NI-MPI přednáška 13

Algebra II

Štěpán Starosta

18. 11. 2024

FIT ČVUT

Příklad $\mathbb{Z}_{12}^{+}$ (1 ze 3)

Příklad 28.1
Uvažme množinu $\mathbb{Z}_{12} := \{0, 1, 2, \ldots, 11\}$ se sčítáním modulo 12. Podle minulé přednášky tato dvojice tvoří aditivní grupu modulo 12 značenou $\mathbb{Z}_{12}^{+}$.

Příklad $\mathbb{Z}_{12}^{+}$ (1 ze 3)

Příklad 28.1
Uvažme množinu $\mathbb{Z}_{12} := \{0, 1, 2, \ldots, 11\}$ se sčítáním modulo 12. Podle minulé přednášky tato dvojice tvoří aditivní grupu modulo 12 značenou $\mathbb{Z}_{12}^{+}$.

Otázka: Jaká jiná množina M tvoří s operací sčítání $\mod 12$ grupu?

Příklad $\mathbb{Z}_{12}^{+}$ (1 ze 3)

Příklad 28.1
Uvažme množinu $\mathbb{Z}_{12} := \{0, 1, 2, \ldots, 11\}$ se sčítáním modulo 12. Podle minulé přednášky tato dvojice tvoří aditivní grupu modulo 12 značenou $\mathbb{Z}_{12}^{+}$.

Otázka: Jaká jiná množina M tvoří s operací sčítání $\mod 12$ grupu?

Aby tato binární operace měla smysl, musí být $M \subseteq \mathbb{Z}_{12}$:

Otázka (upřesnění): Jaké podmnožiny $\mathbb{Z}_{12}$ tvoří s operací sčítání $\mod 12$ grupu?

Příklad $\mathbb{Z}_{12}^{+}$ (1 ze 3)

Příklad 28.1
Uvažme množinu $\mathbb{Z}_{12} := \{0, 1, 2, \ldots, 11\}$ se sčítáním modulo 12. Podle minulé přednášky tato dvojice tvoří aditivní grupu modulo 12 značenou $\mathbb{Z}_{12}^{+}$.

Otázka: Jaká jiná množina M tvoří s operací sčítání $\mod 12$ grupu?

Aby tato binární operace měla smysl, musí být $M \subseteq \mathbb{Z}_{12}$:

Otázka (upřesnění): Jaké podmnožiny $\mathbb{Z}_{12}$ tvoří s operací sčítání $\mod 12$ grupu?

Odpověď: Je jich poměrně hodně a abychom přišli na to, jak je získat, položme si podotázku:

Podotázka: Jaká nejmenší podmnožina $\mathbb{Z}_{12}$ tvoří s operací $+_{12}$ (sčítání modulo 12) grupu a obsahuje číslo $2 \in \mathbb{Z}_{12}$?

Příklad $\mathbb{Z}_{12}^{+}$ (2 ze 3)

Hledáme množinu $M \subseteq \mathbb{Z}_{12}$ tak, aby $2 \in M$ a $(M, +_{12})$ byla grupa:

Příklad $\mathbb{Z}_{12}^{+}$ (2 ze 3)

Hledáme množinu $M \subseteq \mathbb{Z}_{12}$ tak, aby $2 \in M$ a $(M, +_{12})$ byla grupa:

- M musí být vůči sčítání modulo 12 uzavřená:
  - musí proto obsahovat $2 +_{12} 2 = \mathbf{4}$, $2 +_{12} 4 = \mathbf{6}$, $4 +_{12} 6 = \mathbf{10}, \ldots$

Příklad $\mathbb{Z}_{12}^{+}$ (2 ze 3)

Hledáme množinu $M \subseteq \mathbb{Z}_{12}$ tak, aby $2 \in M$ a $(M, +_{12})$ byla grupa:

- M musí být vůči sčítání modulo 12 uzavřená:
  - musí proto obsahovat $2 +_{12} 2 = \mathbf{4}$, $2 +_{12} 4 = \mathbf{6}$, $4 +_{12} 6 = \mathbf{10}, \ldots$
  - množina $\{0, 2, 4, 6, 8, 10\}$ už je uzavřená a tedy máme grupoid

Příklad $\mathbb{Z}_{12}^{+}$ (2 ze 3)

Hledáme množinu $M \subseteq \mathbb{Z}_{12}$ tak, aby $2 \in M$ a $(M, +_{12})$ byla grupa:

- M musí být vůči sčítání modulo 12 uzavřená:
  - musí proto obsahovat $2 +_{12} 2 = \mathbf{4}$, $2 +_{12} 4 = \mathbf{6}$, $4 +_{12} 6 = \mathbf{10}, \ldots$
  - množina $\{0, 2, 4, 6, 8, 10\}$ už je uzavřená a tedy máme grupoid
- operace sčítání modulo 12 i na této podmnožině zůstává asociativní, je to pologrupa,

Příklad $\mathbb{Z}_{12}^{+}$ (2 ze 3)

Hledáme množinu $M \subseteq \mathbb{Z}_{12}$ tak, aby $2 \in M$ a $(M, +_{12})$ byla grupa:

- M musí být vůči sčítání modulo 12 uzavřená:
  - musí proto obsahovat $2 +_{12} 2 = \mathbf{4}$, $2 +_{12} 4 = \mathbf{6}$, $4 +_{12} 6 = \mathbf{10}, \ldots$
  - množina $\{0, 2, 4, 6, 8, 10\}$ už je uzavřená a tedy máme grupoid
- operace sčítání modulo 12 i na této podmnožině zůstává asociativní, je to pologrupa,
- 0 zůstává neutrálním prvkem, je to monoid,

Příklad $\mathbb{Z}_{12}^{+}$ (2 ze 3)

Hledáme množinu $M \subseteq \mathbb{Z}_{12}$ tak, aby $2 \in M$ a $(M, +_{12})$ byla grupa:

- M musí být vůči sčítání modulo 12 uzavřená:
  - musí proto obsahovat $2 +_{12} 2 = \mathbf{4}$, $2 +_{12} 4 = \mathbf{6}$, $4 +_{12} 6 = \mathbf{10}, \ldots$
  - množina $\{0, 2, 4, 6, 8, 10\}$ už je uzavřená a tedy máme grupoid
- operace sčítání modulo 12 i na této podmnožině zůstává asociativní, je to pologrupa,
- 0 zůstává neutrálním prvkem, je to monoid,
- a každý prvek má inverzní prvek patřící do této množiny ($-0 = 0$, $-2 = 10$, $-4 = 8$, $-6 = 6$, $-8 = 4$, $-10 = 2$), je to grupa.

Příklad $\mathbb{Z}_{12}^{+}$ (2 ze 3)

Hledáme množinu $M \subseteq \mathbb{Z}_{12}$ tak, aby $2 \in M$ a $(M, +_{12})$ byla grupa:

- M musí být vůči sčítání modulo 12 uzavřená:
  - musí proto obsahovat $2 +_{12} 2 = \mathbf{4}$, $2 +_{12} 4 = \mathbf{6}$, $4 +_{12} 6 = \mathbf{10}, \ldots$
  - množina $\{0, 2, 4, 6, 8, 10\}$ už je uzavřená a tedy máme grupoid
- operace sčítání modulo 12 i na této podmnožině zůstává asociativní, je to pologrupa,
- 0 zůstává neutrálním prvkem, je to monoid,
- a každý prvek má inverzní prvek patřící do této množiny ($-0 = 0$, $-2 = 10$, $-4 = 8$, $-6 = 6$, $-8 = 4$, $-10 = 2$), je to grupa.

Hledaná množina je tedy $M = \{0, 2, 4, 6, 8, 10\}$: říkáme, že M je podgrupa generovaná množinou $\{2\}$.

