1. Mooreova-Penroseova pseudoinverze

Nechť $\varphi : U \to V$ je lineární zobrazení mezi Eukleidovskými prostory. Zabývejme se otázkou, zda existuje inverzní zobrazení a v případě, že neexistuje, otázkou, jak blízko se k inverzi můžeme přiblížit. Nechť tedy $\psi : V \to U$ je libovolné zobrazení a zkoumejme složení $\psi\varphi$ a $\varphi\psi$. Zřejmě je $\psi\varphi = 0$ na $\ker\varphi$ a nejlepší, co můžeme očekávat, je, že bude toto složení rovno identitě na nějakém doplňku $\ker\varphi$. Symetricky můžeme očekávat $\varphi\psi = \mathrm{id}$ pouze na nějakém doplňku $\ker\psi$.

Definice 1.1. Lineární zobrazení $\psi : V \to U$ se nazývá *Mooreova-Penroseova pseudoinverze* lineárního zobrazení $\varphi : U \to V$, jestliže

- $\psi\varphi = \mathrm{id}$ na $(\ker\varphi)^\perp$ a
- $\varphi\psi = \mathrm{id}$ na $(\ker\psi)^\perp$.

Protože je vždy $\psi\varphi = 0$, je první podmínka ekvivalentní tomu, že $\psi\varphi$ je kolmá projekce na $(\ker\varphi)^\perp$.

Lemma 1.2. *Pro Mooreovu-Penroseovu pseudoinverzi platí* $\mathrm{im}\,\varphi = (\ker\psi)^\perp$.

Důkaz. Podle druhé podmínky z definice platí $(\ker\psi)^\perp \subseteq \mathrm{im}\,\varphi$, ukážeme nyní opačnou inkluzi. Prvně si uvědomme, že platí $\varphi\psi\varphi = \varphi$ — na $\ker\varphi$ jsou obě strany nulové a na $(\ker\varphi)^\perp$ to plyne z první podmínky. Jinými slovy tato rovnost znamená, že $\varphi\psi = \mathrm{id}$ na $\mathrm{im}\,\varphi$. Zároveň je však kompozice $\varphi\psi$ projekce, musí tedy nutně $\mathrm{im}\,\varphi$ ležet v jejím obraze $(\ker\psi)^\perp$. □

Symbolicky budeme situaci z předchozí definice/lemmatu znázorňovat diagramem

$$\begin{array}{ccc} (\ker\varphi)^\perp & \underset{\psi}{\overset{\varphi}{\underset{\cong}{\rightleftarrows}}} & \mathrm{im}\,\varphi \\ \oplus & & \oplus \\ \ker\varphi & & (\mathrm{im}\,\varphi)^\perp \end{array}$$

kde fakt, že ψ je naznačené jako zobrazení $\mathrm{im}\,\varphi \to (\ker\varphi)^\perp$ značí, že je nulové na komplementu $(\mathrm{im}\,\varphi)^\perp$ a jeho komponenta v $\ker\varphi$ je taktéž nulová. Značka $\cong$ uprostřed značí, že jakožto zobrazení mezi $(\ker\varphi)^\perp$ a $\mathrm{im}\,\varphi$ jsou φ a ψ vzájemně inverzní.

Jiné výhodné značení je pomocí blokových matic. Pokud zvolíme na U bázi tak, že vektory ze začátku tvoří bázi $(\ker\varphi)^\perp$, zatímco vektory z konce tvoří bázi $\ker\varphi$ a analogicky pro V a podprostory $\mathrm{im}\,\varphi$, $(\mathrm{im}\,\varphi)^\perp$, lze matice φ a ψ psát v blokovém tvaru

$$\varphi = \begin{pmatrix} A & 0 \\ 0 & 0 \end{pmatrix}, \qquad \psi = \begin{pmatrix} A^{-1} & 0 \\ 0 & 0 \end{pmatrix}$$

U první matice dva nulové bloky napravo značí, že $\varphi|_{\ker\varphi} = 0$, zatímco dva nulové bloky dole značí, že komponenta φ v $(\mathrm{im}\,\varphi)^\perp$ je nulová.

Zřejmě také naopak v situaci z předchozího diagramu je $(\mathrm{im}\,\varphi)^\perp = \ker\psi$ a ψ je Mooreovou-Penroseovou pseudoinverzí φ. Tímto dostáváme jednoduše následující tvrzení.

Tvrzení 1.3. *Nechť $\varphi : U \to V$ je lineární zobrazení mezi Eukleidovskými prostory (konečné dimenze). Potom Mooreova-Penroseova pseudoinverze existuje a je jediná. Značíme ji φ^+.* □

Tradičně se Mooreova-Penroseova pseudoinverze definuje pomocí singulárního rozkladu (singular value decomposition). Tento přístup je výhodný i z dalších důvodů. Uvažujme proto adjungované zobrazení $\varphi^* : V \to U$.

Lemma 1.4. *Zobrazení $\varphi^*\varphi$ je samoadjungované a platí $\langle\varphi^*\varphi(u), u\rangle \geq 0$ (říkáme, že $\varphi^*\varphi$ je pozitivně semidefinitní). Navíc* $\ker(\varphi^*\varphi) = \ker\varphi$.

Důkaz. Z definice adjungovaného zobrazení platí

$$\langle\varphi^*\varphi(u), u'\rangle = \langle\varphi(u), \varphi(u')\rangle = \langle u, \varphi^*\varphi(u')\rangle$$

a navíc prostřední člen je pro $u = u'$ nezáporný.

Inkluze $\ker(\varphi^*\varphi) \supseteq \ker\varphi$ je zřejmá. Je-li naopak $\varphi^*\varphi(u) = 0$, pak také $0 = \langle\varphi^*\varphi(u), u\rangle = |\varphi(u)|^2$ a proto $\varphi(u) = 0$, tedy $u \in \ker\varphi$. □

Podle tohoto lemmatu existuje na U ortonormální báze $\alpha = (u_1, \ldots, u_m)$ složená z vlastních vektorů $\varphi^*\varphi$ a můžeme ji zvolit tak, že

$$[u_{r+1}, \ldots, u_m] = \ker(\varphi^*\varphi) = \ker\varphi$$

a tím pádem

$$[u_1, \ldots, u_r] = (\ker\varphi)^\perp.$$

Nechť vlastní čísla příslušná $u_1, \ldots, u_m$ jsou $\lambda_1, \ldots, \lambda_m$. Podle naší volby $\lambda_{r+1} = \cdots = \lambda_m = 0$ a zbylá λ_i jsou nenulová. Stále podle předchozího lemmatu platí

$$\lambda_i = \langle\lambda_i u_i, u_i\rangle = \langle\varphi^*\varphi(u_i), u_i\rangle \geq 0$$

Zkonstruujme nyní vhodnou ortonormální bázi V, vzhledem k níž bude mít φ co nejjednodušší tvar. Prvně se zabývejme obrazem φ, který je generován $\varphi(u_1), \ldots, \varphi(u_r)$:

$$\langle\varphi(u_i), \varphi(u_j)\rangle = \langle\varphi^*\varphi(u_i), u_j\rangle = \lambda_i\langle u_i, u_j\rangle = \lambda_i\delta_{ij}.$$

Jsou tedy vektory $\varphi(u_i)$ navzájem kolmé o velikostech

$$|\varphi(u_i)| = \sqrt{\lambda_i} = s_i.$$

Tato čísla nazýváme *singulární hodnoty* zobrazení φ. Položíme

$$v_i = \tfrac{1}{s_i}\varphi(u_i)$$

pro $i = 1, \ldots, r$ a doplníme $v_1, \ldots, v_r$ do ortonormální báze $\beta = (v_1, \ldots, v_n)$ prostoru V.

Vzhledem k těmto bázím má φ matici

$$(\varphi)_{\beta\alpha} = \begin{pmatrix} s_1 & 0 & \cdots & \cdots & 0 \\ 0 & \ddots & \ddots & & \vdots \\ \vdots & \ddots & s_r & \ddots & \vdots \\ \vdots & & \ddots & 0 & \ddots \\ 0 & \cdots & \cdots & \ddots & \ddots \end{pmatrix}$$

(tato matice má rozměry $m \times n$). Poznamenejme, že matice adjungovaného zobrazení φ^* je "stejná", akorát má rozměry $n \times m$. V těchto bázích je také extrémně jednoduché napsat

Mooreovu-Penroseovu pseudoinverzi

$$(\varphi^+)_{\alpha\beta} = \begin{pmatrix} (s_1)^{-1} & 0 & \cdots & \cdots & 0 \\ 0 & \ddots & \ddots & & \vdots \\ \vdots & \ddots & (s_r)^{-1} & \ddots & \vdots \\ \vdots & & \ddots & 0 & \ddots \\ 0 & \cdots & \cdots & \ddots & \ddots \end{pmatrix}$$

Tímto souřadnicovým zápisem se často Mooreova-Penroseova pseudoinverze definuje. Elegantně to lze provést následující úvahou. Pracujme pro jednoduchost ve standardních Eukleidovských prostorech a místo φ pracujme s maticí M. Ve výše popsaných bázích α, β má M diagonální matici, označme ji Σ. To znamená, že lze psát

$$M = P\Sigma Q^*,$$

kde P, Q jsou ortogonální matice. Tomuto rozkladu matice M se říká singulární rozklad. Mooreovu-Penroseovu pseudoinverzi potom můžeme spočítat jako $M^+ = Q\Sigma^+P^*$, kde Σ^+ vznikne (tak jako výše) z diagonální matice Σ inverzí všech nenulových prvků.

Poznamenejme ještě, že z matice $(\varphi)_{\beta\alpha}$ lze také odvodit geometrický význam singulárních hodnot. Uvážíme-li v U jednotkovou sféru, pak její obraz při zobrazení φ je (v některých směrech možná zdegenerovaný) elipsoid, jehož délky poloos jsou právě singulární hodnoty.

Tvrzení 1.5. *Platí následující vztahy*

- *Je-li φ injektivní, potom $\varphi^+ = (\varphi^*\varphi)^{-1}\varphi^*$.*
- *Je-li φ surjektivní, potom $\varphi^+ = \varphi^*(\varphi\varphi^*)^{-1}$.*

Důkaz. V bázích α, β jsou všechny uvažované matice diagonální. V případě injektivního φ má $\varphi^*\varphi$ na diagonále pouze čísla s_i^2. Proto $(\varphi^*\varphi)^{-1}$ existuje a má na diagonále čísla s_i^{-2} a tím pádem pravá strana má na diagonále prvky s_i^{-1}. Týž diagonální tvar levé strany jsme odvodili před tvrzením. Podobná analýza funguje v případě surjektivního φ. □

Věta 1.6. *Platí*

(1) $\varphi\varphi^+\varphi = \varphi$
(2) $\varphi^+\varphi\varphi^+ = \varphi^+$
(3) $\varphi^+\varphi$ *je samoadjungované*
(4) $\varphi\varphi^+$ *je samoadjungované*

Naopak každé zobrazení splňující tyto čtyři vztahy je Mooreovou-Penroseovou pseudoinverzí.

Důkaz. Je jednoduché ověřit vztahy z tvrzení pro Mooreovu-Penroseovu pseudoinverzi; vlastnosti (3) a (4) platí proto, že příslušné kompozice jsou kolmé projekce na podprostory $\operatorname{im}\varphi$ a $(\ker\varphi)^\perp$. V tomto i opačném směru je podstatné si uvědomit, že projekce je samoadjungovaná, právě když je kolmá[1].

Podle (1) a (3) je $\varphi^+\varphi$ samoadjungovaná projekce (neboť $(\varphi^+\varphi)^2 = \varphi^+\varphi$) ve směru $\ker(\varphi^+\varphi) = \ker\varphi$, nutně tedy kolmá. Proto je jejím obrazem $(\ker\varphi)^\perp$ a φ^+ tedy splňuje první definiční vztah.

[1]Podle definice je projekce p je samoadjungovaná, právě když $\langle u, p(v)\rangle = \langle p(u), v\rangle$. Tato podmínka je triviálně splněná pro $u, v \in \ker p$ a $u, v \in \operatorname{im} p$. Pro $u \in \ker p$, $v \in \operatorname{im} p$ tato podmínka je $\langle u, v\rangle = 0$, tedy právě $\ker p \perp \operatorname{im} p$. Zbylý případ $u \in \operatorname{im} p$, $v \in \ker p$ je symetrický.

Téměř v jakékoliv knize pojednávající o Mooreově-Penroseově pseudoinverzi lze najít alternativní důkaz hrubou silou. □

2. Aproximace řešení soustavy lineárních rovnic

Zabývejme se soustavou lineárních rovnic $Ax = v$. Pokud je matice A čtvercová a invertibilní, lze formálně tuto soustavu vyřešit vynásobením inverzí A^{-1},

$$x = A^{-1}Ax = A^{-1}v.$$

V případě, že A nemá inverzi nebo dokonce není ani čtvercová, lze stále něco říct o řešeních pomocí Mooreovy-Penroseovy pseudoinverze.

Tvrzení 2.1. *Soustava $Ax = v$ má řešení, právě když*

$$AA^+v = v$$

Důkaz. Pokud platí $AA^+v = v$, pak zřejmě A^+v je řešením. Naopak, pokud $Ax = v$ pro nějaké x, potom

$$AA^+v = AA^+Ax = Ax = v.$$

Jiný důkaz spočívá v tom, že AA^+ je projekce na $\operatorname{im} A$, a proto rovnost $AA^+v = v$ je ekvivalentní tomu, že $v \in \operatorname{im} A$, což je zřejmě to samé, že soustava má řešení. □

Vidíme tedy, že i v případě, že A nemá inverzi, nebo dokonce není ani čtvercová, můžeme nějaké její řešení (v případě, že existuje) najít jako A^+v. V následujícím ukážeme, jaký geometrický význam toto řešení má. Obecněji se budeme zabývat otázkou geometrického významu A^+v i v případě, kdy soustava $Ax = v$ nemusí nutně mít řešení.

Řekneme, že x je nejlepší aproximace řešení, jestliže minimalizuje výraz $|Ax - v|$, tj. pokud pro libovolné y platí

$$|Ax - v| \leq |Ay - v|$$

Zřejmě je tedy Ax bod $\operatorname{im} A$, který je nejblíž v, je to tedy kolmá projekce vektoru v do podprostoru $\operatorname{im} A$. Tu umíme podle předchozího napsat pomocí pseudoinverze jako AA^+v. Platí tedy

Lemma 2.2. *Vektor x je nejlepší aproximací řešení soustavy $Ax = v$, právě když platí*

$$Ax = AA^+v.$$

Zejména tedy A^+v je nejlepší aproximace řešení. Obecně je takových nejlepších aproximací víc. Mezi nimi lze A^+v charakterizovat pomocí následující věty

Věta 2.3. *Vektor A^+v je nejlepší aproximace řešení soustavy $Ax = v$ s nejmenší normou, "zkráceně" nejmenší nejlepší aproximace řešení.*

Důkaz. Množina nejlepších aproximací je právě množinou řešení soustavy

$$Ax = AA^+v$$

a jedná se tedy o afinní podprostor se zaměřením $\ker A$. Vektor z tohoto afinního podprostoru s nejmenší normou je tedy jediný a to právě ten, který je kolmý na zaměření $\ker A$. Přitom ale $A^+v \in \operatorname{im} A^+ = (\ker A)^\perp$. □

Příklad 2.4 (Aproximace přímkou)**.** Nechť jsou v rovině dány body $(x_1, y_1), \ldots, (x_n, y_n)$. Úkolem je vést těmito body přímku. Pokud by to bylo možné přesně, existovaly by a, b (koeficienty v rovnici přímky $a + bx = y$) takové, že

$$\begin{aligned} a \cdot 1 + b \cdot x_1 &= y_1 \\ \vdots \qquad & \qquad \vdots \\ a \cdot 1 + b \cdot x_n &= y_n \end{aligned}$$

Naším úkolem je tedy vyřešit soustavu (vzhledem k neznámým a, b) s rozšířenou maticí

$$\left(\begin{array}{cc|c} 1 & x_1 & y_1 \\ \vdots & \vdots & \vdots \\ 1 & x_n & y_n \end{array}\right)$$

Její nejmenší nejlepší aproximace řešení je

$$(a, b)^T = \begin{pmatrix} 1 & x_1 \\ \vdots & \vdots \\ 1 & x_n \end{pmatrix}^+ \cdot \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}$$

Přímka s rovnicí $y = a + bx$ se nazývá aproximací přímkou zadané n-tice bodů. Je potřeba však vysvětlit, v jakém smyslu je to nejoptimálnější odpověď na naší otázku proložení přímky zadanými body. Tato přímka minimalizuje

$$\sum_{i=1}^{n} \big((a + bx_i) - y_i\big)^2,$$

tedy odchylku funkčních hodnot $a + bx_i$ od zadaných y_i. Tato aproximace se používá, pokud víme, že zadané hodnoty y_i můžou být zatíženy chybou, ale x_i jsou naměřeny přesně.

