# Algebra III - vse naloge z izpitnih rokov

## Grupe in podgrupe.

**1.** Dana je množica $G = \{x + y\sqrt{5} \mid x^2 - 5y^2 = 1,\ x, y \in \mathbb{Q}\}$. Pokaži, da je $(G, \cdot)$ grupa, kjer je $\cdot$ običajno množenje realnih števil. Ali je grupa $G$ abelska?

**2.** Naj bo $G$ grupa in $a, b, c \in G$ elementi grupe $G$, za katere velja $a \cdot b \cdot c = e$, kjer je $e$ enota grupe $G$. Pokaži, da potem velja tudi $b \cdot c \cdot a = e$.

**3.** Dana je množica $G = \{2x + 3y \mid x - 3y = 0,\ x, y \in \mathbb{Z}\}$.

(a.) Pokaži, da je $(G, +)$ grupa, kjer je $+$ običajno seštevanje celih števil.

(b.) Dana je podgrupa $H = \{2x + 3y \mid x - 3y = 0,\ y = 2k,\ x, k \in \mathbb{Z}\}$ grupe $G$. Napiši Cayley-evo tabelo za $G/H$.

**4.** Dana je množica $G = \{f_1, f_2, f_3, f_4\}$ kje so $f_1$, $f_2$, $f_3$ in $f_4$ preslikave definirane z

$$f_1(x) = x, \qquad f_2(x) = -x, \qquad f_3(x) = \frac{1}{x}, \qquad f_4(x) = -\frac{1}{x}, \qquad x \in \mathbb{R}, x \neq 0.$$

Pokaži, da je $(G, \circ)$ grupa, kjer je $\circ$ označuje običajno komponiranje funkcij.

**5.** Dani sta množici $H_0 = \{\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{Mat}_{2\times 2}(\mathbb{R}) \mid a + b + c + d = 0\}$ in $H_1 = \{\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{Mat}_{2\times 2}(\mathbb{R}) \mid a + b + c + d = 1\}$. Preveri, ali množici $H_0$ in $H_1$ tvorita grupi glede na operacijo seštevanja matrik. Odgovore utemeljite!

**6.** Naj bo $X$ neprazna množica. Potenčno množico $\mathcal{P}(X)$ opremimo z operacijo $\backslash$ (razlika množic)

$$\mathcal{A}\backslash\mathcal{B} := \{x \mid x \in \mathcal{A} \text{ in } x \notin \mathcal{B}\}, \quad \forall \mathcal{A}, \mathcal{B} \in \mathcal{P}(X).$$

Ali je množica $\mathcal{P}(X)$ zaprta glede na operacijo $\backslash$? Ali je operacija $\backslash$ asociativna na množici $\mathcal{P}(X)$? Odgovor utemelji!

**7.** Pokaži, da je množica $\mathcal{A} = \{\begin{bmatrix} x & y \\ 0 & 1 \end{bmatrix} \mid x, y \in \mathbb{R},\ x \neq 0\}$ zaprta za operacijo (običajnega) matričnega množenja. Ali je operacija matričnega množenja komutativna na množici $\mathcal{A}$? Ali ima vsak element iz množice $\mathcal{A}$ inverz? Odgovore utemelji!

**8.** Dana je polgrupa $(\{f : \mathbb{R} \to [0, 1]\}, \circ)$. Poišči leve in desne enote v tej polgrupi. (Spomnimo se: Za $(M, \circ)$ rečemo, da je polgrupa, če je operacija $\circ$ zaprta in asociativna.)

**9.** (a) Naj bo $S$ množica moči $n \in \mathcal{N}$. Koliko različnih binarnih operacij lahko definiramo na množici $S$?

(b) Dokažite, da tvorijo vse matrike oblike

$$\begin{bmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{bmatrix}, \qquad \alpha \in \mathbb{R}$$

grupo za običajno operacijo množenja matrik.

**10.** (a) Dana je končna grupa reda $n$. Pokaži, da se vsak element te grupe pojavi natanko enkrat v vsaki vrstici in vsakem stolpcu Cayleyeve tabele te grupe.

(b) Dana je množica $\mathcal{A} = \{A, B, C, D, P, Q, R\}$, in dana je binarna operacija $*$ definirana na množici $\mathcal{A}$, tako da je $(\mathcal{A}, *)$ grupa. Izpolni dano tabelo na desni strani tako, da bo $\mathcal{A}$ abelska grupa.

| * | A | B | C | D | P | Q | R |
|---|---|---|---|---|---|---|---|
| A | A | B | C | D | P | Q | R |
| B | B | | | | | R | |
| C | C | | | | R | | |
| D | D | | | R | | | |
| P | P | | R | | | | |
| Q | Q | R | | | | D | P |
| R | R | | | | | P | Q |

## Ciklične grupe.

**11.** Za vse podgrupe reda 8 v grupi $\mathbb{Z}_{32}$ napiši vse njihove generatorje.

**12.** Katere od naslednjih trditev so pravilne? Odgovore utemelji!

(a) Naj bodo $x_1, x_2, \ldots, x_n$ elementi poljubne grupe $G$. Potem velja

$$(x_1 x_2 \cdots x_n)^{-1} = x_n^{-1} \cdots x_2^{-1} x_1^{-1}.$$

(b) Vsaka grupa reda 79 je ciklična.

(c) Grupa $\mathbf{Z}_{35}$ ima 24 generatorjev.

(d) Grupa $G$ z enoto $e$, v kateri velja $x^2 = e$ za vsak $x \in G$, je abelska.

**13.** Naj bo $G$ ciklična grupa generirana z matriko

$$A = \begin{bmatrix} 1 & 1 \\ -1 & 0 \end{bmatrix}.$$

(a) Kateri so preostali elementi grupe $G$? Svojo trditev obrazložite.

(b) Zapiši Cayley-evo tabelo za grupo $G$.

(c) Ali je $G$ abelska grupa?

(c) Napišite vse generatorje grupe $G$.

**14.** Naj bosta $H$ in $K$ končni podgrupi grupe $G$, ter da je $\gcd(|H|, |K|)$ praštevilo. Pokaži da je $H \cap K$ ciklična grupa.

**15.** Določi vse elemente reda 9 v grupi $\mathbb{Z}_{108}$. Za vse podgrupe reda 9 v grupi $\mathbb{Z}_{108}$ napiši vse njihove generatorje.

**16.** Naj bosta $A$ in $B$ končni ciklični grupi, za kateri velja $|A| = n$ in $|B| = m$.

(a) Če je $n = 2$ in $m = 3$ pokaži, da je $A \times B$ ciklična grupa.

(b) Če je $n = 2$ in $m = 2$ pokaži, da $A \times B$ ni ciklična grupa.

(c) Ali je $A \times B$ ciklična, če je $n = 4$ in $m = 6$?

**17.** Naj bo $G = (\mathbb{Z}_{126}, +)$ dana grupa.

(a) Poišči vse možne rede elementov grupe $G$. Za vsakega od možnih redov podaj element grupe $G$, ki ima tak red.

(b) Za vsakega od možnih redov določi število elementov grupe $G$, ki imajo ta red.

(c) Določi število (cikličnih) podgrup grupe $G$, ki so reda 7 (odgovor obrazloži brez uporabe znane trditve s predavanja ali vaj).

## Permutacijske grupe.

**18.** Naj bosta $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 4 & 5 & 1 & 7 & 8 & 6 \end{pmatrix}$ in $\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 3 & 8 & 7 & 6 & 5 & 2 & 4 \end{pmatrix}$ elementa simetrične grupe $S_8$.

(a) Napiši $\alpha$, $\beta$ in $\alpha\beta$ kot produkt disjunktnih ciklov.
(b) Napiši $\alpha$, $\beta$ in $\alpha\beta$ kot produkt 2-ciklov (kot produkt transpozicij).
(c) Določi $\alpha^{-2}$.

**19.** Naj bosta $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 3 & 5 & 4 & 6 \end{pmatrix}$ in $\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 1 & 2 & 4 & 3 & 5 \end{pmatrix}$.

(a) Napiši $\alpha$, $\beta$ in $\alpha\beta$ kot produkt 2-ciklov (kot produkt transpozicij).
(b) Določi red permutacij $\alpha$ in $\beta$.
(c) Določi $\alpha^{-3}$.

