

# Algebra I — Cvičení

Podle následující sbírky probíhalo cvičení na PřF v semestru Jaro 2003. Příklady jsou rozděleny na ty, které jsme dělali na cvičení (označeno **C**), úlohy na kterých lze procvičovat probranou látku (**P**), doplňující úlohy, které přesahují sylaby předmětu nebo jsou obtížnější (**D**) a konečně zadání příkladů ze zápočtových testů (**Z**).

Podstatná část příkladů je převzata od kolegů, jmenovitě doc. Kučery, doc. Poláka a Mgr. Kunce, s kterými jsem dříve při přípravě cvičení spolupracoval.

Veškeré připomínky, opravy a komentáře jsou vítány na adrese [klima@math.muni.cz](mailto:klima@math.muni.cz).

Ondřej Klíma

Verze květen 2003.

## Cvičení 1

**C11** Rozhodněte, zda daný grupoid je pologrupa, zda obsahuje (levý, pravý) neutrální prvek, (levý, pravý) nulový prvek, zda je to grupa a zda je operace komutativní.

- 1) Celá čísla s operací sčítání.
- 2) Reálná čísla s operací násobení.
- 3) Celá čísla s operací odečítání.
- 4) Přirozená čísla s operací největší společný dělitel.

**C12** Pro dané množiny matic typu 2 krát 2 nad reálnými čísly rozhodněte zda je sčítání, resp. násobení, matic operací na této množině. Pokud se jedná o operaci, zjistěte, zda je operace asociativní či komutativní, zda obsahuje neutrální prvek, a zda se jedná o grupu.

- 1) Množina všech matic nad celými čísly.
- 2) Množina všech matic nad racionálními čísly.
- 3) Množina všech regulárních matic nad racionálními čísly.
- 4) Množina všech matic s nulou v levém dolním rohu a s jedničkami na diagonále.
- 5) Množina všech regulárních matic nad celými čísly.

**C13** Pro množinu  $X$  značíme  $P(X)$  množinu všech podmnožin množiny  $X$ . Pro následující operace určete, zda grupoid  $P(X)$  je pologrupou, zda je operace komutativní a nalezněte neutrální prvek.

- 1) Průnik.
- 2) Sjednocení.
- 3) Množinový rozdíl. ( $Y \setminus Z = \{x \in Y \mid x \notin Z\}$ )
- 4) Symetrický rozdíl. ( $Y \div Z = (Y \setminus Z) \cup (Z \setminus Y)$ )

**C14** Určete, zda operace na tříprvkové množině  $\{a, b, c\}$  daná tabulkou je komutativní, asociativní a zda má neutrální prvek.

1) 

$\circ$	$a$	$b$	$c$
$a$	$b$	$a$	$a$
$b$	$a$	$b$	$a$
$c$	$a$	$a$	$a$

2) 

$\circ$	$a$	$b$	$c$
$a$	$b$	$a$	$a$
$b$	$a$	$b$	$c$
$c$	$a$	$c$	$a$

3) 

$\circ$	$a$	$b$	$c$
$a$	$a$	$a$	$a$
$b$	$b$	$b$	$b$
$c$	$c$	$c$	$c$

**C15** Prvek  $e$  pologrupy  $(G, \cdot)$  se nazývá idempotent jestliže  $e \cdot e = e$ . Ukažte, že každá grupa obsahuje právě jeden idempotent.

**P11** Pro množinu  $X$  označme  $T(X)$  množinu všech transformací, tj.  $T(X) = \{f : X \rightarrow X\}$ , a  $PT(X)$  množinu všech parciálních transformací, tj.  $PT(X) = \{f : Y \rightarrow X \mid Y \subseteq X\}$ . Ukažte, že  $(T(X), \circ)$  a  $(PT(X), \circ)$ , kde  $\circ$  je operace skládání zobrazení, jsou monoidy. Pro danou množinu transformací (resp. parciálních transformací) určete, zda společně s operací skládání zobrazení tvoří grupoid, pologrupu, či grupu. (Pozor: odpovědi se mohou lišit v případech kdy  $X$  je jednoprvková, resp. konečná, resp. nekonečná.)

- 1) Všechna injektivní zobrazení.
- 2) Všechna surjektivní zobrazení.
- 3) Všechna bijektivní zobrazení.

**P12** Doplňte následující tabulku operace na tříprvkové množině tak, aby výsledný grupoid byl pologrupou.

$\circ$	$a$	$b$	$c$
$a$	$b$	$a$	$c$
$b$			
$c$			

**P13** Následující tabulku je možno jediným způsobem doplnit na tabulku operace  $\cdot$  v pologrupě  $(S, \cdot)$ , kde  $S = \{a, b, c, d, e, f\}$ .

$\cdot$	$a$	$b$	$c$	$d$	$e$	$f$
$a$	$a$	$b$	$c$	$d$		$f$
$b$	$b$	$e$	$c$	$d$	$b$	$f$
$c$	$c$	$c$	$f$	$c$	$c$	$d$
$d$	$d$		$c$	$d$	$d$	$f$
$e$	$e$	$b$	$c$	$d$	$e$	$f$
$f$	$f$	$f$	$d$	$f$	$f$	$c$

1. Určete, kterému prvku z množiny  $S$  se rovná  $d \cdot b$ , resp.  $a \cdot e$ , v pologrupě  $(S, \cdot)$ .
2. Určete všechny idempotenty.
3. Vypište všechny pravé neutrální prvky.
4. Vypište všechny levé nulové prvky.
5. Určete všechny podmnožiny  $G \subseteq S$  takové, že  $(G, \cdot)$  je grupa.
6. Lze původní tabulku doplnit tak, aby byla operace  $\cdot$  v grupoidu  $(S, \cdot)$  komutativní?

**D11** V pologrupě matic  $(Mat_2(\mathbb{Q}), \cdot)$  typu 2 krát 2 nad racionálními čísly s operací násobení matic určete všechny idempotenty. Pro každý idempotent  $e$  určete některou netriviální podmnožinu, které společně s operací  $\cdot$  tvoří grupu s neutrálním prvkem  $e$ .

**D12 = D31**

## Cvičení 2

**Z2-A** Uvažme na množině  $R = \{\rho \subseteq X \times X\}$  všech relací na množině  $X$  operaci  $\circ$  definovanou vztahem

$$\rho \circ \pi = \{(x, y) \in X \times X \mid \exists z \in X : (x, z) \in \pi, (z, y) \in \rho\}.$$

Ukažte, že  $\circ$  je asociativní. Určete neutrální prvek. Rozhodněte zda  $(S, \circ)$ , kde  $S = \{\rho \in R \mid \rho \text{ symetrická}\}$ , je grupoid.

**Z2-B** Uvažme na množině  $R = \{\rho \subseteq X \times X\}$  všech relací na množině  $X$  operaci  $\square$  definovanou vztahem

$$\rho \square \pi = \{(x, y) \in X \times X \mid \exists z \in X : (x, z) \in \rho, (z, y) \in \pi\}.$$

Ukažte, že  $\square$  je asociativní. Určete nulový prvek. Rozhodněte zda  $(T, \square)$ , kde  $T = \{\rho \in R \mid \rho \text{ tranzitivní}\}$ , je grupoid.

**Z2-C** Uvažujme množinu  $\mathcal{O} = \{(a, b) \mid a, b \in \mathbb{R}, a < b\} \cup \{\emptyset\}$  otevřených intervalů reálných čísel. Ukažte, že průnik  $\cap$  je operací na této množině. Rozhodněte, zda je operace  $\cap$  asociativní a zda existuje neutrální a nulový prvek. Je  $(\mathcal{O}, \cap)$  grupa?

**Z2-D** Uvažujme množinu  $\mathcal{N} = \{(a, b) \mid a, b \in \mathbb{R}, a < 0 < b\}$  otevřených intervalů reálných čísel. Ukažte, že sjednocení  $\cup$  je operací na této množině. Rozhodněte, zda je operace  $\cup$  asociativní a zda existuje neutrální a nulový prvek. Je  $(\mathcal{N}, \cup)$  grupa?

**C21+P21** Rozhodněte, zda daný grupoid  $(G, \circ)$  je grupa.

- 1)  $G$  je množina nenulových racionálních čísel a operace  $\circ$  je dána předpisem  $x \circ y = |x \cdot y|$ .
- 2)  $G$  je interval  $\langle 0, 1 \rangle$  a operace  $\circ$  je dána předpisem  $x \circ y = x + y - [x + y]$ , kde  $[z]$  značí celou část z čísla  $z$ , tj. největší celé číslo menší nebo rovno  $z$ .
- 3)  $G$  je množina celých čísel a operace  $\circ$  je dána předpisem  $x \circ y = x + (-1)^x y$ .
- 4)  $G$  je množina uspořádaných dvojic reálných čísel, přičemž první z nich není 0 a operace  $\circ$  je dána předpisem  $(x, y) \circ (u, v) = (xu, xv + y)$ .
- 5)  $G$  je množina komplexních čísel, jejichž reálná i imaginární část je celočíselná a operace  $\circ$  je sčítání komplexních čísel.

**C22+D21**

- 1) Dokažte, že v libovolné grupě platí tzv. Zákony o krácení ( $ab = ac \implies b = c, ba = ca \implies b = c$ ).
- 2) Dokažte, že konečná pologrupa v které platí zákony o krácení je grupa.
- 3) Udejte příklad nekonečné pologrupy, která není grupou, ale platí v ní zákony o krácení.
- 4) Udejte příklad tříprvkového grupoidu, který není grupou, ale platí v něm zákony o krácení. Ukažte, že grupoid není pologrupou.
- 5) Udejte příklad pětiprvkového grupoidu s neutrálním prvkem, který není grupou, ale platí v něm zákony o krácení. Ukažte, že grupoid není pologrupou.

**C23** Určete kolik je dvouprvkových, resp. tříprvkových, resp. čtyřprvkových grup.

**P22** Dokažte, že v konečné grupě o sudém počtu prvků existuje prvek, který je inverzní k sobě samému a není to neutrální prvek.