3. Něco málo k dualitě

Nechť $U \subseteq V$ je vektorový podprostor a uvažujme vložení

$$\iota : U \hookrightarrow V$$

a k němu duální surjektivní zobrazení

$$\iota^* : V^* \twoheadrightarrow U^*,$$

které je zřejmě dáno předpisem $\eta \mapsto \eta|_U$. Definujme

$$U^\perp = \ker \iota^* = \{\eta \in V^* \mid \forall u \in U : (\eta, u) = 0\},$$

kde podmínku $(\eta, u) = 0$ si lze představovat jako "$\eta \perp U$ neboli $\eta \in U^\perp$"; proto také tento podprostor duálního prostoru značíme tímto symbolem.

Pokud je V reálný vektorový prostor se skalárním součinem, je zobrazení

$$R : V \to V^*, \qquad v \mapsto \langle v, - \rangle$$

izomorfismus a lze jej použít pro ztotožnění V^* s V. Při tomto ztotožnění

$$U^\perp \approx \{v \in V \mid \forall u \in U : (Rv, u) = 0\},$$

přičemž $(Rv, u) = Rv(u) = \langle v, - \rangle(u) = \langle v, u \rangle$. Jedná se tedy o opravdový kolmý doplněk a není špatné si jej takto představovat i pokud nemáme skalární součin k dispozici.

Vraťme se nyní do obecné situace. Přiřazení $U \mapsto U^\perp$ je zobrazení

$$D_V : \{\text{podprostory } V\} \longrightarrow \{\text{podprostory } V^*\},$$

které zjevně obrací uspořádání, tj. pokud $U_0 \subseteq U_1$, pak $U_0^\perp \supseteq U_1^\perp$. Navíc, pokud U má dimenzi d, pak $U^\perp$ má dimenzi $n-d$ (také říkáme, že má kodimenzi d). To je proto, že je jádrem surjektivního zobrazení $V^* \twoheadrightarrow U^*$ z n-rozměrného do d-rozměrného prostoru.

Naším dalším krokem bude ukázat, že zobrazení D_V je bijekce (a tedy antiizomorfismus uspořádaných množin – ve skutečnosti svazů). Zabývejme se proto tím, co se stane při druhé aplikaci "kolmého doplňku". Geometrická intuice z Eukleidovských prostorů říká, že druhý kolmý doplněk musí nutně obsahovat původní prostor a ve skutečnosti se musí rovnat, protože mají stejné dimenze. Stejný argument funguje i obecně, jen je potřeba druhý kolmý doplněk nejprve převést z V^{**} do V. Označíme-li vložení $\kappa : U^\perp \hookrightarrow V^*$, je prostor $U^{\perp\perp}$ jádrem

$$V \cong V^{**} \xrightarrow{\kappa^*} U^{\perp *},$$

které posílá $v \mapsto \mathrm{ev}_v \mapsto \mathrm{ev}_v|_{U^\perp}$. Při identifikaci $V \cong V^{**}$ je tedy $U^{\perp\perp}$ množina všech vektorů v, které se nulují na všech formách z $U^\perp$. Protože se však všechny formy z $U^\perp$ podle definice nulují na U, platí $U \subseteq U^{\perp\perp}$. Zároveň mají oba prostory stejnou dimenzi, musí být tedy totožné, $U^{\perp\perp} = U$.

Věta 3.1. *Zobrazení $U \mapsto U^\perp$ určuje bijektivní zobrazení*

$$D_V : \{\textit{podprostory } V\} \longrightarrow \{\textit{podprostory } V^*\}$$

s následujícími vlastnostmi

- *D_V převrací uspořádání,*
- *je-li U dimenze d, pak $D_V U = U^\perp$ je dimenze $n-d$,*
- *$(U_0 \cap U_1)^\perp = U_0^\perp + U_1^\perp$,*
- *$(U_0 + U_1)^\perp = U_0^\perp \cap U_1^\perp$*

Důkaz. Vše je důsledkem prvního bodu, dokonce i vztah mezi dimenzemi. Můžeme totiž vyčíst dimenzi U jako délku d nejdelšího striktně rostoucího řetězce podprostorů $0 = U_0 \subsetneq U_1 \subsetneq \cdots \subsetneq U_d = U$. □

Pěknou aplikací je popsání svazku všech rovin v prostoru procházejících danou přímkou p. Přechodem ke kolmým doplňkům to znamená popsat všechny přímky obsažené v rovině $p^\perp$. To je ale jednoduché – jejich směrové vektory jsou právě všechny nenulové prvky $p^\perp$. Pokud je p zadaná implicitně jako řešení soustavy $\alpha(v) = \beta(v) = 0$ dvou rovnic, je $p^\perp = [\alpha, \beta]$ a přímka ležící v $p^\perp$ je proto generovaná libovolnou jejich nenulovou lineární kombinací $a\alpha + b\beta$. Přechodem zpátky vidíme, že rovnice odpovídající roviny obsahující p je $(a\alpha + b\beta)(v) = 0$, ve výsledku tedy libovolná nenulová lineární kombinace definujících rovin přímky p.

Dalším vztahem mezi podprostory V a V^* je ten mezi implicitním a parametrickým popisem. Nechť je podprostor $W \subseteq V^*$ zadán parametricky jako $W = [\eta^1, \ldots, \eta^k]$. Potom

$$W^\perp = \{v \in V \mid \forall \eta \in W : (\eta, v) = 0\}.$$

Protože je však W popsán parametricky, stačí podmínky zkontrolovat na generátorech,

$$W^\perp = \{v \in V \mid (\eta^1, v) = \cdots = (\eta^k, v) = 0\}.$$

To je ale popis $W^\perp$ jako prostoru řešení soustavy lineárních rovnic $\eta^1(v) = 0, \ldots, \eta^k(v) = 0$, tedy implicitní popis. Stejný princip funguje naopak. Je-li $U = [v_1, \ldots, v_d]$, pak

$$U^\perp = \{\eta \in V^* \mid (\eta, v_1) = \cdots = (\eta, v_d) = 0.\}$$

Formálně tak převod parametrického popisu na implicitní je elementární. Parametrický popis U je ekvivalentní implicitnímu popisu $U^\perp$, ten lze pomocí vyřešení soustavy s parametry převést na parametrický popis, který je zpětně ekvivalentní implicitnímu popisu U.

Tvrzení 3.2. *Nechť jsou na V zadány formy $\eta^0, \eta^1, \dots, \eta^k$. Jestliže libovolné $v \in V$ splňující*

$$\eta^1(v) = \dots = \eta^k(v) = 0$$

splňuje zároveň $\eta^0(v) = 0$, pak $\eta^0 \in [\eta^1, \dots, \eta^k]$.

Poznámka. Opačná implikace je triviální: je-li $\eta^0 \in [\eta^1, \dots, \eta^k]$, pak z $\eta^1(v) = \cdots \eta^k(v) = 0$ plyne jednoduše $\eta^0(v) = 0$.

V případě implikace $(\eta^1(v) = \cdots = \eta^k(v) = 0) \Rightarrow (\eta^0(v) = 0)$ můžeme mluvit o tom, že rovnice $\eta^0(v) = 0$ je logickým důsledkem zmíněné soustavy. Věta tedy říká, že pokud je $\eta^0(v) = 0$ logickým důsledkem, je ve skutečnosti "algebraickým" důsledkem; lze odvodit ze soustavy tím nejtriviálnějším možným způsobem – je kombinací rovnic soustavy. V jistém smyslu se jedná o úplnost jistého logického systému: implikace, které platí, jsou právě ty, které lze dokázat (pomocí zmíněného jednoduchého pravidla).

Důkaz. Implikaci lze vyjádřit jako

$$[\eta^0, \eta^1, \dots, \eta^k]^\perp = [\eta^1, \dots, \eta^k]^\perp.$$

Druhou aplikací D_V dostáváme $[\eta^0, \eta^1, \dots, \eta^k] = [\eta^1, \dots, \eta^k]$ a zejména $\eta^0 \in [\eta^1, \dots, \eta^k]$. □

Následující tvrzení je dobře známe z teorie řešení soustavy lineárních rovnic a lze jej vyvodit z Gaussovy eliminační metody. Uvádíme zde alternativní důkaz pomocí duality.

Tvrzení 3.3. *Soustava rovnic $Ax+b = 0$ nemá řešení, právě když existuje lineární kombinace jejích řádků (tedy rovnic) tvaru $1 = 0$.*

Důkaz. Trik spočívá v "projektivizaci" soustavy. Původní soustava nemá řešení, právě když každé řešení soustavy $Ax + bt = 0$ splňuje také $t = 0$. Podle předchozího tvrzení to nastane právě když forma zadaná řádkem $(0, \dots, 0, 1)$ je lineární kombinací řádků rozšířené matice $(A \,|\, b)$. □

Poznámka. Obecné vyjádření duality: $(-,-)\colon U \times V \to \mathbb{K}$ bilineární zobrazení takové, že $U \to V^*$, $u \mapsto (u, -)$ a $V \to U^*$, $v \mapsto (-, v)$ jsou izomorfismy. Tenzorový přístup: existují $\varepsilon\colon U \otimes V \to \mathbb{K}$ a $\delta\colon \mathbb{K} \to V \otimes U$ takové, že $V \xrightarrow{\delta\otimes\mathrm{id}} V \otimes U \otimes V \xrightarrow{\mathrm{id}\otimes\varepsilon} V$ a $U \xrightarrow{\mathrm{id}\otimes\delta} U \otimes V \otimes U \xrightarrow{\varepsilon\otimes\mathrm{id}} U$ jsou identická zobrazení.

4. Něco málo k tenzorovému součinu

Pointa tenzorového součinu je, že chceme převést bilineární zobrazení na lineární. Konkrétně bilineární zobrazení $U \times V \to W$ bude ekvivalentní lineárnímu zobrazení $U \otimes V \to W$. Symbolicky

$$\mathrm{Lin}_2(U, V; W) \cong \mathrm{Hom}(U \otimes V, W),$$

kde však pro úplnost říkáme víc než v předchozím – vyžadujeme, aby se jednalo o izomorfismus vektorových prostorů (a ne jen o bijekci). Tímto vztahem je tenzorový součin určen jednoznačně až na izomorfismus a ve většině aplikací není potřeba znát přesnou definici a vystačíme si s touto vlastností. Pokusme se s její pomocí "odvodit" definici tenzorového součinu. Dosaďme do uvedeného vztahu $W = \Bbbk$. Dostáváme

$$\mathrm{Lin}_2(U, V; \Bbbk) \cong (U \otimes V)^*.$$

Budeme-li nyní předpokládat, že má $U \otimes V$ konečnou dimenzi, lze psát

$$U \otimes V \cong \mathrm{Lin}_2(U, V; \Bbbk)^*$$

Chceme-li tedy dostát tomu, že tenzorový součin převádí bilineární zobrazení na lineární, jsme vedeni k následujícímu:

Definice 4.1. Nechť U a V jsou vektorové prostory konečné dimenze. Definujeme jejich *tenzorový součin* $U \otimes V \stackrel{\text{def}}{=} \mathrm{Lin}_2(U, V; \Bbbk)^*$.

Definujme nyní bilineární zobrazení $t : U \times V \to U \otimes V$ předpisem

$$t(u, v) : \Phi \mapsto \Phi(u, v),$$

jedná se tedy o "evaluaci" (viz srovnání druhého duálu s původním vektorovým prostorem). V následujícím budeme značit $u \otimes v = t(u, v)$ a je to tedy zobrazení, které každou bilineární formu posílá na její hodnotu na dvojici (u, v).

Lemma 4.2. *Zobrazení t je bilineární, tj.*

$$(a_1 u_1 + a_2 u_2) \otimes v = a_1 \cdot u_1 \otimes v + a_2 \cdot u_2 \otimes v$$

a analogicky pro druhou složku.

Důkaz. Levá strana je dána evaluací

$$\Phi \mapsto \Phi(a_1 u_1 + a_2 u_2, v),$$

zatímco pravá je dána jako lineární kombinace evaluací, tedy

$$\Phi \mapsto a_1 \Phi(u_1, v) + a_2 \Phi(u_2, v).$$

Tyto dva výrazy se rovnají díky bilinearitě Φ. □

Věta 4.3. *Nechť vektory $\{e_i \mid i = 1, \ldots, n\}$, tvoří bázi prostoru U a vektory $\{\widetilde{e}_j \mid j = 1, \ldots, m\}$, tvoří bázi prostoru V. Pak vektory $\{e_i \otimes \widetilde{e}_j \mid i = 1, \ldots, n; j = 1, \ldots, m\}$, tvoří bázi prostoru $U \otimes V$.*

Poznámka. Při práci s tenzorovým součinem je výhodnější se vzdát uspořádání prvků báze a pracovat s neuspořádanými bázemi. V dalším budeme zkracovat na "$\{e_i\}$ je báze U".

Před tím, než budeme moct dokázat předchozí větu, je dobré popsat bázi prostoru všech bilineárních forem. Nechť tedy máme báze jako ze znění věty a k nim duální báze f^i a $\widetilde{f}^j$. Definujme bilineární formu

$$f^i \cdot \widetilde{f}^j : U \times V \to \Bbbk, \qquad (u, v) \mapsto f^i(u) \widetilde{f}^j(v)$$

(součin funkčních hodnot – prvků tělesa $\Bbbk$). Prvně dokážeme

Lemma 4.4. *Množina $\{f^i \cdot \widetilde{f}^j\}$ tvoří bázi $\mathrm{Lin}_2(U, V; \Bbbk)$.*

Důkaz. Pointou důkazu je, že dvě bilineární formy se rovnají, právě když dávají stejné hodnoty na všech dvojicích $(e_r, \widetilde{e}_s)$ bázových vektorů. Pokusme se napsat bilineární formu Φ jako kombinaci

$$\Phi = \sum_{i,j} \Phi_{ij} \cdot (f^i \cdot \widetilde{f}^j).$$

Tato rovnost bude podle předchozího splněna, právě když pro každé r, s bude platit

$$\Phi(e_r, \widetilde{e}_s) = \sum_{i,j} \Phi_{ij} \cdot (f^i \cdot \widetilde{f}^j)(e_r, \widetilde{e}_s) = \sum_{i,j} \Phi_{ij} \underbrace{f^i(e_r)}_{\delta^i_r} \underbrace{\widetilde{f}^j(\widetilde{e}_s)}_{\delta^j_s} = \Phi_{rs}.$$

Je tedy vidět, že koeficienty existují a to jediné, $\Phi_{rs} = \Phi(e_r, \widetilde{e}_s)$. To ale přesně znamená, že daná množina je báze. □

Důkaz Věty 4.3. Ukážeme nyní, že $\{e_i \otimes \widetilde{e}_j\}$ tvoří duální bázi k bázi $\{f^i \cdot \widetilde{f}^j\}$ z lemmatu. Stačí tedy počítat

$$(e_i \otimes \widetilde{e}_j)(f^r \cdot \widetilde{f}^s) = (f^r \cdot \widetilde{f}^s)(e_i, \widetilde{e}_j) = f^r(e_i)\widetilde{f}^s(\widetilde{e}_j) = \delta^r_i \delta^s_j,$$

což je 0 s vyjímkou případu $i = r$, $j = s$. To je ale přesně podmínka na duální bázi. □

Vraťme se nyní ke vztahu, který jsme použili k motivaci definice tenzorového součinu a ověřme, že opravdu platí. Připomeňme kanonické zobrazení $t : U \times V \to U \otimes V$ dané $(u, v) \mapsto u \otimes v$.

