa reda 3

$$\text{red} A = 3 \Rightarrow \text{red}(L \cdot A) = 6$$

Torej najdeno je 8 elementov reda 6

Ostane nam pa 8 elementov

Torej obdelaj s treh podgrupe sistema,  
ker n: je pa ena za vse

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

$I, -I$  in se 6 drugih elementov

$$ij = k \quad i^2 = j^2 = k^2 = -1$$

$$A = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} = \begin{bmatrix} 2 & 3 \\ 3 & 2 \end{bmatrix} = \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix} = I$$

$$B = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} = -I$$

inemo  $A, -A, B, -B$



$$C = AB = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 3 & 2 \\ 1 & 3 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

③ Pokazj, da je grupe reda  $8p$  resljive

Réš/jira:

$$G = G_0 > G_1 > G_2 \dots > G_n = \{1\}$$

$G_i \trianglelefteq G_{i+1} \quad G_i / G_{i+1}$  abelove

ekvivalentno

$$G > G' > G'' \dots > G^{(n)} \dots$$

$$\exists n \in \mathbb{N} \text{ da je } G^{(n)} = \{1\}$$

Dejstvo: Nej bo  $H \trianglelefteq G$  in  $H$  in  $G/H$  resljivi

$\Rightarrow G$  je resljiva

$$|G| = 8p = 2^3 \cdot p$$

$$p=2 \Rightarrow |G|=2^4$$

iz predavanj ven o de so grupe  $p^n$  resljive

kr:  $Z(G) \neq \{1\}$  za konkrete grupe

$$|Z(G)| = p^k$$

$a \in Z(G)$  reda  $p$

$$\langle a \rangle \cong C_p \subseteq Z_G$$

$$\langle a \rangle \trianglelefteq G$$

$$|G/\langle a \rangle| = p^{n-1}$$

indukcija ...  
takoj je  $G$  resljiva

$$p \neq 2 \Rightarrow 8p = 2^3 \cdot p$$

2-podgrupe so leva reda 8

$p$ -podgrupe so leva 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. so leva je cikl.

$H \cong \mathbb{Z}_p$  je resljiva

$$|G/H| = 8 = p^n \text{ je resljiva}$$

$$p=3 \Rightarrow$$

$$n_3 \in \{1, 4\}$$

$$n_3 = 4 \Rightarrow$$

$$\text{red } G = 24$$

8 elementov reda 3 niso v  $\mathbb{Z}_3^2$  pa je

$$n_2 \in \{1, 3\}$$

$n_2 \Rightarrow 1 \quad n_2$  je odlike reda 8

$$|G/\mathbb{Z}_2| = 3 \quad \text{je resljiva}$$

$$n_2 \Rightarrow 3 \text{ reda } 8$$

~~3 elementi~~ elementi parne n!  
trivialni

ne potisneva

$$H, n_1, n_2 \in \{2, 4\}$$

$$H, n_1, n_2 \in \{2, 4\}$$

# Polinom vs polinomske funkcije

$$f(x) = x^2 + x \in \mathbb{Z}_2[x] \quad \text{rational polinome}$$

$$g(x) = 0 \in \mathbb{Z}_2[x]$$

$$h(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$$

Dva polinoma sta enake če imata enake koefficiente

Polinom določuje polinomska funkcijo

$$\tilde{f}(x) = \tilde{g}(x) \quad \text{ker } \tilde{f}(0) = \tilde{g}(0) \text{ in } \tilde{f}(1) = \tilde{g}(1)$$

(4) Določi kvadratni polinom iz  $\mathbb{Z}_4[X]$  ki mu pripada nizelna polinomska funkcija

(5) Naj bo  $F$ -polje. Pokaži da sta naslednje pogoji ekvivalentne

a)  $F$  je končno

b) obstajata različne polinome

$f(x), g(x) \in F[X] \text{ z enako privadeljajo polinomske funkcije}$

(4)

$$\begin{array}{c} x(x-1)(x-2)(x-3) \in \mathbb{Z}_4[X] \\ \hline x & x^2 & 2x \\ \hline 0 & 0 & 0 \\ 1 & 1 & 2 \\ 2 & 0 & 0 \\ 3 & 1 & 2 \end{array} \quad p(x) = 2x^2 + 2x$$

(5)  $F$  je končno polje

$$F = \{a_1, a_2, \dots, a_n\}$$

naredimo:  $(x-a_1)(x-a_2) \cdots (x-a_n)$   
imma nizelne polinomske funkcije

b)  $\Rightarrow a)$

$$\tilde{p}(x) = \tilde{f}(x) \quad \text{Resmo da } n \geq k$$

$$a_n x^n + \dots + a_0 = b_n x^k + \dots + b_0$$

$$a_n x^n + \dots + a_{k+1} x^k + (a_k - b_k) x^k + \dots + (a_0 - b_0) = 0$$

$(f-g)x$  je enačba polinoma

Vemo:  $p(a) \in F[x]$  in  $p'(a) = 0 \Rightarrow (x-a) | p(x)$

$$(f-g)(x) = (x-a) \cdot k \quad \forall a \in F$$

$$\text{st}(f-g) = d$$

vemo  $(a_1, \dots, a_d)$

~~(f-g))~~  $(x-a_i) | (f-g)$  za vse  $a_i$

$$\text{Zato } (f-g)(x) = (x-a_1) \cdots (x-a_d)$$

sterz: 

N-1 ba F pojje derivir de  
nekevstanken polidem  $p(x) \in F[x]$  v  
n razvritih elementih iz F doseže cako  
medrest podeli te sljedeće ~~razsež~~ n

---

v  $a_1, \dots, a_n$  doseže a

$$f(a_1) = \dots = f(a_n) = a$$

~~pređe~~ - a

sljedeći ~~(F(x))~~ ~~(F(x))~~ ~~(F(x))~~

je u vidu  $a_1, \dots, a_n$

tegi  $f(x) = b_0 + b_1(x-a_1) + \dots + b_{n-1}(x-a_{n-1}) + k$

korak ~~je~~  $\Rightarrow$  ~~je~~

① Razstavi na nerazcepne faktorje nad  $\mathbb{R}$

a)  $x^5 - 81x$

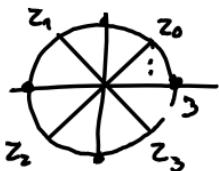
b)  $x^5 + 81x$

Vsek polinom st  $\geq 3$  je razcepem

a)  $x(x^4 - 81) = x(x^2 - 9)(x^2 + 9) =$   
 $= x(x - 3)(x + 3)(x^2 + 9)$

b)  $x(x^4 + 81) =$

$x^4 = -81$



$x^4 + 81 = (x - z_0)(x - z_1)(x - z_2)(x - z_3)$

$= (x^2 + 2ax + (a^2 + b^2))(x^2 + 2\frac{ak}{c}x + (k^2 + b^2))$   
 $a = \frac{\sqrt{2}}{2} \cdot 3 \quad b = \frac{\sqrt{2}}{2} \cdot 3$

$(x - (a+bi))(x - (a-bi)) = x^2 - 2ax + a^2 + b^2$   
 $c = -\frac{\sqrt{2}}{2} \cdot 3 \quad d = \frac{\sqrt{2}}{2} \cdot 3$

$x^2 - 2ax + a^2 + b^2 = x^2 - 2ax + a^2 + b^2$

$x(x^4 + 81) = x(x^2 + 3\sqrt{2}x + 9)(x^2 - 3\sqrt{2}x + 9)$

(2) Pokazi, že je  $f(x)$  neraccepem nad  $\mathbb{Q}$ :

a)  $f(x) = 7x^6 + 30x^3 - 6x^2 + 60$

b)  $f(x) = \frac{2}{7}x^5 - \frac{7}{2}x^2 - x + 2$

Eisensteinaov test

$P \in \mathbb{P}$ .  $f(x) = a_n x^n + \dots + a_1 x + a_0 \quad a_i \in \mathbb{Z}$

$p \mid a_{n-1}, \dots, a_1 \quad p \nmid a_n \quad p^2 \nmid a_0$

$\Rightarrow f(x)$  n: raccepem nad  $\mathbb{Q}$

a)  $7x^6 + 30x^3 - 6x^2 + 60$

$p=3 \Rightarrow$  n: raccepem nad  $\mathbb{Q}$

b)  $14f(x) = 4x^5 - 49x^2 - 14x + 28$

$p=7 \Rightarrow f(x)$  n: raccepem nad  $\mathbb{Q}$

$f(x)$  neraccepem  $\Leftrightarrow 14f(x)$  neraccepem

③

$$f(x) = x^n + 1$$

Pokazi da je f(x) nerazcepen nad Q  
 $\Leftrightarrow n = 2^k \quad k \geq 1$

$$\begin{aligned} (\Rightarrow) \quad n &= 2 \quad x^2 + 1 \quad \text{nerazcepen} \\ n &= 3 \quad x^3 + 1 = (x+1)(x^2 - x + 1) \\ n &= 5 \quad x^5 + 1 = (x+1)(\dots) \end{aligned}$$

↗  
večja zaključek:  $k \geq 1$

Rečimo da n: oblike  $2^k$

Torej  $n = 2^k \cdot l \quad l \dots \text{l}: \text{lo stevilo}$

$\ell \geq 3$

$$x^6 + 1 = x^{2 \cdot 3} + 1 = (x^2)^3 + 1 = (x^2 + 1)(x^4 - x^2 + 1)$$

$$x^{2^k l} + 1 = (x^{2^k})^l + 1 = (x^{2^k} + 1)(\dots)$$

$$\leftarrow \begin{array}{c} x^2 + 1 \\ x^4 + 1 \end{array}$$

če Eisensteinkov kriterij ne deluje za  $f(x)$ ,  
lahko probemo za  $f(x+1)$

$$f(x+1) = (x+1)^4 + 1 = x^4 + 4x^3 + 6x^2 + 4x + 2$$

$$p=2$$

Torej n: razcepen

ker  $f(x+1)$  nerazcepen  $\Leftrightarrow$  f(x) n: razcepen

$$\begin{aligned} f(x+1) &= (x+1)^{2^k} + 1 = \sum_{i=0}^{2^k} \binom{2^k}{i} x^{2^k} + 1 = \\ &= x^{2^k} + \sum_{i=0}^{2^k-1} \binom{2^k}{i} x^{2^k} + 2 \end{aligned}$$

