Matematický ústav Slezské univerzity v Opavě

Učební texty k přednášce ALGEBRA II, letní semestr 2002/2003

Michal Marvan

# 18. První rozklad lineární transformace

V této přednášce $V$ označuje vektorový prostor (obvykle konečněrozměrný) nad polem $P$ a $f : V \longrightarrow V$ je jistá pevně zvolená lineární transformace. Pro praktické výpočty se stačí omezit na vektorový prostor $V = P^n$ a lineární transformaci $f : P^n \longrightarrow P^n$, $f(u) = Au$, kde $A$ je čtvercová matice.

Budeme se zabývat rozkladem prostoru $V$ na přímý součet tzv. invariantních podprostorů, s čímž je spojeno uvedení matice $A$ do blokově diagonálního tvaru. První (primární) rozklad je indukován rozkladem anulujícího (např. charakteristického) polynomu na nesoudělné součinitele (například kořenové činitele).

## 1. Invariantní podprostory

Je-li $U \subseteq V$ podprostor, pak symbolem $fU$ označujeme jeho obraz při zobrazení $f$, to jest, podprostor $\{ f(u) \mid u \in U \}$.

**1.1. Definice.** Podprostor $U \subseteq V$ se nazývá *invariantní* (vzhledem k lineární transformaci $f$), když platí $fU \subseteq U$, tj. když pro každé $u \in U$ je $f(u) \in U$.

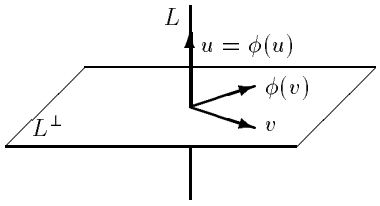
Je-li $U$ invariantní podprostor, pak zobrazení $U \longrightarrow U$, zadané předpisem $u \longmapsto f(u)$, nazýváme *restrikce* (česky *ohraničení*) lineárního zobrazení $f$ na invariantní podprostor $U$. Značí se $f|_U : U \longrightarrow U$ a je zřejmě opět lineární (ověřte).

**Příklad.** (1) Celý prostor $V$ a nulový podprostor jsou invariantní podprostory.

(2) Je-li $f : v \longmapsto cv$, pak je každý podprostor invariantní.

(3) Je-li $u$ vlastní vektor s vlastní hodnotou $c$, pak $[\![u]\!]$ je invariantní podprostor a $f|_{[\![u]\!]}$ je zobrazení $v \longmapsto cv$.

(4) Uvažujme o rotaci $\phi$ v prostoru $E^3$ kolem osy $L$ procházející počátkem 0 o úhel $\alpha \in (0, 2\pi)$. Invariantní podporostory jsou nulový podprostor $\{0\}$, osa rotace $L$, její ortogonální doplněk $L^\perp$ a celý prostor $E^3$. Libovolný vektor $u \in L$ se zobrazí sám na sebe, proto $\phi|_L$ je identické zobrazení $\mathrm{id}_L$. Libovolný vektor $v \in L^\perp$ zůstane v rovině $L^\perp$ a $\phi|_{L^\perp}$ je otáčení roviny $L^\perp$ o úhel $\alpha$.




(5) Uvažujme o zrcadlení $\zeta$ v prostoru $E^3$ vzhledem k rovině $U$ procházející počátkem 0. Invariantní podporostory jsou nulový podprostor $\{0\}$, rovina $U$ a každý její podprostor $V \subseteq U$, ortogonální doplněk $U^\perp$ a celý prostor $E^3$. Zobrazení $\zeta|_V$ je identické zobrazení $\mathrm{id}_V$. Zobrazení $\zeta|_{U^\perp}$ je zrcadlení přímky $U^\perp$ vzhledem k počátku 0.

**Cvičení.** (1) Jednorozměrný podprostor $[\![u]\!]$, $u \neq 0$, je invariantní právě tehdy, když $u$ je vlastní vektor. Dokažte.

(2) Průnik a součet invariantních podprostorů jsou invariantní podprostory. Dokažte.

(3) $\mathrm{Ker}\, f$ je invariantní podprostor. Dokažte. Co je $f|_{\mathrm{Ker}\, f}$?

(4) $\mathrm{Im}\, f$ je invariantní podprostor. Dokažte.

(5) Buď $v \in V$ libovolný vektor. Dokažte, že $[\![v, f(v), f(f(v)), f(f(f(v))), \ldots]\!]$ je invariantní podprostor.

(6) Nechť lineární transformace $f, g : V \longrightarrow V$ komutují, to jest, $f \circ g = g \circ f$. Buď $U \subseteq V$ invariantní podprostor vzhledem k transformaci $f$. Pak je $gU$ invariantní podprostor i vzhledem k transformaci $f$.

