ALGEBRA 1

kratek pregled rezultatov in definicij

Boris Lavrič

1. Končno razsežni vektorski prostori

Vektorski prostor V nad obsegom $\mathcal{O}$ je Abelova grupa $(V, +)$ skupaj s preslikavo

$$\mathcal{O} \times V \longrightarrow V, \quad (\alpha, x) \longmapsto \alpha x,$$

ki izpolnjuje pogoje

(1) $\alpha(x + y) = \alpha x + \alpha y$,

(2) $(\alpha + \beta)x = \alpha x + \beta x$,

(3) $(\alpha\beta)x = \alpha(\beta x)$,

(4) $1 \cdot x = x$

za vsak par $\alpha, \beta \in \mathcal{O}$ in vsak par $x, y \in V$.

Elemente množice V navadno imenujemo *vektorji*, elemente obsega $\mathcal{O}$ *skalarji*, preslikavo $(\alpha, x) \longmapsto \alpha x$ iz definicije pa *množenje s skalarji.*

Primer vektorskega prostora nad obsegom $\mathcal{O}$ je množica urejenih n-teric

$$\mathcal{O}^n = \{(\alpha_1, \ldots, \alpha_n) : \ \alpha_i \in \mathcal{O}, \ \ i = 1, \ldots, n\},$$

opremljena z operacijama seštevanja in množenja s skalarji, ki sta definirani po komponentah:

$$(\alpha_1, \ldots, \alpha_n) + (\beta_1, \ldots, \beta_n) = (\alpha_1 + \beta_1, \ldots, \alpha_n + \beta_n),$$
$$\alpha(\gamma_1, \ldots, \gamma_n) = (\alpha\gamma_1, \ldots, \alpha\gamma_n).$$

Naj bo V vektorski prostor nad obsegom $\mathcal{O}$ in $U \subseteq V$ podmnožica, zaprta za seštevanje in množenje s skalarji. Potem je $(U, +)$ Abelova grupa, množenje s skalarji $\mathcal{O} \times U \longrightarrow U$, podedovano iz $\mathcal{O} \times V \longrightarrow V$, pa ustreza pogojem iz definicije vektorskega prostora, torej je U (skupaj z operacijama) vektorski prostor nad $\mathcal{O}$. Pravimo mu *vektorski podprostor* (vektorskega) prostora V.

Vsak vektorski podprostor vsebuje ničelni vektor 0 in je zaprt za tvorjenje linearnih kombinacij. Presek vektorskih podprostorov danega vektorskega prostora je vektorski podprostor.

Naj bo $M \subseteq V$. Presek vseh vektorskih podprostorov prostora V, ki vsebujejo M, imenujemo *linearna ogrinjača* množice M in zaznamujemo z $Lin\, M$. Linearna ogrinjača množice M je vektorski podprostor, ki vsebuje M in je vsebovan v vsakem vektorskem podprostoru, ki vsebuje M. Linearna ogrinjača prazne množice je trivialni podprostor $\{0\}$, linearna ogrinjača neprazne množice M pa je množica vseh *linearnih kombinacij* elementov iz M, torej elementov oblike

$$\alpha_1 v_1 + \ldots + \alpha_k v_k, \qquad \alpha_i \in \mathcal{O},\, v_i \in M, \;\; i = 1, \ldots, k.$$

Podmnožici $M \subseteq V$ pravimo *ogrodje* (vektorskega prostora V), kadar je njena linearna ogrinjača enaka V, torej $Lin\, M = V$. Podmnožica M netrivialnega vektorskaga prostora V je njegovo ogrodje natanko takrat, kadar je vsak $v \in V$ linearna kombinacija vektorjev iz množice M.

Naj bosta V_1 in V_2 podprostora vektorskega prostora V. Linearna ogrinjača njune unije $Lin\,(V_1 \cup V_2)$ je vektorski podprostor

$$V_1 + V_2 = \{v_1 + v_2 :\; v_1 \in V_1, v_2 \in V_2\},$$

ki mu pravimo *vsota podprostorov* V_1 in V_2. Kadar velja $V_1 \cap V_2 = \{0\}$, je vsota $V_1 + V_2$ *prema* ali *direktna*. Za direktno vsoto podprostorov V_1 in V_2 uporabljamo zapis $V_1 \oplus V_2$.

Izrek 1.1. *Naj bosta V_1 in V_2 podprostora vektorskega prostora V. Potem je $V = V_1 \oplus V_2$ natanko takrat, kadar za vsak $x \in V$ obstajata enolično določena elementa $v_1 \in V_1$ in $v_2 \in V_2$, za katera velja $x = v_1 + v_2$.*

Vektorji $v_1, v_2, \ldots, v_k \in V$ so *linearno neodvisni*, kadar za njihove linearne kombinacije velja sklep

$$\alpha_1 v_1 + \alpha_2 v_2 + \ldots + \alpha_k v_k = 0 \implies \alpha_1 = \alpha_2 = \cdots = \alpha_k = 0,$$

in *linearno odvisni*, kadar ta sklep ne velja. Vektorji $v_1, v_2, \ldots, v_k$ so linearno odvisni natanko takrat, kadar je vsaj eden od njih linearna kombinacija drugih.

Podmnožica $M \subseteq V$ je *linearno neodvisna*, kadar vsako njeno končno podmnožico tvorijo linearno neodvisni vektorji. *Baza* vektorskega prostora V je linearno neodvisna podmnožica $B \subseteq V$, ki je hkrati ogrodje prostora V.

Izrek 1.2. *Naj bo V netrivialen vektorski prostor s končnim ogrodjem. Potem lahko iz tega ogrodja izberemo bazo prostora V. Vse baze prostora V imajo enako elementov.*

Število elementov (katerekoli) baze vektorskega prostora V s končnim ogrodjem imenujemo *razsežnost* ali *dimenzija* prostora V in zaznamujemo z $\dim V$. Dimenzija trivialnega prostora $\{0\}$ je enaka 0. Kadar ima vektorski prostor V končno ogrodje, pravimo, da je *končno razsežen* in to zaznamujemo z $\dim V < \infty$.

Vektorski prostor urejenih n-teric $\mathcal{O}^n$ je n-razsežen. Elementi

$$e_i = (\overbrace{0,\ldots,0}^{i-1},1,0,\ldots,0) \in \mathcal{O}^n, \quad i=1,\ldots,n,$$

tvorijo bazo prostora $\mathcal{O}^n$, ki jo imenujemo *standardna baza.*

Izrek 1.3. *Podmnožica vektorskega prostora V, sestavljena iz (med sabo različnih) vektorjev $v_1,\ldots v_n \in V$ je baza prostora V natanko takrat, kadar za vsak vektor $x \in V$ obstaja natanko ena taka urejena n-terica skalarjev $\alpha_1,\ldots,\alpha_n$, da velja $x=\alpha_1 v_1+\ldots+\alpha_n v_n$.*

Izrek 1.4. *Netrivialen končno razsežen vektorski prostor nad obsegom $\mathcal{O}$ je izomorfen vektorskemu prostoru $\mathcal{O}^n$, kjer je $n=\dim V$.*

Izrek 1.5. *Končno razsežna vektorska prostora nad istim obsegom sta izomorfna natanko takrat, kadar imata enako razsežnost.*

Izrek 1.6. *Naj bosta V_1 in V_2 vektorska podprostora končno razsežnega vektorskega prostora V. Potem velja*

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

V posebnem primeru $V=V_1\oplus V_2$ velja ekvivalenca

$$V=V_1\oplus V_2 \iff \dim V=\dim V_1+\dim V_2.$$

Naj bo V vektorski prostor nad obsegom $\mathcal{O}$ in U njegov podprostor. Relacija $\sim$ na V, definirana s predpisom

$$x\sim y \iff x-y\in U$$

je ekvivalenčna relacija, usklajena z operacijama vektorskega prostora V. Ekvivalenčni razred $[x]$ elementa $x\in V$ je enak

$$x+U=\{x+u:\ u\in U\}.$$

Kvocientna množica $V/\!\sim\,=\{[x]:\ x\in V\}$, opremljena z operacijama

$$[x]+[y]=[x+y], \qquad \alpha[x]=[\alpha x], \quad x,y\in V,\alpha\in\mathcal{O}$$

je vektorski prostor nad $\mathcal{O}$. Imenujemo ga *kvocientni* prostor (vektorskega prostora V po podprostoru U) in zaznamujemo z V/U.