$\binom{2^k}{i}$  je sod  $\Leftrightarrow 1 \leq i \leq 2^k-1$

Potem velja kriterij za  $p=2$

$$f(x+1) = (x+1)^{2^{k+1}} + 1 =$$

$$((x+1)^{2^k})^2 + 1 =$$

Po induktivnosti je dokazan,

$$= (x^{2^k} + \underbrace{\text{sodi}}_{+ 1} + 1)^2 + 1 =$$

$$= x^{2^{k+1}} + \underbrace{\text{sodi}}_{+ 2} + 2$$

④  $\exists \forall n=2,3,4,5,6$

zapis polinom  $f_n(x) = x^n + 1$

je produkt nezáporných polynomů nad  $\mathbb{Z}_2$

⑤ Polynom  $f(x) = x^4 + 1$  zapis je produkt

nezá. nad  $\mathbb{Z}_3$

⑥  $f(x) = x^4 - 2x^3 - 2x + 4$  zapis je produkt  
nezá. nad  $\mathbb{Z}_2$ ,

jež má kořen  $(x-1) \Leftrightarrow f(1) = 0$

$x^2 + x + 1$  je člen: nezáporní v  $\mathbb{Z}_2[x]$   
stupně 2

$$f(x) = x^4 + 2$$

Lemma 2: monostische rotektive in 2 Faktoren

a) linearer Faktor +

$$f(1) = 0$$

$$f(x) = (x-1)(\dots)$$

$$(x^4 + 2) \cdot (x-1) = (x^4 + 2)(x+2)$$

$$x^4 + 2 = (x^2 + 1)(x-1)(x+1)$$

⑥

$$f(x) = x^4 - 2x^3 - 2x + 4 =$$

$$= x^3(x-2) - 2(x-2) =$$

$$= (x^3 - 2)(x-2)$$

isomorph  $x^3 = 2$  zu  $\text{neb } x \in \mathbb{Z}_7$

0	0	0
1	1	1
2	8	1
3	27	-1
-3	-27	1
-2		-1
-1		-1

$$\Rightarrow x^3 - 2 \not\mid$$

nerazteilen

## Kako dosegimo razcepnost nad $\mathbb{Q}$

- 1) Eisensteinov test za  $f(x)$
- 2)  $\rightsquigarrow f(x+1)$
- 3)  $\rightsquigarrow$  preved na polinom nad  $\mathbb{Z}_p$

⑦ Naj bodo  $a_0, \dots, a_n \in \mathbb{Z}$  in  $p \in \mathbb{P}$   
potem

če je polinom  $a_n x^n + \dots + a_1 x + a_0$  razcepna nad  $\mathbb{Q}$   
je  $a_n (\text{mod } p) x^n + \dots + a_1 (\text{mod } p) + a_0 (\text{mod } p)$   
razcepna nad  $\mathbb{Z}_p$

Posledično: če je  $a_n (\text{mod } p) x^n + \dots + a_0 (\text{mod } p)$   
nerazcepna nad  $\mathbb{Z}_p$  je  $a_n x^n + \dots + a_0$   
nerazcepna nad  $\mathbb{Q}$

$\rightarrow$  Po predpostavki je  $p(x)$  razcepna nad  $\mathbb{Q}$ .

$$p(x) = g(x) \cdot k(x) \quad g, k \text{ nekonst}$$

$$= (b_m x^m + \dots + b_0) (c_l x^l + \dots + c_0)$$

$$m+l=n$$

$$a_n = b_m \cdot c_l$$

$\rightarrow p \nmid b_m, c_l$

$\mathbb{Z} \rightarrow \mathbb{Z}_p$

$$n \mapsto n \text{ mod } p$$

sugjetiv:  
homomorfizam  
kelobanje

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

$$\begin{array}{ccc} \mathbb{Z}[x] & \xrightarrow{\text{res}} & \mathbb{Z}_p[x] \\ \underbrace{a_n x^n + \dots + a_0}_{f(x)} & \longmapsto & \underbrace{(a_n \text{ mod } p)x^n + \dots + (a_0 \text{ mod } p)}_{f(x) \text{ mod } p} \\ \text{DN: to je homomorfizam kelobanje} \end{array}$$

$$p(x) \text{ mod } p = (g(x) \text{ mod } p)(k(x) \text{ mod } p)$$

ker  $b_m$  in  $c_l$  nista deljiva s  $p$

Torej se stopnja ohramča

$a, b, c$  like sterke  $\Rightarrow p(x) = ax^4 + bx + c$  neraezen  
nad  $\mathbb{Q}$

---

$$p(x) = 7x^5 + 3x^3 + 1 \text{ neraezen nad } \mathbb{Q}$$

$$p(x) = x^5 + x^3 + 1 \bmod 2$$

$$p(0) = 1$$

$$p(1) = 1$$

De b: bil rezaen je eden od faktor  
 $x^2 + x + 1$

$$(x^5 + x^3 + 1) : (x^2 + x + 1) = x^3 - x^2$$

$$\begin{array}{r} -x^3 - x^4 - x^3 \\ \hline -x^4 - x^3 + x^2 + 1 \end{array}$$

$$\begin{array}{r} +x^4 + x^3 + x^2 \\ \hline 1 \neq 0 \quad n: \text{defjiv} \Rightarrow n: \text{rezaen} \end{array}$$

$$p(x) = 36x^3 + 7x + 6$$

$$p(x) \equiv x^3 + 2x + 1 \pmod{5}$$

$$p(0) = 1$$

$$p(1) = 4$$

$$p(2) = 3$$

$$p(-1) = 3$$

$$p(3) = 4 \quad \text{nicht null} \Rightarrow \text{nicht reziproker}$$

(4)  $a_1, \dots, a_n$  razăriile cele sterile

Potrivit deje  $p(x) = (x-a_1) \dots (x-a_n) - 1$   
nerazăpat ned  $\Omega$

Recunoaște je razărieni

$$p(x) = g(x) \cdot r(x) \quad \text{st}(g(x)) + \text{st}(r(x)) = \text{st}(p(x))$$

Baza de rezolvare: căruță  $\geq n+1$

$$\forall i \in \{1, \dots, n\} \quad p(a_i) = -1 \Rightarrow p(a_i) r(a_i) = -1$$

$g$  în  $r$  imite cele coeficiente

$$g(a_i) = \pm 1 \quad r(a_i) = \mp 1$$

Atunci:

$$\text{I } g(a_i) = 1, r(a_i) = -1$$

$$\text{II } g(a_i) = -1, r(a_i) = 1$$

Baza de rezolvare: căruță  $\geq n+1$  (recunoaște)

$$\text{st}(g) \leq \frac{n}{2}$$
 Baza de rezolvare

$$g(a_i) - 1 = 0$$

$$g(x) - 1 \text{ imite } > \frac{n}{2} \text{ nicio } \times$$

$$\Rightarrow \text{st}(g(x)) = \frac{n}{2} \text{ și } \text{st}(r(x)) = \frac{n}{2}$$

$$g(x) = b_k x^k + \dots + b_0 \quad r(x) = c_k x^k + \dots + c_0$$

$$\text{st}(g(x) - r(x)) \leq \frac{n}{2} - 1$$

Recunoaște I urmărește  $a_1, \dots, a_{\frac{n}{2}}$

În II urmărește  $a_{\frac{n}{2}+1}, \dots, a_n$

$g(x) - 1$  nu are nicio razărie între  $a_1, \dots, a_{\frac{n}{2}}$

$r(x) - 1$  nu are nicio razărie între  $a_{\frac{n}{2}+1}, \dots, a_n$

$$(g(x) - 1)(r(x) - 1) = \underbrace{g(x) \cdot r(x)}_{-1} - r(x) - g(x) + 1 =$$

$$= -(g(x) + r(x)) \text{ nu are } a_1, \dots, a_n \text{ nicio razărie}$$

$\times$  prevedea nicio razărie

$a_1, \dots, a_n$  reelle Zahlen oder Stützstellen

Polynom der ge

$$p(x) = (x-a_1)^2 \cdots (x-a_n)^2 + 1 \text{ nenne es ein neues } Q$$

Rechnen wir je  $\exists r, g \in \mathbb{Q}[X]$  rekenet

$$p(x) = r(x) \cdot g(x)$$

$$p(a_i) = 1$$

$$\forall i \Rightarrow r(a_i) \cdot g(a_i) = 1$$

$$r(a_i) = g(a_i) = \pm 1$$

$p(x) > 0 \quad \forall x \Rightarrow p(x)$  nimmt nicht  $\Rightarrow$   
 $r(x)$  in  $g(x)$  nimmt nicht

$$r(a_i) = 1 \quad \text{in } r(a_j) = -1 \quad \times$$

ker je zweit  $\Rightarrow$

$$(\forall a_i, r(a_i) = 1) \vee (\forall a_i, r(a_i) = -1) \\ \Rightarrow \operatorname{tg}(a_i)$$

$$\text{BZS} \quad r(a_i) = g(a_i) = 1 \quad \forall i:$$

$$r(x) - n \text{ Werte } \geq n \text{ nicht } \Rightarrow \operatorname{st}(r(x)) \geq n \\ \rightarrow \operatorname{st} g(x) \geq$$

$$\Rightarrow \operatorname{st}(r(x)) = \operatorname{st}(g(x)) = n$$

$$\operatorname{st}(p(x) + \operatorname{st}(g(x))) = \operatorname{st}(g(x)) = 2n$$

$$r(a_i) \cdot g(a_i) = 0 \Rightarrow$$

$$\operatorname{st}(g(a_i) - r(a_i)) \geq \sum a_i = 0$$

$$\Rightarrow \cancel{g(x)} - r(x) \quad r(x) = g(x)$$

$$\Rightarrow p(x) = r^2(x)$$

$$p(x) = \underbrace{(x-a_1) \cdots (x-a_n)}_{r(x)} + 1 = r^2(x)$$

$$A^2(x) - r^2(x) = -1$$

$$(r(x) - A(x))(r(x) + A(x)) = 1$$

$$\Rightarrow r(x) - A(x) \text{ je konstanten in} \\ A(x) + r(x) \text{ je konstanten}$$

