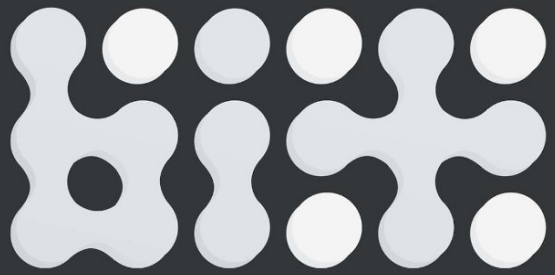

Algebra Komputerowa

Elementy Teorii Grup

Filip Zieliński

2025

Spis Treści

Definicja

Grupa $(G, \cdot)$ jest **grupą cykliczną** wtw. gdy, istnieje taki element $a \in G$, że każdy element grupy G jest jego potęgą, to znaczy

$$\forall g \in G \; \exists k \in \mathbb{Z} : \quad g = a^k.$$

Element a nazywamy wtedy *generatorem grupy cyklicznej*

Uwaga

W konwencji multiplikatywnej mówimy o k-tej *potędze elementu* a i zapisujemy ją jako $a^k = \underbrace{a \cdot a \cdot \ldots \cdot a}_{k}$, natomiast w konwencji addytywnej, mówimy o k-tej *wielokrotności elementu* a i zapisujemy $k \cdot a = \underbrace{a + a + \ldots + a}_{k}$.

Konwencja

Jeśli a jest generatorem grupy G to piszemy $G = \langle a \rangle$.

Przykład

Grupami cyklicznymi są np.

1. $(\sqrt[n]{1}, \cdot)$
2. $(\mathbb{Z}_n, +)$
3. $\mathbb{Z}$

Abelowość grup cyklicznych

Obserwacja

Każda grupa cykliczna jest abelowa.

Dowód.

Rozważmy grupę $\langle a \rangle$. Wystarczy zauważyć, że z łączności wprost wynika $a^p a^q = a^q a^p$. □

Skończone grupy cykliczne

Twierdzenie

Grupa cykliczna $\langle a \rangle$ jest skończona wtedy i tylko wtedy, gdy istnieją liczby całkowite p, q, gdzie $p \neq q$, takie, że $a^p = a^q$.

Skończone grupy cykliczne

Twierdzenie

Grupa cykliczna $\langle a \rangle$ jest skończona wtedy i tylko wtedy, gdy istnieją liczby całkowite p, q, gdzie $p \neq q$, takie, że $a^p = a^q$.

Obserwacja

Grupę cykliczną rzędu n można zapisać w postaci $\{a^0, a^1 \ldots, a^{n-1}\}$, natomiast nieskończoną grupę cykliczną w postaci $\{\ldots, a^{-1}, a^0, a^1, \ldots\}$.

Wniosek

Grupa cykliczna $\langle a \rangle$ jest nieskończona wtedy i tylko wtedy, gdy dla każdego $p \neq q$, $p, q \in \mathbb{Z}$ zachodzi $a^p \neq a^q$.

Izomorfizm grup cyklicznych

KOŁO NAUKOWE

Twierdzenie

Wszystkie grupy cykliczne nieskończonego rzędu są izomorficzne.
Wszystkie grupy cykliczne skończone równych rzędów są izomorficzne.

Podgrupy grup cyklicznych

Twierdzenie

Niech $G = \langle a \rangle$ będzie grupą cykliczną, a H jej podgrupą, $H < G$. Wtedy $H = \{\mathbf{1}\}$, albo H jest grupą cykliczną postaci $\langle a^m \rangle$ dla pewnego $m \in \mathbb{N}$. Dodatkowo:

- Jeżeli G jest grupą nieskończoną, to dla każdego $p, q \in \mathbb{N}$, $p \neq q$ zachodzi $\langle a^p \rangle \neq \langle a^q \rangle$.
- Jeżeli G jest grupą skończoną rzędu n, to każda podgrupa jest postaci $\langle a^m \rangle$ dla pewnego m będącego dzielnikiem n. Wtedy G ma tyle różnych podgrup, ile dzielników naturalnych liczba n. Podgrupa $\langle a^m \rangle$ ma dokłanie $q = \frac{n}{m}$ elementów.

Niech będzie dana grupa G i jej podgrupa H.

Definicja

Warstwą lewostronną elementu $a \in G$ względem podgrupy H nazywamy zbiór $\{ah \mid h \in H\}$ i oznaczamy przez aH.

Definicja

Warstwą prawostronną elementu $a \in G$ względem podgrupy H nazywamy zbiór $\{ha \mid h \in H\}$ i oznaczamy przez Ha.

Obserwacja

Niech $b \in G$. Wtedy

$$b \in aH \Leftrightarrow (\exists h \in H : b = ah) \Leftrightarrow (\exists h \in H : a^{-1}b = h) \Leftrightarrow a^{-1}b \in H.$$

Analogicznie

$$b \in Ha \Leftrightarrow ba^{-1} \in H.$$

Obserwacja

Niech $b \in G$. Wtedy

$$b \in aH \Leftrightarrow (\exists h \in H : b = ah) \Leftrightarrow (\exists h \in H : a^{-1}b = h) \Leftrightarrow a^{-1}b \in H.$$

Analogicznie

$$b \in Ha \Leftrightarrow ba^{-1} \in H.$$

Konwencja

W zapisie addytywnym warstwy oznaczamy przez $a + H$.

Obserwacja

W grupie abelowej G zachodzi

$$\forall a \in G \forall H < G \quad aH = Ha.$$