1 Konačnodimenzionalni prostori

Polje je skup K s barem dva elementa na kome su zadane dvije komutativne i asocijativne binarne operacije, zbrajanje

$$+ : K \times K \to K, \qquad (\alpha, \beta) \mapsto \alpha + \beta)$$

i množenje

$$\cdot : K \times K \to K, \qquad (\alpha, \beta) \mapsto \alpha\beta),$$

tako da vrijedi:

(a) $(K, +)$ je grupa s neutralnim elementom 0;

(b) $(K \setminus \{0\}, \cdot)$ je grupa s neutralnim elementom 1;

(c) množenje je distributivno u odnosu na zbrajanje: $\alpha(\beta + \gamma) = \alpha\beta + \alpha\gamma$.

Glavni primjeri polja su polje realnih brojeva $\mathbb{R}$, polje kompleksnih brojeva $\mathbb{C}$ i polje racionalnih brojeva $\mathbb{Q}$.

Vektorski prostor nad poljem K je neprazan skup V koji je komutativna grupa s obzirom na operaciju zbrajanja $(+ : V \times V \to V, (v, w) \mapsto v + w)$ i na kojem je definirana operacija množenja elementima polja K (tj. preslikavanje $K \times V \to V, (\lambda, v) \mapsto \lambda v)$ koja je distributivna s obzirom na obje operacije zbrajanja:

$$\lambda(v + w) = \lambda v + \lambda w \qquad \text{i} \qquad (\lambda + \mu)v = \lambda v + \mu v \qquad \forall \lambda, \mu \in K,\ \forall v, w \in V,$$

ima svojstvo kvaziasocijativnosti:

$$(\lambda\mu)v = \lambda(\mu v) \qquad \forall \lambda, \mu \in K,\ \forall v \in V,$$

i jedinica 1 ima svojstvo:

$$1v = v \qquad \forall v \in V.$$

Potprostor vektorskog prostora V je podskup $W \subseteq V$ koji je i sam vektorski prostor nad istim poljem s obzirom na iste operacije. To zapravo znači da je W neprazan podskup od V i da vrijedi:

$$v, w \in W \Rightarrow v + w \in W, \qquad v \in W \ \text{ i } \ \lambda \in K \Rightarrow \lambda v \in W.$$

Kada želimo iskazati da je W potprostor vektorskog prostora V pisat ćemo $W \leq V$.

Propozicija 1.1 *Neka je V vektorski prostor nad poljem K i neka je Σ bilo koji skup potprostora od V. Tada je i presjek $\bigcap_{W \in \Sigma} W$ svih potprostora iz Σ također potprostor od V.*

Dokaz: Označimo sa U presjek svih potprostora iz skupa Σ. Neka su v i w bilo koji vektori iz U. Kako je U presjek svih potprostora $W \in \Sigma$, to su $v, w \in W$ za svaki $W \in \Sigma$. Kako je svaki W potprostor, odatle slijedi $v + w \in W$ za svaki $W \in \Sigma$. Budući da je U presjek svih $W \in \Sigma$ slijedi $v + w \in U$. Sasvim analogno dokazuje se da za svaki $v \in U$ i za svaki $\lambda \in K$ vrijedi $\lambda v \in U$.

Potprostor U iz prethodne propozicije je najveći potprostor koji je sadržan u svakom potprostoru iz skupa Σ ; dakle, ako je $X \leq W$ za svaki $W \in \Sigma$ onda vrijedi $U \supseteq X$.

Neka je sada S bilo kakav podskup vektorskog prostora V. Označimo sa Σ skup svih potprostora od V koji sadrže skup S : $\Sigma = \{X \leq V; X \supseteq S\}$ Stavimo:

$$[S] = \bigcap_{W \in \Sigma} W.$$

Očito je $[S]$ najmanji potprostor od V koji sadrži skup S : ako je W potprostor od V i ako $W \supseteq S$, onda $W \supseteq [S]$.

Propozicija 1.2 *$[S]$ je skup svih linearnih kombinacija vektora iz S.*

Dokaz: Dokažimo prvo da je svaka linearna kombinacija vektora iz S u $[S]$, a nakon toga da je svaki vektor $v \in S$ linearna kombinacija vektora iz S. Neka je X skup svih linearnih kombinacija vektora iz S. $[S]$ sadrži skup S, pa sadrži i sve linearne kombinacije vektora iz S, jer je $[S]$ potprostor po propoziciji 1.1. Zaključujemo da vrijedi $[S] \supseteq X$.

Dokažimo i obrnutu inkluziju, a time i skupovnu jednakost. U tu svrhu najprije uočimo da je X potprostor. Doista neka su x i y vektori iz X. Svaki od njih je tada linearna kombinacija vektora iz S. Stoga postoje vektori $x_1, x_2, \ldots, x_n, y_1, y_2, \ldots, y_m$ iz S i skalari $\lambda_1, \lambda_2, \ldots, \lambda_n, \mu_1, \mu_2, \ldots, \mu_m$ iz K, takvi da je

$$x = \lambda_1 x_1 + \lambda_2 x_2 + \ldots + \lambda_n x_n \qquad \text{i} \qquad y = \mu_1 y_1 + \mu_2 y_2 + \ldots + \mu_m y_m.$$

Tada je $x + y = \lambda_1 x_1 + \lambda_2 x_2 + \ldots + \lambda_n x_n + \mu_1 y_1 + \mu_2 y_2 + \ldots + \mu_m y_m$, dakle $x + y$ je linearna kombinacija vektora iz S, odnosno $x + y \in X$. Nadalje, za bilo koji skalar $\lambda \in K$ je $\lambda x = \lambda\lambda_1 x_1 + \lambda\lambda_2 x_2 + \ldots + \lambda\lambda_n x_n$ linearna kombinacija vektora iz S, dakle $\lambda x \in X$. To pokazuje da je X potprostor. Svaki vektor $v \in S$ ja linearna kombinacija vektora iz S $(v = 1v)$ pa slijedi da potprostor X sadrži skup S. Budući da je $[S]$ najmanji potprostor koji sadrži skup S, zaključujemo da vrijedi i obrnuta inkluzija $[S] \subseteq X$.

$[S]$ se zove **potprostor generiran skupom** S ili **potprostor razapet skupom** S. Ako je $W = [S]$ kažemo da **skup** S **razapinje potprostor** W.

Neka je V vektorski prostor nad poljem K i neka je S podskup od V. Skup S je **linearno nezavisan** ako vrijedi:

$$x \notin [S \setminus \{x\}] \qquad \forall x \in S.$$

Obratno, S je **linearno zavisan** ako je neki $x \in S$ linearna kombinacija preostalih vektora iz S. Lako se vidi da je S linearno nezavisan ako i samo ako za bilo koje međusobno različite vektore $x_1, x_2, \ldots, x_n \in S$ vrijedi:

$$\lambda_1, \lambda_2, \ldots, \lambda_n \in K, \qquad \lambda_1 x_1 + \lambda_2 x_2 + \ldots + \lambda_n x_n = 0 \;\Rightarrow\; \lambda_1 = \lambda_2 = \ldots = \lambda_n = 0.$$

Skup je linearno zavisan ako i samo ako postoji $n \in \mathbb{N}$ i postoje međusobno različiti vektori $x_1, x_2, \ldots, x_n \in S$ i postoje skalari $\lambda_1, \lambda_2, \ldots, \lambda_n \in K \setminus \{0\}$ takvi da je

$$\lambda_1 x_1 + \lambda_2 x_2 + \ldots + \lambda_n x_n = 0.$$

Lema 1.1 *Neka je S podskup vektorskog prostora V i neka je $x \in S$. Pretpostavimo da je $x \in [S \setminus \{x\}]$. Tada je $[S \setminus \{x\}] = [S]$.*

Dokaz: Kako je $S \setminus \{x\} \subseteq S$ očito je $[S \setminus \{x\}] \subseteq [S]$. Nadalje, iz $x \in [S \setminus \{x\}]$ slijedi $S \subseteq [S \setminus \{x\}]$, a odatle $[S] \subseteq [S \setminus \{x\}]$. Iz dvije inkluzije slijedi jednakost $[S \setminus \{x\}] = [S]$.

Baza vektorskog prostora V je podskup B od V sa sljedeća dva svojstva:

(*a*) skup B je linearno nezavisan,

(*b*) $[B] = V$.

Ako je B baza od V, svaki vektor iz V može se na jedinstven način prikazati kao linearna kombinacija vektora iz B. Precizno, za svaki $x \in V$ postoji jedinstvena funkcija $\varphi : B \to K$ koja ima sljedeća dva svojstva:

(*a*) za samo konačno mnogo vektora $v \in B$ je $\varphi(v) \neq 0$;

(*b*) $x = \sum_{v \in B} \varphi(v) v$.

Vektorski prostor V zove se **konačnodimenzionalan** ako postoji konačan skup S takav da je $[S] = V$. U daljnjem ćemo sa $|A|$ označavati broj elemenata bilo kojeg konačnog skupa A.

Teorem 1.1 *Neka je V konačnodimenzionalan vektorski prostor nad poljem K.*

(*a*) *Postoji konačna baza prostora V.*

(*b*) *Svaka baza prostora V je konačna.*

(*c*) *Ako su B_1 i B_2 dvije baze od V onda je $|B_1| = |B_2|$. Broj elemenata bilo koje baze od V zove se* **dimenzija** *od V i označava* $\dim V$, *ili preciznije* $\dim_K V$.

(*d*) *Ako je S linearno nezavisan podskup od V, S je sadržan u nekoj bazi od V.*

(*e*) *Ako je S podskup koji razapinje V, onda S sadrži neku bazu od V.*

(*f*) *Ako je S linearno nezavisan podskup od V koji ima $n = \dim V$ elemenata, onda je S baza od V.*

(*g*) *Ako je W potprostor od V, onda je prostor W konačnodimenzionalan i* $\dim W \leq \dim V$. *Nadalje, znak jednakosti* $(\dim W = \dim V)$ *vrijedi ako i samo ako je $W = V$.*

Dokaz: Dokazujemo najprije tvrdnju:

(e') *Ako je S konačan podskup od V koji razapinje V, onda S sadrži bazu od V.*

Dokaz tvrdnje (e'). Imamo dvije mogućnosti: skup S je ili linearno nezavisan ili linearno zavisan. Ako je S linearno nezavisan onda je S baza od V. Ako je S linearno zavisan, onda postoji $x \in S$ takav da je $x \in [S \setminus \{x\}]$. Prema lemi 1.1 tada za skup $S_1 = S \setminus \{x\}$ vrijedi $[S_1] = [S] = V$. Sada ponovimo isti postupak sa skupom S_1. Kako je skup S konačan, nakon izuzimanja konačno mnogo vektora iz S dobit ćemo linearno nezavisan podskup od S koji razapinje prostor V, tj. doći ćemo do baze od V sadržane u S.

Iz dokazane tvrdnje (e') odmah slijedi tvrdnja (a).

Dokažimo sada sljedeću pomoćnu tvrdnju:

Lema 1.2 *Ako je S konačan podskup vektorskog prostora V i ako je T linearno nezavisan podskup od $[S]$ onda je skup T konačan i $|T| \leq |S|$.*

Dokaz leme 1.2. Tu ćemo tvrdnju dokazati matematičkom indukcijom u odnosu na broj $|S|$ elemenata skupa S.

Baza indukcije: Pretpostavimo da je $|S| = 1$, tj. $S = \{x\}$. Neka je T linearno nezavisan podskup od $[S]$. Treba dokazati da skup T nema više od jednog elementa. Pretpostavimo suprotno ($|T| \geq 2$) i neka su y i z međusobno različiti elementi od T. Kako je skup T sadržan u potprostoru

$[S] = [\{x\}] = \{\lambda x; \lambda \in K\}$, postoje međusobno različiti $\lambda, \mu \in K$ takvi da je $y = \lambda x$ i $z = \mu x$. Kako su λ i μ međusobno različiti, bar jedan od njih je različit od nule. No tada imamo netrivijalnu linearnu kombinaciju vektora y i z koja je jednaka nuli: $\lambda z - \mu y = 0$. Dakle, skup $\{y, z\} \subseteq T$ je linearno zavisan, pa je i T linearno zavisan, suprotno pretpostavci. Dakle, nije moguće da T ima više od jednog elementa.

Korak indukcije: Pretpostavimo da je tvrdnja dokazana ako je $|S| = n - 1$. Neka je $|S| = n$ ($S = \{x_1, x_2, \ldots, x_n\}$) i neka je T linearno nezavisan podskup od $[S]$. Treba dokazati da T nema više od n elemenata. Pretpostavimo suprotno i neka su $y_1, y_2, \ldots, y_n, y_{n+1}$ međusobno različiti elementi od T. Kako je T sadržan u $[S] = [\{x_1, x_2, \ldots, x_n\}]$ svaki od tih $n + 1$ vektora je linearna kombinacija vektora $x_1, x_2, \ldots, x_n$:

$$\begin{aligned}
y_1 &= \alpha_{1,1}x_1 + \alpha_{1,2}x_2 + \ldots + \alpha_{1,n}x_n \\
y_2 &= \alpha_{2,1}x_1 + \alpha_{2,2}x_2 + \ldots + \alpha_{2,n}x_n \\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
y_n &= \alpha_{n,1}x_1 + \alpha_{n,2}x_2 + \ldots + \alpha_{n,n}x_n \\
y_{n+1} &= \alpha_{n+1,1}x_1 + \alpha_{n+1,2}x_2 + \ldots + \alpha_{n+1,n}x_n
\end{aligned}$$

Kako je skup T linearno nezavisan, svi su njegovi elementi različiti od nule. Posebno je $y_{n+1} \neq 0$. No tada je barem jedan od koeficijenata $\alpha_{n+1,1}, \alpha_{n+1,2}, \ldots, \alpha_{n+1,n}$ različit od nule. Uz eventualnu novu numeraciju elemenata od S možemo pretpostaviti da je $\alpha_{n+1,n} \neq 0$. No tada iz posljednje od gornjih jednakosti slijedi:

$$x_n = \frac{1}{\alpha_{n+1,n}}y_{n+1} - \frac{\alpha_{n+1,1}}{\alpha_{n+1,n}}x_1 - \frac{\alpha_{n+1,2}}{\alpha_{n+1,n}}x_2 - \ldots - \frac{\alpha_{n+1,n-1}}{\alpha_{n+1,n}}x_{n-1}$$

Uvrstimo ovo u prvih n gornjih jednakosti. Uz oznake $z_k = y_k - \frac{\alpha_{k,n}}{\alpha_{n+1,n}}y_{n+1}$ za $k = 1, 2, \ldots, n$ i $\beta_{i,j} = \alpha_{i,j} - \frac{\alpha_{i,n}\alpha_{n+1,j}}{\alpha_{n+1,n}}$ za $i = 1, 2, \ldots, n$ i $j = 1, 2, \ldots, n - 1$ nakon sređivanja dobivamo:

$$\begin{aligned}
z_1 &= \beta_{1,1}x_1 + \beta_{1,2}x_2 + \ldots + \beta_{1,n-1}x_{n-1} \\
z_2 &= \beta_{2,1}x_1 + \beta_{2,2}x_2 + \ldots + \beta_{2,n-1}x_{n-1} \\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
z_n &= \beta_{n,1}x_1 + \beta_{n,2}x_2 + \ldots + \beta_{n,n-1}x_{n-1}
\end{aligned}$$

Iz gornjih jednakosti slijedi da je $\{z_1, z_2, \ldots, z_n\}$ podskup potprostora razapetog skupom $S^* = \{x_1, x_2, \ldots, x_{n-1}\}$ pa je po pretpostavci indukcije taj $n-$člani skup linearno zavisan. Dakle, postoje $\lambda_1, \lambda_2, \ldots, \lambda_n \in K$, koji nisu svi jednaki nuli, takvi da je

$$\lambda_1 z_1 + \lambda_2 z_2 + \ldots + \lambda_n z_n = 0.$$

Uvrstimo li $z_k = y_k - \frac{\alpha_{k,n}}{\alpha_{n+1,n}}y_{n+1}$ za $k = 1, 2, \ldots, n$ nakon sređivanja dobivamo:

$$\lambda_1 y_1 + \lambda_2 y_2 + \ldots + \lambda_n y_n + \lambda y_{n+1} = 0,$$

uz oznaku $\lambda = -\frac{\lambda_1\alpha_{1,n}}{\alpha_{n+1,n}} - \frac{\lambda_2\alpha_{2,n}}{\alpha_{n+1,n}} - \ldots - \frac{\lambda_n\alpha_{n,n}}{\alpha_{n+1,n}}$. Budući da $\lambda_1, \lambda_2, \ldots, \lambda_n$ nisu svi jednaki nuli, radi se o netrivijalnoj linearnoj kombinaciji. Prema tome, skup $\{y_1, y_2, \ldots, y_{n+1}\}$ je linearno zavisan, što je u suprotnosti s pretpostavkom da je skup T linearno nezavisan. Prema tome, nije moguće da skup T ima više od n elemenata, odnosno dokazali smo da je $|T| \leq n$.

Time je lema 1.2 u potpunosti dokazana.

Dokažimo sada tvrdnju (b). Ako je B_1 konačna baza od V i B_2 bilo koja baza od V, tada je B_2 linearno nezavisan podskup od $V = [B_1]$, pa prema lemi 1.2 slijedi da je skup B_2 konačan i $|B_2| \leq |B_1|$. Time je tvrdnja (b) dokazana, a slijedi i tvrdnja (c) jer se analogno zamjenivši uloge B_2 i B_1 dobiva da je $|B_1| \leq |B_2|$.

Da bismo dokazali tvrdnju (d) dokažimo najprije sljedeću lemu:

Lema 1.3 *Neka je S linearno nezavisan podskup vektorskog prostora V. Pretpostavimo da je $x \in V \setminus [S]$. Tada je skup $S \cup \{x\}$ linearno nezavisan.*

Dokaz leme 1.3. Neka su $x_1, x_2, \ldots, x_n$ međusobno različiti elementi od S i pretpostavimo da su skalari $\lambda, \lambda_1, \lambda_2, \ldots, \lambda_n \in K$ takvi da je

$$\lambda x + \lambda_1 x_1 + \lambda_2 x_2 + \ldots + \lambda_n x_n = 0.$$

Treba dokazati da su svi koeficijenti $\lambda, \lambda_1, \lambda_2, \ldots, \lambda_n$ jednaki nuli. Kada bi λ bilo različito od nule iz gornje bi jednakosti slijedilo da se x može napisati kao linearna kombinacija vektora $x_1, x_2, \ldots, x_n$ a odatle da je $x \in [S]$, suprotno pretpostavci $x \in V \setminus [S]$. Prema tome je $\lambda = 0$. Sada iz gornje jednakosti izlazi da je $\lambda_1 x_1 + \lambda_2 x_2 + \ldots + \lambda_n x_n = 0$. Budući da je po pretpostavci skup S linearno nezavisan, slijedi $\lambda_1 = \lambda_2 = \ldots = \lambda_n = 0$. Time je lema 1.3 dokazana.

Prijeđimo sada na dokaz tvrdnje (d). Označimo sa n dimenziju vektorskog prostora V. Neka je S linearno nezavisan podskup od V. Prema lemi 1.2 imamo $|S| = k \leq n$. Sada imamo dvije mogućnosti: ili je $[S] = V$ ili je $[S] \neq V$. Ako je $[S] = V$, onda je S baza od V. Uzmimo da je $[S] \neq V$. Neka je $x \in V \setminus [S]$. Prema lemi 1.3 skup $S^* = S \cup \{x\}$ je linearno nezavisan, pa je prema lemi 1.2 $|S^*| = k + 1 \leq n$. Isto razmatranje sada možemo ponoviti za skup S^* umjesto skupa S. Razmatranje se ponavlja sve dok ne dođemo do baze od V, a to će se sigurno dogoditi jer svakim korakom dolazimo do linearno nezavisnog skupa čiji se broj elemenata povećao za jedan. Prema lemi 1.2 tih koraka može biti najviše $n - k$.

Dokažimo sada tvrdnju (e). Neka S podskup od V koji ga razapinje: $[S] = V$. Neka je x_1 vektor iz S različit od nule. Tada je skup $S_1 = \{x_1\}$ linearno nezavisan. Ako je $[S_1] = V$, onda je S_1 baza od V. Ako je $[S_1] \neq V$, onda skup S nije sadržan u $[S_1]$, pa možemo izabrati $x_2 \in S \setminus [S_1]$. Prema lemi 1.3 skup $S_2 = \{x_1, x_2\}$ je linearno nezavisan. Razmatranje ponavljamo sa skupom S_2 umjesto skupa S_1. Budući da linearno nezavisan skup prema lemi 1.2 ne može imati više od $n = \dim V$ elemenata, nakon konačno mnogo koraka doći ćemo do baze od V koja je sadržana u S.

Dokažimo sada tvrdnju (f). Neka je S linearno nezavisan skup koji ima $n = \dim V$ elemenata. Treba dokazati da je S baza od V, tj. da je $[S] = V$. Pretpostavimo suprotno, tj. $[S] \neq V$. No tada je za $x \in V \setminus [S]$ prema lemi 1.3 skup $S \cup \{x\}$ linearno nezavisan i ima $n + 1 > \dim V$ elemenata, a to je nemoguće zbog leme 1.2. Stoga je pretpostavka $[S] \neq V$ pogrešna, tj vrijedi $[S] = V$.

Napokon, dokažimo još tvrdnju (g). Neka je W potprostor od V i neka je $n = \dim V$. Ako je $W = \{0\}$, onda je $\dim W = 0$. Pretpostavimo da je $W \neq 0$. Neka je $x_1 \in W, x_1 \neq 0$. Tada je skup $S_1 = \{x_1\}$ linearno nezavisan. Ako je $[S_1] = W$, S_1 je baza od W. Ako je $[S_1] \neq W$, uzmimo $x_2 \in W \setminus [S_1]$. Prema lemi 1.3 $S_2 = \{x_1, x_2\}$ je linearno nezavisan. Ako je $[S_2] = W$, S_2 je baza do W. Ako je $S_2 \neq W$, uzmimo $x_3 \in W \setminus [S_2]$. Prema lemi 1.3 $S_3 = \{x_1, x_2 x_3\}$ je linearno nezavisan. Ovaj postupak nastavljamo sve dok ne dođemo do konačne baze od W. To će se sigurno dogoditi jer u svakom koraku dobivamo linearno nezavisan podskup od $W \subseteq V$, koji po lemi 1.2 ne može imati više od $\dim V$ elemenata. Odavde slijedi da je potprostor W konačnodimenzionalan i da je $\dim W \leq \dim V$. Ako je $\dim W = \dim V$, onda baza od W ima $\dim V$ elemenata, pa je po tvrdnji (e) to ujedno baza od V. No tada je očito $W = V$.

Prema propoziciji 1.1 presjek bilo koliko potprostora je opet potprostor. S unijom je drugačija situacija. Lako se može vidjeti da je već za dva potprostora U i W njihova unija $U \cup W$ potprostor ako i samo ako je ili $U \subseteq W$ (i tada je $U \cup W = W$) ili $W \subseteq U$ (i tada je $U \cup W = U$). Međutim, za dva potprostora U i W možemo promatrati najmanji potprostor X koji sadrži oba ta potprostora, tj. koji sadrži $U \cup W, X = [U \cup W]$.

Propozicija 1.3 $[U \cup W] = \{u + w; u \in U, w \in W\}$.

Dokaz: Ako su $u \in U$ i $w \in W$ onda su oba vektora sadržana u uniji $U \cup W$ dakle i u $[U \cup W]$. Kako je $[U \cup W]$ potprostor slijedi $u + w \in [U \cup W]$. Time je dokazana inkluzija

$$[U \cup W] \supseteq \{u + w; u \in U, w \in W\}.$$

Dokažimo i obratnu inkluziju. Neka je $x \in [U \cup W]$. Tada je prema propoziciji 1.2 x linearna kombinacija vektora iz $U \cup W$. To znači da možemo naći vektore $x_1, \ldots, x_n \in U$, $y_1, \ldots, y_m \in W$ i skalare $\lambda_1, \ldots, \lambda_n, \mu_1, \ldots, \mu_m \in K$, takve da je

$$x = \lambda_1 x_1 + \lambda_2 x_2 + \ldots + \lambda_n x_n + \mu_1 y_1 + \mu_2 y_2 + \ldots + \mu_m y_m.$$

Stavimo li $u = \lambda_1 x_1 + \lambda_2 x_2 + \ldots + \lambda_n x_n$ i $w = \mu_1 y_1 + \mu_2 y_2 + \ldots + \mu_m y_m$ imamo $u \in U, w \in W$ i $x = u + w$. Prema tome vrijedi i obrnuta inkluzija

$$[U \cup W] \subseteq \{u + w; u \in U, w \in W\},$$

odnosno vrijedi jednakost $[U \cup W] = \{u + w; u \in U, w \in W\}$.

Zbog toga se $[U \cup W]$ zove **suma potprostora** U i W i označava $U + W$. Konstrukciju možemo napraviti i za više potprostora $W_1, W_2, \ldots, W_n$:

$$W_1 + W_2 + \ldots + W_n = [W_1 \cup W_2 \cup \ldots \cup W_n] = \{w_1 + w_2 + \ldots + w_n;\ w_1 \in W_1, w_2 \in W_2, \ldots, w_n \in W_n\},$$

pa i za bilo koji skup Σ potprostora od V :

$$\begin{aligned} \textstyle\sum_{W \in \Sigma} W &= \Big[\textstyle\bigcup_{W \in \Sigma} W\Big] = \{v \in V; \exists n \in \mathbb{N}, \exists W_1, W_2, \ldots, W_n \in \Sigma, \\ &\quad \exists w_1 \in W_1, w_2 \in W_2, \ldots, w_n \in W_n, \text{td.}\, v = w_1 + w_2 + \ldots + w_n\}. \end{aligned}$$

Propozicija 1.4 *Ako su U i W konačnodimenzionalni potprostori vektorskog prostora V, onda je i potprostor $U + W$ konačnodimenzionalan i vrijedi:*

$$\dim(U + W) = \dim U + \dim W - \dim(U \cap W).$$

Dokaz: Neka je $\dim U = p$, $\dim W = q$ i $\dim U \cap W = k$. Zbog tvrdnje (g) teorema 1.1 je $k \leq p$ i $k \leq q$. Konstruirat ćemo sada bazu od $U + W$ koja ima $p + q - k$ elemenata i time će propozicija biti dokazana, jer je dimenzija broj elemenata baze.

Neka je $\{x_1, x_2, \ldots, x_k\}$ baza od $U \cap W$. Kako je $U \cap W$ potprostor od U, prema tvrdnji (d) teorema 1.1 ta je baza od $U \cap W$ sadržana u nekoj bazi od U, tj. možemo naći bazu od U oblika $\{x_1, x_2, \ldots, x_k, y_{k+1}, y_{k+2}, \ldots, y_p\}$. Analogno možemo naći bazu od W oblika $\{x_1, x_2, \ldots, x_k, z_{k+1}, z_{k+2}, \ldots, z_q\}$. Dokazat ćemo sada da je

$$B = \{x_1, x_2, \ldots, x_k, y_{k+1}, y_{k+2}, \ldots, y_p, z_{k+1}, z_{k+2}, \ldots, z_q\}$$

baza od $U + W$.

Dokažimo najprije da je skup B linearno nezavisan. Neka su $\alpha_1, \ldots, \alpha_k, \beta_{k+1}, \ldots, \beta_p, \gamma_{k+1}, \ldots, \gamma_q$ skalari iz K takvi da je

$$\alpha_1 x_1 + \ldots + \alpha_k x_k + \beta_{k+1} y_{k+1} + \ldots + \beta_p y_p + \gamma_{k+1} z_{k+1} + \ldots + \gamma_q z_q = 0.$$

Treba dokazati da su svi skalari $\alpha_1, \ldots, \alpha_k, \beta_{k+1}, \ldots, \beta_p, \gamma_{k+1}, \ldots, \gamma_q$ jednaki nuli. Gornja jednakost se može zapisati ovako:

$$\alpha_1 x_1 + \ldots + \alpha_k x_k + \beta_{k+1} y_{k+1} + \ldots + \beta_p y_p = -\gamma_{k+1} z_{k+1} - \ldots - \gamma_q z_q.$$

Označimo li taj vektor sa x, lijeva strana pokazuje da je $x \in U$, a desna da je $x \in W$. Stoga je $x \in U \cap W$, a kako je $\{x_1, x_2, \ldots, x_k\}$ baza od $U \cap W$, možemo naći skalare $\lambda_1, \lambda_2, \ldots, \lambda_k \in K$ takve da je

$$x = \lambda_1 x_1 + \ldots + \lambda_k x_k.$$

Kako je vektor x jednak desnoj strani prethodne jednakosti, imamo

$$\lambda_1 x_1 + \ldots + \lambda_k x_k = -\gamma_{k+1} z_{k+1} - \ldots - \gamma_q z_q,$$

odnosno

$$\lambda_1 x_1 + \ldots + \lambda_k x_k + \gamma_{k+1} z_{k+1} + \ldots + \gamma_q z_q = 0.$$

Budući da je $\{x_1, x_2, \ldots, x_k, z_{k+1}, z_{k+2}, \ldots, z_q\}$ baza od W, taj je skup linearno nezavisan, pa iz gornje jednakosti slijedi da su svi koeficijenti jednaki nuli, a posebno $\gamma_{k+1} = \ldots = \gamma_q = 0$. Tada je $x = 0$, pa slijedi i

$$\alpha_1 x_1 + \ldots + \alpha_k x_k + \beta_{k+1} y_{k+1} + \ldots + \beta_p y_p = 0.$$

Budući da je $\{x_1, x_2, \ldots, x_k, y_{k+1}, y_{k+2}, \ldots, y_p\}$ baza od U, taj je skup linearno nezavisan, pa iz gornje jednakosti slijedi $\alpha_1 = \ldots = \alpha_k = \beta_{k+1} = \ldots = \beta_p = 0$. Dakle, svi koeficijenti $\alpha_1, \ldots, \alpha_k, \beta_{k+1}, \ldots, \beta_p, \gamma_{k+1}, \ldots, \gamma_q$ jednaki su nuli, pa smo time dokazali da je skup B linearno nezavisan.

Treba još dokazati da skup B razapinje potprostor $U + W$. Neka je x bilo koji vektor iz $U + W$. Tada je prema propoziciji 1.3 $x = u + w$ za neke $u \in U$ i $w \in W$. $\{x_1, \ldots, x_k, y_{k+1}, \ldots, y_p\}$ je baza od U i $\{x_1, \ldots, x_k, z_{k+1}, \ldots, z_q\}$ je baza od W, pa možemo naći skalare $\alpha_1, \alpha_2, \ldots, \alpha_p, \beta_1, \beta_2, \ldots, \beta_q$ iz K takve da je

$$u = \alpha_1 x_1 + \ldots + \alpha_k x_k + \alpha_{k+1} y_{k+1} + \ldots + \alpha_p y_p \quad \text{i} \quad w = \beta_1 x_1 + \ldots + \beta_k x_k + \beta_{k+1} z_{k+1} + \ldots + \beta_q x_q.$$

Slijedi

$$x = u + w = (\alpha_1 + \beta_1) x_1 + \ldots + (\alpha_k + \beta_k) x_k + \alpha_{k+1} y_{k+1} + \ldots + \alpha_p y_p + \beta_{k+1} z_{k+1} + \ldots + \beta_q z_q.$$

Posljednja jednakost pokazuje da je bilo bilo koji vektor $x \in U + W$ linearna kombinacija vektora iz B, dakle B razapinje potprostor $U + W$.

Napomenimo da za dimenziju sume više potprostora nemamo tako jednostavnu formulu. Ako su X, Y i Z potprostori od V onda je moguće samo dokazati nejednakost

$$\dim(X+Y+Z) \leq \dim X + \dim Y + \dim Z - \dim(X \cap Y) - \dim(X \cap Z) - \dim(Y \cap Z) + \dim(X \cap Y \cap Z).$$

Slične nejednakosti vrijede i u slučaju više konačnodimenzionalnih potprostora.

Prema propoziciji 1.4 dimenzija sume dvaju konačnodimenzionalnih potprostora je najveća i jednaka $\dim U + \dim W$ ako i samo ako je $U \cap W = \{0\}$. U općem slučaju (a ne samo ako su potprostori konačnodimenzionalni), ako je $U \cap W = \{0\}$ kažemo da je **suma** $U + W$ **direktna** i umjesto $U + W$ pišemo $U \dotplus W$. Suma je direktna ako i samo ako za svaki $v \in U + W$ postoje jedinstveni $u \in U$ i $w \in W$ takvi da je $v = u + w$, ili ekvivalentno, ako za $u \in U$ i $w \in W$ vrijedi $u + w = 0$ ako i samo ako je $u = 0$ i $w = 0$.

Općenitije, za potprostore $W_1, W_2, \ldots, W_n$ kažemo da tvore direktnu sumu, koju onda označavamo sa $W_1 \dotplus W_2 \dotplus \ldots \dotplus W_n$, ako za svaki vektor v iz potprostora $W_1 + W_2 + \ldots + W_n$ postoje jedinstveni vektori $w_1 \in W_1, w_2 \in W_2, \ldots, w_n \in W_n$, takvi da je $v = w_1 + w_2 + \ldots + w_n$, ili ekvivalentno, ako za bilo koje vektore $w_1 \in W_1, w_2 \in W_2, \ldots, w_n \in W_n$ vrijedi $w_1 + w_2 + \ldots + w_n = 0$

ako i samo ako je $w_1 = w_2 = \ldots = w_n = 0$. Ako su $B_1, B_2, \ldots, B_n$ baze redom od $W_1, W_2, \ldots, W_n$, onda je njihova unija $B_1 \cup B_2 \cup \ldots \cup B_n$ baza direktne sume $W_1 \dot{+} W_2 \dot{+} \ldots \dot{+} W_n$. Prema tome je

$$\dim(W_1 \dot{+} W_2 \dot{+} \ldots \dot{+} W_n) = \dim W_1 + \dim W_2 + \ldots + \dim W_n.$$

Ako je V vektorski prostor i X njegov potprostor, **direktni komplement** od X u V je svaki potprostor Y takav da je $V = X \dot{+} Y$.

Propozicija 1.5 *Neka je V konačnodimenzionalan vektorski prostor i X njegov potprostor. Postoji direktni komplement od X u V.*

Dokaz: Neka je $\{x_1, x_2, \ldots, x_k\}$ baza od X. Prema tvrdnji (d) teorema 1.1 postoje vektori $x_{k+1}, \ldots, x_n$ takvi da je $\{x_1, x_2, \ldots, x_k, x_{k+1}, \ldots, x_n\}$ baza od V. Stavimo $Y = [\{x_{k+1}, \ldots, x_n\}]$. Tada je Y potprostor od V i $\{x_{k+1}, \ldots, x_n\}$ je njegova baza. Svaki vektor v prostora V može se prikazati kao linearna kombinacija vektora baze od V :

$$v = \alpha_1 x_1 + \ldots + \alpha_n x_n.$$

Stavimo sada

$$x = \alpha_1 x_1 + \ldots + \alpha_k x_k \qquad \text{i} \qquad y = \alpha_{k+1} x_{k+1} + \ldots + \alpha_n x_n.$$

Tada je $x \in X$, $y \in Y$ i $v = x + y$. Prema tome je $V = X + Y$. Nadalje, za $v \in X \cap Y$ postoje $\lambda_1, \ldots, \lambda_k \in K$ i $\lambda_{k+1}, \ldots, \lambda_n \in K$ takvi da je

$$v = \lambda_1 x_1 + \ldots + \lambda_k x_k \qquad \text{i} \qquad v = \lambda_{k+1} x_{k+1} + \ldots + \lambda_n x_n.$$

Odatle je $\lambda_1 x_1 + \ldots + \lambda_k x_k - \lambda_{k+1} x_{k+1} - \ldots - \lambda_n x_n = 0$. Zbog linearne nezavisnosti baze $\{x_1, x_2, \ldots, x_k, x_{k+1}, \ldots, x_n\}$ slijedi $\lambda_1 = \lambda_2 = \ldots = \lambda_k = \lambda_{k+1} = \ldots = \lambda_n = 0$. Zaključujemo da je $v = 0$, a to pokazuje da je $X \cap Y = \{0\}$, odnosno $V = X \dot{+} Y$. Prema tome, Y je direktni komplement od X u V.

Razmatrat ćemo sada još jednu važnu konstrukciju u teoriji vektorskih prostora, a to je **kvocijentni prostor**. Neka je V vektorski prostor i W potprostor. U skupu V definiramo relaciju $\sim$ na sljedeći način:

$$x \sim y \Leftrightarrow x - y \in W.$$

Dokažimo najprije da je $\sim$ relacija ekvivalencije. Za bilo koji $x \in V$ vrijedi $x - x = 0 \in W$, jer nulvektor je sadržan u svakom potprostoru. Prema tome je $x \sim x$. Nadalje, ako je $x \sim y$, tj. $x - y \in W$, onda je $y - x = -(x - y) \in W$, dakle vrijedi i $y \sim x$. Nadalje, iz $x \sim y$ i $y \sim z$ slijedi $x - y \in W$ i $y - z \in W$, dakle i $x - z = (x - y) + (y - z) \in W$. Prema tome je $x \sim z$. Time je dokazano da je $\sim$ relacija ekvivalencije.