**20.** Naj bosta $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 1 & 5 & 4 & 8 & 6 & 7 \end{pmatrix}$ in $\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 1 & 7 & 8 & 6 & 5 & 4 & 2 \end{pmatrix}$.

(a) Napiši $\alpha\beta$ in $\beta^2\alpha$ kot produkt disjunktnih ciklov.

(b) Napiši $\alpha\beta$ in $\beta^2\alpha$ kot produkt 2-ciklov (torej kot produkt transpozicij).

(c) Določi $\alpha^{-1}$, $\beta^{-1}$ in $(\alpha\beta)^{456}$.

**21.** Naj bo $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 7 & 3 & 6 & 2 & 8 & 4 & 9 & 5 & 1 \end{pmatrix}$. Izračunaj $\pi^{-1}$, $\pi^{2017}$ in $\pi^{-2}\pi^4$. Napiši $\pi^{-2}\pi^4$ kot produkt 2-ciklov (torej kot produkt transpozicij).

**22.** Podane so naslednje permutacije:

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}, \quad \beta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix}, \quad \gamma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}, \quad \delta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}.$$

(a) Zapišite ciklične dekompozicije permutacij.

(b) Permutacije izrazite kot produkt transpozicij.

(c) Izračunajte $\alpha\beta$, $\beta\alpha$, $\alpha^{-1}\beta$, $\beta\alpha^2$, $(\alpha\beta)^{-2}$, $\alpha\beta\alpha^3$, $\gamma^{-1}\beta\gamma^{-1}$ in $\gamma\beta^2\alpha$.

**23.** Dana je simetrična grupa $S_5$ (grupa vseh permutacij množice $\{1, 2, 3, 4, 5\}$).

(a) Pokaži, da $S_5$ ni abelska.

(b) Določi število elementov reda 3 grupe $S_5$.

(c) Določi število elementov reda 2 grupe $S_5$

(d) Določi redove vseh $5! = 120$ elementov iz $S_5$.

## Izomorfizmi grup.

**24.** Naj bo $G = \mathbb{Z}_3 \times \mathbb{Z}_3$ in $H = \mathbb{Z}_9$. Ali je $G \cong H$? Odgovor utemelji!

**25.** Naj bo $G = \mathbb{Z}_2 \times \mathbb{Z}_3$ in $H = \mathbb{Z}_6$. Ali je $G \cong H$? Odgovor utemeljite!

**26.** Poišči grupo permutacij, ki je izomorfna grupi $\mathbb{Z}_4$. Napiši Cayleyevo tabelo za $\mathbb{Z}_4$ ter za dobljeno grupu permutacij.

**27.** Konstruiraj Cayley-evo tabelo za alternirajoči grupi $A_2$ in $A_3$. Ali je $\mathbb{Z}_3 \cong A_3$? (Odgovor razloži.)

**28.** Naj bo $f : G \longrightarrow G'$ homomorfizem grup in $H \leq G$. Pokaži, da je

$$f(H) \leq G'.$$

## Odseki in Lagrangeov izrek.

**29.** Napiši vse leve odseke podgrupe $\langle(1432)\rangle$ v grupi $S_4$.

**30.** Poišči vse leve odseke podgrupe $H$ v grupi $G$, če je:
(a) $G = \mathbb{Z}_{24}$ in $H = \langle 4\rangle$.
(b) $G = S_3$ in $H = \langle(23)\rangle$.

**31.** Naj bo $S_4$ simetrična grupa reda 4!.
(a) Določite podgrupo grupe $S_4$, ki vsebuje 6 elementov.
(b) Koliko podgrup reda 6 obstaja v grupi $S_4$?
(c) Če je $H = \langle(12), (13)\rangle$, določite vse leve odseke podgrupe $H$ v grupi $S_4$.

**32.** Naj bo $G$ dana grupa in naj bo $|G| = 8$. Pokaži, da mora $G$ vsebovati element reda 2.

**33.** Naj bo $S_{[0,1]}$ množica vseh bijekcij iz intervala $[0, 1]$ na interval $[0, 1]$.

(a) Pokaži, da je $S_{[0,1]}$ grupa glede na operacijo komponiranja preslikav.

(b) Naj bo $T = \{\alpha \in S_{[0,1]} \mid \alpha(0) = 0\}$. Pokaži, da je $T$ podgrupa grupe $S_{[0,1]}$ (razloži tudi, zakaj je $T$ neprazna množica).

(c) Pokaži, da je $\{\sigma \in S_{[0,1]} \mid \sigma(0) = 1\}$ levi odsek podgrupe $T$ v grupi $S_{[0,1]}$.

(d) Določi $[S_{[0,1]} : T]$.

## Direktni produkt grup.

**34.** Množica $G = \mathbb{Z}_4 \times \mathbb{Z}_2$ tvori grupo glede na operacijo seštevanja.
(a) Napiši Cayley-evo tabelo grupe $G$.
(b) Za vse podgrupe reda 4 v grupi $G$ napiši vse njihove generatorje.
(c) Poišči vse leve odseke podgrupe $H = \langle(1, 1)\rangle$ v grupi $G$.

**35.** Določi število elementov reda 12 v grupi $\mathbb{Z}_3 \times \mathbb{Z}_4 \times U(9)$.

## Podgrupe edinke. Kvocientne grupe.

**36.** Naj bo $U(20) = \{i \in \mathbb{N} \mid 1 \leq i \leq 20,\ \gcd(i, 20) = 1\}$. Vemo, da je $U(20)$ grupa za množenje po modulu 20. Naj bo $H = \langle 9 \rangle$ ciklična podgrupa grupe $U(20)$, generirana z 9.

(a.) Poišči vse desne odseke podgrupe $H$ v grupi $U(20)$.

(b.) Napiši Cayley-evo tabelo za $U(20)/H$.

(c.) Poišči vse podgrupe grupe $U(20)/H$.

**37.** (a) Dana je grupa $G = \{1, 8, 12, 14, 18, 21, 27, 31, 34, 38, 44, 47, 51, 53, 57, 64\}$ za operacijo množenja po modulu 65, in naj bo $H = \langle 12 \rangle$ podgrupa grupe $G$. Napiši Cayley-evo tabelo za $G/H$.

(b) Določi red elementa $8\langle 16 \rangle$ v grupi $U(105)/\langle 16 \rangle$.

**38.** (a) Poišči odseke podgrupe $\langle 4 \rangle$ v grupi $\mathbb{Z}_{12}$ in konstruiraj Cayley-evo tabelo za kvocientno grupo $\mathbb{Z}_{12}/\langle 4 \rangle$.

(b) Če obstaja, poišči kak netrivialni homomorfizem $\varphi : \mathbb{Z}_{12} \to \mathbb{Z}_4$.

**39.** Poišči indeks podgrupe $\langle 3 \rangle$ v grupi $\mathbb{Z}_{24}$. Poišči indeks podgrupe $\langle (2, 3) \rangle$ v grupi $\mathbb{Z}_4 \times \mathbb{Z}_6$. Napiši Cayley-evo tabelo za kvocientno grupo $\mathbb{Z}_{24}/\langle 3 \rangle$.

**40.** (a) Naj bo $G$ grupa reda 77 in naj bo $H$ podgrupa grupe $G$ reda 11. Pokaži, da je $H$ edinka grupe $G$.

(Spomnimo se: Za končne podgrupe $H$ in $K$ grupe $G$ velja

$$|HK| = \frac{|H||K|}{|H \cap K|}$$

kjer je $HK = \{hk \mid h \in H,\ k \in K\}$.)

(b) Naj bosta $H$ in $K$ edinki grupe $G$, tako da velja $H \cap K = \{e\}$, $|H| = p$ ($p$ je praštevilo) in $|K| = 4$. Če je $HK = G$, potem pokaži, da je $G$ abelska.

(Spomnimo se: Če sta $H$ in $K$ edinki grupe $G$ in če je $H \cap K = \{e\}$, potem je $hk = kh$ za vsak $h \in H$ in $k \in K$).

## Homomorfizmi grup.

**41.** Dana je grupa $G = \{1, 2, ..., 12\}$ z operacijo množenja po modulu 13. Določi vse homomorfizme iz grupe $G$ v grupo $(\mathbb{Z}_6, +)$.

**42.** Dani sta grupi $(\mathbb{Z}_9, +)$ in $(\mathbb{Z}_3, +)$. Poišči vse homomorfizme iz grupe $\mathbb{Z}_9$ v grupo $\mathbb{Z}_3$.

