Algebra I

Wykład III

Grzegorz Bobiński (UMK)

Definicja

Podzbiór Y półgrupy X nazywamy podpółgrupą, jeśli

$$\forall_{y_1,y_2 \in Y}\ y_1 \cdot y_2 \in Y.$$

Uwaga

Jeśli Y jest podpółgrupą półgrupy X, to funkcja $\cdot|^{Y}_{Y\times Y}\colon Y \times Y \to Y$ jest działaniem w zbiorze Y, które również oznaczamy symbolem $\cdot$.

Wtedy $(Y, \cdot)$ jest półgrupą.

Innymi słowy, podzbiór Y półgrupy X jest podpółgrupą, jeśli zbiór Y wraz z funkcją $\cdot := \cdot|^{Y}_{Y\times Y}$ jest (poprawnie zdefiniowaną) półgrupą.

Definicja

Zbiór Y nazywamy podmonoidem/podgrupą monoidu/grupy X, jeśli Y jest podpółgrupą półgrupy X oraz $(Y, \cdot)$ jest monoidem/grupą.

Zbiór S nazywamy podpierścieniem pierścienia R, jeśli S jest podgrupą grupy addytywnej pierścienia R oraz S jest podmonoidem monoidu multiplikatywnego pierścienia R.

Uwaga

Zbiór S jest podpierścieniem pierścienia R wtedy i tylko wtedy, gdy S jest podpółgrupą grupy addytywnej pierścienia R, S jest podpółgrupą monoidu multiplikatywnego pierścienia R oraz $(S, +, \cdot)$ jest pierścieniem.

Terminologia i Oznaczenie

Sfromułowanie „Y jest podstrukturą struktury X" oznacza, że
X jest pierścieniem/grupą/monoidem/półgrupą, a
Y jest podpierścieniem/podgrupą/podmonoidem/podpółgrupą struktury X, odpowiednio.
Jeśli Y jest podstrukturą stuktury X, to piszemy $Y \leq X$.

Uwaga

Jeśli $Y \leq X$ i $Z \leq Y$ (tego samego typu), to $Z \leq X$, tj. relacja bycia podstrukturą jest przechodnia.

Stwierdzenie 1.7/Definicja

Jeśli $Y \leq X$, to odwzorowanie $\mu\colon Y \to X$, $\mu(y) := y$, $y \in Y$, jest monomorfizmem, który nazywamy naturalnym włożeniem.

Dowód

Mamy

$$\mu(y_1 \cdot y_2) = y_1 \cdot y_2 = \mu(y_1) \cdot \mu(y_2). \quad \square$$

Stwierdzenie 1.8

(1) Podzbiór Y monoidu X jest podmonoidem wtedy i tylko wtedy, gdy spełnione są warunki:

(a) jeśli $y_1, y_2 \in Y$, to $y_1 \cdot y_2 \in Y$;
(b) istnieje $e \in Y$ taki, że

$$\forall_{y \in Y}\ e \cdot y = y = y \cdot e.$$

(2) Podzbiór H grupy G jest podgrupą wtedy i tylko wtedy, gdy spełnione są warunki:

(a) jeśli $h_1, h_2 \in H$, to $h_1 \cdot h_2 \in H$;
(b) $1 \in H$;
(c) jeśli $h \in H$, to $h^{-1} \in H$.

(3) Podzbiór S pierścienia R jest podpierścieniem wtedy i tylko wtedy, gdy spełnione są warunki:

(a) jeśli $s_1, s_2 \in S$, to $s_1 + s_2 \in S$;
(b) $0 \in S$;
(c) jeśli $s \in S$, to $-s \in S$;
(d) jeśli $s_1, s_2 \in S$, to $s_1 \cdot s_2 \in S$;
(e) istnieje $e \in S$ taki, że

$$\forall_{s \in S}\ e \cdot s = s = s \cdot e.$$

Dowód

(1) Oczywiste.

