Invertibilní prvky

Označení. Nechť $(G, \cdot)$ je grupoid s neutrálním prvkem. Víme, že tento neutrální prvek je v G jediný. Budeme jej označovat symbolem 1 (přestože to nemusí být přirozené číslo 1).

Invertibilní prvky

Označení. Nechť $(G, \cdot)$ je grupoid s neutrálním prvkem. Víme, že tento neutrální prvek je v G jediný. Budeme jej označovat symbolem 1 (přestože to nemusí být přirozené číslo 1).

Definice. Nechť $(G, \cdot)$ je pologrupa s neutrálním prvkem 1. Pokud k nějakému $a \in G$ existuje v G prvek inverzní, říkáme, že prvek a je **invertibilní**.

Invertibilní prvky

Označení. Nechť $(G, \cdot)$ je grupoid s neutrálním prvkem. Víme, že tento neutrální prvek je v G jediný. Budeme jej označovat symbolem 1 (přestože to nemusí být přirozené číslo 1).

Definice. Nechť $(G, \cdot)$ je pologrupa s neutrálním prvkem 1. Pokud k nějakému $a \in G$ existuje v G prvek inverzní, říkáme, že prvek a je **invertibilní**. Inverzní prvek k prvku a budeme označovat symbolem a^{-1} (víme totiž, že v pologrupě existuje k danému prvku nejvýše jeden prvek inverzní).

Invertibilní prvky

Označení. Nechť $(G, \cdot)$ je grupoid s neutrálním prvkem. Víme, že tento neutrální prvek je v G jediný. Budeme jej označovat symbolem 1 (přestože to nemusí být přirozené číslo 1).

Definice. Nechť $(G, \cdot)$ je pologrupa s neutrálním prvkem 1. Pokud k nějakému $a \in G$ existuje v G prvek inverzní, říkáme, že prvek a je **invertibilní**. Inverzní prvek k prvku a budeme označovat symbolem a^{-1} (víme totiž, že v pologrupě existuje k danému prvku nejvýše jeden prvek inverzní).

Věta. Nechť $(G, \cdot)$ je pologrupa s neutrálním prvkem 1, nechť a, b jsou libovolné invertibilní prvky z G. Pak platí

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

Invertibilní prvky

Označení. Nechť $(G, \cdot)$ je grupoid s neutrálním prvkem. Víme, že tento neutrální prvek je v G jediný. Budeme jej označovat symbolem 1 (přestože to nemusí být přirozené číslo 1).

Definice. Nechť $(G, \cdot)$ je pologrupa s neutrálním prvkem 1. Pokud k nějakému $a \in G$ existuje v G prvek inverzní, říkáme, že prvek a je **invertibilní**. Inverzní prvek k prvku a budeme označovat symbolem a^{-1} (víme totiž, že v pologrupě existuje k danému prvku nejvýše jeden prvek inverzní).

Věta. Nechť $(G, \cdot)$ je pologrupa s neutrálním prvkem 1, nechť a, b jsou libovolné invertibilní prvky z G. Pak platí

$$\begin{aligned} 1^{-1} &= 1, \\ (a^{-1})^{-1} &= a, \end{aligned}$$

Invertibilní prvky

Označení. Nechť $(G, \cdot)$ je grupoid s neutrálním prvkem. Víme, že tento neutrální prvek je v G jediný. Budeme jej označovat symbolem 1 (přestože to nemusí být přirozené číslo 1).

Definice. Nechť $(G, \cdot)$ je pologrupa s neutrálním prvkem 1. Pokud k nějakému $a \in G$ existuje v G prvek inverzní, říkáme, že prvek a je **invertibilní**. Inverzní prvek k prvku a budeme označovat symbolem a^{-1} (víme totiž, že v pologrupě existuje k danému prvku nejvýše jeden prvek inverzní).

Věta. Nechť $(G, \cdot)$ je pologrupa s neutrálním prvkem 1, nechť a, b jsou libovolné invertibilní prvky z G. Pak platí

$$\begin{aligned} 1^{-1} &= 1, \\ (a^{-1})^{-1} &= a, \\ (a \cdot b)^{-1} &= b^{-1} \cdot a^{-1}. \end{aligned}$$

[Věta 4.6, str. 24]

Množina všech invertibilních prvků pologrupy tvoří grupu

Věta. *Nechť* $(G, \cdot)$ *je pologrupa s neutrálním prvkem* 1, H *množina všech invertibilních prvků z* G. *Pak* $(H, \cdot)$ *je grupa.* [Věta 4.7, str. 25]

Množina všech invertibilních prvků pologrupy tvoří grupu

Věta. *Nechť* $(G, \cdot)$ *je pologrupa s neutrálním prvkem* 1, H *množina všech invertibilních prvků z* G. *Pak* $(H, \cdot)$ *je grupa.* [Věta 4.7, str. 25]

Poznámka. Operace $\cdot$ na množině H je zúžením původní operace na množině G (má pro prvky z $H \times H$ stejný předpis, ale je definována na menším definičním oboru $H \times H$ a má menší obor hodnot H).

Množina všech invertibilních prvků pologrupy tvoří grupu

Věta. *Nechť* $(G, \cdot)$ *je pologrupa s neutrálním prvkem* 1, H *množina všech invertibilních prvků z* G. *Pak* $(H, \cdot)$ *je grupa.* [Věta 4.7, str. 25]

Poznámka. Operace $\cdot$ na množině H je zúžením původní operace na množině G (má pro prvky z $H \times H$ stejný předpis, ale je definována na menším definičním oboru $H \times H$ a má menší obor hodnot H). Dopouštíme se vědomě jisté nepřesnosti: jestliže $G \neq H$, jsou tyto operace dvě různá zobrazení, přesto je obě značíme stejným symbolem $\cdot$ (s nadějí, že nedojde k nedorozumění).

Množina všech invertibilních prvků pologrupy tvoří grupu

Věta. *Nechť* $(G, \cdot)$ *je pologrupa s neutrálním prvkem* 1, H *množina všech invertibilních prvků z* G. *Pak* $(H, \cdot)$ *je grupa.* [Věta 4.7, str. 25]

Poznámka. Operace $\cdot$ na množině H je zúžením původní operace na množině G (má pro prvky z $H \times H$ stejný předpis, ale je definována na menším definičním oboru $H \times H$ a má menší obor hodnot H). Dopouštíme se vědomě jisté nepřesnosti: jestliže $G \neq H$, jsou tyto operace dvě různá zobrazení, přesto je obě značíme stejným symbolem $\cdot$ (s nadějí, že nedojde k nedorozumění).

Příklad. Užitím předchozí věty z pologrupy $(\mathbb{Q}, \cdot)$, dostaneme grupu $(\mathbb{Q}^*, \cdot)$,

Množina všech invertibilních prvků pologrupy tvoří grupu

Věta. *Nechť $(G, \cdot)$ je pologrupa s neutrálním prvkem 1, H množina všech invertibilních prvků z G. Pak $(H, \cdot)$ je grupa.* [Věta 4.7, str. 25]

Poznámka. Operace $\cdot$ na množině H je zúžením původní operace na množině G (má pro prvky z $H \times H$ stejný předpis, ale je definována na menším definičním oboru $H \times H$ a má menší obor hodnot H). Dopouštíme se vědomě jisté nepřesnosti: jestliže $G \neq H$, jsou tyto operace dvě různá zobrazení, přesto je obě značíme stejným symbolem $\cdot$ (s nadějí, že nedojde k nedorozumění).

Příklad. Užitím předchozí věty z pologrupy $(\mathbb{Q}, \cdot)$, dostaneme grupu $(\mathbb{Q}^*, \cdot)$, podobně z pologrupy $(\mathbb{Z}, \cdot)$ dostaneme grupu $(\{1, -1\}, \cdot)$.

Množina všech invertibilních prvků pologrupy tvoří grupu

Věta. *Nechť $(G, \cdot)$ je pologrupa s neutrálním prvkem 1, H množina všech invertibilních prvků z G. Pak $(H, \cdot)$ je grupa.* [Věta 4.7, str. 25]

Poznámka. Operace $\cdot$ na množině H je zúžením původní operace na množině G (má pro prvky z $H \times H$ stejný předpis, ale je definována na menším definičním oboru $H \times H$ a má menší obor hodnot H). Dopouštíme se vědomě jisté nepřesnosti: jestliže $G \neq H$, jsou tyto operace dvě různá zobrazení, přesto je obě značíme stejným symbolem $\cdot$ (s nadějí, že nedojde k nedorozumění).

