6. Wykład 6: Wolne grupy abelowe. Moduły wolne.

Definicja 6.1. *Grupę abelową $(F,+)$ nazywamy* **wolną grupą abelową,** *gdy $F = \sum_{i\in I}\langle f_i\rangle$, gdzie $r(f_i) = +\infty$, $i \in I$. Rodzinę $\{f_i : i \in I\}$ nazywamy* **bazą** *(lub* **zbiorem wolnych generatorów***) wolnej grupy abelowej F.*

Twierdzenie 6.1. (1) *Niech F będzie wolną grupą abelową z bazą $\{f_i : i \in I\}$. Każdy element $f \in F$ ma jednoznaczne przedstawienie postaci*

$$f = \sum_{i\in I} x_i f_i,$$

gdzie $x_i \in \mathbb{Z}$ oraz $x_i = 0$ dla prawie wszystkich $i \in I$.

(2) *Istnieje wolna grupa abelowa o bazie dowolnej mocy.*

(3) *Każde dwie wolne grupy abelowe o bazach równej mocy są izomorficzne.*

Dowód. (1) Teza wynika wprost z definicji koproduktu grup abelowych.

(2) Ustalmy liczbę kardynalną $\mathfrak{m}$ i niech I będzie takim zbiorem, że $|I| = \mathfrak{m}$. Wówczas grupa $\sum_{i\in I}\mathbb{Z}$ jest wolną grupą abelową.

(3) Ustalmy wolne grupy abelowe F i G o bazach $\{f_i : i \in I\}$ i $\{g_j : j \in J\}$, odpowiednio, gdzie $|I| = |J|$. Istnieje wówczas zbiór K taki, że $\{f_i : i \in I\} = \{f_k : k \in K\}$ oraz $\{g_j : j \in J\} = \{g_k : k \in K\}$ i możemy zdefiniować odwzorowanie $\phi : F \to G$ wzorem

$$\phi(\sum_{k\in K} x_k f_k) = x_k g_k.$$

Bez trudu sprawdzamy, że ϕ jest homomorfizmem i bijekcją, a więc izomorfizmem.

□

Twierdzenie 6.2. *Dowolne dwie bazy wolnej grupy abelowej są tej samej mocy.*

Dowód. Ustalmy wolną grupę abelową F z bazą $\{f_i : i \in I\}$. Oznaczmy $nF = \{nf : f \in F\}$. Zauważmy, że nF jest wolną grupą abelową, dla $n \in \mathbb{N}$: istotnie, dla ustalonego $n \in \mathbb{N}$ bez trudu widzimy, że $nF = \sum_{i\in I}\langle nf_i\rangle$ oraz $r(nf_i) = \infty$, $i \in I$.

Ustalmy liczbę pierwszą p i rozważmy grupę ilorazową F/pF. Zdefiniujmy działanie $\cdot : \mathbb{Z}_p \times F/pF \to F/pF$ wzorem

$$x \cdot (f + pF) = xf + pF, \text{ dla } x \in \mathbb{Z}_p, f + pF \in F/pF.$$

Łatwo sprawdzamy, że F/pF jest przestrzenią wektorową nad ciałem $\mathbb{Z}_p$. Pokażemy, że $\{f_i + pF : i \in I\}$ jest bazą przestrzeni F/pF.

Oczywiście $\{f_i + pF : i \in I\}$ jest układem generatorów dla F/pF i wystarczy pokazać, że jest też układem liniowo niezależnym. Ustalmy $n \in N$ i załóżmy, że dla pewnych $x_1, \ldots, x_n \in \mathbb{Z}_p$ zachodzi

$$x_1(f_{i_1} + pF) + \ldots + x_n(f_{i_n} + pF) = 0 + pF.$$

Wówczas $x_1 f_{i_1} + \ldots + x_n f_{i_n} \in pF$, czyli dla pewnych $y_{j_1}, \ldots, y_{j_m} \in \mathbb{Z}_p$:

$$x_1 f_{i_1} + \ldots + x_n f_{i_n} = y_{j_1} p f_{j_1} + \ldots + y_{j_m} p f_{j_m},$$

skąd $n = m$, $i_1 = j_1, \ldots, i_n = j_n$ oraz

$$x_1 = y_1 p, \ldots, x_n = y_n p,$$

czyli $x_1 = \ldots = x_n = 0$ w $\mathbb{Z}_p$.

