

### Ciklične grupe

Žano Križofanič

Grupa  $G$  je ciklična ako je  $G$  generisana jednim elementom, tj. postoji  $a \in G$  t.d.  $G = \langle a \rangle$ .

- Primeri
- 1°  $\mathbb{Z} = (\mathbb{Z}, +, ;, 0) = \langle 1 \rangle$ ,  $\mathbb{Z} = \{ \dots, -2, -1, 0, 1, 2, \dots \}$
  - 2°  $\mathbb{Z}_n = (\mathbb{Z}_n, +_n, \cdot, 0) = \langle 1 \rangle$ ,  $\mathbb{Z}_n = \{ 0, 1, \dots, n-1 \}$ ,
  - 3°  $C_n = \{ x \in \mathbb{C} / x^n = 1 \} = \langle \varepsilon \rangle$ ,  $\varepsilon = e^{\frac{2\pi i}{n}} = \cos \frac{2\pi}{n} + i \sin \frac{2\pi}{n}$   
 $\mathbb{C}$  = grup kompleksnih brojeva  
 $C_n = (C_n, \cdot, \cdot, 1)$ .

Teorema 1. Neka je  $G = \langle a \rangle$ .

- a) Ako je  $\text{red}(a) = n$ , onda  $G = \{ 1, a, \dots, a^{n-1} \}$ ; za  $0 \leq i < j < n$ ,  $a^i \neq a^j$ .
- b) Ako je  $\text{red}(a) = \infty$ , onda  $G = \{ \dots, a^{-2}, a^{-1}, 1, a, a^2, \dots \} = \{ a^i / i \in \mathbb{Z} \}$ ,  
 $i \neq j \Rightarrow a^i \neq a^j$ .

Dokaz a) Neka je  $d \in \mathbb{Z}$ . Tada postoji  $q, r \in \mathbb{Z}$ , t.d.

(1)  $d = nq + r$ ,  $0 \leq r < n$ .

S druge strane  $\langle a \rangle = \{ a^d / d \in \mathbb{Z} \}$  pa prema (1)

$G = \langle a \rangle = \{ a^i / 0 \leq i < n \} = \{ 1, a, a^2, \dots, a^{n-1} \}$ .

Ako  $0 \leq i < j < n$  onda  $a^i \neq a^j$ , jer u suprotnom  $a^{j-i} = 1$ ,  $0 < j-i < n$ , što je # prema  $\text{red}(a) = n$ .

- b) Neka su  $d, \beta \in \mathbb{Z}$ ,  $d < \beta$ . Ako  $a^d = a^\beta$ , onda  $a^{\beta-d} = 1$ ,  $\beta-d \neq 0$ , # prema pretpostavci  $\text{red}(a) = \infty$ .

Teorema 2. Neka su  $G, H$  ciklične grupe istog reda. Tada  $G \cong H$ .

Dokaz Neka su  $G = \langle a \rangle$ ,  $H = \langle b \rangle$ .

a) Ako je  $\text{red}(a) = \text{red}(b) = n$  onda je  $f = \begin{pmatrix} 1 & a & a^2 & \dots & a^{n-1} \\ 1 & b & b^2 & \dots & b^{n-1} \end{pmatrix}$

$f: G \cong H$ .

Zaista,  $f$  je 1-1 i na jer  $G = \{ 1, \dots, a^{n-1} \}$ ,  $H = \{ 1, \dots, b^{n-1} \}$  i

$|G| = |H| = n$ . Takođe,  $f$  je homomorfizam:

za  $a^i, a^j \in G$ , neka je  $k = \text{rest}(i+j, n) = i +_n j$ . Tada

$a^i \cdot a^j = a^{i+j} = a^{k+n} = a^k = a^{i+j}$ , pa  
 $f(a^i \cdot a^j) = f(a^{i+j}) = f(a^k) = b^k = b^{i+j} = b^i \cdot b^j = f(a^i) f(a^j)$ .

- b)  $\text{red}(a) = \text{red}(b) = \infty$ . Tada  $f: G \cong H$ , gde

$f: a^d \mapsto b^d, d \in \mathbb{Z}$ .

Davle sve ciklične grupe su:

$C_1, C_2, C_3, \dots$  (konacne ciklične grupe)  
 $C_\infty$  (beskonacna ciklična grupa)

i stavite  $C_n \cong (\mathbb{Z}_n, +, 0)$ ,  $C_\infty \cong (\mathbb{Z}, +, 0)$ .

Teorema 3 a) Homomorfna slika ciklične grupe je ciklična grupa.

b) Podgrupa ciklične grupe je ciklična grupa.

c) Neka su  $m, n \in \mathbb{N}^+$ . Tada  $C_{mn} \cong C_m \times C_n$  ako  $(m, n) = 1$ .

Dokaz a) Neka je  $G = \langle a \rangle$  i  $h: G \xrightarrow{h} H$ , tj.  $H = hG$ .

Tada  $H = \langle h(a) \rangle$ .

b) Neka je  $G = \langle a \rangle$  i  $H < G$ . P.P.  $\text{red}(H) > 1$ . Neka je  $k \in \mathbb{N}^+$  najmanji (pozitivan prirodan broj) takav da  $a^k \in H$ . Kako je  $H < G$  to  $\langle a^k \rangle \subseteq H$ . Neka je  $x \in H$ . Tada postoji  $i \in \mathbb{Z}$  d.d.  $x = a^i$ . Neka su  $q, r \in \mathbb{Z}$  d.d.

$$i = k \cdot q + r, \quad 0 \leq r < k.$$

Tada  $a^r = a^i \cdot (a^k)^{-q}$  pa  $a^r \in H$  jer  $a^i, a^k \in H$ .

S obzirom na izbor broja  $k$ , sledi da je  $r = 0$ , pa

$x = a^i = (a^k)^q$  tj.  $x \in \langle a^k \rangle$ . Davle  $H = \langle a^k \rangle$ ,

tj.  $H$  je ciklična.

c) Neka su  $m, n \in \mathbb{N}^+$ ,  $(m, n) = 1$ . Prema teoremi o razlaganju prostene  $\mathbb{Z}_{mn}$ , važi  $\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n$ , tj.

$$(\mathbb{Z}_{mn}, +_{mn}, '0, 1) \cong (\mathbb{Z}_m, +_m, '0, 1) \times (\mathbb{Z}_n, +_n, '0, 1)$$

$$\text{pa } (\mathbb{Z}_{mn}, +_{mn}, 0) \cong (\mathbb{Z}_m, +_m, 0) \times (\mathbb{Z}_n, +_n, 0).$$

Davle  $C_{mn} \cong C_m \times C_n$  jer  $C_{mn} \cong (\mathbb{Z}_{mn}, +_{mn}, 0)$ ,  $C_m \cong (\mathbb{Z}_m, +_m, 0)$ .

Pretpostavimo  $(m, n) \neq 1$ , tj.  $\text{red} = (m, n)$ ,  $d > 1$ . Neka je

$k = \frac{mn}{d}$ . Dalje,  $C_m \times C_n = \langle \bar{a}, \bar{b} \rangle$ , gde  $\bar{a} = (a, 1)$ ,  $\bar{b} = (1, b)$

i  $\text{red}(a) = m$ ,  $\text{red}(b) = n$ . Tada

$$a^k = a^{m \cdot \frac{n}{d}} = (a^m)^{\frac{n}{d}} = 1 \quad \text{i slično } b^k = b^{n \cdot \frac{m}{d}} = (b^n)^{\frac{m}{d}} = 1, \text{ pa}$$

za paritetan  $(a^i, b^j) \in C_m \times C_n$ ,

$$(a^i, b^j)^k = ((a^k)^i, (b^k)^j) = (1, 1), \text{ tj. } \forall x \in C_m \times C_n,$$

$\text{red}(x) \leq k < mn$ , pa  $C_m \times C_n \neq C_{mn}$ . ▣

Teorema 4. Neka su  $n, k, u \in \mathbb{N}^+$  i pretpostavimo da  $k | n$ . Tada postoji tačno jedna podgrupa  $H < \mathbb{C}_n$ ,  $\text{red}(H) = k$ .