(3) Natychmiast z (1) i (2).

Stwierdzenie 1.8

(2) Podzbiór H grupy G jest podgrupą wtedy i tylko wtedy, gdy spełnione są warunki:

(a) jeśli $h_1, h_2 \in H$, to $h_1 \cdot h_2 \in H$;
(b) $1 \in H$;
(c) jeśli $h \in H$, to $h^{-1} \in H$.

Dowód (kont.)

(2) $\Leftarrow$: Oczywiste.

$\Rightarrow$: Musimy pokazać, że jeśli $H \leq G$, to (b) i (c), tzn. $1 \in H$ oraz $\forall_{h \in H}\ h^{-1} \in H$.

Ponieważ H jest podmonoidem grupy G, więc na mocy (1) istnieje $e \in H$ taki, że $e \cdot e = e$.

Wtedy

$$1 = e \cdot e^{-1} = e \cdot e \cdot e^{-1} = e \cdot 1 = e \in H.$$

W szczególności, 1 jest elementem neutralnym grupy H.

Ustalmy teraz $h \in H$.

Istnieje $l \in H$ takie, że $h \cdot l = 1$.

Wtedy

$$h^{-1} = h^{-1} \cdot 1 = h^{-1} \cdot h \cdot l = 1 \cdot l = l \in H. \quad \square$$

Uwaga

Z powyższego dowodu wynika, że jeśli G jest grupą, a Y jest podmonoidem grupy G, to $1 \in Y$.

Przykłady (podgrup)

- Jeśli G jest grupą, to $\{1\}, G \leq G$.
- Jeśli $n \in \mathbb{Z}$, to $n\mathbb{Z} := \{k \in \mathbb{Z} : n \mid k\} \leq \mathbb{Z}$.
- Jeśli $F = \mathbb{Q}$ lub $F = \mathbb{R}$, to $F_+ \leq F^\times$.
- $\mathbb{T} := \{z \in \mathbb{C} : |z| = 1\} \leq \mathbb{C}^\times$.
- Jeśli $n \in \mathbb{N}_+$, to i $A_n := \{\sigma \in S_n : \operatorname{sgn}\sigma = 1\} \leq S_n$. A_n nazywamy n-tą grupą alternującą.
- Jeśli V jest przestrzenią liniową, to
  $\mathrm{GL}(V) := \{f\colon V \to V : f$ jest odwracalnym przekształceniem liniowym$\} \leq S_V$.
- Jeśli G jest grupą, to $\mathrm{Aut}(G) := \{\varphi\colon G \to G : \varphi$ jest automorfizmem grupy $G\} \leq S_G$.
- Jeśli F jest ciałem, $n \in \mathbb{N}_+$ i $\mathrm{SL}_n(F) := \{A \in \mathrm{GL}_n(F) : \det A = 1\} \leq \mathrm{GL}_n(F)$.

Przykłady (podpierścieni)

- Jeśli R jest pierścieniem, to $\{0\}, R \leq R$.
- $\mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R} \leq \mathbb{C}$.
- Jeśli R jest pierścieniem i $S \leq R$, to $S[X] \leq R[X]$.
- Jeśli R jest pierścieniem, to $R[X] \leq R[[X]]$.
- Jeśli $n \in \mathbb{N}_+$ i R jest pierścieniem, to $R[X^n] := \{\sum_k a_k X^{nk}\} \leq R[X]$.
- $\{0, 2, 4\} \leq \mathbb{Z}_6$.
  Zauważmy, że $1 \notin \{0, 2, 4\}$, ale $4 \cdot 0 = 0$, $4 \cdot 2 = 2$ i $4 \cdot 4 = 4$.
- Zbiór funkcji ciągłych $[0, 1] \to \mathbb{R}$ jest podpierścieniem pierścienia $R^{[0,1]}$.

