Wybrane metody algebraiczne
Wykład 1 - powtórka z teorii grup

Andrzej Sładek
sladek@ux2.math.us.edu.pl

Instytut Matematyki, Uniwersytet Śląski w Katowicach

Definicja

Zbiór G z działaniem $*$ oraz wyróżnionym elementem e nazywamy **grupą**, jeśli

Definicja

Zbiór G z działaniem $*$ oraz wyróżnionym elementem e nazywamy **grupą**, jeśli

działanie jest łączne

Definicja

Zbiór G z działaniem $*$ oraz wyróżnionym elementem e nazywamy **grupą**, jeśli

działanie jest łączne

$$\forall_{a,b,c \in G} \quad a * (b * c) = (a * b) * c$$

Definicja

Zbiór G z działaniem $*$ oraz wyróżnionym elementem e nazywamy **grupą**, jeśli

działanie jest łączne

$$\forall_{a,b,c \in G} \quad a * (b * c) = (a * b) * c$$

e jest elementem neutralnym

Definicja

Zbiór G z działaniem $*$ oraz wyróżnionym elementem e nazywamy **grupą**, jeśli

działanie jest łączne

$$\forall_{a,b,c \in G} \quad a * (b * c) = (a * b) * c$$

e jest elementem neutralnym

$$\forall_{a \in G} \quad a * e = e * a = a$$

Definicja

Zbiór G z działaniem $*$ oraz wyróżnionym elementem e nazywamy **grupą**, jeśli

działanie jest łączne

$$\forall_{a,b,c \in G} \quad a * (b * c) = (a * b) * c$$

e jest elementem neutralnym

$$\forall_{a \in G} \quad a * e = e * a = a$$

każdy element $a \in G$ posiada element odwrotny (przeciwny)

Definicja

Zbiór G z działaniem $*$ oraz wyróżnionym elementem e nazywamy **grupą**, jeśli

działanie jest łączne

$$\forall_{a,b,c \in G} \quad a * (b * c) = (a * b) * c$$

e jest elementem neutralnym

$$\forall_{a \in G} \quad a * e = e * a = a$$

każdy element $a \in G$ posiada element odwrotny (przeciwny)

$$\forall_{a \in G} \exists_{b \in G} \quad a * b = b * a = e.$$

Definicja

Zbiór G z działaniem $*$ oraz wyróżnionym elementem e nazywamy **grupą**, jeśli

działanie jest łączne

$$\forall_{a,b,c \in G} \quad a * (b * c) = (a * b) * c$$

e jest elementem neutralnym

$$\forall_{a \in G} \quad a * e = e * a = a$$

każdy element $a \in G$ posiada element odwrotny (przeciwny)

$$\forall_{a \in G} \exists_{b \in G} \quad a * b = b * a = e.$$

Ponadto, jeśli

działanie $*$ jest przemienne

Definicja

Zbiór G z działaniem $*$ oraz wyróżnionym elementem e nazywamy **grupą**, jeśli

działanie jest łączne

$$\forall_{a,b,c \in G} \quad a * (b * c) = (a * b) * c$$

e jest elementem neutralnym

$$\forall_{a \in G} \quad a * e = e * a = a$$

każdy element $a \in G$ posiada element odwrotny (przeciwny)

$$\forall_{a \in G} \exists_{b \in G} \quad a * b = b * a = e.$$

Ponadto, jeśli

działanie $*$ jest przemienne

$$\forall_{a,b \in G} \quad a * b = b * a,$$

to grupę G nazywamy **przemienną** lub **abelową**.

Przykłady

1. Zbiór liczb wymiernych (całkowitych, rzeczywistych) z działaniem $+$ jest grupą przemienną.

Przykłady

1. Zbiór liczb wymiernych (całkowitych, rzeczywistych) z działaniem $+$ jest grupą przemienną.
2. Zbiór liczb wymiernych (rzeczywistych) różnych od zera z działaniem $\cdot$ jest grupą przemienną.

Przykłady

1. Zbiór liczb wymiernych (całkowitych, rzeczywistych) z działaniem $+$ jest grupą przemienną.
2. Zbiór liczb wymiernych (rzeczywistych) różnych od zera z działaniem $\cdot$ jest grupą przemienną.
3. Niech $n \geqslant 2$ będzie liczbą naturalną oraz niech $\mathbb{Z}_n := \{0, 1..., n-1\}$. W zbiorze tym określamy działanie: $a \oplus b := (a+b)_n$). Zbiór $\mathbb{Z}_n$ z tym działaniem jest grupą przemienną.

Przykłady

1. Zbiór liczb wymiernych (całkowitych, rzeczywistych) z działaniem $+$ jest grupą przemienną.
2. Zbiór liczb wymiernych (rzeczywistych) różnych od zera z działaniem $\cdot$ jest grupą przemienną.
3. Niech $n \geqslant 2$ będzie liczbą naturalną oraz niech $\mathbb{Z}_n := \{0, 1..., n-1\}$. W zbiorze tym określamy działanie: $a \oplus b := (a+b)_n$). Zbiór $\mathbb{Z}_n$ z tym działaniem jest grupą przemienną.
4. Zbiór $G = \{e\}$ (z oczywistym działaniem) jest grupą. Nazywamy ją grupą trywialną.

Przykłady

1. Zbiór liczb wymiernych (całkowitych, rzeczywistych) z działaniem $+$ jest grupą przemienną.
2. Zbiór liczb wymiernych (rzeczywistych) różnych od zera z działaniem $\cdot$ jest grupą przemienną.
3. Niech $n \geqslant 2$ będzie liczbą naturalną oraz niech $\mathbb{Z}_n := \{0, 1..., n-1\}$. W zbiorze tym określamy działanie: $a \oplus b := (a+b)_n$). Zbiór $\mathbb{Z}_n$ z tym działaniem jest grupą przemienną.
4. Zbiór $G = \{e\}$ (z oczywistym działaniem) jest grupą. Nazywamy ją grupą trywialną.
5. Niech X będzie niepustym zbiorem. Zbiór $S(X)$ wzajemnie jednoznacznych przekształceń zbioru X na siebie (tzn. permutacji zbioru X) z działaniem składania przekształceń jest grupą (nieprzemienną, jeśli X zawiera co najmniej 3 elementy). Jeśli X jest zbiorme n-elementowyn, to grupę oznaczamy $S(n)$.

Przykłady

1. Zbiór liczb wymiernych (całkowitych, rzeczywistych) z działaniem $+$ jest grupą przemienną.
2. Zbiór liczb wymiernych (rzeczywistych) różnych od zera z działaniem $\cdot$ jest grupą przemienną.
3. Niech $n \geqslant 2$ będzie liczbą naturalną oraz niech $\mathbb{Z}_n := \{0, 1..., n-1\}$. W zbiorze tym określamy działanie: $a \oplus b := (a+b)_n$). Zbiór $\mathbb{Z}_n$ z tym działaniem jest grupą przemienną.
4. Zbiór $G = \{e\}$ (z oczywistym działaniem) jest grupą. Nazywamy ją grupą trywialną.
5. Niech X będzie niepustym zbiorem. Zbiór $S(X)$ wzajemnie jednoznacznych przekształceń zbioru X na siebie (tzn. permutacji zbioru X) z działaniem składania przekształceń jest grupą (nieprzemienną, jeśli X zawiera co najmniej 3 elementy). Jeśli X jest zbiorme n-elementowyn, to grupę oznaczamy $S(n)$.
6. Zbiór $\mathrm{GL}(n, K) = \{A \in K_n^n : \det(A) \neq 0\}$ z działaniem mnożenia macierzy jest grupą i to nieprzemienną, gdy $n \geqslant 2$.