Dokaz Neka je  $\mathbb{C}_n = \langle a \rangle$ . Tada  $H = \langle a^{\frac{n}{k}} \rangle$  je reda  $k$  i  $H < \mathbb{C}_n$ .  
Dokažimo da je  $H$  jedina podgrupa reda  $k$  grupe  $\mathbb{C}_n$ . Neka je  $H' < \mathbb{C}_n$ ,  $|H'| = k$ . Prema dokazu Teorema 3b, postoji  $i \in \mathbb{N}^+$  ( $k$  uzlov  $k > 1$ ; za  $k = 1$  tvrdenje trivijalno sledi) t.d.  $H' = \langle a^i \rangle$ , i pri tome  $i$  je najmanji pozitivni broj na dem. osloncu. Kako je  $\text{red}(H') = k$ , to  $a^{ik} = 1$  pa  $ik = 0 \pmod n$ , tj.  $n | ik$ . Kako  $k | n$ , za h.k.  $i$  je najmanji n. broj da  $n | ik$ , to  $ik = n$ , pa  $i = \frac{n}{k}$ , tj.  $H' = \langle a^{\frac{n}{k}} \rangle = H$ .

Teorema 5 Neka je  $S = \{b \in \mathbb{C}_n \mid \mathbb{C}_n = \langle b \rangle\}$ . Tada  $|S| = \varphi(n)$ , gde je  $\varphi(n)$  Eulerova f-ija.

Dokaz Neka je  $\mathbb{C}_n = \langle a \rangle$ , i neka je  $b \in S$ . Tada  $b = a^i$  za neki  $i \in \mathbb{Z}_n \setminus \{0\}$ . Kako  $\mathbb{C}_n = \langle b \rangle$  to za neki  $k$ ,  $b^k = a$  tj.  $a^{ik} = a$ , odakle  $ik = 1 \pmod n$  pa  $i \in \Phi(n)$  (jer je  $i$  jednoka prstena  $\mathbb{Z}_n$ ).  
S druge strane, neka je  $i \in \Phi(n)$ . Tada za neki  $k \in \mathbb{Z}_n$ ,  $ik = 1 \pmod n$ , pa  $ik = 1 + dn$  za neki  $d \in \mathbb{Z}$ . Onda  $a^{ik} = a^{1+dn} = a^1 \cdot a^{dn} = a$ , pa za proizvoljno  $x \in \mathbb{C}_n$  za odgovarajuće  $j \in \mathbb{N}$  imamo  
 $x = a^j = (a^{ik})^j = (a^i)^{kj}$  tj.  $x \in \langle a^i \rangle$ , pa  $\mathbb{C}_n = \langle a^i \rangle$ .  
Dakle,  $\mathbb{C}_n = \langle a^i \rangle$  ako i  $i \in \Phi_n$ , pa  $|S| = |\Phi(n)| = \varphi(n)$ .  $\square$

Odatde imamo sledeće zanimljive primere:

1° Neka je  $d | n$ ,  $S_d = \{x \in \mathbb{C}_n \mid \text{red}(x) = d\}$ . Prema Lagranževom teoremi,  $\mathbb{C}_n = \bigcup_{d|n} S_d$  i to je disjunktna unija, pa

$$n = |\mathbb{C}_n| = \sum_{d|n} |S_d|.$$

Ako je  $H_d < \mathbb{C}_n$  podgrupa (jedina prema Teoremu 4) grupe  $\mathbb{C}_n$  reda  $d$ , to je  $S_d$  skup generatora grupe  $H_d$  pa prema Teoremu 5,

$$n = \sum_{d|n} \varphi(d).$$

Prema teoremi inverzije, onda  $\varphi(n) = \sum_{d|n} \mu(d) \frac{n}{d} = n \sum_{d|n} \frac{\mu(d)}{d}$ .

2°  $\text{Aut } \mathbb{C}_n \cong \Phi_n$ .  
Zaista,  $f \in \text{Aut } \mathbb{C}_n$  u potpunosti je određena vrednošću  $f(a)$ , gde  $\mathbb{C}_n = \langle a \rangle$ , jer  $f(a^i) = f(a)^i$ . S druge strane ako  $\mathbb{C}_n = \langle a \rangle$  onda  $f^{-1}(\mathbb{C}_n) = \langle fa \rangle$  pa je  $fa$  generator grupe  $\mathbb{C}_n$ .

Takođe, ako  $P_n = \langle a \rangle$  onda za  $K \in \Phi(n)$ , razlikovane  $f: C_n \rightarrow C_n$  definišamo sa

$$f(a^i) = a^{ki}, \quad i=0, 1, \dots, n-1$$

jesto automorfizam grupe  $P_n$ :

$$\begin{aligned} f(a^i \cdot a^j) &= f(a^{i+j}) = f(a^{i+j}) = a^{k(i+j)} = a^{k \cdot i + k \cdot j} \\ &= a^{k \cdot i} \cdot a^{k \cdot j} \end{aligned}$$

ti:  $f$  je homomorfizam, a da je 1-1 sledi iz empirije da je  $f(C_n) = C_n$ .

Daube,  $\text{Aut } C_n = \{ f_k \mid k \in \Phi(n) \}$ , gde je  $f_k(a) = a^k$ .

Neka je  $F: \Phi(n) \rightarrow \text{Aut } C_n, F: k \mapsto f_k, k \in \Phi(n)$ .

Čade: a)  $F$  je 1-1 i na (prema metodi)

b)  $F: \Phi(n) \rightarrow \text{Aut } C_n$ .

Neka su  $l, k \in \Phi(n)$  i neka je  $s = l \cdot k$ .

$$\text{Čade } (f_k \circ f_l)(a) = (a^l)^k = a^{lk} = a^{l \cdot k} = f_s(a)$$

pa  $f_s = f_k \circ f_l$  jer se  $f_s$  i  $f_k \circ f_l$  podudaraju na generatoru  $a$ .

$$a^{lk} = a^{l \cdot k} \text{ jer } a^{l \cdot n \cdot k} = a^{lk + ln} = a^{lk} \cdot a^{ln} = a^{lk} \cdot 1$$

Daube,  $F$  je 1-1 i na homomorfizma grupe  $\Phi(n)$  na grupu

$$\text{Aut } C_n \text{ pa } \Phi(n) \cong \text{Aut } C_n.$$

Primer Odrediti grupu  $\text{Aut } C_{12}$ .

Rešenje  $\text{Aut } C_{12} \cong \Phi(12) = \Phi(3 \cdot 4) \cong \Phi(3) \times \Phi(4) \cong C_2 \times C_2$ .

Zadatak Odrediti  $\text{Aut } C_{100}$

Zadatak Dokazati da  $C_\infty \times C_\infty \not\cong C_\infty$  i napišite  $C_\infty^m \cong C_\infty^n$  ako  $m=n$ .

Zadatak Da li ulaza cikličnih grupa abrajne algebarski varijetet? Objasnite.

Zadatak Dokazati da je svaka ciklična grupa homomorfnu sline grupe  $C_\infty$ .

# Abelove grupe

April 2000  
Zeno Mujajlovic

2-1

Grupa  $G$  je Abelova ako je komutativna, tj. ako za sve  $x, y \in G$ ,  
 $x \cdot y = y \cdot x$ . U slučajju Abelovih grupa često se koristi aditivna

notacija:

## multiplikativna notacija

$$G = (G, \cdot, ^{-1}, 1)$$

$$x \cdot y = z$$

$$y = x^{-1}, \quad z = x y^{-1}$$

$$y = x^n, \quad n \in \mathbb{Z}$$

$$y = x_1^{d_1} x_2^{d_2} \dots x_k^{d_k}$$

$$y = \prod_{i=1}^n x_i$$

## aditivna notacija

$$A = (A, +, -, 0)$$

$$x + y = z$$

$$y = -x, \quad z = x - y$$

$$y = nx, \quad n \in \mathbb{Z}$$

$$y = d_1 x_1 + d_2 x_2 + \dots + d_k x_k$$

$(d_1, \dots, d_k \in \mathbb{Z})$

$$y = \sum_{i=1}^n x_i$$

## Idejaliteti koji važe u svim grupama

$$(x^m)^n = x^{mn}$$

$$(m, n \in \mathbb{Z})$$

$$n(mx) = (mn)x$$

$$x^{m+n} = x^m \cdot x^n$$

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

$$(m+n)x = (mx) + (nx)$$

$$-(x+y) = (-y) + (-x)$$

odnosno u slučajju Ab. grupe

$$-(x+y) = (-x) + (-y)$$

## Idejaliteti koji važe u Abelovim grupama

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

$$(xy)^m = x^m y^m$$

$$\prod_{i \in I} x_{p_i} = \prod_{i \in I} x_i$$

$$-(x+y) = (-x) + (-y)$$

$$m(x+y) = mx + my$$

$$\sum_{i \in I} x_{p_i} = \sum_{i \in I} x_i$$

$$p \in S_n, \quad I = \{1, \dots, n\}$$

## Konstrukcije:

$$G = H \cdot K, \quad H, K < G$$

$G$  je unutrašnji proizvod  
podgrupa  $H, K$ ;  $G = HK, H \cap K = \{1\}$

$$A = B + C, \quad B, C < A$$

$A$  je direktna suma podgrupa  
 $B$  i  $C$ ;  $A = B \dot{+} C, B \cap C = \{0\}$ .

