PIERŚCIEŃ ENDOMORFIZMÓW I POJĘCIE WYMIARU

Niech M będzie dowolnym R-modułem. Odwzorowanie liniowe z M do M nazywamy <u>endomorfizmem</u>. Izomorfizm liniowy z M do M nazywamy <u>automorfizmem</u>. Używamy oznaczeń $\mathrm{End}_R(M) := \mathrm{Hom}_R(M, M)$, $\mathrm{Aut}_R(M) := \{ f \in \mathrm{End}_R(M) \mid f \text{ jest bijekcją} \}$.

Ze względu na składanie odwzorowań, $\mathrm{Aut}_R(M)$ jest grupą. Elementem neutralnym jest id. Ze względu na składanie odwzorowań i punktowe dodawanie, $\mathrm{End}_R(M)$ jest pierścieniem. Zerem jest odwzorowanie zerowe a jedynką id. Jeśli M posiada bazę I, to macierzą endomorfizmu f w bazie I nazywamy macierz f w bazach I i I. Zatem endomorfizm modułu wolnego zawsze możemy zapisać jako macierz kwadratową.

Macierze kwadratowe tworzą pierścień $M_I(R)$ ze względu na mnożenie macierzy i dodawanie punktowe. Zerem jest odwzorowanie zerowe a jedynką macierz

$$I \times I \ni (i,j) \longmapsto \delta_{ij} := \begin{cases} 1 & \text{dla } i=j \\ 0 & \text{dla } i \neq j \end{cases} \in R.$$

Przyporządkowanie endomorfizmowi jego macierzy kwadratowej zadaje izomorfizm pierścieni:

$$\mathrm{End}_R(M) \ni f \longmapsto M_f \in M_I(R).$$

Grupę wszystkich macierzy odwracalnych oznaczamy przez $GL_I(R)$. Jest ona obrazem $\mathrm{Aut}_R(M)$ przy powyższym izomorfizmie pierścieni.

Przykład: $R = \mathbb{Z}$, $M = \mathbb{Z}^2$.

$$\begin{pmatrix} 0 & 5 \\ 3 & 2 \end{pmatrix} + \begin{pmatrix} 8 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 8 & 5 \\ 4 & 3 \end{pmatrix} \in M_2(\mathbb{Z})$$

$$\begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^{\in GL_2(\mathbb{Z})} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}^{\in GL_2(\mathbb{Z})} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Jak się zmienia macierz endomorfizmu przy zmianie bazy? Niech B i C będą bazami prawego R-modułu M. Niech $f \in \mathrm{End}_R(M)$. Przez $M_{BC}(f)$ oznaczymy macierz $B \times C \ni (i,j) \xmapsto{M_{BC}(f)} f_{ij}^{BC} \in R$, gdzie f_{ij}^{BC} jest jedynym elementem R spełniającym $f(j) = \sum_{i \in B} i f_{ij}^{BC}$. Wtedy

$$M_{BB}(f) = M_{BB}(id \circ f \circ id)$$
$$= M_{BC}(id) M_{CC}(f) M_{CB}(id),$$

$$M_{BC}(id) M_{CB}(id) = M_{BB}(id \circ id) = 1 \in M_B(R),$$
$$M_{CB}(id) M_{BC}(id) = M_{CC}(id \circ id) = 1 \in M_C(R).$$

Przykład: $R = \mathbb{Z}$, $M = \mathbb{Z}^2$, $f(m,n) := (m+n, m-n)$, $B = \{(1,0), (0,1)\}$, $C = \{(1,1), (1,0)\}$.

Porządkując bazy tak jak są napisane, otrzymujemy:

$$\left.\begin{aligned} f(1,0) &= (1,0)\cdot 1 + (0,1)\cdot 1 \\ f(0,1) &= (1,0)\cdot 1 + (0,1)\cdot(-1) \end{aligned}\right\} \Longleftrightarrow M_{BB}(f) = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

$$\left.\begin{aligned} f(1,1) &= (2,0) = (1,1)\cdot 0 + (1,0)\cdot 2 \\ f(1,0) &= (1,1) = (1,1)\cdot 1 + (1,0)\cdot 0 \end{aligned}\right\} \Longleftrightarrow M_{CC}(f) = \begin{pmatrix} 0 & 1 \\ 2 & 0 \end{pmatrix}$$

$$\left.\begin{aligned} id(1,0) &= (1,1)\cdot 0 + (1,0)\cdot 1 \\ id(0,1) &= (1,1)\cdot 1 + (1,0)\cdot(-1) \end{aligned}\right\} \Longleftrightarrow M_{CB}(id) = \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix}$$

$$\left.\begin{aligned} id(1,1) &= (1,0)\cdot 1 + (0,1)\cdot 1 \\ id(1,0) &= (1,0)\cdot 1 + (0,1)\cdot 0 \end{aligned}\right\} \Longleftrightarrow M_{BC}(id) = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$$

$$M_{BC}(id)\, M_{CC}(f)\, M_{CB}(id) = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 2 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix}$$

$$= \begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = M_{BB}(f)$$

$$\begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix}$$

Do wprowadzenia pojęcia wymiaru potrzebujemy zebrać razem pewne <u>fakty</u>:

① Jeśli moduł M nad dowolnym pierścieniem R ma <u>nieskończoną</u> bazę B, to każda inna baza M jest równoliczna z B.

<u>Uwaga</u>: Istnieją pierścienie (nieprzemienne) nad którymi <u>skończone</u> bazy tego samego modułu mogą być <u>różnoliczne</u>: $R^m \cong R^n \not\Rightarrow m = n$. Np. $R^2 \cong R$.

② Ogólne twierdzenie ① połączone z Lematem Steinitz'a daje nam:

<u>Twierdzenie</u>: Wszystkie bazy dowolnej niezerowej przestrzeni wektorowej są równoliczne.

<u>Wniosek</u>: Wszystkie bazy dowolnego modułu wolnego nad niezerowym <u>przemiennym</u> pierścieniem są równoliczne.

<u>Dowód</u> oparty jest na istnieniu homomorfizmu z pierścienia przemiennego R na ciało K_R (np. $\mathbb{Z}$ na $\mathbb{Z}/p\mathbb{Z}$) zamieniającego moduł wolny $\bigoplus_{i\in I} R$ w przestrzeń wektorową $\bigoplus_{i\in I} K_R$.

Wymiarem modułu wolnego M nad niezerowym przemiennym pierścieniem k nazywamy $\dim_k M :=$ ilość elementów jego bazy. W szczególności każda niezerowa przestrzeń wektorowa ma dodatni lub ∞ wymiar. Za wymiar przestrzeni zerowej (modułu zerowego) przyjmujemy 0.

Twierdzenie: Jeśli $0 \to K \to L \xrightarrow{\pi} M \to 0$ jest ciągiem dokładnym wolnych modułów nad niezerowym przemiennym pierścieniem k i $\dim_k K = m$, $\dim_k M = n$, to $\dim_k L = m+n$.

Dowód: Do zadania odwzorowania liniowego na module wolnym potrzeba i wystarcza zadać go dowolnie na jego bazie. Zatem każda surjekcja $\pi : L \to M$ na moduł wolny rozszczepia się odwzorowaniem liniowym $M \xrightarrow{s} L$ zadanym przez wybór: $\forall b \in$ baza M $\exists m_b \in \pi^{-1}(b)$. Stąd $L \cong K \oplus M \cong k^m \oplus k^n = k^{m+n}$. ∎