

Teorija linearne algebre za ustni izpit — IŠRM 2023/24

ANTON LUKA ŠIJANEC

1. julij 2024

Povzetek

Povzeto po zapiskih s predavanj prof. Cimpriča.

Kazalo

I	Teorija	4
1	Prvi semester	4
1.1	Vektorji v \mathbb{R}^n	4
1.1.1	Linearna kombinacija vektorjev	4
1.1.2	Linearna neodvisnost vektorjev	5
1.1.3	Ogrodje in baza	5
1.1.4	Norma in skalarni produkt	5
1.1.5	Vektorski in mešani produkt	6
1.1.6	Premica v \mathbb{R}^n	7
1.1.7	Ravnine v \mathbb{R}^n	8
1.1.8	Regresijska premica	8
1.2	Sistemi linearnih enačb	9
1.2.1	Linearna enačba	9
1.2.2	Sistem linearnih enačb	9
1.2.3	Klasifikacija sistemov linearnih enačb	10
1.2.4	Reševanje sistema	10
1.2.5	Homogeni sistemi	11
1.2.6	Predoločeni sistemi	12
1.2.7	Poddoločeni sistemi	12
1.3	Matrike	13
1.3.1	Matrični zapis sistema linearnih enačb	13
1.3.2	Postopek iskanja splošene rešitve predločenega sistema	14
1.3.3	Najkrajša rešitev sistema	14
1.3.4	Inverzi matrik	15
1.3.5	Karakterizacija obrnljivih matrik	16
1.4	Determinante	17
1.4.1	Računanje determinant	18
1.4.2	Lastnosti determinante	18
1.4.3	Cramerjevo pravilo — eksplicitna formula za rešitve kvadratnega sistema linearnih enačb	20
1.4.4	Formula za inverz matrike	20
1.5	Algebrske strukture	21
1.5.1	Uvod	21
1.5.2	Podstrukture	23
1.5.3	Homomorfizmi	24
1.5.4	Bigrupoidi, polkolobarji, kolobarji	25
1.5.5	Podkolobarji	26
1.5.6	Homomorfizmi kolobarjev	27

1.6	Vektorski prostori	27
1.6.1	Podprostori vektorskih prostorov — vektorski podprostori	28
1.6.2	Vsota podprostorov	30
1.6.3	Baze	30
1.6.4	Obstoj baze	31
1.6.5	Dopolnitev LN množice do baze	32
1.6.6	Prehod na novo bazo	34
2	Drugi semester	35
2.1	Linearne preslikave	35
2.1.1	F^n je linearno izomorfen n -razsežnem V nad F	36
2.1.2	Matrika linearne preslikave — linearni izomorfizem $M_{m,n}(F) \rightarrow \mathcal{L}(F^n, F^m)$	36
2.1.3	Lastnosti matrik linearnih preslikav	37
2.1.4	Jedro in slika linearne preslikave	38
2.1.5	Ekvivalentnost matrik	40
2.1.6	Podobnost matrik	41
2.1.7	Zadosten pogoj za diagonalizabilnost	43
2.1.8	Algebraične in geometrijske vekčratnosti	44
2.1.9	Minimalni polinom matrike	45
2.1.10	Ničle minimalnega polinoma	45
2.1.11	Korenski podprostori	47
2.1.12	Jordanska kanonična forma	48
2.1.13	Funkcije matrik	50
2.2	Vektorski prostori s skalarnim produktom	51
2.2.1	Norma	52
2.2.2	Ortogonalne množice in ortogonalne baze	53
2.2.3	Fourierov razvoj	54
2.2.4	Parsevalova identiteta	54
2.2.5	Projekcija na podprostor	54
2.2.6	Obstoj ortogonalne baze — Gram-Schmidtova ortogonalizacija	55
2.2.7	Ortogonalni komplement	56
2.3	Adjungirana linearna preslikava	57
2.3.1	Matrika adjungirane linearne preslikave	58
2.3.2	Jedro in slika adjungirane linearne preslikave	58
2.3.3	Lastne vrednosti adjungirane linearne preslikave	59
2.3.4	Normalne matrike	60
2.3.5	Ortogonalne/unitarne matrike	60
2.3.6	Simetrične/hermitske matrike	62
2.3.7	Pozitivno (semi)definitne matrike	62
2.3.8	Singularni razcep (angl. singular value decomposition — SVD)	63
2.3.9	Pseudoinverz — Moore-Penroseov inverz	66
2.4	Kvadratne forme	70
II	Vaja za ustni izpit	71
3	Prvo vprašanje	71
3.0.1	$\det AB = \det A \det B$	72
3.1	Baze vektorskega prostora	72
3.1.1	Linearno neodvisne množice	72
3.1.2	Ogrodje	72
3.1.3	Definicija baze	72
3.1.4	Dimenzija prostora	72
3.2	Cramerovo pravilo	72
3.2.1	Trditev in dokaz	72
3.3	Obrnljive matrike	72
3.3.1	Definicija obrnljivosti	72

3.3.2	Produkt obrnljivih matrik je obrnljiva matrika	72
3.3.3	Karakterizacija obrnljivih matrik z dokazom	72
3.3.4	$\text{Ker } A = \{0\} \Leftrightarrow A$ obrnljiva	72
3.3.5	A ima desni inverz $\Rightarrow A$ obrnljiva	72
3.3.6	Formula za inverz matrike z dokazom	72
3.4	Vektorski podprostor	72
3.5	Elementarne matrike	72
3.6	Pod-/predoločeni sistem	72
3.6.1	Definicija, iskanje posplošene rešitve z izpeljavo	72
3.6.2	Moč ogrodja \geq moč LN množice	72
3.6.3	Vsak poddoločen sistem ima netrivialno rešitev	72
3.7	Regressijska premica	73
3.7.1	Definicija	73
3.8	Vektorski/mešani produkt	73
3.9	Grupe/polgrupe	73
3.9.1	Definicija in lastnosti grupe	73
3.9.2	Definicija homomorfizma	73
3.9.3	Primeri homomorfizmov z dokazi	73
3.9.4	Definicija permutacijske grupe in dokaz, da je grupa	73
3.9.5	Primeri grup	73
3.9.6	Dokaz, da so ortogonalne matrike podgrupa v grupi obrnljivih matrik	73
3.9.7	Matrika permutacije	73
3.9.8	Dokaz, da je preslikava, ki permutaciji priredi matriko, homomorfizem	73
3.10	Projekcija točke na premico/ravnino	73
3.11	$\det A = \det A^T$	73
3.12	Formula za inverz	73
3.13	Homogeni sistemi enačb	73
4	Drugo vprašanje	73
4.1	Diagonalizacija	74
4.1.1	Definicija, trditve	74
4.2	Prehod na novo bazo	74
4.2.1	Prehodna matrika in njene lastnosti	74
4.2.2	Predstavitve vektorjev in linearnih preslikav z različnimi bazami	74
4.2.3	Razvoj vektorja po eni in drugi bazi (prehod vektorja na drugo bazo)	74
4.3	Matrika linearne preslikave	74
4.4	Rang matrike	74
4.4.1	Definicija	74
4.4.2	Dokaz, da je rang število LN stolpcev	74
4.4.3	Dimenzijska formula za podprostore	74
4.5	$\text{rang } A = \text{rang } A^T$	74
4.6	Ekvivalentnost matrik	74
4.6.1	Definicija	74
4.6.2	Dokaz, da je relacija ekvivalenčna	74
4.6.3	Dokaz, da je vsaka matrika ekvivalentna matriki I_r , t. j. bločni matriki, katere zgornji levi blok je I dimenzije r , drugi trije bloki pa so ničelne matrike.	74
4.7	Jedro/slika	74
4.8	Minimalni polinom	74
4.8.1	Definicija karakterističnega in minimalnega polinoma	74
4.9	Cayley-Hamiltonov izrek	74
4.9.1	Trditev in dokaz	74
4.10	Korenski razcep	74
4.10.1	Definicija korenskih podprostorov	74
4.10.2	Presek različnih korenskih podprostorov je trivialen	74
4.10.3	Vsota korenskih podprostorov je direktna (se sklicuje na zgornjo trditev)	74
4.11	Osnovna formula rang + ničnost	74
4.11.1	Definicija	74

4.12	Funkcije matrik	74
5	Tretje vprašanje	74
5.0.1	Singularni razcep: Konstrukcija Q_1, Q_2, D in dokaz $A = Q_1 D Q_2^{-1}$	75
5.1	Ortogonalne/unitarne matrike	75
5.1.1	Definicija	75
5.1.2	Dokaz $AA^* = I$	75
5.1.3	Lastne vrednosti	75
5.1.4	Prehodna matrika iz ONB v drugo ONB ima ortogonalne stolpce (dokaz)	75
5.2	Kvadratne krivulje	75
5.3	Psevdo inverz	75
5.3.1	Definicija	75
5.4	Najkrajša posplošena rešitev sistema	75
5.4.1	Definicija, trditve in dokaz	75
5.5	Simetrične matrike	75
5.5.1	Vse o simetričnih matrikah	75
5.6	Adjungirana linearna preslikava	75
5.6.1	Definicija in celotna formulacija	75
5.6.2	Rieszov izrek	75
5.6.3	Dokaz obstoja in enoličnosti kot posledica Rieszovega izreka	75
5.6.4	Formula za matriko linearne preslikave in $\langle Au, v \rangle = v^* Au = \langle u, A^* v \rangle$	75
5.6.5	Lastne vrednosti adjungirane matrike	75
5.7	Klasifikacija skalarnih produktov	75
5.8	Normalne matrike	75
5.8.1	Definicija, lastnosti, izreki, dokazi	75
5.8.2	A normalna $\Rightarrow A$ in A^* imata isto množico lastnih vrednosti	75
5.8.3	$\text{Ker}(A - xI) = \text{Ker}(A - \bar{x}I)$ za normalno A	75
5.9	Ortogonalni komplement	75
5.9.1	Formula za ortogonalno projekcijo	75
5.10	Izrek o reprezentaciji linearnih funkcionalov	75
5.11	Pozitivno semidefinitne matrike	75
5.11.1	Definicija, lastnosti.	75
5.11.2	Dokaz, da imajo nenegativne lastne vrednosti.	75
5.11.3	Kvadratni koren pozitivno semidefinitne matrike.	75
5.11.4	$A \geq 0 \Rightarrow A$ sebiadjungirana	75
5.12	Ortogonalne in ortonormirane baze/Gram-Schmidt	75

Del I

Teorija

1 Prvi semester

1.1 Vektorji v \mathbb{R}^n

Identificiramo n -tice realnih števil, točke v \mathbb{R}^n , množice paroma enakih geometrijskih vektorjev.

Osnovne operacije z vektorji: Vsota (po komponentah) in množenje s skalarjem (po komponentah), kjer je skalar realno število.

Lastnosti teh računskih operacij: asociativnost in komutativnost vsote, aditivna enota, $-\vec{a} = (-1) \cdot \vec{a}$, leva in desna distributivnost, homogenost, multiplikativna enota.

1.1.1 Linearna kombinacija vektorjev

Definicija. Linearna kombinacija vektorjev $\vec{v}_1, \dots, \vec{v}_n$ je izraz oblike $\alpha_1 \vec{v}_1 + \dots + \alpha_n \vec{v}_n$, kjer so $\alpha_1, \dots, \alpha_n$ skalarji.

Definicija. Množico vseh linearnih kombinacij vektorjev $\vec{v}_1, \dots, \vec{v}_n$ označimo z $\mathcal{L}in \{\vec{v}_1, \dots, \vec{v}_n\}$ in ji pravimo linearna ogrinjača (angl. span). $\mathcal{L}in \{\vec{v}_1, \dots, \vec{v}_n\} = \{\alpha_1 \vec{v}_1 + \dots + \alpha_n \vec{v}_n; \forall \alpha_1, \dots, \alpha_n \in \mathbb{R}\}$

1.1.2 Linearna neodvisnost vektorjev

Ideja En vektor je linearno neodvisen, če ni enak $\vec{0}$. Dva, če ne ležita na isti premici. Trije, če ne ležijo na isti ravnini.

Definicija 1. Vektorji $\vec{v}_1, \dots, \vec{v}_n$ so linearno odvisni, če se da enega izmed njih izraziti z linearno kombinacijo preostalih $n - 1$ vektorjev. Vektorji so linearno neodvisni, če niso linearno odvisni (in obratno).

Definicija 2. Vektorji v_1, \dots, v_n so linearno neodvisni, če za vsake skalarje, ki zadoščajo $\alpha_1 v_1 + \dots + \alpha_n v_n = 0$, velja $\alpha_1 = \dots = \alpha_n = 0$. ZDB poleg $\alpha_1 = \dots = \alpha_n = 0$ ne obstajajo nobeni drugi $\alpha_1, \dots, \alpha_n$, kjer bi veljalo $\alpha_1 v_1 + \dots + \alpha_n v_n = 0$.

Definicija 3. v_1, \dots, v_n so linearno neodvisni, če se da vsak vektor na kvečjemu en način izraziti kot linearno kombinacijo v_1, \dots, v_n .

Izrek. Te tri definicije so ekvivalentne.

Dokaz. Dokazujemo ekvivalenco:

(1 \Rightarrow 2) Recimo, da so v_1, \dots, v_n linearno odvisni v smislu 1. Dokažimo, da so tedaj linearno odvisni tudi v smislu 2. Obstaja tak i , da lahko v_i izrazimo z linearno kombinacijo preostalih, torej $v_i = \alpha_1 v_1 + \dots + \alpha_{i-1} v_{i-1} + \alpha_{i+1} v_{i+1} + \dots + \alpha_n v_n$ za neke α . Sledi $0 = \alpha_1 v_1 + \dots + \alpha_{i-1} v_{i-1} + (-1) v_i + \alpha_{i+1} v_{i+1} + \dots + \alpha_n v_n$, kar pomeni, da obstaja linearna kombinacija, ki je enaka 0, toda niso vsi koeficienti 0 (že koeficient pred v_i je -1), tedaj so vektorji po definiciji 2 linearno odvisni.

(2 \Rightarrow 1) Recimo, da so v_1, \dots, v_n linearno odvisno v smislu 2. Tedaj obstajajo α , ki niso vse 0, da velja $\alpha_1 v_1 + \dots + \alpha_n v_n = 0$. Tedaj $\exists i \ni: \alpha_i \neq 0$ in velja

$$\alpha_i v_i = -\alpha_1 v_1 - \dots - \alpha_{i-1} v_{i-1} - \alpha_{i+1} v_{i+1} - \dots - \alpha_n v_n \quad / : \alpha_i$$

$$v_i = -\frac{\alpha_1}{\alpha_i} v_1 - \dots - \frac{\alpha_{i-1}}{\alpha_i} v_{i-1} - \frac{\alpha_{i+1}}{\alpha_i} v_{i+1} - \dots - \frac{\alpha_n}{\alpha_i} v_n,$$

s čimer smo v_i izrazili kot linearno kombinacijo preostalih vektorjev.

(2 \Leftrightarrow 3) Naj bodo v_1, \dots, v_n LN. Recimo, da obstaja v , ki se ga da na dva načina izraziti kot linearno kombinacijo v_1, \dots, v_n . Naj bo $v = \alpha_1 v_1 + \dots + \alpha_n v_n = \beta_1 v_1 + \dots + \beta_n v_n$. Sledi $0 = (\alpha_1 - \beta_1) v_1 + \dots + (\alpha_n - \beta_n) v_n$. Po definiciji 2 velja $\forall i: \alpha_i - \beta_i = 0 \Leftrightarrow \alpha_i = \beta_i$, torej sta načina, s katerima izrazimo v , enaka, torej lahko v izrazimo na kvečjemu en način z v_1, \dots, v_n , kar ustreza definiciji 3.

□

1.1.3 Ogrodje in baza

Definicija. Vektorji v_1, \dots, v_n so ogrodje (angl. span), če $\mathcal{L}in\{v_1, \dots, v_n\} = \mathbb{R}^n \Leftrightarrow \forall v \in \mathbb{R}^n \exists \alpha_1, \dots, \alpha_n \in \mathbb{R} \ni: v = \alpha_1 v_1 + \dots + \alpha_n v_n$.

Definicija. Vektorji v_1, \dots, v_n so baza, če so LN in ogrodje $\Leftrightarrow \forall v \in \mathbb{R}^n: \exists! \alpha_1, \dots, \alpha_n \in \mathbb{R} \ni: v = \alpha_1 v_1 + \dots + \alpha_n v_n$. ZDB vsak vektor $\in \mathbb{R}^n$ se da na natanko en način izraziti kot LK v_1, \dots, v_n .

Zgled. Primer baze je standardna baza $\mathbb{R}^n: \{(1, 0, 0, \dots, 0), (0, 1, 0, \dots, 0), (0, 0, 1, \dots, 0), (0, 0, 0, \dots, 1)\}$. To pa ni edina baza. Primer nestandardne baze v \mathbb{R}^3 je $\{(1, 1, 1), (0, 1, 1), (0, 0, 1)\}$.

1.1.4 Norma in skalarni produkt

Definicija. Norma vektorja $v = (\alpha_1, \dots, \alpha_n)$ je definirana z $\|v\| = \sqrt{\alpha_1^2 + \dots + \alpha_n^2}$. Geometrijski pomen norme je dolžina krajevnega vektorja z glavo v v .

Osnovne lastnosti norme: $\|v\| \geq 0$, $\|v\| = 0 \Rightarrow v = \vec{0}$, $\|\alpha v\| = |\alpha| \cdot \|v\|$, $\|u + v\| \leq \|u\| + \|v\|$ (trikotniška neenakost)

Definicija. Skalarni produkt $u = (\alpha_1, \dots, \alpha_n), v = (\beta_1, \dots, \beta_n)$ označimo z $\langle u, v \rangle := \alpha_1 \beta_1 + \dots + \alpha_n \beta_n$. Obstaja tudi druga oznaka in pripadajoča drugačna definicija $u \cdot v := \|u\| \cdot \|v\| \cdot \cos \varphi$, kjer je φ kot med u, v .

Trditev. Velja $\langle u, v \rangle = u \cdot v$.