$\times$  ker im Achsenstrich

# Razširitev polj

$E, F$  polj:

$$E \subseteq F \quad [F:E] \text{ stopnja razširitve}$$

$\downarrow$

$\dim F$  kot vektorštevje polja nad  $E$

$a \in F$

$E(a)$  - razširitev  $F$  s pomogočjo  $A$

↳ najmanjše podpolje  $F, k$  vsebuje  $E$  in  $a$

npr.  $\mathbb{Q}(\sqrt{2}) \supseteq \mathbb{Q}$

"   
  $\{a + b\sqrt{2}; a, b \in \mathbb{Q}\}$

$$[E(a): E] = \text{st}(\min; \text{mehr}; \text{polinom } a \text{ v } E)$$

$$\text{st}(m_a(x)) \quad m_a(x) \in E[x]$$

Če moremo  $E \subseteq F \subseteq G$  razširitev,

$$\text{če } [G:E]=m, [G:F]=k, [F:E]=n \Rightarrow m=kn$$

$$E \subseteq F \quad \alpha \in F$$

$$E(\alpha) = E \Leftrightarrow [E(\alpha) : E] = 1$$

( $\Rightarrow$ ) minimaln: polynom  $x - \alpha \in E$

( $\Leftarrow$ ) Bese  $E(\alpha)$  nad  $E$  je  $\{1\}$

$$\alpha = \alpha \cdot 1 \in E$$
$$\in E$$

①  
Pokerz)  $R(\alpha) = \mathbb{C} \iff \alpha \in \mathbb{C} - R$

$\Rightarrow$  Recmo de  $\alpha \in R$

Potem  $R(\alpha) = R$

$\Leftarrow \alpha \in \mathbb{C} - R$

$$R \subseteq R(\alpha) \subseteq \mathbb{C} \quad [\mathbb{C}:R] = 2$$

outro  $R \neq R(\alpha) \Rightarrow [R(\alpha):R] \geq 2$

$$\Rightarrow [R(\alpha):R] = 2 \rightarrow \overbrace{[R(\alpha):\mathbb{C}]}^{\text{v}} = 1$$

$$\Rightarrow \mathbb{C} = R(\alpha)$$

$$\text{Naj b} \alpha [E:F] = 12$$

Po posm zakej elementiz  $E$  ne mre biti  
algebraiden stopnje 8 nad  $F$

---

a je alg. ne stopnje k nad  $F$  ce

$$[F(\alpha) : F] = k$$

$\Leftrightarrow$  min polinom  $m_\alpha(x) \in F[x]$  ima  
stopnjo k

---

$$[E:F] = 12$$

$$\underbrace{F \subseteq F(\alpha) \subseteq E}_{8}$$

12

$$8 \cdot k = 12$$

$$k = \frac{3}{2} \notin \mathbb{Z}$$

\*

Primer:

$$\mathbb{Q}(\sqrt[12]{2})$$

$x^{12} - 2$  je minimalni polinom po Eisensteineru  
koridzje

$$\sqrt[4]{2} = \alpha^3 \in \mathbb{Q}(\sqrt[12]{2})$$

$$\underbrace{\mathbb{Q}}_4 \subseteq \underbrace{\mathbb{Q}(\sqrt[4]{2})}_3 \subseteq \underbrace{\mathbb{Q}(\sqrt[12]{2})}_1$$

12

Nej bo n lho stevilo

4.4

$\forall a \in \mathbb{Q} (\sqrt[n]{2}) - \mathbb{Q}$  velyz  $a^2 \notin \mathbb{Q}$

...

② Nej bo  $[E:F] = p$  pravljivo  
 $\exists F$

Po pravljivo elementi  $E/F$  je alg. stopenji  
p nad  $F$

$F \subseteq F(\alpha) \subseteq E$  verne

$$\underbrace{\quad}_{\geq 2r} \underbrace{\quad}_K \underbrace{\quad}_P$$

$$p = r \cdot k \Rightarrow r=1 \vee k=1$$

$$\Rightarrow k=1$$

$$\Rightarrow r=p$$

$$③ \text{Kohde je } [\mathbb{Q}(\tilde{\alpha}) : \mathbb{Q}]?$$

$$\text{Kohde je } [\mathbb{Q}(3\sqrt[3]{7} + 4\sqrt[3]{49}) : \mathbb{Q}]?$$

$$\alpha^2 = 9 - 6\sqrt{7} + 7$$

$$(x^2 - 6x)(\alpha) = 16 - 6\sqrt{7} - 18 + 6\sqrt{7} = -2$$

$$\begin{array}{c} p(x) = x^2 - 6x + 2 \\ \uparrow \text{nur reellen, } \text{Eisenstein} \\ \text{stg. raditive} = 2 \end{array}$$

2. nac*h*

$$[\mathbb{Q}(\sqrt{7}) : \mathbb{Q}] = r \quad \alpha \in \mathbb{Q}(\sqrt{7})$$

$$\Rightarrow \mathbb{Q} \subseteq \mathbb{Q}(\alpha) \subseteq \mathbb{Q}(\sqrt{7})$$

$$\underbrace{\quad}_{r \neq 1} \quad \underbrace{\quad}_{1} \quad \underbrace{\quad}_{2}$$

$$\Rightarrow r = 2$$

$$[\mathbb{Q}(3 - 5\sqrt[3]{7} + 4\sqrt[3]{49})]$$

$$\text{Vom } [\mathbb{Q}(\sqrt[3]{7}) : \mathbb{Q}] = 3 \quad \text{ker } x^3 - 7 \text{ ist: } b \in \mathbb{Q}(\sqrt[3]{7})$$

$$\begin{array}{c} \mathbb{Q} \subseteq \mathbb{Q}(b) \subseteq \mathbb{Q}(\sqrt[3]{7}) \\ b \notin \mathbb{Q} \Rightarrow r \neq 1 \quad \Rightarrow r = 3 \end{array}$$

$$b \in \mathbb{Q} \quad 3 - 5\sqrt[3]{7} + 4\sqrt[3]{49} = \alpha$$

$$4x^2 - 5x + 3 - \alpha \quad \text{anihiliert } \sqrt[3]{7}$$

Anmerkung:  $x^3 - 7$  tridi anihiliert in  $\mathbb{N}$ :

delj: v  $\times$

Naspratuje linear: neodvisnosti

(Baza: 1,  $\sqrt[3]{7}$ ,  $\sqrt[3]{49}$ )

$$p(x) = 3 - 5x + 4x^2$$

$$\Rightarrow (p(x), x^3 - 7) = 1$$

$$\alpha(x)p(x) + \beta(x)(x^3 - 7) = 1$$

$$x = \sqrt[3]{7}$$

$$b^{-1} = \alpha(\sqrt[3]{7})$$

⑤ Kekiko ju  $[\mathbb{Q}(\underbrace{\sqrt[3]{3+\sqrt{3}}}_{\alpha}) : \mathbb{Q}]$

$$\alpha^6 = (3+\sqrt{3})^2 = 9 + 6\sqrt{3} + 3 = 12 + 6\sqrt{3}$$

$$\alpha^3 = 3 + \sqrt{3}$$

$$\alpha^6 - 6\alpha^3 = 12 - 18 + 6\sqrt{3} - 6\sqrt{3} = -6$$

$$\alpha^6 - 6\sqrt{3} + 6 \quad P_6 \text{ eisensteinkinse}$$

$$\Rightarrow [\mathbb{Q}(\sqrt[3]{3+\sqrt{3}}) : \mathbb{Q}]$$

$\Delta_6$  algebraic:

$$\text{Pf der } \Rightarrow [F(\alpha, \beta) : F] = [F(\alpha) : F] \cdot [F(\beta) : F]$$

$$F \subseteq \underbrace{F(\alpha)}_{m} \subseteq \underbrace{F(\alpha, \beta)}_{k}$$

Zeile 5 ist s:  
zu j;

$$F \subseteq \underbrace{F(\beta)}_{n} \subseteq \underbrace{F(\alpha, \beta)}_{c}$$

$$F(\alpha, \beta) = mk = nc$$

$$\Rightarrow m | [F(\alpha, \beta) : F] \wedge n | [F(\alpha, \beta) : F]$$

$$\Rightarrow mn | [F(\alpha, \beta) : F]$$

$$[F(\beta) : F] = n \Rightarrow \exists p(x) \in F[X], p(\beta) = 0$$

in je neigen

$$p(x) \in F[\kappa]$$

$$\Rightarrow p(x) \in F(\alpha)[\kappa]$$

$$p(\beta) = 0$$

$$\Rightarrow [F(\alpha, \beta) : F(\alpha)] \leq n \Rightarrow k \leq n \Rightarrow$$

$$[F(\alpha, \beta) : F] = mk \leq m \cdot n \Rightarrow = m \cdot n$$

④ ~~問~~

$$[\mathbb{Q}(\sqrt{3}, \sqrt[3]{7}) : \mathbb{Q}] = ?$$

$$2 \cdot 3 = 6$$

$$\textcircled{8} \quad [\mathbb{Q}(\sqrt{3} + \sqrt[3]{5}) : \mathbb{Q}] = ?$$

\textcircled{9} Paket da ja

$$[\mathbb{Q}(\sqrt{3}, i) : \mathbb{Q}] = 4$$

Parize; a, da je  $\mathbb{Q}$   $\mathbb{Q}(a) = \mathbb{Q}(\sqrt{3}, i)$

---

Komentar

irrek o primitivem elementu

$$\mathbb{Q}(\sqrt{3}, \sqrt[3]{5}) = \mathbb{Q}(\sqrt{3} + \sqrt[3]{5})$$

---

$$[\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2 \quad [\mathbb{Q}(\cdot)] = 2$$

