

Cyklické grupy

Připomeňme značení zavedené dříve. Jestliže $(G, \cdot)$ je grupa, $a \in G$, pak:

$\forall n \in \mathbb{N}$:

$$a^n = a \cdot a \cdot \dots \cdot a \quad (n\text{-krát})$$

$$a^{-n} = a^{-1} \cdot a^{-1} \cdot \dots \cdot a^{-1} \quad (n\text{-krát a platí } (a^{-1})^n = a^{-n})$$

navíc $a^0 = e \dots$ neutrální prvek grupy $(G, \cdot)$

Dále připomeňme (viz přednáška „Lagrangeova věta“), že řádem prvku $a \in G$ nazýváme nejmenší $n \in \mathbb{N}$ takové, že:

$$a^n = e.$$

Pokud takové přirozené číslo n neexistuje, říkáme, že a je nekonečného řádu. Značíme $|a| = n$ (případně $|a| = \infty$).

Def. (Cyklická grupa): Grupa $(G, \cdot)$ je cyklická grupa právě tehdy, když existuje $a \in G$ takové, že:

$$G = \{ a^n \mid n \in \mathbb{Z} \}$$

Prvek a nazýváme generátorem grupy $(G, \cdot)$ a značíme $G = \langle a \rangle$. (Tj. $(\langle a \rangle, \cdot)$ je grupa generovaná prvkem a .)

Příklad 1. Uvažujme grupu $(G, \cdot)$, kde $G = \{1, 2, 3, 4\}$ a $\cdot$ je násobení modulo 5.

I.) $a = 3$ $\Rightarrow a^1 = 3, a^2 = 4, a^3 = 2, a^4 = 1, a^5 = 3, \dots$

$\Rightarrow G = \{a^n \mid n \in \{1, 2, 3, 4\}\} = \{a^n \mid n \in \mathbb{N}\} \stackrel{\uparrow}{=} \{a^n \mid n \in \mathbb{Z}\}$

jak to?
kde je prvek $\bar{a}^3$?!
 $\bar{a}^5$?!
 $\vdots$

Vidíme, že prvek $a=3$ je řádu 4, to jest, $a^4 = 1 = e \Rightarrow a \cdot a^3 = 1 \Rightarrow \bar{a}^1 = a^3 \Rightarrow$

$$\begin{aligned} a^0 &= a^4 = 1 \\ \bar{a}^1 &= a^3 = 2 \\ \bar{a}^2 &= (a^3)^2 = 4 \\ \bar{a}^3 &= (a^3)^3 = 3 \\ \bar{a}^4 &= (a^3)^4 = 1 \\ &\vdots \end{aligned}$$

$\Rightarrow$ opravdu $G = \{3^n \mid n \in \mathbb{Z}\} \Rightarrow G = \langle 3 \rangle \Rightarrow$

$(G, \cdot)$ je cyklická grupa a jejím generátorem je $a=3$

II.) Z Lagrangeovy věty plyne, že řád prvku dělí řád grupy (neboť mocninou prvku a , tj. $H = \{a^n \mid n \in \mathbb{N}\}$ tvoří podgrupu v $(G, \cdot)$).

a	a^1	a^2	a^3	a^4
1	1	1	1	1
2	2	4	3	1
3	3	4	2	1
4	4	1	4	1

$\Rightarrow a=1$ generuje (cyklickou) podgrupu $\langle 1 \rangle, \cdot$ řádu 1. ($\langle 1 \rangle = \{1\}$)

$\Rightarrow a=2$ generuje cyklickou grupu $\langle 2 \rangle, \cdot = (G, \cdot)$.

$\Rightarrow a=3$ generuje cyklickou grupu $\langle 3 \rangle, \cdot = (G, \cdot)$.

$\Rightarrow a=4$ generuje (cyklickou) podgrupu $\langle 4 \rangle, \cdot = \{1, 4\}, \cdot$

Poznámka: Z Příkladu 1 je zřejmé, že každý prvek $a \in G$ grupy $(G, \cdot)$ je generátorem nějaké grupy - je to nějaká podgrupa grupy $(G, \cdot)$. Jestliže $\exists a \in G$: řád prvku $a = |a| = |G| \in \mathbb{N}$, pak $(G, \cdot)$ je cyklická grupa (později uvidíme, že toto je splněno i pro $|a| = \infty$).