Dokaz. Uporabimo kosinusni izrek, ki pravi, da v trikotniku s stranicami dolžin a, b, c velja $c^2 = a^2 + b^2 - 2ab \cos \varphi$, kjer je φ kot med b in c . Za vektorja v in u z vmesnim kotom φ torej velja

$$\|u - v\|^2 = \|u\|^2 + \|v\|^2 - 2\|u\| \cdot \|v\| \cdot \cos \varphi.$$

Obenem velja $\|u\|^2 = \alpha_1^2 + \dots + \alpha_n^2 = \langle u, u \rangle$, torej lahko zgornjo enačbo prepisemo v

$$\langle u - v, u - v \rangle = \langle u, u \rangle + \langle v, v \rangle - 2\|u\| \cdot \|v\| \cdot \cos \varphi.$$

Naj bo $w = u - v$. Iz prihodnosti si izposodimo obe linearnosti in simetričnosti.

$$\langle u - v, u - v \rangle = \langle u - v, w \rangle = \langle u, w \rangle - \langle v, w \rangle = \langle u, u - v \rangle - \langle v, u - v \rangle = \langle u, u \rangle - \langle u, v \rangle - \langle v, u \rangle + \langle v, v \rangle$$

Prišli smo do enačbe

$$\begin{aligned} \cancel{\langle u, u \rangle} - 2\langle u, v \rangle + \cancel{\langle v, v \rangle} &= \cancel{\langle u, u \rangle} + \cancel{\langle v, v \rangle} - 2\|u\| \cdot \|v\| \cdot \cos \varphi & / : -2 \\ \langle u, v \rangle &= \|u\| \cdot \|v\| \cdot \cos \varphi. \end{aligned}$$

□

Trditev. Paralelogramska identiteta. $\|u + v\|^2 + \|u - v\|^2 = 2\|u\|^2 + 2\|v\|^2$ ZDB vsota kvadratov dolžin obeh diagonal je enota vsoti kvadratov dolžin vseh štirih stranic.

Dokaz.

$$\|u + v\|^2 = \langle u + v, u + v \rangle = \langle u, u + v \rangle + \langle v, u + v \rangle = \langle u, u \rangle + \langle u, v \rangle + \langle v, u \rangle + \langle v, v \rangle$$

$$\|u - v\|^2 = \langle u - v, u - v \rangle = \langle u, u - v \rangle - \langle v, u - v \rangle = \langle u, u \rangle - \langle u, v \rangle - \langle v, u \rangle + \langle v, v \rangle$$

$$\|u + v\|^2 + \|u - v\|^2 = 2\langle u, u \rangle + 2\langle v, v \rangle = 2\|u\|^2 + 2\|v\|^2$$

□

Trditev. Cauchy-Schwarzova neenakost. $|\langle u, v \rangle| \leq \|u\| \cdot \|v\|$

Dokaz. $|\langle u, v \rangle| = \| \|u\| \cdot \|v\| \cdot \cos \varphi \| = \|u\| \cdot \|v\| \cdot |\cos \varphi| \leq \|u\| \cdot \|v\|$, kajti $|\cos \varphi| \in [0, 1]$.

□

Trditev. Trikotniška neenakost. $\|u + v\| \leq \|u\| + \|v\|$

Dokaz. Sledi iz Cauchy-Schwarzove. Velja

$$-\|u\| \cdot \|v\| \leq \langle u, v \rangle \leq \|u\| \cdot \|v\| \quad / \cdot 2$$

$$-2\|u\| \cdot \|v\| \leq 2\langle u, v \rangle \leq 2\|u\| \cdot \|v\| \quad / + \|u\|^2 + \|v\|^2$$

$$-2\|u\| \cdot \|v\| + \|u\|^2 + \|v\|^2 \leq \cancel{2\langle u, v \rangle + \|u\|^2 + \|v\|^2} \leq 2\|u\| \cdot \|v\| + \|u\|^2 + \|v\|^2$$

uporabimo kosinusni izrek na levi strani enačbe, desno pa zložimo v kvadrat:

$$\|u + v\|^2 \leq (\|u\| + \|v\|)^2 \quad / \sqrt{}$$

$$\|u + v\| \leq \|u\| + \|v\|$$

□

Trditev. Za neničelna vektorja velja $u \perp v \Leftrightarrow \langle u, v \rangle = 0$.

Dokaz. $\langle u, v \rangle = u \cdot v = \|u\| \cdot \|v\| \cdot \cos \varphi$, kar je $0 \Leftrightarrow \varphi = \pi = 90^\circ$.

□

1.1.5 Vektorski in mešani produkt

Definirana sta le za vektorje v \mathbb{R}^3 .

Definicija. Naj bo $u = (\alpha_1, \alpha_2, \alpha_3)$, $v = (\beta_1, \beta_2, \beta_3)$. $u \times v = (\alpha_2\beta_3 - \alpha_3\beta_2, \alpha_3\beta_1 - \alpha_1\beta_3, \alpha_1\beta_2 - \alpha_2\beta_1)$.

Geometrijski pomen Vektor $u \times v$ je pravokoten na u in v , njegova dolžina je $\|u\| \cdot \|v\| \cdot \sin \varphi$, kar je ploščina paralelograma, ki ga oklepata u in v .

Pravilo desnega vijaka nam je v pomoč pri določanju usmeritve vektorskega produkta. Če iztegnjen kazalec desne roke predstavlja u in iztegnjen sredinec v , iztegnjen palec kaže v smeri $u \times v$.

Trditev. Lagrangeva identiteta. $\|u \times v\|^2 + \langle u, v \rangle^2 = \|u\|^2 \cdot \|v\|^2$

Definicija. Mešani produkt vektorjev u, v, w je skalar $\langle u \times v, w \rangle$. Oznaka: $[u, v, w] = \langle u \times v, w \rangle$.

Geometrijski pomen Volumen paralelipeda, ki ga določajo u, v, w . Razlaga: $[u, v, w] = \langle u \times v, w \rangle = \|u \times v\| \cdot \|w\| \cdot \cos \varphi$; $\|u \times v\|$ je namreč ploščina osnovne ploskve, $\|w\| \cdot \cos \varphi$ pa je višina paralelipeda.

Trditev. Osnovne lastnosti vektorskega produkta so $u \times u = 0$, $u \times v = -(v \times u)$, $(\alpha u + \beta v) \times w = \alpha(u \times w) + \beta(v \times w)$ (linearnost)

Trditev. Osnovne lastnosti mešanega produkta so linearnost v vsakem faktorju, menjava dveh faktorjev spremeni predznak ($[u, v, w] = -[v, u, w]$), ciklični pomik ne spremeni vrednosti ($[u, v, w] = [v, w, u] = [w, u, v]$).

1.1.6 Premica v \mathbb{R}^n

Premico lahko podamo z

- dvema različnima točkama
- s točko r_0 in neničelnim smernim vektorjem \vec{p} . Premica je tako množica točk $\{\vec{r} = r_0 + t\vec{p}; \forall t \in \mathbb{R}\}$. Taki enačbi premice rečemo parametrična.
- s točko in normalo (v \mathbb{R}^2 ; v \mathbb{R}^n potrebujemo točko in $n - 1$ normal)

Nadaljujmo s parametričnim zapisom $\vec{r} = r_0 + t\vec{p}$. Če točke zapišemo po komponentah, dobimo parametrično enačbo premice po komponentah: $(x, y, z) = (x_0, y_0, z_0) + t(p_1, p_2, p_3)$.

$$x = x_0 + tp_1$$

$$y = y_0 + tp_2$$

$$z = z_0 + tp_3$$

Sedaj lahko iz vsake enačbe izrazimo t in dobimo normalno enačbo premice v \mathbb{R}^n :

$$t = \frac{x - x_0}{p_1} = \frac{y - y_0}{p_2} = \frac{z - z_0}{p_3}, \text{ oziroma v splošnem za premico v } \mathbb{R}^n: t = \frac{x_{10} - x_1}{p_1} = \dots = \frac{x_{n0} - x_n}{p_n}$$

Osnovne naloge s premicami so projekcija točke na premico, zrcaljenje točke čez premico in razdalja med točko in premico.

Iskanje projekcije dane točke na dano premico (skica prepuščena bralcu) r_1 projiciramo na $\vec{r} = r_0 + t\vec{p}$ in dobimo r_1 . Za r_1 vemo, da leži na premici, torej $\exists t \in \mathbb{R} \ni: r_1 = r_0 + t\vec{p}$. Poleg tega vemo, da je $r_1 - r_1$ pravokoten na premico oz. njen smerni vektor \vec{p} , torej $\langle r_1 - r_1, \vec{p} \rangle = 0$. Ti dve enačbi združimo, da dobimo t , ki ga nato vstavimo v prvo enačbo:

$$\langle r_0 + t\vec{p} - r_1, \vec{p} \rangle = 0 \implies \langle r_0, \vec{p} \rangle + t \langle \vec{p}, \vec{p} \rangle - \langle r_1, \vec{p} \rangle = 0 \implies t = \frac{\langle r_1, \vec{p} \rangle - \langle r_0, \vec{p} \rangle}{\langle \vec{p}, \vec{p} \rangle}$$

$$r_1 = r_0 + t\vec{p} = r_0 + \frac{\langle r_1, \vec{p} \rangle - \langle r_0, \vec{p} \rangle}{\langle \vec{p}, \vec{p} \rangle} \vec{p}$$

Spotoma si lahko izpišemo obrazec za oddaljenost točke od premice: $a = \left\| r_1 - r_1 \right\|$ in obrazec za zrcalno sliko (r_1'): $r_1' = \frac{r_1 + r_1}{2} \implies r_1' = 2r_1 - r_1$.

1.1.7 Ravnine v \mathbb{R}^n

Ravnino lahko podamo

- s tremi nekolinearnimi točkami
- s točko na ravnini in dvema neničelnima smernima vektorjema, ki sta linearno neodvisna. Ravnina je tako množica točk $\{\vec{r} = \vec{r}_0 + s\vec{p} + t\vec{q}; \forall s, t \in \mathbb{R}\}$. Taki enačbi ravnine rečemo parametrična.
- s točko in na ravnini in normalo (v \mathbb{R}^3 ; v \mathbb{R}^n poleg točke potrebujemo $n - 2$ normal)

Nadaljujmo s parametričnim zapisom $\vec{r} = \vec{r}_0 + s\vec{p} + t\vec{q}$. Če točke zapišemo po komponentah, dobimo parametrično enačbo ravnine po komponentah: $(x, y, z) = (x_0, y_0, z_0) + s(p_1, p_2, p_3) + t(q_1, q_2, q_3)$.

$$x = x_0 + sp_1 + tq_1$$

$$y = y_0 + sp_2 + tq_2$$

$$z = y_0 + sp_3 + tq_3$$

Normalna enačba ravnine v \mathbb{R}^3 (skica prepuščena bralcu) Vemo, da je \vec{n} (normala) pravokotna na vse vektorje v ravnini, tudi na $\vec{r} - \vec{r}_0$ za poljuben \vec{r} na ravnini. Velja torej normalna enačba ravnine: $\langle \vec{r} - \vec{r}_0, \vec{n} \rangle = 0$. Razpišimo jo po komponentah, da na koncu dobimo normalno enačbo ravnine po komponentah:

$$\langle (x, y, z) - (x_0, y_0, z_0), (n_1, n_2, n_3) \rangle = 0 = \langle (x - x_0, y - y_0, z - z_0), (n_1, n_2, n_3) \rangle$$

$$n_1(x - x_0) + n_2(y - y_0) + n_3(z - z_0) = 0 = n_1x - n_1x_0 + n_2y - n_2y_0 + n_3z - n_3z_0 = 0$$

$$n_1x + n_2y + n_3z = n_1x_0 + n_2y_0 + n_3z_0 = d$$

Iskanje pravokotne projekcije dane točke na dano ravnino (skica prepuščena bralcu) Projicirati želimo \vec{r}_1 v $r_1^{\vec{}}$ na ravnini $\vec{r} = \vec{r}_0 + s\vec{p} + t\vec{q}$. Vemo, da $r_1^{\vec{}}$ leži na ravnini, zato $\exists s, t \in \mathbb{R} \ni: r_1^{\vec{}} = \vec{r}_0 + s\vec{p} + t\vec{q}$. Poleg tega vemo, da je $r_1^{\vec{}} - \vec{r}_1$ pravokoten na ravnino oz. na \vec{p} in na \vec{q} hkrati, torej $\langle r_1^{\vec{}} - \vec{r}_1, \vec{p} \rangle = 0 = \langle r_1^{\vec{}} - \vec{r}_1, \vec{q} \rangle$. Vstavimo $r_1^{\vec{}}$ iz prve enačbe v drugo in dobimo

$$\langle \vec{r}_0 + s\vec{p} + t\vec{q} - \vec{r}_1, \vec{p} \rangle = 0 = \langle \vec{r}_0 + s\vec{p} + t\vec{q} - \vec{r}_1, \vec{q} \rangle$$

$$\langle \vec{r}_0, \vec{p} \rangle + s \langle \vec{p}, \vec{p} \rangle + t \langle \vec{q}, \vec{p} \rangle - \langle \vec{r}_1, \vec{p} \rangle = 0 = \langle \vec{r}_0, \vec{q} \rangle + s \langle \vec{p}, \vec{q} \rangle + t \langle \vec{q}, \vec{q} \rangle - \langle \vec{r}_1, \vec{q} \rangle$$

dobimo sistem dveh enačb

$$s \langle \vec{p}, \vec{p} \rangle + t \langle \vec{q}, \vec{p} \rangle = \langle \vec{r}_1 - \vec{r}_0, \vec{p} \rangle$$

$$s \langle \vec{p}, \vec{q} \rangle + t \langle \vec{q}, \vec{q} \rangle = \langle \vec{r}_1 - \vec{r}_0, \vec{q} \rangle$$

sistem rešimo in dobljena s, t vstavimo v prvo enačbo zgoraj, da dobimo $r_1^{\vec{}}$.

1.1.8 Regresijska premica

Regresijska premica je primer uporabe zgornje naloge. V ravnini je danih n točk $(x_1, y_1), \dots, (x_n, y_n)$. Iščemo tako premico $y = ax + b$, ki se najbolj prilega tem točkam. Prileganje premice točkam merimo z metodo najmanjših kvadratov: naj bo d_i navpična razdalja med (x_i, y_i) in premico $y = ax + b$, torej razdalja med točkama (x_i, y_i) in $(x_i, ax_i + b)$, kar je $|y_i - ax_i - b|$. Minimizarati želimo vsoto kvadratov navpičnih razdalj, torej izraz $d_1^2 + \dots + d_n^2 = (y_1 - ax_1 - b)^2 + \dots + (y_n - ax_n - b)^2 = \|(y_1 - ax_1 - b, \dots, y_n - ax_n - b)\|^2 = \|(y_1, \dots, y_n) - a(x_1, \dots, x_n) - b(1, \dots, 1)\|^2$.

Če je torej $\vec{r} = \vec{0} + a(x_1, \dots, x_n) + b(1, \dots, 1)$ hiperravnina v n -dimenzionalnem prostoru, bo norma, ki jo želimo minimizarati, najmanjša tedaj, ko a, b izberemo tako, da najdemo projekcijo (y_1, \dots, y_n) na to hiperravnino (skica prepuščena bralcu). Rešimo sedaj nalogo projekcije točke na ravnino:

Označimo $\vec{y} := (y_1, \dots, y_n)$, $\vec{x} := (x_1, \dots, x_n)$, $\vec{1} = (1, \dots, 1)$. Vemo, da $\vec{y} - a\vec{x} - b\vec{1} \perp \vec{x}, \vec{1}$, torej $\langle \vec{y} - a\vec{x} - b\vec{1}, \vec{x} \rangle = 0 = \langle \vec{y} - a\vec{x} - b\vec{1}, \vec{1} \rangle$ in dobimo sistem enačb

$$\langle \vec{y}, \vec{x} \rangle = a \langle \vec{x}, \vec{x} \rangle + b \langle \vec{1}, \vec{x} \rangle$$

$$\langle \vec{y}, \vec{1} \rangle = a \langle \vec{x}, \vec{1} \rangle + b \langle \vec{1}, \vec{1} \rangle.$$

V sistem sedaj vstavimo definicije točk (x_i, y_i) in ga nato delimo s številom točk, da dobimo sistem s povprečji, ki ga nato rešimo (izluščimo a, b):

$$\begin{aligned} \sum_{i=1}^n y_i x_i &= a \sum_{i=1}^n x_i^2 + b \sum_{i=1}^n x_i & / : n \\ \sum_{i=1}^n y_i &= a \sum_{i=1}^n x_i + b \sum_{i=1}^n 1 = a \sum_{i=1}^n x_i + bn & / : n \\ \bar{y}\bar{x} &= a\bar{x}^2 + b\bar{x} \\ \bar{y} &= a\bar{x} + b \implies \bar{y} - a\bar{x} = b \\ \bar{y}\bar{x} = a\bar{x}^2 + (\bar{y} - a\bar{x})\bar{x} &= a\bar{x}^2 + \bar{y} \cdot \bar{x} - a\bar{x}^2 \implies a(\bar{x}^2 - \bar{x}^2) = \bar{y}\bar{x} - \bar{y} \cdot \bar{x} \implies a = \frac{\bar{y}\bar{x} - \bar{y} \cdot \bar{x}}{\bar{x}^2 - \bar{x}^2} \end{aligned}$$

1.2 Sistemi linearnih enačb

Ta sekcija, z izjemo prve podsekcije, je precej dobesedno povzeta po profesorjevi beamer skripti.

1.2.1 Linearna enačba

Definicija. \sim je enačba oblike $a_1x_1 + \dots + a_nx_n = b$ in vsebuje koeficiente, spremenljivke in desno stran. Množica rešitev so vse n -terice realnih števil, ki zadoščajo enačbi $R = \{(x_1, \dots, x_n) \in \mathbb{R}^n; a_1x_1 + \dots + a_nx_n = b\}$. Če so vsi koeficienti 0, pravimo, da je enačba trivialna, sicer (torej čim je en koeficient neničeln) je netrivialna.

