Algebra 1

Luka Horjak (luka.horjak@student.fmf.uni-lj.si)

5. junij 2021

Kazalo

Uvod

V tem dokumentu so zbrani moji zapiski s predavanj predmeta Algebra 1 v letu 2020/21. Predavatelj v tem letu je bil prof. dr. Primož Moravec.

Zapiski niso popolni. Manjka večina zgledov, ki pomagajo pri razumevanju definicij in izrekov. Poleg tega nisem dokazoval čisto vsakega izreka, pogosto sem ga označil kot očitnega ali pa le nakazal pomembnejše korake v dokazu.

Zelo verjetno se mi je pri pregledu zapiskov izmuznila kakšna napaka – popravki so vselej dobrodošli.

1 Vektorji v prostoru

»Pravila so mislim da taka da če padete ustni izpit potem morate še enkrat na pisnega, neko grozno pravilo je pa mogoče se bomo tega celo držali.«

—prof. dr. Primož Moravec

1.1 Krajevni vektorji

Definicija 1.1.1. *Prostor* je kartezični produkt

$$\mathbb{R}^3 = \mathbb{R} \times \mathbb{R} \times \mathbb{R} = \{(x, y, z) \mid x, y, z \in \mathbb{R}\} = \left\{ \begin{bmatrix} x \\ y \\ z \end{bmatrix} : x, y, z \in \mathbb{R} \right\}.$$

Vsaki točki $T(x, y, z)$ lahko priredimo usmerjeno daljico, ki se začne v O in konča v tej točki. Tej daljici pravimo *krajevni vektor* točke T.

Krajevni vektor zapisujemo s komponentami v obliki

$$\vec{r} = \begin{bmatrix} x \\ y \\ z \end{bmatrix} \quad \text{ali} \quad \vec{r} = (x, y, z).$$

Tako lahko opišemo poljuben vektor $\overrightarrow{AB}$, kjer sta $A(x_1, y_1, z_1)$ in $B(x_2, y_2, z_2)$ točki v prostoru, na naslednji način:

$$\overrightarrow{AB} = \begin{bmatrix} x_2 - x_1 \\ y_2 - y_1 \\ z_2 - z_1 \end{bmatrix}$$

1.2 Računanje z vektorji

Definicija 1.2.1. Za vektorja $\vec{a} = (x_1, y_1, z_1)$ in $\vec{b} = (x_2, y_2, z_2)$ je njuna vsota vektor, pri čemer je

$$\vec{a} + \vec{b} = \begin{bmatrix} x_1 + x_2 \\ y_1 + y_2 \\ z_1 + z_2 \end{bmatrix}.$$

Definicija 1.2.2. Za vektor $\vec{a} = (x_1, y_1, z_1)$ in $\lambda \in \mathbb{R}$ je njun produkt vektor, pri čemer je

$$\lambda \vec{a} = \begin{bmatrix} \lambda x \\ \lambda y \\ \lambda z \end{bmatrix}.$$

Definicija 1.2.3. *Ničelni vektor* je vektor, ki ga označujemo z $\vec{0} = (0, 0, 0)$.

Definicija 1.2.4. *Nasprotni vektor* vektorja $\vec{a}$ je vektor $-\vec{a} = -1 \cdot \vec{a}$.

Opomba 1.2.4.1. Naj bodo $\vec{a}, \vec{b}, \vec{c} \in \mathbb{R}^3$ in $\alpha, \beta \in \mathbb{R}$. Potem veljajo:

i) Komutativnost: $\vec{a} + \vec{b} = \vec{b} + \vec{a}$

ii) Asociativnost seštevanja: $(\vec{a} + \vec{b}) + \vec{c} = \vec{a} + (\vec{b} + \vec{c})$

iii) Nevtralni element za seštevanje: $\vec{a} + \vec{0} = \vec{0} + \vec{a} = \vec{a}$

iv) Nasprotni element: $\vec{a} + (\overrightarrow{-a}) = -\vec{a} + \vec{a} = \vec{0}$

v) »Distributivnost vektorjev«: $\alpha(\vec{a} + \vec{b}) = \alpha\vec{a} + \alpha\vec{b}$

vi) »Distributivnost skalarjev«: $(\alpha + \beta)\vec{a} = \alpha\vec{a} + \beta\vec{a}$

vii) Homogenost: $\alpha(\beta\vec{a}) = (\alpha\beta)\vec{a}$

viii) Nevtralni element za množenje: $1 \cdot \vec{a} = \vec{a}$

1.3 Linearna kombinacija

Definicija 1.3.1. Naj bodo $\vec{a}_1, \vec{a}_2, \ldots, \vec{a}_n \in \mathbb{R}^3$ in $\alpha_1, \alpha_2, \ldots, \alpha_n \in \mathbb{R}$. *Linearna kombinacija* vektorjev $\vec{a}_1, \vec{a}_2, \ldots, \vec{a}_n$ je vektor oblike

$$\alpha_1 \vec{a}_1 + \alpha_2 \vec{a}_2 + \cdots + \alpha_n \vec{a}_n.$$

Definicija 1.3.2. Vektorji $\vec{a}_1, \vec{a}_2, \ldots, \vec{a}_n \in \mathbb{R}^3$ so *linearno neodvisni*, če iz

$$\alpha_1 \vec{a}_1 + \alpha_2 \vec{a}_2 + \cdots + \alpha_n \vec{a}_n = \vec{0}$$

sledi $\alpha_1 = \alpha_2 = \cdots = \alpha_n = 0$.

Posledica 1.3.2.1. Vektorji so linearno odvisni, če lahko enega izmed njih izrazimo kot linearno kombinacijo ostalih. Največje število neodvisnih vektorjev v prostoru $\mathbb{R}^n$ je n, teh n vektorjev pa tvori bazo.

1.4 Skalarni produkt vektorjev

Definicija 1.4.1. *Skalarni produkt* vektorjev $\vec{a} = (x_1, y_1, z_1)$ in $\vec{b} = (x_2, y_2, z_2)$ je skalar

$$\vec{a} \cdot \vec{b} = x_1x_2 + y_1y_2 + z_1z_2.$$

Opomba 1.4.1.1. V posebnem primeru je

$$\vec{a} \cdot \vec{a} = x_1^2 + y_1^2 + z_1^2 = |\vec{a}|^2,$$

kjer je $|\vec{a}|$ dolžina vektorja.

Posledica 1.4.1.2. Naj bodo $\vec{a}, \vec{b}, \vec{c} \in \mathbb{R}^3$ in $\alpha \in \mathbb{R}$. Potem velja

i) $\vec{a} \cdot \vec{a} \geq 0$

ii) $\vec{a} \cdot \vec{a} = 0 \iff \vec{a} = \vec{0}$

iii) $\vec{a} \cdot \vec{b} = \vec{b} \cdot \vec{a}$

iv) $(\vec{a} + \vec{b}) \cdot \vec{c} = \vec{a} \cdot \vec{c} + \vec{b} \cdot \vec{c}$

v) $(\alpha\vec{a}) \cdot \vec{b} = \alpha(\vec{a} \cdot \vec{b})$

Geometrijsko lahko skalarni produkt interpretiramo kot produkt dolžine $\vec{a}$ in dolžine vektorja, ki ga dobimo, če $\vec{b}$ projeciramo na $\vec{a}$, saj velja

$$\vec{a} \cdot \vec{b} = |\vec{a}| \cdot \left|\vec{b}\right| \cdot \cos\left(\sphericalangle\left(\vec{a}, \vec{b}\right)\right).$$

Definicija 1.4.2. Vektorja $\vec{a}$ in $\vec{b}$ sta *pravokotna* natanko tedaj, ko je $\vec{a} \cdot \vec{b} = 0$.

1.5 Vektorski produkt vektorjev

Definicija 1.5.1. *Vektorski produkt* vektorjev $\vec{a} = (x_1, y_1, z_1)$ in $\vec{b} = (x_2, y_2, z_2)$ je vektor

$$\vec{a} \times \vec{b} = \begin{bmatrix} y_1 z_2 - z_1 y_2 \\ z_1 x_2 - x_1 z_2 \\ x_1 y_2 - y_1 x_2 \end{bmatrix}.$$

Posledica 1.5.1.1. Naj bodo $\vec{a}, \vec{b}, \vec{c} \in \mathbb{R}^3$ in $\alpha \in \mathbb{R}$. Potem velja

i) $\vec{a} \times \vec{a} = 0$

ii) $\vec{a} \times \vec{b} = -\vec{b} \times \vec{a}$

iii) $\vec{a} \times (\vec{b} + \vec{c}) = \vec{a} \times \vec{b} + \vec{a} \times \vec{c}$

iv) $(\alpha \vec{a}) \times \vec{b} = \alpha(\vec{a} \times \vec{b})$

v) $(\vec{a} \times \vec{b}) \times \vec{c} = (\vec{a} \cdot \vec{c}) \cdot \vec{b} - (\vec{b} \cdot \vec{c}) \cdot \vec{a}$

Definicija 1.5.2. Mešani produkt vektorjev $\vec{a}, \vec{b}, \vec{c} \in \mathbb{R}^3$ je skalar

$$\left[\vec{a}, \vec{b}, \vec{c}\right] = (\vec{a} \times \vec{b}) \cdot \vec{c}.$$

Trditev 1.5.3. Velja $\left[\vec{a}, \vec{b}, \vec{c}\right] = -\left[\vec{a}, \vec{c}, \vec{b}\right]$. Podobno velja, če zamenjamo poljubna dva vektorja.

Trditev 1.5.4. Naj bosta $\vec{a}, \vec{b} \in \mathbb{R}^3$. Potem velja

$$\left|\vec{a} \times \vec{b}\right|^2 + (\vec{a} \cdot \vec{b})^2 = |\vec{a}|^2 \cdot \left|\vec{b}\right|^2.$$

Dokaz. Velja

$$\begin{aligned} \left|\vec{a} \times \vec{b}\right|^2 &= (\vec{a} \times \vec{b}) \cdot (\vec{a} \times \vec{b}) \\ &= \left[\vec{a}, \vec{b}, \vec{a} \times \vec{b}\right] \\ &= \left[\vec{a} \times \vec{b}, \vec{a}, \vec{b}\right] \\ &= ((\vec{a} \times \vec{b}) \times \vec{a}) \cdot \vec{b} \\ &= ((\vec{a} \cdot \vec{a}) \cdot \vec{b} - (\vec{b} \cdot \vec{a}) \cdot \vec{a}) \cdot \vec{b} \\ &= (\vec{a} \cdot \vec{a}) \cdot (\vec{b} \cdot \vec{b}) - (\vec{a} \cdot \vec{b})^2. \end{aligned}$$

□

Trditev 1.5.5. Naj bosta $\vec{a}, \vec{b} \in \mathbb{R}^3$.

i) $\vec{a} \times \vec{b}$ je pravokoten na $\vec{a}$ in $\vec{b}$.

ii) $\left|\vec{a} \times \vec{b}\right|$ je ploščina paralelograma med $\vec{a}$ in $\vec{b}$.

Dokaz. Uporabimo prejšnje trditve:

i) $(\vec{a} \times \vec{b}) \cdot \vec{a} = \left[\vec{a}, \vec{b}, \vec{a}\right] = -\left[\vec{a}, \vec{a}, \vec{b}\right] = 0.$

ii) Velja

$$\left|\vec{a} \times \vec{b}\right|^2 = |\vec{a}|^2 \cdot \left|\vec{b}\right|^2 - (\vec{a} \cdot \vec{b})^2 = |\vec{a}|^2 \cdot \left|\vec{b}\right|^2 \cdot (1 - \cos^2 \varphi) = |\vec{a}|^2 \cdot \left|\vec{b}\right|^2 \cdot \sin^2 \varphi. \ \square$$

Trditev 1.5.6. Mešani produkt vektorjev $\vec{a}, \vec{b}, \vec{c} \in \mathbb{R}^3$ je enak volumnu *paralelepipeda*, ki ga tej vektorji omejujejo.

1.6 Objekti v prostoru

Dve točki v prostoru določata natanko eno premico. Premico lahko opišemo tudi z eno točko in neničelnim vektorjem, ki ležita na njej. Temu vektorju pravimo *smerni vektor*. *Parametrična enačba premice* je oblike

$$\vec{r} = \vec{r_1} + t \cdot \vec{s},$$

kjer t preteče vsa realna števila. Ekvivalentno je

$$\begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} x_0 \\ y_0 \\ z_0 \end{bmatrix} + t \begin{bmatrix} \alpha \\ \beta \\ \gamma \end{bmatrix}$$

in

$$T(\alpha \cdot t + x_0, \beta \cdot t + y_0, \gamma \cdot t + z_0).$$

Kanonična enačbe premice je oblike

$$\frac{x - x_0}{\alpha} = \frac{y - y_0}{\beta} = \frac{z - z_0}{\gamma}.$$

Trditev 1.6.1. Naj bo T točka v prostoru, točka T_1 in vektor $\vec{s}$ pa na premici p. Razdalja med točko T in premico p je enaka

$$d = \frac{\left|\overrightarrow{T_1T} \times \vec{s}\right|}{|\vec{s}|}.$$

Ravnina je natanko določena s tremi nekolinearnimi točkami. Lahko jo določimo tudi s točko na ravnini in vektorjem, pravokotnim na ravnino. Temu vektorju pravimo *normala*.

S pomočjo normale $\vec{n}$ izpeljemo *vektorsko enačbo ravnine*

$$(\vec{r} - \vec{r_1}) \cdot \vec{n} = 0.$$

Če ta vektor izrazimo v koordinatah, dobimo

$$(x - x_1)a + (y - y_1)b + (z - z_1)c = 0,$$

oziroma

$$ax + by + cz = d.$$

Enačbo ravnine, na kateri ležijo tri nekolinearne točke, lahko dobimo tako, da z vektorskim produktom poiščemo normalo.

Trditev 1.6.2. Razdalja točke T od ravnine, določene z normalo $\vec{n}$ in točko T_1, je enaka

$$d = \frac{\left|\vec{n} \cdot \overrightarrow{T_1T}\right|}{|\vec{n}|}.$$

Trditev 1.6.3. Razdaljo med premicama, določenima zaporedoma s paroma $(T_1, \vec{s_1})$ in $(T_2, \vec{s}_2)$, izračunamo po enačbi

$$d = \frac{\left|\overrightarrow{T_1T_2} \cdot (\vec{s_1} \times \vec{s}_2)\right|}{|\vec{s_1} \times \vec{s}_2|}.$$

2 Relacije, operacije in algebraične strukture

»Krompirji in kolerabe so nazaj.«
»A misliš da bomo pri Algebri 2
potem imeli pomaranče in mango?«
—Teja in Gabi

2.1 Relacije

Definicija 2.1.1. Naj bo X neprazna množica. *Relacija* na X je podmnožica v $X \times X$. »x je v relaciji R z y« označimo z $(x, y) \in R$ ali $x\ R\ y$.

Definicija 2.1.2. Relacija R na X je

i) *refleksivna*, če $x\ R\ x\ \forall x \in X$

ii) *simetrična*, če $x\ R\ y \iff y\ R\ x\ \forall x, y \in X$

iii) *antisimetrična*, če $x\ R\ y$ in $y\ R\ x \implies x = y\ \forall x, y \in X$

iv) *tranzitivna*, če $x\ R\ y$ in $y\ R\ z \implies x\ R\ z\ \forall x, y, z \in X$

Definicija 2.1.3. Relacija je

i) *ekvivalenčna*, če je refleksivna, simetrična in tranzitivna

ii) *delna urejenost*, če je refleksivna, antisimetrična in tranzitivna

Definicija 2.1.4. Naj bo $\sim$ ekvivalenčna relacija na X. *Ekvivalenčni razred* elementa $x \in X$ je množica

$$[x] = \{a \in X \mid x \sim a\}.$$

Definicija 2.1.5. Naj bo $\sim$ ekvivalenčna relacija na X. *Kvocientna množica* množice X glede na $\sim$ je

$$X/\sim = \{[x] \mid x \in X\}.$$

Trditev 2.1.6. Naj bo $\sim$ ekvivalenčna relacija na X in $a, b \in X$. Potem velja bodisi $[a] = [b]$ bodisi $[a] \cap [b] = \emptyset$. Ekvivalentno je X disjunktna unija ekvivalenčnih razredov.

Dokaz. Če je $c \in [a] \cap [b]$, je za vse $x \in [a]$

$$x \sim a \sim c \sim b,$$

oziroma $x \in [b]$. Simetrično velja, če je $x \in [b]$. □

2.2 Operacije

Definicija 2.2.1. Naj bo X neprazna množica. *Operacija* na X je vsaka preslikava $X \times X \to X$. Označimo $\circ\colon X \times X \to X$ in namesto $\circ(a, b)$ pišemo $a \circ b$.

Definicija 2.2.2. Naj bo $\circ$ operacija na X. Operacija je

i) *komutativna*, če $a \circ b = b \circ a \ \forall a, b \in X$

ii) *asociativna*, če $(a \circ b) \circ c = a \circ (b \circ c) \ \forall a, b, c \in X$

Definicija 2.2.3. Naj bo $\circ$ operacija na X. Za element $e \in X$ pravimo, da je *enota* ali *nevtralni element* za $\circ$, če velja

$$e \circ x = x \circ e = x \quad \forall x \in X.$$

Trditev 2.2.4. Naj bo X množica z operacijo $\circ$. Če obstaja enota za to operacijo, je enolično določena.

Dokaz. Za enoti e_1 in e_2 je po definiciji

$$e_1 = e_1 \circ e_2 = e_2.$$ □

Definicija 2.2.5. Naj bo X množica z operacijo $\circ$ in naj bo Y njena neprazna podmnožica. Pravimo, da je Y *zaprta za operacijo* $\circ$, če $\forall a, b \in Y$ velja $a \circ b \in Y$.

Opomba 2.2.5.1. Če je Y zaprta za $\circ$, je tudi Y opremljena s to operacijo.

2.3 Grupe

Definicija 2.3.1. Naj bo $(X, \circ)$ množica z operacijo $\circ$.

i) $(X, \circ)$ je *polgrupa*, če je $\circ$ asociativna

ii) $(X, \circ)$ je *monoid*, če je polgrupa in ima enoto za $\circ$

iii) $(X, \circ)$ je *grupa*, če je monoid in ima vsak element X *inverz* glede na $\circ$:

$$\forall a \in X\ \exists b \in X\colon \quad a \circ b = b \circ a = e.$$

Kadar je $\circ$ komutativna, govorimo o *komutativni polgrupi*, *komutativnem monoidu* in *abelovi grupi*.

Trditev 2.3.2. V grupi je inverz elementa enolično določen.

Dokaz. Naj bosta b in c inverza elementa a v grupi $(G, \circ)$. Potem je

$$b = b \circ (a \circ c) = (b \circ a) \circ c = c. \qquad \square$$

Za element $a \in G$ označimo njegov inverz z a^{-1}.

Definicija 2.3.3. Naj bo $(G, \circ)$ grupa in $H \subseteq G$ neprazna podmnožica. Pravimo, da je H *podgrupa* v grupi G, če je tudi $(H, \circ)$ grupa.

Definicija 2.3.4. Naj bosta $(G, \circ)$ in $(H, *)$ grupi. Funkcija $f\colon (G, \circ) \to (H, *)$ je *homomorfizem grup*, če velja

$$\forall a, b \in G\colon f(a \circ b) = f(a) * f(b).$$

Bijektivnim homomorfizmom pravimo *izomorfizmi*. Grupi sta *izomorfni*, če med njima obstaja izomorfizem.

