7. Wykład 7: Przestrzenie wektorowe i wymiar.

Rezultaty dotyczące rangi wolnych grup abelowych (część (3) Twierdzenia 6.1 oraz Twierdzenie 6.2) nie przenoszą się bezpośrednio na moduły wolne i wymagają bardziej finezyjnego podejścia. Omówimy teraz pokrótce te zagadnienia.

Twierdzenie 7.1. *Niech R będzie pierścieniem z jedynką, niech M będzie lewym R-modułem wolnym z nieskończoną bazą $\{f_i : i \in I\}$. Wówczas dowolna baza M jest równoliczna z $\{f_i : i \in I\}$.*

Dowód. Załóżmy, że $M = \sum_{i\in I}\langle f_i\rangle$, gdzie $\langle f_i\rangle \cong R$, $i \in I$ i ustalmy dowolną bazę $\{g_j : j \in J\}$ modułu M, to znaczy niech $M \cong \sum_{j\in J}\langle g_j\rangle$, gdzie $\langle g_j\rangle \cong R$, $j \in J$.

Pokażemy najpierw, że baza $\{g_j : j \in J\}$ jest nieskończona. Przypuśćmy bowiem, że $\{g_j : j \in J\}$ jest skończona. Ponieważ zbiór $\{g_j : j \in J\}$ w szczególności generuje M oraz każdy element g_j, $j \in J$, jest skończoną kombinacją elementów f_i, $i \in I$, istnieje skończony zbiór $\{f_1, \dots, f_m\} \subset \{f_i : i \in I\}$ generujący M. Ponieważ baza $\{f_i : i \in I\}$ jest nieskończona, istnieje element $f \in \{f_i : i \in I\}\backslash\{f_1, \dots, f_m\}$. Wówczas $f = \sum_{i=1}^{m} x_i f_i$, dla pewnych $x_i \in R$, oraz $f = f$ są dwoma różnymi przedstawieniami $f \in M$, co daje sprzeczność.

Niech $\mathcal{P}(\{g_j : j \in J\})$ oznacza rodzinę wszystkich skończonych podzbiorów zbioru $\{g_j : j \in J\}$. Zdefiniujmy odwzorowanie $\Phi : \{f_i : i \in I\} \to \mathcal{P}(\{g_j : j \in J\})$ wzorem

$$\Phi(f) = \{g_1, \dots, g_n\}, \text{ jeżeli } f \text{ ma przedstawienie } f = \sum_{j=1}^{n} x_j g_j \text{ dla pewnych } x_i \in R\backslash\{0\}.$$

Ponieważ $\{g_j : j \in J\}$ jest bazą, elementy $g_1, \dots, g_n$ są jednoznacznie wyznaczone i Φ jest niniejszym dobrze określoną funkcją.

Pokażemy, że $\operatorname{im}\Phi$ jest nieskończony. Na odwrót, przypuśćmy, że $\operatorname{im}\Phi$ jest skończony. Wówczas $\bigcup_{S\in\operatorname{im}\Phi} S$ jest skończonym podzbiorem $\{g_j : j \in J\}$ generującym $\{f_i : i \in I\}$, a więc M. Jak poprzednio, ponieważ baza $\{g_j : j \in J\}$ jest nieskończona, istnieje element $g \in \{g_j : j \in J\}\backslash\bigcup_{S\in\operatorname{im}\Phi} S$. Wówczas $g = \sum_{g_i\in\bigcup_{S\in\operatorname{im}\Phi} S} x_i g_i$, dla pewnych $x_i \in R$, oraz $g = g$, co daje sprzeczność.

Ustalmy $T \in \operatorname{im}\Phi$. Pokażemy, że zbiór $\Phi^{-1}(T)$ jest skończony. Ustalmy w tym celu element $f \in \Phi^{-1}(T)$. Wówczas $f \in \langle T\rangle$. Wobec tego $\Phi^{-1}(T) \subset \langle T\rangle$. Ponieważ T jest skończony i każdy element $g \in T$ jest skończoną kombinacją f_i, $i \in I$, istnieje skończony podzbiór $S \subset \{f_i : i \in I\}$ taki, że $\langle T\rangle \subset \langle S\rangle$. Wobec tego $f \in \langle S\rangle$ i f jest kombinacją elementów zbioru S, a zatem $f \in S$, w przeciwnym bowiem razie otrzymujemy dwa możliwe przedstawienia elementu f. Tym samym $\Phi^{-1}(T) \subset S$ i jako taki jest skończony.

