

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 $(z_1 z_2^{-1})^n = \left(\frac{z_1}{z_2}\right)^n = \frac{z_1^n}{z_2^n} = \frac{1}{1} = 1$, 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

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

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

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

Wówczas

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