Primeri Abelovih grupa:  $\mathbb{C}_n$ ,  $(\mathbb{Z}, +, 0)$ ,  $(\mathbb{Q}, +, 0)$ ,  $(\mathbb{Q} \setminus \{0\}, \cdot, 1)$ , ...

Primeri grupa koje nisu Abelove:  $S_n$  - grupa permutacija skupa  $\{1, 2, \dots, n\}$ .  
 $D_n$  - dihedralska grupa - grupa simetrija pravilnog  $n$ -ougla.

Teorema Abelove grupe čine algebarski varijetet.

Dakle, klasa Abelovih grupa zadovoljava je za:

- podgrupe
- homomorfne slike
- Operaciju proizvoda algebi
- Konstrukciju količnikove algebre.

Napomena Svaka podgrupa Abelove grupe  $G$  je normalna u  $G$  tj.  
 $H < G \Rightarrow H \triangleleft G$ . Dakle, ako je  $H < G$ , postoji i dobro je  
 definirana količnikova grupa  $G/H$ .

Teorema o razlaganju konačno-generisanih Abelovih grupa

Ciklične grupe su Abelove grupe. Dakle za neke  $n_1, \dots, n_k \in \mathbb{N}^+$ ,  
 $\mathbb{C}_{n_1} \times \mathbb{C}_{n_2} \times \dots \times \mathbb{C}_{n_k}$  je Abelova grupa (i to konačna). Ima li  
 drugih Abelovih grupa? Nema! O tome govori upravo sledeća  
 teorema:

Svaka konačno generisana Abelova grupa je proizvod  
 cikličnih grupa.

Re no isto izlaziimo dokaz ove teoreme, dokazatiemo nevoliko  
 pomoćnih tvrdjenja - lema koje su od nezavisnog  
 interesa.

Lema 1 Neka su  $a_1, a_2, \dots, a_n \in \mathbb{Z}$ ,  $n \geq 2$ , takvi da je  $(a_1, a_2, \dots, a_n) = 1$ ,  
 tj.  $\text{NZD}(a_1, a_2, \dots, a_n) = 1$ . Tada postoji kvadratna matrica  $M$  reda  $n$   
 nad  $\mathbb{Z}$  takva da je  $\det M = 1$ .

Dokaz izvodimo indukcijom po  $n$ .

Slučaj  $n=2$  Neka su  $a_1, a_2 \in \mathbb{Z}$ ,  $(a_1, a_2) = 1$ . Prema Bernouij teoremi  
 postoji  $\alpha, \beta \in \mathbb{Z}$  takvi da je  $\alpha a_1 + \beta a_2 = 1$ . Gdele za

$$M = \begin{bmatrix} a_1 & a_2 \\ -\beta & \alpha \end{bmatrix} \text{ važi } \det M = 1.$$

Pretpostavimo  $H$ , da tvrdjenje važi za  $n-1$ . Neka su  $a_1, \dots, a_n \in \mathbb{Z}$  takvi da je  $(a_1, a_2, \dots, a_n) = 1$ . Neka je  $d = (a_1, a_2, \dots, a_{n-1})$  i neka su  $b_1, b_2, \dots, b_{n-1} \in \mathbb{Z}$  takvi da je  $a_1 = b_1 d, a_2 = b_2 d, \dots, a_{n-1} = b_{n-1} d$ . Tada  $(b_1, b_2, \dots, b_{n-1}) = 1$ , te prema induktivnoj hipotezi

postoji matrica  
(nad  $\mathbb{Z}$ )  $M = \begin{bmatrix} b_1 & b_2 & \dots & b_{n-1} \\ * & & & \end{bmatrix}$  reda  $n-1$ , t.d.  $\det M = 1$ .

Dalje,  $(a_n, d) = 1$ , te prema Bernovoj teoremi postoji  $s, t \in \mathbb{Z}$  takvi da je  $a_n t + d s = 1$ . Neka je matrica  $M'$  nad  $\mathbb{Z}$  određena pomoću  $M$  na sledeći način:

$$M' = \begin{bmatrix} a_1 & a_2 & \dots & a_{n-1} & a_n \\ * & & & & \vdots \\ \varepsilon t b_1 & \varepsilon t b_2 & \dots & \varepsilon t b_{n-1} & s \end{bmatrix} \quad \text{gde je } \varepsilon \in \{1, -1\} \text{ i gde o'je se tačna vrednost za } \varepsilon \text{ utvrditi kasnije.}$$

Dalje,  $M'$  je reda  $n$  i važi:

$$\det M' = \begin{vmatrix} d b_1 & d b_2 & \dots & d b_{n-1} & a_n \\ * & & & & 0 \\ \varepsilon t b_1 & \varepsilon t b_2 & \dots & \varepsilon t b_{n-1} & s \end{vmatrix} = (-1)^{n+1} a_n \begin{vmatrix} * & & & \\ \varepsilon t b_1 & \dots & \varepsilon t b_{n-1} & \end{vmatrix} + s \begin{vmatrix} d b_1 & \dots & d b_{n-1} \\ * & & \end{vmatrix} =$$

$$\pm \varepsilon t (-1)^{n+1} a_n \begin{vmatrix} b_1 & \dots & b_{n-1} \\ * & & \end{vmatrix} + s d \begin{vmatrix} b_1 & \dots & b_{n-1} \\ * & & \end{vmatrix} =$$

$$a_n t + d s = 1, \quad \text{birajući } \varepsilon \text{ tako da je } \pm \varepsilon (-1)^{n+1} = 1. \quad \square$$

Posledica 1 Neka su  $a_1, \dots, a_n \in \mathbb{Z}$  takvi da je  $(a_1, a_2, \dots, a_n) = 1$ . (Kopirajte Bernove teoreme) Tada diofantska jednačina

$$a_1 x_1 + a_2 x_2 + \dots + a_n x_n = 1$$

ima rešenje ( $a \in \mathbb{Z}$ ).

Dokaz Neka je prema prethodnoj teoremi  $M = \begin{bmatrix} a_1 & a_2 & \dots & a_n \\ * & & & \end{bmatrix}$  matrica reda  $n$  nad  $\mathbb{Z}$  takva da je  $\det M = 1$ .

Tada prema Laplasovoj teoremi, razvijajući  $\det M$  po prvoj vrstici,

$$a_1 D_1 + a_2 D_2 + \dots + a_n D_n = 1 \quad ; \quad D_i \in \mathbb{Z}, \quad i=1, 2, \dots, n.$$

Dalje, možemo uzeti da je  $x_1 = D_1, \dots, x_n = D_n$ .

Zadatak Naci opšte rešenje diofantovske jednačine  $6x + 10y + 15z = 1$ .

Rešenje Kako  $(6, 10, 15) = 1$ , ova jednačina ima rešenje.

Partikularno rešenje: Rešavajući ove jednačine u  $\mathbb{Z}$  nalazimo  $4y + 3z = 1$ ,  
odakle,  $y_0 = 1, z_0 = -1$ , te iz prve jednačine,  $x_0 = 1$ ,  
tj. partikularno rešenje je  $x_0 = 1, y_0 = 1, z_0 = -1$ .