Pripomba. Za trivialno enačbo velja $R = \begin{cases} \emptyset & ; b \neq 0 \\ \mathbb{R}^n & ; b = 0 \end{cases}$. Za netrivialno enačbo pa velja $a_i \neq 0$, torej:

$$a_1x_1 + \dots + a_ix_i + \dots + a_nx_n = b$$

$$a_1x_1 + \dots + a_{i-1}x_{i-1} + a_{i+1}x_{i+1} + \dots + a_nx_n = b - a_ix_i = -a_i \left(x_i - \frac{b}{a_i} \right)$$

$$a_1x_1 + \dots + a_{i-1}x_{i-1} + a_i \left(x_i - \frac{b}{a_i} \right) + a_{i+1}x_{i+1} + \dots + a_nx_n = 0$$

$$\left\langle (a_i, \dots, a_n), \left(x_1, \dots, x_{i-1}, x_i - \frac{b}{a_i}, x_{i+1}, \dots, x_n \right) \right\rangle = 0 = \left\langle (a_i, \dots, a_n), (x_1, \dots, x_i, \dots, x_n) - \left(0, \dots, 0, \frac{b}{a_i}, 0, \dots, 0 \right) \right\rangle$$

Tu lahko označimo $\vec{n} := (a_i, \dots, a_n)$, $\vec{r} = (x_1, \dots, x_i, \dots, x_n)$, $\vec{r}_0 = \left(0, \dots, 0, \frac{b}{a_i}, 0, \dots, 0 \right)$ in dobimo $\langle \vec{n}, \vec{r} - \vec{r}_0 \rangle$, kar je normalna enačba premice v \mathbb{R}^2 , normalna enačba ravnine v \mathbb{R}^3 oziroma normalna enačba hiperravnine v \mathbb{R}^n .

1.2.2 Sistem linearnih enačb

Definicija. Sistem m linearnih enačb z n spremenljivkami je sistem enačb oblike

$$\begin{array}{ccccccc} a_{1,1}x_1 & + & \dots & + & a_{1,n}x_n & = & b_1 \\ \vdots & & & & \vdots & & \vdots \\ a_{m,1}x_1 & + & \dots & + & a_{m,n}x_n & = & b_m \end{array}$$

Dejstvo. Množica rešitev sistema je $\mathbb{R}^n \Leftrightarrow \forall i, j : a_{i,j} = b_i = 0$. Sicer je množica rešitev presek hiperravnin v \mathbb{R}^n — rešitev posameznih enačb. To vključuje tudi primer prazne množice rešitev, saj je takšna na primer presek dveh vzporednih hiperravnin.

Zgled. Množica rešitev 2×2 sistema je lahko

- cela ravnina
- premica v ravnini

- točka v ravnini
- prazna množica

Pripomba. Enako velja za množico rešitev 3×2 sistema.

Pripomba. Množica rešitev sistema 2×3 pa ne more biti točka v prostoru, lahko pa je cel prostor, ravnina v prostoru, premica v prostoru ali prazna množica.

Algebraičen pomen rešitev sistema Rešitve sistema

$$\begin{array}{ccccccc} a_{1,1}x_1 & + & \cdots & + & a_{1,n}x_n & = & b_1 \\ \vdots & & & & \vdots & & \vdots \\ a_{m,1}x_1 & + & \cdots & + & a_{m,n}x_n & = & b_m \end{array}$$

lahko zapišemo kot linearno kombinacijo stolpcev sistema in spremenljivk:

$$(b_1, \dots, b_m) = (a_{1,1}x_1 + \cdots + a_{1,n}x_n, \dots, a_{m,1}x_1 + \cdots + a_{m,n}x_n) = x_1(a_{1,1}, \dots, a_{m,1}) + \cdots + x_n(a_{1,n}, \dots, a_{m,n})$$

$$\vec{b} = x_1\vec{a}_1 + \cdots + x_n\vec{a}_n$$

1.2.3 Klasifikacija sistemov linearnih enačb

Sisteme linearnih enačb delimo glede na velikost na

- kvadratne (toliko enačb kot spremenljivk),
- poddoločene (več spremenljivk kot enačb),
- predoločene (več enačb kot spremenljivk);

glede na rešljivost na

- nerešljive (prazna množica rešitev),
- enolično rešljive (množica rešitev je singleton),
- neenolično rešljive (moč množice rešitev je več kot 1);

glede na obliko desnih strani na

- homogene (vektor desnih strani je ničeln)
- nehomogene (vektor desnih strani je neničen)

Pripomba. Če sta \vec{x} in \vec{y} dve različni rešitvi sistema, je rešitev sistema tudi $(1-t)\vec{x} + t\vec{y}$ za vsak realen t , torej ima vsak neenolično rešljiv sistem neskončno rešitev.

Pripomba. Pogosto (a nikakor ne vedno) se zgodi, da je kvadraten sistem enolično rešljiv, predoločen sistem nerešljiv, poddoločen sistem pa neenolično rešljiv.

Pripomba. Homogen sistem je vedno rešljiv, saj obstaja trivialna rešitev $\vec{0}$. Vprašanje pri homogenih sistemih je torej, kdaj je enolično in kdaj neenolično rešljiv. Dokazali bomo, da je vsak poddoločen homogen sistem linearnih enačb neenolično rešljiv.

1.2.4 Reševanje sistema

Sisteme lahko rešujemo z izločanjem spremenljivk. Iz ene enačbe izrazimo spremenljivko in jo vstavimo v druge enačbe, da izrazimo zopet nove spremenljivke, ki jih spet vstavimo v nove enačbe, iz katerih spremenljivk še nismo izražali in tako naprej, vse dokler ne pridemo do zadnjega možnega izražanja (dodatno branje prepuščeno bralcu).

Sisteme pa lahko rešujemo tudi z Gaussovo metodo. Trdimo, da se rešitev sistema ne spremeni, če na njem uporabimo naslednje elementarne vrstične transformacije:

- menjava vrstnega reda enačb,

- množenje enačbe z neničelno konstanto,
- prištevanje večkratnika ene enačbe k drugi.

Z Gaussovo metodo (dodatno branje prepuščeno bralcu) mrcvarimo razširjeno matriko sistema, dokler ne dobimo reducirane kvadratne stopničaste forme (angl. row echelon), ki izgleda takole (\times reprezentira poljubno realno številko, 0 ničlo in 1 enico):

$$\left[\begin{array}{cccccccccccccccc|c} 0 & \cdots & 0 & 1 & \times & \cdots & \times & 0 & \times & \cdots & \times & 0 & \times & \cdots & \times & 0 & \cdots & \times \\ \vdots & & \vdots & 0 & 0 & \cdots & 0 & 1 & \times & \cdots & \times & 0 & \times & \cdots & \times & 0 & \cdots & \times \\ & & & \vdots & \vdots & & \vdots & 0 & 0 & \cdots & 0 & 1 & \times & \cdots & \times & 0 & \cdots & \times \\ & & & & & & \vdots & \vdots & & & \vdots & 0 & 0 & \cdots & 0 & 1 & \cdots & \times \\ & & & & & & & & & & \vdots & \vdots & & & \vdots & 0 & \cdots & \vdots \\ \vdots & & \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots & & \vdots & \vdots & & \vdots \\ 0 & \cdots & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & \cdots & 0 & 0 & \cdots & \times \end{array} \right]$$

1.2.5 Homogeni sistemi

Definicija. Sistem je homogen, če je vektor desnih strani ničeln.

Vedno ima rešitev $\vec{0}$. Linearna kombinacija dveh rešitev homogenega sistema je spet njegova rešitev. Splošna rešitev nehomogenega sistema je vsota partikularne rešitve tega nehomogenega sistema in splošne rešitve njemu prirejenega homogenega sistema.

Pripomba. V tem razdelku nehomogen sistem pomeni nenujno homogen sistem (torej splošen sistem linearnih enačb), torej je vsak homogen sistem nehomogen.

Trditev 4. Vsak poddoločen homogen sistem ima vsaj eno netrivialno rešitev.

Dokaz. Dokaz z indukcijo po številu enačb.

Baza $a_1x_1 + \cdots + a_nx_n = 0$ za $n \geq 2$. Če je $a_n = 0$, je netrivialna rešitev $(0, \dots, 0, 1)$, sicer pa $(0, \dots, 0, -a_n, a_{n-1})$.

Korak Denimo, da velja za vse poddoločene homogene sisteme z $m - 1$ vrsticami. Vzemimo poljuben homogen sistem z $n > m$ stolpci (da je poddoločen). Če je $a_n = 0$, je netrivialna rešitev $(0, \dots, 0, 1)$, sicer pa iz ene od enačb izrazimo x_n s preostalimi spremenljivkami. Dobljen izraz vstavimo v preostalih $m - 1$ enačb z $n - 1$ spremenljivkami in dobljen sistem uredimo. Po I. P. ima slednji netrivialno rešitev $(\alpha_1, \dots, \alpha_{n-1})$. To rešitev vstavimo v izraz za x_n in dobimo α_n in s tem $(\alpha_1, \dots, \alpha_{n-1}, \alpha_n)$ kot netrivialno rešitev sistema z m vrsticami. □

Trditev. Linearna kombinacija dveh rešitev homogenega sistema je spet njegova rešitev.

Dokaz. Če sta (s_1, \dots, s_n) in (t_1, \dots, t_n) dve rešitvi homogenega sistema, velja za $\vec{s} \forall i : \langle (a_{i,1}, \dots, a_{i,n}), (s_1, \dots, s_n) \rangle = a_{i,1}s_1 + \cdots + a_{i,n}s_n = 0$ in enako za \vec{t} . Dokažimo $\forall \alpha, \beta \in \mathbb{R}, i : \langle (a_{i,1}, \dots, a_{i,n}), \alpha (s_1, \dots, s_n) + \beta (t_1, \dots, t_n) \rangle = 0$.

$$\begin{aligned} \langle (a_{i,1}, \dots, a_{i,n}), \alpha (s_1, \dots, s_n) + \beta (t_1, \dots, t_n) \rangle &= \langle \alpha (s_1, \dots, s_n) + \beta (t_1, \dots, t_n), (a_{i,1}, \dots, a_{i,n}) \rangle = \\ &= \alpha \langle \vec{s}, (a_{i,1}, \dots, a_{i,n}) \rangle + \beta \langle \vec{t}, (a_{i,1}, \dots, a_{i,n}) \rangle = \alpha \cdot 0 + \beta \cdot 0 \end{aligned}$$

□

Trditev. Splošna rešitev \vec{x} rešljivega nehomogenega sistema s partikularno rešitvijo \vec{p} je $\vec{x} = \vec{p} + \vec{h}$, kjer je \vec{h} rešitev temu sistemu prirejenega homogenega sistema (desno stvar smo prepisali z ničlami).

Pripomba. Trdimo, da je množica rešitev nehomogenega sistema samo množica rešitev prirejenega homogenega sistema, premaknjena za partikularno rešitev nehomogenega sistema.

Dokaz. Velja $\forall i : \langle \vec{p}, (a_{i,1}, \dots, a_{i,n}) \rangle = b_i \wedge \langle \vec{h}, (a_{i,1}, \dots, a_{i,n}) \rangle = 0$. Dokažimo $\forall i : \langle \vec{p} + \vec{h}, (a_{i,1}, \dots, a_{i,n}) \rangle = b_i$.

$$\langle \vec{p} + \vec{h}, (a_{i,1}, \dots, a_{i,n}) \rangle = \langle \vec{p}, (a_{i,1}, \dots, a_{i,n}) \rangle + \langle \vec{h}, (a_{i,1}, \dots, a_{i,n}) \rangle = b_i + 0 = b_i$$

□

1.2.6 Predoločeni sistemi

Predoločen sistem, torej tak z več enačbami kot spremenljivkami, je običajno, a ne nujno, nerešljiv.

Definicija. Posplošena rešitev sistema linearnih enačb je taka n -terica števil (x_1, \dots, x_n) , za katero je vektor levih strani $(a_{1,1}x_1 + \dots + a_{1,n}x_n, \dots, a_{m,1}x_1 + \dots + a_{m,n}x_n)$ najbližje vektorju desnih strani (b_1, \dots, b_m) .

Pripomba. Če je sistem rešljiv, se njegova rešitev ujema s posplošeno rešitvijo. Po metodi najmanjših kvadratov želimo minimizirati izraz $(a_{1,1}x_1 + \dots + a_{1,n}x_n - b_1)^2 + \dots + (a_{m,1}x_1 + \dots + a_{m,n}x_n - b_m)^2$ oziroma kvadrat norme razlike $\left\| x_1 \vec{a}_1 + \dots + x_n \vec{a}_n - \vec{b} \right\|^2$.¹ Podobno kot pri regresijski premici želimo pravokotno projicirati \vec{b} na $\mathcal{L} \text{in} \{ \vec{a}_1, \dots, \vec{a}_n \}$. Iščemo torej take skalarje (x_1, \dots, x_n) , da je $\vec{a}_1 x_1 + \dots + \vec{a}_n x_n - \vec{b} \perp \vec{a}_1, \dots, \vec{a}_n$ (hkrati pravokotna na vse vektorje, ki določajo to linearno ogrinjajočo). Preuredimo skalarne produkte in zopet dobimo sistem enačb:

$$\begin{aligned} \left\langle \vec{a}_1 x_1 + \dots + \vec{a}_n x_n - \vec{b}, \vec{a}_1 \right\rangle &= \dots = \left\langle \vec{a}_1 x_1 + \dots + \vec{a}_n x_n - \vec{b}, \vec{a}_n \right\rangle = 0 \\ x_1 \langle \vec{a}_1, \vec{a}_1 \rangle + \dots + x_n \langle \vec{a}_n, \vec{a}_1 \rangle &= \left\langle \vec{b}, \vec{a}_1 \right\rangle \\ &\dots \\ x_1 \langle \vec{a}_1, \vec{a}_n \rangle + \dots + x_n \langle \vec{a}_n, \vec{a}_n \rangle &= \left\langle \vec{b}, \vec{a}_n \right\rangle \end{aligned}$$

Pripomba. Izkaže se, da je zgornji sistem vedno rešljiv. Enolično takrat, ko so $\{ \vec{a}_1, \dots, \vec{a}_n \}$ linearno neodvisni. Če je neenolično rešljiv, pa poiščemo njegovo najkrajšo rešitev.

1.2.7 Poddoločeni sistemi

Trditev. Poddoločen sistem, torej tak, ki ima več spremenljivk kot enačb, ima neskončno rešitev, čim je rešljiv.

Dokaz. Sledi iz zgornjih dokazov, da ima vsak poddoločen homogen sistem neskončno rešitev in da je $\vec{p} + \vec{h}$ splošna rešitev nehomogenega sistema, če je \vec{p} partikularna rešitev tega sistema in \vec{h} splošna rešitev prirejenega homogenega sistema. \square

Pripomba. Seveda je lahko poddoločen sistem nerešljiv. Trivialen primer: $x + y + z = 1$, $x + y + z = 2$.

Kadar ima sistem neskončno rešitev, nas često zanima najkrajša (recimo zadnja opomba v prejšnji sekciji). Geometrijski gledano je najkrajša rešitev pravokotna projekcija izhodišča na presek hiperravnin, ki so množica rešitve sistema. Vsaka enačba določa eno hiperravnino v normalni obliki, torej $\langle \vec{r}, \vec{n}_i \rangle = b_i$. Projekcija izhodišča na hiperravnino v normalni obliki je presečišče premice, ki gre skozi izhodišče in je pravokotna na ravnino, torej $\vec{r} = t \vec{n}_i$, in ravnine same. Vstavimo drugo enačbo v prvo in dobimo $\langle t \vec{n}_i, \vec{n}_i \rangle = b_i$ in izrazimo $t = \frac{b_i}{\langle \vec{n}_i, \vec{n}_i \rangle}$, s čimer dobimo $\vec{r} = \frac{b_i}{\langle \vec{n}_i, \vec{n}_i \rangle} \vec{n}_i$. Doslej je to le projekcija na eno hiperravnino.

Za pravokotno projekcijo na presek hiperravnin pa najprej določimo ravnino, ki je pravokotna na vse hiperravnine sistema, torej $\vec{r} = t_1 \vec{n}_1 + \dots + t_m \vec{n}_m$, in najdemo presek te ravnine z vsemi hiperravninami. To storimo tako, da enačbo ravnine vstavimo v enačbe hiperravnin in jih uredimo: $\langle \vec{r}, \vec{n}_i \rangle = b_i \sim \langle t_1 \vec{n}_1 + \dots + t_m \vec{n}_m, \vec{n}_i \rangle = b_i \sim t_1 \langle \vec{n}_1, \vec{n}_i \rangle + \dots + t_m \langle \vec{n}_m, \vec{n}_i \rangle = b_i$. To nam da sistem enačb

$$\begin{aligned} t_1 \langle \vec{n}_1, \vec{n}_1 \rangle + \dots + t_m \langle \vec{n}_m, \vec{n}_1 \rangle &= b_1 \\ &\dots \\ t_1 \langle \vec{n}_1, \vec{n}_m \rangle + \dots + t_m \langle \vec{n}_m, \vec{n}_m \rangle &= b_m \end{aligned}$$

Rešimo sistem in dobimo (t_1, \dots, t_m) , kar vstavimo v enačbo ravnine $\vec{r} = t_1 \vec{n}_1 + \dots + t_m \vec{n}_m$, da dobimo najkrajšo rešitev.

¹Z \vec{a}_i označujemo stolpcične vektorje sistema, torej $\vec{a}_i = (a_{1,i}, \dots, a_{m,i})$.

1.3 Matrike

Definicija. $m \times n$ matrika je element $(\mathbb{R}^n)^m$, torej $A = ((a_{1,1}, \dots, a_{1,n}), \dots, (a_{m,1}, \dots, a_{m,n}))$. Ima m vrstic in n stolpcev, zato jo pišemo takole:

$$A = \begin{bmatrix} a_{1,1} & \cdots & a_{1,n} \\ \vdots & & \vdots \\ a_{m,1} & \cdots & a_{m,n} \end{bmatrix}$$

Matrikam velikosti $1 \times n$ pravimo vrstični vektor, matrikam velikosti $m \times 1$ pa stolpični vektor. Obe vrsti običajno identificiramo z vektorji. [1] identificiramo z 1. Na preseku i -te vrstice in j -tega stolpca matrike se nahaja element $a_{i,j}$.

