ALGEBARSKE STRUKTURE

POLUGRUPE I GRUPE

- binarna operacija na X: $X \times X \to X$ (npr. $x+y$, $x-y$)
- binarna operacija je asocijativna ako vrijedi

$$x \circ (y \circ z) = (x \circ y) \circ z$$

- polugrupa - skup X s asocijativnom binarnom operacijom

- homomorfizam polugrupa $(X, \circ)$ i $(Y, \cdot)$ je preslikavanje $f: X \to Y$ za koje vrijedi

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

- $(X, \cdot)$ polugrupa; neutralni element je $e \in X$ t.d.

$$x \cdot e = e \cdot x = x \quad , x \in X$$

jedinstven!

- monoid - polugrupa koja ima neutralni element

- grupa - monoid u kojem za svaki x postoji x^{-1} t.d.

$$x^{-1} \cdot x = x \cdot x^{-1} = e$$

jedinstven!

- dokaz da je nešto grupa s obzirom na neku binarnu operaciju: pokazati zatvorenost, asocijativnost, postojanje neutralnog elementa i inverza

- abelova (komutativna) grupa : $x \cdot y = y \cdot x$
- $\mathbb{Z}_m = \{0, 1, 2, \ldots, m-1\}$ ostatci pri dijeljenju s m
- homomorfizam grupa = homomorfizam polugrupa

- $S \neq 0$, $B(S)$ - skup svih bijekcija (permutacija) $S \to S$, grupa s obzirom na kompoziciju f-ja

  $S = \{1, 2, \ldots, n\} \longrightarrow B(S) = S_n$, simetrična grupa stupnja n

  $|S_n| = n!$
- permutacija $f : \begin{pmatrix} 1 & 2 & \cdots & n \\ f(1) & f(2) & \cdots & f(n) \end{pmatrix}$

  npr.

  $S_3 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \cdots \right\}$ $3! = 6$

  prvo desni: 1 ide u 3, 3 ide u 3

  S_n nije abelova, jer

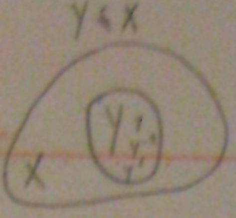
  $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \neq \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$ $(23) \neq (13)$

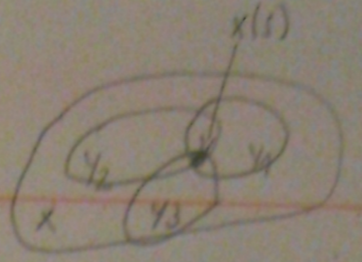
- permutacija se može prikazati kao produkt disjunktnih ciklusa $(i_1 i_2 \ldots i_r)$, npr.

  $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 5 & 2 & 8 & 1 & 6 & 7 & 4 \end{pmatrix} = (1\ 3\ 2\ 5)(4\ 8)(6)(7) = (1325)(48)$

- u ciklusu nemamo duplice; cikluse duljine 1 ne pišemo
- ciklus duljine 2 - transpozicija
- $\forall$ permutacija se može napisati kao produkt transpozicija; rastav nije jedinstven, ali je uvijek iste parnosti $\longrightarrow$ parnost permutacije

$(1325)(48) = (13)(32)(25)(48)$





- Y je podgrupa od X ako: $Y \subseteq X$, $y^{-1} \in Y$, $yy' \in Y$; oznaka: $Y \leq X$
  - dokaz: dokazati da je $yy^{-1} \in Y$
- podgrupa generirana skupom S: $S \subseteq X$, presjek svih podgrupa od X koje sadrže S; oznaka: $X(S)$

- ciklička grupa - grupa generirana s jednim elementom
- provjera da li je el. generator - da li sa njim možemo dobiti sve el. grupe!

- X grupa, $Y \leq X$, $a \in X$
- red podgrupe - njen kardinalni br.
- red elementa a - red podgrupe $X(a)$ generirane el. a, tj. najmanji r t.d je $a^r = e$, $e \in X$

može se „kratiti"

- određivanje reda el. u $(\mathbb{Z}_n, +_n)$: $el \cdot r \equiv 0 \pmod{n} \rightarrow r$ je red

ili potenciramo $(\mathbb{Z}_n^*, \cdot_n)$: $el^r \equiv 1 \pmod{n}$

- provjera: dodajemo el. i gledamo koje sve ostatke dobivamo; br. različitih ostataka = red elementa

- injekcija - razl. x-evi u razl. y-one
- surjekcija - svi y-oni pogođeni
- bijekcija - injekcija i surjekcija; svaki x ima svoj y, svaki y ima svoj x

