Masarykova Univerzita v Brně
Přírodovědecká fakulta

GRUPY – SBÍRKA PŘÍKLADŮ

bakalářská práce

Brno 2005 Vít Musil

Prohlašuji, že jsem tuto bakalářskou práci vypracoval samostatně s použitím uvedené literatury.

v Brně, 9. května 2005 .....
Vít Musil

Obsah

Úvod

Tento materiál by měl sloužit jako pomůcka k praktickému procvičení látky probírané v první části (*Grupy*) skript *Jiří Rosický, Algebra*. Pro přehlednost jsou proto jednotlivé kapitoly pojmenovány a značeny zcela totožně. Na úvod každé z nich jsou shrnuty nejdůležitější fakta z teorie, jako věty, definice a podobně, které pomohou při řešení některých příkladů. V části označené jako TEST jsou shromážděny otázky na něž se odpovídá pouze ano nebo ne, otázky jsou formulovány tak, že vyžadují pozorné přečtení. Pak následuje několik příkladů s podrobně rozepsaným řešením, na něž navazují příklady bez řešení, jejichž výsledky jsou na konci celé publikace.

Příklady jsem čerpal z těch, které jsme řešili na cvičení, ze starších písemek *doc. RNDr. R. Kučery, CSc.* a ze sbírky *Mgr. O. Klímy, PhD.*, jenž je vedoucím mé bakalářské práce a jemuž bych chtěl poděkovat za cenné připomínky při psaní.

Grupy

1 Pojem grupy

Definice 1.1: Množina G spolu s operací $\cdot$ se nazývá *grupoid*. Označujeme jej symbolem $(G, \cdot)$. Grupoid nazveme *komutativní*, resp. *asociativní*, jestliže je operace $\cdot$ komutativní, resp. asociativní. Asociativní grupoid se též nazývá *pologrupa*. [1, Definice 1.4 strana 7]

Definice 1.2: Prvek $e \in G$ se nazývá *jednotkovým prvkem* nebo též *neutrálním prvkem* grupoidu G, jestliže

$$a \cdot a = a \cdot e = a$$

pro libovolné $a \in G$. [1, Definice 1.5 strana 8]

Věta 1.3: *Grupoid má nejvýše jeden jednotkový prvek.* [1, Věta 1.6 strana 8]

Věta 1.4: *Buď G pologrupa s jednotkovým prvkem, $a \in G$. Pak existuje nejvýše jeden prvek v G inverzní k a.* [1, Věta 1.8 strana 8]

Definice 1.5: Grupoid G se nazývá *grupa*, jestliže je asociativní, má jednotkový prvek a k libovolnému jeho prvku existuje prvek inverzní.
[1, Definice 1.9 strana 8]

Úloha i: Je dán grupoid $(\mathbb{R}, \circ)$, zjistěte jestli je asociativní, přitom

$$x \circ y = (x + y) \cdot (1 + xy).$$

Řešení:
$(x \circ y) \circ z = \big((x+y)\cdot(1+xy)\big) \circ z = \big((x+y)\cdot(1+xy)+z\big)\cdot\Big(1+\big((x+y)\cdot(1+xy)\big)\cdot z\Big)$
$x \circ (y \circ z) = x \circ \big((y+z)\cdot(1+yz)\big) = \big(x+(y+z)\cdot(1+yz)\big)\cdot\Big(1+x\cdot\big((y+z)\cdot(1+yz)\big)\Big)$
Pokud dosadíme například za $x = -1, y = 1, z = 2$, pak dostaneme dva různé (2 a -64) výsledky. Grupoid tedy není asociativní.

Úloha ii: Rozhodněte, zda je grupoid $(G, \circ)$ grupa, kde $G = \mathbb{Q}^*$ a pro libovolná $x, y \in G$ platí $x \circ y = |x \cdot y|$

Řešení:

- Je to pologrupa? **ANO**
  Nechť $x, y, z \in G$ pak $x \circ (y \circ z) = x \circ |y \cdot z| = |x \cdot y \cdot z|$
  $(x \circ y) \circ z = |x \cdot y| \circ y = |x \cdot y \cdot z|$
- Neutrální prvek n? **NE**
  Musíme najít takový prvek $e \in G$, že pro libovolné $x \in G$ platí $e \circ x = x \circ e = x$
  Mějme například $x = -3$, pak $-3 \circ e = |-3 \cdot e|$ by se mělo rovnat -3, hned vidíme, že takové e neexistuje.
  Tedy $(G, \circ)$ není grupa.

Úloha iii: Rozhodněte, zda je $(M_2(\mathbb{Z}), +)$ grupa, popřípadě jestli je tato grupa komutativní. (Symbol $M_2(\mathbb{Z})$ značí množinu všech matic typu 2/2, jejíž prvky jsou z množiny $\mathbb{Z}$.)

Řešení:

- Jedná se o grupoid? **ANO**, protože $+$ je operací na množině $(M_2(\mathbb{Z}), +)$.
- Jedná se o pologrupu? **ANO**, protože $+$ je asociativní.
- Existuje neutrální prvek? **ANO**, je jím matice $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$.
- Má každý prvek prvek inverzní? **ANO**, k matici $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ je to matice $\begin{pmatrix} -a & -b \\ -c & -d \end{pmatrix}$.

TEST:

1. V každé pologrupě s neutrálním prvkem ke každému prvku existuje nejvýše jeden prvek inverzní.
2. V každém grupoidu s neutrálním prvkem existuje ke každému prvku nejvýše jeden prvek inverzní.
3. Každý grupoid má právě jeden neutrální prvek

Příklad 1.1: Je dána množina G a operace $\circ$ na této množině. Rozhodněte, je-li $(G, \circ)$ grupoid.

a) $G = \mathbb{N}$ a pro libovolné $x, y \in G$ platí $x \circ y = x - y$,

b) $G = \{-1, 0, 1\}$ a pro libovolné $x, y \in G$ platí $x \circ y = x \cdot y$,

c) $G = \{-1, 0, 1\}$ a pro libovolné $x, y \in G$ platí $x \circ y = x + y$,

d) $G = \{1, 2, 3, 5, 10, 15, 20, 30\}$ a pro libovolné $x, y \in G$ platí $x \circ y = (x, y)$, kde (x, y), značí největší společný dělitel čísel x a y.

Příklad 1.2: Dokažte větu 1.3 a větu 1.4.

Příklad 1.3: Na množině $G = \{a, b, c, d\}$ je dána operace $\circ$ tabulkou. Rozhodněte, zda je grupoid $(G, \circ)$ komutativní, resp. asociativní, resp. jestli má neutrální prvek.

a)

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

b)

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

Příklad 1.4: Napište multiplikativní tabulku grupy $(G, \cdot)$, kde $G = \{e, f, g\}$, když víte, že $e \cdot f = g$

Příklad 1.5: Je dána množina $G = \{a, b, c\}$ a částečná tabulka operace $\circ$ na množině G.

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

Doplňte tabulku tak, aby $(G, \circ)$

a) byl grupoid s neutrálním prvkem,

b) byl grupoid v němž má každý prvek inverzi,

c) byla pologrupa,

d) byla grupa.

Příklad 1.6: Nechť G je libovolná množina, která má alespoň dva prvky. Na G definujeme operaci $\circ$ takto: $x \circ y = x$, pro $\forall x, y \in G$. Zjistěte jestli $(G, \circ)$ je grupa, resp. pologrupa, je-li tato komutativní a má neutrální prvek. Co se změní, jestliže bude množina G jednoprvková?

Příklad 1.7: Je dán komutativní grupoid $(G, \circ)$. Rozhodněte, zda je $(G, \circ)$ komutativní grupou. Přitom:

a) $G = \mathbb{Q}^+$; $\circ$ je násobení čísel,

b) $G = \mathbb{Q}^*$; $x \circ y = |x \cdot y|$,

c) $G = \{x \in \mathbb{R} \mid x \neq 0 \wedge |x| \leq 1\}$; $\circ$ je násobení čísel,

d) $G = \langle 0, 1)$; $x \circ y = x + y - [x + y]$,

e) $G = \{a + b \cdot i \mid a, b \in Z\}$; $\circ$ je sčítání komplexních čísel,

f) $G = \{a + \sqrt{5} \cdot b \cdot i \mid a, b \in Q \wedge (a^2 + b^2) \neq 0\}$; $\circ$ je násobení komplexních čísel,

kde $\mathbb{Q}^+$ značí množinu všech kladných racionálních čísel resp. $[x+y]$ značí celou část reálného čísla $x + y$, tj. největší celé číslo, které nepřevyšuje číslo $x + y$.

Příklad 1.8: Uvažme množinu $M = \{(a, b) \mid a, b \in \mathbb{R},\ a < 0 < b\} \cup 0$ otevřených intervalů reálných čísel. Ukažte, že průnik $\cap$ je operací na této množině. Rozhodněte, zda je operace $\cap$ asociativní a zda existuje neutrální prvek. Je $(M, \cap)$ grupa?

Příklad 1.9: Uvažme množinu $N = \{(a, b) \mid a, b \in \mathbb{R},\ a < 0 < b\}$ otevřených intervalů reálných čísel. Ukažte, že sjednocení $\cup$ je operací na této množině. Rozhodněte, zda je operace $\cup$ asociativní a zda existuje neutrální prvek. Je $(N, \cup)$ grupa?

Příklad 1.10: Definujeme zobrazení $f_i : \mathbb{R} - \{0, 1\} \to \mathbb{R} - \{0, 1\}$ pro $i = 1, 2, \ldots, 6$ takto:

$f_1(x) = x$ $\quad f_2(x) = \frac{1}{x}$ $\quad f_3(x) = 1 - x$

$f_4(x) = \frac{x}{x-1}$ $\quad f_5(x) = \frac{x-1}{x}$ $\quad f_6(x) = \frac{1}{1-x}$

Vytvořte tabulku množiny $G = \{f_1, f_2 f_3, f_4, f_5, f_6\}$ s operací skládání zobrazení a dokažte, že se jedná nekomutativní grupu.

Příklad 1.11: Rozhodněte, zda $(\mathbb{Q}, \circ)$, kde $x \circ y = 2 \cdot (x \cdot y + x + y) + 1$ pro libovolné $x, y \in \mathbb{Q}$ je grupa. Své tvrzení dokažte.

Příklad 1.12: Nechť $(G, \circ)$ je grupa a a nějaký její pevně zvolený prvek. Dokažte, že potom $(G, \diamond)$ je také grupa, kde operace $\diamond$ je definována předpisem $g \diamond h = g \circ a \circ h$.

2 Permutace

Definice 2.1: Buď X množina. Bijektivní zobrazení množiny X na sebe nazýváme *permutace* množiny X. Množina všech permutací množiny X se označuje symbolem $S(X)$. [1, Definice 2.2 strana 10]

Věta 2.2: *Každou neidentickou permutaci množiny* $\{1, \ldots, n\}$ *lze rozložit v součin navzájem nezávislých cyklů. Tento rozklad je určen jednoznačně, až na pořadí cyklů.* [1, Věta 2.5 strana 12]

Definice 2.3: Buď f permutace množiny $\{1, \ldots, n\}$. Řekneme, že uspořádaná dvojice $[i, j]$ je *inverze* permutace f, jestliže $1 \leq i < j \leq n$ a $f(i) > f(j)$. Permutace f se nazývá *sudá* nebo *lichá* podle toho, zda má sudý nebo lichý počet inverzí. *Parita* $p(f)$ permutace f se definuje rovna číslu 1, pokud permutace f je sudá, a číslu -1, je-li f lichá. [1, Definice 2.7 strana 13]

Věta 2.4: *Součin k transpozic je sudá permutace $\Leftrightarrow$ k je sudé číslo.* [1, Věta 2.8 strana 13]

Věta 2.5: *Buďte f, g permutace množiny $\{1,\ldots,n\}$. Pak*

$$p(f \circ g) = p(f) \cdot p(g).$$

[1, Věta 2.9 strana 13]

Úloha i: Je dána permutace $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 5 & 4 & 1 & 2 & 3 & 9 & 7 & 6 & 8 \end{pmatrix}$, zapište tuto permutaci, jako složení navzájem nezávislých cyklů.

Řešení: Při řešení postupujeme takto, vybereme například první prvek **1** a do cyklu za něj zapíšeme prvek, na který se zobrazuje $(1, \mathbf{5}, ?)$, za něj ten, na nějž se zobrazuje $(1, 5, \mathbf{3}, ?)$ a tak pořád dál. Pokud se posledně zapsaný prvek v cyklu zobrazuje na první v cyklu, cyklus uzavřeme $(1, 5, 3)$ a složíme ho s dalším nezávislým cyklem, který utvoříme zcela analogicky z prvků, které ještě nejsou v cyklech obsaženy. Prvek, který se zobrazuje sám na sebe v takovémto zápisu neuvádíme. Celkový výsledek je tedy

$$f = (1, 5, 3) \circ (2, 4) \circ (6, 9, 8)$$

Úloha ii: Jsou dány permutace

$$a = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}, \quad b = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 1 & 2 & 3 & 5 \end{pmatrix}$$

a) Zapište tyto permutace jako složení navzájem nezávislých cyklů.

b) Spočtěte permutaci $a \circ b$.

c) Spočtěte permutaci a^{15}.

d) Rozložte permutaci b na součin transpozic.

Řešení:
a) Jako v předešlém příkladě: $a = (1,2,3) \circ (4,5), b = (1,4,3,2)$

b) Nejprve si permutace zapíšeme jako složení nezávislých cyklů a ty pak složíme $a \circ b = (1,2,3) \circ (4,5) \circ (1,4,3,2)$. Začneme od prvního cyklu (nejvíce vpravo), 1 se podle něj zobrazí na 4, podle druhého přejde 4 na 5 a poslední nechá 5 na 5 a tedy po prvním kroku máme $(1,5,?)$ a pokračujeme, 5 se podle prvního nemění, podle druhého přejde na 4 a poslední nechává opět 4 na sebe samu, po druhém projití dostáváme tedy $(1,5,4,?)$ a takto pokračujeme dál. Celkově tedy dostaneme, že $a \circ b = (1,2,3) \circ (4,5) \circ (1,4,3,2) = (1,5,4)$

c) Opět si nejprve zapíšeme permutaci jako složení nezávislých cyklů. Poté můžeme každý cyklus umocňovat zvlášť, tedy: $a^{15} = (1,2,3)^{15} \circ (4,5)^{15}$. Víme, že pokud cyklus délky k umocníme na n, takové, že $k \mid n$ přejde tento cyklus na identitu, pak už není těžké získat výsledek

$$a^{15} = (1,2,3)^{15} \circ (4,5)^{15} = (1,2,3)^{5 \cdot 3} \circ (4,5)^{7 \cdot 2+1} = (4,5).$$

d)Jelikož víme, že každou permutaci lze zapsat jako součin transpozic takto $(i_1, \dots i_k) = (i_1, i_k) \circ \cdots \circ (i_1, i_3) \circ (i_1, i_2)$, pak tedy $b = (1,2) \circ (1,3) \circ (1,4)$.

