Ciklične grupe i neke osobine podgrupa

Definicija ($\langle a \rangle$)

Za svaki element a iz grupe G, definirimo $\langle a \rangle$ na sljedeći način

$$\langle a \rangle = \{ a^n \mid n \in \mathbb{Z} \}.$$

Primjetimo da eksponent od a uključuje sve negativne cijele brojeve, kao i nulu, i sve pozitivne cijele brojeve (prema definiciji a^0 je identitet).

(#) Neka je G grupa i neka je a proizvoljan element grupe G. Pokazati da je $\langle a \rangle$ podgrupa grupe G.

Rj:

Primjetimo da je $a \in \langle a \rangle$ tj. $\langle a \rangle$ je neprazno

ZATVORENOST

$a^n, a^m \in \langle a \rangle \Rightarrow a^n \cdot a^m = a^{n+m} \in \langle a \rangle$

. Isto tako primjetimo da je $a^n \cdot (a^m)^{-1} = a^{n-m} \in \langle a \rangle$

ASOCIJATIVNOST

Operacija u $\langle a \rangle$ je ista kao i operacija od G iz čega slijedi množenje je asocijativno.

NEUTRALNI ELEMENT

$\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$ a prema definiciji $a^0 = e$

$\Rightarrow e \in \langle a \rangle$ (e je jedinični element iz G)

INVERZNI ELEMENT

Primjetimo da za $\forall a^n \in \langle a \rangle$ $a^n \cdot a^{-n} = a^0 = e$

$a^{-n} \cdot a^n = a^0 = e$

a^{-n} je inverz od a^n ($a^{-n} \in \langle a \rangle$).

$\langle a \rangle$ je podgrupa grupe G.

(#) Skup $U(10) = \{k \in \mathbb{N} \mid k < 10, \gcd(k, 10) = 1\}$ formira grupu u odnosu na operaciju množenja modulo 10. Izračunati $\langle 3 \rangle$.

Rj.

$U(10) = \{1, 3, 7, 9\}$

$\langle 3 \rangle = \{3^n \mid n \in \mathbb{Z}\}$

$3^0 = 1$

$3^2 = 9$

$3^3 = 7$

$3^4 = 3^3 \cdot 3 = 1$

$3^5 = 3^4 \cdot 3 = 1 \cdot 3 = 3$

$3^6 = 3^4 \cdot 3^2 = 9$

$\vdots$

$3^{-1} = 7$

$3 \cdot 3^{-1} = 1$

$3 \cdot x = 1$

$x = 7$

$3^{-2} = 9$

$3^2 3^{-2} = 1$

$9 \cdot x = 1$

$x = 9$

$3^{-3} = 3$

$3^3 \cdot 3^{-3} = 1$

$7 \cdot x = 1$

$x = 3$

$\vdots$

$\langle 3 \rangle = \{1, 3, 7, 9\}$

(#) Data je grupa $(\mathbb{Z}_{10}, +)$. Odrediti $\langle 2 \rangle$.

Rj:

$\mathbb{Z}_{10} = \{0, 1, 2, \ldots, 9\}$

Operacija u grupi $\mathbb{Z}_{10}$ je sabiranje.

$\langle 2 \rangle = \{ n \cdot 2 \mid n \in \mathbb{Z} \}$

a^n je oblika na u aditivnoj grupi

$1 \cdot 2 = 2$

$2 + 2 = 4$

$3 \cdot 2 = 6$

$4 \cdot 2 = 8$

$5 \cdot 2 = 0$

$6 \cdot 2 = 2$

$\vdots$

$(-1) \cdot 2 = 8$

$2 + (-2) = 0$

$2 + x = 0$

$x = 8$

$(-2) \cdot 2 = 6$

$4 + 2 \cdot (-2) = 0$

$4 + x = 0$

$x = 6$

$\vdots$

$\langle 2 \rangle = \{0, 2, 4, 6, 8\}$.

(#) Data je grupa $(\mathbb{Z}, +)$. Odrediti $\langle -1 \rangle$.

