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 $a = b \cdot c$.

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 $0 \leq r < m$. [Věta 3.1, str. 14]

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 $0 \leq r < m$. [Věta 3.1, str. 14]

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

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 $0 \leq r < m$. [Věta 3.1, str. 14]

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 $c \mid b$.

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 $0 \leq r < m$. [Věta 3.1, str. 14]

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).

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 $0 \leq r < m$. [Věta 3.1, str. 14]

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. $(0, 0) = 0$.

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 $0 \leq r < m$. [Věta 3.1, str. 14]

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.

Eukleidův algoritmus

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

$$a = b \cdot q_0 + r_0$$

Eukleidův algoritmus

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

$$a = b \cdot q_0 + r_0$$

$$b = r_0 \cdot q_1 + r_1$$

Eukleidův algoritmus

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

$$a = b \cdot q_0 + r_0$$

$$b = r_0 \cdot q_1 + r_1$$

$$r_0 = r_1 \cdot q_2 + r_2$$

Eukleidův algoritmus

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

$$\begin{aligned} a &= b \cdot q_0 + r_0 \\ b &= r_0 \cdot q_1 + r_1 \\ r_0 &= r_1 \cdot q_2 + r_2 \\ r_1 &= r_2 \cdot q_3 + r_3 \end{aligned}$$

Eukleidův algoritmus

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

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

Eukleidův algoritmus

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

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

Eukleidův 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 $r_{n+1} = 0$.

Eukleidův 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* $(a, b) = r_n$. [Věta 3.2, str. 15]

Eukleidův 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* $(a, b) = r_n$. [Věta 3.2, str. 15]

Věta (Bezoutova rovnost). *Pro libovolná $a, b \in \mathbb{Z}$ existují $u, v \in \mathbb{Z}$ tak, že* $(a, b) = u \cdot a + v \cdot b$. [Věta 3.3, str. 16]

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 $b \mid c$.

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.

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 $|a \cdot b|$.

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.

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.

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 $\frac{|a \cdot b|}{(a,b)}$.*

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.*

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.*

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

Důkaz věty o nejmenším společném násobku

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. Zřejmě $\frac{|a \cdot b|}{(a,b)} = \pm \frac{b}{(a,b)} \cdot a = \pm \frac{a}{(a,b)} \cdot b$ je společný násobek čísel a, b.

Důkaz věty o nejmenším společném násobku

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. Zřejmě $\frac{|a \cdot b|}{(a,b)} = \pm \frac{b}{(a,b)} \cdot a = \pm \frac{a}{(a,b)} \cdot b$ je společný násobek čísel a, b.

Bezoutova věta dává $u, v \in \mathbb{Z}$ taková, že $(a, b) = u \cdot a + v \cdot b$.

Důkaz věty o nejmenším společném násobku

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. Zřejmě $\frac{|a \cdot b|}{(a,b)} = \pm\frac{b}{(a,b)} \cdot a = \pm\frac{a}{(a,b)} \cdot b$ je společný násobek čísel a, b.

Bezoutova věta dává $u, v \in \mathbb{Z}$ taková, že $(a, b) = u \cdot a + v \cdot b$.

Nechť c je libovolný společný násobek čísel a, b.

Důkaz věty o nejmenším společném násobku

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. Zřejmě $\frac{|a \cdot b|}{(a,b)} = \pm \frac{b}{(a,b)} \cdot a = \pm \frac{a}{(a,b)} \cdot b$ je společný násobek čísel a, b.

Bezoutova věta dává $u, v \in \mathbb{Z}$ taková, že $(a, b) = u \cdot a + v \cdot b$.

Nechť c je libovolný společný násobek čísel a, b. Pak existují celá čísla x, y tak, že $c = x \cdot a = y \cdot b$.

Důkaz věty o nejmenším společném násobku

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. Zřejmě $\frac{|a \cdot b|}{(a,b)} = \pm\frac{b}{(a,b)} \cdot a = \pm\frac{a}{(a,b)} \cdot b$ je společný násobek čísel a, b.

Bezoutova věta dává $u, v \in \mathbb{Z}$ taková, že $(a, b) = u \cdot a + v \cdot b$.

Nechť c je libovolný společný násobek čísel a, b. Pak existují celá čísla x, y tak, že $c = x \cdot a = y \cdot b$. Proto

$$(a, b) \cdot c = u \cdot a \cdot c + v \cdot b \cdot c = a \cdot b \cdot (u \cdot y + v \cdot x),$$

Důkaz věty o nejmenším společném násobku

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. Zřejmě $\frac{|a \cdot b|}{(a,b)} = \pm\frac{b}{(a,b)} \cdot a = \pm\frac{a}{(a,b)} \cdot b$ je společný násobek čísel a, b.

Bezoutova věta dává $u, v \in \mathbb{Z}$ taková, že $(a, b) = u \cdot a + v \cdot b$.

Nechť c je libovolný společný násobek čísel a, b. Pak existují celá čísla x, y tak, že $c = x \cdot a = y \cdot b$. Proto

$$(a, b) \cdot c = u \cdot a \cdot c + v \cdot b \cdot c = a \cdot b \cdot (u \cdot y + v \cdot x),$$

a tedy $c = \frac{a \cdot b}{(a,b)} \cdot (u \cdot y + v \cdot x)$.

Důkaz věty o nejmenším společném násobku

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. Zřejmě $\frac{|a \cdot b|}{(a,b)} = \pm\frac{b}{(a,b)} \cdot a = \pm\frac{a}{(a,b)} \cdot b$ je společný násobek čísel a, b.

Bezoutova věta dává $u, v \in \mathbb{Z}$ taková, že $(a, b) = u \cdot a + v \cdot b$.

Nechť c je libovolný společný násobek čísel a, b. Pak existují celá čísla x, y tak, že $c = x \cdot a = y \cdot b$. Proto

$$(a, b) \cdot c = u \cdot a \cdot c + v \cdot b \cdot c = a \cdot b \cdot (u \cdot y + v \cdot x),$$

a tedy $c = \frac{a \cdot b}{(a,b)} \cdot (u \cdot y + v \cdot x)$. Tedy c je dělitelné číslem $\frac{|a \cdot b|}{(a,b)}$.

Důkaz věty o nejmenším společném násobku

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. Zřejmě $\frac{|a \cdot b|}{(a,b)} = \pm\frac{b}{(a,b)} \cdot a = \pm\frac{a}{(a,b)} \cdot b$ je společný násobek čísel a, b.

Bezoutova věta dává $u, v \in \mathbb{Z}$ taková, že $(a, b) = u \cdot a + v \cdot b$.

Nechť c je libovolný společný násobek čísel a, b. Pak existují celá čísla x, y tak, že $c = x \cdot a = y \cdot b$. Proto

$$(a, b) \cdot c = u \cdot a \cdot c + v \cdot b \cdot c = a \cdot b \cdot (u \cdot y + v \cdot x),$$

a tedy $c = \frac{a \cdot b}{(a,b)} \cdot (u \cdot y + v \cdot x)$. Tedy c je dělitelné číslem $\frac{|a \cdot b|}{(a,b)}$.

Je-li navíc $c > 0$, plyne odtud, že $c \geq \frac{|a \cdot b|}{(a,b)}$.

Další důsledky Bezoutovy rovnosti

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

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 $(0, 0) = 0$.

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

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

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

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

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

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

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

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 $u \cdot a + v \cdot b = 1$.

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

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

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

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

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

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

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

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

[Důsledek 3.5, str. 16]

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

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

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

Důsledek. *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.* [Věta 3.6, str. 16]

Důsledek. *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.* [Věta 3.6, str. 16]

Důsledek. *Prvočísel je nekonečně mnoho.* [Jsou-li $p_1, p_2, \ldots, p_n$ všechna prvočísla, neexistuje prvočíslo, které by dělilo číslo $1 + p_1 p_2 \ldots p_n$.]

Důsledek. *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.* [Věta 3.6, str. 16]

Důsledek. *Prvočísel je nekonečně mnoho.* [Jsou-li $p_1, p_2, \ldots, p_n$ všechna prvočísla, neexistuje prvočíslo, které by dělilo číslo $1 + p_1 p_2 \ldots p_n$.]

