PIERŚCIEŃ MACIERZY I POJĘCIE WYMIARU

Piotr M. Hajac
Uniwersytet Warszawski

Wykład 13, 15.01.2014

Typeset by Jakub Szczepanik.

Pierścień endomorfizmów i grupa automorfizmów

Niech M będzie dowolnym prawym R-modułem. Przypomnijmy że odwzorowanie liniowe z M do M nazywamy endomorfizmem, a izomorfizm liniowy z M do M nazywamy automorfizmem. Używamy oznaczeń $\mathrm{End}_R(M) := \mathrm{Hom}_R(M, M)$ oraz $\mathrm{Aut}_R(M) := \{ f \in \mathrm{End}_R(M) \mid f \text{ jest bijekcją}\}$.

Przypomnijmy też że ze względu na składanie odwzorowań i punktowe dodawanie $\mathrm{End}_R(M)$ jest pierścieniem gdzie zerem jest odwzorowanie zerowe a jedynką id. Ze względu na składanie odwzorowań $\mathrm{Aut}_R(M)$ jest grupą gdzie elementem neutralnym jest id.

Jeśli M posiada bazę I, to macierzą endomorfizmu f w bazie I nazywamy macierz f w bazach I i I. Rozpatrzmy odwzorowanie

$$\boxed{F_I : \mathrm{End}_R(M) \ni f \longmapsto M_{II}(f) \in M_I^{cf}(R)},$$

gdzie $M_I^{cf}(R) := \{A \in M_I(R) \mid \forall \ i \in I : A_{ji} \neq 0 \text{ dla skończonej ilości } j\}$. Obraz grupy automorfizmów $F_I(\mathrm{Aut}_R(M))$ oznaczamy przez $GL_I(R)$.

Pierścień macierzy i ogólna grupa liniowa

Wiemy już że F_I jest bijekcją przekształcającą składanie endomorfizmów w mnożenie macierzy, a punktowe dodawanie endomorfizmów punktowe dodawanie macierzy. Widać że $F_I(0) = 0$ oraz łatwo sprawdzić że $F_I(\mathrm{id}) = 1_I$, gdzie

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

Zatem $(M_I^{cf}, +, 0, \cdot, 1_I)$ jest pierścieniem, a F_I jest izomorfizmem pierścieni.

Podobnie, $(GL_I(R), \cdot, 1_I)$ jest grupą, a zawężenie F_I do

$$\mathrm{Aut}_R(M) \ni f \longmapsto F_I(f) \in GL_I(R) := F_I(\mathrm{Aut}_R(M))$$

izomorfizmem grup. Bijektywność F_I implikuje że $GL_I(R)$ to grupa wszystkich odwracalnych macierzy w $M_I^{cf}(R)$. Nazywamy ją ogólną grupą linową. Jeżeli $I = \{1, ..., n\}$, stosujemy oznaczenie $GL_n(R)$.

Przykład

Niech $R = \mathbb{Z}$ oraz $M = \mathbb{Z}^2$. Jako przykład dodawania macierzy mamy:

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

Zaś jako przykład mnożenia macierzy odwracalnych mamy:

$$\begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^{\in GL_2(\mathbb{Z})} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} =: 1_2 \in GL_2(\mathbb{Z})\,,$$

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}^{\in GL_2(\mathbb{Z})} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} =: 1_2 \in GL_2(\mathbb{Z})\,.$$

Zmiana bazy

Jak się zmienia macierz endomorfizmu przy zmianie bazy? Niech B i C będą bazami prawego R-modułu M oraz $f \in \mathrm{End}_R(M)$. Wtedy

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

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

Niech $R = \mathbb{Z}$, $M = \mathbb{Z}^2$, $f(m,n) = (m+n, m-n)$, $B = \{(1,0),(0,1)\}$, $C = \{(1,1),(1,0)\}$. Porządkując bazy tak jak są napisane, otrzymujemy:

$$\left.\begin{array}{l} f(1,0) = (1,0)\cdot 1 + (0,1)\cdot 1 \\ f(0,1) = (1,0)\cdot 1 + (0,1)\cdot(-1) \end{array}\right\} \quad \Leftrightarrow \quad M_{BB}(f) = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix},$$

$$\left.\begin{array}{l} f(1,1) = (2,0) = (1,1)\cdot 0 + (1,0)\cdot 2 \\ f(1,0) = (1,1) = (1,1)\cdot 1 + (1,0)\cdot 0 \end{array}\right\} \quad \Leftrightarrow \quad M_{CC}(f) = \begin{pmatrix} 0 & 1 \\ 2 & 0 \end{pmatrix},$$

