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. [$(AB)(B^{-1}A^{-1}) = I$]

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. [$z_1 \cdot z_2 = e^{i\theta_1} \cdot e^{i\theta_1}$; $|z_1 z_2| = 1$]

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.

[$g_1 \cdot g_2 = \underbrace{x_1x_2 + 2y_1y_2}_{\in\mathbb{Q}} + \underbrace{(x_1y_2 + x_2y_1)}_{\in\mathbb{Q}}\sqrt{2}$; $1^\circ\ x_1 \neq 0, x_2 \neq 0$...]

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 $G = \{a \in \mathbb{R} \mid a > 0, a \neq 1\}$ 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. [$c = \log_5 b$, $a^c \neq 1$; $(a * b) * c = a^{\log_5 b \cdot \log_5 c} = a * (b * c)$; ni komutativna]

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	d	c	d
d				

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

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

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. [$a * d = d$, $b * c = a$, $d * b = c$, $d * c = b$]

7. Dana je množica $G = \{a, b, c\}$. Določite število različnih binarnih operacij definiranih na množici G. Koliko izmed njih je komutativnih? [3^9 različnih, 3^6 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 $\mathbb{Z}$. [zaprta, asocijativna, komutativna]

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 $\mathbb{R}^+$. [zaprta, ni asocijativna, ni komutativna]

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 $U_n = \{z \in \mathbb{C} \,|\, z^n = 1\}$ (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. $[1 = |z^n| = |z|^n|e^{in\varphi}| \Rightarrow |z| = 1...]$

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

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. 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? $[A, B, A^2 = I, AB = C, CA = D, C^2 = E$; ni abelska$]$

13. 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. $[e = 2;\ a' = \frac{4}{a}$; je grupa$]$

14. Naj bo G grupa, ki ima naslednjo lastnost: $\forall g \in G\ g^2 = e$. Pokaži, da je G abelska grupa. $[ab \in G,\ (ab)^2 = e]$

15. Naj bo G grupa z operacijo množenja, in naj bosta $a, b \in G$ dana elementa. Dokaži, da za vsako pozitivno število n velja:

$$(aba^{-1})^n = ab^n a^{-1}.$$

$[(aba^{-1})^1 = ab^1a^{-1}]$

16. 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. $[(ab)^2 = a^2b^2]$

17. 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. $[(AB)(B^{-1}A^{-1}) = I]$

18. Naj bo n pozitivno celo število in naj bo $n\mathbb{Z} = \{nm \,|\, m \in \mathbb{Z}\}$. Pokaži, da je $(n\mathbb{Z}, +)$ grupa. $[e = 0,\ a' = n(-m)]$

19. 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. $[G$ je grupa$]$