# Celočíselné matice, SNF, prezentace abelovských grup

$\mathrm{Mat}_{n\times m}\mathbb{Z}$ ... matice s celočíselnými prvky

$A \in \mathrm{Mat}_{n\times m}\mathbb{Z}$ zadává zobrazení $\mathbb{Z}^m \xrightarrow{A} \mathbb{Z}^n$, $x \longmapsto A\cdot x$ — zjevně homo grup $A(x+y)=Ax+Ay$

**Tvrzení.** Zobrazení $\mathrm{Mat}_{n\times m}\mathbb{Z} \longrightarrow \mathrm{Hom}(\mathbb{Z}^m,\mathbb{Z}^n)$ je bijekce.

$$(\varphi(e_1)\cdots\varphi(e_m)) \longleftarrow \varphi$$

**Důkaz.** $\varphi: \mathbb{Z}^m \longrightarrow \mathbb{Z}^n$

$$\varphi(x) = \varphi(x^1 e_1 + \dots + x^m e_m) = x^1\cdot\varphi(e_1)+\dots+x^m\varphi(e_m) = \left(\varphi(e_1)\cdots\varphi(e_m)\right)\begin{pmatrix}x^1\\ \vdots\\ x^m\end{pmatrix} = A\cdot x$$

$$e_1 = \begin{pmatrix}1\\0\\ \vdots\\0\end{pmatrix}, \quad e_m = \begin{pmatrix}0\\ \vdots\\0\\1\end{pmatrix}$$

$\square$

Implicitně používáme:

$M$ komutativní grupa psaná aditivně $\Rightarrow$ v $M$ umíme „násobit celými čísly"

$$k\cdot x = \underbrace{x+\dots+x}_{k\times} \qquad 0\cdot x = 0 \qquad (-k)\cdot x = \underbrace{(-x)+\dots+(-x)}_{k\times}$$

$\leadsto$ násobení „skaláry" $\mathbb{Z}\times M \to M$, ale $\mathbb{Z}$ není těleso $\Rightarrow$ spousta LA neplatí

$\leadsto$ homomorfismy grup zachovávají toto násobení $\Rightarrow$ jsou „lineární"

Cíl: vyjádřit $A: \mathbb{Z}^m \longrightarrow \mathbb{Z}^n$ „ve vhodných bázích"

$P\cdot A\cdot Q$ — $P$, $Q$ invertibilní

$\Rightarrow A, B$ ... $\exists P,Q: B = PAQ$

$\Leftrightarrow \mathrm{rk}\, A = \mathrm{rk}\, B$

jak to vyjde v LA?

$$\begin{array}{ccc} & \ker^{\perp} & \ker \\ \mathrm{im} & E & 0 \\ \mathrm{im}^{\perp} & 0 & 0 \end{array} \qquad \Bbbk^m \xrightarrow{A} \Bbbk^n$$

$[\bar e_1,\dots,\bar e_r, \underbrace{\bar e_{r+1},\dots,\bar e_m}_{\text{báze ker } A}] \qquad [e_1,\dots,e_r, e_{r+1},\dots,e_n]$

$e_i = A\bar e_i$

**Tvrzení.** Matice $A \in \mathrm{Mat}_{n\times m}\mathbb{Z}$ je invertibilní $\Leftrightarrow$ $n=m$ a $\det A = \pm 1$.

**Důkaz.** • Nechť $B \in \mathrm{Mat}_{m\times n}\mathbb{Z}$ je inverze k $A$. Potom jsou inverzní i nad $\mathbb{Q}$

$\Rightarrow n=m$ a $\underbrace{\det A}_{\in\mathbb{Z}}\cdot\underbrace{\det B}_{\in\mathbb{Z}} = \det(A\cdot B) = \det E = 1$.

