Algebra - pátý díl

Lenka Zalabová

Ústav matematiky a biomatematiky, Přírodovědecká fakulta, Jihočeská univerzita v Českých Budějovicích

zima 2012

Obsah

Běžné počítání

Theorem

- *Buď $(G, *)$ pologrupa, $n > 1$ přirozené číslo, $a_1, a_2, \ldots, a_n \in G$. Pak výsledek součinu prvků $a_1 * a_2 * \cdots * a_n$ nezáleží na jejich uzávorkování.*
- *Buď $(G, *)$ komutativní pologrupa, $n > 1$ přirozené číslo, $a_1, a_2, \ldots, a_n \in G$. Pak výsledek součinu prvků $a_1 * a_2 * \cdots * a_n$ nezáleží na jejich pořadí.*

Proof: ... matematická indukce

Mocniny v pologrupě

Buď $(G, *)$ pologrupa, n přirozené číslo, $a \in G$. *Mocninu* a^n definujeme jako součin

$$\underbrace{a * a * \cdots * a}_{n}.$$

Tedy mocnina je součin n exemplářů prvku a. Z předchozího je jasné, že mocnina je určena jednoznačně.

Mocniny v pologrupě

Buď $(G, *)$ pologrupa, n přirozené číslo, $a \in G$. *Mocninu* a^n definujeme jako součin

$$\underbrace{a * a * \cdots * a}_{n}.$$

Tedy mocnina je součin n exemplářů prvku a. Z předchozího je jasné, že mocnina je určena jednoznačně.

Theorem

Buď $(G, *)$ pologrupa, m, n přirozená čísla, $a \in G$. Pak platí:

1. $a^m * a^n = a^{m+n}$,
2. $(a^m)^n = a^{m \cdot n}$.

Proof: ...

Mocniny v pologrupě s jednotkovým prvkem

Buď $(G, *)$ pologrupa s jednotkovým prvkem. Pokud existuje inverzní prvek k prvku $a \in G$, označme ho a^{-1}. Prvek, ke kterému existuje inverze, se nazývá *invertibilní*.

Mocniny v pologrupě s jednotkovým prvkem

Buď $(G, *)$ pologrupa s jednotkovým prvkem. Pokud existuje inverzní prvek k prvku $a \in G$, označme ho a^{-1}. Prvek, ke kterému existuje inverze, se nazývá *invertibilní*.

Theorem

Buď $(G, *)$ pologrupa s jednotkovým prvkem e. Pak platí:

1. $e^{-1} = e$,
2. $(a^{-1})^{-1} = a$, *kde* $a \in G$ *invertibilní,*
3. $(a_1 * a_2 * \cdots * a_n)^{-1} = a_n^{-1} * \cdots * a_2^{-1} * a_1^{-1}$, *kde* $a_1, a_2, \ldots, a_n$ *jsou libovolné invertibilní prvky* G.

Proof: ...

Mocniny v grupě

Buď $(G, *)$ grupa, n přirozené číslo, $a \in G$. Klademe

- $a^{-n} = (a^n)^{-1}$,
- $a^0 = e$.

Mocniny v grupě

Buď $(G, *)$ grupa, n přirozené číslo, $a \in G$. Klademe

- $a^{-n} = (a^n)^{-1}$,
- $a^0 = e$.

Theorem

Buď $(G, *)$ grupa, m, n celá čísla, $a \in G$. Pak platí:

1. $a^m * a^n = a^{m+n}$,
2. $(a^m)^n = a^{m \cdot n}$.

Proof: ...

Co to je podgrupa?

Definition

Buď $(G, *)$ grupa a H podmnožina množiny G. Řekneme, že H je *podgrupa* grupy G, jestliže jsou splněny následující tři podmínky:

1. Pokud $a, b \in H$, pak taky $a * b \in H$. Neboli množina H je *uzavřená* vzhledem k operaci $*$.
2. Platí $e \in H$, kde e je jednotkový prvek grupy G.
3. Pokud $a \in H$, pak taky $a^{-1} \in H$, kde a^{-1} je inverze k prvku a v $(G, *)$.

