21. POLYNOMICKÉ INVARIANTY PODOBNOSTI MATÍC

V tejto kapitole najprv prirodzene rozšírime oblasť pôsobnosti polynomických funkcií aj na maticové resp. operátorové argumenty. To nám umožní dokázať kľúčovú vlastnosť charakteristického polynómu, známu pod názvom *Cayleyho-Hamiltonova veta*, a zaviesť ďalší dôležitý polynomický invariant podobnosti matíc – tzv. *minimálny polynóm*.

V druhej polovici sa informatívne oboznámime s dvoma typmi sústav polynómov, z ktorých každá úplným a jednoznačným spôsobom charakterizuje triedu všetkých matíc daného lineárneho operátora resp. triedu všetkých matíc podobných s danou štvorcovou maticou. Na ich základe potom zostrojíme dva nové typy kanonických tvarov matíc lineárnych operátorov, ktorých určenie si – na rozdiel od Jordanovho kanonického tvaru – nevyžaduje znalosť spektra a nevybočuje z pôvodného poľa. Vopred prezraďme aspoň ich názvy: pôjde o tzv. *sústavu elementárnych deliteľov* a *sústavu invariantných faktorov*, ku ktorým prislúcha tzv. *primárny kanonický tvar* resp. *racionálny kanonický tvar matice.*

21.1. Polynomické maticové funkcie

Každý polynóm $f(x) = c_0 + c_1x + \ldots + c_mx^m = \sum_{i=0}^{m} c_ix^i$ nad poľom K prirodzene definuje (rovnako značenú) funkciu $f\colon K \to K$ danú dosadením hodnoty $a \in K$ za premennú x, t. j. $f(a) = c_0 + c_1a + \ldots + c_ma^m = \sum_{i=0}^{m} c_ia^i$. Tak isto však môžeme do polynómu $f(x)$ dosadiť za premennú x ľubovoľnú štvorcovú maticu $\boldsymbol{A} \in K^{n\times n}$. Tým dostaneme *polynomickú maticovú funkciu* $f\colon K^{n\times n} \to K^{n\times n}$ danú predpisom

$$f(\boldsymbol{A}) = c_0\boldsymbol{I} + c_1\boldsymbol{A} + \ldots + c_m\boldsymbol{A}^m = \sum_{i=0}^{m} c_i\boldsymbol{A}^i.$$

Podobne definuje polynóm $f(x)$ funkciu $f\colon \mathcal{L}(V,V) \to \mathcal{L}(V,V)$ na vektorovom priestore $\mathcal{L}(V,V)$ všetkých lineárnych operátorov $\varphi\colon V \to V$. Stačí položiť

$$f(\varphi) = c_0 \operatorname{id}_V + c_1\varphi + \ldots + c_m\varphi^m = \sum_{i=0}^{m} c_i\varphi^i,$$

kde φ^i je i-ta iterácia operátora φ, t.j. $\varphi^0 = \operatorname{id}_V$, $\varphi^1 = \varphi$, $\varphi^2 = \varphi\circ\varphi$, atď.

Keďže v centre našej našej pozornosti zostávajú i naďalej konečnorozmerné vektorové priestory, obmedzíme sa na štúdium maticových funkcií, ktoré sú o niečo názornejšie, a uspokojíme sa s poznámkou, že príslušné výsledky možno na operátorové funkcie jednoducho preniesť na základe vzájomne jednoznačnej korešpondencie medzi operátormi $\varphi \in \mathcal{L}(V,V)$ a maticami $\boldsymbol{A} \in K^{n\times n}$ (danej voľbou vhodnej bázy n-rozmerného priestoru V).

Naše štúdium polynomických maticových funkcií začneme niekoľkými jednoduchými pozorovaniami, ktoré navyše plne oprávňujú takýto prístup.

21.1.1. Tvrdenie. *Nech $f(x) \in K[x]$, $\boldsymbol{A}, \boldsymbol{P} \in K^{n\times n}$, pričom $\boldsymbol{P}$ je regulárna. Potom*

$$f\big(\boldsymbol{P}\cdot\boldsymbol{A}\cdot\boldsymbol{P}^{-1}\big) = \boldsymbol{P}\cdot f(\boldsymbol{A})\cdot\boldsymbol{P}^{-1}.$$

Dôkaz. Stačí si uvedomiť, že

$$\big(\boldsymbol{P}\cdot\boldsymbol{A}\cdot\boldsymbol{P}^{-1}\big)^2 = \boldsymbol{P}\cdot\boldsymbol{A}\cdot\boldsymbol{P}^{-1}\cdot\boldsymbol{P}\cdot\boldsymbol{A}\cdot\boldsymbol{P}^{-1} = \boldsymbol{P}\cdot\boldsymbol{A}^2\cdot\boldsymbol{P}^{-1},$$

pričom tento vzťah možno zrejmým spôsobom zovšeobecniť aj na vyššie mocniny. Dokončenie dôkazu už možno prenechať čitateľovi.

21.1.2. Dôsledok. *Nech $f(x) \in K[x]$, $\boldsymbol{A}, \boldsymbol{B} \in K^{n\times n}$. Potom*

$$\boldsymbol{A} \approx \boldsymbol{B} \;\Rightarrow\; f(\boldsymbol{A}) \approx f(\boldsymbol{B}).$$

Taktiež jednoduchý dôkaz nasledujúcej lemy prenechávame ako cvičenie čitateľovi.

21.1.3. Lema. *Nech $f(x) \in K[x]$, $\boldsymbol{A}_1 \in K^{n_1\times n_1}$, … , $\boldsymbol{A}_k \in K^{n_k\times n_k}$. Potom*

$$f\big(\operatorname{diag}(\boldsymbol{A}_1,\dots,\boldsymbol{A}_k)\big) = \operatorname{diag}\big(f(\boldsymbol{A}_1),\dots,f(\boldsymbol{A}_k)\big).$$

Teraz už môžeme uviesť nasledujúci efektný výsledok.

21.1.4. Veta. *(Cayley-Hamilton) Pre ľubovoľnú maticu $\boldsymbol{A} \in K^{n\times n}$ platí*

$$\mathrm{ch}_{\boldsymbol{A}}(\boldsymbol{A}) = \boldsymbol{0},$$

t. j. matica $\boldsymbol{A}$ vyhovuje svojej charakteristickej rovnici.

V dôkaze využijeme poznatky o Jordanovom kanonickom tvare z predchádzajúcej kapitoly.

Nech L je konečné rozšírenie poľa K, v ktorom má $\boldsymbol{A}$ spektrum plnej algebraickej váhy n. Označme $\boldsymbol{J} = \operatorname{diag}\big(\boldsymbol{J}_{n_1}(\lambda_1),\dots,\boldsymbol{J}_{n_k}(\lambda_k)\big) \in L^{n\times n}$ Jordanov kanonický tvar matice $\boldsymbol{A}$ a $\boldsymbol{P} \in L^{n\times n}$ regulárnu maticu, ktorej stĺpce tvoria vektory príslušnej Jordanovej bázy. Potom $\boldsymbol{A} = \boldsymbol{P}\cdot\boldsymbol{J}\cdot\boldsymbol{P}^{-1}$, $\mathrm{ch}_{\boldsymbol{A}}(x) = \mathrm{ch}_{\boldsymbol{J}}(x)$ a podľa tvrdenia 21.1.1

$$\mathrm{ch}_{\boldsymbol{A}}(\boldsymbol{A}) = \mathrm{ch}_{\boldsymbol{J}}(\boldsymbol{A}) = \boldsymbol{P}\cdot\mathrm{ch}_{\boldsymbol{J}}(\boldsymbol{J})\cdot\boldsymbol{P}^{-1}.$$

Stačí teda dokázať rovnosť $\mathrm{ch}_{\boldsymbol{J}}(\boldsymbol{J}) = \boldsymbol{0}$ pre matice v JKT. Z tvrdenia 19.1.1 vyplýva

$$\mathrm{ch}_{\boldsymbol{J}}(x) = \mathrm{ch}_{\boldsymbol{J}_1}(x)\dots\mathrm{ch}_{\boldsymbol{J}_k}(x) = (\lambda_1 - x)^{n_1}\dots(\lambda_k - x)^{n_k},$$

kde $\boldsymbol{J}_i = \boldsymbol{J}_{n_i}(\lambda_i)$ pre $1 \le i \le k$. Teda podľa lemy 21.1.3 je $\mathrm{ch}_{\boldsymbol{J}}(\boldsymbol{J})$ blokovo diagonálna matica s diagonálnymi blokmi

$$\mathrm{ch}_{\boldsymbol{J}}(\boldsymbol{J}_i) = (\lambda_1\boldsymbol{I}_{n_i} - \boldsymbol{J}_i)^{n_1}\dots(\lambda_k\boldsymbol{I}_{n_i} - \boldsymbol{J}_i)^{n_k}$$

pre $1 \le i \le k$. V i-tom bloku sa ako i-ty činiteľ nachádza mocnina $(\lambda_i\boldsymbol{I}_{n_i} - \boldsymbol{J}_i)^{n_i} = \boldsymbol{0}$ nilpotentnej matice $\lambda_i\boldsymbol{I}_{n_i} - \boldsymbol{J}_i = -\boldsymbol{J}_{n_i}(0)$ rádu n_i (pozri začiatok paragrafu 20.5). Preto každý blok i celý výraz $\mathrm{ch}_{\boldsymbol{J}}(\boldsymbol{J})$ sú nevyhnutne nulové matice.