**P23** Doplňte tabulku operace  $*$  tak, aby vznikla grupa  $(\{a, b, c\}, *)$ :

$\circ$	$a$	$b$	$c$
$a$			
$b$	$c$	$a$	
$c$			

**P24** Nechť  $(G, \circ)$  je grupa a  $a$  nějaký její pevně zvolený prvek. Dokažte, že potom  $(G, \square)$  je také grupa, kde operace  $\square$  je definována předpisem  $g \square h = g \circ a \circ h$ .

**D22** Dokažte, že grupy jsou právě ty pologrupy pro něž platí:

$$\forall a, b \exists x, y : ax = b, ya = b.$$

**D23** Určete všechny dvouprvkové pologrupy (až na izomorfismus, tj. přejmenování prvků).

### Cvičení 3

**Z3-A** 1) Nechť  $S = \{a, b\}$  a pro operaci  $\cdot$  platí:  $a \cdot a = b$ ,  $b \cdot b = a$ . Ukažte, že  $(S, \cdot)$  není pologrupa.

2) Napište multiplikační tabulku grupy  $(G, \cdot)$ , kde  $G = \{e, f, g\}$ , víte-li, že  $e \cdot f = g$ .

**Z3-C** 1) Nechť  $S = \{a, b, c\}$  a pro operaci  $\cdot$  platí:  $a \cdot a = c$ ,  $c \cdot c = c$ . Ukažte, že  $(S, \cdot)$  není grupa.

2) Napište multiplikační tabulku komutativní pologrupy  $(M, \cdot)$ , kde  $M = \{e, f, g\}$ , víte-li, že  $e \cdot f = g$  a že každý prvek je idempotentem.

**D31** Dokažte, že v každé konečné pologrupě existuje idempotent.

**C24+C31** Nechť

$$s = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 4 & 7 & 2 & 1 & 9 & 8 & 6 & 5 \end{pmatrix}, t = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 5 & 2 & 1 & 4 & 3 & 8 & 7 & 6 & 9 \end{pmatrix}, u = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 8 & 1 & 4 & 6 & 3 & 7 & 5 & 9 & 2 \end{pmatrix}.$$

- 1) Rozložte permutace  $s, t, u$  na součin nezávislých cyklů.
- 2) Spočítejte součiny  $s \circ t$ ,  $t \circ s$ ,  $s \circ u \circ t$ . Použijte jak "dvojřádkový" zápis, tak rozklad na nezávislé cykly.
- 3) Spočítejte  $s^3, s^{20}, t^{53}, t^{103}, u^{211}$ .
- 4) Určete inverzní prvky  $s^{-1}, t^{-1}, u^{-1}$ .
- 5) Spočítejte permutace  $(s^{120} \circ t^{-3})^{17} \circ u^{23}$  a  $(u^{-23} \circ s)^{134} \circ t^4$ .
- 6) Permutace  $s, t, u$  rozložte na součin transpozic a určete jejich paritu.

**C32** Napište permutace  $f = (2, 3, 4, 5) \circ (1, 3, 6, 8)$  a  $g = (1, 4, 6) \circ (2, 7, 4, 8, 3) \circ (1, 5)$  jako součin 10 transpozic.

**P31** Dokažte že permutace  $(s^3 \circ t^{-17})^{18} \circ s^{10}$  je sudá permutace pro libovolné permutace  $s, t \in \mathbb{S}_9$ .

**P33** Určete všechny permutace  $a$  z grupy  $\mathbb{S}_8$  takové, že  $a^2 = (1, 2, 3)(4, 5, 6)$ . Podobně určete  $b$  takové, že  $b^4 = (1, 2, 3, 4, 5, 6, 7)$ .

**P32** Určete všechny permutace  $f$  z grupy  $\mathbb{S}_8$  takové, že  $f^3 = (1, 2)(3, 4)(5, 6)$ .

**P33**

- 1) Ukažte, že libovolnou permutaci v  $\mathbb{S}_n$  lze rozložit na součin transpozic tvaru  $(1, i)$ .
- 2) Ukažte, že libovolnou sudou permutaci v  $\mathbb{S}_n$  lze rozložit na součin cyklů tvaru  $(1, 2, i)$ .

**P34** Jestliže  $a$  je cyklus délky  $n$ , pak  $a^k = id$  právě když  $n$  dělí  $k$ . Pokud  $n$  nedělí  $k$  pak je  $a^k$  součinem  $d$  nezávislých cyklů délky  $\frac{n}{d}$ , kde  $d$  je největší společný dělitel  $n$  a  $k$ .

**D32** Ukažte, že libovolnou permutaci v  $\mathbb{S}_n$  lze rozložit na součin cyklů  $(1, 2)$  a  $(1, 2, \dots, n)$ .

**D33** Určete následující grupy symetrií (jako podmnožiny  $\mathbb{S}_n$ , pro vhodné  $n$ , nebo alespoň určete počty prvků).

- 1)  $\mathbb{D}_3$  grupa symetrií rovnostranného trojúhelníka,
- 2)  $\mathbb{D}_4$  grupa symetrií čtverce,
- 3)  $\mathbb{D}_n$  grupa symetrií pravidelného  $n$ -úhelníku (určete alespoň počet prvků),
- 4) grupa symetrií pravidelného čtyřstěnu.
- 5) \* grupa symetrií krychle.

**D34\*** Určete které prvky  $a \in \mathbb{S}_n$  lze psát ve tvaru  $b^2c^2$  pro vhodné  $b, c \in \mathbb{S}_n$ .

## Cvičení 4

**Z4-A** 1) Jsou dány permutace  $f, g \in \mathbb{S}_9$ . Platí  $f = (5, 8, 7, 6) \circ (1, 4, 2), g = (1, 5, 2, 6) \circ (2, 4, 7, 9, 5)$ . Zapište permutace  $f^{-1}, g^{21}, h = (f^{11} \circ g^{-3})^{20}$  ve tvaru součinu nezávislých cyklů.

Permutace  $f$  a  $g$  napište jako součin transpozic a určete paritu těchto permutací.

2) Určete pro která přirozená čísla  $n \in \mathbb{N}$  existuje permutace  $s \in \mathbb{S}_9$  taková, že  $s^n = (1, 2, 3)$ .

**Z4-B** 1) Jsou dány permutace  $f, g \in \mathbb{S}_9$ . Platí  $f = (8, 6, 7, 5) \circ (1, 4, 2), g = (1, 8, 2, 5) \circ (2, 4, 7, 9, 8)$ . Zapište permutace  $f^{-1}, g^{20}, h = (f^{11} \circ g^{-4})^{-20}$  ve tvaru součinu nezávislých cyklů.

Permutace  $f$  a  $g$  napište jako součin transpozic a určete paritu těchto permutací.

2) Určete pro která přirozená čísla  $n \in \mathbb{N}$  existuje permutace  $s \in \mathbb{S}_9$  taková, že  $s^n = (1, 2, 3, 4)$ .

**Z4-C** 1) Jsou dány permutace  $f, g \in \mathbb{S}_9$ . Platí  $f = (1, 7) \circ (2, 8) \circ (3, 5, 6, 4, 9), g = (3, 8, 4, 5, 7) \circ (1, 6, 9, 3, 4)$ . Zapište permutace  $f^{-1}, g^{10}, h = (f^9 \circ g^{-5})^{20}$  ve tvaru součinu nezávislých cyklů.

Permutace  $f$  a  $g$  napište jako součin transpozic a určete paritu těchto permutací.

2) Rozhodněte zda existuje permutace  $s \in \mathbb{S}_9$  taková, že  $(s \circ (1, 2, 3))^2 \circ (s \circ (2, 3, 4))^2 = (1, 2, 3, 4)$ . (Uveďte příklad nebo důkaz.)

**Z4-D** 1) Jsou dány permutace  $f, g \in \mathbb{S}_9$ . Platí  $f = (1, 7) \circ (2, 8) \circ (3, 5, 9, 4, 6), g = (1, 3, 2, 4, 5) \circ (3, 4, 7, 9, 6)$ . Zapište permutace  $f^{-1}, g^{27}, h = (f^9 \circ g^{-3})^{30}$  ve tvaru součinu nezávislých cyklů.

Permutace  $f$  a  $g$  napište jako součin transpozic a určete paritu těchto permutací.

2) Rozhodněte zda existuje permutace  $s \in \mathbb{S}_9$  taková, že  $s^2 \circ (1, 2) \circ s^2 = (1, 2) \circ s^2 \circ (1, 2)$ . (Uveďte příklad nebo důkaz.)

**C41+P41** Spočítejte 1)  $[4]_{15}^{-1} \in \mathbb{Z}_{15}$ , 2)  $[17]_{181}^{-1} \in \mathbb{Z}_{181}$ , 3)  $[49]_{226}^{-1} \in \mathbb{Z}_{226}$ , 4)  $[49]_{225}^{-1} \in \mathbb{Z}_{225}$ , 5)  $[125]_{1296}^{-1} \in \mathbb{Z}_{1296}$ .

**C42+P42** Spočítejte 1)  $[2^k + 1]_{2^{2k+1}}^{-1} \in \mathbb{Z}_{2^{2k+1}}$ , 2)  $[2^k - 1]_{2^{2k+1}}^{-1} \in \mathbb{Z}_{2^{2k+1}}$ , 3)  $[m^2 - m + 1]_{m^3 - 1}^{-1} \in \mathbb{Z}_{m^3 - 1}$ .

**C43+P43** Určete kolik prvků má grupa  $(\mathbb{Z}_n^*, \cdot)$  pro následující  $n$  a popište její multiplikativní tabulku.

1)  $n = 5$ , 2)  $n = 7$ , 3)  $n = 8$ .

**C44** Určete kolik prvků mají grupy  $(\mathbb{Z}_n^*, \cdot)$  pro následující  $n$ :

1)  $n = 24$ , 2)  $n = 306$ , 3)  $n = 5225$ .