Definicija. Seštevanje matrik je definirano le za matrike enakih dimenzij. Vsota matrik $A + B$ je matrika

$$A + B = \begin{bmatrix} a_{1,1} + b_{1,1} & \cdots & a_{1,n} + b_{1,n} \\ \vdots & & \vdots \\ a_{m,1} + b_{m,1} & \cdots & a_{m,n} + b_{m,n} \end{bmatrix}$$

Pripomba. Ničelna matrika 0 je aditivna enota.

$$0 = \begin{bmatrix} 0 & \cdots & 0 \\ \vdots & & \vdots \\ 0 & \cdots & 0 \end{bmatrix}$$

Definicija. Produkt matrike s skalarjem.

$$A \cdot \alpha = \alpha \cdot A = \begin{bmatrix} \alpha a_{1,1} & \cdots & \alpha a_{1,n} \\ \vdots & & \vdots \\ \alpha a_{m,1} & \cdots & \alpha a_{m,n} \end{bmatrix}$$

Definicija. Produkt dveh matrik $A_{m \times n} \cdot B_{n \times p} = C_{m \times p}$. Velja $c_{i,j} = \sum_{k=1}^n a_{i,k} b_{j,k}$. (razmislek prepuščen bralcu)

Pripomba. Kvadratna matrika identiteta I je multiplikativna enota: $i_{ij} = \begin{cases} 0 & ; i \neq j \\ 1 & ; i = j \end{cases}$.

Definicija. Transponiranje matrike $A_{m \times n}^T = B_{n \times m}$. $b_{ij} = a_{ji}$.

Pripomba. Lastnosti transponiranja: $(A^T)^T = A$, $(A + B)^T = A^T + B^T$, $(\alpha A)^T = \alpha A^T$, $(AB)^T = B^T A^T$, $I^T = I$, $0^T = 0$.

1.3.1 Matrični zapis sistema linearnih enačb

Matrika koeficientov vsebuje koeficiente, imenujmo jo A (ena vrstica matrike je ena enačba v sistemu). Stolpični vektor spremenljivk vsebuje spremenljivke $\vec{x} = (x_1, \dots, x_n)$. Vektor desne strani vsebuje desne strani $\vec{b} = (b_1, \dots, b_m)$. Sistem torej zapišemo kot $A\vec{x} = \vec{b}$.

Tudi Gaussovo metodo lahko zapišemo matrično. Trem elementarnim preoblikovanjem, ki ne spremenijo množice rešitev, priredimo ustrezne t. i. elementarne matrice:

- $E_{i,j}(\alpha)$: identiteta, ki ji na i, j -to mesto prištejemo α . Ustreza prištevanju α -kratnika j -te vrstice k i -ti vrstici.
- P_{ij} : v I zamenjamo i -to in j -to vrstico. Ustreza zamenjavi i -te in j -te vrstice.
- $E_i(\alpha)$: v I pomnožiš i -to vrstico z α . Ustreza množenju i -te vrstice s skalarjem α .

Dejstvo. Vsako matriko je moč z levim množenjem z elementarnimi matrikami (Gaussova metoda) prevesti na reducirano vrstično stopničasto formo/obliko. ZDB $\forall A \in M(\mathbb{R}) \exists E_1, \dots, E_k \ni R = E_1 \cdots E_k \cdot A$ je r. v. s. f. Ko rešujemo sistem s temi matrikami množimo levo in desno stran sistema.

1.3.2 Postopek iskanja posplošene rešitve predoločenega sistema

1. Sistem $A\vec{x} = \vec{b}$ z leve pomnožimo z A^T in dobimo sistem $A^T A\vec{x} = A^T \vec{b}$.
2. Poiščemo običajno rešitev dobljenega sistema, za katero se izkaže, da vselej obstaja (dokaz v 2. semestru).
3. Dokažemo, da je običajna rešitev $A^T A\vec{x} = A^T \vec{b}$ enaka posplošeni rešitvi $A\vec{x} = \vec{b}$.

Dokaz. $\|A\vec{x} - \vec{b}\|^2$ bi radi minimizirali. Naj bo \vec{x}_0 običajna rešitev sistema $A^T A\vec{x} = A^T \vec{b}$.

$$\|A\vec{x} - \vec{b}\|^2 = \|A\vec{x} - A\vec{x}_0 + A\vec{x}_0 - \vec{b}\|^2$$

Naj bosta $\vec{u} = A\vec{x} - A\vec{x}_0$ in $\vec{v} = A\vec{x}_0 - \vec{b}$. Trdimo, da $\vec{u} \perp \vec{v}$, torej $\langle \vec{u}, \vec{v} \rangle = 0$. Dokažimo:

$$\begin{aligned} \langle A\vec{x} - A\vec{x}_0, A\vec{x}_0 - \vec{b} \rangle &= \langle A(\vec{x} - \vec{x}_0), A\vec{x}_0 - \vec{b} \rangle = (A\vec{x}_0 - \vec{b})^T A(\vec{x} - \vec{x}_0) = (A\vec{x}_0 - \vec{b})^T (A^T)^T (\vec{x} - \vec{x}_0) = \\ &= (A^T (A\vec{x}_0 - \vec{b}))^T (\vec{x} - \vec{x}_0) = (A^T A\vec{x}_0 - A^T \vec{b}) (\vec{x} - \vec{x}_0) \stackrel{\text{predpostavka o } \vec{x}_0}{=} \mathbf{0} (\vec{x} - \vec{x}_0) \end{aligned}$$

Ker sedaj vemo, da sta \vec{u} in \vec{v} pravokotna, lahko uporabimo Pitagorov izrek, ki za njiju pravi $\|\vec{u} + \vec{v}\|^2 = \|\vec{u}\|^2 + \|\vec{v}\|^2$. V naslednjih izpeljavah je \vec{x} poljuben, \vec{x}_0 pa kot prej.

$$\begin{aligned} \|A\vec{x} - \vec{b}\|^2 &= \|A\vec{x} - A\vec{x}_0 + A\vec{x}_0 - \vec{b}\|^2 = \|A\vec{x} - A\vec{x}_0\|^2 + \|A\vec{x}_0 - \vec{b}\|^2 \geq \|A\vec{x}_0 - \vec{b}\|^2 \\ \|A\vec{x} - \vec{b}\|^2 &\geq \|A\vec{x}_0 - \vec{b}\|^2, \end{aligned}$$

kar pomeni, da je \vec{x}_0 manjši ali enak kot vsi ostale n -terice spremenljivk. □

1.3.3 Najkrajša rešitev sistema

Ta sekcija je precej dobesedno povzeta po profesorjevi beamer skripti.

Sistem $A\vec{x} = \vec{b}$ je lahko neenolično rešljiv. Tedaj nas često zanima po normi najkrajša rešitev sistema.

Trditev. Najkrajša rešitev sistema $A\vec{x} = \vec{b}$ je $A^T \vec{y}_0$, kjer je \vec{y}_0 poljubna rešitev sistema $AA^T \vec{y} = \vec{b}$.

Dokaz. Naj bo \vec{x}_0 poljubna rešitev sistema $A\vec{x} = \vec{b}$ in \vec{y}_0 poljubna rešitev sistema $AA^T \vec{y} = \vec{b}$. Dokažali bi radi, da velja $\|A^T \vec{y}_0\|^2 \leq \|\vec{x}_0\|^2$. Podobno, kot v prejšnji sekciji:

$$\|\vec{x}_0\|^2 = \|\vec{x}_0 - A^T \vec{y}_0 + A^T \vec{y}_0\|^2 = \|u + v\|^2$$

Dokažimo, da sta $\vec{u} = \vec{x}_0 - A^T \vec{y}_0$ in $\vec{v} = A^T \vec{y}_0$ pravokotna, da lahko uporabimo pitagorov izrek v drugi vrstici:

$$\begin{aligned} \langle \vec{x}_0 - A^T \vec{y}_0, A^T \vec{y}_0 \rangle &= (\vec{x}_0 - A^T \vec{y}_0)^T A^T \vec{y}_0 = (A(\vec{x}_0 - A^T \vec{y}_0))^T \vec{y}_0 = (A\vec{x}_0 - AA^T \vec{y}_0)^T \vec{y}_0 = (\vec{b} - \vec{b})^T \vec{y}_0 = 0 \\ \|u + v\|^2 &= \|u\|^2 + \|v\|^2 = \|\vec{x}_0 - A^T \vec{y}_0 + A^T \vec{y}_0\|^2 = \|\vec{x}_0 - A^T \vec{y}_0\|^2 + \|A^T \vec{y}_0\|^2 \geq \|A^T \vec{y}_0\|^2 \\ \|\vec{x}_0\|^2 &\geq \|A^T \vec{y}_0\|^2 \end{aligned}$$

□

Pripomba. Iz rešljivosti $A\vec{x} = \vec{b}$ sledi rešljivost $AA^T \vec{y} = \vec{b}$, toda to znamo dokazati šele v drugem semestru.

1.3.4 Inverzi matrik

Definicija. Matrika B je inverz matrike A , če velja $AB = I$ in $BA = I$. Matrika A je obrnljiva, če ima inverz, sicer je neobrnjljiva.

Trditev. Če inverz obstaja, je enoličen.

Dokaz. Naj bosta B_1 in B_2 inverza A . Velja $AB_1 = B_1A = AB_2 = B_2A = I$. $B_1 = B_1I = B_1(AB_2) = (B_1A)B_2 = IB_2 = B_2$. \square

Definicija. Če inverz A obstaja, ga označimo z A^{-1} .

Zgled. Primeri obrnljivih matrik:

- Identična matrika I : $I \cdot I = I$, $I^{-1} = I$
- Elementarne matrike:
 - $E_{ij}(\alpha) \cdot E_{ij}(-\alpha) = I$, torej $E_{ij}(\alpha)^{-1} = E_{ij}(-\alpha)$
 - $P_{ij} \cdot P_{ij} = I$, torej $P_{ij}^{-1} = P_{ij}$
 - $E_i(\alpha) \cdot E_i(\alpha^{-1}) = I$, torej $E_i(\alpha)^{-1} = E_i(\alpha^{-1})$

Trditev. Produkt obrnljivih matrik je obrnljiva matrika.

Dokaz. Naj bodo A_1, \dots, A_n obrnljive matrike, torej po definiciji velja $A_1 \cdots A_n \cdot A_n^{-1} \cdots A_1^{-1} = A_n \cdots A_1 \cdot A_1^{-1} \cdots A_n^{-1} = I$. Opazimo, da velja $(A_1 \cdots A_n)^{-1} = A_1^{-1} \cdots A_n^{-1}$. \square

Pripomba. Vsaka obrnljiva matrika je produkt elementarnih matrik. Dokaz sledi kasneje.

Zgled. Primeri neobrnjljivih matrik:

- Ničelna matrika, saj pri množenju s katerokoli matriko pridela ničelno matriko in velja $I \neq 0$.
- Matrike z ničelnim stolpcem/vrstico.

Dokaz. Naj ima A vrstico samih ničel. Tedaj za vsako B velja, da ima AB vrstico samih ničel (očitno po definiciji množenja). AB zato ne more biti I , saj I ne vsebuje nobene vrstice samih ničel. Podobno za ničelni stolpec. \square

- Nekvadratne matrike

Dokaz. Naj ima $A_{m \times n}$ več vrstic kot stolpcev ($m > n$). PDDRAA obstaja B , da $AB = I$. Uporabimo Gaussovo metodo na A . Z levim množenjem A z nekimi elementarnimi matrikami lahko pridelamo RVSO. $E_1 \cdots E_n A = R$. $E_1 \cdots E_n AB = E_1 \cdots E_n I = E_1 \cdots E_n = RB$. Toda R ima po konstrukciji ničelno vrstico (je namreč A podobna RVSO in a ima več vrstic kot stolpcev). Potemtakem ima tudi RB ničelno vrstico, torej je neobrnjljiva, toda RB je enak produktu elementarnih matrik, torej bi morala biti obrnljiva. \nrightarrow \square

Pripomba. Iz $AB = I$ ne sledi nujno $BA = I$. Primer: $A = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$, $B = \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 0 \end{bmatrix}$, $AB = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$,

$BA = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix}$. Velja pa to za kvadratne matrike. Dokaz kasneje.

1.3.5 Karakterizacija obrnljivih matrik

Izrek. Za vsako kvadratno matriko A so naslednje trditve ekvivalentne:

1. A je obrnljiva
2. A ima levi inverz ($\exists B \ni: BA = I$)
3. A ima desni inverz ($\exists B \ni: AB = I$)
4. stolpci A so linearno neodvisni
5. $\forall \vec{x} : A\vec{x} = 0 \Rightarrow \vec{x} = 0$
6. stolpci A so ogrodje
7. $\forall \vec{b} \exists \vec{x} \ni: A\vec{x} = \vec{b}$
8. RVSO A je I
9. A je produkt elementarnih matrik

Shema dokaza teh ekvivalenc je zanimiv graf. Bralcu je prepuščena njegova skica.

Dokaz. Dokazujemo ekvivalenco.

(1 \Rightarrow 2) Sledi iz definicije.

(1 \Rightarrow 3) Sledi iz definicije.

(2 \Rightarrow 5) Naj $\exists B \ni: BA = I$. Dokažimo, da $\forall \vec{x} : A\vec{x} = 0 \Rightarrow \vec{x} = 0$. Pa dajmo: $A\vec{x} = 0 \Rightarrow B(A\vec{x}) = B0 = 0 = (BA)\vec{x} = I\vec{x} = \vec{x}$.

(3 \Rightarrow 7) Naj $\exists B \ni: AB = I$. Dokažimo, da $\forall \vec{b} \exists \vec{x} \ni: A\vec{x} = \vec{b}$. Vzemimo $\vec{x} = B\vec{b}$. Tedaj $A\vec{x} = AB\vec{b} = I\vec{b} = \vec{b}$.

(5 \Rightarrow 4) Naj $\forall \vec{x} : A\vec{x} = 0 \Rightarrow \vec{x} = 0$. Dokažimo, da so stolpci A linearno neodvisni. Naj bo $A = \begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \cdots & a_{nn} \end{bmatrix}$,

$$\vec{x} = \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}. \text{ Tedaj } A\vec{x} = \begin{bmatrix} a_{11}x_1 & \cdots & a_{1n}x_n \\ \vdots & & \vdots \\ a_{n1}x_1 & \cdots & a_{nn}x_n \end{bmatrix} = \begin{bmatrix} a_{11} \\ \vdots \\ a_{m1} \end{bmatrix} x_1 + \cdots + \begin{bmatrix} a_{1n} \\ \vdots \\ a_{mn} \end{bmatrix} x_n = \vec{a}_1 x_1 + \cdots + \vec{a}_n x_n.$$

Po definiciji 2 za linearno neodvisnost mora veljati $\vec{a}_1 x_1 + \cdots + \vec{a}_n x_n = 0 \Rightarrow x_1 = \cdots = x_n = 0$. Ravno to pa smo predpostavili.

(7 \Rightarrow 6) Uporabimo iste oznake kot zgoraj. Za poljuben \vec{b} iščemo tak \vec{x} , da je $\vec{a}_1 x_1 + \cdots + \vec{a}_n x_n = A\vec{x} = \vec{b}$ (definicija ogrodja). Po predpostavki 7 velja, da $\forall \vec{b} \exists \vec{x} \ni: A\vec{x} = \vec{b}$. Torej po predpostavki najdemo ustrezen \vec{x} za poljuben \vec{b} .

(4 \Rightarrow 8) Za dokaz uvedimo nekaj lem, ki dokažejo trditev.

Lema 1. Če ima $A_{n \times n}$ LN stolpce in če je $C_{n \times n}$ obrnljiva, ima tudi CA LN stolpce.

Dokaz. Naj bodo a_1, \dots, a_n stolpci A . Velja $Ax = 0 \Rightarrow x = 0$. Dokazati želimo, da $CAx = 0 \Rightarrow x = 0$. Predpostavimo $CAx = 0$. Množimo obe strani z C^{-1} . $C^{-1}CAx = C^{-1}0 \sim IAx = 0 \sim Ax = 0 \Rightarrow x = 0$. \square

Lema 2. Če ima A LN stolpce, ima njena RVSO LN stolpce.

Dokaz. Po Gaussu obstajajo take elementarne E_1, \dots, E_n , da je $E_n \cdots E_1 A = R$ RVSO. Po lemi 1 ima $E_1 A$ LN stolpce, prav tako $E_2 E_1 A$ in tako dalje, vse do $E_n \cdots E_1 A = R$. \square

Lema 3. Če ima RVSO R LN stolpce, je enaka identiteti.

Dokaz. PDDRAA $R \neq I$. Tedaj ima bodisi ničelni stolpec bodisi stopnico, daljšo od 1. Če ima ničelni stolpec, ni LN. \rightarrow . Če ima stopnico, daljšo od 1, kar pomeni, da v vrstici takoj za prvo enico obstajajo neki neničelni \times -i, pa je stolpec z nekim neničelnim \times -om linearna kombinacija ostalih stolpcev, torej stolpci R niso LN \rightarrow . \square

(6 \Rightarrow 8) Predpostavimo, da so stolpci A ogrodje in dokazujemo, da RVSO A je I .

Lema 1. Če so stolpci $A_{n \times n}$ ogrodje in če je $C_{n \times n}$ obrnljiva, so tudi stolpci CA ogrodje.

Dokaz. Naj bodo stolpci A ogrodje. Torej $\forall b \exists x \ni: Ax = C^{-1}b$. Množimo obe strani z C^{-1} . $\forall b \exists x \ni: CAx = b$ — stolpci CA so ogrodje. \square

Lema 2. Če so stolpci A ogrodje, so stolpci njene RVSO ogrodje.

Dokaz. Po Gaussu obstajajo take elementarne E_1, \dots, E_n , da je $E_n \cdots E_1 A = R$ RVSO. Po lemi 1 so stolpci $E_1 A$ ogrodje in tudi stolpci $E_2 E_1 A$ so ogrodje in tako dalje vse do R . \square

Lema 3. Če so stolpci RVSO R ogrodje, je $R = I$.