Caylyeho-Hamiltonovu vetu možno využiť na výpočet mocnín štvorcových matíc.

21.1.5. Príklad. Matica

$$\boldsymbol{A} = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 2 & -2 \\ -1 & 3 & 0 \end{pmatrix} \in \mathbb{R}^{3\times 3}$$

má charakteristický polynóm

$$\mathrm{ch}_{\boldsymbol{A}}(x) = \det(\boldsymbol{A} - x\boldsymbol{I}) = 8 - 7x + 3x^2 - x^3.$$

Preto

$$\begin{aligned} \boldsymbol{A}^3 &= 8\boldsymbol{I} - 7\boldsymbol{A} + 3\boldsymbol{A}^2, \\ \boldsymbol{A}^4 &= 8\boldsymbol{A} - 7\boldsymbol{A}^2 + 3\boldsymbol{A}^3 = 8\boldsymbol{A} - 7\boldsymbol{A}^2 + 24\boldsymbol{I} - 21\boldsymbol{A} + 9\boldsymbol{A}^2 \\ &= 24\boldsymbol{I} - 13\boldsymbol{A} + 2\boldsymbol{A}^2, \\ \boldsymbol{A}^5 &= 24\boldsymbol{A} - 13\boldsymbol{A}^2 + 2\boldsymbol{A}^3 = 24\boldsymbol{A} - 13\boldsymbol{A}^2 + 16\boldsymbol{I} - 14\boldsymbol{A} + 6\boldsymbol{A}^2 \\ &= 16\boldsymbol{I} + 10\boldsymbol{A} - 7\boldsymbol{A}^2, \qquad \text{atď.} \end{aligned}$$

Všetky vyššie mocniny matice $\boldsymbol{A}$ teda možno vyjadriť pomocou jej nultej, prvej a druhej mocniny, presnejšie, ako hodnoty vhodných polynómov nanajvýš druhého stupňa pre maticu $\boldsymbol{A}$.

V prípade, že poznáme JKT matice $\boldsymbol{A} \in K^{n\times n}$ a príslušnú maticu prechodu, máme k dispozícii ešte efektívnejší spôsob výpočtu hodnôt $f(\boldsymbol{A})$ pre polynómy $f(x) = \sum_{i=0}^{m} c_i x^i \in K[x]$. Ak $\boldsymbol{J} = \operatorname{diag}\big(\boldsymbol{J}_{n_1}(\lambda_1), \dots, \boldsymbol{J}_{n_k}(\lambda_k)\big)$ je JKT matice $\boldsymbol{A}$ a $\boldsymbol{P}$ je príslušná matica prechodu, t. j. $\boldsymbol{A} = \boldsymbol{P} \cdot \boldsymbol{J} \cdot \boldsymbol{P}^{-1}$, tak podľa tvrdenia 21.1.1 a lemy 21.1.3 platí

$$f(\boldsymbol{A}) = \boldsymbol{P} \cdot f(\boldsymbol{J}) \cdot \boldsymbol{P}^{-1} = \boldsymbol{P} \cdot \operatorname{diag}\Big(f\big(\boldsymbol{J}_{n_1}(\lambda_1)\big), \dots, f\big(\boldsymbol{J}_{n_k}(\lambda_k)\big)\Big) \cdot \boldsymbol{P}^{-1}.$$

Preto sa stačí naučiť počítať hodnoty polynómov pre Jordanove bunky $\boldsymbol{J}_n(\lambda)$. Samozrejme, začneme polynómami x^m. Na výpočet mocniny $\boldsymbol{J}_n(\lambda)^m$ sa nám zíde nasledujúca maticová verzia *binomickej vety*, ktorú možno dokázať indukciou rovnako ako binomickú vetu v príslušnom poli. Hovoríme, že matice $\boldsymbol{A}$, $\boldsymbol{B} \in K^{n\times n}$ *komutujú*, ak $\boldsymbol{A} \cdot \boldsymbol{B} = \boldsymbol{B} \cdot \boldsymbol{A}$.

21.1.6. Lema. *Nech matice $\boldsymbol{A}$, $\boldsymbol{B} \in K^{n\times n}$ komutujú. Potom pre ľubovoľné $m \in \mathbb{N}$ platí*

$$(\boldsymbol{A} + \boldsymbol{B})^m = \sum_{i=0}^{m} \binom{m}{i} \boldsymbol{A}^{m-i} \boldsymbol{B}^i.$$

Ak si ešte uvedomíme, že $\boldsymbol{J}_n(\lambda) = \lambda \boldsymbol{I}_n + \boldsymbol{J}_n(0) = \lambda \boldsymbol{I}_n + \boldsymbol{J}_n$, pričom $(\lambda \boldsymbol{I}_n) \cdot \boldsymbol{A} = \lambda \boldsymbol{A} = \boldsymbol{A} \cdot (\lambda \boldsymbol{I}_n)$, teda matica $\lambda \boldsymbol{I}_n$ komutuje s každou maticou $\boldsymbol{A} \in \boldsymbol{K}^{n\times n}$, okamžite z toho dostávame

$$\boldsymbol{J}_n(\lambda)^m = \sum_{i=0}^{m} \binom{m}{i} \lambda^{m-i} \boldsymbol{J}_n^i.$$

Mocniny nilpotentej matice $\boldsymbol{J}_n$ už vypočítame ľahko na základe vzťahov

$$\boldsymbol{J}_n^m \cdot \boldsymbol{e}_i = \begin{cases} \mathbf{0}, & \text{pre } 1 \leq i \leq m, \\ \boldsymbol{e}_{i+m}, & \text{pre } m \leq i \leq n. \end{cases}$$

Takže pre $m \geq n$ je $\boldsymbol{J}_n^m = \mathbf{0}$, a pre $0 \leq m < n$ je to bloková matica

$$\boldsymbol{J}_n^m = \begin{pmatrix} \mathbf{0}_{n-m\,m} & \boldsymbol{J}_{n-m} \\ \mathbf{0}_{m\,m} & \mathbf{0}_{m\,n-m} \end{pmatrix}.$$

Po dosadení do binomickej vety a sčítaní všetkých členov dostávame hľadaný vzorec.

21.1.7. Lema. *Pre ľubovoľné $m, n \in \mathbb{N}$, $n \geq 1$, $\lambda \in K$ platí*

$$\boldsymbol{J}_n(\lambda)^m = \begin{pmatrix} \lambda^m & \binom{m}{1}\lambda^{m-1} & \dots & \binom{m}{n-1}\lambda^{m-n+1} \\ 0 & \lambda^m & \dots & \binom{m}{n-2}\lambda^{m-n+2} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & \lambda^m \end{pmatrix},$$

pričom pre $j > m$ definitoricky kladieme $\binom{m}{j}\lambda^{m-j} = 0$.

Pre polynóm $f(x) = \sum_{i=0}^m c_i x^i \in K[x]$ definujeme jeho *formálnu p-tu deriváciu* ako polynóm

$$f^{(p)}(x) = \sum_{i=p}^{m} i(i-1)\dots(i-p+1)c_i x^{i-p} = \sum_{i=0}^{m-p} \frac{(i+p)!}{i!} c_{i+p} x^i;$$

pre $i = 1$ samozrejme píšeme $f^{(1)}(x) = f'(x)$. Pre $K = \mathbb{R}$ formálna derivácia splýva s obvyklou deriváciou $f^{(p)}(x) = \mathrm{d}^p f(x)/\,\mathrm{d}x^p$, definovanou pomocou známej limity.

Všimnime si, že prvky matice $\boldsymbol{J}_n(\lambda)^m$ možno vyjadriť aj pomocou formálnych derivácií polynómu $f(x) = x^m$ v bode $x = \lambda$:

$$\binom{m}{j}\lambda^{m-j} = \frac{1}{j!} f^{(j)}(\lambda).$$

Z toho a lineárnosti operátora derivácie už priamo vyplýva nasledujúci všeobecný vzorec.

21.1.8. Veta. *Nech $f(x) \in K[x]$ je ľubovoľný polynóm, $\lambda \in K$ a $1 \leq n \in \mathbb{N}$. Potom*

$$f\big(\boldsymbol{J}_n(\lambda)\big) = \begin{pmatrix} f(\lambda) & \frac{1}{1!}f'(\lambda) & \dots & \frac{1}{(n-1)!}f^{(n-1)}(\lambda) \\ 0 & f(\lambda) & \dots & \frac{1}{(n-2)!}f^{(n-2)}(\lambda) \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & f(\lambda) \end{pmatrix}.$$

Keby sa niekomu zdal tento vzorec príliš komplikovaný, snáď ho uteší, ak mu pripomenieme, že „typická“ štvorcová matica nad $\mathbb{R}$ či $\mathbb{C}$ je podobná s diagonálnou. Pre $\boldsymbol{A} = \boldsymbol{P} \cdot \operatorname{diag}(\lambda_1, \dots, \lambda_n) \cdot \boldsymbol{P}^{-1}$, máme $f(\boldsymbol{A}) = \boldsymbol{P} \cdot \operatorname{diag}\big(f(\lambda_1), \dots, f(\lambda_n)\big) \cdot \boldsymbol{P}^{-1}$, a basta.