Věta 4.5. *Existují přirozené izomorfismy*

$$\mathrm{Hom}(U \otimes V, W) \xrightarrow{\cong} \mathrm{Lin}_2(U, V; W) \xleftarrow{\cong} \mathrm{Hom}(U, \mathrm{Hom}(V, W)),$$

první z nichž je dán $\varphi \mapsto \varphi \circ t$.

Důkaz. První izomorfismus je zjevně lineární zobrazení a jedná se o bijekci podle univerzální vlastnosti tenzorového součinu. Druhé zobrazení posílá $f : U \to \mathrm{Hom}(V, W)$ na

$$(u, v) \mapsto f(u)(v).$$

Je to přesně zobrazení zprostředkující bijekci $(W^V)^U \cong W^{U \times V}$, kterou znáte z diskrétní matematiky, jenom je zúžené na vhodně lineární zobrazení. Jeho inverze posílá $g : U \times V \to W$ na $u \mapsto g(u, -)$, kde $g(u, -)$ je "parciální zobrazení" $v \mapsto g(u, v)$. □

Tvrzení 4.6. *Zobrazení*

$$U^* \otimes V^* \to \mathrm{Lin}_2(U, V; \Bbbk) \cong (U \otimes V)^*$$

dané předpisem $\eta \otimes \theta \mapsto \eta \cdot \theta$ je izomorfismus.

Důkaz. Zobrazení převádí bázi $f^i \otimes \widetilde{f}^j$ na bázi $f^i \cdot \widetilde{f}^j$. □

Poznámka. Striktně vzato by bylo logičtější psát $V^* \otimes U^* \cong (U \otimes V)^*$.

Jakožto zobrazení $U \otimes V \to \Bbbk$ je obraz $\eta \otimes \theta$ dán předpisem $u \otimes v \mapsto \eta(u) \cdot \theta(v)$ a lze jej tedy popsat jako kompozici

$$U \otimes V \xrightarrow{\eta \otimes \theta} \Bbbk \otimes \Bbbk \cong \Bbbk,$$

kde přirozený izomorfismus $\Bbbk \otimes \Bbbk \cong \Bbbk$ je dán předpisem $a \otimes b \mapsto ab$.

V dalším budeme potřebovat analogii předchozího tvrzení pro antisymetrické tenzory. Z technických důvodů změníme předchozí zobrazení vynásobením konstantou $q!$.

Tvrzení 4.7. *Zobrazení $\Lambda^q V^* \to \mathrm{Lin}_q(V, \dots, V; \Bbbk)_{\mathrm{antisym}}$ dané předpisem*

$$\eta^1 \wedge \cdots \wedge \eta^q \mapsto \sum_{\sigma \in \Sigma_q} \mathrm{sign}\, \sigma \cdot \eta^{\sigma(1)} \cdots \eta^{\sigma(q)}$$

je izomorfismus.

Důkaz. Prvně se zabývejme tím, jaký efekt na multilineární formu příslušnou tenzoru $t \in (V^*)^{\otimes q}$ má permutace σ:

$$\begin{aligned}(\rho_\sigma(\eta^1 \otimes \cdots \otimes \eta^q))(v_1, \ldots, v_q) &= (\eta^{\sigma(1)} \otimes \cdots \otimes \eta^{\sigma(q)})(v_1, \ldots, v_q) \\ &= \eta^{\sigma(1)}(v_1) \cdot \cdots \cdot \eta^{\sigma(q)}(v_q) = \eta^1(v_{\sigma^{-1}(1)}) \cdot \cdots \cdot \eta^q(v_{\sigma^{-1}(q)}) \\ &= (\eta^1 \otimes \cdots \otimes \eta^q)(v_{\sigma^{-1}(1)}, \ldots, v_{\sigma^{-1}(q)})\end{aligned}$$

Proto obecně platí $(\rho_\sigma t)(v_1, \ldots, v_q) = t(v_{\sigma^{-1}(1)}, \ldots, v_{\sigma^{-1}(q)})$ a zejména t je antisymetrický, právě když je antisymetrická příslušná multilineární forma. Proto se izomorfismus z předchozího tvrzení zúží na izomorfismus $\Lambda^q V^*$ s podprostorem antisymetrických q-lineárních forem. Vynásobení číslem $q!$ na tom nic nezmění. □

Vysvětleme nyní, proč je vynásobení číslem $q!$ výhodné. Je to proto, že platí

$$(f^{i_1} \wedge \cdots \wedge f^{i_q})(e_{i_1}, \ldots, e_{i_q}) = 1.$$

To se nám bude hodit v příští kapitole. Uveďme nyní ještě verzi věty o determinantu pro antisymetrické multilineární formy. Je-li $\varphi : U \to U$ lineární zobrazení, platí

$$\begin{aligned}((\varphi^*)^{\otimes n}(\eta^1 \otimes \cdots \otimes \eta^n))(u_1, \ldots, u_n) &= (\varphi^*\eta^1 \otimes \cdots \otimes \varphi^*\eta^n)(u_1, \ldots, u_n) \\ &= (\varphi^*\eta^1)(u_1) \cdot \cdots \cdot (\varphi^*\eta^n)(u_n) = \eta^1(\varphi(u_1)) \cdot \cdots \cdot \eta^n(\varphi(u_n)) \\ &= (\eta^1 \otimes \cdots \otimes \eta^n)(\varphi(u_1), \ldots, \varphi(u_n))\end{aligned}$$

a stejný vztah tedy platí i pro antisymetrické n-lineární formy,

$$\omega(\varphi(u_1), \ldots, \varphi(u_n)) = ((\varphi^*)^{\wedge n}\omega)(u_1, \ldots, u_n) = \det\varphi \cdot \omega(u_1, \ldots, u_n),$$

(jelikož samozřejmě platí $\det\varphi^* = \det\varphi$).

Poznámka. Zatímco vložení $\Lambda^q U \to U^{\otimes q}$ není homomorfismus algeber, existuje kanonický homomorfismus $U^{\otimes q} \to \Lambda^q U$, který na abstraktní úrovni posílá $u_1 \otimes \cdots \otimes u_q \mapsto u_1 \wedge \cdots \wedge u_q$ (tady je lépe uvažovat o $\Lambda^q U$ jako o abstraktním prostoru s vlastností $\mathrm{Hom}(\Lambda^q U, V) \cong \mathrm{Lin}_q(U, \ldots, U; V)_{\mathrm{antisym}}$ – antisymetrizace je pak duální k inkluzi antisymetrických zobrazení do všech zobrazení; konkrétní realizace pro U konečné dimenze je $\Lambda^q U = \mathrm{Lin}_q(U, \ldots, U; \mathbb{K})^*_{\mathrm{antisym}}$). Popíšeme nyní vztah vnější mocniny a antisymetrických tenzorů: uvažme evaluaci

$$\mathrm{ev}\colon (U^{\otimes q})^* \otimes U^{\otimes q} \to \mathbb{K}$$

a zužme ji na antisymetrické formy $(\Lambda^q U)^* \cong \mathrm{Lin}_q(U, \ldots, U; \mathbb{K})_{\mathrm{antisym}} \subseteq \mathrm{Lin}_q(U, \ldots, U; \mathbb{K}) \cong (U^{\otimes q})^*$. Díky antisymetrii se pak toto zúžení faktorizuje skrz

$$\mathrm{ev}\colon (\Lambda^q U)^* \otimes \Lambda^q U \to \mathbb{K}$$

které je dualitou. Přitom duální bázový prvek k $e_{i_1} \wedge \cdots \wedge e_{i_q}$ je $q!A(f^{i_1} \otimes \cdots \otimes f^{i_q})$ (nebo $q!A(f^{i_q} \otimes \cdots \otimes f^{i_1})$ pro logičtější verzi Tvrzení 4.6). Budeme proto používat ztotožnění $\Lambda^q U^* \cong (\Lambda^q U)^*$, $f^{i_1} \wedge \cdots \wedge f^{i_q} = q!A(f^{i_1} \otimes \cdots \otimes f^{i_q})$, které respektuje kanonické báze obou prostorů.

5. Determinanty, objemy a orientace

Nechť U je vektorový prostor dimenze n. Potom vnější mocnina $\Lambda^n U^*$ má dimenzi 1 a v dalším ji budeme ztotožňovat s prostorem všech antisymetrických n-lineárních forem na U. Libovolný její nenulový prvek (nutně tedy generátor) nazýváme *objemovou formou* na U a značíme jej

$$\mathrm{Vol} \in \mathrm{Lin}_n(U, \ldots, U; \mathbb{R})_{\mathrm{antisym}}.$$

Jeho hodnotu na vektorech $u_1, \dots, u_n$ nazýváme *orientovaným objemem* rovnoběžnostěnu určeného těmito vektory. Díky objemové formě můžeme interpretovat determinant operátoru $\varphi : U \to U$. Jeho vnější mocnina

$$(\varphi^*)^{\wedge n} : \Lambda^n U^* \to \Lambda^n U^*$$

totiž posílá Vol na nějaký násobek Vol a z části o vnějších mocninách víme, že je to právě

$$\mathrm{Vol}(\varphi(u_1), \dots, \varphi(u_n)) = (\det \varphi) \cdot \mathrm{Vol}(u_1, \dots, u_n).$$

Znamená to tedy, že operátor φ zvětšuje objem právě $(\det \varphi)$-krát. Tato vlastnost nezávisí na volbě objemové formy – podstatné je, že se jedná o "relativní tvrzení", tedy neříkáme nic o tom, jaký je výsledný objem, ale pouze ho porovnáváme s původním. Pokud bychom však chtěli definovat determinant lineárního zobrazení mezi dvěma různými vektorovými prostory (stejné dimenze), museli bychom na nich zafixovat objemové formy.

Souvisejícím pojmem je orientace *reálného* vektorového prostoru U. Řekneme, že dvě báze $(e_1, \dots, e_n)$ a $(\widetilde{e}_1, \dots, \widetilde{e}_n)$ jsou *shodně orientované*, jestliže platí

$$\widetilde{e}_1 \wedge \cdots \wedge \widetilde{e}_n = c \cdot (e_1 \wedge \cdots \wedge e_n)$$

pro nějaké kladné $c \in \mathbb{R}$. Konstanta c je tímto vztahem samozřejmě jednoznačně určena – jedná se o determinant matice přechodu od první báze k druhé – a je tedy nenulová. Pro c záporné mluvíme o *opačně orientovaných* bázích. Takto nám na množině všech bází vzniká relace ekvivalence mající právě dvě třídy, které nazýváme *orientace* U. Pokud je na U zvolena orientace, říkáme, že je U *orientovaný* a prvky vybrané orientace nazýváme *kladné báze*, zatímco zbylé jsou *záporné báze*.

Příklad 5.1. Na $\mathbb{R}^n$ definujme standardní orientaci jako třídu bází obsahující standardní bázi $(e_1, \dots, e_n)$.

Příklad 5.2. Nechť V je komplexní vektorový prostor a $V^{\mathbb{R}}$ značí reálný vektorový prostor s touž nosnou množinou, týmž sčítáním, ale s násobením skaláry zúženém na reálná čísla; mluvíme o realifikaci V. Na $V^{\mathbb{R}}$ existuje kanonická orientace (závisející samozřejmě na komplexní struktuře), kterou nyní popíšeme. Zvolme libovolnou bázi $(e_1, \dots, e_n)$ komplexního prostoru V. Potom

$$(e_1, ie_1, \dots, e_n, ie_n)$$

je báze reálného prostoru $V^{\mathbb{R}}$ a prohlásíme ji za kladnou bázi. Je potřeba ukázat, že pro jinou volbu komplexní báze bude vzniklá reálná báze shodně orientovaná a tím pádem dostáváme opravdu dobře definovanou orientaci.

Matice přechodu mezi dvěma komplexními bázemi je však libovolná invertibilní komplexní matice a musíme tedy ukázat, že reálná matice příslušná libovolné invertibilní matici má kladný determinant. Rozložme komplexní matici přechodu na součin elementárních matic. Příslušná matice přechodu mezi reálnými bázemi je tak opět součinem jistých "elementárních" matic. Přičítání (komplexního) násobku dá matici determinantu 1, prohození dvou řádků taktéž (příslušná reálná matice odpovídá prohození dvou dvojic řádků). Násobení komplexním číslem má příslušnou reálnou matici vzniklou z jednotkové výměnou dvou jedniček za blok

$$\begin{pmatrix} a & -b \\ b & a \end{pmatrix},$$

který má determinant $a^2 + b^2 > 0$.

Vraťme se nyní k obecné situaci reálného vektorového prostoru U.

Věta 5.3. *Dvě báze α, β jsou shodně orientované, právě když je lze spojit cestou, tj. právě když existuje spojité zobrazení*

$$\gamma : [0,1] \to U \times \cdots \times U = U^n$$

splňující následující

- $\gamma(0) = \alpha$, $\gamma(1) = \beta$ *a*
- *pro každé* $t \in [0,1]$ *je n-tice* $\gamma(t)$ *bází* U.

Poznámka. Spojitost jistě dává smysl pro $U = \mathbb{R}^n$. Avšak libovolný (konečně rozměrný) reálný vektorový prostor je izomorfní $\mathbb{R}^n$ a spojitost lze definovat ve smyslu tohoto izomorfismu – hlavně na volbě takového izomorfismu nezávisí.

Důkaz. Není těžké se přesvědčit, že každou čtvercovou matici s *kladným* determinantem lze napsat jako součin elementárních s kladným determinantem. Prohození dvou sloupců lze nahradit kompozicí operací $I \to I + II$, $II \to II - I$, $I \to I + II$, která samozřejmě zároveň s prohozením sloupců také jeden z nich vynásobí číslem -1, ale Gaussova eliminace lze provádět i s touto operací. Vynásobení dvou sloupců číslem -1 lze nahradit provedením dvou předchozích složených operací za sebou.

Dále není těžké se přesvědčit, že každá z elementárních matic T_i s kladným determinantem lze spojit s jednotkovou maticí E cestou Γ_i procházející pouze maticemi s kladným determinantem. Jejich součin $T = T_1 \cdots T_k$ pak lze spojit s jednotkovou maticí jednoduše pomocí cesty

$$t \mapsto \Gamma_1(t) \cdots \Gamma_k(t).$$

Jelikož však platí

$$\alpha = \beta \cdot T,$$

hledaná cesta mezi bázemi α, β lze volit například jako

$$t \mapsto \beta \cdot \Gamma_1(t) \cdots \Gamma_k(t).$$

V opačném směru veličina $(\det \mathrm{id}_{\gamma(t)\alpha}) \in \mathbb{R}^\times$ závisí spojitě na t a její hodnota pro $t = 0$ je 1. Proto i její hodnota pro $t = 1$ musí být kladná, tj. $(\det \mathrm{id}_{\beta\alpha}) > 0$ a báze α, β jsou shodně orientované. □

Důležitým příkladem objemové formy je objemová forma vzniklá ze skalárního součinu na *orientovaném* Eukleidovském prostoru $\mathcal{E}$. To by nemělo být překvapující – skalární součin na $\mathcal{E}$ udává smysl velikosti vektorů a úhlů mezi nimi; z těchto údajů lze objem spočítat. Objemová forma však udává orientovaný objem, proto je navíc potřeba ještě volba orientace. Z jiného úhlu pohledu na Eukleidovském prostoru jsou dvě objemové formy a není žádný důvod preferovat jednu z nich; ten nastává až při zafixování orientace. Pro neorientovaný Eukleidovský prostor bychom mohli nadefinovat pouze neorientovanou objemovou "formu" $|\operatorname{Vol}|$; k ní se vrátíme za chvíli.

