Normalne podgrupe. Faktorske grupe.

Definicija (normalna podgrupa)

Podgrupa H grupe G nazivamo normalna podgrupa grupe G ako je $aH = Ha$ za sve $a \in G$. Ovo označavamo sa $H \triangleleft G$.

Neka je G Abelova grupa. Pokazati da je svaka podgrupa H grupe G normalna podgrupa.

Rj.

Neka je h proizvoljan element podgrupe H.

Primjetimo da za $\forall g \in G$ vrijedi $gh = hg$

Drugim riječima $gH = Hg$ za $\forall g \in G$ $\Rightarrow$ $H \triangleleft G$.

$$\left(gH = \{gh \mid h \in H\} = \{hg \mid h \in H\} = Hg \right)$$

#

(a) Neka je $H = \{(1), (12)\}$. Da li je H normalna podgrupa grupe S_3?

(b) Neka je $N = \{(1), (123), (132)\}$. Da li je $N \triangleleft S_3$?

Rj.

(a) Primjetimo da je
$$(123)H = \{(123), (13)\}$$
$$H(123) = \{(123), (23)\}$$

$\Rightarrow$ H nije normalna podgrupa grupe S_3.

(b)

$$N = \{(1), (123), (132)\}$$

$$(12)N = N(12) = \{(12), (13), (23)\}$$

N je normalna podgrupa grupe S_3.

Teorema (test za normalne podgrupe)

Podgrupa H grupe G je normalna u grupi G ako i samo ako $xHx^{-1} \subseteq H$ za sve $x \in G$.

dokaz:

Pretpostavimo da je H normalna u grupi G. Tada za bilo koji $x \in G$ i $h \in H$ postoji $h' \in H$ takav da

$$xh = h'x$$

$$\Rightarrow \quad xhx^{-1} = h' \quad \Rightarrow \quad xHx^{-1} \subseteq H$$

Obrnuto, pretpostavimo da je $xHx^{-1} \subseteq H$ za sve $x \in G$.

$x = a \Rightarrow aHa^{-1} \subseteq H \Rightarrow aH \subseteq Ha. \quad \ldots (1)$

S druge strane

$x = a^{-1} \Rightarrow a^{-1}H(a^{-1})^{-1} \subseteq H \Rightarrow a^{-1}Ha \subseteq H \Rightarrow$

$\Rightarrow \quad Ha \subseteq aH \quad \ldots (2)$

(1) i $(2) \Rightarrow aH = Ha$

(#) Neka je $H = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mid a, b, c \in \mathbb{R} \text{ i } ac \neq 0 \right\}$. Da li je $H \triangleleft GL_2(\mathbb{R})$? Obrazložiti svoju tvrdnju.

Rj.

Pokazaćemo da H nije normalna podgrupa grupe $GL_2(\mathbb{R})$. Drugim riječima ~~odredićemo~~ pronaći ćemo matrice $A \in GL_2(\mathbb{R})$ i $B \in H$ takve da $ABA^{-1} \notin H$.

$$A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad A \cdot A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \Rightarrow \begin{array}{l} A = A^{-1} \\ A \in GL_2(\mathbb{R}) \end{array}$$

Neka je $B = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. Primjetimo da $B \in H$.

$$ABA^{-1} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$$

Primjetimo da $ABA^{-1} \notin H$.

H ne zadovoljava uslove prethodne teoreme (test za normalne podgrupe) pa H nije normalna podgrupa grupe G.

(#) Pokazati da je A_n normalna podgrupa grupe S_n.

Rj. I način

$|S_n| = n!$ $\qquad |A_n| = \frac{n!}{2}$

$\#(\text{lijevih klasa od } A_n \text{ u } S_n) = [S_n : A_n] = \frac{|S_n|}{|A_n|} = \frac{n!}{\frac{n!}{2}} = 2$

$\#(\text{desnih klasa od } A_n \text{ u } S_n) = \#(\text{lijevih klasa od } A_n \text{ u } S_n) = 2$

Želimo pokazati da je $aA_n = A_n a$ za $\forall a \in S_n$.

- Ako je $a \in A_n$ tada $aA_n = A_n = A_n a$
- Ako $a \notin A_n$ tada $aA_n \neq A_n \neq A_n a$

$S_n = A_n \cup aA_n$ disjunktna unija dvije različite lijeve klase

$S_n = A_n \cup A_n a$ disjunktna unija dvije različite desne klase

$A_n \cup aA_n = A_n \cup A_n a \xRightarrow{\text{disjunktne unije}} aA_n = A_n a \quad \forall a \notin A_n$

A_n je normalna podgrupa grupe S_n s obzirom da je

$aA_n = A_n a$ za sve $a \in S_n$

II način

$A_n = \{\text{parne permutacije na } n \text{ elemenata}\}$

Pokažimo da $\sigma A_n \sigma^{-1} \subseteq A_n$

$\alpha \in A_n \Rightarrow \alpha$ parna permutacija (prema definiciji od A_n)

$\Rightarrow \sigma \alpha \sigma^{-1}$ je parna permutacija za sve $\sigma \in S_n$

$\Rightarrow \sigma \alpha \sigma^{-1} \in A_n \Rightarrow \sigma A_n \sigma^{-1} \subseteq A_n$

Prema prethodnoj Teoremu A_n je normalna podgrupa grupe S_n.

(#) Neka su H i J normalne podgrupe grupe G. Ako je $H \cap J = \{e\}$ (e je identitet) pokazati da je $xy = yx$ za sve $x \in H$, $y \in J$.

Rj.

$x \in H$, $y \in J$ proizvoljna dva elementa

Posmatrajmo element $xyx^{-1}y^{-1} \in G$.