• Nechť naopak $A$ je čtvercová s $\det A = \pm 1$. Existuje $A^{-1} \in \mathrm{Mat}_{n\times n}\mathbb{Q}$ a je dána vzorečkem

$$A^{-1} = \underbrace{\frac{1}{\det A}}_{\in\mathbb{Z}}\underbrace{(\text{matice alg. doplňků se znaménky a transponovaná})}_{\text{celočíselná}} \in \mathrm{Mat}_{n\times n}\mathbb{Z}. \quad \square$$

**Poznámka.** Stejný důkaz funguje nad libovolným komutativním okruhem $R$. (podmínka na determinant je $\det A \in R^{\times}$)

Je-li $R$ obor integrity, použijeme místo $R$ podílové těleso $Q(R)$.

Jinak: $M \subseteq R$ lib. max. ideál $\leadsto \Bbbk = R/M$ a opět dostaneme $n=m$

formulka pro inverzi funguje stejně.

Bez komutativity: existují invertibilní nečtvercové matice!

v důkazu se používaly determinanty — nedávají smysl

## Věta (o Smithově normálním tvaru = SNF).

Nechť $A \in \mathrm{Mat}_{n \times m}\, \mathbb{Z}$. Pak existují invertibilní matice $P, Q$ t.ž.

- $P, Q$ jsou součiny elementárních matic nad $\mathbb{Z}$
- $$P^{-1} A Q = \left(\begin{array}{c|c} \begin{matrix} q_1 & & \\ & \ddots & \\ & & q_r \end{matrix} & 0 \\ \hline 0 & 0 \end{array}\right) = S$$ přičemž $q_1 \mid \cdots \mid q_r$ } matice ve Smithově normálním tvaru
- čísla $q_1, \ldots, q_r$ jsou jednoznačná až na znaménko (pro nás kladná $\Rightarrow$ jednoznačná); nazývají se invariantní faktory.
- konkrétněji:

  $d_i = \gcd\{\text{minory } i \times i \text{ matice } A\}$; $d_0 = 1$ ← jediný minor $\det() = 1$ ?

  $q_i = d_i / d_{i-1}$ ← $d_1 = \gcd\{\text{prvky matice } A\}$

Důkaz. • Algoritmus vyložíme na cvičení – kombinace Eukleidova algoritmu k vyrobení nejv. spol. děl. prvků matice a Gaussovy eliminace k následné eliminaci prvků mimo diagonálu (obojí pomocí elementárních operací).

• Studujme, co se děje s $d_i$ při (ne nutně elem. / invert. operacích):

$B = P \cdot A \quad \Rightarrow$ řádky $B$ jsou kombinacemi řádků $A$

$\begin{pmatrix} b^1 \\ \vdots \\ b^n \end{pmatrix} = P \cdot \begin{pmatrix} a^1 \\ \vdots \\ a^n \end{pmatrix} \quad \Rightarrow$ minory $B$ jsou kombinacemi minorů $A$ ($\Rightarrow$ dělitelné $d_i(A)$)

$b^i = p^i_1 a^1 + \cdots + p^i_n a^n \quad \Rightarrow \quad d_i(A) \mid d_i(B)$

Je-li $P$ invertibilní, pak $A = P^{-1} \cdot B \quad \Rightarrow \quad d_i(A) \overset{\pm}{=} d_i(B)$

$\Rightarrow \quad d_i(A)/d_{i-1}(A) = d_i(B)/d_{i-1}(B)$

To samé pro sloupcové operace. $\gcd\{q_{j_1} \cdots q_{j_i}\} = q_1 \cdots q_i$

$$\Rightarrow \quad d_i(A)/d_{i-1}(A) = d_i(S)/d_{i-1}(S) = q_1 \cdots q_i / q_1 \cdots q_{i-1} = q_i. \qquad \square$$

$$S = P^{-1} A Q \iff A = P S Q^{-1}$$

$$\left(\begin{array}{c|c} \begin{matrix} q_1 & & \\ & \ddots & \\ & & q_r \end{matrix} & 0 \\ \hline 0 & 0 \end{array}\right) \begin{pmatrix} x^1 \\ \vdots \\ x^r \\ x^{r+1} \\ \vdots \\ x^m \end{pmatrix} = \begin{pmatrix} q_1 x^1 \\ \vdots \\ q_r x^r \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

$$\Rightarrow \quad \mathrm{im}\, A = P(\mathrm{im}\, S) = P[q_1 e_1, \ldots, q_r e_r] = [q_1 \cdot Pe_1, \ldots, q_r \cdot Pe_r]$$