Definicija 2.3.5. Naj bo X neprazna množica in

$$\operatorname{Sym} X = \{f\colon X \to X \mid f \text{ je bijektivna}\}.$$

Potem je $(\operatorname{Sym} X, \circ)$ grupa, kjer je $\circ$ operacija kompozitum. Njena enota je id. $\operatorname{Sym} X$ imenujemo *grupa simetrij* množice X.

Definicija 2.3.6. Če je X končna množica z n elementi, označimo $\operatorname{Sym} X = S_n$. S_n je *simetrična grupa* na n elementih. Elementom grupe S_n pravimo *permutacije*. Velja $|S_n| = n!$.

Permutacije označujemo z malimi grškimi črkami:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}, \quad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix}, \quad \sigma \circ \tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix}$$

Poseben primer permutacij so *cikli*. $\sigma = (j_1\ j_2\ \ldots\ j_k)$ je cikel dolžine k, kjer je $\sigma(j_i) = j_{i+1}$, kjer gledamo indekse po modulu k. Ciklom dolžine 2 pravimo *transpozicije*.

Vsako permutacijo lahko zapišemo kot kompozitum (produkt) disjunktnih ciklov ali produkt transpozicij:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 3 & 2 & 5 & 1 & 6 \end{pmatrix} = (1\ 4\ 5) \circ (2\ 3) = (2\ 3) \circ (1\ 4\ 5) = (4\ 5) \circ (2\ 3) \circ (1\ 5)$$

Definicija 2.3.7. Naj bo σ permutacija množice $\{1, \ldots, n\}$ in naj bosta $i < j$ elementa te množice. Pravimo, da je par (i, j) *inverzija* za σ, če velja $\sigma(i) > \sigma(j)$. Številu vseh inverzij pravimo *indeks* permutacije σ in ga označimo z $\operatorname{ind}\sigma$. Številu $\operatorname{sgn}\sigma = (-1)^{\operatorname{ind}\sigma}$ pravimo *signatura* ali *znak* permutacije σ.

Definicija 2.3.8. Permutacijam $\sigma \in S_n$, za katere je $\operatorname{sgn}\sigma = 1$, pravimo *sode* permutacije, ostalim pa *lihe*.

Trditev 2.3.9. Naj bosta σ in $\widetilde{\sigma}$ permutaciji, za kateri je $\sigma(i) = \widetilde{\sigma}(j)$, $\sigma(j) = \widetilde{\sigma}(i)$ in $\sigma(k) = \widetilde{\sigma}(k)$ za vse ostale k. Potem je $\operatorname{sgn}\widetilde{\sigma} = -\operatorname{sgn}\sigma$.

Dokaz. Preštejemo lahko, da se spremeni vrstni red lihega števila parov. Paru (i, k) se namreč spremeni natanko tedaj kot paru (j, k), spremeni pa se tudi vrstni red (i, j). □

Posledica 2.3.9.1. Permutacija je soda natanko tedaj, ko jo lahko zapišemo kot produkt sodega števila transpozicij.

Posledica 2.3.9.2. Za poljubni permutaciji $\sigma, \tau \in S_n$ je $\operatorname{sgn}\sigma^{-1} = \operatorname{sgn}\sigma$ in $\operatorname{sgn}(\sigma \circ \tau) = \operatorname{sgn}\sigma \cdot \operatorname{sgn}\tau$.

2.4 Kolobarji, obsegi in polja

Definicija 2.4.1. Naj bo K neprazna množica z operacijama $+\colon K \times K \to K$ in $\cdot\colon K \times K \to K$. Pravimo, da je $(K, +, \cdot)$ *kolobar*, če velja:

i) $(K, +)$ je abelova grupa
   - enoto označimo z 0
   - inverz a označimo z $-a$

ii) $(K, \cdot)$ je polgrupa

iii) leva in desna distributivnost

Definicija 2.4.2. Naj bo $(K, +, \cdot)$ kolobar.

i) Če ima K nevtralen element za množenje, pravimo, da je K *kolobar z enico*. Nevtralni element označimo z 1.

ii) Če je množenje v K komutativno, pravimo, da je K *komutativen kolobar*.

iii) Če je K kolobar z enico, za katerega velja, da je $K \setminus \{0\}$ za množenje grupa, pravimo, da je K *obseg*.

iv) Komutativnim obsegom pravimo *polja*.

Definicija 2.4.3. Naj bo $(K, +, \cdot)$ kolobar in $L \subseteq K$ neprazna podmnožica. Pravimo, da je L *podkolobar v* K, če je $(L, +, \cdot)$ tudi kolobar.

Definicija 2.4.4. Naj bosta $(K, +_1, \cdot_1)$ in $(L, +_2, \cdot_2)$ kolobarja. *Homomorfizem kolobarjev* je preslikava $f\colon (K, +_1, \cdot_1) \to (L, +_2, \cdot_2)$, za katero je

$$\forall a, b \in K\colon f(a +_1 b) = f(a) +_2 f(b) \quad \text{in} \quad (a \cdot_1 b) = f(a) \cdot_2 f(b).$$

Bijektivnim homomorfizmom pravimo *izomorfizmi*. Kolobarja sta *izomorfna*, če med njima obstaja izomorfizem.

3 Vektorski prostori

»A so zdaj vaje ali pouk?«

—Jan Kamnikar

3.1 Definicija

Definicija 3.1.1. Naj bo $V \neq \emptyset$ z operacijo

$$+ \colon V \times V \to V, \qquad (u, v) \mapsto u + v.$$

Naj bo $\mathbb{F}$ polje in recimo, da imamo preslikavo

$$\cdot \colon \mathbb{F} \times V \to V, \qquad (\alpha, v) \mapsto \alpha v.$$

Pravimo, da je V *vektorski prostor* nad poljem $\mathbb{F}$, če veljajo naslednji pogoji:

i) $(V, +)$ je abelova grupa. Enoto za $+$ označimo z 0, inverz v pa z $-v$

ii) $(\alpha + \beta)v = \alpha v + \beta v$ velja $\forall \alpha, \beta \in \mathbb{F}, \forall v \in V$

iii) $\alpha(u + v) = \alpha u + \alpha v$ velja $\forall \alpha \in \mathbb{F}, \forall u, v \in V$

iv) $\alpha(\beta v) = (\alpha\beta)v$ velja $\forall \alpha, \beta \in \mathbb{F}, \forall v \in V$

v) $1 \cdot v = v$ velja $\forall v \in V$

Elementom V pravimo *vektorji*, elementom $\mathbb{F}$ pa *skalarji*.

Primer vektorskega prostora je $V = \mathbb{F}^n$ nad $\mathbb{F}$ za neko polje $\mathbb{F}$. Vpeljemo lahko

$$\begin{bmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{bmatrix} + \begin{bmatrix} \beta_1 \\ \beta_2 \\ \vdots \\ \beta_n \end{bmatrix} = \begin{bmatrix} \alpha_1 + \beta_1 \\ \alpha_2 + \beta_2 \\ \vdots \\ \alpha_n + \beta_n \end{bmatrix} \qquad \text{in} \qquad \alpha \cdot \begin{bmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{bmatrix} = \begin{bmatrix} \alpha\alpha_1 \\ \alpha\alpha_2 \\ \vdots \\ \alpha\alpha_n \end{bmatrix}$$

Ti operaciji zadoščata zgornjim pogojem.

Ta primer lahko tudi posplošimo. Naj bo X neprazna množica, $\mathbb{F}$ polje in

$$\mathbb{F}^X = \{f \mid f \colon X \to \mathbb{F}\}.$$

Na tej množici vpeljemo seštevanje in množenje s skalarjem. Za $f, g \in \mathbb{F}^X$ definiramo

$$(f + g)(x) = f(x) + g(x) \qquad \text{in} \qquad (\lambda f)(x) = \lambda f(x).$$

Trditev 3.1.2. Naj bo V vektorski prostor nad $\mathbb{F}$.

i) $0 \cdot v = 0$ velja $\forall v \in V$

ii) $\alpha \cdot 0 = 0$ velja $\forall \alpha \in \mathbb{F}$

iii) $(-1) \cdot v = -v$

Dokaz. The proof is obvious and need not be mentioned. □

Definicija 3.1.3. Naj bo V vektorski prostor nad $\mathbb{F}$ in U neprazna podmnožica V. Pravimo, da je U *vektorski podprostor v* V, če je U za dano seštevanje in množenje s skalarjem tudi vektorski prostor nad $\mathbb{F}$. Označimo $U \leq V$.

Opomba 3.1.3.1. To pomeni naslednje:

- $(U, +)$ je podgrupa v $(V, +)$
- $\forall u \in U, \alpha \in \mathbb{F}$ je $\alpha u \in U$

Trditev 3.1.4. Naj bo V vektorski prostor nad $\mathbb{F}$ in $U \subseteq V$ neprazna podmnožica. Potem je U vektorski podprostor v V natanko tedaj, ko je za poljubna vektorja $u_1, u_2 \in U$ in skalarja $\alpha_1, \alpha_2 \in \mathbb{F}$

$$\alpha_1 u_1 + \alpha_2 u_2 \in U.$$

Dokaz. The proof is obvious and need not be mentioned. □

Opomba 3.1.4.1. Vsak podprostor U vektorskega prostora V vsebuje ničelni vektor.

Trditev 3.1.5. Naj bo $\mathbb{F}$ polje in $\mathbb{F}^{\mathbb{F}} = \{\text{vse funkcije } \mathbb{F} \to \mathbb{F}\}$. Potem je

$$\mathbb{F}[x] = \left\{ p \in \mathbb{F}^{\mathbb{F}} \;\middle|\; p(x) = \sum_{i=0}^{n} a_i x^i, n \geq 0, a_i \in \mathbb{F} \right\}$$

vektorski podprostor v $\mathbb{F}^{\mathbb{F}}$. Za poljuben n je

$$\mathbb{F}_n[x] = \left\{ p \in \mathbb{F}^{\mathbb{F}} \;\middle|\; p(x) = \sum_{i=0}^{n} a_i x^i, a_i \in \mathbb{F} \right\}$$

vektorski podprostor v $\mathbb{F}[x]$.

Dokaz. The proof is obvious and need not be mentioned. □

3.2 Kvocientni prostori

Definicija 3.2.1. Naj bo V vektorski prostor nad $\mathbb{F}$, U pa podprostor v V. Na množici V definiramo relacijo $\sim$:

$$\forall x, y \in V : x \sim y \iff x - y \in U$$

Trditev 3.2.2. $\sim$ je ekvivalenčna relacija na V.

Dokaz. The proof is obvious and need not be mentioned. □

Za tako definirano relacijo $\sim$ označimo $V/U = V/\sim$.

Elementi V/U so

$$v \in V : [v] = \{x \in V \mid x \sim v\} = \{x \in V \mid x = v + u, u \in U\} = v + U.$$

Izrek 3.2.3. Naj bo V vektorski prostor nad $\mathbb{F}$ in $U \leq V$. Potem V/U postane vektorski prostor nad $\mathbb{F}$ z naslednjim seštevanjem in množenje s skalarjem:

$$(v_1 + U) + (v_2 + U) = (v_1 + v_2) + U$$
$$\alpha \cdot (v + U) = \alpha v + U$$

V/U je *kvocientni prostor* prostora V glede na U.

Dokaz. The proof is obvious and need not be mentioned. □

Opomba 3.2.3.1. V V/U je U nevtralni element.

Definicija 3.2.4. Naj bo V vektorski prostor nad $\mathbb{F}$ in V_1, V_2 podprostora v V. Potem označimo

$$V_1 + V_2 = \{v_1 + v_2 \mid v_1 \in V_1, v_2 \in V_2\}.$$

Tej množici pravimo *vsota podprostorov* V_1 *in* V_2.

Trditev 3.2.5. Naj bo V vektorski prostor nad $\mathbb{F}$ in $V_1, V_2 \leq V$. Potem sta tudi $V_1 \cap V_2$ in $V_1 + V_2$ podprostora V.

Dokaz. The proof is obvious and need not be mentioned. □

Opomba 3.2.5.1. Unija je vektorski prostor le, če je $V_1 \subseteq V_2$ ali $V_2 \subseteq V_1$.

Definicija 3.2.6. Naj bo V vektorski prostor nad $\mathbb{F}$ in $V_1, V_2, \ldots, V_n \leq V$. Pravimo, da je V *direktna vsota* podprostorov $V_1, V_2, \ldots V_n$, če velja:

i) $V = V_1 + V_2 + \ldots V_n$

ii) $V_i \cap (V_1 + V_2 + \cdots + V_{i-1} + V_{i+1} + \cdots + V_n) = \{0\}$ za vse i.

Označimo $V = V_1 \oplus V_2 \oplus \cdots \oplus V_n$

Izrek 3.2.7. Naj bo V vektorski prostor in $V_1, V_2, \ldots, V_n \leq V$. Potem je

$$V = V_1 \oplus V_2 \oplus \cdots \oplus V_n$$

natanko tedaj, ko se da vsak $v \in V$ na enoličen način zapisati kot $v = v_1 + v_2 + \cdots + v_n$ za $v_i \in V_i$.

Dokaz. The proof is obvious and need not be mentioned. □

3.3 Homomorfizmi vektorskih prostorov

Definicija 3.3.1. Naj bosta U in V vektorska prostora nad $\mathbb{F}$. Za preslikavo $A\colon U \to V$ pravimo, da je *homomorfizem vektorskih prostorov* oziroma *linearna preslikava*, če velja:

i) Aditivnost: $\forall u_1, u_2 \in U\colon A(u_1 + u_2) = A(u_1) + A(u_2)$

ii) Homogenost: $\forall u \in U, \alpha \in \mathbb{F}\colon A(\alpha u) = \alpha A(u)$

Krajše pišemo $A(u) = Au$.

Definicija 3.3.2. Naj bosta U in V vektorska prostora nad $\mathbb{F}$. Množico vseh linearnih preslikav $U \to V$ označimo z $\mathrm{Hom}_{\mathbb{F}}(U, V)$.

Definicija 3.3.3. Naj bo $A \in \mathrm{Hom}_{\mathbb{F}}(U, V)$.

i) A je *monomorfizem*, če je injektivna.

ii) A je *epimorfizem*, če je surjektivna.

iii) A je *izomorfizem*, če je bijektivna.

Definicija 3.3.4. Linearnim preslikavam $A\colon U \to U$ pravimo *endomorfizmi* prostora U. Označimo $\mathrm{End}_{\mathbb{F}}(U) = \mathrm{Hom}_{\mathbb{F}}(U, U)$.

Definicija 3.3.5. Vektorska prostora U in V nad $\mathbb{F}$ sta *izomorfna*, če med njima obstaja izomorfizem. Označimo $U \cong V$.

Opomba 3.3.5.1. Če je A izomorfizem vektorskih prostorov, je tudi njegov inverz izomorfizem.

Trditev 3.3.6. Preslikava $A\colon U \to V$ je linearna natanko tedaj, ko je

$$A(\alpha u_1 + \beta u_2) = \alpha A u_1 + \beta A u_2$$

za vse $\alpha, \beta \in \mathbb{F}$ in $u_1, u_2 \in U$.

Dokaz. The proof is obvious and need not be mentioned. □

Trditev 3.3.7. Če je $A\colon U \to V$ bijektivna linearna preslikava, je tudi $A^{-1}\colon V \to U$ linearna.

Dokaz. Za $u_1 = A^{-1}v_1$ in $u_2 = A^{-1}v_2$ je

$$A^{-1}(\alpha v_1 + \beta v_2) = A^{-1}(A(\alpha u_1 + \beta u_2)) = \alpha A^{-1} v_1 + \beta A^{-1} v_2.$$ □

Definicija 3.3.8. Naj bosta U in V vektorska prostora nad $\mathbb{F}$. Na $\mathrm{Hom}_{\mathbb{F}}(U, V)$ definiramo seštevanje in množenje s skalarjem:

- $A, B \in \mathrm{Hom}_{\mathbb{F}}(U, V)\colon (A + B)u = Au + Bu$
- $\alpha \in \mathbb{F}$, $A \in \mathrm{Hom}_{\mathbb{F}}(U, V)\colon (\alpha A)u = \alpha A u$

Trditev 3.3.9. Ob zgornjih definicijah $\mathrm{Hom}_{\mathbb{F}}(U, V)$ postane vektorski prostor nad $\mathbb{F}$.

Dokaz. The proof is obvious and need not be mentioned. □

Trditev 3.3.10. Naj bo $A \in \mathrm{Hom}_{\mathbb{F}}(U, V)$ in $B \in \mathrm{Hom}_{\mathbb{F}}(V, W)$. Potem je kompozitum $B \circ A \in \mathrm{Hom}_{\mathbb{F}}(U, W)$.

Dokaz. Velja

$$B(A(\alpha u + \beta v)) = B(\alpha Au + \beta Av) = \alpha B(Au) + \beta B(Av).$$ □

Definicija 3.3.11. Naj bo A neprazna množica in $\mathbb{F}$ polje. Recimo, da imamo na A operaciji $+$ in $\cdot$ ter množenje s skalarjem. Pravimo, da je A *algebra* nad poljem $\mathbb{F}$, če velja:

i) A s seštevanjem in množenjem s skalarjem je vektorski prostor nad $\mathbb{F}$

ii) $(A, +, \cdot)$ je kolobar

iii) $\forall a, b \in A$, $\forall \alpha \in \mathbb{F}$: $\alpha(a \cdot b) = (\alpha a) \cdot b = a \cdot (\alpha b)$

Posledica 3.3.11.1. $\mathrm{End}_{\mathbb{F}}(U)$ je z zgornjim seštevanjem, kompozitumom in množenjem s skalarjem algebra nad $\mathbb{F}$.

Trditev 3.3.12. Naj bo $A \colon U \to V$ linearna preslikava. Potem je $A0 = 0$.

Dokaz. Po definiciji je

$$A0 = A(0 \cdot u) = 0 \cdot Au = 0.$$ □

3.4 Jedro in slika linearne preslikave

Definicija 3.4.1. Naj bo $A\colon U \to V$ linearna preslikava.

Jedro linearne preslikave A je množica

$$\ker A = \{u \in U \mid Au = 0\}.$$

Slika linearne preslikave A je množica

$$\operatorname{im} A = \{Au \mid u \in U\}.$$

Izrek 3.4.2. Naj bo $A\colon U \to V$ linearna. Potem je $\ker A$ podprostor v U in $\operatorname{im} A$ podprostor v V.

Dokaz. The proof is obvious and need not be mentioned. □

Trditev 3.4.3. Naj bo $A\colon U \to V$ linearna preslikava.

i) A je injektivna natanko tedaj, ko je $\ker A = \{0\}$.

ii) A je surjektivna natanko tedaj, ko je $\operatorname{im} A = V$.

Dokaz. The proof is obvious and need not be mentioned. □

Izrek 3.4.4 (1. izrek o izomorfizmu)**.** Naj bo $A\colon U \to V$ linearna preslikava. Potem je

$$U/\ker A \cong \operatorname{im} A.$$

Izrek 3.4.5 (2. izrek o izomorfizmu)**.** Naj bosta V_1 in V_2 podprostora vektorskega prostora V. Potem je

$$(V_1 + V_2)/V_1 \cong V_2/(V_1 \cap V_2).$$

Izrek 3.4.6 (3. izrek o izomorfizmu)**.** Naj bodo $U \leq V \leq W$ vektorski prostori. Potem je V/U podprostor v W/U in je

$$(W/U)/(V/U) \cong W/V.$$

Opomba 3.4.6.1. Kadar dokazujemo $U/U_1 \cong V$, lahko konstruiramo $A\colon U \to V$, da bo

- $\operatorname{im} A = V$
- $\ker A = U_1$

Po 1. izreku o izomorfizmu (3.4.4) sledi izomorfnost.

