1. Wykład 1: Pojęcie modułu. Podmoduły. Podmoduły generowane przez zbiór.

Definicja 1.1. *Niech R będzie pierścieniem, M addytywną grupą przemienną. M nazywamy* **lewym R-modułem,** *jeżeli na M określone jest działanie zewnętrzne z pierścieniem skalarów R $\cdot : R \times M \to M$ takie, że*

(1) $\forall a \in R \forall m_1, m_2 \in M[a(m_1 + m_2) = am_1 + am_2]$,
(2) $\forall a_1, a_2 \in R \forall m \in M[(a_1 + a_2)m = a_1m + a_2m]$,
(3) $\forall a_1, a_2 \in R \forall m \in M[(a_1a_2)m = a_1(a_2m)]$.

Jeżeli R jest pierścieniem z jedynką i spełniony jest dodatkowo warunek

(4) $\forall m \in M(1m = m)$,

to M nazywamy **lewym unitarnym R-modułem.** *W analogiczny sposób definiujemy* **prawy R-moduł** *i* **prawy unitarny R-moduł.**

Uwaga 1.1. *Niech R będzie pierścieniem, M lewym unitarnym R-modułem. Wówczas:*

(1) $\forall a_1, a_2 \in R \forall m \in M[(a_1 - a_2)m = a_1m - a_2m]$,
(2) $\forall m \in M(0m = 0)$.

Jeżeli R jest pierścieniem z jedynką, a M lewym unitarnym R-modułem, to

(3) $\forall m \in M[(-1)m = -m]$.

Dowód. (1) Ustalmy $a_1, a_2 \in R$, $m \in M$. Wówczas $(a_1 - a_2)m + a_2m = (a_1 - a_2 + a_2)m = a_1m$.
(2) Wynika z (1) dla $a_1 = a_2 = 1$.
(3) Wynika z (1) dla $a_1 = 0$, $a_2 = 1$.

□

Uwaga 1.2. *Niech R będzie pierścieniem, M addytywną grupą przemienną. Wówczas M jest lewym R-modułem wtedy i tylko wtedy, gdy istnieje homomorfizm pierścieni $\phi : R \to \mathrm{End}M$.*

Dowód. ($\Rightarrow$): Zdefiniujmy odwzorowanie $\phi : R \to \mathrm{End}M$ wzorem

$$\phi(a)(m) = am.$$

Z łatwością sprawdzamy, że wówczas ϕ jest homomorfizmem.
($\Leftarrow$): Zdefiniujmy działanie $\cdot : R \times M \to M$ wzorem

$$a \cdot m = \phi(a)(m).$$

Z łatwością sprawdzamy, że wówczas M jest lewym R-modułem. □

Przykłady:

(1) Niech F będzie ciałem, V przestrzenią wektorową nad ciałem F. Wówczas V jest lewym unitarnym F-modułem.
(2) Niech A będzie addytywną grupą abelową. Wówczas A jest lewym unitarnym $\mathbb{Z}$-modułem.
(3) Niech R będzie pierścieniem, I ideałem lewostronnym w R. Wówczas I jest lewym R-modułem.
(4) Niech R będzie pierścieniem. Wówczas R jest lewym R-modułem.
(5) Niech V będzie przestrzenią wektorową nad ciałem F, niech $\tau \in \mathrm{End}V$, niech $\phi : F[x] \to \mathrm{End}V$ będzie dane wzorem $\phi(f) = f(\tau)$. Wówczas V jest lewym unitarnym $F[x]$-modułem.

Definicja 1.2. *Niech R będzie pierścieniem, M lewym R-modułem. Podzbiór N zbioru M nazywamy* **podmodułem** *modułu M, gdy $(N, \cdot \restriction_{R \times N})$ jest lewym R-modułem. Oznaczamy $N < M$.*

Przykłady:

(6) Niech F będzie ciałem, V przestrzenią wektorową nad ciałem F, W podprzestrzenią przestrzeni V. Wówczas W jest podmodułem V.
(7) Niech A będzie addytywną grupą abelową, B podgrupą grupy A. Wówczas B jest podmodułem A.
(8) Niech R będzie pierścieniem, I ideałem lewostronnym w R. Wówczas I jest podmodułem modułu R.
(9) Niech V będzie przestrzenią wektorową nad ciałem F, niech $\tau \in \mathrm{End}V$, niech W będzie podprzestrzenią τ-niezmienniczą przestrzeni V. Wówczas W jest podmodułem $F[x]$-modułu V.
(10) Niech R będzie pierścieniem, M lewym R-modułem, I ideałem lewostronnym R. Wówczas $IM = \{a_1m_1 + \ldots + a_nm_n : a_i \in I, m_i \in M\} < M$.