Důsledek. *Čísla $a, b \in \mathbb{Z}$ jsou nesoudělná, právě když neexistuje prvočíslo p dělící a i b.* [Jsou-li a, b soudělná, nějaké prvočíslo musí dělit číslo $(a, b) > 1$.]

Důsledek. *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.* [Věta 3.6, str. 16]

Důsledek. *Prvočísel je nekonečně mnoho.* [Jsou-li $p_1, p_2, \ldots, p_n$ všechna prvočísla, neexistuje prvočíslo, které by dělilo číslo $1 + p_1 p_2 \ldots p_n$.]

Důsledek. *Čísla $a, b \in \mathbb{Z}$ jsou nesoudělná, právě když neexistuje prvočíslo p dělící a i b.* [Jsou-li a, b soudělná, nějaké prvočíslo musí dělit číslo $(a, b) > 1$.]

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.

Důsledek. *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.* [Věta 3.6, str. 16]

Důsledek. *Prvočísel je nekonečně mnoho.* [Jsou-li $p_1, p_2, \ldots, p_n$ všechna prvočísla, neexistuje prvočíslo, které by dělilo číslo $1 + p_1 p_2 \ldots p_n$.]

Důsledek. *Čísla $a, b \in \mathbb{Z}$ jsou nesoudělná, právě když neexistuje prvočíslo p dělící a i b.* [Jsou-li a, b soudělná, nějaké prvočíslo musí dělit číslo $(a, b) > 1$.]

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.

Důsledek. *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.* [Věta 3.6, str. 16]

Důsledek. *Prvočísel je nekonečně mnoho.* [Jsou-li $p_1, p_2, \ldots, p_n$ všechna prvočísla, neexistuje prvočíslo, které by dělilo číslo $1 + p_1 p_2 \ldots p_n$.]

Důsledek. *Čísla $a, b \in \mathbb{Z}$ jsou nesoudělná, právě když neexistuje prvočíslo p dělící a i b.* [Jsou-li a, b soudělná, nějaké prvočíslo musí dělit číslo $(a, b) > 1$.]

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 $m \mid a - b$.

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 $m \mid a - b$.

Věta. *Nechť $m \in \mathbb{N}$, $a, b \in \mathbb{Z}$. Platí $a \equiv b \pmod{m}$, právě když čísla a, b mají stejný zbytek po dělení číslem m.*

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 $m \mid a - b$.

Věta. *Nechť $m \in \mathbb{N}$, $a, b \in \mathbb{Z}$. Platí $a \equiv b \pmod{m}$, právě když čísla 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.

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 $m \mid a - b$.

Věta. *Nechť $m \in \mathbb{N}$, $a, b \in \mathbb{Z}$. Platí $a \equiv b \pmod{m}$, právě když čísla 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. Množinu všech zbytkových tříd podle modulu $m \in \mathbb{N}$ značíme $\mathbb{Z}_m$.

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 $m \mid a - b$.

Věta. *Nechť $m \in \mathbb{N}$, $a, b \in \mathbb{Z}$. Platí $a \equiv b \pmod{m}$, právě když čísla 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. Množinu všech zbytkových tříd podle modulu $m \in \mathbb{N}$ značíme $\mathbb{Z}_m$.

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.

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 $m \mid a - b$.

Věta. Nechť $m \in \mathbb{N}$, $a, b \in \mathbb{Z}$. Platí $a \equiv b \pmod{m}$, právě když čísla 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. Množinu všech zbytkových tříd podle modulu $m \in \mathbb{N}$ značíme $\mathbb{Z}_m$.

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. Protože těmito zbytky jsou čísla $0, 1, \ldots, m-1$ a každá třída obsahuje jediný zbytek, je těchto tříd právě m a platí

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

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 $m \mid a - b$.

Věta. *Nechť $m \in \mathbb{N}$, $a, b \in \mathbb{Z}$. Platí $a \equiv b \pmod{m}$, právě když čísla 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. Množinu všech zbytkových tříd podle modulu $m \in \mathbb{N}$ značíme $\mathbb{Z}_m$.

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. Protože těmito zbytky jsou čísla $0, 1, \ldots, m-1$ a každá třída obsahuje jediný zbytek, je těchto tříd právě m a platí

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

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

Operace na množině $\mathbb{Z}_m$

Definice. Nechť G je množina. Libovolné zobrazení $G \times G \to G$ se nazývá (binární) **operace** na množině G.

Operace na množině $\mathbb{Z}_m$

Definice. Nechť G je množina. Libovolné zobrazení $G \times G \to G$ se nazývá (binární) **operace** na množině G.

Označení. Operace budeme značit symbolem $\cdot$ (případně $+$, $\circ$, $\bullet$ apod.), obraz dvojice $[a, b] \in G \times G$ v operaci $\cdot$ symbolem $a \cdot b$.

Operace na množině $\mathbb{Z}_m$

Definice. Nechť G je množina. Libovolné zobrazení $G \times G \to G$ se nazývá (binární) **operace** na množině G.

Označení. Operace budeme značit symbolem $\cdot$ (případně $+$, $\circ$, $\bullet$ apod.), obraz dvojice $[a, b] \in G \times G$ v operaci $\cdot$ symbolem $a \cdot b$.

Příklad. Sčítání i násobení jsou příklady operací na kterékoli z množin $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ nebo $\mathbb{C}$.

Operace na množině $\mathbb{Z}_m$

Definice. Nechť G je množina. Libovolné zobrazení $G \times G \to G$ se nazývá (binární) **operace** na množině G.

Označení. Operace budeme značit symbolem $\cdot$ (případně $+$, $\circ$, $\bullet$ apod.), obraz dvojice $[a, b] \in G \times G$ v operaci $\cdot$ symbolem $a \cdot b$.

Příklad. Sčítání i násobení jsou příklady operací na kterékoli z množin $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ nebo $\mathbb{C}$.

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

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

[Věta 3.9, str. 18]

Operace na množině $\mathbb{Z}_m$

Definice. Nechť G je množina. Libovolné zobrazení $G \times G \to G$ se nazývá (binární) **operace** na množině G.

Označení. Operace budeme značit symbolem $\cdot$ (případně $+$, $\circ$, $\bullet$ apod.), obraz dvojice $[a, b] \in G \times G$ v operaci $\cdot$ symbolem $a \cdot b$.

Příklad. Sčítání i násobení jsou příklady operací na kterékoli z množin $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ nebo $\mathbb{C}$.

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*

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

[Věta 3.9, str. 18]

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 $\mathbb{Z}_m$.

Vlastnosti operací, grupoid

Definice. Operace $\cdot$ na množině G se nazývá

- **komutativní**, jestliže $\forall a, b \in G\colon\ a \cdot b = b \cdot a$;

Vlastnosti operací, grupoid

Definice. Operace $\cdot$ na množině G se nazývá

- **komutativní**, jestliže $\forall a, b \in G\colon\ a \cdot b = b \cdot a$;
- **asociativní**, jestliže $\forall a, b, c \in G\colon\ a \cdot (b \cdot c) = (a \cdot b) \cdot c$.

Vlastnosti operací, grupoid

Definice. Operace $\cdot$ na množině G se nazývá

- **komutativní**, jestliže $\forall a, b \in G\colon\ a \cdot b = b \cdot a$;
- **asociativní**, jestliže $\forall a, b, c \in G\colon\ a \cdot (b \cdot c) = (a \cdot b) \cdot c$.

Definice. Množina G spolu s operací $\cdot$ na G se nazývá **grupoid**, označujeme jej $(G, \cdot)$, nebo jen G, bude-li z kontextu jasné, jakou operaci máme na mysli.

Vlastnosti operací, grupoid

Definice. Operace $\cdot$ na množině G se nazývá

- **komutativní**, jestliže $\forall a, b \in G\colon\ a \cdot b = b \cdot a$;
- **asociativní**, jestliže $\forall a, b, c \in G\colon\ a \cdot (b \cdot c) = (a \cdot b) \cdot c$.