Příklad. Užitím předchozí věty z pologrupy $(\mathbb{Q}, \cdot)$, dostaneme grupu $(\mathbb{Q}^*, \cdot)$, podobně z pologrupy $(\mathbb{Z}, \cdot)$ dostaneme grupu $(\{1, -1\}, \cdot)$. Tak jsme také pro libovolnou množinu X z pologrupy $(X^X, \circ)$ vytvořili grupu permutací $(\mathbb{S}(X), \circ)$.

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

Věta. *Nechť $m \in \mathbb{N}$, $a \in \mathbb{Z}$ jsou libovolná. Zbytková třída $[a]_m$ je invertibilní v pologrupě $(\mathbb{Z}_m, \cdot)$, právě když celá čísla a, m jsou nesoudělná.* [Věta 3.13, str. 19]

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

Věta. *Nechť $m \in \mathbb{N}$, $a \in \mathbb{Z}$ jsou libovolná. Zbytková třída $[a]_m$ je invertibilní v pologrupě $(\mathbb{Z}_m, \cdot)$, právě když celá čísla a, m jsou nesoudělná.* [Věta 3.13, str. 19]

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

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

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

Věta. *Nechť $m \in \mathbb{N}$, $a \in \mathbb{Z}$ jsou libovolná. Zbytková třída $[a]_m$ je invertibilní v pologrupě $(\mathbb{Z}_m, \cdot)$, právě když celá čísla a, m jsou nesoudělná.* [Věta 3.13, str. 19]

Označení. Pro libovolné $m \in \mathbb{N}$ označme $\mathbb{Z}_m^\times$ množinu všech zbytkových tříd $[a]_m$, které jsou invertibilní 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.*

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

Věta. *Nechť $m \in \mathbb{N}$, $a \in \mathbb{Z}$ jsou libovolná. Zbytková třída $[a]_m$ je invertibilní v pologrupě $(\mathbb{Z}_m, \cdot)$, právě když celá čísla a, m jsou nesoudělná.* [Věta 3.13, str. 19]

Označení. Pro libovolné $m \in \mathbb{N}$ označme $\mathbb{Z}_m^\times$ množinu všech zbytkových tříd $[a]_m$, které jsou invertibilní 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

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

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

Věta. *Nechť $m \in \mathbb{N}$, $a \in \mathbb{Z}$ jsou libovolná. Zbytková třída $[a]_m$ je invertibilní v pologrupě $(\mathbb{Z}_m, \cdot)$, právě když celá čísla a, m jsou nesoudělná.* [Věta 3.13, str. 19]

Označení. Pro libovolné $m \in \mathbb{N}$ označme $\mathbb{Z}_m^\times$ množinu všech zbytkových tříd $[a]_m$, které jsou invertibilní 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 $|\mathbb{Z}_m^\times| = \varphi(m)$.*

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

Věta. *Nechť $m \in \mathbb{N}$, $a \in \mathbb{Z}$ jsou libovolná. Zbytková třída $[a]_m$ je invertibilní v pologrupě $(\mathbb{Z}_m, \cdot)$, právě když celá čísla a, m jsou nesoudělná.* [Věta 3.13, str. 19]

Označení. Pro libovolné $m \in \mathbb{N}$ označme $\mathbb{Z}_m^\times$ množinu všech zbytkových tříd $[a]_m$, které jsou invertibilní 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**.

První věta o Eulerově funkci $\varphi(m) = |\mathbb{Z}_m^\times|$

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

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

Příklad. $\varphi(1) = 1$, $\varphi(2) = 1$, $\varphi(3) = 2$, $\varphi(4) = 2$, $\varphi(5) = 4$, ...

První věta o Eulerově funkci $\varphi(m) = |\mathbb{Z}_m^\times|$

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

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

Příklad. $\varphi(1) = 1$, $\varphi(2) = 1$, $\varphi(3) = 2$, $\varphi(4) = 2$, $\varphi(5) = 4$, ...

Věta. *Je-li p prvočíslo a $n \in \mathbb{N}$, pak* $\varphi(p^n) = (p-1) \cdot p^{n-1}$.

První věta o Eulerově funkci $\varphi(m) = |\mathbb{Z}_m^\times|$

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

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

Příklad. $\varphi(1) = 1$, $\varphi(2) = 1$, $\varphi(3) = 2$, $\varphi(4) = 2$, $\varphi(5) = 4$, ...

Věta. *Je-li p prvočíslo a $n \in \mathbb{N}$, pak* $\varphi(p^n) = (p-1) \cdot p^{n-1}$.

Důkaz. Čísla soudělná s p^n jsou právě ta, která jsou dělitelná p.

První věta o Eulerově funkci $\varphi(m) = |\mathbb{Z}_m^\times|$

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

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

Příklad. $\varphi(1) = 1$, $\varphi(2) = 1$, $\varphi(3) = 2$, $\varphi(4) = 2$, $\varphi(5) = 4$, ...

Věta. *Je-li p prvočíslo a $n \in \mathbb{N}$, pak* $\varphi(p^n) = (p-1) \cdot p^{n-1}$.

Důkaz. Čísla soudělná s p^n jsou právě ta, která jsou dělitelná p.
Z každých p po sobě jdoucích čísel je právě jedno dělitelné p.

První věta o Eulerově funkci $\varphi(m) = |\mathbb{Z}_m^\times|$

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

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

Příklad. $\varphi(1) = 1$, $\varphi(2) = 1$, $\varphi(3) = 2$, $\varphi(4) = 2$, $\varphi(5) = 4$, ...

Věta. *Je-li p prvočíslo a $n \in \mathbb{N}$, pak* $\varphi(p^n) = (p-1) \cdot p^{n-1}$.

Důkaz. Čísla soudělná s p^n jsou právě ta, která jsou dělitelná p.

Z každých p po sobě jdoucích čísel je právě jedno dělitelné p.

Proto je mezi čísly $1, 2, \ldots, p^n$ právě $\frac{p^n}{p} = p^{n-1}$ čísel, která jsou soudělná s p^n.

První věta o Eulerově funkci $\varphi(m) = |\mathbb{Z}_m^\times|$

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

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

Příklad. $\varphi(1) = 1$, $\varphi(2) = 1$, $\varphi(3) = 2$, $\varphi(4) = 2$, $\varphi(5) = 4$, ...

Věta. *Je-li p prvočíslo a $n \in \mathbb{N}$, pak* $\varphi(p^n) = (p-1) \cdot p^{n-1}$.

Důkaz. Čísla soudělná s p^n jsou právě ta, která jsou dělitelná p.

Z každých p po sobě jdoucích čísel je právě jedno dělitelné p.

Proto je mezi čísly $1, 2, \ldots, p^n$ právě $\frac{p^n}{p} = p^{n-1}$ čísel, která jsou soudělná s p^n.

Nesoudělných s p^n je mezi nimi právě $\varphi(p^n)$ čísel.

První věta o Eulerově funkci $\varphi(m) = |\mathbb{Z}_m^\times|$

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

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

Příklad. $\varphi(1) = 1$, $\varphi(2) = 1$, $\varphi(3) = 2$, $\varphi(4) = 2$, $\varphi(5) = 4$, ...

Věta. *Je-li p prvočíslo a $n \in \mathbb{N}$, pak* $\varphi(p^n) = (p-1) \cdot p^{n-1}$.

Důkaz. Čísla soudělná s p^n jsou právě ta, která jsou dělitelná p.

Z každých p po sobě jdoucích čísel je právě jedno dělitelné p.

Proto je mezi čísly $1, 2, \ldots, p^n$ právě $\frac{p^n}{p} = p^{n-1}$ čísel, která jsou soudělná s p^n.

Nesoudělných s p^n je mezi nimi právě $\varphi(p^n)$ čísel.

Je tedy $\varphi(p^n) = p^n - p^{n-1} = (p-1) \cdot p^{n-1}$.

Druhá věta o Eulerově funkci $\varphi(m) = |\mathbb{Z}_m^\times|$

Věta. *Jsou-li* $a, b \in \mathbb{N}$ *nesoudělná přirozená čísla, pak* $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$.