Nějaké příklady

1. Množina $\mathbb{Z}$ tvoří podgrupu v $(\mathbb{Q}, +)$ a $(\mathbb{R}, +)$. Podobně $\mathbb{Q}$ tvoří podgrupu $(\mathbb{R}, +)$. Množina $\mathbb{N}$ netvoří podgrupu v $(\mathbb{Z}, +)$, protože nesplňuje (2) a (3).

Nějaké příklady

1. Množina $\mathbb{Z}$ tvoří podgrupu v $(\mathbb{Q}, +)$ a $(\mathbb{R}, +)$. Podobně $\mathbb{Q}$ tvoří podgrupu $(\mathbb{R}, +)$. Množina $\mathbb{N}$ netvoří podgrupu v $(\mathbb{Z}, +)$, protože nesplňuje (2) a (3).
2. Buď $n \in \mathbb{Z}$. Pak množina $n\mathbb{Z} = \{n \cdot a : a \in \mathbb{Z}\}$ je podgrupa v $(\mathbb{Z}, +)$.

Nějaké příklady

1. Množina $\mathbb{Z}$ tvoří podgrupu v $(\mathbb{Q}, +)$ a $(\mathbb{R}, +)$. Podobně $\mathbb{Q}$ tvoří podgrupu $(\mathbb{R}, +)$. Množina $\mathbb{N}$ netvoří podgrupu v $(\mathbb{Z}, +)$, protože nesplňuje (2) a (3).
2. Buď $n \in \mathbb{Z}$. Pak množina $n\mathbb{Z} = \{n \cdot a : a \in \mathbb{Z}\}$ je podgrupa v $(\mathbb{Z}, +)$.
3. Množina $\mathbb{R}^+$ kladných reálných čísel je podgrupa v $(\mathbb{R}^*, \cdot)$, kde $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$.

Nějaké příklady

1. Množina $\mathbb{Z}$ tvoří podgrupu v $(\mathbb{Q}, +)$ a $(\mathbb{R}, +)$. Podobně $\mathbb{Q}$ tvoří podgrupu $(\mathbb{R}, +)$. Množina $\mathbb{N}$ netvoří podgrupu v $(\mathbb{Z}, +)$, protože nesplňuje (2) a (3).
2. Buď $n \in \mathbb{Z}$. Pak množina $n\mathbb{Z} = \{n \cdot a : a \in \mathbb{Z}\}$ je podgrupa v $(\mathbb{Z}, +)$.
3. Množina $\mathbb{R}^+$ kladných reálných čísel je podgrupa v $(\mathbb{R}^*, \cdot)$, kde $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$.
4. Množina $\mathcal{A}_n$ všech sudých permutací n-prvkové množiny tvoří podgrupu v $(S_n, \circ)$.

Nějaké příklady

1. Množina $\mathbb{Z}$ tvoří podgrupu v $(\mathbb{Q}, +)$ a $(\mathbb{R}, +)$. Podobně $\mathbb{Q}$ tvoří podgrupu $(\mathbb{R}, +)$. Množina $\mathbb{N}$ netvoří podgrupu v $(\mathbb{Z}, +)$, protože nesplňuje (2) a (3).
2. Buď $n \in \mathbb{Z}$. Pak množina $n\mathbb{Z} = \{n \cdot a : a \in \mathbb{Z}\}$ je podgrupa v $(\mathbb{Z}, +)$.
3. Množina $\mathbb{R}^+$ kladných reálných čísel je podgrupa v $(\mathbb{R}^*, \cdot)$, kde $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$.
4. Množina $\mathcal{A}_n$ všech sudých permutací n-prvkové množiny tvoří podgrupu v $(S_n, \circ)$.
5. Libovolná grupa $(G, *)$ má podgrupy $\{e\}$ a G. Zřejmě $\{e\}$ je nejmenší a G je největší. Tyto podgrupy se nazývají *nevlastní*. Ostatní podgrupy se nazývají *vlastní*.