21.2. Minimálny polynóm

Charakteristický polynóm štvorcovej matice $\boldsymbol{A}$ nie je nevyhnutne polynómom najnižšieho možného stupňa, ktorý anuluje maticu $\boldsymbol{A}$. Napríklad charakteristický polynóm matice $\boldsymbol{J} = \operatorname{diag}\big(\boldsymbol{J}_m(\lambda), \boldsymbol{J}_n(\lambda)\big)$ v JKT je zrejme $(\lambda - x)^{m+n}$. Avšak už polynóm $f(x) = (\lambda - x)^{\max(m,n)}$ ju anuluje, t. j. platí $f(\boldsymbol{J}) = \boldsymbol{0}$.

Minimálnym polynómom matice $\boldsymbol{A} \in K^{n\times n}$ nazývame polynóm nad K najnižšieho možného stupňa, ktorý anuluje maticu $\boldsymbol{A}$ a je navyše *normovaný* (t. j. rôzny od 0 a s koeficientom 1 pri najvyššej mocnine x).

Keďže napríklad $(-1)^n \operatorname{ch}_{\boldsymbol{A}}(x)$ je normovaný polynóm anulujúci maticu $\boldsymbol{A} \in K^{n\times n}$, minimálny polynóm matice $\boldsymbol{A}$ určite existuje a má stupeň $\leq n$. Taktiež ľahko nahliadneme, že je určený jednoznačne. Keby totiž $f(x)$, $g(x)$ boli dva rôzne minimálne polynómy matice $\boldsymbol{A}$, tak by museli mať rovnaký stupeň. Potom by však vhodný skalárny násobok polynómu $f(x) - g(x)$ bol normovaný polynóm nižšieho stupňa, ktorý tiež anuluje maticu $\boldsymbol{A}$.

To nás oprávňuje zaviesť pre minimálny polynóm matice $\boldsymbol{A}$ označenie $\mu_{\boldsymbol{A}}(x)$. Celkom obdobne možno definovať aj *minimálny polynóm* $\mu_\varphi(x)$ *lineárneho operátora* φ na konečnorozmernom vektorovom priestore V.

Z tvrdenia 21.1.1 okamžite vyplýva očakávaný výsledok.

21.2.1. Tvrdenie. *Podobné matice majú rovnaký minimálny polynóm. Minimálny polynóm lineárneho operátora na konečnorozmernom vektorovom priestore sa rovná minimálnemu polynómu jeho matice vzhľadom na ľubovoľnú bázu.*

Minimálny polynóm je tak popri charakteristickom polynóme ďalším dôležitým invariantom podobnosti matíc.

21.2.2. Tvrdenie. *Nech* $\boldsymbol{A} \in K^{n\times n}$, $f(x) \in K[x]$. *Potom* $f(\boldsymbol{A}) = \boldsymbol{0}$, *práve vtedy, keď minimálny polynóm* $\mu_{\boldsymbol{A}}(x)$ *delí polynóm* $f(x)$. *V dôsledku toho minimálny polynóm matice* $\boldsymbol{A}$ *delí jej charakteristický polynóm.*

Dôkaz. Zrejme stačí dokázať prvú časť tvrdenia, a v tej je netriválna len jedna implikácia. Nech teda $f(\boldsymbol{A}) = \boldsymbol{0}$. Označme $r(x) \in K[x]$ zvyšok po delení polynómu $f(x)$ minimálnym polynómom $\mu_{\boldsymbol{A}}(x)$. Teda stupeň $r(x)$ je menší ako stupeň $\mu_{\boldsymbol{A}}(x)$ a existuje čiastočný podiel $q(x) \in K[x]$ taký, že $f(x) = q(x)\,\mu_{\boldsymbol{A}}(x) + r(x)$. Potom $r(\boldsymbol{A}) = f(\boldsymbol{A}) - q(\boldsymbol{A})\,\mu_{\boldsymbol{A}}(\boldsymbol{A}) = \boldsymbol{0}$, takže nevyhnutne $r(x) = 0$, čiže $\mu_{\boldsymbol{A}}(x)$ delí $f(x)$. V opačnom prípade by totiž vhodný skalárny násobok nenulového zvyšku $r(x)$ bol normovaný polynóm nižšieho stupňa ako $\mu_{\boldsymbol{A}}(x)$ anulujúci maticu $\boldsymbol{A}$.

Minimálny polynóm matice možno určiť z jej Jordanovho kanonického tvaru. Na to stačí poznať minimálny polynóm matíc v JKT. Jednoduchú odpoveď na túto otázku dáva nasledujúce tvrdenie. Jedna časť jeho dôkazu je v podstate zahrnutá v dôkaze vety 21.1.4, zvyšok vyplýva z tvrdenia 21.2.2 a z faktu, že polynóm $(x - \lambda)^m$ pre $m < n$ neanuluje Jordanovu bunku $\boldsymbol{J}_n(\lambda)$.

21.2.3. Tvrdenie. *Nech* $\boldsymbol{J} = \operatorname{diag}\big(\boldsymbol{J}_{n_1}(\lambda_1), \dots, \boldsymbol{J}_{n_k}(\lambda_k)\big)$ *je JKT matice* $\boldsymbol{A} \in K^{n\times n}$. *Potom minimálny polynóm* $\mu_{\boldsymbol{A}}(x) = \mu_{\boldsymbol{J}}(x)$ *je súčinom mocnín* $(x-\lambda)^{m(\lambda)}$ *lineárnych faktorov* $x - \lambda$ *s exponentmi* $m(\lambda) = \max\{n_i;\ \lambda_i = \lambda\}$ *pre* $\lambda \in \operatorname{Spec}\boldsymbol{A}$.

Na druhej strane, charakteristický polynóm $\mathrm{ch}_{\boldsymbol{A}}(x) = \mathrm{ch}_{\boldsymbol{J}}(x)$ je v takom prípade súčinom mocnín $(\lambda - x)^{n(\lambda)}$ (až na znamienko) rovnakých lineárnych faktorov s exponentmi $n(\lambda) = \sum_{\lambda_i=\lambda} n_i$.

21.2.4. Dôsledok. *Pre maticu $\boldsymbol{A} \in K^{n\times n}$ platí $\mu_{\boldsymbol{A}}(x) = (-1)^n \,\mathrm{ch}_{\boldsymbol{A}}(x)$ práve vtedy, keď sa v JKT matice $\boldsymbol{A}$ každá vlastná hodnota $\lambda \in \operatorname{Spec} \boldsymbol{A}$ vyskytuje v práve jednej Jordanovej bunke $\boldsymbol{J}_{n_i}(\lambda_i)$.*

Napr. charakteristický polynóm matice $\boldsymbol{I}_4$ je $(x-1)^4$, kým jej minimálny polynóm je „len“ $x - 1$. Na druhej strane, pre diagonálnu maticu $\boldsymbol{A} = \operatorname{diag}(0, 1, 2, 3)$ platí $\mathrm{ch}_{\boldsymbol{A}}(x) = x(x-1)(x-2)(x-3) = \mu_{\boldsymbol{A}}(x)$.

Ukážeme si, že každý normovaný polynóm

$$f(x) = x^n - c_1x^{n-1} - \ldots - c_{n-1}x - c_n \in K[x]$$

je minimálnym polynómom vhodnej matice $\boldsymbol{A} \in K^{n\times n}$. Označme

$$\boldsymbol{M}_f = \begin{pmatrix} c_1 & 1 & 0 & \ldots & 0 \\ c_2 & 0 & 1 & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ c_{n-1} & 0 & 0 & \ldots & 1 \\ c_n & 0 & 0 & \ldots & 0 \end{pmatrix};$$

maticu $\boldsymbol{M}_f$ nazývame *pridruženou maticou polynómu* $f(x)$.

Napríklad pridruženou maticou polynómu x^n je Jordanova bunka $\boldsymbol{J}_n(0)$.

