ODWZOROWANIA LINIOWE

Motywacja: Przechodzimy od rozwiązywania jednego równania wielomianowego do rozwiązywania układu wielu równań jednomianowych (liniowych). Jest to domena algebry liniowej. Rozpatrzmy taki przykład:

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

Szukamy x i y. Pomnóżmy drugie równanie przez a i podstawmy do niego ax z pierwszego równania:

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

$$\implies (ad - bc)y = -c\alpha + a\beta$$

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

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

$$\Rightarrow (bc-ad)x=b\beta-d\alpha \iff (ad-bc)x=d\alpha-b\beta.$$

Zatem

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

Jeśli $ad-bc\neq 0$ i nie jest dzielnikiem 0, 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 $\exists (ad-bc)^{-1}$, to

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

Rozwiązanie takiego układu równań liniowych istnieje i jest jedyne. Wyrażenie $ad-bc$ nazywa się wyznacznikiem macierzy $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$.
Macierz jest odwracalna $\iff$ 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 macierzach możemy myśleć jako o odwzorowaniach liniowych pomiędzy przestrzeniami wektorowymi $V \xrightarrow{f} V$.
Odwracalność macierzy oznacza wtedy bijektywność odwzorowania. Nasz układ równań liniowych zapisujemy wtedy w postaci $f(v)=w$, a jego rozwiązanie jako

$$v=f^{-1}(f(v))=f^{-1}(w).$$

Grupę abelową $(M, +, 0)$ wyposażoną w łączne działanie pierścienia $(R, +, 0, \cdot, 1)$ z lewej strony

$R \times M \longrightarrow M$ $(\forall r, s \in R, m\ M: r(sm) = (rs)m)$

nazywamy <u>lewym modułem nad R</u> $\Longleftrightarrow$

(M1) $\forall r, s \in R, m \in M: \quad (r+s)m = rm + sm,$

(M2) $\forall r \in R, m, n \in M: \quad r(m+n) = rm + rn,$

(M3) $\forall m \in M: \quad 1 \cdot m = m.$

Prawy moduł nad R definiujemy analogicznie.

<u>Pierwsze spostrzeżenia i przykłady</u>:

(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 $\mathbb{Z}$: $ng = \underbrace{g + \ldots + g}_{n\text{-razy}}$, $(-n)g = \underbrace{-g - \ldots - g}_{n\text{-razy}}$.

⑥ Każdy pierścień R jest modułem nad sobą samym.

⑦ $R_n[\mathbb{N}] := \{\alpha \in R[\mathbb{N}] \mid \deg(\alpha) \leq n\} \cup \{0\}$ jest modułem nad R.

⑧ Jeśli M jest R-modułem i $X \neq \emptyset$, to $Map(X, M)$ jest modułem z działaniami punktowymi zarówno nad $Map(X, R)$ jak i R.

Niech M będzie lewym modułem nad R. Podzbiór $N \subseteq M$ nazywamy <u>podmodułem</u> M $\Leftrightarrow$ (① $(N, +, 0)$ jest podgrupą $(M, +, 0)$ oraz ② $\forall r \in R, n \in N: rn \in N$)

Niech M i N będą lewymi R-modułami. Odwzorowanie $M \xrightarrow{f} N$ nazywamy <u>liniowym</u> (lub <u>homomorfizmem modułów</u>) $\Leftrightarrow$ (L1) $\forall m, m' \in M: f(m+m') = f(m) + f(m')$ (homomorfizm grup) oraz (L2) $\forall r \in R, m M: f(rm) = r f(m)$).

Jądrem odwzorowania liniowego $M \xrightarrow{f} N$

nazywamy $\boxed{\mathrm{Ker}\, f := \{m \in M \mid f(m) = 0\}}$.

Z liniowości f wynika że $\mathrm{Ker}\, f$ jest podmodułem M. Odwzorowanie f jest injektywne $\Leftrightarrow \mathrm{Ker}\, f = 0$. Injektywny homomorfizm nazywamy monomorfizmem.

Modułem ilorazowym modułu M przez podmoduł N nazywamy $M/N := M/Q_N$, gdzie

$\boxed{Q_N := \{(m, m') \in M^2 \mid m - m' \in N\}}$ jest relacją

równoważności. Struktura modułu na M/N jest indukowane ze struktury modułu na M ($[m] + [m'] := [m + m']$, itd.).

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

podmodułem N. Kojądrem f nazywamy moduł ilorazowy $\boxed{\mathrm{Coker}\, f := \frac{N}{\mathrm{Im}\, f}}$. Odwzorowanie f jest surjektywne $\Leftrightarrow \mathrm{Coker}\, f = 0$.

Surjektywny homomorfizm nazywamy epimorfizmem.