1 Grupa

Definicija (binarna operacija)

Binarna operacija na množici S je vsaka preslikava, ki slika iz kartezičnega produkta $S \times S$ nazaj v množico S. Običajno jo označimo z oznako $*$, to je $* : S \times S \to S$. Dogovorimo se, da za $a, b, c \in S$ namesto $c = *(a, b)$ pišemo $c = a * b = ab$.

Definicija (zaprtost za operacijo $*$)

Naj bo $*$ binarna operacija na S i naj bo $H \subseteq S$ neprazna podmnožica. Če je $a*b \in H$ za poljubna $a, b \in H$, potem rečemo, da je $*$ notranja operacija za H, oziroma, da je H zaprta podmnožica za operacijo $*$.

1. Pokaži, da je podmnožica $GL_n(\mathbb{R})$ množice $\mathrm{Mat}_{n\times n}(\mathbb{R})$ ki jo sestavljajo od vseh $n \times n$ obrnljive matrike, zaprta glede na množenje matrik.

2. Naj bo $U = \{z \in \mathbb{C} : |z| = 1\}$ (U je krožnica v kompleksni ravnini s centrom v izhodišču in polmerom 1). Pokaži, da je množica U zaprta glede na množenje.

3. Naj bo G množica vseh realnih števil oblike $x + y\sqrt{2}$, kjer sta $x, y \in \mathbb{Q}$ racionalni števil, ki nista hkrati enaki ničli. Pokaži, da je G zaprta glede na običajeno množenje.

Definicija (asociativnost, komutativnost)

Binarna operacija $*$ na množici S je asociativna, če za poljubne $a, b, c \in S$ velja $(a*b)*c = a*(b*c)$. Rečemo tudi, da za $*$ velja asociativnost.

Binarna operacija $*$ na množici S je komutativna, če za poljuben par $a, b \in S$ velja $a * b = b * a$. Rečemo tudi, da za $*$ velja komutativnost.

4. Dana je množica $G = \{a \in \mathbb{R} \,|\, a > 0, a \neq 1\}$ in dana je operacija $*$ definirana na naslednji način: $a * b = a^{\log_5 b}$. Preveri, ali je $*$ binarna operacija, ter ali je asociativna in komutativna na množici G.

Za končne množice, se binarno operacijo na množici lahko definira s pomočjo tabele, v kateri so vsi elementi množice natisnjeni zgoraj in na levi strani vsake vrste. Vedno zahtevamo, da so vsi elementi natisnjeni v istem vrstnem redu. Takšna tabela se imenuje Cayley-eva tabela. Npr. Cayley-eva tabela za $(\mathbb{Z}_5, +)$ je dana na desni strani.

$+$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$*$	a	b	c	d
a	a	b		d
b		a	c	d
c	c	c	c	d
d				

5. Tabelo dano na levi strani dopolni na takšen način, da bo $*$ komutativna binarna operacija na množici $S = \{a, b, c, d\}$.

6. Tabelo dano na desni strani se lahko dopolni tako da bo $*$ asociativna binarna operacija na množici $S = \{a, b, c, d\}$. S predpostavko, da je to mogoče, izračunaj manjkajoče elemente.

$*$	a	b	c	d
a	a	b	c	
b	b	d		c
c	c	a	d	b
d	d			a

7. Dana je množica $G = \{a, b, c\}$. Določite število različnih binarnih operacij definiranih na množici G. Koliko izmed njih je komutativnih?

8. Na množici celih števil $\mathbb{Z}$ je definirana operacija $*$ na naslednji način: $a * b = a + b - 1$. Preveri, ali je $*$ binarna operacija, ter če je komutativna in asociativna na množic $\mathbb{Z}$.

9. Na množici pozitivnih realnih števil $\mathbb{R}^+$ je definirana operacija $*$ na naslednji način: $a * b = a^b$. Preveri, ali je $*$ binarna operacija, ter če je komutativna in asociativna na množic $\mathbb{R}^+$.

Definicija (nevtralni element, inverz (obrat))

Naj bo $*$ binarna operacija definirana na množici G.

Elementu $e \in G$ pravimo nevtralni element operacije $*$, če za vsak $a \in G$ velja $a * e = e * a = a$.

Elementu a' pravimo inverz elementa a glede na operacijo $*$, če velja $a * a' = e$ in $a' * a = e$, kje je e nevtralni element.

10. Naj bo $U_n = \{z \in \mathbb{C} \mid z^n = 1\}$ (množica U_n se imenuje množica n-tih korenov od 1). Pokaži da: (i) je U_n zaprta glede na običajno množenje; (ii) obstaja nevtralni element; (iii) ima vsak element $z \in U_n$ inverz.

