# Struktura endomorfizmov

Klemen Šivic

24. april 2020

## 1 Karakteristični in minimalni polinom

V tem poglavju si bomo ogledali, kako poiščemo lastne vrednosti endomorfizma. Najprej ponovimo nekaj definicij in rezultatov iz poglajva o determinantah.

**Definicija 1.1.** Endomorfizem $\mathcal{A} \in \mathcal{L}(V)$ *se da diagonalizirati*, kadar obstaja taka baza $\mathcal{B}$ prostora $V$, da je matrika $\mathcal{A}_{\mathcal{B}}^{\mathcal{B}}$ diagonalna.

**Definicija 1.2.** Naj bo $\mathcal{A}$ endomorfizem prostora $V$. Skalar $\alpha \in \mathcal{O}$ je *lastna vrednost* endomorfizma $\mathcal{A}$, kadar obstaja neničelni vektor $v \in V$, da je $\mathcal{A}v = \alpha v$. Vsak tak neničelni vektor $v$ se imenuje *lastni vektor* endomorfizma $\mathcal{A}$ za lastno vrednost $\alpha$.

Naj bo $\alpha \in \mathcal{O}$ lastna vrednost endomorfizma $\mathcal{A} \in \mathcal{L}(V)$. Vemo (Trditev 1.6 iz poglavja o determinantah), da je množica $\{v \in V; \mathcal{A}v = \alpha v\}$ vektorski podprostor prostora $V$, ki mu pravimo *lastni podprostor* endomorfizma $\mathcal{A}$ za lastno vrednost $\alpha$. Enak je $\ker(\mathcal{A} - \alpha\,\mathrm{id}_V)$ in je sestavljen iz vseh lastnih vektorjev, ki pripadajo lastni vrednosti $\alpha$, in vektorja 0. Njegova razsežnost se imenuje *geometrična večkratnost* lastne vrednosti $\alpha$.

Kakšna je zveza med diagonalizacijo endomorfizma in lastnimi vrednostmi, smo ugotovili že v poglavju o determinantah (Trditev 1.8).

**Trditev 1.3.** *Endomorfizem $\mathcal{A} \in \mathcal{L}(V)$ se da diagonalizirati natanko takrat, ko obstaja baza prostora $V$, sestavljena iz lastnih vektorjev endomorfizma $\mathcal{A}$.*

Prav tako smo že ugotovili, kako lastne vrednosti karakteriziramo z determinanto (Trditev 3.15).

**Trditev 1.4.** *Skalar $\lambda \in \mathcal{O}$ je lastna vrednost endomorfizma $\mathcal{A} \in \mathcal{L}(V)$ natanko takrat, ko za neko in zato za vsako matriko $A$, ki pripada endomorfizmu $\mathcal{A}$, velja* $\det(A - \lambda I) = 0$.

Naj bo $A \in \mathcal{O}^{n\times n}$. Po definiciji je

$$\det(A - \lambda I) = \sum_{\pi \in S_n} s(\pi)(a_{\pi(1),1} - \lambda\delta_{\pi(1),1}) \cdots (a_{\pi(n),n} - \lambda\delta_{\pi(n),n}), \tag{1}$$

kjer je $\delta_{ij}$ *Kroneckerjev delta*, definiran z $\delta_{ij} = \left\{ \begin{array}{ll} 1; & i = j \\ 0; & i \neq j \end{array} \right.$. Vsak člen v zgornji vsoti je vsota produktov členov matrike in potenc $\lambda$, torej je $\det(A - \lambda I)$ polinom v $\lambda$ s koeficienti iz obsega $\mathcal{O}$.

**Definicija 1.5.** Polinom $\det(A - \lambda I)$ se imenuje *karakteristični polinom* matrike $A \in \mathcal{O}^{n\times n}$. Označimo ga z $\Delta_A(\lambda)$.

Če je $A \in \mathcal{O}^{n\times n}$, potem je stopnja polinoma $\Delta_A(\lambda)$ očitno največ $n$, saj je vsak člen v vsoti (1) produkt $n$ linearnih polinomov. Ugotovimo, ali je stopnja enaka $n$ ali morda manjša. V vsoti (1) dobimo člen $\lambda^n$ le v primeru, ko je $\delta_{\pi(i),i} = 1$ za vsak $i = 1, \ldots, n$, torej ko je $\pi(i) = i$ za vsak $i = 1, \ldots, n$. Z drugimi besedami, $\lambda^n$ dobimo natanko v enem členu vsote (1), in sicer tistem, kjer je $\pi = \mathrm{id}$. To pa že pomeni, da je stopnja polinoma $\Delta_A(\lambda)$ enaka $n$, njegov vodilni koeficient pa je enak $(-1)^n$. Iz enakosti (1) vidimo tudi, da je konstantni člen polinoma $\Delta_A(\lambda)$ enak $\det A$.

**Trditev 1.6.** *Podobni matriki imata enak karakteristični polinom.*

*Dokaz.* Naj bo $B = P^{-1}AP$ za neko obrnljivo matriko $P$. Če upoštevamo, da je determinanta multiplikativna in da je determinanta inverza matrike $P$ enaka inverzu determinante matrike $P$, dobimo

$$\begin{aligned}\Delta_B(\lambda) &= \det(B - \lambda I) = \det(P^{-1}AP - \lambda I) = \det(P^{-1}(A - \lambda I)P) \\ &= (\det P^{-1})\det(A - \lambda I)\det P = (\det P)^{-1}\Delta_A(\lambda)\det P = \Delta_A(\lambda),\end{aligned}$$

kar je bilo treba dokazati. □

Zaradi te trditve ima smisel naslednja definicija.

**Definicija 1.7.** *Karakteristični polinom endomorfizma* $\mathcal{A} \in \mathcal{L}(V)$ je $\Delta_A(\lambda)$, kjer je $A$ poljubna matrika, ki pripada endomorfizmu $\mathcal{A}$. Karakteristični polinom endomorfizma $\mathcal{A}$ označimo z $\Delta_{\mathcal{A}}(\lambda)$. Če je $A$ poljubna matrika, ki glede na neko bazo prostora $V$ pripada endomorfizmu $\mathcal{A}$, je torej $\Delta_{\mathcal{A}}(\lambda) = \Delta_A(\lambda)$.

Iz Trditve 1.4 zdaj takoj sledi

**Posledica 1.8.** *Skalar $\lambda \in \mathcal{O}$ je lastna vrednost endomorfizma $\mathcal{A} \in \mathcal{L}(V)$ natanko takrat, ko je ničla karakterističnega polinoma endomorfizma $\mathcal{A}$.*

**Primer 1.9.** Endomorfizem vektorskega prostora nad splošnim obsegom lahko nima nobene lastne vrednosti. Na primer, naj bo $A = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$. Spomnimo se, da matrika $A$ določa endomorfizem $A\colon \mathbb{R}^2 \to \mathbb{R}^2$, ki vsak vektor $x \in \mathbb{R}^2$ preslika v $Ax$, in da temu endomorfizmu v standardni bazi prostora $\mathbb{R}^2$ ustreza matrika $A$. Torej so lastne vrednosti endomorfizma $A$ natanko **realne** ničle karakterističnega polinoma matrike $A$. Toda

$$\Delta_A(\lambda) = \begin{vmatrix} -\lambda & 1 \\ -1 & -\lambda \end{vmatrix} = \lambda^2 + 1,$$

ta polinom pa nima nobene realne ničle. To pomeni, da endomorfizem $A$ nima nobene lastne vrednosti. V konkretnem primeru je to mogoče videti tudi geometrijsko. Endomorfizem $A$ je namreč rotacija za $-\frac{\pi}{2}$, jasno pa je, da rotacija za kot $\alpha \notin \{k\pi; k \in \mathbb{Z}\}$ nobenega neničelnega vektorja ne more preslikati v njegov večkratnik.

Da se bomo izognili situacijam kot v zgornjem primeru, bomo odslej (in do konca poglavja o strukturi endomorfizmov) predpostavili, da je $\mathcal{O} = \mathbb{C}$. Vzrok za to je:

**Izrek 1.10** (Osnovni izrek algebre)**.** *Vsak nekonstanten kompleksen polinom ima vsaj eno ničlo v $\mathbb{C}$.*

Noben dokaz tega dokaza ni enostaven. Mi bomo dokaz izpustili, običajno pa se ga dokaže pri Analizi 2.

V skladu z našim dogovorom, da bo vedno $\mathcal{O} = \mathbb{C}$, tudi definiramo:

**Definicija 1.11.** *Lastne vrednosti matrike $A$* so kompleksne ničle karakterističnega polinoma $\Delta_A(\lambda)$.

Z drugimi besedami, lastne vrednosti $n \times n$ matrike $A$ so lastne vrednosti endomorfizma $A\colon \mathbb{C}^n \to \mathbb{C}^n$, ki vsak $x \in \mathbb{C}^n$ slika v $Ax$. Tudi če je $A$ realna matrika, jo torej obravnavamo kot kompleksno matriko. Prav tako pravimo, da *se da matriko $A \in \mathbb{C}^{n\times n}$ diagonalizirati*, kadar se da diagonalizirati endomorfizem $\mathbb{C}^n \to \mathbb{C}^n$, definiran s predpison $x \mapsto Ax$. To je torej natanko takrat, ko obstaja **kompleksna** obrnljiva matrika $P$, da je matrika $P^{-1}AP$ diagonalna. Kaj je v tem primeru matrika $P$? Ker je matrika $P^{-1}AP$ diagonalna, za vsak $i = 1, \ldots, n$ obstaja $\lambda_i \in \mathbb{C}$, da je $P^{-1}APe_i = \lambda_i e_i$. Torej je $A(Pe_i) = \lambda_i(Pe_i)$ za vsak $i$. To pomeni, da je $i$-ti stolpec matrike $P$ lastni vektor matrike $A$ za lastno vrednost $\lambda_i$.

**Definicija 1.12.** Množico vseh lastnih vrednosti matrike $A$ (oziroma endomorfizma $\mathcal{A}$) imenujemo *spekter* matrike $A$ (oziroma endomorfizma $\mathcal{A}$) in ga označimo s $\sigma(A)$ (oziroma $\sigma(\mathcal{A})$).

Ker je $\mathcal{O} = \mathbb{C}$, lahko karakteristični polinom matrike $A \in \mathcal{O}^{n\times n}$ zapišemo v obliki

$$\Delta_A(\lambda) = (-1)^n(\lambda - \lambda_1)^{n_1} \cdots (\lambda - \lambda_k)^{n_k},$$

kjer so $\lambda_1, \ldots, \lambda_k$ vse različne ničle polinoma $\Delta_A(\lambda)$ in $n_1 + \cdots + n_k = n$. Potem je $\sigma(A) = \{\lambda_1, \ldots, \lambda_k\}$. Za vsak $j = 1, \ldots, k$ število $n_j$ imenujemo *algebraična večkratnost* lastne vrednosti $\lambda_j$ matrike $A$. Enak sklep velja za lastne vrednosti endomorfizma $\mathcal{A} \in \mathcal{L}(V)$ in na enak način so definirane algebraične večkratnosti lastnih vrednosti endomorfizma $\mathcal{A}$.

Zgornji razmislek nam pove, da ima $n \times n$ matrika (oz. endomorfizem $n$-razsežnega vektorskega prostora) največ $n$ različnih lastnih vrednosti.

**Primer 1.13.** Poiščimo lastne vrednosti in lastne vektorje matrike

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

algebraične in geometrične večkratnosti lastnih vrednosti ter ugotovimo, ali se da matriko $A$ diagonalizirati.

Najprej poiščimo lastne vrednosti matrike $A$. Za to bomo potrebovali njen karakteristični polinom

$$\Delta_A(\lambda) = \begin{vmatrix} 2-\lambda & 1 & 2 & 0 \\ -1 & -\lambda & -1 & 0 \\ -1 & -1 & -1-\lambda & 0 \\ 0 & 0 & -1 & 1-\lambda \end{vmatrix}.$$

Ker so v zadnjem stolpcu matrike $A - \lambda I$ tri ničle, se zgornjo determinanto splača razviti po zadnjem stolpcu. Dobimo

$$\Delta_A(\lambda) = (1-\lambda) \begin{vmatrix} 2-\lambda & 1 & 2 \\ -1 & -\lambda & -1 \\ -1 & -1 & -1-\lambda \end{vmatrix}.$$

(Isti rezultat bi dobili tudi, če bi namesto razvoja upoštevali formulo za izračun bločno spodnje trikotne matrike.) Zdaj pa uporabimo pravilo za izračun $3 \times 3$ determinante, da dobimo

$$\Delta_A(\lambda) = (1-\lambda)\Big((2-\lambda)(-\lambda)(-1-\lambda)+1+2-(2-\lambda)-(1+\lambda)-2\lambda\Big) = (1-\lambda)(-\lambda^3+\lambda^2) = \lambda^2(1-\lambda)^2.$$

V zvezi s tem računom omenimo, da se splača čim več faktorjev karakterističnega čim prej izpostaviti, saj bo treba polinom v končni fazi razstaviti. Iščemo namreč ničle polinoma $\Delta_A(\lambda)$, in v našem primeru sta to 0 in 1. Torej sta 0 in 1 edini lastni vrednosti matrike $A$, obe imata algebraično večkratnost enako 2.

Poiščimo še lastne vektorje. Po definiciji so lastni vektorji matrike $A$ za lastno vrednost $\lambda$ neničelni elementi jedra matrike $A - \lambda I$. Lastni vrednosti 0 in 1 obravnavajmo posebej.

Lastni podprostor matrike $A$ za lastno vrednost 0 je jedro matrike $A$. Poiščemo ga s pomočjo Gaussove eliminacije:

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

Vektor $\begin{bmatrix} x \\ y \\ z \\ w \end{bmatrix}$ je torej v jedru matrike $A$ natanko takrat, ko je $z = w$, $y = 0$ in $x = -z = -w$.

Torej je lastni podprostor matrike $A$ za lastno vrednost 0 enak $\ker A = \left\{ \begin{bmatrix} -w \\ 0 \\ w \\ w \end{bmatrix} ; w \in \mathbb{C} \right\}$.

Ta prostor je 1-razsežen, njegov bazni vektor je npr. $\begin{bmatrix} -1 \\ 0 \\ 1 \\ 1 \end{bmatrix}$. Geometrična večkratnost lastne vrednosti 0 matrike $A$ je torej enaka 1.

Naredimo enako še za lastno vrednost 1. Lastni podprostor za to lastno vrednost je jedro matrike $A - I$. Izračunajmo ga:

$$A - I = \begin{bmatrix} 1 & 1 & 2 & 0 \\ -1 & -1 & -1 & 0 \\ -1 & -1 & -2 & 0 \\ 0 & 0 & -1 & 0 \end{bmatrix} \sim \begin{bmatrix} 1 & 1 & 2 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 \end{bmatrix} \sim \begin{bmatrix} 1 & 1 & 2 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}.$$

Vektor $\begin{bmatrix} x \\ y \\ z \\ w \end{bmatrix}$ je v jedru te matrike natanko takrat, ko je $z = 0$ in $x = -y$, torej je lastni podprostor matrike $A$ za lastno vrednost 1 enak $\ker(A - I) = \left\{ \begin{bmatrix} -y \\ y \\ 0 \\ w \end{bmatrix} ; y, w \in \mathbb{C} \right\}$. Ta prostor je 2-razsežen, njegova baza je npr. $\left\{ \begin{bmatrix} -1 \\ 1 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} \right\}$. To pomeni, da je geometrična večkratnost lastne vrednosti 1 matrike $A$ enaka 2.

Ker je lastni podprostor matrike $A$ za lastno vrednost 0 1-razsežen, lastni podprostor za lastno vrednost 1 pa 2-razsežen, je linearna ogrinjača lastnih vektorjev 3-razsežna. Torej ne obstaja baza prostora $\mathbb{C}^4$ sestavljena iz lastnih vektorjev matrike $A$, kar pomeni, da se $A$ ne da diagonalizirati.

V prejšnjem primeru smo videli, da so geometrične večkratnosti lastnih vrednosti manjše (ali enake) od algebraičnih. To ni slučaj, kar nam pove naslednja trditev.