Dokaz. PDDRAA $R \neq I$. Tedaj ima bodisi ničelni stolpec bodisi stopnico, daljšo od 1. Če ima ničelni stolpec, stolpci niso ogrodje zaradi enoličnosti moči baze (dimenzije prostora). \rightarrow Če ima stopnico, daljšo od 1, pa je stolpec z nekim neničelnim \times -om linearna kombinacija ostalih stolpcev, torej stolpci R niso ogrodje zaradi enoličnosti moči baze (dimenzije prostora) \rightarrow . \square

(8 \Rightarrow 9) Predpostavimo, da je $R := \text{RVSO}(A) = I$. Dokažimo, da je A produkt elementarnih matrik. Po Gaussu obstajajo take elementarne matrike E_1, \dots, E_n , da $E_n \cdots E_1 A = R$. Elementarne matrike so obrnljive, zato množimo z leve najprej z E_n^{-1} , nato z E_{n-1}^{-1} , vse do E_1^{-1} in dobimo $A = E_1^{-1} \cdots E_n^{-1} R$. Upoštevamo, da je inverz elementarne matrike elementarna matrika in da je $R = I$. Tedaj $A = E_1^{-1} \cdots E_n^{-1}$. \square

Trditev. A je obrnljiva $\Leftrightarrow A^T$ obrnljiva.

Dokaz. Velja $AB = I \Leftrightarrow (AB)^T = I^T \Leftrightarrow B^T A^T = I$ in $BA = I \Leftrightarrow (BA)^T = I^T \Leftrightarrow A^T B^T = I$. \square

Posledica. $(A^T)^{-1} = (A^{-1})^T$ in vrstice so LN in ogrodje.

Pripomba. Inverz A lahko izračunamo po Gaussu. Zapišemo razširjeno matriko $[A, I]$ in na obeh applyamo iste elementarne transformacije, da A pretvorimo v RVSO. Če je A obrnljiva, dobimo na levi identiteto, na desni pa A^{-1} .

1.4 Determinante

Definicija. Vsaki kvadratni matriki A priredimo število $\det A$. Definicija za 1×1 matrike: $\det [a] := a$. Rekurzivna definicija za $n \times n$ matrike:

$$\det \begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \cdots & a_{nn} \end{bmatrix} = \sum_{k=1}^n (-1)^{k+1} a_{1k} \det A_{1k},$$

kjer A_{ij} predstavlja A brez i -te vrstice in j -tega stolpca. Tej formuli razvoja se reče „razvoj determinante po prvi vrstici“.

Zgled. 2×2 determinanta. $\det \begin{bmatrix} a & b \\ c & d \end{bmatrix} = ad - bc$. Geometrijski pomen je ploščina paralelograma, ki ga razpenjata (c, d) in (a, b) , kajti ploščina bi bila $(a+c)(b+d) - 2bc - 2\frac{cd}{2} - 2\frac{ab}{2} = \cancel{ab} + \cancel{cb} + ad + \cancel{cd} - 2bc - \cancel{cd} - \cancel{ab} = ad - bc$. Če zamenjamo vrstni red vektorjev, pa dobimo za predznak napačen rezultat, torej je ploščina enaka $\left| \det \begin{bmatrix} a & b \\ c & d \end{bmatrix} \right|$.

Zgled. 3×3 determinanta.

$$\det \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix} = a_{11} \det \begin{bmatrix} a_{22} & a_{23} \\ a_{32} & a_{33} \end{bmatrix} - a_{12} \det \begin{bmatrix} a_{21} & a_{23} \\ a_{31} & a_{33} \end{bmatrix} + a_{13} \det \begin{bmatrix} a_{21} & a_{22} \\ a_{31} & a_{32} \end{bmatrix} =$$

$$a_{11}(a_{22}a_{33} - a_{23}a_{32}) - a_{12}(a_{21}a_{33} - a_{23}a_{31}) + a_{13}(a_{21}a_{32} - a_{22}a_{31})$$

To si lahko zapomnimo s Saurusovim pravilom. Pripisemo na desno stran prva dva stolpca in seštejemo produkte po šestih diagonalah. Naraščajoče diagonale (tiste s pozitivnim koeficientom, če bi jih risali kot premice v ravnini) prej negiramo. Geometrijski

Zgled. Vektorski produkt. Velja:

$$\langle (x, y, z), (a_{21}, a_{22}, a_{23}) \times (a_{31}, a_{32}, a_{33}) \rangle = \det \begin{bmatrix} x & y & z \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix},$$

torej je $[(a_{11}, a_{12}, a_{13}), (a_{21}, a_{22}, a_{23}), (a_{31}, a_{32}, a_{33})]$ (mešani produkt) determinanta matrike A , torej je $|\det A|$ ploščina paralelipeda, ki ga razpenjajo trije vrstični vektorji A .

1.4.1 Računanje determinant

Determinante računati po definiciji je precej zahtevno (bojda $O(n!)$) za $n \times n$ determinanto. Boljšo računsko zahtevnost dobimo z Gaussovo metodo. Oglejmo si najprej posplošeno definicijo determinante: „razvoj po poljubni i -ti vrstici“

$$\det A = \sum_{j=1}^n (-1)^{i+j} a_{ij} \det A_{ij}$$

„razvoj po poljubnem j -tem stolpcu“

$$\det A = \sum_{i=1}^n (-1)^{i+j} a_{ij} \det A_{ij}$$

Ti dve formuli sta še vedno nepolinomske zahtevnosti, uporabni pa sta v primerih, ko imamo veliko ničel na kaki vrstici/stolpcu. Determinanta zgornjetrikotne matrike je po tej formuli produkt diagonalcev.

Kako pa se determinanta obnaša pri elementarnih vrstičnih transformacijah iz Gaussove metode?

- menjava vrstic \implies determinanti se spremeni predznak
- množenje vrstice z $\alpha \implies$ determinanta se pomnoži z α
- prištevanje večkratnika ene vrstice k drugi \implies determinanta se ne spremeni

Časovna zahtevnost Gaussove metode je bojda polinomska $O(n^3)$.

Ideja dokaza veljavnosti Gaussove metode: Indukcija po velikosti matrike.

Baza: 2×2 matrike

Korak: Razvoj po vrstici, ki je elementarna transformacija ne spremeni, dobiš $n(n-1) \times (n-1)$ determinant, ki so veljavne po I. P.

1.4.2 Lastnosti determinante

Trditve. Velja

1. $\det(AB) = \det A \det B$
2. $\det A^T = \det A$
3. $\det \begin{bmatrix} A & B \\ 0 & C \end{bmatrix} = \det A \det C$

Dokaz. Dokazujemo tri trditve

1. Dokazujemo $\det(AB) = \det A \det B$. Obravnavajmo dva posebna primera:

- (a) A je elementarna: obrat pomeni množenje determinante z -1 , množenje vrstice z α množi determinanto z α , prištevanje večkratnika vrstice k drugi vrstici množi determinanto z 1 . Očitno torej trditev velja, če je A elementarna.
- (b) A ima ničelno vrstico: tedaj ima tudi AB ničelno vrstico in je $\det A = 0$ in $\det AB = 0$, torej očitno trditev velja, če ima A ničelno vrstico.

Obravnavajmo še splošen primer: Po Gaussovi metodi obstajajo take elementarne E_1, \dots, E_n , da je $E_n \cdots E_1 A = R$ RVSO. Ker je A kvadratna, je tudi R kvadratna. Ločimo dva primera:

- (a) $R = I$. Tedaj $\det(E_n \cdots E_1 AB) = \det E_n \cdots \det E_1 \det AB = \det(RB) = \det(IB) = \det B$

$$\det I = \det R = \det E_n \cdots \det E_1 \det A \quad / \cdot \det B$$

$$\det I \det B = \det B = \det E_n \cdots \det E_1 \det A \det B$$

$\det B$ zapišimo na dva načina ne levo in desno stran enačbe.

$$\cancel{\det E_n} \cdots \cancel{\det E_1} \det AB = \cancel{\det E_n} \cdots \cancel{\det E_1} \det A \det B$$

$$\det AB = \det A \det B$$

Pripomba. $\exists A^{-1} \Leftrightarrow \det A \neq 0$

Dokaz. Predpostavimo A je obrnljiva. Tedaj $\exists A^{-1} = B \ni: AB = I \xrightarrow{\circ \det} \det(AB) = \det I$. PDDRAA $\det A \neq 0$, tedaj $\det AB = \det B \det A = 0 \neq \det I = 1$. $\rightarrow \times$

Predpostavimo sedaj A ni obrnljiva. Tedaj $\nexists A^{-1} \Rightarrow \exists E_n, \dots, E_1 \ni: E_n \cdots E_1 A = R$ ima ničelno vrstico. Uporabimo isti razmislek kot spodaj, torej $\det R = 0 \Rightarrow 0 = \det R = \det E_n \cdots \det E_1 \det A$. Ker so determinante elementarnih matrik vse neničelne, mora biti $\det A$ ničeln, da je produkt ničeln. \square

- (b) R ima ničelno vrstico. Tedaj $\det(R) = 0 \Rightarrow 0 = \det R = \det E_n \cdots \det E_1 \det A$. Ker so determinante elementarnih matrik vse neničelne, mora biti $\det A$ ničeln, da je produkt ničeln.

2. Dokazujemo $\det A^T = \det A$.

- (a) Če je A elementarna matrika, to drži: $\det P_{ij} = -1 = \det P_{ij}^T = \det P_{ij}$, $\det E_i(\alpha) = \alpha = \det E_i(\alpha)^T = \det E_i(\alpha)$, $\det E_{ij}(\alpha) = 1 = \det E_{ji}(\alpha)^T = \det E_{ij}(\alpha)^T$.
- (b) Če ima A ničelno vrstico, to drži, saj ima tedaj A^T ničeln stolpec in $\det A = 0 = \det A^T$.
- (c) Splošen primer: Po Gaussovi metodi $\exists E_n, \dots, E_1 \ni: E_n \cdots E_1 A = \text{RVSO}(A) = R$. Zopet ločimo dva primera:

i. $R = I$. $\det R = \det R^T = 1$

ii. R ima ničelno vrstico. $\det R = \det R^T = 0$

Sedaj vemo, da $\det R = \det R^T$. Računajmo:

$$\det R = \det R^T$$

$$\det(E_n \cdots E_1 A) = \det(E_n \cdots E_1 A)^T$$

$$\det(E_n \cdots E_1 A) = \det(A^T E_1^T \cdots E_n^T)$$

$$\cancel{\det E_n} \cdots \cancel{\det E_1} \det A = \det A^T \cancel{\det E_1^T} \cdots \cancel{\det E_n^T}$$

$$\det A = \det A^T$$

3. Dokazujemo $\det \begin{bmatrix} A & B \\ 0 & C \end{bmatrix} = \det A \det C$. Levi izraz v enačbi vsebuje t. i. bločno matriko. Upoštevamo poprej dokazano multiplikativnost determinante in opazimo, da pri bločnem množenju matrik velja

$$\begin{bmatrix} A & B \\ 0 & C \end{bmatrix} = \begin{bmatrix} I & 0 \\ 0 & C \end{bmatrix} \begin{bmatrix} A & B \\ 0 & I \end{bmatrix}$$

$$\det \begin{bmatrix} A & B \\ 0 & C \end{bmatrix} = \det \begin{bmatrix} I & 0 \\ 0 & C \end{bmatrix} \det \begin{bmatrix} A & B \\ 0 & I \end{bmatrix}$$

$$\det \begin{bmatrix} A & B \\ 0 & C \end{bmatrix} = \det C \det A$$

Pojasnilo: Za $\det C$ si razpišemo bločno matriko, za $\det A$ si zopet razpišemo bločno matriko in nato z Gaussovimi transformacijami z enicami iz spodnjega desnega bloka izničimo zgornji desni blok (B).

□

1.4.3 Cramerjevo pravilo — eksplicitna formula za rešitve kvadratnega sistema linearnih enačb

Radi bi dobili eksplicitne formule za komponente rešitve x_i kvadratnega sistema linearnih enačb $A\vec{x} = \vec{b}$. Izpeljimo torej eksplicitno formulo. Druga/srednja matrika je identična, v kateri smo i -ti stolpec zamenjali z vektorjem spremenljivk \vec{x} (to označimo z $I_i(\vec{x})$), tretja/desna matrika pa je matrika koeficientov v kateri smo i -ti stolpec zamenjali z vektorjem desnih strani b (to označimo z $A_i(\vec{x})$).

$$\begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \cdots & a_{nn} \end{bmatrix} \begin{bmatrix} 1 & 0 & x_1 & \cdots & 0 \\ & \ddots & \vdots & & \\ & & 1 & x_{i-1} & \\ & & & x_i & \\ & & & x_{i+1} & 1 \\ & & & \vdots & \ddots \\ 0 & & x_n & 0 & 1 \end{bmatrix} = \begin{bmatrix} a_{11} & \cdots & b_1 & \cdots & a_{1n} \\ \vdots & & \vdots & & \vdots \\ a_{i1} & & b_i & & a_{in} \\ \vdots & & \vdots & & \vdots \\ a_{n1} & \cdots & b_n & \cdots & a_{nn} \end{bmatrix}$$

$$\begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \cdots & a_{nn} \end{bmatrix} \begin{bmatrix} 1 & 0 & x_1 & \cdots & 0 \\ & \ddots & \vdots & & \\ & & 1 & x_{i-1} & \\ & & & x_i & \\ & & & x_{i+1} & 1 \\ & & & \vdots & \ddots \\ 0 & & x_n & 0 & 1 \end{bmatrix} = \begin{bmatrix} a_{11} & \cdots & a_{11}x_1 + \cdots + a_{1n}x_n & \cdots & a_{1n} \\ \vdots & & \vdots & & \vdots \\ a_{i1} & & a_{i1}x_1 + \cdots + a_{in}x_n & & a_{in} \\ \vdots & & \vdots & & \vdots \\ a_{n1} & \cdots & a_{n1}x_1 + \cdots + a_{nn}x_n & \cdots & a_{nn} \end{bmatrix}$$

$$AI_i(\vec{x}) = A_i(\vec{b}) \quad / \det$$

$$\det(AI_i(\vec{x})) = \det A_i(\vec{b})$$

$$\det A \det I_i(\vec{x}) = \det A_i(\vec{b})$$

Izračunamo $\det I_i(\vec{x})$ z razvojem po i -ti vrstici.

$$\det A \cdot x_i = \det A_i(\vec{b})$$

$$x_i = \frac{\det A_i(\vec{b})}{\det A}$$

1.4.4 Formula za inverz matrike

Za dano obrnljivo $A_{n \times n}$ iščemo eksplicitno formulo za celice X , da velja $AX = I$. Ideja: najprej bomo problem prevedli na reševanje sistemov linearnih enačb in uporabili Cramerjevo pravilo ter končno poenostavili formule. Naj bodo $\vec{x}_1, \dots, \vec{x}_n$ stolpci X in $\vec{i}_1, \dots, \vec{i}_n$. Potemtakem je $[A\vec{x}_1 \ \cdots \ A\vec{x}_n] = A[\vec{x}_1 \ \cdots \ \vec{x}_n] = AX = I =$

$[\vec{i}_1 \ \dots \ \vec{i}_n]$. Primerjajmo sedaj stolpce na obeh straneh: $\forall i \in \{1..n\} : A\vec{x}_i = \vec{i}_i$. ZDB za vsak stolpec X smo dobili sistem $n \times n$ linearnih enačb. Te sisteme $A\vec{x}_j = \vec{i}_j$ bomo rešili s Cramerjevim pravilom.

$$x_{ij} = (\vec{x}_j)_i = \frac{\det A_i(\vec{i}_j)}{\det A} \text{ razvoj po } \underline{j}\text{-ti vrstici } \frac{\det A_{ji} \cdot (-1)^{j+i}}{\det A}$$

$$X = A^{-1} = \begin{bmatrix} \frac{\det A_{11} \cdot (-1)^{1+1}}{\det A} & \dots & \frac{\det A_{n1} \cdot (-1)^{n+1}}{\det A} \\ \vdots & & \vdots \\ \frac{\det A_{1n} \cdot (-1)^{1+n}}{\det A} & \dots & \frac{\det A_{nn} \cdot (-1)^{n+n}}{\det A} \end{bmatrix} = \frac{1}{\det A} \begin{bmatrix} \det A_{11} \cdot (-1)^{1+1} & \dots & \det A_{1n} \cdot (-1)^{1+1} \\ \vdots & & \vdots \\ \det A_{n1} \cdot (-1)^{n+1} & \dots & \det A_{nn} \cdot (-1)^{n+n} \end{bmatrix}^T = \frac{1}{\det A} \tilde{A}^T,$$

kjer \tilde{A} pravimo kofaktorska matrika.

1.5 Algebrske strukture

1.5.1 Uvod

Naj bo M neprazna množica. Operacija na M pove, kako iz dveh elementov M dobimo nov element M . Na primer, če $a, b \in M$, je $a \circ b$ nov element M .

Definicija. Operacija na M je funkcija $\circ : M \times M \rightarrow M$, kjer je $M \times M$ kartezični produkt (urejeni pari). $(a, b) \mapsto \circ(a, b)$, slednje pa označimo z $\circ(a, b) = a \circ b$.

Na isti množici imamo lahko več različno definiranih operacij. Ločimo jih tako, da uvedemo pojem grupoida.

Definicija. Grupoid je (neprazna množica, izbrana operacija $\circ : M \times M \rightarrow M$). Na primer (M, \circ) .

Še posebej nas zanimajo operacije z lepimi lastnostmi, denimo asociativnost, komutativnost, obstoj enot, inverzov.

Definicija. Grupoid, katerega \circ je asociativna $\Leftrightarrow \forall a, b, c \in M : (a \circ b) \circ c = a \circ (b \circ c)$, je polgrupa. Tedaj skladnja dopušča pisanje brez oklepajev: $a \circ b \circ c \circ d$ je nedvoumen/veljaven izraz, ko je \circ asociativna.

Definicija. Komutativnost: \circ je komutativna $\Leftrightarrow \forall a, b \in M : a \circ b = b \circ a$. Grupoidom s komutativno operacijo pravimo, da so komutativni.

Zgled. Asociativni in komutativni grupoidi (komutativne polgrupe): (\mathbb{N}, \cdot) , (\mathbb{Q}, \cdot) , $(\mathbb{N}, +)$ — številske operacije.

Zgled. Asociativni, a ne komutativni grupoidi (nekomutativne polgrupe): $(M_{n \times n}(\mathbb{R}), \cdot)$ — množenje matrik.

Zgled. Komutativni, a ne asociativni grupoidi: Jordanski produkt matrik: $A \circ B = \frac{1}{2}(AB + BA)$.

Zgled. Niti komutativni niti asociativni grupoidi: Vektorski produkt v \mathbb{R}^3 : (\mathbb{R}^3, \times) .