Skup svih klasa ekvivalencije u skupu V u odnosu na tu relaciju ekvivalencije označavat ćemo sa V/W. Opisat ćemo sada pobliže svaku pojedinu klasu ekvivalencije, tj. svaki element skupa V/W. Neka je $x \in V$ i neka je $[x]$ njegova klasa ekvivalencije, tj. $[x] = \{y \in V; y \sim x\}$. Ako je $y \in [x]$ tada je $w = y - x \in W$ i $y = x + w$. Dakle imamo inkluziju

$$[x] \subseteq \{x + w; w \in W\}.$$

Dokažimo i obrnutu inkluziju. Ako je $w \in W$ i $y = x + w$, tada je $y - x = w \in W$, dakle $y \sim x$ ili $y \in [x]$. Time je dokazana i obrnuta inkluzija

$$[x] \supseteq \{x + w; w \in W\},$$

tj. imamo jednakost $[x] = \{x + w; w \in W\}$. Stoga ćemo klasu ekvivalencije $[x]$ koja sadrži vektor x označavati sa $x + W$:

$$[x] = x + W = \{x + w; w \in W\}.$$

U skup V/W uvest ćemo sada operaciju zbrajanja i množenja skalarima iz K :

$$(x + W) + (y + W) = (x + y) + W, \qquad \lambda(x + W) = (\lambda x) + W.$$

Dokažimo da su ove operacije dobro definirane, tj. da rezultati ne ovise o izboru predstavnika klasa. Neka su $x \sim x'$ i $y \sim y'$, tj. $x + W = x' + W$ i $y + W = y' + W$. To znači da vrijedi $x - x' \in W$ i $y - y' \in W$. Tada je

$$(x + y) - (x' + y') = (x - x') + (y - y') \in W,$$

dakle je $(x + y) \sim (x' + y')$, odnosno $(x + y) + W = (x' + y') + W$. Time smo dokazali da je zbrajanje u V/W dobro definirano. Sasvim analogno dokazuje se da je i množenje skalarom dobro definirano, tj. da je $(\lambda x) + W = (\lambda x') + W$.

S tako definiranim operacijama skup V/W postaje vektorski prostor nad poljem K. Doista, iz komutativnosti i asocijativnosti zbrajanja vektora u V neposredno slijedi komutativnost i asocijativnost zbrajanja elemenata skupa V/W :

$$(x + W) + (y + W) = (x + y) + W = (y + x) + W = (y + W) + (x + W),$$

$$((x+W)+(y+W))+(z+W) = ((x+y)+z)+W = (x+(y+z))+W = (x+W)+((y+W)+(z+W)).$$

Nadalje, element $0 + W = W$ je neutralan u V/W u odnosu na zbrajanje, a element $(-x) + W$ je suprotan elementu $x + W$ u odnosu na zbrajanje u V/W :

$$(0+W)+(x+W) = (0+x)+W = x+W, \qquad (x+W)+((-x)+W) = (x-x)+W = 0+W.$$

Prema tome, V/W je u odnosu na definirano zbrajanje komutativna grupa. Neposredno se provjerava i odnos množenja skalarom prema zbrajanju u V/W :

$$\lambda((x + W) + (y + W)) = \lambda((x + y) + W) = \lambda(x + y) + W =$$

$$= (\lambda x + \lambda y) + W = (\lambda x + W) + (\lambda y + W) = \lambda(x + W) + \lambda(y + W);$$

$$(\lambda+\mu)(x+W) = (\lambda+\mu)x+W = (\lambda x+\mu x)+W = (\lambda x+W)+(\mu x+W) = \lambda(x+W)+\mu(x+W);$$

$$(\lambda\mu)(x + W) = (\lambda\mu)x + W = \lambda(\mu x + W) = \lambda(\mu(x + W)).$$

Time je dokazano da je V/W s definiranim operacijama vektorski prostor nad poljem K. V/W se zove **kvocijentni prostor prostora** V **po potprostoru** W.

Propozicija 1.6 *Ako je V konačnodimenzionalan vektorski prostor i W njegov potprostor, tada je i kvocijentni prostor V/W konačnodimenzionalan i vrijedi:*

$$\dim V/W = \dim V - \dim W.$$

Dokaz: Neka je $k = \dim W$ i $n = \dim V$ (naravno, $k \leq n$). Izaberimo bazu $\{x_1, x_2, \ldots, x_k\}$ od W. Prema tvrdnji (d) teorema 1.1 ona se može dopuniti do baze $\{x_1, x_2, \ldots, x_k, x_{k+1}, \ldots, x_n\}$ od V. Dokazat ćemo sada da je $\{x_{k+1} + W, \ldots, x_n + W\}$ baza od V/W i time će propozicija biti dokazana jer je broj tih vektora u V/W jednak $n - k$.

Dokažimo najprije da je taj skup vektora u V/W linearno nezavisan. Neka su $\lambda_{k+1}, \ldots, \lambda_n \in K$ takvi da je

$$0 = \lambda_{k+1}(x_{k+1} + W) + \ldots + \lambda_n(x_n + W) = (\lambda_{k+1}x_{k+1} + \ldots + \lambda_n x_n) + W.$$

Dakle $(\lambda_{k+1}x_{k+1} + \ldots + \lambda_n x_n) \sim 0$ ili $(\lambda_{k+1}x_{k+1} + \ldots + \lambda_n x_n) \in W$. Taj se vektor može prikazati kao linearna kombinacija vektora baze $\{x_1, x_2, \ldots, x_k\}$ potprostora W, tj. postoje $\lambda_1, \ldots, \lambda_k \in K$ takvi da je

$$\lambda_{k+1}x_{k+1} + \ldots + \lambda_n x_n = \lambda_1 x_1 + \ldots + \lambda_k x_k.$$

Odatle slijedi

$$-\lambda_1 x_1 - \ldots - \lambda_k x_k + \lambda_{k+1}x_{k+1} + \ldots + \lambda_n x_n = 0.$$

Međutim, skup vektora $\{x_1, x_2, \ldots, x_k, x_{k+1}, \ldots, x_n\}$ je baza od V, dakle taj je skup linearno nezavisan. Iz gornje jednakosti slijedi da su nužno svi koeficijenti jednaki nuli. Posebno, $\lambda_{k+1} = \lambda_{k+2} = \ldots = \lambda_n = 0$. To pokazuje da je skup vektora $\{x_{k+1}+W, \ldots, x_n+W\}$ u vektorskom prostoru V/W linearno nezavisan.

Treba još dokazati da skup vektora $\{x_{k+1}+W, \ldots, x_n+W\}$ razapinje cijeli prostor V/W. Neka je $x \in V$ proizvoljan (tj. $x + W \in V/W$ je proizvoljan). Tada je x linearna kombinacija vektora baze $\{x_1, \ldots, x_n\}$ prostora V, tj. postoje $\lambda_1, \ldots, \lambda_n \in K$ takvi da je

$$x = \lambda_1 x_1 + \ldots + \lambda_k x_k + \lambda_{k+1}x_{k+1} + \ldots + \lambda_n x_n.$$

Stavimo $w = \lambda_1 x_1 + \ldots + \lambda_k x_k$. Tada je $w \in W$, pa je

$$x + W = (x - w) + W = (\lambda_{k+1}x_{k+1} + \ldots + \lambda_n x_n) + W = \lambda_{k+1}(x_{k+1} + W) + \ldots + \lambda_n(x_n + W).$$

Time je propozicija u potpunosti dokazana.

Za vektorski prostor V i njegov potprostor W preslikavanje $\pi : V \to V/W$, koje svakom vektoru $x \in V$ pridružuje njegovu klasu ekvivalencije $[x] = x + W$, zove se **kvocijentno preslikavanje**:

$$\pi(x) = [x] = x + w, \quad x \in V.$$

Primijetimo da vrijedi:

$$\pi(x + y) = \pi(x) + \pi(y), \quad x, y \in V; \qquad \pi(\lambda x) = \lambda\pi(x), \quad \lambda \in K, \ x \in V.$$

2 Linearni operatori

Ako su V i W vektorski prostori, svako preslikavanje $A : V \to W$ zove se **operator**. Operator A je **aditivan** ako vrijedi:

$$A(x+y) = A(x) + A(y), \qquad \forall x, y \in V.$$

Ako su V i W vektorski prostori nad istim poljem K, operator A je **homogen** ako vrijedi:

$$A(\lambda x) = \lambda A(x), \qquad \forall \lambda \in K,\ \forall x \in V.$$

Operator A je **linearan**, ako je aditivan i homogen, tj. ako vrijedi:

$$A(\lambda x + \mu y) = \lambda A(x) + \mu A(y), \qquad \forall \lambda, \mu \in K,\ \forall x, y \in V.$$

Ako je A linearan operator, obično se umjesto $A(x)$ piše Ax.

Za vektorske prostore V i W nad istim poljem K sa $L(V,W)$ ćemo označavati skup svih linearnih operatora $A : V \to W$. U taj skup uvodimo operaciju zbrajanja: ako su $A, B \in L(V,W)$ sa $A+B$ označavamo operator sa V u W definiran relacijom

$$(A+B)(v) = Av + Bv, \qquad v \in V.$$

Nadalje, uvodimo i operaciju množenja elemenata od $L(V,W)$ skalarima iz polja K: ako je $A \in L(V,W)$ i $\lambda \in K$ sa λA označavamo operator sa V u W definiran relacijom

$$(\lambda A)(v) = \lambda(Av),\ \ v \in V.$$

Lako se vidi da su tako definirani operatori $A+B$ i λA linearni, dakle elementi od $L(V,W)$. Također, jednostavno se dokazuje da uz tako definirane operacije skup $L(V,W)$ svih linearnih operatora sa V u W postaje vektorski prostor nad poljem K.

Ako su V, W i U tri vektorska prostora i ako su $A \in L(V,W)$ i $B \in L(W,U)$ onda definiramo $BA : V \to U$ kao kompoziciju funkcija: $(BA)(V) = B(Av)$, $v \in V$. Tako definiran operator je linearan, $BA \in L(V,U)$, i zove se **produkt operatora** B i A. Tako definiran produkt ima svojstvo asocijativnosti: ako su $A \in L(V,W)$, $B \in L(W,U)$ i $C \in L(U,X)$ onda je $(CB)A = C(BA)$.

Pri svakoj definiciji postavlja se pitanje smislenosti te definicije, a prije svega nije li skup definiranih objekata prazan. Egzistenciju mnoštva linearnih operatora u slučaju konačnodimenzionalne domene garantira sljedeća propozicija:

Propozicija 2.1 *Neka su V i W vektorski prostori nad poljem K i pretpostavimo da je V konačnodimenzionalan. Neka je $\{e_1, e_2, \ldots, e_n\}$ baza od V i neka su $w_1, w_2, \ldots, w_n$ proizvoljni vektori iz W. Tada postoji jedinstven $A \in L(V,W)$ takav da vrijedi*

$$Ae_j = w_j \ \ \textit{za}\ \ j = 1, 2, \ldots, n.$$

Dokaz: Egzistencija: Svaki vektor $x \in V$ na jedinstven način može se prikazati kao linearna kombinacija vektora baze:

$$x = \alpha_1 e_1 + \alpha_2 e_2 + \ldots + \alpha_n e_n.$$

Za taj vektor x stavimo

$$A(x) = \alpha_1 w_1 + \alpha_2 w_2 + \ldots + \alpha_n w_n.$$

Tako smo definirali operator $A : V \to W$ za kojeg očito vrijedi $A(e_j) = w_j$ za $j = 1, 2, \ldots, n$. Dokažimo da je taj operator linearan. Neka su $\lambda, \mu \in K$ i neka je pored x zadan još jedan vektor $y \in V$ s prikazom u bazi:

$$y = \beta_1 e_1 + \beta_2 e_2 + \ldots + \beta_n e_n.$$

Tada je

$$A(y) = \beta_1 w_1 + \beta_2 w_2 + \ldots + \beta_n w_n.$$

Nadalje,

$$(\lambda x + \mu y) = (\lambda\alpha_1 + \mu\beta_1)e_1 + (\lambda\alpha_2 + \mu\beta_2)e_2 + \ldots + (\lambda\alpha_n + \mu\beta_n)e_n,$$

pa slijedi

$$A(\lambda x + \mu y) = (\lambda\alpha_1 + \mu\beta_1)w_1 + (\lambda\alpha_2 + \mu\beta_2)w_2 + \ldots + (\lambda\alpha_n + \mu\beta_n)w_n =$$

$$= \lambda(\alpha_1 w_1 + \alpha_2 w_2 + \ldots + \alpha_n w_n) + \mu(\beta_1 w_1 + \beta_2 w_2 + \ldots + \beta_n w_n) = \lambda A(x) + \mu A(y).$$

Time je dokazana egzistencija.

Jedinstvenost: Pretpostavimo da su $A, B \in L(V, W)$ takvi da je $Ae_j = w_j$ i $Be_j = w_j$ za $j = 1, 2, \ldots, n$. Za proizvoljan vektor $x = \alpha_1 e_1 + \alpha_2 e_2 + \ldots + \alpha_n e_n$ iz prostora V zbog linearnosti operatora A i B imamo:

$$Ax = \alpha_1 Ae_1 + \alpha_2 Ae_2 + \ldots + \alpha_n Ae_n = \alpha_1 w_1 + \alpha_2 w_2 + \ldots + \alpha_n w_n = \alpha_1 Be_1 + \alpha_2 Be_2 + \ldots + \alpha_n Be_n = Bx.$$

Dakle, $Ax = Bx$ za svaki vektor $x \in V$, a to znači $A = B$ i jedinstvenost je dokazana.

Propozicija 2.2 *Ako su vektorski prostori V i W konačnodimenzionalni, tada je i prostor $L(V, W)$ konačnodimenzionalan i* $\dim L(V, W) = (\dim V) \cdot (\dim W)$.

Dokaz: Neka je $\{e_1, e_2, \ldots, e_n\}$ baza prostora V i $f = \{f_1, f_2, \ldots, f_m\}$ baza prostora W. Zbog propozicije 2.1 za svaki par indeksa $(i, j)\,(1 \le i \le m,\ 1 \le j \le n)$ postoji jedinstven linearan operator $E_{ij} : V \to W$ takav da vrijedi:

$$E_{ij} e_k = \delta_{jk} f_i, \quad 1 \le k \le n, \quad 1 \le i \le m, \quad 1 \le j \le n.$$

Dokazat ćemo da je $\{E_{ij}; 1 \le i \le m, 1 \le j \le n\}$ baza od $L(V, W)$. Dokažimo prvo linearnu nezavisnost. Neka su $\lambda_{ij} \in K$ takvi da je $\sum_{i,j} \lambda_{ij} E_{ij} = 0$. Primjenom te linearne kombinacije operatora na vektor e_k dobivamo za svaki $k = 1, \ldots, n)$:

$$0 = \sum_{i,j} \lambda_{ij} E_{ij} e_k = \sum_{i,j} \lambda_{ij} \delta_{jk} f_i = \sum_i \lambda_{ik} f_i.$$

Kako je skup vektora $\{f_1, f_2, \ldots, f_m\}$ linearno nezavisan zaključujemo da je $\lambda_{1k} = \lambda_{2k} = \ldots = \lambda_{mk} = 0$ i to vrijedi za svaki $k \in \{1, 2, \ldots, n\}$. Dakle, svi koeficijenti λ_{ij} su jednaki nuli. Dokažimo sada da operatori E_{ij} razapinju prostor $L(V, W)$. Neka je $A \in L(V, W)$. Za svaki $j \in \{1, 2, \ldots, n\}$ Ae_j je vektor iz W pa se može prikazati kao linearna kombinacija vektora iz baze od W :

$$Ae_j = \alpha_{1j} f_1 + \alpha_{2j} f_2 + \ldots + \alpha_{mj} f_m = \sum_i \alpha_{ij} f_i.$$

Imamo:

$$\Big(\sum_{i,k} \alpha_{ik} E_{ik}\Big) e_j = \sum_{i,k} \alpha_{ik} \delta_{kj} f_i = \sum_i \alpha_{ij} f_i = Ae_j.$$

Dakle, linearni operatori A i $\sum_{i,k} \alpha_{ik} E_{ik}$ poprimaju iste vrijednosti na svim vektorima baze od V. Zbog jedinstvenosti u propoziciji 2.1 imamo jednakost $A = \sum_{i,k} \alpha_{ik} E_{ik}$. Time je dokazano da operatori E_{ij} razapinju prostor $L(V, W)$, pa je propozicija u potpunosti dokazana.

Konstrukcija u dokazu da operatori E_{ij} razapinju prostor $L(V, W)$ zapravo znači pridruživanje matrica operatorima. Neka su vektorski prostori V i W konačnodimenzionalni i neka je $A : V \to W$ linearan operator. Neka je $e = \{e_1, e_2, \ldots, e_n\}$ uređena baza prostora V i $f = \{f_1, f_2, \ldots, f_m\}$ uređena baza prostora W. $Ae_1, Ae_2, \ldots, Ae_n$ su vektori prostora W pa se svaki od njih može napisati kao linearna kombinacija vektora iz baze f. Drugim riječima, postoje skalari $\alpha_{ij} \in K$ $(1 \leq i \leq m,\ 1 \leq j \leq n)$ takvi da vrijedi:

$$
\begin{array}{l}
Ae_1 = \alpha_{11} f_1 + \alpha_{21} f_2 + \ldots + \alpha_{m1} f_m, \\
Ae_2 = \alpha_{12} f_1 + \alpha_{22} f_2 + \ldots + \alpha_{m2} f_m, \\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
Ae_j = \alpha_{1j} f_1 + \alpha_{2j} f_2 + \ldots + \alpha_{mj} f_m, \\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
Ae_n = \alpha_{1n} f_1 + \alpha_{2n} f_2 + \ldots + \alpha_{mn} f_m.
\end{array}
$$

Matrica s m redaka i n stupaca, koja se dobije tako da koeficijente u prikazu vektora Ae_j stavimo kao $j-$ti stupac, zove se **matrica operatora** A **u paru baza** (f, e) i označava $A(f, e)$:

$$
A(f,e) = \begin{bmatrix}
\alpha_{11} & \alpha_{12} & \alpha_{13} & \cdots & \alpha_{1n} \\
\alpha_{21} & \alpha_{22} & \alpha_{23} & \cdots & \alpha_{2n} \\
\alpha_{31} & \alpha_{32} & \alpha_{33} & \cdots & \alpha_{3n} \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
\alpha_{m1} & \alpha_{m2} & \alpha_{m3} & \cdots & \alpha_{mn}
\end{bmatrix}
$$

Dokazi tvrdnji sljedeće propozicije, koje izostavljamo, sastoje se u neposrednoj primjeni definicije matrice operatora u zadanom paru baza i definicija operacija u prostorima linearnih operatora.

Propozicija 2.3 *Neka su V, W i U konačnodimenzionalni vektorski prostori nad istim poljem K i neka su redom $e = \{e_1, e_2, \ldots, e_n\}$, $f = \{f_1, f_2, \ldots, f_m\}$ i $g = \{g_1, g_2, \ldots, g_p\}$ uređene baze tih prostora.*

(*a*) *Ako su $A, B \in L(V, W)$ i $\lambda, \mu \in K$, onda je $(\lambda A + \mu B)(f, e) = \lambda A(f, e) + \mu B(f, e)$.*

(*b*) *Ako su $A \in L(V, W)$ i $B \in L(W, U)$, onda je $(BA)(g, e) = B(g, f)A(f, e)$.*

Za vektorske prostore V i W nad istim poljem linearan operator $A : V \to W$ zove se **izomorfizam** ako je A bijekcija sa V na W. Ako takav A postoji, kažemo da je vektorski prostor V **izomorfan** vektorskom prostoru W i pišemo $V \simeq W$. Operator identitete $I = I_V : V \to V$ je očito izomorfizam, pa vrijedi $V \simeq V$ za svaki vektorski prostor V. Nadalje, ako je $A : V \to W$ izomorfizam, onda je i inverzno preslikavanje $A^{-1} : W \to V$ izomorfizam. Dakle, iz $V \simeq W$ slijedi $W \simeq V$. Napokon, ako su $A : V \to W$ i $B : W \to U$ izomorfizmi, onda je i njihov produkt $BA : V \to U$ izomorfizam. Dakle, iz $V \simeq W$ i $W \simeq U$ slijedi $V \simeq U$. Ova razmatranja pokazuju da je *biti izomorfan* relacija ekvivalencije među vektorskim prostorima.

Teorem 2.1 *Neka su V i W konačnodimenzionalni vektorski prostori nad istim poljem K.*

(1) *Neka je $A \in L(V, W)$. Tada su sljedeća četiri svojstva međusobno ekvivalentna:*

  (*a*) *A je izomorfizam.*

  (*b*) *Za neku bazu $e = \{e_1, e_2, \ldots, e_n\}$ od V, $Ae = \{Ae_1, Ae_2, \ldots, Ae_n\}$ je baza od W.*

(c) *Za svaku bazu e od V je Ae baza od W.*

(d) *Postoje baze e od V i f od W takve da je $A(f,e)$ jedinična matrica.*

(2) *Vektorski prostori V i W su izomorfni ako i samo ako je $\dim V = \dim W$. Posebno, svaki $n-$dimenzionalan vektorski prostor nad poljem K izomorfan je vektorskom prostoru K^n.*

Dokaz: (1) Evidentno je da $(c) \Rightarrow (b)$.

Dokažimo da $(b) \Rightarrow (a)$. Pretpostavljamo, dakle, da je Ae baza od W za neku bazu e od V. Treba dokazati da odatle slijedi da je $A : V \to W$ bijekcija. Neka su x, y vektori iz V takvi da je $Ax = Ay$. Zbog linearnosti operatora A tada je $A(x-y) = 0$. Vektor $x-y$ prikažemo kao linearnu kombinaciju vektora baze e prostora V :

$$x - y = \lambda_1 e_1 + \lambda_2 e_2 + \ldots + \lambda_n e_n.$$

Tada imamo:

$$0 = A(x-y) = \lambda_1 Ae_1 + \lambda_2 Ae_2 + \ldots + \lambda_n Ae_n.$$

Po pretpostavci je $Ae = \{Ae_1, Ae_2, \ldots, Ae_n\}$ baza prostora W pa slijedi $\lambda_1 = \lambda_2 = \ldots = = \lambda_n = 0$. Odatle je $x - y = 0$, odnosno $x = y$. Dakle, A je injekcija. Treba još dokazati da je $A : V \to W$ surjekcija. Neka je $w \in W$. Vektor w prikažemo pomoću vektora baze Ae prostora W: $w = \lambda_1 Ae_1 + \lambda_2 Ae_2 + \ldots + \lambda_n Ae_n$. Stavimo $x = \lambda_1 e_1 + \ldots + \lambda_n x_n$. Tada je očito $Ax = w$. Dakle je $R(A) = W$, tj. A je surjekcija. Time je dokazano da iz (b) slijedi (a).

Dokažimo sada da iz (a) slijedi (c). Pretpostavljamo da je $A : V \to W$ izomorfizam i neka je $e = \{e_1, e_2, \ldots, e_n\}$ bilo koja baza od V. Treba dokazati da je $Ae = \{Ae_1, Ae_2, \ldots, Ae_n\}$ baza od W. Dokažimo prvo linearnu nezavisnost od Ae. Neka su $\lambda_1, \lambda_2, \ldots, \lambda_n \in K$ takvi da je $\lambda_1 Ae_1 + \lambda_2 Ae_2 + \ldots + \lambda_n Ae_n = 0$. Zbog linearnosti od A slijedi $A(\lambda_1 e_1 + \lambda_2 e_2 + \ldots + \lambda_n e_n) = 0$. Također je i $A(0) = 0$. Kako je po pretpostavci A izomorfizam, dakle i injekcija, iz jednakosti

$$A(\lambda_1 e_1 + \lambda_2 e_2 + \ldots + \lambda_n e_n) = 0 = A(0)$$

slijedi

$$\lambda_1 e_1 + \lambda_2 e_2 + \ldots + \lambda_n e_n = 0.$$

Međutim, $e = \{e_1, e_2, \ldots, e_n\}$ je baza, dakle linearno nezavisan podskup od V, pa slijedi $\lambda_1 = \lambda_2 = \ldots = \lambda_n = 0$. To pokazuje da je Ae linearno nezavisan podskup od W. Treba još dokazati da skup Ae razapinje čitav prostor W. Neka je $w \in W$. Kako je po pretpostavci A izomorfizam, dakle i surjekcija, postoji $x \in V$ takav da je $Ax = w$. Vektor x prikažemo kao linearnu kombinaciju vektora baze e : $x = \lambda_1 e_1 + \lambda_2 e_2 + \ldots + \lambda_n e_n$. Tada zbog linearnosti operatora A imamo:

$$w = Ax = A(\lambda_1 e_1 + \lambda_2 e_2 + \ldots + \lambda_n e_n) = \lambda_1 Ae_1 + \lambda_2 Ae_2 + \ldots + \lambda_n Ae_n.$$

Time je dokazano da je proizvoljan vektor $w \in W$ linearna kombinacija vektora iz Ae. Dakle, Ae je baza od W, pa vrijedi (c).

Dokazali smo da su svojstva (a), (b) i (c) međusobno ekvivalentna. Dokazat ćemo sada da je svojstvo (b) ekvivalentno svojstvu (d) i time će tvrdnja (1) biti u potpunosti dokazana. Pretpostavimo da vrijedi (b) i neka je e baza od V takva da je $f = Ae$ baza od W. Tada je $Ae_1 = f_1, Ae_2 = f_2, \ldots, Ae_n = f_n$, pa vidimo da je $A(f,e)$ jedinična matrica. Dakle, iz (b) slijedi (d). Pretpostavimo sada da vrijedi (d) i neka su e i f baze od V i W takve da je $A(f,e)$ jedinična matrica. To znači da je $Ae_1 = f_1, Ae_2 = f_2, \ldots, Ae_n = f_n$, tj. $Ae = f$. Dakle, e je baza od V takva da je Ae baza od W, tj. vrijedi (b).

(2) Pretpostavimo da je $\dim V = \dim W = n$ i neka su $e = \{e_1, e_2, \ldots, e_n\}$ baza od V i $f = \{f_1, f_2, \ldots, f_n\}$ baza od W. Prema propoziciji 2.1 postoji jedinstven $A \in L(V,W)$ takav da je

$Ae_1 = f_1, Ae_2 = f_2, \dots, Ae_n = f_n$, tj. $Ae = f$. Prema dokazanoj tvrdnji (1) (konkretno iz ekvivalentnosti svojstava (a) i (b)) slijedi da je A izomorfizam, tj. prostori V i W su izomorfni. Vrijedi i obrnuta implikacija, jer ako su prostori V i W izomorfni onda iz dokazane tvrdnje (1) evidentno slijedi da su im dimenzije jednake. Napokon, kako je očito $\dim K^n = n$ (naime, vektori $(1, 0, \dots, 0)$, $(0, 1, 0, \dots, 0)$, $\dots$, $(0, \dots, 0, 1)$ tvore bazu prostora K^n i ima ih n), svaki $n-$dimenzionalan vektorski prostor nad poljem K izomorfan je prostoru K^n.

Time je teorem 2.1 u potpunosti dokazan.

Teorem 2.2 *Neka su V i W konačnodimenzionalni vektorski prostori nad poljem K i neka su $e = \{e_1, e_2, \dots, e_n\}$ baza od V i $f = \{f_1, f_2, \dots, f_m\}$ baza od W. Tada je $A \mapsto A(f, e)$ izomorfizam vektorskog prostora $L(V, W)$ na vektorski prostor $M_{m,n}(K)$ svih matrica sa m redaka i n stupaca.*

Dokaz: Prema tvrdnji (a) propozicije 2.3 to je preslikavanje linearno.

Dokažimo da je to preslikavanje injekcija. Neka su A i B operatori iz $L(V, W)$ takvi da je $A(f, e) = B(f, e)$. Iz definicije matrice operatora u određenom paru baza odatle slijedi da je $Ae_1 = Be_1, Ae_2 = Be_2, \dots, Ae_n = Be_n$. Iz jedinstvenosti u propoziciji 2.1 odatle slijedi $A = B$. Time je dokazano da je preslikavanje $A \mapsto A(f, e)$ injektivno.

Treba još dokazati da je preslikavanje $A \mapsto A(f, e)$ surjekcija sa $L(V, W)$ na $M_{m,n}(K)$. Neka je C bilo koja matrica iz $M_{m,n}(K)$ i neka je sa α_{ij} označen element te matrice na presjecištu $i-$tog retka i $j-$tog stupca ($i = 1, 2, \dots, m$, $j = 1, 2, \dots, n$). Stavimo

$$\begin{aligned} w_1 &= \alpha_{11} f_1 + \alpha_{21} f_2 + \ldots + \alpha_{m1} f_m, \\ w_2 &= \alpha_{12} f_1 + \alpha_{22} f_2 + \ldots + \alpha_{m2} f_m, \\ &\dots\dots\dots\dots\dots\dots\dots\dots \\ w_n &= \alpha_{1n} f_1 + \alpha_{2n} f_2 + \ldots + \alpha_{mn} f_m. \end{aligned}$$

Po propoziciji 2.1 postoji operator $A \in L(V, W)$ takav da vrijedi

$$Ae_1 = w_1, \ Ae_2 = w_2, \ \dots, Ae_n = w_n.$$

Tada je $A(f, e) = C$. Dakle, $A \mapsto A(f, e)$ je surjekcija sa $L(V, W)$ na $M_{m,n}(K)$.

Time je teorem 2.2 dokazan.

Neka je $A \in L(V, W)$. Definiramo potprostore:

$$R(A) = \mathrm{Im} A = \{Av; v \in V\} \le W; \qquad N(A) = \mathrm{Ker} A = \{v \in V; Av = 0\} \le V.$$

$R(A)$ se zove **slika** ili **područje vrijednosti** operatora A, a $N(A)$ **jezgra** ili **nulprostor** operatora A. Ako je potprostor $R(A)$ konačnodimenzionalan, broj $r(A) = \dim R(A)$ zove se **rang operatora** A. Ako je potprostor $N(A)$ konačnodimenzionalan, broj $d(A) = \dim N(A)$ zove se **defekt operatora** A. Operator A je injekcija ako i samo ako je $N(A) = \{0\}$, tj. $d(A) = 0$. Operator A je surjekcija ako i samo ako je $R(A) = W$, odnosno, u slučaju konačnodimenzionalnog prostora W, ako i samo ako je $r(A) = \dim W$.

Teorem 2.3 (teorem o rangu i defektu) *Neka je $A \in L(V, W)$ pri čemu je prostor V konačnodimenzionalan. Tada je $\dim V = r(A) + d(A)$.*

Dokažimo najprije sljedeću pomoćnu tvrdnju:

Lema 2.1 *Neka je $A \in L(V, W)$ i neka je Y direktni komplement od $N(A)$ u prostoru V : $V = N(A) \dot{+} Y$. Definiramo preslikavanje $\varphi : Y \to R(A)$ relacijom $\varphi(y) = Ay$, $y \in Y$. Tada je φ izomorfizam vektorskog prostora Y na vektorski prostor $R(A)$.*

Dokaz leme 2.1: Iz linearnosti operatora A slijedi da je preslikavanje φ linearno. Dokažimo sada da je preslikavanje φ injektivno. Neka su y' i y'' vektori iz Y takvi da je $\varphi(y') = \varphi(y'')$. Tada za vektor $y = y' - y''$ iz potprostora Y vrijedi:

$$Ay = Ay' - Ay'' = \varphi(y') - \varphi(y'') = 0.$$

Prema tome je $y \in N(A) \cap Y$. Međutim, suma potprostora $N(A)$ i Y je direktna što znači da je njihov presjek jednak $\{0\}$. Slijedi $y = 0$, tj. $y' = y''$. Time je dokazano da je φ injekcija. Treba još dokazati da je φ surjekcija sa Y na $R(A)$. Neka je $w \in R(A)$. Prema definiciji potprostora $R(A)$ postoji $v \in V$ takav da je $w = Av$. Kako je $V = N(A) \dot{+} Y$ postoje $z \in N(A)$ i $y \in Y$ takvi da je $v = z + y$. Sada je $w = Av = Az + Ay = Ay = \varphi(y)$. Time je dokazano da je φ surjekcija i lema je u potpunosti dokazana.

Dokaz teorema 2.3: Prema propoziciji 1.5 postoji potprostor Y prostora V takav da je $V = Y \dot{+} N(A)$. Kako se radi o direktnoj sumi, to je

$$\dim V = \dim Y + \dim N(A) = \dim Y + d(A).$$

Prema upravo dokazanoj lemi 2.1 prostor Y izomorfan je prostoru $R(A)$, pa su im po tvrdnji (2) teorema 2.1 dimenzije iste: $\dim Y = \dim R(A) = r(A)$. Time je teorem 2.3 dokazan.

Promatrajmo sada situaciju $V = W$. Pišemo kraće $L(V, V) = L(V)$, te ako je e baza od V i $A \in L(V)$ pišemo $A(e)$ umjesto $A(e, e)$. Ako je $\dim V = n$ onda je dimenzija prostora $L(V)$ jednaka n^2, a $A(e)$ je kvadratna matrica $n-$tog reda. Primijetimo da je u vektorskom prostoru $L(V)$ osim operacija zbrajanja i množenja skalarom definirana i operacija množenja: za $A, B \in L(V)$ je i $AB \in L(V)$.

Za izomorfizam $A : V \to V$ upotrebljavamo i naziv **regularan operator**. Primjetimo da iz teorema o rangu i defektu za operator $A \in L(V)$ slijedi:

$$A \text{ injekcija} \iff d(A) = 0 \iff r(A) = n \iff A \text{ surjekcija}.$$

Dakle, $A \in L(V)$ je injekcija ako i samo ako je A surjekcija, dakle, regularan operator.

Skup svih regularnih operatora na prostoru V je grupa s obzirom na množenje operatora. Tu grupu označavamo sa $GL(V)$. Ona je izomorfna grupi $GL_n(K)$ regularnih kvadratnih matrica $n-$tog reda (izomorfizam je $A \mapsto A(e)$ za bilo koju bazu e od V). Ako je $n > 1$ ta je grupa nekomutativna.

Neka su $e = \{e_1, e_2, \ldots, e_n\}$ i $e' = \{e'_1, e'_2, \ldots, e'_n\}$ dvije baze od V. Prema propoziciji 2.1 postoji jedinstven linearan operator $T : V \to V$ takav da je $Te = e'$ (tj. $Te_j = e'_j$ za $j = 1, \ldots, n$). Prema tvrdnji *(1)* teorema 2.1 T je izomorfizam tj. $T \in GL(V)$. T se zove **operator prijelaza iz baze** e **u bazu** e'. Ako sa τ_{ij} označimo elemente kvadratne matrice $T(e)$, uočimo da za jedinični operator $I = I_V$ na prostoru V vrijedi:

$$Ie'_j = e'_j = Te_j = \tau_{1j}e_1 + \tau_{2j}e_2 + \ldots + \tau_{nj}e_n.$$

To pokazuje da je matrica operatora T u bazi e jednaka matrici jediničnog operatora I u paru baza (e, e') :

$$T(e) = I(e, e').$$

Ta činjenica omogućuje vrlo jednostavan dokaz veze između matrica istog operatora u raznim parovima baza:

Propozicija 2.4 *Neka su V i W konačnodimenzionalni vektorski prostori i $A \in L(V,W)$. Neka su e i e' baze od V, f i f' baze od W i $T \in GL(V)$ i $S \in GL(W)$ pripadni operatori prijelaza: $Te = e'$, $Sf = f'$. Tada je*

$$A(f',e') = S(f)^{-1}A(f,e)T(e).$$

Dokaz: Prema tvrdnji (b) propozicije 2.3 i zbog jednakosti $T(e) = I_V(e,e')$ i $S(f) = I_W(f,f')$ imamo:

$$A(f,e)T(e) = A(f,e)I_V(e,e') = (AI_V)(f,e') = A(f,e') =$$
$$= (I_WA)(f,e') = I_W(f,f')A(f',e') = S(f)A(f',e')$$

a množenjem slijeva s inverznom matricom od regularne matrice $S(f)$ dobivamo upravo jednakost koju dokazujemo: $A(f',e') = S(f)^{-1}A(f,e)T(e)$.

Teorem 2.4 *Neka su V i W konačnodimenzionalni vektorski prostori i neka su $A, B \in L(V,W)$.*

(1) *Sljedeća su dva svojstva međusobno ekvivalentna:*

   (a) *Postoje $T \in GL(V)$ i $S \in GL(W)$ takvi da je $A = SBT$.*

   (b) $r(A) = r(B)$.

(2) *Vrijedi $r(A) = r$ ako i samo ako postoje baze e od V i f od W takve da je $A(f,e) = E_{m,n,r}$. Pri tome je $n = \dim V$, $m = \dim W$ i $E_{m,n,r}$ je matrica s m redaka i n stupaca koja ima sve elemente 0 osim jedinične matrice formata $r \times r$ u gornjem lijevom kvadrantu.*

Dokaz: Dokažimo najprije tvrdnju (2). Neka je $A \in L(V,W)$, $\dim V = n$, $\dim W = m$ i pretpostavimo da je $r(A) = r$. Prema teoremu o rangu i defektu tada je $d(A) = \dim N(A) = n - r$. Prema propoziciji 1.5 postoji potprostor Y prostora V takav da je $V = Y \dot{+} N(A)$ i tada je $\dim Y = r$. Izaberimo bazu $\{e_1, e_2, \ldots, e_r\}$ od Y i bazu $\{e_{r+1}, e_{r+2}, \ldots, e_n\}$ od $N(A)$. Tada je $e = \{e_1, e_2, \ldots, e_r, e_{r+1}, \ldots, e_n\}$ baza od V. Nadalje, stavimo $f_j = Ae_j$ za $j = 1, 2, \ldots, r$. Po lemi 2.1 $\{f_1, \ldots, f_r\}$ je baza od $R(A)$. Dopunimo tu bazu do baze $f = \{f_1, \ldots, f_r, f_{r+1}, \ldots, f_m\}$ od W. Tada imamo:

$$Ae_1 = f_1,\ Ae_2 = f_2,\ \ldots,\ Ae_r = f_r,\ Ae_{r+1} = 0,\ \ldots,\ Ae_n = 0.$$

To pokazuje da je $A(f,e) = E_{m,n,r}$.

