Základy algebry

Martin Kuřil

Abstrakt

Tento studijní text je ve fázi přípravy. Z toho plynou 2 věci: 1. Text obsahuje chyby (doufám, že jich není mnoho a že nejsou zásadní). Za chyby se omlouvám a budu rád, pokud mne na ně upozorníte. 2. Text bude nadále upravován, především budou přidávány další kapitoly.

I když text ještě není hotov, domnívám se, že může dobře sloužit jako studijní text.

Text je vhodný pro samostudium a jako studijní opora pro studenty distanční a kombinované formy studia. V textu jsou vyloženy základy teorie grup od zavedení pojmu grupy až po některé hlubší výsledky (Sylowova věta, popis všech konečných komutativních grup). Dále budou postupně vyloženy základy teorie okruhů. Výklad je veden ve volném tempu a je provázen mnoha příklady. Důkazy tvrzení a vět jsou až nezvykle podrobné.

Obsah

GRUPY

1 Základní pojmy teorie grup

1.1 Definice grupy

V celém textu budeme používat následující označení pro číselné množiny:

- $\mathbb{N}$ značí množinu všech přirozených čísel bez nuly, $\mathbb{N} = \{1, 2, 3, \dots\}$
- $\mathbb{N}_0$ značí množinu všech přirozených čísel s nulou, $\mathbb{N}_0 = \{0, 1, 2, 3, \dots\}$
- $\mathbb{Z}$ značí množinu všech celých čísel, $\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$
- $\mathbb{Q}$ značí množinu všech racionálních čísel
- $\mathbb{R}$ značí množinu všech reálných čísel
- $\mathbb{C}$ značí množinu všech komplexních čísel
- $\mathbb{Z}^+$ značí množinu všech kladných celých čísel
- $\mathbb{Q}^+$ značí množinu všech kladných racionálních čísel
- $\mathbb{R}^+$ značí množinu všech kladných reálných čísel
- $\mathbb{S}$ značí množinu všech sudých celých čísel, $\mathbb{S} = \{\dots, -4, -2, 0, 2, 4, \dots\}$
- $\mathbb{Q}^\times$ značí množinu všech racionálních čísel bez nuly
- $\mathbb{R}^\times$ značí množinu všech reálných čísel bez nuly
- $\mathbb{C}^\times$ značí množinu všech komplexních čísel bez nuly

Mohutnost (kardinalitu) množiny M budeme značit $card(M)$. Specielně, jestliže M je konečná množina, pak $card(M)$ označuje počet prvků množiny M.

V kapitole 1 jsou opravdu uvedeny základní pojmy a poznatky. Dále, v průběhu výkladu, je budeme používat zcela běžně, velmi často bez odkazu na příslušnou definici, tvrzení či větu.

1.1.1. Definice. Nechť A je množina. Zobrazení množiny $A \times A$ do množiny A se nazývá **(binární) operace** na množině A. Je-li $*$ operace na množině A, pak místo $*((x, y))$ píšeme $x * y$ (pro všechna $x, y \in A$).

1.1.2. Definice. Nechť $*$ a $\square$ jsou binární operace na množině A.

1. Říkáme, že operace $*$ je **asociativní**, pokud pro všechna $x, y, z \in A$ platí
$$x * (y * z) = (x * y) * z.$$

2. Říkáme, že operace $*$ je **komutativní**, pokud pro všechna $x, y \in A$ platí
$$x * y = y * x.$$

3. Říkáme, že operace $\square$ je **distributivní** vzhledem k operaci $*$, pokud pro všechna $x, y, z \in A$ platí
$$x\square(y * z) = (x\square y) * (x\square z),\ (y * z)\square x = (y\square x) * (z\square x).$$

4. Nechť $e \in A$. Říkáme, že e je **neutrální prvek** operace $*$, pokud pro všechna $x \in A$ platí
$$e * x = x,\ x * e = x.$$

5. Nechť $e, x, y \in A$, e je neutrální prvek operace $*$. Říkáme, že prvek y je **inverzní** (**inverze**) k prvku x vzhledem k operaci $*$, pokud platí
$$x * y = e,\ y * x = e.$$

1.1.3. Tvrzení.

1. *Každá operace má nejvýše jeden neutrální prvek.*

2. *Pro každou asoociativní operaci s neutrálním prvkem platí: Ke každému prvku existuje nejvýše jeden prvek inverzní.*

Důkaz.

1. Nechť $*$ je operace na množině A. Nechť e_1, e_2 jsou neutrální prvky operace $*$. Chceme: $e_1 = e_2$. Počítejme: $e_1 = e_1 * e_2 = e_2$ (první rovnost plyne z toho, že e_2 je neutrální, druhá rovnost plyne z toho, že e_1 je neutrální).

2. Nechť $*$ je asociativní operace na množině A s neutrálním prvkem e. Nechť $x, y_1, y_2 \in A$, y_1 a y_2 jsou inverze k x. Chceme: $y_1 = y_2$. Počítejme:

$$y_1 = y_1 * e = y_1 * (x * y_2) = (y_1 * x) * y_2 = e * y_2 = y_2.$$

V případě binárních operací se velmi často používá multiplikativní nebo aditivní symbolika.

Multiplikativní symbolika: Operace se značí $\cdot$ a nazývá se násobení. Neutrální prvek se značí 1 a nazývá se jednotkový prvek. Inverzní prvek k prvku x se značí x^{-1} nebo $\frac{1}{x}$.

Aditivní symbolika: Používá se především pro komutativní operace. Operace se značí $+$ a nazývá se sčítání. Neutrální prvek se značí 0 a nazývá se nulový prvek. Inverzní prvek k prvku x se značí $-x$ a nazývá se opačný prvek k prvku x.

1.1.4. Definice. Grupa je množina spolu s binární operací, jež je asociativní, má neutrální prvek a každý prvek má prvek inverzní.

1.1.5. Tvrzení. *Nechť G je grupa, $x, y \in G$. Platí:*

1. $(x^{-1})^{-1} = x$
2. $(x \cdot y)^{-1} = y^{-1} \cdot x^{-1}$

(Použili jsme multiplikativní symboliku.)

Důkaz.

1. *Důkaz přenecháváme čtenáři.*
2. *Je třeba ukázat, že platí dvě rovnosti:* $(x \cdot y) \cdot (y^{-1} \cdot x^{-1}) = 1$, $(y^{-1} \cdot x^{-1}) \cdot (x \cdot y) = 1$. *Počítejme:*
   $(x \cdot y) \cdot (y^{-1} \cdot x^{-1}) = x \cdot (y \cdot y^{-1}) \cdot x^{-1} = x \cdot 1 \cdot x^{-1} = x \cdot x^{-1} = 1,$
   $(y^{-1} \cdot x^{-1}) \cdot (x \cdot y) = y^{-1} \cdot (x^{-1} \cdot x) \cdot y = y^{-1} \cdot 1 \cdot y = y^{-1} \cdot y = 1.$

Nyní tři poznámky k terminologii a jedna k symbolice:

1. Grupa s jedním prvkem se nazývá **triviální**. Grupy, které mají více než jeden prvek, se nazývají **netriviální**.

2. Říkáme, že grupa je **komutativní** (neboli Abelova), pokud binární operace v grupě je komutativní.

3. Počet prvků konečné grupy G nazýváme **řád grupy** G. Tedy řád grupy G je číslo $card(G)$.

4. Jestliže používáme multiplikativní symboliku, pak místo $x \cdot y$ často píšeme xy (týká se to samozřejmě libovolných prvků x, y).

1.1.6. Tvrzení. (zákony o krácení) *Buď G grupa, $x, y, z \in G$. Pak platí:*

1. *Jestliže $xy = xz$, pak $y = z$.*

2. *Jestliže $yx = zx$, pak $y = z$.*

Důkaz.

1. Nechť $xy = xz$. Pak

$$y = 1y = (x^{-1}x)y = x^{-1}(xy) = x^{-1}(xz) = (x^{-1}x)z = 1z = z.$$

2. Obdobně jako část 1.

Nechť G je konečná grupa řádu n, $G = \{a_1, a_2, \ldots, a_n\}$. **Multiplikativní tabulka** (tabulka násobení) grupy G je následující schéma:

	a_1	a_2	$\ldots$	a_n
a_1	$a_1 \cdot a_1$	$a_1 \cdot a_2$	$\ldots$	$a_1 \cdot a_n$
a_2	$a_2 \cdot a_1$	$a_2 \cdot a_2$	$\ldots$	$a_2 \cdot a_n$
$\vdots$	$\vdots$			
a_n	$a_n \cdot a_1$	$a_n \cdot a_2$	$\ldots$	$a_n \cdot a_n$

V každém řádku multiplikativní tabulky jsou vypsány v určitém pořadí všechny prvky grupy G. Zdůvodnění: Nechť $i \in \{1, 2, \ldots, n\}$. Tvrdíme, že prvky $a_i \cdot a_1, a_i \cdot a_2, \ldots, a_i \cdot a_n$ jsou navzájem různé. Kdyby tomu tak nebylo, bylo by $a_i \cdot a_k = a_i \cdot a_l$ pro nějaká $k, l \in \{1, 2, \ldots n\}$, $k \neq l$. Pak by ovšem bylo $a_k = a_l$, $k = l$ (užili jsme zákon o krácení), což by byl spor.

Obdobně platí, že v každém sloupci multiplikativní tabulky jsou vypsány v určitém pořadí všechny prvky grupy G.

Bývá zvykem sestrojovat multiplikativní tabulku tak, že a_1 je neutrální prvek.

1.1.7. Příklad. Buď $G \subseteq \mathbb{C}$, $G = \{1, i, -1, -i\}$. Snadno se lze přesvědčit, že pro všechna $x, y \in G$ je $x \cdot y \in G$ (operace násobení je zde obvyklé násobení komplexních čísel). Tudíž: násobení komplexních čísel je operace na množině G. Tato operace je asociativní, má neutrální prvek 1 a ke každému prvku existuje prvek inverzní ($1^{-1} = 1$, $i^{-1} = -i$, $(-1)^{-1} = -1$, $(-i)^{-1} = i$). Právě jsme ověřili, že G spolu s operací násobení komplexních čísel je grupa. Sestrojíme multiplikativní tabulku grupy G:

	1	i	-1	$-i$
1	1	i	-1	$-i$
i	i	-1	$-i$	1
-1	-1	$-i$	1	i
$-i$	$-i$	1	i	-1

Uvedeme nyní několik málo příkladů grup. V této souvislosti upozorňujeme, že celá druhá kapitola tohoto studijního textu je věnována příkladům grup.

1.1.8. Příklad.

1. Množiny $\mathbb{S}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ spolu s operací sčítání jsou nekonečné komutativní grupy. Neutrálním prvkem je číslo 0.

2. Množiny $\mathbb{Q}^\times$, $\mathbb{R}^\times$, $\mathbb{C}^\times$, $\mathbb{Q}^+$, $\mathbb{R}^+$ spolu s operací násobení jsou nekonečné komutativní grupy. Neutrálním prvkem je číslo 1.

3. Příkladem konečné grupy je grupa triviální, tj. grupa obsahující pouze neutrální prvek 1. Netriviální konečná grupa je například grupa řádu 4 uvedená v 1.1.7.

1.2 Mocniny

1.2.1. Definice. Nechť G je grupa, $a \in G$, k je kladné celé číslo. Klademe

$$a^k = \underbrace{a \cdot a \ldots a \cdot a}_{k}.$$

1.2.2. Tvrzení. *Nechť G je grupa, $a \in G$, k, l jsou kladná celá čísla. Pak platí:*

1. $a^k \cdot a^l = a^{k+l}$
2. $(a^k)^l = a^{k \cdot l}$

Důkaz.

1. $a^k \cdot a^l = (\underbrace{a \ldots a}_{k}) \cdot (\underbrace{a \ldots a}_{l}) = \underbrace{a \ldots a}_{k+l} = a^{k+l}$
2. $(a^k)^l = \underbrace{(\underbrace{a \ldots a}_{k}) \cdot (\underbrace{a \ldots a}_{k}) \ldots (\underbrace{a \ldots a}_{k})}_{l} = \underbrace{a \ldots a}_{k \cdot l} = a^{k \cdot l}$

1.2.3. Tvrzení. *Nechť G je grupa, $a \in G$, k je kladné celé číslo. Pak platí:*

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

Důkaz. Postupujme indukcí vzhledem ke k.

1. Nechť $k = 1$. Platí: $(a^{-1})^1 = a^{-1}$, $(a^1)^{-1} = a^{-1}$.
2. Nechť $k \geq 1$. Indukční předpoklad: $(a^{-1})^k = (a^k)^{-1}$.
   Chceme: $(a^{-1})^{k+1} = (a^{k+1})^{-1}$. Počítejme:

$$(a^{k+1})^{-1} = (a^k \cdot a)^{-1} = a^{-1} \cdot (a^k)^{-1} = a^{-1} \cdot (a^{-1})^k = (a^{-1})^{k+1}.$$

1.2.4. Definice. Nechť G je grupa, $a \in G$, k je záporné celé číslo. Klademe

$$a^0 = 1,\ a^k = (a^{-1})^{-k} = (a^{-k})^{-1}.$$

1.2.5. Věta. *Nechť G je grupa, $a \in G$, k, l jsou celá čísla. Pak platí:*

1. $a^k \cdot a^l = a^{k+l}$
2. $(a^k)^l = a^{k \cdot l}$

Důkaz.

1. Jestliže $k = 0$, pak
   $a^k \cdot a^l = a^0 \cdot a^l = 1 \cdot a^l = a^l$,
   $a^{k+l} = a^{0+l} = a^l$.
   Jestliže $l = 0$, pak
   $a^k \cdot a^l = a^k \cdot a^0 = a^k \cdot 1 = a^k$,
   $a^{k+l} = a^{k+0} = a^k$.
   Nechť tedy $k \neq 0$, $l \neq 0$. Rozdělíme důkaz do čtyř částí:
   (I) $k > 0$, $l > 0$
   (II) $k > 0$, $l < 0$
   (III) $k < 0$, $l > 0$
   (IV) $k < 0$, $l < 0$
   ad (I): Tvrzení plyne z 1.2.2.
   ad (II): Rozdělíme důkaz do tří částí:
   (a) $k > -l$
   (b) $k = -l$
   (c) $k < -l$
   ad (a): $a^k \cdot a^l = \underbrace{a \dots a}_{k} \cdot \underbrace{a^{-1} \dots a^{-1}}_{-l} = a^{k-(-l)} = a^{k+l}$
   ad (b): $a^k \cdot a^l = \underbrace{a \dots a}_{k} \cdot \underbrace{a^{-1} \dots a^{-1}}_{-l} = 1 = a^0 = a^{k+l}$
   ad (c): $a^k \cdot a^l = \underbrace{a \dots a}_{k} \cdot \underbrace{a^{-1} \dots a^{-1}}_{-l} = (a^{-1})^{-l-k} = (a^{-1})^{-(k+l)} = a^{k+l}$
   ad (III): Rozdělíme důkaz do tří částí:
   (a) $-k < l$
   (b) $-k = l$

(c) $-k > l$
ad (a): $a^k \cdot a^l = \underbrace{a^{-1} \dots a^{-1}}_{-k} \cdot \underbrace{a \dots a}_{l} = a^{l-(-k)} = a^{k+l}$
ad (b): $a^k \cdot a^l = \underbrace{a^{-1} \dots a^{-1}}_{-k} \cdot \underbrace{a \dots a}_{l} = 1 = a^0 = a^{k+l}$
ad (c): $a^k \cdot a^l = \underbrace{a^{-1} \dots a^{-1}}_{-k} \cdot \underbrace{a \dots a}_{l} = (a^{-1})^{-k-l} = (a^{-1})^{-(k+l)} = a^{k+l}$
ad (IV): $a^k \cdot a^l = (a^{-1})^{-k} \cdot (a^{-1})^{-l} = (a^{-1})^{(-k)+(-l)} = (a^{-1})^{-(k+l)} = a^{k+l}$.

2. Jestliže $k = 0$, pak
$(a^k)^l = (a^0)^l = 1^l = 1$,
$a^{k \cdot l} = a^{0 \cdot l} = a^0 = 1$.
Jestliže $l = 0$, pak
$(a^k)^l = (a^k)^0 = 1$,
$a^{k \cdot l} = a^{k \cdot 0} = a^0 = 1$.
Nechť tedy $k \neq 0$, $l \neq 0$. Rozdělíme důkaz do čtyř částí:
(I) $k > 0$, $l > 0$
(II) $k > 0$, $l < 0$
(III) $k < 0$, $l > 0$
(IV) $k < 0$, $l < 0$.
ad (I): Tvrzení plyne z 1.2.2.
ad (II): $(a^k)^l = ((a^k)^{-l})^{-1} = (a^{k \cdot (-l)})^{-1} = (a^{-(k \cdot l)})^{-1} = a^{k \cdot l}$
ad (III): $(a^k)^l = ((a^{-1})^{-k})^l = (a^{-1})^{(-k) \cdot l} = (a^{-1})^{-(k \cdot l)} = a^{k \cdot l}$
ad (IV): $(a^k)^l = ((a^{-1})^{-k})^l = (((a^{-1})^{-k})^{-l})^{-1} = ((a^{-1})^{(-k) \cdot (-l)})^{-1} = ((a^{-1})^{k \cdot l})^{-1} = ((a^{k \cdot l})^{-1})^{-1} = a^{k \cdot l}$.

1.2.6. Definice. Nechť G je grupa, $a \in G$. Jestliže existuje kladné celé číslo k takové, že $a^k = 1$, pak **řád prvku** a je $\min\{k \in \mathbb{N} |\ a^k = 1\}$. Jestliže pro všechna kladná celá čísla k je $a^k \neq 1$, pak **řád prvku** a je ∞.

1.2.7. Tvrzení. *Nechť G je konečná grupa řádu n. Pak všechny prvky grupy G mají konečný řád menší nebo rovný číslu n. (Poznámka: Uvidíme později, že řád každého prvku grupy G dělí číslo n.)*

Důkaz. Buď $a \in G$. Prvky $1, a, a^2, \dots, a^n$ nemohou být navzájem různé, neboť by to znamenalo, že G má více než n prvků. Existují tedy $i, j \in \{0, 1, \dots, n\}$ tak, že $a^i = a^j$, $i < j$. Pak $a^i \cdot a^{-i} = a^j \cdot a^{-i}$, $a^0 = a^{j-i}$, $1 = a^{j-i}$. Položme $k = j - i$. Je k celé číslo, $k > 0$, $a^k = 1$, $k \leq n$. Zřejmě tedy prvek a má řád menší nebo roven číslu n.

1.2.8. Příklad.

1. Pro každý prvek a grupy G platí:
   prvek a má řád 1 právě tehdy, když $a = 1$.

2. V libovolné grupě jsou řády prvků a, a^{-1} stejné. Zdůvodnění: Nechť k je celé číslo. Pak
   $a^k = 1$ právě tehdy, když $(a^{-1})^k = 1$.

1.2.9. Poznámka. Při použití aditivní symboliky místo a^n píšeme na. Buď a prvek grupy $\mathbb{C}$ (s operací sčítání), buď n celé číslo. Pak $na = n \cdot a$ (zde $n \cdot a$ označuje součin celého čísla n a komplexního čísla a). Zdůvodnění rozdělíme na 3 případy:
(I) $n = 0$
(II) $n > 0$
(III) $n < 0$.
ad (I): $0a = 0$ (viz definici 1.2.4.), $0 \cdot a = 0$
ad (II): $na = \underbrace{a + \cdots + a}_{n} = (\underbrace{1 + \cdots + 1}_{n}) \cdot a = n \cdot a$
ad (III): $na = (-n)(-a) = (-n) \cdot (-a) = n \cdot a$.

1.2.10. Příklad. Uvažme grupu $\mathbb{Z}$ s operací sčítání. Číslo 0 má řád 1, ostatní čísla mají řád ∞ (pro každé kladné celé číslo k a každé $x \in \mathbb{Z}$, $x \neq 0$, totiž máme $k \cdot x \neq 0$).

1.2.11. Příklad. Uvažme grupu $\mathbb{C}^\times$ s operací násobení. Najděme všechna čísla řádu 4. Jestliže $x \in \mathbb{C}^\times$, x má řád 4, pak $x^4 = 1$. Takže $x \in \{1, i, -1, -i\}$. Počítejme:
$1^1 = 1$
$i^1 = i$, $i^2 = -1$, $i^3 = -i$, $i^4 = 1$
$(-1)^1 = -1$, $(-1)^2 = 1$
$(-i)^1 = -i$, $(-i)^2 = -1$, $(-i)^3 = i$, $(-i)^4 = 1$
Zjistili jsme, že 1 má řád 1, i má řád 4, -1 má řád 2, $-i$ má řád 4. Uzavíráme: grupa $\mathbb{C}^\times$ má dva prvky řádu 4, totiž i a $-i$.

Podívejme se ještě na umocňování prvků v komutativních grupách. Samozřejmě, dosud uvedená pravidla platí ve všech grupách, tedy také v komutativních. Avšak v komutativních grupách navíc platí

1.2.12. Věta. *Nechť G je komutativní grupa, $a, b \in G$, k je celé číslo. Pak*

$$(a \cdot b)^k = a^k \cdot b^k.$$

Důkaz. Rozdělíme důkaz na tři případy:
(I) $k > 0$
(II) $k = 0$
(III) $k < 0$
ad (I): Postupujme indukcí vzhledem ke k.
Nechť $k = 1$. Pak $(a \cdot b)^1 = a \cdot b$, $a^1 \cdot b^1 = a \cdot b$.
Nechť $k \geq 1$. Indukční předpoklad: $(a \cdot b)^k = a^k \cdot b^k$. Chceme: $(a \cdot b)^{k+1} = a^{k+1} \cdot b^{k+1}$. Počítejme: $(a \cdot b)^{k+1} = (a \cdot b)^k \cdot (a \cdot b) = a^k \cdot b^k \cdot a \cdot b = (a^k \cdot a) \cdot (b^k \cdot b) = a^{k+1} \cdot b^{k+1}$.
ad (II): Je $(a \cdot b)^0 = 1$, $a^0 \cdot b^0 = 1 \cdot 1 = 1$.
ad (III):Budeme počítat a při výpočtu použijeme již dokázanou část (I): $(a \cdot b)^k = ((a \cdot b)^{-k})^{-1} = (a^{-k} \cdot b^{-k})^{-1} = (b^{-k})^{-1} \cdot (a^{-k})^{-1} = b^k \cdot a^k = a^k \cdot b^k$.

Nechť G je grupa, $a \in G$, a má konečný řád n. Je $a^n = 1$. Zabývejme se nyní určením všech celých čísel k splňujících $a^k = 1$.

1.2.13. Tvrzení. *Nechť G je grupa, $a \in G$, a má konečný řád n. Pro každé celé číslo k platí*

$$a^k = 1 \Longleftrightarrow n/k.$$

Důkaz.

1. Předpokládejme, že $a^k = 1$. Vydělme se zbytkem číslo k nčíslem n. Existují celá čísla q, r, $0 \leq r < n$, splňující $k = nq + r$. Potom

   $$a^k = a^{nq+r} = (a^n)^q \cdot a^r = 1^q \cdot a^r = 1 \cdot a^r = a^r.$$

   Takže $a^r = 1$. Jelikož $0 \leq r < n$ a n je řád prvku a, musí být $r = 0$. Takže $k = nq$, n/k.

2. Předpokládejme, že n/k. Existuje tedy celé číslo q splňující $k = nq$. Potom

   $$a^k = a^{nq} = (a^n)^q = 1^q = 1.$$

1.3 Homomorfismy

1.3.1. Definice. Nechť G_1, G_2 jsou grupy, $\varphi : G_1 \to G_2$. Zobrazení φ se nazývá **homomorfismus** grupy G_1 do grupy G_2, pokud pro všechna $x, y \in G_1$ platí

$$\varphi(x \cdot y) = \varphi(x) \cdot \varphi(y).$$

1.3.2. Tvrzení. *Nechť G_1, G_2 jsou grupy, $\varphi : G_1 \to G_2$ je homomorfismus. Platí:*

1. $\varphi(1) = 1$
2. $\varphi(x^{-1}) = (\varphi(x))^{-1}$ *(pro libovolné $x \in G_1$).*

Důkaz.

1. $\varphi(1) = \varphi(1 \cdot 1) = \varphi(1) \cdot \varphi(1)$, takže $\varphi(1) \cdot 1 = \varphi(1) \cdot \varphi(1)$ a použijeme zákon o krácení.
2. $\varphi(x) \cdot (\varphi(x))^{-1} = 1 = \varphi(1) = \varphi(x \cdot x^{-1}) = \varphi(x) \cdot \varphi(x^{-1})$ a použijeme zákon o krácení.

1.3.3. Tvrzení. *Nechť G_1, G_2, G_3 jsou grupy, $\varphi : G_1 \to G_2$, $\psi : G_2 \to G_3$ jsou homomorfismy. Pak $\varphi\psi : G_1 \to G_3$ je homomorfismus.*

Důkaz. Buďte $x, y \in G_1$. Pak $(\varphi\psi)(x \cdot y) = \psi(\varphi(x \cdot y)) = \psi(\varphi(x) \cdot \varphi(y)) = \psi(\varphi(x)) \cdot \psi(\varphi(y)) = (\varphi\psi)(x) \cdot (\varphi\psi)(y)$.

1.3.4. Příklad. Nechť G_1, G_2 jsou grupy. Definujeme zobrazení $\varphi : G_1 \to G_2$. Pro každé $x \in G_1$ položíme $\varphi(x) = 1$. Pak φ je homomorfismus. Zdůvodnění: Buďte $x, y \in G_1$. Pak $\varphi(x \cdot y) = 1$, $\varphi(x) \cdot \varphi(y) = 1 \cdot 1 = 1$.

1.3.5. Příklad. Nechť $\varphi : \mathbb{Z} \to \mathbb{Z}$, $\varphi(x) = 3 \cdot x$ pro každé $x \in \mathbb{Z}$. Pak φ je homomorfismus. Zdůvodnění: Buďte $x, y \in \mathbb{Z}$. Pak $\varphi(x + y) = 3 \cdot (x + y) = 3 \cdot x + 3 \cdot y = \varphi(x) + \varphi(y)$.

1.3.6. Příklad. Uvažujme grupu $\mathbb{Z}$ s operací sčítání a grupu $\mathbb{Q}^\times$ s operací násobení. Definujme zobrazení $\varphi : \mathbb{Z} \to \mathbb{Q}^\times$ takto:

$$\varphi(x) = \begin{cases} 1 & x \in \mathbb{S} \\ -1 & x \in \mathbb{Z} - \mathbb{S}. \end{cases}$$

Pak φ je homomorfismus grup. Zdůvodnění: Zvolme libovolně $x, y \in \mathbb{Z}$. Potřebujeme, aby $\varphi(x+y) = \varphi(x) \cdot \varphi(y)$. Rozlišíme 4 případy:
(I) x je sudé, y je sudé
(II) x je sudé, y je liché
(III) x je liché, y je sudé
(IV) x je liché, y je liché.
ad (I): Číslo $x+y$ je sudé. Takže $\varphi(x+y) = 1$, $\varphi(x) \cdot \varphi(y) = 1 \cdot 1 = 1$.
ad (II): Číslo $x+y$ je liché. Takže $\varphi(x+y) = -1$, $\varphi(x) \cdot \varphi(y) = 1 \cdot (-1) = -1$.
ad (III): Číslo $x+y$ je liché. Takže $\varphi(x+y) = -1$, $\varphi(x) \cdot \varphi(y) = (-1) \cdot 1 = -1$.
ad (IV): Číslo $x+y$ je sudé. Takže $\varphi(x+y) = 1$, $\varphi(x) \cdot \varphi(y) = (-1) \cdot (-1) = 1$.

Zabývejme se nyní otázkou, kdy dvě grupy G_1, G_2 jsou v podstatě stejné, i když třeba mají jiné prvky. Předpokládejme nejdříve, že grupa G_1 je konečná řádu n. Pak zřejmě grupa G_2 musí být konečná a musí mít stejný počet prvků jako G_1, tj. G_2 má řád n. Nechť grupa G_1 má prvky $a_1, a_2, \ldots, a_n$. Jestliže grupa G_2 je v podstatě stejná jako grupa G_1, pak prvky grupy G_2 lze seřadit do posloupnosti $b_1, b_2, \ldots, b_n$ tak, že multiplikativní tabulka grupy G_1 je v podstatě stejná, jako multiplikativní tabulka grupy G_2. Co tím míníme? Zvolme libovolně $i, j \in \{1, 2, \ldots, n\}$. V tabulce grupy G_1 na pozici (i, j) je prvek $a_i \cdot a_j = a_k$, v tabulce grupy G_2 na pozici (i, j) je prvek $b_i \cdot b_j = b_l$. Jestliže multiplikativní tabulka grupy G_1 je v podstatě stejná, jako multiplikativní tabulka grupy G_2, pak $k = l$. Seřazení $b_1, b_2, \ldots, b_n$ dává bijekci $\varphi : G_1 \to G_2$ takovou, že $\varphi(a_1) = b_1, \varphi(a_2) = b_2, \ldots, \varphi(a_n) = b_n$. Tato bijekce pro libovolná $i, j \in \{1, 2, \ldots, n\}$ splňuje

$$\varphi(a_i \cdot a_j) = \varphi(a_k) = b_k = b_i \cdot b_j = \varphi(a_i) \cdot \varphi(a_j).$$

Shrňme tedy, co jsme zjistili:
Jestliže dvě konečné grupy G_1, G_2 jsou v podstatě stejné, pak existuje bijekce $\varphi : G_1 \to G_2$ taková, že pro všechna $x, y \in G_1$ je $\varphi(x \cdot y) = \varphi(x) \cdot \varphi(y)$.

Výše uvedená úvaha nás motivuje k následující definici. Přitom se již neomezujeme na konečné grupy a slovní obrat "grupy G_1, G_2 jsou v podstatě stejné"nahrazujeme obratem "grupy G_1, G_2 jsou izomorfní".

1.3.7. Definice. Nechť G_1, G_2 jsou grupy. Říkáme, že grupy G_1, G_2 jsou **izomorfní**, pokud existuje bijekce $\varphi : G_1 \to G_2$ splňující

$$\varphi(x \cdot y) = \varphi(x) \cdot \varphi(y)$$

pro všechna $x, y \in G_1$. To, že grupy G_1, G_2 jsou izomorfní, zapisujeme symbolicky $G_1 \cong G_2$. Zobrazení φ nazýváme **izomorfismus** grupy G_1 na grupu G_2. (Všimněme si, že izomorfismus je totéž, co bijektivní homomorfismus.)

1.3.8. Tvrzení. *Nechť G je grupa. Zobrazení $id : G \to G$ dané předpisem $id(x) = x$ pro každé $x \in G$, je izomorfismus.*

Důkaz. Důkaz přenecháváme čtenáři.

1.3.9. Tvrzení. *Nechť G_1, G_2 jsou grupy, $\varphi : G_1 \to G_2$ je izomorfismus. Pak $\varphi^{-1} : G_2 \to G_1$ je izomorfismus.*

Důkaz. Ze základů matematiky víme, že $\varphi^{-1} : G_2 \to G_1$ je bijekce. Zvolme $x, y \in G_2$. Chceme: $\varphi^{-1}(x \cdot y) = \varphi^{-1}(x) \cdot \varphi^{-1}(y)$. Protože zobrazení φ je prosté, tak stačí ukázat, že $\varphi(\varphi^{-1}(x \cdot y)) = \varphi(\varphi^{-1}(x) \cdot \varphi^{-1}(y))$. Ovšem
$\varphi(\varphi^{-1}(x \cdot y)) = x \cdot y$,
$\varphi(\varphi^{-1}(x) \cdot \varphi^{-1}(y)) = \varphi(\varphi^{-1}(x)) \cdot \varphi(\varphi^{-1}(y)) = x \cdot y$.

1.3.10. Tvrzení. *Nechť G_1, G_2, G_3 jsou grupy, $\varphi : G_1 \to G_2$ je izomorfismus, $\psi : G_2 \to G_3$ je izomorfismus. Pak $\varphi\psi : G_1 \to G_3$ je izomorfismus.*

Důkaz. Ze základů matematiky víme, že $\varphi\psi$ je bijekce. Pak stačí použít tvrzení 1.3.3.

1.3.11. Tvrzení. *Nechť G je grupa. Pak $G \cong G$.*

Důkaz. Důkaz přenecháváme čtenáři.

1.3.12. Tvrzení. *Nechť G_1, G_2 jsou grupy. Jestliže $G_1 \cong G_2$, pak $G_2 \cong G_1$.*

Důkaz. Důkaz přenecháváme čtenáři.

1.3.13. Tvrzení. *Nechť G_1, G_2, G_3 jsou grupy. Jestliže $G_1 \cong G_2$ a $G_2 \cong G_3$, pak $G_1 \cong G_3$.*

Důkaz. Důkaz přenecháváme čtenáři.

1.3.14. Příklad. Grupy $\mathbb{Z}$, $\mathbb{S}$ (obě s operací sčítání) jsou izomorfní. Izomorfismem je zobrazení $\varphi : \mathbb{Z} \to \mathbb{S}$ dané předpisem $\varphi(x) = 2x$ (pro všechna $x \in \mathbb{Z}$).

1.3.15. Příklad. Grupa $\mathbb{R}$ s operací sčítání a grupa $\mathbb{R}^+$ s operací násobení jsou izomorfní. Izomorfismem je zobrazení $\varphi : \mathbb{R} \to \mathbb{R}^+$ dané předpisem $\varphi(x) = \exp(x)$ (pro všechna $x \in \mathbb{R}$). Vskutku, ze základů matematické analýzy víme, že φ je bijekce. Dále, nechť $x, y \in \mathbb{R}$. Pak

$$\varphi(x + y) = \exp(x + y) = \exp(x) \cdot \exp(y) = \varphi(x) \cdot \varphi(y).$$

1.4 Podgrupy

Mějme nějakou grupu G a nějakou její podmnožinu H (tj. $H \subseteq G$). Jsou-li $x, y \in H$, pak v grupě G lze určit součin $x \cdot y$. Samozřejmě, pro všechna $x, y, z \in H$ je $x \cdot (y \cdot z) = (x \cdot y) \cdot z$. Zdá se tedy, že podmnožina H bude sama grupou, budeme-li prvky z množiny H násobit stejně, jako násobíme tyto prvky v grupě G. Uvažme například grupu $\mathbb{Z}$ a $H = \{1, 2\}$. Pak $1 \in H$, $2 \in H$, avšak $1 + 2 = 3 \notin H$. Tudíž, aby podmnožina H byla grupa, musí pro všechna $x, y \in H$ platit:

$$x \in H \wedge y \in H \Rightarrow x \cdot y \in H.$$

Aby podmnožina H byla grupa, musí také obsahovat nějaký neutrální prvek e. Pak bude v H platit $e \cdot e = e$. Jistě též v G platí $1 \cdot e = e$ (1 je neutrální prvek grupy G). Protože v H násobíme stejně jako v G, nutně $e \cdot e = 1 \cdot e$. Zákon o krácení dává $e = 1$. Dostáváme další požadavek zajišťující, aby podmnožina H grupy G byla grupa:

$$1 \in H.$$

Dále, aby podmnožina H byla grupa, musí pro každé $x \in H$ existovat $y \in H$ takové, že $x \cdot y = 1$, $y \cdot x = 1$ (násobíme v H). Protože v grupě G je $x \cdot x^{-1} = 1$ a v H násobíme stejně jako v G, máme $x \cdot y = x \cdot x^{-1}$. Zákon o krácení dává $y = x^{-1}$. Dostáváme další (již poslední) požadavek zajišťující, aby podmnožina H grupy G byla grupa. Pro všechna $x \in H$ musí platit

$$x \in H \Rightarrow x^{-1} \in H.$$

Provedená úvaha nás motivuje k následující definici, která popisuje ty podmnožiny H grupy G, jež jsou grupami, násobíme-li prvky z H stejně jako v G. Takovéto podmnožiny budeme nazývat podgrupy.

1.4.1. Definice. Nechť G je grupa, $H \subseteq G$. Říkáme, že H je **podgrupa** grupy G, pokud platí:

1. $1 \in H$
2. Jestliže $x \in H$, pak $x^{-1} \in H$.
3. Jestliže $x, y \in H$, pak $x \cdot y \in H$.

1.4.2. Příklad. Nechť G je grupa. Pak $\{1\}$ a G jsou podgrupy grupy G. Každá podgrupa H grupy G, pro kterou $H \neq G$, se nazývá **vlastní**. Podgrupa $\{1\}$ se nazývá **triviální** podgrupa.

1.4.3. Příklad. $\mathbb{S}$ je podgrupa grupy $\mathbb{Z}$, $\mathbb{Z}$ je podgrupa grupy $\mathbb{Q}$, $\mathbb{Q}$ je podgrupa grupy $\mathbb{R}$, $\mathbb{R}$ je podgrupa grupy $\mathbb{C}$ (uvažujeme operaci sčítání čísel).

1.4.4. Příklad. $\mathbb{Q}^\times$ je podgrupa grupy $\mathbb{R}^\times$, $\mathbb{R}^\times$ je podgrupa grupy $\mathbb{C}^\times$ (uvažujeme operaci násobení čísel).

1.4.5. Příklad. Buď $H = \{x \in \mathbb{C} |\ |x| = 1\}$. Pak H je podgrupa grupy $\mathbb{C}^\times$ a $\{1, -1\}$ je podgrupa grupy H.

1.4.6. Tvrzení. *Nechť G je grupa, H_1, H_2 jsou podgrupy grupy G. Pak $H_1 \cap H_2$ je podgrupa grupy G.*

Důkaz. Je třeba ukázat tři věci:
(I) $1 \in H_1 \cap H_2$
(II) Jestliže $x \in H_1 \cap H_2$, pak $x^{-1} \in H_1 \cap H_2$.
(III) Jestliže $x, y \in H_1 \cap H_2$, pak $x \cdot y \in H_1 \cap H_2$.
ad (I): Protože H_1, H_2 jsou podgrupy, je $1 \in H_1$, $1 \in H_2$. Pak ovšem $1 \in H_1 \cap H_2$.
ad (II): Nechť $x \in H_1 \cap H_2$. Chceme: $x^{-1} \in H_1 \cap H_2$. Je $x \in H_1$, $x \in H_2$. Protože H_1, H_2 jsou podgrupy, je $x^{-1} \in H_1$, $x^{-1} \in H_2$. Pak $x^{-1} \in H_1 \cap H_2$.
ad (III): Nechť $x, y \in H_1 \cap H_2$. Chceme: $x \cdot y \in H_1 \cap H_2$. Protože $x, y \in H_1 \cap H_2$, máme $x, y \in H_1$ a také $x, y \in H_2$. Jelikož H_1 je podgrupa, je $x \cdot y \in H_1$. Jelikož H_2 je podgrupa, je $x \cdot y \in H_2$. Celkem: $x \cdot y \in H_1 \cap H_2$.

1.4.7. Tvrzení. *Nechť G je grupa, H_i pro $i \in I$ ($I \neq \emptyset$) jsou podgrupy grupy G. Pak $\bigcap_{i \in I} H_i$ je podgrupa grupy G.*

Důkaz. Důkaz přenecháváme čtenáři.

1.4.8. Definice. Nechť G_1, G_2 jsou grupy, $\varphi : G_1 \to G_2$ je homomorfismus. Definujeme **jádro** homomorfismu φ jako

$$\ker \varphi = \{x \in G_1 |\ \varphi(x) = 1\}$$

a **obraz** homomorfismu φ jako

$$\text{im } \varphi = \{\varphi(x) |\ x \in G_1\}.$$

1.4.9. Příklad. Uvažme homomorfismus $\varphi : \mathbb{Z} \to \mathbb{Q}^\times$ z příkladu 1.3.6. Pak $\ker \varphi = \mathbb{S}$, $\text{im } \varphi = \{1, -1\}$.

1.4.10. Tvrzení. *Nechť G_1, G_2 jsou grupy, $\varphi : G_1 \to G_2$ je homomorfismus. Pak $\ker \varphi$ je podgrupa grupy G_1 a $\text{im } \varphi$ je podgrupa grupy G_2.*

Důkaz. Nejprve dokážeme, že $\ker \varphi$ je podgrupa grupy G_1. Je třeba ukázat tři věci:
(I) $1 \in \ker \varphi$
(II) Jestliže $x \in \ker \varphi$, pak $x^{-1} \in \ker \varphi$.
(III) Jestliže $x, y \in \ker \varphi$, pak $x \cdot y \in \ker \varphi$.
ad (I): Chceme: $\varphi(1) = 1$. To však víme (viz 1.3.2.).
ad (II): Nechť $x \in \ker \varphi$. Chceme: $x^{-1} \in \ker \varphi$. Protože $x \in \ker \varphi$, je $\varphi(x) = 1$. Počítejme: $\varphi(x^{-1}) = (\varphi(x))^{-1} = 1^{-1} = 1$ (použili jsme 1.3.2.). Protože $\varphi(x^{-1}) = 1$, je $x^{-1} \in \ker \varphi$.
ad (III): Nechť $x, y \in \ker \varphi$. Chceme: $x \cdot y \in \ker \varphi$. Protože $x, y \in \ker \varphi$, je $\varphi(x) = 1$, $\varphi(y) = 1$. Počítejme: $\varphi(x \cdot y) = \varphi(x) \cdot \varphi(y) = 1 \cdot 1 = 1$. Protože $\varphi(x \cdot y) = 1$, je $x \cdot y \in \ker \varphi$.
Nyní dokážeme, že $\text{im } \varphi$ je podgrupa grupy G_2. Je třeba ukázat tři věci:
(I) $1 \in \text{im } \varphi$
(II) Jestliže $y \in \text{im } \varphi$, pak $y^{-1} \in \text{im } \varphi$.
(III) Jestliže $y, z \in \text{im } \varphi$, pak $y \cdot z \in \text{im } \varphi$.
ad (I): Je $\varphi(1) = 1$ (viz 1.3.2.), takže $1 \in \text{im } \varphi$.
ad (II): Nechť $y \in \text{im } \varphi$. Chceme: $y^{-1} \in \text{im } \varphi$. Protože $y \in \text{im } \varphi$, existuje $x \in G_1$, $y = \varphi(x)$. Pak $y^{-1} = (\varphi(x))^{-1} = \varphi(x^{-1})$ (použili jsme 1.3.2.) a tudíž $y^{-1} \in \text{im } \varphi$.
ad (III): Nechť $y, z \in \text{im } \varphi$. Chceme: $y \cdot z \in \text{im } \varphi$. Protože $y, z \in \text{im } \varphi$, existují $u, v \in G_1$, $y = \varphi(u)$, $z = \varphi(v)$. Pak $y \cdot z = \varphi(u) \cdot \varphi(v) = \varphi(u \cdot v)$ a tudíž $y \cdot z \in \text{im } \varphi$.

K tvrzení 1.4.10. učiňme ještě poznámku. Jestliže homorfismus φ je injektivní (prostý), pak zobrazení $\varphi : G_1 \to \text{im } \varphi$ je injektivní a surjektivní současně, tj. je to bijekce. Tudíž, jestliže homomorfismus φ je injektivní, pak zobrazení $\varphi : G_1 \to \text{im } \varphi$ je izomorfismus a $G_1 \cong \text{im } \varphi$.

Nyní nás bude zajímat tato otázka: Nechť G je grupa a H je její podmnožina, tj. $M \subseteq G$. Zřejmě M nemusí být podgrupa grupy G. Bude nás tedy zajímat nejmenší podgrupa grupy G, která obsahuje množinu M. Takovou podgrupu grupy G budeme nazývat podgrupa generovaná množinou M.

1.4.11. Definice. Nechť G je grupa, $M \subseteq G$, $H \subseteq G$. Říkáme, že H je podgrupa grupy G **generovaná** množinou M, pokud platí:

1. H je podgrupa grupy G
2. $M \subseteq H$
3. Jestliže $M \subseteq K$, K je podgrupa grupy G, pak $H \subseteq K$.

1.4.12. Tvrzení. *Nechť G je grupa, $M \subseteq G$. Pak podgrupa grupy G generovaná množinou M vždy existuje a je určená jednoznačně.*

Důkaz.

1. Existence. Nechť H_i, $i \in I$, je systém všech podgrup grupy G, které jsou nadmnožinou množiny M. Je $I \neq \emptyset$, protože G je podgrupa grupy G a $M \subseteq G$. Položme $H = \bigcap_{i \in I} H_i$. Ukážeme, že H je podgrupa grupy G generovaná množinou M. Je třeba prověřit:
   (i) H je podgrupa grupy G
   (ii) $M \subseteq H$
   (iii) Jestliže $M \subseteq K$, K je podgrupa grupy G, pak $H \subseteq K$.
   ad (i): Viz 1.4.7.
   ad (ii): Pro každé $i \in I$ máme $M \subseteq H_i$, což dává $M \subseteq \bigcap_{i \in I} H_i = H$.
   ad (iii): Nechť $M \subseteq K$, K je podgrupa grupy G. Pak existuje $i_0 \in I$, $K = H_{i_0}$. Z toho plyne, že $H = \bigcap_{i \in I} H_i \subseteq H_{i_0} = K$.

2. Jednoznačnost. Buďte $H_1, H_2 \subseteq G$, H_1 a H_2 jsou podgrupy grupy G generované množinou M. Chceme: $H_1 = H_2$. Víme, že H_2 je podgrupa grupy G, $M \subseteq H_2$ (použili jsme 1. a 2. z definice 1.4.11.). Dále víme, že H_1 splňuje 3. z definice 1.4.11., což dává $H_1 \subseteq H_2$. Výměnou role mezi H_1 a H_2 dostaneme, že $H_2 \subseteq H_1$. Celkem tedy $H_1 = H_2$.

Tvrzení 1.4.12 umožní zavést označení pro podgrupu generovanou množinou M. Tuto podgrupu budeme značit $\langle M \rangle$. Množinu M nazýváme množinou **generátorů** grupy $\langle M \rangle$. Pokud $M = \{a_1, a_2, \ldots, a_n\}$, pak hovoříme o podgrupě generované prvky $a_1, a_2, \ldots, a_n$ a označujeme ji často stručně $\langle a_1, a_2, \ldots, a_n \rangle$.

1.4.13. Tvrzení. *Nechť G je grupa, H je podgrupa grupy G, $a \in H$, n je celé číslo. Pak $a^n \in H$.*

Důkaz. Nejdříve dokážeme pomocné tvrzení: Jestliže $b \in H$, k je kladné celé číslo, pak $b^k \in H$. Postupujme indukcí vzhledem ke k.
$k = 1$: $b^k = b^1 = b \in H$
$k \geq 1$: Indukční předpoklad: $b^k \in H$. Chceme: $b^{k+1} \in H$. Počítejme: $b^{k+1} = b^k \cdot b^1 = b^k \cdot b \in H$ (protože H je podgrupa a $b^k, b \in H$).
Nyní již dokážeme, že $a^n \in H$. Rozlišíme tři případy:
(I) $n > 0$
(II) $n = 0$
(III) $n < 0$
ad (I): Aplikujeme pomocné tvzení na $b = a$, $k = n$.
ad (II): $a^n = a^0 = 1 \in H$ (protože H je podgrupa)
ad (III): $a^n = (a^{-1})^{-n} \in H$ (Jelikož H je podgrupa, je $a^{-1} \in H$. Pak aplikujeme pomocné tvrzení na $b = a^{-1}$, $k = -n$.)

1.4.14. Věta. *Nechť G je grupa, $a \in G$. Pak $\langle a \rangle = \{a^n |\ n \in \mathbb{Z}\}$.*

Důkaz. Označme $H = \{a^n |\ n \in \mathbb{Z}\}$. Je třeba ukázat následující:
(I) H je podgrupa grupy G
(II) $a \in H$
(III) Jestliže K je podgrupa grupy G, $a \in K$, pak $H \subseteq K$.
ad (I): Je třeba prověřit tři věci:
(a) $1 \in H$
(b) Jestliže $x \in H$, pak $x^{-1} \in H$.
(c) Jestliže $x, y \in H$, pak $x \cdot y \in H$.
ad (a): $1 = a^0 \in H$ (je $0 \in \mathbb{Z}$)
ad (b): Nechť $x \in H$. Pak $x = a^n$ pro jisté $n \in \mathbb{Z}$. Je $x^{-1} = (a^n)^{-1} = a^{-n} \in H$ (zřejmě $-n \in \mathbb{Z}$).
ad (c): Nechť $x, y \in H$. Pak $x = a^k$, $y = a^l$ pro jistá $k, l \in \mathbb{Z}$. Je $x \cdot y = a^k \cdot a^l = a^{k+l} \in H$ (zřejmě $k + l \in \mathbb{Z}$).
ad (II): $a = a^1 \in H$ (je $1 \in \mathbb{Z}$)

ad (III): Nechť K je podgrupa grupy G, $a \in K$. Chceme: $H \subseteq K$. Buď $x \in H$. Je $x = a^n$ pro jisté $n \in \mathbb{Z}$. Dle tvrzení 1.4.13 je $a^n \in K$. Tudíž $x \in K$. Protože x bylo libovolné, máme $H \subseteq K$.

1.4.15. Příklad. V libovolné grupě G je $\langle \emptyset \rangle = \{1\}$.

1.4.16. Příklad. V tomto příkladu bude základní grupou množina $\mathbb{Z}$ s operací sčítání. Pak $\langle 1 \rangle = \mathbb{Z}$, $\langle 2 \rangle = \mathbb{S}$. Vskutku,
$\langle 1 \rangle = \{n \cdot 1 |\ n \in \mathbb{Z}\} = \{n |\ n \in \mathbb{Z}\} = \mathbb{Z}$,
$\langle 2 \rangle = \{n \cdot 2 |\ n \in \mathbb{Z}\} = \mathbb{S}$.

1.4.17. Příklad. V tomto příkladu bude základní grupou množina $\mathbb{R}^\times$ s operací násobení. Nechť P je množina všech prvočísel. Zřejmě $P \subseteq \mathbb{R}^\times$. Ukážeme, že $\langle P \rangle = \mathbb{Q}^+$.

1. $\langle P \rangle \subseteq \mathbb{Q}^+$:
   Je $P \subseteq \mathbb{Q}^+$ a $\mathbb{Q}^+$ je podgrupa grupy $\mathbb{R}^\times$. Proto $\langle P \rangle \subseteq \mathbb{Q}^+$.

2. $\mathbb{Q}^+ \subseteq \langle P \rangle$:
   Nejdříve si uvědomíme, že $\mathbb{N} \subseteq \langle P \rangle$. Zřejmě $1 \in \langle P \rangle$. Buď $a \in \mathbb{N}$, $a \neq 1$. Pak existují $p_1, \ldots, p_k \in P$, $e_1, \ldots, e_k \in \mathbb{N}$, $a = p_1^{e_1} \ldots p_k^{e_k}$. Prvočíslo $p_1 \in P \subseteq \langle P \rangle$. Dle 1.4.13. je $p_1^{e_1} \in \langle P \rangle$. Obdobně pak $p_2^{e_2} \in \langle P \rangle, \ldots, p_k^{e_k} \in \langle P \rangle$. Protože podgrupa $\langle P \rangle$ je uzavřena vzhledem k součinu, máme $a = p_1^{e_1} p_2^{e_2} \ldots p_k^{e_k} \in \langle P \rangle$. Buď nyní $x \in \mathbb{Q}^+$. Existují $a, b \in \mathbb{N}$, $x = \frac{a}{b}$. Víme již, že $a, b \in \langle P \rangle$. Pak $\frac{1}{b} \in \langle P \rangle$, $x = a \cdot \frac{1}{b} \in \langle P \rangle$. Jelikož prvek $x \in \mathbb{Q}^+$ byl libovolný, dostali jsme výsledek $\mathbb{Q}^+ \subseteq \langle P \rangle$.

1.4.18. Tvrzení. *Nechť G je grupa, $a \in G$, a má řád $n \in \mathbb{N}$. Pak $\langle a \rangle$ má řád n a $\langle a \rangle = \{1, a, a^2, \ldots, a^{n-1}\}$.*

Důkaz. Dle 1.4.14. je $\langle a \rangle = \{a^k |\ k \in \mathbb{Z}\}$. Chceme tedy ukázat, že $\{a^k |\ k \in \mathbb{Z}\} = \{1, a, a^2, \ldots, a^{n-1}\}$.
$\{1, a, a^2, \ldots, a^{n-1}\} \subseteq \{a^k |\ k \in \mathbb{Z}\}$: To je zřejmé.
$\{a^k |\ k \in \mathbb{Z}\} \subseteq \{1, a, a^2, \ldots, a^{n-1}\}$: Buď $k \in \mathbb{Z}$. Číslo k vydělíme se zbytkem číslem n. Existují $q, r \in \mathbb{Z}$, $k = q \cdot n + r$, $0 \leq r < n$. Pak $a^k = a^{qn+r} = a^{qn} \cdot a^r = (a^n)^q \cdot a^r = 1^q \cdot a^r = 1 \cdot a^r = a^r$. Jelikož $0 \leq r < n$, je $a^k \in \{1, a, a^2, \ldots, a^{n-1}\}$. Zbývá ukázat, že prvky $1, a, a^2, \ldots, a^{n-1}$ jsou navzájem různé. Předpokládejme opak, tj. $a^i = a^j$ pro nějaká $i, j \in \{0, 1, \ldots, n-1\}$, $i < j$. Pak $1 = a^{j-i}$,

kde $j - i \in \mathbb{N}$ a přitom $j - i \leq (n-1) - 0 = n - 1 < n$. Dostali jsme spor s faktem, že číslo n je řád prvku a.

Zavedeme teď pojem, který bude hrát zásadní roli v kapitole o faktorových grupách.

1.4.19. Definice. Podgrupa H grupy G se nazývá **normální**, jestliže

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

pro libovolné prvky $g \in G$, $h \in H$.

Pro komutativní grupy pojem normální podgrupy nepřináší nic nového. V komutativní grupě je každá podgrupa normální, poněvadž $g \cdot h \cdot g^{-1} = g \cdot g^{-1} \cdot h = 1 \cdot h = h$.

Nechť G je grupa, $A \subseteq G$, $B \subseteq G$. Je přirozené, že klademe

$$A \cdot B = AB = \{x \cdot y |\ x \in A, y \in B\}.$$

1.4.20. Tvrzení. *Nechť G je grupa. Nechť H a K jsou normální podgrupy grupy G. Pak HK je normální podgrupa grupy G.*

Důkaz. Je třeba prověřit následující:
(I) $1 \in HK$
(II) Jestliže $x \in HK$, pak $x^{-1} \in HK$.
(III) Jestliže $x, y \in HK$, pak $x \cdot y \in HK$.
(IV) Jestliže $z \in G$, $x \in HK$, pak $zxz^{-1} \in HK$.
ad (I): $1 = 1 \cdot 1 \in HK$ (uvědomme si, že $1 \in H$, $1 \in K$, protože H, K jsou podgrupy)
ad (II): Nechť $x \in HK$. Existují $a \in H$, $b \in K$, $x = ab$. Pak $x^{-1} = b^{-1}a^{-1} = 1 \cdot b^{-1} \cdot a^{-1} = a^{-1}ab^{-1}a^{-1} = a^{-1} \cdot (ab^{-1}a^{-1})$. Jelikož H je podgrupa a $a \in H$, je $a^{-1} \in H$. Jelikož K je podgrupa a $b \in K$, je $b^{-1} \in K$. Ovšem podgrupa K je normální, což dává $ab^{-1}a^{-1} \in K$. Celkem: $a^{-1} \in H$, $ab^{-1}a^{-1} \in K$, tedy $x^{-1} \in HK$.
ad (III): Nechť $x, y \in HK$. Existují $a, c \in H$, $b, d \in K$, $x = ab$, $y = cd$. Pak $xy = abcd = abc \cdot 1 \cdot d = abcb^{-1}bd = (a(bcb^{-1}))(bd)$. Jelikož $c \in H$ a H je normální podgrupa, je $bcb^{-1} \in H$. Protože H je podgrupa, je $a(bcb^{-1}) \in H$. Protože K je podgrupa, je $bd \in K$. Celkem: $a(bcb^{-1}) \in H$, $bd \in K$, tedy

$xy \in HK$.
ad (IV): Nechť $z \in G$, $x \in HK$. Existují $a \in H$, $b \in K$, $x = ab$. Pak $zxz^{-1} = zabz^{-1} = za \cdot 1 \cdot bz^{-1} = zaz^{-1}zbz^{-1} = (zaz^{-1})(zbz^{-1})$. Jelikož podgrupa H je normální, je $zaz^{-1} \in H$. Jelikož podgrupa K je normální, je $zbz^{-1} \in K$. Pak tedy $zxz^{-1} \in HK$.