Nechť $(e_1, \ldots, e_n)$ je libovolná kladně orientovaná ortonormální báze. Kanonickou objemovou formu zafixujeme požadavkem

$$\operatorname{Vol}(e_1, \ldots, e_n) = 1.$$

Je-li $(f^1, \ldots, f^n)$ duální báze, pak platí

$$(f^1 \wedge \cdots \wedge f^n)(e_1, \ldots, e_n) = \sum_{\sigma \in \Sigma_n} \operatorname{sign} \sigma \cdot f^{\sigma(1)}(e_1) \cdots f^{\sigma(n)}(e_n) = 1,$$

neboť jediný nenulový člen se objevuje pro $\sigma = \mathrm{id}$. Lze tedy položit

$$\mathrm{Vol} = f^1 \wedge \cdots \wedge f^n.$$

Z tohoto vztahu lze vidět, že objemová forma nezávisí na volbě kladné ortonormální báze – matice přechodu mezi dvěma ortonormálními bázemi je ortogonální a má tedy determinant ± 1; pokud jsou báze navíc kladné, musí být roven 1 a to stejné platí pro determinant matice přechodu mezi duálními bázemi (je totiž stejný). Ve výsledku pro jinou volbu báze $(\widetilde{e}_1, \ldots, \widetilde{e}_n)$ a k ní duální $(\widetilde{f}^1, \ldots, \widetilde{f}^n)$ platí

$$\mathrm{Vol} = f^1 \wedge \cdots \wedge f^n = \widetilde{f}^1 \wedge \cdots \wedge \widetilde{f}^n.$$

Pro orientovaný objem platí vztah

$$\mathrm{Vol}(u_1, \ldots, u_n) = \sum_{\sigma \in \Sigma_n} \operatorname{sign} \sigma \cdot f^{\sigma(1)}(u_1) \cdots f^{\sigma(n)}(u_n) = \det \begin{pmatrix} f^1(u_1) & \cdots & f^1(u_n) \\ \vdots & & \vdots \\ f^n(u_1) & \cdots & f^n(u_n) \end{pmatrix}$$

Jelikož $f^i(u_j)$ je i-tá souřadnice vektoru u_j, můžeme výpočet shrnout v následujícím.

Tvrzení 5.4. *Orientovaný objem* $\mathrm{Vol}(u_1, \ldots, u_n)$ *lze spočítat jako determinant matice, jejíž* j*-tý sloupec je tvořen souřadnicemi vektoru* u_j *v libovolné kladné ortonormální bázi (ta však musí být stejná pro všechny sloupce).*

Jeho druhou mocninu lze spočítat jako Gramův determinant

$$(\mathrm{Vol}(u_1, \ldots, u_n))^2 = \det(\langle u_i, u_j \rangle)$$

z matice, jejíž prvek na pozici (i, j) *je skalární součin* $\langle u_i, u_j \rangle$*.*

Důkaz. Druhé tvrzení plyne z prvního vynásobením popsaných matice zleva maticí k ní transponovanou. Na pozici (i, j) dostaneme součin i-tého a j-tého sloupce, tedy

$$\sum_k f^k(u_i) f^k(u_j) = \langle u_i, u_j \rangle$$

(jedná se o vzorec pro skalární součin v ortonormálních souřadnicích). □

Jako důsledek dostáváme vzorec pro neorientovaný objem na Eukleidovském prostoru jako odmocninu z Gramova determinantu – ten závisí pouze na skalárním součinu a nikoliv na orientaci. Z tohoto pohledu lze interpretovat Gramův-Schmidtův ortogonalizační proces jako vzorec pro objem. Během něj totiž měníme každý vektor pouze přičítáním násobků předchozích vektorů a nemění se tedy orientovaný objem. Přitom po provedení celého procesu a pro vzniklý ortogonální systém $(v_1, \ldots, v_n)$ je Gramova matice diagonální a neorientovaný objem je tak roven

$$|\mathrm{Vol}(u_1, \ldots, u_n)| = |v_1| \cdots |v_n|,$$

součinu velikostí vektorů $v_1, \ldots, v_n$. Znaménko je též jako u původního orientovaného objemu a je tedy určeno tím, zda je $(u_1, \ldots, u_n)$ báze kladná či záporná (v případě, že se nejedná vůbec o bázi, je objem beztak nulový). Přitom velikost vektoru v_i je rovna výšce rovnoběžnostěnu určeného $u_1, \ldots, u_i$ s podstavou danou prvními $i - 1$ vektory. Jedná se tedy o vzorec

$$\text{objem rovnoběžnostěnu} = \text{objem postavy} \times \text{výška}$$

Hlavní význam této formulky je v tom, že po několika stránkách je snad konečně zřejmé, proč tomuto objektu říkáme orientovaný objem.

6. Geometrie v rovině a prostoru

Prvně se zabývejme rovinou $\mathcal{E}_2$, kterou budeme chápat jako $\mathbb{R}^2$ se standardním skalárním součinem a standardní orientací. Ta je mimochodem totožná s tou vzniklou z komplexní struktury na $\mathbb{C} = \mathbb{R}^2$.

Pro vektory $u, v \in \mathcal{E}_2$ počítejme neorientovaný objem z Gramova determinantu

$$(\mathrm{Vol}(u,v))^2 = \begin{vmatrix} \langle u,u\rangle & \langle u,v\rangle \\ \langle v,u\rangle & \langle v,v\rangle \end{vmatrix} = |u|^2|v|^2 - \langle u,v\rangle^2 = |u|^2|v|^2 \sin^2\alpha,$$

kde α je úhel mezi vektory u, v a rovnost plyne z $\langle u,v\rangle = |u||v|\cos\alpha$. Odmocněním dostáváme vztah

$$|\,\mathrm{Vol}(u,v)| = |u||v||\sin\alpha|.$$

Standardně bereme $\alpha \in [0,\pi]$, díky orientaci můžeme nyní rozšířit definiční obor na $\alpha \in (-\pi,\pi]$ a zvolit znaménko podle orientace (u,v). Mluvíme pak o *orientovaném úhlu* od vektoru u k vektoru v a můžeme psát

$$\begin{vmatrix} u^1 & v^1 \\ u^2 & v^2 \end{vmatrix} = \mathrm{Vol}(u,v) = |u||v|\sin\alpha.$$

Budeme psát $\alpha = \sphericalangle(u,v)$.

Orientovaný úhel se hodí v úlohách, ve kterých je potřeba (zejména algoritmicky) rozhodnout o viditelnosti objektů v rovině. Dalším případem je úloha rozhodnout, zda mnohoúhelník $A_1\cdots A_n$ zadaný posloupností vrcholů je kladně či záporně orientovaný (v případě, že nevíme, zda je konvexní). Velice jednoduchým způsobem (alespoň z teoretického pohledu) je spočítat všechny orientované úhly

$$\sphericalangle(A_nA_1, A_1A_2), \sphericalangle(A_1A_2, A_2A_3), \ldots, \sphericalangle(A_{n-1}A_n, A_nA_1)$$

podél mnohoúhelníka a sečíst je. Pokud je součet roven 2π, je mnohoúhelník kladně orientovaný, pokud -2π, je záporně orientovaný. Ostatní případy nemohou pro mnohoúhelník nastat a lze takto i detekovat některé případy, kdy se nejedná o mnohoúhelník (zdaleka ne však všechny). V případě, kdy je mnohoúhelník konvexní, budou mít všechny úhly stejné znaménko a to lze spočítat pomocí orientovaného objemu (u čtyřúhelníku stačí spočítat znaménka i v nekonvexním případě). Jiným řešením je sečíst orientované objemy

$$\tfrac{1}{2}\,\mathrm{Vol}(A_1A_2, A_1A_3) + \cdots + \tfrac{1}{2}\,\mathrm{Vol}(A_1A_{n-1}, A_1A_n).$$

Pokud je výsledek kladný, je mnohoúhelník kladně orientovaný a naopak.

Příklad 6.1. Ukažme nyní, že výše uvedený součet vyjadřuje obsah mnohoúhelníku $A_1\cdots A_n$. V prvním kroku dokážeme o něco obecněji, že součet

$$\mathrm{Vol}(XA_1, XA_2) + \cdots + \mathrm{Vol}(XA_{n-1}, XA_n) + \mathrm{Vol}(XA_n, XA_1)$$

nezávisí na volbě bodu X. To je tím, že

$$\begin{aligned}\mathrm{Vol}(YA_i, YA_{i+1}) &= \mathrm{Vol}(YX + XA_i, YX + XA_{i+1}) \\ &= \mathrm{Vol}(XA_i, XA_{i+1}) + \mathrm{Vol}(YX, XA_{i+1}) + \mathrm{Vol}(XA_i, YX),\end{aligned}$$

kde členy $\mathrm{Vol}(YX, XA_{i+1})$ se při sečtení vyruší se členy $\mathrm{Vol}(XA_i, YX) = -\mathrm{Vol}(YX, XA_i)$.

V dalším kroku ukážeme, že existuje vnitřní diagonála A_iA_j, která protíná mnohoúhelník pouze v koncových bodech. Pak lze induktivně předpokládat, že vzorec pro obsah funguje pro oba mnohoúhelníky vzniklé rozdělením podél A_iA_j a jejich sečtením dokázat, že tento vzorec funguje také pro náš mnohoúhelník. Nechť A_i je bod s nejmenší x-ovou souřadnicí. Pokud

leží uvnitř trojúhelníku $A_{i-1}A_iA_{i+1}$ nějaký další vrchol mnohoúhelníku, zvolíme za A_j ten s nejmenší x-ovou souřadnicí. Pokud ne, zvolíme za dělící diagonálu $A_{i-1}A_{i+1}$.

Poznámka. Orientovaná Eukleidovská rovina[2] je kanonicky (jednorozměrným) komplexním vektorovým prostorem: izomorfismus $\mathbb{C} \to V$ je zadán tím, že posílá $1 \mapsto e_1$ a $i \mapsto e_2$, kde (e_1, e_2) je libovolná kladně orientovaná ortonormální báze. Jiná volba se liší o matici z $\mathrm{SO}(2) = \mathrm{U}(1)$ a proto je komplexní struktura jednoznačná. Tím lze také definovat orientovaný úhel mezi nenulovými vektory u, v jako $\sphericalangle(u, v) = \arg(v/u)$ — je totiž $v = z \cdot u$ pro jediné komplexní číslo z, jehož argument je přesně onen orientovaný úhel.

Neorientovaná rovina má dvě komplexní struktury, které se navzájem liší o komplexní konjugaci. Ve výsledku je tak úhel jednoznačný až na znaménko.

Přejděme nyní ke standardnímu orientovanému Eukleidovskému třírozměrnému prostoru $\mathcal{E}_3$. Krom skalárního součinu lze na $\mathcal{E}_3$ definovat vektorový součin pomocí objemové formy. Po dosazení dvou vektorů $u, v \in \mathcal{E}_3$ se z objemové formy stane lineární forma

$$\mathrm{Vol}(u, v, -) : \mathcal{E}_3 \to \mathbb{R}.$$

Každá lineární forma je rovna skalárnímu součinu s jednoznačně určeným vektorem, který v tomto případě značíme $u \times v$. Je tedy definován vztahem

$$\mathrm{Vol}(u, v, w) = \langle u \times v, w \rangle.$$

V kladné ortonormální bázi lze vektorový součin spočítat jako

$$\langle u \times v, w \rangle = \begin{vmatrix} u^1 & v^1 & w^1 \\ u^2 & v^2 & w^2 \\ u^3 & v^3 & w^3 \end{vmatrix} = \begin{vmatrix} u^1 & v^1 & \langle e_1, w \rangle \\ u^2 & v^2 & \langle e_2, w \rangle \\ u^3 & v^3 & \langle e_3, w \rangle \end{vmatrix} = \left\langle \begin{vmatrix} u^1 & v^1 & e_1 \\ u^2 & v^2 & e_2 \\ u^3 & v^3 & e_3 \end{vmatrix}, w \right\rangle,$$

kde determinant napravo sice nedává formálně smysl, pokud jej však rozvineme podle třetího sloupce, dostaneme korektní vzorec

$$u \times v = \begin{vmatrix} u^2 & v^2 \\ u^3 & v^3 \end{vmatrix} e_1 + \begin{vmatrix} u^3 & v^3 \\ u^1 & v^1 \end{vmatrix} e_2 + \begin{vmatrix} u^1 & v^1 \\ u^2 & v^2 \end{vmatrix} e_3.$$

Jeho korektnost plyne ze vztahu $(u \times v)^i = \langle u \times v, e_i \rangle = \mathrm{Vol}(u, v, e_i)$ pro souřadnice v ortonormální bázi.

Zabývejme se nyní abstraktními vlastnostmi vektorového součinu. Z antisymetrie platí

$$\langle u \times v, u \rangle = \mathrm{Vol}(u, v, u) = 0,$$

a proto je $u \times v$ kolmý na u a analogicky také na v. Tím je určen jeho směr, nyní určíme orientaci a na závěr jeho velikost. Orientace je dána tím, že

$$\mathrm{Vol}(u, v, u \times v) = \langle u \times v, u \times v \rangle \geq 0$$

a je tedy $(u, v, u \times v)$ kladně orientovaná (za předpokladu, že se jedná o bázi; v opačném případě však $u \times v = 0$ a jeho orientaci není potřeba určovat).

[2]Ve skutečnosti stačí mít skalární součin zadán až na násobek — takové struktuře se říká konformní; lze v ní měřit úhly a porovnávat velikosti. Typickým příkladem konformního zobrazení, které není ortogonální, je stejnolehlost.

Zbývá spočítat velikost $u \times v$. Pomocí Gramova determinantu

$$|u \times v|^2 = \langle u \times v, u \times v\rangle = \operatorname{Vol}(u, v, u \times v) = \begin{vmatrix} \langle u,u\rangle & \langle u,v\rangle & 0 \\ \langle v,u\rangle & \langle v,v\rangle & 0 \\ 0 & 0 & \langle u\times v, u\times v\rangle \end{vmatrix}^{1/2}$$
$$= \left(|u|^2|v|^2 - \langle u,v\rangle^2\right)^{1/2} \cdot |u \times v|$$

Pomocí úhlu α mezi vektory u, v dostáváme finální vztah

$$|u \times v| = |u||v| \sin\alpha.$$

Tentokrát není možné přiřadit úhlu α orientaci jako v rovinném případě.

Věta 6.2. *Vektorový součin má následující vlastnosti (které ho jednoznačně určují)*

- *Vektorový součin $- \times -$ je antisymetrické bilineární zobrazení.*
- *Vektor $u \times v$ je kolmý na u a v.*
- *Vektor $u \times v$ je nenulový, právě když jsou u, v lineárně nezávislé a pak*
- *báze $(u, v, u \times v)$ je kladně orientovaná.*
- *Platí $|u \times v| = |u||v| \sin \sphericalangle(u, v)$.*

7. Vztah kvaternionů a orientovaného objemu

Obecně můžeme říct, že objemová forma je *kompatibilní* se skalárním součinem, jestliže $|\operatorname{Vol}(u_1, \dots, u_n)| = |u_1| \cdots |u_n|$ kdykoliv $u_1, \dots, u_n$ tvoří ortonormální systém vektorů. Nad $\mathbb{R}$ je pak objemová forma Vol určena jednoznačně až na znaménko (orientaci), nad $\mathbb{C}$ jednoznačně až na násobek komplexní jednotkou. Jednoduchou modifikací ortonormální báze lze najít takovou ortonormální bázi, jejíž objem je roven 1. Standardní báze $\mathbb{R}^n$ a $\mathbb{C}^n$ jsou příklady takových bází.

Zabývejme se prvně krátce situací v reálné Eukleidovské rovině $\mathcal{E}_2$. Objemová forma je

$$\operatorname{Vol}\colon \mathcal{E}_2 \times \mathcal{E}_2 \to \mathbb{R},$$

kterou můžeme díky skalárnímu součinu přepsat jako

$$\operatorname{Vol}(u, v) = \langle Iu, v\rangle.$$

Protože je objemová forma kompatibilní se skalárním součinem, máme

$$\operatorname{Vol}(e_1, e_1) = 0, \qquad \operatorname{Vol}(e_1, e_2) = 1, \qquad \operatorname{Vol}(e_2, e_1) = -1, \qquad \operatorname{Vol}(e_2, e_2) = 0$$

a tedy $Ie_1 = e_2$, $Ie_2 = -e_1$. Díky tomu $I^2 = -\operatorname{id}$ a zobrazení I zadává na V strukturu komplexního vektorového prostoru: $v(a + bi) = va + I(vb)$ (samozřejmě, I je rotace o $90°$ v kladném směru).