**Trditev 1.14.** *Za vsako matriko $A \in \mathbb{C}^{n \times n}$ velja:*

1. *Če je $\alpha$ lastna vrednost matrike $A$, potem je njena algebraična večkratnost večja ali enaka kot geometrična.*

2. *Matriko $A$ se da diagonalizirati natanko takrat, ko ima vsaka njena lastna vrednost algebraično večkratnost enako geometrični.*

*Enako velja za endomorfizme.*

*Dokaz.* 1. Naj bo $m$ geometrična večkratnost lastne vrednosti $\alpha$. Potem obstajajo linearno neodvisni vektorji $v_1, \ldots, v_m \in \mathbb{C}^n$, da je $\ker(A - \alpha I) = \operatorname{Lin}\{v_1, \ldots, v_m\}$. Linearno neodvisno množico $\{v_1, \ldots, v_m\}$ dopolnimo do baze $\mathcal{B}$ prostora $\mathbb{C}^n$. Ker so $v_1, \ldots, v_m$ lastni vektorji matrike $A$ za lastno vrednost $\alpha$, je glede na bazo $\mathcal{B}$ matrika endomorfizma $A \in \mathcal{L}(\mathbb{C}^n)$ oblike $A_{\mathcal{B}}^{\mathcal{B}} = \begin{bmatrix} \alpha I_m & B \\ 0 & C \end{bmatrix}$ za neki matriki $B \in \mathbb{C}^{m \times (n-m)}$ in $C \in \mathbb{C}^{(n-m) \times (n-m)}$. Upoštevamo pravilo za determinanto bločno trikotne matrike in dobimo

$$\Delta_A(\lambda) = \det(A_{\mathcal{B}}^{\mathcal{B}} - \lambda I) = (\alpha - \lambda)^m \det(C - \lambda I).$$

$\alpha$ je torej vsaj $m$-kratna ničla karakterističnega polinoma matrike $A$, kar pomeni, da je njena algebraična večkratnost vsaj $m$.

2. Naj bodo $\lambda_1, \ldots, \lambda_k$ vse različne lastne vrednosti matrike $A$, $n_1, \ldots, n_k$ njihove algebraične večkratnosti in $m_1, \ldots, m_k$ njihove geometrične večkratnosti. Potem vemo, da je $n_1 + \cdots + n_k = n$ in $m_j \leq n_j$ za vsak $j = 1, \ldots, k$.

   Predpostavimo najprej, da se matriko $A$ da diagonalizirati. To pomeni, da obstaja baza prostora $\mathbb{C}^n$, sestavljena iz lastnih vektorjev matrike $A$. Linearno neodvisnih lastnih vektorjev matrike $A$ ne more biti več kot $m_1 + \cdots + m_k$, torej je

$$n \leq m_1 + \cdots + m_k \leq n_1 + \cdots + n_k = n.$$

   Leva in desna stran neenakosti sta enaki, zato morajo v vseh neenakostih veljati enakosti. Torej je $m_j = n_j$ za vsak $j = 1, \ldots, k$.

   Obratno, predpostavimo, da je $m_j = n_j$ za vsak $j = 1, \ldots, k$. Potem za vsako lastno vrednost $\lambda_j$ obstajajo linearno neodvisni lastni vektorji $v_{1,j}, \ldots, v_{n_j,j} \in \mathbb{C}^n$. Množica $\mathcal{B} = \{v_{i,j}; j = 1, \ldots, k, \forall j : 1 \leq i \leq n_j\}$ potem vsebuje $n_1 + \ldots + n_k = n$ lastnih vektorjev matrike $A$. Da bo trditev dokazana, je treba dokazati, da je $\mathcal{B}$ baza, in za to zadošča dokazati, da je linearno neodvisna množica. Pa predpostavimo, da je

$$\sum_{j=1}^{k} \sum_{i=1}^{n_j} \alpha_{ij} v_{i,j} = 0$$

   za neke skalarje $\alpha_{ij} \in \mathbb{C}$. Za vsak $j$ označimo $w_j = \sum_{i=1}^{n_j} \alpha_{ij} v_{i,j}$. Za fiksen $j$ vektorji $v_{1,j}, \ldots, v_{n_j,j}$ pripadajo lastnemu podprostoru matrike $A$ za lastno vrednost $\lambda_j$, zato je tudi $w_j \in \ker(A - \lambda_j I)$. Z besedami, vsak vektor $w_j$ je bodisi lastni vektor matrike $A$ za lastno vrednost $\lambda_j$ bodisi je enak 0. Ker so lastne vrednosti $\lambda_1, \ldots, \lambda_k$ paroma različne, so kakršni koli lastni vektorji, ki jim pripadajo, linearno neodvisni. Ker je $w_1 + \cdots + w_k = 0$, vektorji $w_1, \ldots, w_k$ niso lastni vektorji matrike $A$, ampak morajo biti vsi enaki 0. Za vsak $j$ je torej $\sum_{i=1}^{n_j} \alpha_{ij} v_{i,j} = 0$. Ker so vektorji $v_{1,j}, \ldots, v_{n_j,j}$ linearno neodvisni, od tod sledi $\alpha_{ij} = 0$ za vsak $j = 1, \ldots, k$ in vsak $i = 1, \ldots, n_j$. Množica $\mathcal{B}$ je torej linearno neodvisna, kar je bilo treba dokazati.

Za endomorfizme je dokaz enak. □

Pomemben izrek o karakterističnem polinomu matrike je Cayley-Hamiltonov izrek. Preden ga formuliramo, moramo še definirati, kdaj je matrika ničla polinoma. Če je $p(\lambda) = a_0 + a_1\lambda + \cdots a_k\lambda^k$ poljuben polinom in $A \in \mathbb{C}^{n \times n}$ poljubna kvadratna matrika, potem lahko izračunamo matriko $a_0 I + a_1 A + \cdots + a_k A^k \in \mathbb{C}^{n \times n}$. Ta izraz označimo s $p(A)$ in ga imenujemo *vrednost polinoma $p$ v matriki $A$*. V posebnem primeru se lahko zgodi, da je $p(A)$ ničelna matrika. V tem primeru pravimo, da je matrika $A$ *ničla* polinoma $p$.

**Izrek 1.15** (Cayley-Hamiltonov izrek). *Vsaka kvadratna matrika je ničla svojega karakterističnega polinoma. Zapisano s simboli: $\Delta_A(A) = 0$ za vsako kvadratno matriko $A$.*

*Dokaz.* Za vsajk $\lambda \in \mathbb{C}$ naj bo $B(\lambda) = \widetilde{A - \lambda I}$ prirejenka matrike $A - \lambda I$. Potem vemo, da za vsak $\lambda \in \mathbb{C}$ velja

$$B(\lambda)^T(A - \lambda I) = \det(A - \lambda I) \cdot I = \Delta_A(\lambda) I. \tag{2}$$

Označimo $B(\lambda) = [b_{ij}(\lambda)]_{i,j=1}^n$. Členi $b_{ij}(\lambda)$ so $(n-1) \times (n-1)$ poddeterminante matrike $A - \lambda I$, katere členi so linearni polinomi v $\lambda$, zato je vsak člen $b_{ij}(\lambda)$ polinom v spremenljivki $\lambda$ stopnje največ $n-1$. Matriko $B(\lambda)$ torej lahko zapišemo kot vsoto $B(\lambda) = B_0 + B_1\lambda + \cdots + B_{n-1}\lambda^{n-1}$ za neke matrike $B_0, B_1, \ldots, B_{n-1} \in \mathbb{C}^{n\times n}$. To je torej polinom, ki ima za koeficiente matrike. Pravimo mu *matrični polinom*. Naj bo $\Delta_A(\lambda) = a_0 + a_1\lambda + \cdots + a_n\lambda^n$. Potem iz (2) sledi, da za vsak $\lambda \in \mathbb{C}$ velja

$$\begin{aligned} & a_0 I + (a_1 I)\lambda + \cdots + (a_n I)\lambda^n = \Delta_A(\lambda) I = (B_0^T + B_1^T\lambda + \cdots + B_{n-1}^T\lambda^{n-1})(A - \lambda I) \\ = \; & B_0^T A + (B_1^T A - B_0^T)\lambda + (B_2^T A - B_1^T)\lambda^2 + \cdots + (B_{n-1}^T A - B_{n-2}^T)\lambda^{n-1} - B_{n-1}^T\lambda^n. \end{aligned}$$

Leva in desna stran zgornje enakosti sta torej matrična polinoma, ki sta enaka za vsak $\lambda \in \mathbb{C}$. Če polinome napišemo po členih, dobimo na vsaki strani enakosti $n^2$ skalarnih polinomov, in istoležni polinomi zavzamejo enako vrednost za vsak $\lambda \in \mathbb{C}$. Skalarna polinoma, ki zavzameta enake vrednosti v vseh kompleksnih številih, pa sta enaka (t.j. imata enake koeficiente). Torej je $n^2$ skalarnih polinomov na levi enakih istoležnim polinomom na desni, in matrični polinom na levi je enak matričnemu polinomu na desni (t.j. matrična polinoma imata enake koeficiente). Sledi:

$$\begin{aligned} B_0^T A &= a_0 I \\ B_1^T A - B_0^T &= a_1 I \\ B_2^T A - B_1^T &= a_2 I \\ &\vdots \\ B_{n-1}^T A - B_{n-2}^T &= a_{n-1} I \\ -B_{n-1}^T &= a_n I. \end{aligned}$$

Zdaj pa prvo enakost z desne pomnožimo z $I$, drugo z $A$, tretjo z $A^2$, ..., predzadnjo z $A^{n-1}$, zadnjo z $A^n$ in vse dobljene enakosti seštejemo. Dobimo

$$0 = a_0 I + a_1 A + \cdots + a_n A^n = \Delta_A(A),$$

kar je bilo treba dokazati. □

**Posledica 1.16.** *Če je $A \in \mathbb{C}^{n\times n}$ obrnljiva matrika, obstaja polinom $p(\lambda) \in \mathbb{C}[\lambda]$, da je $A^{-1} = p(A)$. Z besedami, inverz obrnljive matrike $A$ leži v podalgebri algebre $\mathbb{C}^{n\times n}$, generirani z matriko $A$.*

*Dokaz.* Naj bo $\Delta_A(\lambda) = a_0 + a_1\lambda + \cdots + a_n\lambda^n$ karakteristični polinom matrike $A$. Ker je $A$ obrnljiva, je

$$a_0 = \Delta_A(0) = \det A \neq 0.$$

Po Cayley-Hamiltonovem izreku je

$$a_n A^n + \cdots + a_1 A = -a_0 I.$$

Ker je $a_0$ obrnljiv, lahko zgornjo enačbo z $-a_0$ delimo. Po drugi strani pa lahko na levi strani z leve ali z desne izpostavimo $A$. Torej je

$$A\left(-\frac{a_n}{a_0}A^{n-1} - \cdots - \frac{a_1}{a_0}I\right) = \left(-\frac{a_n}{a_0}A^{n-1} - \cdots - \frac{a_1}{a_0}I\right)A = I.$$

To pa pomeni, da je

$$A^{-1} = -\frac{a_n}{a_0}A^{n-1} - \cdots - \frac{a_1}{a_0}I,$$

kar je polinom v matriki $A$. □

**Definicija 1.17.** *Minimalni polinom* matrike $A \in \mathbb{C}^{n\times n}$ je polinom z vodilnim koeficientom 1, ki ima ničlo $A$ in je med neničelnimi polinomi, ki imajo ničlo $A$, najmanjše stopnje. Označimo ga z $m_A(\lambda)$.

Definicija minimalnega polinoma nam ne pove niti, ali minimalni polinom matrike sploh obstaja, niti, ali je v primeru, ko obstaja, z matriko enolično določen. Zato najprej utemeljimo, da je oboje res: minimalni polinom vedno obstaja in je en sam. Za obstoj se spomnimo, da je po Cayley-Hamiltonovem izreku $A$ ničla karakterističnega polinoma $\Delta_A(\lambda)$. Torej obstaja neničelni polinom (karakteristični), ki ima $A$ za ničlo. Potem pa gotovo obstaja neničelni polinom najmanjše možne stopnje, ki ima $A$ za ničlo. Ta polinom delimo z vodilnim koeficientom in dobimo minimalni polinom matrike $A$.

Za enoličnost pa predpostavimo, da sta $p(\lambda) = a_0 + a_1\lambda + \cdots + a_k\lambda^k$ in $q(\lambda) = b_0 + b_1\lambda + \cdots + b_m\lambda^m$ minimalna polinoma za $A$. Ker je minimalni polinom po definiciji najmanjše možne stopnje, mora biti seveda $m = k$. Po definiciji minimalnega polinoma je tudi $a_k = b_k = 1$. Torej je

$$a_0I + a_1A + \cdots + a_{k-1}A^{k-1} + A^k = b_0I + b_1A + \cdots + b_{k-1}A^{k-1} + A^k = 0.$$

Potem pa je seveda

$$(a_0 - b_0)I + (a_1 - b_1)A + \cdots + (a_{k-1} - b_{k-1})A^{k-1} = 0.$$

Matrika $A$ je torej ničla polinoma $r(\lambda) = p(\lambda) - q(\lambda)$, ki pa je strogo manjše stopnje kot $p(\lambda)$ in $q(\lambda)$. Po minimalnosti stopnje torej sledi, da je polinom $r(\lambda)$ ničeln, torej sta polinoma $p(\lambda)$ in $q(\lambda)$ enaka.

Dokažimo zdaj nekatere lastnosti minimalnega polinoma matrike. Za dokaz prve izmed lastnosti se najprej iz gimnazije spomnimo osnovnega izreka o deljenju polinomov. Dokazali ga ne bomo, sledi pa iz algoritma deljenja za polinome.

**Izrek 1.18** (Osnovni izrek o deljenju polinomov)**.** *Če je $\mathcal{O}$ poljuben obseg in $p(\lambda), q(\lambda) \in \mathcal{O}[\lambda]$ poljubna polinoma, pri čemer je $q(\lambda)$ neničeln, potem obstajata (enolična) polinoma $k(\lambda), r(\lambda) \in \mathcal{O}[\lambda]$, da ima $r(\lambda)$ strogo manjšo stopnjo kot $q(\lambda)$ in je $p(\lambda) = q(\lambda)k(\lambda) + r(\lambda)$. Polinom $k(\lambda)$ se imenuje* kvocient*, polinom $r(\lambda)$ pa* ostanek *polinoma $p(\lambda)$ pri deljenju s $q(\lambda)$.*

**Trditev 1.19.** *Vsak neničelni polinom, ki ima za ničlo matriko $A$, je deljiv z minimalnim polinomom matrike $A$.*

*Dokaz.* Naj bo $p(\lambda)$ polinom, ki ima $A$ za ničlo, $m_A(\lambda)$ pa minimalni polinom matrike $A$. Po osnovnem izreku o deljenju polinomov obstajata polinoma $k(\lambda)$ in $r(\lambda)$, da je $r(\lambda)$ strogo manjše stopnje kot $m_A(\lambda)$ in velja $p(\lambda) = m_A(\lambda)k(\lambda) + r(\lambda)$. To je enakost polinomov, zato morata polinoma na levi in desni strani imeti enako vrednost v matriki $A$. Ker je $p(A) = 0$ po predpostavki, $m_A(A) = 0$ pa po definiciji minimalnega polinoma, sledi

$$0 = p(A) = m_A(A)k(A) + r(A) = r(A).$$

$A$ je torej ničla polinoma $r(\lambda)$, ki pa je nižje stopnje kot minimalni polinom matrike $A$. To je možno le, ko je $r(\lambda)$ ničelni polinom, oziroma ko je $p(\lambda) = m_A(\lambda)k(\lambda)$, oziroma z besedami, ko je polinom $p(\lambda)$ deljiv z minimalnim polinomom matrike $A$. □

Iz te trditve in Cayley-Hamiltonovega izreka takoj sledi:

**Posledica 1.20.** *Minimalni polinom matrike vedno deli njen karakteristični polinom.*

Od tod očitno sledi:

**Posledica 1.21.** *Vsaka ničla minimalnega polinoma matrike $A$ je tudi ničla karakterističnega polinoma matrike $A$.*

Čeprav karakteristični polinom ne deli minimalnega, pa velja obrat zadnje posledice.