Sada rešavamo homogeni jednačinu

$$6X + 10Y + 15Z = 0, \text{ uzimajući: } X = x - x_0, Y = y - y_0, Z = z - z_0.$$

odakle  $6X + 10Y = -15Z$ . Ova jednačina ima rešenje (prema B.T.)

ako  $2 | Z$ . Neka je  $Z = 2\alpha$ . Tada se poslednja jednačina svodi na  
 $3X + 5Y = -15\alpha$ . Opšte rešenje ove jednačine je

$$X = -30\alpha + 5\beta, Y = 15\alpha - 3\beta, \alpha, \beta \in \mathbb{Z}, \text{ te je opšte rešenje}$$

$$\text{povećane jednačine: } x = 1 - 30\alpha + 5\beta, y = 1 + 15\alpha - 3\beta, z = -1 + 2\alpha. \quad \square$$

Lema 2 Neka je  $A = (A, +, 0)$  Abelova grupa i PP da je  $A$  generisana sa  $n$  elemenata ( $n \in \mathbb{N}^+$ ), tj. postojе  $x_1, \dots, x_n \in A$  takvi da je  $A = \langle x_1, x_2, \dots, x_n \rangle$ . Dalje, neka su  $a_1, a_2, \dots, a_n \in \mathbb{Z}$  takvi da je  $(a_1, a_2, \dots, a_n) = 1$  i neka je  $y_1 = a_1x_1 + a_2x_2 + \dots + a_nx_n$ .

Tada postojе  $y_2, \dots, y_n \in A$  takvi da je  $A = \langle y_1, y_2, \dots, y_n \rangle$ .  
(Lema o promeni baze).

Dokaz Neka je prema lemi 1,  $M = \begin{bmatrix} a_1 & a_2 & \dots & a_n \\ * & * & \dots & * \end{bmatrix}$ ,  $\det M = \pm 1$  i

neka je  $\begin{bmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{bmatrix} = M \cdot \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix}$ . Dalje, s obzirom da je  $\det M = \pm 1$ ,  
 $M^{-1} = \frac{1}{\det M} \cdot \text{adj}(M)$  to je i matrica  $M^{-1}$   
- celobrojna! Otkuda

$$\begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} = M^{-1} \begin{bmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{bmatrix}, \text{ pa kako } A = \langle x_1, \dots, x_n \rangle, \text{ to je i}$$
$$A = \langle y_1, \dots, y_n \rangle \text{ jer za } x \in A,$$

za neke cele  $d_1, \dots, d_n, x = d_1x_1 + \dots + d_nx_n$ , te kako su linearne kombinacije zadovoljene za supstituciju linearnih formi, to je za neke  $\beta_1, \dots, \beta_n \in \mathbb{Z}, x = \beta_1y_1 + \dots + \beta_ny_n$  tj.  $x \in \langle y_1, \dots, y_n \rangle$ .  $\square$



Neka je  $A$  konačno generisana Abelova grupa. Tada postoji najmanji prirodan broj  $n$  takav da je  $A$  generisana sa  $n$  elemenata. Ovaj broj  $n$  nazivamo rangom grupe  $A$  i pišemo  $\text{rang } A = n$ .

Daule, ako je  $\text{rang } A = n$ , onda postoji  $x_1, \dots, x_n \in A$  takvi da je  $A = \langle x_1, \dots, x_n \rangle$  i za sve  $k < n$  i sve  $y_1, \dots, y_k \in A$ ,  $A \neq \langle y_1, \dots, y_k \rangle$ .

Dokaz temelje o razlaganju konačno generisanih Abelovih grupa. Dokaz vršimo indukcijom po rang  $A$ . Koristimo aditivnu notaciju, dakle dokazujemo da je konačno generisana Abelova grupa  $A = (A, +, 0)$  direktna (konačna) suma cikličkih grupa.

$\text{rang } A = 1$  Tada  $A = \langle a \rangle$  pa je  $A$  ciklička.

$\text{rang } A = n > 1$  Daule  $A$  je generisana sa  $n$  elemenata ali ne i sa manjim brojem. Razlikujemo dva slučaja:

- a) postoji  $x_1, \dots, x_n \in A$  takvi da  $A = \langle x_1, \dots, x_n \rangle$  i bar jedan od elemenata  $x_1, \dots, x_n$  je konačnog reda.
- b) Ako je  $A = \langle x_1, \dots, x_n \rangle$ , onda su svi elementi  $x_1, \dots, x_n$  beskonačnog reda.

Pretpostavimo najpre slučaj (a). Neka su  $x_1, \dots, x_n \in A$  takvi da je  $A = \langle x_1, \dots, x_n \rangle$  i  $\{x_1, \dots, x_n\}$  sadrži element  $x$  najnižeg reda  $n$  odnosi na sve generatorske skupove  $\{y_1, \dots, y_n\}$  grupe  $A$ , tj: ako  $A = \langle y_1, \dots, y_n \rangle$  onda  $\text{red } x \leq \text{red } y_1, \dots, \text{red } y_n$ . Možemo pretpostaviti da je  $x = x_n$ .

Neka je  $H = \langle x_1, \dots, x_{n-1} \rangle$  i  $K = \langle x_n \rangle$ . Tada je  $\text{rang } H = n-1$  jer bi u suprotnom bilo  $\text{rang } A < n$ . Daule, po indukivnoj hipotezi  $H$  je direktna suma (konačna) cikličkih grupa, a takode i grupa  $K$  je ciklička. Prema tome dosta je da dokazemo da je  $A$  direktna suma grupa  $H$  i  $K$ , tj:  $A = H \oplus K$ .

Jedino treba dokazati  $H \cap K = \langle 0 \rangle$ . PP suprotno, tj: neka je  $u \in H \cap K$  i  $\text{red } u > 1$ .

Tada  $u = d_1 x_1 + \dots + d_{n-1} x_{n-1}$  za neke  $d_1, \dots, d_{n-1} \in \mathbb{Z}$  jer  $u \in \langle x_1, \dots, x_{n-1} \rangle$

$u = d_n x_n$  za neke  $d_n \in \mathbb{Z}$  jer  $u \in \langle x_n \rangle$ .

Neka je  $d = (d_1, d_2, \dots, d_{n-1}, d_n)$  i neka su  $a_1, \dots, a_n \in \mathbb{Z}$  takvi da je  
 $d_1 = a_1 d, \dots, d_n = a_n d$

i neka je  $v = a_1 x_1 + \dots + a_{n-1} x_{n-1} - a_n x_n$ .

Tada  $(a_1, \dots, a_n) = 1$ , te prema Lemi 2 postoji  $v_2, \dots, v_n$  takvi da je  $A = \langle v, v_2, \dots, v_n \rangle$ .

S druge strane,  $d \cdot v = d_1 x_1 + \dots + d_{n-1} x_{n-1} - d_n x_n = 0$ , pa

$$\text{red } v \leq d \leq d_n < \text{red } x_n$$

Što je kontradikcija prema izboru elementa  $x_n$ : da je  $x_n$  najmanjeg reda u svim generatorima skupine od  $n$  elementa grupe  $A$ .

Dakle,  $H \cap K = \langle 0 \rangle$  pa  $A = H + K$ , te je

$A$  konačna direktna suma cikličkih grupa, odnosno  $A$  je itomorfna konačnom proizvodu cikličkih grupa.

Slučaj b: Svaki element u svom generatorima skupine od  $n$  elementa grupe  $A$  je beskonačnog reda. U tom slučaju dokazuje se da je  $A \cong \mathbb{Z}^n = (\mathbb{Z}, +, 0)^n$ . ▣

Posljedica 1 Svaka konačna Abelova grupa itomorfna je (konačnom) proizvodu cikličkih grupa.

Dokaz Ako je  $A$  konačna, onda je i konačno generisana jer  $A = \langle A \rangle$ .

Primer Opisati do na itomorfizam sve Abelove grupe reda 100.