Příklad $\mathbb{Z}_{12}^{+}$ (3 ze 3)

Podobně jako jsme vygenerovali množinu pro prvek 2, můžeme postupovat i pro jiné prvky $\mathbb{Z}_{12}$:

$$\{2\} \rightarrow \qquad \{0, 2, 4, 6, 8, 10\}$$

Příklad $\mathbb{Z}_{12}^{+}$ (3 ze 3)

Podobně jako jsme vygenerovali množinu pro prvek 2, můžeme postupovat i pro jiné prvky $\mathbb{Z}_{12}$:

$$\{0\} \rightarrow \quad \{0\}$$

$$\{2\} \rightarrow \quad \{0, 2, 4, 6, 8, 10\}$$

Příklad $\mathbb{Z}_{12}^{+}$ (3 ze 3)

Podobně jako jsme vygenerovali množinu pro prvek 2, můžeme postupovat i pro jiné prvky $\mathbb{Z}_{12}$:

$$\begin{aligned} \{0\} &\to \{0\} \\ \{1\} &\to \{0,1,2,3,4,5,6,7,8,9,10,11\} \\ \{2\} &\to \{0,2,4,6,8,10\} \end{aligned}$$

Příklad $\mathbb{Z}_{12}^{+}$ (3 ze 3)

Podobně jako jsme vygenerovali množinu pro prvek 2, můžeme postupovat i pro jiné prvky $\mathbb{Z}_{12}$:

$$
\begin{aligned}
\{0\} &\to \{0\} \\
\{1\} &\to \{0,1,2,3,4,5,6,7,8,9,10,11\} \\
\{2\} &\to \{0,2,4,6,8,10\} \\
\{3\} &\to \{0,3,6,9\} \\
\{4\} &\to \{0,4,8\}
\end{aligned}
$$

Příklad $\mathbb{Z}_{12}^{+}$ (3 ze 3)

Podobně jako jsme vygenerovali množinu pro prvek 2, můžeme postupovat i pro jiné prvky $\mathbb{Z}_{12}$:

$$
\begin{aligned}
\{0\} &\to \{0\} \\
\{1\} &\to \{0,1,2,3,4,5,6,7,8,9,10,11\} \\
\{2\} &\to \{0,2,4,6,8,10\} \\
\{3\} &\to \{0,3,6,9\} \\
\{4\} &\to \{0,4,8\} \\
\{5\} &\to \{0,5,10,3,8,1,6,11,4,9,2,7\}
\end{aligned}
$$

Příklad $\mathbb{Z}_{12}^{+}$ (3 ze 3)

Podobně jako jsme vygenerovali množinu pro prvek 2, můžeme postupovat i pro jiné prvky $\mathbb{Z}_{12}$:

$$
\begin{aligned}
\{0\} &\to \{0\} \\
\{1\} &\to \{0,1,2,3,4,5,6,7,8,9,10,11\} \\
\{2\} &\to \{0,2,4,6,8,10\} \\
\{3\} &\to \{0,3,6,9\} \\
\{4\} &\to \{0,4,8\} \\
\{5\} &\to \{0,5,10,3,8,1,6,11,4,9,2,7\} \\
\{6\} &\to \{0,6\}
\end{aligned}
$$

Příklad $\mathbb{Z}_{12}^{+}$ (3 ze 3)

Podobně jako jsme vygenerovali množinu pro prvek 2, můžeme postupovat i pro jiné prvky $\mathbb{Z}_{12}$:

$$
\begin{aligned}
\{0\} &\to \{0\} \\
\{1\} &\to \{0,1,2,3,4,5,6,7,8,9,10,11\} \\
\{2\} &\to \{0,2,4,6,8,10\} \\
\{3\} &\to \{0,3,6,9\} \\
\{4\} &\to \{0,4,8\} \\
\{5\} &\to \{0,5,10,3,8,1,6,11,4,9,2,7\} \quad \leftarrow \{7\} \\
\{6\} &\to \{0,6\}
\end{aligned}
$$

Příklad $\mathbb{Z}_{12}^{+}$ (3 ze 3)

Podobně jako jsme vygenerovali množinu pro prvek 2, můžeme postupovat i pro jiné prvky $\mathbb{Z}_{12}$:

$$
\begin{array}{lcl}
\{0\} \to & \{0\} & \\
\{1\} \to & \{0,1,2,3,4,5,6,7,8,9,10,11\} & \leftarrow \{11\} \\
\{2\} \to & \{0,2,4,6,8,10\} & \leftarrow \{10\} \\
\{3\} \to & \{0,3,6,9\} & \leftarrow \{9\} \\
\{4\} \to & \{0,4,8\} & \leftarrow \{8\} \\
\{5\} \to & \{0,5,10,3,8,1,6,11,4,9,2,7\} & \leftarrow \{7\} \\
\{6\} \to & \{0,6\} &
\end{array}
$$

Příklad $\mathbb{Z}_{12}^{+}$ (3 ze 3)

Podobně jako jsme vygenerovali množinu pro prvek 2, můžeme postupovat i pro jiné prvky $\mathbb{Z}_{12}$:

$$
\begin{array}{lcl}
\{0\} \to & \{0\} & \\
\{1\} \to & \{0,1,2,3,4,5,6,7,8,9,10,11\} & \leftarrow \{11\} \\
\{2\} \to & \{0,2,4,6,8,10\} & \leftarrow \{10\} \\
\{3\} \to & \{0,3,6,9\} & \leftarrow \{9\} \\
\{4\} \to & \{0,4,8\} & \leftarrow \{8\} \\
\{5\} \to & \{0,5,10,3,8,1,6,11,4,9,2,7\} & \leftarrow \{7\} \\
\{6\} \to & \{0,6\} &
\end{array}
$$

Závěr: nalezli jsme 6 různých množin M takových, že $(M, +_{12})$ tvoří grupu.

Definice podgrupy

Definice 28.2 (Podgrupa (*subgroup*))

Buď $G = (M, \circ)$ grupa. Podgrupou grupy G nazveme libovolnou dvojici $H = (N, \circ)$ takovou, že

- $N \subseteq M$,
- $(N, \circ)$ je grupa.

Definice podgrupy

Definice 28.2 (Podgrupa (*subgroup*))

Buď $G = (M, \circ)$ grupa. Podgrupou grupy G nazveme libovolnou dvojici $H = (N, \circ)$ takovou, že

- $N \subseteq M$,
- $(N, \circ)$ je grupa.

- Tato konstrukce, kde se z dané struktury vezme podstruktura, která má stejné vlastnosti, je v matematice častá: vzpomeňte lineární prostor a podprostor.

Definice podgrupy

Definice 28.2 (Podgrupa (*subgroup*))

Buď $G = (M, \circ)$ grupa. Podgrupou grupy G nazveme libovolnou dvojici $H = (N, \circ)$ takovou, že

- $N \subseteq M$,
- $(N, \circ)$ je grupa.

- Tato konstrukce, kde se z dané struktury vezme podstruktura, která má stejné vlastnosti, je v matematice častá: vzpomeňte lineární prostor a podprostor.
- Podobně bychom mohli definovat podgrupoid, podpologrupu a podmonoid, ale nebudeme.

Definice podgrupy

Definice 28.2 (Podgrupa (*subgroup*))

Buď $G = (M, \circ)$ grupa. Podgrupou grupy G nazveme libovolnou dvojici $H = (N, \circ)$ takovou, že

- $N \subseteq M$,
- $(N, \circ)$ je grupa.

- Tato konstrukce, kde se z dané struktury vezme podstruktura, která má stejné vlastnosti, je v matematice častá: vzpomeňte lineární prostor a podprostor.
- Podobně bychom mohli definovat podgrupoid, podpologrupu a podmonoid, ale nebudeme.
- Binární operaci v grupě $G = (M, \circ)$ chápeme jako zobrazení z $M \times M$ do M, operace v podgrupě $H = (N, \circ)$ je tedy exaktně řečeno zúžení původní operace na množinu $N \times N$.

(Ne)triviální podgrupy

V každé grupě $G = (M, \circ)$ s alespoň dvěma prvky existují vždy alespoň dvě (různé) podgrupy:

- grupa obsahující pouze neutrální prvek: $(\{e\}, \circ)$
- a grupa samotná: $G = (M, \circ)$.

Těmto dvěma grupám se říká triviální podgrupy, ostatním podgrupám se říká netriviální nebo vlastní podgrupy.

(Ne)triviální podgrupy

V každé grupě $G = (M, \circ)$ s alespoň dvěma prvky existují vždy alespoň dvě (různé) podgrupy:

- grupa obsahující pouze neutrální prvek: $(\{e\}, \circ)$
- a grupa samotná: $G = (M, \circ)$.

Těmto dvěma grupám se říká triviální podgrupy, ostatním podgrupám se říká netriviální nebo vlastní podgrupy.

Kontrolní otázka 28.1

Je-li H podgrupa grupy G, musí být vždy neutrální prvek v H shodný s neutrálním prvkem G?

Základní cvičení 17.1

Mějme grupu $\mathbb{Z}_8^\times$. Kolik má prvků? Najděte všechny vlastní podgrupy této grupy.

Průnik podgrup je opět podgrupa

Věta 28.3

Pro každé i z indexové množiny $\mathcal{I}$ buď H_i podgrupa grupy $G = (M, \circ)$, potom platí, že

$$H' = \bigcap_{i \in \mathcal{I}} H_i \quad \textit{je také podgrupa grupy } G.$$

Průnik podgrup je opět podgrupa

Věta 28.3

Pro každé i z indexové množiny $\mathcal{I}$ buď H_i podgrupa grupy $G = (M, \circ)$, potom platí, že

$$H' = \bigcap_{i \in \mathcal{I}} H_i \quad \textit{je také podgrupa grupy } G.$$

Důkaz.