Ponieważ moc dowolnych dwóch baz przestrzeni liniowej jest taka sama, więc i moc dowolnych dwóch baz wolnej grupy abelowej jest taka sama. □

Definicja 6.2. *Niech F będzie wolną grupą abelową. Moc dowolnej jej bazy nazywamy* **rangą** *wolnej grupy abelowej i oznaczamy* $\operatorname{rank} F$.

Wniosek 6.1. *Dowolne dwie wolne grupy abelowe są izomorficzne wtedy i tylko wtedy, gdy mają równe rangi.*

Twierdzenie 6.3 (własność uniwersalna wolnych grup abelowych)**.** *Niech $(F,+)$ będzie grupą abelową. Wówczas F jest wolną grupą abelową o bazie $\{f_i : i \in I\}$ wtedy i tylko wtedy, gdy dla dowolnej grupy abelowej H i jej rodziny elementów $\{h_i : i \in I\}$ istnieje dokładnie jeden homomorfizm $h : F \to H$ taki, że $h(f_i) = h_i$.*

Dowód. ($\Rightarrow$): Zdefiniujmy odwzorowanie $h : F \to H$ wzorem

$$h(\sum_{i\in I} x_i f_i) = \sum_{i\in I} x_i h_i,$$

gdzie $x_i \in \mathbb{Z}$ oraz $x_i = 0$ dla prawie wszystkich $i \in I$, zaś w grupie H przyjęliśmy notację addytywną. Bez trudu sprawdzamy, że h jest dobrze określonym homomorfizmem o żądanych własnościach.

($\Leftarrow$) : Załóżmy, że dla dowolnej grupy abelowej H i jej rodziny elementów $\{h_i : i \in I\}$ istnieje homomorfizm $h : F \to H$ taki, że $h(f_i) = h_i$. Wobec Twierdzenia 6.1 (3) istnieje wolna grupa abelowa B o bazie $\{h_i : i \in I\}$. Homomorfizm h jest wtedy izomorfizmem wolnych grup abelowych, a więc w szczególności F jest wolna. □

Twierdzenie 6.4. *Każda grupa abelowa jest homomorficznym obrazem pewnej wolnej grupy abelowej.*

Dowód. Pokażemy, że dla każdej grupy abelowej A istnieje wolna grupa abelowa F i jej podgrupa H taka, że $A \cong F/H$. Niech $\{a_i : i\imath I\}$ będzie zbiorem generatorów grupy A. Wobec Twierdzenia 6.1 (3) istnieje wolna grupa abelowa F o bazie $\{a_i : i \in I\}$. Wobec Twierdzenia 6.3 istnieje homomorfizm $h : F \to A$, który w tym wypadku będzie surjekcją. Niech $H = \ker h$. Wówczas $H < F$ i stosując twierdzenie o izomorfizmie otrzymujemy, że $A \cong F/H$. □

Twierdzenie 6.5. *Podgrupa wolnej grupy abelowej jest wolną grupą abelową.*

Lemat 6.1. *Niech $(F,+)$ będzie grupą abelową. Wówczas F jest wolną grupą abelową wtedy i tylko wtedy, gdy istnieje rosnący ciąg podgrup*

$$\{0\} = N_0 \subsetneq N_1 \subsetneq \ldots \subsetneq N_\alpha \subsetneq \ldots \subsetneq N_\gamma = F, \alpha, \gamma \in Ord$$

taki, że dla dowolnych $\alpha < \gamma$

$$N_{\alpha+1}/N_\alpha \cong \mathbb{Z}.$$

Dowód. ($\Leftarrow$) : Niech F będzie grupą abelową i niech

$$\{0\} = N_0 \subsetneq N_1 \subsetneq \ldots \subsetneq N_\alpha \subsetneq \ldots \subsetneq N_\gamma = F, \alpha, \gamma \in Ord$$