**Trditev 1.22.** *Vsaka ničla karakterističnega polinoma matrike $A \in \mathbb{C}^{n\times n}$ je tudi ničla minimalnega polinoma matrike $A$.*

*Dokaz.* Naj bo $\alpha \in \mathbb{C}$ ničla karakterističnega polinoma $\Delta_A(\lambda)$. To pomeni, da je $\alpha$ lastna vrednost, torej obstaja neničelni vektor $v \in \mathbb{C}^n$, da je $Av = \alpha v$. Naj bo $m_A(\lambda)$ niminalni polinom matrike $A$. Po osnovnem izreku o deljenju polinomov obstajata polinom $p(\lambda) \in \mathbb{C}[\lambda]$ in konstanta $c \in \mathbb{C}$, da je $m_A(\lambda) = (\lambda-\alpha)p(\lambda)+c$. Polinoma na levi in desni strani sta enaka, zato zavzameta isto vrednost v matriki $A$. Torej je

$$m_A(A) = (A-\alpha I)p(A) + cI.$$

Leva stran zgornje enačbe je po definiciji minimalnega polinoma enaka 0. Na desni pa upoštevamo, da vsaka dva polinoma v isti matriki komutirata. (Razmislite, zakaj.) Torej je $(A-\alpha I)p(A) = p(A)\cdot(A-\alpha I)$ in zato

$$p(A)\cdot(A-\alpha I) + cI = 0.$$

Na obeh straneh enačbe imamo $n\times n$ matriko, ki jo lahko z desne pomnožimo z vektorjem $v$. Dobimo

$$p(A)\cdot(Av-\alpha v) + cv = 0.$$

Ker je $v$ lastni vektor matrike $A$ za lastno vrednost $\alpha$, je prvi člen v zgornji vsoti enak 0, torej je $cv = 0$. Vektor $v$ je neničeln, zato je $c = 0$. To pa pomeni, da je $m_A(\lambda) = (\lambda-\alpha)p(\lambda)$, oziroma z besedami, minimalni polinom matrike $A$ je deljiv s polinomom $\lambda - \alpha$. To pa pomeni, da je $\alpha$ ničla minimalnega polinoma matrike $A$. $\square$

Iz zadnje trditve in posledic pred njo sledi:

**Posledica 1.23.** *Naj bo $A \in \mathbb{C}^{n\times n}$ poljubna matrika. Vemo že, da je njen karakteristični polinom oblike $\Delta_A(\lambda) = (-1)^n(\lambda-\lambda_1)^{n_1}(\lambda-\lambda_2)^{n_2}\cdots(\lambda-\lambda_k)^{n_k}$, kjer so $\lambda_1,\ldots,\lambda_k$ vse različne lastne vrednosti matrike $A$ in $n_1,\ldots,n_k$ naravna števila, za katera je $n_1+\cdots+n_k = n$. Minimalni polinom je potem oblike $m_A(\lambda) = (\lambda-\lambda_1)^{m_1}(\lambda-\lambda_2)^{m_2}\cdots(\lambda-\lambda_k)^{m_k}$, kjer za vsak $j = 1,\ldots,k$ velja $1 \le m_j \le n_j$.*

**Primer 1.24.** Poiščimo minimalni polinom matrike $A = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$.

To bomo storili tako, da bomo najprej poiskali karakteristični polinom. Po pravilu za izračun determinante zgornje trikotne matrike je

$$\Delta_A(\lambda) = \left| \begin{matrix} 1-\lambda & 0 & 0 & 0 \\ 0 & -\lambda & 1 & 0 \\ 0 & 0 & -\lambda & 0 \\ 0 & 0 & 0 & -\lambda \end{matrix} \right] = (\lambda-1)\lambda^3.$$

Torej je $m_A(\lambda) = (\lambda-1)\lambda^k$ za nek $k \in \{1,2,3\}$. Poiskati moramo torej le še eksponent $k$. To storimo tako, da izračunamo $(A-I)A^k$. Za $k = 1$ dobimo

$$(A-I)A = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & -1 & 1 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \neq 0,$$

torej $(\lambda-1)\lambda$ ni minimalni polinom matrike $A$. Za $k=2$ pa je

$$(A-I)A^2 = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} = 0,$$

kar pomeni, da je $m_A(\lambda) = (\lambda-1)\lambda^2$.

Oglejmo si še, kako je z minimalnim polinomom pri spremembi baze.

**Trditev 1.25.** *Podobni matriki imata enak minimalni polinom.*

*Dokaz.* Naj bo $B = P^{-1}AP$ in $m_A(\lambda) = a_0 + a_1\lambda + \cdots + a_m\lambda^m$ minimalni polinom matrike $A$. Potem je

$$\begin{aligned} m_A(B) &= a_0I + a_1B + \cdots + a_mB^m = a_0I + a_1(P^{-1}AP) + \cdots + a_m(P^{-1}AP)^m \\ &= a_0I + a_1P^{-1}AP + a_2P^{-1}A^2P + \cdots + a_mP^{-1}A^mP \\ &= P^{-1}(a_0I + a_1A + a_2A^2 + \cdots + a_mA^m)P = P^{-1}m_A(A)P = 0, \end{aligned}$$

saj je $m_A(\lambda)$ minimalni polinom matrike $A$. Matrika $B$ je ničla polinoma $m_A(\lambda)$, zato po Trditvi 1.19 minimalni polinom $m_B(\lambda)$ matrike $B$ deli $m_A(\lambda)$. Ker je $A = PBP^{-1}$, zgornji argument lahko ponovimo, tako da zamenjamo $A$ in $B$ med seboj ter $P$ s $P^{-1}$. Tako dobimo, da je $m_B(A) = 0$ in posledično $m_A(\lambda)$ deli $m_B(\lambda)$. Ugotovili smo torej, da $m_A(\lambda)$ deli $m_B(\lambda)$ in $m_B(\lambda)$ deli $m_A(\lambda)$. To je mogoče le, ko je $m_B(\lambda) = cm_A(\lambda)$ za neko neničelno konstanto $c$. Toda vodilna koeficienta polinomov $m_A(\lambda)$ in $m_B(\lambda)$ sta oba enaka 1, od koder sledi $c=1$ in $m_B(\lambda) = m_A(\lambda)$. □

Zaradi te trditve je smiselna naslednja definicija.

**Definicija 1.26.** *Minimalni polinom endomorfizma $\mathcal{A} \in \mathcal{L}(V)$ je $m_A(\lambda)$, kjer je $A$ poljubna matrika, ki glede na neko bazo pripada endomorfizmu $\mathcal{A}$. Minimalni polinom endomorfizma $\mathcal{A}$ označimo z $m_{\mathcal{A}}(\lambda)$. Torej je $m_{\mathcal{A}}(\lambda) = m_A(\lambda)$, kjer je $A$ poljubna matrika, ki pripada endomorfizmu $\mathcal{A}$.*

Podobno, kot smo definirali vrednost polinoma v matriki, lahko definiramo tudi vrednost polinoma v endomorfizmu. Naj bo $p(\lambda) = a_0 + a_1\lambda + \cdots + a_k\lambda^k$ poljuben polinom in $\mathcal{A}$ endomorfizem vektorskega prostora $V$. Potem lahko izračunamo

$$a_0\mathrm{id}_V + a_1\mathcal{A} + a_2\mathcal{A}^2 + \cdots + a_k\mathcal{A}^k = a_0\mathrm{id}_V + a_1\mathcal{A} + a_2\mathcal{A}\circ\mathcal{A} + \cdots + a_k\underbrace{\mathcal{A}\circ\cdots\circ\mathcal{A}}_{k},$$

kar je spet endomorfizem prostora $V$. Označimo ga s $p(\mathcal{A})$ in imenujemo *vrednost polinoma $p(\lambda)$ v endomorfizmu $\mathcal{A}$*. Podobno kot pri matrikah rečemo, da je endomorfizem $\mathcal{A}$ *ničla* polinoma $p(\lambda)$, kadar je $p(\mathcal{A}) = 0$. Ekvivalentno bi lahko minimalni polinom endomorfizma definirali na enak način kot minimalni polinom matrike, kar nam pove naslednja trditev.

**Trditev 1.27.** *Minimalni polinom endomorfizma $\mathcal{A}$ je polinom z vodilnim koeficientom 1, ki ima $\mathcal{A}$ za ničlo in je najmanjše možne stopnje med neničelnimi polinomi, ki imajo $\mathcal{A}$ za ničlo.*

*Dokaz.* Naj bo $\mathcal{A}$ endomorfizem prostora $V$ in $\mathcal{B}$ poljubna baza prostora $V$. Spomnimo se, da je s predpisom $\Phi(\mathcal{A}) = \mathcal{A}_{\mathcal{B}}^{\mathcal{B}}$ definiran izomorfizem algeber $\Phi\colon \mathcal{L}(V) \to \mathbb{C}^{n\times n}$ (če je $\dim V = n$).

Oglejmo si, kako izomorfizem algeber preslika polinom v endomorfizmu. Naj bo $p(\lambda) = a_0 + a_1\lambda + \cdots + a_k\lambda^k \in \mathbb{C}[\lambda]$ poljuben polinom. Potem je

$$\begin{aligned}\Phi(p(\mathcal{A})) &= \Phi\left(a_0 \mathrm{id}_V + a_1\mathcal{A} + a_2\mathcal{A}\circ\mathcal{A} + \cdots + a_k \underbrace{\mathcal{A}\circ\cdots\circ\mathcal{A}}_{k}\right) \\ &= a_0\Phi(\mathrm{id}_V) + a_1\Phi(\mathcal{A}) + a_2\Phi(\mathcal{A})\Phi(\mathcal{A}) + \cdots + a_k \underbrace{\Phi(\mathcal{A})\cdots\Phi(\mathcal{A})}_{k} \\ &= a_0 I + a_1\Phi(\mathcal{A}) + \cdots + a_k\Phi(\mathcal{A})^k = p(\Phi(\mathcal{A})).\end{aligned}$$

Pri tem smo upoštevali, da je $\Phi$ homomorfizem algeber, ki torej slika kompozitum endomorfizmov v produkt matrik.

Naj bo $m_{\mathcal{A}}(\lambda)$ minimalni polinom endomorfizma $\mathcal{A}$. Njegov vodilni koeficient je enak 1 po definiciji. Dokažimo, da je $\mathcal{A}$ njegova ničla. Po definiciji minimalnega polinoma endomorfizma je vsaka matrika, ki pripada endomorfizmu $\mathcal{A}$, ničla polinoma $m_{\mathcal{A}}(\lambda)$. Torej je $m_{\mathcal{A}}(\Phi(\mathcal{A})) = 0$. Kot smo dokazali zgoraj, potem velja tudi $\Phi(m_{\mathcal{A}}(\mathcal{A})) = 0$. Ker je $\Phi$ injektiven, pa od tod sledi $m_{\mathcal{A}}(\mathcal{A}) = 0$, kar je bilo treba dokazati.

Dokažimo še, da je polinom $m_{\mathcal{A}}(\lambda)$ najnižje možne stopnje, ki ima $\mathcal{A}$ za ničlo. Naj bo $p(\lambda) \in \mathbb{C}[\lambda]$ še nek drug neničeln polinom, za katerega je $p(\mathcal{A}) = 0$. Potem je seveda tudi $\Phi(p(\mathcal{A})) = 0$ in po zgornji enakosti tudi $p(\Phi(\mathcal{A}))$. Z besedami, matrika $\Phi(\mathcal{A})$ je ničla polinoma $p(\lambda)$. Po Trditvi 1.19 od tod sledi, da je polinom $p(\lambda)$ deljiv z minimalnim polinomom matrike $\Phi(\mathcal{A})$. Po definiciji minimalnega polinoma endomorfizma pa je $m_{\mathcal{A}}(\lambda) = m_{\Phi(\mathcal{A})}(\lambda)$, kar pomeni, da je polinom $p(\lambda)$ deljiv z minimalnim polinomom endomorfizma $\mathcal{A}$. V posebnem primeru je torej stopnja polinoma $m_{\mathcal{A}}(\lambda)$ manjša ali enaka stopnji polinoma $p(\lambda)$. □

V zgornjem dokazu smo dokazali tudi, da Trditev 1.19 ne velja le za matrike, ampak tudi za endomorfizme.

## 2 Korenski podprostori

V prejšnjem poglavju smo si ogledali več karakterizacij, kdaj se endomorfizem da diagonalizirati. V nadaljevanju bomo poiskali "lepo"matriko, ki pripada endomorfizmu, v primeru, ko se tega ne da diagonalizirati. Za začetek bomo v tem poglavju dokazali, da endomorfizmu vedno pripada boločno diagonalna matrika, kjer ima vsak diagonalni blok le eno lastno vrednost.

**Definicija 2.1.** Naj bo $\mathcal{A}$ endomorfizem vektorskega prostora $V$. Vektorski podprostor $U$ prostora $V$ je *invarianten* za endomorfizem $\mathcal{A}$, kadar je $\mathcal{A}x \in U$ za vsak $x \in U$. To zapišemo tudi kot $\mathcal{A}U \subseteq U$.

**Primeri 2.2.** 1. $\{0\}$ in $V$ sta invariantna podprostora vsakega endomorfizma prostora $V$.

2. Jedro in slika endomorfizma $\mathcal{A}$ sta vedno invariantna za $\mathcal{A}$. Če je namreč $x \in \ker\mathcal{A}$, potem je $\mathcal{A}x = 0$, kar seveda tudi pripada jedru $\ker\mathcal{A}$. Podobno, če je $x \in \operatorname{im}\mathcal{A}$, potem je po definiciji slike tudi $\mathcal{A}x \in \operatorname{im}\mathcal{A}$ (in za to niti ni nujno, da je $x \in \operatorname{im}\mathcal{A}$).

3. Vsak lastni podprostor endomorfizma $\mathcal{A}$ je invarianten za $\mathcal{A}$. Če je namreč $\mathcal{A}x = \lambda x$, potem je tudi
$$\mathcal{A}(\mathcal{A}x) = \mathcal{A}(\lambda x) = \lambda(\mathcal{A}x),$$
kar pomeni, da je $\mathcal{A}x \in \ker(\mathcal{A} - \lambda\,\mathrm{id}_V)$.

4. Naj bo $\mathcal{A} \in \mathcal{L}(\mathbb{R}^3)$ rotacija za $\frac{\pi}{2}$ okrog $z$-osi. Vemo že, da sta invariantna prostora $\{0\}$ in $\mathbb{R}^3$. $z$-os se pri rotaciji ohranja, kar pomeni, da je invarianten podprostor za $\mathcal{A}$. Natančneje,

$z$-os je lastni podprostor za $\mathcal{A}$ za lastno vrednost 1. Prav tako se vsak vektor iz ravnine $z = 0$ preslika v vektor iz te ravnine, kar pomeni, da je tudi ravnina $z = 0$ invarianten podprostor za $\mathcal{A}$, ni pa lastni podprostor.

Naj bo $U \subseteq V$ invarianten podprostor za endomorfizem $\mathcal{A} \in \mathcal{L}(V)$. Potem po definiciji invariantnega podprostora velja $\mathcal{A}x \in U$ za vsak $x \in U$. Torej je zožitev $\mathcal{A}|_U$ preslikava, ki slika iz $U$ v $U$. Ker je $\mathcal{A}$ linearna preslikava, je tudi $\mathcal{A}|_U$ linearna preslikava, torej endomorfizem prostora $U$.

**Trditev 2.3.** *Naj bo $U \subseteq V$ invarianten podprostor za endomorfizem $\mathcal{A} \in \mathcal{L}(V)$ in naj bo $\{u_1, \ldots, u_m\}$ baza prostora $U$. To bazo dopolnimo do baze $\mathcal{B} = \{u_1, \ldots, u_m, v_1, \ldots, v_k\}$ prostora $V$. Potem je matrika $\mathcal{A}_{\mathcal{B}}^{\mathcal{B}}$ bločno zgornje trikotna. Natančneje, enaka je $\begin{bmatrix} A_1 & A_2 \\ 0 & A_3 \end{bmatrix}$, kjer je $A_1 \in \mathbb{C}^{m\times m}$, $A_2 \in \mathbb{C}^{m\times k}$ in $A_3 \in \mathbb{C}^{k\times k}$ in je $A_1$ matrika endomorfizma $\mathcal{A}|_U$ prostora $U$, zapisana glede na bazo $\{u_1, \ldots, u_m\}$.*

*Dokaz.* Ker je $U$ invarianten podprostor za $\mathcal{A}$, za vsak $j = 1, \ldots, m$ velja $\mathcal{A}u_j \in U$ in $\mathcal{A}u_j = \mathcal{A}|_U u_j$. Ker je $\{u_1, \ldots, u_m\}$ baza za $U$, torej obstajajo skalarji $a_{ij} \in \mathbb{C}$ $(1 \le i, j \le m)$, da za vsak $j = 1, \ldots, m$ velja $\mathcal{A}u_j = a_{1j}u_1 + \cdots + a_{mj}u_m$. To pomeni, da je matrika endomorfizma $\mathcal{A}|_U$ prostora $U$ glede na bazo $\{u_1, \ldots, u_m\}$ enaka $A_1 = \begin{bmatrix} a_{11} & \cdots & a_{1m} \\ \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{mm} \end{bmatrix}$. Seveda za vsak $j = 1, \ldots, m$ velja tudi $\mathcal{A}u_j = a_{1j}u_1 + \cdots + a_{mj}u_m + 0\cdot v_1 + \cdots + 0\cdot v_k$, kar pomeni, da je podmatrika matrike $\mathcal{A}_{\mathcal{B}}^{\mathcal{B}}$, sestavljena iz prvih $m$ stolpcev, enaka $\begin{bmatrix} A_1 \\ 0 \end{bmatrix}$, in zato je $\mathcal{A}_{\mathcal{B}}^{\mathcal{B}} = \begin{bmatrix} A_1 & A_2 \\ 0 & A_3 \end{bmatrix}$ za neki matriki $A_2 \in \mathbb{C}^{m\times k}$ in $A_3 \in \mathbb{C}^{k\times k}$. □

**Primeri 2.4.**

1. Naj bo $V$ prostor realnih polinomov stopnje največ 2 in $\mathcal{A}\colon V \to V$ odvajanje. Konstantni polinomi tvorijo lastni podprostor endomorfizma $\mathcal{A}$ za lastno vrednost 0, kar je invarianten podprostor za $\mathcal{A}$. Ta podprostor je enorazsežen z bazo $\{1\}$. To bazo dopolnimo do baze $\{1, x, x^2\}$ prostora $V$. V tej bazi je matrika endomorfizma $\mathcal{A}$ enaka $\left[\begin{array}{c|cc} 0 & 1 & 0 \\ \hline 0 & 0 & 2 \\ 0 & 0 & 0 \end{array}\right]$. Vidimo, da je matrika zgornje trikotna in da zgornji levi $1\times 1$ blok ustreza zožitvi endomorfizma $\mathcal{A}$ na podprostor konstantnih polinomov, saj je zožitev endomorfizma $\mathcal{A}$ na ta podprostor ničelna preslikava.