Rj.

$$\langle -1 \rangle = \{ n \cdot (-1) \mid n \in \mathbb{Z} \}$$

$0 \cdot (-1) = 0$
$1 \cdot (-1) = -1$
$2 \cdot (-1) = -2$
$3 \cdot (-1) = -3$
$4 \cdot (-1) = 4$
$\vdots$

$(-1) \cdot (-1) = 1$
$(-2)(-1) = 2$
$(-3)(-1) = 3$
$(-4)(-1) = 4$
$\vdots$

$$\langle -1 \rangle = \mathbb{Z}$$

Definicija

Podgrupa $\langle a \rangle$ nazivamo ciklička podgrupa od G generisana sa a. U slučaju kada je $G = \langle a \rangle$, kažemo da je G ciklička grupa i da je a generator od G. (Ciklička grupa može imati više generatora). Primetimo da iako niz $\ldots, a^{-2}, a^{-1}, a^0, a^1, a^2, \ldots$ ima beskonačno mnogo elemenata, može se desiti da skup $\{a^n \mid n \in \mathbb{Z}\}$ ima samo konačno mnogo elemenata. Također primetite da kako je $a^i a^j = a^{i+j} = a^{j+i} = a^j a^i$ svaka ciklička grupa je Abelova.

(#) Skup $G = \{I, A, B, AB, BA, ABA\}$ zajedno sa operacijom množenja formira grupu, čija je Cayley-eva tabela

	I	A	B	AB	BA	ABA
I	I	A	B	AB	BA	ABA
A	A	I	AB	B	ABA	BA
B	B	BA	I	ABA	A	AB
AB	AB	ABA	A	BA	I	B
BA	BA	B	ABA	I	AB	A
ABA	ABA	AB	BA	A	B	I

(a) Odrediti sve ciklične podgrupe grupe G. Za svaku podgrupu, ispišite sve moguće generatore.

(b) Za svako $g \in G$, izračunati $|g|$. Objasniti svoje zaključke.

Rj.

(a) $\langle I \rangle = \{I\}$

$A \cdot A = I \qquad \langle A \rangle = \{I, A\}$

$B \cdot B = I \qquad \langle B \rangle = \{I, B\}$

$AB \cdot AB = BA$

$AB \cdot BA = I$

$\langle AB \rangle = \{I, AB, BA\} = \langle BA \rangle$

isto dobijemo i za BA

$ABA \cdot ABA = I$

$\langle ABA \rangle = \{I, ABA\}$

(b) Iz dijela pod (a) vidimo

$|I| = 1$

$|A| = 2 \qquad |AB| = 3$

$|B| = 2 \qquad |BA| = 3$

$|ABA| = 1$.

Ciklične podgrupe grupe G su $\langle I \rangle = \{I\}$, $\langle A \rangle = \{I, A\}$, $\langle B \rangle = \{I, B\}$, $\langle AB \rangle = \langle BA \rangle = \{I, AB, BA\}$ i $\langle ABA \rangle = \{I, ABA\}$

(#) Data je grupa G, i data su dva elementa $a, b \in G$ koja imaju osobinu $|a|=4$ i $|b|=2$. Ako je $a^3b=ba$ odrediti red od ab.

Rj.

$|a|=4 \Rightarrow a^4=e$

$$\left.\begin{array}{l} a^3\cdot a=e \\ a\cdot a^3=e \end{array}\right\} \Rightarrow a^{-1}=a^3$$

$$a^2\cdot a^2=e \Rightarrow (a^2)^{-1}=a^2$$

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

$|b|=2 \Rightarrow b^2=e$

$$b\cdot b=e \Rightarrow b^{-1}=b$$

$a^3b=ba \quad / \cdot a$ sa lijeve strane

$\underbrace{a^4}_{=e}b=aba$

$b=aba \quad / \cdot b$ sa desne strane

$\underbrace{b\cdot b}_{=e}=abab$

$e=(ab)^2 \Rightarrow |ab|=2$

(#) Neka je G data grupa i neka su $a, b \in G$ elementi grupe G za koje vrijedi $|a|=4$ i $|b|=2$. Objasniti zašto slučaj $a^2b = ba$ nije moguć.