będzie takim rosnącym ciągiem podgrup, że dla dowolnych $\alpha < \gamma$

$$N_{\alpha+1}/N_\alpha \cong \mathbb{Z}.$$

Niech dla $\alpha < \gamma$ element $a_{\alpha+1} \in N_{\alpha+1}$ będzie taki, że

$$N_{\alpha+1}/N_\alpha = \langle a_{\alpha+1} + N_\alpha \rangle.$$

Stosując indukcję pozaskończoną, pokażemy, że $F = \sum_{\alpha<\gamma} \langle a_{\alpha+1} \rangle$. Dla $\gamma = 1$ teza jest oczywista. Dla $\gamma > 1$ załóżmy, że dla wszystkich $\alpha < \gamma$ twierdzenie jest prawdziwe. Ustalmy $0 \neq g \in F$. Niech $\beta \in Ord$ będzie taką liczbą, że $g \in N_\beta$ i $g \notin N_{\beta-1}$. Ponieważ $N_\beta/N_{\beta-1} = \langle a_\beta + N_{\beta-1} \rangle$, więc istnieją liczba $n \in \mathbb{N}$

i element $g_1 \in N_{\beta-1}$ takie, że $g = na_\beta + g_1$. Ponieważ $\beta - 1 < \gamma$, więc na mocy założenia indukcyjnego istnieje dokładnie jedno przedstawienie

$$g_1 = n_1 a_1 + \ldots + n_{\beta-1} a_{\beta-1},$$

gdzie $n_\alpha \in \mathbb{Z}$ i $n_\alpha = 0$ dla prawie wszystkich $\alpha < \beta - 1$. Stąd

$$g = n_1 a_1 + \ldots + n_{\beta-1} a_{\beta-1} + n a_\beta.$$

Pozostaje sprawdzić, że $r(a_{\alpha+1}) = \infty$, $\alpha < \gamma$. Przypuśćmy, że $r(a_{\beta+1}) < \infty$, dla pewnego $\beta < \gamma$. Wówczas $r(a_{\beta+1} + N_\beta) < \infty$ i $\mathbb{Z} \cong N_{\beta+1}/N_\beta \supsetneq \langle a_{\beta+1} + N_\beta \rangle$, wbrew wyborowi $a_{\beta+1}$.

($\Rightarrow$) : Niech F będzie wolną grupą abelową o bazie $\{f_\alpha : \alpha < \gamma\}$. Definiujemy ciąg:

- $N_0 = \{0\}$,
- $N_{\alpha+1} = \langle f_{\alpha+1} + N_\alpha \rangle$, gdy α nie jest graniczna,
- $N_\alpha = \bigcup_{\beta<\alpha} N_\beta$, gdy α jest graniczna.

Wówczas $\{0\} = N_0 \subsetneq N_1 \subsetneq \ldots \subsetneq N_\alpha \subsetneq \ldots \subsetneq N_\gamma$ jest rosnącym ciągiem podgrup i $N_{\alpha+1}/N_\alpha \cong \mathbb{Z}$. □

Przechodzimy teraz do dowodu twierdzenia.

Dowód. Niech F będzie wolną grupą abelową, niech $A < F$ i niech

$$\{0\} = N_0 \subsetneq N_1 \subsetneq \ldots \subsetneq N_\alpha \subsetneq \ldots \subsetneq N_\gamma = F$$

będzie takim rosnącym ciągiem podgrup, że dla dowolnych $\alpha < \gamma$

$$N_{\alpha+1}/N_\alpha \cong \mathbb{Z}.$$

Rozważmy ciąg

$$\{0\} = A \cap N_0 \subseteq A \cap N_1 \subseteq \ldots \subseteq A \cap N_\alpha \subseteq \ldots \subseteq A \cap N_\gamma = A$$

i – ewentualnie zmieniając numerację – wyrzućmy wszystkie składniki, w których nie zachodzą ostre inkluzje. Otrzymujemy ciąg:

$$\{0\} = A \cap N_0 \subseteq A \cap N_{i_1} \subseteq \ldots \subseteq A \cap N_{i_\alpha} \subseteq \ldots \subseteq A \cap N_\tau = A.$$