Definice. Množina G spolu s operací $\cdot$ na G se nazývá **grupoid**, označujeme jej $(G, \cdot)$, nebo jen G, bude-li z kontextu jasné, jakou operaci máme na mysli.

Definice. Grupoid $(G, \cdot)$ se nazývá

- **komutativní grupoid**, jestliže $\cdot$ je komutativní operace na G;

Vlastnosti operací, grupoid

Definice. Operace $\cdot$ na množině G se nazývá

- **komutativní**, jestliže $\forall a, b \in G\colon\ a \cdot b = b \cdot a$;
- **asociativní**, jestliže $\forall a, b, c \in G\colon\ a \cdot (b \cdot c) = (a \cdot b) \cdot c$.

Definice. Množina G spolu s operací $\cdot$ na G se nazývá **grupoid**, označujeme jej $(G, \cdot)$, nebo jen G, bude-li z kontextu jasné, jakou operaci máme na mysli.

Definice. Grupoid $(G, \cdot)$ se nazývá

- **komutativní grupoid**, jestliže $\cdot$ je komutativní operace na G;
- **pologrupa**, jestliže $\cdot$ je asociativní operace na G;

Vlastnosti operací, grupoid

Definice. Operace $\cdot$ na množině G se nazývá

- **komutativní**, jestliže $\forall a, b \in G\colon\ a \cdot b = b \cdot a$;
- **asociativní**, jestliže $\forall a, b, c \in G\colon\ a \cdot (b \cdot c) = (a \cdot b) \cdot c$.

Definice. Množina G spolu s operací $\cdot$ na G se nazývá **grupoid**, označujeme jej $(G, \cdot)$, nebo jen G, bude-li z kontextu jasné, jakou operaci máme na mysli.

Definice. Grupoid $(G, \cdot)$ se nazývá

- **komutativní grupoid**, jestliže $\cdot$ je komutativní operace na G;
- **pologrupa**, jestliže $\cdot$ je asociativní operace na G;
- **komutativní pologrupa**, jestliže $\cdot$ je komutativní a asociativní operace na G.

Vlastnosti operací, grupoid

Definice. Operace $\cdot$ na množině G se nazývá

- **komutativní**, jestliže $\forall a, b \in G\colon\ a \cdot b = b \cdot a$;
- **asociativní**, jestliže $\forall a, b, c \in G\colon\ a \cdot (b \cdot c) = (a \cdot b) \cdot c$.

Definice. Množina G spolu s operací $\cdot$ na G se nazývá **grupoid**, označujeme jej $(G, \cdot)$, nebo jen G, bude-li z kontextu jasné, jakou operaci máme na mysli.

Definice. Grupoid $(G, \cdot)$ se nazývá

- **komutativní grupoid**, jestliže $\cdot$ je komutativní operace na G;
- **pologrupa**, jestliže $\cdot$ je asociativní operace na G;
- **komutativní pologrupa**, jestliže $\cdot$ je komutativní a asociativní operace na G.

Definice. Nechť $(G, \cdot)$ je grupoid. Prvek $e \in G$ se nazývá **neutrální prvek** (neboli **jednotkový prvek**) tohoto grupoidu, jestliže $\forall a \in G\colon\ e \cdot a = a \cdot e = a$.

Vlastnosti operací, grupoid

Definice. Operace $\cdot$ na množině G se nazývá

- **komutativní**, jestliže $\forall a, b \in G\colon\ a \cdot b = b \cdot a$;
- **asociativní**, jestliže $\forall a, b, c \in G\colon\ a \cdot (b \cdot c) = (a \cdot b) \cdot c$.

Definice. Množina G spolu s operací $\cdot$ na G se nazývá **grupoid**, označujeme jej $(G, \cdot)$, nebo jen G, bude-li z kontextu jasné, jakou operaci máme na mysli.

Definice. Grupoid $(G, \cdot)$ se nazývá

- **komutativní grupoid**, jestliže $\cdot$ je komutativní operace na G;
- **pologrupa**, jestliže $\cdot$ je asociativní operace na G;
- **komutativní pologrupa**, jestliže $\cdot$ je komutativní a asociativní operace na G.

Definice. Nechť $(G, \cdot)$ je grupoid. Prvek $e \in G$ se nazývá **neutrální prvek** (neboli **jednotkový prvek**) tohoto grupoidu, jestliže $\forall a \in G\colon\ e \cdot a = a \cdot e = a$.

Věta. Každý grupoid má nejvýše jeden neutrální prvek. [Věta 1.6, str. 8]

Grupa, komutativní grupa

Definice. Nechť $(G, \cdot)$ grupoid s neutrálním prvkem e a nechť je pevně dáno $a \in G$. Prvek $b \in G$ se nazývá **inverzním prvkem** k prvku a (v grupoidu G), jestliže platí $a \cdot b = b \cdot a = e$.

Grupa, komutativní grupa

Definice. Nechť $(G, \cdot)$ grupoid s neutrálním prvkem e a nechť je pevně dáno $a \in G$. Prvek $b \in G$ se nazývá **inverzním prvkem** k prvku a (v grupoidu G), jestliže platí $a \cdot b = b \cdot a = e$.

Věta. V libovolné pologrupě s neutrálním prvkem ke každému prvku existuje nejvýše jeden prvek inverzní. [Věta 1.8, str. 8]

Grupa, komutativní grupa

Definice. Nechť $(G, \cdot)$ grupoid s neutrálním prvkem e a nechť je pevně dáno $a \in G$. Prvek $b \in G$ se nazývá **inverzním prvkem** k prvku a (v grupoidu G), jestliže platí $a \cdot b = b \cdot a = e$.

Věta. V libovolné pologrupě s neutrálním prvkem ke každému prvku existuje nejvýše jeden prvek inverzní. [Věta 1.8, str. 8]

Definice. Grupoid $(G, \cdot)$ se nazývá **grupa**, jestliže

Grupa, komutativní grupa

Definice. Nechť $(G, \cdot)$ grupoid s neutrálním prvkem e a nechť je pevně dáno $a \in G$. Prvek $b \in G$ se nazývá **inverzním prvkem** k prvku a (v grupoidu G), jestliže platí $a \cdot b = b \cdot a = e$.

Věta. V libovolné pologrupě s neutrálním prvkem ke každému prvku existuje nejvýše jeden prvek inverzní. [Věta 1.8, str. 8]

Definice. Grupoid $(G, \cdot)$ se nazývá **grupa**, jestliže

- $(G, \cdot)$ je pologrupa,

Grupa, komutativní grupa

Definice. Nechť $(G, \cdot)$ grupoid s neutrálním prvkem e a nechť je pevně dáno $a \in G$. Prvek $b \in G$ se nazývá **inverzním prvkem** k prvku a (v grupoidu G), jestliže platí $a \cdot b = b \cdot a = e$.

Věta. V libovolné pologrupě s neutrálním prvkem ke každému prvku existuje nejvýše jeden prvek inverzní. [Věta 1.8, str. 8]

Definice. Grupoid $(G, \cdot)$ se nazývá **grupa**, jestliže

- $(G, \cdot)$ je pologrupa,
- $(G, \cdot)$ má neutrální prvek,

Grupa, komutativní grupa

Definice. Nechť $(G, \cdot)$ grupoid s neutrálním prvkem e a nechť je pevně dáno $a \in G$. Prvek $b \in G$ se nazývá **inverzním prvkem** k prvku a (v grupoidu G), jestliže platí $a \cdot b = b \cdot a = e$.

Věta. V libovolné pologrupě s neutrálním prvkem ke každému prvku existuje nejvýše jeden prvek inverzní. [Věta 1.8, str. 8]

Definice. Grupoid $(G, \cdot)$ se nazývá **grupa**, jestliže

- $(G, \cdot)$ je pologrupa,
- $(G, \cdot)$ má neutrální prvek,
- ke každému prvku $a \in G$ existuje v $(G, \cdot)$ prvek inverzní.