**C45** Určete řád permutace  $(1, 2, 4, 5) \circ (3, 7, 8) \circ (6, 9)$  resp.  $(1, 2, 4, 5, 3, 6, 7, 9) \circ (3, 7, 8) \circ (6, 2, 9)$ .

**C46** Určete řád prvku  $[k]_n$  v  $(\mathbb{Z}_n, +)$ .

**C47** Určete řády všech prvků v  $(\mathbb{Z}_n^*, \cdot)$  pro  $n = 7, 8, 12, 13$ .

**P44** V  $GL_2(\mathbb{Z}_3)$  (grupa regulárních matic nad  $\mathbb{Z}_3$ ) určete řády prvků  $\begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}$  a  $\begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}$ .

**P45** Ukažte, že pro libovolné  $n > 2$  je  $\varphi(n)$  sudé číslo.

**P46** Určete všechna přirozená čísla  $m$ , pro která platí  $\varphi(m) = 18$ .

**D41** Určete všechna přirozená čísla  $n$  taková, že  $\varphi(n) \mid n$ .

## Cvičení 5

**Z5-A** 1) Určete  $[49]_{1000}^{-1} \in \mathbb{Z}_{1000}$ .

2) Určete řád prvku  $[4]_{35}$  v grupě  $\mathbb{Z}_{35}^*$ .

**Z5-C** 1) Určete  $[45]_{478}^{-1}$  v  $\mathbb{Z}_{478}$ .

2) Určete  $\varphi(1000)$ .

**C51+P51** Určete zbytek po dělení daných čísel číslem 17.

1)  $2^{50} + 3^{50} + 4^{50}$ , 2)  $5^{40} + 6^{40} + 7^{40} + 8^{40}$ , 3)  $4^{4^4} + 5^{5^5}$ , 4)  $13^{13^{13}} + 15^{15^{15}}$ .

**C52+P52** Určete zbytek po dělení čísla  $a^{9^9-3^{10}}$  číslem 44, pro  $a = 8, 9, 10, 11$ .

**P53** Ukažte, že číslo  $2^{60} + 7^{30}$  je dělitelné číslem 13.

**D51** Dokažte, že pro libovolné  $n \in \mathbb{N}$  je číslo  $2^{2^{2n+1}} + 3$  číslo složené.

**D52** Dokažte Čínskou zbytkovou větu: Nechť je dáno  $k \in \mathbb{N}$  a  $k$ -tice  $m_1, \dots, m_k$  po dvou nesoudělných přirozených čísel. Pak pro libovolnou  $k$ -tici  $c_1, \dots, c_k$  přirozených čísel existuje  $x \in \mathbb{N}$  takové, že  $x \equiv c_i \pmod{m_i}$  pro  $i = 1, \dots, k$ . Navíc je toto  $x$  určeno jednoznačně mod  $m_1 \cdot \dots \cdot m_k$ ; přesněji, všechna tato čísla dávají stejný zbytek po dělení číslem  $m_1 \cdot \dots \cdot m_k$ .

**C53+P54** Ukažte, že podmnožina kladných reálných čísel, resp. kladných racionálních čísel, resp.  $\mathbb{Q}(\sqrt{3}) = \{a + b\sqrt{3} \mid a, b \in \mathbb{Q}\}$  je podgrupa grupy  $(\mathbb{R}^*, \cdot)$ .

**C54** Popište všechny podgrupy grupy  $(\mathbb{Z}, +)$ .

**C55** Popište všechny podgrupy grupy  $(\mathbb{Z}_{10}, +)$ .

**P55** Popište všechny podgrupy grupy  $(\mathbb{Z}_n, +)$ .

**P56** Ukažte, že množina sudých permutací tvoří podgrupu grupy  $\mathbb{S}_n$  pro libovolné  $n \in \mathbb{N}$ .

**D53** Popište všechny podgrupy grupy symetrií  $\mathbb{D}_n$  pro  $n = 3, 4$ .

## Cvičení 6

**Z6** Určete zbytek po dělení čísla **A**  $8^{8^8} + 11^{11^{11}}$ , **B**  $7^{7^7} + 12^{12^{12}}$  číslem 20, resp. **C**  $8^{8^8} + 13^{13^{13}}$ , **D**  $7^{7^7} + 21^{21^{21}}$  číslem 18.

**C61** Popište svaz podgrup  $\mathbb{S}_3$  a  $\mathbb{A}_4$ .

**C62+P61** Určete podgrupu  $\mathbb{S}_8$  generovanou množinou  $X$ :

1)  $X = \{(4, 5, 2, 1) \circ (4, 6, 3, 1, 5, 2), (4, 5, 2, 1) \circ (4, 5, 6) \circ (2, 1, 3)\}$ ,

2)  $X = \{(1, 5, 8) \circ (1, 4, 2, 5) \circ (1, 5, 2), (1, 2, 6, 4, 8, 5) \circ (1, 4, 6, 2)\}$ ,

3)  $X = \{(1, 8, 2, 3, 5) \circ (1, 2, 6, 7, 8), (4, 7, 6, 2) \circ (2, 4, 8)\}$ ,

4)  $X = \{(1, 2)(3, 4), (2, 3)(4, 5)\}$ .

5)  $X = \{(2, 4, 6), (4, 7, 2), (3, 2, 4)\}$ . **D**

**D61** Určete podgrupu  $\mathbb{S}_n$  generovanou množinou  $\{(1, 2), (1, 2, 3, \dots, n)\}$ .

**C63** V  $(\mathbb{Z}_{60}, +)$  určete podgrupu generovanou množinou  $\{[6]_{60}, [15]_{60}\}$ .

**P62** V  $GL_2(\mathbb{Z}_2)$  (grupa regulárních matic řádu 2 nad  $\mathbb{Z}_2$ ) určete podgrupu generovanou množinou  $X$ :

1)  $X = \left\{ \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\}$ , 2)  $X = \left\{ \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \right\}$ , 3)  $X = \left\{ \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\}$ .

A podobně v  $GL_2(\mathbb{Z}_3)$  určete podgrupu generovanou množinou

$$Y = \left\{ \begin{pmatrix} 2 & 1 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 2 & 2 \end{pmatrix} \right\} \cdot (\mathbf{D})$$

**P63** V grupě  $(\mathbb{R}, +)$ , resp.  $(\mathbb{R}^*, \cdot)$ , určete podgrupu generovanou prvkem  $\sqrt[3]{2}$ .

**P64** V grupě  $(\mathbb{C}^*, \cdot)$  určete podgrupu generovanou prvkem  $\frac{\sqrt{2}}{2} + i \frac{\sqrt{2}}{2}$ .

**D62** Určete všechny konečné podgrupy grupy  $(\mathbb{R}^*, \cdot)$ , resp.  $(\mathbb{C}^*, \cdot)$ .

**P65** V grupě z příkladu **P21-3**) určete podgrupu generovanou množinou prvků a)  $\{3\}$ , b)  $\{6\}$ , c)  $\{3, 7\}$ .

**D63** Určete všechny podgrupy grupy z příkladu **P21-3**).

## Cvičení 7

**Z7** Určete podgrupu grupy  $\mathbb{S}_8$  generovanou množinou  $\mathbf{C} = \{(1, 8)(2, 3)(4, 5), (1, 3, 5, 8, 2, 4)(6, 7)\}$ , resp.  $\mathbf{A} = \{(1, 2, 3), (1, 2)(3, 5)\}$ . Kolik má tato podgrupa prvků?

**C71** Nechť je dána grupa  $G$  a její dvě podgrupy  $H$  a  $K$ . Dokažte, že

$$\langle H \cup K \rangle = \{a_1 b_1 \dots a_n b_n \mid n \in \mathbb{N}, a_i \in H, b_i \in K\}.$$

**C72** Dokažte, že  $(\mathbb{Z}_7^*, \cdot)$  je izomorfní s  $(\mathbb{Z}_6, +)$  a  $(\mathbb{Z}_8^*, \cdot)$  je izomorfní s  $(\mathbb{Z}_2, +) \times (\mathbb{Z}_2, +)$ . (Ukažte, že předpis  $f([a]_6) = [3]_7^a$  definuje izomorfismus  $f : (\mathbb{Z}_6, +) \rightarrow (\mathbb{Z}_7^*, \cdot)$ .)

**P71** U každého z následujících předpisů (kde  $a, b \in \mathbb{Z}$ ,  $p, q \in \mathbb{Z} \setminus \{0\}$ ) rozhodněte zda zadává zobrazení. Pokud ano, rozhodněte, zda se jedná o homomorfismus či dokonce izomorfismus grup.

$$\alpha, \bar{\alpha} : (\mathbb{Z}_4, +) \times (\mathbb{Z}_3, +) \rightarrow (\mathbb{Z}_{12}, +)$$

$$\alpha([a]_4, [b]_3) = [6a + 4b]_{12}$$

$$\bar{\alpha}([a]_4, [b]_3) = [a - b]_{12}$$

$$\beta : (\mathbb{Z}_3^*, \cdot) \times (\mathbb{Z}_5, +) \rightarrow (\mathbb{Z}_5, +)$$

$$\beta([a]_3, [b]_5) = [b^{|a|}]_5$$

$$\gamma : (\mathbb{Q} \setminus \{0\}, \cdot) \rightarrow (\mathbb{Q} \setminus \{0\}, \cdot)$$

$$\gamma(p/q) = q/p$$

$$\delta : (\mathbb{Z}_{15}, +) \rightarrow (\mathbb{Z}_5, +) \times (\mathbb{Z}_3, +)$$

$$\delta([a]_{15}) = ([a]_5, [a]_3)$$

$$\epsilon, \bar{\epsilon} : (\mathbb{Z}_3, +) \rightarrow (\mathbb{A}_4, \circ)$$

$$\epsilon([a]_3) = (1, 2, 4) \circ (1, 3, 2)^a \circ (1, 4, 2)$$

$$\bar{\epsilon}([a]_3) = (1, 2)(3, 4) \circ (1, 2, 3)^a$$

**C73** Dokažte, že předpis  $f([a]_{20}) = (1, 2, 3, 4, 5)^a$  definuje homomorfismus  $f : (\mathbb{Z}_{20}, +) \rightarrow (\mathbb{S}_7, \circ)$ .