Druhá věta o Eulerově funkci $\varphi(m) = |\mathbb{Z}_m^\times|$

Věta. *Jsou-li $a, b \in \mathbb{N}$ nesoudělná přirozená čísla, pak* $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$.

Důkaz. Protože $(a, b) = 1$, nejmenší společný násobek čísel a, b je $a \cdot b$.

Druhá věta o Eulerově funkci $\varphi(m) = |\mathbb{Z}_m^\times|$

Věta. *Jsou-li $a, b \in \mathbb{N}$ nesoudělná přirozená čísla, pak* $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$.

Důkaz. Protože $(a, b) = 1$, nejmenší společný násobek čísel a, b je $a \cdot b$. Definujme zobrazení $f : \mathbb{Z}_{ab} \to \mathbb{Z}_a \times \mathbb{Z}_b$ předpisem $f([c]_{ab}) = ([c]_a, [c]_b)$ pro libovolné $c \in \mathbb{Z}$.

Druhá věta o Eulerově funkci $\varphi(m) = |\mathbb{Z}_m^\times|$

Věta. *Jsou-li $a, b \in \mathbb{N}$ nesoudělná přirozená čísla, pak* $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$.

Důkaz. Protože $(a, b) = 1$, nejmenší společný násobek čísel a, b je $a \cdot b$. Definujme zobrazení $f : \mathbb{Z}_{ab} \to \mathbb{Z}_a \times \mathbb{Z}_b$ předpisem $f([c]_{ab}) = ([c]_a, [c]_b)$ pro libovolné $c \in \mathbb{Z}$.
Je třeba ověřit korektnost této definice:

Druhá věta o Eulerově funkci $\varphi(m) = |\mathbb{Z}_m^\times|$

Věta. *Jsou-li $a, b \in \mathbb{N}$ nesoudělná přirozená čísla, pak* $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$.

Důkaz. Protože $(a, b) = 1$, nejmenší společný násobek čísel a, b je $a \cdot b$. Definujme zobrazení $f : \mathbb{Z}_{ab} \to \mathbb{Z}_a \times \mathbb{Z}_b$ předpisem $f([c]_{ab}) = ([c]_a, [c]_b)$ pro libovolné $c \in \mathbb{Z}$.
Je třeba ověřit korektnost této definice: pro libovolné $c, d \in \mathbb{Z}$ platí $[c]_{ab} = [d]_{ab}$, právě když $ab \mid c - d$.

Druhá věta o Eulerově funkci $\varphi(m) = |\mathbb{Z}_m^\times|$

Věta. *Jsou-li $a, b \in \mathbb{N}$ nesoudělná přirozená čísla, pak* $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$.

Důkaz. Protože $(a, b) = 1$, nejmenší společný násobek čísel a, b je $a \cdot b$. Definujme zobrazení $f : \mathbb{Z}_{ab} \to \mathbb{Z}_a \times \mathbb{Z}_b$ předpisem $f([c]_{ab}) = ([c]_a, [c]_b)$ pro libovolné $c \in \mathbb{Z}$.
Je třeba ověřit korektnost této definice: pro libovolné $c, d \in \mathbb{Z}$ platí $[c]_{ab} = [d]_{ab}$, právě když $ab \mid c - d$.
Protože ab je nejmenší společný násobek čísel a, b, platí
$ab \mid c - d \;\Leftrightarrow\; a \mid c - d \;\wedge\; b \mid c - d$.

Druhá věta o Eulerově funkci $\varphi(m) = |\mathbb{Z}_m^\times|$

Věta. *Jsou-li $a, b \in \mathbb{N}$ nesoudělná přirozená čísla, pak* $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$.

Důkaz. Protože $(a, b) = 1$, nejmenší společný násobek čísel a, b je $a \cdot b$. Definujme zobrazení $f : \mathbb{Z}_{ab} \to \mathbb{Z}_a \times \mathbb{Z}_b$ předpisem $f([c]_{ab}) = ([c]_a, [c]_b)$ pro libovolné $c \in \mathbb{Z}$.
Je třeba ověřit korektnost této definice: pro libovolné $c, d \in \mathbb{Z}$ platí $[c]_{ab} = [d]_{ab}$, právě když $ab \mid c - d$.
Protože ab je nejmenší společný násobek čísel a, b, platí $ab \mid c - d \;\Leftrightarrow\; a \mid c - d \;\wedge\; b \mid c - d$.
Celkem tedy $[c]_{ab} = [d]_{ab} \;\Leftrightarrow\; ([c]_a, [c]_b) = ([d]_a, [d]_b)$.

Druhá věta o Eulerově funkci $\varphi(m) = |\mathbb{Z}_m^\times|$

Věta. *Jsou-li $a, b \in \mathbb{N}$ nesoudělná přirozená čísla, pak* $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$.

Důkaz. Protože $(a, b) = 1$, nejmenší společný násobek čísel a, b je $a \cdot b$. Definujme zobrazení $f : \mathbb{Z}_{ab} \to \mathbb{Z}_a \times \mathbb{Z}_b$ předpisem $f([c]_{ab}) = ([c]_a, [c]_b)$ pro libovolné $c \in \mathbb{Z}$.
Je třeba ověřit korektnost této definice: pro libovolné $c, d \in \mathbb{Z}$ platí $[c]_{ab} = [d]_{ab}$, právě když $ab \mid c - d$.
Protože ab je nejmenší společný násobek čísel a, b, platí $ab \mid c - d \;\Leftrightarrow\; a \mid c - d \;\wedge\; b \mid c - d$.
Celkem tedy $[c]_{ab} = [d]_{ab} \;\Leftrightarrow\; ([c]_a, [c]_b) = ([d]_a, [d]_b)$.
Ověřili jsme nejen korektnost definice f, ale i to, že f je injektivní.
A protože množiny $\mathbb{Z}_{ab}$ i $\mathbb{Z}_a \times \mathbb{Z}_b$ mají obě ab prvků, je f bijekce.

Druhá věta o Eulerově funkci $\varphi(m) = |\mathbb{Z}_m^\times|$

Věta. *Jsou-li $a, b \in \mathbb{N}$ nesoudělná přirozená čísla, pak* $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$.

Důkaz. Protože $(a, b) = 1$, nejmenší společný násobek čísel a, b je $a \cdot b$. Definujme zobrazení $f : \mathbb{Z}_{ab} \to \mathbb{Z}_a \times \mathbb{Z}_b$ předpisem $f([c]_{ab}) = ([c]_a, [c]_b)$ pro libovolné $c \in \mathbb{Z}$.
Je třeba ověřit korektnost této definice: pro libovolné $c, d \in \mathbb{Z}$ platí $[c]_{ab} = [d]_{ab}$, právě když $ab \mid c - d$.
Protože ab je nejmenší společný násobek čísel a, b, platí
$ab \mid c - d \;\Leftrightarrow\; a \mid c - d \;\wedge\; b \mid c - d$.
Celkem tedy $[c]_{ab} = [d]_{ab} \;\Leftrightarrow\; ([c]_a, [c]_b) = ([d]_a, [d]_b)$.
Ověřili jsme nejen korektnost definice f, ale i to, že f je injektivní.
A protože množiny $\mathbb{Z}_{ab}$ i $\mathbb{Z}_a \times \mathbb{Z}_b$ mají obě ab prvků, je f bijekce.
Libovolné $c \in \mathbb{Z}$ splňuje $(c, ab) \neq 1$, právě když existuje prvočíslo p tak, že $p \mid c$ a současně $p \mid ab$,

Druhá věta o Eulerově funkci $\varphi(m) = |\mathbb{Z}_m^\times|$

Věta. *Jsou-li $a, b \in \mathbb{N}$ nesoudělná přirozená čísla, pak* $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$.

