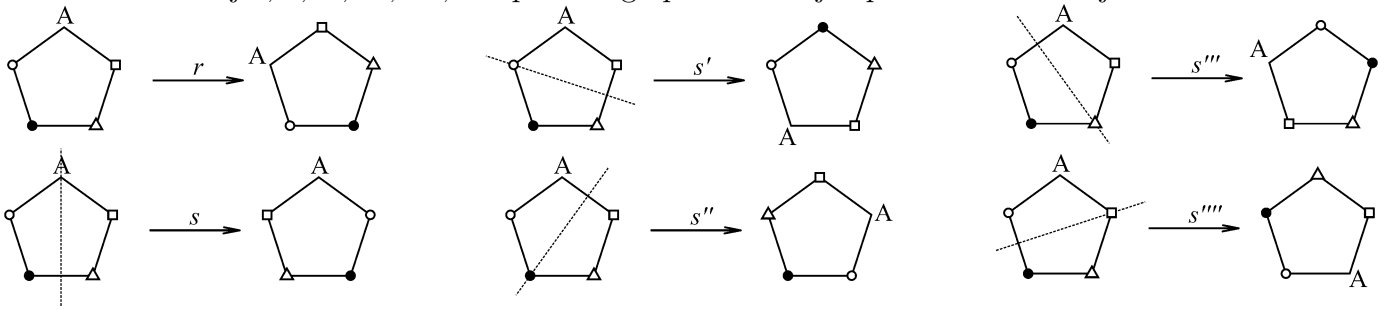
4 Podgrupe generirane z množico elementov in nekatere lastnosti cikličnih podgrup

1. Šest simetrij r, s, s', s'', s''', s'''' pravilnega petkotnika je opisanih z naslednjimi slikami.



Simetrije s', s'', s''', s'''', $s's''''$ in $s'''s''$ izrazi s simetrijami r in s.

Spomnimo se: Grupa G je ciklična, če obstaja $a \in G$ tako, da je vsak element grupe G enak neki potenci elementa a. Element a imenujemo generator grupe G.

Definicija ($\langle M \rangle$)
Naj bo G grupa in naj bo $M \subseteq G$, $M \neq \emptyset$. Podgrupa, generirana z M (oznaka $\langle M \rangle$) je najmanjša podgrupa grupe G, ki vsebuje M. Elemente množice M imenujemo generatorji grupe $\langle M \rangle$.

Podgrupo $\langle M \rangle$ lahko definiramo takole: Naj bo $M \subseteq G$ neka podmnožica v grupi G. Najmanjša podgrupa v G, ki vsebuje M, je

$$\langle M \rangle = \bigcap \{H \leq G : M \subset H\}$$

Množica M generira grupo G, če velja $\langle M \rangle = G$.

Opomba. Če je G ciklična grupa, potem obstaja M moči 1, ki generira G. Če je $M = \{a\}$ potem namesto $\langle \{a\} \rangle$ pišemo $\langle a \rangle$.
Če $M = \{a, b\}$ potem namesto $\langle \{a, b\} \rangle$ pišemo $\langle a, b \rangle$. Če je $M = \{a, b, ..., c\}$, potem namesto $\langle \{a, b, ..., c\} \rangle$ pišemo $\langle a, b, ..., c \rangle$.

2. Dana je grupa $D_5 = \{e, r = R_{72}, r^2, r^3, r^4, s, rs, r^2s, r^3s, r^4s\}$ (grupa vseh simetrij pravilnega petkotnika glede na operacijo kompozicije - ta grupa je znana pod imenom diederska grupa reda 10). Dana je tudi njena Cayley-eva tabela (tabela levo).
(a) Določi vse ciklične podgrupe grupe D_5.
(b) Določi $\langle r, s \rangle$, $\langle r^2, rs \rangle$, $\langle r, r^3 \rangle$, $\langle rs, r^3s \rangle$ in $\langle r^2s, r^4s \rangle$.
(c) Določi vse podgrupe grupe D_5.