Izrek 1.7. *Naj bo U podprostor končno razsežnega vektorskega prostora V. Potem je kvocientni prostor V/U končno razsežen in ima dimenzijo*

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

2. Linearne preslikave in matrike

Naj bosta U in V vektorska prostora nad obsegom $\mathcal{O}$. Preslikava $\mathcal{A} : V \longrightarrow U$ je *linearna* ali *homomorfizem vektorskih prostorov*, kadar izpolnjuje pogoja

(1) $\mathcal{A}(x+y) = \mathcal{A}x + \mathcal{A}y \qquad \forall x, y \in V$.

(2) $\mathcal{A}(\alpha x) = \alpha \mathcal{A}x \qquad \forall \alpha \in \mathcal{O},\ \forall x \in V$.

Pogoj (1) imenujemo *aditivnost*, pogoj (2) pa *homogenost* preslikave $\mathcal{A}$.

Jedro linearne preslikave $\mathcal{A} : V \longrightarrow U$ je množica

$$\ker \mathcal{A} = \{x \in V :\ \mathcal{A}x = 0\},$$

slika te preslikave pa njena zaloga vrednosti

$$\operatorname{im} \mathcal{A} = \{\mathcal{A}x :\ x \in V\}.$$

Jedro $\ker \mathcal{A}$ je podprostor domene V, slika $\operatorname{im} \mathcal{A}$ pa podprostor kodomene U. Linearna preslikava je injektivna natanko takrat, kadar je njeno jedro trivialno.

Izrek 2.1. *Naj bosta U in V vektorska prostora istim obsegom in $\mathcal{A} : V \longrightarrow U$ linearna preslikava. Potem je preslikava $F : V/\ker \mathcal{A} \longrightarrow \operatorname{im} \mathcal{A}$, definirana s predpisom $F([x]) = \mathcal{A}x$, $x \in V$, izomorfizem med kvocientnim prostorom $V/\ker \mathcal{A}$ in sliko $\operatorname{im} \mathcal{A}$. Kadar je preslikava $\mathcal{A}$ injektivna, sta vektorska prostora V in $\operatorname{im} \mathcal{A}$ izomorfna.*

Naj bo odslej obseg $\mathcal{O}$ komutativen. Množica vseh linearnih preslikav $\mathcal{A} : V \longrightarrow U$, opremljena z operacijama seštevanja in množenja s skalarji iz $\mathcal{O}$, definiranima po točkah, je vektorski prostor nad $\mathcal{O}$. Zaznamujemo ga z $\mathcal{L}(V, U)$.

Izrek 2.2. *Naj bosta U in V netrivialna končno razsežna vektorska prostora nad obsegom $\mathcal{O}$ z dimenzijama $m = \dim U$, $n = \dim V$. Potem je vektorski prostor $\mathcal{L}(V, U)$ linearnih preslikav $V \longrightarrow U$ izomorfen vektorskemu prostoru $m \times n$ matrik $\mathcal{O}^{m,n}$.*

Izomorfizem med $\mathcal{L}(V, U)$ in $\mathcal{O}^{m,n}$ lahko konstruiramo tako, da izberemo urejeni bazi prostorov V, U in vsaki preslikavi iz $\mathcal{L}(V, U)$ priredimo matriko glede na ti dve bazi. V posebnem primeru $V = \mathcal{O}^n$, $U = \mathcal{O}^m$ z izbranima standardnima bazama s takim izomorfizmom $\mathcal{L}(\mathcal{O}^n, \mathcal{O}^m) \longrightarrow \mathcal{O}^{m,n}$ poistovetimo oba prostora. Preslikava $A \in \mathcal{L}(\mathcal{O}^n, \mathcal{O}^m)$ je torej matrika, katere stolpci so slike standardne baze $\{f_1, \ldots, f_n\}$ prostora $\mathcal{O}^n$, $A^{(j)} = Af_j$, $j = 1, \ldots, n$.

Izrek 2.3. *Naj bosta U in V končno razsežna vektorska prostora nad istim obsegom in $\mathcal{A} \in \mathcal{L}(V, U)$. Potem jedro in sliko preslikave $\mathcal{A}$ veže formula*

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

Razsežnost slike preslikave $\mathcal{A} \in \mathcal{L}(V, U)$ med končno razsežnima vektorskima prostoroma imenujemo *rang* (preslikave) $\mathcal{A}$ in zaznamujemo z $\operatorname{rang} \mathcal{A}$, torej

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

Izrek 2.4. *Naj bosta U in V končno razsežna vektorska prostora nad istim obsegom in $\mathcal{A} \in \mathcal{L}(V, U)$. Potem je $\mathcal{A}$ je injektivna natanko takrat, kadar je $\operatorname{rang} \mathcal{A} = \dim V$, surjektivna pa natanko takrat, kadar je $\operatorname{rang} \mathcal{A} = \dim U$. Rang prelikave $\mathcal{A}$ je enak rangu matrike, ki pripada tej preslikavi (glede na katerikoli bazi).*

Izrek 2.5. *Rang matrike je enak največjemu številu njenih linearno neodvisnih stolpcev. Matrika in njena transponiranka imata enak rang. Rang matrike je enak največjemu številu njenih linearno neodvisnih vrstic.*

Izrek 2.6. *Sistem linearnih enačb $Ax = b$ je neprotisloven natanko takrat, kadar ima matrika A enak rang kot razširjena matrika $[A \,|\, b]$. Kadar je sistem $Ax = b$ neprotisloven, je množica vseh njegovih rešitev enaka $v + \ker \mathcal{A}$, kjer je v poljubna rešitev tega sistema.*

Naj bo V vektorski prostor nad obsegom $\mathcal{O}$. Linearno preslikavo iz V v $\mathcal{O}$ imenujemo *linearni funkcional*, vektorski prostor $V^* = \mathcal{L}(V, \mathcal{O})$ vseh linearnih funkcionalov na V pa *dualni prostor* prostora V. Za končno razsežen vektorski prostor V velja $\dim V^* = \dim V$.

Naj bo $\{v_1, \ldots, v_n\}$ baza n-razsežnega prostora V. Podmnožica $\{\varphi_1, \ldots, \varphi_n\} \subseteq V^*$, ki ustreza pogoju $\varphi_i(v_j) = \delta_{ij}$ za vsak $i, j \in \{1, \ldots, n\}$, je baza prostora V^*. Imenujemo jo *dualna baza* k bazi $\{v_1, \ldots, v_n\}$.

Naj bosta U in V vektorska prostora nad $\mathcal{O}$ in $\mathcal{A} \in \mathcal{L}(V, U)$. Za vsak $\varphi \in U^*$ je $\varphi\mathcal{A} \in V^*$, preslikava $\varphi \longmapsto \varphi\mathcal{A}$ iz U^* v V^* pa je linearna. Imenujemo jo *dualna preslikava* preslikave $\mathcal{A}$ in jo zaznamujemo z $\mathcal{A}^d$. Torej

$$\mathcal{A}^d(\varphi) = \varphi\mathcal{A}, \qquad \mathcal{A}^d \in \mathcal{L}(U^*, V^*).$$

Izrek 2.7. *Naj bo A matrika, ki pripada linearni preslikavi $\mathcal{A} \in \mathcal{L}(V, U)$ glede na dani urejeni bazi $\mathcal{V} \subseteq V$ in $\mathcal{U} \subseteq U$. Potem dualni preslikavi $\mathcal{A}^d \in \mathcal{L}(U^*, V^*)$ glede na dualni bazi k bazama $\mathcal{U}$ in $\mathcal{V}$ pripada matrika $A^\top$. Preslikava $\mathcal{A}$ in njena dualna preslikava $\mathcal{A}^d$ imata enak rang.*

Izrek 2.8. *Naj bo V netrivialen končno razsežen vektorski prostor nad obsegom $\mathcal{O}$ dimenzije $n = \dim V$. Potem je algebra $\mathcal{L}(V)$ endomorfizmov prostora V izomorfna algebri kvadratnih $n \times n$ matrik $\mathcal{O}^{n,n}$.*

Izrek 2.9. *Za endomorfizem $\mathcal{A}$ končno razsežnega vektorskega prostora V so ekvivalentne naslednje izjave:*

(1) *$\mathcal{A}$ je obrnljiv;*
(2) *$\mathcal{A}$ je injektiven;*
(3) *$\mathcal{A}$ je surjektiven;*
(4) $\operatorname{rang} \mathcal{A} = \dim V$.