sloupce matice $P$

$$\Rightarrow \quad \ker A = Q(\ker S) = Q[e_{r+1}, \ldots, e_m] = [Qe_{r+1}, \ldots, Qe_m]$$

sloupce matice $Q$

# Prezentace konečně generovaných abelovských grup

Cíl. Strukturní věta pro kon. gen. ab. grupy = popis až na izo

$M$ kon. gen. abelovská grupa, generovaná $a_1, \ldots, a_n$
(abelovská = komutativní, píšeme aditivně)

$\varphi: \mathbb{Z}^n \longrightarrow M$, $\varphi(x) = (a_1, \ldots, a_n) \begin{pmatrix} x^1 \\ \vdots \end{pmatrix}$ surjektivní homomorfismus komutativní, píšeme aditivně

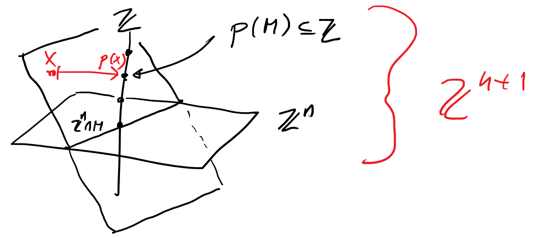
$$\varphi: \mathbb{Z}^n \longrightarrow M, \qquad \varphi(x) = (a_1, \dots, a_n)\cdot\begin{pmatrix} x^1 \\ \vdots \\ x^n \end{pmatrix} \qquad \text{surjektivní homomorfismus}$$
$$e_i \longmapsto a_i \qquad \begin{pmatrix} x^1 \\ \vdots \\ x^n \end{pmatrix} = x^1\cdot e_1 + \dots + x^n\cdot e_n$$

$\Rightarrow$ $M \cong \mathbb{Z}^n/\ker\varphi$ … pochopit kon. gen. ab. grupy = pochopit podgrupy $\mathbb{Z}^n$ a příslušné kvocienty

**Věta.** Každá podgrupa $\mathbb{Z}^n$ je konečně generovaná (ve skutečnosti izomorfní $\mathbb{Z}^m$ pro $m \le n$).

**Důkaz.** Indukcí: • $n = 0$ triviální

• $M \subseteq \mathbb{Z}^{n+1}$ podgrupa $\qquad \overset{(x^0, x^1, \dots, x^n)}{\mathbb{Z}^{n+1}} = \overset{x^0}{\mathbb{Z}} \times \overset{(x^1, \dots, x^n)}{\mathbb{Z}^n}$




Označme $p: \mathbb{Z}^{n+1} \to \mathbb{Z}$ projekci na první složku, pak $\ker p \cong \mathbb{Z}^n$

a $\ker p \cap M = [a_1, \dots, a_m]$.

$p(M) \subseteq \mathbb{Z}$ podgrupa $\Rightarrow$ $p(M) = \mathbb{Z}\cdot t$, $t = p(a_0)$ $\qquad a_0 \in M$

Tvrdíme, že $M = [a_0, a_1, \dots, a_m]$

$x \in M \Rightarrow p(x) \in p(M) = \mathbb{Z}\cdot t \Rightarrow p(x) = y^0\cdot t = p(y^0\cdot a_0)$

Tedy $x - y^0 a_0 \in \ker p \cap M \Rightarrow x - y^0 a_0 = y^1 a_1 + \dots + y^m a_m$.

