2 Moduły.

2.1 Pojęcie modułu.

Definicja 2.1. *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. $\forall a\in R \forall m_1, m_2\in M\; [a\,(m_1+m_2)=a\,m_1+a\,m_2]$,
2. $\forall a_1, a_2\in R \forall m\in M\; [(a_1+a_2)\,m=a_1\,m+a_2\,m]$,
3. $\forall a_1, a_2\in R \forall m\in M\; [(a_1\,a_2)\,m=a_1\,(a_2\,m)]$.

Jeżeli R jest pierścieniem z jedynką i spełniony jest dodatkowo warunek

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

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

Uwaga 2.2. Niech R będzie pierścieniem, M lewym unitarnym R-modułem. Wówczas:

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

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

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

Uwaga 2.3. Niech R będzie pierścieniem, M addytywną grupą przemienną. Wówczas M jest lewym R-modułem wtedy i tylko wtedy, gdy istnieje homomorfizm pierścieni $\phi\colon R \to \operatorname{End} M$.

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 $\tau \in \operatorname{End} V$, niech $\phi \colon F[x] \to \operatorname{End} V$ będzie dane wzorem $\phi(f) = f(\tau)$. Wówczas V jest lewym unitarnym $F[x]$-modułem.

2.2 Podmoduły.

Definicja 2.4. *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:

1. Niech F będzie ciałem, V przestrzenią wektorową nad ciałem F, W podprzestrzenią przestrzeni V. Wówczas W jest podmodułem V.

2. Niech A będzie addytywną grupą abelową, B podgrupą grupy A. Wówczas B jest podmodułem A.

3. Niech R będzie pierścieniem, I ideałem lewostronnym w R. Wówczas I jest podmodułem modułu R.

4. Niech V będzie przestrzenią wektorową nad ciałem F, niech $\tau \in \langle \mathrm{End} \rangle V$, niech W będzie podprzestrzenią τ-niezmienniczą przestrzeni V. Wówczas W jest podmodułem $F[x]$-modułu V.

5. Niech R będzie pierścieniem, M lewym R-modułem, I ideałem lewostronnym R. Wówczas $IM = \{a_1 m_1 + \ldots + a_n m_n : a_i \in I, m_i \in M\} < M$.

Stwierdzenie 2.5. *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.*

Definicja 2.6. *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 $A = \{a_1, ..., a_n\}$ to oznaczamy*

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

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

Stwierdzenie 2.7. *Niech R będzie pierścieniem, M lewym R-modułem oraz $A \subset G$ pewnym zbiorem. Wówczas*

$$\langle A\rangle = \{r_1\, a_1 + \ldots + r_n\, a_n + k_1\, b_1 + \ldots + k_m\, b_m : n, m \in \mathbb{N}, r_i \in R, a_i, b_i \in A, k_i \in \mathbb{Z}\}.$$

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

$$\langle A\rangle = \{r_1\, a_1 + \ldots + r_n\, a_n : n \in \langle \mathsf{N}\rangle, r_i \in R, a_i \in A\}.$$

Przykłady:

1. Niech F będzie ciałem, V przestrzenią wektorową nad ciałem F. Każda podprzestrzeń jednowymiarowa jest podmodułem cyklicznym. Każda podprzestrzeń skończeniewymiarowa jest podmodułem skończenie generowanym.
2. Niech A będzie addytywną grupą abelową. Każda podgrupa cykliczna jest podmodułem cyklicznym.
3. Niech R będzie pierścieniem. Każdy ideał główny jest podmodułem cyklicznym.
4. Niech V będzie skończeniewymiarową przestrzenią wektorową nad ciałem F, niech $\tau \in \operatorname{End} V$. Wówczas $F[x]$-moduł V jest skończenie generowany.

Definicja 2.8. *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 $N_1 + N_2$*

Stwierdzenie 2.9. *Niech R będzie pierścieniem, M lewym R-modułem, $N_1, N_2 < M$. Wówczas:*

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

2.3 Homomorfizmy modułów.

Definicja 2.10. *Niech R będzie pierścieniem, M, N lewymi R-modułami.*

1. *Odwzorowanie $\phi\colon M \to N$ nazywamy* ***homomorfizmem****, jeśli:*
   - $\forall m_1, m_2 \in M\, [\phi\,(m_1 + m_2) = \phi(m_1) + \phi(m_2)]$,
   - $\forall a \in R \forall m \in M\, [\phi\,(a\, m) = a\, \phi(m)]$.

