Algebra I

Wykład V

Grzegorz Bobiński (UMK)

Umowa

W tym podrozdziale badamy tylko grupy.

Przypomnienie

Jeśli $H \leq G$, to zdefiniowaliśmy relację równoważności $\sim_H$ wzorem

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

Definicja

Jeśli $H \leq G$, to definiujemy relację $\sim'_H$ wzorem:

$$g_1 \sim'_H g_2 :\iff g_2 \cdot g_1^{-1} \in H.$$

Uwaga

Jeśli $H \trianglelefteq G$, to $\sim'_H = \sim_H$.

Dowód

Mamy

$$g_1 \sim'_H g_2 \overset{\text{def.}}{\Longrightarrow} g_2 g_1^{-1} \in H \overset{H \trianglelefteq G}{\Longrightarrow} g_1^{-1} g_2 = g_1^{-1} \cdot g_2 g_1^{-1} \cdot (g_1^{-1})^{-1} \in H \overset{\text{def.}}{\Longrightarrow} g_1 \sim_H g_2.$$

Analogicznie

$$g_1 \sim_H g_2 \implies g_1 \sim'_H g_2. \quad \square$$

Lemat 1.27

Jeśli $H \leq G$, to $\sim'_H$ jest relacją równoważności.

Dowód

Ćwiczenie. $\square$

Notacja

Jeśli $H \leq G$, to $H\backslash G := G/\sim'_H$.

Notacja

Jeśli $g \in G$ oraz $X \subseteq G$, to

$$gX := \{g \cdot h : h \in X\} \qquad \text{i} \qquad Xg := \{h \cdot g : h \in X\}.$$

Definicja

Jeśli $g \in G$ oraz $H \leq G$, to gH i Hg nazywamy warstwami lewo- i prawostronną elementu g względem H.

Lemat 1.28

Jeśli $H \leq G$ i $g \in G$, to

$$[g]_{\sim_H} = gH \qquad \text{i} \qquad [g]_{\sim'_H} = Hg.$$

Dowód

Mamy

$$g' \in [g]_{\sim_H} \overset{\text{def.}}{\Longrightarrow} g \sim_H g' \overset{\text{def.}}{\Longrightarrow} g^{-1} \cdot g' \in H \overset{\text{def.}}{\Longrightarrow} g' = g \cdot (g^{-1} \cdot g') \in gH.$$

Podobnie,

$$g' \in gH \overset{\text{def.}}{\Longrightarrow} g' = g \cdot h \text{ dla pewnego } h \in H \Longrightarrow g^{-1} \cdot g' = h \in H$$

$$\overset{\text{def.}}{\Longrightarrow} g \sim_H g' \overset{\text{def.}}{\Longrightarrow} g' \in [g]_{\sim_H}. \quad \square$$

Uwaga

Z Lematu 1.28 wynika, że jeśli $I \trianglelefteq R$ oraz $r \in R$, to

$$[r]_{\sim_I} = r + I.$$

Lemat 1.29

Jeśli $H \leq G$, to $|G/H| = |H\backslash G|$.

Dowód

Definiujemy $\Phi\colon G/H \to H\backslash G$ wzorem

$$\Phi([g]_{\sim_H}) = [g^{-1}]_{\sim'_H} \qquad (g \in G).$$

Zauważmy, że ta funkcje jest poprawnie określona.

Istotnie,

$$[g_1]_{\sim_H} = [g_2]_{\sim_H} \implies g_1^{-1} \cdot g_2 \in H \overset{H\leq G}{\implies} g_2^{-1} \cdot (g_1^{-1})^{-1} = (g_1^{-1} \cdot g_2)^{-1} \in H$$
$$\implies [g_1^{-1}]_{\sim'_H} = [g_2^{-1}]_{\sim'_H}.$$

Podobnie pokazujemy, że funkcja $\Psi\colon H\backslash G \to G/H$ dana wzorem

$$\Psi([g]_{\sim'_H}) = [g^{-1}]_{\sim_H} \qquad (g \in G)$$

jest poprawnie określona.

Ponadto $\Phi \circ \Psi = \mathrm{Id}_{H\backslash G}$ i $\Psi \circ \Phi = \mathrm{Id}_{G/H}$. □

Definicja

Jeśli $H \leq G$, to liczbę $|G/H| = |H\backslash G|$ nazywamy indeksem podgrupy H w grupie G i oznaczamy $[G : H]$.

Twierdzenie 1.30 (Lagrange)

Jeśli $H \leq G$, to

$$|G| = |H| \cdot [G : H].$$

Twierdzenie 1.30 (Lagrange)

Jeśli $H \leq G$, to

$$|G| = |H| \cdot [G : H].$$

Dowód

Wiadomo, że jeśli

- $\sim$ jest relacją równoważności w zbiorze X,
- istnieje liczba kardynalna $\mathfrak{a}$ taka, że $|Y| = \mathfrak{a}$ dla każdej klasy abstrakcji $Y \in X/\sim$,

to

$$|X| = \mathfrak{a} \cdot |X/\sim|.$$

Chcemy zastosować powyższy fakt dla $X = G$ i $\sim = \sim_H$.

