Pologrupy, monoidy a grupy

Definice

Pologrupa je množina M vybavená binární operací $\cdot\colon M^2 \longrightarrow M$, která je asociativní, tj.

$$a \cdot (b \cdot c) = (a \cdot b) \cdot c$$

pro všechny $a, b, c \in M$. Pokud je operace $\cdot$ splňuje

$$a \cdot b = b \cdot a$$

pro všechny $a, b \in M$, pak M nazýváme komutativní pologrupa.

Definice

(Komutativní) monoid M je (komutativní) pologrupa, kde existuje neutrální prvek $1 \in M$ takový, že

$$1 \cdot x = x = x \cdot 1\,.$$

Příklady

1. Kladná přirozená čísla $\mathbb{N} \setminus \{0\}$ se sčítáním tvoří komutativní pologrupu, protože sčítání je asociativní.
2. Kladná přirozená čísla $\mathbb{N} \setminus \{0\}$ s násobením tvoří komutativní monoid, protože sčítání je asociativní a $1 \cdot x = x = x \cdot 1$.
3. Nechť Σ je abeceda. Pak jazyk Σ^* všech konečných slov nad Σ tvoří pologrupu s operací řetězení slov, tj. $w_1 \cdot w_2 = w_1 w_2$. Pro $\Sigma = \{a, b, c\}$ platí např.

   $$(aab \cdot ba) \cdot bb = aabbabb = aab \cdot (ba \cdot bb)\,.$$

   Není komutativní, protože např.

   $$ab \cdot b = abb \neq bab = b \cdot ab$$

   Pokud do Σ^* přidáme prázdné slovo ε, pak Σ^* tvoří monoid, protože $\varepsilon \cdot w = w = w \cdot \varepsilon$.

Příklad

Mějme neprázdnou množinu M. Pak množina M^M všech funkcí z M do M tvoří monoid s operací skládání funkcí $\circ$. Neutrální prvek je identické zobrazení $id\colon M \longrightarrow M$. Tedy $\circ\colon (M^M)^2 \longrightarrow M^M$, která funkcím $f, g \in M^M$ přiřadí funkci $f \circ g \in M^M$ definovanou:

$$(f \circ g)(x) = f(g(x)), \qquad x \in M.$$

Ověříme neutralitu id:

$$(id \circ f)(x) = id(f(x)) = f(x)$$

$$(f \circ id)(x) = f(id(x)) = f(x)$$

Ověříme asociativitu $\circ$:

$$\begin{aligned}((f \circ g) \circ h)(x) &= (f \circ g)(h(x)) = f(g(h(x))) = \\ &= f((g \circ h)(x)) = (f \circ (g \circ h))(x)\end{aligned}$$

Definice

Grupa G je monoid, kde každý prvek je invertibilní, tj. pro každé $a \in G$ existuje $b \in G$ takové, že $a \cdot b = b \cdot a = 1$.
Pokud je G komutativní, pak G nazýváme Abelovská grupa.

Tvrzení

Nech G je grupa a $a \in G$. Pak prvek $b \in G$, který splňuje $a \cdot b = 1 = b \cdot a$, existuje právě jeden a značí se a^{-1}.

Notace

Značení $(G, \cdot, ^{-1}, 1)$ používá tzv. multiplikativní notaci. Pro $n \in \mathbb{N}$ symbol a^n značí n-násobný součin $a \cdot a \cdots a$.
Pro Abelovské grupy se také používá aditivní notace $(G, +, -, 0)$.
Pak místo a^n používáme $na = a + a + \cdots + a$.

Poznámka

Okruh s jednotkou $(K, +, \cdot, 0, 1)$ je algebra, kde $(K, +, -, 0)$ tvoří Abelovskou grupu, $(K, \cdot, 1)$ je monoid a platí distributivní zákony:

$$a \cdot (b + c) = a \cdot b + a \cdot c\,, \quad (a + b) \cdot c = a \cdot c + b \cdot c\,.$$

Těleso je okruh s jednotkou, kde navíc $(K \setminus \{0\}, \cdot, {}^{-1}, 1)$ tvoří grupu.
Tedy např. $(\mathbb{Z}_m, +, -, 0)$ je Abelovská grupa a $(\mathbb{Z}_m, \cdot, 1)$ je komutativní monoid. Pokud je m prvočíslo, pak $(\mathbb{Z}_m \setminus \{0\}, \cdot, {}^{-1}, 1)$ je Abelovská grupa.

Příklad

Nechť M je n-prvková množina ($n \geq 1$) a S_n je množina všech bijekcí z M do M. Pak S_n tvoří grupu $(S_n, \circ, {}^{-1}, id)$ s operací skládání funkcí $\circ$ a neutrálním prvkem id. Grupa S_n se nazývá grupa permutací.

Definice

Nechť $(G, \cdot, ^{-1}, 1)$ je grupa a $\emptyset \neq S \subseteq G$. Pak S se nazývá podgrupa G, pokud je S uzavřená na $\cdot$ a $^{-1}$, tj. pro všechny $a, b \in S$ platí:

1. $a \cdot b \in S$,
2. $a^{-1} \in S$.

