M. Brašar, Uvod v algebro, osnutek novega učbenika

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

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

$$S \times S \longrightarrow S$$

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

$A \subseteq \mathbb{Z}$ je zaprta za operacijo $\cdot$ če

$a, b \in A \Rightarrow a \cdot b \in A$

$|S| = n$

Koliko je binarnih operacij

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

- je asociativna če

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

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

V splošnem: indukcija

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

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

$n \ge 4$

Poglejmo si zadjo uporabo operacije

$$\underbrace{(a_1 \cdot \ldots \cdot a_l)}_{\text{postavljeni oklepaji notri}} \cdot \underbrace{(a_{l+1} \cdot \ldots \cdot a_n)}_{\text{postavljeni oklepaji notri}}$$

$$1 \le l \le n-1$$

Recimo da je $(a_1 \cdot \ldots \cdot a_l)$ oblikovano v

$a_1(a_2(\ldots \cdot a_l))$ in tudi drugi oblike.

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

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

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

Monoid je polgrupa z enoto

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

(enota mora biti obojestranska)

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

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

$ls = 1 = sr$

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

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

Naj bo S končen monoid

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

Dokaži da je S obrnljiv

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

$S^0, S, S^2, S^3, \ldots$ v tem zaporedju so ponavljanja

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

$$t^2 s^2 = t \cdot t \cdot s \cdot s = ts = 1$$

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

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

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

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

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

$$s^m = 1$$

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

s^{m-1} je desni inverz

■

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

Navedi vsaj dva različna leva inverza

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

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

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

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

$f \circ g(x) = g(2x) = x$ ✓

$h \circ f(x) = x$ ni desnega kar je leva relacija leva

$f : n \longmapsto 2n+2$

Naj bo $(S, \cdot)$ monoid. Ali sta elementa $x, y \in S$ obrljiva, če je obrljiv element

a) $x \cdot yx$

b) $x \cdot y$

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

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

desni in levi inverz

$y \cdot xf = fxy$

$x \cdot y \cdot x \cdot f = xfxy = 1 = \underbrace{fx \cdot y \cdot x}_{y \cdot xf}$

$(xfx)y = y(xfx) = 1$

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

Protipimer

$g : n \longmapsto 2n \qquad f \circ g = id$

$f : 2n \longmapsto n$

$2n+1 \longmapsto 0$

Grupa $(G, \cdot)$ je
1. monoid (asociativnost, enota)
2. $\forall g \in G. \exists g^{-1} \in G. \; g \cdot g^{-1} = g^{-1} \cdot g = 1$

G grupa, $a, b \in G$

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

$a^{-1} / \; ax = b$ $\qquad$ $xa = b \; / a^{-1}$ $\qquad$ dve različni enačbi

$x = a^{-1}b$ $\qquad$ $x = ba^{-1}$

Obratno: Naj bo $(S, \cdot)$ polgrupa z deljenjem (torej $\forall a, b \in S.$ sta enačbi $ax = b$ in $xa = b$ sta rešljivi)

Pokaži da je S grupa

$ax = b$ vzamemo $b = 1$

$ax = 1$ $\qquad$ $xa = 1$

$x = a^{-1}$ $\qquad$ a ima levi in desni: torej je obrnljiv. Zaključena

Torej ima inverz

Ampak ni nujno da ima S enoto

Hočemo pokazati da ima S enoto

$b = a$

$ax = a$ $\qquad$ $xa = a$

$x = 1_a$ $\qquad$ desna enota

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

$b \cdot a = ba 1_a$

$1_a = xb = by$

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

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

za $b = a$ je enačba rešljiva

$a \circ x = a$ x ... desni inverz a
$y \circ a = a$ y ... levi inverz a

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

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

1_a je desna enota

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

y je 1_a

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

Dokaži: dokaži vsaka grupa s štirimi elementi abelova

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

Recimo da $ab \neq ba$ ($ab \in G$, $ba \in G$)

1) $ab = 1$ b je desni inverz za a torej je inverz tudi levi torej $ba = 1$

2) $ab = a$ $\quad b = 1$ ✗

3) $ab = b \,/\, b^{-1}$ $\quad a = 1$ ✗

4) $ab = c$

enako velja za ba

torej $ba = c = ab$ ✗

Trditev: V $\forall$grupi: $xy=1$ sled $yx=1$, iz

le v abelovi grupi: iz

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

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

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

$\Rightarrow zyx=1$

G ni abelova, ampak

$xyz=1 \not\Rightarrow zyx=1$

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

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

Dokaži da lger velja v grupi

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

b) Ali enačba $x^2 = a$ je rešljiva v vsaki grupi

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

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

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

$x = a$

a)

$a, b \in G$

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

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

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

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

$a \circ b = b \circ a$ ✓

b) Ali je $x^2 = a$ rešljiva vedno

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

za $a = 3$

$2x = 3$ ni rešitve v $\mathbb{Z}$

c) $x^2 = a$ največ dve rešitvi?

D_{2n} je grupa rotacij

vsako zrcaljenje za $n \geq 2$ je protiprimer

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

Simetrična grupa S_n

$\pi \in S_n$ je soda oz. liha če je produkt sode mnogo transpozicij

$\pi \in S_n$ zapisano kot produkt disjunktnih ciklov

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

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

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

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

$sgn(\pi) = (-1)^k$ k ... št transpozicij

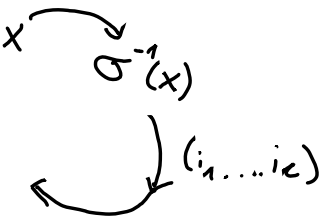
če je σ n-cikel $\Rightarrow sin(\sigma) = (-1)^{n-1}$

Naj bo $\sigma \in S_n$

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

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

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



$x = \sigma(i_1)$ $\quad \sigma(i_1 \dots i_k)\sigma^{-1}(\sigma(i_1)) =$

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

$= \sigma(i_2)$

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

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

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

npr:

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

Dokaži da sta σ in σ' konjugirani:

$\Leftrightarrow$ imata enako cikelj. tip

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

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

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

Vidimo da so cikli enako dolgi

$\Leftarrow$ Recimo da

$\sigma = (i_1 \dots i_{k_1})(j_1 \dots j_{k_2})(\dots)$

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

Definirajmo π da velja

$\pi: i_j^l \longmapsto I_j$ za $\forall j$

$\sigma' = (\pi(i_1^1) \dots \pi(i_{k_1}^1))(\dots)$

Vemo tudi da $\sigma' = \pi(i_1 \dots i_{k_1})(\dots)\dots\pi^{-1}$

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

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

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

za $n \geq 2$

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

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

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

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

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

$\pi_2 = \sigma$ kjer σ ima negibne točke v 1, 2

Koliko jih je ?

$2 \cdot (n-2)!$

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

centralizator elementa $(1,2)$

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

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

direktna vsota permutacijskih grup

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

$(k, k+1)$ kjer

$1 \leq k \leq n-1$

$\pi = (i_1\ i_2)(i_3\ i_4)\ldots\ldots$

Transpozicijo (i_1, i_2) zapišemo preko transpozicij:

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

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

$(i\ j)$

$j - i > 1$

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

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

3. poglavje

H, K konen: podgrupi grupe G

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

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

$|hK| = |K|$

Recimo da imamo 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 grupa in $H \leq G$

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

$\Leftrightarrow$ $\underline{2|H| < |G|}$

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

$\#$. odsekov G po H je vsaj 3

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

Prvi odsek je zagotovo H

$eH \Leftrightarrow aH \Leftrightarrow a \in H$ $\lightning$ aH je odsek

$aH = bH = abH$

$aH = abH \Leftrightarrow eH = bH$ $\lightning$

Torej mamo tri različne

$\Leftarrow$ imamo vsaj tri odseke

$aH \neq bH \neq H$

$b^{-1} \notin H$

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

$a^{-1}H = aH$

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

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

ciklične grupe

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

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

Lagrangeev izrek

Red podgrupe deli red grupe

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

$\Leftrightarrow k \mid n$

take grupe ena sama

$n = k \cdot l$

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

zakaj ni druge podgrupe reda k

$H < Z_n$ reda k

$H = \{\underset{0}{h_1}, \ldots h_k\}$

$red(h_i) \mid k$

$t \in Z_n \quad red\, t \mid k \Leftrightarrow tk = 0 \text{ v } Z_n$

torej $n \mid tk$

$k \cdot l \mid tk$

$l \mid t$

$t \in \langle l \rangle$

Torej $h_i \in \langle l \rangle$ Torej $H = \langle l \rangle$

Pokaži da je podgrupa ciklične grupe ciklična

$G = \langle a \rangle$

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

2) $G = \langle a \rangle$; $a^n = 1$

$\{1, a, a^2, \dots a^{n-1}\}$

$G = \mathbb{R}_n$

Podgrupe v $\mathbb{Z}$:

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

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

$H \neq \{0\}$

$n > 0$ in n najmanjše pozitiven element H

Pokažimo $H = n\mathbb{Z}$

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

$k \in H$. $n \nmid k$

$d = D(n,k)$ največji skupni delitelj

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

$d \in H$ $\quad \lightning$

Določi red od $k \in \mathbb{Z}_n$

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

$red(0) = 1$ $\quad$ $red(1) = n$

$red(k) = r$ je najmanjše tako št. da $n \mid rk$

$g = D(n,k)$

$n = g\alpha$

$k = g\beta$

$g\alpha \mid r g\beta$

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

$\alpha \mid r\beta$

$r = \alpha$

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

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

Ko sta n, k tuja

$\mathbb{Z}_2 \oplus \mathbb{Z}_3$ je ciklična

$\mathbb{Z}_2 \oplus \mathbb{Z}_2$ ni ciklična, ker nima elementa reda 4

$(1,1)$ generira celo grupo

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

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

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

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

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

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

DN: Każdy $\mathbb{Z}_m \oplus \mathbb{Z}_n$ abelowy

Naj bo G neskončna grupa.
Pokaži, da ima G neskončno mnogo podgrup

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

2. G nima elementa neskončnega reda

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

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

$\langle a \rangle$ je končna

in tako lahko nadaljujemo

2. način

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

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

Potem bi bila G končna unija končnih množic $*$

Pokaži:

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

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

3) $red(ab) = red(ba)$

4) Al: imata v G grupi elementa $a^{-1}b^{-1}$ in $a^{-1}b$ enak red kot ab

1) Recimo da ~~je~~ red kvečjemu

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

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

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

zaradi simetrije je to enakost

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

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

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

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

$a^r = b^{-1}b = 1$ ✓

3) $red(ab) = red(ba)$

$(ab)^r = 1$ ~~bod~~ $r \cdot 1$ $ba^{r-1} = a^{-1}b^{-1}$

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

$(ba)^r = baba \ldots ba = (ba)^{r-1}ba =$

$= a^{-1}b^{-1}ba = 1$ ✓

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

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

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

$= red(a^{-1}b^{-1})$ ✓

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

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

$a = 2$ $b = 1$

$a + b = 0$ $red(a+b) = 0$

$red(2-1) = red(1) = 3$

n^2 vseh možnosti. $\left(\frac{n}{2}\right)^2$ lahko zavrže
4, 3 in gre same vase. Vecja polovica.

Pokaži kaj je grupa

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

$A = [-2, -1]$

Kje generirana z $A \leq G$

če vsak $g \in G$ oblike

$g = a_1^{\varepsilon_1} \cdot \ldots \cdot a_n^{\varepsilon_n}$ $\quad g = a_1^{\pm 1} a_2^{\pm 1} a_3^{\pm 1} \ldots a_n^{\pm 1}$

$a_1 \in A$, $\varepsilon_i = \pm 1$

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

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

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

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

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

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

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

1) Določi red podgrupe ← moč grupe generirane z A

$Gl_n(\mathbb{C})$ generirane z matrikama

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

2) Opiši podgrupo grupe $Gl_2(\mathbb{C})$

generirane z $A=\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$

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

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

$red(\{A\})=4$ $\quad A^{-1}=A^3$

$B^3=1$ $\quad B^{-1}=B^2$

$A^kB^n=A^sB^n$

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

Katere iz naslednjih množic so kolobarji za običajno seštevanje in množenje

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

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

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

$\{p+q\sqrt{2} ; p,q \in \mathbb{Q}\}$

komutativno ✓ vse

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

0 ✓

$$= \frac{\dots}{2(2nc+n+c)+1}$$ ✓

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

$$\frac{1}{2 \cdot 0 + 1} = 1$$ ✓

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

$c+m$

$m-1$

$2a+b$

$m+n\sqrt{2}+k+c\sqrt{2} =$ ✓

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

$= mk+2cn+\sqrt{2}(nk+mk)$ ✓

$1+0\sqrt{n} = 1$ ✓

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

$A, B \subseteq X$

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

$A \cdot B = A \cap B$

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

Velja: $A^2 = A$ za $\forall A$ ← idempotent

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

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

($a + a = 0$ za $\forall a$)

a) notranja operacija očitno

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

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

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

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

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

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

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

$(A \cap B) + (A \cap C) = AB + AC$ ■

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

komutativnost

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

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

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

$AB + BA = 0$

$B = A$

$AA + AA = 0$

$A + A = 0$

$AB = -BA$

$-BA = BA$

$AB = BA$ ■

idempotent: $x^2 = x$

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

Najbo $A \in M_n(\mathbb{R})$ matrika ~~ničelna~~ ranga nagveč ena. Pokaži da $A^2 = \lambda A$ za nek λ. Poišči kak idempotenten, ki ni diagonalna in kak ~~ni ničelen~~ nilpotenten, ki ni trikotna

$$A = \begin{bmatrix} c_1a_1 & c_1a_2 & \dots & c_1a_n \\ c_2a_1 & c_2a_2 & \dots & c_2a_n \\ \vdots & & & \\ c_na_1 & c_na_2 & \dots & c_na_n \end{bmatrix} =$$

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

$$A^2 = \begin{bmatrix} c_1 \\ \vdots \\ c_n \end{bmatrix} [a_1 \dots a_n] \begin{bmatrix} c_1 \\ \vdots \\ c_n \end{bmatrix} [a_1 \dots a_n]$$

$$\lambda \in \mathbb{R}$$

$$= \lambda A$$

$$a_1c_1 + a_2c_2 = 1$$
$$1 \cdot 3 + (-2) \cdot 1 = 1$$

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

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

$$c_1a_1 + a_2c_2 = 0$$
$$1 \cdot 2 + 2(-1) = 0$$

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

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

1) x nilpotent kolobarja K
pokaži, da je element $1-x$ obrnljiv

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

1) $x^n = 0$

$$\frac{1}{1-x} = \sum_{n=0}^{\infty} x^n = \sum_{i=1}^{n} x^{n-i} =$$

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

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

$$1 - x^n = 1$$

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

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

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

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

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

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

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

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

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

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

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

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

Algebra nad poljem

$(A, \cdot, +)$ - 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 končno razsežna algebra
Dokaži:

a) Vsak neničelen element je bodisi delitelj ničle, bodisi obrnljiv
b) če ima $a \in A$ levi ali desni inverz je obrnljiv
c) če je 1 obseg je vsaka algebra podobseg

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

a) Naj bo n tak da so $1, \ldots a^{n-1}$ lin neodvisni in a^n je l. odvisen

$\lambda_0 + \lambda_1 a_1 + \ldots + \lambda_n a_n = 0$
gotovo $\lambda_n \neq 0$

$\lambda_0 \neq 0 \Rightarrow$

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

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

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

a je obrnljiv

$\lambda_0 = 0 \Rightarrow$

$a(\lambda_1 + \ldots \lambda_n a^{n-1}) = 0$
$\neq 0$ (ker $\lambda_n \neq 0$)

Torej je a delitelj ničle

b) a ima levi inverz

$ba = 1$

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

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

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

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

$\alpha_n \neq 0$ po predpostavki:

$\Rightarrow$ b je obrnljiv poprejšnji tedaj

njegov inverz

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

$ba = 1 \quad xb = 1$

$x = a$

$ab = 1$

c) A je okruh

B podalgebra

Nech $b \in B$; $b \neq 0$: Dokaž: $b^{-1} \in B$

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

X množica

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

$P_x = \{x\}^c$

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

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

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

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

$P_x + P_y = X$ je pokrivanje

$P \subseteq \mathcal{T}_{kk}$ očitno

(4,5)

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

homeomorfen netřivia

Produkt topologických prostorů

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

$1<a<4$

$ae^{pi} \longmapsto (f(a), g(\rho))$

4.8.