Jistě je H' podmnožinou M a je neprázdná.

Průnik podgrup je opět podgrupa

Věta 28.3

Pro každé i z indexové množiny $\mathcal{I}$ buď H_i podgrupa grupy $G = (M, \circ)$, potom platí, že

$$H' = \bigcap_{i \in \mathcal{I}} H_i \quad \textit{je také podgrupa grupy } G.$$

Důkaz.

Jistě je H' podmnožinou M a je neprázdná.

- H' je uzavřená vůči operaci $\circ$:
  pro všechna $a, b \in H'$ platí: pro všechna $i \in \mathcal{I}$ máme $a, b \in H_i$, a jelikož H_i jsou uzavřené vůči $\circ$, tak platí $a \circ b \in H_i$;
  celkem tedy pro všechna $a, b \in H'$ máme $a \circ b \in H'$ a uzavřenost je dokázána.

Průnik podgrup je opět podgrupa

Věta 28.3

Pro každé i z indexové množiny $\mathcal{I}$ buď H_i podgrupa grupy $G = (M, \circ)$, potom platí, že

$$H' = \bigcap_{i \in \mathcal{I}} H_i \quad \textit{je také podgrupa grupy } G.$$

Důkaz.

Jistě je H' podmnožinou M a je neprázdná.

- H' je uzavřená vůči operaci $\circ$:
  pro všechna $a, b \in H'$ platí: pro všechna $i \in \mathcal{I}$ máme $a, b \in H_i$, a jelikož H_i jsou uzavřené vůči $\circ$, tak platí $a \circ b \in H_i$;
  celkem tedy pro všechna $a, b \in H'$ máme $a \circ b \in H'$ a uzavřenost je dokázána.
- Operace jistě zůstává asociativní, neutrální prvek zůstává stejný jako v G.

Průnik podgrup je opět podgrupa

Věta 28.3

Pro každé i z indexové množiny $\mathcal{I}$ buď H_i podgrupa grupy $G = (M, \circ)$, potom platí, že

$$H' = \bigcap_{i \in \mathcal{I}} H_i \quad \textit{je také podgrupa grupy } G.$$

Důkaz.

Jistě je H' podmnožinou M a je neprázdná.

- H' je uzavřená vůči operaci $\circ$:
  pro všechna $a, b \in H'$ platí: pro všechna $i \in \mathcal{I}$ máme $a, b \in H_i$, a jelikož H_i jsou uzavřené vůči $\circ$, tak platí $a \circ b \in H_i$;
  celkem tedy pro všechna $a, b \in H'$ máme $a \circ b \in H'$ a uzavřenost je dokázána.
- Operace jistě zůstává asociativní, neutrální prvek zůstává stejný jako v G.
- Uzavřenost vůči inverzi prvku se ukáže stejně jako uzavřenost vůči operaci $\circ$. □

Indexová množina může být konečná (např. $\mathcal{I} = \{1, 2, \ldots, n\}$) i nekonečná.

Kritérium pro „být podgrupou“

Při ověřování, zda-li jistá podmnožina již známe grupy vytváří podgrupu, nemusíme ověřovat všechny podmínky v definici grupy. Máme k dispozici následující užitečnou větu:

Věta 28.4

Buď $G = (M, \circ)$ grupa a $N \subseteq M$ neprázdná množina. Dvojice $H = (N, \circ)$ je podgrupa grupy G, právě když pro každé $a, b \in N$ platí $a \circ b^{-1} \in N$.

Kritérium pro „být podgrupou“

Při ověřování, zda-li jistá podmnožina již známe grupy vytváří podgrupu, nemusíme ověřovat všechny podmínky v definici grupy. Máme k dispozici následující užitečnou větu:

Věta 28.4

Buď $G = (M, \circ)$ grupa a $N \subseteq M$ neprázdná množina. Dvojice $H = (N, \circ)$ je podgrupa grupy G, právě když pro každé $a, b \in N$ platí $a \circ b^{-1} \in N$.

Důkaz.

Implikace zleva doprava je zřejmá. Ověřme implikaci zprava doleva.

Kritérium pro „být podgrupou“

Při ověřování, zda-li jistá podmnožina již známe grupy vytváří podgrupu, nemusíme ověřovat všechny podmínky v definici grupy. Máme k dispozici následující užitečnou větu:

Věta 28.4

Buď $G = (M, \circ)$ grupa a $N \subseteq M$ neprázdná množina. Dvojice $H = (N, \circ)$ je podgrupa grupy G, právě když pro každé $a, b \in N$ platí $a \circ b^{-1} \in N$.

Důkaz.

Implikace zleva doprava je zřejmá. Ověřme implikaci zprava doleva.

Postupně zkontrolujeme, že $(N, \circ)$ je grupa.

- Operaci $\circ$ jsme nijak nezměnili a její asociativita je tedy zachována.

Kritérium pro „být podgrupou“

Při ověřování, zda-li jistá podmnožina již známe grupy vytváří podgrupu, nemusíme ověřovat všechny podmínky v definici grupy. Máme k dispozici následující užitečnou větu:

Věta 28.4

Buď $G = (M, \circ)$ grupa a $N \subseteq M$ neprázdná množina. Dvojice $H = (N, \circ)$ je podgrupa grupy G, právě když pro každé $a, b \in N$ platí $a \circ b^{-1} \in N$.

Důkaz.

Implikace zleva doprava je zřejmá. Ověřme implikaci zprava doleva.

Postupně zkontrolujeme, že $(N, \circ)$ je grupa.

- Operaci $\circ$ jsme nijak nezměnili a její asociativita je tedy zachována.
- Vezměme $a \in N$, potom $e = a \circ a^{-1} \in N$.

Kritérium pro „být podgrupou“

Při ověřování, zda-li jistá podmnožina již známe grupy vytváří podgrupu, nemusíme ověřovat všechny podmínky v definici grupy. Máme k dispozici následující užitečnou větu:

Věta 28.4

Buď $G = (M, \circ)$ grupa a $N \subseteq M$ neprázdná množina. Dvojice $H = (N, \circ)$ je podgrupa grupy G, právě když pro každé $a, b \in N$ platí $a \circ b^{-1} \in N$.

Důkaz.

Implikace zleva doprava je zřejmá. Ověřme implikaci zprava doleva.

Postupně zkontrolujeme, že $(N, \circ)$ je grupa.

- Operaci $\circ$ jsme nijak nezměnili a její asociativita je tedy zachována.
- Vezměme $a \in N$, potom $e = a \circ a^{-1} \in N$.
- Uvažme $a \in N$, potom $a^{-1} = e \circ a^{-1} \in N$.

Kritérium pro „být podgrupou“

Při ověřování, zda-li jistá podmnožina již známe grupy vytváří podgrupu, nemusíme ověřovat všechny podmínky v definici grupy. Máme k dispozici následující užitečnou větu:

Věta 28.4

Buď $G = (M, \circ)$ grupa a $N \subseteq M$ neprázdná množina. Dvojice $H = (N, \circ)$ je podgrupa grupy G, právě když pro každé $a, b \in N$ platí $a \circ b^{-1} \in N$.

Důkaz.

Implikace zleva doprava je zřejmá. Ověřme implikaci zprava doleva.

Postupně zkontrolujeme, že $(N, \circ)$ je grupa.

- Operaci $\circ$ jsme nijak nezměnili a její asociativita je tedy zachována.
- Vezměme $a \in N$, potom $e = a \circ a^{-1} \in N$.
- Uvažme $a \in N$, potom $a^{-1} = e \circ a^{-1} \in N$.
- Pro $a, b \in N$ platí $a \circ b = a \circ (b^{-1})^{-1} \in N$. □

Řád grupy

Definice 29.1 (Řád (*order*))

Řád grupy $G = (M, \circ)$ nazýváme počet prvků množiny M. Je-li M nekonečná množina, řekneme, že její řád je nekonečno. Řád grupy G značíme $\#G$. Má-li G konečný řád, řekneme, že G je konečná (grupa), jinak nekonečná (grupa).

Řád grupy

Definice 29.1 (Řád (*order*))

Řád grupy $G = (M, \circ)$ nazýváme počet prvků množiny M. Je-li M nekonečná množina, řekneme, že její řád je nekonečno. Řád grupy G značíme $\#G$. Má-li G konečný řád, řekneme, že G je konečná (grupa), jinak nekonečná (grupa).

Příklad 29.2 (pokračování)

Grupa $\mathbb{Z}_{12}^{+}$ je řádu 12. Existuje v ní 6 podgrup:

dvě triviální

$$\{0\} \quad \text{a} \quad \{0,1,2,3,4,5,6,7,8,9,10,11\}$$

řádů 1 a 12 a čtyři vlastní

$$\{0,6\},\ \{0,4,8\},\ \{0,3,6,9\} \quad \text{a} \quad \{0,2,4,6,8,10\}$$

řádů $2, 3, 4$ a 6.

