7 Odseki in Lagrangeov izrek

Definicija (levi odsek, desni odsek)
Naj bo G grupa, $H \leq G$ in $a \leq G$. Potem je množica $aH = \{ah \mid h \in H\}$ levi odsek podgrupe H, ki vsebuje a in $Ha = \{ha \mid h \in H\}$ desni odsek podgrupe H, ki vsebuje a.

1. Naj bo H podgrupa grupe $\mathbb{Z}_6$ ki vsebuje elementa 0 in 3. Poišči vse leve in vse desne odseke podgrupe H v grupi $\mathbb{Z}_6$ [$0 + H = 3 + H = \{0, 3\}$, $1 + H = 4 + H = \{1, 4\}$, $2 + H = 5 + H = \{2, 5\}$]

2. Naj bo D_4 diederska grupa reda 8, in naj bo $\mathcal{K} = \{R_0, R_{180}\}$ podgrupa grupe D_4. Uporabi Cayley-evo tabelo, ki smo jo imeli v eni od prejšnjih nalog, in napiši vse leve odseke podgrupe $\mathcal{K}$ v grupi D_4. [$R_0\mathcal{K} = R_{180}\mathcal{K} = \{R_0, R_{180}\}$, $R_{90}\mathcal{K} = R_{270}\mathcal{K} = \{R_{90}, R_{270}\}$, $H\mathcal{K} = V\mathcal{K} = \{H, V\}$, $\{D, D'\}$]

3. (a) Naj bo $H = \{(1), (13)\}$ podgrupa grupe S_3. Preveri, ali je $(132)H = H(132)$.
[$(132)H = \{(12), (132)\} \neq \{(23), (132)\} = H(132)$]

(b) Naj bo $H = \{0, 3, 6\}$ podgrupa grupe $\mathbb{Z}_9$ glede na operacijo seštevanja. Preveri, ali je $6 + H = 5 + H$ in ali je $4 + H = 8 + H$. Določi, $5 + H \cap 8 + H$. [$5 + H \cap 8 + H = 5 + H = 8 + H$]

4. Naj bo $K = \{(1), (12)\}$ podgrupa grupe S_3. Poišči vse leve in vse desne odseke podgrupe K v grupi S_3. [$K(1) = K(12)$, $K(13) = K(132)$, $K(23) = K(123)$]

5. Imejmo grupo $U(20)$ in njeno ciklično podgrupo $H = \langle 9 \rangle$.

(a) Pokaži, da je H podgrupa grupe $U(20)$ in napiši vse leve odseke podgrupe H.
[$\{1, 9\}$, $\{3, 7\}$, $\{11, 19\}$, $\{13, 17\}$]

(b) Množica vseh levih odsek podgrupe H določa grupo $U(20)/H$ glede na operacijo $(aH)(bH) = abH$. Napiši, Cayley-evo tabelo za $U(20)/H$. [$(3H)(11H) = 13H$, $(3H)(13H) = 11H$]

(c) Določi vse podgrupe grupe $U(20)/H$. [$\{e\}$, $U(20)/H$, $\{1H, 3H\}$, $\{1H, 11H\}$, $\{1H, 13H\}$]

6. (a) Imejmo grupo $(\mathbb{Z}, +)$ in označimo z H podgrupo $4\mathbb{Z}$ grupe $\mathbb{Z}$. Napiši štiri leve odseke podgrupe H v $\mathbb{Z}$.
[$0 + H = \{..., -4, 0, 4, ...\}$, $1 + H = \{..., -3, 1, 5, ...\}$, $2 + H = \{..., -2, 2, 6, ...\}$, $3 + H = \{..., -1, 3, 7, ...\}$]

(b) Naj bosta $1 + H$ in $2 + H$ odseka iz točke (a). Kaj bomo dobili, če seštejmo ta dva odseka? Napiši splošno formulo za vsoto $n + H$ in $m + H$.
[$(n + H) + (m + H) = (n + m) + H = (n + m \bmod 4) + H$]

7. Naj bo H podgrupa grupe G, in naj bosta a in b elementa grupe G. Pokaži, da

(a) $a \in aH$. [$a = ae \in aH$]

(b) $aH = H$ če in samo če $a \in H$. [$a = ae \in aH = H$; $h \in H$, $a^{-1}h \in H$, $h = a(a^{-1}h) \in aH$]

(c) $(ab)H = a(bH)$ in $H(ab) = (Ha)b$. [$(ab)h = a(bh)$, $h(ab) = (ha)b$]

(d) $aH = bH$ če in samo če $a \in bH$.
[$a = ae \in aH = bH$; $a \in bH$, $a = bh$, $aH = (bh)H = b(hH) = bH$]

(e) $aH = bH$ ali $aH \cap bH = \emptyset$. [$c \in aH \cap bH$, $cH = aH$, $cH = bH$]

(f) $aH = bH$ če in samo če $a^{-1}b \in H$. [$aH = bH \Leftrightarrow H = a^{-1}bH$]

(g) $|aH| = |bH|$. [$\phi : aH \to bH$, $\phi(ah) = bh$, ϕ je bijekcija]

(h) $aH = Ha$ če in samo če $H = aHa^{-1}$. [$aH = Ha \Leftrightarrow (aH)a^{-1} = (Ha)a^{-1} \Leftrightarrow ...$]