**43.** Naj bo $U(10) = \{k \in \mathbb{N} \mid 1 \leq k \leq 10,\ \gcd(k, 10) = 1\}$. Vemo, da je $U(10)$ grupa za množenje po modulu 10.

(a) Določi vse edinke grupe $U(10)$.

(b) Izračunaj center grupe $U(10)$.

(c) Določi vse homomorfizme iz grupe $U(10)$ v grupo $(\mathbb{Z}_8, +)$.

**44.** Določi vse homomorfizme iz grupe $\mathbb{Z}_4$ v grupo $\mathbb{Z}_2 \times \mathbb{Z}_2$.

**45.** Uporabi prvi izrek o izomorfizmu, in pokaži, da je $\mathbb{Z} \times \mathbb{Z}/\langle(2,7)\rangle \cong \mathbb{Z}$.

**46.** Naj bo dana grupa $G = \{z \in \mathbb{C} \mid |z| = 1\}$ za operacijo množenja kompleksnih števil in podmnožica $H = \{1, -1\} \subseteq G$. Pokaži, da je $H$ podgrupa edinka v $G$ in da velja $G/H \cong G$.

**47.** Naj bo $\mathbb{R}^*$ grupa neničelnih realnih števil glede na operacijo množenja. Uporabi prvi izrek o izomorfizmu, in pokaži da je

$$\mathbb{R}^*/\langle -1\rangle \cong \mathbb{R}^+.$$

## Delovanje grupe na množici.

**48.** Naj bo $G$ grupa realnih števil z operacijo seštevanja $(\mathbb{R}, +)$. Za $r \in G$ ter $(x, y) \in \mathbb{R}^2$ definirajmo $r * (x, y) = (x + ry, y)$. Naj bo $T$ poljubna točka v ravnini.

(a.) Pokaži, da je preslikava $* : G \times \mathbb{R}^2 \to \mathbb{R}^2$ delovanje grupe $G$ na množici $\mathbb{R}^2$.

(b) Geometrijsko opiši orbito, ki vsebuje točko $T$.

(c) Poišči stabilizator $G_T$.

(d) Če je $H = \{(1, 2), (2, 3)\} \subseteq \mathbb{R}^2$, določi $5 + G_H$.

**49.** Naj bo $G$ podgrupa grupe $S_8$, generirana z elementoma $(123)(45)$ in $(78)$. Potem $G$ kot grupa permutacij deluje na množici $X = \{1, 2, ..., 8\}$. Poišči orbito in stabilizator vseh elementov množice $X$.

**50.** Naj bo $G$ poljubna grupa, ki deluje na neki množici $X$. Predpostavimo, da je pri tem delovanju 6 orbit. Naj bo $H \leq G$ in naj bo $[G : H] = 3$. Koliko orbit ima lahko delovanje podgrupe $H$ na množici $X$?

**51.** Za vsako od naslednjih delovanj grupe $G$ na množici $X$, opiši orbito in stabilizator danega elementa $x \in X$.

(a) $X =$ kvadrat, $G = \mathrm{Sym}(X)$ in $x =$ ogljišče kvadrata.

(b) $X = \{1, 2, 3, 4\}$, $G = A_4$ in $x = 4$.

(c) $X = \mathbb{R}^2$, $G = \mathrm{GL}_2(\mathbb{R})$ in $x = (1, 2)^\top$.

**52.** Naj bo $D_6$ diederska grupa reda 6. Grupa $D_6$ deluje na množici $X = \{A, B, C\}$ ogljišč enakostraničnega trikotnika $\triangle ABC$. Določite orbito in stabilizator vsakega elementa iz množice $X$ glede na delovanje grupe $D_6$.

**53.** Dan je pravilni petkotnik katerega, ogljišča so označena s števili 1, 2, 3, 4 in 5. Naj bo $G$ grupa vseh simetrij pravilnega petokotnika 12345 in naj bo $H = G_1$ ($H$ je stabilizator ogljišča 1 v grupi $G$).

(a) Določi element $\alpha \in G$ za katerega je $\alpha(1) = 4$. Poišči orbito ogljišča 1 glede na grupo $G$.

(b) Določi element $\beta \in H$ za katerega je $\beta(2) = 5$. Poišči orbito ogljišča 2 glede na grupo $H$.

(c) Ispiši vse elemente stabilizatora $H_2$.

(d) Uporabi orbita-stabilizator izrek in dokaži, da je $|G| = 10$.

**54.** Naj bo $\mathcal{O}$ grupa vseh simetrij kocke (rotacija, zrcaljenje, drsno zrcaljenje,...). Grupa $\mathcal{O}$ deluje na množici $\{v_1, v_2, ..., v_8\}$ ogljišč kocke. Določi stabilizator ogljišča $v_1$ v grupi $\mathcal{O}$. Uporabi orbita-stabilizator izrek in dokaži, da je $|\mathcal{O}| = 48$.

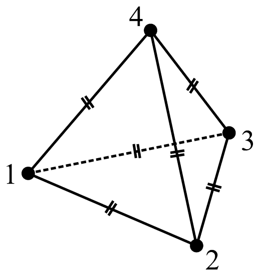
**55.** Diederska grupa $G = D_6$ na naraven način deluje na množici oglišč pravilnega 6-kotnika, označimo jo z $X = \{1,2,3,4,5,6\}$. Enako velja za njene podgrupe $H = \langle \rho \rangle$, $K = \langle \tau \rangle$ in $L = \langle \tau\rho \rangle$ kjer je $\rho = (123456)$ in $\tau = (26)(35)$.

(a) Poišči orbite delovanj grup $G$, $H$, $K$ in $L$ na $X$!

(b) Spomnimo se: Delovanje je tranzitivno, če za poljubna $x_1, x_2 \in X$, obstaja $g \in G$, da je $x_1 = g * x_2$. Katera izmed delovanj $G$, $H$, $K$ in $L$ so tranzitivna?

(c) Spomnimo se: Delovanje je zvesto, če $\forall g \in G : g * x = x \ \forall x \in X \Rightarrow g = e$. Je delovanje $G$ na $X$ zvesto? Kaj pa ostala delovanja?

**56.** Naj bo $\mathcal{O}$ grupa vseh simetrij tetraedra (rotacija, zrcaljenje, drsno zrcaljenje,...). Grupa $\mathcal{O}$ deluje na množici $\{v_1, v_2, v_3, v_4\}$ ogljišč tetraedra. Določi stabilizator ogljišča $v_1$ glede na to delovanje. Uporabi orbita-stabilizator izrek in izračunaj $|\mathcal{O}|$.




## Center. Normalizator elementa.

**57.** Množica $G = \{1, -1, i, -i, j, -j, k, -k\}$ tvori grupo glede na operacijo množenja, in njena Cayley-eva tabela je dana na desni strani.

(a.) Določi vse edinke grupe $G$.

(b.) Izračunaj center grupe $G$.

(c.) Izračunaj normalizator ter centralizator elementov $j$ in $-k$.

| $*$ | $1$ | $-1$ | $i$ | $-i$ | $j$ | $-j$ | $k$ | $-k$ |
|---|---|---|---|---|---|---|---|---|
| $1$ | $1$ | $-1$ | $i$ | $-i$ | $j$ | $-j$ | $k$ | $-k$ |
| $-1$ | $-1$ | $1$ | $-i$ | $i$ | $-j$ | $j$ | $-k$ | $k$ |
| $i$ | $i$ | $-i$ | $-1$ | $1$ | $k$ | $-k$ | $-j$ | $j$ |
| $-i$ | $-i$ | $i$ | $1$ | $-1$ | $-k$ | $k$ | $j$ | $-j$ |
| $j$ | $j$ | $-j$ | $-k$ | $k$ | $-1$ | $1$ | $i$ | $-i$ |
| $-j$ | $-j$ | $j$ | $k$ | $-k$ | $1$ | $-1$ | $-i$ | $i$ |
| $k$ | $k$ | $-k$ | $j$ | $-j$ | $-i$ | $i$ | $-1$ | $1$ |
| $-k$ | $-k$ | $k$ | $-j$ | $j$ | $i$ | $-i$ | $1$ | $-1$ |

| $\circ$ | $1$ | $a$ | $b$ | $c$ | $d$ | $e$ | $f$ | $g$ |
|---|---|---|---|---|---|---|---|---|
| $1$ | $1$ | $a$ | $b$ | $c$ | $d$ | $e$ | $f$ | $g$ |
| $a$ | $a$ | $e$ | $c$ | $g$ | $b$ | $f$ | $1$ | $d$ |
| $b$ | $b$ | $c$ | $f$ | $1$ | $e$ | $g$ | $d$ | $a$ |
| $c$ | $c$ | $g$ | $1$ | $a$ | $f$ | $d$ | $b$ | $e$ |
| $d$ | $d$ | $b$ | $e$ | $f$ | $a$ | $c$ | $g$ | $1$ |
| $e$ | $e$ | $f$ | $g$ | $d$ | $c$ | $1$ | $a$ | $b$ |
| $f$ | $f$ | $1$ | $d$ | $b$ | $g$ | $a$ | $e$ | $c$ |
| $g$ | $g$ | $d$ | $a$ | $e$ | $1$ | $b$ | $c$ | $f$ |

**58.** Množica $G = \{1, a, b, c, d, e, f, g\}$ tvori grupo glede na binarno operacijo $\circ$. Njena Cayley-eva tabela je dana na levi strani.