1.4.21. Tvrzení. *Nechť G je grupa, H, K jsou normální podgrupy grupy G. Pak*

$$\langle H \cup K \rangle = HK.$$

Důkaz. Je třeba prověřit následující:
(I) HK je podgrupa grupy G
(II) $H \subseteq HK$, $K \subseteq HK$
(III) Jestliže Q je podgrupa grupy G, $H \cup K \subseteq Q$, pak $HK \subseteq Q$.
ad (I): Viz 1.4.20.
ad (II): Nechť $x \in H$. Je $x = x \cdot 1 \in HK$, protože $1 \in K$. Tudíž $H \subseteq HK$. Nechť $y \in K$. Je $y = 1 \cdot y \in HK$, protože $1 \in H$. Tudíž $K \subseteq HK$.
ad (III): Nechť Q je podgrupa grupy G, $H \cup K \subseteq Q$. Buď $x \in HK$. Chceme: $x \in Q$. Existují $a \in H$, $b \in K$, $x = ab$. Protože $H \cup K \subseteq Q$, je $a \in Q$, $b \in Q$. Protože Q je podgrupa, je $x = ab \in Q$.

1.5 Součiny grup

V této kapitole se naučíme jednu základní konstrukci, jak ze dvou daných grup vytvořit grupu další (velmi jednoduchým a přirozeným způsobem).

1.5.1. Tvrzení. *Nechť jsou dány grupy G_1, G_2. Na kartézském součinu $G_1 \times G_2$ definujeme operaci násobení následovně:*

$$(a, b) \cdot (c, d) = (ac, bd)$$

pro libovolná $(a, b), (c, d) \in G_1 \times G_2$.
Potom $G_1 \times G_2$ je grupa.

Důkaz. Musíme dokázat:
(I) operace je asociativní
(II) operace má neutrální prvek

(III) ke každému prvku existuje prvek inverzní
ad (I): Nechť $(a,b),(c,d),(e,f) \in G_1 \times G_2$. Počítejme:
$(a,b)\cdot((c,d)\cdot(e,f)) = (a,b)\cdot(ce,df) = (a(ce),b(df)) = ((ac)e,(bd)f) = (ac,bd)\cdot(e,f) = ((a,b)\cdot(c,d))\cdot(e,f)$.
ad (II): Neutrálním prvkem je dvojice $(1,1)$. Prověříme to. Buď $(a,b) \in G_1 \times G_2$. Pak $(1,1)\cdot(a,b) = (1\cdot a, 1\cdot b) = (a,b)$, $(a,b)\cdot(1,1) = (a\cdot 1, b\cdot 1) = (a,b)$.
ad (III): Buď $(a,b) \in G_1 \times G_2$. Počítejme:
$(a,b)\cdot(a^{-1},b^{-1}) = (aa^{-1},bb^{-1}) = (1,1)$, $(a^{-1},b^{-1})\cdot(a,b) = (a^{-1}a,b^{-1}b) = (1,1)$.
Tudíž $(a,b)^{-1} = (a^{-1},b^{-1})$.

1.5.2. Definice. Grupa $G_1 \times G_2$ sestrojená v 1.5.1. se nazývá **součin** grup G_1 a G_2.

1.5.3. Příklad. Pro libovolnou grupu G platí $G \cong G \times \{1\}$.

1.5.4. Příklad. Nechť $G = \{1,-1\} \subseteq \mathbb{Q}^\times$. Snadno se lze přesvědčit, že G je podgrupa grupy $\mathbb{Q}^\times$ (operací je násobení čísel). Sestrojíme multiplikativní tabulku grupy $G \times G$:

	$(1,1)$	$(1,-1)$	$(-1,1)$	$(-1,-1)$
$(1,1)$	$(1,1)$	$(1,-1)$	$(-1,1)$	$(-1,-1)$
$(1,-1)$	$(1,-1)$	$(1,1)$	$(-1,-1)$	$(-1,1)$
$(-1,1)$	$(-1,1)$	$(-1,-1)$	$(1,1)$	$(1,-1)$
$(-1,-1)$	$(-1,-1)$	$(-1,1)$	$(1,-1)$	$(1,1)$

Následující tvrzení ukazuje, že součin grup je v podstatě asociativní. Při zápisu součinu více grup tudíž nemusíme psát závorky.

1.5.5. Tvrzení. *Nechť G_1, G_2, G_3 jsou grupy. Pak*

$$G_1 \times (G_2 \times G_3) \cong (G_1 \times G_2) \times G_3.$$

Důkaz. Definujme zobrazení $\varphi : G_1 \times (G_2 \times G_3) \to (G_1 \times G_2) \times G_3$ takto:

$$\varphi((x,(y,z))) = ((x,y),z)$$

pro $(x,(y,z)) \in G_1 \times (G_2 \times G_3)$.
φ je injekce:
Nechť $(x,(y,z)),(u,(v,w)) \in G_1 \times (G_2 \times G_3)$, $\varphi((x,(y,z))) = \varphi((u,(v,w)))$.
Chceme: $(x,(y,z)) = (u,(v,w))$.
Víme, že $((x,y),z) = ((u,v),w)$. Pak $(x,y) = (u,v)$, $z = w$ a tedy $x = u$, $y = v$, $z = w$. Z toho plyne, že $x = u$, $(y,z) = (v,w)$ a tedy $(x,(y,z)) = (u,(v,w))$.
φ je surjekce:
Nechť $((u,v),w) \in (G_1 \times G_2) \times G_3$. Hledáme $(x,(y,z)) \in G_1 \times (G_2 \times G_3)$ tak, aby $\varphi((x,(y,z))) = ((u,v),w)$. Zvolíme $x = u$, $y = v$, $z = w$.
φ je homomorfismus:
Nechť $(x,(y,z)),(u,(v,w)) \in G_1 \times (G_2 \times G_3)$. Pak

$$\begin{aligned}
\varphi((x,(y,z)) \cdot (u,(v,w))) &= \varphi((x \cdot u,(y,z) \cdot (v,w))) \\
&= \varphi((x \cdot u,(y \cdot v, z \cdot w))) \\
&= ((x \cdot u, y \cdot v), z \cdot w) \\
&= ((x,y) \cdot (u,v), z \cdot w) \\
&= ((x,y),z) \cdot ((u,v),w) \\
&= \varphi((x,(y,z))) \cdot \varphi((u,(v,w))).
\end{aligned}$$

Následující tvrzení ukazuje, že součin grup je v podstatě komutativní. Při zápisu součinu více grup tudíž nemusíme psát závorky (viz 1.5.5.) a nezáleží na pořadí.

1.5.6. Tvrzení. *Nechť G_1, G_2 jsou grupy. Pak*

$$G_1 \times G_2 \cong G_2 \times G_1.$$

Důkaz. Definujme zobrazení $\varphi : G_1 \times G_2 \to G_2 \times G_1$ takto:

$$\varphi((x,y)) = (y,x)$$

pro $(x,y) \in G_1 \times G_2$.
Čtenář se sám přesvědčí, že φ je bijekce.

φ je homomorfismus:
Nechť $(x,y),(u,v) \in G_1 \times G_2$. Pak

$$\begin{aligned}\varphi((x,y)\cdot(u,v)) &= \varphi((x\cdot u, y\cdot v))\\ &= (y\cdot v, x\cdot u)\\ &= (y,x)\cdot(v,u)\\ &= \varphi((x,y))\cdot\varphi((u,v)).\end{aligned}$$

Umíme zatím dvě grupy vynásobit. Můžeme grupu rozložit na součin?

1.5.7. Věta. *Nechť G je grupa, H, K jsou normální podgrupy grupy G. Jestliže $HK = G$ a $H \cap K = \{1\}$, pak $G \cong H \times K$.*

Důkaz. Budeme definovat zobrazení $\varphi : H \times K \to G$. Pro $(x,y) \in H \times K$ položíme $\varphi((x,y)) = x \cdot y$. V dalším ukážeme, že φ je izomorfismus.
(I) φ je injekce:
Nechť $(x,y),(u,v) \in H \times K$, $\varphi((x,y)) = \varphi((u,v))$. Chceme: $(x,y) = (u,v)$.
Víme, že $x \cdot y = u \cdot v$. Pak $x = uvy^{-1}$, $u^{-1}x = vy^{-1}$. Jelikož $u \in H$ a H je podgrupa, je $u^{-1} \in H$. Ovšem také $x \in H$, takže $u^{-1}x \in H$ (opět jsme použili fakt, že H je podgrupa). Obdobně $vy^{-1} \in K$. Pak $u^{-1}x = vy^{-1} \in H \cap K$. Protože $H \cap K = \{1\}$, máme $u^{-1}x = 1$, $vy^{-1} = 1$, a tedy $x = u$, $v = y$, $(x,y) = (u,v)$.
(II): φ je surjekce:
Buď $g \in G$. Hledáme $(x,y) \in H \times K$ takové, že $\varphi((x,y)) = g$. Jelikož $G = HK$, je $g \in HK$, $g = xy$ pro nějaká $x \in H$, $y \in K$. Pak $(x,y) \in H \times K$ a $\varphi((x,y)) = xy = g$.
(III): φ je homomorfismus:
Nechť $(x,y),(u,v) \in H \times K$. Chceme: $\varphi((x,y)\cdot(u,v)) = \varphi((x,y))\cdot\varphi((u,v))$.
Je
$\varphi((x,y)\cdot(u,v)) = \varphi((xu,yv)) = xuyv$,
$\varphi((x,y))\cdot\varphi((u,v)) = xy \cdot uv$.
Chceme tedy dokázat, že $xuyv = xyuv$.
Uvažme prvek $uyu^{-1}y^{-1}$.
Protože $u \in H$, je $u^{-1} \in H$. Protože podgrupa H je normální, je $yu^{-1}y^{-1} \in H$. Již víme: $u \in H$, $yu^{-1}y^{-1} \in H$. Pak $uyu^{-1}y^{-1} \in H$.
Protože $y \in K$ a podgrupa K je normální, je $uyu^{-1} \in K$. Protože $y \in K$, je

$y^{-1} \in K$. Již víme: $uyu^{-1} \in K$, $y^{-1} \in K$. Pak $uyu^{-1}y^{-1} \in K$.
Právě jsme zjistili, že $uyu^{-1}y^{-1} \in H \cap K$. Ovšem $H \cap K = \{1\}$, takže $uyu^{-1}y^{-1} = 1$, $uyu^{-1} = y$, $uy = yu$, $xuyv = xyuv$.

1.5.8. Příklad. Nechť $G = \{x \in \mathbb{C} |\ x^6 = 1\}$. Pak G je podgrupa grupy $\mathbb{C}^\times$.
Abychom se o tom přesvědčili, prověříme tři záležitosti:
(I) $1 \in G$
(II) Jestliže $x \in G$, pak $x^{-1} \in G$.
(III) Jestliže $x, y \in G$, pak $x \cdot y \in G$.
ad (I): $1^6 = 1$, takže $1 \in G$
ad (II): Nechť $x \in G$. Pak $x^6 = 1$ a tedy $(x^{-1})^6 = (x^6)^{-1} = 1^{-1} = 1$. To dává $x^{-1} \in G$.
ad (III): Nechť $x, y \in G$. Pak $x^6 = 1$, $y^6 = 1$ a tedy $(x \cdot y)^6 = x^6 \cdot y^6 = 1 \cdot 1 = 1$. To dává $x \cdot y \in G$.
Prvky grupy G zjistíme vyřešením rovnice $x^6 = 1$ v oboru komplexních čísel. Víme, že tato rovnice má 6 řešení:
$x_0 = \cos 0 \cdot \frac{2\pi}{6} + i \sin 0 \cdot \frac{2\pi}{6} = (\cos \frac{2\pi}{6} + i \sin \frac{2\pi}{6})^0$
$x_1 = \cos 1 \cdot \frac{2\pi}{6} + i \sin 1 \cdot \frac{2\pi}{6} = (\cos \frac{2\pi}{6} + i \sin \frac{2\pi}{6})^1$
$x_2 = \cos 2 \cdot \frac{2\pi}{6} + i \sin 2 \cdot \frac{2\pi}{6} = (\cos \frac{2\pi}{6} + i \sin \frac{2\pi}{6})^2$
$x_3 = \cos 3 \cdot \frac{2\pi}{6} + i \sin 3 \cdot \frac{2\pi}{6} = (\cos \frac{2\pi}{6} + i \sin \frac{2\pi}{6})^3$
$x_4 = \cos 4 \cdot \frac{2\pi}{6} + i \sin 4 \cdot \frac{2\pi}{6} = (\cos \frac{2\pi}{6} + i \sin \frac{2\pi}{6})^4$
$x_5 = \cos 5 \cdot \frac{2\pi}{6} + i \sin 5 \cdot \frac{2\pi}{6} = (\cos \frac{2\pi}{6} + i \sin \frac{2\pi}{6})^5$.
Položme $\varepsilon = \cos \frac{2\pi}{6} + i \sin \frac{2\pi}{6} = \cos \frac{\pi}{3} + i \sin \frac{\pi}{3}$. Pak

$$G = \{\varepsilon^0, \varepsilon^1, \varepsilon^2, \varepsilon^3, \varepsilon^4, \varepsilon^5\}.$$

Sestrojíme multiplikativní tabulku grupy G.

	ε^0	ε^1	ε^2	ε^3	ε^4	ε^5
ε^0	ε^0	ε^1	ε^2	ε^3	ε^4	ε^5
ε^1	ε^1	ε^2	ε^3	ε^4	ε^5	ε^0
ε^2	ε^2	ε^3	ε^4	ε^5	ε^0	ε^1
ε^3	ε^3	ε^4	ε^5	ε^0	ε^1	ε^2
ε^4	ε^4	ε^5	ε^0	ε^1	ε^2	ε^3
ε^5	ε^5	ε^0	ε^1	ε^2	ε^3	ε^4

Uvedeme ukázku, jak jsme provedli méně zřejmé výpočty:

$$\varepsilon^4 \cdot \varepsilon^5 = \varepsilon^9 = \varepsilon^6 \cdot \varepsilon^3 = 1 \cdot \varepsilon^3 = \varepsilon^3.$$

Při těchto výpočtech jsme vždy využívali fakt, že $\varepsilon^6 = 1$.
Položme nyní $H = \{\varepsilon^0, \varepsilon^3\}$, $K = \{\varepsilon^0, \varepsilon^2, \varepsilon^4\}$. Snadno se lze přesvědčit, že H a K jsou (normální) podgrupy grupy G. Zřejmě $H \cap K = \{\varepsilon^0\} = \{1\}$.
Dále si všimněme, že $HK = G$. Inkluze $HK \subseteq G$ je jasná. Přesvědčíme se, že $G \subseteq HK$:
$\varepsilon^0 = \varepsilon^0 \cdot \varepsilon^0 \in HK$
$\varepsilon^1 = \varepsilon^3 \cdot \varepsilon^4 \in HK$
$\varepsilon^2 = \varepsilon^0 \cdot \varepsilon^2 \in HK$
$\varepsilon^3 = \varepsilon^3 \cdot \varepsilon^0 \in HK$
$\varepsilon^4 = \varepsilon^0 \cdot \varepsilon^4 \in HK$
$\varepsilon^5 = \varepsilon^3 \cdot \varepsilon^2 \in HK$.
Podle věty 1.5.7. je $G \cong H \times K$.
V důkazu věty 1.5.7. je ukázáno, jak lze najít izomorfismus $\varphi : H \times K \to G$. Postupuje se takto:
$\varphi((\varepsilon^0, \varepsilon^0)) = \varepsilon^0 \cdot \varepsilon^0 = \varepsilon^0$
$\varphi((\varepsilon^0, \varepsilon^2)) = \varepsilon^0 \cdot \varepsilon^2 = \varepsilon^2$
$\varphi((\varepsilon^0, \varepsilon^4)) = \varepsilon^0 \cdot \varepsilon^4 = \varepsilon^4$
$\varphi((\varepsilon^3, \varepsilon^0)) = \varepsilon^3 \cdot \varepsilon^0 = \varepsilon^3$
$\varphi((\varepsilon^3, \varepsilon^2)) = \varepsilon^3 \cdot \varepsilon^2 = \varepsilon^5$
$\varphi((\varepsilon^3, \varepsilon^4)) = \varepsilon^3 \cdot \varepsilon^4 = \varepsilon^1$.
Sestrojíme nyní multiplikativní tabulku grupy $H \times K$:

	$(\varepsilon^0, \varepsilon^0)$	$(\varepsilon^3, \varepsilon^4)$	$(\varepsilon^0, \varepsilon^2)$	$(\varepsilon^3, \varepsilon^0)$	$(\varepsilon^0, \varepsilon^4)$	$(\varepsilon^3, \varepsilon^2)$
$(\varepsilon^0, \varepsilon^0)$	$(\varepsilon^0, \varepsilon^0)$	$(\varepsilon^3, \varepsilon^4)$	$(\varepsilon^0, \varepsilon^2)$	$(\varepsilon^3, \varepsilon^0)$	$(\varepsilon^0, \varepsilon^4)$	$(\varepsilon^3, \varepsilon^2)$
$(\varepsilon^3, \varepsilon^4)$	$(\varepsilon^3, \varepsilon^4)$	$(\varepsilon^0, \varepsilon^2)$	$(\varepsilon^3, \varepsilon^0)$	$(\varepsilon^0, \varepsilon^4)$	$(\varepsilon^3, \varepsilon^2)$	$(\varepsilon^0, \varepsilon^0)$
$(\varepsilon^0, \varepsilon^2)$	$(\varepsilon^0, \varepsilon^2)$	$(\varepsilon^3, \varepsilon^0)$	$(\varepsilon^0, \varepsilon^4)$	$(\varepsilon^3, \varepsilon^2)$	$(\varepsilon^0, \varepsilon^0)$	$(\varepsilon^3, \varepsilon^4)$
$(\varepsilon^3, \varepsilon^0)$	$(\varepsilon^3, \varepsilon^0)$	$(\varepsilon^0, \varepsilon^4)$	$(\varepsilon^3, \varepsilon^2)$	$(\varepsilon^0, \varepsilon^0)$	$(\varepsilon^3, \varepsilon^4)$	$(\varepsilon^0, \varepsilon^2)$
$(\varepsilon^0, \varepsilon^4)$	$(\varepsilon^0, \varepsilon^4)$	$(\varepsilon^3, \varepsilon^2)$	$(\varepsilon^0, \varepsilon^0)$	$(\varepsilon^3, \varepsilon^4)$	$(\varepsilon^0, \varepsilon^2)$	$(\varepsilon^3, \varepsilon^0)$
$(\varepsilon^3, \varepsilon^2)$	$(\varepsilon^3, \varepsilon^2)$	$(\varepsilon^0, \varepsilon^0)$	$(\varepsilon^3, \varepsilon^4)$	$(\varepsilon^0, \varepsilon^2)$	$(\varepsilon^3, \varepsilon^0)$	$(\varepsilon^0, \varepsilon^4)$

Vyřešíme ještě otázku, za jakých podmínek je součin dvou grup komutativní grupa.

1.5.9. Tvrzení. *Nechť G_1, G_2 jsou grupy. Grupa $G_1 \times G_2$ je komutativní právě tehdy, když obě grupy G_1, G_2 jsou komutativní.*

Důkaz. Předpokládejme nejdříve, že grupa $G_1 \times G_2$ je komutativní. Buď $a, b \in G_1$. Pak $(a, 1), (b, 1) \in G_1 \times G_2$,

$(a,1)\cdot(b,1) = (a\cdot b, 1\cdot 1) = (a\cdot b, 1)$,
$(b,1)\cdot(a,1) = (b\cdot a, 1\cdot 1) = (b\cdot a, 1)$.
Protože grupa $G_1 \times G_2$ je komutativní, je $(a,1)\cdot(b,1) = (b,1)\cdot(a,1)$, čili $(a\cdot b, 1) = (b\cdot a, 1)$. Z toho vyplývá, že $a\cdot b = b\cdot a$. Prvky a, b byly libovolné, takže grupa G_1 je komutativní. Obdobně se dokáže, že grupa G_2 je komutativní.
Předpokládejme nyní naopak, že grupy G_1, G_2 jsou komutativní.
Nechť $(x,y),(u,v) \in G_1 \times G_2$. Pak
$(x,y)\cdot(u,v) = (x\cdot u, y\cdot v) = (u\cdot x, v\cdot y) = (u,v)\cdot(x,y)$
a grupa $G_1 \times G_2$ je komutativní.

2 Příklady grup

2.1 Aditivní grupa okruhu

Připomeňme nejdříve tři definice.

2.1.1. Definice. Okruh je množina spolu se dvěma binárními operacemi, většinou zvanými sčítání a násobení, přičemž vzhledem ke sčítání se jedná o komutativní grupu a násobení je distributivní vzhledem ke sčítání. Okruh se nazývá **asociativní** (**komutativní**, **s jednotkovým prvkem**), pokud operace násobení je asociativní (komutativní, má neutrální prvek).

2.1.2. Definice. Obor integrity je asociativní a komutativní okruh, v němž pro každé dva prvky x, y platí:
Jestliže $x \cdot y = 0$, pak $x = 0$ nebo $y = 0$.

2.1.3. Definice. Těleso je aspoň dvouprvkový asociativní okruh s jednotkovým prvkem (označme jej 1), v němž pro každý nenulový prvek x existuje prvek y takový, že $x \cdot y = y \cdot x = 1$. Prvek y se značí x^{-1} nebo $\frac{1}{x}$. Značení je možno zavést, neboť prvek y je určen jednoznačně (nechť $x \cdot z = z \cdot x = 1$; pak $y = y \cdot 1 = y \cdot (x \cdot z) = (y \cdot x) \cdot z = 1 \cdot z = z$). Je-li v tělese násobení komutativní, pak hovoříme o **komutativním tělese**. Protože v tomto textu budeme pracovat výhradně s komutativními tělesy, budeme pro stručnost místo názvu komutativní těleso používat pouze slovo těleso.

Číselné množiny $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ spolu s operacemi sčítání a násobení jsou okruhy. Specielně, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ spolu s operací sčítání jsou komutativní grupy.

Nechť $\sim$ je ekvivalence na neprázdné množině A. Položme pro libovolné $a \in A$, $\overline{a} = \{x \in A |\ x \sim a\}$.

Nyní zopakujeme definici kongruence modulo m.

2.1.4. Definice. Nechť a, b, m jsou celá čísla, $m > 0$. Říkáme, že a je **kongruentní** s b **modulo** m, pokud m dělí $b - a$. Tento vztah zapisujeme $a \equiv b\ (m)$. Bude-li z kontextu jasné, o jaké m se jedná, můžeme psát pouze $a \equiv b$.

2.1.5. Tvrzení. $\equiv$ *je relace ekvivalence na množině* $\mathbb{Z}$.

Důkaz. Například [3], 1.2.17.

Faktorovou množinu $\mathbb{Z}/\equiv$ budeme značit $\mathbb{Z}_m$.

2.1.6. Tvrzení. *Množina $\mathbb{Z}_m$ má přesně m prvků, totiž $\overline{0}, \overline{1}, \ldots, \overline{m-1}$.*

Důkaz. Například [3], 1.2.18.

2.1.7. Tvrzení. *Nechť $a, b, c, d \in \mathbb{Z}$. Jestliže $a \equiv c$, $b \equiv d$, pak $a + b \equiv c + d$, $a \cdot b \equiv c \cdot d$.*

Důkaz. Například [3], 1.2.19.

2.1.8. Tvrzení. *Nechť na $\mathbb{Z}_m$ definujeme sčítání a násobení takto: $\overline{a} + \overline{b} = \overline{a+b}$, $\overline{a} \cdot \overline{b} = \overline{a \cdot b}$ $(a, b \in \mathbb{Z})$. Pak $\mathbb{Z}_m$ je komutativní asociativní okruh s jednotkovým prvkem $\overline{1}$.*

Důkaz. Například [3], 1.2.20.

2.1.9. Tvrzení. *Nechť m je celé číslo, $m > 1$. Platí: $\mathbb{Z}_m$ je těleso právě tehdy, když m je prvočíslo.*

Důkaz. Například [3], 1.2.21.

Vidíme, že máme k dispozici nekonečně mnoho příkladů komutativních grup $\mathbb{Z}_m$ (uvažujeme operaci sčítání). Pro ilustraci uvedeme tabulku operace sčítání v grupě $\mathbb{Z}_5$.

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$

2.2 Grupa jednotek okruhu

Jestliže R je asociativní okruh s jednotkovým prvkem 1, pak prvek x je **jednotka** okruhu R, pokud existuje $y \in R$ s vlastností $x \cdot y = 1$, $y \cdot x = 1$. Množinu všech jednotek okruhu R označíme $U(R)$.

2.2.1. Tvrzení. *Nechť R je asociativní okruh s jednotkovým prvkem. Platí: $U(R)$ spolu s operací násobení je grupa.*

Důkaz. Ukážeme nejdříve, že množina $U(R)$ je uzavřená vzhledem k operaci násobení. Nechť $x, u \in U(R)$. Chceme: $x \cdot u \in U(R)$. Existují $y, v \in R$ tak, že $x \cdot y = 1$, $y \cdot x = 1$, $u \cdot v = 1$, $v \cdot u = 1$. Počítejme:
$(x \cdot u) \cdot (v \cdot y) = x \cdot (u \cdot v) \cdot y = x \cdot 1 \cdot y = x \cdot y = 1$,
$(v \cdot y) \cdot (x \cdot u) = v \cdot (y \cdot x) \cdot u = v \cdot 1 \cdot u = v \cdot u = 1$.
Spočítali jsme, že $x \cdot u \in U(R)$.
Nyní víme, že násobení je operace na množině $U(R)$. Tato operace je asociativní, jelikož okruh R je asociativní.
Tato operace má neutrální prvek, jelikož $1 \cdot 1 = 1$ a tedy $1 \in U(R)$.
Nechť $x \in U(R)$. Pak existuje $y \in R$, $x \cdot y = 1$, $y \cdot x = 1$. Zřejmě $y \in U(R)$.
Celkem: $U(R)$ spolu s operací násobení je grupa.

Pro těleso T označme $T^\times$ množinu všech nenulových prvků tělesa T.

2.2.2. Tvrzení. *Nechť T je těleso. Pak $U(T) = T^\times$. Specielně, $T^\times$ spolu s operací násobení je komutativní grupa.*

Důkaz. Nechť $x \in U(T)$. Chceme: $x \in T^\times$. Předpokládejme opak, tj. $x = 0$. Jelikož x je jednotka tělesa T, existuje $y \in T$, $x \cdot y = 1$. Ovšem $x = 0$, takže $0 \cdot y = 1$, $0 = 1$. Pak pro libovolné $a \in T$ máme $0 \cdot a = 1 \cdot a$, $0 = a$. Tudíž těleso T má pouze jeden prvek , spor. Nutně tedy $x \neq 0$, $x \in T^\times$.
Naopak, nechť $x \in T^\times$. Chceme: $x \in U(T)$. Dle definice tělesa existuje $y \in T$, $x \cdot y = 1$, $y \cdot x = 1$. Pak $x \in U(T)$.
Zbytek tvrzení plyne z 2.2.1. a z faktu, že násobení v tělese je komutativní.

Vzhledem k výše uvedenému dostáváme příklady komutativních grup $U(\mathbb{Z})$, $\mathbb{Q}^\times$, $\mathbb{R}^\times$, $\mathbb{C}^\times$, $U(\mathbb{Z}_m)$, $\mathbb{Z}_p^\times$ (p je prvočíslo). Grupy $\mathbb{Q}^\times$, $\mathbb{R}^\times$, $\mathbb{C}^\times$ jsou nekonečné. Grupa $U(\mathbb{Z})$ má dva prvky, čísla 1, -1. Zde je tabulka násobení v grupě $U(\mathbb{Z})$:

$\cdot$	1	-1
1	1	-1
-1	-1	1

Grupa $\mathbb{Z}_p^\times$ má $p-1$ prvků. Pro ilustraci uvedeme tabulku násobení v grupě $\mathbb{Z}_5^\times$.

$\cdot$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{2}$	$\overline{2}$	$\overline{4}$	$\overline{1}$	$\overline{3}$
$\overline{3}$	$\overline{3}$	$\overline{1}$	$\overline{4}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Je zřejmé, že grupa $U(\mathbb{Z}_m)$ je konečná. Budeme se nyní zabývat otázkou, jaký je přesný počet prvků grupy $U(\mathbb{Z}_m)$.

Připomeňme si, že pro celá čísla a, b symbol $NSD(a,b)$ značí největší společný dělitel čísel a, b.

2.2.3. Definice. Eulerova funkce φ je definována následovně:
Jestliže n je celé číslo, $n > 0$, pak

$$\varphi(n) = card(\{k \in \mathbb{Z} |\ 0 \leq k < n,\ NSD(k,n) = 1\}).$$

2.2.4. Věta. (Bezoutova rovnost) *Pro libovolná celá čísla a, b existují celá čísla u,v taková, že*

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

Důkaz. Pokud $a = b = 0$, je $NSD(a,b) = 0$ a stačí vzít $u = v = 0$.
Nechť $a \neq 0$ nebo $b \neq 0$. Pro určitost předpokládejme, že $a \neq 0$. Buď

$$M = \{x \cdot a + y \cdot b |\ x, y \in \mathbb{Z}, x \cdot a + y \cdot b > 0\}.$$

Je-li $a > 0$, pak $1 \cdot a + 0 \cdot b \in M$. Je-li $a < 0$, pak $(-1) \cdot a + 0 \cdot b \in M$. Tudíž $M \neq \emptyset$. Buď $d = \min M$. Uvědomme si, že $d = u \cdot a + v \cdot b$ pro jistá $u, v \in \mathbb{Z}$. Ukážeme, že $d = NSD(a,b)$. Je třeba ukázat dvě věci:
(I) d dělí a, d dělí b
(II) Jestliže $e \in \mathbb{Z}$, e dělí a, e dělí b, pak e dělí d.
ad (I): Ukážeme, že d dělí a. Fakt, že d dělí b, se ukáže obdobně. Číslo a vydělme se zbytkem číslem d: $a = d \cdot q + r$, $q, r \in \mathbb{Z}$, $0 \leq r < d$. Chceme: $r = 0$. Předpokládejme, že $0 < r$. Platí:

$$\begin{aligned} a &= (u \cdot a + v \cdot b) \cdot q + r \\ a &= uqa + vqb + r \\ a - uqa - vqb &= r \\ (1 - uq) \cdot a + (-vq) \cdot b &= r \end{aligned}$$

Jelikož $1-uq$, $-vq$ jsou celá čísla a $r > 0$, je $r \in M$. Ovšem $r < d$, $d = \min M$. Dostali jsme spor. Takže $0 = r$.

ad (II): Nechť $e \in \mathbb{Z}$, e dělí a, e dělí b. Chceme: e dělí d. Existují $r, s \in \mathbb{Z}$, $a = e \cdot r$, $b = e \cdot s$. Pak

$$d = ua + vb = uer + ves = e(ur + vs).$$

Dokázali jsme, že e dělí d.

2.2.5. Tvrzení. *Nechť m je kladné celé číslo. Pro každé celé číslo k platí:*

$$\overline{k} \in U(\mathbb{Z}_m) \iff NSD(k, m) = 1.$$

Důkaz. Buď k celé číslo.
Nechť $\overline{k} \in U(\mathbb{Z}_m)$. Chceme: $NSD(k, m) = 1$.
Existuje celé číslo l, $\overline{k} \cdot \overline{l} = \overline{1}$. Tedy $\overline{kl} = \overline{1}$, $kl \equiv 1\ (m)$, m dělí $1 - kl$, $1 - kl = mq$ pro nějaké $q \in \mathbb{Z}$. Buď $d \in \mathbb{Z}$, d dělí k, d dělí m. Je třeba ukázat, že d dělí 1. Pak bude jasné, že $NSD(k, m) = 1$. Je $1 = mq + kl$. Protože d dělí m, d dělí k, dostáváme: d dělí 1.
Nechť $NSD(k, m) = 1$. Chceme: $\overline{k} \in U(\mathbb{Z}_m)$. Použijeme Bezoutovu rovnost (2.2.4.). Existují taková celá čísla u, v, že $1 = uk + vm$. Pak $1 - uk = vm$, m dělí $1 - uk$, $uk \equiv 1\ (m)$, $\overline{uk} = \overline{1}$, $\overline{u} \cdot \overline{k} = \overline{1}$. Vidíme, že $\overline{k}$ je jednotka okruhu $\mathbb{Z}_m$ (čili $\overline{k} \in U(\mathbb{Z}_m)$).

2.2.6. Věta. *Nechť m je kladné celé číslo. Platí:*

$$card(U(\mathbb{Z}_m)) = \varphi(m).$$

Důkaz. Uvědomme si, že okruh $\mathbb{Z}_m$ má přesně m prvků, totiž $\overline{0}, \overline{1}, \ldots, \overline{m-1}$ (viz 2.1.6.). Buď k celé číslo, $0 \leq k \leq m - 1$. Dle 2.2.5. je $\overline{k} \in U(\mathbb{Z}_m)$ právě tehdy, když $NSD(k, m) = 1$. Pak

$$card(U(\mathbb{Z}_m)) = card(\{k \in \mathbb{Z} |\ 0 \leq k < m,\ NSD(k, m) = 1\}).$$

Nyní si pouze uvědomme, že

$$\varphi(m) = card(\{k \in \mathbb{Z} |\ 0 \leq k < m,\ NSD(k, m) = 1\}).$$

Zvolme například $m = 10$. Je $\varphi(10) = 4$, tudíž $card(U(\mathbb{Z}_{10})) = 4$. Prvky grupy $U(\mathbb{Z}_{10})$ jsou $\overline{1}$, $\overline{3}$, $\overline{7}$, $\overline{9}$. Zde je tabulka násobení v grupě $U(\mathbb{Z}_{10})$:

$\cdot$	$\overline{1}$	$\overline{3}$	$\overline{7}$	$\overline{9}$
$\overline{1}$	$\overline{1}$	$\overline{3}$	$\overline{7}$	$\overline{9}$
$\overline{3}$	$\overline{3}$	$\overline{9}$	$\overline{1}$	$\overline{7}$
$\overline{7}$	$\overline{7}$	$\overline{1}$	$\overline{9}$	$\overline{3}$
$\overline{9}$	$\overline{9}$	$\overline{7}$	$\overline{3}$	$\overline{1}$

2.3 Symetrická grupa

S největší pravděpodobností již znáte pojem permutace. Například v lineární algebře se o něm většinou hovoří před vyslovením definice determinantu matice.

2.3.1. Definice. Nechť M je množina. **Permutací množiny** M rozumíme každou bijekci množiny M na množinu M. Množinu všech permutací množiny M budeme značit $S(M)$. Tedy

$$S(M) = \{\pi : M \to M |\ \pi \text{ je permutace}\}.$$

2.3.2. Věta. *Množina $S(M)$ s operací skládání zobrazení je grupa.*

Důkaz. Například [3], 6.1.2.

2.3.3. Definice. Grupa $S(M)$ se nazývá **symetrická grupa množiny** M. Nechť $n \in \mathbb{N}$. Místo $S(\{1, 2, \ldots, n\})$ píšeme S_n a hovoříme o symetrické grupě n prvků.

2.3.4. Věta. *Nechť M je množina. Platí:*
Grupa $S(M)$ je komutativní právě tehdy, když množina M má nejvýše 2 prvky.
Specielně: S_1, S_2 jsou komutativní, S_3, S_4, S_5, S_6 atd. jsou nekomutativní.

Důkaz. Například [3], 6.1.4.

2.3.5. Věta. *Nechť $n \in \mathbb{N}$. Grupa S_n je konečná a má $n!$ prvků.*

Důkaz. Důkaz přenecháváme čtenáři.

2.3.6. Označení. Nechť $n \in \mathbb{N}$, $\pi \in S_n$. Někdy budeme psát

$$\pi = \begin{pmatrix} 1 & 2 & \dots & n \\ \pi(1) & \pi(2) & \dots & \pi(n) \end{pmatrix}.$$

2.3.7. Definice. Nechť $n \in \mathbb{N}$, $i, j \in \{1, 2, \dots, n\}$, $i \neq j$. Definujeme permutaci $(i \leftrightarrow j) \in S_n$ takto:
$(i \leftrightarrow j)(i) = j$
$(i \leftrightarrow j)(j) = i$
$(i \leftrightarrow j)(k) = k$ pro každé $k \in \{1, 2, \dots, n\} - \{i, j\}$.
Permutace $(i \leftrightarrow j)$ se nazývá **transpozice** prvků i a j.

2.3.8. Věta. *Nechť $n \in \mathbb{N}$, $n \geq 2$, $\pi \in S_n$. Platí:*
existují transpozice $\tau_1, \tau_2, \dots, \tau_k \in S_n$ ($k \in \mathbb{N}$) tak, že $\pi = \tau_1 \tau_2 \dots \tau_k$.

Důkaz. Například [3], 6.1.8.

2.3.9. Definice. Nechť $n \in \mathbb{N}$, $\pi \in S_n$, $(i, j) \in \{1, 2, \dots, n\}^2$.
Dvojice (i, j) se nazývá **inverze** v permutaci π, platí-li:

1. $i < j$
2. $\pi(i) > \pi(j)$.

π se nazývá **sudá permutace**, je-li počet všech inverzí v permutaci π sudý.
π se nazývá **lichá permutace**, je-li počet všech inverzí v permutaci π lichý.
Dále definujeme

$$Sg(\pi) = \begin{cases} 1 & \text{pro sudou permutaci } \pi \\ -1 & \text{pro lichou permutaci } \pi. \end{cases}$$

2.3.10. Tvrzení. *Nechť $n \in \mathbb{N}$, $\tau \in S_n$, τ je transpozice. Platí: $Sg(\tau) = -1$.*

Důkaz. Například [3], 6.2.2.

2.3.11. Věta. *Nechť $n \in \mathbb{N}$, $\pi, \tau \in S_n$, τ je transpozice. Platí: $Sg(\tau\pi) = -Sg(\pi)$.*

Důkaz. Například [3], 6.2.3.

2.3.12. Věta. *Nechť $n \in \mathbb{N}$, $\pi, \rho \in S_n$. Platí:*

$$Sg(\pi\rho) = Sg(\pi) \cdot Sg(\rho).$$

Důkaz. Například [3], 6.2.4.

2.3.13. Příklad. Uvedeme příklad symetrické grupy S_3. Grupa S_3 není komutativní (viz 2.3.4.) a má $3! = 6$ prvků:

$$i = \begin{pmatrix}123\\123\end{pmatrix}, a = \begin{pmatrix}123\\132\end{pmatrix}, b = \begin{pmatrix}123\\321\end{pmatrix}, c = \begin{pmatrix}123\\213\end{pmatrix}, d = \begin{pmatrix}123\\231\end{pmatrix}, e = \begin{pmatrix}123\\312\end{pmatrix}.$$

Počítejme:

$$\begin{aligned}
a \cdot a &= \begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix} = \begin{pmatrix}1&2&3\\1&2&3\end{pmatrix} = i\\
a \cdot b &= \begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix} = \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix} = e\\
a \cdot c &= \begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix} = \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix} = d\\
a \cdot d &= \begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix} = \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix} = c\\
a \cdot e &= \begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix} = \begin{pmatrix}1&2&3\\3&2&1\end{pmatrix} = b\\
b \cdot a &= \begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix} = \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix} = d\\
b \cdot b &= \begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix} = \begin{pmatrix}1&2&3\\1&2&3\end{pmatrix} = i\\
b \cdot c &= \begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix} = \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix} = e\\
b \cdot d &= \begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix} = \begin{pmatrix}1&2&3\\1&3&2\end{pmatrix} = a\\
b \cdot e &= \begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix} = \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix} = c\\
c \cdot a &= \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix} = \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix} = e\\
c \cdot b &= \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix} = \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix} = d\\
c \cdot c &= \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix} = \begin{pmatrix}1&2&3\\1&2&3\end{pmatrix} = i\\
c \cdot d &= \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix} = \begin{pmatrix}1&2&3\\3&2&1\end{pmatrix} = b\\
c \cdot e &= \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix} = \begin{pmatrix}1&2&3\\1&3&2\end{pmatrix} = a\\
d \cdot a &= \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix} = \begin{pmatrix}1&2&3\\3&2&1\end{pmatrix} = b\\
d \cdot b &= \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix} = \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix} = c\\
d \cdot c &= \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix} = \begin{pmatrix}1&2&3\\1&3&2\end{pmatrix} = a\\
d \cdot d &= \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix} = \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix} = e\\
d \cdot e &= \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix} = \begin{pmatrix}1&2&3\\1&2&3\end{pmatrix} = i\\
e \cdot a &= \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix} = \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix} = c\\
e \cdot b &= \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix} = \begin{pmatrix}1&2&3\\1&3&2\end{pmatrix} = a\\
e \cdot c &= \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix} = \begin{pmatrix}1&2&3\\3&2&1\end{pmatrix} = b\\
e \cdot d &= \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix} = \begin{pmatrix}1&2&3\\1&2&3\end{pmatrix} = i\\
e \cdot e &= \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix} = \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix} = d.
\end{aligned}$$

Tabulka násobení v grupě S_3 vypadá následovně:

	i	a	b	c	d	e
i	i	a	b	c	d	e
a	a	i	e	d	c	b
b	b	d	i	e	a	c
c	c	e	d	i	b	a
d	d	b	c	a	e	i
e	e	c	a	b	i	d

Nyní permutace z grupy S_3 rozložíme na součin transpozic (viz 2.3.8.).

$$\begin{aligned} i &= (1 \leftrightarrow 2)(1 \leftrightarrow 2) \\ a &= (2 \leftrightarrow 3) \\ b &= (1 \leftrightarrow 3) \\ c &= (1 \leftrightarrow 2) \\ d &= (1 \leftrightarrow 2)(1 \leftrightarrow 3) \\ e &= (1 \leftrightarrow 3)(1 \leftrightarrow 2) \end{aligned}$$

Konečně, pro každé $\pi \in S_3$ určíme $Sg(\pi)$.
V permutaci i je nula inverzí, takže $Sg(i) = 1$.
V permutaci a je jedna inverze $(2, 3)$, takže $Sg(a) = -1$.
V permutaci b jsou tři inverze $(1, 2)$, $(1, 3)$, $(2, 3)$, takže $Sg(b) = -1$.
V permutaci c je jedna inverze $(1, 2)$, takže $Sg(c) = -1$.
V permutaci d jsou dvě inverze $(1, 3)$, $(2, 3)$, takže $Sg(d) = 1$.
V permutaci e jsou dvě inverze $(1, 2)$, $(1, 3)$, takže $Sg(e) = 1$.

Nyní dokážeme: Jestliže považujeme izomorfní grupy za stejné, pak jediné grupy, které existují, jsou symetrické grupy a jejich podgrupy.

2.3.14. Věta. (Cayley, 1878) *Nechť G je grupa. Pak G je izomorfní nějaké podgrupě symetrické grupy $S(G)$. Specielně: Jestliže G má konečný řád n, pak G je izomorfní nějaké podgrupě grupy S_n.*

Důkaz. Buď $a \in G$. Definujeme zobrazení $\varphi(a) : G \to G$ takto:

$$\varphi(a) = xa$$

$(x \in G)$.
Ukážeme, že $\varphi(a)$ je bijekce, tj. že $\varphi(a) \in S(G)$.
(I) $\varphi(a)$ je injekce:
Nechť $x, y \in G$, $\varphi(a)(x) = \varphi(a)(y)$. Chceme: $x = y$.
Víme, že $xa = ya$. Dle zákonů o krácení pak $x = y$.
(II) $\varphi(a)$ je surjekce:
Buď $y \in G$. Hledáme $x \in G$ takové, že $\varphi(a)(x) = y$.
Položme $x = ya^{-1}$. Pak $\varphi(a)(x) = \varphi(a)(ya^{-1}) = (ya^{-1})a = y(aa^{-1}) = y \cdot 1 = y$.
Máme tedy zobrazení $\varphi : G \to S(G)$. Ukážeme, že φ je injektivní homomorfismus.

(I) φ je injekce:
Nechť $a, b \in G$, $\varphi(a) = \varphi(b)$. Chceme: $a = b$.
Určitě $\varphi(a)(1) = \varphi(b)(1)$. Takže $1 \cdot a = 1 \cdot b$, $a = b$.
(II) φ je homomorfismus:
Nechť $a, b \in G$. Chceme: $\varphi(ab) = \varphi(a)\varphi(b)$.
Je potřeba dokázat rovnost zobrazení $\varphi(ab)$, $\varphi(a)\varphi(b)$. Máme tedy pro každé $x \in G$ ukázat, že $\varphi(ab)(x) = (\varphi(a)\varphi(b))(x)$.
Počítejme:
$(\varphi(a)\varphi(b))(x) = \varphi(b)(\varphi(a)(x)) = \varphi(b)(xa) = (xa)b = x(ab) = \varphi(ab)(x)$.
Na závěr si uvědomme, že grupa G je izomorfní podgrupě $\varphi(G)$ grupy $S(G)$.

2.3.15. Příklad. Grupa $\mathbb{Z}_4$ je izomorfní jisté podgrupě v S_4. Vezměme zobrazení $\varphi : \mathbb{Z}_4 \to S(\mathbb{Z}_4)$ z důkazu věty 2.3.14. Pro stručnost budeme psát pouze 0 místo $\overline{0}$, 1 místo $\overline{1}$ atd.

$$\varphi(0) = \begin{pmatrix}0123\\0123\end{pmatrix} = i,\ \varphi(1) = \begin{pmatrix}0123\\1230\end{pmatrix} = a$$

$$\varphi(2) = \begin{pmatrix}0123\\2301\end{pmatrix} = b,\ \varphi(3) = \begin{pmatrix}0123\\3012\end{pmatrix} = c$$

$$\begin{array}{rcccccl}
a \cdot a &=& \left(\begin{smallmatrix}0123\\1230\end{smallmatrix}\right)\left(\begin{smallmatrix}0123\\1230\end{smallmatrix}\right) &=& \left(\begin{smallmatrix}0123\\2301\end{smallmatrix}\right) &=& b \\
a \cdot b &=& \left(\begin{smallmatrix}0123\\1230\end{smallmatrix}\right)\left(\begin{smallmatrix}0123\\2301\end{smallmatrix}\right) &=& \left(\begin{smallmatrix}0123\\3012\end{smallmatrix}\right) &=& c \\
a \cdot c &=& \left(\begin{smallmatrix}0123\\1230\end{smallmatrix}\right)\left(\begin{smallmatrix}0123\\3012\end{smallmatrix}\right) &=& \left(\begin{smallmatrix}0123\\0123\end{smallmatrix}\right) &=& i \\
b \cdot a &=& \left(\begin{smallmatrix}0123\\2301\end{smallmatrix}\right)\left(\begin{smallmatrix}0123\\1230\end{smallmatrix}\right) &=& \left(\begin{smallmatrix}0123\\3012\end{smallmatrix}\right) &=& c \\
b \cdot b &=& \left(\begin{smallmatrix}0123\\2301\end{smallmatrix}\right)\left(\begin{smallmatrix}0123\\2301\end{smallmatrix}\right) &=& \left(\begin{smallmatrix}0123\\0123\end{smallmatrix}\right) &=& i \\
b \cdot c &=& \left(\begin{smallmatrix}0123\\2301\end{smallmatrix}\right)\left(\begin{smallmatrix}0123\\3012\end{smallmatrix}\right) &=& \left(\begin{smallmatrix}0123\\1230\end{smallmatrix}\right) &=& a \\
c \cdot a &=& \left(\begin{smallmatrix}0123\\3012\end{smallmatrix}\right)\left(\begin{smallmatrix}0123\\1230\end{smallmatrix}\right) &=& \left(\begin{smallmatrix}0123\\0123\end{smallmatrix}\right) &=& i \\
c \cdot b &=& \left(\begin{smallmatrix}0123\\3012\end{smallmatrix}\right)\left(\begin{smallmatrix}0123\\2301\end{smallmatrix}\right) &=& \left(\begin{smallmatrix}0123\\1230\end{smallmatrix}\right) &=& a \\
c \cdot c &=& \left(\begin{smallmatrix}0123\\3012\end{smallmatrix}\right)\left(\begin{smallmatrix}0123\\3012\end{smallmatrix}\right) &=& \left(\begin{smallmatrix}0123\\2301\end{smallmatrix}\right) &=& b
\end{array}$$

Grupy $\mathbb{Z}_4$ a $\varphi(\mathbb{Z}_4)$ jsou izomorfní - snadno to nahlédneme při porovnání tabulek násobení v obou grupách.

$\mathbb{Z}_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\varphi(\mathbb{Z}_4)$	i	a	b	c
i	i	a	b	c
a	a	b	c	i
b	b	c	i	a
c	c	i	a	b

2.4 Alternující grupa

2.4.1. Označení. Nechť $n \in \mathbb{N}$. Klademe

$$A_n = \{\pi \in S_n |\ Sg(\pi) = 1\}.$$

2.4.2. Tvrzení. *Nechť $n \in \mathbb{N}$. Platí: A_n je podgrupa grupy S_n.*

Důkaz. Například [3], 6.3.2.

Grupa A_n se nazývá **alternující grupa** n prvků.

2.4.3. Tvrzení. *Nechť $n \in \mathbb{N}$, $n \geq 2$. Platí: $card(A_n) = \frac{1}{2} card(S_n)$ (tedy $card(A_n) = \frac{n!}{2}$).*

Důkaz. Například [3], 6.3.3.

2.4.4. Příklad. Alternující grupa A_3 má $\frac{3!}{2} = 3$ prvky. Vypišme všechny prvky grupy S_3:

$$i = \begin{pmatrix}123\\123\end{pmatrix}, a = \begin{pmatrix}123\\132\end{pmatrix}, b = \begin{pmatrix}123\\321\end{pmatrix}, c = \begin{pmatrix}123\\213\end{pmatrix}, d = \begin{pmatrix}123\\231\end{pmatrix}, e = \begin{pmatrix}123\\312\end{pmatrix}.$$

V příkladu 2.3.13. jsme zjistili, že $Sg(i) = 1$, $Sg(a) = -1$, $Sg(b) = -1$, $Sg(c) = -1$, $Sg(d) = 1$, $Sg(e) = 1$. Takže $A_3 = \{i, d, e\}$. Uvedeme ještě tabulku násobení v grupě A_3.

A_3	i	d	e
i	i	d	e
d	d	e	i
e	e	i	d

2.5 Obecná lineární grupa

Nechť T je těleso, $m, n \in \mathbb{N}$. Množinu všech matic typu (m, n) nad tělesem T budeme značit $T_{m,n}$.

Jestliže $A \in T_{m,n}$, pak $h(A)$ značí hodnost matice A. Jestliže $A \in T_{n,n}$, pak $|A|$ značí determinant matice A a A^{-1} značí matici inverzní k matici A.

Nechť $A \in T_{n,n}$. Uvažme následující tři výroky:
(I) $h(A) = n$
(II) $|A| \neq 0$
(III) matice A^{-1} existuje.

Z lineární algebry víme, že výroky (I), (II), (III) jsou ekvivalentní. Matice A, pro niž jsou výroky (I), (II) a (III) pravdivé, se nazývá regulární.

Podrobnější informace o maticích (včetně důkazů) může čtenář najít například v kapitolách 5 a 7 studijního textu [3].

Nechť $GL(n, T)$ je množina všech čtvercových regulárních matic n-tého stupně nad tělesem T. Tedy

$$GL(n, T) = \{A \in T_{n,n} |\ h(A) = n\}.$$

2.5.1. Tvrzení. *Množina $GL(n, T)$ s operací násobení matic je grupa.*

Důkaz. Nejdříve se musíme přesvědčit, že množina $GL(n, T)$ je uzavřená vzhledem k operaci násobení matic. Nechť $A, B \in GL(n, T)$. Chceme: $A \cdot B \in GL(n, T)$. Víme: $A, B \in T_{n,n}$, $|A| \neq 0$, $|B| \neq 0$. Zřejmě $A \cdot B \in T_{n,n}$. Dále, $|A \cdot B| = |A| \cdot |B| \neq 0$. Vidíme, že $A \cdot B \in GL(n, T)$. Je dobře známo, že operace násobení čtvercových matic n-tého stupně je asociativní a má neutrální prvek E_n (jednotková matice n-tého stupně). Uvědomme si, že $|E_n| = 1 \neq 0$, takže $E_n \in GL(n, T)$. Nechť $A \in GL(n, T)$. Protože A je regulární, existuje matice A^{-1}. Platí: $A \cdot A^{-1} = A^{-1} \cdot A = E_n$. Pro determinanty pak máme $|A \cdot A^{-1}| = |E_n|$, $|A| \cdot |A^{-1}| = 1$. Z toho vyplývá, že $|A^{-1}| \neq 0$ a tudíž $A^{-1} \in GL(n, T)$.

2.5.2. Definice. Nechť T je těleso, $n \in \mathbb{N}$. Grupa $GL(n, T)$ se nazývá **obecná lineární grupa**.

Všimněme si, že $GL(1, T) \cong T^{\times}$.

2.5.3. Tvrzení. *Nechť T je těleso, $n \in \mathbb{N}$. Platí: grupa $GL(n, T)$ je komutativní právě tehdy, když $n = 1$.*

Důkaz.
$\Rightarrow$: Předpokládejme, že $n > 1$. Ukážeme, že $GL(n,T)$ není komutativní.
Definujeme matici $A \in T_{n,n}$ takto: $a_{ii} = 1$ pro $1 \leq i \leq n$, $a_{12} = 1$, $a_{ij} = 0$ v ostatních případech.
Definujeme matici $B \in T_{n,n}$ takto: $b_{ii} = 1$ pro $1 \leq i \leq n$, $b_{21} = 1$, $b_{ij} = 0$ v ostatních případech.
Položme $C = A \cdot B$, $D = B \cdot A$. Je $c_{11} = 1 + 1$, $d_{11} = 1$. Předpokládejme, že $c_{11} = d_{11}$. Pak $1 + 1 = 1$, $1 = 0$, spor. Nutně tedy $c_{11} \neq d_{11}$, $C \neq D$, $A \cdot B \neq B \cdot A$. Dále, $|A| = 1$, $|B| = 1$, takže $A, B \in GL(n,T)$. Ukázali jsme, že grupa $GL(n,T)$ není komutativní.
$\Leftarrow$: Grupa $GL(1,T)$ je komutativní, protože $GL(1,T) \cong T^{\times}$.

2.5.4. Tvrzení. *Nechť T je těleso, $n \in \mathbb{N}$. Platí: grupa $GL(n,T)$ je konečná právě tehdy, když těleso T je konečné.*

Důkaz.
$\Rightarrow$: Předpokládejme, že těleso T je nekonečné. Ukážeme, že grupa $GL(n,T)$ je nekonečná. Buď $c \in T$, $c \neq 0$. Uvažme následující diagonální matici $A \in T_{n,n}$: $a_{11} = c$, $a_{ii} = 1$ pro $2 \leq i \leq n$. Je $|A| = c \neq 0$, takže $A \in GL(n,T)$. Sestrojili jsme nekonečně mnoho prvků grupy $GL(n,T)$.
$\Leftarrow$: Grupa $GL(n,T)$ je konečná, protože množina $T_{n,n}$ je konečná.

Jestliže p je prvočíslo, pak $\mathbb{Z}_p$ je těleso. Grupa $GL(n,\mathbb{Z}_p)$ se někdy označuje $GL(n,p)$. Kolik prvků má grupa $GL(n,p)$?