Nyní se zabývejme stejnou situací v "komplexní Eukleidovské rovině" $\mathcal{E}_2$. Objemová forma je $\operatorname{Vol}\colon \mathcal{E}_2 \times \mathcal{E}_2 \to \mathbb{C}$, kterou můžeme díky skalárnímu součinu přepsat jako

$$\operatorname{Vol}(u, v) = \langle Ju, v\rangle.$$

Tentokrát je $J\colon \overline{\mathcal{E}_2} \to \mathcal{E}_2$ "konjugovaně lineární",

$$\langle J(u\alpha), v\rangle = \operatorname{Vol}(u\alpha, v) = \alpha \operatorname{Vol}(u, v) = \alpha\langle Ju, v\rangle = \langle (Ju)\overline{\alpha}, v\rangle,$$

tj. $J(u\alpha) = (Ju)\overline{\alpha}$. Z kompatibility se skalárním součinem $Je_1 = e_2$, $Je_2 = -e_1$ a proto $J^2 = -\operatorname{id}$ (druhá iterace už je lineární) a zobrazení J zadává na $\mathcal{E}_2$ strukturu kvaternionického vektorového prostoru: definujme kvaternionickou algebru $\mathbb{H}$ jako podalgebru generovanou I, $J \in \operatorname{Hom}_{\mathbb{R}}(V, V)$, kde $I = iE$ je násobení imaginární jednotkou i. Ukážeme, že

jako vektorový prostor je generovaná E, I, J, $K = IJ$: už víme, že platí $I^2 = J^2 = -E$, $IJ = -JI = K$, počítejme nyní $K^2 = -JIIJ = J^2 = -E$ a obdobně $JK = -KJ = I$, $KI = -IK = J$. Platí

$$Ee_1 = e_1, \qquad Ie_1 = e_1 i, \qquad Je_1 = e_2, \qquad Ke_1 = e_2 i$$

a tedy zobrazení $\mathbb{H} \to \mathcal{E}_2$, $Q \mapsto Qe_1$ je izomorfismus. Obrazy E, I, J, K značíme postupně 1, i, j, k a v dalším budeme o $\mathbb{H}$ uvažovat jako o prostoru $\mathbb{R}^4 = [1, i, j, k]$ společně s násobením daným výše uvedenými vztahy.

	1	i	j	k
1	1	i	j	k
i	i	-1	k	$-j$
j	j	$-k$	-1	i
k	k	j	$-i$	-1

8. Dodatek ke geometrii v prostoru

V této části dáme do souvislosti geometrii v prostoru s kvaterniony. Připomeňme, že kvaterniony vzniknou z komplexních čísel přidáním jednotky j, která antikomutuje s komplexní jednotkou i, tj. platí $ij = -ji$, a splňuje $i^2 = j^2 = -1$. Označme $k = ij$. Potom máme následující

$$q = (a + xi) + (y + zi)j = a + (xi + yj + zk).$$

Číslo a nazveme *reálnou částí* kvaternionu q a $v = xi + yj + zk$ jeho *vektorovou částí*; lze totiž tuto část ztotožnit s vektorem $(x, y, z) \in \mathbb{R}^3$. Chápeme proto komplexní jednotky i, j, k jako vektory standardní báze. Pro jejich součin platí jednoduché vztahy, díky nimž se snadno ověří, že

$$v \cdot w = -\langle v, w\rangle + v \times w.$$

Jelikož je skalární součin komutativní a vektorový součin antikomutativní, dostáváme snadno vztahy

$$\langle v, w\rangle = -\tfrac{1}{2}(vw + wv) = -\operatorname{Re}(uv), \quad v \times w = \tfrac{1}{2}(vw - wv) = \operatorname{Im}(uv).$$

Orientovaný objem $\operatorname{Vol}(u, v, w)$ snadno získáme jako reálnou část

$$\operatorname{Vol}(u, v, w) = -\tfrac{1}{4}(uvw - vuw + wuv - wvu) = -\operatorname{Re}(uvw).$$

Zabývejme se nyní inverzí kvaternionu $q = a+v$. K tomu nám poslouží konjugovaný kvaternion $q^* = a - v$. Platí

$$q^*q = (a - v)(a + v) = aa - vv = aa + \langle v, v\rangle = |a|^2 + |v|^2 = |q|^2$$

a tedy $q^{-1} = |q|^{-2}q^*$. Zejména, pokud je q jednotkový kvaternion, tj. $|q| = 1$, dostáváme $q^{-1} = q^*$. Kvaterniony mají také goniometrický tvar; my si vystačíme s jednotkovými kvaterniony, pro něž platí

$$q = \cos\varphi + v \sin\varphi,$$

kde $\varphi \in [0, \pi]$ a $v \in \mathbb{R}^3$ je jednoznačně určený jednotkový vektor s vyjímkou $q = \pm 1$, kdy není určený vůbec. Občas je také výhodné zapisovat

$$e^{\varphi v} = \cos\varphi + v \sin\varphi.$$

Tento vztah dává smysl zejména, když výraz vlevo rozvineme do Taylorovy řady a využijeme vztahu $v^2 = -|v|^2 = -1$. Pro inverzní kvaternion platí $(e^{\varphi v})^{-1} = e^{-\varphi v}$. Obecně pak platí vztah

$$\log(e^v e^w) = v + w + v \times w + \cdots$$

a známé pravidlo pro násobení mocnin v kvaternionech neplatí — důvodem je, že nejsou komutativní. Obecně platí $vw = wv$, právě když $v \parallel w$ a $vw = -wv$, právě když je $v \perp w$. Lze proto spočítat pro $v \parallel w$

$$e^{\varphi v} w e^{-\varphi v} = e^{\varphi v} e^{-\varphi v} w = w,$$

což znamená, že vektor w se touto konjugací zachovává. Naopak pro $v \perp w$ platí

$$w e^{-\varphi v} = w(\cos\varphi - v \sin\varphi) = (\cos\varphi + v\sin\varphi)w = e^{\varphi v} w$$

a proto

$$e^{\varphi v} w e^{-\varphi v} = e^{\varphi v} e^{\varphi v} w = e^{2\varphi v} w = (\cos 2\varphi) w + (\sin 2\varphi) v \times w.$$

Vektor $v \times w$ je kolmý jak na v, tak na w a má stejnou velikost jako w. Leží tedy $e^{\varphi v} w e^{-\varphi v}$ na kružnici procházející w a $v \times w$ a nachází se od w vzdálen o úhel 2φ. Ve výsledku tak konjugace $e^{\varphi v}$ geometricky odpovídá rotaci o úhel 2φ okolo osy dané vektorem v. Z těchto úvah plyne poměrně praktický popis toho, jak spočítat složení dvou rotací.

Nechť například R je rotace okolo osy x o úhel $60°$ a S je rotace okolo osy z o úhel $90°$. Potom R odpovídá konjugaci kvaternionem $e^{\pi/6 \cdot i}$ a S konjugaci $e^{\pi/4 \cdot k}$. Jejich složení je potom dané kvaternionem

$$\begin{aligned} SR \sim e^{\pi/4 \cdot k} e^{\pi/6 \cdot i} &= (\sqrt{2}/2 + \sqrt{2}/2 \cdot k)(\sqrt{3}/2 + 1/2 \cdot i) \\ &= \sqrt{6}/4 + \sqrt{2}/4 \cdot i + \sqrt{2}/4 \cdot j + \sqrt{6}/4 \cdot k. \end{aligned}$$

Ve výsledku se tak jedná o rotaci okolo osy dané vektorem $(1, 1, \sqrt{3})$ o úhel $2\arccos(\sqrt{6}/4)$.

Poznamenejme, že tento příklad lze počítat také pomocí matic. Složení dvou zadaných rotací má matici

$$\begin{pmatrix} 0 & -1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 0 \\ 0 & \frac{1}{2} & -\frac{\sqrt{3}}{2} \\ 0 & \frac{\sqrt{3}}{2} & \frac{1}{2} \end{pmatrix} = \begin{pmatrix} 0 & -\frac{1}{2} & \frac{\sqrt{3}}{2} \\ 1 & 0 & 0 \\ 0 & \frac{\sqrt{3}}{2} & \frac{1}{2} \end{pmatrix}.$$

Vlastní vektor příslušný vlastnímu číslu 1 je $(1, 1, \sqrt{3})$, jak se snadno spočítá, a stopa této matice je

$$\tfrac{1}{2} = 1 + (\cos\varphi + i\sin\varphi) + (\cos\varphi - i\sin\varphi) = 1 + 2\cos\varphi,$$

z čehož vychází $\varphi = \arccos(-\frac{1}{4})$. Těžší je zjistit, jestli se jedná o rotaci v kladném či záporném směru.

Podobně se dají reprezentovat reflexe. Zobrazení $w \mapsto vwv$ je na vektorech $v \parallel w$ rovno

$$vwv = vvw = -w$$

a na vektorech $v \perp w$ rovno

$$vwv = -vvw = w.$$

Jedná se tedy o reflexi vzhledem k rovině kolmé na vektor v (opět předpokládáme, že $|v| = 1$). Zabývejme se nyní tím, co se stane při složení dvou reflexí, prvně podle roviny kolmé na v a poté podle roviny kolmé na v'. Dostaneme

$$w \mapsto v'vwvv' = (-v'v)w(-vv') = (\langle v', v\rangle - v' \times v)w(\langle v, v'\rangle - v \times v'),$$

tj. rotaci okolo vektoru $v \times v' = -v' \times v$ o úhel $2 \arccos\langle v', v\rangle$.

9. Smithův normální tvar celočíselných matic

Celočíselná matice tvaru $n \times m$ je kolekce celých čísel $A = (a^i_j)$ indexovaná dvojicemi $i = 1, \dots, n$, $j = 1, \dots, m$. Píšeme $A \in \mathrm{Mat}_{n\times m} \mathbb{Z}$. Celočíselné matice odpovídají homomorfismům grup:

Lemma 9.1. *Homomorfismy grup $\mathbb{Z}^m \to \mathbb{Z}^n$ odpovídají přesně celočíselným maticím typu $m \times n$. Matice $A \in \mathrm{Mat}_{n\times m} \mathbb{Z}$ odpovídá homomorfismu $x \mapsto Ax$.*

Důkaz. Každý homomorfismus grup $\varphi : \mathbb{Z}^m \to \mathbb{Z}^n$ je jednoznačně určen obrazy $\varphi(e_1), \dots, \varphi(e_m)$, které ale můžou být libovolné:

$$\varphi(a_1, \dots, a_m) = \varphi(a_1 e_1 + \cdots + a_m e_m) = a_1\varphi(e_1) + \cdots + a_m\varphi(e_m).$$

Tyto obrazy jsou přesně sloupce matice A. □

Naším cílem bude nyní každý takový homomorfismus reprezentovat "ve vhodných bázích" co nejjednodušší maticí. Pro jednoduchost zde budeme změnu báze definovat jako izomorfismus. Bude nás tedy zajímat nalezení invertibilních matic P a Q takových, že $P^{-1}AQ$ je co nejjednodušší. Stejně jako v případě vektorových prostorů dostaneme invertibilní matice pomocí elementárních řádkových/sloupcových operací, jen musíme dávat pozor na násobení řádků a sloupců. Jediné operace tohoto typu, které jsou invertibilní, jsou totiž násobení ± 1.

V dalším proto budeme za řádkové operace považovat pouze: přičtení násobku jednoho řádku k druhému, prohození dvou řádků a vynásobení řádku číslem -1. To samé samozřejmě platí pro sloupcové operace.

Obecně máme následující charakterizaci:

Lemma 9.2. *Celočíselná matice A je invertibilní, právě když je čtvercová a její determinant je roven ± 1.*

Důkaz. Prvně si uvědomme, že libovolná celočíselná inverze je zároveň inverzí nad $\mathbb{Q}$ a proto musí být matice A čtvercová (s nenulovým determinantem). Zároveň

$$1 = \det E = \det(AA^{-1}) = \det A \cdot \det A^{-1}$$

a, jelikož A^{-1} je celočíselná, musí být také celočíselný její determinant, $\det A^{-1} \in \mathbb{Z}$. Proto $\det A = \pm 1$.

Nechť naopak A je čtvercová, jejíž determinant je ± 1. Potom inverzní matici můžeme spočítat pomocí matice algebraických doplňků:

$$A^{-1} = \tfrac{1}{\det A} \cdot A_{\mathrm{adj}}$$

a je celočíselná. □

Poznámka. Podobný důkaz funguje nad libovolným komutativním okruhem R (to by mělo být zřejmé alespoň pro obor integrity, kde $\mathbb{Q}$ je nahrazeno podílovým tělesem): matice $A \in \mathrm{Mat}_{n\times m} R$ je invertibilní, právě když $m = n$ a $\det A \in R^\times$ je invertibilní. Komutativita okruhu R je důležitá – bez ní by jednak nebylo možné definovat determinant a navíc existují okruhy s invertibilními obdelníkovými maticemi!

Věta 9.3 (o Smithově normálním tvaru)**.** *Pro libovolnou celočíselnou matici A existují invertibilní celočíselné matice P a Q takové, že*

$$A = P \begin{pmatrix} q_1 & 0 & \cdots & \cdots & \cdots & 0 \\ 0 & q_2 & \ddots & & & \vdots \\ \vdots & \ddots & \ddots & \ddots & & \vdots \\ \vdots & & \ddots & q_r & \ddots & \vdots \\ \vdots & & & \ddots & 0 & \ddots \\ 0 & \cdots & \cdots & \cdots & \ddots & \ddots \end{pmatrix} Q^{-1},$$

kde $q_1|q_2|\cdots|q_r$ se postupně dělí. Čísla q_i se nazývají invariantní faktory*, pravá strana se nazývá* Smithův normální tvar *celočíselné matice A. Každý jiný takový se liší pouze znaménky q_i. Konkrétněji*

$$q_1 \cdots q_i = \gcd\{\det S \mid S \text{ je submatice } A \text{ tvaru } i \times i\} \tag{1}$$

Poznámka. Je tedy vhodné vyžadovat $q_i > 0$ a tyto jsou potom určené zcela jednoznačně. V dalším budeme vždy tuto volbu preferovat.

Důkaz. Hlavním krokem je pomocí řádkových a sloupcových operací vyrobit v levém horním rohu největší společný dělitel všech prvků matice, dále pomocí něj vyeliminovat všechny prvky pod ním a vpravo od něj a následně použít indukci.

Základním krokem je vytvoření největšího společného dělitele prvků ležících v témž řádku nebo sloupci. K tomu budeme využívat Eukleidův algoritmus, který spočítá největšího společného dělitele následujícím způsobem: jsou-li a, b taková, že $|a| > |b|$, vydělíme číslo a číslem b se zbytkem, $a = qb + r$. Potom

$$\gcd(a, b) = \gcd(r, b).$$

Po konečném (ve skutečnosti velmi malém) počtu kroků vyjde $r = 0$; potom příslušné b v tomto kroku je hledaný největší společný dělitel.

Vraťme se nyní k naší matici A. Prvně přesuňme na pozici $(1, 1)$ pomoci operací libovolný nenulový prvek matice A (rozmyslete si zvlášť případ $A = 0$). V dalších krocích se bude vždy prvek na této pozici zmenšovat, díky čemuž bude náš algoritmus konečný.

