Algebra I

Wykład IV

Grzegorz Bobiński (UMK)

Definicja

Relacją kongurencji (kongruencją) w półgrupie (monoidzie, grupie) X nazywamy każdą relację równoważności $\sim$ w zbiorze X taką, że

$$\forall_{x_1,x_2,y_1,y_2\in X}\ x_1 \sim x_2 \wedge y_1 \sim y_2 \implies x_1 \cdot y_1 \sim x_2 \cdot y_2.$$

Jeśli R jest pierścieniem, to relacja $\sim$ w zbiorze R jest kongurencją w pierścieniu R, jeśli $\sim$ jest kongurencją w grupie addytywnej i monoidzie multiplikatywnym pierścienia R.

Przykłady

- Jeśli $n \in \mathbb{N}_+$, to $\equiv_n$ jest kongruencją w (grupie/pierścieniu) $\mathbb{Z}$.
- Jeśli R jest pierścieniem, $r \in R$ oraz $f \sim g :\iff f(r) = g(r)$, $f, g \in R[X]$, to $\sim$ jest kongruencją w $R[X]$.
- Niech $\varphi\colon X \to Y$ będzie homomorfizmem.

  Definiujemy $\sim_\varphi$ wzorem:

  $$x_1 \sim_\varphi x_2 \qquad :\iff \qquad \varphi(x_1) = \varphi(x_2) \qquad (x_1, x_2 \in X).$$

  Wtedy $\sim_\varphi$ jest kongruencją w X.

  Zauważmy, że dwa powyższe przykłady kongruencji są szczególnymi przykładami relacji tego typu.

  Innymi przykładami są:

  - Jeśli F jest ciałem, $n \in \mathbb{N}_+$ i $A \sim B :\iff \det A = \det B$ $(A, B \in \mathrm{GL}_n(F))$, to $\sim$ jest kongruencją w $\mathrm{GL}_n(F)$.
  - Jeśli $n \in \mathbb{N}_+$ i $\sigma \sim \tau :\iff \operatorname{sgn}\sigma = \operatorname{sgn}\tau$ $(\sigma, \tau \in S_n)$, to $\sim$ jest kongruencją w S_n.

Lemat 1.18

Niech $\sim$ będzie kongruencją w grupie G.
Jeśli $g, h \in G$ oraz $g \sim h$, to $g^{-1} \sim h^{-1}$.

Dowód

Mamy

$$g^{-1} = g^{-1} \cdot 1 = g^{-1} \cdot h \cdot h^{-1} \sim g^{-1} \cdot g \cdot h^{-1} = 1 \cdot h^{-1} = h^{-1}. \quad \square$$

Stwierdzenie 1.19

Jeśli $\sim$ jest kongruencją w półgrupie X i w $X/\sim$ definiujemy $\cdot$ wzorem

$$[x_1]_\sim \cdot [x_2]_\sim := [x_1 \cdot x_2]_\sim \qquad (x_1, x_2 \in X),$$

to powyższa definicja jest poprawna.

Dowód

Ćwiczenie. $\square$

Uwaga

Powyższe stwierdzenie można stosować oczywiście również w przypadku monoidów i grup.
W konsekwencji, możemy je także stosować w przypadku pierścieni.

Przykłady

- $(\mathbb{Z}/\equiv_n, +, \cdot)$ można utożsamić $(\mathbb{Z}_n, +_n, \cdot_n)$.
- $\mathbb{C}$ można utożsamić z $\mathbb{R}[X]/\sim$, gdzie

$$\sum a_k X^k \sim \sum b_k X^k : \iff \sum_k (-1)^k a_{2k} = \sum_k (-1)^k b_{2k} \text{ i } \sum_k (-1)^k a_{2k+1} = \sum_k (-1)^k b_{2k+1}.$$

Stwierdzenie 1.20 / Definicja

Jeśli $\sim$ jest kongruencją w pierścieniu/grupie/monoidzie/półgrupie X, to $X/\sim$ jest pierścieniem/grupą/monoidem/półgrupą, który(ą) nazywamy pierścieniem/grupą/monoidem/półgrupą ilorazowym(ą).

Dowód

Wersja dla pierścieni.

Łatwo sprawdzić, że $+$ i $\cdot$ w $X/\sim$ są łączne i przemienne oraz $\cdot$ jest rodzielne względem $+$.