Rozklad prostoru $V$ na přímý součet invariantních podprostorů vede ke zjednodušení matice transformace $f$.

**1.2. Tvrzení.** *Nechť existuje přímý rozklad $V = U_1 \dotplus U_2$, kde $U_1, U_2$ jsou invariantní podprostory. Zvolme nějakou bázi $e_1, \ldots, e_m$ v podprostoru $U_1$ a nějakou bázi $e_{m+1}, \ldots, e_n$ v podprostoru $U_2$. Pak $e_1, \ldots, e_n$ je báze v prostoru $V$ a transformace $f$ v ní má matici tvaru*

$$A = \begin{pmatrix} a_{11} & \cdots & a_{1m} & 0 & \cdots & 0 \\ \vdots & & \vdots & \vdots & & \vdots \\ a_{m1} & \cdots & a_{mm} & 0 & \cdots & 0 \\ 0 & \cdots & 0 & a_{m+1,m+1} & \cdots & a_{m+1,n} \\ \vdots & & \vdots & \vdots & & \vdots \\ 0 & \cdots & 0 & a_{n,m+1} & \cdots & a_{nn} \end{pmatrix}.$$

*Označíme-li*

$$A_1 = \begin{pmatrix} a_{11} & \cdots & a_{1m} \\ \vdots & & \vdots \\ a_{m1} & \cdots & a_{mm} \end{pmatrix}, \qquad A_2 = \begin{pmatrix} a_{m+1,m+1} & \cdots & a_{m+1,n} \\ \vdots & & \vdots \\ a_{n,m+1} & \cdots & a_{nn} \end{pmatrix}.$$

*pak $A_i$ je matice lineární transformace $f|_{U_i}$.*

**1.3. Důkaz.** Jako cvičení ověřte, že $e_1, \ldots, e_n$ je báze v prostoru $V$.

Ohledně matice $A$ víme, že prvních $m$ jejích sloupců je tvořeno souřadnicemi vektorů $f(e_1), \ldots, f(e_m)$ v bázi $e_1, \ldots, e_n$. Vektory $f(e_1), \ldots, f(e_m)$ ovšem leží v podprostoru $U_1$ s bazí $e_1, \ldots, e_m$, takže zbývající bázové vektory $e_{m+1}, \ldots, e_n$ budou mít nulové koeficienty. Submatice $A_1$ je pak maticí zobrazení $f|_U$ v bázi $e_1, \ldots, e_m$ (ověřte). Zbytek analogicky.

O shora uvedené matici $A$ říkáme, že je v blokově diagonálním tvaru s bloky $A_1$, $A_2$ na diagonále. Stručně zapisujeme

$$A = \begin{pmatrix} A_1 & 0 \\ 0 & A_2 \end{pmatrix}$$

Říkáme též, že $A$ je *přímý součet submatic* $A_1$ a $A_2$.

Podobně se v případě přímého součtu $V = U_1 \dotplus \cdots \dotplus U_n$ invariantních podprostorů $U_1$, …, $U_n$, matice zobrazení $f$ rozpadá na přímý součet submatic $A_1, \ldots A_n$ odpovídajících lineárním zobrazením $f|_{U_1}$, …, $f|_{U_n}$:

$$A = \begin{pmatrix} A_1 & 0 & \cdots & 0 \\ 0 & A_2 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & A_n \end{pmatrix},$$

O matici $A$ pak rovněž pravíme, že je blokově diagonální.

Často se stává, že existuje dostatek jednorozměrných invariantních podprostorů (generovaných vlastními vektory), takže prostor $V$ lze rozložit na jejich přímý součet. Bloky jsou potom velikosti 1, a znovu dostáváme již známý případ diagonalizovatelné matice.

## 2. Anulující polynomy

Od tohoto místa se omezíme na případ lineární transformace $f : P^n \longrightarrow P^n$, $f(u) = Au$, kde $A$ je čtvercová matice. Poznamenejme, že každou lineární transformaci $f$ konečněrozměrného vektorového prostoru $V$ můžeme takto interpretovat. Stačí zvolit bázi prostoru $V$ a tím i izomorfismus $V \cong P^n$ a matici $A$ zavést jako matici lineárního zobrazení $f$ v této bázi. Nejde proto o žádné podstatné omezení.