11. Operacija "običajno" množenje je binarna operacija na množici $G = \left\{ \frac{1+2m}{1-2n} : m, n \in \mathbb{Z} \right\}$. Preveri če (i) obstaja nevtralni element; (ii) ima vsak element $a \in G$ inverz.

Definicija (grupa, abelska grupa)

Grupa $(G, *)$ je množica G skupaj z operacijo $*$ na G, ki zadošča naslednjim aksiomom:
(ZAPRTOST) Za vse $a, b \in G$ velja $a * b \in G$;
(ASOCIATIVNOST) Za vse $a, b, c \in G$ velja $(a * b) * c = a * (b * c)$.
(NEVTRALNI ELEMENT) Obstaja tak element $e \in G$, da za vsak element $a \in G$ velja $e * a = a * e = a$.
(INVERZNI ELEMENT) Za vsak element $a \in G$ obstaja $a' \in G$, za katerega velja $a * a' = a' * a = e$.

Če za binarno operacijo $*$ velja še, da je komutativna, to je, če za poljubna $a, b \in G$ velja $a * b = b * a$, pravimo, da je grupa abelska oziroma komutativna.

Če je operacija grupe $*$ množenje, potem se nevtralni element imenuje enota oziroma identiteta, in operacijo navadno izpuščamo, torej namesto grupa $(G, *)$ pišemo grupa G, namesto $a * b$ pa kar ab.

12. Ali je množica
$$G = \{X \in \mathrm{Mat}_{2\times 2}(\mathbb{R}) : \det(X) = 1\}$$
glede na običajno množenje matrik grupa? Obrazložiti svojo trditev.

13. Naj bo $GL_n(\mathbb{R}) \subseteq \mathrm{Mat}_{n\times n}(\mathbb{R})$ množica vseh $n \times n$ obrnljivih matrik, katerih elementi so realna števila. Predpostavimo, da je G grupa s šestimi elementi iz $GL_2(\mathbb{R})$ glede na operacijo množenja matrik. Pretpostavimo tudi, da velja $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \in G$ in $\begin{pmatrix} -1 & -1 \\ 0 & 1 \end{pmatrix} \in G$.

(a) Kateri so preostali elementi v G? Obrazložiti svojo trditev.

(b) Zapiši Cayley-evo tabelo za G.

(c) Ali je G abelska grupa?

14. Naj bo $\mathbb{Q}^+$ množica pozitivnih racionalnih števil, in naj bo $*$ operacija definirana na množici $\mathbb{Q}^+$ na naslednji način: $a * b = \frac{ab}{2}$. Preveri, ali je $(\mathbb{Q}^+, *)$ grupa.

15. Naj bo G grupa, ki ima naslednjo lastnost: $\forall g \in G\ g^2 = e$. Pokaži, da je G abelska grupa.

16. Naj bo G grupa z operacijo množenja, in naj bosta $a, b \in G$ dana elementa. Dokaži, da za vsako pozitivno število n velja:
$$(aba^{-1})^n = ab^n a^{-1}.$$

17. Naj bo G grupa, ki ima naslednjo lastnost: $a, b \in G$, $n \in \mathbb{Z}^+ \Rightarrow (ab)^n = a^n b^n$. Pokaži, da je G abelska grupa.

18. Dana je podmnožica $GL_n(\mathbb{R})$ množice $\mathrm{Mat}_{n\times n}(\mathbb{R})$, ki vsebuje vse $n \times n$ obrnljive metrike. Pokaži, da je $GL_n(\mathbb{R})$ grupa glede na operacijo množenja metrik.

19. Naj bo n pozitivno celo število in naj bo $n\mathbb{Z} = \{nm \mid m \in \mathbb{Z}\}$. Pokaži, da je $(n\mathbb{Z}, +)$ grupa.

Niels Abel Niels Henrik Abel, one of the foremost mathematicians of the 19th century, was born in Norway on August 5, 1802. At the age of 16, he began reading the classic mathematical works of Newton, Euler, Lagrange, and Gauss. When Abel was 18 years old, his father died, and the burden of supporting the family fell upon him. He took in private pupils and did odd jobs, while continuing to do mathematical research. At the age of 19, Abel solved a problem that had vexed leading mathematicians for hundreds of years. He proved that, unlike the situation for equations of degree 4 or less, there is no finite (closed) formula for the solution of the general fifth-degree equation.

