

Paweł Gładki

Elementy algebry abstrakcyjnej A

<http://www.math.us.edu.pl/~pgladki/>

Konsultacje:

Środa, 15:00-16:00, p. 527, Bankowa 14 (co 2 tyg.)

Jeżeli chcesz spotkać się z prowadzącym podczas konsultacji, postaraj się powiadomić go o tym przed lub po zajęciach, zadzwoń do jego pokoju, lub wyślij mu emaila.

Zasady zaliczania przedmiotu:

- ▶ 2 kolokwia, każde warte 15 punktów,
- ▶ 2 sprawdziany, każdy warty 6 punktów,
- ▶ aktywność na zajęciach, warta 3 punkty,
- ▶ egzamin, warty 55 punktów.

Do egzaminu przystępują tylko te osoby, które uzyskają zaliczenie z ćwiczeń.

Warunkiem zaliczenia ćwiczeń jest zdobycie co najmniej 25 punktów.

Warunkiem zdania egzaminu jest zdobycie co najmniej 60 punktów.

Każde kolokwium będzie trwało 90 minut, każdy sprawdzian 20 minut, a egzamin końcowy 180 minut.

Sprawdziany odbędą się na zajęciach w tygodniach:

- ▶ **13–18 marca**
- ▶ **15–19 maja**

Kolokwia odbędą się na zajęciach w tygodniach:

- ▶ **3–7 kwietnia**
- ▶ **5–9 czerwca**

Egzamin odbędzie się

- ▶ **12 czerwca.**

Plan wykładu:

- 02.22 Grupy i izomorfizmy grup. Podgrupy, podgrupy generowane przez zbiór.
- 03.01 Warstwy grupy względem podgrupy. Twierdzenie Lagrange'a. Rząd elementu grupy. Grupy cykliczne.
- 03.08 Homomorfizmy grup, podgrupy normalne. Grupa ilorazowa, twierdzenie o homomorfizmie.
- 03.15 Grupy permutacji.
- 03.22 Pojęcie pierścienia. Podpierścienie, podpierścienie generowane przez zbiór. Specjalne typy elementów pierścienia.

- 03.29 Homomorfizmy pierścieni, ideały pierścieni. Ideały generowane przez zbiór. Ideały pierwsze i maksymalne.
- 04.05 Konstrukcja pierścienia wielomianów jednej zmiennej. Wartość wielomianu, pierwiastki wielomianu, funkcja wielomianowa. Wielokrotne pierwiastki wielomianów. Różniczkowanie wielomianów.
- 04.12 Wielomiany wielu zmiennych. Wielomiany symetryczne.
- 04.19 Lokalizacja pierścienia względem zbioru mnożliwatywnego. Pierścień lokalny.
- 04.26 Podstawowe pojęcia teorii podzielności.

- 05.10 Podciała, podciała generowane przez zbiór, rozszerzenia ciał. Charakterystyka pierścienia i ciała, ciała proste i klasyfikacja ciał prostych.
- 05.17 Rozszerzenie ciała o pierwiastek wielomianu. Ciało rozkładu wielomianu. Ciało algebraicznie domknięte.
- 05.24 Baza i stopień rozszerzenia. Elementy algebraiczne i przestępne. Rozszerzenia algebraiczne i skończone. Algebraiczne domknięcie ciała.
- 05.31 Ciała skończone.
- 06.07 Struktura grupy elementów odwracalnych ciała skończonego.

Literatura:

1. Białynicki-Birula, *Algebra*, PWN, Warszawa 2009.
2. A.I. Kostrykin, *Wstęp do algebry*, PWN, Warszawa 2004.
3. W. Marzantowski, P. Zarzycki, *Elementarna teoria liczb*, PWN, Warszawa 2006.
4. A. Iwaszkiewicz-Rudoszańska, *Wstęp do algebry i teorii liczb*, Wydawnictwo UAM, Poznań 2009.
5. A. Mostowski, M. Stark, *Elementy algebry wyższej*, PWN, Warszawa 1968.
6. W. Narkiewicz, *Teoria liczb*, PWN, Warszawa 2003.
7. W. Sierpiński, *Arytmetyka teoretyczna*, PWN, Warszawa 1967.

Grupy i izomorfizmy grup.

Definicja

Niech A będzie niepustym zbiorem.

Działaniem wewnętrznym (lub, krótko, działaniem) w zbiorze A nazywamy funkcję $*$: $A \times A \rightarrow A$.

Niech ponadto B będzie niepustym zbiorem.

