

Lastne vrednosti - 3. del

4. Minimalni polinom matrike

Označimo s $\mathbb{C}[x]$ množico vseh polinomov v x s kompleksnimi koeficienti. Z $M_n(\mathbb{C})$ označimo množico vseh kompleksnih $n \times n$ matrik.

V polinom $p(x) = c_n x^n + c_{n-1} x^{n-1} + \dots + c_1 x + c_0 \in \mathbb{C}[x]$, bi radi namesto x vstavili matriko $A \in M_n(\mathbb{C})$. Problem je v tem, ker so členi $c_n A^n, c_{n-1} A^{n-1}, \dots, c_1 A$ matrike, člen c_0 pa je skalar. Zato v $p(x)$ člen c_0 pomnožimo z $x^0 = 1$, v $p(A)$ pa ga pomnožimo z $A^0 := I$. Torej je

$$p(A) := c_n A^n + c_{n-1} A^{n-1} + \dots + c_1 A + c_0 I$$

Opomba: V nadaljevanju bomo večkrat potrebovali, da iz $p(x) = p_1(x)p_2(x)$ sledi $p(A) = p_1(A)p_2(A)$. To ni povsem očitno, ampak je treba napraviti kratek račun.

Sedaj smo nared za glavno definicijo tega razdelka:

Definicija minimalnega polinoma

Polinom $m \in \mathbb{C}[x]$ je **minimalni polinom** matrike $A \in M_n(\mathbb{C})$, če velja:

- (1) $m(A) = 0$,
- (2) m ima vodilni koeficient 1.
- (3) med vsemi polinomi, ki zadoščajo (1) in (2), ima m najnižjo stopnjo.

Prepričajmo se najprej, da je definicija smiselna.

Trditev 1: (Obstoj in enoličnost minimalnega polinoma)

Vsaka matrika A ima natanko en minimalni polinom. Označimo ga z m_A .

Dokaz bomo razbili v več korakov.

Vzemimo poljubno matriko $A \in M_n(\mathbb{C})$.

1. korak Konstruirajmo najprej tak polinom $p \in \mathbb{C}[x]$, ki zadošča $p(A) = 0$ in ki ima vodilni koeficient enak ena.

Očitno je $M_n(\mathbb{C})$ vektorski prostor nad $\mathbb{C}$ dimenzije n^2 . Ker ima množica $\{I, A, A^2, \dots, A^{n^2}\}$ en element več od dimenzije, je linearno odvisna. Obstajajo torej taki $c_0, c_1, c_2, \dots, c_{n^2} \in \mathbb{C}$, od katerih je vsaj en neničeln, da velja $\sum_{i=0}^{n^2} c_i A^i = 0$. Polinom $p(x)$ dobimo tako, da polinom $\sum_{i=0}^{n^2} c_i x^i$ delimo z njegovim vodilnim koeficientom.

2. korak Matrika A ima vsaj en minimalni polinom.

Naj bo $\mathcal{M}$ množica vseh polinomov, ki zadoščajo točkam (1) in (2) iz definicije minimalnega polinoma. Po 1. koraku je množica $\mathcal{M}$ neprazna. Vzemimo v množici $\mathcal{M}$ polinom z najnižjo stopnjo. Tak polinom potem zadošča vsem trem točkam iz definicije minimalnega polinoma.

3. korak Naj bo m minimalni polinom matrike A in naj bo p tak polinom, ki zadošča $p(A) = 0$. Potem m deli p .

Po izreku o deljenju z ostankom obstajata taka polinoma k in r , da velja $p = km + r$ in $\deg r < \deg m$. Ker je $m(A) = 0$ in $p(A) = 0$, je tudi $r(A) = 0$. Če bi bil r neničeln polinom, bi ga delili z vodilnim koeficientom in bi dobili tak polinom, ki zadošča točkam (1) in (2) iz definicije minimalnega polinoma in je nižje stopnje od m . To je v nasprotju s predpostavko, da m zadošča točki (3) iz definicije minimalnega polinoma. Torej je r ničeln polinom.