Úloha iii: Dokažte, že permutace $(s^8 \circ t^{11} \circ s^{16} \circ t^{13})$ je vždy sudá.

Řešení:
Využijme toho, že $p(a^n) = p(a)^n$ a tedy jakákoli permutace umocněná na sudé číslo je sudá. Tedy:
$p(s^8) \cdot p(t^{11}) \circ p(s^{16}) \circ p(t^{13}) = 1 \cdot p(t^{11}) \cdot 1 \cdot p(t^{13}) = p(t^{11} \circ t^{13}) = p(t^{24}) = 1$
Tím je tvrzení dokázáno.

♣ ♣ ♣ ♣ ♣

TEST:

1. Každá transpozice je lichou permutací.
2. Každou neidentickou permutaci konečné množiny lze rozložit do součinu transpozic.
3. Každá lichá permutace je transpozici.
4. Grupa $(\mathbb{S}_n, \circ)$ je komutativní pro každé $n \in \mathbb{N}$.
5. Pro každé $n \in \mathbb{N}$, $n \geq 3$ je grupa $(\mathbb{D}_n, \circ)$ komutativní (grupa $(\mathbb{D}_n, \circ)$ je grupa všech symetrií pravidelného n-úhelníka).
6. Cyklus délky 5 umocněný na 321 má lichou paritu.
7. $\mathbb{S}_6$, tj. grupa všech permutací na šesti prvcích, má 36 prvků.

♣ ♣ ♣ ♣ ♣

Příklad 2.1: Jsou dány permutace f,g,$h \in \mathbb{S}_9$ předpisem

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 9 & 3 & 7 & 8 & 1 & 4 & 2 & 6 & 5 \end{pmatrix},$$

$$g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 8 & 1 & 5 & 2 & 6 & 3 & 7 & 4 & 9 \end{pmatrix}, \quad h = f \circ g.$$

a) Napište permutace f, g a h jako složení navzájem nezávislých cyklů.

b) Určete paritu permutací f, g a h.

c) Spočtěte permutaci $f^{100} \circ g^{100}$ a napište ji jako součin navzájem nezávislých cyklů.

Příklad 2.2: Jsou dány permutace u,v,$w \in \mathbb{S}_9$ předpisem

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

$$v = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 5 & 2 & 1 & 4 & 3 & 8 & 7 & 6 & 9 \end{pmatrix},$$

$$w = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 8 & 1 & 4 & 6 & 3 & 7 & 5 & 9 & 2 \end{pmatrix},$$

a) Zapište permutace u, v, w jako složení nezávislých cyklů.

b) Spočtěte permutace $u \circ v$, $v \circ u$, $w \circ v$.

c) Spočtěte permutace $w \circ v \circ u$, $w \circ v \circ w$, $v \circ w \circ u$.

d) Spočtěte permutaci v^{103}.

e) Spočtěte permutaci w^{27}.

f) Spočtěte permutaci $u^{120} \circ v^{-3}$.

g) Zapište permutaci $v^{32} \circ w^{32}$ jako součin transpozic a určete její paritu.

h) Zapište permutace u, v, w jako součin transpozic a ucrčete jejich paritu.

Příklad 2.3: Určete inverzní prvky u^{-1}, v^{-1}, w^{-1} z předešlého příkladu.

Příklad 2.4: Mějme permutace $f, g \in \mathbb{S}_n$. Určete paritu permutace $f^7 \circ g^8 \circ f^9$.

Příklad 2.5: Určete všechny permutace $f \in \mathbb{S}_6$, pro něž platí $f^2 = (1,2) \circ (3,4)$.

Příklad 2.6: Určete všechny permutace $a \in \mathbb{S}_8$ takové, že $a^2 = (1,2,3) \circ (4,5,6)$.

Příklad 2.7: V grupě $(\mathbb{S}_5, \circ)$ všech permutací pětiprvkové množiny $\{1,2,3,4,5\}$ najděte permutaci f takovou, že $(1,3) \circ (2,4,5) \circ f \circ (1,4) = \mathrm{id}$.

Příklad 2.8: 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.

Příklad 2.9: Dokažte, že permutace $(s^3 \circ t^{-17})^{18} \circ s^{10}$ je sudá permutace pro libovolné $s,\ t \in \mathbb{S}_9$.

3 Grupy zbytkových tříd

Definice 3.1: Nechť $a, b \in \mathbb{Z}$, řekneme, že a dělí b, pokud $\exists c \in \mathbb{Z}$, tak že $b = a \cdot c$, píšeme $a \mid b$. [1, strana 14]

Definice 3.2: Nechť $a, b \in \mathbb{Z}$. Definujeme *největší společný dělitel* $(a, b) = d$, kde:

1. $d \mid a, d \mid b$
2. $\forall \delta \in \mathbb{Z}, \delta \mid a, \delta \mid b \Rightarrow \delta \mid d$
3. $d \geq 0$

Čísla $a, b \in \mathbb{Z}$ se nazývají *nesoudělná* pokud $(a, b) = 1$.
[1, strana 15]

Věta 3.3: (Euklidův algoritmus) *Nechť $a, b \in \mathbb{N}$ označme $a_1 = a, a_2 = b$ a pro $n \geq 3$ položme a_n rovno zbytku po dělení a_{n-2} číslem a_{n-1}. Po konečném počtu kroků dostaneme $a_k = 0$. Pak $(a, b) = a_{k-1}$.* [1, strana 15]

Důsledek: (Bezoutova rovnost) *Pro libovolná celá čísla a,b existují celá čísla u,v taková, že*

$$a \cdot u + b \cdot v = (a, b).$$

[1, Věta 3.3 (Bezoutova rovnost) strana 15]

Definice 3.4: Buď n přirozené číslo. Množiny $[a]_n = \{k \cdot n + a \mid k \in \mathbb{Z}\}$, kde $a \in \mathbb{Z}$ se nazývají *zbytkové třídy podle modulu n.* Množinu všech zbytkových tříd podle modulu n se označuje symbolem $\mathbb{Z}_n$. [1, Definice 3.7 strana 17]

Věta 3.5: *Buď n přirozené, a celé číslo. Zbytková třída $[a]_n$ má inverzní prvek v $(\mathbb{Z}_n, \cdot)$, právě když čísla a, n jsou nesoudělná.* [1, Věta 3.13 strana 19]

Definice 3.6: Buď $1 < n$ přirozené číslo. Symbolem $\varphi(n)$ označíme počet všech přirozených čísel menších než n a nesoudělných s n. Funkce φ je tzv. *Eulerova funkce.* Klademe $\varphi(1) = 1$. [1, Definice 3.15 strana 20]

Věta 3.7: *Pro libovolné prvočíslo p je $\varphi(p^k) = (p-1) \cdot p^{k-1}$.*
Pro libovolná nesoudělná přirozená čísla a, b je $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$.
[1, Věta 3.16 strana 20]

Úloha i: Pomocí Euklidova algoritmu zjistěte $(600, 9432)$.

Řešení:

$$\begin{aligned} 9432 &= 1 \cdot 6000 + 3432 \\ 6000 &= 1 \cdot 3432 + 2568 \\ 3432 &= 1 \cdot 2568 + 864 \\ 2568 &= 2 \cdot 864 + 840 \\ 864 &= 1 \cdot 840 + 24 \\ 840 &= 35 \cdot 24 + 0 \end{aligned}$$

Největším společným dělitelem je tedy 24.

Úloha ii: Dokažte, že čísla $2n + 1$ a $9n + 4$ jsou nesoudělná pro libovolné $n \in \mathbb{N}$.

Řešení: Máme vlastně dokázat $(2n + 1, 9n + 4) = 1$. Použijeme Euklidův algortimus:

$$\begin{aligned} 9n + 4 &= 4 \cdot (2n + 1) + n \\ 2n + 1 &= 2 \cdot n + 1 \\ n &= n \cdot 1 + 0 \end{aligned}$$

Tím je tvrzení dokázáno.

Úloha iii: Zjistěte kolik inverzních prvků má komutativní pologrupa $(\mathbb{Z}_{12}, \cdot)$.

Řešení: Podle věty 1.3.4. je počet prvků majících v $(\mathbb{Z}_n, \cdot)$ inverzi roven $\varphi(n)$. Tedy počet inverzních prvků v $(\mathbb{Z}_{12}, \cdot)$ je roven $\varphi(12) = 4$.

Úloha iv: Určete inverzní prvek ke zbytkové třídě modulo 540, která obsahuje číslo 17.

Řešení: Víme, že inverzní prvek exituje, pokud jsou čísla nesoudělná, to nejlépe zjistíme pomocí Euklidova algortimu:

$$\begin{aligned} 540 &= 31 \cdot 17 + 13 \\ 17 &= 1 \cdot 13 + 4 \\ 13 &= 3 \cdot 4 + 1 \\ 4 &= 4 \cdot 1 + 0 \end{aligned}$$

Zjistili jsme tedy, že čísla jsou nesoudělná a tudíž můžeme hledat inverzní prvek, k tomu využijeme Bezoutovu rovnost:
$1 = 13 - 3 \cdot 4 = 13 - 3 \cdot (17 - 13) = -3 \cdot 17 + 4 \cdot 13 = -3 \cdot 17 + 4 \cdot (540 - 31 \cdot 17) =$
$= 4 \cdot 540 - 127 \cdot 17$
To znamená, že $[17]_{540}^{-1} = [-127]_{540} = [413]_{540}$.

Úloha v: Nalezněte všechna $m \in \mathbb{N}$, pro která je $\varphi(m)$ liché.

Řešení:

1. Jestliže m je dělitelné lichým prvočíslem p pak $p-1 \mid \varphi(m) \Rightarrow \varphi(m)$ je sudé číslo.
2. Žádné liché prvočíslo nedělí m, pak $m = 2^k, k \in \mathbb{N}_0$. Je-li $k = 0$, pak $\varphi(m) = \varphi(2^0) = \varphi(1) = 1$, je-li $k > 0$, pak $\varphi(m) = \varphi(2^k) = 1 \cdot 2^{k-1}$ a to je liché právě, když $k = 1$.
   $\varphi(m)$ je liché, jestliže $m = 1, 2$.

Úloha vi: Zjistěte pro která $m \in \mathbb{N}$ je $\varphi(m) = 16$.

Řešení: Nechť $m = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \cdots \cdot p_k^{\alpha_k}$, p_i jsou různá prvočísla a $\alpha_i \in \mathbb{N}$ pro $i =$

$= \{1, 2, \cdots, k\}$.
$\varphi(m) = (p_1 - 1) \cdot p_1^{\alpha_1 - 1} \cdot (p_2 - 1) \cdot p_2^{\alpha_2 - 1} \cdot \cdots \cdot (p_k - 1) \cdot p_k^{\alpha_k - 1} = 16 = 2^4$, to znamená, že

$$m = 2^\alpha \cdot 3^\beta \cdot 5^\gamma \cdot 17^\delta, \ \alpha, \beta, \gamma, \delta \in \mathbb{N}_0,$$
$$\varphi(m) = \varphi(2^\alpha) \cdot \varphi(3^\beta) \cdot \varphi(5^\gamma) \cdot \varphi(17^\delta).$$

Nyní provedeme úvahu jakých hodnot mohou nabývat $\alpha, \beta, \gamma, \delta$. Nejlepší je začít u mocniny nejvyššího prvočísla tedy u δ.

1. Je zřejmé, že δ může být nanejvýš rovna 1 a zároveň musí být $\varphi(2^\alpha) \cdot \varphi(3^\beta) \cdot \varphi(5^\gamma) = 1$, jinak bychom dostali $\varphi(m) \geq 272$.
   Nechť $\delta = 1 \wedge \alpha = \beta = \gamma = 0$, pak $m = 17$ a máme první řešení.
   Nechť $\delta = \alpha = 1 \wedge \beta = \gamma = 0$, pak $m = 2 \cdot 17 = 34$.
   Tím jsme vyčerpali všechny možnosti pro $\delta = 1$ a dále v řešení budeme uvažovat $\delta = 0$.
2. Když tedy $\delta = 0$ pak $m = 2^\alpha \cdot 3^\beta \cdot 5^\gamma$, nyní zauvažujeme γ.
   Kdyby $\gamma \geq 2$ tak $\varphi(m) \geq 20$, to znamená, že γ může být nejvýše 1.
   Nechť tedy $\gamma = 1 \wedge \alpha, \beta \geq 1$.

$$\begin{aligned} \varphi(m) = \varphi(2^\alpha) \cdot \varphi(3^\beta) \cdot \varphi(5) &= 16 \\ 2^{\alpha-1} \cdot 2 \cdot 3^{\beta-1} \cdot 4 &= 16 \\ 2^{\alpha-1} \cdot 3^{\beta-1} &= 2 \\ \alpha &= 2 \\ \beta &= 1 \\ \text{A tedy } m &= 60 \end{aligned}$$

Nechť dále $\gamma = 1 \wedge \alpha = 0 \wedge \beta \geq 1$.

$$\begin{aligned} \varphi(m) = \varphi(3^\beta) \cdot \varphi(5) &= 16 \\ 2 \cdot 3^{\beta-1} \cdot 4 &= 16 \\ 3^{\beta-1} &= 2 \end{aligned}$$

Nemá řešení.

Dále nechť $\gamma = 1 \wedge \beta = 0 \wedge \alpha \geq 1$.

$$\begin{aligned} \varphi(m) = \varphi(2^\alpha) \cdot \varphi(5) &= 16 \\ 2^{\alpha-1} \cdot 4 &= 16 \\ 2^{\alpha-1} &= 4 \\ \alpha &= 3 \\ \text{A tedy } m &= 40 \end{aligned}$$

Tím je $\gamma = 1$ a v úvahách budeme pokračovat pro $\gamma = 0$.