$(-\infty, 0) + [0, \infty) \to \mathbb{R}$

$in_1(x) \to x$
$in_2(x) \to x$

surj ✓
inj ✓

vezmast:

$$f^*(a,b) = \begin{cases} in_1^*(a,0) \cup in_2^*([0,b)) & a<0<b \quad ✓ \\ in_1^*(a,b) & a,b<0 \quad ✓ \\ in_2^*(a,b) & a,b \geq 0 \quad ✓ \end{cases}$$

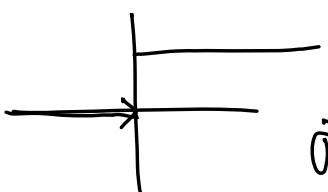
Homeomorfizem?

N: Ker je povezan drugi ni

inverz ni: vezem

$in_2[0,1) \longmapsto [0,1)$

b)



Heavisidova funkcija je vezna

49

$\forall A$ podprostor $(X, \mathcal{T}_{KK})$ | ima $\mathcal{T}_{KK}$

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

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

za A kompakten ... očitno

za A nekompakten:

(4.10.)

$\mathbb{N}_{\text{diskr}} \xrightarrow{i} \mathbb{R}_{\text{evk}}$

Vsaka preslikava iz diskretne topologije je zvezna

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

ali slika odprte množica v odprte?

$i_*(\{1\}) = \{1\}$ terej ; ni odprta

Vsaka slika bo zgit, terej vsaka zgit ⊆ množica slika v zgit

NTSE: naslednje trditve so ekvivalentne

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

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

$i_*(\{g_3\}) = \{g_3\}$ n: oggetto $\vee$ $\mathbb{Q}$-ok

$\Rightarrow$ ipotesi violata

π_0 ✓

ovvero disk $\longrightarrow$ nodisk ✓

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

Kvaternionska grupa

$$ij = k \quad ji = -k$$
$$jk = i \quad kj = -i$$
$$ki = j \quad ik = -j$$

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

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

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

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

1) Za katere $h \in \mathbb{H}$ je rešljiva enačba

$ix - xi = h$

Poišči vse rešitve enačbe $ix - xi = h$

2) Poišči vse rešitve enačbe $x^2 - 1$ v $\mathbb{H}$

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

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

$h + \bar{h} = 0 \Leftrightarrow \exists x \in \mathbb{H} \quad hx \neq xh \quad h^2 x = x h^2$

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

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

V $\mathbb{C}$: $\alpha = -(h + \bar{h})$, $\beta = h \cdot \bar{h}$ } Vietov izrek

Recimo da

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

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

$h \cdot \vec{h} = \vec{h} h$

$\| h \|^2 = \| \bar{h} \|^2$

$\| h \|^2$

Nič od zgo α in β

■

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

$h + \bar{h} = 0 \iff \forall x \; \exists x . \; hx \neq xh$
$h^2 x = x h^2$

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

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

$h^2 x = -\|h\|^2 x = x(-\|h\|^2) = x h^2$ ✓

Izberemo x, h: ne komutirata

$h = \alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k$ brez izgube splošnosti $\alpha_2 \neq 0$

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

$\alpha_2 k = -\alpha_2 k$

$\alpha_2 = 0$ ↯

$\Leftarrow$ $hx \neq xh$
$h^2 x = x h^2 \qquad h^2 = -\alpha h + \beta$
Recimo da $\alpha = -(h+\bar{h}) \neq 0$
$(-\alpha h + \beta) x = x(-\alpha h + \beta)$

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

$\alpha h x = \alpha x h$

$hx = xh$ ↯

Torej $\alpha = 0$

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

$h + \bar{h} = 0$

∎

6) Podkolobar generiran z 3i: $\mathbb{Z} \subseteq \mathbb{C}$

7) $5-6i$ in $2+5i$:

c): zapiši za seštevanje

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

$1 \to \mathbb{Z} \subseteq k$

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

$(n+k3i)^c$

$(3i)^2 = -9 \in \mathbb{Z}$ ✓

Torej je podkolobar $A = \{n+k3i, n,k \in \mathbb{Z}\}$

④

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

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

$\mathbb{Z} \subseteq k$

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

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

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

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

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

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

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

$3i \in K$

$5-6i \in A$

$A \subseteq K$

$2+5i \in A$

in A je kolobar, torej $A \geq K$

Torej $A = K$

8) Določi podalgebro algebre

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

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

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

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

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

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

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

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

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

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

G je grupa

zaprtost za seštevanje in inverziranje

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

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

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

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

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

Brez α_1 kjer je neničelnih α_i končno mnogo

Ali je kolobar?

- $\cdot$-podgrupa je
- enota vsebuje
- enota
- zaprtost za množenje ✓

(ker pri lihih potencah je soda kot liha potenca, in pri lihi je 2 terej je pri lihih 2

podprostor (seštevanje + množenje s skalarjem

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

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

podalgebra

- podkolobar + množenje s skalarjem αk $\alpha \in \mathbb{R}$

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

$= \mathbb{R}[x] - \lim\{x\}$

je res najmanjša zaradi zaprtosti

5. poglavje

$\varphi : G \longrightarrow H$ je homomorfizem grup, če φ ohranja operacijo

$\varphi(gh) = \varphi(g)\varphi(h)$

izomorfizem = homomorfizem + bijekcija

avtomorfizem = izomorfizem vase

Naj bo $\rho : G \to H$ homomorfizem in $a \in G$ ima končen red.
Pokaži, da $\text{red}(\rho(a)) \mid \text{red}(a)$
Če je ρ vložitev (monomorfizem) sta reda enaka.

$a^n = 1$

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

$\| $

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

Recimo da je vložitev

Recimo da je injektivna

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

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

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

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

torej je to edini element za katerega

~~$\rho(1) = 1$~~

$\rho(a^t)$

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

$a^k = 1$

torej $t = n \quad k = n$

Naj bo G grupa in $a \in G$. Pokaži:

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

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

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

$\varphi(1) = a$

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

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

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

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

$\mathbb{Z}_n \to G$

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

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

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

$\Leftarrow$

$a^n = 1$

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

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

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

↑ $\mathbb{R} - \{0\}$

Recimo da dosta izomorfizam f

$red(a) = n \quad a^n = 1$

Vsi elementi racan ~~ake~~ $\{1, -1\}$ imaju nesklenuto red v $\mathbb{R}^*$

$red(-1) = 2$

- red elementa se dokazuje, ampak v $\mathbb{R}^+$ ni elementa reda 2

za $\mathbb{C}^*$

$|a| \neq 1 \Rightarrow$ ~~beda~~ ima neskončen red

Poglimo elemen $red \in (\mathbb{N} - \{1, 2\})$

$i^4 = 1 \quad red(i) = 4$

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

↑ komutativna ↑ nekomutativna

4) Pojasni zakaj endomorfizem algebre $M_2(\mathbb{R})$ ne more preslikati matrike E_{11} v E_{12} pri tem pa ker endomorfizem ρ, da je $\rho(E_{11}) = E_{12}$.

5) Naj bo A ~~matrika~~

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

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

Preveri: da sta A in A' k-naseni in $A \cong A'$. Pokaži, da A ni izomorfna algebri $M_2(\mathbb{R})$

G

E_{11} je idempotent

Recimo da je

$\rho(E_{11}) = \rho(E_{11} \cdot E_{11}) =$ [illegible]

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

$\rho(E_{11}) = E_{22}$

$\rho(E_{22}) = E_{11}$ zorad idempotentnosti

$\rho(E_{12}) =$

$$\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$ v vsakem primeru

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

$\pi = (12)$ $\qquad E_{11} \cdot E_{12} = E_{12}$

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

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

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

$H < G$

H je edinka

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

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

$H_2 = \langle z \rangle$ (ker ima indeks 2)

$([D_8 : H_1] = 2$

$(8 : 4 = 2)$

$[D_8 : H_2] = 4$

$rH_2 = H_2 r$

$r\{1, z\} = \{r, rz\}$ $\quad \{1, z\} \cdot r = \{r, zr\} = \{r, r^3 z\}$

$\neq$

Torej H_2 ni edinka

Podobno v D_{2n}

$H \lhd G$ $\quad G/H$ ... kvocientna grupa

↘ množica vseh odsekov

$g_1H \cdot g_2H = (g_1g_2)H$

$(g_1H)^{-1} = g_1^{-1}H$

enota: $H = 1 \cdot H$

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

Dokaži da je G abelova grupa

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

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

$G/Z(G) = gZ(G)$

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

V element lahko zapišemo kot a^kz, kjer $z \in Z(G)$

$a^kz \cdot a^nc = a^k(za^n)c =$

$= a^k(a^nz)c = a^{k+n}zc =$

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

$= a^{n+k} \cdot cz = a^n(a^kc)z = (a^nc)(a^kz)$

② Naj bo $|G| = 55$. Pokaži

a) ∀ prava podgrupa G je ciklična

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

a) red podgrupe deli red G

red podgrupe je 11 ali 5 ali 1 → ciklične $\{1\}$

$\mathbb{Z}_p$ je edina grupa p do izomorfizma natančno.

Ta je ciklična

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

Po prvi: nalogi $G/Z(G)$ kvocient ni ciklična

Recimo da center ni trivialen

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

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

in taka grupa je ciklična, torej ✳

③ Pojasni, da lahko 33 zamenjamo s produktom dveh praštevil

Ali lahko tudi z 8 ?

če imamo $p \cdot q$ $(p \neq q)$ potem podobno kot 2b)

če imamo red p^2, potem podobno kot pri 2b)

~~Z(D8)~~ $Z(D_8) = \{1, r^2\}$

in D_8 ni abelova

$Z(Q) = \{\pm 1\}$ in Q ni abelova

↑ kvaternionske

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

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

grupa reda 4, ki ni ciklična

N: ciklična, ker nima elementa reda 4

1. izrek o izomorfizmu

$\varphi: G \twoheadrightarrow H$ epimorfizem

Potem velja: $\ker \varphi \trianglelefteq G$

$G/\ker\varphi \cong H$

Naj bo G grupa vseh nekonstantnih linearnih funkcij

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

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

enota: x

inverzi:

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

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

$a^{-1}x + ba^{-1}$ je inverz

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

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

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

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

④ $f: G \longrightarrow \mathbb{R}^*$

$f(ax+b) = a$

f je homomorfizem

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

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

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

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

$N = \ker f \lhd G$

surjektivnost:

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

⑤

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

$f: ae^{i\alpha} \longmapsto e^{i\alpha}$

surjektivna ✓ $\quad f(z) = \frac{z}{|z|}$

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

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

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

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

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

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

⑥ $\dfrac{\mathbb{R}^*}{\mathbb{R}^+}$ $\qquad f: \mathbb{R}^* \longrightarrow ? \{-1, 1\}$

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

$f(a) \longrightarrow \dfrac{a}{|a|}$

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

homomorfizem: $f(a \cdot b) = \dfrac{ab}{|ab|} = \dfrac{a}{|a|} \cdot \dfrac{b}{|b|}$

$= f(a) \cdot f(b)$ ✓

surjektivno: $\dfrac{1}{1} = 1$ $\quad f(1) = 1$ $\quad f(-1) = 1$ $\quad \dfrac{-1}{1} = -1$

⑦ Kako znamo je izomorfna grupa U_n/SU_n

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

⑨ $? \cong \mathbb{R}/\mathbb{Z}$

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

$$\rho: U_n \longrightarrow T$$
$$A \longmapsto \det A$$
$$\rho(A \cdot B) = \det(A \cdot B) = \det A \cdot \det B$$

surjektivno se

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

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

⑧ $\frac{T}{N} = T$

$\rho: e^{i\varphi} \longmapsto e^{i2\varphi}$ je homomorfizam
$\Rightarrow$ sur ✓

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

⑨ $\mathbb{R}/\mathbb{Z} \longrightarrow [0, 1)$

~~$0,a_1a_2\ldots \longrightarrow 0,a_1\ldots$~~

$$n \longrightarrow e^{i2n\pi}$$

$$x \longrightarrow e^{i2x\pi}$$
$$\mathbb{R}/\mathbb{Z} \longrightarrow T$$

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

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

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

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

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

Pokaži, da je center enostavnega kolobarja polje

rabimo komutativnost in obstoj 1

$Z(K)$ je kolobar in je komutativen

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

$ab = b \cdot a$ „ka

generirama ak ideal

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

$ak + at = a(k+t)$ ✓

$a \in ak$ torej je ak neničelni

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

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

Pokažimo da je $b \in Z(G)$

$k \in K$

$k = (ab)k = k(kb) = akb$

$bk = bakb = kb$

za poljuben k

$\Rightarrow pr_1 I = I_1$

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

enako za I_2

K_1, K_2 kolobarja oblike $I_1 \times I_2$ $I_1 \trianglelefteq K_1$ in $I_2 \trianglelefteq K_2$

