Wykład 10. Moduły.

R: pierścień z 1 (niekoniecznie przemienny)

Def. 10.3 $(M, +, r)_{r\in R}$: moduł (domyślnie: lewostronny) nad R

[R-moduł lewostronny], gdy:

[mnożenie przez skalar $r \in R$ z lewej
$M \ni x \longmapsto \underset{rx}{r \cdot x} \in M$]

(1) $(M, +)$: grupa abelowa, 0: zero modułu M

(2) • $r(m_1+m_2) = rm_1 + rm_2$

• $(r_1+r_2)m = r_1 m + r_2 m$

• $r_1(r_2 m) = (r_1 r_2)m$

• $1m = m$

[wariant: moduł prawostronny nad R:

$M \ni x \longmapsto \underset{xr}{x \cdot r} \in M$,

$(m_1+m_2)r = m_1 r + m_2 r$

$\vdots$

$m(r_1 r_2) = (mr_1)r_2$ $\Leftarrow$!!!

• Gdy R: przemienny $\Rightarrow$ lewostronny R-moduł = prawostronny R-moduł.

dokładniej:

gdy $(M,+,r)_{r\in R}$: R-moduł lewostronny,
to $(M,+,r)_{r\in R}$: R-moduł prawostronny
i vice versa.

<u>Przykłady</u> 1. $R=K$ ciało $\Rightarrow$ przestrzeń liniowa nad K to K-moduł.

2. G: grupa abelowa $\Rightarrow$
G ma naturalną strukturę $\mathbb{Z}$-modułu:
$$\overset{\shortparallel}{G} \quad (G,\underset{\substack{\uparrow \\ \text{grupowe}}}{+},k)_{k\in\mathbb{Z}} \qquad k\cdot g = k\text{-ta krotność } g \text{ w } G.$$

3. G: grupa abelowa

$$\mathrm{End}(G) = \{f: G\to G : f \text{ endomorfizm}\}$$

pierścień z jedynką, zero: funkcja zerowa $0: G\to G$.

$+$: $(f+g)(x) = f(x)+g(x)$, $f,g\in \mathrm{End}(G)$

$\cdot$: $(f\cdot g)(x) = f(g(x))$ złożenie

$\cdot$ $1 = id_G$

G: moduł nad $\mathrm{End}(G)$: dla $f\in\mathrm{End}(G)$, $x\in G$.
$$f\cdot x = f(x).$$

4. Zał, że $j : R \longrightarrow End(G)$: homomorfizm pierścieni z jednością $(j(1_R) = id_G)$.

j wyznacza w G strukturę R-modułu:

$(G, +, r)_{r \in R}$: $r \cdot g = j(r)(g)$

Na odwrót:

Gdy $(G, +, r)_{r \in R}$: R-moduł, to dla $r \in R$:

$j(r) : G \longrightarrow G$, $j(r)(g) \overset{def}{=} r \cdot g$, $j(g) \in End(G)$

oraz $R \ni r \longrightarrow j(r) \in End(G)$

daje $j : R \longrightarrow End(G)$ homomorfizm pierścieni z 1.

5. $R_1 \subset R$ podpierścień $\Rightarrow$ R jest modułem nad R_1

$(R, +, r)_{r \in R_1}$, $\underset{R_1}{\underset{\Uparrow}{r}} \cdot \underset{R}{\underset{\Uparrow}{x}}$ liczone w R.

6. $j : R_1 \longrightarrow R$ homomorfizm pierścieni z 1, $M = (M, +, r)_{r \in R}$: R-moduł

$\Rightarrow M : R_1$-moduł : $r_1 \cdot m \overset{def}{=} \underset{R}{\underset{\Uparrow}{j(r_1)}} \cdot m$.

7. R : pierścień, ~~KR~~ $I \subseteq R$: ideał lewostronny (tzn. $(I, +) < (R, +)$ oraz $RI \subset I$). Wtedy I : R-moduł.

Def. 10.4. Zał, że M: R-moduł oraz $N \subseteq M$. Wtedy N: R-podmoduł M, gdy N: R-moduł względem działań z M.

tzn: (1) $(N,+) < (M,+)$ $(\Rightarrow N \neq \emptyset)$

(2) N zamknięty względem mnożenia przez skalary $r \in R$, w M.

Uwaga 10.5 Zał, że M: R-moduł.

(1) $0 \cdot m = 0$

(2) $r \cdot 0 = 0$

(3) $(-1) \cdot m = -m$.

(M,+) grupa

<u>D-d</u> (1) $0 \cdot m = (0+0) \cdot m = 0m + 0m \Rightarrow 0m = 0$

(2) $r \cdot 0 = r(0+0) = r0 + r0 \Rightarrow r0 = 0$

(3) $(-1) \cdot m + \underbrace{1 \cdot m}_{= m} = ((-1)+1) \cdot m = 0 \cdot m = 0$

$\Rightarrow (-1) \cdot m = -m$

Uwaga 10.6 (M: R-moduł).

Przekrój dowolnej $\neq \emptyset$ rodziny podmodułów M jest podmodułem M.

<u>Przykład</u>: $\{0\} \subseteq M$: podmoduł zerowy.