	e	r	r^2	r^3	r^4	s	rs	r^2s	r^3s	r^4s
e	e	r	r^2	r^3	r^4	s	rs	r^2s	r^3s	r^4s
r	r	r^2	r^3	r^4	e	rs	r^2s	r^3s	r^4s	s
r^2	r^2	r^3	r^4	e	r	r^2s	r^3s	r^4s	s	rs
r^3	r^3	r^4	e	r	r^2	r^3s	r^4s	s	rs	r^2s
r^4	r^4	e	r	r^2	r^3	r^4s	s	rs	r^2s	r^3s
s	s	r^4s	r^3s	r^2s	rs	e	r^4	r^3	r^2	r
rs	rs	s	r^4s	r^3s	r^2s	r	e	r^4	r^3	r^2
r^2s	r^2s	rs	s	r^4s	r^3s	r^2	r	e	r^4	r^3
r^3s	r^3s	r^2s	rs	s	r^4s	r^3	r^2	r	e	r^4
r^4s	r^4s	r^3s	r^2s	rs	s	r^4	r^3	r^2	r	e

3. (a) Dana je grupa $(\mathbb{Z}_{20}, +)$. Določi $\langle 8, 14 \rangle$. Ali je $\langle 2 \rangle = \langle 8, 14 \rangle$?

(b) Dana je grupa $(\mathbb{Z}, +)$. Določi $\langle 8, 13 \rangle$.

(c) Dana je diederska grupa D_4. Določi $\langle H, V \rangle$ in $\langle R_{90}, V \rangle$.

4. (a) Dana je grupa $\mathbb{C}^*$, grupa vseh neničelnih kopleksnih števil glede na operacijo množenja. Določi $\langle 1, i \rangle$. Ali je $\langle 1, i \rangle = \langle i \rangle$?

(b) Dana je grupa $(\mathbb{C}, +)$. Določi $\langle 1, i \rangle$.

(c) Dana je grupa $(\mathbb{R}, +)$. Določi $\langle 2, \pi, \sqrt{2} \rangle$.

5. Dana je grupa v kateri a, b, c in d komutirajo. Določi $\langle a, b, c, d \rangle$.

6. Dana je diederska grupa D_n reda $2n$ (grupa vseh simetrij pravilnega n-kotnika glede na

operacijo kompozicije) in naj bo R rotacija za $\frac{360}{n}$ stopinj. Določi $\langle R \rangle$.

7. Določi grupo ki vsebuje elemente a in b take, da je $|a| = |b| = 2$, in da je

(a) $|ab| = 3$, (b) $|ab| = 4$, (c) $|ab| = 5$.

Ali lahko kaj povemo o relacijah med $|a|$, $|b|$ in $|ab|$?

8. Določi red grupe G, ki je generirana z dvema elementoma x in y, ki imata naslednjo lastnost: $x^3 = y^2 = (xy)^2 = 1$. Napiši vse mogoče podgrupe grupe G.

9. Dan je grupa $(\mathbb{Q}, +)$. Pokaži, da to grupo ni mogoče generirati s končno mnogo elementov.

10. (i) Pokaži, da je $H = \left\{ \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix} \mid n \in \mathbb{Z} \right\}$ ciklična podgrupa grupe $\mathrm{GL}_2(\mathbb{R})$.

(ii) S primerom pokaži, da produkt elementov končnega reda v neabelski grupi ni nujno končnega reda.

11. (a) Naj bo G ciklična grupa reda 6. Koliko elementov grupe G generira G?
(b) Naj bo G ciklična grupa reda n. Določi koliko elementov grupe G generira grupo G.

12. Naj bo G grupa in naj bo $a \in G$ končnega reda. Pokaži, da je $|a| = |\langle a \rangle|$.

13. Pokaži, da je vsaka podgrupa ciklične grupe ciklična.

14. Naj bo G ciklična grupa reda n.

(i) Pokaži, da red poljubne podgrupe grupe G deli n.

(ii) Naj bo r celo število, ki deli n. Pokaži, da G vsebuje natanko eno podgrupo reda r.

Izrek (fundamentalni izrek za ciklične grupe)
Vsaka podgrupa ciklične grupe je ciklična. Poleg tega, če je $|\langle a \rangle| = n$, potem je red katere koli podgrupe grupe $\langle a \rangle$ delitelj števila n; in za vsaki pozitivni deljitelj k števila n, ima grupa $\langle a \rangle$ natanko eno podgrupo reda k - in sicer $\langle a^{\frac{n}{k}} \rangle$.

Posledica. Za vsak pozitiven delitelj k števila n, je množica $\langle n/k \rangle$ podgrupa grupe $\mathbb{Z}_n$ reda k. Poleg tega, te podgrupe so edine podgrupe grupe $\mathbb{Z}_n$.

15. Dokaži fundamentalni izrek za ciklične grupe in njeno posledico zgoraj.

16. (i) Naj bo G ciklična grupa reda 30. Izpiši vse podgrupe grupe G.

(ii) Izpiši vse podgrupe grupe $\mathbb{Z}_{30}$.