3.5 Končnorazsežni vektorski prostori

Definicija 3.5.1. Naj bo V vektorski prostor nad $\mathbb{F}$ in naj bo X neprazna podmnožica v V. Z $\operatorname{Lin} X$ označimo *linearno ogrinjačo* množice X, ki jo definiramo kot

$$\operatorname{Lin} X = \left\{ \sum_{i=1}^{k} \alpha_i x_i \;\middle|\; k \in \mathbb{N}, \alpha_i \in \mathbb{F}, x_i \in X \right\}.$$

Trditev 3.5.2. Naj bo X podmnožica vektorskega prostora V. Potem je $\operatorname{Lin} X$ najmanjši vektorski podprostor v V, ki vsebuje X.

Dokaz. Očitno je $\operatorname{Lin} X$ vektorski prostor. Naj bo $X \subseteq U$, kjer je $U \leq V$ vektorski podprostor. Potem je po definiciji tudi vsaka linearna kombinacija vektorjev iz X v U. □

Definicija 3.5.3. Naj bo V vektorski prostor in X neprazna podmnožica v V. Pravimo, da je X *ogrodje* za V, če je $\operatorname{Lin} X = V$.

Definicija 3.5.4. Vektorski prostor je *končnorazsežen*, če ima končno ogrodje.

Trditev 3.5.5. Če je X ogrodje prostora V in $X \subseteq Y \subseteq V$, je tudi Y ogrodje prostora V.

Dokaz. The proof is obvious and need not be mentioned. □

Trditev 3.5.6. Recimo, da je X ogrodje prostora V in recimo, da je $x \in X$ linearna kombinacija od x različnih vektorjev iz X. Potem je $X \setminus \{x\}$ tudi ogrodje prostora V.

Dokaz. V reprezentaciji poljubnega vektorja $v \in V$ z vektorji iz X preprosto x nadomestimo z linearno kombinacijo, s katero ga lahko izrazimo. □

Definicija 3.5.7. Naj bo V vektorski prostor nad $\mathbb{F}$ in $\{v_1, v_2, \ldots, v_n\}$ množica vektorjev iz V. Pravimo, da so $v_1, v_2, \ldots, v_n$ *linearno neodvisni*, če iz enakosti

$$\sum_{i=1}^{n} \alpha_i v_i = 0,$$

kjer so $\alpha_i \in \mathbb{F}$, sledi $\alpha_i = 0$ za vse i. V nasprotnem primeru pravimo, da so *linearno odvisni*.

Opomba 3.5.7.1. Če so vektorji linearno odvisni, lahko enega izmed njih izrazimo z linearno kombinacijo ostalih.

Definicija 3.5.8. Naj bo V vektorski prostor in naj bo $\mathcal{B} = \{v_1, v_2, \ldots, v_n\}$ množica vektorjev iz V. Pravimo, da je $\mathcal{B}$ *baza* prostora V, če

i) $\mathcal{B}$ je ogrodje V

ii) vektorji iz $\mathcal{B}$ so linearno neodvisni

Izrek 3.5.9. Netrivialen vektorski prostor je končnorazsežen natanko tedaj, ko ima bazo.

Dokaz. Vzemimo poljubno končno ogrodje prostora X, nato pa po trditvi 3.5.6 postopoma iz X odstranjujemo vektorje, dokler niso vsi linearno neodvisni. Ostane nam baza prostora. □

3.6 Lastnosti baz končnorazsežnih prostorov

Trditev 3.6.1. Naj bo $\mathcal{B} = \{v_1, v_2, \ldots, v_n\}$ baza vektorskega prostora V. Potem se da vsak vektor $v \in V$ na enoličen način zapisati kot linearno kombinacijo vektorjev iz $\mathcal{B}$.

Dokaz. $\mathcal{B}$ je ogrodje, zato lahko vsak v zapišemo kot linearno kombinacijo vektorjev iz $\mathcal{B}$. Če ga lahko kot linearno kombinacijo zapišemo na dva načina, ju preprosto odštejemo. Ostane nam vektor 0, izražen z vektorji iz $\mathcal{B}$. To je nemogoče pri različnih zapisih z bazo $\mathcal{B}$, saj so vektorji iz $\mathcal{B}$ linearno neodvisni. □

Lema 3.6.2. Naj bo V vektorski prostor in $X = \{u_1, u_2, \ldots, u_m\}$ ogrodje V. Naj bo $Y = \{v_1, v_2, \ldots, v_n\}$ množica linearno neodvisnih vektorjev iz V. Potem je $n \leq m$.

Dokaz. Vektorje v X lahko zaporedoma zamenjujemo z vektorji iz Y. Poljuben vektor iz Y lahko izrazimo kot linearno kombinacijo vektorjev iz X, nato pa enega izmed u_i v tem zapisu zamenjamo s tem vektorjem. Tak u_i bo vedno obstajal, saj so vektorji iz Y linearno neodvisni. Algoritem se konča, ko so vsi elementi Y v množici X, kar pomeni, da je $n \leq m$. □

Posledica 3.6.2.1. Vse baze končnorazsežnega prostora imajo isto moč.

Definicija 3.6.3. Naj bo V končnorazsežen vektorski prostor. *Dimenzija* prostora V je število vektorjev v bazi prostora V. Označimo jo z $\dim V$.

Trditev 3.6.4. Recimo, da je V končnorazsežen vektorski prostor in U podprostor v V. Recimo, da je $\mathcal{B}$ baza podprostora U. Potem lahko $\mathcal{B}$ dopolnimo do baze celega prostora.

Dokaz. V $\mathcal{B}$ postopoma dodajamo linearno neodvisne vektorje. Po lemi 3.6.2 lahko dodamo le končno mnogo vektorjev. Na tej točki je tako $\mathcal{B}$ ogrodje V, kar pomeni, da je baza prostora. □

Posledica 3.6.4.1. Naj bo V končnorazsežen prostor in $\dim V = n$. Če je X podmnožica v V, ki vsebuje natanko n linearno neodvisnih vektorjev, je X baza prostora V.

Posledica 3.6.4.2. Naj bo V končnorazsežen vektorski prostor in $U \leq V$. Potem je $\dim U \leq \dim V$ z enakostjo natanko tedaj, ko je $U = V$.

Izrek 3.6.5. Naj bo V vektorski prostor nad $\mathbb{F}$ in $\dim V = n$. Potem je $V \cong \mathbb{F}^n$.

Dokaz. Naj bo A linearna preslikava, ki vsakemu baznemu vektorju v_i priredi vektor $e_i = (0, \ldots, 0, 1, 0, \ldots, 0)$, kjer je 1 na i-tem mestu. Ni težko preveriti, da je A izomorfizem. □

Opomba 3.6.5.1. Množici $\{e_1, \ldots, e_n\}$ pravimo *standardna baza* prostora $\mathbb{F}^n$.

Izrek 3.6.6. Naj bosta U in V končnorazsežna vektorska prostora nad $\mathbb{F}$. Potem je $U \cong V$ natanko tedaj, ko je $\dim U = \dim V$.

Dokaz. Če je $\dim U = \dim V$, je po prejšnjem izreku

$$U \cong \mathbb{F}^{\dim U} \cong V,$$

$\cong$ pa je ekvivalenčna relacija (vzamemo kompozitum).

Če je $U \cong V$, potem ni težko preveriti, da izomorfizem med njima bazo U preslika v bazo V. To pomeni, da je $\dim U = \dim V$. □

Trditev 3.6.7. Naj bo V končnorazsežen vektorski prostor in U podprostor v V. Potem obstaja tak podprostor W v V, da je $V = U \oplus W$ in $\dim V = \dim U + \dim W$.

Dokaz. Bazo U dopolnimo do baze V. W definiramo kot linearno ogrinjačo vektorjev, ki smo jih dodali. □

Trditev 3.6.8. Naj bo V končnorazsežen prostor in $U \leq V$. Potem je

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

Dokaz. V 2. izrek o izomorfizmu (3.4.5) vstavimo $V_1 = W$ in $V_2 = U$, pri čemer je $V = U \oplus W$. □

Trditev 3.6.9. Naj bo V končnorazsežen vektorski prostor in $V_1, V_2 \leq V$. Potem je

$$\dim(V_1 + V_2) = \dim V_1 + \dim V_2 - \dim(V_1 \cap V_2).$$

Dokaz. Uporabimo 2. izrek o izomorfizmu (3.4.5) in prejšnjo trditev. □

Posledica 3.6.9.1. $\dim(V_1 \oplus V_2) = \dim V_1 + \dim V_2$.

Trditev 3.6.10. Naj bosta U in V končnorazsežna vektorska prostora nad $\mathbb{F}$ in $A\colon U \to V$ linearna preslikava. Potem je

$$\dim \ker A + \dim \operatorname{im} A = \dim U.$$

Dokaz. Uporabimo 1. izrek o izomorfizmu (3.4.4). □

Definicija 3.6.11. Naj bo $A\colon U \to V$ linearna. Številu

$$\operatorname{rang} A = \dim \operatorname{im} A$$

pravimo *rang* preslikave A.

4 Matrike

»Aja pa snemati moram začeti."
—prof. dr. Primož Moravec, preden je pozabil začeti snemati

4.1 Linearne preslikave med končnorazsežnimi vektorskimi prostori in matrike

Od tu dalje obravnavamo le končnorazsežne vektorske prostore.

Naj bosta U, V vektorska prostora nad $\mathbb{F}$. Izberimo bazi prostorov U in V

$$\mathcal{B} = \{u_i \mid i \leq n\},$$
$$\mathcal{C} = \{v_i \mid i \leq m\}.$$

Naj bo $A\colon U \to V$ linearna preslikava.

Trditev 4.1.1. *A je natanko določena s slikami vektorjev iz $\mathcal{B}$.*

Dokaz. Vsak vektor iz U lahko izrazimo kot linearno kombinacijo baznih vektorjev. □

Vektorje Au_i lahko razvijemo po bazi $\mathcal{C}$:

$$Au_i = \sum_{j=1}^{m} \alpha_{j,i} v_j$$

Definicija 4.1.2. Tabeli

$$A_{\mathcal{CB}} = \begin{bmatrix} \alpha_{1,1} & \alpha_{1,2} & \dots & \alpha_{1,n} \\ \alpha_{2,1} & \alpha_{2,2} & \dots & \alpha_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_{m,1} & \alpha_{m,1} & \dots & \alpha_{m,n} \end{bmatrix}$$

pravimo *matrika*, ki pripada linearni preslikavi A glede na bazi $\mathcal{B}$ in $\mathcal{C}$. Pravimo, da je ta matrika $m \times n$ matrika nad $\mathbb{F}$. Označimo

$$\mathbb{F}^{m\times n} = \{\text{vse } m \times n \text{ matrike nad poljem } \mathbb{F}\}.$$

Recimo, da imamo matriko $A \in \mathbb{F}^{m\times n}$. Potem ta matrika določa linearno preslikavo

$$A\colon \mathbb{F}^n \to \mathbb{F}^m$$

na naslednji način:

Izberemo standardno bazo $\mathbb{F}^n\colon \mathcal{S} = \{e_1, e_2, \dots, e_n\}$. Vektorju e_i priredimo i-ti stolpec matrike A.

Trditev 4.1.3. Naj bosta U in V vektorska prostora nad $\mathbb{F}$, $\mathcal{B}$ in $\mathcal{C}$ pa bazi za U in V. Potem je preslikava

$$\Phi_{\mathcal{CB}} \colon \operatorname{Hom}_{\mathbb{F}}(U,V) \to \mathbb{F}^{m\times n}, \quad \Phi_{\mathcal{CB}}(A) = A_{\mathcal{CB}}$$

bijekcija.

Dokaz. Ni težko videti, da lahko vsaki matriki priredimo linearno preslikavo, različni linearni preslikavi pa imata različni matriki. □

Definicija 4.1.4. Naj $\mathbb{F}^{m\times n}$ definiramo seštevanje in množenje s skalarjem iz $\mathbb{F}$ na naslednji način:

i) Za $A, B \in \mathbb{F}^{m\times n}$, kjer je $A = [a_{i,j}]_{\substack{1\le i\le m\\ 1\le j\le n}}$ in $B = [b_{i,j}]_{\substack{1\le i\le m\\ 1\le j\le n}}$, je

$$A + B = [a_{i,j} + b_{i,j}]_{\substack{1\le i\le m\\ 1\le j\le n}}.$$

ii) Za $A \in \mathbb{F}^{m\times n}$, kjer je $A = [a_{i,j}]_{\substack{1\le i\le m\\ 1\le j\le n}}$, je

$$\alpha \cdot A = [\alpha \cdot a_{i,j}]_{\substack{1\le i\le m\\ 1\le j\le n}}.$$

Opomba 4.1.4.1. To seštevanje in množenje s skalarjem se ujema s seštevanjem in množenjem s skalarjem, ki smo jih definirali za vektorje.

Trditev 4.1.5. $F^{m\times n}$ z zgoraj definiranim seštevanjem in množenjem s skalarjem postane vektorski prostor nad $\mathbb{F}$.

Dokaz. The proof is obvious and need not be mentioned. □

Izrek 4.1.6. Naj bosta U in V končnorazsežna vektorska prostora nad $\mathbb{F}$, $\mathcal{B}$ in $\mathcal{C}$ pa njuni bazi. Potem je

$$\Phi_{\mathcal{CB}} \colon \operatorname{Hom}_{\mathbb{F}}(U,V) \to \mathbb{F}^{m\times n}, \quad \Phi_{\mathcal{CB}}(A) = A_{\mathcal{CB}}$$

izomorfizem vektorskih prostorov.

Dokaz. The proof is obvious and need not be mentioned. □

V posebnem primeru, ko imamo linearno preslikavo $A \colon \mathbb{F}^n \to \mathbb{F}^m$, lahko za $\mathbb{F}^n$ in $\mathbb{F}^m$ izberemo standardni bazi

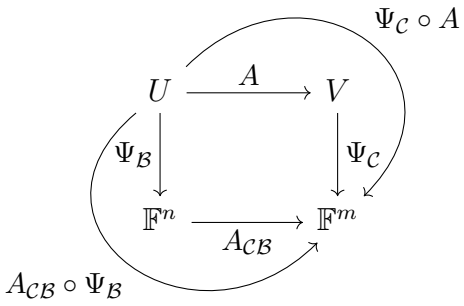
$$\mathcal{B} = \{e_1, e_2, \ldots, e_n\} \quad \text{in} \quad \mathcal{C} = \{f_1, f_2, \ldots, f_m\}.$$

Potem je i-ta komponenta vektorja Ax kar »skalarni produkt« i-te vrstice matrike $A_{\mathcal{CB}}$ in stolpca x.

Definicija 4.1.7. Naj bo $A \in \mathbb{F}^{m\times n}$ in $x \in \mathbb{F}^n$. *Produkt matrike A z vektorjem x* je vektor $A \cdot x$, katerega i-ta komponenta je skalarni produkt i-te vrstice matrike A in stolpca x.

Opomba 4.1.7.1. Če je $A \colon \mathbb{F}^m \to \mathbb{F}^n$ in sta $\mathcal{B}$ ter $\mathcal{C}$ standardni bazi, potem je $Ax = A_{\mathcal{CB}} \cdot x$.

Izrek 4.1.8. Naj bo $A\colon U \to V$ linearna preslikava in $\mathcal{B} = \{u_i \mid 0 < i \leq n\}$ ter $\mathcal{C} = \{v_i \mid 0 < i \leq m\}$ bazi U in V. Naj bosta $\Psi_{\mathcal{B}}\colon U \to \mathbb{F}^n$ in $\Psi_{\mathcal{C}}\colon V \to \mathbb{F}^m$ izomorfizma, za katera je $\Psi_{\mathcal{B}} u_i = e_i$ in $\Psi_{\mathcal{C}} v_i = f_i$, kjer sta $\{e_i \mid 0 < i \leq n\}$ in $\{f_i \mid 0 < i \leq m\}$ standardni bazi. Potem je $\Psi_{\mathcal{C}} \circ A = A_{\mathcal{CB}} \circ \Psi_{\mathcal{B}}$.



Slika 1: Izrek 4.1.8 – »diagram komutira«

Dokaz. Dovolj je trditev dokazati za bazne vektorje. Velja pa

$$(\Psi_{\mathcal{C}} \circ A)u_i = \Psi_{\mathcal{C}}(Au_i) = \Psi_{\mathcal{C}}\left(\sum_{j=1}^{m} a_{j,i} v_j\right) = \sum_{j=1}^{m} a_{j,i} f_j$$

in

$$(A_{\mathcal{CB}} \circ \Psi_{\mathcal{B}})u_i = A_{\mathcal{CB}}(\Psi_{\mathcal{B}} u_i) = A_{\mathcal{CB}} e_i = A_{\mathcal{CB}} \cdot e_i = \sum_{j=1}^{m} a_{j,i} f_j. \qquad \square$$

4.2 Množenje matrik

Definicija 4.2.1. Naj bo $A \in \mathbb{F}^{m\times n}$ in $B \in \mathbb{F}^{n\times p}$. Definiramo matriko $A\cdot B \in \mathbb{F}^{m\times p}$ tako, da je element (i,j) matrike skalarni produkt i-te vrstice matrike A in j-tega stolpca matrike B, oziroma

$$\sum_{k=1}^{n} a_{i,k}\cdot b_{k,j}.$$

Izrek 4.2.2. Naj bosta $A\colon U \to V$ in $B\colon W \to U$ linearni preslikavi. Naj bodo $\mathcal{B}$, $\mathcal{C}$ in $\mathcal{D}$ zaporedoma baze U, V in W. Za linearno preslikavo $A\circ B\colon W \to V$ velja

$$(A\circ B)_{\mathcal{CD}} = A_{\mathcal{CB}}\cdot B_{\mathcal{BD}}.$$

Dokaz. Opazimo, da je množenje asociativno. □

Posledica 4.2.2.1. Če so produkti in vsote definirani, veljajo naslednje lastnosti:

1. $A\cdot(BC) = (AB)\cdot C$
2. $A\cdot(B+C) = AB + AC$
3. $(B+C)\cdot A = BA + CA$
4. $(\alpha A)B = A(\alpha B) = \alpha(AB)$

4.3 Dualni prostor in dualna preslikava

Definicija 4.3.1. Naj bo V vektorski prostor nad $\mathbb{F}$. *Linearen funkcional* je linearna preslikava $\varphi\colon V \to \mathbb{F}$. *Dualni prostor* vektorskega prostora V je množica vseh linearnih funkcionalov, ki slikajo iz V v $\mathbb{F}$, oziroma $V^* = \mathrm{Hom}_{\mathbb{F}}(V, \mathbb{F})$.

Izrek 4.3.2. Naj bo $\{v_1, \ldots, v_n\}$ baza prostora V. Definiramo linearne funkcionale $\varphi_1, \ldots, \varphi_n \in V^*$ na naslednji način:

$$\varphi_i(v_j) = \begin{cases} 1, & i = j \\ 0, & i \neq j \end{cases}$$

Potem je $\{\varphi_1, \ldots, \varphi_n\}$ baza prostora V^*. Tej bazi pravimo *dualna baza* baze $\{v_1, \ldots, v_n\}$.