Stwierdzenie 1.9

Niech G będzie grupą i $H \subseteq G$.
Wtedy $H \leq G$ wtedy i tylko wtedy, gdy $H \neq \varnothing$ i

$$\forall_{h_1, h_2 \in H}\ h_1 \cdot h_2^{-1} \in H.$$

Przypomnienie

(1.8)(2): $H \leq G \iff$

(a) jeśli $h_1, h_2 \in H$, to $h_1 \cdot h_2 \in H$;

(b) $1 \in H$;

(c) jeśli $h \in H$, to $h^{-1} \in H$.

Dowód

$\Rightarrow$: Załóżmy, że $H \leq G$.
Wtedy $1 \in H$, więc $H \neq \varnothing$.
Jeśli $h_1, h_2 \in H$, to $h_2^{-1} \in H$, więc $h_1 \cdot h_2^{-1} \in H$.
$\Leftarrow$: Wybierzmy $h_0 \in H$ (wiemy, że $H \neq \varnothing$).
Wtedy $1 = h_0 \cdot h_0^{-1} \in H$.
Jeśli $h \in H$, to $h^{-1} = 1 \cdot h^{-1} \in H$.
Jeśli $h_1, h_2 \in H$, to $h_2^{-1} \in H$, więc $h_1 \cdot h_2 = h_1 \cdot (h_2^{-1})^{-1} \in H$. $\square$

Definicja

Jeśli $\varphi\colon X \to Y$ jest homomorfizmem, to

$$\operatorname{Im}\varphi := \varphi(X)(= \{\varphi(x) : x \in X\}).$$

$\operatorname{Im}\varphi$ nazywamy obrazem homomorfizmu φ.

Stwierdzenie 1.10

Jeśli $\varphi\colon X \to Y$ jest homomorfizmem oraz $X' \leq X$, to $\varphi(X') \leq Y$.
W szczególności, $\operatorname{Im}\varphi \leq Y$.

Stwierdzenie 1.10

Jeśli $\varphi\colon X \to Y$ jest homomorfizmem oraz $X' \leq X$, to $\varphi(X') \leq Y$.

Przypomnienie

(1.8)(3): $S \leq R \iff$

(a) jeśli $s_1, s_2 \in S$, to $s_1 + s_2 \in S$; ✓

(b) $0 \in S$;

(c) jeśli $s \in S$, to $-s \in S$;

(d) jeśli $s_1, s_2 \in S$, to $s_1 \cdot s_2 \in S$; ✓

(e) istnieje $e \in S$ taki, że $e \cdot s = s = s \cdot e$ dla wszystkich $s \in S$.

Dowód

Udowodnimy to stwierdzenie w przypadku pierścieni (korzystając z (1.8)(3)).
(a)+(d): Załóżmy, że $y_1, y_2 \in \varphi(X')$.
Z definicji istnieją $x_1, x_2 \in X'$ takie, że

$$\varphi(x_1) = y_1 \qquad \text{i} \qquad \varphi(x_2) = y_2.$$

Ponieważ $X' \leq X$, więc $x_1 + x_2, x_1 \cdot x_2 \in X'$ ((1.8)(3)(a)+(d) dla $S = X'$ i $R = X$).
Wtedy

$$y_1 + y_2 = \varphi(x_1) + \varphi(x_2) = \varphi(x_1 + x_2) \in \varphi(X').$$

Analogicznie,

$$y_1 \cdot y_2 = \varphi(x_1) \cdot \varphi(x_2) = \varphi(x_1 \cdot x_2) \in \varphi(X').$$

Stwierdzenie 1.10

Jeśli $\varphi\colon X \to Y$ jest homomorfizmem oraz $X' \leq X$, to $\varphi(X') \leq Y$.