Lagrangeova věta

Věta 29.3 (Lagrangeova)

Buď H podgrupa konečné grupy G. Potom řád H je dělitelem řádu G.

Lagrangeova věta

Věta 29.3 (Lagrangeova)

Buď H podgrupa konečné grupy G. Potom řád H je dělitelem řádu G.

Důkaz.

Důkaz je naznačen v handoutu. □

Lagrangeova věta

Věta 29.3 (Lagrangeova)

Buď H podgrupa konečné grupy G. Potom řád H je dělitelem řádu G.

Důkaz.

Důkaz je naznačen v handoutu. □

- Tato věta spojuje abstraktní strukturu grupy s pojmem dělitelnosti a tedy i s pojmem prvočísla.

Lagrangeova věta

Věta 29.3 (Lagrangeova)

Buď H podgrupa konečné grupy G. Potom řád H je dělitelem řádu G.

Důkaz.

Důkaz je naznačen v handoutu. □

- Tato věta spojuje abstraktní strukturu grupy s pojmem dělitelnosti a tedy i s pojmem prvočísla.
- **Důsledek**: Grupa s prvočíselným řádem má pouze triviální podgrupy.

Lagrangeova věta

Věta 29.3 (Lagrangeova)

Buď H podgrupa konečné grupy G. Potom řád H je dělitelem řádu G.

Důkaz.

Důkaz je naznačen v handoutu. □

- Tato věta spojuje abstraktní strukturu grupy s pojmem dělitelnosti a tedy i s pojmem prvočísla.
- **Důsledek**: Grupa s prvočíselným řádem má pouze triviální podgrupy.
- Například grupa $\mathbb{Z}_{11}^{+}$ má pouze dvě podgrupy $\{0\}$ a sebe samu.

Lagrangeova věta

Věta 29.3 (Lagrangeova)

Buď H podgrupa konečné grupy G. Potom řád H je dělitelem řádu G.

Důkaz.

Důkaz je naznačen v handoutu. □

- Tato věta spojuje abstraktní strukturu grupy s pojmem dělitelnosti a tedy i s pojmem prvočísla.
- **Důsledek**: Grupa s prvočíselným řádem má pouze triviální podgrupy.
- Například grupa $\mathbb{Z}_{11}^{+}$ má pouze dvě podgrupy $\{0\}$ a sebe samu.

Kontrolní otázka 29.1

Buď G grupa řádu n a $k \in \mathbb{N}$ takové, že k dělí n. Může nastat situace, že v G neexistuje podgrupa řádu k?

Pro zvídavé: jak je to tedy s dalšími podgrupami?

Věta 29.4 (Sylowova věta)

Buď G grupa konečného řádu n a číslo p prvočíselný dělitel čísla n. Pokud p^k dělí n (pro k kladné celé), pak grupa G obsahuje podgrupu řádu p^k.

(Pro $k = 1$ též Cauchyho věta.)

28. Podgrupy

29. Řád grupy a Lagrangeova věta

30. Generující množiny a generátory grup

31. Cyklické grupy

32. (Malá) Fermatova věta

Grupa generovaná množinou (1 ze 3)

Připomenutí: V lineární algebře hraje důležitou roli báze vektorového prostoru. V teorii grup má podobný význam generující množina, resp. generátor.

Při zafixované grupě G a neprázdné množině N, $N \subseteq G$, zavádíme toto značení:

$$\langle N \rangle := \bigcap \{H : H \text{ je podgrupa grupy } G \text{ obsahující } N\}.$$

Grupa generovaná množinou (1 ze 3)

Připomenutí: V lineární algebře hraje důležitou roli báze vektorového prostoru. V teorii grup má podobný význam generující množina, resp. generátor.

Při zafixované grupě G a neprázdné množině N, $N \subseteq G$, zavádíme toto značení:

$$\langle N \rangle := \bigcap \{H : H \text{ je podgrupa grupy } G \text{ obsahující } N\}.$$

Věta 30.1

Buď $G = (M, \circ)$ grupa a $N \subseteq M$ neprázdná množina. Množina $\langle N \rangle$ je podgrupou grupy G obsahující množinu N.

Grupa generovaná množinou (1 ze 3)

Připomenutí: V lineární algebře hraje důležitou roli báze vektorového prostoru. V teorii grup má podobný význam generující množina, resp. generátor.

Při zafixované grupě G a neprázdné množině N, $N \subseteq G$, zavádíme toto značení:

$$\langle N \rangle := \bigcap \{H : H \text{ je podgrupa grupy } G \text{ obsahující } N\}.$$

Věta 30.1

Buď $G = (M, \circ)$ grupa a $N \subseteq M$ neprázdná množina. Množina $\langle N \rangle$ je podgrupou grupy G obsahující množinu N.

Důkaz.

$\langle N \rangle$ je grupa dle předchozí věty o průniku grup.

Každá z H obsahuje množinu N a proto i průnik všech těchto H, tj. $\langle N \rangle$, obsahuje N. □

Grupa generovaná množinou (2 ze 3)

Definice 30.2

Podgrupu $\langle N \rangle$ grupy G pro neprázdnou N, $N \subseteq M$, nazýváme podgrupou generovanou množinou N. Množinu N pak nazýváme generující množinou grupy $\langle N \rangle$.

Speciálně pro jednoprvkovou množinu $N = \{a\}$ zavádíme značení $\langle a \rangle := \langle \{a\} \rangle$. V tomto případě o a mluvíme jako o generátoru grupy $\langle a \rangle$.

Grupa generovaná množinou (2 ze 3)

Definice 30.2

Podgrupu $\langle N \rangle$ grupy G pro neprázdnou N, $N \subseteq M$, nazýváme podgrupou generovanou množinou N. Množinu N pak nazýváme generující množinou grupy $\langle N \rangle$.

Speciálně pro jednoprvkovou množinu $N = \{a\}$ zavádíme značení $\langle a \rangle := \langle \{a\} \rangle$. V tomto případě o a mluvíme jako o generátoru grupy $\langle a \rangle$.

Poznámka: $\langle N \rangle$ je nejmenší podgrupa grupy G obsahující množinu N. Z kontextu musí být čtenáři jasné, o jaké grupě se bavíme (v notaci $\langle N \rangle$ je to potlačeno).

Grupa generovaná množinou (2 ze 3)

Definice 30.2

Podgrupu $\langle N \rangle$ grupy G pro neprázdnou N, $N \subseteq M$, nazýváme podgrupou generovanou množinou N. Množinu N pak nazýváme generující množinou grupy $\langle N \rangle$.

Speciálně pro jednoprvkovou množinu $N = \{a\}$ zavádíme značení $\langle a \rangle := \langle \{a\} \rangle$. V tomto případě o a mluvíme jako o generátoru grupy $\langle a \rangle$.

Poznámka: $\langle N \rangle$ je nejmenší podgrupa grupy G obsahující množinu N. Z kontextu musí být čtenáři jasné, o jaké grupě se bavíme (v notaci $\langle N \rangle$ je to potlačeno).

Příklad 30.3

V grupě $\mathbb{Z}_{12}^{+}$ jsme ukázali, že $\langle 2 \rangle = \big(\{0, 2, 4, 6, 8, 10\},\, +_{12}\big)$.

Grupa generovaná množinou (2 ze 3)

Definice 30.2

Podgrupu $\langle N \rangle$ grupy G pro neprázdnou N, $N \subseteq M$, nazýváme podgrupou generovanou množinou N. Množinu N pak nazýváme generující množinou grupy $\langle N \rangle$.

Speciálně pro jednoprvkovou množinu $N = \{a\}$ zavádíme značení $\langle a \rangle := \langle \{a\} \rangle$. V tomto případě o a mluvíme jako o generátoru grupy $\langle a \rangle$.

Poznámka: $\langle N \rangle$ je nejmenší podgrupa grupy G obsahující množinu N. Z kontextu musí být čtenáři jasné, o jaké grupě se bavíme (v notaci $\langle N \rangle$ je to potlačeno).

Příklad 30.3
V grupě $\mathbb{Z}_{12}^+$ jsme ukázali, že $\langle 2 \rangle = \big(\{0, 2, 4, 6, 8, 10\}, +_{12}\big)$.

Příklad 30.4
Grupa $\mathbb{Z}_{12}^+$ je generována např. množinami $\{1\}$ a $\{5\}$, tzn.

$$\langle 1 \rangle = \langle 5 \rangle = \mathbb{Z}_{12}^+.$$

Ekvivalentně řečeno, prvky 1 i 5 jsou generátory $\mathbb{Z}_{12}^+$.

