Algebra I

Wykład XII

Grzegorz Bobiński (UMK)

Cel

Celem tego rozdziału jest udowodnienie, że jeśli G jest skończoną grupą abelową, to istnieją jednoznacznie wyznaczone $p_1, \ldots, p_k \in \mathbb{P}$ 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.

Na tym wykładzie zajmiemy się istnieniem.

Strategia

I Istnieją $p_1, \ldots, p_k \in \mathbb{P}$ oraz grupy $G_1, \ldots, G_k$ takie, że

$$G \simeq G_1 \oplus \cdots \oplus G_k$$

oraz $|G_i| = p_i^{m_i}$ dla każdego i.

II Jeśli $|G| = p^m$ dla $p \in \mathbb{P}$ i $m \in \mathbb{N}$, to istnieją $n_1, \ldots, n_l \in \mathbb{N}_+$ takie, że

$$G \simeq \mathbb{Z}_{p^{n_1}} \oplus \cdots \oplus \mathbb{Z}_{p^{n_l}}.$$

Przypomnienie

(3.8): $k \cdot g = 0 \implies \operatorname{ord}(g) \mid k$.

Krok I

Istnieją $p_1, \ldots, p_k \in \mathbb{P}$ takie, że

$$G \simeq G_1 \oplus \cdots \oplus G_k$$

oraz $|G_i| = p_i^{m_i}$ dla każdego i.

Lemat 3.11

Niech $p \in \mathbb{P}$.

Jeśli G jest skończoną grupą abelową taką, że $\mathrm{ord}(g)$ jest potęgą liczby p dla każdego $g \in G$, to $|G|$ jest również potęgą liczby p.

Dowód

Indukcja na $|G|$.

Gdy $|G| = 1$, to teza jest oczywista.

Załóżmy, że $|G| > 1$ i ustalmy $g \in G \setminus \{0\}$.

Niech $H := \langle g \rangle$.

Wtedy $|H| = \mathrm{ord}(g)$ jest potęgą liczby p.

Niech $G' := G/H$.

Wtedy $|G'| = \frac{|G|}{|H|} < |G|$.

Pokażemy za chwilę, że $\mathrm{ord}(x)$ jest potęgą liczby p dla każdego $x \in G'$.

Wtedy z założenia indukcyjnego otrzymamy, że $|G'|$ jest potęgą liczby p.

Ponieważ $|G| = |G'| \cdot |H|$, to zakończy dowód.

Ustalmy $x \in G'$. Wtedy $x = g + H$ dla pewnego $g \in G$.

Ponieważ $\mathrm{ord}(g) \cdot g = 0$, więc $\mathrm{ord}(g) \cdot x = \mathrm{ord}(g) \cdot (g + H) = 0 + H$, zatem $\mathrm{ord}(x) \mid \mathrm{ord}(g)$ (na mocy (3.8)). Ponieważ $\mathrm{ord}(g)$ jest potęga liczby p, więc $\mathrm{ord}(x)$ jest potęgą liczby p. □

Stwierdzenie 3.12

Jeśli G jest skończoną grupą abelową, to istnieją $p_1, \ldots, p_k \in \mathbb{P}$ oraz grupy $G_1, \ldots, G_k$ takie, że

$$G \simeq G_1 \oplus \cdots \oplus G_k$$

oraz $|G_i|$ jest potęga liczby p_i dla każdego i.

Dowód

Niech

$$|G| = p_1^{l_1} \cdots p_k^{l_k}$$

dla parami różnych $p_1, \ldots, p_k \in \mathbb{P}$ oraz $l_1, \ldots, l_k \in \mathbb{N}_+$.

Dla każdego i niech

$$G_i := \{g \in G \mid p_i^{l_i} \cdot g = 0\}.$$

Łatwo widać, że $G_1, \ldots, G_n \leq G$, gdyż grupa G jest abelowa.

(3.8) $\implies$ jeśli $g \in G_i$, to $\operatorname{ord}(g) \mid p_i^{l_i}$ $\implies$ $\operatorname{ord}(g)$ jest potęgą liczby p_i.

(3.11) $\implies$ $|G_i|$ jest potęgą liczby p_i dla każdego i.