Symbolem $P[x]$ označíme okruh polynomů jedné neurčité $x$ s koeficienty z pole $P$. Algebra polynomů bude vyložena v jiné přednášce; pro základní porozumění tomuto textu stačí vědět, že každý polynom $f \in P[x]$ lze rozložit na součin dále nerozložitelných činitelů. Ty jsou potom nutně po dvou nesoudělné (žádné dva nemají nekonstantního společného dělitele). Příkladem je *kořenový rozklad* polynomu $f \in \mathbf{C}[x]$:

$$f = (x - \xi_1)^{k_1}(x - \xi_2)^{k_2} \cdots (x - \xi_r)^{k_r},$$

kde $\xi_i \in \mathbf{C}$ jsou kořeny polynomu $f$ a $k_i$ jsou jejich násobnosti.

**2.1. Označení.** Buď $A$ čtvercová matice. Buď $p = a_m x^m + \cdots + a_1 x + a_0 \in P[x]$ polynom s koeficienty z pole $P$. Položme $p(A) = a_m A^m + \cdots + a_1 A + a_0 E$, kde $E$ je jednotková matice stejného rozměru jako matice $A$. Říkáme, že matice $p(A)$ je výsledkem dosazení matice $A$ do polynomu $p$.

**2.2. Tvrzení.** *Jsou-li $p, q \in P[x]$ dva polynomy, pak platí*

$$(p + q)(A) = p(A) + q(A), \qquad (pq)(A) = p(A)\, q(A)$$

*pro libovolnou čtvercovou matici $A$.*

**2.3. Důkaz.** Cvičení.

**2.4. Důsledek.** *Pro libovolnou čtvercovou matici $A$ máme*

$$p(A)\, q(A) = q(A)\, p(A),$$

*tj. matice získané dosazením $A$ do různých polynomů komutují.*

Může se stát, že dosazením do polynomu získáme nulovou matici.

**2.5. Definice.** Nechť $p \in P[x]$, $p \neq 0$. Řekneme, že $p$ je *anulující polynom* čtvercové matice $A$, jestliže $p(A) = 0$.

Z následujícího tvrzení vyplývá, že anulující polynom matice lineární transformace nezávisí na volbě báze.

**2.6. Tvrzení.** *Podobné matice mají stejné anulující polynomy.*

**2.7. Důkaz.** Platí $(Q^{-1}AQ)^i = Q^{-1}AQ \cdot Q^{-1}AQ \cdots Q^{-1}AQ = Q^{-1}A^iQ$, načež

$$\begin{aligned} p(Q^{-1}AQ) &= a_m(Q^{-1}AQ)^m + \cdots + a_1 Q^{-1}AQ + a_0 E \\ &= a_m Q^{-1}A^m Q + \cdots + a_1 Q^{-1}AQ + a_0 E \\ &= Q^{-1}(a_m A^m + \cdots + a_1 A + a_0 E)Q \\ &= Q^{-1}p(A)Q. \end{aligned}$$

Odtud tvrzení.

Později uvidíme, že všechny čtvercové matice mají nějaký anulující polynom $q$.

**2.8. Tvrzení.** *Buď $q$ anulující polynom matice $A$. Nechť existuje rozklad $q = q_1 q_2 \cdots q_m$, kde polynomy $q_1, \ldots, q_m$ jsou po dvou nesoudělné. Uvažujme o lineárním zobrazení $f_i : P^n \longrightarrow P^n$, $u \longmapsto q_i(A)u$. Označme $U_i = \operatorname{Ker} f_i \subseteq P^n$, $i = 1, \ldots, m$. Pak platí:*

(i) *Každý podprostor $U_i$ je invariantní;*

(ii) $P^n = U_1 \dot{+} \cdots \dot{+} U_m$;

(iii) *polynom $q_i$ je anulujícím polynomem matice transformace $f|_{U_i}$, pro každé $i = 1, \ldots, m$.*

**2.9. Důkaz.** (i) Nechť $u \in U_i$, tj. $q_i(A)u = 0$. Pak $q_i(A)Au = Aq_i(A)u = A0 = 0$ (použili jsme tvrzení, že $A$ a $q_i(A)$ spolu komutují). Tudíž, $Au \in U_i$.