Przypomnienie

(1.8)(3): $S \leq R \iff$

(a) jeśli $s_1, s_2 \in S$, to $s_1 + s_2 \in S$; ✓

(b) $0 \in S$; ✓

(c) jeśli $s \in S$, to $-s \in S$; ✓

(d) jeśli $s_1, s_2 \in S$, to $s_1 \cdot s_2 \in S$; ✓

(e) istnieje $e \in S$ taki, że $e \cdot s = s = s \cdot e$ dla wszystkich $s \in S$. ✓

(1.5): $\varphi(0_R) = 0_S$ i $\varphi(-r) = -\varphi(r)$.

Dowód (kont.)

(b): $0_X \in X'$ ((1.8)(b) dla $S = X'$). Z (1.5) wynika, że

$$0_Y = \varphi(0_X) \in \varphi(X').$$

(c) + (e): Jeśli $y \in \varphi(X')$, to z definicji istnieje $x \in X'$ taki, że $y = \varphi(x)$.
Wtedy $-x \in X'$ ((1.8)(c) dla $S = X'$) i z (1.5) wynika, że

$$-y = -\varphi(x) = \varphi(-x) \in \varphi(X').$$

Ponadto, jeśli e jest elementem neutralnym dla mnożenia w X' (istnieje na mocy (1.8)(e) dla $S = X'$), to

$$\varphi(e) \cdot y = \varphi(e) \cdot \varphi(x) = \varphi(e \cdot x) = \varphi(x) = y.$$

Podobnie,

$$y \cdot \varphi(e) = y. \quad \square$$

Definicja

Jeśli $\varphi\colon G \to H$ jest homomorfizmem grup, to

$$\operatorname{Ker}\varphi := \varphi^{-1}(1_H)(= \{g \in G : \varphi(g) = 1_H\}).$$

$\operatorname{Ker}\varphi$ nazywamy jądrem homomorfizmu φ.

Uwaga

Ponieważ każdy homomorfizm pierścieni jest homomorfizmem grup addytywnych tych pierścieni, więc jeśli $\varphi\colon R \to S$ jest homomorfizmem pierścieni, to

$$\operatorname{Ker}\varphi = \{r \in R : \varphi(r) = 0_S\}.$$

Stwierdzenie 1.11

Jeśli $\varphi\colon G \to H$ jest homomorfizmem grup i $H' \leq H$, to $\varphi^{-1}(H') \leq G$.
W szczególności, $\operatorname{Ker}\varphi \leq G$.

(Kontr)przykład (dla pieścieni)

Niech $\varphi\colon \mathbb{Z} \to \mathbb{Z}_6$, $\varphi(k) := k \bmod 6$, $k \in \mathbb{Z}$.
Mamy:

- $\{0, 2, 4\} \leq \mathbb{Z}_6$, ale
- $\varphi^{-1}(\{0, 2, 4\}) = \{0, \pm 2, \pm 4, \ldots\} \not\leq \mathbb{Z}$.

Stwierdzenie 1.11

Jeśli $\varphi\colon G \to H$ jest homomorfizmem grup i $H' \leq H$, to $\varphi^{-1}(H') \leq G$.

Przypomnienie

(1.9): $K \leq L \iff K \neq \varnothing$ i $k_1 \cdot k_2^{-1} \in K$ dla wszystkich $k_1, k_2 \in K$.
(1.5): $\varphi(1_G) = 1_H$ i $\varphi(g^{-1}) = (\varphi(g))^{-1}$.
(1.8)(2)(b): $K \leq L \Rightarrow 1_L \in K$.

Dowód

Skorzystamy z (1.9).
Mamy $1_H \in H'$ ((1.8)(2)(b) dla $K = H'$ i $L = H$), więc

$$\varphi(1_G) = 1_H \in H',$$

zatem $1_G \in \varphi^{-1}(H')$, w szczególności $\varphi^{-1}(H') \neq \varnothing$.

Niech $g_1, g_2 \in \varphi^{-1}(H')$.

Musimy sprawdzić, czy $g_1 \cdot g_2^{-1} \in \varphi^{-1}(H')$.