Przykład

$$\left.\begin{array}{l} \mathrm{id}(1,0) = (1,1)\cdot 0 + (1,0)\cdot 1 \\ \mathrm{id}(0,1) = (1,1)\cdot 1 + (1,0)\cdot(-1) \end{array}\right\} \quad \Leftrightarrow \quad M_{CB}(\mathrm{id}) = \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix},$$

$$\left.\begin{array}{l} \mathrm{id}(1,1) = (1,0)\cdot 1 + (0,1)\cdot 1 \\ \mathrm{id}(1,0) = (1,0)\cdot 1 + (0,1)\cdot 0 \end{array}\right\} \quad \Leftrightarrow \quad M_{BC}(\mathrm{id}) = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}.$$

Łatwo sprawdzić że

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

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

$$M_{BC}(\mathrm{id})M_{CB}(\mathrm{id}) = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Równoliczność baz

Istnieją pierścienie nieprzemienne nad którymi skończone bazy tego samego modułu mogą być różnoliczne: $R^m \cong R^n \not\Rightarrow m = n$. Np. $R^2 \cong R$. Jednakże:

Twierdzenie

Jeśli moduł M na dowolnym pierścieniem R ma nieskończoną bazę B, to każda inna baza M jest równoliczna z B.

To twierdzenie połączone z Lematem Steinitza daje nam:

Twierdzenie

Wszystkie bazy dowolnej niezerowej przestrzeni wektorowej są równoliczne.

Wniosek

Wszystkie bazy dowolnego modułu wolnego nad przemiennym pierścieniem sa równoliczne.

Wymiar

<u>**Szkic dowódu:**</u> Rozumowanie oparte jest na istnieniu homomorfizmu z pieścienia 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 $\bigoplus_{i\in I} k_R$. ■

Definicja

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.

Dodawanie wymiarów

Twierdzenie

Niech $0 \to K \to L \xrightarrow{\pi} M \to 0$ *będzie ciągiem dokładnym modułów nad niezerowym przemiennym pierścieniem* k*. Jeżeli moduły* K *i* M *są wolne, to* L *też jest modułem wolnym oraz*

$$\dim_k L = \dim_k K + \dim_k M .$$

Lemat

Do zadania odwzorowania liniowego na module wolnym M *nad pierścieniem* R *wystarcza zadać go dowolnie na jego bazie.*

Dowód lematu: Niech B będzie bazą M, a N dowolnym R-modułem. Weźmy dowolne odwzorowanie $F : B \to N$. Wtedy odwzorowanie $f : M \to N$ dane wzorem $f(m) = \sum_{b \in B} F(b)\, m_b$, gdzie $m =: \sum_{b \in B} b\, m_b$, jest odwzorowaniem liniowym. ∎

Dowód twierdzenia

Z surjektywności π wynika że $\forall\ b \in B\, \exists\ l_b \in \pi^{-1}(b)$. Na mocy lematu odwzorowanie $B \ni b \mapsto l_b \in L$ możemy rozszerzyć do odwzorowania liniowego $M \xrightarrow{s} L$. Rozszczepia ono π:

$$\begin{aligned}(\pi \circ s)(m) = \pi\Big(s\big(\sum_{b\in B} b\, m_b\big)\Big) &= \pi\Big(\sum_{b\in B} s(b)\, m_b\Big) \\ &= \sum_{b\in B} \pi(l_b)\, m_b = \sum_{b\in B} b\, m_b = m.\end{aligned}$$

Tak więc dzięki twierdzeniu o rozszczepianiu mamy $L \cong K \oplus M$. W połączeniu z twierdzeniem o bazie dostajemy

$$L \cong \bigoplus_{a\in A} k \oplus \bigoplus_{b\in B} k\,,$$

gdzie A jest bazą K. Zatem L jest modułem wolnym posiadającym bazę równoliczną z $A \coprod B$. ∎