Izrek 2.10. *Kvadratna matrika reda n je obrnljiva natanko takrat, kadar je njen rang enak n.*

Izrek 2.11. *Naj bosta U in V netrivialna končno razsežna vektorska prostora nad istim obsegom in $\mathcal{A} \in \mathcal{L}(V, U)$. Zaznamujmo z A matriko, ki pripada preslikavi $\mathcal{A}$ glede na urejeni bazi $\mathcal{V} \subset V$ in $\mathcal{U} \subset U$, z A' pa matriko, ki pripada $\mathcal{A}$ glede na urejeni bazi $\mathcal{V}' \subset V$ in $\mathcal{U}' \subset U$. Naj bo P prehodna matrika med bazama $\mathcal{V}$ in $\mathcal{V}'$, Q pa prehodna matrika med bazama $\mathcal{U}$ in $\mathcal{U}'$. Potem matriki A' in A povezuje enakost*

$$A' = Q^{-1} A P.$$

Matrika $B \in \mathcal{O}^{m,n}$ je *ekvivalentna* matriki $A \in \mathcal{O}^{m,n}$, $B \sim A$, kadar obstajata taki obrnljivi matriki $P \in \mathcal{O}^{n,n}$ in $Q \in \mathcal{O}^{m,m}$, da velja $B = Q^{-1} A P$.

Ekvivalentnost matrik je ekvivalenčna relacija v prostoru $\mathcal{O}^{m,n}$. Vse matrike, ki pripadajo dani linearni preslikavi, so med sabo ekvivalentne.

Izrek 2.12. *Naj bosta U in V netrivialna končno razsežna vektorska prostora nad obsegom $\mathcal{O}$ in $\mathcal{A} \in \mathcal{L}(V, U)$. Potem obstajata taki urejeni bazi $\mathcal{V} \subset V$ in $\mathcal{U} \subset U$, da ima matrika $A \in \mathcal{O}^{m,n}$, ki pripada preslikavi $\mathcal{A}$ glede na ti dve bazi, obliko*

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

pri čemer je število enic na diagonali enako $r = \operatorname{rang} \mathcal{A}$, vsi drugi členi pa so ničle.

Izrek 2.13. *Matriki $A, B \in \mathcal{O}^{m,n}$ sta ekvivalentni natanko takrat, kadar imata enak rang.*

Izrek 2.14. *Naj bo V netrivialen končno razsežen vektorski prostor in $\mathcal{A} \in \mathcal{L}(V)$. Zaznamujmo z A matriko, ki pripada endomorfizmu $\mathcal{A}$ glede na urejeno bazo $\mathcal{V} \subset V$, z A' pa matriko, ki pripada $\mathcal{A}$ glede na urejeno bazo $\mathcal{V}' \subset V$. Naj bo P prehodna matrika med* *bazama $\mathcal{V}$ in $\mathcal{V}'$. Potem matriki A' in A povezuje enakost*

$$A' = P^{-1}AP.$$

Matrika $B \in \mathcal{O}^{n,n}$ je *podobna* matriki $A \in \mathcal{O}^{n,n}$, kadar obstaja taka obrnljiva matrika $P \in \mathcal{O}^{n,n}$, da velja $B = P^{-1}AP$.

Podobnost matrik je ekvivalenčna relacija v prostoru $\mathcal{O}^{n,n}$. Vse matrike, ki pripadajo danemu endomorfizmu, so med sabo podobne.

Naj bo $\mathcal{A} \in \mathcal{L}(V)$ endomorfizem končno razsežnega prostora V. Pravimo, da se $\mathcal{A}$ da *diagonalizirati*, kadar obstaja taka baza prostora V, da je matrika, ki v njej pripada endomorfizmu $\mathcal{A}$, diagonalna.

Neničelni vektor $x \in V$ imenujemo *lastni vektor* endomorfizma $\mathcal{A} \in \mathcal{L}(V)$, kadar obstaja tak $\lambda \in \mathcal{O}$, da je $\mathcal{A}x = \lambda x$. Skalar λ je enolično določen z lastnim vektorjem in mu pravimo *lastna vrednost* endomorfizma $\mathcal{A}$.

Spekter endomorfizma $\mathcal{A}$ je množica vseh njegovih lastnih vrednosti. Spekter $\mathcal{A}$ zaznamujemo s $\operatorname{sp}\mathcal{A}$.

Skalar $\lambda \in \mathcal{O}$ je lastna vrednost endomorfizma $\mathcal{A}$ natanko takrat, kadar je jedro $\ker(\mathcal{A} - \lambda\mathcal{I})$ netrivialno. To jedro (kadar je netrivialno) imenujemo *lastni podprostor* endomorfizma $\mathcal{A}$, ki pripada lastni vrednosti λ.

Izrek 2.15. *Endomorfizem $\mathcal{A} \in \mathcal{L}(V)$ končno razsežnega prostora V se da diagonalizirati natanko takrat, kadar obstaja baza prostora V, sestavljena iz lastnih vektorjev endomorfizma $\mathcal{A}$.*

Izrek 2.16. *Lastni vektorji, ki pripadajo različnim lastnim vrednostim danega endomorfizma, so linearno neodvisni.*

Izrek 2.17. *Če ima endomorfizem končno razsežnega prostora toliko različnih lastnih vrednosti kot je dimenzija prostora, se ga da diagonalizirati.*

3. Determinante

Naj bosta U in V vektorska prostora nad (komutativnim) obsegom $\mathcal{O}$ in $n \in \mathbb{N}$. Preslikava $F : V^n \longrightarrow U$ je *n-linearna*, kadar so za vsako n-terico $(v_1, \ldots, v_n) \in V^n$ preslikave $F_i : V \longrightarrow U$, $i = 1, \ldots, n$, definirane s predpisom

$$F_i(x) = F(v_1, \ldots, v_{i-1}, x, v_{i+1}, \ldots, v_n), \quad x \in V,$$

linearne. Preslikava $F : V^n \longrightarrow U$ je *antisimetrična*, kadar za vsako n-terico $(v_1, \ldots, v_n) \in V^n$ velja

$$F(v_1, \ldots, v_i, \ldots, v_j \ldots, v_n) = -F(v_1, \ldots, v_j, \ldots, v_i, \ldots, v_n),$$

kjer je $1 \leq i < j \leq n$.

V posebnem primeru $V = \mathcal{O}^n$ prostor n-teric V^n poistovetimo s prostorom kvadratnih matrik $\mathcal{O}^{n,n}$, tako da vsako n-terico stolpcev $(v_1, \ldots, v_n) \in (\mathcal{O}^n)^n$ razumemo kot matriko $[v_1 \ldots v_n] \in \mathcal{O}^{n,n}$, matriko $A \in \mathcal{O}^{n,n}$ pa kot n-terico njenih stolpcev $(A^{(1)}, \ldots, A^{(n)}) \in (\mathcal{O}^n)^n$.

Izrek 3.1. *Naj bo $F : \mathcal{O}^{n,n} \longrightarrow \mathcal{O}$ n-linearen antisimetričen funkcional. Potem za vsako matriko $A = [a_{ij}]_{i,j=1}^n \in \mathcal{O}^{n,n}$ velja*

$$F(A) = (\det A) F(I),$$

kjer je $I \in \mathcal{O}^{n,n}$ enotska matrika in

$$\det A = \sum_{\pi \in S_n} s(\pi)\, a_{i_1 1} a_{i_2 2} \ldots a_{i_n n},$$

vsota pa teče po vseh permutacijah

$$\pi = \begin{pmatrix} 1 & 2 & \ldots & n \\ i_1 & i_2 & \ldots & i_n \end{pmatrix}$$

reda n.

Izrek 3.2. *Determinanta* $\det : \mathcal{O}^{n,n} \longrightarrow \mathcal{O}$, $A \longmapsto \det A$, *je n-linearen antisimetričen funkcional, ki ustreza pogoju* $\det I = 1$.

Izrek 3.3. *Determinanta matrike je enaka determinanti njene transponiranke,*

$$\det A = \det A^\top,$$

izrazimo jo lahko tudi v obliki

$$\det A = \sum_{\pi \in S_n} s(\pi)\, a_{1 j_1} a_{2 j_2} \ldots a_{n j_n},$$

kjer vsota teče po vseh permutacijah

$$\pi = \begin{pmatrix} 1 & 2 & \ldots & n \\ j_1 & j_2 & \ldots & j_n \end{pmatrix}$$

reda n.