Důležitá pozorování

Theorem

- *Buď H podgrupa grupy $(G, *)$. Pak $*$ určuje operaci na množině H a $(H, *)$ je sama o sobě grupa.*
- *Je-li $(G, *)$ komutativní, pak je i $(H, *)$ komutativní.*

Proof: ...

Důležitá pozorování

Theorem

- *Buď H podgrupa grupy $(G, *)$. Pak $*$ určuje operaci na množině H a $(H, *)$ je sama o sobě grupa.*
- *Je-li $(G, *)$ komutativní, pak je i $(H, *)$ komutativní.*

Proof: ...

Theorem

Buď H podgrupa grupy $(G, *)$ a K podgrupa grupy $(H, *)$. Pak K je podgrupa grupy $(G, *)$.

Proof: ... zřejmé

Průniky podgrup

Theorem

Buďte H_i podgrupy grupy $(G, *)$, kde i probíhá nějakou neprázdnou množinu indexů I. Pak $\cap_{i \in I} H_i$ je podgrupa v G.

Neboli: Průnik libovolného počtu podgrup grupy G je zase podgrupa grupy G.

Průniky podgrup

Theorem

Buďte H_i podgrupy grupy $(G, *)$, kde i probíhá nějakou neprázdnou množinu indexů I. Pak $\cap_{i \in I} H_i$ je podgrupa v G.

Neboli: Průnik libovolného počtu podgrup grupy G je zase podgrupa grupy G.

Example

V grupě $(\mathbb{Z}, +)$ uvažme podgrupy
$2\mathbb{Z} = \{2a : a \in \mathbb{Z}\} = \{\ldots, -6, -4, -2, 0, 2, 4, 6, \ldots\}$ a
$3\mathbb{Z} = \{3a : a \in \mathbb{Z}\} = \{\ldots, -9, -6, -3, 0, 3, 6, 9, \ldots\}$.

Průniky podgrup

Theorem

Buďte H_i podgrupy grupy $(G, *)$, kde i probíhá nějakou neprázdnou množinu indexů I. Pak $\cap_{i \in I} H_i$ je podgrupa v G.

Neboli: Průnik libovolného počtu podgrup grupy G je zase podgrupa grupy G.

Example

V grupě $(\mathbb{Z}, +)$ uvažme podgrupy
$2\mathbb{Z} = \{2a : a \in \mathbb{Z}\} = \{\ldots, -6, -4, -2, 0, 2, 4, 6, \ldots\}$ a
$3\mathbb{Z} = \{3a : a \in \mathbb{Z}\} = \{\ldots, -9, -6, -3, 0, 3, 6, 9, \ldots\}$.
Pak $2\mathbb{Z} \cap 3\mathbb{Z} =$

Průniky podgrup

Theorem

Buďte H_i podgrupy grupy $(G, *)$, kde i probíhá nějakou neprázdnou množinu indexů I. Pak $\cap_{i \in I} H_i$ je podgrupa v G.

Neboli: Průnik libovolného počtu podgrup grupy G je zase podgrupa grupy G.

Example

V grupě $(\mathbb{Z}, +)$ uvažme podgrupy
$2\mathbb{Z} = \{2a : a \in \mathbb{Z}\} = \{\ldots, -6, -4, -2, 0, 2, 4, 6, \ldots\}$ a
$3\mathbb{Z} = \{3a : a \in \mathbb{Z}\} = \{\ldots, -9, -6, -3, 0, 3, 6, 9, \ldots\}$.
Pak $2\mathbb{Z} \cap 3\mathbb{Z} = 6\mathbb{Z}$, což je podgrupa $(\mathbb{Z}, +)$.

Generování

- Buď $(G, *)$ grupa a buď M podmnožina G. Symbolem $\langle M \rangle$ označme průnik všech podgrup $(G, *)$, které obsahují množinu M.