Rešenje:  $100 = 2^2 \cdot 5^2$ , pa umnogiči: u okviru prethodne teorije, Lagranževu teoriju o podgrupama i Teoremu 3c kod cikličkih grupa, nalazimo sledeće Abelove grupe reda 100:

$$\mathbb{C}_4 \times \mathbb{C}_{25} = \mathbb{C}_{100}, \quad \mathbb{C}_4 \times \mathbb{C}_5^2 = \mathbb{C}_{20} \times \mathbb{C}_5, \quad \mathbb{C}_2^2 \times \mathbb{C}_{25} = \mathbb{C}_2 \times \mathbb{C}_{50}, \quad \mathbb{C}_2^2 \times \mathbb{C}_5^2 = \mathbb{C}_{10}^2.$$

Napomena:  $\mathbb{C}_4 \times \mathbb{C}_5^2 \not\cong \mathbb{C}_2^2 \times \mathbb{C}_{25}$  jer, na primer,  $\mathbb{C}_2^2 \times \mathbb{C}_{25}$  ima element reda 25, dok grupa  $\mathbb{C}_4 \times \mathbb{C}_5^2$  nema element reda 25. IZ sličnog razloga i ostali parovi navedenih grupa nisu međusobno itomorfne.

Zadatak Opisati do na itomorfizam sve grupe reda 150.

Paralelca 2. Neka je  $A$  konačna Abelova grupa reda  $n$  i neka je  $p$  prost broj,  $p|n$ . Tada  $A$  ima element reda  $n$ .

Dokaz Prema teoremi o dekompoziciji <sup>u.g.</sup> Abelovih grupa,  $A$  je proizvod cikličkih grupa:  $A = C_{n_1} \times \dots \times C_{n_k}$ . Tada za neki  $i \leq k$ ,  $p|n_i$ . Ako je  $C_{n_i} = \langle a \rangle$ , tada je  $a^{\frac{n_i}{p}}$  element reda  $p$  u  $A$ .

Paralelca 3. Neka je  $F = (F, +, \cdot, 0, 1)$  polje i neka je  $G < (F \setminus \{0\}, \cdot, 1)$  konačna, tj.  $G$  je konačna podgrupa multiplikativne grupe  $F^* = (F \setminus \{0\}, \cdot, 1)$  polja  $F$ . Tada je  $G$  ciklička grupa.

Dokaz Prema teoremi o reprezentaciji u.g. Abelovih grupa,  $G$  je kon. proizvod cikličkih grupa. Ako je  $G$  nije ciklička, onda postoje cikličke grupe  $H, K < G$  t.d.  $H \cap K = \langle 1 \rangle$  i redovi njih grupa nisu uzajamno prosti, tj.  $(|H|, |K|) > 1$ . Neka je  $p$  prost broj t.d.  $p|(H|, |K|)$ . Tada postoji  $a \in H, b \in K$  t.d. red  $a = p$ , red  $b = p$  i  $\langle 1, a, \dots, a^{p-1} \rangle \cap \langle 1, b, \dots, b^{p-1} \rangle = \langle 1 \rangle$ , tj.  $\langle a \rangle \cap \langle b \rangle = \langle 1 \rangle$ . Neka je  $S = \langle 1, a, \dots, a^{p-1}, b, b^2, \dots, b^{p-1} \rangle$ .

Tada za  $x \in S, x^p = 1$ , ta jednačina  $x^p - 1 = 0$  ima  $|S| = 2p - 1 > p$  rešenja, uprkos činjenici da polin. stepena  $p$  u polju mora imati najviše  $p$  rešenja. Dakle,  $G$  je ciklička.  $\square$

Paralelca 4. Neka je  $p$  prost broj. Tada je  $\mathbb{Z}_p^* = (\mathbb{Z}_p \setminus \{0\}, \cdot, p, 1)$  ciklička grupa, dakle,  $\mathbb{Z}_p^* \cong C_{p-1}$ .

Zadatak Neka grupni identitet  $u=v$  važi u svim cikličkim grupama. Tada  $u=v$  važi u svim Abelovim grupama.

Zadatak Neka je  $p$  prost broj. Dokazati da je  $\mathbb{Q}$  polje grupa  $\mathbb{Q}(p)$  ciklička.

Zadatak Neka je  $A$  Abelova grupa reda  $n$  i neka  $u|n, v|n \in \mathbb{N}$ . Dokazati da  $A$  sadrži podgrupu reda  $u$ .

# Abelove grupe sa deljenjem

April 2020  
Zvezdano

3-7

Def. Abelova grupa  $A$  je grupa sa deljenjem ako za svaki  $n \in \mathbb{N}^+$  i svaki  $a \in A$  jednačina  $n \cdot x = a$  ima rešenje ( $10 \times$ ).

Primer 1.  $(\mathbb{Q}, +, 0)$  je Ab. grupa sa deljenjem.

2.  $(\mathbb{R}, +, 0)$  je Ab. grupa sa deljenjem.

Osobine Abelovih grupa sa deljenjem

1. Homomorfna slika Ab. grupe sa deljenjem je Ab. grupa sa deljenjem.
2. Preizvod dveju Ab. grupa sa deljenjem je Ab. grupa sa deljenjem.

Dokaz. 1. Neka je  $A$  Ab. grupa sa deljenjem,  $h: A \xrightarrow{h} B$ .

Da li je jednačina  $n \cdot x = b$ ,  $n \in \mathbb{N}^+$ ,  $b \in B$ , uvek rešiva u  $B$ ?

Neka je  $a \in A$  t.d.  $h(a) = b$  ( $h$  je na!), i neka je

$d \in A$  t.d.  $n \cdot d = a$  ( $A$  je Ab. grupa sa deljenjem!). Tada

$h(nd) = h(a)$ , tj:  $n \cdot h(d) = b$ , tj:  $h(d)$  je rešenje jedn.  $n \cdot x = b$ .

2. Neka su  $A, B$  Ab. grupe sa deljenjem i neka su  $(a, b) \in A \times B$ .

Neka su  $a' \in A$ ,  $b' \in B$  tačni d.  $n \cdot a' = a$ ,  $n \cdot b' = b$ ,  $n \in \mathbb{N}^+$ .

Tada je  $(a', b')$  rešenje jedn.  $n \cdot (x, y) = (a, b)$  u  $A \times B$ .  $\square$

Def. Grupa  $G$  je bez torzije, ako je svaki  $x \in G \setminus \{1\}$  beskonačnog reda.

Teorema Neka je  $A = (A, +, 0)$  Ab. grupa sa deljenjem i bez torzije.

Onda je  $A$  vektorski prostor nad poljem racionalnih brojeva  $\mathbb{Q} = (\mathbb{Q}, +, \cdot, 0, 1)$ .

Dokaz Neka je  $A = (A, \mathbb{Q}, \cdot)$  gde je operacija množenja vektora

$a \in A$  i skalar  $t \in \mathbb{Q}$ ,  $t = \frac{p}{q}$ ,  $p, q \in \mathbb{Z}$ , definisano na sledeći način:

$$b = \frac{p}{q} \cdot a \Leftrightarrow qb = p \cdot a,$$

tj:  $b$  je rešenje jednačine  $qx = pa$ .

Prisetimo da je ovako određeno  $b$  jedinstveno. Naime, ako je  $qb' = pa$ ,

onda  $q(b-b') = 0$  pa  $b-b' = 0$  jer je  $A$  grupa bez torzije. Dakle

operacija množenja vektora i skalara je dobro definisana.

Ostalo je da se dokaže sledeće tvrdnje:

a)  $1 \cdot x = x$ , b)  $(\alpha + \beta)x = (\alpha x) + (\beta x)$  c)  $\alpha(x + y) = (\alpha x) + (\alpha y)$   
 d)  $(\alpha\beta)x = \alpha(\beta x)$ .

Dokazimo, na primer, (d): Najpre prenesimo da za  $u \in \mathbb{Z} \setminus \{0\}$  vazi:

$ux = ux \Rightarrow x = y, \quad x, y \in A.$

Dalje, neka je  $z = \alpha(\beta x) = \frac{p}{q} \left( \frac{p'}{q'} x \right)$ . Tada  $qz = pg$ , gde je  $y = \frac{p'}{q'} x$ . Onda  $q'(qz) = q'(pg)$ , pa  $(qq')z = p(q'y) = p(p'x)$

ti:  $(qq')z = (pp')x$ , odakle  $z = \frac{pp'}{qq'} x = (\alpha\beta)x$  tj:

$\alpha(\beta x) = (\alpha\beta)x$  za  $\alpha, \beta \in \mathbb{Q}, x \in A, \alpha = \frac{p}{q}, \beta = \frac{p'}{q'}$ ,

$p, p' \in \mathbb{Z}, q, q' \in \mathbb{N}^+$ . Onda smo koristili da je za  $u, v \in \mathbb{Z}$

$m(nx) = (m n)x$ ,

na primer za  $u, v \in \mathbb{N}^+$ :  $m(ux) = (m u)x = \underbrace{x + x + \dots + x}_{m \text{ puta}}$

Slicno se dokazuju idealnosti (b) i (c).

