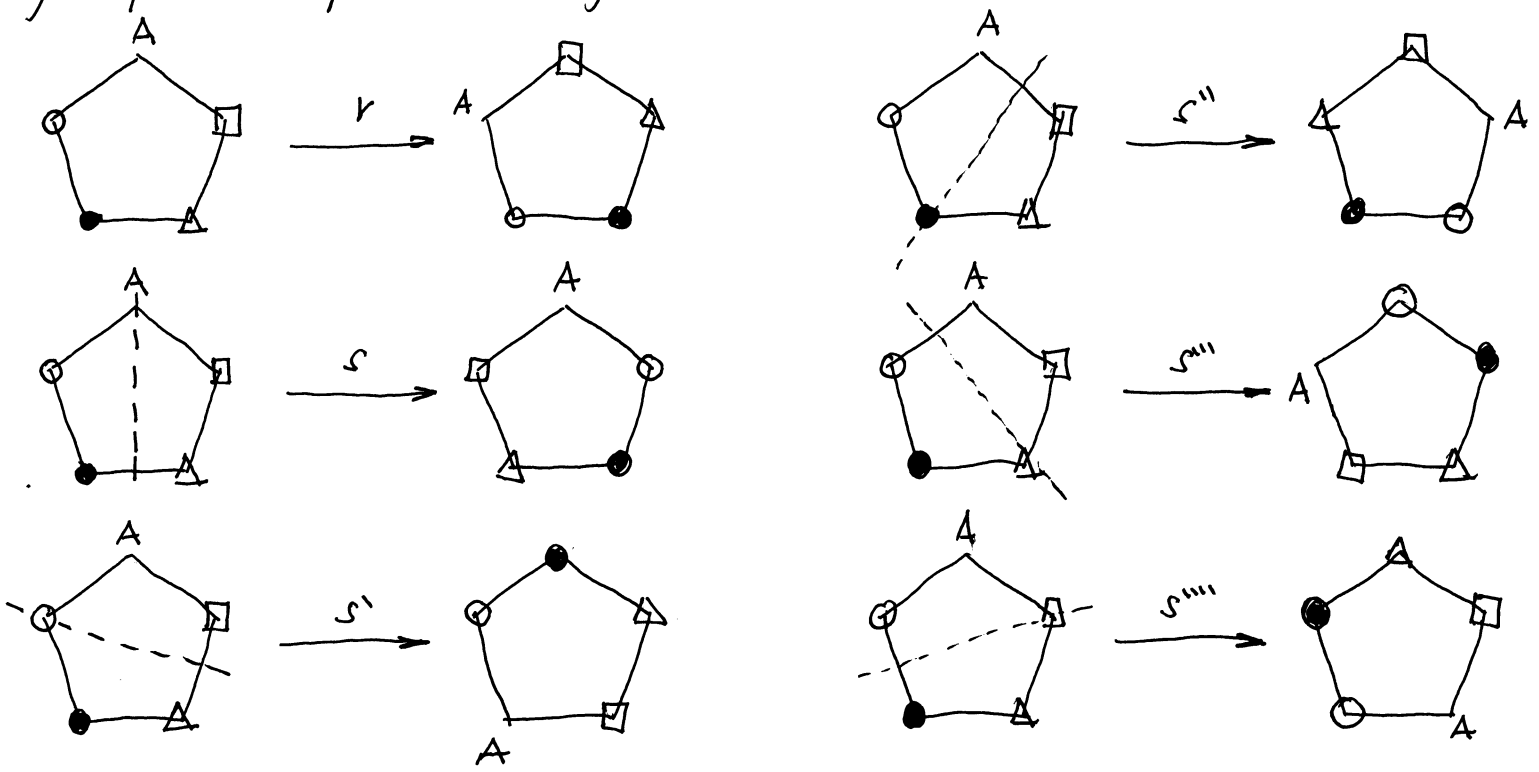
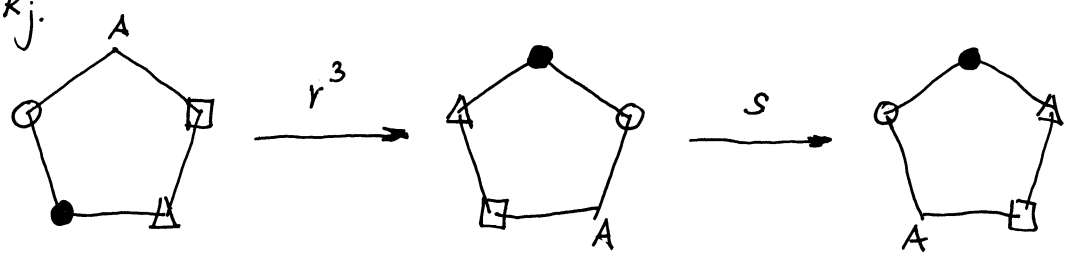
Podgrupe generisane skupom elemenata i neke osobine cikličkih grupa

(#) Šest simetrija $r, s, s', s'', s''', s''''$ pravilnog petokuta je opisano pomoću sljedećih slika

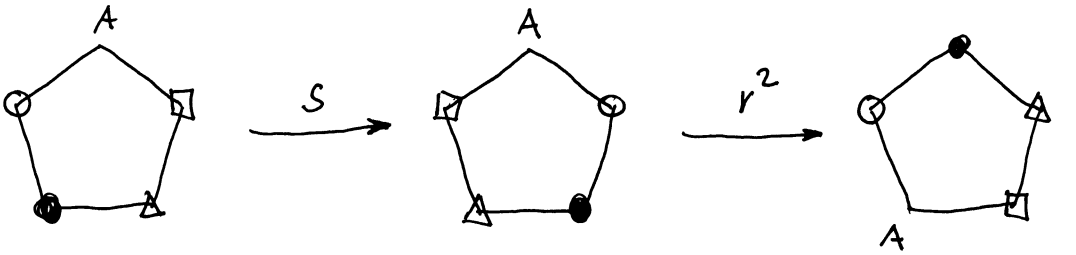


Simetrije s', s'', s''', s'''', $s's''''$ i $s'''s''$ izraziti preko r i s.

