Klase podgrupe i Lagrangeov teorem

Definicija (lijeva klasa, desna klasa)

Neka je G grupa i neka je H podgrupa grupe G. Definišimo lijevu klasu podgrupe H sa predstavnikom $g \in G$ na sljedeći način

$$gH = \{gh \mid h \in H\}.$$

Skup gH nazivamo i lijeva klasa podgrupe H u G određena elementom $g \in G$.

Na sličan način definišemo i desnu klasu

$$Hg = \{hg \mid h \in H\}$$

(#) Neka je H podgrupa grupe $\mathbb{Z}_6$ koja sadrži elemente 0 i 3. Odrediti sve lijeve i sve desne klase podgrupe H u $\mathbb{Z}_6$.

R.

$H = \{0, 3\}$

$\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$

$0 + H = \{0, 3\}$ $\quad$ $3 + H = \{0, 3\}$

$1 + H = \{1, 4\}$ $\quad$ $4 + H = \{1, 4\}$

$2 + H = \{2, 5\}$ $\quad$ $5 + H = \{2, 5\}$

Lijeve klase podgrupe H u G su $\{0, 3\}$, $\{1, 4\}$, $\{2, 5\}$.

Kako je $\mathbb{Z}_6$ komutativna grupa, to su lijeva i desna klasa identički jednake.

Desne klase podgrupe H u G su

$H + 0 = H + 3 = \{0, 3\}$

$H + 1 = H + 4 = \{1, 4\}$

$H + 2 = H + 5 = \{2, 5\}$

Neka je D_4 diedralna grupa reda 8, i neka je $\mathcal{K} = \{R_0, R_{180}\}$ podgrupa grupe D_4. Iskoristiti Cayley-evu tabelu grupe D_4, koju smo imali u jednom od prethodnih zadataka, i napisati sve lijeve klase od $\mathcal{K}$ u D_4.

Rj.

$$\mathcal{K} = \{R_0, R_{180}\}$$

$$D_4 = \{R_0, R_{90}, R_{180}, R_{270}, H, V, D, D'\}$$

$$R_0\mathcal{K} = \mathcal{K}$$

$$R_{90}\mathcal{K} = \{R_{90}, R_{270}\}$$

$$R_{180}\mathcal{K} = \mathcal{K}$$

$$R_{270}\mathcal{K} = \{R_{270}, R_{90}\} = R_{90}\mathcal{K}$$

$$H\mathcal{K} = \{H, V\}$$

$$V\mathcal{K} = \{V, H\} = H\mathcal{K}$$

$$D\mathcal{K} = \{D, D'\}$$

$$D'\mathcal{K} = \{D', D\} = D\mathcal{K}$$

Lijeve klase od $\mathcal{K}$ u D_4 su

$$\{R_0, R_{180}\}, \{R_{90}, R_{270}\}, \{H, V\}, \{D, D'\}.$$

(i) Neka je $H=\{(1),(13)\}$ podgrupa grupe S_3. Provjeriti da li je $(132)H = H(132)$

(ii) Neka je $H=\{0,3,6\}$ podgrupa grupe $\mathbb{Z}_9$ u odnosu na operaciju sabiranja. Provjeriti da li je $6+H=5+H$ i da li je $4+H=8+H$. Izračunati $5+H \cap 8+H$.

Rj.

(i) $H=\{(1),(13)\}$

$$(132)H = \{(132)(1), (132)(13)\} = \{(132), (12)(3)\} = \{(12), (132)\}$$

$$H(132) = \{(1)(132), (13)(132)\} = \{(132), (23)\} = \{(23), (132)\}$$

Prema tome $(132)H \neq H(132)$

(ii)

$H=\{0,3,6\}$

$$\left.\begin{array}{l} 6+H=\{6,0,3\}=\{0,3,6\} \\ 5+H=\{5,8,2\}=\{2,5,8\} \end{array}\right\} \Rightarrow \quad 6+H \neq 5+H$$

$$\left.\begin{array}{l} 4+H=\{4,7,1\}=\{1,4,7\} \\ 8+H=\{8,2,5\}=\{2,5,8\} \end{array}\right\} \Rightarrow \quad 4+H \neq 8+H$$

Primjetimo da je $5+H = 8+H = \{2,5,8\}$ pa je

$$5+H \cap 8+H = 5+H = 8+H.$$

Neka je K podgrupa grupe S_3 koja je definisana sa permutacijama $\{(1), (12)\}$. Odrediti sve lijeve i sve desne klase podgrupe K u S_3.

