2 Nekatere družine grup in podgrupe

1. Recimo, da smo odstranili področje kvadratne oblike iz ravnine, ga premaknili na nek način, nato pa kvadrat vrnili nazaj na mesto, ki ga je prvotno zasedal. Opišite vse možne načine, na katere se to lahko stori. Natančneje, želimo opisati možne odnose med štartnim položajem kvadrata in njegovo končno pozicijo v smislu gibanja (zanima nas samo končni učinek gibanja, ne pa gibanje samo. Recimo, vrtenje za 90° in vrtenje za 450° smatramo kot enaka, saj je končni učinek enak).

Definicija (simetrija geometrijskega lika)
Simetrija geometrijskega lika je preureditev oglišč in stranic lika na tak način, da se ohranjajo vsa oglišča in stranice lika, njihovi medsebojni odnos, ter razdalje in koti.

2. Dana je množica
$D_4 = \{R_0, R_{90}, R_{180}, R_{270}, H, V, D, D'\}$
kje osem elementov množice predstavlja osem simetrij kvadrata, ki smo jih ugotovili v predhodni nalogi. Dana je tudi Cayley-eva tabela D_4 glede na operacijo kompozicije.

	R_0	R_{90}	R_{180}	R_{270}	H	V	D	D'
R_0	R_0	R_{90}	R_{180}	R_{270}	H	V	D	D'
R_{90}	R_{90}	R_{180}	R_{270}	R_0	D'	D	H	V
R_{180}	R_{180}	R_{270}	R_0	R_{90}	V	H	D'	D
R_{270}	R_{270}	R_0	R_{90}	R_{180}	D	D'	V	H
H	H	D	V	D'	R_0	R_{180}	R_{90}	R_{270}
V	V	D'	H	D	R_{180}	R_0	R_{270}	R_{90}
D	D	V	D'	H	R_{270}	R_{90}	R_0	R_{180}
D'	D'	H	D	V	R_{90}	R_{270}	R_{180}	R_0

(i) Ali je množica D_4 zaprta glede na operacijo kompozicije?
(ii) Ali obstaja enota?
(iii) Ali ima vsak element inverz?
(iv) Ali se vsak element iz D_4 pojavi natanko enkrat v tabeli v vsaki vrstici in vsakem stolpcu?
(v) Ali je množica D_4 grupa glede na operacijo kompozicije? Ali je grupa abelska?

Pripomba. Osem simetrij kvadrata R_0, R_{90}, R_{180}, R_{270}, H, V, D in D' skupaj z operacijo kompozicije, tvorita grupo, ki jo imenujemo diederska grupa reda 8 (red grupe je število elementov grupe). Ta grupa bo označena z D_4.

Multiplikativna grupa		Aditiva groupa	
$a \cdot b$ ali ab	množenje	$a + b$	seštevanje
e ali 1	enota	0	enota
a^{-1}	inverz od a	$-a$	inverz od a
a^n	potenca od a	na	večkratnik od a
ab^{-1}	kvocijent	$a - b$	razlika

Če je dana multiplikativna grupa G in če je $g \in G$ potem: bomo $g \cdot g$ označevali z g^2, ggg z g^3, ..., $\underbrace{gg...g}_{\text{n dejavniki}}$ z g^n. Tabela levo prikazuje razliko med aditivno in multiplikativno grupo.

Dogovorimo se, da za $a \in G$ namesto $\underbrace{a^{-1} \cdot a^{-1} \cdot ... \cdot a^{-1}}_{n}$ pišemo a^{-n} (kje je a^{-1} inverz elementa a).

Definicija (red grupe, red elementa)
Kardinalnost ali red grupe G je enaka kardinalnosti pripadajoče množice G. Če je torej G končna množica, gre za število elementov v grupi G. Grupa, ki vsebuje neskončno elementov, je neskončnega reda. Red grupe G označimo z $|G|$.

Naj bo G grupa in $g \in G$. Red elementa g je najmanjše pozitivno naravno število n, da je $g^n = e$. Red elementa g označimo z $|g|$ (oziroma $o(g)$). Če tako število n ne obstaja, pravimo, da je g neskončnega reda. Nevtralni element je edini element reda 1.

3. Dana je grupa D_4 (diederska grupa simetrij kvadrata - glej prejšnja dva problema). Določi red grupe, ter določi red elementov R_0, R_{90} in H.

4. Naj bo G grupa, in naj bo $g \in G$ konačnega reda. Pokaži, da obstaja pozitivno število k tako da velja $g^{-1} = g^k$ (kje je g^{-1} inverz elementa g).