Działaniem zewnętrznym w zbiorze A nazywamy funkcję $*$: $B \times A \rightarrow A$.

Uwaga

To, że w zbiorze A określono działanie wewnętrzne $$ w szczególności oznacza, że:*

1. $\forall x, y \in A [*(x, y) \text{ istnieje}],$
2. $\forall x, y \in A [*(x, y) \in A].$

Zamiast (x, y) będziemy na ogół pisać $x * y$.*

Podobnie, jeśli $B \neq \emptyset$, to to, że w zbiorze A określono działanie zewnętrzne $\diamond$ w szczególności oznacza, że:

1. $\forall a \in B \forall x \in A [\diamond(a, x) \text{ istnieje}],$
2. $\forall a \in B \forall x \in A [\diamond(a, x) \in A].$

Zamiast $\diamond(a, x)$ będziemy na ogół pisać $a \diamond x$.

Na tym wykładzie będziemy zajmować się prawie wyłącznie działaniami wewnętrznymi.

Przykłady:

1. Dodawanie liczb naturalnych jest działaniem w zbiorze $\mathbb{N}$. Zauważmy, że dodawanie możemy formalnie zdefiniować rekurencyjnie jako funkcję $d : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$ warunkiem:

$$d(x, y) = \begin{cases} d(x, 0) = x \\ d(x, S(y)) = S(d(x, y)), \end{cases}$$

gdzie $S : \mathbb{N} \rightarrow \mathbb{N}$ oznacza funkcję następnika liczb naturalnych.

Symbol “+” dla oznaczenia dodawania wprowadził w 1489 roku Johannes Widmann.

2. Mnożenie liczb naturalnych jest działaniem w zbiorze $\mathbb{N}$. Podobnie jak dodawanie, mnożenie możemy zdefiniować rekurencyjnie jako funkcję $m : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$ daną warunkiem:

$$m(x, y) = \begin{cases} m(x, 0) = 0, \\ m(x, S(y)) = m(x, y) + x, \end{cases}$$

gdzie, jak poprzednio, $S : \mathbb{N} \rightarrow \mathbb{N}$ oznacza funkcję następnika liczb naturalnych.

Znak “ $\times$ ” dla oznaczenia mnożenia wprowadził w 1631 roku William Oughtred, zaś symbol “ $\cdot$ ” zaproponował Gottfried Wilhelm von Leibniz w roku 1698.

3. Odejmowanie i dzielenie nie są działaniami w zbiorze $\mathbb{N}$:
 $3 - 5 \notin \mathbb{N}$ oraz $1 \div 2 \notin \mathbb{N}$.

Z drugiej strony, odejmowanie jest działaniem w $\mathbb{Z}$, a dzielenie jest działaniem w $\mathbb{Q} \setminus \{0\}$.

4. Mnożenie wektorów na płaszczyźnie przez skalary rzeczywiste jest przykładem działania zewnętrznego.

Definicja

Niech A będzie niepustym zbiorem, a $*$ i $\circ$ działaniami w A .

1. Mówimy, że $*$ jest **łączne**, jeżeli

$$\forall x, y, z \in A [x * (y * z) = (x * y) * z].$$

2. Mówimy, że $*$ jest **przemienne**, jeżeli

$$\forall x, y \in A [x * y = y * x].$$

3. Mówimy, że $*$ ma **element neutralny** e , jeżeli

$$\forall x \in A [x * e = e * x = x].$$

4. Mówimy, że y jest **elementem odwrotnym** do x , jeżeli

$$x * y = y * x = e.$$

5. Mówimy, że $\circ$ jest **rozdzielne** względem $*$, jeżeli

$$\forall x, y, z \in A [x \circ (y * z) = x \circ y * x \circ z].$$

Przykłady:

5. Dodawanie i mnożenie liczb naturalnych są łączne i przemienne.

0 jest elementem neutralnym dodawania, a 1 jest elementem neutralnym mnożenia.

Ponadto mnożenie jest rozdzielne względem dodawania.

1 nie ma elementu odwrotnego względem dodawania, a 2 nie ma elementu odwrotnego względem mnożenia.

6. Rozważmy dodawanie i mnożenie liczb całkowitych.

Każda liczba całkowita ma element odwrotny względem dodawania, ale 2 nie ma elementu odwrotnego względem mnożenia.

7. Rozważmy dodawanie i mnożenie liczb wymiernych.

Każda liczba wymierna ma element odwrotny względem dodawania i każda niezerowa liczba wymierna ma element odwrotny względem mnożenia.