$\Rightarrow x = y^0 a_0 + y^1 a_1 + \dots + y^m a_m$. $\square$

---

$$\mathbb{Z}^n \overset{\varphi}{\twoheadrightarrow} M$$

$$\mathbb{Z}^m \overset{\psi}{\twoheadrightarrow} \ker\varphi \overset{\text{in}}{\hookrightarrow} \mathbb{Z}^n \overset{\varphi}{\twoheadrightarrow} M, \qquad R = \text{in}\circ\psi : \mathbb{Z}^m \to \mathbb{Z}^n$$

$\left(\begin{array}{l} \varphi: M \to N \\ \operatorname{coker}\varphi = N/\operatorname{im}\varphi \end{array}\right)$

$\Rightarrow$ $M \cong \mathbb{Z}^n/\ker\varphi = \mathbb{Z}^n/\operatorname{im} R =: \operatorname{coker} R$

$\mathbb{Z}^m \xrightarrow{R} \mathbb{Z}^n \overset{\varphi}{\twoheadrightarrow} M$ nazveme prezentací abelovské grupy $M$

$\uparrow$ relace $M$ $\qquad$ $\uparrow$ generátory $M$

$\left.\begin{array}{l} \bullet\ \varphi \text{ surjektivní} \\ \bullet\ \operatorname{im} R = \ker\varphi \end{array}\right\}$ $M \cong \operatorname{coker} R$ $\leftarrow$ matice $R \in \mathrm{Mat}_{n\times m}\mathbb{Z}$ určuje $M$ až na izo

(co řekne SNF?

$S = P^{-1}\cdot R\cdot Q$

$$\begin{array}{ccccc} \mathbb{Z}^m & \xrightarrow{R} & \mathbb{Z}^n & \longrightarrow & \operatorname{coker} R \cong M \\ Q\uparrow\cong & & \cong\uparrow P & & \uparrow\cong \\ \mathbb{Z}^m & \xrightarrow[S]{} & \mathbb{Z}^n & \longrightarrow & \operatorname{coker} S \cong\ ? \end{array}$$

$\operatorname{coker} R = \mathbb{Z}^n/\operatorname{im} R$, $\quad \operatorname{coker} S = \mathbb{Z}^n/\operatorname{im} S$

určeno $P$: $\qquad Px + \operatorname{im} R$
$\qquad\qquad\qquad\qquad \uparrow$
(inverze určena $P^{-1}$) $\quad x + \operatorname{im} S$

$(P(\operatorname{im} S) = \operatorname{im} PS$
$= \operatorname{im} RQ$
$\subseteq \operatorname{im} R)$

**Tvrzení.** $S = \left(\begin{array}{c|c} \begin{matrix} q_1 & & \\ & \ddots & \\ & & q_r \end{matrix} & 0 \\ \hline 0 & 0 \end{array}\right)$ $\Rightarrow$ $\operatorname{coker} S \cong \mathbb{Z}/q_1 \times \dots \times \mathbb{Z}/q_r \times \mathbb{Z}^{n-r}$.

$\uparrow$ $S$ ve SNF

$\operatorname{coker} S = \mathbb{Z}^n/\operatorname{im} S = \mathbb{Z}\times\dots\times\mathbb{Z}\times\mathbb{Z}\times\dots\times\mathbb{Z} / \mathbb{Z}q_1\times\dots\mathbb{Z}q_r\times 0\times\dots\times 0$

$$\begin{array}{ccc} \mathbb{Z}^n & \twoheadrightarrow & \operatorname{coker} R \\ P\uparrow & \nearrow & \uparrow \exists! \\ \mathbb{Z}^n & \twoheadrightarrow & \operatorname{coker} S \end{array}$$

$\longmapsto (x^1 + \mathbb{Z}q_1, \dots, x^r + \mathbb{Z}q_r, x^{r+1}, \dots, x^n)$

S ve SNF

$$\mathbb{Z}^n/\operatorname{im} S = \mathbb{Z}\times\cdots\times\mathbb{Z}\times\mathbb{Z}\times\cdots\times\mathbb{Z}/\mathbb{Z}q_1\times\cdots\mathbb{Z}q_r\times 0\times\cdots\times 0$$

$\mathbb{Z}^n \to$ cokerS

$$(x^1,\dots,x^n)+\operatorname{im} S \longleftrightarrow (x^1+\mathbb{Z}q_1,\dots,x^r+\mathbb{Z}q_r,x^{r+1},\dots,x^n)$$

**Důkaz.** □

Zjevně můžeme vynechat všechny činitele $\mathbb{Z}/1=0$.