Pomocí Eukleidova algoritmu a jeho implementací pomocí řádkových a sloupcových operací můžeme dosáhnout toho, že prvek v levém horním rohu dělí všechny prvky pod ním a také vpravo od něj,

$$B = \begin{pmatrix} b_1^1 & 0 & \cdots & 0 \\ 0 & * & \cdots & * \\ \vdots & \vdots & & \vdots \\ 0 & * & \cdots & * \end{pmatrix}.$$

Pokud by nyní prvek b_1^1 nedělil nějaký prvek matice B, můžeme jej pomocí přičtení řádku dostat do prvního řádku a pomocí předchozího opět na pozici $(1, 1)$ vyrobit prvek (nutně menší!), který jej již dělit bude. Po konečném počtu kroku tak b_1^1 dělí všechny prvky matice B. Na submatici vzniklou vynecháním prvního řádku a sloupce můžeme použít indukční předpoklad a převést jej na Smithův normální tvar. Protože b_1^1 dělil všechny prvky této submatice, dělí i levý horní roh jejího Smithova normálního tvaru (z konkrétního popisu ze znění věty) a tím pádem i všechny ostatní prvky.

Zbývá dokázat jednoznačnost. Podle předchozího jsou nutně matice P a Q součinem elementárních matic. Zároveň je téměř jasné (přesně to dokážeme v následujícím odstavci), že pravá strana (1) pro Smithův normální tvar je právě součin $q_1 \cdots q_i$. Stačí tak ukázat, že pravá strana je invariantní vůčí řádkovým operacím (invariance vůčí sloupcovým operacím pak plyne ze symetrie).

Vraťme se prvně krátce k největšímu společnému děliteli subdeterminantů matice B v Smithově normálním tvaru. Zřejmě, pokud submatice obsahuje k-tý řádek, nikoliv však k-tý sloupec matice B, pak její determinant je nulový (jelikož obsahuje nulový řádek). Proto stačí uvažovat submatice složené z nějakých řádků a týchž sloupců. Ty jsou diagonální a jejich determinant je roven součinu prvků na diagonále – libovolných i prvků diagonály B. Tedy největší společný dělitel z (1) je

$$\gcd\{q_{k_1} \cdots q_{k_i} \mid 1 \leq k_1 < \cdots < k_i \leq r\} = q_1 \cdots q_i$$

Zbývá dokázat invarianci největšího společného dělitele subdeterminantů vzhledem k řádkovým operacím. Invariance vzhledem k prohození řádků a vzhledem k přenásobení řádku číslem -1 je zřejmá – prvky množiny subdeterminantů maximálně změní znaménka, což nemá na největší společný dělitel žádný vliv. Invariance vzhledem k přičítání násobku řádku k jinému je o něco složitější. Množina subdeterminantů se změní následujícím způsobem. Každý nový subdeterminant je celočíselnou kombinací subdeterminantů předchozí matice. Zejména je tedy dělitelný největším společným dělitelem subdeterminantů před operací. Ve výsledku je nový největší společný dělitel násobkem předchozího. Protože však byla operace invertibilní, lze provést i v opačném směru a dostáváme taktéž opačnou dělitelnost. Proto se tito největší společní dělitelé nezmění. □

Smithův normální tvar je vhodný k algoritmickým výpočtům s komutativními grupami. Platí totiž následující vztahy

$$\begin{aligned} \operatorname{im} A &= \langle q_1 \cdot Pe_1, \ldots, q_r \cdot Pe_r \rangle \\ \ker A &= \langle Qe_{r+1}, \ldots, Qe_m \rangle, \end{aligned}$$

tedy obraz i jádro homomorfismu A lze jednoduchým způsobem vyjádřit ze sloupců matic P a Q a z invariantních faktorů q_i.

10. Prezentace konečně generovaných komutativních grup

Nechť M je komutativní grupa. V následujícím budeme komutativní grupy uvažovat vždy aditivně, tj. grupovou operaci budeme značit $+$, jednotku 0 a inverzi prvku x značíme $-x$.

Nechť $a \in \mathbb{Z}$ a $x \in M$. Definujme $a \cdot x$ jako 0, pokud $a = 0$, jako

$$\underbrace{x + \cdots + x}_{a\times}$$

pokud $a > 0$ a jako $(-a) \cdot (-x)$, pokud $a < 0$. Toto označení by čtenáři mělo být známe z multiplikativního zápisu x^a, kde značí přesně to stejné. Výhodou tohoto zápisu je, že v každé (komutativní) grupě umíme automaticky násobit celými čísly, můžeme se tedy bavit o celočíselných kombinacích a používat okamžitě některé další pojmy z vektorových prostorů.

Nechť $x_1, \ldots, x_n \in M$ jsou libovolné prvky komutativní grupy M. Uvažujme následující homomorfismus grup

$$\varphi : \mathbb{Z}^n \to M, \qquad (a_1, \ldots, a_n) \mapsto a_1 x_1 + \cdots a_n x_n,$$

který není od věci zapisovat jako "řádkový vektor" $(x_1, \ldots, x_n)$ (ve vektorových prostorech jsou vektory brány jako sloupcové a proto se jejich n-tice – zejména báze – organizují do řádků. To má tu výhodu, že je můžeme jednoduše zprava násobit sloupcem koeficientů a dostat tak jejich lineární kombinace. Případně je můžeme zprava násobit maticemi a dostat nové soubory vektorů, hlavně pak nové báze. Přesně to samé máme na mysli zde).

Lemma 10.1. *Zobrazení φ je skutečně homomorfismus grup. Navíc platí*

(1) *φ je surjektivní, právě když prvky $x_1, \ldots, x_n$ generují M.*
(2) *φ je injektivní, právě když jsou "lineárně nezávislé nad $\mathbb{Z}$".*

□

Omezme se nyní na situaci, kdy prvky $x_1, \ldots, x_n$ generují M. Potom je φ podle předchozího surjektivní a z algebry známe následující fakt.

$$M \cong \mathbb{Z}^n / \ker \varphi$$

K pochopení konečně generovaných komutativních grup bude tedy dobré zkoumat grupu $\mathbb{Z}^n$ a její podgrupy.

Věta 10.2. *Každá podgrupa $\mathbb{Z}^n$ je opět konečně generovaná a ve skutečnosti izomorfní $\mathbb{Z}^m$ pro nějaké $m \leq n$.*

Důkaz. Budeme postupovat induktivně. Pro $n = 1$ máme $M \subseteq \mathbb{Z}$ a víme, že vždy $M = a \cdot \mathbb{Z}$. Máme tedy dvě možnosti. Pokud $a = 0$, je $M \cong \mathbb{Z}^0$, v opačném případě $M \cong \mathbb{Z}^1$.

Nechť nyní $M \subseteq \mathbb{Z}^{n+1}$ a uvažme projekci

$$p : \mathbb{Z}^{n+1} \to \mathbb{Z}, \qquad (a_1, \ldots, a_{n+1}) \mapsto a_{n+1}$$

Opět $p(M) \subseteq \mathbb{Z}$ je podgrupa a tedy $p(M) = \mathbb{Z} \cdot a$. Nechť $c \in M$ je nějaké takové, že $a = p(c)$. Dále uvažme podgrupu $\ker p \subseteq \mathbb{Z}^{n+1}$, která je zřejmě izomorfní $\mathbb{Z}^n$ a můžeme tedy na ní aplikovat indukční předpoklad. Nechť tedy

$$M \cap \ker p = \langle b_1, \ldots, b_m \rangle$$

Tvrdíme nyní, že $M = \langle b_1, \ldots, b_m, c \rangle$. Uvažme proto libovolné $x \in M$. Podle konstrukce máme $p(x) = ka$ a

$$x = kc + (x - kc),$$

kde $x - kc \in M \cap \ker p$ a tedy

$$x = kc + l_1 b_1 + \cdots + l_m b_m.$$

Podrobnějším prozkoumáním důkazu lze též dokázat induktivně, že prvky $b_1, \ldots, b_m, c$ jsou lineárně nezávislé nad $\mathbb{Z}$, pokud jsou lineárně nezávislé $b_1, \ldots, b_m$ a $a \neq 0$. □

Poznámka. Podobné tvrzení pro nekomutativní grupy neplatí. Existuje grupa, která je generována dvěma prvky (jedná se o volnou grupu na dvou generátorech), která obsahuje jako podgrupu grupu, která je generovaná třemi, čtyřmi, ... prvky a dokonce i podgrupu, která není konečně generovaná.

Přejděme nyní k hlavnímu konceptu této části – prezentacím. Nechť M je komutativní grupa generovaná prvky $x_1, \ldots, x_n$ a uvažme surjektivní homomorfismus

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

jako předtím. Podle předchozí věty je $\ker\varphi$ opět konečně generovaná komutativní grupa a můžeme tedy najít další surjektivní homomorfismus

$$\psi : \mathbb{Z}^m \twoheadrightarrow \ker\varphi.$$

Zavedeme-li pro složení $\mathbb{Z}^m \to \ker\varphi \hookrightarrow \mathbb{Z}^n$ označení A, budeme vzniklou situaci zapisovat

$$\mathbb{Z}^m \xrightarrow{A} \mathbb{Z}^n \xrightarrow{\varphi} M.$$

V každé takové posloupnosti budeme vyžadovat, aby φ byl surjektivní homomorfismus grup a $\ker\varphi = \operatorname{im} A$. Potom dostáváme izomorfismus

$$M \cong \mathbb{Z}^n/\ker\varphi = \mathbb{Z}^n/\operatorname{im} A.$$

Všimněme si, že pravá strana $\mathbb{Z}^n/\operatorname{im} A$ závisí pouze na homomorfismu (matici) A. Říkáme proto, že A prezentuje komutativní grupu M.

Poznámka. Prezentace grupy M lze definovat konkrétněji pomocí generátorů M a relací mezi nimi. Generátory $e_1, \dots, e_n$ grupy $\mathbb{Z}^n$ odpovídají (zvoleným) generátorům $x_1, \dots, x_n$ grupy M a generátory grupy $\mathbb{Z}^m$ budou odpovídat relacím mezi $x_1, \dots, x_n$. Obrazy generátorů $e_j \in \mathbb{Z}^m$ jsou nějaké celočíselné kombinace

$$a_{1j}e_1 + \cdots + a_{nj}e_n.$$

Z podmínky $\ker\varphi = \operatorname{im} A$ plyne, že analogické kombinace

$$a_{1j}x_1 + \cdots + a_{nj}x_n$$

jsou nulové. To jsou přesně ony zmiňované relace mezi generátory M a M je v jistém smyslu "nejobecnější" komutativní grupa s generátory $x_1, \dots, x_n$ splňujícími tento systém relací. Přesněji, je-li N jiná komutativní grupa s prvky $y_1, \dots, y_n$ splňujícími tytéž relace

$$a_{1j}y_1 + \cdots + a_{nj}y_n = 0,$$

existuje jediný homomorfismus grup $M \to N$ posílající x_i na y_i. Tento fakt nebudeme dokazovat, poznamenejme ale, že plyne (celkem snadno) z univerzální vlastnosti kvocientu $\mathbb{Z}^n/\operatorname{im} A$.

Konečně generované komutativní grupy jsou ve výsledku prezentovány celočíselnými maticemi. Nyní ukážeme, že ze znalosti Smithova normálního tvaru lze prezentovanou grupu zcela zrekonstruovat, samozřejmě až na izomorfismus. Obecněji se zabývejme případem ekvivalentních matic a jimi prezentovaných komutativních grup

$$\begin{array}{ccccc}
\mathbb{Z}^m & \xrightarrow{A} & \mathbb{Z}^n & \longrightarrow & M \\
{\scriptstyle\cong}\downarrow{\scriptstyle Q} & & {\scriptstyle\cong}\downarrow{\scriptstyle P} & & \vdots \\
\mathbb{Z}^m & \xrightarrow[A']{} & \mathbb{Z}^n & \longrightarrow & M'
\end{array}$$

Tvrdíme, že naznačený homomorfismus $M \to M'$ existuje a je to navíc izomorfismus. Prezentované grupy můžeme ztotožnit s kvocienty podle obrazů a hledáme tedy homomorfismus

$$\mathbb{Z}^n/\operatorname{im} A \to \mathbb{Z}^n/\operatorname{im} A'.$$

Ten lze jednoduše definovat předpisem

$$x + \operatorname{im} A \mapsto Px + \operatorname{im} A'.$$

Jelikož se každý jiný reprezentant třídy $x + \operatorname{im} A$ liší od x o prvek tvaru Ay, příslušná pravá strana se změní o třídu prvku $PAy = A'Qy \in \operatorname{im} A'$ a zůstane proto stejná; zobrazení je

dobře definované. Inverzní zobrazení je určené týmž předpisem s P nahrazeným P^{-1}. Tento výsledek lze vyjádřit heslem: izomorfní prezentace určují izomorfní grupy.

Zabývejme se nyní tím, jakou grupu prezentuje matice ve Smithově normálním tvaru.

Lemma 10.3. *Je-li A ve Smithově normálním tvaru s nenulovými prvky $q_1|\cdots|q_r$ na diagonále, pak*

$$\mathbb{Z}^n/\operatorname{im} A \xrightarrow{\cong} \mathbb{Z}/q_1 \times \cdots \mathbb{Z}/q_r \times \mathbb{Z}^{n-r}$$

Důkaz. Potřebné zobrazení se definuje snadno

$$(x_1,\ldots,x_n) + \operatorname{im} A \mapsto ([x_1],\ldots,[x_r],x_{r+1},\ldots,x_n)$$

a je jednoduché ověřit, že se jedná o dobře definovaný homomorfismus grup. Stejně snadno se definuje i inverzní zobrazení. □

V kombinaci s předchozími úvahami dostáváme první část následující věty.

Věta 10.4. *Každá konečně generovaná komutativní grupa je izomorfní součinu cyklických grup*

$$\mathbb{Z}/q_1 \times \cdots \times \mathbb{Z}/q_r \times \mathbb{Z}^k, \tag{2}$$

kde $1 \neq q_1|\cdots|q_r$. Dvě takové grupy jsou izomorfní, právě když se rovnají odpovídající řády $q_1,\ldots,q_r$ konečných cyklických faktorů a exponenty k beztorzních částí.

Důkaz. Existenční část plyne z toho, že každá konečně generovaná komutativní grupa má prezentaci a ta je ekvivalentní prezentaci ve Smithově normálním tvaru. Činitele tvaru $\mathbb{Z}/1 = 0$ můžeme vynechat.

Jednoznačnost se dokáže následovně. Jsou-li dvě grupy tvaru (2) izomorfní, musí být izomorfní i jejich torzní části $\mathbb{Z}/q_1 \times \cdots \times \mathbb{Z}/q_r$. Přitom q_r je řád největší konečné cyklické podgrupy a musí být tedy stejný pro obě grupy. Součin zbylých konečných cyklických grup je kvocient torzní části podle její největší cyklické podgrupy a musí být tedy opět izomorfní pro obě grupy. Podle indukčního předpokladu se musí tedy rovnat všechna odpovídající $q_1,\ldots,q_r$. Kvocient podle torzní části je roven $\mathbb{Z}^k$ a opět musí být tato grupa izomorfní odpovídající grupě $\mathbb{Z}^{k'}$. Tento izomorfismus je zprostředkován invertibilní maticí. Jelikož každá taková musí být nutně čtvercová, dostáváme $k = k'$. □

Je-li M konečná, lze dát invariantnímu faktoru q_n následující význam. Jedná se o nejmenší číslo t vzhledem k dělitelnosti (což je téměř to samé co vzhledem k velikosti), pro které $t \cdot M = 0$, tedy nejmenší číslo dělitelné řádem každého prvku. Poněkud abstraktněji definujme $\operatorname{Ann}(M) = \{t \in \mathbb{Z} \mid t \cdot M = 0\}$, anihilátor komutativní grupy M. Jedná se vždy o podgrupu a platí $\operatorname{Ann}(M) = \mathbb{Z} \cdot q_n$.

Podobnou iterpretaci lze dát s trochou práce i zbývajícím invariantním faktorům, konkrétně

$$\operatorname{Ann}(\Lambda^{n-i+1}M) = \mathbb{Z} \cdot q_i,$$

k tomu je však potřeba definovat vnější mocniny komutativních grup, což značně přesahuje obsah kurzu.