Grupa, komutativní grupa

Definice. Nechť $(G, \cdot)$ grupoid s neutrálním prvkem e a nechť je pevně dáno $a \in G$. Prvek $b \in G$ se nazývá **inverzním prvkem** k prvku a (v grupoidu G), jestliže platí $a \cdot b = b \cdot a = e$.

Věta. V libovolné pologrupě s neutrálním prvkem ke každému prvku existuje nejvýše jeden prvek inverzní. [Věta 1.8, str. 8]

Definice. Grupoid $(G, \cdot)$ se nazývá **grupa**, jestliže

- $(G, \cdot)$ je pologrupa,
- $(G, \cdot)$ má neutrální prvek,
- ke každému prvku $a \in G$ existuje v $(G, \cdot)$ prvek inverzní.

Označení. V grupě $(G, \cdot)$ tedy ke každému prvku $a \in G$ existuje právě jeden prvek inverzní, značíme jej a^{-1}.

Grupa, komutativní grupa

Definice. Nechť $(G, \cdot)$ grupoid s neutrálním prvkem e a nechť je pevně dáno $a \in G$. Prvek $b \in G$ se nazývá **inverzním prvkem** k prvku a (v grupoidu G), jestliže platí $a \cdot b = b \cdot a = e$.

Věta. V libovolné pologrupě s neutrálním prvkem ke každému prvku existuje nejvýše jeden prvek inverzní. [Věta 1.8, str. 8]

Definice. Grupoid $(G, \cdot)$ se nazývá **grupa**, jestliže

- $(G, \cdot)$ je pologrupa,
- $(G, \cdot)$ má neutrální prvek,
- ke každému prvku $a \in G$ existuje v $(G, \cdot)$ prvek inverzní.

Označení. V grupě $(G, \cdot)$ tedy ke každému prvku $a \in G$ existuje právě jeden prvek inverzní, značíme jej a^{-1}.

Definice. Je-li $(G, \cdot)$ grupa a je-li navíc operace $\cdot$ komutativní, hovoříme o **komutativní grupě**.

Grupa, komutativní grupa

Definice. Nechť $(G, \cdot)$ grupoid s neutrálním prvkem e a nechť je pevně dáno $a \in G$. Prvek $b \in G$ se nazývá **inverzním prvkem** k prvku a (v grupoidu G), jestliže platí $a \cdot b = b \cdot a = e$.

Věta. V libovolné pologrupě s neutrálním prvkem ke každému prvku existuje nejvýše jeden prvek inverzní. [Věta 1.8, str. 8]

Definice. Grupoid $(G, \cdot)$ se nazývá **grupa**, jestliže

- $(G, \cdot)$ je pologrupa,
- $(G, \cdot)$ má neutrální prvek,
- ke každému prvku $a \in G$ existuje v $(G, \cdot)$ prvek inverzní.

Označení. V grupě $(G, \cdot)$ tedy ke každému prvku $a \in G$ existuje právě jeden prvek inverzní, značíme jej a^{-1}.

Definice. Je-li $(G, \cdot)$ grupa a je-li navíc operace $\cdot$ komutativní, hovoříme o **komutativní grupě**.

Definice. Grupa $(G, \cdot)$ se nazývá **triviální**, má-li množina G jediný prvek, tj. $G = \{e\}$. (Tento jediný prvek e je pak nutně neutrální, neboť musí platit $e \cdot e = e$.)

Příklady grup

Příklad. $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$ jsou komutativní grupy.

Příklady grup

Příklad. $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$ jsou komutativní grupy.

Poznámka. V případě, kdy pro operaci používáme symbol $+$, často místo inverzní prvek používáme termín **opačný prvek**.

Příklady grup

Příklad. $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$ jsou komutativní grupy.

Poznámka. V případě, kdy pro operaci používáme symbol $+$, často místo inverzní prvek používáme termín **opačný prvek**.

Příklad. $(\mathbb{Q}, \cdot)$, $(\mathbb{R}, \cdot)$, $(\mathbb{C}, \cdot)$ jsou komutativní pologrupy s neutrálním prvkem 1, ale nejsou to grupy, neboť k prvku 0 neexistuje prvek inverzní.

Příklady grup

Příklad. $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$ jsou komutativní grupy.

Poznámka. V případě, kdy pro operaci používáme symbol $+$, často místo inverzní prvek používáme termín **opačný prvek**.

Příklad. $(\mathbb{Q}, \cdot)$, $(\mathbb{R}, \cdot)$, $(\mathbb{C}, \cdot)$ jsou komutativní pologrupy s neutrálním prvkem 1, ale nejsou to grupy, neboť k prvku 0 neexistuje prvek inverzní.

Příklad. $(\mathbb{Q}^*, \cdot)$, $(\mathbb{R}^*, \cdot)$, $(\mathbb{C}^*, \cdot)$ jsou komutativní grupy, kde $\mathbb{Q}^* = \mathbb{Q} - \{0\}$, $\mathbb{R}^* = \mathbb{R} - \{0\}$, $\mathbb{C}^* = \mathbb{C} - \{0\}$.

Příklady grup

Příklad. $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$ jsou komutativní grupy.

Poznámka. V případě, kdy pro operaci používáme symbol $+$, často místo inverzní prvek používáme termín **opačný prvek**.

Příklad. $(\mathbb{Q}, \cdot)$, $(\mathbb{R}, \cdot)$, $(\mathbb{C}, \cdot)$ jsou komutativní pologrupy s neutrálním prvkem 1, ale nejsou to grupy, neboť k prvku 0 neexistuje prvek inverzní.

Příklad. $(\mathbb{Q}^*, \cdot)$, $(\mathbb{R}^*, \cdot)$, $(\mathbb{C}^*, \cdot)$ jsou komutativní grupy, kde $\mathbb{Q}^* = \mathbb{Q} - \{0\}$, $\mathbb{R}^* = \mathbb{R} - \{0\}$, $\mathbb{C}^* = \mathbb{C} - \{0\}$.

Věta. Pro libovolné $m \in \mathbb{N}$ je $(\mathbb{Z}_m, +)$ komutativní grupa s neutrálním prvkem $[0]_m$, v níž inverzním (neboli opačným) prvkem k libovolné třídě $[a]_m$ je třída $[-a]_m$. [Věta 3.11, str. 19]

Příklady grup

Příklad. $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$ jsou komutativní grupy.

Poznámka. V případě, kdy pro operaci používáme symbol $+$, často místo inverzní prvek používáme termín **opačný prvek**.

Příklad. $(\mathbb{Q}, \cdot)$, $(\mathbb{R}, \cdot)$, $(\mathbb{C}, \cdot)$ jsou komutativní pologrupy s neutrálním prvkem 1, ale nejsou to grupy, neboť k prvku 0 neexistuje prvek inverzní.

Příklad. $(\mathbb{Q}^*, \cdot)$, $(\mathbb{R}^*, \cdot)$, $(\mathbb{C}^*, \cdot)$ jsou komutativní grupy, kde $\mathbb{Q}^* = \mathbb{Q} - \{0\}$, $\mathbb{R}^* = \mathbb{R} - \{0\}$, $\mathbb{C}^* = \mathbb{C} - \{0\}$.

Věta. Pro libovolné $m \in \mathbb{N}$ je $(\mathbb{Z}_m, +)$ komutativní grupa s neutrálním prvkem $[0]_m$, v níž inverzním (neboli opačným) prvkem k libovolné třídě $[a]_m$ je třída $[-a]_m$. [Věta 3.11, str. 19]

Věta. Pro libovolné $m \in \mathbb{N}$ je $(\mathbb{Z}_m, \cdot)$ komutativní pologrupa s neutrálním prvkem $[1]_m$. [Věta 3.12, str. 19]

Příklady grup

Příklad. $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$ jsou komutativní grupy.

Poznámka. V případě, kdy pro operaci používáme symbol $+$, často místo inverzní prvek používáme termín **opačný prvek**.

Příklad. $(\mathbb{Q}, \cdot)$, $(\mathbb{R}, \cdot)$, $(\mathbb{C}, \cdot)$ jsou komutativní pologrupy s neutrálním prvkem 1, ale nejsou to grupy, neboť k prvku 0 neexistuje prvek inverzní.