**Věta.** Každá konečně generovaná abelovská grupa je izomorfní

$$\mathbb{Z}/q_1\times\cdots\times\mathbb{Z}/q_r\times\mathbb{Z}^k \qquad \text{kde} \qquad 1\neq q_1\mid\cdots\mid q_r \quad , k\geq 0$$

a tyto parametry jsou jednoznačné. $\Longrightarrow$ kanonický tvar

**Důkaz.** Existenci máme, jednoznačnost uvidíme dšlikon z další věty. □

$$q=p_1^{t_1}\cdots p_s^{t_s} \Longrightarrow \mathbb{Z}/q=\mathbb{Z}/p_1^{t_1}\times\cdots\times\mathbb{Z}/p_s^{t_s}$$

Tvrzení $\begin{pmatrix} p_1^{t_1} & & \\ & \ddots & \\ & & p_s^{t_s}\end{pmatrix}$ má SNF $\begin{pmatrix} 1 & & & \\ & \ddots & & \\ & & 1 & \\ & & & \underbrace{p_1^{t_1}\cdots p_s^{t_s}}_{q}\end{pmatrix}$

$\mathbb{Z}/1\times\cdots\times\mathbb{Z}/1\times\mathbb{Z}/q$

**Věta.** Každá konečně generovaná abelovská grupa je izomorfní

$$\mathbb{Z}/p_1^{t_1}\times\cdots\times\mathbb{Z}/p_s^{t_s}\times\mathbb{Z}^k \qquad \text{kde } p_1,\dots,p_s \text{ jsou prvočísla, } t_1,\dots,t_s\geq 1,\ k\geq 0$$

a tyto parametry jsou jednoznačné. $\Longrightarrow$ kanonický tvar

**Důkaz.** Existenci opět máme. Jednoznačnost:

$$M=\mathbb{Z}/p_1^{t_1}\times\cdots\times\mathbb{Z}/p_s^{t_s}\times\mathbb{Z}^k$$

$$\mathbb{Z}/q^t\big/p\cdot\mathbb{Z}/q^t = 0$$

$\uparrow$ p invertibilní modulo $q^t$

$\Rightarrow p\cdot\mathbb{Z}/q^t=\mathbb{Z}/q^t$

$\gcd(p,q^t)=1$

Bezoutovo lemma

$a\cdot p+b\cdot q^t=1$

$a\cdot p\equiv 1 \pmod{q^t}$

v $\mathbb{Z}/q^t$

$x=p\cdot(p^{-1}\cdot x)$

$$\Rightarrow M/p\cdot M=\prod_{p_i=p}\mathbb{Z}/p\times(\mathbb{Z}/p)^k$$

$$p\cdot M/p^2\cdot M=\prod_{\substack{p_i=p\\ t_i\geq 2}}\mathbb{Z}/p\times(\mathbb{Z}/p)^k$$

$$p^{t-1}M/p^t\cdot M=\prod_{\substack{p_i=p\\ t_i\geq t}}\mathbb{Z}/p\times(\mathbb{Z}/p)^k$$

rozpozná všechna prvočísla $p_i$

a všechny exponenty $t_i$

a taky $k=\operatorname{rk} M$

$\llcorner$ tzv. ránk M. □

Jednoznačnost v první větě: podobně nebo jako důsledek jednozn. zde.

**Příklad.** Určete SNF celočíselné matice

$$\mathbb{Z}/2\times\boxed{\mathbb{Z}/2}\times\mathbb{Z}/4\times\boxed{\mathbb{Z}/9}\times\mathbb{Z}/27$$

$$\cong \mathbb{Z}/2\times\mathbb{Z}/18\times\mathbb{Z}/108$$

$$\begin{pmatrix}51 & 30\end{pmatrix}\sim\begin{pmatrix}21 & 30\end{pmatrix}\sim\begin{pmatrix}21 & 9\end{pmatrix}\sim\begin{pmatrix}3 & 9\end{pmatrix}\sim\begin{pmatrix}3 & 0\end{pmatrix} \longleftarrow \text{SNF}$$