(a) Določi vse ciklične podgrupe grupe $G$. Za vsako ciklično podgrupo napiši vse njene generatorje.

(b) Za vsak $x \in G$ izračunaj $|x|$. Odgovor obrazloži!

(c.) Izračunaj center grupe $G$.

(d.) Izračunaj normalizator ter centralizator elementov $a$ in $g$.

## Izreki Sylowa.

**59.** Poišči vse Sylowe 2-podgrupe grupe $D_{10}$ (diederska grupa vseh simetrij pravilnega 10-kotnika glede na operacijo kompozicije).

**60.** Pokaži, da grupa $G$ reda 992 ne more biti enostavna.

**61.** Množica $G = \{I, A, B, AB, BA, ABA\}$ tvori grupo glede na operacijo množenja, in njena Cayley-eva tabela je podana na desni strani. Določite vse Sylowe 2-podgrupe grupe $G$ ter vse Sylowe 3-podgrupe grupe $G$.

| | $I$ | $A$ | $B$ | $AB$ | $BA$ | $ABA$ |
|---|---|---|---|---|---|---|
| $I$ | $I$ | $A$ | $B$ | $AB$ | $BA$ | $ABA$ |
| $A$ | $A$ | $I$ | $AB$ | $B$ | $ABA$ | $BA$ |
| $B$ | $B$ | $BA$ | $I$ | $ABA$ | $A$ | $AB$ |
| $AB$ | $AB$ | $ABA$ | $A$ | $BA$ | $I$ | $B$ |
| $BA$ | $BA$ | $B$ | $ABA$ | $I$ | $AB$ | $A$ |
| $ABA$ | $ABA$ | $AB$ | $BA$ | $A$ | $B$ | $I$ |

**62.** Poišči mogoče število Sylowih 3-podgrup in Sylowih 7-podgrup v grupi reda 3087.

**63.** Pokaži, da mora grupa reda 63 vsebovati element reda 3.

(a) Z uporabo Cauchy-evega izreka.

(b) Brez uporabe Cauchy-evega izreka ali izreka Sylowa.

**64.** Pokaži, da je vsaka abelska grupa reda 15 ciklična.

**65.** Naj bo $G$ enostavna grupa reda 168. Koliko elemntov reda 7 je v $G$?

## Rešitve.

**1.** $(x_1 + y_1\sqrt{5})(x_2 + y_2\sqrt{5}) = (x_1x_2 + 5y_1y_2) + (x_1y_2 + y_1x_2)\sqrt{5}$, $(x_1x_2 + 5y_1y_2)^2 - 5(x_1y_2 + y_1x_2)^2 = 1$, $1 = 1 + 0\sqrt{5} \in G$, $(x + y\sqrt{5})^{-1} = x - y\sqrt{5} \in G$.

**2.** $abc = e$, $bc = a^{-1}$, $bca = e$.

**3.** (a.) $(2x_1 + 3y_1) + (2x_2 + 3y_2) = 2(x_1 + x_2) + 3(y_1 + y_2)$, $(x_1 + x_2) - 3(y_1 + y_2) = 0$, $0 = 2 \cdot 0 + 3 \cdot 0$, $(2x + 3y) + (2(-x) + 3(-y)) = 0$. (b.) $G = \{..., -45, -36, -27, -18, -9, 0, 9, 18, 27, 36, 45, ...\}$, $H = \{..., -36, -18, 0, 18, 36, ...\}$

| $+$ | $H$ | $9+H$ |
|---|---|---|
| $H$ | $H$ | $9+H$ |
| $9+H$ | $9+H$ | $H$ |

**4.**

| $\circ$ | $f_1$ | $f_2$ | $f_3$ | $f_4$ |
|---|---|---|---|---|
| $f_1$ | $f_1$ | $f_2$ | $f_3$ | $f_4$ |
| $f_2$ | $f_2$ | $f_1$ | $f_4$ | $f_3$ |
| $f_3$ | $f_3$ | $f_4$ | $f_1$ | $f_2$ |
| $f_4$ | $f_4$ | $f_3$ | $f_2$ | $f_1$ |

**5.** $H_0 : (a + a_1) + (b + b_1) + (c + c_1) + (d + d_1) = 0$ je zaprta; je asociativna; identiteta je $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$; $\begin{bmatrix} -a & -b \\ -c & -d \end{bmatrix}$ je inverz za $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$; $H_0$ je grupa. $H_1$ ni grupa (ni zaprta), npr. $\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} \in H_1$ ampak $\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} \notin H_1$.

**6.** je zaprta, ni asociativna. Npr. če je $\mathcal{A} := \{a\} \subset \mathcal{P}(X)$ in $\mathcal{B} := \emptyset \subset \mathcal{P}(X)$ potem $(\mathcal{A}\backslash\mathcal{B})\backslash\mathcal{A} = \emptyset$, $\mathcal{A}\backslash(\mathcal{B}\backslash\mathcal{A}) = \mathcal{A}$...

**7.** je zaprta, ni komutativna, inverz je $\begin{bmatrix} \frac{1}{x} & -\frac{y}{x} \\ 0 & 1 \end{bmatrix} \in \mathcal{A}$.

**8.** Leva identiteta je $e(x) = \begin{cases} x & \text{če} \;\; x \in [0,1], \\ 1 & \text{če} \;\; x \in \mathbb{R}\backslash[0,1]. \end{cases}$

Polgrupa nima desne identitete.

**9.** (a) $|S| = n \Rightarrow |S \times S| = n^2$. Vsak od $n^2$ elementov se lahko preslika v $n$ različnih elementov; $n \cdot n \cdot ... \cdot n = n^{n^2} \Rightarrow$ obstaja $n^{n^2}$ različnih binarnih operacij.

(b) $\begin{bmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{bmatrix} \cdot \begin{bmatrix} \cos\beta & -\sin\beta \\ \sin\beta & \cos\beta \end{bmatrix} = \begin{bmatrix} \cos(\alpha+\beta) & -\sin(\alpha+\beta) \\ \sin(\alpha+\beta) & \cos(\alpha+\beta) \end{bmatrix}$;

$\begin{bmatrix} \cos 0 & -\sin 0 \\ \sin 0 & \cos 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$;

$\begin{bmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{bmatrix} \cdot \begin{bmatrix} \cos(-\alpha) & -\sin(-\alpha) \\ \sin(-\alpha) & \cos(-\alpha) \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} \cos(-\alpha) & -\sin(-\alpha) \\ \sin(-\alpha) & \cos(-\alpha) \end{bmatrix} \cdot \begin{bmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{bmatrix}$.