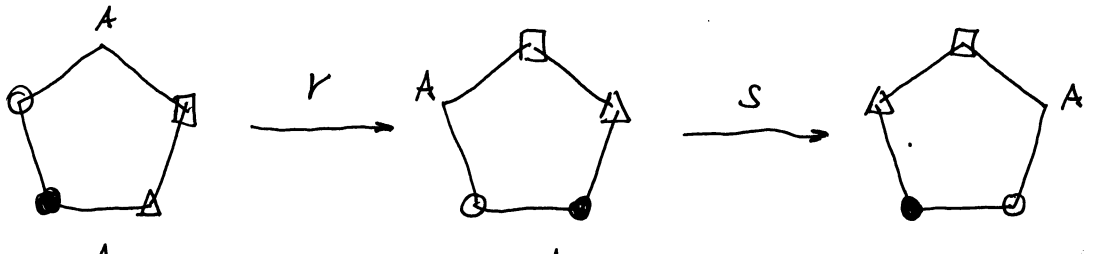
Rj.



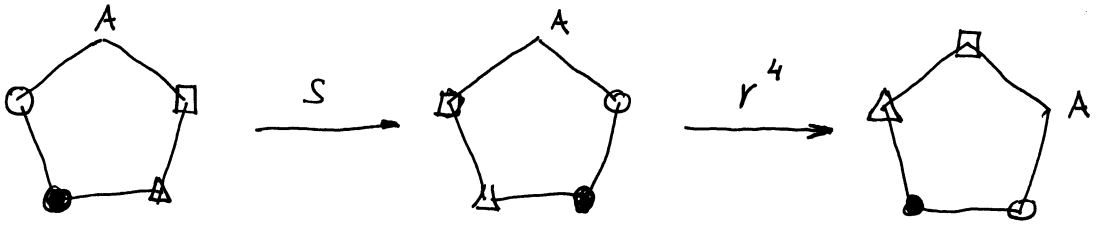
$\Rightarrow \quad s' = sr^3$



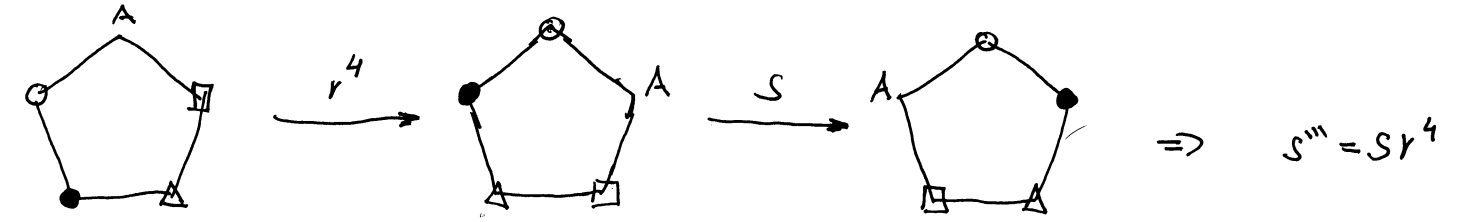
$\Rightarrow \quad s' = r^2 s$



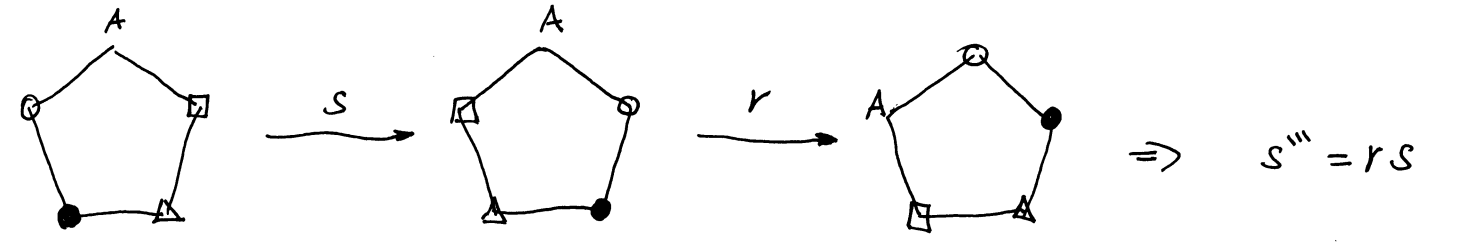
$\Rightarrow \quad s'' = sr$



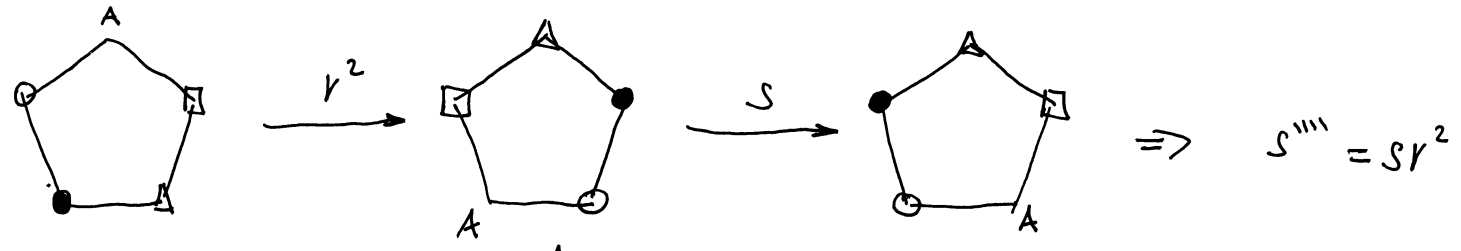
$\Rightarrow \quad s'' = r^4 s$



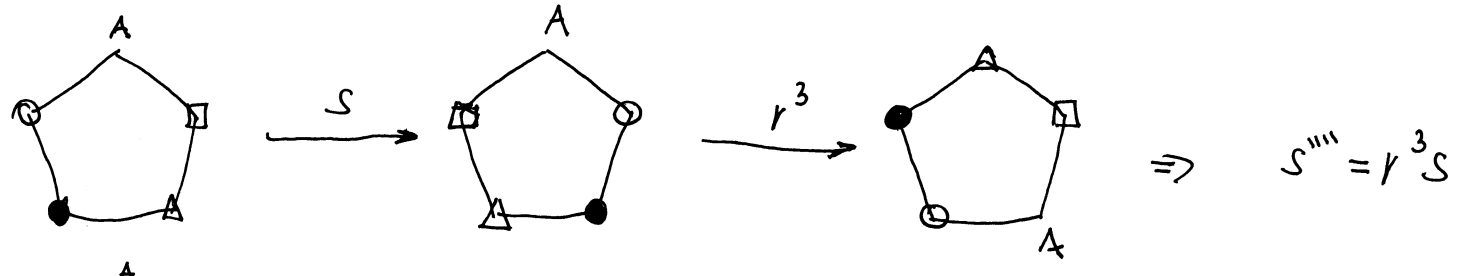
$\Rightarrow \quad s''' = sr^4$



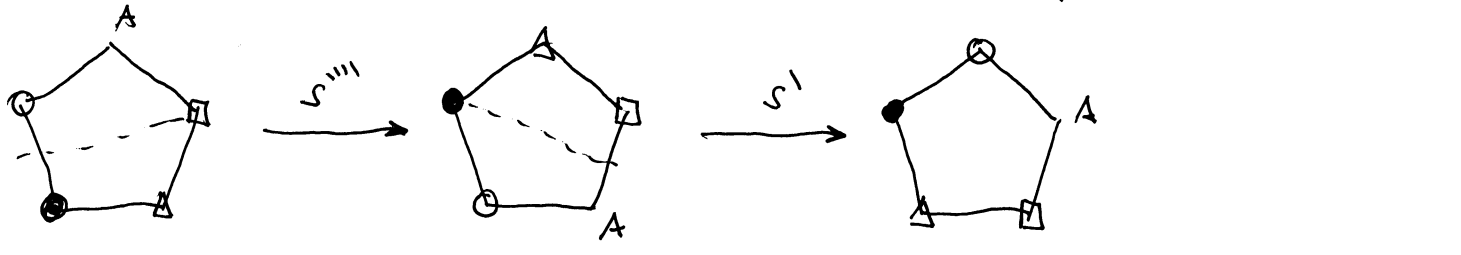
$\Rightarrow \quad s''' = rs$

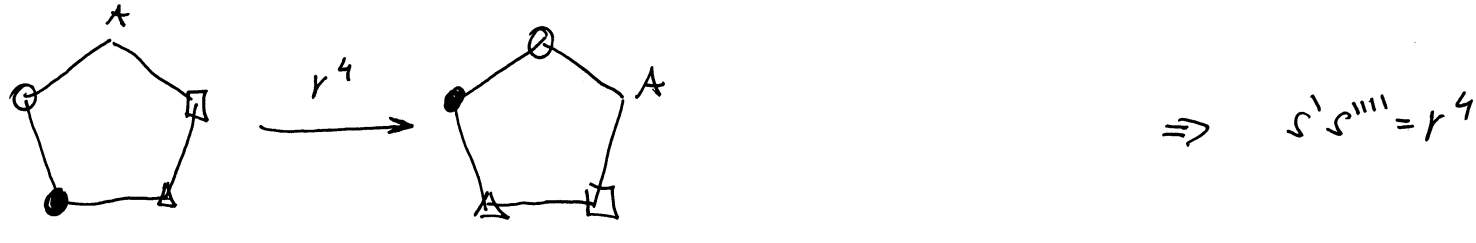


$\Rightarrow \quad s'''' = sr^2$

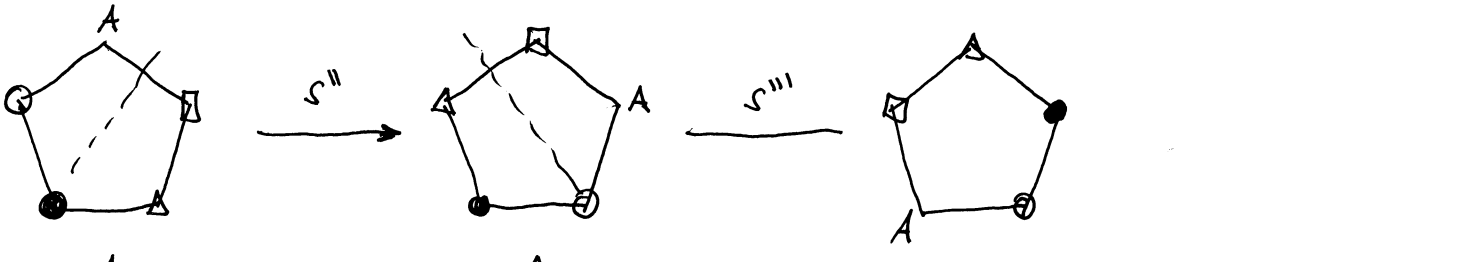


$\Rightarrow \quad s'''' = r^3 s$





$\Rightarrow \quad s's'''' = r^4$



$\Rightarrow \quad s'''s'' = r^2$

Za proizvoljan element a grupe G, često je korisno da razmišljamo o grupi $\langle a \rangle$ kao o najmanjoj podgrupi grupe G koja sadrži a. Ova oznaka se može proširiti na bilo koju familiju S elemenata iz grupe G definišući $\langle S \rangle$ kao podgrupu od G sa osobinom