Da na, zaista je  $A = (A, \mathbb{Q}, \cdot)$  vektorski prostor. Ako je  $\dim A = n$ , onda  $A \cong \mathbb{Q}^n$ , tj: ( $n \in \mathbb{N}^+$ ):

Teorema Neka je  $\dim A = n$ . Tada  $A \cong (\mathbb{Q}^n, +, 0)$ , odakle

$A = A_1 \dot{+} A_2 \dot{+} \dots \dot{+} A_n$ , gde  $A_i \cong (\mathbb{Q}, +, 0), 1 \leq i \leq n$ .

Vazi i apitije, ako je  $\dim A = \kappa, \kappa \in \text{CARD}$ , tda

$A = \sum_{i \in I} A_i, \quad |I| = \kappa, \quad A_i \cong (\mathbb{Q}, +, 0), i \in I.$

tj: svaka Abelova grupa sa deljenjem i bez torzije, direktno je suma izomorfnih kopija aditivne grupe racionalnih brojeva.

Na primer,  $(\mathbb{R}, +, 0) = \sum_{i \in I} \mathbb{R}_i, \quad |I| = c = 2^{\aleph_0}, \quad \mathbb{R}_i \cong (\mathbb{Q}, +, 0).$

Zadatak Navesti primer Abelove grupe sa deljenjem u kojoj su svi elementi konačnog reda.

Zadatak a) odrediti  $\text{Aut}(\mathbb{Q}, +, 0)$ , b)  $\text{Aut}(\mathbb{R}, +, 0)$ .  
 (opisati).

Zadatak Neka je  $A$  Abelova grupa sa deljenjem. Tada je  $A$  beskonačna grupa.

6 Lema 1° Neka su  $A, B$  konačne podgrupe grupe  $G$ . Tada

$$|AB| = \frac{|A| \cdot |B|}{|A \cap B|}$$

2° Neka je  $G$  grupa i  $Z(G)$  centar grupe  $G$ , tj:  
 $Z(G) = \{x \in G \mid (\forall g \in G) \ xg = gx\}$ . Tada

a)  $H < Z(G) \Rightarrow H \triangleleft G$ .

b)  $H < Z(G)$  i  $G/H$  je ciklična  $\Rightarrow G$  je Abelova.

3° Neka je  $G$  grupa takva da je  $(\forall a \in G) \ a^2 = e$ .  
 Tada je  $G$  Abelova.

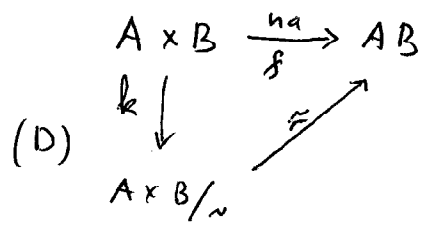
4°  $|G:H| = 2 \Rightarrow H \triangleleft G$ . ( $H < G$ ).

5° Neka je grupa  $G$  generisana skupom  $S$  i nema je  
 za sve  $x, y \in S, \ xy = yx$ . Tada je  $G$  Abelova.

Donat 1°. Neka je  $f: A \times B \rightarrow AB$  definisano sa

$$f = (a, b) \mapsto ab, \quad (a, b) \in A \times B.$$

Prema teoriji o razlaganju homomorfizma  
 imamo sledeći komutativan dijagram



Ovde je  $n$  jezgro preslikovanja  $f$ , tj.

Relacija ekvivalencije na  $A \times B$

definisana sa:  $(a_1, b_1) \sim (a_2, b_2)$  akko  $f(a_1, b_1) = f(a_2, b_2)$ .

$$\text{Nemo je } (a_1, b_1) \sim (a_2, b_2) \Leftrightarrow a_1 b_1 = a_2 b_2$$

$$\Leftrightarrow a_2^{-1} a_1 = b_2 b_1^{-1}$$

$$\Leftrightarrow (\exists t \in A \cap B) (a_2^{-1} a_1 = t \wedge b_2 b_1^{-1} = t)$$

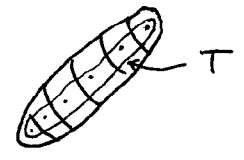
$$\Leftrightarrow (\exists t \in A \cap B) (a_1 = a_2 t \wedge b_2 = t b_1),$$

nalazimo  $(a, b) / \sim = \{ (at^{-1}, tb) \mid t \in A \cap B \}$ . Onda

(1)  $| (a, b) / \sim | = |A \cap B|$  za proizvoljne  $a \in A, b \in B$ .

$A \times B$  je disjunktne unija klasa ekvivalencija, tj.

(2)  $A \times B = \bigcup_{(a,b) \in T} (a, b) / \sim$ ,  $T$  je transversala (izborni skup)  
 partije  $A \times B / \sim$ .



Transverzala  $T$  ima tačno onoliko  
 elemenata koliko ima klasa ekvivalencije, te

prema (D),  $|T| = |AB|$ . Tada iz (2) nalazimo

$$|A| \cdot |B| = |A \times B| = \sum_{(a,b) \in T} |(a,b) / \sim| = |T| \cdot |A \cap B| = |AB| \cdot |A \cap B|.$$

2<sup>o</sup>) Neka je  $H < Z(G)$ . Tada za proizvoljno  $g \in G$ ,

$$gH = \{gx \mid x \in H\} = \{xg \mid x \in H\} = Hg$$

je i za proizvoljno  $x \in Z(G)$ , dakle i za  $x \in H$ ,  $xg = gx$ .

B) Neka je  $H < Z(G)$  i pretpostavimo da je  $G/H$  ciklična. Puzetimo da je prema (a)  $G/H$  dobro definisana grupa, kako je  $G/H$  ciklična postoji  $a \in G$  tako da je

$$G/H = \langle aH \rangle. \text{ Ako je } G/H \text{ konačna ciklična grupa}$$

onda  $G/H = \{H, aH, a^2H, \dots, a^{n-1}H\}$ , gde su  $a^iH$ ,  $0 \leq i < n$ ,

disjunktni neseti grupe  $G$  i onda  $G = H \cup aH \cup \dots \cup a^{n-1}H$ .

Neka su  $x, y \in G$ , Tada postoji  $0 \leq i, j \leq n-1$ ,  $h_1, h_2 \in H$  tako da je  $x = a^i h_1$ ,  $y = a^j h_2$ . S obzirom da  $h_1, h_2$

komutiraju sa svim elementima grupe  $G$  i da je

$$a^i \cdot a^j = a^{i+j} = a^{j+i} = a^j \cdot a^i, \text{ nalazimo}$$

$$xy = h_1 a^i h_2 a^j = \dots = h_2 a^j h_1 a^i = y \cdot x.$$

Ako je  $G/H$  beskonačna ciklična grupa, onda

$$G/H = \{\dots, a^{-2}H, a^{-1}H, H, aH, a^2H, \dots\} \text{ i}$$

$$G = \bigcup_{n \in \mathbb{Z}} a^n H, \text{ i dokaz da je za } x, y \in G, xy = yx,$$

izvede se na isti način.

3<sup>o</sup> PP da je za sve  $x \in G$ ,  $x^2 = e$ ,  $e$  je jedinica grupe  $G$ .

Tada za proizvoljne  $a, b \in G$ ,  $(ab)^2 = e$ , tj:

$$abab = e, \text{ odakle, } abab^2 = eb \text{ tj: } aba = b, \text{ te } aba^2 = ba, \text{ tj: } ab = ba.$$

4<sup>o</sup> Pretpostavimo da je  $|G:H| = 2$ ,  $H < G$ . Tada

a) za  $x \in H$ ,  $xH = Hx = H$ .

b) za  $x \in G \setminus H$ ,  $xH = G \setminus H = Hx$

u svakom slučaju, za proizvoljno  $x \in G$ ,  $xH = Hx$ , tj:  $H \triangleleft G$ .