3. Nyní $m = 2^\alpha \cdot 3^\beta$. Nechť $\alpha, \beta \geq 1$.

$$\begin{aligned} \varphi(m) = \varphi(2^\alpha) \cdot \varphi(3^\beta) &= 16 \\ 2^{\alpha-1} \cdot 2 \cdot 3^{\beta-1} &= 16 \\ 2^{\alpha-1} \cdot 3^{\beta-1} &= 8 \\ \alpha &= 4 \\ \beta &= 1 \\ \text{A tedy } m &= 48 \end{aligned}$$

Nechť $\alpha = 0 \wedge \beta \geq 1$. Pak $\varphi(m) = \varphi(3^\beta) = 3^{\beta-1} = 8$, což nemá řešení.
A konečně nechť $\beta = 0 \wedge \alpha \geq 1$. Pak $\varphi(m) = \varphi(2^\alpha) = 2^{\alpha-1} = 16$, $\alpha = 5$ a tedy $m = 32$.

Celkově $m = \{17, 32, 34, 40, 48, 60\}$.

TEST:

1. Pro libovolné přirozené číslo $m > 2$ platí, že $\varphi(m)$ je sudé číslo.
2. Pro libovolné přirozené číslo m platí $\varphi(m)^2 \mid \varphi(m^2)$.
3. Pro libovoné číslo $n \in \mathbb{N}$ je $(\mathbb{Z}_n, \cdot)$ grupa.
4. Pro libovoné prvočíslo p je $(\mathbb{Z}_p, \cdot)$ grupa.
5. Rozhodněte zda je $(\mathbb{Z}_9, \cdot)$ komutativní pologrupa.
6. Pro libovolné prvočíslo p jsou grupy $(\mathbb{Z}_p^*, \cdot)$ (grupa zbytkových tříd modulo p neobsahující zbytkovou třídu s reprezentantem $[0]_p$) a $(\mathbb{Z}_p^\times, \cdot)$ (grupa všech invertibilních zbytkových tříd modulo p) totožné.

Příklad 3.1: Nalezněte $(111, 107)$ a vyjádřete jej Bezoutovou rovností.

Příklad 3.2: Pro která $n \in \mathbb{N}$ jsou čísla $2n - 1$ a $9n + 4$ nesoudělná?

Příklad 3.3: Nalezněte inverzní prvek k $[49]_{1000}$ v $(\mathbb{Z}_{1000}, \cdot)$.

Příklad 3.4: Rozhodněte, zda existuje inverzní zbytková třída ke třídě obsahující číslo 67 modulo 103 a pokud ano, nalezněte ji.

Příklad 3.5: Kolik existuje inverzních prvků v
a) $(\mathbb{Z}_{1021}, \cdot)$ b) $(\mathbb{Z}_{4725}, \cdot)$

Příklad 3.6: Vypočítejte:
a) $\varphi(635)$ b) $\varphi(1221)$ c) $\varphi(1331)$

Příklad 3.7: Určete pro která $n \in \mathbb{N}$ platí $\varphi(5^n) = 100$.

Příklad 3.8: Dokažte, že pro každé $n \in \mathbb{N}$ platí $\varphi(4n+2) = \varphi(2n+1)$.

Příklad 3.9: Spočtěte:
a) $[2^k+1]^{-1}_{2^{2k}+1}$ v $\mathbb{Z}_{2^{2k}+1}$ b) $[2^k-1]^{-1}_{2^{2k}+1}$ v $\mathbb{Z}_{2^{2k}+1}$ c) $[m^2-m+1]^{-1}_{m^3-1}$ v $\mathbb{Z}_{m^3-1}$

Příklad 3.10: Zjistěte, pro která $m \in \mathbb{N}$ je $\varphi(m) = 18$.

Příklad 3.11: Určete kolik prvků mají grupy $(\mathbb{Z}_n^\times, \cdot)$ pro následující n:
a) $n = 24$ b) $n = 306$ c) $n = 5225$

Příklad 3.12: Najděte všechna $x \in \mathbb{N}$ tak, že $13x$ dává zbytek 7 po dělení 1000 respektive 100.

4 Základní vlastnosti grup

Věta 4.1: *Buď G pologrupa s jednotkovým prvkem. Pak platí:*

(1) $1^{-1} = 1$,

(2) $(a^{-1})^{-1} = a$,

(3) $(a_1 \cdot a_2 \cdot \cdots \cdot a_n)^{-1} = a_n^{-1} \cdot \cdots \cdot a_2^{-1} \cdot a_1 - 1$,

kde a, $a_1, \ldots a_n$ jsou libovolné invertibilní prvky z G.
[1, Věta 4.6 strana 24]

Věta 4.2: *Buď $(G, \cdot)$ pologrupa s jednotkovým prvkem, H množina všech invertibilních prvků z G. Pak $(H, \cdot)$ je grupa.* [1, Věta 4.7 strana 26]

Definice 4.3: *Řád* prvku a grupy G definujeme jako nejmenší přirozené číslo n takové, že $a^n = 1$. Pokud takové přirozené číslo neexistuje, řekneme, že řád prvku a je ∞. [1, Definice 4.11 strana 26]

Věta 4.4: *Buď G grupa, $a \in G$. Je-li řád prvku a přirozené číslo n, pak :*

(1) pro libovolné celé číslo k platí $a^k = a^r$, kde r je zbytek po dělení čísla k číslem n,

(2) $a^k \neq a^m$ *pro libovolná navzájem různá celá čísla* $0 < k,\ m \leq n$.

Je-li prvek a řádu ∞, pak:

(3) $a^k \neq a^m$ *pro libovolná navzájem různá celá čísla $k,\ m$.*

[1, Věta 4.13 strana 26]

Věta 4.5: *Buď G grupa, $a \in G$ a k přirozené číslo. Pak $a^k = 1$právě, když řád prvku a dělí číslo k.*[1, Důsledek 4.14 strana 27]

Věta 4.6: *Buď G grupa, $a \in G$ prvek řádu n, $n = k \cdot m$. Pak prvek a^k je řádu m.* [1, Důsledek 4.15 strana 27]

Věta 4.7: *Buď G grupa, $a, b, c \in G$. Pak platí:*

$$a \cdot b = a \cdot c \Rightarrow b = c,$$
$$b \cdot a = c \cdot a \Rightarrow b = c.$$

Tyto vztahy se nazývají zákony o krácení. [1, Věta 4.17 strana 27]

Definice 4.8: Počet prvků konečné grupy G nazýváme *řád* této grupy. Označujeme jej symbolem $|G|$. [1, Definice 6.5 strana 34]

Úloha i: V grupě $(\mathbb{Z}_{14}^{\times}, \cdot)$ invertibilních zbytkových tříd modulo 14 spočítejte řád prvku $[5]_{14}$.

Řešení:

- $[5]_{14}^2 = [25]_{14} = [-3]_{14}$
- $[5]_{14}^3 = [-3]_{14} \cdot [5]_{14} = [-15]_{14} = [-1]_{14}$
- $[1]_{14} = [-1]_{14}^2 = ([5]_{14}^3)^2 = [5]_{14}^6$

Jelikož ani 4 a 5 nejsou řádem prvku $[5]_{14}$ v grupě $(\mathbb{Z}_{14}^{\times}, \cdot)$ je jím tedy 6.

Úloha ii: V grupě $(\mathbb{Z}_{13}^{\times}, \cdot)$ invertibilních zbytkových tříd modulo 13 spočítejte řády všech prvků.

Řešení: Jelikož je modul prvočíselný, obsahuje grupa $(\mathbb{Z}_{13}^{\times}, \cdot)$ dvanáct prvků (obsahuje reprezentanty všech zbytkových tříd modulo 13 kromě zbytkové třídy s reprezentantem 0). Nejlepší je zapisovat si výsledky do tabulky.

Prvek	Řád	Prvek	Řád
$[1]_{13}$	1	$[7]_{13}$	12
$[2]_{13}$	12	$[8]_{13}$	4
$[3]_{13}$	3	$[9]_{13}$	3
$[4]_{13}$	6	$[10]_{13}$	6
$[5]_{13}$	4	$[11]_{13}$	12
$[6]_{13}$	12	$[12]_{13}$	2

(Poznámka: Podrobnější postup hledání řádu prvku viz předešlá úloha.)

- $[1]_{13}$ - neutrální prvek, je vždy řádu 1
- $[2]_{13}^6 = [64]_{13} = [-1]_{13}$
  $[2]_{13}^{12} = [1]_{13}$
- $[3]_{13}^2 = [9]_{13} = [-4]_{13}$
  $[3]_{13}^3 = [-12]_{13} = [1]_{13}$
- $[4]_{13} = [2]_{13}^2$
  $[2]_{13}^{12} = [4]_{13}^6$
- $[5]_{13}^2 = [25]_{13} = [-1]_{13}$
  $[5]_{13}^4 = [2]_{13}$
- $[6]_{13}^6 = [46656]_{13} = [-1]_{13}$
  $[6]_{13}^{12} = [1]_{13}$
- $[7]_{13}^6 = [117649]_{13} = [-1]_{13}$
  $[7]_{13}^{12} = [1]_{13}$
- $[8]_{13}^{12} = [2]_{13}^3$
  $[2]_{13}^{12} = [8]_{13}^3$
- $[9]_{13}^3 = [729]_{13} = [1]_{13}$
- $[10]_{13}^3 = [1000]_{13} = [-1]_{13}$
  $[10]_{13}^6 = [1]_{13}$
- $[11]_{13}^6 = [1771561]_{13} = [-1]_{13}$
  $[11]_{13}^{12} = [1]_{13}$
- $[12]_{13}^2 = [144]_{13} = [1]_{13}$

TEST:

1. V libovolné komutativní grupě platí, že řád součinu dvou prvků je roven součinu řádu těchto prvků.
2. Jestliže nějaká grupa obsahuje prvek řádu 6, pak obsahuje i prvek řádu 3.
3. Všechny prvky libovolné nekonečné grupy jsou nekonečného řádu.
4. V libovolné komutativní grupě platí, že řád součinu dvou prvků je roven nejmenšímu společnému násobku řádu těchto prvků.
5. Řád libovolné konečné cyklické grupy je prvočíslo.
6. V libovolné grupě je jen konečně mnoho prvků konečného řádu.
7. Jestliže nějaká grupa obsahuje prvek řádu 2 a též prvek řádu 3, pak obsahuje i prvek řádu 6.
8. Je-li řád konečné grupy $(G, \cdot)$ dělitelný prvočíslem p, pak grupa $(G, \cdot)$ obsahuje prvek řádu p.
9. V každé grupě platí, že součin libovolných dvou prvků nekonečného řádu je opět prvek nekonečného řádu.
10. Existuje nekonečná grupa s prvkem konečného řádu.
11. Řád prvku a grupy $(G, \circ)$ je roven 1 právě, když a je neutrálním prvkem grupy $(G, \circ)$.
12. V libovolné pologrupě s neutrálním prvkem tvoří množina všech invertibilních prvků grupu.

Příklad 4.1: V grupě $(\mathbb{Z}_{15}^{\times}, \cdot)$ invertibilních zbytkových tříd modulo 15 spočítejte řád prvku $[7]_{15}$.

Příklad 4.2: V grupě $(\mathbb{GL}_2(\mathbb{R}), \cdot)$ regulárních matic typu 2×2 s reálnými prvky určete řád matice A a řád matice B, kde

$$A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \qquad B = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Příklad 4.3: Určete všechna přirozená čísla m taková, že v aditivní grupě $(\mathbb{Z}_{24}, +)$ zbytkových tříd modulo 24 existuje aspoň jeden prvek řádu m.

Příklad 4.4: Určete řád permutace $(1, 2, 4, 5) \circ (3, 7, 8) \circ (6, 9)$, respektive $(1, 2, 4, 5, 3, 6, 7, 9) \circ (3, 7, 8) \circ (6, 2, 9)$.

Příklad 4.5: V dané grupě určete řády všech prvků:
a) $(\mathbb{Z}_7^{\times}, \cdot)$ b) $(\mathbb{Z}_8, +)$ c) $(\mathbb{Z}_6^{\times}, \cdot)$

Příklad 4.6: V grupě $(\mathbb{R}^*, \cdot)$ nalezněte všechny prvky konečného řádu a určete jejich řád.

Příklad 4.7: V grupě $(\mathbb{C}^*, \cdot)$ nalezněte všechny prvky konečného řádu.

Příklad 4.8: Určete všechna $n \in \mathbb{N}$ tak, že v $\mathbb{S}_n$ exituje prvek řádu 26,27,32 a 33.

Příklad 4.9: Určete řád prvku $[k]_n$ v $(\mathbb{Z}_n, +)$.

Příklad 4.10: Dokažte, že konečná pologrupa v níž platí zákony o krácení je grupa.

Příklad 4.11: Udejte příklad tříprvkového grupoidu, který není grupu, ale ptatí v něm zákony o krácení. Ukažte, že grupoid není pologrupou.

5 Podgrupy

Věta 5.1: *Buď H podgrupa grupy $(G, \cdot)$. Pak $\cdot$ určuje operaci na množině H a H je grupa vzhledem k této operaci. Je-li navíc grupa G komutativní, pak i H je komutativní grupa.* [1, Věta 5.3 strana 29]

Věta 5.2: *Buďte H_i podgrupy grupy G, kde i probíhá nějakou množinu $I \neq \emptyset$. Pak $\bigcap_{i \in I} H_i$ je podgrupa v G.* [1, Věta 5.5 strana 29]

Definice 5.3: Buď M podmnožina grupy G. Symbolem $\langle M \rangle$ označíme průnik všech podgrup grupy G obsahujících množinu M. Podle předchozí věty je $\langle M \rangle$ podgrupa grupy G, a sice nejmenší podgrupa grupy G obsahující množinu M. Nazývá se podgrupa *generovaná* množinou M. Množinu M nazýváme množinou *generátorů* grupy $\langle M \rangle$. Pokud $M = \{a_1, \ldots, a_n\}$, pak hovoříme o podgrupě generované prvky $a_1, \ldots a_n$ a označujeme ji stručně $\langle a_1, \ldots a_n \rangle$.
[1, Definice 5.6 strana 30]

Úloha i: Popište všechny podgrupy grupy $(\mathbb{Z}, +)$.