21.2.5. Tvrdenie. *Nech $f(x) \in K^{(n)}[x]$ je normovaný polynóm. Potom $f(x)$ je minimálnym polynómom svojej pridruženej matice $\boldsymbol{M}_f$; jej charakteristický polynóm je $(-1)^n f(x)$.*

Dôkaz. Nech $f(x) = x^n - \sum_{i=1}^n c_i x^{n-i}$. Matica $\boldsymbol{M}_f$ zobrazuje vektory kanonickej bázy $\boldsymbol{\varepsilon}$ v K^n podľa schémy

$$\boldsymbol{e}_n \mapsto \boldsymbol{e}_{n-1} \mapsto \ldots \mapsto \boldsymbol{e}_2 \mapsto \boldsymbol{e}_1 \mapsto (c_1, c_2 \ldots, c_{n-1}, c_n)^T,$$

z ktorej vyplývajú rovnosti $\boldsymbol{e}_i = \boldsymbol{M}_f^{n-i} \cdot \boldsymbol{e}_n$, pre $1 \le i \le n$, a tiež

$$\boldsymbol{M}_f^n \cdot \boldsymbol{e}_n = \boldsymbol{M}_f \cdot \boldsymbol{e}_1 = \sum_{i=1}^n c_i \boldsymbol{e}_i = \sum_{i=1}^n c_i \boldsymbol{M}_f^{n-i} \cdot \boldsymbol{e}_n.$$

Keďže matice $\boldsymbol{M}_f$ a $f(\boldsymbol{M}_f)$ zrejme komutujú, platí

$$\begin{aligned} f(\boldsymbol{M}_f) \cdot \boldsymbol{e}_i &= f(\boldsymbol{M}_f) \cdot \boldsymbol{M}_f^{n-i} \cdot \boldsymbol{e}_n = \boldsymbol{M}_f^{n-i} \cdot f(\boldsymbol{M}_f) \cdot \boldsymbol{e}_n \\ &= \boldsymbol{M}_f^{n-i} \cdot \left(\boldsymbol{M}_f^n \cdot \boldsymbol{e}_n - \sum_{i=1}^n c_i \boldsymbol{M}_f^{n-i} \cdot \boldsymbol{e}_n \right) = \boldsymbol{0} \end{aligned}$$

pre každé $i \le n$, v dôsledku čoho $f(\boldsymbol{M}_f) = \boldsymbol{0}$.

Ak $g(x) = \sum_{i=0}^{m} d_i x^i$ je polynóm stupňa $m < n$, tak

$$g(\boldsymbol{M}_f) \cdot \boldsymbol{e}_n = \sum_{i=0}^{m} d_i \boldsymbol{M}_f^i \cdot \boldsymbol{e}_n = d_0 \boldsymbol{e}_n + d_1 \boldsymbol{e}_{n-1} + \ldots + d_m \boldsymbol{e}_{n-m}.$$

Z lineárnej nezávislosti vektorov $\boldsymbol{e}_{n-m}, \ldots, \boldsymbol{e}_n$ však vyplýva, že uvedená lineárna kombinácia sa môže rovnať $\mathbf{0}$, len ak sú všetky koeficienty d_i rovné 0, t. j. keď $g(x) = 0$. Teda $f(x)$ je naozaj minimálny polynóm matice $\boldsymbol{M}_f$.

Kedže charakteristický polynóm matice $\boldsymbol{M}_f$ je stupňa n s koeficientom $(-1)^n$ pri najvyššej mocnine premennej x, a je deliteľný jej minimálnym polynómom $\mu_{\boldsymbol{M}_f}(x) = f(x)$, ktorý je rovnakého stupňa, nevyhnutne platí $\mathrm{ch}_{\boldsymbol{M}_f}(x) = (-1)^n f(x)$.

21.3. Cyklické podpriestory

V tomto paragrafe dáme pre zmenu prednosť reči lineárnych operátorov. Je na čitateľovi, aby si v prípade potreby sformuloval príslušné pojmy a výsledky v jazyku matíc.

Nech $S \subseteq V$ je invariantný podpriestor lineárneho operátora $\varphi\colon V \to V$. Hovoríme, že S je *cyklický podpriestor* operátora φ, ak existuje vektor $\boldsymbol{v} \in S$ taký, že nejaká konečná postupnosť $\boldsymbol{v}, \varphi(\boldsymbol{v}), \ldots, \varphi^{k-1}(\boldsymbol{v})$ jeho iterovaných obrazov tvorí bázu podpriestoru S. Vektor $\boldsymbol{v}$ nazývame *cyklickým generátorom* podpriestoru S a bázu $\big(\boldsymbol{v}, \varphi(\boldsymbol{v}), \ldots, \varphi^{k-1}(\boldsymbol{v})\big)$, prípadne v obrátenom poradí $\big(\varphi^{k-1}(\boldsymbol{v}), \ldots, \varphi(\boldsymbol{v}), \boldsymbol{v}\big)$, nazývame *cyklickou bázou* podpriestoru S (vzhľadom na φ).

Každý nenulový vektor $\boldsymbol{v} \in V$ je cyklickým generátorom práve jedného cyklického podpriestoru operátora φ. Keďže V je konečnorozmerný, v postupnosti obrazov $\boldsymbol{v}, \varphi(\boldsymbol{v}), \varphi^2(\boldsymbol{v}), \ldots$ sa raz musí vyskytnúť člen, ktorý je lineárnou kombináciou predchádzajúcich. Označme k najmenšie prirodzené číslo, pre ktoré to nastane. Potom vektory $\boldsymbol{v}, \varphi(\boldsymbol{v}), \ldots, \varphi^{k-1}(\boldsymbol{v})$ sú lineárne nezávislé a

$$\varphi^k(\boldsymbol{v}) = c_1 \varphi^{k-1}(\boldsymbol{v}) + \ldots + c_{k-1}\varphi(\boldsymbol{v}) + c_k \boldsymbol{v}$$

pre nejaké $c_1, \ldots, c_k \in K$. Zrejme všetky dalšie obrazy $\varphi^l(\boldsymbol{v})$, $l \geq k$, sú takisto v lineárnom obale $S = \big[\boldsymbol{v}, \varphi(\boldsymbol{v}), \ldots, \varphi^{k-1}(\boldsymbol{v})\big]$, takže S je cyklický podpriestor operátora φ s cyklickým generátorom $\boldsymbol{v}$. Maticou zúženého operátora $\varphi \restriction S$ vzhľadom na cyklickú bázu $\big(\varphi^{k-1}(\boldsymbol{v}), \ldots, \varphi(\boldsymbol{v}), \boldsymbol{v}\big)$ je pridružená matica $\boldsymbol{M}_f$ polynómu $f(x) = x^k - c_1 x^{k-1} - \ldots - c_{k-1}x - c_k$. Tento polynóm nazývame *cyklickým rádom* vektora $\boldsymbol{v}$ (vzhľadom na φ).

Ako uvidíme v nasledujúcej kapitole, v aplikáciách lineárnej algebry na diferenciálne rovnice hrajú významnú úlohu lineárne operátory $\varphi\colon \mathbb{R}^n \to \mathbb{R}^n$ (teda vlastne matice $\boldsymbol{A} \in \mathbb{R}^{n\times n}$), vzhľadom na ktoré je celý priestor $\mathbb{R}^n$ cyklický. Tým nadobúda na dôležitosti otázka charakterizácie takýchto operátorov a matíc, ktorá nás vracia späť k dôsledku 21.2.4.

21.3.1. Tvrdenie. *Nech $\varphi\colon V \to V$ je lineárny operátor na n-rozmernom vektorovom priestore V. Potom nasledujúce podmienky sú ekvivalentné:*

(i) V je cyklickým podpriestorom operátora φ;

(ii) *maticou φ vo vhodnej báze priestoru V je pridružená matica $\boldsymbol{M}_f$ nejakého normovaného polynómu $f(x)$ stupňa n;*
(iii) *minimálny polynóm $\mu_\varphi(x)$ má stupeň n;*
(iv) $\mu_\varphi(x) = (-1)^n \operatorname{ch}_\varphi(x)$;
(v) *v Jordanovej matici operátora φ (nad nejakým konečným rozšírením poľa K) sa každá vlastná hodnota $\lambda \in \operatorname{Spec}\varphi$ vyskytuje v práve jednej Jordanovej bunke.*

Ešte inak môžeme povedať, že vektor $\boldsymbol{v} \in V$ je cyklickým generátorom priestoru V vzhľadom na lineárny operátor φ práve vtedy, keď jeho cyklickým rádom je polynóm $(-1)^n \operatorname{ch}_\varphi(x)$.

*21.4. Primárny a racionálny kanonický tvar

Tento paragraf má prevažne informatívny charakter a v našom kurze naň nebudeme nadväzovať. Obsahuje stručný prehľad niektorých základných pojmov a výsledkov o ďalších kanonických tvaroch matíc lineárnych operátorov a invariantoch podobnosti štvorcových matíc, ktoré uvádzame bez dôkazov. Čitateľ s hlbším záujmom o túto problematiku, môže siahnuť po inej dostupnej literatúre.[1]

Jordanov kanonický tvar zostáva i naďalej našim „hlavným“ kanonickým tvarom. Jeho prednosti sa zakladajú na jednoduchých pravidlách výpočtu mocnín a – v dôsledku toho – aj hodnôt iných funkcií pre Jordanove bunky $\boldsymbol{J}_n(\lambda)$. Popri tom však Jordanov tvar má i dve nezanedbateľné nevýhody. Predovšetkým, na jeho určenie je potrebná znalosť spektra príslušného lineárneho operátora alebo matice, čo môže byť problém najmä pri vyšších dimenziách. Po druhé, JKT je dosiahnuteľný len pre operátory či matice s plnou algebraickou váhou spektra; v prípade, že tomu tak nie je, musíme napr. JKT matice $\boldsymbol{A} \in K^{n\times n}$ hľadať až v nejakom rozšírení L pôvodného poľa K.

V tomto paragrafe sa zoznámime s dvoma typmi kanonických tvarov matíc, ktorých určenie si nevyžaduje znalosť spektra a – ani v prípade jeho neúplnej algebraickej váhy – nevybočuje z pôvodného poľa. Začneme však ďalším malým prídavkom k našim mimovoľne sa rozrastajúcim vedomostiam o polynómoch.