Wniosek 10.6. $A \subseteq M \Rightarrow$ istnieje najmniejszy podmoduł $N \subseteq M$ zawierający A

$\uparrow$ podmoduł M generowany przez A.

$N = \{\sum r_i a_i : r_i \in R, a_i \in A\} \cup \{0\}$.

- $N_1, N_2 \subseteq M$: podmoduły $\Rightarrow N_1 + N_2$: podmoduł M

(podobnie : $N_1 + \ldots + N_k$)

- Produkt R-modułów $M \times N$, podobnie jak dla przestrzeni liniowych.

- ~~$N_1 + \ldots + N_k$ jest~~ suma prosta:

$M = N_1 \oplus \ldots \oplus N_k$ (dla $N_1, \ldots, N_k \subset M$ podmodułów), gdy

$\forall m \in M \; \exists! \; n_1 \in N_1, \ldots, n_k \in N_k \quad m = n_1 + \ldots + n_k$

Homomorfizm R-modułów: $h : M \to N \ldots$

<u>Przykłady</u>: . $id_M : M \longrightarrow M$

. $0 : M \longrightarrow M$, $0(x) = 0$.

- typowa terminologia:
  izo-, endo-, auto-morfizm...

- $F : M_1 \times \ldots \times M_n \longrightarrow M$ n-liniowe odwzorowanie R-modułów, gdy ~~R~~ F: liniowe na każdej współrzędnej.

- Niech $h : M \longrightarrow N$ homomorfizm R-modułów.
  - dla $N' \subseteq N$ podmodułu, $h^{-1}[N'] \subset M$ podmoduł.
  - dla $M' \subset M$ podmodułu, $h[M'] \subset N$ —//—.

- Niech $M' \subset M$ podmoduł. Wtedy
  $M/M' = \{x + M' : x \in M\}$: moduł ilorazowy
  warstwy M' w M
  (działania jak zwykle)

TW. 10.7 (zasadnicze tw. o homomorfizmie R-modułów)

$$\begin{tikzcd} M \arrow[r, "f"] \arrow[d, "\text{ilorazowe}"'] \arrow[dr, phantom, "\#"] & N \\ M/\mathrm{Ker}\, f \arrow[ur, dashed, "\exists!\, \bar{f}"'] & \end{tikzcd}$$

f ← homomorfizm R-modułów.

$\exists!\, \bar{f}$: monomorfizm R-modułów.

TW. 10.8 (o faktoryzacji) Niech $f : M \to N$, $g : M \to U$ homomorfizmy R-modułów.

Wtedy:

$$\begin{tikzcd} M \arrow[r, "f"] \arrow[d, "g"'] \arrow[dr, phantom, "\#"] & N \\ U \arrow[ur, dashed, "\exists h"'] & \end{tikzcd} \iff \mathrm{Ker}\, f \supseteq \mathrm{Ker}\, g$$

- $h: M \longrightarrow N$ jest 1-1 $\Leftrightarrow \ker h = \{0\}$

$\underbrace{\mathrm{Hom}_R(M,N)}_{R\text{-moduł}} = \{h: M \longrightarrow N : h: \text{homomorfizm } R\text{-modułów}\}$

(dla R: przemiennego!)

- $(h_0 + h_1)(m) = h_0(m) + h_1(m)$
- $(r h)(m) = r \cdot h(m)$

Nasz cel: Zrozumieć moduły.

Dany M: R-moduł.

Np Jeśli $M = \bigoplus_i M_i$, gdzie $M_i \subset M$ "małe" podmoduły, już zrozumiane, to wtedy rozumiemy M.

Def. 10.9. (M - R-moduł)

M jest R-modułem <u>prostym</u>, gdy $M \neq \{0\}$ i

$$\underset{\text{podmoduł}}{\forall N \subset M} \ (N = \{0\} \text{ lub } N = M).$$

- Dla M: R-modułu, $\underbrace{\mathrm{End}_R(M)}_{\text{pierścień, podpierścień } \mathrm{End}(M,+)} = \{\text{endomorfizmy } M\}$.

Lemat 10.10 (Lemat Schura).

M : R-moduł prosty $\Rightarrow$ $\mathrm{End}_R(M)$: pierścień z dzieleniem

(tzn. każdy $0 \neq f \in \mathrm{End}_R(M)$ ma element odwrotny)

<u>D-d</u>.

Niech $0 \neq f \in \mathrm{End}_R(M)$.

Wtedy $\mathrm{Im}\, f = M$, $\ker f = \{0\}$ $\Rightarrow$ f : odwracalny (automorfizm).

Zał., że M : R-moduł oraz $K = \mathrm{End}_R(M)$: pierścień z dzieleniem ("ciało nieprzemienne").

Wtedy M : K-moduł, przestrzeń liniowa nad K

Zał., że $n = \dim_K M < \infty$. Wtedy $\mathrm{End}_K(M) \cong M_{n\times n}(K)$

- $R \ni r \mapsto \varphi_r : M \longrightarrow M$, $\varphi_r \in \mathrm{End}_K(M)$
  $\varphi_r(m) = r \cdot m$ (zad.)

$R \ni r \longrightarrow m(\varphi_r) \in M_{n\times n}(K)$

$R \longrightarrow M_{n\times n}(K)$ homomorfizm pierścieni z 1

- teoria reprezentacji pierścieni.