**C74+P72** Pro libovolnou grupu  $(G, \cdot)$  označme  $\text{Aut}(G) = \{f : G \rightarrow G \mid f \text{ izomorfismus}\}$  množinu všech automorfismů grupy  $G$  a  $\text{End}(G) = \{f : G \rightarrow G \mid f \text{ homomorfismus}\}$  množinu všech endomorfismů grupy  $G$ .

i) Ukažte, že  $(\text{End}(G), \circ)$ , kde  $\circ$  je skládání zobrazení, je monoid a  $\text{Aut}(G)$  je podmnožina invertibilních prvků, tj.  $(\text{Aut}(G), \circ)$  je grupa.

- ii) Dokažte, že pro libovolný prvek  $a \in G$  je zobrazení  $\rho_a$  automorfismus grupy  $G$ , kde  $\rho_a : G \rightarrow G$  je definováno vztahem  $\rho_a(x) = axa^{-1}$ . (Hovoříme o vnitřních automorfismech.)
- iii) Ukažte, že množina všech vnitřních automorfismů  $\text{Inn}(G) = \{\rho_a \mid a \in G\}$  je podgrupa grupy  $(\text{Aut}(G), \circ)$ .
- iv) Dokažte, že zobrazení  $\rho : G \rightarrow \text{Aut}(G)$  dané předpisem  $\rho(a) = \rho_a$  je homomorfismus grup.

**C75** Popište všechny endomorfismy a automorfismy grupy  $(\mathbb{Z}, +)$ . Určete čemu je izomorfní monoid  $\text{End}(\mathbb{Z})$  a grupa  $\text{Aut}(\mathbb{Z})$ .

**P73** Popište všechny endomorfismy a automorfismy grupy  $(\mathbb{Z}_n, +)$ . Určete čemu je izomorfní monoid  $\text{End}(\mathbb{Z}_n)$  a grupa  $\text{Aut}(\mathbb{Z}_n)$ .

**D71** Popište všechny homomorfismy z grupy  $(\mathbb{Z}_n, +)$  do grupy  $(\mathbb{Z}_k, +)$ .

**P74** Nechť  $f : G \rightarrow H$  je izomorfismus grup. Ukažte, že řády prvků  $a$  a  $f(a)$  jsou stejné. Co lze říci o řádech prvků  $a$  a  $f(a)$  v případě, že  $f : G \rightarrow H$  je homomorfismus.

**P75** Dokažte, že zobrazení  $f : G \rightarrow G$  definované předpisem  $f(x) = x^{-1}$  je izomorfismus právě tehdy, když grupa  $G$  je komutativní.

**P76** Dokažte, že pro libovolné grupy  $G$  a  $H$  jsou grupy  $G \times H$  a  $H \times G$  izomorfní.

**D72** Nechť  $X = \{1, \dots, n\}$ . Ukažte, že grupa  $(P(X), \div)$  z příkladu **C13-4** je izomorfní grupě  $\mathbb{Z}_2^n$ . ( $\mathbb{Z}_2^n$  je součin  $n$  kopií grupy  $\mathbb{Z}_2$ .)

**P77** Uvažme grupu  $(G, \cdot)$  matic typu 3 krát 3 nad  $\mathbb{Z}$ , které jsou v horním trojúhelníkovém tvaru s jedničkami na hlavní diagonále, tj.

$$G = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \mid a, b, c \in \mathbb{Z} \right\},$$

kde  $\cdot$  je násobení matic. Definujme nyní zobrazení  $f : (G, \cdot) \rightarrow (\mathbb{Z}, +)$ , které matici

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}$$

přiřadí číslo  $a - c$ . Dokažte, že zobrazení  $f$  je homomorfismus grup.

## Cvičení 8

**Z8** U následujících předpisů (kde  $a, b \in \mathbb{Z}$ ,  $s \in \mathbb{S}_6$ ) rozhodněte zda zadávají zobrazení. Pokud ano, rozhodněte, zda se jedná o homomorfismus či dokonce izomorfismus grup. Odpovědi zdůvodněte!

**A**  $\alpha : (\mathbb{Z}_2, +) \times (\mathbb{Z}_5, +) \rightarrow (\mathbb{Z}_{10}, +)$ ,  $\alpha([a]_2, [b]_5) = [a + b]_{10}$ ;  $\beta : (\mathbb{S}_6, \circ) \rightarrow (\mathbb{S}_6, \circ)$ ,  $\beta(s) = (1, 2) \circ s \circ (1, 2)$ .

**B**  $\alpha : (\mathbb{Z}_2, +) \times (\mathbb{Z}_5, +) \rightarrow (\mathbb{Z}_{10}, +)$ ,  $\alpha([a]_2, [b]_5) = [5a + 2b]_{10}$ ;  $\beta : (\mathbb{S}_6, \circ) \rightarrow (\mathbb{S}_6, \circ)$ ,  $\beta(s) = s^2$ .

**C**  $\alpha : (\mathbb{Z}_4, +) \rightarrow (\mathbb{C}^*, \cdot)$ ,  $\alpha([a]_4) = i^a$ ;  $\beta : (\mathbb{Z}, +) \rightarrow (\mathbb{Z}_3, +)$ ,  $\beta(a) = [a]_3$ .

**D**  $\alpha : (\mathbb{Z}_5, +) \rightarrow (\mathbb{C}^*, \cdot)$ ,  $\alpha([a]_5) = i^a$ ;  $\beta : (\mathbb{Z}, +) \rightarrow (\mathbb{Z}_2, +)$ ,  $\beta(a) = [a]_2$ .

**C81+P81** Určete jádra a obrazy homomorfismů z příkladů **Z8**.

**P82** Buď  $\alpha$  homomorfismus grupy  $(\mathbb{Z}_{30}, +)$  do grupy  $(\mathbb{Z}_{20}, +)$  definovaný předpisem  $\alpha([a]_{30}) = [6a]_{20}$ . Dále nechť  $\beta$  je homomorfismus grupy  $(\mathbb{Z}_{20}, +)$  do grupy  $(\mathbb{S}_5, \circ)$  definovaný předpisem  $\beta([b]_{20}) = (1, 2, 3, 4, 5)^b$ . Určete jádra homomorfismů  $\alpha$ ,  $\beta$  a  $\beta \circ \alpha$ .

**P83** Určete jádro homomorfismu  $f$  z příkladu **P77**. Ověřte, že se jedná o normální podgrupu grupy  $G$ . (Uvědomte si, že jádro je vždy normální podgrupa.)



**C82** Popište všechny normální podgrupy grup  $(\mathbb{S}_3, \circ)$  a  $(\mathbb{A}_4, \circ)$ . Ukažte, že  $\mathbb{A}_n$  je normální podgrupa grupy  $\mathbb{S}_n$  pro libovolné  $n \in \mathbb{N}$ . (Povšimněte si, že existuje normální podgrupa  $N$  grupy  $H$  — normální podgrupy grupy  $(\mathbb{A}_4, \circ)$  — která není normální podgrupou  $(\mathbb{A}_4, \circ)$ .)

**D81** Necht'  $n \in \mathbb{N}$ ,  $n > 4$ . Dokažte, že  $\mathbb{A}_n$  nemá vlastní normální podgrupy a že je to jediná netriviální normální podgrupa  $\mathbb{S}_n$ .

**C83+P84** Uvažme grupu  $(\text{GL}_2(\mathbb{Q}), \cdot)$  regulárních matic dva krát dva nad racionálními čísly. Necht'  $G$  je podgrupa všech matic, které jsou v horním trojúhelníkovém tvaru s jedničkou v pravém dolním rohu,  $H$  je podgrupa všech diagonálních matic a  $N$  její podgrupa, kde čísla na diagonále jsou si rovna.

$$G = \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \mid a \in \mathbb{Q}^*, b \in \mathbb{Q} \right\}, \quad H = \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \mid a, b \in \mathbb{Q}^* \right\}, \quad N = \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \mid a \in \mathbb{Q}^* \right\}.$$

Určete, zda jsou tyto podgrupy normální.

**P85** V příkladech **P62—65** určete normální podgrupu generovanou danou množinou.

**D82** Které podgrupy z příkladu **D63** jsou normální?

**P86** Dokažte, že  $\text{Inn}(G)$  v **P72-iii** je normální podgrupa.

**C84** Buď dána grupa  $(G, \circ)$  nekonstantních lineárních zobrazení reálných čísel

$$G = \{f : \mathbb{R} \rightarrow \mathbb{R} \mid f(x) = ax + b, a \in \mathbb{R}^*, b \in \mathbb{R}\}$$

s operací skládání zobrazení  $\circ$ . Uvažme v této grupě dvě podgrupy:

$$T = \{f : \mathbb{R} \rightarrow \mathbb{R} \mid f(x) = ax, a \in \mathbb{R}^*\},$$

$$S = \{f : \mathbb{R} \rightarrow \mathbb{R} \mid f(x) = x + b, b \in \mathbb{R}\}.$$

Která z nich je normální podgrupou grupy  $(G, \circ)$ ? Popište u obou pravý i levý rozklad.

**P87** Popište levý rozklad grupy  $(\mathbb{A}_4, \circ)$  sudých permutací na množině  $\{1, 2, 3, 4\}$  podle podgrupy generované permutací  $(2, 1, 4)$ .

**P88** Určete počet levých tříd grupy  $(\mathbb{Z}, +) \times (\mathbb{Z}, +)$  podle podgrupy  $H = \{(m, n) ; 6 \mid (m - 2n)\}$ .