① Punkt:  $F(a^k, a^\ell) = F(a^d)$ ;  $d = (k, \ell)$

②  $[\mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}) : \mathbb{Q}]$  in  $[\mathbb{Q}(\sqrt[6]{2}, \sqrt[6]{2}) : \mathbb{Q}]$

$$\begin{aligned} k &= d \cdot \alpha \\ l &= d \cdot \beta \end{aligned} \quad \begin{aligned} a^k &= a^{d\alpha} = (a^d)^\alpha \\ a^l &= a^{d\beta} = (a^d)^\beta \end{aligned}$$

$$F(a^k, a^l) \subseteq F(a^d)$$

Dann ist ja  $a^d$  in  $F(a^k, a^l)$

$$d = mk + nl \quad m, n \in \mathbb{Z}$$

$$a^d = a^{mk+nl} = (a^k)^m \cdot (a^l)^n \in F(a^k, a^l)$$

$$\textcircled{2} \quad \mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}) = \mathbb{Q}(z^{\frac{1}{6}})$$

$$z^{\frac{1}{2}}, z^{\frac{1}{3}} = z^{\frac{1}{6} \cdot 3}, z^{\frac{1}{6} \cdot 2}$$

$$[\mathbb{Q}(z^{\frac{1}{6}}) : \mathbb{Q}] = 6$$

Ker  $x^6 - 2$  mindestens polieren  
in je neunzehnten  $\varphi$ -eisensteiner

$$\mathbb{Q}(\sqrt[6]{2}, \sqrt[6]{2}) = \mathbb{Q}(\sqrt[12]{2})$$

$$2^{\frac{1}{4}} = 2^{\frac{3}{12}} \quad [\because \dots] = 12$$

$$2^{\frac{1}{6}} = 2^{\frac{2}{12}} \quad \begin{matrix} \text{Ker } x^{12} - 2 \\ \text{heraus } \varphi \text{-eisensteiner} \end{matrix}$$

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

$$[\mathbb{Q}(\sqrt[6]{3}, i) : \mathbb{Q}(\sqrt{3} + i)]$$

$$\mathbb{Q}(\sqrt[6]{3}, i) \supseteq \overbrace{\mathbb{Q}(\sqrt{3} + i)}^F$$

$$\sqrt{3} + i = 3^{\frac{1}{2}} + i = 3^{\frac{3}{6}} + i = (\sqrt{6})^3 + i \in F$$

$$\mathbb{Q}(\sqrt{3} + i) = \mathbb{Q}(\sqrt{3}, i)$$

$$\subseteq \checkmark$$

$$2 \quad a = \sqrt{3} + i$$

$$i = a - \sqrt{3}$$

$$-1 = a^2 - 2\sqrt{3} + 3$$

$$2\sqrt{3} = a^2 + 4$$

$$\underbrace{\mathbb{Q}}_{1} \subseteq \mathbb{Q}(\sqrt{3}, i) \subseteq \mathbb{Q}(\sqrt[6]{3}, i)$$

$$\underbrace{\mathbb{Q}}_{2} \subseteq \mathbb{Q}(\sqrt{3}) \subseteq \mathbb{Q}(\sqrt{3}, i) \subseteq \mathbb{Q}(\sqrt[6]{3}, i)$$

$$\underbrace{\qquad}_{4}$$

$$\underbrace{\mathbb{Q} \subseteq \mathbb{Q}(i)}_{2} \subseteq \underbrace{\mathbb{Q}(\sqrt[6]{3}, i)}_{6}$$

$$\underbrace{\qquad}_{12}$$

12

$$\Rightarrow [\mathbb{Q}(\sqrt[6]{3}, i) : \mathbb{Q}(\sqrt{3} + i)] = 3$$

6) Pokézni, da  $\mathbb{Q}(\sqrt{3}) \neq \mathbb{Q}(\sqrt{2})$

② Negj leda  $a_1, \dots, a_n$  algel. ned F

Pokéz:

$$[F(a_1, \dots, a_n) : F] \leq [F(a_1) : F] \cdots [F(a_n) : F]$$

③ Negj leda  $\rho: \mathbb{Q}(\sqrt{2}) \rightarrow \mathbb{Q}(\sqrt{3})$  i-formatívan

$$\rho(1) = 1 \quad \wedge \quad \rho(0) = 0$$

$$\rho(2) = 2 \quad \text{ker } 1+1=2 \quad \rho(1)+\rho(1)=2$$

$$\rho(n) = n \quad \forall n \in \mathbb{Z} \quad \rho(n^{-1}) = \rho(n)^{-1} = n^{-1}$$

$$\rho\left(\frac{m}{n}\right) = \rho(m \cdot n^{-1}) = \rho(m) \cdot \rho(n^{-1}) = m \cdot n^{-1}$$

→  $\rho$  áhranja racionálne čísla

$$\rho(a+b\sqrt{2}) = a+b\rho(\sqrt{2})$$

$$\rho(\sqrt{2}) = \alpha + \beta\sqrt{3}$$

$$\rho(2) = \alpha^2 + 2\alpha\beta\sqrt{3} + 3\beta^2 = 2$$

$$2\alpha\beta\sqrt{3} = \underbrace{2 - \alpha^2 - 3\beta^2}_{\in \mathbb{Q}}$$

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



$$\beta = 0 \Rightarrow \alpha^2 = 2 \quad \alpha \notin \mathbb{Q} \quad *$$

$$\alpha = 0 \Rightarrow 3\beta^2 = 2 \Rightarrow \beta = \sqrt{\frac{2}{3}} \notin \mathbb{Q}$$

amplak  
nem  
rational

⑦

$n=2:$

$$\underline{F(a,b)} \leq \underline{F(a) \cdot F(b)}$$

$$[F(a,b) : F] \leq \underbrace{[F(a) : F]}_k \cdot \underbrace{[F(b) : F]}_m$$

$$\underbrace{F \subseteq F(a)}_k \subseteq \underbrace{F(a,b)}_m$$

Vemo:  $[F : F(b)] = m \Rightarrow \exists p(x)$  nerez  $c \in F[x]$   
 $p(b) = 0 \quad \text{st}(p(x)) = m$

$$p(x) \in F(a)[x]$$

$p(x)$  je mordne rezgen

Torej minimelni polinom st.  $\leq m$

Podobno za vec njev

⑧ Nejlepši a1, ..., an algebraični: stopnje 2

Pokazi da stopnja razstavljive

$$[F(a_1, \dots, a_n) : F] = 2^k \text{ za neki } k \leq n$$

⑨ Za razlike preostala pa...

$$[\mathbb{Q}(g_1, \dots, g_n) : \mathbb{Q}] = 2^k$$

$$\underbrace{F \subseteq F(g_1)}_2 \subseteq \underbrace{F(g_1, g_2)}_{\leq 2} \subseteq \underbrace{F(g_1, g_2, g_3)}_2 \subseteq \dots \subseteq F(g_1, \dots, g_n)$$

$\Rightarrow$  Vseki imamo izbirko 1 ali 2

Razina je pa k 2  $\Rightarrow$

$$[F(a_1, \dots, a_n) : F] = 2^k \quad k \leq n$$

⑩ Dokazati mimo in A\_p

$$x^2 - p \text{ ni razcegan v } \mathbb{Q}(g_1, \dots, g_n) \in \mathbb{P}$$

$$\mathbb{Q} \subseteq \underbrace{\mathbb{Q}(\sqrt{2})}_F \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3}) \subseteq \dots$$

$$\text{Vemo: } F(\sqrt{a}, \sqrt{b}) \supseteq F$$

$$\sqrt{a}, \sqrt{b}, \sqrt{ab} \notin F$$

$$\underbrace{F \subseteq F(\sqrt{a})}_{2} \subseteq \underbrace{F(\sqrt{a}, \sqrt{b})}_{?}$$

$$F \subseteq F(\sqrt{b}) \subseteq F(\sqrt{a}, \sqrt{b})$$

$$\sqrt{b} = \alpha + \beta\sqrt{a} \quad \alpha, \beta \in F$$

$$b = \alpha^2 + 2\alpha\beta\sqrt{a} + \beta^2 a$$

$$2\alpha\beta\sqrt{a} = b - \alpha^2 - \beta^2 a$$

$$\text{če } \alpha, \beta \neq 0 \Rightarrow \sqrt{a} \in F$$

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

$$\alpha = 0 \Rightarrow b = \beta^2 a$$

$\Rightarrow a_1, \dots, a_n \in F$  en  $a_1, \dots, a_n$  nide

18.4

$$h(x) := g \operatorname{cd}(f(x), f'(x))$$

$$h(x) = \alpha x_1 f(x) + \beta(x) \cdot p^1(x) \in F(x)$$

$$h(x) \neq 1 \Rightarrow$$

$$(x-b)_k \in A \quad e \in [k]$$

$$\rightarrow \text{neut } E : (x \rightarrow \perp) | (f(x), f'(x))$$

$$b - 2x \leq f$$

$$f(x) = (x-6)r(x)$$

$$f'(x) = r(x) + (x-b)r'(x)$$

$$\Rightarrow (x-6) \mid r(cx) \Rightarrow$$

$$(x-6)^2 \int f(x) dx$$

←

f<sub>as</sub> f<sub>as</sub>' type

$$1 = \alpha(x) \cdot f(x) + \beta(x) f'(x) \quad \in F(x)$$

$$\exists a \in E \quad \text{da} \quad (x-a)^2 \mid f(x)$$

$$f(x) = (x - \alpha)^2 k(\alpha)$$

$$f'(x) = 2(x-a)kcx + k_2(x-a)^2$$

$$1 = \underset{\text{systems}}{\overset{\Rightarrow}{\circ}} x = a$$

2) Naj bo  $F$  polje karakteristike 0

in  $F \subseteq E$   $E/F$

Pokaži:  $a \in E$  je  $k$ -kratna nula po  $F$   $\iff$

$$\iff f(a) = f'(a) = \dots = f^{(k-1)}(a) = 0$$

$$\text{in } f^{(k)}(a) \neq 0$$

$a$  je  $k$ -kratna nula po  $F$   $\iff$

$$(x-a)^k \mid f(x) \quad \text{in } (x-a)^{k+1} \nmid f(x)$$

$$f(x) = f(a) + \frac{f'(a)}{1!}(x-a) + \frac{f''(a)}{2!}(x-a)^2 + \dots$$

(Lahko ker char  $F = 0$ )