Důkaz. Protože $(a, b) = 1$, nejmenší společný násobek čísel a, b je $a \cdot b$. Definujme zobrazení $f : \mathbb{Z}_{ab} \to \mathbb{Z}_a \times \mathbb{Z}_b$ předpisem $f([c]_{ab}) = ([c]_a, [c]_b)$ pro libovolné $c \in \mathbb{Z}$.
Je třeba ověřit korektnost této definice: pro libovolné $c, d \in \mathbb{Z}$ platí $[c]_{ab} = [d]_{ab}$, právě když $ab \mid c - d$.
Protože ab je nejmenší společný násobek čísel a, b, platí $ab \mid c - d \;\Leftrightarrow\; a \mid c - d \;\wedge\; b \mid c - d$.
Celkem tedy $[c]_{ab} = [d]_{ab} \;\Leftrightarrow\; ([c]_a, [c]_b) = ([d]_a, [d]_b)$.
Ověřili jsme nejen korektnost definice f, ale i to, že f je injektivní.
A protože množiny $\mathbb{Z}_{ab}$ i $\mathbb{Z}_a \times \mathbb{Z}_b$ mají obě ab prvků, je f bijekce.
Libovolné $c \in \mathbb{Z}$ splňuje $(c, ab) \neq 1$, právě když existuje prvočíslo p tak, že $p \mid c$ a současně $p \mid ab$, tj. že $p \mid c$, $p \mid a$ nebo $p \mid c$, $p \mid b$,

Druhá věta o Eulerově funkci $\varphi(m) = |\mathbb{Z}_m^\times|$

Věta. *Jsou-li $a, b \in \mathbb{N}$ nesoudělná přirozená čísla, pak* $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$.

Důkaz. Protože $(a, b) = 1$, nejmenší společný násobek čísel a, b je $a \cdot b$. Definujme zobrazení $f : \mathbb{Z}_{ab} \to \mathbb{Z}_a \times \mathbb{Z}_b$ předpisem $f([c]_{ab}) = ([c]_a, [c]_b)$ pro libovolné $c \in \mathbb{Z}$.
Je třeba ověřit korektnost této definice: pro libovolné $c, d \in \mathbb{Z}$ platí $[c]_{ab} = [d]_{ab}$, právě když $ab \mid c - d$.
Protože ab je nejmenší společný násobek čísel a, b, platí $ab \mid c - d \;\Leftrightarrow\; a \mid c - d \;\wedge\; b \mid c - d$.
Celkem tedy $[c]_{ab} = [d]_{ab} \;\Leftrightarrow\; ([c]_a, [c]_b) = ([d]_a, [d]_b)$.
Ověřili jsme nejen korektnost definice f, ale i to, že f je injektivní.
A protože množiny $\mathbb{Z}_{ab}$ i $\mathbb{Z}_a \times \mathbb{Z}_b$ mají obě ab prvků, je f bijekce.
Libovolné $c \in \mathbb{Z}$ splňuje $(c, ab) \neq 1$, právě když existuje prvočíslo p tak, že $p \mid c$ a současně $p \mid ab$, tj. že $p \mid c$, $p \mid a$ nebo $p \mid c$, $p \mid b$, tj. právě když $(c, a) \neq 1$ nebo $(c, b) \neq 1$.

Druhá věta o Eulerově funkci $\varphi(m) = |\mathbb{Z}_m^\times|$

Věta. *Jsou-li $a, b \in \mathbb{N}$ nesoudělná přirozená čísla, pak* $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$.

Důkaz. Protože $(a, b) = 1$, nejmenší společný násobek čísel a, b je $a \cdot b$. Definujme zobrazení $f : \mathbb{Z}_{ab} \to \mathbb{Z}_a \times \mathbb{Z}_b$ předpisem $f([c]_{ab}) = ([c]_a, [c]_b)$ pro libovolné $c \in \mathbb{Z}$.
Je třeba ověřit korektnost této definice: pro libovolné $c, d \in \mathbb{Z}$ platí $[c]_{ab} = [d]_{ab}$, právě když $ab \mid c - d$.
Protože ab je nejmenší společný násobek čísel a, b, platí $ab \mid c - d \;\Leftrightarrow\; a \mid c - d \;\wedge\; b \mid c - d$.
Celkem tedy $[c]_{ab} = [d]_{ab} \;\Leftrightarrow\; ([c]_a, [c]_b) = ([d]_a, [d]_b)$.
Ověřili jsme nejen korektnost definice f, ale i to, že f je injektivní.
A protože množiny $\mathbb{Z}_{ab}$ i $\mathbb{Z}_a \times \mathbb{Z}_b$ mají obě ab prvků, je f bijekce.
Libovolné $c \in \mathbb{Z}$ splňuje $(c, ab) \neq 1$, právě když existuje prvočíslo p tak, že $p \mid c$ a současně $p \mid ab$, tj. že $p \mid c$, $p \mid a$ nebo $p \mid c$, $p \mid b$, tj. právě když $(c, a) \neq 1$ nebo $(c, b) \neq 1$. Celkem tedy $[c]_{ab} \in \mathbb{Z}_{ab}^\times$, právě když $f([c]_{ab}) \in \mathbb{Z}_a^\times \times \mathbb{Z}_b^\times$.

Druhá věta o Eulerově funkci $\varphi(m) = |\mathbb{Z}_m^\times|$

Věta. *Jsou-li $a, b \in \mathbb{N}$ nesoudělná přirozená čísla, pak* $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$.

Důkaz. Protože $(a, b) = 1$, nejmenší společný násobek čísel a, b je $a \cdot b$. Definujme zobrazení $f : \mathbb{Z}_{ab} \to \mathbb{Z}_a \times \mathbb{Z}_b$ předpisem $f([c]_{ab}) = ([c]_a, [c]_b)$ pro libovolné $c \in \mathbb{Z}$.
Je třeba ověřit korektnost této definice: pro libovolné $c, d \in \mathbb{Z}$ platí $[c]_{ab} = [d]_{ab}$, právě když $ab \mid c - d$.
Protože ab je nejmenší společný násobek čísel a, b, platí $ab \mid c - d \;\Leftrightarrow\; a \mid c - d \;\wedge\; b \mid c - d$.
Celkem tedy $[c]_{ab} = [d]_{ab} \;\Leftrightarrow\; ([c]_a, [c]_b) = ([d]_a, [d]_b)$.
Ověřili jsme nejen korektnost definice f, ale i to, že f je injektivní.
A protože množiny $\mathbb{Z}_{ab}$ i $\mathbb{Z}_a \times \mathbb{Z}_b$ mají obě ab prvků, je f bijekce.
Libovolné $c \in \mathbb{Z}$ splňuje $(c, ab) \neq 1$, právě když existuje prvočíslo p tak, že $p \mid c$ a současně $p \mid ab$, tj. že $p \mid c$, $p \mid a$ nebo $p \mid c$, $p \mid b$, tj. právě když $(c, a) \neq 1$ nebo $(c, b) \neq 1$. Celkem tedy $[c]_{ab} \in \mathbb{Z}_{ab}^\times$, právě když $f([c]_{ab}) \in \mathbb{Z}_a^\times \times \mathbb{Z}_b^\times$. Proto $|\mathbb{Z}_{ab}^\times| = |\mathbb{Z}_a^\times| \cdot |\mathbb{Z}_b^\times|$.

Výpočet hodnot Eulerovy funkce $\varphi(m) = |\mathbb{Z}_m^\times|$

Příklad. Předpoklad o nesoudělnosti je v předchozí větě podstatný, platí třeba $\varphi(2 \cdot 2) = 2 \neq 1 = \varphi(2) \cdot \varphi(2)$.

Výpočet hodnot Eulerovy funkce $\varphi(m) = |\mathbb{Z}_m^\times|$

Příklad. Předpoklad o nesoudělnosti je v předchozí větě podstatný, platí třeba $\varphi(2 \cdot 2) = 2 \neq 1 = \varphi(2) \cdot \varphi(2)$.

Důsledek. *Nechť $m \in \mathbb{N}$, $m > 1$. Rozložme m na součin mocnin různých prvočísel, tj.*

$$m = p_1^{e_1} \cdot p_2^{e_2} \cdots p_s^{e_s},$$

kde p_1, p_2, ..., p_s jsou různá prvočísla, $e_1, e_2, \ldots, e_s \in \mathbb{N}$.

Výpočet hodnot Eulerovy funkce $\varphi(m) = |\mathbb{Z}_m^\times|$

Příklad. Předpoklad o nesoudělnosti je v předchozí větě podstatný, platí třeba $\varphi(2 \cdot 2) = 2 \neq 1 = \varphi(2) \cdot \varphi(2)$.

