



# **Algebra Komputerowa**

## **Elementy Teorii Grup [1]**

**Filip Zieliński**

2025

1. Grupy Cykliczne
2. Warstwy
3. Podgrupy Normalne
4. Jądro Homomorfizmu
5. Kongruencje w grupach

### 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

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

### 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

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

### Uwaga

Przez całą prezentację w przeważającej większości stosujemy konwencje grupy mnożeniowej, z tym wyjątkiem, że element neutralny oznaczamy jako  $e$  zamiast  $1$ .

### 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

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

Element  $a$  nazywamy wtedy *generatorem grupy cyklicznej*

### Uwaga

W konwencji multiplikatywnej mówimy o  $k$ -tej potędze elementu  $a$  i zapisujemy ją jako  $a^k = \underbrace{a \cdot a \cdot \dots \cdot a}_k$ , natomiast w konwencji

addytywnej, mówimy o  $k$ -tej wielokrotności elementu  $a$  i zapisujemy  $k \cdot a = \underbrace{a + a + \dots + a}_k$ .

## 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.  $\mathbb{Z}$

## Obserwacja

Każda grupa cykliczna jest abelowa.

## Dowód.

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

### Twierdzenie

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



## 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  $\{a^0, a^1, \dots, a^{n-1}\}$ , natomiast nieskończoną grupę cykliczną w postaci  $\{\dots, a^{-1}, a^0, a^1, \dots\}$ .

## Wniosek

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

## Twierdzenie

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

## 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 dokładnie  $q = \frac{n}{m}$  elementów.

## 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

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

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

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

## Twierdzenie

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



## 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  $\varphi : aH \rightarrow bH$  zadane przez  $\varphi(ah) = bh$  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  $a^{-1}H$ ).

### 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 względem tej samej podgrupy  $H$  zadane wzorem  $\varphi(aH) = Ha^{-1}$  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

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

## 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

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

## 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  $\text{ord}_G(a) \mid \text{ord}(G) \quad \forall a \in G$ .

## Wniosek

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

## Dowód.

Niech  $\text{ord}_G(a) = m$ . 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.

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

## Twierdzenie

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

## Dowód.

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

## Definicja

Niech  $G$  będzie grupą, a  $H$  jej podgrupą. Mówimy, że  $H$  jest **Podgrupą normalną**  $G$ , jeżeli zachodzi  $\forall a \in G \quad aH = Ha$  (równość 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  $aHa^{-1}$  jako  $aHa^{-1} = \{aha^{-1} \mid h \in H\}$ . 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  $H$  wynosi 2, 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 określonym 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 określonym 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  $\varphi : G \rightarrow G'$ . Jądro homomorfizmu  $\varphi$  to zbiór

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

gdzie  $e'$  to element neutralny grupy  $G'$ .

## Twierdzenie

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

## Twierdzenie

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

## Dowód.

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



## Twierdzenie

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

## Twierdzenie

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

## Dowód.

Jest to homomorfizm ponieważ

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

## Twierdzenie

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

## Dowód.

Jest to homomorfizm ponieważ

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

## Konwencja

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

## Wniosek

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

### Wniosek

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

### Twierdzenie

Jeśli  $\varphi$  jest homomorfizmem grupy  $G$  na grupę  $G'$ , to istnieje izomorfizm  $\psi : G' \rightarrow G / \ker \varphi$ , dla którego przemienny jest diagram

$$\begin{array}{ccc} G & \xrightarrow{\varphi} & G \\ & \searrow \nu & \downarrow \psi \\ & & G' / \ker \varphi \end{array}$$

gdzie  $\nu$  to homomorfizm kanoniczny.

## Definicja

Relacja  $R \subseteq X \times X$ , gdzie  $X \neq \emptyset$  jest **relacją równoważności** jeżeli są spełnione następujące warunki

1.  $\forall x \in X \quad xRx$  (zwrotność)
2.  $\forall x, y \in X \quad xRy \Rightarrow yRx$  (symetryczność)
3.  $\forall x, y, z \in X \quad xRy \wedge yRz \Rightarrow xRz$  (przechodniość)

## Definicja

Niech  $R \subseteq X \times X$  będzie relacją równoważności. **Klasą abstrakcji** elementu  $x \in X$  nazywamy zbiór

$$[x]_R = \{y \in X \mid xRy\}$$

## Definicja

Niech  $X$  będzie niepustym zbiorem. **Podziałem zbioru** (rozbiciem zbioru)  $X$  nazywamy taką rodzinę  $\Pi$  niepustych jego podzbiorów, że każdy element należy dokładnie do jednego podzbioru tej rodziny. To znaczy, rodzina  $\Pi = \{X_t\}_{t \in T}$  podzbiorów  $X$  jest jego podziałem wtedy i tylko wtedy, gdy

1.  $X_t \neq \emptyset$  dla każdego  $t \in T$ ,
2. jeśli  $X_i \neq X_j$ , to  $X_i \cap X_j = \emptyset$ ,
3.  $X = \bigcup_{t \in T} X_t$ .