Przykłady

1. Zbiór liczb wymiernych (całkowitych, rzeczywistych) z działaniem $+$ jest grupą przemienną.
2. Zbiór liczb wymiernych (rzeczywistych) różnych od zera z działaniem $\cdot$ jest grupą przemienną.
3. Niech $n \geqslant 2$ będzie liczbą naturalną oraz niech $\mathbb{Z}_n := \{0, 1..., n-1\}$. W zbiorze tym określamy działanie: $a \oplus b := (a+b)_n$). Zbiór $\mathbb{Z}_n$ z tym działaniem jest grupą przemienną.
4. Zbiór $G = \{e\}$ (z oczywistym działaniem) jest grupą. Nazywamy ją grupą trywialną.
5. Niech X będzie niepustym zbiorem. Zbiór $S(X)$ wzajemnie jednoznacznych przekształceń zbioru X na siebie (tzn. permutacji zbioru X) z działaniem składania przekształceń jest grupą (nieprzemienną, jeśli X zawiera co najmniej 3 elementy). Jeśli X jest zbiorme n-elementowyn, to grupę oznaczamy $S(n)$.
6. Zbiór $\mathrm{GL}(n, K) = \{A \in K_n^n : \det(A) \neq 0\}$ z działaniem mnożenia macierzy jest grupą i to nieprzemienną, gdy $n \geqslant 2$.
7. Niech $G_1, ..., G_n$ będą grupami z działaniami odpowiednio $*_1, ..., *_n$. Wtedy zbiór $G_1 \times ... \times G_n$ z działaniem $(a_1, ..., a_n) * (b_1, ..., b_n) = (a_1 *_1 b_1, ..., a_n *_n b_n)$ jest grupą. Nazywamy ją **iloczynem kartezjańskim grup** $G_1, ..., G_n$.

Definicja

Niepusty podzbiór H grupy G (z działaniem $*$) nazywamy **podgrupą** grupy G (i ozn. $H < G$), jeśli spełniony jest warunek

$$a, b \in H \implies a * b^{-1} \in H.$$

Definicja

Niepusty podzbiór H grupy G (z działaniem $*$) nazywamy **podgrupą** grupy G (i ozn. $H < G$), jeśli spełniony jest warunek

$$a, b \in H \implies a * b^{-1} \in H.$$

Uwaga

Niech $H < G$.

- Działanie $*$ zacieśnione do podzbioru H jest działaniem w zbiorze H,

Definicja

Niepusty podzbiór H grupy G (z działaniem $*$) nazywamy **podgrupą** grupy G (i ozn. $H < G$), jeśli spełniony jest warunek

$$a, b \in H \implies a * b^{-1} \in H.$$

Uwaga

Niech $H < G$.

- Działanie $*$ zacieśnione do podzbioru H jest działaniem w zbiorze H,
- Zbiór H z tym zacieśnionym działaniem jest grupą.

Definicja

Niepusty podzbiór H grupy G (z działaniem $*$) nazywamy **podgrupą** grupy G (i ozn. $H < G$), jeśli spełniony jest warunek

$$a, b \in H \implies a * b^{-1} \in H.$$

Uwaga

Niech $H < G$.

- Działanie $*$ zacieśnione do podzbioru H jest działaniem w zbiorze H,
- Zbiór H z tym zacieśnionym działaniem jest grupą.

Definicja

Niepusty podzbiór H grupy G (z działaniem $*$) nazywamy **podgrupą** grupy G (i ozn. $H < G$), jeśli spełniony jest warunek

$$a, b \in H \implies a * b^{-1} \in H.$$

Uwaga

Niech $H < G$.

- Działanie $*$ zacieśnione do podzbioru H jest działaniem w zbiorze H,
- Zbiór H z tym zacieśnionym działaniem jest grupą.

Przykłady

- $\{e\} < G$ (podgrupa trywialna), $G < G$ (podgrupa niewłaściwa)

Definicja

Niepusty podzbiór H grupy G (z działaniem $*$) nazywamy **podgrupą** grupy G (i ozn. $H < G$), jeśli spełniony jest warunek

$$a, b \in H \implies a * b^{-1} \in H.$$

Uwaga

Niech $H < G$.

- Działanie $*$ zacieśnione do podzbioru H jest działaniem w zbiorze H,
- Zbiór H z tym zacieśnionym działaniem jest grupą.

Przykłady

- $\{e\} < G$ (podgrupa trywialna), $G < G$ (podgrupa niewłaściwa)
- $\mathbb{Z} < \mathbb{Q} < \mathbb{R}$ (z działaniem $+$)

Definicja

Niepusty podzbiór H grupy G (z działaniem $*$) nazywamy **podgrupą** grupy G (i ozn. $H < G$), jeśli spełniony jest warunek

$$a, b \in H \implies a * b^{-1} \in H.$$

Uwaga

Niech $H < G$.

- Działanie $*$ zacieśnione do podzbioru H jest działaniem w zbiorze H,
- Zbiór H z tym zacieśnionym działaniem jest grupą.

Przykłady

- $\{e\} < G$ (podgrupa trywialna), $G < G$ (podgrupa niewłaściwa)
- $\mathbb{Z} < \mathbb{Q} < \mathbb{R}$ (z działaniem $+$)
- $\mathbb{Q} \setminus \{0\} < \mathbb{R} \setminus \{0\}$ (z działaniem $\cdot$)

Definicja

Niepusty podzbiór H grupy G (z działaniem $*$) nazywamy **podgrupą** grupy G (i ozn. $H < G$), jeśli spełniony jest warunek

$$a, b \in H \implies a * b^{-1} \in H.$$

Uwaga

Niech $H < G$.

- Działanie $*$ zacieśnione do podzbioru H jest działaniem w zbiorze H,
- Zbiór H z tym zacieśnionym działaniem jest grupą.

Przykłady

- $\{e\} < G$ (podgrupa trywialna), $G < G$ (podgrupa niewłaściwa)
- $\mathbb{Z} < \mathbb{Q} < \mathbb{R}$ (z działaniem $+$)
- $\mathbb{Q} \setminus \{0\} < \mathbb{R} \setminus \{0\}$ (z działaniem $\cdot$)
- Zbiór $D(n)$ izometrii n-kąta formnego jest podgrupą grupy $S(\mathbb{R}^2)$.

Definicja

Niepusty podzbiór H grupy G (z działaniem $*$) nazywamy **podgrupą** grupy G (i ozn. $H < G$), jeśli spełniony jest warunek

$$a, b \in H \implies a * b^{-1} \in H.$$

Uwaga

Niech $H < G$.

- Działanie $*$ zacieśnione do podzbioru H jest działaniem w zbiorze H,
- Zbiór H z tym zacieśnionym działaniem jest grupą.

Przykłady

- $\{e\} < G$ (podgrupa trywialna), $G < G$ (podgrupa niewłaściwa)
- $\mathbb{Z} < \mathbb{Q} < \mathbb{R}$ (z działaniem $+$)
- $\mathbb{Q} \setminus \{0\} < \mathbb{R} \setminus \{0\}$ (z działaniem $\cdot$)
- Zbiór $D(n)$ izometrii n-kąta formnego jest podgrupą grupy $S(\mathbb{R}^2)$.
- Zbiór obrotów $\{O_0, O_{120}, O_{240}\}$ jest podgrupą grupy $D(3)$ izometrii trójkąta równobocznego.

Definicja

Niepusty podzbiór H grupy G (z działaniem $*$) nazywamy **podgrupą** grupy G (i ozn. $H < G$), jeśli spełniony jest warunek

$$a, b \in H \implies a * b^{-1} \in H.$$

Uwaga

Niech $H < G$.

- Działanie $*$ zacieśnione do podzbioru H jest działaniem w zbiorze H,
- Zbiór H z tym zacieśnionym działaniem jest grupą.

Przykłady

- $\{e\} < G$ (podgrupa trywialna), $G < G$ (podgrupa niewłaściwa)
- $\mathbb{Z} < \mathbb{Q} < \mathbb{R}$ (z działaniem $+$)
- $\mathbb{Q} \setminus \{0\} < \mathbb{R} \setminus \{0\}$ (z działaniem $\cdot$)
- Zbiór $D(n)$ izometrii n-kąta formnego jest podgrupą grupy $S(\mathbb{R}^2)$.
- Zbiór obrotów $\{O_0, O_{120}, O_{240}\}$ jest podgrupą grupy $D(3)$ izometrii trójkąta równobocznego.
- $\mathrm{SL}(n, K) = \{A \in \mathrm{GL}(n, K) : \det(A) = 1\} < \mathrm{GL}(n, K)$.