Důsledek. *Nechť $m \in \mathbb{N}$, $m > 1$. Rozložme m na součin mocnin různých prvočísel, tj.*

$$m = p_1^{e_1} \cdot p_2^{e_2} \cdots p_s^{e_s},$$

kde p_1, p_2, ..., p_s jsou různá prvočísla, $e_1, e_2, \ldots, e_s \in \mathbb{N}$. Pak platí

$$\varphi(m) = (p_1 - 1) \cdot p_1^{e_1 - 1} \cdot (p_2 - 1) \cdot p_2^{e_2 - 1} \cdots (p_s - 1) \cdot p_s^{e_s - 1}$$

Výpočet hodnot Eulerovy funkce $\varphi(m) = |\mathbb{Z}_m^\times|$

Příklad. Předpoklad o nesoudělnosti je v předchozí větě podstatný, platí třeba $\varphi(2 \cdot 2) = 2 \neq 1 = \varphi(2) \cdot \varphi(2)$.

Důsledek. *Nechť $m \in \mathbb{N}$, $m > 1$. Rozložme m na součin mocnin různých prvočísel, tj.*

$$m = p_1^{e_1} \cdot p_2^{e_2} \cdots p_s^{e_s},$$

kde p_1, p_2, …, p_s jsou různá prvočísla, $e_1, e_2, \ldots, e_s \in \mathbb{N}$. Pak platí

$$\varphi(m) = (p_1 - 1) \cdot p_1^{e_1 - 1} \cdot (p_2 - 1) \cdot p_2^{e_2 - 1} \cdots (p_s - 1) \cdot p_s^{e_s - 1},$$

což je možné zapsat také takto:

$$\varphi(m) = m \cdot \prod_{\text{prvočíslo } p \mid m} \left(1 - \tfrac{1}{p}\right).$$

Grupa $(\mathbb{S}_n, \circ)$ všech permutací množiny $\{1, 2, \ldots, n\}$

Poznámka. Připomeňme, že $\mathbb{S}(X)$ značí množinu všech permutací na množině X, tj. všech bijekcí $X \to X$, a že spolu s operací skládání zobrazení tato množina tvoří grupu $(\mathbb{S}(X), \circ)$, které říkáme grupa permutací na množině X.

Grupa $(\mathbb{S}_n, \circ)$ všech permutací množiny $\{1, 2, \ldots, n\}$

Poznámka. Připomeňme, že $\mathbb{S}(X)$ značí množinu všech permutací na množině X, tj. všech bijekcí $X \to X$, a že spolu s operací skládání zobrazení tato množina tvoří grupu $(\mathbb{S}(X), \circ)$, které říkáme grupa permutací na množině X. Pokud $X = \{1, 2, \ldots, n\}$, píšeme místo $\mathbb{S}(\{1, 2, \ldots, n\})$ stručně jen $\mathbb{S}_n$.

Grupa $(\mathbb{S}_n, \circ)$ všech permutací množiny $\{1, 2, \ldots, n\}$

Poznámka. Připomeňme, že $\mathbb{S}(X)$ značí množinu všech permutací na množině X, tj. všech bijekcí $X \to X$, a že spolu s operací skládání zobrazení tato množina tvoří grupu $(\mathbb{S}(X), \circ)$, které říkáme grupa permutací na množině X. Pokud $X = \{1, 2, \ldots, n\}$, píšeme místo $\mathbb{S}(\{1, 2, \ldots, n\})$ stručně jen $\mathbb{S}_n$.
Jak označovat prvky grupy $\mathbb{S}_n$?

Grupa $(\mathbb{S}_n, \circ)$ všech permutací množiny $\{1, 2, \ldots, n\}$

Poznámka. Připomeňme, že $\mathbb{S}(X)$ značí množinu všech permutací na množině X, tj. všech bijekcí $X \to X$, a že spolu s operací skládání zobrazení tato množina tvoří grupu $(\mathbb{S}(X), \circ)$, které říkáme grupa permutací na množině X. Pokud $X = \{1, 2, \ldots, n\}$, píšeme místo $\mathbb{S}(\{1, 2, \ldots, n\})$ stručně jen $\mathbb{S}_n$.
Jak označovat prvky grupy $\mathbb{S}_n$? Například pro $n = 6$ můžeme tentýž prvek grupy $\mathbb{S}_6$ zadat

dvouřádkovou maticí $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 1 & 5 & 2 & 6 & 3 \end{pmatrix}$

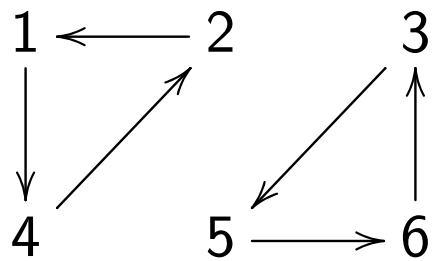
Grupa $(\mathbb{S}_n, \circ)$ všech permutací množiny $\{1, 2, \ldots, n\}$

Poznámka. Připomeňme, že $\mathbb{S}(X)$ značí množinu všech permutací na množině X, tj. všech bijekcí $X \to X$, a že spolu s operací skládání zobrazení tato množina tvoří grupu $(\mathbb{S}(X), \circ)$, které říkáme grupa permutací na množině X. Pokud $X = \{1, 2, \ldots, n\}$, píšeme místo $\mathbb{S}(\{1, 2, \ldots, n\})$ stručně jen $\mathbb{S}_n$.
Jak označovat prvky grupy $\mathbb{S}_n$? Například pro $n = 6$ můžeme tentýž prvek grupy $\mathbb{S}_6$ zadat

dvouřádkovou maticí

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 1 & 5 & 2 & 6 & 3 \end{pmatrix}$$

orientovaným grafem



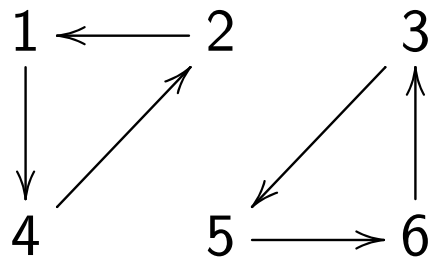
Grupa $(\mathbb{S}_n, \circ)$ všech permutací množiny $\{1, 2, \ldots, n\}$

Poznámka. Připomeňme, že $\mathbb{S}(X)$ značí množinu všech permutací na množině X, tj. všech bijekcí $X \to X$, a že spolu s operací skládání zobrazení tato množina tvoří grupu $(\mathbb{S}(X), \circ)$, které říkáme grupa permutací na množině X. Pokud $X = \{1, 2, \ldots, n\}$, píšeme místo $\mathbb{S}(\{1, 2, \ldots, n\})$ stručně jen $\mathbb{S}_n$.
Jak označovat prvky grupy $\mathbb{S}_n$? Například pro $n = 6$ můžeme tentýž prvek grupy $\mathbb{S}_6$ zadat

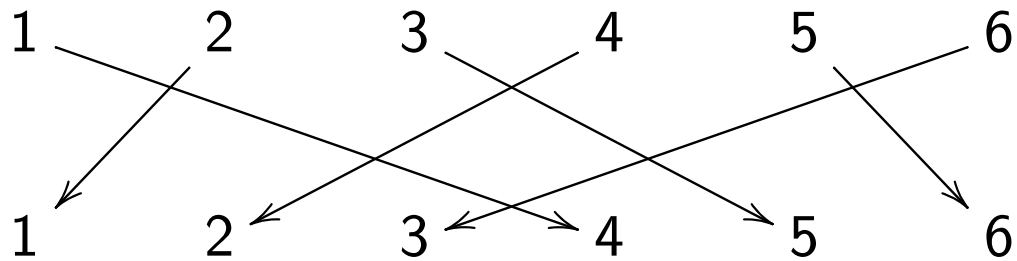
dvouřádkovou maticí

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 1 & 5 & 2 & 6 & 3 \end{pmatrix}$$

orientovaným grafem



anebo schématem



Cykly a transpozice

Definice. Nechť $i_1, \ldots, i_k$ jsou různé prvky množiny $\{1, 2, \ldots, n\}$, přičemž $k \geq 2$. Permutaci z $\mathbb{S}_n$ takovou, že

$$i_1 \mapsto i_2, \quad i_2 \mapsto i_3, \quad i_3 \mapsto i_4, \quad \ldots, \quad i_{k-1} \mapsto i_k, \quad i_k \mapsto i_1,$$

přičemž pro všechny prvky $a \in \{1, 2, \ldots, n\}$, $a \notin \{i_1, \ldots, i_k\}$ platí $a \mapsto a$,

Cykly a transpozice

Definice. Nechť $i_1, \ldots, i_k$ jsou různé prvky množiny $\{1, 2, \ldots, n\}$, přičemž $k \geq 2$. Permutaci z $\mathbb{S}_n$ takovou, že

$$i_1 \mapsto i_2, \quad i_2 \mapsto i_3, \quad i_3 \mapsto i_4, \quad \ldots, \quad i_{k-1} \mapsto i_k, \quad i_k \mapsto i_1,$$

přičemž pro všechny prvky $a \in \{1, 2, \ldots, n\}$, $a \notin \{i_1, \ldots, i_k\}$ platí $a \mapsto a$, nazýváme **cyklem délky** k a značíme $(i_1, \ldots, i_k)$.