Příklad. $(\mathbb{Q}^*, \cdot)$, $(\mathbb{R}^*, \cdot)$, $(\mathbb{C}^*, \cdot)$ jsou komutativní grupy, kde $\mathbb{Q}^* = \mathbb{Q} - \{0\}$, $\mathbb{R}^* = \mathbb{R} - \{0\}$, $\mathbb{C}^* = \mathbb{C} - \{0\}$.

Věta. Pro libovolné $m \in \mathbb{N}$ je $(\mathbb{Z}_m, +)$ komutativní grupa s neutrálním prvkem $[0]_m$, v níž inverzním (neboli opačným) prvkem k libovolné třídě $[a]_m$ je třída $[-a]_m$. [Věta 3.11, str. 19]

Věta. Pro libovolné $m \in \mathbb{N}$ je $(\mathbb{Z}_m, \cdot)$ komutativní pologrupa s neutrálním prvkem $[1]_m$. [Věta 3.12, str. 19]

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.

Několik pojmů týkajících se zobrazení

Poznámka. Připomeňme, že zobrazení $f : A \to B$ se nazývá

- **injekce**, jestliže $\forall a_1, a_2 \in A$: $(f(a_1) = f(a_2) \implies a_1 = a_2)$;

Několik pojmů týkajících se zobrazení

Poznámka. Připomeňme, že zobrazení $f : A \to B$ se nazývá

- **injekce**, jestliže $\forall a_1, a_2 \in A$: $(f(a_1) = f(a_2) \implies a_1 = a_2)$;
- **surjekce**, jestliže $\forall b \in B\ \exists a \in A$: $f(a) = b$;

Několik pojmů týkajících se zobrazení

Poznámka. Připomeňme, že zobrazení $f : A \to B$ se nazývá

- **injekce**, jestliže $\forall a_1, a_2 \in A$: $(f(a_1) = f(a_2) \implies a_1 = a_2)$;
- **surjekce**, jestliže $\forall b \in B\ \exists a \in A$: $f(a) = b$;
- **bijekce**, jestliže je injekce a také surjekce.

Několik pojmů týkajících se zobrazení

Poznámka. Připomeňme, že zobrazení $f : A \to B$ se nazývá

- **injekce**, jestliže $\forall a_1, a_2 \in A$: $(f(a_1) = f(a_2) \implies a_1 = a_2)$;
- **surjekce**, jestliže $\forall b \in B\ \exists a \in A$: $f(a) = b$;
- **bijekce**, jestliže je injekce a také surjekce.

Je-li také $g : B \to C$ zobrazení, jejich složením $g \circ f$ (čti g po f) rozumíme zobrazení $g \circ f : A \to C$ definované předpisem

$$(g \circ f)(a) = g(f(a)) \qquad \text{pro libovolné } a \in A.$$

Několik pojmů týkajících se zobrazení

Poznámka. Připomeňme, že zobrazení $f : A \to B$ se nazývá

- **injekce**, jestliže $\forall a_1, a_2 \in A$: $(f(a_1) = f(a_2) \implies a_1 = a_2)$;
- **surjekce**, jestliže $\forall b \in B\ \exists a \in A$: $f(a) = b$;
- **bijekce**, jestliže je injekce a také surjekce.

Je-li také $g : B \to C$ zobrazení, jejich složením $g \circ f$ (čti g po f) rozumíme zobrazení $g \circ f : A \to C$ definované předpisem

$$(g \circ f)(a) = g(f(a)) \qquad \text{pro libovolné } a \in A.$$

Poznámka. Je-li zobrazení $f : A \to B$ bijekce, je k němu inverzní zobrazení $f^{-1} : B \to A$ definováno takto: pro libovolné $b \in B$ definujeme prvek $f^{-1}(b)$ jako ten jediný prvek množiny A, který je zobrazením f zobrazen na prvek b.

Několik pojmů týkajících se zobrazení

Poznámka. Připomeňme, že zobrazení $f : A \to B$ se nazývá

- **injekce**, jestliže $\forall a_1, a_2 \in A$: $(f(a_1) = f(a_2) \implies a_1 = a_2)$;
- **surjekce**, jestliže $\forall b \in B\ \exists a \in A$: $f(a) = b$;
- **bijekce**, jestliže je injekce a také surjekce.

Je-li také $g : B \to C$ zobrazení, jejich složením $g \circ f$ (čti g po f) rozumíme zobrazení $g \circ f : A \to C$ definované předpisem

$$(g \circ f)(a) = g(f(a)) \qquad \text{pro libovolné } a \in A.$$

Poznámka. Je-li zobrazení $f : A \to B$ bijekce, je k němu inverzní zobrazení $f^{-1} : B \to A$ definováno takto: pro libovolné $b \in B$ definujeme prvek $f^{-1}(b)$ jako ten jediný prvek množiny A, který je zobrazením f zobrazen na prvek b. Pak tedy platí

$$\forall b \in B: f(f^{-1}(b)) = b,$$

Několik pojmů týkajících se zobrazení

Poznámka. Připomeňme, že zobrazení $f : A \to B$ se nazývá

- **injekce**, jestliže $\forall a_1, a_2 \in A$: $(f(a_1) = f(a_2) \implies a_1 = a_2)$;
- **surjekce**, jestliže $\forall b \in B\ \exists a \in A$: $f(a) = b$;
- **bijekce**, jestliže je injekce a také surjekce.

Je-li také $g : B \to C$ zobrazení, jejich složením $g \circ f$ (čti g po f) rozumíme zobrazení $g \circ f : A \to C$ definované předpisem

$$(g \circ f)(a) = g(f(a)) \qquad \text{pro libovolné } a \in A.$$

Poznámka. Je-li zobrazení $f : A \to B$ bijekce, je k němu inverzní zobrazení $f^{-1} : B \to A$ definováno takto: pro libovolné $b \in B$ definujeme prvek $f^{-1}(b)$ jako ten jediný prvek množiny A, který je zobrazením f zobrazen na prvek b. Pak tedy platí

$$\forall b \in B: f(f^{-1}(b)) = b,$$
$$\forall a \in A: f^{-1}(f(a)) = a.$$

Několik pojmů týkajících se zobrazení

Poznámka. Připomeňme, že zobrazení $f : A \to B$ se nazývá

- **injekce**, jestliže $\forall a_1, a_2 \in A$: $(f(a_1) = f(a_2) \implies a_1 = a_2)$;
- **surjekce**, jestliže $\forall b \in B\ \exists a \in A$: $f(a) = b$;
- **bijekce**, jestliže je injekce a také surjekce.

Je-li také $g : B \to C$ zobrazení, jejich složením $g \circ f$ (čti g po f) rozumíme zobrazení $g \circ f : A \to C$ definované předpisem

$$(g \circ f)(a) = g(f(a)) \qquad \text{pro libovolné } a \in A.$$

Poznámka. Je-li zobrazení $f : A \to B$ bijekce, je k němu inverzní zobrazení $f^{-1} : B \to A$ definováno takto: pro libovolné $b \in B$ definujeme prvek $f^{-1}(b)$ jako ten jediný prvek množiny A, který je zobrazením f zobrazen na prvek b. Pak tedy platí

$$\forall b \in B: f(f^{-1}(b)) = b,$$
$$\forall a \in A: f^{-1}(f(a)) = a.$$

Zobrazení $f^{-1} : B \to A$ je také bijekce.

Grupa permutací

Poznámka. Připomeňme, že skládání zobrazení je asociativní: jsou-li $f : A \to B$, $g : B \to C$, $h : C \to D$ zobrazení, pak $h \circ (g \circ f) = (h \circ g) \circ f$.

Grupa permutací

Poznámka. Připomeňme, že skládání zobrazení je asociativní: jsou-li $f : A \to B$, $g : B \to C$, $h : C \to D$ zobrazení, pak $h \circ (g \circ f) = (h \circ g) \circ f$. Skutečně, na obou stranách jsou zobrazení $A \to D$, stačí ověřit, že mají stejný předpis.