$I_1 \times I_2 = \{(a,b) \; ; \; ak_1 = k_1 a \; ; \; bk_2 = k_2 b\}$

aditivna podgrupa

Naj bo $I \trianglelefteq \overset{K}{K_1 \times K_2}$

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

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

Kaprtest za podobnost:

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

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

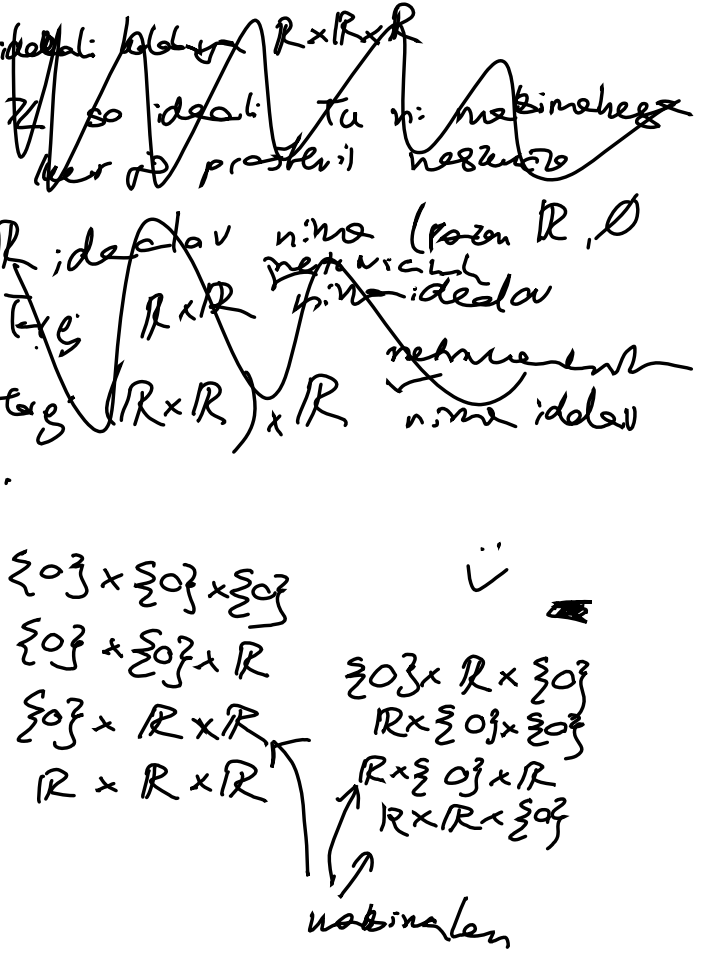
Opomba: Za grupe podobno to ne velja

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

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

$H_1 \trianglelefteq \mathbb{Z}_2$ ~~ni~~ $H_2 \trianglelefteq \mathbb{Z}_2$

(5)


$\mathbb{R}\times\mathbb{R}\times\mathbb{R}$
$\{0\}\times\{0\}\times\{0\}$
$\{0\}\times\{0\}\times\mathbb{R}$
$\{0\}\times\mathbb{R}\times\mathbb{R}$
$\mathbb{R}\times\mathbb{R}\times\mathbb{R}$
$\{0\}\times\mathbb{R}\times\{0\}$
$\mathbb{R}\times\{0\}\times\{0\}$
$\mathbb{R}\times\{0\}\times\mathbb{R}$
$\mathbb{R}\times\mathbb{R}\times\{0\}$
maksimalen

$(g(x))$ ... glavni: kolobarja $F[x]$

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

Presek in vsota ideala (x^2+x) in (x^2-x) v kolobarju $R[x]$ (in produkt: I, J)

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

$IJ = \{\sum_{i=1}^{n} x_i y_i \; ; \; x_i \in I \; y_i \in J\}$

(1) $I \cap J$

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

Večkratniki: prvega in drugega so večkratniki

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

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

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

Rešitev $h(x)(x^2+x)(x^2-x) \in I \cdot J$

$I+J$

$I = (2)$
$J = (6)$ $\quad I+J = (2)$

$I+J = (x)$

$I+J \subseteq (x)$

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

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

$(x) \subseteq I+J$

dovolj je pokazat $x \in I+J$

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

$\in I \qquad \in J$

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

② -||- $\mathbb{R}[x]/x^2+1$ -||-

③ Ali je izomorfen $\mathbb{R}[x]/x^2-1$?

$I = (x^2+1)$ $(f(x))$ ... glavni ideal $= \{p(x)\cdot f(x) ; f(x) \in \mathbb{R}[x]\}$

Odseki imajo oblik $f(x)+I$

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

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

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

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

→ stopnja manjša od 2 (ker $x^2 \neq 1$)

Vseh odsekov ima oblik

$ax+b+I$

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

$a=c \quad b=d$

(ker mora biti večkratnik od x^2+1)

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

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

$a=1 \quad c=1$
$b=i \quad d=-i$ ...

$(x+i)(x-i) = x^2+1 \in I$ ✓

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

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

③ Ali je izomorfen kolobarju ? Ne ker ima ~~8~~ ta delitelja nica, tisti par ne

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

③ Naj bodo $I_1, \dots I_s$ ideali: kolobarja K

in velja $I_i + I_j = K$ za $\forall i \neq j$

Definirajmo $\varphi: K \longrightarrow K/I_1 * K/I_2 * \dots * K/I_s$

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

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

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

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

$(a+I_1 \dots a+I_s) + (b+I_1, \dots b+I_s)$ ✓

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

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

surjektivnost

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

$a_i - a \in I$ za $\forall$

Dovolj je pokazati da $\exists a_i$ da $(0, \dots a_i+I_i, \dots 0)$ leži v imp. Preostali ad $(0, \dots 1+I_i \dots 0)$ bosta rešitev

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

velja $I_i + I_j = K$ za $\forall i \neq j$

$1 \quad a_1 = a_2+b_2 = a_3+b_3 = \dots a_s+b_s$ $\quad a_i \in I_1$, $b_i \in I_i$

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

$a_2a_3 \dots a_s + \dots + \underbrace{b_2b_3 \dots b_s}$

člani del ki nima neke $i \in I_1$

$1+I_1 = b_2b_3 \dots b_s + I_1$

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

$\in I_2 \dots I_s$

$A \in \ker\varphi \Leftrightarrow a \in I_1, I_2 \dots I_s$

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

④ (Kitajski izrek o ostankih)

Naj bodo $n_1, \dots, n_s$ po parih tuja cela števila. Pokaži da za poljubna cela števila $a_1 \dots a_s$ $\exists$ celo število a, ze katero velja

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

Če je $b \equiv a_i \pmod{n_i} \Rightarrow n_1 \dots n_s \mid (a-b)$

Poišči ~~x ∈ Z da velja~~

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

$x \equiv 2 \pmod 3$

$x \equiv 1 \pmod 4$

$x \equiv 3 \pmod 7$

$x = 17$ je ena rešitev

Naj bo c kolobar vse konvergentnih realnih zaporedij in C_0 množica vseh zaporedij z limito 0

Pokaži da je C_0 maksimalni ideal C in ~~kvocientni kolobar~~ $C/C_0 \cong$

⑥ Pokaži, da je kolobar

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

Poišči take ideale I in J kolobarja

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

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

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

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

$\varphi(\underbrace{a_0 + a_1 x + a_2 x^2 \ldots}_{}) + a_n x^n) = \begin{bmatrix} a_0 & a_1 \\ 0 & a_0 \end{bmatrix}$

ali:

$\varphi(a_0 + a_1 x + \ldots a_n x^n) \cdot (b_0 + b_1 x + \ldots b_n x^n)) =$

$= \varphi(a_0 b_0 + x(a_0 b_1 + b_0 a_1) + \ldots) =$

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

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

~~sestavljanje~~: aditka

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

$\ker \varphi$: $\begin{bmatrix} 0 & 0 \\ c & 0 \end{bmatrix} = \varphi(0 + 0 + x^2 \underbrace{g(x)}_{n}) =$

$\varphi(1) = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ ✓ $\qquad I$

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

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

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

$\rho\left(\begin{bmatrix} m & k \\ 0 & n \end{bmatrix}\begin{bmatrix} a & b \\ 0 & c \end{bmatrix}\right) = \rho\left(\begin{bmatrix} mk & \cdots \\ 0 & nc \end{bmatrix}\right) =$

$(mk, nc) = (m,n)\cdot(a,c)$ mod 2.

odd+odd=even

$\ker\rho = \begin{bmatrix} 0+\mathbb{Z}_2 & k \\ 0 & 0+\mathbb{Z}_2 \end{bmatrix} = (0,0)$ ✓

$\rho\begin{bmatrix} m & k \\ 0 & n \end{bmatrix} = m \pmod 4$

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

$K, H < G$

$H \trianglelefteq G$ in $K \trianglelefteq H$

$K \trianglelefteq H \trianglelefteq G$

Ali je $K \trianglelefteq G$

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

Podgrupa $N \overset{N}{\leq} G$ je <u>karakteristična</u>, če

$\varphi(N) \subseteq N$ za $\forall\ \varphi \in Aut(G)$

karakteristična grupa je edinka

Pokaži:

a) $\{1, -1, i, -i\}$ je edinka, ni pa karakteristična

b) $\forall G \neq \{1\}.\ G \times \{1\} \trianglelefteq G \times G$ ni pa karakteristična podgrupa

c) $Z(G)$ je karakteristična podgrupa

d) $K \overset{kar}{\leq} G$ $H \overset{kr}{\subset} G$ potem je $K \overset{kar}{\subset} G$

① G .... p-grupa
H ... q-grupa $\quad p \neq 2$ praštevili

G in H sta ciklična $\Leftrightarrow$ $G \oplus H$ 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 tuji

$\Leftarrow$ $G \oplus H$ ciklična, torej je abelova
$\Rightarrow G$ in H sta tudi abelovi

$|G \oplus H| = p^s \cdot 2^t$ $\qquad G' \qquad H'$

$G \oplus H \cong \mathbb{Z}_{p^{\alpha_1}} \oplus \dots \oplus \mathbb{Z}_{p^{\alpha_k}} \oplus \mathbb{Z}_{2^{\beta_1}} \oplus \dots \oplus \mathbb{Z}_{2^{\beta_l}}$

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

$G' \ni a'_G \; \text{red}\, a'_G = s \;\wedge\; H' \ni a'_H \; . \; \text{red}\, a'_H = t$

zaradi enoličnosti razvoja $G \oplus H$
zaključimo da $G \cong G'$ in $H \cong H'$

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

---

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

$|G| = n$

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

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

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

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

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

BŠZS: $p = p_1$

Dokažimo: G ima $p-1$ elemento 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 ■

$(\Leftarrow)$

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

ker je končna abelova grupa

$\rightarrow p-1$ elementov reda p

Pokazati moramo da je $k = 1$

Recimo da $k \neq 1$

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

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

$p^{\alpha_k - 1}, \dots (p-1)p^{\alpha_k - 1}$ imajo red p

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

Torej $k = 1$ to velja za vse ✗

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

Torej je ciklična

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

---

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

Recimo da $|G|=200$ abelova
Pokaži: G ima podgrupo reda 20

200	2
100	2
50	2
25	5
5	5

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

$G = G_1 \oplus G_2$ (red 8, red 25)

$H = H_1 \oplus H_2$ (red 4, red 5)

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

Vse možnosti:

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

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

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

Podobno za G_2

Naj bo m $m|n$ poljuben

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

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

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

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

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

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

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

Pa velikosti:

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

Potem je

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

rela

$\dots = p^j$

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

2. naloga za (4)

$H \leq A_4$ podgrupa reda 6

imamo 2 možnosti:

1) $H \cong S_3$

2) $H \cong C_6$ ~~ne, ker A_4 nima~~ nima elementa reda 6

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

$\Rightarrow H = \{\overbrace{(12)(3,4)}^{A}, \overbrace{(13)(24)}^{B}, \overbrace{(14)(23)}^{C}, 1, 2\text{ 3-cikla}, 1\}$

1) $\{A, B, C, 1\}$ je $< A_4$ ~~test~~ $H = 6$: ni mimo podgrupe stopnje 3

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

- ampak $ab = ba$ $ac = ca$ $bc = cb$

⑤ Pokaži da je podgrupa

$B = \langle (1,1), (1,3) \rangle$ grupe $\mathbb{Z} \oplus \mathbb{Z}$ izomorfna grupi $\mathbb{Z} \oplus \mathbb{Z}$ in da je

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

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

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

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

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

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

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

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

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

$\varphi(1,0) \longmapsto (1,1)$

$\varphi(0,1) \longmapsto (1,3)$

φ si razširi do homomorfizma

$\varphi(\alpha_{(1,0)} + \beta_{(0,1)}) = \alpha(1,1) + \beta(1,3)$

$\| \qquad\qquad \|$

$\varphi(\alpha \cdot 1, \beta) \qquad (\alpha+\beta, \alpha+3\beta)$

$\| \quad (\alpha, \alpha) + (\beta, 3\beta)$ ✓

φ je injektiven

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

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

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

$\alpha + 3\beta = 0$

$2\beta = 0 \Rightarrow \beta = 0 \Rightarrow \alpha = 0$

sur.

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

$\ker \varphi = B$

$\varphi(\alpha, \beta) = (\alpha + \beta) \bmod 2$

je homomorfizem

surj: $\varphi(1,1) = 0$

$\varphi(1,0) = 1$

$\ker \varphi$: $\alpha + \beta \bmod 2 = 0$

$C = \{ \alpha + \beta \bmod 2 = 0$

$C = B$

$B \subseteq C$

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

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

$\alpha + 3\alpha + \beta + \beta = 4\alpha + 2\beta$ je sod

$C \subseteq B$

~~$(a+b) \cdot 2c$~~

$(a,b) \in C$ poljuben $a + b = 2c$

$a = \alpha + \beta$

$b = \alpha + 3\beta$

$\alpha - b = 2\beta$

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

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

obstaja rešitev

⑥ Ponovimo:

elementa σ in $\pi \in S_n$ sta konjugirana

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

$\Leftrightarrow \sigma$ in π imata enako ciklično strukturo (enako št enako dolgih ciklov)

Cilj: Konjugiranostni razredi v A_n

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

1) $C(\sigma) \subseteq A_n \Rightarrow$ konjugiranostni razred σ v S_n razpade na 2 enako velika razreda v A_n

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

3) Iz predavanj sledi: moč razreda deli red grupe

Ta razred razpade na 2

Opiši konjugirane razrede v S_4 in A_4

V A_4 imamo 4 razrede
(id, produkt dveh disjunktnih ciklov, ...)

