5 Permutacijske grupe

Definicija (permutacij množice A, grupa permutacij množice A)

Permutacij množice A je bijekcija iz A v A.

Množica vseh permutacij množice A je grupa glede na operacijo kompozicije funkcij. To grupo imenujemo grupa permutacij množice A.

1. (a) Podaj primer permutacije množice $\{1,2,3,4\}$. Dobljeno permutacijo α napiši v vrstni obliki $\begin{pmatrix} 1 & 2 & 3 & 4 \\ \alpha(1) & \alpha(2) & \alpha(3) & \alpha(4) \end{pmatrix}$.

(b) Permutacijo $\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 3 & 1 & 6 & 2 & 4 \end{pmatrix}$ množice $\{1,2,3,4,5,6\}$ prikaži grafično (s pomočjo Vene-ovega diagrami), in izračunaj $\beta(3)$, $\beta(5)$ in $\beta(6)$.

(c) Dana sta permotacij $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 3 & 5 & 1 \end{pmatrix}$ in $\gamma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 1 & 2 & 3 \end{pmatrix}$ množice $\{1,2,3,4,5\}$. Izračunaj $\gamma\sigma$ in $\sigma\gamma$.

Definicija (simetrična grupa S_n, permutacijska grupa)

Grupa vseh permutacij množice $\{1,2,...,n\}$ se imenuje simetrična grupa reda n in se označuje z S_n. Elementi grupe S_n imajo obliko $\alpha = \begin{pmatrix} 1 & 2 & ... & n \\ \alpha(1) & \alpha(2) & ... & \alpha(n) \end{pmatrix}$.

Podgrupa grupe S_n se imenuje permutacijska grupa.

2. (a) Napiši vse elemente grupe S_3. Ali je S_3 abelska grupa?

(b) Dani so elementi $a, b, c \in S_4$, $a = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$, $b = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$, $c = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$. Določi red grupe $\langle a, b, c \rangle$.

(c) Določi red grupe S_n.

Definicija (cikli permutacije)

Naj bo $\sigma \in S_n$. Če obstaja niz $x_1, x_2, ..., x_r \in \{1,2,...,n\}$, tak da je

$\sigma(x_i) = x_{i+1}$ $(i = 1,2,...,r-1)$

$\sigma(x_r) = x_1$

$\sigma(x) = x$ $(x \notin \{x_1, x_2, ..., x_r\})$

tedaj permutacijo σ označimo z $(x_1\, x_2 \ldots x_{r-1}\, x_r)$ in jo imenujemo cikel dolžine r. Cikel dolžine dva (2-cikel) se imenuje transpozicij.

Dva cikla $(a_1\, a_2 \ldots a_r)$ in $(b_1\, b_2 \ldots b_s)$ sta disjunktna če in samo če sta množici $\{a_1, a_2, ..., a_r\}$ in $\{b_1, b_2, ..., b_s\}$ disjunktni.

3. (a) Permutaciji $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 5 & 4 \end{pmatrix}$ in $\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 1 & 2 & 3 \end{pmatrix}$ napiši kot produkt disjunktnih ciklov (v cikličnem zapisu), potem pa izračunaj $\alpha\beta$.

(b) Permutacijo $\mathrm{id} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix}$ napiši v cikličnem zapisu.

4. Naj bosta $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 1 & 3 & 5 & 4 & 7 & 6 & 8 \end{pmatrix}$ in $\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 3 & 8 & 7 & 6 & 5 & 2 & 4 \end{pmatrix}$.

(a) Napiši α in β kot produkt disjunktnih ciklov.

(b) Napiši α in β kot produkt 2-ciklov (kot produkt transpozicij).

(c) Določi α^{-1}, β^{-1}, α^{554} in β^{455}.

5. (a) Permutaciji $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 4 & 6 & 5 & 3 \end{pmatrix}$

in $\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 3 & 1 & 6 & 2 & 4 \end{pmatrix}$ napiši v obliki produkta ciklov. Določi α^{-1} in β^{-1}.

(b) Dana sta dva elementa grupe S_8, $\alpha = (13)(27)(456)(8)$ in $\beta = (1237)(648)(5)$. Produkt $\alpha\beta$ napiši v obliko disjunktinih ciklov (v ciklični zapisi). Določi $(\alpha\beta)^{-1}$.

6. (a) Pokaži, da se vsaka permutacija končne množice lahko napiše kot cikel ali kot produkt disjunktnih ciklov.

(b) Pokaži, da če je par ciklov $\alpha = (a_1, a_2, ..., a_m)$ in $\beta = (b_1, b_2, ..., b_n)$ disjunktan, potem je $\alpha\beta = \beta\alpha$.