$\Rightarrow$  predpostavimo  $a$   $k$ -kratna nula

$$f(x) = f(a) + \dots + \underbrace{\frac{(x-a)^{k-1}}{k!} f^{(k-1)}(x)}_{\text{nevedljiv}} + (x-a)^k h(x)$$

$$f(a) = 0$$

$x$   
nevedljiv

$(x-a) \dots (x-a)^k \Rightarrow$  linearne neodvis.

$$\Rightarrow f(x) = \frac{f'(a)}{1!} - \dots - \frac{f^{(k-1)}(a)}{(k-1)!} = 0$$

$\Rightarrow$

\*

$$f(x) = 0 \dots f^{(k-1)}(x) = 0$$

$$f^{(k)}(a) \neq 0$$

Opomba.  $f(x)$  nerezogen ( $\exists \epsilon > 0$   $|f(x)|_n < \epsilon$ )

$$\text{st } (f'(x)) < f(x)$$

$$\Rightarrow ((f(x), f'(x)) \neq 1 \Leftrightarrow f'(x) = 0)$$

③ Pojasni: zakaj  $\mathbb{Q}(\sqrt{2})$  je razpredno polje vsakega izmed polinomov

$$x^2 - 2$$

$$3x^3 - 6x$$

$$x^4 - 3x^2 + 2$$

Razpredno polje  $f(x)$  je najmanjša razširitev  $E$  polja  $F$ , da  $f(x)$  razpredne v  $E$  na linearne faktorje

$\alpha_1, \dots, \alpha_k$  vse nicle  $f(x)$

$$E = F(\alpha_1, \dots, \alpha_k)$$

$$f(x) = x^2 - 2 \quad \text{nicle: } \sqrt{2}, -\sqrt{2}$$

$$\Rightarrow (x - \sqrt{2})(x + \sqrt{2})$$

$$\mathbb{Q}(\sqrt{2}, -\sqrt{2}) = \mathbb{Q}(\sqrt{2})$$

$$\begin{aligned} f(x) &= 3x^3 - 6x = 3x(x^2 - 2) = 3x(x - \sqrt{2})(x + \sqrt{2}) \\ \Rightarrow \mathbb{Q}(0, \sqrt{2}, -\sqrt{2}) &= \mathbb{Q}(\sqrt{2}) \end{aligned}$$

$$\begin{aligned} f(x) &= x^4 - 3x^2 + 2 = (x^2 - 2)(x^2 - 1) = \\ &= (x - \sqrt{2})(x + \sqrt{2})(x - 1)(x + 1) \end{aligned}$$

$$\rightarrow \mathbb{Q}(\sqrt{2})$$

④ Pojedini zakej je  $\mathbb{Q}(\sqrt{2}, \sqrt{3})$   
razpredno polje polinoma

$$x^4 - 5x^2 + 6 \in \mathbb{Q}[x]$$

$$P(x) = (x^2 - 2)(x^2 - 3) = (x - \sqrt{2})(x + \sqrt{2})(x - \sqrt{3})(x + \sqrt{3})$$

$$E = \mathbb{Q}(\sqrt{2}, -\sqrt{2}, \sqrt{3}, -\sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$$

## ⑤ Označimo

$\omega = -\frac{1}{2} + i \frac{\sqrt{3}}{2}$  primjativ; 3 koren iz enote

Pozor!:  $\mathbb{Q}(\sqrt[3]{2}, \omega)$  dobiva razpadno polje  
polinoma  $x^3 - 2 \in \mathbb{Q}[x]$

Pošto stepenje razpadnoga polja nad  $\mathbb{Q}$

$$x^3 - 2 = (x - \sqrt[3]{2})(x^2 + \sqrt[3]{2}x + 2)$$

$$\mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2) = \mathbb{Q}(\sqrt[3]{2}, \omega)$$

$\subseteq \checkmark$

$$2 \quad \omega = \frac{\sqrt[3]{2}\omega}{\sqrt[3]{2}}$$

stepenje:

$$\overbrace{\mathbb{Q}}^1 \subseteq \overbrace{\mathbb{Q}(\omega)}^2$$

$$\underbrace{\mathbb{Q}}_3 \subseteq \underbrace{\mathbb{Q}(\sqrt[3]{2})}_2 \subseteq \underbrace{\mathbb{Q}(\sqrt[3]{2}, \omega)}_{\leq 2 \neq 1} \Rightarrow 6$$

$$\left(\omega + \frac{1}{2}\right)^2 = \left(i \frac{\sqrt{3}}{2}\right)^2 = -\frac{3}{2}$$

$$\text{pol. } \left(x + \frac{1}{2}\right)^2 \oplus$$

### 6) Pokazi

a)  $\mathbb{Q}(\zeta)$  je razredno polje podleme

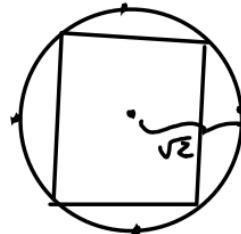
$$x^4 + 4 \in \mathbb{Q}[x]$$

b)  $\mathbb{Q}(\sqrt[4]{2}, i)$  je razredno polje podleme

$$x^4 + 2 \in \mathbb{Q}[x]$$

c)  $\mathbb{Q}(\sqrt[4]{2}, i)$  razredno polje  $x^4 + 1 \in \mathbb{Q}[x]$

a)  $x^4 - 4 = \cancel{(x-2)} \cdot \cancel{(x+2)} (1+i)(1-i)(-1+i)(-1-i)$



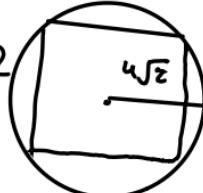
$$x^4 = -4$$

$$\sqrt[4]{2} \frac{\sqrt{2}}{2} (1+i) \cdot \sqrt[4]{2} \frac{\sqrt{2}}{2} (-1+i)$$

$$\sqrt[4]{2} \frac{\sqrt{2}}{2} (-1-i) \cdot \sqrt[4]{2} \frac{\sqrt{2}}{2} (1-i)$$

Razredno polje:  $\mathbb{Q}(i, -i) = \mathbb{Q}(i)$

b)  $x^4 + 2$



$$x^4 = -2$$

$$x^4 + 2 = \cancel{4\sqrt[4]{2} \frac{\sqrt{2}}{2}} (1+i) = \cancel{\frac{4\sqrt{2}}{4}} = \frac{1}{4\sqrt{2}}$$

$$x^4 + 2 = \left(x - \frac{1}{4\sqrt{2}} (1+i)\right) \left(x - \frac{1}{4\sqrt{2}} (1-i)\right) \dots$$

$$\mathbb{Q}\left(\frac{1}{4\sqrt{2}} (1+i), \dots\right)$$

$$\supseteq \checkmark$$

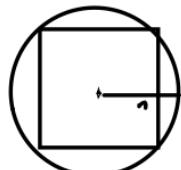
$$i : \frac{1}{4\sqrt{2}} (1+i) - \frac{1}{4\sqrt{2}} (1-i) = \frac{1}{4\sqrt{2}} (2i).$$

$$\frac{1}{4\sqrt{2}} = \frac{1}{4\sqrt{2}} ((1+i) + (1-i)) = \frac{2}{4\sqrt{2}}$$

$$i \Rightarrow \cancel{\sqrt[4]{2}}$$

/2

c)  $x^4 + 1 = \left(x - \frac{\sqrt[4]{2}}{2} (1+i)\right) \left(x - \frac{\sqrt[4]{2}}{2} (1-i)\right) \left(x - \frac{\sqrt[4]{2}}{2} (-1+i)\right) \left(x - \frac{\sqrt[4]{2}}{2} (-1-i)\right)$



$\subseteq \checkmark$

$$\sqrt{2} : \alpha + \beta = \frac{\sqrt{2}}{2} (2) = \sqrt{2}$$

$$i : \frac{\sqrt{2}}{2} (\alpha + \beta) = \frac{\sqrt{2}}{2} (2i) \cdot \sqrt{2} = ;$$

$f(x) \in F[x]$  st( $f(x)$ ) = n

E - razpredno polje po F

$$\text{pošto } [E:F] \leq n!$$

in  $n! [E:F]$  će f(x) nerazgren.

$$X^3 - 2 : [E:F] \leq 6$$

$$3 \mid [E:F]$$

$$E = F(a_1, \dots, a_k) \quad a_i \text{ nicle } k \leq n$$

$$F \subseteq \underbrace{F(a_1)}_{\leq n} \subseteq \dots \subseteq F(a_n) \leq n!$$

$\leq n \leq (n-1) \dots 1$

↑ ker smo smo nicle že uvelizan  
stopnja mn. rednega polinoma

$$f(x) = (x-a_1) g(x) \text{ nad } F(a_1)$$

$$\deg(g) = n-1$$

$$\text{če } n: \text{ razgren} \Rightarrow \underbrace{g \in F(a_1)}_h$$

Zemeda 15 min



Definio de  $F$  ni algebraična zgrada

$\exists f(a)$  ki nima nicle v  $F$

Naj bo  $a$  ta nicle.  $F(a)$  naj bo razširitev

$a \in F(a) \Rightarrow F(a) \neq F$

Prva stopnja  $n \Rightarrow [F(a) : F] \leq n$

Ker je končno

③

Naj bo  $E \geq R$  konce razsiritev realnih števil  
Pokaži da je  $E \cong \mathbb{C}$

Ne tabl.