   Zbiór wszystkich homomorfizmów modułu M w N oznaczamy $Hom_R(M, N)$.
2. *Homomorfizm $\phi\colon M \to N$ nazywamy* ***monomorfizmem kategoryjnym modułów,*** *jeśli dla dowolnych lewego R-modułu K i homomorfizmów $\psi_1, \psi_2\colon K \to M$:*
$$\textit{jeśli } \phi \circ \psi_1 = \phi \circ \psi_2 \textit{ to } \psi_1 = \psi_2.$$
3. *Homomorfizm $\phi\colon M \to N$ nazywamy* ***epimorfizmem kategoryjnym modułów,*** *jeśli dla dowolnych lewego R-modułu K i homomorfizmów $\psi_1, \psi_2\colon N \to K$:*
$$\textit{jeśli } \psi_1 \circ \phi = \psi_2 \circ \phi \textit{ to } \psi_1 = \psi_2.$$
4. *Homomorfizm $\phi\colon M \to N$ nazywamy* ***izomorfizmem,*** *jeśli jest różnowartościowy i surjektywny. Dwa moduły M i N nazywamy* ***izomorficznymi,*** *jeśli istnieje między nimi izomorfizm, co oznaczamy przez $M \cong N$.*
5. *Jeśli $\phi\colon M \to N$ jest homomorfizmem, to zbiór $\phi^{-1}(0_N)$ nazywamy* ***jądrem*** *i oznaczamy $\operatorname{Ker}\phi$, a zbiór $\phi(M)$* ***obrazem*** *i oznaczamy $\operatorname{Im}\phi$.*

Przykłady:

1. Niech V, W będą przestrzeniami liniowymi nad ciałem F, $\phi \colon V \to W$ przekształceniem liniowym. Wówczas ϕ jest homomorfizmem modułów.

2. Niech A, B będą grupami abelowymi, $\phi \colon A \to B$ homomorfizmem grup. Wówczas ϕ jest homomorfizmem modułów.

3. Niech M, N będą lewymi R-modułami, $\phi \colon M \to N$ niech będzie dane wzorem $\phi(m) = 0_N$. Wówczas ϕ jest homomorfizmem modułów, nazywamy go **homomorfizmem zerowym.**

Stwierdzenie 2.11. *Niech R będzie pierścieniem, M, N lewymi R-modułami, $\phi\colon M \to N$ homomorfizmem modułów. Wówczas:*

1. $\operatorname{Ker}\phi < M$, $\operatorname{Im}\phi < N$;
2. *ϕ jest homomorfizmem różnowartościowym wtedy i tylko wtedy, gdy $\ker\phi = \{0_M\}$;*
3. *ϕ jest homomorfizmem surjektywnym wtedy i tylko wtedy, gdy $\operatorname{Im}\phi = N$;*
4. *ϕ jest izomorfizmem wtedy i tylko wtedy, gdy istnieje homomorfizm $\psi\colon N \to M$ taki, że*

$$\phi \circ \psi = i\,d_N \; oraz \; \psi \circ \phi = i\,d_M;$$

5. *ϕ jest homomorfizmem różnowartościowym wtedy i tylko wtedy, gdy jest monomorfizmem kategoryjnym modułów;*
6. *ϕ jest homomorfizmem surjektywnym wtedy i tylko wtedy, gdy jest epimorfizmem kategoryjnym modułów.*

Stwierdzenie 2.12. *Niech R będzie pierścieniem, M, N lewymi R-modułami, $\phi\colon M \to N$ homomorfizmem modułów, niech $M_1 < M$, $N_1 < N$. Wówczas:*

1. $\phi(M_1) < N$;
2. $\phi^{-1}(N_1) < M$.

Stwierdzenie 2.13. *Niech R będzie pierścieniem, M, N lewymi R-modułami, $\pi\colon M \to N$ homomorfizmem surjektywnym modułów i niech $K = \operatorname{Ker}\pi$. Oznaczmy*

$$\mathcal{M} = \{M_1 \colon M_1 < M \; oraz \; K \subset M_1\}, \mathcal{N} = \{N_1 \colon N_1 < N\}.$$

Wówczas odwzorowania

$$\phi\colon \mathcal{M} \to \mathcal{N}, \phi(M_1) = \pi(M_1),$$

$$\psi\colon \mathcal{N} \to \mathcal{N}, \psi(N_1) = \pi^{-1}(N)\,1)$$

są wzajemnie odwrotne.

2.4 Moduł ilorazowy i twierdzenie o homomorfizmie.

Definicja 2.14. *Niech R będzie pierścieniem, M lewym R-modułem, $N < M$. Oznaczmy*

$$m + N = \{m + n : n \in N\},$$

$$M / N = \{m + N : m \in M\}$$

i w zbiorze M / N określmy działania dodowania i mnożenia zewnętrznego:

$$(m_1 + N) + (m_2 + N) = (m_1 + m_2) + N,$$

$$a\,(m + N) = a\,m + N.$$

Wówczas M / N jest lewym R-modułem, nazywamy go ***modułem ilorazowym*** *M względem N.*

Przykłady:

1. Niech V będzie przestrzenią wektorową nad ciałem F, niech $W < V$. Wówczas przestrzeń ilorazowa V/W jest modułem ilorazowym.
2. Niech A będzie grupą abelową, niech $B < A$. Wówczas grupa ilorazowa A/B jest modułem ilorazowym.
3. Niech R będzie pierścieniem, niech $I \lhd R$. Wówczas pierścień ilorazowy R/I jest modułem ilorazowym.