V S_4 je

1) id
2) en dvacikel
3) dva dvacikla
4) en tricikel
5) 4-cikel

② Opiši konjugiranostni razred grup

Q in D_8

"Js bi podvojil število nalog in jo del naslednjema"

-bor

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

$Z(Q) = \{1, -1\} \Rightarrow \{1\}, \{-1\}$ sta konjugira razreda

i: Vemo: moč orbite je enaka indeksu centralizatorja

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

Torej orbita iŋa ima 2 elementa

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

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

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

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

Podobno za vse ostale j ink

Torj $Q_j = \{j, -j\} \quad Q \cdot k = \{k, -k\}$

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

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

$C(r) = \{id, r, r^2, r^3\}$ to so vsi ker če bi bila še kaj več bi morala biti 8, ampak r ni v centru, ker ima največ 4

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

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

$zrz^{-1} = zzr^3 = r^3$

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

$|D_8 \cdot z| = 2$

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

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

ostaneta zr in zr^3 ne moreta biti sama ker če bi bila sama bi bila v centru

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

⑥ Naj bo $g = (1\ 6\ 9)(2\ 10)(3\ 4\ 5\ 7\ 8) \in S_{10}$

Opiši orbite in stabilizatorje za naravno delovanje grupe $G = \langle g \rangle$ na množici $X = \{1, \ldots, 10\}$

tj $h \cdot x = hx$

(4) $G \leq GLn(\mathbb{R})$

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

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

$A \cdot v = Av$

Opiši orbite tega delovanja, če

a) $G = GLn(\mathbb{R})$

b) $G = O_n(\mathbb{R})$

c) G je iz diagonalnih matrik v $GLn(\mathbb{R})$

d) G je sestavljena iz vseh zgornje trikotnih obrljivih matrik

V točkah a in d) poišči stabilizator vektorja

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

a) $A \cdot 0 = 0$ za $\forall A \in GLn(\mathbb{R})$

1) $\{0\}$

Naj bosta v in w neničelna vektorja

Dopolnimo v in w do vsaka svoje baze

n. obstaja prehodna matrika da velja

$v \mapsto w$

Torej druga orbita je vse ostalo

b) $\{O\}$ orbita

množenje z ortogonalnim ohranja dolžino teorij

če sta v in u v isti orbiti morata imeti iste orbite

normiramo u in v in ju dopolnimo do ortonormirane baze. Obstaja prehodna ortogonalna matrika in preslika $\frac{u}{\|u\|}$ v $\frac{v}{\|v\|}$ torej skalarji

u v v ker $\|u\| = \|v\|$

$\Rightarrow$ u in v sta v isti orbiti

$\Leftarrow$ ista norma

c) G = diagonalna matrika

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

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

nicle se ne ispih mogoče bot v

z^n

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

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

$y \neq 0 \Rightarrow \begin{bmatrix} b \in \mathbb{R} \\ a \in \mathbb{R} \end{bmatrix}$

~~dve orbiti~~:

Podobno za več dimenzij

1) zadnjih k je $\neq 0 \Rightarrow$ { zadnjih k so $\neq 0$

2) Torej je $n - k$ ali bolj

Burinsidova lema

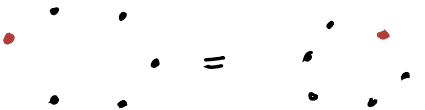
$G \curvearrowright X$

orbit: $\frac{1}{|G|} \sum_{g \in G} |g^x|$

$g^x = \{x \in X ; gx = x$

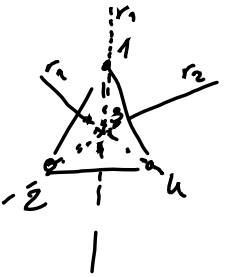
6 korald n različnih barv

Poišči število ogrlic, ki jih lahko sestavimo.
(ogrlica: sta enaki če se da eno preoblikati
v drug z rotacijo ali zrcaljenjem



(3) Na koliko načinov se da pobarvati lica pravilnega tetraedra z rdečo modro in zeleno tako da jih natanko eno lice modro

(4) Na koliko načinov se da pobarvati robove pravilnega tetraedra z rdečo in modro



$\{\frac{2\pi}{3}, \frac{4\pi}{3}\} \times 4 \cup \{id\}$

$r_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix} = (2\ 4\ 3)$

$r_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix} = (1\ 3\ 4)$

$r_1 \cdot r_2 = (2\ 4\ 3)(1\ 3\ 4) = (1\ 2\ 4) = r_3$

$z_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} = (1\ 3)(2\ 4)$

$z_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} = (1\ 2)(3\ 4)$

$z_3 = (1\ 4)(2\ 3)$

A_4

$S_4 \geq G \geq A_4$

$G \neq A_4 \Rightarrow G = S_4$ ker pa ne velja

g	št neg točk
1 : id	$4 \cdot 2^3$
8 : (i j k)	$1 \cdot 2$
3 : (ij)(kl)	0

$\frac{1}{12}(4 \cdot 2^3 + 8 \cdot 2) = \frac{2}{3}(4+2) = 4$

Izrek: Sylowa

$|G| = t \cdot p^s \quad p \nmid t \quad p \ldots$ praštevilo

p-podgrupa Sylowa je podgrupa moči p^s

$n_p \ldots$ število p-podgrup sylowa

$n_p \equiv 1 \mod p$

$n_p \mid |G|$

$n_p \mid t$

Dokaz: $n_p \mid t$

$n_p \mid t \cdot p^s \qquad (n_p, p) = 1$

$(n_p, p^s) = 1 \Rightarrow n_p \mid t$

⑤ Pokaži da ima S_4 4 3-podgrupe Sylowa

⑥ Pokaži da je vsaka 2-podgrupa Sylowa S_4 izomorfna D_8

Navedi vse 2-podgrupe Sylowa in elemente s katerimi so dane generirane!

$|S_4| = 24 = 3 \cdot 2^3$

3 podgrupa Sylowa ima moč 3

2-podgrupa Sylowa ima moč 8

$n_3 \mid 8 \quad n_3 \equiv 1 \bmod 3$

$n_3 = \{1, 4\}$

$n_2 \mid 3$

$n_2 \equiv 1 \bmod 2$

$n_2 = \{1, 3\}$

Velja: $n_p = 1 \Leftrightarrow$ p-ga podgrupa Sylowa je edinka

$P_1 = \langle (1,2,3) \rangle$

$P_2 = \langle (2\,4\,2) \rangle$

$P_3 = \langle (1\,3\,4) \rangle \Rightarrow n_3 = 4$

$P_4 = \langle (2\,3\,4) \rangle$

za n_2:

$H_1 = \{(1,2,3,4), (1\,3)(2\,4), (1\,4\,3\,2), (1\,2)(3\,4), (1\,4)(2\,3), (1\,3)(2\,4), id\}$

To je 2-podgrupa Sylowa S_4

$H_2 = \{(1\,3\,2\,4), (1\,2)(3\,4), (1\,4\,2\,3), (1\,3)(2\,4), (1\,4)(2\,3), (1\,2)(3\,4)\}$

(vse ostale konjugiranke z $(2,3)$)

DN: H_3 in element ki konjugira H_1 in H_3

Pomembne uporabe izrekov izrekov Sylowa: iskanje enost. grup. (Nima drugih edinke)

Enostavna grupa: nima pravih delit

$|A_5| = 60$

A_5 je enostavna

(7) Pokaži da (poljuben) grupa reda n ni enostavna če:

a) $n = 88$

b) $n = 30$

c) $n = 48$

d) $n = 36$

a) $n = 88 = 2^3 \cdot 11$

$p_1 = 11 \rightarrow n_{11} = 1 \mod 11$

$n_{11} | 8 \Rightarrow n_{11} = 1$

$\Rightarrow$ ker je edina je edinka

b) $n = 30 = 2 \cdot 3 \cdot 5$

$p_1 = 2 \quad n_2 = 1 \mod 2$

$n_2 \nmid 15$

$n_2 \in \{1, 3, 5\}$

$p_3 = 5$

$n_5 = 1 \mod 5$

$n_5 | 6$

$n_5 : \{1, 6\}$

Recimo da imamo 6 podgrup reda 5

Njihov presek je samo id

Torej je 24 elementov reda 5

Če $n_3 = 10$

Vseh 20 elementov reda 3

$20 + 24 > 30$

ali: $n_3 = 1$ ali: $n_5 = 1$

① $H \leq G$ onecmo

$N_G(H) = \{ g \in G : gHg^{-1} = H \}$ $\left(\begin{matrix} H \trianglelefteq G \Rightarrow \\ G = N_G(H) \end{matrix} \right)$

$C_G(G) = \{ g \in G ; ghg^{-1} = h \text{ za } \forall h \in H \}$

$\Updownarrow$

Pokaži $\quad gh = hg$

$N_G(H)/C_G(H)$ izomorfna $Aut(H)$

ocitno: $C_G(H) \trianglelefteq N_G(H)$

$\varphi : N_G(H) \longrightarrow Aut(H)$

$g \longmapsto \varphi_g \quad (\varphi_g(h) = ghg^{-1})$

$\varphi_{g_1} \circ \varphi_{g_2} = \varphi_{g_1 \cdot g_2}$ ocitno

$\ker \varphi = \{ g \in N_G(H), \varphi(g) = 1 \} =$

$\qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad \| \; id_H$

$\{ g \in N_G(H) ; ghg^{-1} = g \} = C_G(H)$

$\frac{N_G(H)}{C_G(H)} \cong im \varphi \leq \langle Aut(H) \rangle$

② Najbo $G = \mathbb{H}^*$ (neničelni kvaternioni)

$H = \{1, -1, i, -i\} < G$

Določi $N_G(H)$, $C_G(H)$ in pokaži:

$$\frac{N_G(H)}{C_G(H)} \cong \mathbb{Z}_2 \cong Aut(H)$$

gHg^{-1}

$g(-1)g^{-1} = -1 \in H$

$N_G(H) = \{g \in G ; gig^{-1} \in H\}$

$gig^{-1} = 1$

$gi = 1g$

$i = 1$ *

$gig^{-1} = i$

$gi = ig$ torej iščemo centralizator i

$g = a + bi + cj + dk$

$gi = ig \Leftrightarrow g = a + bi$

$gig^{-1} = -i$

$gi = -ig$

$ai - b - ck + dj = (ai - b + ck - dj)$

$ai - bi = -ai + b$

$2ai = 2b$

$ai = b$ * $a = b = 0$

$g = ck + dj$

$gig^{-1} = i \Rightarrow$

$g(-i)g^{-1} = -i$

$N_G(H) = \{a + bi ; a, b \in \mathbb{R}, a^2 + b^2 \neq 0\} \cup$

$\{cj + dk ; c, d \in \mathbb{R}, c^2 + d^2 \neq 0\}$

$C_G(H) = \{a + bi ; a, b \in \mathbb{R}, a^2 + b^2 \neq 0\}$

$Aut(H)$

$H \cong \mathbb{Z}_4 \quad H = \langle i \rangle$

$Aut(H) = \{id_H ; (i \mapsto -i)\}$ (zaradi dimenzije redov)

$Aut(H) \cong \mathbb{Z}_2$

def: $\varphi : N_G(H) \longrightarrow Aut(H)$

$g \longmapsto (h \mapsto ghg^{-1})$

$g \mapsto id_H \Rightarrow h = ghg^{-1}$ za $\forall h$

$\Leftrightarrow g \in C_G(H)$

za $g = cj + dk$

poljuben $g \mapsto (i \mapsto (-i))$

ker ni v centralizatorju, torej jo tisto

ker ostane

3) Pokaži da grupa reda 48 ne more biti enostavna

4) -||- reda 36 ne more biti enostavna

$48 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 3 = 2^4 \cdot 3$

2 podgrupa Sylova ima red 16
3-podgrupa Sylova ima red 3

n_2 .... št 2-podgrup

$n_2 = 1 \pmod 2 \qquad n_2 \mid 3$

$n_2 \in \{1, 3\}$

če $n_2 = 1$ bi pomenilo da je edinka, torej grupa ni enostavna

Recimo da je $n_2 = 3$ torej so 3 take podgrupe

Naj bosta H, K dve podgrupi

$|H \cap K| = \{1, 2, 4, 8, 16\}$

$|HK| = \frac{|H| \cdot |K|}{|H \cap K|} = \frac{16 \cdot 16}{|H \cap K|} \leq 48$

$|H \cap K| \geq \frac{16}{3}$

$|H \cap K| = 8$

$N_G(H \cap K) \leq G$

$H \cap K \lhd H$
$H \cap K \lhd K$ $\Rightarrow$ ~~$HK \leq$~~

$hxh^{-1} \in H \cap K \Rightarrow h \in N_G(H \cap K)$

$H \subseteq N_G(H \cap K)$
$K \subseteq N_G(H \cap K)$

$|N_G(H \cap K)| \geq |H| + |K| - |H \cap K| = 24$

torej $|N_G(H \cap K)| \in \{24, 48\}$

Ne sme biti 24, ker potem bi bila edinka (ker indeks 2)

Če $|N_G(H \cap K)|$ cela grupa je $H \cap K$ edinka v G

⑤ Naj bo G končna grupa $H < G$

$[G:H] = m$

Pokaži: $|G| \nmid m!$ G ne more biti enostavna

Primeri:

$m = 3$:

H je indeksa 3

$\Rightarrow G$ ne more biti enostavna

$|G| = 48$

H 2-podgrupa Sylowa

$[G:H] = 3$

G ne more biti enostavna

$G \cdot H = \{gH ; g \in H\}$

$|G \cdot H| = m$

G deluje na množici odsekov

$g \cdot hH = ghH$

(Delovanje je $\rho: G \longrightarrow Sym(G \cdot H)$

$\rho: g \mapsto \rho_g(hH) = ghH$

ρ je homomorfizem

$\frac{G}{\ker \rho} \cong im\rho \leq Sym(G \cdot H)$

$\ker \rho \trianglelefteq G$

$\ker \rho \notin \{\{1\}, G\}$

$|im\rho| \mid m!$ $\leftarrow |G \cdot H| = m$

$\|$

$|G/\ker \rho|$ $\quad G = |im\rho| \cdot |\ker \rho|$

če $|\ker \rho| = 1 \Rightarrow |G| \nmid m!$ $*$

če $|\ker \rho| = G \Leftrightarrow$

$\rho_g(hH) = hH$

$g \neq 1 \Rightarrow \rho_g = \begin{pmatrix} H & h_1H & \dots \\ gH & & \end{pmatrix}$

$g \notin H \Rightarrow gH \neq H$

$\Rightarrow \rho_g \neq id$

$|G| = 3 \cdot 2^k \qquad k \geq 2$

G ni enostavna

2-podgrupa Sylova je reda 2^k in je indeksa 3

H je 2-podgrupa Sylova

$[G:H] = 3$

$m = 3$

$k \geq 2 \Rightarrow |G| \geq 12 \Rightarrow |G| \nmid 6!$

④ Naj bo $|G| = 2m$; m liho

Pokaži, da ima G podgrupo indeksa 2 in zato ne more biti enostavna

---

iz reki sylova nedelujejo :i

Iščemo grupo reda m

Iščemo $f: G \longrightarrow \mathbb{Z}_2$ surj

$\Rightarrow \ker f \trianglelefteq G \quad [G : \ker f] = 2$

Cauchy $\Rightarrow \exists a \in G : a^2 = 1$

$G \curvearrowright G$ s levimi al: $\rho_g(h) = gh$

$\rho : G \longrightarrow Sym(G)$

$\rho(g) = \rho_g \qquad \rho_g(h) = gh$

$\rho_a(h) = ah$
$\rho_a(ah) = h$ Al: je lahko $ah = h$

$\Leftrightarrow a = 1$ ker a red 2 $\not\Rightarrow$

ρ_a je produkt transpozic (zamenjuje dva elementa) in nima negibnih točk $\Rightarrow$ je produkt m transpozic

$sgn(\rho_a) = -1$

$G \xrightarrow{\rho} Sym(G) \xrightarrow{sgn} \{1, -1\}$

kompozitum homomorfizmov
sgn je surjektivna ker id in ρ_a slikata v 1 oz -1 resp.