Definicja

Niepusty podzbiór H grupy G (z działaniem $*$) nazywamy **podgrupą** grupy G (i ozn. $H < G$), jeśli spełniony jest warunek

$$a, b \in H \implies a * b^{-1} \in H.$$

Uwaga

Niech $H < G$.

- Działanie $*$ zacieśnione do podzbioru H jest działaniem w zbiorze H,
- Zbiór H z tym zacieśnionym działaniem jest grupą.

Przykłady

- $\{e\} < G$ (podgrupa trywialna), $G < G$ (podgrupa niewłaściwa)
- $\mathbb{Z} < \mathbb{Q} < \mathbb{R}$ (z działaniem $+$)
- $\mathbb{Q} \setminus \{0\} < \mathbb{R} \setminus \{0\}$ (z działaniem $\cdot$)
- Zbiór $D(n)$ izometrii n-kąta formnego jest podgrupą grupy $S(\mathbb{R}^2)$.
- Zbiór obrotów $\{O_0, O_{120}, O_{240}\}$ jest podgrupą grupy $D(3)$ izometrii trójkąta równobocznego.
- $\mathrm{SL}(n, K) = \{A \in \mathrm{GL}(n, K) : \det(A) = 1\} < \mathrm{GL}(n, K)$.
- Zbiór $A(n)$ permutacji parzystych jest podgrupą grupy $S(n)$.

Definicja

Jeśli $H < G, a \in G$, to zbiór

$$aH = \{ah; h \in H\} \qquad (Ha = \{ha : h \in H\})$$

nazywamy **warstwą prawostronną** (**lewostronną**) grupy G względem podgrupy H wyznaczoną przez element a.

Definicja

Jeśli $H < G, a \in G$, to zbiór

$$aH = \{ah; h \in H\} \qquad (Ha = \{ha : h \in H\})$$

nazywamy **warstwą prawostronną** (**lewostronną**) grupy G względem podgrupy H wyznaczoną przez element a.
Zbiory warstw prawostronnych i lewostronnych grupy G względem podgrupy H są równoliczne i ich wspólną moc oznaczamy $[G : H]$ i nazywamy **indeksem** podgrupy H w grupie G.

Definicja

Jeśli $H < G, a \in G$, to zbiór

$$aH = \{ah; h \in H\} \qquad (Ha = \{ha : h \in H\})$$

nazywamy **warstwą prawostronną** (**lewostronną**) grupy G względem podgrupy H wyznaczoną przez element a.
Zbiory warstw prawostronnych i lewostronnych grupy G względem podgrupy H są równoliczne i ich wspólną moc oznaczamy $[G : H]$ i nazywamy **indeksem** podgrupy H w grupie G.

Twierdzenie Lagrange'a

Jeśli H jest podgrupą skończonej grupy G, to $|G| = |H| \cdot [G : H]$.

Definicja

Jeśli $H < G, a \in G$, to zbiór

$$aH = \{ah; h \in H\} \qquad (Ha = \{ha : h \in H\})$$

nazywamy **warstwą prawostronną** (**lewostronną**) grupy G względem podgrupy H wyznaczoną przez element a.
Zbiory warstw prawostronnych i lewostronnych grupy G względem podgrupy H są równoliczne i ich wspólną moc oznaczamy $[G : H]$ i nazywamy **indeksem** podgrupy H w grupie G.

Twierdzenie Lagrange'a

Jeśli H jest podgrupą skończonej grupy G, to $|G| = |H| \cdot [G : H]$.

Wniosek

Jeśli H jest pogrupą skończonej grupy G, to $|H|$ jak i $[G : H]$ dzielą $|G|$.

Definicja

Jeśli G jest grupą oraz $A \subseteq G$, to najmniejszą podgrupę (A) grupy G zawierającą A nazywamy **podgrupą generowaną** przez A.

Definicja

Jeśli G jest grupą oraz $A \subseteq G$, to najmniejszą podgrupę (A) grupy G zawierającą A nazywamy **podgrupą generowaną** przez A.

Łatwo pokazać, że

$$(A) = \{a_1^{\varepsilon_1} ... a_n^{\varepsilon_n} : n \in \mathbb{N}, a_1, ..., a_n \in A, \varepsilon_1, ..., \varepsilon_n \in \{-1, 1\}\}.$$

Definicja

Jeśli G jest grupą oraz $A \subseteq G$, to najmniejszą podgrupę (A) grupy G zawierającą A nazywamy **podgrupą generowaną** przez A.

Łatwo pokazać, że

$$(A) = \{a_1^{\varepsilon_1} ... a_n^{\varepsilon_n} : n \in \mathbb{N}, a_1, ..., a_n \in A, \varepsilon_1, ..., \varepsilon_n \in \{-1, 1\}\}.$$

W szczególności, gdy $A = \{a\}$, to

$$(A) = \{a^k : k \in \mathbb{Z}\}.$$

Definicja

Jeśli G jest grupą oraz $A \subseteq G$, to najmniejszą podgrupę (A) grupy G zawierającą A nazywamy **podgrupą generowaną** przez A.

Łatwo pokazać, że

$$(A) = \{a_1^{\varepsilon_1} ... a_n^{\varepsilon_n} : n \in \mathbb{N}, a_1, ..., a_n \in A, \varepsilon_1, ..., \varepsilon_n \in \{-1, 1\}\}.$$

W szczególności, gdy $A = \{a\}$, to

$$(A) = \{a^k : k \in \mathbb{Z}\}.$$

Taką grupę nazywamy **cykliczną**.

Definicja

Jeśli G jest grupą oraz $A \subseteq G$, to najmniejszą podgrupę (A) grupy G zawierającą A nazywamy **podgrupą generowaną** przez A.

Łatwo pokazać, że

$$(A) = \{a_1^{\varepsilon_1} ... a_n^{\varepsilon_n} : n \in \mathbb{N}, a_1, ..., a_n \in A, \varepsilon_1, ..., \varepsilon_n \in \{-1, 1\}\}.$$

W szczególności, gdy $A = \{a\}$, to

$$(A) = \{a^k : k \in \mathbb{Z}\}.$$

Taką grupę nazywamy **cykliczną**. Jest ona oczywiście grupą abelową.

Definicja

Jeśli G jest grupą oraz $A \subseteq G$, to najmniejszą podgrupę (A) grupy G zawierającą A nazywamy **podgrupą generowaną** przez A.

Łatwo pokazać, że

$$(A) = \{a_1^{\varepsilon_1} ... a_n^{\varepsilon_n} : n \in \mathbb{N}, a_1, ..., a_n \in A, \varepsilon_1, ..., \varepsilon_n \in \{-1, 1\}\}.$$

W szczególności, gdy $A = \{a\}$, to

$$(A) = \{a^k : k \in \mathbb{Z}\}.$$

Taką grupę nazywamy **cykliczną**. Jest ona oczywiście grupą abelową.

Definicja

Jeśli a jest elementem grupy G oraz istnieje $n \in \mathbb{N}$ takie, że $a^n = 1$, to

$$r(a) = \min\{k \in \mathbb{N} : a^k = 1\}$$

nazywamy **rzędem elementu** a.

Definicja

Jeśli G jest grupą oraz $A \subseteq G$, to najmniejszą podgrupę (A) grupy G zawierającą A nazywamy **podgrupą generowaną** przez A.

Łatwo pokazać, że

$$(A) = \{a_1^{\varepsilon_1} ... a_n^{\varepsilon_n} : n \in \mathbb{N}, a_1, ..., a_n \in A, \varepsilon_1, ..., \varepsilon_n \in \{-1, 1\}\}.$$

W szczególności, gdy $A = \{a\}$, to

$$(A) = \{a^k : k \in \mathbb{Z}\}.$$

Taką grupę nazywamy **cykliczną**. Jest ona oczywiście grupą abelową.