Ponieważ F jest abelowa, więc $A \lhd F$, a zatem

$$A \cap N_{\alpha+1}/A \cap N_\alpha \cong N_{\alpha+1}/N_\alpha \cong \mathbb{Z}, \text{ dla } \alpha < \gamma.$$

□

Twierdzenie 6.6 (o składniku prostym)**.** *Niech $(A, +)$ będzie grupą abelową.*

(1) *Niech F będzie wolną grupą abelową, a $h : A \to F$ homomorfizmem surjektywnym. Wówczas istnieje podgrupa $F' < A$ taka, że*

$$F \cong F' \text{ oraz } A = F' \oplus \ker h.$$

(2) *Niech H będzie podrupą grupy A a A/H wolną grupą abelową. Wówczas istnieje podgrupa $B < A$ taka, że*

$$B \text{ jest wolną grupą abelową oraz } A = B \oplus H.$$

Dowód. (1) Niech F będzie wolną grupą abelową o bazie $\{f_i : i \in I\}$. Niech $a_i \in A$, $i \in I$, będzie takim elementem, że $h(a_i) = f_i$, niech $F' = \langle \{a_i : i \in I\} \rangle$. Oczywiście F' jest wolną grupą abelową. Pozostaje sprawdzić, że $A = F' \oplus \ker h$.

Ustalmy $a \in A$. Wówczas

$$h(a) = \sum_{i \in I} x_i f_i = h\left(\sum_{i \in I} x_i a_i\right).$$

Zatem $a - \sum_{i \in I} x_i a_i \in \ker h$, skąd $A = F' + \ker h$. Ponadto jeśli $a \in F' \cap \ker h$, to $a = \sum_{i \in I} x_i a_i$ oraz $0 = h(a) = \sum_{i \in I} x_i f_i$, zatem wszystkie x_i równe są 0, skąd $a = 0$.

(2) Rozważmy homomorfizm kanoniczny $\kappa : A \to A/H$. Jest to surjekcja na wolną grupę abelową, skąd wobec udowodnionej już części twierdzenia otrzymujemy tezę.

□

Definicja 6.3. *Niech R będzie pierścieniem z jedynką. Lewy unitarny R-moduł M nazywamy* **modułem wolnym,** *gdy $M = \sum_{i \in I} \langle f_i \rangle$, gdzie $\langle f_i \rangle \cong R$, $i \in I$. Rodzinę $\{f_i : i \in I\}$ nazywamy* **bazą** *(lub* **zbiorem wolnych generatorów***) modułu wolnego M.*

Przykłady:

(1) Niech F będzie ciałem, V przestrzenią liniową nad F. Wówczas V jest F-modułem wolnym.
(2) Niech F będzie wolną grupą abelową. Wówczas F jest $\mathbb{Z}$-modułem wolnym.
(3) Niech F będzie ciałem, V przestrzenią liniową nad ciałem F, $\dim V < \infty$, niech $\tau \in \mathrm{End}V$. Wówczas V nie jest $F[x]$-modułem wolnym.

Twierdzenie 6.7. *Niech R będzie pierścieniem z jedynką.*

(1) *Niech M będzie lewym R-modułem wolnym z bazą $\{f_i : i \in I\}$. Każdy element $f \in M$ ma jednoznaczne przedstawienie postaci*

$$f = \sum_{i \in I} x_i f_i,$$

gdzie $x_i \in R$ oraz $x_i = 0$ dla prawie wszystkich $i \in I$.

(2) *Istnieje R-moduł wolny o bazie dowolnej mocy.*

Dowód jest bardzo podobny do dowodu analogicznego rezultatu dla grup i pozostawiamy go czytelnikowi jako nietrudne ćwiczenie.