$(-1)\times \qquad (-1)\times \qquad (-2)\times$

**Příklad.** Určete SNF celočíselné matice

$$\begin{pmatrix}2 & 1 & -1 & 1\\ 4 & 2 & 1 & 6\\ 6 & 2 & 1 & -2\\ 4 & 1 & 2 & 1\end{pmatrix}\sim\begin{pmatrix}1 & -1 & 1 & 2\\ 2 & 1 & 6 & 4\\ 2 & 1 & -2 & 6\\ 1 & 2 & 1 & 4\end{pmatrix}$$

$$\begin{pmatrix}1 & -1 & 1 & 2\end{pmatrix}$$

$$\sim \begin{pmatrix} 1 & -1 & 1 & 2 \\ 0 & 3 & 4 & 0 \\ 0 & 3 & -4 & 2 \\ 0 & 3 & 0 & 2 \end{pmatrix}$$

$$\sim \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 3 & 4 & 0 \\ 0 & 3 & -4 & 2 \\ 0 & 3 & 0 & 2 \end{pmatrix}$$

$$\sim \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 4 & 0 \\ 0 & 7 & -4 & 2 \\ 0 & 3 & 0 & 2 \end{pmatrix}$$

$$\sim \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 4 & 0 \\ 0 & 0 & 24 & 2 \\ 0 & 0 & 12 & 2 \end{pmatrix}$$

$$\sim \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & +1 & 0 & 0 \\ 0 & 0 & 24 & 2 \\ 0 & 0 & 12 & 2 \end{pmatrix}$$

$$\sim \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 2 & 24 \\ 0 & 0 & 2 & 12 \end{pmatrix}$$

$$\sim \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 2 & 24 \\ 0 & 0 & 0 & -12 \end{pmatrix}$$

$$\sim \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 12 \end{pmatrix} \longleftarrow \text{SNF}$$

# Polynomiální matice, SNF, kanonické tvary operátorů

Budeme uvažovat matice s prvky v okruhu $\Bbbk[\lambda]$, kde $\Bbbk$ je těleso

PID; $\mathbb{Z}[\lambda] \supseteq (2, \lambda)$ není hlavní

$\rightsquigarrow$ $\mathrm{Mat}_{n\times m}\, \Bbbk[\lambda]$ matice $n\times m$ s prvky z $\Bbbk[\lambda]$

$\Bbbk[x,y] \supseteq (x,y)$ není hlavní

$\rightsquigarrow$ Lemma. $A \in \mathrm{Mat}_{n\times m}\, \Bbbk[\lambda]$ je invertibilní $\iff$ $n=m$ & $\det A \in \Bbbk^\times$.

konst. nenulové pol.

Věta (o SNF). $A \in \mathrm{Mat}_{n\times m}\, \Bbbk[\lambda] \implies$ existují invertibilní matice $P, Q$ t.ž.

- $P, Q$ jsou součiny elementárních matic nad $\Bbbk[\lambda]$
- $PAQ = \left(\begin{array}{ccc|c} q_1 & & & \\ & \ddots & & 0 \\ & & q_r & \\ \hline & 0 & & 0 \end{array}\right) = S$ 

  přičemž $q_1 \mid \cdots \mid q_r$ $\Bigg\}$ matice ve Smithově normálním tvaru

- polynomy $q_1 \mid \cdots \mid q_r$ jsou jednoznačné až na násobení nenulovým skalárem (pro nás normované $\Rightarrow$ jednoznačné); nazývají se invariantní faktory.
- konkrétněji:

  jediný minor $\det() = 1$ ?

  $d_i = \gcd\{\text{minory } i\times i \text{ matice } A\}$; $d_0 = 1$

  $q_i = d_i / d_{i-1}$

  $d_1 = \gcd\{\text{prvky matice } A\}$

$A \in \mathrm{Mat}_{n\times m}\, \Bbbk \rightsquigarrow$ lineární zobrazení $\Bbbk^m \to \Bbbk^n$

$A \in \mathrm{Mat}_{n\times m}\, \mathbb{Z} \rightsquigarrow$ homomorfismus grup $\mathbb{Z}^m \to \mathbb{Z}^n$