2.5.5. Věta. *Nechť T je konečné těleso, $card(T) = q$. Nechť $n \in \mathbb{N}$. Platí:*

$$card(GL(n,T)) = (q^n - 1) \cdot (q^n - q) \cdot (q^n - q^2) \cdot \cdots \cdot (q^n - q^{n-1}).$$

Důkaz. Je třeba určit počet všech čtvercových regulárních matic n-tého stupně nad tělesem T. Buď $A \in T_{n,n}$. Pro $i \in \{1, 2, \ldots, n\}$ označme i-tý řádek matice A symbolem $\overrightarrow{a_i}$. Chceme, aby A byla regulární. Lze tedy vektor $\overrightarrow{a_1}$ zvolit libovolně až na to, že musí být $\overrightarrow{a_1} \neq \overrightarrow{0}$. Tudíž existuje $q^n - 1$ způsobů, jak zvolit vektor $\overrightarrow{a_1}$. Předpokládejme, že vektor $\overrightarrow{a_1}$ je již vybrán. Vektory $\overrightarrow{a_1}$, $\overrightarrow{a_2}$ jsou lineárně nezávislé. Je tedy $\overrightarrow{a_2} \in T^n - \langle\{\overrightarrow{a_1}\}\rangle$. Tudíž existuje $q^n - q$ způsobů, jak zvolit vektor $\overrightarrow{a_2}$. Vidíme, že první dva řádky matice A lze zvolit $(q^n - 1) \cdot (q^n - q)$ způsoby. Předpokládejme, že vektory $\overrightarrow{a_1}$, $\overrightarrow{a_2}$ jsou již vybrány.

Vektory $\overrightarrow{a_1}, \overrightarrow{a_2}, \overrightarrow{a_3}$ jsou lineárně nezávislé. Je tedy $\overrightarrow{a_3} \in T^n - \langle\{\overrightarrow{a_1}, \overrightarrow{a_2}\}\rangle$. Tudíž existuje $q^n - q^2$ způsobů, jak zvolit vektor $\overrightarrow{a_3}$. Vidíme, že první tři řádky matice A lze zvolit $(q^n-1)\cdot(q^n-q)\cdot(q^n-q^2)$ způsoby. Postupujeme dále až k závěru, že matici A lze zvolit $(q^n-1)\cdot(q^n-q)\cdot(q^n-q^2)\cdot\dots\cdot(q^n-q^{n-1})$ způsoby.

2.5.6. Příklad.

1. Grupa $GL(3,3)$ má $(3^3-1)\cdot(3^3-3)\cdot(3^3-3^2) = 26\cdot 24\cdot 18 = 11232$ prvků.
2. Grupa $GL(3,2)$ má $(2^3-1)\cdot(2^3-2)\cdot(2^3-2^2) = 7\cdot 6\cdot 4 = 168$ prvků.
3. Grupa $GL(2,3)$ má $(3^2-1)\cdot(3^2-3) = 8\cdot 6 = 48$ prvků.
4. Grupa $GL(2,2)$ má $(2^2-1)\cdot(2^2-2) = 3\cdot 2 = 6$ prvků. Jsou to tyto prvky:

$$\begin{pmatrix} \overline{1} & \overline{0} \\ \overline{0} & \overline{1} \end{pmatrix}, \begin{pmatrix} \overline{1} & \overline{0} \\ \overline{1} & \overline{1} \end{pmatrix}, \begin{pmatrix} \overline{0} & \overline{1} \\ \overline{1} & \overline{0} \end{pmatrix}, \begin{pmatrix} \overline{0} & \overline{1} \\ \overline{1} & \overline{1} \end{pmatrix}, \begin{pmatrix} \overline{1} & \overline{1} \\ \overline{1} & \overline{0} \end{pmatrix}, \begin{pmatrix} \overline{1} & \overline{1} \\ \overline{0} & \overline{1} \end{pmatrix}.$$

2.6 Grupa symetrií obrazce

Nejdříve připomeneme pojem metrického prostoru. Nechť X je neprázdná množina, $d : X^2 \to \mathbb{R}$. Dvojice (X,d) se nazývá **metrický prostor**, pokud platí:

1. $d(a,b) \geq 0$ (pro všechna $a,b \in X$)
2. $d(a,b) = 0$ právě tehdy, když $a = b$ (pro všechna $a,b \in X$)
3. $d(a,b) = d(b,a)$ (pro všechna $a,b \in X$)
4. $d(a,b) \leq d(a,c) + d(c,b)$ (pro všechna $a,b,c \in X$).

Zobrazení d se nazývá **metrika**. Prvky metrického prostoru se nazývají zpravidla **body**. Jsou-li a, b body, pak jejich **vzdáleností** rozumíme číslo $d(a,b)$.

Zmíníme nyní dva základní příklady metrických prostorů. Množina $\mathbb{R}$ všech reálných čísel je metrický prostor, definujeme-li $d(a,b) = |a-b|$. Také $\mathbb{R}^2$ je metrický prostor, definujeme-li $d(A,B) = \sqrt{(a_1-b_1)^2 + (a_2-b_2)^2}$ pro

$A = (a_1, a_2)$, $B = (b_1, b_2)$. V příkladech by bylo možno pokračovat ($\mathbb{R}^3$, $\mathbb{R}^4$ atd.). Samozřejmě existují i další metrické prostory.

Kdo má hlubší zájem o metrické prostory, může se obrátit například ke knize [1] nebo ke skriptu [2].

Obrazcem v metrickém prostoru (X, d) rozumíme libovolnou množinu $\Delta \subseteq X$.

2.6.1. Definice. Nechť (X, d) je metrický prostor, $\Delta \subseteq X$. Bijekce $\pi : \Delta \to \Delta$ se nazývá **symetrie** obrazce Δ, pokud pro všechna $a, b \in \Delta$ platí:

$$d(\pi(a), \pi(b)) = d(a, b).$$

Označíme

$$Sym(\Delta) = \{\pi \in S(\Delta) |\ \pi \text{ je symetrie obrazce } \Delta\}.$$

2.6.2. Tvrzení. *Nechť (X, d) je metrický prostor, $\Delta \subseteq X$. Platí: $Sym(\Delta)$ je podgrupa grupy $S(\Delta)$.*

Důkaz. Je třeba dokázat následující tři věci:
(I) $id_\Delta \in Sym(\Delta)$
(II) Jestliže $\pi \in Sym(\Delta)$, pak $\pi^{-1} \in Sym(\Delta)$.
(III) Jestliže $\pi, \varrho \in Sym(\Delta)$, pak $\pi\varrho \in Sym(\Delta)$.
ad (I): Podmínka je zřejmě splněna.
ad (II): Nechť $\pi \in Sym(\Delta)$, nechť $a, b \in \Delta$. Chceme: $d(\pi^{-1}(a), \pi^{-1}(b)) = d(a, b)$. Jelikož $\pi \in Sym(\Delta)$, je $d(\pi(\pi^{-1}(a)), \pi(\pi^{-1}(b))) = d(\pi^{-1}(a), \pi^{-1}(b))$. Stačí si uvědomit, že $\pi(\pi^{-1}(a)) = a$, $\pi(\pi^{-1}(b)) = b$.
ad (III): Nechť $\pi, \varrho \in Sym(\Delta)$, nechť $a, b \in \Delta$. Chceme: $d((\pi\varrho)(a), (\pi\varrho)(b)) = d(a, b)$. Počítejme:

$$\begin{aligned} d((\pi\varrho)(a), (\pi\varrho)(b)) &= d(\varrho(\pi(a)), \varrho(\pi(b))) \\ &= d(\pi(a), \pi(b)) \\ &= d(a, b). \end{aligned}$$

2.6.3. Definice. Nechť (X, d) je metrický prostor, $\Delta \subseteq X$. **Grupu symetrií obrazce** Δ definujeme jako grupu $Sym(\Delta)$.

2.6.4. Příklad. Nechť (X, d) je diskrétní metrický prostor, tedy

$$d(a,b) = \begin{cases} 0 & \text{pokud } a = b \\ 1 & \text{pokud } a \neq b \end{cases}$$

Buď $\Delta \subseteq X$, $\pi \in S(\Delta)$, $a, b \in \Delta$. Jestliže $a = b$, pak $\pi(a) = \pi(b)$, $d(a,b) = 0$, $d(\pi(a), \pi(b)) = 0$. Jestliže $a \neq b$, pak $\pi(a) \neq \pi(b)$, $d(a,b) = 1$, $d(\pi(a), \pi(b)) = 1$. V každém případě tedy $d(\pi(a), \pi(b)) = d(a,b)$ a $\pi \in Sym(\Delta)$. Ukázali jsme, že $Sym(\Delta) = S(\Delta)$.

2.6.5. Příklad. Nechť (X, d) je metrický prostor, A, B, C jsou tři různé body prostoru X. Uvažme $\Delta = \{A, B, C\}$.
Jestliže trojúhelník ABC je rovnostranný, pak zřejmě $Sym(\Delta) = S(\Delta) \cong S_3$.
Nechť trojúhelník ABC je rovnoramenný, nikoli však rovnostranný. Pro určitost předpokládejme, že $d(A,B) = d(A,C)$. Buď $\pi \in Sym(\Delta)$. Snadno se nahlédne, že $\pi(B) = B$, $\pi(C) = C$ nebo $\pi(B) = C$, $\pi(C) = B$. V prvním případě $\pi = \binom{ABC}{ABC}$, ve druhém případě $\pi = \binom{ABC}{ACB}$. Tudíž $Sym(\Delta) = \{\binom{ABC}{ABC}, \binom{ABC}{ACB}\} \cong \mathbb{Z}_2$.
Nechť trojúhelník ABC je obecný, nikoli rovnoramenný. Buď $\pi \in Sym(\Delta)$. Je $\pi(A) = A$, $\pi(B) = B$ nebo $\pi(A) = B$, $\pi(B) = A$. Druhý případ není možný, neboť by dával $\pi = \binom{ABC}{BAC}$, $d(B,C) = d(A,C)$ a trojúhelník ABC by byl rovnoramenný. Takže $\pi = \binom{ABC}{ABC}$ a grupa $Sym(\Delta)$ je triviální.

2.6.6. Příklad. Uvažme metrický prostor $(\mathbb{R}^2, d)$, ve kterém je $d(A,B) = \sqrt{(a_1 - b_1)^2 + (a_2 - b_2)^2}$ pro $A = (a_1, a_2)$, $B = (b_1, b_2)$. Buď K kružnice v $(\mathbb{R}^2, d)$ se středem v bodě $(0,0)$. Grupa $Sym(K)$ je nekonečná. Buď $0 \leq \alpha < 2\pi$. Označme r_α otočení kružnice K o úhel α (střed otočení je v bodě $(0,0)$). Pak $r_\alpha \in Sym(K)$ a tedy grupa $Sym(K)$ má nespočetně mnoho prvků.

2.6.7. Příklad. Uvažme metrický prostor $(\mathbb{R}, d)$, kde $d(a,b) = |a - b|$ pro $a, b \in \mathbb{R}$. Nechť Δ je uzavřený interval $[0,1]$. Nechť $0 \leq c \leq 1$. Definujme zobrazení $f_c : \Delta \to \Delta$ takto:

$$f_c(x) = \begin{cases} c & \text{pro } x = 0 \\ 0 & \text{pro } x = c \\ x & \text{pro } x \neq 0, x \neq c \end{cases}$$

Zřejmě f_c je bijekce a tedy $f_c \in S(\Delta)$. Ukázali jsme, že grupa $S(\Delta)$ je nespočetná.

Nyní uvidíme, že grupa $Sym(\Delta)$ má pouze dva prvky. Buď $f \in Sym(\Delta)$. Je zřejmé, že nastane právě jedna ze dvou následujících možností:
(I) $f(0) = 0$, $f(1) = 1$
(II) $f(0) = 1$, $f(1) = 0$.
ad (I): Nechť $x \in \Delta$. Je $|f(x) - f(0)| = |x - 0|$, tj. $|f(x)| = |x|$, $f(x) = x$. Takže $f = id$.
ad (II): Nechť $x \in \Delta$. Je $|f(x) - f(1)| = |x - 1|$, tj. $|f(x) - 0| = |x - 1|$, $|f(x)| = |x - 1|$, $f(x) = 1 - x$. Ukázali jsme, že $Sym(\Delta) = \{id, f\}$, kde $f(x) = 1 - x$ pro $x \in \Delta$.

2.6.8. Věta. *Nechť $n \in \mathbb{Z}$, $n \geq 3$. Nechť Δ je množina vrcholů pravidelného n-úhelníka v prostoru $\mathbb{R}^2$ s metrikou $d(A, B) = \sqrt{(a_1 - b_1)^2 + (a_2 - b_2)^2}$, kde $A = (a_1, a_2)$, $B = (b_1, b_2)$. Pak $Sym(\Delta)$ je grupa řádu $2n$, která je generována dvěma prvky S a T takovými, že*

$$S^n = 1,\ T^2 = 1 \text{ a } TST = S^{-1}.$$

Důkaz. Pro $k \in \mathbb{Z}$ položme $V_k = (\cos k\frac{2\pi}{n}, \sin k\frac{2\pi}{n})$. Bez újmy na obecnosti lze předpokládat, že $\Delta = \{V_k |\ k \in \mathbb{Z}\} = \{V_0, V_1, \ldots, V_{n-1}\}$. Označme S otočení obrazce Δ o úhel $\frac{2\pi}{n}$ (střed otáčení je v bodě $(0, 0)$). Pro každé $k \in \mathbb{Z}$ je $S(V_k) = V_{k+1}$, $S^2(V_k) = S(S(V_k)) = S(V_{k+1}) = V_{k+2}$, $\ldots$, $S^n(V_k) = V_{k+n} = V_k$. Vidíme, že $S^n = 1$. Označme T osovou souměrnost kolem osy x. Pro každé $k \in \mathbb{Z}$ je $T(V_k) = V_{-k}$, $T^2(V_k) = T(T(V_k)) = T(V_{-k}) = V_k$. Vidíme, že $T^2 = 1$. Buď $k \in \mathbb{Z}$. Pak $TST(V_k) = (ST)(T(V_k)) = (ST)(V_{-k}) = T(S(V_{-k})) = T(V_{-k+1}) = V_{k-1} = S^{-1}(V_k)$. Vidíme, že $TST = S^{-1}$. Jistě $S, T \in Sym(\Delta)$. Prvky 1, S, S^2, $\ldots$, S^{n-1} jsou navzájem různé. Také prvky T, TS, TS^2, $\ldots$, TS^{n-1} jsou navzájem různé. Buď $i, j \in \{0, 1, \ldots, n-1\}$, $S^i = TS^j$. Pak $S^i(V_0) = (TS^j)(V_0)$, $V_i = V_j$, $i = j$. Takže $S^i = TS^i$, $1 = T$, spor. Tudíž 1, S, S^2, $\ldots$, S^{n-1}, T, TS, TS^2, $\ldots$, TS^{n-1} je $2n$ různých prvků grupy $Sym(\Delta)$. Nyní stačí dokázat, že $\{1, S, \ldots, S^{n-1}, T, TS, \ldots, TS^{n-1}\} = Sym(\Delta)$.
$\{1, S, \ldots, S^{n-1}, T, TS, \ldots, TS^{n-1}\} \subseteq Sym(\Delta)$: Toto je jasné.
$Sym(\Delta) \subseteq \{1, S, \ldots, S^{n-1}, T, TS, \ldots, TS^{n-1}\}$: Buď $P \in Sym(\Delta)$. Předpokládejme, že $P(V_0) = V_i$, $i \in \{0, 1, \ldots, n-1\}$. Jsou dvě možnosti:
(I)$P(V_1) = V_{i+1}$
(II) $P(V_1) = V_{i-1}$

ad (I): V tomto případě $P(V_2) = V_{i+2}$ nebo $P(V_2) = V_i$. Druhý případ nenastává, protože $P(V_0) = V_i$. Takže $P(V_2) = V_{i+2}$. Dále pak $P(V_3) = V_{i+3}$ atd. Celkem $P = S^i$.
ad (II): V tomto případě $P(V_2) = V_i$ nebo $P(V_2) = V_{i-2}$. První případ nenastává, protože $P(V_0) = V_i$. Takže $P(V_2) = V_{i-2}$. Dále pak $P(V_3) = V_{i-3}$ atd. Celkem $P(V_k) = V_{-k+i}$ a $P = TS^i$.

2.6.9. Definice. Nechť n je celé číslo, $n \geq 3$. **Dihedrální grupa** D_{2n} je grupa řádu $2n$, která je generována dvěma prvky s a t takovými, že

$$s^n = 1,\ t^2 = 1 \text{ a } tst = s^{-1}.$$

2.6.10. Poznámka. Zabývejme se dihedrální grupou D_{2n}.
Z $tst = s^{-1}$ plyne $t^2st = ts^{-1}$. Protože $t^2 = 1$, máme $st = ts^{-1}$. Pak pro každé nezáporné celé číslo m platí:

$$s^m \cdot t = t \cdot s^{-m}.$$

Nechť $i, k \in \{0, 1\}$, $j, l \in \{0, 1, \ldots, n-1\}$. Vypočítáme součin $(t^i s^j) \cdot (t^k s^l)$.
$k = 0$: $(t^i s^j) \cdot (t^k s^l) = t^i s^j t^0 s^l = t^i s^j s^l = t^i s^{j+l}$
$k = 1$: $(t^i s^j) \cdot (t^k s^l) = t^i (s^j t) s^l = t^i t s^{-j} s^l = t^{i+1} s^{l-j}$
V obou případech $(t^i s^j) \cdot (t^k s^l) = t^u s^v$ pro nějaká celá čísla u, v. S využitím vztahů $t^2 = 1$, $s^n = 1$ pak můžeme tvrdit, že existují $a \in \{0, 1\}$, $b \in \{0, 1, \ldots, n-1\}$ s vlastností

$$(t^i s^j) \cdot (t^k s^l) = t^a s^b.$$

Vypočítejme ještě $(t^i s^j)^{-1}$. Je $(t^i s^j)^{-1} = (s^j)^{-1}(t^i)^{-1} = s^{-j} t^{-i}$. Protože $s^n = 1$, $t^2 = 1$, existují $c \in \{0, 1, \ldots, n-1\}$, $d \in \{0, 1\}$ taková, že $s^{-j} = s^c$, $t^{-i} = t^d$. Pak $(t^i s^j)^{-1} = s^c t^d$.
Jestliže $d = 0$, pak $s^c t^d = s^c t^0 = t^0 s^c = t^d s^c$.
Jestliže $d = 1$, pak $s^c t^d = s^c t = t s^{-c} = t^d s^{-c}$.
Uvážíme-li vztah $s^n = 1$, lze tvrdit následující:
existují $e \in \{0, 1, \ldots, n-1\}$, $d \in \{0, 1\}$ tak, že

$$(t^i s^j)^{-1} = t^d s^e.$$

Nechť nyní

$$H = \{1, s, \ldots, s^{n-1}, t, ts, \ldots, ts^{n-1}\}.$$

Výše provedené výpočty za využití vztahů $s^n = 1$, $t^2 = 1$, $tst = s^{-1}$ ukazují, že H je podgrupa grupy D_{2n}. Jelikož $s, t \in H$, je $\langle s, t\rangle \subseteq H$. Protože $\langle s, t\rangle = D_{2n}$, máme $H = D_{2n}$. Můžeme tedy učinit následující závěry:

1. Grupa D_{2n} má $2n$ prvků, a to konkrétně
$$1, s, s^2, \ldots, s^{n-1}, t, ts, ts^2, \ldots, ts^{n-1}.$$
2. Výpočty v grupě D_{2n} lze provádět pomocí vztahů $s^n = 1$, $t^2 = 1$, $tst = s^{-1}$.
3. Předchozí dva body ukazují, že definice 2.6.9. určuje grupu D_{2n} jednoznačně.
4. Grupa D_{2n} není komutativní. Abychom to zdůvodnili, tak předpokládejme opak, tj. že D_{2n} je komutativní. Pak $ts = st$, $tst = st^2 = s$. Ovšem $tst = s^{-1}$, takže $s = s^{-1}$, $s^2 = 1$. Dostali jsme spor s bodem 1.

2.6.11. Poznámka. Z věty 2.6.8. vyplývá, že dihedrální grupa D_{2n} je grupa symetrií množiny vrcholů pravidelného n-úhelníka.

2.6.12. Příklad. Sestrojíme tabulku násobení v grupě D_6. Dle poznámky 2.6.10. má grupa D_6 těchto 6 prvků:
$$1, s, s^2, t, ts, ts^2.$$
Uvědomme si, že $s^3 = 1$, $t^2 = 1$, $tst = s^{-1}$ (tj. $st = ts^{-1}$).
Nyní provedeme potřebné výpočty:
$s\cdot s = s^2$, $s\cdot s^2 = s^3 = 1$, $s\cdot t = ts^{-1} = ts^2$, $s\cdot ts = ts^{-1}s = t$, $s\cdot ts^2 = ts^{-1}s^2 = ts$
$s^2 \cdot s = s^3 = 1$, $s^2 \cdot s^2 = s^4 = s$, $s^2 \cdot t = sts^{-1} = ts^{-2} = ts$, $s^2 \cdot ts = tss = ts^2$, $s^2 \cdot ts^2 = tss^2 = t$
$t \cdot s = ts$, $t \cdot s^2 = ts^2$, $t \cdot t = t^2 = 1$, $t \cdot ts = s$, $t \cdot ts^2 = s^2$
$ts \cdot s = ts^2$, $ts \cdot s^2 = ts^3 = t$, $ts \cdot t = s^{-1} = s^2$, $ts \cdot ts = s^{-1}s = 1$, $ts \cdot ts^2 = s^{-1}s^2 = s$
$ts^2 \cdot s = t$, $ts^2 \cdot s^2 = ts^4 = ts$, $ts^2 \cdot t = tts = s$, $ts^2 \cdot ts = tts^2 = s^2$, $ts^2 \cdot ts^2 = tt = 1$

Tabulka násobení v grupě D_6 vypadá následovně:

	1	s	s^2	t	ts	ts^2
1	1	s	s^2	t	ts	ts^2
s	s	s^2	1	ts^2	t	ts
s^2	s^2	1	s	ts	ts^2	t
t	t	ts	ts^2	1	s	s^2
ts	ts	ts^2	t	s^2	1	s
ts^2	ts^2	t	ts	s	s^2	1

2.7 Kvaterniony

2.7.1. Definice. Kvaterniony je grupa $\mathbf{Q} = \langle a, b \rangle$ řádu 8, v níž

$$a^4 = 1,\ b^2 = a^2 \text{ a } bab^{-1} = a^{-1}.$$

2.7.2. Poznámka. Zabývejme se podrobněji grupou $\mathbf{Q}$. Položme

$$H = \{1, a, a^2, a^3, b, ab, a^2b, a^3b\}.$$

Jelikož $bab^{-1} = a^{-1}$, máme $ba = a^{-1}b$.
Počítejme:
$1^{-1} = 1$
$a^{-1} = a^3$
$(a^2)^{-1} = a^2$
$(a^3)^{-1} = a$
$b^{-1} = a^2b$ ($b \cdot a^2b = bb^2b = b^4 = (b^2)^2 = (a^2)^2 = a^4 = 1,\ a^2b \cdot b = a^2b^2 = a^2a^2 = a^4 = 1$)
$(ab)^{-1} = a^3b$ ($ab \cdot a^3b = abaa^2b = aa^{-1}ba^2b = bb^2b = b^4 = 1,\ a^3b \cdot ab = a^3a^{-1}bb = a^2b^2 = a^2a^2 = a^4 = 1$)
$(a^2b)^{-1} = b$
$(a^3b)^{-1} = ab$
Ukázali jsme toto: Jestliže $x \in H$, pak $x^{-1} \in H$.
Ze vztahu $ba = a^{-1}b$ vyplývá, že

$$ba^m = a^{-m}b$$

pro každé nezáporné celé číslo m.
Nechť $i, k \in \{0, 1, 2, 3\}$, $j, l \in \{0, 1\}$. Vypočítáme součin

$$(a^i b^j) \cdot (a^k b^l).$$

Jestliže $j = 0$, pak $(a^i b^j) \cdot (a^k b^l) = a^i b^0 a^k b^l = a^{i+k} b^l$.
Jestliže $j = 1$, pak $(a^i b^j) \cdot (a^k b^l) = a^i b a^k b^l = a^i a^{-k} b b^l = a^{i-k} b^{l+1}$. V případě $l = 0$ máme $(a^i b^j) \cdot (a^k b^l) = a^{i-k} b^1$. V případě $l = 1$ máme $(a^i b^j) \cdot (a^k b^l) = a^{i-k} b^2 = a^{i-k} a^2 = a^{i-k+2} b^0$.
Dokázali jsme: existují $u \in \mathbb{Z}$, $v \in \{0, 1\}$ tak, že

$$(a^i b^j) \cdot (a^k b^l) = a^u b^v.$$

Protože $a^4 = 1$, existuje $w \in \{0, 1, 2, 3\}$, $a^u = a^w$. Celkem existují $w \in \{0, 1, 2, 3\}$, $v \in \{0, 1\}$ s vlastností

$$(a^i b^j) \cdot (a^k b^l) = a^w b^v.$$

Právě jsme ukázali toto: Jestliže $x, y \in H$, pak $xy \in H$.
Z dosud provedených výpočtů vyplývá, že H je podgrupa grupy $\mathbf{Q}$. Jelikož $a, b \in H$, je $\langle a, b \rangle \subseteq H$. Ovšem $\langle a, b \rangle = \mathbf{Q}$, takže $\mathbf{Q} = H$.
Můžeme učinit následující závěry:

1. Grupa $\mathbf{Q}$ má přesně 8 prvků, a to konkrétně

$$1, a, a^2, a^3, b, ab, a^2 b, a^3 b.$$

2. Výpočty v grupě $\mathbf{Q}$ lze provádět pomocí vztahů $a^4 = 1$, $b^2 = a^2$, $bab^{-1} = a^{-1}$.

3. Z předchozích dvou bodů vyplývá, že definice 2.7.1. určuje grupu kvaternionů jednoznačně.

4. Grupa $\mathbf{Q}$ není komutativní. Předpokládejme opak. Potom $a^2 b = aab = aba = aa^{-1} b = b$. Dostali jsme spor s bodem 1.

2.7.3. Příklad. Uvažme následující čtvercové matice stupně 2 nad tělesem komplexních čísel:

$$1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \; i = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}, \; j = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \; k = \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix}.$$

Položme

$$G = \{1, i, j, k, -1, -i, -j, -k\}.$$

Množina G má 8 prvků. Je $|1| = |i| = |j| = |k| = |-1| = |-i| = |-j| = |-k| = 1$, takže $G \subseteq GL(2, \mathbb{C})$.
Počítejme:

$$i^2 = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = -1$$

$$j^2 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = -1$$

$$k^2 = \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix} \cdot \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = -1$$

$$ij = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix} = k$$

$$jk = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \cdot \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} = i$$

$$ki = \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix} \cdot \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = j$$

$$ji = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} = -k$$

$$kj = \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix} = -i$$

$$ik = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \cdot \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = -j.$$

Buďte $a, b \in \{1, i, j, k\}$. Pak platí:
$ab \in G$
$(-a)b = -(ab) \in G$
$a(-b) = -(ab) \in G$
$(-a)(-b) = ab \in G$.
Ukázali jsme: Jestliže $x, y \in G$, pak $xy \in G$.
Dále platí:
$1 \cdot 1 = 1$, takže $1^{-1} = 1$
$(-1) \cdot (-1) = 1 \cdot 1 = 1$, takže $(-1)^{-1} = -1$
$a \cdot (-a) = (-a) \cdot a = -a^2 = 1$, takže $a^{-1} = -a$, $(-a)^{-1} = a$ (pro každé $a \in \{i, j, k\}$).
Ukázali jsme: Jestliže $x \in G$, pak $x^{-1} \in G$.
Podařilo se nám dokázat, že G je podgrupa grupy $GL(2, \mathbb{C})$.
Dokážeme nyní, že $G = \langle i, j \rangle$.

$\langle i, j\rangle \subseteq G$: To je jasné.
$G \subseteq \langle i, j\rangle$: $k = ij$, $-1 = i^2$, $-i = i^3$, $-j = j^3$, $-k = ji$.
Všimněme si ještě, že $i^4 = (i^2)^2 = (-1)^2 = 1$, $i^2 = j^2$, $jij^{-1} = ji(-j) = (-k)(-j) = kj = -i = i^{-1}$.
Lze tedy říci, že grupa G sestrojená v tomto příkladě je grupa kvaternionů, tj. $G = \mathbf{Q}$.

3 Lagrangeova věta a její důsledky

3.1 Lagrangeova věta

Nechť G je grupa, $a \in G$, $B \subseteq G$. Místo $\{a\} \cdot B = \{a\}B$ budeme stručně psát $a \cdot B = aB$. Je tedy

$$a \cdot B = aB = \{a \cdot y |\ y \in B\}.$$

Připomeňme si pojem **rozklad množiny**. Nechť M je množina. Rozkladem množiny M rozumíme jakýkoli systém $\mathcal{S}$ podmnožin množiny M s těmito vlastnostmi:

1. Pro všechna $A \in \mathcal{S}$ platí: $A \neq \emptyset$.
2. $\bigcup_{A \in \mathcal{S}} A = M$
3. Pro všechna $A, B \in \mathcal{S}$ platí: Jestliže $A \cap B \neq \emptyset$, pak $A = B$. (Ekvivalentně: Jestliže $A \neq B$, pak $A \cap B = \emptyset$.)

3.1.1. Příklad. Položme
$A = \{3k |\ k \in \mathbb{Z}\} = \{\dots, -6, -3, 0, 3, 6, \dots\}$
$B = \{3k + 1 |\ k \in \mathbb{Z}\} = \{\dots, -5, -2, 1, 4, 7, \dots\}$
$C = \{3k + 2 |\ k \in \mathbb{Z}\} = \{\dots, -4, -1, 2, 5, 8, \dots\}$.
Pak $\{A, B, C\}$ je rozklad množiny $\mathbb{Z}$.

3.1.2. Věta. *Nechť G je grupa, H je podgrupa grupy G. Pak systém množin*

$$\{aH |\ a \in G\}$$

je rozklad množiny G.

Důkaz. Je třeba dokázat následující:
(I) Pro všechna $a \in G$ platí: $aH \neq \emptyset$.
(II) $\bigcup_{a\in G} aH = G$
(III) Pro všechna $a, b \in G$ platí: Jestliže $aH \cap bH \neq \emptyset$, pak $aH = bH$.
ad (I): Jelikož H je podgrupa, je $1 \in H$, a tedy $a = a \cdot 1 \in aH$, $aH \neq \emptyset$.
ad (II):
$\bigcup_{a\in G} aH \subseteq G$: To je jasné.
$G \subseteq \bigcup_{a\in G} aH$: Buď $g \in G$. Pak $g \in gH \subseteq \bigcup_{a\in G} aH$.
ad (III): Nechť $a, b \in G$, $aH \cap bH \neq \emptyset$. Chceme: $aH = bH$. Buď $c \in aH \cap bH$. Existují tedy $h_1, h_2 \in H$, $c = ah_1$, $c = bh_2$. Pak $ah_1 = bh_2$, $a = bh_2h_1^{-1}$. Zvolme libovolně $g \in aH$. Existuje $h \in H$, $g = ah$. Pak $g = bh_2h_1^{-1}h$. Protože $h_2, h_1, h \in H$ a H je podgrupa, je $h_2h_1^{-1}h \in H$ a $g = bh_2h_1^{-1}h \in bH$. Prvek $g \in aH$ jsme volili libovolně. Ukázali jsme tedy, že $aH \subseteq bH$. Obdobně lze ukázat, že $bH \subseteq aH$. Celkem tedy $aH = bH$.

Rozklad $\{aH|\ a \in G\}$ z věty 3.1.2. budeme stručně označovat G/H. Množina aH se nazývá **levá třída** grupy G podle podgrupy H (určená prvkem a). Rozklad G/H je tedy rozklad grupy G na levé třídy podle podgrupy H.

3.1.3. Definice. Nechť G je grupa, H je podgrupa grupy G. Číslo $card(G/H)$ nazýváme **index** podgrupy H v G a značíme ho $[G : H]$.

3.1.4. Příklad. Nechť G je grupa. Pak

$$\begin{aligned}
[G : \{1\}] &= card(G/\{1\}) \\
&= card(\{a \cdot \{1\}|\ a \in G\}) \\
&= card(\{\{a \cdot 1\}|\ a \in G\}) \\
&= card(\{\{a\}|\ a \in G\}) \\
&= card(G).
\end{aligned}$$

3.1.5. Příklad. Nechť G je grupa. Pak

$$\begin{aligned}
[G : G] &= card(G/G) \\
&= card(\{aG|\ a \in G\}) \\
&= card(\{G|\ a \in G\}) \\
&= card(\{G\}) \\
&= 1.
\end{aligned}$$

Využili jsme fakt, že $aG = G$ pro každé $a \in G$. Vztah $aG \subseteq G$ je jasný. Buď $g \in G$. Pak $g = a(a^{-1}g) \in aG$. Tudíž $G \subseteq aG$.

3.1.6. Příklad. Uvažme grupu $\mathbb{Z}$ a její podmnožiny A, B, C z příkladu 3.1.1. Zřejmě A je podgrupa grupy $\mathbb{Z}$ (je $A = \langle 3 \rangle$). Určíme rozklad $\mathbb{Z}/A$.
$0 + A = A$
$1 + A = 1 + \{3k |\ k \in \mathbb{Z}\} = \{1 + 3k |\ k \in \mathbb{Z}\} = B$
$2 + A = 2 + \{3k |\ k \in \mathbb{Z}\} = \{2 + 3k |\ k \in \mathbb{Z}\} = C$
$3 + A = 3 + \{\dots, -6, -3, 0, 3, 6, \dots\} = \{\dots, -3, 0, 3, 6, 9, \dots\} = A$
$4 + A = 4 + \{\dots, -6, -3, 0, 3, 6, \dots\} = \{\dots, -2, 1, 4, 7, 10, \dots\} = B$
$5 + A = 5 + \{\dots, -6, -3, 0, 3, 6, \dots\} = \{\dots, -1, 2, 5, 8, 11, \dots\} = C$
$6 + A = 6 + \{\dots, -6, -3, 0, 3, 6, \dots\} = \{\dots, 0, 3, 6, 9, 12, \dots\} = A$
atd.
Obecně, nechť $x \in \mathbb{Z}$. Nastane právě jeden ze tří případů:
(I) $x = 3l$ pro nějaké $l \in \mathbb{Z}$
(II) $x = 3l + 1$ pro nějaké $l \in \mathbb{Z}$
(III) $x = 3l + 2$ pro nějaké $l \in \mathbb{Z}$.
ad (I): $x + A = A$
ad (II): $x + A = B$
ad (III): $x + A = C$
Tudíž $\mathbb{Z}/A = \{x + A |\ x \in \mathbb{Z}\} = \{A, B, C\}$ a $[\mathbb{Z} : A] = 3$.

3.1.7. Příklad. Uvažme grupu kvaternionů $\mathbf{Q} = \{1, i, j, k, -1, -i, -j, -k\}$ (viz 2.7.3.) a její podgrupu $H = \langle i \rangle = \{1, i, -1, -i\}$. Určíme rozklad $\mathbf{Q}/H$.
$1 \cdot H = H$
$i \cdot H = \{i, -1, -i, 1\} = H$
$j \cdot H = \{j, -k, -j, k\}$
$k \cdot H = \{k, j, -k, -j\}$
$-1 \cdot H = \{-1, -i, 1, i\} = H$
$-i \cdot H = \{-i, 1, i, -1\} = H$
$-j \cdot H = \{-j, k, j, -k\}$
$-k \cdot H = \{-k, -j, k, j\}$
Vidíme, že $\mathbf{Q}/H = \{\{1, i, -1, -i\}, \{j, -k, -j, k\}\}$ a tedy $[\mathbf{Q} : H] = 2$.

3.1.8. Tvrzení. *Nechť G je grupa, H je podgrupa grupy G, $a \in G$. Pak*

$$card(H) = card(aH).$$

Důkaz. Definujme zobrazení $f : H \to aH$ takto:

$$f(x) = ax$$

pro každé $x \in H$. Je zřejmé, že f je surjekce. Ukážeme, že f je injekce. Nechť $x, y \in H$, $f(x) = f(y)$. Chceme: $x = y$. Víme, že $ax = ay$. Stačí použít zákon o krácení.

3.1.9. Věta. (Lagrange) *Nechť G je konečná grupa. Nechť H je podgrupa grupy G. Pak řád podgrupy H dělí řád grupy G (tj. $card(H)/card(G)$) a $card(G) = [G : H] \cdot card(H)$.*

Důkaz. Použijeme rozklad množiny G z věty 3.1.2. Všimněme si, že z konečnosti množiny G vyplývá konečnost množiny H (je $H \subseteq G$) a také konečnost množiny G/H (každá levá třída grupy G podle podgrupy H je neprázdná; kdyby levých tříd bylo nekonečně mnoho, musela by být množina G nekonečná). Ze 3.1.8. plyne, že každá levá třída grupy G podle podgrupy H má stejný počet prvků, totiž $card(H)$. Jelikož počet levých tříd je roven $card(G/H)$, dostáváme

$$card(G/H) \cdot card(H) = card(G)$$

$$[G : H] \cdot card(H) = card(G).$$

Jasným důsledkem právě dokázaného vztahu je fakt $card(H)/card(G)$.

3.1.10. Tvrzení. *Nechť G je konečná grupa. Nechť $a \in G$. Pak prvek a má konečný řád a tento řád dělí řád grupy G.*

Důkaz. Prvek a má konečný řád podle 1.2.7. Řád prvku a označme n. Podle 1.4.18. podgrupa $\langle a \rangle$ má řád n. Podle Lagrangeovy věty řád podgrupy $\langle a \rangle$ dělí řád grupy G. Takže n dělí řád grupy G, řád prvku a dělí řád grupy G.

3.1.11. Tvrzení. *Nechť G je konečná grupa řádu n. Nechť $a \in G$. Pak $a^n = 1$.*

Důkaz. Dle 3.1.10. prvek a má konečný řád k a přitom k/n. Existuje tedy přirozené číslo l tak, že $n = k \cdot l$. Pak $a^n = (a^k)^l = 1^l = 1$.

Lagrangeova věta je základní věta teorie grup. Jako první se nabízí její aplikace při hledání všech podgrup konečné grupy.

3.1.12. Příklad. Úkol: Určete všechny podgrupy grupy $\mathbb{Z}_{8161}$.
Řešení: Buď H podgrupa grupy $\mathbb{Z}_{8161}$. Podle Lagrangeovy věty řád podgrupy H dělí řád grupy $\mathbb{Z}_{8161}$, tedy $card(H)/8161$. Protože 8161 je prvočíslo, máme $card(H) = 1$ nebo $card(H) = 8161$. Tudíž grupa $\mathbb{Z}_{8161}$ má dvě podgrupy, a to $\{\overline{0}\}$ a $\mathbb{Z}_{8161}$.

3.1.13. Příklad. Úkol: Určete všechny podgrupy grupy S_3.
Řešení: Použijeme označení z příkladu 2.3.13. (v něm jsme se zabývali grupou S_3). Uvědomme si, že grupa S_3 má řád $3! = 6$. Podle Lagrangeovy věty pak každá podgrupa grupy S_3 má řád 1, 2, 3 nebo 6.
Při určování podgrup (konečné) grupy G je vhodné zjistit řády všech prvků grupy G. To má dva důvody:

1. Jestliže H je podgrupa grupy G, $a \in H$, pak řád prvku a dělí $card(H)$ (viz 3.1.10.).

2. Jestliže prvek a má řád n, pak $\langle a \rangle$ má řád n a $\langle a \rangle = \{1, a, a^2, \ldots, a^{n-1}\}$ (viz 1.4.18.).

Počítejme:
$a^2 = i$
$b^2 = i$
$c^2 = i$
$d^2 = e$, $d^3 = de = i$
$e^2 = d$, $e^3 = ed = i$.
Zjistili jsme, že prvky a, b, c mají řád 2, prvky d, e mají řád 3.

1. Podgrupy řádu 1: Zřejmě existuje jediná podgrupa řádu 1, a to $\{i\}$.

2. Podgrupy řádu 2: Každá podgrupa řádu 2 má tvar $\{1, x\}$, kde x je prvek řádu 2. Grupa S_3 tedy má tři podgrupy řádu 2: $\{i, a\}$, $\{i, b\}$, $\{i, c\}$.

3. Podgrupy řádu 3: Každá podgrupa řádu 3 má tvar $\{1, x, y\}$, kde x, y jsou prvky řádu 3, $x^2 = y$, $y^2 = x$, $xy = yx = 1$. Grupa S_3 má tedy jednu podgrupu řádu 3, totiž $\{i, d, e\}$. Uvědomme si, že $\{i, d, e\} = A_3$.

4. Podgrupy řádu 6: Zřejmě existuje jediná podgrupa řádu 6, a to S_3.

Shrnutí:
Grupa S_3 má celkem 6 podgrup:
$\{i\}$, $\{i, a\}$, $\{i, b\}$, $\{i, c\}$, A_3, S_3.

3.1.14. Příklad. Najdeme všechny grupy řádu 4. Nechť G je grupa řádu 4. Podle 3.1.10. řády prvků grupy G mohou být pouze čísla 1, 2, 4. Předpokládejme nejdříve, že grupa G obsahuje prvek a řádu 4. Sestrojíme multiplikativní tabulku grupy G:

	a^0	a^1	a^2	a^3
a^0	a^0	a^1	a^2	a^3
a^1	a^1	a^2	a^3	a^0
a^2	a^2	a^3	a^0	a^1
a^3	a^3	a^0	a^1	a^2

Základním vztahem pro sestrojení tabulky je vztah $a^4 = 1$. Potom například $a^3 \cdot a^2 = a^5 = a^4 \cdot a^1 = 1 \cdot a^1 = a^1$.
Vidíme, že $G \cong \mathbb{Z}_4$.
Předpokládejme nyní, že grupa G neobsahuje žádný prvek řádu 4. Pak $G = \{1, a, b, c\}$ a každý z prvků a, b, c má řád 2.
Sestrojíme multiplikativní tabulku grupy G:

	1	a	b	c
1	1	a	b	c
a	a	1	c	b
b	b	c	1	a
c	c	b	a	1

Tabulku jsme sestrojili za využití vztahů $a^2 = b^2 = c^2 = 1$ a faktu, že v žádném řádku (sloupci) tabulky se neopakují prvky.
Sestrojíme multiplikativní tabulku grupy $\mathbb{Z}_2 \times \mathbb{Z}_2$:

	$(\overline{0}, \overline{0})$	$(\overline{0}, \overline{1})$	$(\overline{1}, \overline{0})$	$(\overline{1}, \overline{1})$
$(\overline{0}, \overline{0})$	$(\overline{0}, \overline{0})$	$(\overline{0}, \overline{1})$	$(\overline{1}, \overline{0})$	$(\overline{1}, \overline{1})$
$(\overline{0}, \overline{1})$	$(\overline{0}, \overline{1})$	$(\overline{0}, \overline{0})$	$(\overline{1}, \overline{1})$	$(\overline{1}, \overline{0})$
$(\overline{1}, \overline{0})$	$(\overline{1}, \overline{0})$	$(\overline{1}, \overline{1})$	$(\overline{0}, \overline{0})$	$(\overline{0}, \overline{1})$
$(\overline{1}, \overline{1})$	$(\overline{1}, \overline{1})$	$(\overline{1}, \overline{0})$	$(\overline{0}, \overline{1})$	$(\overline{0}, \overline{0})$

Lze snadno vidět, že zobrazení $f : G \to \mathbb{Z}_2 \times \mathbb{Z}_2$ dané předpisem

$$f(1) = (\overline{0}, \overline{0}),\ f(a) = (\overline{0}, \overline{1}),\ f(b) = (\overline{1}, \overline{0}),\ f(c) = (\overline{1}, \overline{1})$$

je izomorfismus. Takže $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.
Závěrem lze říci, že existují dvě grupy řádu 4, totiž $\mathbb{Z}_4$ a $\mathbb{Z}_2 \times \mathbb{Z}_2$.

3.2 Věty Fermatova a Eulerova

V této části dokážeme pomocí Lagrangeovy věty dva klasické výsledky teorie čísel, Fermatovu a Eulerovu větu.

3.2.1. Věta (Fermat). *Jestliže p je prvočíslo a a je celé číslo, pak $a^p \equiv a\ (p)$.*

Důkaz. Uvažme grupu $\mathbb{Z}_p^\times$. Ta má řád $p-1$. Předpokládejme, že $\overline{a} \neq \overline{0}$. Pak $\overline{a} \in \mathbb{Z}_p^\times$. Dle 3.1.11. platí: $(\overline{a})^{p-1} = \overline{1}$, $(\overline{a})^{p-1} \cdot \overline{a} = \overline{1} \cdot \overline{a}$, $(\overline{a})^p = \overline{a}$, $\overline{a^p} = \overline{a}$, $a^p \equiv a\ (p)$. Zbývá ještě případ $\overline{a} = \overline{0}$. Pak ovšem $\overline{a^p} = (\overline{a})^p = (\overline{0})^p = \overline{0^p} = \overline{0} = \overline{a}$, tj. $a^p \equiv a\ (p)$.

Například, $3^5 = 243 \equiv 3\ (5)$,
$10^{13} = 9999999999990 + 10 = 13 \cdot 769230769230 + 10 \equiv 10\ (13)$.
V následující větě se vyskytuje Eulerova funkce φ (viz 2.2.3.).

3.2.2. Věta (Euler). *Nechť r, s jsou celá čísla, $r > 0$. Jestliže $NSD(r,s) = 1$, pak $s^{\varphi(r)} \equiv 1\ (r)$.*

Důkaz. Uvažme grupu $U(\mathbb{Z}_r)$. Ta má řád $\varphi(r)$ (viz 2.2.6.). Jelikož máme $NSD(r,s) = 1$, je $\overline{s} \in U(\mathbb{Z}_r)$ (viz 2.2.5.). Dle 3.1.11. platí: $(\overline{s})^{\varphi(r)} = \overline{1}$, $\overline{s^{\varphi(r)}} = \overline{1}$, $s^{\varphi(r)} \equiv 1\ (r)$.

3.2.3. Příklad. Určete poslední dvojčíslí čísla 3^{12345}.
Řešení: Je třeba určit zbytek po dělení čísla 3^{12345} číslem 100. $NSD(100,3) = 1$, takže dle Eulerovy věty $3^{\varphi(100)} \equiv 1\ (100)$. Protože $\varphi(100) = 40$, máme $3^{40} \equiv 1\ (100)$. Ovšem $12345 = 308 \cdot 40 + 25$, takže

$$3^{12345} = (3^{40})^{308} \cdot 3^{25} \equiv 1^{308} \cdot 3^{25} = 3^{25}\ (100).$$

Dále, $3^2 = 9$, $3^4 = 81$, $3^8 = 81^2 = 6561 \equiv 61$, $3^{16} \equiv 61^2 = 3721 \equiv 21$, $3^{24} = 3^{16} \cdot 3^8 \equiv 21 \cdot 61 = 1281 \equiv 81$, $3^{25} = 3^{24} \cdot 3 \equiv 81 \cdot 3 = 243 \equiv 43$.
Zjistili jsme, že $3^{12345} \equiv 43\ (100)$. Tudíž, zbytek čísla 3^{12345} po dělení číslem 100 je 43 a poslední dvojčíslí čísla 3^{12345} je 43.

4 Cyklické grupy

4.1 Popis všech cyklických grup

Z jistého úhlu pohledu lze říci, že cyklické grupy jsou nejjednodušší mezi všemi grupami. Jsou to totiž grupy generované jedním prvkem.

4.1.1. Definice. Nechť G je grupa. Jestliže existuje $a \in G$ tak, že $G = \langle a \rangle$, pak se grupa G nazývá **cyklická**. Prvek a nazýváme **generátor** cyklické grupy G.

Uvědomme si, že pro cyklickou grupu $G = \langle a \rangle$ máme vyjádření $G = \{a^n |\ n \in \mathbb{Z}\}$ (viz 1.4.14.).

4.1.2. Příklad. Nechť n je kladné celé číslo. Nechť G je množina všech n-tých komplexních odmocnin z jedné, tedy

$$G = \{x \in \mathbb{C} |\ x^n = 1\}.$$

Snadno se přesvědčíme, že G je podgrupa grupy $\mathbb{C}^\times$.
Je $1 \in G$, neboť $1^n = 1$.
Nechť $x \in G$. Chceme: $x^{-1} \in G$. Je $(x^{-1})^n = (x^n)^{-1} = 1^{-1} = 1$, takže $x^{-1} \in G$.
Nechť $x, y \in G$. Chceme: $x \cdot y \in G$. Je $(x \cdot y)^n = x^n \cdot y^n = 1 \cdot 1 = 1$, takže $x \cdot y \in G$.
Je dobře známo, že počet n-tých komplexních odmocnin z jedné je roven n a že to jsou následující čísla:
$\varepsilon_0 = \cos 0 \cdot \frac{2\pi}{n} + i \sin 0 \cdot \frac{2\pi}{n} = \cos 0 + i \sin 0 = 1$
$\varepsilon_1 = \cos 1 \cdot \frac{2\pi}{n} + i \sin 1 \cdot \frac{2\pi}{n} = \cos \frac{2\pi}{n} + i \sin \frac{2\pi}{n}$
$\varepsilon_2 = \cos 2 \cdot \frac{2\pi}{n} + i \sin 2 \cdot \frac{2\pi}{n}$
$\varepsilon_3 = \cos 3 \cdot \frac{2\pi}{n} + i \sin 3 \cdot \frac{2\pi}{n}$
$\vdots$
$\varepsilon_{n-1} = \cos(n-1) \cdot \frac{2\pi}{n} + i \sin(n-1) \cdot \frac{2\pi}{n}$.
Tudíž $G = \{\varepsilon_0, \varepsilon_1, \ldots \varepsilon_{n-1}\}$.
Dobře je také známa Moivrova věta: Pro každé celé číslo k platí

$$(\cos \alpha + i \sin \alpha)^k = \cos k\alpha + i \sin k\alpha.$$

Specielně, pro každé celé číslo k, $0 \leq k \leq n-1$, máme

$$\varepsilon_1^k = (\cos \frac{2\pi}{n} + i \sin \frac{2\pi}{n})^k = \cos k \cdot \frac{2\pi}{n} + i \sin k \cdot \frac{2\pi}{n} = \varepsilon_k.$$

Závěrem lze konstatovat, že $G = \langle \varepsilon_1 \rangle$ a grupa G je cyklická.

4.1.3. Příklad. V grupě $\mathbb{Z}$ platí: $\langle 1 \rangle = \{n \cdot 1 |\ n \in \mathbb{Z}\} = \{n |\ n \in \mathbb{Z}\} = \mathbb{Z}$. Tedy $\mathbb{Z}$ je nekonečná cyklická grupa.
Nechť n je kladné celé číslo. V grupě $\mathbb{Z}_n$ platí: $\overline{1} + \overline{1} = \overline{2}$, $\overline{1} + \overline{1} + \overline{1} = \overline{3}$, $\overline{1} + \overline{1} + \overline{1} + \overline{1} = \overline{4}$, $\ldots$, $\underbrace{\overline{1} + \overline{1} + \cdots + \overline{1}}_{n-1} = \overline{n-1}$, $\underbrace{\overline{1} + \overline{1} + \cdots + \overline{1}}_{n} = \overline{n} = \overline{0}$. Tedy $\langle \overline{1} \rangle = \mathbb{Z}_n$ a $\mathbb{Z}_n$ je konečná cyklická grupa řádu n.

V následující větě dokážeme, že příklad 4.1.3. uvádí všechny cyklické grupy, které existují (až na izomorfismus).

4.1.4. Věta.
Jestliže G je nekonečná cyklická grupa, pak $G \cong \mathbb{Z}$.
Jestliže G je konečná cyklická grupa řádu n, pak $G \cong \mathbb{Z}_n$.

Důkaz.

1. Předpokládejme, že G je nekonečná cyklická grupa.
   Nechť $a \in G$, $G = \langle a \rangle$. Pro celé číslo n položíme

   $$f(n) = a^n.$$

   Definovali jsme právě zobrazení $f : \mathbb{Z} \to G$. Dokážeme, že f je izomorfismus.
   f je bijekce:
   Protože $G = \{a^n |\ n \in \mathbb{Z}\}$, je jasné, že f je surjekce. Zbývá dokázat, že f je injekce. Nechť k, l jsou celá čísla, $f(k) = f(l)$. Chceme: $k = l$. Víme, že $a^k = a^l$. Pro důkaz sporem předpokládejme, že $k \neq l$. Nechť například $k < l$. Pak $a^k \cdot a^{-k} = a^l \cdot a^{-k}$, $a^0 = a^{l-k}$, $1 = a^{l-k}$. Ovšem $l - k$ je přirozené číslo. Tudíž prvek a má konečný řád a grupa $G = \langle a \rangle$ je konečná (viz 1.4.18.). Dostali jsme spor. Nutně tedy $k = l$.
   f je homomorfismus:
   Buďte $k, l \in \mathbb{Z}$. Pak

   $$f(k + l) = a^{k+l} = a^k \cdot a^l = f(k) \cdot f(l).$$

2. Předpokládejme, že G je konečná cyklická grupa řádu n.
   Nechť $a \in G$, $G = \langle a \rangle$. Prvek a má konečný řád (viz 1.2.7.), který je

roven řádu grupy $\langle a\rangle$ (viz 1.4.18.). Tudíž, prvek a má řád n.
Nechť $k, l \in \mathbb{Z}$, $k \equiv l\ (n)$. Pak $n/l-k$ a existuje celé číslo q, $l-k = q\cdot n$. Potom $l = qn + k$, což dává

$$a^1 = a^{qn+k} = a^{qn} \cdot a^k = (a^n)^q \cdot a^k = 1^q \cdot a^k = 1 \cdot a^k = a^k.$$

Budeme definovat zobrazení $f : \mathbb{Z}_n \to G$ takto:

$$f(\overline{k}) = a^k$$

pro libovolné $k \in \mathbb{Z}$. Nejdříve prověříme, že zobrazení f je definováno korektně: Nechť $k, l \in \mathbb{Z}$, $\overline{k} = \overline{l}$. Je třeba, aby $a^k = a^l$. Avšak $\overline{k} = \overline{l}$ znamená $k \equiv l\ (n)$ a výše provedený výpočet ukazuje, že $a^k = a^l$.
Nyní dokážeme, že zobrazení f je izomorfismus.
f je bijekce:
Protože $G = \{a^n |\ n \in \mathbb{Z}\}$, je jasné, že f je surjekce. Zbývá dokázat, že f je injekce. Nechť k, l jsou celá čísla, $f(\overline{k}) = f(\overline{l})$. Chceme: $\overline{k} = \overline{l}$. Víme, že $a^k = a^l$. Pak $a^k \cdot a^{-k} = a^l \cdot a^{-k}$, $a^0 = a^{l-k}$, $1 = a^{l-k}$. Číslo $l - k$ vydělíme se zbytkem číslem n. Pak $l - k = q \cdot n + r$ pro vhodná celá čísla q, r, $0 \leq r < n$. Nyní

$$1 = a^{l-k} = a^{qn+r} = (a^n)^q \cdot a^r = 1^q \cdot a^r = 1 \cdot a^r = a^r.$$

Protože $0 \leq r < n$ a n je řád prvku a, musí být $r = 0$. Pak ovšem $l - k = q \cdot n$, $n/l - k$, $k \equiv l\ (n)$, $\overline{k} = \overline{l}$.
f je homomorfismus:
Buďte $k, l \in \mathbb{Z}$. Pak

$$f(\overline{k} + \overline{l}) = f(\overline{k+l}) = a^{k+l} = a^k \cdot a^l = f(\overline{k}) \cdot f(\overline{l}).$$

4.1.5. Tvrzení. *Nechť G je konečná grupa řádu n. Jestliže G má nějaký prvek řádu n, pak $G \cong \mathbb{Z}_n$.*

Důkaz. Nechť $a \in G$, a má řád n. Podle 1.4.18. podgrupa $\langle a\rangle$ má řád n. Takže $\langle a\rangle \subseteq G$, $card(\langle a\rangle) = n$, $card(G) = n$. Proto $\langle a\rangle = G$. Ukázali jsme, že grupa G je cyklická. Protože G je konečná cyklická grupa řádu n, je $G \cong \mathbb{Z}_n$ dle věty 4.1.4.