Although Abel died long before the advent of the subjects that now make up abstract algebra, his solution to the quintic problem laid the groundwork for many of these subjects. Just when his work was beginning to receive the attention it deserved, Abel contracted tuberculosis. He died on April 6, 1829, at the age of 26.

In recognition of the fact that there is no Nobel Prize for mathematics, in 2002 Norway established the Abel Prize as the "Nobel Prize in mathematics" in honor of its native son. At approximately the $1,000,000 level, the Abel Prize is now seen as an

award equivalent to a Nobel Prize. `http:`

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

Naloge z izpita lahko najete na:
`http://osebje.famnit.upr.si/~penjic/tests/index.html`

POMEMBNI REZULTATI (Grupa. Red grupe. Red elementa.)

1. V grup je enota enolično določena edinstvena.
2. V grupi je inverz elementa enolično določen.
3. Če je $(G,\cdot)$ grupa, potem je $(a^{-1})^{-1}=a\ \ \forall a\in G$.
4. Če je $(G,\cdot)$ grupa, potem je $(ab)^{-1}=b^{-1}a^{-1}\ \ \forall a,b\in G$.
5. Če je $(G,\cdot)$ grupa in $ab=ac$, potem je $b=c$.
6. Če je $(G,\cdot)$ grupa in $ba=ca$, potem je $b=c$.
7. V končni grupi je red vsakega elementa končan in ne more biti večji od reda grupe.
8. V grupi je red elementa in njegovega inverza isti.

Nekatere družine grup je mogoče povzeti v tabeli spodaj. Tukaj je $\mathbb{R}^*=\mathbb{R}/\{0\}$; $\mathbb{C}^*=\mathbb{C}/\{0\}$; $U(n)=\{k\in\mathbb{N}\,|\,k<n,\gcd(k,n)=1\}$; $\mathrm{SL}_2(\mathbb{R})=\{X\in\mathrm{Mat}_{2\times2}(\mathbb{R}):det(X)=1\}$

Grupa	Operacija	Identiteta	Oblika elementa	Inverz	Abelska
$\mathbb{Z}$	seštevanje	0	k	$-k$	da
$\mathbb{Q}^+$	množenje	1	m/n, $m,n>0$	n/m	da
$\mathbb{Z}_n$	seštevanje modulo n	0	k	$n-k$	da
$\mathbb{R}^*$	množenje	1	x	$1/x$	da
$\mathbb{C}^*$	množenje	1	$a+ib$	$\frac{a}{a^2+b^2}-\frac{bi}{a^2+b^2}$	da
$\mathrm{GL}_2(\mathbb{R})$	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
$U(n)$	množenje modulo n	1	$k,\gcd(k,n)=1$	rešitev $kx\bmod n=1$	da
$\mathbb{R}^n$	seštevanje po komponentah	$(0,0,...,0)^\top$	$(a_1,a_2,...,a_n)^\top$	$(-a_1,-a_2,...,-a_n)^\top$	da
$\mathrm{SL}_2(\mathbb{R})$	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

Rešitve: **1.** $\mathrm{GL}_n(\mathbb{R})=\{A\in\mathrm{Mat}_{n\times n}(\mathbb{R})\,|\,\exists A^{-1}\text{ t.d. }AA^{-1}=I\}$, $(AB)(B^{-1}A^{-1})=I$
2. $z=a+ib=|z|(\cos\varphi+i\sin\varphi)=|z|e^{i\varphi}$, $z_1\cdot z_2=e^{i\theta_1}\cdot e^{i\theta_1}$; $|z_1z_2|=1$
3. $g_1\cdot g_2=\underbrace{x_1x_2+2y_1y_2}_{\in\mathbb{Q}}+\underbrace{(x_1y_2+x_2y_1)}_{\in\mathbb{Q}}\sqrt{2}$; $1^\circ\,x_1\neq0,x_2\neq0$ $2^\circ\,x_1\neq0,y_2\neq0$, $3^\circ\,y_1\neq0,x_2\neq0$, $4^\circ\,y_1\neq0,y_2\neq0$
4. $c=\log_5 b$, $a^c\neq1$, $a^c>0\ \forall c\in\mathbb{R}$; $(a*b)*c=a^{\log_5 b\cdot\log_5 c}=a*(b*c)$; je komutativna, $\log_a b=\frac{\ln b}{\ln a}\Rightarrow\ln b=\ln a\cdot\log_a b\Rightarrow\frac{\ln b}{\ln 5}=\frac{\ln a}{\ln 5}\cdot\log_a b\Rightarrow b^{\frac{\ln a}{\ln 5}}=\frac{\ln b}{\ln 5}\Rightarrow a^{\frac{\ln b}{\ln 5}}=b^{\frac{\ln a}{\ln 5}}\Rightarrow a*b=b*a]$
5. $a*c=c$, $b*a=b$, $d*a=d$, $d*b=d$, $d*c=d$, $d*d=\forall$
6. $a*d=d$, $b*c=a$, $d*b=c$, $d*c=b$
7. 3^9 različnih, 3^6 komutativnih
8. zaprta, asocijativna, komutativna
9. zaprta, ni asocijativna, ni komutativna, $(a*b)*c=a^{bc}$, $a*(b*c)=a^{b^c}$, npr. $7^2\neq2^7$