· Primjetimo $xyx^{-1} \in xJx^{-1} \overset{J \text{ normalna}}{\Longrightarrow} xJx^{-1} \subseteq J$

$\Rightarrow xyx^{-1} \in J$ ...(1)

J podgrupa $\Rightarrow y^{-1} \in J$ ...(2)

(1) i (2) $\Rightarrow xyx^{-1}y^{-1} \in J$

Slično

$$\left.\begin{array}{l} yxy^{-1} \in yHy^{-1} \overset{H \text{ norm.}}{\Longrightarrow} yHy^{-1} \subseteq H \Rightarrow yxy^{-1} \in H \\ x \in H \end{array}\right\} \Rightarrow$$

$\Rightarrow xyx^{-1}y^{-1} \in H$

Time smo dobili da $xyx^{-1}y^{-1} \in J$ i $xyx^{-1}y^{-1} \in H \overset{H \cap J = \{e\}}{\Longrightarrow}$

$xyx^{-1}y^{-1} = e \Rightarrow xyx^{-1} = y \Rightarrow xy = yx \quad \forall x \in H \ \forall y \in J$

q.e.d.

(#) Pretpostavimo da je $N \triangleleft G$ i da je $H \leq G$. Definirimo

$$NH = \{nh : n \in N, h \in H\}.$$

Pokazati da je $NH \leq G$.

Rj. Prisjetimo se:

<u>Teorema</u> (test za podgrupu u jednom koraku)

Neka je G grupa i neka je H neprazan podskup grupe G. Ako je $ab^{-1} \in H$ za proizvoljna dva $a, b \in H$ tada je H podgrupa grupe G.

U rješenju ovog zadatka ćemo koristiti ovu teoremu.

N i H su podgrupe $\Rightarrow$ $e \in N$ i $e \in H$ $\Rightarrow$ $ee = e \in NH$.

$\Rightarrow NH \neq \emptyset$

Sad izaberimo proizvoljna $a, b \in NH$ i pokažimo da $ab^{-1} \in NH$.

$$\left.\begin{array}{l} a \in NH \Rightarrow \exists n_1 \in N \text{ i } h_1 \in H \quad a = n_1 h_1 \\ b \in NH \Rightarrow \exists n_2 \in N \text{ i } h_2 \in H \quad b = n_2 h_2 \end{array}\right\} \Rightarrow ab^{-1} = n_1 h_1 (n_2 h_2)^{-1}$$
$$= n_1 h_1 h_2^{-1} n_2^{-1} \quad \ldots(1)$$

$$N \text{ podgrupa, } n_2 \in N \Rightarrow n_2^{-1} \in N \xRightarrow{N \text{ norm. podgr.}} \underbrace{(h_1 h_2^{-1}) n_2^{-1} (h_1 h_2^{-1})^{-1}}_{= n_3} \in N$$

$$\Rightarrow (h_1 h_2^{-1}) n_2^{-1} = n_3 (h_1 h_2^{-1}) \quad \ldots(2)$$

Uvrstimo (2) u (1):

$$ab^{-1} = n_1 (h_1 h_2^{-1} n_2^{-1}) = \underbrace{(n_1 n_3)}_{\in N} \underbrace{(h_1 h_2^{-1})}_{\in H}$$

zato što su N i H podgrupe

$\Rightarrow ab^{-1} \in H$

q.e.d.

(#) Neka je G grupa i neka je N podgrupa grupe G. Pokazati da je N normalna podgrupa grupe G ako i samo ako $\forall g \in G,\ gNg^{-1} = N$.

R.)

Pretpostavimo da je podgrupa N normalna u grupi G.
U prethodnoj teoremi smo pokazali da je tada $gNg^{-1} \subseteq N\ \forall g \in G$.
Pokažimo da je $N \subseteq gNg^{-1}$.

· $n \in N$

$$\forall g \in G \overset{gNg^{-1} \subseteq N}{\Longrightarrow} g^{-1}ng = g^{-1}n(g^{-1})^{-1} \in N$$

$$\Rightarrow g^{-1}ng = n' \text{ za neko } n' \in N$$

$$\Rightarrow n = gn'g^{-1} \in gNg^{-1}$$

q.e.d.

Pretpostavimo sad da je $gNg^{-1} = N$ za $\forall g \in G$.

$$\Rightarrow \forall n \in N\ \exists n' \in N \text{ t.d. } gng^{-1} = n'$$

$$\Rightarrow gn = n'g \Rightarrow gN \subseteq Ng$$

Slično za $Ng \subseteq gN$.

__Teorem__ (Faktorske grupe)

Neka je G grupa i neka je H normalna podgrupa grupe G. Skup $G/H = \{aH \mid a \in G\}$ je grupa, u odnosu na operaciju $(aH)(bH) = abH$, reda $[G:H]$.

(#) Dokazati teoremu iznad.

Rj. Prvo pokažimo da je operacija dobro definisana. Tj. trebamo pokazati da je korespodencija definisana iznad iz $G/H \times G/H$ u G/H zapravo f-ja. Da bi to dokazali, pretpostavimo da za neke elemente a, a', b i b' iz G, imamo

$$aH = a'H \quad i \quad bH = b'H$$

i provjerimo da li je $aHbH = a'Hb'H$. Tj. provjeriti da je $abH = a'b'H$ (time ćemo pokazati da definicija množenja zavisi samo od klasa a ne od njihovih predstavnika).

$$aH = a'H \Rightarrow \exists h_1 \in H \quad a = a'h_1$$
$$bH = b'H \Rightarrow \exists h_2 \in H \quad b = b'h_2$$

$$a'b'H = ah_1bh_2H = ah_1bH = ah_1Hb = aHb = abH$$

(ovdje smo koristili asocijativnost množenja i činjenicu da je $H \triangleleft G$).

Ostalo je jasno: $eH = H$ je identitet, $a^{-1}H$ je inverz od aH,

$$(aHbH)cH = (ab)HcH = (ab)cH = a(bc)H = (aH)(bc)H = aH(bHcH)$$

Red od G/H je, naravno, broj klasa od H u G.

(#) Dokazati da je faktorska grupa cikličke grupe ciklička.

Rj:

Prisjetimo se:
Grupa G je ciklička ako se može generisati pomoću jednog elementa. Drugim riječima $\exists a \in G$ $G = \langle a \rangle$.
Elementi faktorske grupe G/H su ljeve klase $\{gH \mid g \in G\}$.