Cykly a transpozice

Definice. Nechť $i_1, \ldots, i_k$ jsou různé prvky množiny $\{1, 2, \ldots, n\}$, přičemž $k \geq 2$. Permutaci z $\mathbb{S}_n$ takovou, že

$$i_1 \mapsto i_2, \quad i_2 \mapsto i_3, \quad i_3 \mapsto i_4, \quad \ldots, \quad i_{k-1} \mapsto i_k, \quad i_k \mapsto i_1,$$

přičemž pro všechny prvky $a \in \{1, 2, \ldots, n\}$, $a \notin \{i_1, \ldots, i_k\}$ platí $a \mapsto a$, nazýváme **cyklem délky** k a značíme $(i_1, \ldots, i_k)$. Cykly délky 2 se nazývají **transpozice**.

Cykly a transpozice

Definice. Nechť $i_1, \ldots, i_k$ jsou různé prvky množiny $\{1, 2, \ldots, n\}$, přičemž $k \geq 2$. Permutaci z $\mathbb{S}_n$ takovou, že

$$i_1 \mapsto i_2, \quad i_2 \mapsto i_3, \quad i_3 \mapsto i_4, \quad \ldots, \quad i_{k-1} \mapsto i_k, \quad i_k \mapsto i_1,$$

přičemž pro všechny prvky $a \in \{1, 2, \ldots, n\}$, $a \notin \{i_1, \ldots, i_k\}$ platí $a \mapsto a$, nazýváme **cyklem délky** k a značíme $(i_1, \ldots, i_k)$. Cykly délky 2 se nazývají **transpozice**.

Definice. Cykly $(i_1, \ldots, i_k), (j_1, \ldots, j_r) \in \mathbb{S}_n$ se nazývají **nezávislé**, jsou-li množiny $\{i_1, \ldots, i_k\}$ a $\{j_1, \ldots, j_r\}$ disjunktní (tj. mají-li prázdný průnik).

Cykly a transpozice

Definice. Nechť $i_1, \ldots, i_k$ jsou různé prvky množiny $\{1, 2, \ldots, n\}$, přičemž $k \geq 2$. Permutaci z $\mathbb{S}_n$ takovou, že

$$i_1 \mapsto i_2, \quad i_2 \mapsto i_3, \quad i_3 \mapsto i_4, \quad \ldots, \quad i_{k-1} \mapsto i_k, \quad i_k \mapsto i_1,$$

přičemž pro všechny prvky $a \in \{1, 2, \ldots, n\}$, $a \notin \{i_1, \ldots, i_k\}$ platí $a \mapsto a$, nazýváme **cyklem délky** k a značíme $(i_1, \ldots, i_k)$. Cykly délky 2 se nazývají **transpozice**.

Definice. Cykly $(i_1, \ldots, i_k), (j_1, \ldots, j_r) \in \mathbb{S}_n$ se nazývají **nezávislé**, jsou-li množiny $\{i_1, \ldots, i_k\}$ a $\{j_1, \ldots, j_r\}$ disjunktní (tj. mají-li prázdný průnik).

Věta. Každou neidentickou permutaci $f \in \mathbb{S}_n$ lze napsat jako složení několika nezávislých cyklů, a to jednoznačně až na jejich pořadí. [Věta 2.5, str. 12]

Cykly a transpozice

Definice. Nechť $i_1, \ldots, i_k$ jsou různé prvky množiny $\{1, 2, \ldots, n\}$, přičemž $k \geq 2$. Permutaci z $\mathbb{S}_n$ takovou, že

$$i_1 \mapsto i_2, \quad i_2 \mapsto i_3, \quad i_3 \mapsto i_4, \quad \ldots, \quad i_{k-1} \mapsto i_k, \quad i_k \mapsto i_1,$$

přičemž pro všechny prvky $a \in \{1, 2, \ldots, n\}$, $a \notin \{i_1, \ldots, i_k\}$ platí $a \mapsto a$, nazýváme **cyklem délky** k a značíme $(i_1, \ldots, i_k)$. Cykly délky 2 se nazývají **transpozice**.

Definice. Cykly $(i_1, \ldots, i_k), (j_1, \ldots, j_r) \in \mathbb{S}_n$ se nazývají **nezávislé**, jsou-li množiny $\{i_1, \ldots, i_k\}$ a $\{j_1, \ldots, j_r\}$ disjunktní (tj. mají-li prázdný průnik).

Věta. Každou neidentickou permutaci $f \in \mathbb{S}_n$ lze napsat jako složení několika nezávislých cyklů, a to jednoznačně až na jejich pořadí. [Věta 2.5, str. 12]

Věta. Nechť $n > 1$, pak každou permutaci $f \in \mathbb{S}_n$ lze napsat jako složení několika transpozic. [Věta 2.6, str. 12]

Parita permutace

Definice. Nechť $f \in \mathbb{S}_n$. Řekneme, že uspořádaná dvojice $[i, j]$ je **inverze** permutace f, jestliže $1 \leq i < j \leq n$ a platí $f(i) > f(j)$. Permutace f se nazývá **sudá** nebo **lichá** podle toho, má-li sudý nebo lichý počet inverzí. **Paritu** $p(f)$ permutace f definujeme:

$$p(f) = \begin{cases} 1 & \text{je-li } f \text{ sudá,} \\ -1 & \text{je-li } f \text{ lichá.} \end{cases}$$

Parita permutace

Definice. Nechť $f \in \mathbb{S}_n$. Řekneme, že uspořádaná dvojice $[i, j]$ je **inverze** permutace f, jestliže $1 \leq i < j \leq n$ a platí $f(i) > f(j)$. Permutace f se nazývá **sudá** nebo **lichá** podle toho, má-li sudý nebo lichý počet inverzí. **Paritu** $p(f)$ permutace f definujeme:

$$p(f) = \begin{cases} 1 & \text{je-li } f \text{ sudá,} \\ -1 & \text{je-li } f \text{ lichá.} \end{cases}$$

Poznámka. Paritu permutace f bychom mohli spočítat jako součin

$$p(f) = \prod_{i=1}^{n-1} \prod_{j=i+1}^{n} \frac{f(j) - f(i)}{j - i},$$

ale jistě budou existovat snadnější postupy...

Jak zjistit paritu permutace $f \in \mathbb{S}_n$?

Je-li f dána dvouřádkovou maticí, spočítáme, kolikrát ve spodním řádku „je menší číslo předběhnuto větším“:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 1 & 5 & 2 & 6 & 3 \end{pmatrix}$$

Jak zjistit paritu permutace $f \in \mathbb{S}_n$?

Je-li f dána dvouřádkovou maticí, spočítáme, kolikrát ve spodním řádku „je menší číslo předběhnuto větším“:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 1 & 5 & 2 & 6 & 3 \end{pmatrix}$$

$4 > 1,\ \ 4 > 2,\ \ 4 > 3,\ \ 5 > 2,\ \ 5 > 3,\ \ 6 > 3$

Jak zjistit paritu permutace $f \in \mathbb{S}_n$?