(4.)

Oglejmo si polinom

$$f(x) = x^2 + x + 1 \in \mathbb{Z}_2[x]$$

je nerazcešen nad  $\mathbb{Z}_2[x]$

$\mathbb{Z}_2[x]$ .

$$F = \frac{\mathbb{Z}_2[x]}{(x^2 + x + 1)} \quad I = (x^2 + x + 1)$$

$x^2 + x + 1$  je maksimalni ideal (ker je polinom nerazcešen)

$$\left( \begin{array}{l} (x^2 + x) \text{ n: maksimalni ker } \\ x^2 + x = x(x+1) \text{ Torej } (x) \supseteq (x^2 + x) \end{array} \right)$$

elementi tege polje so  $p(x) + I$

$$p(x) + I = q(x) + I \Leftrightarrow p(x) - q(x) \in I$$

st  $(p(x)) \geq 2$

$$p(x) = \underbrace{a(x) \cdot (x^2 + x + 1)}_{\in I} + g(x)$$

$$\Rightarrow F = \frac{\mathbb{Z}_2[x]}{(x^2 + x + 1)} = \left\{ \begin{array}{l} \text{sestavki} \\ \text{in} \\ \text{merni} \\ \text{polinom} \\ \text{so konstantno} \\ \text{st} \leq 1 \end{array} \right\} = \{0 + I, 1 + I, x + I, x + 1 + I\}$$

$$= \{0, 1, \bar{x}, \bar{x} + 1\} \cong \mathbb{Z}_2$$

$\bar{x}$  je nide  $x^2 + x + 1$  nad F

$$\begin{aligned} \bar{x}^2 + \bar{x} + 1 &= (\bar{x} + I)^2 + (\bar{x} + I) + 1 + I = \\ &= (x^2 + x + 1) + I = I = 0 + I \end{aligned}$$

+	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	$\bar{x}$

$$\bar{x}^2 + 2\bar{x} + 1$$

$$\bar{x} \cdot \bar{x} = Ix^2 + I$$

$$\begin{array}{r} x^2 + (x^2 + x + 1) = 1 \\ -x^2 - x - 1 \\ \hline -x - 1 \end{array}$$

$$\cancel{x^2 + 1}$$

$$\cancel{x^2 + 1}$$

Pokaži da je  $F$  (prejšnja stran)

Razpadna polje  $x^2+x+1 \in \mathbb{Z}_2[x]$

$\bar{x}$  je nicle

Najti merjivo vse nicle

Nosilnosti  $\bar{x}$  in  $\bar{x}+1$

$$f(\bar{x}+1) = \bar{x} + \bar{x} + 1 + 1 = 0$$

Poniam je stopnje 2, torej ima največ dve nisci  $\Rightarrow$  nosilnosti 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  $\log_2(x) \in \mathbb{Z}_p[x]$  nemačen stepen n  
 ipohetib da  $\underbrace{GF(p^n)}_{\text{konkreto polje}} = \frac{\mathbb{Z}_p[x]}{(g(x))}$   
 s  $p^n$  elementi

$$2) \text{ pokuši } 2 \Leftrightarrow |x^{p^n} - x|$$

$$GF(p^n) \text{ je razvedeno polje } x^{p^n} - x$$

$$x^{p^n} - x = \prod_{a \in GF(p^n)} (x-a)$$

Primer:

$$GF(2^2) = \{1, 0, \alpha, \alpha+1\}$$

$$\alpha = \bar{x}$$

$$x^4 - x = x \cdot (x-1)(x-\alpha) \underbrace{(x-(\alpha+1))}_{x^2+x+1} \text{ nad } F$$

$$x^4 - x = x(x-1)(x^2+x+1) \text{ nad } \mathbb{Z}_2$$

1)

Elemente  $F$  so dass:  $p \in x + I$   
 $\text{st}(p(x)) < n$

$$a_0 + a_1 x + \dots + a_{n-1} x^{n-1} + I$$

$$\text{so Elemente} \Rightarrow |F| = p^n$$

Da bzgl.:  $F \cong GF(p^n)$

■

2)

$$\bar{x} \in \text{nicht } g(x+I) = g(x) + I = I = 0$$

$$x^{p^n} - x = \prod_{a \in F} (x-a)$$

$$\bar{x} \in \text{nicht } F, \text{ da } \bar{x} \text{ od } g(\bar{x}) \text{ in } x^{p^n} - x$$

$$\text{in } g(x) + x^{p^n} - x \quad \text{pdem stetig}$$

$$\exists k(x), l(x) \in \mathbb{Z}_p[x] \text{ da } g(x)k(x) + l(x) \cdot (x^{p^n} - x) = 1$$

Vergleiche  $\bar{x}$

$$g(\bar{x})k(\bar{x}) + l(\bar{x})(\bar{x}^{p^n} - \bar{x}) = 1$$

"

"

$$0 = 1 \quad \times$$

## Pokazi

$$\hookrightarrow GF(8) = \mathbb{Z}_2[x] / (x^3 + x + 1)$$

$$b) GF(5) = \mathbb{Z}_3[x] / (x^2 + 1)$$

$$c) GF(16) = \mathbb{Z}_2[x] / (x^4 + x + 1)$$

$\exists$  Reši: Množina  $x^8 - x$  je produkt polinomov iz  $\mathbb{Z}_2[x]$

GF(8) je razdeljena po  $x^8 - x$

Ustvari je prejšnje rezultat, samo razcegnost moramo preveriti

a)  $x^3 + x + 1$  je razcegen inačič

$$0: 0+0+1 = 1$$

$$1: 1+1+1=1 \quad \text{ne je nista}$$

$$I = x^3 + x + 1$$

$$f(x) + I = \overline{f(x)}$$

$$(x^2 + 1)^{-1}$$

$$(x^2 + 1, x^3 + x + 1) = 1 \quad \in I$$

$$1 = s(x)(x^2 + 1) + \underbrace{f(x)(x^3 + x + 1)}_{\in I} \in \mathbb{Z}_2[x]$$

$$\vee \frac{\mathbb{Z}_2[x]}{I} \quad 1 = \overline{s(x)} \cdot \overline{x^2 + 1}$$

c) Vemo od prej da je razcegen polinom invec

$$x^8 - x = x(x^7 - 1) = x(x-1)(x^6 + \dots + 1)$$

$$\mathbb{Z}[x] / x^n - x$$

$\uparrow$   
st 3 ravnacjan (ker je n=3)  
vemo je a reljeg e.)

$$(x^6 + x^5 + x^4 + x^3 + x^2 + x + 1) : (x^3 + x + 1) = x^2 + x^2$$

$$\begin{array}{r} \cancel{x^6} \\ -x^5 \\ \hline x^5 + x^4 \\ -x^5 \\ \hline x^4 + x^3 \\ -x^3 - x^2 \\ \hline x^2 + x \\ -x^2 - x \\ \hline x \end{array}$$

Kerima  $x^8 - x$  same razljevi in se  
e deljivo je se ena mesta



$$x^8 - x = x(x-1)(x^3 + x^2 + x + 1)(x^3 + x^2 + 1)$$

Naj bo  $[L : K] = 2$ . Pokaz de je  $L \supseteq K$  normatna 3,5

Vzemimo nek polinom stopnje 2

$$(x-a)(x-b) = x^2 - x(a+b) + ab$$

Recimo da  $a \in K$   $b \in L - K$

$$\begin{aligned} d &= ab \stackrel{c}{=} \text{mera bidi nad } K \\ &= ab \text{ mera bidi nad } K \end{aligned}$$

$$b = a - c \in K \quad \times$$

Kdaj je razširitev normatna?

•  $L$  je razpadno polje  $f(x) \in K[x]$

• ce  $f(x) \in K[x]$  nerazce v imenici  $L$ ,  
razpede nad  $L$

Določiti ali je naslednja razširitev polje a normirano

Koristna mogoč

a)  $\mathbb{Q}(\sqrt{2}, i)$

b)  $\mathbb{Q}(\sqrt[4]{2})$

c)  $\mathbb{Q}(\sqrt[3]{2}, i)$

d)  
 $f(x) = (x^2 - \sqrt{2})(x+1)$

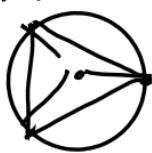
$$\mathbb{Q}(\sqrt{2}, -\sqrt{2}, i, -i) = \mathbb{Q}(\sqrt{2}, i)$$

b)

$$g(x) = x^4 - 2 = (x - \sqrt[4]{2})(x + \sqrt[4]{2})(x - \sqrt[4]{2}i)(x + \sqrt[4]{2}i)$$

B) nepravilno, ima vključno  $\sqrt[4]{2}$  v L in ima kompleksne nicle  $\Rightarrow$  ne razpade na linearne faktorje  $\Rightarrow$  razširitev n: normirana

c)  
 $h(x) = (x^3 - 2)(x+1) =$



$$(x - 3\sqrt{2})(x - \left(\frac{1}{2} + \frac{\sqrt{3}}{2}i\right))(x - \left(\frac{1}{2} - \frac{\sqrt{3}}{2}i\right))$$

$$\downarrow$$

$$\frac{\sqrt{2}}{2} \quad \frac{\sqrt{6}}{2} \quad \frac{\sqrt{3}}{2} \quad \frac{\sqrt{6}}{2}$$

$\ker \sim = \sqrt{3}$  potem  
 leži  $\sqrt{3}$

Base find  $\mathbb{Q}$

$$\{1, \sqrt[3]{2}, \sqrt[3]{4}, i, i\sqrt[3]{2}, i\sqrt[3]{4}\}$$

Rečimo da  $\sqrt{3} \in F \Rightarrow$

$$\sqrt{3} \in \mathbb{Q}(\sqrt[3]{2})$$

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{3}) \subseteq \mathbb{Q}(\sqrt[3]{2})$$