Dokaz. Očitno so φ_i linearno neodvisni. Za poljuben $\varphi \in V^*$ velja

$$\varphi = \sum_{i=1}^{n} \varphi(v_i) \cdot \varphi_i.$$

Dovolj je enakost dokazati za bazne vektorje, kar je trivialno. □

Posledica 4.3.2.1. $\dim V^* = \dim V$, oziroma $V^* \cong V$.

Definicija 4.3.3. Naj bo V vektorski prostor in X neprazna podmnožica v V. Definiramo

$$X^0 = \{\varphi \in V^* \mid \forall x \in X\colon \varphi(x) = 0\}.$$

Množici X^0 pravimo *anihilator* množice X.

Trditev 4.3.4. Če je $X \subseteq V$, je X^0 vektorski podprostor v V^*.

Dokaz. X^0 je jedro preslikave. □

Trditev 4.3.5. Recimo, da je $V = U \oplus W$. Potem je $U^0 \cong W^*$.

Dokaz. Za izomorfizem preprosto izberemo zožitev funkcionala na W. □

Definicija 4.3.6. Naj bo $A\colon U \to V$ linearna preslikava in $\varphi \in V^*$ linearen funkcional. Potem je $\varphi A \in U^*$. To pomeni, da imamo preslikavo $A^*\colon V^* \to U^*$, za katero je $A^*(\varphi) = \varphi A$. Tej preslikavi pravimo *dualna preslikava* preslikave A.

Trditev 4.3.7. A^* je linearna preslikava.

Dokaz. A^* je kompozitum dveh linearnh preslikav, kar je linearna preslikava po trditvi 3.3.10. □

Izrek 4.3.8. Naj bo $A\colon U \to V$ linearna.

i) $\ker A^* = (\mathrm{im}\, A)^0$

ii) $\mathrm{rang}\, A^* = \mathrm{rang}\, A$

Dokaz. i) Veljajo ekvivalence

$$\varphi \in \ker A^* \iff \varphi A = 0 \iff \varphi(Au) = 0 \ \forall u \in U \iff \varphi \in (\operatorname{im} A)^0.$$

ii) Naj bo W tak podprostor V, da je $V = \operatorname{im} A \oplus W$. Po trditvi 4.3.5 je

$$W^* \cong (\operatorname{im} A)^0 \cong \ker A^*.$$

Torej je

$$\operatorname{rang} A^* = \dim V^* - \dim \ker A^* = \dim V - \dim W = \dim \operatorname{im} A = \operatorname{rang} A. \qquad \square$$

Definicija 4.3.9. Naj bo $A \in \mathbb{F}^{m\times n}$. *Transponiranka* matrike A je matrika $A^\top \in \mathbb{F}^{n\times m}$, katere (i,j)-ti element je (j,i)-ti element matrike A.

Posledica 4.3.9.1. Transponiranje je izomorfizem.

Izrek 4.3.10. Naj preslikavi $A\colon U \to V$ v bazah $\mathcal{B}$ in $\mathcal{C}$ prostorov U in V pripada matrika $A_{\mathcal{C}\mathcal{B}}$. Potem dualni preslikavi $A^*\colon V^* \to U^*$ v dualnih bazah $\mathcal{C}^*$ in $\mathcal{B}^*$ pripada matrika

$$A^*_{\mathcal{B}^*\mathcal{C}^*} = (A_{\mathcal{C}\mathcal{B}})^\top.$$

Dokaz. Najprej označimo $\mathcal{B} = \{u_1, \ldots, u_n\}$, $\mathcal{C} = \{v_1, \ldots, v_m\}$, $\mathcal{B}^* = \{\varphi_1, \ldots, \varphi_n\}$ in $\mathcal{C}^* = \{\psi_1, \ldots, \psi_m\}$. Naj bo še $A_{\mathcal{C}\mathcal{B}} = [a_{i,j}]_{\substack{1\le i\le m\\ 1\le j\le n}}$ in $A^*_{\mathcal{B}^*\mathcal{C}^*} = [b_{i,j}]_{\substack{1\le i\le n\\ 1\le j\le m}}$. Potem je

$$(A^*\psi_j)u_i = \left(\sum_{k=1}^{n} b_{k,j}\varphi_k\right) u_i = \sum_{k=1}^{n} b_{k,j}\varphi_k(u_i) = b_{i,j},$$

po drugi strani pa je

$$(A^*\psi_j)u_i = (\psi_k \circ A)u_i = \psi_j\left(\sum_{k=1}^{m} a_{k,i}v_i\right) = \sum_{k=1}^{m} a_{k,i}\psi_j(v_i) = a_{j,i}. \qquad \square$$

Posledica 4.3.10.1. Za matriki A in B, katerih produkt je definiran, je

$$(AB)^\top = B^\top A^\top.$$

4.4 Rang matrike

Definicija 4.4.1. *Rang matrike* je enak rangu preslikave, ki jo ta matrika določa.

Trditev 4.4.2. Za vse linearne preslikave je $\operatorname{rang} A_{\mathcal{CB}} = \operatorname{rang} A$.

Dokaz. Vemo že $\Psi_{\mathcal{C}} \circ A = A_{\mathcal{CB}} \circ \Psi_{\mathcal{B}}$. Po izreku 4.1.8 sledi $\Psi_{\mathcal{C}}(\operatorname{im} A) = \operatorname{im} A_{\mathcal{CB}}$.

$$\begin{array}{ccc} U & \xrightarrow{\quad A \quad} & V \\ {\scriptstyle \Psi_{\mathcal{B}}}\downarrow & \cong \quad\quad \cong & \downarrow{\scriptstyle \Psi_{\mathcal{C}}} \\ \mathbb{F}^n & \xrightarrow[\quad A_{\mathcal{CB}} \quad]{} & \mathbb{F}^m \end{array}$$

Slika 2: Trditev 4.4.2

Sledi

$$\operatorname{rang} A_{\mathcal{CB}} = \dim \operatorname{im} A_{\mathcal{CB}} = \dim \Psi_{\mathcal{C}}(\operatorname{im} A) = \dim \operatorname{im} A. \qquad \square$$

Definicija 4.4.3. *Vrstični rang* matrike je maksimalno število linearno neodvisnih vrstic matrike. Označimo ga z $\operatorname{rang}_v(A)$.

Stolpčni rang matrike je maksimalno število linearno neodvisnih stolpcev matrike. Označimo ga z $\operatorname{rang}_s(A)$.

Izrek 4.4.4. Za poljubno matriko $A \in \mathbb{F}^{m \times n}$ je

$$\operatorname{rang}_v(A) = \operatorname{rang}_s(A) = \operatorname{rang}(A).$$

Dokaz. Dovolj je dokazati $\operatorname{rang} A = \operatorname{rang}_s A$ (matriko transponiramo in uporabimo izrek 4.3.8). Očitno je $\operatorname{im} A = \operatorname{Lin}\{Ae_1, \ldots, Ae_n\}$, to pa so ravno stolpci v matriki. Dimenzija linearne ogrinjače je največja možna linearno neodvisna podmnožica, kar je ravno stolpčni rang. $\square$

Naslednje transformacije matrike A ne spremenijo ranga:

i) Menjava stolpcev ali vrstic

ii) Množenje stolpca ali vrstice z neničelnim skalarjem

iii) Stolpec ali vrstico prištejemo k nekemu drugemu stolpcu ali vrstici

S takimi transformacijami lahko v neničelni matriki prvi element nastavimo na 1, vse ostale elemente v prvem stolpcu in vrstici pa na 0. Nato ta algoritem ponavljamo na manjših matrikah, dokler ne dobimo samih 0. Potem je rang matrike število 1 na diagonali.

4.5 Sistemi linearnih enačb

Obravnavali bomo sisteme m enačb z n neznankami nad poljem $\mathbb{F}$:

$$\begin{aligned}\sum_{i=1}^{n} a_{1,i}x_i &= b_1\\ \sum_{i=1}^{n} a_{2,i}x_i &= b_2\\ &\vdots\\ \sum_{i=1}^{n} a_{m,i}x_i &= b_m\end{aligned}$$

Sestavimo lahko naslednje matrike:

$$A = \begin{bmatrix} a_{1,1} & a_{1,2} & \dots & a_{1,n}\\ a_{2,1} & a_{2,2} & \dots & a_{2,n}\\ \vdots & \vdots & \ddots & \vdots\\ a_{m,1} & a_{m,2} & \dots & a_{m,n}\end{bmatrix}, \quad x = \begin{bmatrix} x_1\\ x_2\\ \vdots\\ x_n\end{bmatrix} \quad \text{in} \quad b = \begin{bmatrix} b_1\\ b_2\\ \vdots\\ b_m\end{bmatrix}.$$

Sistem lahko zapišemo v matrični obliki

$$Ax = b.$$

V posebnem primeru, ko je $b = 0$, dobimo *homogen sistem*. Množica rešitev tega sistema je $\ker A$. Vedno dobimo vsaj eno rešitev – ničelni vektor. Tej rešitvi pravimo *trivialna rešitev*.

Zgornji sistem ima netrivialne rešitve natanko tedaj, ko $\ker A \neq \{0\}$, torej $n > \operatorname{rang} A$. Recimo, da ima $\ker A$ bazo $\{v_1, v_2, \dots, v_k\}$. Potem ima poljubna rešitev enačbe obliko

$$x = \alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_k v_k.$$

Taki rešitvi pravimo *k-parametrična rešitev*.

Izrek 4.5.1. Naj bo $\widetilde{x}$ rešitev sistema $Ax = b$. Potem je množica vseh rešitev tega sistema enaka

$$\widetilde{x} + \ker A.$$

Dokaz. Velja

$$A(x - \widetilde{x}) = Ax - A\widetilde{x} = Ax - b.$$

To pomeni, da je $Ax = b$ natanko tedaj, ko je $x - \widetilde{x} \in \ker A$. □

Napravimo razširjeno matriko sistema $\widetilde{A} = \left[A \,\middle\vdots\, b\right]$. Naslednje transformacije na $\widetilde{A}$ ne spremenijo množice rešitev:

1. Menjava vrstic
2. Menjava stolpcev (spremeni se vrstni red neznank)
3. Vrstico lahko pomnožimo z neničelnim številom

4. Vrstici lahko prištejemo neko drugo vrstico

Izrek 4.5.2 (Kronecker-Capelli)**.** Sistem linearnih enačb ima rešitev natanko tedaj, ko je $\operatorname{rang} \widetilde{A} = \operatorname{rang} A$.

Dokaz. S podobnim algoritmom kot pri iskanju ranga lahko matriko $\widetilde{A}$ transformiramo v

$$\widetilde{A} \sim \left[\begin{array}{ccccccc:c} 1 & 0 & \dots & 0 & * & \dots & * & * \\ 0 & 1 & \dots & 0 & * & \dots & * & * \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & * & \dots & * & * \\ 0 & 0 & \dots & 0 & 0 & \dots & 0 & c_1 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 0 & 0 & \dots & 0 & c_l \end{array}\right]$$

Temu postopku pravimo *Gaussova eliminacija*.

Naj bo $r = \operatorname{rang} A$. Sistem enačb tako postane

$$\begin{aligned} y_1 + *y_{r+1} + *y_{r+2} + \cdots + *y_n &= * \\ y_2 + *y_{r+1} + *y_{r+2} + \cdots + *y_n &= * \\ &\vdots \\ y_r + *y_{r+1} + *y_{r+2} + \cdots + *y_n &= * \\ 0 &= c_1 \\ 0 &= c_2 \\ &\vdots \\ 0 &= c_l, \end{aligned}$$

kjer so y_i neka permutacija x_i. Recimo, da je $c_1 = c_2 = \cdots = c_l = 0$. V nasprotnem primeru namreč nimamo rešitev. Vidimo, da so lahko y_i poljubni za $i > r$ (teh je ravno $\dim \ker A$), tej parametri pa natanko določajo preostale y.

To pomeni, da ima sistem rešitev natanko tedaj, ko je $c_1 = c_2 = \cdots = c_l = 0$, to pa se zgodi natanko tedaj, ko je $\operatorname{rang} \widetilde{A} = \operatorname{rang} A$. □

Posledica 4.5.2.1. Podan je sistem $Ax = b$. Naj bo $\widetilde{A} = [A \mid b]$.

1. Če je $\operatorname{rang} \widetilde{A} \neq \operatorname{rang} A$, sistem nima rešitev.
2. Če je $\operatorname{rang} \widetilde{A} = \operatorname{rang} A = n$, ima sistem natanko eno rešitev.
3. Če je $\operatorname{rang} \widetilde{A} = \operatorname{rang} A < n$, imamo $(n - \operatorname{rang} A)$-parametrično rešitev sistema.

4.6 Endomorfizmi končnorazsežnih vektorskih prostorov in kvadratne matrike

Spomnimo, $\mathrm{End}_{\mathbb{F}}(V)$ je algebra nad $\mathbb{F}$, kjer je V končnorazsežen vektorski prostor nad $\mathbb{F}$.

Izberemo bazo $\mathcal{B}$ prostora V in endomorfizmu A priredimo matriko $A_{\mathcal{BB}} \in \mathbb{F}^{n\times n}$. To pomeni, da imamo preslikavo

$$\Phi_{\mathcal{BB}} \colon \mathrm{End}_{\mathbb{F}}(V) \to \mathbb{F}^{n\times n}, \quad \Phi_{\mathcal{BB}}(A) = A_{\mathcal{BB}}.$$

$\Phi_{\mathcal{BB}}$ je izomorfizem vektorskih prostorov. Na $\mathbb{F}^{n\times n}$ imamo poleg seštevanja in množenja s skalarjem tudi množenje (množenje matrik), zato je tudi $\mathbb{F}^{n\times n}$ algebra nad $\mathbb{F}$.

Definicija 4.6.1. Naj bosta X in Y algebri nad $\mathbb{F}$. *Homomorfizem algeber* je preslikava $f \colon X \to Y$, za katero velja

i) f je linearna

ii) f je homomorfizem kolobarjev

Izrek 4.6.2. $\Phi_{\mathcal{BB}} \colon \mathrm{End}_{\mathbb{F}}(V) \to \mathbb{F}^{n\times n}$ je izomorfizem algeber.

Dokaz. The proof is obvious and need not be mentioned. □

$\mathrm{End}_{\mathbb{F}}(V)$ ima nevtralni element za množenje – id. Pripada ji *identična matrika*

$$\mathrm{id}_{\mathcal{BB}} = I = \begin{bmatrix} 1 & & & & \\ & 1 & & & \\ & & 1 & & \\ & & & \ddots & \\ & & & & 1 \end{bmatrix}$$

I je enota za množenje v $\mathbb{F}^{n\times n}$.

Definicija 4.6.3. Bijektivnim endomorfizmom vektorskega prostora pravimo *avtomorfizmi* vektorskega prostora V:

$$\mathrm{Aut}_{\mathbb{F}}(V) = \{A \mid A \in \mathrm{End}_{\mathbb{F}}(V), A \text{ je bijektivna}\}.$$

Na $\mathrm{Aut}_{\mathbb{F}}(V)$ seštevanje ni operacija, prav tako pa množenje s skalarjem ni dobro definirano. Produkt je operacija na $\mathrm{Aut}_{\mathbb{F}}(V)$, kjer je produkt avtomorfizmov njun kompozitum.

Trditev 4.6.4. $\mathrm{Aut}_{\mathbb{F}}(V)$ z množenjem je grupa.

Dokaz. The proof is obvious and need not be mentioned. □

Trditev 4.6.5. Naj bo $A \in \mathrm{End}_{\mathbb{F}}(V)$. Naslednje trditve so ekvivalentne:

i) $A \in \mathrm{Aut}_{\mathbb{F}}(V)$

ii) A je surjektivna

iii) A je injektivna

iv) $\mathrm{rang}\, A = \dim V$

Dokaz. Če je A avtomorfizem, je surjektivna.

Če je A surjektivna, zaradi $\dim \ker A + \dim \operatorname{im} A = \dim V$ velja $\dim \ker A = 0$, zato je A injektivna.

Če je A injektivna, je $\operatorname{rang} A = \dim V - \dim \ker A = \dim V$.

Če je $\operatorname{rang} A = \dim V$, je A surjektivna, saj je $\operatorname{im} A \leq V$ in $\dim \operatorname{im} A = \dim V$. □

Definicija 4.6.6. Matrika $A \in \mathbb{F}^{n \times n}$ je *obrnljiva*, če obstaja $B \in \mathbb{F}^{n \times n}$, da je

$$A \cdot B = B \cdot A = I.$$

Matriki B pravimo *inverz matrike* A. Pišemo $B = A^{-1}$.

Opomba 4.6.6.1. Če za matriki A in B velja $A \cdot B = I$, potem je tudi $B \cdot A = I$.

Dokaz. A je inverzna preslikava B, zato je B inverzna preslikava A. □

Opomba 4.6.6.2. Matrika $A \in \mathbb{F}^{n \times n}$ je obrnljiva natanko tedaj, ko je $\operatorname{rang} A = n$. Inverz poiščemo z Gaussovo eliminacijo.

4.7 Prehod med bazami

Definicija 4.7.1. *Prehodna matrika* je matrika za identiteto:

$$P_{\mathcal{CB}} = (\mathrm{id})_{\mathcal{CB}}.$$

Trditev 4.7.2. Naj bodo $\mathcal{B}$, $\mathcal{C}$ in $\mathcal{D}$ baze vektorskega prostora V in $v \in V$ vektor.

i) $P_{\mathcal{CB}} \cdot v_{\mathcal{B}} = v_{\mathcal{C}}$.

ii) $P_{\mathcal{CB}}$ je obrnljiva, $P_{\mathcal{CB}}^{-1} = P_{\mathcal{BC}}$

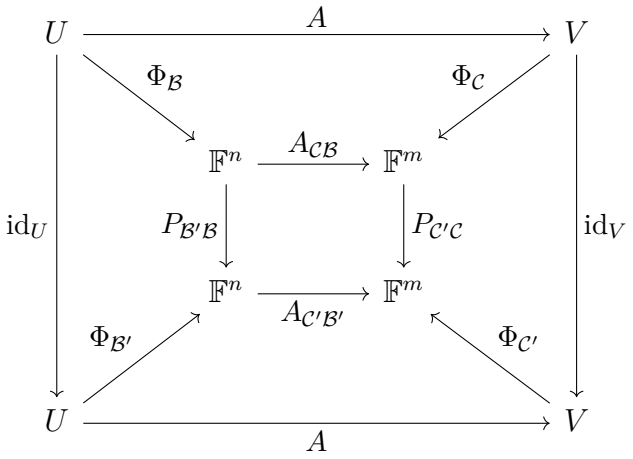
iii) $P_{\mathcal{CD}} \cdot P_{\mathcal{DB}} = P_{\mathcal{CB}}$

Dokaz. Matrike predstavljajo preslikave. □

Recimo, da imamo linearno preslikavo $A\colon U \to V$, kjer sta U in V končnorazsežna netrivialna vektorska prostora. Za U in V izberemo bazi $\mathcal{B}$ in $\mathcal{C}$. Dobimo matriko $A_{\mathcal{CB}}$.

Recimo, da za U in V izberimo še bazi $\mathcal{B}'$ in $\mathcal{C}'$. Dobimo še matriko $A_{\mathcal{C}'\mathcal{B}'}$. Potem je

$$A_{\mathcal{CB}} = P_{\mathcal{CC}'} A_{\mathcal{C}'\mathcal{B}'} P_{\mathcal{B}'\mathcal{B}}.$$



Slika 3: Vemo, da komutirajo zunanji štirikotniki, zato komutira tudi notranji.