17. Koliko podgrup ima grupa $\mathbb{Z}_{2000}$? Odgovor utemelji.

Definicija (Eulerjeva funkcija fi)
Naj bo $\phi(1) = 1$, in za vsako celo število $n > 1$, označimo z $\phi(n)$ število pozitivnih celih števil, ki so manjša od n, in so tuja z n. Tako definirano funkcijo $\phi(n)$ imenujemo Eulerjeva funkcija fi. Opazimo, da iz definicije grupe $U(n)$ sledi, da $|U(n)| = \phi(n)$. Prvih 12 vrednosti funkcije $\phi(n)$ je danih v naslednji tabeli.

n	1	2	3	4	5	6	7	8	9	10	11	12
$\phi(n)$	1	1	2	2	4	2	6	4	6	4	10	4

Izrek (število elementov reda d v ciklični grupi)
Če je d pozitivno celo število ki deli n, potem je število elementov reda d v ciklični grupi reda n eneko $\phi(d)$.

18. Dokaži izrek zgoraj.

19. (a) Dokaži, da ima abelska grupa z dvema elementoma reda 2 vedno podgrupo reda 4.
(b) Najdi primer neciklične grupe, v kateri so vse prave podgrupe ciklične.
(c) Naj bo G grupa in naj bo $a \in G$. Dokaži, da je $\langle a^{-1} \rangle = \langle a \rangle$.
(d) Dokaži, da mora biti grupa reda 3 ciklična.

POMEMBNI REZULTATI (Ciklične grupe.)

9. **(Fundamentalni izrek za ciklične grupe.)** Vsaka podgrupa ciklične grupe je ciklična. Poleg tega, če je $|\langle a\rangle| = n$, potem je red katerekoli podgrupe grupe $\langle a\rangle$ delitelj števila n. Za vsak pozitiven deljitelj k števila n, ima grupa $\langle a\rangle$ natanko eno podgrupo reda k - namreč $\langle a^{\frac{n}{k}}\rangle$.
10. Za vsak pozitiven delitelj k števila n, je množica $\langle n/k\rangle$ podgrupa grupe $\mathbb{Z}_n$ reda k. Poleg tega, te podgrupe so edine podgrupe grupe $\mathbb{Z}_n$.
11. Vsaka podgrupa ciklične grupe je ciklična.
12. Vsaka neskončna ciklična grupa ima natanko dva generatorja.
13. Vsaka prava podgrupa neskončne ciklične grupe je neskončna.
14. Če je d pozitivno celo število ki deli n, potem je število elementov reda d v ciklični grupi reda n eneko $\phi(d)$ ($\phi(n) = |U(n)|$ je Eulerjeva funkcija fi).

Augustin Louis Cauchy

> You see that little young man? Well!
> He will supplant all of us in so far as we are mathematicians.
>
> *Spoken by Lagrange to Laplace about the 11-year-old Cauchy*

Augustin Louis Cauchy was born on August 21, 1789, in Paris. By the time he was 11, both Laplace and Lagrange had recognized Cauchy's extraordinary talent for mathematics. In school he won prizes for Greek, Latin, and the humanities. At the age of 21, he was given a commission in Napoleon's army as a civil engineer. For the next few years, Cauchy attended to his engineering duties while carrying out brilliant mathematical research on the side.

In 1815, at the age of 26, Cauchy was made Professor of Mathematics at the École Polytechnique and was recognized as the leading mathematician in France. Cauchy and his contemporary Gauss were among the last mathematicians to know the whole of mathematics as known at their time, and both made important contributions to nearly every branch, both pure and applied, as well as to physics and astronomy.

Cauchy introduced a new level of rigor into mathematical analysis. We owe our contemporary notions of limit and continuity to him. He gave the first proof of the Fundamental Theorem of Calculus. Cauchy was the founder of complex function theory and a pioneer in the theory of permutation groups and determinants. His total written output of mathematics fills 24 large volumes. He wrote more than 500 research papers after the age of 50. Cauchy died at the age of 67 on May 23, 1857.