Vzhledem k jednoznačnosti z předchozí věty můžeme zformulovat jednoznačnost prezentace konečně generované komutativní grupy. Pro každé dvě prezentace musí jejich Smithovy normální tvary být shodné až na jedničky na diagonále (ty zhruba řečeno odpovídají přidání nového generátoru x společně s relací $x = 0$) a nadbytečné nulové sloupce (ty zase odpovídají relacím, které lze odvodit z ostatních relací).

Mají-li matice A, B stejné rozměry, pak prezentují stejnou grupu, právě když jsou ekvivalentní (ve smyslu, že je lze na sebe převést řádkovými a sloupcovými úpravami).

11. Smithův normální tvar polynomiálních matic

Polynomiální matice tvaru $n \times m$ je kolekce polynomů $A = (a^i_j)$ indexovaná dvojicemi $i = 1, \dots, n$, $j = 1, \dots, m$. Tedy a^i_j je polynom, přesněji polynom s koeficienty v tělese $\mathbb{k}$ a v proměnné λ. Píšeme $A \in \mathrm{Mat}_{n\times m}\, \mathbb{k}[\lambda]$.

Lemma 11.1. *Polynomiální matice A je invertibilní, právě když je čtvercová a její determinant je nenulový konstantní.*

Důkaz. Důkaz se provede stejně jako pro celočíselné matice. □

Věta 11.2 (o Smithově normálním tvaru)**.** *Pro libovolnou polynomiální matici A existují invertibilní polynomiální matice P a Q takové, že*

$$A = P \begin{pmatrix} q_1 & 0 & \cdots & \cdots & \cdots & \cdots & 0 \\ 0 & q_2 & \ddots & & & & \vdots \\ \vdots & \ddots & \ddots & \ddots & & & \vdots \\ \vdots & & \ddots & q_r & \ddots & & \vdots \\ \vdots & & & \ddots & 0 & \ddots & \vdots \\ \vdots & & & & \ddots & \ddots & 0 \\ 0 & \cdots & \cdots & \cdots & \cdots & 0 & 0 \end{pmatrix} Q^{-1},$$

kde $q_1 | q_2 | \cdots | q_r$ se postupně dělí. Polynomy q_i se nazývají invariantní faktory*, pravá strana se nazývá* Smithův normální tvar *polynomiálni matice A. Každý jiný takový se liší pouze vynásobením q_i nenulovou konstantou. Konkrétněji*

$$q_1 \cdots q_i = \gcd\{\det S \mid S \text{ je submatice } A \text{ tvaru } i \times i\} \tag{3}$$

Důkaz. Důkaz se provede stejně jako pro celočíselné matice; jeho základem byl Eukleidův algoritmus, který funguje i nad $\mathbb{k}[\lambda]$. □

Opět můžeme vyžadovat polynomy q_i normované, dostaneme pak Smithův normální tvar zcela jednoznačně.

Poznámka. Je zajímavé se zamyslet nad tím, které (komutativní) okruhy umožňují Smithův normální tvar. Potřebujeme nějakou formu Eukleidova algoritmu a pro tzv. Eukleidovské obory (obory integrity s Eukleidovým algoritmem) není naprosto žádný problém. Ve skutečnosti lze tuto větu zobecnit na obory hlavních ideálů (obory integrity, kde každý ideál je hlavní), nevystačíme si však již s elementárními operacemi: k vyrobení největšího společného dělitele nestačí odčítat násobky, ale jsou potřeba obecnější (invertibilní) lineární kombinace. Ve výsledku se dá ukázat, že nad obory hlavních ideálů již není každá invertibilní matice součinem elementárních. Rozdíl mezi invertibilními maticemi a součiny elementárních matic je jedním z důležitých aspektů studovaných algebraickou K-teorií okruhu R. Ta je velmi důležitá v rozličných odvětvích matematiky – od geometrie, přes algebru až k teorii čísel.

Stejně jako celočíselné matice měly vztah ke konečně generovaným komutativním grupám a jejich prezentacím, mají také polynomiální matice vztah k nějakým matematickým objektům a jejich prezentacím. Pokusme se jejich definici motivovat následujícím porovnáním

číselné matice $A \in \mathrm{Mat}_{n\times m}\,\Bbbk$	lineární zobrazení $\Bbbk^m \to \Bbbk^n$
celočíselné matice $A \in \mathrm{Mat}_{n\times m}\,\mathbb{Z}$	homomorfismy grup $\mathbb{Z}^m \to \mathbb{Z}^n$
polynomiální matice $A \in \mathrm{Mat}_{n\times m}\,\Bbbk[\lambda]$	homomorfismy ??? $\Bbbk[\lambda]^m \to \Bbbk[\lambda]^n$

Definice 11.3. Nechť M je komutativní grupa. Řekneme, že M je $\Bbbk[\lambda]$-*modul*, jestliže je zadáno zobrazení

$$\Bbbk[\lambda] \times M \to M, \qquad (p, x) \mapsto p \cdot x,$$

nazývané "násobení skaláry", splňující obvyklé axiomy vektorového prostoru

$$\begin{aligned} p \cdot (q \cdot x) &= (p \cdot q) \cdot x \\ 1 \cdot x &= x \\ p \cdot (x + y) &= p \cdot x + p \cdot y \\ (p + q) \cdot x &= p \cdot x + q \cdot x \end{aligned}$$

Příklad 11.4. Důležitým $\Bbbk[\lambda]$-modulem je $\Bbbk[\lambda]^n$, tj. množina všech n-tic polynomů společně se sčítáním po složkách a násobením po složkách

$$p \cdot (q_1, \dots, q_n) = (pq_1, \dots, pq_n)$$

Každý $\Bbbk[\lambda]$-modul M je automaticky vektorovým prostorem nad $\Bbbk$: když umíme prvky M násobit polynomy, umíme je zejména násobit konstantními polynomy, které lze jednoduše ztotožnit s prvky tělesa $\Bbbk$, lze psát

$$\Bbbk \hookrightarrow \Bbbk[\lambda].$$

Zároveň násobení lineárním polynomem λ je zobrazení

$$m_\lambda : M \to M, \qquad x \mapsto \lambda \cdot x,$$

o kterém ověříme, že se jedná o lineární zobrazení:

$$m_\lambda(ax + by) = \lambda \cdot ax + \lambda \cdot by = (a\lambda) \cdot x + (b\lambda) \cdot y = a(m_\lambda x) + b(m_\lambda y)$$

Věta 11.5. *Předchozí konstrukce zadává vzájemně jednoznačnou korespondenci*

$$\{\Bbbk[\lambda]\text{-}\textit{moduly } M\} \rightleftarrows \left\{ \begin{matrix} \textit{dvojice } (V,T)\textit{, kde } V \textit{ je vektorový} \\ \textit{prostor a } T : V \to V \textit{ je operátor} \end{matrix} \right\}$$

$$\begin{aligned} M &\longmapsto (M, m_\lambda) \\ V &\longleftarrow\!\shortmid\ (V, T) \end{aligned}$$

Důkaz. Zbývá ukázat, jak se pro operátor $T : V \to V$ na vektorovém prostoru V definuje násobení skaláry z $\Bbbk[\lambda]$. Má-li se jednat o inverzi ke konstrukci (M, m_λ), jsme nuceni položit

$$px = (p_0 + p_1\lambda + \cdots + p_k\lambda^k)x = p_0x + p_1Tx + \cdots + p_kT^kx,$$

kde T^ix značí i-násobnou iteraci operátoru T, tj.

$$T^ix = (T \circ \cdots \circ T)x = T(\cdots T(Tx)\cdots);$$

je totiž $\lambda^ix = \lambda(\cdots\lambda(\lambda x)\cdots) = T(\cdots T(Tx)\cdots)$. □

Z předchozího důkazu si zapamatujme vztah pro násobení polynomem p na $\mathbb{k}[\lambda]$-modulu (V,T). Budeme ho zapisovat ve tvaru

$$p \cdot x = p(T)x,$$

kde $p(T)$ značí, tak jako v důkazu, výsledek formálního dosazení operátoru T do polynomu p, tj. $p(T) = p_0 \operatorname{Id} + p_1 T + \cdots + p_k T^k$.

Poznámka. Hlavní myšlenkou předchozího důkazu je, že okruh polynomů $\mathbb{k}[\lambda]$ je generovaný tělesem $\mathbb{k}$ a jedním prvkem λ splňujícím $a \cdot \lambda = \lambda \cdot a$, tedy prvek λ je přídán "volně" pouze s tím, že má komutovat se všemi prvky z původního tělesa. Pro strukturu modulu to znamená, že musíme zadat násobení prvky tělesa $\mathbb{k}$ (strukturu vektorového prostoru) a násobení prvkem λ, kde jedinou podmínkou je, že tyto mají komutovat, tj. násobení prvkem λ musí být lineární. To je přesně tvrzení věty.

Poznámka. Výhodou uvažování $\mathbb{k}[\lambda]$-modulů namísto operátorů je to, že základním stavebním kamenem (konečně generovaných) $\mathbb{k}[\lambda]$-modulů je $\mathbb{k}[\lambda]^n$ (jak za chvíli uvidíme), který je jako vektorový prostor s operátorem nekonečně rozměrný a tedy z pohledu lineární algebry dost netypický. Konkrétně $\mathbb{k}[\lambda]$ jako vektorový prostor je

$$\mathbb{k}^{\oplus \mathbb{N}_0} = \{(a_0, a_1, \ldots) \mid \exists k \in \mathbb{N}_0 : \forall l \geq k : a_l = 0\},$$

množina posloupností čísel (odpovídajících posloupnostem koeficientů polynomů), která jsou od jistého indexu počínaje všechna nulová. Operátor je pak dán

$$(a_0, a_1, \ldots) \mapsto (0, a_0, a_1, \ldots)$$

Dalším přirozeným pojmem je homomorfismus $\mathbb{k}[\lambda]$-modulů, který je přímou analogií lineárního zobrazení.

Definice 11.6. Nechť M, N jsou dva $\mathbb{k}[\lambda]$-moduly. Zobrazení $\varphi : M \to N$ se nazývá *homomorfismem* $\mathbb{k}[\lambda]$*-modulů*, jestliže platí

$$\varphi(x+y) = \varphi(x) + \varphi(y), \qquad \varphi(px) = p\varphi(x).$$

pro libovolná $x, y \in M$ a $p \in \mathbb{k}[\lambda]$.

Opět převedeme tento pojem do řeči operátorů. Je zřejmé zúžením definiční podmínky na konstantní polynomy, že každý homomorfismus $\mathbb{k}[\lambda]$-modulů je lineární zobrazení.

Tvrzení 11.7. *Nechť jsou dány operátory T na V a S na U. Lineární zobrazení $\varphi : V \to U$ je homomorfismus $\mathbb{k}[\lambda]$-modulů, právě když komutuje následující diagram.*

$$\begin{array}{ccc} V & \xrightarrow{\varphi} & U \\ {\scriptstyle T}\downarrow & & \downarrow{\scriptstyle S} \\ V & \xrightarrow[\varphi]{} & U \end{array}$$

Důkaz. Jelikož je φ lineární, zachovává násobení všemi konstantními polynomy. Zbývá tedy zkontrolovat zachovávání násobení polynomem λ, ale to jsou přesně operátory v diagramu. □

Vraťme se k naší původní motivaci s polynomiálními maticemi.

Lemma 11.8. *Nechť $x_1, \dots, x_n \in M$ jsou libovolné prvky $\Bbbk[\lambda]$-modulu M. Pak existuje jediný homomorfismus $\Bbbk[\lambda]$-modulů $\varphi : \Bbbk[\lambda]^n \to M$ splňující $\varphi(e_i) = x_i$, kde e_i je opět n-tice polynomů $(0, \dots, 0, 1, 0, \dots, 0)$ s konstantním polynomem 1 na i-tém místě.*

Speciálně homomorfismy $\Bbbk[\lambda]$-modulů $\Bbbk[\lambda]^m \to \Bbbk[\lambda]^n$ jsou v bijekci s polynomiálními maticemi $A \in \mathrm{Mat}_{n\times m}\Bbbk[\lambda]$, jejímž i-tým sloupcem je právě obraz e_i. Příslušný homomorfismus je dán $x \mapsto Ax$.

Důkaz. Vše je jasné z rovnosti

$$\begin{aligned}\varphi(p_1, \dots, p_n) &= \varphi(p_1 e_1 + \cdots p_n e_n) = p_1\varphi(e_1) + \cdots + p_n\varphi(e_n)\\ &= p_1 x_1 + \cdots + p_n x_n.\end{aligned}$$

Naopak výsledný vzorec je homomorfismus $\Bbbk[\lambda]$-modulů pro libovolné $x_1, \dots, x_n \in M$. □

V dalším se nám ještě budou hodit kvocienty $\Bbbk[\lambda]$-modulů. Nechť M je $\Bbbk[\lambda]$-modul. Podmodul $N \subseteq M$ je podmnožina uzavřená na nulu, sčítání a násobení skaláry. Zejména je N podgrupa vzhledem ke sčítání. Na kvocientu grup M/N definujeme strukturu $\Bbbk[\lambda]$-modulu následovně:

$$p \cdot (x + N) \stackrel{\text{def}}{=} px + N$$

Je jednoduché ověřit, že se jedná o dobře definované zobrazení, které splňuje všechny axiomy $\Bbbk[\lambda]$-modulu.

12. Kanonická prezentace operátoru na $\Bbbk^n$

Nechť $T : \Bbbk^n \to \Bbbk^n$ je operátor na $\Bbbk^n$ a uvažujme příslušný $\Bbbk[\lambda]$-modul $(\Bbbk^n, T)$. Narozdíl od situace pro konečně generované komutativní grupy existuje kanonická prezentace (tj. taková, která nezávisí na žádných volbách a je "přirozená"). Uvažujme homomorfismus $\Bbbk[\lambda]$-modulů

$$\varphi : \Bbbk[\lambda]^n \to \Bbbk^n$$

jednoznačně určený tím, že posílá $e_i \mapsto e_i$, kde na levé straně je e_i interpretováno jako n-tice polynomů, zatímco na pravé straně jako n-tice čísel[3]. V obou případech se jedná o n-tici složenou z 1 na i-tém místě a z 0 na zbylých místech. Zřejmě je φ surjektivní zobrazení, popíšeme nyní jeho jádro a dostaneme tím prezentaci pro $(\Bbbk^n, T)$.

Tvrzení 12.1. *Nechť T je operátor na $\Bbbk^n$. Potom*

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

je prezentace příslušného $\Bbbk[\lambda]$-modulu.

Důkaz. Zbývá ukázat, že

$$\mathrm{im}(T - \lambda E) = \ker\varphi.$$

Zaprvé platí $\varphi \circ (T - \lambda E) = 0$, neboť pro generátory $e_i \in \Bbbk[\lambda]^n$ platí

$$\varphi \circ (T - \lambda E)(e_i) = \varphi(Te_i - \lambda e_i) = Te_i - Te_i = 0.$$

Proto $\mathrm{im}(T - \lambda E) \subseteq \ker\varphi$. K opačné implikaci pišme pro $v \in \Bbbk[\lambda]^n$

$$v = v_0 + \lambda v_1 + \cdots + \lambda^k v_k,$$

[3]Alternativní pohled na prvky $\Bbbk[\lambda]^n$ je jako polynomy s koeficienty v $\Bbbk^n$. Zobrazení je pak dáno předpisem $v_0 + \lambda v_1 + \cdots + \lambda^k v_k \mapsto v_0 + Tv_1 + \cdots + T^k v_k$.

kde $v_0, v_1, \ldots, v_k$ jsou n-tice konstantních polynomů. Zjevně platí

$$v \equiv v_0 + Tv_1 + \cdots + T^k v_k \pmod{\operatorname{im}(T - \lambda E)},$$

což je n-tice konstantních polynomů, která při ztotožnění s $\Bbbk^n$ přesně odpovídá $\varphi(v)$. Pokud tedy předpokládáme $v \in \ker \varphi$, dostáváme $v \equiv 0$ modulo $\operatorname{im}(T - \lambda E)$ a tedy $v \in \operatorname{im}(T - \lambda E)$. Platí proto i opačná inkluze $\ker \varphi \subseteq \operatorname{im}(T - \lambda E)$. □

Poznámka. Poslední tvrzení dává velice uspokojivé zdůvodnění, proč v matici $T - \lambda E$ je obsaženo vše podstatné týkající se operátoru T. To se tradičně vysvětluje přes kořenové podprostory. Předchozí tvrzení však platí nezávisle na tom, zda těleso $\Bbbk$ je algebraicky uzavřené a hodí se ke zkoumání operátoru i nad obecnými tělesy.