da $\langle S \rangle$ sadrži S i da ako je H proizvoljna podgrupa grupe G koja sadrži S da tada i H također sadrži $\langle S \rangle$. Time je $\langle S \rangle$ najmanja podgrupa grupe G koja sadrži S.
Skup $\langle S \rangle$ nazivamo podgrupa generisana sa S.

(#) Data je grupa $D_5 = \{e, r = R_{72°}, r^2, r^3, r^4, s, rs, r^2s, r^3s, r^4s\}$ (grupa svih simetrija pravilnog petougla u odnosu na operaciju kompozicije - ova grupa je poznata pod imenom dihedralna grupa reda 10) i data je njena Cayleyeva tabela:

	e	r	r^2	r^3	r^4	s	rs	r^2s	r^3s	r^4s
e	e	r	r^2	r^3	r^4	s	rs	r^2s	r^3s	r^4s
r	r	r^2	r^3	r^4	e	rs	r^2s	r^3s	r^4s	s
r^2	r^2	r^3	r^4	e	r	r^2s	r^3s	r^4s	s	rs
r^3	r^3	r^4	e	r	r^2	r^3s	r^4s	s	rs	r^2s
r^4	r^4	e	r	r^2	r^3	r^4s	s	rs	r^2s	r^3s
s	s	r^4s	r^3s	r^2s	rs	e	r^4	r^3	r^2	r
rs	rs	s	r^4s	r^3s	r^2s	r	e	r^4	r^3	r^2
r^2s	r^2s	rs	s	r^4s	r^3s	r^2	r	e	r^4	r^3
r^3s	r^3s	r^2s	rs	s	r^4s	r^3	r^2	r	e	r^4
r^4s	r^4s	r^3s	r^2s	rs	s	r^4	r^3	r^2	r	e

(i) Odrediti sve ciklične podgrupe grupe D_5.