Dokažimo sada obrat. Neka je $A \in L(V,W)$ i neka su $e = \{e_1, \ldots, e_r, e_{r+1}, \ldots, e_n\}$ baza od V i $f = \{f_1, f_2, \ldots, f_r, f_{r+1}, \ldots, f_m\}$ baza od W takve da je $A(f,e) = E_{m,n,r}$. Tada je

$$Ae_1 = f_1,\ Ae_2 = f_2,\ \ldots,\ Ae_r = f_r,\ Ae_{r+1} = 0,\ \ldots,\ Ae_n = 0.$$

Budući da $Ae_1, Ae_2, \ldots, Ae_n$ razapinju $R(A)$, prema gornjim jednakostima je jasno da je $\{f_1, f_2, \ldots, f_r\}$ baza od $R(A)$. Stoga je $r(A) = \dim R(A) = r$. Time je tvrdnja (2) dokazana.

Dokažimo sada tvrdnju (1). Pretpostavimo da vrijedi $r(A) = r(B) = r$. Prema dokazanoj tvrdnji (2) postoje baze e i e' od V i baze f i f' od W takve da vrijedi $A(f,e) = E_{m,n,r} = B(f',e')$. Neka je $T \in GL(V)$ operator prijelaza iz baze e u bazu e' i neka je $S \in GL(W)$ operator prijelaza iz baze f' u bazu f. Primjenom propozicije 2.4 i tvrdnje (b) propozicije 2.3 (uz napomenu da je inverzni operator S^{-1} od S operator prijelaza iz baze f u bazu f' i da je $(S^{-1})(f)^{-1} = S(f)$) dobivamo:

$$A(f,e) = B(f',e') = S(f)B(f,e)T(e) = (SBT)(f,e).$$

Kako je prema teoremu 2.2 preslikavanje $C \mapsto C(f,e)$ izomorfizam sa $L(V,W)$ na $M_{m,n}(K)$, odatle slijedi $A = SBT$. Time smo dokazali da $(b) \Rightarrow (a)$.

Obrnutu implikaciju dokazat ćemo pomoću sljedeće leme:

Lema 2.2 *Neka su V, W i U konačnodimenzionalni vektorski prostori i neka su $A \in L(V, W)$ i $B \in L(W, U)$. Tada je $r(BA) \le r(A)$ i $r(BA) \le r(B)$.*

Dokaz: Imamo $R(BA) = \{BAx; x \in V\} \subseteq \{By; y \in W\} = R(B)$ pa slijedi $r(BA) \le r(B)$. Nadalje, kako je $R(A) = \{Ax; x \in V\}$ imamo

$$R(BA) = \{B(Ax); x \in V\} = \{By; y \in R(A)\}.$$

Stoga, ako je $\{y_1, y_2, \ldots, y_k\}$ baza od $R(A)$, onda skup $\{By_1, By_2, \ldots, By_k\}$ razapinje $R(BA)$, pa je $r(BA) = \dim R(BA) \le k = \dim R(A) = r(A)$.

Dokažimo sada da u tvrdnji (1) teorema 2.4 iz (a) slijedi (b). Pretpostavimo, dakle, da su $A, B \in L(V, W)$ i pretpostavimo da postoje $S \in GL(W)$ i $T \in GL(V)$ takvi da je $A = SBT$. Tada iz leme 2.2 slijedi redom:

$$r(A) = r(S(BT)) \le r(BT) \le r(B).$$

Kako je i $B = S^{-1}AT^{-1}$, analogno se dobiva i $r(B) \le r(A)$. Iz dvije nejednakosti slijedi jednakost $r(A) = r(B)$. Dakle iz (a) slijedi (b) i time je tvrdnja (1) u teoremu 2.4 dokazana.

Neka je V vektorski prostor nad poljem K. Samo polje K je također vektorski prostor nad K i dimenzija mu je 1 (doista, ako je $\alpha \in K$ različit od nule, onda je jednočlan skup $\{\alpha\}$ očito linearno nezavisan i razapinje prostor K : svaki $\beta \in K$ može se pisati $\beta = \lambda\alpha$ za $\lambda = \beta/\alpha \in K$; dakle, $\{\alpha\}$ je baza vektorskog prostora K nad poljem K). Vektorski prostor $V' = L(V, K)$ zove se **dualni prostor** vektorskog prostora V. Njegovi se elementi zovu **linearni funkcionali** (ili **linearne forme**) na vektorskom prostoru V. Ako je V konačnodimenzionalan, onda je prema propoziciji 2.2 i dualan prostor V' konačnodimenzionalan i vrijedi $\dim V' = \dim L(V, K) = (\dim V)(\dim K) = \dim V$.

Prisjetimo se dokaza propozicije 2.2. Uzeli smo bazu $e = \{e_1, e_2, \ldots, e_n\}$ prostora V i bazu $f = \{f_1, f_2, \ldots, f_m\}$ prostora W i onda smo pokazali da operatori $E_{ij} \in L(V, W)$, definirani sa $E_{ij}e_k = \delta_{jk}f_i$ $(1 \le i \le m, 1 \le j \le n, 1 \le k \le n)$ tvore bazu prostora $L(V, W)$. Ako je $e = \{e_1, e_2, \ldots, e_n\}$ baza prostora V, a za bazu jednodimenzionalnog prostora K uzmemo $\{1\}$, onda tim postupkom dolazimo do baze $e' = \{e'_1, e'_2, \ldots, e'_n\}$ prostora V'. Funkcionali e'_j definirani su sa $e'_j(e_k) = \delta_{jk}$ $(j, k \in \{1, 2, \ldots, n\})$. Za bazu e' kažemo da je **dualna** bazi e.

Ako je $e = \{e_1, e_2, \ldots, e_n\}$ baza prostora V, i $e' = \{e'_1, e'_2, \ldots, e'_n\}$ njoj dualna baza prostora V', onda za $x \in V$ možemo pisati $x = \sum_{1 \le k \le n} \alpha_k e_k$. Primijenimo li na tu jednakost linearan funkcional e'_j dobivamo

$$e'_j(x) = \sum_{k=1}^{n} \alpha_k e'_j(e_k) = \sum_{k=1}^{n} \alpha_k \delta_{jk} = \alpha_j.$$

Dakle, za svaki $x \in V$ vrijedi:

$$x = \sum_{j=1}^{n} e'_j(x) e_j.$$

Analogno, ako je $f \in V'$ možemo pisati $f = \sum_{1 \le j \le n} \beta_j e'_j$. Primijenimo li taj linearan funkcional na vektor e_k dobivamo

$$f(e_k) = \sum_{j=1}^{n} \beta_j e'_j(e_k) = \sum_{j=1}^{n} \beta_j \delta_{jk} = \beta_k.$$

Dakle, za svaki $f \in V'$ vrijedi:

$$f = \sum_{j=1}^{n} f(e_j) e'_j.$$

Neka su V i W vektorski prostori nad poljem K i neka je $A \in L(V,W)$. Za $g \in W'$ definiramo preslikavanje $A'(g) : V \to K$ relacijom

$$[A'(g)](v) = g(Av), \ v \in V.$$

Iz linearnosti g i A odmah slijedi da je to preslikavanje linearno, tj. $A'(g) \in V'$. Na taj način definirali smo operator $A' : W' \to V'$. Taj je operator linearan, jer za $\alpha, \beta \in K$ i za $g, h \in W'$ imamo za svaki $v \in V$:

$$[A'(\alpha g + \beta h)](v) = (\alpha g + \beta h)(Av) = \alpha g(Av) + \beta h(Av) =$$

$$= \alpha[A'(g)](v) + \beta[A'(h)](v) = [\alpha A'(g) + \beta A'(h)](v).$$

Za linearan operator $A' \in L(W', V')$ kažemo da je **dualan** linearnom operatoru $A \in L(V,W)$.

Teorem 2.5 *(a) $A \mapsto A'$ je linearno preslikavanje s prostora $L(V,W)$ u prostor $L(W', V')$.*

(b) Ako su $A \in L(V,W)$ i $B \in L(W,U)$ onda je $(BA)' = A'B'$.

(c) Ako su vektorski prostori V i W konačnodimenzionalni onda je $A \mapsto A'$ izomorfizam vektorskog prostora $L(V,W)$ na vektorski prostor $L(W', V')$.

Dokaz: (a) Za $\alpha, \beta \in K$ i $A, B \in L(V,W)$ i za bilo koji $g \in W'$ i bilo koji $v \in V$ imamo:

$$[(\alpha A + \beta B)'g](v) = g((\alpha A + \beta B)v) = g(\alpha Av + \beta Bv) = \alpha g(Av) + \beta g(Bv) =$$

$$= \alpha[A'g](v) + \beta[B'g](v) = [\alpha A'g + \beta B'g](v) = [(\alpha A' + \beta B')g](v).$$

Budući da to vrijedi za svaki vektor $v \in V$ slijedi $(\alpha A + \beta B)'g = (\alpha A' + \beta B')g$. Kako ta jednakost vrijedi za svaki funkcional $g \in W'$ zaključujemo da vrijedi $(\alpha A + \beta B)' = \alpha A' + \beta B'$. Dakle, preslikavanje pridruživanja dualnog operatora $A \mapsto A'$ je linearno.

(b) Za $h \in U'$ i za $v \in V$ nalazimo:

$$[(BA)'h](v) = h(BAv) = [B'h](Av) = [A'B'h](v).$$

Budući da to vrijedi za svaki vektor $v \in V$ slijedi $(BA)'h = A'B'h$. Kako ta jednakost vrijedi za svaki funkcional $h \in U'$ slijedi $(BA)' = A'B'$.

(c) Neka su $e = \{e_1, e_2, \ldots, e_n\}$ i $f = \{f_1, f_2, \ldots, f_m\}$ baze od V i W. Označimo sa $e' = \{e'_1, e'_2, \ldots, e'_n\}$ i $f' = \{f'_1, f'_2, \ldots, f'_m\}$ njima dualne baze od V' i W'. Neka su operatori $E_{ij} \in L(V,W)$ definirani kao u dokazu propozicije 2.2: $E_{ij}e_k = \delta_{jk}f_i$. Znamo da je tada $\{E_{ij} : 1 \leq i \leq m, 1 \leq j \leq n\}$ baza vektorskog prostora $L(V,W)$. Proučimo sada kako dualni operatori $(E_{ij})'$ djeluju na vektore baze f' :

$$[(E_{ij})'f'_p](e_q) = f'_p(E_{ij}e_q) = \delta_{jq}f'_p(f_i) = \delta_{jq}\delta_{ip} = \delta_{ip}e'_j(e_q).$$

Budući da to vrijedi za svaki $q = 1, \ldots, n$, zaključujemo da je $(E_{ij})'f'_p = \delta_{ip}e'_j$. Prema dokazu propozicije 2.2 (primijenjenom na baze f' od W' i e' od V') nalazimo da operatori $(E_{ij})'$ za $1 \leq j \leq n, 1 \leq i \leq m$, tvore bazu prostora $L(W', V')$. Dakle, $A \mapsto A'$ preslikava neku bazu prostora $L(V,W)$ u bazu prostora $L(W', V')$. Prema tvrdnji *(1)* teorema 2.1 to je preslikavanje izomorfizam vektorskih prostora.

Neka su e, f, e' i f' baze iz dokaza tvrdnje (c) prethodnog teorema. Neka je A linearan operator sa V u W. Označimo sa α_{ij} elemente matrice $A(f,e)$ i sa β_{pq} elemente matrice $A'(e',f')$. Tada je $Ae_j = \sum_{1\le i\le m} \alpha_{ij} f_i$. Primijenimo li funkcional f'_q na lijevu i desnu stranu te jednakosti, dobivamo

$$f'_q(Ae_j) = \sum_{i=1}^{m} \alpha_{ij} f'_q(f_i) = \sum_{i=1}^{m} \alpha_{ij}\delta_{iq} = \alpha_{qj}.$$

S druge strane je $A'f'_q = \sum_{1\le p\le n} \beta_{pq} e'_p$ i primijenimo li funkcionale s obje strane te jednakosti na vektor e_j dobivamo

$$[A'f'_q](e_j) = \sum_{p=1}^{n} \beta_{pq} e'_p(e_j) = \sum_{p=1}^{n} \beta_{pq}\delta_{pj} = \beta_{jq}.$$

Prema definiciji dualnog operatora zaključujemo:

$$\beta_{jq} = [A'f'_q](e_j) = f'_q(Ae_j) = \alpha_{qj}.$$

Time smo dokazali:

Propozicija 2.5 *Neka su V i W konačnodimenzionalni vektorski prostori, A linearan operator sa V u W, e i f baze prostora V i W, e' i f' njima dualne baze od V' i W'. Tada su matrice $A(f,e)$ i $A'(e',f')$ međusobno transponirane.*

Za podskup S vektorskog prostora V definiramo

$$S^0 = \{f \in V'; f(x) = 0 \ \forall x \in S\}.$$

Očito je S^0 potprostor dualnog prostora V' za bilo koji podskup S vektorskog prostora V. Potprostor S^0 zove se **anihilator** skupa $S \subseteq V$. Analogno, za podskup T dualnog prostora V' njegov anihilator je potprostor od V :

$$T^0 = \{x \in V; f(x) = 0 \ \forall f \in T\}.$$

Uz ove oznake moguća je dvojba: da li je anihilator T^0 od $T \subseteq V'$ potprostor od V ili mislimo na potprostor dualnog prostora $V'' = (V')'$ od V'? U konačnodimenzionalnom slučaju ta dvojba nestaje, jer se tzv. **bidual** V'' prostora V može identificirati s prostorom V :

Teorem 2.6 *Neka je V vektorski prostor nad poljem K. Za svaki $v \in V$ definiramo preslikavanje $\varphi(v) : V' \to K$ relacijom $[\varphi(v)](f) = f(v), f \in V'$. Tada je preslikavanje $\varphi(v)$ linearno, tj. $\varphi(v) \in V''$. Nadalje, preslikavanje $\varphi : V \to V''$ je linearno. Napokon, ako je prostor V konačnodimenzionalan, φ je izomorfizam prostora V na njegov bidual V''.*

Dokaz: Za $\alpha, \beta \in K$ i $f, g \in V'$ imamo:

$$[\varphi(v)](\alpha f + \beta g) = (\alpha f + \beta g)(v) = \alpha f(v) + \beta g(v) = \alpha[\varphi(v)](f) + \beta[\varphi(v)](g).$$

Dakle, preslikavanje $\varphi(v) : V' \to K$ je linearno, tj. $\varphi(v) \in V''$.

Dokažimo sada da je preslikavanje $\varphi : V \to V''$ linearno. Za $\alpha, \beta \in K$ i $v, w \in V$ imamo za svaki $f \in V'$:

$$[\varphi(\alpha v+\beta w)](f) = f(\alpha v+\beta w) = \alpha f(v)+\beta f(w) = \alpha[\varphi(v)](f)+\beta[\varphi(w)](f) \ = \ [\alpha\varphi(v)+\beta\varphi(w)](f).$$

Kako to vrijedi za svaki funkcional $f \in V'$, slijedi $\varphi(\alpha v + \beta w) = \alpha\varphi(v) + \beta\varphi(w)$, tj. preslikavanje $\varphi : V \to V''$ je linearno.

Napokon, pretpostavimo da je prostor V konačnodimenzionalan. Tada je $\dim V = \dim V' = = \dim V''$. Dakle, po teoremu o rangu i defektu (teorem 2.3) primijenjenom na preslikavanje φ $(r(\varphi) + d(\varphi) = \dim V)$ vidimo da je za dokaz bijektivnosti preslikavanja φ dovoljno dokazati njegovu injektivnost, odnosno, da mu je jezgra jednaka $\{0\}$. Neka je $v \in V$ takav da je $\varphi(v) = 0$. Neka je $\{e_1, e_2, \ldots, e_n\}$ baza od V i $\{e'_1, e'_2, \ldots, e'_n\}$ dualna baza od V'. Tada je $v = \sum_{1 \leq j \leq n} e'_j(v) e_j$. Međutim, za svaki indeks j imamo $e'_j(v) = [\varphi(v)](e'_j) = 0$, pa slijedi $v = 0$. To pokazuje da je φ injekcija, dakle bijekcija, dakle izomorfizam sa V na V''.

Zbog teorema 2.6 u slučaju konačnodimenzionalnog prostora V pomoću izomorfizma φ možemo identificirati prostor V s njegovim bidualom V''. Dakle, vektor $v \in V$ identificira se s linearnim funkcionalom $f \mapsto f(v)$ na prostoru V'. Uz takvu identifikaciju za konačnodimenzionalne vektorske prostore V i W za $A \in L(V, W)$ nalazimo da je $A'' = A$.

Propozicija 2.6 *Neka je V konačnodimenzionalan vektorski prostor, S podskup od V ili od V' i W potprostor od V ili od V'.*

(*a*) $S^0 = [S]^0$.

(*b*) $[S] = S^{00}, W^{00} = W$.

(*c*) $\dim W^0 = \dim V - \dim W$.

(*Pri tome podrazumijevamo da je bidual V'' identificiran s prostorom V pomoću preslikavanja φ iz prethodnog teorema*).

Dokaz: (*a*) Neka je S podskup od V. Iz $S \subseteq [S]$ slijedi obrnuta inkluzija za anihilatore: $S^0 \supseteq [S]^0$. Neka je $f \in S^0$ i neka je $x \in [S]$. Tada je x linearna kombinacija vektora iz S pa zbog linearnosti funkcionala f slijedi $f(x) = 0$. Dakle, $f \in [S]^0$, pa zaključujemo da vrijedi i obrnuta inkluzija $S^0 \subseteq [S]^0$.

(*c*) Neka je $W \leq V$. Izaberimo bazu $\{e_1, e_2, \ldots, e_k\}$ od W i nadopunimo je do baze $\{e_1, e_2, \ldots, e_n\}$ od V. Neka je $\{e'_1, e'_2, \ldots, e'_n\}$ dualna baza od V'. Tada funkcionali $e'_{k+1}, \ldots, e'_n$ poništavaju vektore $e_1, \ldots, e_k$, dakle:

$$e'_{k+1}, \ldots, e'_n \in \{e_1, e_2, \ldots, e_k\}^0 = [\{e_1, e_2, \ldots, e_k\}]^0 = W^0.$$

Neka je $f \in W^0$. Tada je $f(e_1) = f(e_2) = \ldots = f(e_k) = 0$ pa slijedi

$$f = \sum_{j=1}^{n} f(e_j) e'_j = \sum_{j=k+1}^{n} f(e_j) e'_j.$$

To pokazuje da funkcionali $e'_{k+1}, \ldots, e'_n$ razapinju potprostor W^0 dualnog prostora V', dakle $\{e'_{k+1}, \ldots, e'_n\}$ je baza od W^0. Odatle slijedi

$$\dim W^0 = n - k = \dim V - \dim W.$$

(*b*) Za potprostor W od V imamo očito $W \subseteq W^{00}$, a iz (*c*) slijedi

$$\dim W^{00} = \dim V' - \dim W^0 = \dim V - (\dim V - \dim W) = \dim W.$$

Dakle je $W = W^{00}$. Odatle za $S \subseteq V$ vrijedi $[S] = [S]^{00}$, pa zbog (*a*) imamo $[S] = [S]^{00} = ([S]^0)^0 = = (S^0)^0 = S^{00}$.

Propozicija 2.7 *Neka su V i W konačnodimenzionalni vektorski prostori nad istim poljem i $A \in L(V, W)$.*

(*a*) $N(A') = R(A)^0$, $N(A) = R(A')^0$, $R(A') = N(A)^0$, $R(A) = N(A')^0$.

(*b*) $r(A) = r(A')$.

Dokaz: (*a*) Identificiramo li V sa V'' i W sa W'' na temelju teorema 2.6 vidi se da je prva jednakost ekvivalentna s drugom i da je treća jednakost ekvivalentna s četvrtom. Nadalje, iz tvrdnje (*b*) propozicije 2.6 slijedi da je prva jednakost ekvivalentna s četvrtom (i druga s trećom). Dakle, sve četiri jednakosti su međusobno ekvivalentne, pa je dovoljno dokazati jednu od njih, npr. prvu.

Za $f \in W'$ imamo redom:

$$f \in N(A') \iff A'f = 0 \iff (A'f)(v) = 0 \quad \forall v \in V \iff$$

$$\iff f(Av) = 0 \quad \forall v \in V \iff f(w) = 0 \quad \forall w \in R(A) \iff f \in R(A)^0.$$

Dakle, $N(A') = R(A)^0$.

(*b*) Iz (*a*), iz tvrdnje (*c*) propozicije 2.6 i iz teorema o rangu i defektu (teorem 2.3) imamo redom:

$$r(A) = \dim R(A) = \dim N(A')^0 = \dim W' - \dim N(A') = \dim W' - d(A') = r(A').$$

3 Minimalni polinom i spektar

Funkcija $P{:}K \to K$ zove se **polinom** ako je $P(\lambda)$ linearna kombinacija potencija varijable λ:

$$P(\lambda) = \alpha_0 + \alpha_1\lambda + \alpha_2\lambda^2 + \cdots + \alpha_m\lambda^m.$$

Ako je $\alpha_m \neq 0$ broj $m \in \mathbb{N} \cup \{0\}$ zove se **stupanj polinoma** $P(\lambda)$ i označava deg $P(\lambda)$. Dakle, stupanj je najveća potencija u polinomu $P(\lambda)$. Ako je $\alpha_m = 1$ kažemo da je polinom $P(\lambda)$ **normiran**.

Neka je V konačnodimenzionalan vektorski prostor nad poljem K i neka je $A \in L(V) = L(V,V)$. Definiramo potencije operatora A: $A^0 = I$ (jedinični operator), $A^1 = A$, $A^2 = A \cdot A$, $A^3 = A \cdot A^2 = A^2 \cdot A$, i tako dalje, općenito $A^k = A \cdot A^{k-1}$. Potenciranje operatora ima sljedeća očigledna svojstva:

$$A^j \cdot A^k = A^{j+k}, \qquad \left(A^j\right)^k = A^{jk}, \qquad \forall j,k \in \mathbb{N} \cup \{0\}.$$

Linearna kombinacija potencija operatora A je polinom operatora A. Ako je

$$P(\lambda) = \alpha_0 + \alpha_1\lambda + \alpha_2\lambda^2 + \cdots + \alpha_m\lambda^m$$

bilo koji polinom u varijabli $\lambda \in K$, onda ćemo sa $P(A)$ označiti polinom operatora A s istim koeficijentima $\alpha_0, \alpha_1, \ldots, \alpha_m \in K$:

$$P(A) = \alpha_0 I + \alpha_1 A + \alpha_2 A^2 + \cdots + \alpha_m A^m.$$

Budući da je množenje operatora distributivno u odnosu na zbrajanje i budući da vrijedi $A^j A^k = A^{j+k}$, vrijede sljedeća pravila za računanje s polinomima danog operatora A :

$$R(\lambda) = P(\lambda) + Q(\lambda) \quad \Longrightarrow \quad R(A) = P(A) + Q(A),$$

$$S(\lambda) = P(\lambda) \cdot Q(\lambda) \quad \Longrightarrow \quad S(A) = P(A) \cdot Q(A).$$

Sa $\mathcal{L}(A)$ označavat ćemo potprostor od $L(V)$ razapet svim potencijama operatora A. To znači da je $\mathcal{L}(A)$ skup svih linearnih kombinacija potencija $I, A, A^2, \ldots,$ a budući da su linearne kombinacije potencija upravo polinomi operatora A, imamo

$$\mathcal{L}(A) = [\{I, A, A^2, A^3, \ldots\}] = [\{A^k;\ k \in \mathbb{N} \cup \{0\}\}] = \{P(A);\ P(\lambda)\ \text{ polinom}\}.$$

Ako je dimenzija prostora V jednaka n, onda je dimenzija od $L(V)$ jednaka n^2. Prema tome je $\dim \mathcal{L}(A) \leq n^2$. U stvari, ako je $n \geq 2$ onda vrijedi $\dim \mathcal{L}(A) < n^2$. Doista, $\dim \mathcal{L}(A) = n^2$ bi značilo da je $\mathcal{L}(A) = L(V)$, a to nije moguće, jer za bilo koje $B, C \in \mathcal{L}(A)$ vrijedi $BC = CB$, a to nije istina za bilo koje $B, C \in L(V)$.

Posebno, operatori $I, A, A^2, \ldots$ ne mogu biti linearno nezavisni. Neka je m najmanji prirodan broj takav da je $A^m \in [\{I, A, \ldots, A^{m-1}\}]$. Drugim riječima, m je takav da su $I, A, \ldots, A^{m-1}$ su linearno nezavisni, a $I, A, \ldots, A^{m-1}, A^m$ su linearno zavisni. Naravno, $m \leq \dim \mathcal{L}(A)$, dakle $m \leq n^2$. Neka su $\mu_1, \mu_2, \ldots, \mu_m \in K$ takvi da je

$$A^m = \mu_1 A^{m-1} + \mu_2 A^{m-2} + \cdots + \mu_{m-1} A + \mu_m I. \qquad (*)$$

Označimo sa $\mu_A(\lambda)$ polinom

$$\mu_A(\lambda) = \lambda^m - \mu_1\lambda^{m-1} - \cdots - \mu_{m-1}\lambda - \mu_m.$$

Tada je $\mu_A(A) = 0$. Polinom $\mu_A(\lambda)$ zove se **minimalni polinom** operatora A. Minimalni polinom svakog operatora je normiran, tj. koeficijent uz najveću potenciju jednak je 1.

Teorem 3.1 *Neka je V konačnodimenzionalan vektorski prostor, $A \in L(V)$ i neka je m stupanj minimalnog polinoma $\mu_A(\lambda)$ operatora A.*

(*a*) *$\mu_A(\lambda)$ je polinom najnižeg stupnja među svim netrivijalnim polinomima $P(\lambda)$ takvima da je $P(A) = 0$.*

(*b*) *$\dim \mathcal{L}(A) = m$ i $\mathcal{L}(A) = [\{I, A, A^2, \ldots, A^{m-1}\}]$. Drugim riječima, $\{I, A, A^2, \ldots, A^{m-1}\}$ je baza vektorskog prostora $\mathcal{L}(A)$.*

(*c*) *Za polinom $P(\lambda)$ vrijedi $P(A) = 0$ ako i samo ako je polinom $P(\lambda)$ djeljiv s polinomom $\mu_A(\lambda)$, tj. ako i samo ako je $P(\lambda) = Q(\lambda)\mu_A(\lambda)$ za neki polinom $Q(\lambda)$.*

Dokaz: Tvrdnja (a) slijedi neposredno iz činjenice da su operatori $I, A, A^2, \ldots, A^{m-1}$ linearno nezavisni, što znači da je $P(A) \neq 0$ za svaki netrivijalan polinom $P(\lambda)$ stupnja $< m$.

(b) Jasno je da je $[\{I, A, A^2, \ldots, A^{m-1}\}] \subseteq \mathcal{L}(A)$. Dokažimo da vrijedi i obrnuta inkluzija, dakle jednakost. Prije svega, iz $(*)$ slijedi da je $A^m \in [\{I, A, A^2, \ldots, A^{m-1}\}]$. Pomnožimo li $(*)$ sa A dobivamo

$$A^{m+1} = \mu_1 A^m + \mu_2 A^{m-1} + \cdots + \mu_{m-1} A^2 + \mu_m A.$$

Budući da su $A, A^2, \ldots, A^{m-1}, A^m \in [\{I, A, A^2, \ldots, A^{m-1}\}]$, odatle slijedi

$$A^{m+1} \in [\{I, A, A^2, \ldots, A^{m-1}\}].$$

Pomnožimo li sada jednakost $(*)$ sa A^2, dobivamo

$$A^{m+2} = \mu_1 A^{m+1} + \mu_2 A^m + \cdots + \mu_{m-1} A^3 + \mu_m A^2.$$

Budući da su $A^2, A^3, \ldots, A^m, A^{m+1} \in [\{I, A, A^2, \ldots, A^{m-1}\}]$, odatle slijedi

$$A^{m+2} \in [\{I, A, A^2, \ldots, A^{m-1}\}].$$

Nastavimo li na taj način korak po korak nalazimo da su sve potencije operatora A sadržane u potprostoru $[\{I, A, A^2, \ldots, A^{m-1}\}]$. Odatle slijedi tražena obrnuta inkluzija

$$\mathcal{L}(A) \subseteq [\{I, A, A^2, \ldots, A^{m-1}\}].$$

Time smo dokazali da je $\mathcal{L}(A) = [\{I, A, A^2, \ldots, A^{m-1}\}]$, a budući da su operatori $I, A, A^2, \ldots, A^{m-1}$ linearno nezavisni, nalazimo da je $\{I, A, A^2, \ldots, A^{m-1}\}$ baza od $\mathcal{L}(A)$ i da je $\dim \mathcal{L}(A) = m$.

(c) Pretpostavimo da je polinom $P(\lambda)$ djeljiv s polinomom $\mu_A(\lambda)$, tj. da je $P(\lambda) = Q(\lambda)\mu_A(\lambda)$. Tada je $P(A) = Q(A)\mu_A(A)$, pa iz $\mu_A(A) = 0$ slijedi $P(A) = 0$.

Pretpostavimo sada da je $P(\lambda)$ polinom takav da je $P(A) = 0$. Dijeljenjem polinoma $P(\lambda)$ s polinomom $\mu_A(\lambda)$ dolazimo do jednakosti oblika

$$P(\lambda) = Q(\lambda)\mu_A(\lambda) + R(\lambda),$$

pri čemu su $Q(\lambda)$ i $R(\lambda)$ polinomi i ostatak pri dijeljenju $R(\lambda)$ je polinom stupnja manjeg od m, tj. vrijedi $\deg R(\lambda) < \deg \mu_A(\lambda)$. Uvrstimo li u gornju jednakost operator A umjesto varijable λ dolazimo do operatorske jednakosti

$$P(A) = Q(A)\mu_A(A) + R(A).$$

Kako je $P(A) = \mu_A(A) = 0$, odatle slijedi da je $R(A) = 0$. No kako je stupanj polinoma $R(\lambda)$ manji od m, iz (a) zaključujemo da mora biti $R(\lambda) = 0$. To znači da je $P(\lambda) = Q(\lambda)\mu_A(\lambda)$, tj. polinom $P(\lambda)$ je djeljiv s polinomom $\mu_A(\lambda)$.

Prisjetimo se da se operator $A \in L(V)$ zove se **invertibilan** ili **regularan**, ako postoji $B \in L(V)$ takav da je $AB = BA = I$. U tom slučaju takav operator B je jedinstven; doista, ako i za $C \in L(V)$ vrijedi $AC = CA = I$, onda je $B = BI = B(AC) = (BA)C = IC = C$. Taj jedinstveni operator B zove se **invers** operatora A i označava sa A^{-1}. Poznavanje minimalnog polinoma operatora A omogućuje da odmah ustanovimo da li je operator A invertibilan ili nije i ako jest, da izračunamo invers A^{-1} :

Teorem 3.2 *Neka je V konačnodimenzionalan vektorski prostor, $A \in L(V)$ i neka je*

$$\mu_A(\lambda) = \lambda^m - \mu_1\lambda^{m-1} - \cdots - \mu_{m-1}\lambda - \mu_m$$

njegov minimalni polinom. Operator A je invertibilan ako i samo ako je $\mu_A(0) \neq 0$, tj. ako i samo ako je $\mu_m \neq 0$. U tom slučaju je

$$A^{-1} = \frac{1}{\mu_m}A^{m-1} - \frac{\mu_1}{\mu_m}A^{m-2} - \cdots - \frac{\mu_{m-2}}{\mu_m}A - \frac{\mu_{m-1}}{\mu_m}I. \qquad (**)$$

Dakle, A^{-1} je polinom od A, tj. $A^{-1} \in \mathcal{L}(A)$.

Dokaz: Pretpostavimo da je operator A invertibilan. Treba dokazati da je tada $\mu_m \neq 0$. Pretpostavimo suprotno, tj. da je $\mu_m = 0$. Tada iz $(*)$ nalazimo da je

$$A^m - \mu_1 A^{m-1} - \cdots - \mu_{m-2}A^2 - \mu_{m-1}A = 0.$$

Budući da je $A^k \cdot A^{-1} = A^{k-1}\ \forall k \in \mathbb{N}$, iz gornje jednakosti množenjem sa A dobivamo:

$$A^{m-1} - \mu_1 A^{m-2} - \cdots - \mu_{m-2}A - \mu_{m-1}I = 0.$$

No to je nemoguće, jer su operatori $I, A, \ldots, A^{m-1}$ linearno nezavisni. Ova kontradikcija pokazuje da je pretpostavka da je $\mu_m = 0$ nemoguća, pa zaključujemo da je $\mu_m \neq 0$.

Dokažimo sada obrnutu implikaciju. Pretpostavimo da je $\mu_m \neq 0$. Tada iz $(*)$ slijedi

$$I = \frac{1}{\mu_m}A^m - \frac{\mu_1}{\mu_m}A^{m-1} - \cdots - \frac{\mu_{m-2}}{\mu_m}A^2 - \frac{\mu_{m-1}}{\mu_m}A.$$

Stavimo li

$$B = \frac{1}{\mu_m}A^{m-1} - \frac{\mu_1}{\mu_m}A^{m-2} - \cdots - \frac{\mu_{m-2}}{\mu_m}A - \frac{\mu_{m-1}}{\mu_m}I$$

iz gornje jednakosti slijedi da je $AB = BA = I$. Dakle, A je invertibilan i $A^{-1} = B$, tj. vrijedi $(**)$.

Time je teorem u potpunosti dokazan.

Primijetimo da je operator $A \in L(V)$ invertibilan ako i samo ako je A bijekcija, tj. ako i samo ako je A izomorfizam prostora V na samoga sebe. Zbog teorema 2.3 o rangu i defektu $(r(A) + d(A) = \dim V)$ znamo da je A bijekcija ako i samo ako je A injekcija, tj. ako i samo ako je $N(A) = \{0\}$.

Za konačnodimenzionalan vektorski prostor V i za $A \in L(V)$ definiramo **spektar** $\sigma(A)$ operatora A kao skup svih skalara $\lambda_0 \in K$ takvih da operator $A - \lambda_0 I$ nije invertibilan:

$$\sigma(A) = \{\lambda_0 \in K;\ A - \lambda_0 I \ \text{ nije invertibilan}\}.$$

Nadalje, skalar $\lambda_0 \in K$ zove se **svojstvena vrijednost** operatora A ako postoji vektor $v \neq 0$ takav da je $Av = \lambda_0 v$. Svaki se takav vektor v zove **svojstveni vektor** operatora A za svojstvenu vrijednost λ_0.

Propozicija 3.1 *Neka je V konačnodimenzionalan vektorski prostor i $A \in L(V)$. Spektar $\sigma(A)$ operatora A je skup svih svojstvenih vrijednosti tog operatora.*

Dokaz: Doista, imamo redom:

$$\lambda_0 \in \sigma(A) \quad \Longleftrightarrow \quad A-\lambda_0 I \text{ nije invertibilan} \quad \Longleftrightarrow \quad N(A-\lambda_0 I) \neq \{0\} \quad \Longleftrightarrow$$

$$\Longleftrightarrow \quad \exists v \neq 0 \text{ takav da je } (A-\lambda_0 I)v = 0 \quad \Longleftrightarrow \quad \exists v \neq 0 \text{ takav da je } Av = \lambda_0 v.$$

Teorem 3.3 *Neka je V konačnodimenzionalan vektorski prostor i $A \in L(V)$. Tada je spektar operatora A skup svih nultočaka njegovog minimalnog polinoma.*

Dokaz: Spektar $\sigma(A)$ operatora A je skup svih $\lambda_0 \in K$ takvih da operator $A - \lambda_0 I$ nije invertibilan. U teoremu 3.2 ustanovili smo kriterij invertibilnosti linearnog operatora, pa nalazimo

$$\sigma(A) = \{\lambda_0 \in K;\ \mu_{A-\lambda_0 I}(0) = 0\}.$$

Cilj nam je ustanoviti vezu minimalnog polinoma $\mu_{A-\lambda_0 I}(\lambda)$ operatora $A - \lambda_0 I$ s minimalnim polinomom $\mu_A(\lambda)$ operatora A.

Po binomnoj formuli imamo za svaku potenciju k :

$$(A-\lambda_0 I)^k = \sum_{j=0}^{k} \binom{k}{j} A^j (-\lambda_0 I)^{k-j} = \sum_{j=0}^{k} (-1)^{k-j} \binom{k}{j} \lambda_0^{k-j} A^j =$$

$$= A^k - k\lambda_0 A^{k-1} + \binom{k}{2}\lambda_0^2 - \cdots + (-1)^k \lambda_0^k I.$$

Prema tome je $(A-\lambda_0 I)^k \in \mathcal{L}(A)\ \ \forall k \geq 0$, pa zaključujemo da je $\mathcal{L}(A-\lambda_0 I) \subseteq \mathcal{L}(A)$. Ako stavimo $B = A - \lambda_0 I$, onda je $A = B + \lambda_0 I$ pa sasvim analogno imamo i obrnutu inkluziju $\mathcal{L}(A) \subseteq \mathcal{L}(B) = \mathcal{L}(A-\lambda_0 I)$. Iz dvije inkluzije slijedi jednakost $\mathcal{L}(A-\lambda_0 I) = \mathcal{L}(A)$. Prema tvrdnji (b) teorema 3.1 zaključujemo da je $\deg \mu_B(\lambda) = \deg \mu_A(\lambda)$. Označimo taj stupanj sa m i neka je

$$\mu_A(\lambda) = \lambda^m - \mu_1 \lambda^{m-1} - \cdots - \mu_{m-1}\lambda - \mu_m.$$

Definiramo polinom $P(\lambda)$ sa

$$P(\lambda) = \mu_A(\lambda+\lambda_0) = (\lambda+\lambda_0)^m - \mu_1(\lambda+\lambda_0)^{m-1} - \cdots - \mu_{m-1}(\lambda+\lambda_0) - \mu_m.$$

Tada je $P(\lambda)$ polinom stupnja m i ako u njega uvrstimo operator $B = A - \lambda_0 I$, nalazimo

$$P(B) = \mu_A(B + \lambda_0 I) = \mu_A(A) = 0.$$

Prema tvrdnji (c) teorema 3.1 polinom $P(\lambda)$ djeljiv je s polinomom $\mu_B(\lambda)$. Međutim, oba polinoma su stupnja m i normirani su, tj. koeficijent uz najvišu potenciju λ^m jednak je 1. Odatle slijedi da je $\mu_{A-\lambda_0 I}(\lambda) = \mu_B(\lambda) = P(\lambda)$. Posebno, $\mu_{A-\lambda_0 I}(0) = P(0) = \mu_A(\lambda_0)$. Dakle, slijedi tvrdnja teorema:

$$\sigma(A) = \{\lambda_0 \in K;\ \mu_{A-\lambda_0 I}(0) = 0\} = \{\lambda_0 \in K;\ \mu_A(\lambda_0) = 0\}.$$

Prije smo uočili da za svaki $A \in L(V)$ stupanj njegovog minimalnog polinoma $\mu_A(\lambda)$ nije veći od $(\dim V)^2$, štoviše da u slučaju $\dim V \geq 2$ vrijedi $\deg \mu_A(\lambda) < (\dim V)^2$. U stvari, vrijedi znatno točnija nejednakost:

Teorem 3.4 *Neka je V konačnodimenzionalan vektorski prostor i $A \in L(V)$. Tada je*

$$\deg \mu_A(\lambda) \leq \dim V.$$

Dokaz ćemo provesti matematičkom indukcijom u odnosu na $\dim V$.