4. korak Če sta m_1 in m_2 minimalna polinoma matrike A , potem je $m_1 = m_2$.

Ker je $m_2(A) = 0$, po 3. koraku m_1 deli m_2 . Ker je $m_1(A) = 0$, po 3. koraku m_2 deli m_1 . Torej obstaja taka konstanta $c \neq 0$, da je $m_2 = cm_1$. Ker imata oba polinoma vodilni koeficient enak 1, je $c = 1$. □

Radi bi dokazali, da minimalni polinom matrike A deli karakteristični polinom matrike A . Po 3. koraku dokaza Trditve 2, je dovolj dokazati:

Trditev 2: (Cayley-Hamiltonov izrek)

Naj bo $p_A(x)$ karakteristični polinom matrike A . Potem velja $p_A(A) = 0$.

Opomba: Kaj je narobe z naslednjim "dokazom"? V $p_A(x) = \det(A - xI)$ vstavimo $x = A$ in dobimo $p_A(A) = \det(A - AI) = \det 0 = 0$.

Dokaz: Spomnimo se formule $B^{-1} = \frac{1}{\det B} \tilde{B}^T$ za inverz matrike, kjer matriko $\tilde{B}$ dobimo tako, da v matriki B vsak element $b_{i,j}$ zamenjamo z $(-1)^{i+j} \det B_{i,j}$. (B s pobrisano i -to vrstico in j -tim stolpcem je $B_{i,j}$).

Če to formulo pomnožimo z $\det(B)B$ z leve, dobimo $\det(B)I = B \tilde{B}^T$.

Sedaj vstavimo $B = A - xI$ in dobimo $p_A(x)I = (A - xI) \widetilde{(A - xI)}^T$.

Elementi matrike $\widetilde{(A - xI)}^T$ so polinomi v x stopnje $\leq n - 1$. (So namreč determinante velikosti $n - 1$, katerih elementi so polinomi stopnje ≤ 1 .)

V enačbo $p_A(x)I = \widetilde{(A - xI)}^T$ vstavimo

$p_A(x) = c_0 + c_1x + \dots + c_nx^n$, kjer $c_i \in \mathbb{C}$, in

$\widetilde{(A - xI)}^T = B_0 + xB_1 + \dots + x^{n-1}B_{n-1}$, kjer $B_i \in M_n(\mathbb{C})$.

Primerjajmo koeficiente pri potencah x^i , kjer $i = 0, 1, 2, \dots, n-1, n$:

$$\begin{aligned} c_0I &= AB_0 \\ c_1I &= AB_1 - B_0 \\ c_2I &= AB_2 - B_1 \\ &\vdots \\ c_{n-1}I &= AB_{n-1} - B_{n-2} \\ c_nI &= -B_{n-1} \end{aligned}$$

Pomnožimo i -to enačbo z A^i z leve in vse enačbe seštejmo.

Dobimo $c_0I + c_1A + c_2A^2 + \dots + c_{n-1}A^{n-1} + c_nA^n =$

$AB_0 + A(AB_1 - B_0) + A^2(AB_2 - B_1) + \dots + A^{n-1}(AB_{n-1} - B_{n-2}) + A^n(-B_{n-1})$.

Na desni strani odpravimo oklepaje in opazimo, da se vse pokrajša. □

Ker minimalni polinom $m_A(x)$ deli karakteristični polinom $p_A(x)$ in ker je $p_A(x)$ oblike $p_A(x) = (-1)^n(x - \lambda_1)^{n_1} \cdots (x - \lambda_k)^{n_k}$, je $m_A(x)$ oblike

$$m_A(x) = (x - \lambda_1)^{r_1} \cdots (x - \lambda_k)^{r_k}$$

kjer je $r_1 \leq n_1, \dots, r_k \leq n_k$. Radi bi pokazali še, da je $r_1 \geq 1, \dots, r_k \geq 1$:

Trditev 3

Vsaka lastna vrednost matrike A je ničla minimalnega polinoma m_A .