4.1.6. Tvrzení. *Nechť G je konečná grupa řádu p, kde p je prvočíslo. Pak $G \cong \mathbb{Z}_p$.*

Důkaz. Nechť $a \in G$, $a \neq 1$. Řád prvku a označme symbolem k. Podle 3.1.10. víme, že k dělí p. Takže $k = 1$ nebo $k = p$. Případ $k = 1$ nenastává (platilo by totiž $a^k = 1$, $a = 1$), takže $k = p$. Grupa G má prvek řádu p. Podle 4.1.5. pak $G \cong \mathbb{Z}_p$.

4.1.7. Příklad. Najdeme všechny generátory grupy $\mathbb{Z}$. Nechť $a \in \mathbb{Z}$, $\langle a \rangle = \mathbb{Z}$. Připomeňme si, že

$$\langle a \rangle = \{n \cdot a |\ n \in \mathbb{Z}\}.$$

Protože $1 \in \langle a \rangle$, existuje celé číslo n tak, že $na = 1$. Tudíž $n = a = 1$ nebo $n = a = -1$. Ověříme ještě, že $a = 1$ a $a = -1$ jsou vskutku generátory grupy $\mathbb{Z}$. Platí:

$$\langle 1 \rangle = \{n \cdot 1 |\ n \in \mathbb{Z}\} = \{n |\ n \in \mathbb{Z}\} = \mathbb{Z}$$

$$\langle -1 \rangle = \{n \cdot (-1) |\ n \in \mathbb{Z}\} = \{-n |\ n \in \mathbb{Z}\} = \mathbb{Z}.$$

Závěrem můžeme konstatovat, že grupa $\mathbb{Z}$ má přesně dva generátory, totiž čísla 1, -1.

4.1.8. Příklad. Najdeme všechny generátory grupy $\mathbb{Z}_4$. Zřejmě platí:
$\langle \overline{0} \rangle = \{\overline{0}\}$, $\langle \overline{1} \rangle = \mathbb{Z}_4$, $\langle \overline{2} \rangle = \{\overline{0}, \overline{2}\}$, $\langle \overline{3} \rangle = \mathbb{Z}_4$
(v posledním případě si povšimneme vztahů $\overline{3}+\overline{3} = \overline{6} = \overline{2}$, $\overline{3}+\overline{3}+\overline{3} = \overline{9} = \overline{1}$, $\overline{3}+\overline{3}+\overline{3}+\overline{3} = \overline{12} = \overline{0}$).
Můžeme konstatovat, že grupa $\mathbb{Z}_4$ má přesně dva generátory, totiž $\overline{1}$ a $\overline{3}$.

4.1.9. Příklad. Najdeme všechny generátory grupy $\mathbb{Z}_5$. Počítejme:
$\overline{1}+\overline{1} = \overline{2}$, $\overline{1}+\overline{1}+\overline{1} = \overline{3}$, $\overline{1}+\overline{1}+\overline{1}+\overline{1} = \overline{4}$, $\overline{1}+\overline{1}+\overline{1}+\overline{1}+\overline{1} = \overline{5} = \overline{0}$
$\overline{2}+\overline{2} = \overline{4}$, $\overline{2}+\overline{2}+\overline{2} = \overline{6} = \overline{1}$, $\overline{2}+\overline{2}+\overline{2}+\overline{2} = \overline{8} = \overline{3}$, $\overline{2}+\overline{2}+\overline{2}+\overline{2}+\overline{2} = \overline{10} = \overline{0}$
$\overline{3}+\overline{3} = \overline{6} = \overline{1}$, $\overline{3}+\overline{3}+\overline{3} = \overline{9} = \overline{4}$, $\overline{3}+\overline{3}+\overline{3}+\overline{3} = \overline{12} = \overline{2}$, $\overline{3}+\overline{3}+\overline{3}+\overline{3}+\overline{3} = \overline{15} = \overline{0}$
$\overline{4}+\overline{4} = \overline{8} = \overline{3}$, $\overline{4}+\overline{4}+\overline{4} = \overline{12} = \overline{2}$, $\overline{4}+\overline{4}+\overline{4}+\overline{4} = \overline{16} = \overline{1}$, $\overline{4}+\overline{4}+\overline{4}+\overline{4}+\overline{4} = \overline{20} = \overline{0}$.
Můžeme konstatovat, že grupa $\mathbb{Z}_5$ má přesně 4 generátory, totiž $\overline{1}$, $\overline{2}$, $\overline{3}$, $\overline{4}$.

Příklad 4.1.7. nám ukázal, že nekonečná cyklická grupa má 2 generátory. V případě konečných cyklických grup je situace jiná. Konečná cyklická grupa může mít 2 generátory (viz 4.1.8.), může mít ale také 4 generátory (viz 4.1.9.). Jak je to tedy s počtem generátorů konečných cyklických grup?

4.1.10. Tvrzení. *Nechť $G = \langle a \rangle$ je konečná cyklická grupa řádu n. Pro každé celé číslo k platí:*

$$\langle a^k \rangle = G \iff NSD(k, n) = 1.$$

Důkaz. Z 1.2.7. a 1.4.18. plyne, že prvek a má řád n.

1. Předpokládejme, že $\langle a^k \rangle = G$. Protože $a \in G$, je $a \in \langle a^k \rangle = \{(a^k)^u |\ u \in \mathbb{Z}\}$. Existuje tedy celé číslo u s vlastností $a = (a^k)^u = a^{ku}$. Pak $a^{ku-1} = 1$ a tedy $n/ku - 1$ (viz 1.2.13.). Existuje tedy celé číslo v s vlastností $ku - 1 = nv$. Potom $1 = ku - nv$. Buď d celé číslo, d/n a d/k. Jelikož $1 = ku - nv$, dostáváme $d/1$, čili $d = 1$ nebo $d = -1$. Z toho již vyplývá, že $NSD(k, n) = 1$.

2. Předpokládejme, že $NSD(k, n) = 1$. Dle Bezoutovy rovnosti (viz 2.2.4.) existují celá čísla u, v taková, že

$$1 = uk + vn.$$

Pak

$$a = a^1 = a^{uk+vn} = (a^k)^u \cdot (a^n)^v = (a^k)^u \cdot 1^v = (a^k)^u \cdot 1 = (a^k)^u$$

(použili jsme fakt, že prvek a má řád n).
Tudíž $a \in \langle a^k \rangle$. Pak ovšem $\langle a \rangle \subseteq \langle a^k \rangle$ a vzhledem ke skutečnosti, že $\langle a \rangle = G$, dostáváme $G = \langle a^k \rangle$.

4.1.11. Tvrzení. *Nechť G je konečná cyklická grupa řádu n. Pak počet generátorů grupy G je roven $\varphi(n)$, kde φ je Eulerova funkce.*

Důkaz. Protože grupa G je cyklická, existuje prvek $a \in G$ řádu n s vlastností

$$G = \{a^0, a^1, \ldots, a^{n-1}\}.$$

Podle tvrzení 4.1.10. pro každé $k \in \{0, 1, \ldots, n-1\}$ platí:

$$\langle a^k \rangle = G \iff NSD(k, n) = 1.$$

Tudíž počet generátorů grupy G je roven číslu

$$card(\{k \in \mathbb{Z} |\ 0 \leq k < n,\ NSD(k, n) = 1\}),$$

což je ovšem hodnota $\varphi(n)$ (viz definici 2.2.3.).

Například, cyklická grupa $\mathbb{Z}_{100}$ má celkem $\varphi(100) = 40$ generátorů a cyklická grupa $\mathbb{Z}_p$, kde p je prvočíslo, má celkem $\varphi(p) = p - 1$ generátorů.

4.1.12. Tvrzení. *Nechť G je konečná cyklická grupa řádu n. Pak počet prvků grupy G, které mají řád n, je roven $\varphi(n)$, kde φ je Eulerova funkce.*

Důkaz. Vzhledem k 4.1.11. stačí ukázat, že pro každý prvek $a \in G$ platí: prvek a má řád n právě tehdy, když a je generátor grupy G.

1. Předpokládejme, že prvek a má řád n. Pak $\langle a \rangle$ má řád n (viz 1.4.18.). Jelikož $\langle a \rangle \subseteq G$ a grupy $\langle a \rangle$ a G mají stejný konečný řád, je $\langle a \rangle = G$, čili a je generátor grupy G.

2. Předpokládejme, že a je generátor grupy G. Nechť prvek a má řád k. Pak $\langle a \rangle$ má řád k. Jelikož a je generátor grupy G, je $\langle a \rangle = G$ a tedy $k = n$.

4.2 Podgrupy cyklických grup

Pokusme se nejdříve nalézt všechny podgrupy nekonečné cyklické grupy, tedy grupy $\mathbb{Z}$. Buď d nezáporné celé číslo. Samozřejmě,

$$\langle d \rangle = \{nd |\ n \in \mathbb{Z}\}$$

jsou (cyklické) podgrupy grupy $\mathbb{Z}$. Následující tvrzení ukazuje, že grupa $\mathbb{Z}$ už žádné další podgrupy nemá.

4.2.1. Tvrzení. *Buď H podgrupa grupy $\mathbb{Z}$. Pak existuje nezáporné celé číslo d tak, že $H = \langle d \rangle$.*

Důkaz. Jestliže $H = \{0\}$, pak položíme $d = 0$. Nechť $H \neq \{0\}$. Pak existuje $a \in H$, $a \neq 0$. Protože H je podgrupa, je $-a \in H$. Jelikož $a \neq 0$, je jedno z čísel a, $-a$ kladné a množina $H^+ = \{x \in H |\ x > 0\}$ není prázdná. Buď d nejmenší prvek množiny H^+. Ukážeme, že $\langle d \rangle = H$.
Protože $d \in H^+ \subseteq H$, je $\langle d \rangle \subseteq H$.
Nechť $c \in H$. Číslo c vydělíme se zbytkem číslem d. Existují celá čísla q, r taková, že $c = qd + r$, kde $0 \leq r < d$. Předpokládejme, že $r \neq 0$. Je $c \in H$, $d \in H$. Protože H je podgrupa, máme $(-q) \cdot d \in H$, $c + (-q) \cdot d \in H$. Ovšem $c + (-q) \cdot d = r$, takže $r \in H$. Protože $r > 0$, je $r \in H^+$. Avšak $r < d$, což je ve sporu s tím, že d je nejmenší prvek množiny H^+. Dokázali jsme tedy,

že $r = 0$. Pak $c = qd$, $c \in \langle d \rangle$. Prvek $c \in H$ jsme zvolili libovolně, takže $H \subseteq \langle d \rangle$.

Pokusme se nyní nalézt všechny podgrupy konečné cyklické grupy řádu n.

4.2.2. Tvrzení. *Nechť G je konečná cyklická grupa řádu n s generátorem a. Nechť d, e jsou kladná celá čísla splňující $de = n$. Pak podgrupa $\langle a^e \rangle$ má řád d a platí vztah*

$$\langle a^e \rangle = \{a^{ie} |\ i \in \mathbb{Z},\ 0 \leq i < d\} = \{1, a^e, a^{2e}, \ldots, a^{(d-1)\cdot e}\}.$$

Důkaz. Víme, že prvek a má řád n, $G = \{1, a, a^2, \ldots, a^{n-1}\}$,
$\langle a^e \rangle = \{(a^e)^j |\ j \in \mathbb{Z}\} = \{a^{je} |\ j \in \mathbb{Z}\}$.
$\{a^{ie} |\ i \in \mathbb{Z},\ 0 \leq i < d\} \subseteq \langle a^e \rangle$: To je zřejmé.
$\langle a^e \rangle \subseteq \{a^{ie} |\ i \in \mathbb{Z},\ 0 \leq i < d\}$: Zvolme $j \in \mathbb{Z}$. Je třeba ukázat, že existuje $i \in \mathbb{Z}$, $0 \leq i < d$, splňující $a^{je} = a^{ie}$. Vydělme číslo j se zbytkem číslem d. Existují celá čísla q, i, $0 \leq i < d$, $j = qd + i$. Pak $je = qde + ie = qn + ie$,

$$a^{je} = a^{qn+ie} = (a^n)^q \cdot a^{ie} = 1^q \cdot a^{ie} = 1 \cdot a^{ie} = a^{ie}.$$

Zbývá ještě dokázat, že $\langle a^e \rangle$ má řád d. K tomu stačí pouze dokázat, že pro $i \in \mathbb{Z}$, $0 \leq i < d$, je $0 \leq ie < n$. Z $0 \leq i < d$ dostáváme $0 \cdot e \leq i \cdot e < d \cdot e$, tedy $0 \leq ie < n$.

4.2.3. Tvrzení. *Nechť G je konečná cyklická grupa řádu n s generátorem a. Jestliže H je podgrupa grupy G, pak existují kladná celá čísla d, e splňující $de = n$, přičemž $H = \langle a^e \rangle$ a H má řád d.*

Důkaz. Prvek a má řád n a $G = \{1, a, a^2, \ldots, a^{n-1}\}$. Jestliže $H = \{1\}$, pak položíme $d = 1$ a $e = n$. Zřejmě H má řád d, $\langle a^e \rangle = \langle a^n \rangle = \langle 1 \rangle = \{1\} = H$. Nechť nyní $H \neq \{1\}$. Položme $M = \{f \in \mathbb{Z} |\ 0 < f,\ a^f \in H\}$. Množina M je neprázdná, protože $H \neq \{1\}$. Nejmenší prvek množiny M označme e. Zřejmě e je kladné celé číslo, $a^e \in H$. Číslo n vydělíme se zbytkem číslem e. Existují celá čísla d, r, $0 \leq r < e$, $n = de + r$. Pak $r = n + (-d)e$,

$$a^r = a^{n+(-d)e} = a^n \cdot a^{(-d)e} = 1 \cdot (a^e)^{-d} = (a^e)^{-d} \in H$$

(využli jsme fakt, že H je podgrupa a $a^e \in H$).
Kdyny bylo $r > 0$, bylo by $r \in M$, což by byl spor, protože $r < e$. Nutně tedy $r = 0$, $n = de$. Zřejmě d je kladné.
Dokážeme nyní, že $H = \langle a^e \rangle$.
$\langle a^e \rangle \subseteq H$: Tato inkluze plyne ihned z toho, že $a^e \in H$.
$H \subseteq \langle a^e \rangle$: Buď $h \in H$. Chceme: $h \in \langle a^e \rangle$. Prvek h lze zapsat ve tvaru $h = a^k$, kde $k \in \mathbb{Z}$. Vydělme číslo k se zbytkem číslem e. Existují celá čísla u, v, $0 \leq v < e$, $k = eu + v$. Pak $v = k + (-u)e$,

$$a^v = a^{k+(-u)e} = a^k \cdot (a^e)^{-u} = h \cdot (e^e)^{-u}.$$

Využijeme toho, že H je podgrupa. Protože $a^e \in H$, je $(a^e)^{-u} \in H$. Ovšem též $h \in H$, takže $a^v = h \cdot (a^e)^{-u} \in H$. Kdyby platilo $0 < v$, bylo by $v \in M$. To však není možné, protože $v < e$. Nutně tedy $v = 0$. Pak $k = eu$, $h = a^k = a^{eu} = (a^e)^u \in \langle a^e \rangle$. Z tvrzení 4.2.2. plyne, že $\langle a^e \rangle$ má řád d. Tudíž H má řád d.

Ve tvrzeních 4.2.2. a 4.2.3. se nám podařilo přesně popsat všechny podgrupy konečné cyklické grupy G řádu n.

4.2.4. Tvrzení. *Nechť G je konečná cyklická grupa řádu n s generátorem a. Nechť d je kladné celé číslo, d/n. Buď e kladné celé číslo, $n = de$. Pak grupa G má právě jednu podgrupu řádu d, totiž podgrupu*

$$\langle a^e \rangle = \{1, a^e, a^{2e}, \ldots, a^{(d-1)e}\}.$$

Důkaz. Ve 4.2.2. jsme dokázali, že $\langle a^e \rangle$ má řád d a platí vztah

$$\langle a^e \rangle = \{1, a^e, a^{2e}, \ldots, a^{(d-1)e}\}.$$

Buď H podgrupa grupy G, H má řád d. Chceme: $H = \langle a^e \rangle$. Ze 4.2.3. plyne: existují kladná celá čísla u, v splňující $uv = n$, přičemž $H = \langle a^v \rangle$ a H má řád u. Máme $de = uv$. Ovšem $u = d$, z čehož plyne $v = e$ a $H = \langle a^e \rangle$.

4.2.5. Tvrzení. *Každá podgrupa cyklické grupy je cyklická.*

Důkaz. Tvrzení vyplývá z 4.2.1. a 4.2.3.

Nyní pomocí poznatků o konečných cyklických grupách dokážeme větu týkající se Eulerovy funkce φ.

4.2.6. Věta. *Jestliže n je kladné celé číslo, pak*

$$\sum_{d/n} \varphi(d) = n,$$

kde součet se bere přes všechny kladné celočíselné dělitele čísla n.

Důkaz. Buď G konečná cyklická grupa řádu n s generátorem a. Pro kladné celé číslo d označíme symbolem $\psi(d)$ počet všech prvků grupy G, které mají řád d. Protože každý prvek grupy G má řád, jenž je kladným celočíselným dělitelem řádu grupy G (tj. čísla n), platí

$$\sum_{d/n} \psi(d) = n.$$

Stačí tedy ukázat, že pro každý kladný celočíselný dělitel d čísla n je $\psi(d) = \varphi(d)$.
Nechť d je kladné celé číslo, d/n. Buď $b \in G$, b má řád d. Pak $\langle b\rangle$ má řád d a dle 4.2.4. je $\langle b\rangle = \langle a^e\rangle$ (e je kladné celé číslo splňující $n = de$). Protože $b \in \langle b\rangle$, je $b \in \langle a^e\rangle$. Ukázali jsme, že každý prvek řádu d patří do $\langle a^e\rangle$. Je tedy $\psi(d)$ rovno počtu všech prvků grupy $\langle a^e\rangle$, které mají řád d. Jelikož $\langle a^e\rangle$ je konečná cyklická grupa řádu d, je počet prvků grupy $\langle a^e\rangle$ řádu d roven číslu $\varphi(d)$ (viz 4.1.12.). Tudíž $\psi(d) = \varphi(d)$.

Nechť T je těleso. Připomeňme, že symbol $T^\times$ značí multiplikativní grupu nenulových prvků tělesa T. Zabývejme se nyní otázkou, jak vypadají konečné podgrupy grupy $T^\times$. Specielně se tedy budeme zabývat otázkou, jak vypadá grupa $T^\times$ pro konečné těleso T.

4.2.7. Příklad. Uvažme těleso $\mathbb{Z}_7$. Určíme řády prvků grupy $\mathbb{Z}_7^\times$. Počítejme:
$\overline{2}^2 = \overline{4}$, $\overline{2}^3 = \overline{8} = \overline{1}$
$\overline{3}^2 = \overline{9} = \overline{2}$, $\overline{3}^3 = \overline{6}$, $\overline{3}^4 = \overline{18} = \overline{4}$, $\overline{3}^5 = \overline{12} = \overline{5}$, $\overline{3}^6 = \overline{15} = \overline{1}$
$\overline{4}^2 = \overline{16} = \overline{2}$, $\overline{4}^3 = \overline{8} = \overline{1}$
$\overline{5}^2 = \overline{25} = \overline{4}$, $\overline{5}^3 = \overline{20} = \overline{6}$, $\overline{5}^4 = \overline{30} = \overline{2}$, $\overline{5}^5 = \overline{10} = \overline{3}$, $\overline{5}^6 = \overline{15} = \overline{1}$
$\overline{6}^2 = \overline{36} = \overline{1}$.
Zjistili jsme, že $\overline{1}$ má řád 1, $\overline{2}$ má řád 3, $\overline{3}$ má řád 6, $\overline{4}$ má řád 3, $\overline{5}$ má řád 6,

$\overline{6}$ má řád 2.
Všimněme si, že $\langle\overline{3}\rangle = \mathbb{Z}_7^\times$, $\langle\overline{5}\rangle = \mathbb{Z}_7^\times$. Tedy: grupa $\mathbb{Z}_7^\times$ je cyklická. Vidíme též, že grupa $\mathbb{Z}_7^\times$ má dva generátory (jsou to prvky $\overline{3}$ a $\overline{5}$). To je samozřejmě v souladu s tvrzením 4.1.11., dle něhož cyklická grupa řádu 6 má $\varphi(6) = 2$ generátory.

Jak ukazuje následující věta, zjištění z příkladu 4.2.7. není náhodné. Jestliže T je konečné těleso, pak grupa $T^\times$ je cyklická.

4.2.8. Věta. *Nechť T je těleso. Platí:*

1. *Jestliže G je konečná podgrupa grupy $T^\times$, pak G je cyklická.*
2. *Jestliže T je konečné, pak grupa $T^\times$ je cyklická.*

Důkaz. Konstatujeme, že druhá část věty ihned plyne z části první: jestliže těleso T je konečné, pak jistě $T^\times$ je konečná grupa. Dokážeme tedy část první. Buď G konečná podgrupa grupy $T^\times$. Buď n řád grupy G. Buď d kladné celé číslo, d/n. Symbolem $\psi(d)$ označíme počet všech prvků grupy G, které mají řád d. Ukážeme: Jestliže $\psi(d) > 0$, pak $\psi(d) = \varphi(d)$.
Nechť $\psi(d) > 0$. Nechť $a \in G$, a má řád d. Položme $H = \langle a\rangle$. Pak H je cyklická grupa řádu d. Počet prvků grupy H, které mají řád d, je roven $\varphi(d)$ (viz 4.1.12.). K důkazu rovnosti $\psi(d) = \varphi(d)$ stačí ukázat, že v $G - H$ neleží žádný prvek řádu d. Předpokládejme opak. Buď $b \in G - H$, b má řád d. Uvažme polynom $p(x) = x^d - 1$. Polynom p má stupeň d, takže p má nejvýše d kořenů. Protože grupa H má řád d, je $h^d = 1$ pro všechna $h \in H$ (viz 3.1.11.). Pro všechna $h \in H$ tedy platí: $h^d - 1 = 0$, $p(h) = 0$, h je kořen polynomu p. Dále pak b má řád d, takže $b^d = 1$, $b^d - 1 = 0$, $p(b) = 0$, b je kořen polynomu p. Vidíme, že polynom p má aspoň $d+1$ kořenů. To je spor. Předpokládejme, že pro nějaké d je $\psi(d) = 0$. Pak

$$\sum_{d/n} \psi(d) < \sum_{d/n} \varphi(d).$$

Ovšem $\sum_{d/n} \psi(d) = n$ (to je zřejmé) a $\sum_{d/n} \varphi(d) = n$ (věta 4.2.6.), což dává $n < n$, spor. Nutně tedy pro každé d je $\psi(d) > 0$ a tudíž $\psi(d) = \varphi(d)$.
Specielně, $\psi(n) = \varphi(n) > 0$. Vidíme, že grupa G obsahuje prvky řádu n. Tudíž, dle 4.1.5., $G \cong \mathbb{Z}_n$, G je cyklická.

Pro nekonečné těleso T grupa $T^\times$ nemusí být cyklická. Například, grupa $\mathbb{R}^\times$ má nespočetně mnoho prvků. Pro každé $a \in \mathbb{R}^\times$ je $\langle a \rangle = \{a^n |\ n \in \mathbb{Z}\}$, takže grupa $\langle a \rangle$ je spočetná a situace $\langle a \rangle = \mathbb{R}^\times$ nemůže nastat, tj. grupa $\mathbb{R}^\times$ není cyklická.

4.2.9. Tvrzení. *Nechť T je nekonečné těleso, ve kterém $1+1 \neq 0$. Pak grupa $T^\times$ není cyklická.*

Důkaz. Budeme postupovat sporem. Předpokládejme, že grupa $T^\times$ je cyklická. Buď $a \in T^\times$, $\langle a \rangle = T^\times$. Pak

$$T^\times = \{a^n |\ n \in \mathbb{Z}\}.$$

Je $-a \in T^\times$ (jinak by bylo $-a = 0$, což by dalo $0 = a$) a tedy $-a = a^n$ pro nějaké celé číslo n. Z toho plyne $a^n \cdot a^n = (-a) \cdot (-a)$, $a^{2n} = a^2$, $a^{2n-2} = 1$. Jsou tři možnosti, avšak každá dává spor.
(I) $2n - 2 > 0$
(II) $2n - 2 = 0$
(III) $2n - 2 < 0$.
ad (I): Prvek a má konečný řád, grupa $\langle a \rangle = T^\times$ je konečná, spor.
ad (II): $n = 1$, $-a = a$, $0 = a + a$, $0 = a \cdot (1 + 1)$, $0 = 1 + 1$, spor.
ad (III): $a^{2n-2} = 1$, $(a^{2n-2})^{-1} = 1^{-1}$, $a^{-2n+2} = 1$. Číslo $-2n + 2$ je přirozené, takže prvek a má konečný řád, grupa $\langle a \rangle = T^\times$ je konečná, spor.

5 Akce grupy na množině a Sylowova věta

5.1 Akce grupy na množině

5.1.1. Definice. Nechť X je množina a G je grupa. Nechť $\circ : G \times X \to X$. Pro libovolné $(g, x) \in G \times X$ budeme místo $\circ((g, x))$ psát $g \circ x$ nebo jen gx. Zobrazení $\circ$ se nazývá **akce grupy G na množině X**, pokud platí:

1. $1x = x$ pro všechna $x \in X$
2. $g(hx) = (gh)x$ pro všechna $g, h \in G$, $x \in X$.

Uvedeme nyní dva příklady akcí grupy na množině, které později využijeme (v důkazu Sylowovy věty, v důkazu věty o centru p-grupy).

5.1.2. Příklad. Nechť G je grupa, n je kladné celé číslo. Položme

$$X = \{A \subseteq G |\ card(A) = n\}.$$

Budeme definovat akci grupy G na množině X:
Pro $g \in G$, $A \in X$ položíme

$$gA = \{ga |\ a \in A\}.$$

Prověříme, že jsme vskutku definovali akci grupy G na X.

1. Nechť $A \in X$, $A = \{a_1, \ldots, a_n\}$. Pak $gA = \{ga_1, \ldots, ga_n\}$. Ze zákona o krácení ihned plyne, že prvky $ga_1, \ldots, ga_n$ jsou navzájem různé, a tedy $card(gA) = card(A) = n$, $gA \in X$.

2. Nechť $A \in X$. Pak

$$1A = \{1 \cdot a |\ a \in A\} = \{a |\ a \in A\} = A.$$

3. Nechť $A \in X$, $g, h \in G$. Buď $A = \{a_1, \ldots, a_n\}$. Pak

$$\begin{aligned} g(hA) &= g\{ha_1, \ldots, ha_n\} \\ &= \{g(ha_1), \ldots, g(ha_n)\} \\ &= \{(gh)a_1, \ldots, (gh)a_n\} \\ &= (gh)A. \end{aligned}$$

5.1.3. Příklad. Nechť G je grupa. Definujeme akci grupy G na množině G takto:
Pro $g \in G$, $x \in G$,

$$g \circ x = gxg^{-1}.$$

Prověříme, že jsme vskutku definovali akci grupy G na G.

1. Buď $x \in G$. Chceme: $1 \circ x = x$.
   Je $1 \circ x = 1 \cdot x \cdot 1^{-1} = 1 \cdot x \cdot 1 = x$.

2. Buďte $g, h \in G$, $x \in G$. Chceme: $g \circ (h \circ x) = (gh) \circ x$.
   Je $g \circ (h \circ x) = g \circ (hxh^{-1}) = g(hxh^{-1})g^{-1} = (gh)x(h^{-1}g^{-1}) = (gh)x(gh)^{-1} = (gh) \circ x$.

5.1.4. Definice. Nechť je dána akce grupy G na množině X. Nechť $x \in X$. **Orbita** prvku x je množina

$$O(x) = \{gx |\ g \in G\} \subseteq X.$$

5.1.5. Věta. *Nechť je dána akce grupy G na množině X. Pak systém množin*

$$\{O(x) |\ x \in X\}$$

je rozklad množiny X.

Důkaz. Je třeba ukázat následující:
(I) Pro každé $x \in X$ je $O(x) \neq \emptyset$.
(II) $\bigcup_{x \in X} O(x) = X$
(III) Nechť $x, y \in X$, $O(x) \cap O(y) \neq \emptyset$. Chceme: $O(x) = O(y)$.
ad (I): Všimněme si, že $x \in O(x)$. To plyne z rovnosti $1x = x$.
ad (II): Je zřejmé, že $\bigcup_{x \in X} O(x) \subseteq X$. Buď $u \in X$. Pak $u \in O(u) \subseteq \bigcup_{x \in X} O(x)$. Jelikož prvek u byl zvolen libovolně, máme $X \subseteq \bigcup_{x \in X} O(x)$.
ad (III): Buď $z \in O(x) \cap O(y)$. Existují $g, h \in G$ tak, že $z = gx$, $z = hy$. Zvolme libovolně $u \in O(x)$. Existuje $p \in G$, $px = u$. Je $gx = hy$. Z toho pak $g^{-1}(gx) = g^{-1}(hy)$, $(gg^{-1})x = (g^{-1}h)y$, $1x = (g^{-1}h)y$, $x = (g^{-1}h)y$. Dále, $u = px = p((g^{-1}h)y) = (pg^{-1}h)y$. Je $pg^{-1}h \in G$. Vidíme, že $u \in O(y)$. Ukázali jsme, že $O(x) \subseteq O(y)$. Obdobně lze ukázat, že $O(y) \subseteq O(x)$.

5.1.6. Definice. Nechť je dána akce grupy G na množině X. Nechť $x \in X$. **Stabilizátor** prvku x je množina

$$G_x = \{g \in G |\ gx = x\} \subseteq G.$$

5.1.7. Tvrzení. *Nechť je dána akce grupy G na množině X. Nechť $x \in X$. Pak stabilizátor G_x je podgrupa grupy G.*

Důkaz. Je třeba ukázat následující:
(I) $1 \in G_x$
(II) Jestliže $g \in G_x$, pak $g^{-1} \in G_x$.
(III) Jestliže $g, h \in G_x$, pak $gh \in G_x$.

ad (I): $1x = x$, takže $1 \in G_x$
ad (II): Nechť $g \in G_x$. Pak $gx = x$. Z toho dostáváme $g^{-1}(gx) = g^{-1}x$, $(g^{-1}g)x = g^{-1}x$, $1x = g^{-1}x$, $x = g^{-1}x$, $g^{-1} \in G_x$.
ad (III): Nechť $g, h \in G_x$. Pak $gx = x$, $hx = x$. Z toho dostáváme $(gh)x = g(hx) = gx = x$, $gh \in G_x$.

5.1.8. Věta. *Nechť je dána akce grupy G na množině X. Nechť $x \in X$. Pak*

$$card(O(x)) = [G : G_x].$$

Důkaz. Podle definice je $[G : G_x] = card(G/G_x)$. Stačí tedy sestrojit nějakou bijekci $f : G/G_x \to O(x)$.
Nechť $a, b \in G$. Dokážeme toto tvrzení:
Jestliže $aG_x = bG_x$, pak $ax = bx$.
Nechť tedy $aG_x = bG_x$. Je $a \in aG_x$, takže $a \in bG_x$, $a = bg$ pro nějaké $g \in G_x$. Pak $ax = (bg)x = b(gx) = bx$.
Definujme zobrazení $f : G/G_x \to O(x)$ předpisem

$$f(aG_x) = ax$$

(a je libovolný prvek z G). Výše dokázané tvrzení ukazuje, že zobrazení f je definováno korektně.

1. f je injekce:
   Nechť $a, b \in G$, $f(aG_x) = f(bG_x)$. Chceme: $aG_x = bG_x$.
   Víme, že $ax = bx$. Zvolme libovolně $g \in G_x$. Ukážeme, že prvek ag patří do množiny bG_x. Je

   $$ag = 1 \cdot ag = (bb^{-1})(ag) = b(b^{-1}ag).$$

   Nyní
   $(b^{-1}ag)x = (b^{-1}a)(gx) = (b^{-1}a)x = b^{-1}(ax) = b^{-1}(bx) = (b^{-1}b)x = 1x = x$.
   Takže $b^{-1}ag \in G_x$ a tedy $ag \in bG_x$.
   Vzhledem k tomu, že prvek $g \in G_x$ byl zvolen libovolně, máme dokázánu inkluzi $aG_x \subseteq bG_x$. Obdobně lze dokázat, že $bG_x \subseteq aG_x$. Celkem $aG_x = bG_x$.

2. f je surjekce:
   Prvky z $O(x)$ mají tvar ax, kde $a \in G$. Ovšem $f(aG_x) = ax$. Vidíme, že f je surjekce.

5.1.9. Tvrzení. *Nechť je dána akce grupy G na množině X. Nechť grupa G je konečná. Buď $x \in X$. Pak $card(O(x))$ dělí $card(G)$.*

Důkaz. Víme, že stabilizátor G_x je podgrupa grupy G (viz 5.1.7.). Podle Lagrangeovy věty (3.1.9.) platí:

$$card(G) = [G : G_x] \cdot card(G_x).$$

Dle 5.1.8. je $card(O(x)) = [G : G_x]$, takže

$$card(G) = card(O(x)) \cdot card(G_x).$$

Vidíme, že $card(O(x))/card(G)$.

5.2 Věty Sylowova a Cauchyova

Nechť G je konečná grupa řádu n.

Jestliže H je podgrupa grupy G, pak $card(H)/n$. To plyne z Lagrangeovy věty (3.1.9.).

Nechť nyní d je kladné celé číslo, d/n. Položme si otázku, zda v grupě G existuje podgrupa řádu d.

Samozřejmě, v případě $d = 1$ nebo $d = n$ taková podgrupa určitě existuje (pro $d = 1$ jde o podgrupu $\{1\}$, pro $d = n$ jde o podgrupu G). V této kapitole uvidíme, že taková podgrupa vždy existuje v případě $d = p^k$, kde p je prvočíslo a k je nezáporné celé číslo. Nelze však tvrdit, že taková podgrupa vždy existuje pro jakékoli d. V následujícím příkladě uvidíme, že grupa A_4 řádu 12 nemá žádnou podgrupu řádu 6, ačkoli 6/12.

5.2.1. Příklad. Budeme se zabývat grupou A_4. O alternujících grupách je pojednáno v 2.4. Udělejme nyní tuto úmluvu: Permutaci $\pi \in S_n$ (n je přirozené číslo) budeme zapisovat stručně jako posloupnost $\pi(1)\pi(2)\ldots\pi(n)$.
Vypišme nejdříve všechny permutace z S_3 a určeme pro každou z nich počet inverzí.

permutace	123	132	321	213	312	231
počet inverzí	0	1	3	1	2	2

Jedna permutace abc z S_3 určí čtyři permutace z S_4:

$$4abc,\ a4bc,\ ab4c,\ abc4.$$

Počet inverzí v permutaci abc označme k. Pak platí:

permutace	$4abc$	$a4bc$	$ab4c$	$abc4$
počet inverzí	$k+3$	$k+2$	$k+1$	k

Do A_4 patří ty permutace z S_4, které mají sudý počet inverzí. Vypišme nyní všechny permutace z A_4:
$1423 = \pi_1$
$1234 = id$
$4132 = \pi_2$
$1342 = \pi_3$
$4321 = \pi_4$
$3241 = \pi_5$
$4213 = \pi_6$
$2143 = \pi_7$
$3412 = \pi_8$
$3124 = \pi_9$
$2431 = \pi_{10}$
$2314 = \pi_{11}$.
Nyní určíme řády všech permutací z A_4:
$\pi_1^2 = 1342 = \pi_3$, $\pi_1^3 = 1234 = id$, π_1 má řád 3
id má řád 1
$\pi_2^2 = 2431 = \pi_{10}$, $\pi_2^3 = 1234 = id$, π_2 má řád 3
$\pi_3^2 = 1423 = \pi_1$, $\pi_3^3 = 1234 = id$, π_3 má řád 3
$\pi_4^2 = 1234 = id$, π_4 má řád 2
$\pi_5^2 = 4213 = \pi_6$, $\pi_5^3 = 1234 = id$, π_5 má řád 3
$\pi_6^2 = 3241 = \pi_5$, $\pi_6^3 = 1234 = id$, π_6 má řád 3
$\pi_7^2 = 1234 = id$, π_7 má řád 2
$\pi_8^2 = 1234 = id$, π_8 má řád 2
$\pi_9^2 = 2314 = \pi_{11}$, $\pi_9^3 = 1234 = id$, π_9 má řád 3
$\pi_{10}^2 = 4132 = \pi_2$, $\pi_{10}^3 = 1234 = id$, π_{10} má řád 3
$\pi_{11}^2 = 3124 = \pi_9$, $\pi_{11}^3 = 1234 = id$, π_{11} má řád 3.
Zjistili jsme, že grupa A_4
má 1 prvek řádu 1, totiž prvek id
má 3 prvky řádu 2, totiž prvky π_4, π_7, π_8

má 8 prvků řádu 3, totiž prvky π_1, π_2, π_3, π_5, π_6, π_9, π_{10}, π_{11}.
Buď x prvek řádu 3. Pak $\langle x \rangle = \{1, x, x^2\}$.
Prvek x^2 má také řád 3 a $\langle x^2 \rangle = \{1, x^2, x\}$.
Pro libovolnou podgrupu H pak platí:

$$x \in H \iff x^2 \in H.$$

Vidíme, že prvky řádu 3 se budou v podgrupách vyskytovat ve dvojicích x, x^2. Pro grupu A_4 dostáváme následující dvojice:
π_1, π_3
π_2, π_{10}
π_5, π_6
π_9, π_{11}.
Předpokládejme nyní, že H je podgrupa grupy A_4, H má řád 6. Jsou dvě možnosti:

1. H obsahuje 2 prvky řádu 3.
   Jsou čtyři možnosti:
   (I) $H = \{id, \pi_4, \pi_7, \pi_8, \pi_1, \pi_3\}$
   (II) $H = \{id, \pi_4, \pi_7, \pi_8, \pi_2, \pi_{10}\}$
   (III) $H = \{id, \pi_4, \pi_7, \pi_8, \pi_5, \pi_6\}$
   (IV) $H = \{id, \pi_4, \pi_7, \pi_8, \pi_9, \pi_{11}\}$.
   ad (I): $\pi_4 \cdot \pi_1 = 3241 = \pi_5 \in H$, spor.
   ad (II): $\pi_4 \cdot \pi_2 = 2314 = \pi_{11} \in H$, spor.
   ad (III): $\pi_4 \cdot \pi_5 = 1423 = \pi_1 \in H$, spor.
   ad (IV): $\pi_4 \cdot \pi_9 = 4213 = \pi_6 \in H$, spor.

2. H obsahuje 4 prvky řádu 3.
   Je šest možností:
   (I) $H = \{id, \varrho, \pi_1, \pi_3, \pi_2, \pi_{10}\}$
   (II) $H = \{id, \varrho, \pi_1, \pi_3, \pi_5, \pi_6\}$
   (III) $H = \{id, \varrho, \pi_1, \pi_3, \pi_9, \pi_{11}\}$
   (IV) $H = \{id, \varrho, \pi_2, \pi_{10}, \pi_5, \pi_6\}$
   (V) $H = \{id, \varrho, \pi_2, \pi_{10}, \pi_9, \pi_{11}\}$
   (VI) $H = \{id, \varrho, \pi_5, \pi_6, \pi_9, \pi_{11}\}$
   Ve všech šesti případech je $\varrho \in \{\pi_4, \pi_7, \pi_8\}$.
   ad (I): $\pi_1 \cdot \pi_2 = 4213 = \pi_6 \in H$, spor.
   ad (II): $\pi_1 \cdot \pi_5 = 3124 = \pi_9 \in H$, spor.
   ad (III): $\pi_1 \cdot \pi_{11} = 2431 = \pi_{10} \in H$, spor.

ad (IV): $\pi_2 \cdot \pi_5 = 1342 = \pi_3 \in H$, spor.
ad (V): $\pi_2 \cdot \pi_{11} = 4213 = \pi_6 \in H$, spor.
ad (VI): $\pi_5 \cdot \pi_{11} = 1342 = \pi_3 \in H$, spor.

Právě provedený důkaz sporem ukazuje, že grupa A_4 nemá žádnou podgrupu řádu 6. Přitom $card(A_4) = 12$ a $6/12$.

Nyní nás čeká jedno pomocné tvrzení o binomických koeficientech.

5.2.1. Tvrzení. *Nechť p je prvočíslo, m je kladné celé číslo, n je nezáporné celé číslo, p nedělí m. Nechť k, l jsou taková nezáporná celá čísla, že $k+l = n$. Pak p^{l+1} nedělí $\binom{p^n \cdot m}{p^k}$.*

Důkaz. Nechť $k > 0$.

$$\begin{aligned}
\binom{p^n m}{p^k} &= \frac{p^n m(p^n m - 1)\dots(p^n m - (p^k - 1))}{p^k(p^k - 1)\dots(p^k - (p^k - 1))} \\
\binom{p^n m}{p^k} p^k(p^k - 1)..(p^k - (p^k - 1)) &= p^{k+l} m(p^n m - 1)..(p^n m - (p^k - 1)) \\
\binom{p^n m}{p^k} (p^k - 1)\dots(p^k - (p^k - 1)) &= p^l m(p^n m - 1)\dots(p^n m - (p^k - 1))
\end{aligned}$$

Buď $i \in \{1, \dots, p^k - 1\}$. Buď r_i nezáporné celé číslo, s_i kladné celé číslo, $i = p^{r_i} s_i$, p nedělí s_i. Zřejmě $r_i < k$ (jinak by bylo $i = p^{r_i} s_i \geq p^{r_i} \geq p^k$). Platí:

$$p^k - i = p^k - p^{r_i} s_i = p^{r_i}(p^{k-r_i} - s_i).$$

Takže p^{r_i} dělí $p^k - i$, p^{r_i+1} nedělí $p^k - i$ (případ p^{r_i+1} dělí $p^k - i$ by dal p dělí $p^{k-r_i} - s_i$, což by dalo p dělí $p^{k-r_i} - (p^{k-r_i} - s_i) = s_i$).
Dále platí:

$$p^n m - i = p^n m - p^{r_i} s_i = p^{r_i}(p^{n-r_i} m - s_i).$$

Takže p^{r_i} dělí $p^n m - i$, p^{r_i+1} nedělí $p^n m - i$ (případ p^{r_i+1} dělí $p^n m - i$ by dal p dělí $p^{n-r_i} m - s_i$, což by dalo p dělí $p^{n-r_i} m - (p^{n-r_i} m - s_i) = s_i$).
Existují tedy kladná celá čísla u_i, v_i s těmito vlastnostmi:
$p^k - i = p^{r_i} u_i$, p nedělí u_i
$p^n m - i = p^{r_i} v_i$, p nedělí v_i.
Pak

$$\begin{aligned}\binom{p^n m}{p^k} p^{r_1} u_1 \dots p^{r_{p^k-1}} u_{p^k-1} &= p^l m p^{r_1} v_1 \dots p^{r_{p^k-1}} v_{p^k-1} \\ \binom{p^n m}{p^k} u_1 \dots u_{p^k-1} &= p^l m v_1 \dots v_{p^k-1}.\end{aligned}$$

Předpokládejme, že p^{l+1} dělí $\binom{p^n m}{p^k}$. Pak p dělí $mv_1 \dots v_{p^k-1}$. Protože p nedělí m, existuje $i \in \{1, \dots, p^k - 1\}$, p dělí v_i. To je spor.
Tudíž p^{l+1} nedělí $\binom{p^n m}{p^k}$.
Na počátku důkazu jsme vynechali případ $k = 0$. Nyní se k němu vrátíme.
Nechť tedy $k = 0$. Pak $l = n$ a je třeba dokázat, že p^{n+1} nedělí $\binom{p^n m}{p^0} = \binom{p^n m}{1} = p^n m$. Kdyby p^{n+1} dělilo $p^n m$, pak by p dělilo m, což by byl spor. Takže p^{n+1} vskutku nedělí $p^n m$.

5.2.2. Věta. (Sylow) *Nechť G je konečná grupa, p je prvočíslo, k je nezáporné celé číslo. Jestliže p^k dělí řád grupy G, pak G má podgrupu řádu p^k.*

Důkaz. Nechť p^k dělí řád grupy G. Grupa G má řád $p^n m$, kde m je kladné celé číslo, n je nezáporné celé číslo, p nedělí m, $0 \leq k \leq n$.
Nechť X je soubor všech podmnožin grupy G, které mají mohutnost p^k, tj.

$$X = \{A \subseteq G |\ card(A) = p^k\}.$$

Je $card(X) = \binom{p^n m}{p^k}$. Dle tvrzení 5.2.1. p^{l+1} nedělí $card(X)$ (je $k + l = n$).
Definujme akci grupy G na množině X:
Pro $g \in G$, $A \in X$ položíme

$$gA = \{ga |\ a \in A\}.$$

Skutečně jsme definovali akci grupy G na množině X - viz příklad 5.1.2.
Uvědomme si, že systém množin $\{O(A) |\ A \in X\}$ je rozklad množiny X (viz 5.1.5.).
Existuje tedy přirozené číslo r a prvky $A_1, \dots, A_r \in X$ tak, že

$$card(X) = card(O(A_1)) + \dots + card(O(A_r)).$$

Předpokládejme, že pro každé $i \in \{1, 2, \dots, r\}$ platí: $p^{l+1} / card(O(A_i))$. Pak ovšem $p^{l+1} / card(X)$, spor.

Existuje tedy $B \in X$, p^{l+1} nedělí $card(O(B))$.
Buď G_B stabilizátor prvku B. Pak (dle 5.1.8.)

$$card(O(B)) = [G : G_B].$$

Lagrangeova věta říká, že $[G : G_B] \cdot card(G_B) = card(G)$. Z toho dostáváme

$$card(O(B)) \cdot card(G_B) = card(G) = p^n m.$$

Pak $card(G_B) = p^s m'$, kde s je celé číslo, $0 \leq s \leq n$, m' je kladné celé číslo, $m = m'm''$ pro nějaké kladné celé číslo m''.
Je $card(O(B)) = p^{n-s} m''$. Jelikož p^{l+1} nedělí $card(O(B))$, máme $n - s \leq l$, $k + l - s \leq l$, $k \leq s$. Takže $card(G_B) = p^s m' \geq p^s \geq p^k$.
Zvolme nyní $b_0 \in B$. To lze, neboť $card(B) = p^k \geq p^0 = 1$.
Buď $g \in G_B$. Jelikož g je prvek stabilizátoru G_B, je $gB = B$. Je $gb_0 \in gB$, takže $gb_0 \in B$.
Vidíme, že je možno definovat zobrazení $f : G_B \to B$ pomocí předpisu $f(g) = gb_0$ (pro libovolné $g \in G_B$).
Nechť $g, h \in G_B$, $f(g) = f(h)$. Pak $gb_0 = hb_0$, $g = h$ (použili jsme zákon o krácení). Právě jsme dokázali, že zobrazení f je prosté. Z toho vyplývá, že $card(G_B) \leq card(B) = p^k$.
Celkem: $card(G_B) = p^k$.
Víme, že stabilizátor G_B je podgrupa grupy G (viz 5.1.7.). Před chvílí jsme dokázali, že G_B má řád p^k.

Ze Sylowovy věty například vyplývá, že každá grupa řádu $1000 = 2^3 \cdot 5^3$ má určitě podgrupy řádů 2, 4, 8, 5, 25, 125.

Následující věta je důsledkem věty Sylowovy.

5.2.3. Věta. (Cauchy, 1845) *Nechť G je konečná grupa, nechť p je prvočíslo. Jestliže p dělí $card(G)$, pak G obsahuje prvek řádu p.*

Důkaz. Nechť $p/card(G)$. Z věty 5.2.2. plyne, že G má nějakou podgrupu H řádu p. Nechť $a \in H$, $a \neq 1$. Víme, že řád prvku a dělí řád grupy H (viz 3.1.10.), tedy řád prvku a dělí p. Protože $a \neq 1$, má prvek a řád p.

Buďte p prvočíslo, k celé číslo, $k \geq 2$.

Fakt p dělí $card(G)$ zaručuje, že grupa G obsahuje nějaký prvek řádu p (to říká Cauchyova věta).

Fakt p^k dělí $card(G)$ vůbec nezaručuje, že grupa G obsahuje nějaký prvek řádu p^k. Ukazuje to následující příklad.

5.2.4. Příklad. Buďte p prvočíslo, k celé číslo, $k \geq 2$. Uvažme grupu $G = \mathbb{Z}_p^k$. Zřejmě $card(G) = p^k$, takže $p^k / card(G)$. Nechť $x \in \mathbb{Z}_p$. Pak $px = 0$ dle 3.1.11. Nechť $a = (a_1, \ldots, a_k) \in \mathbb{Z}_p^k$. Pak

$$\begin{aligned} pa &= \underbrace{(a_1, \ldots, a_k) + \cdots + (a_1, \ldots, a_k)}_{p} \\ &= (\underbrace{a_1 + \cdots + a_1}_{p}, \ldots, \underbrace{a_k + \cdots + a_k}_{p}) \\ &= (pa_1, \ldots, pa_k) \\ &= (0, \ldots, 0) \\ &= 0. \end{aligned}$$

Vidíme, že prvek a má řád nejvýše p. Závěr: v grupě G neexistuje žádný prvek řádu p^k.

Na závěr této části uvedeme příklad, který předvede aplikaci Cauchyovy věty při důkazu jednoho tvrzení o komutativních grupách.

5.2.5. Příklad. Nechť G je grupa, p a q jsou prvočísla, $p \neq q$. Předpokládejme, že grupa G je komutativní a že má řád pq. Dokážeme:

$$G \cong \mathbb{Z}_{pq} \cong \mathbb{Z}_p \times \mathbb{Z}_q.$$

Podle Cauchyovy věty existují prvky $a, b \in G$, a má řád p, b má řád q. Uvědomme si, že řád prvku ab dělí řád grupy G. Jsou tedy čtyři možnosti:
(I) ab má řád 1
(II) ab má řád p
(III) ab má řád q
(IV) ab má řád pq.
ad (I):
$1 = 1^p = (ab)^p = a^p b^p = 1 \cdot b^p = b^p$, takže $p \geq q$
$1 = 1^q = (ab)^q = a^q b^q = a^q \cdot 1 = a^q$, takže $q \geq p$.
Celkem $p = q$, spor.
ad (II): $1 = (ab)^p = a^p b^p = 1 \cdot b^p = b^p$

Uvažme dělení se zbytkem $p = uq + v$ ($u, v \in \mathbb{Z}$, $0 \leq v < q$). Protože $p \neq q$, je $v \neq 0$, $0 < v < q$. Platí:
$1 = b^p = b^{uq+v} = (b^q)^u \cdot b^v = 1^u \cdot b^v = 1 \cdot b^v = b^v$
Dostali jsme spor, protože q je řád prvku b a $0 < v < q$.
ad (III): Tato možnost vede ke sporu obdobně jako možnost (II).
Protože možnosti (I), (II), (III) dávají spor, nutně nastává varianta (IV). Takže prvek ab má řád pq. Dle 4.1.5. je $G \cong \mathbb{Z}_{pq}$.
Nyní si stačí uvědomit, že grupa $\mathbb{Z}_p \times \mathbb{Z}_q$ je komutativní a že má řád pq. Z toho plyne izomorfismus $\mathbb{Z}_p \times \mathbb{Z}_q \cong \mathbb{Z}_{pq}$.
Například, existuje jediná komutativní grupa řádu 35, a to grupa $\mathbb{Z}_{35} \cong \mathbb{Z}_5 \times \mathbb{Z}_7$.

5.3 Centrum grupy

5.3.1. Definice. Nechť G je grupa. **Centrum** grupy G označujeme $Z(G)$ a definujeme jej jako

$$Z(G) = \{a \in G |\ \forall g \in G : ag = ga\}.$$

5.3.2. Tvrzení. *Nechť G je grupa. Platí:*

1. *$Z(G)$ je normální podgrupa grupy G*
2. *$Z(G)$ je komutativní grupa.*

Důkaz.

1. Je třeba dokázat následující:
   (I) $1 \in Z(G)$
   (II) Jestliže $a \in Z(G)$, pak $a^{-1} \in Z(G)$.
   (III) Jestliže $a, b \in Z(G)$, pak $ab \in Z(G)$.
   (IV) Jestliže $a \in Z(G)$, $g \in G$, pak $gag^{-1} \in Z(G)$.
   ad (I): Buď $g \in G$. Chceme: $g \cdot 1 = 1 \cdot g$. To zřejmě platí.
   ad (II): Nechť $a \in Z(G)$, $g \in G$. Chceme: $a^{-1}g = ga^{-1}$. Víme, že $ag = ga$. Pak $a^{-1}(ag)a^{-1} = a^{-1}(ga)a^{-1}$, $(a^{-1}a)ga^{-1} = a^{-1}g(aa^{-1})$, $1 \cdot ga^{-1} = a^{-1}g \cdot 1$, $ga^{-1} = a^{-1}g$.
   ad (III): Nechť $a, b \in Z(G)$, $g \in G$. Chceme: $(ab)g = g(ab)$. Počítejme:

$(ab)g = a(bg) = a(gb) = (ag)b = (ga)b = g(ab)$.
ad (IV): Nechť $a \in Z(G)$, $g \in G$. Chceme: $gag^{-1} \in Z(G)$. Počítejme: $gag^{-1} = (ga)g^{-1} = (ag)g^{-1} = a(gg^{-1}) = a \cdot 1 = a \in Z(G)$.

2. Tvrzení druhé části je zřejmé.

Co se týče centra grupy G, mohou nastat dva krajní případy.

1. $Z(G) = G$
   Je snadné si rozmyslet, že tento případ nastane právě tehdy, když grupa G je komutativní.

2. $Z(G) = \{1\}$
   V tomto případě říkáme, že grupa G je **bez centra**.

Uvedeme nyní příklady grup bez centra.

5.3.3. Příklad. Nechť M je množina, $card(M) \geq 3$. Pak symetrická grupa $S(M)$ je grupa bez centra, tj. $Z(S(M)) = \{id\}$. Specielně, grupy S_n pro $n \geq 3$ jsou grupy bez centra. Zdůvodnění:
Buď $\pi \in S(M)$, $\pi \neq id$. Ukážeme, že $\pi \notin Z(S(M))$.
Protože $\pi \neq id$, existují $a, b \in M$, $a \neq b$, $\pi(a) = b$. Jsou tři možnosti (teoreticky):
(I) $\pi(b) = a$
(II) $\pi(b) = b$
(III) $\pi(b) \neq a$, $\pi(b) \neq b$
ad (I): Protože $card(M) \geq 3$, existuje $c \in M$, $c \neq a$, $c \neq b$. Definujeme zobrazení $\varrho : M \to M$ takto:
$\varrho(a) = b$
$\varrho(b) = c$
$\varrho(c) = a$
$\varrho(x) = x$ pro $x \in M - \{a, b, c\}$.
Snadno se vidí, že $\varrho \in S(M)$. Počítejme:
$(\pi\varrho)(a) = \varrho(\pi(a)) = \varrho(b) = c$
$(\varrho\pi)(a) = \pi(\varrho(a)) = \pi(b) = a$
$(\pi\varrho)(a) \neq (\varrho\pi)(a) \Rightarrow \pi\varrho \neq \varrho\pi \Rightarrow \pi \notin Z(S(M))$.
ad (II): Tato možnost nenastává, neboť zobrazení π by nebylo prosté.
as (III): Označme $\pi(b) = c$. Je $c \in M$, $c \neq a$, $c \neq b$. Definujme zobrazení $\varrho : M \to M$ takto:

$\varrho(a) = b$
$\varrho(b) = a$
$\varrho(c) = c$
$\varrho(x) = x$ pro $x \in M - \{a, b, c\}$.
Snadno se vidí, že $\varrho \in S(M)$. Počítejme:
$(\pi\varrho)(a) = \varrho(\pi(a)) = \varrho(b) = a$
$(\varrho\pi)(a) = \pi(\varrho(a)) = \pi(b) = c$
$(\pi\varrho)(a) \neq (\varrho\pi)(a) \Rightarrow \pi\varrho \neq \varrho\pi \Rightarrow \pi \notin Z(S(M))$.

Nyní se ještě hodí uvést příklad grupy G, pro kterou $Z(G) \neq G$, $Z(G) \neq \{1\}$.