Generování

- Buď $(G, *)$ grupa a buď M podmnožina G. Symbolem $\langle M \rangle$ označme průnik všech podgrup $(G, *)$, které obsahují množinu M.
- Z předchozího víme, že $\langle M \rangle$ je podgrupa. Je to nejmenší podgrupa grupy $(G, *)$ obsahující množinu M.

Generování

- Buď $(G, *)$ grupa a buď M podmnožina G. Symbolem $\langle M \rangle$ označme průnik všech podgrup $(G, *)$, které obsahují množinu M.
- Z předchozího víme, že $\langle M \rangle$ je podgrupa. Je to nejmenší podgrupa grupy $(G, *)$ obsahující množinu M.
- Podgrupa $\langle M \rangle$ se nazývá podgrupa *generovaná* množinou M. Množinu M nazýváme *množinou generátorů* grupy $\langle M \rangle$.

Generování

- Buď $(G, *)$ grupa a buď M podmnožina G. Symbolem $\langle M \rangle$ označme průnik všech podgrup $(G, *)$, které obsahují množinu M.
- Z předchozího víme, že $\langle M \rangle$ je podgrupa. Je to nejmenší podgrupa grupy $(G, *)$ obsahující množinu M.
- Podgrupa $\langle M \rangle$ se nazývá podgrupa *generovaná* množinou M. Množinu M nazýváme *množinou generátorů* grupy $\langle M \rangle$.
- Pokud $M = \{a_1, a_2, \ldots, a_n\}$, pak hovoříme o grupě generované prvky $a_1, a_2, \ldots, a_n$ a označujeme stručně $\langle a_1, a_2, \ldots, a_n \rangle$.

Jak popsat podgrupu generovanou množinou?

Theorem

Buď $M \neq \emptyset$ podmnožina grupy $(G, *)$. Pak platí:

$$\langle M \rangle = \{a_1 * a_2 * \cdots * a_n : \ n \ \textit{je přirozené číslo},$$
$$a_i \ \textit{nebo} \ a_i^{-1} \ \textit{patří do} \ M \ \textit{pro libovolné} \ i = 1, \ldots, n\}.$$

Proof: ...

Důležitý důsledek

Theorem

Buď $(G, *)$ grupa, $a \in G$. Pak platí

$$\langle a \rangle = \{a^n : n \in \mathbb{Z}\}.$$

Proof: ...

Důležitý důsledek

Theorem

Buď $(G, *)$ *grupa,* $a \in G$*. Pak platí*

$$\langle a \rangle = \{a^n : n \in \mathbb{Z}\}.$$

Proof: ...

Definition

Grupa $(G, *)$ se nazývá *cyklická*, jestliže je generovaná nějakým svým prvkem.

Nějaké příklady

- Grupa $(\mathbb{Z}_6, +)$ je generovaná prvky $[2]_6$ a $[3]_6$, neboli $\mathbb{Z}_6 = \langle [2]_6, [3]_6 \rangle$. Platí:
  $[0]_6 = [3]_6 + [3]_6$,
  $[1]_6 = [2]_6 + [2]_6 + [3]_6$,
  $[4]_6 = [2]_6 + [2]_6$,
  $[5]_6 = [2]_6 + [3]_6$.

Nějaké příklady

- Grupa $(\mathbb{Z}_6, +)$ je generovaná prvky $[2]_6$ a $[3]_6$, neboli $\mathbb{Z}_6 = \langle [2]_6, [3]_6 \rangle$. Platí:
  $[0]_6 = [3]_6 + [3]_6$,
  $[1]_6 = [2]_6 + [2]_6 + [3]_6$,
  $[4]_6 = [2]_6 + [2]_6$,
  $[5]_6 = [2]_6 + [3]_6$.
- Grupa $(\mathbb{Z}_6, +)$ je generovaná prvkem $[1]_6$, neboli $\mathbb{Z}_6 = \langle [1]_6 \rangle$. Platí:
  $[0]_6 = [1]_6 + [1]_6 + [1]_6 + [1]_6 + [1]_6 + [1]_6$,
  $[2]_6 = [1]_6 + [1]_6$,
  $[3]_6 = [1]_6 + [1]_6 + [1]_6$,
  $[4]_6 = [1]_6 + [1]_6 + [1]_6 + [1]_6$,
  $[5]_6 = [1]_6 + [1]_6 + [1]_6 + [1]_6 + [1]_6$.