Řešení: Podgrupy jsou tvaru $k \cdot \mathbb{Z} = \{k \cdot a \mid a \in \mathbb{Z}\}, k \in \mathbb{N}_0$.
Důkaz: Nechť jsou tedy všechny podgrupy tvaru $k \cdot \mathbb{Z} = \{k \cdot a \mid a \in \mathbb{Z}\}, k \in \mathbb{N}_0$ a $H \neq \{0\}$ je libovolná podgrupa grupy $(\mathbb{Z}, +)$. Ukažme, že $H = k \cdot \mathbb{Z}$.
Jelikož $H \neq \{0\}$ existuje tedy v H alespoň jedno přirozené číslo. Nechť k je nejmenší z přirozených čísel v H.

1) $k \cdot \mathbb{Z} \subseteq H$. Nechť $a \in \mathbb{Z}$ je libovolné, ukažme, že $k \cdot a \in H$. Je-li $a \in \mathbb{N}$ dokážeme indukcí:

   α) $a = 1$, pak $k \cdot a = k \cdot 1 = k \in H$.

   β) Předpokládejme, že tvrzení platí pro $a = 1, 2, \cdots, n$ a dokážeme pro $a = n + 1$:
   $k \cdot a = k \cdot (n + 1) = k \cdot n + k \in H$.

   Pokud $a < 0$ pak $-k \cdot a = k \cdot (-a) \in H$.

2) $H \subseteq k \cdot \mathbb{Z}$. Nechť $h \in H$ je libovolný. Dělme se zbytkem: $h = k \cdot q + r, q, r \in \mathbb{Z}, 0 \leq r < k$. Z toho, že $r = h - k \cdot q \in H$ plyne $r = 0$.

Úloha ii: Určete podgrupu grupy $(\mathbb{S}_4, \circ)$ generovanou množinou $M = \{(1,2), (1,3)\}$.

Řešení:

- $(1,2) \circ (1,3) = (1,3,2)$
- $(1,2) \circ (1,3,2) = (1,3)$
- $(1,3) \circ (1,3,2) = (3,2)$
- $(1,3,2)^2 = (1,2,3)$

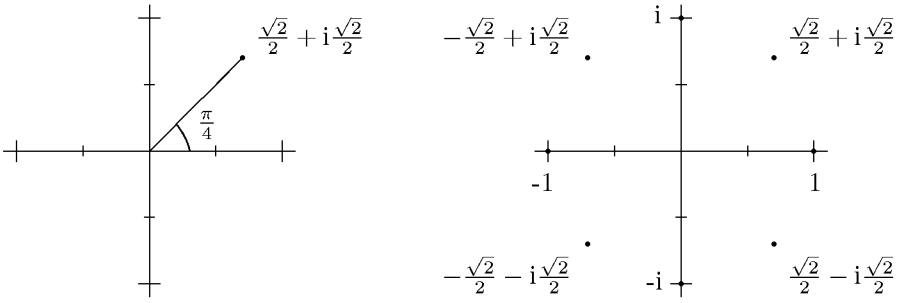
- Dál už nemusíme skládat, protože jsme již vypsali všechny možnosti, proto $\langle M\rangle = \{id, (1,2), (1,3), (2,3), (1,2,3), (1,3,2)\} = \{f \in \mathbb{S}_4 \mid f(4) = 4\}$. Jelikož množina $\langle M\rangle$ je uzavřená vzhledem k operaci $\circ$, obsahuje neutrální prvek a každý prvek v ní má prvek inverzní, je to skutečně podgrupa grupy $(\mathbb{S}_4, \circ)$.

Úloha iii: V grupě $(\mathbb{C}^*, \cdot)$ určete podgrupu generovanou číslem $\frac{\sqrt{2}}{2} + \mathrm{i}\frac{\sqrt{2}}{2}$. Kolik má podgrupa $\langle \frac{\sqrt{2}}{2} + \mathrm{i}\frac{\sqrt{2}}{2}\rangle$ prvků?

Řešení: Nechť $a = \frac{\sqrt{2}}{2} + \mathrm{i}\frac{\sqrt{2}}{2}$, jelikož a je generátorem podgrupy a $a^8 = 1$ (řád prvku a je osm) ihned víme, že podgrupa $\langle \frac{\sqrt{2}}{2} + \mathrm{i}\frac{\sqrt{2}}{2}\rangle$ bude mít osm prvků. Dále můžeme dořešit graficky bod a si vyjádříme v goniometrickém tvaru jako $\cos\frac{\pi}{4} + \mathrm{i}\,\sin\frac{\pi}{4}$ a z *Moivrovy věty* víme, že

$$(\cos\frac{\pi}{4} + \mathrm{i}\,\sin\frac{\pi}{4})^k = (\cos k\frac{\pi}{4} + \mathrm{i}\,\sin k\frac{\pi}{4}).$$

Nyní budeme postupně přičítat úhel $\frac{\pi}{4}$. Vzniklých osm bodů tvoří pravidelný osmiúhelník.



$$\langle \tfrac{\sqrt{2}}{2} + \mathrm{i}\tfrac{\sqrt{2}}{2}\rangle = \{\tfrac{\sqrt{2}}{2} + \mathrm{i}\tfrac{\sqrt{2}}{2},\ \mathrm{i},\ -\tfrac{\sqrt{2}}{2} + \mathrm{i}\tfrac{\sqrt{2}}{2},\ -1,\ -\tfrac{\sqrt{2}}{2} - \mathrm{i}\tfrac{\sqrt{2}}{2},\ -\mathrm{i},\ \tfrac{\sqrt{2}}{2} - \mathrm{i}\tfrac{\sqrt{2}}{2},\ 1\}$$

♣ ♣ ♣ ♣ ♣

TEST:

1. Libovolná podgrupa komutativní grupy je sama komutativní grupou.
2. V grupě nenulových reálných čísel $(\mathbb{R}^*, \cdot)$ existuje konečná netriviální cyklická podgrupa.
3. Každá netriviální grupa má netriviální komutativní podgrupu.
4. V libovolné grupě $(G, \cdot)$ platí, že množina všech prvků $x \in G$, pro které je $x^3 = x^2$, tvoří podgrupu grupy $(G, \cdot)$.
5. V grupě kladných reálných čísel $(\mathbb{R}^+, \cdot)$ existuje netriviální cyklická podgrupa.
6. Každá netriviální podgrupa nekomutativní grupy je nekomutativní.
7. Grupa $(\mathbb{Z}_8, +)$ je cyklická.
8. Grupa $(\mathbb{R}^*, \cdot)$ obsahuje dvouprvkovou podgrupu.

9. Každá konečná cyklická grupa o m prvcích má právě $\varphi(m)$ podgrup.
10. Grupa $(\mathbb{R}, +)$ obsahuje dvouprvkovou podgrupu.
11. Grupa $(\mathbb{C}^*, \cdot)$ obsahuje podgrupu řádu 4.
12. Každá komutativní podgrupa grupy $(\mathbb{S}_n, \circ)$ je cyklická.

Příklad 5.1: Ukažte, že množina $H = \{a + b \cdot i \mid a, b \in \mathbb{Z}\}$, kde $i = \sqrt{-1}$, je podgrupa v grupě $G = (\mathbb{C}, +)$.
Dále nalezněte podgrupu H' grupy G takovou, že $H \subsetneqq H' \subsetneqq \mathbb{C}$.

Příklad 5.2: Popište všechny podgrupy grupy $(\mathbb{S}_3, \circ)$.

Příklad 5.3: V $(\mathbb{Z}_{60})$ určete podgrupu generovanou množinou $\{[6]_{60}, [15]_{60}\}$.

Příklad 5.4: V grupě $(\mathbb{C}^*, \cdot)$ všech nenulových komplexních čísel s operací násobení určete $\langle i, \Theta \rangle$, tj. podgrupu generovanou množinou $\{i, \Theta\}$, kde $i = \sqrt{-1}$ a Θ je řešením rovnice $t^3 = 1$, přičemž $\Theta \neq 1$.
(nápověda: je vhodné uvážit číslo Θ ve tvaru $\Theta = cos\frac{2\pi}{3} + i \cdot sin\frac{2\pi}{3}$)

Příklad 5.5: Určete podgrupu grupy $(\mathbb{S}_8, \circ)$ generovanou množinou X:

a) $X = \{(1,4,5,2) \circ (1,5,2,4,6,3), (1,4,5,2) \circ (4,5,6) \circ (1,3,2)\}$,
b) $X = \{(1,5,8) \circ (1,4,2,5) \circ (1,5,2), (1,2,6,4,8,5) \circ (1,4,6,2)\}$,
c) $X = \{(1,8,2,3,5) \circ (1,2,6,7,8), (4,7,6,2) \circ (2,4,8)\}$,
d) $X = \{(1,2)(3,4), (2,3)(4,5)\}$,
e) $X = \{(2,4,6), (4,7,2), (3,2,4)\}$.

Příklad 5.6: Určete podgrupu $\langle M \rangle$ generovanou množinou

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

v grupě $(\mathbb{A}_4, \circ)$ všech sudých permutací čtyřprvkové množiny $\{1,2,3,4\}$.

Příklad 5.7: Určete podgrupu $\langle M \rangle$ generovanou množinou

$$M = \{([2]_8, [4]_8), ([6]_8, [4]_8)\}.$$

V grupě $(\mathbb{Z}_8, +) \times (\mathbb{Z}_8, +)$. Kolik má podgrupa $\langle M \rangle$ prvků?

Příklad 5.8: V grupách $(\mathbb{R}, +)$ a $(\mathbb{R}^*, \cdot)$ určete podgrupu generovanou prvkem $\sqrt[3]{2}$.

Příklad 5.9: Určete podgrupu grupy $(\mathbb{Z}_7, +)$ generovanou prvkem $[2]_7$.

Příklad 5.10: Ukažte, že dané podmnožiny jsou podgrupy grupy $(\mathbb{R}^*, \cdot)$: a) $\mathbb{R}^+$ b) $\mathbb{Q}^+$ c) $\mathbb{Q}(\sqrt{3}) = \{a + b\sqrt{3} \mid a, b \in \mathbb{Q}\}$.

Příklad 5.11: Popište všechny podgrupy grupy $(\mathbb{Z}_{10}, +)$.

Příklad 5.12: Popište všechny podgrupy grupy $(\mathbb{Z}_n, +)$.

Příklad 5.13: Nechť P je podgrupa grupy $(\mathbb{R}^*, \cdot)$, dokažte, že

$$M_P = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbb{R},\ \det \in P \right\}$$

je podgrupa $(\mathbb{GL}_2(\mathbb{R}), \cdot)$.

Příklad 5.14: Nechť je dána grupa G a její dvě podgrupy H a K. Dokažte, že

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

6 Izomorfismy a součiny grup

Definice 6.1: Buďte G_1, G_2 grupy, $f : G_1 \to G_2$ bijektivni zobrazení. Řekneme, že f je *izomorfismus* grupy G_1 na grupu G_2, jestliže pro libovolné prvky $a,\ b \in G$ platí:

$$f(a) \cdot f(b) = f(a \cdot b).$$

Grupy G_1, G_2 se nazývají *izomorfní*, jestliže existuje izomorfismus $G_1 \to G_2$. Skutečnost, že grupy G_1, G_2 jsou izomorfní, vyjadřujeme zápisem $G_1 \cong G_2$.
[1, Definice 6.1 strana 32]

Věta 6.2: *Buď $f : G_1 \to G_2$ izomorfismus grup. Potom platí:*

$$f(1) = 1$$

a pro libovolný prvek $a \in G_1$ platí:

$$f(a^{-1}) = f(a)^{-1}.$$

[1, Věta 6.4 strana 34]

Věta 6.3: *Libovolná nekonečná cyklická grupa je izomorfní grupě $\mathbb{Z}$. Libovolná konečná cyklická grupa řádu n je izomorfní $\mathbb{Z}_n$.* [1, Věta 6.6 strana 34]

Věta 6.4: *Buďte G_1, G_2 grupy. Definujeme na kartézském součinu $G_1 \times G_2$ množin G_1 a G_2 operaci násobení vztahem*

$$[a, b] \cdot [c, d] = [a \cdot c, b \cdot d].$$

Pak $(G_1 \times G_2, \cdot)$ je grupa.
[1, Věta 6.7 strana 35]

Definice 6.5: Grupa $(G_1 \times G_2, \cdot)$ se nazývá *součinem* grup G_1 a G_2.
[1, Definice 35 strana 35]

Věta 6.6: *Buď G komutativní grupa a H, K její podgrupy takové, že $H \cap K = 1$. Nechť libovolný prvek $a \in G$ lze vyjádřit ve tvaru $a = h \cdot k$, kde $h \in H$, $k \in K$. Pak $G \cong H \times K$.* [1, Věta 6.12 strana 36]

Úloha i: Dokažte, že grupy $(\mathbb{R}^*, \cdot)$ a $(\mathbb{R}^+, \cdot) \times (\mathbb{Z}_2, +)$ jsou izomorfní.

Řešení: Sestrojíme $f : \mathbb{R}^* \to \mathbb{R}^+ \times \mathbb{Z}_2$ předpisem

$$f(r) = \begin{cases} (r, [0]_2), & r > 0 \\ (-r, [1]_2), & r < 0 \end{cases}$$

Nechť $(a, b) \in \mathbb{R}^+ \times \mathbb{Z}_2$ libovolné, $a \in \mathbb{R}^+$ pak $f(a) = (a, [0]_2)$ a $f(-a) = (a, [1]_2)$ z toho plyne, že f je surjektivní.
Nechť $r, s \in \mathbb{R}^*$ takové, že $f(r) = f(s)$, to se nám rozdělí na dva případy

a) $(r, [0]_2) = (s, [0]_2)$ a to je právě, když $r = s$,

b) $(-r, [1]_2) = (-s, [1]_2)$ a to je právě, když $r = s$,

to znamená, že f je i injektvní, a f je tedy bijektivní.
Nechť $r, s \in \mathbb{R}^*$ libovolné, $f(r) \triangle f(s) = (|r|, x) \triangle (|s|, y) = (r \cdot s, x + y)$, kde

$$x = \begin{cases} [0]_2, & r > 0 \\ [1]_2, & r < 0 \end{cases}, \; y = \begin{cases} [0]_2, & s > 0 \\ [1]_2, & s < 0 \end{cases}$$

$$f(r \cdot s) = f(|rs|, z), \text{ kde } z = \begin{cases} [0]_2, & r \cdot s > 0 \\ [1]_2, & r \cdot s < 0 \end{cases}$$

Tím jsme dokázali, že f je izomorfismus.