Hovoríme, že *polynómy* $f(x), g(x) \in K[x]$ stupňa aspoň 1 sú *nesúdeliteľné*, ak okrem konštantných polynómov $0 \neq c \in K$ nemajú v $K[x]$ iné spoločné delitele. Hovoríme, že *polynóm* $p(x) \in K[x]$ stupňa aspoň 1 je *ireducibilný*, ak každý jeho deliteľ je alebo konštantný polynóm alebo skalárny násobok polynómu $p(x)$. Ireducibilné polynómy hrajú v obore $K[x]$ podobnú úlohu ako prvočísla v obore $\mathbb{N}$ alebo $\mathbb{Z}$. Obdobou vety o jednoznačnom rozklade celých čísel na prvočinitele je nasledujúce tvrdenie, ktoré možno pomerne jednoducho dokázať indukciou podľa stupňa polynómu $f(x)$.

21.4.1. Tvrdenie. *Každý polynóm $f(x) \in K[x]$ stupňa aspoň 1 možno rozložiť na súčin tvaru*

$$f(x) = a\,p_1(x)^{\alpha_1} \dots p_k(x)^{\alpha_k}$$

[1] Pozri napr. G. Birkhoff, S. Mac Lane, *Prehad modernej algebry*, ako aj S. Mac Lane, G. Birkhoff, *Algebra.*

kde $0 \neq a \in K$, $\alpha_1, \dots, \alpha_k$ sú kladné celé čísla a $p_1(x), \dots, p_k(x)$ sú navzájom rôzne normované ireducibilné polynómy nad K. Tento rozklad je jednoznačný až na poradie mocnín $p_i(x)^{\alpha_i}$ jednotlivých ireducibilných faktorov $p_i(x)$.

Teraz už môžeme vysloviť vetu o tzv. *primárnom kanonickom tvare.*

21.4.2. Veta. *Nech $\varphi\colon V \to V$ je lineárny operátor na n-rozmernom vektorovom priestore V, ktorého minimálny polynóm má v $K[x]$ rozklad*

$$\mu_\varphi(x) = p_1(x)^{\alpha_1} \dots p_k(x)^{\alpha_k}$$

na súčin mocnín rôznych normovaných ireducibilných polynómov $p_1(x), \dots, p_k(x)$. Potom existujú postupnosti prirodzených čísel $\alpha_i = \alpha_{i1} \geq \alpha_{i2} \geq \dots \geq \alpha_{ir_i} \geq 1$ také, že $\sum_{i=1}^k \sum_{j=1}^{r_i} \alpha_{ij} = n$, a báza priestoru V, vzhľadom na ktorú má matica lineárneho operátora φ blokovo diagonálny tvar

$$\operatorname{diag}\big(\boldsymbol{M}_{p_{11}}, \dots, \boldsymbol{M}_{p_{1r_1}}, \dots\dots, \boldsymbol{M}_{p_{k1}}, \dots, \boldsymbol{M}_{p_{kr_k}}\big)$$

pozostávajúci z pridružených matíc polynómov $p_{ij}(x) = p_i(x)^{\alpha_{ij}}$, kde $1 \leq i \leq k$, $1 \leq j \leq r_j$.

Sústava polynómov $p_{ij}(x) = p_i(x)^{\alpha_{ij}}$ $(1 \leq i \leq k,\ 1 \leq j \leq r_j)$ sa nazýva *sústava elementárnych deliteľov* lineárneho operátora φ, a je až na poradie podsústav $p_{i1}(x), \dots, p_{ir_i}(x)$ určená jednoznačne. Uvedený tvar matice operátora φ sa nazýva *primárny kanonický tvar.* I tento tvar je jednoznačne určený až na poradie sústav blokov $\boldsymbol{M}_{p_{i1}}, \dots, \boldsymbol{M}_{p_{ir_i}}$, pridružených k mocninám toho istého ireducibilného polynómu $p_i(x)$. Charakteristický polynóm operátora φ je (až na znamienko) súčinom všetkých elementárnych deliteľov, t. j.

$$\begin{aligned}\operatorname{ch}_\varphi(x) &= (-1)^n p_{11}(x) \dots p_{1r_1}(x) \dots\dots p_{k1}(x) \dots p_{kr_k}(x) \\ &= (-1)^n p_1(x)^{\alpha_{11}+\dots+\alpha_{1r_1}} \dots\dots p_k(x)^{\alpha_{k1}+\dots+\alpha_{kr_k}}\end{aligned}$$

Primárny kanonický tvar matice lineárneho operátora φ zodpovedá rozkladu priestoru V najprv na priamy súčet invariantných podpriestorov $S_i = \operatorname{Ker} p_i^{\alpha_i}(\varphi)$, o ktorom hovorí tzv. *prvá veta o rozklade.* Podľa tzv. *druhej vety o rozklade* sa každý podpriestor S_i ďalej rozpadá na priamy súčet cyklických podpriestorov $S_{i1}, \dots, S_{ir_i}$, ktorých cyklické rády vzhľadom na φ sú polynómy $p_{ij}(x) = p_i(x)^{\alpha_{ij}}$.

S ohľadom na spomínanú jednoznačnosť možno teraz vetu 21.4.2 vysloviť v reči matíc takto:

21.4.3. Veta. *Každá matica $\boldsymbol{A} \in K^{n\times n}$ je podobná s nejakou s maticou $\boldsymbol{B} \in K^{n\times n}$ v primárnom kanonickom tvare. Matica $\boldsymbol{B}$ je určená jednoznačne až na poradie sústav blokov $\boldsymbol{M}_{p_{i1}}, \dots, \boldsymbol{M}_{p_{ir_i}}$, pridružených k mocninám jednotlivých ireducibilných polynómov $p_i(x) \in K[x]$, ktorých najvyššie mocniny tvoria rozklad minimálneho polynómu $\mu_{\boldsymbol{A}}(x) = p_1(x)^{\alpha_1} \dots p_k(x)^{\alpha_k}$ na po dvoch nesúdeliteľné faktory.*

Ak v uvedenej sústave elementárnych deliteľov položíme $r = \max\{r_i;\ 1 \leq i \leq k\}$, ďalej $\alpha_{ij} = 0$, teda $p_{ij}(x) = p_i(x)^{\alpha_{ij}} = 1$ pre $r_i < j \leq r$, tak po prenásobení „po stĺpcoch“, obdržíme sústavu polynómov

$$h_j(x) = p_{1j}(x) \dots p_{kj}(x) = p_1(x)^{\alpha_{1j}} \dots p_k(x)^{\alpha_{kj}},$$

pre $1 \le j \le r$. Prechod od primárneho k tzv. *racionálnemu kanonickému tvaru* sa zakladá na pozorovaní, že priamy súčet cyklických podpriestorov $S_{1j}, \dots, S_{kj}$ s po dvoch nesúdeliteľnými cyklickými rádmi $p_{1j}(x), \dots, p_{kj}(x)$ je opäť cyklický podpriestor s rádom $h_j(x) = p_{1j}(x) \dots p_{kj}(x)$.

21.4.4. Veta. *Nech $\varphi\colon V \to V$ je lineárný operátor na n-rozmernom vektorovom priestore V. Potom existuje jednoznačne určená postupnosť nekonštantných normovaných polynómov $h_1(x) = \mu_\varphi(x)$, $h_2(x), \dots, h_r(x) \in K[x]$, v ktorej každý nasledujúci člen delí predchádzajúci a súčet ich stupňov je n, ako aj báza priestoru V, vzhľadom na ktorú má matica lineárneho operátora φ blokovo diagonálny tvar*

$$\operatorname{diag}\big(\boldsymbol{M}_{h_1}, \boldsymbol{M}_{h_2}, \dots, \boldsymbol{M}_{h_r}\big),$$

pozostávajúci z pridružených matíc jednotlivých polynómov $h_j(x)$ pre $1 \le j \le r$.

Jednotlivé polynómy $h_j(x)$ sa nazývajú *invariantné faktory* lineárneho operátora φ a celá postupnosť $h_1(x) = \mu_\varphi(x)$, $h_2(x), \dots, h_r(x)$ jeho *sústavou invariantných faktorov.* Uvedený tvar matice operátora φ sa nazýva *racionálny kanonický tvar.* Sústava invariantných faktorov, rovnako ako racionálny kanonický tvar matice operátora φ sú určené jednoznačne, dokonca vrátane poradia jednotlivých polynómov resp. k nim pridružených maticových blokov. Rozkladom každého invariantného faktora na mocniny ireducibilných polynómov možno z ich sústavy spätne získať sústavu elementárnych deliteľov. Charakteristický polynóm operátora φ je (až na znamienko) súčinom všetkých jeho invariantných faktorov, t. j.

$$\operatorname{ch}_\varphi(x) = (-1)^n h_1(x) h_2(x) \dots h_r(x).$$

Vetu 21.4.4 možno v jazyku matíc vysloviť v nasledujúcej podobe.