Rj:

$|a|=4 \Rightarrow a^4 = e,\ a^3 = a^{-1},\ a^{-2} = a^2$

$|b|=2 \Rightarrow b^2 = e,\ b^{-1} = b$

Ako bi vrijedilo da je $a^2b = ba$ tada imamo sljedeće

$a^2b = ba$

$a^2 \underbrace{b \cdot b}_{=e} = bab$

$a^2 = bab$ / $\cdot a$ sa lijeve strane

$a^3 = abab$

$abab = a^3$ / $\cdot a$ sa desne str.

$bab = e$ ...(1)

$abab = a^3$

$abab = a^{-1}$ / $\cdot a$ sa lijeve str.

$a^2bab = e$ / $\cdot a^2$ sa lijeve str.

$bab = a^2$ ...(2)

(1) i (2) $\Rightarrow$ $a^2 = e$

#kontradikcija

Pretpostavka suprotna tvrdnji nas vodi u kontradikciju pa nije tačna. Slučaj $a^2b = ba$ nije moguć.

(#) Data je grupa $(\mathbb{Q}, +)$. Pokazati da ova grupa nije ciklička.

Rj.

Pretpostavimo suprotno tvrdnji tj. pretpostavimo da je $\mathbb{Q}$ ciklička grupa. Tada se ona može generisati racionalnim brojem oblika $\frac{a}{b}$ gdje su $a, b \in \mathbb{Z}$.

Tada skup $\langle \frac{a}{b} \rangle$ sadrži sve višekratnike od $\frac{a}{b}$. Pa ako je $\mathbb{Q} = \langle \frac{a}{b} \rangle$ tada $\frac{a}{2b}$ mora biti cijeli višekratnik od $\frac{a}{b}$. Ali ako

$$c\frac{a}{b} = \frac{a}{2b}$$

tada je $c = \frac{1}{2}$ što nije cijeli broj. Time $\mathbb{Q}$ ne može biti generisan jednim racionalnim brojem, pa $\mathbb{Q}$ nije ciklička grupa.

(#) Neka je G grupa i neka je H neprazan podskup od G. Pokazati da ako je $ab^{-1} \in H$ za proizvoljna $a, b \in H$ tada je H podgrupa grupe G.

R.j.

ASOCIJATIVNOST

Kako je operacija od H ista kao i operacija od G, i kako je $H \subseteq G$, operacija je asocijativna

NEUTRALNI ELEMENT

Kako je H neprazan, možemo izabrati neki $x \in H$. Tada stavljajući $a = x$ i $b = x$ u hipotezu, imamo

$$e = xx^{-1} = ab^{-1} \in H$$

INVERZNI

Da provjerimo da je $x^{-1} \in H$ kadgod je $x \in H$, sve što trebamo uraditi je da izaberemo $a = e$ i $b = x$ i primjenimo tvrdnju iz teksta zadatka

ZATVORENOST

Dokaz će biti gotov ako još pokažemo da je H zatvoren, tj. trebamo pokazati da ako $x, y \in H$ tada imamo $xy \in H$. Već smo pokazali da ako je $y \in H$ tada $y^{-1} \in H$, pa stavljajući $a = x$, $b = y^{-1}$ imamo

$$xy = x(y^{-1})^{-1} = ab^{-1} \in H$$

(#) Neka je G grupa i neka je H neprazan podskup od G. Pokazati da ako je ab u H kadgod su a i b u H (ako je H zatvoren u odnosu na operaciju), i ako je $a^{-1} \in H$ za proizvoljno $a \in H$ (ako je H zatvoren u odnosu na uzimanje inverza) tada je H podgrupa od G.

Rj.

Prema prethodnom zadatku dovoljno je da pokažemo da ako su $a, b \in H$ tada $ab^{-1} \in H$.

Pa izaberimo proizvoljna dva $a, b \in H$. Kako je H zatvoren u odnosu na uzimanje inverza imamo da je $b^{-1} \in H$.