- relacija $\sim$: $Y \leq X$ $x \sim x'$ akko $\exists\, y \in Y$ t.d. $x = x'y$
  klase ekvivalencije označavamo sa $[x]$
- lijeva klasa grupe X po podgrupi Y: $[x] = xY = \{xy : y \in Y\}$
- lijevi kvocijentni skup grupe X po podgrupi Y: X/Y;
  kardinalni br. skupa X/Y : $[X:Y]$; vrijedi
  $$|X| = [X:Y]\,|Y|$$
- desna klasa: Yx ; $|Yx| = |Y| = |xY|$

- podgrupa $Y \leq X$ je normalna ako je $xY = Yx$; oznaka: $Y \triangleleft X$

- ako je grupa X abelova, onda je svaka njezina podgrupa normalna ; trivijalne normalne podgrupe: $\{e\}$ i X
- grupa X je prosta ako nema netrivijalnih normalnih podgrupa
- dokaz da je $Y \leq X$: ab^{-1} mora biti $\in Y$
- dokaz da je $Y \triangleleft X$: aba^{-1} mora biti $\in Y$ $(b \in X!)$

- $f : X \to Y$ homomorfizam ; jezgra homomorfizma f je
  $\mathrm{Ker} f = f^{-1}(e_Y) \subseteq X$; slika homomorfizma f je $\mathrm{Im} f = f(X) \subseteq Y$
- vrijedi $\mathrm{Ker} f \leq X$, $\mathrm{Im} f \leq Y$; $\mathrm{Ker} f \triangleleft X$
- f je monomorfizam ako je f injekcija;
  epimorfizam ako je f surjekcija;
  izomorfizam ako je f bijekcija

- jesu li grupe izomorfne? - pronaći f-ju iz jedne u drugu grupu koja je homomorfizam i bijekcija

- Z_n - sve operacije su modulo n

VERIŽNI RAZLOMAK

- racionalna aproksimacija realnog broja:

$$\alpha = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \dots}}}$$

zapis: $[a_0; a_1, a_2, a_3 \dots]$

jednostavni verižni razlomak - konačan ako je α racionalan

- $a_0, a_1 \dots$ - parcijalni kvocijenti:

$a_0 = [\alpha]$ $\quad \alpha = a_0 + \frac{1}{\alpha_1}$

$a_1 = [\alpha_1]$ $\quad \alpha_1 = a_1 + \frac{1}{\alpha_2}$ ... dok je $a_k \neq \alpha_k$

* ako je $\alpha \in \mathbb{Q}$, tj. $\alpha = \frac{m}{n}$, parcijalni koef. su kvocijenti iz Euklidovog algoritma za m i n

i	-1	0	1	2	$\dots$
a_i	parcijalni kvocijenti				
p_i	1	0			
q_i	0	1			

ili tablica — p_i, q_i } računaju se kao kod Euklida, samo sa +

ručno se računaju nakon rastava

- konvergente verižnog razlomka: → razlomak raspisan do k članova

$$\frac{p_k}{q_k} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \dots + \cfrac{1}{a_k}}} = [a_0; a_1, a_2, \dots, a_k]$$

kvadratna iracionalnost — period

- $\sqrt{d}$ ima razvoj oblika $[a_0; \overline{a_1, a_2, \dots, a_{l-1}, 2a_0}]$
- vrijedi palindromno svojstvo: $a_1 = a_{l-1}$, $a_2 = a_{l-2}$ ...
- razvoj $\sqrt{d}$ u verižni razlomak:

$$\alpha = \sqrt{d} = \frac{s_0 + \sqrt{d}}{t_0}, \quad d \neq \square$$

$$s_0 = 0, \; t_0 = 1, \; a_0 = \lfloor \sqrt{d} \rfloor$$

$$a_i = \left\lfloor \frac{s_i + a_0}{t_i} \right\rfloor \qquad s_{i+1} = a_i t_i - s_i \qquad t_{i+1} = \frac{d - s_{i+1}^2}{t_i}$$

kraj kada dobijemo $a_k = 2a_0$

POLJA LOL :D

- dokaz da je nešto polje: zatvorenost s obzirom na $-$, $\cdot$ i $^{-1}$
- matrice čine polje izomorfno polju $(\mathbb{C}, +, \cdot)$:
  1. provjeriti jesu li matrice prsten (zatvorenost s obz. na $-$ i $\cdot$)
  2. naći bijekciju sa matrica na $\mathbb{C}$ i dokazat da je homomorfizam s obzirom na $+$ i $\cdot$ (zatvoren)

PRSTENI I POLJA, IPAK.