Rj:

$$K = \{(1), (12)\}$$

$$S_3 = \{(1), (12), (13), (23), (123), (132)\}$$

$$(1)K = \{(1), (12)\}$$

$$(12)K = \{(12)(1), (12)(12)\} = \{(1), (12)\}$$

$$(13)K = \{(13)(1), \underbrace{(13)(12)}_{(123)}\} = \{(13), (123)\}$$

$$(23)K = \{(23), (132)\}$$

$$(123)K = \{(13), (123)\}$$

$$(132)K = \{(23), (132)\}$$

Lijeve klase od K su $\{(1), (12)\}$, $\{(13), (123)\}$, $\{(23), (132)\}$.

Desne klase od K su

$$K(1) = K(12) = \{(1), (12)\}$$

$$K(13) = K(132) = \{(13), (132)\}$$

$$K(23) = K(123) = \{(23), (123)\}$$

$$K(132) = \{(1)(132), \underbrace{(12)(132)}_{(13)}\}$$

Primjetimo da u ovom slučaju lijeve klase nisu iste kao i desne klase.

(#) Posmatrajmo grupu $U(20)$ i njezinu cikličku podgrupu $H = \langle 9 \rangle$.

(a) Pokazati da je H podgrupa grupe $U(20)$ i napisati sve lijeve klase od H.

(b) Skup svih lijevih klasa od H formira grupu $U(20)/H$ u odnosu na operaciju $(aH)(bH) = abH$. Napisati Cayleyevu tabelu za $U(20)/H$.

(c) Odrediti sve podgrupe grupe $U(20)/H$.

Rj.

(a) $9 \cdot 9 = 81 \bmod 20 = 1$

$U(20) = \{k \in \mathbb{N} \mid k < 20 \text{ ; } \gcd(k,20) = 1\}$
$= \{1, 3, 7, 9, 11, 13, 17, 19\}$

$H = \{1, 9\}$

Zatvoreno u odnosu na operaciju množenja $\Rightarrow$ H je podgrupa od $U(20)$.

$1H = \{1, 9\}$
$3H = \{3, 27\} = \{3, 7\}$
$7H = \{7, 63\} = \{3, 7\}$

$9H = \{1, 9\}$
$11H = \{11, 99\} = \{11, 19\}$
$13H = \{13, 117\} = \{13, 17\}$

$17H = \{17, 153\}$
$= \{13, 17\}$
$19H = \{11, 19\}$

90
63

Lijeve klase od H su

$\{1, 9\}$, $\{3, 7\}$, $\{11, 19\}$, $\{13, 17\}$

(b)

$1H = \{1, 9\}$
$3H = \{3, 7\}$
$11H = \{11, 19\}$
$13H = \{13, 17\}$

	1H	3H	11H	13H
1H	1H	3H	11H	13H
3H	3H	1H	13H	11H
11H	11H	13H	1H	3H
13H	13H	11H	3H	1H

$(3H)(13H) =$
$= 39H = \{11, 19\}$
$= 11H$

(c)

$$(3H)(3H) = 9H$$

$$(3H)^3 = 7H$$

$$(3H)^4 = 1H$$

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

$$= \{1H, 3H\}$$

$$\langle 11H \rangle = \{1H, 11H\}$$

$$\langle 13H \rangle = \{1H, 13H\}$$

Ako pokušamo kombinacije od dva elementa dobićemo nazad čitavu grupu $U(20)/H$.

Podgrupe od $U(20)/H$ su

$$\{e\},\ U(20)/H,\ \{1H, 3H\},\ \{1H, 11H\},\ \{1H, 13H\}.$$

(#) Posmatrajmo grupu $(\mathbb{Z},+)$ i označimo sa H podgrupu $4\mathbb{Z}$ grupe $\mathbb{Z}$. Napisati četiri lijeve klase podgrupe H u $\mathbb{Z}$.

Rj:

$$H = 4\mathbb{Z} = \{\dots, -12, -8, -4, 0, 4, 8, 12, \dots\}$$

$$0 + H = \{\dots, -12, -8, -4, 0, 4, 8, 12, \dots\}$$

$$1 + H = \{\dots, -11, -7, -3, 1, 5, 9, 13, \dots\}$$

$$2 + H = \{\dots, -10, -6, -2, 2, 6, 10, 14, \dots\}$$

$$3 + H = \{\dots, -9, -5, -1, 3, 7, 11, 15, \dots\}$$

(#) Sa istim oznakama kao u problemu iznad posmatrajmo klase $1+H$ i $2+H$. Šta ćemo dobiti ako saberemo ove dvije klase? Napisati opštu formulu za sumu $n+H$ i $m+H$.

