OD RÓWNAŃ DO ODWZOROWAŃ LINIOWYCH

Piotr M. Hajac
Uniwersytet Warszawski

Wykład 8, 27.11.2013

Typeset by Jakub Szczepanik.

Motywacja

Przechodzimy od rozwiązywania jednego równania wielomianowego do rozwiązywania układu wielu równań jednomianowych (liniowych). Jest to domena algebry liniowej. Rozpatrzmy układ równań z szukanymi x i y zapisany stadardowo i macierzowo:

$$\begin{cases} ax + by = \alpha \\ cx + dy = \beta \end{cases} \qquad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} \alpha \\ \beta \end{pmatrix} .$$

Załóżmy że pierścień współczynników jest przemienny, pomnóżmy drugie równanie przez a, i podstawmy do niego ax z pierwszego równania:

$$\begin{cases} ax + by = \alpha \\ acx + ady = a\beta \end{cases} \quad \Leftrightarrow \quad \begin{cases} ax = \alpha - by \\ c(\alpha - by) + ady = a\beta \end{cases} .$$

Z ostatniego równania wnioskujemy że $(ad - bc)y = -c\alpha + a\beta$.

Rozwiązanie układu równań liniowych

Podobnie, pomnóżmy drugie równanie przez b i podstawmy do niego by z 1-ego równania:

$$\begin{cases} ax + by = \alpha \\ bcx + bdy = b\beta \end{cases} \Leftrightarrow \quad \begin{cases} by = \alpha - ax \\ bcx + d(\alpha - ax) = b\beta \end{cases}.$$

Stąd $(bc - ad)x = b\beta - d\alpha \Leftrightarrow (ad - bc)x = d\alpha - b\beta$. Zatem

$$\boxed{\begin{cases} ax + by = \alpha \\ cx + dy = \beta \end{cases} \Rightarrow \quad \begin{cases} (ad - bc)x = d\alpha - b\beta \\ (ad - bc)y = -c\alpha + a\beta \end{cases}}.$$

Jedyność rozwiązania

Jeśli $ad - bc \neq 0$ i niej jest dzielnikiem zera, to zachodzi także implikacja w drugą stronę. Istotnie, mnożąc 1-e równanie przez a, 2-e przez b i dodając je do siebie otrzymujemy

$$(ad - bc)(ax + by) = ad\alpha - ab\beta - bc\alpha + ba\beta = (ad - bc)\alpha \ .$$

Podobnie, mnożąc 1-e równanie przez c, 2-e przez d i dodając je do siebie dostajemy

$$(ad - bc)(cx + dy) = cd\alpha - cb\beta - dc\alpha + da\beta = (ad - bc)\beta \ .$$

Stąd

$$\begin{cases} (ad - bc)(ax + by - \alpha) = 0 \\ (ad - bc)(cx + dy - \beta) = 0 \end{cases} .$$

Wnioskujemy dalej że, jeśli istnieje $(ad - bc)^{-1}$, to

$$\begin{cases} ax + by = \alpha \\ cx + dy = \beta \end{cases} \quad \Leftrightarrow \quad \begin{cases} x = (ad - bc)^{-1}(d\alpha - b\beta) \\ y = (ad - bc)^{-1}(-c\alpha + a\beta) \end{cases} .$$

Rozwiązanie takiego układu równań liniowych istnieje i jest jedyne.

Macierze odwracalne

Wyrażenie $ad - bc$ nazywa się wyznacznikiem macierzy $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$.
Macierz jest odwracalna $\Leftrightarrow$ jej wyznacznik jest odwracalny.
W postaci macierzowej nasze rozwiązanie możemy zapisać jako:

$$\begin{pmatrix} x \\ y \end{pmatrix} = \underbrace{\frac{1}{ad - bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} \begin{pmatrix} \alpha \\ \beta \end{pmatrix}.$$

O takich macierzach możemy myśleć jako o odwzorowaniach liniowych $f \colon R^2 \to R^2$, gdzie R oznacza przemienny pierścień współczynników. Odwracalność macierzy oznacza bijektywność odwzorowania. Nasz układ równań liniowych zapisujemy wtedy w postaci $f(v) = w$, a jego rozwiązanie jako $v = f^{-1}(w)$.

ISTOTĄ ALGEBRY LINIOWEJ JEST STRUKTURA MODUŁU NA PRZESTRZENI R^n NAD NIEPRZEMIENNYM PIERŚCIENIEM MACIERZY $M_n(R)$!

Wejście modułów

Definition

Grupę abelową $(M, +, 0)$ wyposażoną w łączne działanie pierścienia $(R, +, 0, \cdot, 1)$ z lewej strony $R \times M \to M$, $\forall\, r, s \in R,\ m \in M :\ r(sm) = (rs)m$, nazywamy lewym modułem nad R wtedy i tylko wtedy gdy

- M1 $\forall\, r, s \in R,\ m \in M\colon (r+s)m = rm + sm$,
- M2 $\forall\, r \in R,\ m, n \in M\colon r(m+n) = rm + rn$,
- M3 $\forall\, m \in M\colon 1m = m$.