Dokaz: Naj bo λ lastna vrednost matrike A in naj bo v pripadajoči lastni vektor. Iz $Av = \lambda v$ s popolno indukcijo izpeljemo, da velja $A^k v = \lambda^k v$ za vsak k . Če namreč velja $A^{k-1} v = \lambda^{k-1} v$ za nek k , potem je

$$A^k v = A(A^{k-1} v) = A(\lambda^{k-1} v) = \lambda^{k-1} Av = \lambda^{k-1}(\lambda v) = \lambda^k v.$$

Recimo, da je minimalni polinom oblike $m_A(x) = \sum_{i=0}^r c_i x^i$. Potem velja

$$0 = 0v = m_A(A)v = \sum_{i=0}^r c_i A^i v = \sum_{i=0}^r c_i \lambda^i v = m_A(\lambda)v.$$

Ker je v neničeln, odtod sledi $m_A(\lambda) = 0$.

Kakšna je zveza med minimalnim polinomom in obstojem diagonalizacije?

Trditve 4

Matrika ima diagonalizacijo natanko tedaj, ko njen minimalni polinom nima večkratnih ničel.

Dokaz: Naj bodo $\lambda_1, \dots, \lambda_k$ vse paroma različne lastne vrednosti matrike A . Iz 3. razdelka vemo, da ima A diagonalizacijo natanko tedaj, ko je produkt matrik $A - \lambda_i I$ enak nič. Označimo z $m(x)$ produkt polinomov $x - \lambda_i$, se pravi $m(x) = (x - \lambda_1) \cdots (x - \lambda_k)$. Torej ima A diagonalizacijo natanko tedaj, ko je $m(A) = 0$. Po 3. koraku v dokazu Trditve 1 velja $m(A) = 0$ natanko tedaj, ko minimalni polinom $m_A(x)$ deli polinom $m(x)$. Po Trditvi 3 velja to natanko tedaj, ko je $m_A(x) = m(x)$. $\square$

Primer

Matriki $A = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ in $B = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ imata enak karakteristični polinom toda različna minimalna polinoma $m_A(x) = x - 1$ in $m_B(x) = (x - 1)^2$.

5. Korenski podprostor

Naj bodo $\lambda_1, \dots, \lambda_k$ vse paroma različne lastne vrednosti matrike $A \in M_n(\mathbb{C})$. Vemo, da je karakteristični polinom matrike A oblike

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

minimalni polinom matrike A pa je oblike

$$m_A(x) = (x - \lambda_1)^{r_1} \cdots (x - \lambda_k)^{r_k}$$

kjer števila $r_1, \dots, r_k$ zadoščajo $1 \leq r_1 \leq n_1, \dots, 1 \leq r_k \leq n_k$.

Števila r_i potrebujemo v definiciji korenskega podprostora:

Definicija korenskih vektorjev in korenskega podprostora

Množica $\text{Ker}(A - \lambda_i I)^{r_i}$ je vektorski podprostor v $\mathbb{C}^n$. Pravimo ji **korenski podprostor** matrike A za lastno vrednost λ_i . Njenim neničelnim elementom pravimo **korenski vektorji** matrike A za lastno vrednost λ_i .

Korenske podprostore matrike A bomo potrebovali pri konstrukciji jordske kanonične forme matrike A v naslednjem razdelku. Oglejmo si najprej nekaj njihovih osnovnih lastnosti.

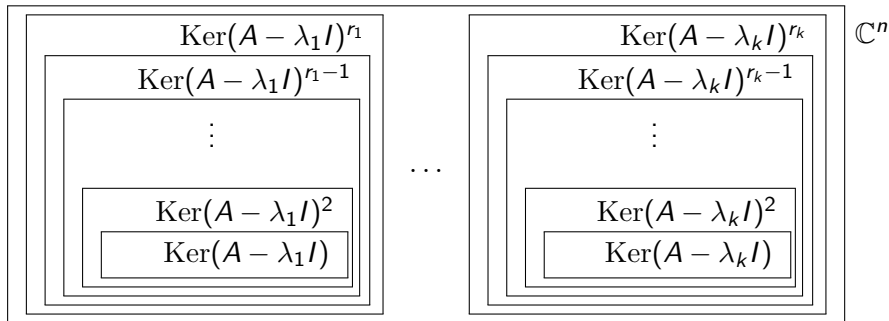
Izrek o korenskem razcepu

Naj bodo A , λ_i , n_i in r_i kot zgoraj.