Nějaké příklady

- Grupa $(\mathbb{Z}_6, +)$ je generovaná prvky $[2]_6$ a $[3]_6$, neboli $\mathbb{Z}_6 = \langle [2]_6, [3]_6 \rangle$. Platí:
  $[0]_6 = [3]_6 + [3]_6$,
  $[1]_6 = [2]_6 + [2]_6 + [3]_6$,
  $[4]_6 = [2]_6 + [2]_6$,
  $[5]_6 = [2]_6 + [3]_6$.
- Grupa $(\mathbb{Z}_6, +)$ je generovaná prvkem $[1]_6$, neboli $\mathbb{Z}_6 = \langle [1]_6 \rangle$. Platí:
  $[0]_6 = [1]_6 + [1]_6 + [1]_6 + [1]_6 + [1]_6 + [1]_6$,
  $[2]_6 = [1]_6 + [1]_6$,
  $[3]_6 = [1]_6 + [1]_6 + [1]_6$,
  $[4]_6 = [1]_6 + [1]_6 + [1]_6 + [1]_6$,
  $[5]_6 = [1]_6 + [1]_6 + [1]_6 + [1]_6 + [1]_6$.
  Tato grupa je tedy cyklická.

Nějaké příklady

- Grupa $(\mathbb{Z}, +)$ je cyklická, je generovaná prvkem 1.

Nějaké příklady

- Grupa $(\mathbb{Z}, +)$ je cyklická, je generovaná prvkem 1.
- Grupa $(\mathbb{Z}_n, +)$ je cyklická, je generovaná prvkem $[1]_n$. Navíc multiplikativní tabulka této grupy je plně popsána vztahem $\underbrace{[1]_n + \cdots + [1]_n}_{n} = [0]_n$.

Nějaké příklady

- Grupa $(\mathbb{Z}, +)$ je cyklická, je generovaná prvkem 1.
- Grupa $(\mathbb{Z}_n, +)$ je cyklická, je generovaná prvkem $[1]_n$. Navíc multiplikativní tabulka této grupy je plně popsána vztahem $\underbrace{[1]_n + \cdots + [1]_n}_{n} = [0]_n$.
- Grupa $(\mathbb{Z}_7^*, \cdot)$, kde $\mathbb{Z}_7^* = \mathbb{Z}_7 \setminus \{[0]_7\}$, je cyklická, je generovaná prvkem $[3]_7$. Platí:
  $[3]_7 \cdot [3]_7 = [2]_7$,
  $[3]_7 \cdot [3]_7 \cdot [3]_7 = [6]_7$,
  $[3]_7 \cdot [3]_7 \cdot [3]_7 \cdot [3]_7 = [4]_7$,
  $[2]_7 \cdot [6]_7 = [5]_7$,
  $[6]_7 \cdot [6]_7 = [1]_7$.

Nějaké příklady

- Grupa D_n všech symetrií pravidelného n-úhelníka je generovaná otočením r o úhel $\frac{2\pi}{n}$ a libovolnou reflexí d, jejíž osa prochází jedním z vrcholů. Platí:

  $$D_n = \langle r, d \rangle = \{r, r^2, \ldots, r^{n-1}, id = r^n, d, r \circ d, \ldots, r^{n-1} \circ d\}.$$

  Navíc multiplikativní tabulka této grupy je plně popsána vztahy $r^n = id, d^2 = id, d \circ r = r^{n-1} \circ d$.