Definicja

Jeśli a jest elementem grupy G oraz istnieje $n \in \mathbb{N}$ takie, że $a^n = 1$, to

$$r(a) = \min\{k \in \mathbb{N} : a^k = 1\}$$

nazywamy **rzędem elementu** a. Jeśli nie istnieje $n \in \mathbb{N}$, że $a^n = 1$, to umownie $r(a) = \infty$.

Rząd elementu ma następujące własności:

Rząd elementu ma następujące własności:

- $a^n = 1 \implies r(a)|n$

Rząd elementu ma następujące własności:

- $a^n = 1 \implies r(a)|n$
- Jeśli $r(a) < \infty$, to $a^n = a^m \iff n \equiv m \pmod{r(a)}$, tzn. $r(a)|n - m$.

Rząd elementu ma następujące własności:

- $a^n = 1 \implies r(a)|n$
- Jeśli $r(a) < \infty$, to $a^n = a^m \iff n \equiv m \pmod{r(a)}$, tzn. $r(a)|n - m$.
- Jeśli $r(a) < \infty$, to $(a) = \{1, a, a^2, ..., a^{r(a)-1}\}$.

Rząd elementu ma następujące własności:

- $a^n = 1 \implies r(a)|n$
- Jeśli $r(a) < \infty$, to $a^n = a^m \iff n \equiv m \pmod{r(a)}$, tzn. $r(a)|n - m$.
- Jeśli $r(a) < \infty$, to $(a) = \{1, a, a^2, ..., a^{r(a)-1}\}$.
- Jeśli a jest elementem skończonej grupy G, to $r(a)$ dzieli $|G|$.

Rząd elementu ma następujące własności:

- $a^n = 1 \implies r(a)|n$
- Jeśli $r(a) < \infty$, to $a^n = a^m \iff n \equiv m \pmod{r(a)}$, tzn. $r(a)|n - m$.
- Jeśli $r(a) < \infty$, to $(a) = \{1, a, a^2, ..., a^{r(a)-1}\}$.
- Jeśli a jest elementem skończonej grupy G, to $r(a)$ dzieli $|G|$.

Rząd elementu ma następujące własności:

- $a^n = 1 \implies r(a)|n$
- Jeśli $r(a) < \infty$, to $a^n = a^m \iff n \equiv m \pmod{r(a)}$, tzn. $r(a)|n - m$.
- Jeśli $r(a) < \infty$, to $(a) = \{1, a, a^2, ..., a^{r(a)-1}\}$.
- Jeśli a jest elementem skończonej grupy G, to $r(a)$ dzieli $|G|$.

Definicja

Jeśli G_1 oraz G_2 są grupami, to odwzorowanie $\varphi : G_1 \longrightarrow G_2$ nazywamy **homomorfizmem**, jeśli

$$\forall_{a,b \in G_1} \quad \varphi(a *_1 b) = \varphi(a) *_2 \varphi(b).$$

Rząd elementu ma następujące własności:

- $a^n = 1 \implies r(a)|n$
- Jeśli $r(a) < \infty$, to $a^n = a^m \iff n \equiv m \pmod{r(a)}$, tzn. $r(a)|n - m$.
- Jeśli $r(a) < \infty$, to $(a) = \{1, a, a^2, ..., a^{r(a)-1}\}$.
- Jeśli a jest elementem skończonej grupy G, to $r(a)$ dzieli $|G|$.

Definicja

Jeśli G_1 oraz G_2 są grupami, to odwzorowanie $\varphi : G_1 \longrightarrow G_2$ nazywamy **homomorfizmem**, jeśli

$$\forall_{a,b \in G_1} \quad \varphi(a *_1 b) = \varphi(a) *_2 \varphi(b).$$

Homomorfizm φ nazywamy

- monomorfizmem, jeśli φ jest różnowartościowe,

Rząd elementu ma następujące własności:

- $a^n = 1 \implies r(a)|n$
- Jeśli $r(a) < \infty$, to $a^n = a^m \iff n \equiv m \pmod{r(a)}$, tzn. $r(a)|n-m$.
- Jeśli $r(a) < \infty$, to $(a) = \{1, a, a^2, ..., a^{r(a)-1}\}$.
- Jeśli a jest elementem skończonej grupy G, to $r(a)$ dzieli $|G|$.

Definicja

Jeśli G_1 oraz G_2 są grupami, to odwzorowanie $\varphi : G_1 \longrightarrow G_2$ nazywamy **homomorfizmem**, jeśli

$$\forall_{a,b \in G_1} \quad \varphi(a *_1 b) = \varphi(a) *_2 \varphi(b).$$

Homomorfizm φ nazywamy

- monomorfizmem, jeśli φ jest różnowartościowe,
- epimorfizmem, jeśli φ jest "na",

Rząd elementu ma następujące własności:

- $a^n = 1 \implies r(a)|n$
- Jeśli $r(a) < \infty$, to $a^n = a^m \iff n \equiv m \pmod{r(a)}$, tzn. $r(a)|n-m$.
- Jeśli $r(a) < \infty$, to $(a) = \{1, a, a^2, ..., a^{r(a)-1}\}$.
- Jeśli a jest elementem skończonej grupy G, to $r(a)$ dzieli $|G|$.

Definicja

Jeśli G_1 oraz G_2 są grupami, to odwzorowanie $\varphi : G_1 \longrightarrow G_2$ nazywamy **homomorfizmem**, jeśli

$$\underset{a,b \in G_1}{\forall} \quad \varphi(a *_1 b) = \varphi(a) *_2 \varphi(b).$$

Homomorfizm φ nazywamy

- monomorfizmem, jeśli φ jest różnowartościowe,
- epimorfizmem, jeśli φ jest "na",
- izomorfizmem, jeśli φ jest wzajemnie jednoznaczne,

Rząd elementu ma następujące własności:

- $a^n = 1 \implies r(a)|n$
- Jeśli $r(a) < \infty$, to $a^n = a^m \iff n \equiv m \pmod{r(a)}$, tzn. $r(a)|n-m$.
- Jeśli $r(a) < \infty$, to $(a) = \{1, a, a^2, ..., a^{r(a)-1}\}$.
- Jeśli a jest elementem skończonej grupy G, to $r(a)$ dzieli $|G|$.

Definicja

Jeśli G_1 oraz G_2 są grupami, to odwzorowanie $\varphi : G_1 \longrightarrow G_2$ nazywamy **homomorfizmem**, jeśli

$$\underset{a,b \in G_1}{\forall} \quad \varphi(a *_1 b) = \varphi(a) *_2 \varphi(b).$$

Homomorfizm φ nazywamy

- monomorfizmem, jeśli φ jest różnowartościowe,
- epimorfizmem, jeśli φ jest "na",
- izomorfizmem, jeśli φ jest wzajemnie jednoznaczne,
- endomorfizmem, jeśli $G_1 = G_2$,

Rząd elementu ma następujące własności:

- $a^n = 1 \implies r(a)|n$
- Jeśli $r(a) < \infty$, to $a^n = a^m \iff n \equiv m \pmod{r(a)}$, tzn. $r(a)|n-m$.
- Jeśli $r(a) < \infty$, to $(a) = \{1, a, a^2, ..., a^{r(a)-1}\}$.
- Jeśli a jest elementem skończonej grupy G, to $r(a)$ dzieli $|G|$.

Definicja

Jeśli G_1 oraz G_2 są grupami, to odwzorowanie $\varphi : G_1 \longrightarrow G_2$ nazywamy **homomorfizmem**, jeśli

$$\underset{a,b \in G_1}{\forall} \quad \varphi(a *_1 b) = \varphi(a) *_2 \varphi(b).$$

Homomorfizm φ nazywamy

- monomorfizmem, jeśli φ jest różnowartościowe,
- epimorfizmem, jeśli φ jest "na",
- izomorfizmem, jeśli φ jest wzajemnie jednoznaczne,
- endomorfizmem, jeśli $G_1 = G_2$,
- automorfizmem, jeśli φ jest izomorfizmem oraz $G_1 = G_2$.

