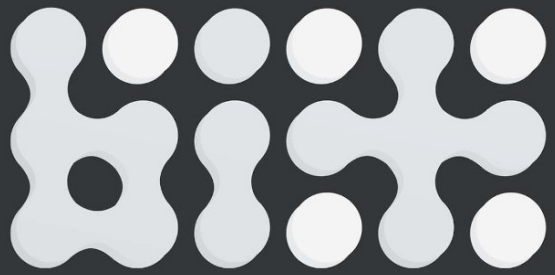

Algebra Komputerowa

Elementy Teorii Grup

Filip Zieliński

2025

Spis Treści

KOŁO NAUKOWE

1. Grupy Cykliczne

2. Warstwy

3. Podgrupy Normalne

4. Jądro Homomorfizmu

Rząd Grupy

Definicja

Niech G będzie grupą. Jeśli G jest grupą skończoną, to rząd G to liczba elementów G. Jeżeli G jest grupą nieskończoną, to mówimy, że rząd grupy G jest nieskończony. Rząd grupy G oznaczamy jako

$$\mathrm{ord}(G)$$

Rząd Grupy

Definicja

Niech G będzie grupą. Jeśli G jest grupą skończoną, to rząd G to liczba elementów G. Jeżeli G jest grupą nieskończoną, to mówimy, że rząd grupy G jest nieskończony. Rząd grupy G oznaczamy jako

$$\mathrm{ord}(G)$$

Uwaga

Przez całą prezentacje w przeważającej większości stosujemy konwencje grupy multiplikatywnej, z tym wyjątkiem, że element neutralny oznaczamy jako e zamiast $\mathbf{1}$.

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

KOŁO NAUKOWE

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

KOŁO NAUKOWE

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

KOŁO NAUKOWE

Twierdzenie

Niech $G = \langle a \rangle$ będzie grupą cykliczną, a H jej podgrupą, $H < G$. Wtedy $H = \{e\}$, 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.

Rząd elementu

Definicja

Jeśli podgrupa $\langle a \rangle$ grupy G jest skończona i ma rząd n, to mówimy, że a jest *elementem rzędu* n. Jeśli $\langle a \rangle$ jest nieskończona to mówimy, że a jest *elementem rzędu nieskończonego*. Rząd elementu a w grupie G oznaczamy jako

$$\mathrm{ord}_G(a)$$

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

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

Równość Warstw

Twierdzenie

Jeśli H jest podgrupą grupy G, to każde dwie warstwy lewostronne (prawostronne) względem H są albo równe albo rozłączne.

Równość Warstw

Twierdzenie

Jeśli H jest podgrupą grupy G, to każde dwie warstwy lewostronne (prawostronne) względem H są albo równe albo rozłączne.

Wniosek

Każdy element grupy G należy do dokładnie jednej warstwy lewostronnej (prawostronnej) względem podgrupy H.

Wniosek

Jeśli H jest podgrupą grupy G to

1. $aH = bH \Leftrightarrow a^{-1}b \in H$
2. $Ha = Hb \Leftrightarrow ba^{-1} \in H$

Twierdzenie

Dowolne dwie lewostronne (prawostronne) warstwy względem tej samej podgrupy są równoliczne.
Dowolna warstwa lewostronna jest równa z dowolną warstwą prawostronną względem tej samej podgrupy.

Twierdzenie

Dowolne dwie lewostronne (prawostronne) warstwy względem tej samej podgrupy są równoliczne.
Dowolna warstwa lewostronna jest równa z dowolną warstwą prawostronną względem tej samej podgrupy.

Dowód.

Dowód dla warstw lewostronnych. Wystarczy pokazać, że $\phi : aH \to bH$ zadane przez $\phi(ah) = bh$ jest bijekcją. Dla drugiego stwierdzenia, wystarczy obserwacja, że $eH = He = H$. □

Twierdzenie

Zbiór odwrotności elementów warstwy lewostronnej aH (prawostronnej Ha) jest warstwą prawostronną Ha^{-1} (lewostronną $a^{-1}H$).