Nějaké příklady

- Grupa D_n všech symetrií pravidelného n-úhelníka je generovaná otočením r o úhel $\frac{2\pi}{n}$ a libovolnou reflexí d, jejíž osa prochází jedním z vrcholů. Platí:

  $$D_n = \langle r, d \rangle = \{r, r^2, \ldots, r^{n-1}, id = r^n, d, r \circ d, \ldots, r^{n-1} \circ d\}.$$

  Navíc multiplikativní tabulka této grupy je plně popsána vztahy $r^n = id, d^2 = id, d \circ r = r^{n-1} \circ d$.
- Grupa C_n všech jeho rotací je podgrupa D_n, která je generovaná prvkem r. Tedy $C_n = \langle r \rangle = \{id, r, r^2, \ldots, r^{n-1}\}$.

Nějaké příklady

- Grupa D_n všech symetrií pravidelného n-úhelníka je generovaná otočením r o úhel $\frac{2\pi}{n}$ a libovolnou reflexí d, jejíž osa prochází jedním z vrcholů. Platí:

  $$D_n = \langle r, d \rangle = \{r, r^2, \ldots, r^{n-1}, id = r^n, d, r \circ d, \ldots, r^{n-1} \circ d\}.$$

  Navíc multiplikativní tabulka této grupy je plně popsána vztahy $r^n = id, d^2 = id, d \circ r = r^{n-1} \circ d$.
- Grupa C_n všech jeho rotací je podgrupa D_n, která je generovaná prvkem r. Tedy $C_n = \langle r \rangle = \{id, r, r^2, \ldots, r^{n-1}\}$.
- Grupa S_n všech permutací n–prvkové množiny je generována množinou všech transpozic. Dokonce stačí vzít pouze transpozice tvaru $(1, i)$ pro $i = 2, \ldots, n$, protože platí $(i, j) = (1, i) \circ (1, j) \circ (1, i)$.

Co to je izomorfismus grup?

Definition

- Buďte $(G, *)$ a $(H, \bullet)$ grupy a $f : G \to H$ bijektivní (vzájemně jednoznačné) zobrazení. Řekneme, že f je izomorfismus grupy G na grupu H, jestliže pro libovolné prvky $a, b \in G$ platí:

$$f(a * b) = f(a) \bullet f(b).$$

- Grupy G, H se nazývají izomorfní, jestliže existuje izomorfismus $G \to H$.
- Toto se obvykle zapisuje jako $G \cong H$.

První příklad

Grupa $(\mathbb{Z}_2, +)$ je izomorfní s grupou $(\{1, -1\}, \cdot)$, což je podgrupa $(\mathbb{R}^*, \cdot)$. Izomorfismus $f : \mathbb{Z}_2 \to \{-1, 1\}$ je dán předpisem:

$$f([0]_2) = 1, \quad f([1]_2) = -1.$$

Proč je zobrazení f izomorfismus?

První příklad

Grupa $(\mathbb{Z}_2, +)$ je izomorfní s grupou $(\{1, -1\}, \cdot)$, což je podgrupa $(\mathbb{R}^*, \cdot)$. Izomorfismus $f : \mathbb{Z}_2 \to \{-1, 1\}$ je dán předpisem:

$$f([0]_2) = 1, \quad f([1]_2) = -1.$$

Proč je zobrazení f izomorfismus?
Zobrazení je zřejmě bijektivní. Zobrazení splňuje:

- $f([0]_2 + [0]_2) = f([0]_2) = 1$, $f([0]_2) \cdot f([0]_2) = 1 \cdot 1 = 1$,

První příklad

Grupa $(\mathbb{Z}_2, +)$ je izomorfní s grupou $(\{1, -1\}, \cdot)$, což je podgrupa $(\mathbb{R}^*, \cdot)$. Izomorfismus $f : \mathbb{Z}_2 \to \{-1, 1\}$ je dán předpisem:

$$f([0]_2) = 1, \quad f([1]_2) = -1.$$

Proč je zobrazení f izomorfismus?
Zobrazení je zřejmě bijektivní. Zobrazení splňuje:

- $f([0]_2 + [0]_2) = f([0]_2) = 1$, $f([0]_2) \cdot f([0]_2) = 1 \cdot 1 = 1$,
- $f([1]_2 + [1]_2) = f([0]_2) = 1$, $f([1]_2) \cdot f([1]_2) = -1 \cdot -1 = 1$,

První příklad

Grupa $(\mathbb{Z}_2, +)$ je izomorfní s grupou $(\{1, -1\}, \cdot)$, což je podgrupa $(\mathbb{R}^*, \cdot)$. Izomorfismus $f : \mathbb{Z}_2 \to \{-1, 1\}$ je dán předpisem:

$$f([0]_2) = 1, \quad f([1]_2) = -1.$$

Proč je zobrazení f izomorfismus?
Zobrazení je zřejmě bijektivní. Zobrazení splňuje:

- $f([0]_2 + [0]_2) = f([0]_2) = 1$, $f([0]_2) \cdot f([0]_2) = 1 \cdot 1 = 1$,
- $f([1]_2 + [1]_2) = f([0]_2) = 1$, $f([1]_2) \cdot f([1]_2) = -1 \cdot -1 = 1$,
- $f([1]_2 + [0]_2) = f([1]_2) = -1$, $f([1]_2) \cdot f([0]_2) = -1 \cdot 1 = -1$,

První příklad

Grupa $(\mathbb{Z}_2, +)$ je izomorfní s grupou $(\{1, -1\}, \cdot)$, což je podgrupa $(\mathbb{R}^*, \cdot)$. Izomorfismus $f : \mathbb{Z}_2 \to \{-1, 1\}$ je dán předpisem:

$$f([0]_2) = 1, \quad f([1]_2) = -1.$$

Proč je zobrazení f izomorfismus?
Zobrazení je zřejmě bijektivní. Zobrazení splňuje:

- $f([0]_2 + [0]_2) = f([0]_2) = 1$, $f([0]_2) \cdot f([0]_2) = 1 \cdot 1 = 1$,
- $f([1]_2 + [1]_2) = f([0]_2) = 1$, $f([1]_2) \cdot f([1]_2) = -1 \cdot -1 = 1$,
- $f([1]_2 + [0]_2) = f([1]_2) = -1$, $f([1]_2) \cdot f([0]_2) = -1 \cdot 1 = -1$,
- $f([0]_2 + [1]_2) = f([1]_2) = -1$, $f([0]_2) \cdot f([1]_2) = 1 \cdot -1 = -1$.

První příklad

Grupa $(\mathbb{Z}_2, +)$ je izomorfní s grupou $(\{1, -1\}, \cdot)$, což je podgrupa $(\mathbb{R}^*, \cdot)$. Izomorfismus $f : \mathbb{Z}_2 \to \{-1, 1\}$ je dán předpisem:

$$f([0]_2) = 1, \quad f([1]_2) = -1.$$

Proč je zobrazení f izomorfismus?
Zobrazení je zřejmě bijektivní. Zobrazení splňuje:

- $f([0]_2 + [0]_2) = f([0]_2) = 1$, $f([0]_2) \cdot f([0]_2) = 1 \cdot 1 = 1$,
- $f([1]_2 + [1]_2) = f([0]_2) = 1$, $f([1]_2) \cdot f([1]_2) = -1 \cdot -1 = 1$,
- $f([1]_2 + [0]_2) = f([1]_2) = -1$, $f([1]_2) \cdot f([0]_2) = -1 \cdot 1 = -1$,
- $f([0]_2 + [1]_2) = f([1]_2) = -1$, $f([0]_2) \cdot f([1]_2) = 1 \cdot -1 = -1$.

Tedy pro libovolné $a, b \in \mathbb{Z}_2$ platí $f(a + b) = f(a) \cdot f(b)$.

Druhý příklad

Grupa $(\mathbb{Z}, +)$ je izomorfní s grupou $(n\mathbb{Z}, +)$ pro libovolné $n \in \mathbb{N}$. Izomorfismus $f : \mathbb{Z} \to n\mathbb{Z}$ je dán pro každé $a \in \mathbb{Z}$ předpisem:

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

Proč je zobrazení f izomorfismus?