$[0]_\sim$ i $[1]_\sim$ są elementami neutralnymi dla $+$ i $\cdot$.

Jeśli $x \in X$, to $[-x]_\sim$ jest elementem przeciwnym do $[x]_\sim$. □

Stwierdzenie 1.21 / Definicja

Jeśli $\sim$ jest kongruencją w strukturze algebraicznej X, to $\pi\colon X \to X/\sim$ dane wzorem

$$\pi(x) := [x]_\sim \qquad (x \in X),$$

jest epimorfizmem, który nazywamy naturalnym rzutowaniem.

Dowód

Mamy

$$\pi(x * y) = [x * y]_\sim = [x]_\sim * [y]_\sim = \pi(x) * \pi(y). \quad \square$$

Uwaga

Niech $\sim$ będzie kongruencją w strukturze algebraicznej X i $\pi\colon X \to X/\sim$ naturalnym rzutowaniem.

Wtedy $\sim = \sim_\pi$.

Definicja

Jeśli $\sim$ jest kongruencją w grupie G, to definiujemy

$$N_\sim := [1]_\sim.$$

Uwaga

Jeśli $\sim$ jest kongruencją w pierścieniu R, to

$$N_\sim = [0]_\sim.$$

Przykłady

- Jeśli $n \in \mathbb{N}_+$, to $N_{\equiv_n} = n\mathbb{Z}$.
- Jeśli $\varphi\colon X \to Y$ jest homomorfizmem grup (lub pierścieni), to $N_{\sim_\varphi} = \operatorname{Ker}\varphi$.

Definicja

Podzbiór N grupy G nazywamy dzielnikiem normalnym, jeśli $N \leq G$ oraz

$$\forall_{g \in G}\ \forall_{h \in N}\ g \cdot h \cdot g^{-1} \in N.$$

Jeśli N jest dzielnikiem normalnym grupy G, to piszemy $N \trianglelefteq G$.

Uwaga

Jeśli grupa G jest abelowa, to $H \trianglelefteq G$ wtedy i tylko wtedy $H \leq G$.

Przykład

Niech

$$H := \left\{ \begin{pmatrix} 123 \\ 123 \end{pmatrix}, \begin{pmatrix} 123 \\ 213 \end{pmatrix} \right\}.$$

Wtedy $H \leq S_3$ i $H \not\trianglelefteq S_3$.

Istotnie

$$\begin{pmatrix} 123 \\ 231 \end{pmatrix} \circ \begin{pmatrix} 123 \\ 213 \end{pmatrix} \circ \begin{pmatrix} 123 \\ 231 \end{pmatrix}^{-1} = \begin{pmatrix} 123 \\ 321 \end{pmatrix} \circ \begin{pmatrix} 123 \\ 312 \end{pmatrix} = \begin{pmatrix} 123 \\ 132 \end{pmatrix} \notin H.$$

Definicja

Podzbiór I pierścienia R nazywamy ideałem, jeśli I jest podgrupą grupy addytywnej pierścienia R oraz

$$\forall_{r \in R}\ \forall_{a \in I}\ r \cdot a \in I.$$

Piszemy $I \trianglelefteq R$.

Przykłady

- Jeśli G jest grupą, to $\{1\}, G \trianglelefteq G$.
- Jeśli R jest pierścieniem, to $\{0\}, R \trianglelefteq R$.
- Jeśli $n \in \mathbb{N}_+$, to $A_n \trianglelefteq S_n$.
- Jeśli $n \in \mathbb{N}_+$, to $n\mathbb{Z} \trianglelefteq \mathbb{Z}$.
  Jeśli $n > 1$, to $n\mathbb{Z} \not\trianglelefteq \mathbb{Z}$.
- Jeśli R jest pierścieniem i $r \in R$, to

$$\{f \in R[X] : f(r) = 0\} \trianglelefteq R[X].$$

Lemat 1.22

(1) Jeśli $\sim$ jest kongruencją w grupie G, to $N_\sim \trianglelefteq G$.

(2) Jeśli $\sim$ jest kongruencją w pierścieniu R, to $N_\sim \trianglelefteq R$.

Przypomnienie

(1.9): $H \leq G \iff H \neq \varnothing$ i $h_1, h_2 \in H \implies h_1 \cdot h_2^{-1} \in H$.