Baza indukcije: Ako je $\dim V = 1$, onda je $(\dim V)^2 = \dim V$, pa je tvrdnja teorema trivijalna jer slijedi iz poznate nam nejednakosti $st\mu_A(\lambda) \leq (\dim V)^2$.

Korak indukcije: Neka je $n \geq 2$ i pretpostavimo da je teorem dokazan ako je $\dim V \leq n-1$. Neka je $\dim V = n$ i neka je $v \in V$, $v \neq 0$. Promatramo niz vektora $v, Av, A^2v, A^3v, \ldots$ Budući da je dimenzija prostora jednaka n, u tom nizu ne može biti više od n linearno nezavisnih vektora. Prema tome, za neki $m \leq n$ vektori $v, Av, \ldots, A^{m-1}v$ su linearno nezavisni, a vektori $v, Av, \ldots, A^{m-1}v, A^m v$ su linearno zavisni. To znači da je m najmanji broj takav da je vektor $A^m v$ linearna kombinacija prethodnih vektora u promatranom nizu:

$$A^m v = \alpha_1 A^{m-1}v + \alpha_2 A^{m-2}v + \cdots + \alpha_{m-1}Av + \alpha_m v. \qquad (*)$$

Stavimo

$$W = [\{v, Av, \ldots, A^{m-1}v\}].$$

Budući da su vektori $v, Av, \ldots, A^{m-1}v$ linearno nezavisni, oni tvore bazu potprostora W, dakle $\dim W = m$. Bilo koji vektor $w \in W$ je linearna kombinacija vektora baze:

$$w = \beta_1 A^{m-1}v + \beta_2 A^{m-2}v + \cdots + \beta_{m-1}Av + \beta_m v.$$

Djelujemo li operatorom A na vektor w, dobivamo

$$Aw = \beta_1 A^m v + \beta_2 A^{m-1}v + \cdots + \beta_{m-1}A^2 v + \beta_m Av.$$

Pomoću jednakosti $(*)$ odatle vidimo da je $Aw \in W$. Na taj način smo dokazali:

$$w \in W \qquad \Longrightarrow \qquad Aw \in W. \qquad (**)$$

Definiramo sada polinom $P(\lambda)$ pomoću koeficijenata iz $(*)$:

$$P(\lambda) = \lambda^m - \alpha_1\lambda^{m-1} - \cdots - \alpha_{m-1}\lambda - \alpha_m.$$

Prema $(*)$ vidimo da je $P(A)v = 0$. Djelujemo li na tu jednakost bilo kojom potencijom A^k operatora A, zbog činjenice da operatori A^k i $P(A)$ komutiraju nalazimo $P(A)A^k v = 0$. Kako vektori oblika $A^k v$ razapinju potprostor W, zaključujemo da vrijedi

$$P(A)w = 0 \qquad \forall w \in W. \qquad (\dagger)$$

Razmatrat ćemo sada odvojeno dvije mogućnosti.

(a) $m = n$. Tada je $W = V$ pa slijedi $P(A) = 0$. Iz teorema 3.1 sada slijedi da je

$$\deg\, \mu_A(\lambda) \leq \deg\, P(\lambda) = m = n,$$

pa je u tom slučaju dokazana tvrdnja teorema.

(b) $m < n$. Promatramo tada kvocijentni prostor $U = V/W$ i definiramo linearan operator $B : U \to U$ relacijom

$$B(x + W) = Ax + W, \qquad x \in V.$$

Ova definicija ima smisla, jer desna strana ne ovisi o izboru predstavnika x klase $x + W \in U$. Doista, ako su $x, y \in V$ takvi da je $x + W = y + W$, onda je $x - y \in W$, pa iz $(**)$ slijedi $Ax - Ay = A(x - y) \in W$, dakle $Ax + W = Ay + W$.

Budući da je $\dim U = \dim V - \dim W = n - m < n$, po pretpostavci indukcije teorem vrijedi za prostor U i operator B. Dakle,

$$\deg\, \mu_B(\lambda) \leq n - m. \qquad (*)$$

Iz definicije operatora B slijedi da je $B^2(x+W) = B(Ax+W) = A^2x+W$. U stvari, indukcijom po k nalazimo da je $B^k(x+W) = A^kx+W$ $\forall k \in \mathbb{N}$ i $\forall x \in V$. Kako je polinom operatora linearna kombinacija potencija tog operatora, odatle slijedi da za svaki polinom $Q(\lambda)$ vrijedi

$$Q(B)(x+W) = Q(A)x+W, \qquad x \in V.$$

Kako je $\mu_B(B) = 0$, odatle zaključujemo

$$\mu_B(A)x+W = 0 \quad \text{u kvocijentnom prostoru U=V/W} \qquad \Longrightarrow \qquad \mu_B(A)x \in W \quad \forall x \in V.$$

Odatle i iz (†) slijedi $P(A)\mu_B(A)x = 0$ $\forall x \in V$, odnosno $P(A)\mu_B(A) = 0$. Sada iz teorema 3.1 i iz (∗) zaključujemo da je

$$\deg\, \mu_A(\lambda) \leq \deg\,[P(\lambda)\mu_B(\lambda)] = \deg\, P(\lambda) + \deg\, \mu_B(\lambda) \leq m + (n-m) = n.$$

Time je proveden korak indukcije, pa je teorem u potpunosti dokazan.

Na potpuno isti način kao za linearan operator definiramo minimalni polinom kvadratne matrice $A \in M_n(K)$: promatramo niz matrica $I, A, A^2, \ldots$ i uočimo najmanji m takav da je A^m linearna kombinacija nižih potencija matrice A :

$$A^m = \mu_1 A^{m-1} + \mu_2 A^{m-2} + \cdots + \mu_{m-1}A + \mu_m I.$$

Minimalni polinom matrice A tada je

$$\mu_A(\lambda) = \lambda - \mu_1\lambda^{m-1} - \cdots - \mu_{m-1}\lambda - \mu_m.$$

Podsjetimo se definicije i svojstava determinante. Determinanta je funkcija $\det : M_n(K) \to K$ definirana na skupu $M_n(K)$ svih kvadratnih matrica $n-$tog reda. Determinanta svakoj matrici A, s elementima α_{ij}, $1 \leq i,j \leq n$, pridružuje skalar $\det A$ definiran formulom:

$$\det A = \sum_{\sigma \in S(n)} \varepsilon(\sigma)\alpha_{1,\sigma(1)}\alpha_{2,\sigma(2)}\cdots\alpha_{n,\sigma(n)} = \sum_{\sigma \in S(n)} \varepsilon(\sigma)\alpha_{\sigma(1),1}\alpha_{\sigma(2),2}\cdots\alpha_{\sigma(n),n}.$$

Pri tome je $S(n)$ grupa permutacija skupa $\{1,2,\ldots,n\}$, a $\varepsilon(\sigma)$ je jednako 1 za parnu a -1 za neparnu permutaciju σ. Determinanta ima sljedeća svojstva:

(1) Ako je neki stupac (ili redak) matrice A sastavljen od samih nula, onda je $\det A = 0$.

(2) Ako je matrica B dobivena iz matrice A zamjenom dvaju stupaca (ili dvaju redaka), onda je $\det B = -\det A$.

(3) Ako je A gornjetrokutasta (ili donjetrokutasta) matrica kojoj su dijagonalni elementi $\alpha_1, \alpha_2, \ldots, \alpha_n$, onda je $\det A = \alpha_1\alpha_2\cdots\alpha_n$.

(4) Ako je matrica B dobivena iz matrice A tako da su svi elementi nekog stupca (ili retka) pomnoženi istim skalarom α, onda je $\det B = \alpha \det A$.

(5) Ako je matrica B dobivena iz matrice A tako da je nekom stupcu dodan drugi stupac pomnožen bilo kojim skalarom α (ili je nekom retku dodan drugi redak pomnožen s α), onda je $\det B = \det A$.

(6) Za transponiranu matricu A' matrice A vrijedi $\det A' = \det A$.

Za kvadratnu matricu $A \in M_n(K)$ s elementima α_{ij} $(i, j = 1, 2, \ldots, n)$ njena **adjunkta** je kvadratna matrica $\widetilde{A} \in M_n(K)$ čiji je element na presjecištu $k-$tog retka i $i-$tog stupca jednak $\beta_{ki} = (-1)^{i+k} \det A_{ik}$, a A_{ik} je matrica iz $M_{n-1}(K)$ koja se iz matrice A dobiva brisanjem $i-$tog retka i $k-$tog stupca.

(7) Vrijedi $\widetilde{A}A = A\widetilde{A} = (\det A)I$, odnosno

$$\sum_{k=1}^{n} (-1)^{i+k} \alpha_{jk} \det A_{ik} = \delta_{ij} \det A, \qquad i, j \in \{1, 2, \ldots, n\},$$

$$\sum_{k=1}^{n} (-1)^{i+k} \alpha_{kj} \det A_{ki} = \delta_{ij} \det A, \qquad i, j \in \{1, 2, \ldots, n\}.$$

Prva od gornjih jednakosti predstavlja tzv. *razvoj determinante po $j-$tom retku* matrice A, a druga *razvoj po $j-$tom stupcu* te matrice.

Pored svojstava **(1)** – **(7)** vrijedi i tzv. Binnet-Cauchyjev teorem:

Teorem 3.5 *Za matrice $A, B \in M_n(K)$ je $\det(AB) = (\det A)(\det B)$.*

Iz tog teorema i iz svojstva **(7)** slijedi:

Korolar 3.1 *Matrica A je regularna ako i samo ako je $\det A \neq 0$. U tom slučaju je $A^{-1} = \frac{1}{\det A}\widetilde{A}$.*

Dokaz: Ako je A regularna, iz $AA^{-1} = I$ zbog teorema 3.5 slijedi $(\det A)(\det A^{-1}) = \det I = 1$. Prema tome je $\det A \neq 0$.

Pretpostavimo sada da je $\det A \neq 0$ i stavimo $B = \frac{1}{\det A}\widetilde{A}$. Tada iz svojstva **(7)** slijedi $BA = AB = I$, dakle A je regularna i $A^{-1} = B$.

Za kvadratnu matricu $A = [\alpha_{ij}] \in M_n(K)$ definiramo polinom

$$\kappa_A(\lambda) = \det(\lambda I - A) = \begin{bmatrix} \lambda - \alpha_{11} & -\alpha_{12} & \cdots & -\alpha_{1n} \\ -\alpha_{21} & \lambda - \alpha_{22} & \cdots & -\alpha_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ -\alpha_{n1} & -\alpha_{n2} & \cdots & \lambda - \alpha_{nn} \end{bmatrix}.$$

$\kappa_A(\lambda)$ se zove **svojstveni** (ili **karakteristični**) **polinom** matrice A. Ako je $A \in M_n(K)$, njen svojstveni polinom $\kappa_A(\lambda)$ je normiran i $\deg \kappa_A(\lambda) = n$:

$$\kappa_A(\lambda) = \lambda^n - \sigma_1 \lambda^{n-1} - \cdots - \sigma_{n-2}\lambda^2 - \sigma_{n-1}\lambda - \sigma_n.$$

Teorem 3.6 (Hamilton-Cayley) *Svaka matrica $A \in M_n(K)$ poništava svoj svojstveni polinom: $\kappa_A(A) = 0$.*

Dokaz: Označimo sa $B(\lambda)$ adjunktu matrice $\lambda I - A$. Po definiciji adjunkte je

$$B(\lambda) = \begin{bmatrix} \beta_{11}(\lambda) & \beta_{12}(\lambda) & \cdots & \beta_{1n}(\lambda) \\ \beta_{21}(\lambda) & \beta_{22}(\lambda) & \cdots & \beta_{2n}(\lambda) \\ \vdots & \vdots & \ddots & \vdots \\ \beta_{n1}(\lambda) & \beta_{n2}(\lambda) & \cdots & \beta_{nn}(\lambda) \end{bmatrix},$$

pri čemu je $\beta_{ij}(\lambda) = (-1)^{i+j}\det(\lambda I - A)_{ji}$, a $(\lambda I - A)_{ji}$ je kvadratna matrica reda $n-1$ koja se iz matrice $\lambda I - A$ dobije brisanjem $j-$tog retka i $i-$tog stupca. Stoga je svaki matrični element $\beta_{ij}(\lambda)$ polinom stupnja $\leq n-1$:

$$\beta_{ij}(\lambda) = \alpha_{ij;n-1}\lambda^{n-1} + \alpha_{ij;n-2}\lambda^{n-2} + \cdots + \alpha_{ij;2}\lambda^2 + \alpha_{ij;1}\lambda + \alpha_{ij;0}.$$

Prema tome, možemo pisati

$$B(\lambda) = \lambda^{n-1}A_{n-1}\lambda^{n-1} + \lambda^{n-2}A_{n-2} + \cdots + \lambda^2 A_2 + \lambda A_1 + A_0,$$

uz oznaku

$$A_k = \begin{bmatrix} \alpha_{11;k} & \alpha_{12;k} & \cdots & \alpha_{1n;k} \\ \alpha_{21;k} & \alpha_{22;k} & \cdots & \alpha_{2n;k} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_{n1;k} & \alpha_{n2;k} & \cdots & \alpha_{nn;k} \end{bmatrix}, \qquad k = 0, 1, \ldots, n-1.$$

Prema svojstvu **(7)** primijenjenom na matricu $\lambda I - A$ nalazimo da vrijedi

$$(\lambda I - A) \cdot B(\lambda) = \det(\lambda I - A) \cdot I,$$

tj.

$$(\lambda I - A)\cdot(\lambda^{n-1}A_{n-1} + \lambda^{n-2}A_{n-2} + \cdots + \lambda^2 A_2 + \lambda A_1 + A_0) = (\lambda^n - \sigma_1\lambda^{n-1} - \cdots - \sigma_{n-2}\lambda^2 - \sigma_{n-1}\lambda - \sigma_n)\cdot I.$$

Ako su dva polinoma jednaka onda su im jednaki odgovarajući koeficijenti pa iz gornje jednakosti dobivamo sljedećih $n+1$ jednakosti koeficijenata uz potencije $\lambda^n, \lambda^{n-1}, \lambda^{n-2}, \ldots, \lambda^j, \ldots, \lambda^1, \lambda^0$:

$$\begin{aligned} A_{n-1} &= I, \\ -AA_{n-1} + A_{n-2} &= -\sigma_1 I, \\ -AA_{n-2} + A_{n-3} &= -\sigma_2 I, \\ &\vdots \\ -AA_{n-j} + A_{n-j-1} &= -\sigma_j I, \\ &\vdots \\ -AA_1 + A_0 &= -\sigma_{n-1} I, \\ -AA_0 &= -\sigma_n I. \end{aligned}$$

Iz prvih n gornjih jednakosti dobivamo redom:

$$\begin{aligned} A_{n-1} &= I, \\ A_{n-2} &= A - \sigma_1 I, \\ A_{n-3} &= A^2 - \sigma_1 A - \sigma_2 I, \\ &\vdots \\ A_{n-j-1} &= A^j - \sigma_1 A^{j-1} - \ldots - \sigma_{j-1}A - \sigma_j I, \\ &\vdots \\ A_0 &= A^{n-1} - \sigma_1 A^{n-2} - \ldots - \sigma_{n-2}A - \sigma_{n-1} I. \end{aligned}$$

Posljednja od prethodnih $n+1$ jednakosti može se napisati $AA_0 - \sigma_n I = 0$ i uvrstimo li u nju gornji izraz za A_0 dobivamo upravo tvrdnju teorema:

$$A^n - \sigma_1 A^{n-1} - \ldots - \sigma_{n-1}A - \sigma_n I = 0.$$

Neka je V konačnodimenzionalan vektorski prostor, $A \in L(V)$, i neka su e i e' dvije baze od V. Označimo sa $S \in GL(V)$ operator prijelaza iz baze e u bazu e' (dakle, $Se_j = e'_j, 1 \leq j \leq n$). Tada po propoziciji 2.4 za matrice operatora A u te dvije baze vrijedi $A(e') = S(e)^{-1}A(e)S(e)$. Po Binnet-Cauchyjevom teoremu 3.5 slijedi

$$\det A(e') = (\det(S(e)^{-1})) \cdot (\det A(e)) \cdot (\det S(e)).$$

Zbog $S(e)^{-1}S(e) = I$ imamo $(\det(S(e)^{-1})) \cdot (\det S(e)) = \det I = 1$, pa iz gornje jednakosti dobivamo

$$\det A(e') = \det A(e).$$

Drugim riječima, determinanta matrice operatora ne ovisi o izboru baze. Stoga pojam determinante možemo proširiti i na operatore i definirati **determinantu operatora**:

$$\det A = \det A(e), \qquad A \in L(V), \qquad e \text{ bilo koja baza prostora } V.$$

Iz teorema 3.5 i njegovoga korolara 3.1 neposredno slijedi:

Teorem 3.7 *Neka je V konačnodimenzionalan vektorski prostor i $A, B \in L(V)$.*

(*a*) *Vrijedi* $\det(AB) = (\det A)(\det B)$.

(*b*) *Operator A je regularan, tj. $A \in GL(V)$, ako i samo ako je* $\det A \neq 0$.

Uz oznake prije teorema 3.7 imamo:

$$\lambda I - A(e') = \lambda I - S(e)^{-1}A(e)S(e) = S(e)^{-1}(\lambda I - A(e))S(e).$$

Odavde slijedi $\kappa_{A(e)}(\lambda) = \kappa_{A(e')}(\lambda)$, dakle svojstveni polinom matrice operatora ne ovisi o tome koju smo bazu odabrali. Stoga možemo definirati **svojstveni** (ili **karakteristični**) **polinom operatora**:

$$\kappa_A(\lambda) = \kappa_{A(e)}(\lambda), \qquad A \in L(V), \qquad e \text{ bilo koja baza prostora } V.$$

Teorem 3.8 *Neka je V konačnodimenzionalan vektorski prostor i $A \in L(V)$.*

(*a*) $\kappa_A(A) = 0$.

(*b*) *Svojstveni polinom $\kappa_A(\lambda)$ djeljiv je s minimalnim polinomom $\mu_A(\lambda)$.*

(*c*) $\sigma(A) = \{\lambda \in K; \kappa_A(\lambda) = 0\}$.

Dokaz: Tvrdnja (a) slijedi iz teorema 3.6, a tvrdnja (b) je neposredna posljedica te tvrdnje (a) i tvrdnje (c) teorema 3.1. Napokon, zbog tvrdnje (b) teorema 3.7 imamo redom:

$$\lambda \in \sigma(A) \iff \lambda I - A \notin GL(V) \iff \det(\lambda I - A) = 0 \iff \kappa_A(\lambda) = 0.$$

Time je i tvrdnja (c) dokazana.

4 Invarijantni potprostori

Neka je V vektorski prostor nad poljem K i $A \in L(V)$. **Potprostor** $W \leq V$ zove se $A-$**invarijantan** (ili **potprostor invarijantan s obzirom na operator** A) ako vrijedi

$$w \in W \qquad \Longrightarrow \qquad Aw \in W,$$

odnosno ako je $AW \subseteq W$.

Pretpostavimo da je W jednodimenzionalan $A-$invarijantan potprostor od V. Za bilo koji $w \in W, w \neq 0$, je tada $W = [\{w\}] = \{\lambda w;\ \lambda \in K\}$. $Aw \in [\{w\}]$ znači da postoji $\lambda \in K$ takav da je $Aw = \lambda w$. Dakle, tada su svi wektori iz W svojstveni vektori operatora A.

Za $\lambda \in \sigma(A)$ upotrebljavat ćemo oznaku:

$$V_\lambda(A) = N(\lambda I - A) = \{v \in V; Av = \lambda v\}.$$

Dakle, $V_\lambda(A)$ je potprostor koji se sastoji od svih svojstvenih vektora operatora A za svojstvenu vrijednost λ.

Ako je W $A-$invarijantni potprostor od V, onda je restrikcija $A \mid W \in L(W)$. Očito je $W_\lambda(A|W) = W \cap V_\lambda(A)$ i $\sigma(A|W) \subseteq \sigma(A)$. Precizno:

$$\sigma(A|W) = \{\lambda \in \sigma(A);\ W \cap V_\lambda(A) \neq \{0\}\}.$$

Pretpostavimo da je $V = V_1 \dot{+} V_2$, pri čemu su V_1 i V_2 $A-$invarijantni potprostori od V. Ako je $e' = \{e_1, e_2, \ldots, e_k\}$ baza od V_1 i $e'' = \{e_{k+1}, e_{k+2}, \ldots, e_n\}$ baza od V_2, onda je $e = \{e_1, e_2, \ldots, e_n\}$ baza od V. Nadalje, matrica $A(e)$ ima u u gornjem lijevom dijelu matricu $(A\,|\,V_1)(e')$, u donjem desnom dijelu matricu $(A|V_2)(e'')$, a ostali elementi su svi jednaki nuli:

$$A(e) \;=\; \begin{bmatrix} (A|V_1)(e') & \vdots & 0 \\ \cdots\cdots\cdots & \vdots & \cdots\cdots\cdots \\ 0 & \vdots & (A|V_2)(e'') \end{bmatrix}$$

Općenitije, ako je $V = V_1 \dot{+} V_2 \dot{+} \ldots \dot{+} V_s$, pri čemu su svi potprostori V_j $(j = 1, 2, \ldots, s)$ $A-$invarijantni, neka je za svako $j \in \{1, 2, \ldots, s\}$ $e^{(j)}$ baza od V_j. Neka je e baza složena redom od tih baza $e^{(1)}, e^{(2)}, \ldots, e^{(s)}$. Tada matrica $A(e)$ ima redom na dijagonali od gornjeg lijevog do donjeg desnog kuta matrice $(A \mid V_1)(e^{(1)}), (A \mid V_2)(e^{(2)}), \ldots, (A \mid V_s)(e^{(s)})$, a sve ostalo su nule. Posebno, matrica operatora A je tim jednostavnija i tim je lakše s njom računati čim je finiji rastav prostora V u direktnu sumu $A-$invarijantnih potprostora. Najjednostavnije je ako su svi potprostori jednodimenzionalni. Tada se odgovarajuća baza e sastoji od svojstvenih vektora operatora A i $A(e)$ je dijagonalna matrica sa svojstvenim vrijednostima na dijagonali.

Neka je $V = X \dot{+} Y$. Tada se svaki vektor $v \in V$ može na jedinstven način napisati u obliku $v = x + y$, $x \in X$, $y \in Y$. Stoga možemo definirati $P : V \to V$ relacijom $P(v) = x$. Očito je $P \in L(V)$, $R(P) = X$, $N(P) = Y$. Nadalje, $X = R(P) = \{v \in V; Pv = v\}$. Tako definiran linearan operator P zove se **projektor** prostora V na potprostor X duž potprostora Y.

Propozicija 4.1 *Operator $P \in L(V)$ je projektor ako i samo ako je $P^2 = P$. Tada je $V = R(P) \dot{+} N(P)$ i P je projektor na $R(P)$ duž $N(P)$.*

Dokaz: Pretpostavimo da je P projektor na X duž Y. Tada je $V = X \dot{+} Y$ i vrijedi $X = R(P)$ i $Y = N(P)$. Za $x \in X$ je $Px = x$. Prema tome, za $v = x + y$, $x \in X$, $y \in Y$, imamo $P^2v = Px =$

$x = Pv$. To pokazuje da je $P^2v = Pv\ \forall v \in V$, dakle $P^2 = P$.

Obratno, pretpostavimo sada da je $P^2 = P$ i dokažimo da je P projektor na $R(P)$ duž $N(P)$. Neka je $v \in R(P) \cap N(P)$. Tada je $Pv = 0$ i $v = Pw$ za neki $w \in V$. Slijedi

$$0 = Pv = P^2w = Pw = v.$$

Dakle, $R(P) \cap N(P) = \{0\}$ pa je suma potprostora $R(P)$ i $N(P)$ direktna. Za svaki $v \in V$ možemo pisati $v = Pv + (v - Pv)$; imamo $Pv \in R(P)$ i

$$P(v - Pv) = Pv - P^2v = Pv - Pv = 0,$$

dakle $v - Pv \in N(P)$. Time je dokazano $V = R(P) \dotplus N(P)$. Za $x \in R(P)$ je $x = Pz$ za neki $z \in V$, pa je $Px = P^2z = Pz = x$. Stoga za $v \in V$, $v = x + y$, $x \in R(P)$, $y \in N(P)$, imamo $Pv = Px + Py = x$. Time je dokazano da je P projektor na $R(P)$ duž $N(P)$.

Ako je P projektor onda je $(I - P)^2 = I - 2P + P^2 = I - P$, dakle $I - P$ je projektor. Očito je $R(I - P) = N(P)$ i $N(I - P) = R(P)$. Dakle, ako je P projektor na X duž Y, onda je $I - P$ projektor na Y duž X.

Propozicija 4.2 *Neka je $A \in L(V)$ i $W \leq V$ i neka je $P \in L(V)$ neki projektor prostora V na potprostor W. Potprostor W je $A-$invarijantan ako i samo ako je $AP = PAP$.*

Dokaz: Pretpostavimo da je potprostor W $A-$invarijantan. Neka je P projektor na W duž nekog potprostora U (naravno, takvog da je $V = W \dotplus U$) i neka je $v \in V$. Neka su $w \in W$ i $u \in U$ takvi da je $v = w + u$. Tada je $Pv = w$, pa je $APv = Aw$. Međutim, po pretpostavci je potprostor W $A-$invarijantan pa je $Aw \in W$. Dakle, za svaki $v \in V$ je $APv \in W$. Kako je $W = R(P) = \{x \in V; Px = x\}$ zaključujemo da je $PAPv = APv$. To vrijedi za svaki $v \in V$ pa slijedi $PAP = AP$.

Pretpostavimo sada da je $AP = PAP$. Za $w \in W = R(P)$ je $Pw = w$, pa zbog jednakosti $AP = PAP$ zaključujemo

$$Aw = APw = PAPw \in R(P) = W.$$

Dakle, potprostor W je $A-$invarijantan.

Propozicija 4.3 *Neka je $A \in L(V)$, $V = W \dotplus U$, i neka je P projektor na W duž U. Tada vrijedi $AP = PA$ ako i samo ako su i W i U $A-$invarijantni.*

Dokaz: Ako su W i U $A-$invarijantni, onda iz propozicije 4.2 slijedi

$$AP = PAP \qquad \text{i} \qquad A(I - P) = (I - P)A(I - P).$$

Iz druge jednakosti slijedi

$$A - AP = A - AP - PA + PAP, \qquad \text{dakle} \qquad PA = PAP.$$

Odatle i iz $AP = PAP$ zaključujemo da vrijedi $AP = PA$.

Pretpostavimo da je $AP = PA$. Tada je $PAP = AP^2 = AP$, pa po propoziciji 4.2 zaključujemo da je potprostor W $A-$invarijantan. $I - P$ je projektor na U duž W. Imamo redom

$$(I - P)A(I - P) = A - PA - AP + PAP = A - PA = A - AP = A(I - P).$$

Stoga je i potprostor U $A-$invarijantan.

Neka je

$$V = V_1 \dot{+} \ldots \dot{+} V_s$$

i neka je P_i projektor na V_i duž potprostora

$$U_i = V_1 \dot{+} \ldots \dot{+} V_{i-1} \dot{+} V_{i+1} \dot{+} \ldots \dot{+} V_s.$$

Dakle, ako je $v \in V$ i $v = v_1 + \ldots + v_s$, $v_1 \in V_1, \ldots, v_s \in V_s$, onda je $P_i v = v_i$, pa slijedi

$$v = P_1 v + \ldots + P_s v = (P_1 + \ldots + P_s)v.$$

Kako to vrijedi za svaki $v \in V$, zaključujemo da je $I = P_1 + \ldots P_s$. Nadalje, za $v \in V$ i za $i \neq j$ imamo $P_j v \in V_j \subseteq N(P_i)$, dakle $P_i P_j v = 0$. To pokazuje da je $P_i P_j = 0$ za $i \neq j$. Zajedno sa $P_i^2 = P_i$ to možemo pisati ovako:

$$P_i P_j = \delta_{ij} P_i, \qquad i, j \in \{1, 2, \ldots, s\}.$$

Konačan niz operatora $(P_1, \ldots, P_s)$ sa svojstvima

$$I = P_1 + \ldots + P_s, \qquad P_i P_j = \delta_{ij} P_i \qquad \forall i, j \in \{1, 2, \ldots, s\}$$

zove se **dekompozicija jedinice**. U tom slučaju imamo rastav prostora V u direktnu sumu potprostora:

$$V = R(P_1) \dot{+} \ldots \dot{+} R(P_s).$$

Nadalje, svi potprostori $R(P_i)$ su $A-$invarijantni ako i samo ako operator A komutira sa svim projektorima $P_1, \ldots, P_s$.

5 Nilpotentni operatori i Fittingova dekompozicija

Jedna od osnovnih metoda za nalaženje $B-$invarijantnih potprostora za neki $B \in L(V)$ je sljedeća jednostavna činjenica:

Lema 5.1 *Neka je V vektorski prostor i $A, B \in L(V)$ linearni operatori koji komutiraju, tj. $AB = BA$. Potprostori $N(A)$ i $R(A)$ su tada $B-$invarijantni. Posebno, ako je $P(\lambda)$ polinom, potprostori $N(P(A))$ i $R(P(A))$ su $B-$invarijantni.*

Dokaz: Ako je $v \in N(A)$ onda imamo $ABv = BAv = 0$, dakle vrijedi $Av \in N(B)$. Prema tome, potprostor $N(A)$ je $B-$invarijantan.

Neka je $v \in R(A)$ i neka je $w \in V$ takav da je $v = Aw$. Imamo $Bv = BAw = = ABw \in R(B)$. Dakle, potprostor $R(A)$ je $B-$invarijantan.

Ako je $BA = AB$, onda je i $BA^k = A^k B \ \ \forall k \in \mathbb{N}$, pa su svi potprostori iz rastućeg niza

$$N(A) \subseteq N(A^2) \subseteq N(A^3) \subseteq \cdots\cdots$$

i svi potprostori iz padajućeg niza

$$R(A) \supseteq R(A^2) \supseteq R(A^3) \supseteq \cdots\cdots$$

$B-$invarijantni.

Propozicija 5.1 *Neka je V vektorski prostor i $A \in L(V)$.*

(a) Ako je $N(A^k) = N(A^{k+1})$ za neko k, onda je $N(A^m) = N(A^k)$ $\forall m \geq k$.

(b) Ako je $R(A^k) = R(A^{k+1})$ za neko k, onda je $R(A^m) = R(A^k)$ $\forall m \geq k$.

Dokaz: (a) Dovoljno je dokazati da je $N(A^{k+2}) = N(A^{k+1})$, jer tada tvrdnja slijedi indukcijom u odnosu na $m > k$. Očito je $N(A^{k+2}) \supseteq N(A^{k+1})$. Dokažimo i obrnutu inkluziju. Neka je $v \in N(A^{k+2})$. Tada imamo

$$0 = A^{k+2}v = A^{k+1}(Av) \ \Rightarrow \ Av \in N(A^{k+1}) = N(A^k) \ \Rightarrow \ 0 = A^k(Av) = A^{k+1}v \ \Rightarrow \ v \in N(A^{k+1}).$$

Dakle, vrijedi i $N(A^{k+2}) \subseteq N(A^{k+1})$.

(b) Analogno, dovoljno je dokazati $R(A^{k+1}) \subseteq R(A^{k+2})$. Neka je $v \in R(A^{k+1})$ i neka je $w \in V$ takav da je $v = A^{k+1}w = A(A^k w)$. Imamo $A^k w \in R(A^k)$, pa zbog pretpostavke da je $R(A^k) = R(A^{k+1})$ zaključujemo da je $A^k w \in R(A^{k+1})$. Dakle, postoji $u \in V$ takav da je $A^k w = A^{k+1}u$. Slijedi

$$v = A^{k+1}(w) = A(A^k w) = A(A^{k+1}u) = A^{k+2}u \in R(A^{k+2}).$$

Time je dokazana i obrnuta inkluzija $R(A^{k+1}) \subseteq R(A^{k+2})$, dakle vrijedi $R(A^{k+1}) = R(A^{k+2})$.

Ako je prostor V konačnodimenzionalan, niz jezgara (odnosno, slika) potencija operatora A ne može biti striktno rastući (odnosno, striktno padajući), jer svaki sljedeći striktno veći (odnosno, striktno manji) član ima dimenziju veću (odnosno, manju) barem za 1. Stoga postoje $k \leq \dim V$ i $r \leq \dim V$ takvi da vrijedi $N(A^m) = N(A^k)$ $\forall m \geq k$ i $R(A^m) = R(A^r)$ $\forall m \geq r$.

Teorem 5.1 *Neka je $V \neq \{0\}$ vektorski prostor i $A \in L(V)$. Pretpostavimo da postoje k i r takvi da je $N(A^k) = N(A^{k+1})$ i $R(A^r) = R(A^{r+1})$ i neka su k i r najmanji takvi. Tada vrijedi $k = r$ i $V = N(A^k) \dotplus R(A^k)$.*

Dokaz: Razmatrat ćemo posebno slučaj konačnodimenzionalnog prostora V, jer će nam kasnije samo taj slučaj trebati i jer je dokaz u tom slučaju znatno jednostavniji. Po teoremu o rangu i defektu (teorem 2.3) vrijedi jednakost $\dim N(A^j) + \dim R(A^j) = \dim V$ za svaki j, dakle vrijedi:

$$N(A^j) = N(A^{j+1}) \qquad \Longleftrightarrow \qquad R(A^j) = R(A^{j+1}).$$

Stoga je očito $k = r$ (i taj je broj $\leq \dim V$). Neka je $v \in N(A^k) \cap R(A^k)$. Tada je $v = A^k w$ za neki $w \in V$. Međutim,

$$0 = A^k v = A^{2k} w \qquad \Longrightarrow \qquad w \in N(A^{2k}) = N(A^k) \qquad \Longrightarrow \qquad v = A^k w = 0.$$

Dakle, $N(A^k) \cap R(A^k) = \{0\}$. Stoga je suma potprostora $N(A^k)$ i $R(A^k)$ direktna, a odatle i iz teorema o rangu i defektu slijedi

$$\dim(N(A^k) \dot{+} R(A^k)) = \dim N(A^k) + \dim R(A^k) = \dim V.$$

Dakle, $V = N(A^k) \dot{+} R(A^k)$.

Dokažimo sada teorem i u općem slučaju, tj. bez pretpostavke da je prostor V konačnodimenzionalan.

Ako je $k = 0$ očito je $r \geq k$. Pretpostavimo da je $k \geq 1$. Neka je $v \in N(A^k) \setminus N(A^{k-1})$, dakle $A^k v = 0$ i $A^{k-1} v \neq 0$. Pretpostavimo da je $r < k$, tj. $R(A^{k-1}) = R(A^k)$. Tada postoji $w \in V$ takav da je $A^{k-1} v = A^k w$. Slijedi

$$0 = A^k v = A^{k+1} w \qquad \Longrightarrow \qquad w \in N(A^{k+1}) = N(A^k) \qquad \Longrightarrow \qquad A^{k-1} v = A^k w = 0$$

suprotno pretpostavci. Ova kontradikcija pokazuje da je pretpostavka $r < k$ bila netočna, pa zaključujemo da mora biti $r \geq k$.

Ako je $r = 0$ očito je $k \geq r$. Pretpostavimo da je $r \geq 1$. Neka je $v \in R(A^{r-1}) \setminus R(A^r)$. Tada je $v = A^{r-1} w$ za neki $w \in V$. Stavimo $u = Av$. Tada je $u = A^r w \in R(A^r) = R(A^{r+1})$, pa postoji $x \in V$ takav da je $u = A^{r+1} x$. Stavimo $y = Ax - w$. Tada je

$$A^r y = A^{r+1} x - A^r w = u - u = 0 \;\text{ i }\; A^{r-1} y = A^r x - A^{r-1} w = A^r x - v \neq 0,$$

jer $v \notin R(A^r)$. Prema tome je $y \in N(A^r) \setminus N(A^{r-1})$. To pokazuje da je $N(A^{r-1}) \subsetneq N(A^r)$, dakle $k \geq r$.

Dvije dokazane nejednakosti $r \geq k$ i $k \geq r$ daju jednakost $k = r$.

Dokaz da je $N(A^k) \cap R(A^k) = \{0\}$ nije koristio pretpostavku konačnodimenzionalnosti, pa vrijedi i u općem slučaju. Neka je $v \in V$. Tada je $A^k v \in R(A^k) = R(A^{2k}) = A^k R(A^k)$, pa postoji $w \in R(A^k)$ takav da je $A^k v = A^k w$. Stavimo $u = v - w$. Tada je $v = u + w, w \in R(A^k), u \in N(A^k)$. Time je dokazano da vrijedi $V = N(A^k) \dot{+} R(A^k)$.