21.4.5. Veta. *Každá matica $\boldsymbol{A} \in K^{n\times n}$ je podobná s jednoznačne určenou maticou v racionálnom kanonickom tvare $\operatorname{diag}\big(\boldsymbol{M}_{h_1}, \boldsymbol{M}_{h_2}, \dots, \boldsymbol{M}_{h_r}\big)$, pozostávajúcom z matíc pridružených k jej invariantným faktorom $h_1(x) = \mu_{\boldsymbol{A}}(x)$, $h_2(x), \dots, h_r(x)$.*

Poznámka. Výslovne zdôrazňujeme, že toľkokrát spomínaná jednoznačnosť sa vzťahuje len na primárny resp. racionálny kanonický tvar matice a nie na príslušnú bázu prípadne maticu prechodu. Napokon, rovnako je tomu aj v prípade JKT.

21.4.6. Príklad. Matica $\boldsymbol{A} \in \mathbb{R}^{6\times 6}$ má minimálny polynóm $\mu_{\boldsymbol{A}}(x) = (x^2+3)(x-1)^2$. Potom jej charakteristický polynóm je $\operatorname{ch}_{\boldsymbol{A}}(x) = (x^2+3)^2(x-1)^2$ alebo $\operatorname{ch}_{\boldsymbol{A}}(x) = (x^2+3)(x-1)^4$.

V prvom prípade sústavu elementárnych deliteľov matice $\boldsymbol{A}$ tvoria polynómy x^2+3, x^2+3, $(x-1)^2$ a sústavu invariantných faktorov polynómy $(x^2+3)(x-1)^2$, x^2+3.

V druhom prípade sú dve možnosti: Sústava elementárnych deliteľov má tvar x^2+3, $(x-1)^2$, $(x-1)^2$, so sústavou invariantných faktorov $(x^2+3)(x-1)^2$, $(x-1)^2$; alebo sústavu elementárnych deliteľov tvoria polynómy x^2+3, $(x-1)^2$, $x-1$, $x-1$ a sústavu invariantných faktorov polynómy $(x^2+3)(x-1)^2$, $x-1$, $x-1$.

*21.5. Výpočet invariantných faktorov

V tomto paragrafe predvedieme, ako možno k danej matici $\boldsymbol{A} \in K^{n\times n}$ zostrojiť sústavu invariantných faktorov. Z nej už vieme priamo napísať racionálny kanonický tvar (ako aj sústavu elementárnych deliteľov a primárny kanonický tvar) tejto matice. Taktiež si ukážeme, ako dostaneme príslušné matice prechodu. Pritom sa opäť sústredíme len na informáciu o podstatných súvislostiach a výpočtových postupoch, a príslušné dôkazy iba naznačíme alebo celkom vynecháme.

Najprv si uvedomme, že prvkami charakteristickej matice matice $\boldsymbol{A} \in K^{n\times n}$ sú polynómy s koeficientmi z poľa K, čiže $\boldsymbol{A} - x\boldsymbol{I} \in K[x]^{n\times n}$ je vlastne maticou nad množinou $K[x]$ všetkých polynómov v premennej x nad poľom K. Tradične sa v tejto súvislosti miesto premennej x zvykne používať premenná λ a maticiam nad množinou polynómov $K[\lambda]$ sa zvykne hovoriť *λ-matice.* Aj my sa prispôsobíme tejto tradícii. Aby sme vyznačili výskyt premennej λ, budeme λ-matice značiť $\boldsymbol{A}(\lambda)$, $\boldsymbol{B}(\lambda)$ a pod. Každú maticu $\boldsymbol{A}$ nad poľom K možno zároveň považovať za λ-maticu, ktorej prvky sú konštantné polynómy; hovoríme, že $\boldsymbol{A} = \boldsymbol{A}(\lambda)$ je *konštantná λ-matica.* Zrejme λ-matice (pokiaľ to dovolia ich rozmery) možno sčítať i násobiť celkom analogicky ako matice nad poľom K. Podobne ako v prípade charakteristickej matice, determinant štvorcovej λ-matice $\boldsymbol{A}(\lambda)$ je vždy polynóm $\det \boldsymbol{A}(\lambda) \in K[\lambda]$.

Elementárnou riadkovou operáciou, krátko λ-ERO, *na λ-matici* $\boldsymbol{A}(\lambda)$ rozumieme

I. výmenu dvoch riadkov matice $\boldsymbol{A}(\lambda)$;
II. vynásobenie niektorého riadku matice $\boldsymbol{A}(\lambda)$ nenulovým skalárom z poľa K;
III. pripočítanie niektorého riadku matice $\boldsymbol{A}(\lambda)$ vynásobeného ľubovoľným polynómom z $K[\lambda]$ k jej inému riadku.

Celkom analogicky definujeme aj *elementárne stĺpcové operácie na λ-maticiach*, krátko λ-ESO. Dve *λ-matice* $\boldsymbol{A}(\lambda)$, $\boldsymbol{B}(\lambda)$ rovnakých rozmerov sa nazývajú *λ-ekvivalentné*, označenie $\boldsymbol{A}(\lambda) \sim_\lambda \boldsymbol{B}(\lambda)$, ak jednu z nich možno dostať z druhej konečným počtom λ-ERO a λ-ESO. Zrejme pre každé $m, n \in \mathbb{N}$ je vzťah $\sim_\lambda$ naozaj ekvivalenciou na množine λ-matíc $K[\lambda]^{m\times n}$.

λ-matica $\boldsymbol{P}(\lambda) \in K[\lambda]^{n\times n}$ sa nazýva *invertibilná*, ak existuje $\boldsymbol{Q}(\lambda) \in K[\lambda]^{n\times n}$ taká, že $\boldsymbol{P}(\lambda)\cdot\boldsymbol{Q}(\lambda) = \boldsymbol{I}_n = \boldsymbol{Q}(\lambda)\cdot\boldsymbol{P}(\lambda)$. Zrejme λ-matica $\boldsymbol{Q}(\lambda) = \boldsymbol{P}(\lambda)^{-1}$ je k danej invertibilnej $\boldsymbol{P}(\lambda)$ určená jednoznačne už jednou z oboch požadovaných rovností.

Čitateľ by si mal sám premyslieť, ako možno λ-ERO a λ-ESO realizovať pomocou násobenia vhodnými invertibilnými λ-maticami. Na základe toho si už ľahko prispôsobí postup z paragrafu 7.4 na výpočet výrazov tvaru $\boldsymbol{P}(\lambda)^{-1}$, $\boldsymbol{P}(\lambda)^{-1}\cdot\boldsymbol{A}(\lambda)$, $\boldsymbol{A}(\lambda)\cdot\boldsymbol{P}(\lambda)^{-1}$ s invertibilnou λ-maticou $\boldsymbol{P}(\lambda)$.

Kľúčom k výpočtu invariantných faktorov je nasledujúca veta.

21.5.1. Veta. *Matice $\boldsymbol{A}$, $\boldsymbol{B} \in K^{n\times n}$ sú podobné práve vtedy, keď ich charakteristické λ-matice $\boldsymbol{A} - \lambda\boldsymbol{I}$, $\boldsymbol{B} - \lambda\boldsymbol{I}$ sú λ-ekvivalentné; presnejšie, ak $\boldsymbol{P}(\lambda), \boldsymbol{Q}(\lambda) \in K[\lambda]^{n\times n}$ sú invertibilné matice také, že $\boldsymbol{B} - \lambda\boldsymbol{I} = \boldsymbol{Q}(\lambda)\cdot(\boldsymbol{A} - \lambda\boldsymbol{I})\cdot\boldsymbol{P}(\lambda)$, tak $\boldsymbol{P}(\lambda) = \boldsymbol{P}$, $\boldsymbol{Q}(\lambda) = \boldsymbol{Q}$ sú konštantné matice, pre ktoré platí $\boldsymbol{Q} = \boldsymbol{P}^{-1}$ a $\boldsymbol{B} = \boldsymbol{Q}\cdot\boldsymbol{A}\cdot\boldsymbol{P}$.*

Náčrt dôkazu. Ak $\boldsymbol{A} \approx \boldsymbol{B}$ a $\boldsymbol{P} \in K^{n\times n}$ je regulárna taká, že $\boldsymbol{B} = \boldsymbol{P}^{-1}\cdot\boldsymbol{A}\cdot\boldsymbol{P}$, tak zrejme $\boldsymbol{B} - \lambda\boldsymbol{I} = \boldsymbol{P}^{-1}\cdot(\boldsymbol{A} - \lambda\boldsymbol{I})\cdot\boldsymbol{P}$, z čoho už vyplýva $\boldsymbol{A} - \lambda\boldsymbol{I} \sim_\lambda \boldsymbol{B} - \lambda\boldsymbol{I}$.

Naopak, pre $\boldsymbol{A} - \lambda\boldsymbol{I} \sim_\lambda \boldsymbol{B} - \lambda\boldsymbol{I}$ existujú invertibilné λ-matice $\boldsymbol{P}(\lambda)$, $\boldsymbol{Q}(\lambda)$ také, že $\boldsymbol{B} - \lambda\boldsymbol{I} = \boldsymbol{Q}(\lambda)\cdot(\boldsymbol{A} - \lambda\boldsymbol{I})\cdot\boldsymbol{P}(\lambda)$. Netriválnym faktom je, že za týchto okolností už

$\boldsymbol{P}(\lambda) = \boldsymbol{P}$, $\boldsymbol{Q}(\lambda) = \boldsymbol{Q}$ musia byť konštantné matice, pre ktoré navyše platí $\boldsymbol{Q} \cdot \boldsymbol{P} = \boldsymbol{I}$ a $\boldsymbol{B} = \boldsymbol{Q} \cdot \boldsymbol{A} \cdot \boldsymbol{P}$, teda $\boldsymbol{A} \approx \boldsymbol{B}$.