Úloha ii: Dokažte, že grupa otočení pravidelného čtyřstěnu je izomorfní grupě $(\mathbb{A}_4, \circ)$.

Řešení: Označme si vrcholy pravidelného čtyřstěnu čísly 1, 2, 3, 4. Každé jeho otočení pak můžeme reprezentovat jako permutaci čísel jeho vrcholů. Každé otočení je jednoznačně určeno polohou jedné ze čtyř stěn (čtyři možnosti) a jednoho ze tří vrcholů této stěny (tři možnosti), podle pravidla součinu tedy existuje celkem dvanáct otočení pravidelného čtyřstěnu. Osm z těchto otočení je podle osy procházející vrcholem a těžištěm protilehlé stěny. Tato otočení jsou reprezentována trojcykly (vrchol, jímž prochází osa zůstává na místě). Tři otočení jsou podle os procházejících středy protilehlých stran, ta jsou reprezentována součinem dvojic transpozic. Poslední otočení je identita. Všechny tyto permutace jsou sudé a jejich počet je roven počtu sudých permutací na čtyřprvkové množině. A jistě skládání otočení odpovídá skládání permutací. Tím je dokázáno, že grupa otočení pravidelného čtyřstěnu je izomorfní grupě $(\mathbb{A}_4, \circ)$.

TEST:

1. Libovolné dvě šestiprvkové grupy jsou izomorfní.
2. Součin cyklických grup je vždy cyklickou grupou.
3. Součin dvou nekomutativních grup je opět nekomutativní grupa.
4. Libovolné dvě tříprvkové grupy jsou izomorfní.
5. Existuje nekonečně mnoho grup, které jsou navzájem neizomorfní a přitom každá má právě dvě podgrupy.
6. Součin komutativních grup je opět komutativní grupa.
7. Součin libovolné komutativní a libovolné nekomutativní grupy je nekomutativní grupa.
8. Grupy $(\mathbb{R}, +)$ a $(\mathbb{R}^+, \cdot)$ jsou izomorfní.
9. Grupy $(\mathbb{S}_3, \circ)$ a $(\mathbb{D}_3, \circ)$ jsou izomorfní.

Příklad 6.1: V grupě $(\mathbb{Z}_5 \times \mathbb{S}_8 \times \mathbb{Z}_7^\times, \cdot)$ spočítejte

$$([2]_5, (1,2,3) \circ (4,7), [5]_7) \cdot ([3]_5, (5,8), [2]_7).$$

Příklad 6.2: Nechť $(G, \circ)$ je grupa a a nějaký její pevně zvolený prvek. Dokažte, že potom $(G, \diamond)$ je také grupa, kde operace $\diamond$ je definována předpisem $g \diamond h = g \circ a \circ h$.

Příklad 6.3: Nechť $(A, \circ)$, $(B, *)$ jsou dané grupy. Na množině $A \times B$ definujeme operaci $\Diamond$ takto:

$$(a_1, b_1) \Diamond (a_2, b_2) = (a_1 \circ a_2, b_1 * b_2), \text{ pro } \forall (a_1, b_1), (a_2, b_2) \in A \times B.$$

Dokažte, že:

a) $(A \times B, \Diamond)$ je grupa

b) grupa $(A \times B, \Diamond)$ je komutativní $\Leftrightarrow$ obě grupy $(A, \circ)$, $(B, *)$ jsou komutativní.

Příklad 6.4: Nechť G je grupa, $f : G \to G$ zobrazení, určené předpisem $f(x) = x^{-1}$ pro libovolné $x \in G$. Dokažte, že f je izomorfismus právě, když G je komutativní.

Příklad 6.5: Dokažte, že $(\mathbb{Z}_7^\times, \cdot)$ je izomorfní s $(\mathbb{Z}_6, +)$.

Příklad 6.6: Dokažte, že $(\mathbb{Z}_8^\times, \cdot)$ je izomorfní s $(\mathbb{Z}_2, +) \times (\mathbb{Z}_2, +)$.

Příklad 6.7: Buď $(G, \cdot)$ libovolná konečná grupa. Pro libovolné $a \in G$ definujeme zobrazení $\psi_a : G \to G$ předpisem $\psi_a(x) = a \cdot x \cdot a^{-1}$. Dokažte, že pro libovolné $a \in G$ je ψ_a izomorfismus grup.

Příklad 6.8: Dokažte, že pro libovolné grupy G a H jsou grupy $G \times H$ a $H \times G$ izomorfní.

Příklad 6.9: Nechť $f : G \to H$ je izomorfismus grup. Ukažte, že řády prvku a a $f(a)$ jsou stejné.

7 Lagrangeova věta

Definice 7.1: Buď G grupa, H její podgrupa, $a \in G$. Množinu

$$a \cdot H = \{a \cdot h \mid h \in H\}$$

nazýváme *levá třída* grupy G podle podgrupy H (určená prvkem a).
[1, Věta 7.1 strana 37]

Věta 7.2: *Buď G grupa, H její podgrupa, $a,\ b \in G$. Pak následující tvrzení jsou ekvivalentní:*

(1) $a \cdot H = b \cdot H$,

(2) $a \in b \cdot H$,

(3) $b^{-1} \cdot a \in H$.

[1, Věta 7.2 strana 37]

Věta 7.3: (Lagrnageova věta) *Řád podgrupy konečné grupy G je dělitelem řádu grupy G.* [1, Věta (Lagrangeova věta) strana 39]

Věta 7.4: (Fermatova věta) *Buď G konečná grupa řádu n, nechť $a \in G$. Pak $a^n = 1$.* [1, Věta (Fermatova věta) strana 39]

Věta 7.5: (Eulerova věta) *Buď n přirozené číslo, buď a celé číslo nesoudělné s n.Pak*

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

[1, Věta (Euler) strana 39]

Úloha i: Dokažte, že pro každé přirozené číslo n je číslo $2^{2^{4n+1}} + 7$ složené.

Řešení: Při důkazu, že je číslo složené (lze zapsat jako součin konečného počtu prvočísel) je nejjednodušší najít alespoň jedno prvočíslo, které toto číslo dělí. Zkusíme si dosadit nízká n, tak můžeme odhadnout která prvočísla by to mohla být. Výsledky si zapíšeme do tabulky:

n	$2^{2^{4n+1}} + 7$
0	11
1	$4294967303 = 11 \cdot 390451573$
2	$11 \cdot \ldots$

Zdá se, že by to mohla být např. 11. Musíme tedy zjistit jestli $11 \mid 2^{2^{4n+1}} + 7$. Z důsledku Lagrangeovy věty [1, Důsledek 7.8] víme, že řád čísla 2 dělí $|\mathbb{Z}_{11}| = \varphi(11) = 10$ a jelikož 2 ani 5 nejsou řádem čísla 2 modulo 11 je jím 10. Při dalším řešení využijeme následující věty.
Nechť $m \in \mathbb{N}$, $a \in \mathbb{Z}$, $(a, m) = 1$. Označme r řád čísla a modulo m. Pak pro libovolná $t, s \in \mathbb{N}_0$ platí

$$a^t \equiv a^s \pmod{m} \Leftrightarrow t \equiv s \pmod{r}.$$

Musíme tedy zjistit s čím je kongruentní 2^{4n+1} modulo 10.
Víme, že $2^{4n} \equiv 1 \pmod 5$, podle pravidel pro počítání s kongruencemi víme, že můžeme obě strany kongruence a modul vynásobit tímtéž přirozeným číslem. Tedy

$$\begin{aligned} 2^{4n} &\equiv 1 \pmod 5 \quad / \cdot 2 \\ 2^{4n+1} &\equiv 2 \pmod{10} \end{aligned}$$

z čehož podle uvedené věty plyne

$$\begin{aligned} 2^{2^{4n+1}} &\equiv 2^2 \pmod{11} \quad / + 7 \\ 2^{2^{4n+1}} + 7 &\equiv 4 + 7 \pmod{11} \\ 2^{2^{4n+1}} + 7 &\equiv 0 \pmod{11} \end{aligned}$$

čímž jsme dokázali, že číslo $2^{2^{4n+1}} + 7$ je složené.

Úloha ii: Určete zbytek po dělení čísla $2^{50} + 3^{50} + 4^{50}$ číslem 17.

Řešení: $[2^{50} + 3^{50} + 4^{50}]_{17} = [2^{50}]_{17} + [3^{50}]_{17} + [4^{50}]_{17} = [2]_{17}^{50} + [3]_{17}^{50} + [4]_{17}^{50}$

- $[4]_{17}^2 = [16]_{17} = [-1]_{17}$
  $[4]_{17}^4 = [-1]_{17}^2 = [1]_{17}$
  $[4]_{17}^{50} = [4]_{17}^{4 \cdot 12+2} = ([4]_{17}^4)^{12} \cdot [4]_{17}^2 = [-1]_{17}$
- $[2]_{17}^8 = [4]_{17}^4 = [1]_{17}$
  $[2]_{17}^{50} = [2]_{17}^{8 \cdot 6+2} = ([2]_{17}^8)^6 \cdot [2]_{17}^2 = [4]_{17}$
- $[3]_{17}^2 = [9]_{17}$
  $[3]^3 = [27]_{17} = [10]_{17}$
  $[3]_{17}^4 = [30]_{17} = [-4]_{17}$
  $[3]^16_{17} = ([3]_{17}^4)^4 = [-4]_{17}^4 = [1]_{17}$
  $[3]^{50} = [3]_{17}^{3 \cdot 16+2} = ([3]_{17}^{16})^3 \cdot [3]_{17}^2 = [9]_{17}$
- $2^{50} + 3^{50} + 4^{50} = [4]_{17} + [-1]_{17} + [9]_{17} = [12]_{17}$
  Zbytek je tedy 12.

Úloha iii: Popište rozklad grupy $(\mathbb{R}^*, \cdot)$ podle podgrupy $\mathbb{R}^+$.

Řešení: Popsat rozklad znamená zjistit, kdy dvě čísla budou patřit do stejné třídy rozkladu. Nechť tedy $a,\ b \in \mathbb{R}^*$ libovolné a zjišťujeme kdy $a \cdot \mathbb{R}^+ = b \cdot \mathbb{R}^+$ to je podle *věty 7.2* právě, když $b^{-1} \cdot a \in \mathbb{R}^+$ a to může nastat ve dvou případech

a) $b^{-1} > 0$ což v grupě $\mathbb{R}^*$ znamená, že $b > 0$ a současně $a > 0$ nebo

b) $b^{-1} < 0$ tedy, že $b < 0$ a současně $a < 0$

Dvě čísla patří do stejné třídy rozkladu právě, když mají stejné znaménko a rozklad grupy $(\mathbb{R}^*, \cdot)$ podle podgrupy $\mathbb{R}^+$ je tedy na třídy obsahující kladná, respektive záporná reálná čísla, nebo-li $\mathbb{R}^*/\mathbb{R}^+ = \{\mathbb{R}^+, \mathbb{R}^-\}$.

♣ ♣ ♣ ♣ ♣

TEST:

1. Řád grupy $(\mathbb{Z}_7, +)$ je 7.
2. Řád grupy $(\mathbb{Z}_8^*, \cdot)$ je 8.
3. Pro každou grupu G, která je řádu 1, platí, že obsahuje pouze neutrální prvek.
4. Řády grupy $(\mathbb{Z}_{10}, +)$ a grupy $(\mathbb{Z}_{11}^*, \cdot)$ jsou rovny 10.
5. Řády grupy $(\mathbb{Z}_n, +)$ a grupy $(\mathbb{Z}_{n+1}^*, \cdot)$ jsou shodné pro libovolné $n \in \mathbb{N}$.
6. Řády grupy $(\mathbb{Z}_{p-1}, +)$ a grupy $(\mathbb{Z}_p^*, \cdot)$ jsou shodné pro libovolné prvočíslo p.

Příklad 7.1: Určete zbytek po dělení čísla 5^{20} číslem 3.

Příklad 7.2: Určete zbytek po dělení daných čísel číslem 17:
a) $5^{40} + 6^{40} + 7^{40} + 8^{40}$ b) $4^{4^4} + 5^{5^5}$ c) $13^{13^{13}} + 14^{14^{14}}$.

Příklad 7.3: Dokažte, že pro libovolné $n \in \mathbb{N}$ je číslo $2^{2^{2n+1}} + 3$ číslo složené.

Příklad 7.4: Popište rozklad grupy $(\mathbb{R}^*, \cdot)$ podle podgrupy $\{-1, 1\}$.

Příklad 7.5: Popište rozklad grupy $(\mathbb{Z}, +)$ podle podgrupy $\langle 2 \rangle$.

Příklad 7.6: Popište levý rozklad grupy $(\mathbb{A}_4, \circ)$ sudých permutací na množině $\{1, 2, 3, 4\}$ podle podgrupy generované permutací $(1, 4, 2)$.

Příklad 7.7: Určete počet levých tříd grupy $(\mathbb{Z}, +) \times (\mathbb{Z}, +)$ podle podgrupy $H = \{(m, n) \mid 6 \mid (m - 2n)\}$.

Příklad 7.8: Popište levý rozklad grupy $(\mathbb{Z}_{16}, +)$ podle podgrupy $4\mathbb{Z} = \{4 \cdot a \mid a \in \mathbb{Z}\}$.