Rj:

$\vdots$	$\vdots$	$\vdots$	
$-11 + (-10) = -21$	$-7 + (-10) = -17$	$-3 + (-10) = -13$	
$-11 + (-6) = -17$	$-7 + (-6) = -13$	$-3 + (-6) = -9$	
$-11 + (-2) = -13$	$-7 + (-2) = -9$	$-3 + (-2) = -5$	
$-11 + (2) = -9$	$-7 + 2 = -5$	$-3 + 2 = -1$	$\dots$
$-11 + 6 = -5$	$-7 + 6 = -1$	$-3 + 6 = 3$	
$-11 + 10 = -1$	$-7 + 10 = 3$	$-3 + 10 = 7$	
$-11 + 14 = 3$	$-7 + 14 = 7$	$-3 + 14 = 11$	
$\vdots$	$\vdots$	$\vdots$	

Sve moguće sume kao rezultat daju $\{\dots, -9, -5, -1, 3, 7, 11, 15, \dots\} = 3 + H$. Opšta formula je

$$(n+H) + (m+H) = (n+m) + H = (n+m \bmod 4) + H$$

(#) Neka je H podgrupa grupe G, i neka su a i b elementi grupe G. Pokazati da

(i) $a \in aH$;

(ii) $aH = H$ ako i samo ako $a \in H$;

(iii) $(ab)H = a(bH)$ i $H(ab) = (Ha)b$.

Rj.

(i) H je podgrupa grupe G $\Rightarrow$ H sadrži jedinični element

$$a = a \cdot e \in aH.$$

(ii) Pretpostavimo da je $aH = H$. Tada $a = ae \in aH = H$ tj. $a \in H$.

Sad pretpostavimo da $a \in H$, i pokažimo da $aH \subseteq H$ i $H \subseteq aH$.

$aH \subseteq H$:

H je podgrupa od G $\Rightarrow$ H je zatvoreno u odnosu na operaciju množenja, pa kako je $a \in H$ to je $aH \subseteq H$

$H \subseteq aH$:

Izaberimo proizvoljni $h \in H$

$$a \in H \text{ i } h \in H \Rightarrow a^{-1}h \in H \Rightarrow h = eh = (aa^{-1})h = a(a^{-1}h) \in aH$$

Rezultat slijedi.

(iii) Ovo slijedi direktno iz osobine $(ab)h = a(bh)$ i $h(ab) = (ha)b$.

(#) Neka je H podgrupa grupe G, i neka su a i b elementi grupe G. Pokazati da

(i) $aH = bH$ ako i samo ako $a \in bH$

(ii) $aH = bH$ ili $aH \cap bH = \emptyset$

(iii) $|aH| = |bH|$.

Rj. (i) Ako je $aH = bH$ tada $a = ae \in aH = bH \Rightarrow a \in bH$.

Obrnuto, ako $a \in bH$ imamo da $a = bh$ gdje je $h \in H$ a time $aH = (bh)H = b(hH) = bH$

(ii) Ova osobina slijedi direktno iz osobine (i), jer ako postoji element $c \in aH \cap bH$ tada $cH = aH$ i $cH = bH$.

(iii) Da bi pokazali da je $|aH| = |bH|$ dovoljno je da definiramo bijekciju sa aH na bH.

Očigledno je da preslikavanje
$$f : aH \to bH$$
$$ah \to bh$$
preslikava aH na bH.

f je injekcija

$$f(ah_1) = f(ah_2) \Rightarrow bh_1 = bh_2 \Rightarrow h_1 = h_2$$

(#) Neka je H podgrupa grupe G, i neka je xH lijeva klasa podgrupe H u G. Pokazati da ako $z \in xH$ tada je $xH = zH$.

Rj.