**P89** Necht' konečná grupa  $(G, \cdot)$  má sudý počet prvků  $2n$  a  $H$  je její  $n$  prvková podgrupa. Dokažte, že  $H$  je normální podgrupa grupy  $(G, \cdot)$ .

## Cvičení 9

**Z9-A** Označme následující podgrupy grupy  $(\mathbb{S}_6, \circ)$ :  $G = \{f \in \mathbb{S}_6 \mid f \text{ sudá}\}$  a  $H = \{f \in G \mid f(3) = 3\}$ , tj.  $H \subset G \subset \mathbb{S}_6$ . Rozdodněte zda

a)  $H$  je normální podgrupa grupy  $(G, \circ)$ ;

b)  $H$  je normální podgrupa grupy  $(\mathbb{S}_6, \circ)$ ;

c)  $G$  je normální podgrupa grupy  $(\mathbb{S}_6, \circ)$ .

Odpovědi zdůvodněte!

**Z9-B** Označme následující podgrupy grupy  $(\mathbb{S}_5, \circ)$ :  $G = \{f \in \mathbb{S}_5 \mid f(3) = 3\}$  a  $H = \{f \in G \mid f \text{ sudá}\}$ , tj.  $H \subset G \subset \mathbb{S}_5$ . Rozdodněte zda

a)  $H$  je normální podgrupa grupy  $(G, \circ)$ ;

b)  $H$  je normální podgrupa grupy  $(\mathbb{S}_5, \circ)$ ;

c)  $G$  je normální podgrupa grupy  $(\mathbb{S}_5, \circ)$ .

Odpovědi zdůvodněte!

**Z9-C** Buď dána následující grupa  $(G, \cdot)$  matic ve speciálním tvaru s operací násobení matic a její podgrupa  $H$ :

$$G = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mid a, c \in \mathbb{R}^*, b \in \mathbb{R} \right\}, \quad H = \left\{ \begin{pmatrix} a & 0 \\ 0 & c \end{pmatrix} \mid a, c \in \mathbb{R}^* \right\}.$$

Dokažte, že  $H$  je podgrupa grupy  $(G, \cdot)$ . Rozhodněte, zda  $H$  je normální podgrupa  $(G, \cdot)$ . Odpověď zdůvodněte!

**Z9-D** Buď dána následující grupa  $(G, \cdot)$  matic ve speciálním tvaru s operací násobení matic a její podgrupa  $H$ :

$$G = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mid a, c \in \mathbb{R}^*, b \in \mathbb{R} \right\}, \quad H = \left\{ \begin{pmatrix} 1 & b \\ 0 & c \end{pmatrix} \mid c \in \mathbb{R}^*, b \in \mathbb{R} \right\}.$$

Dokažte, že  $H$  je podgrupa grupy  $(G, \cdot)$ . Rozhodněte, zda  $H$  je normální podgrupa  $(G, \cdot)$ .

**C91** Určete faktorgrupu z příkladu **C84**.

**C92** Faktorizujte grupu  $\mathbb{Z}$  podgrupou  $k\mathbb{Z} = \{ka \mid a \in \mathbb{Z}\}$ .

**C93** Faktorizujte grupu  $\mathbb{Z}_n$  podgrupou  $k\mathbb{Z}_n = \{kz \mid z \in \mathbb{Z}_n\} = \{[kz]_n \mid z \in \mathbb{Z}\}$ , kde  $k$  dělí  $n$ .

**P91** Čemu je izomorfní faktorgrupa regulárních matic nad reálnými čísly podle podgrupy matic jejichž determinant je roven 1. ( $GL_n(\mathbb{R})/SL_n(\mathbb{R}) \cong ?$ )

**P92** Víme, že množina

$$G = \left\{ \begin{pmatrix} \varepsilon & a \\ 0 & 1 \end{pmatrix} \mid \varepsilon \in \{1, -1\}, a \in \mathbb{Z} \right\}$$

společně s operací násobení matic tvoří grupu  $(G, \cdot)$ . Označme

$$H = \left\{ \begin{pmatrix} 1 & 2b \\ 0 & 1 \end{pmatrix} \mid b \in \mathbb{Z} \right\}$$

podmnožinu  $G$ . Ukažte, že  $H$  je normální podgrupa grupy  $G$ . Popište rozklad  $G/H$ , tj. charakterizujte kdy dvě matice  $\begin{pmatrix} \varepsilon & a \\ 0 & 1 \end{pmatrix}$  a  $\begin{pmatrix} \varepsilon' & a' \\ 0 & 1 \end{pmatrix}$  náleží do stejné třídy rozkladu. Určete počet tříd rozkladu  $G/H$ . Určete, které grupě  $(K, \cdot)$  je izomorfní faktorgrupa  $G/H$ , tj. popište grupu  $(K, \cdot)$  a definujte vhodné zobrazení  $\alpha : G \rightarrow K$  pro něž dokažte, že  $\alpha$  je surjektivní homomorfismus grup, jehož jádrem je  $H$ .

**P93** Uvažme množiny reálných čísel  $G = \{15^p 5^q \mid p, q \in \mathbb{Z}\}$  a  $H = \{3^r \mid r \in \mathbb{Z}\}$  a operaci  $\cdot$  (násobení reálných čísel). Zřejmě  $(G, \cdot)$  je grupa.

1. Ukažte, že  $H$  je normální podgrupa grupy  $(G, \cdot)$ .
2. Pro  $p, \bar{p}, q, \bar{q} \in \mathbb{Z}$  doplňte podmínku  $(\dots)$  tak, aby platilo:

$$15^p 5^q \text{ a } 15^{\bar{p}} 5^{\bar{q}} \text{ náleží do stejné třídy rozkladu } G/H \iff \dots$$

3. Určete, které grupě je izomorfní faktorgrupa  $G/H$ , tj. popište grupu  $(K, \cdot)$  a definujte vhodné zobrazení  $\alpha : G \rightarrow K$ , pro něž dokažte, že  $\alpha$  je surjektivní homomorfismus grup, jehož jádrem je  $H$ .

**P94** Faktorizujte aditivní grupu komplexních čísel podgrupou všech reálných čísel. ( $(\mathbb{C}, +)/\mathbb{R} \cong ?$ )

**P95** Nechť je dána grupa matic

$$G = \left\{ \begin{pmatrix} a & 0 \\ b & c \end{pmatrix} \mid a, c \in \mathbb{Q}^*, b \in \mathbb{Q} \right\}$$

s operací násobení. Dokažte, že podgrupa

$$H = \left\{ \begin{pmatrix} a & 0 \\ b & c \end{pmatrix} \mid a, b, c \in \mathbb{Q}, a, c > 0 \right\}$$

je normální a určete faktorgrupu.

**D91** V příkladu **C82** jsme spočítali jednu netriviální normální podgrupu v  $\mathbb{S}_4$  resp.  $\mathbb{A}_4$ , označme ji  $\mathbb{V}_4$ . Spočtete příslušné faktorgrupy. ( $\mathbb{S}_4/\mathbb{V}_4 \cong ?$ ,  $\mathbb{A}_4/\mathbb{V}_4 \cong ?$ )

**D92** Dokažte, že až na izomorfismus existují pouze dvě  $2p$  prvkové grupy a popište je. (Zde  $p$  je prvočíslo.)

**D93** Určete faktorgrupu z příkladu **P84**.

## Doplňující příklady z teorie grup (svátek 1.5.)

**S1** Dokažte, že následující grupa matic  $(G, \cdot)$  je izomorfní grupě  $(\mathbb{C}^*, \cdot)$ .

$$G = \left\{ \begin{pmatrix} x & y \\ y & x \end{pmatrix} \mid x, y \in \mathbb{R}, x^2 + y^2 > 0 \right\}$$

**S2** Nechť je dána grupa  $G$  a její dvě podgrupy  $H$  a  $K$ . Definujme nyní podmnožinu  $HK$  grupy  $G$ :

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

Dokažte, že pokud je  $K$  normální podgrupa grupy  $G$ , potom je podmnožina  $HK$  podgrupou grupy  $G$ . (Srovnej s příkladem **C71**.) Dále dokažte, že pokud jsou obě podgrupy  $H$  i  $K$  normální, potom je normální i podgrupa  $HK$ .

**S3** Centrum grupy  $(G, \cdot)$  definujeme takto:  $\text{Cent}(G) = \{x \in G \mid \forall y \in G : x \cdot y = y \cdot x\}$ . Dokažte, že centrum libovolné grupy  $(G, \cdot)$  je normální podgrupa této grupy a ukažte, že faktorgrupa je izomorfní grupě  $\text{Inn}(G)$ . Dále určete centrum

- grupy  $(\mathbb{S}_3, \circ)$  všech permutací tříprvkové množiny;
- grupy  $(\mathbb{Z}_7, +)$  zbytkových tříd modulo 7;
- grupy  $(\text{GL}_2(\mathbb{Q}), \cdot)$  regulárních matic  $2 \times 2$  nad racionálním

### S4

- Ukažte, že libovolný automorfismu grupy  $\mathbb{S}_n$  zachovává paritu permutace.
- Určete centrum grupy  $\mathbb{S}_n$  pro libovolné  $n \geq 2$ .
- Dokažte, že pro  $n > 2$  je grupa  $\text{Inn}(\mathbb{S}_n)$  izomorfní grupě  $\mathbb{S}_n$ .
- Dokažte, že  $\text{Aut}(\mathbb{S}_n) \cong \mathbb{S}_n$  pro  $n = 3, 4, 5$ .

**S5** Nechť  $(G, \cdot)$  je grupa,  $n \in \mathbb{N}$  a předpokládejme, že grupa  $G$  obsahuje jedinný prvek řádu  $n$  (označme jej  $a$ ). Dokažte, že tento prvek komutuje s libovolným prvkem grupy  $G$ , tj.  $xa = ax$  pro libovolné  $x \in G$ .