Własności

- Jeżeli $\varphi : G_1 \longrightarrow G_2$ jest homomorfizmem, to

$$\varphi(e_1) = e_2,$$

Własności

- Jeżeli $\varphi : G_1 \longrightarrow G_2$ jest homomorfizmem, to

$$\varphi(e_1) = e_2, \quad \varphi(a^k) = \varphi(a)^k,$$

Własności

- Jeżeli $\varphi : G_1 \longrightarrow G_2$ jest homomorfizmem, to

$$\varphi(e_1) = e_2, \quad \varphi(a^k) = \varphi(a)^k, \quad \varphi(a^{-1}) = \varphi(a)^{-1}.$$

Własności

- Jeżeli $\varphi : G_1 \longrightarrow G_2$ jest homomorfizmem, to

$$\varphi(e_1) = e_2, \quad \varphi(a^k) = \varphi(a)^k, \quad \varphi(a^{-1}) = \varphi(a)^{-1}.$$

- Złożenie homomorfizmów jest homomorfizmem.

Własności

- Jeżeli $\varphi : G_1 \longrightarrow G_2$ jest homomorfizmem, to

$$\varphi(e_1) = e_2, \quad \varphi(a^k) = \varphi(a)^k, \quad \varphi(a^{-1}) = \varphi(a)^{-1}.$$

- Złożenie homomorfizmów jest homomorfizmem.
- Odwzorowanie odwrotne do izomorfizmu jest izomorfizmem.

Własności

- Jeżeli $\varphi : G_1 \longrightarrow G_2$ jest homomorfizmem, to

$$\varphi(e_1) = e_2, \quad \varphi(a^k) = \varphi(a)^k, \quad \varphi(a^{-1}) = \varphi(a)^{-1}.$$

- Złożenie homomorfizmów jest homomorfizmem.
- Odwzorowanie odwrotne do izomorfizmu jest izomorfizmem.

Przykłady

- $\varphi : G_1 \longrightarrow G_2$, $\varphi(a) = e_2$, dla $a \in G_1$ - homomorfizm trywialny,

Własności

- Jeżeli $\varphi : G_1 \longrightarrow G_2$ jest homomorfizmem, to

$$\varphi(e_1) = e_2, \quad \varphi(a^k) = \varphi(a)^k, \quad \varphi(a^{-1}) = \varphi(a)^{-1}.$$

- Złożenie homomorfizmów jest homomorfizmem.
- Odwzorowanie odwrotne do izomorfizmu jest izomorfizmem.

Przykłady

- $\varphi : G_1 \longrightarrow G_2,\ \varphi(a) = e_2,$ dla $a \in G_1$ - homomorfizm trywialny,
- $\mathrm{id}_G : G \longrightarrow G,\ \mathrm{id}_G(a) = a,$ dla $a \in G$ - odwzorowanie identycznościowe,

Własności

- Jeżeli $\varphi : G_1 \longrightarrow G_2$ jest homomorfizmem, to

$$\varphi(e_1) = e_2, \quad \varphi(a^k) = \varphi(a)^k, \quad \varphi(a^{-1}) = \varphi(a)^{-1}.$$

- Złożenie homomorfizmów jest homomorfizmem.
- Odwzorowanie odwrotne do izomorfizmu jest izomorfizmem.

Przykłady

- $\varphi : G_1 \longrightarrow G_2,\ \varphi(a) = e_2,$ dla $a \in G_1$ - homomorfizm trywialny,
- $\mathrm{id}_G : G \longrightarrow G,\ \mathrm{id}_G(a) = a,$ dla $a \in G$ - odwzorowanie identycznościowe,
- $\det : \mathrm{GL}(n, K) \longrightarrow K^*,$

Własności

- Jeżeli $\varphi : G_1 \longrightarrow G_2$ jest homomorfizmem, to

$$\varphi(e_1) = e_2, \quad \varphi(a^k) = \varphi(a)^k, \quad \varphi(a^{-1}) = \varphi(a)^{-1}.$$

- Złożenie homomorfizmów jest homomorfizmem.
- Odwzorowanie odwrotne do izomorfizmu jest izomorfizmem.

Przykłady

- $\varphi : G_1 \longrightarrow G_2,\ \varphi(a) = e_2,$ dla $a \in G_1$ - homomorfizm trywialny,
- $\mathrm{id}_G : G \longrightarrow G,\ \mathrm{id}_G(a) = a,$ dla $a \in G$ - odwzorowanie identycznościowe,
- $\det : \mathrm{GL}(n, K) \longrightarrow K^*,$
- przekształcenie liniowe jest homomorfizmem grup addytywnych przestrzeni liniowych,

Własności

- Jeżeli $\varphi : G_1 \longrightarrow G_2$ jest homomorfizmem, to

$$\varphi(e_1) = e_2, \quad \varphi(a^k) = \varphi(a)^k, \quad \varphi(a^{-1}) = \varphi(a)^{-1}.$$

- Złożenie homomorfizmów jest homomorfizmem.
- Odwzorowanie odwrotne do izomorfizmu jest izomorfizmem.

Przykłady

- $\varphi : G_1 \longrightarrow G_2,\ \varphi(a) = e_2,$ dla $a \in G_1$ - homomorfizm trywialny,
- $\mathrm{id}_G : G \longrightarrow G,\ \mathrm{id}_G(a) = a,$ dla $a \in G$ - odwzorowanie identycznościowe,
- $\det : \mathrm{GL}(n, K) \longrightarrow K^*,$
- przekształcenie liniowe jest homomorfizmem grup addytywnych przestrzeni liniowych,
- $\log_a : \mathbb{R}^+ \longrightarrow \mathbb{R}$ jest izomorfizmem pomiędzy multiplikatywną grupą liczb rzeczywistych dodatnich a grupą addytywną liczb rzeczywistych,

Własności

- Jeżeli $\varphi : G_1 \longrightarrow G_2$ jest homomorfizmem, to

$$\varphi(e_1) = e_2, \quad \varphi(a^k) = \varphi(a)^k, \quad \varphi(a^{-1}) = \varphi(a)^{-1}.$$

- Złożenie homomorfizmów jest homomorfizmem.
- Odwzorowanie odwrotne do izomorfizmu jest izomorfizmem.

Przykłady

- $\varphi : G_1 \longrightarrow G_2,\ \varphi(a) = e_2,$ dla $a \in G_1$ - homomorfizm trywialny,
- $\mathrm{id}_G : G \longrightarrow G,\ \mathrm{id}_G(a) = a,$ dla $a \in G$ - odwzorowanie identycznościowe,
- $\det : \mathrm{GL}(n, K) \longrightarrow K^*,$
- przekształcenie liniowe jest homomorfizmem grup addytywnych przestrzeni liniowych,
- $\log_a : \mathbb{R}^+ \longrightarrow \mathbb{R}$ jest izomorfizmem pomiędzy multiplikatywną grupą liczb rzeczywistych dodatnich a grupą addytywną liczb rzeczywistych,
- $\mathbb{Z} \longrightarrow \mathbb{Z}_n,\ a \longmapsto (a)_n,$

Własności

- Jeżeli $\varphi : G_1 \longrightarrow G_2$ jest homomorfizmem, to

$$\varphi(e_1) = e_2, \quad \varphi(a^k) = \varphi(a)^k, \quad \varphi(a^{-1}) = \varphi(a)^{-1}.$$

- Złożenie homomorfizmów jest homomorfizmem.
- Odwzorowanie odwrotne do izomorfizmu jest izomorfizmem.

Przykłady

- $\varphi : G_1 \longrightarrow G_2,\ \varphi(a) = e_2,$ dla $a \in G_1$ - homomorfizm trywialny,
- $\mathrm{id}_G : G \longrightarrow G,\ \mathrm{id}_G(a) = a,$ dla $a \in G$ - odwzorowanie identycznościowe,
- $\det : \mathrm{GL}(n, K) \longrightarrow K^*,$
- przekształcenie liniowe jest homomorfizmem grup addytywnych przestrzeni liniowych,
- $\log_a : \mathbb{R}^+ \longrightarrow \mathbb{R}$ jest izomorfizmem pomiędzy multiplikatywną grupą liczb rzeczywistych dodatnich a grupą addytywną liczb rzeczywistych,
- $\mathbb{Z} \longrightarrow \mathbb{Z}_n,\ a \longmapsto (a)_n,$
- $\varphi_a : G \longrightarrow G,\ \varphi_a(x) = a^{-1}xa$ dla $x \in G$ - automorfizm wewnętrzny.