(ii) Nejdříve případ $m = 2$. Nechť tedy $f = q_1 q_2$ a polynomy $q_1, q_2$ jsou nesoudělné. Pak existují polynomy $p_1, p_2$ takové, že $1 = q_1 p_1 + q_2 p_2$ (tento fakt bude dokázán v jiné přednášce; některé speciální případy jsou rozebrány ve cvičeních níže). Dosazením matice $A$ získáme rovnost

$$E = q_1(A)p_1(A) + q_2(A)p_2(A),$$

takže pro libovolný vektor $v \in V$ platí

$$v = q_1(A)p_1(A)v + q_2(A)p_2(A)v.$$

Ukažme, že první sčítanec $v_1 := q_1(A)p_1(A)v$ leží v $U_2$, to jest, že $v_1 \in \operatorname{Ker} q_2(A)$. Máme ale

$$q_2(A)v_1 = q_2(A)q_1(A)p_1(A)v = q(A)p_1(A)v = 0,$$

protože $q$ je anulující polynom pro $A$. Podobně se ukáže, že druhý ze sčítanců leží v $U_1$. Tudíž, $v \in U_1 + U_2$. Protože $v$ byl libovolný vektor z $V$, máme $V = U_1 + U_2$.

Ukažme ještě, že $U_1 \cap U_2 = 0$. Nechť tedy $v \in U_1 \cap U_2$, tj. $q_1(A)v = 0$ a $q_2(A)v = 0$. Máme $E = q_1(A)p_1(A) + q_2(A)p_2(A) = p_1(A)q_1(A) + p_2(A)q_2(A)$ (protože $p_i(A)$ a $q_i(A)$ spolu komutují), načež

$$v = p_1(A)q_1(A)v + p_2(A)q_2(A)v = p_1(A)0 + p_2(A)0 = 0.$$

Dokázali jsme tedy, že $V = U_1 \dot{+} U_2$.

Obecný případ $m > 2$ se dokáže indukcí (cvičení).

(iii) Zvolme báze $v_{i1}, \ldots, v_{ir_i}$ v prostorech $U_i$, $r_i = \dim U_i$, $r_1 + \cdots r_m = n$. Jak víme, v bázi tvořené těmito vektory je matice $A$ blokově diagonální a jejím $i$tým blokem je právě matice $A_i$ transformace $f|_{U_i}$ v bázi $v_{i1}, \ldots, v_{ir_i}$. Ukažme, že polynom $q_i$ je anulujícím polynomem matice $A_i$.

Snadno se vidí, že matice $q_i(A)$ je blokově diagonální matice s bloky $q_i(A_1), \ldots, q_i(A_m)$. Protože však $U_i = \operatorname{Ker} q_i(A)$, je blok $q_i(A)$ odpovídající podprostoru $U_i$ nulový, což se mělo dokázat.

Podmínkám předchozího tvrzení vyhovuje například rozklad na kořenové činitele $(x-a)^m$.

**Problém.** Ukažte, že $(x-a)^m u + (x-b)^n v = \text{const}$, pokud

$$u = \sum_{i=0}^{n-1} \frac{(m-1+i)!}{(m-1)!\,i!}(b-x)^i(b-a)^{n-1-i},$$

$$v = \sum_{i=0}^{m-1} \frac{(n-1+i)!}{(n-1)!\,i!}(a-x)^i(a-b)^{m-1-i}.$$

K nalezení právě uvedeného rozkladu musíme znát alespoň jeden anulující polynom.

**2.10. Věta Hamilton–Cayleyova.** *Charakteristický polynom čtvercové matice nad $P$ je jejím anulujícím polynomem.*

**2.11. Důkaz.** Pro libovolnou čtvercovou matici $B$ jsme kdysi odvodili vztah $B \cdot \operatorname{adj} B = \det B \cdot E$. Dosaďme za $B$ matici $A - xE$:

$$(A - xE) \cdot \operatorname{adj}(A - xE) = \chi_A(x) \cdot E.$$

Je-li matice $A$ typu $n/n$, pak je její charakteristický polynom $\chi_A$ polynomem stupně $n$, řekněme $\chi_A = c_n x^n + \cdots + c_1 x + c_0$. Dále je (z definice adjungované matice) jasné, že prvky matice $\operatorname{adj}(A - xE)$ jsou polynomy stupně $n-1$ v $x$. Sdružíme-li sčítance s týmiž mocninami $x$, získáme vyjádření $\operatorname{adj}(A - xE) = C_{n-1}x^{n-1} + \cdots + C_1 x + C_0$, kde $C_i$ jsou čtvercové matice typu $n/n$.

Po dosazení máme

$$(A - xE) \cdot (C_{n-1}x^{n-1} + \cdots + C_1 x + C_0) = (c_n x^n + \cdots + c_1 x + c_0) \cdot E,$$

tj.

$$\begin{aligned} &-C_{n-1}x^n + (AC_{n-1} - C_{n-2})x^{n-1} + \cdots + (AC_1 - C_0)x + AC_0 \\ &\qquad = c_n E x^n + \cdots + c_1 E x + c_0 E. \end{aligned}$$

Porovnáním koeficientů u stejných mocnin $x$ obdržíme

$$\begin{aligned} -C_{n-1} &= c_n E, \\ -C_{n-2} + AC_{n-1} &= c_{n-1}, \\ &\vdots \\ -C_0 + AC_1 &= c_1 \\ AC_0 &= c_0. \end{aligned}$$

Vynásobíme-li $i$-tou rovnost $i$-tou mocninou $A^i$ matice $A$ a vzniklé rovnosti sečteme, získáme

$$0 = c_n A^n + c_{n-1}A^{n-1} + c_1 A + c_0,$$

což se mělo dokázat.