Niech $\Phi^{-1}(T) = \{f_1, \dots, f_n\}$ i zdefiniujmy odwzorowanie $\Psi_T : \Phi^{-1}(T) \to \operatorname{im}\Phi \times \mathbb{N}$ wzorem

$$\Psi_T(f_k) = (T, k).$$

Bez trudu sprawdzamy, że odwzorowanie Ψ_T jest różnowartościowe i że rodzina $\{\Phi^{-1}(T) : T \in \operatorname{im}\Phi\}$ tworzy partycję zbioru $\{f_i : i \in I\}$. Dalej, zdefiniujmy odwzorowanie $\Psi : \{f_i : i \in I\} \to \operatorname{im}\Phi \times \mathbb{N}$ wzorem

$$\Psi(f_k) = \Psi_T(f_k), \text{ o ile } f_k \in \Phi^{-1}(T).$$

Znowu łatwo sprawdzamy, że Ψ jest różnowartościowe i dobrze zdefiniowane. Wobec tego $|\{f_i : i \in I\}| \leqslant |\operatorname{im}\Phi \times \mathbb{N}|$ i tym samym

$$|\{f_i : i \in I\}| \leqslant |\operatorname{im}\Phi \times \mathbb{N}| = |\operatorname{im}\Phi| \cdot \aleph_0 = |\operatorname{im}\Phi| \leqslant |\mathcal{P}(\{g_j : j \in J\})| = |\{g_j : j \in J\}|.$$

Powtarzając rozumowanie z $\{f_i : i \in I\}$ i $\{g_j : j \in J\}$ zamienionymi miejscami otrzymujemy również $|\{f_i : i \in I\}| \geqslant |\{g_j : j \in J\}|$, co kończy dowód. □

Definicja 7.1. *Niech R będzie pierścieniem z jedynką. Jeżeli dowolny niezerowy element R ma element odwrotny, to R nazywamy* **pierścieniem z dzieleniem** *(lub* **ciałem nieprzemiennym**, *lub* **ciałem skośnym**).

Twierdzenie 7.2. *Niech R będzie pierścieniem z dzieleniem, M lewym R-modułem wolnym z bazą $\{f_i : i \in I\}$. Wówczas dowolna baza M jest równoliczna z $\{f_i : i \in I\}$.*

Dowód. Załóżmy, że $M = \sum_{i\in I}\langle f_i\rangle$, gdzie $\langle f_i\rangle \cong R$, $i \in I$ i ustalmy dowolną bazę $\{g_j : j \in J\}$ modułu M, to znaczy niech $M \cong \sum_{j\in J}\langle g_j\rangle$, gdzie $\langle g_j\rangle \cong R$, $j \in J$.