5<sup>o</sup> Neka je  $G = \langle S \rangle$  i pretpostavimo da je za sve  $x, y \in S$ ,  $xy = yx$ . Tada:

a) za  $x, y \in S$  i  $m, n \in \mathbb{N}$ , važi  $x^m y^n = y^n x^m$ .  
 Ovo tvrdjenje lako se dokazuje indukcijom po  $m, n$ .

b) Iz (a) sledi, umnogem na  $x^{-m}$ , odnosno  $y^{-n}$ :

$$x^{-m} y^n = y^n x^{-m}, \quad x^m y^{-n} = y^{-n} x^m, \quad x^{-m} y^{-n} = y^{-n} x^{-m}$$

Onda, za sve  $x, y \in S$ ,  $\alpha, \beta \in \mathbb{Z}$

(1)  $x^\alpha y^\beta = y^\beta x^\alpha$ .

Neka su  $u, v \in G$ . Tada  $u, v \in \langle S \rangle$ , te postoje  $x_1, \dots, x_m \in S$   $d_1, \dots, d_m \in \mathbb{Z}$  i  $y_1, \dots, y_n \in S$ ,  $\beta_1, \dots, \beta_n \in \mathbb{Z}$  takvi da je

$$u = x_1^{d_1} x_2^{d_2} \dots x_m^{d_m}, \quad v = y_1^{\beta_1} y_2^{\beta_2} \dots y_n^{\beta_n}$$

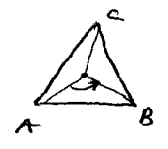
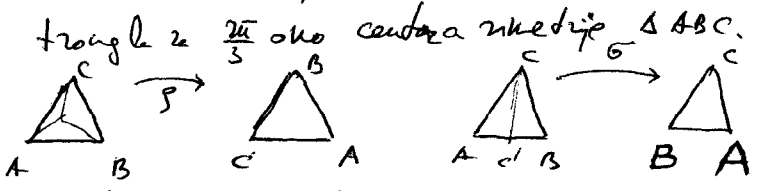
Tada, koristeći (1) nalazimo

$$xy = x_1^{d_1} x_2^{d_2} \dots x_m^{d_m} y_1^{\beta_1} y_2^{\beta_2} \dots y_n^{\beta_n} = \dots = y_1^{\beta_1} y_2^{\beta_2} \dots y_n^{\beta_n} x_1^{d_1} \dots x_m^{d_m} = v \cdot u.$$

Primer 1. Postoji tačno jedna grupa (do na izomorfizam)  $G = \langle a, b \rangle$  gde su  $\text{red}(a) = 3, \text{red}(b) = 2, ba = a^2b$ .

Dokaz Postoji bar jedna takva grupa, to je  $S_3 \cong D_3$

( $S_3$  - grupa permutacija skupa  $\{1, 2, 3\}$ ;  $D_3$  - dihedralska grupa trougla).  $D_3 = \langle \rho, \sigma \rangle$ ,  $\rho$  = rotacija prouhnoj trougla za  $\frac{2\pi}{3}$  oko centra inercije  $\Delta ABC$ .



$\sigma$  - refleksija u odrazu na osu  $cc'$

Tanako,  $S_3 = \langle a, b \rangle, a = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, b = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$

Jedinstvo: Neka je  $G = \langle a, b \rangle, a^3 = 1, b^2 = 1, ba = a^2b$   $\text{red}(a) = 3, \text{red}(b) = 2$ .

Kako je  $ba^2 = a^2ba = a^4b = ab$ , to je

(1)  $\langle a \rangle \triangleleft G$ .

Onda  $G = AB$ , gde  $A = \langle a \rangle, B = \langle b \rangle, |A| = 3, |B| = 2$

$$|G| = |AB| = \frac{|A||B|}{|A \cap B|} = \frac{3 \cdot 2}{1} = 6 \quad \text{jer nisu kongruentni}$$

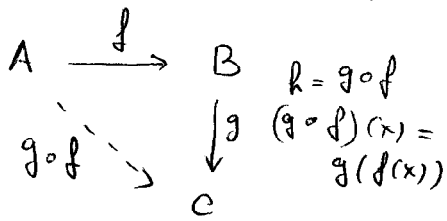
jeremisi  $|A \cap B| \mid |A|, |B|$  tj.  $|A \cap B| \mid 2, 3$  tj.  $|A \cap B| = 1$ . Onda

(2)  $G = \{1, a, a^2, b, ab, a^2b\}$ , ta  $G \cong S_3$ , odn.  $G \cong D_3$

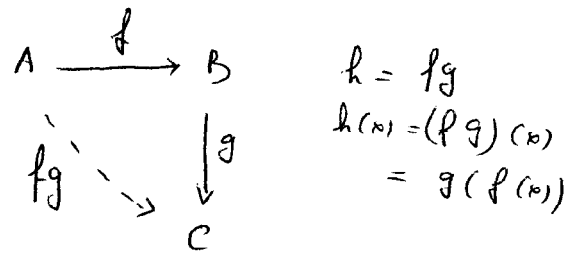


# Dejstvo grupe na skup

Algebarsna notacija slagajna funkcija:



sumpovna notacija



algebarsna notacija

Neka je  $G$  grupa i  $S$  neki neprazan skup.

Dejstvo grupe  $G$  na skup  $S$  je svaki homomorfizam

$$\theta: G \rightarrow \text{Sym}(S)$$

gde je  $\text{Sym}(S) = (\text{Sym}(S), \cdot, i_S)$  simetrična grupa (grupa permutacija) skupa  $S$  u algebarsnoj notaciji.  $i_S$  je identično preslikavanje skupa  $S$ . Dakle,

$$\theta(e) = i_S,$$

$$\theta(gh) = \theta(g)\theta(h) \quad \text{za } g, h \in G; \quad i \text{ za } s \in S;$$

$$\theta(g): S \xrightarrow{na} S; \quad (\theta(g)\theta(h))(s) = \theta(h)(\theta(g)(s))$$

Relacija ekvivalencije dejstva  $\theta$ . Uvodi se u datu razumnu dejstvo  $\theta$  finiranu, umesto  $\theta(g)(s)$  pišemo  $sg$  (kao je grupa data u multiplikativnoj notaciji), odno  $gs$  (kao je grupa  $G$  data u aditivnoj notaciji; naravno,  $G$  je Abelova).

Lema 1    1°  $s^e = s$ ,    2°  $(sg)^h = sgh$ .

Dokaz    1°  $s^e = \theta(e)(s) = i_S(s) = s$

2°  $(sg)^h = \theta(h)(\theta(g)(s)) = (\theta(g)\theta(h))(s) = \theta(gh)(s) = sgh$

Stabilizator elementa  $s \in S$  (u odnosu na dejstvo  $\theta$ ) je

$$G_s = \{g \in G \mid sg = s\}.$$

Lema 2     $G_s < G$ .

Dokaz    1°  $e \in G_s$  jer  $se = s$ . 2° Ako  $g, h \in G_s$  onda  $sg^h = (sg)^h = s^h = s$

pa  $gh \in G_s$ . Takođe, iz  $sg = s$  sledi  $(sg)^{g^{-1}} = s^{g^{-1}} = s$  tj:  $sgg^{-1} = s$

pa  $sg^{-1} = s$ , tj:  $g^{-1} \in G_s$ .

Relacija ekvivalencije dejstva  $\theta$ . Nena je relacija  $\sim$  na  $S$  definirana ovako:

$s \sim t$  akko postoji  $g \in G$  tako da je  $t = sg$ .

Lema 3 Relacija  $\sim$  je relacija ekvivalencije na  $S$ .

Dokaz (R)  $s \sim s$  jer  $se = s$ .

(S) PP  $s \sim t$ . Tada za neki  $g \in G$ ,  $t = sg$ , pa  $s = t g^{-1}$  tj.  $t \sim s$ .

(T) PP  $s \sim t$ ,  $t \sim u$ . Tada za neke  $g, h \in G$ ,  $t = sg$ ,  $u = th$  pa  $u = (sg)h = sgh$  tj.  $s \sim u$ .