Twierdzenie

Jeżeli $\varphi : G_1 \longrightarrow G_2$ jest homomorfizmem, $H_1 < G_1, H_2 < G_2$, to

$$\varphi(H_1) < G_2,$$

Twierdzenie

Jeżeli $\varphi : G_1 \longrightarrow G_2$ jest homomorfizmem, $H_1 < G_1, H_2 < G_2$, to

$$\varphi(H_1) < G_2, \quad \varphi^{-1}(H_2) < G_1.$$

Twierdzenie

Jeżeli $\varphi : G_1 \longrightarrow G_2$ jest homomorfizmem, $H_1 < G_1, H_2 < G_2$, to

$$\varphi(H_1) < G_2, \quad \varphi^{-1}(H_2) < G_1.$$

Definicja

Jeżeli $\varphi : G_1 \longrightarrow G_2$ jest homomorfizmem, to $\ker \varphi = \{a \in G : \varphi(a) = e_2\} = \varphi^{-1}(e_2)$ nazywamy **jądrem**, a $\operatorname{im} \varphi = \varphi(G_1)$ **obrazem** homomorfizmu φ.

Twierdzenie

Jeżeli $\varphi : G_1 \longrightarrow G_2$ jest homomorfizmem, $H_1 < G_1, H_2 < G_2$, to

$$\varphi(H_1) < G_2, \quad \varphi^{-1}(H_2) < G_1.$$

Definicja

Jeżeli $\varphi : G_1 \longrightarrow G_2$ jest homomorfizmem, to $\ker \varphi = \{a \in G : \varphi(a) = e_2\} = \varphi^{-1}(e_2)$ nazywamy **jądrem**, a $\operatorname{im} \varphi = \varphi(G_1)$ **obrazem** homomorfizmu φ.

Uwagi

- $\ker \varphi < G_1, \quad \operatorname{im} \varphi < G_2$.

Twierdzenie

Jeżeli $\varphi : G_1 \longrightarrow G_2$ jest homomorfizmem, $H_1 < G_1, H_2 < G_2$, to

$$\varphi(H_1) < G_2, \quad \varphi^{-1}(H_2) < G_1.$$

Definicja

Jeżeli $\varphi : G_1 \longrightarrow G_2$ jest homomorfizmem, to $\ker \varphi = \{a \in G : \varphi(a) = e_2\} = \varphi^{-1}(e_2)$ nazywamy **jądrem**, a $\operatorname{im} \varphi = \varphi(G_1)$ **obrazem** homomorfizmu φ.

Uwagi

- $\ker \varphi < G_1, \quad \operatorname{im} \varphi < G_2$.
- Homomorfizm φ jest monomorfizmem wtedy i tylko wtedy, gdy $\ker \varphi = \{e_1\}$.

Twierdzenie

Jeżeli $\varphi : G_1 \longrightarrow G_2$ jest homomorfizmem, $H_1 < G_1, H_2 < G_2$, to

$$\varphi(H_1) < G_2, \quad \varphi^{-1}(H_2) < G_1.$$

Definicja

Jeżeli $\varphi : G_1 \longrightarrow G_2$ jest homomorfizmem, to $\ker \varphi = \{a \in G : \varphi(a) = e_2\} = \varphi^{-1}(e_2)$ nazywamy **jądrem**, a $\operatorname{im} \varphi = \varphi(G_1)$ **obrazem** homomorfizmu φ.

Uwagi

- $\ker \varphi < G_1, \quad \operatorname{im} \varphi < G_2$.
- Homomorfizm φ jest monomorfizmem wtedy i tylko wtedy, gdy $\ker \varphi = \{e_1\}$.
- Homomorfizm φ jest epimorfizmem wtedy i tylko wtedy, gdy $\operatorname{im} \varphi = G_2$.

Twierdzenie

Jeżeli $\varphi : G_1 \longrightarrow G_2$ jest homomorfizmem, $H_1 < G_1, H_2 < G_2$, to

$$\varphi(H_1) < G_2, \quad \varphi^{-1}(H_2) < G_1.$$

Definicja

Jeżeli $\varphi : G_1 \longrightarrow G_2$ jest homomorfizmem, to $\ker \varphi = \{a \in G : \varphi(a) = e_2\} = \varphi^{-1}(e_2)$ nazywamy **jądrem**, a $\operatorname{im} \varphi = \varphi(G_1)$ **obrazem** homomorfizmu φ.

Uwagi

- $\ker \varphi < G_1, \quad \operatorname{im} \varphi < G_2$.
- Homomorfizm φ jest monomorfizmem wtedy i tylko wtedy, gdy $\ker \varphi = \{e_1\}$.
- Homomorfizm φ jest epimorfizmem wtedy i tylko wtedy, gdy $\operatorname{im} \varphi = G_2$.
- Homomorfizm φ jest izomorfizmem wtedy i tylko wtedy, gdy $\ker \varphi = \{e_1\}$ oraz $\operatorname{im} \varphi = G_2$.

Definicja

Podgrupę H grupy G nazywamy **podgrupą normalną** (lub **dzielnikiem normalnym**), i oznaczamy $H \lhd G$, jeśli

$$\bigvee_{a \in G} \bigvee_{h \in H} a^{-1}ha \in H.$$

Definicja

Podgrupę H grupy G nazywamy **podgrupą normalną** (lub **dzielnikiem normalnym**), i oznaczamy $H \lhd G$, jeśli

$$\bigvee_{a \in G} \bigvee_{h \in H} a^{-1}ha \in H.$$

Warunek z powyższej definicji można w sposób równoważny sformułować następująco:

$$\bigvee_{a \in G} \bigvee_{h \in H} aH = Ha,$$

Definicja

Podgrupę H grupy G nazywamy **podgrupą normalną** (lub **dzielnikiem normalnym**), i oznaczamy $H \lhd G$, jeśli

$$\bigvee_{a \in G} \bigvee_{h \in H} a^{-1}ha \in H.$$

Warunek z powyższej definicji można w sposób równoważny sformułować następująco:

$$\bigvee_{a \in G} \bigvee_{h \in H} aH = Ha,$$

lub

$$\bigvee_{a \in G} \bigvee_{h \in H} a^{-1}Ha = H.$$

Definicja

Podgrupę H grupy G nazywamy **podgrupą normalną** (lub **dzielnikiem normalnym**), i oznaczamy $H \lhd G$, jeśli

$$\bigvee_{a \in G} \bigvee_{h \in H} a^{-1}ha \in H.$$

Warunek z powyższej definicji można w sposób równoważny sformułować następująco:

$$\bigvee_{a \in G} \bigvee_{h \in H} aH = Ha,$$

lub

$$\bigvee_{a \in G} \bigvee_{h \in H} a^{-1}Ha = H.$$

Przykłady

- W grupie abelowej wszystkie podgrupy są normalne.

Definicja

Podgrupę H grupy G nazywamy **podgrupą normalną** (lub **dzielnikiem normalnym**), i oznaczamy $H \lhd G$, jeśli

$$\bigvee_{a \in G} \bigvee_{h \in H} a^{-1}ha \in H.$$

Warunek z powyższej definicji można w sposób równoważny sformułować następująco:

$$\bigvee_{a \in G} \bigvee_{h \in H} aH = Ha,$$

lub

$$\bigvee_{a \in G} \bigvee_{h \in H} a^{-1}Ha = H.$$

Przykłady

- W grupie abelowej wszystkie podgrupy są normalne.
- $\{e\} \lhd G, \quad G \lhd G.$

Definicja

Podgrupę H grupy G nazywamy **podgrupą normalną** (lub **dzielnikiem normalnym**), i oznaczamy $H \lhd G$, jeśli

$$\bigvee_{a \in G} \bigvee_{h \in H} a^{-1}ha \in H.$$

Warunek z powyższej definicji można w sposób równoważny sformułować następująco:

$$\bigvee_{a \in G} \bigvee_{h \in H} aH = Ha,$$

lub

$$\bigvee_{a \in G} \bigvee_{h \in H} a^{-1}Ha = H.$$

Przykłady

- W grupie abelowej wszystkie podgrupy są normalne.
- $\{e\} \lhd G, \quad G \lhd G.$
- Jądro homomorfizmu jest podgrupą normalną.