10. $1 = |z^n| = |z|^n|e^{in\varphi}| \Rightarrow |z| = 1$, $z^n = 1 \Rightarrow e^{in\varphi} = 1 \Rightarrow \cos n\varphi + i \sin n\varphi = 1 \Rightarrow \cos n\varphi = 1$, $i \sin n\varphi = 0$ $\Rightarrow \exists\, k \in \mathbb{Z}$ t. d. $\varphi = \frac{2k\pi}{n}$; $1 \in U_n$, $1 \cdot z = z \cdot 1 = z$, $z^{n-1} \in U_n$, $z \cdot z^{n-1} = 1$
11. $e = 1$, $a' = \frac{1-2n}{1+2m} = \frac{1+2(-n)}{1+2(-m)} \in G$
12. G je grupa; $\det(AB) = 1$, $A \cdot (B \cdot C) = (A \cdot B) \cdot C$, $\det(I) = 1$, $\forall A \in G$ $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ $A^{-1} = \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$, $A^{-1} \in G$
13. $A = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, B = \begin{bmatrix} -1 & -1 \\ 0 & 1 \end{bmatrix}, A^2 = I, AB = C = \begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix}, CA = D, C^2 = E = \begin{bmatrix} -1 & -1 \\ 1 & 0 \end{bmatrix}$;
$G = \{I, A, B, C, D, E\}$, ni abelska
14. $\frac{ab}{2} \in \mathbb{Q}^+$, $(a * b) * c = \frac{abc}{4} = a * (b * c)$, $e = 2$; $a' = \frac{4}{a}$; je grupa
15. $ab \in G$, $(ab)^2 = e \Rightarrow (ab)(ab) = e \Rightarrow a^2(bab) = a \Rightarrow bab = a \Rightarrow b^2ab = ba \Rightarrow ab = ba$
16. $(aba^{-1})^1 = ab^1a^{-1}$, $(aba^{-1})^2 = (aba^{-1})^1 \cdot (aba^{-1})^1 = ab^1a^{-1}ab^1a^{-1} = ab^2a^{-1}$;
$(aba^{-1})^{n+1} = (aba^{-1})^n \cdot (aba^{-1})^1$
17. $2 \in \mathbb{Z}^+$, $(ab)^2 = a^2b^2 \Rightarrow (ab)(ab) = a^2b^2 \Rightarrow ... \Rightarrow ab = ba$
18. $(AB)(B^{-1}A^{-1}) = I$
19. $a = nm_1$, $b = nm_2$, $a + b = n(m_1 + m_2) \in n\mathbb{Z}$, $e = 0 = 0m \in\ n\mathbb{Z}$, $a' = n(-m) \in n\mathbb{Z}$

Dodatek.[1]

Rešimo nalogo 13(a) z uporabo programskega jezika MAGMA.

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

```
R:=RealField();
Z:=Integers();
Mat := MatrixRing(Z, 2);

A:= Matrix(Mat![0,1, 1,0]);
B:= Matrix(Mat![-1,-1, 0,1]);
A; B;

G:={};
for i in {1..6} do
   Include(~G,A^i);
end for;
for i in {1..6} do
   Include(~G,B^i);
end for;

for X in G do
   for Y in G do
      Include(~G,X*Y);
      Include(~G,Y*X);
   end for;
end for;

G;
```

Izhod:

```
[0 1]
[1 0]
[-1 -1]
[ 0  1]
{
    [-1 -1]
    [ 0  1],

    [-1 -1]
    [ 1  0],

    [ 1  0]
    [-1 -1],

    [0 1]
    [1 0],

    [1 0]
    [0 1],

    [ 0  1]
    [-1 -1]
}
```

[1] Vidi tudi: `http://www.maths.usyd.edu.au/u/bobh/UoS/MATH2008/ctut01.pdf`