Kvadratna matrika $A = [a_{ij}]_{i,j=1}^n$ je *zgornje trikotna* (oziroma *spodnje trikotna*), kadar ima pod diagonalo (oziroma nad diagonalo) ničle, torej $a_{ij} = 0$ za indekse $i > j$ (oziroma za indekse $i < j$). Matrika je *trikotna*, kadar je zgornje trikotna ali spodnje trikotna. Matrika je *diagonalna*, kadar je zgornje trikotna in spodnje trikotna. Kvadratna matrika A je *bločno diagonalna*, kadar ima obliko

$$A = \begin{bmatrix} A_1 & & \\ & \ddots & \\ & & A_k \end{bmatrix},$$

pri čemer so $A_1, \ldots, A_k$ kvadratne matrike (diagonalni bloki), vsi drugi členi pa so enaki 0. Pravimo tudi, da je A *direktna vsota* matrik $A_1, \ldots, A_k$ in zapišemo $A = A_1 \oplus \ldots \oplus A_k$.

Izrek 3.4. *Determinanta trikotne matrike je enaka produktu njenih diagonalnih členov. Determinanta bločno diagonalne matrike je enaka produktu determinant njenih diagonalnih blokov.*

Izrek 3.5. *Determinanta je multiplikativen funkcional,*

$$\det(AB) = (\det A)(\det B).$$

Izrek 3.6. *Podobni matriki imata enako determinanto.*

Vse matrike, ki pripadajo danemu endomorfizmu $\mathcal{A}$ (ne glede na izbor baze), imajo enako determinanto. Ta determinanta je po definiciji *determinanta endomorfizma* $\mathcal{A}$. Zaznamujemo jo z $\det \mathcal{A}$.

Naj bo A kvadratna matrika reda n in $i, j \in \{1, \ldots, n\}$. *Podmatrika* A_{ij} (matrike A) je kvadratna matrika reda $n-1$, ki jo dobimo tako, da iz matrike A odstranimo njeno i-to vrstico in njen j-ti stolpec. *Poddeterminanta* $\widetilde{a}_{ij}$ je definirana z enakostjo

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

Poddeterminante matrike A sestavljajo njeno prirejenko

$$\widetilde{A} = [\widetilde{a}_{ij}]_{i,j=1}^n.$$

Izrek 3.7. *Matrika in njena prirejenka sta povezani z enakostjo*

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

Izrek 3.8. *Kvadratna matrika A je obrnljiva natanko takrat, kadar je* $\det A \neq 0$. *Inverz je večkratnik transponirane prirejenke:*

$$A^{-1} = (\det A)^{-1}\widetilde{A}^\top.$$

Endomorfizem končno razsežnega vektorskega prostora je obrnljiv natanko takrat, kadar ima neničelno determinanto.

Izrek 3.9. *Homogeni sistem linearnih enačb $Ax = 0$ s kvadratno matriko A ima netrivialno rešitev natanko takrat, kadar je $\det A = 0$.*

Izrek 3.10. *Sistem linearnih enačb $Ax = b$ s kvadratno matriko A, ki ima neničelno determinanto, ima natanko eno rešitev $x \in \mathcal{O}^n$. Njene komponente lahko izračunamo po Cramérjevem pravilu*

$$x_j = \frac{\det A_j}{\det A}, \quad j = 1, \dots, n,$$

kjer je A_j matrika $[A^{(1)}, \dots, A^{(j-1)}, b, A^{(j+1)}, \dots, A^{(n)}]$, ki jo dobimo iz A, tako da njen j-ti stolpec $A^{(j)}$ nadomestimo s stolpcem b.

4. Zgradba endomorfizma

Naj bo A kvadratna matrika reda n, $A \in \mathcal{O}^{n,n}$. Polinom

$$\Delta_A(\lambda) = \det(A - \lambda I)$$

imenujemo *karakteristični polinom* matrike A.

Izrek 4.1. *Karakteristični polinom matrike $A \in \mathcal{O}^{n,n}$ je n-te stopnje, njegov vodilni koeficient je $(-1)^n$, njegov prosti člen pa $\det A$. Skalar $\alpha \in \mathcal{O}$ je lastna vrednost matrike A natanko takrat, kadar je ničla njenega karakterističnega polinoma, torej*

$$\alpha \in \operatorname{sp} \mathcal{A} \iff \Delta_A(\alpha) = 0.$$

Izrek 4.2. *Matrika $A \in \mathcal{O}^{n,n}$ je ničla svojega karakterističnega polinoma,*

$$\Delta_A(A) = 0.$$

Naj bo $A \in \mathcal{O}^{n,n}$. Polinom najnižje stopnje z ničlo A in vodilnim koeficientom 1 imenujemo *minimalni polinom* matrike A ter ga zaznamujemo z $m_A(\lambda)$.

Izrek 4.3. *Minimalni polinom je enolično določen z matriko.*

Izrek 4.4. *Karakteristični polinom matrike $A \in \mathcal{O}^{n,n}$ je deljiv z njenim minimalnim polinomom, $m_A(\lambda) | \Delta_A(\lambda)$. Oba imata iste ničle v obsegu $\mathcal{O}$, in sicer lastne vrednosti matrike A.*

Podobni matriki imata isti karakteristični in isti minimalni polinom, zato lahko definiramo *karakteristični polinom* $\Delta_{\mathcal{A}}(\lambda)$ in *minimalni polinom* $m_{\mathcal{A}}(\lambda)$ *endomorfizma* $\mathcal{A}$ s formulama

$$\Delta_{\mathcal{A}}(\lambda) = \Delta_A(\lambda), \qquad m_{\mathcal{A}}(\lambda) = m_A(\lambda),$$

kjer je A katerakoli matrika, ki pripada endomorfizmu $\mathcal{A}$. Velja enakost

$$\Delta_{\mathcal{A}}(\lambda) = \det(\mathcal{A} - \lambda\mathcal{I}),$$

minimalni polinom $m_{\mathcal{A}}(\lambda)$ pa je polinom najnižje stopnje z ničlo $\mathcal{A}$ in vodilnim koeficientom1.

Naj bo $\mathcal{A}$ endomorfizem vektorskega prostora V. Vektorski podprostor $U \subseteq V$ je *invarianten* za $\mathcal{A}$, kadar velja $\mathcal{A}u \in U$ za vsak $u \in U$, torej, kadar je $\mathcal{A}U \subseteq U$. Če je podprostor $U \subseteq V$ invarianten za $\mathcal{A}$, preslikavo $U \longrightarrow U$, ki slika enako kot $\mathcal{A}$, zaznamujemo z $\mathcal{A}_U$ in imenujemo *zožitev endomorfizma* na (invarianten) podprostor U. Za zožitev torej velja $\mathcal{A}_U u = \mathcal{A}u$ za vsak $u \in U$.

Izrek 4.5. *Lastni podprostori endomorfizma $\mathcal{A}$ so invariantni za $\mathcal{A}$.*

Naj bo $\mathcal{A}$ endomorfizem kompleksnega n-razsežnega vektorskega prostora V, $\lambda_1, \ldots, \lambda_k$ pa vse njegove (med sabo različne) lastne vrednosti. Za razcepa karakterističnega in mimimalnega polinoma

$$\Delta_{\mathcal{A}}(\lambda) = (\lambda - \lambda_1)^{n_1} \cdots (\lambda - \lambda_k)^{n_k}, \quad m_{\mathcal{A}}(\lambda) = (\lambda - \lambda_1)^{m_1} \cdots (\lambda - \lambda_k)^{m_k}$$

velja $1 \leq m_j \leq n_j$, $j = 1, \ldots, k$, $n_1 + \ldots + n_k = n$.

Korenski podprostor endomorfizma $\mathcal{A}$, ki pripada lastni vrednosti λ_j, je podprostor

$$W_j = \ker(\mathcal{A} - \lambda_j\mathcal{I})^{m_j}.$$

Izrek . *Vsi korenski podprostori W_j so invariantni za $\mathcal{A}$, prostor V pa je njihova direktna vsota, torej $V = W_1 \oplus \ldots \oplus W_k$.*

Zožitve endomorfizma $\mathcal{A}$ na korenske podprostore W_j, $j = 1, \ldots, k$, zaznamujmo z $\mathcal{A}_j$. Torej $\mathcal{A}_j = \mathcal{A}_{W_j}$.