**10.** (a) Če je $ab = c$ in $ad = c$, potem $b = d$. Če je $ab = c$ in $gb = c$ potem $a = g$.

(b) Vsaka grupa praštevilskega reda je ciklična. Dana grupa je reda 7.

| * | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
| 1 | 1 | 2 | 3 | 4 | 5 | 6 | 0 |
| 2 | 2 | 3 | 4 | 5 | 6 | 0 | 1 |
| 3 | 3 | 4 | 5 | 6 | 0 | 1 | 2 |
| 4 | 4 | 5 | 6 | 0 | 1 | 2 | 3 |
| 5 | 5 | 6 | 0 | 1 | 2 | 3 | 4 |
| 6 | 6 | 0 | 1 | 2 | 3 | 4 | 5 |

$\cong$

| * | A | B | C | D | P | Q | R |
|---|---|---|---|---|---|---|---|
| A | A | B | C | D | P | Q | R |
| B | B | C | D | P | Q | R | A |
| C | C | D | P | Q | R | A | B |
| D | D | P | Q | R | A | B | C |
| P | P | Q | R | A | B | C | D |
| Q | Q | R | A | B | C | D | P |
| R | R | A | B | C | D | P | Q |

**11.** $|\langle 16\rangle| = 2$, $|\langle 8\rangle| = |\langle 24\rangle| = 4$, $|\langle 4\rangle| = |\langle 12\rangle| = |\langle 20\rangle| = |\langle 28\rangle| = 8$.

**12.** (a.) $(x_1x_2...x_n)(x_yx_2...x_n)^{-1} = e$, $(x_1x_2...x_n)(x_n^{-1}\cdots x_2^{-1}x_1^{-1}) = e$. (b.) Naj bo $|G| = 79$. Potem $\forall a \in G$, $a \neq e$, $\langle a\rangle = G$. (c.) Da. ($\langle 0\rangle \neq G$, $\langle 5\rangle \neq G$, $\langle 7\rangle \neq G$,...) (d.) $(xy)^2 = e$, $xyxy = e$, $x^2yxy = x$, $yxy = x$, $xy = yx$.

**13.** (a) $A = \begin{bmatrix} 1 & 1 \\ -1 & 0 \end{bmatrix}$, $A^2 = \begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix}$, $A^3 = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$, $A^4 = \begin{bmatrix} -1 & -1 \\ 1 & 0 \end{bmatrix}$, $A^5 = \begin{bmatrix} 0 & -1 \\ 1 & 1 \end{bmatrix}$,

$A^6 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I$. (b)

| | $I$ | $A$ | $A^2$ | $A^3$ | $A^4$ | $A^5$ |
|---|---|---|---|---|---|---|
| $I$ | $I$ | $A$ | $A^2$ | $A^3$ | $A^4$ | $A^5$ |
| $A$ | $A$ | $A^2$ | $A^3$ | $A^4$ | $A^5$ | $I$ |
| $A^2$ | $A^2$ | $A^3$ | $A^4$ | $A^5$ | $I$ | $A$ |
| $A^3$ | $A^3$ | $A^4$ | $A^5$ | $I$ | $A$ | $A^2$ |
| $A^4$ | $A^4$ | $A^5$ | $I$ | $A$ | $A^2$ | $A^3$ |
| $A^5$ | $A^5$ | $I$ | $A$ | $A^2$ | $A^3$ | $A^4$ |

(c) Da. (d) $G = \langle A\rangle$, $G = \langle A^5\rangle$.

**14.** $H \cap K$ je podgrupa grupe $G$. Če je $k = |H \cap K|$ potem $k$ deli $|H|$ in $k$ deli $|K|$. Če $k$ deli $\gcd(|H|, |K|) \Rightarrow k = 1$ ali $k$ je praštevilo...

**15.** Uporabi izrek: 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 $\mathbb{Z}_n$; ali izrek za 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 $\phi(d)$; ali fundamentalni izrek za ciklične grupe...

$|12| = |24| = |48| = |60| = |84| = |96| = 9$.

**16.** lahko uporabimo izrek $|(a,b)| = \mathrm{lcm}(|a|, |b|)$.

(a) $|A| = 2 \Rightarrow \exists a \in A$ t.d. $|a| = 2$; $|B| = 2 \Rightarrow \exists b \in B$ t.d. $|b| = 3$;... $A \times B = \langle (a,b)\rangle$.

(b) $\forall (a,b) \in A \times B$ imamo $|(a,b)| \leq 2$; ni ciklična

(c) $\forall (a,b) \in A \times B$ imamo $|(a,b)| \leq 12$; ni ciklična

**??.** (a) Grupa G lahko ima elemente reda: 1, 2, 3, 6, 7, 9, 14, 18, 21, 42, 63, 126.

$$|0| = 1,\ |63| = 2,\ |42| = 3,\ |21| = 6,\ |18| = 7,\ |14| = 9,\ |9| = 14,\ |7| = 18,$$

$$|6| = 21,\ |3| = 42,\ |2| = 63,\ |1| = 126$$

(b) $\phi(1) = |U(1)| = 1$, $\phi(2) = |U(2)| = 1$, $\phi(3) = |U(3)| = 2$, $\phi(6) = |U(6)| = 2$, $\phi(7) = |U(7)| = 6$, $\phi(9) = |U(9)| = 6$, $\phi(14) = |U(14)| = 6$, $\phi(18) = |U(18)| = 6$, $\phi(21) = |U(21)| = 12$, $\phi(42) = |U(42)| = 12$, $\phi(63) = |U(63)| = 36$, $\phi(126) = |U(126)| = 36$.

(c) Če je $H = \{e, a, a^2, a^3, ..., a^7\}$ ciklična grupa reda 7 potem, so vsi elementi $\{a, a^2, a^3, ..., a^7\}$ reda 7. Kako je $\phi(7) = 6$ to obstaja samo ena podgrupa grupe $G$ reda 7.

**18.** (a.) $\alpha = (12345)(678)$, $\beta = (23847)(56)$, $\alpha\beta = (12485736)$. (b.) $\alpha = (15)(14)(13)(12)(68)(67)$, $\beta = (27)(24)(28)(23)(56)$, $\alpha\beta = (16)(13)(17)(15)(18)(14)(12)$. (c.) $\alpha^{-2} = (14253)(678)$.

**19.** (a) $\alpha = (12)(45)$, $\beta = (12)(13)(15)(16)$, $\alpha\beta = (13)(15)(14)(16)$. (b) $\alpha^2 = id$, $|\alpha| = 2$, $|\beta| = 5$. (c) $\alpha^{-3} = (12)(45)$.

**20.** (a) $\alpha\beta = (364758)$, $\beta^2 = (178)(234)$, $\beta^2\alpha = (1376)(245)$. (b) $\alpha\beta = (38)(35)(37)(34)(36)$, $\beta^2\alpha = (16)(17)(13)(25)(24)$. (d) $\alpha^{-1} = (132)(45)(678)$, $\beta^{-1} = (128473)(56)$, $(\alpha\beta)^6 = \mathrm{id}$, $(\alpha\beta)^{456} = \mathrm{id}$.

**21.** $\pi = (179)(2364)(58)$, $\pi^{-1} = (971)(4632)(58)$, $|\pi| = \mathrm{lcm}(3,4,2) = 12$, $\pi^{12} = \mathrm{id}$, $\pi^{2017} = \pi$, $\pi^{-2}\pi^4 = \pi^2 = (17)(19)(26)(34)$.

**22.** $\alpha = (1234)$, $\beta = (23)$, $\gamma = (12)(34)$, $\delta = (132)$.

$\alpha = (14)(13)(12)$, $\beta = (23)$, $\gamma = (12)(34)$, $\delta = (12)(13)$.

$\alpha\beta = (124)$, $\beta\alpha = (134)$, $\alpha^{-1}\beta = (143)$, $\beta\alpha^2 = (1243)$, $(\alpha\beta)^{-2} = (124)$, $\alpha\beta\alpha^3 = (34)$, $\gamma^{-1}\beta\gamma^{-1} = (14)$ in $\gamma\beta^2\alpha = (24)$.

**23.** (a) $(12), (13) \in S_5$, $(12)(13) = (132) \neq (123) = (13)(12)$.

(b) $\dfrac{5\cdot4\cdot3}{3} = 20$

(c) $\dfrac{5\cdot4}{2} + \dfrac{5\cdot4\cdot3\cdot2}{8} = 10 + 15 = 25$

(d) 1, 2, 3, 4, 5 in 6.