Izrek o ostanku. Za dano celo število $m \in \mathbb{Z}$ in za pozitivno celo število $n \in \mathbb{Z}^+$ obstajata enolično določena $q \in \mathbb{Z}$ (količnik) in $r \in \mathbb{Z}^+$ (ostanek) tako da velja: $m = nq + r$, in $r \in \{0, 1, ..., n-1\}$.

Operacija modulo

Operacija modulo (mod) vrne ostanek pri celoštevilčnem deljenju (poišče ostanek deljenja ene številke z drugo). Če je $m = nq + r$, $r \in \{0, 1, ..., n-1\}$ ($m \in \mathbb{Z}$, $n \in \mathbb{Z}^+$) potem je

$$m \bmod n = r.$$

Definicija (seštevanje modulo n, množenje modulo n)

Naj bo $\mathbb{Z}_n = \{0, 1, 2, ..., n-1\}$ (kje je $n \geq 1$ fiksno celo število). Na množici $\mathbb{Z}_n$ definiramo operacijo seštevanje modulo n, $+_n$ na naslednji način:

$$+_n : \mathbb{Z}_n \times \mathbb{Z}_n \longrightarrow \mathbb{Z}_n$$
$$(a, b) \longrightarrow a + b \,(\mathrm{mod}\, n)$$

kje število $a+b \,(\mathrm{mod}\, n)$ pomeni ostanek, ki ga dobimo, ko vsoto $a+b$ delimo s n. Pogosto namesto $+_n$ pišemo $+$.

Podobno, na množici $S \subseteq \mathbb{Z}_n$ definiramo operacijo množenje modulo n, $\cdot_n$ na naslednji način:

$$\cdot_n : S \times S \longrightarrow \mathbb{Z}_n$$
$$(a, b) \longrightarrow ab \,(\mathrm{mod}\, n)$$

kje število $ab \,(\mathrm{mod}\, n)$ pomeni ostanek, ki ga dobimo, ko produkt ab delimo s n. Pogosto namesto $\cdot_n$ pišemo $\cdot$.

5. Definirajmo množico $U(10)$ kot množico vseh pozitivnih celih števil manjših od 10, ki so tuji z 10. Z drugimi besedami, $U(10) = \{k \in \mathbb{N} \mid k < 10, \gcd(k, 10) = 1\}$. Zapiši Cayley-evo tabelo za $U(10)$ glede na operacijo množenja modulo 10.

6. Množica $U(15) = \{k \in \mathbb{N} \mid k < 15, \gcd(k, 15) = 1\}$ tvori grupo glede na operacijo množenja modulo 15. Določi red grupe, ter določi red elementov 1, 2, 7 in 11.

7. Napiši Cayley-evo tabelo za množico $\mathbb{Z}_5$ glede na operacijo seštevanja in množenja modulo 5.

8. Dana je grupa $\mathbb{Z}_{10}$ z operacijo seštevanja modulo 10. Določi red grupe, ter določi red elementov 0, 2, 5 in 7.

Definicija (podgrupa)

Naj bo $(G, *)$ grupa. Potem je podmnožica $H \subseteq G$ glede na operacijo $*$ podgrupa grupe G, če je $(H, *)$ grupa. S simboli zapisano: $H \leq G$.

9. Naj bo G abelska grupa glede na operacijo množenja, in naj bo e identiteta. Pokaži, da je $H = \{x^2 \mid x \in G\}$ podgrupa grupe G (podmnožica H je množica vseh "kvadratov" elementov grupe G).

10. Naj bo G abelska grupa glede na operacijo množenja, in naj bo e identiteta. Pokaži, da je $H = \{x \in G \mid x^2 = e\}$ podgrupa grupe G.

11. Naj bo G abelska grupa, in naj bo H podmnožica tistih elementov grupe G, ki so končnega reda. Dokaži, da je H podgrupa grupe G.

12. Dana sta dva elementa R_{90} in V grupe D_4. Naj bo H najmanjša podgrupa, ki vsebuje R_{90} in naj bo K najmanjša podgrupa, ki vsebuje R_{90} in V. Poišči druge elemente podgrupe H in podgrupe K.

13. Določi vse podgrupe grupe D_4.

14. Določi vse podgrupe grupe $\mathbb{Z}_4$.

15. Določi vse podgrupe grupe $\mathbb{Z}_7$.

16. Določi vse podgrupe grupe $\mathbb{Z}_{12}$.

17. Naj bo H končna neprazna podmnožica grupe G. Pokaži, da je H podgrupa grupe G če in samo če $xy \in H$ za poljubna $x, y \in H$.