2. Naj bo $\mathcal{A}\colon \mathbb{R}^3 \to \mathbb{R}^3$ rotacija za kot $\frac{\pi}{2}$ okrog $z$-osi. Iz prejšnjega primera vemo, da sta $z$-os (označimo jo z $U$) in ravnina $z = 0$ (označimo jo z $W$) invariantna podprostora za $\mathcal{A}$. Za $U$ izberimo bazo $\{\vec{k}\}$, za $W$ pa bazo $\{\vec{i}, \vec{j}\}$. Glede na ti dve bazi zožitvi $\mathcal{A}|_U$ pripada matrika $[1]$, zožitvi $\mathcal{A}|_W$ pa matrika $\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$. Naj bo $\mathcal{B} = \{\vec{k}, \vec{i}, \vec{j}\}$. Potem je $\mathcal{A}_{\mathcal{B}}^{\mathcal{B}} = \left[\begin{array}{c|cc} 1 & 0 & 0 \\ \hline 0 & 0 & -1 \\ 0 & 1 & 0 \end{array}\right]$. Vidimo, da je matrika v tem primeru celo bločno diagonalna, diagonalna bloka pa sta matriki, ki pripadata zožitvama endomorfizma $\mathcal{A}$ na $U$ in $W$. V naslednji trditvi bomo videli, da je vzrok v tem, da je $\mathbb{R}^3$ direktna vsota podprostorov $U$ in $W$, ki sta invariantna za $\mathcal{A}$.

**Trditev 2.5.** *Naj bo $\mathcal{A}$ endomorfizem prostora $V$ in $V = V_1 \oplus \cdots \oplus V_k$, kjer je $V_j$ invarianten podprostor za $\mathcal{A}$ za vsak $j = 1, \ldots, k$. Potem je matrika endomorfizma $\mathcal{A}$ v neki bazi bločno* *diagonalna. Natančneje, enaka je* $\begin{bmatrix} A_1 & & & \\ & A_2 & & \\ & & \ddots & \\ & & & A_k \end{bmatrix}$, *kjer je za vsak* $j$ $A_j$ *matrika zožitve* $\mathcal{A}|_{V_j}\colon V_j \to V_j$ *glede na neko bazo prostora* $V_j$. *Pravimo, da je matrika* $A$ direktna vsota *matrik* $A_1, \ldots, A_k$ *in pišemo* $A = A_1 \oplus \cdots \oplus A_k$. *Prav tako pravimo, da je endomorfizem* $\mathcal{A}$ *direktna vsota zožitev* $\mathcal{A}_j = \mathcal{A}|_{V_j}$ *in pišemo* $\mathcal{A} = \mathcal{A}_1 \oplus \cdots \oplus \cdots \mathcal{A}_k$.

*Dokaz.* Trditev je pravzaprav poseben primer prejšnje trditve, zato je tudi dokaz podoben.

Za vsak $j = 1, \ldots, k$ označimo $\mathcal{A}_j = \mathcal{A}|_{V_j}$, izberimo bazo $\mathcal{B}_j = \{v_{1,j}, \ldots, v_{n_j,j}\}$ prostora $V_j$ in naj bo $A_j$ matrika endomorfizma $\mathcal{A}_j \in \mathcal{L}(V_j)$ glede na bazo $\mathcal{B}_j$. Za vsak $j$ označimo še

$$A_j = \begin{bmatrix} a_{1,1}^{(j)} & \cdots & a_{1,n_j}^{(j)} \\ \vdots & \ddots & \vdots \\ a_{n_j,1}^{(j)} & \cdots & a_{n_j,n_j}^{(j)} \end{bmatrix}. \tag{3}$$

To pomeni, da za vsak $j = 1, \ldots, k$ in vsak $i = 1, \ldots, n_j$ velja

$$\mathcal{A}_j v_{i,j} = a_{1,i}^{(j)} v_{1,j} + \cdots + a_{n_j,i}^{(j)} v_{n_j,j}. \tag{4}$$

Ker je $V = V_1 \oplus \cdots \oplus V_k$, vemo, da je $\mathcal{B} = \mathcal{B}_1 \cup \cdots \cup \mathcal{B}_k$ baza prostora $V$. Naj bo $A$ matrika endomorfizma $\mathcal{A}$ glede na bazo $\mathcal{B}$. Element $v_{i,j}$ baze $\mathcal{B}$ (kjer je $1 \leq j \leq k$ in $1 \leq i \leq n_j$) leži v $\mathcal{B}_j$, zato je $\mathcal{A}v_{i,j} = \mathcal{A}_j v_{i,j}$ po definiciji zožitve. Iz (4) torej sledi, da za vsak element $v_{i,j}$ baze $\mathcal{B}$ velja

$$\begin{aligned} \mathcal{A}v_{i,j} &= \mathcal{A}_j v_{i,j} = a_{1,i}^{(j)} v_{1,j} + \cdots + a_{n_j,i}^{(j)} v_{n_j,j} \\ &= 0 \cdot v_{1,1} + \cdots + 0 \cdot v_{n_{j-1},j-1} + a_{1,i}^{(j)} v_{1,j} + \cdots + a_{n_j,i}^{(j)} v_{n_j,j} + 0 \cdot v_{1,j+1} + \cdots + 0 \cdot v_{n_k,k}. \end{aligned}$$

To pomeni, da je za vsak $j = 1, \ldots, k$ in vsak $i = 1, \ldots, n_j$ $(n_1 + \cdots + n_{j-1} + i)$-ti stolpec matrike $A$ enak $\begin{bmatrix} 0 \\ \vdots \\ 0 \\ a_{1,i}^{(j)} \\ \vdots \\ a_{n_j,i}^{(j)} \\ 0 \\ \vdots \\ 0 \end{bmatrix}$. Iz definicije števil $a_{l,i}^{(j)}$, podani v (3), od tod sledi, da je

$$A = \begin{bmatrix} A_1 & & & \\ & A_2 & & \\ & & \ddots & \\ & & & A_k \end{bmatrix}.$$ □

Do konca poglavja o korenskih podprostorih fiksirajmo naslednje oznake. $V$ naj bo $n$-razsežen kompleksen vektorski prostor, $\mathcal{A}$ endomorfizem prostora $V$, $\lambda_1, \ldots, \lambda_k$ vse njegove različne lastne vrednosti, $\Delta_{\mathcal{A}}(\lambda) = (-1)^n(\lambda - \lambda_1)^{n_1} \cdots (\lambda - \lambda_k)^{n_k}$ njegov karakteristični polinom in $m_{\mathcal{A}}(\lambda) = (\lambda - \lambda_1)^{m_1} \cdots (\lambda - \lambda_k)^{m_k}$ njegov minimalni polinom.

**Definicija 2.6.** Podprostor $W_j := \ker(\mathcal{A} - \lambda_j \operatorname{id}_V)^{m_j}$ prostora $V$ se imenuje *korenski podprostor* za endomorfizem $\mathcal{A}$, ki pripada lastni vrednosti $\lambda_j$.

Najprej omenimo, da je množica $W_i$ jedro nekega endomorfizma, zato je res vektorski podprostor prostora $V$. Prav tako očitno velja $\ker(\mathcal{A} - \lambda_j \operatorname{id}_V) \subseteq \ker(\mathcal{A} - \lambda_j \operatorname{id}_V)^{m_j}$, torej korenski podprostor, ki pripada lastni vrednosti $\lambda_j$, vsebuje ustrezni lastni podprostor. V posebnem primeru je vsak korenski podprostor netrivialen.

Radi bi uporabili prejšnjo trditev, kjer bomo za podprostore $V_j$ vzeli korenske podprostore. Na ta način bomo dobili matriko bazo endomorfizma $\mathcal{A}$, ki bo bločno diagonalna. Za to pa moramo preveriti, ali veljajo predpostavke prejšnje trditve, torej ali so korenski podprostori invariantni za $\mathcal{A}$ in ali je $V$ njihova direktna vsota.

**Trditev 2.7.** *Vsak korenski podprostor $W_j = \ker(\mathcal{A} - \lambda_j \operatorname{id}_V)^{m_j}$ je invarianten za endomorfizem $\mathcal{A}$.*

*Dokaz.* Naj bo $x \in W_j$. Po definiciji to pomeni, da je $(\mathcal{A} - \lambda_j \operatorname{id}_V)^{m_j} x = 0$. Endomorfizma $\mathcal{A}$ in $(\mathcal{A} - \lambda_j \operatorname{id}_V)^{m_j}$ komutirata, saj je drugi endomorfizem polinom v $\mathcal{A}$. Zato je

$$(\mathcal{A} - \lambda_j \operatorname{id}_V)^{m_j} (\mathcal{A}x) = \mathcal{A}\, (\mathcal{A} - \lambda_j \operatorname{id}_V)^{m_j}\, x = \mathcal{A}(0) = 0.$$

To pa pomeni, da je $\mathcal{A}x \in \ker(\mathcal{A} - \lambda_j \operatorname{id}_V)^{m_j} = W_j$. Torej je podprostor $W_j$ invarianten za $\mathcal{A}$. $\square$

Za dokaz dejstva, da je $V$ direktna vsota korenskih podprostorov, pa bomo potrebovali naslednji rezultat o polinomih. Izreka ne bomo dokazali, dokaže pa se ga pri Algebri 2.

**Izrek 2.8.** *Naj bo $\mathcal{O}$ poljuben obseg in naj bo $d(\lambda)$ največji skupni delitelj polinomov $p_1(\lambda), \ldots, p_k(\lambda) \in \mathcal{O}[\lambda]$. Potem obstajajo polinomi $q_1(\lambda), \ldots, q_k(\lambda) \in \mathcal{O}[\lambda]$, da je*

$$d(\lambda) = p_1(\lambda)q_1(\lambda) + \cdots + p_k(\lambda)q_k(\lambda).$$

**Opomba 2.9.** Kot že omenjeno, izreka ne bomo dokazali. Spomnimo pa se, da enaka lastnost velja za cela števila: Če je $d$ največji skupni delitelj celih števil $a_1, \ldots, a_k$, potem obstajajo cela števila $b_1, \ldots, b_k$, da je $a_1b_1 + \cdots + a_kb_k = d$. Če je $k = 2$, števili $b_1$ in $b_2$ dobimo z Evklidovem algoritmom. V primeru $k = 2$ tudi polinoma $q_1(\lambda)$ in $q_2(\lambda)$ iz izreka dobimo z Evklidovim algoritmom. Nasploh ima kolobar polinomov nad obsegom podobne računske lastnosti kot cela števila, kar je posledica dejstva, da v obeh kolobarjih velja osnovni izrek o deljenju.

**Izrek 2.10.** *Prostor $V$ je direktna vsota korenskih podprostorov za endomorfizem $\mathcal{A}$. Zapisano s simboli: $V = W_1 \oplus \cdots \oplus W_k$.*

*Dokaz.* Za vsak $j = 1, \ldots, k$ definirajmo polinom

$$p_j(\lambda) = \prod_{i \neq j} (\lambda - \lambda_i)^{m_i} = \frac{m_{\mathcal{A}}(\lambda)}{(\lambda - \lambda_j)^{m_j}} \in \mathbb{C}[\lambda].$$

Polinomi $p_1(\lambda), \ldots, p_k(\lambda)$ očitno nimajo skupne ničle. Po osnovnem izreku algebre so zato tuji: njihovi skupni delitelji so le konstante. Po prejšnjem izreku zato obstajajo polinomi $q_1(\lambda), \ldots, q_k(\lambda) \in \mathbb{C}[\lambda]$, da je

$$p_1(\lambda)q_1(\lambda) + \cdots + p_k(\lambda)q_k(\lambda) = 1.$$

V to enakost polinomov lahko vstavimo endomorfizem $\mathcal{A}$ in dobimo

$$p_1(\mathcal{A})q_1(\mathcal{A}) + \cdots + p_k(\mathcal{A})q_k(\mathcal{A}) = \operatorname{id}_V. \tag{5}$$

Spomnimo se, da je za dokaz enakosti $V = W_1 \oplus \cdots \oplus W_k$ treba dokazati, da se vsak vektor $x \in V$ na enoličen način zapiše kot $x = x_1 + \cdots + x_k$, kjer je $x_j \in W_j$ za vsak $j = 1, \ldots, k$. Najprej dokažimo obstoj takega zapisa. V ta namen za vsak $j = 1, \ldots, k$ definirajmo $x_j = p_j(\mathcal{A})q_j(\mathcal{A})x$. Ker je $(\lambda - \lambda_j)^{m_j} p_j(\lambda) = m_{\mathcal{A}}(\lambda)$, je $(\mathcal{A} - \lambda_j \operatorname{id}_V)^{m_j} p_j(\mathcal{A}) = m_{\mathcal{A}}(\mathcal{A}) = 0$, zato za vsak $j$ velja

$$(\mathcal{A} - \lambda_j \operatorname{id}_V)^{m_j} x_j = (\mathcal{A} - \lambda_j \operatorname{id}_V)^{m_j} p_j(\mathcal{A})q_j(\mathcal{A})x = m_{\mathcal{A}}(\mathcal{A})q_j(\mathcal{A})x = 0.$$

To pomeni, da je $x_j \in \ker(\mathcal{A} - \lambda_j \operatorname{id}_V)^{m_j} = W_j$ za vsak $j = 1, \ldots, k$. Poleg tega iz (5) sledi

$$x_1 + \ldots + x_k = p_1(\mathcal{A})q_1(\mathcal{A})x + \cdots + p_k(\mathcal{A})q_k(\mathcal{A})x = \left(p_1(\mathcal{A})q_1(\mathcal{A}) + \cdots + p_k(\mathcal{A})q_k(\mathcal{A})\right)x = \operatorname{id}_V x = x.$$

Torej je $V = W_1 + \cdots + W_k$.