- 1 Velja $\text{Ker}(A - \lambda_i I) \subset \text{Ker}(A - \lambda_i I)^2 \subset \dots \subset \text{Ker}(A - \lambda_i I)^{r_i} = \text{Ker}(A - \lambda_i I)^{r_i+1} = \text{Ker}(A - \lambda_i I)^{r_i+2} = \dots$, kjer je inkluzija stroga.
- 2 $\dim \text{Ker}(A - \lambda_i I)^{r_i} = n_i$, se pravi, da je dimenzija korenskega podprostora A za λ_i enaka algebraični večkratnosti λ_i .
- 3 $\mathbb{C}^n = \bigoplus_{i=1}^k \text{Ker}(A - \lambda_i I)^{r_i}$, kar pomeni, da za vsak $w \in \mathbb{C}^n$ obstajajo natanko določeni $w_i \in \text{Ker}(A - \lambda_i I)^{r_i}$, ki zadoščajo $w = \sum_{i=1}^k w_i$.

Označimo z $W_i = \text{Ker}(A - \lambda_i I)^{r_i}$ korenski podprostor A za λ_i , z $V_i = \text{Ker}(A - \lambda_i I)$ pa lastni podprostor A za λ_i . Iz prve točke sledi, da je V_i vsebovan v W_i in da sta enaka natanko tedaj, ko je $r_i = 1$.

Izrek o korenskem razcepu nam pove, da imamo naslednjo situacijo:



Velike škatle $\text{Ker}(A - \lambda_i I)^{r_i}$ so korenski podprostorji matrike A . Njihova vsota je $\mathbb{C}^n$. Male škatle $\text{Ker}(A - \lambda_i I)$ so lastni podprostorji matrike A .

Priprave na dokaz izreka

V dokazu izreka bomo potrebovali pojem invariantnega podprostora.

Definicija invariantnega podprostora

Vektorski podprostor U v $\mathbb{C}^n$ je **invarianten** za matriko $A \in M_n(\mathbb{C})$, če za vsak $u \in U$ velja $Au \in U$.

Primeri invariantnih podprostorov matrike A

- Trivialni podprostor $\{0\}$.
- Lastni podprostori matrike A .
- Korenski podprostori matrike A .
- Presek invariantnih podprostorov za A je invarianten podprostor za A .

Dokažimo invariantnost korenskega podprostora $W_i = \text{Ker}(A - \lambda_i I)^{r_i}$. Za vsak $w \in W_i$ velja $(A - \lambda_i I)^{r_i} w = 0$. Če to pomnožimo z A , dobimo $A(A - \lambda_i I)^{r_i} w = 0$. Ker je $A(A - \lambda_i I)^{r_i} = (A - \lambda_i I)^{r_i} A$, od tod sledi $(A - \lambda_i I)^{r_i} Aw = 0$. Torej $Aw \in W_i$. Dokaz ostalih točk je še lažji.

Trditev 1

Vsak netrivialen invarianten podprostor za matriko A vsebuje vsaj en lastni vektor matrike A .

Dokaz: Naj bo U netrivialen invarianten podprostor za A . Ker je $U \neq \{0\}$, ima U bazo, recimo $\mathcal{B} = \{u_1, \dots, u_m\}$. Ker je U invarianten za A , lahko definiramo linearno preslikavo $L: U \rightarrow U$ z $L(u) = Au$.