Příklad 2: Ukážeme příklady cyklických grup v "aditivní notaci."
Pokud místo symbolu $\cdot$ používáme $+$, pak místo a^n značíme $n \cdot a$. Tj. $na = a + a + \dots + a$ (n -krát)

I.) Příkladem nekonečné cyklické grupy je $(\mathbb{Z}, +)$, neboť jejím generátorem je číslo 1 (a to je nekonečného řádu):

$$\mathbb{Z} = \{ n \cdot 1 \mid n \in \mathbb{Z} \} \quad \text{a} \quad \forall n \in \mathbb{N}: n \cdot 1 \neq 0 = e \Rightarrow |1| = \infty.$$

II.) Příkladem konečné cyklické grupy řádu n je $(\mathbb{Z}_n, +)$, kde $+$ je sčítání modulo n . Generátorem je $\bar{1} \in \mathbb{Z}_n$:

$$\mathbb{Z}_n = \{ \bar{1}, \bar{2}, \dots, \bar{n} = \bar{0} \} = \{ n \cdot \bar{1} \mid n \in \mathbb{Z} \}, \text{ řádem } \bar{1} \text{ je } n \text{ (} n \cdot \bar{1} = \bar{n} = \bar{0} \text{)}$$

III.) Srovnáme $(\mathbb{Z}_5 = \{0\}, \cdot)$ (tj. cyklickou grupu z Příkladu 1) s cyklickou grupou $(\mathbb{Z}_4, +)$:

↙ násobení modulo 5

$\cdot$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

zobrazení f :

$$2^0 = 1 \rightarrow 0$$

$$2^1 = 2 \rightarrow 1$$

$$2^2 = 4 \rightarrow 2$$

$$2^3 = 3 \rightarrow 3$$

je izomorfismus

$$f(a^k) = \bar{k}$$

↙ sčítání modulo 4

$+$	0	1	3	2
0	0	1	3	2
1	1	2	0	3
3	3	0	2	1
2	2	3	1	0

Pozn.: Dále ukážeme, že až na izomorfismus jiné cyklické grupy než $(\mathbb{Z}, +)$ a $(\mathbb{Z}_n, +)$ neexistují.

Věta: Necht' $(G_1, \cdot)$ je grupa a $g \in G_1$ je prvek řádu $m \in \mathbb{N} \cup \{\infty\}$. Jestliže $f: G_1 \rightarrow G_2$ je izomorfismus grup $(G_1, \cdot)$ do grup $(G_2, \cdot)$, pak $f(g)$ je prvek grup $(G_2, \cdot)$ řádu m .

(Tzn. „izomorfismus zachovává řád prvků“)

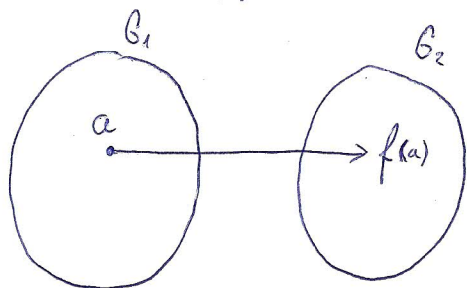
Důkaz: Dříve bylo dokázáno, že v případě, kdy homomorfismus f je bijektivní, platí $\text{Ker } f = \{e_{G_1}\}$. Odtud

$$f(g^k) = (f(g))^k = e_{G_2} \iff g^k = e_{G_1}$$

To znamená, že nejmenší přirozené číslo k pro které $(f(g))^k = e_{G_2}$ je stejné jako nejmenší přirozené číslo pro které $g^k = e_{G_1}$.

Věta: Izomorfní obrazy cyklické grupy je cyklická grupa stejného řádu.