Hovoríme, že *λ-matica* $\boldsymbol{H}(\lambda) \in K[\lambda]^{n\times n}$ je *v kanonickom tvare*, ak $\boldsymbol{H}(\lambda) = \operatorname{diag}(h_1(\lambda), \dots, h_n(\lambda))$ je diagonálna matica, ktorej diagonálne prvky sú normované polynómy alebo 0 a každý nasledujúci člen delí predchádzajúci (pritom nulový polynóm delí len nulový polynóm a je deliteľný každým polynómom, teda v kanonickom tvare z $h_j(\lambda) = 0$ vyplýva $h_i(\lambda) = 0$ pre každé $i \le j$).

Polynóm $d(\lambda)$ je *najväčším spoločným deliteľom polynómov* $f_1(\lambda), \dots, f_k(\lambda)$, ak $d(\lambda)$ delí každý z polynómov $f_i(\lambda)$ a je deliteľný každým polynómom $g(x)$, ktorý delí všetky polynómy $f_i(\lambda)$. Pripomeňme, že minorom matice $\boldsymbol{A}$ rozumieme determinant ľubovoľnej štvorcovej matice, ktorá vznikne z matice $\boldsymbol{A}$ vynechaním niektorých riadkov a stĺpcov.

21.5.2. Veta. *Každá štvorcová λ-matica $\boldsymbol{A}(\lambda)$ je λ-ekvivalentná s jednoznačne určenou λ-maticou $\boldsymbol{H}(\lambda) = \operatorname{diag}(h_1(\lambda), \dots, h_n(\lambda))$ v kanonickom tvare. Pre jej diagonálne prvky platí*

$$h_n(\lambda) = d_1(\lambda), \qquad h_{n-j}(\lambda) = \begin{cases} \frac{d_{j+1}(\lambda)}{d_j(\lambda)}, & \text{ak } d_j(\lambda) \ne 0, \\ 0, & \text{ak } d_j(\lambda) = 0, \end{cases}$$

pre $1 \le j \le n-1$, kde $d_k(\lambda)$ je najväčší spoločný deliteľ všetkých minorov rádu k matice $\boldsymbol{A}(\lambda)$, a ak $d_k(\lambda) \ne 0$, tak je to normovaný polynóm.

Poznámka. (a) Polynómy $d_1(\lambda), \dots, d_n(\lambda)$ sa nazývajú *determinantové delitele* λ-matice $\boldsymbol{A}(\lambda)$. Zrejme $d_n(\lambda)$ sa až na skalárny násobok rovná determinantu $\det \boldsymbol{A}(\lambda)$.

(b) Pokiaľ je $\boldsymbol{H}(\lambda)$ kanonickým tvarom *charakteristickej matice* $\boldsymbol{A} - \lambda\boldsymbol{I}$, tak (z dôvodu zachovania hodnosti pri λ-ERO a λ-ESO) $\boldsymbol{H}(\lambda)$ nemôže obsahovať nulové prvky na diagonále. Preto $\boldsymbol{H}(\lambda) = \operatorname{diag}\big(h_1(\lambda), \dots, h_r(\lambda), 1, \dots, 1\big)$ a jej nekonštantné diagonálne prvky tvoria sústavu invariantných faktorov matice $\boldsymbol{A}$.

Miesto dôkazu len opíšeme algoritmus, ako nájsť kanonický tvar štvorcovej λ-matice $\boldsymbol{A}(\lambda) = \big(a_{ij}(\lambda)\big)_{n\times n}$. Jedna možnosť (tá pracnejšia) spočíva vo výpočte všetkých minorov matice $\boldsymbol{A}(\lambda)$ všetkých možných rádov a ich spoločných deliteľov $d_k(\lambda)$. Efektívnejšia je úprava pomocou λ-ERO a λ-ESO. Kľúčovým faktom je pozorovanie, že determinantové delitele $d_k(\lambda)$ sa pri úprave λ-matice $\boldsymbol{A}(\lambda)$ pomocou λ-ERO a λ-ESO nemenia.

Ak $\boldsymbol{A}(\lambda)$ je nulová matica, sme hotoví. V opačnom prípade možno výmenou riadkov a stĺpcov zariadiť, aby $a_{nn}(\lambda) \ne 0$. Teraz postupne dosiahneme, aby $a_{nn}(\lambda)$ delil všetky prvky v n-tom stĺpci i riadku. Ak napr. $a_{in}(\lambda) = a_{nn}(\lambda)\,p(\lambda) + r(\lambda)$, pričom stupeň zvyšku $r(\lambda) \ne 0$ je menší než stupeň $a_{nn}(\lambda)$, odpočítame od i-teho riadku $p(\lambda)$-násobok n-tého riadku a vymeníme i-ty a n-tý riadok. Tým zakaždým znížime stupeň $a_{nn}(\lambda)$. Pretože konštantný nenulový polynóm delí každý polynóm, po konečnom počte krokov bude $a_{nn}(\lambda)$ deliť všetky prvky $a_{in}(\lambda)$, $a_{nj}(\lambda)$; v tej chvíli môžeme pripočítaním vhodných násobkov posledného riadku resp. stĺpca vynulovať všetky prvky v poslednom stĺpci aj riadku okrem $a_{nn}(\lambda)$.

Pokiaľ $a_{nn}(\lambda)$ nedelí všetky prvky v matici, možno opäť znížiť jeho stupeň. Ak totiž $a_{ij}(\lambda) = a_{nn}(\lambda)\,q(\lambda) + s(\lambda)$, kde zvyšok $s(\lambda) \ne 0$ má menší stupeň, pripočítame i-ty riadok k n-tému a opäť postupujeme podľa predchádzajúceho odstavca.

Po konečnom počte krokov dosiahneme, že $a_{nn}(\lambda)$ delí všetky polynómy v matici a je jediným nenulovým prvkom v n-tom riadku i stĺpci. Navyše, vynásobením vhodným skalárom možno dosiahnuť, aby to bol normovaný polynóm. Teraz aplikujeme rovnaký postup na maticu tvorenú prvými $n-1$ riadkami a stĺpcami takto upravenej matice a postupujeme tak dlho, až kým po konečnom počte krokov nedostaneme kanonický tvar.

Samozrejme, v konkrétnych prípadoch sa nemusíme otrocky držať uvedeného postupu, ale môžeme výhodne využívať podobu upravovanej matice.

21.5.3. Príklad. Nájdeme sústavu invariantných faktorov matice

$$\boldsymbol{A} = \begin{pmatrix} -3 & 9 & -8 & 3 \\ -1 & 3 & -2 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \in \mathbb{R}^{4\times 4}$$

úpravou jej charakteristickej matice

$$\boldsymbol{A} - \lambda \boldsymbol{I} = \begin{pmatrix} -3-\lambda & 9 & -8 & 3 \\ -1 & 3-\lambda & -2 & 1 \\ 0 & 0 & 1-\lambda & 0 \\ 0 & 0 & 0 & 1-\lambda \end{pmatrix}$$

na kanonický tvar. V prvom kroku vymeníme druhý a štvrtý riadok, v druhom pomocou jednotky na mieste $(4,4)$ vynulujeme zvyšné prvky štvrtého riadku i stĺpca. $\boldsymbol{A} - \lambda \boldsymbol{I}$ je tak postupne λ-ekvivalentná s λ-maticami

$$\begin{pmatrix} -3-\lambda & 9 & -8 & 3 \\ 0 & 0 & 0 & 1-\lambda \\ 0 & 0 & 1-\lambda & 0 \\ -1 & 3-\lambda & -2 & 1 \end{pmatrix} \sim_\lambda \begin{pmatrix} -\lambda & 3\lambda & -2 & 0 \\ 1-\lambda & (\lambda-1)(\lambda-3) & 2(1-\lambda) & 0 \\ 0 & 0 & 1-\lambda & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Štvrtý riadok a stĺpec sa pri ďalších úpravách už nebudú meniť, preto ich jednoducho „odpílime“. Teraz odpočítame od druhého riadku tretí, potom vymeníme $(-1/2)$-násobok prvého riadku s tretím. V ďalšom kroku pomocou prvku 1 v pozícii $(3,3)$ vynulujeme zvyšné prvky tretieho stĺpca i riadku a vo výsledku vynásobíme prvý riadok dvomi a druhý šiestimi. Tým dostaneme

$$\begin{pmatrix} 0 & 0 & 1-\lambda \\ 1-\lambda & (\lambda-1)(\lambda-3) & 1-\lambda \\ \lambda/2 & 3\lambda/2 & 1 \end{pmatrix} \sim_\lambda \begin{pmatrix} \lambda(\lambda-1) & 3\lambda(\lambda-1) & 0 \\ 3(\lambda-1)(\lambda-2) & 2(\lambda-1)(4\lambda-9) & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Zase odpílime tretí riadok i stĺpec. Od druhého stĺpca odpočítame trojnásobok prvého a to isté urobíme s riadkami. Ďalej vymeníme $1/6$ prvého stĺpca s druhým. Keďže prvok na mieste $(2,2)$ teraz delí všetky ostatné členy, môžeme pomocou neho vynulovať zvyšok prvého riadku i stĺpca a prenásobením riadkov vhodnými skalármi znormovať diagonálne členy. Postupne tak dostávame

$$\begin{pmatrix} \lambda(\lambda-1) & 0 \\ 6(1-\lambda) & \lambda(1-\lambda) \end{pmatrix} \sim_\lambda \begin{pmatrix} 0 & \lambda(\lambda-1)/6 \\ \lambda(1-\lambda) & 1-\lambda \end{pmatrix} \sim_\lambda \begin{pmatrix} \lambda^2(\lambda-1) & 0 \\ 0 & \lambda-1 \end{pmatrix}.$$