- prsten - skup $\mathbb{R}$ sa binarnim operacijama + i · za koje vrijedi: (R, +) je abelova grupa
  (R, ·) je polugrupa (asocijativna)
  distributivnost · s obzirom na +
  dokaz: zatvorenost s obzirom na − i ·

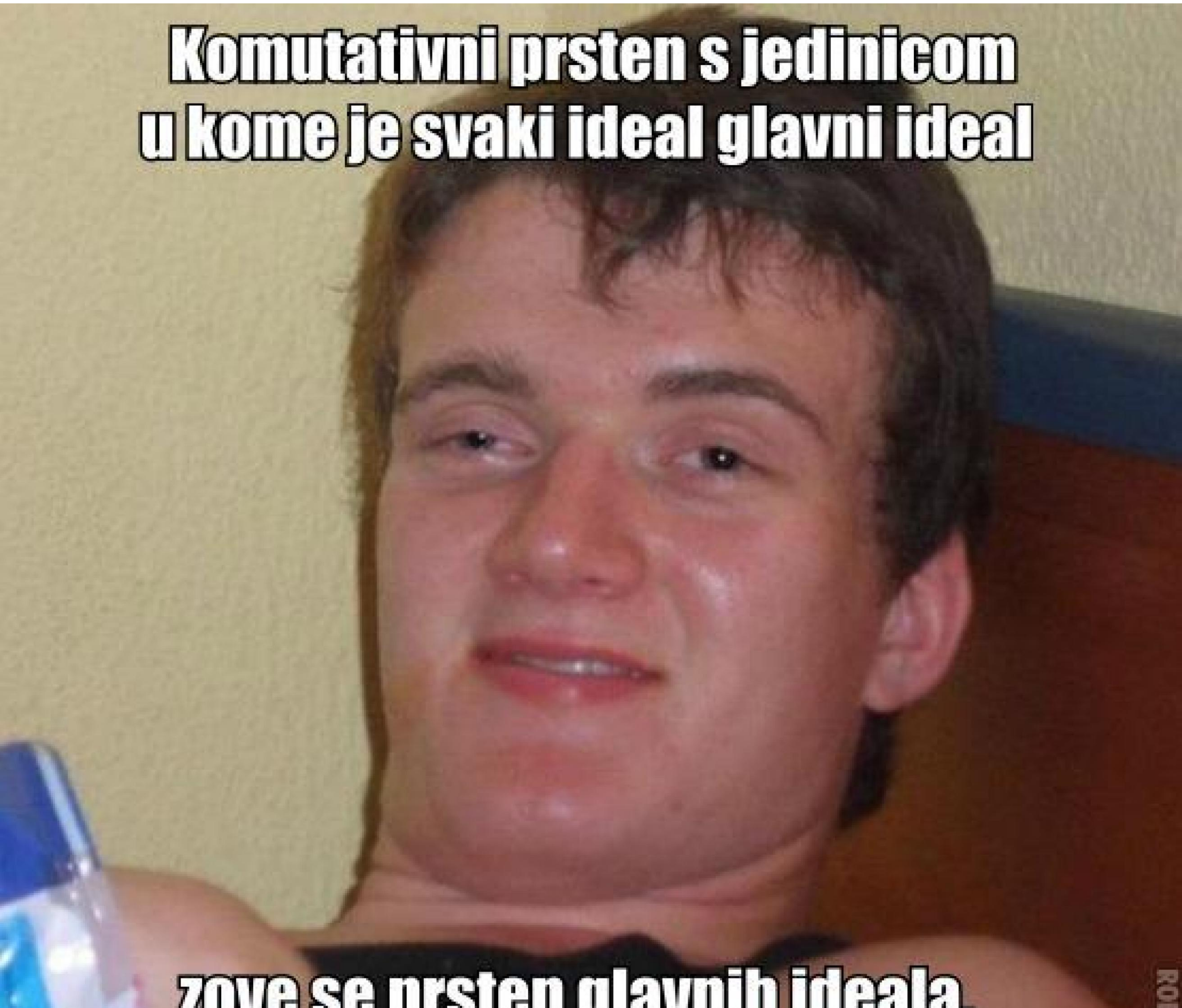
- homomorfizam prstena: $(R, +, \cdot)$ i $(P, +, \cdot)$ prsteni
  preslikavanje $f: R \to P$ za koje vrijedi
  $f(x+y) = f(x) + f(y)$ i $f(xy) = f(x)f(y)$
  provjera: →

- potprsten - $P \subseteq R$, P je prsten s obzirom na operacije iz R

- ideal - potprsten I za koji vrijedi $xI \subseteq I$ i $Ix \subseteq I$, $\forall x \in R$

- polje - zatvoreno s obzirom na − i $^{-1}$

- polinom ireducibilan nad $\mathbb{Z}_n$ - ne može se rastaviti na nultočke koje su u $\mathbb{Z}_n$ $g(a) \neq 0$, $a = \{0, 1, \dots, n-1\}$


Komutativni prsten s jedinicom
u kome je svaki ideal glavni ideal
zove se prsten glavnih ideala.