**2.12. Důsledek.** *Charakteristický polynom čtvercové matice je jejím anulujícím polynomem.*

**Příklad.** Nechť

$$A = \begin{pmatrix} 1 & -1 & 1 \\ 0 & 2 & -1 \\ -1 & 0 & 2 \end{pmatrix}.$$

Charakteristický polynom je $\chi_A = x^3 - 5x^2 + 9x - 5 = (x-1)(x^2 - 4x + 5)$ (ověřte). Vidíme, že $\chi_A$ je součinem nesoudělných polynomů $q_1 = x - 1$ a $q_2 = x^2 - 4x + 5$.

Počítejme $U_1 = \operatorname{Ker} q_1(A) = \operatorname{Ker}(A - E)$. Jádro $\operatorname{Ker}(A-E)$ vypočteme řešením homogenní soustavy s maticí

$$q_1(A) = A - E = \begin{pmatrix} 1 & -1 & 1 \\ 0 & 2 & -1 \\ -1 & 0 & 2 \end{pmatrix} - \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & -1 & 1 \\ 0 & 1 & -1 \\ -1 & 0 & 1 \end{pmatrix}$$

a fundamentálním řešením $e_1 = (1,1,1)$ (ověřte). Dostáváme jednorozměrný invariantní podprostor

$$U_1 = \operatorname{Ker} q_1(A) = [[(1,1,1)]].$$

Podobně $U_2 = \operatorname{Ker} q_2(A) = \operatorname{Ker}(A^2 - 4A + 5E)$. Toto jádro vypočteme řešením homogenní soustavy s maticí

$$q_2(A) = A^2 - 4A + 5E = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 1 & 0 \\ 1 & 1 & 0 \end{pmatrix}$$

a fundamentálním řešením $e_2 = (0,0,1)$, $e_3 = (1,-1,0)$ (ověřte). Dostáváme dvourozměrný invariantní podprostor

$$U_2 = \operatorname{Ker} q_2(A) = [[(0,0,1),(1,-1,0)]],$$

Získali jsme:

(a) přímý rozklad $\mathbf{R}^3 = U_1 \dot{+} U_2$ na invariantní podprostory $U_1$ a $U_2$;

(b) bázi $e_1, e_2, e_3$ s maticí přechodu

$$Q = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 0 & -1 \\ 1 & 1 & 0 \end{pmatrix}$$

v níž má zobrazení $\alpha$ blokově diagonální matici

$$Q^{-1}AQ = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & -1 \\ 0 & 1 & 2 \end{pmatrix}.$$

## 3. Minimální polynom

**Příklad.** Matice

$$A = \begin{pmatrix} -1 & 0 & 2 \\ -2 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix}$$

má anulující polynom $q = x^2 - 1 = (x+1)(x-1)$ (ověřte). Charakteristický polynom matice $A$ je $\chi_A = x^3 - x^2 - x + 1 = (x+1)(x-1)^2$.

Poslední příklad ukazuje, že charakteristický polynom může mít netriviálního dělitele, který je rovněž anulujícím polynomem. Ukažme, že mezi anulujícími polynomy existuje jeden, který dělí všechny ostatní.

**3.1. Definice.** Anulující polynom se nazývá *minimální polynom*, je-li nejmenšího stupně ze všech anulujících polynomů.

Ke každé čtvercové matici $A$ existuje anulující, a proto i minimální polynom.

**3.2. Tvrzení.** *Každý anulující polynom je dělitelný minimálním polynomem.*

**3.3. Důkaz.** Bud' $f$ anulující polynom matice $A$, bud' $g$ minimální polynom matice $A$. Dělme se zbytkem: $f = qg + r$, kde $r = 0$ nebo je stupeň polynomu $r$ ostře menší, než stupeň polynomu $g$. V případě $r = 0$ jsme hotovi. Připusťme opak, tj. $r \neq 0$. Potom

$$0 = f(A) = q(A)g(A) + r(A) = r(A),$$

protože $g(A) = 0$. Tudíž, $r$ je anulující polynom nižšího stupně než polynom $g$, a to je spor.