LINIOWA NIEZALEŻNOŚĆ, ROZPINANIE I BAZY

Niech R będzie dowolnym pierścieniem, a M dowolnym R-modułem. Niech $\emptyset \neq S \subseteq M$. Podzbiór S nazywamy <u>liniowo niezależnym</u> (lub <u>wolnym</u>), a o jego elementach mówimy że są <u>liniowo niezależne</u>, $\Longleftrightarrow$ $\forall$ skończonego $I \subseteq S$:

$$\boxed{\sum_{m \in I} r_m m = 0 \implies \forall m \in I : r_m = 0}.$$

<u>Elementarne uwagi</u>:

① Jeśli powyższa implikacja zachodzi dla skończonego zbioru I, to zachodzi też dla każdego $J \subseteq I$. Istotnie,

$$\sum_{m \in J} r_m m = 0 \implies \sum_{m \in J} r_m m + \sum_{n \in I \setminus J} 0 n = 0 \implies \forall_{m \in J} r_m = 0.$$

Dlatego, jeśli S jest skończony, wystarczy definiować liniową niezależność przez warunek

$$\sum_{m \in S} r_m m = 0 \implies \forall m \in S : r_m = 0.$$

(2) Rozważmy $\mathbb{Q}$ jako $\mathbb{Z}$-moduł. Podzbiór $\emptyset \neq S \subseteq \mathbb{Q}$ jest liniowo niezależny $\iff$ $S = \{r\}$ i $r \neq 0$. Istotnie, $r \neq 0 \iff$ $(n \cdot r = 0 \implies n = 0)$. Jeśli $\frac{p}{q}, \frac{p'}{q'} \in S$, $\frac{p}{q} \neq \frac{p'}{q'}$,

to $qp' \dfrac{p}{q} + (-q'p) \dfrac{p'}{q'} = 0$, a nie jest prawdą, że $qp' = -q'p = 0$, bo wtedy $\frac{p}{q} = 0 = \frac{p'}{q'}$, co przeczy $\frac{p}{q} \neq \frac{p'}{q'}$.

(3) S jest liniowo niezależny $\implies$ ($0 \notin S$ lub $R = 0$).

Zbiory które nie są liniowo niezależne nazywamy <u>liniowo zależnymi</u>. Podobnie, elementy zbiorów liniowo zależnych nazywamy liniowo zależnymi.

Niech $\emptyset \neq S \subseteq M$. <u>Przestrzenią rozpinaną</u> przez S nazywamy zbiór wszystkich skończonych kombinacji liniowych elementów S:

$$\boxed{\operatorname{span}(S) := \left\{ \sum_{m \in S} r_m m \in M \;\middle|\; \begin{array}{l} \forall m \in S: r_m \in R, \\ \text{tylko skończona} \\ \text{ilość } r_m \neq 0 \end{array} \right\}}$$

Elementarne uwagi:

① span(S) jest podmodułem M. Istotnie, $\forall r \in R$, $\sum_{m\in S} r_m m \in \text{span}(S)$: $r \sum_{m\in S} r_m m = \sum_{m\in S} (r r_m) m \in$ span(S). Dalej,

$\sum_{m\in S} r_m m$, $\sum_{m\in S} r'_m m \in \text{span}(S) \Rightarrow \sum_{m\in S} r_m m + \sum_{m\in S} r'_m m$

$= \sum_{m\in S} (r_m + r'_m) m \in \text{span}(S)$.

Wreszcie $\sum_{m\in S} r_m m \in \text{span}(S) \Rightarrow -\sum_{m\in S} r_m m =$

$\sum_{m\in S} (-r_m) m \in \text{span}(S)$.

② Rozważmy pierścień R jako lewy, moduł nad sobą. Wtedy $\text{span}(\{r\}) = R \Leftrightarrow \exists s \in R: sr = 1$. Istotnie, $1 \in R = \text{span}(\{r\}) \Rightarrow \exists s \in R: sr = 1$ oraz $\exists s \in R: sr = 1 \Rightarrow \forall r' \in R: r' = r'1 =$ $r'(sr) = (r's)r \in \text{span}(\{r\})$.

③ Rozważmy $\mathbb{Q}$ jako $\mathbb{Z}$-moduł. Niech $\emptyset \neq S \subseteq \mathbb{Q}$. $\text{span}(S) = \mathbb{Q} \Rightarrow S$ nie jest skończony. Istotnie, sprowadźmy wszystkie

ułamki w S do postaci względnie pierwszej.
(Ułamek jest w postaci względnie pierwszej $\Leftrightarrow$ gcd(licznik, mianownik) = 1 i mianownik > 0.) Jeśli $S = \{\frac{p_1}{q_1}, \dots, \frac{p_n}{q_n}\}$, gdzie wszystkie ułamki $\frac{p_i}{q_i}$ są w postaci względnie pierwszej, to dowolny element $x \in \operatorname{span}(S)$ można zapisać jako

$$x = \sum_{i=1}^{n} k_i \frac{p_i}{q_i} = \frac{\Sigma(\dots)}{q_1 q_2 \cdots q_n}.$$

Zatem największy mianownik dowolnego elementu z span(S) zapisanego w postaci względnie pierwszej jest $\leq q_1 \dots q_n$. Stąd $\mathbb{Q} \ni \frac{1}{(q_1 \dots q_n)+1} \notin \operatorname{span}(S)$.