Jeżeli $|\{f_i : i \in I\}| = \infty$ lub $|\{g_j : j \in J\}| = \infty$, to wobec poprzedniego twierdzenia $|\{f_i : i \in I\}| = |\{g_j : j \in J\}|$. Załóżmy więc, że $\{f_i : i \in I\} = \{f_1, \ldots, f_n\}$ oraz $\{g_j : j \in J\} = \{g_1, \ldots, g_m\}$. Niech $g_m = r_1f_1 + \ldots + r_nf_n$, dla pewnych $r_1, \ldots, r_n \in R$ i powiedzmy, że r_k jest niezerowym elementem o najniższym indeksie. Wówczas $f_k = r_k^{-1}g_m - r_k^{-1}r_{k+1}f_{k+1} - \ldots - r_nf_n$. Wobec tego zbiór $\{g_m, f_1, \ldots, f_{k-1}, f_{k+1}, \ldots, f_n\}$ generuje M. Tym samym $g_{m-1} = s_mg_m + t_1f_1 + \ldots + t_{k-1}f_{k-1} + t_{k+1}f_{k+1} + \ldots + t_nf_n$, dla pewnych $s_m, t_1, \ldots, t_{k-1}, t_{k+1}, \ldots, t_n \in R$. Nie wszystkie t_i są równe zeru (w przeciwnym razie $g_{m-1} - s_mg_m = 0$ dawałoby nietrywialne przedstawienie 0 jako kombinacji $g_1, \ldots, g_m$), niech więc t_j będzie elementem niezerowym o najniższym indeksie. Wówczas $x_j = t_j^{-1}g_{m-1} - t_j^{-1}s_mg_m - t_j^{-1}t_{j+1}f_{j+1} - \ldots - t_j^{-1}t_nf_n$. Wobec tego zbiór $\{g_m, g_{m-1}\} \cup \{f_1, \ldots, f_n\}\backslash\{f_j, f_k\}$ generuje M. Tym samym g_{m-2} jest kombinacją liniową g_m, g_{m-1} i f_i, dla $i \in \{1, \ldots, n\}\backslash\{j, k\}$. Proces dodawania kolejnych g_i i eliminowania kolejnych f_l może być kontynuowany. Pod koniec k-tego kroku otrzymujemy zbiór $\{g_m, g_{m-1}, \ldots, g_{m-k+1}\}$ wraz ze zbiorem $n-k$ elementów f_i, których suma mnogościowa generuje M. Jeśli $n < m$, to pod koniec n-tego kroku otrzymamy, że $\{g_m, \ldots, g_{m-n+1}\}$ generuje M. Ponieważ $m - n + 1 \geqslant 2$, element g_1 byłby liniową kombinacją $\{g_m, \ldots, g_{m-n+1}\}$, co jest niemożliwe. Zatem $n \geqslant m$. Powtarzając rozumowanie z $\{f_i : i \in I\}$ i $\{g_j : j \in J\}$ zamienionymi miejscami otrzymujemy $n = m$. □

Definicja 7.2. *Niech R będzie pierścieniem z jedynką. Jeżeli dla dowolnego lewego R-modułu wolnego M każde dwie bazy są tej samej mocy, to mówimy, że R ma* **własność niezmiennika bazowego** *(lub że jest pierścieniem* **IBP,** invariant basis property*).*

Jeżeli R jest pierścieniem z własnością niezmiennika bazowego, a M lewym R-modułem wolnym, to moc dowolnej bazy modułu M nazywamy jego **rangą.**

Przykład:

(4) Niech R będzie pierścieniem z dzieleniem. Wówczas R ma własność niezmiennika bazowego.

Lemat 7.1. *Niech R będzie pierścieniem z jedynką, niech $I \lhd R$, niech M będzie lewym R-modułem wolnym z bazą $\{f_j : j \in J\}$, niech $\kappa : M \to M/IM$ oznacza epimorfizm kanoniczny oraz*

$$IM = \{r_1m_1 + \ldots + r_nm_n : r_i \in I, m_i \in M, n \in \mathbb{N}\}.$$

Wówczas M/IM jest lewym R/I-modułem wolnym z bazą $\{\kappa(f_j) : j \in J\}$ oraz $|\{f_j : j \in J\}| = |\{\kappa(f_j) : j \in J\}|$.

Dowód. Bez trudu sprawdzamy, że M/IM jest lewym R/I-modułem z mnożeniem zdefiniowanym jako

$$(r + I)(m + IM) = rm + IM, \text{ dla } r + I \in R/I, m + IM \in M/IM.$$

Ustalmy $m + IM \in M/IM$. Wówczas $m = r_1f_1 + \ldots + r_nf_n$, dla pewnych $r_i \in R$, $f_i \in \{f_j : j \in J\}$. Stąd:

$$\begin{aligned} m + IM &= (r_1f_1 + \ldots + r_nf_n) + IM \\ &= (r_1f_1 + IM) + \ldots + (r_nf_n + IM) \\ &= (r_1 + I)(f_1 + IM) + \ldots + (r_n + I)(f_n + IM) \\ &= (r_1 + I)\kappa(f_1) + \ldots + (r_n + I)\kappa(f_n). \end{aligned}$$

Wobec tego zbiór $\{\kappa(f_j) : j \in J\}$ generuje M/IM.