**24.** $G \ncong H$, $\forall (a,b) \in \mathbb{Z}_3 \times \mathbb{Z}_3$ $|(a,b)| \leq 3$.

**25.** $G = \{(0,0),(0,1),(0,2),(1,0),(1,1),(1,2)\}$;

| | (0,0) | (0,1) | (0,2) | (1,0) | (1,1) | (1,2) |
|---|---|---|---|---|---|---|
| (0,0) | (0,0) | (0,1) | (0,2) | (1,0) | (1,1) | (1,2) |
| (0,1) | (0,1) | (0,2) | (0,0) | (1,1) | (1,2) | (1,0) |
| (0,2) | (0,2) | (0,0) | (0,1) | (1,2) | (1,0) | (1,1) |
| (1,0) | (1,0) | (1,1) | (1,2) | (0,0) | (0,1) | (0,2) |
| (1,1) | (1,1) | (1,2) | (1,0) | (0,1) | (0,2) | (0,0) |
| (1,2) | (1,2) | (1,0) | (1,1) | (0,2) | (0,0) | (0,1) |

; $H = \{0,1,2,3,4,5\}$;

| | 0 | 2 | 4 | 3 | 5 | 1 |
|---|---|---|---|---|---|---|
| 0 | 0 | 2 | 4 | 3 | 5 | 1 |
| 2 | 2 | 4 | 0 | 5 | 1 | 3 |
| 4 | 4 | 0 | 2 | 1 | 3 | 5 |
| 3 | 3 | 5 | 1 | 0 | 2 | 4 |
| 5 | 5 | 1 | 3 | 2 | 4 | 0 |
| 1 | 1 | 3 | 5 | 4 | 0 | 2 |

;

Da, $G \cong H$, $\varphi : G \longrightarrow H$ je izomorfizem, kje $\varphi(0,0) = 0$, $\varphi(0,1) = 2$, $\varphi(0,2) = 4$, $\varphi(1,0) = 3$, $\varphi(1,1) = 5$ in $\varphi(1,2) = 1$...

**26.** $T_0 = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 0 & 1 & 2 & 3 \end{pmatrix}$, $T_1 = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 1 & 2 & 3 & 0 \end{pmatrix}$, $T_2 = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 2 & 3 & 0 & 1 \end{pmatrix}$, $T_3 = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 3 & 0 & 1 & 2 \end{pmatrix}$...

**27.** $|A_2| = \frac{2!}{2} = 1$, $A_2 = \{(1)\}$;
$|A_3| = \frac{3!}{2} = 3$, $A_3 = \{(1), (123), (132)\}$;

| $\cdot$ | (1) |
|---|---|
| (1) | (1) |

| $\cdot$ | (1) | (123) | (132) |
|---|---|---|---|
| (1) | (1) | (123) | (132) |
| (123) | (123) | (132) | (1) |
| (132) | (132) | (1) | (123) |

| + | 0 | 1 | 2 |
|---|---|---|---|
| 0 | 0 | 1 | 2 |
| 1 | 1 | 2 | 0 |
| 2 | 2 | 0 | 1 |

$\Rightarrow \mathbb{Z}_3 \cong A_3$.

**28.** $f(e) = e'$, $e' \in f(H)$, $a' \cdot b' = f(a) \cdot f(b) = f(ab) \in f(H)$, $a \cdot a^{-1} = e$, $f(a) \cdot f(a^{-1}) = f(aa^{-1}) = f(e) = e'$...

**29.** $\mathrm{id}H$, $(12)H$, $(13)H$, $(14)H$, $(23)H$ in $(34)H$.

**30.** (a.) $H = \{0, 4, 8, 12, 16, 20\}$, $1 + H = \{1, 5, 9, 13, 17, 21\}$, $2 + H = \{2, 6, 10, 14, 18, 22\}$, $3 + H = \{3, 7, 11, 15, 19, 23\}$. (b.) $H = (23)H = \{\mathrm{id}, (23)\}$, $(12)H = (123)H = \{(12), (123)\}$, $(13)H = (132)H = \{(13), (132)\}$.

**31.** (a) $S_3 \leq S_4$, $S_3 = \{(1), (12), (13), (23), (123), (132)\}$. (b) Obstajajo 4 grupe reda 6. (c) $H = S_3$. Levi odseki so: $(1)H$, $(14)H$, $(24)H$, $(34)H$.

**32.** Uporabi Lagrange-ov izrek. Če je $a \in G$ potem $|a|$ deli $|G|$. Če je $|a| = 2$ potem... Če je $|a| = 4$ potem $a^2 \cdot a^2 = e$... Če je $|a| = 8$ potem $a^4 \cdot a^4 = e$...

**33.** (a) $\circ$ je asocijativna binarna operacija, $\mathrm{id}(x) = x \; \forall x \in [0, 1]$ je nevtralni element, za vsak element obstaja inverz.

(b) $\mathrm{id} \in T \Rightarrow T \neq \emptyset$;
$\forall \alpha, \beta \in T \; (\alpha\beta)(0) = 0$;
$\mathrm{id}(0) = 0 \Rightarrow (\alpha^{-1}\alpha)(0) = 0 \Rightarrow \alpha^{-1}(\alpha(0)) = 0 \Rightarrow \alpha^{-1}(0) = 0 \Rightarrow \alpha^{-1} \in T$.

(c) Naj bo $f : [0, 1] \Rightarrow [0, 1]$ bijekcija t.d. $f(0) = 1$. Potem $fT \subseteq \{\sigma \in S_{[0,1]} \mid \sigma(0) = 1\}$ in $\{\sigma \in S_{[0,1]} \mid \sigma(0) = 1\} \subseteq fT$...

(d) $[S_{[0,1]} : T] = \infty$.

**34.** (a)

| $+$ | $(0,0)$ | $(0,1)$ | $(1,0)$ | $(1,1)$ | $(2,0)$ | $(2,1)$ | $(3,0)$ | $(3,1)$ |
|---|---|---|---|---|---|---|---|---|
| $(0,0)$ | $(0,0)$ | $(0,1)$ | $(1,0)$ | $(1,1)$ | $(2,0)$ | $(2,1)$ | $(3,0)$ | $(3,1)$ |
| $(0,1)$ | $(0,1)$ | $(0,0)$ | $(1,1)$ | $(1,0)$ | $(2,1)$ | $(2,0)$ | $(3,1)$ | $(3,0)$ |
| $(1,0)$ | $(1,0)$ | $(1,1)$ | $(2,0)$ | $(2,1)$ | $(3,0)$ | $(3,1)$ | $(0,0)$ | $(0,1)$ |
| $(1,1)$ | $(1,1)$ | $(1,0)$ | $(2,1)$ | $(2,0)$ | $(3,1)$ | $(3,0)$ | $(0,1)$ | $(0,0)$ |
| $(2,0)$ | $(2,0)$ | $(2,1)$ | $(3,0)$ | $(3,1)$ | $(0,0)$ | $(0,1)$ | $(1,0)$ | $(1,1)$ |
| $(2,1)$ | $(2,1)$ | $(2,0)$ | $(3,1)$ | $(3,0)$ | $(0,1)$ | $(0,0)$ | $(1,1)$ | $(1,0)$ |
| $(3,0)$ | $(3,0)$ | $(3,1)$ | $(0,0)$ | $(0,1)$ | $(1,0)$ | $(1,1)$ | $(2,0)$ | $(2,1)$ |
| $(3,1)$ | $(3,1)$ | $(3,0)$ | $(0,1)$ | $(0,0)$ | $(1,1)$ | $(1,0)$ | $(2,1)$ | $(2,0)$ |

(b) $\langle(1,0)\rangle = \langle(3,0)\rangle = \{(0,0), (1,0), (2,0), (3,0)\}$, $\langle(1,1)\rangle = \langle(3,1)\rangle = \{(0,0), (1,1), (2,0), (3,1)\}$, $\langle(0,1), (2,0)\rangle = \langle(0,1), (2,1)\rangle = \{(0,0), (0,1), (2,0), (2,1)\}$. (c) $H = \{(0,0), (1,1), (2,0), (3,1)\}$, $(0,1) + H = \{(0,1), (1,0), (2,1), (3,0)\}$.