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 6.8. *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 $\{f_1, \ldots, f_m\} \subset \{f_i : i \in I\}$ generujący M. Ponieważ baza $\{f_i : i \in I\}$ jest nieskończona, istnieje element $f \in \{f_i : i \in I\} \setminus \{f_1, \ldots, f_m\}$. 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

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

Ponieważ $\{g_j : j \in J\}$ jest bazą, elementy $g_1, \ldots, g_n$ 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 $g \in \{g_j : j \in J\} \setminus \bigcup_{S\in\operatorname{im}\Phi} S$. 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 $\Phi^{-1}(T) = \{f_1, \ldots, f_n\}$ 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 $|\{f_i : i \in I\}| \leq |\operatorname{im}\Phi \times \mathbb{N}|$ i tym samym

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

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

Definicja 6.4. *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 6.9. *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 $g_m = r_1 f_1 + \ldots + r_n f_n$, dla pewnych $r_1, \ldots, r_n \in R$ i powiedzmy, że r_k jest niezerowym elementem o najniższym indeksie. Wówczas $f_k = r_k^{-1} g_m - r_k^{-1} r_{k+1} f_{k+1} - \ldots - r_n f_n$. Wobec tego zbiór $\{g_m, f_1, \ldots, f_{k-1}, f_{k+1}, \ldots, f_n\}$ generuje M. Tym samym $g_{m-1} = s_m g_m + t_1 f_1 + \ldots + t_{k-1} f_{k-1} + t_{k+1} f_{k+1} + \ldots + t_n f_n$, 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 $g_{m-1} - s_m g_m = 0$ dawałoby nietrywialne przedstawienie 0 jako kombinacji $g_1, \ldots, g_m$), niech więc t_j będzie elementem

niezerowym o najniższym indeksie. Wówczas $x_j = t_j^{-1}g_{m-1} - t_j^{-1}s_m g_m - t_j^{-1}t_{j+1}f_{j+1} - \ldots - t_j^{-1}t_n f_n$. Wobec tego zbiór $\{g_m, g_{m-1}\} \cup \{f_1, \ldots, f_n\} \setminus \{f_j, f_k\}$ generuje M. Tym samym g_{m-2} jest kombinacją liniową g_m, g_{m-1} i f_i, dla $i \in \{1, \ldots, n\} \setminus \{j, k\}$. 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 $m - n + 1 \geq 2$, element g_1 byłby liniową kombinacją $\{g_m, \ldots, g_{m-n+1}\}$, co jest niemożliwe. Zatem $n \geq m$. Powtarzając rozumowanie z $\{f_i : i \in I\}$ i $\{g_j : j \in J\}$ zamienionymi miejscami otrzymujemy $n = m$. □

Definicja 6.5. *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.

Wniosek 6.2. *Niech R będzie pierścieniem z własnością niezmiennika bazowego, niech M i N będą lewymi R-modułami wolnymi. Wówczas $M \cong N$ wtedy i tylko wtedy, gdy bazy M i N są równej mocy.*

Dowód jest bardzo podobny do dowodu analogicznego rezultatu dla grup i pozostawiamy go czytelnikowi jako nietrudne ćwiczenie.

Lemat 6.2. *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*

$$IM = \{r_1 m_1 + \ldots + r_n m_n : r_i \in I, m_i \in M, n \in \mathbb{N}\}.$$

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 $m = r_1 f_1 + \ldots + r_n f_n$, dla pewnych $r_i \in R$, $f_i \in \{f_j : j \in J\}$. Stąd:

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

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 6.10. *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 $|R^m| = |R^n|$.

Twierdzenie 6.11 (własność uniwersalna modułów wolnych)**.** *Niech R będzie pierścieniem z jedynką. Niech M będzie lewym unitarnym R-modułem. Wówczas M jest modułem wolnym o bazie $\{f_i : i \in I\}$ wtedy i tylko wtedy, gdy dla dowolnego lewego unitarnego R-modułu N i jego rodziny elementów $\{h_i : i \in I\}$ istnieje dokładnie jeden homomorfizm $h : M \to N$ taki, że $h(f_i) = h_i$.*

Dowód jest bardzo podobny do dowodu analogicznego rezultatu dla grup i pozostawiamy go czytelnikowi jako nietrudne ćwiczenie.