8. Rozważmy dowolny niepusty zbiór X i rodzinę A wszystkich funkcji $f : X \rightarrow X$ oraz działanie składania funkcji.

Jest to działanie łączne, ale nie jest przemienne.

Funkcja identycznościowa $X \ni x \mapsto x \in X$ jest elementem neutralnym tego działania, a jedyne funkcje, które mają elementy odwrotne, to funkcje różnowartościowe.

Definicja

1. **Algebrą** nazywamy ciąg

$$(A, *_1, \dots, *_n, B_1, \dots, B_m, \cdot_1, \dots, \cdot_m),$$

gdzie A jest niepustym zbiorem, $*_1, \dots, *_n$ działaniami wewnętrznymi w zbiorze A , a $\cdot_1, \dots, \cdot_m$ działaniami zewnętrznymi w zbiorze A (wraz z odpowiadającymi im zbiorami $B_1, \dots, B_m$).

2. **Grupą** nazywamy algebrę $(G, *)$, gdzie $*$ jest łączne, ma element neutralny i każdy element w zbiorze G ma element odwrotny.

Jeżeli ponadto $*$ jest przemienne, to grupę $(G, *)$ nazywamy przemienną (lub abelową).

Przykłady:

9. Przykładami algebr znanymi z wykładu z algebry liniowej są ciała, czyli algebry $(F, +, \cdot)$, gdzie $+$ i $\cdot$ są działaniami łącznymi, przemiennymi, mającymi elementy neutralne, odpowiednio, 0 i 1 oraz takie, że każdy element zbiorów, odpowiednio, F i F^* ma element odwrotny.

Przykładami algebr, w których występują działania zewnętrzne, są przestrzenie liniowe, czyli algebry $(V, +, F, \cdot)$, gdzie $+$ jest działaniem wewnętrznym zbioru F , które jest łączne, przemienne, ma element neutralny i względem którego każdy element zbioru V ma element odwrotny, natomiast $\cdot : F \times V \rightarrow V$ jest pewnym działaniem zewnętrznym, przy czym F jest ciałem.

10. **Grupy liczbowe.** $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$ są przykładami grup przemiennych. $(\mathbb{N}, +)$ nie jest grupą. Podobnie $(\mathbb{Q}^*, \cdot)$, $(\mathbb{R}^*, \cdot)$, $(\mathbb{C}^*, \cdot)$, gdzie $A^* = A \setminus \{0\}$, są grupami przemiennymi. $(\mathbb{N}^*, \cdot)$ i $(\mathbb{Z}^*, \cdot)$ nie są grupami.

11. **Grupy pochodzące od ciała.** Uogólniając poprzedni przykład, dla dowolnego ciała $(F, +, \cdot)$ algebry $(F, +)$ oraz $(F^*, \cdot)$ są grupami przemiennymi.

12. **Grupy reszt.** Niech $n \in \mathbb{N}$ i oznaczmy przez $\mathbb{Z}_n = \{0, 1, \dots, n-1\}$. W zbiorze $\mathbb{Z}_n$ definiujemy **dodawanie modulo n** :

$$x \oplus_n y = \text{reszta z dzielenia } x + y \text{ przez } n$$

oraz **mnożenie modulo n** :

$$x \otimes_n y = \text{reszta z dzielenia } x \cdot y \text{ przez } n.$$

Niech ponadto

$$U(\mathbb{Z}_n) = \{k \in \mathbb{Z}_n : NWD(k, n) = 1\}.$$

$(\mathbb{Z}_n, \oplus_n)$ i $(U(\mathbb{Z}_n), \otimes_n)$ są przykładami grup przemennych. $(\mathbb{Z}_n^*, \otimes_n)$ na ogół nie jest grupą, chyba że n jest liczbą pierwszą – wówczas $\mathbb{Z}_n^* = U(\mathbb{Z}_n)$.

13. Grupy macierzy. Niech F będzie dowolnym ciałem, niech $M(n, F)$ oznacza zbiór macierzy kwadratowych stopnia n o współczynnikach z ciała F .

$(M(n, F), +)$ jest grupą przemienną, przy czym $+$ oznacza tu dodawanie macierzy.

Niech

$$GL(n, F) = \{A \in M(n, F) : \det A \neq 0\}.$$

$(GL(n, F), \cdot)$ jest grupą, która na ogół nie jest przemienna, przy czym $\cdot$ oznacza tu mnożenie macierzy.

Grupe tę nazywamy **grupą liniową stopnia n nad ciałem F** .