Niech R będzie dowolnym pierścieniem, a M dowolnym R-modułem. Niepusty podzbiór $B \subseteq M$ nazywamy <u>bazą</u> M $\Leftrightarrow$

① B jest zbiorem liniowo niezależnym,

② $\operatorname{span}(B) = M$.

Moduł nazywamy <u>wolnym</u> $\Leftrightarrow$ posiada bazę.

<u>Elementarne fakty</u>:

① Każdy pierścień R (nawet zerowy) jest wolnym R-modułem. Zbiór {1} jest zawsze bazą R.

② Dowolna suma prosta $\bigoplus_{i\in I} R$ jest wolnym R-modułem. Bazą (kanoniczną) jest zbiór $\{f_i \in Map(I,R) \mid \forall i,j\in I : f_i(j)=\delta_{ij}\}$, gdzie δ_{ij} jest deltą Kroneckera, tzn.

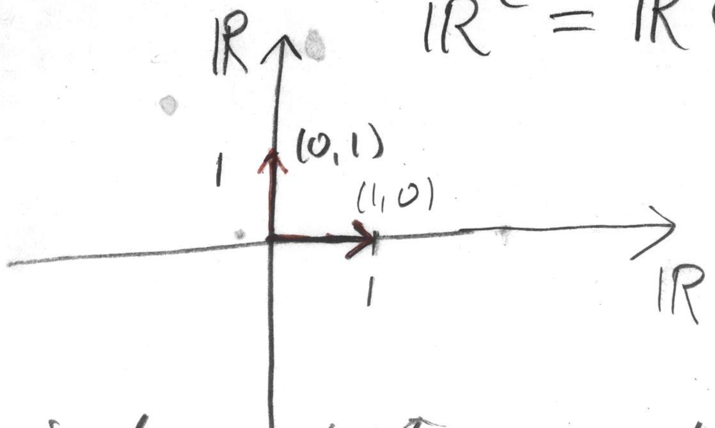
$$\delta_{ij} = \begin{cases} 1 & \text{dla } i=j \\ 0 & \text{dla } i\neq j \end{cases}.$$

Jeśli $I = \mathbb{N}\setminus\{0\}$, piszemy $f_i = (0, \dots, 0, \underset{i\text{-te miejsce}}{1}, 0, \dots)$.

Jeśli $I = \{1, \dots, n\}$, piszemy $\bigoplus_{i\in I} R = R^n$.

R^n jest prototypem modułu wolnego, a zbiór $\{(1,0,\dots,0), (0,1,0,\dots,0), \dots, (0,\dots,0,1)\}$ prototypem bazy. Dla $R=\mathbb{R}$ mamy geometryczną intuicję wprowadzonych pojęć:

$$\mathbb{R}^2 = \mathbb{R}\oplus\mathbb{R}$$



③ $\mathbb{Q}$ <u>nie</u> jest modułem wolnym nad $\mathbb{Z}$ bo nie posiada bazy. Istotnie, żaden zbiór nie może być równocześnie jednoelementowy i nieskończony.

Twierdzenie: Jeśli M jest wolnym R-modułem z bazą B, to odwzorowanie

$$\boxed{\bigoplus_{e\in B} R \ni f \xmapsto{F} \sum_{e\in B} f(e)e \in M}$$

jest izomorfizmem R-modułów.

Dowód: Odwzorowanie F jest ewidentnie liniowe. Skonstruujemy odwzorowanie odwrotne F^{-1}. $\forall m \in M \ \exists! \{r_1, \dots, r_{N_m}\} \subseteq R\setminus\{0\}$, $\{e_1, \dots, e_{N_m}\} \subseteq B$: $\boxed{m = \sum_{k=1}^{N_m} r_k e_k}$. Istotnie, przypuśćmy że mamy 2 rozkłady m:

$\sum_{k=1}^{N_m} r_k e_k = m = \sum_{j=1}^{N'_m} s_j f_j$. Niech $I := \{e_k\}_1^{N_m} \cap \{f_j\}_1^{N'_m}$.

Wtedy $0 = m - m = \sum_{i\in I} (r_i - s_i) e_i + \sum_{k\notin I} r_k e_k + \sum_{j\notin I} (-s_j) f_j$.

Z liniowej niezależności wynika $\forall i \in I : r_i = s_i$, $\forall k \notin I : r_k = 0$, $\forall j \notin I : s_j = 0$. Zatem z założenia niezerowości współczynników rozkład w bazie jest jednoznaczny. Możemy więc zdefiniować $M \ni m \xmapsto{F^{-1}} f_m \in \bigoplus_{e\in B} R$, gdzie $\sum_{e\in B} f_m(e)e := m$, i sprawdzić że $F\circ F^{-1} = \mathrm{id}$ i $F^{-1}\circ F = \mathrm{id}$. ∎