Grupa permutací

Poznámka. Připomeňme, že skládání zobrazení je asociativní: jsou-li $f : A \to B$, $g : B \to C$, $h : C \to D$ zobrazení, pak $h \circ (g \circ f) = (h \circ g) \circ f$. Skutečně, na obou stranách jsou zobrazení $A \to D$, stačí ověřit, že mají stejný předpis. Pro libovolné $a \in A$ je
$(h \circ (g \circ f))(a) = h((g \circ f)(a)) = h(g(f(a)))$,
$((h \circ g) \circ f)(a) = (h \circ g)(f(a)) = h(g(f(a)))$.

Grupa permutací

Poznámka. Připomeňme, že skládání zobrazení je asociativní: jsou-li $f : A \to B$, $g : B \to C$, $h : C \to D$ zobrazení, pak $h \circ (g \circ f) = (h \circ g) \circ f$. Skutečně, na obou stranách jsou zobrazení $A \to D$, stačí ověřit, že mají stejný předpis. Pro libovolné $a \in A$ je
$(h \circ (g \circ f))(a) = h((g \circ f)(a)) = h(g(f(a)))$,
$((h \circ g) \circ f)(a) = (h \circ g)(f(a)) = h(g(f(a)))$.

Příklad. Nechť X je množina, symbolem X^X značíme množinu všech zobrazení $X \to X$.

Grupa permutací

Poznámka. Připomeňme, že skládání zobrazení je asociativní: jsou-li $f : A \to B$, $g : B \to C$, $h : C \to D$ zobrazení, pak $h \circ (g \circ f) = (h \circ g) \circ f$. Skutečně, na obou stranách jsou zobrazení $A \to D$, stačí ověřit, že mají stejný předpis. Pro libovolné $a \in A$ je
$(h \circ (g \circ f))(a) = h((g \circ f)(a)) = h(g(f(a)))$,
$((h \circ g) \circ f)(a) = (h \circ g)(f(a)) = h(g(f(a)))$.

Příklad. Nechť X je množina, symbolem X^X značíme množinu všech zobrazení $X \to X$. Pak $(X^X, \circ)$ je pologrupa, v níž je neutrální prvek identita na X, totiž zobrazení $\mathrm{id} : X \to X$ splňující $\mathrm{id}(x) = x$ pro každé $x \in X$.

Grupa permutací

Poznámka. Připomeňme, že skládání zobrazení je asociativní: jsou-li $f : A \to B$, $g : B \to C$, $h : C \to D$ zobrazení, pak $h \circ (g \circ f) = (h \circ g) \circ f$. Skutečně, na obou stranách jsou zobrazení $A \to D$, stačí ověřit, že mají stejný předpis. Pro libovolné $a \in A$ je
$(h \circ (g \circ f))(a) = h((g \circ f)(a)) = h(g(f(a)))$,
$((h \circ g) \circ f)(a) = (h \circ g)(f(a)) = h(g(f(a)))$.

Příklad. Nechť X je množina, symbolem X^X značíme množinu všech zobrazení $X \to X$. Pak $(X^X, \circ)$ je pologrupa, v níž je neutrální prvek identita na X, totiž zobrazení $\mathrm{id} : X \to X$ splňující $\mathrm{id}(x) = x$ pro každé $x \in X$. K danému $f \in X^X$ existuje inverzní prvek, právě když f je bijekce; je jím inverzní zobrazení f^{-1}.

Grupa permutací

Poznámka. Připomeňme, že skládání zobrazení je asociativní: jsou-li $f : A \to B$, $g : B \to C$, $h : C \to D$ zobrazení, pak $h \circ (g \circ f) = (h \circ g) \circ f$. Skutečně, na obou stranách jsou zobrazení $A \to D$, stačí ověřit, že mají stejný předpis. Pro libovolné $a \in A$ je
$(h \circ (g \circ f))(a) = h((g \circ f)(a)) = h(g(f(a)))$,
$((h \circ g) \circ f)(a) = (h \circ g)(f(a)) = h(g(f(a)))$.

Příklad. Nechť X je množina, symbolem X^X značíme množinu všech zobrazení $X \to X$. Pak $(X^X, \circ)$ je pologrupa, v níž je neutrální prvek identita na X, totiž zobrazení $\mathrm{id} : X \to X$ splňující $\mathrm{id}(x) = x$ pro každé $x \in X$. K danému $f \in X^X$ existuje inverzní prvek, právě když f je bijekce; je jím inverzní zobrazení f^{-1}. Proto má-li množina X alespoň dva prvky, není $(X^X, \circ)$ grupa.

Grupa permutací

Poznámka. Připomeňme, že skládání zobrazení je asociativní: jsou-li $f : A \to B$, $g : B \to C$, $h : C \to D$ zobrazení, pak $h \circ (g \circ f) = (h \circ g) \circ f$. Skutečně, na obou stranách jsou zobrazení $A \to D$, stačí ověřit, že mají stejný předpis. Pro libovolné $a \in A$ je
$(h \circ (g \circ f))(a) = h((g \circ f)(a)) = h(g(f(a)))$,
$((h \circ g) \circ f)(a) = (h \circ g)(f(a)) = h(g(f(a)))$.

Příklad. Nechť X je množina, symbolem X^X značíme množinu všech zobrazení $X \to X$. Pak $(X^X, \circ)$ je pologrupa, v níž je neutrální prvek identita na X, totiž zobrazení $\mathrm{id} : X \to X$ splňující $\mathrm{id}(x) = x$ pro každé $x \in X$. K danému $f \in X^X$ existuje inverzní prvek, právě když f je bijekce; je jím inverzní zobrazení f^{-1}. Proto má-li množina X alespoň dva prvky, není $(X^X, \circ)$ grupa.

Definice. **Permutací** na množině X rozumíme libovolnou bijekci $X \to X$.

Grupa permutací

Poznámka. Připomeňme, že skládání zobrazení je asociativní: jsou-li $f : A \to B$, $g : B \to C$, $h : C \to D$ zobrazení, pak $h \circ (g \circ f) = (h \circ g) \circ f$. Skutečně, na obou stranách jsou zobrazení $A \to D$, stačí ověřit, že mají stejný předpis. Pro libovolné $a \in A$ je
$(h \circ (g \circ f))(a) = h((g \circ f)(a)) = h(g(f(a)))$,
$((h \circ g) \circ f)(a) = (h \circ g)(f(a)) = h(g(f(a)))$.

Příklad. Nechť X je množina, symbolem X^X značíme množinu všech zobrazení $X \to X$. Pak $(X^X, \circ)$ je pologrupa, v níž je neutrální prvek identita na X, totiž zobrazení $\mathrm{id} : X \to X$ splňující $\mathrm{id}(x) = x$ pro každé $x \in X$. K danému $f \in X^X$ existuje inverzní prvek, právě když f je bijekce; je jím inverzní zobrazení f^{-1}. Proto má-li množina X alespoň dva prvky, není $(X^X, \circ)$ grupa.

Definice. **Permutací** na množině X rozumíme libovolnou bijekci $X \to X$. Množinu všech permutací na množině X značíme $\mathbb{S}(X)$.

Grupa permutací

Poznámka. Připomeňme, že skládání zobrazení je asociativní: jsou-li $f : A \to B$, $g : B \to C$, $h : C \to D$ zobrazení, pak $h \circ (g \circ f) = (h \circ g) \circ f$. Skutečně, na obou stranách jsou zobrazení $A \to D$, stačí ověřit, že mají stejný předpis. Pro libovolné $a \in A$ je
$(h \circ (g \circ f))(a) = h((g \circ f)(a)) = h(g(f(a)))$,
$((h \circ g) \circ f)(a) = (h \circ g)(f(a)) = h(g(f(a)))$.

Příklad. Nechť X je množina, symbolem X^X značíme množinu všech zobrazení $X \to X$. Pak $(X^X, \circ)$ je pologrupa, v níž je neutrální prvek identita na X, totiž zobrazení $\mathrm{id} : X \to X$ splňující $\mathrm{id}(x) = x$ pro každé $x \in X$. K danému $f \in X^X$ existuje inverzní prvek, právě když f je bijekce; je jím inverzní zobrazení f^{-1}. Proto má-li množina X alespoň dva prvky, není $(X^X, \circ)$ grupa.