**S6** Nechť  $G$  je grupa a označme  $G'$  podgrupu generovanou množinou prvků tvaru  $[x, y] = x^{-1}y^{-1}xy$ , tj.

$$G' = \{[x_1, y_1][x_2, y_2] \dots [x_n, y_n] \mid n \in \mathbb{N}, x_i, y_i \in G\}.$$

- Dokažte, že  $G'$  je normální podgrupa grupy  $G$ .
- Ukažte, že faktorgrupa  $G/G'$  je komutativní grupa.
- Ukažte, že  $G/G'$  je "největší" komutativní faktorgrupa grupy  $G$ , tj. ukažte, že pokud  $H$  je normální podgrupa grupy  $G$  taková, že  $G/H$  je komutativní grupa, potom  $G' \subseteq H$ .
- Určete "největší" komutativní faktorgrupu pro grupu

$$H = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mid a, c \in \mathbb{Q}^*, b \in \mathbb{Q} \right\}.$$

Totéž pro  $GL_2(\mathbb{Q})$ .

## Burnsidovo lemma (svátek 8.5.)

V následujících příkladech nerozlišujeme mezi obarveními, která mohou na sebe přejít nějakou rotací.

**B1** Kolika způsoby můžeme obarvit hrany krychle  $n$  barvami?

**B2** Kolika způsoby můžeme obarvit vrcholy krychle  $n$  barvami?

**B3** Na každou ze stěn krychle máme nakreslit jednu úhlopříčku. Kolik různých krychlí můžeme získat?

**B4** Na každou ze stěn krychle máme nakreslit šipku mířící diagonálně od jednoho vrcholu k protějším. Kolik různých krychlí můžeme získat?

**B5** Jak se změní odpověď v 3. a 4., máme-li na libovolně mnoha stěnách povoleno také žádnou úhlopříčku (šipku) nekreslit?

**B6** Kolika způsoby můžeme obarvit stěny krychle, mají-li být dvě bílé, dvě černé a dvě červené?

**B7** Kolika způsoby můžeme obarvit strany pravidelného 15-úhelníka  $n$  barvami? Zde nerozlišujeme mezi obarveními, která mohou na sebe přejít nějakou rotací nebo osovou symetrií.

## Cvičení 10

**Z10** Uvažujme normální podgrupu grupy  $(G, +) = (\mathbb{Z}, +) \times (\mathbb{Z}, +)$  definovanou takto:

$$(A) : H = \{(a, b) \in \mathbb{Z} \times \mathbb{Z}; 2 \mid a, 3 \mid b\},$$

$$(B) : H = \{(a, b) \in \mathbb{Z} \times \mathbb{Z}; 5 \mid a, 2 \mid b\},$$

$$(C) : H = \{(a, b) \in \mathbb{Z} \times \mathbb{Z}; 7 \mid 2a + 3b\},$$

$$(D) : H = \{(a, b) \in \mathbb{Z} \times \mathbb{Z}; 5 \mid a + 4b\}.$$

Určete, které grupě je izomorfní faktorgrupa  $G/H$ , tj. popište grupu  $(K, \cdot)$  a definujte vhodné zobrazení  $\alpha : G \rightarrow K$ , pro něž dokažte, že  $\alpha$  je surjektivní homomorfismus grup, jehož jádrem je  $H$ .

**C101** Nalezňte všechny racionální kořeny polynomu  $12x^6 + 8x^5 - 85x^4 + 15x^3 + 55x^2 + x - 6$ .

**P101** Nalezňte všechny racionální kořeny polynomu  $4x^7 - 16x^6 + x^5 + 55x^4 - 35x^3 - 38x^2 + 12x + 8$ .

**P102** Určete takové  $a \in \mathbb{C}$ , pro něž má polynom  $f = 2x^6 - x^5 - 11x^4 - x^3 + ax^2 + 2ax + 8 \in \mathbb{C}[x]$  kořen 2. Pro toto  $a$  určete všechny racionální kořeny polynomu  $f$  včetně násobností.

**C102** Zjistěte násobnost kořene  $-1$  polynomu  $x^5 - ax^2 - ax + 1 \in \mathbb{C}[x]$  v závislosti na parametru  $a \in \mathbb{C}$ .

**C103** Najděte největší společný dělitel a koeficienty do Bezoutovy rovnosti pro dvojici polynomů  $f = x^4 + 1$  a  $g = x^3 - 1$ .

**C104** Nalezňte všechny aspoň dvojnásobné kořeny polynomu  $x^6 + 6x^5 + 15x^4 + 20x^3 + 12x^2 - 4$ .

**P103** Nalezňte všechny aspoň dvojnásobné kořeny polynomu  $x^4 - 2x^3 - x^2 + 2x + 1 \in \mathbb{C}[x]$ .

**P104** O polynomu  $g = x^4 + 2ix^3 + x^2 + 2ix + 1 \in \mathbb{C}[x]$  víte, že má dvojnásobný kořen. Rozložte polynom  $g$  na lineární faktory nad  $\mathbb{C}$ .

**P105** Zjistěte nejdříve všechny racionální kořeny a posléze všechny vícenásobné kořeny polynomů  $f = 12x^7 - 56x^6 + 115x^5 - 141x^4 + 103x^3 - 35x^2 - 3x + 9$  a  $g = 8x^7 - 44x^6 + 70x^5 - 17x^4 - 24x^3 + 10x^2 + 2x - 1$ .

## Cvičení 11

**Z11** Nalezňte všechny racionální kořeny polynomu

**A**  $4x^7 - 23x^5 + 17x^4 + 31x^3 - 49x^2 + 24x - 4$ ,

- B**  $2x^7 - 3x^6 - 20x^5 - x^4 + 66x^3 + 91x^2 + 48x + 9$ ,  
**C**  $4x^5 + 8x^4 - 27x^3 - 79x^2 - 56x - 12$ ,  
**D**  $4x^5 - 35x^3 + 15x^2 + 40x + 12$ .

**P111** Napište rozklady na součin ireducibilních polynomů nad  $\mathbb{C}$ ,  $\mathbb{R}$  resp.  $\mathbb{Q}$  pro všechny polynomy z příkladů Cvičení 10.

**C111** Uvažme následující množiny racionálních čísel:

$$A = \left\{ \frac{m}{p} \mid m, p \in \mathbb{Z}, 3 \nmid p \right\}, \quad B = \left\{ \frac{q}{3^n} \mid n \in \mathbb{N}, q \in \mathbb{Z} \right\}.$$

Rozhoděte, zda  $(A, +, \cdot)$  (resp.  $(B, +, \cdot)$ ), kde operace  $+$  a  $\cdot$  jsou obvyklé sčítání a násobení racionálních čísel, je okruh, případně obor integrity. Jde-li o okruh, charakterizujte jeho jednotky.

**C112** Nechť  $(R, +, \cdot)$  je komutativní okruh. Rozhodněte, zda je okruh i  $(R, +, \square)$ , kde  $\square$  je operace definovaná vztahem  $a \square b = a \cdot b + b \cdot a$  pro libovolné  $a, b \in R$ .

**C113** Určete, zda je okruh  $(\mathbb{Z}_2, +, \cdot) \times (\mathbb{Z}_3, +, \cdot)$  oborem integrity. Je izomorfní s okruhem  $(\mathbb{Z}_6, +, \cdot)$ ?

**C114** Určete všechny ireducibilní polynomy nad  $\mathbb{Z}_2$  stupně menšího než 5.

**P112** Určete všechny ireducibilní polynomy nad  $\mathbb{Z}_3$  stupně menšího než 4.

## Cvičení 12

**C121** Naleznete všechny kořeny polynomu  $x^5 + 5x^4 - x^2 - x + 3$  v  $\mathbb{Z}_7$ .

**C122** Rozložte polynom  $x^5 + 3x^3 + x + 3 \in \mathbb{Z}_5[x]$  na součin ireducibilních polynomů nad  $\mathbb{Z}_5$ .

**C123** Určete, který z polynomů  $f = x^5 + 3x^3 - 9x + 3 \in \mathbb{Z}[x]$  a  $g = x^4 + 4x^3 + 5x^2 - 3 \in \mathbb{Z}[x]$  je ireducibilní nad  $\mathbb{Z}$  a který lze rozložit na součin polynomů nižšího stupně. Napište rozklady polynomů  $f$  a  $g$  na ireducibilní faktory nad  $\mathbb{Z}$ .

**C124** Určete všechny kořeny polynomu  $f = x^7 - 4x^6 + 8x^5 - 7x^4 + 8x^2 - 8x + 4 \in \mathbb{C}[x]$ , víte-li, že má dvojnásobný kořen  $1 + i$ . Rozložte tento polynom na ireducibilní faktory nad  $\mathbb{Q}$ ,  $\mathbb{R}$ , resp.  $\mathbb{C}$ .

**P121** Mezi všemi normovanými polynomy s reálnými koeficienty, které mají jednoduchý kořen  $-\frac{1}{3}$  a dvojnásobný kořen  $3 + 2i$ , naleznete polynom nejmenšího stupně. Rozložte tento polynom na ireducibilní polynomy nad  $\mathbb{Q}$ ,  $\mathbb{R}$ , resp.  $\mathbb{C}$ .

**C125** Určete, které prvky náležejí podokruhu  $\mathbb{Z}[a]$  okruhu  $\mathbb{C}$  pro  $a = \sqrt{3}$ ,  $a = \sqrt[5]{2}$ ,  $a = i$ ,  $a = \cos \frac{2\pi}{3} + i \sin \frac{2\pi}{3} = \xi_3$ ,  $a = \cos \frac{2\pi}{7} + i \sin \frac{2\pi}{7} = \xi_7$ ,  $a = \pi$ .

**P122** Určete, které prvky náležejí podokruhu  $\mathbb{Z}[a]$  okruhu  $\mathbb{C}$  pro  $a = \sqrt{n}$ ,  $a = \sqrt[3]{n}$ ,  $a = i\sqrt{n}$ .