Neka je $V \neq \{0\}$ konačnodimenzionalan vektorski prostor i $A \in L(V)$. Broj k iz teorema 5.1 zove se **nilindeks operatora** A i označava sa $\nu(A)$. Imamo $\nu(A) \leq \dim V$. Ako je $\nu(A) > 0$, tj. ako A nije regularan, onda vrijedi $N(A^{\nu(A)-1}) \subsetneq N(A^{\nu(A)})$; štoviše, vrijedi $N(A^{j-1}) \subsetneq N(A^j)$ $\forall j \leq \nu(A)$; također, $R(A^j) \subsetneq R(A^{j-1})$ $\forall j \leq \nu(A)$.

Za konačnodimenzionalan vektorski prostor V, za $A \in L(V)$ i za $k = \nu(A)$, potprostor $V^0(A) = N(A^k)$ zove se **Fittingova** $0-$**komponenta prostora** V, a $V^1(A) = R(A^k)$ zove se **Fittingova** $1-$**komponenta prostora** V (u odnosu na operator A). Rastav

$$V = V^0(A) \dot{+} V^1(A)$$

zove se **Fittingova dekompozicija prostora** V **u odnosu na operator** A. Operator $A|V^0(A)$ je **Fittingova** $0-$**komponenta operatora** A, a $A \mid V^1(A)$ je **Fittingova** $1-$**komponenta**

operatora A.

Operator $A \in L(V)$ zove se **nilpotentan** ako je $A^k = 0$ za neki k. Najmanji takav k zove se **indeks nilpotentnosti** operatora A; kažemo da je A nilpotentan indeksa k. Očito je tada $k = \nu(A)$ i $V^0(A) = V$.

Teorem 5.2 *Neka je V konačnodimenzionalan vektorski prostor, $A \in L(V)$ i neka je $k = \nu(A)$.*

(*a*) *Restrikcija $A \,|\, V^0(A) \in L(V^0(A))$ je nilpotentan operator indeksa k. Ako je W potprostor od V koji je $A-$invarijantan i takav da je restrikcija $A \,|\, W$ nilpotentan operator, onda je $W \subseteq V^0(A)$.*

(*b*) *Restrikcija $A \,|\, V^1(A) \in L(V^1(A))$ je regularan operator na prostoru $V^1(A)$, $A \,|\, V^1(A) \in GL(V^1(A))$. Ako je W potprostor od V koji je $A-$invarijantan i takav da je $A|W \in GL(W)$, onda je $W \subseteq V^1(A)$.*

Dokaz: (*a*) Za $C = A \,|\, V^0(A)$ očito vrijedi $C^k = 0$ i $C^{k-1} \neq 0$. Dakle, operator C je nilpotentan indeksa $k = \nu(A)$. Pretpostavimo sada da je W $A-$invarijantan potprostor od V takav da je operator $D = A \,|\, W$ nilpotentan, $D^j = 0$. Tada je $A^j w = 0$ $\forall w \in W$, pa slijedi da je $W \subseteq N(A^j) \subseteq V^0(A)$.

(*b*) Imamo $AV^1(A) = AR(A^k) = R(A^{k+1}) = R(A^k) = V^1(A)$. Dakle, $A \,|\, V^1(A)$ je surjektivan operator, a kako se radi o konačnodimenzionalnom prostoru slijedi da je $E \in GL(V^1(A))$. Pretpostavimo sada da je potprostor W $A-$invarijantan i takav da je operator $A \,|\, W$ regularan, $A|W \in GL(W)$. Tada imamo redom

$$AW = W \quad \Longrightarrow \quad A^j W = W \ \ \forall j \quad \Longrightarrow \quad W \subseteq R(A^j) \ \ \forall j \quad \Longrightarrow \quad W \subseteq V^1(A).$$

Time je teorem u potpunosti dokazan.

Pobliže ćemo sada proučiti nilpotentne operatore. Neka je $A \in L(V)$ nilpotentan operator indeksa p, dakle $A^p = 0$ i $A^{p-1} \neq 0$. Tada vrijedi $p = \nu(A)$, $V^0(A) = N(A^p) = V$ i $V^1(A) = \{0\}$. Iz teorema 5.1 je jasno da je $p \leq \dim V$. No to slijedi i iz sljedeće propozicije:

Propozicija 5.2 *Neka je $A \in L(V)$ nilpotentan operator indeksa p i neka je $v \in V$ takav da je $A^{p-1}v \neq 0$ (tj. $v \in V \setminus N(A^{p-1})$). Tada su vektori $v, Av, A^2v, \ldots A^{p-1}v$ linearno nezavisni.*

Dokaz: Neka je

$$\alpha_0 v + \alpha_1 Av + \alpha_2 A^2 v + \ldots + \alpha_{p-1} A^{p-1} v = 0.$$

Ako na tu jednakost djelujemo s operatorom A^{p-1}, dobivamo

$$\alpha_0 A^{p-1} v + \alpha_1 A^p v + \alpha_2 A^{p+1} v + \ldots + \alpha_{p-1} A^{2p-2} v = 0.$$

Međutim, $A^j = 0$ za $j = p, p+1, \ldots, 2p-2$, pa slijedi $\alpha_0 A^{p-1} v = 0$. Kako je $A^{p-1} v \neq 0$, zaključujemo da je $\alpha_0 = 0$. Sada slijedi

$$\alpha_1 Av + \alpha_2 A^2 v + \ldots + \alpha_{p-1} A^{p-1} v = 0.$$

Na tu jednakost djelujemo s operatorom A^{p-2}. Slijedi $\alpha_1 A^{p-1} v = 0$, a odatle $\alpha_1 = 0$. Korak po korak primjenom operatora $A^{p-3}, A^{p-4}, \ldots, A$, dobivamo da su $\alpha_2 = 0$, $\alpha_3 = 0$, $\ldots$, $\alpha_{p-1} = 0$ i time je propozicija dokazana.

Na svakom konačnodimenzionalnom vektorskom prostoru postoji nilpotentan operator indeksa $n = \dim V$. Doista, neka je $e = \{e_1, e_2, \ldots, e_n\}$ baza od V i neka je A linearan operator na prostoru V zadan sa:

$$Ae_1 = 0, \ \ Ae_j = e_{j-1} \text{ za } j = 2, \ldots, n.$$

Tada je $A^n = 0$ i $A^{n-1}e_1 = e_n \neq 0$, dakle $A^{n-1} \neq 0$. Prema tome A je operator indeksa n. Matrica operatora A u bazi e, $A(e) = [\alpha_{ij}]$ ima sve elementa jednake nuli osim $n-1$ elemenata na prvoj gornjoj paraleli uz glavnu dijagonalu gdje su jedinice: $\alpha_{ij} = 0$ za $j \neq i+1$, $\alpha_{i,i+1} = 1$ za $i = 1, 2, \ldots, n-1$. Ta se matrica zove **elementarna Jordanova klijetka** $n-$tog reda i označava J_n :

$$J(n) = \begin{bmatrix} 0 & 1 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 1 \\ 0 & 0 & 0 & 0 & \cdots & 0 \end{bmatrix}$$

Ako je $A \in L(V)$ bilo koji nilpotentan operator indeksa $n = \dim V$, izaberimo vektor $v \in V$ takav da je $A^{n-1}v \neq 0$. Tada su po propoziciji 5.2 vektori $v, Av, A^2v, \ldots, A^{n-1}v$ linearno nezavisni. Budući da ih ima n oni tvore bazu od V. Numerirajmo ih u obrnutom redoslijedu: $e_j = A^{n-j}v$, $1 \leq j \leq n$. Tada je očito $Ae_1 = 0$ i $Ae_j = e_{j-1}$ za $j = 2, \ldots, n$. Stoga je matrica operatora A u bazi $e = \{e_1, e_2, \ldots, e_n\}$ upravo elementarna Jordanova klijetka $n-$tog reda: $A(e) = J_n$.

Teorem 5.3 *Neka je $A \in L(V)$ nilpotentan operator indeksa $n = \dim V$.*

(a) *Postoji baza e od V takva da je $A(e) = J_n$.*

(b) *Ako je $B \in L(V)$ takav da je $AB = BA$, onda postoji polinom P takav da je $B = P(A)$.*

Dokaz: Tvrdnja (a) dokazana je prije iskaza teorema. Dokažimo tvrdnju (b). Neka je e baza iz tvrdnje (a) i $B(e) = [\beta_{ij}]$. Izračunavanjem elemenata lijeve i desne strane matrične jednakosti $J_nB(e) = B(e)J_n$ dobivamo:

$$\beta_{i+1,j} = \beta_{i,j-1}, \ \ 1 \leq i \leq n-1, \ \ 2 \leq j \leq n; \qquad \beta_{i+1,1} = 0, \ \ 1 \leq i \leq n-1; \qquad 0 = \beta_{n,j-1}, \ \ 2 \leq j \leq n.$$

Odavde slijedi:

$$\beta_{ij} = 0 \text{ za } i > j; \qquad \beta_{1,j} = \beta_{2,j+1} = \ldots = \beta_{n-j+1,n} \text{ za } j = 1, 2, \ldots, n.$$

Dakle, $B(e)$ je gornjetrokutasta matrica koja na glavnoj dijagonali i na svakoj paraleli iznad nje ima sve elemente međusobno jednake. Stavimo $\beta_j = \beta_{1,j}$ za $j = 1, 2, \ldots, n$. Uočimo da je $(J_n)^j = A(e)^j$ matrica koja ima sve nule osim $n-j$ elemenata na $j-$toj paraleli iznad glavne dijagonale gdje su jedinice. Slijedi

$$B(e) = \beta_1 I(e) + \beta_2 A(e) + \beta_3 A(e)^2 + \ldots + \beta_n A(e)^{n-1}.$$

Dakle, ako definiramo polinom $P(\lambda)$ s tim koeficijentima,

$$P = \beta_1 + \beta_2\lambda + \beta_3\lambda^2 + \ldots + \beta_n\lambda^{n-1},$$

onda je $B(e) = P(A(e))$, dakle $B(e) = P(A)(e)$, dakle $B = P(A)$.

Ako je indeks nilpotentnosti operatora $A \in L(V)$ manji od $\dim V$, onda se prostor rastavlja u direktnu sumu $A-$invarijantnih potprostora na način da su restrikcije operatora A na te potprostore nilpotentni operatori maksimalnih indeksa nilpotentnosti, tj. svaki je indeks nilpotentnosti jednak dimenziji odgovarajućeg invarijantnog potprostora. Precizno:

Teorem 5.4 *Neka je $A \in L(V)$ nilpotentan operator indeksa $p < \dim V$.*

(*a*) *Postoje $A-$invarijantni potprostori $V_1, V_2, \ldots, V_s$ prostora V takvi da je $V = V_1 \dot{+} V_2 \dot{+} \ldots \dot{+} V_s$ i da je za svako j operator $A_j = A|V_j$ nilpotentan indeksa $p_j = \dim V_j$.*

(*b*) (*Jedinstvenost*) *Broj potprostora u tom rastavu koji su dimenzije k jednak je*

$$r(A^{k+1}) + r(A^{k-1}) - 2r(A^k) \qquad (A^0 = I).$$

Dokaz: (*a*) Dokaz ćemo provesti indukcijom po $\dim V$. Situacija $\dim V = 1$ je nemoguća, jer bi indeks nilpotentnosti morao biti 0, a za svaki operator A je po dogovoru $A^0 = I \neq 0$.

Neka je $\dim V = 2 \Rightarrow$ indeks nilpotentnosti je $1 \Rightarrow A = 0$. Tada svaki rastav prostora u direktnu sumu dva jednodimenzionalna potprostora zadovoljava tvrdnju. Time je baza indukcije dokazana.

Provedimo sada korak indukcije. Neka je $n \geq 3$ i pretpostavimo da je tvrdnja (*a*) dokazana za sve vektorske prostore dimenzije manje od n. Neka je $\dim V = n$. Izaberimo $v \in V$ takav da je $A^{p-1}v \neq 0$. Tada je $p-$dimenzionalan prostor razapet vektorima $A^j v$, $V_1 = [\{v, Av, A^2 v, \ldots, A^{p-1}v\}]$, $A-$invarijantan i restrikcija $A_1 = A|V_1$ je nilpotentan operator indeksa $p_1 = p = \dim V_1$.

Promatrajmo sada dualni prostor V' i dualni operator A'. Imamo

$$(A')^k = (A^k)',$$

pa vidimo da je A' nilpotentan operator istog indeksa p. Izaberimo $f \in V'$ takav da je $f(A^{p-1}v) \neq 0$. Tada je

$$((A')^{p-1}f)(v) = f(A^{p-1}v) \neq 0,$$

dakle je $(A')^{p-1}f \neq 0$. Slijedi da je potprostor razapet funkcionalima $(A')^j f$,

$$Y = [\{f, A'f, (A')^2 f, \ldots, (A')^{p-1}f\}],$$

$p-$dimenzionalan i $A'-$invarijantan. Stavimo

$$X = Y^0 = \{w \in V; g(w) = 0 \ \forall g \in Y\} =$$

$$= \{w \in V; f(w) = (A'f)(w) = ((A')^2 f)(w) = \ldots = ((A')^{p-1}f)(w) = 0\} =$$

$$= \{w \in V; f(w) = f(Aw) = f(A^2 w) = \ldots = f(A^{p-1}w) = 0\}.$$

Prema tvrdnji (*c*) propozicije 2.6 nalazimo da je dimenzija potprostora X jednaka $\dim V - \dim Y = n - p$. Nadalje, potprostor X je $A-$invarijantan. Doista, neka je $w \in X$. Neka je $g \in Y$. Tada je $A'g \in Y$ jer je Y $A'-$invarijantan, pa slijedi $g(Aw) = (A'g)(w) = 0$. Dakle, $g(Aw) = 0 \ \forall g \in Y$, što pokazuje da je $Aw \in X$, a kako je vektor $w \in X$ bio proizvoljan, dokazano je da je potprostor X $A-$invarijantan. Neka je $w \in X \cap V_1$. Kako je $w \in V_1$, to je

$$w = \alpha_0 v + \alpha_1 Av + \ldots + \alpha_{p-1}A^{p-1}v,$$

za neke skalare $\alpha_0, \alpha_1, \ldots, \alpha_{p-1}$. Pretpostavimo da je $w \neq 0$ i neka je $j \in \{0, 1, \ldots, p-1\}$ najmanji takav da je $\alpha_j \neq 0$. Dakle,

$$w = \alpha_j A^j v + \alpha_{j+1}A^{j+1}v + \ldots + \alpha_{p-1}A^{p-1}v.$$

Djelujemo li na lijevu i desnu stranu te jednakosti s operatorom A^{p-j-1} dobivamo $A^{p-j-1}w = \alpha_j A^{p-1}v$. Kako je $w \in X$, to vrijedi i $A^{p-j-1}w \in X$, jer je potprostor X $A-$invarijantan.

Budući da je $\alpha_j \neq 0$, iz jednakosti $A^{p-j-1}w = \alpha_j A^{p-1}v$ slijedi $A^{p-1}v \in X$. Kako je $X = Y^0$ i $f \in Y$ slijedi $f(A^{p-1}v) = 0$, a to je u suprotnosti s izborom funkcionala f. Ova kontradikcija pokazuje da je naša pretpostavka $w \neq 0$ bila pogrešna. Zaključujemo da mora biti $w = 0$. Time je dokazano da je $X \cap V_1 = \{0\}$. Dakle, suma potprostora X i V_1 je direktna. Sada je

$$\dim(V_1 \dotplus X) = \dim V_1 + \dim X = p + (n-p) = n = \dim V, \qquad \Longrightarrow \qquad V_1 \dotplus X = V.$$

Stavimo sada $B = A \,|\, X$. Tada je operator $B \in L(X)$ nilpotentan, jer je $B^p = A^p \,|\, X = 0$. Neka je $p_2 \leq p$ indeks nilpotentnosti operatora B. Ako je $p_2 = \dim X$, dokaz je gotov uz $s = 2$, $V_2 = X$. Ako je $p_2 < \dim X$, primijenimo pretpostavku indukcije na operator B, što možemo jer je $\dim X < n$. Slijedi da postoje $B-$invarijantni potprostori $V_2, \ldots, V_s$ od X (dakle, $A-$invarijantni potprostori od V) takvi da je $X = V_2 \dotplus \ldots \dotplus V_s$ i da je svaka restrikcija $B \,|\, V_j = A \,|\, V_j$ $(2 \leq j \leq s)$ nilpotentan operator indeksa $p_j = \dim V_j$. No tada je

$$V = V_1 \dotplus V_2 \dotplus \ldots \dotplus V_s,$$

i time je tvrdnja (a) dokazana.

Dokažimo sada tvrdnju (b). Očito je

$$r(A) = r(A_1) + r(A_2) + \ldots + r(A_s)$$

i za svaku potenciju $k \geq 0$ vrijedi

$$r(A^k) = r(A_1^k) + r(A_2^k) + \ldots + r(A_s^k).$$

Dakle je:

$$r(A^{k+1}) + r(A^{k-1}) - 2r(A^k) = \sum_{j=1}^{s} [r(A_j^{k+1}) + r(A_j^{k-1}) - 2r(A_j^k)].$$

Izračunajmo $r(A_j^k)$. Operator A_j je nilpotentan maksimalnog indeksa $p_j = \dim V_j$, pa on u nekoj bazi za matricu ima elementarnu Jordanovu klijetku p_j-tog reda. Stoga treba izračunati rang bilo koje potencije elementarne Jordanove klijetke J_r $r-$tog reda. Matrica J_r^k ima sve elemente jednake nuli osim $r-k$ jedinica na paraleli s glavnom dijagonalom. Dakle, $r(J_r^k) = r - k$ za $k = 0, 1, \ldots, r$ i, naravno, $r(J_r^k) = 0$ za $k > r$. Dakle, za $k < p_j$ je

$$r(A_j^{k+1}) + r(A_j^{k-1}) - 2r(A_j^k) = p_j - k - 1 + p_j - k + 1 - 2p_j + 2k = 0;$$

za $k = p_j$ je

$$r(A_j^{p_j+1}) + r(A_j^{p_j-1}) - 2r(A_j^{p_j}) = 0 + 1 - 2 \cdot 0 = 1;$$

za $k > p_j$ je

$$r(A_j^{k+1}) + r(A_j^{k-1}) - 2r(A_j^k) = 0 + 0 - 2 \cdot 0 = 0.$$

Odatle je

$$r(A^{k+1}) + r(A^{k-1}) - 2r(A^k) = \sum_{j=1}^{s} [r(A_j^{k+1}) + r(A_j^{k-1}) - 2r(A_j^k)] = |\{j;\, p_j = k\}|,$$

a to je upravo tvrdnja (b).

Dokazani teorem pokazuje da za svaki nilpotentan operator A na konačnodimenzionalnom vektorskom prostoru V postoji baza e od V takva da je matrica $A(e)$ blok$-$dijagonalna i na dijagonali su joj blokovi koji su elementarne Jordanove klijetke, s tim da je format najveće od njih $p \times p$, gdje je p indeks nilpotentnosti operatora A. Drugim riječima, matrica $A(e)$ ima sve elemente jednake nuli osim na prvoj gornjoj paraleli uz glavnu dijagonalu gdje su raspoređene jedinice i nule (najprije $p_1 - 1$ jedinica, $p_1 = p$, zatim jedna nula, zatim $p_2 - 1$ jedinica, $p_2 \leq p_1$, zatim jedna nula, zatim $p_3 - 1$ jedinica, $p_3 \leq p_2$, itd. i na koncu $p_s - 1$ jedinica).

6 Redukcija linearnog operatora

Neka su $P(\lambda)$ i $Q(\lambda)$ polinomi. Ako je polinom $P(\lambda)$ djeljiv s polinomom $Q(\lambda)$, tj. ako postoji polinom $R(\lambda)$ takav da je $P(\lambda) = R(\lambda)Q(\lambda)$, reći ćemo još da **polinom $Q(\lambda)$ dijeli polinom $P(\lambda)$** i pisati $Q(\lambda)\,|\,P(\lambda)$.

Reći ćemo da su polinomi $P(\lambda)$ i $Q(\lambda)$ **relativno prosti**, ako ne postoji polinom stupnja ≥ 1 koji dijeli i $P(\lambda)$ i $Q(\lambda)$.

Opisat ćemo sada tzv. *Euklidov algoritam* koji se temelji na postupku dijeljenja polinoma s ostatkom. Ako polinom $P(\lambda)$ nije djeljiv s polinomom $Q(\lambda)$, onda postoje polinomi $S_1(\lambda)$ i $R_1(\lambda)$ takvi da je

$$P(\lambda) = S_1(\lambda)Q(\lambda) + R_1(\lambda), \qquad \deg R_1(\lambda) < \deg Q(\lambda).$$

Ako $Q(\lambda)$ nije djeljiv s $R_1(\lambda)$, onda postoje polinomi $S_2(\lambda)$ i $R_2(\lambda)$ takvi da je

$$Q(\lambda) = S_2(\lambda)R_1(\lambda) + R_2(\lambda), \qquad \deg R_2(\lambda) < \deg R_1(\lambda).$$

Ako $R_1(\lambda)$ nije djeljiv s $R_2(\lambda)$, onda postoje polinomi $S_3(\lambda)$ i $R_3(\lambda)$ takvi da je

$$R_1(\lambda) = S_3(\lambda)R_2(\lambda) + R_3(\lambda), \qquad \deg R_3(\lambda) < \deg R_2(\lambda).$$

U svakom ovakvom koraku stupanj ostatka je striktno manji nego stupanj prethodnog ostatka. Prema tome, opisani postupak ne možemo nastavljati u nedogled, nego će se nakon konačno mnogo koraka dogoditi da ostatak dijeli prethodni ostatak. Drugim riječima, za neki k postoje netrivijalni polinomi $S_1(\lambda), S_2(\lambda), \ldots, S_{k+1}$ i netrivijalni polinomi $R_1(\lambda), R_2(\lambda), \ldots, R_k(\lambda)$ takvi da je

$$\deg R_1(\lambda) > \deg R_2(\lambda) > \cdots > \deg R_{k-1} > \deg R_k(\lambda) \geq 0$$

i da vrijedi sljedeći sustav jednakosti

$$\begin{array}{rcl} P(\lambda) & = & S_1(\lambda)Q(\lambda) + R_1(\lambda) \\ Q(\lambda) & = & S_2(\lambda)R_1(\lambda) + R_2(\lambda) \\ R_1(\lambda) & = & S_3(\lambda)R_2(\lambda) + R_3(\lambda) \\ & \vdots & \\ R_{j-1}(\lambda) & = & S_{j+1}(\lambda)R_j(\lambda) + R_{j+1}(\lambda) \\ & \vdots & \\ R_{k-2}(\lambda) & = & S_k(\lambda)R_{k-1}(\lambda) + R_k(\lambda) \\ R_{k-1}(\lambda) & = & S_{k+1}(\lambda)R_k(\lambda). \end{array} \qquad (*)$$

Računski postupak opisan sustavom $(*)$ zove se **Euklidov algoritam**. Ako vrijedi $Q(\lambda)\,|\,P(\lambda)$, algoritam završava već u prvom koraku, tj. $R_1(\lambda) = 0$.

Primijetimo sada da, krenuši od posljednje jednakosti u $(*)$ prema prvoj, redom zaključujemo:

$$R_k(\lambda)\,|\,R_{k-1}(\lambda) \;\Rightarrow\; R_k(\lambda)\,|\,R_{k-2}(\lambda) \;\Rightarrow\; \cdots \;\Rightarrow\; R_k(\lambda)\,|\,R_1(\lambda) \;\Rightarrow\; R_k(\lambda)\,|\,Q(\lambda) \;\Rightarrow\; R_k(\lambda)\,|\,P(\lambda).$$

Dakle, polinom $R_k(\lambda)$ dijeli i polinom $P(\lambda)$ i polinom $Q(\lambda)$.

Pretpostavimo sada da polinom $R(\lambda)$ dijeli i $P(\lambda)$ i $Q(\lambda)$. Krenuši od prve jednakosti u sustavu $(*)$ prema pretposljednjoj sada redom zaključujemo:

$$R(\lambda)\,|\,R_1(\lambda) \;\Rightarrow\; R(\lambda)\,|\,R_2(\lambda) \;\Rightarrow\; R(\lambda)\,|\,R_3(\lambda) \;\Rightarrow\; \cdots\cdots \;\Rightarrow\; R(\lambda)\,|\,R_{k-1}(\lambda) \;\Rightarrow\; R(\lambda)\,|\,R_k(\lambda).$$

Na taj način smo dokazali:

Propozicija 6.1 *Neka su $P(\lambda)$ i $Q(\lambda)$ polinomi. Postoji polinom $M(\lambda)$ sa sljedećim svojstvima:*

(*a*) *$M(\lambda)\,|\,P(\lambda)$ i $M(\lambda)\,|\,Q(\lambda)$.*

(*b*) *Ako je $R(\lambda)$ polinom takav da $R(\lambda)\,|\,P(\lambda)$ i $R(\lambda)\,|\,Q(\lambda)$ tada $R(\lambda)\,|\,M(\lambda)$.*

Polinom $M(\lambda)$ sa svojstvima (a) i (b) iz propozicije 6.1 zove se **najveća zajednička mjera** polinoma $P(\lambda)$ i $Q(\lambda)$. Euklidov algoritam $(*)$ je efikasan računski postupak za pronalaženje najveće zajedničke mjere bilo koja dva polinoma. Očito su sve najveće zajedničke mjere zadanih polinoma $P(\lambda)$ i $Q(\lambda)$ međusobno proporcionalne i točno jedna među njima je normirana. Jedinstvenu normiranu zajedničku mjeru polinoma $P(\lambda)$ i $Q(\lambda)$ označavat ćemo sa $(P(\lambda), Q(\lambda))$.

Teorem 6.1 *Neka su $P(\lambda)$ i $Q(\lambda)$ polinomi.*

(1) *Postoje polinomi $A(\lambda)$ i $B(\lambda)$ takvi da je $(P(\lambda), Q(\lambda)) = A(\lambda)P(\lambda) + B(\lambda)Q(\lambda)$.*

(2) *Sljedeća su tri svojstva međusobno ekvivalentna:*

  (*a*) *Polinomi $P(\lambda)$ i $Q(\lambda)$ su relativno prosti.*

  (*b*) $(P(\lambda), Q(\lambda)) = 1$.

  (*c*) *Postoje polinomi $A(\lambda)$ i $B(\lambda)$ takvi da je $A(\lambda)P(\lambda) + B(\lambda)Q(\lambda) = 1$.*

Dokaz: (1) Iz sustava jednakosti $(*)$ krenuvši od prve prema pretposljednjoj korak po korak nalazimo da za svaki $j \in \{1, 2, \ldots, k\}$ postoje polinomi $A_j(\lambda)$ i $B_j(\lambda)$ takvi da vrijedi $R_j(\lambda) = A_j(\lambda)P(\lambda) + A_j(\lambda)Q(\lambda)$. Time je tvrdnja (1) dokazana, jer je $R_k(\lambda)$ najveća zajednička mjera, dakle polinom proporcionalan polinomu $(P(\lambda), Q(\lambda))$.

(2) Pretpostavimo da su polinomi $P(\lambda)$ i $Q(\lambda)$ relativno prosti. To znači da su samo polinomi stupnja nula, tj. konstante, istovremeni djelitelji polinoma $P(\lambda)$ i $Q(\lambda)$. Dakle, $(P(\lambda), Q(\lambda)) = 1$. Time je dokazano da iz (a) slijedi (b). Nadalje, iz tvrdnje (1) vidimo da iz (b) slijedi (c). Napokon, pretpostavimo da vrijedi (c). Neka je $R(\lambda)$ polinom koji dijeli i $P(\lambda)$ i $Q(\lambda)$. Tada iz (c) slijedi da $R(\lambda)$ dijeli $A(\lambda)P(\lambda) + B(\lambda)Q(\lambda) = 1$. Odatle slijedi da je stupanj polinoma $R(\lambda)$ jednak nuli, tj. $R(\lambda)$ je konstanta. To znači da ne postoji polinom stupnja ≥ 1 koji dijeli i $P(\lambda)$ i $Q(\lambda)$, dakle $P(\lambda)$ i $Q(\lambda)$ su relativno prosti. Time je dokazano da iz (c) slijedi (a).

Ako je V konačnodimenzionalan vektorski prostor i $A \in L(V)$ onda za svaki polinom $P(\lambda)$ operator A komutira s $P(A)$, dakle prema lemi 5.1 potprostori $N(P(A))$ i $R(P(A))$ su $A-$invarijantni. Sljedeća propozicija pokazuje da time ništa ne dobivamo ako su polinomi $P(\lambda)$ i $\mu_A(\lambda)$ relativno prosti.

Propozicija 6.2 *Neka je V konačnodimenzionalan vektorski prostor nad poljem K, $A \in L(V)$ i neka je $P(\lambda)$ polinom. Tada su sljedeća dva svojstva međusobno ekvivalentna:*

(*a*) *Polinomi $P(\lambda)$ i $\mu_A(\lambda)$ su relativno prosti, tj. $(P(\lambda), \mu_A(\lambda)) = 1$.*

(*b*) *Operator $P(A)$ je regularan, tj. $N(P(A)) = \{0\}$ i $R(P(A)) = V$.*

Dokaz: Pretpostavimo da su polinomi $P(\lambda)$ i $\mu_A(\lambda)$ relativno prosti. Tada prema tvrdnji (2) teorema 6.1 postoje polinomi $Q(\lambda)$ i $R(\lambda)$ takvi da je $Q(\lambda)P(\lambda) + R(\lambda)\mu_A(\lambda) = 1$. Uvrštavanjem operatora A slijedi $Q(A)P(A) + R(A)\mu_A(A) = I$. Kako je $\mu_A(A) = 0$ dobivamo $Q(A)P(A) = P(A)Q(A) = I$. Dakle, operator $P(A)$ je regularan. Time je dokazana implikacija $(a) \Rightarrow (b)$.

Pretpostavimo sada da je operator $P(A)$ regularan. Treba dokazati da su tada polinomi $P(\lambda)$

i $\mu_A(\lambda)$ relativno prosti. Pretpostavimo suprotno, tj. da postoji polinom $Q(\lambda)$ stupnja većeg od nule koji dijeli i $P(\lambda)$ i $\mu_A(\lambda)$. Neka su $R(\lambda)$ i $S(\lambda)$ polinomi takvi da je $P(\lambda) = Q(\lambda)R(\lambda)$ i $\mu_A = Q(\lambda)S(\lambda)$. Tada je $P(A) = Q(A)R(A)$, pa iz regularnosti operatora $P(A)$ slijedi da je i operator $Q(A)$ regularan. Kako je $0 = \mu_A(A) = Q(A)S(A)$, regularnost operatora $Q(A)$ ima za posljedicu da je $S(A) = 0$. No to je nemoguće zbog tvrdnje (a) teorema 3.1 i zbog $\deg S(\lambda) < \deg \mu_A(\lambda)$. Ova kontradikcija pokazuje da je pretpostavka da $P(\lambda)$ i $\mu_A(\lambda)$ nisu relativno prosti bila pogrešna, pa zaključujemo da je $(P(\lambda), \mu_A(\lambda)) = 1$. Time je dokazana i obrnuta implikacija $(b) \Rightarrow (a)$.

Ukoliko se polinom P može rastaviti u produkt relativno prostih polinoma, potprostor $N(P(A))$ rastavlja se u odgovarajuću direktnu sumu potprostora:

Propozicija 6.3 *Neka je V konačnodimenzionalan vektorski prostor, $A \in L(V)$, i neka su $P(\lambda)$, $Q(\lambda)$ i $R(\lambda)$ polinomi takvi da je $P(\lambda) = Q(\lambda)R(\lambda)$ i da su $Q(\lambda)$ i $R(\lambda)$ relativno prosti. Tada je*

$$N(P(A)) = N(Q(A)) \dotplus N(R(A)).$$

Dokaz: Budući da su $Q(\lambda)$ i $R(\lambda)$ relativno prosti, prema tvrdnji (2) teorema 6.1 postoje polinomi $S(\lambda)$ i $T(\lambda)$ takvi da je

$$1 = S(\lambda)Q(\lambda) + T(\lambda)R(\lambda) \qquad \Longrightarrow \qquad I = S(A)Q(A) + T(A)R(A) \qquad \Longrightarrow$$

$$\Longrightarrow \qquad v = S(A)Q(A)v + T(A)R(A)v, \quad \forall v \in V.$$

Posebno, ako je $v \in N(P(A))$, stavimo $y = S(A)Q(A)v$ i $x = T(A)R(A)v$. Slijedi $v = x + y$ i pri tome imamo

$$Q(A)x = Q(A)T(A)R(A)v = T(A)P(A)v = 0 \qquad \Rightarrow \qquad x \in N(Q(A)),$$

$$R(A)y = R(A)S(A)Q(A)v = S(A)P(A)v = 0 \qquad \Rightarrow \qquad y \in N(R(A)).$$

Time je dokazano da je $N(P(A)) \subseteq N(Q(A)) + N(R(A))$, a kako su $N(Q(A))$ i $N(R(A))$ očito sadržani u $N(P(A))$, zaključujemo da je $N(P(A)) = N(Q(A)) + N(R(A))$.

Treba još dokazati da je ta suma direktna. Neka je $v \in N(Q(A)) \cap N(R(A))$. Tada je $Q(A)v = R(A)v = 0$, pa slijedi $v = S(A)Q(A)v + T(A)R(A)v = 0$. Dakle, $N(Q(A)) \cap N(R(A)) = \{0\}$, odnosno,

$$N(P(A)) = N(Q(A)) \dotplus N(R(A)).$$

Za dokaz osnovnog teorema 6.2 o redukciji linearnih operatora treba nam još jedna činjenica o polinomima:

Lema 6.1 *Neka su $P(\lambda)$, $Q(\lambda)$ i $R(\lambda)$ polinomi takvi da su $P(\lambda)$ i $Q(\lambda)$ relativno prosti i da su $P(\lambda)$ i $R(\lambda)$ relativno prosti. Tada su polinomi $P(\lambda)$ i $Q(\lambda)R(\lambda)$ relativno prosti.*

Dokaz: Prema tvrdnji (2) teorema 6.1 iz pretpostavke slijedi da postoje polinomi $A(\lambda)$, $B(\lambda)$, $C(\lambda)$ i $D(\lambda)$ takvi da je

$$A(\lambda)P(\lambda) + B(\lambda)Q(\lambda) = 1 \qquad \text{i} \qquad C(\lambda)P(\lambda) + D(\lambda)R(\lambda) = 1.$$

Definiramo sada polinome $E(\lambda)$ i $F(\lambda)$ na sljedeći način:

$$E(\lambda) = A(\lambda)C(\lambda)P(\lambda) + A(\lambda)D(\lambda)R(\lambda) + B(\lambda)C(\lambda)Q(\lambda), \qquad F(\lambda) = B(\lambda)D(\lambda).$$

Izostavljajući oznaku λ za varijablu polinoma tada imamo redom

$$EP + F(QR) = ACP^2 + ADRP + BCQP + BDQR =$$

$$= (AP)(CP) + (AP)(DR) + (BQ)(CP) + (BQ)(DR) = (AP + BQ)(CP + DR) = 1.$$

Ponovnom primjenom tvrdnje (2) teorema 6.1 zaključujemo da su polinomi $P(\lambda)$ i $Q(\lambda)R(\lambda)$ relativno prosti.

Teorem 6.2 *Neka je V konačnodimenzionalan vektorski prostor i $A \in L(V)$. Pretpostavimo da je*

$$\mu_A(\lambda) = \mu_1(\lambda) \cdot \mu_2(\lambda) \cdots \mu_s(\lambda), \qquad (s \geq 2)$$

pri čemu su $\mu_1(\lambda), \mu_2(\lambda), \ldots, \mu_s(\lambda)$ normirani polinomi takvi da su $\mu_i(\lambda)$ i $\mu_j(\lambda)$ relativno prosti za $i \neq j$. Stavimo $V_j = N(\mu_j(A))$ za $j = 1, 2, \ldots, s$.

(*a*) *Svaki od potprostora V_j je $A-$invarijantan.*

(*b*) $V = V_1 \dot{+} V_2 \dot{+} \cdots \dot{+} V_s$.

(*c*) *Za svaki j vrijedi $\mu_j(\lambda) = \mu_{A|V_j}$, tj. $\mu_j(\lambda)$ je minimalni polinom restrikcije $A\,|\,V_j$.*

Dokaz: Tvrdnja (*a*) je neposredna posljedica leme 5.1.

Dokaz tvrdnji (*b*) i (*c*) provest ćemo matematičkom indukcijom u odnosu na $s \geq 2$.

Baza indukcije: Pretpostavljamo da je $s = 2$, tj. da je $\mu_A(\lambda) = \mu_1(\lambda) \cdot \mu_2(\lambda)$ i da su $\mu_1(\lambda)$ i $\mu_2(\lambda)$ normirani polinomi koji su relativno prosti. Sada iz propozicije 6.2 slijedi

$$N(\mu_A(A)) = N(\mu_1(A)) \dot{+} N(\mu_2(A)),$$

a to je upravo tvrdnja (*b*) jer je $\mu_A(A) = 0$, dakle $N(\mu_A(A)) = V$.

