Další příklad grupy: grupa $(\mathbb{D}_n, \circ)$

Příklad. Nechť $n \geq 3$ je přirozené číslo a představme si pravidelný n-úhelník. Označme $\mathbb{D}_n$ množinu všech shodností tohoto n-úhelníka, tedy zobrazení, která zachovávají délky úseček a kterými je náš n-úhelník zobrazen sám na sebe. Pak $\mathbb{D}_n$ má $2n$ prvků, z toho n rotací kolem středu n-úhelníka (včetně identity – rotace o nulový úhel) a n osových souměrností (vzhledem k osám procházejících středem n-úhelníka a také dvěma z vrcholů a středů stran). Náčrtek. Snadno se ověří, že vzhledem ke skládání dostáváme nekomutativní grupu $(\mathbb{D}_n, \circ)$.

Každá shodnost permutuje množinu vrcholů n-úhelníka, přičemž různým shodnostem odpovídají různé permutace vrcholů. Proto, očíslujeme-li vrcholy n-úhelníka po řadě čísly $1, 2, \ldots, n$, lze každou shodnost n-úhelníka ztotožnit s prvkem grupy $\mathcal{S}_n$. Rotace jsou ztotožněny s mocninami cyklu $(1, 2, \ldots, n)$, každá osová souměrnost je ztotožněna se složením několika nezávislých transpozic.

Dělitelnost v $\mathbb{Z}$

Definice. Říkáme, že celé číslo $b \in \mathbb{Z}$ je dělitelem celého čísla $a \in \mathbb{Z}$, píšeme $b \mid a$, existuje-li $c \in \mathbb{Z}$ tak, že $a = b \cdot c$.

Věta (o dělení se zbytkem). Pro každé $a \in \mathbb{Z}$ a $m \in \mathbb{N}$ existuje jediná dvojice čísel $q, r \in \mathbb{Z}$ takových, že $a = m \cdot q + r$ a současně $0 \leq r < m$. Důkaz.

Definice. Číslo q se nazývá **(neúplný) podíl** a číslo r **zbytek** po dělení čísla a číslem m.

Definice. **Společným dělitelem** čísel $a, b \in \mathbb{Z}$ rozumíme každé číslo $c \in \mathbb{Z}$ splňující $c \mid a$ a současně $c \mid b$. Je-li alespoň jedno z čísel a, b nenulové, existuje jen konečně mnoho jejich společných dělitelů; největší z nich se nazývá **největší společný dělitel** čísel a, b, značíme jej (a, b). Jestliže naopak $a = b = 0$, je jejich největší společný dělitel definován jako nula, tj. $(0, 0) = 0$.

Poznámka. Zřejmě platí $(a, b) = (|a|, |b|)$ a $(a, 0) = |a|$, zaměříme se proto na největší společný dělitel přirozených čísel a, b.

Euklidův algoritmus

Pro daná $a, b \in \mathbb{N}$ provádějme postupné dělení se zbytkem:

$$\begin{aligned}
a &= b \cdot q_0 + r_0 \\
b &= r_0 \cdot q_1 + r_1 \\
r_0 &= r_1 \cdot q_2 + r_2 \\
r_1 &= r_2 \cdot q_3 + r_3 \\
&\vdots \\
r_{n-3} &= r_{n-2} \cdot q_{n-1} + r_{n-1} \\
r_{n-2} &= r_{n-1} \cdot q_n + r_n \\
r_{n-1} &= r_n \cdot q_{n+1} + 0
\end{aligned}$$

Přitom $b > r_0 > r_1 > r_2 > \ldots$, proto skutečně po několika děleních nastane $r_{n+1} = 0$.

Věta. *Pro libovolná $a, b \in \mathbb{N}$ platí* $(a, b) = r_n$. Důkaz.

Věta (Bezoutova rovnost). *Pro libovolná $a, b \in \mathbb{Z}$ existují $u, v \in \mathbb{Z}$ tak, že* $(a, b) = u \cdot a + v \cdot b$. Důkaz.

Nejmenší společný násobek

Definice. **Společným násobkem** čísel $a, b \in \mathbb{Z}$ rozumíme každé číslo $c \in \mathbb{Z}$ splňující $a \mid c$ a současně $b \mid c$.

