Žarko Mijajlović

Ciklične grupe

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

Primeri 1° $\mathbb{Z} = (Z, +, -, 0) = \langle 1 \rangle$, $Z = \{\dots, -2, -1, 0, 1, 2, \dots\}$

2° $\mathbb{Z}_n = (Z_n, +_n, -, 0) = \langle 1 \rangle$, $Z_n = \{0, 1, \dots, n-1\}$,

3° $C_n = \{ x \in C \mid x^n = 1 \} = \langle \varepsilon \rangle$, $\varepsilon = e^{\frac{2\pi i}{n}} = \cos\frac{2\pi}{n} + i \sin\frac{2\pi}{n}$

C = skup kompleksnih brojeva

$\mathbb{C}_n = (C_n, \cdot, ^{-1}, 1)$.

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

a) Ako je $\mathrm{red}(a) = n$, onda $G = \{1, a, \dots, a^{n-1}\}$ i za $0 \le i < j < n$, $a^i \ne a^j$.

b) Ako je $\mathrm{red}(a) = \infty$, onda $G = \{\dots, a^{-2}, a^{-1}, 1, a, a^2, \dots\} = \{a^n \mid n \in Z\}$, $i \ne j \Rightarrow a^i \ne a^j$.

Dokaz a) Neka je $\alpha \in Z$. Tada postoje $q, i \in Z$, t.d.

(1) $\alpha = nq + i$, $0 \le i < n$.

S druge strane $\langle a \rangle = \{a^\alpha \mid \alpha \in Z\}$ pa prema (1)

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

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

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

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

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

a) Ako je $\mathrm{red}(a) = \mathrm{red}(b) = n$ 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 $k = \mathrm{rest}(i+j, n) = i +_n j$. Tada

$a^i \cdot a^j = a^{i+j} = a^{qn + k} = a^k = a^{i +_n j}$, 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) $\mathrm{red}(a) = \mathrm{red}(b) = \infty$. Tada $f : G \cong H$, gde

$f : a^\alpha \mapsto b^\alpha$, $\alpha \in Z$.

Dakle sve cikličke grupe su:

$C_1, C_2, C_3, \dots$ (konačne cikličke grupe)

C_∞ (beskonačne cikličke grupe)

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

<u>Teorema 3.</u> a) Homomorfna slika cikličke grupe je ciklična grupa.

b) Podgrupa cikličke grupe je ciklična grupa.

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

<u>Dokaz</u> a) Neka je $G = \langle a \rangle$ i $h : G \xrightarrow{na} H$, tj. $H = hG$.
Tada $H = \langle h(a) \rangle$.

b) Neka je $G = \langle a \rangle$ i $H < G$. P.P. 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 $i \in \mathbb{Z}$ t.d. $x = a^i$. Neka su $q, r \in \mathbb{Z}$ t.d.

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

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. $x \in \langle a^k \rangle$. Dakle $H = \langle a^k \rangle$, tj. H je ciklična.

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

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

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

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

Pretpostavimo $(m,n) \neq 1$, tj. za $d = (m,n)$, $d > 1$. 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 red$(a) = m$, red$(b) = n$. Tada

$a^k = a^{m \cdot \frac{n}{d}} = (a^m)^{\frac{n}{d}} = 1$ i slično $b^k = b^{n \cdot \frac{m}{d}} = (b^n)^{\frac{m}{d}} = 1$, pa za proizvoljan $(a^i, b^j) \in C_m \times C_n$,

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

red$(x) \le k < mn$, pa $C_m \times C_n \not\cong C_{mn}$. ∎

Teorema 4. Neka su $k, n \in N^+$ i pretpostavimo da $k \mid n$. Tada postoji tačno jedna podgrupa $H < C_n$, $red(H) = k$.

Dokaz Neka je $C_n = \langle a \rangle$. Tada $H = \langle a^{\frac{n}{k}} \rangle$ je reda k i $H < C_n$. Dokažimo da je H jedina podgrupa reda k grupe C_n. Neka je $H' < C_n$, $|H'| = k$. Prema dokazu Teoreme 3 b, postoji $i \in N^+$ (uz uslov $k > 1$; za $k = 1$ tvrđenje trivijalno sledi) t.d. $H' = \langle a^i \rangle$, i pri tome i je najmanji pozitivan broj sa tom osobinom. Kako je $red(H') = k$, to $a^{ik} = 1$ pa $ik \equiv 0 \mod n$, tj. $n \mid ik$. Kako $k \mid n$, zato što i je najmanji pr. broj da $n \mid ik$, to $ik = n$, pa $i = \frac{n}{k}$, tj. $H' = \langle a^{\frac{n}{k}} \rangle = H$.