Naj bo $\begin{bmatrix} x_1 \\ \vdots \\ x_m \end{bmatrix}$ lastni vektor matrike $[L]_{\mathcal{B}}$ za lastno vrednost λ . Očitno

$v := x_1 u_1 + \dots + x_m u_m$ pripada U . Pokažimo, da je v lastni vektor za A . Velja namreč $[Lv]_{\mathcal{B}} = [L]_{\mathcal{B}}[v]_{\mathcal{B}} = \lambda[v]_{\mathcal{B}} = [\lambda v]_{\mathcal{B}}$. Torej je $Lv = \lambda v$. $\square$

Dokaz točke (3)

Dokaz točke (3) v izreku bomo razdelili na več trditev.

Trditev 2

Presek dveh različnih korenskih podprostorov matrike A je trivialen.

Dokaz. Ker sta korenska podprostora W_i in W_j invariantna za A , je invarianten za A tudi njun presek. Če je njun presek netrivialen, potem po Trditvi 1 vsebuje lastni vektor za A . Torej je $Av = \lambda v$ za nek neničeln $v \in W_i \cap W_j$. Odtod sledi, da za vsak polinom $p(x)$ velja $p(A)v = p(\lambda)v$. Če vzamemo $p(x) = (x - \lambda_i)^{r_i}$, dobimo $0 = (A - \lambda_i I)^{r_i} v = (\lambda - \lambda_i)^{r_i} v$, odkoder sledi $\lambda = \lambda_i$. Če pa vzamemo $p(x) = (x - \lambda_j)^{r_j}$, potem dobimo $0 = (A - \lambda_j I)^{r_j} v = (\lambda - \lambda_j)^{r_j} v$, odkoder sledi $\lambda = \lambda_j$. Torej je $\lambda_i = \lambda_j$. Odtod sledi $W_i = W_j$, kar je v nasprotju s predpostavko. $\square$

Trditev 3

Če vektorji $w_1 \in W_1, \dots, w_k \in W_k$ zadoščajo $w_1 + \dots + w_k = 0$, potem velja $w_1 = \dots = w_k = 0$.

Dokaz: Dokazali bomo, da za vsak $i = 1, \dots, k$ velja naslednja trditev:

(T_i) Če vektorji $w_1 \in W_1, \dots, w_i \in W_i$ zadoščajo $w_1 + \dots + w_i = 0$, potem velja $w_1 = \dots = w_i = 0$.

Baza indukcije: Trditev (T_1) je očitna.

Indukcijski korak: Recimo, da velja trditev (T_i), kjer $i < k$.

Radi bi dokazali trditev (T_{i+1}). Vzemimo take vektorje

$w_1 \in W_1, \dots, w_i \in W_i, w_{i+1} \in W_{i+1}$, da velja $w_1 + \dots + w_i + w_{i+1} = 0$.

Če to pomnožimo z $(A - \lambda_{i+1}I)^{r_{i+1}}$ z leve, dobimo $w'_1 + \dots + w'_i + 0 = 0$.

Ker je vsak korenski podprostor W_j invarianten in ker vsebuje w_j , vsebuje

tudi $w'_j := (A - \lambda_{i+1}I)^{r_{i+1}}w_j$. Iz $w'_1 + \dots + w'_i = 0$ torej po indukcijski

predpostavki sledi, da velja $w'_1 = \dots = w'_i = 0$. Zato $w_1, \dots, w_i \in W_{i+1}$.

Po Trditvi 2 je $W_1 \cap W_{i+1} = \{0\}, \dots, W_i \cap W_{i+1} = \{0\}$. Odtod sledi, da je $w_1 = \dots = w_i = 0$. Odtod sledi še $w_{i+1} = 0$. □

Opomba: Recimo, da je $\mathcal{B}_i$ baza za korenski podprostor W_i . Iz Trditve 3 sledi, da je $\mathcal{B}_1 \cup \dots \cup \mathcal{B}_k$ baza za vsoto $W_1 + \dots + W_k$ vseh korenskih podprostorov. Torej je $\dim(W_1 + \dots + W_k) = \dim W_1 + \dots + \dim W_k$.

Trditev 4

Vsota vseh korenskih podprostorov matrike A je enaka $\mathbb{C}^n$.