Zgled. $M \neq \emptyset$. F naj bodo vse funkcije $M \rightarrow M$, \circ pa kompozitum dveh funkcij. Izkaže se, da:

- (F, \circ) je vedno polgrupa.

Dokaz. Definicija kompozituma: $(f \circ g)(x) = f(g(x))$.

$$(f \circ g) \circ h \stackrel{?}{=} f \circ (g \circ h)$$

$$\forall x : ((f \circ g) \circ h)(x) = (f \circ g)(h(x)) = f(g(h(x)))$$

$$\forall x : (f \circ (g \circ h))(x) = f((g \circ h)(x)) = f(g(h(x)))$$

□

- Čim ima M vsaj tri elemente, (F, \circ) ni komutativna.

²Tokrat uporabimo indeks j , ker z njim reprezentiramo stolpec in ponavadi, ko govorimo o elementu x_{ij} matrike X , z i označimo vrstico.

Definicija. Naj bo (M, \circ) grupoid. Element $e \in M$ je enota, če $\forall a \in M : e \circ a = a \wedge a \circ e = a$. Če velja le eno v konjunkciji, je e bodisi leva bodisi desna enota (respectively) in v takem primeru e ni enota.

Zgled. Ali spodnji grupoidi imajo enoto in kakšna je?

- $(\mathbb{R}, +)$: enota je 0.
- (\mathbb{N}, \cdot) : enota je 1.
- $(\mathbb{N}, +)$: ni enote, kajti $0 \notin \mathbb{N}$.
- $(M_{n \times n}(\mathbb{R}), \cdot)$: enota je $I_{n \times n}$.

Trditev. Vsak grupoid ima kvečjemu eno enoto. Dve enoti v istem grupoidu sta enaki. Še več: vsaka leva enota je enaka vsaki desni enoti.

Dokaz. Naj bo e leva enota in f desna enota, torej $\forall a : e \circ a = a \wedge a \circ f = a$. Tedaj $e \circ f = f$ in $e \circ f = e$. Ker je vsaka leva enota vsaki desni, sta poljubni enoti enaki. Enota je, če obstaja, ena sama in je obenem edina leva in edina desna enota. \square

Zgled. Lahko se zgodi, da obstaja poljubno različnih levih, a nobene desne enote. Primer so vse matrike oblike $\begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix}$. Račun $\begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} c & d \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} ac & ad \\ 0 & 0 \end{bmatrix}$ pokaže, da so vsi elementi $\begin{bmatrix} 1 & \times \\ 0 & 0 \end{bmatrix}$ leve enote. Iz dejstva, da je več (tu celo neskončno) levih enot, sledi dejstvo, da ni desnih.

Definicija. Polgrupi z enoto pravimo monoid.

Definicija. Naj bo (M, \circ) monoid z enoto e . Inverz elementa $a \in M$ je tak $b \in M \ni b \circ a = e \wedge a \circ b = e$. Elementu, ki zadošča levi strani konjunkcije, pravimo levi inverz a , elementu, ki zadošča desni strani konjunkcije, pa desni inverz a . Inverz a je torej tak element, ki je hkrati levi in desni inverz a .

Pripomba. Ni nujno, da ima vsak element monoida inverz. Primer je $(M_{n \times n}(\mathbb{R}), \cdot)$; niso vse matrike obrnljive.

Trditev. Vsak element monoida ima kvečjemu en inverz. Vsak levi inverz je enak vsakemu desnemu.

Dokaz. Naj bo b levi in c desni inverz a , torej $b \circ a = e = a \circ c$. Računajmo: $b = b \circ e = b \circ (a \circ c) = (b \circ a) \circ c = e \circ c = c$. Če obstaja, je torej inverz en sam, in ta je edini levi in edini desni inverz. \square

Definicija. Ker vemo, da je inverz enoličen, lahko vpeljemo oznako a^{-1} za inverz elementa a .

Zgled. Ali v spodnjih monoidih obstajajo inverzi in kakšni so?

- $(\mathbb{Z}, +)$: inverz a je $-a$.
- (\mathbb{Z}, \cdot) : inverz 1 je 1, inverz -1 je -1 , ostali elementi pa inverza nimajo.
- $(\mathbb{Q} \setminus \{0\}, \cdot)$: inverz a je $\frac{1}{a}$.

Pripomba. Če desnega inverza ni, je lahko levih inverzov več. Primer: Naj bodo M vse funkcije $\mathbb{N} \rightarrow \mathbb{N}$ in naj bo \circ kompozitum funkcij. Tedaj velja:

- $f \in M$ ima levi inverz $\Leftrightarrow f$ injektivna.
- $f \in M$ ima desni inverz $\Leftrightarrow f$ surjektivna.
- $f \in M$ ima inverz $\Leftrightarrow f$ bijektivna.

Zgled. $f(n) = n + 1$ je injektivna, a ne surjektivna. Vsi za komponiranje levi inverzi f so funkcije oblike $g(x) = \begin{cases} x - 1 & ; x > 1 \\ \times & ; x = 1 \end{cases}$ ZDB x lahko slikajo v karkoli, pa bo $(g \circ f)$ še vedno funkcija identiteta.

Zgled. V $(M_{n \times n}(\mathbb{R}), \cdot)$ je vsak levi inverz tudi desni inverz. To je res tudi za funkcije na končni množici, toda ni res v splošnem.

Definicija. Grupa je tak monoid, v katerem ima vsak element inverz. Daljše: grupa je taka neprazna množica G z operacijo \circ , ki zadošča asociativnosti, obstaja enota in za vsak element obstaja njegov inverz. Grupi s komutativno operacijo pravimo Abelova grupa.

Zgled. Nekaj abelovih grup: $(\mathbb{Z}, +)$, $(\mathbb{Q} \setminus \{0\}, \cdot)$, $(M_{n \times n}(\mathbb{R}), +)$, $(\mathbb{R}^n, +)$. Nekaj neabelovih grup: vse obrnljive matrike fiksne dimenzije, vse permutacije neprazne končne množice.

1.5.2 Podstrukture

Naj bo (M, \circ) grupoid. Reciumi, da je N neprazna podmnožica M . Pod temi pogoji se lahko zgodi, da $\exists a, b \in N \ni a \circ b \notin N$.

Zgled. Oglejmo si grupoid $(\mathbb{Z}, +)$. $N \subseteq \mathbb{Z}$ naj bodo liha cela števila. $\forall a, b \in N : a + b \notin N \Rightarrow \exists a, b \in N \ni a + b \notin N$, kajti vsota lihih števil je soda.

Definicija. Pravimo, da je podmnožica $N \subseteq M$ zaprta za \circ , če $\forall a, b \in N : a \circ b \in N$.

Zgled. Oglejmo si spet grupoid $(\mathbb{Z}, +)$. $N \subseteq \mathbb{Z}$ naj bodo soda cela števila. N je zaprta za $+$.

Definicija. Takemu N , kjer je $N \subseteq M$, z implicitno podedovano operacijo $(a \circ_N b = a \circ b)$ pravimo podgrupoid (N, \circ_N) .

Vaja. Pokaži, da je „general linear“ $GL_n(\mathbb{R}) := \{A \in M_{n \times n}(\mathbb{R}) ; \det A \neq 0\}$ grupa za matrično množenje.

Asociativnost je dokazana zgoraj. Enota je I_n . Inverzi obstajajo, ker so determinante neničelne in tudi inverzi imajo neničelne determinante. Preveriti je treba še vsebovanost, torej $\forall A, B \in GL_n(\mathbb{R}) : A \cdot B \in GL_n(\mathbb{R})$. Vzemimo poljubni $A, B \in GL_n(\mathbb{R})$, torej $\det A \neq 0 \wedge \det B \neq 0$. $\det(AB) = \det A \det B \neq 0 \Leftrightarrow \det A \neq 0 \vee \det B \neq 0$, toda ker noben izmed izrazov disjunkcije ne drži, determinanta AB nikdar ni 0. Enota I je vsebovana v $GL_n(\mathbb{R})$, saj $\det I = 1 \neq 0$.

Vaja. Ali je „special linear“ $SL_n(\mathbb{R}) := \{A \in M_{n \times n}(\mathbb{R}) ; \det A = 1\}$ grupa za matrično množenje?

Vse lastnosti (razen vsebovanosti) smo preverili zgoraj. Preveriti je treba vsebovanost, torej ali $\forall A, B \in SL_n(\mathbb{R}) : A \cdot B \in SL_n(\mathbb{R})$. Vzemimo poljubni $A, B \in SL_n(\mathbb{R})$, torej $\det A = 1 \wedge \det B = 1$. $\det(AB) = \det A \det B = 1 \cdot 1 = 1$. Preveriti je treba še, da so inverzi vsebovani. Za poljubno $A \in SL_n(\mathbb{R})$ je $\det A^{-1} = \frac{1}{\det A} = 1$, ker je $\det A = 1$. Enota I je vsebovana v $SL_n(\mathbb{R})$, saj $\det I = 1$.

Dejstvo. Za podedovano operacijo \circ_N v podstrukturi se asociativnost in komutativnost podedujeta, ni pa nujno, da če obstaja enota v (M, \circ) , obstaja enota tudi v (N, \circ_N) . Prav tako ni rečeno, da se podeduje obstoj inverzov.

Definicija. Če je (M, \circ) polgrupa (asociativen grupoid) in $N \subseteq M$, pravimo, da je N podpolgrupa, če je zaprta za \circ .

Definicija 4. Če je (M, \circ) monoid (polgrupa z enoto) in $N \subseteq M$, je N podmonoid, če je zaprt za \circ in vsebuje enoto iz (M, \circ) (prav tisto enoto, glej primer 5 spodaj).

Zgled. (\mathbb{N}, \cdot) je monoid. Soda števila so podpolgrupa (zaprta so za množenje), niso pa podmonoid, saj ne vsebujejo enice (enote).

Zgled 5. $(\mathbb{N} \times \mathbb{N}, \circ)$ je monoid za operacijo $(a, b) \circ (c, d) = (ac, bd)$, saj je enota $(1, 1)$. $(\mathbb{N} \times \{0\}, \circ)$ pa za \circ kot prej je sicer podpolgrupa v $(\mathbb{N} \times \mathbb{N}, \circ)$ in ima enoto $(1, 0)$, vendar, ker $(1, 0) \neq (1, 1)$, to ni podmonoid. Enota mora torej biti, kot pravi definicija 4, ista kot enota v „starševski“ strukturi.

Definicija. Če je (M, \circ) grupa in $N \subseteq M$, pravimo, da je N podgrupa \iff hkrati velja

- je zaprta za \circ ,
- vsebuje isto enoto kot (M, \circ) in
- vsebuje inverz vsakega svojega elementa; ti inverzi pa so itak po enoličnosti enaki inverzom iz (M, \circ) .

Zgled. special linear, SL_n , grupa vseh matrik z determinanto enako 1, je podgrupa „general linear“, GL_n , grupe vseh obrnljivih $n \times n$ matrik, kajti $\det I = 1$, \det je multiplikativna (glej vajo zgoraj) in $\det A = 1 \Leftrightarrow \det A^{-1} = 1$.

Zgled. ortogonalne matrike, O_n , vse $n \times n$ matrike A , ki zadoščajo $A^T A = I$, je podgrupa $GL_n(\mathbb{R})$, kajti:

- Je zaprta:

$$\begin{aligned} A, B \in O_n &\stackrel{?}{\implies} AB \in O_n \\ (AB)^T (AB) &\stackrel{?}{=} I \\ B^T (A^T A) B &\stackrel{?}{=} I \\ I &= I \end{aligned}$$

- Vsebuje enoto I :

$$I^T I = I$$

- Vsebuje inverze vseh svojih elementov: Uporabimo $A^T A = I \Rightarrow A^T = A^{-1}$

$$A \in O_n \stackrel{?}{\Rightarrow} A^{-1} \in O_n$$

$$(A^{-1})^T A^{-1} \stackrel{?}{=} I$$

$$(A^T)^T A^T = AA^T = I$$

Dejstvo. *specialna ortogonalna grupa*, $SO_n := O_n \cap SL_n$ je podgrupa $GL_n(\mathbb{R})$. Dokazati je moč še bolj splošno, namreč, da je presek dveh podgrup spet podgrupa.

Trditev. Naj bo (M, \circ) grupa in $N \subseteq M$ neprazna. Tedaj velja N podgrupa $\Leftrightarrow \forall a, b \in N : a \circ b^{-1} \in N$ (zaprtost za odštevanje — v abelovih grupah namreč običajno operacijo označimo s $+$ in označimo $a + b^{-1} = a - b$).

Dokaz. Dokazujemo ekvivalenco

(\Rightarrow) Naj bo N podgrupa v (M, \circ) . Vzemimo $a, b \in N$. Upoštevamo $b \in N \Rightarrow b^{-1} \in N$ iz definicije podgrupe. Torej velja $a, b^{-1} \in N \Rightarrow a \circ b^{-1} \in N$, zopet iz definicije podgrupe.

(\Leftarrow) Naj $\forall a, b \in N : a \circ b^{-1} \in N$. Preverimo lastnosti iz definicije podgrupe:

- Vsebovanost enote: Ker je N neprazna, vsebuje nek a . Po predpostavki je $a \circ a^{-1} \in N$, $a \circ a^{-1}$ pa je po definiciji inverza enota.
- Vsebovanost inverzov: Naj bo $a \in N$ poljuben. Od prej vemo, da $e \in N$. Po predpostavki, ker $e, a \in N \Rightarrow e \circ a^{-1} \in N$, $e \circ a^{-1}$ pa je po definiciji enote a^{-1} .
- Zaprtost: Naj bosta $a, b \in N$ poljubna. Od prej vemo, da $b^{-1} \in N$. Po predpostavki, ker $a, b^{-1} \in N \Rightarrow a \circ (b^{-1})^{-1} \in N$, $a \circ (b^{-1})^{-1}$ pa je po definiciji inverza $a \circ b$.

□

1.5.3 Homomorfizmi

\sim so operacije, ki „ohranjajo strukturo“.

Definicija. Naj bosta (M_1, \circ_1) in (M_2, \circ_2) dva grupoida. Preslikava $f : M_1 \rightarrow M_2$ je homomorfizem grupoidov, če $\forall a, b \in M_1 : f(a \circ_1 b) = f(a) \circ_2 f(b)$. Enaka definicija v polgrupah. Za homomorfizem monoidov zahtevamo še, da $f(e_1) = e_2$, kjer je e_1 enota M_1 in e_2 enota M_2 .

Zgled. $f : \mathbb{N} \rightarrow \mathbb{N} \times \mathbb{N}$, ki slika $a \mapsto (a, 0)$. \circ_1 naj bo množenje, \circ_2 pa $(a, b) \circ_2 (c, d) = (ac, bd)$ (množenje po komponentah). $(1, 1)$ je enota v $\mathbb{N} \times \mathbb{N}$, 1 pa je enota v \mathbb{N} . f je homomorfizem, ker $f(a \circ_1 b) = (a \cdot b, 0) = (a, 0) \circ_2 (b, 0) = f(a) \circ_2 f(b)$, ni pa homomorfizem monoidov, saj $f(1) = (1, 0) \neq (1, 1)$.

Definicija. Za homomorfizem grup zahtevamo še, da $f(a^{-1}) = f(a)^{-1}$.

Pripomba. Izkaže se, da ohranjanje enote in inverzov pri homomorfizmih grup sledi že iz definicije homomorfizmov grupoidov.

Trditev. Naj bosta (M_1, \circ_1) in (M_2, \circ_2) grupi. Naj bo $f : M_1 \rightarrow M_2$ preslikava, ki je homomorfizem grupoidov. Trdimo, da slika enoto v enoto in inverze v inverze.

Dokaz. Naj bo e_1 enota za (M_1, \circ_1) in e_2 enota za (M_2, \circ_2) . Dokažimo, da $f(e_1) \stackrel{?}{=} e_2$.

$$f(e_1) = f(e_1 \circ_1 e_1) = f(e_1) \circ_2 f(e_1) = f(e_1)^{-1} \circ f(e_1) \circ e_2 = e_2 \circ e_2 = e_2$$

Dokažimo še ohranjanje inverzov, se pravi b je inverz $a \stackrel{?}{\Rightarrow} f(b)$ je inverz $f(a)$.

$$a \circ_1 b = e_1 \stackrel{?}{\Rightarrow} f(a) \circ_2 f(b) = f(a \circ_1 b) = f(e_1) = e_2$$

$$b \circ_1 a = e_1 \stackrel{?}{\Rightarrow} f(b) \circ_2 f(a) = f(b \circ_1 a) = f(e_1) = e_2$$

□

Zgled 6. Primeri homomorfizmov.

1. Determinanta: $M_n(\mathbb{R}) \rightarrow \mathbb{R}$ je homomorfizem, ker ima multiplikativno lastnost: $\det(AB) = \det A \det B$.
2. S_n so vse permutacije množice $\{1..n\}$. Vsaki permutaciji $\sigma \in S_n$ priredimo permutacijsko matriko $P_\sigma \in M_n(\mathbb{R})$ tako, da vsebuje vektorje standardne baze \mathbb{R}^n kot stolpce:

$$P_\sigma := [e_{\sigma(1)} \quad \cdots \quad e_{\sigma(n)}]$$

Imamo preslikavo $S \rightarrow M_n(\mathbb{R})$, ki slika $\sigma \mapsto P_\sigma$ in trdimo, da je homomorfizem. Dokažimo, da je $\forall \sigma, \tau \in S_n : P_{\sigma\circ\tau} = P_\sigma \cdot P_\tau$. Opazimo, da je $\forall i \in \{1..n\} : P_\sigma \vec{e}_i = e_{\sigma(i)}$ (tu množimo matriko z vektorjem). Če namesto i pišemo $\tau(i)$, dobimo $\forall i \in \{1..n\} : P_\sigma e_{\tau(i)} = e_{(\sigma\circ\tau)(i)}$. Preverimo sedaj množenje $P_\sigma P_\tau = P_\sigma [e_{\tau(1)} \quad \cdots \quad e_{\tau(n)}] = [P_\sigma e_{\tau(1)} \quad \cdots \quad P_\sigma e_{\tau(n)}] = [e_{(\sigma\circ\tau)(1)} \quad \cdots \quad e_{(\sigma\circ\tau)(n)}] = P_{\sigma\circ\tau}$. Preslikava je res homomorfizem.