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

Dokaz Neka je $C_n = \langle a \rangle$, i neka je $b \in S$. Tada $b = a^i$ za neki $i \in Z_n \setminus \{0\}$. Kako $C_n = \langle b \rangle$ to za neki k, $b^k = a$ tj. $a^{ik} = a$, odakle $ik \equiv 1 \mod n$ pa $i \in \Phi(n)$ (jer je i jedinica prstena Z_n).
S druge strane, neka je $i \in \Phi(n)$. Tada za neki $k \in Z_n$, $ik \equiv 1 \mod n$, pa $ik = 1 + dn$ za neki $d \in Z$. Odatle $a^{ik} = a^{1+dn} = a^1 \cdot a^{dn} = a$, pa za proizvoljno $x \in C_n$ za odgovarajuće $j \in N$ imamo

$x = a^j = (a^{ik})^j = (a^i)^{kj}$ tj. $x \in \langle a^i \rangle$, pa $C_n = \langle a^i \rangle$.

Dakle, $C_n = \langle a^i \rangle$ akko $i \in \Phi_n$, pa $|S| = |\Phi(n)| = \varphi(n)$. ∎

Odavde imamo sledeće zanimljive primene:

1° Neka je $d \mid n$, $S_d = \{ x \in C_n \mid red(x) = d \}$. Prema Lagranžovoj teoremi, $C_n = \bigcup_{d \mid n} S_d$ i to je disjunktna unija, pa

$$n = |C_n| = \sum_{d \mid n} |S_d|.$$

Ako je $H_d < C_n$ podgrupa (jedina prema Teoremi 4) grupe C_n reda d, to je S_d skup generatora grupe H_d pa prema Teoremi 5,

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

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

2° $Aut\, C_n \cong \Phi_n$.
Zaista, $f \in Aut\, C_n$ u potpunosti je određen vrednošću $f(a)$, gde $C_n = \langle a \rangle$, jer $f(a^i) = f(a)^i$. S druge strane ako $C_n = \langle a \rangle$ onda $C_n = f(C_n) = \langle fa \rangle$ pa je fa generator grupe C_n.

Takođe, ako $C_n = \langle a \rangle$ onda za $k \in \Phi(n)$, preslikavanje $f: C_n \to C_n$ definisano sa

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

jeste automorfizam grupe C_n:

$$f(a^i \cdot a^j) = f(a^{i+j}) = f(a^{i +_n j}) = a^{k(i +_n j)} = a^{k \cdot_n (i +_n j)}$$

$$= a^{k \cdot_n i +_n k \cdot_n j} = a^{k \cdot_n i} \cdot a^{k \cdot_n j} = a^{ki} \cdot a^{kj} = f(a^i) f(a^j)$$

tj. f je homomorfizam, a da je 1-1 sledi iz činjenice da je $f(C_n) = C_n$.

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

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

Tada: a) F je 1-1 i na (prema prethodnom)

b) $F : \Phi(n) \to \mathrm{Aut}\, C_n$.

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

Tada $(f_k \circ f_l)(a) = (a^l)^k = a^{lk} = a^{l \cdot_n k} = f_s(a)$

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

$a^{lk} = a^{l \cdot_n k}$ jer $a^{l \cdot_n k} = a^{lk + dn} = a^{lk} \cdot a^{dn} = a^{lk} \cdot 1$

Dakle, F je 1-1 i na homomorfizam grupe $\Phi(n)$ na grupu $\mathrm{Aut}\, C_n$ pa $\Phi(n) \cong \mathrm{Aut}\, C_n$.

<u>Primer</u> Odrediti grupu $\mathrm{Aut}\, C_{12}$.

<u>Rešenje</u> $\mathrm{Aut}\, C_{12} \cong \Phi(12) = \Phi(3 \cdot 4) \cong \Phi(3) \times \Phi(4) \cong C_2 \times C_2$.

<u>Zadatak</u> Odrediti $\mathrm{Aut}\, C_{100}$

<u>Zadatak</u> Dokazati da $C_\infty \times C_\infty \not\cong C_\infty$ i uopšte $C_\infty^m \cong C_\infty^n$ akko $m = n$.

<u>Zadatak</u> Da li klasa cikličnih grupa obrazuje algebarski varijetet? Obrazložiti.

<u>Zadatak</u> Dokazati da je svaka ciklična grupa homomorfna slika grupe C_∞.