5.3.4. Příklad. Uvažme grupu kvaternionů $\mathbf{Q}$ (viz část 2.7.). Grupa $\mathbf{Q}$ není komutativní, takže $Z(\mathbf{Q}) \neq \mathbf{Q}$. Pro všechna $\alpha \in \mathbf{Q}$ je $(-1)\cdot\alpha = -\alpha$, $\alpha\cdot(-1) = -\alpha$, což dává $-1 \in Z(\mathbf{Q})$. Je tedy $Z(\mathbf{Q}) \neq \{1\}$.

5.3.5. Definice. Nechť G je grupa, p je prvočíslo. Grupa G se nazývá **p-grupa**, pokud její řád je roven p^k, kde k je nějaké kladné celé číslo.

5.3.6. Věta. *Nechť G je grupa, p je prvočíslo. Jestliže G je p-grupa, pak $Z(G) \neq \{1\}$.*

Důkaz. Předpokládejme, že G je p-grupa. Existuje kladné celé číslo k tak, že $card(G) = p^k$. Definujeme akci grupy G na množině G takto:

$$g \circ x = gxg^{-1}$$

pro $g \in G$, $x \in G$.
Opravdu jsme definovali akci grupy G na G, jak je ukázáno v příkladu 5.1.3.
Nechť $x \in G$, $x \in Z(G)$. Zvolme $g \in G$ libovolně. Pak $g \circ x = gxg^{-1} = (gx)g^{-1} = (xg)g^{-1} = x(gg^{-1}) = x \cdot 1 = x$. Takže $O(x) = \{x\}$.
Nechť $x \in G$, $O(x) = \{x\}$. Zvolme $g \in G$ libovolně. Pak $g \circ x = x$, $gxg^{-1} = x$, $(gxg^{-1})g = xg$, $(gx)(g^{-1}g) = xg$, $gx \cdot 1 = xg$, $gx = xg$. Takže $x \in Z(G)$.
Právě jsme dokázali následující ekvivalenci: Pro všechna $x \in G$,

$$x \in Z(G) \Leftrightarrow O(x) = \{x\}.$$

Víme, že soubor $\{O(x) |\ x \in G\}$ je rozklad množiny G (viz 5.1.5.). Existuje přirozené číslo r, prvky $x_1, x_2, \ldots, x_r \in G$,

$$G = O(x_1) \cup O(x_2) \cup \cdots \cup O(x_r),$$

a přitom pro všechna $i, j \in \{1, \ldots, r\}$ platí

$$i \neq j \Rightarrow O(x_i) \cap O(x_j) = \emptyset.$$

Nechť číslo $s \in \{1, \ldots, r\}$ má tuto vlastnost:

$$i \in \{1, \ldots, s\} \Leftrightarrow O(x_i) = \{x_i\}.$$

Takže

$$G = \{x_1\} \cup \cdots \cup \{x_s\} \cup O(x_{s+1}) \cup \cdots \cup O(x_r),$$
$$G = \{x_1, \ldots, x_s\} \cup O(x_{s+1}) \cup \cdots \cup O(x_r).$$

Dle výše dokázaného (jednoprvkovou orbitu mají právě prvky centra) je $Z(G) = \{x_1, \ldots, x_s\}$, takže

$$G = Z(G) \cup O(x_{s+1}) \cup \cdots \cup O(x_r),$$

$$card(G) = card(Z(G)) + card(O(x_{s+1})) + \cdots + card(O(x_r)).$$

Pro $j \in \{s+1, \ldots, r\}$ máme $card(O(x_j))/p^k$ (viz 5.1.9.), tudíž $card(O(x_j)) = p^{k_j}$ pro celé číslo k_j, $0 < k_j \leq k$ (je $k_j > 0$, protože $O(x_j) \neq \{x_j\}$). Nyní

$$p^k = card(Z(G)) + p^{k_{s+1}} + \cdots + p^{k_r}.$$

Je zřejmé, že $p/card(Z(G))$, a tedy $Z(G) \neq \{1\}$.

Samozřejmě, věta 5.3.6. je v souladu s příkladem 5.3.4. Grupa kvaternionů $\mathbf{Q}$ má řád 8, takže je to 2-grupa a nutně $Z(\mathbf{Q}) \neq \{1\}$.

Na závěr této části pomocí věty 5.3.6. dokážeme, že neexistuje žádná nekomutativní grupa řádu p^2 (p je prvočíslo).

5.3.7. Věta. *Nechť G je grupa, p je prvočíslo. Jestliže G má řád p^2, pak G je komutativní.*

Důkaz. Nechť G má řád p^2. Nechť $v \in G$. Položme

$$H = \{av^k |\ a \in Z(G),\ k \in \mathbb{Z}\}.$$

Dokážeme, že H je komutativní podgrupa grupy G. K tomu je třeba dokázat:
(I) $1 \in H$
(II) Jestliže $x \in H$, pak $x^{-1} \in H$.

(III) Jestliže $x, y \in H$, pak $xy \in H$.
(IV) Jestliže $x, y \in H$, pak $xy = yx$.
ad (I): $1 = 1 \cdot 1 = 1 \cdot v^0$. Protože $1 \in Z(G)$, $0 \in \mathbb{Z}$, je $1 \in H$.
ad (II): Nechť $x \in H$. Chceme: $x^{-1} \in H$. Existují $a \in Z(G)$, $k \in \mathbb{Z}$, $x = av^k$. Pak $x^{-1} = (av^k)^{-1} = (v^k)^{-1}a^{-1} = v^{-k}a^{-1}$. Protože $Z(G)$ je podgrupa, je $a^{-1} \in Z(G)$, $x^{-1} = v^{-k}a^{-1} = a^{-1}v^{-k} \in H$.
ad (III): Nechť $x, y \in H$. Chceme: $xy \in H$. Existují $a, b \in Z(G)$, $k, l \in \mathbb{Z}$, $x = av^k$, $y = bv^l$. Pak $xy = (av^k)(bv^l) = a(v^k b)v^l = a(bv^k)v^l = (ab)(v^k v^l) = (ab)v^{k+l}$. Protože $Z(G)$ je podgrupa, je $ab \in Z(G)$. Pak $xy = (ab)v^{k+l} \in H$.
ad (IV): Nechť $x, y \in H$. Chceme: $xy = yx$. Existují $a, b \in Z(G)$, $k, l \in \mathbb{Z}$, $x = av^k$, $y = bv^l$. V části (III) jsme již spočítali $xy = (ab)v^{k+l}$. Dále, $yx = (bv^l)(av^k) = b(v^l a)v^k = b(av^l)v^k = (ba)(v^l v^k) = (ab)v^{l+k}$. Podařilo se nám tedy ukázat, že $xy = yx$.
Dáke dokážeme, že $Z(G) \subseteq H$.
Zvolme libovolně $a \in Z(G)$. Chceme: $a \in H$. Ovšem $a = a \cdot 1 = av^0 \in H$.
Podle 5.3.6. je $Z(G) \neq \{1\}$. $Z(G)$ je podgrupa grupy G (5.3.2.). Dle Lagrangeovy věty (3.1.9.) pak $card(Z(G))/p^2$. Vzhledem k faktu $Z(G) \neq \{1\}$ tedy víme, že $card(Z(G)) = p$ nebo $card(Z(G)) = p^2$. Varianta $card(Z(G)) = p^2$ je příznivá - plyne z ní $Z(G) = G$ a tedy G je komutarivní. Stačí tudíž vyloučit variantu $card(Z(G)) = p$. Postupujme sporem. Předpokládejme, že $card(Z(G)) = p$. Buď $v \in G - Z(G)$. Uvažme výše zavedenou podgrupu H. Je $v = 1 \cdot v^1 \in H$. Takže $Z(G) \subseteq H$, $Z(G) \neq H$. Pak nutně $card(H) = p^2$, $H = G$ (řád podgrupy H totiž dělí p^2 dle Lagrangeovy věty a víme, že $card(H) > card(Z(G)) = p$). Protože H je komutativní, je G komutativní. Pak ovšem $Z(G) = G$, $card(Z(G)) = p^2$, spor.

6 Faktorové grupy

6.1 Definice faktorové grupy

Nechť m je kladné celé číslo. Položme

$$H_m = \{km |\ k \in \mathbb{Z}\}.$$

Snadno se lze přesvědčit, že H_m je podgrupa grupy $\mathbb{Z}$.

Víme, že systém množin

$$\{a + H_m |\ a \in \mathbb{Z}\}$$

je rozklad množiny $\mathbb{Z}$ (věta 3.1.2.). Tento rozklad značíme $\mathbb{Z}/H_m$.

Povšimněme si, že pro každou levou třídu grupy $\mathbb{Z}$ podle podgrupy H_m platí: $a+H_m = \overline{a}$, kde, pro připomenutí, $\overline{a} = \{x \in \mathbb{Z} |\ x \equiv a\ (m)\}$. Zdůvodnění následuje:

1. $a + H_m \subseteq \overline{a}$:
   Nechť $x \in a + H_m$. Pak existuje celé číslo k s vlastností $x = a + km$. Pak $x - a = km$, m dělí $x - a$, $x \equiv a\ (m)$. To ovšem znamená, že $x \in \overline{a}$.

2. $\overline{a} \subseteq a + H_m$:
   Nechť $x \in \overline{a}$. Pak $x \equiv a\ (m)$, m dělí $x - a$, $x - a = km$ pro nějaké $k \in \mathbb{Z}$. Pak $x = a + km$ pro $k \in \mathbb{Z}$, $x \in a + H_m$.

Takže $\mathbb{Z}/H_m = \{a + H_m |\ a \in \mathbb{Z}\} = \{\overline{a} |\ a \in \mathbb{Z}\} = \mathbb{Z}_m$ a pro libovolná $a, b \in \mathbb{Z}$ platí:

$$(a + H_m) + (b + H_m) = \overline{a} + \overline{b} = \overline{a + b} = (a + b) + H_m.$$

Nyní se pokusíme o zobecnění. Buď G libovolná grupa, buď H podgrupa grupy G. Na množině G/H definujme násobení následujícím předpisem:

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

(a, b jsou libovolné prvky z G).

Musíme být opatrní. Skutečně jsme definovali operaci na G/H? Příklad ukazuje, že obecně nikoli.

6.1.1. Příklad. Uvažme grupu S_3. Přijměme označení z příkladu 2.3.13., v němž jsme se grupou S_3 zabývali. Jelikož $a^2 = i$, má prvek a řád 2 a $H = \{i, a\}$ je podgrupa grupy S_3. Mělo by být $(bH) \cdot (bH) = (bb)H = iH = H$. Také by mělo být $(dH) \cdot (dH) = (dd)H = eH = e \cdot \{i, a\} = \{ei, ea\} = \{e, c\}$. Všimněme si však, že $bH = b \cdot \{i, a\} = \{bi, ba\} = \{b, d\}$, $dH = d \cdot \{i, a\} = \{di, da\} = \{d, b\}$. Tudíž $bH = dH$. Pak ovšem $(bH) \cdot (bH) = (dH) \cdot (dH)$, tedy $H = \{e, c\}$, spor. Získaný spor ukazuje, že definice násobení na množině G/H není korektní (aspoň pro $G = S_3$ a $H = \{i, a\}$ vede ke sporu).

Zesílíme předpoklad o podgrupě H. Předpokládejme, že podgrupa H je normální (viz 1.4.19.). Samozřejmě, v případě komutativní grupy G se o žádné zesílení nejedná, neboť každá podgrupa komutativní grupy je normální.

6.1.2. Tvrzení. *Nechť G je grupa, nechť H je normální podgrupa grupy G. Pak předpis*

$$(aH) \cdot (bH) = (ab)H$$

$(a, b \in G)$ korektně definuje operaci na množině G/H a G/H s touto operací je grupa.

Důkaz. Zabývejme se nejdříve korektností definice. Nechť $a, b, c, d \in G$, $aH = cH$, $bH = dH$. Chceme: $(ab)H = (cd)H$. Buď $x \in (ab)H$. Ukážeme, že $x \in (cd)H$. Existuje $h \in H$ tak, že $x = abh$. Jelikož $a = a \cdot 1$ a $1 \in H$, je $a \in H$. Ovšem $aH = cH$, takže $a \in cH$. Existuje $u \in H$, $a = cu$. Jelikož $b = b \cdot 1$ a $1 \in H$, je $b \in bH$. Ovšem $bH = dH$, takže $b \in dH$. Existuje $v \in H$, $b = dv$. Pak $x = abh = (cu)(dv)h$. Počítejme:

$$x = cudvh = c \cdot 1 \cdot udvh = c(dd^{-1})udvh = (cd)((d^{-1}ud)vh).$$

Je $d^{-1}ud = d^{-1}u(d^{-1})^{-1}$. Protože $u \in H$ a podgrupa H je normální, je $d^{-1}ud \in H$. Protože $d^{-1}ud, v, h \in H$, máme $(d^{-1}ud)vh \in H$ (H je podgrupa). Pak ovšem $x = (cd)((d^{-1}ud)vh) \in (cd)H$. Prvek $x \in (ab)H$ jsme zvolili libovolně, takže je dokázána inkluze $(ab)H \subseteq (cd)H$. Obdobně lze dokázat, že $(cd)H \subseteq (ab)H$, a tedy $(ab)H = (cd)H$.
Zbývá dokázat, že G/H je grupa.

1. Buďte $a, b, c \in G$. Chceme: $(aH) \cdot ((bH) \cdot (cH)) = ((aH) \cdot (bH)) \cdot (cH)$. Počítejme:

$$\begin{aligned}(aH) \cdot ((bH) \cdot (cH)) &= (aH) \cdot (bc)H \\ &= (a(bc))H \\ &= ((ab)c)H \\ &= (ab)H \cdot (cH) \\ &= ((aH) \cdot (bH)) \cdot (cH).\end{aligned}$$

2. Buď $a \in G$. Pak

$$(1H) \cdot (aH) = (1 \cdot a)H = aH, \ (aH) \cdot (1H) = (a \cdot 1)H = aH.$$

Vidíme, že $1H = H$ je neutrální prvek.

3. Buď $a \in G$. Pak

$$(aH) \cdot (a^{-1}H) = (aa^{-1})H = 1H = H,$$
$$(a^{-1}H) \cdot (aH) = (a^{-1}a)H = 1H = H.$$

Vidíme, že prvek $a^{-1}H$ je inverzní k prvku aH.

6.1.3. Definice. Nechť G je grupa, nechť H je normální podgrupa grupy G. Grupa G/H z tvrzení 6.1.2. se nazývá **faktorová grupa** grupy G podle podgrupy H.

Vzhledem k tvrzení 6.1.2. podgrupa $H = \{i, a\}$ nemůže být normální podgrupou grupy S_3 (vracíme se ještě krátce k příkladu 6.1.1.). Vskutku, $a \in H$, $b \in S_3$, přitom však $bab^{-1} = bab = db = c \notin H$ (označení, stejně jako v 6.1.1., je vzato z 2.3.13.).

6.1.4. Příklad. Zopakujme jeden základní příklad faktorové grupy. Nechť m je kladné celé číslo. Položme $H_m = \{km |\ k \in \mathbb{Z}\}$. Pak H_m je (normální) podgrupa grupy $\mathbb{Z}$ a $\mathbb{Z}/H_m = \mathbb{Z}_m$.

6.1.5. Příklad. Uvažme grupu $\mathbb{C}^\times$ a její podgrupu $H = \{x \in \mathbb{C} |\ |x| = 1\}$ (viz 1.4.5.). Dále uvažme grupu $\mathbb{R}$ a její podgrupu $\mathbb{Z}$. Protože $\mathbb{R}$ je komutativní, je $\mathbb{Z}$ normální podgrupa grupy $\mathbb{R}$. Definujme zobrazení $f : \mathbb{R}/\mathbb{Z} \to H$ takto: Pro $a \in \mathbb{R}$ klademe

$$f(a + \mathbb{Z}) = \cos 2\pi a + i \sin 2\pi a.$$

Prověříme nejprve, že zobrazení f je definováno korektně.

1. Chceme: $\cos 2\pi a + i \sin 2\pi a \in H$.
   To platí, neboť $|\cos 2\pi a + i \sin 2\pi a| = \sqrt{\cos^2 2\pi a + \sin^2 2\pi a} = \sqrt{1} = 1$.

2. Nechť $a, b \in \mathbb{R}$, $a + \mathbb{Z} = b + \mathbb{Z}$. Chceme: $\cos 2\pi a + i \sin 2\pi a = \cos 2\pi b + i \sin 2\pi b$.
   Je $0 \in \mathbb{Z}$, takže $a = a + 0 \in a + \mathbb{Z}$. Pak $a \in b + \mathbb{Z}$. Existuje $k \in \mathbb{Z}$, $a = b + k$. Z toho plyne

$$\begin{aligned} \cos 2\pi a + i \sin 2\pi a &= \cos 2\pi(b + k) + i \sin 2\pi(b + k) \\ &= \cos(2\pi b + 2\pi k) + i \sin(2\pi b + 2\pi k) \\ &= \cos 2\pi b + i \sin 2\pi b. \end{aligned}$$

   Využili jsme fakt, že funkce cos, sin mají periodu 2π.

Nyní se přesvědčíme, že f je izomorfismus:

1. f je homomorfismus:
   Nechť $a, b \in \mathbb{R}$. Chceme: $f((a+\mathbb{Z})+(b+\mathbb{Z})) = f(a+\mathbb{Z}) \cdot f(b+\mathbb{Z})$.
   Počítejme:
   $f((a+\mathbb{Z})+(b+\mathbb{Z}))$
   $= f((a+b)+\mathbb{Z})$
   $= \cos 2\pi(a+b) + i \sin 2\pi(a+b)$
   $= \cos(2\pi a + 2\pi b) + i \sin(2\pi a + 2\pi b)$
   $= (\cos 2\pi a \cdot \cos 2\pi b - \sin 2\pi a \cdot \sin 2\pi b) + i(\sin 2\pi a \cdot \cos 2\pi b + \cos 2\pi a \cdot \sin 2\pi b)$,
   $f(a+\mathbb{Z}) \cdot f(b+\mathbb{Z})$
   $= (\cos 2\pi a + i \sin 2\pi a) \cdot (\cos 2\pi b + i \sin 2\pi b)$
   $= \cos 2\pi a \cdot \cos 2\pi b + i \cos 2\pi a \cdot \sin 2\pi b + i \sin 2\pi a \cdot \cos 2\pi b - \sin 2\pi a \cdot \sin 2\pi b$
   $= (\cos 2\pi a \cdot \cos 2\pi b - \sin 2\pi a \cdot \sin 2\pi b) + i(\sin 2\pi a \cdot \cos 2\pi b + \cos 2\pi a \cdot \sin 2\pi b)$.
   Vidíme, že $f((a+\mathbb{Z})+(b+\mathbb{Z})) = f(a+\mathbb{Z}) \cdot f(b+\mathbb{Z})$.

2. f je injekce:
   Nechť $a, b \in \mathbb{R}$, $f(a+\mathbb{Z}) = f(b+\mathbb{Z})$. Chceme: $a+\mathbb{Z} = b+\mathbb{Z}$.
   Víme, že $\cos 2\pi a + i \sin 2\pi a = \cos 2\pi b + i \sin 2\pi b$. Pak $\cos 2\pi a = \cos 2\pi b$, $\sin 2\pi a = \sin 2\pi b$. Tedy

$$\begin{aligned} \cos 2\pi a - \cos 2\pi b &= -2 \cdot \sin \frac{2\pi a + 2\pi b}{2} \cdot \sin \frac{2\pi a - 2\pi b}{2} \\ &= -2 \cdot \sin(\pi a + \pi b) \cdot \sin(\pi a - \pi b) \\ &= 0, \end{aligned}$$

$$\begin{aligned} \sin 2\pi a - \sin 2\pi b &= 2 \cdot \cos \frac{2\pi a + 2\pi b}{2} \cdot \sin \frac{2\pi a - 2\pi b}{2} \\ &= 2 \cdot \cos(\pi a + \pi b) \cdot \sin(\pi a - \pi b) \\ &= 0. \end{aligned}$$

   Předpokládejme, že $\sin(\pi a - \pi b) \neq 0$. Pak musí být $\sin(\pi a + \pi b) = 0$ a $\cos(\pi a + \pi b) = 0$. Existují tedy celá čísla k, l s vlastnostmi $\pi a + \pi b = k\pi$, $\pi a + \pi b = \frac{\pi}{2} + l\pi$. Odtud $k\pi = \frac{\pi}{2} + l\pi$, $k = \frac{1}{2} + l$, $2k = 1 + 2l$, sudé číslo je rovno lichému číslu, spor.
   Nutně tedy $\sin(\pi a - \pi b) = 0$. Pak existuje celé číslo k, $\pi a - \pi b = k\pi$,

$a - b = k$. Ukážeme, že $a + \mathbb{Z} = b + \mathbb{Z}$.
Buď $x \in a + \mathbb{Z}$. Existuje $l \in \mathbb{Z}$, $x = a + l$. Pak $x = (b + k) + l = b + (k + l) \in b + \mathbb{Z}$. Ukázali jsme, že $a + \mathbb{Z} \subseteq b + \mathbb{Z}$.
Buď $x \in b + \mathbb{Z}$. Existuje $m \in \mathbb{Z}$, $x = b + m$. Pak $x = (a - k) + m = a + (m - k) \in a + \mathbb{Z}$. Ukázali jsme, že $b + \mathbb{Z} \subseteq a + \mathbb{Z}$.
Celkem tedy $a + \mathbb{Z} = b + \mathbb{Z}$.

3. f je surjekce:
Nechť $x \in H$. Hledáme $a \in \mathbb{R}$ tak, aby $f(a + \mathbb{Z}) = x$.
Existuje $\alpha \in \mathbb{R}$ tak, že $x = |x| \cdot (\cos\alpha + i \sin\alpha) = 1 \cdot (\cos\alpha + i \sin\alpha) = \cos\alpha + i \sin\alpha$ (tzv. goniometrické vyjádření čísla x). Buď $a = \frac{\alpha}{2\pi}$. Pak $a \in \mathbb{R}$ a

$$\begin{aligned} f(a + \mathbb{Z}) &= \cos 2\pi a + i \sin 2\pi a \\ &= \cos 2\pi \cdot \frac{\alpha}{2\pi} + i \sin 2\pi \cdot \frac{\alpha}{2\pi} \\ &= \cos\alpha + i \sin\alpha \\ &= x. \end{aligned}$$

Sestrojili jsme izomorfismus $f : \mathbb{R}/\mathbb{Z} \to H$. Tudíž $\mathbb{R}/\mathbb{Z} \cong H = \{x \in \mathbb{C} |\ |x| = 1\}$.

6.2 Faktorové grupy a homomorfismy

Připomeňme si, že pro homomorfismus $f : G_1 \to G_2$ je jádro $\ker f$ definováno jako $\ker f = \{x \in G_1 |\ f(x) = 1\}$.

6.2.1. Věta. *Nechť G je grupa, H je normální podgrupa grupy G. Definujme zobrazení $f : G \to G/H$ předpisem*

$$f(a) = aH$$

pro $a \in G$. Pak f je surjektivní homomorfismus a $\ker f = H$.

Důkaz.

1. f je homomorfismus:
Nechť $a, b \in G$. Počítejme:

$$f(a \cdot b) = (a \cdot b)H = (aH) \cdot (bH) = f(a) \cdot f(b).$$

2. f je surjekce:
   Nechť $x \in G/H$. Hledáme $a \in G$ tak, aby $f(a) = x$.
   Existuje $a \in G$, $x = aH$. Pak $f(a) = aH = x$.

3. $\ker f = H$:
   Nechť $a \in \ker f$. Chceme: $a \in H$.
   Je $f(a) = 1 \cdot H$, tj $aH = H$. Protože $a = a \cdot 1 \in aH$, máme $a \in H$.
   Nechť $a \in H$. Chceme: $a \in \ker f$.
   Je třeba ukázat, že $f(a) = 1 \cdot H$, tj. $aH = H$.
   $aH \subseteq H$:
   Buď $x \in aH$. Existuje $h \in H$, $x = ah$. Protože $a, h \in H$, H je podgrupa, je $ah \in H$. Takže $x \in H$.
   $H \subseteq aH$:
   Buď $x \in H$. Je $x = 1 \cdot x = (aa^{-1})x = a(a^{-1}x)$. Protože $a \in H$, H je podgrupa, je $a^{-1} \in H$. Protože $x \in H$, je též $a^{-1}x \in H$. Pak $x = a(a^{-1}x) \in aH$.

Nechť G_1, G_2 jsou grupy, $f : G_1 \to G_2$ je homomorfismus. Víme již, že $\ker f$ je podgrupa grupy G_1 (viz 1.4.10.). Platí dokonce víc, jak ukazuje další tvrzení.

6.2.2. Tvrzení. *Nechť G_1, G_2 jsou grupy, $f : G_1 \to G_2$ je homomorfismus. Pak $\ker f$ je normální podgrupa grupy G_1.*

Důkaz. Z 1.4.10. víme, že $\ker f$ je podgrupa grupy G_1. Zbývá ještě ukázat následující:
Nechť $h \in \ker f$, $g \in G_1$. Chceme: $ghg^{-1} \in \ker f$. Počítejme:

$$f(ghg^{-1}) = f(g)f(h)f(g^{-1}) = f(g) \cdot 1 \cdot f(g^{-1}) = f(g)f(g)^{-1} = 1.$$

Vidíme, že $ghg^{-1} \in \ker f$.

V případě homomorfismu $f : G_1 \to G_2$ lze tedy vždy uvažovat faktorovou grupu $G_1/\ker f$. O této grupě (v případě, že f je surjekce) vypovídá následující věta.

6.2.3. Věta. *Nechť G_1, G_2 jsou grupy, $f : G_1 \to G_2$ je surjektivní homomorfismus. Pak $G_1/\ker f \cong G_2$.*

Důkaz. Definujme zobrazení $g : G_1/\ker f \to G_2$ takto:

$$g(a \ker f) = f(a)$$

($a \in G_1$). Nejprve musíme dokázat, že zobrazení g je definováno korektně. Nechť tedy $a, b \in G_1$, $a \ker f = b \ker f$. Je třeba, aby $f(a) = f(b)$. Je $1 \in \ker f$, takže $a = a \cdot 1 \in a \ker f$. Pak ovšem $a \in b \ker f$ a existuje $c \in \ker f$, $a = bc$. Nyní $f(a) = f(bc) = f(b)f(c) = f(b) \cdot 1 = f(b)$.
Ukážeme, že g je izomorfismus.

1. g je homomorfismus:
   Buďte $a, b \in G_1$. Chceme: $g((a \ker f) \cdot (b \ker f)) = g(a \ker f) \cdot g(b \ker f)$.
   Počítejme:
   $g((a \ker f) \cdot (b \ker f)) = g((ab) \ker f) = f(ab) = f(a) \cdot f(b) = g(a \ker f) \cdot g(b \ker f)$.

2. g je injekce:
   Buďte $a, b \in G_1$, $g(a \ker f) = g(b \ker f)$. Chceme: $a \ker f = b \ker f$.
   Víme, že $f(a) = f(b)$.
   Buď $x \in a \ker f$. Existuje $c \in \ker f$, $x = ac$. Pak $x = 1 \cdot ac = (bb^{-1})ac = b(b^{-1}ac)$. Platí: $f(b^{-1}ac) = f(b)^{-1}f(a)f(c) = f(b)^{-1}f(b) \cdot 1 = 1$, takže $b^{-1}ac \in \ker f$. Jako důsledek máme $x = b(b^{-1}ac) \in b \ker f$. Jelikož prvek $x \in a \ker f$ jsme volili libovolně, dokázali jsme inkluzi $a \ker f \subseteq b \ker f$. Obdobně se dokáže, že $b \ker f \subseteq a \ker f$. Celkem pak $a \ker f = b \ker f$.

3. g je surjekce:
   Buď $y \in G_2$. Hledáme $a \in G_1$ tak, aby $g(a \ker f) = y$. Protože zobrazení f je surjekce, existuje $a \in G_1$, $f(a) = y$. Pak ovšem $g(a \ker f) = f(a) = y$.

Našli jsme izomorfismus $g : G_1/\ker f \to G_2$. V důsledku pak $G_1/\ker f \cong G_2$.

Uvedeme teď několik příkladů ilustrujících větu 6.2.3.

6.2.4. Příklad. Nechť G je grupa. Uvažme zobrazení $f : G \to \{1\}$ dané vztahem $f(x) = 1$ pro každé $x \in G$. Zřejmě f je surjektivní homomorfismus. Pak $G/\ker f \cong \{1\}$. Ovšem $\ker f = G$, takže $G/G \cong \{1\}$.

6.2.5. Příklad. Nechť G je grupa. Uvažme identické zobrazení $id : G \to G$. Zřejmě id je izomorfismus. Pak $G/\ker id \cong G$. Ovšem $\ker id = \{1\}$, takže $G/\{1\} \cong G$.

6.2.6. Příklad. Uvažme zobrazení $f : \mathbb{R}^\times \to \mathbb{R}^+$ dané předpisem $f(x) = |x|$ (pro libovolné $x \in \mathbb{R}^\times$). Buďte $x, y \in \mathbb{R}^\times$. Pak

$$f(x \cdot y) = |x \cdot y| = |x| \cdot |y| = f(x) \cdot f(y).$$

Vidíme, že f je homomorfismus.
Dále, nechť $y \in \mathbb{R}^+$ je libovolný prvek. Pak $y \in \mathbb{R}^\times$ a $f(y) = |y| = y$. Vidíme, že f je surjekce.
Dle věty 6.2.3. pak $\mathbb{R}^\times/\ker f \cong \mathbb{R}^+$. Jak vypadá $\ker f$? Dle definice $\ker f = \{x \in \mathbb{R}^\times |\ f(x) = 1\}$. Tedy

$$\ker f = \{x \in \mathbb{R}^\times |\ |x| = 1\} = \{1, -1\}.$$

Na závěr lze říci, že $\mathbb{R}^\times/\{1, -1\} \cong \mathbb{R}^+$.

6.2.7. Příklad. Množina $\{1, -1\}$ spolu s operací násobení je grupa (je to podgrupa grupy $\mathbb{R}^\times$). Nechť n je celé číslo, $n \geq 2$. Všimněme si, že zobrazení $Sg : S_n \to \{1, -1\}$ je surjektivní homomorfismus. Nechť $\pi, \rho \in S_n$. Pak $Sg(\pi\rho) = Sg(\pi) \cdot Sg(\rho)$ (viz 2.3.12.). Takže Sg je homomorfismus. Zobrazení Sg je surjekce, neboť sudé permutace z S_n zobrazuje na 1 a liché permutace z S_n zobrazuje na -1 (přitom je důležité si uvědomit, že v S_n vždy existují sudé i liché permutace - všech sudých permutací je $\frac{n!}{2}$, všech lichých permutací je také $\frac{n!}{2}$). Podle 6.2.3. je $S_n/\ker Sg \cong \{1, -1\}$. Jak vypadá $\ker Sg$? Je

$$\ker Sg = \{\pi \in S_n |\ Sg(\pi) = 1\} = A_n$$

(viz 2.4.1.).
Závěrem lze konstatovat, že $S_n/A_n \cong \{1, -1\}$.

6.2.8. Příklad. V tomto příkladu se zabýváme obecnou lineární grupou (viz část 2.5). Nechť n je kladné celé číslo, nechť T je těleso. Uvažme zobrazení $f : GL(n, T) \to T^\times$ dané předpisem

$$f(A) = |A|$$

($A \in GL(n, T)$). Připomeňme, že $|A|$ značí determinant matice A.
Zobrazení f je surjektivní homomorfismus:

1. Nechť $A, B \in GL(n,T)$. Pak

$$f(AB) = |AB| = |A| \cdot |B| = f(A) \cdot f(B).$$

2. Buď $c \in T^\times$. Hledáme $A \in GL(n,T)$ tak, aby $f(A) = c$.
Definujme matici $A \in T_{n,n}$ takto:
$a_{11} = c$, $a_{ii} = 1$ pro $i \in \{2, \ldots, n\}$, $a_{ij} = 0$ pro $i, j \in \{1, 2, \ldots, n\}$, $i \neq j$.
Pak $|A| = a_{11} \cdot a_{22} \cdots a_{nn} = c \cdot 1 \cdots 1 = c \neq 0$.
Tudíž $A \in GL(n,T)$ a také $f(A) = |A| = c$.

Nyní aplikujeme 6.2.3. a dostáváme $GL(n,T)/\ker f \cong T^\times$.
Je

$$\begin{aligned} \ker f &= \{A \in GL(n,T) |\ f(A) = 1\} \\ &= \{A \in GL(n,T) |\ |A| = 1\} \\ &= \{A \in T_{n,n} |\ |A| = 1\}. \end{aligned}$$

Podgrupa $\{A \in T_{n,n} |\ |A| = 1\}$ grupy $GL(n,T)$ se označuje $SL(n,T)$ a nazývá se **speciální lineární grupa**.
Ukázali jsme tedy, že $GL(n,T)/SL(n,T) \cong T^\times$.

7 Konečné (zvláště komutativní) grupy

7.1 Nerozložitelné grupy

Zopakujme si některé základní poznatky o celých číslech. Celá čísla lze násobit a toto násobení je asociativní a komutativní. Významnou roli hrají prvočísla. Celé číslo $p > 1$ se nazývá prvočíslo, pokud pro všechna kladná celá čísla u, v platí

$$p = uv \ \Rightarrow \ (u = 1 \ \vee \ v = 1).$$

Také grupy lze násobit. Máme na mysli součin grup zavedený v části 1.5. Násobení grup je také asociativní a komutativní, a to v následujícím smyslu: Pro všechny grupy G_1, G_2, G_3 platí

$$(G_1 \times G_2) \times G_3 \cong G_1 \times (G_2 \times G_3), \ G_1 \times G_2 \cong G_2 \times G_1$$

(viz 1.5.5. a 1.5.6.). Analogií pojmu prvočíslo je pojem nerozložitelná grupa.

7.1.1. Definice. Nechť G je grupa, $card(G) > 1$. Grupa G se nazývá **nerozložitelná**, pokud pro všechny grupy H, K platí

$$G \cong H \times K \;\Rightarrow\; (H = \{1\} \vee K = \{1\}).$$

7.1.2. Příklad. Každá grupa G řádu p, kde p je prvočíslo, je nerozložitelná. Nechť $G \cong H \times K$. Pak $card(G) = card(H) \cdot card(K)$, $p = card(H) \cdot card(K)$. Jelikož p je prvočíslo, je $card(H) = 1$ nebo $card(K) = 1$. Pak ovšem $H = \{1\}$ nebo $K = \{1\}$.

7.1.3. Příklad. Nechť p je prvočíslo. Každá cyklická p-grupa je nerozložitelná. Buď G cyklická p-grupa. Existuje $a \in G$, $G = \langle a \rangle$. Existuje celé číslo n, $n > 0$, $card(G) = p^n$. Dokážeme sporem,že grupa G je nerozložitelná. Předpokládejme, že G je rozložitelná (tj. není nerozložitelná). Pak existují grupy H, K, $G \cong H \times K$, $H \neq \{1\}$, $K \neq \{1\}$. Je $card(G) = card(H) \cdot card(K)$, $card(H) > 1$, $card(K) > 1$. Protože $card(G) = p^n$, je $card(H) = p^i$, $card(K) = p^j$, přičemž i, j jsou celá čísla, $i > 0$, $j > 0$, $i + j = n$. Bez újmy na obecnosti lze předpokládat, že $i \leq j$. Pro každý prvek $k \in K$ je

$$k^{p^j} = 1$$

(viz 3.1.11.). Dále, pro každý prvek $h \in H$ je

$$h^{p^j} = h^{p^i \cdot p^{j-i}} = (h^{p^i})^{p^{j-i}} = 1^{p^{j-i}} = 1.$$

Nechť $h \in H$, $k \in K$. Pak

$$(h, k)^{p^j} = (h^{p^j}, k^{p^j}) = (1, 1).$$

Takže každý prvek grupy $H \times K$ má řád nejvýše p^j. Ovšem $G \cong H \times K$, takže každý prvek grupy G má řád nejvýše p^j.
Označme r řád prvku a. Je $r \leq p^j$ (neboť $a \in G$). Podgrupa $\langle a \rangle$ má řád r (viz 1.4.18.). Protože $G = \langle a \rangle$, G má řád r. Všimněme si, že $0 < i$, což dává $p^0 < p^i$, $p^0 \cdot p^j < p^i \cdot p^j$, $p^{0+j} < p^{i+j}$, $p^j < p^n$. Platí:

$$card(G) = r \leq p^j < p^n = card(G).$$

Je tedy $card(G) < card(G)$. Dostali jsme spor. Tudíž G je nerozložitelná.
Uvědomme si ještě, že cyklické p-grupy jsou (až na izomorfismus) právě grupy $\mathbb{Z}_{p^n}$, kde n je celé číslo, $n > 0$ (viz 4.1.4.).
V tomto příkladu jsme tudíž ukázali nerozložitelnost grup $\mathbb{Z}_{p^n}$, kde p je prvočíslo a n je celé číslo, $n > 0$.

Máme již k dispozici příklady konečných nerozložitelných komutativních grup (jsou to grupy $\mathbb{Z}_{p^n}$). Uvedeme dále příklady konečných nerozložitelných nekomutativních grup.

7.1.4. Příklad. Nechť p je prvočíslo. Každá nekomutativní grupa řádu p^3 je nerozložitelná. Buď G nekomutativní grupa řádu p^3. Dokážeme sporem, že G je nerozložitelná. Předpokládejme, že G je rozložitelná. Pak existují grupy H, K, přičemž $G \cong H \times K$, $H \neq \{1\}$, $K \neq \{1\}$. Potom $card(G) = card(H) \cdot card(K)$, $card(H) > 1$, $card(K) > 1$. Jelikož $card(G) = p^3$, je $card(H) = p$, $card(K) = p^2$ nebo $card(H) = p^2$, $card(K) = p$. Nechť například $card(H) = p$, $card(K) = p^2$ (situace $card(H) = p^2$, $card(K) = p$ je obdobná). Uvědomme si, že $H \cong \mathbb{Z}_p$ (viz 4.1.6.), tudíž H je komutativní. Také K je komutativní dle 5.3.7. Pak ovšem $H \times K$ je komutativní (viz 1.5.9.). Jelikož $G \cong H \times K$, je G komutativní, spor. Závěr: G je nerozložitelná.
Uveďme ještě konkrétní příklad konečné nerozložitelné nekomutativní grupy. Je to třeba grupa kvaternionů $\mathbf{Q}$ – má totiž řád $8 = 2^3$ a není komutativní.

Snad bude ještě vhodné uvést aspoň jeden příklad nekonečné nerozložitelné grupy.

7.1.5. Příklad. Vezměme grupu $\mathbb{Z}$. Ukážeme, že $\mathbb{Z}$ je nerozložitelná. Nechť H, K jsou grupy, $\mathbb{Z} \cong H \times K$. Protože grupy H, K jsou komutativní, použijeme pro ně aditivní symboliku. Položme $A = H \times \{0\}$, $B = \{0\} \times K$. Množiny A, B jsou podgrupy grupy $H \times K$. Ukážeme to pro množinu A (důkaz pro B je obdobný).

1. Je $0 \in H$, takže $(0,0) \in H \times \{0\} = A$. Přitom $(0,0)$ je neutrální prvek grupy $H \times K$.

2. Nechť $x \in A$. Chceme: $-x \in A$.
   Je $x = (h,0)$ pro nějaké $h \in H$. Pak $-x = -(h,0) = (-h,-0) = (-h,0) \in H \times \{0\} = A$.

3. Nechť $x, y \in A$. Chceme: $x + y \in A$.
   Je $x = (r, 0)$, $y = (s, 0)$ pro nějaká $r, s \in H$. Pak $x+y = (r, 0)+(s, 0) = (r + s, 0 + 0) = (r + s, 0) \in H \times \{0\} = A$.

Všimněme si, že $A \cap B = \{(0, 0)\}$. Nyní dokážeme sporem, že $A = \{(0, 0)\}$ nebo $B = \{(0, 0)\}$. Předpokládejme, že $A \neq \{(0, 0)\}$ a $B \neq \{(0, 0)\}$. Tedy: v $H \times K$ existují dvě netriviální podgrupy, jejichž průnikem je podgrupa triviální (triviální podgrupou rozumíme podgrupu $\{(0, 0)\}$). Protože $\mathbb{Z} \cong H \times K$, existují v $\mathbb{Z}$ podgrupy C, D, $C \cap D = \{0\}$, $C \neq \{0\}$, $D \neq \{0\}$. Dle 4.2.1. existují nezáporná celá čísla c, d tak že $C = \langle c\rangle$, $D = \langle d\rangle$. Protože $C \neq \{0\}$, $D \neq \{0\}$, je $c \neq 0$, $d \neq 0$. Víme, že $\langle c\rangle = \{nc|\ n \in \mathbb{Z}\}$, $D = \{nd|\ n \in \mathbb{Z}\}$. Pak $dc \in \langle c\rangle$, $cd \in \langle d\rangle$, $cd \in C \cap D$. Jelikož $cd \neq 0$, dostáváme se ke sporu s faktem $C \cap D = \{0\}$. Tudíž $A = \{(0, 0)\}$ nebo $B = \{(0, 0)\}$. Nechť $A = \{(0, 0)\}$. Protože $A = H \times \{0\}$, musí být $H = \{0\}$. Nechť $B = \{(0, 0)\}$. Protože $B = \{0\} \times K$, musí být $K = \{0\}$. Závěr: grupa $\mathbb{Z}$ je nerozložitelná.

Vzpomínejme dále. Velký význam prvočísel spočívá v tom, že každé celé číslo n, $n > 1$, lze rozložit na součin prvočísel:

$$n = p_1 p_2 \cdots p_k$$

($p_1, p_2, \ldots, p_k$ jsou prvočísla, ne nutně navzájem různá).
Analogii pro konečné grupy dokážeme v následující větě.

7.1.6. Věta. *Nechť G je konečná grupa, $card(G) > 1$. Pak existuje kladné celé číslo k a nerozložitelné grupy $H_1, H_2, \ldots, H_k$ takové, že*

$$G \cong H_1 \times H_2 \times \cdots \times H_k.$$

Důkaz. Budeme postupovat indukcí vzhledem ke $card(G)$.

1. $card(G) = 2$
   Grupa G má řád 2 a 2 je prvočíslo. Takže G je nerozložitelná (viz 7.1.2.). Bude tedy $k = 1$ a $H_1 = G$.

2. $card(G) > 2$
   Jsou dvě možnosti:
   (I) G je nerozložitelná

(II) G je rozložitelná
ad (I): Položíme $k = 1$, $H_1 = G$.
ad(II): Existují grupy A, B takové, že $G \cong A \times B$, $A \neq \{1\}$, $B \neq \{1\}$. Je $card(G) = card(A) \cdot card(B)$, $card(A) > 1$, $card(B) > 1$. Zřejmě $card(A) < card(G)$, $card(B) < card(G)$. Dle indukčního předpokladu existuje kladné celé číslo r a nerozložitelné grupy $C_1, \ldots, C_r$ tak, že $A \cong C_1 \times \cdots \times C_r$. Dle indukčního předpokladu existuje kladné celé číslo s a nerozložitelné grupy $D_1, \ldots, D_s$ tak, že $B \cong D_1 \times \cdots \times D_s$. Pak

$$G \cong A \times B \cong C_1 \times \cdots \times C_r \times D_1 \times \cdots \times D_s.$$

Nyní stačí položit $k = r + s$, $H_1 = C_1, \ldots, H_r = C_r$,
$H_{r+1} = D_1, \ldots, H_{r+s} = H_k = D_s$.

V čem je význam věty 7.1.6.? V určitém smyslu lze říci: Kdybychom znali všechny nerozložitelné konečné grupy, pak bychom znali všechny konečné grupy. Jeden dosti speciální případ se nám podaří vyřešit v následující části tohoto studijního textu. Popíšeme všechny konečné nerozložitelné komutativní grupy a tím budeme vlastně znát všechny konečné komutativní grupy.

Vraťme se ještě k rozkladům přirozených čísel na součin prvočísel. Důležitou vlastností těchto rozkladů je jednoznačnost.
Nechť n je celé číslo, $n > 1$. Nechť k, l jsou kladná celá čísla, $p_1, \ldots, p_k$, $q_1, \ldots, q_l$ jsou prvočísla. Předpokládejme, že

$$n = p_1 \cdots p_k, \; n = q_1 \cdots q_l.$$

Pak $k = l$ a existuje permutace π množiny $\{1, \ldots, l\}$ tak, že $p_i = q_{\pi(i)}$ pro všechna $i \in \{1, \ldots, l\}$.

Naskýtá se přirozená otázka: Platí jednoznačnost také pro rozklad konečných grup na součin nerozložitelných grup? Kladnou odpověď dává následující Krullova - Schmidtova věta, kterou uvedeme bez důkazu. Větu lze vyslovit i v obecnějším znění, nikoli jen pro konečné grupy. Pro konečné grupy větu poprvé dokázal Remak v roce 1911.

7.1.7. Věta. (Krull - Schmidt) *Nechť G je konečná grupa, $card(G) > 1$. Nechť s, t jsou kladná celá čísla, $H_1, \ldots, H_s$, $K_1, \ldots, K_t$ jsou nerozložitelné grupy. Předpokládejme, že $G \cong H_1 \times \cdots \times H_s$, $G \cong K_1 \times \ldots K_t$. Pak $s = t$*

a existuje permutace π množiny $\{1,\dots,t\}$ tak, že $H_i \cong K_{\pi(i)}$ pro všechna $i \in \{1,\dots,t\}$.

Důkaz. Věta (v obecnějším znění, nikoli jen pro konečné grupy) je dokázána například v knize [4], kde se jedná o větu 6.36.

7.2 Popis všech konečných komutativních grup

Pokusíme se nyní získat popis všech konečných komutativních grup. Buď G konečná komutativní grupa, $card(G) > 1$. Podle věty 7.1.6. je $G \cong H_1 \times \cdots \times H_k$, kde $H_1,\dots,H_k$ jsou nerozložitelné grupy. Samozřejmě, grupy $H_1,\dots,H_k$ jsou také konečné a komutativní (viz 1.5.9.).

Lze tedy říci: Abychom popsali všechny konečné komutativní grupy, bude stačit, když popíšeme všechny konečné komutativní nerozložitelné grupy.

7.2.1. Tvrzení. *Nechť G je komutativní grupa řádu $m \cdot n$, kde m a n jsou celá čísla, $m > 1$, $n > 1$, m a n jsou nesoudělná. Pak grupa G je rozložitelná.*

Důkaz. Buď $H = \{x \in G |\ x^m = 1\}$, $K = \{x \in G |\ x^n = 1\}$.
Ukážeme, že H je podgrupa grupy G. Je třeba ukázat následující:
(I) $1 \in H$
(II) Jestliže $x \in H$, pak $x^{-1} \in H$.
(III) Jestliže $x, y \in H$, pak $xy \in H$.
ad (I): $1^m = 1$, takže $1 \in H$
ad (II): Nechť $x \in H$. Chceme: $x^{-1} \in H$. Víme, že $x^m = 1$. Pak $(x^{-1})^m = (x^m)^{-1} = 1^{-1} = 1$, takže $x^{-1} \in H$.
ad (III): Nechť $x, y \in H$. Chceme: $xy \in H$. Víme, že $x^m = 1$, $y^m = 1$. Pak $(xy)^m = x^m y^m = 1 \cdot 1 = 1$, takže $xy \in H$.
Obdobně lze dokázat, že také K je podgrupa grupy G. Protože G je komutativní, jsou podgrupy H a K normální. Nyní dokážeme, že $HK = G$. Inkluze $HK \subseteq G$ je zžejmá. Buď tedy $x \in G$. Potřebujeme, aby $x \in HK$. Protože čísla m, n jsou nesoudělná, existují celá čísla u, v taková, že $1 = um + vn$ (viz 2.2.4.). Pak

$$x = x^1 = x^{vn+um} = x^{vn} \cdot x^{um}.$$

Všimněme si, že $(x^{vn})^m = (x^v)^{mn} = 1$ (využili jsme 3.1.11.). Vidíme, že $x^{vn} \in H$. Dále, $(x^{um})^n = (x^u)^{mn} = 1$, což dává $x^{um} \in K$. Poněvadž $x = x^{vn} \cdot x^{um}$, $x^{vn} \in H$, $x^{um} \in K$, je $x \in HK$.

Nyní dokážeme, že $H \cap K = \{1\}$.
Buď $x \in H \cap K$. Chceme: $x = 1$. Protože $x \in H$, je $x^m = 1$. Protože $x \in K$, je $x^n = 1$. Použijeme opět rovnost $1 = um + vn$. Dostáváme

$$x = x^1 = x^{um+vn} = x^{um} \cdot x^{vn} = (x^m)^u \cdot (x^n)^v = 1^u \cdot 1^v = 1 \cdot 1 = 1.$$

Víme toto: H, K jsou normální podgrupy grupy G, $G = HK$, $H \cap K = \{1\}$. Podle věty 1.5.7. pak $G \cong H \times K$.
Zbývá ještě dokázat, že $H \neq \{1\}$, $K \neq \{1\}$.
Jelikož $m > 1$, existuje prvočíslo p, p dělí m. Buď q kladné celé číslo, $m = pq$. Je $card(G) = mn = pqn$, takže p dělí $card(G)$. Dle Cauchyovy věty (5.2.3.) existuje prvek $a \in G$, a má řád p. Jistě $a \neq 1$. Dále, $a^m = a^{pq} = (a^p)^q = 1^q = 1$, takže $a \in H$. Zjistili jsme, že $H \neq \{1\}$. Obdobně lze dokázat, že $K \neq \{1\}$.

Nechť G je konečná komutativní grupa, $card(G) > 1$. Nechť $card(G) = p_1^{k_1} \cdots p_s^{k_s}$, kde s je celé číslo, $s \geq 2$, $p_1, \ldots, p_s$ jsou navzájem různá prvočísla, $k_1 \ldots, k_s$ jsou kladná celá čísla. Položme $m = p_1^{k_1}$, $n = p_2^{k_2} \cdots p_s^{k_s}$. Pak m, n jsou celá čísla, $m > 1$, $n > 1$, m a n jsou nesoudělná, $card(G) = m \cdot n$. Podle tvrzení 7.2.1. je grupa G rozložitelná. Chceme-li, aby grupa G byla nerozložitelná, musí být $s = 1$. Tudíž, konečné komutativní nerozložitelné grupy musíme hledat mezi p-grupami (p je prvočíslo).

7.2.2. Tvrzení. *Nechť p je prvočíslo. Nechť G je komutativní p-grupa, která není cyklická. Pak grupa G je rozložitelná.*

Důkaz. Grupa G má řád p^n, kde n je kladné celé číslo. Specielně, $card(G) > 1$.
Každý prvek grupy G má řád p^l, kde l je celé číslo, $0 \leq l \leq n$ (viz 3.1.10.).
Buď $a \in G$ prvek, který má největší řád. Nechť tento řád je p^k. Je k celé číslo, $0 < k < n$ (případ $k = 0$ by dával $card(G) = 1$, případ $k = n$ by znamenal, že grupa G je cyklická).
Buď H podgrupa grupy G s těmito vlastnostmi:

1. $H \cap \langle a \rangle = \{1\}$
2. Pro libovolnou podgrupu K grupy G platí: Jestliže $K \cap \langle a \rangle = \{1\}$, pak $card(K) \leq card(H)$.

Nyní dokážeme pomocné tvrzení:
Nechť $x \in G$. Jestliže $x^p \in \langle a \rangle H$, pak $x \in \langle a \rangle H$.
Předpokládejme, že $x^p \in \langle a \rangle H$. Pak $x^p = a^r h$ pro nějaké celé číslo r a nějaké $h \in H$. Řád prvku x je roven p^m, kde m je celé číslo, $0 \leq m \leq k$. Pak $x^{p^k} = (x^{p^m})^{p^{k-m}} = 1^{p^{k-m}} = 1$. Platí:

$$1 = (x^p)^{p^{k-1}} = (a^r h)^{p^{k-1}} = (a^r)^{p^{k-1}} \cdot h^{p^{k-1}} = a^{rp^{k-1}} \cdot h^{p^{k-1}}.$$

Takže $a^{rp^{k-1}} = h^{-p^{k-1}}$. Je $a^{rp^{k-1}} \in \langle a \rangle$, $h^{-p^{k-1}} \in H$ (protože $h \in H$ a H je podgrupa). Pak $a^{rp^{k-1}} \in \langle a \rangle \cap H$, což dává $a^{rp^{k-1}} = 1$. Protože prvek a má řád p^k, máme p^k / rp^{k-1} (viz 1.2.13.). Tedy $r = ps$ pro nějaké celé číslo s. Dosazením dostáváme $h = x^p a^{-r} = x^p a^{-ps} = x^p (a^{-s})^p = (xa^{-s})^p$. Předpokládejme, že $xa^{-s} \in H$. Pak $x = a^s \cdot (xa^{-s}) \in \langle a \rangle H$. Předpokládejme tedy dále, že $xa^{-s} \notin H$. Položme $K = \langle xa^{-s} \rangle H$. Pak K je podgrupa grupy G (viz 1.4.20.). Jestliže $w \in H$, pak $w = 1 \cdot w \in \langle xa^{-s} \rangle H = K$. Takže $H \subseteq K$. Je $xa^{-s} = (xa^{-s}) \cdot 1 \in \langle xa^{-s} \rangle H = K$. Takže $H \neq K$. Pak $card(H) < card(K)$. Dle druhé podmínky z vymezení podgrupy H plyne, že $K \cap \langle a \rangle \neq \{1\}$. Existuje tedy prvek $y \in K \cap \langle a \rangle$, $y \neq 1$. Protože $y \in K$, existuje celé číslo t a prvek $w \in H$, $y = (xa^{-s})^t \cdot w$. Protože $y \in \langle a \rangle$, existuje celé číslo u, $y = a^u$. Předpokládejme, že $t = pt'$ (t' je celé číslo). Pak

$$(xa^{-s})^t = (xa^{-s})^{pt'} = (x^p a^{-sp})^{t'} = (x^p a^{-r})^{t'} \in H,$$

takže $y = (xa^{-s})^t \cdot w \in H$, $a^u \in H$. Jistě $a^u \in \langle a \rangle$, tudíž $a^u \in H \cap \langle a \rangle = \{1\}$, $a^u = 1$. Ovšem $y = a^u$, $y = 1$, spor. Nutně tedy $NSD(p, t) = 1$. Podle 2.2.4. existují celá čísla i, j splňující $ip + jt = 1$. Je

$$x = x^{ip+jt} = x^{ip} \cdot x^{jt} = (x^p)^i \cdot (x^t)^j.$$

Uvědomme si, že $\langle a \rangle H$ je podgrupa grupy G (viz 1.4.20.). Předpokládáme, že $x^p \in \langle a \rangle H$. Tudíž $(x^p)^i \in \langle a \rangle H$. Dále, $(xa^{-s})^t w = a^u$, $x^t a^{-st} w = a^u$, $x^t = a^{u+st} \cdot w^{-1} \in \langle a \rangle H$. Tudíž $(x^t)^j \in \langle a \rangle H$. Jelikož $x = (x^p)^i \cdot (x^t)^j$, máme $x \in \langle a \rangle H$. Důkaz pomocného tvrzení je ukončen.
Grupa G je komutativní, takže $\langle a \rangle$ a H jsou normální podgrupy grupy G.
Jistě $\langle a \rangle \cap H = \{1\}$.
Ukážeme, že $\langle a \rangle H = G$.
Inkluze $\langle a \rangle H \subseteq G$ je zřejmá.
Chceme: $G \subseteq \langle a \rangle H$. Buď $g \in G$ libovolný prvek. Pak $g^{p^n} = 1 \in \langle a \rangle H$ (viz 3.1.11.). Nyní opakovaně použijeme naše pomocné tvrzení. Je $(g^{p^{n-1}})^p \in$

$\langle a\rangle H$, takže $g^{p^{n-1}} \in \langle a\rangle H$. A tak dále, až $g^p \in \langle a\rangle H$ dává $g \in \langle a\rangle H$.
Podle věty 1.5.7. je $G \cong \langle a\rangle \times H$.
Zbývá dokázat, že $\langle a\rangle \neq \{1\}$, $H \neq \{1\}$. Předpokládejme, že $\langle a\rangle = \{1\}$. Pak $a = 1$, $G = \{1\}$, spor. Nutně tedy $\langle a\rangle \neq \{1\}$. Předpokládejme, že $H = \{1\}$. Pak $G \cong \langle a\rangle \times \{1\} \cong \langle a\rangle$. Tudíž grupa G je cyklická, spor. Nutně tedy $H \neq \{1\}$.