Dokažimo da vrijedi i tvrdnja (*c*) u slučaju $s = 2$. Stavimo $A_1 = A\,|\,V_1$. Za bilo koji $v \in V_1$ vrijedi $\mu_1(A)v = 0$. Međutim, $\mu_1(A)\,|\,V_1 = \mu_1(A_1)$, pa zaključujemo da je $\mu_1(A_1)v = 0$ $\forall v \in V_1$, dakle $\mu_1(A_1) = 0$. Primjenom tvrdnje (*c*) teorema 3.1 na operator A_1 zaključujemo da je polinom $\mu_1(\lambda)$ djeljiv s minimalnim polinomom $\mu_{A_1}(\lambda)$ operatora A_1, tj. vrijedi $\mu_{A_1}(\lambda) \,|\, \mu_1(\lambda)$. Nadalje, stavimo $P(\lambda) = \mu_{A_1}(\lambda)\mu_2(\lambda)$. Za $v \in V_1$ sada imamo

$$P(A)v = P(A_1)v = \mu_{A_1}(A_1)\mu_2(A_1)v = 0, \qquad \text{jer je} \qquad \mu_{A_1}(A_1) = 0.$$

Također, za $v \in V_2$ imamo

$$P(A)v = \mu_{A_1}(A)\mu_2(A)v = 0, \qquad \text{jer je} \qquad v \in V_2 = N(\mu_2(A)).$$

Dakle, vrijedi $P(A)\,|\,V_1 = 0$ i $P(A)\,|\,V_2 = 0$, a kako je $V = V_1 \dot{+} V_2$ zaključujemo da je $P(A) = 0$. Ponovnom primjenom tvrdnje (*c*) teorema 3.1, sada na operator A, nalazimo da polinom $\mu_A(\lambda)$ dijeli polinom $P(\lambda)$. Dakle, postoji polinom $Q(\lambda)$ takav da je $P(\lambda) = \mu_A(\lambda)Q(\lambda)$. To znači da je $\mu_{A_1}(\lambda)\mu_2(\lambda) = \mu_1(\lambda)\mu_2(\lambda)Q(\lambda)$, pa slijedi $\mu_{A_1}(\lambda) = \mu_1(\lambda)Q(\lambda)$. Time smo dokazali da vrijedi $\mu_1(\lambda) \,|\, \mu_{A_1}(\lambda)$ i $\mu_{A_1}(\lambda) \,|\, \mu_1(\lambda)$. Budući da su polinomi $\mu_{A_1}(\lambda)$ i $\mu_1(\lambda)$ normirani, zaključujemo da je $\mu_1(\lambda) = \mu_{A_1}(\lambda) = \mu_{A|V_1}(\lambda)$. Sasvim analogno nalazimo i $\mu_2(\lambda) = \mu_{A|V_2}(\lambda)$.

Time smo dokazali da tvrdnje (*b*) i (*c*) vrijede ako je $s = 2$, odnosno, u potpunosti je proveden dokaz baze indukcije.

Korak indukcije: Pretpostavimo sada da je $s \geq 3$ i da su tvrdnje (*b*) i (*c*) dokazane u slučaju rastava minimalnog polinoma u produkt $s - 1$ normiranih relativno prostih polinoma. Stavimo sada $\mu' = \mu_2(\lambda) \cdots \mu_s(\lambda)$, $V' = N(\mu'(A))$ i $A' = A\,|\,V'$. Iz leme 6.1 slijedi da su polinomi $\mu_1(\lambda)$ i $\mu'(\lambda)$ relativno prosti. Prema dokazanoj bazi indukcije slijedi da je

$$V = V_1 \dot{+} V', \qquad \mu_1(\lambda) = \mu_{A|V_1}(\lambda) \quad \text{i} \quad \mu'(\lambda) = \mu_{A'}(\lambda).$$

Sada iz pretpostavke indukcije slijedi da je

$$V' = V_2 \dotplus \cdots \dotplus V_s, \qquad \text{dakle} \qquad V = V_1 \dotplus V_2 \dotplus \cdots \dotplus V_s,$$

i da je

$$\mu_j(\lambda) = \mu_{A'|V_j}(\lambda) = \mu_{A|V_j}(\lambda) \ \text{ za } \ j = 2, \ldots, s, \qquad \text{dakle} \qquad \mu_j(\lambda) = \mu_{A|V_j}(\lambda) \ \text{ za } \ j = 1, 2, \ldots, s.$$

Time je korak indukcije proveden, pa je teorem u potpunosti dokazan.

Napomena. Fittingova dekompozicija može se provesti i pomoću teorema 6.2. Doista, ako 0 nije u $\sigma(A)$, tj. 0 nije nultočka od $\mu_A(\lambda)$, onda je po teoremu 3.2 operator A regularan, dakle $V^0(A) = \{0\}$ i $V^1(A) = V$. Ako je 0 $k-$struka nultočka polinoma $\mu_A(\lambda)$, onda je $\mu_A = \lambda^k \nu(\lambda)$ i $\nu(0) \neq 0$. Tada su polinomi λ^k i ν relativno prosti, pa zbog tvrdnje (b) teorema 6.2 vrijedi $V = N(A^k) \dotplus N(\nu(A))$. Operator $A \,|\, N(A^k)$ je očito nilpotentan. Nadalje, po tvrdnji (c) teorema 6.2 je $\mu_{A|N(\nu(A))}(\lambda) = \nu(\lambda)$ i $\nu(0) \neq 0$, pa po teoremu 3.2 slijedi da je operator $A \mid N(\nu(A))$ regularan. Dakle, $V^0(A) = N(A^k)$ i $V^1 = N(\nu(A))$. Kako su polinomi λ^k i $\nu(\lambda)$ relativno prosti, postoje polinomi $P(\lambda)$ i $Q(\lambda)$ takvi da je $\lambda^k P(\lambda) + \nu(\lambda) Q(\lambda) = 1$. Dakle, $A^k P(A) + Q(A)\nu(A) = I$. Iz te jednakosti zaključujemo

$$v \in N(\nu(A)) \ \Rightarrow \ v = A^k P(A) v + Q(A)\nu(A) v = A^k P(A) v \ \Rightarrow \ v \in R(A^k),$$

dakle, $N(\nu(A)) \subseteq R(A^k)$. Međutim, kako je $V = N(A^k) \dotplus N(\nu(A))$, po teoremu 2.3 o rangu i defektu primijenjenom na operator A^k slijedi da je $\dim N(\nu(A)) = \dim R(A^k)$. Odavde i iz $N(\nu(A)) \subseteq R(A^k)$ slijedi $N(\nu(A)) = R(A^k)$. Dakle, $V^1(A) = R(A^k)$.

Razmotrimo sada posebno slučaj kada je polje K algebarski zatvoreno, npr. $K = \mathbb{C}$. Tada svaki nekonstantan polinom ima nultočku. Ako je α_1 nultočka polinoma $P(\lambda)$, tj. ako je $P(\alpha_1) = 0$, onda je polinom $P(\lambda)$ djeljiv s polinomom $\lambda - \alpha_1$. Doista, ako provedemo postupak dijeljenja polinoma $P(\lambda)$ s polinomom $\lambda - \alpha_1$ stupnja 1 dolazimo do jednakosti oblika $P(\lambda) = (\lambda - \alpha_1)Q(\lambda) + R(\lambda)$, pri čemu je $\deg R(\lambda) < 1$, dakle, $R(\lambda)$ je konstanta, $R(\lambda) \equiv \alpha \in \mathbb{C}$. Ako u jednakost

$$P(\lambda) = (\lambda - \alpha_1)Q(\lambda) + \alpha$$

uvrstimo $\lambda = \alpha_1$, slijedi $\alpha = 0$. Dakle, $P(\lambda) = (\lambda - \alpha_1)Q(\lambda)$. Ako je $\deg Q(\lambda) \geq 1$, onda i polinom $Q(\lambda)$ ima neku nultočku α_2, pa slijedi $P(\lambda) = (\lambda - \alpha_1)(\lambda - \alpha_2)R(\lambda)$, za neki polinom $R(\lambda)$ stupnja $\deg P(\lambda) - 2$. Nastavimo li taj postupak dolazimo do $n = \deg P(\lambda)$ nultočaka $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ polinoma $P(\lambda)$ i do konstante $\alpha \in \mathbb{C}$ takvih da je

$$P(\lambda) = \alpha \cdot (\lambda - \alpha_1) \cdot (\lambda - \alpha_2) \cdots (\lambda - \alpha_n).$$

Među nultočkama $\alpha_1, \alpha_2, \ldots, \alpha_n$ može biti i međusobno jednakih, odnosno neke nultočke polinoma $P(\lambda)$ mogu biti višestruke. Možemo pretpostaviti da smo numeraciju nultočaka proveli tako da su $\alpha_1, \ldots, \alpha_s$ međusobno različite i da su $\alpha_{n+1}, \ldots, \alpha_n \in \{\alpha_1, \ldots, \alpha_s\}$. Ako je još k tome polinom $P(\lambda)$ normiran, onda za neke prirodne brojeve $p_1, \ldots, p_s$ vrijedi

$$P(\lambda) = (\lambda - \alpha_1)^{p_1}(\lambda - \alpha_2)^{p_2} \cdots (\lambda - \alpha_s)^{p_s}, \qquad \alpha_i \neq \alpha_j \ \text{ za } \ i \neq j.$$

Naravno, tada je $\deg P(\lambda) = p_1 + p_2 + \cdots + p_s$.

Neka su sada $\alpha, \beta \in \mathbb{C}$, $\alpha \neq \beta$. Tada za polinome

$$A(\lambda) = \frac{1}{\alpha - \beta}\lambda - \frac{\beta + 1}{\alpha - \beta} \qquad \text{i} \qquad B(\lambda) = -\frac{1}{\alpha - 1}\lambda + \frac{\alpha + 1}{\alpha - \beta}$$

nalazimo

$$A(\lambda)(\lambda-\alpha)+B(\lambda)(\lambda-\beta)=\frac{(\lambda-\beta-1)(\lambda-\alpha)-(\lambda-\alpha-1)(\lambda-\beta)}{\alpha-\beta}=$$

$$\frac{\lambda^2-(\alpha+\beta+1)\lambda+\alpha(\beta+1)-\lambda^2+(\alpha+\beta+1)\lambda-\beta(\alpha+1)}{\alpha-\beta}=1.$$

Iz tvrdnje (2) teorema 6.1 slijedi da su polinomi $\lambda-\alpha$ i $\lambda-\beta$ relativno prosti ako su α i β međusobno različiti. Prema lemi 6.1 i bilo koje potencije $(\lambda-\alpha)^p$ i $(\lambda-\beta)^q$ su relativno prosti polinomi.

Neka je sada V kompleksan konačnodimenzionalan vektorski prostor i $A\in L(V)$. Neka je $\sigma(A)=\{\alpha_1,\alpha_2,\ldots,\alpha_s\}$ pri čemu je $\alpha_i\neq\alpha_j$ za $i\neq j$. Tada su $\alpha_1,\alpha_2,\ldots,\alpha_s$ sve međusobno različite nultočke minimalnog polinoma $\mu_A(\lambda)$ operatora A i prema pretodnom razmatranju imamo

$$\mu_A(\lambda)=(\lambda-\alpha_1)^{p_1}(\lambda-\alpha_2)^{p_2}\cdots(\lambda-\alpha_s)^{p_s}$$

za neke prirodne brojeve $p_1,p_2,\ldots,p_s$. Nadalje, vidjeli smo da su za $i\neq j$ polinomi $(\lambda-\alpha_i)^{p_i}$ i $(\lambda-\alpha_j)^{p_j}$ relativno prosti. Stavimo $V_j=N\left((A-\alpha_j)^{p_j}\right)$. Po teoremu 6.2 tada su $V_1,V_2,\ldots,V_s$ $A-$invarijantni potprostori i vrijedi:

$$V=V_1\dotplus V_2\dotplus\cdots\dotplus V_s,\qquad \mu_{A_j}(\lambda)=(\lambda-\alpha_j)^{p_j}\ \text{ za }\ A_j=A|V_j,\ \ j=1,2,\ldots,s.$$

Kako je $(\lambda-\alpha_j)^{p_j}$ minimalni polinom operatora $A_j=A|V_j$, zaključujemo da je operator $A_j-\alpha_jI_{V_j}$ nilpotentan (I_{V_j} je oznaka za jedinični operator na prostoru V_j) i da mu je indeks nilpotentnosti jednak p_j. Prema teoremima 5.3 i 5.4 slijedi da u nekoj bazi $e^{(j)}$ potprostora V_j operator $A_j-\alpha_jI_{V_j}$ ima matricu koja je blok$-$dijagonalna, a svaki blok na dijagonali je elementarna Jordanova klijetka, s tim da najveća od tih klijetki ima format $p_j\times p_j$. Tada i operator A_j ima u toj bazi blok$-$dijagonalnu matricu, a blokovi na dijagonali su oblika:

$$\begin{bmatrix}\alpha_j & 1 & 0 & \cdots & 0 & 0\\ 0 & \alpha_j & 1 & \cdots & 0 & 0\\ 0 & 0 & \alpha_j & \cdots & 0 & 0\\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots\\ 0 & 0 & 0 & \cdots & \alpha_j & 1\\ 0 & 0 & 0 & \cdots & 0 & \alpha_j\end{bmatrix}.$$

Na taj način dokazali smo teorem o Jordanovoj formi matrice linearnog operatora:

Teorem 6.3 *Neka je V konačnodimenzionalan vektorski prostor nad algebarski zatvorenim poljem K (npr. $K=\mathbb{C}$) i neka je $A\in L(V)$. Neka je $\sigma(A)=\{\alpha_1,\alpha_2,\ldots,\alpha_s\}$, pri čemu je $\alpha_j\neq\alpha_k$ za $j\neq k$. Dakle,*

$$\mu_A(\lambda)=(\lambda-\alpha_1)^{p_1}(\lambda-\alpha_2)^{p_2}\cdots(\lambda-\alpha_s)^{p_s},\qquad \alpha_j\neq\alpha_k\ \ \textit{ako je}\ \ j\neq k,\qquad p_1,p_2,\ldots,p_k\in\mathbb{N}.$$

Stavimo

$$V_j=N\left((A-\alpha_jI_j)^{p_j}\right),\qquad A_j=A|V_j,\qquad B_j=A_j-\alpha_jI_j$$

(I_j je jedinični operator na prostoru V_j). B_j je nilpotentan operator indeksa P_jh. Postoji baza e prostora V (sastav-ljena redom od baza $e^{(1)},e^{(2)},\ldots,e^{(s)}$ potprostora $V_1,V_2,\ldots,V_s$) u kojoj operator A ima blok$-$dijagonalnu matricu (tzv. **Jordanova forma** *matrice operatora A) čiji su blokovi $\alpha_jI_j(e^{(j)})+B_j(e^{(j)})$, $1\leq j\leq s$. Nadalje, svaka matrica $B_j(e^{(j)})$ je blok$-$dijagonalna i blokovi su joj elementarne Jordanove klijetke od kojih najveća ima format $p_j\times p_j$.*

7 Unitarni prostori

U ovoj točki polje K nad kojim promatramo vektorske prostore će stalno biti ili polje $\mathbb{R}$ realnih brojeva ili polje $\mathbb{C}$ kompleksnih brojeva. Vektorski prostor nad poljem $\mathbb{R}$ obično se zove **realan vektorski prostor**, a nad poljem $\mathbb{C}$ **kompleksan vektorski prostor**.

Skalarni produkt na vektorskom prostoru X je preslikavanje $(\cdot|\cdot) : X \times X \to K$ (svakom uređenom paru vektora $(x, y) \in X \times X$ pridružen je skalar $(x|y) \in K$) sa sljedećim svojstvima:
linearnost u prvoj varijabli:

$$(\lambda x + \mu y|z) = \lambda(x|z) + \mu(y|z), \;\; \lambda, \mu \in K, \;\; x, y, z \in X;$$

hermitska simetrija:

$$(x|y) = \overline{(y|x)}, \qquad x, y \in X;$$

(u slučaju $K = \mathbb{R}$ svojstvo je $(x|y) = (y|x)$ i kraće se zove simetrija)
pozitivnost:

$$(x|x) \geq 0, \qquad x \in X;$$

definitnost:

$$(x|x) = 0 \qquad \Leftrightarrow \qquad x = 0.$$

Vektorski prostor na kome je zadan skalarni produkt zove se **unitaran prostor**. Skalarni produkt je zbog li-nearnosti u prvoj varijabli i zbog hermitske simetrije antilinearan u drugoj varijabi: $(x|\lambda y + \mu y) = \overline{\lambda}(x|y) + \overline{\mu}(x|z)$; u slučaju $K = \mathbb{R}$ imamo linearnost i u drugoj varijabli: $(x|\lambda y + \mu z) = \lambda(x|y) + \mu(x|z)$. Preslikavanje $V \times V \to K$ zove se **bilinearno** ako je linearno i u prvoj varijabli i u drugoj varijabli; ako je V kompleksan vektorski prostor, preslikavanje $V \times V \to \mathbb{C}$ zove se **seskvilinearno** ako je linearno u prvoj varijabli i antilinearno u drugoj varijabli. Dakle, skalarni produkt na realnom vektorskom prostoru je bilinearan, a na kompleksnom vektorskom prostoru seskvilinearan.

U unitarnom prostoru skalarni produkt dviju linearnih kombinacija može se računati član po član:

$$\Big(\sum_{j=1}^{n} \alpha_j x_j \Big| \sum_{k=1}^{m} \beta_k y_k\Big) = \sum_{j=1}^{n} \sum_{k=1}^{m} \alpha_j \overline{\beta_k} (x_j|y_k).$$

Teorem 7.1 *Neka je X unitaran prostor. Za $x \in X$ stavimo $\|x\| = \sqrt{(x|x)}$ (nenegativan drugi korijen). Tada funkcija $x \mapsto \|x\|$ s vektorskog prostora X u skup $\mathbb{R}_+ = \{\lambda \in \mathbb{R}; \lambda \geq 0\}$ ima sljedeća svojstva:*

(*a*) *za $x \in X$ vrijedi $\|x\| = 0$ ako i samo ako je $x = 0$;*

(*b*) *za $x \in X$ i $\lambda \in K$ vrijedi $\|\lambda x\| = |\lambda| \cdot \|x\|$;*

(*c*) *za $x, y \in X$ vrijedi tzv.* **nejednakost trokuta***: $\|x\| + \|y\| \leq \|x + y\|$.*

Nadalje, za bilo koje $x, y \in X$ vrijedi tzv. **nejednakost Cauchy−Schwarz−Buniakowskog***:*

$$|(x|y)| \leq \|x\| \cdot \|y\|,$$

pri čemu vrijedi znak jednakosti ako i samo ako su x i y proporcionalni.

Dokaz: Svojstvo (a) neposredna je posljedica definitnosti skalarnog produkta. Svojstvo (b) posljedica je li-nearnosti i hermitske simetrije:

$$\|\lambda x\|^2 = (\lambda x|\lambda x) = \lambda\overline{\lambda}(x|x) = |\lambda|^2\|x\|^2.$$

Dokažimo sada nejednakost Cauchy−Schwarz−Buniakowskog. Za vektore $x, y \in X$ zbog pozitivnosti norme, linearnosti skalarnog produkta u prvoj varijabli i hermitske simetrije imamo redom:

$$\begin{aligned} 0 &\leq \|(x|x)y - (y|x)x\|^2 = ((x|x)y - (y|x)x|(x|x)y - (y|x)x) = \\ &= \|x\|^4\|y\|^2 - \|x\|^2|(y|x)|^2 - \|x\|^2(y|x)(x|y) + \|x\|^2|(y|x)|^2 = \\ &= \|x\|^4\|y\|^2 - \|x\|^2|(x|y)|^2 = \|x\|^2(\|x\|^2\|y\|^2 - |(x|y)|^2). \end{aligned}$$

Ako je $x = 0$, očito je $|(x|y)| = \|x\| \cdot \|y\|$ (obje strane su nula); nadalje, tada su x i y proporcionalni $(x = 0 \cdot y)$. Ako je $x \neq 0$ tada je $\|x\| \neq 0$ i iz gornje nejednakosti dijeljenjem sa $\|x\|^2$ dobivamo $0 \leq \|x\|^2\|y\|^2 - |(x|y)|^2$, a to je upravo nejednakost Cauchy−Schwarz−Buniakowskog. Nadalje, iz definitnosti norme primijenjene na normu vektora $(x|x)y - (y|x)x$ slijedi da u nejednakosti Cauchy−Schwarz−Buniakowskog vrijedi znak jednakosti ako i samo ako je $(x|x)y = (y|x)x$, tj. ako i samo ako su x i y proporcionalni.

Ostaje nam da još dokažemo svojstvo (c). Za $x, y \in X$ primjenom svojstava skalarnog produkta i nejednakosti Cauchy−Schwarz−Buniakowskog nalazimo redom:

$$\|x + y\|^2 = (x + y|x + y) = (x|x) + (x|y) + (y|x) + (y|y) = \|x\|^2 + 2 \cdot \mathrm{Re}\,(x|y) + \|y\|^2 \leq$$

$$\leq \|x\|^2 + 2 \cdot |(x|y)| + \|y\|^2 \leq \|x\|^2 + 2 \cdot \|x\| \cdot \|y\| + \|y\|^2 = (\|x\| + \|y\|)^2.$$

Time je dokazana i nejednakost trokuta.

Funkcija $x \mapsto \|x\|$ definirana na vektorskom prostoru X i s vrijednostima u skupu $\mathbb{R}_+$ koja ima svojstva (a), (b) i (c) iz teorema 7.1 zove se **norma** na vektorskom prostoru X. Vektorski prostor na kome je zadana norma zove se **normiran prostor**.

Ako je X normiran prostor s normom $\|\cdot\|$ postavlja se pitanje da li je možda ta norma dobivena iz nekog skalarnog produkta na prostoru X. Vrlo jednostavan odgovor na to pitanje, kojeg navodimo bez dokaza, vezan je uz jednu geometrijsku jednakost, koja vrijedi za bilo koji paralelogram u ravnini: zbroj kvadrata duljina stranica paralelograma jednak je zbroju kvadrata duljina njegovih dviju dijagonala.

Teorem 7.2 (P. Jordan – J. von Neumann) *Neka je X normiran prostor s normom $x \mapsto \|x\|$. Tada su sljedeća dva svojstva međusobno ekvivalentna:*

(a) *Postoji skalarni produkt $(x, y) \mapsto (x|y)$ na X takav da je $\|x\| = \sqrt{(x|x)}$.*

(b) *Za bilo koje $x, y \in X$ vrijedi tzv.* **jednakost paralelograma***:*

$$\|x + y\|^2 + \|x - y\|^2 = 2\|x\|^2 + 2\|y\|^2.$$

U tom je slučaju skalarni produkt sa svojstvom $\|x\| = \sqrt{(x|x)}$ jedinstven i u slučaju polja $K = \mathbb{R}$ zadan je sa:

$$(x|y) = \frac{1}{4}(\|x + y\|^2 - \|x - y\|^2),$$

a u slučaju $K = \mathbb{C}$ sa:

$$(x|y) = \frac{1}{4}(\|x + y\|^2 - \|x - y\|^2 + i\|x + iy\|^2 - i\|x - iy\|^2).$$

Za vektore x, y iz unitarnog prostora X kažemo da su **ortogonalni** (ili **okomiti**) jedan na drugoga i pišemo $x \perp y$ ako je $(x|y) = 0$. Za **vektor** $x \in X$ kažemo da je **ortogonalan na podskup** $S \subseteq X$ i pišemo $x \perp S$ ako je $x \perp y$ za svaki $y \in S$. Za podskupove S i T unitarnog prostora X kažemo da su međusobno **ortogonalni** i pišemo $S \perp T$ ako je $x \perp T$ za svaki $x \in S$. Za svaki podskup S unitarnog prostora X lako se vidi da je $S^{\perp} = \{x \in X; x \perp S\}$ potprostor od X. Nadalje, $S^{\perp} = [S]^{\perp}$ i $S^{\perp} \cap [S] = \{0\}$.

Podskup $S \subseteq X$ zove se **ortogonalan** ako su bilo koja dva njegova elementa međusobno ortogonalna: $x, y \in S$, $x \neq y \Rightarrow (x|y) = 0$. Skup S zove se **ortonormiran**, ako je on ortogonalan i svaki $x \in S$ je jedinični, tj. $\|x\| = 1$.

Propozicija 7.1 *Ako je S ortogonalan podskup unitarnog prostora X i $0 \notin S$, onda je skup S linearno nezavisan.*

Dokaz: Neka su $x_1, x_2, \ldots, x_n \in S$ međusobno različiti vektori i neka su $\lambda_1, \lambda_2, \ldots, \lambda_n \in K$ takvi da je $\lambda_1 x_1 + \lambda_2 x_2 + \ldots + \lambda_n x_n = 0$. Tada zbog međusobne ortogonalnosti vektora $x_1, x_2, \ldots, x_n$ za svaki $j \in \{1, \ldots, n\}$ imamo:

$$0 = (\lambda_1 x_1 + \ldots + \lambda_j x_j + \ldots + \lambda_n x_n | x_j) = \lambda_1 (x_1|x_j) + \ldots + \lambda_j (x_j|x_j) + \ldots + \lambda_n (x_n|x_j) = \lambda_j (x_j|x_j).$$

Kako je $(x_j|x_j) \neq 0$ slijedi $\lambda_j = 0 \ \forall j$. Dakle, skup S je linearno nezavisan.

Posebno, svaki ortonormiran skup je linearno nezavisan. Ortonormiran skup koji je baza od V zove se **ortonormirana baza** od V.

Teorem 7.3 *Neka je $\{e_1, \ldots, e_k\}$ ortonormiran podskup unitarnog prostora X i neka je $x \in X$.*

(a) *Vrijedi tzv.* **Besselova nejednakost**

$$\sum_{j=1}^{k} |(x|e_j)|^2 \leq \|x\|^2.$$

Pri tome vrijedi znak jednakosti ako i samo ako je $x \in [\{e_1, \ldots, e_k\}]$. U tom slučaju je

$$x = \sum_{j=1}^{k} (x|e_j) e_j.$$

(b) *Stavimo*

$$x_0 = \sum_{j=1}^{k} (x|e_j) e_j.$$

Za svaki $y \in [\{e_1, \ldots, e_k\}]$, $y \neq x_0$, vrijedi striktna nejednakost

$$\|x - x_0\| < \|x - y\|.$$

Dakle, x_0 je jedinstvena najbolja aproksimacija vektora x vektorom iz potprostora razapetog vektorima $e_1, \ldots, e_k$.

Dokaz: Dokažimo najprije tvrdnju (b). Neka je $y \in [\{e_1, \ldots, e_k\}]$, dakle za neke skalare $\alpha_1, \ldots, \alpha_k$ je

$$y = \sum_{j=1}^{k} \alpha_j e_j.$$

Primijetimo da je $(e_i|e_j) = \delta_{ij}$. Stoga imamo redom:

$$\|x-y\|^2 - \|x-x_0\|^2 = \Big(x - \sum_{j=1}^{k} \alpha_j e_j \Big| x - \sum_{j=1}^{k} \alpha_j e_j\Big) - \Big(x - \sum_{j=1}^{k} (x|e_j)e_j \Big| x - \sum_{j=1}^{k} (x|e_j)e_j\Big) =$$

$$= (x|x) - \sum_{j=1}^{k} \overline{\alpha_j}(x|e_j) - \sum_{j=1}^{k} \alpha_j \overline{(x|e_j)} + \sum_{j=1}^{k} |\alpha_j|^2 - (x|x) + \sum_{j=1}^{k} \overline{(x|e_j)}(x|e_j) + \sum_{j=1}^{k} (x|e_j)\overline{(x|e_j)} - \sum_{j=1}^{k} |(x|e_j)|^2.$$

U posljednjem se izrazu skraćuju prvi i peti član, te sedmi i osmi član, pa ostaje

$$\|x-y\|^2 - \|x-x_0\|^2 =$$

$$= \sum_{j=1}^{k} |\alpha_j|^2 - \sum_{j=1}^{k} \overline{\alpha_j}(x|e_j) - \sum_{j=1}^{k} \alpha_j \overline{(x|e_j)} + \sum_{j=1}^{k} |(x|e_j)|^2.$$

Odatle je

$$\|x-y\|^2 - \|x-x_0\|^2 = \sum_{j=1}^{k} |\alpha_j - (x|e_j)|^2.$$

Prema tome, ako je $\alpha_j \neq (x|e_j)$ za bilo koji $j \in \{1, 2, \ldots, k\}$, tj. ako je $y \neq x_0$, onda imamo striktnu nejednakost $\|x-y\|^2 - \|x-x_0\|^2 > 0$, odnosno $\|x-x_0\| < \|x-y\|$. Time je dokazana tvrdnja (b).

Dokažimo sada tvrdnju (a). Kao u dokazu tvrdnje (b) nalazimo:

$$0 \leq \Big\| x - \sum_{j=1}^{k} (x|e_j)e_j \Big\|^2 = \|x\|^2 - \sum_{j=1}^{k} |(x|e_j)|^2.$$

Odatle slijedi Besselova nejednakost. Nadalje, vrijedi znak jednakosti ako i samo ako je

$$x = \sum_{j=1}^{k} (x|e_j)e_j.$$

No, koristeći tvrdnju (b) vidimo da je to ispunjeno ako i samo ako je $x \in [\{e_1, \ldots, e_k\}]$.

Sljedeći teorem rješava pitanje egzistencije (pa čak i konstrukcije) ortonormirane baze u konačnodimenzionalnom unitarnom prostoru.

Teorem 7.4 (Gram–Schmidt) *Neka je X unitaran prostor i neka je $x_1, x_2, x_3, \ldots$ konačan ili beskonačan linearno nezavisan niz vektora prostora X.*

(a) *Postoji ortonormiran niz $e_1, e_2, e_3, \ldots$ u X sa svojstvom da je*

$$[\{x_1, x_2, \ldots, x_k\}] = [\{e_1, e_2 \ldots, e_k\}] \qquad \forall k. \tag{1}$$

(*b*) *Uz dodatni uvjet*

$$(e_k|x_k) > 0 \qquad \forall k \tag{2}$$

ortonormiran niz $e_1, e_2, e_3, \ldots$ *iz tvrdnje* (*a*) *je jedinstven.*

Dokaz: $[\{e_1\}] = [\{x_1\}]$ znači da je $e_1 = \alpha x_1$ za neki skalar α. Iz zahtjeva $\|e_1\| = 1$ slijedi da mora biti $|\alpha| = \frac{1}{\|x_1\|}$. Nadalje, $(e_1|x_1) = \alpha\|x_1\|^2$, pa dodatni zahtjev $(e_1|x_1) > 0$ znači da mora biti $\alpha > 0$. Dakle, $\alpha = \frac{1}{\|x_1\|}$, tj $e_1 = \frac{1}{\|x_1\|}x_1$ je jedini jedinični vektor takav da je $[\{e_1\}] = [\{x_1\}]$ i $(e_1|x_1) > 0$.

Pretpostavimo da smo našli ortonormirane vektore $e_1, \ldots, e_n$ takve da vrijede (1) i (2) za $k = 1, 2, \ldots, n$. Dokazat ćemo sada da postoji jedinstven jedinični vektor e_{n+1} takav da vrijede (1) i (2) za $k = n + 1$. Na taj način će teorem 7.4 matematičkom indukcijom biti u potpunosti dokazan.

Zahtjev (1) za $k = n + 1$ znači da mora biti $e_{n+1} \in [\{x_1, x_2, \ldots, x_n, x_{n+1}\}]$, a kako je po pretpostavci $[\{x_1, x_2, \ldots, x_n\}] = [\{e_1, \ldots, e_n\}]$, to znači da mora biti $e_{n+1} \in [\{e_1, \ldots, e_n, x_{n+1}\}]$. Tražimo dakle vektor e_{n+1} u obliku

$$e_{n+1} = \alpha x_{n+1} + \alpha_1 e_1 + \alpha_2 e_2 + \ldots + \alpha_n e_n.$$

Za $1 \le k \le n$ mora biti $0 = (e_{n+1}|e_k) = \alpha(x_{n+1}|e_k) + \alpha_k$, a to znači $\alpha_k = -\alpha(x_{n+1}|e_k)$ za $k = 1, 2, \ldots, n$. Prema tome,

$$e_{n+1} = \alpha y, \text{ gdje je } y = x_{n+1} - (x_{n+1}|e_1)e_1 - (x_{n+1}|e_2)e_2 - \ldots - (x_{n+1}|e_n)e_n.$$

Vektor e_{n+1} je jedinični ako i samo ako je $|\alpha| = \frac{1}{\|y\|}$. Nadalje, imamo

$$(e_{n+1}|x_{n+1}) = \alpha\Big(x_{n+1} - \sum_{k=1}^{n}(x_{n+1}|e_k)e_k\Big|x_{n+1}\Big) = \alpha[\|x_{n+1}\|^2 - \sum_{k=1}^{n}|(x_{n+1}|e_k)|^2].$$

Prema tvrdnji (*a*) teorema 7.3 izraz u uglatoj zagradi je striktno pozitivan jer zbog linearne nezavisnosti vektor x_{n+1} nije u potprostoru $[\{x_1, x_2, \ldots, x_n\}] = = [\{e_1, e_2, \ldots, e_n\}]$. Dakle $(e_{n+1}|x_{n+1}) > 0$ ako i samo ako je $\alpha > 0$. To znači da mora biti $\alpha = \frac{1}{\|y\|}$. Dakle, postoji jedan i samo jedan jedinični vektor e_{n+1} takav da vrijede (1) i (2) za $k = n + 1$. To je vektor $e_{n+1} = \frac{1}{\|y\|}y$ pri čemu je $y = x_{n+1} - \sum_{1\le k\le n}(x_{n+1}|e_k)e_k$.

Za jedinstveni niz $e_1, e_2, e_3, \ldots$ iz tvrdnje (*b*) teorema 7.4 kažemo da je iz niza $x_1, x_2, x_3, \ldots$ dobiven **Gram−Schmidtovim postupkom ortonormiranja**.

Korolar 7.1 *Neka je X konačnodimenzionalan unitaran prostor. Tada postoji ortonormirana baza od X. Štoviše, svaki ortonormiran podskup od X sadržan je u nekoj ortonormiranoj bazi od X.*

Dokaz: Neka je $\{x_1, \ldots, x_k\}$ ortonormiran podskup od X. Tada je taj skup linearno nezavisan, pa je sadržan u nekoj bazi $\{x_1, \ldots, x_k, x_{k+1}, \ldots, x_n\}$ od X. Gram−Schmidtovim postupkom ortonormiranja dolazimo do ortonormirane baze $\{e_1, \ldots, e_k, e_{k+1}, \ldots, e_n\}$ od X. Iz dokaza teorema 7.4 i iz ortonormiranosti skupa $\{x_1, \ldots, x_k\}$ je jasno da je $e_1 = x_1, \ldots, e_k = x_k$. Dakle, ortonormiran skup $\{x_1, \ldots, x_k\}$ sadržan je u ortonormiranoj bazi $\{x_1, \ldots, x_k, e_{k+1}, \ldots, e_n\}$.

Za vektore $x_1, x_2, \ldots, x_n$ unitarnog prostora X stavimo:

$$G(x_1, x_2, \ldots, x_n) = \begin{bmatrix} (x_1|x_1) & (x_1|x_2) & \cdots & (x_1|x_n) \\ (x_2|x_1) & (x_2|x_2) & \cdots & (x_2|x_n) \\ \vdots & \vdots & \ddots & \vdots \\ (x_n|x_1) & (x_n|x_2) & \cdots & (x_n|x_n) \end{bmatrix}$$

Dakle, $G(x_1, x_2, \ldots, x_n)$ je kvadratna matrica $n-$tog reda čiji je element u $i-$tom retku i $j-$tom stupcu jednak $(x_i|x_j)$. Ta se matrica zove **Gramova matrica** vektora $x_1, x_2, \ldots, x_n$. Njena se determinanta označava $\Gamma(x_1, x_2, \ldots, x_n)$ i zove **Gramova determinanta** vektora $x_1, x_2, \ldots, x_n$:

$$\Gamma(x_1, x_2, \ldots, x_n) = \det \begin{bmatrix} (x_1|x_1) & (x_1|x_2) & \cdots & (x_1|x_n) \\ (x_2|x_1) & (x_2|x_2) & \cdots & (x_2|x_n) \\ \vdots & \vdots & \ddots & \vdots \\ (x_n|x_1) & (x_n|x_2) & \cdots & (x_n|x_n) \end{bmatrix}$$

Teorem 7.5 *Neka je X unitaran prostor. Vektori $x_1, x_2, \ldots, x_n \in X$ su linearno nezavisni ako i samo ako je njihova Gramova matrica $G(x_1, x_2, \ldots, x_n)$ regularna, odnosno, ako i samo ako je $\Gamma(x_1, x_2, \ldots, x_n) \neq 0$. U tom slučaju je $\Gamma(x_1, x_2, \ldots, x_n) > 0$.*

Dokaz: Pretpostavimo da su vektori $x_1, x_2, \ldots, x_n$ linearno zavisni i neka su $\lambda_1, \ldots, \lambda_n$ skalari (od kojih je barem jedan različit od nule) takvi da je $\sum_{1\leq k\leq n} \lambda_k x_k = 0$. Tada za svaki $j \in \{1, \ldots, n\}$ vrijedi

$$0 = \Big(\sum_{k=1}^{n} \lambda_k x_k \Big| x_j \Big) = \sum_{k=1}^{n} \lambda_k (x_k|x_j).$$

To znači da sljedeći homogen sustav od n linearnih jednadžbi sa n nepoznanica $\lambda_1, \ldots, \lambda_n$ ima netrivijalno rješenje:

$$\begin{array}{c} (x_1|x_1)\lambda_1 + (x_2|x_1)\lambda_2 + \ldots + (x_n|x_1)\lambda_n = 0 \\ (x_1|x_2)\lambda_1 + (x_2|x_2)\lambda_2 + \ldots + (x_n|x_2)\lambda_n = 0 \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ (x_1|x_n)\lambda_1 + (x_2|x_n)\lambda_2 + \ldots + (x_n|x_n)\lambda_n = 0 \end{array} \tag{3}$$

To znači da je matrica tog sustava singularna. No, matrica sustava (3) je upravo transponirana matrica matrice $G(x_1, x_2, \ldots, x_n)$. Time smo dokazali da iz linearne zavisnosti vektora $x_1, x_2, \ldots, x_n$ slijedi da je matrica $G(x_1, x_2, \ldots, x_n)$ singularna.