Pokażemy, że

$$G \simeq G_1 \oplus \cdots \oplus G_k.$$

Dokładniej, pokażemy, że homomorfizm $\varphi\colon G_1 \oplus \cdots \oplus G_k \to G$ dany wzorem

$$\varphi(g_1, \ldots, g_k) := g_1 + \cdots + g_k \qquad (g_1 \in G_1, \ \ldots, \ g_k \in G_k),$$

jest izomorfizmem.

Setup

$$|G| = p_1^{l_1} \cdots p_k^{l_n}, \qquad G_i := \{g \in G \mid p_i^{l_i} \cdot g = 0\}.$$
$$\varphi\colon G_1 \oplus \cdots \oplus G_k \to G, \quad \varphi(g_1, \ldots, g_k) := g_1 + \cdots + g_k \qquad (g_1 \in G_1, \ \ldots, \ g_k \in G_k).$$

φ jest mono.

Przypuśćmy, że

$$g_1 + \cdots + g_k = 0$$

dla pewnych $g_1 \in G_1, \ldots, g_k \in G_k$.

Ustalmy $i \in \{1, \ldots, k\}$.

Wiemy, że istnieją $m, l \in \mathbb{Z}$ takie, że

$$mp_i^{l_i} + lp_1^{l_1} \cdots p_{i-1}^{l_{i-1}} p_{i+1}^{l_{i+1}} \cdots p_k^{l_k} = 1.$$

Wtedy

$$\begin{aligned} g_i &= 1 \cdot g_i = (mp_i^{l_i} + lp_1^{l_1} \cdots p_{i-1}^{l_{i-1}} p_{i+1}^{l_{i+1}} \cdots p_k^{l_k}) \cdot g_i \\ &= mp_i^{l_i} \cdot g_i + lp_1^{l_1} \cdots p_{i-1}^{l_{i-1}} p_{i+1}^{l_{i+1}} \cdots p_k^{l_k} \cdot g_i \\ &= 0 - lp_1^{l_1} \cdots p_{i-1}^{l_{i-1}} p_{i+1}^{l_{i+1}} \cdots p_k^{l_k} \cdot (g_1 + \cdots + g_{i-1} + g_{i+1} + \cdots + g_k) \\ &= -(0 + \cdots + 0) = 0. \end{aligned}$$

Setup

$$|G| = p_1^{l_1} \cdots p_k^{l_k}, \qquad G_i := \{g \in G \mid p_i^{l_i} \cdot g = 0\}.$$
$$\varphi\colon G_1 \oplus \cdots \oplus G_k \to G, \quad \varphi(g_1, \ldots, g_k) := g_1 + \cdots + g_k \qquad (g_1 \in G_1,\ \ldots,\ g_k \in G_k).$$

φ jest epi.

Niech $g \in G$.

Ponieważ

$$\mathrm{NWD}\Big(\frac{|G|}{p_1^{l_1}}, \ldots, \frac{|G|}{p_k^{l_k}}\Big) = 1,$$

więc istnieją $m_1, \ldots, m_k \in \mathbb{Z}$ takie, że

$$m_1 \frac{|G|}{p_1^{l_1}} + \cdots + m_k \frac{|G|}{p_k^{l_k}} = 1.$$

Niech

$$g_i := m_i \frac{|G|}{p_i^{l_i}} \cdot g, \qquad i = 1, \ldots, k.$$

Wtedy

$$p_i^{l_i} \cdot g_i = m_i |G| \cdot g = 0,$$

gdyż $\mathrm{ord}(g) \mid |G|$, więc $g_1 \in G_1,\ \ldots,\ g_k \in G_k$.