Definicja

Podgrupę H grupy G nazywamy **podgrupą normalną** (lub **dzielnikiem normalnym**), i oznaczamy $H \lhd G$, jeśli

$$\bigvee_{a \in G} \bigvee_{h \in H} a^{-1}ha \in H.$$

Warunek z powyższej definicji można w sposób równoważny sformułować następująco:

$$\bigvee_{a \in G} \bigvee_{h \in H} aH = Ha,$$

lub

$$\bigvee_{a \in G} \bigvee_{h \in H} a^{-1}Ha = H.$$

Przykłady

- W grupie abelowej wszystkie podgrupy są normalne.
- $\{e\} \lhd G, \quad G \lhd G.$
- Jądro homomorfizmu jest podgrupą normalną.
- Jeśli $[G : H] = 2$, to $H \lhd G$.

Niech $H \triangleleft G$. W zbiorze G/H warstw grupy G względem podgrupy H można poprawnie zdefiniować działanie:

$$(aH) \cdot (bH) = abH, \ a, b \in G.$$

Wtedy

- zbiór G/H wraz z tym działaniem jest grupą,

Niech $H \triangleleft G$. W zbiorze G/H warstw grupy G względem podgrupy H można poprawnie zdefiniować działanie:

$$(aH) \cdot (bH) = abH, \ a, b \in G.$$

Wtedy

- zbiór G/H wraz z tym działaniem jest grupą,
- odwzorowanie $\kappa : G \longrightarrow G/H, \ a \longmapsto aH$, jest epimorfizmem oraz $\ker \kappa = H$.

Niech $H \triangleleft G$. W zbiorze G/H warstw grupy G względem podgrupy H można poprawnie zdefiniować działanie:

$$(aH) \cdot (bH) = abH, \ a, b \in G.$$

Wtedy

- zbiór G/H wraz z tym działaniem jest grupą,
- odwzorowanie $\kappa : G \longrightarrow G/H, \ a \longmapsto aH$, jest epimorfizmem oraz $\ker \kappa = H$.

Niech $H \triangleleft G$. W zbiorze G/H warstw grupy G względem podgrupy H można poprawnie zdefiniować działanie:

$$(aH) \cdot (bH) = abH, \ a, b \in G.$$

Wtedy

- zbiór G/H wraz z tym działaniem jest grupą,
- odwzorowanie $\kappa : G \longrightarrow G/H, \ a \longmapsto aH$, jest epimorfizmem oraz $\ker \kappa = H$.

Grupę G/H nazywamy **grupą ilorazową** grupy G względem podgrupy H, a epimorfizm κ **epimorfizmem kanonicznym**.

Niech $H \triangleleft G$. W zbiorze G/H warstw grupy G względem podgrupy H można poprawnie zdefiniować działanie:

$$(aH) \cdot (bH) = abH, \ a, b \in G.$$

Wtedy

- zbiór G/H wraz z tym działaniem jest grupą,
- odwzorowanie $\kappa : G \longrightarrow G/H, \ a \longmapsto aH$, jest epimorfizmem oraz $\ker \kappa = H$.

Grupę G/H nazywamy **grupą ilorazową** grupy G względem podgrupy H, a epimorfizm κ **epimorfizmem kanonicznym**.

Twierdzenie o homomorfiźmie grup

Niech $\varphi : G_1 \longrightarrow G_2$ będzie homomorfizmem, $H \triangleleft G_1$, $H \subseteq \ker \varphi$. Wtedy istnieje dokładnie jeden homommorfizm $\bar{\varphi} : G_1/H \longrightarrow G_2$ taki, że $\varphi = \bar{\varphi} \circ \kappa$.

Niech $H \triangleleft G$. W zbiorze G/H warstw grupy G względem podgrupy H można poprawnie zdefiniować działanie:

$$(aH) \cdot (bH) = abH, \ a, b \in G.$$

Wtedy

- zbiór G/H wraz z tym działaniem jest grupą,
- odwzorowanie $\kappa : G \longrightarrow G/H, \ a \longmapsto aH$, jest epimorfizmem oraz $\ker \kappa = H$.

Grupę G/H nazywamy **grupą ilorazową** grupy G względem podgrupy H, a epimorfizm κ **epimorfizmem kanonicznym**.

Twierdzenie o homomorfiźmie grup

Niech $\varphi : G_1 \longrightarrow G_2$ będzie homomorfizmem, $H \triangleleft G_1$, $H \subseteq \ker \varphi$. Wtedy istnieje dokładnie jeden homommorfizm $\bar{\varphi} : G_1/H \longrightarrow G_2$ taki, że $\varphi = \bar{\varphi} \circ \kappa$.
Ponadto

- $\bar{\varphi}$ jest monomorfizmem wtedy i tylko wtedy, gdy $H = \ker \varphi$.

Niech $H \triangleleft G$. W zbiorze G/H warstw grupy G względem podgrupy H można poprawnie zdefiniować działanie:

$$(aH) \cdot (bH) = abH, \ a, b \in G.$$

Wtedy

- zbiór G/H wraz z tym działaniem jest grupą,
- odwzorowanie $\kappa : G \longrightarrow G/H, \ a \longmapsto aH$, jest epimorfizmem oraz $\ker \kappa = H$.

Grupę G/H nazywamy **grupą ilorazową** grupy G względem podgrupy H, a epimorfizm κ **epimorfizmem kanonicznym**.

Twierdzenie o homomorfiźmie grup

Niech $\varphi : G_1 \longrightarrow G_2$ będzie homomorfizmem, $H \triangleleft G_1$, $H \subseteq \ker \varphi$. Wtedy istnieje dokładnie jeden homommorfizm $\bar{\varphi} : G_1/H \longrightarrow G_2$ taki, że $\varphi = \bar{\varphi} \circ \kappa$.
Ponadto

- $\bar{\varphi}$ jest monomorfizmem wtedy i tylko wtedy, gdy $H = \ker \varphi$.
- $\bar{\varphi}$ jest epimorfizmem wtedy i tylko wtedy, gdy φ jest epimorfizmem.

Niech $H \triangleleft G$. W zbiorze G/H warstw grupy G względem podgrupy H można poprawnie zdefiniować działanie:

$$(aH) \cdot (bH) = abH, \ a, b \in G.$$

Wtedy

- zbiór G/H wraz z tym działaniem jest grupą,
- odwzorowanie $\kappa : G \longrightarrow G/H, \ a \longmapsto aH$, jest epimorfizmem oraz $\ker \kappa = H$.

Grupę G/H nazywamy **grupą ilorazową** grupy G względem podgrupy H, a epimorfizm κ **epimorfizmem kanonicznym**.

Twierdzenie o homomorfiźmie grup

Niech $\varphi : G_1 \longrightarrow G_2$ będzie homomorfizmem, $H \triangleleft G_1$, $H \subseteq \ker \varphi$. Wtedy istnieje dokładnie jeden homommorfizm $\bar{\varphi} : G_1/H \longrightarrow G_2$ taki, że $\varphi = \bar{\varphi} \circ \kappa$.
Ponadto

- $\bar{\varphi}$ jest monomorfizmem wtedy i tylko wtedy, gdy $H = \ker \varphi$.
- $\bar{\varphi}$ jest epimorfizmem wtedy i tylko wtedy, gdy φ jest epimorfizmem.
- $\bar{\varphi}$ jest izomorfizmem wtedy i tylko wtedy, gdy $H = \ker \varphi$ oraz φ jest epimorfizmem.