Uwaga 2.15. Niech R będzie pierścieniem, M lewym R-modułem, $N < M$. Wówczas odwzorowanie $\kappa\colon M \to M\,/\,N$ dane wzorem $\kappa(m) = m + N$ jest homomorfizmem surjektywnym oraz $\ker \kappa = N$. Nazywamy go **epimorfizmem kanonicznym.**

Wniosek 2.16. *Niech R będzie pierścieniem, M lewym R-modułem, $N \subset M$. Wówczas $N < M$ wtedy i tylko wtedy, gdy N jest jądrem pewnego homomorfizmu.*

Twierdzenie 2.17. (o homomorfizmie) *Niech* R *będzie pierścieniem,* M, N_1, N_2 *lewymi* R-*modułami,* $\phi_1\colon M \to N_1$ *homomorfizmem surjektywnym,* $\phi_2\colon M \to N_2$ *homomorfizmem.*

1. *Jeśli istnieje homomorfizm* $\psi\colon N_1 \to N_2$ *taki, że* $\psi \circ \phi_1 = \phi_2$*, to* $\ker \phi_1 \subset \ker \phi_2$.
2. *Jeśli* $\ker \phi_1 \subset \ker \phi_2$*, to istnieje dokładnie jeden homomorfizm* $\psi\colon N_1 \to N_2$ *taki, że* $\psi \circ \phi_1 = \phi_2$*. Ponadto wówczas* $\mathrm{Im}\psi = \mathrm{Im}\phi_2$ *oraz* $\mathrm{Ker}\,\psi = \phi_1(\mathrm{Ker}\,\phi_2)$.

Wniosek 2.18. *Niech R będzie pierścieniem, M, N_1, N_2 lewymi R-modułami, $\phi_1\colon M \to N_1$ homomorfizmem surjektywnym, $\phi_2\colon M \to N_2$ homomorfizmem. Niech ponadto $\operatorname{Ker}\phi_1 \subset \operatorname{Ker}\phi_2$. Wówczas istnieje dokładnie jeden homomorfizm $\psi\colon N_1 \to N_2$ taki, że $\psi \circ \phi_1 = \phi_2$ oraz:*

1. *jeśli ϕ_2 jest surjektywny, to ψ jest surjektywny;*
2. *jeśli $\operatorname{Ker}\phi_1 = \operatorname{Ker}\phi_2$, to ψ jest różnowartościowy;*
3. *jeśli ϕ_2 jest surjektywny i $\ker\phi_1 = \ker\phi_2$, to ψ jest izomorfizmem.*

Wniosek 2.19. (twierdzenie o homomorfizmie dla modułów ilorazowych) *Niech R będzie pierścieniem, M, N lewymi R-modułami, $K < M$, $\phi: M \to N$ homomorfizmem.*

1. *Jeśli istnieje homomorfizm $\psi: M / K \to N$ taki, że $\psi \circ \kappa = \phi$ (gdzie $\kappa: M \to M / N$ oznacza epimorfizm kanoniczny), to $K \subset \operatorname{Ker} \phi$.*
2. *Jeśli $K \subset \operatorname{Ker} \phi$, to istnieje dokładnie jeden homomorfizm $\psi: M / K \to N$ taki, że $\psi \circ \kappa = \phi$. Ponadto wówczas $\operatorname{Im} \psi = \operatorname{Im} \phi$ oraz $\operatorname{Ker} \psi = \kappa(\operatorname{Ker} \phi)$.*

Wniosek 2.20. *Niech R będzie pierścieniem, M, N lewymi R-modułami, $K < M$, $\phi\colon M \to N$ homomorfizmem. Niech ponadto $K \subset \operatorname{Ker} \phi$. Wówczas istnieje dokładnie jeden homomorfizm $\psi\colon M / K \to N$ taki, że $\psi \circ \kappa = \phi$ (gdzie $\kappa\colon M \to M / N$ oznacza epimorfizm kanoniczny) oraz*

1. *jeśli ϕ jest surjektywny, to ψ jest surjektywny;*
2. *jeśli $K = \operatorname{Ker} \phi$, to ψ jest różnowartościowy;*
3. *jeśli ϕ jest surjektywny i $K = \operatorname{Ker} \phi$, to ψ jest izomorfizmem.*

Wniosek 2.21. (I twierdzenie Noether-Dedekinda o izomorfizmie) *Niech* R *będzie pierścieniem,* M, N *lewymi* R*-modułami,* $\phi\colon M \to N$ *homomorfizmem. Wówczas*

$$\mathrm{Im}\phi \cong M / \ker \phi.$$