**35.** $\mathbb{Z}_3 = \{0, 1, 2\}$, $|0| = 1$, $|1| = 3$, $|2| = 3$; $\mathbb{Z}_4 = \{0, 1, 2, 3\}$, $|0| = 1$, $|1| = 4$, $|2| = 2$, $|3| = 4$; $U(9) = \{1, 2, 4, 5, 7, 8\}$, $|1| = 1$, $|2| = 6$, $|4| = 3$, $|5| = 6$, $|7| = 3$, $|8| = 2$; $\forall (g_1, g_2, g_3) \in \mathbb{Z}_3 \times \mathbb{Z}_4 \times U(9)$ imamo $12 = |(g_1, g_2, g_3)| = \mathrm{lcm}(|g_1|, |g_2|, |g_3|)$ če in samo če $(|g_1|, |g_2|, |g_3|) \in \{(1, 4, 3), (1, 4, 6), (3, 4, 1), (3, 4, 2), (3, 4, 3), (3, 4, 6)\}$... 32 elementa

**36.** (a.) Vsi desni odseki podgrupe $H$ v grupi $U(20)$ so $\{1, 9\}$, $\{3, 7\}$, $\{11, 19\}$ in $\{13, 17\}$. (b.) $U(20)/H = \{1H, 3H, 11H, 13H\}$.

| $\cdot$ | $1H$ | $3H$ | $11H$ | $13H$ |
|---|---|---|---|---|
| $1H$ | $1H$ | $3H$ | $11H$ | $13H$ |
| $3H$ | $3H$ | $1H$ | $13H$ | $11H$ |
| $11H$ | $11H$ | $13H$ | $1H$ | $3H$ |
| $13H$ | $13H$ | $11H$ | $3H$ | $1H$ |

(c.) Vse podgrupe grupe $U(20)/H$ so $\{1H\}$, $\{1H, 3H\}$, $\{1H, 11H\}$, $\{1H, 13H\}$ in $U(20)/H$.

**37.**

| $\cdot$ | $H$ | $8H$ | $18H$ | $27H$ |
|---|---|---|---|---|
| $H$ | $H$ | $8H$ | $18H$ | $27H$ |
| $8H$ | $8H$ | $27H$ | $H$ | $18H$ |
| $18H$ | $18H$ | $H$ | $27H$ | $8H$ |
| $27H$ | $27H$ | $18H$ | $8H$ | $H$ |

; (b) $|8\langle 16\rangle| = 4$.

**38.** (a) $\{0,4,8\}, \{1,5,9\}, \{2,6,10\}, \{3,7,11\}$,

| $+$ | $\langle 4\rangle$ | $1+\langle 4\rangle$ | $2+\langle 4\rangle$ | $3+\langle 4\rangle$ |
|---|---|---|---|---|
| $\langle 4\rangle$ | $\langle 4\rangle$ | $1+\langle 4\rangle$ | $2+\langle 4\rangle$ | $3+\langle 4\rangle$ |
| $1+\langle 4\rangle$ | $1+\langle 4\rangle$ | $2+\langle 4\rangle$ | $3+\langle 4\rangle$ | $\langle 4\rangle$ |
| $2+\langle 4\rangle$ | $2+\langle 4\rangle$ | $3+\langle 4\rangle$ | $\langle 4\rangle$ | $1+\langle 4\rangle$ |
| $3+\langle 4\rangle$ | $3+\langle 4\rangle$ | $\langle 4\rangle$ | $1+\langle 4\rangle$ | $2+\langle 4\rangle$ |

(b) Naj bo $\varphi(1) = a$.
$12 = 1+1+...+1 = 0$, $\varphi(0) = \varphi(12) = \varphi(1+...+1) = \varphi(1)+...+\varphi(1) = 12a = 0$. Če je $a = 1$, potem $\varphi(j) = j$ je homomorfizem.

**39.** $\langle 3\rangle = \{0,3,6,9,12,15,18,21\}$, $|\langle 3\rangle| = 8$, $[\mathbb{Z}_{24} : \langle 3\rangle] = 3$.
$\langle(2,3)\rangle = \{(0,0),(2,3)\}$, $|\langle(2,3)\rangle| = 2$, $[\mathbb{Z}_4 \times \mathbb{Z}_6 : \langle(2,3)\rangle] = 12$.

| $+$ | $\langle 3\rangle$ | $1+\langle 3\rangle$ | $2+\langle 3\rangle$ |
|---|---|---|---|
| $\langle 3\rangle$ | $\langle 3\rangle$ | $1+\langle 3\rangle$ | $2+\langle 3\rangle$ |
| $1+\langle 3\rangle$ | $1+\langle 3\rangle$ | $2+\langle 3\rangle$ | $\langle 3\rangle$ |
| $2+\langle 3\rangle$ | $2+\langle 3\rangle$ | $\langle 3\rangle$ | $1+\langle 3\rangle$ |

**40.** (a) 11 deli 77, $\exists a$ t.d. $|a| = 11$, $|\langle a\rangle| = 11$, $H := \langle a\rangle$.
Če je $|K| = 11$ in $H \neq K$ potem $|H \cap K| = 1$, $7 = |G| \geq |HK| = 121$, protislovje.
Obstaja natanko ena grupa reda 11. $\forall g \in G$, $gHg^{-1}$ je podgrupa reda 11,... $\Rightarrow H \lhd G$.

(b) $|H| = p$, p je praštevilo $\Rightarrow H$ je abelska.
$|K| = 4 \Rightarrow$ bodisi $K \cong \mathbb{Z}_4$ ali $K \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \Rightarrow K$ je abelska.
$g_1g_2 = (h_1k_1)(h_2k_2) = ... = (h_2h_1)(k_1k_2) = ... = (h_2k_2)(h_1k_1) = g_2g_1 \qquad \Rightarrow \qquad G$ je abelska.

**41.** Obstaja 6 različnih homomorfizema, $\phi : G \to \mathbb{Z}_6$, $2^k \to ka$ za $a \in \{0,1,2,3,4,5,6\}$.

**42.** $\phi_1(x) = 0$, $\forall x \in \mathbb{Z}_9$; $\qquad \phi_2(x) = 2x \bmod 3$, $\forall x \in \mathbb{Z}_9$.

**43.** (a) $\{1\}$, $\{1,9\}$ in $U(10)$. (b) $Z(U(10)) = U(10)$. (c) Obstajajo 4 homomorfizma.
$\phi : U(10) \longrightarrow \mathbb{Z}_8$, $\phi(3^k) = ka$, kje je $a \in \{0,2,4,6\}$.

**44.** Homomorfizmi so

| $x$ | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| $\varphi_1(x)$ | (0,0) | (0,0) | (0,0) | (0,0) |
| $\varphi_2(x)$ | (0,0) | (0,1) | (0,0) | (0,1) |
| $\varphi_3(x)$ | (0,0) | (1,0) | (0,0) | (1,0) |
| $\varphi_4(x)$ | (0,0) | (1,1) | (0,0) | (1,1) |

**45.** Če je $\phi : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ definirana z $\phi(a,b) = 7a - 2b$ potem je $\phi$ homomorfizem, $\phi(\mathbb{Z} \times \mathbb{Z}) = \mathbb{Z}$ in $\ker\phi = \langle(2,7)\rangle$...

**46.** $zHz^{-1} = z\{1,-1\}z^{-1} = H$; Definirajmo $\phi : G \to G$ t.d. $\phi(z) = z^2$. Potem za $\forall x \in G$ $\phi(x) \in G$, $\phi$ je homomorfizem, $\phi(G) = G$ in $\ker(\phi) = H$. Zdaj uporabimo prvi izrek o izomorfizmu.

**47.** $\langle -1\rangle = \{1,-1\}$, $\{x \in \mathbb{R}^* : |x| = 1\} = \{1,-1\}$.
Naj bo $\phi : \mathbb{R}^* \longrightarrow \mathbb{R}^+$ definiran s $x \longrightarrow |x|$. Potem je $\phi$ homomorfizem grup, $\ker(\phi) = \langle -1\rangle$ in $\phi(\mathbb{R}^*) = \mathbb{R}^+$...

**48.** (a.) $0 * (x,y) = (x,y)$, $(r+s)*(x,y) = r*(s*(x,y))$. (b.) $G_T = \{(x+ry, y) : r \in \mathbb{R}\}$, premica skozi točko T vzporedna s x-osjo. (c.) $G_T = \{0\}$. (d.) $5 + G_H = \{5\}$.

**49.** $G1 = G2 = G3 = \{1,2,3\}$, $G4 = G5 = \{4,5\}$, $G6 = \{6\}$, $G7 = G8 = \{7,8\}$;
$G_1 = G_2 = G_3 = G_4 = G_5 = \langle(78)\rangle$, $G_6 = G$, $G_7 = G_8 = \langle(123)(45)\rangle$.