18. Naj bo G grupa, in naj bo H neprazna podmnožica možice G. Pokaži, da če je $ab^{-1} \in H$ za poljubna $a, b \in H$, potem je H podgrupa grupe G.

19. Naj bo G grupa, in naj bo H neprazna podmnožica grupe G. Pokazati, da če je ab v H kadarkoli sta a in b v H (torej, če je H zaprta glede na operacijo množenja), in če je a^{-1} v H za poljuben $a \in H$ (torej, če je H zaprta za inverze), potem je H podgrupa grupe G.

Lema Naj bo G grupa, in naj bo H neprazna podmnožica grupe G. H je podgrupa grupe G če je (i) $H \neq \emptyset$ in (ii) $\forall a, b \in H$ $ab^{-1} \in H$.

Lema Naj bo G grupa, in naj bo H neprazna podmnožica grupe G. H je podgrupa grupe G če je (i) $H \neq \emptyset$, (ii) H zaprta glede na operacijo množenja in (iii) $\forall a \in H$ imamo $a^{-1} \in H$ (da vsak a iz H ima inverz v H).

Arthur Cayley. Arthur Cayley was born on August 16, 1821, in England. His genius showed itself at an early age. He published his first research paper while an undergraduate of 20, and in the next year he published eight papers. While still in his early 20s, he originated the concept of n-dimensional geometry.

After graduating from Trinity College, Cambridge, Cayley stayed on for three years as a tutor. At the age of 25, he began a 14-year career as a lawyer. During this period, he published approximately 200 mathematical papers, many of which are now classics.

In 1863, Cayley accepted the newly established Sadlerian professorship of mathematics at Cambridge University. He spent the rest of his life in that position. One of his notable accomplishments was his role in the successful effort to have women admitted to Cambridge.

Among Cayley's many innovations in mathematics were the notions of an abstract group and a group algebra, and the matrix concept. He made major contributions to geometry and linear algebra. Cayley and his lifelong friend and collaborator J. J. Sylvester were the founders of the theory of invariants, which was later to play an important role in the theory of relativity.

Cayley's collected works comprise 13 volumes, each about 600 pages in length. He died on January 26, 1895.

To find more information about Cayley, visit: `http://www-groups.dcs.st-and.ac.uk/~history/`

POMEMBNI REZULTATI (Podgrupe.)

1. Če je H podgrupa grupe G potem
   (i) Je identiteta podgrupe H in grupe G ista.
   (ii) Je inverz elementa v podgrupi H glede na grupo H in G isti.
   (iii) Je red elementa v podgrupi H glede na grupo H in G isti.
2. Naj bo G grupa z binarno operacijo množenja. Podmnožica H grupe G je podgrupa grupe G če velja eden od naslednji ekvivalentnih pogojov:
   (a) $ab \in H$, $a^{-1} \in H \ \ \forall a, b \in H$
   (b) $ab^{-1} \in H \ \ \forall a, b \in H$
   Če je H končna je H podgrupa grupe G, če je $ab \in H \ \ \forall a, b \in H$.
3. Presek dveh podgrup grupe je tudi podgrupa grupe.