Důkaz: Předpokládejme, že $(G_1, \cdot)$ je cyklická grupa řádu $m \in \mathbb{N} \cup \{\infty\}$ generovaná prvkem $a \in G_1$ a $f: G_1 \rightarrow G_2$ je izomorfismus grup $(G_1, \cdot)$ do $(G_2, \cdot)$.



$$(f \text{ je homomorfismus} \Rightarrow f(a^k) = (f(a))^k)$$

f je surjektivní $\Rightarrow$

$$G_2 = f(G_1) = \{f(a^k) \mid k \in \mathbb{Z}\} = \{(f(a))^k \mid k \in \mathbb{Z}\} = \langle f(a) \rangle$$

$\Rightarrow f(a)$ je generátorem $G_2 \Rightarrow (G_2, \cdot)$ je cyklická

$f(a)$ je podle předchozího též stejného řádu jako $a \Rightarrow$

G_2 je stejného řádu jako G_1

□

Věta: Grupa $(G, \cdot)$, kde $|G| = \infty$ je cyklická $\Leftrightarrow (G, \cdot) \cong (\mathbb{Z}, +)$

Grupa $(G, \cdot)$, kde $|G| = n$ je cyklická $\Leftrightarrow (G, \cdot) \cong (\mathbb{Z}/n\mathbb{Z}, +)$

Důkaz: Nejprve uvažujme případ $|G| = \infty$.

$\Rightarrow$ Předpokládejme, že $G = \{a^k \mid k \in \mathbb{Z}\}$ a definujme
obrazení $f: G \rightarrow \mathbb{Z}$ předpisem:

$$\forall k \in \mathbb{Z} : f(a^k) = k$$

Dokažeme, že f je izomorfismus.

1.) f je homomorfismus:

$$\forall m, n \in \mathbb{Z} : f(a^m) + f(a^n) = m + n = f(a^{m+n}) = f(a^m \cdot a^n)$$

2.) f je injektivní:

$$f(a^m) = f(a^n) \Rightarrow m = n \Rightarrow a^m = a^n$$

3.) f je surjektivní:

$$\forall y \in \mathbb{Z} : f(a^y) = y$$

$\Leftarrow$ $(\mathbb{Z}, +)$ je cyklická grupa generovaná prvem 1 nekonečného řádu. Izomorfní obraz $(\mathbb{Z}, +)$ je tedy také cyklická grupa nekonečného řádu. (Uvažme, že $f: \mathbb{Z} \rightarrow G$ je izomorfismus).

Uvažujme případ $|G| = n \in \mathbb{N}$

$\Rightarrow$ Předpokládejme, že $G = \{a, a^2, \dots, \underbrace{a^n}_{=e}\}$ a definujme zobrazení $f: G \rightarrow \mathbb{Z}/n\mathbb{Z}$ předpisem:

$$\forall k \in \{1, \dots, n\}: f(a^k) = k + n\mathbb{Z}$$

Dokažeme, že f je izomorfismus.

1.) f je homomorfismus:

$$\begin{aligned} \forall p, q \in \{1, \dots, n\}: f(a^p) + f(a^q) &= (p + n\mathbb{Z}) + (q + n\mathbb{Z}) = (p+q) + n\mathbb{Z} = \\ &= f(a^{p+q}) = f(a^p \cdot a^q) \end{aligned}$$

2.) f je injektivní:

$$\begin{aligned} \forall p, q \in \{1, \dots, n\}: f(a^p) = f(a^q) &\Rightarrow p + n\mathbb{Z} = q + n\mathbb{Z} \Rightarrow (-q + p) + n\mathbb{Z} = n\mathbb{Z} \\ &\Rightarrow -q + p \in n\mathbb{Z} \Rightarrow p - q = k \cdot n, \text{ kde } k \in \mathbb{Z} \\ &\Rightarrow a^{p-q} = a^{k \cdot n} = e \quad \text{ / } a^q \\ &a^p = a^q \quad \text{ protože } a^n = e \end{aligned}$$

3.) f je surjektivní:

$$\mathbb{Z}/n\mathbb{Z} = \{ \cancel{a}^k + n\mathbb{Z} \mid k \in \{1, \dots, n\} \} \Rightarrow$$

$$\forall \cancel{a}^k + n\mathbb{Z} : f(a^k) = k + n\mathbb{Z}$$

$\square$ $(\mathbb{Z}/n\mathbb{Z}, +)$ je cyklická grupa řádu n generovaná prvkem $1 + n\mathbb{Z}$. Proto její izomorfní obraz je také cyklická grupa řádu n . (Uvažme, že $f^{-1}: \mathbb{Z}/n\mathbb{Z} \rightarrow G$ je izomorfismus) $\square$