(ii) Odrediti $\langle r, s\rangle$, $\langle r^2, rs\rangle$, $\langle r, r^3\rangle$, $\langle rs, r^3s\rangle$ i $\langle r^3s, r^4s\rangle$.

(iii) Odrediti sve podgrupe grupe D_5.

Rj.

(i) Posmatrajući datu Cayleyevu tabelu imamo

$\langle e\rangle = \{e\}$

$\langle r\rangle = \{e, r, r^2, r^3, r^4\}$

$\langle r^2\rangle = \{e, r, r^2, r^3, r^4\} = \langle r\rangle$

$\langle r^3\rangle = \langle r\rangle$

$\langle r^4\rangle = \langle r\rangle$

$\langle s\rangle = \{e, s\}$

$\langle rs\rangle = \{e, rs\}$

$\langle r^2s\rangle = \{e, r^2s\}$

$\langle r^3s\rangle = \{e, r^3s\}$

$\langle r^4s\rangle = \{e, r^4s\}$

(ii) Promatrajući Cayley-evu tablicu

$\langle r, s \rangle = D_4$

$\langle r^2, rs \rangle = D_4$

$\langle r, r^3 \rangle = \{e, r, r^2, r^3, r^4\}$

$\langle rs, r^3 s \rangle = D_4$

$\langle r^3 s, r^4 s \rangle = D_4$

(iii) Podgrupe sa jednim generatorom su

rotacije: $\{e\}$, $\langle r \rangle = \{e, r, r^2, r^3, r^4\}$

refleksije: $\langle s \rangle = \{e, s\}$, $\langle rs \rangle = \{e, rs\}$, $\langle r^2 s \rangle = \{e, r^2 s\}$

$\langle r^3 s \rangle = \{e, r^3 s\}$, $\langle r^4 s \rangle = \{e, r^4 s\}$

Primjetimo da ne možemo dodati nikakvu refleksiju podgrupi generisanoj sa r, s obzirom da ćemo onda dobiti r i s u podgrupi, iz čega ćemo dobiti čitavu grupu D_5.

Ako dodamo refleksiju u refleksionu podgrupu, dobićemo rotaciju, i kao što smo upravo rekli, podgrupa sa rotacijom i refleksijom je čitava grupa.

Pa jedine podgrupe su one koje smo ispisali, kao i sam D_5.

(#) Data je grupa $(\mathbb{Z}_{20}, +)$. Odrediti $\langle 8, 14 \rangle$. Da li je $\langle 2 \rangle = \langle 8, 14 \rangle$?

Rj.

$8 + 14 = 2$

$2 + 8 = 10$

$2 + 2 = 4$

$2 + 4 = 6$

$\vdots$

$\langle 8, 14 \rangle = \{0, 2, 4, \ldots, 18\}$

Da $\langle 2 \rangle = \langle 8, 14 \rangle$, jednakost je tačna.

(#) Data je grupa $(\mathbb{Z}, +)$. Odrediti $\langle 8, 13 \rangle$.

Rj.

$8 + 13 = 21$

$13 - 8 = 5$

$8 - 5 = 3$

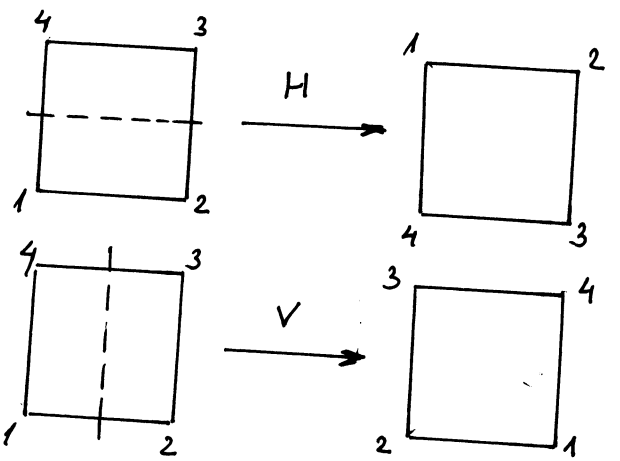
$5 - 3 = 2$

$3 - 2 = 1 \Rightarrow \langle 8, 13 \rangle = \mathbb{Z}$.

(#) Data je dihedralna grupa D_4. Odrediti $\langle H, V\rangle$ i $\langle R_{90}, V\rangle$.

Rj.

Prisjetimo se



$$\langle H, V\rangle = \{H, H^2, V, HV\} = \{R_0, R_{180}, H, V\}$$

$$\langle R_{90}, V\rangle = \{R_{90}, R_{90}^2, R_{90}^3, R_{90}^4, V, R_{90}V, R_{90}^2V, R_{90}^3V\} = D_4$$

(#) Data je grupa $\mathbb{C}^*$, grupa nenula kompleksnih brojeva u odnosu na operaciju množenja. Odrediti $\langle 1, i\rangle$. Da li je $\langle 1, i\rangle = \langle i\rangle$.

Rj.

$$\langle 1, i\rangle = \{1, i, -1, -i\} = \langle i\rangle$$

$$\downarrow i^2$$

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

Rj.:

$$\langle 1, i \rangle = \{ a + ib \mid a, b \in \mathbb{Z} \}$$

$1+1=2$
$1+2=3$
$1+3=4$
$\vdots$

Ova grupa se nekad naziva "Gaussovi cijeli".

(#) Data je grupa $(\mathbb{R}, +)$. Odrediti $\langle 2, \pi, \sqrt{2} \rangle$.

Rj.:

$2+2 = 2 \cdot 2$
$2+4 = 3 \cdot 2$
$2+6 = 4 \cdot 2$
$\vdots$

$$\langle 2, \pi, \sqrt{2} \rangle = \{ 2a + \pi b + c\sqrt{2} \mid a, b, c \in \mathbb{Z} \}.$$

(#) Data je grupa u kojoj a, b, c, d komutiraju. Odrediti $\langle a, b, c, d \rangle$.