Definicija 4.7.3. Naj bosta $A, B \in \mathbb{F}^{m\times n}$ matriki. Pravimo, da sta A in B *ekvivalentni*, če obstajata obrnljivi matriki $P \in \mathbb{F}^{m\times m}$ in $Q \in \mathbb{F}^{n\times n}$, da je

$$B = PAQ.$$

Označimo $A \sim B$.

Opomba 4.7.3.1. Če linearni preslikavi priredimo matriki glede na različna para baz, sta ti matriki vedno ekvivalentni.

Posledica 4.7.3.2. $\sim$ je ekvivalenčna.

Dokaz. The proof is obvious and need not be mentioned. □

Lema 4.7.4. Naj bo $A \in \mathbb{F}^{m\times n}$ in $P \in \mathbb{F}^{m\times m}$ ter $Q \in \mathbb{F}^{n\times n}$ obrnljivi matriki. Potem je

i) $\operatorname{rang} PA = \operatorname{rang} A$

ii) $\operatorname{rang} AQ = \operatorname{rang} A$

iii) Če je $A \sim B$, je $\operatorname{rang} B = \operatorname{rang} A$

Dokaz. Matrike gledamo kot linearne preslikave. Naj bo $\{v_1, v_2, \ldots, v_r\}$ baza $\operatorname{im} A$. Potem je $\{Pv_1, Pv_2, \ldots, Pv_r\}$ baza $\operatorname{im} PA$, saj je P obrnljiva, torej injektivna.

Spomnimo se, da je $\operatorname{rang}(AQ) = \operatorname{rang}(AQ)^\top = \operatorname{rang} Q^\top A^\top$, kar dokaže drugo točko, saj je $Q^\top$ tudi obrnljiva.

Tretja točka je direktna posledica prvih dveh. □

Lema 4.7.5. Recimo, da je $A\colon U \to V$ linearna. Potem obstajata bazi $\mathcal{B}$ za U in $\mathcal{C}$ za V, da je

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

Dokaz. Naj bo $\{w_1, w_2, \ldots, w_k\}$ baza $\ker A$. To bazo dopolnimo do baze U

$$\mathcal{B} = \{u_1, u_2, \ldots, u_l, w_1, w_2, \ldots, w_k\}.$$

Potem je $\{Au_1, Au_2, \ldots, Au_l\}$ baza $\operatorname{im} A$. Če jo dopolnimo do baze $\mathcal{C}$ prostora V, sta $\mathcal{B}$ in $\mathcal{C}$ ravno iskani bazi. □

Izrek 4.7.6. $m \times n$ matriki A in B sta ekvivalentni natanko tedaj, ko je $\operatorname{rang} A = \operatorname{rang} B$.

Dokaz. Uporabimo prejšnjo lemo. □

Definicija 4.7.7. Matriki $A, B \in \mathbb{F}^{n\times n}$ sta *podobni*, če obstaja taka obrnljiva matrika $P \in \mathbb{F}^{n\times n}$, da je

$$B = P^{-1}AP.$$

Opomba 4.7.7.1. Matriki istega endomorfizma v različnih bazah sta si podobni.

Opomba 4.7.7.2. Vsaki podobni matriki sta ekvivalentni.

Trditev 4.7.8. Podobnost je ekvivalenčna relacija.

Dokaz. The proof is obvious and need not be mentioned. □

4.8 Determinante kvadratnih matrik

Definicija 4.8.1. Preslikava $F\colon U^n \to V$ je *n-linearna*, če so vse preslikave

$$\begin{aligned} U &\to V \\ u &\mapsto F(u_1, \dots, u_{i-1}, u, u_{i+1}, \dots) \end{aligned}$$

linearne za vsak i in $u_j \in U$.

Opomba 4.8.1.1. 1-linearne preslikave so ravno linearne preslikave. 2-linearnim preslikavam pravimo tudi *bilinearne* preslikave.

Definicija 4.8.2. Naj bo $F\colon U^n \to V$ n-linearna. Pravimo, da je F *antisimetrična*, če velja

$$F(u_1, \dots, u_i, \dots, u_j, \dots, u_n) = -F(u_1, \dots, u_j, \dots, u_i, \dots, u_n).$$

Trditev 4.8.3. Naj bo $F\colon U^n \to V$ n-linearna antisimetrična preslikava. Recimo, da so $u_1, u_2, \dots, u_n \in U$ in $u_i = u_j$ za neka $i \neq j$. Potem je

$$F(u_1, u_2, \dots, u_n) = 0.$$

Dokaz. The proof is obvious and need not be mentioned. □

Trditev 4.8.4. Naj bo $F\colon U^n \to V$ n-linearna antisimetrična preslikava. Potem

$$F(u_1, \dots, u_i, \dots, u_j + \alpha u_i, \dots, u_n) = F(u_1, \dots, u_i, \dots, u_j, \dots, u_n)$$

Dokaz. The proof is obvious and need not be mentioned. □

Zdaj se omejimo na primer $U = \mathbb{F}^n$, $V = \mathbb{F}$. Naj bo

$$F\colon (\mathbb{F}^n)^n \to \mathbb{F}$$

n-linearna antisimetrična preslikava (funkcional). Elemente $(\mathbb{F}^n)^n$ lahko identificiramo z matrikami. Označimo

$$e_i = \begin{bmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix}.$$

Potem je

$$\begin{aligned} F(A) &= F(Ae_1, Ae_2, \dots, Ae_n) \\ &= \sum_{\sigma \in S_n} F(a_{\sigma(1),1} e_{\sigma(1)}, \dots, a_{\sigma(n),n} e_{\sigma(n)}) \\ &= \sum_{\sigma \in S_n} \left(\prod_{i=1}^{n} a_{\sigma(i),i} \cdot F(e_{\sigma(1)}, \dots, e_{\sigma(n)}) \right) \\ &= \sum_{\sigma \in S_n} \left(\operatorname{sgn} \sigma \cdot \prod_{i=1}^{n} a_{\sigma(i),i} \right) \cdot F(I). \end{aligned}$$

Definicija 4.8.5. Naj bo $A = [a_{i,j}]_{i,j=1,\dots,n}$ matrika v $\mathbb{F}^{n\times n}$. Skalarju

$$\det A = \sum_{\sigma\in S_n} \left(\operatorname{sgn}\sigma \cdot \prod_{i=1}^{n} a_{\sigma(i),i} \right)$$

pravimo *determinanta matrike* A.

Opomba 4.8.5.1. Če je $F\colon (\mathbb{F}^n)^n \to \mathbb{F}$ antisimetrična n-linearna preslikava, je

$$F(A) = \det A \cdot F(I).$$

Trditev 4.8.6. Velja $\det A = \det A^\top$.

Dokaz. Determinanto lahko zapišemo tudi kot

$$\begin{aligned}
\det A &= \sum_{\sigma\in S_n} \left(\operatorname{sgn}\sigma \cdot \prod_{i=1}^{n} a_{i,\sigma^{-1}(i)} \right) \\
&= \sum_{\sigma\in S_n} \left(\operatorname{sgn}\sigma^{-1} \cdot \prod_{i=1}^{n} a_{i,\sigma(i)} \right) \\
&= \sum_{\sigma\in S_n} \left(\operatorname{sgn}\sigma \cdot \prod_{i=1}^{n} a_{i,\sigma(i)} \right) \\
&= \det A^\top.
\end{aligned}$$

□

Opomba 4.8.6.1. Če je

$$A = \begin{bmatrix} a_{1,1} & a_{1,2} & \dots & a_{1,n} \\ a_{2,1} & a_{2,2} & \dots & a_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n,1} & a_{n,2} & \dots & a_{n,n} \end{bmatrix}$$

pišemo

$$\det A = \begin{vmatrix} a_{1,1} & a_{1,2} & \dots & a_{1,n} \\ a_{2,1} & a_{2,2} & \dots & a_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n,1} & a_{n,2} & \dots & a_{n,n} \end{vmatrix}$$

Izrek 4.8.7. Preslikava $\det\colon \mathbb{F}^{n\times n} \to \mathbb{F}$ je n-linearen antisimetričen funkcional.

Dokaz. The proof is obvious and need not be mentioned. □

Opomba 4.8.7.1. Iz izreka sledi

$$\begin{vmatrix} b_{1,1}+c_{1,1} & a_{1,2} & \dots & a_{1,n} \\ b_{2,1}+c_{2,1} & a_{2,2} & \dots & a_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ b_{n,1}+c_{n,1} & a_{n,2} & \dots & a_{n,n} \end{vmatrix} = \begin{vmatrix} b_{1,1} & a_{1,2} & \dots & a_{1,n} \\ b_{2,1} & a_{2,2} & \dots & a_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ b_{n,1} & a_{n,2} & \dots & a_{n,n} \end{vmatrix} + \begin{vmatrix} c_{1,1} & a_{1,2} & \dots & a_{1,n} \\ c_{2,1} & a_{2,2} & \dots & a_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ c_{n,1} & a_{n,2} & \dots & a_{n,n} \end{vmatrix}$$

Podobno velja za ostale stolpce in vrstice. Če v matriki zamenjamo poljubna stolpca oziroma vrstici, je det nove matrike enaka nasprotni vrednosti det začetne matrike. Če ima A dva enaka stolpca oziroma vrstici, je tako $\det A = 0$.

Izrek 4.8.8. $\det\colon \mathbb{F}^{n\times n} \to \mathbb{F}^n$ je multiplikativna.

Dokaz. Definirajmo preslikavo $F\colon \mathbb{F}^{n\times n} \to \mathbb{F}$ kot

$$F(v_1, v_2, \ldots, v_n) = \det(Av_1, Av_2, \ldots, Av_n).$$

Vidimo, da je F n-linearna in antisimetrična. Ker je $F(I) = \det A$, pa je

$$\det(AB) = F(B) = \det A \cdot \det B.$$ □

Definicija 4.8.9. Naj bo $A = [a_{i,j}]_{i,j=1,\ldots,n}$. Označimo z $A_{i,j}$ matriko, ki jo dobimo, če v A odstranimo i-to vrstico in j-ti stolpec. *(i,j)-ti kofaktor* definiramo kot

$$\widetilde{a}_{i,j} = (-1)^{i+j} \cdot \det A_{i,j}.$$

Izrek 4.8.10. Naj bo $A = [a_{i,j}]_{i,j=1,\ldots,n}$ matrika. Potem je za vse i

$$\det A = \sum_{j=1}^{n} a_{i,j} \cdot \widetilde{a}_{i,j}.$$

Simetrično velja za stolpce.

Dokaz. Oglejmo si $\det(A^{(1)}, \ldots, A^{(j-1)}, e_i, A^{(j+1)}, \ldots)$. Očitno je enaka $\widetilde{a}_{i,j}$, saj lahko $a_{i,j}$ z menjavami stolpcev in vrstic prestavimo na zadnje mesto v matriki, pri tem pa se predznak spremeni $2n - i - j$-krat. Zdaj upoštevamo, da je det n-linearna, s čemer smo končali. □

Opomba 4.8.10.1. Zgornji vsoti pravimo *razvoj determinante* po i-ti vrstici oziroma j-tem stolpcu.

Posledica 4.8.10.2. Pri računanju determinant si lahko pomagamo z naslednjimi dejstvi:

i) Če v matriki zamenjamo dve vrstici ali stolpca, se determinanti spremeni le predznak

ii) Izpostavljamo lahko skupne faktorje

iii) Če v matriki nekemu stolpcu oziroma vrstici prištejemo večkratnik nekega drugega stolpca oziramo vrstice, se determinanta ne spremeni

Trditev 4.8.11. Naj bo A $n \times n$ matrika, B pa $m \times m$ matrika. Potem je

$$\begin{vmatrix} A & C \\ 0 & B \end{vmatrix} = \det A \cdot \det B.$$

Dokaz. The proof is obvious and need not be mentioned. □

Definicija 4.8.12. Matrikam oblike

$$\begin{bmatrix} a_{1,1} & a_{1,2} & \dots & a_{1,n} \\ & a_{2,2} & \dots & a_{2,n} \\ & & \ddots & \vdots \\ & & & a_{n,n} \end{bmatrix}$$

pravimo *zgornjetrikotne matrike*. Matrikam oblike

$$\begin{bmatrix} a_{1,1} & & & \\ & a_{2,2} & & \\ & & \ddots & \\ & & & a_{n,n} \end{bmatrix}$$

pravimo *diagonalne matrike*.

Posledica 4.8.12.1. Determinanta zgornjetrikotnih in diagonalnih matrik je kar produkt diagonalnih elementov.

Dokaz. The proof is obvious and need not be mentioned. □

Definicija 4.8.13. Naj bo $A = [a_{i,j}]$ $n \times n$ matrika. Matriki

$$\widetilde{A} = \begin{bmatrix} \widetilde{a}_{1,1} & \widetilde{a}_{1,2} & \dots & \widetilde{a}_{1,n} \\ \widetilde{a}_{2,1} & \widetilde{a}_{2,2} & \dots & \widetilde{a}_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ \widetilde{a}_{n,1} & \widetilde{a}_{n,2} & \dots & \widetilde{a}_{n,n} \end{bmatrix}$$

pravimo *prirejenka* matrike A.

Trditev 4.8.14. Velja

$$A \cdot \widetilde{A}^\top = \det A \cdot I.$$

Dokaz. Velja

$$\sum_{k=1}^{n} a_{i,k}\widetilde{a}_{i,1} = \det A$$

in

$$\sum_{k=1}^{n} a_{i,k}\widetilde{a}_{j,k} = 0,$$

saj je to ravno determinanta matrike z dvema enakima vrsticama. □

Izrek 4.8.15. Naj bo $A \in \mathbb{F}^{n\times n}$. Potem je A obrnljiva natanko tedaj, ko je $\det A \neq 0$.

Dokaz. Naj bo $AB = I$. Potem je $\det A \cdot \det B = \det(AB) = \det I = 1$, zato je $\det A \neq 0$.

Če je $\det A \neq 0$, pa je

$$A \cdot \frac{1}{\det A}\widetilde{A}^\top = I.$$ □

Izrek 4.8.16 (Cramerjevo pravilo)**.** Naj bo $A \in \mathbb{F}^{n\times n}$ in $b \in \mathbb{F}^n$. Recimo, da je A obrnljiva. Naj bo A_i matrika, ki jo dobimo, če v matriki A i-ti stolpec zamenjamo s stolpcem b. Potem rešitve sistema $Ax = b$ dobimo iz formule

$$x_i = \frac{\det A_i}{\det A}.$$

Dokaz. Sistem je ekvivalenten

$$\det A \cdot x = \widetilde{A}^\top b.$$ □

Trditev 4.8.17. Če sta A in B podobni matriki, je $\det A = \det B$.

Dokaz. The proof is obvious and need not be mentioned. □

Definicija 4.8.18. Naj bo V končnorazsežen vektorski prostor nad $\mathbb{F}$ in $A\colon V \to V$ linearna preslikava. Naj bo $\mathcal{B}$ baza prostora V. *Determinanta endomorfizma* A je

$$\det A = \det A_{\mathcal{B}\mathcal{B}}.$$

Opomba 4.8.18.1. Po prejšnji trditvi je $\det A$ dobro definirana.

Definicija 4.8.19. Naj bo $A \in \mathbb{F}^{m\times n}$ in $1 \leq k \leq \min\{m, n\}$. *Minor* reda k je determinanta matrike, katere členi se nahajajo v izbranih k vrsticah in k stolpcih matrike A.

Lema 4.8.20. Naj bo A $m \times n$ matrika. Če so vsi minorji reda k enaki 0, so tudi vsi minorji večjih redov enaki 0.

Dokaz. The proof is obvious and need not be mentioned. □

Izrek 4.8.21. Naj bo A $m \times n$ matrika. Potem je $\operatorname{rang} A$ enak največji vrednosti k, za katero obstaja neničelni minor reda k.

Dokaz. The proof is obvious and need not be mentioned. □

5 Lastne vrednosti in lastni vektorji

»Jaz se opravičujem za zvočne efekte zraven ampak mi pes smrči tako da... To je bil nematematičen del predavanj.«

—prof. dr. Primož Moravec

5.1 Lastne vrednosti

Definicija 5.1.1. Naj bo V vektorski prostor nad poljem $\mathbb{F}$ in $A\colon V \to V$ linearna preslikava. Za neničeln vektor $v \in V$ pravimo, da je *lasten vektor* endomorfizma A, če obstaja $\lambda \in \mathbb{F}$, da velja

$$Av = \lambda v.$$

Skalarju λ pravimo *lastna vrednost* preslikave A.

Definicija 5.1.2. Naj bo $A \in \mathbb{F}^{n\times n}$. Pravimo, da je $v \in \mathbb{F}^n \setminus \{0\}$ *lasten vektor* matrike A, če obstaja $\lambda \in \mathbb{F}$, da velja

$$Av = \lambda v.$$

Skalarju λ pravimo *lastna vrednost* matrike A.

Trditev 5.1.3. Lastni vektorji preslikave A za lastno vrednost λ so natanko neničelni elementi iz $\ker(A - \lambda I)$.

Dokaz. The proof is obvious and need not be mentioned. □

Posledica 5.1.3.1. λ je lastna vrednost za A natanko tedaj, ko je $\det(A - \lambda I) = 0$.

Definicija 5.1.4. Če je λ lastna vrednost preslikave A, podprostoru $\ker(A-\lambda I)$ pravimo *lastni podprostor* za lastno vrednost λ.

Definicija 5.1.5. Polinomu $p_A(\lambda) = \det(A - \lambda I)$ pravimo *karakteristični polinom*.

Trditev 5.1.6. Podobni matriki imata isti karakterističen polinom.

Dokaz. Naj bo $B = PAP^{-1}$. Velja

$$p_B(\lambda) = \det(B-\lambda I) = \det(PAP^{-1}-\lambda PP^{-1}) = \det P\cdot\det(A-\lambda I)\cdot\det P^{-1} = p_A(\lambda).$$ □

Definicija 5.1.7. Naj bo λ lastna vrednost preslikave A.

i) $g(\lambda) = \dim\ker(A - \lambda I)$ imenujemo *geometrijska večkratnost* lastne vrednosti λ.

ii) Večkratnosti λ kot ničle karakterističnega polinoma pravimo *algebraična večkratnost* lastne vrednosti λ.

Definicija 5.1.8. Naj bo $A\colon V \to V$. Pravimo, da se da A *diagonalizirati*, če obstaja taka baza $\mathcal{B}$ prostora V, da je $A_{\mathcal{B}\mathcal{B}}$ diagonalna.

Naj bo $A \in \mathbb{F}^{n\times n}$. Pravimo, da se da A *diagonalizirati*, če je podobna neki diagonalni matriki.

Trditev 5.1.9. Lastne vrednosti diagonalne matrike so ravno elementi na diagonali te matrike.

Dokaz. The proof is obvious and need not be mentioned. □

Izrek 5.1.10. Naj bo $A\colon V \to V$. A se da diagonalizirati natanko tedaj, ko obstaja baza prostora V, sestavljena iz lastnih vektorjev preslikave A.

Dokaz. The proof is obvious and need not be mentioned. □

Trditev 5.1.11. Naj bo $A\colon V \to V$ linearna in $v_1, v_2, \ldots, v_m \in V$ neničelni vektorji, za katere velja $Av_i = \lambda_i v_i$ za paroma različne λ_i. Potem so $v_1, v_2, \ldots, v_m$ linearno neodvisni.