Załóżmy, że $(r_1 + I)\kappa(f_1) + \ldots + (r_m + I)\kappa(f_m) = 0$ dla pewnych $r_i \in R$, $f_i \in \{f_j : j \in J\}$. Wówczas:

$$0 = \sum_{i=1}^{m}(r_i + I)\kappa(f_i) = \sum_{i=1}^{m}(r_i + I)(f_i + IM) = \sum_{i=1}^{m} r_i f_i + IM,$$

skąd $\sum_{i=1}^{m} r_i f_i \in IM$. Zatem $\sum_{i=1}^{m} r_i f_i = \sum_{j=1}^{k} s_j g_j$, dla pewnych $s_j \in I$, $g_j \in M$. Ponieważ każdy g_j jest kombinacją $\{f_j : j \in J\}$ oraz I jest ideałem, $\sum_{j=1}^{k} s_j g_j$ jest kombinacją elementów zbioru $\{f_j : j \in J\}$ ze współczynnikami z I:

$$\sum_{i=1}^{m} r_i f_i = \sum_{j=1}^{k} s_j g_j = \sum_{l=1}^{d} c_l h_l, \text{ dla pewnych } c_l \in I, h_l \in \{f_j : j \in J\}.$$

Stąd $m = d$, $r_i = c_i$, $f_i = h_i$, a więc $r_i + I = 0$ w R/I dla $i \in \{1, \ldots, m\}$, czyli $\{\kappa(f_j) : j \in J\}$ jest liniowo niezależny nad R/I.

Niech $f_i, f_j \in \{f_j : j \in J\}$ oraz niech $\kappa(f_i) = \kappa(f_j)$. Wówczas

$$(1_R + I)\kappa(f_i) - (1_R + I)\kappa(f_j) = 0.$$

Gdyby $f_i \neq f_j$, to wówczas $1_R \in I$, co byłoby sprzecznością. Zatem $f_i = f_j$ i κ jest różnowartościowe. □

Twierdzenie 7.3. *Niech R i S będą pierścieniami z jedynką, niech $f : R \to S$ będzie epimorfizmem. Jeśli S ma własność niezmiennika bazowego, to R również ma własność niezmiennika bazowego.*

Dowód. Niech $I = \ker f$. Wówczas oczywiście $R/I \cong S$. Niech M będzie lewym R-modułem wolnym a $\{f_i : i \in I\}$ oraz $\{g_j : j \in J\}$ jego bazami. Niech $\kappa : M \to M/IM$ oznacza epimorfizm kanoniczny. Wobec poprzedniego lematu M/IM jest R/I-modułem wolnym z bazami $\{\kappa(f_i) : i \in I\}$ oraz $\{\kappa(g_j) : j \in J\}$. Ponieważ $R/I \cong S$, więc $|\{\kappa(f_i) : i \in I\}| = |\{\kappa(g_j) : j \in J\}|$, skąd $|\{f_i : i \in I\}| = |\{g_j : j \in J\}|$. □

Przykłady:

(5) Niech R będzie pierścieniem przemiennym z jedynką. Wówczas R ma własnóść niezmiennika bazowego; faktycznie, (0) można rozszerzyć do ideału maksymalnego I, a zatem R/I jest ciałem, w szczególności zaś pierścieniem z dzieleniem oraz $\kappa : R \to R/I$ jest surjekcją.

(6) Niech R będzie pierścieniem lokalnym z jedynką. Wówczas R ma własność niezmiennika bazowego; faktycznie, R ma dokładnie jeden lewy ideał maksymalny I, a zatem – naśladując dowód twierdzenia, orzekającego, iż pierścień ilorazowy pierścienia przemiennego z jedynką modulo ideał maksymalny jest ciałem – stwierdzamy, że R/I jest pierścieniem z dzieleniem oraz $\kappa : R \to R/I$ jest surjekcją.

(7) Niech R będzie pierścieniem skończonym. Wówczas R ma własność niezmiennika bazowego; faktycznie, $R^m \cong R^n$ pociąga $|R^m| = |R^n|$.