Niech

$$SL(n, F) = \{A \in M(n, F) : \det A = 1\}.$$

$(SL(n, F), \cdot)$ jest grupą, która na ogół nie jest przemienna.

Grupe tę nazywamy **specjalną grupą liniową stopnia n nad ciałem F** .

14. **Grupy związane z przestrzenią liniową.** Niech V będzie przestrzenią liniową. $(V, +)$ jest grupą przemenną, przy czym $+$ oznacza tu dodawanie wektorów.

Oznaczmy przez $Aut(V)$ zbiór automorfizmów liniowych przestrzeni V .

$(Aut(V), \circ)$ jest grupą, która na ogół nie jest przemienna, przy czym $\circ$ jest tu działaniem składania przekształceń liniowych.

Załóżmy, że w przestrzeni V zdefiniowaliśmy funkcjonal dwuliniowy ξ określający na V strukturę przestrzeni euklidesowej.

Oznaczmy przez $O(V)$ zbiór automorfizmów ortogonalnych przestrzeni V .

$(O(V), \circ)$ jest grupą, która na ogół nie jest przemienna.

Grupę tę nazywamy **grupą ortogonalną przestrzeni (V, ξ)** .

15. **Grupy funkcji.** Niech $(G, *)$ będzie grupą, niech $X \neq \emptyset$.
W rodzinie funkcji

$$G^X = \{f : X \rightarrow G : f \text{ jest funkcją}\}$$

definiujemy działanie

$$(f \diamond g)(x) = f(x) * g(x).$$

$(G^X, \diamond)$ jest grupą, która jest przemienna, gdy G jest przemienna.

16. **Grupy zadane tabelkami Cayleya.** Działania w grupach często wygodnie jest zapisywać w tabelkach Cayleya.

Na przykład tabelka działań w grupie $(\mathbb{Z}_5^*, \otimes_5)$ wygląda następująco:

$\otimes_5$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

Przykładem grupy zadanej przez tabelkę Cayleya, która nie ma odpowiednika wśród grup liczbowych, jest **grupa czwórkowa Kleina** $(K_4, \cdot)$, gdzie $K_4 = \{a, b, c, d\}$ oraz działanie $\cdot$ zdefiniowane jest następująco:

$\cdot$	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	a	b
d	d	c	b	a

17. Grupy przekształceń. Niech $X \neq \emptyset$, niech

$$S(X) = \{f : X \rightarrow X : f \text{ jest bijekcją}\}.$$

$(S(X), \circ)$ jest grupą, która na ogół nie jest przemienna, przy czym $\circ$ oznacza tu działanie składania funkcji.

Jeśli $X = \{1, 2, \dots, n\}$, to grupę $S(X)$ oznaczamy przez $S(n)$ i nazywamy **grupą symetryczną stopnia n** albo **grupą permutacji stopnia n** .

Dla grup symetrycznych przyjmujemy następującą notację: jeśli $\sigma \in S(n)$ i $\sigma(1) = i_1, \dots, \sigma(n) = i_n$, to piszemy

$$\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix}.$$

Na przykład dla $n = 3$ elementy grupy $S(3)$ to następujące funkcje:

$$\begin{array}{lll} id_3 : \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} & o_1 : \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} & o_2 : \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \\ s_1 : \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} & s_2 : \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} & s_3 : \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}. \end{array}$$

Tym samym tabelka działań w grupie $S(3)$ wygląda następująco:

$\circ$	id_3	o_1	o_2	s_1	s_2	s_3
id_3	id_3	o_1	o_2	s_1	s_2	s_3
o_1	o_1	o_2	id_3	s_2	s_3	s_1
o_2	o_2	id_3	o_1	s_3	s_1	s_2
s_1	s_1	s_3	s_2	id_3	o_2	o_1
s_2	s_2	s_1	s_3	o_1	id_3	o_2
s_3	s_3	s_2	s_1	o_2	o_1	id_3

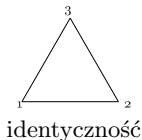
Widzimy, że jest to przykład grupy nieprzemiennej:

$$s_1 \circ o_1 = s_2 \text{ ale } o_1 \circ s_1 = s_3.$$

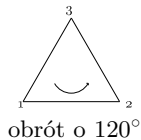
18. **Grupy izometrii własnych n -kąta foremnego.** Dla $n \geq 3$, $n \in \mathbb{N}$, oznaczmy przez $D(n)$ zbiór izometrii własnych n -kąta foremnego.
 $(D(n), \circ)$ jest grupą.