Dokaz. Predpostavimo nasprotno. Naj bo k najmanjše število, za katerega je

$$v_k = \alpha_1 v_1 + \cdots + \alpha_{k-1} v_{k-1}.$$

Potem je

$$\lambda_k v_k = \lambda_1 \alpha_1 v_1 + \cdots + \lambda_{k-1} \alpha_{k-1} v_{k-1}.$$

Tako dobimo

$$(\lambda_k - \lambda_1)\alpha_1 v_1 + \cdots + (\lambda_k - \lambda_{k-1})\alpha_{k-1} v_{k-1} = 0,$$

kar je seveda protislovje. □

5.2 Karakteristični in minimalni polinomi

Definicija 5.2.1. *Matrični polinom* je izraz

$$p(\lambda) = A_k\lambda^k + A_{k-1}\lambda^{k-1} + \cdots + A_1\lambda + A_0,$$

kjer so $A_i \in \mathbb{F}^{n\times n}$.

Opomba 5.2.1.1. λ lahko v zgornji definiciji zamenjamo tudi z matriko.

Definicija 5.2.2. Matrika $B \in \mathbb{F}^{n\times n}$ je *ničla* matričnega polinoma p, če je $p(B) = 0$.

Izrek 5.2.3 (Bezout)**.** Naj bo $A \in \mathbb{F}^{n\times n}$ in p matrični polinom iz $\mathbb{F}^{n\times n}$ stopnje k. Potem obstajata matrični polinom q stopnje $k-1$ in matrika $R \in \mathbb{F}^{n\times n}$, za katera je

$$p(\lambda) = q(\lambda)\cdot(A - \lambda I) + R.$$

Pri tem sta q in R enolično določena.

Dokaz. Koeficiente q po vrsti izrazimo z nastavkom. Na koncu dobimo $R = p(A)$. □

Izrek 5.2.4 (Cayley-Hamilton)**.** Naj bo $A \in \mathbb{F}^{n\times n}$ matrika. Potem je

$$p_A(A) = 0.$$

Dokaz. Oglejmo si $\left(\widetilde{A - \lambda I}\right)^\top$. Elementi matrike so polinomi v λ. Velja

$$\left(\widetilde{A - \lambda I}\right)^\top \cdot (A - \lambda I) = \det(A - \lambda I)\cdot I.$$

Sledi

$$p_A(\lambda) = \left(\widetilde{A - \lambda I}\right)^\top \cdot (A - \lambda I).$$

Po Bezoutovem izreku je $0 = R = p_A(A)$. □

Definicija 5.2.5. Naj bo $A \in \mathbb{F}^{n\times n}$. Polinom $m_A(\lambda)$ je *minimalni polinom* matrike A, če velja:

i) Vodilni koeficient m_A je 1,

ii) $m_A(A) = 0$,

iii) Za vsak neničeln polinom q nižje stopnje je $q(A) \neq 0$.

Izrek 5.2.6. Minimalni polinom matrike je enolično določen.

Dokaz. Če sta p in q minimalna polinoma, je $(p-q)(A) = 0$. □

Trditev 5.2.7. Minimalni polinom matrike A deli njen karakteristični polinom.

Dokaz. Velja

$$p_A(\lambda) = q(\lambda) \cdot m_A(\lambda) + r(\lambda).$$

Sledi, da je $r(A) = 0$, torej je $r \equiv 0$. □

Izrek 5.2.8. V $\mathbb{C}$ ima m_A iste ničle kot p_A.

Dokaz. Ničle p_A so ravno lastne vrednosti matrike. Ker je $m_A(A) = 0$, je

$$0 = m_A(A)x = m_A(\lambda_i)I \cdot x$$

za lastni vektor x. Ker je $x \neq 0$, je $m_A(\lambda_i) = 0$. □

Trditev 5.2.9. Podobni matriki imata isti minimalni polinom.

Dokaz. Naj bo $B = P^{-1}AP$. Recimo, da je $p(A) = 0$. Potem je $p(B) = 0$. □

Definicija 5.2.10. Naj bo $A\colon V \to V$. Minimalni polinom endomorfizma A je minimalni polinom matrike $A_{\mathcal{BB}}$, kjer je $\mathcal{B}$ baza prostora V.

6 Struktura endomorfizmov končnorazsežnih vetorskih prostorov nad $\mathbb{C}$

»Mene malo skrbi če bodo kakšna vprašanja, ker ne znam več dobro algebre.«
»Ni panike, mi tudi ne.«
—prof. dr. Primož Moravec

6.1 Korenski podprostori

Definicija 6.1.1. Naj bo $A\colon V \to V$ linearna preslikava. Podprostor $U \leq V$ je *invarianten* za A, če velja

$$A(U) \subseteq U.$$

Opomba 6.1.1.1. Če je $A\colon V \to V$ in je podprostor U invarianten za A, potem je $A|_U$ endomorfizem prostora U.

Trditev 6.1.2. Naj bo $V = V_1 \oplus \cdots \oplus V_r$, kjer so V_i invariantni podporostori za linearno preslikavo $A\colon V \to V$. Naj bodo $\mathcal{B}_i$ baze podprostorov V_i in $\mathcal{B} = \bigcup \mathcal{B}_i$ baza prostora V. Potem je $A_{\mathcal{B}\mathcal{B}}$ bločna diagonalna matrika.

Dokaz. The proof is obvious and need not be mentioned. □

Definicija 6.1.3. Naj bo $A\colon V \to V$ endomorfizem, kjer je V vektorski prostor nad $\mathbb{C}$, in naj bo

$$p_A(\lambda) = (-1)^n \prod_{i=1}^{n} (\lambda - \lambda_i)^{n_i}$$

njegov karakteristični polinom,

$$m_A(\lambda) = \prod_{i=1}^{n} (\lambda - \lambda_i)^{m_i}$$

pa njegov minimalni polinom. Prostor

$$W_i = \ker(A - \lambda_i I)^{m_i}$$

imenujemo *korenski podprostor* prostora V, ki pripada endomorfizmu A za lastno vrednot λ_i.

Trditev 6.1.4. Podprostori $W_1, W_2, \ldots, W_k$ so invariantni za A in velja

$$V = W_1 \oplus W_2 \oplus \cdots \oplus W_k.$$

Dokaz. Naj bo $x \in W_i$. Sledi, da je $(A - \lambda_i I)^{m_i} x = 0$, zato je tudi $(A - \lambda_i I)^{m_i}(Ax) = A \cdot (A - \lambda_i I)^{m_i} x = 0$, saj A in $(A - \lambda_i I)$ komutirata. Sledi, da so W_i invariantni za A.

Označimo

$$p_i(\lambda) = \prod_{\substack{1 \leq j \leq n \\ j \neq i}} (\lambda - \lambda_j I)^{m_j}.$$

Tej polinomi so si seveda tuji. Po Bezoutovi lemi sledi, da obstajajo kompleksni polinomi $q_1, q_2, \ldots, q_k$, da velja

$$\sum_{i=1}^{k} p_i q_i = 1.$$

Označimo $x_i = p_i(A)q_i(A)x$. Potem je

$$\sum_{i=1}^{k} x_i = \sum_{i=1}^{n} p_i(A)q_i(A)x = x.$$

Ker velja

$$(A - \lambda_i I)^{m_i} x_i = (A - \lambda_i I)^{m_i} p_i(A)q_i(A)x = m_A(A)q_i(A)x = 0,$$

se da vsak $x \in V$ zapisati kot vsota vektorjev iz W_i. Dokazati moramo še, da je ta zapis enoličen. Predpostavimo, da je

$$x = \sum_{i=1}^{k} x_i = \sum_{i=1}^{k} x_i'.$$

Naj bo $y_i = x_i - x_i'$. Dovolj je tako pokazati, da je $y_i = 0$ za vse i. Opazimo, da za $i \neq j$ velja $p_i(A)y_j = 0$. Velja namreč $y_i \in W_i$, saj je $(\lambda - \lambda_j)^{m_j}$ faktor p_i. Ker je

$$\sum_{i=1}^{k} y_i = 0,$$

je tudi $p_i(A)y_i = 0$. Velja pa

$$y_i = Iy_i = \left(\sum_{j=1}^{k} p_j(A)q_j(A) \right) y_i = 0,$$

saj p_j in q_j komutirata. □

Trditev 6.1.5. Naj bo $A_i = A|_{W_i}$. Potem je

$$p_{A_i}(\lambda) = \pm(\lambda - \lambda_i)^{n_i} \quad \text{in} \quad m_{A_i}(\lambda) = \pm(\lambda - \lambda_i)^{m_i}.$$

Dokaz. Naj bo $I_i = I|_i$. Potem je $(A_i - \lambda_i I_i)^{m_i}$ ničelna preslikava. Za $q(\lambda) = (\lambda - \lambda_i)^{m_i}$ tako velja $q(A_i) = 0$, zato m_{A_i} deli q. Naj bo $m_{A_i}(\lambda) = (\lambda - \lambda_i)^{s_i}$. Naj bo

$$f(\lambda) = \prod_{i=1}^{k} (\lambda - \lambda_i)^{s_i}.$$

Zaradi minimalnosti m_A je dovolj dokazati $f(A) = 0$. Vidimo pa, da za poljuben $x \in V$ velja $f(A)x = 0$ (x razpišemo po korenskih podprostorih).

Ker m_{A-i} deli p_{A_i} in imata polinoma isto množico ničel, velja

$$p_{A_i}(\lambda) = \pm(\lambda - \lambda_i)^{r_i}.$$

Ker lahko A bločno diagonaliziramo, pa velja

$$p_A(\lambda) = \pm \prod_{i=1}^{n} (\lambda - \lambda_i)^{r_i},$$

zato je $r_i = n_i$. □

6.2 Endomorfizmi z eno samo lastno vrednostjo

Naj bo V n-dimenzionalen vektorski prostor in $A\colon V \to V$ endomorfizem z eno samo lastno vrednostjo ρ. Naj bosta $p_A(\lambda) = (-1)^n(\lambda - \rho)^n$ in $m_A(\lambda) = (\lambda - \rho)^m$ njegov karakteristični in minimalni polinom.

Trditev 6.2.1. Naj bo $B = A - \rho I$. Potem je

$$p_B(\lambda) = (-1)^n\lambda^n \quad \text{in} \quad m_B(\lambda) = \lambda^m.$$

Dokaz. The proof is obvious and need not be mentioned. □

Definicija 6.2.2. Endomorfizem A je *nilpotenten*, če obstaja tak m, da je $A^m = 0$.

Trditev 6.2.3. Velja

$$\{0\} \subset \ker B \subset \ker B^2 \subset \cdots \subset \ker B^m = V.$$

Dokaz. Očitno je $\ker B^i \subseteq \ker B^{i+1}$. Predpostavimo, da je $\ker B^i = \ker B^{i+1}$ Naj bo $x \in \ker B^{i+2}$. Sledi, da je

$$0 = B^{i+1}(Bx) = B^i(Bx) = B^{i+1}x,$$

zato je $\ker B^{i+2} = \ker B^{i+1}$. Induktivno sledi, da je $\ker B^m = \ker B^i$, kar je seveda protislovje. □

Trditev 6.2.4. Velja $x \in \ker B^i \iff Bx \in \ker B^{i-1}$.

Dokaz. The proof is obvious and need not be mentioned. □

Definicija 6.2.5. Naj bo X neprazna množica vektorjev iz V. Pravimo, da je X *i-linearno neodvisna*, če velja:

i) $X \subseteq \ker B^i$,

ii) Vektorji iz X so linearno neodvisni,

iii) $\operatorname{Lin} X \cap \ker B^{i-1} = \{0\}$.

Trditev 6.2.6. Če je množica X i-linearno neodvisna, je množica

$$BX = \{Bx \mid x \in X\}$$

$(i-1)$-linearno neodvisna.

Dokaz. Očitno je $BX \subseteq \ker B^{i-1}$. Recimo, da je

$$\sum_{i=1}^{k} \alpha_i \cdot Bx_i = 0.$$

Sledi, da je

$$B\left(\sum_{i=1}^{k} \alpha_i x_i\right) = 0.$$

Sledi, da je

$$\sum_{i=1}^{k} \alpha_i x_i = 0,$$

torej so vse α_i enake 0.

Naj bo $y \in \mathrm{Lin}(BX) \cap \ker B^{i-2}$. Sledi, da je

$$0 = B^{i-2}y = B^{i-2}\left(B\left(\sum_{i=1}^{k} \alpha_i x_i\right)\right).$$

Sledi, da je $y = 0$. □

Definicija 6.2.7. Naj bo B nilpotenten endomorfizem, za katerega je $B^m = 0$. Obstaja podprostor U_i v V, da je

$$\ker B^{m-i+1} = \ker B^{m-i} \oplus U_i.$$

Naj bo

$$\mathcal{U}_i = \left\{u_1^{(i)}, u_2^{(i)}, \ldots, u_{s_i}^{(i)}\right\}$$

baza prostora U_i, za katero je $B\mathcal{U}_{i-1} \subseteq \mathcal{U}_i$. Množici

$$\mathcal{U} = \bigcup_{i=1}^{m} \mathcal{U}_i$$

pravimo *Jordanova baza* endomorfizma B.

Opomba 6.2.7.1. Množica $\mathcal{U}_i$ je $m - i + 1$-linearno neodvisna.

Trditev 6.2.8. Velja

$$V = U_1 \oplus U_2 \oplus \cdots \oplus U_m.$$

Dokaz. The proof is obvious and need not be mentioned. □

Posledica 6.2.8.1. Jordanova baza je baza prostora V.

Definicija 6.2.9. *Jordanova forma* je matrika

$$J(B) = B_{\mathcal{U}\mathcal{U}},$$

pri čemer $\mathcal{U}$ vzamemo v vrstnem redu

$$\mathcal{U} = \left\{u_1^{(m)}, u_1^{(m-1)}, \ldots, u_1^{(1)}, u_2^{(m)}, \ldots\right\}.$$

Opomba 6.2.9.1. Jordanova forma je oblike

$$J(B) = \begin{bmatrix} \underbrace{\begin{bmatrix} 0 & 1 & 0 & \ldots & 0 \\ 0 & 0 & 1 & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \ldots & 1 \\ 0 & 0 & 0 & \ldots & 0 \end{bmatrix}}_{\textit{Jordanova kletka}} & & \\ & \ddots & \\ & & \begin{bmatrix} 0 & 1 & 0 & \ldots & 0 \\ 0 & 0 & 1 & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \ldots & 1 \\ 0 & 0 & 0 & \ldots & 0 \end{bmatrix} \end{bmatrix}$$

Posledica 6.2.9.2. Matrika endomorfizma A z edino lastno vrednostjo ρ v Jordanovi bazi je oblike

$$J(A) = \begin{bmatrix} \boxed{\begin{matrix} \rho & 1 & & \\ & \rho & \ddots & \\ & & \ddots & 1 \\ & & & \rho \end{matrix}} & & \\ & \ddots & \\ & & \boxed{\begin{matrix} \rho & 1 & & \\ & \rho & \ddots & \\ & & \ddots & 1 \\ & & & \rho \end{matrix}} \end{bmatrix}$$

Tej matriki pravimo *Jordanova forma* endomorfizma A.

Definicija 6.2.10. *Jordanova forma* endomorfizma A je diagonalno bločna matrika Jordanovih form zožitev endomorfizma na korenske podprostore.

Opomba 6.2.10.1. Če je $A \in \mathbb{C}^{n\times n}$, lahko A gledamo kot endomorfizem. Jordanovi formi tega endomorfizma pravimo *Jordanova forma* matrike A. Če je $\mathcal{U}$ Jordanova baza, je $J(A) = A_{\mathcal{U}\mathcal{U}}$ in

$$A = P_{\mathcal{S}\mathcal{U}} J(A) P_{\mathcal{U}\mathcal{S}}.$$

6.3 Spektralna razčlenitev endomorfizma

Definicija 6.3.1. Preslikava $P\colon V \to V$ je *projektor*, če obstajata podprostora V_1 in V_2 v V, da velja:

i) $V = V_1 \oplus V_2$

ii) $\forall x \in V_1\colon Px = x$

iii) $\forall x \in V_2\colon Px = 0$

Pravimo, da je P projektor na V_1 vzdolž V_2.

Trditev 6.3.2. P je projektor natanko tedaj, ko je $P^2 = P$. V tem primeru P projicira na $\operatorname{im} P$ vzdolž $\ker P$.

Dokaz. The proof is obvious and need not be mentioned. □

Trditev 6.3.3. Naj bo

$$V = V_1 \oplus V_2 \oplus \cdots \oplus V_k.$$

Naj bo P_i projektor na V_i vzdolž direktne vsote preostalih prostorov V_i'. Potem velja

i) $\sum_{i=1}^{k} P_i = I$

ii) Če je $i \neq j$, je $P_iP_j = 0$

Dokaz. The proof is obvious and need not be mentioned. □

Trditev 6.3.4. Naj bo P projektor in A endomorfizem prostora V. Recimo, da sta $\ker P$ in $\operatorname{im} P$ invariantna za A. Potem je

$$AP = PA.$$

Dokaz. The proof is obvious and need not be mentioned. □

Trditev 6.3.5. Naj bo $A\colon V \to V$ endomorfizem nad $\mathbb{C}$ in

$$m_A = \prod_{i=1}^{k} (\lambda - \lambda_i)^{m_i}$$

njegov minimalni polinom. Naj bodo $W_i = \ker(A - \lambda_i I)^{m_i}$ korenski podprostori prostora V. Naj bo P_i projektor na W_i vzdolž W_i'. naj bo $N_i = (A - \lambda_i I)P_i$. Velja

i) $N_iP_i = P_iN_i = N_i$

ii) $N_iP_j = P_jN_i = 0$ za $i \neq j$

iii) $N_i^{m_i} = 0$, $N_i^{m_i - 1} \neq 0$

iv) $N_iN_j = 0$ za $i \neq j$

v) $(\lambda_iP_i + N_i)(\lambda_jP_j + N_j) = 0$ za $i \neq j$

Dokaz. Uporabimo prejšnje trditve o projektorjih:

i) Velja
$$N_iP_i = (A - \lambda_i I)P_i^2 = N_i$$
in
$$P_iN_i = P_iAP_i - \lambda_i P_i^2 = (A - \lambda_i I)P_i = N_i.$$

ii) Velja $N_iP_j = (A - \lambda_i I)P_iP_j = 0$ in
$$P_jN_i = P_j(A - \lambda_i I)P_i = AP_jP_i = 0.$$

iii) Ker $A - \lambda_i I$ in P_i komutirata, je $N_i^m = (A - \lambda_i I)^m P_i$. S tem je trditev dokazana, saj je minimalni polinom zožitve $A - \lambda_i I$ na W_i enak λ^{m_i}.

iv) Podobno kot pri prejšnjih točkah je
$$N_iN_j = (A - \lambda_i I)(A - \lambda_j I)P_iP_j = 0.$$

v) Sledi direktno iz ii) in iv). □

Trditev 6.3.6. Velja
$$A = \sum_{i=1}^{k}(N_i + \lambda_i I)P_i = \sum_{i=1}^{k}(N_i + \lambda_i P_i).$$
Takemu zapisu pravimo *spektralna razčlenitev endomorfizma.*

Dokaz. The proof is obvious and need not be mentioned. □

Trditev 6.3.7. Velja
$$A^n = \sum_{i=1}^{k}(N_i + \lambda_i P_i)^n.$$

Dokaz. The proof is obvious and need not be mentioned. □

Posledica 6.3.7.1. Če potenciramo Jordanovo formo, lahko potenciramo vsako kletko posebej.