Nyní již máme k dispozici popis všech konečných komutativních nerozložitelných grup.

7.2.3. Věta. *Nechť G je konečná komutativní grupa, $card(G) > 1$. Pak G je nerozložitelná právě tehdy, když G je cyklická p-grupa pro nějaké prvočíslo p. Jinými slovy: G je nerozložitelná právě tehdy, když $G \cong \mathbb{Z}_{p^n}$ (p je prvočíslo, n je kladné celé číslo).*

Důkaz.

1. Předpokládejme, že G je nerozložitelná. Pro důkaz sporem předpokládejme, že G není cyklická p-grupa pro žádné prvočíslo p. Jsou dvě možnosti:
   (I) G není p-grupa pro žádné prvočíslo p
   (II) G je p-grupa pro nějaké prvočíslo p, avšak G není cyklická
   ad (I): Existují navzájem různá prvočísla $p_1, \ldots, p_s$ a kladná celá čísla $k_1, \ldots, k_s$ tak, že $card(G) = p_1^{k_1} \cdots p_s^{k_s}$. Protože G není p-grupa pro žádné prvočíslo p, je $s \geq 2$. Položme $m = p_1^{k_1}$, $n = p_2^{k_2} \cdots p_s^{k_s}$. Zřejmě m, n jsou celá čísla, $m > 1$, $n > 1$, $NSD(m, n) = 1$, $card(G) = m \cdot n$. Podle 7.2.1. je grupa G rozložitelná. Spor.
   ad (II): Dle 7.2.2. je G rozložitelná. Spor.

2. Předpokládejme, že G je cyklická p-grupa pro nějaké prvočíslo p. Nerozložitelnost grupy G jsme ukázali v příkladu 7.1.3.

A konečně nyní již máme k dispozici popis všech konečných komutativních grup.

7.2.4. Věta. *Nechť G je konečná komutativní grupa, $card(G) > 1$. Pak existuje kladné celé číslo k, prvočísla $p_1, \ldots, p_k$ (ne nutně různá), kladná celá čísla $n_1, \ldots, n_k$ tak, že*

$$G \cong \mathbb{Z}_{p_1^{n_1}} \times \mathbb{Z}_{p_2^{n_2}} \times \cdots \times \mathbb{Z}_{p_k^{n_k}}.$$

Důkaz. Podle věty 7.1.6. existuje kladné celé číslo k a nerozložitelné grupy $H_1, H_2, \ldots, H_k$ takové, že

$$G \cong H_1 \times H_2 \times \cdots \times H_k.$$

Protože G je konečná, jsou grupy $H_1, \ldots, H_k$ konečné. Protože G je komutativní, jsou grupy $H_1, \ldots, H_k$ komutativní (viz 1.5.9.). Podle věty 7.2.3. existují prvočísla p_i (pro $i \in \{1, \ldots, k\}$) a kladná celá čísla n_i tak, že $H_i \cong \mathbb{Z}_{p_i^{n_i}}$. Celkem pak

$$G \cong \mathbb{Z}_{p_1^{n_1}} \times \cdots \times \mathbb{Z}_{p_k^{n_k}}.$$

7.2.5. Poznámka.

1. V rozkladu konečné komutativní grupy G na součin cyklických p-grup, uvedeném ve větě 7.2.4., jsou činitelé určeni jednoznačně až na pořadí. Vyplývá to z věty Krullovy - Schmidtovy (7.1.7.) a z toho, že cyklické p-grupy jsou nerozložitelné (věta 7.2.3.).

2. Pro rozklad konečné komutativní grupy G uvedený ve větě 7.2.4. zřejmě platí
$$card(G) = p_1^{n_1} \cdot p_2^{n_2} \cdots p_k^{n_k}.$$
Chceme-li tedy najít všechny komutativní grupy řádu n, pak zapíšeme číslo n všemi možnými způsoby ve tvaru
$$n = p_1^{n_1} \cdot p_2^{n_2} \cdots p_k^{n_k},$$
kde $p_1, p_2, \ldots, p_k$ jsou prvočísla (ne nutně různá), $n_1, n_2, \ldots, n_k$ jsou kladná celá čísla. Přitom ovšem dva zápisy, které se liší pouze pořadím činitelů, považujeme za stejné.

7.2.6. Příklad. Uvedeme soupis všech komutativních grup řádu 1000. Použijeme větu 7.2.4. Máme tyto možnosti:
$1000 = 2 \cdot 2 \cdot 2 \cdot 5 \cdot 5 \cdot 5$, tomu odpovídá grupa $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_5 \times \mathbb{Z}_5 \times \mathbb{Z}_5$
$1000 = 2 \cdot 2 \cdot 2 \cdot 5 \cdot 25$, tomu odpovídá grupa $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_5 \times \mathbb{Z}_{25}$
$1000 = 2 \cdot 2 \cdot 2 \cdot 125$, tomu odpovídá grupa $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{125}$

$1000 = 2 \cdot 4 \cdot 5 \cdot 5 \cdot 5$, tomu odpovídá grupa $\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_5 \times \mathbb{Z}_5 \times \mathbb{Z}_5$
$1000 = 2 \cdot 4 \cdot 5 \cdot 25$, tomu odpovídá grupa $\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_5 \times \mathbb{Z}_{25}$
$1000 = 2 \cdot 4 \cdot 125$, tomu odpovídá grupa $\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_{125}$
$1000 = 8 \cdot 5 \cdot 5 \cdot 5$, tomu odpovídá grupa $\mathbb{Z}_8 \times \mathbb{Z}_5 \times \mathbb{Z}_5 \times \mathbb{Z}_5$
$1000 = 8 \cdot 5 \cdot 25$, tomu odpovídá grupa $\mathbb{Z}_8 \times \mathbb{Z}_5 \times \mathbb{Z}_{25}$
$1000 = 8 \cdot 125$, tomu odpovídá grupa $\mathbb{Z}_8 \times \mathbb{Z}_{125}$.
Existuje tedy celkem 9 komutativních grup řádu 1000.

7.2.7. Příklad. Uvedeme soupis všech komutativních grup řádu 2010. Použijeme větu 7.2.4. Je $2010 = 2{\cdot}3{\cdot}5{\cdot}67$, přičemž 2, 3, 5, 67 jsou prvočísla. Existuje tedy jediná komutativní grupa řádu 2010, a to grupa $\mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_{67}$. Samozřejmě, cyklická grupa $\mathbb{Z}_{2010}$ je také komutativní grupa řádu 2010. Proto $\mathbb{Z}_{2010} \cong \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_{67}$.

7.2.8. Příklad. Kolik existuje komutativních grup řádu 1000000?
Je $1000000 = 2^6 \cdot 5^6$. Postupujeme podle poznámky 7.2.5., část druhá. Číslo 2^6 lze zapsat těmito způsoby:

$$2^6,\ 2 \cdot 2^5,\ 2^2 \cdot 2^4,\ 2^3 \cdot 2^3,\ 2 \cdot 2 \cdot 2^4,\ 2 \cdot 2^2 \cdot 2^3,\ 2^2 \cdot 2^2 \cdot 2^2,$$

$$2 \cdot 2 \cdot 2 \cdot 2^3,\ 2 \cdot 2 \cdot 2^2 \cdot 2^2,\ 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2^2,\ 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2.$$

Způsobů je 11. Obdobně, číslo 5^6 lze také zapsat jedenácti způsoby. Počet všech zápisů čísla $2^6 \cdot 5^6$ je tedy $11 \cdot 11 = 121$.
Závěr: Existuje celkem 121 komutativních grup řádu 1000000.

7.3 Grupy malých řádů

V této části podáme úplný přehled všech grup až do řádu 11. Izomorfní grupy budeme, samozřejmě, považovat za stejné.

7.3.1. Tvrzení. *Existuje jediná grupa řádu* 2, *totiž grupa* $\mathbb{Z}_2$.

Důkaz. Tvrzení 4.1.6. pro $p = 2$.

7.3.2. Tvrzení. *Existuje jediná grupa řádu* 3, *totiž grupa* $\mathbb{Z}_3$.

Důkaz. Tvrzení 4.1.6. pro $p = 3$.

7.3.3. Tvrzení. *Existují právě dvě grupy řádu* 4, *totiž grupy* $\mathbb{Z}_4$ *a* $\mathbb{Z}_2 \times \mathbb{Z}_2$.

Důkaz. Příklad 3.1.14.

7.3.4. Tvrzení. *Existuje právě jedna grupa řádu* 5*, totiž grupa* $\mathbb{Z}_5$*.*

Důkaz. Tvrzení 4.1.6. pro $p = 5$.

7.3.5. Věta. *Nechť* p *je liché prvočíslo,* G *je grupa. Jestliže* G *má řád* $2p$*, pak* G *je cyklická nebo dihedrální (tj.* $G \cong \mathbb{Z}_{2p} \cong \mathbb{Z}_2 \times \mathbb{Z}_p$ *nebo* $G \cong D_{2p}$*).*

Důkaz. Podle Cauchyovy věty (5.2.3.) grupa G obsahuje nějaký prvek s řádu p a nějaký prvek t řádu 2. Podgrupa $\langle s\rangle$ má p prvků, $\langle s\rangle = \{1, s, \ldots, s^{p-1}\}$ (viz 1.4.18.).
Prvky $t, ts, \ldots, ts^{p-1}$ jsou navzájem různé. Předpokládejme opak, tj. $0 \leq i < j \leq p-1$, $ts^i = ts^j$. Pak $t^2s^i = t^2s^j$, $1 \cdot s^i = 1 \cdot s^j$, $s^i = s^j$, spor.
Předpokládejme nyní, že existují $i, j \in \{0, \ldots, p-1\}$ s vlastností $s^i = ts^j$. Pak $s^is^{-j} = ts^js^{-j}$, $s^{i-j} = ts^0$, $s^{i-j} = t$. Takže $t \in \langle s\rangle$. Protože řád prvku dělí řád grupy, $2/p$. To je spor.
Máme již dokázáno, že

$$1, s, \ldots, s^{p-1}, t, ts, \ldots, ts^{p-1}$$

jsou navzájem různé prvky. Jejich počet je $2p$, takže

$$G = \{1, s, \ldots, s^{p-1}, t, ts, \ldots, ts^{p-1}\}.$$

Je zřejmé, že $G = \langle s, t\rangle$.
Jistě $st \in G$. Jsou dvě možnosti:
(I) $st = s^i$ pro nějaké $i \in \{0, \ldots, p-1\}$
(II) $st = ts^i$ pro nějaké $i \in \{0, \ldots, p-1\}$.
ad (I): $st = s^i$, takže $s^{-1}st = s^{-1}s^i$, $t = s^{i-1}$, $t \in \langle s\rangle$, spor. Vidíme, že varianta (I) nenastává.
ad (II): $st = ts^i$, takže $tst = t^2s^i$, $tst = s^i$. Případ $i = 0$ dává $tst = 1$,

$ttstt = tt$, $s = 1$, spor. Tudíž $i \in \{1, \ldots, p-1\}$. Je

$$\begin{aligned}(tst)^i &= \underbrace{(tst)(tst)\cdots(tst)}_{i} \\ &= tst^2st^2\cdots t^2st \\ &= ts^it \\ &= t(tst)t \\ &= t^2st^2 \\ &= s.\end{aligned}$$

Ovšem také $(tst)^i = (s^i)^i = s^{i^2}$. Pak $s^{i^2} = s$, $s^{i^2}s^{-1} = ss^{-1}$, $s^{i^2-1} = 1$. Protože prvek s má řád p, máme p/i^2-1 (viz 1.2.13.). Tudíž $p/(i+1)\cdot(i-1)$. Jelikož p je prvočíslo, $p/i+1$ nebo $p/i-1$.
Nechť $p/i+1$.
Pak $i+1 = kp$ pro nějaké celé číslo k. Odtud $i = kp-1$,

$$s^i = s^{kp-1} = s^{kp}\cdot s^{-1} = (s^p)^k\cdot s^{-1} = 1^k\cdot s^{-1} = 1\cdot s^{-1} = s^{-1}.$$

Pak $tst = s^{-1}$. Shrňme si, co víme: G je grupa řádu $2p$, $\langle s,t\rangle = G$, $s^p = 1$, $t^2 = 1$, $tst = s^{-1}$. Dle definice 2.6.9. je $G \cong D_{2p}$.
Nechť $p/i-1$.
Pak $i-1 = kp$ pro nějaké celé číslo k. Odtud $i = kp+1$,

$$s^i = s^{kp+1} = s^{kp}\cdot s = (s^p)^k\cdot s = 1^k\cdot s = 1\cdot s = s.$$

Pak $tst = s$, $tst^2 = st$, $ts = st$. Protože prvky grupy G jsou tvaru t^as^b, kde $a \in \{0,1\}$, $b \in \{0,\ldots,p-1\}$, lze snadno nahlédnout, že grupa G je komutativní. V příkladu 5.2.5. jsme ukázali, že $G \cong \mathbb{Z}_{2p} \cong \mathbb{Z}_2 \times \mathbb{Z}_p$.

7.3.6. Tvrzení. *Existují právě dvě grupy řádu* 6, *totiž* $\mathbb{Z}_6 \cong \mathbb{Z}_2 \times \mathbb{Z}_3$ *a* $D_6 \cong S_3$.

Důkaz. Viz 7.3.5. pro $p = 3$. Označme Δ množinu vrcholů rovnostranného trojúhelníka. Je $D_6 \cong Sym(\Delta)$ (viz 2.6.11.). Ovšem $Sym(\Delta) = S(\Delta) \cong S_3$ (viz 2.6.5.). Takže $D_6 \cong S_3$. Grupy $\mathbb{Z}_6$ a S_3 nejsou izomorfní, protože $\mathbb{Z}_6$ je komutativní a S_3 není komutativní.

7.3.7. Tvrzení. *Existuje jediná grupa řádu* 7, *totiž grupa* $\mathbb{Z}_7$.

Důkaz. Tvrzení 4.1.6. pro $p = 7$.

7.3.8. Tvrzení. *Nechť G je grupa. Jestliže $a^2 = 1$ pro každé $a \in G$, pak G je komutativní.*

Důkaz. Nechť $x, y \in G$. Pak $(xy)^2 = 1$, $xyxy = 1$, $x(xyxy)y = x \cdot 1 \cdot y$, $x^2yxy^2 = xy$, $1 \cdot yx \cdot 1 = xy$, $yx = xy$.

7.3.9. Tvrzení. *Nechť G je grupa řádu 8. Jestliže G není komutativní, pak $G \cong \mathbf{Q}$ nebo $G \cong D_8$.*

Důkaz. Buď G nekomutativní grupa řádu 8. Řád prvku dělí řád grupy (3.1.10.), takže každý prvek grupy G má řád 1 (takový prvek existuje právě jeden, totiž 1), 2, 4, nebo 8. Kdyby grupa G měla nějaký prvek řádu 8, byla by $G \cong \mathbb{Z}_8$ (dle 4.1.5.), tedy G by byla komutativní, což by byl spor. Tudíž každý prvek grupy G má řád 1, 2 nebo 4. Předpokládejme, že v grupě G neexistuje žádný prvek řádu 4. Pak pro každé $a \in G$ je $a^2 = 1$ a podle 7.3.8. je G komutativní. To je spor. Dosavadní pozorování shrneme takto:
Každý prvek grupy G má řád 1, 2 nebo 4, přičemž aspoň jeden prvek má řád 4.
Buď $a \in G$, a má řád 4. Podgrupa $\langle a \rangle$ má řád 4, $\langle a \rangle = \{1, a, a^2, a^3\}$.
Nechť $b \in G$, $b \notin \langle a \rangle$.
Prvky b, ba, ba^2, ba^3 jsou navzájem různé. Předpokládejme opak. Pak existují $0 \leq i < j \leq 3$, $ba^i = ba^j$. Z toho však plyne $a^i = a^j$, což je spor.
Předpokládejme, že $i, j \in \{0, 1, 2, 3\}$, $a^i = ba^j$. Pak $a^i a^{-j} = ba^j a^{-j}$, $a^{i-j} = ba^{j-j}$, $a^{i-j} = ba^0$, $a^{i-j} = b \cdot 1$, $a^{i-j} = b$. Tudíž $b \in \langle a \rangle$, spor.
Ukázali jsme, že prvky 1, a, a^2, a^3, b, ba, ba^2, ba^3 jsou navzájem různé. Protože těchto prvků je 8 a $card(G) = 8$, je

$$G = \{1, a, a^2, a^3, b, ba, ba^2, ba^3\}.$$

Všimněme si, že $\langle a, b \rangle = G$.
Předpokládejme, že $b^2 = ba^i$ pro nějaké $i \in \{0, 1, 2, 3\}$. Pak $b = a^i$ (využili jsme zákon o krácení), $b \in \langle a \rangle$, spor. Nutně tedy $b^2 \in \{1, a, a^2, a^3\}$. Teoreticky tedy máme 4 možnosti:
(I) $b^2 = 1$
(II) $b^2 = a$
(III) $b^2 = a^2$
(IV) $b^2 = a^3$.

ad (I): Předpokládejme, že $bab = ba^i$ pro nějaké $i \in \{0,1,2,3\}$. Pak $ab = a^i$ (použili jsme zákon o krácení), $a^{-1}ab = a^{-1}a^i$, $b = a^{i-1}$, $b \in \langle a \rangle$, spor. Nutně tedy $bab \in \{1, a, a^2, a^3\}$.
Případ $bab = 1$ dává $b(bab)b = b \cdot 1 \cdot b$, $b^2ab^2 = b^2$, $1 \cdot a \cdot 1 = 1$, $a = 1$, což není pravda.
Případ $bab = a$ dává $bbab = ba$, $b^2ab = ba$, $1 \cdot ab = ba$, $ab = ba$. Prvky grupy G mají tvar b^ia^j, kde $i \in \{0,1\}$, $j \in \{0,1,2,3\}$. Z $ab = ba$ tudíž plyne, že G je komutativní. To však není pravda.
Případ $bab = a^2$ dává $(bab)^2 = (a^2)^2$, $babbab = a^4$, $bab^2ab = 1$, $baab = 1$, $ba^2b = 1$, $b(ba^2b)b = b \cdot 1 \cdot b$, $b^2a^2b^2 = b^2$, $1 \cdot a^2 \cdot 1 = 1$, $a^2 = 1$, což není pravda.
Musí tedy být $bab = a^3$. Jelikož $a^4 = 1$, je $a^3 = a^{-1}$.
Zjistili jsme, že v případě (I) platí: $\langle a, b \rangle = G$, $a^4 = 1$, $b^2 = 1$, $bab = a^{-1}$. Podle definice 2.6.9. je $G \cong D_8$.
ad (II): Je $b \neq 1$, $b^2 \neq 1$. Protože b má řád 1, 2 nebo 4, musí být $b^4 = 1$. Pak ovšem $a^2 = (b^2)^2 = b^4 = 1$, spor. Vidíme, že případ (II) vůbec nenastává.
ad (III): Je $b^4 = (b^2)^2 = (a^2)^2 = a^4 = 1$.
Předpokládejme, že $bab^3 = ba^i$ pro nějaké $i \in \{0,1,2,3\}$. Pak $ab^3 = a^i$ (použili jsme zákon o krácení), $a^{-1}ab^3 = a^{-1}a^i$, $b^3 = a^{i-1}$, $bb^2 = a^{i-1}$, $ba^2 = a^{i-1}$, $ba^2a^{-2} = a^{i-1}a^{-2}$, $b = a^{i-3}$, $b \in \langle a \rangle$, spor. Nutně tedy $bab^3 \in \{1, a, a^2, a^3\}$.
Případ $bab^3 = 1$ dává $bab^3b = 1 \cdot b$, $bab^4 = b$, $ba \cdot 1 = b$, $ba = b \cdot 1$, $a = 1$ (použili jsme zákon o krácení), což není pravda.
Případ $bab^3 = a$ dává $bab^3b = ab$, $bab^4 = ab$, $ba \cdot 1 = ab$, $ba = ab$. Tudíž G je komutativní. Tao však není pravda.
Případ $bab^3 = a^2$ dává $bab^3b = a^2b$, $bab^4 = b^2b$, $ba \cdot 1 = bb^2$, $ba = ba^2$, $a = a^2$, $1 = a$, což není pravda.
Musí tedy být $bab^3 = a^3$. Jelikož $a^4 = 1$, je $a^3 = a^{-1}$. Jelikož $b^4 = 1$, je $b^3 = b^{-1}$.
Zjistili jsme, že v případě (III) platí: $\langle a, b \rangle = G$, $a^4 = 1$, $b^2 = a^2$, $bab^{-1} = a^{-1}$. Podle definice 2.7.1. je $G \cong \mathbf{Q}$.
ad (IV): Je $b \neq 1$, $b^2 \neq 1$. Protože b má řád 1, 2 nebo 4, musí být $b^4 = 1$. Pak ovšem $a^6 = (a^3)^2 = (b^2)^2 = b^4 = 1$, $a^4a^2 = 1$, $1 \cdot a^2 = 1$, $a^2 = 1$, spor. Vidíme, že případ (IV) vůbec nenastává.

7.3.10. Tvrzení. *Existuje právě pět grup řádu* 8, *totiž* $\mathbb{Z}_8$, $\mathbb{Z}_2 \times \mathbb{Z}_4$, $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, $\mathbf{Q}$ *a* D_8.

Důkaz. Všechny uvedené grupy mají řád 8. Ukážeme, že jsou navzájem neizomorfní.

Nejdříve se zabývejme komutativními grupami. Pro každé $x \in \mathbb{Z}_4$ je $4x = \overline{0}$ (viz 3.1.11.). Obdobně, pro každé $x \in \mathbb{Z}_2$ je $2x = \overline{0}$, $4x = 2(2x) = 2\overline{0} = \overline{0}$. Grupa $\mathbb{Z}_8$ má prvek řádu 8, například je to $\overline{1}$. Pro každé $(a, b) \in \mathbb{Z}_2 \times \mathbb{Z}_4$ je $4(a, b) = (4a, 4b) = (\overline{0}, \overline{0})$, takže každý prvek grupy $\mathbb{Z}_2 \times \mathbb{Z}_4$ má řád nejvýše 4. Tudíž v $\mathbb{Z}_2 \times \mathbb{Z}_4$ neexistuje prvek řádu 8, $\mathbb{Z}_8$ a $\mathbb{Z}_2 \times \mathbb{Z}_4$ nejsou izomorfní. Pro každé $(a, b, c) \in \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ je $2(a, b, c) = (2a, 2b, 2c) = (\overline{0}, \overline{0}, \overline{0})$, takže každý prvek grupy $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ má řád nejvýše 2. Tudíž v $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ neexistuje prvek řádu 8, $\mathbb{Z}_8$ a $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ nejsou izomorfní. Grupa $\mathbb{Z}_2 \times \mathbb{Z}_4$ má prvek řádu 4, například $(\overline{0}, \overline{1})$. Viděli jsme již, že každý prvek grupy $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ má řád nejvýše 2. Tudíž grupy $\mathbb{Z}_2 \times \mathbb{Z}_4$ a $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ nejsou izomorfní.
Zabývejme se nyní nekomutativními grupami, tedy grupami $\mathbf{Q}$ a D_8. Grupa $\mathbf{Q}$ má právě jeden prvek řádu 2, totiž prvek -1. Grupa D_8 má aspoň dva prvky řádu 2, například to jsou prvky t a s^2. Tudíž grupy $\mathbf{Q}$ a D_8 nejsou izomorfní.
Zbývá ještě dokázat, že každá grupa G řádu 8 je izomorfní jedné z pěti uvedených grup.
Jestliže G je komutativní, pak $G \cong \mathbb{Z}_8$ nebo $G \cong \mathbb{Z}_2 \times \mathbb{Z}_4$ nebo $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ na základě věty 7.2.4.
Jestliže G není komutativní, pak $G \cong \mathbf{Q}$ nebo $G \cong D_8$ na základě tvrzení 7.3.9.

7.3.11. Věta. *Nechť p je prvočíslo. Existují právě dvě grupy řádu p^2, totiž grupy $\mathbb{Z}_{p^2}$ a $\mathbb{Z}_p \times \mathbb{Z}_p$.*

Důkaz. Buď G grupa řádu p^2. Víme, že G je komutativní (viz 5.3.7.). Podle 7.2.4. je $G \cong \mathbb{Z}_{p^2}$ nebo $G \cong \mathbb{Z}_p \times \mathbb{Z}_p$. Pro každé $x \in \mathbb{Z}_p$ je $px = \overline{0}$ (viz 3.1.11.). Buď $(a, b) \in \mathbb{Z}_p \times \mathbb{Z}_p$. Pak $p(a, b) = (pa, pb) = (\overline{0}, \overline{0})$. Vidíme, že každý prvek grupy $\mathbb{Z}_p \times \mathbb{Z}_p$ má řád nejvýše p. Pak ovšem grupy $\mathbb{Z}_{p^2}$ a $\mathbb{Z}_p \times \mathbb{Z}_p$ nejsou izomorfní, jelikož grupa $\mathbb{Z}_{p^2}$ obsahuje prvek řádu p^2, například je to prvek $\overline{1}$.

7.3.12. Tvrzení. *Existují právě dvě grupy řádu 9, totiž grupy $\mathbb{Z}_9$ a $\mathbb{Z}_3 \times \mathbb{Z}_3$.*

Důkaz. Věta 7.3.11. pro $p = 3$.

7.3.13. Tvrzení. *Existují právě dvě grupy řádu 10, totiž grupy $\mathbb{Z}_{10} \cong \mathbb{Z}_2 \times \mathbb{Z}_5$ a D_{10}.*

Důkaz. Věta 7.3.5. pro $p = 5$. Grupy $\mathbb{Z}_{10}$ a D_{10} nejsou izomorfní, neboť $\mathbb{Z}_{10}$ je komutativní a D_{10} není komutativní.

7.3.14. Tvrzení. *Existuje jediná grupa řádu* 11*, totiž grupa* $\mathbb{Z}_{11}$*.*

Důkaz. Tvrzení 4.1.6. pro $p = 11$.

Nyní již můžeme podat úplný přehled všech grup řádu 1 až 11. Tento přehled je obsahem následující věty.

7.3.15. Věta. *Existuje celkem* 19 *grup řádu* 1 *až* 11*. Jsou to následující grupy:*

1. *grupy řádu* 1*:* $\{1\}$
2. *grupy řádu* 2*:* $\mathbb{Z}_2$
3. *grupy řádu* 3*:* $\mathbb{Z}_3$
4. *grupy řádu* 4*:* $\mathbb{Z}_4$, $\mathbb{Z}_2 \times \mathbb{Z}_2$
5. *grupy řádu* 5*:* $\mathbb{Z}_5$
6. *grupy řádu* 6*:* $\mathbb{Z}_6 \cong \mathbb{Z}_2 \times \mathbb{Z}_3$, $D_6 \cong S_3$
7. *grupy řádu* 7*:* $\mathbb{Z}_7$
8. *grupy řádu* 8*:* $\mathbb{Z}_8$, $\mathbb{Z}_2 \times \mathbb{Z}_4$, $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, $\mathbf{Q}$, D_8
9. *grupy řádu* 9*:* $\mathbb{Z}_9$, $\mathbb{Z}_3 \times \mathbb{Z}_3$
10. *grupy řádu* 10*:* $\mathbb{Z}_{10} \cong \mathbb{Z}_2 \times \mathbb{Z}_5$, D_{10}
11. *grupy řádu* 11*:* $\mathbb{Z}_{11}$*.*

Důkaz. Tvrzení 7.3.1., 7.3.2., 7.3.3., 7.3.4., 7.3.6., 7.3.7., 7.3.10., 7.3.12., 7.3.13., 7.3.14.

7.3.16. Příklad. Určíme všechny grupy řádů 121 a 122.
Je $121 = 11^2$ a 11 je prvočíslo. Podle věty 7.3.11. existují právě dvě grupy řádu 121, a to grupy $\mathbb{Z}_{121}$ a $\mathbb{Z}_{11} \times \mathbb{Z}_{11}$.

Je $122 = 2 \cdot 61$ a 61 je prvočíslo. Na základě věty 7.3.5. existují právě dvě grupy řádu 122, a to grupy $\mathbb{Z}_{122} \cong \mathbb{Z}_2 \times \mathbb{Z}_{61}$ a D_{122}.

Na závěr se ještě zmíníme o funkci $\mathcal{G}(n)$. Pro kladné celé číslo n definujeme $\mathcal{G}(n)$ jako počet všech navzájem neizomorfních grup řádu n. V tabulce jsou uvedeny hodnoty $\mathcal{G}(n)$ pro některá n. Uvedené hodnoty lze nalézt v knize [4] na stranách 85 a 86.

n	$\mathcal{G}(n)$
1	1
2	1
3	1
4	2
5	1
6	2
7	1
8	5
9	2
10	2
11	1
12	5
13	1
14	2
15	1
16	14
17	1
18	5
19	1
20	5
21	2
22	2
23	1
24	15
25	2
26	2
27	5
28	4
29	1
30	4
31	1
32	51
64	267
128	2328
256	56092

OKRUHY

8 Základní pojmy teorie okruhů

8.1 Definice okruhu

Grupa je algebraická struktura s jednou binární operací. Začneme se nyní zabývat strukturami se dvěma binárními operacemi. Zopakujeme tři definice, které jsme uvedli již v části 2.1.

8.1.1. Definice. Okruh je množina spolu se dvěma binárními operacemi, většinou zvanými sčítání a násobení, přičemž vzhledem ke sčítání se jedná o komutativní grupu a násobení je distributivní vzhledem ke sčítání. Okruh se nazývá **asociativní** (**komutativní**, **s jednotkovým prvkem**), pokud operace násobení je asociativní (komutativní, má neutrální prvek).

8.1.2. Definice. Obor integrity je asociativní a komutativní okruh, v němž pro každé dva prvky x, y platí:
Jestliže $x \cdot y = 0$, pak $x = 0$ nebo $y = 0$.

8.1.3. Definice. Těleso je aspoň dvouprvkový asociativní okruh s jednotkovým prvkem (označme jej 1), v němž pro každý nenulový prvek x existuje prvek y takový, že $x \cdot y = y \cdot x = 1$. Prvek y se značí x^{-1} nebo $\frac{1}{x}$. Značení je možno zavést, neboť prvek y je určen jednoznačně (nechť $x \cdot z = z \cdot x = 1$; pak $y = y \cdot 1 = y \cdot (x \cdot z) = (y \cdot x) \cdot z = 1 \cdot z = z$). Je-li v tělese násobení komutativní, pak hovoříme o **komutativním tělese**. Protože v tomto textu budeme pracovat výhradně s komutativními tělesy, budeme pro stručnost místo názvu komutativní těleso používat pouze slovo těleso.

Nechť R je okruh. Z definice okruhu víme, že množina R spolu s operací sčítání je komutativbní grupa. Tuto grupu nazýváme **aditivní grupa okruhu** R.

Číselné množiny $\mathbb{S}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ spolu s operacemi sčítání a násobení jsou komutativní asociativní okruhy. Přitom $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ jsou okruhy s jednotkovým prvkem. Dokonce $\mathbb{Z}$ je obor integrity a $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ jsou tělesa. Také pro každé kladné celé číslo m je $\mathbb{Z}_m$ komutativní asociativní okruh s jednotkovým prvkem (viz 2.1.8.). Celá následující kapitola tohoto studijního textu je věnována příkladům okruhů.

Při počítání v okruzích budeme dávat operaci násobení přednost před operací sčítání. Jinak řečeno, $(x \cdot y) + z$ budeme většinou zapisovat zkráceně jako $x \cdot y + z$ či pouze jako $xy + z$ (pro libovolné prvky x, y, z daného okruhu).

Podobně, $-(x \cdot y)$ budeme většinou zapisovat zkráceně jako $-x \cdot y$ či pouze jako $-xy$.

Následující tvrzení obsahuje základní pravidla pro počítání v okruzích. Tato pravidla budeme potom používat zcela běžně, bez dalšího vysvětlování.

8.1.4. Tvrzení. *Nechť R je okruh. Pro všechna $x, y \in R$ platí:*

1. $x \cdot 0 = 0 \cdot x = 0$
2. $x \cdot (-y) = (-x) \cdot y = -(x \cdot y)$
3. $(-x) \cdot (-y) = x \cdot y$

Důkaz.

1. Počítejme: $x \cdot 0 + 0 = x \cdot 0 = x \cdot (0 + 0) = x \cdot 0 + x \cdot 0$. Takže $x \cdot 0 + 0 = x \cdot 0 + x \cdot 0$. Použijeme zákon o krácení v aditivní grupě okruhu R a dostaneme $0 = x \cdot 0$. Obdobně lze dokázat vztah $0 \cdot x = 0$.
2. Je třeba ukázat, že $x \cdot (-y) + x \cdot y = 0$ a $(-x) \cdot y + x \cdot y = 0$. Počítejme:
   $x \cdot (-y) + x \cdot y = x \cdot ((-y) + y) = x \cdot 0 = 0$
   $(-x) \cdot y + x \cdot y = ((-x) + x) \cdot y = 0 \cdot y = 0$
   Při výpočtu jsme použili již dokázanou první část tvrzení.
3. Počítejme: $(-x) \cdot (-y) = -(x \cdot (-y)) = -(-(x \cdot y)) = x \cdot y$. Při výpočtu jsme použili dvakrát již dokázanou druhou část tvrzení.

Učiníme ještě jednu úmluvu týkající se značení. Nechť x, y jsou prvky nějakého okruhu. Pak zápis $x - y$ bude zkratkou za zápis $x + (-y)$.

8.1.5. Tvrzení. *Nechť R je okruh, $x, y, z \in R$. Pak platí:*

1. $x(y - z) = xy - xz$, $(x - y)z = xz - yz$
2. $x - y = 0$ *právě tehdy, když* $x = y$.

Důkaz.

1. Z distributivity násobení vzhledem ke sčítání dostaneme

   $$x(y-z) = x(y+(-z)) = xy+x(-z) = xy+(-(xz)) = xy+(-xz) = xy-xz$$

   Podobně je možno dokázat rovnost $(x-y)z = xz - yz$.

2. Nechť nejprve $x - y = 0$. Pak $x + (-y) = 0$, $(x + (-y)) + y = 0 + y$, $x + ((-y) + y) = y$, $x + 0 = y$, $x = y$.
   Nechť nyní $x = y$. Pak $x + (-y) = y + (-y)$, $x - y = 0$.

Víme, že v grupě platí zákony o krácení (viz 1.1.6.). Nechť R je okruh, $x, y, z \in R$. Platí tedy: jestliže $x + y = x + z$, pak $y = z$.

Jeden ze zákonů o krácení pro operaci násobení by dával: jestliže $xy = xz$, pak $y = z$.

Takové pravidlo však neplatí v žádném okruhu s aspoň dvěma prvky. Je-li totiž R okruh s aspoň dvěma prvky, pak existují $y, z \in R$, $y \neq z$, přitom však $0 \cdot y = 0 = 0 \cdot z$.

Zdá se, že pomoci by mohl předpoklad nenulovosti prvku x (tedy prvku, kterým krátíme). Ani to však nestačí. Buď R komutativní asociativní okruh, který není oborem integrity. Existují tedy $x, y \in R$, $xy = 0$, $x \neq 0$, $y \neq 0$. Pak $x \cdot y = x \cdot 0$ (oba součiny mají hodnotu 0), $x \neq 0$, a přitom $y \neq 0$. Takže zákon o krácení nenulovým prvkem (pro operaci násobení) neplatí v R.

V oborech integrity však již zákon o krácení nenulovým prvkem platí.

8.1.6. Tvrzení. (zákon o krácení nenulovým prvkem) *Nechť R je obor integrity, $x, y, z \in R$. Jestliže $xy = xz$ a $x \neq 0$, pak $y = z$.*

Důkaz. Nechť $xy = xz$, $x \neq 0$. Pak $xy - xz = 0$, $x(y - z) = 0$. Protože R je obor integrity, máme $x = 0$ nebo $y - z = 0$. Ovšem $x \neq 0$, takže $y - z = 0$. Pak $y = z$.

Vyjasníme nyní vztah mezi okruhy, obory integrity a tělesy.

8.1.7. Tvrzení.

1. *Každé těleso je aspoň dvouprvkový obor integrity s jednotkovým prvkem.*

2. Každý obor integrity je komutativní asociativní okruh.

Důkaz.

1. Nechť T je těleso. Z definice tělesa ihned vyplývá, že T je aspoň dvouprvkový asociativní a komutativní okruh s jednotkovým prvkem. Zbývá ukázat, že pro všechna $x, y \in T$ platí: jestliže $xy = 0$, pak $x = 0$ nebo $y = 0$. Nechť $x, y \in T$, $xy = 0$. V případě $x = 0$ jsme hotovi. Buď tedy $x \neq 0$. Uvědomme si, že v T existuje prvek x^{-1}. Protože $xy = 0$, je $x^{-1} \cdot (xy) = x^{-1} \cdot 0$, $(x^{-1} \cdot x)y = 0$, $1 \cdot y = 0$, $y = 0$.

2. Tvrzení plyne ihned z definice oboru integrity.

Následující poznámku lze chápat jako doplněk Tvrzení 8.1.7.

8.1.8. Poznámka.

1. Existuje těleso, například $\mathbb{Q}$.

2. Existuje nějaký aspoň dvouprvkový obor integrity s jednotkovým prvkem, který není těleso. Je to například obor integrity $\mathbb{Z}$.

3. Existuje komutativní asociativní okruh, který není obor integrity. Je to například okruh $\mathbb{Z}_6$. Dle 2.1.6. množina $\mathbb{Z}_6$ má přesně 6 prvků, totiž $\overline{0}$, $\overline{1}$, $\overline{2}$, $\overline{3}$, $\overline{4}$, $\overline{5}$. Dle 2.1.8. $\mathbb{Z}_6$ je komutativní asociativní okruh s jednotkovým prvkem $\overline{1}$. Přitom $\overline{2} \neq \overline{0}$, $\overline{3} \neq \overline{0}$, $\overline{2} \cdot \overline{3} = \overline{2 \cdot 3} = \overline{6} = \overline{0}$, takže $\mathbb{Z}_6$ není obor integrity.

4. Existuje algebraická struktura se dvěma binárními operacemi, která není okruh. Je to například množina $\mathbb{N}$ s operacemi sčítání a násobení. Zdůvodnění: Předpokládejme, že operace sčítání na množině $\mathbb{N}$ má neutrální prvek e. Pak $e + e = e$, což dává $e = 0$, takže $0 \in \mathbb{N}$, spor. Tudíž operace sčítání na množině $\mathbb{N}$ nemá neutrální prvek a tedy $\mathbb{N}$ s operací sčítání není grupa. Operace násobení na množině $\mathbb{N}$ má neutrální prvek 1. Předpokládejme, že množina $\mathbb{N}$ s operací násobení je grupa. Pak k číslu 2 existuje prvek inverzní, neboli existuje přirozené číslo x takově, že $2x = 1$. Takže 1 je sudé číslo, spor. Tudíž $\mathbb{N}$ s operací násobení není grupa. Protože množina $\mathbb{N}$ není grupa ani s operací sčítání, ani s operací násobení, není $\mathbb{N}$ okruh.

Třídu všech těles označme $\mathbf{T}$, třídu všech oborů integrity označme $\mathbf{I}$, třídu všech okruhů označme $\mathbf{R}$ a třídu všech algebraických struktur se dvěma binárními operacemi označme $\mathbf{A}$. Z 8.1.7. a 8.1.8. dostáváme:

$$\emptyset \neq \mathbf{T} \subset \mathbf{I} \subset \mathbf{R} \subset \mathbf{A}$$

$$\mathbb{Q} \in \mathbf{T},\ \mathbb{Z} \in \mathbf{I} - \mathbf{T},\ \mathbb{Z}_6 \in \mathbf{R} - \mathbf{I},\ \mathbb{N} \in \mathbf{A} - \mathbf{R}.$$

Je zajímavé, že pro konečné obory integrity obrácením první části Tvrzení 8.1.7. dostáváme pravdivý výrok. Platí totiž

8.1.9. Tvrzení. *Každý konečný aspoň dvouprvkový obor integrity s jednotkovým prvkem je těleso.*

Důkaz. Nechť I je konečný obor integrity s jednotkovým prvkem, $card(I) = n$, n je celé číslo, $n \geq 2$. Z definice oboru integrity plyne, že I je asociativní a komutativní okruh. Zbývá ukázat, že pro každé $x \in I$, $x \neq 0$, existuje $y \in I$, $xy = 1$. Nechť $I = \{a_1, a_2, \ldots, a_n\}$. Zvolme libovolně $x \in I$, $x \neq 0$, a uvažme množinu $J = \{xa_1, xa_2, \ldots, xa_n\}$. Zřejmě $J \subseteq I$. Ukážeme, že $card(J) = n$. Zřejmě $card(J) \leq n$. Předpokládejme, že $card(J) \neq n$. Pak existují $k, l \in \{1, 2, \ldots, n\}$, $k \neq l$, $xa_k = xa_l$. Zákon o krácení nenulovým prvkem dává $a_k = a_l$. Pak ovšem $card(I) < n$, spor. Nutně tedy $card(J) = n$. Shrňme to, co již víme: $card(I) = n$, $J \subseteq I$, $card(J) = n$. Z toho plyne, že $J = I$. Je $1 \in I$, takže $1 \in J$. Pak ovšem $1 = xa_p$ pro nějaké $p \in \{1, 2, \ldots, n\}$. Stačí položit $y = a_p$.

8.2 Homomorfismy

8.2.1. Definice. Nechť R_1, R_2 jsou okruhy, $\varphi : R_1 \to R_2$. Zobrazení φ se nazývá **homomorfismus** okruhu R_1 do okruhu R_2, pokud pro všechna $x, y \in R_1$ platí

$$\varphi(x + y) = \varphi(x) + \varphi(y),\ \varphi(x \cdot y) = \varphi(x) \cdot \varphi(y).$$

Všimněme si, že homomorfismus okruhu R_1 do okruhu R_2 je také homomorfismus aditivní grupy okruhu R_1 do aditivní grupy okruhu R_2. Jak ukazuje následující příklad, opak platit nemusí.

8.2.2. Příklad. Nechť $\varphi : \mathbb{Z} \to \mathbb{S}$, $\varphi(x) = 4x$ pro všechna $x \in \mathbb{Z}$. Pro libovolná $x, y \in \mathbb{Z}$ je $\varphi(x+y) = 4(x+y) = 4x+4y = \varphi(x)+\varphi(y)$, takže φ je homomorfismus aditivní grupy okruhu $\mathbb{Z}$ do aditivní grupy okruhu $\mathbb{S}$. Avšak φ není homomorfismus okruhu $\mathbb{Z}$ do okruhu $\mathbb{S}$, protože například $\varphi(2 \cdot 3) = \varphi(6) = 4 \cdot 6 = 24$, $\varphi(2) \cdot \varphi(3) = (4 \cdot 2) \cdot (4 \cdot 3) = 8 \cdot 12 = 96$.

8.2.3. Příklad. Nechť m je kladné celé číslo, $\varphi : \mathbb{Z} \to \mathbb{Z}_m$, $\varphi(x) = \overline{x}$ pro všechna $x \in \mathbb{Z}$. Pro libovolná $x, y \in \mathbb{Z}$ je

$$\varphi(x+y) = \overline{x+y} = \overline{x} + \overline{y} = \varphi(x) + \varphi(y)$$

$$\varphi(x \cdot y) = \overline{x \cdot y} = \overline{x} \cdot \overline{y} = \varphi(x) \cdot \varphi(y)$$

a tedy φ je homomorfismus okruhu $\mathbb{Z}$ na okruh $\mathbb{Z}_m$ (zobrazení φ je surjektivní, jak ihned vidíme z rovnosti $\mathbb{Z}_m = \{\overline{0}, \overline{1} \ldots, \overline{m-1}\}$ - viz 2.1.6.).

8.2.4. Příklad. Nechť R_1, R_2 jsou okruhy. Definujme zobrazení $\varphi : R_1 \to R_2$ předpisem $\varphi(x) = 0$ pro všechna $x \in R_1$. Pak φ je homomorfismus, jak se lze snadno přesvědčit. Tento homomorfismus φ nazýváme **nulový** (nebo také **triviální**), ostatní homomorfismy jsou **nenulové** (**netriviální**).

8.2.5. Tvrzení. *Nechť R_1 je okruh s jednotkovým prvkem, R_2 je okruh, $\varphi : R_1 \to R_2$ je homomorfismus. Platí: homomorfismus φ je nulový právě tehdy, když $\varphi(1) = 0$.*

Důkaz. Jestliže φ je nulový, pak jistě $\varphi(1) = 0$. Naopak, nechť $\varphi(1) = 0$. Ukážeme, že φ je nulový. Zvolme libovolně $x \in R_1$ a počítejme:

$$\varphi(x) = \varphi(x \cdot 1) = \varphi(x) \cdot \varphi(1) = \varphi(x) \cdot 0 = 0.$$

8.2.6. Tvrzení. *Nechť R_1, R_2 jsou okruhy, $\varphi : R_1 \to R_2$ je homomorfismus. Platí:*

1. $\varphi(0) = 0$
2. $\varphi(-x) = -\varphi(x)$ *(pro libovolné $x \in R_1$).*

Důkaz. Stačí si uvědomit, že φ je homomorfismus aditivní grupy okruhu R_1 do aditivní grupy okruhu R_2 a použít Tvrzení 1.3.2.

Nechť R_1, R_2 jsou okruhy s jednotkovým prvkem, $\varphi : R_1 \to R_2$ je homomorfismus. Možná bychom očekávali, že bude $\varphi(1) = 1$. Toto očekávání je nereálné, jak ukazuje případ nulového homomorfismu. Dokonce však i v případě nenulového homomorfismu φ může být $\varphi(1) \neq 1$.

8.2.7. Příklad. Uvažme okruh $\mathbb{Z}_6$ s jednotkovým prvkem $\overline{1}$ a zobrazení $\varphi : \mathbb{Z}_6 \to \mathbb{Z}_6$ dané předpisem $\varphi(x) = \overline{3} \cdot x$ (pro libovolné $x \in \mathbb{Z}_6$). Ukážeme, že φ je homomorfismus okruhů. Zvolme libovolně $x, y \in \mathbb{Z}_6$ a počítejme:
$\varphi(x + y) = \overline{3} \cdot (x + y) = \overline{3} \cdot x + \overline{3} \cdot y = \varphi(x) + \varphi(y)$,
$\varphi(x \cdot y) = \overline{3} \cdot (x \cdot y) = \overline{9} \cdot x \cdot y = \overline{3 \cdot 3} \cdot x \cdot y = \overline{3} \cdot \overline{3} \cdot x \cdot y = \overline{3} \cdot x \cdot \overline{3} \cdot y = \varphi(x) \cdot \varphi(y)$
(při výpočtu jsme použili fakt, že $3 \equiv 9$ (6), což dává $\overline{3} = \overline{9}$ v $\mathbb{Z}_6$).
Je $\varphi(\overline{1}) = \overline{3} \cdot \overline{1} = \overline{3 \cdot 1} = \overline{3} \neq \overline{0}$, takže homomorfismus φ není nulový. Rovnost $\varphi(\overline{1}) = \overline{3}$ také dává $\varphi(\overline{1}) \neq \overline{1}$.

V případě dvou oborů integrity s jednotkovým prvkem a nenulového homomorfismu prvního oboru integrity do druhého oboru integrity však již konečně platí, že obrazem jednotkového prvku je jednotkový prvek,

8.2.8. Tvrzení. *Nechť I_1, I_2 jsou obory integrity s jednotkovým prvkem a $\varphi : I_1 \to I_2$ je nenulový homomorfismus. Pak $\varphi(1) = 1$.*

Důkaz. Protože homomorfismus φ je nenulový, je $\varphi(1) \neq 0$ (viz Tvrzení 8.2.5.). Dále, $\varphi(1) \cdot 1 = \varphi(1) = \varphi(1 \cdot 1) = \varphi(1) \cdot \varphi(1)$, takže $\varphi(1) \cdot 1 = \varphi(1) \cdot \varphi(1)$. Použitím zákona o krácení nenulovým prvkem, konkrétně budeme krátit prvkem $\varphi(1)$, dostaneme $1 = \varphi(1)$.

8.2.9. Tvrzení. *Nechť T_1, T_2 jsou tělesa, $\varphi : T_1 \to T_2$ je nenulový homomorfismus. Pak platí:*

1. $\varphi(0) = 0$
2. $\varphi(-x) = -\varphi(x)$ *(pro libovolné $x \in T_1$)*
3. $\varphi(1) = 1$
4. *jestliže $x \neq 0$, pak $\varphi(x) \neq 0$ a $\varphi(x^{-1}) = \varphi(x)^{-1}$ (pro libovolné $x \in T_1$).*

Důkaz.

1. viz Tvrzení 8.2.6.

2. viz Tvrzení 8.2.6.

3. viz Tvrzení 8.2.8. (je důležité si uvědomit, že každé těleso je obor integrity s jednotkovým prvkem)

4. Nechť $x \in T_1$, $x \neq 0$. Předpokládejme, že $\varphi(x) = 0$. Pak
$\varphi(1) = \varphi(x \cdot x^{-1}) = \varphi(x) \cdot \varphi(x^{-1}) = 0 \cdot \varphi(x^{-1}) = 0$, takže $\varphi(1) = 0$, což dle Tvrzení 8.2.5. znamená, že homomorfismus φ je nulový. To je spor. Nutně tedy $\varphi(x) \neq 0$. Víme již, že $\varphi(1) = 1$. Toho využijeme v následujícím výpočtu. Platí:
$\varphi(x^{-1}) = 1 \cdot \varphi(x^{-1}) = (\varphi(x)^{-1} \cdot \varphi(x)) \cdot \varphi(x^{-1}) = \varphi(x)^{-1} \cdot (\varphi(x) \cdot \varphi(x^{-1})) =$
$\varphi(x)^{-1} \cdot \varphi(x \cdot x^{-1}) = \varphi(x)^{-1} \cdot \varphi(1) = \varphi(x)^{-1} \cdot 1 = \varphi(x)^{-1}$.

8.2.10. Tvrzení. *Nechť R_1, R_2, R_3 jsou okruhy, $\varphi : R_1 \to R_2$ je homomorfismus, $\psi : R_2 \to R_3$ je homomorfismus. Potom $\varphi\psi : R_1 \to R_3$ je homomorfismus.*

Důkaz. Nechť $x, y \in R_1$. Počítejme:
$(\varphi\psi)(x + y) = \psi(\varphi(x + y)) = \psi(\varphi(x) + \varphi(y)) = \psi(\varphi(x)) + \psi(\varphi(y)) = (\varphi\psi)(x) + (\varphi\psi)(y)$,
$(\varphi\psi)(x \cdot y) = \psi(\varphi(x \cdot y)) = \psi(\varphi(x) \cdot \varphi(y)) = \psi(\varphi(x)) \cdot \psi(\varphi(y)) = (\varphi\psi)(x) \cdot (\varphi\psi)(y)$.

Zabývejme se nyní otázkou, jak formalizovat naši představu, že dva okruhy R_1 a R_2 jsou v podstatě stejné.

Nechť okruhy R_1 a R_2 jsou v podstatě stejné. Pak by mělo existovat vzájemně jednoznačné zobrazení $\varphi : R_1 \to R_2$ takové, že pro všechna $x, y, u, v \in R_1$ platí:

$$x + y = u \wedge x \cdot y = v \Longrightarrow \varphi(x) + \varphi(y) = \varphi(u) \wedge \varphi(x) \cdot \varphi(y) = \varphi(v).$$

Tedy sčítání a násobení v R_2 prostřednictvím vzájemně jednoznačného zobrazení φ koresponduje se sčítáním a násobením v R_1. V takovém případě zvolme libovolná $x, y \in R_1$, označme $x + y$ jako u a označme $x \cdot y$ jako v. Pak

$$\varphi(x + y) = \varphi(u) = \varphi(x) + \varphi(y), \ \varphi(x \cdot y) = \varphi(v) = \varphi(x) \cdot \varphi(y).$$

Nyní již vyslovíme formální definici toho, že okruhy R_1 a R_2 jsou v podstatě stejné. Místo slovního obratu "jsou v podstatě stejné"použijeme slovní obrat "jsou izomorfní".

8.2.11. Definice. Nechť R_1, R_2 jsou okruhy. Říkáme, že okruhy R_1, R_2 jsou **izomorfní**, pokud existuje bijekce $\varphi : R_1 \to R_2$ splňující

$$\varphi(x+y) = \varphi(x) + \varphi(y),\ \varphi(x \cdot y) = \varphi(x) \cdot \varphi(y)$$

pro všechna $x, y \in R_1$. To, že okruhy R_1, R_2 jsou izomorfní, zapisujeme symbolicky $R_1 \cong R_2$. Zobrazení φ nazýváme **izomorfismus** okruhu R_1 na okruh R_2. (Všimněme si, že izomorfismus je totéž, co bijektivní homomorfismus.)

8.2.12. Tvrzení. *Nechť R je okruh. Zobrazení $id : R \to R$ dané předpisem $id(x) = x$ pro každé $x \in R$, je izomorfismus.*

Důkaz. Důkaz přenecháváme čtenáři.

8.2.13. Tvrzení. *Nechť R_1, R_2 jsou okruhy, $\varphi : R_1 \to R_2$ je izomorfismus. Pak $\varphi^{-1} : R_2 \to R_1$ je izomorfismus.*

Důkaz. Ze základů matematiky víme, že $\varphi^{-1} : R_2 \to R_1$ je bijekce. Zvolme $x, y \in R_2$. Chceme: $\varphi^{-1}(x+y) = \varphi^{-1}(x) + \varphi^{-1}(y)$ a $\varphi^{-1}(x \cdot y) = \varphi^{-1}(x) \cdot \varphi^{-1}(y)$. Protože zobrazení φ je prosté, tak stačí ukázat, že $\varphi(\varphi^{-1}(x+y)) = \varphi(\varphi^{-1}(x) + \varphi^{-1}(y))$ a $\varphi(\varphi^{-1}(x \cdot y)) = \varphi(\varphi^{-1}(x) \cdot \varphi^{-1}(y))$. Ovšem
$\varphi(\varphi^{-1}(x+y)) = x + y$,
$\varphi(\varphi^{-1}(x) + \varphi^{-1}(y)) = \varphi(\varphi^{-1}(x)) + \varphi(\varphi^{-1}(y)) = x + y$,
$\varphi(\varphi^{-1}(x \cdot y)) = x \cdot y$,
$\varphi(\varphi^{-1}(x) \cdot \varphi^{-1}(y)) = \varphi(\varphi^{-1}(x)) \cdot \varphi(\varphi^{-1}(y)) = x \cdot y$.

8.2.14. Tvrzení. *Nechť R_1, R_2, R_3 jsou okruhy, $\varphi : R_1 \to R_2$ je izomorfismus, $\psi : R_2 \to R_3$ je izomorfismus. Pak $\varphi\psi : R_1 \to R_3$ je izomorfismus.*

Důkaz. Ze základů matematiky víme, že $\varphi\psi$ je bijekce. Pak stačí použít tvrzení 8.2.10.

8.2.15. Tvrzení. *Nechť R je okruh. Pak $R \cong R$.*

Důkaz. Důkaz přenecháváme čtenáři.

8.2.16. Tvrzení. *Nechť R_1, R_2 jsou okruhy. Jestliže $R_1 \cong R_2$, pak $R_2 \cong R_1$.*

Důkaz. Důkaz přenecháváme čtenáři.

8.2.17. Tvrzení. *Nechť R_1, R_2, R_3 jsou okruhy. Jestliže $R_1 \cong R_2$ a $R_2 \cong R_3$, pak $R_1 \cong R_3$.*

Důkaz. Důkaz přenecháváme čtenáři.