Rj.:

$$\langle a, b, c, d \rangle = \{ a^q b^r c^s d^t \mid q, r, s, t \in \mathbb{Z} \}.$$

(#) Data je dihedralna grupa D_n reda $2n$ (grupa svih simetrija pravilnog n-ugla u odnosu na operaciju kompozicije) i neka je R rotacija od $\frac{360}{n}$ stepeni. Odrediti $\langle R \rangle$.

Rj.

Kako je R rotacija od $\frac{360}{n}$ stepeni primjetimo da je

$$R^n = R_{360^\circ} = e, \quad R^{n+1} = R, \quad R^{n+2} = R^2, \ldots$$

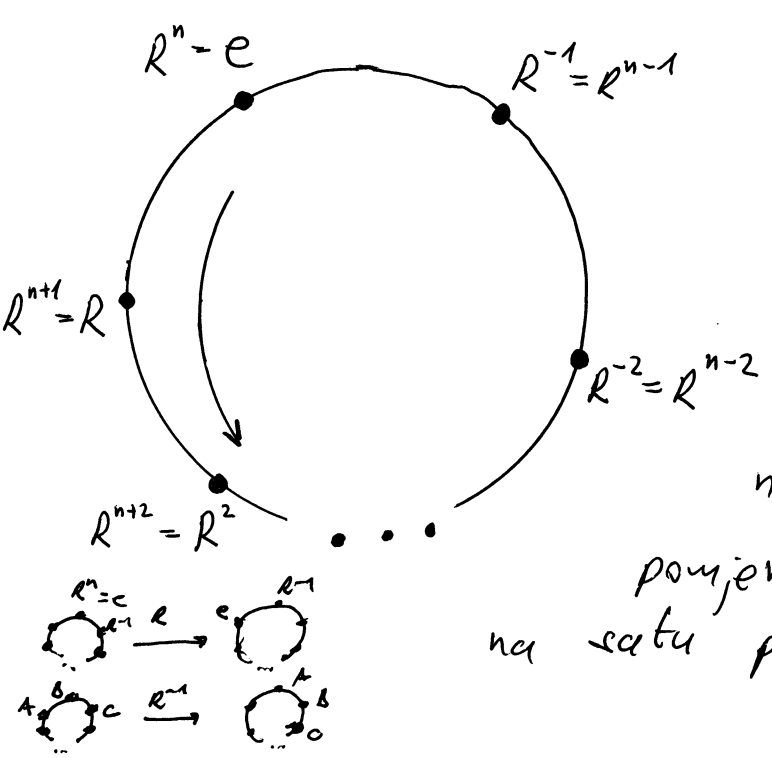
Slično

$$R^{-1} = R^{n-1}, \quad R^{-2} = R^{n-2}, \quad R^{-3} = R^{n-3}, \ldots$$

tako da je

$$\langle R \rangle = \{ e, R, R^2, \ldots, R^{n-1} \}$$

Primjetimo da se stepeni od R "vraćaju na istu poziciju" periodično sa periodom n.



Vizuelno, dižući R na sljedeći pozitivni stepen je isto kao pomjerajući u suprotnom smjeru kazaljke na satu sljedeći krug na sljedeći vrh, dok je dižući R na sljedeći negativni stepen je isto kao pomjerajući oko kruga u smjeru kazaljke na satu po jedan vrh.

(#) Pronaći grupu koja sadrži elemente a i b takve da $|a|=|b|=2$, i da je

(a) $|ab|=3$,

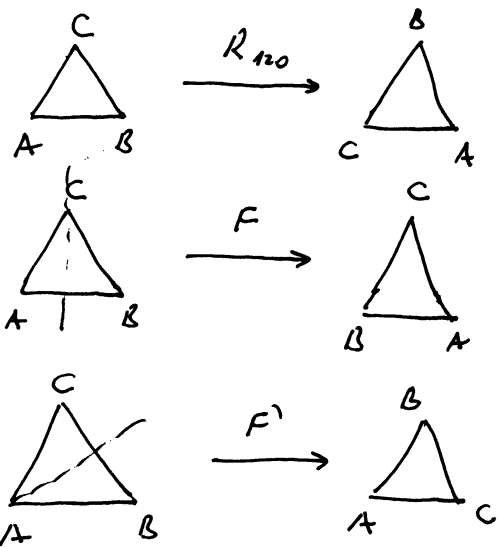
(b) $|ab|=4$,

(c) $|ab|=5$.

Može li se isto reći o relacijama između $|a|$, $|b|$ i $|ab|$?

Rj.

(a) Posmatrajmo dihedralnu grupu D_3 i elemente R_{120}, F i F' definisane na sljedeći način



Primjetimo da je

$|F|=2$

$|F'|=2$

$|FF'|=3$

(s obzirom da je $FF'=R_{120}$)

(b) U dihedralnoj grupi D_4 neka je $a=H$ i $b=D'$. Oba a i b su obrtaji pa imaju red 2. A kako je $ab=HD'=R_{90}$ to je $|HD'|=4$.

(c) U grupi D_5 dva različita obrtaja F_i i F_j $(i\neq j)$ kombinovana daju nenula rotaciju, a svaka nenula rotacija u D_5 ima red 5.

Izgleda da ne postoji nikakva relacija između $|a|$, $|b|$ i $|ab|$. Niti je $|ab|=|a||b|$ niti $|a|$ ili $|b|$ dijele $|ab|$.

(#) Odrediti red grupe G koja je generirana sa dva elementa x i y, za koje vrijedi relacija

$$x^3 = y^2 = (xy)^2 = 1.$$

Ispišite sve podgrupe grupe G.

Rj.