Nyní dáme dohromady kanonickou prezentaci se Smithovým normálním tvarem tak, jak jsme učinili pro konečně generované komutativní grupy. Nechť Smithův normální tvar $T - \lambda E$ je polynomiální matice $S(\lambda)$. Její vztah ke kanonické prezentaci je vyjádřen v následujícím diagramu

$$\begin{array}{ccccc}
\Bbbk[\lambda]^n & \xrightarrow{T-\lambda E} & \Bbbk[\lambda]^n & \longrightarrow & (\Bbbk^n, T) \\
{\scriptstyle Q(\lambda)}\downarrow\cong & & \cong\downarrow{\scriptstyle P(\lambda)} & & \downarrow\cong \\
\Bbbk[\lambda]^n & \xrightarrow[S(\lambda)]{} & \Bbbk[\lambda]^n & \longrightarrow & \Bbbk[\lambda]^n / \operatorname{im} S(\lambda)
\end{array}$$

Opět se jednoduše přesvědčíme, že

$$\Bbbk[\lambda]^n / \operatorname{im} S(\lambda) \cong \Bbbk[\lambda]/(q_1) \times \cdots \times \Bbbk[\lambda]/(q_n),$$

kde $q_1 | \cdots | q_n$ jsou polynomy vyskytující se na diagonále Smithova normálního tvaru $S(\lambda)$.

Věta 12.2. *Dva operátory T, T' jsou podobné, právě když polynomiální matice $T - \lambda E$, $T' - \lambda E$ mají týž Smithův normální tvar. Zejména lze problém podobnosti řešit algoritmicky.*

Poznámka. Nad algebraicky uzavřeným tělesem lze problém podobnosti "řešit" s pomocí Jordanova kanonického tvaru. Algoritmicky je však tento přístup nevhodný, protože obecně nelze spočítat vlastní čísla a tím pádem ani Jordanův kanonický tvar. Na druhou stranu Smithův normální tvar je zcela algoritmický.

Důkaz. Jsou-li operátory T a T' podobné, $T' = PTP^{-1}$, budou podobné i

$$T' - \lambda E = P(T - \lambda E)P^{-1}.$$

Tím spíš budou ekvivalentní a proto budou mít týž Smithův normální tvar.

Nechť naopak $T - \lambda E$, $T' - \lambda E$ mají týž Smithův normální tvar. Potom jsou ekvivalentní a podle předchozího diagramu jsou izomorfní prezentované moduly $(\Bbbk^n, T) \cong (\Bbbk^n, T')$. To ale přesně znamená, že operátory jsou podobné podle Tvrzení 11.7. □

Poznámka. Výhodou oproti případu komutativních grup je existence kanonické prezentace. O něco obtížněji lze také dokázat, že dva $\Bbbk[\lambda]$-moduly prezentované libovolnými (v kontrastu s kanonickými) polynomiálními maticemi týchž rozměrů jsou izomorfní, právě když mají tyto matice týž Smithův normální tvar; viz případ komutativních grup.

Místo Jordanova kanonického tvaru je možné popsat jiný kanonický tvar, který nevyžaduje nalezení kořenů charakteristického polynomu a lze jej spočítat algoritmicky. Jelikož je

$$(\Bbbk^n, T) \cong \Bbbk[\lambda]/(q_1) \times \cdots \times \Bbbk[\lambda]/(q_n),$$

stačí popsat $\Bbbk[\lambda]$-modul $\Bbbk[\lambda]/(q)$ jako vektorový prostor společně s operátorem. Nalezneme vhodnou (kanonickou) bázi a v ní matici příslušného operátoru m_λ. Nechť $q = a_0 + a_1\lambda + \cdots + a_{k-1}\lambda^{k-1} + \lambda^k$. Potom takovou bází je $\alpha = ([1], [\lambda], \cdots, [\lambda^{k-1}])$ a jednoduše

$$(m_\lambda)_{\alpha\alpha} = \begin{pmatrix} 0 & \cdots & \cdots & 0 & -a_0 \\ 1 & \ddots & & \vdots & -a_1 \\ 0 & \ddots & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & 0 & \vdots \\ 0 & \cdots & 0 & 1 & -a_{k-1} \end{pmatrix}.$$

Operátor na součinu modulů je blokově diagonální a tedy $(\Bbbk^n, T)$ má ve vhodné bázi blokově diagonální tvar s bloky výše uvedeného tvaru na diagonále. Tento tvar se nazývá *racionální kanonický tvar* operátoru – pro jeho kanoničnost je však nutno vyžadovat, aby se polynomy příslušné jednotlivým blokům postupně dělily tak jako ve Smithově kanonickém tvaru.

Invariantní faktor q_n má poměrně jednoduchou interpretaci v řeči $\Bbbk[\lambda]$-modulů, z níž lze jednoduše dokázat následující větu.

Tvrzení 12.3 (Cayleyho-Hamiltonova věta)**.** *Nechť $\chi(\lambda) = \det(T - \lambda E)$ značí charakteristický polynom T. Potom platí $\chi(T) = 0$.*

Důkaz. Z věty o Smithově normálním tvaru platí $\chi = q_1 \cdots q_n$. Přitom pro libovolné

$$x \in \Bbbk[\lambda]/(q_1) \times \cdots \times \Bbbk[\lambda]/(q_n)$$

zjevně platí $q_n x = 0$. Protože je však tento $\Bbbk[\lambda]$-modul izomorfní $(\Bbbk^n, T)$, platí to samé i pro $\Bbbk[\lambda]$-modul $(\Bbbk^n, T)$. Pro libovolné $v \in \Bbbk^n$ tak máme $q_n(T)v = 0$. Protože ale toto platí pro libovolné v, musí být $q_n(T) = 0$ jakožto operátory na $\Bbbk^n$. Tím spíš tedy $\chi(T) = 0$. □

Definice 12.4. Z důkazu předchozí věty plyne, že ve skutečnosti platí již $q_n(T) = 0$ a není těžké se přesvědčit, že q_n je nejmenší polynom (vzhledem k dělitelnosti), pro který tento vztah platí. Nazývá se *minimální polynom* operátoru T.

Poznámka. Opět poněkud abstraktněji lze minimální polynom popsat následovně. Definujme anihilátor $\Bbbk[\lambda]$-modulu M jako

$$\mathrm{Ann}(M) = \{p \in \Bbbk[\lambda] \mid p \cdot M = 0\}.$$

Není těžké se přesvědčit, že se vždy jedná o ideál a v našem případě je $\mathrm{Ann}(M) = (q_n)$. Opět s trochou práce lze dát význam i zbylým invariantním faktorům,

$$\mathrm{Ann}(\Lambda^{n-i+1}_{\Bbbk[\lambda]} M) = (q_i),$$

kde například $\Lambda^2_{\Bbbk[\lambda]} M$ je kvocient $\Lambda^2 M$ podle podprostoru generovaného rozdíly $Tx \wedge y - x \wedge Ty$. Operátor na tomto kvocientu je zadán předpisem

$$T[x \wedge y] \stackrel{\text{def}}{=} [Tx \wedge y] = [x \wedge Ty].$$

13. Jordanův kanonický tvar

Jelikož Smithův normální tvar $T - \lambda E$ zcela určuje operátor T až na podobnost, nemělo by být překvapením, že z něj lze spočítat Jordanův kanonický tvar T. Nechť proto nyní $\Bbbk$ je

algebraicky uzavřené těleso. Potom každý cyklický modul $\Bbbk[\lambda]/(q)$ lze psát s využitím rozkladu $q = (\lambda - \lambda_1)^{r_1} \cdots (\lambda - \lambda_k)^{r_k}$ ve tvaru[4]

$$\Bbbk[\lambda]/(q) \cong \Bbbk[\lambda]/((\lambda - \lambda_1)^{r_1}) \times \cdots \times \Bbbk[\lambda]/((\lambda - \lambda_k)^{r_k})$$

(formální podobnost s rozkladem na prvočinitele není vůbec náhodná). Zbývá tedy popsat $\Bbbk[\lambda]$-modul tvaru

$$\Bbbk[\lambda]/((\lambda - \lambda_0)^r).$$

Tvrzení 13.1. *Cyklický $\Bbbk[\lambda]$-modul $\Bbbk[\lambda]/((\lambda - \lambda_0)^r)$ je izomorfní operátoru na $\Bbbk^r$ s maticí*

$$\begin{pmatrix} \lambda_0 & 1 & 0 & \cdots & 0 \\ 0 & \ddots & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & 0 \\ \vdots & & \ddots & \ddots & 1 \\ 0 & \cdots & \cdots & 0 & \lambda_0 \end{pmatrix}$$

Důkaz. Jakožto vektorový prostor má $\Bbbk[\lambda]/((\lambda - \lambda_0)^r)$ bázi

$$([(\lambda - \lambda_0)^{r-1}], \ldots, [\lambda - \lambda_0], [1])$$

Počítejme matici operátoru m_λ (násobení polynomem λ) vzhledem k této bázi. Zjevně platí

$$\lambda[(\lambda - \lambda_0)^{i-1}] = \big((\lambda - \lambda_0) + \lambda_0\big)[(\lambda - \lambda_0)^{i-1}] = [(\lambda - \lambda_0)^i] + \lambda_0[(\lambda - \lambda_0)^{i-1}].$$

V případě $i = r$ pak $[(\lambda - \lambda_0)^r] = 0$ a dostáváme přesně matici z tvrzení. □

Lemma 13.2. *Součinu $\Bbbk[\lambda]$-modulů odpovídajících operátorům odpovídá operátor v blokovém tvaru s jednotlivými operátory na diagonále.*

Důkaz. Vše je jasné z toho, že v součinu $\Bbbk[\lambda]$-modulů se násobení děje po složkách. □

Věta 13.3. *Je-li těleso $\Bbbk$ algebraicky uzavřené, je každý operátor podobný operátoru v Jordanově kanonickém tvaru. Obecněji tvrzení platí pro operátor T nad libovolným tělesem, nad kterým se charakteristický polynom T zcela rozkládá.* □

Je-li $T - \lambda E$ ekvivalentní $J - \lambda E$, řekněme

$$J - \lambda E = P(\lambda)(T - \lambda E)Q(\lambda),$$

(nyní u $Q(\lambda)$ nebudeme psát inverzi, protože v tomto tvaru dostaneme ekvivalenci z algoritmu počítajícím Smithův normální tvar) lze spočítat matice přechodu mezi oběma operátory. Začněme s maticí přechodu od T k J. Tu dostaneme z následujícího diagramu

$$\begin{array}{ccccc} \Bbbk[\lambda]^n & \xrightarrow{T-\lambda E} & \Bbbk[\lambda]^n & \xrightarrow{\leftarrow\ -\ \rightarrow} & (\Bbbk^n, T) \\ \cong\uparrow Q(\lambda) & & \cong\downarrow P(\lambda) & & \cong\downarrow R \\ \Bbbk[\lambda]^n & \xrightarrow[J-\lambda E]{} & \Bbbk[\lambda]^n & \xrightarrow[\mathrm{ev}_J]{} & (\Bbbk^n, J) \end{array}$$

naznačené zobrazení $\Bbbk^n \to \Bbbk[\lambda]^n$ zobrazí n-tici čísel na n-tici příslušných konstantních polynomů (a nejedná se o homomorfismus $\Bbbk[\lambda]$-modulů). Složením dostaneme pro

$$P = P_0 + \lambda P_1 + \cdots + \lambda^k P_k$$

[4] Jednoduchý důkaz tohoto faktu využívá Smithův normální tvar — $\Bbbk[\lambda]$-modul napravo je prezentován diagonální maticí s mocninami $(\lambda - \lambda_i)^{r_i}$ na diagonále; její Smithův normální tvar má na diagonále $1, \ldots, 1, q$.

následující vyjádření

$$v \mapsto \mathrm{ev}_J(P(\lambda)v) = (P_0 + JP_1 + \cdots + J^k P_k)v = P^{\mathrm{left}}(J)v,$$

kde poslední zápis značí dosazení matice J do polynomiální matice $P(\lambda)$ zleva.

Matice přechodu v opačném směru lze získat buď jako inverzní matici k $P^{\mathrm{left}}(J)$ nebo pomocí transponování všech matic (formálně přechodu k duálním prostorům). Konkrétně dostáváme diagram

$$\begin{array}{ccccc}
\Bbbk[\lambda]^n & \xrightarrow{T^*-\lambda E} & \Bbbk[\lambda]^n & \xleftarrow{\ -\ -\ \ -\ } & (\Bbbk^n, T^*) \\
\cong\uparrow & & \cong\downarrow & & \cong\downarrow \\
\Bbbk[\lambda]^n & \xrightarrow[J^*-\lambda E]{} & \Bbbk[\lambda]^n & \longrightarrow & (\Bbbk^n, J^*)
\end{array}$$

nebo jednodušeji rovnici

$$J^* - \lambda E = Q^*(\lambda)(T^* - \lambda E)P^*(\lambda)$$

Podle předchozího dostáváme $S^* = (Q^*)^{\mathrm{left}}(J^*)$ a zpětným transponováním

$$\begin{aligned} S &= ((Q^*)^{\mathrm{left}}(J^*))^* = (Q_0^* + J^*Q_1^* + \cdots + (J^*)^k Q_k^*)^* \\ &= Q_0 + Q_1 J + \cdots + Q_k J^k = Q^{\mathrm{right}}(J). \end{aligned}$$

Jelikož je S matice přechodu od J k T, skládají se její sloupce z vektorů báze, v níž T nabývá Jordanova kanonického tvaru J. Matici $Q(\lambda)$ lze získat tak, že veškeré sloupcové operace provádíme zároveň na matici $T - \lambda E$ a na jednotkové matici (řádkové operace však pouze na $T - \lambda E$). Pokud takto převedeme $T - \lambda E$ na $J - \lambda E$, vytvoří sloupcové operace přesně matici $Q(\lambda)$. Dosadíme-li pak do ní matici J zprava, získáme hledanou matici přechodu S.

Vhodnou adaptací lze výpočet zjednodušit. Není potřeba pomocí dalších operací převádět Smithův normální tvar na $J - \lambda E$, neboť lze využít bázi $\Bbbk[\lambda]^n / \operatorname{im} B$ z důkazu Tvrzení 13.1, kde B je Smithův normální tvar $T - \lambda E$. Uveďme si to na příkladu

$$B = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & 1 & 0 \\ 0 & \cdots & 0 & (\lambda - \lambda_0)^r \end{pmatrix}$$

Potom forma f^i na prostoru $\Bbbk^n$ vpravo nahoře se zobrazí na formu na $\Bbbk[\lambda]^n$ s týmž názvem, dále pak pomocí $Q^*(\lambda)$ na $f^iQ(\lambda)$, tj. na i-tý řádek matice $Q(\lambda)$. Na závěr je potřeba spočítat, jakou formu na $\Bbbk^n$ v pravém dolním rohu tato reprezentuje. Vyjádříme ji proto ve tvaru[5]

$$f^iQ(\lambda) \equiv \sum_j f^r(\lambda - \lambda_0)^j a_j^i$$

modulo $\operatorname{im} B = (f^1, \ldots, f^{r-1}, f^r(\lambda - \lambda_0)^r)$. Matice a_j^i je hledanou maticí přechodu (v případě $B = J - \lambda E$ se výpočet zjednodušil tím, že počítání modulo $\operatorname{im} B$ je dosazování J).

[5]Koeficienty a_j^i jsou členy Taylorova rozvoje polynomu $(f^iQ(\lambda))_r$ (tj. prvku $Q(\lambda)_r^i$ matice $Q(\lambda)$) v bodě λ_0.