$A \in \mathrm{Mat}_{n\times m}\, \Bbbk[\lambda] \rightsquigarrow$ homomorfismus čeho? $\Bbbk[\lambda]^m \to \Bbbk[\lambda]^n$

$\Big\}$ sčítání a násobení skaláry

$\Leftarrow$ „jediný" rozdíl je v tom, že $\Bbbk[\lambda]$ není těleso

Definice. $\Bbbk[\lambda]$-modul je abelovská grupa $M$ společně s operací násobení skaláry

$$\Bbbk[\lambda] \times M \longrightarrow M$$
$$(p, x) \longmapsto p\cdot x$$

splňující
$$p\cdot(q\cdot x) = (p\cdot q)\cdot x, \quad 1\cdot x = x,$$
$$(p+q)\cdot x = p\cdot x + q\cdot x, \quad p\cdot(x+y) = p\cdot x + p\cdot y$$

Příklad. $M = \Bbbk[\lambda]^n$ s operacemi „po složkách"

$$p\cdot(q_1, \dots, q_n) = (p\cdot q_1, \dots, p\cdot q_n)$$

násobení polynomy $\iff$ $\Big\{$ násobení skaláry z $\Bbbk$ ... monomem $\lambda$ ... zobrazení $m_\lambda : M \to M$

násobení polynomy $\iff \begin{cases} \text{násobení skaláry z } \Bbbk \\ \text{násobení monomem } \lambda \dots \text{ zobrazení } m_\lambda : M \to M \\ \qquad\qquad\qquad\qquad\qquad\qquad\qquad x \mapsto \lambda\cdot x \end{cases}$

$\Rightarrow$ snadné

$$\Leftarrow \quad p\cdot x = (p_0 + p_1\lambda + \dots + p_k\lambda^k)\cdot x = p_0 x + p_1(\lambda\cdot x) + \dots + p_k(\lambda\cdot(\dots\lambda\cdot(\lambda\cdot x)\dots))$$
$$= p_0 x + p_1\, m_\lambda(x) + \dots + p_k\, m_\lambda^k(x)$$
$$= (p_0\, id + p_1 m_\lambda + \dots + p_k m_\lambda^k)(x)$$

**Věta.** Struktura $\Bbbk[\lambda]$-modulu na $M \iff \begin{cases} \text{struktura v.p.} / \Bbbk \text{ na } M \\ \text{lin. operátor } T : M \to M \end{cases}$

$T = m_\lambda$ je lineární: $m_\lambda(ax+by)$
$= \lambda\cdot(ax+by)$
$= a(\lambda x) + b(\lambda y)$
$= a\, m_\lambda(x) + b\, m_\lambda(y)$

$\lambda\cdot ax$
$=(\lambda a)\cdot x$
$=(a\lambda)\cdot x = a\cdot\lambda x$

Podle předchozího můžeme psát $p\cdot x = p(T)x$

kde $p(T) = p_0\cdot Id + p_1\cdot T + \dots + p_k\cdot T^k$

**Příklad.** $\Bbbk[\lambda]$ jakožto $\Bbbk[\lambda]$-modul snadný; jakožto v.p. $/\Bbbk$ s operátorem

$$\left.\begin{aligned} \Bbbk[\lambda] = \Bbbk^{\oplus\mathbb{N}_0} &= \{(a_0,a_1,\dots) \mid a_k = 0 \quad \forall k \gg 0\} \\ T(a_0,a_1,\dots) &= (0,a_0,a_1,\dots) \end{aligned}\right\} \text{komplikovanější}$$

**Definice.** Zobrazení $\varphi : M \to N$ se nazývá homomorfismus $\Bbbk[\lambda]$-modulů, jestliže $\varphi(px+qy) = p\,\varphi(x) + q\,\varphi(y)$.