Trditev. Kompozitum dveh homomorfizmov je tudi sam zopet homomorfizem.

Dokaz. Imejmo tri grupoide in homomorfizma, ki slikata med njimi takole: $(M_1, \circ_1) \xrightarrow{f} (M_2, \circ_2) \xrightarrow{g} (M_3, \circ_3)$. Dokažimo, da je $g \circ f$ spet homomorfizem.

$$(g \circ f)(a \circ_1 b) = g(f(a \circ_1 b)) = g(f(a) \circ_2 f(b)) = g(f(a)) \circ_3 g(f(b)) = (g \circ f)(a) \circ_3 (g \circ f)(b)$$

□

Zgled. $S_n \xrightarrow{\sigma} M_n(\mathbb{R}) \xrightarrow{\det} \mathbb{R}$, kjer je σ preslikava iz točke 2 zgleđa 6 zgoraj. $\text{sgn} = \det \circ \sigma$, kjer je sgn parnost permutacije. Preslikava sgn je homomorfizem, ker je kompozitum dveh homomorfizmov.

Definicija. Izomorfizem je preslikava, ki je bijektivna in je homomorfizem. Dve grupi sta izomorfni, kadar med njima obstaja izomorfizem.

Pripomba. S stališča algebre sta dve izomorfni grupi v abstraktnem smislu enaki, saj je izomorfizem zgolj reverzibilno preimenovanje elementov.

1.5.4 Bigrupoidi, polkolobarji, kolobarji

Definicija. Neprazni množici M z dvema operacijama \circ_1 in \circ_2 pravimo bigrupoid in ga označimo z (M, \circ_1, \circ_2) . Običajno operaciji označimo z $+, \cdot$, tedaj bigrupoid pišemo kot $(M, +, \cdot)$.

„Če $+ \text{ in } \cdot$ ena z drugo nimata nobene zveze, je vseeno, če ju študiramo skupaj ali posebej.“

Definicija. Distributivnost je značilnost bigrupoida $(M, +, \cdot)$. Ločimo levo distributivnost: $\forall a, b, c \in M : a \cdot (b + c) = a \cdot b + a \cdot c$ in desno distributivnost: $\forall a, b, c \in M : (a + b) \cdot c = a \cdot c + b \cdot c$.

Definicija. Bigrupoid, ki zadošča levi in desni distributivnosti, je distributiven.

Definicija. Distributiven bigrupoid, je polkolobar, če je $(M, +)$ komutativna polgrupa.

Definicija. Distributiven grupoid je kolobar, če je $(M, +)$ komutativna grupa.

Zgled. Primer polkolobarja, ki ni kolobar, je $(\mathbb{N}, +, \cdot)$. Ni enote niti inverza za $+$, $(\mathbb{N}, +)$ pa je polgrupa.

Kolobarje delimo glede na lastnosti operacije \cdot :

Definicija. Asociativen kolobar je tak, kjer je \cdot asociativna operacija $\sim (M, \cdot)$ je polgrupa.

Zgled. Primer kolobarja, ki ni asociativen, je $(\mathbb{R}^3, +, \times)$, kjer je \times vektorski produkt. Primer kolobarja, ki je asociativen, je $(M_n(\mathbb{R}), +, \cdot)$, kjer je \cdot matrično množenje.

Definicija. Asociativen kolobar z enoto je tak, ki ima multiplikativno enoto, torej enoto za drugo operacijo $\sim (M, \cdot)$ je monoid. Tipično se enoto za \cdot označi z 1, enoto za $+$ pa z 0.

Zgled. Primer asociativnega kolobarja brez enote je (soda $\mathbb{N}, +, \cdot$). Primer asociativnega kolobarja z enoto je $(\mathbb{N}, +, \cdot)$.

Definicija. b je inverz a , če $b \cdot a = e$ in $a \cdot b = e$, kjer je e multiplikativna enota kolobarja.

Pripomba. Element 0 nima nikoli inverza, ker $\forall a \in M : 0 \cdot a = 0$.

Dokaz. $0 \cdot a = (0 + 0) \cdot a = 0 \cdot a + 0 \cdot a$ (dokaz velja za kolobarje, ne pa polkolobarje, ker imamo pravilo krajšanja³ le, kadar je $(M, +)$ grupa). \square

Definicija. Asociativen kolobar z enoto, v katerem ima vsak neničen element inverz, je obseg.

Definicija. Kolobar je komutativen, če je \cdot komutativna operacija ($+$ je itak po definiciji že komutativna).

Definicija. Komutativen obseg je polje.

Zgled. Primeri polj: $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$, $(F[\mathbb{R}], +, \cdot)$, kjer je $F[\mathbb{R}]$ polje racionalnih funkcij.

Zgled. Primer obsega, ki ni polje: $(\mathbb{H}, +, \cdot)$.

Definicija. Kvaternioni so $M_{2 \times 2}(\mathbb{R})$ take oblike: za $\alpha, \beta \in \mathbb{C}$ je $\mathbb{H} := \begin{bmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{bmatrix} = \begin{bmatrix} a + bi & c + di \\ -c + di & a - bi \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} a + \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix} b + \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} c + \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix} d = 1a + bi + cj + dk$ za $a, b, c, d \in \mathbb{R}$ in dimenzije 1, i, j, k .

Zgled. Primer kolobarja: Naj bo X neprazna množica in R kolobar. R^X so vse funkcije $X \rightarrow R$. Naj bosta $f, g \in R^X$. Definirajmo operaciji:

$$+ \quad f + g := (f + g)(x) = f(x) + g(x)$$

$$\cdot \quad f \cdot g := (f \cdot g)(x) = f(x) \cdot g(x)$$

1.5.5 Podkolobarji

Definicija. Podbigrupoid od $(M, +, \cdot)$ je taka podmnožica $N \subseteq M$, ki je zaprta za $+$ in \cdot . ZDB $N \subseteq M$ je podbigrupoid v $(M, +)$ in (M, \cdot) .

Definicija. Podkolobar kolobarja $(M, +, \cdot)$ je taka podmnožica $N \subseteq M$, da je N podgrupa v $(M, +)$ in N podbigrupoid v $(N, \cdot) \Leftrightarrow N$ zaprta za \cdot . Skrajšana definicija je torej, da je $\forall a, b \in N : a + b^{-1} \in N \wedge a \cdot b \in N$, torej zaprtost za odštevanje in množenje.

Zgled. Primeri podkolobarjev

- v $(M_n(\mathbb{R}), +, \cdot)$
 - zgornjetrikotne matrike
 - diagonalne matrike
 - matrike s spodnjo vrstico ničelno
 - matrike z ničelnim i -tim stolpcem
 - $M_n(\mathbb{Z}), M_n(\mathbb{Q})$
 - matrike oblike $\begin{bmatrix} a & b \\ b & a \end{bmatrix}$
- v $(\mathbb{R}^{[a,b]}, +, \cdot)$ (vse funkcije $[a, b] \rightarrow \mathbb{R}$ za seštevanje in množenje)
 - vse omejene funkcije
 - vse zvezne funkcije
 - vse odvedljive funkcije

Definicija. Podobseg obsega $(M, +, \cdot)$ je taka $N \subseteq M$, da velja:

- N podgrupa v $(M, +)$

³Dokaz v mojih Odgovorih na vprašanja za ustni izpit Diskretnih struktur 2 IŠRM

- $N \setminus \{0\}$ podgrupa v $(M \setminus \{0\}, \cdot)$

ZDB: N je zaprta za odštevanje (seštevanje z aditivnim inverzom) in za deljenje (množenje z multiplikativnim inverzom) z neničelnimi elementi.

Zgled. Primeri podobsegov:

- \mathbb{R} je podobseg v $(\mathbb{C}, +, \cdot)$
- \mathbb{Q} je podobseg v $(\mathbb{R}, +, \cdot)$

Zgled. Izkaže se, da je najmanjše podpolje v \mathbb{R} , ki vsebuje \mathbb{Q} in $\sqrt{3}$ množica $\{a + b\sqrt{3}; \forall a, b \in \mathbb{Q}\}$. Očitno je zaprt za odštevanje. Za deljenje?

$$\begin{aligned} \frac{a + b\sqrt{3}}{c + d\sqrt{3}} &= \frac{(a + b\sqrt{3})(c - d\sqrt{3})}{(c + d\sqrt{3})(c - d\sqrt{3})} = \frac{ac - ad\sqrt{3} + bc\sqrt{3} - 3bd}{c^2 - 3d^2} = \frac{ac - 3bd + (bc - ad)\sqrt{3}}{c^2 - 3d^2} = \\ &= \frac{ac - 3bd}{c^2 - 3d^2} + \frac{bc - ad}{c^2 - 3d^2}\sqrt{3} \end{aligned}$$

1.5.6 Homomorfizmi kolobarjev

Definicija. Naj bosta $(M_1, +_1, \cdot_1)$ in $(M_2, +_2, \cdot_2)$ kolobarja. $f : M_1 \rightarrow M_2$ je homomorfizem kolobarjev $\Leftrightarrow \forall a, b \in M_1 : f(a +_1 b) = f(a) +_2 f(b) \wedge f(a \cdot_1 b) = f(a) \cdot_2 f(b)$. ZDB f mora biti homomorfizem grupoidov $(M_1, +_1) \rightarrow (M_2, +_2)$ in $(M_1, \cdot_1) \rightarrow (M_2, \cdot_2)$. Za homomorfizem kolobarjev z enoto zahtevamo še $f(1_1) = 1_2$.

Zgled. $f : M_2(\mathbb{R}) \rightarrow M_3(\mathbb{R})$ s predpisom $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \mapsto \begin{bmatrix} a & b & 0 \\ c & d & 0 \\ 0 & 0 & 0 \end{bmatrix}$ je homomorfizem kolobarjev, ni pa homomorfizem kolobarjev z enoto, kajti $f\left(\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}\right) = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix}$, kar ni enota v $M_3(\mathbb{R})$ (I_3) za implicitni operaciji $+$ in \cdot .

Zgled. $g : M_n(\mathbb{R}) \rightarrow M_n(\mathbb{R})$ ki slika $A \mapsto S^{-1}AS$, kjer je S neka fiksna obrnljiva matrika v $M_n(\mathbb{R})$. Uporabimo implicitni operaciji $+$ in \cdot za matrike. Računa $g(A + B) = S^{-1}(A + B)S = S^{-1}AS + S^{-1}BS = g(A) + g(B)$ in $g(AB) = S^{-1}ABS = S^{-1}AIBS = S^{-1}ASS^{-1}BS = g(A)g(B)$ pokažeta, da je g homomorfizem kolobarjev, celo z enoto, kajti $g(I) = S^{-1}IS = S^{-1}S = I$.

Zgled. $h : \mathbb{C} \rightarrow M_n(\mathbb{R})$ s predpisom $\alpha + \beta i \rightarrow \begin{bmatrix} \alpha & \beta \\ -\beta & \alpha \end{bmatrix}$ je homomorfizem kolobarjev z enoto.

Zgled. Kolobar ostankov $\mathbb{Z}_n := \{0..(n-1)\}$ je asociativni kolobar z enoto. Če je p praštevilo, pa je celo \mathbb{Z}_p polje za implicitni operaciji seštevanje in množenja po modulu.

1.6 Vektorski prostori

Ideja: Vektorski prostor je Abelova grupa z dodatno strukturo — množenje s skalarjem.

Definicija. Naj bo $(F, +, \cdot)$ polje. Vektorski prostor z operacijama $V + V \rightarrow V$ in $F \cdot V \rightarrow V$ nad F je taka $(V, +, \cdot)$, da velja:

1. $(V, +)$ je abelova grupa: komutativnost, asociativnost, enota, aditivni inverzi
2. Lastnosti množenja s skalarjem. $\forall \alpha, \beta \in F, a, b \in V :$

- (a) $\alpha(a + b) = \alpha a + \alpha b$
- (b) $(\alpha + \beta)a = \alpha a + \beta a$
- (c) $(\alpha \cdot \beta) \cdot a = \alpha \cdot (\beta \cdot a)$
- (d) $1 \cdot a = a$

Alternativna abstraktna formulacija aksiomov množenja s skalarjem se glasi:

$\forall \alpha \in F$ priredimo preslikavo $\varphi_\alpha : V \rightarrow V$, ki pošlje $v \mapsto \alpha v$. Štiri zgornje aksiome množenja s skalarjem sedaj označimo z abstraktnimi formulacijami:

- (a) $\varphi_\alpha(a+b) \stackrel{\text{def.}}{=} \alpha(a+b) = \alpha a + \alpha b \stackrel{\text{def.}}{=} \varphi_\alpha(a) + \varphi_\alpha(b)$ — vidimo, da je φ_α homomorfizem iz $(V, +)$ v $(V, +)$.
- (b) $\varphi_{\alpha+\beta}(a) \stackrel{\text{def.}}{=} (\alpha+\beta)a = \alpha a + \beta a \stackrel{\text{def.}}{=} \varphi_\alpha a + \varphi_\beta a$ — torej $\varphi_{\alpha+\beta} = \varphi_\alpha + \varphi_\beta$.
- (c) $\varphi_{\alpha\beta} a \stackrel{\text{def.}}{=} (\alpha\beta)a = \alpha(\beta a) \stackrel{\text{def.}}{=} \varphi_\alpha(\varphi_\beta(a)) = (\varphi_\alpha \circ \varphi_\beta)(a)$ — torej $\varphi_{\alpha\beta} = \varphi_\alpha \circ \varphi_\beta$.
- (d) $\varphi_1 a \stackrel{\text{def.}}{=} 1a = a$ — torej $\varphi_1 = id$.

Pripomba. Če v definiciji vektorskega prostora zamenjamo polje F s kolobarjem F , dobimo definicijo **modula** nad F .

Zgled. Primeri vektorskih prostorov:

- standarden primer: naj bo F polje in $n \in \mathbb{N}$. Naj bo $V = F^n$, + seštevanje po komponentah in \cdot množenje s skalarjem po komponentah. Pod temi pogoji je $(V, +, \cdot)$ vektorski prostor — ustreza vsem osmim aksiomom.
- Naj bo F polje in $n, m \in \mathbb{N}$. Naj bo $V := M_{m,n}(F) = m \times n$ matrice nad F . + in \cdot definiramo kot pri matrikah.
- Naj bo F polje, $S \neq \emptyset$ množica. Naj bo $V := F^S$ (vse funkcije $S \rightarrow F$). Naj bosta $\varphi, \tau : S \rightarrow F$. Definirajmo $\forall s \in S$ operaciji $(\varphi + \tau)(s) = \varphi(s) + \tau(s)$ in $(\varphi \cdot \tau)(s) = \varphi(s) \cdot \tau(s)$. Tedaj je V vektorski prostor. Ta definicija je podobna kot definiciji z n -terico elementov polja, saj lahko n -terico identificiramo s funkcijo $\{\alpha_1, \dots, \alpha_n\} \rightarrow F$, toda ta primer dovoli neskončno razsežne vektorske prostore, saj S ni nujno končna, n -terica pa nekako implicitno je, saj $n \in \mathbb{N}$.
- Polinomi. Naj bo $V := F[x]$ (polinomi v spremenljivki x s koeficienti v F). Seštevanje definirajmo po komponentah: $(\alpha + \beta x + \gamma x^2) + (\pi + \tau x) = (\alpha + \pi + (\beta + \tau)x + \gamma x^2)$, množenje s skalarjem pa takole: $\alpha(a + bx + cx^2) = \alpha a + \alpha bx + \alpha cx^2$.
- Naj bosta V_1 in V_2 dva vektorska prostora nad istim poljem F . Tvorimo nov vektorski prostor nad F , ki mu pravimo „direktna vsota“ V_1 in V_2 in ga označimo z $V_1 \oplus V_2 := \{(v_1, v_2); \forall v_1 \in V_1, v_2 \in V_2\}$. Seštevamo po komponentah: $(v_1, v_2) + (v'_1, v'_2) = (v_1 + v'_1, v_2 + v'_2)$, s skalarjem pa množimo prvi komponento: $\forall \alpha \in F : \alpha(v_1, v_2) = (\alpha v_1, v_2)$. Definicijo lahko posplošimo na n vektorskih prostorov. Tedaj so elementi prostora urejene n -terice.

1.6.1 Podprostori vektorskih prostorov — vektorski podprostori

Definicija. Naj bo $(V, +, \cdot)$ vektorski prostor nad F . Vektorski podprostor je taka neprazna podmnožica V , ki je zaprta za seštevanje in množenje s skalarjem. Natančneje: $(W, +, \cdot)$ je vektorski podprostor $(V, +, \cdot) \iff$ velja hkrati:

1. $W \subseteq V$ in $W \neq \emptyset$
2. $\forall a, b \in W : a + b \in W$
3. $\forall a \in W, \alpha \in F : \alpha a \in W$

Lastnosti 2 in 3 je moč združiti v eno: $\forall a_i, a_2 \in W, \alpha_1, \alpha_2 \in F : \alpha_1 a_1 + \alpha_2 a_2 \in W$.

Z drugimi besedami je vektorski podprostor taka podmnožica, ki vsebuje vse linearne kombinacije svojih elementov. Odštevanje $a - b$ je poseben primer linearne kombinacije, kajti $a_1 - a_2 = 1a_1 + (-1)a_2$. Sledi, da mora biti $(W, +)$ podgrupa $(V, +)$, torej taka podmnožica V , ki je zaprta za odštevanje.

Zgled. Primeri vektorskih podprostorov:

- Naj bo $V = \mathbb{R}^2$ (ravnina). Vsi vektorski podprostori V so premice, ki gredo skozi izhodišče, izhodišče samo in cela ravnina. Slednja sta t. i. trivialna podprostora.

Pripomba. $\forall (V, +, \cdot)$ vektorski prostor : $\{0\}, V$ sta vektorska podprostora. Imenujemo ju trivialna vektorska podprostora.

Trditev. Vsak podprostor vsebuje aditivno enoto 0.

Dokaz. Po definiciji je vsak vektorski podprostor neprazen, torej $\exists w \in W$. Polje gotovo vsebuje aditivno enoto 0, torej po aksiomu 3 za podprostore sledi $0 \cdot w \in W$. Dokažimo $0 \cdot w \stackrel{?}{=} 0$: $\cancel{0} \cdot w = (0 + 0) \cdot w = 0 \cdot w + \cancel{0} \cdot w$ (pravilo krajšanja v grupi), torej $0 = 0 \cdot w$. \square

Trditev. Množica rešitev homogene (desna stran je 0) linearne enačbe je vselej vektorski podprostor.