Izrek 4.6. *Endomorfizem kompleksnega končno razsežnega vektorskega prostora je direktna vsota svojih zožitev na korenske podprostore,*

$$\mathcal{A} = \mathcal{A}_1 \oplus \ldots \oplus \mathcal{A}_k.$$

Zožitev $\mathcal{A}_j$ ima eno samo lastno vrednost λ_j. Za karakteristični in minimalni polinom zožitve $\mathcal{A}_j$ velja

$$\Delta_{\mathcal{A}_j}(\lambda) = (-1)^{n_j}(\lambda - \lambda_j)^{n_j}, \quad m_{\mathcal{A}_j}(\lambda) = (\lambda - \lambda_j)^{m_j}.$$

Razsežnost korenskega podprostora W_j je enaka n_j.

Jordanova celica (s skalarjem ρ na diagonali) je matrika oblike

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

z diagonalnimi členi ρ, enicami (na vzporednici) tik nad njimi in ničlami povsod drugod. Jordanova celica J_ρ reda 1 nima niti enic niti ničel in je enaka $[\rho]$.

Izrek 4.7. *Naj bo V kompleksen končno razsežen vektorski prostor in $\mathcal{B} \in \mathcal{L}(V)$ nilpotenten endomorfizem z indeksom nilpotentnosti r. Potem obstaja taka baza prostora V (Jordanova baza za $\mathcal{B}$), da je matrika $J(\mathcal{B})$, ki pripada endomorfizmu $\mathcal{B}$ v tej bazi, direktna vsota Jordanovih celic z ničlami na glavni diagonali. Pri tem so Jordanove celice urejene po velikosti glede na red od največje do najmanjše. Število teh celic je enako razsežnosti jedra $\ker \mathcal{B}$, največja med njimi (torej prva) pa ima red r.*

Izrek 4.8. *Naj bo V kompleksen končno razsežen vektorski prostor in $\mathcal{A} \in \mathcal{L}(V)$. Potem v vsakem korenskem podprostoru W_j endomorfizma $\mathcal{A}$ obstaja taka urejena baza (Jordanova baza za zožitev $\mathcal{A}_j$), da je matrika $J(\mathcal{A}_j)$, ki pripada endomorfizmu $\mathcal{A}_j$ v tej bazi, direktna vsota Jordanovih celic z lastnimi vrednostmi λ_j na glavni diagonali. Pri tem so Jordanove celice matrike $J(\mathcal{A}_j)$ urejene po velikosti glede na red od največje do najmanjše. Število teh celic je enako razsežnosti lastnega podprostora endomorfizma $\mathcal{A}$ za lastno vrednost λ_j, največja (prva) celica pa ima red m_j. V prostoru V obstaja taka urejena baza (Jordanova baza endomorfizma $\mathcal{A}$), da je (Jordanova) matrika $J(\mathcal{A})$, ki pripada endomorfizmu $\mathcal{A}$ v tej bazi, direktna vsota matrik $J(\mathcal{A}_j)$,*

$$J(\mathcal{A}) = J(\mathcal{A}_1) \oplus \ldots \oplus J(\mathcal{A}_k).$$

Jordanova matrika $J(\mathcal{A})$ je določena do vrstnega reda direktnih sumandov (blokov) $J(\mathcal{A}_j)$ natančno.

Izrek 4.9. *Kvadratna kompleksna matrika A je podobna svoji Jordanovi matriki $J(A)$. Velja $J(A) = P^{-1}AP$, pri čemer je P obrnljiva matrika, katere stolpci tvorijo Jordanovo bazo matrike A. Kvadratni kompleksni matriki istega reda sta podobni natanko takrat, kadar se njuni Jordanovi matriki razlikujeta kvečjemu v vrstnem redu blokov, ki vsebujejo vse Jordanove celice z eno lastno vrednostjo na diagonali.*

Naj bo J_ρ Jordanova celica reda s, f pa kompleksna funkcija, analitična v okolici točke ρ. Potem je vrednost funkcije f pri J_ρ dana s formulo

$$f(J_\rho) = \begin{bmatrix} f(\rho) & f'(\rho) & \frac{f''(\rho)}{2} & \cdots & \frac{f^{(s-1)}(\rho)}{(s-1)!} \\ & \ddots & \ddots & \ddots & \vdots \\ & & \ddots & \ddots & \frac{f''(\rho)}{2} \\ & & & \ddots & f'(\rho) \\ & & & & f(\rho) \end{bmatrix}.$$

Naj bo matrika $J = J_{\rho_1} \oplus \ldots \oplus J_{\rho_t}$ direktna vsota Jordanovih celic, f pa kompleksna funkcija, analitična v okolici množice $\{\rho_1, \ldots, \rho_t\}$. Potem je vrednost funkcije f pri J dana s formulo $f(J) = f(J_{\rho_1}) \oplus \ldots \oplus f(J_{\rho_t})$.

Naj bo A kvadratna kompleksna matrika, $A = PJP^{-1}$, kjer je $J = J(A)$ Jordanova kanonska forma matrike A in P ustrezna obrnljiva matrika, f pa kompleksna funkcija, analitična v okolici spektra $\{\lambda_1, \ldots, \lambda_k\}$ matrike A. Potem je vrednost funkcije $f(A)$ dana s predpisom $f(A) = Pf(J)P^{-1}$.

Izrek 4.10. *Naj bo $\mathcal{F}(A)$ algebra kompleksnih funkcij, analitičnih v okolici spektra matrike A. Potem je preslikava $f \longmapsto f(A)$ homomorfizem med algebrama $\mathcal{F}(A)$ in $\mathbb{C}^{n,n}$, ki konstantno funkcijo $1_\mathbb{C}$ preslika v enotsko matriko I, identično funkcijo $\mathrm{id}_\mathbb{C}$ pa v A, torej*

(1) $(f+g)(A) = f(A) + g(A)$;

(2) $(\alpha f)(A) = \alpha f(A)$;

(3) $(f \cdot g)(A) = f(A)g(A)$.

(4) $1_\mathbb{C}(A) = I$ *in* $\mathrm{id}_\mathbb{C}(A) = A$.

Za vsako funkcijo $f \in \mathcal{F}(A)$ je spekter slike $f(A)$ enak sliki spektra matrike A, torej $\mathrm{sp} f(A) = \{f(\lambda_1), \ldots, f(\lambda_k)\}$, *kjer je* $\mathrm{sp} A = \{\lambda_1, \ldots, \lambda_k\}$.

5. Vektorski prostori s skalarnim produktom

Naj bo $\mathbb{F}$ obseg realnih ali kompleksnih števil in V vektorski prostor nad $\mathbb{F}$. Preslikava

$$V \times V \longrightarrow \mathbb{F}, \qquad (x,y) \longmapsto \langle x, y\rangle$$

je *skalarni produkt* na V, kadar izpolnjuje pogoje

(1) $\langle x, x\rangle > 0$ za vsak $x \in V \setminus \{0\}$ in

(2) $\langle x+y, z\rangle = \langle x, z\rangle + \langle y, z\rangle$,

(3) $\langle \alpha x, y\rangle = \alpha\langle x, y\rangle$,

(4) $\langle x, y\rangle = \overline{\langle y, x\rangle}$

za vsak $x, y, z \in V$ in vsak $\alpha \in \mathbb{F}$.

Skalarni produkt je torej aditiven in homogen (zato linearen) v prvem faktorju. Skalarni produkt je aditiven in *poševno homogen* v drugem faktorju:

$\langle x, y+z\rangle = \langle x,y\rangle + \langle x,z\rangle,$

$\langle x, \alpha y\rangle = \overline{\alpha}\langle x,y\rangle$

za vsak $x,y,z \in V$ in vsak $\alpha \in \mathbb{F}$. Za vsak $x \in V$ velja

$$\langle x,x\rangle \geq 0 \text{ in } \langle x,0\rangle = \langle 0,x\rangle = 0.$$

Število

$$\|x\| = \sqrt{\langle x,x\rangle}, \quad x \in V,$$

imenujemo *norma* ali *dolžina* vektorja x. Za vsak $x \in V$ in vsak $\alpha \in \mathbb{F}$ velja enakost $\|\alpha x\| = |\alpha| \cdot \|x\|$.

Izrek 5.1. *V vektorskem prostoru V s skalarnim produktom velja ocena*

$$|\langle x,y\rangle| \leq \|x\| \cdot \|y\| \qquad \forall x,y \in V,$$

ki jo imenujemo tudi neenakost Cauchyja, Bunjakovskega in Schwarza*. V njej je dosežen enačaj natanko takrat, kadar sta vektorja x in y linearno odvisna.*

Izrek 5.2. *V vektorskem prostoru V s skalarnim produktom velja* trikotniška neenakost

$$\|x+y\| \leq \|x\| + \|y\| \qquad \forall x,y \in V.$$

Če je v njej dosežen enačaj, sta vektorja x in y linearno odvisna.

