7 Odseki in Lagrangeov izrek

Definicija (levi odsek, desni odsek)
Naj bo G grupa, $H \leq G$ in $a \in G$. 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 ($H = \{0, 3\}$). Poišči vse leve in vse desne odseke podgrupe H v grupi $\mathbb{Z}_6$.

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.

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

(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, $5 + H \cap 8 + H$.

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

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.

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

(c) Določi vse podgrupe grupe $U(20)/H$.

6. (a) Imejmo grupo $(\mathbb{Z}, +)$ in označimo z H podgrupo $4\mathbb{Z}$ grupe $\mathbb{Z}$ ($H := 4\mathbb{Z}$). Napiši štiri leve odseke podgrupe H v $\mathbb{Z}$.

(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 $m + H$.

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

(a) $a \in aH$.

(b) $aH = H$ če in samo če $a \in H$.

(c) $(ab)H = a(bH)$ in $H(ab) = (Ha)b$.

(d) $aH = bH$ če in samo če $a \in bH$.

(e) $aH = bH$ ali $aH \cap bH = \emptyset$.

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

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

(h) $aH = Ha$ če in samo če $H = aHa^{-1}$.

(i) aH je podgrupa grupe G če in samo če $a \in H$.

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 $H \cap K$.

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.

10. Naj bo H podgrupa grupe G. Pokaži, da je grupa G disjunktna unija levih odsekov podgrupe H v grupi G.

Definicija (indeks)
Naj bo G grupa in $H \leq G$. Indeks podgrupe H v grupi G značujemo z $[G : H]$ (ali s $|G : H|$) in ga definiramo kot število levih odsekov podgrupe H v grupi G.

11. Določi indeks

(a) podgrupe $H = \{0, 3\}$ v grupi $\mathbb{Z}_6$;

(b) podgrupe $\mathcal{K} = \{R_0, R_{180}\}$ v grupi D_4;

(c) podgrupe $K = \{(1), (12)\}$ v grupi S_3;

(d) podgrupe $H = \langle 9 \rangle$ v grupi $U(20)$.

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.

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.

14. Naj bo G grupa reda 4.

(a) Pokaži, da ima vsak element grupe G red 1, 2 ali 4.

(b) Kaj lahko zaključimo o grupi G, če vemo, da ta grupa vsebuje element reda štiri.

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

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

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.

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.

19. Pokaži, da ima grupa reda 30 lahko največ 7 podgrup reda 5.

Évariste Galois

> Galois at seventeen was making discoveries of epochal significance in the theory of equations, discoveries whose consequences are not yet exhausted after more than a century.
>
> *E. T. Bell, Men of Mathematics*

Évariste Galois (pronounced gal-WAH) was born on October 25, 1811, near Paris. Although he had mastered the works of Legendre and Lagrange at age 15, Galois twice failed his entrance examination to the École Polytechnique. He did not know some basic mathematics, and he did mathematics almost entirely in his head, to the annoyance of the examiner.

At 18, Galois wrote his important research on the theory of equations and submitted it to the French Academy of Sciences for publication. The paper was given to Cauchy for refereeing. Cauchy, impressed by the paper, agreed to present it to the academy, but he never did. At the age of 19, Galois entered a paper of the highest quality in the competition for the Grand Prize in Mathematics, given by the French Academy of Sciences. The paper was given to Fourier, who died shortly thereafter. Galois's paper was never seen again.

Galois spent most of the last year and a half of his life in prison for revolutionary political offenses. While in prison, he attempted suicide and prophesied that he would die in a duel. On May 30, 1832, Galois was shot in a duel; he died the next day at the age of 20.

Among the many concepts introduced by Galois are normal subgroups, isomorphisms, simple groups, finite fields, and Galois theory. His work provided a method for disposing of several famous constructability problems, such as trisecting an arbitrary angle and doubling a cube. In his book Love and Math Edward Frenkel wrote "His [Galois's] brilliant insight has forever changed the way people think about numbers and equations." Galois's entire works fill only 60 pages.

POMEMBNI REZULTATI (Odseki in Lagrangeov izrek.)

1. Če je H podgrupa grupe G, potem sta vsaka dva desna (ali leva) odseka podgrupe H v grupi G enaka ali disjunktna.
2. Če je H podgrupa grupe G, potem obstaja bijektivna korespodenca med vsakima dvema desnima (ali levima) odsekoma podgrupe H v grupi G.
3. Če je H podgrupa grupe G, potem je unija vseh desnih (ali levih) odsekov podgrupe H v grupi G enaka grupi G.
4. Če je H podgrupa grupe G, potem desni (ali levi) odseki podgrupe H v grupi G porodio particijo grupe G.
5. **Lagrangeov izrek**. Red vsake podgrupe končne grupe deli red grupe.
6. Če je G končna grupa glede na operacijo množenja potem je $a^{o(G)} = e \ \forall a \in G$.