Dokaz: Če v oceno $n(L_1 \cdots L_k) \leq n(L_1) + \dots + n(L_k)$ iz prejšnjega poglavja, vstavimo $L_i = (A - \lambda_i I)^{r_i}$ in upoštevamo $L_1 \cdots L_k = m_A(A) = 0$ ter $n(L_i) = \dim \operatorname{Ker}(A - \lambda_i I)^{r_i} = \dim W_i$, dobimo, da velja ocena $n \leq \dim W_1 + \dots + \dim W_k$. Po opombi zgoraj (ki ste jo delali na vajah) iz Trditve 3 sledi, da je $\dim(W_1 + \dots + W_k) = \dim W_1 + \dots + \dim W_k$. Ker je torej $\dim(W_1 + \dots + W_k) \geq n$, velja $W_1 + \dots + W_k = \mathbb{C}^n$. $\square$

Opomba: Trditvi 3 in 4 nam dasta ravno točko (3) v izreku.

Dokaz točke (2)

Označimo $t_i := \dim W_i$ za vsak $i = 1, \dots, k$. Radi bi pokazali, da je $t_i = n_i$. Naj bo $\mathcal{B}_i = \{v_{i,1}, \dots, v_{i,t_i}\}$ baza za W_i . Ker je podprostor W_i invarianten za A , obstajajo taka števila $\alpha_{i,j,j'}$, da velja

$$\begin{aligned} Av_{i,1} &= \alpha_{i,1,1}v_{i,1} + \dots + \alpha_{i,1,t_i}v_{i,t_i} \\ &\vdots \\ Av_{i,t_i} &= \alpha_{i,t_i,1}v_{i,1} + \dots + \alpha_{i,t_i,t_i}v_{i,t_i} \end{aligned}$$

V matrični obliki to zapišemo kot $AP_i = P_iA_i$, kjer je

$$A_i = \begin{bmatrix} \alpha_{i,1,1} & \dots & \alpha_{i,t_i,1} \\ \vdots & \ddots & \vdots \\ \alpha_{i,1,t_i} & \dots & \alpha_{i,t_i,t_i} \end{bmatrix}, \quad P_i := [v_{i,1} \dots v_{i,t_i}]$$

Odtod sledi

$$A[P_1 \dots P_k] = [P_1 \dots P_k] \begin{bmatrix} A_1 & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & A_k \end{bmatrix} \quad (1)$$

Matrike $P := [P_1 \dots P_k]$ je obrnljiva, ker je (po že dokazani točki (3) v izreku) unija baz $\mathcal{B}_i$ baza za $\mathbb{C}^n$. Označimo z A' bločno diagonalno matriko iz A_i -jev. Po formuli (1) je $A' = P^{-1}AP$, torej imata A in A' enak karakteristični polinom

$$\det(A - xI) = \det(A_1 - xI) \cdots \det(A_k - xI). \quad (2)$$

Pokažimo, da je λ_i edina lastna vrednost matrike A_i . Potem je $\det(A_i - xI) = (\lambda_i - x)^{t_i}$. To vstavimo v formulo (2) in dobimo $t_i = n_i$.

Naj bo μ_i poljubna lastna vrednost matrike A_i in naj bo $u_i \in \mathbb{C}^{t_i}$ pripadajoči lastni vektor. Potem je

$$A(P_i u_i) = (AP_i)u_i = (P_i A_i)u_i = P_i(A_i u_i) = P_i(\mu_i u_i) = \mu_i P_i u_i \quad (3)$$

Ker je $P_i u_i$ linearna kombinacija stolpcev P_i in ker so stolpci P_i v W_i je $P_i u_i \in W_i$. Poleg tega je $P_i u_i \neq 0$, ker je $u_i \neq 0$ in ker so stolpci P_i linearno neodvisni. Po definiciji W_i je $(A - \lambda_i I)^{r_i} P_i u_i = 0$. Iz formule (3) sledi, da je $(A - \lambda_i I)^{r_i} P_i u_i = (\mu_i - \lambda_i)^{r_i} P_i u_i$. Torej je $\mu_i = \lambda_i$.