**P123** Uvažme zobrazení  $f : \mathbb{C} \rightarrow \mathbb{R}$  definované takto:  $f(a + bi) = a + b$  pro  $a, b \in \mathbb{R}$ . Rozhodněte, zda je  $f$  homomorfismus okruhu  $(\mathbb{C}, +, \cdot)$  do okruhu  $(\mathbb{R}, +, \cdot)$ .

**P124** Určete všechny čtveřice  $(a, b, c, d) \in \mathbb{R}^4$  takové, že předpis  $\alpha(r + si) = (ar + bs) + (cr + ds)i$ , pro  $r, s \in \mathbb{R}$ , definuje homomorfismus  $\alpha : \mathbb{C} \rightarrow \mathbb{C}$  okruhu  $\mathbb{C}$  do sebe. Pro které z nich se jedná o izomorfismus?

**P125** Buď  $\mathbb{Q}(\sqrt{3}) = \{a + b\sqrt{3} \mid a, b \in \mathbb{Q}\}$  podokruh okruhu  $(\mathbb{R}, +, \cdot)$ . Ukažte, že  $(\mathbb{Q}(\sqrt{3}), +, \cdot)$  je těleso. Dokažte, že libovolný okruhový homomorfismus  $\alpha : \mathbb{Q}(\sqrt{3}) \rightarrow \mathbb{C}$  je identický na množině racionálních čísel, tj.  $\forall r \in \mathbb{Q} : \alpha(r) = r$ . Popište všechny okruhové homomorfismy  $\alpha : \mathbb{Q}(\sqrt{3}) \rightarrow \mathbb{C}$ . Které z nich jsou izomorfismy?

# Návody, výsledky, poznámky

**P11** Složení injektivních (resp. surjektivních, resp. bijektivních) transformací je injektivní (resp. surjektivní, resp. bijektivní). Všechny množiny obsahují identitu a proto se jedná o monoidy. Pro konečnou množinu  $X$  jsou všechny tři množiny stejné a tvoří grupu. Pro nekonečnou množinu  $X$  tvoří grupu pouze bijekce. V případě parciálních transformací:  $X$  konečná množina - surjektivní a bijektivní transformace jsou permutace a jedná se o grupu, injektivní tvoří pouze monoid;  $X$  nekonečná množina - pouze monoid ve všech případech.

**P12** Doplnění  $ba = a$ ,  $bb = b$ ,  $cx = xc = c$  pro libovolné  $x$  je jediné možné.

**P13** 1)  $db=fc=fc=b$ , 2)  $ae=abb=bb=e$ , 3) a, 4) nejsou, 5)  $\{a\}$ ,  $\{e\}$ ,  $\{b, e\}$ ,  $\{d\}$ ,  $\{c, d, f\}$ , 6) ano - viz 1.

**Z2-A**

$$(\rho \circ \pi) \circ \sigma = \{(x, y) \mid \exists z \in X : (x, z) \in \sigma, (z, y) \in \rho \circ \pi\} = \{(x, y) \mid \exists z, u \in X : (x, z) \in \sigma, (z, u) \in \pi, (u, y) \in \rho\},$$

podobně

$$\rho \circ (\pi \circ \sigma) = \{(x, y) \mid \exists a \in X : (x, a) \in \pi \circ \sigma, (a, y) \in \rho\} = \{(x, y) \mid \exists a, b \in X : (x, b) \in \sigma, (b, a) \in \pi, (a, y) \in \rho\}$$

a rovnost je evidentní. Neutrálním prvkem je "identita"  $\{(x, x) \mid x \in X\}$ . Pro prázdnou a jednoprvkovou množinu je každá relace symetrická a tudíž jde o grupoid. Pokud obsahuje aspoň dva různé prvky  $a, b$ , pak pro  $\rho = \{(b, b)\}$ ,  $\pi = \{(a, b), (b, a)\}$  není relace  $\rho \circ \pi = \{(a, b)\}$  symetrická. Obecně tedy nejde o grupoid.

**Z2-B** Asociativita - viz A. Nulový prvek je "prázdná relace"  $\emptyset$ . Pokud  $|X| \leq 2$  je každá relace tranzitivní a jde tudíž o grupoid. Pokud množina  $X$  obsahuje aspoň tři různé prvky  $a, b, c$ , pak pro  $\rho = \{(a, a), (b, c)\}$ ,  $\pi = \{(a, b), (c, c)\}$  není relace  $\rho \circ \pi = \{(a, b), (b, c)\}$  tranzitivní. Obecně tedy nejde o grupoid.

**Z2-C, D** Operace jsou asociativní obecně, proto jsou asociativní i na daných množinách  $\mathcal{O}$ ,  $\mathcal{N}$ . Prvek  $\emptyset$  je nulový prvek v  $\mathcal{O}$  a neutrální v  $\mathcal{N}$ . Neutrální prvek v  $\mathcal{O}$  a nulový v  $\mathcal{N}$  neexistují. Grupy to nejsou.

**C21+P21** 1) Ne, 2) Ano, 3) Ano, 4) Ano, 5) Ano.

**P22** Uvědomte si, že podmnožina  $S = \{x \in G \mid x = x^{-1}\}$  má sudý počet prvků.

**P23** Z tabulky je vidět, že neutrální prvek je  $c$ .

**Z3-A** 1) Pokud  $ab = a$  pak  $a = bb = (aa)b = a(ab) = aa = b$  a pokud  $ab = b$  pak  $a = bb = (aa)b = a(ab) = ab = b$ . 2) Z  $ef = g$  plyne, že neutrální prvek je  $g$  a pak se už snadno doplní tabulka podle zákona o krácení.

**Z3-C** 1) V grupě je právě jeden idempotent a to neutrální prvek. Pokud by  $S$  byla grupa, pak  $c$  je neutrální prvek a vidíme, že po doplnění výsledků násobením prvkem  $c$  tabulku nelze doplnit dle zákona o krácení. 2) Víme, že  $ee = e$ ,  $ff = f$ ,  $gg = g$  (idempotenti). Dále  $eg = e(ef) = (ee)f = ef = g$ ,  $gf = (ef)f = e(ff) = ef$  a multiplikativní tabulku doplníme jednoznačně díky komutativitě.

**D31** Ukažte, že pro libovolný prvek  $s$  obsahuje (konečná!) množina  $\{s^k \mid k \in \mathbb{N}\}$  právě jeden idempotent.

**P31** Pro libovolnou permutaci  $f$  je  $f^{2n}$  sudá permutace pro libovolné  $n \in \mathbb{N}$ . Zadaná permutace je tudíž součinem dvou sudých permutací.

**P32** Popsanou vlastnost má permutace  $(1, 2) \circ (3, 4) \circ (5, 6)$  a potom 8 cyklů délky 6.

**P33** Využijeme faktu, že každou permutaci lze psát jako součin transpozic. Každou z nich lze potom rozepsat na součin  $(i, j) = (1, i)(1, j)(1, i)$ . Pokud je permutace sudá, pak se dle předchozího dá psát jako součin sudého počtu transpozic typu  $(1, i)$ . Tento součin rozdělíme po dvou a každou dvojici vyjádříme takto:  $(1, i)(1, j) = (1, j, i) = (1, 2, i)^2(1, 2, j)(1, 2, i)$ .

**D32** Označme  $c = (1, 2) \circ (1, 2, \dots, n) = (2, 3, \dots, n)$ . Potom  $(1, i) = c^{i-2}(1, 2)c^{n-i+1}$  a použijeme P33.

**D33** 1-3) skripta. 4)  $\mathbb{S}_4$  5) Grupa má 48 prvků. Její popis zkuste později. (Rozdělte symetrie na přímé, tj. ty které lze "fyzicky" provést (rotace, ...) a nepřímé, tj. ty které nelze provést (sředová souměrnost, ...) Popište grupu přímých symetrií a ukažte, že každá nepřímá lze uvažovat jako součin jednoznačně určené přímé symetrie a středové souměrnosti.)

**D34** Každý takový prvek je sudá permutace. Lze ukázat, že i naopak každou sudou permutaci lze psát v tomto tvaru. S cykly liché délky není žádná potíž a cykly sudé délky nejdříve rozložte na součin transpozice a cyklu liché délky.

**P45** Pro každé číslo  $n$  dělitelné lichým prvočíslem  $p$  je  $\varphi(n)$  dělitelné  $p-1$  a tudíž číslem sudým. Číslo, které není dělitelné lichým prvočíslem, je tvaru  $2^k$  pro  $k > 1$  a proto je  $\varphi(n)$  mocnina čísla 2.

**P46** Jsou to čísla 19, 27, 38, 54.

**D41**  $n = 2^x 3^y$ , pro  $x \in \mathbb{N}$ ,  $y \in \mathbb{N}_0$ .

**D51** Ukažte, že zadané číslo je dělitelné číslem 7.

**D52** Každé číslo  $x$ ,  $0 \leq x < m_1 \cdots m_k$  zadává  $k$ -tici zbytků  $(c_i)_{i=1}^k$  po dělení čísla  $m_i$ . Pokud si uvědomíme, že dvojice různých čísel  $x$  a  $y$  dává různou  $k$ -tici (neboť existuje  $m_i$  které nedělí číslo  $x - y$ ) dostaneme bijekci mezi těmito čísly a  $k$ -ticemi  $(c_i)_{i=1}^k$ , kde  $0 \leq c_i < m_i$ .

**D53**  $D_3$  má celkem 6 podgrup: triviální, 3 dvouprvkové (osová souměrnost a identita), 1 tříprvkovou (rotace) a 1 šestprvkovou (celé  $D_3$ ).

$D_4$  má celkem 10 podgrup: triviální, 5 dvouprvkových ( $4 \times$  osová souměrnost a identita, středová souměrnost a identita), 3 tříprvkové (rotace,  $2 \times$  kolmé osové souměrnosti, středová souměrnost a identita) a 1 osmiprvkovou (celé  $D_4$ )—napište si je též jako podgrupy  $S_4$ .