$\Rightarrow \ker \rho \trianglelefteq G \; ; [G : \ker \rho] = 2$

⑧ p - prost

Koliko različitih p-podgrup Sylowa ima S_p

⑨ Koliko p-podgrup Sylowa ima A_5 če

a) $p=2$
b) $p=3$
c) $p=5$

$|S_p| = p! = p(p-1)!$

P podgrupa Sylowa ima red p

$n_p \equiv 1 \bmod p \qquad n_p \mid (p-1)!$

P podgrupa Sylowa je $\cong \mathbb{Z}_p$

S_p ima $(p-1)!$ p-ciklov

$\Rightarrow \quad \frac{(p-1)!}{(p-1)} = (p-2)$ p-podgrupa Sylowa

Komutatorska grupa rešljive grupe

G, Grupa $A, B \subseteq G$

Označimo z $[A,B]$ podgenerirano z $[a,b] = a^{-1}b^{-1}ab$ kjer $a \in A$, $b \in B$

Z G' označimo $[G,G]$ - komutatorska podgrupa grupe G

---

1) Naj bo $H < G$ Pokaži da je $H \lhd G \Leftrightarrow [H,G] < H$

2) Pokaži da je $G' \lhd G$ in G/G' abelova

3) Naj bo H edinka in G/H abelova. Pokaži $G' \subseteq H$

$H \lhd G \Leftrightarrow [h,g] \in H \quad \forall g \in G, \forall h \in H$

$H \lhd G \Leftrightarrow gHg^{-1} \in H \ \forall g \in G \Leftrightarrow$

$ghg^{-1} \in H \ \forall g \in G, \forall h \in H$

$(\Rightarrow)$

$h^{-1}g^{-1}hg \in H$

$\in H$ (underbrace $g^{-1}hg$), $\in H$ (underbrace h^{-1})

$(\Leftarrow)\ h^{-1}g^{-1}hg \in H$

2) $G' \lhd G \Leftrightarrow \forall g \in G \ h \in G' \ ghg^{-1} \in G'$

Dovolj je pokazati za generator

$a^{-1}b^{-1}ab = [a,b]$

$g[a,b]g^{-1} \in G'$

$gaba^{-1}b^{-1}g^{-1} =$ $[gag^{-1}, gbg^{-1}]$

$gag^{-1}gbg^{-1}gag^{-1}gbg^{-1} =$

$[gag^{-1}, gbg^{-1}]$ To pa m. dk

malo pridt $[gag^{-1}, gbg^{-1}]$

(3)

$H \lhd G$ in G/H abelova

Dovolj pokazati $\forall a,b \in G.\ [a,b] \in H$

Velmo $\forall a,b \in G.\ (ab)H = (ba)H \iff$

$(b^{-1}a^{-1}ba) \in H$

$\Rightarrow [b,a] \in H$ ∎

(4)

Poišči komutatorsko podgrupo

a) A_4

b) Q

c) S_n, $n \geq 3$

a) D_{2n} $n \geq 3$

a) $K = \{id, (12)(3,4), (13)(24), (14)(2,3)\} \trianglelefteq A_4$

$|A_4/K| = 3 \Rightarrow A_4/K$ je abelova

Po nalogi 3 $\Rightarrow G' \leq K$

$G' = \{1\} \Leftrightarrow G$ abelova

Torej $A_4' \neq \{1\} \Rightarrow$ je reda 2 ali 4

BSZS $(12)(34) \in A_4' \Rightarrow A_4' = K$

$g(12)(34)g^{-1} \in A_4'$

$g = (132) \Rightarrow$

$(31)(24) \in A_4'$

b) $Q = \{\pm 1, \pm i, \pm j, \pm k\}$

$H = \{\pm 1, \pm i\}$ $\quad |Q/H| = 2 \Rightarrow$ je abelova

$\Downarrow \quad H \triangleleft G$

$\Rightarrow \quad Q' \leq H$

Podobno $\quad Q' \leq H_j \quad \Rightarrow Q' = \{\pm 1\}$

c) $S_n \quad n \geq 3$

$|S_3| = 6$

A_3 je edinka

S_3/A_3 je abelova

$\Rightarrow S_3' \subseteq A_3$

Podobno $S_n \subseteq A_n$

$(a,b)(a,d)(a,b)(a,d) = (a\ b\ d)$

$(a\ b\ d) = [(a,b),(a,d)] \in S_n' \Rightarrow A_n \leq S_n'$

① Koliko elementov reda 7 je v enostavni grupi reda 168

J

168	2
84	2
42	2
21	3
7	7

$168 = 2^3 \cdot 3 \cdot 7$

Obstaja 7-podgrupa Sylowa in je izomorfna $\mathbb{Z}_7$ ki ima 7 elementov reda 7

$n_7 \equiv 1 \mod 7 \quad n_7 \mid 2^3 \cdot 3$

$n_7 \in \{1, 8\}$

$n_7 = 1 \Leftrightarrow H$ je edinka. $\lightning$ (ker enostavna)

$\Rightarrow n_7 = 8$. selejo se vsaki v enakih

$8 \cdot 6 + 1 = 49$

49 elementov reda 7

(2) Pokaži da je 2-podgrupi $Sl_2(\mathbb{Z}_3)$ izomorfna grupi Q injc edink

$|Sl_2(\mathbb{Z}_3)| =$

$= \frac{|Gl_2|}{2} = 24 = 2^3 \cdot 3$

Gl_2: $\begin{bmatrix} \begin{bmatrix} \cdot & \cdot \\ \cdot & \cdot \end{bmatrix} & \begin{bmatrix} \cdot \\ \cdot \end{bmatrix} \\ \cdot & \cdot \end{bmatrix}$ $|Gl_2| = 48$

$3 \cdot 3 - 1 = 8$ $\quad 3-3$

$n_2 | 3 \quad n_2 \equiv 1 \bmod 2$

$\Rightarrow n_2 = \{1, 3\}$

$\varphi: Gl_2 \to \{-1, 1\}$

$A \mapsto \det A$

$\ker \varphi = Sl_2$

~~2-podgrupa Sylowa je edinka~~

~~ima red 8~~

$n_3 | 8 \quad n_3 \equiv 1 \bmod 3$

$n_3 \in \{1, 4\}$

$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^n = \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix}$ ima red 3

$\{e, \underbrace{\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}}_{A}, \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}\}$ je 3 podgrupa Sylowa

$\{e, \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 2 & 1 \end{bmatrix}\}$ je 3 podgrupa Sylowa

Torej jih je 4

$4 \cdot 2 = 8$ elementa reda 3

$\text{red} A = 3 \Rightarrow \text{red}(-A) = 6$

Torej najdemo še 8 elementov reda 6

Ostane nam še 8 elementov

Torej obstaja ena podgrupa Sylowa, ker ni: ple ca za več

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

$I, -I$ in še 6 drugih elementov

$ij = k \quad i^2 = j^2 = k^2 = -1$

$A^2 = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix}\begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} = \begin{bmatrix} 2 & 3 \\ 3 & 2 \end{bmatrix} = \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix} = -I$

$B^2 \quad \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}\begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} = -I$

imamo $A, -A, B, -B$

$C = AB = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix}\begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 3 & 2 \\ 1 & 3 \end{bmatrix} = \begin{bmatrix} 0 & 2 \\ 2 & 0 \end{bmatrix}$

③ Pokaži, da je grupa reda $8p$; $p \neq 2$ rešljive

Rešljiva:

$G = G_0 > G_1 > G_2 > \dots > G_n = \{1\}$

$G_i \trianglerighteq G_{i+1}$ G_i/G_{i+1} abelova

ekvivalentno

$G > G' > G'' > \dots > G^{(n)} > \dots$

$\exists n \in \mathbb{N}$ da je $G^{(n)} = \{1\}$

Dejstvo: Naj bo $H \trianglelefteq G$ in H in G/H rešljivi

$\Rightarrow$ G je rešljiva

$|G| = 8p = 2^3 \cdot p$

$p = 2 \Rightarrow |G| = 2^4$

iz predavanj vem, da so grupe reda p^n rešljive

ker: $Z(G) \neq \{1\}$ za končne grupe

$|Z(G)| = p^k$

$a \in Z(G)$ reda p

$\langle a \rangle \cong C_p \leq Z_G$

$\langle a \rangle \trianglelefteq G$

$|G/\langle a \rangle| = p^{n-1}$

indukcija ...

torej je G rešljiva

$p \neq 2 \Rightarrow 8p = 2^3 \cdot p$

2-podgrupa solva reda 8

p-podgrupa solva reda p

$n_p \mid 8$ $n_p \equiv 1 \bmod p$

$n_p \in \{1\}$ za $p > 7$ in $p = 5$

$\Rightarrow$ p-podgr. solva je cikl.

$H \cong \mathbb{Z}_p$ je rešljiva

$|G/H| = 8 = p^n$ je rešljiva

$p = 3 \Rightarrow$

$n_3 \in \{1, 4\}$

$n_3 = 4 \Rightarrow$

$\text{red } G = 24$

8 elementov reda 3 niso v ~~eni~~ 2-podgrupi

$n_2 \in \{1, 3\}$

$n_2 \Rightarrow 1$ n_2 je edinka reda 8

$|G/N_2| = 3$ rešljiva

$n_2 \Rightarrow 3$ reda 8

~~3 različni elementi~~ presek ni trivialen

ker pač tako

$H_1 \cap H_2 \in \{2, 4\}$

Polinom vs polinomska funkcija

$f(x) = x^2 + x \in \mathbb{Z}_2[x]$

$g(x) = 0 \in \mathbb{Z}_2[x]$

različna polinoma

$h(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$

Dva polinoma sta enaka če imata enake koeficiente

Polinom definira polinomsko funkcijo

$\tilde{f}(x) = \tilde{g}(x)$ ker $\tilde{f}(0) = \tilde{g}(0)$ in $\tilde{f}(1) = \tilde{g}(1)$

④

Določi kvadratni polinom iz $\mathbb{Z}_4[x]$ ki mu pripada ničelna polinomska funkcija

⑤ Naj bo F-polj. Pokaži da so naslednje pogoji ekvivalentna

a) F je končno

b) obstajata različna polinoma $f(x), g(x) \in F[x]$ ki enako pripadajo polinomske funkcije

---

④

$$x(x-1)(x-2)(x-3) \in \mathbb{Z}_4[x]$$

x	x^2	$2x$
0	0	0
1	1	2
2	0	0
3	1	2

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

⑤ F je končno polj

$F = \{a_1, a_2, \dots, a_n\}$

naredimo: $(x-a_1)(x-a_2)\cdot\dots\cdot(x-a_n)$

ima ničelno polinomsko funkcijo

b) $\Rightarrow$ a)

$\tilde{p}(x) = \tilde{f}(x)$ Recimo da $n \geq k$

$a_n x^n + \dots + a_0 = b_k x^k + \dots + b_0$

$a_n x^n + \dots + a_{k+1} x^k + (a_k - b_k) x^k + \dots + (a_0 - b_0) = \tilde{0}$

$(f-g)x$ je ničelno polinom

Vemo: $f(x) \in F[x] \wedge f(a) = 0 \Rightarrow (x-a) \mid f(x)$

$(f-g)(x) = (x-a) \cdot k \quad \forall a \in F$

$st(f-g) = d$

Vzamemo $(a_1, \dots, a_{d+1})$

$(x-a_i) \mid (f-g)$ za vsak a_i

potem $(f-g)(x) = (x-a_1)\cdot\dots\cdot(x-a_{d+1})\cdot k$

stopnja $\geq$ stopnja

Naj bo F poljе. Denimo da

neničelen polinom $P(x) \in F[x]$ v

n različnih elementih iz F doseže enako

vrednost potem že stopnja $\geq n$

---

v $a_1 \dots a_n$ doseže a

$P(a_1) = \dots = P(a_n) = a$

odvaja: $(P-a)(x)$ ima $a_1 \dots a_n$

torej $P(x) - a = k(x-a_1)\dots(x-a_n)$

[illegible]

① Razstavi na nerazcepne faktorje nad $\mathbb{R}$

a) $x^5 - 81x$

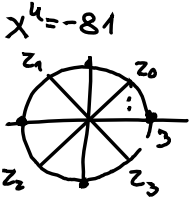
b) $x^5 + 81x$

Vsak polinom st ≥ 3 je razcepen

a) $x(x^4 - 81) = x(x^2 - 9)(x^2 + 9) =$

$= x(x-3)(x+3)(x^2+9)$

b) $x(x^4 + 81) =$



$x^4 + 81 = (x - z_0)(x - z_1)(x - z_2)(x - z_3)$

$= (x^2 + 2ax + (a^2+b^2))(x^2 + 2cx + (c^2+d^2))$

$a = \frac{\sqrt{2}}{2} \cdot 3 \quad b = \frac{\sqrt{2}}{2} \cdot 3$

$c = -\frac{\sqrt{2}}{2} 3 \quad d = \frac{\sqrt{2}}{2} \cdot 3$

$(x - (a+bi))(x - (a-bi)) = x^2 - 2ax + a^2 + b^2$

$x(x^4 + 81) = x(x^2 + 3\sqrt{2}x + 9)(x^2 - 3\sqrt{2}x + 9)$

② Pokaži, da je $f(x)$ nerazcepen nad $\mathbb{Q}$:

a) $f(x) = 7x^6 + 30x^3 - 6x^2 + 60$

b) $f(x) = \frac{2}{7}x^5 - \frac{7}{2}x^2 - x + 2$

Eisensteinov test

$p \in \mathbb{P}$. $f(x) = a_n x^n + \ldots + ax + a_0$ $\quad a_i \in \mathbb{Z}$