Red elementa x je 3 $(x^3 = 1)$

Red elementa y je 2 $(y^2 = 1)$

$y^2 = 1 \Rightarrow y^{-1} = y$

$x^3 = 1 \Rightarrow x^2 \cdot x = x \cdot x^2 = 1 \Rightarrow x^{-1} = x^2$

$(xy)^2 = 1 \Rightarrow (xy)(xy) = 1 \Rightarrow xy = (xy)^{-1}$

$\Downarrow$

$xy = y^{-1}x^{-1} \overset{y^{-1}=y}{\Longrightarrow} xy = yx^{-1} = yx^2$

Time imamo

element	x	y	xy	1
inverz	x^2	y	xy	1

$(xy)(xy) = 1$

$x(yx)y = 1$

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

$yx = x^{-1}y^{-1} = x^2y$

a dobili smo da je i $xy = yx^2$

$yx = x^2y$

Napravimo Cayley-evu tablicu

	1	x	x^2	y	xy	yx
1	1	x	x^2	y	xy	yx
x	x	x^2	1	xy	yx	y
x^2	x^2	1	x	yx	y	xy
y	y	yx	xy	1	x^2	x
xy	xy	y	yx	x	1	x^2
yx	yx	xy	y	x^2	x	1

$yx = x^2y \Rightarrow xyx = y$

$x^2y = yx \Rightarrow x^2yx = yx^2 = xy$

$xy = yx^2 \Rightarrow yxy = x^2$

$xy = yx^2 \Rightarrow xyx^2 = yx$

$yx^2 = xy \Rightarrow yx^2y = x$

$(yx)^2 = (yx)(yx) = (x^2y)(yx) = 1$

Red grupe G je 6.

Odredimo podgrupe.

Najmanja podgrupa koja sadrži 1 je $\{1\}$ tj. $\langle 1\rangle = \{1\}$

Najmanja podgrupa koja sadrži x je $\{1, x, x^2\}$ tj. $\langle x\rangle = \{1, x, x^2\}$

——— // ——— x^2 je $\{1, x, x^2\}$ tj. $\langle x^2\rangle = \{1, x, x^2\}$

——— // ——— y je $\{1, y\}$ tj. $\langle y\rangle = \{1, y\}$

——— // ——— xy je $\{1, xy\}$ tj. $\langle xy\rangle = \{1, xy\}$

——— // ——— yx je $\{1, yx\}$ tj. $\langle yx\rangle = \{1, yx\}$

Time smo dobili podgrupe $\{1\}, \{1, x, x^2\}, \{1, y\}, \{1, xy\}, \{1, yx\}$

Što je sa podgrupama sa dva generatora.

$\langle 1, x\rangle = \langle x\rangle = \{1, x, x^2\}$

$\langle 1, y\rangle = \langle y\rangle, \ldots, \langle 1, yx\rangle = \langle yx\rangle$

ZAVRŠITI ZA VJEŽBU

(#) Data je grupa $(\mathbb{Q},+)$. Pokazati da se ova grupa ne može generisati sa konačno mnogo elemenata.

R.j. Pretpostavimo suprotno tvrdnji tj. pretpostavimo da je

$$\mathbb{Q} = \left\langle \frac{a_1}{b_1}, \frac{a_2}{b_2}, \ldots, \frac{a_n}{b_n} \right\rangle$$

Kako je broj $\frac{1}{2b_1b_2\ldots b_n} \in \mathbb{Q}$ to postoje cijeli brojevi $c_1, c_2, \ldots, c_n$ takvi da

$$c_1\frac{a_1}{b_1} + c_2\frac{a_2}{b_2} + \ldots + c_n\frac{a_n}{b_n} = \frac{1}{2b_1b_2\ldots b_n}$$

Sabirajući razlomke na lijevoj strani dobićemo

$$c_1\frac{a_1}{b_1} + c_2\frac{a_2}{b_2} + \ldots + c_n\frac{a_n}{b_n} = \frac{A_1+A_2+\ldots+A_n}{b_1b_2\ldots b_n}$$

gdje je $A_i = c_i a_i b_1 \ldots b_{i-1} b_{i+1} \ldots b_n$. Da bi olakšali zapis napišimo da je $A = A_1 + A_2 + \ldots + A_n$. Primjetimo da kako su A_i $(1 \le i \le n)$ cijeli to i A mora biti cijeli broj. Tvrdimo da

$$\frac{A}{b_1b_2\ldots b_n} = \frac{1}{2b_1b_2\ldots b_n}$$

Ovo je jedino moguće ako je $A = \frac{1}{2}$

#kontradikcija
(A je cio broj)

Pretpostavka suprotna tvrdnji nas vodi u kontradikciju pa nije tačna. Grupa $\mathbb{Q}$ se ne može generisati sa konačnim skupom racionalnih brojeva.

(#) Pokazati da je $H = \left\{ \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix} \mid n \in \mathbb{Z} \right\}$ ciklička podgrupa grupe $GL_2(\mathbb{R})$.

R.j.

Promatrajmo produkt dva proizvoljna elementa $\begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix}$ i $\begin{bmatrix} 1 & m \\ 0 & 1 \end{bmatrix}$ ove podgrupe.

$$\begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & m \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & m+n \\ 0 & 1 \end{bmatrix}$$

Vidimo da se produkt dviju matrice svodi na sabiranje vrijednosti na poziciji a_{12}.

Neka je $A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$. Primjetimo

$$A^2 = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}, \quad A^3 = \begin{bmatrix} 1 & 3 \\ 0 & 1 \end{bmatrix}, \quad A^4 = \begin{bmatrix} 1 & 4 \\ 0 & 1 \end{bmatrix}, \dots$$

Matem. indukcija lako pok. $A^k = \begin{bmatrix} 1 & k \\ 0 & 1 \end{bmatrix}$, $k \in \mathbb{Z}$

Time

$$\left\langle \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \right\rangle = H.$$

(#) Primjerom pokazati da proizvod elemenata konačnog reda u neabelovoj grupi ne mora imati konačan red.

Rj. Neka je $G = GL_2(\mathbb{R}) = \{M \in Mat_{2\times 2}(\mathbb{R}) \mid \exists M^{-1}\}$ i promatrajmo matrice $A = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$ i $B = \begin{bmatrix} 1 & 1 \\ 0 & -1 \end{bmatrix}$.

Primjetimo da je $A^2 = B^2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ tj. da obe ove matrice imaju red 2.

$$AB = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \quad (AB)^2 = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}, \quad (AB)^3 = \begin{bmatrix} 1 & 3 \\ 0 & 1 \end{bmatrix}, \ldots$$

$$(AB)^n = \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix}$$ (ovo nije teško pokazati matematičkom indukcijom).

Ovo znači da je $\forall n > 1 \quad (AB)^n \neq \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ pa je red od AB beskonačan.

(#) Neka je G ciklička grupa reda 6. Koliko elemenata grupe generiše G?

Rj:

Kako je G ciklička grupa, neka je $G = \{1, g, g^2, g^3, g^4, g^5\}$.