Odwrotności Elementów Warstw

KOŁO NAUKOWE

Twierdzenie

Zbiór odwrotności elementów warstwy lewostronnej aH (prawostronnej Ha) jest warstwą prawostronną Ha^{-1} (lewostronną $a^{-1}H$).

Dowód.

Dowód dla warstw lewostronnych. $b \in aH \Rightarrow b = ah$ dla pewnego $h \in H$. Wtedy $b^{-1} = (ah)^{-1} = h^{-1}a^{-1} \in Ha^{-1}$.
Weźmy $c \in Ha^{-1} \Rightarrow c = h_1a^{-1}$ dla pewnego $h_1 \in H$. Zauważmy, że $c = c_1^{-1}$ dla $c_1 = ah_1^{-1} \in aH$. □

Wniosek

Zbiór wszystkich warstw lewostronnych względem podgrupy H jest równoliczny ze zbiorem wszystkich warstw prawostronnych względem podgrupy H.

Dowód.

Na podstawie poprzedniego twierdzenia, zauważmy, że odwzorowanie prowadzące ze zbioru warstw lewostronnych w zbiór warstw prawostronnych wzgledem tej samej podgrupy H zadane wzorem $\phi(aH) = Ha^{-1}$ jest bijekcją. □

Definicja

Niech G będzie grupą skończoną, a H jej podgrupą. **Indeksem podgrupy H** w grupie G nazywamy liczbę warstw lewostronnych grupy G względem H. Indeks podgrupy H w grupie G oznaczamy przez $[G : H]$

Twierdzenie (Lagrange'a)

Niech G będzie grupą skończoną, a H jej podgrupą. Wtedy

$$\mathrm{ord}(G) = \mathrm{ord}(H)[G : H].$$

Definicja

Niech G będzie grupą skończoną, a H jej podgrupą. **Indeksem podgrupy H** w grupie G nazywamy liczbę warstw lewostronnych grupy G względem H. Indeks podgrupy H w grupie G oznaczamy przez $[G : H]$

Twierdzenie (Lagrange'a)

Niech G będzie grupą skończoną, a H jej podgrupą. Wtedy

$$\mathrm{ord}(G) = \mathrm{ord}(H)[G : H].$$

Dowód.

Wystarczy obserwacja, że każdy element należy do dokładnie jednej warstwy oraz każda warstwa jest równoliczna. □

Wniosek

Rząd elementu grupy skończonej jest dzielnikiem rzędu grupy, to znaczy dla grupy G zachodzi $\mathrm{ord}_G(a) \mid \mathrm{ord}(G) \quad \forall a \in G$.

Wniosek

W grupie skończonej G rzędu n zachodzi $a^n = e$ dla każdego $a \in G$

Dowód.

Niech $\mathrm{ord}_G(a) = m$. Wtedy $n = mq$. Zatem $a^n = (a^m)^q = e^q = e$ □

Twierdzenie

Grupa skończona G, której rząd jest liczbą pierwszą jest grupą cykliczną.

Twierdzenie

Grupa skończona G, której rząd jest liczbą pierwszą jest grupą cykliczną.

Dowód.

$\mathrm{ord}(G) > 1$, zatem istnieje $a \in G$, różny od e. Ponieważ $\mathrm{ord}_G(a) \mid \mathrm{ord}(G)$ oraz jedynym elementem rzędu 1 jest element neutralny, to $\mathrm{ord}_G(a) = \mathrm{ord}(G)$ zatem $\langle a \rangle = G$. □

Twierdzenie

Grupa skończona G, której rząd jest liczbą pierwszą jest grupą cykliczną.

Dowód.