Pretpostavimo sada da je matrica $G(x_1, x_2, \ldots, x_n)$ singularna. Tada je i transponirana matrica singularna, što znači da sustav jednadžbi (3) ima netrivijalno rješenje $\lambda_1, \lambda_2, \ldots, \lambda_n$ (dakle, $\lambda_j \neq 0$ za barem jedan indeks j). Stavimo $y = \sum_{1\leq k\leq n} \lambda_k x_k$. Sustav jednadžbi (3) može se kraće zapisati ovako

$$(y|x_j) = 0, \qquad j = 1, 2, \ldots, n.$$

To znači da je $y \perp [\{x_1, x_2, \ldots, x_n\}]$. Međutim, $y \in [\{x_1, x_2, \ldots, x_n\}]$, pa slijedi $y \perp y$, odnosno $(y|y) = 0$. No to je moguće samo ako je $y = 0$, tj. $\sum_{1\leq k\leq n} \lambda_k x_k = 0$. To pokazuje da su vektori $x_1, x_2, \ldots, x_n$ linearno zavisni.

Dokazali smo da su vektori $x_1, x_2, \ldots, x_n$ linearno zavisni ako i samo ako je singularna njihova Gramova matrica $G(x_1, x_2, \ldots, x_n)$. Ekvivalentno, vektori $x_1, x_2, \ldots, x_n$ su linearno nezavisni ako i samo ako je njihova Gramova matrica $G(x_1, x_2, \ldots, x_n)$ regularna.

Dokažimo još pozitivnost Gramove determinante. Pretpostavimo da su vektori $x_1, x_2, \ldots, x_n$ linearno nezavisni. Stavimo

$$x = \sum_{k=1}^{n} (-1)^{n+k} \alpha_k x_k,$$

pri čemu je α_k determinanta matrice reda $n-1$, koja se iz Gramove matrice $G(x_1, x_2, \ldots, x_n)$ dobije tako da se izbriše $k-$ti redak i $n-$ti stupac. Vektor x možemo shvatiti kao razvoj po $n-$tom stupcu determinante matrice koja se iz $G(x_1, x_2, \ldots, x_n)$ dobije tako da se zadnji stupac zamijeni stupcem vektora $x_1, x_2, \ldots, x_n$:

$$x = \det \begin{bmatrix} (x_1|x_1) & (x_1|x_2) & \cdots & (x_1|x_{n-1}) & x_1 \\ (x_2|x_1) & (x_2|x_2) & \cdots & (x_2|x_{n-1}) & x_2 \\ \vdots & \vdots & & \vdots & \vdots \\ (x_n|x_1) & (x_n|x_2) & \cdots & (x_n|x_{n-1}) & x_n \end{bmatrix}$$

Posebno, primijetimo da je $\alpha_n = \Gamma(x_1, x_2, \ldots, x_{n-1})$.

Uz uvedene oznake imamo

$$(x|x_j) = \sum_{k=1}^{n} (-1)^{n+k} \alpha_k (x_k|x_j) = \Gamma_j(x_1, x_2, \ldots, x_n),$$

pri čemu je $\Gamma_j(x_1, x_2, \ldots, x_n)$ oznaka za determinantu matrice koja se iz Gramove matrice dobije tako da se zadnji stupac zamijeni $j-$tim stupcem iste matrice:

$$\Gamma_j(x_1, x_2, \ldots, x_n) = \det \begin{bmatrix} (x_1|x_1) & (x_1|x_2) & \cdots & (x_1|x_{n-1}) & (x_1|x_j) \\ (x_2|x_1) & (x_2|x_2) & \cdots & (x_2|x_{n-1}) & (x_2|x_j) \\ \vdots & \vdots & & \vdots & \\ (x_n|x_1) & (x_n|x_2) & \cdots & (x_n|x_{n-1} & (x_n|x_j) \end{bmatrix}$$

Za $1 \le j \le n-1$ u $\Gamma_j(x_1, x_2, \ldots, x_n)$ su $j-$ti i $n-$ti stupac jednaki, pa je $\Gamma_j(x_1, x_2, \ldots, x_n) = 0$. Nadalje, $\Gamma_n(x_1, x_2, \ldots, x_n) = \Gamma(x_1, x_2, \ldots, x_n)$. Dakle, vrijedi

$$(x|x_j) = 0 \qquad \text{za} \qquad j = 1, \ldots, n-1 \qquad \text{i} \qquad (x|x_n) = \Gamma(x_1, x_2, \ldots, x_n).$$

Odatle je

$$0 \le (x|x) = \Big(x\Big|\sum_{k=1}^{n} (-1)^{n+k} \alpha_k x_k\Big) = \overline{\alpha_n}(x|x_n) = \overline{\Gamma(x_1, x_2, \ldots, x_{n-1})}\Gamma(x_1, x_2, \ldots, x_n).$$

Isto zaključivanje mogli smo provesti za vektore $x_1, \ldots, x_k$ za bilo koji $k \in \{2, \ldots, n\}$. Dakle, vrijedi:

$$\overline{\Gamma(x_1, x_2, \ldots, x_{k-1})}\Gamma(x_1, x_2, \ldots, x_k) \ge 0 \;\text{ za }\; k = 2, \ldots, n.$$

Ali vektori $x_1, x_2, \ldots, x_n$ su linearno nezavisni, pa su sve determinante

$$\Gamma(x_1),\;\; \Gamma(x_1, x_2),\; \ldots\;,\; \Gamma(x_1, x_2, \ldots, x_n)$$

različite od nule. Budući da vrijedi $\Gamma(x_1) = \|x_1\|^2 > 0$, iz gornje nejednakosti za $k = 2$ slijedi $\Gamma(x_1, x_2) > 0$, odatle i iz gornje nejednakosti za $k = 3$ slijedi $\Gamma(x_1, x_2, x_3) > 0$, i tako redom korak po korak sve do $\Gamma(x_1, x_2, \ldots, x_n) > 0$.

Napomena: Nejednakost $\Gamma(x_1, x_2, \ldots, x_n) \ge 0$, s tim da vrijedi znak jednakosti ako i samo ako su vektori $x_1, x_2, \ldots, x_n$ linearno zavisni, je generalizacija nejednakosti Cauchy–Schwarz–Buniakowskog, jer je

$$\Gamma(x, y) = \det \begin{bmatrix} (x|x) & (x|y) \\ (y|x) & (y|y) \end{bmatrix} = \|x\|^2\|y\|^2 - |(x|y)|^2.$$

Teorem 7.6 *Neka je $x_1, x_2, \ldots$ linearno nezavisan niz u unitarnom prostoru X. Jedinstveni ortonormiran niz $e_1, e_2, \ldots$ iz tvrdnje (b) teorema 7.4 dan je formulama*

$$e_1 = \frac{1}{\|x_1\|}x_1, \quad e_k = \frac{\det \begin{bmatrix} (x_1|x_1) & (x_1|x_2) & \cdots & (x_1|x_{k-1}) & x_1 \\ (x_2|x_1) & (x_2|x_2) & \cdots & (x_2|x_{k-1}) & x_2 \\ \vdots & \vdots & & \vdots & \vdots \\ (x_k|x_1) & (x_k|x_2) & \cdots & (x_k|x_{k-1}) & x_k \end{bmatrix}}{\sqrt{\Gamma(x_1, x_2, \ldots, x_{k-1})\Gamma(x_1, x_2, \ldots, x_k)}}, \ k \geq 2,$$

Dakle, za $k \geq 2$ je $e_k = \frac{1}{\sqrt{\Gamma(x_1,x_2,\ldots,x_{k-1})\Gamma(x_1,x_2,\ldots,x_k)}} y_k$ pri čemu je vektor y_k zadan kao determinanta matrice koja se iz Gramove matrice $G(x_1, x_2, \ldots, x_k)$ dobije tako da se zadnji ($k-ti$) stupac zamijeni stupcem vektora $x_1, x_2, \ldots, x_k$ (preciznije, y_k je razvoj te determinante po zadnjem stupcu).

Dokaz: Neka su vektori y_k definirani kao u iskazu teorema:

$$y_1 = x_1, \quad y_k = \det \begin{bmatrix} (x_1|x_1) & (x_1|x_2) & \cdots & (x_1|x_{k-1}) & x_1 \\ (x_2|x_1) & (x_2|x_2) & \cdots & (x_2|x_{k-1}) & x_2 \\ \vdots & \vdots & & \vdots & \vdots \\ (x_k|x_1) & (x_k|x_2) & \cdots & (x_k|x_{k-1}) & x_k \end{bmatrix} \quad \text{za } \ k \geq 2.$$

U dokazu teorema 7.5 vidjeli smo da je tada:

$$(y_k|x_j) = 0 \quad \text{za} \quad 1 \leq j \leq k-1; \qquad (y_k|x_k) = \Gamma(x_1, x_2, \ldots, x_k);$$

$$\|y_k\|^2 = \Gamma(x_1, x_2, \ldots, x_{k-1})\Gamma(x_1, x_2, \ldots, x_k).$$

Vektor y_j je linearna kombinacija vektora $x_1, x_2, \ldots, x_j$. Stoga je

$$[\{y_1, \ldots, y_k\}] \subseteq [\{x_1, \ldots, x_k\}].$$

Nadalje, za $j < k$ vektor y_j je linearna kombinacija vektora $x_1, x_2, \ldots, x_j$, pa zbog $(y_k|x_i) = 0$ za $i < k$ slijedi $(y_k|y_j) = 0$. To pokazuje da su vektori niza $y_1, y_2, y_3, \ldots$ međusobno ortogonalni. Kako je

$$(y_k, x_k) = \Gamma(x_1, x_2, \ldots, x_n) > 0,$$

to je $y_k \neq 0 \ \forall k$. Iz propozicije 7.1 zaključujemo da su vektori $y_1, y_2, y_3, \ldots$ linearno nezavisni, pa slijedi $\dim[\{y_1, \ldots, y_k\}] = k$. Zbog inkluzije $[\{y_1, \ldots, y_k\}] \subseteq [\{x_1, \ldots, x_k\}]$ slijedi jednakost $[\{y_1, \ldots, y_k\}] = [\{x_1, \ldots, x_k\}]$. Napokon, neka su $e_1, e_2, e_3, \ldots$ vektori iz iskaza teorema: $e_k = \frac{1}{\|y_k\|} y_k$. Tada je $e_1, e_2, e_3, \ldots$ ortonormiran niz, $[\{e_1, \ldots, e_k\}] = [\{x_1, \ldots, x_k\}] \, \forall k$ i

$$(x_k|e_k) = \frac{(x_k|y_k)}{\sqrt{\Gamma(x_1, x_2, \ldots, x_k)\Gamma(x_1, x_2, \ldots, x_{k-1})}} = \sqrt{\frac{\Gamma(x_1, x_2, \ldots, x_k)}{\Gamma(x_1, x_2, \ldots, x_{k-1})}} > 0.$$

Time je teorem u potpunosti dokazan.

Teorem 7.7 (teorem o ortogonalnoj projekciji) *Neka je X unitaran prostor i Y konačnodimenzionalan potprostor. Tada je $X = Y \dot{+} Y^{\perp}$. Drugim riječima, za svaki vektor $x \in X$ postoje jedinstveni vektori $y \in Y$ i $z \in Y^{\perp}$ takvi da je $x = y + z$. Nadalje, ako je X konačnodimenzionalan, vrijedi $Y^{\perp\perp} = Y$.*

Dokaz: Neka je $\{e_1, \ldots, e_n\}$ ortonormirana baza od Y. Za dani vektor $x \in X$ stavimo

$$y = \sum_{1 \le k \le n} (x|e_k)e_k \quad \text{i} \quad z = x - y, \quad \text{dakle} \quad x = y + z.$$

Tada je $y \in Y$. Nadalje, za bilo koji $j \in \{1, \ldots, n\}$ je

$$(z|e_j) = (x|e_j) - \left(\sum_{k=1}^{n} (x|e_k)e_k \middle| e_j \right) = (x|e_j) - \sum_{k=1}^{n} (x|e_k)\delta_{kj} = 0,$$

dakle $z \perp [\{e_1, e_2, \ldots, e_n\}] = Y$. Treba još dokazati jedinstvenost takvih vektora. Ako pretpostavimo da su i $y' \in Y$ i $z' \perp Y$ takvi da je $x = y' + z'$, onda je $y + z = y' + z'$, dakle $y - y' = z' - z$. Označimo taj vektor sa u. Tada $u = y - y'$ pokazuje da je $u \in Y$, a $u = z' - z$ pokazuje da je $u \perp Y$. No tada je $u \perp u$, dakle $(u|u) = 0$, odakle slijedi $u = 0$. Dakle, $y' = y$ i $z' = z$.

Dokažimo još posljednju tvrdnju. Prema dokazanom imamo $\dim Y^{\perp} = \dim X - \dim Y$, a odatle

$$\dim Y^{\perp\perp} = \dim X - \dim Y^{\perp} = \dim X - (\dim X - \dim Y) = \dim Y.$$

Kako je očito $Y \subseteq Y^{\perp\perp}$, slijedi $Y^{\perp\perp} = Y$.

Ako je $e = \{e_1, e_2, \ldots, e_n\}$ ortonormirana baza od X onda je $(e_j|e_k) = \delta_{jk}$. Proizvoljan vektor $x \in X$ može se napisati kao linearna kombinacija vektora baze:

$$x = \sum_{j=1}^{n} \alpha_j e_j.$$

Skalarni produkt obje strane te jednakosti s vektorom e_k daje

$$(x|e_k) = \left(\sum_{j=1}^{n} \alpha_j e_j \middle| e_k \right) = \sum_{j=1}^{n} \alpha_j \delta_{jk} = \alpha_k.$$

Dakle, za svaki vektor $x \in X$ vrijedi:

$$x = \sum_{j=1}^{n} (x|e_j)e_j.$$

Ako je $f = \{f_1, f_2, \ldots, f_m\}$ ortonormirana baza drugog unitarnog prostora Y i $A \in L(X, Y)$ sličan račun pokazuje da je element matrice $A(f, e)$ na presjecištu $i-$tog retka i $j-$tog stupca jednak $\alpha_{ij} = (Ae_j|f_i)$:

$$A(f, e) = \begin{bmatrix} (Ae_1|e_1) & (Ae_2|e_1) & \cdots & (Ae_n|e_1) \\ (Ae_1|e_2) & (Ae_2|e_2) & \cdots & (Ae_n|e_2) \\ \vdots & \vdots & \ddots & \vdots \\ (Ae_1|e_n) & (Ae_2|e_n) & \cdots & (Ae_n|e_n) \end{bmatrix}$$

Za konačnodimenzionalan unitaran prostor X svi linearni funkcionali na X mogu se opisati pomoću vektora prostora X :

Teorem 7.8 *Neka je X konačnodimenzionalan unitaran prostor. Za svaki $f \in X'$ postoji jedinstven $y \in X$ takav da vrijedi $f(x) = (x|y)$ za svaki $x \in X$. Označimo li taj y sa $\varphi(f)$, dobivamo preslikavanje $\varphi : X' \to X$ sa svojstvima:*

(a) *φ je bijekcija sa X' na X.*

(b) *Za $f, g \in X'$ i $\lambda, \mu \in K$ vrijedi $\varphi(\lambda f + \mu g) = \overline{\lambda}\varphi(f) + \overline{\mu}\varphi(g)$.*

Dokaz: Neka je $f \in X'$. Ako je $f = 0$ očito za $y = 0$ vrijedi

$$f(x) = (x|y) \qquad \forall x \in X.$$

Neka je $f \neq 0$. Jezgra $N(f) = \{x \in X; f(x) = 0\}$ funkcionala f je potprostor od X. Prema teoremu 7.7 imamo $X = N(f) \dot{+} N(f)^{\perp}$. Rang funkcionala f jednak je 1, jer zbog $f \neq 0$ imamo $R(f) = K$. Po teoremu o rangu i defektu (teorem 2.3) slijedi da je defekt $d(f) = \dim N(f) = \dim X - 1$. Kako je $X = N(f) \dot{+} N(f)^{\perp}$, zaključujemo da je potprostor $N(f)^{\perp}$ jednodimenzionalan. Neka je e jedinični vektor u $N(f)^{\perp}$. Stavimo $y = \overline{f(e)}e$. Neka je x bilo koji vektor iz X. Kako je $X = N(f) \dot{+} N(f)^{\perp}$, postoje skalari $\lambda \in \mathbb{C}$ i vektor $z \in N(f)$ takvi da je $x = \lambda e + z$. Sada je

$$(x) = f(\lambda e + z) = \lambda f(e) + f(z) = \lambda f(e),$$

jer je $z \in N(f)$. Nadalje,

$$(x|y) = (\lambda e + z|\overline{f(e)}e) = \lambda f(e)(e|e) + f(e)(z|e) = \lambda f(e).$$

jer je vektor e jedinični i okomit na $N(f)$. Dakle, vektor y zadovoljava

$$f(x) = (x|y) \qquad \forall x \in X.$$

Dokažimo sada da je takav vektor y jedinstven. Pretpostavimo da i y' ima svojstvo $f(x) = (x|y')$ $\forall x \in X$. Tada je $(x|y - y') = 0$ $\forall x \in X$, pa slijedi $y - y' = 0$, tj. $y = y'$.

Dakle, preslikavanje $\varphi : X' \to X$ iz iskaza teorema je dobro definirano. Iz definicije je jasno da je φ injekcija. To je i surjekcija, jer je za bilo koji $y \in X$ sa $f(x) = (x|y)$ zadan linearan funkcional f na prostoru X i $\varphi(f) = y$.

Napokon, ako su $\lambda, \mu \in K$ i $f, g \in X'$, za svaki $x \in X$ imamo

$$(x|\overline{\lambda}\varphi(f) + \overline{\mu}\varphi(g)) = \lambda(x|\varphi(f)) + \mu(x|\varphi(g)) = \lambda f(x) + \mu g(x) = (\lambda f + \mu g)(x) \; = \; (x|\varphi(\lambda f + \mu g)).$$

Dakle je $\varphi(\lambda f + \mu g) = \overline{\lambda}\varphi(f) + \overline{\mu}\varphi(g)$ i time je teorem 7.8 dokazan.

Teorem 7.9 *Neka su X i Y konačnodimenzionalni unitarni prostori. Za svaki $A \in L(X, Y)$ postoji jedinstven $A^* \in L(Y, X)$ takav da je $(Ax|y) = (x|A^*y)$ za svaki $x \in X$ i svaki $y \in Y$. Vrijedi:*

(a) *$A^{**} = A$ za svaki $A \in L(X, Y)$.*

(b) *$A \mapsto A^*$ je antilinearna bijekcija sa $L(X, Y)$ na $L(Y, X)$.*

(c) *Za $A \in L(X, Y)$ i $B \in L(Y, Z)$ je $(BA)^* = A^*B^*$.*

Dokaz: Neka je $A \in L(X, Y)$ i $y \in Y$. Tada je sa $x \mapsto (Ax|y)$ definiran linearan funkcional na prostoru X. Prema teoremu 7.8 postoji jedinstven vektor iz X, označit ćemo ga sa $A^*(y)$, takav da vrijedi $(Ax|y) = (x|A^*(y))$ $\forall x \in X$. Na taj način došli smo do dobro definiranog preslikavanja $A^* : Y \to X$.

Dokažimo da je operator A^* linearan. Za dane $\lambda, \mu \in K$ i $y, z \in Y$ i za bilo koji $x \in X$ imamo

$$(x|A^*(\lambda y + \mu z) - \lambda A^*(y) - \mu A^*(z)) =$$

$$= (x|A^*(\lambda y + \mu z)) - \overline{\lambda}(x|A^*(y)) - \overline{\mu}(x|A^*(z)) = (Ax|\lambda y + \mu z) - \overline{\lambda}(Ax|y) - \overline{\mu}(Ax|z) = 0,$$

jer je skalarni produkt antilinearan u drugom argumentu. Kako to vrijedi za svaki vektor $x \in X$ zaključujemo da je $A^*(\lambda y + \mu z) = \lambda A^*(y) + \mu A^*(z)$.

Očito je $A^{**} = A$, a odatle odmah slijedi da je preslikavanje $A \mapsto A^*$ bijektivno. Doista, ako za $B \in L(Y, X)$ stavimo $A = B^*$, onda je $A^* = B^{**} = B$. Dakle, preslikavanje $A \mapsto A^*$ je surjektivno. Nadalje, ako su $A, C \in L(X, Y)$ takvi da je $A^* = C^*$, onda imamo $A = A^{**} = C^{**} = C$. Dakle, to preslikavanje je i injektivno.

Dokažimo sada da je preslikavanje $A \mapsto A^*$ antilinearno. Za $\lambda, \mu \in K$ i $A, B \in L(X, Y)$ imamo za svaki $x \in X$ i svaki $y \in Y$:

$$(x|(\lambda A + \mu B)^* y) = ((\lambda A + \mu B)x|y) = \lambda(Ax|y) + \mu(Bx|y) =$$

$$= \lambda(x|A^*y) + \mu(x|B^*z) = (x|\overline{\lambda}A^*y + \overline{\mu}B^*y) = (x|(\overline{\lambda}A^* + \overline{\mu}B^*)y).$$

Dakle je $(\lambda A + \mu B)^* = \overline{\lambda}A^* + \overline{\mu}B^*$, odnosno preslikavanje $A \mapsto A^*$ je antilinearno.

Napokon, za unitarne prostore X, Y i Z, i za $A \in B(X, Y)$, $B \in B(Y, Z)$, $x \in X$ i $z \in Z$ imamo
$(x|A^*B^*z) = (Ax|B^*z) = (BAx|z) = (x|(BA)^*z)$. Dakle je $(BA)^* = A^*B^*$.

Za operator A^* kažemo da je **adjungiran** operatoru A.

Propozicija 7.2 *Neka su X i Y konačnodimenzionalni unitarni prostori i $A \in L(X, Y)$. Tada vrijedi*

$$N(A) = R(A^*)^\perp, \ \ R(A) = N(A^*)^\perp, \ \ N(A^*) = R(A)^\perp, \ \ R(A^*) = N(A)^\perp.$$

Dokaz: Zbog činjenice $A^{**} = A$ zamjenom uloga A i A^* vidimo da su međusobno ekvivalentne prva i treća jednakost, a isto tako i druga i četvrta jednakost. Nadalje, kako je po teoremu 7.7 $R(A)^{\perp\perp} = R(A)$, druga i treća jednakost su međusobno ekvivalentne. Dakle, sve četiri jednakosti su međusobno ekvivalentne pa je dovoljno dokazati jednu od njih, npr. prvu. Za $x \in X$ imamo redom:

$$x \in N(A) \quad \Leftrightarrow \quad Ax = 0 \quad \Leftrightarrow \ (Ax|y) = 0 \ \forall y \in Y \quad \Leftrightarrow \quad (x|A^*y) = 0 \ \forall y \in Y \quad \Leftrightarrow \quad x \perp R(A^*).$$

Dakle je $N(A) = R(A^*)^\perp$.

Za konačnodimenzionalan unitaran prostor X operator $A \in L(X)$ zove se:

– **hermitski,** ako vrijedi $A^* = A$;

– **antihermitski,** ako vrijedi $A^* = -A$;

– **unitaran,** ako je $AA^* = A^*A = I$; tj. A je invertibilan u $L(X)$ i $A^{-1} = A^*$;

– **normalan,** ako je $AA^* = A^*A$.

Primijetimo da su i hermitski i antihermitski i unitarni operatori normalni operatori.

Propozicija 7.3 *Neka je X konačnodimenzionalan unitaran prostor i neka je $A \in L(X)$.*

(*a*) *Ako je operator A hermitski i $(Ax|x) = 0 \ \forall x \in X$ onda je $A = 0$.*

(*b*) *Operator A je normalan ako i samo ako je $\|Ax\| = \|A^*x\| \ \forall x \in X$.*

(*c*) *Ako je operator A normalan onda je $N(A) = N(A^*)$.*

(*d*) *Ako je operator A normalan i* $Ax = \alpha x$ *za* $x \in X$ *i* $\alpha \in \mathbb{C}$, *onda je* $A^*x)\overline{\alpha}x$.

Dokaz: (*a*) Za bilo koje $x, y \in X$ imamo:

$$0 = (A(x+y)|x+y) = (Ax|x) + (Ax|y) + (Ay|x) + (Ay|y) = (Ax|y) + (y|Ax) = 2\mathrm{Re}(Ax|y).$$

Dakle je $\mathrm{Re}(Ax|y) = 0 \ \forall x, y \in X$. Tada slijedi i

$$0 = \mathrm{Re}(Ax|iy) = \mathrm{Re}[(-i)(Ax|y)] = \mathrm{Im}(Ax|y).$$

Stoga je $(Ax|y) = 0 \ \forall x, y \in X$. Odatle slijedi $Ax = 0 \ \forall x \in X$, dakle $A = 0$.

(*b*) Pretpostavimo da je operator A normalan. Za $x \in X$ tada imamo:

$$\|Ax\|^2 = (Ax|Ax) = (A^*Ax|x) = (AA^*x|x) = (A^*x|A^*x) = \|A^*x\|^2.$$

Obratno, ako pretpostavimo da vrijedi $\|Ax\| = \|A^*x\| \ \forall x \in X$, onda dobivamo:

$$0 = \|Ax\|^2 - \|A^*x\|^2 = (Ax|Ax) - (A^*x|A^*x) = (A^*Ax|x) - (AA^*x|x) = ((A^*A - AA^*)x|x).$$

Dakle, za hermitski operator $B = A^*A - AA^*$ vrijedi $(Bx|x) = 0 \ \forall x \in X$. Prema (*a*) slijedi $B = 0$, tj. $A^*A = AA^*$.

Tvrdnja (*c*) slijedi neposredno iz tvrdnje (*b*) ($Ax = 0 \ \Leftrightarrow \ A^*x = 0$).

(*d*) Stavimo $B = A - \alpha I$. Tada je operator B normalan i $B^* = A^* - \overline{\alpha}I$. Zbog (*c*) nalazimo:

$$Ax = \alpha x \qquad \Rightarrow \qquad x \in N(B) \qquad \Rightarrow \qquad x \in N(B^*) \qquad \Rightarrow \qquad A^*x = \overline{\alpha}x.$$

Teorem 7.10 *Neka je X konačnodimenzionalan kompleksan unitaran prostor i neka je* $A \in L(X)$. *Sljedeća su dva svojstva međusobno ekvivalentna:*

(*a*) *Operator A je normalan.*

(*b*) *Postoji ortonormirana baza e takva da je matrica A(e) dijagonalna.*

Dokaz: Pretpostavimo da vrijedi (*b*) i neka je $e = \{e_1, e_2, \ldots, e_n\}$ ortonormirana baza od X takva da je matrica $A(e)$ dijagonalna. Neka su redom $\alpha_1, \alpha_2, \ldots, \alpha_n$ dijagonalni elementi matrice $A(e)$. To znači da je $Ae_j = \alpha_j e_j$ za $j = 1, 2, \ldots, n$. Prema tvrdnji (*d*) propozicije 7.3 tada je $A^*e_j = \overline{\alpha_j}e_j$ za $j = 1, 2, \ldots, n$, što znači da je i matrica $A^*(e)$ dijagonalna. Dijagonalne matrice međusobno komutiraju pa imamo

$$(A^*A)(e) = A^*(e)A(e) = A(e)A^*(e) = (AA^*)(e).$$

Odatle slijedi da je $AA^* = A^*A$, odnosno operator A je normalan. Time je dokazano da iz (*b*) slijedi (*a*).

Dokažimo sada da iz (*a*) slijedi (*b*). Tu ćemo implikaciju dokazati matematičkom indukcijom u odnosu na $\dim X$. Baza indukcije $\dim X = 1$ je trivijalna, jer je svaka matrica operatora na jednodimenzionalnom prostoru dijagonalna. Da provedemo korak indukcije, pretpostavimo da je $n \geq 2$ i da je implikacija (*a*) $\Rightarrow$ (*b*) dokazana ako je $\dim X < n$. Neka je $\dim X = n$ i neka je operator $A \in L(X)$ normalan. Neka α neka svojstvena vrijednost od A i e_1 neki pripadni jedinični svojstveni vektor: $Ae_1 = \alpha e_1$. Prema tvrdnji (*d*) propozicije 7.3 tada je $A^*e = \overline{\alpha}e_1$. Stavimo $Y = [\{e_1\}]^\perp = \{x \in X;\ (x|e_1) = 0\}$. Ako je $x \in Y$, imamo $(Ax|e_1) = (x|A^*e_1) = (x|\overline{\alpha}e_1) = \alpha(x|e_1) = 0$, tj. $Ax \in X$. Dakle vrijedi $x \in Y \ \Rightarrow \ Ax \in Y$, tj. potprostor Y je $A-$invarijantan. Analogno se dokazuje da je Y i A^*-invarijantan. Restrikcija $A|Y$ je normalan operator na unitarnom prostoru Y. Kako je $\dim\, Y = \dim\, X - 1 = n - 1 < n$, po pretpostavci indukcije postoji ortonormirana baza $\{e_2, \dots, e_n\}$ od Y u kojoj operator $A|Y$ ima dijagonalnu matricu. No tada je $e = \{e_1, e_2, \dots, e_n\}$ ortonormirana baza od X takva da je matrica $A(e)$ dijagonalna.

Time je teorem u potpunosti dokazan.

Može se dokazati da vrijedi i više od implikacije $(a) \Rightarrow (b)$: *Ako je X konačnodimenzionalan kompleksan unitaran prostor i ako je $\mathfrak{A}$ podskup od $L(X)$ koji se sastoji od normalnih operatora koji međusobno komutiraju, onda postoji ortonormirana baza e od X, takva da je matrica $A(e)$ dijagonalna za svaki operator $A \in \mathfrak{A}$.*

Za konačnodimenzionalan unitaran prostor X označimo sa $U(X)$ skup svih unitarnih operatora $A \in L(X)$.

Propozicija 7.4 *$U(X)$ je podgrupa grupe $GL(X)$.*

Dokaz: Po definiciji je svaki unitaran operator regularan, dakle vrijedi $U(X) \subseteq GL(X)$. Očito je $I^* = I = I^{-1}$, dakle, $I \in U(X)$. Za $A, B \in U(X)$ imamo $(AB)^* = B^*A^* = B^{-1}A^{-1} = (AB)^{-1}$, dakle $AB \in U(X)$. Napokon, za $A \in U(X)$ je $(A^{-1})^* = (A^*)^{-1} = (A^{-1})^{-1}$, pa slijedi $A^{-1} \in U(X)$.

Propozicija 7.5 *Operator $A \in L(X)$ je unitaran ako i samo ako vrijedi*

$$(Ax|Ay) = (x|y) \qquad \forall x, y \in X.$$

Dokaz: Ako je $A \in U(X)$ onda je $A^*A = I$, pa za bilo koje vektore $x, y \in X$ imamo

$$(Ax|Ay) = (x|A^*Ay) = (x|Iy) = (x|y).$$

Pretpostavimo da vrijedi $(Ax|Ay) = (x|y)\ \forall x, y \in X$. Tada je

$$(x|A^*Ay) = (Ax|Ay) = (x|y) = (x|Iy) \qquad \forall x, y \in X,$$

pa slijedi $A^*A = I$. Odatle je $A^* = A^{-1}$, dakle, $A \in U(X)$.

Grupa $U(X)$ ima u odnosu na ortonormirane baze istu ulogu kao i grupa $GL(X)$ u odnosu na proizvoljne baze:

Teorem 7.11 *Neka je X konačnodimenzionalan unitaran prostor.*

(a) *Ako je $A \in L(X)$ i ako je za neku ortonormiranu bazu $e = \{e_1, \dots, e_n\}$ od X i $Ae = \{Ae_1, \dots, Ae_n\}$ ortonormirana baza od X, onda je $A \in U(X)$.*

(b) *Ako je $A \in U(X)$ i ako je e ortonormirana baza od X onda je i Ae ortonormirana baza od X.*

Dokaz: (a) Neka su $x, y \in X$ i $x = \sum_{k=1}^n \alpha_k e_k$, $y = \sum_{k=1}^n \beta_k e_k$. Tada imamo redom:

$$(Ax|Ay) = \Big(\sum_{k=1}^n \alpha_k Ae_k \Big| \sum_{j=1}^n \beta_j Ae_j\Big) = \sum_{k=1}^n \sum_{j=1}^n \alpha_k \overline{\beta_j} (Ae_k|Ae_j) = \sum_{k=1}^n \sum_{j=1}^n \alpha_k \overline{\beta_j} \delta_{kj} =$$

$$= \sum_{k=1}^n \sum_{j=1}^n \alpha_k \overline{\beta_j} (e_k|e_j) = \Big(\sum_{k=1}^n \alpha_k e_k \Big| \sum_{j=1}^n \beta_j e_j\Big) = (x|y).$$

(*b*) Neka je $A \in U(X)$ i neka je $e = \{e_1, e_2, \ldots, e_n\}$ ortonormirana baza od X. Tada je

$$(Ae_k|Ae_j) = (e_k|A^*Ae_j) = (e_k|e_j) = \delta_{kj}.$$

Dakle, Ae je ortonormirana baza od X.

Za hermitske operatore teorem 7.10 o dijagonalizaciji vrijedi ne samo za kompleksne nego i za realne unitarne prostore.

Teorem 7.12 *Neka je X konačnodimenzionalan realan ili kompleksan vektorski prostor i $A \in L(X)$ hermitski operator.*

(*a*) *Svi koeficijenti i sve nultočke polinoma $\mu_A(\lambda)$ su realni.*

(*b*) *Postoji ortonormirana baza e prostora X sastavljena od svojstvenih vektora operatora A, tj. takva da je matrica $A(e)$ dijagonalna.*

Dokaz: (*a*) Pretpostavimo prvo da je $K = \mathbb{C}$. Neka je $\alpha \in \sigma(A)$ i neka je $e \in X$ pripadni jedinični svojstveni vektor. Tada je

$$\lambda = \lambda(e|e) = (\lambda e|e) = (Ae|e) = (e|Ae) = (e|\lambda e) = \overline{\lambda}(e|e) = \overline{\lambda} \qquad \Longrightarrow \qquad \alpha \in \mathbb{R}.$$

Dakle, $\sigma(A) \subseteq \mathbb{R}$, pa slijedi da su sve nultočke polinoma $\mu_a(\lambda)$ realne. Nadalje, tada je

$$\mu_A(\lambda) = (\lambda - \alpha_1)(\lambda - \alpha_2)\cdots(\lambda - \alpha_m) \qquad \text{za neke} \;\; \alpha_1, \alpha_2, \cdots, \alpha_m \in \mathbb{R},$$

odakle slijedi da su svi koeficijenti polinoma $\mu_A(\lambda)$ realni.

Neka je sada $K = \mathbb{R}$. Tada su očito svi koeficijenti polinoma $\mu_A(\lambda)$ realni. Dakažimo još da su i u ovom slučaju sve nultočke polinoma $\mu_A(\lambda)$ realne. Pretpostavimo suprotno, tj. da postoji $\lambda_0 \in \mathbb{C} \setminus \mathbb{R}$ takav da je $\mu_A(\lambda_0) = 0$. Budući da su koeficijenti polinoma $\mu_A(\lambda)$ realni, slijedi da je i $\overline{\lambda_0}$ nultočka polinoma $\mu(\lambda)$. Tada je polinom $\mu_A(\lambda)$ djeljiv s realnim polinomom $(\lambda - \lambda_0)(\lambda - \overline{\lambda_0})$. Stavimo $\lambda_0 = \sigma + i\rho$, gdje su $\sigma, \rho \in \mathbb{R}$ i $\rho \neq 0$. Tada je

$$(\lambda - \lambda_0)(\lambda - \overline{\lambda_0}) = (\lambda - \sigma - i\rho)(\lambda - \sigma + i\rho) = (\lambda - \sigma)^2 + \rho^2.$$

Dakle, za neki realni polinom $\nu(\lambda)$ vrijedi

$$\mu_A(\lambda) = [(\lambda - \sigma)^2 + \rho^2]\nu(\lambda).$$

Odatle je

$$0 = \mu_A(A) = [(A - \sigma I)^2 + \rho^2 I]\nu(A).$$

Imamo $\deg \nu(\lambda) = \deg \mu_A(\lambda) - 2 < \deg \mu_A(\lambda)$, dakle $\nu(A) \neq 0$. To znači da postoji vektor $x \in X$ takav da je $y = \nu(A)x \neq 0$. Tada je $[(A - \sigma I)^2 + \rho^2 I]y = 0$. Kako je operator A hermitski i $\sigma \in \mathbb{R}$, slijedi da je i operator $A - \sigma I$ hermitski. Stoga imamo

$$0 = ([(A - \sigma I)^2 + \rho^2 I]y|y) = ((A - \sigma I)^2 y|y) + \rho^2 (y|y) =$$

$$= ((A - \sigma I)y|(A - \sigma I)y) + \rho^2 (y|y) = \|(A - \sigma I)y\|^2 + \rho^2 \|y\|^2.$$

No to je nemoguće, jer je $\|(A - \sigma I)y\|^2 \geq 0$ i $\rho^2 \|(y\|^2 > 0$. Ova kontradikcija pokazuje da je pogrešna bila pretpostavka o postojanju nultočke od $\mu_A(\lambda)$ koja nije realna. Time je dokazano da je i u slučaju $K = \mathbb{R}$ svaka nultočka polinoma $\mu_A(\lambda)$ realna.