Ponadto

$$\varphi(g_1, \ldots, g_k) = g_1 + \cdots + g_k = m_1 \tfrac{|G|}{p_1^{l_1}} \cdot g + \cdots + m_k \tfrac{|G|}{p_k^{l_k}} \cdot g$$
$$= \Big(m_1 \tfrac{|G|}{p_1^{l_1}} + \cdots + m_k \tfrac{|G|}{p_k^{l_k}}\Big) \cdot g = 1 \cdot g = g,$$

co kończy dowód. □

Krok II

Jeśli $|G| = p^m$ dla $p \in \mathbb{P}$ i $m \in \mathbb{N}$, to istnieją $n_1, \ldots, n_l \in \mathbb{N}_+$ takie, że

$$G \simeq \mathbb{Z}_{p^{n_1}} \oplus \cdots \oplus \mathbb{Z}_{p^{n_l}}.$$

Lemat 3.9

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

$$\sup\{\mathrm{ord}(g) : g \in G\} \geq \sup\{\mathrm{ord}(h) : h \in H\}.$$

Dowód

Musimy pokazać, że dla każdego $h \in H$ istnieje $g \in G$ taki, że $\mathrm{ord}(h) \leq \mathrm{ord}(g)$.

Ustalmy $h \in H$.

Ponieważ φ jest epi, więc istnieje $g \in G$ taki, że $\varphi(g) = h$.

Jeśli $\mathrm{ord}(g) = \infty$, to oczywiście $\mathrm{ord}(g) \geq \mathrm{ord}(h)$.

W przeciwnym wypadku

$$\mathrm{ord}(g) \cdot h = \mathrm{ord}(g) \cdot \varphi(g) = \varphi(\mathrm{ord}(g) \cdot g) = \varphi(0) = 0,$$

więc $\mathrm{ord}(h) \leq \mathrm{ord}(g)$ na mocy (3.8) (lub (1.32)). □

Stwierdzenie 3.10

Niech G będzie grupą (abelową), której rząd jest potęgą liczby $p \in \mathbb{P}$.
Wtedy istnieją $n_1, \ldots, n_l \in \mathbb{N}_+$ takie, że

$$G \simeq \mathbb{Z}_{p^{n_1}} \oplus \cdots \oplus \mathbb{Z}_{p^{n_l}}.$$

Dowód

Indukcja ze względu na $|G|$.
Gdy $|G| = 1$, to teza jest oczywista (pusta suma prosta).
Jeśli $|G| > 1$, to wybierzmy $g_0 \in G$ taki, że

$$\operatorname{ord}(g_0) = \max\{\operatorname{ord}(g) : g \in G\}.$$

(1.31) $\implies$ $\operatorname{ord}(g_0) \mid |G|$.
W szczególności, $\operatorname{ord}(g_0) = p^{n_0}$ dla pewnego $n_0 \in \mathbb{N}_+$.
Niech $H := \langle g_0 \rangle$.
(3.7) $\implies$ $H \simeq \mathbb{Z}_{p^{n_0}}$.
(1.30) $\implies$ $|G/H| = |G|/|H|$ jest potęgą liczby p i $|G/H| < |G|$.
(ZI) $\implies$ $n_1, \ldots, n_l \in \mathbb{N}_+$ takie, że

$$G/H \simeq \mathbb{Z}_{p^{n_1}} \oplus \cdots \oplus \mathbb{Z}_{p^{n_l}}.$$

Powyższy izomorfizm będziemy traktować jako utożsamienie.
Dla zakończenia dowodu wystarczy pokazać, że $G \simeq H \oplus G/H$.
Na mocy (3.4) w tym celu należy skonstruować homomorfizm $\mu\colon G/H \to G$ taki, że $(\pi \circ \mu)(x) = x$ dla każdego $x \in G/H$, gdzie $\pi\colon G \to G/H$ jest naturalnym rzutowaniem.

Setup

$H = \langle g_0 \rangle$, $\operatorname{ord}(g_0) = p^{n_0} = \max\{\operatorname{ord}(g) : g \in G\}$,
$\pi\colon G \to \mathbb{Z}_{p^{n_1}} \oplus \cdots \oplus \mathbb{Z}_{p^{n_l}}$ epimorfizm taki, że $\operatorname{Ker}\pi = H$.
Cel: Skonstruować $\mu\colon \mathbb{Z}_{p^{n_1}} \oplus \cdots \oplus \mathbb{Z}_{p^{n_l}} \to G$ taki, że $\pi \circ \mu = \mathrm{Id}_{\mathbb{Z}_{p^{n_1}} \oplus \cdots \oplus \mathbb{Z}_{p^{n_l}}}$.