Pretpostavimo da je $G = \langle a \rangle$. Neka je G/H neka faktorska grupa (bilo koja) grupe G. Trebamo pokazati da je G/H ciklička.

Proizvoljan element iz G/H je oblika gH za neki $g \in G$.
Kako je G ciklička, postoji cijeli i takav da $g = a^i$.
Pa je $gH = a^i H$.

$$a^i H = \underbrace{aH \cdot aH \cdot \ldots \cdot aH}_{i \text{ puta}} = (aH)^i$$

Time je $gH = (aH)^i$ za proizvoljnu klasu gH.

Time je G/H generisan sa aH, pa je G/H ciklička grupa (prema definiciji cikličke grupe).

(#) Pokazati da je faktorska grupa Abelove grupe Abelova.

Rj.

Prisjetimo se: Grupa G je Abelova akko $ab = ba$ $\forall a, b \in G$

Neka je G abelova grupa i neka je G/H neka faktorska grupa. Trebamo pokazati da je G/H abelova.

Izaberimo proizvoljna dva elementa aH, bH grupe G/H.

Tada

$$(aH)(bH) = (ab)H = (ba)H = (bH)(aH)$$

Prema tome G/H je Abelova.

(#) Neka je $H = \langle 4 \rangle$ podgrupa grupe $G = \mathbb{Z}$ generisana brojem 4.

(a) Napisati sve elemente grupe $H = \langle 4 \rangle$.

(b) Pokazati da je H normalna podgrupa grupe G.

(c) Napisati elemente faktorske grupe $G/H = \mathbb{Z}/\langle 4 \rangle$.

(d) Napisati Cayley-evu tabelu za $\mathbb{Z}/\langle 4 \rangle$.

(e) Odrediti red elementa $2 + \langle 4 \rangle$ u grupi $\mathbb{Z}/\langle 4 \rangle$.

Rj.

(a) Primjetimo da je operacija u grupi $G = \mathbb{Z}$ sabiranje.

$$H = \langle 4 \rangle = \{\ldots -8, -4, 0, 4, 8, \ldots\} = \{4k \mid k \in \mathbb{Z}\}$$

(b) Sabiranje u grupi $\mathbb{Z}$ je komutativno. Pa kako je $G = (\mathbb{Z}, +)$ Abelova grupa to je $\langle 4 \rangle$ normalna podgrupa. (U jednom od prethodnih zadataka smo pokazali da je svaka podgrupa Abelove grupe normalna podgrupa)

(c) Posmatrajmo sljedeće četri klase

$$0 + \langle 4 \rangle = \{\ldots, -8, -4, 0, 4, 8, \ldots\}$$
$$1 + \langle 4 \rangle = \{\ldots, -11, -7, -3, 1, 5, 9, \ldots\}$$
$$2 + \langle 4 \rangle = \{\ldots, -10, -6, -2, 2, 6, 10, \ldots\}$$
$$3 + \langle 4 \rangle = \{\ldots, -9, -5, -1, 3, 7, 11, \ldots\}$$

Tvrdimo da nema više klasa. Ako je $k \in \mathbb{Z}$ tada je $k = 4q + r$, gdje je $0 \le r < 4$; a time $k + \langle 4 \rangle = r + 4q + \langle 4 \rangle = r + \langle 4 \rangle$. Prema tome

$$\mathbb{Z}/\langle 4 \rangle = \{0 + \langle 4 \rangle, 1 + \langle 4 \rangle, 2 + \langle 4 \rangle, 3 + \langle 4 \rangle\}.$$

d)

	$0+\langle 4\rangle$	$1+\langle 4\rangle$	$2+\langle 4\rangle$	$3+\langle 4\rangle$
$0+\langle 4\rangle$	$0+\langle 4\rangle$	$1+\langle 4\rangle$	$2+\langle 4\rangle$	$3+\langle 4\rangle$
$1+\langle 4\rangle$	$1+\langle 4\rangle$	$2+\langle 4\rangle$	$3+\langle 4\rangle$	$0+\langle 4\rangle$
$2+\langle 4\rangle$	$2+\langle 4\rangle$	$3+\langle 4\rangle$	$0+\langle 4\rangle$	$1+\langle 4\rangle$
$3+\langle 4\rangle$	$3+\langle 4\rangle$	$0+\langle 4\rangle$	$1+\langle 4\rangle$	$2+\langle 4\rangle$

e) $|2+\langle 4\rangle| = 2$ kao element grupe $\mathbb{Z}/\langle 4\rangle$.

(#) Odrediti red elementa $2+\langle 5\rangle$ u grupi $\mathbb{Z}/\langle 5\rangle$.

Rj.

$$\mathbb{Z}/\langle 5\rangle = \{0+\langle 5\rangle,\ 1+\langle 5\rangle,\ 2+\langle 5\rangle,\ 3+\langle 5\rangle,\ 4+\langle 5\rangle\}$$

$0+\langle 5\rangle$ je neutralni element

$$(2+\langle 5\rangle)+(2+\langle 5\rangle) = 4+\langle 5\rangle$$

$$(4+\langle 5\rangle)+(2+\langle 5\rangle) = 1+\langle 5\rangle$$

$$(1+\langle 5\rangle)+(2+\langle 5\rangle) = 3+\langle 5\rangle$$

$$(3+\langle 5\rangle)+(2+\langle 5\rangle) = 0+\langle 5\rangle$$

$|2+\langle 5\rangle| = 5$ kao element grupe $\mathbb{Z}/\langle 5\rangle$.

(#) Neka je $H = \langle 6 \rangle$ podgrupa grupe $G = \mathbb{Z}_{18}$.

(a) Napisati sve elemente grupe $H = \langle 6 \rangle$.

(b) Pokazati da je H normalna podgrupa grupe G.

(c) Napisati sve elemente faktorske grupe $\mathbb{Z}_{18}/\langle 6 \rangle$.