Mocnina prvku (připomenutí)

V grupě $G = (M, \circ)$ s neutrálním prvkem e definujeme pro každý prvek $g \in M$ a kladné $n \in \mathbb{N}$ n-tou mocninu a $(-n)$-tou mocninu prvku g takto:

$$g^0 = e$$
$$g^n = \underbrace{g \circ g \circ \cdots \circ g}_{n \text{ krát}}$$
$$g^n \circ g^{-n} = e$$

Mocnina prvku (připomenutí)

V grupě $G = (M, \circ)$ s neutrálním prvkem e definujeme pro každý prvek $g \in M$ a kladné $n \in \mathbb{N}$ n-tou mocninu a $(-n)$-tou mocninu prvku g takto:

$$g^0 = e$$
$$g^n = \underbrace{g \circ g \circ \cdots \circ g}_{n \text{ krát}}$$
$$g^n \circ g^{-n} = e$$

- Výše uvedené značení používáme i v grupě $(M, \cdot)$ s multiplikativní notací.

Mocnina prvku (připomenutí)

V grupě $G = (M, \circ)$ s neutrálním prvkem e definujeme pro každý prvek $g \in M$ a kladné $n \in \mathbb{N}$ n-tou mocninu a $(-n)$-tou mocninu prvku g takto:

$$g^0 = e$$
$$g^n = \underbrace{g \circ g \circ \cdots \circ g}_{n \text{ krát}}$$
$$g^n \circ g^{-n} = e$$

- Výše uvedené značení používáme i v grupě $(M, \cdot)$ s multiplikativní notací.
- Pro aditivní zápis grupy $G = (M, +)$ se používá n-tý násobek prvku g a značí se $n \times g$ resp. $-n \times g = n \times (-g)$.

Mocnina prvku (připomenutí)

V grupě $G = (M, \circ)$ s neutrálním prvkem e definujeme pro každý prvek $g \in M$ a kladné $n \in \mathbb{N}$ n-tou mocninu a $(-n)$-tou mocninu prvku g takto:

$$g^0 = e$$
$$g^n = \underbrace{g \circ g \circ \cdots \circ g}_{n \text{ krát}}$$
$$g^n \circ g^{-n} = e$$

- Výše uvedené značení používáme i v grupě $(M, \cdot)$ s multiplikativní notací.
- Pro aditivní zápis grupy $G = (M, +)$ se používá n-tý násobek prvku g a značí se $n \times g$ resp. $-n \times g = n \times (-g)$.
- Uvědomte si, že $g \circ g \circ \cdots \circ g$ můžeme psát bez závorek díky asociativitě.

Mocnina prvku (připomenutí)

V grupě $G = (M, \circ)$ s neutrálním prvkem e definujeme pro každý prvek $g \in M$ a kladné $n \in \mathbb{N}$ n-tou mocninu a $(-n)$-tou mocninu prvku g takto:

$$g^0 = e$$
$$g^n = \underbrace{g \circ g \circ \cdots \circ g}_{n \text{ krát}}$$
$$g^n \circ g^{-n} = e$$

- Výše uvedené značení používáme i v grupě $(M, \cdot)$ s multiplikativní notací.
- Pro aditivní zápis grupy $G = (M, +)$ se používá n-tý násobek prvku g a značí se $n \times g$ resp. $-n \times g = n \times (-g)$.
- Uvědomte si, že $g \circ g \circ \cdots \circ g$ můžeme psát bez závorek díky asociativitě.
- Pro všechna $n, m \in \mathbb{Z}$ platí zažité $g^{n+m} = g^n \circ g^m$ a $g^{nm} = (g^n)^m$.

Grupa generovaná množinou (3 ze 3)

Věta 30.5

Buď $G = (M, \circ)$ grupa a $N \subseteq M$ neprázdná množina. Potom všechny prvky patřící do $\langle N \rangle$ lze získat pomocí „grupového obalu“

$$\langle N \rangle = \left\{ a_1^{k_1} \circ a_2^{k_2} \circ \cdots \circ a_n^{k_n} \ : \ n \in \mathbb{N},\, k_i \in \mathbb{Z},\, a_i \in N \right\}.$$

Grupa generovaná množinou (3 ze 3)

Věta 30.5

Buď $G = (M, \circ)$ grupa a $N \subseteq M$ neprázdná množina. Potom všechny prvky patřící do $\langle N \rangle$ lze získat pomocí „grupového obalu“

$$\langle N \rangle = \left\{ a_1^{k_1} \circ a_2^{k_2} \circ \cdots \circ a_n^{k_n} \ : \ n \in \mathbb{N},\, k_i \in \mathbb{Z},\, a_i \in N \right\}.$$

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

Grupa generovaná množinou (3 ze 3)

Věta 30.5

Buď $G = (M, \circ)$ grupa a $N \subseteq M$ neprázdná množina. Potom všechny prvky patřící do $\langle N \rangle$ lze získat pomocí „grupového obalu“

$$\langle N \rangle = \left\{ a_1^{k_1} \circ a_2^{k_2} \circ \cdots \circ a_n^{k_n} \ : \ n \in \mathbb{N},\, k_i \in \mathbb{Z},\, a_i \in N \right\}.$$

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

Množina celých čísel, $\mathbb{Z}$, obsahuje i *záporná* čísla (například -5).

Příklad: Jak nagenerovat $\mathbb{Z}_n^+$?

Poznámka: Viděli jsme, že grupa $\mathbb{Z}_{12}^+$ je rovna $\langle 1 \rangle$, $\langle 5 \rangle$, $\langle 7 \rangle$ a $\langle 11 \rangle$.

Příklad: Jak nagenerovat $\mathbb{Z}_n^+$?

Poznámka: Viděli jsme, že grupa $\mathbb{Z}_{12}^+$ je rovna $\langle 1 \rangle$, $\langle 5 \rangle$, $\langle 7 \rangle$ a $\langle 11 \rangle$.

Snadné pozorování: platí $\langle 1 \rangle = \mathbb{Z}_n^+$. Ovšem v $\mathbb{Z}_n^\times$ platí $\langle 1 \rangle = \{1\}$.

Příklad: Jak nagenerovat $\mathbb{Z}_n^+$?

Poznámka: Viděli jsme, že grupa $\mathbb{Z}_{12}^+$ je rovna $\langle 1 \rangle$, $\langle 5 \rangle$, $\langle 7 \rangle$ a $\langle 11 \rangle$.

Snadné pozorování: platí $\langle 1 \rangle = \mathbb{Z}_n^+$. Ovšem v $\mathbb{Z}_n^\times$ platí $\langle 1 \rangle = \{1\}$.

Věta 31.1

Grupa $\mathbb{Z}_n^+$ je rovna $\langle k \rangle$, $k \in \mathbb{Z}_n^+$, tehdy, a jen tehdy, když k a n jsou nesoudělná čísla.

Příklad: Jak nagenerovat $\mathbb{Z}_n^+$?

Poznámka: Viděli jsme, že grupa $\mathbb{Z}_{12}^+$ je rovna $\langle 1 \rangle$, $\langle 5 \rangle$, $\langle 7 \rangle$ a $\langle 11 \rangle$.

Snadné pozorování: platí $\langle 1 \rangle = \mathbb{Z}_n^+$. Ovšem v $\mathbb{Z}_n^\times$ platí $\langle 1 \rangle = \{1\}$.

Věta 31.1

Grupa $\mathbb{Z}_n^+$ je rovna $\langle k \rangle$, $k \in \mathbb{Z}_n^+$, tehdy, a jen tehdy, když k a n jsou nesoudělná čísla.

Tato věta bude důsledkem obecné věty, kterou si dokážeme později, a faktu, že $\langle 1 \rangle = \mathbb{Z}_n^+$ pro všechna $n \geq 2$.

Příklad: Jak nagenerovat $\mathbb{Z}_n^\times$?

Příklad 31.2
V grupě $\mathbb{Z}_{11}^\times$ platí

$$2^1 = 2 \qquad 2^3 = 8 \qquad 2^5 = 10 \qquad 2^7 = 7 \qquad 2^9 = 6$$
$$2^2 = 4 \qquad 2^4 = 5 \qquad 2^6 = 9 \qquad 2^8 = 3 \qquad 2^{10} = 1$$

a proto $\langle 2 \rangle = \mathbb{Z}_{11}^\times$, tj. 2 je její generátor.

Příklad: Jak nagenerovat $\mathbb{Z}_n^\times$?