April 2000
Žarko Mijajlović

Abelove grupe

Grupa $\mathbb{G}$ je Abelova ako je komutativna, tj. ako za sve $x, y \in G$, $x \cdot y = y \cdot x$. U slučaju Abelovih grupa često se koristi aditivna notacija:

multiplikativna notacija	aditivna notacija
$\mathbb{G} = (G, \cdot, ^{-1}, 1)$	$\mathbb{A} = (A, +, -, 0)$
$x \cdot y = z$	$x + y = z$
$y = x^{-1}$, $z = x y^{-1}$	$y = -x$, $z = x - y$
$y = x^n$, $n \in \mathbb{Z}$	$y = nx$, $n \in \mathbb{Z}$
$y = x_1^{d_1} x_2^{d_2} \cdots x_k^{d_k}$	$y = d_1 x_1 + d_2 x_2 + \cdots + d_k x_k$ $(d_1, \ldots, d_k \in \mathbb{Z})$
$y = \prod_{i=1}^{n} x_i$	$y = \sum_{i=1}^{n} x_i$

Identiteti koji važe u svim grupama

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

$(x^m)^n = x^{mn}$	$n(mx) = (mn)x$
$x^{m+n} = x^m \cdot x^n$	$(m+n)x = (mx) + (nx)$
$(xy)^{-1} = y^{-1} x^{-1}$	$-(x+y) = (-y) + (-x)$

odnosno u slučaju Ab. grupa
$-(x+y) = (-x) + (-y)$

Identiteti koji važe u Abelovim grupama

$(xy)^{-1} = x^{-1} y^{-1}$	$-(x+y) = (-x) + (-y)$
$(xy)^m = x^m y^m$	$m(x+y) = mx + my$
$\prod_{i \in I} x_{p_i} = \prod_{i \in I} x_i$	$\sum_{i \in I} x_{p_i} = \sum_{i \in I} x_i$

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

Konstrukcije:

$G = H \cdot K$, $H, K < G$	$\mathbb{A} = B + C$, $B, C < \mathbb{A}$
$\mathbb{G}$ je unutrašnji proizvod podgrupa H, K; $G = HK$, $H \cap K = \langle 1 \rangle$	$\mathbb{A}$ je direktna suma podgrupa B i C; $\mathbb{A} = B \dot{+} C$, $B \cap C = \langle 0 \rangle$.

Primeri Abelovih grupa: $\mathbb{C}_n$, $(\mathbb{Z},+,0)$, $(\mathbb{Q},+,0)$, $(\mathbb{Q}\setminus\{0\},\cdot,1)$, ...
Primeri grupa koje nisu Abelove: $\mathbb{S}_n$ – grupa permutacija skupa $\{1,2,\dots,n\}$.
$\mathbb{D}_n$ – dijedarska grupa – grupa simetrija pravilnog n-tougla.

<u>Teorema</u> Abelove grupe čine algebarski varijetet.
Dakle, klasa Abelovih grupa zatvorena je za:
- podgrupe
- homomorfne slike
- operaciju proizvoda algebri
- konstrukciju količničke algebre.

<u>Napomena</u> 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 definisana količnička grupa G/H.

<u>Teorema o razlaganju konačno-generisanih Abelovih grupa</u>

Ciklične grupe su Abelove grupe. Dakle za ma koje $n_1,\dots,n_k \in N^+$, $\mathbb{C}_{n_1}\times\mathbb{C}_{n_2}\times\dots\times\mathbb{C}_{n_k}$ 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.

Pre no što izložimo dokaz ove teoreme, dokazaćemo nekoliko pomoćnih tvrđenja – lema koje su od nezavisnog interesa.

<u>Lema 1</u> 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. $NZD(a_1,a_2,\dots,a_n)=1$. Tada postoji kvadratna matrica M reda n nad $\mathbb{Z}$ takva da je $\det M = 1$.

<u>Dokaz</u> izvodimo indukcijom po n.

<u>Slučaj $n=2$</u> Neka su $a_1,a_2\in\mathbb{Z}$, $(a_1,a_2)=1$. Prema Bezuovoj teoremi postoje $\alpha,\beta\in\mathbb{Z}$ takvi da je $\alpha a_1+\beta a_2=1$. Otuda za
$M=\begin{bmatrix} a_1 & a_2 \\ -\beta & +\alpha \end{bmatrix}$ važi $\det M = 1$.

Pretpostavimo IH, da tvrđenje 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 $\mathbb{Z}$)

$$M = \begin{bmatrix} b_1 & b_2 & \cdots & b_{n-1} \\ & & * & \end{bmatrix}$$

reda $n-1$, t.d. $\det M = 1$.

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

$$M' = \begin{bmatrix} a_1 & a_2 & \cdots & a_{n-1} & a_n \\ & & * & & 0 \\ & & & & \vdots \\ & & & & 0 \\ \varepsilon t b_1 & \varepsilon t b_2 & \cdots & \varepsilon t b_{n-1} & s \end{bmatrix}$$

gde je $\varepsilon \in \{1, -1\}$ i gde će se tačna vrednost za ε odrediti kasnije.

Dakle, M' je reda n i važi:

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

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

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

<u>Posledica 1</u> (uopštenje Bezuove teoreme) Neka su $a_1, \dots, a_n \in \mathbb{Z}$ takvi da je $(a_1, a_2, \dots, a_n) = 1$. Tada diofantovska jednačina

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

ima rešenje (u $\mathbb{Z}$).