(d) Napisati Cayley-evu tabelu za $\mathbb{Z}_{18}/\langle 6 \rangle$.

(e) Odrediti redove elemenata $2 + \langle 6 \rangle$, $3 + \langle 6 \rangle$ i $5 + \langle 6 \rangle$.

Rj.

$$\mathbb{Z}_{18} = \{0, 1, 2, 3, 4, \ldots, 15, 16, 17\}$$

(a)

$$H = \langle 6 \rangle = \{0, 6, 12\}$$

(b) U jednom od prethodnih zadataka smo pokazali da je svaka podgrupa Abelove grupe normalna podgrupa. Kako je $(\mathbb{Z}_{18}, +)$ Abelova grupa, to je $\langle 6 \rangle$ normalna podgrupa grupe $\mathbb{Z}_{18}$.

(npr. $\forall a \in \mathbb{Z}_{18}$ $\quad a + \langle 6 \rangle + (-a) = \{a + 0 + (-a), a + 6 + (-a), a + 12 + (-a)\} = H$)

(c) Za proizvoljan $k \in \mathbb{Z}_{18}$ $\quad k = 6g + r$ za neki $g \in \{0,1,2\}$ i $0 \le r < 6$,

a time $\quad k + \langle 6 \rangle = r + 6g + \langle 6 \rangle = r + \langle 6 \rangle$

$$\mathbb{Z}_{18}/\langle 6 \rangle = \{0 + \langle 6 \rangle, 1 + \langle 6 \rangle, 2 + \langle 6 \rangle, 3 + \langle 6 \rangle, 4 + \langle 6 \rangle, 5 + \langle 6 \rangle\}$$

(d)

	$0+\langle 6\rangle$	$1+\langle 6\rangle$	$2+\langle 6\rangle$	$3+\langle 6\rangle$	$4+\langle 6\rangle$	$5+\langle 6\rangle$
$0+\langle 6\rangle$	$0+\langle 6\rangle$	$1+\langle 6\rangle$	$2+\langle 6\rangle$	$3+\langle 6\rangle$	$4+\langle 6\rangle$	$5+\langle 6\rangle$
$1+\langle 6\rangle$	$1+\langle 6\rangle$	$2+\langle 6\rangle$	$3+\langle 6\rangle$	$4+\langle 6\rangle$	$5+\langle 6\rangle$	$0+\langle 6\rangle$
$2+\langle 6\rangle$	$2+\langle 6\rangle$	$3+\langle 6\rangle$	$4+\langle 6\rangle$	$5+\langle 6\rangle$	$0+\langle 6\rangle$	$1+\langle 6\rangle$
$3+\langle 6\rangle$	$3+\langle 6\rangle$	$4+\langle 6\rangle$	$5+\langle 6\rangle$	$0+\langle 6\rangle$	$1+\langle 6\rangle$	$2+\langle 6\rangle$
$4+\langle 6\rangle$	$4+\langle 6\rangle$	$5+\langle 6\rangle$	$0+\langle 6\rangle$	$1+\langle 6\rangle$	$2+\langle 6\rangle$	$3+\langle 6\rangle$
$5+\langle 6\rangle$	$5+\langle 6\rangle$	$0+\langle 6\rangle$	$1+\langle 6\rangle$	$2+\langle 6\rangle$	$3+\langle 6\rangle$	$4+\langle 6\rangle$

npr. $(5+H)+(4+H)=5+4+H=9+H=3+6+H=3+H$,

(e)

$|2+\langle 6\rangle| = 3$

$|3+\langle 6\rangle| = 2$

$|5+\langle 6\rangle| = 6$

(#) Neka je $\mathcal{K} = \{R_0, R_{180}\}$ podgrupa dihedralne grupe D_4. Napisati Cayleyevu tabelu za $D_4/\mathcal{K}$. (Po potrebi upotrebiti multiplikativnu tabelu za D_4 koju smo imali u jednom od prethodnih zadataka).

Rj: $\mathcal{K} = \{R_0\ R_{180}\}$

$$D_4/\mathcal{K} = \{\mathcal{K},\ R_{90}\mathcal{K},\ H\mathcal{K},\ D\mathcal{K}\}$$

Cayleyeva tabela

	$\mathcal{K}$	$R_{90}\mathcal{K}$	$H\mathcal{K}$	$D\mathcal{K}$
$\mathcal{K}$	$\mathcal{K}$	$R_{90}\mathcal{K}$	$H\mathcal{K}$	$D\mathcal{K}$
$R_{90}\mathcal{K}$	$R_{90}\mathcal{K}$	$\mathcal{K}$	$D\mathcal{K}$	$H\mathcal{K}$
$H\mathcal{K}$	$H\mathcal{K}$	$D\mathcal{K}$	$\mathcal{K}$	$R_{90}\mathcal{K}$
$D\mathcal{K}$	$D\mathcal{K}$	$H\mathcal{K}$	$R_{90}\mathcal{K}$	$\mathcal{K}$

Primjetimo da iako je $R_{90}H = D'$, u tabeli smo napisali koristili $D\mathcal{K}$ za $R_{90}\mathcal{K}H\mathcal{K}$ zato što je $D'\mathcal{K} = D\mathcal{K}$).

$D_4/\mathcal{K}$ nam daje dobru mogućnost da pokažemo na koji način je faktorska grupa grupe G povezana sa samom grupom G. Pretpostavimo da smo zaglavlja kolona Cayleyeve tabele grupe D_4 napisali na takav način da su klase od $\mathcal{K}$ u susjednim kolonama (vidi sljedeću tabelu). Tada se multiplikativna tabela za D_4 može particionisati kvadratiće koji predstavljaju klase od $\mathcal{K}$, i zamjena koja mijenja kvadratić koji sadrži element x sa klasom $x\mathcal{K}$ daje Cayley-evu tabelu za $D_4/\mathcal{K}$.