Příklad 31.2
V grupě $\mathbb{Z}_{11}^\times$ platí

$$2^1 = 2 \qquad 2^3 = 8 \qquad 2^5 = 10 \qquad 2^7 = 7 \qquad 2^9 = 6$$
$$2^2 = 4 \qquad 2^4 = 5 \qquad 2^6 = 9 \qquad 2^8 = 3 \qquad 2^{10} = 1$$

a proto $\langle 2 \rangle = \mathbb{Z}_{11}^\times$, tj. 2 je její generátor.

Příklad 31.3
V grupě $\mathbb{Z}_8^\times$ (její nosič je $\{1, 3, 5, 7\}$) platí

$$3^2 = 1 \qquad 5^2 = 1 \qquad 7^2 = 1$$

a proto tato grupa nemá jednoprvkovou generující množinu, nemá generátor.

Na druhou stranu ale platí $\langle \{3, 5\} \rangle = \mathbb{Z}_8^\times$. Což je pořád lepší než takřka triviální $\langle \{3, 5, 7\} \rangle = \mathbb{Z}_8^\times$.

Příklad: Jak nagenerovat $\mathbb{Z}_n^\times$?

Příklad 31.2
V grupě $\mathbb{Z}_{11}^\times$ platí

$$2^1 = 2 \qquad 2^3 = 8 \qquad 2^5 = 10 \qquad 2^7 = 7 \qquad 2^9 = 6$$
$$2^2 = 4 \qquad 2^4 = 5 \qquad 2^6 = 9 \qquad 2^8 = 3 \qquad 2^{10} = 1$$

a proto $\langle 2 \rangle = \mathbb{Z}_{11}^\times$, tj. 2 je její generátor.

Příklad 31.3
V grupě $\mathbb{Z}_8^\times$ (její nosič je $\{1, 3, 5, 7\}$) platí

$$3^2 = 1 \qquad 5^2 = 1 \qquad 7^2 = 1$$

a proto tato grupa nemá jednoprvkovou generující množinu, nemá generátor.

Na druhou stranu ale platí $\langle \{3, 5\} \rangle = \mathbb{Z}_8^\times$. Což je pořád lepší než takřka triviální $\langle \{3, 5, 7\} \rangle = \mathbb{Z}_8^\times$.

K problému existence generátorů grup $\mathbb{Z}_n^\times$ se vrátíme později v přednášce.

Definice cyklické grupy

Ne každá grupa má jednoprvkovou generující množinou (generátor). Dává proto smysl zavést následující pojem, jehož název, jak uvidíme později, odkazuje na strukturu takovýchto grup.

Definice 31.4 (Cyklická grupa (*cyclic group*))

Grupa $G = (M, \circ)$ se nazývá cyklická, pokud existuje prvek $a \in M$ takový, že $\langle a \rangle = G$. Tomuto prvku se říká generátor cyklické grupy G.

Definice cyklické grupy

Ne každá grupa má jednoprvkovou generující množinou (generátor). Dává proto smysl zavést následující pojem, jehož název, jak uvidíme později, odkazuje na strukturu takovýchto grup.

Definice 31.4 (Cyklická grupa (*cyclic group*))

Grupa $G = (M, \circ)$ se nazývá cyklická, pokud existuje prvek $a \in M$ takový, že $\langle a \rangle = G$. Tomuto prvku se říká generátor cyklické grupy G.

Na předchozích příkladech jsme si ukázali:

- $\mathbb{Z}_n^+$ jsou cyklické grupy pro všechna n a generátorem jsou všechna kladná $k \leq n$ nesoudělná s n. Speciálně, číslo 1 je generátor každé $\mathbb{Z}_n^+$.

Definice cyklické grupy

Ne každá grupa má jednoprvkovou generující množinou (generátor). Dává proto smysl zavést následující pojem, jehož název, jak uvidíme později, odkazuje na strukturu takovýchto grup.

Definice 31.4 (Cyklická grupa (*cyclic group*))

Grupa $G = (M, \circ)$ se nazývá cyklická, pokud existuje prvek $a \in M$ takový, že $\langle a \rangle = G$. Tomuto prvku se říká generátor cyklické grupy G.

Na předchozích příkladech jsme si ukázali:

- $\mathbb{Z}_n^+$ jsou cyklické grupy pro všechna n a generátorem jsou všechna kladná $k \leq n$ nesoudělná s n. Speciálně, číslo 1 je generátor každé $\mathbb{Z}_n^+$.
- Co grupa $(\mathbb{Z}, +)$?

Definice cyklické grupy

Ne každá grupa má jednoprvkovou generující množinou (generátor). Dává proto smysl zavést následující pojem, jehož název, jak uvidíme později, odkazuje na strukturu takovýchto grup.

Definice 31.4 (Cyklická grupa (*cyclic group*))

Grupa $G = (M, \circ)$ se nazývá cyklická, pokud existuje prvek $a \in M$ takový, že $\langle a \rangle = G$. Tomuto prvku se říká generátor cyklické grupy G.

Na předchozích příkladech jsme si ukázali:

- $\mathbb{Z}_n^+$ jsou cyklické grupy pro všechna n a generátorem jsou všechna kladná $k \leq n$ nesoudělná s n. Speciálně, číslo 1 je generátor každé $\mathbb{Z}_n^+$.
- Co grupa $(\mathbb{Z}, +)$?

Definice cyklické grupy

Ne každá grupa má jednoprvkovou generující množinou (generátor). Dává proto smysl zavést následující pojem, jehož název, jak uvidíme později, odkazuje na strukturu takovýchto grup.

Definice 31.4 (Cyklická grupa (*cyclic group*))

Grupa $G = (M, \circ)$ se nazývá cyklická, pokud existuje prvek $a \in M$ takový, že $\langle a \rangle = G$. Tomuto prvku se říká generátor cyklické grupy G.

Na předchozích příkladech jsme si ukázali:

- $\mathbb{Z}_n^+$ jsou cyklické grupy pro všechna n a generátorem jsou všechna kladná $k \leq n$ nesoudělná s n. Speciálně, číslo 1 je generátor každé $\mathbb{Z}_n^+$.
- Co grupa $(\mathbb{Z}, +)$?
- $\mathbb{Z}_{11}^\times$ je také cyklická, s generátorem 2. $\mathbb{Z}_8^\times$ není cyklická.

Řád prvku

Definice 31.5

Buď g prvek grupy G. Pokud existuje kladné celé číslo m splňující $g^m = e$, pak nejmenší m s touto vlastností nazýváme řádem prvku g. Pokud takové m neexistuje, pak řekneme, že řád prvku g je nekonečno. Řád prvku g značíme $\mathrm{ord}(g)$.

Řád prvku

Definice 31.5

Buď g prvek grupy G. Pokud existuje kladné celé číslo m splňující $g^m = e$, pak nejmenší m s touto vlastností nazýváme řádem prvku g. Pokud takové m neexistuje, pak řekneme, že řád prvku g je nekonečno. Řád prvku g značíme $\mathrm{ord}(g)$.

Poznámka: Řád prvku g je roven řádu grupy $\langle g \rangle$, platí tedy rovnost

$$\mathrm{ord}(g) = \#\langle g \rangle.$$

Řád prvku

Definice 31.5

Buď g prvek grupy G. Pokud existuje kladné celé číslo m splňující $g^m = e$, pak nejmenší m s touto vlastností nazýváme řádem prvku g. Pokud takové m neexistuje, pak řekneme, že řád prvku g je nekonečno. Řád prvku g značíme $\mathrm{ord}(g)$.

Poznámka: Řád prvku g je roven řádu grupy $\langle g \rangle$, platí tedy rovnost

$$\mathrm{ord}(g) = \#\langle g \rangle.$$

Dále platí: nechť $k \in \mathbb{Z}$, pak $g^k = e \iff k = \ell \cdot \mathrm{ord}(g)$ pro nějaké celé ℓ.

Kdy je $\mathbb{Z}_n^\times$ cyklická?

Věta 31.6

$\mathbb{Z}_n^\times$ je cyklická, právě když n je 2, 4, p^k, nebo $2p^k$, kde p je liché prvočíslo a k je kladné celé číslo.

Kdy je $\mathbb{Z}_n^\times$ cyklická?

Věta 31.6

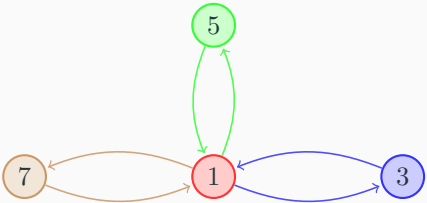
$\mathbb{Z}_n^\times$ je cyklická, právě když n je 2, 4, p^k, nebo $2p^k$, kde p je liché prvočíslo a k je kladné celé číslo.

Kdy je $\mathbb{Z}_n^\times$ cyklická?

