Algebra I

Wykład XI

Grzegorz Bobiński (UMK)

3 Klasyfikacja skończonych grup abelowych

Notacja

Przez cały rozdział wszystkie rozważane grupy będą grupami abelowymi.

Działanie w rozważanych grupach będziemy oznaczać symbolem $+$, więc w szczególności przez 0 będziemy oznaczać element neutralny.

Cel

Celem tego rozdziału jest udowodnienie, że jeśli G jest skończoną grupą abelową, to istnieją jednoznacznie wyznaczone: $(k \in \mathbb{N})$, $p_1, \ldots, p_k \in \mathbb{P}$, $(l_1 \ldots, l_k \in \mathbb{N}_+)$ oraz $n_{i,j} \in \mathbb{N}_+$, $i \in \{1, \ldots, k\}$, $j \in \{1, \ldots, l_i\}$, takie, że

$$G \simeq \bigoplus_{i=1}^{k} \bigoplus_{j=1}^{l_i} \mathbb{Z}_{p_i^{n_{i,j}}},$$

$p_1 < p_2 < \cdots < p_k$ oraz

$$n_{i,1} \leq n_{i,2} \leq \cdots \leq n_{i,l_i},$$

dla każdego i.

3.1 Sumy proste

Definicja

Jeśli G i H są grupami, to sumą prostą grup G i H nazywamy zbiór $G \times H$ z działaniem po współrzędnych, tzn. jeśli $g_1, g_2 \in G$ i $h_1, h_2 \in H$, to

$$(g_1, h_1) + (g_2, h_2) := (g_1 + g_2, h_1 + h_2).$$

Sumę prostą grup G i H oznaczamy symbolem $G \oplus H$.

Uwaga

Suma prosta grup (abelowych) jest grupą (abelową).

Jeśli G, H i K są grupami, to

$$G \oplus H \simeq H \oplus G \qquad \text{i} \qquad (G \oplus H) \oplus K \simeq G \oplus (H \oplus K).$$

W związku w powyższym, jeśli $G_1, \ldots, G_n$ są grupami, to definicja

$$\bigoplus_{i=1}^{n} G_i := G_1 \oplus \cdots \oplus G_n$$

jest poprawna.

Lemma 3.1

Niech $G_1, \ldots, G_m$ i $H_1, \ldots, H_n$ będą grupami.
Jeśli $\varphi_{j,i}\colon G_i \to H_j$, $i \in \{1, \ldots, m\}$, $j \in \{1, \ldots, n\}$, są homomorfizmami, to funkcja

$$\varphi\colon G_1 \oplus \cdots \oplus G_m \to H_1 \oplus \cdots \oplus H_n$$

dana wzorem

$$\varphi(g_1, \ldots, g_m) := (\varphi_{1,1}(g_1) + \cdots + \varphi_{1,m}(g_m), \ldots, \varphi_{n,1}(g_1) + \cdots + \varphi_{n,m}(g_m))$$
$$(g_1 \in G_1, \ \ldots, \ g_m \in G_m),$$

jest homomorfizmem grup.

Dowód

Ćwiczenie. □

Definicja

Jeśli G i H są grupami oraz istnieje grupa H' taka, że $H \oplus H' \simeq G$, to mówimy, że H jest składnikiem prostym grupy G.

Uwaga

Jeśli H i H' są grupami, to istnieją homomorfizmy $\mu\colon H \to H \oplus H'$ i $\pi\colon H \oplus H' \to H$ takie, że $\pi \circ \mu = \mathrm{Id}_H$.

Stwierdzenie 3.2

Niech G i H będą grupami.

Jeśli istnieją homomorfizmy $\mu\colon H \to G$ oraz $\pi\colon G \to H$ takie, że $\pi \circ \mu = \mathrm{Id}_H$, to

$$G \simeq H \oplus \operatorname{Ker} \pi.$$

Stwierdzenie 3.2

Niech G i H będą grupami.
Jeśli istnieją homomorfizmy $\mu\colon H \to G$ oraz $\pi\colon G \to H$ takie, że $\pi \circ \mu = \mathrm{Id}_H$, to

$$G \simeq H \oplus \operatorname{Ker}\pi.$$

Dowód

Definiujemy homomorfizm $\varphi\colon H \oplus \operatorname{Ker}\pi \to G$ wzorem

$$\varphi(h, g) := \mu(h) + g \qquad (h \in H,\ g \in \operatorname{Ker}\pi).$$

Pokażemy, że φ jest izomorfizmem.
1°. φ jest mono.
Ustalmy $h \in H$ i $g \in \operatorname{Ker}\pi$ takie, że $\mu(h) + g = 0$.
Wtedy

$$h = h + 0 = \pi(\mu(h)) + \pi(g) = \pi(\mu(h) + g) = \pi(0) = 0.$$

Ponadto,

$$g = -\mu(h) = -\mu(0) = -0 = 0.$$

2°. φ jest epi.
Ustalmy $g \in G$.
Niech

$$h := \pi(g) \qquad \text{i} \qquad g' := g - \mu(\pi(g)).$$

Wtedy

$$\pi(g') = \pi(g) - \pi(\mu(\pi(g)) = \pi(g) - \pi(g) = 0,$$

więc $(h, g') \in H \oplus \operatorname{Ker}\pi$.
Ponadto,

$$\varphi(h, g') = \mu(h) + g' = \mu(\pi(g)) + g - \mu(\pi(g)) = g. \qquad \square$$