Na primjer, kada prelazimo sa Cayleyeve tabele grupe D_4, u Cayleyevu tabelu grupe $D_4/\mathcal{K}$, kvadrat

H	V
V	H

postaje element $H\mathcal{K}$. Slično, kvadrat

D	D'
D'	D

postaje element $D\mathcal{K}$ i tako dalje.

	R_0	R_{180}	R_{90}	R_{270}	H	V	D	D'
R_0	R_0	R_{180}	R_{90}	R_{270}	H	V	D	D'
R_{180}	R_{180}	R_0	R_{270}	R_{90}	V	H	D'	D
R_{90}	R_{90}	R_{270}	R_{180}	R_0	D'	D	H	V
R_{270}	R_{270}	R_{90}	R_0	R_{180}	D	D'	V	H
H	H	V	D	D'	R_0	R_{180}	R_{90}	R_{270}
V	V	H	D'	D	R_{180}	R_0	R_{270}	R_{90}
D	D	D'	V	H	R_{270}	R_{90}	R_0	R_{180}
D'	D'	D	H	V	R_{90}	R_{270}	R_{180}	R_0

(#) Neka je $G = H \times K$, gdje su H i K date grupe. Pokazati da je $H \times 1 \triangleleft G$, gdje je $1 = \{1\}$ grupa koja sadrži samo identitet.

Rj.

$G = H \times K$

$H \times 1 \triangleleft G \iff H \times 1 \triangleleft H \times K$

Želimo pokazati da je $g(H \times 1)g^{-1} \subseteq H \times 1$ za $\forall g \in G$.

Neka je $(h,1)$ proizvoljni element iz $H \times 1$ $((h,1) \in H \times 1)$.

Tada za $\forall g \in G$ $(g = (g_1, g_2) \in H \times K)$ imamo da je $g^{-1} = (g_1^{-1}, g_2^{-1})$ i

$$g(h,1)g^{-1} = (g_1 h g_1^{-1}, g_2 1 g_2^{-1}) = (\underbrace{g_1 h g_1^{-1}}_{\in H}, 1) \in H \times 1$$

Time smo pokazali da je $g(H \times 1)g^{-1} \subseteq H \times 1$ $\forall g \in G$

Prema tome $H \times 1 \triangleleft G$.

\# Pronaći redove datih faktorskih grupa:

(a) $(\mathbb{Z}_4 \times \mathbb{Z}_4)/(\langle 2\rangle \times \langle 2\rangle)$;

(b) $(\mathbb{Z}_{12} \times \mathbb{Z}_{18})/\langle(4,3)\rangle$.

Rj.

(a) $\langle 2\rangle \subseteq \mathbb{Z}_4$

$\langle 2\rangle = \{0,2\} \Rightarrow \quad \langle 2\rangle \times \langle 2\rangle = \{(0,0),(0,2),(2,0),(2,2)\}$

$$|\langle 2\rangle \times \langle 2\rangle| = 4$$

$|\mathbb{Z}_4 \times \mathbb{Z}_4| = 16$

Red faktorske grupe $(\mathbb{Z}_4 \times \mathbb{Z}_4)/(\langle 2\rangle \times \langle 2\rangle)$ je $\frac{16}{4} = 4$

(b)

$\langle(4,3)\rangle \subseteq \mathbb{Z}_{12} \times \mathbb{Z}_{18}$

$(4,3)+(4,3)=(8,6)$

$(8,6)+(4,3)=(0,9)$

$(0,9)+(4,3)=(4,12)$

$(4,12)+(4,3)=(8,15)$

$(8,15)+(4,3)=(0,0)$

$\Rightarrow |(4,3)| = 6$

$\Downarrow$

$|\langle(4,3)\rangle| = 6$

Red faktorske grupe $(\mathbb{Z}_{12} \times \mathbb{Z}_{18})/\langle(4,3)\rangle$ je $\frac{12 \cdot 18}{6} = 2 \cdot 18 = 36$.

7. Let $K = \langle 15 \rangle$ be the subgroup of $G = \mathbb{Z}$ generated by 15.

(a) List the elements of $K = \langle 15 \rangle$.
<u>Answer:</u> $K = \langle 15 \rangle = \{15k \mid k \in \mathbb{Z}\}$

(b) Prove that K is normal subgroup of G.
<u>Proof:</u> $(\mathbb{Z}+)$ is Abelian group and any subgroup of an Abelian group is normal (from 5).

(c) List the elements of the factor group $G/K = \mathbb{Z}/\langle 15 \rangle$.
<u>Answer:</u> $G/K = \mathbb{Z}/\langle 15 \rangle = \{i + \langle 15 \rangle \mid 0 \le i \le 14\}$. (There are 15 elements.)
!!! This is just one way of expressing these cosets. Notice that there are many ways of expressing the same coset, eg. $(2+\langle 15 \rangle) = (17+\langle 15 \rangle) = (32+\langle 15 \rangle) = (-13+\langle 15 \rangle) = \dots$.

(d) Write the Cayley table of $G/K = \mathbb{Z}/\langle 15 \rangle$.
<u>Answer:</u> Don't have to actually write it, but make sure that you know what it would look like.

(e) What is the order of $3 + K = 3 + \langle 15 \rangle$ in $\mathbb{Z}/\langle 15 \rangle$?
<u>Answer:</u> $|3 + \langle 15 \rangle| = 5$ in $\mathbb{Z}/\langle 15 \rangle$, since
$(3 + \langle 15 \rangle) + (3 + \langle 15 \rangle) + (3 + \langle 15 \rangle) + (3 + \langle 15 \rangle) + (3 + \langle 15 \rangle) = (15 + \langle 15 \rangle) = (0 + \langle 15 \rangle)$.

(f) What is the order of $4 + K = 4 + \langle 15 \rangle$ in $\mathbb{Z}/\langle 15 \rangle$?
<u>Answer:</u> $|4 + \langle 15 \rangle| = 15$ in $\mathbb{Z}/\langle 15 \rangle$.

(g) What is the order of $5 + K = 5 + \langle 15 \rangle$ in $\mathbb{Z}/\langle 15 \rangle$?
<u>Answer:</u> $|5 + \langle 15 \rangle| = 3$ in $\mathbb{Z}/\langle 15 \rangle$.