## Definicja

Niech  $R \subseteq X \times X$  będzie relacją równoważności. **Zbiorem ilorazowym** relacji  $R$  nazywamy rodzinę klas abstrakcji elementów z  $X$  i oznaczamy

$$X/R = \{[x]_R \mid x \in X\}.$$



## Definicja

Niech  $R \subseteq X \times X$  będzie relacją równoważności. **Zbiorem ilorazowym** relacji  $R$  nazywamy rodzinę klas abstrakcji elementów z  $X$  i oznaczamy

$$X/R = \{[x]_R \mid x \in X\}.$$

## Twierdzenie

Niech  $R \subseteq X \times X$  będzie relacją równoważności. Zbiór ilorazowy  $X/R$  jest podziałem zbioru  $X$ .

## Twierdzenie

Niech  $X$  będzie niepustym zbiorem, a  $\Pi = \{X_t\}_{t \in T}$  jego podziałem. Relacja  $R \subseteq X \times X$  określona wzorem

$$xRy \Leftrightarrow \exists t \in T : x, y \in X_t$$

jest relacją równoważności.

## Twierdzenie

Niech  $X$  będzie niepustym zbiorem, a  $\Pi = \{X_t\}_{t \in T}$  jego podziałem. Relacja  $R \subseteq X \times X$  określona wzorem

$$xRy \Leftrightarrow \exists t \in T : x, y \in X_t$$

jest relacją równoważności.

## Twierdzenie

Niech  $G$  będzie grupą, a  $H$  jej podgrupą. Rodzina warstw lewostronnych  $\{Ha \mid a \in G\}$  jest podziałem zbioru  $G$ . Rodzina warstw prawostronnych  $\{aH \mid a \in G\}$  jest podziałem zbioru  $G$ . Relacje równoważności generowane przez te podziały oznaczamy odpowiednio przez  $\overset{L}{\equiv}$  oraz  $\overset{R}{\equiv}$ .

## Obserwacja

Jeżeli  $H$  jest podgrupą normalną  $G$  to zbiór warstw lewostronnych i prawostronnych  $G/H$  są sobie równe, zatem relacje równoważności indukowane przez nie są tą samą relacją.

## Konwencja

Zwykle piszemy po prostu  $a \equiv_H b$  lub  $a \equiv b (H)$  lub  $a \equiv b \pmod{H}$ .

## Wniosek

Jeżeli  $H \trianglelefteq G$  oraz  $a, b \in G$ , to po prostu

$$a \equiv b \pmod{H} \Leftrightarrow a^{-1}b \in H.$$

### Obserwacja

Niech  $G$  będzie grupą,  $H \trianglelefteq G$  oraz  $a, b, c, d \in G$ . Załóżmy, że  $a \equiv b \pmod{H}$  oraz  $c \equiv d \pmod{H}$ . Wynika z tego, że  $aH = bH$  oraz  $cH = dH$ . Ponieważ  $G/H$  jest grupą, mamy  $aH \cdot bH = cH \cdot dH \Leftrightarrow (ac)H = (bd)H \Leftrightarrow ac \equiv bd \pmod{H}$ .

### Obserwacja

Niech  $G$  będzie grupą,  $H \trianglelefteq G$  oraz  $a, b, c, d \in G$ . Załóżmy, że  $a \equiv b \pmod{H}$  oraz  $c \equiv d \pmod{H}$ . Wynika z tego, że  $aH = bH$  oraz  $cH = dH$ . Ponieważ  $G/H$  jest grupą, mamy  $aH \cdot bH = cH \cdot dH \Leftrightarrow (ac)H = (bd)H \Leftrightarrow ac \equiv bd \pmod{H}$ .

### Definicja

Relacja równoważności  $R$  w zbiorze  $G$ , który jest grupą, nazywa się **kongruencją**, jeśli zachodzi

$$\forall a, b, c, d \in G \quad aRb \wedge cRd \Rightarrow (ac)R(bd)$$

## Twierdzenie

Jeśli  $H$  jest podgrupą normalną grupy  $G$ , to relacja przystawania elementów modulo  $H$  jest kongruencją.

### Twierdzenie

Jeśli  $H$  jest podgrupą normalną grupy  $G$ , to relacja przystawania elementów modulo  $H$  jest kongruencją.

### Twierdzenie

Jeśli relacja  $R$  jest kongruencją w grupie  $G$ , to klasa abstrakcji  $H$  zawierające element neutralny grupy  $G$  jest podgrupą normalną oraz zachodzi  $G/R = G/H$ .



Prezentacja bardzo mocno korzysta z rozdziału *XII* poniższej książki.

- [1] [Bolesław Gleichgewicht](#). *Algebra : podręcznik dla kierunków nauczycielskich studiów matematycznych*. [PWN](#), 1976.

Pytania, wątpliwości, uwagi ?