Rešitve: **1.** [R_0 = rotacija od 0° (brez sprememb v položaju), R_{90}, R_{180}, ..., D, D', $\square CZPB \xrightarrow{R_{90}} \square BCZP$, $\square CZPB \xrightarrow{R_{180}} \square PBCZ$, $\square CZPB \xrightarrow{H} \square ZCBP$] **2.**(i) [je zaprta]; (ii) [$e = R_0$] (iii) [imajo] (iv) [da] (v) [je grupa, ni abelska]. **3.** [$|D_4| = 8$, $|R_0| = 1$, $|R_{90}| = 4$, $|H| = 2$] **4.** [$g^n = e$, $gg^{n-1} = g^{n-1}g = e$] **5.** [$3 \cdot 7 = 1$, $3 \cdot 9 = 7$, $7 \cdot 1 = 7$, $7 \cdot 3 = 1$, $7 \cdot 7 = 9$, $7 \cdot 9 = 3$, $9 \cdot 1 = 9$, $9 \cdot 3 = 7$, $9 \cdot 7 = 3$, $9 \cdot 9 = 1$] **6.** [$|U(15)| = 8$, $|1| = 1$, $|2| = 4$, $|7| = 4$, $|11| = 2$] **7.** [$3 \cdot 2 = 1$, $3 \cdot 3 = 4$, $3 \cdot 4 = 2$] **8.** [$|\mathbb{Z}_{10}| = 10$, $|0| = 1$, $|2| = 5$, $|5| = 2$, $|7| = 10$] **9.** [$x^2y^2 = (xy)^2$, $e^2 = e$, $x^{-1} \in G \Rightarrow (x^{-1})^2 \in H$] **10.** [$(xy)^2 = x^2y^2 = e$, $e^2 = e$, $x \cdot x = e$] **11.** [$x, y \in H$, $|x| = n$, $|y| = m$ $(n, m \in \mathbb{Z})$, $(xy)^{nm} = x^{nm}y^{nm}$, $x^{nm} = (x^n)^m = e^m$; $x^n = e$, $e = x^{-n} = (x^{-1})^n$] **12.** [$H = \{R_0, R_{90}, R_{180}, R_{270}\}$] **13.** [$\{R_0\}$, $\{R_0, R_{90}, R_{180}, R_{270}\}$, $\{R_0, R_{180}\}$, $\{R_0, H\}$, $\{R_0, V\}$, $\{R_0, D\}$, $\{R_0, D'\}$, $\{R_0, R_{180}, H, V\}$, $\{R_0, R_{180}, D, D'\}$, D_4] **14.** [$\{0\}$, $\{0, 2\}$, $\{0, 1, 2, 3\}$] **15.** [$\{0\}$, $\mathbb{Z}_7$] **16.** [$\{0\}$, $\{0, 2, 4, 6, 8, 10\}$, $\{0, 3, 6, 9\}$, $\{0, 4, 8\}$, $\{0, 6\}$, $\mathbb{Z}_{12}$] **17.** [$x \in H$, $S = \{x, x^2, x^3, ..., x^n, ...\}$, $S \subset H$, $\exists i \neq j$ t.d. $x^i = x^j$, $e = x^{j-i} \Rightarrow e \in H$, $x \cdot x^{n-1} = e$, $x^{-1} = x^{n-1}$] **18.** [$e = xx^{-1} = ab^{-1} \in H$, $ex^{-1} = ab^{-1}$, $xy = x(y^{-1})^{-1} = ab^{-1} \in H$] **19.** [$a, b \in H$, $b^{-1} \in H$, $ab^{-1} \in H$]

Dodatek.[2]

Rešimo nalogo 5., 6. in 12. z uporabo programskega jezika MAGMA.

Odprti: `http://magma.maths.usyd.edu.au/calc/`

5.

```
U10 := { Integers() | a : a in [1..9]
| GCD(a, 10) eq 1 };

printf "U(10)= ";
U10;

" ";
"Cayley table for U(10) is: ";

printf " * | ";
for i in U10 do
   printf " %o  ", i;
end for;
" ";

printf "----";
for i in U10 do
   printf "-%o", "---";
end for;
" ";

for j in U10 do
    printf " %o |  ", j;
    for i in U10 do
       printf "%o   ", i*j mod 10;
    end for;
    " ";
end for;
```

Izhod:

```
U(10)= { 1, 3, 7, 9 }

Cayley table for U(10) is:
 * |  1   3   7   9
--------------------
 1 |  1   3   7   9
 3 |  3   9   1   7
 7 |  7   1   9   3
 9 |  9   7   3   1
```

6.

```
 U15 := { Integers() | a : a in [1..14]
| GCD(a, 15) eq 1 };

U15;

for i in [1..#U15] do
   printf "Za vrednost od i= %o ", i; " ";
   printf "2^i mod 15 = %o ", 2^i mod 15; " ";
   printf "7^i mod 15 = %o ", 7^i mod 15; " ";
   printf "11^i mod 15 = %o ", 11^i mod 15; " ";
   "---------";
end for
```

12.(a)

```
G := Sym(4);

r90 := G ! (1,2,3,4);

D4 := sub< G | r90 >;

for x in D4 do
   x;
end for;
```

Izhod:

```
Id(D4)
(1, 2, 3, 4)
(1, 4, 3, 2)
(1, 3)(2, 4)
```

12.(b)

```
G := Sym(4);

r90 := G ! (1,2,3,4);
v := G ! (1,4)(2,3);

D4 := sub< G | r90, v >;

for x in D4 do
   x;
end for;
```

Izhod:

```
Id(D4)
(1, 2, 3, 4)
(1, 4, 3, 2)
(1, 3)(2, 4)
(2, 4)
(1, 2)(3, 4)
(1, 4)(2, 3)
(1, 3)
```

[2]Vidi tudi: `http://www.maths.usyd.edu.au/u/bobh/UoS/MATH2008/ctut02.pdf`