Je-li f dána dvouřádkovou maticí, spočítáme, kolikrát ve spodním řádku „je menší číslo předběhnuto větším“:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 1 & 5 & 2 & 6 & 3 \end{pmatrix}$$

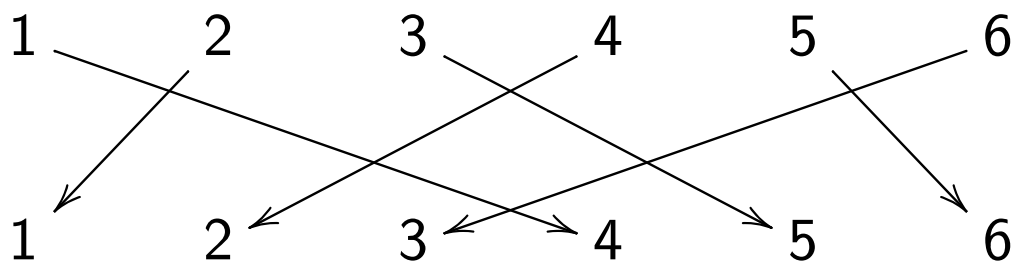
$4 > 1$, $4 > 2$, $4 > 3$, $5 > 2$, $5 > 3$, $6 > 3$:
šest inverzí – sudá permutace.

Jak zjistit paritu permutace $f \in \mathbb{S}_n$?

Je-li f dána dvouřádkovou maticí, spočítáme, kolikrát ve spodním řádku „je menší číslo předběhnuto větším“:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 1 & 5 & 2 & 6 & 3 \end{pmatrix}$$

$4 > 1$, $4 > 2$, $4 > 3$, $5 > 2$, $5 > 3$, $6 > 3$:
šest inverzí – sudá permutace.
Je-li f dána schématem

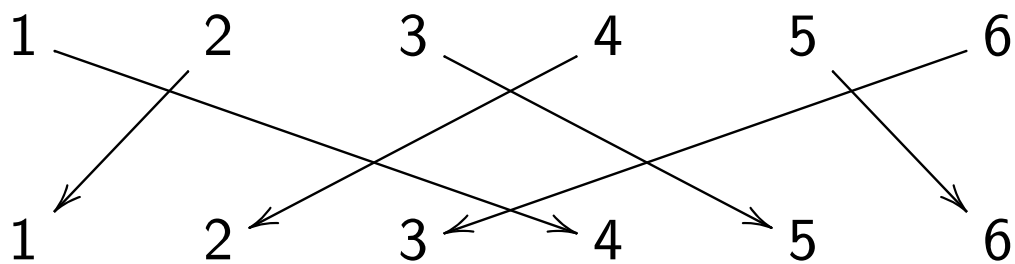


Jak zjistit paritu permutace $f \in \mathbb{S}_n$?

Je-li f dána dvouřádkovou maticí, spočítáme, kolikrát ve spodním řádku „je menší číslo předběhnuto větším“:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 1 & 5 & 2 & 6 & 3 \end{pmatrix}$$

$4 > 1$, $4 > 2$, $4 > 3$, $5 > 2$, $5 > 3$, $6 > 3$:
šest inverzí – sudá permutace.
Je-li f dána schématem



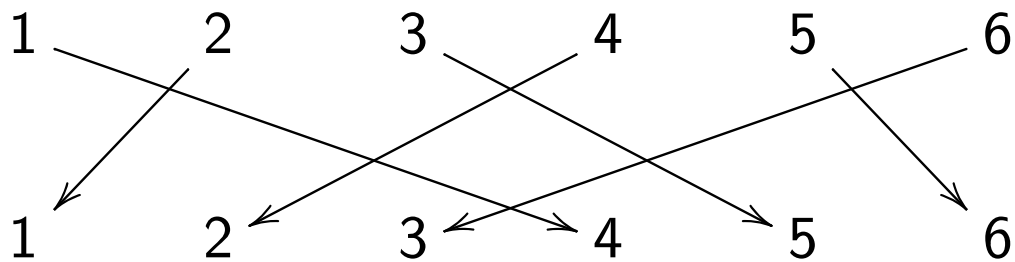
spočítáme, kolikrát se protínají šipky

Jak zjistit paritu permutace $f \in \mathbb{S}_n$?

Je-li f dána dvouřádkovou maticí, spočítáme, kolikrát ve spodním řádku „je menší číslo předběhnuto větším“:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 1 & 5 & 2 & 6 & 3 \end{pmatrix}$$

$4 > 1,\ \ 4 > 2,\ \ 4 > 3,\ \ 5 > 2,\ \ 5 > 3,\ \ 6 > 3$:
šest inverzí – sudá permutace.
Je-li f dána schématem



spočítáme, kolikrát se protínají šipky:
šest průsečíků - šest inverzí - sudá permutace.

A co parita permutace $f \in \mathbb{S}_n$ zapsané jako složení cyklů?

Věta. *Pro libovolné* $f, g \in \mathbb{S}_n$ *platí*

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

A co parita permutace $f \in \mathbb{S}_n$ zapsané jako složení cyklů?

Věta. *Pro libovolné* $f, g \in \mathbb{S}_n$ *platí*

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

Jinými slovy: složením libovolných dvou permutací stejné parity dostaneme sudou permutaci, kdežto složením libovolných dvou permutací různé parity dostaneme lichou permutaci. [Věta 2.9, str. 13]

A co parita permutace $f \in \mathbb{S}_n$ zapsané jako složení cyklů?

Věta. *Pro libovolné $f, g \in \mathbb{S}_n$ platí*

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

Jinými slovy: složením libovolných dvou permutací stejné parity dostaneme sudou permutaci, kdežto složením libovolných dvou permutací různé parity dostaneme lichou permutaci. [Věta 2.9, str. 13]

Důsledek. *Složení sudého počtu transpozic je sudá permutace, složení lichého počtu transpozic je lichá permutace.* [Každá transpozice je lichá permutace.]

A co parita permutace $f \in \mathbb{S}_n$ zapsané jako složení cyklů?

Věta. *Pro libovolné $f, g \in \mathbb{S}_n$ platí*

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

Jinými slovy: složením libovolných dvou permutací stejné parity dostaneme sudou permutaci, kdežto složením libovolných dvou permutací různé parity dostaneme lichou permutaci. [Věta 2.9, str. 13]

Důsledek. *Složení sudého počtu transpozic je sudá permutace, složení lichého počtu transpozic je lichá permutace.* [Každá transpozice je lichá permutace.]

Důsledek. *Cyklus liché délky je sudá permutace a cyklus sudé délky je lichá permutace.* [Cyklus délky k lze psát jako složení $k - 1$ transpozic.]

A co parita permutace $f \in \mathbb{S}_n$ zapsané jako složení cyklů?

Věta. *Pro libovolné $f, g \in \mathbb{S}_n$ platí*

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

Jinými slovy: složením libovolných dvou permutací stejné parity dostaneme sudou permutaci, kdežto složením libovolných dvou permutací různé parity dostaneme lichou permutaci. [Věta 2.9, str. 13]

Důsledek. *Složení sudého počtu transpozic je sudá permutace, složení lichého počtu transpozic je lichá permutace.* [Každá transpozice je lichá permutace.]

Důsledek. *Cyklus liché délky je sudá permutace a cyklus sudé délky je lichá permutace.* [Cyklus délky k lze psát jako složení $k - 1$ transpozic.]

Důsledek. *Neidentická permutace je sudá, právě když ve svém rozkladu na složení cyklů (ať už závislých či nezávislých) má sudý počet cyklů sudé délky.*

A co parita permutace $f \in \mathbb{S}_n$ zapsané jako složení cyklů?

Věta. *Pro libovolné $f, g \in \mathbb{S}_n$ platí*

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

Jinými slovy: složením libovolných dvou permutací stejné parity dostaneme sudou permutaci, kdežto složením libovolných dvou permutací různé parity dostaneme lichou permutaci. [Věta 2.9, str. 13]

Důsledek. *Složení sudého počtu transpozic je sudá permutace, složení lichého počtu transpozic je lichá permutace.* [Každá transpozice je lichá permutace.]

Důsledek. *Cyklus liché délky je sudá permutace a cyklus sudé délky je lichá permutace.* [Cyklus délky k lze psát jako složení $k - 1$ transpozic.]