7. (a) Naj bo S_n simetrična grupa. Identiteto $\mathrm{id} \in S_n$ zapiši kot produkt cikli dolžine 2 (kot produkt transpozicij).

(b) Permutacije (12345) in (1632)(457) napiši kot produkt transpozicij.

8. Pokaži, da se vsaka permutacija v S_n ($n > 2$) lahko napiše kot produkt ciklov dolžine 2 (kot produkt transpozicij).

Lema Naj bo id identiteta grupe S_n. Če je $\mathrm{id} = \beta_1\beta_2...\beta_r$, kjer so β-i transpozicije, potem je r sodo število.

9. Dokaži Lemo zgoraj.

10. Naj bo α dana permutacija. Če je $\alpha = \beta_1\beta_2...\beta_r$ in $\alpha = \gamma_1\gamma_2...\gamma_s$ kjer so β-i in γ-i transpozicije. Pokaži, da sta r in s bodisi oba soda, bodisi oba liha.

Definicija (sode in lihe permutacije)
Permutacija $\alpha \in S_n$ je soda, če se lahko napiše kot produkt sodo mnogo transpozicij (tj. cikli oblike (ij)). Permutacija $\alpha \in S_n$ je liha, če ni soda.

11. Če je α soda permutacija, pokaži da je α^{-1} tudi soda. Če je α liha, pokaži da je α^{-1} tudi liha.

12. Naj bo A_n množica vseh sodih permitacij iz grupe S_n. Pokaži, da je A_n grupa glede na operaciji kompozicije (tj. glede na operacijo ki je podedovana iz S_n).

Definicija (alternativna grupa reda n) Grupo sodih permutacij na n elementih označujemo z A_n in imenujemo alternirajoča grupa reda n.

13. (a) Ali lihe permutacije iz S_n oblikujejo grupo? Obrazloži svojo trditev.

(b) Pokaži, da se permutacija (1234) ne more napisati kot produkt 3-ciklov, (kot produkt ciklov dolžine 3).

14. (a) Določi vse elemente grup A_2, A_3 in A_4. Ali je katera od teh grup abelska?

(b) Določi in dokaži formulo za število elementov grupe A_n.

15. Pokaži, da je permutacija lihega reda vedno soda permutacija. (Z drugimi besedami, pokaži, da če ima $\alpha \in S_n$ lih red, te da je $\alpha \in A_n$).

16. Pokaži, da je funkcija iz končne množice S nase injekcija če in samo če je surjekcija. Ali je to res, če je S neskončna množica?

Trditev (red permutacije) Naj bo α produkt disjunktnih ciklov dolžin k_1, k_2, ..., k_r. Potem je red permutacije α najmanjši skupni večkratnik naravnih števil k_1, k_2, ..., k_r.

17. Dokaži Trditev zgoraj.

18. Določi rede vsake od naslednjih permutacij: (a) (124)(357), (b) (124)(95367), (c) (124)(35), (d) (124)(357869), (e) (1235)(24567), (f) (345)(245).

19. (a) Določi rede vseh $7! = 5040$ elementov iz S_7.

(b) Določi število elementov reda 3 grupe S_7.

Alan Turing

> Every time you use a phone, or a computer, you use the ideas that Alan Turin invented. Alan discovered intelligence in computers, and today he surrounds us. A true hero of mankind.
>
> *Eric E. Schmidt, Executive Chairman, Google*

On Time magazine's list of the 100 most influential people of the twentieth century was Alan Turing, a mathematician born in London on June 23, 1912. While a college student Turing developed ideas that would lay the foundation for theoretical computer science and artificial intelligence. After graduating from college Turing became a crucial member of a team of cryptologists working for the British government who successfully broke the Enigma codes.

Turing's life took a tragic turn in 1952 when he admitted that he had engaged in homosexual acts in his home, which was a felony in Britain at that time. As punishment, he was chemically castrated and subjected to estrogen treatments. Despondent by this treatment, he committed suicide two years later by eating an apple laced with cyanide at the age of 41.

Today Turing is widely honored for his fundamental contributions to computer science and his role in the defeat of Germany in World War II. Many rooms, lecture halls, and buildings at universities around the world have been named in honor of Turing. The annual award for contributions to the computing community, which is widely consider to be the equivalent to a Nobel Prize, is called the "Turing Award."

In 2013, Queen Elizabeth II granted Turing a pardon and issued a statement saying Turing's treatment was unjust and "Turing was an exceptional man with a brilliant mind who deserves to be remembered and recognized for his fantastic contribution to the war effort and his legacy to science."

POMEMBNI REZULTATI (Permutacijske grupe.)