**P61** 2)  $\langle X \rangle = \langle \{(1, 8, 5), (2, 4)\} \rangle = \{(1, 8, 5)^a \circ (2, 4)^b \mid a = 0, 1, 2; b = 0, 1\}$  (6 prvků)

3)  $\langle X \rangle = \langle \{(1, 3, 5), (2, 6, 7), (4, 8)\} \rangle$  (18 prvků)

4) Pro  $a = (1, 2)(3, 4)$ ,  $b = (2, 3)(4, 5)$  máme  $ab = (1, 2, 4, 5, 3)$ , tedy  $(ab)^5 = \text{id}$ . Podgrupa  $\langle X \rangle = \{(ab)^i a^j \mid i = 0, 1, 2, 3, 4; j = 0, 1\}$ , kde  $b = (ab)^4 a$ , má 10 prvků. (Lze ji také popsat jako grupu pravidelného pětiúhelníka s vrcholy označenými po řadě 1,2,4,5 a 3.)

5)  $\langle X \rangle = \{f \in \mathbb{A}_8 \mid f(1) = 1, f(5) = 5, f(8) = 8\}$  podle P33-2). Podgrupa má 60 prvků.

**D61**  $S_n$  dle D32.

**P62**  $GL_2(\mathbb{Z}_2)$  má 6 prvků. 1) dvouprvková podgrupa, 2) tříprvková podgrupa, 3) celá grupa  $GL_2(\mathbb{Z}_2)$ .

Označme  $G = \{A \in GL_2(\mathbb{Z}_3) \mid |A| = [1]_3\}$  podgrupu  $GL_2(\mathbb{Z}_3)$ . Ukažte, že  $\langle Y \rangle = G$ . Snadno se vidí  $\langle Y \rangle \subseteq G$ . Dále  $G$  má 24 prvků a zbývá tedy ukázat, že  $\langle Y \rangle$  má více než 12 prvků.

**P63**  $\{k \cdot \sqrt[3]{2} \mid k \in \mathbb{Z}\}$  v  $(\mathbb{R}, +)$ , resp.  $\{\sqrt[3]{2^k} \mid k \in \mathbb{Z}\}$  v  $(\mathbb{R}^*, \cdot)$ .

**P64**  $\frac{\sqrt{2}}{2} + i \frac{\sqrt{2}}{2} = \cos \frac{\pi}{4} + i \sin \frac{\pi}{4}$  je prvek řádu 8, proto se jedná o osmiprvkovou podgrupu  $\{\pm \frac{\sqrt{2}}{2} \pm i \frac{\sqrt{2}}{2}, \pm 1, \pm i\} = \{\cos \frac{k\pi}{4} + i \sin \frac{k\pi}{4} \mid k \in \mathbb{Z}\}$ .

**D62** V případě  $\mathbb{R}^*$  je to pouze  $\{1\}$  a  $\{1, -1\}$ . Pro  $\mathbb{C}^*$  máme pro každé přirozené číslo  $n$  právě jednu  $n$ -prvkovou podgrupu  $\{\cos \frac{2k\pi}{n} + i \sin \frac{2k\pi}{n} \mid k \in \mathbb{Z}\}$ .

**P65** a)  $\{0, 3\}$ , b)  $6\mathbb{Z}$ , c)  $[0]_4 \cup [3]_4$ .

**D63** Rozlišete několik případů 1) podgrupa neobsahuje liché číslo  $\dots 2k\mathbb{Z}$ ; 2) obsahuje liché  $l$ , ale ne nenulové sudé  $\dots \{0, l\}$ ; 3) obsahuje lichá i sudá a nechť  $k$  je nejmenší sudé přirozené,  $l$  nejmenší liché přirozené  $\dots [0]_k \cup [l]_k$ .

**P71**  $\alpha$  hom.,  $\bar{\alpha}$  není zobr.,  $\beta$  není zobr.,  $\gamma$  izo.,  $\delta$  izo.,  $\epsilon$  hom.,  $\bar{\epsilon}$  zobr. ale není hom.

**P73**  $(\mathbb{Z}_n, \cdot)$  resp.  $(\mathbb{Z}_n^*, \cdot)$ .

**D71** Nechť  $\varphi$  je homomorfismus a  $\varphi([1]_n) = [a]_k$ . Potom  $\varphi([x]_n) = [ax]_k$  a proto musí platit  $k \mid an$ . Počet homomorfismů je tudíž  $(n, k)$ .

**P74** Je-li  $f$  homomorfismus, potom řád prvku  $f(a)$  dělí řád prvku  $a$ . Proto v případě, že  $f$  je izomorfismu platí i opak a tudíž jsou řady stejné.

**D72** Definujte  $\varphi: \mathbb{Z}_2^n \rightarrow P(X)$  takto:  $\varphi(a) = \{i \in X \mid a_i = [1]_2\}$ , kde  $a = (a_i)_{i=1}^n \in \mathbb{Z}_2^n$ .

**P82**  $J(\alpha) = \{[a]_{30} \mid [6a]_{20} = [0]_{20}\} = \{[0]_{30}, [10]_{30}, [20]_{30}\}$ ,  $J(\beta) = \{[0]_{20}, [5]_{20}, [10]_{20}, [15]_{20}\}$ ,  $J(\beta \circ \alpha) = 5\mathbb{Z}_{30}$ .

**P83**

$$J(f) = \left\{ \left( \begin{array}{ccc} 1 & a & b \\ 0 & 1 & a \\ 0 & 0 & 1 \end{array} \mid a, b \in \mathbb{Z} \right) \right\},$$

**D81** Viz. např. Birkhoff, MacLane: Algebra. Návod: nejdříve ukažte, že pokud podgrupa obsahuje nějakou permutaci, pak obsahuje i nějaký cyklus délky 3 a využijte příkladu **P33**.

**P84**  $H$  ne,  $N$  ano.

**P85** 2) celá grupa  $GL_2(\mathbb{Z}_2)$ . 2) tříprvková podgrupa, 3) celá grupa  $GL_2(\mathbb{Z}_2)$ .  $G = \{A \in GL_2(\mathbb{Z}_3) \mid |A| = [1]_3\}$  je normální podgrupa. **3,4** komutativní grupy, tj.  $\langle X \rangle_N = \langle X \rangle$ . **5 a,c)**  $[0]_4 \cup [3]_4$ , b)  $\langle X \rangle_N = \langle X \rangle$ .

**P87**  $H = \langle (2, 1, 4) \rangle = \{\text{id}, (1, 2, 4), (1, 4, 2)\}$ .  $\mathbb{A}_4/H$  má 4 prvky ( $4 = \frac{12}{3}$ ) a to:

$H$ ,

$(1, 2)(3, 4)H = \{(1, 2)(3, 4), (2, 3, 4), (1, 3, 4)\}$ ,

$(1, 3)(2, 4)H = \{(1, 3)(2, 4), (1, 4, 3), (1, 2, 3)\}$ ,

$(1, 4)(2, 3)H = \{(1, 4)(2, 3), (1, 3, 2), (2, 4, 3)\}$ .

**P88** 6, rozmyslete si, kdy  $(m, n) + H = (\bar{m}, \bar{n}) + H$ .

**P89** Má-li podgrupa  $n$  prvků, pak pravý i levý rozklad má dvě třídy a to  $H$  a  $G \setminus H$ . Rozklady jsou tudíž stejné a podgrupa je normální.

**P91**  $(\mathbb{R}^*, \cdot)$  — vhodné zobrazení je přiřazení determinantu.

**P92** Dané dvě matice jsou ve stejné třídě rozkladu právě tehdy, když  $\varepsilon = \varepsilon'$  a  $2 \mid a - a'$ . Faktorgrupa je izomorfní  $\mathbb{Z}_2 \times \mathbb{Z}_2$ , nebo jinak  $\alpha : G \rightarrow \mathbb{Z}^* \times \mathbb{Z}_2$  definujeme

$$\alpha \left( \begin{pmatrix} \varepsilon & a \\ 0 & 1 \end{pmatrix} \right) = (\varepsilon, [a]_2).$$

**P93** 2.  $p + q = \bar{p} + \bar{q}$ . 3.  $\mathbb{Z}$ ;  $\alpha : G \rightarrow \mathbb{Z}$  definujeme  $\alpha(15^p 5^q) = p + q$ .

**P94**  $\mathbb{R}$ ;  $\alpha : \mathbb{C} \rightarrow \mathbb{R}$ ,  $\alpha(a + bi) = b$ .

**P95**  $\mathbb{Z}_2 \times \mathbb{Z}_2$ .

**D91**  $\mathbb{S}_3, \mathbb{Z}_3$ .

**D92** Ukažte, že pokud grupa obsahuje pouze prvky řádu 2, pak je komutativní a má potom počet prvků  $2^n$  pro vhodné  $n$ . Pokud v grupě existuje prvek řádu  $2p$  pak je izomorfní  $\mathbb{Z}_{2p}$  pokud tam není prvek řádu  $2p$ , pak je izomorfní  $\mathbb{D}_p$ .

**D93**  $(\mathbb{S}\mathbb{L}_2(\mathbb{Q}), \cdot)$ .

**C101**  $1, 2, -3, -\frac{1}{2}, -\frac{1}{2}, \frac{1}{3}$ .

**P102**  $a = 10$ ; kořeny  $2, 2, -2, -\frac{1}{2}$ .

**C102** Pro  $a = -5$  dvojnásobný, jinak jednoduchý.

**C104**  $(f, f') = x^2 + 2x + 2$ .

**Z11** **C**  $3, -2, -2, -\frac{1}{2}, -\frac{1}{2}$ ; **D**  $-3, 2, 2, -\frac{1}{2}, -\frac{1}{2}$

**C121**  $[1]_7, [1]_7, [5]_7, [5]_7, [5]_7$

**C122**  $(x + 2)(x^2 + x + 4)(x^2 + 2x + 4)$