Time $ab^{-1} \in H$ prema zatvorenosti u odnosu na operaciju množenja.

Napomena

Prema prethodnom zadatku da bi pokazali da je H podgrupa grupe G dovoljno je da pokažemo da je $H \neq \emptyset$, da je H zatvoren te da $\forall a \in H$ imamo $a^{-1} \in H$ (da svaki a iz H ima inverz u H).

Prema prvom zadatku da bi pokazali da je H podgrupa grupe G dovoljno je da pokažemo da je $H \neq \emptyset$ te da $\forall a, b \in H$ $ab^{-1} \in H$.

(#) Neka je G Abelova grupa. Pokazati da je

$$H = \{x \in G \mid |x| \text{ je konačno}\}$$

podgrupa grupe G.

R.j.

Primjetimo da je $e^1 = e \Rightarrow H \neq \emptyset$ $(e \in H)$.

Možemo primjeniti tvrdnju prethodnog zadatka i samo pokazati da $\forall a, b \in H$ vrijedi $ab \in H$ i da $a^{-1} \in H$.

ZATVORENOST

$a, b \in H$ i neka je $|a| = m$, $|b| = n$

Kako je G abelova $(ab)^{mn} = (a^m)^n \cdot (b^n)^m = e^n e^m = e$

$\Rightarrow$ ab je konačnog reda

(ovo ne mora značiti da je $|ab| = mn$)

$\Rightarrow$ $ab \in H$

INVERZ

$a \in H$, $|a| = m \Rightarrow (a^{-1})^m = (a^m)^{-1} = e^{-1} = e$

$\Rightarrow$ a^{-1} je konačnog reda $\Rightarrow$ $a^{-1} \in H$

(#) Pokazati da za svaki element a grupe G, postoji jedinstven element $b \in G$ takav da $ab = ba = e$.

Kj:

Pretpostavimo da su i b i c inverzi od a u G.

$$ba = ab = e$$
$$ca = ac = e$$

Kako je $ab = e = ac$ to je $ab = ac$

$$\Downarrow$$
$$a^{-1}(ab) = a^{-1}(ac)$$
$$\Downarrow$$
$$b = c$$

g.e.d.

(#) Neka je G grupa i neka su $a, b \in G$. Pokazati da je tada $(ab)^{-1} = b^{-1}a^{-1}$.

Kj.

Primjetimo da je

$$(ab)(ab)^{-1} = e$$

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

Kako je prema prethodnom zadatku inverz jedinstven to je $(ab)^{-1} = b^{-1}a^{-1}$.

(#) Neka je G Abelova grupa i neka su H i K podgrupe od G. Pokazati da je

$$HK = \{hk \mid h \in H,\ k \in K\}$$

podgrupa grupe G.

R.j.

NEPRAZAN

· Primjetimo da $e = ee$ pripada $\overset{u}{\forall} HK$ zato što je $e \in H$ i $e \in K$. Time je $H \neq \emptyset$

ZATVORENOST

$a, b \in HK \Rightarrow$ prema definiciji $\exists h_1, h_2 \in H$ i $k_1, k_2 \in K$ t.d.

$$a = h_1 k_1 \ ; \ b = h_2 k_2.$$

Kako je G Abelova i kako su H i K podgrupe od G imamo

$$ab = (h_1 k_1)(h_2 k_2) = h_1 \underbrace{(k_1 h_2)}_{= h_2 k_1} k_2 = \underbrace{(h_1 h_2)}_{\in H} \underbrace{(k_1 k_2)}_{\in K} \in HK$$

$\Rightarrow ab \in HK \Rightarrow HK$ je zatvoreno

INVERZ

$a \in HK \Rightarrow \exists h_1 \in H,\ k_1 \in K$ t.d. $a = h_1 k_1$

$$a^{-1} = (h_1 k_1)^{-1} = k_1^{-1} h_1^{-1} = h_1^{-1} k_1^{-1} \in HK$$

HK je podgrupa grupe G.