Dokazati je treba še enoličnost razcepa $x = x_1 + \cdots + x_k$. Naj bo torej $x = x_1 + \cdots + x_k = y_1 + \cdots + y_k$, kjer sta $x_j, y_j \in W_j$ za vsak $j$. Za vsak $j$ definirajmo $z_j = y_j - x_j$. Ker je $W_j$ vektorski podprostor prostora $V$, je $z_j \in W_j$ za vsak $j$. Poleg tega velja

$$z_1 + \cdots + z_k = 0. \tag{6}$$

Če je $i \neq j$, potem je

$$p_i(\mathcal{A})z_j = \prod_{l \neq i} (\mathcal{A} - \lambda_l \operatorname{id}_V)^{m_l} z_j = \prod_{l \neq i,j} (\mathcal{A} - \lambda_l \operatorname{id}_V)^{m_l} \left((\mathcal{A} - \lambda_j \operatorname{id}_V)^{m_j} z_j\right) = 0,$$

kjer smo na koncu upoštevali, da je $z_j \in W_j = \ker(\mathcal{A} - \lambda_j \operatorname{id}_V)^{m_j}$. Iz enakosti (6) zdaj sledi še

$$p_j(\mathcal{A})z_j = \sum_{i=1}^{k} p_j(\mathcal{A})z_i = p_j(\mathcal{A}) \left(\sum_{i=1}^{k} z_i\right) = p_j(\mathcal{A})(0) = 0.$$

Dokazali smo torej, da je $p_i(\mathcal{A})z_j = 0$ za vsaka $i, j = 1, \ldots, k$. Če upoštevamo, da endomorfizma $p_j(\mathcal{A})$ in $q_j(\mathcal{A})$ komutirata, zdaj iz (5) sledi

$$z_j = \operatorname{id}_V z_j = \sum_{i=1}^{k} p_i(\mathcal{A})q_i(\mathcal{A})z_j = \sum_{i=1}^{k} q_i(\mathcal{A}) \left(p_i(\mathcal{A})z_j\right) = 0$$

za vsak $j$. To pomeni, da je $x_j = y_j$ za vsak $j = 1, \ldots, k$, torej je vsota $V = W_1 + \cdots + W_k$ direktna. $\square$

Iz Trditve 2.5 in tega izreka takoj sledi:

**Posledica 2.11.** *V neki bazi endomorfizmu $\mathcal{A}$ pripada matrika* $A = \begin{bmatrix} A_1 & & & \\ & A_2 & & \\ & & \ddots & \\ & & & A_k \end{bmatrix}$, *kjer je za vsak $j$ $A_j$ matrika, ki v neki bazi pripada zožitvi $\mathcal{A}|_{W_j} \in \mathcal{L}(W_j)$.*

Ugotovimo še, kakšne so velikosti matrik $A_j$ in kako so njihovi karakteristični in minimalni polinomi povezani s karakterističnim in minimalnim polinomom matrike $A$ (oz. endomorfizma $\mathcal{A}$).

**Izrek 2.12.** *Za $j = 1, \ldots, k$ definirajmo $\mathcal{A}_j = \mathcal{A}|_{W_j} \in \mathcal{L}(W_j)$. Potem je $\Delta_{\mathcal{A}_j}(\lambda) = (-1)^{n_j}(\lambda - \lambda_j)^{n_j}$ karakteristični polinom zožitve $\mathcal{A}_j$, $m_{\mathcal{A}_j}(\lambda) = (\lambda - \lambda_j)^{m_j}$ pa njen minimalni polinom.*

*Dokaz.* V neki bazi prostora $V$ je matrika $A$, ki pripada endomorfizmu $\mathcal{A}$, kot v prejšnji posledici. Po pravilu za determinanto bločno diagonalne matrike zdaj sledi

$$\Delta_{\mathcal{A}}(\lambda) = \Delta_A(\lambda) = \det(A - \lambda I) = \det(A_1 - \lambda I) \cdots \det(A_k - \lambda I) = \Delta_{\mathcal{A}_1}(\lambda) \cdots \Delta_{\mathcal{A}_k}(\lambda). \tag{7}$$

Za vsak $j = 1, \ldots, k$ in vsak $x \in W_j$ je

$$(\mathcal{A}_j - \lambda_j \operatorname{id}_{W_j})^{m_j} x = ((\mathcal{A} - \lambda_j \operatorname{id}_V)^{m_j})\,|_{W_j} x = (\mathcal{A} - \lambda_j \operatorname{id}_V)^{m_j} x = 0$$

po definiciji prostora $W_j$. To pa pomeni, da je $(\mathcal{A}_j - \lambda_j \operatorname{id}_{W_j})^{m_j} = 0$, kar z drugimi besedami pomeni, da je $\mathcal{A}_j$ ničla polinoma $(\lambda - \lambda_j)^{m_j}$. Po definiciji minimalnega polinoma potem minimalni polinom $m_{\mathcal{A}_j}(\lambda)$ endomorfizma $\mathcal{A}_j$ deli polinom $(\lambda - \lambda_j)^{m_j}$ za vsak $j$. To je možno le, ko je $m_{\mathcal{A}_j}(\lambda) = (\lambda - \lambda_j)^{s_j}$ za nek $s_j \in \{1, \ldots, m_j\}$. Ker imata karakteristični in minimalni polinom endomorfizma iste ničle (z morda drugačnimi večkratnostmi), od tod sledi še $\Delta_{\mathcal{A}_j}(\lambda) = (-1)^{t_j}(\lambda - \lambda_j)^{t_j}$ za nek $t_j \geq s_j$. Iz enakosti (7) zdaj sledi

$$(-1)^n(\lambda-\lambda_1)^{n_1} \cdots (\lambda-\lambda_k)^{n_k} = \Delta_{\mathcal{A}}(\lambda) = \Delta_{\mathcal{A}_1}(\lambda) \cdots \Delta_{\mathcal{A}_k}(\lambda) = (-1)^{t_1+\cdots+t_k}(\lambda-\lambda_1)^{t_1} \cdots (\lambda-\lambda_k)^{t_k}.$$

Enaka polinoma imata enake večkratnosti ničel, zato je $t_j = n_j$ za vsak $j = 1, \ldots, k$. Sledi, da je $\Delta_{\mathcal{A}_j}(\lambda) = (-1)^{n_j}(\lambda - \lambda_j)^{n_j}$ za vsak $j$.

Poiščimo še minimalne polinome zožitev $\mathcal{A}_j$. Vemo že, da za vsak $j$ velja $m_{\mathcal{A}_j}(\lambda) = (\lambda - \lambda_j)^{s_j}$ za nek $s_j \in \{1, \ldots, m_j\}$. Definirajmo $p(\lambda) = (\lambda - \lambda_1)^{s_1} \cdots (\lambda - \lambda_k)^{s_k}$. Dokazali bomo, da je $p(\mathcal{A}) = 0$. V ta namen izberimo poljuben $x \in V$. Ker je $V$ direktna vsota podprostorov $W_1, \ldots, W_k$, vektor $x$ lahko zapišemo v obliki $x = x_1 + \cdots + x_k$, kjer je $x_j \in W_j$ za vsak $j$. Zdaj pa lahko izračunamo

$$\begin{aligned}
p(\mathcal{A})x &= \prod_{i=1}^{k} (\mathcal{A} - \lambda_i \operatorname{id}_V)^{s_i} \left( \sum_{j=1}^{k} x_j \right) = \sum_{j=1}^{k} \prod_{i=1}^{k} (\mathcal{A} - \lambda_i \operatorname{id}_V)^{s_i} x_j \\
&= \sum_{j=1}^{k} \left( \prod_{i \neq j} (\mathcal{A} - \lambda_i \operatorname{id}_V)^{s_i} \left( (\mathcal{A} - \lambda_j \operatorname{id}_V)^{s_j} x_j \right) \right) \\
&= \sum_{j=1}^{k} \left( \prod_{i \neq j} (\mathcal{A} - \lambda_i \operatorname{id}_V)^{s_i} \left( (\mathcal{A}_j - \lambda_j \operatorname{id}_{W_j})^{s_j} x_j \right) \right) = 0.
\end{aligned}$$

Pri tem smo upoštevali, da za vsak $j$ velja $x_j \in W_j$ in zato $(\mathcal{A} - \lambda_j \operatorname{id}_V)^{s_j} x_j = (\mathcal{A}_j - \lambda_j \operatorname{id}_{W_j})^{s_j} x_j$ ter da je $(\lambda - \lambda_j)^{s_j}$ minimalni polinom endomorfizma $\mathcal{A}_j$ in je zato $(\mathcal{A}_j - \lambda_j \operatorname{id}_{W_j})^{s_j} = 0$. Dokazali smo torej, da je $p(\mathcal{A}) = 0$. Od tod pa sledi, da je polinom $p(\lambda)$ deljiv z minimalnim polinomom endomorfizma $\mathcal{A}$. Torej je polinom $(\lambda - \lambda_1)^{s_1} \cdots (\lambda - \lambda_k)^{s_k}$ deljiv s polinomom $(\lambda - \lambda_1)^{m_1} \cdots (\lambda - \lambda_k)^{m_k}$. To pa je možno le, ko je $m_j \leq s_j$ za vsak $j = 1, \ldots, k$. Vemo pa že, da je $s_j \leq m_j$, torej je $s_j = m_j$ za vsak $j$. Minimalni polinom zožitve $\mathcal{A}_j$ je torej za vsak $j$ enak $(\lambda - \lambda_j)^{m_j}$.

□

Ker je stopnja karakterističnega polinoma matrike enaka velikosti matrike, iz zgornjega izreka takoj sledi:

**Posledica 2.13.** $A_j \in \mathbb{C}^{n_j \times n_j}$ *za vsak* $j = 1, \ldots, k$.

**Posledica 2.14.** *Endomorfizem se da diagonalizirati natanko takrat, ko ima njegov minimalni polinom same enostavne ničle (t.j. stopnje 1).*

*Dokaz.* Najprej predpostavimo, da se endomorfizem $\mathcal{A}$ da diagonalizirati in naj bo $A$ pripadajoča diagonalna matrika, $\lambda_1, \ldots, \lambda_k$ pa vse različne lastne vrednosti endomorfizma $\mathcal{A}$. Definirajmo $p(\lambda) = (\lambda - \lambda_1) \cdots (\lambda - \lambda_k)$. Matrika $A$ ima po diagonali elemente $\lambda_1, \ldots, \lambda_k$, pri čemer se nekateri lahko pojavijo večkrat. Od tod očitno sledi, da je $p(A) = 0$. To pomeni, da je polinom $p(\lambda)$ deljiv z minimalnim polinomom endomorfizma $\mathcal{A}$. Ker pa vemo, da morajo biti vse lastne vrednosti $\lambda_1, \ldots, \lambda_k$ ničle minimalnega polinoma, je minimalni polinom deljiv s $p(\lambda)$. Torej je $m_{\mathcal{A}}(\lambda) = p(\lambda)$, ta polinom pa ima očitno same enostavne ničle.

Obratno, predpostavimo, da je ima minimalni polinom $m_{\mathcal{A}}(\lambda)$ endomorfizma $\mathcal{A}$ same enostavne ničle $\lambda_1, \ldots, \lambda_k$. Po prejšnjem izreku je $m_{\mathcal{A}_j}(\lambda) = \lambda - \lambda_j$ minimalni polinom zožitve $\mathcal{A}_j = \mathcal{A}|_{W_j}$ endomorfizma $\mathcal{A}$ na korenski podprostor $W_j$ za vsak $j$. Po definiciji minimalnega polinoma to pomeni, da je $\mathcal{A}_j = \lambda_j \mathrm{id}_{W_j}$ za vsak $j$. Identiteto se seveda da diagonalizirati, ker je $V$ direktna vsota korenskih podprostorov $W_1, \ldots, W_k$, pa sledi, da se tudi $\mathcal{A}$ da diagonalizirati, njegova matrika pa je enaka $\lambda_1 I \oplus \cdots \oplus \lambda_k I$. □

# 3 Jordanova kanonična forma

V prejšnjem poglavju smo videli, da je vsak endomorfizem vektorskega prostora direktna vsota zožitev na korenske podprostore in da ima vsaka zožitev na korenski podprostor eno samo lastno vrednost. Posledično je vsaka kvadratna matrika podobna neki bločno diagonalni matriki, kjer ima vsak diagonalni blok le eno lastno vrednost. Cilj tega poglavja je najti čim enostavnejšo obliko teh diagonalnih blokov.

## 3.1 Endomorfizmi z eno samo lastno vrednostjo

Uvedimo naslednje oznake: $V$ naj bo $n$-razsežen vektorski prostor nad $\mathbb{C}$ in $\mathcal{A} \in \mathcal{L}(V)$ endomorfizem prostora $V$ z eno samo lastno vrednostjo $\rho$. Potem vemo, da je karakteristični polinom endomorfizma enak $\Delta_{\mathcal{A}}(\lambda) = (-1)^n(\lambda - \rho)^n$, minimalni polinom pa je oblike $m_{\mathcal{A}}(\lambda) = (\lambda - \rho)^r$ za nek $r \in \{1, \ldots, n\}$. Po definiciji minimalnega polinoma to pomeni, da je $(\mathcal{A} - \rho\,\mathrm{id}_V)^r = 0$ in $(\mathcal{A} - \rho\,\mathrm{id}_V)^{r-1} \neq 0$ (kjer upoštevamo, da je $(\mathcal{A} - \rho\,\mathrm{id}_V)^0 = \mathrm{id}_V$). Podobno kot smo pri računanju lastnih vektorjev od endomorfizma odšteli večkratnik identitete, tudi tu naredimo enako: definirajmo $\mathcal{N} = \mathcal{A} - \rho\,\mathrm{id}_V$. Potem je $\mathcal{N}^r = 0$ in $\mathcal{N}^{r-1} \neq 0$.

**Definicija 3.1.** Endomorfizem $\mathcal{N}$ prostora $V$, za katerega velja $\mathcal{N}^r = 0$ za nek $r \in \mathbb{N}$, se imenuje *nilpotenten* endomorfizem. Najmanjše število $r \in \mathbb{N}$, za katero je $\mathcal{N}^r = 0$, pa se imenuje *indeks nilpotentnosti* endomorfizma $\mathcal{N}$.

Za endomorfizem $\mathcal{N}$, definiran zgoraj, seveda velja $\Delta_{\mathcal{N}}(\lambda) = (-1)^n\lambda^n$ in $m_{\mathcal{N}}(\lambda) = \lambda^r$. Če matrika $N$ pripada endomorfizmu $\mathcal{N}$ v neki bazi, potem v isti bazi endomorfizmu $\mathcal{A} = \mathcal{N} + \rho\,\mathrm{id}_V$ pripada matrika $N + \rho I$. Dovolj je torej najti čim enostavnejšo matriko, ki pripada nilpotentnemu endomorfizmu, in potem dobimo tudi enostavno matriko za endomorfizem, ki ima poljubno (a samo eno) lastno vrednost.

**Lema 3.2.** *Naj bo $\mathcal{N} \in \mathcal{L}(V)$ kot zgoraj. Za vsak $j \in \mathbb{N}_0$ označimo $V_j = \ker \mathcal{N}^j$. Potem za podprostore $V_j$ prostora $V$ velja:*

1. *$V_j = V$ za $j \geq r$.*
2. *$\{0\} = V_0 \subseteq V_1 \subseteq \cdots \subseteq V_{r-1} \subseteq V_r = V$.*
3. *Za vsak $j \geq 1$ velja $x \in V_j \Leftrightarrow \mathcal{N}x \in V_{j-1}$.*

*Dokaz.*

1. Za $j \geq r$ je $\mathcal{N}^j = \mathcal{N}^{j-r}\mathcal{N}^r = 0$, zato je $V_j = \ker 0 = V$.
2. Ker je $\mathcal{N}^0 = \mathrm{id}_V$, je $V_0 = \ker \mathcal{N}^0 = \{0\}$. Vemo tudi že, da je $V_r = V$. Dokažimo še, da za vsak $j = 0, \ldots, r-1$ velja $V_j \subseteq V_{j+1}$. Naj bo $x \in V_j$ poljuben. Potem je $\mathcal{N}^j x = 0$ po definiciji prostora $V_j$. Potem pa je seveda tudi $\mathcal{N}^{j+1}x = \mathcal{N}(\mathcal{N}^j x) = \mathcal{N}(0) = 0$, torej je $x \in \ker \mathcal{N}^{j+1} = V_{j+1}$. Sledi $V_j \subseteq V_{j+1}$.
3. Očitno velja naslednja veriga ekvivalenc:
$$x \in V_j \Leftrightarrow \mathcal{N}^j x = 0 \Leftrightarrow \mathcal{N}^{j-1}(\mathcal{N}x) = 0 \Leftrightarrow \mathcal{N}x \in \ker \mathcal{N}^{j-1} = V_{j-1}.$$

□

**Lema 3.3.** *Naj bo $j \geq 2$ in naj bo $\mathcal{B} = \{v_1, \dots, v_k\} \subseteq V_j$ linearno neodvisna množica, za katero velja $\operatorname{Lin} \mathcal{B} \cap V_{j-1} = \{0\}$. Potem je množica $\mathcal{N}(\mathcal{B}) = \{\mathcal{N}v_1, \dots, \mathcal{N}v_k\}$ linearno neodvisna in velja $\mathcal{N}(\mathcal{B}) \subseteq V_{j-1}$ in $\operatorname{Lin}(\mathcal{N}(\mathcal{B})) \cap V_{j-2} = \{0\}$.*

*Dokaz.* Da je $\mathcal{N}(\mathcal{B}) \subseteq V_{j-1}$, sledi neposredno iz tretje točke prejšnje leme.