Po opätovnom pripojení odpílených riadkov a stĺpcov máme

$$\boldsymbol{A} - \lambda \boldsymbol{I} \sim_\lambda \operatorname{diag}\bigl(\lambda^2(\lambda-1), \lambda-1, 1, 1\bigr),$$

pričom posledná λ-matica už je v kanonickom tvare. Nekonštantné polynómy v nej, t. j. $\lambda^2(\lambda-1) = \lambda^3 - \lambda^2$, $\lambda - 1$, tvoria sústavu invariantných faktorov matice $\boldsymbol{A}$. Jej sústava elementárnych deliteľov preto je λ^2, $\lambda-1$, $\lambda-1$. Na základe toho už môžeme napísať racionálny, primárny i Jordanov kanonický tvar matice $\boldsymbol{A}$:

$$\begin{aligned}\boldsymbol{A} &\approx \operatorname{diag}\bigl(\boldsymbol{M}_{\lambda^2(\lambda-1)}, \boldsymbol{M}_{\lambda-1}\bigr) = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \\ &\approx \operatorname{diag}\bigl(\boldsymbol{M}_{\lambda^2}, \boldsymbol{M}_{\lambda-1}, \boldsymbol{M}_{\lambda-1}\bigr) = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} = \operatorname{diag}\bigl(\boldsymbol{J}_2(0), 1, 1\bigr).\end{aligned}$$

Všimnite si, že primárny a Jordanov kanonický tvar matice $\boldsymbol{A}$ (náhodou) splývajú.

Keby nám napr. vyšlo

$$\boldsymbol{A} - \lambda \boldsymbol{I} \sim_\lambda \operatorname{diag}\bigl((\lambda^2 - \lambda + 3)(\lambda-2)^2, 1, 1, 1\bigr),$$

znamenalo by to, že sústava invariantných faktorov pozostáva z jediného polynómu $(\lambda^2-\lambda+3)(\lambda-2)^2 = \lambda^4 - 5\lambda^3 + 11\lambda^2 - 16\lambda + 12$, sústava elementárnych deliteľov z dvoch polynómov $\lambda^2 - \lambda + 3$, $(\lambda-2)^2 = \lambda^2 - 4\lambda + 4$ a racionálny resp. primárny kanonický tvar matice $\boldsymbol{A}$ je

$$\begin{aligned}\boldsymbol{A} &\approx \boldsymbol{M}_{(\lambda^2-\lambda+3)(\lambda-2)^2} = \begin{pmatrix} 5 & 1 & 0 & 0 \\ -11 & 0 & 1 & 0 \\ 16 & 0 & 0 & 1 \\ -12 & 0 & 0 & 0 \end{pmatrix} \\ &\approx \operatorname{diag}\bigl(\boldsymbol{M}_{\lambda^2-\lambda+3}, \boldsymbol{M}_{(\lambda-2)^2}\bigr) = \begin{pmatrix} 1 & 1 & 0 & 0 \\ -3 & 0 & 0 & 0 \\ 0 & 0 & 4 & 1 \\ 0 & 0 & -4 & 0 \end{pmatrix}.\end{aligned}$$

Keďže polynóm $\lambda^2 - \lambda + 3$ je ireducibilný nad $\mathbb{R}$ (má dva korene $(1 \pm \mathrm{i}\sqrt{11})/2 \in \mathbb{C}$), JKT matice $\boldsymbol{A}$ nad $\mathbb{R}$ neexistuje. Jej komplexný resp. zovšeobecnený JKT (pozri paragraf 20.3) by bol

$$\begin{aligned}\boldsymbol{A} &\approx \operatorname{diag}\bigl((1+\mathrm{i}\sqrt{11})/2, (1-\mathrm{i}\sqrt{11})/2, \boldsymbol{J}_2(2)\bigr) \\ &\approx \operatorname{diag}\left(\boldsymbol{J}_1\Bigl(\begin{smallmatrix} 1/2 & -\sqrt{11}/2 \\ \sqrt{11}/2 & 1/2 \end{smallmatrix}\Bigr), \boldsymbol{J}_2(2)\right) = \begin{pmatrix} 1/2 & -\sqrt{11}/2 & 0 & 0 \\ \sqrt{11}/2 & 1/2 & 0 & 0 \\ 0 & 0 & 2 & 1 \\ 0 & 0 & 0 & 2 \end{pmatrix}.\end{aligned}$$

K úprave na kanonický tvar však navyše patrí nájdenie príslušnej bázy resp. matice prechodu. Nech teda $\boldsymbol{A} - \lambda \boldsymbol{I} \sim_\lambda \boldsymbol{H}(\lambda)$, kde λ-matica $\boldsymbol{H}(\lambda)$ je v kanonickom tvare a $\boldsymbol{C} \approx \boldsymbol{A}$ je niektorý z kanonických tvarov (racionálny, primárny či Jordanov) matice $\boldsymbol{A}$, zostrojený na základe $\boldsymbol{H}(\lambda)$. Potom tiež $\boldsymbol{C} - \lambda \boldsymbol{I} \sim_\lambda \boldsymbol{H}(\lambda)$. Preto existujú invertibilné λ-matice $\boldsymbol{P}_1(\lambda)$, $\boldsymbol{Q}_1(\lambda)$, $\boldsymbol{P}_2(\lambda)$, $\boldsymbol{Q}_2(\lambda)$ také, že

$$\boldsymbol{Q}_1(\lambda) \cdot (\boldsymbol{A} - \lambda \boldsymbol{I}) \cdot \boldsymbol{P}_1(\lambda) = \boldsymbol{H}(\lambda) = \boldsymbol{Q}_2(\lambda) \cdot (\boldsymbol{C} - \lambda \boldsymbol{I}) \cdot \boldsymbol{P}_2(\lambda).$$

V dôsledku toho

$$\boldsymbol{Q}_2(\lambda)^{-1} \cdot \boldsymbol{Q}_1(\lambda) \cdot (\boldsymbol{A} - \lambda \boldsymbol{I}) \cdot \boldsymbol{P}_1(\lambda) \cdot \boldsymbol{P}_2(\lambda)^{-1} = \boldsymbol{C} - \lambda \boldsymbol{I},$$

takže podľa vety 21.5.1 sú $\boldsymbol{P} = \boldsymbol{P}_1(\lambda) \cdot \boldsymbol{P}_2(\lambda)^{-1}$, $\boldsymbol{Q} = \boldsymbol{Q}_2(\lambda)^{-1} \cdot \boldsymbol{Q}_1(\lambda)$ konštantné matice a platí $\boldsymbol{Q} = \boldsymbol{P}^{-1}$ a $\boldsymbol{C} = \boldsymbol{P}^{-1} \cdot \boldsymbol{A} \cdot \boldsymbol{P}$. To znamená, že lineárny operátor $\boldsymbol{x} \mapsto \boldsymbol{A} \cdot \boldsymbol{x}$ má v báze priestoru K^n tvorenej stĺpcami matice $\boldsymbol{P}$ maticu v príslušnom kanonickom tvare $\boldsymbol{C}$.

Stačí teda pri úprave $\boldsymbol{A} - \lambda \boldsymbol{I} \longrightarrow \boldsymbol{H}(\lambda)$ pomocou λ-ERO a λ-ESO zaznamenať *len stĺpcové* operácie rovnakými λ-ESO na jednotkovej matici $\boldsymbol{I}$, čím získame $\boldsymbol{P}_1(\lambda)$. Ďalej treba vykonať úpravu $\boldsymbol{C} - \lambda \boldsymbol{I} \longrightarrow \boldsymbol{H}(\lambda)$ (čo vzhľadom na špeciálny tvar matice $\boldsymbol{C}$ býva podstatne jednoduchšie) a opäť zaznamenať *len stĺpcové* operácie zodpovedajúcimi λ-ESO na matici $\boldsymbol{I}$. Tým získame maticu $\boldsymbol{P}_2(\lambda)$. Hľadaná matica prechodu potom je $\boldsymbol{P} = \boldsymbol{P}_1(\lambda) \cdot \boldsymbol{P}_2(\lambda)^{-1}$.

Na ostatok si ešte uvedomme, že (po doplnení vynechaných tvrdení a dôkazov) obsahujú paragrafy 21.4 a 21.5 návod na nový dôkaz vety o Jordanovom kanonickom tvare.