Definice

Nechť S je podgrupa grupy G a $a \in G$. Pak množinu $a \cdot S = \{a \cdot s \mid s \in S\}$ nazýváme levou třídou rozkladu grupy G podle podgrupy S.

Ekvivalence indukovaná podgrupou

Mějme grupu G a její podgrupu S. Definujeme relaci $R_S \subseteq G \times G$ takto:

$$a \; R_S \; b \text{ iff } a^{-1} \cdot b \in S.$$

Lemma

Relace R_S je ekvivalence na G jejíž třídy ekvivalence jsou $[a]_{R_S} = a \cdot S$.

Věta (Lagrange)

Pro podgrupu S konečné grupy G, platí, že $|S|$ dělí $|G|$.

Definice

Říkáme, že dvě grupy G, H jsou izomorfní (značení $G \cong H$), pokud existuje bijekce $f\colon G \longrightarrow H$ taková, že $f(a \cdot b) = f(a) \cdot f(b)$ pro všechny $a, b \in G$.

Definice

Grupa $(G, \cdot, ^{-1}, 1)$ se nazývá cyklická, pokud existuje $g \in G$ takové, že $G = \{g^n \mid n \in \mathbb{N}\}$.
Pokud G je konečná, pak nejmenší $n \in \mathbb{N}$ takové, že $g^n = 1$, se nazývá řád grupy G.

Věta

Konečná cyklická grupa řádu m je izomorfní s grupou $(\mathbb{Z}_m, +, -, 0)$.

Definice

Mějme konečnou grupu G a $g \in G$. Pak $S(g) = \{g^n \in G \mid n \in \mathbb{N}\}$ je cyklická podgrupa G generovaná prvkem g. Řád prvku g se definuje jako řád grupy $S(g)$, tj. $|S(g)|$. Pozn. $|S(g)|$ dělí $|G|$ (Lagrangeova věta).

Cyklické podgrupy $\mathbb{Z}_m$

- Nechť $(\mathbb{Z}_m, +, -, 0)$ je konečná cyklická grupa řádu m a $g \in \mathbb{Z}_m$.
- Řád prvku g je nejmenší $k \in \mathbb{N}$ takové, že $kg = 0$, tj. $kg = \mathrm{lcm}(g, m)$.
- Protože $\mathrm{lcm}(g, m) = gm/\mathrm{gcd}(g, m)$, platí $k = m/\mathrm{gcd}(g, m)$.
- Tedy $S(g) = \mathbb{Z}_m$ iff řád g je m iff $\mathrm{gcd}(g, m) = 1$.
- Existuje tedy $\varphi(m)$ prvků v $\mathbb{Z}_m$, které mají řád m (tzv. primitivní elementy).

Příklad

- Např. v $\mathbb{Z}_{10}$ platí $S(4) = \{4, 8, 2, 6, 0\} \neq \mathbb{Z}_{10}$, tj. řád 4 je 5.
- Naopak $S(7) = \{7, 4, 1, 8, 5, 2, 9, 6, 3, 0\} = \mathbb{Z}_{10}$, tj. řád 7 je 10.
- Existuje $\varphi(10) = 4$ prvků řádu 10, konkrétně $\{1, 3, 7, 9\}$.
- Ostatní prvky mají řád menší. Konkrétně $S(0) = \{0\}$, $S(5) = \{0, 5\}$ a $S(2) = S(4) = S(6) = S(8) = \{0, 2, 4, 6, 8\}$.

Tvrzení

Pro každý dělitel d čísla $m \geq 1$ má grupa $(\mathbb{Z}_m, +, -, 0)$ právě jednu cyklickou podgrupu řádu d.

Důsledek

Pro přirozené číslo $m \geq 1$ platí:

$$m = \sum_{d:d|m} \varphi(d)\,.$$

Definice

Nechť $\mathbb{K}$ je konečné těleso. Pak symbolem $\mathbb{K}^*$ značíme multiplikativní grupu nenulových prvků tělesa $\mathbb{K}$, tj. $\mathbb{K}^* = (\mathbb{K} \setminus \{0\}, \cdot, {}^{-1}, 1)$.

Věta

Grupa $\mathbb{K}^*$ má maximálně jednu cyklickou podgrupu řádu n pro každé $n \geq 1$. Pokud pro dané n tato podgrupa existuje, pak její prvky $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ splňují

$$x^n - 1 = (x-1)(x-\alpha)\cdots(x-\alpha^{n-1}) .$$

Věta

Nechť $\mathbb{K}$ *je konečné těleso o* q *prvcích. Pak*

1. *každý nenulový prvek* $\alpha \in \mathbb{K}$ *splňuje rovnici* $\alpha^{q-1} = 1$,
2. *prvky tělesa* $\mathbb{K}$ *jsou navzájem různé kořeny polynomu* $x^q - x$, *tj.*

$$x^q - x = \prod_{\alpha \in \mathbb{K}} (x - \alpha)\,.$$

Věta

Nechť $\mathbb{K}$ *je konečné těleso o* q *prvcích. Pak* $\mathbb{K}^*$ *je cyklická grupa, tj.* $\mathbb{K} \setminus \{0\} = \{1, \alpha, \alpha^2, \ldots, \alpha^{q-2}\}$, *kde* α *je primitivní prvek grupy* $\mathbb{K}^*$.