Dokažimo linearno neodvisnost množice $\mathcal{N}(\mathcal{B})$. Če je $\alpha_1 \mathcal{N}v_1 + \cdots + \alpha_k \mathcal{N}v_k = 0$, potem je

$$\mathcal{N}(\alpha_1 v_1 + \cdots + \alpha_k v_k) = 0 \in \ker \mathcal{N}^{j-2} = V_{j-2},$$

saj je $j \geq 2$. Po tretji točki prejšnje leme potem sledi $\alpha_1 v_1 + \cdots + \alpha_k v_k \in V_{j-1}$. Ker je $\alpha_1 v_1 + \cdots + \alpha_k v_k \in \operatorname{Lin} \mathcal{B}$ in je $\operatorname{Lin} \mathcal{B} \cap V_{j-1} = \{0\}$, od tod sledi $\alpha_1 v_1 + \cdots + \alpha_k v_k = 0$. Iz linearne neodvisnosti množice $\mathcal{B}$ zdaj sledi $\alpha_1 = \cdots = \alpha_k = 0$. Množica $\mathcal{N}(\mathcal{B})$ je torej linearno neodvisna.

Dokažimo še, da je $\operatorname{Lin}(\mathcal{N}(\mathcal{B})) \cap V_{j-2} = \{0\}$. Pa naj bo $x$ vektor v tem preseku. Potem je $x \in V_{j-2}$ in $x = \beta_1 \mathcal{N}v_1 + \cdots + \beta_k \mathcal{N}v_k$ za neke $\beta_1, \dots, \beta_k \in \mathbb{C}$. Torej je $\mathcal{N}(\beta_1 v_1 + \cdots + \beta_k v_k) \in V_{j-2}$. Spet uporabimo tretjo točko prejšnje trditve in dobimo $\beta_1 v_1 + \cdots + \beta_k v_k \in V_{j-1}$. Kot v prejšnjem odstavku iz enakosti $\operatorname{Lin} \mathcal{B} \cap V_{j-1} = \{0\}$ spet sledi $\beta_1 v_1 + \cdots + \beta_k v_k = 0$, in linearna neodvisnost množice $\mathcal{B}$ nam da $\beta_1 = \cdots = \beta_k = 0$. Torej je $x = 0$. □

**Posledica 3.4.** $\{0\} = V_0 \subsetneq V_1 \subsetneq \cdots \subsetneq V_{r-1} \subsetneq V_r = V$.

*Dokaz.* Dokazati moramo le, da je $V_j \neq V_{j-1}$ za $j = 1, \dots, r$. To bomo dokazali z obratno indukcijo. Natančneje, dokazali bomo, da za vsak $j = 1, \dots, r$ obstaja linearno neodvisna množica $\mathcal{B}_j \subseteq V_j$, da je $\operatorname{Lin} \mathcal{B}_j \cap V_{j-1} = \{0\}$. Od tod bo očitno sledilo $V_{j-1} \subsetneq V_j$.

Ker je $r$ indeks nilpotentnosti endomorfizma $\mathcal{N}$, je $\mathcal{N}^{r-1} \neq 0$. To pa pomeni, da je $V_{r-1} = \ker \mathcal{N}^{r-1} \neq V = V_r$. Neko bazo $\mathcal{B}'$ prostora $V_{r-1}$ z neko množico $\mathcal{B}_r$ dopolnimo do baze prostora $V_r$. Množica $\mathcal{B}_r$ je linearno neodvisna, velja pa tudi $\operatorname{Lin} \mathcal{B}_r \cap V_{r-1} = \{0\}$, saj v nasprotnem primeru množica $\mathcal{B}' \cup \mathcal{B}_r$ ne bi bila linearno neodvisna. Bazo indukcije smo tako dokazali.

Predpostavimo zdaj, da je $j \geq 1$ in da obstaja linearno neodvisna množica $\mathcal{B}_{j+1} \subseteq V_{j+1}$, da je $\operatorname{Lin} \mathcal{B}_{j+1} \cap V_j = \{0\}$. Po prejšnji lemi je potem množica $\mathcal{B}_j := \mathcal{N}(\mathcal{B}_{j+1}) \subseteq V_j$ linearno neodvisna in velja $\operatorname{Lin} \mathcal{B}_j \cap V_{j-1} = \{0\}$. S tem je dokazan še indukcijski korak. Posledica torej velja. □

## 3.2 Konstrukcija Jordanove baze

Za dani endomorfizem prostora $V$ bomo konstruirali bazo prostora $V$, glede na katero bo matrika danega endomorfizma zelo enostavna. Baza se bo imenovala Jordanova baza danega endomorfizma, matrika endomorfizma, zapisana v Jordanovi bazi, pa Jordanova matrika endomorfizma.

Najprej si oglejmo primer, ko imamo nilpotenten endomorfizem $\mathcal{N} \in \mathcal{L}(V)$. Naj bo $r$ indeks nilpotentnosti endomorfizma $\mathcal{N}$. Privzemimo tudi vse ostale oznake iz rezdelka 3.1. Po Posledici 3.4 je $V_{r-1} \neq V_r = V$. Zato obstaja komplement $U_r$ podprostora $V_{r-1}$ v $V$, torej tak podprostor, da je $V_r = U_r \oplus V_{r-1}$. Naj bo $\mathcal{B}_r = \{v_1^{(r)}, \dots, v_{s_r}^{(r)}\}$ baza podprostora $U_r \subseteq V_r$. Za $j = 1, \dots, s_r$ označimo $v_j^{(r-1)} = \mathcal{N}v_j^{(r)}$. Množica $\mathcal{B}_r$ je seveda linearno neodvisna, po definiciji direktne vsote pa je tudi $\operatorname{Lin} \mathcal{B}_r \cap V_{r-1} = U_r \cap V_{r-1} = \{0\}$. Če je $r \geq 2$, je po Lemi 3.3 potem tudi množica $\mathcal{N}(\mathcal{B}_r) = \{v_1^{(r-1)}, \dots, v_{s_r}^{(r-1)}\} \subseteq V_{r-1}$ linearno neodvisna in velja $\operatorname{Lin}(\mathcal{N}(\mathcal{B}_r)) \cap V_{r-2} = \{0\}$. To pomeni, da je množica $\mathcal{N}(\mathcal{B}_r)$ vsebovana v nekem komplementu podprostora $V_{r-2}$ v $V_{r-1}$, t.j. takem podorostoru $U_{r-1}$ prostora $V_{r-1}$, da je $V_{r-1} = U_{r-1} \oplus V_{r-2}$. Množica $\mathcal{N}(\mathcal{B}_r)$ je linearno neodvisna, zato jo lahko dopolnimo do baze $\mathcal{B}_{r-1} = \{v_1^{(r-1)}, \dots, v_{s_r}^{(r-1)}, \dots, v_{s_{r-1}}^{(r-1)}\}$ prostora $U_{r-1}$. $\mathcal{B}_{r-1}$ je linearno neodvisna podmnožica $V_{r-1}$, za katero po definiciji direktne vsote velja $\operatorname{Lin} \mathcal{B}_{r-1} \cap V_{r-2}$, zato v primeru $r \geq 3$ Lemo 3.3 lahko uporabimo za $\mathcal{B}_{r-1}$. Postopek ponavljamo. Za vsak $j = 1, \dots, r$ tako dobimo podprostor $U_j$ prostora $V_j$, da je $V_j = U_j \oplus V_{j-1}$, in tako bazo $\mathcal{B}_j = \{v_1^{(j)}, \dots, v_{s_j}^{(j)}\}$ podprostora $U_j$, da v primeru $j < r$ za vsak $i = 1, \dots, s_{j+1}$ velja $v_i^{(j)} = \mathcal{N}v_i^{(j+1)}$. Po konstrukciji je

$$V = V_r = U_r \oplus V_{r-1} = U_r \oplus U_{r-1} \oplus V_{r-2} = \cdots = U_r \oplus U_{r-1} \oplus \cdots \oplus U_1 \oplus V_0 = U_r \oplus U_{r-1} \oplus \cdots \oplus U_1.$$

Za vsak $j = 1, \ldots, r$ je $\mathcal{B}_j$ baza prostora $U_j$, zato iz enakosti $V = U_r \oplus \cdots \oplus U_1$ sledi, da je $\mathcal{B} = \mathcal{B}_r \cup \cdots \cup \mathcal{B}_1$ baza prostora $V$ in da je $\mathcal{B}_i \cap \mathcal{B}_j = \varnothing$ za $i \neq j$. Bazo $\mathcal{B}$ uredimo na naslednji način: $\mathcal{B} = \{v_1^{(1)}, v_1^{(2)}, \ldots, v_1^{(r)}, v_2^{(1)}, \ldots\}$. Tako urejeno bazo $\mathcal{B}$ prostora $V$ imenujemo *Jordanova baza* za nilpotent $\mathcal{N}$. Matriko, ki pripada endomorfizmu $\mathcal{N}$ v Jordanovi bazi, imenujemo *Jordanova matrika* endomorfizma $\mathcal{N}$ in jo označimo z $\mathcal{J}(\mathcal{N})$.

Izračunajmo $\mathcal{J}(\mathcal{N})$. Vemo že, da je $\mathcal{N} v_i^{(j)} = v_i^{(j-1)}$ za vsaka $j = 2, \ldots, r$ in $i = 1, \ldots, s_j$. Poleg tega je $V_1 = \ker \mathcal{N}$, zato je $\mathcal{N} v_i^{(1)} = 0$ za vsak $i = 1, \ldots, s_1$. Če po vrsti izračunamo vrednosti endomorfizma $\mathcal{N}$ v baznih vektorjih, tako velja:

$$\begin{array}{rcl} \mathcal{N} v_1^{(1)} & = & 0 \\ \mathcal{N} v_1^{(2)} & = & v_1^{(1)} \\ & \vdots & \\ \mathcal{N} v_1^{(r)} & = & v_1^{(r-1)} \\ \mathcal{N} v_2^{(1)} & = & 0 \\ \mathcal{N} v_2^{(2)} & = & v_2^{(1)} \\ & \vdots & \end{array}$$

Torej je

$$\mathcal{J}(\mathcal{N}) = \left[\begin{array}{c|c|c|c} \begin{matrix}0&1&&&\\&0&1&&\\&&0&\ddots&\\&&&\ddots&1\\&&&&0\end{matrix} & & & \\ \hline & \begin{matrix}0&1&&\\&0&\ddots&\\&&\ddots&1\\&&&0\end{matrix} & & \\ \hline & & \ddots & \\ \hline & & & \begin{matrix}0&1&&\\&0&\ddots&\\&&\ddots&1\\&&&0\end{matrix} \end{array}\right].$$

Vidimo, da je matrika $\mathcal{J}(\mathcal{N})$ bločno diagonalna in da ima same ničle, razen nad diagonalo ima nekaj enic. Matriki $J_t = \begin{bmatrix} 0 & 1 & & \\ & 0 & \ddots & \\ & & \ddots & 1 \\ & & & 0 \end{bmatrix} \in \mathbb{C}^{t \times t}$ pravimo *Jordanova celica* velikost $t \times t$ za lastno vrednost 0, pri čemer pri $t = 1$ definiramo $J_1 = 0$. Matrika $\mathcal{J}(\mathcal{N})$ je torej direktna vsota Jordanovih celic. Pri tem velikosti celic po diagonali ne naraščajo, velikost največje Jordanove celice pa je enaka indeksu nilpotentnosti endomorfizma $\mathcal{N}$. Število celic je enako $\dim \ker \mathcal{N}$, torej geometrični večkratnosti lastne vrednosti 0 endomorfizma $\mathcal{N}$.

**Primer 3.5.** Poiščimo Jordanovo bazo in Jordanovo matriko matrike

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

Jordanova baza in Jordanova matrika dane matrike $A$ sta po definiciji enaka Jordanovi bazi in Jordanovi matriki endomorfizma $A\colon \mathbb{C}^5 \to \mathbb{C}^5$ (oziroma v splošnem $A\colon \mathbb{C}^n \to \mathbb{C}^n$), definiranega s predpisom $x \mapsto Ax$.

Najprej poiščimo lastne vrednosti matrike (oziroma endomorfizma) $A$. V ta namen najprej izračunajmo karakteristični polinom

$$\begin{aligned}
\Delta_A(\lambda) &= \begin{vmatrix} -1-\lambda & 1 & -1 & -1 & -1 \\ 1 & -\lambda & 0 & 1 & 1 \\ 0 & 0 & -\lambda & 0 & 0 \\ 1 & 0 & 1 & 1-\lambda & 1 \\ 0 & -1 & 0 & 0 & -\lambda \end{vmatrix} = -\lambda \begin{vmatrix} -1-\lambda & 1 & -1 & -1 \\ 1 & -\lambda & 1 & 1 \\ 1 & 0 & 1-\lambda & 1 \\ 0 & -1 & 0 & -\lambda \end{vmatrix} \\
&= \lambda \begin{vmatrix} -1-\lambda & -1 & -1 \\ 1 & 1 & 1 \\ 1 & 1-\lambda & 1 \end{vmatrix} + \lambda^2 \begin{vmatrix} -1-\lambda & 1 & -1 \\ 1 & -\lambda & 1 \\ 1 & 0 & 1-\lambda \end{vmatrix} \\
&= \lambda \begin{vmatrix} -\lambda & 0 & 0 \\ 1 & 1 & 1 \\ 0 & -\lambda & 0 \end{vmatrix} + \lambda^2\left((1+\lambda)\lambda(1-\lambda) + 1 - (1-\lambda) - \lambda\right) = -\lambda^3 + \lambda^3(1-\lambda^2) = -\lambda^5.
\end{aligned}$$

Edina lastna vrednost matrike $A$ je torej 0 (z algebraično večkratnostjo 5), zato je minimalni polinom oblike $m_A(\lambda) = \lambda^r$ za nek $r$. Matrika $A$ je torej nilpotentna. Poiščimo indeks nilpotentnosti $r$. To storimo tako, da izračunamo potence matrike $A$:

$$A^2 = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ -1 & 0 & 0 & -1 & -1 \end{bmatrix}, A^3 = 0.$$

Sledi, da je $r = 3$. Od tod že vemo, da bo največja Jordanova celica v matriki $\mathcal{J}(A)$ velikosti $3 \times 3$. Da poiščemo Jordanovo bazo, moramo najprej poiskati $\dim\ker A^3 - \dim\ker A^2 = 5 - \dim\ker A^2$ linearno neodvisnih vektorjev v $\ker A^3 \setminus \ker A^2$. Očitno je

$$\ker A^2 = \left\{ \begin{bmatrix} -w-v \\ y \\ z \\ w \\ v \end{bmatrix} ; y, z, w, v \in \mathbb{C} \right\},$$

torej je $\dim A^2 = 4$ in $\dim A^3 - \dim A^2 = 1$. To pomeni, da bo imela matrika $\mathcal{J}(A)$ eno Jordanovo celico velikosti $3 \times 3$. Vektor v $\ker A^3 \setminus \ker A^2$ v skladu z oznakami iz definicije Jordanove baze označimo z $v_1^{(3)}$. Za ta vektor lahko vzamemo poljuben vektor v $\ker A^3 \setminus \ker A^2$, definirajmo na primer $v_1^{(3)} = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}$. Vektorju $v_1^{(3)}$ pravimo *korenski vektor*.