$p \mid a_{n-1}, \ldots, a_0 \quad p \nmid a_n \quad p^2 \nmid a_0$

$\Rightarrow$ $f(x)$ ni razcepen nad $\mathbb{Q}$

a) $7x^2 + 30x^3 - 6x^2 + 60$

$p = 3 \Rightarrow$ ni razcepen nad $\mathbb{Q}$

b) $14 f(x) = 4x^5 - 49x^2 - 14x + 28$

$p = 7 \Rightarrow$ $P(x)$ ni razcepen nad $\mathbb{Q}$

$f(x)$ nerazcepen $\Leftrightarrow$ $14 f(x)$ nerazcepen

(3)

$f(x) = x^n + 1$

Pokaži da je $f(x)$ nerazcepen nad $\mathbb{Q}$

$\Leftrightarrow n = 2^k \quad k \geq 1$

($\Rightarrow$) $n = 2 \quad x^2+1$ nerazcepen

$n = 3 \quad x^3+1 = (x+1)(x^2 - x + 1)$

$n = 5 \quad x^5+1 = (x+1)(\ldots)$

↗ velja za katero koli liho n

Recimo da n ni oblike 2^k

Torej $n = 2^k \cdot l$ $l \ldots$ liho število

$l \geq 3$

$x^6+1 = x^{2\cdot 3}+1 = (x^2)^3+1 = (x^2+1)(x^4-x^2+1)$

$x^{2^k l}+1 = (x^{2^k})^l + 1 = (x^{2^k}+1)(\ldots)$

$\Leftarrow$ x^2+1 ✓

x^n+1

Če Eisensteinov kriterij ne deluje za $f(x)$, lahko probamo za $f(x+1)$

$f(x+1) = (x+1)^4+1 = x^4+4x^3+6x^2+4x+2$

$p = 2$

Torej n ni razcepen

ker $f(x+1)$ nerazcepen $\Leftrightarrow f(x)$ ni razcepen

$f(x+1) = (x+1)^{2^k}+1 = \sum_{i=0}^{2^k} \binom{2^k}{i} x^{2^k} + 1 =$

$= x^{2^k} + \sum_{i=0}^{2^k-1} \binom{2^k}{i} x^{2^k} + 2$

$\binom{2^k}{i}$ je sod za $1 \leq i \leq 2^k - 1$

Potem velja kriterij za $p = 2$

$f(x+1) = (x+1)^{2^{k+1}} + 1 =$

$((x+1)^{2^k})^2 + 1 =$

Po indukcijski predpostavki:

$= (x^{2^k} + \underbrace{\text{sodi}}_{\text{sodi}} + 1)^2 + 1 =$

$= x^{2^{k+1}} + \underbrace{\text{sodi}}_{\text{sodi}} + 2$

④ za $\forall n = 2,3,4,5,6$

zapiš polinom $f_n(x) = x^n + 1$

kot produkt nerazcepnih polinomov nad $\mathbb{Z}_2$

⑤ Polinom $f(x) = x^4 + 2$ zapiši kot produkt

nerac. nad $\mathbb{Z}_3$

⑥ $f(x) = x^4 - 2x^3 - 2x + 4$ zapiši kot produkt

nerac. nad $\mathbb{Z}_7$

pol. ima faktor $(x-b) \Leftrightarrow f(b) = 0$

$x^2 + x + 1$ je edini nerazcepni v $\mathbb{Z}_2[x]$ stopnja 2

$f(x) = x^4 + 2$

Imamo 2 možnosti: razstavitve na 2 faktorja

•) linearen faktor +

$f(1) = 0$

$f(x) = (x-1)(\dots)$

$(x^4+2) : (x-1) = (x^4+2)(x+2)$

$x^4+2 = (x^2+1)(x-1)(x+1)$

⑥

$f(x) = x^4 - 2x^3 - 2x + 4 =$

$= x^3(x-2) - 2(x-2) =$

$= (x^3-2)(x-2)$

iščemo $x^3 = 2$ za neke $x \in \mathbb{Z}_7$

0	0
1	1
2	8
3	27
-3	-27
-2	
-1	

0
1
1
-1
1
-1
-1

$\Rightarrow x^3 - 2$ se ne razcepe

kako dokažimo razcepnost nad $\mathbb{Q}$

1) Eisensteinov test za $f(x)$
2) $\rightsquigarrow f(x+1)$
3) $\rightsquigarrow$ prevod ne polinom nad $\mathbb{Z}_p$

---

⑦ Naj bodo $a_0, \dots a_n \in \mathbb{Z}$ in $p \in \mathbb{P}$

$p \nmid a_n$

če je polinom $a_n x^n + \dots + a_1 x + a_0$ razcepen nad $\mathbb{Q}$

je $a_n \pmod p\, x^n + \dots + a_1 \pmod p + a_0 \pmod p$ razcepen nad $\mathbb{Z}_p$

Posledično: če je $a_n \pmod p\, x^n + \dots + a_0 \pmod p$ nerazcepen nad $\mathbb{Z}_p$ je $a_n x^n + \dots a_0$ nerazcepen nad $\mathbb{Q}$

$\Rightarrow$ Po predpostavki je $p(x)$ razcepen nad $\mathbb{Q}$

$p(x) = g(x) \cdot k(x)$ g, k nekonst

$= (b_m x^m + \dots + b_0)(c_\ell x^\ell + \dots + c_0)$

$m + \ell = n$

$a_n = b_m \cdot c_\ell$

$\rightarrow p \nmid b_m, c_\ell$

$\mathbb{Z} \longrightarrow \mathbb{Z}_p$

$n \longmapsto n \bmod p$

surjektivni homomorfizem kolobarjev

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

$\mathbb{Z}[x] \longrightarrow \mathbb{Z}_p[x]$

$a_n x^n + \dots + a_0 \longmapsto \overbrace{(a_n \bmod p) x^n + \dots (a_0 \bmod p)}^{f(x) \bmod p}$

DN: to je homomorfizem kolobarjev

$p(x) \bmod p = (g(x) \bmod p)(k(x) \bmod p)$

ker b_m in c_ℓ nista deljiva s p

faktorizacija ohranja

a, b, c liha števila $\Rightarrow p(x) = ax^4 + bx + c$ nerazcepen nad $\mathbb{Q}$

$p(x) = 7x^5 + 3x^2 + 1$ nerazcepen nad $\mathbb{Q}$

$p(x) = x^5 + x^2 + 1 \mod 2$

$p(0) = 1$

$p(1) = 1$

če bi bil razcepen je eden od faktorjev

$x^2 + x + 1$

$$(x^5 + x^2 + 1) : (x^2 + x + 1) = x^3 - x^2$$

$$-x^3 - x^4 - x^3$$

$$-x^4 - x^3 + x^2 + 1$$

$$+x^4 + x^3 + x^2$$

je ostanek

$1 \neq 0$ ni deljiv $\Rightarrow$ ni razcepen

$p(x) = 36x^3 + 7x + 6$

$p(x) = x^3 + 2x + 1 \mod 5$

$p(0) = 1$
$p(1) = 4$
$p(2) = 3$
$p(-1) = 3$
$p(3) = 4$ nima nicel $\Rightarrow$ ni razcepen

(4) $a_1 \dots a_n$ različna cela števila

Pokaži da je $p(x) = (x-a_1)\cdot\dots\cdot(x-a_n) - 1$ nerazcepen nad $\mathbb{Q}$

Recimo da je razcepen

$p(x) = g(x)\cdot r(x)$ $\quad st(g(x)) + st(r(x)) = st(p(x))$

BSZS vadilno; člen $g(x), r(x) \neq 1$

Vi ∈ [n]. $p(a_i) = -1 \Rightarrow p(a_i)\, r(a_i) = -1$

g in r imata cele koeficiente

$g(a_i) = \pm 1 \quad r(a_i) = \mp 1$

∀i:

I $g(a_i) = 1, r(a_i) = -1$

II $g(a_i) = -1 \; r(a_i) = 1$

BŠZS. I ali II velja v večini polovici (recimo I) ali enako

$st(g) \leq \frac{n}{2}$ BŠZS

$g(a_i) - 1 = 0$

$g(x) - 1$ ima $> \frac{n}{2}$ nicel ↯

$\Rightarrow st(g(x)) = \frac{n}{2}$ in $st(r(x)) = \frac{n}{2}$

$g(x) = b_k x^k + \dots + b_0 \qquad r(x) = c_k x^k + \dots + c_0$

$st(g(x) - r(x)) \leq \frac{n}{2} - 1$

Recimo da I velja za $a_1 \dots a_{\frac{n}{2}}$
in II velja za $a_{\frac{n}{2}+1}, \dots, a_n$

$g(x) - 1$ ima nicle za $a_1, \dots a_{\frac{n}{2}}$

$r(x) - 1$ ima nicle za $a_{\frac{n}{2}+1}, \dots a_n$

$(g(x)-1)(r(x)-1) = \underbrace{g(x)\cdot r(x)}_{-1} - r(x) - g(x) + 1 =$

$= -(g(x) + r(x))$ ima $a_1 \dots a_n$ nicel

↯ preveč nicel

$a_1 \dots a_n$ različna cela števila

Pokaži da je

$p(x) = (x-a_1)^2 \dots (x-a_n)^2 + 1$ nerazcepen nad $\mathbb{Z}$

Recimo da je $\exists r, g \in \mathbb{Z}[x]$ nekonst

$p(x) = r(x) \cdot g(x)$

$p(a_i) = 1$

$\forall i \Rightarrow r(a_i) \cdot g(a_i) = 1$

$r(a_i) = g(a_i) = \pm 1$

$p(x) > 0 \ \forall x \Rightarrow p(x)$ nima ničel $\Rightarrow$
$r(x)$ in $g(x)$ nimata ničel

$r(a_i) = 1$ in $r(a_j) = -1$ $\times$
ker je vezan $\Rightarrow$

$(\forall a_i . r(a_i) = 1) \vee (\forall a_i . r(a_i) = -1)$
$\Rightarrow \| g(a_i)$

BSZS $r(a_i) = g(a_i) = 1 \ \forall i$

$r(x) - n$ ima $\geq n$ ničel $\Rightarrow st(r(x)) \geq n$
$\| \quad st\, g(x) \geq$

$\Rightarrow st(r(x)) = st(g(x)) = n$

$st(p(x)) = st(g(x)) = 2n$

$r(a_i) - g(a_i) = 0 \Rightarrow$

$st(r(x) - g(x)) \geq n \ \forall a_i = 0$

$\Rightarrow$ ~~$g(x) = r(x)$~~ $r(x) = g(x)$

$\Rightarrow p(x) = r^2(x)$

$p(x) = \underbrace{((x-a_1) \dots (x-a_n))}_{A(x)}^2 + 1 = r^2(x)$

$A^2(x) - r^2(x) = -1$

$(r(x) - A(x))(r(x) + A(x)) = 1$

$\Rightarrow r(x) - A(x)$ je konstanten in
$A(x) + r(x)$ je konstanten

$\times$ ker ima $A(x)$ stopnjo n

Razširitve polj

E, F polj:

$E \subseteq F$ $\qquad$ $[F:E]$ stopnja razširitve

$\downarrow$

dim F kot vektorskega polja nad E

$a \in F$

$E(a)$ - razširitev F s pomočjo A

$\searrow$ najmanjše podpolje F, ki vsebuje E in a

npr: $\mathbb{Q}(\sqrt{2}) \supseteq \mathbb{Q}$

$$\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \,;\, a, b \in \mathbb{Q}\}$$

$[E(a):E] =$ st(minimalni polinom a v E)

st$(m_a(x))$ $\qquad$ $m_a x \in E[x]$

Če imamo $E \subseteq F \subseteq G$ zaporedje razširitev,

če $[G:E] = m$, $[G:F] = k$ $[F:E] = n$ $\Rightarrow m = kn$

$E \subseteq F \quad a \in F$

$E(a) = E \iff [E(a) : E] = 1$

($\Rightarrow$) minimalni polinom $x - a \in E$

($\Leftarrow$) Baza $E(a)$ nad E je $\{1\}$

$a = \underset{\in E}{\alpha} \cdot 1 \in E$

(1)

Pokaži $\mathbb{R}(a) = \mathbb{C} \iff a \in \mathbb{C} - \mathbb{R}$

$\Rightarrow$ Recimo da $a \in \mathbb{R}$

Potem $\mathbb{R}(a) = \mathbb{R}$

$\Leftarrow$ $a \in \mathbb{C} - \mathbb{R}$

$\mathbb{R} \subseteq \mathbb{R}(a) \subseteq \mathbb{C}$ $\quad [\mathbb{C} : \mathbb{R}] = 2$

oziroma $\mathbb{R} \neq \mathbb{R}(a) \Rightarrow [\mathbb{R}(a) : \mathbb{R}] \geq 2$

$\Rightarrow [\mathbb{R}(a) : \mathbb{R}] = 2 \rightarrow [\mathbb{R}(a) : \mathbb{C}] = 1$

$\Rightarrow \mathbb{C} = \mathbb{R}(a)$

Naj bo $[E:F] = 12$

Poiščimo zakaj elementi z E ne more biti algebraičen stopnje 8 nad F

---

a je alg. na stopnje k nad F če

$[F(a):F] = k$

$\Leftrightarrow$ min polinom $m_a(x) \in F[x]$ ima stopnjo k

---

$[E:F] = 12$

$F \subseteq F(a) \subseteq E$

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 Eisensteinovem kriteriju

$\sqrt[4]{2} = a^3 \in \mathbb{Q}(\sqrt[12]{2})$

$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[4]{2}) \subseteq \mathbb{Q}(\sqrt[12]{2})$

4 | 3

12

Naj bo n liho število

$\forall a \in \mathbb{Q}(\sqrt[n]{2}) - \mathbb{Q}$ velja $a^2 \notin \mathbb{Q}$

...

(2) Naj bo $[E:F] = p$ praštevilo

$\exists\, \geq F$

Popati v elementih E/F je alg. stopnja p nad F

$F \subseteq F(a) \subseteq E$ za neko

$\geq 2^r$ K

p

$p = r \cdot k \Rightarrow r = 1 \vee k = 1$

$\Rightarrow k = 1$

$\Rightarrow r = p$

③ Koliko je $[\mathbb{Q}(\widetilde{3-\sqrt{7}}):\mathbb{Q}]$?

koliko je $[\mathbb{Q}(3-5\sqrt[3]{7}+4\sqrt[3]{49}):\mathbb{Q}]$?