$z \in xH \Rightarrow \exists h \in H$ t.d. $z = xh \Leftrightarrow zh^{-1} = x$

POKAŽIMO DA JE $xH \subseteq zH$

$y \in xH \Rightarrow \exists g \in H$ t.d. $y = xg \overset{x = zh^{-1}}{\Rightarrow} y = z\underbrace{h^{-1}g}_{\in H} \Rightarrow y \in zH$

Prema tome $xH \subseteq zH$ ...(1)

POKAŽIMO DA JE $zH \subseteq xH$

$y \in zH \Rightarrow \exists s \in H$ t.d. $y = zs \overset{z = xh}{\Rightarrow} y = x\underbrace{hs}_{\in H} \Rightarrow y \in xH$

Time $zH \subseteq xH$ ...(2)

Na osnovu (1) i (2) možemo zaključiti da je $xH = zH$.

(#) Neka je H podgrupa grupe G. Pokazati da $g_1H=g_2H$ ako i samo ako $g_1^{-1}g_2\in H$.

Rj.

Pretpostavimo da je $g_1H=g_2H$.

Kako je H podgrupa, identitet e je u H. Pa imamo $g_2\in g_2H$.

Sad

$$g_2\in g_2H \text{ i } g_2H=g_1H \Rightarrow \exists h\in H \text{ t.d. } g_2=g_1h$$

Množeći obe strane sa g_1^{-1} sa lijeva imamo da je

$$g_1^{-1}g_2=h$$

Kako je $h\in H$ to je $g_1^{-1}g_2\in H$.

Pretpostavimo da $g_1^{-1}g_2\in H$.

Izaberimo proizvoljni $h\in H$, i posmatrajmo g_1h $(g_1h\in g_1H)$.

$g_1^{-1}g_2\in H \Rightarrow (g_1^{-1}g_2)^{-1}\in H \Rightarrow g_2^{-1}g_1\in H$ želimo pokazati da je $g_1h\in g_2H$.

Sad $h\in H$ i $g_2^{-1}g_1\in H$ povlači da $g_2^{-1}g_1h\in H$

Označimo ovaj element sa h' tj. $h'=g_2^{-1}g_1h$ $(h'\in H)$

Primjetimo da je $h=(g_1^{-1}g_2)(g_2^{-1}g_1)h=(g_1^{-1}g_2)h' \Rightarrow g_1h=g_2h'$.

g_2h' je po definiciji element od g_2H. Time smo pokazali da je svaki element od g_1H također element od g_2H.

Kako su oznake g_1 i g_2 proizvoljne, prema istom argumentu imamo da je svaki element od g_2H također element od g_1H. Prema tome $g_1H=g_2H$.

(#) Neka je H podgrupa grupe G, i neka su a i b elementi grupe G. Pokazati da

(i) $aH = Ha$ ako i samo ako $H = aHa^{-1}$.

(ii) aH je podgrupa grupe G ako i samo ako $a \in H$

Rj.

(i) $aH = Ha \iff (aH)a^{-1} = (Ha)a^{-1} \iff (aH)a^{-1} = H(aa^{-1}) \iff$

$\iff aHa^{-1} = H$

(ii) Pretpostavimo da je aH podgrupa grupe G.

Tada aH sadrži jedinični element $e \Rightarrow aH \cap eH \neq \emptyset$

Ranije smo pokazali da $c, d \in G$ $cH = dH$ ili $cH \cap dH = \emptyset$

Ovo znači da $aH = eH = H \Rightarrow a = ae \in aH = H \Rightarrow a \in H$

Obrnuto, pretpostavimo da $a \in H$.

H podgrupa $\Rightarrow$ H zatvoreno $\Rightarrow aH \subseteq H$

$h \in H \Rightarrow a^{-1}h \in H \Rightarrow h = eh = a(a^{-1}h) \in aH \Rightarrow h \in aH \Rightarrow H \subseteq aH$

Prema tome $aH = H$.

$aH \cap eH \neq \emptyset$, pa neka je $c \in aH \cap eH$

$$\left.\begin{array}{l} c \in aH \Rightarrow cH = aH \\ c \in eH \Rightarrow cH = eH \end{array}\right\} \Rightarrow aH = eH$$

$c \in aH \Rightarrow c = ah$ za $h \in H \Rightarrow cH = (ah)H = a(hH) = aH$

Neka su H i K podgrupe grupe G. Pokazati da je presjek $xH \cap yK$ dvije klase od H i K ili prazan skup ili klasa podgrupe $H \cap K$.