Niech $e_i := (0, \ldots, 0, 1, 0, \ldots, 0)$, przy czym 1 jest na i-tym miejscu.
Zauważmy, że $\operatorname{ord}(e_i) = p^{n_i}$, więc $p^{n_i} = \operatorname{ord}(e_i) \leq p^{n_0}$ na mocy (3.9), zatem $n_i \leq n_0$.
Wybierzmy $g_i' \in G$ takie, że $\pi(g_i') = e_i$.
Mamy

$$\pi(p^{n_i} \cdot g_i') = p^{n_i} \cdot \pi(g_i') = p^{n_i} \cdot e_i = (0, \ldots, 0),$$

więc $p^{n_i} \cdot g_i' \in \operatorname{Ker}\pi = H$.
Stąd $p^{n_i} \cdot g_i' = k_i \cdot g_0$ dla pewnego $k_i \in \mathbb{Z}$.

Wiemy, że $\operatorname{ord}(g_i') = p^{n_i'}$ dla pewnego $n_i' \leq n_0$.

Stąd $p^{n_0} \cdot g_i' = p^{n_0 - n_i'} p^{n_i'} \cdot g_i' = p^{n_0 - n_i'} \cdot 0 = 0$, więc
$p^{n_0 - n_i} k_i \cdot g_0 = p^{n_0 - n_i} p^{n_i} \cdot g_i' = p^{n_0} \cdot g_i' = 0$, zatem $p^{n_0} \mid p^{n_0 - n_i} k_i$ na mocy (3.8).
Z powyższego $p^{n_i} \mid k_i$, więc istnieje $k_i' \in \mathbb{Z}$ taka, że $k_i = p^{n_i} k_i'$.
Niech $g_i := g_i' - k_i' \cdot g_0$.
Wtedy $\pi(g_i) = \pi(g_i') = e_i$ oraz

$$p^{n_i} \cdot g_i = p^{n_i} \cdot g_i' - p^{n_i} k_i' \cdot g_0 = k_i \cdot g_0 - k_i \cdot g_0 = 0.$$

W szczególności, $\operatorname{ord}(g_i) \mid p^{n_i} = \operatorname{ord}(e_i)$ na mocy (3.8).
(3.6) + (3.1) $\implies$ istnieje homomorfizm $\mu\colon \mathbb{Z}_{p^{n_1}} \oplus \cdots \oplus \mathbb{Z}_{p^{n_l}} \to G$ taki, że $\mu(e_i) = g_i$ dla każdego i.
Wtedy $\pi(\mu(e_i)) = \pi(g_i) = e_i$ dla każdego i, więc $\pi \circ \mu = \mathrm{Id}_{\mathbb{Z}_{p^{n_1}} \oplus \cdots \oplus \mathbb{Z}_{p^{n_l}}}$ na mocy (3.5). □

Stwierdzenie 3.12

Jeśli G jest skończoną grupą abelową, to istnieją $p_1, \ldots, p_k \in \mathbb{P}$ oraz grupy $G_1, \ldots, G_k$ takie, że

$$G \simeq G_1 \oplus \cdots \oplus G_k$$

oraz $|G_i| = p_i^{m_i}$ dla każdego i.

Stwierdzenie 3.10

Niech G będzie grupą (abelową), której rząd jest potęgą liczby $p \in \mathbb{P}$.
Wtedy istnieją $n_1, \ldots, n_l \in \mathbb{N}_+$ takie, że

$$G \simeq \mathbb{Z}_{p^{n_1}} \oplus \cdots \oplus \mathbb{Z}_{p^{n_l}}.$$

Wniosek 3.13

Jeśli G jest skończoną grupą abelową, to istnieją $p_1 < \cdots < p_n \in \mathbb{P}$, $l_1, \ldots, l_n \in \mathbb{N}_+$ oraz $n_{ij} \in \mathbb{N}_+$, $i = 1, \ldots, n$, $j = 1, \ldots, l_i$, takie, że

$$G \simeq \bigoplus_{i=1}^{n} \bigoplus_{j=1}^{l_i} \mathbb{Z}_{p^{n_{ij}}}. \quad \square$$