Rešitve: **1.** [$s' = sr^3 = r^2s$, $s'' = sr = r^4s$, $s''' = sr^4 = rs$, $s'''' = sr^2 = r^3s$, $s's'''' = r^4$, $s'''s'' = r^2$] **2.** [$\langle e\rangle = \{e\}$, $\langle r\rangle = \{e, r, r^2, r^3, r^4\}$, $\langle s\rangle = \{e, s\}$, $\langle rs\rangle = \{e, rs\}$, $\langle r^2s\rangle = \{e, r^2s\}$, $\langle r^3s\rangle = \{e, r^3s\}$, $\langle r^4s\rangle = \{e, r^4s\}$] **3.**(a) [$\langle 8, 14\rangle = \{0, 2, 4, ..., 18\} = \langle 2\rangle$]; (b) [$\langle 8, 13\rangle = \mathbb{Z}$]; (c) [$\langle H, V\rangle = \{R_0, R_{180}, H, V\}$, $\langle R_{90}, V\rangle = D_4$]. **4.** (a) [$\langle 1, i\rangle = \{1, i, -i, -i\} = \langle i\rangle$]; (b) [$\langle 1, i\rangle = \{a + ib \mid a, b \in \mathbb{Z}\}$]; (c) [$\langle 2, \pi, \sqrt{2}\rangle = \{2a + \pi b + c\sqrt{2} \mid a, b, c \in \mathbb{Z}\}$]. **5.** [$\langle a, b, c, d\rangle = \{a^q b^r c^s d^t \mid q, r, s, t \in \mathbb{Z}\}$] **6.** [$\langle R\rangle = \{e, R, R^2, ..., R^{n-1}\}$] **7.**(a) [$D_3$]; (b) [$D_4$]; (c) [$D_5$]. **8.** [$(xy)^2 = 1$, $xyxy = 1$, $xyx = y$, $yxyx = y^2 = 1$, $(yx)^2 = 1$] [$|G| = 6$, $G = \{1, x, x^2, y, xy, yx\}$, $xy = (xy)^{-1} \Rightarrow xy = yx^2$, $yx = x^2y$] **9.** [$\mathbb{Q} = \langle \frac{a_1}{b_1}, \frac{a_2}{b_2}, ..., \frac{a_n}{b_n}, \rangle$, $\exists c_1, c_2, ..., c_n$ t.d. $c_1\frac{a_1}{b_1} + c_2\frac{a_2}{b_2} + ... + c_n\frac{a_n}{b_n} = \frac{1}{2b_1b_2...b_n}$, $c_1\frac{a_1}{b_1} + c_2\frac{a_2}{b_2} + ... + c_n\frac{a_n}{b_n} = \frac{A_1+A_2+...+A_n}{b_1b_2...b_n}$, $\frac{A}{b_1b_2...b_n} = \frac{1}{2b_1b_2...b_n}$, $A = \frac{1}{2}$] **10.** (i) [$\begin{bmatrix}1 & n\\ 0 & 1\end{bmatrix} \cdot \begin{bmatrix}1 & m\\ 0 & 1\end{bmatrix} = \begin{bmatrix}1 & n+m\\ 0 & 1\end{bmatrix}$, $\langle \begin{bmatrix}1 & 1\\ 0 & 1\end{bmatrix}\rangle = H$] (ii) [$G = \mathrm{GL}_2(\mathbb{R})$, $A = \begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}$, $B = \begin{bmatrix}1 & 1\\ 0 & -1\end{bmatrix}$, $|A| = 2$, $|B| = 2$, $|AB| = \infty$] **11.** (a) [$\{1, g, g^2, g^3, g^4, g^5\} = G = \langle g\rangle = \langle g^5\rangle$] (b) [$1^\circ$ $\gcd(i, n) = 1$, $1 = ip + nt$, $g = g^{ip}$, $g \in \langle g^i\rangle$, 2° $\gcd(i, n) = d > 1$, $i = sd$, $n = pd$, $(g^i)^p = 1$, $|g^i| \leq p < n$] **12.** [$\forall k \in \mathbb{Z}$, $a^k \in \{e, a, a^2, ..., a^{n-1}\}$, vsi elementi iz $\{e, a, a^2, ..., a^{n-1}\}$ so različni, $\langle a\rangle = \{e, a, a^2, ..., a^{n-1}\}$] **13.** [$1^\circ$ $H = \{e\}$; 2° $H \neq \{e\}$; naj bo H podgrupa, $\exists t > 0$ $a^t \in H$, naj bo m najmanjši celi t.d. $a^m \in H$, (i)