(i) aH je podgrupa grupe G če in samo če $a \in H$.
[$e \in aH$, $aH \cap eH \neq \emptyset$, $aH = eH = H$, $a \in H$; $a \in H$, $aH = H$]

8. Naj bosta H in K podgrupi grupe G. Pokaži, da je presek $xH \cap yK$ dveh odsekov podgrup H in K ali prazna množica ali odsek podgrupe $H \cap K$. [$w \in xH \cap yK \Leftrightarrow w \in z(H \cap K)$]

Lema

Naj bo H podgrupa grupe G in prevzemimo, da je $g_1, g_2 \in G$. Potem so naslednji pogoji enakovredni

1. $g_1H = g_2H$; 2. $Hg_1^{-1} = Hg_2^{-1}$;
3. $g_1H \subseteq g_2H$; 4. $g_2 \in g_1H$;
5. $g_1^{-1}g_2 \in H$.

9. Dokaži Lemo zgoraj.
[$g_1H = g_2H \Rightarrow Hg_1^{-1} = Hg_2^{-1} \Rightarrow g_1H \subseteq g_2H \Rightarrow ... \Rightarrow g_1^{-1}g_2 \in H \Rightarrow g_1H = g_2H$]

10. Naj bo H podgrupa grupe G. Pokaži, da je grupa G disjunktna unija levih odsekov podgrupe H v grupi G. [$g_1H = g_2H$, $a \in g_1H \cap g_2H$, $g_1 = g_2h_2h_1^{-1}$, $g_1 \in g_2H$]

Definicija (indeks)

Naj bo G grupa in $H \leq G$. Indeks podgrupe H v grupi G značujemo z $[G : H]$ in ga definiramo kot število levih odsekov podgrupe H v grupi G.

11. Določi indeks

(a) podgrupe $H = \{0, 3\}$ v grupi $\mathbb{Z}_6$; [$[\mathbb{Z}_6 : H] = 3$]
(b) podgrupe $\mathcal{K} = \{R_0, R_{180}\}$ v grupi D_4; [$[D_4 : \mathcal{K}] = 4$]
(c) podgrupe $K = \{(1), (12)\}$ v grupi S_3; [$[S_3 : K] = 3$]
(d) podgrupe $H = \langle 9 \rangle$ v grupi $U(20)$. [$[U(20) : \langle 9 \rangle] = 4$]

12. Naj bo H podgrupa grupe G. Pokaži, da je število levih odsekov podgrupe H v grupi G enako številu desnih odsekov podgrupe H v grupi G. [$\phi : \mathcal{L}_H \to \mathcal{R}_H$, $\phi(gH) = Hg^{-1}$, ϕ je bijekcija]

Izrek (Lagrangev izrek: $|H|$ deli $|G|$)

Naj bo G končna grupa in H njena podgrupa. Potem $|H|$ (red podgrupe H) deli $|G|$ (red grupe G). Poleg tega, število različnih levih (desnih) odsekov podgrupe H v grupi G je enak $\dfrac{|G|}{|H|}$.

13. Dokaži Lagrangev izrek zgoraj. [$G = a_1H \cup a_2H \cup ... \cup a_rH$, $|G| = |a_1H| + |a_2H| + ... + |a_rH|$]

14. Naj bo G grupa reda 4.

(a) Pokaži, da ima vsak element grupe G red 1, 2 ali 4. [ker 1, 2 in 4 delijo 4]
(b) Kaj lahko zaključimo o grupi G, če vemo, da ta grupa vsebuje element reda štiri. [G cikl.]

15. Naj bo $\sigma = (1234)(23)$ element grupe S_5. Določi indeks podgrupe $\langle \sigma \rangle$ v grupi S_5. [40]

16. Naj bosta a in b elementa grupe G. Če je $|a| = 10$ in $|b| = 21$, pokaži, da je potem $\langle a \rangle \cap \langle b \rangle = \{e\}$. [$c \in \langle a \rangle \cap \langle b \rangle$, $|c|$ deli 10, $|c|$ deli 21]

17. Naj bo G grupa reda 4. Pokaži, da je G bodisi ciklična grupa, ali pa je $x^2 = 1$ za vsak $x \in G$. Pokaži tudi, da mora biti G abelska grupa. [vsaka cikl. gr. je abel.; $(ab)(ab) = 1$, $ababba = ba$, $ab = ba$]

Posledica

(i) Če je G končna grupa in $H \leq G$ potem je $[G : H] = \frac{|G|}{|H|}$.
(ii) V končni grupi, red vsakega elementa grupe deli red grupe.
(iii) Grupa praštevilskega reda je ciklična.
(iv) Če je G končna grupa in $a \in G$ potem $a^{|G|} = e$.
(v) Za vsako celo število a in za vsako praštevilo p, $a^p \bmod p = a \bmod p$.

18. Dokaži Posledico zgoraj. [uporabi Lagrangev izrek]

19. Pokaži, da ima grupa reda 30 lahko največ 7 podgrup reda 5. [$H = \{e, a, b, c, d\}$, $|a| = |b| = |c| = |d| = 5$, $H_1 \leq G$ in $H_2 \leq G$ ($|H_1| = |H_2| = 5$ in $H_1 \neq H_2$) $\Rightarrow H_1 \cap H_2 = \{e\}$, $4n + 1$]