$a^2 = 9 - 6\sqrt{7} + 7$

$(x^2 - 6x)(a) = 16 - 6\sqrt{7} - 18 + 6\sqrt{7} = -2$

$\rightsquigarrow p(x) \; x^2 - 6x + 2$

↖ nerazložen, po Eisensteinu

stoga $\deg = 2$

2. način

$[\mathbb{Q}(\sqrt{7}) : \mathbb{Q}] = 2 \quad a \in \mathbb{Q}(\sqrt{7})$

$\Rightarrow \quad \mathbb{Q} \subseteq \mathbb{Q}(a) \subseteq \mathbb{Q}(\sqrt{7})$

$r \neq 1$

2

$\Rightarrow r = 2$

$[\mathbb{Q}(3-5\sqrt[3]{7}+4\sqrt[3]{49})$

Vemo $[\mathbb{Q}(\sqrt[3]{7}):\mathbb{Q}] = 3$ ker $x^3 - 7$ ni razložen

$b \in \mathbb{Q}(\sqrt[3]{7})$

$\mathbb{Q} \subseteq \mathbb{Q}(b) \subseteq \mathbb{Q}(\sqrt[3]{7})$

$b \notin \mathbb{Q} \Rightarrow r \neq 1 \Rightarrow r = 3$

$b \in \mathbb{Q} \quad 3 - 5\sqrt[3]{7} + 4\sqrt[3]{49} = \alpha$

$4x^2 - 5x + 3 - \alpha$ anihilira $\sqrt[3]{7}$

Annpk $x^3 - 7$ mali anihilira in ni delji v $\times$

Nasprotuje linearn: neodvisnosti

(Baza: 1. $\sqrt[3]{7}$, $\sqrt[3]{49}$)

$p(x) = 3 - 5x + 4x^2$

D $(p(x), x^3 - 7) = 1$

$\alpha(x)p(x) + \beta(x)(x^3 - 7) = 1$

$x = \sqrt[3]{7}$

$b^{-1} = \alpha(\sqrt[3]{7})$

⑤ Koliko je $[\mathbb{Q}(\underbrace{\sqrt[3]{3+\sqrt{3}}}_{a}) : \mathbb{Q}]$

$a^6 = (3+\sqrt{3})^2 = 9 + 6\sqrt{3} + 3 = 12 + 6\sqrt{3}$

$a^3 = 3+\sqrt{3}$

$a^6 - 6a^3 = 12 - 18 + 6\sqrt{3} - 6\sqrt{3} = -6$

$a^6 - 6\sqrt{3} + 6$ Po eisensteinu

$\Rightarrow [\mathbb{Q}(\sqrt[3]{3+\sqrt{3}}) : \mathbb{Q}$

a, b algebraični:

Pokaži $[F(a,b):F] = [F(a):F] \cdot [F(b):F]$

če sta si: tuji

$F \subseteq \underbrace{F(a)}_{m} \subseteq \underbrace{F(a,b)}_{k}$

$F \subseteq \underbrace{F(b)}_{n} \subseteq \underbrace{F(a,b)}_{c}$

$F(a,b) = mk = nc$

$\Rightarrow m \mid [F(a,b):F] \wedge n \mid [F(a,b):F]$

$\Rightarrow mn \mid [F(a,b):F]$

$[F(b):F] = n \Rightarrow \exists p(x) \in F[x] . \; p(b) = 0$ in je neprevedljiv

$p(x) \in F[x]$

$\Rightarrow p(x) \in F(a)[x]$

$p(b) = 0$

$\Rightarrow [F(a,b) : F(a)] \leq n \Rightarrow k \leq n \Rightarrow$

$[F(a,b):F] = mk \leq m \cdot n \Rightarrow = m \cdot n$ ●

(6)

$[\mathbb{Q}(\sqrt{3}, \sqrt[3]{7}) : \mathbb{Q}] = 2$

$2 \cdot 3 = 6$

⑧ $[\mathbb{Q}(\sqrt{3}+\sqrt[3]{5}):\mathbb{Q}] = ?$

⑤ Pokaži da je

$[\mathbb{Q}(\sqrt{3},i):\mathbb{Q}] = 4$

Pokaži a, da je $\mathbb{Q}(a) = \mathbb{Q}(\sqrt{3},i)$

Komentar

izrek o primitivnem elementu

$\mathbb{Q}(\sqrt{3},\sqrt[3]{5}) = \mathbb{Q}(\sqrt{3}+\sqrt[3]{5})$

$[\mathbb{Q}(\sqrt{3}):\mathbb{Q}] = 2 \quad [\mathbb{Q}(i):\mathbb{Q}] = 2$

① Pokaži: $F(a^k, a^l) = F(a^d)$; $d = (k, l)$

② $[\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) : \mathbb{Q}]$ in $[\mathbb{Q}(\sqrt[4]{2}, \sqrt[6]{2}) : \mathbb{Q}]$

$k = d \cdot \alpha$ $\quad a^k = a^{d\alpha} = (a^d)^\alpha$

$l = d \cdot \beta$ $\quad a^l = a^{d\beta} = (a^d)^\beta$

$F(a^k, a^l) \subseteq F(a^d)$

Dovolj je pokazati da $a^d \in F(a^k, a^l)$

$d = mk + nl \quad m, n \in \mathbb{Z}$

$a^d = a^{mk+nl} = (a^k)^m \cdot (a^l)^n \in F(a^k, a^l)$

② $\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) = \mathbb{Q}(2^{\frac{1}{6}})$

$2^{\frac{1}{2}}, 2^{\frac{1}{3}} = 2^{\frac{1}{6} \cdot 3}, 2^{\frac{1}{6} \cdot 2}$

$[\mathbb{Q}(2^{\frac{1}{6}}) : \mathbb{Q}] = 6$

ker $x^6 - 2$ minimalni polinom in je nerazcepen po eisensteinu

$\mathbb{Q}(\sqrt[4]{2}, \sqrt[6]{2}) = \mathbb{Q}(\sqrt[12]{2})$

$2^{\frac{1}{4}} = 2^{\frac{3}{12}}$ $\quad [\mathbb{Q} : \mathbb{Q}] = 12$

$2^{\frac{1}{6}} = 2^{\frac{2}{12}}$ $\quad$ ker $x^{12} - 2$ nerazc po eisku

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 $[\mathbb{Q}\,\sqrt[6]{2}:\mathbb{Q}(\sqrt{2})]$

Kolika je

$$[\mathbb{Q}(\sqrt[6]{3}, i) : \mathbb{Q}(\sqrt{3}+i)]$$

$$\mathbb{Q}(\sqrt[6]{3}, i) = \mathbb{Q}(\sqrt{3}+i)$$

$$\sqrt{3}+i = 3^{\frac{1}{2}}+i = 3^{\frac{3}{6}}+i = (\sqrt[6]{3})^3+i \in F$$

$\Rightarrow \mathbb{Q}(\sqrt{3}+i) = \mathbb{Q}(\sqrt{3}, i)$

$\subseteq$ ✓

2 $a = \sqrt{3}+i$

$i = a - \sqrt{3}$

$-1 = a^2 - a2\sqrt{3} + 3$

$a2\sqrt{3} = a^2 + 4$

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{3}, i) \subseteq \mathbb{Q}(\sqrt[6]{3}, i)$$

$$\mathbb{Q} \subset \mathbb{Q}(\sqrt{3}) \subseteq \mathbb{Q}(\sqrt{3}, i) \subseteq \mathbb{Q}(\sqrt[6]{3}, i)$$

$2 \quad 2$ (4)

$\mathbb{Q} \subset \mathbb{Q}(i) \subseteq \mathbb{Q}(\sqrt[6]{3}, i)$

$2 \quad 6$

12

$\Rightarrow [\mathbb{Q}(\sqrt[6]{3}, i) : \mathbb{Q}(\sqrt{3}+i)] = 3$

6 Pokaži da $\mathbb{Q}(\sqrt{3}) \neq \mathbb{Q}(\sqrt{2})$

7 Naj bodo $a_1, \dots, a_n$ algeb. nad F

Pokaži

$$[F(a_1, \dots, a_n) : F] \leq [F(a_1) : F] \cdots [F(a_n) : F]$$

6 Naj bo $\varphi : \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{3})$ izomorfizem

$\varphi(1) = 1 \quad \wedge \varphi(0) = 0$

$\varphi(2) = 2$ ker $1+1=2 \quad \varphi(1) + \varphi(1) = 2$

$\varphi(n) = n$ za $\forall n \in \mathbb{Z} \qquad \varphi(n^{-1}) = \varphi(n)^{-1} = n^{-1}$

$$\varphi\left(\frac{m}{n}\right) = \varphi(m \cdot n^{-1}) = \varphi(m) \cdot \varphi(n^{-1}) = m \cdot n^{-1}$$

$\rightsquigarrow \varphi$ ohranja racionalna števila

$\varphi(a + b\sqrt{2}) = a + b\varphi(\sqrt{2})$

$\varphi(\sqrt{2}) = \alpha + \beta\sqrt{3}$

$\varphi(2) = \alpha^2 + 2\alpha\beta\sqrt{3} + 3\beta^2 = 2$

$$\underbrace{2\alpha\beta\sqrt{3}}_{\in \mathbb{Q}} = \underbrace{2 - \alpha^2 - 3\beta^2}_{\in \mathbb{Q}}$$

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

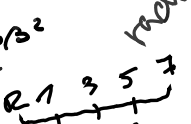
$\beta = 0 \Rightarrow \alpha^2 = 2 \quad \alpha \notin \mathbb{Q}$ *

$\alpha = 0 \Rightarrow 3\beta^2 = 2 \Rightarrow \beta = \sqrt{\frac{2}{3}} \notin \mathbb{Q}$

1. naj

Ajg

To je rešljivo v



nekaterih

ampak

ne bi

rekel

⑦

$n=2$:

$F(a,b) \leq F(a) \cdot F(b)$

$[F(a,b):F] \leq \underbrace{[F(a):F]}_{k} \cdot \underbrace{[F(b):F]}_{m}$

$\underbrace{F \leq F(a)}_{k} \leq F(a,b)$

Vemo: $[F:F(b)] = m \Rightarrow \exists p(x)$ nerazcep $\in F[x]$.
$p(b) = 0$ st$(p(x)) = m$

$p(x) \in F(a)[x]$

$p(x)$ je morda razcepen

Torej minimalni polinom st $\leq m$

Podobno za več njev

⑧ Naj bodo $a_1, \dots, a_n$ algebraični stopnje 2
Pokaži da stopnje razširitve

$[F(a_1, \dots, a_n) : F] = 2^k$ za neki $k \leq n$

⑨ Za različna praštevila $p_1, \dots, p_n$

$[\mathbb{Q}(\sqrt{p_1}, \dots, \sqrt{p_n}) : \mathbb{Q}] = 2^k$

$$F \underset{2}{\subseteq} F(a_1) \underset{\leq 2}{\subseteq} F(a_1, a_2) \underset{\leq 2}{\subseteq} F(a_1, a_2, a_3) \underset{\leq 2}{\subseteq} \dots \subseteq F(a_1, \dots, a_n)$$

$\Rightarrow$ Vsaki imamo izbiro 1 ali 2
Recimo da je k 2 $\Rightarrow$

$[F(a_1, \dots, a_n) : F] = 2^k \quad k \leq n$

⑩ Dokaži moramo za $\forall p \in \mathbb{P}$

$X^2 - p$ ni razcepen v $\mathbb{Q}(g_1, \dots, g_n)$

$$\mathbb{Q} \subseteq \underset{F}{\mathbb{Q}(\sqrt{2})} \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3}) \subseteq \dots$$

Velja: $F(\sqrt{a}, \sqrt{b}) \supseteq F$
$\sqrt{a}, \sqrt{b}, \sqrt{ab} \notin F$

$$F \underset{2}{\subseteq} F(\sqrt{a}) \underset{?}{\subseteq} F(\sqrt{a}, \sqrt{b})$$

$F \subseteq F(\sqrt{b}) \subseteq F(\sqrt{a}, \sqrt{b})$

$\sqrt{b} = \alpha + \beta\sqrt{a} \quad \alpha, \beta \in F$

$b = \alpha^2 + 2\alpha\beta\sqrt{a} + \beta^2 a$

$2\alpha\beta\sqrt{a} = b - \alpha^2 - \beta^2\alpha$

če $\alpha\beta \neq 0 \Rightarrow \sqrt{a} \in F$

$\Rightarrow \alpha\beta = 0$
$\alpha = 0 \Rightarrow b = \beta^2 a$

$\Rightarrow a_1, \dots, a_n \in F$ encontrare radici

$h(x) := \gcd(f(x), f'(x))$

$h(x) = \deg A \; f(x) + \beta(x) \cdot f'(x) \in F[x]$

$h(x) \neq 1 \Rightarrow$

$(x-b) k(x) \in E[x]$

$\Rightarrow$ modulo $(x-b) \mid (f(x), f'(x))$

b è zero di f

$f(x) = (x-b) r(x)$

$f'(x) = r(x) + (x-b) r'(x)$

$\Rightarrow (x-b) \mid r(x) \Rightarrow$

$(x-b)^2 \mid f(x)$

$\Leftarrow$

f e f' sono tali

$1 = \alpha(x) \cdot f(x) + \beta(x) f'(x) \quad \in F[x]$

$\exists a \in E$ tale che $(x-a)^2 \mid f(x)$

$f(x) = (x-a)^2 k(x)$

$f'(x) = 2(x-a) k(x) + k'(x)(x-a)^2$

$\Rightarrow$

$1 = 0$ valendo $x = a$ ✗

② Naj bo F polje karakteristike 0 in $F \subseteq E$ E/F

Pokaži: $a \in E$ je k-kratna ničla $f(x) \iff$

$\iff f(a) = f'(a) = \dots = f^{(k-1)}(a) = 0$ in $f^{(k)}(a) \neq 0$

> a je k-kratna ničla $f(x)$ če $(x-a)^k \mid f(x)$ in $(x-a)^{k+1} \nmid f(x)$

$f(x) = f(a) + \frac{f'(a)}{1}(x-a) + \frac{f''(a)}{2!}(x-2)^2 + \dots$

(Lahko kes char $F = 0$)

$\Rightarrow$ predpostavimo a k-kratna ničla

$f(x) = f(a) + \dots \frac{(x-a)^{k-1}}{k-1} f^{(k-1)}(a) + (x-a)^k h(x)$

$*$ neodvisi den.