$M = (V,T), \qquad N = (U,S)$

**Věta.** $\varphi : V \to U$ je homomorfismus $\Bbbk[\lambda]$-modulů, právě když je lineární a komutuje diagram

$$\begin{tikzcd} V \arrow[r, "\varphi"] \arrow[d, "T"'] & U \arrow[d, "S"] \\ V \arrow[r, "\varphi"] & U \end{tikzcd}$$

$\leftarrow$ pro isomorfismus $\varphi$
$S = \varphi T \varphi^{-1}$ ... podobnost operátorů

**Důkaz.** linearita = zachovává násobení konst. polynomy
diagram = zachovává násobení polynomem $\lambda$ $\square$

**Věta.** Homomorfismus $\Bbbk[\lambda]$-modulů $\varphi : \Bbbk[\lambda]^n \to M$ je jednoznačně určen (libovolnými) obrazy $\varphi(e_1),\dots,\varphi(e_n) \in M$. Zejména homomorfismy $\Bbbk[\lambda]$-modulů $\Bbbk[\lambda]^m \to \Bbbk[\lambda]^n$ jsou v bijekci s maticemi z $\mathrm{Mat}_{n\times m}\,\Bbbk[\lambda]$.

**Důkaz.** $$\varphi\begin{pmatrix} p^1 \\ \vdots \\ p^n \end{pmatrix} = \varphi(p^1\cdot e_1 + \dots + p^n\cdot e_n) = p^1\cdot\varphi(e_1) + \dots + p^n\cdot\varphi(e_n)$$
$$= (\varphi(e_1) \ \dots \ \varphi(e_n)) \begin{pmatrix} p^1 \\ \vdots \\ p^n \end{pmatrix}. \qquad \square$$

Alternativně můžeme psát $\begin{pmatrix} p^1 \\ \vdots \\ p^n \end{pmatrix} = v_0 + \lambda v_1 + \dots + \lambda^k v_k \implies$

$\implies \varphi\begin{pmatrix} p^1 \\ \vdots \\ p^k \end{pmatrix} = \varphi(v_0) + \lambda\varphi(v_1) + \dots + \lambda^k \varphi(v_k)$ ... pomocí lin. zobr. $\varphi : \mathbb{k}^n \to M$.

**Definice.** $N \subseteq M$ $\mathbb{k}[\lambda]$-podmodul $\implies$ $M/N = \{x + N \mid x \in M\}$ je opět $\mathbb{k}[\lambda]$-modul s násobení skaláry

$$p \cdot (x+N) \overset{def}{=} px + N.$$

## Kanonická prezentace operátoru na $\mathbb{k}^n$

Mějme operátor $T$ na $\mathbb{k}^n$, tj. $T \in \mathrm{Mat}_{n\times n}\mathbb{k}$.

$$\mathbb{k}[\lambda]^n \xrightarrow{T-\lambda E} \mathbb{k}[\lambda]^n \xrightarrow{\varphi} (\mathbb{k}^n, T)$$

$e_i \longmapsto e_i \implies \varphi(v_0 + \lambda v_1 + \dots + \lambda^k v_k) = v_0 + Tv_1 + \dots + T^k v_k$

**Věta** $\mathrm{im}\,(T-\lambda E) = \ker\varphi \implies (\mathbb{k}^n, T) \cong \mathrm{coker}\,(T-\lambda E) = \mathbb{k}[\lambda]^n / \mathrm{im}\,(T-\lambda E)$

**Důkaz.** $\subseteq$ znamená $\varphi \circ (T-\lambda E) = 0 \iff \varphi((T-\lambda E)e_i) = 0$

ale $\varphi((T-\lambda E)e_i) = \varphi(Te_i - \lambda e_i) = Te_i - Te_i = 0$ ✓

$\supseteq$ nechť $x = v_0 + \lambda v_1 + \dots + \lambda^k v_k \in \ker\varphi$, ukážeme, že $v \equiv 0$ (mod $\mathrm{im}\,(T-\lambda E)$)

přitom $Tv \equiv \lambda v$ (mod $\mathrm{im}\,(T-\lambda E)$)

$\implies x \equiv v_0 + Tv_1 + \dots + T^k v_k = \varphi(x) = 0$ ✓ $\square$

$\implies$ opět $\mathrm{SNF}(T-\lambda E)$ má zásadní roli při klasifikaci $\mathbb{k}[\lambda]$-modulů $(\mathbb{k}^n, T)$ až na isomorfismus

$=$ operátorů $T$ na $\mathbb{k}^n$ až na podobnost.