Drugi korak je, da poiščemo $\dim\ker A^2 - \dim\ker A = 4 - \dim\ker A$ vektorjev v $\ker A^2 \setminus \ker A$. Eden od teh vektorjev je $v_1^{(2)} = Av_1^{(3)} = \begin{bmatrix} -1 \\ 1 \\ 0 \\ 1 \\ 0 \end{bmatrix}$. Za ostale vektorje je treba najprej poiskati jedro matrike $A$. Z Gaussovo eliminacijo dobimo

$$A \sim \begin{bmatrix} -1 & 1 & -1 & -1 & -1 \\ 0 & 1 & -1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix},$$

torej je $\ker A = \left\{ \begin{bmatrix} -w-v \\ 0 \\ 0 \\ w \\ v \end{bmatrix} ; v, w \in \mathbb{C} \right\}$ in $\dim\ker A = 2$. To med drugim pomeni, da ima $\mathcal{J}(A)$ dve Jordanovi celici. Ker je največja celica velikosti $3 \times 3$, ni druge možnosti kot, da je

$$\mathcal{J}(A) = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

Za določitev Jordanove baze potrebujemo še en korenski vektor $v_2^{(2)}$, t.j. tak vektor v $\ker A^2 \setminus \ker A$, da nobena netrivialna linearna kombinacija $v_1^{(2)}$ in $v_2^{(2)}$ ne bo v jedru matrike $A$. Vzamemo lahko $v_2^{(2)} = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 0 \end{bmatrix}$. Preostala vektorja v Jordanovi bazi pa sta $v_1^{(1)} = Av_1^{(2)} = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \\ -1 \end{bmatrix}$ in $v_2^{(1)} = Av_2^{(2)} = \begin{bmatrix} -1 \\ 0 \\ 0 \\ 1 \\ 0 \end{bmatrix}$. Ker je $\mathcal{B} = \{v_1^{(1)}, v_1^{(2)}, v_1^{(3)}, v_2^{(1)}, v_2^{(2)}\}$ Jordanova baza, je

$$P = [v_1^{(1)}, v_1^{(2)}, v_1^{(3)}, v_2^{(1)}, v_2^{(2)}] = \mathrm{id}_S^{\mathcal{B}} = \begin{bmatrix} 1 & -1 & 1 & -1 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ -1 & 0 & 0 & 0 & 0 \end{bmatrix}$$

prehodna matrika med standardno bazo in bazo $\mathcal{B}$. Zato velja

$$\mathcal{J}(A) = A_{\mathcal{B}}^{\mathcal{B}} = \mathrm{id}_{\mathcal{B}}^S A_S^S \mathrm{id}_S^{\mathcal{B}} = P^{-1}AP.$$

Vsak naj to sam preveri z računom.

Obravnavajmo zdaj primer, ko je $\mathcal{A} \in \mathcal{L}(V)$ poljuben endomorfizem z eno samo lastno vrednostjo $\rho$. *Jordanova baza* za $\mathcal{A}$ je ista kot Jordanova baza za nilpotenten endomorfizem

$\mathcal{N} = \mathcal{A} - \rho\,\mathrm{id}_V$. Od tod sledi, da je $\mathcal{J}(\mathcal{A}) = \mathcal{J}(\mathcal{N}) + \rho I$ in je torej $\mathcal{J}(\mathcal{A})$ direktna vsota *Jordanovih celic* $J_t(\rho) = \begin{bmatrix} \rho & 1 & & \\ & \rho & \ddots & \\ & & \ddots & 1 \\ & & & \rho \end{bmatrix} \in \mathbb{C}^{t\times t}$ *za lastno vrednost* $\rho$. Število teh celic je enako geometrični večkratnosti lastne vrednosti $\rho$, velikost največje celice pa stopnji minimalnega polinoma $m_{\mathcal{A}}(\lambda)$.

Oglejmo si zdaj splošni primer. Naj bo $\mathcal{A} \in \mathcal{L}(V)$ poljuben endomorfizem prostora $V$ in $\{\lambda_1, \ldots, \lambda_k\}$ spekter endomorfizma $\mathcal{A}$. Za vsak $j = 1, \ldots, k$ naj bo $W_j$ korenski podprostor za $\mathcal{A}$, ki pripada lastni vrednosti $\lambda_j$. *Jordanova baza* endomorfizma $\mathcal{A}$ je zdaj definirana kot urejena unija Jordanovih baz zožitev $\mathcal{A}|_{W_j}$. Jordanova matrika endomorfizma $\mathcal{A}$, ki je definirana kot matrika endomorfizma $\mathcal{A}$ glede na Jordanovo bazo, je torej enaka $\mathcal{J}(\mathcal{A}) = \mathcal{J}(\mathcal{A}|_{W_1}) \oplus \cdots \oplus \mathcal{J}(\mathcal{A}|_{W_k})$. To pomeni, da je matrika $\mathcal{J}(\mathcal{A})$ enaka direktni vsoti Jordanovih celic oblike $J_t(\lambda_i)$. Pri tem velja:

- Lastna vrednost $\lambda_j$ se na diagonali matrike $\mathcal{J}(\mathcal{A})$ pojavi tolikokrat, kolikor je njena algebraična večkratnost.
- Za vsak $j$ je število celic oblike $J_t(\lambda_j)$ enako geometrični večkratnosti lastne vrednosti $\lambda_j$.
- Pri fiksnem $j$ je največja celica oblike $J_t(\lambda_j)$ velikosti $m_j \times m_j$, kjer je $m_j$ red ničle $\lambda_j$ v minimalnem polinomu $m_{\mathcal{A}}(\lambda)$.

Za vsak endomorfizem obstajata torej Jordanova baza in Jordanova matrika za ta endomorfizem. V posebnem primeru je vsaka matrika podobna neki Jordanovi matriki. Jordanova baza endomorfizma ni enolična, je pa enolična njegova Jordanova matrika. Hitro se da namreč videti, da je za vsako lastno vrednost $\lambda_j$ endomorfizma $\mathcal{A}$ število Jordanovih celic v matriki $\mathcal{J}(\mathcal{A})$, ki so velikosti vsaj $t \times t$ in pripadajo lastni vrednosti $\lambda_j$, enako

$$\dim\left(\ker(\mathcal{A} - \lambda_j\,\mathrm{id}_V)^t\right) - \dim\left(\ker(\mathcal{A} - \lambda_j\,\mathrm{id}_V)^{t-1}\right).$$

To število pa je z endomorfizmom $\mathcal{A}$ enolično določeno. Ker vsakemu endomorfizmu (oz. matriki) pripada natanko ena Jordanova matrika, Jordanovi matriki pravimo tudi *Jordanova kanonična forma* endomorfizma (oz. matrike).

Poglejmo si, kako poiščemo Jordanovo matriko in Jordanovo bazo endomorfizma z več lastnimi vrednostmi.

**Primer 3.6.** Poiščimo Jordanovo bazo in Jordanovo kanonično formo matrike

$$A = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & -1 & 0 & 0 \\ -1 & 0 & 0 & -1 & -3 & -3 \\ 1 & 0 & 1 & 1 & 2 & 1 \\ 1 & 0 & 0 & 0 & 2 & 2 \\ -1 & 0 & 0 & 0 & -1 & -1 \end{bmatrix}.$$

Kot v prejšnjem primeru najprej izračunamo karakteristični polinom

$$\begin{aligned}
\Delta_A(\lambda) &= \begin{vmatrix} -\lambda & 0 & 0 & 1 & 1 & 1 \\ 1 & -\lambda & 0 & -1 & 0 & 0 \\ -1 & 0 & -\lambda & -1 & -3 & -3 \\ 1 & 0 & 1 & 1-\lambda & 2 & 1 \\ 1 & 0 & 0 & 0 & 2-\lambda & 2 \\ -1 & 0 & 0 & 0 & -1 & -1-\lambda \end{vmatrix} = -\lambda \begin{vmatrix} -\lambda & 0 & 1 & 1 & 1 \\ -1 & -\lambda & -1 & -3 & -3 \\ 1 & 1 & 1-\lambda & 2 & 1 \\ 1 & 0 & 0 & 2-\lambda & 2 \\ -1 & 0 & 0 & -1 & -1-\lambda \end{vmatrix} \\
&= -\lambda \begin{vmatrix} 0 & 0 & 1 & 1+\lambda & 1+\lambda+\lambda^2 \\ 0 & -\lambda & -1 & -2 & -2+\lambda \\ 0 & 1 & 1-\lambda & 1 & -\lambda \\ 0 & 0 & 0 & 1-\lambda & 1-\lambda \\ -1 & 0 & 0 & -1 & -1-\lambda \end{vmatrix} = \lambda \begin{vmatrix} 0 & 1 & 1+\lambda & 1+\lambda+\lambda^2 \\ -\lambda & -1 & -2 & -2+\lambda \\ 1 & 1-\lambda & 1 & -\lambda \\ 0 & 0 & 1-\lambda & 1-\lambda \end{vmatrix} \\
&= \lambda(1-\lambda) \begin{vmatrix} 0 & 1 & 1+\lambda & 1+\lambda+\lambda^2 \\ -\lambda & -1 & -2 & -2+\lambda \\ 1 & 1-\lambda & 1 & -\lambda \\ 0 & 0 & 1 & 1 \end{vmatrix} = \lambda(1-\lambda) \begin{vmatrix} 0 & 1 & 0 & \lambda^2 \\ -\lambda & -1 & 0 & \lambda \\ 1 & 1-\lambda & 0 & -1-\lambda \\ 0 & 0 & 1 & 1 \end{vmatrix} \\
&= -\lambda(1-\lambda) \begin{vmatrix} 0 & 1 & \lambda^2 \\ -\lambda & -1 & \lambda \\ 1 & 1-\lambda & -1-\lambda \end{vmatrix} = -\lambda(1-\lambda) \begin{vmatrix} 0 & 1 & \lambda^2 \\ 0 & -1+\lambda-\lambda^2 & -\lambda^2 \\ 1 & 1-\lambda & -1-\lambda \end{vmatrix} \\
&= -\lambda(1-\lambda) \begin{vmatrix} 1 & \lambda^2 \\ -1+\lambda-\lambda^2 & -\lambda^2 \end{vmatrix} = -\lambda^3(1-\lambda) \begin{vmatrix} 1 & 1 \\ -1+\lambda-\lambda^2 & -1 \end{vmatrix} \\
&= -\lambda^3(1-\lambda)(-1+1-\lambda+\lambda^2) = \lambda^4(1-\lambda)^2.
\end{aligned}$$

Lastni vrednosti matrike $A$ sta torej 0 z algebraično večkratnostjo 4 in 1 z algebraično večkratnostjo 2.

Najprej poiščimo Jordanovo bazo zožitve endomorfizma $A$ na korenski podprostor za lastno vrednost 0. Za to potrebujemo red ničle 0 v minimalnem polinomu. Če je $k$ strogo manjši od reda ničle 0 v minimalnem polinomu, potem ima $k$-ta potenca zožitve endomorfizma $A$ na korenski podprostor za lastno vrednost 0 strogo večji rang kot $(k+1)$-ta potenca te zožitve. Če je $k$ večji ali enak redu ničle 0 v minimalnem polinomu, pa sta tako $k$-ta kot $(k+1)$-ta potenca zožitve enakega ranga, saj sta obe enaki 0. Ker je zožitev endomorfizma $A$ na korenski podprostor za lastno vrednost 1 obrnljiva, $\mathbb{C}^6$ pa je direktna vsota obeh korenskih podprostorov, velja tudi, da ima $k$-ta potenca matrike $A$ strogo večji rang kot $(k+1)$-ta potenca, kadar je $k$ manjši od reda ničle 0 v minimalnem polinomu, in enak rang kot $(k+1)$-ta potenca, kadar je $k$ večji ali enak redu ničle 0 v minimalnem polinomu. Da dobimo red ničle 0 v minimalnem polinomu, moramo torej ugotoviti, kdaj se rang potenc matrike $A$ stabilizira. Izračunajmo:

$$\begin{aligned}
A &= \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & -1 & 0 & 0 \\ -1 & 0 & 0 & -1 & -3 & -3 \\ 1 & 0 & 1 & 1 & 2 & 1 \\ 1 & 0 & 0 & 0 & 2 & 2 \\ -1 & 0 & 0 & 0 & -1 & -1 \end{bmatrix} \sim \begin{bmatrix} 1 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & -2 & -3 & -3 \\ 0 & 0 & 1 & 2 & 2 & 1 \\ 0 & 0 & 0 & 1 & 2 & 2 \\ 0 & 0 & 0 & -1 & -1 & -1 \end{bmatrix} \\
&\sim \begin{bmatrix} 1 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 2 & 2 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & -1 & -1 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \sim \begin{bmatrix} 1 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 2 & 2 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \Rightarrow \operatorname{rang} A = 4,
\end{aligned}$$

$$
\begin{aligned}
A^2 &= \begin{bmatrix} 1 & 0 & 1 & 1 & 3 & 2 \\ -1 & 0 & -1 & 0 & -1 & 0 \\ -1 & 0 & -1 & -2 & -6 & -5 \\ 1 & 0 & 1 & 1 & 3 & 2 \\ 0 & 0 & 0 & 1 & 3 & 3 \\ 0 & 0 & 0 & -1 & -2 & -2 \end{bmatrix} \sim \begin{bmatrix} 1 & 0 & 1 & 1 & 3 & 2 \\ 0 & 0 & 0 & 1 & 2 & 2 \\ 0 & 0 & 0 & -1 & -3 & -3 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 3 & 3 \\ 0 & 0 & 0 & -1 & -2 & -2 \end{bmatrix} \\
&\sim \begin{bmatrix} 1 & 0 & 1 & 1 & 3 & 2 \\ 0 & 0 & 0 & 1 & 2 & 2 \\ 0 & 0 & 0 & 0 & -1 & -1 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \Rightarrow \operatorname{rang} A^2 = 3,
\end{aligned}
$$

$$
\begin{aligned}
A^3 &= \begin{bmatrix} 1 & 0 & 1 & 1 & 4 & 3 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ -2 & 0 & -2 & -2 & -9 & -7 \\ 1 & 0 & 1 & 1 & 4 & 3 \\ 1 & 0 & 1 & 1 & 5 & 4 \\ -1 & 0 & -1 & -1 & -4 & -3 \end{bmatrix} \sim \begin{bmatrix} 1 & 0 & 1 & 1 & 4 & 3 \\ 0 & 0 & 0 & 0 & -1 & -1 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \\
&\sim \begin{bmatrix} 1 & 0 & 1 & 1 & 4 & 3 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \Rightarrow \operatorname{rang} A^3 = 2,
\end{aligned}
$$

$$
\begin{aligned}
A^4 &= \begin{bmatrix} 1 & 0 & 1 & 1 & 5 & 4 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ -2 & 0 & -2 & -2 & -11 & -9 \\ 1 & 0 & 1 & 1 & 5 & 4 \\ 1 & 0 & 1 & 1 & 6 & 5 \\ -1 & 0 & -1 & -1 & -5 & -4 \end{bmatrix} \sim \begin{bmatrix} 1 & 0 & 1 & 1 & 5 & 4 \\ 0 & 0 & 0 & 0 & -1 & -1 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \\
&\sim \begin{bmatrix} 1 & 0 & 1 & 1 & 5 & 4 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \Rightarrow \operatorname{rang} A^4 = 2.
\end{aligned}
$$

To pomeni, da je red ničle 0 v minimalnem polinomu matrike $A$ enak 3, matrika $\mathcal{J}(A)$ pa ima eno Jordanovo celico velikosti $3 \times 3$ in eno velikosti $1 \times 1$.

Vektorje Jordanove baze izračunamo na enak način kot v prejšnjem primeru. Najprej poiščemo poljuben korenski vektor $v_1^{(3)} \in \ker A^3 \setminus \ker A^2$. Vzemimo npr. $v_1^{(3)} = \begin{bmatrix} -1 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \end{bmatrix}$. Potem pa izračunamo $v_1^{(2)} = Av_1^{(3)} = \begin{bmatrix} 1 \\ -2 \\ 0 \\ 0 \\ -1 \\ 1 \end{bmatrix}$ in $v_1^{(1)} = Av_1^{(2)} = A^2 v_1^{(3)} = \begin{bmatrix} 0 \\ 1 \\ -1 \\ 0 \\ 1 \\ -1 \end{bmatrix}$. Vektor $v_1^{(1)}$ z $v_2^{(1)}$ dopolnimo do baze jedra matrike $A$. Vzamemo lahko $v_2^{(1)} = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}$.