Příklad 7.9: Určete levý rozklad grupy $(\mathbb{GL}_2(\mathbb{Z}_2), \cdot)$ všech regulárních matic nad $\mathbb{Z}_2$ podle podgrupy

$$H = \left\{ \begin{pmatrix} [1]_2 & [0]_2 \\ [0]_2 & [1]_2 \end{pmatrix}, \begin{pmatrix} [1]_2 & [1]_2 \\ [1]_2 & [0]_2 \end{pmatrix} \right\}.$$

8 Homomorfismy grup

Definice 8.1: Buď $f : G_1 \to G_2$ homomorfismus grup. Množina

$$J(f) = \{x \in G \mid f(x) = 1\}$$

se nazývá *jádro homomorfismu* f. [1, Definice 8.1 strana 41]

Definice 8.2: Buď $f : G_1 \to G_2$ surjektivní homomorfismus. Pak grupa G_2 se nazývá *homomorfní obraz* grupy G_1. [1, Definice 8.7 strana 42]

Definice 8.3: Buď $f : G_1 \to G_2$ homomorfismus grup. Množina

$$J(f) = \{x \in G_1 \mid f(x) = 1\}$$

se nazývá *jádro homomorfismu* f. [1, Definice 8.10 strana 42]

Věta 8.4: *Homomorfismus $f : G_1 \to G_2$ je injektivní právě, když $J(f) = \{1\}$.* [1, Věta 8.11 strana 43]

Úloha i: Je dán předpis $f : (\mathbb{Z}_3, +) \to (\mathbb{S}_4, \circ)$, kde $f([a]_3) = (1,2) \circ (3,4) \circ (1,2,3)^a$, rozhodněte, zda korektně zadává zobrazení a zda se jedná o homorfismus.

Řešení: Zjistit zda se jedná o korektně zadané zobrazení znamená dokázat, že nezáleží na volbě reprezentantů téže zbytkové třídy. To znamená zjistit zda platí rovnost $f([a]_3) = f([a+3k]_3),\ k \in \mathbb{Z}$. Ale $(1,2) \circ (3,4) \circ (1,2,3)^{a+3k} = (1,2) \circ (3,4) \circ (1,2,3)^a$, protože $(1,2,3)$ je řádu 3. Rovnost tedy platí a předpis korektně definuje zobrazení.
Nyní zjistíme, zda se jedná o homomorfismus. Nebo-li ověříme platnost rovnosti

$$f([a]_3 + [b]_3) = f([a]_3) \circ f([b]_3),$$

$f([a]_3 + [b]_3) = (1,2) \circ (3,4) \circ (1,2,3)^{a+b} = (1,2) \circ (3,4) \circ (1,2,3)^a \circ (1,2,3)^b$.
$f([a]_3) \circ f([b]_3) = (1,2) \circ (3,4) \circ (1,2,3)^a \circ (1,2) \circ (3,4) \circ (1,2,3)^b$.
Vidíme, že dané zobrazení není homomorfismus.

TEST:

1. Pro libovolné dvě grupy $(G, \cdot)$ a $(H, \cdot)$ existuje homomorfismus grupy $(G, \cdot)$ do grupy $(H, \cdot)$.
2. Homomorfismus grup je injektvní, je-li jeho jádro jednoprvkové.
3. Libovolný surjektivní homomorfismus grup má alespoň dvouprvkové jádro.
4. Existuje surjektivní homomorfismus grupy konečného řádu do grupy nekonečného řádu.

5. Pro libovolné dvě grupy $(G, \cdot)$ a $(H, \cdot)$ existuje surjektivní homomorfismus grupy $(G, \cdot)$ do grupy $(H, \cdot)$.
6. Pro každý homomorfismus platí, že jeho jádro obsahuje neutrální prvek.
7. Je-li $f : G \to G$ homomorfismus grup, pak pro každý prvek $a \in G$ platí, že prvky a a $f(a)$ mají stejný řád.
8. Pro libovolnou grupu $(G, \cdot)$ platí, že množina všech homomorfismů $f : G \to G$ spolu s operací skládání zobrazení je pologrupa s neutrálním prvkem.

Příklad 8.1: Rozhodněte, zda dané předpisy korektně definují zobrazení a zda se jedná o homomorfismus nebo dokonce izomorfismus grup.

a) $\alpha : (\mathbb{Z}_4, +) \times (\mathbb{Z}_3, +) \to (\mathbb{Z}_{12}, +)$, kde $\alpha(([a]_4, [b]_3)) = [a - b]_{12}$,
b) $\beta : (\mathbb{Z}_4, +) \times (\mathbb{Z}_3, +) \to (\mathbb{Z}_{12}, +)$, kde $\beta(([a]_4, [b]_3)) = [6a + 4b]_{12}$,
c) $\gamma : (\mathbb{Z}_3^*, \cdot) \times (\mathbb{Z}_5, +) \to (\mathbb{Z}_5, +)$, kde $\gamma(([a]_3, [b]_5)) = [b^{|a|}]_5$,
d) $\delta : (\mathbb{Z}_{15}) \to (\mathbb{Z}_5, +) \times (\mathbb{Z}_3, +)$, kde $\delta([a]_{15}) = ([a]_5, [a]_3)$,
e) $\epsilon : (\mathbb{Q}^*, \cdot) \to (\mathbb{Q}^*, \cdot)$, kde $\epsilon(p/q) = q/p$.

Příklad 8.2: Určete obrazy a jádra homomorfismů z předešlého příkladu.

Příklad 8.3: Dokažte, že zobrazení α grupy $(\mathbb{Z}_{30}, +)$ do grupy $(\mathbb{Z}_{20}, +)$ definovaný předpisem $\alpha([a]_{30}) = [6a]_{20}$ je homomorfismus grup, dále dokažte, že zobrazení β grupy $(\mathbb{Z}_{20}, +)$ do grupy $(\mathbb{S}_6, \circ)$ definovaný předpisem $\beta([a]_{20}) = = (1, 2, 3, 4, 5)^b$ je také homomorfismus grup. Nakonec určete jádra homomorfismů

a) $J(\alpha)$ b) $J(\beta)$ c) $J((\beta \circ \alpha))$.

Příklad 8.4: Homomorfismus α grupy $(\mathbb{Z}_6, +)$ do grupy $(\mathbb{S}_6, \circ)$ je dán předpisem $\alpha([a]_6) = (1, 2, 3) \circ (1, 2, 3)^\alpha \circ (1, 2, 3)$ pro libovolné celé číslo a. Homomorfismus β grupy $(\mathbb{Z}_3, +) \times (\mathbb{Z}_4, +)$ do grupy $(\mathbb{Z}_6, +)$ je dán předpisem $\beta(([b]_3, [c]_4)) = [2b + 3c]_6$ pro libovolná celá čísla b, c. Určete následující jádra homomorfismů.

a) $J(\alpha)$ b) $J(\beta)$ c) $J((\alpha \circ \beta))$.

Příklad 8.5: Spočtěte jádro a obraz homomorfismu α z grupy $(\mathbb{Z}_{36}^\times, \cdot)$ do grupy $(\mathbb{Z}_{108}^\times, \cdot)$ daného předpisem $\alpha([a]_{36}) = [27a - 26]_{108}$, kde $a \in \mathbb{Z}$.

Příklad 8.6: Dokažte, že předpis $f[a]_{20} = (1, 2, 3, 4, 5)^a$ definuje homomorfismus $f : (\mathbb{Z}_{20}, +) \to (\mathbb{S}_7, \circ)$.

Příklad 8.7: Nechť G je grupa, $f : G \to G$ zobrazení, určené předpisem $f(x) = x \cdot x$ pro libovolné $x \in G$. Dokažte, že f je izomorfismus právě,když G je komutativní.

Příklad 8.8: Buď $(G, \cdot)$ libovolná konečná grupa. Pro libovolné $a \in G$ definujeme zobrazení $\psi_a : G \to G$ předpisem $\psi_a(x) = a \cdot x \cdot a^{-1}$. Dokažte, že zobrazení $\Psi : G \to \mathbb{S}(G)$ dané předpisem $\Psi(a) = \psi_a$ je homomorfismus grupy $(G, \cdot)$ do grupy $(\mathbb{S}(G), \circ)$ všech permutací množiny G.

Příklad 8.9: Uvažme grupu $(G, \cdot)$ matic typu 3/3 nad $\mathbb{Z}$, které jsou následujícího tvaru

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

kde $\cdot$ je násobení matic. Definujeme nyní zobrazení $f : (G, \cdot) \to (\mathbb{Z}, +)$, 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.

Příklad 8.10: Popište všechny homomorfismy grupy $(\mathbb{S}_3, \circ)$ do grupy $(\mathbb{Z}_8, +)$. Kolik jich je?

9 Faktorové grupy

Definice 9.1: Podgrupa H grupy G se nazývá *normální*, jestliže

$$a \cdot h \cdot a^{-1} \in H$$

pro libovolné prvky $a \in G,\ h \in H$. [1, Definice 9.1 strana 45]

Věta 9.2: *Buď G grupa, H její normální podgrupa. Pak zobrazení*

$$p : G \to G/H \text{ dané vztahem } p(a) = a \cdot H$$

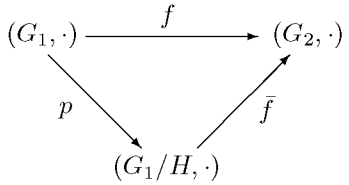
je surjektivní homomorfismus. Jeho jádro je rovno H. [1, Věta 9.5 strana]

Definice 9.3: Grupa $(G/H, \cdot)$ se nazývá *faktorová grupa* grupy G podle podgrupy H. Homomorfismus p se nazývá *projekce* grupy G na faktorovou grupu G/H. [1, Definice 9.6 strana 46]

Věta 9.4: (Hlavní věta o faktorových grupách) *Buď $f : G_1 \to G_2$ homomorfismus grup a H normální podgrupa v G_1 taková, že $H \subseteq J(f)$. Pak existuje jediný homomorfismus $\bar{f} : G_1/H \to G_2$, jehož složení*

$$\bar{f} \circ p : G_1 \to G_1/H \to G_2$$

s projekcí p je rovno homomorfismu f.



[1, Věta 9.10 (Hlavní věta o faktorových grupách) strana 47]

Věta 9.5: *Buď $f : G_1 \to G_2$ surjektivní homomorfismus grup. Pak grupy G_2 a $G_1/J(f)$ jsou izomorfní.* [1, Věta 9.11 strana 48]

Úloha i: Rozhodněte zda podgrupa generovaná transpozicí $(1, 2)$ je normální podgrupa v $(\mathbb{S}_3, \circ)$.

Řešení: Transpozice $(1, 2)$ generuje podgrupu $H = \{(1, 2), \mathrm{id}\}$ grupy $(\mathbb{S}_3, \circ)$. Protože platí

$$(1, 2, 3) \circ (1, 2) \circ (3, 2, 1) = (2, 3) \notin H,$$

není podgrupa H normální.

Úloha ii: Uvažme grupu všech regulárních matic řádu 2 s racionálními prvky $(\mathbb{GL}_2(\mathbb{Q}), \cdot)$. Označme $\mathbb{SL}_2(\mathbb{Q})$ množinu všech těch matic z $\mathbb{GL}_2(\mathbb{Q})$, které mají determinant 1:

$$\mathbb{SL}_2(\mathbb{Q}) = \{A \in \mathbb{GL}_2(\mathbb{Q}) \mid |A| = 1\}.$$

a) Dokažte, že množina $\mathbb{SL}_2(\mathbb{Q})$ je podgrupou grupy $\mathbb{GL}_2(\mathbb{Q})$.

b) Dokažte, že množina $\mathbb{SL}_2(\mathbb{Q})$ je normální podgrupou grupy $\mathbb{GL}_2(\mathbb{Q})$.

c) Popište, jak vypadá a čemu je izomorfní faktorgrupa $\mathbb{GL}_2(\mathbb{Q})/\mathbb{SL}_2(\mathbb{Q})$.

Řešení:

ad a) Nechť $A,\ B \in \mathbb{SL}_2(\mathbb{Q})$ libovolné. Pak $|A \cdot B| = |A| \cdot |B| = 1 \cdot 1 = 1$ a množina $\mathbb{SL}_2(\mathbb{Q})$ je tedy uzavřena k operaci násobení matic.
Jistě $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in \mathbb{SL}_2(\mathbb{Q})$.
Jelikož pro libovolnou regulární matici A ptatí $|A^{-1}| = |A|^{-1}$ tak také pro každou matici $B \in \mathbb{SL}_2(\mathbb{Q})$ platí, že $B^{-1} \in \mathbb{SL}_2(\mathbb{Q})$.
Dokázali jsme, že $\mathbb{SL}_2(\mathbb{Q})$ je skutečně podgrupou $(\mathbb{GL}_2(\mathbb{Q}), \cdot)$.

ad b) Nechť $A \in (\mathbb{GL}_2(\mathbb{Q}), \cdot),\ H \in \mathbb{SL}_2(\mathbb{Q})$. $|A \cdot H \cdot A^{-1}| = |A| \cdot |H| \cdot |A^{-1}| = |A| \cdot |A^{-1}| = 1$. Množina $\mathbb{SL}_2(\mathbb{Q})$ je pak normální podgrupa $(\mathbb{GL}_2(\mathbb{Q}), \cdot)$.

ad c) Popsat jak vypadá rozklad $\mathbb{GL}_2(\mathbb{Q})/\mathbb{SL}_2(\mathbb{Q})$, znamená určit, kdy dvě matice $A,\ B \in \mathbb{GL}_2(\mathbb{Q})$ leží ve stejné třídě rozkladu.
Tedy kdy $A \cdot \mathbb{SL}_2(\mathbb{Q}) = B \cdot \mathbb{SL}_2(\mathbb{Q})$, to je podle *věty 7.2* právě, když $B^{-1} \cdot A \in \mathbb{SL}_2(\mathbb{Q})$ tedy, když $|B^{-1} \cdot A| = 1$, což je ekvivalentní $|B^{-1}| \cdot |A| = 1$ a to je shodné s $|A| = |B|$. Dvě matice tedy náleží do stejné třídy rozkladu pokud mají stejný determinant.
Abychom mohli zjistit čemu je izomorfní faktorgrupa $\mathbb{GL}_2(\mathbb{Q})/\mathbb{SL}_2(\mathbb{Q})$ musíme najít surjektivní homomorfismus grup $h : \mathbb{GL}_2(\mathbb{Q}) \to K$ jehož jádrem je $\mathbb{SL}_2(\mathbb{Q})$. Jelikož již víme jak vypadá rozklad $\mathbb{GL}_2(\mathbb{Q})/\mathbb{SL}_2(\mathbb{Q})$, určíme grupu K a předpis h tak, že zjistíme, jak na množině $\mathbb{GL}_2(\mathbb{Q})/\mathbb{SL}_2(\mathbb{Q})$ vypadá operace $\cdot$.
Označíme si $M_r = \{A \mid |A| = r,\ r \in \mathbb{Q}^*\}$ třídu rozkladu, jejíž matice mají determinant rove r.
Nechť $A \in M_a,\ |A| = a$ a $B \in M_b,\ |B| = b$ libovolné, pak $A \cdot B = C$, jelikož $|A| \cdot |B| = |A \cdot B| = |C| = a \cdot b$, a tedy $C \in M_{a \cdot b}$.
Operace $\cdot$ na množině $\mathbb{GL}_2(\mathbb{Q})/\mathbb{SL}_2(\mathbb{Q})$ tedy vypadá jako násobení čísel v grupě $(\mathbb{Q}^*, \cdot)$. Potom zbývá dokázat, že

$$h : (\mathbb{GL}_2(\mathbb{Q}), \cdot) \to (\mathbb{Q}^*, \cdot),\ h(A) = |A|$$

je surjektivní homomorfismus, jehož jádrem je $\mathbb{SL}_2(\mathbb{Q})$.