$\mathrm{ord}(G) > 1$, zatem istnieje $a \in G$, różny od e. Ponieważ $\mathrm{ord}_G(a) \mid \mathrm{ord}(G)$ oraz jedynym elementem rzędu 1 jest element neutralny, to $\mathrm{ord}_G(a) = \mathrm{ord}(G)$ zatem $\langle a \rangle = G$. □

Wniosek

Grupa różna od jednoelementowej nie zawiera podgrup właściwych wtedy i tylko wtedy gdy jest skończona i jej rząd jest liczbą pierwszą.

Podgrupa Normalna

KOŁO NAUKOWE

Definicja

Niech G będzie grupą, a H jej podgrupą. Mówimy, że H jest **Podgrupą normalną** G, jeżeli zachodzi $\forall a \in G \quad aH = Ha$ (równośc warstw prawostronnych i lewostronnych).

Konwencja

Jeżeli H jest podgrupą normalną grupy G to zapisujemy $H \trianglelefteq G$.

Konwencja

Funkcjonuje też równoważne określenie jako *Dzielnik Normalny*.

Obserwacja

Każda podgrupa grupy abelowej jest podgrupą normalną.

Obserwacja

Każda podgrupa grupy abelowej jest podgrupą normalną.

Obserwacja

Każda grupa zawiera trywialne podgrupy normalne - samą siebie i podgrupę jednoelementową (element neutralny).

Obserwacja

Każda podgrupa grupy abelowej jest podgrupą normalną.

Obserwacja

Każda grupa zawiera trywialne podgrupy normalne - samą siebie i podgrupę jednoelementową (element neutralny).

Twierdzenie

Rozważmy grupę G i jej podgrupę H. Zdefiniujmy zbiór Gdzie $aHa^{-1} = \{aha^{-1} \mid h \in H\}$. Następujące warunki są równoważne:

1. $\forall a \in G \quad aH = Ha$
2. $\forall a \in G \quad aHa^{-1} = H$
3. $\forall a \in G \quad aHa^{-1} \subseteq H$

Przykład

- Rozważmy grupę $GL_n(R)$ wszystkich nieosobliwych macierzy $n \times n$ oraz jej podgrupę $SL_n(R)$ wszystkich macierzy $n \times n$ o wyznaczniku równym 1. Zachodzi $SL_n(R) \trianglelefteq GL_n(R)$
- Rozważmy grupę n-elementowych permutacji S_n oraz jej podgrupę permutacji parzystych A_n. Zachodzi $A_n \trianglelefteq S_n$.

Przykład

- Rozważmy grupę $GL_n(R)$ wszystkich nieosobliwych macierzy $n \times n$ oraz jej podgrupę $SL_n(R)$ wszystkich macierzy $n \times n$ o wyznaczniku równym 1. Zachodzi $SL_n(R) \trianglelefteq GL_n(R)$
- Rozważmy grupę n-elementowych permutacji S_n oraz jej podgrupę permutacji parzystych A_n. Zachodzi $A_n \trianglelefteq S_n$.

Lemat

Jeżeli liczba warstw lewostronnych (zatem też prawostronnych) względem podgrupy $H < G$ to zachodzi $H \trianglelefteq G$.

Twierdzenie

Niech będzie dany zbiór warstw grupy G względem jej podgrupy normalnej H. Wówczas odwzorowanie określone wzorem

$$aH \circ bH = (ab)H$$

określa poprawne działanie w tym zbiorze. Zbiór warstw z tak okreslonym działaniem jest grupą.

Twierdzenie

Niech będzie dany zbiór warstw grupy G względem jej podgrupy normalnej H. Wówczas odwzorowanie określone wzorem

$$aH \circ bH = (ab)H$$

określa poprawne działanie w tym zbiorze. Zbiór warstw z tak okreslonym działaniem jest grupą.