Enak postopek zdaj naredimo za lastno vrednost 1. Najprej ugotovimo, kdaj se rangi potenc matrike $A - I$ stabilizirajo. Izračunajmo:

$$
\begin{aligned}
A - I &= \begin{bmatrix} -1 & 0 & 0 & 1 & 1 & 1 \\ 1 & -1 & 0 & -1 & 0 & 0 \\ -1 & 0 & -1 & -1 & -3 & -3 \\ 1 & 0 & 1 & 0 & 2 & 1 \\ 1 & 0 & 0 & 0 & 1 & 2 \\ -1 & 0 & 0 & 0 & -1 & -2 \end{bmatrix} \sim \begin{bmatrix} -1 & 0 & 0 & 1 & 1 & 1 \\ 0 & -1 & 0 & 0 & 1 & 1 \\ 0 & 0 & -1 & -2 & -4 & -4 \\ 0 & 0 & 1 & 1 & 3 & 2 \\ 0 & 0 & 0 & 1 & 2 & 3 \\ 0 & 0 & 0 & -1 & -2 & -3 \end{bmatrix} \\
&\sim \begin{bmatrix} -1 & 0 & 0 & 1 & 1 & 1 \\ 0 & -1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 2 & 4 & 4 \\ 0 & 0 & 0 & -1 & -1 & -2 \\ 0 & 0 & 0 & 1 & 2 & 3 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \sim \begin{bmatrix} -1 & 0 & 0 & 1 & 1 & 1 \\ 0 & -1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 2 & 4 & 4 \\ 0 & 0 & 0 & 1 & 1 & 2 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \Rightarrow \operatorname{rang}(A - I) = 5.
\end{aligned}
$$

Od tod že lahko izračunamo Jordanovo kanonično formo matrike $A$. Ker je korenski podprostor za lastno vrednost 0 4-razsežen, je korenski podprostor za lastno vrednost 1 2-razsežen. Ker pa je $\dim \ker(A - I) = 1$, sledi, da ima $\mathcal{J}(A)$ eno Jordanovo celico za lastno vrednost 1. Velikost te celice mora biti seveda $2 \times 2$. Torej je

$$
\mathcal{J}(A) = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}.
$$

Za Jordanovo bazo pa potrebujemo še vektor iz jedra matrike $(A - I)^2$, zato izračunamo:

$$
\begin{aligned}
(A - I)^2 &= \begin{bmatrix} 2 & 0 & 1 & -1 & 1 & 0 \\ -1 & 1 & -1 & 2 & -1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 \\ -1 & 0 & -1 & 0 & -1 & 0 \\ -2 & 0 & 0 & 1 & 0 & -1 \\ 2 & 0 & 0 & -1 & 0 & 1 \end{bmatrix} \sim \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & -1 & 2 & -1 & 1 \\ 0 & 0 & 1 & -1 & 1 & -2 \\ 0 & 0 & -1 & 0 & -1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & -1 & 0 & -1 \end{bmatrix} \\
&\sim \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & -1 & 2 & -1 & 1 \\ 0 & 0 & 1 & -1 & 1 & -2 \\ 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}.
\end{aligned}
$$

Od tod sledi $\ker(A-I)^2 = \left\{ \begin{bmatrix} -u \\ 2u \\ u-v \\ -u \\ v \\ u \end{bmatrix} ; v, u \in \mathbb{C} \right\}$. Za korenski vektor $v_3^{(2)}$ lahko vzamemo poljuben vektor iz $\ker(A-I)^2 \setminus \ker(A-I)$. Vzemimo npr. $v_3^{(2)} = \begin{bmatrix} 0 \\ 0 \\ -1 \\ 0 \\ 1 \\ 0 \end{bmatrix}$. Potem je $v_3^{(1)} = (A - I)v_3^{(2)} = \begin{bmatrix} 1 \\ 0 \\ -2 \\ 1 \\ 1 \\ -1 \end{bmatrix}$. Urejena Jordanova baza za matriko $A$ je torej $\{v_1^{(1)}, v_1^{(2)}, v_1^{(3)}, v_2^{(1)}, v_3^{(1)}, v_3^{(2)}\}$.

### 3.3 Funkcije matrik

Definirali bomo, kako izračunamo funkcije matrik. Polinome v matriki že znamo izračunati, zato si najprej oglejmo izračun teh. Naj bo $A \in \mathbb{C}^{n \times n}$ poljubna matrika in $p(\lambda) \in \mathbb{C}[\lambda]$ polinom. Vemo, da je $A = P\mathcal{J}(A)P^{-1}$, kjer je $\mathcal{J}(A)$ Jordanova matrika matrike $A$, $P$ pa prehodna matrika, katere stolpci so elementi Jordanove baze. Prav tako že vemo, da je $p(A) = Pp(\mathcal{J}(A))P^{-1}$. Ker je $\mathcal{J}(A)$ direktna vsota Jordanovih celic $J_t(\lambda_i)$, je po definiciji seštevanja in množenja matrik tudi $p(\mathcal{J}(A))$ direktna vsota matrik $p(J_t(\lambda_i))$. Izračunajmo torej $p(J_t(\rho))$, kjer je $\rho \in \mathbb{C}$ poljuben. Jordanovo celico $J_t(\rho)$ lahko pišemo v obliki $J_t(\rho) = \rho I + N$, kjer je $N = \begin{bmatrix} 0 & 1 & & \\ & 0 & \ddots & \\ & & \ddots & 1 \\ & & & 0 \end{bmatrix} \in \mathbb{C}^{t \times t}$ nilpotent ($t \times t$ Jordanova celica za lastno vrednost 0). Potem je

$$N^2 = \begin{bmatrix} 0 & 0 & 1 & & \\ & 0 & 0 & \ddots & \\ & & \ddots & \ddots & 1 \\ & & & 0 & 0 \\ & & & & 0 \end{bmatrix}, N^3 = \begin{bmatrix} 0 & 0 & 0 & 1 & & \\ & 0 & 0 & 0 & \ddots & \\ & & \ddots & \ddots & \ddots & 1 \\ & & & 0 & 0 & 0 \\ & & & & 0 & 0 \\ & & & & & 0 \end{bmatrix}, \ldots, N^{t-1} = \begin{bmatrix} 0 & \cdots & 0 & 1 \\ & \ddots & & 0 \\ & & \ddots & \vdots \\ & & & 0 \end{bmatrix}$$

in $N^j = 0$ za $j \geq t$. Ker bi radi izračunali $p(\rho I + N)$, se splača polinom $p(\lambda)$ razviti po bazi $\{1, \lambda - \rho, (\lambda - \rho)^2, (\lambda - \rho)^3, \ldots\}$ (in ne po standardni bazi $\{1, \lambda, \lambda^2, \ldots\}$). Dobimo

$$p(\lambda) = c_0 + c_1(\lambda - \rho) + c_2(\lambda - \rho)^2 + c_3(\lambda - \rho)^2 + \cdots$$

za neke $c_i \in \mathbb{C}$. Pri tem je očitno $c_0 = p(\rho)$. Ostale koeficiente izračunamo tako, da polinom odvajamo:

$$p'(\lambda) = c_1 + 2c_2(\lambda - \rho) + 3c_3(\lambda - \rho)^3 + \cdots .$$

Sledi $c_1 = p'(\rho)$. Če še enkrat odvajamo, dobimo

$$p''(\lambda) = 2c_2 + 6c_3(\lambda - \rho) + \cdots .$$

Torej je $c_2 = \frac{p''(\rho)}{2}, c_3 = \frac{p'''(\rho)}{6}, \ldots$. V splošnem je $c_j = \frac{p^{(j)}(\rho)}{j!}$, torej je

$$p(\lambda) = \sum_{j=0}^{k} \frac{p^{(j)}(\rho)}{j!}(\lambda - \rho)^j,$$

kjer je $k$ stopnja polinoma $p(\lambda)$. Sledi

$$p(J_t(\rho)) = p(\rho I + N) = \sum_{j=0}^{k} \frac{p^{(j)}(\rho)}{j!} N^j = \begin{bmatrix} p(\rho) & p'(\rho) & \frac{1}{2}p''(\rho) & \cdots & \frac{1}{(t-1)!}p^{(t-1)}(\rho) \\ & \ddots & \ddots & \ddots & \vdots \\ & & \ddots & \ddots & \frac{1}{2}p''(\rho) \\ & & & \ddots & p'(\rho) \\ & & & & p(\rho) \end{bmatrix}.$$

Zdaj bomo na enak način definirali vrednost *analitične funkcije* (t.j. take, ki jo je mogoče razviti v Taylorjevo vrsto) v matriki. Najprej definirajmo funkcijo v Jordanovi celici.

**Definicija 3.7.** Naj bo $D \subseteq \mathbb{C}$ odprta množica, ki vsebuje $\rho$. Za funkcijo $f\colon D \to \mathbb{C}$, ki jo je mogoče razviti v Taylorjevo vrsto

$$f(\lambda) = \sum_{j=0}^{\infty} \frac{1}{j!} f^{(j)}(\rho)(\lambda - \rho)^j,$$

definiramo

$$f(J_t(\rho)) = f(\rho I + N) = \sum_{j=0}^{t-1} \frac{1}{j!} f^{(j)}(\rho) N^j = \begin{bmatrix} f(\rho) & f'(\rho) & \frac{1}{2}f''(\rho) & \cdots & \frac{1}{(t-1)!}f^{(t-1)}(\rho) \\ & \ddots & \ddots & \ddots & \vdots \\ & & \ddots & \ddots & \frac{1}{2}f''(\rho) \\ & & & \ddots & f'(\rho) \\ & & & & f(\rho) \end{bmatrix}.$$

Zgornja vsota je končna, ker je $N^t = 0$.

Zdaj, ko znamo definirati analitično funkcijo v Jordanovi celici, jo lahko definiramo v splošni matriki.

**Definicija 3.8.** Naj bo $f$ kompleksna funkcija, ki se jo da v okolici spektra matrike $A$ razviti v Taylorjevo vrsto, in naj bo $A = P\mathcal{J}(A)P^{-1}$, kjer je $\mathcal{J}(A) = J_{t_1}(\rho_1) \oplus \cdots \oplus J_{t_k}(\rho_k)$ (in kjer števila $\rho_j$ niso nujno različna). Potem definiramo

$$f(\mathcal{J}(A)) = f(J_{t_1}(\rho_1)) \oplus \cdots \oplus f(J_{t_k}(\rho_k))$$

in

$$f(A) = Pf(\mathcal{J}(A))P^{-1}.$$

**Opombe 3.9.**

1. Če je $i \neq j$, potem za definicijo $f(J_{t_i}(\rho_i))$ uporabimo drug razvoj funkcije $f$ v Taylorjevo vrsto (okrog točke $\rho_i$) kot za definicijo $f(J_{t_j}(\rho_j))$ (okrog točke $\rho_j$).
2. Pred definicijo smo dokazali, da se definicija matrike $f(A)$ ujema z že znano definicijo, če je $f$ polinom.
3. Pri funkcionalni analizi se $f(A)$ definira na druge načine (z integralom, s Taylorjevo vrsto,...). Te definicije so ekvivalentne zgornji.

4. Da se pokazati, da za vsako matriko $A$ in vsako funkcijo $f$ kot zgoraj obstaja polinom $p$ (ki je odvisen od $f$ in od $A$), da je $f(A) = p(A)$.

5. Jordanova baza ni enolična, torej lahko obstajata različni obrnljivi matriki $P$ in $Q$, da je $A = P\mathcal{J}(A)P^{-1} = Q\mathcal{J}(A)Q^{-1}$. Da se pokazati (na primer s pomočjo prejšnje točke), da je potem $Pf(\mathcal{J}(A))P^{-1} = Qf(\mathcal{J}(A))Q^{-1}$. To pomeni, da je zgornja definicija dobra.

Zgoraj smo razmislili, da je definicija funkcije matrik dobra. Vprašati pa se je treba tudi, ali je *smiselna*. Na primer, če je $f(z) = \frac{1}{z}$, potem pričakujemo, da bo matrika $f(A)$ definirana, ko bo $A$ obrnljiva, in da bo tedaj $f(A) = A^{-1}$. Ali pa, če imamo funkcijo $f(z) = \sqrt{z}$, definirano na primernem območju, potem pričakujemo, da bo za matriko $f(A)$ veljalo $f(A) \cdot f(A) = A$. Da take enakosti res veljajo, nam pove naslednja trditev. Dokazali je ne bomo, saj se kompleksne analitične (holomorfne) funkcije obravnavajo šele pri Analizi 2.

**Trditev 3.10.** *Naj bo $\mathcal{F}$ algebra vseh kompleksnih funkcij, ki jih je mogoče v okolici spektra matrike $A$ razviti v Taylorjevo vrsto in naj bo $\Phi\colon \mathcal{F} \to \mathbb{C}^{n\times n}$ preslikava, definirana s predpisom $\Phi(f) = f(A)$. Potem velja:*

1. $\Phi(\alpha f + \beta g) = \alpha\Phi(f) + \beta\Phi(g)$ *za vse* $\alpha, \beta \in \mathbb{C}$ *in* $f, g \in \mathcal{F}$.

2. $\Phi(f \cdot g) = \Phi(f) \cdot \Phi(g)$ *za vse* $f, g \in \mathcal{F}$.

3. *Naj bo* $1 \in \mathcal{F}$ *konstantna funkcija 1. Potem je* $\Phi(1) = I$.

4. $\Phi(\mathrm{id}_{\mathbb{C}}) = A$.

Z besedami, trditev nam pove, da je $\Phi$ homomorfizem algeber, ki identiteto slika v matriko $A$.

**Primer 3.11.** Izračunajmo $f(J)$ in $g(J)$, kjer je $J = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{bmatrix}$, $f(z) = \sin z$ in $g(z) = \cos z$.

Matrika $J$ je že v Jordanovi kanonični formi, edina njena lastna vrednost je 0. Zato je treba izračunati odvode funkcij $f$ in $g$ v točki 0. Ker je $f'(z) = \cos z$ in $f''(z) = -\sin z$, je $f(0) = 0$, $f'(0) = 1$ in $f''(0) = 0$. Zato je

$$\sin J = \begin{bmatrix} f(0) & f'(0) & \frac{1}{2}f''(0) \\ 0 & f(0) & f'(0) \\ 0 & 0 & f(0) \end{bmatrix} = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{bmatrix} = J.$$

Podobno je $g'(z) = -\sin z$ in $g''(z) = -\cos z$, zato je $g(0) = 1$, $g'(0) = 0$, $g''(0) = -1$ in

$$\cos J = \begin{bmatrix} g(0) & g'(0) & \frac{1}{2}g''(0) \\ 0 & g(0) & g'(0) \\ 0 & 0 & g(0) \end{bmatrix} = \begin{bmatrix} 1 & 0 & -\frac{1}{2} \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

Prejšnja trditev je utemeljila smiselnost definicije funkcij matrike. Za sinus in kosinus na primer velja $\sin^2 z + \cos^2 z = 1$ za vsak $z \in \mathbb{C}$, zato pričakujemo, da mora veljati $\sin^2 J + \cos^2 J = I$. Preverimo, da to res velja:

$$\sin^2 J + \cos^2 J = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{bmatrix}^2 + \begin{bmatrix} 1 & 0 & -\frac{1}{2} \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}^2 = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} + \begin{bmatrix} 1 & 0 & -1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = I.$$

**Primer 3.12.** Naj bo $J = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}$. Matrika je v Jordanovi kanonični formi, edina njena lastna vrednost pa je 1. Pri Analizi 2 se lahko naučimo, da je korenska funkcija holomorfna npr. na celi kompleksni ravnini, razen na množici nepozitivnih realnih števil, če definiramo, da je vrednost korena kompleksno število s pozitivnim realnim delom. V posebnem primeru je korenska funkcija analitična na okolici števila 1, zato lahko izračunamo $f(J)$, kjer je $f(z) = \sqrt{z}$.

Ker je $f'(z) = \frac{1}{2}z^{-\frac{1}{2}}$ in $f''(z) = -\frac{1}{4}z^{-\frac{3}{2}}$, je $f(1) = 1$, $f'(1) = \frac{1}{2}$ in $\frac{1}{2}f''(1) = -\frac{1}{8}$, zato je $\sqrt{J} = \begin{bmatrix} 1 & \frac{1}{2} & -\frac{1}{8} \\ 0 & 1 & \frac{1}{2} \\ 0 & 0 & 1 \end{bmatrix}$. Vsak se lahko sam prepriča, da za matriko $\sqrt{J}$ velja $\sqrt{J} \cdot \sqrt{J} = J$, kar pričakujemo za koren matrike.

Omenimo še izrek o preslikavi spektra:

**Izrek 3.13** (Izrek o preslikavi spektra)**.** *Naj bo $A$ poljubna kompleksna kvadratna matrika in $f$ kompleksna funkcija, ki se jo da v okolici spektra matrike $A$ razviti v Taylorjevo vrsto. Če je $\{\lambda_1, \ldots, \lambda_k\}$ spekter matrike $A$, potem je $\{f(\lambda_1), \ldots, f(\lambda_k)\}$ spekter matrike $f(A)$. Poleg tega je algebraična večkratnost vsake lastne vrednosti $\lambda$ matrike $f(A)$ enaka vsoti algebraičnih večkratnosti vseh tistih lastnih vrednosti matrike $A$, ki jih $f$ preslika v $\lambda$.*

*Dokaz.* Zaradi enakosti $f(A) = Pf(\mathcal{J}(A))P^{-1}$ zadošča izrek dokazati za vse Jordanove matrike. Po definiciji funkcije matrike je $f(\mathcal{J}(A))$ zgornje trikotna matrika, torej so njene lastne vrednosti natanko diagonalni elementi. Diagonalni elementi pa so natanko slike diagonalnih elementov matrike $\mathcal{J}(A)$ (torej njenih lastnih vrednosti), če na njih uporabimo funkcijo $f$. Izrek tako sledi. $\square$