Rj.:

Pretpostavimo da je $xH \cap yK \neq \emptyset$, i neka je $z \in xH \cap yK$.

$$z \in xH \xRightarrow{\text{prethodni zadatak}} xH = zH$$

$$z \in yK \xRightarrow{\text{prethodni zadatak}} yK = zK$$

Sad imamo

$$w \in xH \cap yK \iff w \in zH \cap zK \iff \exists h \in H\ \exists k \in K \text{ t.d. } w = zh = zk$$

$$\iff z^{-1}w = h = k \overset{h \in H}{\underset{k \in K}{\Longrightarrow}} z^{-1}w \in H \cap K$$

$$\iff w \in z(H \cap K)$$

Time je $xH \cap yK$ jednako $z(H \cap K)$, klasa od $H \cap K$.

Lema

Neka je H podgrupa grupe G i pretpostavimo da je $g_1, g_2 \in G$. Tada su sljedeći uslovi ekvivalentni

1. $g_1 H = g_2 H$;
2. $H g_1^{-1} = H g_2^{-1}$
3. $g_1 H \subseteq g_2 H$
4. $g_2 \in g_1 H$
5. $g_1^{-1} g_2 \in H$

(#) Dokazati lemu iznad.

Rj.: Pokažimo da vrijedi niz implikacija

$$g_1 H = g_2 H \Rightarrow H g_1^{-1} = H g_2^{-1} \Rightarrow g_1 H \subseteq g_2 H \Rightarrow g_2 \in g_1 H \Rightarrow g_1^{-1} g_2 \in H$$

$$\Rightarrow g_1 H = g_2 H.$$

(i) Pokažimo da $g_1 H = g_2 H$ povlači da $H g_1^{-1} = H g_2^{-1}$.

$$g \in H g_1^{-1} \overset{\exists u \in H}{\Rightarrow} g = u g_1^{-1} \Rightarrow g^{-1} = g_1 u^{-1} \overset{u^{-1} \in H}{\Rightarrow} g^{-1} \in g_1 H$$

$$\Rightarrow g^{-1} \in g_1 H = g_2 H \overset{\exists v \in H}{\Rightarrow} g^{-1} = g_2 v \Rightarrow g = v^{-1} g_2^{-1} \Rightarrow g \in H g_2^{-1}$$

Time smo pokazali da $H g_1^{-1} \subseteq H g_2^{-1}$

Slično bi pokazali da je $H g_2^{-1} \subseteq H g_1^{-1} \Rightarrow H g_1^{-1} = H g_2^{-1}$.

(ii) Pokažimo da $Hg_1^{-1} = Hg_2^{-1}$ povlači da $g_1 H \subseteq g_2 H$.

$$g \in g_1 H \overset{\exists h \in H}{\Longrightarrow} g = g_1 h \Rightarrow g^{-1} = h^{-1} g_1^{-1} \in H g_1^{-1} = H g_2^{-1}$$

$$\Rightarrow g^{-1} \in H g_2^{-1} \overset{\exists u \in H}{\Longrightarrow} g^{-1} = u g_2^{-1} \Rightarrow g = g_2 u^{-1} \in g_2 H \Rightarrow g \in g_2 H$$

Time smo pokazali da $g_1 H \subseteq g_2 H$

(iii) Pokažimo da $g_1 H \subseteq g_2 H$ povlači da $g_2 \in g_1 H$.

Posmatrajmo $g_1 H \cap g_2 H$. Kako je $g_1 H \subseteq g_2 H$ to $g_1 H \cap g_2 H \neq \emptyset$

$$\Rightarrow \exists c \in g_1 H \cap g_2 H$$

$$\left.\begin{array}{l} c \in g_1 H \overset{\exists h \in H}{\Longrightarrow} c = g_1 h \Rightarrow cH = (g_1 h) H = g_1 (hH) = g_1 H \\ c \in g_2 H \overset{\exists u \in H}{\Longrightarrow} c = g_2 u \Rightarrow cH = (g_2 u) H = g_2 (uH) = g_2 H \end{array}\right\} \Rightarrow g_1 H = g_2 H$$

$$g_2 = g_2 e = g_2 H = g_1 H \Rightarrow g_2 \in g_1 H$$

(iv) Pokažimo da $g_2 \in g_1 H$ povlači da $g_1^{-1} g_2 \in H$.

$$g_2 \in g_1 H \overset{\exists h \in H}{\Longrightarrow} g_2 = g_1 h \Rightarrow g_1^{-1} g_2 = h \in H \Rightarrow g_1^{-1} g_2 \in H.$$

(v) Na kraju pokažimo da $g_1^{-1} g_2 \in H$ povlači $g_1 H = g_2 H$.

$$g_1^{-1} g_2 \in H \Rightarrow g_1^{-1} g_2 H = H \Rightarrow g_2 H = g_1 H$$

\# Neka je H podgrupa grupe G. Pokazati da lijeve klase od H u G particioniraju grupu G. Tj. pokazati da je grupa G disjunktna unija lijevih klasa od H u G.