**50.** $|H| = \frac{1}{3}|Gx||G_x|$, $|H| \leq |Hx||G_x|$. Delovanje podgrupe $H$ na množici $X$ ima lahko od 6 do 18 orbit.

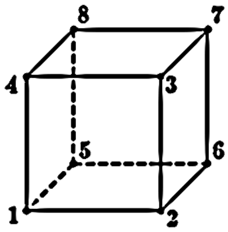
**51.** (a) $X = \square ABCD$, $G = D_4$, $Gx = \{A,B,C,D\}$, $G_x = \{R_0, D'\}$. (b) $Gx = \{1,2,3,4\} = X$, $G_x = \{id, (123), (132)\}$. (c) $Gx = \mathbb{R}^2 \backslash \{(0,0)^\top\}$,

$$G_x = \left\{ \begin{pmatrix} t & \frac{1}{2}(1-t) \\ 2-2s & s \end{pmatrix} : s,t \in \mathbb{R},\ s+t-1 \neq 0 \right\}.$$

**52.** $G = D_3 = \{id, \rho, \rho^2, \sigma, \sigma\rho, \sigma\rho^2\}$, $GA = \{A, B, C\} = X$, $G_A = \{id, \sigma\}$, $G_B = \{id, \sigma\rho\}$, $G_C = \{id, \sigma\rho^2\}$.

**53.** $G = D_5$, $H = \{(1), (25)(34)\}$, $\alpha = (14)(23)$, $G1 = \{1, 2, 3, 4, 5\}$, $\beta = (25)(34)$, $H2 = \{2, 5\}$, $H_2 = \{(1)\}$...

**54.** Če so $\{1, 2, 3, 4, 5, 6, 7, 8\}$ ogljišč kocke potem




$$\mathcal{O}_1 = \{(1), (254)(368), (245)(386), (25)(38), (36)(45), (24)(68)\}.$$

Če so $\{v_1, v_2, v_3, v_4, v_5, v_6, v_7, v_8\}$ ogljišč kocke potem $|\mathcal{O}| = |\mathcal{O}v_1| \cdot |\mathcal{O}_{v_1}| = 8|\mathcal{O}_{v_1}|$, $|\mathcal{O}_{v_1}| = |\mathcal{O}_{v_1}v_2| \cdot |\mathcal{O}_{v_1v_2}| = 3|\mathcal{O}_{v_1v_2}|$, $|\mathcal{O}_{v_1v_2}| = |\mathcal{O}_{v_1v_2}v_4| \cdot |\mathcal{O}_{v_1v_2v_4}| = 2|\mathcal{O}_{v_1v_2v_4}|$,...

**55.** (a) Orbite delovanj grup $G$ je $X$; orbite delovanj grup $H$ je $X$; orbite delovanj grup $K$ so $\{1\}$, $\{2, 6\}$, $\{3, 5\}$ in $\{4\}$; orbite delovanj grup $L$ so $\{1, 6\}$, $\{2, 5\}$ in $\{3, 4\}$.

(b) H in K sta tranzitivna, K in L nista.

(c) Vse štiri grupe so zvesta.

**56.** $|\mathcal{O}| = |\mathcal{O}1| \cdot |\mathcal{O}_1| = 4|\mathcal{O}_1|$, $\quad |\mathcal{O}_1| = |\mathcal{O}_12| \cdot |\mathcal{O}_{12}| = 3|\mathcal{O}_{12}|$, $\quad |\mathcal{O}_{12}| = |\mathcal{O}_{12}3| \cdot \mathcal{O}_{123} = 2 \cdot 1$ $\Rightarrow |\mathcal{O}| = 24 \Rightarrow |\mathcal{O}_1| = 6$,

$$\mathcal{O}_1 = \left\{\begin{pmatrix}1 & 2 & 3 & 4\\ 1 & 2 & 3 & 4\end{pmatrix}, \begin{pmatrix}1 & 2 & 3 & 4\\ 1 & 2 & 4 & 3\end{pmatrix}, \begin{pmatrix}1 & 2 & 3 & 4\\ 1 & 3 & 2 & 4\end{pmatrix}, \begin{pmatrix}1 & 2 & 3 & 4\\ 1 & 3 & 4 & 2\end{pmatrix}, \begin{pmatrix}1 & 2 & 3 & 4\\ 1 & 4 & 2 & 3\end{pmatrix}, \begin{pmatrix}1 & 2 & 3 & 4\\ 1 & 4 & 3 & 2\end{pmatrix}\right\}.$$

**57.** (a.) Vse edinke grupe $G$ so $\{1\}$, $\{1, -1\}$, $\{1, -1, i, -i\}$, $\{1, -1, j, -j\}$, $\{1, -1, k, -k\}$ in $\{1, -1, i, -i, j, -j, k, -k\}$. (b.) $Z(G) = \{1, -1\}$. (c.) $N(j) = \{1, -1, j, -j\}$, $N(-k) = \{1, -1, k, -k\}$.

**58.** (a.) $\langle 1 \rangle = \{1\}$, $\langle a \rangle = \{1, a, e, f\}$, $\langle e \rangle = \{1, e\}$, $\langle f \rangle = \{1, a, e, f\}$, $\langle b \rangle = \langle c \rangle = \langle d \rangle = \langle g \rangle = G$. (b.) $|1| = 1$, $|e| = 2$, $|a| = |f| = 4$, $|b| = |c| = |d| = |g| = 8$. (c.) $Z(G) = G$. (d.) $N(a) = N(g) = G$.

**59.** $D_{10} = \{R_0, R_{36}, R_{36}^2, R_{36}^3, R_{36}^4, R_{36}^5, R_{36}^6, R_{36}^7, R_{36}^8, R_{36}^9, F, R_{36}F, R_{36}^2F, R_{36}^3F, R_{36}^4F, R_{36}^5F, R_{36}^6F, R_{36}^7F, R_{36}^8F, R_{36}^9F, \}$, $|D_{10}| = 20$. Vse Sylowe 2-podgrupe grupe $D_{10}$ so $\{R_0, R_{36}^5, F, R_{36}^5F\}$, $\{R_0, R_{36}^5, R_{36}F, R_{36}^6F\}$, $\{R_0, R_{36}^2F, F, R_{36}^7F\}$, $\{R_0, R_{36}^3F, F, R_{36}^8F\}$ in $\{R_0, R_{36}^4F, F, R_{36}^9F\}$.

**60.** $992 = 2^5 \cdot 31$, $n_2 \in \{1, 31\}$, $n_{31} \in \{1, 2^5\}$...

**61.** Sylowe 2-podgrupe grupe $G$ so $\{I, A\}$, $\{I, B\}$, $\{I, ABA\}$. Sylowe 3-podgrupe grupe $G$ so $\{I, AB, BA\}$.

**62.** $|G| = 3087 = 3^2 \cdot 7^3$; $1 + 3m$ deli $|G|$ za $m \in \{0, 2, 16, 114\}$;... $1 + 7m$ deli $|G|$ za $m = 0$;...

**63.** (b) Naj bo $G$ dana grupa, $|G| = 63$. Lagrangeov izrek $\Rightarrow$ če je $a \in G$ potem $|a| \in \{1, 3, 7, 9, 21, 63\}$. Prvo moramo pokazati, da $G \backslash \{e\}$ ima najmanjše en element, ki ni reda 7...

**64.** $|G| = 15 = 3 \cdot 5$,
Cauchijev izrek za abelske grupe $\Rightarrow \exists a, b \in G$, $a \neq e$, $b \neq e$, $|a| = 3$, $|b| = 5$...
Naj bo $c = ab$. Potem $|c| \notin \{1, 3, 5\}$...
$|c| = 15 \Rightarrow G = \langle c \rangle$.

**65.** $|G| = 2^3 \cdot 3 \cdot 7$, $|G| = 7 \cdot 24$, $\gcd(7, 24) = 1 \Rightarrow$ obstaja najmanj ena podgrupa $H$ reda 7, $H$ je Sylowa 7 podgrupa.

$|G| = 7 \cdot 24$, $\gcd(7, 24) = 1 \Rightarrow$ število Sylowih 7-podgrup je oblike $1 + 7m$, $1 + 7m$ deli $168 \Rightarrow$ ... število Sylowih 7-podgrup je $8 \Rightarrow$ obstaja $7 + 7 \cdot 6 = 49$ elementov reda 7.

Več na `http://osebje.famnit.upr.si/~penjic/`