Naj bo V vektorski prostor s skalarnim produktom. Vektorja $x,y \in V$ sta med sabo *pravokotna* ali *ortogonalna*, $x \perp y$, kadar velja $\langle x,y\rangle = 0$. Podmnožica $M \subseteq V$ je *ortogonalna*, kadar za vsak par $x,y \in M$, $x \neq y$, velja $\langle x,y\rangle = 0$. Podmnožica $M \subseteq V$ je *ortonormirana*, kadar je ortogonalna in za vsak $x \in M$ velja $\|x\| = 1$.

Izrek 5.3. *Naj bo M podmnožica vektorskega prostora s skalarnim produktom. Če je M ortogonalna, je $M \setminus \{0\}$ linearno neodvisna. Če je M ortonormirana, je linearno neodvisna.*

Izrek 5.4. *Naj bodo $x_1,\dots,x_m$ linearno neodvisni elementi vektorskega prostora V s skalarnim produktom. Potem obstaja taka ortogonalna podmnožica $\{y_1,\dots,y_m\}$ prostora V, da je*

$$\mathrm{Lin}\{y_1,\dots,y_k\} = \mathrm{Lin}\{x_1,\dots,x_k\}, \quad k=1,\dots,m.$$

Vektorje y_j lahko dobimo s pomočjo rekurzivne formule

$$y_k = x_k - \sum_{j=1}^{k-1} \frac{\langle x_j, y_j\rangle}{\|y_j\|^2} y_j, \quad k=1,\dots,m.$$

Vektorji $z_j = \frac{y_j}{\|y_j\|}$ *tvorijo ortonormirano množico* $\{z_1, \ldots, z_m\}$, *ki ustreza pogoju*

$$\mathrm{Lin}\{z_1, \ldots, z_k\} = \mathrm{Lin}\{x_1, \ldots, x_k\}, \quad k = 1, \ldots, m.$$

Izrek 5.5. *Vsak netrivialen končno razsežen vektorski prostor s skalarnim produktom ima ortonormirano bazo. Vsako ortonormirano podmnožico takšnega prostora lahko dopolnimo do ortonormirane baze.*

Izrek 5.6. *Netrivialen* n*-razsežen vektorski prostor s skalarnim produktom, definiran nad obsegom* $\mathbb{F}$, *je izomorfen (kot vektorskih prostor s skalarnim produktom) vektorskemu prostoru* $\mathbb{F}^n$ *s standardnim skalarnim produktom. Končno razsežna vektorska prostora s skalarnim produktom, definirana nad istim obsegom, sta izomorfna natanko takrat, kadar imata enako dimenzijo.*

Podmnožici M in N vektorskega prostora V s skalarnim produktom sta med sabo *pravokotni* ali *ortogonalni*, $M \perp N$, kadar za vsak $x \in M$ in vsak $y \in N$ velja $x \perp y$. Vsota $V = V_1 + V_2$ podprostorov $V_1 \subseteq V$ in $V_2 \subseteq V$ je *ortogonalna*, $V = V_1 \boxplus V_2$, kadar je $V_1 \perp V_2$. *Pravokotni* ali *ortogonalni komplement* podmnožice $M \subseteq V$ je množica $M^\perp = \{x \in V : x \perp y \ \ \forall y \in M\}$.

Izrek 5.7. *Ortogonalna vsota podprostorov vektorskega prostora* V *s skalarnim produktom je direktna. Če je* V *ortogonalna vsota dveh podprostorov, je vsak od njiju ortogonalni komplement drugega, torej*

$$V = V_1 \boxplus V_2 \implies V_1^\perp = V_2,\ V_2^\perp = V_1.$$

Izrek 5.8. *Naj bo* V *končno razsežen vektorski prostor s skalarnim produktom in* U *njegov vektorski podprostor. Potem velja*

$$V = U \boxplus U^\perp \quad \text{in} \quad U^{\perp\perp} = U.$$

Če je $\{v_1, \ldots, v_k\}$ *ortonormirana baza podprostora* U, *je preslikava* $\mathcal{P} : V \longrightarrow V$, *dana s predpisom*

$$\mathcal{P}x = \sum_{j=1}^{k} \langle x, v_j \rangle v_j, \quad x \in V,$$

pravokotni projektor prostora V *na podprostor* U.

6. Hermitsko adjungirani in normalni endomorfizmi

Naj bo V vektorski prostor s skalarnim produktom in $y \in V$. Potem je preslikava $\varphi_y : V \longrightarrow \mathbb{F}$, definirana s predpisom $\varphi_y(x) = \langle x, y \rangle$, linearen funkcional, torej $\varphi_y \in V^*$.

Izrek 6.1. *Naj bo V končno razsežen vektorski prostor s skalarnim produktom. Za vsak linearen funkcional $\varphi \in V^*$ obstaja tak element $y \in V$, da je $\varphi = \varphi_y$, torej*

$$\varphi(x) = \langle x, y \rangle \quad \forall x \in V.$$

Pri tem je element y enolično določen s funkcionalom φ.

Izrek 6.2. *Naj bo V končno razsežen vektorski prostor s skalarnim produktom in $\mathcal{A}$ endomorfizem na njem, $\mathcal{A} \in \mathcal{L}(V)$. Potem obstaja tak endomorfizem $\mathcal{A}^* \in \mathcal{L}(V)$, da je*

$$\langle \mathcal{A}x, y \rangle = \langle x, \mathcal{A}^* y \rangle \quad \forall x, y \in V.$$

Preslikavo $\mathcal{A}^*$ imenujemo *hermitsko adjungirani* endomorfizem (endomorfizma $\mathcal{A}$) in je enolično določena z enakostjo iz izreka.

Izrek 6.3. *Naj bo V končno razsežen vektorski prostor s skalarnim produktom. Preslikava $\mathcal{L}(V) \longrightarrow \mathcal{L}(V)$, dana s predpisom $\mathcal{A} \longmapsto \mathcal{A}^*$, ima naslednje lastnosti:*

(1) $\mathcal{A}^{**} = \mathcal{A}$;

(2) $(\mathcal{A} + \mathcal{B})^* = \mathcal{A}^* + \mathcal{B}^*$;

(3) $(\alpha\mathcal{A})^* = \overline{\alpha}\mathcal{A}^*$;

(4) $(\mathcal{A}\mathcal{B})^* = \mathcal{B}^*\mathcal{A}^*$;

(5) $\mathcal{I}^* = \mathcal{I}, \quad 0^* = 0$.

Preslikava $\mathcal{A} \mapsto \mathcal{A}^*$ je torej involucija in poševni antiavtomorfizem algebre $\mathcal{L}(V)$.

Izrek 6.4. *Naj bo V končno razsežen vektorski prostor s skalarnim produktom in $\mathcal{A} \in \mathcal{L}(V)$. Potem je podprostor $U \subseteq V$ invarianten za $\mathcal{A}$ natanko takrat, kadar je njegov pravokotni komplement $U^\perp$ invarianten za $\mathcal{A}^*$.*

Izrek 6.5. *Naj bo V končno razsežen vektorski prostor s skalarnim produktom, $\mathcal{A} \in \mathcal{L}(V)$ in $A = [a_{ij}]_{i,j=1}^n$ matrika, ki pripada endomorfizmu $\mathcal{A}$ v (urejeni) ortonormirani bazi $\{v_1, \dots, v_n\}$. Potem je*

$$a_{ij} = \langle \mathcal{A}v_j, v_i \rangle \quad \forall i, j \in \{1, \dots, n\},$$

hermitsko adjungiranemu endomorfizmu $\mathcal{A}^*$ pa v tej bazi pripada hermitska transponiranka $A^H = \overline{A}^\top$ matrike A.

Endomorfizem $\mathcal{A}$ končno razsežnega vektorskega prostora s skalarnim roduktom je *normalen*, kadar velja $\mathcal{A}\mathcal{A}^* = \mathcal{A}^*\mathcal{A}$. Matrika $A \in \mathbb{F}^{n,n}$ je *normalna*, kadar velja $AA^H = A^H A$.