Rj. Neka su $g_1 H$ i $g_2 H$ dvije klase podgrupe H grupe G. Trebamo pokazati da je ili $g_1 H \cap g_2 H = \emptyset$ ili $g_1 H = g_2 H$.

Pretpostavimo da je $g_1 H \cap g_2 H \neq \emptyset$ i da $a \in g_1 H \cap g_2 H$.

Tada prema definiciji lijevih klasa $a = g_1 h_1 = g_2 h_2$ za neke elemente h_1 i h_2 iz H.

Time $g_1 = g_2 h_2 h_1^{-1} \Rightarrow g_1 \in g_2 H$.

Prema prethodnoj Lemi $g_1 H = g_2 H$.

Definicija (indeks)

Neka je G grupa i neka je H podgrupa grupe G. Indeks podgrupe H u grupi G definišemo kao broj lijevih klasa od H u G (podgrupe H u grupi G). Indeks podgrupe H u grupi G ćemo označavati sa $[G:H]$.

\# Odrediti indeks

(i) podgrupe $H=\{0,3\}$ u grupi $\mathbb{Z}_6$.

(ii) podgrupe $\mathcal{K}=\{R_0, R_{180}\}$ u dihedralnoj grupi D_4.

(iii) podgrupe $K=\{(1),(12)\}$ u grupi S_3.

(iv) podgrupe $H=\langle 9\rangle$ u grupi $U(20)$.

Rj.

(i) Prema jednom od prethodnih zadataka imamo da

$$0+H=3+H=\{0,3\}$$
$$1+H=4+H=\{1,4\}$$
$$2+H=5+H=\{2,5\}$$

Indeks podgrupe $H=\{0,3\}$ u grupi $\mathbb{Z}_6$ je 3 tj. $[\mathbb{Z}_6:H]=3$.

(ii) Prema jednom od prethodnih zadataka imamo da

$$R_0\mathcal{K}=R_{180}\mathcal{K}=\{R_0,R_{180}\}$$
$$R_{90}\mathcal{K}=R_{270}\mathcal{K}=\{R_{90},R_{270}\}$$
$$H\mathcal{K}=V\mathcal{K}=\{H,V\}$$
$$D\mathcal{K}=D'\mathcal{K}=\{D,D'\}$$

Indeks podgrupe $\mathcal{K}=\{R_0,R_{180}\}$ u grupi D_4 je 4 tj. $[D_4:\mathcal{K}]=4$.

(iii) Prema jednom od prethodnih zadataka $(1)K=(12)K$, $(13)K=(123)K$, $(23)K=(132)K$

$\Rightarrow$ $[S_3:K]=3$

(iv) $1H=9H$, $3H=7H$, $11H=19H$, $13H=17H$ $\Rightarrow$ $[U(20):\langle 9\rangle]=4$

(#) Neka je H podgrupa grupe G. Pokazati da je broj lijevih klasa podgrupe H u grupi G jednak broju desnih klasa podgrupe H u grupi G.

Rj.:

Označimo redom sa $\mathcal{L}_H$ i $\mathcal{R}_H$ skup svih lijevih i desnih klasa od H u G. Ako uspijemo definisati bijektivno preslikavanje $\phi : \mathcal{L}_H \to \mathcal{R}_H$ tada ćemo imati rješenje zadatka.

. Definišimo ϕ na sljedeći način

$$\phi : \mathcal{L}_H \to \mathcal{R}_H$$
$$gH \to Hg^{-1}.$$

Prema prethodnoj Lemi preslikavanje ϕ je dobro definisano; tj. ako $g_1H = g_2H \Rightarrow Hg_1^{-1} = Hg_2^{-1}$.