Klasa ekvivalencije elementa  $s \in S$  naziva se orbitom i obeležava se sa  $sG$ . Dakle

$$sG = sG = \{ sg \mid g \in G \}.$$

Lema 4 Nena je  $s \in S$ . Tada  $|sG| = |G : G_s|$ .

Dokaz Primetimo da je  $|G : G_s| = |G/G_s|$ , gde je

$G/G_s = \{ G_s \cdot g \mid g \in G \}$  (Napomena:  $G/G_s$  ne mora biti grupa, ovaj skup uvek je bidegrupa akko  $G_s \triangleleft G$ ).

Dalje, za  $g, h \in G$  vazi:

$$\begin{aligned} sg = sh &\Leftrightarrow sgh^{-1} = s \Leftrightarrow gh^{-1} \in G_s \Leftrightarrow G_s gh^{-1} = G_s \\ &\Leftrightarrow G_s g = G_s h \end{aligned}$$

Dakle, preslikavanje  $\Phi: sG \rightarrow G/G_s$  definirano sa

$$\Phi: sg \mapsto G_s \cdot g$$

je dobro definirano i jeste 1-1. Očigledno  $\Phi$  je na, pa

$$|sG| = |G/G_s| = |G : G_s|.$$

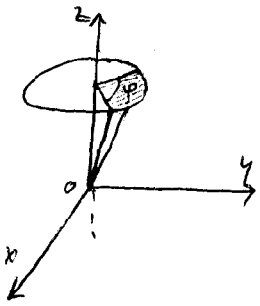
Klasovna jednaost Nena grupa  $G$  deluje na skup  $S$ .

Tada se  $S$  moze predstaviti kao disjunktna unija orbita

$$S = \bigcup_{s \in T} sG, \quad T \text{ je transverzala partitije } \{sG \mid s \in S\}$$

$$\text{pa } |S| = \sum_{s \in T} |sG| = \sum_{s \in T} |G : G_s|, \text{ tj.}$$

$$|S| = \sum_{s \in T} |G : G_s| \quad \leftarrow \text{klasovna jednaost}$$

Primer 1.

Neka je  $G = (R, +, 0)$ ,  $S = R^3$

Neka je za  $\varphi \in R$ ,  $\theta(\varphi): R^3 \rightarrow R^3$  rotacija  
prstena  $R^3$  oko z-ose za ugao  $\varphi$ .

Tada  $\theta(\varphi_1 + \varphi_2) = \theta(\varphi_1) \circ \theta(\varphi_2)$ , pa je  $\theta$  desno  
(ozigodno  $\theta(0) = \text{id}_{R^3}$ ).

Za  $n \in R^3$ ,  $G_n = \{ \theta(k) \mid k \in Z \} \cong Z$ ,

dok je orbita tačke  $n$  (ako  $n \neq z$ -osi)

$n^G =$  kružnica sa centrom na  $z$ -osi, leži u ravni  
paralelnoj  $oxy$ -ravni.  
 $\text{ker } \theta = \{ \theta(k) \mid k \in Z \} \cong Z$ .

Primer 2.

$G = (R, +, 0)$ ,  $S = P(R^3) = \{ X \mid X \in R^3 \}$

za  $\hat{\theta}: G \rightarrow \text{Sym}(S)$ ,  $\hat{\theta}(X) = \theta[X]$ , gde

je  $\theta$  preslikavanje iz prethodnog primera.

Za pogodno izabrane kružnice  $K \in P(R^3)$ , orbita  
kružnice  $K$  lic'e torus (more bih i sfera).

Primer 3 Neka je  $G$  grupa, i  $\sigma: G \rightarrow \text{Sym}(G)$  definisano

za  $\sigma(g)(x) \stackrel{\text{def}}{=} \sigma_g(x) = g^{-1}xg$ ,  $g, x \in G$ . Tada

$$\sigma(gh)(x) = (gh)^{-1}xgh = h^{-1}g^{-1}xgh = \sigma_h(\sigma_g(x)) = (\sigma_g \circ \sigma_h)(x)$$

pa  $\sigma(gh) = \sigma_g \circ \sigma_h$  tj.  $\sigma$  je desno grupno  $G$  na domenu  $G$   
je grupe. Tada

$$a) G_x = \{ g \in G \mid xg = x \} = \{ g \in G \mid g^{-1}xg = x \} = \{ g \in G \mid xg = gx \} = C(x).$$

tj. stabilizator el.  $x$  je njegov centralizator.

$$b) x^G = \{ xg \mid g \in G \} = \{ y \in G \mid y \text{ je konjugovan sa } x \}.$$

$$c) \text{ker } \sigma = \{ g \in G \mid \sigma(g) = \text{id}_S \} = \{ g \in G \mid (\forall s \in S) s^g = s \}$$

$$= \bigcap_{s \in S} G_s \text{ tj. za fiksirano desno } \sigma: G \rightarrow \text{Sym } S$$

$$\text{ker } \sigma = \bigcap_{s \in S} G_s. \text{ Specijalno za desno } \sigma$$

$$\text{ker } \sigma = \bigcap_{x \in G} C(x) = Z(G). \text{ Pretpostavimo da } x \in Z(G) \text{ akno } C(x) = G$$

$$d) \text{Klasovna jednakost: } |G| = \sum_{x \in T} |G : G_x| =$$

$$\sum_{\substack{x \in T \\ x \in Z(G)}} |G : C(x)| + \sum_{\substack{x \in T \\ x \notin Z(G)}} |G : C(x)| = \sum_{x \in Z(G)} 1 + \sum_{\substack{x \in T \\ x \notin Z(G)}} |G : C(x)| = |Z(G)| + \sum_{\substack{x \in T \\ x \notin Z(G)}} |G : C(x)|$$

Davle, klasovna jednakost u ovom slučaju izgleda

$$|G| = |Z(G)| + \sum_{\substack{x \in T \\ x \notin Z(G)}} |G : C(x)|, \quad T \text{ je transversala dejstva } G.$$

p-grupe

Konačna grupa  $G$  je p-grupa, gde je  $p$  prost broj, ako je  $\text{red}(G) = p^n$  za neki  $n \in \mathbb{N}^+$ . Davle, svaka grupa reda 8 je p-grupa (za  $p=2$ ), svaka grupa reda 25 je p-grupa (za  $p=5$ ) itd.

Teorema Svaka p-grupa ima netrivialni centar.

Dokaz Ako  $x \notin Z(G)$ , onda je  $C(x)$  prava podgrupa grupe  $G$ , pa je u tom slučaju  $|G : C(x)| = p \cdot d$  za neki  $d \in \mathbb{N}$ , jer  $|G : C(x)|$  deli  $\text{red}(G) = p^n$ . Onda iz klasovne jednakosti

imalismo

$$|G| = |Z(G)| + \sum_{x \in T, x \notin Z(G)} |G : C(x)|$$

$$p^n = |Z(G)| + n \cdot p, \quad \text{pa } p \mid |Z(G)|. \text{ Davle}$$

$Z(G) \neq \langle 1 \rangle$ , jer  $Z(G)$  ima bar  $p$  elemenata. □

Posledica Svaka p-grupa ima element reda  $p$ .

Dokaz  $Z(G) < G$  je Abelova i netrivialna, pa prema Kaiperovoj lemi za Abelove grupe,  $Z(G)$  ima element  $a$  reda  $p$ . Naravno,  $a$  je element grupe  $G$  reda  $p$ .

grupe reda  $p^2$ ,  $p \geq 3$  su Postoje dve grupe reda  $p^2$ . To su

$C_{p^2}$  i  $C_p^2 = C_p \times C_p$ . Kao što ćemo videti, drugu grupu reda  $p^2$  nema. Nema, jer  $\text{red}(G) = p^2$  i nema je  $a \in Z(G)$ ,  $\text{red}(a) = p$ , taj element jeste taj prema prethodnoj posledici. Tada  $\langle a \rangle < G$  te

$$|G / \langle a \rangle| = p, \quad \text{pa je } G / \langle a \rangle \text{ ciklična. Prema 6 lema}$$

$G$  je Abelova, tj.  $G$  je isomorfna  $C_{p^2}$  ili  $C_p^2$ . □

Sve grupe reda 4:  $C_4$ ,  $C_2^2 = K_4$  (ključna četvorka grupa)

$$9: C_9, C_3^2 = C_3 \times C_3.$$