1. Množica S_A vseh permutacij neprazne množice A je grupa glede na operacijo kompozicije funkcij.
2. Vsaka grupa je izomorfna neki permutacijski grupi (Cayley).
3. Vsaka permutacija se lahko napiše kot produkt transpozicij.
4. Množica vseh sodih permutacij končne množice je grupa glede na operacijo kompozicije funkcij.
5. Red permutacije končne množice zapisane kot produkt disjunktnih ciklov je najmanjši skupni večkratnik dolžine ciklov.
6. Če je π permutacija potem $\pi(a_1a_2...a_k)\pi^{-1} = (\pi(a_1)\pi(a_2)...\pi(a_k))$.

Rešitve: **1.**(a) $[\begin{pmatrix}1&2&3&4\\2&3&1&4\end{pmatrix}]$; (b) $[\beta(3)=1,\ \beta(5)=2,\ \beta(6)=4]$; (c) $[\gamma\sigma = \begin{pmatrix}1&2&3&4&5\\4&2&1&3&5\end{pmatrix}$, $\sigma\gamma = \begin{pmatrix}1&2&3&4&5\\1&5&2&4&3\end{pmatrix}]$. **2.**(a) $[|S_3|=6]$; (b) $[|\langle a,b,c\rangle|=4]$; (c) $[|S_n|=n!]$ **3.**(a) $[\alpha=(12)(45),$ $\beta=(153)(24),\ \alpha\beta=(14)(253)]$; [id = (5) = (1) = ...] **4.**(a) $[\alpha=(12)(45)(67),\ \beta=(23847)(56)]$; (b) $[\beta=(27)(24)(28)(23)(56)]$; (c) $[\alpha^{554}=\mathrm{id},\ \beta^{455}=(56)]$. **5.**(a) $[\alpha=(12)(346),\ \beta=(1523)(46),$ $\alpha^{-1}=(643)(12),\ \beta^{-1}=(46)(3251)]$; (b) $[(\alpha\beta)^{-1}=(56)(48)(2371)]$. **6.**(a) $[a_1\in A,$ $a_2=\alpha(a_1), a_3=\alpha(a_2)=\alpha^2(a_1), ..., \alpha^m(a_1)=a_1,\ \alpha=(a_1,a_2,...,a_m)(...)...]$; (b) $[S=\{a_1,a_2,...,a_m,b_1,b_2,...b_n,c_1,c_2,...,c_k\},\ \alpha\beta(x)=\beta\alpha(x),\ \forall x\in S]$. **7.**(a) [id = (12)(12)]; (b) [(12345) = (15)(14)(13)(12)]. **8.** $[(a_1,a_2,...,a_k)(b_1,b_2,...,b_t)(c_1,c_2,...,c_s)=(a_1,a_k)...(a_1a_2)(b_1,b_t)..$ $..(b_1,b_2)...(c_1,c_2)]$ **9.** [uporabi matematično indukcijo; $\alpha=\beta_1\beta_2...\beta_r=\beta_1\beta_2...\beta_{r-1}(ab),\ \beta_r=(ab),\ 1^\circ$ $\beta_{r-1}\beta_r=(ab)(ab)\Rightarrow\beta_{r-1}\beta_r=id;\ 2^\circ\ \beta_{r-1}\beta_r=(ac)(ab)\Rightarrow\beta_{r-1}\beta_r=(abc)=(ab)(bc),\ 3^\circ\ \beta_{r-1}\beta_r=(bc)(ab)$ $\Rightarrow\beta_{r-1}\beta_r=(acb)=(ac)(cb),\ 4^\circ\ \beta_{r-1}\beta_r=(cd)(ab)\Rightarrow\beta_{r-1}\beta_r=(ab)(cd);$ $\alpha=\beta_1...\beta_{r-2}\beta_{r-1}\beta_r=\beta_{r-2}\gamma_{r-1}\gamma_r,\ a\notin\gamma_r$ ...] **10.** [id $=\gamma_1\gamma_2...\gamma_s\beta_r...\beta_2\beta_1$, uporabi zgoraj lemo] **11.** $[\alpha=\tau_1\tau_2...\tau_m,\ \alpha^{-1}=\tau_m\tau_{m-1}...\tau_1]$ **12.** [id = (12)(12), $\alpha^{-1}\in A_n$] **13.**(a) [Ne.] (b) [(1234) je liha permutacija] **14.**(a) $[|A_2|=1,\ |A_3|=3,\ |A_4|=12]$; (b) $[|A_n|=n!/2,\ S_n=A_n\cup B_n,\ \phi:A_n\to B_n,$