Primjetimo da je

$|1| = 1$

$|g^2| = 3$

$|g^3| = 2$

$|g^4| = 3$

$|g| = 6$

$|g^5| = 6$

Jedini elementi reda 6 su g i g^5, pa oni jedini mogu biti generatori za G.

(#) Neka je G ciklička grupa reda n. Odrediti koliko elemenata generiše grupu G.

Rj:

Neka je $G=\{1, g, \dots, g^{n-1}\}$ data ciklička grupa reda n, i pokažimo da je broj generatora ove grupe jednak broju cijelih m $(1<m<n)$ koji su relativno prosti sa n.

Podjelimo rješenje u dva slučaja

1° $\gcd(i,n)=1$

Ako je $\gcd(i,n)=1$ tada postoje cijeli brojevi $p,t\in\mathbb{Z}$ t.d.

$$1=ip+nt$$

Time

$$g=g^1=g^{ip+nt}=g^{ip}\cdot g^{nt}=g^{ip}\cdot(g^n)^t=g^{ip} \Rightarrow g^{ip}=g$$

$$\Rightarrow g\in\langle g^i\rangle \Rightarrow \langle g^i\rangle = G$$

2° $\gcd(i,n)=d>1$

Ako je $\gcd(i,n)=d>1 \Rightarrow \exists p,s\in\mathbb{Z}$ $i=sd$, $n=pd$ sa $p<n$.

Sad primjetimo

$$(g^i)^p=(g^{sd})^p=(g^{pd})^s=(g^n)^s=1 \text{ tj. } (g^i)^p=1.$$

Time

$$|g^i|\leq p<n \Rightarrow \langle g^i\rangle \neq G$$

(#) Neka je G grupa, i neka je $a \in G$ konačnog reda.
Pokazati da $|a| = |\langle a \rangle|$.

Rj.
Pretpostavimo da je $|a| = n$ i pokažimo da $\langle a \rangle = \{e, a, \dots, a^{n-1}\}$.
Odmah nije teško vidjeti da su elementi $e, a, \dots, a^{n-1}$ u $\langle a \rangle$. ...(1)

Sad pretpostavimo da je a^k proizvoljan element iz $\langle a \rangle$.
Prema Teoremi o ostatku cjelobrojnog dijeljenja | postoje cijeli q i r takvi da

$$k = nq + r \quad \text{gdje je} \quad 0 \le r < n.$$

Tada

$$a^k = a^{qn+r} = a^{qn} \cdot a^r = (a^n)^q a^r = e a^r = a^r \Rightarrow a^k \in \{e, a, a^2, \dots, a^{n-1}\}.$$ ...(2)

Na osnovu (1) i (2) $\Rightarrow \langle a \rangle = \{e, a, a^2, \dots, a^{n-1}\}$.

Pokažimo još da su svi elementi skupa $\{e, a, a^2, \dots, a^{n-1}\}$ različiti.

Neka je $a^i = a^j$ za neke $i, j \in \{0, 1, 2, \dots, n-1\}$. Tada $a^{i-j} = e$.
Kako su $0 \le i, j \le n-1$ to mora biti $i - j = 0 \Rightarrow i = j$.

Možemo zaključiti $|a| = |\langle a \rangle|$.

(#) Pokazati da je svaka podgrupa cikličke grupe cikličke.

Rj:

Neka je data ciklička grupa G i neka je H podgrupa grupe G. Pokažimo da je H ciklička grupa.

Ako H sadrži samo identitet tada je H ciklička podgrupa i zadatak je gotov.

Pa pretpostavimo da je $H \neq \{e\}$.

Prvo što želimo pokazati je da H sadrži element oblika a^t gdje je t pozitivno. Kako je $G = \langle a \rangle$ svaki element iz G je oblika a^t za neko t. Ako je $t < 0$, kako je $a^t \in H$ (H podgr.) to je $a^{-t} \in H$ i $-t > 0$. Time smo pokazali da H sadrži element oblika a^t, gdje je $t > 0$.

Sad neka je m najmanji pozitivni cijeli za koji je $a^m \in H$.

$a^m \in H \Rightarrow a^{-m} \in H$; $a^{2m} \in H \Rightarrow a^{-2m} \in H$; $a^{3m} \in H \Rightarrow \ldots \langle a^m \rangle \subseteq H$

Tvrdimo da je $H = \langle a^m \rangle$. Neka je b proizvoljan element iz H i pokažimo da je $b \in \langle a^m \rangle$. $b \in G = \langle a \rangle \Rightarrow b = a^k$ za neko k.

Primjenimo Teorem o ostatku (algoritam dijeljenja) na brojevima k i m.

$\Rightarrow \exists q, r \quad k = mq + r, \quad 0 \leq r < m$

$$b = a^k = a^{mq+r} = a^{mq} a^r \Rightarrow a^r = \underbrace{a^{-mq}}_{\in H} a^k = \underbrace{a^{-mq}}_{\in H} \underbrace{b}_{\in H} \Rightarrow a^r \in H$$

Ali cijeli m je najmanji pozitivni cijeli t.d. $a^m \in H$. Kako $0 \leq r < m$ i $a^r = 0 \Rightarrow r = 0 \Rightarrow b = a^k = a^{mq} = (a^m)^q \in \langle a^m \rangle \Rightarrow H = \langle a^m \rangle$ q.e.d.

(#) Neka je $G=\langle a\rangle$ ciklička grupa reda n. Pokazati da red proizvoljne podgrupe grupe G dijeli n.

Rj.

$|G|=n$

Neka je H proizvoljna podgrupa grupe G.

Prema prethodnom zadatku H je ciklička podgrupa

$\Rightarrow \exists$ najmanji pozitivni m t.d. $a^m \in H$ i mijedi $H=\langle a^m\rangle$ (vidi dokaz prethodnog zadatka)

(kako je H podgrupa grupe G svi elementi su oblika a^t za neko $t\in\mathbb{Z}$. Ako je $t<0$ kako $a^{-t}\in H$ to $-t>0$)

Sad ako primjenimo Teorem o ostatku (algoritam dijeljenja) na cijele m i n dobićemo da $\exists k>0$, r ($k,r\in\mathbb{Z}$) t.d

$$n=mk+r \quad (0\le r<m)$$

$$e=a^n=a^{mk+r}=a^{mk}\cdot a^r \Rightarrow a^r=a^{-mk}\in H \overset{\text{m najm. pozit.}}{\Rightarrow} r=0$$

Time je $n=mk$ i $(a^m)^k=e \Rightarrow |a^m|=k$

Kako je $|a^m|=|\langle a^m\rangle|$ to je $|H|=k$.