(h) What is the order of $6 + K = 6 + \langle 15 \rangle$ in $\mathbb{Z}/\langle 15 \rangle$?
<u>Answer:</u> $|6 + \langle 15 \rangle| = 5$ in $\mathbb{Z}/\langle 15 \rangle$,

(i) Prove that G/K is cyclic.
<u>Answer:</u> $\mathbb{Z}/\langle 15 \rangle$ is generated by $1 + \langle 15 \rangle$, hence it is cyclic.
underlineAnswer 2: $\mathbb{Z}/\langle 15 \rangle$ is cyclic since it is factor of the cyclic group $(\mathbb{Z}, +)$ (this group is generated by 1).

(j) Prove that $G/K = \mathbb{Z}/\langle 15 \rangle$ is isomorphic to $\mathbb{Z}_{15}$.
<u>Answer:</u>

- *One way - using the First Isomorphism Theorem:*
  - Define a group homomorphism: $f : \mathbb{Z} \to \mathbb{Z}_{15}$:
    - Since $\mathbb{Z}$ is cyclic it is enough to define homomorphism on a generator, and extend to all other elements.
    - Define $f(1) := 1(mod15)$ and $f(n1) := n1\ (mod15)$ (i.e. $f(n) := n\ (mod15)$)
    - Since $|1| = \infty$ for $1 \in \mathbb{Z}$ and $|f(1)| = 15$ for $f(1) = 1 \in \mathbb{Z}/\langle 15 \rangle$ we have $|f(1)| \mid |1|$.
  - Claim 1: f is onto (this is quite clear, but here is a detailed proof).

  - * Elements of $\mathbb{Z}_{15}$ are integers $\{0, 1, 2, \ldots, 14\}$
    * For each $n \in \{0, 1, 2, \ldots, 14\} = \mathbb{Z}_{15}$ consider $n \in \mathbb{Z}$.
    * Then $f(n) = n \in \mathbb{Z}_{15}$. Hence f is onto.
  - $Im(f) = \mathbb{Z}_{15}$ (As stated in class this is equivalent to f being onto.)
  - Claim 2: $Ker(f) = \langle 15 \rangle < \mathbb{Z}$ (this is quite clear, but here is a detailed proof).
    * $Ker(f) = \{n \in \mathbb{Z} \mid f(n) = 0 \in \mathbb{Z}_{15}\}$
    * $n \ (mod 15) = r \in \{0, 1, \ldots, 14\}$, where r is the remainder after dividing n by 15, i.e. $n = 15k + r$, for some integer k.
    * If $n \in Ker(f)$ then $f(n) = 0$ and therefore $n = 15k \in \langle 15 \rangle < \mathbb{Z}$.
    * Therefore $Ker(f) \subset \langle 15 \rangle$.
    * $\langle 15 \rangle \subset Ker(f)$ is clear since $x \in \langle 15 \rangle$ implies $x = 15k$ for some integer k and therefore $f(x) = f(15k) = 15k(mod 15) = 0 in \mathbb{Z}_{15}$.
  - First Isomorphism Theorem states: If $f : G \to G'$ is a group homomorphism then $G/Ker(f) \cong Im(f)$.
  - $\mathbb{Z}/\langle 15 \rangle \cong \mathbb{Z}_{15}$

- *Another way, by defining isomorphism and checking all details of being isomorphism:*
  - Elements of $\mathbb{Z}/\langle 15 \rangle$ are left cosets, and operation is addition of cosets (as defined for factor groups!)
  - Elements of $\mathbb{Z}_{15}$: $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14\}$ and addition is modulo 15.
  - Define the map: $f : \mathbb{Z}/\langle 15 \rangle \to \mathbb{Z}_{15}$ by $f(i + \langle 15 \rangle) = r_i$, where r_i is the remainder after dividing i by 15.
    * Notice that f, as defined, is a mapping from $\mathbb{Z}/\langle 15 \rangle$ to $\mathbb{Z}_{15}$ since the values of f are the remainders after dividing by 15, hence they are non-negative integers between 0 and 14.
    * Prove that f is well-defined:
      Suppose the same coset $(i + \langle 15 \rangle)$ is given by another integer j, i.e.
      $(i + \langle 15 \rangle) = (j + \langle 15 \rangle)$.
      Then $f(i + \langle 15 \rangle) = r_i \in \mathbb{Z}_{15}$ and $f(j + \langle 15 \rangle) = r_j \in \mathbb{Z}_{15}$.
      To show that f is well defined we must show that $f(i + \langle 15 \rangle) = f(j + \langle 15 \rangle)$, i.e. WTS $r_i = r_j \in \mathbb{Z}_{15}$.
      From $(i + \langle 15 \rangle) = (j + \langle 15 \rangle)$ it follows that $j \in (i + \langle 15 \rangle)$ and therefore $j = i + k15$ for some integer $k \in \mathbb{Z}$.
      By definition of remainders: $i = n \cdot 15 + r_i$ and $j = m \cdot 15 + r_j$, with $0 \leq r_i, r_j < 15$.
      Therefore from $j = i + k15$, we have $m \cdot 15 + r_j = n \cdot 15 + r_i + k15$. Hence $r_j - r_i = (k + n - m) \cdot 15$ which is an integer multiple of 15. Since the remainders are $0 \leq r_i, r_j < 15$, it follows that $r_j = r_i$.
      Therefore f is a well defined function.