8.2.18. Příklad. Uvažme zobrazení $\varphi : \mathbb{C} \to \mathbb{C}$ dané předpisem $\varphi(a + b\mathrm{i}) = a - b\mathrm{i}$ (a, b jsou reálná čísla). Ukážeme, že φ je izomorfismus tělesa $\mathbb{C}$ na těleso $\mathbb{C}$. Nejdříve ukážeme, že φ je homomorfismus. Nechť a, b, c, d jsou reálná čísla. Počítejme:
$\varphi((a+b\mathrm{i})+(c+d\mathrm{i})) = \varphi((a+c)+(b+d)\mathrm{i}) = (a+c)-(b+d)\mathrm{i} = (a-b\mathrm{i})+(c-d\mathrm{i}) = \varphi(a + b\mathrm{i}) + \varphi(c + d\mathrm{i})$,
$\varphi((a + b\mathrm{i}) \cdot (c + d\mathrm{i})) = \varphi((ac - bd) + (ad + bc)\mathrm{i}) = (ac - bd) - (ad + bc)\mathrm{i} = (a - b\mathrm{i}) \cdot (c - d\mathrm{i}) = \varphi(a + b\mathrm{i}) \cdot \varphi(c + d\mathrm{i})$.
Přesvědčíme se ještě, že φ je bijekce.
φ je injekce: Nechť a, b, c, d jsou reálná čísla, $\varphi(a + b\mathrm{i}) = \varphi(c + d\mathrm{i})$. Chceme: $a + b\mathrm{i} = c + d\mathrm{i}$. Víme, že $a - b\mathrm{i} = c - d\mathrm{i}$, $a + (-b)\mathrm{i} = c + (-d)\mathrm{i}$. Pak $a = c$, $-b = -d$, $b = d$, takže $a + b\mathrm{i} = c + d\mathrm{i}$.
φ je surjekce: Nechť c, d jsou reálná čísla. Hledáme reálná čísla a, b taková, že $\varphi(a + b\mathrm{i}) = c + d\mathrm{i}$. Položme $a = c$, $b = -d$. Pak $\varphi(a + b\mathrm{i}) = a - b\mathrm{i} = a + (-b)\mathrm{i} = c + d\mathrm{i}$.

8.2.19. Příklad. Najdeme všechny izomorfismy $\psi : \mathbb{C} \to \mathbb{C}$ takové, že $\psi(r) = r$ pro každé reálné číslo r. Buď tedy ψ nějaký takový izomorfismus. Nechť a, b jsou reálná čísla. Pak

$$\psi(a + b\mathrm{i}) = \psi(a) + \psi(b) \cdot \psi(\mathrm{i}) = a + b \cdot \psi(\mathrm{i}).$$

Vidíme, že k určení izomorfismu ψ je podstatné znát hodnotu $\psi(\mathrm{i})$. Nechť $\psi(\mathrm{i}) = x + y\mathrm{i}$, kde x, y jsou reálná čísla. Pak

$$-1 = \psi(-1) = \psi(\mathrm{i}^2) = (\psi(\mathrm{i}))^2 = (x + y\mathrm{i})^2 = (x^2 - y^2) + 2xy\mathrm{i},$$

$$-1 + 0 \cdot \mathrm{i} = (x^2 - y^2) + 2xy\mathrm{i}.$$

Z toho dostáváme: $x^2 - y^2 = -1$, $2xy = 0$.
Jelikož $2xy = 0$, je $x = 0$ nebo $y = 0$. Případ $y = 0$ dává $x^2 = -1$, což nelze

(x je reálné číslo, takže $x^2 \geq 0$). Nutně tedy $x = 0$. Pak $-y^2 = -1$, $y^2 = 1$. Jsou dvě možnosti: $y = 1$ nebo $y = -1$. Postupně obě možnosti probereme.

1. $y = 1$: Je $\psi(i) = 0 + 1 \cdot \mathrm{i} = \mathrm{i}$, takže

   $$\psi(a + b\mathrm{i}) = a + b\mathrm{i}$$

   (pro libovolná reálná čísla a, b). Je tedy ψ izomorfismus id z tvrzení 8.2.12.

2. $y = -1$: Je $\psi(\mathrm{i}) = 0 + (-1) \cdot \mathrm{i} = -\mathrm{i}$, takže

   $$\psi(a + b\mathrm{i}) = a + b \cdot (-\mathrm{i}) = a - b\mathrm{i}$$

   (pro libovolná reálná čísla a, b). Je tedy ψ roven izomorfismu φ z příkladu 8.2.18.

Závěr: Existují právě dva izomorfismy $\psi : \mathbb{C} \to \mathbb{C}$ takové, že $\psi(r) = r$ pro každé reálné číslo r. Jsou to izomorfismy

$$\psi_1(a + b\mathrm{i}) = a + b\mathrm{i}, \ \psi_2(a + b\mathrm{i}) = a - b\mathrm{i}$$

(a, b jsou libovolná reálná čísla).

8.3 Podokruhy a ideály

Nechť R je okruh. Operaci sčítání v okruhu R označme $+$ a operaci násobení v okruhu R označme $\cdot$. Nechť $S \subseteq R$. Pokusíme se zformulovat nutné a postačující podmínky, jejichž splnění znamená, že množina S spolu s operacemi $+$ a $\cdot$ je okruh (právě v takovém případě budeme S považovat za podokruh okruhu R).

Předpokládejme nejprve, že množina S spolu s operacemi $+$ a $\cdot$ je okruh.

Jsou $+$ a $\cdot$ operace na množině S, takže pro všechna $x, y \in S$ máme $x + y \in S$, $x \cdot y \in S$.

Dále, množina S s operací $+$ je komutativní grupa. Existuje prvek $e \in S$ splňující $e + x = x$ pro každé $x \in S$. Pak $e + e = e$ (sčítáme v S) a $e + 0 = e$ (sčítáme v R a využíváme toho, že 0 je neutrální prvek operace sčítání v okruhu R). Dostáváme $e + e = e + 0$ a po krácení v aditivní grupě okruhu R máme $e = 0$. Ukázali jsme, že $0 \in S$. Zvolme nyní libovolně prvek $x \in S$. Protože S s operací $+$ je grupa, existuje $y \in S$, $x + y = e = 0$. Je $x \in R$ a v okruhu R máme $x + (-x) = 0$. Tudíž $x + y = x + (-x)$ a po krácení v aditivní grupě okruhu R dostáváme $y = -x$, tedy $-x \in S$.

Platí tedy:

1. pro všechna $x, y \in S$ je $x + y \in S$ a $x \cdot y \in S$

2. $0 \in S$

3. pro všechna $x \in S$ je $-x \in S$.

Předpokládejme nyní, že právě zformulované podmínky 1,2 a 3 jsou splněny. Ukážeme, že množina S spolu s operacemi $+$ a $\cdot$ je okruh.

Splnění podmínky 1 zajišťuje, že $+$ a $\cdot$ jsou operace na množině S.

Nejdříve ukážeme, že S spolu s operací $+$ je komutativní grupa. Pro libovolné prvky $x, y, z \in R$ je $x+(y+z) = (x+y)+z$, $x+y = y+x$, $x+0 = x$, $x + (-x) = 0$. Jelikož $S \subseteq R$, platí uvedené rovnosti také pro libovolná $x, y, z \in S$. Tedy: operace $+$ je asociativní a komutativní na množině S, 0 je neutrální prvek operace $+$ na množině S (zde je důležité, že $0 \in S$ dle podmínky 2), ke každému prvku množiny S existuje v množině S prvek opačný (zde je důležité, že $-x \in S$ pro každé $x \in S$ dle podmínky 3).

Zbývá ukázat, že na množině S je operace $\cdot$ distributivní vzhledem k operaci $+$. Pro všechna $x, y, z \in R$ je $x \cdot (y + z) = x \cdot y + x \cdot z$ a $(y + z) \cdot x = y \cdot x + z \cdot x$. Protože $S \subseteq R$, platí uvedená rovnost také pro všechna $x, y, z \in S$.

Nyní je snad již dostatečně vysvětleno, proč následující definice dobře popisuje naše chápání pojmu podokruh okruhu, tedy že podokruhem okruhu R jsou právě ty podmnožiny S množiny R, které jsou samy okruhem, pokud pro prvky množiny S je jejich součet (součin) roven součtu (součinu) v okruhu R.

8.3.1. Definice. Nechť R je okruh, $S \subseteq R$. Pak S se nazývá **podokruh** okruhu R, platí-li

1. pro všechna $x, y \in S$ je $x + y \in S$ a $x \cdot y \in S$

2. $0 \in S$

3. pro všechna $x \in S$ je $-x \in S$.

8.3.2. Příklady.

1. Nechť R je libovolný okruh. Pak $\{0\}$ a R jsou podokruhy okruhu R.

2. $\mathbb{Z}$ je podokruhem tělesa $\mathbb{Q}$ (uvažujeme obvyklé operace sčítání a násobení čísel); tento příklad ukazuje, že podokruh tělesa nemusí být těleso.

3. $\mathbb{S}$ je podokruhem okruhu $\mathbb{Z}$; tento příklad ukazuje, že podokruh okruhu s jednotkovým prvkem nemusí být okruh s jednotkovým prvkem.

8.3.3. Tvrzení. *Nechť R je okruh, S je podokruh okruhu R. Platí:*

1. *Jestliže R je asociativní, pak také S je asociativní.*
2. *Jestliže R je komutativní, pak také S je komutativní.*
3. *Jestliže R je obor integrity, pak také S je obor integrity.*

Důkaz. Dokážeme pouze část 1, zbytek důkazu je obdobný a čtenář si jej snadno udělá sám. Předpokládejme, že okruh R je asociativní. Pro všechna $x, y, z \in R$ je $x(yz) = (xy)z$. Samozřejmě také $x(yz) = (xy)z$ pro všechna $x, y, z \in S$, protože $S \subseteq R$ a součin libovolných dvou prvků v S je roven jejich součinu v R.

8.3.4. Tvrzení. *Nechť R je okruh, S_1, S_2 jsou podokruhy okruhu R. Pak $S_1 \cap S_2$ je podokruh okruhu R.*

Důkaz. Je třeba dokázat následující:
(I) pro všechna $x, y \in S_1 \cap S_2$ je $x + y \in S_1 \cap S_2$ a $xy \in S_1 \cap S_2$
(II) $0 \in S_1 \cap S_2$
(III) pro všechna $x \in S_1 \cap S_2$ je $-x \in S_1 \cap S_2$
ad (I): Nechť $x, y \in S_1 \cap S_2$. Je $x, y \in S_1$ a $x, y \in S_2$. Protože S_1 je podokruh okruhu R, je $x + y \in S_1$ a $xy \in S_1$. Protože S_2 je podokruh okruhu R, je $x + y \in S_2$ a $xy \in S_2$. Z $x + y \in S_1$ a $x + y \in S_2$ dostáváme $x + y \in S_1 \cap S_2$, z $xy \in S_1$ a $xy \in S_2$ dostáváme $xy \in S_1 \cap S_2$.
ad (II): Jelikož S_1 je podokruh okruhu R, je $0 \in S_1$. Jelikož S_2 je podokruh okruhu R, je $0 \in S_2$. Celkem: $0 \in S_1 \cap S_2$.
ad (III): Nechť $x \in S_1 \cap S_2$. Pak $x \in S_1$ a $x \in S_2$. Protože S_1 je podokruh okruhu R, je $-x \in S_1$. Protože S_2 je podokruh okruhu R, je $-x \in S_2$. Celkem: $-x \in S_1 \cap S_2$.

8.3.5. Tvrzení. *Nechť R je okruh, S_i pro $i \in I$ ($I \neq \emptyset$) jsou podokruhy okruhu R. Pak $\bigcap_{i \in I} S_i$ je podokruh okruhu R.*

Důkaz. Důkaz přenecháváme čtenáři.

Jestliže R je okruh a $M \subseteq R$, pak zřejmě M nemusí být podokruh okruhu R. Bude nás nyní zajímat nejmenší podokruh okruhu R obsahující množinu M. Takový podokruh budeme nazývat podokruh okruhu R generovaný množinou M.

8.3.6. Definice. Nechť R je okruh a $M \subseteq R$. Pak S se nazývá **podokruh okruhu R generovaný množinou M**, jsou-li splněny následující tři podmínky:

1. S je podokruh okruhu R
2. $M \subseteq S$
3. pro všechna K platí: jestliže K je podokruh okruhu R a $M \subseteq K$, pak $S \subseteq K$.

8.3.7. Tvrzení. *Nechť R je okruh a $M \subseteq R$. Pak podokruh okruhu R generovaný množinou M existuje a je určen jednoznačně.*

Důkaz.
existence:
Nechť S_i, pro $i \in I$, je systém všech podokruhů okruhu R obsahujících množinu M. Je $I \neq \emptyset$, protože R je podokruh okruhu R a $M \subseteq R$. Položme $S = \bigcap_{i \in I} S_i$. Ukážeme, že S splňuje podmínky z definice 8.3.6.
ad 1: S je podokruh okruhu R dle 8.3.5.
ad 2: Chceme: $M \subseteq S$. Pro každé $i \in I$ je $M \subseteq S_i$, takže $M \subseteq \bigcap_{i \in I} S_i = S$.
ad 3: Nechť K je podokruh okruhu R, $M \subseteq K$. Chceme: $S \subseteq K$. Protože S_i, pro $i \in I$, je systém všech podokruhů okruhu R obsahujících M, musí být $K = S_j$ pro nějaké $j \in I$. Pak $\bigcap_{i \in I} S_i \subseteq S_j$, $S \subseteq K$.
jednoznačnost:
Nechť S, S' jsou podokruhy okruhu R generované množinou M. Chceme: $S = S'$. Platí:
1: S je podokruh okruhu R
2: $M \subseteq S$
3: pro všechna K platí: jestliže K je podokruh okruhu R a $M \subseteq K$, pak $S \subseteq K$
1': S' je podokruh okruhu R
2': $M \subseteq S'$
3': pro všechna K platí: jestliže K je podokruh okruhu R a $M \subseteq K$, pak

$S' \subseteq K$.
Z 1, 2 a 3' (pro $K = S$) dostáváme $S' \subseteq S$. Z 1',2' a 3 (pro $K = S'$) dostáváme $S \subseteq S'$. Celkem tedy $S = S'$.

Díky Tvrzení 8.3.7 můžeme zavést označení: Nechť R je okruh a $M \subseteq R$. Jednoznačně daný podokruh okruhu R generovaný množinou M budeme značit $\langle M \rangle$. Množina M se nazývá množina **generátorů** okruhu $\langle M \rangle$. Pokud množina M je konečná, $M = \{a_1, a_2, \ldots, a_n\}$, pak hovoříme o podokruhu generovaném prvky $a_1, a_2, \ldots, a_n$ a značíme jej často stručně $\langle a_1, a_2, \ldots, a_n \rangle$.

Nechť R je okruh, S je podokruh okruhu R, $a \in R$. Podokruh $\langle S \cup \{a\} \rangle$ okruhu R budeme označovat $S[a]$.

8.3.8. Příklad. $\mathbb{R}$ je podokruh tělesa $\mathbb{C}$, $i \in \mathbb{C}$. Je $\mathbb{C} = \mathbb{R}[i]$. Zdůvodnění: Zřejmě $\mathbb{R}[i] \subseteq \mathbb{C}$. Ukážeme, že $\mathbb{C} \subseteq \mathbb{R}[i]$. Nechť a, b jsou libovolná reálná čísla. Chceme: $a + bi \in \mathbb{R}[i]$. Je $a, b, i \in \mathbb{R} \cup \{i\} \subseteq \langle \mathbb{R} \cup \{i\} \rangle$, takže $a, b, i \in \mathbb{R}[i]$. Protože $\mathbb{R}[i]$ je podokruh, dostáváme postupně $bi \in \mathbb{R}[i]$, $a + bi \in \mathbb{R}[i]$.

Také v okruzích používáme známé symboly $\sum$ a $\prod$. Nyní vymezíme (připomeneme) jejich význam.

Nechť R je okruh, m, n jsou celá čísla, pro každé celé číslo i, $m \leq i \leq n$, je $a_i \in R$. Pak

$$\sum_{m \leq i \leq n} a_i = \begin{cases} a_m + a_{m+1} + \cdots + a_n & \text{pro } m \leq n \\ 0 & \text{pro } m > n \end{cases}$$

Jestliže navíc R je asociativní okruh s jednotkovým prvkem, pak

$$\prod_{m \leq i \leq n} a_i = \begin{cases} a_m \cdot a_{m+1} \cdot \cdots \cdot a_n & \text{pro } m \leq n \\ 1 & \text{pro } m > n \end{cases}$$

Uvědomme si, že pro celá čísla k, l je $k < l$ ekvivalentní s $k \leq l - 1$, takže například

$$\sum_{0 \leq i < n} a_i = \sum_{0 \leq i \leq n-1} a_i.$$

8.3.9. Věta. *Nechť R je komutativní asociativní okruh s jednotkovým prvkem, S je podokruh okruhu R, $1 \in S$, $a \in R$, n je nezáporné celé číslo, $s_0, s_1, \ldots, s_n \in S$, $a^{n+1} = s_0 + s_1 a + s_2 a^2 + \cdots + s_n a^n$. Pak*

$$S[a] = \{u_0 + u_1 a + u_2 a^2 + \cdots + u_n a^n |\ u_0, u_1, u_2, \ldots, u_n \in S\}.$$

Důkaz. Dokážeme nejprve

Pomocné tvrzení: Nechť $u_0, u_1, \ldots, u_n \in S$, $v \in S$. Pro každé nezáporné celé číslo j platí:

$$\left(\sum_{0\leq i\leq n} u_i a^i\right) \cdot va^j = \sum_{0\leq i\leq n} v_i a^i$$

pro nějaká $v_0, v_1, \ldots, v_n \in S$.

Důkaz Pomocného tvrzení: Postupujme indukcí vzhledem k j.
$j = 0$:

$$\begin{aligned}\left(\sum_{0\leq i\leq n} u_i a^i\right) \cdot va^0 &= \left(\sum_{0\leq i\leq n} u_i a^i\right) \cdot v \cdot 1\\ &= \left(\sum_{0\leq i\leq n} u_i a^i\right) \cdot v\\ &= \sum_{0\leq i\leq n} u_i v a^i\\ &= \sum_{0\leq i\leq n} (u_i v) a^i\end{aligned}$$

Pro celé číslo i, $0 \leq i \leq n$, položíme $v_i = u_i v$; je $u_i, v \in S$ a S je podokruh, takže $u_i v \in S$, $v_i \in S$.
$j > 0$:

$$\begin{aligned}\left(\sum_{0\leq i\leq n} u_i a^i\right) \cdot va^j &= \left(\sum_{0\leq i\leq n} u_i a^i\right) \cdot va^{j-1}a\\ &= \left(\left(\sum_{0\leq i\leq n} u_i a^i\right) \cdot va^{j-1}\right) \cdot a\end{aligned}$$

Podle indukčního předpokladu existují $w_0, w_1, \ldots, w_n \in S$,

$$\left(\sum_{0\leq i\leq n} u_i a^i\right) \cdot va^{j-1} = \sum_{0\leq i\leq n} w_i a^i$$

Pak

$$\begin{aligned}
\left(\sum_{0\le i\le n} u_i a^i\right)\cdot va^j &= \left(\sum_{0\le i\le n} w_i a^i\right)\cdot a \\
&= \sum_{0\le i\le n} w_i a^i a \\
&= \sum_{0\le i\le n} w_i a^{i+1} \\
&= \left(\sum_{0\le i<n} w_i a^{i+1}\right) + w_n a^{n+1} \\
&= \left(\sum_{0\le i<n} w_i a^{i+1}\right) + w_n \cdot \sum_{0\le i\le n} s_i a^i \\
&= \left(\sum_{0+1\le i+1<n+1} w_{(i+1)-1} a^{i+1}\right) + \sum_{0\le i\le n} w_n s_i a^i \\
&= \left(\sum_{1\le i<n+1} w_{i-1} a^i\right) + \sum_{0\le i\le n} w_n s_i a^i \\
&= w_n s_0 a^0 + \left(\sum_{1\le i\le n} w_{i-1} a^i\right) + \sum_{1\le i\le n} w_n s_i a^i \\
&= w_n s_0 a^0 + \sum_{1\le i\le n} (w_{i-1} a^i + w_n s_i a^i) \\
&= (w_n s_0) a^0 + \sum_{1\le i\le n} (w_{i-1} + w_n s_i) a^i
\end{aligned}$$

Pro celé číslo i, $1 \le i \le n$, položme $v_i = w_{i-1} + w_n s_i$; je $w_{i-1}, w_n, s_i \in S$ a S je podokruh, takže $w_{i-1} + w_n s_i \in S$, $v_i \in S$. Dále položme $v_0 = w_n s_0$; je $w_n, s_0 \in S$ a S je podokruh, takže $w_n s_0 \in S$, $v_0 \in S$. Nyní

$$\begin{aligned}
\left(\sum_{0\le i\le n} u_i a^i\right)\cdot va^j &= (w_n s_0) a^0 + \sum_{1\le i\le n} (w_{i-1} + w_n s_i) a^i \\
&= v_0 a^0 + \sum_{1\le i\le n} v_i a^i \\
&= \sum_{0\le i\le n} v_i a^i
\end{aligned}$$

Konec důkazu Pomocného tvrzení.
Položme

$$T = \{u_0 + u_1 a + u_2 a^2 + \cdots + u_n a^n |\ u_0, u_1, u_2, \ldots, u_n \in S\}.$$

Dokážeme, že $T = S[a]$.

1. T je podokruh okruhu R:
   Nechť $x, y \in T$. Chceme: $x + y \in T$, $xy \in T$.
   Existují $u_0, u_1, \ldots, u_n \in S$, $v_0, v_1, \ldots, v_n \in S$ tak, že

$$x = \sum_{0 \le i \le n} u_i a^i,\ y = \sum_{0 \le i \le n} v_i a^i.$$

   Počítejme:

$$\begin{aligned} x + y &= \left(\sum_{0 \le i \le n} u_i a^i\right) + \left(\sum_{0 \le i \le n} v_i a^i\right) \\ &= \sum_{0 \le i \le n} (u_i a^i + v_i a^i) \\ &= \sum_{0 \le i \le n} (u_i + v_i) a^i \end{aligned}$$

   Pro každé celé číslo i, $0 \le i \le n$, je $u_i, v_i \in S$ a přitom S je podokruh, takže $u_i + v_i \in S$. Proto $\sum_{0 \le i \le n} (u_i + v_i) a^i \in T$, $x + y \in T$.
   Počítejme dále:

$$\begin{aligned} xy &= \left(\sum_{0 \le i \le n} u_i a^i\right) \cdot \left(\sum_{0 \le i \le n} v_i a^i\right) \\ &= \left(\sum_{0 \le i \le n} u_i a^i\right) \cdot (v_0 a^0 + v_1 a^1 + \cdots + v_n a^n) \\ &= \left(\sum_{0 \le i \le n} u_i a^i\right) \cdot v_0 a^0 + \left(\sum_{0 \le i \le n} u_i a^i\right) \cdot v_1 a^1 + \cdots + \left(\sum_{0 \le i \le n} u_i a^i\right) \cdot v_n a^n \end{aligned}$$

   Nechť j je celé číslo, $0 \le j \le n$. Podle Pomocného tvrzení existují $v_{j,0}, v_{j,1}, \ldots, v_{j,n} \in S$ tak, že

$$\left(\sum_{0 \le i \le n} u_i a^i\right) \cdot v_j a^j = \sum_{0 \le i \le n} v_{j,i} a^i.$$

Pak

$$\begin{aligned} xy &= \left(\sum_{0\le i\le n} u_i a^i\right)\cdot v_0 a^0 + \left(\sum_{0\le i\le n} u_i a^i\right)\cdot v_1 a^1 + \cdots + \left(\sum_{0\le i\le n} u_i a^i\right)\cdot v_n a^n \\ &= \left(\sum_{0\le i\le n} v_{0,i} a^i\right) + \left(\sum_{0\le i\le n} v_{1,i} a^i\right) + \cdots + \left(\sum_{0\le i\le n} v_{n,i} a^i\right) \\ &= \sum_{0\le i\le n} (v_{0,i} a^i + v_{1,i} a^i + \cdots + v_{n,i} a^i) \\ &= \sum_{0\le i\le n} (v_{0,i} + v_{1,i} + \cdots + v_{n,i}) a^i \end{aligned}$$

Pro každé celé číslo i, $0 \le i \le n$, je $v_{0,i}, v_{1,i}, \ldots, v_{n,i} \in S$ a přitom S je podokruh, takže $v_{0,i} + v_{1,i} + \cdots + v_{n,i} \in S$. Proto $\sum_{0\le i\le n}(v_{0,i} + v_{1,i} + \cdots + v_{n,i})a^i \in T$, $xy \in T$.

Nechť nyní $x \in T$. Chceme: $-x \in T$.
Je $x = u_0 + u_1 a + \cdots + u_n a^n$ pro nějaká $u_0, u_1, \ldots, u_n \in S$. Počítejme:

$$\begin{aligned} -x &= -(u_0 + u_1 a + \cdots + u_n a^n) \\ &= (-u_0) + (-(u_1 a)) + \cdots + (-(u_n a^n)) \\ &= (-u_0) + (-u_1)a + \cdots + (-u_n)a^n \end{aligned}$$

Jelikož S je podokruh, máme $-u_0, -u_1, \ldots, -u_n \in S$ a tedy $(-u_0) + (-u_1)a + \cdots + (-u_n)a^n \in T$, $-x \in T$.

Ještě je třeba ukázat, že $0 \in T$. Stačí si uvědomit, že $0 \in S$ (S je podokruh), takže $0 = 0 + 0 \cdot a + \cdots + 0 \cdot a^n \in T$.

Nyní je tedy konečně dokázáno, že T je podokruh okruhu R.

2. $S \cup \{a\} \subseteq T$:
Nejprve ukážeme, že $S \subseteq T$. Nechť $s \in S$. Chceme: $s \in T$.
S je podokruh, takže $0 \in S$. Pak $s + 0 \cdot a + \cdots + 0 \cdot a^n \in T$. Ovšem $s + 0 \cdot a + \cdots + 0 \cdot a^n = s + 0 + \cdots + 0 = s$, takže $s \in T$.
Ještě ukážeme, že $a \in T$.
Předpokládejme nejprve, že $n = 0$. Pak $a^{0+1} = s_0$, přičemž $s_0 \in S$; uvážíme-li, že $a^{0+1} = a^1 = a$, dostáváme $a \in S$. Již jsme dokázali, že $S \subseteq T$, takže $a \in T$. Nyní předpokládejme, že $n > 0$. Uvědomme si, že $0, 1 \in S$. Pak $0 + 1 \cdot a + 0 \cdot a^2 + \cdots + 0 \cdot a^n \in T$. Ovšem $0 + 1 \cdot a + 0 \cdot a^2 + \cdots + 0 \cdot a^n = 0 + a + 0 + \cdots + 0 = a$ a tedy $a \in T$.

3. Nechť K je podokruh okruhu R, $S \cup \{a\} \subseteq K$. Chceme: $T \subseteq K$.
   Nechť $x \in T$. Ukážeme, že $x \in K$. Je $x = u_0 + u_1 a + \cdots + u_n a^n$ pro nějaká $u_0, u_1, \ldots, u_n \in S$. Zvolme libovolně celé číslo i, $0 < i \leq n$. Je $u_i a^i \in K$, protože $u_i \in K$, $a \in K$ a K je podokruh. Máme tedy $u_0, u_1 a, \ldots, u_n a^n \in K$. Jelikož K je podokruh, je $u_0 + u_1 a + \cdots + u_n a^n \in K$, $x \in K$.

Nyní máme dokázáno, že $T = \langle S \cup \{a\} \rangle$, $T = S[a]$. Věta je dokázána.

Připomeneme nyní pojem algebraické celé číslo.

8.3.10. Definice. Nechť n je kladné celé číslo. Komplexní číslo α se nazývá **algebraické celé číslo stupně** n, platí-li:

1. Existují celá čísla $c_0, c_1, \ldots, c_{n-1}$ taková, že $c_0 + c_1\alpha + \cdots + c_{n-1}\alpha^{n-1} + \alpha^n = 0$.

2. Pro všechna celá čísla $d_0, d_1, \ldots, d_{n-1}$ platí: jestliže $d_0 + d_1\alpha + \cdots + d_{n-1}\alpha^{n-1} = 0$, pak $d_0 = d_1 = \cdots = d_{n-1} = 0$.

8.3.11. Příklady.

1. Každé celé číslo je algebraické celé číslo stupně 1.

2. $\sqrt{2}$ je algebraické celé číslo stupně 2.
   Zdůvodnění:
   Položme $c_0 = -2$, $c_1 = 0$. Čísla c_0, c_1 jsou celá, $c_0 + c_1\sqrt{2} + (\sqrt{2})^2 = -2 + 0 \cdot \sqrt{2} + (\sqrt{2})^2 = -2 + 0 + 2 = 0$. Dále, nechť d_0, d_1 jsou celá čísla, $d_0 + d_1\sqrt{2} = 0$. Chceme: $d_0 = d_1 = 0$. Předpokládejme, že $d_1 \neq 0$. Pak $\sqrt{2} = -\frac{d_0}{d_1}$. Ovšem číslo $-\frac{d_0}{d_1}$ je racionální, takže $\sqrt{2}$ je racionální číslo, spor. Nutně tedy $d_1 = 0$. Pak $d_0 + 0 \cdot \sqrt{2} = 0$, $d_0 = 0$.

3. $i = \sqrt{-1}$ je algebraické celé číslo stupně 2.
   Zdůvodnění:
   Položme $c_0 = 1$, $c_1 = 0$. Čísla c_0, c_1 jsou celá, $c_0 + c_1 i + i^2 = 1 + 0 \cdot i + i^2 = 1 + 0 + (-1) = 0$. Dále, nechť d_0, d_1 jsou celá čísla, $d_0 + d_1 i = 0$. Chceme: $d_0 = d_1 = 0$. To zřejmě platí.

4. $\frac{1}{2}$ není algebraické celé číslo.
   Zdůvodnění:
   Předpokládejme, že $\frac{1}{2}$ je algebraické celé číslo stupně n. Pak n je kladné celé číslo a existují celá čísla $c_0, c_1, \ldots, c_{n-1}$ taková, že $c_0 + c_1 \cdot \frac{1}{2} + \cdots + c_{n-1} \cdot (\frac{1}{2})^{n-1} + (\frac{1}{2})^n = 0$. Pak

$$\begin{aligned} \left(c_0 + c_1 \cdot \frac{1}{2} + \cdots + c_{n-1} \cdot \left(\frac{1}{2}\right)^{n-1} + \left(\frac{1}{2}\right)^n\right) \cdot 2^n &= 0 \cdot 2^n \\ c_0 \cdot 2^n + c_1 \cdot 2^{n-1} + \cdots + c_{n-1} \cdot 2 + 1 &= 0. \end{aligned}$$

   Dostáváme spor, protože v poslední rovnosti je na levé straně liché celé číslo, kdežto na straně pravé je sudé cele číslo. Závěr: $\frac{1}{2}$ není algebraické celé číslo.

8.3.12. Věta. *Nechť α je algebraické celé číslo stupně $n+1$. Pak*

$$\mathbb{Z}[\alpha] = \{u_0 + u_1\alpha + \cdots + u_n\alpha^n |\ u_0, u_1, \ldots, u_n \in \mathbb{Z}\},$$

přičemž vyjádření prvků okruhu $\mathbb{Z}[\alpha]$ ve tvaru $u_0 + u_1\alpha + \cdots + u_n\alpha^n$, kde $u_0, u_1, \ldots, u_n$ jsou celá čísla, je jednoznačné.

Důkaz. Jelikož α je algebraické celé číslo stupně $n+1$, je n nezáporné celé číslo a existují celá čísla $c_0, c_1, \ldots, c_n$ tak, že $c_0 + c_1\alpha + \cdots + c_n\alpha^n + \alpha^{n+1} = 0$. Uvědomme si, že $\mathbb{C}$ je těleso (tedy také komutativní asociativní okruh s jednotkovým prvkem), $\mathbb{Z}$ je podokruh tělesa $\mathbb{C}$, $1 \in \mathbb{Z}$, $\alpha \in \mathbb{C}$, n je nezáporné celé číslo, $-c_0, -c_1, \ldots, -c_n \in \mathbb{Z}$, $\alpha^{n+1} = -(c_0 + c_1\alpha + \cdots + c_n\alpha^n) = (-c_0) + (-c_1)\alpha + \cdots + (-c_n)\alpha^n$. Použitím věty 8.3.9. dostáváme $\mathbb{Z}[\alpha] = \{u_0 + u_1\alpha + \cdots + u_n \cdot \alpha^n |\ u_0, u_1, \ldots, u_n \in \mathbb{Z}\}$. Ještě je třeba ukázat jednoznačnost vyjádření prvků okruhu $\mathbb{Z}[\alpha]$ ve tvaru $u_0 + u_1\alpha + \cdots + u_n\alpha^n$, kde $u_0, u_1, \ldots, u_n$ jsou celá čísla. Nechť tedy $u_0, u_1, \ldots, u_n \in \mathbb{Z}$, $v_0, v_1, \ldots, v_n \in \mathbb{Z}$, $u_0 + u_1\alpha + \cdots + u_n\alpha^n = v_0 + v_1\alpha + \cdots + v_n\alpha^n$. Chceme: $u_j = v_j$ pro všechna celá čísla j, $0 \leq j \leq n$. Máme

$$\begin{aligned} u_0 + u_1\alpha + \cdots + u_n\alpha^n &= v_0 + v_1\alpha + \cdots + v_n\alpha^n \\ (u_0 + u_1\alpha + \cdots + u_n\alpha^n) - (v_0 + v_1\alpha + \cdots + v_n\alpha^n) &= 0 \\ (u_0 - v_0) + (u_1 - v_1)\alpha + \cdots + (u_n - v_n)\alpha^n &= 0 \end{aligned}$$

Uvědomme si, že pro všechna celá čísla j, $0 \leq j \leq n$, je $u_j - v_j \in \mathbb{Z}$. Protože α je algebraické celé číslo stupně $n+1$, máme $u_j - v_j = 0$, $u_j = v_j$, a to pro všechna celá čísla j, $0 \leq j \leq n$.

Okruhy $\mathbb{Z}[\alpha]$, kde α je algebraické celé číslo stupně 2, budeme podrobněji zkoumat v části 9.1. Specielně se budeme zabývat oborem integrity $\mathbb{Z}[\sqrt{-1}] = \mathbb{Z}[i]$ zvaným obor integrity **Gaussových celých čísel**.

Na závěr této části podáme základní informace o speciálních podokruzích zvaných ideály.

8.3.13. Definice. Nechť R je okruh, $I \subseteq R$. Množina I se nazývá **ideál** v okruhu R, jestliže platí

1. pro všechna $x, y \in I$ je $x + y \in I$
2. pro všechna $x \in I$, $z \in R$ je $zx \in I$ a $xz \in I$
3. $0 \in I$
4. pro všechna $x \in I$ je $-x \in I$.

8.3.14. Poznámka.

1. Jestliže I je ideál v okruhu R, pak I je podokruh okruhu R. V definici ideálu je silnější požadavek na uzavřenost vzhledem k součinu: má být $zx \in I$ a $xz \in I$ pro všechna $x \in I$, $z \in R$, nikoli pouze pro všechna $x, z \in I$. Například $\mathbb{Z}$ je podokruh tělesa $\mathbb{Q}$ (součet a součin dvou celých čísel je celé číslo, 0 je celé číslo, opačné číslo ke každému celému číslu je opět celé číslo), avšak $\mathbb{Z}$ není ideál v tělese $\mathbb{Q}$ – stačí si uvědomit, že $1 \in \mathbb{Z}$, $\frac{1}{2} \in \mathbb{Q}$, avšak $1 \cdot \frac{1}{2} = \frac{1}{2} \notin \mathbb{Z}$.
2. $\{0\}$ a R jsou ideály v každém okruhu R. Tyto ideály se nazývají **nevlastní**, ostatní ideály se nazývají **vlastní**.
3. V tělese jsou pouze nevlastní ideály. Zdůvodnění: Nechť T je těleso, I je ideál v I. Chceme: $I = \{0\}$ nebo $I = T$. Je-li $I = \{0\}$, jsme hotovi. Nechť tedy $I \neq \{0\}$. Protože $0 \in I$, musí existovat prvek $a \in I$, $a \neq 0$. Ukážeme, že $I = T$. Jistě $I \subseteq T$. Zbývá dokázat, že $T \subseteq I$. Zvolme libovolně $x \in T$. Chceme: $x \in I$. Využijeme toho, že $a \in T$ (je $I \subseteq T$), $a \neq 0$, takže v T existuje prvek a^{-1}. Protože I je ideál v T a $a \in I$, máme $(xa^{-1})a \in I$; ovšem $(xa^{-1})a = x(aa^{-1}) = x \cdot 1 = x$, takže $x \in I$.

Následující tvrzení ukazuje, že v případě komutativních okruhů s jednotkovým prvkem je možno definici ideálu zkrátit - některé podmínky z definice lze vynechat.

8.3.15. Tvrzení. *Nechť R je komutativní okruh s jednotkovým prvkem, $I \subseteq R$. Platí: I je ideál v okruhu R právě tehdy, když platí:*

1. *pro všechna $x, y \in I$ je $x + y \in I$*
2. *pro všechna $x \in I$, $z \in R$ je $zx \in I$*
3. *$0 \in I$.*

Důkaz. Vidíme ihned, že ideál I v okruhu R splňuje uvedené tři podmínky. Předpokládejme nyní, že podmnožina I okruhu R splňujem uvedené tři podmínky. Prověříme, že I splňuje všechny podmínky z definice ideálu:

1. pro všechna $x, y \in I$ je $x + y \in I$: To předpokládáme.
2. pro všechna $x \in I$, $z \in R$ je $zx \in I$ a $xz \in I$: Nechť $x \in I$, $z \in R$. Pak $zx \in I$ dle předpokladu; $xz \in I$ díky tomu, že R je komutativní okruh a v něm $xz = zx$.
3. $0 \in I$: To předpokládáme.
4. pro všechna $x \in I$ je $-x \in I$: Nechť $x \in I$. Chceme: $-x \in I$. Je $-1 \in R$ (R je okruh s jednotkovým prvkem) a dle předpokladu číslo 2 pak $(-1) \cdot x \in I$. Ovšem $(-1) \cdot x = -(1 \cdot x) = -x$, takže $-x \in I$.

8.3.16. Tvrzení. *Nechť R je okruh, I_1, I_2 jsou ideály v R. Pak $I_1 \cap I_2$ je ideál v R.*

Důkaz. Je $I_1 \cap I_2 \subseteq R$. Prověříme, že množina $I_1 \cap I_2$ splňuje všechny podmínky z definice ideálu:

1. pro všechna $x, y \in I_1 \cap I_2$ je $x + y \in I_1 \cap I_2$: Nechť $x, y \in I_1 \cap I_2$. Chceme: $x + y \in I_1 \cap I_2$. Je $x, y \in I_1$. Protože I_1 je ideál, máme $x + y \in I_1$. Také $x, y \in I_2$, I_2 je ideál a tedy $x + y \in I_2$. Ukázali jsme, že $x + y \in I_1$ a také $x + y \in I_2$. Proto $x + y \in I_1 \cap I_2$.

2. pro všechna $x \in I_1 \cap I_2$, $z \in R$ je $zx \in I_1 \cap I_2$ a $xz \in I_1 \cap I_2$: Nechť $x \in I_1 \cap I_2$, $z \in R$. Chceme: $zx \in I_1 \cap I_2$ a $xz \in I_1 \cap I_2$. Je $x \in I_1$. Protože I_1 je ideál, máme $zx \in I_1$ a také $xz \in I_1$. Také $x \in I_2$, I_2 je ideál a tedy $zx \in I_2$, $xz \in I_2$. Ukázali jsme, že $zx, xz \in I_1$ a $zx, xz \in I_2$. Proto $zx, xz \in I_1 \cap I_2$.

3. $0 \in I_1 \cap I_2$: Protože I_1 je ideál, je $0 \in I_1$. Protože I_2 je ideál, je $0 \in I_2$. Celkem tedy $0 \in I_1 \cap I_2$.

4. pro všechna $x \in I_1 \cap I_2$ je $-x \in I_1 \cap I_2$: Je $x \in I_1$ a I_1 je ideál, takže $-x \in I_1$. Také $x \in I_2$, I_2 je ideál a tedy $-x \in I_2$. Ukázali jsme, že $-x \in I_1$ a také $-x \in I_2$. Proto $-x \in I_1 \cap I_2$.

Právě dokázané tvrzení snadno zobecníme.

8.3.17. Tvrzení. *Nechť R je okruh, I_j, pro každé $j \in J$, $J \neq \emptyset$, je ideál v R. Pak $\bigcap_{j \in J} I_j$ je ideál v R.*

Důkaz. Tvrzení se dokáže obdobně jak tvrzení 8.3.16. a důkaz přenecháváme čtenáři.

Podmnožina M okruhu R samozřejmě nemusí být ideálem v R. Bude nás tedy zajímat nejmenší ideál okruhu R obsahující množinu M – tento ideál budeme nazývat ideál generovaný podmnožinou M.

8.3.18. Definice. Nechť R je okruh, $M \subseteq R$, $I \subseteq R$. Pak I se nazývá **ideál generovaný podmnožinou** M, platí-li:

1. I je ideál v okruhu R

2. $M \subseteq I$

3. pro všechna $K \subseteq R$ platí: jestliže K je ideál v okruhu R a $M \subseteq K$, pak $I \subseteq K$.

8.3.19. Tvrzení. *Nechť R je okruh, $M \subseteq R$. Platí: Ideál generovaný množinou M existuje a je určen jednoznačně.*

Důkaz.
existence:

Nechť I_j, $j \in J$, je soubor všech ideálů v okruhu R, které obsahují množinu M. Je $J \neq \emptyset$, protože R je ideál v R a $M \subseteq R$. Položme $I = \bigcap_{j \in J} I_j$. Ukážeme, že I splňuje všechny podmínky z definice ideálu generovaného množinou M. Zřejmě $I \subseteq R$.

1. I je ideál v okruhu R: viz 8.3.17.
2. $M \subseteq I$: pro každé $j \in J$ je $M \subseteq I_j$, takže $M \subseteq \bigcap_{j \in J} I_j$, $M \subseteq I$.
3. pro všechna $K \subseteq R$ platí: jestliže K je ideál v okruhu R a $M \subseteq K$, pak $I \subseteq K$: Nechť K je ideál v R, $M \subseteq K$. Chceme: $I \subseteq K$. Je $K = I_p$ pro nějaké $p \in J$ a tedy $\bigcap_{j \in J} I_j \subseteq I_p$, $I \subseteq K$.

jednoznačnost:
Nechť $I \subseteq R$, $J \subseteq R$, I, J jsou ideály generované množinou M. Chceme: $I = J$. Víme:

1. I je ideál v okruhu R
2. $M \subseteq I$
3. pro všechna $K \subseteq R$ platí: jestliže K je ideál v okruhu R a $M \subseteq K$, pak $I \subseteq K$.

a také

4. J je ideál v okruhu R
5. $M \subseteq J$
6. pro všechna $K \subseteq R$ platí: jestliže K je ideál v okruhu R a $M \subseteq K$, pak $J \subseteq K$.

Z 1,2 a 6 (pro $K = I$) máme $J \subseteq I$. Z 4,5 a 3 (pro $K = J$) máme $I \subseteq J$. Takže $I \subseteq J$ a $J \subseteq I$, což dává $I = J$.

Tvrzení 8.3.19. umožňuje zavést označení. Nechť R je okruh, $M \subseteq R$. Pak ideál generovaný podmnožinou M budeme označovat (M). Jestliže M je konečná, $M = \{a_1, a_2, \ldots, a_n\}$, pak místo $(\{a_1, a_2, \ldots, a_n\})$ budeme často stručněji psát $(a_1, a_2, \ldots, a_n)$ a hovoříme někdy o ideálu generovaném prvky $a_1, a_2, \ldots, a_n$.

Dobré bude znát také nějaké více konstruktivní vymezení ideálu generovaného podmnožinou M okruhu R – zatím známe pouze dvě vymezení, a to definici a fakt, že ideál generovaný podmnožinou M je roven průniku všech ideálů v okruhu R obsahujících množinu M (viz důkaz tvrzení 8.3.19.). Konstruktivní popis ideálu generovaného podmnožinou asociativního komutativního okruhu s jednotkovým prvkem podáváme v následující větě.

8.3.20. Věta. *Nechť R je asociativní komutativní okruh s jednotkovým prvkem, n je kladné celé číslo, $a_1, a_2, \ldots, a_n \in R$. Pak*

$$(a_1, a_2, \ldots, a_n) = \{r_1a_1 + r_2a_2 + \cdots + r_na_n |\ r_1, r_2, \ldots, r_n \in R\}.$$

Důkaz. Nechť $I = \{r_1a_1 + r_2a_2 + \cdots + r_na_n |\ r_1, r_2, \ldots, r_n \in R\}$. Jistě $I \subseteq R$. Ukážeme, že I splňuje všechny podmínky z definice ideálu generovaného prvky $a_1, a_2, \ldots, a_n$.

1. I je ideál v okruhu R: R je komutativní asocioativní okruh s jednotkovým prvkem, takže můžeme použít tvrzení 8.3.15.
   Nechť $x, y \in I$. Chceme: $x + y \in I$.
   Je $x = r_1a_1 + r_2a_2 + \cdots + r_na_n$, kde $r_1, r_2, \ldots, r_n \in R$, a $y = s_1a_1 + s_2a_2 + \cdots + s_na_n$, kde $s_1, s_2, \ldots, s_n \in R$. Pak

   $$\begin{aligned} x + y &= (r_1a_1 + r_2a_2 + \cdots + r_na_n) + (s_1a_1 + s_2a_2 + \cdots + s_na_n) \\ &= r_1a_1 + s_1a_1 + r_2a_2 + s_2a_2 + \cdots + r_na_n + s_na_n \\ &= (r_1 + s_1)a_1 + (r_2 + s_2)a_2 \cdots + (r_n + s_n)a_n \end{aligned}$$

   Uvědomme si, že $r_1 + s_1, r_2 + s_2, \ldots, r_n + s_n \in R$, takže $x + y \in I$.
   Nechť $x \in I$, $z \in R$. Chceme: $zx \in I$.
   Je $x = r_1a_1 + r_2a_2 + \cdots + r_na_n$, kde $r_1, r_2, \ldots, r_n \in R$. Pak

   $$\begin{aligned} zx &= z \cdot (r_1a_1 + r_2a_2 + \cdots + r_na_n) \\ &= z(r_1a_1) + z(r_2a_2) + \cdots + z(r_na_n) \\ &= (zr_1)a_1 + (zr_2)a_2 + \cdots + (zr_n)a_n \end{aligned}$$

   Uvědomme si, že $zr_1, zr_2, \ldots, zr_n \in R$, takže $zx \in I$.
   Chceme: $0 \in I$.
   Je $0 \in R$, takže $0 \cdot a_1 + 0 \cdot a_2 + \cdots + 0 \cdot a_n \in I$. Ovšem $0 \cdot a_1 + 0 \cdot a_2 + \cdots + 0 \cdot a_n = 0 + 0 + \cdots + 0 = 0$, tudíž $0 \in I$.

2. $\{a_1, a_2, \ldots, a_n\} \subseteq I$: Buď i celé číslo, $1 \leq i \leq n$. Chceme: $a_i \in I$.
   Je $0, 1 \in R$, takže $0 \cdot a_1 + \cdots + 0 \cdot a_{i-1} + 1 \cdot a_i + 0 \cdot a_{i+1} + \cdots + \cdot 0 \cdot a_n \in I$. Ovšem $0 \cdot a_1 + \cdots + 0 \cdot a_{i-1} + 1 \cdot a_i + 0 \cdot a_{i+1} + \cdots + 0 \cdot a_n = 0 + \cdots + 0 + a_i + 0 \cdots + 0 = a_i$, tudíž $a_i \in I$.

3. pro všechna $K \subseteq R$ platí: jestliže K je ideál v okruhu R a $\{a_1, \ldots, a_n\} \subseteq K$, pak $I \subseteq K$.
   Nechť $K \subseteq R$, K je ideál v okruhu R, $\{a_1, a_2, \ldots, a_n\} \subseteq K$. Chceme: $I \subseteq K$.
   Buď $x \in I$. Je třeba ukázat, že $x \in K$. Je $x = r_1 a_1 + r_2 a_2 + \cdots + r_n a_n$, kde $r_1, r_2, \ldots, r_n \in R$. Protože $r_1 \in R$, $a_1 \in K$ (víme, že $\{a_1, a_2, \ldots, a_n\} \subseteq K$) a K je ideál v okruhu R, je $r_1 a_1 \in K$; obdobně se zdůvodní, že $r_2 a_2, \ldots, r_n a_n \in K$. Celkem máme $r_1 a_1, r_2 a_2, \ldots, r_n a_n \in K$ a také víme, že K je ideál. Proto $r_1 a_1 + r_2 a_2 + \cdots + r_n a_n \in K$, $x \in K$.

8.3.21. Definice. Nechť R je okruh, I je ideál v okruhu R. Ideál I se nazývá **hlavní**, pokud I je generován jedním prvkem okruhu R (tedy pokud existuje $a \in R$ tak, že $I = (a)$). Jestliže každý ideál v okruhu R je hlavní, pak R se nazývá **okruh hlavních ideálů**.

8.3.22. Příklady.

1. V každém okruhu R je ideál $\{0\}$ hlavní. Je totiž $\{0\} = (\{0\}) = (0)$.

2. Nechť R je okruh s jednotkovým prvkem. Pak ideál R je hlavní. Je totiž $R = (\{1\}) = (1)$. Zdůvodnění:
   R je ideál v R: to platí
   $\{1\} \subseteq R$: to platí, protože 1 je jednotkový prvek okruhu R
   Nechť $K \subseteq R$, K je ideál v okruhu R, $\{1\} \subseteq K$. Chceme: $R \subseteq K$. Zvolme libovolně $x \in R$. Ukážeme, že $x \in K$. Je $1 \in K$ (protože $\{1\} \subseteq K$) a také K je ideál, což dává $x \cdot 1 \in K$, $x \in K$.

3. Každé těleso je okruh hlavních ideálů. Zdůvodnění: V tělese T jsou pouze nevlastní ideály $\{0\}$ a T (viz 8.3.14.) a tyto ideály jsou hlavní (viz výše body 1 a 2).

8.3.23. Tvrzení. *Obor integrity celých čísel $\mathbb{Z}$ je okruh hlavních ideálů.*

Důkaz. Nechť I je ideál v $\mathbb{Z}$. Ukážeme, že ideál I je hlavní. Jestliže $I = \{0\}$, pak I je hlavní, protože $\{0\} = (0)$. Nechť tedy $I \neq \{0\}$. Protože $0 \in I$ (to dle definice splňuje každý ideál), existuje $b \in I$, $b \neq 0$. Buď $M = \{x \in I |\ x > 0\}$. Je $M \subseteq I$. Ukážeme nyní, že $M \neq \emptyset$. Je-li $b > 0$, je $b \in M$ a jsme hotovi. Nechť tedy $b < 0$. Máme: $-1 \in \mathbb{Z}$, $b \in I$, I je ideál v $\mathbb{Z}$, takže $(-1) \cdot b \in I$, $-b \in I$; stačí si uvědomit, že $-b > 0$, tudíž $-b \in M$. Víme tedy, že $M \neq \emptyset$, $M \subseteq \mathbb{N}$. Proto existuje $a = \min M$ (každá neprázdná množina přirozených čísel má nejmenší prvek). Je $a \in M$, specielně $a > 0$ a $a \in I$. Ukážeme, že $I = (a)$; pak bude jasné, že ideál I je hlavní. $\mathbb{Z}$ je asociativní komutativní okruh s jednotkovým prvkem a můžeme použít větu 8.3.20., podle které $(a) = \{ra |\ r \in \mathbb{Z}\}$. Postačí již jen dokázat, že $\{ra |\ r \in \mathbb{Z}\} = I$.
$\{ra |\ r \in \mathbb{Z}\} \subseteq I$:
Nechť r je celé číslo. Chceme: $ra \in I$. Ovšem $a \in I$ a I je ideál v $\mathbb{Z}$, takže $ra \in I$.
$I \subseteq \{ra |\ r \in \mathbb{Z}\}$:
Nechť $x \in I$. Chceme: $x \in \{ra |\ r \in \mathbb{Z}\}$. Číslo x vydělíme se zbytkem číslem a (každé celé číslo lze vydělit se zbytkem každým kladným celým číslem): $x = ra + z$, kde r, z jsou celá čísla, $0 \leq z < a$. Dokážeme, že $z = 0$; pak bude $x = ra$ a důkaz bude hotov. Předpokládejme, že $z \neq 0$. Je tedy $z > 0$. Je $z = x - ra = x + (-r)a$. Víme, že $x \in I$. Dále $-r \in \mathbb{Z}$, I je ideál, takže $(-r)a \in I$. Máme $x \in I$, $(-r)a \in I$, I je ideál, tudíž $x + (-r)a \in I$, $z \in I$. Tudíž $z > 0$, $z \in I$, $z \in M$. Je $a = \min M$ a tedy $a \leq z$. Také $z < a$, celkem tedy $a < a$, spor. Nutně tedy $z = 0$.

Víme již, že každé těleso je okruh hlavních ideálů (příklad 8.3.22.) a také $\mathbb{Z}$ je okruh hlavních ideálů. Další příklady okruhů hlavních ideálů poznáme v kapitole 10 nazvané Eukleidovské obory integrity – dokážeme v ní totiž, že každý Eukleidovský obor integrity je okruh hlavních ideálů. Mezi Eukleidovské obory integrity patří například obor integrity celých čísel $\mathbb{Z}$ (tvrzení 8.3.23. je tedy specielním případem obecnějšího tvrzení) a také obor integrity Gaussových celých čísel $\mathbb{Z}[i]$.

Na závěr této kapitoly uvedeme příklad oboru integrity, který není okruhem hlavních ideálů.

8.3.24. Příklad. Uvažme podokruh $\mathbb{Z}[\sqrt{-5}]$ tělesa $\mathbb{C}$. Ukážeme nejprve, že $\sqrt{-5}$ je algebraické celé číslo stupně 2 (viz definici 8.3.10.). Položme $c_0 = 5$, $c_1 = 0$. Čísla c_0, c_1 jsou celá a $c_0 + c_1 \cdot \sqrt{-5} + (\sqrt{-5})^2 = 5 + 0 \cdot \sqrt{-5} + (\sqrt{-5})^2 = 5 + 0 + (-5) = 0$. Dále, nechť d_0, d_1 jsou celá čísla, $d_0 + d_1 \cdot \sqrt{-5} = 0$. Chceme:

$d_0 = d_1 = 0$. Je $d_1 \cdot \sqrt{-5} = -d_0$, $d_1^2 \cdot (-5) = d_0^2$. Předpokládejme, že $d_1 \neq 0$; pak $d_1^2 \cdot (-5) < 0$, $0 \leq d_0^2$, takže $d_1^2 \cdot (-5) < d_0^2$, spor. Nutně tedy $d_1 = 0$, $d_0 + 0 \cdot \sqrt{-5} = 0$, $d_0 + 0 = 0$, $d_0 = 0$. Nyní je dokázáno, že $\sqrt{-5}$ je algebraické celé číslo stupně 2. Dle 8.3.12. je $\mathbb{Z}[\sqrt{-5}] = \{u_0 + u_1 \cdot \sqrt{-5} |\ u_0, u_1 \in \mathbb{Z}\}$, přičemž vyjádření prvků okruhu $\mathbb{Z}[\sqrt{-5}]$ ve tvaru $u_0 + u_1 \cdot \sqrt{-5}$, kde u_0, u_1 jsou celá čísla, je jednoznačné. $\mathbb{Z}[\sqrt{-5}]$ je podokruh tělesa, takže je to obor integrity. Platí: $\mathbb{Z}[\sqrt{-5}]$ je obor integrity, který není okruhem hlavních ideálů.