Na przykład grupa $D(3)$ składa się z następujących izometrii trójkąta równobocznego:

$ID_3 :$



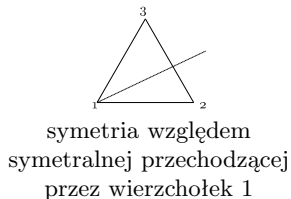
$O_1 :$



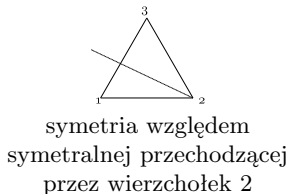
$O_2 :$



$S_1 :$



$S_2 :$



$S_3 :$

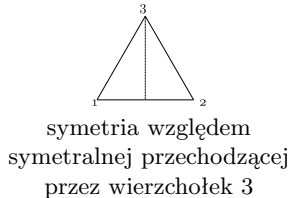


Tabela działań w grupie $D(3)$ wygląda zatem następująco:

$\circ$	ID_3	O_1	O_2	S_1	S_2	S_3
ID_3	ID_3	O_1	O_2	S_1	S_2	S_3
O_1	O_1	O_2	ID_3	S_2	S_3	S_1
O_2	O_2	ID_3	O_1	S_3	S_1	S_2
S_1	S_1	S_3	S_2	ID_3	O_2	O_1
S_2	S_2	S_1	S_3	O_1	ID_3	O_2
S_3	S_3	S_2	S_1	O_2	O_1	ID_3

.

19. Skończony produkt grup. Niech $(G_1, *_1), \dots, (G_n, *_n)$ będą grupami.

W produkcie kartezjańskim $G = G_1 \times \dots \times G_n$ definiujemy działanie “po współrzędnych”:

$$(a_1, \dots, a_n) * (b_1, \dots, b_n) = (a_1 *_1 b_1, \dots, a_n *_n b_n).$$

$(G, *)$ jest grupą.

Jako przykład rozważmy grupy $(\mathbb{Z}_2, \oplus_2)$ i $(\mathbb{Z}_2, \oplus_2)$. Wówczas

$$\mathbb{Z}_2 \times \mathbb{Z}_2 = \{(0, 0), (0, 1), (1, 0), (1, 1)\}$$

i tabelka działań wygląda następująco:

*	(0, 0)	(0, 1)	(1, 0)	(1, 1)
(0, 0)	(0, 0)	(0, 1)	(1, 0)	(1, 1)
(0, 1)	(0, 1)	(0, 0)	(1, 1)	(1, 0)
(1, 0)	(1, 0)	(1, 1)	(0, 0)	(0, 1)
(1, 1)	(1, 1)	(1, 0)	(0, 1)	(0, 0)

Definicja

Niech $(G_1, *_1)$ i $(G_2, *_2)$ będą grupami.

Funkcję $f : G_1 \rightarrow G_2$ nazywamy **izomorfizmem grup**, jeżeli jest bijekcją i spełniony jest warunek

$$\forall x, y \in G_1 [f(x *_1 y) = f(x) *_2 f(y)].$$

Jeżeli istnieje izomorfizm $f : G_1 \rightarrow G_2$, to grupy G_1 i G_2 nazywamy **izomorficznymi**, co oznaczamy przez $G_1 \cong G_2$.

Przykłady:

20. Grupy $S(3)$ i $D(3)$ są izomorficzne.

Istotnie, rozważmy funkcję $f : S(3) \rightarrow D(3)$, którą, dla wygody oznaczeń, zdefiniujemy tabelką jako:

σ	id_3	o_1	o_2	s_1	s_2	s_3
$f(\sigma)$	ID_3	O_1	O_2	S_1	S_2	S_3

Oczywiście jest to bijekcja.

Porównując tabelki działań w $S(3)$ i $D(3)$ widzimy, że jest to też izomorfizm grup.

21. Grupy K_4 i $\mathbb{Z}_2 \times \mathbb{Z}_2$ są izomorficzne.

Istotnie, izomorfizm ustala funkcja $f : K_4 \rightarrow \mathbb{Z}_2 \times \mathbb{Z}_2$ dana tabelką

x	a	b	c	d
$f(x)$	$(0, 0)$	$(0, 1)$	$(1, 0)$	$(1, 1)$

W dowolnej grupie $(G, *)$ wprowadzamy oznaczenie

$$\prod_{i=1}^n x_i = x_1 * \dots * x_n.$$

W szczególności $\prod_{i=1}^n x = x^n$.