Poznámka. Je-li $a = 0$ nebo $b = 0$, je jediným společným násobkem čísel a, b číslo 0. V opačném případě existují kladné společné násobky, například $|a \cdot b|$.

Definice. Jsou-li obě čísla $a, b \in \mathbb{Z}$ nenulová, rozumíme **nejmenším společným násobkem** čísel a, b nejmenšího ze všech kladných společných násobků těchto čísel. Je-li alespoň jedno z čísel a, b nulové, definujeme nejmenší společný násobek čísel a, b jako nulu.

Věta. *Nechť $a, b \in \mathbb{Z}$, $a \neq 0 \neq b$. Pak nejmenším společným násobkem čísel a, b je číslo $\frac{|a \cdot b|}{(a,b)}$. Pro libovolné číslo $c \in \mathbb{Z}$ platí, že c je společným násobkem čísel a, b, právě když c je dělitelné nejmenším společným násobkem čísel a, b.* Důkaz.

Poznámka. Druhá část předchozí věty platí i v případě, kdy je některé z čísel a, b nulové.

Další důsledky Bezoutovy rovnosti

Věta (Bezoutova rovnost). *Pro libovolná $a, b \in \mathbb{Z}$ existují $u, v \in \mathbb{Z}$ tak, že* $(a, b) = u \cdot a + v \cdot b$.

Následující důsledek vysvětluje, proč jsme dodefinovali $(0, 0) = 0$.

Důsledek. *Pro libovolná $a, b, d \in \mathbb{Z}$ platí*

$$d \mid (a, b) \quad \Longleftrightarrow \quad d \mid a, \quad d \mid b.$$ Důkaz.

Definice. Čísla $a, b \in \mathbb{Z}$ se nazývají **nesoudělná**, jestliže $(a, b) = 1$.

Důsledek. *Čísla $a, b \in \mathbb{Z}$ jsou nesoudělná, právě když existují $u, v \in \mathbb{Z}$ tak, že* $u \cdot a + v \cdot b = 1$.

Důsledek. *Pro libovolná $a, b, c \in \mathbb{Z}$ platí*

$$a \mid b \cdot c, \quad (a, b) = 1 \quad \Longrightarrow \quad a \mid c.$$ Důkaz.

Definice. Přirozené číslo p se nazývá **prvočíslo**, jestliže jeho jediným dělitelem větším než 1 je p samotné.

Věta. *Pro libovolné prvočíslo p a libovolná $b, c \in \mathbb{Z}$ platí*

$$p \mid b \cdot c \quad \Longrightarrow \quad p \mid b \quad \text{nebo} \quad p \mid c.$$

Věta (o jednoznačném rozkladu v $\mathbb{Z}$). *Libovolné celé číslo $a > 1$ je buď prvočíslo, nebo jej lze napsat jako součin několika prvočísel, a to jednoznačně až na pořadí činitelů.* Důkaz.

Důsledek. *Prvočísel je nekonečně mnoho.*

Důsledek. *Čísla $a, b \in \mathbb{Z}$ jsou nesoudělná, právě když neexistuje prvočíslo p dělící a i b.* Důkaz.

Poznámka. Předchozí větu lze pro malá přirozená čísla užít k hledání největšího společného dělitele tak, že obě čísla rozložíme na součin prvočísel a zjistíme, která prvočísla se vyskytují v obou rozkladech. Obecně však nalézt rozklad na prvočinitele je mnohem obtížnější úkol než nalézt největšího společného dělitele. Celý systém bezpečné komunikace v současnosti je založen na tom, že neumíme rozložit přirozené číslo, které je součinem dvou velkých (řekněme 150-ciferných) prvočísel (výpočet, který by trval několik století, je z praktického hlediska pochopitelně bezcenný).

Kongruence, zbytkové třídy

Definice. Nechť $m \in \mathbb{N}$, $a, b \in \mathbb{Z}$. Říkáme, že a, b jsou **kongruentní** modulo m, a píšeme $a \equiv b \pmod{m}$, jestliže $m \mid a - b$.

Poznámka. Zřejmě $a \equiv b \pmod{m}$, právě když a, b mají stejný zbytek po dělení číslem m.