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

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

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

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

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

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

Partikularno rešenje: Rešavajući ove jednačine u $\mathbb{Z}_6$ nalazimo $4y+3z=1$, odakle, $y_0=1$, $z_0=-1$, te iz polazne jednačine, $x_0=1$, tj. partikularno rešenje je $x_0=1$, $y_0=1$, $z_0=-1$.

Sada rešavamo homogenu jednačinu

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

odakle $6X+10Y=-15Z$. Ova jednačina ima rešenje (prema B.T.) akko $2|Z$. Neka je $Z=2\alpha$. Tada se poslednja jednačina svodi na $3X+5Y=-15\alpha$. Opšte rešenje ove jednačine je

$X=-30\alpha+5\beta$, $Y=15\alpha-3\beta$, $\alpha,\beta\in\mathbb{Z}$, pa je opšte rešenje polazne jednačine: $x=1-30\alpha+5\beta$, $y=1+15\alpha-3\beta$, $z=-1+2\alpha$. ▨

Lema 2 Neka je $\mathbb{A}=(A,+,0)$ Abelova grupa i pp da je $\mathbb{A}$ generisana sa n elemenata ($n\in N^+$), tj. postoje $x_1,\dots,x_n\in A$ takvi da je $\mathbb{A}=\langle x_1,x_2,\dots,x_n\rangle$. 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 postoje $y_2,\dots,y_n\in A$ takvi da je $\mathbb{A}=\langle y_1,y_2,\dots,y_n\rangle$.
(Lema o promeni baze).

Dokaz Neka je prema Lemi 1, $M=\begin{bmatrix} a_1 & a_2 & \dots & a_n \\ & * & \end{bmatrix}$, $\det M=1$ 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 $\det M=1$, $M^{-1}=\frac{1}{\det M}\cdot\operatorname{adj}(M)$ to je i matrica M^{-1} celobrojna! Otuda

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

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

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

Dokaz teoreme o razlaganju konačno generisanih Abelovih grupa. Dokaz izvodimo indukcijom po $\text{rang}\, A$. Koristimo aditivnu notaciju, dakle dokazujemo da je konačno generisana Abelova grupa $\mathbb{A} = (A, +, 0)$ direktna (konačna) suma cikličnih grupa.

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

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

a) postoje $x_1, \dots, x_n \in A$ takvi da $\mathbb{A} = \langle x_1, \dots, x_n \rangle$ i bar jedan od elemenata $x_1, \dots, x_n$ je konačnog reda.

b) Ako je $\mathbb{A} = \langle x_1, \dots, x_n \rangle$, 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 $\mathbb{A} = \langle x_1, \dots, x_n \rangle$ i $\{x_1, \dots, x_n\}$ sadrži element x najnižeg reda u odnosu na sve generatorske skupove $\{y_1, \dots, y_n\}$ grupe $\mathbb{A}$, tj. ako $\mathbb{A} = \langle y_1, \dots, y_n \rangle$ onda $\text{red}\, x \le \text{red}\, y_1, \dots, \text{red}\, y_n$.
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 $\text{rang}\, \mathbb{A} < n$. Dakle, po induktivnoj hipotezi $\mathbb{H}$ je direktna suma (konačna) cikličnih grupa, a takođe i grupa $\mathbb{K}$ je ciklična. Prema tome dosta je da dokažemo da je $\mathbb{A}$ direktna suma grupa $\mathbb{H}$ i $\mathbb{K}$, tj. $\mathbb{A} = \mathbb{H} \dotplus \mathbb{K}$.
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 neko $d_n \in \mathbb{Z}_g$ 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 postoje $v_2, \dots, v_n$ takvi da je $\mathbb{A} = \langle v, v_2, \dots, v_n \rangle$.

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

red $v \le d \le d_n <$ red x_n

što je kontradikcija prema izboru elementa x_n: da je x_n najmanjeg reda u svim generatorskim skupovima od n elemenata grupe $\mathbb{A}$.

Dakle, $\mathbb{H} \cap \mathbb{K} = \langle 0 \rangle$ pa $\mathbb{A} = \mathbb{H} \dotplus \mathbb{K}$, te je $\mathbb{A}$ konačna direktna suma cikličnih grupa, odnosno $\mathbb{A}$ je izomorfna konačnom proizvodu cikličnih grupa.

Slučaj b: Svaki element u svakom generatorskom skupu od n elemenata grupe $\mathbb{A}$ je beskonačnog reda. U tom slučaju dokazuje se da je $\mathbb{A} \cong \mathbb{Z}^n = (\mathbb{Z}, +, 0)^n$. ▨

Posledica 1 Svaka konačna Abelova grupa izomorfna je (konačnom) proizvodu cikličnih grupa.

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

Primer Opisati do na izomorfizam sve Abelove grupe reda 100.

Rešenje: $100 = 2^2 \cdot 5^2$, pa uzimajući u obzir prethodnu teoremu, Langranžeovu teoremu o podgrupama i Teoremu 3c kod cikličnih grupa, nalazimo sledeće Abelove grupe reda 100:

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

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 izomorfne.