Tradycyjnie używamy w teorii grup dwóch równoległych terminologii, addytywnej i mnożymy, według następującego schematu:

Definicja	Notacja addytywna	Notacja mnożymy
działanie	$+$ dodawanie suma	$\cdot$ mnożenie iloczyn
element neutralny	0 zero	1 jedyńska
potęga	nx wielokrotność	x^n potęga
element odwrotny	$-x$ element przeciwny	x^{-1} element odwrotny

Twierdzenie

Niech $(G, *)$ będzie grupą. Wówczas:

1. *element neutralny e jest wyznaczony jednoznacznie;*
2. $\prod_{i=1}^m x_i * \prod_{j=m+1}^{m+n} x_j = \prod_{k=1}^{m+n} x_k$, dla $x_1, \dots, x_{m+n} \in G$;
3. $x^{m+n} = x^m x^n$, dla $x \in G$;
4. $(x^m)^n = x^{mn}$, dla $x \in G$;
5. *element odwrotny jest wyznaczony jednoznacznie;*
6. $(x_1^{n_1} * \dots * x_k^{n_k})^{-1} = x_k^{-n_k} * \dots * x_1^{-n_1}$, dla $x_1, \dots, x_k \in G$;
7. $(x^{-1})^{-1} = x$, dla $x \in G$;
8. $(x^{-1} * y * x)^n = x^{-1} * y^n * x$, dla $x, y \in G$;
9. jeżeli $x * y = x * z$, to $y = z$ oraz jeżeli $y * x = z * x$, to $y = z$ (**prawo skracania**).

Dowód.

Udowodnimy dla przykładu część (1):

jeśli e i e' są dwoma elementami neutralnymi, to wówczas

$$e = e * e' = e'$$

.



Podgrupy, podgrupy generowane
przez zbiór.

Definicja

Niech $(G, \cdot)$ będzie grupą.

Podzbiór $H \neq \emptyset$ zbioru G nazywamy **podgrupą** grupy G (piszemy $H < G$), gdy $(H, \cdot|_{H \times H})$ jest grupą.

Przykłady:

1. $\mathbb{Z} < \mathbb{R}$ z dodawaniem;
2. $\mathbb{R}^* < \mathbb{C}^*$ z mnożeniem;
3. $SL(n, F) < GL(n, F)$ z mnożeniem macierzy;
4. $\mathbb{Z}_n$ nie jest podgrupą grupy $\mathbb{Z}$.

Twierdzenie

Niech $\emptyset \neq H \subset G$ i niech $(G, \cdot)$ będzie grupą.

Następujące warunki są równoważne:

1. $H < G$;
2. H ma następujące własności:
 - ▶ $1_G \in H$,
 - ▶ $\forall x, y \in H (xy \in H)$,
 - ▶ $\forall x \in H (x^{-1} \in H)$;
3. H ma następującą własność:
 - ▶ $\forall x, y \in H (xy^{-1} \in H)$.

Dowód.

Równoważność $(1) \Leftrightarrow (2)$ jest oczywista.

Dla dowodu implikacji $(2) \Rightarrow (3)$ ustalmy $x, y \in H$.

Mamy, że $y^{-1} \in H$, więc $xy^{-1} \in H$.

Pozostaje udowodnić implikację $(3) \Rightarrow (1)$.

Ponieważ $H \neq \emptyset$, więc istnieje $x \in H$.

Stąd

$$1_G = xx^{-1} \in H.$$

Dalej:

$$x^{-1} = 1_G x^{-1} \in H.$$

Ustalmy $x, y \in H$.

Wówczas $y^{-1} \in H$, a zatem:

$$xy = x(y^{-1})^{-1} \in H.$$



Przykłady:

5. Zauważmy, że $\mu_n(\mathbb{C}) = \{z \in \mathbb{C}^* : z^n = 1\} < \mathbb{C}^*$.

Istotnie, ustalmy $z_1, z_2 \in \mu_n(\mathbb{C})$, a zatem niech $z_1^n = 1$ i $z_2^n = 1$.

Wówczas $(z_1 z_2^{-1})^n = (\frac{z_1}{z_2})^n = \frac{z_1^n}{z_2^n} = \frac{1}{1} = 1$, czyli $z_1 z_2^{-1} \in \mu_n(\mathbb{C})$.

6. Zauważmy, że $\{0, 2, 4\} < \mathbb{Z}_6$ z dodawaniem.

Istotnie, $0 \in \{0, 2, 4\}$, dodawanie na każdej parze nie wychodzi poza zbiór $\{0, 2, 4\}$ oraz 0 jest elementem symetrycznym dla 0, 2 dla 4 i 4 dla 2.