ϕ JE JEDAN-NA-JEDAN

$$\phi(g_1H) = \phi(g_2H) \Rightarrow Hg_1^{-1} = Hg_2^{-1} \xRightarrow[\text{Lema}]{\text{prethodna}} g_1H = g_2H$$

ϕ JE NA

Neka je Hg proizvoljan element iz $\mathcal{R}_H$. Primjetimo da je

$$\phi(g^{-1}H) = Hg$$

Teorem (Lagrange-ov teorem: $|H|$ dijeli $|G|$)

Ako je G konačna grupa i H podgrupa grupe G, tada $|H|$ dijeli $|G|$. Štoviše, broj različitih lijevih (desnih) klasa od H u G je $\frac{|G|}{|H|}$.

Dokazati teorem iznad.

Rj: Neka su $a_1H, a_2H, \dots, a_rH$ različite lijeve klase od H u G.

Tada, za svako $a \in G$ imamo da $aH = a_iH$ za neko i. Kako $a \in aH$ to svaki element od G pripada jednoj lijevoj klasi a_iH. Simbolima

$$G = a_1H \cup a_2H \cup \dots \cup a_rH.$$

S obzirom da je $aH = bH$ ili $aH \cap bH = \phi$, možemo zaključiti da je ova unija disjunktna, pa je

$$|G| = |a_1H| + |a_2H| + \dots + |a_rH|.$$

Na kraju, kako je $|a_iH| = |H|$ za svako i, imamo da $|G| = r|H|$.

(i) Neka je G grupa reda 4. Pokazati da svaki element grupe G mora imati red 1, 2 ili 4.

Rj.: Ako je $|G|=4$, prema Lagrange-ovoj teoremi svi elementi od G moraju imati red koji dijeli 4 tj. 1, 2 ili 4.

(ii) Šta možemo zaključiti o grupi G ($|G|=4$) ako znamo da ova grupa sadrži element reda četri.

Rj.: Ako je $g \in G$ element reda 4, to znači da je

$$G = \{1, g, g^2, g^3\}$$

iz čega možemo zaključiti da je G ciklička grupa.

(#) Neka je $\sigma = (1234)(23)$ element grupe S_5. Odrediti indeks podgrupe $\langle \sigma \rangle$ u grupi S_5.

Rj. Označimo sa $H = \langle \sigma \rangle$ i odredimo red podgrupe H.

$$\sigma = (1234)(23) = (124)$$

$$\sigma^2 = (124)(124) = (142)$$

$$\sigma^3 = (124)(142) = (1)(2)(4) = id$$

$$H = \{ id, (124), (142) \}$$

$$|H| = 3$$

$$|S_5| = 5 \cdot 4 \cdot 3 \cdot 2 = 10 \cdot 12 = 120$$

Prema Lagrange-ovoj teoremi broj lijevih klasa podgrupe H u grupi G je jednak $\frac{|G|}{|H|}$.

U našem slučaju $\frac{|S_5|}{|H|} = \frac{120}{3} = 40$

$$[S_5 : \langle \sigma \rangle] = 40.$$

\# Neka su a i b elementi grupe G. Ako je $|a| = 10$ i $|b| = 21$, pokazati da je tada $\langle a \rangle \cap \langle b \rangle = \{e\}$.

Rj:

Neka je c element iz $\langle a \rangle \cap \langle b \rangle$

$c \in \langle a \rangle \Rightarrow$ $\langle c \rangle$ podgrupa grupe $\langle a \rangle$ $\xRightarrow{\text{Lagrangeov teorem}}$

red podgrupe $\langle c \rangle$ dijeli red $\langle a \rangle$ $\Rightarrow$

red od c dijeli 10 ...(1)

$c \in \langle b \rangle \Rightarrow$ $\langle c \rangle$ podgrupa grupe $\langle b \rangle$ $\xRightarrow{\text{Lagrangeov teorem}}$

red podgrupe $\langle c \rangle$ dijeli red $\langle b \rangle$ $\Rightarrow$

red od c dijeli 21

$$\left.\begin{array}{l} |c| \mid 10 \\ |c| \mid 21 \end{array}\right\} \Rightarrow |c| = 1 \Rightarrow c = e$$

Možemo zaključiti $\langle a \rangle \cap \langle b \rangle = \{e\}$

(#) Neka je G grupa reda 4. Pokazati da ili je G ciklička grupa ili $x^2=1$ za svaki $x\in G$. Pokazati da G također mora biti Abelova grupa.

Rj.: Izaberimo $x\in G$ i posmatrajmo $H=\langle a\rangle$.