Věta 31.6

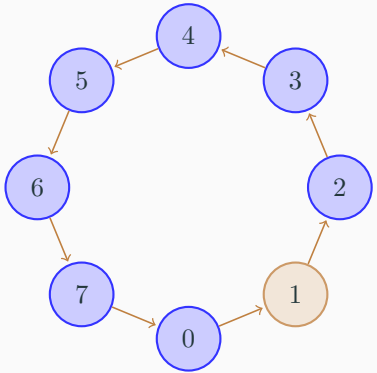
$\mathbb{Z}_n^\times$ je cyklická, právě když n je 2, 4, p^k, nebo $2p^k$, kde p je liché prvočíslo a k je kladné celé číslo.

Například $\mathbb{Z}_8^\times$ není cyklická, jak je pěkně vidět z jejího Cayleyho grafu (barva hrany udává jakým prvkem se násobí a odpovídá barvě vrcholů).



Proč „cyklická“?

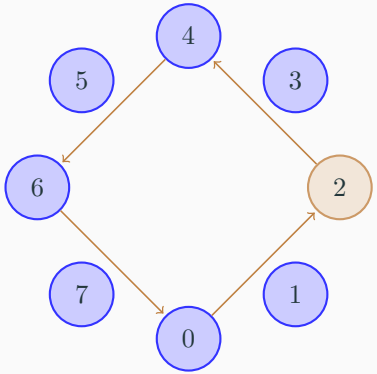
Uvažujme aditivní grupu $\mathbb{Z}_8^+$.



$\langle 1 \rangle = \mathbb{Z}_8^+$, 1 je generátor $\mathbb{Z}_8^+$.

Proč „cyklická“?

Uvažujme aditivní grupu $\mathbb{Z}_8^+$.

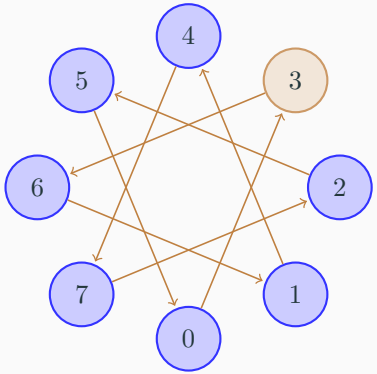


$\langle 1 \rangle = \mathbb{Z}_8^+$, 1 je generátor $\mathbb{Z}_8^+$.

$\langle 2 \rangle = \{0, 2, 4, 6\}$, 2 není generátor $\mathbb{Z}_8^+$.

Proč „cyklická“?

Uvažujme aditivní grupu $\mathbb{Z}_8^+$.



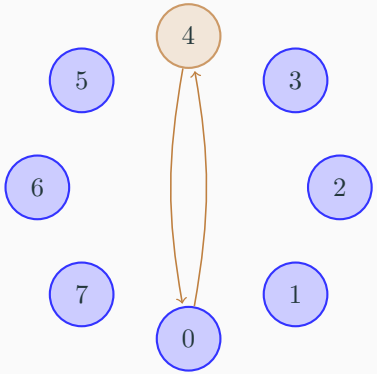
$\langle 1 \rangle = \mathbb{Z}_8^+$, 1 je generátor $\mathbb{Z}_8^+$.

$\langle 2 \rangle = \{0, 2, 4, 6\}$, 2 není generátor $\mathbb{Z}_8^+$.

$\langle 3 \rangle = \mathbb{Z}_8^+$, 3 je generátor $\mathbb{Z}_8^+$.

Proč „cyklická“?

Uvažujme aditivní grupu $\mathbb{Z}_8^+$.



$\langle 1 \rangle = \mathbb{Z}_8^+$, 1 je generátor $\mathbb{Z}_8^+$.

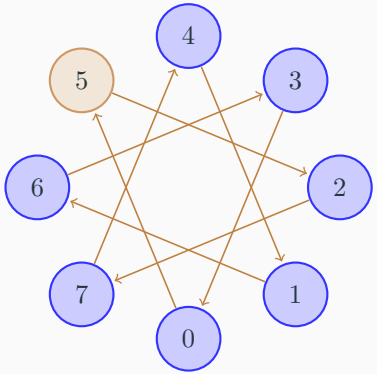
$\langle 2 \rangle = \{0, 2, 4, 6\}$, 2 není generátor $\mathbb{Z}_8^+$.

$\langle 3 \rangle = \mathbb{Z}_8^+$, 3 je generátor $\mathbb{Z}_8^+$.

$\langle 4 \rangle = \{0, 4\}$, 4 není generátor $\mathbb{Z}_8^+$.

Proč „cyklická“?

Uvažujme aditivní grupu $\mathbb{Z}_8^+$.



$\langle 1 \rangle = \mathbb{Z}_8^+$, 1 je generátor $\mathbb{Z}_8^+$.

$\langle 2 \rangle = \{0, 2, 4, 6\}$, 2 není generátor $\mathbb{Z}_8^+$.

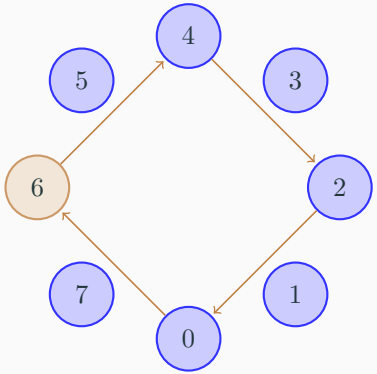
$\langle 3 \rangle = \mathbb{Z}_8^+$, 3 je generátor $\mathbb{Z}_8^+$.

$\langle 4 \rangle = \{0, 4\}$, 4 není generátor $\mathbb{Z}_8^+$.

$\langle 5 \rangle = \mathbb{Z}_8^+$, 5 je generátor $\mathbb{Z}_8^+$.

Proč „cyklická“?

Uvažujme aditivní grupu $\mathbb{Z}_8^+$.



$\langle 1 \rangle = \mathbb{Z}_8^+$, 1 je generátor $\mathbb{Z}_8^+$.

$\langle 2 \rangle = \{0, 2, 4, 6\}$, 2 není generátor $\mathbb{Z}_8^+$.

$\langle 3 \rangle = \mathbb{Z}_8^+$, 3 je generátor $\mathbb{Z}_8^+$.

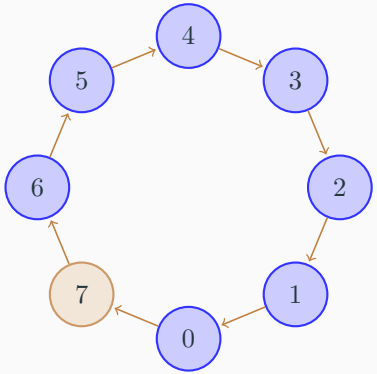
$\langle 4 \rangle = \{0, 4\}$, 4 není generátor $\mathbb{Z}_8^+$.

$\langle 5 \rangle = \mathbb{Z}_8^+$, 5 je generátor $\mathbb{Z}_8^+$.

$\langle 6 \rangle = \{0, 2, 4, 6\}$, 6 není generátor $\mathbb{Z}_8^+$.

Proč „cyklická“?

Uvažujme aditivní grupu $\mathbb{Z}_8^+$.



$\langle 1 \rangle = \mathbb{Z}_8^+$, 1 je generátor $\mathbb{Z}_8^+$.

$\langle 2 \rangle = \{0, 2, 4, 6\}$, 2 není generátor $\mathbb{Z}_8^+$.

$\langle 3 \rangle = \mathbb{Z}_8^+$, 3 je generátor $\mathbb{Z}_8^+$.

$\langle 4 \rangle = \{0, 4\}$, 4 není generátor $\mathbb{Z}_8^+$.

$\langle 5 \rangle = \mathbb{Z}_8^+$, 5 je generátor $\mathbb{Z}_8^+$.

$\langle 6 \rangle = \{0, 2, 4, 6\}$, 6 není generátor $\mathbb{Z}_8^+$.

$\langle 7 \rangle = \mathbb{Z}_8^+$, 7 je generátor $\mathbb{Z}_8^+$.

Jak najít všechny generátory (1 ze 3)

Obecně najít generátory není úplně jednoduchý úkol (např. v grupách $\mathbb{Z}_p^\times$ to moc neumíme), ale pokud už jeden najdeme, je snadné najít i ty ostatní.

Věta 31.7

Je-li $(G, \circ)$ cyklická grupa řádu n a a nějaký její generátor, potom a^k je také generátor tehdy, a jen tehdy, když k a n jsou nesoudělná (tj. $\gcd(k, n) = 1$).

Jak najít všechny generátory (1 ze 3)

Obecně najít generátory není úplně jednoduchý úkol (např. v grupách $\mathbb{Z}_p^\times$ to moc neumíme), ale pokud už jeden najdeme, je snadné najít i ty ostatní.