1. Homomorfismus: $h(A \cdot B) = |A \cdot B| = |A| \cdot |B| = h(A) \cdot h(B)$,
2. h je surjektivní: zřejmé,
3. $J(h) = \mathbb{SL}_2(\mathbb{Q})$: $J(h) = \{A \in \mathbb{GL}_2(\mathbb{Q}) \mid |A| = 1\} = \mathbb{SL}_2(\mathbb{Q})$.

Tím jsme dokázali, že $\mathbb{GL}_2(\mathbb{Q})/\mathbb{SL}_2(\mathbb{Q})$ je izomorfní $\mathbb{Q}^*$.

Úloha iii: Nalezněte čemu je izomorfní faktorgrupa komplexních čísel podle podgrupy realných čísel ($\mathbb{C}/\mathbb{R} \cong ?$).

Řešení: Stejně jako v předešlé úloze musíme najít surjektivní homomorfismus $h : (\mathbb{C}, +) \to (K, \cdot)$ jehož jádrem je $\mathbb{R}$. Grupa $(K, \cdot)$ je pak ona hledaná grupa izomorfní faktorgrupě $(\mathbb{C}/\mathbb{R}, +)$.
Grupu K a předpis h opět určíme tak, že zjistíme jak vypadá rozklad $\mathbb{C}/\mathbb{R}$ a jak na něm vypadá operace $+$. Rozklad určíme následovně:
Nejprve si napíšeme jak vypadají levé třídy rozkladu

$$(a + i \cdot b) + \mathbb{R} = \{(a + i \cdot b) + r \mid r \in \mathbb{R}\},$$

nyní zjistíme, kdy dvě komplexní čísla $(a + i \cdot b)$ a $(\bar{a} + i \cdot \bar{b})$ patří do stejné třídy rozkladu. Tedy, kdy $(a + i \cdot b) + \mathbb{R} = (\bar{a} + i \cdot \bar{b}) + \mathbb{R}$.
To je právě, když $(-\bar{a} - i \cdot \bar{b}) + (a + i \cdot b) \in \mathbb{R}$ a to je jen tehdy, když $b - \bar{b} = 0$ nebo-li $b = \bar{b}$. Označíme si $\mathbb{R}_b = \{a + i \cdot b \mid a \in \mathbb{R}\}$ pak $\mathbb{C}/\mathbb{R} = \{\mathbb{R}_b \mid b \in \mathbb{R}\}$.
Protože $\mathbb{R}_b \cdot \mathbb{R}_{\bar{b}} = \{a + i \cdot b \mid a \in \mathbb{R}\} \cdot \{\bar{a} + i \cdot \bar{b} \mid \bar{a} \in \mathbb{R}\} = \{(a + \bar{a}) + i \cdot (b + \bar{b})\} = \mathbb{R}_{b+\bar{b}}$, vidíme, že hledanou grupou K je $(\mathbb{R}, +)$ a předpis

$$h : (\mathbb{C}, +) \to (\mathbb{R}, +), \ h(a + i \cdot b) = b.$$

Zbývá tedy dokázat, že h je surjektivní homomorfismus s $J(h) = \mathbb{R}$.

1. Homomorfismus: $h((x + i \cdot y) + (a + i \cdot b)) = h(x + y + i \cdot (y + b)) = x + a = \\ = h(x + i \cdot y) + h(a + i \cdot b)$,
2. h je surjektivní: zřejmé,
3. $J(h) = \mathbb{R}$: $J(h) = \{(a + i \cdot b) \in \mathbb{C} \mid h(a + i \cdot b) = 0, \ a, b \in \mathbb{R}\} = \\ = \{a + i \cdot b \mid a \in \mathbb{R}, b = 0\} = \mathbb{R}$.

Tím jsme dokázali, že $(\mathbb{C}/\mathbb{R}, +) \cong (\mathbb{R}, +)$.

TEST:

1. Libovolná faktorgrupa cyklické grupy je cyklickou grupou.
2. V libovolné grupě platí, že každá její normální podgrupa je komutativní.
3. Je-li $f : G \to H$ homomorfismus grupy $(G, \cdot)$ do grupy $(H, \cdot)$, potom grupa $(H, \cdot)$ je izomorfní s nějakou faktorgrupou grupy $(G, \cdot)$.
4. V libovolné grupě platí, že každá její podgrupa je normální.
5. V libovolné grupě platí, že každá její komutativní podgrupa je normální.
6. Pro libovolnou grupu $(G, \cdot)$ a libovolnou její normální podgrupu H platí: Je-li $(H, \cdot)$ komutativní, potom je faktorgrupa $(G/H, \cdot)$ komutativní.

Příklad 9.1: Rozhodněte, zda je $\langle M \rangle$ normální podgrupa grupy $(\mathbb{S}_4, \circ)$, $M = \{(1, 3), (3, 4)\}$.

Příklad 9.2: Mějme následující podgrupy grupy $(\mathbb{S}_6, \circ)$

$$G = \{f \in \mathbb{S}_6 \mid f \text{ sudá}\}$$
$$H = \{f \in G \mid f(3) = 3\}$$

tedy $H \subset G \subset \mathbb{S}_6$. Rozhodněte, 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 $(\mathbb{S}_6, \circ)$

Příklad 9.3: V komutativní grupě $(G, \cdot)$ uvažme podmnožinu D všech prvků, jejichž druhá mocnina je neutrální prvek e:

$$D = \{x \in G \mid x \cdot x = e\}.$$

Dokažte, že D je

a) podgrupa grupy $(G, \cdot)$,

b) normální podgrupa grupy $(G, \cdot)$.

Příklad 9.4: Popište všechny normální podgrupy grup $(\mathbb{S}_3, \circ)$ a $(\mathbb{A}_4, \circ)$. Ukažte, že grupa $(\mathbb{A}_n, \circ)$ je normální podgrupa grupy $(\mathbb{S}_n, \circ)$ pro libovolné $n \in \mathbb{N}$.

Příklad 9.5: Buď dána grupa $(G, \circ)$ nekonstantních lineárních zobrazení reálných čísel

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

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

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

Která z nich je normální podgrupou grupy $(G, \circ)$?

Příklad 9.6: Uvažujme normální podgrupu grupy $(G, +) = (\mathbb{Z}, +) \times (\mathbb{Z}, +)$ definovanou takto:

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

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

Určete, která grupa $(K, \cdot)$ je izomorfní faktorgrupě G/H, dále definujte vhodné zobrazení $\varphi : G \to K$, pro něž dokážete, že φ je surjektivní homomorfismus grup, jehož jádrem je H.

Příklad 9.7: V komutativní grupě $(G, \cdot)$ s neutrálním prvkem e uvažme podmnožinu K všech prvků grupy G konečného řádu, tedy

$$K = \{x \mid \exists n \in \mathbb{N}\ |x^n = e\}.$$

Dokažte, že

a) K je normální podgrupa grupy $(G, \cdot)$,

b) ve faktorgrupě $(G/K, \cdot)$ mají všechny prvky (mimo neutrální) stejný řád.

Příklad 9.8: Uvažme množiny reálných čísel $G = \{3^p 15^q \mid p, q \in \mathbb{Z}\}$, a $H = \{3^r \mid r \in \mathbb{Z}\}$ a operaci $\cdot$ (násobení reálných čísel). Zřejmě $(G, \cdot)$ je grupa.

a) ukažte, že H je normální podgrupa v G,

b) popište faktorgrupu G/H, které grupě je izomorfní?

Příklad 9.9: Nechť je dána grupa matic $(G, \cdot)$ (s operací násobení matic) a její normální podgrupa H. Určete faktorgrupu G/H:

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

Příklad 9.10: Víme, že množina

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

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 množiny 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 $\begin{pmatrix} \bar{\varepsilon} & \bar{a} \\ 0 & 1 \end{pmatrix}$ 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 $\alpha : G \to K$ pro něž dokažte, že α je surjektivní homomorfismus grup, jehož jádrem je H.

Příklad 9.11: Nechť $(G, \cdot)$ je grupa. Pro libovolné $a,\ b \in G$ definujeme $[a, b] = = a^{-1} \cdot b^{-1} \cdot a \cdot b$. Dokažte, že množina

$$\bar{G} = \{[a_1, b_1] \cdot \cdots \cdot [a_n, b_n] \mid n \in \mathbb{N},\ a_1, \ldots a_n, b_1, \ldots, b_n \in g\}$$

je normální podgrupa grupy G a že faktorgrupa $(G, \cdot)/(\bar{G}, \cdot)$ je komutativní.

10 Konečné grupy

Definice 10.1: Množina

$$C = \{a \in G \mid a \cdot x = x \cdot a \text{ pro libovolné } x \in G\}$$

se nazývá *centrum* grupy G. [1, Definice 10.4 strana 49]

Věta 10.2:(Sylow) *Buď G konečná grupa a p prvočíslo takové, že jeho $k-$tá mocnina dělí řád grupy G. Pak G obsahuje podgrupu řádu p^k.*
[1, Věta 10.8 (Sylow) strana 50]

Věta 10.3:(Sylow) *Buď G konečná grupa, p prvočíslo a k největší celé číslo takové, že p^k dělí řád grupy G. Buď r počet podgrup řádu p^k v grupě G. Pak $r \equiv 1 \bmod p$.* [1, Věta 10.8 (Sylow) strana 50]

Definice 10.4: Nechť p je prvočíslo a G je konečná komutativní grupa. *p-Sylowská podgrupa* grupy G je libovolná její podgrupa o p^k prvcích, kde k je největší přirozené číslo s vlastností $p^k \mid |G|$.

Definice 10.5: Buď p prvočíslo. Grupy řádu p^k, kde $k > 0$, se nazývají *p-grupy.* [1, Definice 10.11 strana 52]

Věta 10.6: *Buď G konečná komutativní grupa, $|G| > 1$. Pak*

$$G \cong \mathbb{Z}_{p_1^{k_1}} \times \cdots \times \mathbb{Z}_{p_m^{k_m}},$$

kde $p_1, \ldots, p_m$ jsou prvočísla a $k_1, \ldots, k_m$ jsou přirozená čísla. Tento rozklad grupy G na součin netriviálních cyklických p-grup je určen jednoznačně, až na pořadí činitelů. [1, Věta 10.13 strana 52]

♣ ♣ ♣ ♣ ♣

Úloha i: Popište všechny (až na izomorfismus) komutativní grupy o 12 prvcích.

Řešení: Vyřešit tento příklad znamená, zjistit kolika způsoby mohu číslo 12 napsat jako součin mocnin prvočísel (ne nutně různých).
$12 = 2^2 \cdot 3 = 2 \cdot 2 \cdot 3$. Existují tedy právě dvě komutativní grupy o 12 prvcích: $\mathbb{Z}_4 \times \mathbb{Z}_3$ a $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3$.

Úloha ii: Nalezněte všechny 3-Sylowské podgrupy grupy $(\mathbb{S}_5, \circ)$.

Řešení: $|\mathbb{S}_5| = 5! = 120 = 2^3 \cdot 3 \cdot 5$
Největší mocnina trojky, která dělí 120 je 3^1. 3-Sylowská podgrupa bude mít tedy tři prvky. Je to například podgrupa $\langle(1,2,3)\rangle = \langle(1,3,2)\rangle$.
Označme si S množinu všech 3-Sylowských podgrup.

$$S = \{\langle(k,l,m)\rangle \mid k,l,m \in \{1,2,3,4,5\} \wedge k \neq l \neq m\}.$$

$|S| = \binom{5}{3} = \frac{5!}{3! \cdot 2!} = \frac{120}{12} = 10$, existuje tedy deset 3-Sylowských podgrup grupy $(\mathbb{S}_5, \circ)$

♣ ♣ ♣ ♣ ♣

TEST:

1. Je-li počet prvků nějaké grupy prvočíslo, pak je tato grupa komutativní.
2. Každá konečná komutativní grupa je izomorfní vhodnému součinu konečných cyklických grup.
3. Každá konečná grupa je izomorfní s grupou permutací vhodné neprázdné konečné množiny.

Příklad 10.1: Určete centrum grupy

a) $(\mathbb{S}_3, \circ)$ všech permutací tříprvkové množiny

b) $(\mathbb{Z}_7, +)$ zbytkových tříd modulo 7

c) $(\mathbb{GL}_2(\mathbb{Q}), \cdot)$ regulárních matic 2×2 nad racionálními čísly.

Příklad 10.2: Popište všechny (až na izomorfismus) komutativní grupy o 120 prvcích.

Příklad 10.3: Kolik existuje komutativních grup o 32 prvcích (až na izomorfismus)?

Příklad 10.4: Nalezněte alespoň jednu 2-Sylowskou podgrupu grupy $(\mathbb{S}_5, \circ)$.

Výsledky příkladů

1 Pojem grupy

TEST: 1.ano, 2.ne, 3.ne.

1.1 a) ne, b) ano, c) ne, d) ano.

1.3

a) není komutativní, není asociativní, nemá neutrální prvek,

b) není komutativní, není asociativní, prvek d je neutrální.

1.4

$\cdot$	e	f	g
e	f	g	e
f	g	e	f
g	e	f	g

1.6 $(G, \circ)$ je nekomutativní pologrupa, která nemá neutrální prvek. Bude-li množina G jednoprvková pak $(G, \circ)$ bude komutativní pologrupa s neutrálním prvkem.

1.7 a) ano, b) ne, c) ne, d) ano, e) ano, f) ano.