$f(a) = 0$

$(x-a) \dots (x-a)^k$ so linearno neodvisni

$\Rightarrow$

$f'(a) = \dots = f^{(k-1)}(a) = 0$

$(k-1)!$

$*$

$\Rightarrow$

$f(x) = a \dots f^{(k-1)}(a) = 0$

$f^{(k)}(a) \neq 0$

Opomba. $f(x)$ nerazcepen $(\Leftrightarrow 1 \mid f(x)$ in $f(x) \mid f(x))$

Sl. $(f'(x)) < f(x)$

$\Rightarrow ((f(x), f'(x)) \neq 1 \Leftrightarrow f'(x) \equiv 0)$

(3) Pojasni zakaj $\mathbb{Q}(\sqrt{2})$ je razpadno polje vsakega izmed polinomov

$x^2 - 2$

$3x^3 - 6x$

$x^4 - 3x^2 + 2$

Razpadno polje $f(x)$ je najmanjša razširitev E polja F, da $f(x)$ razpade nad E na linearne faktorje

$\alpha_1, \ldots, \alpha_k$ vse ničle $f(x)$

$E = F(\alpha_1, \ldots, \alpha_k)$

$f(x) = x^2 - 2$ ničle: $\sqrt{2}, -\sqrt{2}$

$\Rightarrow (x - \sqrt{2})(x + \sqrt{2})$

$\mathbb{Q}(\sqrt{2}, -\sqrt{2}) = \mathbb{Q}(\sqrt{2})$

$p(x) = 3x^3 - 6x = 3x(x^2 - 2x) = 3x(x - \sqrt{2})(x + \sqrt{2})$

$\Rightarrow \mathbb{Q}(0, \sqrt{2}, -\sqrt{2}) = \mathbb{Q}(\sqrt{2})$

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

$(x - \sqrt{2})(x + \sqrt{2})(x - 1)(x + 1)$

$\Rightarrow \mathbb{Q}(\sqrt{2})$

(4) Pojasni zakaj je $\mathbb{Q}(\sqrt{2},\sqrt{3})$ razpadno polje polinoma

$x^4-5x^2+6 \in \mathbb{Q}[x]$

RA: $= (x^2-2)(x^2-3) = (x-\sqrt{2})(x+\sqrt{2})(x-\sqrt{3})(x+\sqrt{3})$

$E = \mathbb{Q}(\sqrt{2},-\sqrt{2},\sqrt{3},-\sqrt{3}) = \mathbb{Q}(\sqrt{2},\sqrt{3})$

⑤ Označimo

$\omega = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$ primitivni 3 koren iz enote

Pdvzt: $\mathbb{Q}(\sqrt[3]{2}, \omega)$ delitveno razpadno polje polinoma $x^3 - 2 \in \mathbb{Q}[x]$

Poišči stopnjo razpadnega polja nad $\mathbb{Q}$

$$x^3 - 2 = (x - \sqrt[3]{2})(x^2 + \sqrt[3]{2}x + 2)$$

$\mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2) = \mathbb{Q}(\sqrt[3]{2}, \omega)$

$\leq$ ✓

$2 \quad \omega = \frac{\sqrt[3]{2}\omega}{\sqrt[3]{2}}$

$\mathbb{Q} \subseteq \mathbb{Q}(\omega)$ (2)

stopnja:

$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{Q}(\sqrt[3]{2}, \omega)$ (3, ≤ 2, $\neq 1$) $\Rightarrow$ 6

$\left(\omega + \frac{1}{2}\right)^2 = \left(i\frac{\sqrt{3}}{2}\right)^2 = -\frac{3}{2}$

$p(x) = \left(x + \frac{1}{2}\right)^2 + \frac{3}{2}$

(6) Pokaži

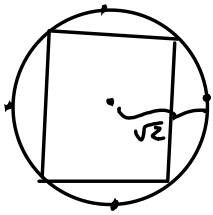
a) $\mathbb{Q}(i)$ je razpadno polje polinoma $x^4+4 \in \mathbb{Q}[x]$

b) $\mathbb{Q}(\sqrt[4]{2}, i)$ je razpadno polje polinoma $x^4+2 \in \mathbb{Q}[x]$

c) $\mathbb{Q}(\sqrt{2}, i)$ razpadno polje $x^4+1 \in \mathbb{Q}[x]$

---

a) $x^4+4i^2 = (x^2+2i)(x^2-2i) = (x-(1+i))(x-(-1+i))(x-(-1-i))(x-(1-i))$



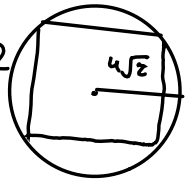
$x^4 = -4$

$\sqrt{2}\frac{\sqrt{2}}{2}(1+i)\cdot\sqrt{2}\frac{\sqrt{2}}{2}(-1+i)$

$\sqrt{2}\frac{\sqrt{2}}{2}(-1-i)\sqrt{2}\frac{\sqrt{2}}{2}(1-i)$

Razpadno polje: $\mathbb{Q}(i,-i) = \mathbb{Q}(i)$

b) x^4+2



$x^4 = -2$

$x^4+2 = \frac{\sqrt[4]{2}\sqrt{2}}{2}(1+i) = \frac{\sqrt[4]{2}}{\sqrt[4]{4}} = \frac{1}{\sqrt[4]{2}}$

$x^4+2 = \left(x-\frac{1}{\sqrt[4]{2}}(1+i)\right)\left(x-\frac{1}{\sqrt[4]{2}}(1-i)\right)\ldots$

$\mathbb{Q}\left(\frac{1}{\sqrt[4]{2}}(1+i),\ldots\right) \supseteq$ ✓

$i: \frac{1}{\sqrt[4]{2}}(1+i)-\frac{1}{\sqrt[4]{2}}(-1+i) = \frac{1}{\sqrt[4]{2}}(2i)$

$\frac{1}{\sqrt[4]{2}} = \frac{1}{\sqrt[4]{2}}\left((1+i)+(1-i)\right) = \frac{2}{\sqrt[4]{2}}$

$i \Rightarrow$ ✓ $\cdot\sqrt[4]{2}$ ✓ $:2$

c) $x^4+1 = \left(x-\frac{\sqrt{2}}{2}(1+i)\right)^{\alpha}\left(x-\frac{\sqrt{2}}{2}(1-i)\right)^{\beta}\left(x-\frac{\sqrt{2}}{2}(-1+i)\right)^{\gamma}\left(x-\frac{\sqrt{2}}{2}(-1-i)\right)^{\delta}$

$\subseteq$ ✓

$\sqrt{2}$: $\alpha+\beta = \frac{\sqrt{2}}{2}(2) = \sqrt{2}$

i: $\frac{\sqrt{2}}{2}(\alpha+\gamma = \frac{\sqrt{2}}{2}(2i)\cdot\frac{\sqrt{2}}{2} = i$

$f(x) \in F[x]$ st $(f(x)) = n$

E - razpadno polje $f(x)$

Potem: $[E:F] \leq n!$

in $n \mid [E:F]$ če $f(x)$ nerazcepen

$x^3 - 2$: $[E:F] \leq 6$

$3 \mid [E:F]$

$E = F(a_1, \ldots, a_k)$ a_i niče $k \leq n$

$F \subseteq F(a_1) \subseteq \ldots\ldots \subseteq F(a_k) \leq n!$

$\leq n$ $\leq (n-1)$ $\ldots$ $--$

Strogo manjša moč polinoma

Ker smo ena niče že vzeli a_1

$f(x) = (x - a_1)\, g(x)$ nad $F(a_1)$

$\text{st } g(x) = n - 1$

Če ni razcepen $\Rightarrow$ ~~E~~ $F \subsetneq F(a_1)$

n

Izmeda 15 minut

$\Leftarrow$

Denimo da F ni algebraično zaprto

$\exists f(x)$ ki nima nicle v F

Naj bo a ta nicla. $F(a)$ najbo razširitev

$a \in F(a) \Rightarrow F(a) \neq F$

f ima stopnjo $n \Rightarrow [F(a):F] \leq n$

ker je konč

③

Naj bo $E \supsetneq \mathbb{R}$ končna razširitev realnih števil

Pokaži, da je $E \simeq \mathbb{C}$

Na tabli:

(4.)

Oglejmo si polinom

$f(x) = x^2+x+1 \in \mathbb{Z}_2[x]$

je nerazcepen nad $\mathbb{Z}_2[x]$

$\mathbb{Z}_2[x]$.

$I = (x^2+x+1)$

$F = \mathbb{Z}_2[x] / (x^2+x+1)$

x^2+x+1 je maksimalen ideal (ker je polinom nerazcepen)

((x^2+x) ni maksimalen ker $x^2+x = x(x+1)$ Torej $(x) \supseteq (x^2+x)$ — vsi večkratniki x-a, večkratnik tega)

elementi tega polja so $p(x) + I$

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

$st(p(x)) \geq 2$

$p(x) = \underbrace{\alpha(x) \cdot (x^2+x+1)}_{\in I} + g(x)$

$st \leq 1$ (sestavljajo ga samo konstante in linearni polinomi)

$\Rightarrow F = \mathbb{Z}_2[x] / (x^2+x+1) = \{0+I, 1+I, x+I, x+1+I\}$

$= \{0, 1, \bar{x}, \bar{x}+1\} \supseteq \mathbb{Z}_2$

$\bar{x}$ je ničla x^2+x+1 nad F

$\bar{x}^2 + \bar{x} + 1 = (x+I)^2 + (x+I) + 1 + I =$

$= (x^2+x+1) + I = I = 0 + I$

+	0	1	$\bar{x}$	$\bar{x}+1$
0	0	1	$\bar{x}$	$\bar{x}+1$
1	1	0	$\bar{x}+1$	$\bar{x}$
$\bar{x}$	$\bar{x}$	$\bar{x}+1$	0	1
$\bar{x}+1$	$\bar{x}+1$	$\bar{x}$	1	0

·	0	1	$\bar{x}$	$\bar{x}+1$
0	0	0	0	0
1	0	1	$\bar{x}$	$\bar{x}+1$
$\bar{x}$	0	$\bar{x}$	$\bar{x}+1$	1
$\bar{x}+1$	0	$\bar{x}+1$	1	$\bar{x}$

$\bar{x}^2 + 2\bar{x} + 1$

$\bar{x} \cdot \bar{x} = x^2 + I$

$x^2 : (x^2+x+1) = 1$

$-x^2 - x - 1$

$-x - 1$

$x+1$

x^2+1

Pokaži, da je F (prejšnja stran)

Razpadna polje $x^2+x+1 \in \mathbb{Z}_2[x]$

$\bar{x}$ je nicla

Najdi manjka use nicle

Kozhadi $\bar{x}$ in $\bar{x}+1$

$f(\bar{x}+1) = \bar{x}+\bar{x}+1+1 = 0$

Polinom je stopnje 2, torej ima največ dve nicli $\Rightarrow$ natančno use nicle $\Rightarrow$

$\mathbb{Z}_2(\bar{x}, \bar{x}+1)$ je razpadno polje

$\mathbb{Z}_2(\bar{x}) = F$ po definiciji F

Naj bo $g(x) \in \mathbb{Z}_p[x]$ nerazcepen polinom stopnje n

Potem je $GF(p^n) = \dfrac{\mathbb{Z}_p[x]}{(g(x))}$

končno polje s p^n elementi

2) pokaži $g(x) \mid x^{p^n} - x$

> $GF(p^n)$ je razpadno polje $x^{p^n} - x$
>
> $$x^{p^n} - x = \prod_{a \in GF(p^n)} (x-a)$$

Primer:

$\{a = \bar{x}\}$

$GF(2^2) = \{0, 1, a, a+1\}$

$x^4 - x = x(x-1)(x-a)(x-(a+1))$ nad F

x^2+x+1

$x^4 - x = x(x-1)(x^2+x+1)$ nad $\mathbb{Z}_2$

1)

Elementi F so oblike: $p(x)+I$

$st(p(x)) < n$

$$a_0 + a_1 x + \dots + a_{n-1} x^{n-1} + I$$

so elementi $\Rightarrow |F| = p^n$

po teoriji: $F \cong GF(p^n)$ ∎

2) $\bar{x}$ je ničla $\overset{\text{vsr}}{\forall}\ g(x+I) = g(x) + I = I = 0$

$$x^{p^n} - x = \prod_{a \in F} (x-a)$$

$\bar{x}$ je ničla v F, ki [illegible] od $\mathbb{Z}_p[x]$ in $x^{p^n}-x$

če $g(x) \nmid x^{p^n}-x$ pdem sta si tuji

$\exists\, k(x), l(x) \in \mathbb{Z}_p[x]$ da $g(x)k(x) + l(x)\cdot(x^{p^n}-x) = 1$

vstavimo $\bar{x}$

$$\underset{0}{g(\bar{x})}\,k(x) + l(x)\,\underset{0}{(\bar{x}^{p^n} - \bar{x})} = 1$$

$$0 = 1 \quad \times$$

Poleti

a) $GF(8) = \frac{\mathbb{Z}_2[x]}{(x^3+x+1)}$

b) $GF(9) = \frac{\mathbb{Z}_3[x]}{(x^2+1)}$

c) $GF(16) = \frac{\mathbb{Z}_2[x]}{(x^4+x+1)}$

3/ Razčleni kubo $x^8 - x$ kot produkt polinomov iz $\mathbb{Z}_2[x]$

$GF(8)$ je razpadno polje $x^8 - x$

vse skupaj iz prejšnje naloge, samo nerazcepnost moramo preveriti

a) x^3+x+1 če je razcepen ima ničlo

0: $0+0+1 = 1$

1: $1+1+1 = 1$ torej nima ničle

$I = x^3+x+1$

$f(x) + I = \overline{f(x)}$

$(\overline{x^2+1})^{-1}$

$(x^2+1, x^3+x+1) = 1$

$1 = s(x)(x^2+1) + \underbrace{t(x)(x^3+x+1)}_{\in I}$ v $\mathbb{Z}_2[x]$

v $\frac{\mathbb{Z}_2[x]}{I}$ $\quad 1 = \overline{s(x)} \cdot \overline{x^2+1}$

c) Vemo od prej da je nerazcepen potemtakem inverz

DN

$x^6 - x = x(x^5 - 1) = x(x-1)(x^4 + \dots + 1)$

$2(4) \mid x^{p^n} - x$

↑ 3 nerazcepen (ker je $n=3$)
velma iz a nalogo 3

$(x^6 + x^5 + x^4 + x^3 + x + 1) : (x^3 + x + 1) = x^2 + x^2$

$-x^6 - x^4 - x^3$

$x^5 + x^4 + x + 1$

$-x^5 - x^3 - x^2$

$x^4 - x^3 - x^2 + x + 1$

Ker ima $x^6 - x$ samo različne ničle in se
e deliteli je še ena ničla

$x^6 - x = x(x-1)(x^3 + x + 1)(x^3 + x^2 + 1)$