- Let $f : \mathbb{Z}/\langle 15\rangle \to \mathbb{Z}_{15}$ defined by $f(i + \langle 15\rangle) = r_i$, where r_i is the remainder after dividing i by 15. Then f is "one-to-one" function.
  Proof: Suppose there are $a, b \in \mathbb{Z}/\langle 15\rangle$ such that $f(a) = f(b)$. WTS $a = b$.
  From $a, b \in \mathbb{Z}/\langle 15\rangle$, it follows that $a = i + \langle 15\rangle$ and $b = j + \langle 15\rangle$.
  From $f(a) = f(b)$ it follows $f(i + \langle 15\rangle) = f(j + \langle 15\rangle)$, and by definition of f it follows that $r_i = r_j$.
  So $i = n \cdot 15 + r_i$ and $j = m \cdot 15 + r_j$. Therefore $i - j$ is a multiple of 15, hence and element of the subgroup $\langle 15\rangle$.
  Therefore $a = i + \langle 15\rangle = j + \langle 15\rangle = b$.
  Therefore f is a one-to-one function.
- $f : \mathbb{Z}/\langle 15\rangle \to \mathbb{Z}_{15}$ is onto.
  Proof: Let $y \in \mathbb{Z}_{15}$. WTS: there is an $x \in \mathbb{Z}/\langle 15\rangle$ such that $f(x) = y$.
  Since $y \in \mathbb{Z}_{15}$, y is an integer $0 \leq y < 15$.
  Let $x = y + \langle 15\rangle \in \mathbb{Z}/\langle 15\rangle$.
  Then $f(x) = f(y + \langle 15\rangle) = r_y$. Since $0 \leq y < 15$, it follows that $r_y = y$.
  Therefore $f(x) = y$.
  Therefore f is onto.
- $f(a + b) = f(a) + f(b)$
  Proof: Let $a, b \in \mathbb{Z}/\langle 15\rangle$.
  From $a, b \in \mathbb{Z}/\langle 15\rangle$, it follows that $a = i + \langle 15\rangle$ and $b = j + \langle 15\rangle$.
  Then it follows that $a + b = (i + \langle 15\rangle) + (j + \langle 15\rangle) = (i + j) + \langle 15\rangle$
  $f(a + b) = (i + j)\ (mod 15)$
  $f(a) + f(b) = i\ (mod 15) + j\ (mod 15) = (i + j)\ (mod 15)$
  Therefore $f(a + b) = f(a) + f(b)$

– Therefore $f : \mathbb{Z}/\langle 15\rangle \to \mathbb{Z}_{15}$ is an isomorphism. $\square$

8. Let $G = \langle 6 \rangle$ and $H = \langle 24 \rangle$ be subgroups of $\mathbb{Z}$. Show that H is a normal subgroup of G. Write the cosets of H in G. Write the Cayley table for G/H.

Answer: G and H are subgroups of $\mathbb{Z}$, hence operation is addition.

$G = \langle 6 \rangle = \{0, \pm 6, \pm 12, \pm 18, \pm 24, \pm 30, \pm 36, \pm 42, \pm 48, \dots\} = \{6j \mid j \in \mathbb{Z}\}$, multiples of 6.
$H = \langle 24 \rangle = \{0, \pm 24, \pm 48, \dots\} = \{24j \mid j \in \mathbb{Z}\}$, i.e. all integer multiples of 24.

- H is a normal subgroup of G.
  - H is a nonempty subset of G, since elements of H are elements of G (integer multiples of 24 are multiples of 6).
  - H is closed under operation: If $a, b \in H$, then $a = 24m$, and $b = 24n$. Therefore $a + b = 24m + 24n = 24(m + n) \in H$.
  - H is closed under inverses: If $a \in H$, then $a = 24m$. Therefore $-a = 24 \cdot (-m)$, hence $-a \in H$.
  - Since $\mathbb{Z}$ is abelian, G is also abelian and therefore any subgroup of G is normal. Hence H is normal in G.
- Cosets of $H = \langle 24 \rangle$ in $G = \langle 6 \rangle$ are:
  $H = 0 + H = 0 + \langle 24 \rangle = \{\dots, -48, -24, 0, 24, 48, \dots\}$,
  $6 + H = 6 + \langle 24 \rangle = \{\dots, -42, -18, 6, 30, 54, \dots\}$,
  $12 + H = 12 + \langle 24 \rangle = \{\dots, -36, -12, 12, 36, 60, \dots\}$,
  $18 + H = 18 + \langle 24 \rangle = \{\dots, -30, -6, 18, 42, 66, \dots\}$.
- Elements of G/H are the four cosets written above and the Cayley table is:

$G/H = \langle 6 \rangle / \langle 24 \rangle$	$0 + \langle 24 \rangle$	$6 + \langle 24 \rangle$	$12 + \langle 24 \rangle$	$18 + \langle 24 \rangle$
$0 + \langle 24 \rangle$	$0 + \langle 24 \rangle$	$6 + \langle 24 \rangle$	$12 + \langle 24 \rangle$	$18 + \langle 24 \rangle$
$6 + \langle 24 \rangle$	$6 + \langle 24 \rangle$	$12 + \langle 24 \rangle$	$18 + \langle 24 \rangle$	$0 + \langle 24 \rangle$
$12 + \langle 24 \rangle$	$12 + \langle 24 \rangle$	$18 + \langle 24 \rangle$	$0 + \langle 24 \rangle$	$6 + \langle 24 \rangle$
$18 + \langle 24 \rangle$	$18 + \langle 24 \rangle$	$0 + \langle 24 \rangle$	$6 + \langle 24 \rangle$	$12 + \langle 24 \rangle$

9. Viewing $\langle 6 \rangle$ and $\langle 24 \rangle$ as subgroups of $\mathbb{Z}$, prove that $\langle 6 \rangle / \langle 24 \rangle$ is isomorphic to $\mathbb{Z}_4$.

Proof: Elements of $\langle 6 \rangle / \langle 24 \rangle$ are the 4 cosets: $\{(0 + \langle 24 \rangle), (6 + \langle 24 \rangle), (12 + \langle 24 \rangle), (18 + \langle 24 \rangle)\}$ with the above multiplication table.

$|6 + \langle 24 \rangle| = 4$ since $(6 + \langle 24 \rangle) + (6 + \langle 24 \rangle) + (6 + \langle 24 \rangle) + (6 + \langle 24 \rangle) = (0 + \langle 24 \rangle)$.

So $\langle 6 \rangle / \langle 24 \rangle$ can be generated by one element of order 4, therefore it is cyclic of order 4.