S obzirom da je $n=mk$ to red podgrupe H dijeli red grupe G

Q.e.d

(#) Neka je G ciklička grupa reda n, i neka je r cijeli broj koji dijeli n. Pokazati da G sadrži tačno jednu podgrupu reda r.

Rj.

Neka je G ciklička grupa reda n. Tada $G=\{1, g, g^2, \dots, g^{n-1}\}$.

Ako r dijeli n tada postoji cijeli p takav da

$$n = rp. \qquad \dots (1)$$

Podgrupa $H=\{g^p, g^{2p}, \dots, g^{(r-1)p}, g^{rp}=g^n=1\}$ generisana sa g^p je podgrupa reda r.

Štaviše, kako je G ciklička sve njene podgrupe su ciklične. Time ako postoji jos jedna podgrupa H' reda r grupe G ona mora biti ciklička i H' je generisana sa elementom grupe G reda r. Neka je $H'=\langle g^k \rangle$. Tada

$$(g^k)^r = 1 \Rightarrow kr = ns \text{ za neki cijeli } s$$

Ako iskoristimo i (1) imamo $kr = ns = rps$

$$\Rightarrow k = \frac{n}{r} \cdot s = ps \Rightarrow g^k = g^{ps} = (g^p)^s \in \langle g^p \rangle$$

$$\Rightarrow H' \subseteq H$$

S druge strane kako je $|H'| = r = |H|$ to je $H' = H$.

Zadaci za vježbu

1. Dokazati da Abelova grupa sa dva elementa reda 2 mora imati podgrupu reda 4.

2. Pronaći primjer necikličnih grupa, čije su sve prave podgrupe ciklične.

3. Neka je G grupa i neka je $a \in G$. Dokazati da $\langle a^{-1} \rangle = \langle a \rangle$.

4. Dokazati da grupa reda 3 mora biti ciklička.

10. *Prove that an Abelian group with two elements of order 2 must have a subgroup of order 4.*

Let G be an Abelian group and let $a, b \in G$ with $a \neq b$ and $|a| = |b| = 2$. We want to show that $\{e, a, b, ab\}$ is a subgroup of G of order 4. First we show it is closed via a Cayley table:

	e	a	b	ab
e	e	a	b	ab
a	a	a^2	ab	aab
b	b	ba	b^2	bab
ab	ab	aba	abb	$abab$

	e	a	b	ab
e	e	a	b	ab
a	a	e	ab	b
b	b	ab	e	a
ab	ab	b	a	e

We simplify to the table on the right using $a^2 = b^2 = e$, since the order of both a and b are 2, and $ab = ba$, since G is Abelian.
By the Finite Subgroup Test, if a nonempty subset is closed, then it is a subgroup. So, $\{e, a, b, ab\} \leqslant G$.

It looks like our subgroup has order 4, but what if two elements of the set are actually the same? We know neither a nor b are the identity, since they both have order 2, and e always has order 1. If $a = ab$ or $b = ab$, then a or b is the identity, which we know if not true. So, could $ab = e$? If $ab = e$, then $a^{-1} = b$, but $a^2 = e$, so a^{-1} also equals a. Since inverses are unique, this means that $a = b$. Since we chose a and b to be distinct, this is a contradiction. Thus, we have four distinct elements, so the order of the subgroup is 4. ✓

7. *Find an example of a noncyclic group, all of whose proper subgroups are cyclic.*

$U(8) = \{1, 3, 5, 7\}$ with multiplication modulo 8 is an example of a noncyclic group all of whose proper subgroups are cyclic:

$$\begin{aligned} <3> &= \{1, 3\} \\ <5> &= \{1, 5\} \\ <7> &= \{1, 7\} \end{aligned}$$

There are no other proper subgroups of $U(8)$.

11. *Let G be a group and let $a \in G$. Prove that $< a^{-1} > = < a >$.*

To show the two subgroups are equal, we'll show that each subgroup contains the other.

($\subseteq$) Let $x \in < a^{-1} >$. So $x = (a^{-1})^n$ or some $n \in \mathbb{Z}$.

$$\begin{aligned} x &= (a^{-1})^n \\ &= \underbrace{a^{-1}a^{-1}\cdots a^{-1}}_{n \text{ times}} \\ &= \underbrace{(a\dot{a}\cdots a)^{-1}}_{n \text{ times}} \text{ by Problem 16 in Chapter 2} \\ &= (a^n)^{-1} \end{aligned}$$

Clearly $a^n \in < a >$, and $< a >$ is a subgroup so it is closed under inverses, thus $(a^n)^{-1} \in < a >$.

($\supseteq$) Let $x \in < a >$. So $x = a^n$ or some $n \in \mathbb{Z}$.

$$\begin{aligned} x &= (a)^n \\ &= \underbrace{a \cdot a \cdots a}_{n \text{ times}} \\ &= \underbrace{(a^{-1} \cdot a^{-1} \cdots a^{-1})^{-1}}_{n \text{ times}} \text{ by Problem 16 in Chapter 2} \\ &= ((a^{-1})^n)^{-1} \end{aligned}$$

Clearly $(a^{-1})^n \in < a^{-1} >$, and $< a^{-1} >$ is a subgroup so it is closed under inverses, thus $((a^{-1})^n)^{-1} \in < a^{-1} >$.

22. *Prove that a group of order 3 must be cyclic.*

Let G be a group with three elements, and suppose that G is not cyclic. We know G must have an identity element, e, and two non-identity elements, a and b. Since G is not cyclic, the orders of a and b must be strictly less than 3, the order of G, but they also must be strictly greater than 1, since a and b are not the identity. Thus $|a| = |b| = 2$. We know G must be closed, so $ab \in \{e, a, b\}$. If $ab = e$, then $ab^2 = b$ which means $a = b$, since $b^2 = e$, which isn't true. If $ab = a$ or $ab = b$ cancellation gives that $b = e$ or $a = e$, which is also not true. Thus, $ab \notin \{e, a, b\}$ so G is not closed and hence, not a group. This is a contradiction, so G must be cyclic.