Definice. Nechť $m \in \mathbb{N}$. Pro libovolné $a \in \mathbb{Z}$ definujeme množinu $[a]_m = \{a + k \cdot m;\ k \in \mathbb{Z}\}$, kterou nazýváme **zbytková třída** modulo m obsahující a.

Poznámka. Množina $[a]_m = \{a + k \cdot m;\ k \in \mathbb{Z}\}$ se skládá z právě těch celých čísel, která mají stejný zbytek po dělení číslem m jako číslo a.

Věta. *Pro libovolná* $a, b \in \mathbb{Z}$, $m \in \mathbb{N}$ *nastává* $[a]_m = [b]_m$ *právě tehdy, když* $a \equiv b \pmod{m}$. Důkaz.

Označení. Množinu všech zbytkových tříd podle modulu $m \in \mathbb{N}$ značíme $\mathbb{Z}_m$. Je tedy

$$\mathbb{Z}_m = \{[0]_m, [1]_m, [2]_m, \ldots, [m-1]_m\}.$$

Operace na množině $\mathbb{Z}_m$

Věta. *Nechť $m \in \mathbb{N}$, $a, b, c, d \in \mathbb{Z}$ jsou libovolná. Jestliže platí $[a]_m = [c]_m$, $[b]_m = [d]_m$, pak také*

$$[a + b]_m = [c + d]_m, \qquad [a \cdot b]_m = [c \cdot d]_m.$$ Důkaz.

Důsledek. *Nechť $m \in \mathbb{N}$. Vztahy*

$$[a]_m + [b]_m = [a + b]_m, \qquad [a]_m \cdot [b]_m = [a \cdot b]_m$$

pro libovolná $a, b \in \mathbb{Z}$ definují operace $+$ a $\cdot$ na množině $\mathbb{Z}_m$.

Věta. *Pro libovolné $m \in \mathbb{N}$ je $(\mathbb{Z}_m, +)$ komutativní grupa s neutrálním prvkem $[0]_m$, v níž inverzním prvkem k libovolné třídě $[a]_m$ je třída $[-a]_m$.*

Věta. *Pro libovolné $m \in \mathbb{N}$ je $(\mathbb{Z}_m, \cdot)$ komutativní pologrupa s neutrálním prvkem $[1]_m$.*

Poznámka. Jestliže $m > 1$, pro každé $a \in \mathbb{Z}$ platí $[a]_m \cdot [0]_m = [a \cdot 0]_m = [0]_m \neq [1]_m$, a tedy $(\mathbb{Z}_m, \cdot)$ není grupa.

Grupa $(\mathbb{Z}_m^\times, \cdot)$

Věta. *Nechť $m \in \mathbb{N}$, $a \in \mathbb{Z}$ jsou libovolná. Zbytková třída $[a]_m$ má inverzní prvek v pologrupě $(\mathbb{Z}_m, \cdot)$, právě když celá čísla a, m jsou nesoudělná.* Důkaz.

Označení. Pro libovolné $m \in \mathbb{N}$ označme $\mathbb{Z}_m^\times$ množinu všech zbytkových tříd $[a]_m$, které mají inverzní prvek v pologrupě $(\mathbb{Z}_m, \cdot)$, tedy

$$\mathbb{Z}_m^\times = \{[a]_m;\ a \in \mathbb{Z},\ (a, m) = 1\}.$$

Důsledek. *Pro každé $m \in \mathbb{N}$ je $(\mathbb{Z}_m^\times, \cdot)$ komutativní grupa.*

Označení. Pro libovolné $m \in \mathbb{N}$ označme $\varphi(m)$ počet všech přirozených čísel nepřevyšujících m, která jsou nesoudělná s m, tedy

$$\varphi(m) = |\{a \in \mathbb{Z};\ 0 < a \leq m,\ (a, m) = 1\}|.$$

Důsledek. *Pro libovolné $m \in \mathbb{N}$ platí $|\mathbb{Z}_m^\times| = \varphi(m)$.*

Definice. Výše definované zobrazení $\varphi : \mathbb{N} \to \mathbb{N}$ se nazývá **Eulerova funkce**. Příklad.