Wtedy

$$|X/\sim| = |G/\sim_H| = |G/H| = [G : H].$$

Zatem dla zakończenia dowodu wystarczy pokazać, że $|Y| = |H|$ dla każdego $Y \in G/H$.

Ustalmy $Y \in G/H$.

Wtedy $Y = [g]_{\sim_H}$ dla pewnego $g \in G$.

(1.28) $\implies$ $Y = gH$.

Definiujemy $\Phi\colon H \to gH$ wzorem $\Phi(h) := gh$, $h \in H$.

Z definicji zbioru gH funkcja jest dobrze określona oraz jest surjekcją.

Pokażemy, że Φ jest również injekcją.

To będzie oznaczało, że Φ jest bijekcją, a więc zgodnie z zapowiedzią

$$|H| = |gH| = |Y|.$$

Ustalmy $h_1, h_2 \in H$ takie, że $\Phi(h_1) = \Phi(h_2)$.

Wtedy

$$h_1 = g^{-1} \cdot g \cdot h_1 = g^{-1} \cdot \Phi(h_1) = g^{-1} \cdot \Phi(h_2) = g^{-1} \cdot g \cdot h_2 = h_2. \quad \square$$

Twierdzenie 1.30 (Lagrange)

Jeśli $H \leq G$, to

$$|G| = |H| \cdot [G : H].$$

Definicja

Rzędem grupy nazywamy liczbę jej elementów.

Wniosek 1.31

Jeśli $|G| < \infty$ i $H \leq G$, to $|H|$ dzieli $|G|$.
Innymi słowy, rząd podgrupy dzieli rząd grupy.

Definicja

Rzędem elementu g grupy G nazywamy

$$\operatorname{ord}(g) := |\langle g \rangle|.$$

Stwierdzenie 1.32

Jeśli $g \in G$, to

$$\operatorname{ord}(g) = \min\{n \in \mathbb{N}_+ : g^n = 1\}.$$

Ponadto, jeśli $\operatorname{ord}(g) < \infty$, to

$$\langle g \rangle = \{g^k : k \in \{0, 1, \ldots, \operatorname{ord}(g) - 1\}\}.$$

Uwaga

W powyższym stwierdzeniu zakładamy, że $\min \varnothing := \infty$.

Stwierdzenie 1.32

Jeśli $g \in G$, to

$$\operatorname{ord}(g) = \min\{n \in \mathbb{N}_+ : g^n = 1\}.$$

Ponadto, jeśli $\operatorname{ord}(g) < \infty$, to

$$\langle g \rangle = \{g^k : k \in \{0, 1, \ldots, \operatorname{ord}(g) - 1\}\}.$$

Przypomnienie

(1.16): $\langle g \rangle = \{g^l : l \in \mathbb{Z}\}$.

Dowód

Niech

$$m := \min\{n \in \mathbb{N}_+ : g^n = 1\}.$$

Pokażmy najpierw, że elementy g^k, $0 \leq k < m$, są parami różne.
Istotnie, przypuśćmy, że $g^k = g^l$ dla $k, l \in \mathbb{Z}$ takich, że $0 \leq k < l < m$.
Wtedy

$$g^{l-k} = g^l \cdot (g^k)^{-1} = 1$$

oraz $l - k \in \mathbb{N}_+$ i $l - k < m$, co jest niemożliwe wobec definicji liczby m.
(1.16) $\implies$ jeśli $m = \infty$, to $\operatorname{ord}(g) = m$.
Istotnie,

$$m = \infty \geq \operatorname{ord}(g) = |\langle g \rangle| = |\{g^l : l \in \mathbb{Z}\}| \geq |\{g^k : k \in \mathbb{N}\}| = |\{g^k : 0 \leq k < m\}| = m.$$

Stwierdzenie 1.32

Jeśli $g \in G$, to

$$\operatorname{ord}(g) = \min\{n \in \mathbb{N}_+ : g^n = 1\}.$$

Ponadto, jeśli $\operatorname{ord}(g) < \infty$, to

$$\langle g \rangle = \{g^k : k \in \{0, 1, \ldots, \operatorname{ord}(g) - 1\}\}.$$

Przypomnienie

(1.16): $\langle g \rangle = \{g^l : l \in \mathbb{Z}\}$.

Załóżmy, że $m < \infty$.

Pokażemy, że dla każdego $l \in \mathbb{Z}$ istnieje $k \in \mathbb{Z}$ takie, że $0 \leq k < m$ i $g^l = g^k$.

Wiemy, że istnieją $q, k \in \mathbb{Z}$ takie, że $l = q \cdot m + k$ i $0 \leq k < m$.

Wtedy

$$g^l = (g^m)^q \cdot g^k = 1^q \cdot g^k = 1 \cdot g^k = g^k.$$

Z powyższego,

$$\langle g \rangle = \{g^k : k \in \{0, 1, \ldots, m - 1\}\}.$$

W szczególności,

$$\operatorname{ord}(g) = |\langle g \rangle| = |\{g^k : k \in \{0, 1, \ldots, m - 1\}\}| = m. \quad \square$$