Stwierdzenie 3.2

Niech G i H będą grupami.
Jeśli istnieją homomorfizmy $\mu\colon H \to G$ oraz $\pi\colon G \to H$ takie, że $\pi \circ \mu = \mathrm{Id}_H$, to

$$G \simeq H \oplus \operatorname{Ker} \pi.$$

Wniosek 3.3

Jeśli $H \leq G$ i istnieje homomorfizm $\pi\colon G \to H$ taki, że $\pi(h) = h$ dla każdego $h \in H$, to

$$G \simeq H \oplus \operatorname{Ker} \pi.$$

Dowód

Wynika natychmiast z (3.2) (jako $\mu\colon H \to G$ bierzemy naturalne włożenie). □

Wniosek 3.4

Jeśli $H' \leq G$ (grupy abelowe) i istnieje $\mu\colon G/H' \to G$ taki, że $\pi \circ \mu = \mathrm{Id}_{G/H'}$, gdzie $\pi\colon G \to G/H'$ jest naturalnym rzutowaniem, to

$$G \simeq G/H' \oplus H'.$$

Dowód

Wynika z (3.2), gdyż $\operatorname{Ker} \pi = H'$. □

3.2 Grupy cykliczne

Definicja

Grupę G nazywamy cykliczną, jeśli istnieje element $g \in G$ taki, że $G = \langle g \rangle$.
Element $g \in G$ taki, że $\langle g \rangle = G$, nazywamy generatorem grupy G.

Lemat 3.5

Niech $G = \langle X \rangle$.
Jeśli $\varphi, \psi \colon G \to H$ są homomorfizmami takimi, że $\varphi(g) = \psi(g)$ dla każdego $g \in X$, to $\varphi = \psi$.

Dowód

Niech G' będzie zbiorem elementów $g \in G$ takich, że $\varphi(g) = \psi(g)$.
Łatwo sprawdzić, że $G' \leq G$.
Ponadto z założenia $X \subseteq G'$, więc

$$G = \langle X \rangle \subseteq G' \subseteq G. \quad \square$$

Stwierdzenie 3.6

Niech $G = \langle g \rangle$ i $n := \mathrm{ord}(g) < \infty$.
Jeśli $h \in H$ i $\mathrm{ord}(h) \mid n$, to istnieje jedyny homomorfizm $\varphi\colon G \to H$ taki, że $\varphi(g) = h$.

Dowód

Jedność φ wynika z (3.5).
Wiemy z (1.32), że

$$G = \{k \cdot g : k \in \{0, 1, \ldots, n-1\}\}.$$

Definiujemy funkcję $\varphi\colon G \to H$ wzorem

$$\varphi(k \cdot g) := k \cdot h \qquad (k \in \{0, 1, \ldots, n-1\}).$$

Aby pokazać, że φ jest homomorfizmem, ustalmy $k, l \in \{0, 1, \ldots, n-1\}$.
Wtedy $k \cdot g + l \cdot g = ((k + l) \bmod n) \cdot g$, więc

$$\varphi(k \cdot g + l \cdot g) = ((k + l) \bmod n) \cdot h.$$

Z drugiej strony,

$$\varphi(k \cdot g) + \varphi(l \cdot g) = (k + l) \cdot h.$$

Stąd

$$(\varphi(k \cdot g) + \varphi(l \cdot g)) - \varphi(k \cdot g + l \cdot g) = (((k + l) \operatorname{div} n)n) \cdot h = 0,$$

gdyż $\mathrm{ord}(h) \mid n$.
Innymi słowy,

$$\varphi(k \cdot g + l \cdot g) = \varphi(k \cdot g) + \varphi(l \cdot g). \quad \square$$

Stwierdzenie 3.6

Niech $G = \langle g \rangle$ i $n := \mathrm{ord}(g) < \infty$.
Jeśli $h \in H$ i $\mathrm{ord}(h) \mid n$, to istnieje jedyny homomorfizm $\varphi\colon G \to H$ taki, że $\varphi(g) = h$.

Stwierdzenie 3.7

Jeśli G jest skończoną grupą cykliczną, to $G \simeq \mathbb{Z}_n$, gdzie $n := |G|$.

Dowód

Ustalmy generator g grupy G.
(3.6) $\implies$ istnieją homomorfizmy $\varphi\colon G \to \mathbb{Z}_n$ i $\psi\colon \mathbb{Z}_n \to G$ takie, że $\varphi(g) = 1$ i $\psi(1) = g$.
Wtedy $\varphi(\psi(1)) = 1$ i $\psi(\varphi(g)) = g$, więc $\varphi \circ \psi = \mathrm{Id}_{\mathbb{Z}_n}$ i $\psi \circ \varphi = \mathrm{Id}_G$ na mocy (3.6). □

Wniosek 3.8

Niech $g \in G$.

(1) Jeśli $\mathrm{ord}(g) < \infty$ i $k \cdot g = 0$ dla pewnego $k \in \mathbb{Z}$, to $\mathrm{ord}(g) \mid k$.

(2) Jeśli $k \cdot g = 0$ dla pewnego $k \neq 0$, to $\mathrm{ord}(g) < \infty$ (a więc w szczególności $\mathrm{ord}(g) \mid k$).

Dowód

(1) Niech $H := \langle g \rangle$ i $n := \mathrm{ord}(g)$.
(3.6) $\implies$ istnieje homomorfizm $\varphi\colon H \to \mathbb{Z}_n$ taki, że $\varphi(g) = 1$.
Ponieważ $k \cdot g = 0$, więc $k \cdot 1 = 0$ w $\mathbb{Z}_n$, zatem $n \mid k$.
(2) Jeśli $k \cdot g = 0$, to $|k| \cdot g = 0$.
Zatem, gdy $k \neq 0$, to $\{m \in \mathbb{N}_+ : m \cdot g = 1\} \neq \varnothing$.
Stąd $\mathrm{ord}(g) < \infty$ na mocy (1.32). □