Rešitve: **1.** $[0+H = 3+H = \{0,3\},\ 1+H = 4+H = \{1,4\},\ 2+H = 5+H = \{2,5\}]$ **2.** $[R_0\mathcal{K} = = R_{180}\mathcal{K} = \{R_0, R_{180}\},\ R_{90}\mathcal{K} = R_{270}\mathcal{K} = \{R_{90}, R_{270}\},\ H\mathcal{K} = V\mathcal{K} = \{H, V\},\ \{D, D'\}]$ **3.**(a) $[(132)H = = \{(12),(132)\} \neq \{(23),(132)\} = H(132)]$; (b) $[5+H \cap 8+H = 5+H = 8+H]$. **4.** $[K(1) = K(12),\ K(13) = K(132),\ K(23) = K(123)]$ **5.**(a) $[\{1,9\},\ \{3,7\},\ \{11,19\},\ \{13,17\}]$; (b) $[(3H)(11H) = 13H,\ (3H)(13H) = 11H]$; (c) $[\{e\},\ U(20)/H,\ \{1H,3H\},\ \{1H,11H\},\ \{1H,13H\}]$. **6.**(a) $[0+H = \{...,-4,0,4,...\},\ 1+H = \{...,-3,1,5,...\},\ 2+H = \{...,-2,2,6,...\},\ 3+H = \{...,-1,3,7,...\}]$; (b) $[(n+H)+(m+H) = (n+m)+H = (n+m \bmod 4)+H]$ **7.**(a) $[a = ae \in aH]$; (b) $[a = ae \in aH = H;\ h \in H,\ a^{-1}h \in H,\ h = a(a^{-1}h) \in aH]$; (c) $[(ab)h = a(bh),\ h(ab) = (ha)b]$; (d) $[a = ae \in aH = bH;\ a \in bH,\ a = bh,\ aH = (bh)H = b(hH) = bH]$; (e) $[c \in aH \cap bH,\ cH = aH,\ cH = bH]$; (f) $[aH = bH \Leftrightarrow H = a^{-1}bH]$; (g) $[\phi : aH \to bH,\ \phi(ah) = bh,\ \phi$ je bijekcija$]$; (h) $[aH = Ha \Leftrightarrow (aH)a^{-1} = (Ha)a^{-1} \Leftrightarrow ...]$; (i) $[e \in aH,\ aH \cap eH \neq \emptyset,\ aH = eH = H,\ a \in H;\ a \in H,\ aH = H]$. **8.** $[w \in xH \cap yK \Leftrightarrow w \in z(H \cap K)]$ **9.** $[g_1H = g_2H \Rightarrow Hg_1^{-1} = Hg_2^{-1}$

$\Rightarrow g_1H \subseteq g_2H \Rightarrow ... \Rightarrow g_1^{-1}g_2 \in H \Rightarrow g_1H = g_2H$] **10.** [$g_1H = g_2H$, $a \in g_1H \cap g_2H$, $g_1 = g_2h_2h_1^{-1}$, $g_1 \in g_2H$] **11.**(a) [$[\mathbb{Z}_6 : H] = 3$]; (b) [$[D_4 : \mathcal{K}] = 4$]; (c) [$[S_3 : K] = 3$]; (d) [$[U(20) : \langle 9 \rangle] = 4$]. **12.** [$\phi : \mathcal{L}_H \to \mathcal{R}_H$, $\phi(gH) = Hg^{-1}$, ϕ je bijekcija] **13.** [$G = a_1H \cup a_2H \cup ... \cup a_rH$, $|G| = |a_1H| + |a_2H| + ... + |a_rH|$] **14.**(a) [ker 1, 2 in 4 delijo 4]; (b) [G cikl.] **15.** [40] **16.** [$c \in \langle a \rangle \cap \langle b \rangle$, $|c|$ deli 10, $|c|$ deli 21] **17.** [vsaka cikl. gr. je abel.; $(ab)(ab) = 1$, $ababba = ba$, $ab = ba$] **18.** [uporabi Lagrangev izrek] **19.** [$H = \{e, a, b, c, d\}$, $|a| = |b| = |c| = |d| = 5$, $H_1 \leq G$ in $H_2 \leq G$ ($|H_1| = |H_2| = 5$ in $H_1 \neq H_2$) $\Rightarrow H_1 \cap H_2 = \{e\}$, $4n + 1$]

Appendix.[181920]

dictionaries

literal	// None, just empty constructor:
	`d := AssociativeArray();`
	`d["t"] := 1;`
	`d["f"] := 0;`

size	`#d;`
lookup	`d["t"];`
update	`d["f"] := -1;`
missing key behavior	Runtime error
is key present	`IsDefined(d, "t");`
delete	`Remove(~d, "t");`
keys and values as arrays	`Keys(d);`

functions

define function	`add := function(a, b)`
	`  return a + b;`
	`end function;`
	// no return value:
	`show := procedure(s)`
	`  print(s);`
	`end procedure;`

invoke function	`add(3, 7);`

execution control

if	`if n gt 0 then`
	`  print "positive";`
	`else`
	`  if n lt 0 then`
	`  print "negative";`
	`  else`
	`  print "zero";`
	`  end if;`
	`end if;`

while	`i := 0;`
	`while i lt 10 do`
	`  print i;`
	`  i := i + 1;`
	`end while;`

for	`for i := 0 to 9 by 1 do` (or `for i in [0..9] do`)
	`  print i;`
	`end for;`

break	`break;`

[18]To write MAGMA code please open: `http://magma.maths.usyd.edu.au/calc/`

[19]See also: `http://www.maths.usyd.edu.au/u/bobh/UoS/MATH2008/ctut07.pdf`

[20]or `http://hyperpolyglot.org/more-computer-algebra`