2

3

$\sqrt[3]{3}$



Ali je razstriter  $\mathbb{Z}_3(x^3) \subseteq \mathbb{Z}_3(x)$  normativ

$\mathbb{Z}_3(x)$ -polje racionalnih funkcij nad  $\mathbb{Z}_3$  od spr.  $x$

$$\frac{x^3+x^6}{2x^3-1} \in \mathbb{Z}_3(x^3) \subseteq \mathbb{Z}_3(x)$$

$$f(t) \in \mathbb{Z}_3(x^3)[t]$$

$$f(t) = t^2 + \frac{x^3+1}{x^6} t + \frac{x^3+1}{x^6+x^6}$$

$$\mathbb{Z}_3(x) = \mathbb{Z}_3(x^3)(x)$$

$$f(t) = t^3 - x^3 \in \mathbb{Z}_3(x^3)[t]$$

$$f(x) = 0$$

$$[\mathbb{Z}_3(x) : \mathbb{Z}_3(x^3)] \leq 3$$

$$f(t) = t^3 - x^3 = (t-x)^3$$

nima nicle v  $\mathbb{Z}_3(x^3)$  in je neomejena

$$\Rightarrow = 1 \text{ ali } 3 \quad (\text{ker ne more biti 2}) \\ \text{in } \neq 1 \Rightarrow = 3$$

$\mathbb{Z}_3(x)$  je razgradno polje za

$$P(x) = t^3 - x^3 \Rightarrow \text{to je normativne razstiteri, ker}$$

$$\mathbb{Z}_3(x_3)(x) = \mathbb{Z}_3(x^3, x) = \mathbb{Z}_3(x)$$

(4) Poišči primitivni element razšir.

$$a) \mathbb{Q}(\sqrt{2}, \sqrt{3}) \supseteq \mathbb{Q}$$

$$b) \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}) \supsetneq \mathbb{Q}$$

(5) Poišči parne  $a, b$  alg. razm. in

$$\mathbb{Q}(a, b) \neq \mathbb{Q}(a+b)$$

Navedi  $\alpha \in \mathbb{Q}$  da  $\mathbb{Q}(a, b) = \mathbb{Q}(a, \alpha b)$

Izpeljeva

$$\mathbb{Q}(\alpha, \beta) = \mathbb{Q}(\beta + c\alpha), \text{ kjer } c \in \mathbb{Q},$$

$$c \neq c_{ij} = \frac{\alpha_i - \beta_i}{\alpha_j - \beta_j} \quad j \neq i$$

kjer so  $\beta = \beta_1, \dots, \beta_n$  so nicle m: minimalne  
polinome za  $\beta$  in  $\alpha = \alpha_1, \dots, \alpha_m$  nicle  
minimalne polinome za  $\alpha$

$$\Rightarrow \mathbb{Q}(\sqrt{2}, \sqrt{3})$$

$$P(x) = x^2 - 2 \quad f(x) = x^2 - 3$$

$$\text{nicle: } \sqrt{2}, -\sqrt{2}, \sqrt{3}, -\sqrt{3}$$

$$C = \left\{ 0, \frac{-2\sqrt{3}}{2\sqrt{2}} \right\} = \left\{ 0, \frac{\sqrt{3}}{\sqrt{2}} \right\}$$

Marni primitivni elementi  $\mathbb{Q} - C = \mathbb{Q} - \Sigma \alpha_j$   
(konstant pri katerih kjer v meravljaju)

$$\sqrt{3} + c\sqrt{2}$$

$$b) \underbrace{\mathbb{Q}(\sqrt{2} + \sqrt{3}, \sqrt{5})}_{\text{"1. Reime}}$$

$$P(x) = x^2 - 5 \quad f(x) =$$

$$\beta_1 = \sqrt{5} \quad \beta_2 = -\sqrt{5}$$

$$\mathbb{Q}(\sqrt{2}, \sqrt{3}) \supseteq \mathbb{Q}$$

Galoisova razstrelitev (normalna, končna, separabilna)

$$\sigma \in \text{Aut}(\mathbb{Q}(\sqrt{2}, \sqrt{3})) = \text{Gal}(E/\mathbb{Q})$$

$$\sigma(1) = 1$$

$$\sigma\left(\frac{p}{q}\right) = \frac{p}{q} \quad \text{za } p \in \mathbb{Q} \quad (\text{ker obrange deljenje in sestavljanje})$$

$$\sigma \in \text{Gal}(E/\mathbb{Q})$$

$$\sigma(\sqrt{2}) = \pm \sqrt{2}$$

$$\sigma(\sqrt{3}) = \pm \sqrt{3} \quad \text{skladomorfizem}$$

$$\text{Vemo močnosti rabe } = 4 = |\text{Gal}(E/\mathbb{Q})|$$

$$\Rightarrow \text{Vse te močnosti so automorfizmi}$$

$$\sigma(2 + \sqrt{3}) = \sigma(2) + \sigma(\sqrt{3}) \quad \text{je oblike } I\sqrt{2} \pm \sqrt{3}$$

f naj bo minimalni polinom za  $\alpha = \sqrt{2} + \sqrt{3}$

$$f(x) = 0$$

$$\sigma(f(\alpha)) = 0$$

nicle 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 4 različnih automorfizmov

ki skupaj določijo  $\sqrt{2} + \sqrt{3}$  v eno od teh niclev

lahko bi bilo tudi več nidel, ampak je minimalni polinom

stepnjo 4

$$C = \left\{ 0, \frac{\sqrt{2}}{\sqrt{5}}, \frac{\sqrt{3}}{\sqrt{5}}, \frac{\sqrt{2} + \sqrt{3}}{\sqrt{5}} \right\}$$

$$\mathbb{Q} - C = \mathbb{Q} - \Sigma \alpha_j$$

$$\alpha + \beta \text{ je primitiven}$$

$$\sqrt{2} + \sqrt{3} + \sqrt{5} \text{ je primitiven}$$

(5)

$$\mathbb{Q}(a, b) \neq \mathbb{Q}(a+b)$$

$$\mathbb{Q}(\sqrt{2}, -\sqrt{2}) = \mathbb{Q}(0)$$

$$a = \sqrt{2} - \sqrt{3}$$

$$b = \sqrt{3}$$

ki pa k

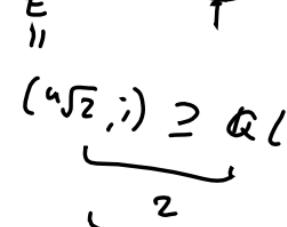
$$\mathbb{Q}(a) \neq \mathbb{Q}(b) ?$$

$$\mathbb{Q}(\sqrt{2} - \sqrt{3}, \sqrt{3}) \neq \mathbb{Q}(\sqrt{2})$$

$$\alpha_2 = \sqrt{2} + \sqrt{3}$$

$$\frac{\alpha_2 - \alpha}{\beta_2 - \beta_1} = \frac{2\sqrt{3}}{-2\sqrt{3}} = -1$$

$$f(x) = x^4 - 2 = (x - \sqrt[4]{2})(x + \sqrt[4]{2})(x + i\sqrt[4]{2})(x - i\sqrt[4]{2})$$



$$\mathbb{Q}(\sqrt[4]{2}, i) \supseteq \mathbb{Q}(\sqrt[4]{2}) \supseteq \mathbb{Q}$$

2      4  
         8

Ali je ta razširitev galoisova? da

- 1)  $\text{Gal}(E/\mathbb{Q}) = ? = \text{Aut}(E)$  ← racionelne številke
- 2)  $\text{Gal}(\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}) = ? = \text{Aut}(\mathbb{Q}(\sqrt[4]{2}))$  negatvne

$$\text{Gal}(F/k) = \{\sigma \in \text{Aut}(F); \sigma(k) = k \ \forall k \in K\}$$

Ko je na dezn.  $\mathbb{Q}$  je  $\text{Gal} = \text{Aut}$

$$\begin{array}{ll} 2) \text{i)} \sqrt[4]{2} \mapsto \sqrt[4]{2} & x^4 - 2 = (x - \sqrt[4]{2})(x + \sqrt[4]{2})(x^2 + 2) \\ \text{ii)} \sqrt[4]{2} \mapsto -\sqrt[4]{2} & \text{Slike je določena z enim} \Rightarrow 2 \text{ možnosti} \\ \text{Baza } \{1, \sqrt[4]{2}, \sqrt[4]{4}, \sqrt[4]{8}\} \end{array}$$

Ustvarjuje 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 množico:  $\sigma(a+b) = \sigma(a)\sigma(b)$

$$a, b \in \{1, \sqrt[4]{2}, \sqrt[4]{4}, \sqrt[4]{8}\}$$

$$\alpha = \sqrt[4]{2}$$

$$\sigma(\alpha^k \alpha^m) = \sigma(\alpha^{k+m}) = (-1)^{k+m} \alpha^{k+m}$$

$$|\text{Gal}(\mathbb{Q}(\sqrt[4]{2}), \mathbb{Q})| = 2 \neq 4$$

$\Rightarrow$  n: galoisova C s t min polinome

$$1) \mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q} \text{ je normalna} \Rightarrow \text{polinome}$$

ker je razpred no polje

z n nizem: je vedno podgrupa  $S_4$

st razširitive =  $|\text{Gal}(\text{razšr. de})|$

$$f(x) = x^4 - 2$$

$r_1, r_2, r_3, r_4$  nöle st nich

$$1) G = \text{Gal}(\dots) \leq S_4 \leftarrow \text{Galoasova grupe}$$

z n nizem: je vedno

$$2) G \text{ deluje tranzitivno} \rightarrow \text{podgrupe } S_4$$

na  $\{r_1, \dots, r_4\}$  Time ena orbita je vsi

$$V_i, j. \exists \sigma \in G. \sigma(r_i) = \sigma(r_j)$$

ker ima orbita velja, da je moč vsaj 4 (v splošnem vsaj 2) (ker tekoča boli nista boli pravilna tekoča boli nista)

Vemo da je grupe  $D_8$

Vemo  $D_8 \leq S_4$  ker je grupe slike

je vsake niza redgrupe nöai &

0. izmetne v  $S_4$

Deklinacija slike nöai, grevati!