Zadatak Opisati do na izomorfizam sve grupe reda 150.

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

Dokaz. Prema teoremi o dekompoziciji k.g. Abelovih grupa, A je proizvod cikličnih grupa: $A = C_{n_1} \times \dots \times C_{n_k}$. Tada za neki $1 \le i \le k$, $p \mid n_i$. Ako je $C_{n_i} = \langle a \rangle$, tada je $a^{\frac{n_i}{p}}$ element reda p u A. ∎

Posledica 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 ciklična grupa.

Dokaz. Prema teoremi o reprezentaciji k.g. Abelovih grupa, G je kon. proizvod cikličnih grupa. Ako je G nije ciklična, onda postoje ciklične grupe $H, K < G$ t.d. $H \cap K = \langle 1 \rangle$ i redovi ovih grupa nisu uzajamno prosti, tj. $(|H|, |K|) > 1$. Neka je p prost broj t.d. $p \mid (|H|, |K|)$. Tada postoji $a \in H$, $b \in K$ t.d. red $a = p$, red $b = p$ i $\{1, a, \dots, a^{p-1}\} \cap \{1, b, \dots, b^{p-1}\} = \{1\}$, tj: $\langle a \rangle \cap \langle b \rangle = \langle 1 \rangle$. Neka je $S = \{1, a, \dots, a^{p-1}, b, b^2, \dots, b^{p-1}\}$. Tada za $x \in S$, $x^p = 1$, pa jednačina $x^p - 1 = 0$ ima $|S| = 2p - 1 > p$ rešenja, suprotno činjenici da polinom stepena p u polju može imati najviše p rešenja. Dakle, G je ciklična. ∎

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

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

Zadatak. Neka je p prost broj. Dokazati da je Ojlerova grupa $\Phi(p)$ ciklična.

Zadatak. Neka je A Abelova grupa reda n i neka $k \mid n$, $k, n \in N$. Dokazati da A sadrži podgrupu reda k.

Abelove grupe sa deljenjem

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

Primer 1° $(Q, +, 0)$ je Ab. grupa sa deljenjem.

2° $(R, +, 0)$ je Ab. grupa sa deljenjem.

Osobine Abelovih grupa sa deljenjem

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

Dokaz. 1. Neka je A Ab. grupa sa deljenjem, $h : A \xrightarrow{na} \mathbb{B}$.
Da li je jednačina $n \cdot x = b$, $n \in N^+$, $b \in B$, moguće rešiti u $\mathbb{B}$?
Neka je $a \in A$ t.d. $h(a) = b$ (h je na!), i neka je $d \in A$ t.d. $n \cdot d = a$ ($\mathbb{A}$ je Ab. grupa sa deljenjem!). Tada $h(nd) = h(a)$, tj. $n\,h(d) = b$, tj. $h(d)$ je rešenje jedn. $nx = b$.

2. Neka su $\mathbb{A}, \mathbb{B}$ Ab. grupe sa deljenjem i neka su $(a, b) \in A \times B$.
Neka su $a' \in A$, $b' \in B$ takvi da $n \cdot a' = a$, $n \cdot b' = b$, $n \in N^+$.
Tada je (a', b') rešenje jedn. $n \cdot (x, y) = (a, b)$ u $A \times \mathbb{B}$. ☒

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

Teorema Neka je $\mathbb{A} = (A, +, 0)$ Ab. grupa sa deljenjem i bez torzije.
Onda je $\mathbb{A}$ vektorski prostor nad poljem racionalnih brojeva $\mathbb{Q} = (Q, +, \cdot, 0, 1)$.

Dokaz Neka je $\mathcal{A} = (\mathbb{A}, Q, \cdot)$ gde je operacija množenja vektora $a \in A$ i skalara $t \in Q$, $t = \frac{p}{q}$, $p, q \in Z$, definisano na sledeći način:

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

tj. b je rešenje jednačine $qx = pa$.

Primetimo da je ovako određeno b jedinstveno. Naime, ako je $qb' = pa$, onda $q(b - b') = 0$ pa $b = b'$ jer je $\mathbb{A}$ grupa bez torzije. Dakle operacija množenja vektora i skalara je dobro definisana.
Ostalo je da se dokažu sledeće aksiome:

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

d) $(\alpha\beta)x = \alpha(\beta x)$.

