Cyklické grupy

24. februára 2025

Mocnina v grupe

$$x^n = \underbrace{x \circ \ldots \circ x}_{n\text{-krát}}$$

Formálnejšie:

- $x^{n+1} = x^n \circ x$
- $x^0 = e$
- $x^{-n} = (x^{-1})^n$

Mocnina v grupe

Lema

Nech $(G, \circ)$ *je grupa,* $x, y \in G$, $m, n \in \mathbb{Z}$. *Potom platí:*

(i) *Ak* $x \circ y = y \circ x$, *tak* $x \circ y^n = y^n \circ x$.

(ii) *Ak* $x \circ y = y \circ x$, *tak platí aj* $(x \circ y)^n = x^n \circ y^n$.

(iii) $x^{-n} = (x^n)^{-1}$

(iv) $x^{m+n} = x^m \circ x^n = x^n \circ x^m$

(v) $(x^m)^n = x^{mn}$

Rád prvku

Definícia

Nech $(G, \circ)$ je grupa a $x \in G$. *Rád prvku* x v grupe G je najmenšie číslo $n \in \mathbb{N}$ také, že $n > 0$ a

$$x^n = e.$$

Ak také číslo neexistuje, rád prvku x sa definuje ako ∞.

Rád prvku

- Pre homomorfizmus platí: $f(a^n) = f(a)^n$.
- Izomorfizmus zachováva rády prvkov.
- $\mathbb{Z}_2 \times \mathbb{Z}_2$ a $\mathbb{Z}_4$ nie sú izomorfné.

Konečná podgrupa

Tvrdenie

Nech $(G,*)$ je grupa a $H \subseteq G$, $H \neq \emptyset$ je jej <u>konečná</u> podmnožina. Potom H je podgrupa G práve vtedy, keď platí

$$a, b \in H \ \Rightarrow a * b \in H. \tag{1}$$

Cyklické grupy

Definícia

Cyklická grupa je grupa G, ktorá je generovaná nejakým jej prvkom $a \in G$.

Prvok a, ktorý generuje grupu G, nazývame *generátor* grupy G.

Napríklad $\mathbb{Z} = [1] = [-1]$.

Cyklické grupy

Lema

Ak $(G, *)$ je grupa a $a \in G$, tak $H = \{a^n; n \in \mathbb{Z}\}$ je podgrupa grupy G.

Veta

Ak G je cyklická grupa a a je jej generátor, tak

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

t.j. G pozostáva práve z mocnín generátora a.

$$[a] = \{a^n; n \in \mathbb{Z}\}$$

Cyklické grupy

Lema

Ak $a \in G$, kde G je grupa, a rád prvku a je $n \in \mathbb{N}$, tak

$$a^m = a^k \qquad \Leftrightarrow \qquad n \mid m - k.$$

Ak rád prvku a je ∞, tak

$$a^m = a^k \qquad \Leftrightarrow \qquad m = k.$$

Cyklické grupy

Dôsledok

Ak $a \in G$, kde G je grupa, a rád prvku a je $n \in \mathbb{N}$, tak

$$a^m = e \qquad \Leftrightarrow \qquad n \mid m.$$

Ak rád prvku a je ∞, tak

$$a^m = e \qquad \Leftrightarrow \qquad m = 0.$$

Cyklické grupy

Veta

Nech G je cyklická grupa a a je jej generátor. Ak rád prvku a je $n \in \mathbb{N}$, tak $G \cong (\mathbb{Z}_n, \oplus)$. Ak rád prvku a je ∞, tak $G \cong (\mathbb{Z}, +)$. (Teda každá cyklická grupa je izomorfná so $\mathbb{Z}$ alebo so $\mathbb{Z}_n$).

Každá cyklická grupa je izomorfná so $(\mathbb{Z}, +)$ alebo $(\mathbb{Z}_n, \oplus)$.

Cyklické grupy

Každá cyklická grupa je izomorfná so $(\mathbb{Z}, +)$ alebo $(\mathbb{Z}_n, \oplus)$.
Konečný rád: $f : k \mapsto a^k$, $f : \mathbb{Z}_n \to G$

$$a^{k+l} = a^k a^l = a^{k+l} = a^{k \oplus l}$$

Nekonečný rád: $f : \mathbb{Z} \to G$, $f(n) = a^n$

$$f(k+l) = a^{k+l} = a^k a^l = f(k)f(l)$$

Cyklické grupy

Veta
Každá podgrupa cyklickej grupy je cyklická.

Veta
Homomorfný obraz cyklickej grupy je cyklická grupa.

Súčin cyklických grúp

Veta

Grupa $\mathbb{Z}_m \times \mathbb{Z}_n$ *je cyklická práve vtedy, keď* m *a* n *sú nesúdeliteľné, t.j. ich najväčší spoločný deliteľ* $\gcd(m, n) = 1$. *V takomto prípade je prvok* $(1, 1)$ *jej generátorom.*