merimo ne leri:

$$r_1 \mapsto r_2 \quad \sqrt[4]{2} \mapsto -\sqrt[4]{2} \quad \sigma(a) = i a$$

$$r_2 \mapsto r_3 \quad i a \mapsto -a \quad \sigma(i a) = -a$$

$$\sigma(i) \sigma(a)$$

$$-a = \sigma(i) \cdot i a \quad / \cdot a^{-1}$$

$$-1 = \sigma(i) i \quad / \cdot i^{-1}$$

$$i = \sigma(i) \quad / \cdot i^{-1}$$

$$L_1 = \mathbb{Q}(\sqrt{-1})$$

$$L_2 = \mathbb{Q}(\sqrt{2})$$

$$L_3 = \mathbb{Q}(\sqrt[3]{2})$$

$$[E:L] = [E:L_2] = [E:L_3] =$$

$$\text{points} = \text{Gal}(E/\mathbb{Q}_p), \quad \text{Gal}(EL_2) \subset \text{Gal}(EL_3)$$

$$\mathbb{Q} \subseteq L_1 \subseteq \mathbb{Q}(\sqrt{2}, ;)$$

$\xrightarrow{\text{Gal}}$

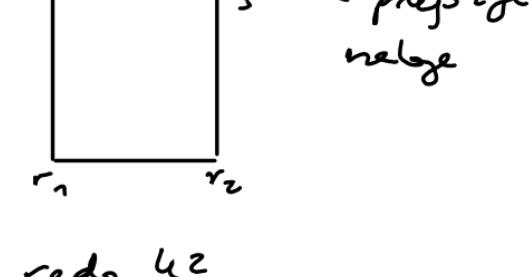
?

$\xrightarrow{\text{Gal}}$

$$G \models (L / L_1) = [E : L_1]$$

A diagram consisting of two nested brackets. The inner bracket, located at the bottom, has a horizontal line with arrows at both ends and a vertical line on its left side, with the number "8" written below it. The outer bracket, located at the top, has a horizontal line with arrows at both ends and a vertical line on its left side, with the number "2" written above it.

$$r_a \leq D_8$$



$$r \geq d, r, r^2, r^3$$

$$2) \{id, r^2, z, zr^2\} \stackrel{\cong}{=} \mathbb{K}_2$$

$$3) \quad (\overline{1, (r_2, r_4)}, (r_1, r_3), (r_4, r_3)(r_4,$$

$$G_1 = \{e \in E : \alpha(e) = \text{loss}_1\}$$

zakro od leh ayus so neg!

$$G_n: \sqrt[n]{z} \rightarrow \sqrt[n]{z} -$$

$$\text{Ed } (\mathbb{E}/L_1) : \quad \sigma(\cdot) = ;$$

{1, 3}  $\swarrow$

$$\rightarrow r_2 \rightarrow r_3 \rightarrow r_n,$$

$$r_3 = r$$

$r_{T=-1}$

$$\sigma(i) = \sigma_{\frac{r_2}{r_1}}.$$

$$\sigma(z) = \frac{r_3}{z} = -4\sqrt{\varepsilon}$$

- ; "  $\sqrt{2}$  - : -

1

$$r_2 r_4 - \sqrt{2}$$

178

$$(\mathbf{r}_1 \cdot \mathbf{u})(\mathbf{r}_2 \cdot \mathbf{r}_3) (\nabla \mathcal{E}) = -\nabla \mathcal{E}$$

$$L_2 \approx L_3$$

- 2

$$G \triangleleft (E/L_1)$$
$$E = L_1$$

$$\{e \in E : \sigma(e) = e, \forall \sigma \in G \triangleleft (E/L_1)\} \stackrel{C_a}{\sim} Q(\cdot)$$

Vemo : je notr:  
in st nad  $\oplus$  rabi blts 2  $\Rightarrow Q \subset$

$$[E : L_1] = 4 \Rightarrow L_1 : Q = 2$$

$$f(x) = x^4 + bx^2 + c \in \mathbb{Q}[x]$$

nicle:  $y = x^2$ :  $y^2 + by + c$

nicle:  $\pm\alpha \pm\beta$

$$\sigma(\pm\alpha) \in \{\pm\alpha\}; \{\pm\beta\}$$

$$\rho_{\text{addition}} = \sigma(\pm\beta)$$

$$|G| < 8$$

$$G \leq D_8$$

$$\begin{aligned} G &\text{ so vseen die rechnung } \Rightarrow \\ E &= \mathbb{Q} \Rightarrow G = \text{id}_3 \end{aligned}$$

$$\gamma = \alpha \beta \quad \leftarrow \text{rich}$$

$$\delta^2 \in \mathbb{Q} \quad \delta^2 = \alpha^2 \beta^2 = c$$

$$f(x) = (x^2 - \alpha^2)(x^2 - \beta^2) =$$

$\gamma$  ist ein Polynom  $x^2 - c$

$$\sigma(\gamma) = \pm \gamma$$

Orbit  $\gamma$   
Kern  $\text{st}(\gamma)$

$$|G \cdot \gamma| = [G : G_\gamma]$$

id

$$\alpha \mapsto \beta \Rightarrow \beta \mapsto \alpha$$

$$\alpha \mapsto -\beta \Rightarrow \beta \mapsto -\alpha$$

produkt technisch

ist eine Gruppe  $K_4$

$$G_\gamma = K_4 \cap G$$

$$1) \text{ Es ist } \gamma \subset \mathbb{Q} \Rightarrow \sigma(\gamma) = \gamma$$

$$|G \cdot \gamma| = 1 \Rightarrow |G| = |G \cap K_4| \Rightarrow G \leq K_4$$

2)

$$\sigma^2: G_\alpha^2 \Rightarrow \sigma(\alpha) = \pm \alpha \quad \sigma(\beta) = \pm \beta$$

$$\begin{array}{c} -\beta \\ \square \\ \alpha \end{array}$$

zu erlangen  $\Leftrightarrow$  2 Werte

$$\langle z, r^2 \rangle = K_4$$

$$|G_{\alpha^2}| = [G : G_{\alpha^2}]$$

$$\begin{matrix} \parallel \\ 1 \Leftrightarrow \alpha^2 \in \mathbb{Q} \end{matrix}$$

passende Untergруппen  $G \leq K_4$

3) Welcher  $\gamma$   $G \leq C_4$ ?

$$\delta = \alpha^3 \beta - \beta^3 \alpha \quad C_4 \text{ stabilisiert } G \quad \delta \leq C_4$$

$$|G_\delta| = 1 \Leftrightarrow \delta \in \mathbb{Q} \Leftrightarrow G \leq C_4$$

$$\delta^2 = \alpha^2 \beta^2 (\alpha^2 - \beta^2)^2 = c(\alpha^2 - \beta^2)^2$$

$$D = b^2 - 4c = (\alpha^2 - \beta^2)^2$$

$$\delta^2 = c(b^2 - 4c) \in \mathbb{Q}$$

reduziert  
nach re  
quadrat

$$x^4 + 4x^2 + 2 \quad \text{jiherazegen}$$

fast herazegen  $\Rightarrow$  Gal beliebig transzitiv

$$D = 16 - 8 = 8$$

$$c \cdot D = 16 \quad \text{j} \ddot{\text{a}} \text{ populärwadrat}$$

$$\Rightarrow Gal \subseteq C_G \Rightarrow Gal = C_G$$

Naj bo  $f(x) \in \mathbb{Q}[x]$  nerezec pol st 3

$\Leftrightarrow$  ima eno realno n: c76

potem Gal f  $\cong S_3$

$a \in \mathbb{R}$  n:de

3 n:de  $\Rightarrow$

$G \leq S_3$

$$\mathbb{Q} \subseteq \mathbb{Q}(a) \subseteq E$$



$$|G|=6$$

$$\Rightarrow G \cong S_3$$

$$f(x) = x^3 + ax^2 + bx + c \in \mathbb{Q}[x] \text{ nerezcen}$$

$$x_{1,2} = \frac{-b \pm \sqrt{D}}{2} \text{ za kvaradne}$$

$$(x_1 - x_2)^2 = D$$

$$D = ((x_1 - x_2)(x_1 - x_3)(x_2 - x_3))^2 \dots \text{ diskrim: nante}$$

simetričn: polinom od  $x_1, x_2, x_3$  n:de f(x)

za  $x_1, x_2, x_3$  n:de f(x)

$$\rightarrow g(x_1, x_2, x_3) = g(x_{\sigma(1)}, x_{\sigma(2)}, x_{\sigma(3)})$$

Osnov: rrek o sim. polinomih

vezk simetričn: polinom se da izisti

$$x_1 + x_2 + x_3$$

preko osnovnih

$$x_1 x_2 + x_1 x_3 + x_2 x_3$$

sim. polinomau

$$x_1 x_2 x_3$$

$$D = 18abc + a^2b^2 - 4b^3 - 4a^3c - 27c^2$$

$$\text{te } \sqrt{D} \in \mathbb{Q} \Rightarrow \sqrt{D} \rightarrow \sqrt{D}$$

$$f(x) = x^3 - 2$$

$$D = -108$$

n: kubik  
rac. sterile



$$G \cong S_3$$

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

$$D = 202$$

3 reelle n; 6 le apah  $G \cong S_3$

$$g(x) = x^3 - 3x + 1 \text{ nerangen}$$

$$D = 81$$

kubik reelln

sterile

$$\Rightarrow G \cong C_3$$

$f(x) \in \mathbb{Q}[x]$   
nieszcz pol. st. 5

$G$  posiada 5-cikl

$$|G \cdot x_1| \leq 5 = [G : G_{x_1}] = 5$$

$$5 \mid |G|$$

$\exists \sigma \text{ rede } 5 \cup G \subseteq S_5$

$\sigma$  je 5-cikl

$$\sigma = (x_1, x_2, x_3, x_4, x_5)$$

$$\sigma^2 = (x_1, x_3, x_5, x_2, x_4)$$

$S_5$  je generowany przez  $(12345)$