Důsledek. *Neidentická permutace je sudá, právě když ve svém rozkladu na složení cyklů (ať už závislých či nezávislých) má sudý počet cyklů sudé délky. Je tedy lichá, právě když v tomto rozkladu má lichý počet cyklů sudé délky.*

A co parita permutace $f \in \mathbb{S}_n$ zapsané jako složení cyklů?

Věta. *Pro libovolné $f, g \in \mathbb{S}_n$ platí*

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

Jinými slovy: složením libovolných dvou permutací stejné parity dostaneme sudou permutaci, kdežto složením libovolných dvou permutací různé parity dostaneme lichou permutaci. [Věta 2.9, str. 13]

Důsledek. *Složení sudého počtu transpozic je sudá permutace, složení lichého počtu transpozic je lichá permutace.* [Každá transpozice je lichá permutace.]

Důsledek. *Cyklus liché délky je sudá permutace a cyklus sudé délky je lichá permutace.* [Cyklus délky k lze psát jako složení $k - 1$ transpozic.]

Důsledek. *Neidentická permutace je sudá, právě když ve svém rozkladu na složení cyklů (ať už závislých či nezávislých) má sudý počet cyklů sudé délky. Je tedy lichá, právě když v tomto rozkladu má lichý počet cyklů sudé délky. Na počtu cyklů liché délky tedy vůbec nezáleží.*

Aditivní a multiplikativní grupy matic

Příklad. Nechť R značí kteroukoli z číselných množin $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, pak pro libovolné $m, n \in \mathbb{N}$ definujeme $M_{n,m}(R)$ jako množinu všech matic typu $n \times m$ s prvky z R.

Aditivní a multiplikativní grupy matic

Příklad. Nechť R značí kteroukoli z číselných množin $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, pak pro libovolné $m, n \in \mathbb{N}$ definujeme $M_{n,m}(R)$ jako množinu všech matic typu $n \times m$ s prvky z R. Pak $(M_{n,m}(R), +)$ je komutativní grupa (zde $+$ značí sčítání matic).

Aditivní a multiplikativní grupy matic

Příklad. Nechť R značí kteroukoli z číselných množin $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, pak pro libovolné $m, n \in \mathbb{N}$ definujeme $M_{n,m}(R)$ jako množinu všech matic typu $n \times m$ s prvky z R. Pak $(M_{n,m}(R), +)$ je komutativní grupa (zde $+$ značí sčítání matic).

Abychom pro nějakou matici A spočítat součin $A \cdot A$, potřebujeme, aby byla čtvercová.

Aditivní a multiplikativní grupy matic

Příklad. Nechť R značí kteroukoli z číselných množin $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, pak pro libovolné $m, n \in \mathbb{N}$ definujeme $M_{n,m}(R)$ jako množinu všech matic typu $n \times m$ s prvky z R. Pak $(M_{n,m}(R), +)$ je komutativní grupa (zde $+$ značí sčítání matic).

Abychom pro nějakou matici A spočítat součin $A \cdot A$, potřebujeme, aby byla čtvercová. Proto se musíme omezit na čtvercové matice, chceme-li hovořit o operaci násobení na nějaké množině matic.

Aditivní a multiplikativní grupy matic

Příklad. Nechť R značí kteroukoli z číselných množin $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, pak pro libovolné $m, n \in \mathbb{N}$ definujeme $M_{n,m}(R)$ jako množinu všech matic typu $n \times m$ s prvky z R. Pak $(M_{n,m}(R), +)$ je komutativní grupa (zde $+$ značí sčítání matic).

Abychom pro nějakou matici A spočítat součin $A \cdot A$, potřebujeme, aby byla čtvercová. Proto se musíme omezit na čtvercové matice, chceme-li hovořit o operaci násobení na nějaké množině matic.

Ať už je R kterákoli z číselných množin $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, tak vždy $(M_{n,n}(R), \cdot)$, kde $\cdot$ značí násobení matic, je pologrupa s neutrálním prvkem.

Aditivní a multiplikativní grupy matic

Příklad. Nechť R značí kteroukoli z číselných množin $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, pak pro libovolné $m, n \in \mathbb{N}$ definujeme $M_{n,m}(R)$ jako množinu všech matic typu $n \times m$ s prvky z R. Pak $(M_{n,m}(R), +)$ je komutativní grupa (zde $+$ značí sčítání matic).

Abychom pro nějakou matici A spočítat součin $A \cdot A$, potřebujeme, aby byla čtvercová. Proto se musíme omezit na čtvercové matice, chceme-li hovořit o operaci násobení na nějaké množině matic.

Ať už je R kterákoli z číselných množin $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, tak vždy $(M_{n,n}(R), \cdot)$, kde $\cdot$ značí násobení matic, je pologrupa s neutrálním prvkem. Víme, že pak množina invertibilních prvků této pologrupy tvoří grupu.

Aditivní a multiplikativní grupy matic

Příklad. Nechť R značí kteroukoli z číselných množin $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, pak pro libovolné $m, n \in \mathbb{N}$ definujeme $M_{n,m}(R)$ jako množinu všech matic typu $n \times m$ s prvky z R. Pak $(M_{n,m}(R), +)$ je komutativní grupa (zde $+$ značí sčítání matic).

Abychom pro nějakou matici A spočítat součin $A \cdot A$, potřebujeme, aby byla čtvercová. Proto se musíme omezit na čtvercové matice, chceme-li hovořit o operaci násobení na nějaké množině matic.

Ať už je R kterákoli z číselných množin $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, tak vždy $(M_{n,n}(R), \cdot)$, kde $\cdot$ značí násobení matic, je pologrupa s neutrálním prvkem. Víme, že pak množina invertibilních prvků této pologrupy tvoří grupu.

Je-li R kterákoli z číselných množin $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ (tedy nyní $R \neq \mathbb{Z}$), tak invertibilní prvky jsou právě regulární matice (tj. matice s nenulovým determinantem).

Aditivní a multiplikativní grupy matic

Příklad. Nechť R značí kteroukoli z číselných množin $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, pak pro libovolné $m, n \in \mathbb{N}$ definujeme $M_{n,m}(R)$ jako množinu všech matic typu $n \times m$ s prvky z R. Pak $(M_{n,m}(R), +)$ je komutativní grupa (zde $+$ značí sčítání matic).

Abychom pro nějakou matici A spočítat součin $A \cdot A$, potřebujeme, aby byla čtvercová. Proto se musíme omezit na čtvercové matice, chceme-li hovořit o operaci násobení na nějaké množině matic.

Ať už je R kterákoli z číselných množin $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, tak vždy $(M_{n,n}(R), \cdot)$, kde $\cdot$ značí násobení matic, je pologrupa s neutrálním prvkem. Víme, že pak množina invertibilních prvků této pologrupy tvoří grupu.

Je-li R kterákoli z číselných množin $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ (tedy nyní $R \neq \mathbb{Z}$), tak invertibilní prvky jsou právě regulární matice (tj. matice s nenulovým determinantem). Označme $\mathbb{GL}_n(R)$ množinu všech regulárních matic typu $n \times n$ s prvky z R.

Aditivní a multiplikativní grupy matic

Příklad. Nechť R značí kteroukoli z číselných množin $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, pak pro libovolné $m, n \in \mathbb{N}$ definujeme $M_{n,m}(R)$ jako množinu všech matic typu $n \times m$ s prvky z R. Pak $(M_{n,m}(R), +)$ je komutativní grupa (zde $+$ značí sčítání matic).

Abychom pro nějakou matici A spočítat součin $A \cdot A$, potřebujeme, aby byla čtvercová. Proto se musíme omezit na čtvercové matice, chceme-li hovořit o operaci násobení na nějaké množině matic.

Ať už je R kterákoli z číselných množin $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, tak vždy $(M_{n,n}(R), \cdot)$, kde $\cdot$ značí násobení matic, je pologrupa s neutrálním prvkem. Víme, že pak množina invertibilních prvků této pologrupy tvoří grupu.

Je-li R kterákoli z číselných množin $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ (tedy nyní $R \neq \mathbb{Z}$), tak invertibilní prvky jsou právě regulární matice (tj. matice s nenulovým determinantem). Označme $\mathbb{GL}_n(R)$ množinu všech regulárních matic typu $n \times n$ s prvky z R. Pak $(\mathbb{GL}_n(R), \cdot)$ je grupa, která není komutativní, je-li $n \geq 2$.