

2 Nekatero 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 (zanimajo 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).

[R_0 = rotacija od 0° (brez sprememb v položaju), R_{90} , R_{180} , ..., D , D']

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.

(i) Ali je množica D_4 zaprta glede na operacijo kompozicije? [je

zaprta]

(ii) Ali obstaja enota? [$e = R_0$]

(iii) Ali ima vsak element inverz? [imajo]

(iv) Ali se vsak element iz D_4 pojavi natanko enkrat v tabeli v vsaki vrstici in vsakem stolpcu? [da]

(v) Ali je množica D_4 grupa glede na operacijo kompozicije? Ali je grupa abelska? [je grupa, ni abelska]

	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

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		Aditivna grupa	
$a \cdot b$ 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 , $g \cdot g \cdot g$ z g^3 , ..., $\underbrace{gg \dots g}_n$ z g^n . Tabela levo prikazuje razliko med aditivno in multiplikativno grupo.

Dogovorimo se, da za $a \in G$ namesto $\underbrace{a^{-1} \cdot a^{-1} \cdot \dots \cdot a^{-1}}_n$ 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 . [$|D_4| = 8, |R_0| = 1, |R_{90}| = 4, |H| = 2$]

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). [$g^n = e, gg^{n-1} = g^{n-1}g = e$]

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 $r \in \{0, 1, \dots, n-1\}$.

Operacija modulo

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

$$m \bmod n = r.$$

Definicija (seštevanje modulo n , množenje modulo n)

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

$$+_n : \mathbb{Z}_n \times \mathbb{Z}_n \longrightarrow \mathbb{Z}_n$$

$$(a, b) \longrightarrow a + b \pmod{n}$$

kje število $a + b \pmod{n}$ 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:

$$\cdot_n : S \times S \longrightarrow \mathbb{Z}_n$$

$$(a, b) \longrightarrow ab \pmod{n}$$

kje število $ab \pmod{n}$ 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. $[3 \cdot 7 = 1, 3 \cdot 9 = 7]$

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. $[|U(15)| = 8, |7| = 4]$

7. Napiši Cayley-evo tabelo za množico \mathbb{Z}_5 glede na operacijo seštevanja in množenja modulo 5. $[3 \cdot 2 = 1, 3 \cdot 3 = 4, 3 \cdot 4 = 2]$

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

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). $[x^2 y^2 = (xy)^2]$

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 . $[(xy)^2 = x^2 y^2 = e, e^2 = e]$

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 . $[(xy)^{nm} = x^{nm} y^{nm}, x^{nm} = (x^n)^m = e^m]$

12. Naj bo R_{90} element iz grupe D_4 , in naj bo H najmanjša podgrupa, ki vsebuje R_{90} . Poišči druge elemente podgrupe H . $[H = \{R_0, R_{90}, R_{180}, R_{270}\}]$

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 in samo če $xy \in H$ za poljubna $x, y \in H$.

Grupa	Operacija	Identiteta	Oblika elementa	Inverz	Abelska	Nekatere družine
\mathbb{Z}	seštevanje	0	k	$-k$	da	grup je mogoče
\mathbb{Q}^+	množenje	1	$m/n, m, n > 0$	n/m	da	povzeti v tabeli levo.
\mathbb{Z}_n	seštevanje modulo n	0	k	$n - k$	da	Tukaj je $\mathbb{R}^* = \mathbb{R}/\{0\}$;
\mathbb{R}^*	množenje	1	x	$1/x$	da	$\mathbb{C}^* = \mathbb{C}/\{0\}$;
\mathbb{C}^*	množenje	1	$a + ib$	$\frac{a}{a^2+b^2} - \frac{bi}{a^2+b^2}$	da	$U(n) = \{k \in \mathbb{N} \mid k <$
$GL_2(\mathbb{R})$	množenje matrik	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$	$\begin{pmatrix} \frac{d}{ad-bc} & \frac{-b}{ad-bc} \\ \frac{-c}{ad-bc} & \frac{a}{ad-bc} \end{pmatrix}$	ne	$n, \gcd(k, n) = 1\}$;
$U(n)$	množenje modulo n	1	$k, \gcd(k, n) = 1$	rešitev $kx \bmod n = 1$	da	$SL_2(\mathbb{R}) = \{X \in$
\mathbb{R}^n	seštevanje po komponentah	$(0, 0, \dots, 0)^\top$	$(a_1, a_2, \dots, a_n)^\top$	$(-a_1, -a_2, \dots, -a_n)^\top$	da	$Mat_{2 \times 2}(\mathbb{R})$
$SL_2(\mathbb{R})$	množenje matrik	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} a & b \\ c & d \end{pmatrix}, ad - bc = 1$	$\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$	ne	:
D_n	kompozicija	R_0	R_α, L	$R_{360-\alpha}, L$	ne	$det(X) = 1\}$