Z definicji $\varphi(g_1), \varphi(g_2) \in H'$, więc

$$\varphi(g_1 \cdot g_2^{-1}) = \varphi(g_1) \cdot (\varphi(g_2))^{-1} \overset{\in}{\underset{\text{(1.9) dla } K = H'}{}} H'.$$

Zatem $g_1 \cdot g_2^{-1} \in \varphi^{-1}(H')$. $\square$

Stwierdzenie 1.12

Niech $\varphi\colon G \to H$ będzie homomorfizmem grup.

(1) φ jest monomorfizmem wtedy i tylko wtedy, gdy $\operatorname{Ker}\varphi = \{1\}$.

(2) φ jest epimorfizmem wtedy i tylko wtedy, gdy $\operatorname{Im}\varphi = H$.

(3) φ jest izomorfizmem wtedy i tylko wtedy, gdy $\operatorname{Ker}\varphi = \{1\}$ i $\operatorname{Im}\varphi = H$.

Uwaga

$\operatorname{Ker}\varphi = \{1\} \iff |\operatorname{Ker}\varphi| = 1$.

Przypomnienie

(1.6): izo = mono + epi.

(1.5): $\varphi(1_G) = 1_H$.

Dowód

(3): Natychmiast z (1), (2) oraz (1.6).

(2): Oczywisty.

(1) $\Rightarrow$: Natychmiast z (1.5).

Istotnie, z założenia $|\operatorname{Ker}\varphi| \leq 1$, a z (1.5) $1_G \in \operatorname{Ker}\varphi$.

Zatem $\operatorname{Ker}\varphi = \{1_G\}$.

$\Leftarrow$: Załóżmy, że $\operatorname{Ker}\varphi = \{1_G\}$, i przypuśćmy, że $\varphi(g_1) = \varphi(g_2)$.

Wtedy

$$\varphi(g_1 \cdot g_2^{-1}) = \varphi(g_1) \cdot (\varphi(g_2))^{-1} = \varphi(g_1) \cdot (\varphi(g_1))^{-1} = 1_H,$$

a więc $g_1 \cdot g_2^{-1} \in \operatorname{Ker}\varphi$. Stąd $g_1 \cdot g_2^{-1} = 1_H$, a więc $g_1 = g_2$. $\square$

Lemat 1.13

Niech G będzie grupą.
Jeśli $H_i \leq G$, $i \in I$, to

$$\bigcap_{i \in I} H_i \leq G.$$

Przypomnienie

(1.9): $H \leq G \iff H \neq \varnothing$ i $h_1 \cdot h_2^{-1} \in H$ dla wszystkich $h_1, h_2 \in H$.
(1.8)(2)(b): $H \leq G \Rightarrow 1 \in H$.

Dowód

Skorzystamy z (1.9).
(1.8)(2)(b) $\Rightarrow 1 \in H_i$ dla każdego $i \Rightarrow 1 \in \bigcap_i H_i \Rightarrow \bigcap_i H_i \neq \varnothing$.
Niech $h_1, h_2 \in \bigcap_i H_i$.
Wtedy $h_1, h_2 \in H_i$ dla każdego i.
(1.9) $\Rightarrow h_1 \cdot h_2^{-1} \in H_i$ dla każdego $i \Rightarrow h_1 \cdot h_2^{-1} \in \bigcap_i H_i$. $\square$

(Kontr)przykład (dla pierścieni)

Niech $R := \mathbb{Z}_2 \times \mathbb{Z}_4$. Wtedy

$$S_1 := \{(0,0),(0,1),(0,2),(0,3)\} \leq R \quad \text{i} \quad S_2 := \{(0,0),(1,1),(0,2),(1,3)\} \leq R,$$

ale $S_1 \cap S_2 \not\leq R$.

Stwierdzenie 1.14/Definicja/Oznacznie

Jeśli G jest grupą i $X \subseteq G$, to istnieje najmniejsza (w sensie inkluzji) podgrupa grupy G zawierająca zbiór X.