Twierdzenie 1.1. *Niech R będzie pierścieniem, M lewym R-modułem, $\mathcal{R} = \{N_i : i \in I\}$ rodziną podmodułów modułu M. Wówczas:*
(1) $\bigcap_{i\in I} N_i$ *jest podmodułem modułu M,*
(2) $\bigcup_{i\in I} N_i$ *jest podmodułem modułu M, o ile $\mathcal{R}$ jest łańcuchem.*

Dowód jest bardzo podobny do dowodu analogicznego rezultatu dla grup, w związku z czym pozostawiamy go Czytelnikowi jako nietrudne ćwiczenie.

Definicja 1.3. *Niech R będzie pierścieniem, M lewym R-modułem oraz $A \subset G$ pewnym zbiorem. Najmniejszy w sensie inkluzji podmoduł modułu M zawierający zbiór A (tj. przekrój wszystkich podmodułów modułu M zawierających A) nazywamy* **podmodułem generowanym przez** *A i oznaczamy $\langle A\rangle$.*

Każdy zbiór A o tej własności, że $\langle A\rangle = M$ nazywamy **zbiorem generatorów** *modułu M. Jeśli $A = \{a_1, \ldots, a_n\}$ to oznaczamy*

$$\langle a_1, \ldots, a_n\rangle = \langle A\rangle.$$

Mówimy, że moduł jest **skończenie generowany** *(odpowiednio,* **cykliczny***), gdy istnieje skończony (odpowiednio, jednoelementowy) zbiór jego generatorów.*

Twierdzenie 1.2 (o postaci elementów podmodułu generowanego przez zbiór)**.** *Niech R będzie pierścieniem, M lewym R-modułem oraz $A \subset G$ pewnym zbiorem. Wówczas*

$$\langle A\rangle = \{r_1a_1 + \ldots + r_na_n + k_1b_1 + \ldots + k_mb_m : n, m \in \mathbb{N}, r_i \in R, a_i, b_i \in A, k_i \in \mathbb{Z}\}.$$

Jeżeli R jest pierścieniem z jedynką, a M unitarnym R-modułem, to wówczas:

$$\langle A\rangle = \{r_1a_1 + \ldots + r_na_n : n \in \mathbb{N}, r_i \in R, a_i \in A\}.$$

Dowód jest bardzo podobny do dowodu analogicznego rezultatu dla grup, w związku z czym pozostawiamy go Czytelnikowi jako nietrudne ćwiczenie.

Przykłady:
(11) Niech F będzie ciałem, V przestrzenią wektorową nad ciałem F. Każda podprzestrzeń jednowymiarowa jest podmodułem cyklicznym. Każda podprzestrzeń skończeniewymiarowa jest podmodułem skończenie generowanym.
(12) Niech A będzie addytywną grupą abelową. Każda podgrupa cykliczna jest podmodułem cyklicznym.
(13) Niech R będzie pierścieniem. Każdy ideał główny jest podmodułem cyklicznym.
(14) Niech V będzie skończeniewymiarową przestrzenią wektorową nad ciałem F, niech $\tau \in \mathrm{End}V$. Wówczas $F[x]$-moduł V jest skończenie generowany.

Definicja 1.4. *Niech R będzie pierścieniem, M lewym R-modułem, $N_1, N_2 < M$. Podmoduł $\langle N_1 \cup N_2\rangle$ nazywamy* **sumą algebraiczną** *N_1 i N_2 i oznaczamy $N_1 + N_2$.*

Twierdzenie 1.3 (o postaci elementów sumy algebraicznej podmodułów)**.** *Niech R będzie pierścieniem, M lewym R-modułem, $N_1, N_2 < M$. Wówczas:*

$$N_1 + N_2 = \{n_1 + n_2 : n_1 \in N_1, n_2 \in N_2\}.$$

Dowód jest bardzo podobny do dowodu analogicznego rezultatu dla grup, w związku z czym pozostawiamy go Czytelnikowi jako nietrudne ćwiczenie.

Twierdzenie 1.4 (Dedekinda)**.** *Niech R będzie pierścieniem, M lewym R-modułem, $K, L, N < M$ i niech $K \supset L$. Wówczas*

$$K \cap (L + N) = L + K \cap N.$$

Dowód. Inkluzja ($\supset$) jest oczywista, skupmy się na dowodzie inkluzji ($\subset$). Ustalmy $x \in K \cap (L + N)$. Ponieważ w szczególności $x \in L + N$, więc $x = y + z$ dla pewnych $y \in L$, $z \in N$. Stąd $z = x - y \in K$, skoro $x \in K$ oraz $y \in L \subset K$. Zatem $z \in K \cap N$ i tym samym $x \in L + K \cap N$. □