Druhý příklad

Grupa $(\mathbb{Z}, +)$ je izomorfní s grupou $(n\mathbb{Z}, +)$ pro libovolné $n \in \mathbb{N}$. Izomorfismus $f : \mathbb{Z} \to n\mathbb{Z}$ je dán pro každé $a \in \mathbb{Z}$ předpisem:

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

Proč je zobrazení f izomorfismus?
Zobrazení je zřejmě bijektivní. Zobrazení splňuje:

$$f(a+b) = n \cdot (a+b) = n \cdot a + n \cdot b,$$
$$f(a) + f(b) = n \cdot a + n \cdot b$$

pro libovolná $a, b \in \mathbb{Z}$. Dostaneme $f(a+b) = f(a) + f(b)$.

Třetí příklad

Grupa $(\mathbb{R}^+, \cdot)$ je izomorfní s grupou $(\mathbb{R}, +)$. Izomorfismus je dán zobrazením

$$log : \mathbb{R}^+ \to \mathbb{R}.$$

Proč je zobrazení *log* izomorfismus?

Třetí příklad

Grupa $(\mathbb{R}^+, \cdot)$ je izomorfní s grupou $(\mathbb{R}, +)$. Izomorfismus je dán zobrazením

$$log : \mathbb{R}^+ \to \mathbb{R}.$$

Proč je zobrazení *log* izomorfismus?
Z analýzy víte, že zobrazení je bijektivní. Zbytek plyne ze známého vztahu

$$log(a \cdot b) = log(a) + \log(b)$$

pro libovolná $a, b \in \mathbb{R}^+$.

Čtvrtý příklad

Grupa $(\mathbb{Z}_6, +)$ je izomorfní s grupou $(\mathbb{Z}_7^*, \cdot)$. Izomorfismus $f : \mathbb{Z}_6 \to \mathbb{Z}_7^*$ je dán předpisem

$$\begin{aligned} f([0]_6) &= [1]_7, \quad f([1]_6) = [3]_7, \\ f([2]_6) &= [2]_7, \quad f([3]_6) = [6]_7, \\ f([4]_6) &= [4]_7, \quad f([5]_6) = [5]_7. \end{aligned}$$

Proč je zobrazení f izomorfismus?

Čtvrtý příklad

Grupa $(\mathbb{Z}_6, +)$ je izomorfní s grupou $(\mathbb{Z}_7^*, \cdot)$. Izomorfismus $f : \mathbb{Z}_6 \to \mathbb{Z}_7^*$ je dán předpisem

$$\begin{aligned} f([0]_6) &= [1]_7, \quad f([1]_6) = [3]_7, \\ f([2]_6) &= [2]_7, \quad f([3]_6) = [6]_7, \\ f([4]_6) &= [4]_7, \quad f([5]_6) = [5]_7. \end{aligned}$$

Proč je zobrazení f izomorfismus?
Stačí porovnat sčítací tabulku $\mathbb{Z}_6$ a multiplikativní tabulku $\mathbb{Z}_7^*$.

A teď obecně

Definition

Počet prvků grupy G se nazývá *řád* grupy G.

A teď obecně

Definition

Počet prvků grupy G se nazývá *řád* grupy G.

Theorem

- *Libovolná nekonečná cyklická grupa je izomorfní grupě* $(\mathbb{Z}, +)$.
- *Libovolná konečná cyklická grupa řádu n je izomorfní grupě* $(\mathbb{Z}_n, +)$.

Proof: ...

Cayleyova věta

Theorem

- *Libovolná grupa je izomorfní nějaké podgrupě grupy všech permutací $(S(X), \circ)$ nějaké vhodné množiny X.*
  (Množina X může být nekonečná!)
- *Každá konečná grupa řádu n je izomorfní nějaké podgrupě grupy $(S_n, \circ)$ všech permutací n-prvkové množiny.*