Definicja

Grupę warstw grupy G względem podgrupy normalnej H zdefiniowanej jak powyżej nazywamy **Grupą ilorazową** grupy G względem podgrupy H lub grupą ilorazową G modulo H i oznaczamy symbolem G/H

Przykład

1. $G/\{1\} \cong G$.
2. $G/G \cong \{1\}$.
3. $\mathbb{Z}/7\mathbb{Z} \cong \mathbb{Z}_7$

Konwencja

Działanie w grupie warstw zazwyczaj oznaczamy tak samo jak działanie w grupie, co nie prowadzi do nieporozumień. Tak więc zwykle piszemy $aH \cdot bH$ w konwencji multiplikatywnej, bądź $(a + H) + (b + H)$ w zapisie addytywnym.

Definicja

Rozważmy grupy G, G' oraz homomorfizm $\phi : G \to G'$. Jądro homomorfizmu ϕ to zbiór

$$\ker \phi = \phi^{-1}(\{e'\}) = \{a \in G \mid \phi(a) = e'\}$$

gdzie e' to element neutralny grupy G'.

Jądro, a podgrupy normalne

Jądro Homomorfizmu

KOŁO NAUKOWE

Twierdzenie

Jeśli $\phi : G \to G'$ jest homomorfizmem grup G, G' to $\ker \phi$ jest podgrupą normalną grupy G.

Twierdzenie

Jeśli $\phi : G \to G'$ jest homomorfizmem grup G, G' to $\ker \phi$ jest podgrupą normalną grupy G.

Dowód.

Dowód faktu, że jądro jest podgrupą był w zestawie zadań. Skorzystajmy z warunku równoważnego definicji podgrupy normalnej. $\ker \phi \trianglelefteq G \Leftrightarrow \forall a \in G \quad a \ker \phi a^{-1} \subseteq \ker \phi$. Weźmy dowolny $k \in \ker \phi$ oraz dowolny $a \in G$. Zachodzi $\phi(aka^{-1}) = \phi(a)\phi(k)\phi(a^{-}1) = \phi(a)e'\phi(a^{-1}) = \phi(aa^{-1}) = \phi(e) = e'$, zatem $\forall a \in g \; \forall k \in \ker \phi \quad aka^{-1} \in \ker \phi \Leftrightarrow \forall a \in G \quad a \ker \phi a^{-1} \subseteq \ker \phi$. □

Twierdzenie

Rozważmy grupę G i jej podgrupę normalną H. Odwzorowanie $\psi : G \to G/H$ zadane wzorem $\psi(a) = aH$ jest homomorfizmem oraz $\ker \psi = H$.

Twierdzenie

Rozważmy grupę G i jej podgrupę normalną H. Odwzorowanie $\psi : G \to G/H$ zadane wzorem $\psi(a) = aH$ jest homomorfizmem oraz $\ker \psi = H$.

Dowód.

Jest to homomorfizm ponieważ $\psi(ab) = (ab)H = aH \cdot bH = \psi(a)\psi(b)$. Elementem neutralnym grupy G/H jest warstwa $eH = H = hH \forall h \in H$. Zatem faktycznie $\ker \psi = \{a \mid \psi(a) = H\} = H$. □

Twierdzenie

Rozważmy grupę G i jej podgrupę normalną H. Odwzorowanie $\psi : G \to G/H$ zadane wzorem $\psi(a) = aH$ jest homomorfizmem oraz $\ker \psi = H$.

Dowód.

Jest to homomorfizm ponieważ $\psi(ab) = (ab)H = aH \cdot bH = \psi(a)\psi(b)$. Elementem neutralnym grupy G/H jest warstwa $eH = H = hH \forall h \in H$. Zatem faktycznie $\ker \psi = \{a \mid \psi(a) = H\} = H$. □

Konwencja

Tak zadany homomorfizm z G do G/H nazywamy *homomorfizmem kanonicznym*.

Pełna charakterystyka jądra

KOŁO NAUKOWE

Wniosek

Każda podgrupa normalna jest jądrem homomorfizmu oraz jądrami homomorfizmów są tylko podgrupy normalne.

Pytania, wątpliwości, uwagi ?