Dokažimo, na primer, (d): Najpre primetimo da za $n\in Z\setminus\{0\}$ važi:

$$nx = ny \Rightarrow x=y,\quad x,y\in A.$$

Dalje, neka je $z = \alpha(\beta x) = \frac{p}{q}\left(\frac{p'}{q'}x\right)$. Tada $qz = py$, gde je $y = \frac{p'}{q'}\cdot x$. Odavde $q'(qz) = q'(py)$, pa $(qq')z = p(q'y) = p(p'x)$ tj. $(qq')z = (pp')x$, odakle $z = \frac{pp'}{qq'}\cdot x = (\alpha\beta)x$ tj:

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

$p,p'\in Z$, $q,q'\in N^+$. Ovde smo koristili da je za $m,n\in Z$

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

na primer za $m,n\in N^+$: $m(nx) = (mn)x = \underbrace{x+x+\dots+x}_{mn \text{ sabiraka}}$.

Slično se dokazuju identiteti (b) i (c).

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

Teorema Neka je $\dim A = n$. Tada $A\cong (Q^n,+,0)$, odnosno

$$A = A_1 \dotplus A_2 \dotplus \dots \dotplus A_n, \text{ gde } A_i \cong (Q,+,0),\ 1\le i\le n.$$

Važi i opštije, ako je $\dim A = \kappa$, $\kappa\in CARD$, onda

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

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

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

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

Zadatak a) Odrediti (opisati) $Aut(Q,+,0)$, b) $Aut(R,+,0)$.

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

6 Lema 1° Neka su A i 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 neka je za sve $x,y\in S$, $xy = yx$. Tada je G Abelova.

Dokaz 1°. Neka je $f: A\times B \to AB$ definisano sa
$$f:(a,b)\mapsto ab,\quad (a,b)\in A\times B.$$

Prema teoremi o razlaganju homomorfizma imamo sledeći komutativan dijagram (D)

$$\begin{tikzcd} A\times B \arrow[r, "na", "f"'] \arrow[d, "k"'] & AB \\ A\times B/\sim \arrow[ur, "\cong"'] & \end{tikzcd}$$

Ovde je $\sim$ jezgro preslikavanja f, tj. relacija ekvivalencije skupa $A\times B$ definisana sa: $(a_1,b_1)\sim(a_2,b_2)$ akko $f(a_1,b_1) = f(a_2,b_2)$.

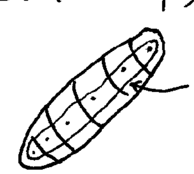
Kako je
$$\begin{aligned}(a_1,b_1)\sim(a_2,b_2) &\Leftrightarrow a_1b_1 = a_2b_2\\ &\Leftrightarrow a_2^{-1}a_1 = b_2b_1^{-1}\\ &\Leftrightarrow (\exists t\in A\cap B)(a_2^{-1}a_1 = t \wedge b_2b_1^{-1} = t)\\ &\Leftrightarrow (\exists t\in A\cap B)(a_1 = a_2t \wedge b_2 = tb_1),\end{aligned}$$

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

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

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

(2) $A\times B = \bigcup\limits_{(a,b)\in T} (a,b)/\sim$, T je transverzala (izborni skup) particije $A\times B/\sim$.


T

Transverzala T ima tačno onoliko elemenata koliko ima klasa ekvivalencije, te prema (D), $|T| = |AB|$. Tada iz (2) nalazimo

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

2° a) Neka je $H < Z(G)$. Tada za proizvoljno $g \in G$,

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

jer 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 ciklička. Primetimo da je prema (a) G/H dobro definisana grupa. Kako je G/H ciklička postoji $a \in G$ tako da je $G/H = \langle aH \rangle$. Ako je G/H konačna ciklička grupa onda $G/H = \{H, aH, a^2H, \dots, a^{n-1}H\}$, gde su a^iH, $0 \le i < n$, disjunktni koseti grupe G i onda $G = H \cup aH \cup \dots \cup a^{n-1}H$. Neka su $x, y \in G$. Tada postoje $0 \le i, j \le n-1$, $h_1, h_2 \in H$ takvi 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 $a^i \cdot a^j = a^{i+j} = a^{j+i} = a^j \cdot a^i$, 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 ciklička grupa, onda $G/H = \{\dots, a^{-2}H, a^{-1}H, H, aH, a^2H, \dots\}$ i $G = \bigcup_{n \in \mathbb{Z}} a^n H$, i dokaz da je za $x, y \in G$, $xy = yx$, izvodi se na isti način.

3° 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. $abab = e$, odakle, $abab^2 = eb$ tj. $aba = b$, pa $aba^2 = ba$, tj. $ab = ba$.

4° 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. $H \trianglelefteq G$.