(#) Neka je G grupa nenula realnih brojeva u odnosu na operaciju množenja. Proveriti da li su

$$H = \{ x \in G \mid x = 1 \text{ ili } x \text{ je iracionalan} \},$$

$$K = \{ x \in G \mid x \geq 1 \}$$

podgrupe grupe G.

Rj.

Primetimo da je $\sqrt{2} \in H$, ali $\sqrt{2} \cdot \sqrt{2} = 2 \notin H$

H nije podgrupa grupe G.

S druge strane $2 \in K$ ali $2^{-1} = \frac{1}{2} \notin K$.

K nije podgrupa od G.

(#) Neka je H neprazan konačan podskup grupe G. Pokazati da ako je H zatvoren u odnosu na operaciju od G, tada je H podgrupa od G.

dokaz:

S pogledom na jedan od prethodnih zadataka, jedino što treba da pokažemo je da $a^{-1} \in H$ za proizvoljni $a \in H$.

Izaberimo proizvoljno $a \in H$.

Ako je $a = e$ tada $a^{-1} = e^{-1} = e = a \in H \Rightarrow a^{-1} \in H$ i zadatak je završen

Ako je $a \neq e$, posmatrajmo niz

$$a, a^2, a^3, \ldots$$

Prema zatvorenosti svi ovi elementi pripadaju H. Kako je H konačno nisu svi ovi elementi različiti, recimo da je $a^i = a^j$ za neko $i > j$. Tada $a^{i-j} = e$; a kako je $a \neq e$ to je $i - j > 1$. Time

$$a\, a^{i-j-1} = a^{i-j} = e \quad \Rightarrow \quad a^{i-j-1} = a^{-1}$$

Ali $i - j - 1 \geq 1 \Rightarrow a^{i-j-1} \in H$ čime je zadatak završen.

(#) Element $x \in G$ zadovoljava $x^2 = e$ tačno onda kada je $x = x^{-1}$. Iskoristiti ovo opažanje i pokazati da grupa parnog reda mora sadržavati neparan broj elemenata reda 2.

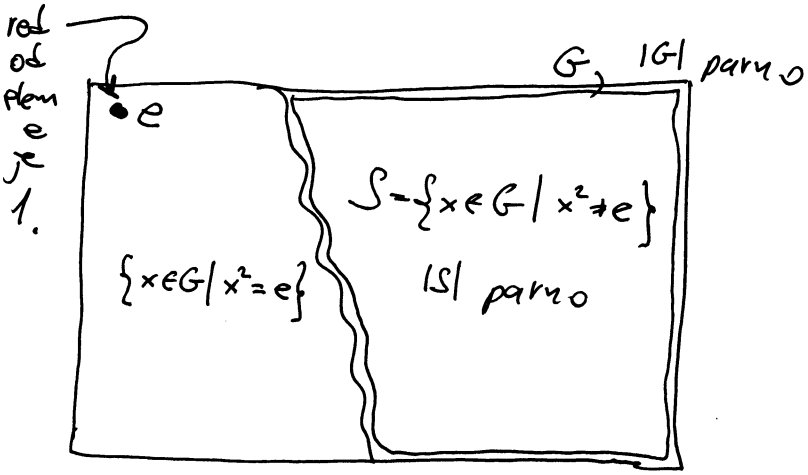
Rj. Neka je G grupa parnog reda. Kao i ranije, označimo sa $|G|$ red grupe G. Pa možemo pisati

$$|G| = 2n \quad \text{za neki } n \in \mathbb{Z}.$$

Neka je S skup elemenata iz G čiji je red veći od 2. Kako jedino identitet i elementi reda 2 zadovoljavaju jednakost $x^2 = e$ možemo pisati

$$S = \{x \in G \mid x^2 \neq e\}$$

Želimo pokazati da S ima paran broj elemenata.