Izrek 6.6. *Naj bo V končno razsežen vektorski prostor s skalarnim produktom in $\mathcal{A} \in \mathcal{L}(V)$. Potem je $\mathcal{A}$ normalen natanko takrat, kadar velja*

$$\langle \mathcal{A}x, \mathcal{A}y \rangle = \langle \mathcal{A}^*x, \mathcal{A}^*y \rangle \quad \forall x, y \in V.$$

Izrek . *Normalen endomorfizem $\mathcal{A} \in \mathcal{L}(V)$ ima naslednje lastnosti:*

(1) $\|\mathcal{A}x\| = \|\mathcal{A}^*x\|$ *za vsak* $x \in V$*;*

(2) $\ker \mathcal{A} = \ker \mathcal{A}^*$*;*

(3) *Če je* $\mathcal{A}x = \lambda x$*, potem je* $\mathcal{A}^*x = \overline{\lambda}x$*.*

Izrek 6.7. *Lastni vektorji normalnega endomorfizma, ki pripadajo različnim lastnim vrednostim, so paroma pravokotni med sabo. Če ima normalen endomorfizem na n-razsežnem vektorskem prostoru s skalarnim produktom n različnih lastnih vrednosti, se da diagonalizirati v ortonormirani bazi.*

Izrek 6.8. *Normalni endomorfizem končno razsežnega kompleksnega vektorskega prostora s skalarnim produktom (unitarnega prostora) se da diagonalizirati v ortonormirani bazi. Normalni endomorfizem končno razsežnega realnega vektorskega prostora s skalarnim produktom (evklidskega prostora), katerega karakteristični polinom ima vse ničle realne, se da diagonalizirati v ortonormirani bazi.*

Endomorfizem $\mathcal{A}$ končno razsežnega vektorskega prostora s skalarnim produktom je *sebi adjungiran*, kadar velja $\mathcal{A}^* = \mathcal{A}$. Matrika $A \in \mathbb{F}^{n,n}$ je *hermitska*, kadar velja $A^H = A$. Realna matrika je hermitska natanko takrat, kadar je simetrična.

Izrek 6.9. *Sebi adjungirani endomorfizem končno razsežnega vektorskega prostora s skalarnim produktom se da diagonalizirati v ortonormirani bazi. Pripadajoča diagonalna matrika (z lastnimi vrednostmi endomorfizma na diagonali) je realna.*

Endomorfizem $\mathcal{A}$ končno razsežnega vektorskega prostora s skalarnim produktom je *unitaren*, kadar velja $\mathcal{A}\mathcal{A}^* = \mathcal{A}^*\mathcal{A} = \mathcal{I}$. Matrika $A \in \mathbb{F}^{n,n}$ je *unitarna*, kadar velja $AA^H = A^H A = I$. Realna unitarna matrika je *ortogonalna*, $AA^T = A^T A = I$.

Izrek 6.10. *Za endomorfizem $\mathcal{A}$ končno razsežnega vektorskega prostora V s skalarnim produktom so ekvivalentne naslednje izjave:*

(1) *$\mathcal{A}$ je unitaren,* $\mathcal{A}\mathcal{A}^* = \mathcal{A}^*\mathcal{A} = \mathcal{I}$*;*

(2) $\mathcal{A}$ *je avtomorfizem prostora s skalarnim produktom,*

$$\langle \mathcal{A}x, \mathcal{A}y \rangle = \langle x, y \rangle \quad \forall x, y \in V;$$

(3) $\mathcal{A}^*\mathcal{A} = \mathcal{I}$ *ali* $\mathcal{A}\mathcal{A}^* = \mathcal{I}$.

(4) $\mathcal{A}$ *je izometrija,* $\|\mathcal{A}x\| = \|x\|$ *za vsak* $x \in V$.

Izrek 6.11. *Unitarni endomorfizem končno razsežnega kompleksnega vektorskega prostora s skalarnim produktom se da diagonalizirati v ortonormirani bazi. Pripadajoča diagonalna matrika ima na diagonali člene (lastne vrednosti endomorfizma) z absolutno vrednostjo* 1.

Izrek 6.12. *Množica vseh unitarnih endomorfizmov končno razsežnega vektorskega prostora s skalarnim produktom je zaprta za množenje in invertiranje, torej je grupa za množenje.*

Izrek 6.13. *Endomorfizem* $\mathcal{A}$ *končno razsežnega vektorskega prostora* V *s skalarnim produktom je unitaren natanko takrat, kadar vsako (ali vsaj eno) ortonormirano bazo prostora* V *preslika v ortonormirano množico. Prehodna matrika med dvema ortonormiranima bazama prostora* V *je unitarna.*

Matrika $B \in \mathbb{C}^{n,n}$ je *unitarno podobna* matriki $A \in \mathbb{C}^{n,n}$, kadar obstaja taka unitarna matrika $U \in \mathbb{C}^{n,n}$, da je $B = U^H A U$. Unitarna podobnost je ekvivalenčna relacija na $\mathbb{C}^{n,n}$. Vse matrike, ki pripadajo danemu endomorfizmu končno razsežnega vektorskega prostora s skalarnim produktom v ortonormiranih bazah, so med sabo unitarno podobne.

Izrek 6.14. *Normalna kompleksna matrika je unitarno podobna diagonalni matriki, hermitska matrika je unitarno podobna realni diagonalni matriki, realna simetrična matrika pa je ortogonalno podobna (realni) diagonalni matriki.*

Sebi adjungirani endomorfizem $\mathcal{A} \in \mathcal{L}(V)$ je *pozitivno semidefiniten*, kadar velja

$$\langle \mathcal{A}x, x \rangle \geq 0 \quad \forall x \in V.$$

Kadar v zgornji neenakosti za vsak $x \neq 0$ velja stroga neenakost, pravimo, da je (sebi adjungirani) endomorfizem $\mathcal{A}$ *pozitivno definiten.*

Izrek 6.15. *Sebi adjungirani endomorfizem* $\mathcal{A}$ *je pozitivno semidefiniten natanko takrat, kadar so vse njegove lastne vrednosti nenegativne, pozitivno definiten pa natanko takrat, kadar so vse njegove lastne vrednosti (strogo) pozitivne.*

Izrek 6.16. *Realna simetrična matrika A je pozitivno definitna natanko takrat, kadar koeficienti a_j njenega karakterističnega polinoma*

$$\Delta_A(\lambda) = a_0 + a_1\lambda + \ldots + a_n\lambda^n$$

alternirajo po predznaku, torej kadar velja $(-1)^j a_j > 0$, $j = 0, 1, \ldots, n$.

Izrek 6.17. *Simetrična matrika $A \in \mathbb{R}^{n,n}$ je pozitivno definitna natanko takrat, kadar imajo njene vogalne podmatrike $A_k = [a_{ij}]_{i,j=1}^k$ pozitivne determinante,* $\det A_k > 0$, *$k = 1, \ldots n$.*

7. Kvadratni funkcionali

Izrek 7.1. *Za vsak bilinearen funkcional $F : \mathbb{R}^n \times \mathbb{R}^n \longrightarrow \mathbb{R}$ obstaja taka matrika $A \in \mathbb{R}^{n,n}$, da velja*

$$F(x, y) = \langle Ax, y\rangle = y^\top Ax, \quad x, y \in \mathbb{R}^n,$$

kjer $\langle\cdot,\cdot\rangle$ označuje standardni skalarni produkt v $\mathbb{R}^n$.

Kvadratni funkcional na prostoru $\mathbb{R}^n$ je funkcija $K : \mathbb{R}^n \longrightarrow \mathbb{R}$ oblike $K(x) = F(x, x)$, kjer je $F : \mathbb{R}^n \times \mathbb{R}^n \longrightarrow \mathbb{R}$ bilinearen funkcional. Za vsak kvadratni funkcional K na $\mathbb{R}^n$ obstaja taka realna simetrična matrika $A = [a_{ij}]_{i,j=1}^n$, da je $K = K_A$, kjer je

$$K_A(x) = \langle Ax, x\rangle = x^\top Ax, \quad x \in \mathbb{R}^n.$$

Kvadratni funkcional lahko izrazimo s komponentami spremenljivke x:

$$K_A(x) = \sum_{i,j=1}^n a_{ij}x_ix_j, \quad x = (x_1, \ldots, x_n)^\top \in \mathbb{R}^n.$$

Naj bo P obrnljiva realna kvadratna matrika reda n in $x = Py$, $y \in \mathbb{R}^n$, potem velja

$$K_A(x) = x^\top Ax = (Py)^\top APy = y^\top P^\top APy = K_{P^\top AP}(y),$$

torej je $K_A(x) = K_B(y)$ za realno simetrično matriko $B = P^\top AP$.