5° 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 $m, n \in N$, važi $x^m y^n = y^n x^m$.
Ovo tvrđenje lako se dokazuje indukcijom po m, n.

b) Iz (a) sledi, množenjem sa x^{-m}, odnosno y^{-n}:

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

Dakle, za sve $x, y \in S$, $\alpha, \beta \in Z$

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

Neka su $u, v \in G$. Tada $u, v \in \langle S \rangle$, te postoje $x_1, \dots, x_m \in S$, $\alpha_1, \dots, \alpha_m \in Z$ i $y_1, \dots, y_n \in S$, $\beta_1, \dots, \beta_n \in Z$ takvi da je

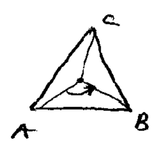
$$u = x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_m^{\alpha_m}, \qquad v = y_1^{\beta_1} y_2^{\beta_2} \cdots y_n^{\beta_n}.$$

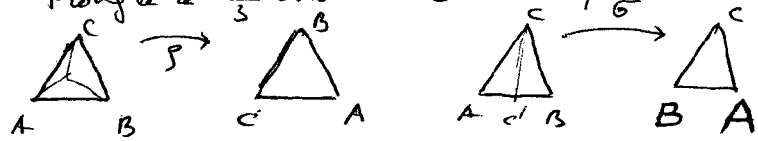
Tada, koristeći (1) nalazimo

$$xy = x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_m^{\alpha_m} y_1^{\beta_1} y_2^{\beta_2} \cdots y_n^{\beta_n} = \cdots = y_1^{\beta_1} \cdots y_n^{\beta_n} x_1^{\alpha_1} \cdots x_m^{\alpha_m} = v \cdot u.$$

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

Dokaz Postoji bar jedna takva grupa, to je $S_3 \cong D_3$
(S_3 - grupa permutacija skupa $\{1,2,3\}$; D_3 - dijedarska grupa trougla). $D_3 = \langle \rho, \sigma \rangle$, ρ = rotacija pravilnog trougla za $\frac{2\pi}{3}$ oko centra medijana ΔABC.





σ - refleksija u odnosu na osu cc'

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

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

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

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

Otuda $G = AB$, gde $A = \langle a \rangle$, $B = \langle b \rangle$, te 4

$$|G| = |AB| = \frac{|A||B|}{|A \cap B|} = \frac{3 \cdot 2}{1} = 6$$

jer prema Lagranževoj teoremi $|A \cap B| \mid |A|, |B|$ tj. $|A \cap B| \mid 2, 3$ pa $|A \cap B| = 1$. Otuda

(2) $G = \{1, a, a^2, b, ab, a^2 b\}$, pa $G \cong S_3$, odnosno $G \cong D_3$

Dejstvo grupe na skup

Algebarska notacija slaganja funkcija:

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[dr, dashed, "g\circ f"'] & B \arrow[d, "g"] \\ & C \end{tikzcd} \quad h = g\circ f \quad (g\circ f)(x) = g(f(x))$$

skupovna notacija

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[dr, dashed, "fg"'] & B \arrow[d, "g"] \\ & C \end{tikzcd} \quad h = fg \quad h(x) = (fg)(x) = g(f(x))$$

algebarska notacija

Neka je G grupa i S neki neprazan skup.
Dejstvo grupe G na skup S je svaki homomorfizam
$$\theta : G \longrightarrow \$ym(S)$$
gde je $\$ym(S) = (Sym(S), \cdot, i_S)$ simetrična grupa (grupa permutacija) skupa S u algebarskoj notaciji. i_S je identičko preslikavanje skupa S. Dakle,

$\theta(e) = i_S$,

$\theta(gh) = \theta(g)\theta(h)$ za $g, h \in G$; i za $s \in S$:

$\theta(g) : S \xrightarrow[1-1]{na} S$; $\quad (\theta(g)\theta(h))(s) = \theta(h)(\theta(g)(s))$

Relacija ekvivalencije dejstva θ. Ukoliko je u datom razmatranju dejstvo θ fiksirano, umesto $\theta(g)(s)$ pišemo s^g (ako je grupa data u multiplikativnoj notaciji), odnosno gs (ako je grupa G data u aditivnoj notaciji i, naravno, G je Abelova).

Lema 1 $\quad 1°\ s^e = s, \quad 2°\ (s^g)^h = s^{gh}$.

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

$2°\ (s^g)^h = \theta(h)(\theta(g)(s)) = (\theta(g)\theta(h))(s) = \theta(gh)(s) = s^{gh}$.

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

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

Lema 2 $\quad G_s < G$.

Dokaz $\quad 1°\ e \in G_s$ jer $s^e = s$. $2°$ Ako $g, h \in G_s$ onda $s^{gh} = (s^g)^h = s^h = s$ pa $gh \in G_s$. Takođe, iz $s^g = s$ sledi $(s^g)^{g^{-1}} = s^{g^{-1}}$ tj. $s^{gg^{-1}} = s^{g^{-1}}$ pa $s^{g^{-1}} = s^e = s$, tj. $g^{-1} \in G_s$.

<u>Relacija ekvivalencije dejstva θ</u>. Neka je relacija $\sim$ skupa S definisana ovako:

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

<u>Lema 3</u> Relacija $\sim$ je relacija ekvivalencije skupa S.

<u>Dokaz</u> (R) $s \sim s$ jer $s^e = s$.