6.4 Funkcije matrik in endomorfizmov

Trditev 6.4.1. Naj bo

$$J = \begin{bmatrix} \rho & 1 & & \\ & \rho & \ddots & \\ & & \ddots & 1 \\ & & & \rho \end{bmatrix}$$

Jordanova kletka. Potem je

$$J^n = \begin{bmatrix} \binom{n}{0}\rho^n & \binom{n}{1}\rho^{n-1} & \cdots & \\ & \binom{n}{0}\rho^n & \ddots & \vdots \\ & & \ddots & \binom{n}{1}\rho^{n-1} \\ & & & \binom{n}{0}\rho^n \end{bmatrix}$$

Dokaz. Razpišemo lahko

$$J^n = (N + \rho I)^n = \sum_{k=0}^{n} \binom{n}{k} \rho^{n-k} N^k. \qquad \square$$

Posledica 6.4.1.1. Velja

$$p(A) = P \cdot p(J(A)) \cdot P^{-1}.$$

Trditev 6.4.2. Naj bo J Jordanova kletka in P polinom. Potem je

$$p(J) = \begin{bmatrix} p(\rho) & \frac{p'(\rho)}{1!} & \frac{p''(\rho)}{2!} & \cdots & \\ & p(\rho) & \frac{p'(\rho)}{1!} & \ddots & \vdots \\ & & p(\rho) & \ddots & \frac{p''(\rho)}{2!} \\ & & & \ddots & \frac{p'(\rho)}{1!} \\ & & & & p(\rho) \end{bmatrix}$$

Dokaz. p lahko razpišemo kot Taylorjev polinom v okolici točke ρ. $\square$

Definicija 6.4.3. Naj bo f dovolj gladka funkcija in J Jordanova kletka. Potem definiramo

$$f(J) = \begin{bmatrix} f(\rho) & \frac{f'(\rho)}{1!} & \frac{f''(\rho)}{2!} & \cdots & \\ & f(\rho) & \frac{f'(\rho)}{1!} & \ddots & \vdots \\ & & f(\rho) & \ddots & \frac{f''(\rho)}{2!} \\ & & & \ddots & \frac{f'(\rho)}{1!} \\ & & & & f(\rho) \end{bmatrix}$$

Podobno definiramo $f(A) = Pf(J(A))P^{-1}$, pri čemer f uporabimo na vsaki kletki posebej.

7 Vektorski prostori s skalarnim produktom

7.1 Skalarni produkt

Definicija 7.1.1. Naj bo $\mathbb{F} \in \{\mathbb{R}, \mathbb{C}\}$ in V vektorski prostor nad $\mathbb{F}$. *Skalarni produkt* na V je preslikava $\langle \cdot, \cdot \rangle : V \times V \to \mathbb{F}$, ki vektorjema (u, v) priredi skalar $\langle u, v \rangle$, ki zadošča naslednjim pogojem:

i) Pozitivna definitnost:
   - $\forall x \in V\colon\ \langle x, x \rangle \geq 0$
   - $\langle x, x \rangle = 0 \iff x = 0$

ii) Aditivnost v 1. faktorju: $\forall x, y, z \in V\colon\ \langle x + y, z \rangle = \langle x, z \rangle + \langle y, z \rangle$

iii) Homogenost v 1. faktorju: $\forall x, y \in V,\ \forall \alpha \in \mathbb{F}\colon\ \langle \alpha x, y \rangle = \alpha \langle x, y \rangle$

iv) Poševna komutativnost: $\forall x, y \in V\colon\ \langle x, y \rangle = \overline{\langle y, x \rangle}$

Posledica 7.1.1.1. Naj bo $\langle\ ,\ \rangle$ skalarni produkt na V. Potem velja

i) $\forall x, y, z \in V\colon\ \langle x, y + z \rangle = \langle x, y \rangle + \langle x, z \rangle$

ii) $\forall x, y \in V,\ \forall \alpha \in \mathbb{F}\colon\ \langle x, \alpha y \rangle = \overline{\alpha} \langle x, y \rangle$

Definicija 7.1.2. Naj bo V vektorski prostor s skalarnim produktom in $x \in V$. Potem

$$\|x\| = \sqrt{\langle x, x \rangle}$$

imenujemo *norma* vektorja x.

Izrek 7.1.3 (Cauchy–Schwarzova neenakost)**.** Naj bo V vektorski prostor s skalarnim produktom. Potem je

$$\|x\| \cdot \|y\| \geq |\langle x, y \rangle| .$$

Enakost velja natanko tedaj, ko sta x in y linearno odvisna.

Dokaz. Opazimo, da je[1]

$$\begin{aligned} 0 &\leq \|\langle y, y \rangle\, x - \langle x, y \rangle\, y\|^2 \\ &= \langle \langle y, y \rangle\, x - \langle x, y \rangle\, y, \langle y, y \rangle\, x - \langle x, y \rangle\, y \rangle \\ &= \langle y, y \rangle \cdot \overline{\langle y, y \rangle} \cdot \langle x, x \rangle - \langle y, y \rangle \cdot \overline{\langle x, y \rangle} \cdot \langle x, y \rangle \\ &= \|y\|^4 \cdot \|x\|^2 - \|y\|^2 \cdot |\langle x, y \rangle|^2 \\ &= \|y\|^2 \left(\|y\|^2 \cdot \|x\|^2 - |\langle x, y \rangle|^2 \right). \end{aligned}$$

□

Trditev 7.1.4. Naj bo V vektorski prostor s skalarnim produktom. Potem velja:

i) $\|x\| \geq 0$ z enakostjo natanko tedaj, ko je $x = 0$

ii) $\|\alpha x\| = |\alpha| \cdot \|x\|$

iii) $\|x + y\| \leq \|x\| + \|y\|$

[1] V tretji vrstici se preostala dva člena pokrajšata.

Dokaz. Dokažimo trikotniško neenakost. Po Cauchyjevi neenakosti je

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

Definicija 7.1.5. Naj bo V poljuben vektorski prostor. *Norma* na V je preslikava $\|\cdot\| : V \to \mathbb{F}$, ki zadošča lastnostim trditve 7.1.4. Pravimo, da je V *normiran prostor*.

Definicija 7.1.6. Naj bo V normiran prostor in $x, y \in V$. *Razdalja*[2] med vektorjema x in y je

$$d(x,y) = \|x-y\| .$$

[2] S tem predpisom postane (V,d) *metrični prostor*.

7.2 Ortogonalnost

Naj bo V vektorski prostor s skalarnim produktom.

Definicija 7.2.1. Vektorja $u, v \in V$ sta *ortogonalna*, če je $\langle u, v \rangle = 0$.

Definicija 7.2.2. *Kot med vektorjema* u in v je definiran s predpisom

$$\cos \varphi = \operatorname{Re}\left(\frac{\langle u, v \rangle}{\|u\| \cdot \|v\|} \right).$$

Trditev 7.2.3. Če so $v_1, v_2, \ldots, v_k$ neničelni paroma pravokotni vektorji, so linearno neodvisni.

Dokaz. V nasprotnem primeru velja

$$0 = \langle 0, v_i \rangle = \left\langle \sum_{j=1}^{k} \alpha_j v_j, v_i \right\rangle = \alpha_i \cdot \langle v_i, v_i \rangle . \qquad \square$$

Posledica 7.2.3.1. Če je $\dim V = n$, ima vsaka množica neničelnih pravokotnih vektorjev kvečjemu n elementov.

Definicija 7.2.4. Naj bo X podmnožica v V. Pravimo, da je X *ortogonalna* množica, če velja

$$\forall x, y \in X \colon \langle x, y \rangle = 0.$$

Izrek 7.2.5 (Pitagora)**.** Naj bo V vektorski prostor s skalarnim produktom in $u, v \in V$ ortogonalna vektorja. Potem je

$$\|u + v\|^2 = \|u\|^2 + \|v\|^2 .$$

Dokaz. The proof is obvious and need not be mentioned. $\square$

Definicija 7.2.6. Naj bo X podmnožica v V. Pravimo, da je X *ortonomirana* množica, če je ortogonalna in velja

$$\forall x \in X \colon \|x\| = 1.$$

Izrek 7.2.7. Recimo, da so vektorji $v_1, v_2, \ldots, v_k$ linearno neodvisni vektorji v V. Potem obstajajo paroma ortogonalni vektorji $u_1, u_2, \ldots, u_k$, za katere je

$$\operatorname{Lin}\{u_1, u_2, \ldots, u_k\} = \operatorname{Lin}\{v_1, v_2, \ldots, v_k\} .$$

Dokaz. Indukcija (*Gram–Schmidt ortogonalizacija*). $\square$

Posledica 7.2.7.1. Vsak končnorazsežen vektorski prostor s skalarnim produktom ima ortonormirano bazo.

Trditev 7.2.8. Naj bo $\{u_1, \ldots, u_n\}$ ortonormirana baza vektorskega prostora V in $v \in V$. Potem je

$$v = \sum_{i=1}^{n} \langle v, u_i \rangle \cdot u_i .$$

Dokaz. The proof is obvious and need not be mentioned. □

Definicija 7.2.9. Naj bosta V_1 in V_2 vektorska prostora nad $\mathbb{F}$ s skalarnima produktoma $\langle \cdot, \cdot \rangle_1$ in $\langle \cdot, \cdot \rangle_2$. *Izomorfizem vektorskih prostorov s skalarnim produktom* je preslikava $A \colon V_1 \to V_2$, za katero velja:

i) A je izomorfizem vektorskih prostorov

ii) $\forall x, y \in V_1 \colon \langle Ax, Ay \rangle_2 = \langle x, y \rangle_1$

Izrek 7.2.10. Naj bo V vektorski prostor s skalarnim produktom in dimenzijo n. Potem je V izomorfen $\mathbb{F}^n$ z običajnim skalarnim produktom.

Dokaz. Vzamemo izomorfizem, ki ortonormirani bazi priredi standardno bazo. □

Definicija 7.2.11. Naj bo V vektorski prostor s skalarnim produktom in X ter Y neprazni množici v V. Pravimo, da sta množici X in Y *ortogonalni*, če velja

$$\forall x \in X, \forall y \in Y \colon \langle x, y \rangle = 0.$$

Pišemo $X \perp Y$.

Trditev 7.2.12. Če je $X \perp Y$, je tudi $\operatorname{Lin} X \perp \operatorname{Lin} Y$.

Dokaz. The proof is obvious and need not be mentioned. □

Definicija 7.2.13. Naj bo V vektorski prostor s skalarnim produktom in $V_1, V_2, \ldots, V_k$ podprostori v V. Vsota

$$V_1 + V_2 + \cdots + V_k$$

je *pravokotna vsota*, če za vse $i \neq j$ velja $V_i \perp V_j$.

Trditev 7.2.14. Vsaka pravokotna vsota je direktna vsota.

Dokaz. The proof is obvious and need not be mentioned. □

Definicija 7.2.15. Naj bo V vektorski prostor s skalarnim produktom in X neprazna podmnožica v V. Množici

$$X^\perp = \{v \in V \mid \forall x \in X \colon \langle v, x \rangle = 0\}$$

pravimo *ortogonalni komplement* množice X v V.

Trditev 7.2.16. Ob zgornjih oznakah je $X^\perp$ vedno podprostor v V.

Dokaz. The proof is obvious and need not be mentioned. □

Trditev 7.2.17. Naj bo V vektorski prostor s skalarnim produktom in $\{v_1, \ldots, v_n\}$ njegova ortonormirana baza. Naj bo

$$V_1 = \operatorname{Lin}\{v_1, \ldots, v_k\} \quad \text{in} \quad V_2 = \operatorname{Lin}\{v_{k+1}, \ldots, v_n\}.$$

Potem je $V = V_1 \oplus V_2$, $V_1^\perp = V_2$ in $V_2^\perp = V_1$.

Dokaz. The proof is obvious and need not be mentioned. □

Izrek 7.2.18. Naj bo V vektorski prostor s skalarnimi produktom in U podprostor v V. Potem velja

i) $V = U \oplus U^{\perp}$

ii) $\left(U^{\perp}\right)^{\perp} = U$

Dokaz. Za U izberemo ortonormirano bazo. To bazo lahko razširimo do ortonormirane baze V in uporabimo trditev 7.2.17. □

7.3 Pravokotne projekcije

Definicija 7.3.1. Projektorju $P\colon V \to V$ na U vzdolž $U^\perp$ pravimo *pravokotni projektor* na podprostor U.

Opomba 7.3.1.1. Naj bo P pravokoten projektor na U. Naj bo $\{u_1, \ldots, u_m\}$ ortonormirana baza U. Potem je

$$Px = \sum_{i=1}^{m} \langle x, u_i \rangle \, u_i.$$

Izrek 7.3.2. Če je P pravokotni projektor na podprostor U vektorskega prostora V in $v \in V$, potem je Pv tisti vektor v U, ki je najbližji vektorju v.

Dokaz. Naj bosta $v \in V$ in $u \in U$ vektorja. Potem je po Pitagorovem izreku

$$\|v - u\|^2 = \|v - Pv + Pv - u\|^2 = \|v - Pv\|^2 + \|Pv - u\|^2 . \qquad \square$$

7.4 Adjungirani prostor

Izrek 7.4.1 (Riesz)**.** Naj bo $\varphi_z \colon V \to \mathbb{F}$ za $z \in V$ linearen funkcional, za katerega je

$$\varphi_z(v) = \langle v, z \rangle .$$

Naj bo $\Phi \colon V \to V^*$ preslikava, za katero je $\Phi(z) = \varphi_z$.[3] Preslikava Φ je bijekcija prostorov V in V^*.

Dokaz. Če je $\Phi(z) = \Phi(w)$, dobimo $\langle v, z - w \rangle = 0$ za vse $v \in V$. Če vstavimo $v = z - w$, dobimo $z = w$, zato je Φ injektivna. Vidimo še, da je

$$\varphi(v) = \left\langle v, \sum_{i=1}^{n} \overline{\varphi(e_i)} \cdot e_i \right\rangle ,$$

kjer je $\{e_1, \ldots, e_n\}$ ortonormirana baza V. □

Definicija 7.4.2. Naj bosta U in V končnorazsežna vektorska prostora s skalarnima produktoma $\langle \cdot, \cdot \rangle_U$ in $\langle \cdot, \cdot \rangle_V$ ter naj bo $A \colon U \to V$ linearna preslikava. Za vektor $v \in V$ naj bo $\varphi \colon U \to \mathbb{F}$ preslikava, za katero je $\varphi(u) = \langle Au, v \rangle_V$. Po Rieszovem izreku obstaja tak vektor $x \in U$, da je

$$\langle Au, v \rangle_V = \langle u, x \rangle_U .$$

Preslikavi $A^* \colon V \to U$, za katero je pri zgornjih oznakah $A^* v = x$, pravimo *adjungirana preslikava*.

Trditev 7.4.3. A^* je linearna.

Dokaz. The proof is obvious and need not be mentioned. □

Trditev 7.4.4. Naj bodo U, V in W vektorski prostori s skalarnim produktom.

i) Če $A, B \colon U \to V$, potem $(A + B)^* = A^* + B^*$.

ii) Če $A \colon U \to V$ in $\alpha \in \mathbb{F}$, potem $(\alpha A)^* = \overline{\alpha} \cdot A^*$.

iii) Če $A \colon U \to V$, potem $(A^*)^* = A$.

iv) Naj bo $I \colon U \to U$. Potem je $I^* = I$.

v) Recimo, da $A \colon U \to V$ in $B \colon V \to W$. Potem je $(BA)^* = A^* B^*$.

Dokaz. Dokažimo točko v). Za $w \in W$ in $u \in U$ velja

$$\begin{aligned} \langle u, (BA)^* w \rangle_U &= \langle BAu, w \rangle_W \\ &= \langle Au, B^* w \rangle_V \\ &= \langle u, A^* B^* w \rangle_U . \end{aligned}$$

□

Izrek 7.4.5. Naj bo $A \colon U \to V$ homomorfizem vektorskih prostorov s skalarnim produktom. Naj bosta $A^* \colon V \to U$ in $A^d \colon V^* \to U^*$ njena adjungirana in dualna preslikava. Naj bosta $\Phi_U \colon U \to U^*$ in $\Phi_V \colon V \to V^*$ poševna izomorfizma iz Rieszovega izreka. Potem je

$$\Phi_U \circ A^* = A^d \circ \Phi_V .$$

[3] Ta preslikava je *poševno linearna* – aditivna in poševno homogena.

Dokaz. Naj bo $v \in V$. Potem je

$$(\Phi_U \circ A^*)\, v = \Phi_U\left(A^* v\right) = \varphi_{A^* v}.$$

Za poljuben $u \in U$ je

$$\varphi_{A^* v} = \langle Au, v\rangle_V .$$

Po drugi strani pa je

$$\left(A^d \circ \Phi_V\right) v = A^d \circ \varphi_v = \varphi_v \circ A,$$

za poljuben $u \in U$ pa je

$$\varphi_v \circ Au = \langle Au, v\rangle . \qquad \square$$

$$\begin{array}{ccc} V & \xrightarrow{A^*} & U \\ {\scriptstyle \Phi_V}\downarrow & & \downarrow{\scriptstyle \Phi_U} \\ V^* & \xrightarrow[A^d]{} & U^* \end{array}$$

Slika 4: Izrek 7.4.5 – »diagram komutira«

Trditev 7.4.6. Če je $\{v_1, \ldots, v_n\}$ ortonormirana baza, je $\Phi\{v_1, \ldots, v_n\}$ dualna baza.

Dokaz. The proof is obvious and need not be mentioned. $\square$

Izrek 7.4.7. Naj bo $A\colon U \to V$ linearna preslikava in A^* njena adjungirana preslikava. Naj bosta $\mathcal{B}$ in $\mathcal{C}$ ortonormirani bazi prostorov U in V ter $A_{\mathcal{CB}}$ matrika preslikave A v teh bazah. Potem je

$$A^*_{\mathcal{BC}} = \overline{A_{\mathcal{CB}}}^{\top}.$$

To matriko označimo z $A^{\mathsf{H}}_{\mathcal{CB}}$.[4]

Dokaz. Naj bo $\mathcal{B} = \{u_1, \ldots, u_n\}$ in $\mathcal{C} = \{v_1, \ldots, v_n\}$. Velja

$$Au_i = \sum_{j=1}^{m} \langle Au_i, v_j\rangle_V \, v_j$$

in

$$A^* v_i = \sum_{j=1}^{m} \langle A^* v_i, u_j\rangle_U \, u_j = \sum_{j=1}^{m} \overline{\langle Au_j, v_i\rangle_V} u_j. \qquad \square$$

[4] Beremo *A hermitsko.*

7.5 Ednomorfizmi prostorov s skalarnim produktom

Izrek 7.5.1 (Schur)**.** Za $A\colon V \to V$ obstaja taka ortonormirana baza $\mathcal{BB}$, da je $A_{\mathcal{BB}}$ zgornje trikotna matrika.