Dowód

(1) $1 \in [1]_\sim = N_\sim \implies N_\sim \neq \varnothing$.

Jeśli $g_1, g_2 \in N_\sim$, to $g_1 \sim 1$ i z (1.18) $g_2^{-1} \sim 1^{-1} = 1$.

Stąd $g_1 \cdot g_2^{-1} \sim 1 \cdot 1 = 1$, a więc $g_1 \cdot g_2^{-1} \in N_\sim$.

Zatem $N_\sim \leq G$ na mocy (1.9).

Jeśli $g \in G$ i $h \in N_\sim$, to

$$g \cdot h \cdot g^{-1} \sim g \cdot 1 \cdot g^{-1} = 1.$$

Zatem $g \cdot h \cdot g^{-1} \in N_\sim$.

(2) Z (1) wiemy już, że $N_\sim \leq (R, +)$.

Ustalmy $r \in R$ i $a \in N_\sim$.

Wtedy $r \cdot a \sim r \cdot 0 = 0$.

Zatem $r \cdot a \in N_\sim$. $\square$

Definicja

Jeśli H jest podgrupą grupy G, to definiujemy

$$g_1 \sim_H g_2 : \iff g_1^{-1} \cdot g_2 \in H.$$

Uwaga

Jeśli I jest ideałem pierścienia R, to

$$r_1 \sim_I r_2 \iff r_2 - r_1 \in I.$$

Lemat 1.23

(1) Jeśli G jest grupa i $H \leq G$, to $\sim_H$ jest relacją równoważności w G.

(2) Jeśli G jest grupa i $N \trianglelefteq G$, to $\sim_N$ jest kongruencją w G.

(3) Jeśli R jest pierścieniem i $I \trianglelefteq R$, to $\sim_I$ jest kongruencją w R.

Dowód

(1) [Zwrotność]: $g^{-1}g = 1 \in H \implies g \sim_H g$.

[Symetryczność]:

$g_1 \sim_H g_2 \implies g_1^{-1}g_2 \in H \implies (g_1^{-1}g_2)^{-1} \in H \implies g_2^{-1}g_1 \in H \implies g_2 \sim_H g_1$.

[Przechodniość]:

$g_1 \sim_H g_2 \wedge g_2 \sim_H g_3 \implies g_1^{-1}g_2, g_2^{-1}g_3 \in H \implies (g_1^{-1}g_2) \cdot (g_2^{-1}g_3) \in H \implies g_1^{-1}g_3 \in H \implies g_1 \sim_H g_3$.

Lemat 1.23

(1) Jeśli G jest grupa i $H \leq G$, to $\sim_H$ jest relacją równoważności w G.

(2) Jeśli G jest grupa i $N \trianglelefteq G$, to $\sim_N$ jest kongruencją w G.

(3) Jeśli R jest pierścieniem i $I \trianglelefteq R$, to $\sim_I$ jest kongruencją w R.

Dowód (kont.)

(2) Niech $g_1 \sim_N g_2$ i $h_1 \sim_N h_2$.

Mamy

$$(g_1 \cdot h_1)^{-1} \cdot g_2 \cdot h_2 = h_1^{-1} \cdot g_1^{-1} \cdot g_2 \cdot h_2 = h_1^{-1} \cdot g_1^{-1} \cdot g_2 \cdot h_1 \cdot h_1^{-1} \cdot h_2.$$

Z założenia, $g_1^{-1} \cdot g_2, h_1^{-1} \cdot h_2 \in N$.

Ponieważ $N \trianglelefteq G$, więc $h_1^{-1} \cdot (g_1^{-1} \cdot g_2) \cdot h_1 \in N$.

Ostatecznie,

$$(g_1 \cdot h_1)^{-1} \cdot g_2 \cdot h_2 = h_1^{-1} \cdot g_1^{-1} \cdot g_2 \cdot h_1 \cdot h_1^{-1} \cdot h_2 \in N,$$

a więc $g_1 h_1 \sim_N g_2 h_2$.

(3) Niech $r_1 \sim_I r_2$ i $s_1 \sim_I s_2$.

Mamy

$$r_2 \cdot s_2 - r_1 \cdot s_1 = r_2 \cdot (s_2 - s_1) + s_1 \cdot (r_2 - r_1).$$

Z założenia, $r_2 - r_1, s_2 - s_1 \in I$.