$\phi(\alpha) = (12)\alpha$, ϕ bijekcija; $|A_n| = |B_n|$]. **15.** [$\alpha^{2n+1} = e$, $\alpha = \tau_1\tau_2...\tau_m$, ...] **16.** [uporabi matematično indukcijo po velikosti množice] **17.** [$\alpha = (a_1a_2...a_n) \Rightarrow |\alpha| = n$; $\alpha = (a_1a_2...a_m)$, $\beta = (b_1b_2...b_n)$, $|\alpha| = m$, $|\beta| = n$; $k := \mathrm{lcm}(m, n)$, $(\alpha\beta)^k = \alpha^k\beta^k = \mathrm{id}$, $|\alpha\beta|$ deli k; $|\alpha\beta| = t$, $(\alpha\beta)^t = id$, $\alpha^t = \beta^{-t}$, $\alpha^t = \mathrm{id} = \beta^{i-t}$, m deli t, n deli $t \Rightarrow k = t$ ...] **18.** [(a) 3 (b) 15 (c) 6 (d) 6 (e) 12 (f) 2] **19.** [(a) 7, $\mathrm{lcm}(6, 1) = 6$, $\mathrm{lcm}(5, 2) = 10$, $\mathrm{lcm}(5, 1, 1) = 5$, $\mathrm{lcm}(4, 3) = 12$, $\mathrm{lcm}(4, 2, 1) = 4$, $\mathrm{lcm}(4, 1, 1, 1) = 4$, $\mathrm{lcm}(3, 3, 1) = 3$, $\mathrm{lcm}(3, 2, 2) = 6$, $\mathrm{lcm}(3, 2, 1, 1) = 6$, $\mathrm{lcm}(3, 1, 1, 1, 1) = 3$, $\mathrm{lcm}(2, 2, 2, 1) = 2$, $\mathrm{lcm}(2, 2, 1, 1, 1) = 2$, $\mathrm{lcm}(2, 1, 1, 1, 1, 1) = 2$, $\mathrm{lcm}(1, 1, 1, 1, 1, 1, 1) = 1$; $\alpha \in \mathcal{S}_7 \Rightarrow |\alpha| \in \{1, 2, 3, 4, 5, 6, 7, 10, 12\}$.] [(b) $\mathrm{lcm}(a, b) = 3$, $1 \le a \le 7$, $1 \le b \le 7$, $a + b \le 7 \Rightarrow a = 1$, $b = 3$ ali $a = 3$, $b = 3$. $\#(a_1a_2a_3) = (7 \cdot 6 \cdot 5)/3 = 70$ (npr. $(a_1a_2a_3) = (a_3a_1a_2) = (a_2a_3a_1)$); $\#(a_1a_2a_3)(a_5a_6a_7) = ((7 \cdot 6 \cdot 5)/3) \cdot ((4 \cdot 3 \cdot 2)/3) \cdot 1/2 = 280$ (npr. $(a_1a_2a_3)(a_5a_6a_7) = (a_5a_6a_7)(a_1a_2a_3)$). $\#\alpha$ t.d. $|\alpha| = 3$ je 350]

Appendix.[91011]

sets	
literal	`{1,2,3};`
size	`#{1,2,3};`
add element	`s:={1,2,3};` `Inlude(~s,4);`
remove element	`s:={1,2,3};` `Exclude(~s,1);`
membership test	`7 in {6,7,8};`
disjoint test	`IsDisjoint({1,2,3},{2,3,4});`
union	`//{1,2,3,4}:` `s:={1,2,3} join {2,3,4};`
intersection	`//{2,3}:` `s:={1,2,3} meet {2,3,4};`
relative complement	`//{1}:` `s:={1,2,3} diff {2,3,4};`

arithmetic sequences	
unit difference	`[1..100];`
difference of 10	`[1..100 by 10];`
difference of 0.1	`[0.1*i: i in [1..1000]];`

permutations	
permutation from disjoint cycles	`S4:=Sym(4);` `p:=S4!(1,2)(3,4);`
permutation from list	`S4:=Sym(4);` `p2:=elt<S4|2,1,4,3>;`
compose	`S4:=Sym(4);` `S4!(1,2)(3,4) * S4!(1,3);`

invert	`S3:=Sym(3);`
	`S3!(1,2,3)^-1;`
	`Inverse(S3!(1,2,3));`

power	`S5:=Sym(5);` `S5!(1,2,3,4,5)^3;`
order	`S3:=Sym(3);` `Order(S3!(1,2,3));`

[9]Open: `http://magma.maths.usyd.edu.au/calc/`

[10]Vidi See also: `http://www.maths.usyd.edu.au/u/bobh/UoS/MATH2008/ctut05.pdf`

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