Prawy moduł nad R definiujemy analogicznie.

Definition

Niech M będzie lewym modułem nad R. Podzbiór $N \subseteq M$ nazywamy podmodułem M wtedy i tylko wtedy gdy

1. $(N, +, 0)$ jest podgrupą $(M, +, 0)$,
2. $\forall\, r \in R,\ n \in N\colon rn \in N$.

Spostrzeżenia i przykłady

1. $\forall\, m \in M : 0m = 0m + m - m = 0m + 1m - m =$
$(0+1)m - m = 1m - m = m - m = 0.$
2. $\forall\, r \in R : r0 = r0 + r0 - r0 = r(0+0) - r0 = r0 - r0 = 0.$
3. $\forall\, r \in R, m \in M : (-r)m = -(rm)$ bo
$rm + (-r)m = (r-r)m = 0m = 0.$
4. $\forall\, r \in R, m \in M : r(-m) = -(rm)$ bo
$rm + r(-m) = r(m-m) = r0 = 0.$
5. Każda grupa abelowa G jest modułem nad $\mathbb{Z}$:
$ng := \underbrace{g + ... + g}_{n\text{-razy}}, \quad (-n)g := \underbrace{-g - ... - g}_{n\text{-razy}}.$
6. Każdy pierścień R jest modułem nad sobą samym.
7. $R_n[\mathbb{N}] := \{\alpha \in R[\mathbb{N}] \mid \deg(\alpha) \leqslant n\} \cup \{0\}$ jest modułem nad R.
8. Jeśli M jest R-modułem i $X \neq \emptyset$, to $\mathrm{Map}(X, M)$ jest modułem z działaniami punktowymi zarówno nad $\mathrm{Map}(X, R)$ jak i nad R.

Moduł ilorazowy

Fundamentalnymi przykładami modułów są:

1. skończeniewymiarowe przestrzenie wektorowe (algebra liniowa),
2. ∞-wymiarowe przestrzenie Hilberta (mechanika kwantowa),
3. przestrzenie cięć wiązek tensorowych na rozmaitości (ogólna teoria względności),
4. moduły projektywne i moduły Hilberta (jeden z głównych nurtów współczesnej matematyki: K-teoria i KK-teoria).

Definition

Modułem ilorazowym modułu M przez podmoduł N nazywamy $M/N := M/Q_N$, gdzie $Q_N := \{(m, m') \in M^2 \mid m - m' \in N\}$ jest relacją równoważności. Struktura modułu na M/N jest indukowana ze struktury modułu na M:

$$[m] + [m'] := [m + m'], \qquad r[m] := [rm].$$

Odwzorowanie liniowe

Definition

Niech M i N będą lewymi R-modułami. Odwzorowanie $M \xrightarrow{f} N$ nazywamy liniowym (lub homomorfizmem modułów) $\Leftrightarrow$

1. $\forall\, m, m' \in M: \; f(m + m') = f(m) + f(m')$,
2. $\forall\, r \in R,\; m \in M: \; f(rm) = r f(m)$.

Z liniowości f wynika że obraz f, czyli zbiór $\operatorname{Im} f := \{n \in N \mid \exists\, m \in M : f(m) = n\}$, jest podmodułem N.

Definitions

Jądrem i kojądrem odwzorowania liniowego $M \xrightarrow{f} N$ nazywamy odpowiednio

$$\operatorname{Ker} f := \{m \in M \mid f(m) = 0\}, \qquad \operatorname{Coker} f := \frac{N}{\operatorname{Im} f}\,.$$

Z liniowości f wynika też że $\operatorname{Ker} f$ jest podmodułem M.

Twierdzenie o obrazie

Odwzorowanie liniowe f jest:

1. injektywne $\Leftrightarrow \mathrm{Ker}\, f = 0$.
2. surjektywne $\Leftrightarrow \mathrm{Coker}\, f = 0$.

Theorem

Dla dowolnego odwzorowania liniowego $f : M \to N$ zachodzi

$$\mathrm{Im}\, f \cong \frac{M}{\mathrm{Ker}\, f} \ .$$

Dowód: Odwzorowanie liniowe f indukuje odwzorowanie liniowe

$$M/\,\mathrm{Ker}\, f \ni [m] \stackrel{\tilde{f}}{\longmapsto} f(m) \in \mathrm{Im}\, f \ .$$

Jest ewidentnie dobrze zdefiniowane, liniowe i surjektywne.
Wreszcie jest injektywne bo

$$\tilde{f}([m]) = 0 \ \Leftrightarrow \ f(m) = 0 \ \Leftrightarrow \ m \in \mathrm{Ker}\, f \ \Leftrightarrow \ [m] = 0. \qquad \blacksquare$$