Tę grupę nazywamy podgrupą generowaną przez zbiór X oraz oznaczamy $\langle X \rangle$.

Dowód

Niech H_i, $i \in I$, będą wszystkimi podgrupami grupy G zawierającymi zbiór X.

Wtedy $H := \bigcap_{i \in I} H_i$ jest szukaną podgrupą.

Istotnie: 1° $H \leq G$ na mocy (1.13).

2°: $X \subseteq H_i$ dla każdego $i \in I \Rightarrow X \subseteq \bigcap_i H_i = H$.

3°: Jeśli $H' \leq G$ i $X \subseteq H'$, to $H' = H_j$ dla pewnego j, więc $H' = H_j \supseteq \bigcap_i H_i = H$. $\square$

Notacja

$\langle g_1, \ldots, g_n \rangle := \langle \{g_1, \ldots, g_n\} \rangle$.

Stwierdzenie 1.15

Niech G będzie grupą.
Jeśli $X \subseteq G$, to

$$\langle X \rangle = \{g_1^{\varepsilon_1} \cdots g_n^{\varepsilon_n} : n \in \mathbb{N},\ g_1, \ldots, g_n \in X,\ \varepsilon_1, \ldots, \varepsilon_n \in \{\pm 1\}\}.$$

Dowód

Niech

$$H_0 := \{g_1^{\varepsilon_1} \cdots g_n^{\varepsilon_n} : n \in \mathbb{N},\ g_1, \ldots, g_n \in X,\ \varepsilon_1, \ldots, \varepsilon_n \in \{\pm 1\}\}.$$

Łatwo zauważyć, że

- $H_0 \leq G$,
  $[1 = g_1^{\varepsilon_1} \cdots g_n^{\varepsilon_n}$ dla $n = 0 \Rightarrow 1 \in H_0 \Rightarrow H_0 \neq \varnothing$;
  $g_1^{\varepsilon_1} \cdots g_n^{\varepsilon_n} \cdot (h_1^{\varepsilon_1} \cdots h_m^{\varepsilon_m})^{-1} = g_1^{\varepsilon_1} \cdots g_n^{\varepsilon_n} \cdot h_m^{-\varepsilon_m} \cdots h_1^{-\varepsilon_1}]$
- $X \subseteq H_0$,
  $[g = g^1]$
- jeśli $H \leq G$ i $X \subseteq H$, to $H_0 \subseteq H$.
  $[X \subseteq H \Rightarrow g_1, \ldots, g_n \in H \Rightarrow g_1^{\varepsilon_1}, \ldots, g_n^{\varepsilon_n} \in H \Rightarrow g_1^{\varepsilon_1} \cdots g_n^{\varepsilon_n} \in H]$

Stąd $H_0 = \langle X \rangle$. $\square$

Stwierdzenie 1.15

Niech G będzie grupą.
Jeśli $X \subseteq G$, to

$$\langle X \rangle = \{g_1^{\varepsilon_1} \cdots g_n^{\varepsilon_n} : n \in \mathbb{N},\ g_1, \ldots, g_n \in X,\ \varepsilon_1, \ldots, \varepsilon_n \in \{\pm 1\}\}.$$

Wniosek 1.16

Jeśli g jest elementem grupy G, to

$$\langle g \rangle = \{g^m : m \in \mathbb{Z}\}.$$

Dowód

Wystarczy zauważyć, że

$$g^{\varepsilon_1} \cdots g^{\varepsilon_n} = g^{\varepsilon_1 + \cdots + \varepsilon_n}. \quad \square$$

Wniosek 1.17

Jeśli G jest grupą abelową oraz $g_1, \ldots, g_m \in G$, to

$$\langle g_1, \ldots, g_m \rangle = \{g_1^{k_1} \cdots g_m^{k_m} : k_1, \ldots, k_m \in \mathbb{Z}\}. \quad \square$$