Skąd łatwo widać, że $r_2 \cdot s_2 - r_1 \cdot s_1 \in I$. $\square$

Notacja

Jeśli G jest grupą i $H \leq G$, to $G/H := G/\sim_H$.
Jeśli $X \subseteq G$, to

$$X/H := \{[x]_{\sim_H} : x \in X\}.$$

Jeśli R jest pierścieniem i $I \trianglelefteq R$, to $R/I := R/\sim_I$.
Jeśli $X \subseteq R$, to

$$X/I := \{[x]_{\sim_I} : x \in X\}.$$

Przykłady

- Jeśli $H = G$, to $|G/H| = 1$.
- Jeśli G jest grupą, to $G/\{1\} \simeq G$.
- Jeśli R jest pierścieniem, to $R/\{0\} \simeq R$.

Stwierdzenie 1.24

(1) Jeśli $\sim$ jest kongruencją w grupie G, to $\sim_{N_\sim} = \sim$.

(2) Jeśli G jest grupą i $N \trianglelefteq G$, to $N_{\sim_N} = N$.

Uwaga

Z powyższego stwierdzenia otrzymujemy również odpowiednią wersję dla pierścieni.

Dowód

(1) Mamy

$$g_1 \sim_{N_\sim} g_2 \implies g_1^{-1} \cdot g_2 \in N_\sim \implies g_1^{-1} \cdot g_2 \sim 1 \implies g_2 \sim g_1 \implies g_1 \sim g_2.$$

Analogicznie,

$$g_1 \sim g_2 \implies g_2 \sim g_1 \implies g_1^{-1} \cdot g_2 \sim 1 \implies g_1^{-1} \cdot g_2 \in N_\sim \implies g_1 \sim_{N_\sim} g_2.$$

(2) Mamy

$$g \in N_{\sim_N} \implies g \sim_N 1 \implies g^{-1} = g^{-1} \cdot 1 \in N \implies g = (g^{-1})^{-1} \in N.$$

Analogicznie

$$g \in N \implies g^{-1} \cdot 1 = g^{-1} \in N \implies g \sim_N 1 \implies g \in N_{\sim_N}. \quad \square$$

Stwierdzenie 1.25

Jeśli $\varphi\colon X \to Y$ jest homomorfizmem grup/pierścieni i $N \trianglelefteq Y$, to $\varphi^{-1}(N) \trianglelefteq X$.
W szczególności, $\operatorname{Ker}\varphi \trianglelefteq X$.

Przypomnienie

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

Dowód

Wiemy z (1.11), że $\varphi^{-1}(N) \leq X$.
Ustalmy $x \in X$ i $g \in \varphi^{-1}(N)$.
Wtedy $\varphi(g) \in N$, więc

$$\varphi(x \cdot g \cdot x^{-1}) = \varphi(x) \cdot \varphi(g) \cdot (\varphi(x))^{-1} \in N.$$

Stąd $x \cdot g \cdot x^{-1} \in \varphi^{-1}(N)$.
Wersję dla pierścieni dowodzimy podobnie. □

Stwierdzenie 1.26

Jeśli $\varphi\colon X \to Y$ jest epimorfizmem grup/pierścieni i $N \trianglelefteq X$, to $\varphi(N) \trianglelefteq Y$.

Przypomnienie

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

Dowód

Wiemy z (1.10), że $\varphi(N) \leq Y$.

Ustalmy $y \in Y$ i $h \in \varphi(N)$.

Wtedy istnieje $g \in N$ taki, że $h = \varphi(g)$.

Istnieje $x \in X$ taki, że $\varphi(x) = y$ [gdyż φ jest epi].

Wtedy $x \cdot g \cdot x^{-1} \in N$.

Stąd

$$y \cdot h \cdot y^{-1} = \varphi(x) \cdot \varphi(g) \cdot (\varphi(x))^{-1} = \varphi(x \cdot g \cdot x^{-1}) \in \varphi(N).$$

Wersję dla pierścieni dowodzimy podobnie. $\square$

(Kontr)przykład

Jeśli G jest grupą, $H \leq G$ i $H \not\trianglelefteq G$, to $H \trianglelefteq H$, ale $\mu(H) = H \not\trianglelefteq G$, gdzie $\mu\colon H \to G$ jest naturalnym włożeniem.