1.8 Je asociativní, neexistuje neutrální prvek, není grupou.

1.9 Je asociativní, neexistuje neutrální prvek, není grupou.

1.10

$\circ$	f_1	f_2	f_3	f_4	f_5	f_6
f_1	f_1	f_2	f_3	f_4	f_5	f_6
f_2	f_2	f_1	f_6	f_5	f_4	f_3
f_3	f_3	f_5	f_1	f_6	f_2	f_4
f_4	f_4	f_6	f_5	f_1	f_3	f_2
f_5	f_5	f_3	f_4	f_2	f_6	f_1
f_6	f_6	f_4	f_2	f_3	f_1	f_5

1.11 Ano, jedná se o grupu.

2 Permutace

TEST: 1.ano, 2.ano, 3.ne, 4.ne, 5.ne, 6.ne, 7.ne.

2.1

a) $f = (1,9,5)\circ(2,3,7)\circ(4,8,6)$, $g = (1,8,4,2)\circ(3,5,6)$, $h = (1,6,7,2,9,5,4,3)$,

b) $p(f) =$ sudá, $p(g) =$ lichá, $p(h) =$ lichá,

c) $f^{100} \circ g^{100} = (3,1,9,5,4,8,6,7,2)$.

2.2

a) $u = (1,3,7,8,6,9,5)\circ(2,4)$, $v = (1,5,3)\circ(6,8)$, $w = (1,8,9,2)\circ(3,4,6,7,5)$

b) $u\circ v = (2,4)\circ(5,7,8,9)$, $v\circ u = (2,4)\circ(3,7,6,9)$, $w\circ v = (1,3,8,7,5,4,6,9,2)$,

c) $u \circ v \circ w = (1,8,9,4) \circ (2,6) \circ (3,5)$, $w \circ v \circ w = (1,7,4,9) \circ (2,3,6,5,8)$,
$v \circ w \circ u = (1,4,5,6,2,8,7,9)$,

d) $v^{103} = (1,5,3) \circ (6,8)$,

e) $w^{27} = (1,2,9,8) \circ (3,6,5,4,7)$,

f) $u^{120} \circ v^{-3} = (1,3,7,8,9,5)$,

g) $v^{32} \circ w^{32} = (1,6) \circ (1,3) \circ (4,5) \circ (4,7)$, sudá

h) $u = (1,5) \circ (1,9) \circ (1,6) \circ (1,8) \circ (1,7) \circ (1,3) \circ (2,4)$, lichá
$v = (1,3) \circ (1,5) \circ (6,8)$, lichá
$w = (1,2) \circ (1,9) \circ (1,8) \circ (3,5) \circ (3,7) \circ (3,6) \circ (3,4)$, lichá.

2.3 $u^{-1} = (1,5,9,6,8,7,3) \circ (2,4)$, $v^{-1} = (1,3,5) \circ (6,8)$,
$w^{-1} = (1,2,9,8) \circ (3,5,7,6,4)$.

2.4 Sudá.

2.5 $f_1 = (1,3,2,4)$, $f_2 = (1,4,2,3)$, $f_3 = (1,3,2,4) \circ (5,6)$,
$f_4 = (1,4,2,3) \circ (5,6)$.

2.6 $a_1 = (1,4,2,5,3,6)$, $a_2 = (1,5,2,6,3,4)$, $a_3 = (1,6,2,4,3,5)$,
$a_4 = (1,3,2) \circ (4,6,5)$, $a_5 = (1,4,2,5,3,6) \circ (7,8)$,
$a_6 = (1,5,2,6,3,4) \circ (7,8)$, $a_7 = (1,6,2,4,3,5) \circ (7,8)$,
$a_8 = (1,3,2) \circ (4,6,5) \circ (7,8)$.

2.7 $f = (2,4,5)^{-1} \circ (1,3)^{-1} \circ (1,4)^{-1} = (1,2,5,4,3)$.

3 Grupy zbytkových tříd

TEST: 1.ano, 2.ne, 3.ne, 4.ne, 5.ano, 6.ano.

3.1 $(111,107) = 1$, $1 = 27 \cdot 111 - 28 \cdot 107$.

3.2 $n \neq 9 + 17 \cdot k \mid k \in \mathbb{Z}$.

3.3 $[49]^{-1}_{1000} = [449]_{1000}$.

3.4 Existuje, je to zbytková třída $[20]_{103}$.

3.5 a) 1020, b) 2160.

3.6 a) 504, b) 720, c) 1210.

3.7 $n = 3$.

3.9 a) $[1 + (2^k + 1)(2^{k-1})]_{2^{2k}+1}$, b) $[1 + (2^k - 1)(2^{k-1})]_{2^{2k}+1}$, c) $[1 + \frac{m^3-m}{2}]_{m^3-1}$.

3.10 $m = \{19, 27, 38, 54\}$.

3.11 a) 16, b)96, c) 3600.

3.12 a) 539, b) 39.

4 Základní vlastnosti grup

TEST: 1.ne, 2.ano, 3.ne, 4.ne, 5.ne, 6.ano, 7.ne, 8.ano, 9.ne, 10.ano, 11.ano, 12.ano.

4.1 4.

4.2 Řád matice A je 4, řád matice B je ∞.

4.3 $m \in \{1, 2, 3, 4, 6, 8, 12, 24\}$.

4.4 12, respektive 14.

4.5 a)

Prvek	Řád
$[1]_7$	1
$[2]_7$	3
$[3]_7$	6
$[4]_7$	3
$[5]_7$	6
$[6]_7$	2

b)

Prvek	Řád
$[0]_6$	1
$[1]_6$	6
$[2]_6$	3
$[3]_6$	2
$[4]_6$	3
$[5]_6$	6

c)

Prvek	Řád
$[1]_6$	1
$[5]_6$	2

4.6 Číslo 1 je řádu 1, číslo -1 je řádu 2, ostatní čísla jsou řádu ∞.

4.7 $\{\frac{\sqrt{2}}{2} + \mathrm{i}\frac{\sqrt{2}}{2},\ \mathrm{i},\ -\frac{\sqrt{2}}{2} + \mathrm{i}\frac{\sqrt{2}}{2},\ -1,\ -\frac{\sqrt{2}}{2} - \mathrm{i}\frac{\sqrt{2}}{2},\ -\mathrm{i},\ \frac{\sqrt{2}}{2} - \mathrm{i}\frac{\sqrt{2}}{2},\ 1\}$

4.9 Označme $d = (n, k)$, pak řád prvku je $\frac{n}{d}$.

5 Podgrupy

TEST: 1.ano, 2.ano, 3.ano, 4.ano, 5.ano, 6.ne, 7.ano, 8.ano, 9.ne, 10.ne, 11.ano. 12.ne.

5.2 $\mathbb{S}_3$, $\{\mathrm{id}\}$, $\{\mathrm{id}, (1,2)\}$, $\{\mathrm{id}, (1,3)\}$, $\{\mathrm{id}, (2,3)\}$, $\{\mathrm{id}, (1,2,3), (1,3,2)\}$.

5.3 $\langle [3]_{60} \rangle$.

5.5 a) $\langle X \rangle = \langle \{, 1, 2, 5) \circ (4, 6, 3), (1, 3) \circ (2, 4) \circ (5, 6) \}$, b) $\langle X \rangle = \langle \{(1, 8, 5), (2, 4)\} \rangle$,
c) $\langle X \rangle = \langle \{(1, 3, 5), (2, 6, 7), (4, 8)\} \rangle$,
d) $\langle X \rangle = \{(1, 2, 4, 5, 3)^i \circ ((1, 2) \circ (3, 4))^j \mid i = 0, 1, 2, 3, 4 \mid j = 0, 1\}$,
e) $\langle X \rangle = \{f \in \mathbb{A}_8 \mid f(1) = 1, f(5) = 5, f(8) = 8\}$.

5.6 $\langle M \rangle = \mathbb{A}_4$.

5.7 $\langle M \rangle = \{([0]_8, [0]_8), ([2]_8, [4]_8), ([4]_8, [0]_8), ([6]_8, [4]_8)\} = \langle ([2]_8, [4]_8) \rangle$, $|\langle M \rangle| = 4$.

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

5.9 $(\mathbb{Z}_7, +)$.

6 Izomorfismy a součiny grup

TEST: 1.ne, 2.ne, 3.ano, 4.ano, 5.ano, 6.ano, 7.ano, 8.ano, 9.ano.

6.1 $([0]_5, (1, 2, 3) \circ (4, 7) \circ (5, 8), [3]_7)$.

7 Lagrangeova věta

TEST: 1.ano, 2.ne, 3.ano, 4.ano, 5.ne, 6.ano.

7.1 1.

7.2 a) 15, b) 13, c) 9.

7.4 $\mathbb{R}^*/\{1, -1\} = \{\{a, -a\} \mid a \in \mathbb{R}^*\}$.

7.5 $\mathbb{Z}_2$.

7.6 $\big\{\{(1, 2) \circ (3, 4), (2, 3, 4), (1, 3, 4)\}$, $\{(1, 3) \circ (2, 4), (1, 4, 3), (1, 2, 3)\}$, $\{(1, 4) \circ (2, 3), (1, 3, 2), (2, 4, 3)\}\big\}$.

7.7 6.

7.8 $\{\{[0]_{16},[4]_{16},[8]_{16},[12]_{16}\},\{[1]_{16},[5]_{16},[9]_{16},[13]_{16}\},\{[2]_{16},[6]_{16},[10]_{16},[14]_{16}\},$
$\{[3]_{16},[7]_{16},[11]_{16},[15]_{16}\}\}$

7.9 $\left\{H,\quad \left\{\begin{pmatrix}[0]_2 & [1]_2\\ [1]_2 & [0]_2\end{pmatrix},\begin{pmatrix}[0]_2 & [1]_2\\ [1]_2 & [1]_2\end{pmatrix}\right\},\quad \left\{\begin{pmatrix}[1]_2 & [0]_2\\ [1]_2 & [1]_2\end{pmatrix},\begin{pmatrix}[1]_2 & [1]_2\\ [1]_2 & [0]_2\end{pmatrix}\right\}\right\}$

8 Homomorfismy grup

TEST: 1.ano, 2.ano, 3.ne, 4.ne, 5.ne, 6.ano, 7.ne, 8.ano.

8.1 a) není zobrazení, b) homomorfismus, c) není zobrazení, d) izomorfismus, e) izomorfismus.

8.2 b) $O(\beta)=,\ J(\beta)=\{[a]_4,[b]_3\ |12\mid 6a+4b\}$,
d) $O(\delta)=(\mathbb{Z}_5,+)\times(\mathbb{Z}_3,+),\ J(\delta)=\{[0]_{15}\}$, e) $O(\epsilon)=(\mathbb{Q}^*,\cdot),\ J(\epsilon)=\{1\}$.

8.3 a) $J(\alpha)=\{[a]_{30}\mid 20\mid 6a\}$, b) $J(\beta)=\{[b]_{20}\mid 5\mid b\}$,
c) $J(\beta\circ\alpha)=5\mathbb{Z}_{30}$.

8.4 a) $J(\alpha)=\{[1]_6,[4]_6\}$, b) $J(\beta)=\{[b]_3,[c]_4\mid 6\mid 2b+3c\}$,
c) $J(\alpha\circ\beta)=\{([2]_3,[0]_4),([1]_3,[2]_4\}$.

8.5 $J(\alpha)=\{[a]_{36}\mid a\in\mathbb{Z},\ (a,36)=1,\ [27a-36]_{108}=[1]_{108}\}=\{[1]_{36},[5]_{36},[13]_{36},[17]_{36},[25]_{36},[29]_{36}\}$,
$O(\alpha)=\{[27a-36]_{108}\mid a\in\mathbb{Z},\ (a,36)=1\}=\{[1]_{108},[55]_{108}\}$.

8.10 Právě dva.

9 Faktorové grupy

TEST: 1.ano, 2.ne, 3.ne, 4.ne, 5.ne, 6.ne.

9.1 Není.

9.2 a) ne, b) ne, c) ano.

9.5 S.

9.6 a) $K=(\mathbb{Z}_2,\mathbb{Z}_3),\ \varphi((a,b))=([a]_2,[b]_3)$
b) $K=(\mathbb{Z}_7),\ \varphi((a,b))=([2\cdot a+3\cdot b]_7)$

9.8 b) Dvě čísla patří do stejné třídy rozkladu, pravě když
$p+q=\bar{p}+\bar{q}$, $G/H\cong\mathbb{Z}$.

9.9 $\mathbb{Z}_2\times\mathbb{Z}_2$.

9.10 Dvě matice patří do stejné třídy rozkladu právě, když $\epsilon=\bar{\epsilon}$ a $2\mid a+\bar{a}$,je izomorfní grupě $\mathbb{Z}^*\times\mathbb{Z}_2$.

10 Konečné grupy

TEST: 1.ano, 2.ano, 3.ne.

10.1 a) $\{\mathrm{id}\}$, b) $\{\mathbb{Z}_7\}$, c) $\left\{ \begin{pmatrix} k & 0 \\ 0 & k \end{pmatrix} \mid k \in \mathbb{Q}^* \right\}$.

10.2 $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5$, $\mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_4 \times \mathbb{Z}_5$, $\mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_8$.

10.3 7.

10.4 Jsou to osmiprvkové podgrupy, např. $\{\mathrm{id}, (1,3), (2,4), (1,2,3,4), (1,4,3,2), (1,2)\circ (3,4), (1,4)\circ(2,3)\}$ - grupa symetrií čtverce.

Literatura

[1] J. Rosický: *Algebra*, MU, Brno 2002, 4.vydání

[2] O. Klíma: *Cvičení - jaro 2003*, www.math.muni.cz/∼klima

[3] R. Kučera: *Písemky ke zkoušce z minulých let*, www.math.muni.cz/∼kucera

[4] P. Horák: *Cvičení z algebry a teoretické aritmetiky I*, MU, Brno 1998, 2.vydání

[5] J. Weil: *Rozpracovaná řešení úloh z vyšší algebry*, Academia, Praha 1987

[6] G. Birkhoff, S. Mac Lane: *Prehľad modernej algebry* (slovenský překlad), ALFA, Bratislava společně s SNTL, Praha 1979

[7] O. Borůvka: *Základy teorie grupoidů a grup*, Československá akademia věd, Praha 1962