Twierdzenie 6.12. *Niech R będzie pierścieniem, niech K będzie lewym R-modułem. Wówczas K jest homomorficznym obrazem pewnego lewego R modułu M o następującej własności:*

> *istnieje podzbiór $\{f_i : i \in I\}$ zbioru M taki, że dla każdego lewego R-modułu N i jego rodziny elementów $\{h_i : i \in I\}$ istnieje dokładnie jeden homomorfizm $h : M \to N$ taki, że $h(f_i) = h_i$.*

Dowód jest bardzo podobny do dowodu analogicznego rezultatu dla grup i pozostawiamy go czytelnikowi jako nietrudne ćwiczenie.

Wniosek 6.3. *Niech R będzie pierścieniem z jedynką. Każdy lewy unitarny R-moduł jest homomorficznym obrazem pewnego R-modułu wolnego.*

Okazuje się, że moduły wolne nie są zamknięte na branie podmodułów:

Przykład:

(8) Niech F będzie ciałem, niech $J = (x, y) \lhd F[x, y]$. Wówczas $F[x, y]$ jest F-modułem wolnym, a J jego podmodułem, który nie jest wolny.

Twierdzenie 6.13. *Niech R będzie pierścieniem, niech M_3 będzie lewym R-modułem o następującej własności:*

istnieje podzbiór $\{f_i : i \in I\}$ zbioru M_3 taki, że dla każdego lewego R-modułu N i jego rodziny elementów $\{h_i : i \in I\}$ istnieje dokładnie jeden homomorfizm $h : M_3 \to N$ taki, że $h(f_i) = h_i$.

Wówczas ciąg dokładny

$$0 \to M_1 \xrightarrow{f} M_2 \xrightarrow{g} M_3 \to 0$$

jest rozszczepialny.

Dowód. Niech $\{f_i : i \in I\}$ będzie takim podzbiorem zbioru M_3, że dla każdego lewego R-modułu N i jego rodziny elementów $\{h_i : i \in I\}$ istnieje dokładnie jeden homomorfizm $h : M_3 \to N$ taki, że $h(f_i) = h_i$. Zauważmy, iż $\{f_i : i \in I\}$ jest zbiorem generatorów M_3: gdyby istniał $m \in M_3 \setminus \langle\{f_i : i \in I\}\rangle$, to wówczas id_{M_3} oraz $\xi : M_3 \to M_3$ dane wzorem

$$\xi(m_3) = \begin{cases} m_3, & \text{gdy } m_3 \in \langle\{f_i : i \in I\}\rangle \\ 0, & \text{gdy } m_3 \notin \langle\{f_i : i \in I\}\rangle \end{cases}$$

byłyby dwoma różnymi homomorfizmami modułu M_3 w samego siebie przeprowadzającymi $\{f_i : i \in I\}$ na $\{f_i : i \in I\}$.

Ponieważ g jest surjekcją, dla każdego $i \in I$ istnieje $a_i \in M_2$ taki, że $g(a_i) = f_i$. Wobec własności modułu M_3, istnieje homomorfizm $\phi : M_3 \to M_2$ taki, że $\phi(f_i) = a_i$. Oczywiście $g \circ \phi(f_i) = f_i$ i ponieważ $\{f_i : i \in I\}$ generuje M_3, więc $g \circ \phi = id_{M_3}$. Tym samym ciąg jest rozszczepialny. □

Wniosek 6.4. *Niech R będzie pierścieniem z jedynką, niech M_3 będzie lewym R-modułem wolnym. Wówczas ciąg dokładny lewych R-modułów unitarnych i ich homomorfizmów*

$$0 \to M_1 \xrightarrow{f} M_2 \xrightarrow{g} M_3 \to 0$$

jest rozszczepialny.

Wniosek 6.5 (twierdzenie o składniku prostym)**.** *Niech R będzie pierścieniem, niech K będzie lewym R-modułem.*

(1) *Niech M będzie lewym R-modułem o następującej własności:*
istnieje podzbiór $\{f_i : i \in I\}$ zbioru M taki, że dla każdego lewego R-modułu N i jego rodziny elementów $\{h_i : i \in I\}$ istnieje dokładnie jeden homomorfizm $h : M \to N$ taki, że $h(f_i) = h_i$,
niech $h : K \to M$ będzie homomorfizmem surjektywnym. Wówczas istnieje podmoduł $M' < K$ taki, że

$$M \cong M' \text{ oraz } K = M' \oplus \ker h.$$

(2) *Niech L będzie podmodułem modułu K a K/L lewym R-modułem o następującej własności:*
istnieje podzbiór $\{f_i' + L : i \in I\}$ zbioru K/L taki, że dla każdego lewego R-modułu N i jego rodziny elementów $\{h_i : i \in I\}$ istnieje dokładnie jeden homomorfizm $h : K/L \to N$ taki, że $h(f_i' + L) = h_i$