7. Zauważmy, że $2\mathbb{Z} = \{2k : k \in \mathbb{Z}\} < \mathbb{Z}$ z dodawaniem.

Istotnie, ustalmy $x, y \in 2\mathbb{Z}$, a zatem niech $x = 2k$ i $y = 2l$.

Wówczas $x - y = 2k - 2l = 2(k - l)$, czyli $x - y \in 2\mathbb{Z}$.

8. Zauważmy, że jeśli G jest dowolną grupą, to

$$\{1_G\} < G \text{ oraz } G < G.$$

Podgrupy te nazywamy **podgrupami niewłaściwymi**,
wszystkie pozostałe – **podgrupami właściwymi**.

Twierdzenie

Niech $\mathcal{R} = \{H_i : i \in I\}$ będzie rodziną podgrup grupy G ;

1. $\bigcap_{i \in I} H_i$ jest podgrupą grupy G ,
2. $\bigcup_{i \in I} H_i$ jest podgrupą grupy G , o ile $\mathcal{R}$ jest łańcuchem.

Dowód.

1. Oznaczmy $F = \bigcap_{i \in I} H_i$. Ustalmy $x, y \in F$.

Wtedy

$$\forall i \in I (x, y \in H_i),$$

a zatem

$$\forall i \in I (xy^{-1} \in H_i),$$

czyli $xy^{-1} \in F$.

2. Oznaczmy $F = \bigcup_{i \in I} H_i$.

Ustalmy $x, y \in F$.

Wtedy

$$\exists i_0 \in I (x, y \in H_{i_0}),$$

a zatem

$$\exists i_0 \in I (xy^{-1} \in H_{i_0}),$$

czyli $xy^{-1} \in F$.



Definicja

Niech $(G, \cdot)$ będzie grupą oraz $A \subset G$ pewnym zbiorem.

Najmniejszą w sensie inkluzji podgrupę grupy G zawierającą zbiór A (tj. przekrój wszystkich podgrup grupy G zawierających A) nazywamy **podgrupą generowaną przez A** i oznaczamy $\langle A \rangle$.

Uwaga

Podgrupa grupy G generowana przez zbiór A ma następujące własności:

1. $\langle A \rangle < G$,
2. $A \subset \langle A \rangle$,
3. *jeśli $H < G$ oraz $A \subset H$, to wtedy $\langle A \rangle < H$.*

Definicja

*Każdy zbiór A o tej własności, że $\langle A \rangle = G$ nazywamy **zbiorem generatorów** grupy G .*

Jeśli $A = \{a_1, \dots, a_n\}$ to oznaczamy

$$\langle a_1, \dots, a_n \rangle = \langle A \rangle.$$

*Mówimy, że grupa jest **skończenie generowana**, gdy istnieją elementy $g_1, \dots, g_n \in G$ takie, że*

$$G = \langle g_1, \dots, g_n \rangle.$$

Uwaga

W szczególności grupa skończenie generowana nie musi być skończona, na przykład $\mathbb{Z} = \langle 1 \rangle$.

Twierdzenie (o postaci elementów podgrupy generowanej przez zbiór)

Niech $(G, \cdot)$ będzie grupą, niech $A \subset G$.

Wówczas

$$\langle A \rangle = \{a_1^{k_1} a_2^{k_2} \dots a_n^{k_n} : n \in \mathbb{N}, k_i \in \mathbb{Z}, a_i \in A\}.$$

Dowód:

Oznaczmy

$$A_1 = \{a_1^{k_1} a_2^{k_2} \dots a_n^{k_n} : n \in \mathbb{N}, k_i \in \mathbb{Z}, a_i \in A\}.$$

Pokażemy, że $A_1 < G$.

Zauważmy, że $1_G \in A_1$:

Istotnie, weźmy $a_1 \in A$.

Wtedy z definicji potęgi $a_1^0 = 1_G \in A_1$.

Zauważmy dalej, że dla $x, y \in A_1$ zachodzi $xy \in A_1$:

Istotnie, ustalmy $x = a_1^{k_1} a_2^{k_2} \dots a_n^{k_n}$, $y = b_1^{l_1} b_2^{l_2} \dots b_m^{l_m}$, $n, m \in \mathbb{N}$, $k_i, l_i \in \mathbb{Z}$, $a_i, b_i \in A$.

Mamy:

$$xy = a_1^{k_1} a_2^{k_2} \dots a_n^{k_n} b_1^{l_1} b_2^{l_2} \dots b_m^{l_m} \in A_1.$$

Na koniec zauważmy, że dla $x \in A_1$ zachodzi $x^{-1} \in A_1$:

Istotnie, ustalmy $x = a_1^{k_1} a_2^{k_2} \dots a_n^{k_n}$, $n \in \mathbb{N}$, $k_i \in \mathbb{Z}$, $a_i \in A$.