Realna kvadratna matrika B je *kongruentna* realni simetrični matriki A, kadar obstaja taka realna obrnljiva matrika P, da je $B = P^\top AP$. Kongruentnost je ekvivalenčna relacija na množici vseh realnih simetričnih matrik danega reda.

Izrek 7.2. *Realna simetrična matrika A je kongruentna diagonalni matriki*

$$B = \begin{bmatrix} I_p & & \\ & -I_q & \\ & & O_r \end{bmatrix},$$

kjer I_s označuje enotsko matriko reda s, O_r pa ničelno matriko reda reda r (v primerih $p = 0$, $q = 0$ in $r = 0$ matrik ni). Števili p in q sta enolično določeni z matriko A, njuna vsota pa je enaka rangu matrike A.

Izrek 7.3. *Vsak kvadratni funkcional spremenljivke x se da zapisati v novi spremenljivki y s samimi popolnimi kvadrati*

$$\sum_{i,j=1}^{n} a_{ij} x_i x_j = y_1^2 + \ldots + y_p^2 - y_{p+1}^2 - \ldots - y_{p+q}^2,$$

pri čemer prehod $x = Py$ med spremenljivkama omogoča obrnljiva matrika P, za katero je $B = P^\top AP$ diagonalna matrika iz prejšnjega izreka.

Krivulja drugega reda je množica rešitev $(x, y) \in \mathbb{R}^2$ enačbe

$$ax^2 + 2bxy + cy^2 + dx + ey + f = 0$$

z danimi realnimi koeficienti $a, b, \ldots, f$, ki ustrezajo pogoju $|a| + |b| + |c| > 0$. Kvadratni del enačbe je kvadratna forma, določena z neničelno (realno simetrično) matriko

$$A = \begin{bmatrix} a & b \\ b & c \end{bmatrix},$$

linearni del pa linearna forma, dana z vektorjem (d, e).

Z ortogonalno matriko Q, katere stolpca sta med sabo pravokotna normirana lastna vektorja matrike A, uvedemo novi spremenljivki u, v in diagonaliziramo A,

$$\begin{bmatrix} u \\ v \end{bmatrix} = Q^\top \begin{bmatrix} x \\ y \end{bmatrix}, \qquad Q^\top AQ = \begin{bmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{bmatrix}.$$

Enačba krivulje ima v novih spremenljivkah obliko

$$\lambda_1 u^2 + \lambda_2 v^2 + pu + qv + r = 0,$$

pri čemer sta λ_1, λ_2 (realni) lastni vrednosti A in je vsaj ena od njiju neničelna.

Naj bo najprej matrika A obrnljiva, torej $ac - b^2 = \det A = \lambda_1\lambda_2 \neq 0$. Potem s translacijo vektorja $(u, v)^\top$ za ustrezen vektor $(\alpha, \beta)^\top$ in uvedbo novih spremenljivk

$$X = u + \alpha, \;\; Y = v + \beta$$

enačbo krivulje poenostavimo do

$$\lambda_1 X^2 + \lambda_2 Y^2 + s = 0,$$

pri čemer je $\lambda_1 \neq 0$, $\lambda_2 \neq 0$. Če je $ac - b^2 > 0$, je krivulja elipsa (v posebnem krožnica), točka ali prazna množica, če pa je $ac - b^2 < 0$, je krivulja hiperbola ali par premic, ki se sekata.

Naj bo zdaj matrika A neobrnljiva, torej $ac - b^2 = \det A = \lambda_1\lambda_2 = 0$. Ena od lastnih vrednosti, je tedaj enaka 0, druga pa ne. Enačbo krivulje podobno kot v prejšnjem primeru lahko poenostavimo v

$$\lambda_1 X^2 + qY + s = 0 \quad \text{ali} \quad \lambda_2 Y^2 + pX + s = 0,$$

pri čemer je $\lambda_1 \neq 0$ v prvem primeru in $\lambda_2 \neq 0$ v drugem. V splošnem je krivulja parabola, lahko pa je sestavljena iz dveh vzporednic, ene (dvojne) premice ali pa je prazna množica.

Ploskev drugega reda je množica rešitev $(x, y, z) \in \mathbb{R}^3$ enačbe

$$a_{11}x^2 + a_{22}y^2 + a_{33}z^2 + 2a_{12}xy + 2a_{13}xz + 2a_{23}yz + ex + fy + gz + h = 0$$

z danimi realnimi koeficienti, pri čemer je realna simetrična matrika $A = [a_{ij}]_{i,j=1}^3$, ki določa kvadratni del enačbe $K_A(x, y, z)$, različna od nič.

Z ortogonalno matriko Q, katere stolpci so med sabo pravokotni normirani lastni vektorji matrike A, uvedemo nove spremenljivke in diagonaliziramo A,

$$\begin{bmatrix} u \\ v \\ w \end{bmatrix} = Q^\top \begin{bmatrix} x \\ y \\ z \end{bmatrix}, \qquad Q^\top A Q = \begin{bmatrix} \lambda_1 & & \\ & \lambda_2 & \\ & & \lambda_3 \end{bmatrix}.$$

Enačba ploskve ima v novih spremenljivkah obliko

$$\lambda_1 u^2 + \lambda_2 v^2 + \lambda_3 w^2 + pu + qv + rw + s = 0,$$

pri čemer so λ_1, λ_2 in λ_3 (realne) lastne vrednosti A in je vsaj ena od njih neničelna.

Naj bo najprej matrika A obrnljiva, torej $\det A = \lambda_1\lambda_2\lambda_3 \neq 0$. Potem z ustrezno translacijo vektorja $(u, v, w)^\top$ in uvedbo novih spremenljivk

$$X = u + \alpha, \;\; Y = v + \beta, \;\; Z = w + \gamma$$

enačbo krivulje poenostavimo do

$$\lambda_1 X^2 + \lambda_2 Y^2 + \lambda_3 Z^2 + t = 0.$$

Nato ločimo naslednji možnosti.

Če so vse lastne vrednosti matrike A istega predznaka (torej, kadar je A kongruentna I ali $-I$), lahko enačbo preoblikujemo v

$$\frac{X^2}{a^2} + \frac{Y^2}{b^2} + \frac{Z^2}{c^2} = d, \qquad d \in \{-1, 1, 0\}.$$

Ploskev je tedaj elipsoid (v posebnem sfera), točka ali prazna množica.

Če lastne vrednosti matrike A nimajo istega predznaka, lahko enačbo preoblikujemo v

$$\frac{X^2}{a^2} + \frac{Y^2}{b^2} - \frac{Z^2}{c^2} = d, \qquad d \in \{-1, 1, 0\}.$$

Ploskev je tedaj pri $d = 1$ enodelni eliptični hiperboloid, pri $d = -1$ dvodelni eliptični hiperboloid, pri $d = 0$ pa eliptični stožec.

Naj bo zdaj matrika A neobrnljiva, torej $\det A = \lambda_1\lambda_2\lambda_3 = 0$. Podobno kot v prejšnjih primerih lahko enačbo ploskve preoblikujemo v eno od naslednjih možnosti.

Če sta dve lastni vrednosti A neničelni in istega predznaka, na primer $\lambda_1\lambda_2 > 0$, potem dobimo bodisi

$$\frac{X^2}{a^2} + \frac{Y^2}{b^2} = d, \quad d \in \{-1, 1, 0\}$$

bodisi

$$\frac{X^2}{a^2} + \frac{Y^2}{b^2} = 2pZ, \qquad p \neq 0.$$

V prvem primeru je ploskev eliptični valj, premica ali prazna množica, v drugem pa eliptični paraboloid.

Če sta dve lastni vrednosti A neničelni in različnih predznakov, na primer $\lambda_1\lambda_2 < 0$, potem dobimo bodisi

$$\frac{X^2}{a^2} - \frac{Y^2}{b^2} = d, \quad d \in \{-1, 1, 0\}$$

bodisi

$$\frac{X^2}{a^2} - \frac{Y^2}{b^2} = 2pZ, \qquad p \neq 0.$$

V prvem primeru je ploskev hiperbolični valj ali ravnini, ki se sekata, v drugem pa hiperbolični paraboloid.

Če je le ena lastna vrednost A različna od nič, na primer $\lambda_1 \neq 0$, potem dobimo bodisi

$$X^2 = c, \qquad c \in \mathbb{R},$$

bodisi

$$X^2 = 2pY + 2qZ, \quad |p| + |q| > 0.$$

V prvem primeru je ploskev sestavljena iz dveh vzporednih ravnin, ene (dvojne) ravnine, lahko pa je prazna množica, v drugem primeru pa je parabolični valj.