(*b*) Zbog (*a*) se dokaz implikacije (*a*) $\Rightarrow$ (*b*) u teoremu 7.10 može bez izmjene provesti i ako je

A hermitski operator na konačnodimenzionalnom realnom unitarnom prostoru X. Naime, uzmemo li bilo koju nultočku $\alpha_1 \in \mathbb{R}$ minimalnog polinoma $\mu_A(\lambda)$ operatora A, onda je $\alpha_1 \in \sigma(A)$, pa postoji jedinični vektor $e_1 \in X$ takav da je $Ae_1 = \alpha_1 e_1$. Tada je $Y = [\{e_1\}]^\perp$ $A-$invarijantan potprostor:

$$y \perp e_1 \quad \Longrightarrow \quad (Ay|e_1) = (y|Ae_1) = (y|\alpha_1 e_1) = \alpha_1(x|e_1) = 0 \quad \Longrightarrow \quad Ay \perp e_1.$$

Operator $A|Y$ je hermitski, pa koristeći matematičku indukciju dolazimo do ortonormirane baze $\{e_2, \ldots, e_n\}$ od Y sastavljene od svojstvenih vektora operatora $A|Y$. No tada je $\{e_1, e_2, \ldots, e_n\}$ ortonormirana baza od X sastavljena od svojstvenih vektora operatora A.

8 Funkcije operatora

U cijelom ovom poglavlju V predstavlja konačnodimenzionalan vektorski prostor nad poljem $\mathbb{C}$ kompleksnih brojeva. Za svaki polinom $P(\lambda)$ i svaki $A \in L(V)$ dobro je definiran operator $P(A)$ i pridruživanje $P(\lambda) \mapsto P(A)$ prevodi računske operacije s polinomima u računske operacije s operatorima:

(1) Ako je $P(\lambda) = 1$, onda je $P(A) = I$.

(2) Ako je $Q(\lambda) = \alpha P(\lambda)$, onda je $Q(A) = \alpha P(A)$ $(\alpha \in \mathbb{C})$.

(3) Ako je $R(\lambda) = P(\lambda) + Q(\lambda)$, onda je $R(A) = P(A) + Q(A)$.

(4) Ako je $S(\lambda) = P(\lambda)Q(\lambda)$, onda je $S(A) = P(A)Q(A)$.

Označimo sa $\mathcal{P}$ skup svih polinoma. To je podskup skupa svih funkcija $\mathbb{C}^{\mathbb{C}}$ sa $\mathbb{C}$ u $\mathbb{C}$. Cilj je ovog poglavlja da za svaki linearan operator $A \in L(V)$ preslikavanje $P(\lambda) \mapsto P(A)$ sa $\mathcal{P}$ u $L(V)$ proširimo do preslikavanja sa čim većeg podskupa od $\mathbb{C}^{\mathbb{C}}$ u $L(V)$, ali tako da i dalje vrijede pravila $(1) - (4)$.

Funkcije najsličnije polinomima su redovi potencija

$$f(\lambda) = \sum_{k=0}^{\infty} \alpha_k \lambda^k, \qquad \lambda \in \mathbb{C}.$$

Ako gornji red potencija konvergira za svaki $\lambda \in \mathbb{C}$, funkcija $f : \mathbb{C} \to \mathbb{C}$ koju taj red definira zove se **cijela funkcija**. U tom slučaju prirodno je pokušati definirati $f(A)$ kao odgovarajući red potencija operatora A :

$$f(A) = \sum_{k=0}^{\infty} \alpha_k A^k, \qquad A \in L(V).$$

Međutim, da bismo mogli promatrati redove potencija linearnog operatora, treba nam pojam konvergencije u prostoru operatora. Neka su V i W konačnodimenzionalni vektorski prostori nad poljem $\mathbb{C}$. Za niz $(A_k)_{k\in\mathbb{N}}$ u $L(V,W)$ i za $A \in L(V,W)$ kažemo da **niz operatora** (A_k) **konvergira** prema operatoru A i pišemo $A = \lim_{k\to\infty} A_k$ ako postoje baza $e = \{e_1, e_2, \dots, e_n\}$ prostora V i baza $f = \{f_1, f_2, \dots, f_m\}$ prostora W takve da za matrice

$$A_k(f,e) = \begin{bmatrix} \alpha_{11}^{(k)} & \alpha_{12}^{(k)} & \cdots & \alpha_{1n}^{(k)} \\ \alpha_{21}^{(k)} & \alpha_{22}^{(k)} & \cdots & \alpha_{2n}^{(k)} \\ \vdots & \vdots & & \vdots \\ \alpha_{m1}^{(k)} & \alpha_{m2}^{(k)} & \cdots & \alpha_{mn}^{(k)} \end{bmatrix} \qquad \text{i} \qquad A(f,e) = \begin{bmatrix} \alpha_{11} & \alpha_{12} & \cdots & \alpha_{1n} \\ \alpha_{21} & \alpha_{22} & \cdots & \alpha_{2n} \\ \vdots & \vdots & & \vdots \\ \alpha_{m1} & \alpha_{m2} & \cdots & \alpha_{mn} \end{bmatrix}$$

vrijedi

$$\alpha_{ij} = \lim_{k\to\infty} \alpha_{ij}^{(k)} \qquad \forall i \in \{1,2,\dots,m\}, \qquad \forall j \in \{1,2,\dots,n\}. \qquad (*)$$

Primijetimo da ta definicija konvergencije u prostoru $L(V,W)$ samo prividno ovisi o tome koje smo baze e i f izabrali. Doista, neka su $e' = \{e'_1, e'_2, \dots, e'_n\}$ druga baza od V i $f' = \{f'_1, f'_2, \dots, f'_m\}$ druga baza od W. Neka su $S \in GL(V)$ i $T \in GL(W)$ operatori prijelaza: $Se_i = e'_i$, $1 \le i \le n$, $Tf_j = f'_j$, $1 \le j \le m$. Prema propoziciji 2.4 tada vrijedi

$$A_k(f',e') = S(f)^{-1} A_k(f,e) T(e), \quad k \in \mathbb{N}, \qquad \text{i} \qquad A(f',e') = S(f)^{-1} A(f,e) T(e). \qquad (**)$$

Izaberimo oznake za elemente matrica:

$$A_k(f',e') = \begin{bmatrix} \beta_{11}^{(k)} & \beta_{12}^{(k)} & \cdots & \beta_{1n}^{(k)} \\ \beta_{21}^{(k)} & \beta_{22}^{(k)} & \cdots & \beta_{2n}^{(k)} \\ \vdots & \vdots & & \vdots \\ \beta_{m1}^{(k)} & \beta_{m2}^{(k)} & \cdots & \beta_{mn}^{(k)} \end{bmatrix}, \qquad A(f',e') = \begin{bmatrix} \beta_{11} & \beta_{12} & \cdots & \beta_{1n} \\ \beta_{21} & \beta_{22} & \cdots & \beta_{2n} \\ \vdots & \vdots & & \vdots \\ \beta_{m1} & \beta_{m2} & \cdots & \beta_{mn} \end{bmatrix},$$

$$S(f)^{-1} = \begin{bmatrix} \sigma_{11} & \sigma_{12} & \cdots & \sigma_{1m} \\ \sigma_{21} & \sigma_{22} & \cdots & \sigma_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_{m1} & \sigma_{m2} & \cdots & \sigma_{mm} \end{bmatrix}, \qquad T(e) = \begin{bmatrix} \tau_{11} & \tau_{12} & \cdots & \tau_{1n} \\ \tau_{21} & \tau_{22} & \cdots & \tau_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ \tau_{n1} & \tau_{n2} & \cdots & \tau_{nn} \end{bmatrix}.$$

Pisane pomoću elemenata matrične jednakosti $(**)$ izgledaju ovako:

$$\beta_{pq}^{(k)} = \sum_{i=1}^{m}\sum_{j=1}^{n} \sigma_{pi}\alpha_{ij}^{(k)}\tau_{jq} \qquad (k \in \mathbb{N}) \qquad \text{i} \qquad \beta_{pq} = \sum_{i=1}^{m}\sum_{j=1}^{n} \sigma_{pi}\alpha_{ij}\tau_{jq}.$$

Iz tih jednakosti i iz $(*)$ neposredno slijedi

$$\beta_{pq} = \lim_{k\to\infty} \beta_{pq}^{(k)} \qquad \forall p \in \{1,2,\ldots,m\}, \qquad \forall q \in \{1,2,\ldots,n\}.$$

Dakle, konvergencija matričnih elemenata iz definicije konvergencije operatora ispunjena je u svim parovima baza u dva vektorska prostora.

Za **red operatora** $\sum_{k=0}^{\infty} A_k$ kažemo da **konvergira**, ako konvergira niz (S_k) parcijalnih suma, gdje je

$$S_k = \sum_{j=0}^{k} A_k.$$

Limes niza parcijalnih sume zove se tada suma toga reda.

Propozicija 8.1 *Neka je $f : \mathbb{C} \to \mathbb{C}$ cijela funkcija:*

$$f(\lambda) = \sum_{k=0}^{\infty} \alpha_k \lambda^k, \qquad \lambda \in \mathbb{C},$$

i neka je $A \in L(V)$. Tada red operatora

$$\sum_{k=0}^{\infty} \alpha_k A^k$$

konvergira.

Dokaz: Iz teorije analitičkih funkcija kompleksne varijable znamo da ako red potencija

$$\sum_{k=0}^{\infty} \alpha_k \lambda^k$$

konvergira za svaki $\lambda \in \mathbb{C}$, onda taj red apsolutno konvergira za svaki $\lambda \in \mathbb{C}$, tj. konvergira red apsolutnih vrijednosti

$$\sum_{k=0}^{\infty} |\alpha_k| \cdot |\lambda|^k.$$

Neka je $e = \{e_1, e_2, \ldots, e_n\}$ baza od V i neka su α_{ij} elementi matrice operatora A u toj bazi:

$$A(e) = \begin{bmatrix} \alpha_{11} & \alpha_{12} & \cdots & \alpha_{1n} \\ \alpha_{21} & \alpha_{22} & \cdots & \alpha_{2n} \\ \vdots & \vdots & & \vdots \\ \alpha_{n1} & \alpha_{n2} & \cdots & \alpha_{nn} \end{bmatrix}.$$

Nadalje, za bilo koji $k \geq 0$ označimo sa $\alpha_{ij}^{(k)}$ elemente matrice $A^k(e) = A(e)^k$:

$$A^k(e) = \begin{bmatrix} \alpha_{11}^{(k)} & \alpha_{12}^{(k)} & \cdots & \alpha_{1n}^{(k)} \\ \alpha_{21}^{(k)} & \alpha_{22}^{(k)} & \cdots & \alpha_{2n}^{(k)} \\ \vdots & \vdots & & \vdots \\ \alpha_{n1}^{(k)} & \alpha_{n2}^{(k)} & \cdots & \alpha_{nn}^{(k)} \end{bmatrix}.$$

Neka je $M > 0$ takav da je $|\alpha_{ij}| \leq M \quad \forall i, j$. Tada za svako $k \geq 0$ vrijedi

$$|\alpha_{ij}^{(k)}| \leq (nM)^k, \qquad \forall i, j. \qquad\qquad (\dagger)$$

Dokazat ćemo nejednakost $(\dagger)$ indukcijom u odnosu na $k \geq 0$. Što se tiče baze indukcije, tj. za $k = 0$, nejednakost $(\dagger)$ je očito istinita, jer je $A^0 = I$, dakle, $\alpha_{ij}^{(0)} = \delta_{ij}$. Pretpostavimo sada da $(\dagger)$ vrijedi za neki $k \geq 0$. Tada zbog jednakosti $A^{k+1} = A \cdot A^k$ imamo redom

$$|\alpha_{ij}^{(k+1)}| = \Big|\sum_{\ell=1}^{n} \alpha_{i\ell}\alpha_{\ell j}^{(k)}\Big| \leq \sum_{\ell=1}^{n} |\alpha_{i\ell}| \cdot |\alpha_{\ell j}^{(k)}| \leq \sum_{\ell=1}^{n} M(nM)^k = (nM)^{k+1}.$$

Time je proveden korak indukcije i time je dokazana nejednakost $(\dagger)$ za sve $k \geq 0$. Odatle slijedi da je $|\alpha_k \alpha_{ij}^{(k)}| \leq (nM)^k$, dakle red apsolutnih vrijednosti $\sum_{k=0}^{\infty} |\alpha_k \alpha_{ij}^{(k)}|$ majoriziran je konvergentnim redom $\sum_{k=0}^{\infty} |\alpha_{ij}|(nM)^k$. Zaključujemo da svi redovi $\sum_{k=0}^{\infty} \alpha_k \alpha_{ij}^{(k)}$, $i, j \in \{1, \ldots, n\}$, konvergiraju apsolutno. No to znači da red operatora $\sum_{k=0}^{\infty} \alpha_k A^k$ konvergira.

Za cijelu funkciju f iz propozicije 8.1 i za operator $A \in L(V)$ stavljamo

$$f(A) = \sum_{k=0}^{\infty} \alpha_k A^k.$$

Operator $f(A)$ zove se **cijela funkcija operatora** A.

Propozicija 8.2 *Neka su $f, g : \mathbb{C} \to \mathbb{C}$ cijele funkcije, $\alpha \in \mathbb{C}$ i $A \in L(V)$. Tada je*

$$(\alpha f)(A) = \alpha f(A), \qquad (f + g)(A) = f(A) + g(A), \qquad (f \cdot g)(A) = f(A)g(A).$$

Dokaz: Neka je

$$f(\lambda) = \sum_{k=0}^{\infty} \alpha_k \lambda^k \qquad \text{i} \qquad g(\lambda) = \sum_{k=0}^{\infty} \beta_k \lambda^k.$$

Tada je

$$(\alpha f)(\lambda) = \sum_{k=0}^{\infty} \alpha\alpha_k \lambda^k \qquad \text{i} \qquad (f + g)(\lambda) = \sum_{k=0}^{\infty} (\alpha_k + \beta_k) A^k,$$

pa imamo redom

$$(\alpha f)(A)=\sum_{k=0}^{\infty}\alpha\alpha_k A^k=\lim_{m\to\infty}\sum_{k=0}^{m}\alpha\alpha_k A^k=\lim_{m\to\infty}\alpha\sum_{k=0}^{m}\alpha_k A^k=$$

$$=\alpha\lim_{m\to\infty}\sum_{k=0}^{m}\alpha_k A^k=\alpha\sum_{k=0}^{\infty}\alpha_k A^k=\alpha f(A)$$

i

$$(f+g)(A)=\sum_{k=0}^{\infty}(\alpha_k+\beta_k)A^k=\lim_{m\to\infty}\sum_{k=0}^{m}(\alpha_k+\beta_k)A^k=\lim_{m\to\infty}\Big(\sum_{k=0}^{m}\alpha_k A^k+\sum_{k=0}^{m}\beta_k A^k\Big)=$$

$$=\lim_{m\to\infty}\sum_{k=0}^{m}\alpha_k A^k+\lim_{m\to\infty}\sum_{k=0}^{m}\beta_k A^k=\sum_{k=0}^{\infty}\alpha_k A^k+\sum_{k=0}^{\infty}\beta_k A^k=f(A)+g(A).$$

Dokažimo još i treću jednakost. Neka je e baza prostora. Za bilo koji operator $B\in L(V)$ sa $B(e)_{ij}$ ćemo označiti element matrice $B(e)$ na presjecištu $i-$tog retka i $j-$tog stupca. Prema dokazu propozicije 8.1 redovi matričnih elemenata apsolutno su konvergentni, pa u njihovom produktu možemo po volji mijenjati redoslijed članova i po volji ih grupirati. Stoga imamo

$$[f(A)g(A)](e)_{ij}=\sum_{\ell=1}^{n}f(A)(e)_{i\ell}g(A)(e)_{\ell j}=\sum_{\ell=1}^{n}\Big[\sum_{k=0}^{\infty}\alpha_k\alpha_{i\ell}^{(k)}\Big]\cdot\Big[\sum_{s=0}^{\infty}\beta_s\alpha_{\ell j}^{(s)}\Big]=$$

$$=\sum_{k=0}^{\infty}\sum_{s=0}^{\infty}\alpha_k\beta_s\sum_{ell=1}^{n}\alpha_{i\ell}^{(k)}\alpha_{\ell j}^{(s)}=\sum_{k=0}^{\infty}\sum_{s=0}^{\infty}\alpha_{ij}^{(k+s)}=\sum_{m=0}^{\infty}\Big(\sum_{r=0}^{m}\alpha_r\beta_{m-r}\Big)\alpha_{ij}^{(m)}.$$

S druge strane imamo

$$(f\cdot g)(\lambda)=\sum_{m=0}^{\infty}\Big(\sum_{r=0}^{m}\alpha_r\beta_{m-r}\Big)A^m,$$

pa slijedi

$$[(f\cdot g)(A)](e)_{ij}=\sum_{m=0}^{\infty}\Big(\sum_{r=0}^{m}\alpha_r\beta_{m-r}\Big)\alpha_{ij}^{(m)}.$$

Dakle, vrijedi $[f(A)g(A)](e)_{ij}=[(f\cdot g)(A)](e)_{ij}\;\;\forall i,j\in\{1,\ldots,n\}$, a to znači da je $(f\cdot g)(A)=$ $=f(A)g(A)$. Time je propozicija u potpunosti dokazana.

Primjeri operatorskih jednakosti vezanih uz identitete koje zadovoljavaju neke poznate cijele funkcije:

$$\sin A+i\cos A=e^{iA},\quad (\cos A)^2+(\sin A)^2=I,\quad \sin 2A=2\sin A\cos A,\quad \cos 2A=(\cos A)^2-(\sin A)^2.$$

Prema teoremu 6.3 za operator $A\in L(V)$ postoji baza e prostora V u kojoj je

$$A(e)=\begin{bmatrix}\lambda_1 I_1+J_1 & 0 & \cdots & 0\\ 0 & \lambda_2 I_2+J_2 & \cdots & 0\\ \vdots & \vdots & \ddots & \vdots\\ 0 & 0 & \cdots & \lambda_s I_s+J_s\end{bmatrix},$$

gdje je I_j jedinična matrica formata $n_j\times n_j$, J_j je elementarna Jordanova klijetka formata $n_j\times n_j$ i $\sigma(A)=\{\lambda_1,\lambda_2,\ldots,\lambda_s\}$ (pri tome svojstvene vrijednosti $\lambda_1,\lambda_2,\ldots,\lambda_s$ ne moraju biti međusobno različite). Primijetimo sada da je $k-$ta potencija blok$-$dijagonalne matrice ponovo blok$-$dijagonalna matrica čiji su blokovi $k-$te potencije odgovarajućih blokova matrice koju potenciramo:

$$A^k(e) = \begin{bmatrix} (\lambda_1 I_1 + J_1)^k & 0 & \cdots & 0 \\ 0 & (\lambda_2 I_2 + J_2)^k & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & (\lambda_s I_s + J_s)^k \end{bmatrix}.$$

Odatle slijedi da za cijelu funkciju

$$f(\lambda) = \sum_{k=0}^{\infty} \alpha_k \lambda^k$$

vrijedi

$$[f(A)](e) = \begin{bmatrix} f(\lambda_1 I_1 + J_1) & 0 & \cdots & 0 \\ 0 & f(\lambda_2 I_2 + J_2) & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & f(\lambda_s I_s + J_s) \end{bmatrix}.$$

Ovo nam je polazište za definiciju funkcije $f(A)$ operatora A za općenitije funkcije f. Stoga ćemo u daljnjem promatrati problem definicije $f(\lambda_0 I + J)$, gdje je I jedinična matrica formata $n \times n$, a J je elementarna Jordanova klijetka istog formata.

Lema 8.1 *Neka je $f : K(\lambda_1, r) \to \mathbb{C}$ funkcija koja je definirana i analitička na krugu*

$$K(\lambda_1, r) = \{\lambda \in \mathbb{C};\ |\lambda - \lambda_1| < r\}$$

i neka je

$$f(\lambda) = \sum_{k=0}^{\infty} \alpha_k (\lambda - \lambda_1)^k$$

njen Taylorov red oko točke λ_1 (koji konvergira apsolutno za svaki $\lambda \in K(\lambda_1, r)$). Za svaku točku $\lambda_0 \in K(\lambda_1, r)$ red matrica

$$\sum_{k=0}^{\infty} \alpha_k ((\lambda_0 - \lambda_1) I + J)^k$$

konvergira i suma mu je

$$f(\lambda_0) I + \frac{f'(\lambda_0}{1!} J + \frac{f''(\lambda_0}{2!} J^2 + \cdots + \frac{f^{(n-1)}(\lambda_0}{(n-1)!} J^{n-1}.$$

Dokaz: Stavimo za bilo koji $p \in \mathbb{N}$:

$$S_p = \sum_{k=0}^{p} \alpha_k ((\lambda_0 - \lambda_1) I + J)^k \qquad \text{i} \qquad f_p(\lambda) = \sum_{k=0}^{p} \alpha_k (\lambda - \lambda_1)^k.$$

Primjenom binomnog poučka nalazimo za svaki k :

$$((\lambda_0 - \lambda_1) I + J)^k = (\lambda_0 - \lambda_1)^k I + \binom{k}{1} (\lambda_0 - \lambda_1)^{k-1} J + \binom{k}{2} (\lambda_0 - \lambda_1)^{k-2} J^2 + \cdots + \binom{k}{k-1} (\lambda_0 - \lambda_1) J^{k-1} + J^k.$$

S druge strane, imamo

$$\binom{k}{j} (\lambda_0 - \lambda_1)^{k-j} = \frac{k!}{j!(k-j)!} (\lambda_0 - \lambda_1)^{k-j} = \frac{1}{j!} \frac{\mathrm{d}^j}{\mathrm{d}\lambda^j} (\lambda - \lambda_1)^k \Big|_{\lambda = \lambda_0},$$

pa nalazimo:

$$((\lambda_0-\lambda_1)I+J)^k = \Big[(\lambda-\lambda_1)^k I+\frac{1}{1!}\frac{\mathrm{d}}{\mathrm{d}\lambda}(\lambda-\lambda_1)^k J+\frac{1}{2!}\frac{\mathrm{d}^2}{\mathrm{d}\lambda^2}(\lambda-\lambda_0)^k J^2+\cdots+\frac{1}{k!}\frac{\mathrm{d}^k}{\mathrm{d}\lambda^k}(\lambda-\lambda_1)^k J^k\Big]\Big|_{\lambda=\lambda_0}. \qquad (*)$$

Za $k \geq n$ imamo $J^n = J^{n+1} = \cdots = J^k = 0$, pa u izrazu $(*)$ ne treba pisati sve članove, nego samo do člana

$$\frac{1}{(n-1)!}\frac{\mathrm{d}^{n-1}}{\mathrm{d}\lambda^{n-1}}(\lambda-\lambda_1)^k\Big|_{\lambda=\lambda_0} J^{n-1}.$$

S druge strane, za $k < n-1$ imamo

$$\frac{1}{j!}\frac{\mathrm{d}^j}{\mathrm{d}\lambda^j}(\lambda-\lambda_1)^k = 0 \qquad \text{za} \qquad j = k+1,\ldots,n-1,$$

pa u izrazu $(*)$ s desne strane možemo dopisati sumande

$$\frac{1}{(k+1)!}\frac{\mathrm{d}^{k+1}}{\mathrm{d}\lambda^{k+1}}(\lambda-\lambda_1)^k\Big|_{\lambda=\lambda_0} J^k + \cdots + \frac{1}{(n-1)!}\frac{\mathrm{d}^{n-1}}{\mathrm{d}\lambda^{n-1}}(\lambda-\lambda_1)^k\Big|_{\lambda=\lambda_0} J^{n-1}.$$

Dakle, za svaki $k \geq 0$ je

$$((\lambda_0-\lambda_1)I+J)^k =$$

$$= \Big[(\lambda-\lambda_1)^k I + \frac{1}{1!}\frac{\mathrm{d}}{\mathrm{d}\lambda}(\lambda-\lambda_1)^k J + \frac{1}{2!}\frac{\mathrm{d}^2}{\mathrm{d}\lambda^2}(\lambda-\lambda_1)^k J^2 + \cdots + \frac{1}{(n-1)!}\frac{\mathrm{d}^{n-1}}{\mathrm{d}\lambda^{n-1}}(\lambda-\lambda_1)^k J^{n-1}\Big]\Big|_{\lambda=\lambda_0}.$$

Pomnožimo li gornju jednakost sa α_k i zbrojimo po k od 0 do p, s lijeve strane jednakosti dobivamo upravo prije definiranu matricu S_p. Dakle,

$$S_p = \sum_{k=0}^{p}\alpha_k\Big[(\lambda-\lambda_1)^k I+\frac{1}{1!}\frac{\mathrm{d}}{\mathrm{d}\lambda}(\lambda-\lambda_1)^k J+\frac{1}{2!}\frac{\mathrm{d}^2}{\mathrm{d}\lambda^2}(\lambda-\lambda_1)^k J^2+\cdots+\frac{1}{(n-1)!}\frac{\mathrm{d}^{n-1}}{\mathrm{d}\lambda^{n-1}}(\lambda-\lambda_1)^k J^{n-1}\Big]\Big|_{\lambda=\lambda_0} =$$

$$= f_p(\lambda_0)I + \frac{1}{1!}f_p'(\lambda_0)J + \frac{1}{2!}f_p''(\lambda_0)J^2 + \cdots + \frac{1}{(n-1)!}f_p^{(n-1)}(\lambda_0)J^{n-1}.$$

Odatle slijedi tvrdnja leme, jer je

$$\lim_{p\to\infty} f_p(\lambda_0) = f(\lambda_0) \qquad \text{i} \qquad \lim_{p\to\infty} f_p^{(j)}(\lambda_0) = f^{(j)}(\lambda_0) \ \text{ za } \ j = 1,\ldots,n-1.$$

Iz leme 8.1 i iz razmatranja prije te leme nameće nam se kako da općenitije definiramo funkciju $f(A)$ operatora A i za koje sve funkcije f je takva definicija moguća.

Definicija 8.1 *Neka je* $A \in L(V)$ *i* $\mu_A(\lambda) = (\lambda-\lambda_1)^{p_1}(\lambda-\lambda_2)^{p_2}\cdots(\lambda-\lambda_t)^{p_t}$ *pri čemu su* $\lambda_1,\lambda_2,\ldots,\lambda_t \in \mathbb{C}$ *međusobno različiti. Sa* $\mathcal{F}(A)$ *označimo skup svih funkcija* f *iz* $\mathbb{C}$ *u* $\mathbb{C}$ *sa sljedećim svojstvima:*

(1) *Domena* $D(f)$ *funkcije* f *sadrži* $\sigma(A)$.

(2) *Ako je* $p_j > 0$, $D(f)$ *sadrži neki krug* $K(\lambda_j, r_r)$ *oko točke* λ_j *i na tom krugu je funkcija* f *analitička.*

Neka je sada e baza prostora V u kojoj matrica operatora A ima Jordanovu formu kao u teoremu 6.3. Pri tome, ako je $s > t$ onda se podrazumijeva da su $\lambda_{t+1}, \ldots, \lambda_s \in \sigma(A) = \{\lambda_1, \ldots, \lambda_t\}$. Za $f \in \mathcal{F}(A)$ za svaki $j \in \{1, 2, \ldots, s\}$ stavljamo

$$f(\lambda_j I_j + J_j) = \sum_{k=0}^{p_j-1} \frac{1}{k!} f^{(k)}(\lambda_j) J_j^k = \begin{bmatrix} f(\lambda_j) & \frac{f'(\lambda_j)}{1!} & \frac{[''(\lambda_j)}{2!} & \cdots & \frac{f^{(p_j-2)}(\lambda_j)}{(p_j-2)!} & \frac{f^{(p_j-1)}(\lambda_j)}{(p_j-1)!} \\ 0 & f(\lambda_j) & \frac{f'(\lambda_j)}{1!} & \cdots & \frac{f^{(p_j-3)}(\lambda_j)}{(p_j-3)!} & \frac{f^{(p_j-2)}(\lambda_j)}{(p_j-2)!} \\ 0 & 0 & f(\lambda_j) & \cdots & \frac{f^{(p_j-4)}(\lambda_j)}{(p_j-4)!} & \frac{f^{(p_j-3)}(\lambda_j)}{(p_j-3)!} \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & f(\lambda_j) & \frac{f'(\lambda_j)}{1!} \\ 0 & 0 & 0 & \cdots & 0 & f(\lambda_j) \end{bmatrix}.$$

Tada funkciju $f(A)$ operatora A definiramo pomoću matrice operatora $f(A)$ u bazi e :

$$[f(A)](e) = \begin{bmatrix} f(\lambda_1 I_1 + J_1) & 0 & \cdots & 0 \\ 0 & f(\lambda_2 I_2 + J_2) & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & f(\lambda_s I_s + J_s) \end{bmatrix}.$$

Teorem 8.1 *Neka je V konačnodimenzionalan vektorski prostor nad $\mathbb{C}$, $A \in L(V)$, $\sigma(A) = \{\lambda_1, \lambda_2, \ldots, \lambda_t\}$, pri čemu su $\lambda_1, \lambda_2, \ldots, \lambda_t$ međusobno različiti, i neka je*

$$\mu_A(\lambda) = (\lambda - \lambda_1)^{p_1}(\lambda - \lambda_2)^{p_2} \cdots (\lambda - \lambda_t)^{p_t}.$$

(a) *Ako je $f(\lambda) = 1 \;\; \forall \lambda \in \mathbb{C}$ onda je $f \in \mathcal{F}(A)$ i $f(A) = I$.*

(b) *Ako je $f(\lambda) = \lambda \;\; \forall \lambda \in \mathbb{C}$ onda je $f \in \mathcal{F}(A)$ i $f(A) = A$.*

(c) *Neka su $f, g \in \mathcal{F}(A)$ i $\alpha, \beta \in \mathbb{C}$. Definiramo funkciju h tako da je $D(h) = D(f) \cap D(g)$ i $h(\lambda) = \alpha f(\lambda) + \beta f(\lambda)$. Tada je $h \in \mathcal{F}(A)$ i $h(A) = \alpha f(A) + \beta g(A)$.*

(d) *Neka su $f, g \in \mathcal{F}(A)$. Definiramo funkciju $h = g$ tako da je $D(h) = D(f) \cap D(g)$ i $h(\lambda) = f(\lambda)g(\lambda)$. Tada je $h \in \mathcal{F}(A)$ i $h(A) = f(A)g(A)$.*

(e) *Pretpostavimo da su $f, g \in \mathcal{F}(A)$ takve da je $f^{(k)}(\lambda_j) = g^{(k)}(\lambda_j)$ za $0 \le k \le p_j - 1$ i za $1 \le j \le t$. Tada je $f(A) = g(A)$.*

(f) *Neka je $f \in \mathcal{F}(A)$ i neka je (f_k) niz u $\mathcal{F}(A)$. Pretpostavimo da vrijedi*

$$f^{(i)}(\lambda_j) = \lim_{k \to \infty} f_k^{(i)}(\lambda_j) \;\; za \;\; k = 0, 1, \ldots, p_j - 1 \;\; i \; za \;\; j = 1, 2, \ldots, t.$$

Tada je

$$f(A) = \lim_{k \to \infty} f_k(A).$$

(g) *Za $f \in \mathcal{F}(A)$ vrijedi $\sigma(f(A)) = f(\sigma(A)) = \{f(\lambda_1), f(\lambda_2), \ldots, f(\lambda_t)\}$.*

Dokaz: Tvrdnje (a), (b), (c), (e) i (f) su očigledne.

(d) Stavimo $V_j = N((A - \lambda_j I)^{p_j})$, $1 \le j \le t$. Tada znamo da su svi potprostori V_j $A-$invarijantni i da je $V = V_1 \dotplus V_2 \dotplus V_t$. Imamo redom

$$f(A)g(A)|V_j = (f(A)|V_j) \cdot (g(A)|V_j) = f(A|V_j)g(A|V_j) = \Big(\sum_{i=0}^{p_j-1} \frac{f^{(i)}(\lambda_j}{i!} J^i \Big) \cdot \Big(\sum_{k=0}^{p_j-1} \frac{g^{(k)}(\lambda_j)}{k!} J^k \Big) =$$

$$= \sum_{\ell=0}^{p_j-1}\Big(\sum_{k=0}^{\ell}\frac{f^{\ell-k}(\lambda_j)}{(\ell-k)!}\cdot\frac{g^{(k)}(\lambda_j)}{k!}\Big)J^\ell = \sum_{\ell=0}^{p_j-1}\Big(\frac{1}{\ell!}\sum_{k=0}^{\ell}\binom{\ell}{k}f^{(\ell-k)}(\lambda_j)g^{(k)}(\lambda_j)\Big)^\ell =$$

$$= \sum_{\ell=0}^{p_j-1}\frac{h^{(\ell)}(\lambda_j)}{\ell!}J^\ell = h(A\,|\,V_j) = h(A)\,|\,V_j.$$

Kako to vrijedi za sve $j = 1, 2, \ldots, t$ i kako je $V = V_1 \dotplus V_2 \dotplus \cdots \dotplus V_t$, slijedi $f(A)g(A) = h(A)$.

(g) Imamo redom ekvivalencije:

$$\lambda_0 \in \sigma(f(A)) \quad \Longleftrightarrow \quad \det(\lambda_0 I(e) - [f(A)](e)) = 0 \quad \Longleftrightarrow$$

$$\Longleftrightarrow \quad (\lambda_0 - f(\lambda_1))^{n_1})\lambda_0 - f(\lambda_2))^{n_2}\cdots(\lambda_0 - f(\lambda_t))^{n_t} = 0 \;\; (n_j = \dim V_j) \quad \Longleftrightarrow$$

$$\Longleftrightarrow \lambda_0 \in \{f(\lambda_1), f(\lambda_2), \ldots, f(\lambda_t)\}.$$

Na koncu ćemo dokazati još jednu važnu činjenicu, a to je da je $f(A) \in \mathcal{L}(A)$ za svaku funkciju $f \in \mathcal{F}(A)$. U tu svrhu treba nam jedan važan interpolacioni teorem o polinomima, kojeg navodimo bez dokaza:

Teorem 8.2 (**Lagrange−Sylvester**) *Neka su $\lambda_1, \lambda_2, \ldots, \lambda_t \in \mathbb{C}$ međusobno različiti i neka su $p_1, p_2, \ldots, p_t \in \mathbb{N}$. Nadalje, neka su zadani $\beta_{ij} \in \mathbb{C}$ za $i = 0, 1, \ldots, p_j - 1$ i za $j = 1, 2, \ldots, t$. Postoji jedinstven polinom $P(\lambda)$ stupnja manjeg od $p_1 + p_2 + \cdots + p_t$ takav da vrijedi*

$$P^{(i)}(\lambda_j) = \beta_{ij}, \qquad 0 \le i \le p_j - 1, \qquad 1 \le j \le t.$$

Polinom $P(\lambda)$ iz teorema 8.2 zove se **Lagrange−Sylvesterov interpolacioni polinom**, a ako je $p_1 = p_2 = \cdots = p_t = 1$ naziv je **Lagrangeov interpolacioni polinom**.

Teorem 8.3 *Neka je $A \in L(V)$, $\deg \mu_A(\lambda) = m$ i $f \in \mathcal{F}(A)$. Postoji jedinstven polinom $P(\lambda)$ stupnja $< m$ takav da je $P(A) = f(A)$.*

Dokaz: Prema Lagrange−Sylvesterovom teoremu 8.2 postoji polinom $P(\lambda)$ stupnja $< m$ takav da je

$$P^{(i)}(\lambda_j) = f^{(i)}(\lambda_j), \qquad 0 \le i \le p_j - 1, \qquad 1 \le j \le t.$$

Prema tvrdnji (e) teorema 8.1 tada je $f(A) = P(A)$. Time je dokazana egzistencija.

Dokažimo još jedinstvenost. Neka su $P(\lambda)$ i $Q(\lambda)$ polinomi stupnja $< m$ takvi da je $f(A) = P(A)$ i $f(A) = Q(A)$. Tada za polinom $S(\lambda) = P(\lambda) - Q(\lambda)$ vrijedi $\deg S(\lambda) < m$ i $S(A) = 0$. Prema tvrdnji (a) teorema 3.1 slijedi $S(\lambda) = 0$, dakle $P(\lambda) = Q(\lambda)$.

Lagrange−Sylvesterov teorem 8.2 omogućuje efikasno izračunavanje funkcija operatora. Naime, za svaki par indeksa $k \in \{0, 1, \ldots, p_\ell - 1\}$ i $\ell \in \{1, 2, \ldots, t\}$ prema tom teoremu postoji jedinstven polinom $G_{k\ell}(\lambda)$ stupnja $< m$ takav da vrijedi

$$G^i_{k\ell}(\lambda_j) = \delta_{ik}\delta_{j\ell}.$$

Stavimo tada $P_{k\ell} = G_{k\ell}(A)$. Tada se iz formule za funkciju operatora lako vidi da je za svaku funkciju $f \in \mathcal{F}(A)$

$$f(A) = \sum_{k=1}^{t}\Big(\sum_{\ell=0}^{p_k-1} f^{(\ell)}(\lambda_k)P_{k\ell}\Big).$$

Da bismo odredili operatore $P_{k\ell}$, čije poznavanje znači vrlo lako izračunavanje operatora $f(A)$ za svaku funkciju $f \in \mathcal{F}(A)$, nije nam nužno pronalaziti polinome $G_{k\ell}(\lambda)$. Dovoljno je gornju jednakost napisati za funkcije $f_s(\lambda) = \lambda^s$ za $s = 0, 1, \ldots, m$. Tada dobivamo sustav od m jednadžbi s $p_1 + p_2 + \cdots + p_t = m$ nepoznanica $P_{k\ell}$:

$$A^s = \sum_{k=1}^{t} \Big(\sum_{\ell=0}^{p_k-1} \frac{s!}{(s-\ell)!} \lambda_k^{s-\ell} P_{k\ell} \Big) \qquad 0 \le s \le m-1.$$

Eksplicitnim rješavanjem tih jednadžbi dolazimo do operatora $P_{k\ell}$.

Primijetimo još da nije teško dokazati da je

$$\{P_{k\ell};\ 0 \le \ell \le p_k - 1,\ 1 \le k \le t\}$$

baza vektorskog prostora $\mathcal{L}(A)$.