Ako je $|H|=4$ tada je $H=G$, pa je G ciklička grupa i zadatak je završen.

Pretpostavimo da je $|H|<4$. Kako je H podgrupa grupe G, prema Lagrange-ovoj teoremi imamo da $|H|=2$ ili $|H|=1$, što povlači da je red elementa x 2 ili je red elementa x 1. $(|x|=|\langle x\rangle|)$.

$$\left.\begin{array}{l} \text{Ako je } |x|=2 \Rightarrow x^2=1 \\ \text{Ako je } |x|=1 \Rightarrow x=1 \Rightarrow x^2=1 \end{array}\right\} \Rightarrow \text{u oba slučaja } x^2=1.$$

Pokažimo još da je G Abelova grupa.

Ako je G ciklička grupa tada je G Abelova, s obzirom da su sve cikličke grupe abelove.

Ako je $x^2=1$ za $\forall x\in G$ tada

$$(ab)(ab)=1 \quad \forall a,b\in G \Rightarrow ababba=ba$$

$$\Rightarrow aba1a=ba \Rightarrow abaa=ba \Rightarrow ab1=ba$$

$$\Rightarrow ab=ba$$

iz čega tvrdnja slijedi.

Korolar

(i) Ako je G konačna grupa i H podgrupa grupe G tada $[G:H] = \frac{|G|}{|H|}$.

(ii) U konačnoj grupi, red svakog elementa grupe dijeli red grupe

(iii) Grupa prostog reda je ciklička

(iv) Ako je G konačna grupa i $a \in G$ tada $a^{|G|} = e$.

(v) Za svaki cijeli a i za svaki prost p, $a^p \bmod p = a \bmod p$.

(#) Dokazati korolar iznad.

Rj.

(i) Prema Lagrange-ovoj teoremi broj različitih lijevih klasa od H u G je $\frac{|G|}{|H|}$. Prema tome $[G:H] = \frac{|G|}{|H|}$

(ii) Prisjetimo se da je red elementa jednak redu podgrupe generisane sa tim elementom

(iii) Pretpostavimo da je G prostog reda. Neka je $a \in G$ i $a \neq e$. Tada $|\langle a\rangle|$ dijeli $|G|$ i $|\langle a\rangle| \neq 1$. Time $|\langle a\rangle| = |G|$ iz čega tvrdnja slijedi.

(iv) Prema tvrdnji (ii) imamo da $|G| = |a|k$ za neki pozitivan cijeli k. Time $a^{|G|} = a^{|a|k} = (a^{|a|})^k = e^k = e$.

(v) Prema algoritmu djeljenja (teoremu o ostatku) $a = pm + r$ za neki $0 \leq r < p$. Time ako je $a \bmod p = r$, dovoljno je da dokažemo da $r^p \bmod p = r$. Ako je $r = 0$ rezultat je trivijalan, pa možemo pretpostaviti da je $r \in U(p)$ (prisjetimo se da $U(p) = \{1, 2, \ldots, p-1\}$ u odnosu na operaciju modulo p. Tada, prema tvrdnji (iv): $r^{p-1} \bmod p = 1$, i time $r^p \bmod p = r$.

(#) Pokazati da grupa reda 30 može imati najviše 7 podgrupa reda 5.

Rj. Neka je G data grupa, $|G|=30$ i neka je $H \leq G$ t.d. $|H|=5$. Kako je H podgrupa to $e \in H$, a ostale elemente označimo sa a, b, c i d tj. $H=\{e, a, b, c, d\}$

Kako je $\langle a\rangle \leq H$, $\langle b\rangle \leq H$, $\langle c\rangle \leq H$ i $\langle d\rangle \leq H$ to prema Lagrangeovoj ~~teor.~~ $|a|$ djeli 5, $|b|$ djeli 5, $|c|$ djeli 5 i $|d|$ djeli 5

$\Rightarrow$ $|a|=|b|=|c|=|d|=5$, i svi ovi elementi generišu H.

Time svake dvije različite podgrupe $H_1 \leq G$ i $H_2 \leq G$ reda 5 se mogu sjeći samo u identitetu e, s obzirom da bi bilo koji ne-jedinični element u presjeku generisao obe te grupe.

Pa ako postoji n različitih podgrupa reda 5, one moraju imati najmanje $4n+1$ element (s obzirom da moramo posmatrati jedinicu e).

Prematome, grupa reda 30 može imati najviše 7 podgrupa reda 5.