Koristićemo ideju da ako element ima red veći od 2, on je različit od svog inverza, pa elementi od S dolaze u parovima. Da bi bili precizniji, napišimo S kao sljedeću uniju

$$S = \bigcup_{x \in S} \{x, x^{-1}\}$$

Kasnije ćemo pokazati da je red od x^{-1} isti kao red od x, pa je ova unija zaista S. Kako je $x^2 \neq e$ za $x \in S$, imamo

da $x \neq x^{-1}$, pa svaki skup u ovoj uniji ima dva različita elementa. Kako je inverz jedinstven, dva skupa oblika $\{x_1, x_1^{-1}\}$, $\{x_2, x_2^{-1}\}$ su jednaki ili disjunktni. Pa možemo napisati S kao disjunktnu uniju skupova od kojih svaki ima dva elementa. Time S ima paran broj elemenata. Neka je $2m$ broj elemenata od S, za neki $m \in \mathbb{Z}$.

Neka je T skup elemenata grupe G reda 2, i neka je k broj elemenata od T. Kako je G disjunktna unija od T, S i $\{e\}$, broj elemenata grupe G je jednak broju elemenata od T plus broj elemenata od S plus 1. Tj. $2n = 2m + k + 1$. Rješenje za k je

$$k = 2(n-m) - 1$$

Kako su $n, m \in \mathbb{Z}$ dobili smo da je k neparno.

Time smo pokazali da postoji neparan broj elemenata reda 2.

(#) Neka su x i g elementi grupe G. Pokazati da x i gxg^{-1} imaju isti red. Poslije toga pokazati da xy i yx imaju isti red za bilo koja dva elementa $x, y \in G$.

Rj.

Neka je G grupa i neka je $x, y, g \in G$. Označimo (kao i do sad) red elementa x sa $|x|$. Pretpostavimo da je $|x| = n$ i $|gxg^{-1}| = m$. Trebamo pokazati da je $n = m$. Prisjetimo se da je red elementa x najmanji broj n t.d. $x^n = e$.

Prvo ćemo pokazati da je red od gxg^{-1} najviše n. Možemo iskoristiti osobine grupe da bi pokazali da je

$$gxg^{-1} \cdot gxg^{-1} = gx^2g^{-1}.$$

Poslije toga možemo uraditi sljedeće

$$(gxg^{-1})^n = \underbrace{gxg^{-1} \cdot gxg^{-1} \cdot \ldots \cdot gxg^{-1}}_{n \text{ puta}}$$

$$= gx^ng^{-1} = |x^n = e| = gg^{-1} = e$$

Time smo pokazali da je $(gxg^{-1})^n = e$, pa je $|gxg^{-1}| \leq |x|$. S obzirom da je ovo tačno za proizvoljne x i g, neka je $x' = gxg^{-1}$ i neka je $g' = g^{-1}$. Prema onome što smo upravo pokazali

$$|g'x'g'^{-1}| \leq |x'|.$$

Ali kako je $g'^{-1} = g$ imamo da $g'x'g'^{-1} = g^{-1}(gxg^{-1})g = x$. Prema tome $|g'xg'^{-1}| \leq |x'|$ u stvari znači da $|x| \leq |gxg^{-1}|$. Time je $|gxg^{-1}| = |x|$.

Sljedeće što želimo pokazati je da $|xy| = |yx|$. Pretpostavimo da je $|xy| = n$. Tada

$$\underbrace{xy \cdot xy \cdot \ldots \cdot xy}_{n \text{ puta}} = e$$

Množeći obe strane sa y^{-1} sa desne strane, dobićemo

$$xy \cdot \ldots \cdot xy \cdot y^{-1} = ey^{-1}$$

$$\underbrace{xy \cdot \ldots \cdot xy}_{n-1 \text{ puta}} \cdot x = y^{-1}$$

Sad množeći sa y sa lijeve strane

$$y \cdot \underbrace{xy \ldots xy}_{n-1 \text{ puta}} \cdot x = \underbrace{yy^{-1}}_{=e}$$

Primjetimo da u zadnjoj jednakosti imamo yx pomnožen sa samim sobom n puta. Time je $|yx| \leq |xy|$.

Kako je ovo tačno za proizvoljno x i y, možemo zamijeniti uloge od x i y i time (također) dobiti $|xy| \leq |yx|$.

Prema tome $|xy| = |yx|$

q.e.d.