The group $\mathbb{Z}_4$ is also cyclic of order 4. By theorem: "Any two cyclic groups of the same order are isomorphic.", it follows that $\langle 6 \rangle / \langle 24 \rangle$ is isomorphic to $\mathbb{Z}_4$.

10. Let $\langle 8 \rangle$ be the subgroup of $\mathbb{Z}_{48}$.

(a) What is the order of the factor group $\mathbb{Z}_{48}/\langle 8 \rangle$?
<u>Answer:</u> Elements of $\mathbb{Z}_{48}$ are $\{0, 1, 2, 3, \ldots 46, 47\}$ and $|\mathbb{Z}_{48}| = 48$.
Elements of $\langle 8 \rangle \subset \mathbb{Z}_{48}$ are $\{0, 8, 16, 24, 32, 40\}$ and $|\langle 8 \rangle| = 6$.
Therefore the order of the factor group is: $|\mathbb{Z}_{48}/\langle 8 \rangle| = |\mathbb{Z}_{48}|/|\langle 8 \rangle| = 48/6 = 8$.

(b) What is the order of $2 + \langle 8 \rangle$ in the factor group $\mathbb{Z}_{48}/\langle 8 \rangle$?
<u>Answer:</u> Elements of $\mathbb{Z}_{48}/\langle 8 \rangle$ are the following cosets:
$\{(0 + \langle 8 \rangle), (1 + \langle 8 \rangle), (2 + \langle 8 \rangle), (3 + \langle 8 \rangle), (4 + \langle 8 \rangle), (5 + \langle 8 \rangle), (6 + \langle 8 \rangle), (7 + \langle 8 \rangle)\}$.
The order of $(2 + \langle 8 \rangle)$ is $|(2 + \langle 8 \rangle| = 4$ since 4 is the smallest number of times $(2 + \langle 8 \rangle)$ must be added to itself in order to get the identity, i.e. such that $(2 + \langle 8 \rangle) + (2 + \langle 8 \rangle) + (2 + \langle 8 \rangle) + (2 + \langle 8 \rangle) = (0 + \langle 8 \rangle)$.

11. Let $G = U(16)$ be the group of units modulo 16.

(a) What is the order of G?
<u>Answer:</u> $G = \{1, 3, 5, 7, 9, 11, 13, 15\}$. So $|G| = 8$.
We also know that $|U(16)| = \phi(16) = \phi(2^4) = 2^3(2 - 1) = 8$.

(b) What is the order of $15 \in U(16)$?
<u>Answer:</u> $15 \cdot 15 = 225 \equiv 1(mod 16)$. Therefore $|15| = 2$ in $U(16)$.
(Another way: $15 \cdot 15 = (-1)(-1) = 1 \equiv 1(mod 16)$)

(c) Let $H =< 15 >$ be the subgroup of $U(16)$ generated by 15. What is the order of the factor group $U(16)/H$?
<u>Answer:</u> $|G| = 8$, $|H| = 2$. Therefore $|G/H| = |G|/|H| = 8/2 = 4$
Also, in more details: $H =< 15 >= \{1, 15\}$.
Elements of G/H are the left cosets of H in G:
$1H = \{1, 15\} = 15H$,
$3H = \{3, 13\} = 13H$
$5H = \{5, 11\} = 11H$
$7H = \{7, 9\} = 9H$

(d) Make the Cayley table of the factor group $U(16)/H$.
<u>Answer:</u>

G/H	$1H$	$3H$	$5H$	$7H$
1H	$1H$	$3H$	$5H$	$7H$
3H	$3H$	$7H$	$1H$	$5H$
5H	$5H$	$1H$	$7H$	$3H$
7H	$7H$	$5H$	$3H$	$1H$

(1) (a) What is the order of the element $3\langle 16\rangle$ within the group $U(35)/\langle 16\rangle$?

Solution. One can compute that $\langle 16\rangle = \{1, 16, 11\}$. We just need to compute powers of $3\langle 16\rangle = \{3, 13, 33\}$ until we hit the identity element of $U(35)/\langle 16\rangle$ (the identity element being $\langle 16\rangle$ itself):

$$\begin{aligned}
(3\langle 16\rangle)^1 &= 3\langle 16\rangle = \{3, 13, 33\} \neq \{1, 16, 11\} \\
(3\langle 16\rangle)^2 &= (3\langle 16\rangle)(3\langle 16\rangle) = 9\langle 16\rangle = \{9, 4, 29\} \neq \{1, 16, 11\} \\
(3\langle 16\rangle)^3 &= (9\langle 16\rangle)(3\langle 16\rangle) = 27\langle 16\rangle = \{27, 12, 17\} \neq \{1, 16, 11\} \\
(3\langle 16\rangle)^4 &= (27\langle 16\rangle)(3\langle 16\rangle) = \{11, 1, 16\}
\end{aligned}$$

Hence $|3\langle 16\rangle| = 4$.
[Note: we've included more computations above than are necessary. We must find the smallest $k > 0$ so that $(3\langle 16\rangle)^k = \langle 16\rangle$. Since $(3\langle 16\rangle)^k = 3^k\langle 16\rangle$, this is equivalent to finding the smallest $k > 0$ with $3^k \in \langle 16\rangle$. One then computes powers of 3 until an element from $\langle 16\rangle$ appears.] □

(b) Suppose that G is a group and $H \triangleleft G$; suppose that $g \in G$ is given so that g has finite order. Prove that the order of gH (as an element of G/H) is finite and divides the order of g (as an element of G). [Note: we now have two meanings for "the order of gH;" one is in thinking of gH as a set of elements, and the other in thinking of gH as an element of the group G/H. In both parts of this problem, we're interested in the order of these cosets as elements in their respective factor groups.]

Solution. Let $n = |g|$. This means that $g^n = e$; in particular this gives $(gH)^n = g^n H = eH = H$. By the order divides lemma, we have $|gH|$ divides n. (In particular, $|gH| < \infty$.) □