Dokaz. Naj bo $\mathcal{C}$ Jordanova baza prostora V za preslikavo A. Na $\mathcal{C}$ naredimo Gram–Schmidtovo ortogonalizacijo, s tem pa očitno ohranimo ničle pod diagonalo. □

Opomba 7.5.1.1. Recimo, da se da endomorfizem $A\colon V \to V$ diagonalizirati v ortonormirani bazi. Potem je

$$AA^* = A^*A.$$

Definicija 7.5.2. Naj bo V vektorski prostor s skalarnim produktom. Endomorfizem $A\colon V \to V$ je *normalen*, če velja $AA^* = A^*A$.

Definicija 7.5.3. Matrika $A \in \mathbb{F}^{n\times n}$ je *normalna*, če je $AA^{\mathsf{H}} = A^{\mathsf{H}}A$.

Trditev 7.5.4. A je normalna preslikava natanko tedaj, ko za vse $x, y \in V$ velja

$$\langle Ax, Ay\rangle = \langle A^*x, A^*y\rangle .$$

Dokaz. Naj ob A normalna. Potem je

$$\langle Ax, Ay\rangle = \langle x, A^*Ay\rangle = \langle A^*x, A^*y\rangle .$$

Če velja zgornja enakost, pa dobimo

$$\langle A^*Ax, y\rangle = \langle Ax, Ay\rangle = \langle A^*x, A^*y\rangle = \langle AA^*x, y\rangle .$$

Sledi, da je $A^*A = AA^*$. □

Posledica 7.5.4.1. Če je A normalna, velja

i) $\|Ax\| = \|A^*x\|$.

ii) $\ker A = \ker A^*$.

Trditev 7.5.5. Naj bo $A\colon V \to V$ normalna in $v \in V$ lastni vektor A za lastno vrednost λ. Potem je v tudi lasten vektor za A^* z lastno vrednostjo $\overline{\lambda}$.

Dokaz. Opazimo, da je tudi $A-\lambda I$ normalna. Sledi, da je $\ker(A-\lambda I) = \ker(A^*-\overline{\lambda}I)$. □

Trditev 7.5.6. Naj bo $A\colon V \to V$ normalna in λ_1, λ_2 različni lastni vrednosti s pripadajočima vektorjema v_1 in v_2. Potem je $v_1 \perp v_2$.

Dokaz. Velja $Av_1 = \lambda_1 v_1$ in $Av_2 = \lambda_2 v_2$. Sledi, da je

$$\lambda_2 \langle v_1, v_2\rangle = \langle v_1, A^*v_2\rangle = \langle Av_1, v_2\rangle = \lambda_1 \langle v_1, v_2\rangle .$$ □

Trditev 7.5.7. Naj bo A endomorfizem nad V in $U \leq V$ podprostor. Potem je U invarianten za A natanko tedaj, ko je $U^\perp$ invarianten za A^*.

Dokaz. Oboje je ekvivalentno

$$0 = \langle Ax, y\rangle = \langle x, A^*y\rangle\,. \qquad \square$$

Izrek 7.5.8. Naj bo $A\colon V \to V$ normalna preslikava. Potem obstaja ortonormirana baza prostora V, sestavljena iz lastnih vektorjev preslikave A.

Dokaz. Karakteristični polinom A je nekonstanten kompleksni polinom z vsaj eno ničlo λ_1, ki je lastna vrednost A z lastnim vektrojem v_1. Potem je

$$U = \operatorname{Lin}\{v_1\}$$

invarianten za A, prav tako pa je invarianten za A^*. Sledi, da je $U^\perp$ invariatnen za A^* in A. Ker je $V = U \oplus U^\perp$ in je $A|_{U^\perp}$ prav tako normalna, lahko zaključimo z indukcijo. $\square$

7.6 Sebiadjungirani endomorfizmi, hermitske in simetrične matrike

Definicija 7.6.1. $A\colon V \to V$ je *sebiadjungirana*, če velja $A^* = A$.

Definicija 7.6.2. $A \in \mathbb{C}^{n\times n}$ je *hermitska*, če je $A^{\mathsf{H}} = A$.

Definicija 7.6.3. $A \in \mathbb{R}^{n\times n}$ je *simetrična*, če je $A^\top = A$.

Opomba 7.6.3.1. Če je A sebiadjungirana, je tudi normalna.

Trditev 7.6.4. Če je $A\colon V \to V$ sebiadjungirana, so vse lastne vrednosti realne.

Dokaz. Velja

$$\lambda v = Av = A^*v = \overline{\lambda}v.$$

□

Trditev 7.6.5. Naj bo $A\colon V \to V$ sebiadjungirana. Recimo, da za vse $v \in V$ velja

$$\langle Av, v\rangle = 0.$$

Potem je $A = 0$.

Dokaz. Naj bosta $x, y \in V$ poljubna. Potem je

$$0 = \langle A(x+y), x+y\rangle = \langle Ax, y\rangle + \langle Ay, x\rangle = \langle Ax, y\rangle + \langle y, Ax\rangle\,.$$

S substitucijo $y \to Ax$ dobimo $Ax = 0$. □

Trditev 7.6.6. Naj bo $A\colon V \to V$ linearna preslikava. Potem obstajata enolično določeni sebiadjungirani linearni preslikavi $B, C\colon V \to V$, za kateri je

$$A = B + iC.$$

Dokaz. Zgornjo enakost adjungiramo. Dobimo

$$B = \frac{A + A^*}{2} \quad \text{in} \quad C = \frac{A - A^*}{2i},$$

ki sta očitno sebiadjungirani. □

Trditev 7.6.7. Preslikava $A\colon V \to V$ je sebiadjungirana natanko tedaj, ko za vsak $v \in V$ velja

$$\langle Av, v\rangle \in \mathbb{R}.$$

Dokaz. Oboje je ekvivalentno

$$\langle Av, v\rangle = \langle v, A^*v\rangle = \langle v, Av\rangle = \overline{\langle Av, v\rangle}.$$

□

7.7 Unitarni endomorfizmi, unitarne in ortogonalne matrike

Definicija 7.7.1. Naj bo $A\colon V \to V$. Pravimo, da je A *unitarna*, če velja

$$AA^* = A^*A = I.$$

Definicija 7.7.2. Matrika $A \in \mathbb{C}^{n\times n}$ je *unitarna*, če velja

$$A^{\mathsf{H}}A = AA^{\mathsf{H}} = I.$$

Definicija 7.7.3. Matrika $A \in \mathbb{R}^{n\times n}$ je *ortogonalna*, če velja

$$A^\top A = AA^\top = I.$$

Opomba 7.7.3.1. $\mathrm{GL}(V) = \{A\colon V \to V \mid A \text{ je obrnljiva}\}$ je grupa za kompozitum. Pravimo ji *splošna linearna grupa avtomorfizmov prostora* V. Podobno je tudi

$$\mathrm{GL}_n(\mathbb{F}) = \left\{A \in \mathbb{F}^{n\times n} \;\middle|\; A \text{ je obrnljiva}\right\}$$

grupa. Velja, da je

$$\mathrm{U}(V) = \{A\colon V \to V \mid A \text{ je unitarna}\}$$

podgrupa v $\mathrm{GL}(V)$.

Trditev 7.7.4. Za $A\colon V \to V$ so ekvivalentne naslednje trditve:

1. A je unitarna
2. Za vse $x, y \in V$ velja $\langle Ax, Ay\rangle = \langle x, y\rangle$
3. A je *izometrija*: Za vse $x \in V$ je $\|Ax\| = \|x\|$.

Dokaz. Če je A unitarna, je za vse $x, y \in V$

$$\langle Ax, Ay\rangle = \langle x, A^*Ay\rangle = \langle x, y\rangle .$$

Iz te enakosti očitno sledi, da je A izometrija. Če je A izometrija, naj bo $B = A^*A - I$. Potem je

$$B^* = (A^*A - I)^* = A^*A - I = B,$$

zato je B sebiadjungirana. Velja pa

$$\langle Bx, x\rangle = \langle A^*Ax, x\rangle - \langle x, x\rangle = \|Ax\|^2 - \|x\|^2 = 0,$$

zato je po trditvi 7.6.5 $B = 0$. □

Trditev 7.7.5. Naj bo $A\colon V \to V$ in $\{v_1, \ldots, v_n\}$ ortonormirana baza prostora V. Potem je

$$\{Av_1, \ldots, Av_n\}$$

ortonormirana baza prostora V natanko tedaj, ko je A unitarna.

Dokaz. Če je A unitarna, je

$$\langle Av_i, Av_j \rangle = \begin{cases} 0, & i \neq j \\ 1, & i = j \end{cases}$$

Naj bo $\{Av_1, \ldots, Av_n\}$ ortonormirana baza in $v \in V$ poljuben. Naj bo

$$v = \sum_{i=1}^{n} \alpha_i v_i.$$

Sledi

$$\|v\|^2 = \langle v, v \rangle = \sum_{i=1}^{n} \alpha_i \overline{\alpha_i}$$

in

$$\|Av\|^2 = \langle Av, Av \rangle = \left\langle \sum_{i=1}^{n} \alpha_i Av_i, \sum_{i=1}^{n} \alpha_i Av_i \right\rangle = \sum_{i=1}^{n} \alpha_i \overline{\alpha_i}. \qquad \square$$

Izrek 7.7.6. Naj bo $A \colon V \to V$ unitarna. Potem vse lastne vrednosti A ležijo na enotski krožnici.

Dokaz. Za lastno vrednost λ z lastnim vektorjem v velja

$$\|v\| = \|Av\| = \|\lambda v\| = |\lambda| \cdot \|v\|. \qquad \square$$

Trditev 7.7.7. Matrika $A \in \mathbb{C}^{n \times n}$ je unitarna natanko tedaj, ko njeni stolpci tvorijo ortonormirano bazo prostora $\mathbb{C}^n$ z običajnim skalarnim produktom.

Dokaz. The proof is obvious and need not be mentioned. $\square$

Definicija 7.7.8. Naj bosta A in B $n \times n$ matriki. Pravimo, da sta A in B *unitarno podobni*, če obstaja taka unitarna matrika P, da je[5]

$$A = PBP^{\mathsf{H}}.$$

Opomba 7.7.8.1. Relacija unitarne podobnosti je ekvivalenčna.

Posledica 7.7.8.2. Vsaka normalna matrika je unitarno podobna diagonalni matriki.

[5] Matriko B lahko dobimo tako, da naredimo prehod na ortonormirano bazo.

7.8 Pozitivno definitni endomorfimi in matrike

Definicija 7.8.1. Naj bo $A\colon V \to V$ sebiadjungiran endomorfizem. Pravimo, da je A *pozitivno definiten*, če za vsak neničelni $v \in V$ velja

$$\langle Av, v\rangle > 0.$$

Opomba 7.8.1.1. Lahko definiramo tudi *pozitivno semidefiniten* endomorfizem, za katerega za vsak $v \in V$ velja $\langle Av, v\rangle \geq 0$. Podobni definiciji uvedemo za matrike.

Izrek 7.8.2. Naj bo $A\colon V \to V$ sebiadjungiran endomorfizem. Potem je A pozitivno definiten natanko tedaj, ko so vse lastne vrednosti preslikave A pozitivne.

Dokaz. Če je A pozitivno definiten, je

$$0 < \langle \lambda v, v\rangle = \lambda \cdot \|v\|^2$$

za lastno vrednost λ z lastnim vektorjem v.

Recimo, da so vse lastne vrednosti preslikave A pozitivne. Naj bo $\{v_1, \ldots, v_n\}$ ortonormirana baza prostora V, sestavljena iz lastnih vektorjev A. Sledi, da je

$$\langle Av, v\rangle = \left\langle \sum_{i=1}^{n} \alpha_i \lambda_i v_i, \sum_{i=1}^{n} \alpha_i v_i \right\rangle = \sum_{i=1}^{n} \alpha_i \overline{\alpha_i} \cdot \lambda_i \cdot \langle v_i, v_i\rangle > 0. \qquad \square$$

Trditev 7.8.3. Naj bo $A \in \mathbb{F}^{n\times n}$ pozitivno definitna matrika. Potem veljajo naslednje trditve:

1. Vsi diagonalni elementi A so pozitivni.
2. $\det A > 0$.
3. Vse matrike A_k so pozitivno definitne, kjer A_k označuje $k \times k$ matriko v prvih k vrsticah in k stolpcih matrike A.

Dokaz.

1. Naj bo $\{e_i, \ldots, e_n\}$ standardna baza $\mathbb{F}^n$. Vemo, da je $\langle Ae_i, e_i\rangle > 0$, kar smo želeli.
2. Vietova formula.
3. Vidimo, da je $A_k^{\mathsf{H}} = A_k$. Naj bo $v \in \mathbb{F}^k \setminus \{0\}$. Dokazujemo, da je $\langle A_k v, v\rangle > 0$, kar je ekvivalentno $\langle A\widetilde{v}, \widetilde{v}\rangle > 0$, kjer je $\widetilde{v} \in \mathbb{F}^n$ vektor, ki ga dobimo, če vektorju v dodamo $n - k$ ničel. $\square$

Trditev 7.8.4. Naj bo A hermitska. Potem je A pozitivno definitna natanko tedaj, ko je $\det A_k > 0$ za vsak k.

Izrek 7.8.5. Naj bo A hermitska matrika. Potem je A pozitivno definitna natanko tedaj, ko predznaki koeficientov njenega karakterističnega polinoma alternirajo.

Dokaz. Predznaki koeficientov karakterističnega polinoma pozitivno definitnih matrik očitno alternirajo po Vietovih formulah. Recimo, da predznaki karakterističnega polinoma matrike A alternirajo. Naj bo $\alpha \leq 0$ poljubno število. Potem je $p_A(\alpha) > 0$, zato so vse ničle pozitivne. $\square$

Trditev 7.8.6. Naj bo $A\colon V \to V$ hermitska. Potem je preslikava $F(u,v) = \langle Au, v\rangle$ skalarni produkt na V natanko tedaj, ko je A pozitivno definitna.

Dokaz. The proof is obvious and need not be mentioned. □

8 Kvadratne forme

»Hotelo je biti roža, ratalo je pa kot štruca kruha z luknjo."

—prof. dr. Primož Moravec

8.1 Definicija

Definicija 8.1.1. Naj bo $\mathbb{R}^n$ opremljen z običajnim skalarnim produktom in $A \in \mathbb{R}^{n\times n}$ simetrična matrika. *Kvadratna forma*, ki pripada matriki A, je preslikava $K\colon \mathbb{R}^n \to \mathbb{R}$ s predpisom

$$K(x) = \langle Ax, x\rangle .$$

Opomba 8.1.1.1. Naj bo $\{e_1, \ldots, e_n\}$ standardna baza $\mathbb{R}^n$. Potem je

$$K(x) = \sum_{\substack{i=1\\ j=1}}^{n} x_i x_j a_{i,j}.$$

Opomba 8.1.1.2. Naj bo K kvadratna forma matrike A. Obstaja ortonormirana baza prostora $\mathbb{R}^n$, sestavljena iz lastnih vektorjev A. Torej obstajata ortogonalna matrika P in diagonalna matrika D, za kateri je $A = PDP^\top$. Sledi, da je

$$K(x) = \langle Ax, x\rangle = \left\langle DP^\top x, P^\top x\right\rangle = \widetilde{K}(y),$$

kjer je $\widetilde{K}$ kvadratna forma matrike D in $y = P^\top x$. Tako dobimo

$$\widetilde{K}(y) = \sum_{i=1}^{n} \lambda_i y_i^2.$$

Opazimo še, da so elementi nove baze ortonormirani lastni vektorji A.

Definicija 8.1.2. Naj bosta A in B simetrični matriki v $\mathbb{R}^{n\times n}$. Pravimo, da sta A in B *kongruentni*, če obstaja taka obrnljiva matrika P, da je

$$B = P^\top AP.$$

Kvadratni formi F in $\widetilde{F}$ sta kongruentni, če sta pripadajoči matriki kongruentni.

Opomba 8.1.2.1. Relacija kongruentnosti je ekvivalenčna na množici simetričnih $n \times n$ matrik. Vsaka simetrična matrika je kongruentna neki diagonalni matriki, vsaka kvadratna forma pa je kongruentna neki kvadratni formi brez mešanih členov.

Izrek 8.1.3 (Sylvester)**.** Vsaka simetrična matrika je kongruentna matriki oblike

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

Pri tem sta število 1 in -1 enolično določena za vse matrike iz danega ekvivalenčnega razreda glede na relacijo kongruentnosti.

Dokaz. Naj bo A $n \times n$ simetrična matrika. Sledi, da je $A = PDP^\top$, kjer je D diagonalna matrika. Pri tem si lahko elemente D izberemo tako, da so na začetku pozitivne lastne vrednosti A, za njimi negativne, na koncu pa še 0. D lahko dalje zapišemo kot

$$D = \begin{bmatrix} \sqrt{\lambda_1} & & & & & & \\ & \ddots & & & & & \\ & & \sqrt{-\lambda_{p+1}} & & & & \\ & & & \ddots & & & \\ & & & & 1 & & \\ & & & & & \ddots & \\ & & & & & & \end{bmatrix} \cdot B \cdot \begin{bmatrix} \sqrt{\lambda_1} & & & & & & \\ & \ddots & & & & & \\ & & \sqrt{-\lambda_{p+1}} & & & & \\ & & & \ddots & & & \\ & & & & 1 & & \\ & & & & & \ddots & \\ & & & & & & \end{bmatrix}.$$

Predpostavimo, da obstajata dve različni matriki B in C zgornje oblike, ki sta kongruentni. S p, q, p' in q' označimo število 1 in -1 v posamični matriki. Predpostavimo, da je $p > p'$. Naj bo $V_1 = \operatorname{Lin}\{e_1, \ldots, e_p\}$ in $V_2 = \operatorname{Lin}\{P^{-1}e_p, \ldots, P^{-1}e_n\}$. Potem je $\dim V_1 = p$ in $\dim V_2 = n - p + 1$. Sledi, da je $\dim(V_1 \cap V_2) > 0$. Naj bo $x \in V_1 \cap V_2$ neničeln vektor. Potem je

$$\langle Bx, x\rangle = x_1^2 + \cdots + x_p^2 > 0.$$

Po drugi strani pa velja

$$\langle Bx, x\rangle = \left\langle P^\top CPx, x\right\rangle = \langle CPx, Px\rangle = \langle Cy, y\rangle = -y_p^2 - \cdots - y_n^2 \leq 0,$$

kar je očitno protislovje. Sledi, da je $p = p'$.. S primerjavo rangov dobimo še $q = q'$. □

Posledica 8.1.3.1. Vsaka kvadratna forma je kongruentna kvadratni formi oblike

$$\widetilde{K}(y) = y_1^2 + \cdots + y_p^2 - y_{p+1}^2 - \cdots - y_{p+q}^2.$$

Paru (p, q) pravimo *signatura*. Dve kvadratni formi sta kongruentni natanko tedaj, ko imata enako signaturo.

8.2 Krivulje in ploskve drugega reda

Definicija 8.2.1. *Krivulja drugega reda* je množica točk v $\mathbb{R}^2$, ki zadoščajo enačbi

$$ax^2 + 2bxy + cy^2 + dx + ey + f = 0.$$

Definicija 8.2.2. *Ploskev drugega reda* je množica točk v $\mathbb{R}^3$, ki zadoščajo enačbi

$$ax^2 + by^2 + cz^2 + 2dxy + 2eyz + 2fzx + gx + hy + iz + j = 0.$$

Opomba 8.2.2.1. V obeh primerih lahko z uporabo Sylvestrovega izreka naredimo prehod na bazo, v kateri ne bo mešanih členov, s tem pa lahko krivuljo oziroma ploskev narišemo.

Stvarno kazalo