$\langle a^m\rangle \subseteq H$, (ii) $b \in G$, $b = a^k$, $k = mq + r$, $0 \le r < m$... $\langle a^m\rangle = H$] **14.** (i) [$|G| = n$, $H = \langle a^m\rangle$, $n = mk + r$, $r = 0$, $n = mk$, $|H| = k$] (ii) [$G = \{1, g, g^2, ..., g^{n-1}\}$, $n = rp$, $H = \{g^p, g^{2p}, ..., g^{(r-1)p}, g^{rp} = g^n = 1\}$, $H' = \langle g^k\rangle$, $k = ps$, $H' \subseteq H$] **15.** — **16.** (i) [Če k deli 30 potem podgrupa reda k je $\langle a^{30/k}\rangle$. $\langle a^{30}\rangle = \{e\}$, $|\langle a^{30}\rangle| = 1$, $\langle a^{15}\rangle = \{e, a^{15}\}$, $|\langle a^{15}\rangle| = 2$, $\langle a^{10}\rangle = \{e, a^{10}, a^{20}\}$, $|\langle a^{15}\rangle| = 3$, $\langle a^6\rangle = \{e, a^6, a^{12}, a^{18}, a^{24}\}$, $|\langle a^6\rangle| = 5$, $\langle a^5\rangle = \{e, a^5, a^{10}, a^{15}, a^{20}, a^{25}\}$, $|\langle a^5\rangle| = 6$, $\langle a^3\rangle = \{e, a^3, a^6, ..., a^{27}\}$, $|\langle a^3\rangle| = 10$, $\langle a^2\rangle = \{e, a^2, a^4, ..., a^{28}\}$, $|\langle a^2\rangle| = 15$, $\langle a\rangle = \{e, a, a^2, ..., a^{29}\}$, $|\langle a\rangle| = 30$.] (ii) [$\langle 1\rangle$, $\langle 2\rangle$, $\langle 3\rangle$, $\langle 5\rangle$, $\langle 6\rangle$, $\langle 10\rangle$, $\langle 15\rangle$, $\langle 30\rangle$] **17.** Število $2000 = 2^4 \cdot 5^3$ ima 20 deliteljev. Za vsak delitelj d števila 2000 je $\langle 2000/d\rangle$ podgrupa moči d. Imamo 20 podgrup različnih moči... **18.** Obstaja točno ena podgrupa reda d, recimo $\langle a\rangle$. Vsak element reda d generira $\langle a\rangle$. Element a^k generira $\langle a\rangle$ če in samo če $\gcd(k, d) = 1$. **19.** (a) [$|a| = |b| = 2$, $G = \{e, a, b, ab\}$, $a \ne e$, $b \ne e$, $a \ne ab$, $b \ne ab$, $ab \ne e$]; (b) [$U(8) = \{1, 3, 5, 7\}$, $\langle 3\rangle$, $\langle 5\rangle$, $\langle 7\rangle$]; (c) [$\subseteq$: $x \in \langle a^{-1}\rangle$, $x = (a^n)^{-1}$, $x \in \langle a\rangle$; $\supseteq$: $x \in \langle a\rangle$, $x = ((a^{-1})^n)^{-1}$, $x \in \langle a^{-1}\rangle$].

Dodatek.[6][7][8]

strings

string literal	`"don't say \"no\""`
newline in literal	A line break in a string literal results in a newline in the string unless preceded by a backslash.
literal escapes	`\" \\ \n \r \t`

concatenate	`"one " cat "two " cat "three";`
	`"one " * "two " * "three";`
	`&cat ["one ", "two ", "three "];`
	`&* ["one ", "two ", "three "];`

replicate	`hbar := "-" ^ 80;`
number to string	`"value: " * IntegerToString(8);`
split	`Split("foo,bar,baz", ",");`
length	`# "hello";`

index of substring	`Index("hello", "el");`
	`Position("hello", "el");`
	`/* both return 0 if substring not found */`

extract substring	`Substring("hello", 2, 2);`

arrays

literal	`a := [1, 2, 3];`
size	`# [1, 2, 3];`
lookup	`// indices start at one:` `[6, 7, 8][1];`
update	`a[1] := 7;`
out-of-bounds behavior	Runtime error on lookup. For update, size of array is increased if necessary; runtime error to look up unassigned slot in between assigned slots.

manipulate back	`a := [6, 7, 8];`
	`// a not modified:`
	`a2 := Append(a, 9);`
	`// a2 not modified:`
	`a3 := Prune(a2);`
	`// a modified:`
	`Append(~a, 9);`
	`Prune(~a);`

[6] Odpri: `http://magma.maths.usyd.edu.au/calc/`

[7] Vidi tudi: `http://www.maths.usyd.edu.au/u/bobh/UoS/MATH2008/ctut04.pdf`

[8] ali `http://hyperpolyglot.org/more-computer-algebra`