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

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

$u = (s^g)^h = s^{gh}$ tj. $s \sim u$. ▨

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

$$s/_\sim = s^G = \{ s^g \mid g \in G \}.$$

<u>Lema 4</u> Neka je $s \in S$. Tada $|s^G| = |G : G_s|$.

<u>Dokaz</u> 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 koseta biće grupa akko $G_s \lhd G$).

Dalje, za $g, h \in G$ važi:

$$s^g = s^h \iff s^{gh^{-1}} = s \iff gh^{-1} \in G_s \iff G_s gh^{-1} = G_s$$
$$\iff G_s g = G_s h$$

Dakle, preslikavanje $\Phi : s^G \to G/G_s$ definisano sa

$$\Phi : s^g \mapsto G_s \cdot g$$

je dobro definisano i jeste 1-1. Očigledno Φ je <u>na</u>, pa

$|s^G| = |G/G_s| = |G : G_s|$. ▨

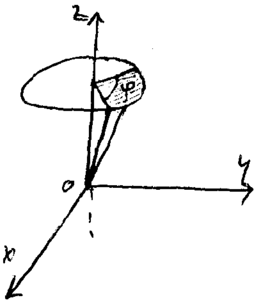
<u>Klasovna jednakost</u> Neka grupa G dejstvuje na skup S. Tada se S može predstaviti kao disjunktna unija orbita

$$S = \bigcup_{s \in T} s^G \quad , T \text{ je transverzala particije } \{ s^G \mid s \in S \}$$

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

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

Primer 1. Neka je $\mathbb{G} = (R,+,0)$, $S = R^3$



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

Tada $\theta(\varphi_1+\varphi_2) = \theta(\varphi_1)\theta(\varphi_2)$, pa je θ dejstvo (očigledno $\theta(0) = i_{R^3}$).

Za $M \in R^3$, $G_M = \{2\pi k \mid k \in Z\} \cong \mathbb{Z}$,

dok je orbita tačke M (ako $M \notin$ z-osi)

M^G = kružnica sa centrom na z-osi; leži u ravni paralelnoj oxy-ravni.

$\ker\theta = \{2\pi k \mid k \in Z\} \cong \mathbb{Z}$.

Primer 2. $G = (R,+,0)$, $S = P(R^3) = \{X \mid X \subseteq R^3\}$

Za $\bar\theta : G \to \mathrm{Sym}(S)$, $\bar\theta(X) = \theta[X]$, gde je θ preslikavanje iz prethodnog primera.

Za pogodno izabranu kružnicu $K \in P(R^3)$, orbita kružnice K biće torus (može biti i sfera).

Primer 3. Neka je G grupa, i $\sigma : G \to \mathrm{Sym}(G)$ definisano sa $\sigma(g)(x) \overset{def}{=} \sigma_g(x) = g^{-1}xg$, $g, x \in G$. Tada

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

pa $\sigma(gh) = \sigma_g \sigma_h$ tj. σ je dejstvo grupe G na domen G te grupe. Tada

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

tj. stabilizator el. x je njegov centralizator.

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

c) $\ker\theta = \{g \in G \mid \theta(g) = i_S\} = \{g \in G \mid (\forall s \in S)\ s^g = s\}$

$= \bigcap_{s \in S} G_s$ tj. za proizvoljno dejstvo $\theta : G \to \mathrm{Sym}\, S$

$\ker\theta = \bigcap_{s \in S} G_s$. Specijalno za dejstvo σ

$\ker\sigma = \bigcap_{x \in G} C(x) = Z(G)$. Primetimo da $x \in Z(G)$ akko $C(x) = G$

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

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

Dakle, klasovna jednakost u ovom slučaju izgleda

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

p-grupe

Konačna grupa G je p-grupa, gdje je p prost broj, ako je $red(G) = p^n$ za neki $n \in N^+$. Dakle, 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 netrivijalni centar.

Dokaz Ako $x \notin Z(G)$, onda je $C(x)$ prava podgrupa grupe G, pa je u tom slučaju $|G : C(x)| = p\cdot\alpha$ za neki $\alpha \in N$, jer $|G : C(x)|$ dijeli $red(G) = p^n$. Odatle iz klasovne jednakosti nalazimo

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

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

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

Posledica Svaka p-grupa ima element reda p.

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

Grupe reda p^2, $p \in Prost$ Postoje dve grupe reda p^2. To su C_{p^2} i $C_p^2 = C_p \times C_p$. Kao što ćemo videti, drugih grupa reda p^2 nema. Neka je $red(G) = p^2$ i neka je $a \in Z(G)$, $red(a) = p$, taj element postoji prema prethodnoj posledici. Tada $\langle a \rangle \triangleleft G$ te $|G/\langle a\rangle| = p$, pa je $G/\langle a \rangle$ ciklično. Prema 6 lema G je Abelova, tj. G je izomorfna C_{p^2} ili C_p^2. $\boxtimes$

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

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