Definice. **Permutací** na množině X rozumíme libovolnou bijekci $X \to X$. Množinu všech permutací na množině X značíme $\mathbb{S}(X)$.

Příklad. $(\mathbb{S}(X), \circ)$ je grupa, nazývaná **grupa permutací** na X.

Grupa permutací

Poznámka. Připomeňme, že skládání zobrazení je asociativní: jsou-li $f : A \to B$, $g : B \to C$, $h : C \to D$ zobrazení, pak $h \circ (g \circ f) = (h \circ g) \circ f$. Skutečně, na obou stranách jsou zobrazení $A \to D$, stačí ověřit, že mají stejný předpis. Pro libovolné $a \in A$ je
$(h \circ (g \circ f))(a) = h((g \circ f)(a)) = h(g(f(a)))$,
$((h \circ g) \circ f)(a) = (h \circ g)(f(a)) = h(g(f(a)))$.

Příklad. Nechť X je množina, symbolem X^X značíme množinu všech zobrazení $X \to X$. Pak $(X^X, \circ)$ je pologrupa, v níž je neutrální prvek identita na X, totiž zobrazení $\mathrm{id} : X \to X$ splňující $\mathrm{id}(x) = x$ pro každé $x \in X$. K danému $f \in X^X$ existuje inverzní prvek, právě když f je bijekce; je jím inverzní zobrazení f^{-1}. Proto má-li množina X alespoň dva prvky, není $(X^X, \circ)$ grupa.

Definice. **Permutací** na množině X rozumíme libovolnou bijekci $X \to X$. Množinu všech permutací na množině X značíme $\mathbb{S}(X)$.

Příklad. $(\mathbb{S}(X), \circ)$ je grupa, nazývaná **grupa permutací** na X. Grupa $(\mathbb{S}(X), \circ)$ není komutativní, má-li množina X alespoň tři prvky.

Grupa shodností roviny

Příklad. Mějme dánu rovinu ρ.

Grupa shodností roviny

Příklad. Mějme dánu rovinu ρ.

Shodností roviny ρ rozumíme libovolné zobrazení $f : \rho \to \rho$ zachovávající vzdálenosti bodů, tj. pro libovolné body $A, B \in \rho$ je vzdálenost bodů A, B stejná jako vzdálenost jejich obrazů $f(A), f(B)$.

Grupa shodností roviny

Příklad. Mějme dánu rovinu ρ.

Shodností roviny ρ rozumíme libovolné zobrazení $f : \rho \to \rho$ zachovávající vzdálenosti bodů, tj. pro libovolné body $A, B \in \rho$ je vzdálenost bodů A, B stejná jako vzdálenost jejich obrazů $f(A), f(B)$.

Shodností roviny ρ je například každé její posunutí nebo rotace nebo osová souměrnost.

Grupa shodností roviny

Příklad. Mějme dánu rovinu ρ.

Shodností roviny ρ rozumíme libovolné zobrazení $f : \rho \to \rho$ zachovávající vzdálenosti bodů, tj. pro libovolné body $A, B \in \rho$ je vzdálenost bodů A, B stejná jako vzdálenost jejich obrazů $f(A), f(B)$.

Shodností roviny ρ je například každé její posunutí nebo rotace nebo osová souměrnost.

Každá shodnost roviny ρ je bijekce a k ní inverzní zobrazení je také shodnost roviny ρ.

Grupa shodností roviny

Příklad. Mějme dánu rovinu ρ.

Shodností roviny ρ rozumíme libovolné zobrazení $f : \rho \to \rho$ zachovávající vzdálenosti bodů, tj. pro libovolné body $A, B \in \rho$ je vzdálenost bodů A, B stejná jako vzdálenost jejich obrazů $f(A), f(B)$.

Shodností roviny ρ je například každé její posunutí nebo rotace nebo osová souměrnost.

Každá shodnost roviny ρ je bijekce a k ní inverzní zobrazení je také shodnost roviny ρ.

Zřejmě složením libovolných dvou shodností roviny ρ dostaneme opět shodnost roviny ρ.

Grupa shodností roviny

Příklad. Mějme dánu rovinu ρ.

Shodností roviny ρ rozumíme libovolné zobrazení $f : \rho \to \rho$ zachovávající vzdálenosti bodů, tj. pro libovolné body $A, B \in \rho$ je vzdálenost bodů A, B stejná jako vzdálenost jejich obrazů $f(A), f(B)$.

Shodností roviny ρ je například každé její posunutí nebo rotace nebo osová souměrnost.

Každá shodnost roviny ρ je bijekce a k ní inverzní zobrazení je také shodnost roviny ρ.

Zřejmě složením libovolných dvou shodností roviny ρ dostaneme opět shodnost roviny ρ.

Dostáváme, že množina všech shodností roviny ρ spolu s operací skládání je grupa, jejímž neutrálním prvkem je identita id.

Grupa všech shodností pravidelného n-úhelníka

Příklad. Pro dané přirozené číslo $n \geq 3$ si představme pravidelný n-úhelník.

Grupa všech shodností pravidelného n-úhelníka

Příklad. Pro dané přirozené číslo $n \geq 3$ si představme pravidelný n-úhelník. Označme $\mathbb{D}_n$ množinu všech shodností tohoto n-úhelníka, tedy zobrazení, která zachovávají vzdálenosti bodů a kterými je náš n-úhelník zobrazen sám na sebe.

Grupa všech shodností pravidelného n-úhelníka

Příklad. Pro dané přirozené číslo $n \geq 3$ si představme pravidelný n-úhelník. Označme $\mathbb{D}_n$ množinu všech shodností tohoto n-úhelníka, tedy zobrazení, která zachovávají vzdálenosti bodů a kterými je náš n-úhelník zobrazen sám na sebe.

Příkladem shodnosti tohoto n-úhelníka je libovolná rotace kolem středu n-úhelníka taková, že vrcholy se zobrazí opět na vrcholy.

Grupa všech shodností pravidelného n-úhelníka

Příklad. Pro dané přirozené číslo $n \geq 3$ si představme pravidelný n-úhelník. Označme $\mathbb{D}_n$ množinu všech shodností tohoto n-úhelníka, tedy zobrazení, která zachovávají vzdálenosti bodů a kterými je náš n-úhelník zobrazen sám na sebe.

Příkladem shodnosti tohoto n-úhelníka je libovolná rotace kolem středu n-úhelníka taková, že vrcholy se zobrazí opět na vrcholy. Takových rotací je právě n, započítáme-li i rotaci o nulový úhel, tj. identitu.

Grupa všech shodností pravidelného n-úhelníka

Příklad. Pro dané přirozené číslo $n \geq 3$ si představme pravidelný n-úhelník. Označme $\mathbb{D}_n$ množinu všech shodností tohoto n-úhelníka, tedy zobrazení, která zachovávají vzdálenosti bodů a kterými je náš n-úhelník zobrazen sám na sebe.

Příkladem shodnosti tohoto n-úhelníka je libovolná rotace kolem středu n-úhelníka taková, že vrcholy se zobrazí opět na vrcholy. Takových rotací je právě n, započítáme-li i rotaci o nulový úhel, tj. identitu.

Dalším příkladem shodnosti je osová souměrnost vzhledem k ose procházející středem n-úhelníka a některým z vrcholů či středů stran (pro liché n prochází vrcholem a středem protější strany, pro sudé n prochází protějšími vrcholy anebo středy protějších stran).

Grupa všech shodností pravidelného n-úhelníka

Příklad. Pro dané přirozené číslo $n \geq 3$ si představme pravidelný n-úhelník. Označme $\mathbb{D}_n$ množinu všech shodností tohoto n-úhelníka, tedy zobrazení, která zachovávají vzdálenosti bodů a kterými je náš n-úhelník zobrazen sám na sebe.

Příkladem shodnosti tohoto n-úhelníka je libovolná rotace kolem středu n-úhelníka taková, že vrcholy se zobrazí opět na vrcholy. Takových rotací je právě n, započítáme-li i rotaci o nulový úhel, tj. identitu.