Niech $H \triangleleft G$. W zbiorze G/H warstw grupy G względem podgrupy H można poprawnie zdefiniować działanie:

$$(aH) \cdot (bH) = abH, \ a, b \in G.$$

Wtedy

- zbiór G/H wraz z tym działaniem jest grupą,
- odwzorowanie $\kappa : G \longrightarrow G/H, \ a \longmapsto aH$, jest epimorfizmem oraz $\ker \kappa = H$.

Grupę G/H nazywamy **grupą ilorazową** grupy G względem podgrupy H, a epimorfizm κ **epimorfizmem kanonicznym**.

Twierdzenie o homomorfiźmie grup

Niech $\varphi : G_1 \longrightarrow G_2$ będzie homomorfizmem, $H \triangleleft G_1$, $H \subseteq \ker \varphi$. Wtedy istnieje dokładnie jeden homommorfizm $\bar{\varphi} : G_1/H \longrightarrow G_2$ taki, że $\varphi = \bar{\varphi} \circ \kappa$.
Ponadto

- $\bar{\varphi}$ jest monomorfizmem wtedy i tylko wtedy, gdy $H = \ker \varphi$.
- $\bar{\varphi}$ jest epimorfizmem wtedy i tylko wtedy, gdy φ jest epimorfizmem.
- $\bar{\varphi}$ jest izomorfizmem wtedy i tylko wtedy, gdy $H = \ker \varphi$ oraz φ jest epimorfizmem.

Niech $H \triangleleft G$. W zbiorze G/H warstw grupy G względem podgrupy H można poprawnie zdefiniować działanie:

$$(aH) \cdot (bH) = abH, \ a, b \in G.$$

Wtedy

- zbiór G/H wraz z tym działaniem jest grupą,
- odwzorowanie $\kappa : G \longrightarrow G/H, \ a \longmapsto aH$, jest epimorfizmem oraz $\ker \kappa = H$.

Grupę G/H nazywamy **grupą ilorazową** grupy G względem podgrupy H, a epimorfizm κ **epimorfizmem kanonicznym**.

Twierdzenie o homomorfiźmie grup

Niech $\varphi : G_1 \longrightarrow G_2$ będzie homomorfizmem, $H \triangleleft G_1$, $H \subseteq \ker \varphi$. Wtedy istnieje dokładnie jeden homommorfizm $\bar{\varphi} : G_1/H \longrightarrow G_2$ taki, że $\varphi = \bar{\varphi} \circ \kappa$.
Ponadto

- $\bar{\varphi}$ jest monomorfizmem wtedy i tylko wtedy, gdy $H = \ker \varphi$.
- $\bar{\varphi}$ jest epimorfizmem wtedy i tylko wtedy, gdy φ jest epimorfizmem.
- $\bar{\varphi}$ jest izomorfizmem wtedy i tylko wtedy, gdy $H = \ker \varphi$ oraz φ jest epimorfizmem.

Wniosek, twierdzenie o izomorfiźmie grup

Jeśli $\varphi : G_1 \longrightarrow G_2$ jest homomorfizmem, to $G_1/\ker \varphi \cong \operatorname{im} \varphi$.

Elementy a i b grupy G nazywamy **sprzężonymi**, jeśli istnieje element $c \in G$ taki, że $a = c^{-1}bc$.

Elementy a i b grupy G nazywamy **sprzężonymi**, jeśli istnieje element $c \in G$ taki, że $a = c^{-1}bc$.
Relacja sprzężenia jest relacją równoważnościową i rozbija grupę G na rozłączne klasy abstrakcji.

Elementy a i b grupy G nazywamy **sprzężonymi**, jeśli istnieje element $c \in G$ taki, że $a = c^{-1}bc$.
Relacja sprzężenia jest relacją równoważnościową i rozbija grupę G na rozłączne klasy abstrakcji.
Klasy sprzężoności będą odgrywały ważną rolę w dalszych wykładach. Pewne własności klas abstrakcji znajdziemy w zestawie zadań 1.

Elementy a i b grupy G nazywamy **sprzężonymi**, jeśli istnieje element $c \in G$ taki, że $a = c^{-1}bc$.
Relacja sprzężenia jest relacją równoważnościową i rozbija grupę G na rozłączne klasy abstrakcji.
Klasy sprzężoności będą odgrywały ważną rolę w dalszych wykładach. Pewne własności klas abstrakcji znajdziemy w zestawie zadań 1.

Definicja

Dla elementów a, b grupy G element $[a, b] = a^{-1}b^{-1}ab$ nazywamy **komutatorem**, a $[G, G] = (\{[a, b] : a, b \in G\})$ nazywamy **komutantem** grupy G.

Elementy a i b grupy G nazywamy **sprzężonymi**, jeśli istnieje element $c \in G$ taki, że $a = c^{-1}bc$.
Relacja sprzężenia jest relacją równoważnościową i rozbija grupę G na rozłączne klasy abstrakcji.
Klasy sprzężoności będą odgrywały ważną rolę w dalszych wykładach. Pewne własności klas abstrakcji znajdziemy w zestawie zadań 1.

Definicja

Dla elementów a, b grupy G element $[a, b] = a^{-1}b^{-1}ab$ nazywamy **komutatorem**, a $[G, G] = (\{[a, b] : a, b \in G\})$ nazywamy **komutantem** grupy G.

Twierdzenie

- $[G, G] \triangleleft G$,

Elementy a i b grupy G nazywamy **sprzężonymi**, jeśli istnieje element $c \in G$ taki, że $a = c^{-1}bc$.
Relacja sprzężenia jest relacją równoważnościową i rozbija grupę G na rozłączne klasy abstrakcji.
Klasy sprzężoności będą odgrywały ważną rolę w dalszych wykładach. Pewne własności klas abstrakcji znajdziemy w zestawie zadań 1.

Definicja

Dla elementów a, b grupy G element $[a, b] = a^{-1}b^{-1}ab$ nazywamy **komutatorem**, a $[G, G] = (\{[a, b] : a, b \in G\})$ nazywamy **komutantem** grupy G.

Twierdzenie

- $[G, G] \triangleleft G$,
- $\operatorname{im}\varphi$ jest grupą abelową wtedy i tylko wtedy, gdy $[G, G] \subseteq \ker\varphi$.

Elementy a i b grupy G nazywamy **sprzężonymi**, jeśli istnieje element $c \in G$ taki, że $a = c^{-1}bc$.
Relacja sprzężenia jest relacją równoważnościową i rozbija grupę G na rozłączne klasy abstrakcji.
Klasy sprzężoności będą odgrywały ważną rolę w dalszych wykładach. Pewne własności klas abstrakcji znajdziemy w zestawie zadań 1.

Definicja

Dla elementów a, b grupy G element $[a, b] = a^{-1}b^{-1}ab$ nazywamy **komutatorem**, a $[G, G] = (\{[a, b] : a, b \in G\})$ nazywamy **komutantem** grupy G.

Twierdzenie

- $[G, G] \triangleleft G$,
- $\operatorname{im}\varphi$ jest grupą abelową wtedy i tylko wtedy, gdy $[G, G] \subseteq \ker\varphi$.
- $[G, G] < H < G \Longrightarrow H \triangleleft G$.

Definicja

Centrum grupy G nazywamy zbiór

$$Z(G) = \{a \in G; \underset{b \in G}{\forall} ab = ba\}.$$

Definicja

Centrum grupy G nazywamy zbiór

$$Z(G) = \{a \in G; \underset{b \in G}{\forall} ab = ba\}.$$

Uwagi

- $Z(G) \triangleleft G$,

Definicja

Centrum grupy G nazywamy zbiór

$$Z(G) = \{a \in G; \underset{b \in G}{\forall} ab = ba\}.$$

Uwagi

- $Z(G) \triangleleft G$,
- $Z(G) = G \iff G$ jest grupą abelową ,

Definicja

Centrum grupy G nazywamy zbiór

$$Z(G) = \{a \in G; \underset{b \in G}{\forall} ab = ba\}.$$

Uwagi

- $Z(G) \triangleleft G$,
- $Z(G) = G \iff G$ jest grupą abelową ,
- jeśli $G/Z(G)$ jest grupą cykliczną, to G jest grupą abelową (patrz zadanie 2 w zestawie 1.