Dokaz točke (1)

Dokaz točke (1) v izreku bomo razdelili v več korakov.

1. korak Če je $m \leq m'$, potem velja $\text{Ker}(A - \lambda_i I)^m \subseteq \text{Ker}(A - \lambda_i I)^{m'}$.

Za vsak $v \in \text{Ker}(A - \lambda_i I)^m$ velja $(A - \lambda_i I)^m v = 0$. Pomnožimo to z leve z $(A - \lambda_i I)^{m'-m}$ in dobimo $(A - \lambda_i I)^{m'} v = 0$. Torej je $v \in \text{Ker}(A - \lambda_i I)^{m'}$.

2. korak Za vsak $r'_i \geq r_i$ je $\text{Ker}(A - \lambda_i I)^{r'_i} = \text{Ker}(A - \lambda_i I)^{r_i}$.

Označimo $W'_i := \text{Ker}(A - \lambda_i I)^{r'_i}$ in $n'_i = \dim W'_i$. Po 1. koraku je $W_i \subseteq W'_i$, zato je $n_i \leq n'_i$. Kot v dokazu Trditve 3 vidimo, da za poljubne $w'_i \in W'_i$, ki zadoščajo $w'_1 + \dots + w'_k = 0$, velja $w'_1 = \dots = w'_k = 0$. Kot v opombi za Trditvijo 3 odtod sledi, da je $n'_1 + \dots + n'_k = n$. Odtod in iz $n_i \leq n'_i$ sledi, da je $n'_i = n_i$ za vsak i . Torej je $W'_i = W_i$ za vsak i .

3. korak Za vsak i je $\text{Ker}(A - \lambda_i I)^{r_i-1} \neq \text{Ker}(A - \lambda_i I)^{r_i}$.

Če bi za nek i veljal enačaj, potem bomo pokazali, da bi polinom $m_i(x) := m_A(x)/(x - \lambda_i)$ zadoščal $m_i(A) = 0$, kar bi bilo v nasprotju z definicijo minimalnega polinoma. Vzemimo poljuben $w \in \mathbb{C}^n$.

Po Trditvi 4 obstajajo taki $w_j \in W_j$, da velja $w = \sum_{j=1}^k w_j$.

Za vsak $j \neq i$ velja $(A - \lambda_j)^{r_j} w_j = 0$, odkoder sledi $m_i(A) w_j = 0$.

Za $j = i$ pa velja $(A - \lambda_j)^{r_j-1} w_j = 0$, torej je tudi $m_i(A) w_j = 0$.

Odtod sledi $m_i(A) w = 0$. Ker je to res za vsak $w \in \mathbb{C}^n$, je $m_i(A) = 0$.

4. korak Če velja $\text{Ker}(A - \lambda_i I)^m \neq \text{Ker}(A - \lambda_i I)^{m+1}$ za nek $m \geq 1$ in nek $i = 1, \dots, k$, potem velja tudi $\text{Ker}(A - \lambda_i I)^{m-1} \neq \text{Ker}(A - \lambda_i I)^m$.

Predpostavimo, da velja $\text{Ker}(A - \lambda_i I)^{m-1} = \text{Ker}(A - \lambda_i I)^m$.

Dokazujemo, da velja $\text{Ker}(A - \lambda_i I)^m = \text{Ker}(A - \lambda_i I)^{m+1}$. Vzemimo poljuben $v \in \text{Ker}(A - \lambda_i I)^{m+1}$. Potem $(A - \lambda_i)v \in \text{Ker}(A - \lambda_i I)^m$.

Torej $(A - \lambda_i)v \in \text{Ker}(A - \lambda_i I)^{m-1}$ po predpostavki. Odtod sledi, da $v \in \text{Ker}(A - \lambda_i I)^m$. Torej je $\text{Ker}(A - \lambda_i I)^m \supseteq \text{Ker}(A - \lambda_i I)^{m+1}$.

Obratna inkluzija sledi iz 1. koraka.