Dalším příkladem shodnosti je osová souměrnost vzhledem k ose procházející středem n-úhelníka a některým z vrcholů či středů stran (pro liché n prochází vrcholem a středem protější strany, pro sudé n prochází protějšími vrcholy anebo středy protějších stran). Takových osových souměrností je právě n.

Grupa všech shodností pravidelného n-úhelníka

Příklad. Pro dané přirozené číslo $n \geq 3$ si představme pravidelný n-úhelník. Označme $\mathbb{D}_n$ množinu všech shodností tohoto n-úhelníka, tedy zobrazení, která zachovávají vzdálenosti bodů a kterými je náš n-úhelník zobrazen sám na sebe.

Příkladem shodnosti tohoto n-úhelníka je libovolná rotace kolem středu n-úhelníka taková, že vrcholy se zobrazí opět na vrcholy. Takových rotací je právě n, započítáme-li i rotaci o nulový úhel, tj. identitu.

Dalším příkladem shodnosti je osová souměrnost vzhledem k ose procházející středem n-úhelníka a některým z vrcholů či středů stran (pro liché n prochází vrcholem a středem protější strany, pro sudé n prochází protějšími vrcholy anebo středy protějších stran). Takových osových souměrností je právě n.

Celkem jsme zatím našli $2n$ shodností našeho n-úhelníka.

Grupa $(\mathbb{D}_n, \circ)$ shodností pravidelného n-úhelníka

Každou shodností našeho n-úhelníka se musí libovolný vrchol n-úhelníka zobrazit na nějaký vrchol, každá dvojice sousedních vrcholů se musí zobrazit na některou dvojici sousedních vrcholů.

Grupa $(\mathbb{D}_n, \circ)$ shodností pravidelného n-úhelníka

Každou shodností našeho n-úhelníka se musí libovolný vrchol n-úhelníka zobrazit na nějaký vrchol, každá dvojice sousedních vrcholů se musí zobrazit na některou dvojici sousedních vrcholů.

Zvolme pevně dva sousední vrcholy A, B. Každou shodností se musí vrchol A zobrazit na některý z n vrcholů (pro jeho volbu máme n možností) a vrchol B se musí zobrazit na některý ze dvou jeho sousedních vrcholů (pro jeho volbu máme nyní jen 2 možnosti).

Grupa $(\mathbb{D}_n, \circ)$ shodností pravidelného n-úhelníka

Každou shodností našeho n-úhelníka se musí libovolný vrchol n-úhelníka zobrazit na nějaký vrchol, každá dvojice sousedních vrcholů se musí zobrazit na některou dvojici sousedních vrcholů.

Zvolme pevně dva sousední vrcholy A, B. Každou shodností se musí vrchol A zobrazit na některý z n vrcholů (pro jeho volbu máme n možností) a vrchol B se musí zobrazit na některý ze dvou jeho sousedních vrcholů (pro jeho volbu máme nyní jen 2 možnosti). Přitom obrazy těchto dvou vrcholů A, B je celá shodnost jednoznačně určena.

Grupa $(\mathbb{D}_n, \circ)$ shodností pravidelného n-úhelníka

Každou shodností našeho n-úhelníka se musí libovolný vrchol n-úhelníka zobrazit na nějaký vrchol, každá dvojice sousedních vrcholů se musí zobrazit na některou dvojici sousedních vrcholů.

Zvolme pevně dva sousední vrcholy A, B. Každou shodností se musí vrchol A zobrazit na některý z n vrcholů (pro jeho volbu máme n možností) a vrchol B se musí zobrazit na některý ze dvou jeho sousedních vrcholů (pro jeho volbu máme nyní jen 2 možnosti). Přitom obrazy těchto dvou vrcholů A, B je celá shodnost jednoznačně určena.

Proto shodností pravidelného n-úhelníka nemůže být více než $2n$.

Grupa $(\mathbb{D}_n, \circ)$ shodností pravidelného n-úhelníka

Každou shodností našeho n-úhelníka se musí libovolný vrchol n-úhelníka zobrazit na nějaký vrchol, každá dvojice sousedních vrcholů se musí zobrazit na některou dvojici sousedních vrcholů.

Zvolme pevně dva sousední vrcholy A, B. Každou shodností se musí vrchol A zobrazit na některý z n vrcholů (pro jeho volbu máme n možností) a vrchol B se musí zobrazit na některý ze dvou jeho sousedních vrcholů (pro jeho volbu máme nyní jen 2 možnosti). Přitom obrazy těchto dvou vrcholů A, B je celá shodnost jednoznačně určena.

Proto shodností pravidelného n-úhelníka nemůže být více než $2n$. A protože jsme jich už $2n$ našli, je jich právě $2n$.

Grupa $(\mathbb{D}_n, \circ)$ shodností pravidelného n-úhelníka

Každou shodností našeho n-úhelníka se musí libovolný vrchol n-úhelníka zobrazit na nějaký vrchol, každá dvojice sousedních vrcholů se musí zobrazit na některou dvojici sousedních vrcholů.

Zvolme pevně dva sousední vrcholy A, B. Každou shodností se musí vrchol A zobrazit na některý z n vrcholů (pro jeho volbu máme n možností) a vrchol B se musí zobrazit na některý ze dvou jeho sousedních vrcholů (pro jeho volbu máme nyní jen 2 možnosti). Přitom obrazy těchto dvou vrcholů A, B je celá shodnost jednoznačně určena.

Proto shodností pravidelného n-úhelníka nemůže být více než $2n$. A protože jsme jich už $2n$ našli, je jich právě $2n$.

Složením libovolných dvou shodností dostaneme opět shodnost; inverzní zobrazení k libovolné shodnosti je shodnost.

Grupa $(\mathbb{D}_n, \circ)$ shodností pravidelného n-úhelníka

Každou shodností našeho n-úhelníka se musí libovolný vrchol n-úhelníka zobrazit na nějaký vrchol, každá dvojice sousedních vrcholů se musí zobrazit na některou dvojici sousedních vrcholů.

Zvolme pevně dva sousední vrcholy A, B. Každou shodností se musí vrchol A zobrazit na některý z n vrcholů (pro jeho volbu máme n možností) a vrchol B se musí zobrazit na některý ze dvou jeho sousedních vrcholů (pro jeho volbu máme nyní jen 2 možnosti). Přitom obrazy těchto dvou vrcholů A, B je celá shodnost jednoznačně určena.

Proto shodností pravidelného n-úhelníka nemůže být více než $2n$. A protože jsme jich už $2n$ našli, je jich právě $2n$.

Složením libovolných dvou shodností dostaneme opět shodnost; inverzní zobrazení k libovolné shodnosti je shodnost. Proto je množina $\mathbb{D}_n$ spolu s operací skládání grupou, která má $2n$ prvků.

Grupa $(\mathbb{D}_n, \circ)$ shodností pravidelného n-úhelníka

Každou shodností našeho n-úhelníka se musí libovolný vrchol n-úhelníka zobrazit na nějaký vrchol, každá dvojice sousedních vrcholů se musí zobrazit na některou dvojici sousedních vrcholů.

Zvolme pevně dva sousední vrcholy A, B. Každou shodností se musí vrchol A zobrazit na některý z n vrcholů (pro jeho volbu máme n možností) a vrchol B se musí zobrazit na některý ze dvou jeho sousedních vrcholů (pro jeho volbu máme nyní jen 2 možnosti). Přitom obrazy těchto dvou vrcholů A, B je celá shodnost jednoznačně určena.

Proto shodností pravidelného n-úhelníka nemůže být více než $2n$. A protože jsme jich už $2n$ našli, je jich právě $2n$.

Složením libovolných dvou shodností dostaneme opět shodnost; inverzní zobrazení k libovolné shodnosti je shodnost. Proto je množina $\mathbb{D}_n$ spolu s operací skládání grupou, která má $2n$ prvků.

Snadno se ověří, že tato grupa $(\mathbb{D}_n, \circ)$ není komutativní.