Mamy:

$$x^{-1} = (a_1^{k_1} a_2^{k_2} \dots a_n^{k_n})^{-1} = a_n^{-k_n} a_{n-1}^{-k_{n-1}} \dots a_1^{-k_1} \in A_1.$$

Pozostaje pokazać, że $A_1 = \langle A \rangle$.

Inkluzja $(\supset)$ jest oczywista, pozostaje wykazać inkluzję $(\subset)$.

Dowód prowadzimy przez indukcję względem n .

Dla $n = 1$ ustalmy $a_1 \in A$.

Z definicji podgrupy, $a_1^{k_1}$ należy do wszystkich podgrup zawierających a_1 , a więc i zbiór A , zatem z definicji $a_1^{k_1} \in \langle A \rangle$.

Założmy, że twierdzenie zachodzi dla pewnej ustalonej liczby $n > 1$, a więc że dla $a_1, a_2, \dots, a_n \in A$, $k_1, \dots, k_n \in \mathbb{Z}$ zachodzi

$$a_1^{k_1} \dots a_n^{k_n} \in \langle A \rangle.$$

Wówczas dla dla $a_1, a_2, \dots, a_n, a_{n+1} \in A$, $k_1, \dots, k_n, k_{n+1} \in \mathbb{Z}$ zachodzi

$$\underbrace{a_1^{k_1} \dots a_n^{k_n}}_{\in \langle A \rangle} \underbrace{a_{n+1}^{k_{n+1}}}_{\in \langle A \rangle} \in \langle A \rangle.$$

Wniosek

1. Niech G będzie grupą oraz niech $a \in G$.

Wówczas

$$\langle a \rangle = \{a^k : k \in \mathbb{Z}\}.$$

2. Niech $(G, \cdot)$ będzie grupą abelową oraz niech $\{a_1, \dots, a_n\} \subset G$.

Wówczas

$$\langle a_1, \dots, a_n \rangle = \{a_1^{k_1} \dots a_n^{k_n} : k_i \in \mathbb{Z}\}.$$

Przykłady:

- 9. $\langle 1 \rangle = \mathbb{Z}$;
- 10. $\langle 1 \rangle = \mathbb{Z}_n, n \in \mathbb{N}$;
- 11. $\langle 2, 3 \rangle = \{2k + 3l : k, l \in \mathbb{Z}\} < \mathbb{Z}$;
- 12. $\langle 4, 5 \rangle = \{4^n 5^m : n, m \in \mathbb{Z}\} < \mathbb{R}^*$;

13. W grupie $D(3) = \{ID_3, O_1, O_2, S_1, S_2, S_3\}$ mamy:

$$\langle ID_3 \rangle = \{ID_3\},$$

$$\langle O_1 \rangle = \{ID_3, O_1, O_2\},$$

$$\langle O_2 \rangle = \{ID_3, O_1, O_2\},$$

$$\langle S_1 \rangle = \{ID_3, S_1\},$$

$$\langle S_2 \rangle = \{ID_3, S_2\},$$

$$\langle S_3 \rangle = \{ID_3, S_3\},$$

$$\langle O_1, S_1 \rangle = D(3);$$

14. $\mathbb{Q}^* = \langle \{\pm p_1^{k_1} \dots p_n^{k_n} : n \in \mathbb{N}, k_i \in \mathbb{Z}, p_i \in \mathbb{P}\} \rangle$, gdzie $\mathbb{P}$ oznacza zbiór liczb pierwszych;

15. W grupie $GL(n, F)$ rozważmy macierze postaci

$$T_{ij}(a) = \begin{bmatrix} 1 & 0 & \dots & 0 & \dots & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 & \dots & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 & \dots & a & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 0 & \dots & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 0 & \dots & 0 & \dots & 1 \end{bmatrix} \quad \begin{matrix} i \\ j \end{matrix} \quad \text{oraz}$$

$$O_i(a) = \begin{bmatrix} 1 & 0 & \dots & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & a & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 0 & \dots & 1 \end{bmatrix} \quad i$$

zwane, odpowiednio, **transwekcjami** oraz **dylatacjami**.

Wówczas

$$GL(n, F) = \langle \{T_{ij}(a), O_i(b) : a, b \in F, i, j \in \{1, \dots, n\}\} \rangle.$$