Wówczas istnieje podmoduł $K' < K$ o następującej własności:
istnieje podzbiór $\{f_i'' : i \in I\}$ zbioru K' taki, że dla każdego lewego R-modułu N i jego rodziny elementów $\{h_i : i \in I\}$ istnieje dokładnie jeden homomorfizm $h : K' \to N$ taki, że $h(f_i'') = h_i$,
oraz $K = K' \oplus L$.

Dowód. Dla dowodu pierwszej części wystarczy zauważyć, że ciąg

$$K \xrightarrow{h} M \to 0$$

jest rozszczepialny. Druga część wynika z pierwszej podobnie, jak analogiczny rezultat dla grup. □

Wniosek 6.6 (twierdzenie o składniku prostym dla modułów unitarnych)**.** *Niech R będzie pierścieniem z jedynką, niech K będzie lewym unitarnym R-modułem.*

(1) *Niech M będzie lewym R-modułem wolnym, niech $h : K \to M$ będzie homomorfizmem surjektywnym. Wówczas istnieje podmoduł $M' < K$ taki, że*

$$M \cong M' \text{ oraz } K = M' \oplus \ker h.$$

(2) *Niech L będzie podmodułem modułu K a K/L lewym R-modułem wolnym. Wówczas istnieje podmoduł $K' < K$ taki, że*

$$K' \text{ jest wolny oraz } K = K' \oplus L.$$

Twierdzenie 6.14. *Niech R będzie pierścieniem, niech M będzie lewym R-modułem o następującej własności:*

istnieje podzbiór $\{f_i : i \in I\}$ zbioru M taki, że dla każdego lewego R-modułu N i jego rodziny elementów $\{h_i : i \in I\}$ istnieje dokładnie jeden homomorfizm $h : M \to N$ taki, że $h(f_i) = h_i$,

niech K będzie lewym R-modułem, niech $h : M \to K$ będzie homomorfizmem. Wówczas dla każdego lewego R-modułu L i dla każdego epimorfizmu $g : L \to K$ istnieje homomorfizm $f : M \to L$ taki, że $h = g \circ f$.

Dowód. Rozważmy diagram:

$$\begin{array}{ccccc} & & M & & \\ & & \downarrow{\scriptstyle h} & & \\ L & \xrightarrow{g} & K & \longrightarrow & 0 \end{array}$$

Ponieważ g jest surjekcją, więc ciąg $L \xrightarrow{g} K \to 0$ jest dokładny. Niech $\{f_i : i \in I\}$ będzie takim podzbiorem zbioru M, że dla każdego lewego R-modułu N i jego rodziny elementów $\{h_i : i \in I\}$ istnieje dokładnie jeden homomorfizm $h : M \to N$ taki, że $h(f_i) = h_i$. Tak jak w poprzednich dowodach zauważamy, że $\{f_i : i \in I\}$ jest zbiorem generatorów M. Dla każdego $i \in I$ istnieje $a_i \in L$ taki, że $h(f_i) = g(a_i)$. Wobec własności modułu M, istnieje homomorfizm $f : M \to L$ taki, że $f(f_i) = a_i$, $i \in I$. Ponadto $g(f(f_i)) = h(f_i)$, $i \in I$, więc $h = g \circ f$. □

Wniosek 6.7. *Niech R będzie pierścieniem z jedynką, niech M będzie lewym R-modułem wolnym, niech K będzie lewym unitarnym R-modułem, niech $h : M \to K$ będzie homomorfizmem. Wówczas dla każdego lewego unitarnego R-modułu L i dla każdego epimorfizmu $g : L \to K$ istnieje homomorfizm $f : M \to L$ taki, że $h = g \circ f$.*