Zdůvodnění:

Je $3, 2 + \sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]$. Ukážeme, že ideál $(3, 2 + \sqrt{-5})$ není hlavní. Využijeme přitom zobrazení $N : \mathbb{Z}[\sqrt{-5}] \to \mathbb{N}_0$ definované následovně: pro celá čísla a, b je

$$N(a + b\sqrt{-5}) = a^2 + 5b^2.$$

Zobrazení N má důležitou vlastnost: pro všechna $\alpha, \beta \in \mathbb{Z}[\sqrt{-5}]$ je

$$N(\alpha\beta) = N(\alpha)N(\beta).$$

Opravdu, nechť $\alpha \in \mathbb{Z}[\sqrt{-5}]$, $\alpha = a + b\sqrt{-5}$, $\beta \in \mathbb{Z}[\sqrt{-5}]$, $\beta = c + d\sqrt{-5}$, kde a, b, c, d jsou celá čísla. Počítejme:

$$\begin{aligned} \alpha\beta &= (a + b\sqrt{-5})(c + d\sqrt{-5}) \\ &= ac + ad\sqrt{-5} + bc\sqrt{-5} - 5bd \\ &= (ac - 5bd) + (ad + bc)\sqrt{-5} \end{aligned}$$

$$\begin{aligned} N(\alpha\beta) &= N((ac - 5bd) + (ad + bc)\sqrt{-5}) \\ &= (ac - 5bd)^2 + 5(ad + bc)^2 \\ &= a^2c^2 - 10abcd + 25b^2d^2 + 5(a^2d^2 + 2abcd + b^2c^2) \\ &= a^2c^2 - 10abcd + 25b^2d^2 + 5a^2d^2 + 10abcd + 5b^2c^2 \\ &= a^2c^2 + 25b^2d^2 + 5a^2d^2 + 5b^2c^2 \end{aligned}$$

$$\begin{aligned} N(\alpha)N(\beta) &= N(a + b\sqrt{-5})N(c + d\sqrt{-5}) \\ &= (a^2 + 5b^2)(c^2 + 5d^2) \\ &= a^2c^2 + 5a^2d^2 + 5b^2c^2 + 25b^2d^2 \\ &= a^2c^2 + 25b^2d^2 + 5a^2d^2 + 5b^2c^2 \\ &= N(\alpha\beta) \end{aligned}$$

Postupujme sporem. Předpokládáme tedy, že $(3, 2+\sqrt{-5})$ je hlavní ideál. Pak existuje $\alpha \in \mathbb{Z}[\sqrt{-5}]$, $(\alpha) = (3, 2+\sqrt{-5})$. Je $\mathbb{Z}[\sqrt{-5}]$ asociativní komutativní okruh s jednotkovým prvkem, můžeme tedy použít větu 8.3.20. Dle této věty

$$(\alpha) = \{\beta\alpha |\ \beta \in \mathbb{Z}[\sqrt{-5}]\},\ (3, 2+\sqrt{-5}) = \{\beta\cdot 3+\gamma\cdot(2+\sqrt{-5}) |\ \beta, \gamma \in \mathbb{Z}[\sqrt{-5}]\}.$$

Je $3 \in (3, 2+\sqrt{-5})$, takže $3 \in (\alpha)$, $3 = \beta\alpha$ pro nějaké $\beta \in \mathbb{Z}[\sqrt{-5}]$. Pak $N(3) = N(\beta\alpha) = N(\beta)N(\alpha), 9 = N(\beta)N(\alpha)$. Uvědomme si, že $N(\alpha), N(\beta) \in \mathbb{N}_0$, což dává $N(\alpha) \in \{1, 3, 9\}$. Jsou tedy pouze tři možnosti pro hodnotu $N(\alpha)$.Uvidíme dále, že každá z těchto tří možností dá spor. Tím bude dokázáno, že ideál $(3, 2+\sqrt{-5})$ není hlavní. Nechť $\alpha = a + b\sqrt{-5}$, kde a, b jsou celá čísla. Je tedy $N(\alpha) = a^2 + 5b^2$.

1. $N(\alpha) = 1$:
   Máme $a^2 + 5b^2 = 1$. Případ $b \neq 0$ dává $b^2 \geq 1$, $5b^2 \geq 5$, $1 = a^2 + 5b^2 \geq 5b^2 \geq 5$, $1 \geq 5$, spor. Musí tedy být $b = 0$. Pak $a^2 = 1$, $a \in \{1, -1\}$.
   $a = 1$:
   Je $\alpha = 1 + 0 \cdot \sqrt{-5} = 1$. Máme $\alpha \in (\alpha)$, takže $\alpha \in (3, 2+\sqrt{-5})$, $1 \in (3, 2+\sqrt{-5})$. Pak $1 = \beta\cdot 3+\gamma\cdot(2+\sqrt{-5})$ pro nějaká $\beta, \gamma \in \mathbb{Z}[\sqrt{-5}]$. Buďte $\beta = u_0 + u_1 \cdot \sqrt{-5}$, $\gamma = v_0 + v_1 \cdot \sqrt{-5}$, kde u_0, u_1, v_0, v_1 jsou celá čísla. Počítejme:

   $$\begin{aligned} \beta \cdot 3 + \gamma \cdot (2 + \sqrt{-5}) &= (u_0 + u_1\sqrt{-5}) \cdot 3 + (v_0 + v_1\sqrt{-5}) \cdot (2 + \sqrt{-5}) \\ &= 3u_0 + 3u_1\sqrt{-5} + 2v_0 + 2v_1\sqrt{-5} + v_0\sqrt{-5} - 5v_1 \\ &= (3u_0 + 2v_0 - 5v_1) + (3u_1 + v_0 + 2v_1)\sqrt{-5} \end{aligned}$$

   Je tedy $3u_0+2v_0-5v_1 = 1$, $3u_1+v_0+2v_1 = 0$; pak $3u_0+2v_0-5v_1 = 1$, $-6u_1 - 2v_0 - 4v_1 = 0$ a sečtením dostaneme $3u_0 - 9v_1 - 6u_1 = 1$, což dává $3(u_0 - 3v_1 - 2u_1) = 1$, číslo 1 je celočíselným násobkem čísla 3, spor.
   $a = -1$:
   Je $\alpha = -1+0\cdot\sqrt{-5} = -1$. Máme $\alpha \in (\alpha)$, takže $\alpha \in (3, 2+\sqrt{-5})$, $-1 \in (3, 2 + \sqrt{-5})$. Protože $(3, 2 + \sqrt{-5})$ je ideál, je $-(-1) \in (3, 2 + \sqrt{-5})$, $1 \in (3, 2 + \sqrt{-5})$. To však dává spor, jak jsme před chvílí ukázali.

2. $N(\alpha) = 3$:
   Máme $a^2 + 5b^2 = 3$. Případ $b \neq 0$ dává $b^2 \geq 1$, $5b^2 \geq 5$, $3 = a^2 + 5b^2 \geq 5b^2 \geq 5$, $3 \geq 5$, spor. Případ $b = 0$ dává $a^2 = 3$, spor (čtverec celého čísla nemůže být roven číslu 3).

3. $N(\alpha) = 9$:
Máme $a^2 + 5b^2 = 9$. Případ $b \notin \{0, 1, -1\}$ dává $b^2 \geq 4$, $5b^2 \geq 20$, $9 = a^2 + 5b^2 \geq 5b^0 \geq 20$, $9 \geq 20$, spor. Musí tedy být $b \in \{0, 1, -1\}$. Probereme postupně tři možnosti pro hodnotu čísla b. Všechny dají spor.
$b = 0$:
Je $a^2 = 9$, $a \in \{3, -3\}$. Předpokládejme nejdříve, že $a = 3$. Pak $\alpha = 3 + 0 \cdot \sqrt{-5} = 3$, $(3) = (3, 2 + \sqrt{-5})$. Je $2 + \sqrt{-5} \in (3, 2 + \sqrt{-5})$, takže $2 + \sqrt{-5} \in (3)$. Pak $2 + \sqrt{-5} = \beta \cdot 3$ pro nějaké $\beta \in \mathbb{Z}[\sqrt{-5}]$. Nechť $\beta = c + d\sqrt{-5}$, kde c, d jsou celá čísla. Potom $2 + \sqrt{-5} = (c + d\sqrt{-5}) \cdot 3 = 3c + 3d\sqrt{-5}$, a tedy $2 = 3c$, $1 = 3d$, spor (číslo 1 není celočíselným násobkem čísla 3). Nyní předpokládejme, že $a = -3$. Pak $\alpha = -3 + 0 \cdot \sqrt{-5} = -3$, $(-3) = (3, 2 + \sqrt{-5})$. Je $2 + \sqrt{-5} \in (3, 2+\sqrt{-5})$, takže $2+\sqrt{-5} \in (-3)$. Pak $2+\sqrt{-5} = \gamma \cdot (-3)$ pro nějaké $\gamma \in \mathbb{Z}[\sqrt{-5}]$. Nechť $\gamma = e + f\sqrt{-5}$, kde e, f jsou celá čísla. Potom $2 + \sqrt{-5} = (e + f\sqrt{-5}) \cdot (-3) = (-3e - 3f\sqrt{-5})$, a tedy $2 = -3e$, $1 = -3f$, spor (číslo 1 není celočíselným násobkem čísla -3).
$b = 1$:
Je $a^2 + 5 = 9$, $a^2 = 4$, $a \in \{2, -2\}$. Předpokládejme nejdříve, že $a = 2$. Pak $\alpha = 2+\sqrt{-5}$, $(2+\sqrt{-5}) = (3, 2+\sqrt{-5})$. Je $3 \in (3, 2+\sqrt{-5})$, takže $3 \in (2 + \sqrt{-5})$. Pak $3 = \beta \cdot (2 + \sqrt{-5})$ pro nějaké $\beta \in \mathbb{Z}[\sqrt{-5}]$. Nechť $\beta = c + d\sqrt{-5}$, kde c, d jsou celá čísla. Potom $3 = (c + d\sqrt{-5})(2 + \sqrt{-5}) = 2c + 2d\sqrt{-5} + c\sqrt{-5} - 5d = (2c - 5d) + (c + 2d)\sqrt{-5}$ a tedy $2c - 5d = 3$, $c + 2d = 0$. Dostáváme $-3d = 1$, spor (číslo 1 není celočíselným násobkem čísla -3). Předpokládejme nyní, že $a = -2$. Pak $\alpha = -2+\sqrt{-5}$, $(-2+\sqrt{-5}) = (3, 2+\sqrt{-5})$. Je $3 \in (3, 2+\sqrt{-5})$, takže $3 \in (-2+\sqrt{-5})$. Pak $3 = \gamma \cdot (-2+\sqrt{-5})$ pro nějaké $\gamma \in \mathbb{Z}[\sqrt{-5}]$. Nechť $\gamma = e + f\sqrt{-5}$, kde e, f jsou celá čísla. Potom $3 = (e + f\sqrt{-5})(-2 + \sqrt{-5}) = -2e - 2f\sqrt{-5} + e\sqrt{-5} - 5f = (-2e - 5f) + (e - 2f)\sqrt{-5}$ a tedy $-2e - 5f = 3$, $e - 2f = 0$. Dostáváme $-3f = 1$, spor (číslo 1 není celočíselným násobkem čísla -3).
$b = -1$:
Je $a^2 + 5 = 9$, $a^2 = 4$, $a \in \{2, -2\}$. Předpokládejme nejdříve, že $a = 2$. Pak $\alpha = 2-\sqrt{-5}$, $(2-\sqrt{-5}) = (3, 2+\sqrt{-5})$. Je $3 \in (3, 2+\sqrt{-5})$, takže $3 \in (2 - \sqrt{-5})$. Pak $3 = \beta \cdot (2 - \sqrt{-5})$ pro nějaké $\beta \in \mathbb{Z}[\sqrt{-5}]$. Nechť $\beta = c + d\sqrt{-5}$, kde c, d jsou celá čísla. Potom $3 = (c + d\sqrt{-5})(2 - \sqrt{-5}) = 2c + 2d\sqrt{-5} - c\sqrt{-5} + 5d = (2c + 5d) + (-c + 2d)\sqrt{-5}$ a tedy $2c + 5d = 3$, $-c + 2d = 0$. Dostáváme $3d = 1$, spor (číslo 1 není

celočíselným násobkem čísla 3). Předpokládejme nyní, že $a = -2$. Pak $\alpha = -2-\sqrt{-5}$, $(-2-\sqrt{-5}) = (3, 2+\sqrt{-5})$. Je $3 \in (3, 2+\sqrt{-5})$, takže $3 \in (-2-\sqrt{-5})$. Pak $3 = \gamma\cdot(-2-\sqrt{-5})$ pro nějaké $\gamma \in \mathbb{Z}[\sqrt{-5}]$. Nechť $\gamma = e + f\sqrt{-5}$, kde e, f jsou celá čísla. Potom $3 = (e + f\sqrt{-5})(-2 - \sqrt{-5}) = -2e - 2f\sqrt{-5} - e\sqrt{-5} + 5f = (-2e + 5f) + (-e - 2f)\sqrt{-5}$ a tedy $-2e + 5f = 3$, $-e - 2f = 0$. Dostáváme $3f = 1$, spor (číslo 1 není celočíselným násobkem čísla 3).

9 Příklady okruhů

9.1 Okruh kvadratických celých čísel

Nejprve k názvu této části. Co jsou kvadratická celá čísla? Jsou to algebraická celá čísla stupně 2 (jedná se tedy pouze o jiné pojmenování).

9.1.1. Definice. Nechť a je celé číslo. Číslo a se nazývá **bezčtvercové**, pokud pro všechna kladná celá čísla b platí:

$$b^2/a \Longrightarrow b = 1.$$

9.1.2. Tvrzení. *Nechť a je celé číslo. Číslo a je bezčtvercové právě tehdy, když pro všechna prvočísla p platí: $\neg(p^2/a)$.*

Důkaz.

1. Předpokládejme, že a je bezčtvercové. Nechť p je libovolné prvočíslo. Chceme: $\neg(p^2/a)$. Předpokládejme naopak, že p^2/a. Protože a je bezčtvercové, je $p = 1$. To je spor.

2. Předokládejme, že pro všechna prvočísla p platí: $\neg(p^2/a)$. Chceme: a je bezčtvercové. Buď b kladné celé číslo, b^2/a. Musíme ukázat, že $b = 1$. Předpokládejme naopak, že $b \neq 1$. Existuje tedy prvočíslo p takové, že p/b. Pak $b = pc$ pro nějaké celé číslo c. Jelikož b^2/a, máme $a = b^2d$ pro nějaké celé číslo d. Pak $a = b^2d = (pc)^2d = p^2c^2d$. Vidíme, že p^2/a. To je spor.

9.1.3. Tvrzení. *Nechť a je celé číslo. Platí: a je bezčtvercové právě tehdy, když $-a$ je bezčtvercové.*

Důkaz.

1. Předpokládejme, že a je bezčtvercové. Chceme: $-a$ je bezčtvercové. Nechť b je kladné celé číslo, $b^2/-a$. Musíme ukázat, že $b = 1$. Existuje celé číslo c, $-a = b^2c$. Pak $a = b^2(-c)$. Protože a je bezčvercové, je $b = 1$.

2. Předpokládejme, že $-a$ je bečtvercové. Chceme: a je bezčtvercové. Dle již dokázaného je číslo $-(-a)$ bezčtvercové. Stačí si uvědomit, že $-(-a) = a$.

9.1.4. Tvrzení. *Nechť $a = p_1p_2 \cdots p_k$, kde $p_1, p_2, \ldots, p_k$ jsou vzájemně různá prvočísla. Pak a je bezčtvercové.*

Důkaz. Použijeme 9.1.2. Buď p prvočíslo. Chceme: $\neg(p^2/a)$. Předpokládejme, že p^2/a. Pak $a = p^2b$, kde b je kladné celé číslo. Nechť $b = q_1q_2 \cdots q_l$ je prvočíselný rozklad čísla b (pro $b = 1$ je $l = 0$). Pro číslo a nyní máme dva prvočíselné rozklady: $a = p_1p_2 \cdots p_k$ a $a = ppq_1q_2 \cdots q_l$. Tyto rozklady jsou různé, jelikož prvočísla $p_1, p_2, \ldots, p_k$ jsou vzájemně různá. Dostali jsme spor s jednoznačností prvočíselného rozkladu.

9.1.5. Příklad. Určíme všechna bezčtvercová celá čísla a splňující $0 \leq a \leq 20$:

$0 = 2^2 \cdot 0$	NENÍ bezčtvercové
1	JE bezčtvercové
2	JE bezčtvercové
3	JE bezčtvercové
$4 = 2^2$	NENÍ bezčtvercové
5	JE bezčtvercové
$6 = 2 \cdot 3$	JE bezčtvercové
7	JE bezčtvercové
$8 = 2^2 \cdot 2$	NENÍ bezčtvercové
$9 = 3^2$	NENÍ bezčtvercové
$10 = 2 \cdot 5$	JE bezčtvercové
11	JE bezčtvercové
$12 = 2^2 \cdot 3$	NENÍ bezčtvercové
13	JE bezčtvercové
$14 = 2 \cdot 7$	JE bezčtvercové
$15 = 3 \cdot 5$	JE bezčtvercové
$16 = 4^2$	NENÍ bezčtvercové
17	JE bezčtvercové
$18 = 3^2 \cdot 2$	NENÍ bezčtvercové
19	JE bezčtvercové
$20 = 2^2 \cdot 5$	NENÍ bezčtvercové

Seznam všech bezčtvercových celých čísel a splňujících $0 \leq a \leq 20$: $1, 2, 3, 5, 6, 7, 10, 11, 13, 14, 15, 17, 19$.

Ukážeme nyní, že každé nenulové celé číslo lze rozložit na součin čtverce kladného celého čísla a bezčtvercového celého čísla.

9.1.6. Tvrzení. *Nechť D je celé číslo, $D \neq 0$. Pak existují celá čísla c, d taková, že $c > 0$, d je bezčtvercové, $D = c^2 d$.*

Důkaz. Rozlišíme tři případy.

1. $D = 1$: Položíme $c = d = 1$.

2. $D > 1$: Buď
$$D = p_1^{e_1} \cdots p_k^{e_k}$$
prvočíselný rozklad čísla D, kde $p_1, p_2, \ldots, p_k$ jsou vzájemně různá prvočísla, $e_1, e_2, \ldots, e_k$ jsou kladná celá čísla. Pro $i = 1, \ldots, k$ je
$$e_i = 2s_i + t_i$$

kde s_i, t_i jsou celá čísla, $s_i \geq 0$, $t_i \in \{0, 1\}$. Je

$$\begin{aligned} D &= p_1^{e_1} \cdots p_k^{e_k} \\ &= p_1^{2s_1+t_1} \cdots p_k^{2s_k+t_k} \\ &= (p_1^{2s_1} \cdots p_k^{2s_k})(p_1^{t_1} \cdots p_k^{t_k}) \\ &= ((p_1^{s_1})^2 \cdots (p_k^{s_k})^2)(p_1^{t_1} \cdots p_k^{t_k}) \\ &= (p_1^{s_1} \cdots p_k^{s_k})^2 (p_1^{t_1} \cdots p_k^{t_k}) \end{aligned}$$

Položíme $c = p_1^{s_1} \cdots p_k^{s_k}$, $d = p_1^{t_1} \cdots p_k^{t_k}$. Pak $D = c^2 d$, c je kladné celé číslo, d je bezčtvercové celé číslo – pro $t_1 = \cdots = t_k = 0$ je $d = 1$, v ostatních případech je d bezčtvercové celé číslo dle 9.1.4.

3. $D < 0$: Je $-D > 0$ a dle již dokázaného máme $-D = c^2 d$ pro nějaká celá čísla c, d, $c > 0$, d bezčtvercové. Pak $D = c^2(-d)$ a stačí si uvědomit, že $-d$ je bezčtvercové celé číslo (viz 9.1.3.).

9.1.7. Příklad. Najdeme kladné celé číslo c a bezčtvercové celé číslo d splňující $580025176500 = c^2 d$. Můžeme postupovat tak, jako v důkazu tvrzení 9.1.6. Je

$$\begin{aligned} 580025176500 &= 2^2 \cdot 3 \cdot 5^3 \cdot 7^4 \cdot 11^5 \\ &= 2^{2\cdot 1+0} \cdot 3^{2\cdot 0+1} \cdot 5^{2\cdot 1+1} \cdot 7^{2\cdot 2+0} \cdot 11^{2\cdot 2+1} \\ &= (2^1 \cdot 3^0 \cdot 5^1 \cdot 7^2 \cdot 11^2)^2 \cdot 2^0 \cdot 3^1 \cdot 5^1 \cdot 7^0 \cdot 11^1 \\ &= 59290^2 \cdot 165 \end{aligned}$$

Vezmeme tedy $c = 59290$ a $d = 165$.

Buď d bezčtvercové celé číslo, $d \neq 1$. Položme

$$\theta = \begin{cases} \sqrt{d} & \text{pokud } d \equiv 2\ (4) \text{ nebo } d \equiv 3\ (4) \\ \frac{-1+\sqrt{d}}{2} & \text{pokud } d \equiv 1\ (4) \end{cases}$$

Uvědomme si, že případ $d \equiv 0\ (4)$ nenastává, protože $d \equiv 0\ (4)$ znamená $4/d - 0$, $4/d$, $2^2/d$.

Dále si všimněme, že číslo θ je jednoznačně určeno číslem d, takže místo θ bychom vlastně měli přesněji psát $\theta(d)$ či θ_d.

9.1.8. Tvrzení. *Nechť d je bezčtvercové celé číslo, $d \neq 1$. Pak platí:*

1. *číslo $\sqrt{d}$ není racionální*

2. *číslo θ není racionální.*

Důkaz.

1. Provedeme důkaz sporem. Předpokládejme, že $\sqrt{d} = q$, kde q je racionální číslo. Jsou dvě možnosti:

   (a) $d < 0$:
   $d = q^2$, $q^2 < 0$, spor

   (b) $d > 1$:
   Nechť $q = \frac{a}{b}$, kde a, b jsou nesoudělná kladná celá čísla.

$$\begin{aligned} q &= \frac{a}{b} \\ q^2 &= \frac{a^2}{b^2} \\ d &= \frac{a^2}{b^2} \\ b^2 d &= a^2 \end{aligned}$$

   Buď p prvočíslo, p/d. Pak $d = pk$, kde k je kladné celé číslo. Je $b^2pk = a^2$, takže p/a^2. Protože p je prvočíslo, dostáváme p/a. Pak $a = pl$, kde l je kladné celé číslo. Platí:

$$\begin{aligned} b^2pk &= p^2l^2 \\ b^2k &= pl^2 \end{aligned}$$

   Vidíme, že p/b^2k. Protože p je prvočíslo, máme p/b nebo p/k. Uvidíme, že oba případy dají spor.
   p/b: Víme již, že p/a. Celkem tedy p/a a p/b, což je spor s tím, že a, b jsou nesoudělná.
   p/k: Máme $k = pm$, kde m je celé číslo. Pak $d = pk = p \cdot pm = p^2m$, p^2/d, což je spor s tím, že d je bezčtvercové celé číslo.

2. Opět provedeme důkaz sporem. Předpokládejme, že $\theta = q$, kde q je racionální číslo. Jsou dvě možnosti:

(a) $d \equiv 2\ (4)$ nebo $d \equiv 3\ (4)$:
Je $\theta = \sqrt{d}$, takže $\sqrt{d} = q$, $\sqrt{d}$ je racionální číslo. Dostali jsme spor s již dokázanou první částí tvrzení 9.1.8.

(b) $d \equiv 1\ (4)$:
Je $\theta = \frac{-1+\sqrt{d}}{2}$, takže $\frac{-1+\sqrt{d}}{2} = q$, $\sqrt{d} = 2q + 1$. Protože q je racionální číslo, je také $2q + 1$ racionální číslo, takže $\sqrt{d}$ je racionální číslo. Opět jsme dostali spor s již dokázanou první částí tvrzení 9.1.8.

9.1.9. Tvrzení. *Nechť d je bezčtvercové celé číslo, $d \neq 1$. Pak platí: číslo θ je algebraické celé číslo stupně* 2.

Důkaz. Jistě θ je komplexní číslo. Musíme ukázat, že θ splňuje podmínky z definice 8.3.10.

1. Chceme: Existují celá čísla c_0, c_1 taková, že $c_0 + c_1\theta + \theta^2 = 0$.
Rozlišíme dva případy:

   (a) $d \equiv 2\ (4)$ nebo $d \equiv 3\ (4)$:
   Je $\theta = \sqrt{d}$. Položme $c_0 = -d$, $c_1 = 0$. Čísla c_0, c_1 jsou celá a

   $$c_0 + c_1\theta + \theta^2 = (-d) + 0 \cdot \sqrt{d} + (\sqrt{d})^2 = -d + 0 + d = 0.$$

   (b) $d \equiv 1\ (4)$:
   Je $\theta = \frac{-1+\sqrt{d}}{2}$. Položme $c_0 = \frac{1-d}{4}$, $c_1 = 1$. Číslo c_1 je celé. Ukážeme, že také číslo c_0 je celé. Je $1 \equiv d\ (4)$, takže $4/1 - d$, $\frac{1-d}{4}$ je celé číslo, c_0 je celé číslo. Počítejme:

   $$\begin{aligned} c_0 + c_1\theta + \theta^2 &= \frac{1-d}{4} + 1 \cdot \frac{-1+\sqrt{d}}{2} + \left(\frac{-1+\sqrt{d}}{2}\right)^2 \\ &= \frac{1-d}{4} + \frac{-1+\sqrt{d}}{2} + \frac{1-2\sqrt{d}+d}{4} \\ &= \frac{1-d-2+2\sqrt{d}+1-2\sqrt{d}+d}{4} \\ &= \frac{0}{4} \\ &= 0 \end{aligned}$$

2. Chceme: Pro všechna celá čísla d_0, d_1 platí: jestliže $d_0 + d_1\theta = 0$, pak $d_0 = d_1 = 0$.
   Nechť d_0, d_1 jsou celá čísla, $d_0 + d_1\theta = 0$. Chceme: $d_0 = d_1 = 0$. Předpokládejme, že $d_1 \neq 0$. Pak $\theta = \frac{-d_0}{d_1}$. Jelikož čísla d_0, d_1 jsou celá, je θ číslo racionální. To je spor s 9.1.8. Nutně tedy $d_1 = 0$. Pak $d_0 + 0 \cdot \theta = 0$, $d_0 = 0$.

Nechť d je bezčtvercové celé číslo, $d \neq 1$. Připomeňme, že

$$\theta = \begin{cases} \sqrt{d} & \text{pokud } d \equiv 2\ (4) \text{ nebo } d \equiv 3\ (4) \\ \frac{-1+\sqrt{d}}{2} & \text{pokud } d \equiv 1\ (4) \end{cases}$$

Položme

$$R_d = \mathbb{Z}[\theta]$$

Okruh R_d nazýváme **okruh kvadratických celých čísel**.
Dle 9.1.9 je θ algebraické celé číslo stupně 2. Věta 8.3.12 pak dává:

$$R_d = \{a + b\theta \mid a, b \in \mathbb{Z}\},$$

přičemž vyjádření prvků okruhu R_d ve tvaru $a + b\theta$, kde a, b jsou celá čísla, je jednoznačné.
Uvedeme dva význačné případy:

- Okruh **Gaussových celých čísel** je okruh $R_{-1} = \mathbb{Z}[\sqrt{-1}] = \mathbb{Z}[i]$.
- Okruh **Eisensteinových celých čísel** je okruh $R_{-3} = \mathbb{Z}[\theta]$, kde $\theta = \frac{-1+\sqrt{-3}}{2} = \frac{-1+i\sqrt{3}}{2}$; v tomto případě se často používá označení $\omega = \frac{-1+\sqrt{-3}}{2}$ a okruh Eisensteinových celých čísel je tedy okruh $\mathbb{Z}[\omega]$.

Následující dvě tvrzení ospravedlňují název "okruh kvadratických celých čísel".

9.1.10. Tvrzení. *Nechť d je bezčtvercové celé číslo, $d \neq 1$. Pak platí: každý prvek okruhu R_d je algebraické celé číslo stupně nejvýše 2.*

Důkaz. Nechť $\alpha \in R_d$. Je $\alpha = a + b\theta$ pro nějaká celá čísla a, b. Chceme: α je algebraické celé číslo stupně nejvýše 2. Rozlišíme dva případy:

1. $b = 0$:
   Je $\alpha = a + 0 \cdot \theta = a + 0 = a$, takže α je celé číslo a tedy α je algebraické celé číslo stupně 1.

2. $b \neq 0$:
   Jistě α je komplexní číslo (protože θ je komplexní číslo, a, b jsou celá čísla). Ukážeme, že α je algebraické celé číslo stupně 2. Musíme ukázat, že α splňuje podmínky uvedené v definici 8.3.10.

   (a) Chceme: Existují celá čísla k_0, k_1 taková, že $k_0 + k_1\alpha + \alpha^2 = 0$.
   Jelikož θ je algebraické celé číslo stupně 2 (viz 9.1.9), existují celá čísla c_0, c_1 taková, že $c_0 + c_1\theta + \theta^2 = 0$. Položme $k_0 = a^2 + b^2c_0 - abc_1$, $k_1 = bc_1 - 2a$. Protože a, b, c_0, c_1 jsou celá čísla, jsou čísla k_0, k_1 celá. Počítejme:

$$\begin{aligned} k_0 + k_1\alpha + \alpha^2 &= (a^2 + b^2c_0 - abc_1) + (bc_1 - 2a)(a + b\theta) + \\ &\quad (a + b\theta)^2 \\ &= a^2 + b^2c_0 - abc_1 + bc_1a + b^2c_1\theta - 2a^2 - 2ab\theta + \\ &\quad a^2 + 2ab\theta + b^2\theta^2 \\ &= b^2c_0 + b^2c_1\theta + b^2\theta^2 \\ &= b^2c_0 + b^2c_1\theta + b^2(-c_0 - c_1\theta) \\ &= b^2c_0 + b^2c_1\theta - b^2c_0 - b^2c_1\theta \\ &= 0 \end{aligned}$$

   (b) Chceme: Pro všechna celá čísla d_0, d_1 platí: jestliže $d_0 + d_1\alpha = 0$, pak $d_0 = d_1 = 0$.
   Nechť d_0, d_1 jsou celá čísla, $d_0 + d_1\alpha = 0$. Pak $d_0 + d_1(a + b\theta) = 0$, $d_0 + d_1a + d_1b\theta = 0$, $(d_0 + d_1a) + d_1b\theta = 0$. Víme, že θ je algebraické celé číslo stupně 2 a $d_0 + d_1a$, d_1b jsou celá čísla. Proto $d_0 + d_1a = 0$ a $d_1b = 0$. Je $b \neq 0$, takže $d_1b = 0$ dává $d_1 = 0$. Pak $d_0 + d_1a = d_0 + 0 \cdot a = d_0 + 0 = d_0$ a tedy $d_0 = 0$.

9.1.11. Tvrzení. *Nechť α je algebraické celé číslo stupně 2. Pak existuje bezčtvercové celé číslo d, $d \neq 1$, takové, že $\alpha \in R_d$.*

Důkaz. Existují celá čísla p, q taková, že $\alpha^2 + p\alpha + q = 0$. Pak

$$\alpha = \frac{-p + j\sqrt{D}}{2}$$

kde $D = p^2 - 4q$, $j \in \{1, -1\}$.

Jistě D je celé číslo. Ukážeme, že $D \neq 0$. Předpokládejme naopak, že $D = 0$. Pak $p^2 = 4q$. Z toho plyne, že číslo p je sudé. Je

$$\alpha = \frac{-p + j \cdot \sqrt{0}}{2} = \frac{-p + j \cdot 0}{2} = \frac{-p}{2}$$

Jelikož číslo p je sudé, je α celé číslo. Pak α je algebraické celé číslo stupně 1, spor. Nutně tedy $D \neq 0$.

Dle 9.1.6 existují celá čísla c, d taková, že $c > 0$, d je bezčtvercové, $D = c^2 d$. Pak $\sqrt{D} = c\sqrt{d}$ a

$$\alpha = \frac{-p + jc\sqrt{d}}{2}$$

Ukážeme, že $d \neq 1$. Předpokládejme naopak, že $d = 1$. Pak $D = c^2$, $c^2 = p^2 - 4q$, $4q = p^2 - c^2$. Vidíme, že číslo $p^2 - c^2$ je sudé. Z toho plyne, že čísla p, c mají stejnou paritu (tedy jsou obě sudá nebo jsou obě lichá). Je

$$\alpha = \frac{-p + jc \cdot \sqrt{1}}{2} = \frac{-p + jc \cdot 1}{2} = \frac{-p + jc}{2}$$

Jelikož čísla p, c mají stejnou paritu, mají stejnou paritu také čísla $-p$ a jc, takže číslo $-p + jc$ je sudé a číslo α je celé. Pak ovšem α je algebraické celé číslo stupně 1, spor. Nutně tedy $d \neq 1$.

Víme nyní, že d je bezčtvercové celé číslo, $d \neq 1$.

Ukážeme, že $\alpha \in R_d$. Připomeňme, že $R_d = \{a + b\theta |\ a, b \in \mathbb{Z}\}$. Rozlišíme 3 případy:

1. $d \equiv 2\ (4)$
   Je $\theta = \sqrt{d}$. Dále,

   $$p^2 \equiv p^2 - 4q = D = c^2 d \equiv c^2 \cdot 2\ (4)$$

   $$p^2 \equiv 2c^2\ (4)$$

   Takže $4 / p^2 - 2c^2$, $p^2 - 2c^2 = 4k$ (k je celé číslo), $p^2 = 2c^2 + 4k$. Vidíme, že číslo p^2 je sudé, takže číslo p je také sudé. Pak $p = 2l$ pro nějaké celé číslo l, $4l^2 = 2c^2 + 4k$, $2l^2 = c^2 + 2k$, $c^2 = 2l^2 - 2k$. Vidíme, že číslo c^2 je sudé, takže číslo c je také sudé. Je

   $$\alpha = \frac{-p}{2} + \frac{jc}{2}\sqrt{d} = \frac{-p}{2} + \frac{jc}{2}\theta$$

   Protože čísla p, c jsou sudá, jsou čísla $\frac{-p}{2}$, $\frac{jc}{2}$ celá a tedy $\alpha \in R_d$.

2. $d \equiv 3\ (4)$
   Je $\theta = \sqrt{d}$. Dále,

$$p^2 \equiv p^2 - 4q = D = c^2 d \equiv c^2 \cdot 3\ (4)$$

$$p^2 \equiv 3c^2\ (4)$$

   Takže $4/p^2 - 3c^2$, $p^2 - 3c^2 = 4k$ (k je celé číslo), $p^2 = 3c^2 + 4k$.

   Předpokládejme, že číslo c je liché. Pak $c = 2l + 1$ (l je celé číslo),

$$p^2 = 3(2l+1)^2 + 4k = 3(4l^2 + 4l + 1) + 4k = 12l^2 + 12l + 3 + 4k$$

$$p^2 = 12l^2 + 12l + 3 + 4k$$

   Z toho plyne, že číslo p^2 je liché a tedy také p je liché. Pak $p = 2m + 1$ (m je celé číslo),

$$\begin{aligned} 4m^2 + 4m + 1 &= 12l^2 + 12l + 3 + 4k \\ 4m^2 + 4m &= 12l^2 + 12l + 2 + 4k \\ 2m^2 + 2m &= 6l^2 + 6l + 1 + 2k \end{aligned}$$

   Dostáváme spor, neboť číslo $2m^2 + 2m$ je sudé a číslo $6l^2 + 6l + 1 + 2k$ je liché. Nutně tedy číslo c je sudé.

   Pak ovšem p^2 je sudé (jelikož $p^2 = 3c^2 + 4k$, c je sudé), a tedy také p je sudé. Je

$$\alpha = \frac{-p}{2} + \frac{jc}{2}\sqrt{d} = \frac{-p}{2} + \frac{jc}{2}\theta$$

   Protože čísla p, c jsou sudá, jsou čísla $\frac{-p}{2}$, $\frac{jc}{2}$ celá a tedy $\alpha \in R_d$.

3. $d \equiv 1\ (4)$
   Je $\theta = \frac{-1+\sqrt{d}}{2}$. Dále,

$$p^2 \equiv p^2 - 4q = D = c^2 d \equiv c^2 \cdot 1\ (4)$$

$$p^2 \equiv c^2\ (4)$$

Takže $4|p^2-c^2$, $p^2-c^2=4k$ (k je celé číslo). Vidíme, že číslo p^2-c^2 je sudé. Z toho plyne, že p, c mají stejnou paritu. Je

$$\begin{aligned}\alpha &= \frac{-p+jc\sqrt{d}}{2}\\ &= \frac{(-p+jc)+jc(-1+\sqrt{d})}{2}\\ &= \frac{-p+jc}{2}+jc\cdot\frac{-1+\sqrt{d}}{2}\\ &= \frac{-p+jc}{2}+jc\theta\end{aligned}$$

Jelikož čísla p, c mají stejnou paritu, mají stejnou paritu také čísla $-p$, jc, takže číslo $\frac{-p+jc}{2}$ je celé a tedy $\alpha\in R_d$.

Množinu všech bezčtvercových celých čísel označme SF. Z tvrzení 9.1.10 a 9.1.11 vyplývá, že

$$\bigcup_{d\in SF,\ d\neq 1} R_d$$

je právě množina všech algebraických celých čísel stupně nejvýše 2.

9.1.12. Poznámka. Pokusíme se nyní aspoň trochu objasnit, proč pro bezčtvercová celá čísla d, $d\neq 1$, $d\equiv 1\ (4)$, klademe $\theta=\frac{-1+\sqrt{d}}{2}$ a nikoli $\theta=\sqrt{d}$ jako v případech $d\equiv 2\ (4)$ nebo $d\equiv 3\ (4)$.

Nechť d je bezčtvercové celé číslo, $d\neq 1$, $d\equiv 1\ (4)$. Je tedy $R_d=\mathbb{Z}[\theta]$, kde $\theta=\frac{-1+\sqrt{d}}{2}$. Všimněme si, že v tomto případě je sice $\mathbb{Z}[\sqrt{d}]\subseteq R_d$, avšak $\mathbb{Z}[\sqrt{d}]\neq R_d$, čili $\mathbb{Z}[\sqrt{d}]\subset R_d$. Je $\sqrt{d}=1+2\theta$, takže $\sqrt{d}\in\mathbb{Z}[\theta]$, $\sqrt{d}\in R_d$. Máme tedy $\mathbb{Z}\subseteq R_d$, $\sqrt{d}\in R_d$, což dává $\mathbb{Z}[\sqrt{d}]\subseteq R_d$. Avšak $\theta\in R_d$, $\theta\notin\mathbb{Z}[\sqrt{d}]$, což zase dává $\mathbb{Z}[\sqrt{d}]\neq R_d$.

Proč $\theta\notin\mathbb{Z}[\sqrt{d}]$? Ukážeme dokonce, že $\theta=\frac{-1+\sqrt{d}}{2}$ (což je algebraické celé číslo stupně 2 dle 9.1.9) nepatří do $\mathbb{Z}[\sqrt{e}]$ pro žádné bezčtvercové celé číslo e, $e\neq 1$. Předpokládejme naopak, že $\theta\in\mathbb{Z}[\sqrt{e}]$ pro nějaké bezčtvercové celé číslo e, $e\neq 1$. Je $\mathbb{Z}[\sqrt{e}]=\{u_0+u_1\sqrt{e}|\ u_0,u_1\in\mathbb{Z}\}$ (použijeme 8.3.9 pro $R=\mathbb{C}$, $S=\mathbb{Z}$, $a=\sqrt{e}$, $n=1$, $s_0=e$, $s_1=0$), takže $\theta=a+b\sqrt{e}$ pro nějaká

celá čísla a, b. Pak

$$\begin{aligned}\frac{-1+\sqrt{d}}{2} &= a+b\sqrt{e}\\ -1+\sqrt{d} &= 2a+2b\sqrt{e}\\ \sqrt{d} &= (2a+1)+2b\sqrt{e}\\ d &= (2a+1)^2+4(2a+1)b\sqrt{e}+4b^2e\end{aligned}$$

Předpokládejme, že $(2a+1)b \neq 0$. Pak

$$\sqrt{e} = \frac{d-(2a+1)^2-4b^2e}{4(2a+1)b}$$

a vidíme, že $\sqrt{e}$ je racionální číslo. To je ve sporu s 9.1.8. Musí tedy být $(2a+1)b = 0$. Nastává aspoň jedna ze dvou variant, obě však dají spor:

- $2a+1=0$: $d = 4b^2e = 2^2b^2e$, $2^2|d$; protože d je bezčtvercové celé číslo a $2>0$, je $2=1$, spor.
- $b=0$: $\sqrt{d} = 2a+1$, $\sqrt{d}$ je celé číslo, spor s 9.1.8.

Nutně tedy θ nepatří do $\mathbb{Z}[\sqrt{e}]$ pro žádné bezčtvercové celé číslo e, $e \neq 1$.

Z již dokázaného vyplývá, že

$$\bigcup_{d\in SF,\ d\neq 1} \mathbb{Z}[\sqrt{d}] \subset \bigcup_{d\in SF,\ d\neq 1} R_d$$

Vidíme, že množina $\bigcup_{d\in SF,\ d\neq 1} \mathbb{Z}[\sqrt{d}]$ neobsahuje všechna kvadratická celá čísla.

Buď d bezčtvercové celé číslo, $d \neq 1$. Nechť a, b jsou celá čísla.

Pro $a+b\theta \in R_d$ klademe

$$N(a+b\theta) = \begin{cases} a^2-db^2 & \text{pokud } d\equiv 2\ (4) \text{ nebo } d\equiv 3\ (4)\\ a^2-ab+\frac{1-d}{4}b^2 & \text{pokud } d\equiv 1\ (4)\end{cases}$$

Číslo $N(a+b\theta)$ se nazývá **norma** čísla (prvku) $a+b\theta$. Všimněme si, že $N(a+b\theta)$ je vždy celé číslo – to je ihned vidět pro $d\equiv 2\ (4)$ nebo $d\equiv 3\ (4)$;

v případě $d \equiv 1\ (4)$ máme $4/1 - d$ a tedy $\frac{1-d}{4}$ je celé číslo. Je tedy norma zobrazení

$$N : R_d \longrightarrow \mathbb{Z}$$

9.1.13. Příklad.

1. Okruh Gaussových celých čísel je okruh $R_{-1} = \mathbb{Z}[\sqrt{-1}] = \mathbb{Z}[i]$. Pro normu Gaussových celých čísel dostáváme vztah

$$N(a + bi) = a^2 + b^2$$

2. Okruh Eisensteinových celých čísel je okruh $R_{-3} = \mathbb{Z}[\theta]$, kde $\theta = \frac{-1+\sqrt{-3}}{2} = \frac{-1+i\sqrt{3}}{2}$. Pro normu Eisensteinových celých čísel dostáváme vztah

$$N(a + b\theta) = a^2 - ab + b^2$$

9.1.14. Tvrzení. *Nechť d je bezčtvercové celé číslo, $d < 0$. Pro každé $\alpha \in R_d$ je $N(\alpha) \geq 0$ a přitom*

$$N(\alpha) = 0 \Longleftrightarrow \alpha = 0$$

Důkaz. Nechť $\alpha = a + b\theta$, kde a, b jsou celá čísla. Rozlišíme dva případy:

1. $d \equiv 2\ (4)$ nebo $d \equiv 3\ (4)$:
   Je
   $$N(\alpha) = a^2 - db^2 = a^2 + (-d)b^2$$
   Čísla a^2 a $(-d)b^2$ jsou nezáporná, takže $N(\alpha) \geq 0$.

   Pro $\alpha = 0$ je $a = b = 0$, takže $N(\alpha) = 0$.

   Nechť $N(\alpha) = 0$. Ukážeme: $\alpha = 0$. Jelikož $0 = N(\alpha) = a^2 + (-d)b^2$ a čísla a^2 a $(-d)b^2$ jsou nezáporná, musí být $a^2 = 0$ a $(-d)b^2 = 0$, takže $a = b = 0$, $\alpha = 0$.

2. $d \equiv 1\ (4)$:
   Je
   $$N(\alpha) = a^2 - ab + \frac{1-d}{4}b^2 = \left(a - \frac{b}{2}\right)^2 + \frac{(-d)b^2}{4}$$

Čísla $(a-\frac{b}{2})^2$ a $\frac{(-d)b^2}{4}$ jsou nezáporná, takže $N(\alpha) \geq 0$.

Pro $\alpha = 0$ je $a = b = 0$, takže $N(\alpha) = 0$.

Nechť $N(\alpha) = 0$. Ukážeme: $\alpha = 0$. Jelikož $0 = N(\alpha) = \left(a - \frac{b}{2}\right)^2 + \frac{(-d)b^2}{4}$ a čísla $\left(a - \frac{b}{2}\right)^2$ a $\frac{(-d)b^2}{4}$ jsou nezáporná, musí být $(a-\frac{b}{2})^2 = 0$ a $\frac{(-d)b^2}{4} = 0$, takže $a - \frac{b}{2} = 0$ a $b = 0$, což dává $a = b = 0$, $\alpha = 0$.

Na závěr této části dokážeme důležitou a často využívanou vlastnost normy.

9.1.15. Věta. *Nechť d je bezčtvercové celé číslo, $d \neq 1$. Pro všechna $\alpha, \beta \in R_d$ platí:*

$$N(\alpha\beta) = N(\alpha)N(\beta)$$

Důkaz. Nechť a, b, u, v jsou celá čísla, $\alpha = a + b\theta$, $\beta = u + v\theta$. Rozlišíme dva případy:

1. $d \equiv 2\ (4)$ nebo $d \equiv 3\ (4)$: Je $\theta = \sqrt{d}$. Počítejme:

$$\begin{aligned} \alpha\beta &= (a + b\theta)(u + v\theta) \\ &= au + av\theta + bu\theta + bv\theta^2 \\ &= au + av\theta + bu\theta + bvd \\ &= (au + bvd) + (av + bu)\theta \end{aligned}$$

Takže

$$\begin{aligned} N(\alpha\beta) &= (au + bvd)^2 - d(av + bu)^2 \\ &= a^2u^2 + 2aubvd + b^2v^2d^2 - d(a^2v^2 + 2avbu + b^2u^2) \\ &= a^2u^2 + 2aubvd + b^2v^2d^2 - da^2v^2 - 2davbu - db^2u^2 \\ &= a^2u^2 + b^2v^2d^2 - da^2v^2 - db^2u^2 \\ &= (a^2 - db^2)(u^2 - dv^2) \\ &= N(\alpha)N(\beta) \end{aligned}$$

2. $d \equiv 1\ (4)$: Je $\theta = \frac{-1+\sqrt{d}}{2}$. Počítejme:

$$\begin{aligned}
\theta^2 &= \left(\frac{-1+\sqrt{d}}{2}\right)^2 \\
&= \frac{1-2\sqrt{d}+d}{4} \\
&= \frac{d-1+2-2\sqrt{d}}{4} \\
&= \frac{d-1}{4} + \frac{2-2\sqrt{d}}{4} \\
&= \frac{d-1}{4} + \frac{1-\sqrt{d}}{2} \\
&= \frac{d-1}{4} - \frac{-1+\sqrt{d}}{2} \\
&= \frac{d-1}{4} - \theta
\end{aligned}$$

Je tedy

$$\theta^2 = \frac{d-1}{4} - \theta$$

Pak

$$\begin{aligned}
\alpha\beta &= (a+b\theta)(u+v\theta) \\
&= au + av\theta + bu\theta + bv\theta^2 \\
&= au + av\theta + bu\theta + bv\left(\frac{d-1}{4} - \theta\right) \\
&= \left(au + \frac{d-1}{4}bv\right) + (av + bu - bv)\theta
\end{aligned}$$

Takže

$$\begin{aligned}
N(\alpha\beta) &= \left(au + \frac{d-1}{4}bv\right)^2 \\
&\quad - \left(au + \frac{d-1}{4}bv\right)\cdot(av + bu - bv) \\
&\quad + \frac{1-d}{4}(av + bu - bv)^2 \\
&= a^2u^2 + \frac{d-1}{2}abuv + \left(\frac{d-1}{4}\right)^2 b^2v^2 \\
&\quad - a^2uv - abu^2 + abuv \\
&\quad - \frac{d-1}{4}abv^2 - \frac{d-1}{4}b^2uv + \frac{d-1}{4}b^2v^2 \\
&\quad + \frac{1-d}{4}a^2v^2 + \frac{1-d}{4}b^2u^2 + \frac{1-d}{4}b^2v^2 \\
&\quad + \frac{1-d}{2}abuv - \frac{1-d}{2}abv^2 - \frac{1-d}{2}b^2uv \\
&= a^2u^2 + abuv + \left(\frac{d-1}{4}\right)^2 b^2v^2 \\
&\quad - a^2uv - abu^2 - \frac{1-d}{4}abv^2 \\
&\quad - \frac{1-d}{4}b^2uv + \frac{1-d}{4}a^2v^2 + \frac{1-d}{4}b^2u^2 \\
&= \left(a^2 - ab + \frac{1-d}{4}b^2\right)\left(u^2 - uv + \frac{1-d}{4}v^2\right) \\
&= N(\alpha)N(\beta)
\end{aligned}$$

9.1.16. Poznámka. Vlastnost normy uevedenou ve větě 9.1.15 lze s úspěchem využít při studiu dělitelnosti v okruhu kvadratických celých čísel.

Nechť d je bezčtvercové celé číslo, $d \neq 1$. Pro všechna $\alpha, \beta \in R_d$ platí:

$$\alpha/\beta \Longrightarrow N(\alpha)/N(\beta)$$

Zdůvodnění: Nechť α/β. Pak existuje $\gamma \in R_d$, $\beta = \alpha\gamma$. Pak $N(\beta) = N(\alpha\gamma) = N(\alpha)N(\gamma)$, $N(\beta) = N(\alpha)N(\gamma)$, $N(\alpha)/N(\beta)$.

Důležité je, že dělitelnost v R_d je převedena na dělitelnost v $\mathbb{Z}$ (kde o ní mnoho víme – viz teorii čísel).

Samozřejmě, je třeba být opatrný, jedná se pouze o jednosměrný převod – z $N(\alpha)/N(\beta)$ obecně nevyplývá, že α/β. Například pro $1+2i, 1+3i \in \mathbb{Z}[i]$ máme:

1. $N(1+2i)/N(1+3i)$: To je jasné, neboť $N(1+2i) = 5$, $N(1+3i) = 10$.

2. $\neg(1+2i/1+3i)$: Předpokládejme naopak, že $1+2i/1+3i$. Pak existují celá čísla x, y taková, že $(1+2i)(x+yi) = 1+3i$. Je $(1+2i)(x+yi) = (x-2y)+(2x+y)i$, takže $x-2y = 1$ a $2x+y = 3$, což dává $5x = 7$, spor (připomeňme, že x je celé číslo).

9.2 Okruh zbytkových tříd

Pod názvem "okruh zbytkových tříd"se skrývají okruhy $\mathbb{Z}_m$, s nimiž jsme se již seznámili v části 2.1 Aditivní grupa okruhu. Jak již víme (právě z části 2.1), okruhy $\mathbb{Z}_m$ těsně souvisí s kongruencemi modulo m v oboru integrity $\mathbb{Z}$. V části 10.4 Počítání modulo pak zařadíme okruhy zbytkových tříd do širšího rámce – v části 10.4 budeme zkoumat počítání modulo v libovolném oboru integrity.

9.3 Maticový okruh

Matice jsou základním matematickým objektem. Znáte je dobře z Lineární algebry. Pokud si chcete matice zopakovat, podívejte se například do studijního textu [3] a projděte si v něm kapitolu 5 Matice (nad tělesem).

Omezíme se zde (stejně jako v textu [3]) pouze na matice nad tělesem. Nechť m, n jsou kladná celá čísla. Množinu všech matic typu (m, n) nad tělesem T značíme $T_{m,n}$ (v souladu s [3]). Symbolem O značíme nulovou matici, tj. matici, která má všechny prvky rovny 0 (kde 0 je neutrální prvek operace sčítání v tělese T).

Matice téhož typu je možno sčítat. Je snadné ukázat, že množina $T_{m,n}$ spolu s operací sčítání matic je komutativní grupa s neutrálním prvkem O.

Nechť m, n, p jsou kladná celá čísla. Připomeňme si, že pro všechna $A \in T_{m,p}$ a $B \in T_{p,n}$ lze vypočítat součin $A \cdot B$; přitom bude $AB \in T_{m,n}$.

Pro libovolné dvě čtvercové matice stupně n nad tělesem T lze tedy určit jejich součet i součin. Takže sčítání matic a násobení matic jsou binární operace na množině $T_{n,n}$. Již jsme hovořili o tom, že množina $T_{n,n}$ spolu s operací sčítání matic je komutativní grupa. Pro všechna $A, B, C \in T_{n,n}$ je $A(B+C) = AB + AC$ a také $(B+C)A = BA + CA$ (viz větu 5.2.5. v [3]).

Můžeme tedy konstatovat, že $T_{n,n}$ spolu s operacemi sčítání a násobení matic je okruh. Tento okruh budeme značit $M_n(T)$.

Navíc, operace násobení čtvercových matic stupně n nad tělesem T je asociativní (opět, viz větu 5.2.5. v [3]) a má neutrální prvek E, kde E je jednotková matice splňující $e_{ii} = 1$ (neutrální prvek operace $\cdot$ v tělese T) pro všechna $i \in \{1, \ldots, n\}$ a $e_{ij} = 0$ (neutrální prvek operace $+$ v tělese T) pro všechna $i, j \in \{1, \ldots, n\}$, $i \neq j$. Můžeme tedy říci, že platí

9.3.1. Tvrzení. *$M_n(T)$ je asociativní okruh s jednotkovým prvkem E.*

9.3.2. Poznámka. Jaké další kvality má okruh $M_n(T)$?

1. Pro $n = 1$ máme $M_1(T) \cong T$. Isomorfismem je zobrazení $\varphi : T \longrightarrow M_1(T)$ dané předpisem $\varphi(a) = (a)$ (pro $a \in T$).

2. Nechť n je celé číslo, $n > 1$. Definujme matice $A, B \in T_{n,n}$ takto:

$$a_{ij} = \begin{cases} 1 & \text{pokud } i = 1 \wedge j = 1 \\ 0 & \text{pokud } i \neq 1 \vee j \neq 1 \end{cases}$$

$$b_{ij} = \begin{cases} 1 & \text{pokud } i = n \wedge j = 1 \\ 0 & \text{pokud } i \neq n \vee j \neq 1 \end{cases}$$

   Pak máme

$$A \neq O,\ B \neq O,\ AB = O,\ BA = B,\ AB \neq BA$$

   Vidíme, že pro $n > 1$ okruh $M_n(T)$ není obor integrity a není komutativní, a to bez ohledu na těleso T.

13 Kořeny polynomů

13.1 Kořeny polynomů, jejich násobnost a počet

13.2 Základní věta algebry a její důsledky

13.3 Algebraické a transcendentní prvky

13.4 Binomické rovnice

13.5 Kvadratické a kubické rovnice

13.6 Kořeny polynomů nad celými čísly

13.7 Hornerovo schéma

14 Konečná tělesa

14.1 Charakteristika tělesa, prvotěleso

14.2 Počet prvků konečného tělesa

14.3 Počet ireducibilních monických polynomů daného stupně

14.4 Konstrukce konečných těles

Reference

[1] Eduard Čech, *Bodové množiny*, Academia, Praha, 1974

[2] Zuzana Došlá, Ondřej Došlý, *Metrické prostory – Teorie a příklady*, Masarykova univerzita, Brno, 2006

[3] Martin Kuřil, studijní text *Lineární algebra*
http://katmatprf.ujepurkyne.com/materialy/KMA_kuril_LINALGkapitola01.pdf
http://katmatprf.ujepurkyne.com/materialy/KMA_kuril_LINALGkapitola02.pdf
http://katmatprf.ujepurkyne.com/materialy/KMA_kuril_LINALGkapitola03.pdf
http://katmatprf.ujepurkyne.com/materialy/KMA_kuril_LINALGkapitola04.pdf
http://katmatprf.ujepurkyne.com/materialy/KMA_kuril_LINALGkapitola05.pdf
http://katmatprf.ujepurkyne.com/materialy/KMA_kuril_LINALGkapitola06.pdf
http://katmatprf.ujepurkyne.com/materialy/KMA_kuril_LINALGkapitola07.pdf
http://katmatprf.ujepurkyne.com/materialy/KMA_kuril_LINALGkapitola08.pdf
poznámka: text k elektronické publikaci připravil Jan Šimek

[4] Joseph J. Rotman, *An Introduction to the Theory of Groups*, Springer, New York, 1999