Věta 31.7

Je-li $(G, \circ)$ cyklická grupa řádu n a a nějaký její generátor, potom a^k je také generátor tehdy, a jen tehdy, když k a n jsou nesoudělná (tj. $\gcd(k, n) = 1$).

Důkaz.

($\Rightarrow$) Jelikož $\langle a^k \rangle = G$, pak existuje $u \in Z$ tak, že $(a^k)^u = a$. Tedy $a^{uk-1} = e$. Prvek a je generátor G, tedy existuje $v \in \mathbb{Z}$ tak, že $uk - 1 = v \cdot \mathrm{ord}(g)$. Protože $\mathrm{ord}(g) = n$, dostaneme $1 = uk - vn$ a to již implikuje nesoudělnost, neboť:

Pomocné lemma: Buď $D = \{mk + \ell n \mid m, l \in \mathbb{Z}\}$ a $d = \min\{|x| \mid x \in D \setminus \{0\}\}$, potom $d = \gcd(k, n)$.

Důkaz tohoto lemmatu:

Jak najít všechny generátory (2 ze 3)

Důkaz: pokračování.

- d dělí n: kdyby ne, je $n = jd + r$ pro $0 < r < d$, ale pak $r = n - jd \in D$ je menší než d, spor.
- d dělí k: stejně
- d' dělí k a n, pak ale dělí i d, neb d je celočíselná lin. kombinace těchto dvou čísel. A tedy $d' \leq d$.

(konec důkazu lemmatu)

($\Leftarrow$): $\gcd(k, n) = 1$ a tedy existují u a v tak, že $un + vk = 1$ a tedy

$$a = a^{un+vk} = a^{un} a^{vk} = a^{u \operatorname{ord}(g)} a^{vk} = a^{vk} = (a^k)^v.$$

Z toho už plyne, že a^k je generátor, neb jím jde vygenerovat jiný generátor.

Vskutku: mějme $b \in G$, hledejme $\ell \in \mathbb{Z}$ takové, že $(a^k)^\ell = b$. Protože $\langle a \rangle = G$, existuje $t \in \mathbb{Z}$ takové, že $b = a^t$. Tedy $b = (a^t)^{vk} = (a^k)^{vt}$ a tedy $\ell = vt$. □

Jak najít všechny generátory (3 ze 3)

Důsledek 31.8

V cyklické grupě řádu n je počet generátorů roven $\varphi(n)$.

- φ je Eulerova funkce, která každému kladnému celému číslu n přiřazuje počet kladných celých čísel menších než n, která jsou s ním nesoudělná,

Jak najít všechny generátory (3 ze 3)

Důsledek 31.8

V cyklické grupě řádu n je počet generátorů roven $\varphi(n)$.

- φ je Eulerova funkce, která každému kladnému celému číslu n přiřazuje počet kladných celých čísel menších než n, která jsou s ním nesoudělná,

- Pro prvočíslo p je $\mathbb{Z}_p^\times$ cyklická grupa řádu $p-1$ a má tedy $\varphi(p-1)$ generátorů.

Jak najít všechny generátory (3 ze 3)

Důsledek 31.8

V cyklické grupě řádu n je počet generátorů roven $\varphi(n)$.

- φ je Eulerova funkce, která každému kladnému celému číslu n přiřazuje počet kladných celých čísel menších než n, která jsou s ním nesoudělná,
- Pro prvočíslo p je $\mathbb{Z}_p^\times$ cyklická grupa řádu $p-1$ a má tedy $\varphi(p-1)$ generátorů.
- Není znám efektivní algoritmus pro výpočet $\varphi(n)$.

Podgrupy cyklické grupy jsou cyklické

Věta 31.9

Libovolná podgrupa cyklické grupy je opět cyklická grupa.

Podgrupy cyklické grupy jsou cyklické

Věta 31.9

Libovolná podgrupa cyklické grupy je opět cyklická grupa.

Důkaz.

- Buď $G = \langle a \rangle$ cyklická grupa a H její vlastní podgrupa. Buď q nejmenší kladné celé číslo takové, že $a^q \in H$. Ukážeme, že $H = \langle a^q \rangle$ a tím bude důkaz hotov.

Podgrupy cyklické grupy jsou cyklické

Věta 31.9

Libovolná podgrupa cyklické grupy je opět cyklická grupa.

Důkaz.

- Buď $G = \langle a \rangle$ cyklická grupa a H její vlastní podgrupa. Buď q nejmenší kladné celé číslo takové, že $a^q \in H$. Ukážeme, že $H = \langle a^q \rangle$ a tím bude důkaz hotov.
- Jistě platí, že $\langle a^q \rangle \subseteq H$. Dokážeme-li, že platí $H \subseteq \langle a^q \rangle$, pak se musejí tyto množiny rovnat.

Podgrupy cyklické grupy jsou cyklické

Věta 31.9

Libovolná podgrupa cyklické grupy je opět cyklická grupa.

Důkaz.

- Buď $G = \langle a \rangle$ cyklická grupa a H její vlastní podgrupa. Buď q nejmenší kladné celé číslo takové, že $a^q \in H$. Ukážeme, že $H = \langle a^q \rangle$ a tím bude důkaz hotov.
- Jistě platí, že $\langle a^q \rangle \subseteq H$. Dokážeme-li, že platí $H \subseteq \langle a^q \rangle$, pak se musejí tyto množiny rovnat.
- Buď x nějaký prvek H a p takové, že $x = a^p$. Existují celá čísla u, v tak, že $d = \gcd(q, p) = uq + vp$. Potom $a^d = (a^q)^u \circ (a^p)^v \in H$ a tedy $d \geq q$, Současně $\gcd(q, p) = d \leq q$, proto $d = q$ a existuje k tak, že $p = kq$. Odtud konečně dostáváme $x = a^p = (a^q)^k \in \langle a^q \rangle$ a důkaz je hotov. □

28. Podgrupy

29. Řád grupy a Lagrangeova věta

30. Generující množiny a generátory grup

31. Cyklické grupy

32. (Malá) Fermatova věta

Malá Fermatova věta (1 ze 2)

Důsledkem Lagrangeovy věty je:

Věta 32.1

V grupě $G = (M, \circ)$ řádu n platí pro všechny prvky $a \in M$, že

$$a^n = e, \qquad \text{kde } e \text{ je neutrální prvek.}$$

Důkaz.

- Cyklická grupa $\langle a \rangle$ je podgrupou grupy G.
- Dle Lagrangeovy věty tedy platí, že $\#\langle a \rangle$ dělí n, tzn. že existuje $k \in \mathbb{N}$ takové, že $n = k \cdot \#\langle a \rangle$.

Malá Fermatova věta (1 ze 2)

Důsledkem Lagrangeovy věty je:

Věta 32.1

V grupě $G = (M, \circ)$ řádu n platí pro všechny prvky $a \in M$, že

$$a^n = e, \qquad \text{kde } e \text{ je neutrální prvek.}$$

Důkaz.

- Cyklická grupa $\langle a \rangle$ je podgrupou grupy G.
- Dle Lagrangeovy věty tedy platí, že $\#\langle a \rangle$ dělí n, tzn. že existuje $k \in \mathbb{N}$ takové, že $n = k \cdot \#\langle a \rangle$.
- Máme tedy $a^n = a^{k \cdot \#\langle a \rangle} = (a^{\#\langle a \rangle})^k = (a^{\operatorname{ord} a})^k = e^k = e$. □

Malá Fermatova věta (2 ze 2)

- Grupa $\mathbb{Z}_p^\times$ má řád $p-1$.

Malá Fermatova věta (2 ze 2)

- Grupa $\mathbb{Z}_p^\times$ má řád $p-1$.

- Aplikováním předchozí věty na tuto grupu získáme malou Fermatovu větu.

Malá Fermatova věta (2 ze 2)

- Grupa $\mathbb{Z}_p^\times$ má řád $p-1$.

- Aplikováním předchozí věty na tuto grupu získáme malou Fermatovu větu.

Důsledek 32.2 (Malá Fermatova věta)

Pro libovolné prvočíslo p a libovolné $1 \leq a < p$ platí

$$a^{p-1} \equiv 1 \pmod{p}.$$

Základní cvičení 18.2

(a) Je 5 generátor grupy $\mathbb{Z}_{23}^{\times}$? (Pokuste se toto ověřit či vyvrátit bez nutnosti výčtu množiny generované prvkem 5.)

(b) Je 2 generátor grupy $\mathbb{Z}_{23}^{\times}$?

(c) Nalezněte všechny generátory grupy $\mathbb{Z}_{23}^{\times}$.

Základní cvičení 18.3

Ukažte že množina $H = \{a^{11} : a \in \mathbb{Z}_{23}^{\times}\}$ je podgrupa grupy $\mathbb{Z}_{23}^{\times}$ a zjistěte její řád.