Dokaz. Imamo $\alpha_1 x_1 + \dots + \alpha_n x_n = 0$. Če sta $\vec{a} = (a_1, \dots, a_n)$ in $\vec{b} = (b_1, \dots, b_n)$ rešitvi, velja $\alpha_1 a_1 + \dots + \alpha_n a_n = 0$ in $\alpha_1 b_1 + \dots + \alpha_n b_n = 0$. Vzemimo poljubna $\alpha, \beta \in F$ in si oglejmo $\alpha \vec{a} + \beta \vec{b}$:

$$\alpha (\alpha_1 a_1 + \dots + \alpha_n a_n) + \beta (\alpha_1 b_1 + \dots + \alpha_n b_n) = 0$$

$$\alpha_1 (\alpha a_1 + \beta b_1) + \dots + \alpha_n (\alpha a_n + \beta b_n) = 0$$

Vzemimo koeficiente v oklepajih pred α_i v enačbi pred to vrstico in jih zložimo v vektor. Tedaj je $\alpha \vec{a} + \beta \vec{b} = (\alpha a_1 + \beta b_1, \dots, \alpha a_n + \beta b_n)$ spet rešitev homogene linearne enačbe. Ker je linearna kombinacija elementov vektorskega podprostora spet element vektorskega podprostora, je po definiciji množica rešitev homogene linearne enačbe res vselej vektorski podprostor. \square

Pripomba. Podoben računa velja tudi za množico rešitev sistema linearnih enačb, kar sicer sledi tudi iz naslednje trditve.

Trditev. Presek dveh podprostorov je tudi sam spet podprostor.

Dokaz. Naj bosta W_1, W_2 podprostora v V . Dokažimo, da je $W_1 \cap W_2$ spet podprostor. Vzemimo poljubna $a, b \in W_1 \cap W_2$ in poljubna $\alpha, \beta \in F$. Dokažimo, da je $\alpha a + \beta b \in W_1 \cap W_2$. Vemo, da $a, b \in W_1$ in $a, b \in W_2$. Ker je podprostor po definiciji zaprt za linearne kombinacije svojih elementov, je $\alpha a + \beta b \in W_1$ in $\alpha a + \beta b \in W_2$, torej $\alpha a + \beta b \in W_1 \cap W_2$, torej je presek podprostorov res zaprt za LK svojih elementov in je s tem tudi sam podprostor.

Pripomba. Slednji dokaz lahko očitno posplošimo na več podprostorov. Presek nikdar ni prazen, saj vsi podprostori vsebujejo aditivno enoto 0 (dokaz za to je malce višje). \square

1.6.2 Vsota podprostorov

Definicija. Naj bosta W_1 in W_2 podprostora v V . Vsoto podprostorov W_1 in W_2 označimo z $W_1 + W_2 = \{w_1 + w_2; \forall w_1 \in W_1, w_2 \in W_2\}$.

Trditev. Vsota podprostorov je tudi sama spet podprostor.

Dokaz. Naj bosta $a, b \in W_1 + W_2$ poljubna. Tedaj po definiciji $a = a_1 + a_2$, kjer $a_1 \in W_1$ in $a_2 \in W_2$, in $b = b_1 + b_2$, kjer $b_1 \in W_1$ in $b_2 \in W_2$. $\forall \alpha, \beta \in F$:

$$\alpha a + \beta b = \alpha(a_1 + a_2) + \beta(b_1 + b_2) = \alpha a_1 + \alpha a_2 + \beta b_1 + \beta b_2 = (\alpha a_1 + \beta b_1) + (\alpha a_2 + \beta b_2) \in W_1 + W_2,$$

kajti $(\alpha a_1 + \beta b_1) \in W_1$ in $(\alpha a_2 + \beta b_2) \in W_2$, saj sta to linearni kombinaciji elementov prostorov. Njuna vsota pa je element $W_1 + W_2$ po definiciji vsote podprostorov. \square

1.6.3 Baze

Definicija. Naj bo V vektorski prostor nad poljem F . Množica $\{v_1, \dots, v_n\}$ je baza, če je LN in če je ogrodje.

Definicija. Množica $\{v_1, \dots, v_n\}$ je LN, če za vsake $\alpha_1, \dots, \alpha_n \in F$, ki zadoščajo $\alpha_1 v_1 + \dots + \alpha_n v_n = 0$ velja $\alpha_1 = \dots = \alpha_n = 0$. Ekvivalentni definiciji LN:

- $\{v_1, \dots, v_n\}$ je LN $\Leftrightarrow \forall v \in V$ se da kvečjemu na en način izraziti kot linearno kombinacijo $\{v_1, \dots, v_n\}$.
- $\{v_1, \dots, v_n\}$ je LN $\Leftrightarrow \nexists v \in \{v_1, \dots, v_n\}$, da bi se ga dalo izraziti kot LK preostalih elementov.

Dokaz ekvivalentnosti teh definicij je enak tistemu za $V = \mathbb{R}^n$ višje.

Definicija. Množica $\{v_1, \dots, v_n\}$ je ogrodje $\Leftrightarrow \forall v \in V$ se da na vsaj en način izraziti kot LK te množice $\Leftrightarrow \mathcal{L}in\{v_1, \dots, v_n\} = V$.

Zgled. Primeri baz:

- standardna baza: Naj bo $V = F^n$. $v_1 = (1, 0, 0, \dots, 0, 0)$, $v_2 = (0, 1, 0, \dots, 0, 0)$, ..., $v_n = (0, 0, 0, \dots, 0, 1)$. Da je $\{v_1, \dots, v_n\} \subseteq F^n$ res baza, preverimo z determinanto ($\det A \neq 0 \Leftrightarrow \exists A^{-1} \Leftrightarrow$ stolpci so baza prostora):

$$\det [v_1 \ \dots \ v_n] = 0 \Leftrightarrow \{v_1, \dots, v_n\} \text{ ni baza}$$

- baze v $F[x]_{<n}$ (polinomi stopnje, manjše od n)
 - standardna baza: $\{1, x, x^2, x^3, \dots, x^{n-1}\}$
 - vzemimo paroma različne $\alpha_1, \dots, \alpha_n \in F$ in definirajmo $p_i(x) = (x - \alpha_1) \cdots (x - \alpha_{i-1})(x - \alpha_{i+1}) \cdots (x - \alpha_n)$ za vsak $i \in \{1..n\}$, kar je polinom stopnje $n - 1$. $\{\alpha_1 p_1(x), \dots, \alpha_n p_n(x)\}$ je baza za $F[x]_{<n}$.

Dokaz. Dokazujemo, da so LN in ogrodje: \square

- * LN: $\beta_1 p_1(x) + \dots + \beta_n p_n(x) = 0 \stackrel{?}{\Rightarrow} \beta_1 = \dots = \beta_n = 0$. Opazimo, da $p_i(\alpha_j) = 0 \Leftrightarrow i = j$. Torej če za x vstavimo katerikoli α_i , bodo vsi členi 0, razen $\beta_i p_i(x)$. Ker pa α_i ni ničla $p_i(x)$, je $\beta_i = 0$, čim je $\beta_i p_i(x) = 0$. Preverjati je treba le α_i , ker je dovolj najti eno vrednost spremenljivke, v kateri se vrednosti polinomov ne ujemajo, da lahko rečemo, da polinomi niso isti.
- * ogrodje: Trdimo, da za vsak polinom velja formula $f(x) = \frac{f(\alpha_1)}{p_1(\alpha_1)} p_1(x) + \dots + \frac{f(\alpha_n)}{p_n(\alpha_n)} p_n(x)$. Obe strani enačbe imata stopnjo največ $n - 1$ in se ujemata v n različnih točkah. Če za x vstavimo α_i za vsak i , dobimo 0 v vseh členih, razen v i -tem, kjer se vrednost $f(x)$ ujema z vrednostjo $f(\alpha_i)$.

1.6.4 Obstoje baze

Omejimo se na končno razsežne vektorske prostore.

Definicija. Vektorski prostor je končno razsežen, če ima končno ogrodje: $\exists n \in \mathbb{N} \exists v_1, \dots, v_n \ni V = \mathcal{L}in \{v_1, \dots, v_n\}$.

Izrek. *obstoje baze.* Vsak končno razsežen vektorski prostor ima vsaj eno bazo.

Dokaz. Naj bo V KRVP in naj bo $\{v_1, \dots, v_n\}$ njegovo ogrodje. Ker ogrodje ni nujno LN, naj bo S minimalna/najmanjša podmnožica $\{v_1, \dots, v_n\}$, ki je še ogrodje za V . Trdimo, da je S baza za V . Po konstrukciji je ogrodje, dokažimo še, da je LN: PDDRAA S je linearno odvisna. Tedaj $\exists v_i \in S \ni v_i$ je LK $S \setminus \{v_i\}$. Dokažimo, da je $S \setminus \{v_i\}$ ogrodje manjše moči, kar bi bilo v protislovju s predpostavko. Tedaj obstajajo koeficienti, da velja $v_i = \alpha_1 v_1 + \dots + \alpha_{i-1} v_{i-1} + \alpha_{i+1} v_{i+1} + \dots + \alpha_n v_n$. Vzemimo poljuben $v \in V$. Ker je S ogrodje V , obstajajo neki koeficienti β_1, \dots, β_n , da velja

$$\begin{aligned} v &= \beta_1 v_1 + \dots + \beta_i v_i + \dots + \beta_n v_n = \beta_1 v_1 + \dots + \beta_i (\alpha_1 v_1 + \dots + \alpha_{i-1} v_{i-1} + \alpha_{i+1} v_{i+1} + \dots + \alpha_n v_n) + \dots + \beta_n v_n = \\ &= (\beta_1 + \beta_i \alpha_1) v_1 + \dots + (\beta_{i-1} + \beta_i \alpha_{i-1}) v_{i-1} + (\beta_{i+1} + \beta_i \alpha_{i+1}) v_{i+1} + \dots + (\beta_n + \beta_i \alpha_n) v_n \end{aligned}$$

To pa je \rightarrow , saj je bilo rečeno, da je S najmanjše ogrodje, mi pa smo razvili poljuben v po manjšem ogrodju. Torej ima vsak KRVP bazo in vsako ogrodje ima podmnožico, ki je baza. \square

Trditev 7. enoličnost moči baze. Naj bo V KRVP z n -elementno bazo. Tedaj velja vse to:

1. \forall LN množica A v V ima $\leq n$ elementov
2. \forall ogrodje v V ima $\geq n$ elementov
3. \forall baza v V ima n elementov

Dokaz. Dokaz je dolg.

Lema 1. Vsak poddoločen homogen sistem linearnih enačb ima netrivialno rešitev.

Dokaz. Dokaz se nahaja pod identično trditvijo 4 na strani 11. \square

Lema 2. Če je u_1, \dots, u_m LN množica v V in v_1, \dots, v_n ogrodje za V , je $m \leq n$. ZDB moč katerekoli LN množice je manjša ali enaka od kateregakoli ogrodja v V .

Dokaz. RAAPDD u_1, \dots, u_m je LN, v_1, \dots, v_n je ogrodje in $m > n$. Iščemo protislovje. Vsakega od u_i lahko razvijemo po v .

$$\begin{array}{ccccccc} u_1 & = & \alpha_{11} v_1 & + & \dots & + & \alpha_{1n} v_n \\ \vdots & & \vdots & & & & \vdots \\ u_m & = & \alpha_{m1} v_1 & + & \dots & + & \alpha_{mn} v_n \end{array}$$

$\forall i \in \{1..m\}$ pomnožimo i -to enačbo s skalarjem x_i in jih seštejmo. \vec{x} so abstraktne spremenljivke. Tedaj:

$$\begin{aligned} x_1 u_1 + \dots + x_m u_m &= x_1 (\alpha_{11} v_1 + \dots + \alpha_{1n} v_n) + \dots + x_m (\alpha_{m1} v_1 + \dots + \alpha_{mn} v_n) = \\ &= v_1 (\alpha_{11} x_1 + \dots + \alpha_{m1} x_m) + \dots + v_n (\alpha_{1n} x_1 + \dots + \alpha_{mn} x_m) \end{aligned}$$

Izenačimo koeficiente za v_i z 0 in dobimo poddoločen homogen sistem enačb (ima n enačb in m spremenljivk, po predpostavki pa velja $m > n$):

$$\begin{array}{ccccccc} \alpha_{11}x_1 & + & \cdots & + & \alpha_{m1}x_m & = & 0 \\ \vdots & & & & \vdots & & \vdots \\ \alpha_{1n}x_1 & + & \cdots & + & \alpha_{mn}x_m & = & 0 \end{array}$$

Po lemi 1 na prejšnji strani ima ta sistem netrivialno rešitev, recimo (μ_1, \dots, μ_m) . Če to rešitev vstavimo v $u_1x_1 + \dots + u_mx_m$, dobimo $u_1\mu_1 + \dots + u_m\mu_m = 0$. Ker so u_1, \dots, u_m LN, so $\mu_1 = \dots = \mu_m = 0$, kar je v --- s predpostavko. \square

1. \forall baza je ogrodje \Rightarrow po lemi 2 na prejšnji strani velja, da ima vsaka LN množica manj ali enako elementov kot vsako ogrodje, torej tudi manj ali enako kot n .
2. \forall baza je LN \Rightarrow po lemi 2 na prejšnji strani velja, da ima vsako ogrodje več ali enako elementov kot vsaka LN, torej tudi več ali enako kot n .
3. Sledi iz zgornjih dveh točk, saj je baza tako ogrodje kot LN hkrati.

\square

Definicija. Naj bo V KRVP. Njegova dimenzija, $\dim V$, je moč baze v V .

Zgled. $\dim F^n = n$, $\dim M_{m \times n}(\mathbb{F}) = m \cdot n$.

1.6.5 Dopolnitev LN množice do baze

Trditve. Naj bo V vektorski prostor z dimenzijo n . Trdimo, da

1. ima vsaka LN množica $\leq n$ elementov,
2. je vsaka LN množica v V z n elementi baza,
3. lahko vsako LN množico v V dopolnimo do baze.

Dokaz. Dokaz je dolg

Lema 1. Če so $v_1, \dots, v_m \in V$ LN in če $v_{m+1} \notin \mathcal{L}\text{in}\{v_1, \dots, v_m\}$, potem so tudi v_1, \dots, v_m, v_{m+1} LN.

Dokaz. Naj velja $\alpha_1v_1 + \dots + \alpha_{m+1}v_{m+1} = 0$ za nek $\vec{\alpha} \in F^{m+1}$. Dokažimo $\vec{\alpha} = \vec{0}$. Če $\alpha_{m+1} = 0$, sledi $\alpha_1v_1 + \dots + \alpha_mv_m = 0$, ker pa so po predpostavki v_1, \dots, v_m LN, je $\vec{\alpha} = \vec{0}$. Sicer pa, če PDDRAA $\alpha_{m+1} \neq 0$, lahko z α_{m+1} delimo:

$$\begin{aligned} \alpha_1v_1 + \dots + \alpha_{m+1}v_{m+1} &= 0 \\ \alpha_{m+1}v_{m+1} &= -\alpha_1v_1 - \dots - \alpha_mv_m \\ v_{m+1} &= \frac{-\alpha_1}{\alpha_{m+1}}v_1 + \dots + \frac{-\alpha_m}{\alpha_{m+1}}v_m \end{aligned}$$

Tedaj pridemo do --- , saj smo v_{m+1} izrazili kot LK $\{v_1, \dots, v_m\}$, po predpostavki pa je vendar $v_{m+1} \notin \mathcal{L}\text{in}\{v_1, \dots, v_m\}$. \square

1. že dokazano z dokazom trditve 7 na prejšnji strani v razdelku 1.6.4.

2. Vsaka LN množica v V z n elementi je baza. PDDRAA v_1, \dots, v_n je LN, ki ni baza. Tedaj v_1, \dots, v_n ni ogrodje. Tedaj $\mathcal{L}\text{in}\{v_1, \dots, v_n\} \neq V$. Zatorej $\exists v_{n+1} \in V \ni: \{v_1, \dots, v_n, v_{n+1}\}$ je LN, kar je v \dashv s trditvijo, da ima vsaka LN množica v V kvečjemu n elementov.
3. Vsako LN množico v V z n elementi lahko dopolnimo do baze. Naj bo v_1, \dots, v_m LN množica v V . Vemo, da je $m \leq n$. Če $m = n$, je v_1, \dots, v_m baza po zgornji trditvi. Sicer pa je $m < n$: Tedaj v_1, \dots, v_m ni ogrodje, sicer bi imeli neko LN množico z več elementi kot neko ogrodje, saj ima po popraj dokazanem vsako ogrodje vsaj toliko elementov kot vsaka LN množica. Ker v_1, \dots, v_m ni ogrodje, $\exists v_{m+1} \notin \mathcal{L}\text{in}\{v_1, \dots, v_m\}$. Po lemi 1 je torej v_1, \dots, v_{m+1} LN množica. Če je $m + 1 = n$, je to že baza, sicer ponavljamo dodajanje elementov, dokler ne dodamo k elementov in dosežemo $m + k = n$. Tedaj je to baza. Naredili smo $k = m - n$ korakov.

Uporabna vrednost tega izreka sta dva nova izreka o dimenzijah podprostorov: □

Trditev. Če je V je KRVP in W njegov podprostor, je $\dim W \leq \dim V$.

Dokaz. PDDRAA $\dim W > \dim V$. Čim ima baza W večjo moč kot baza V , obstaja v W LN množica z večjo močjo kot baza V . Toda ker je ta LN množica LN tudi v V , obstaja v V LN množica z več elementi kot baza V , kar je v \dashv s trditvijo 7 na strani 31 v razdelku 1.6.4. □

Trditev. dimenzijska formula za podprostore. Naj bo V KRVP in W_1, W_2 podprostora v V . Velja $\dim(W_1 + W_2) = \dim W_1 + \dim W_2 - \dim(W_1 \cap W_2)$. Vsota vektorskih podprostorov je definirana v razdelku 1.6.2 na strani 30.

Dokaz. Izberimo bazo w_1, \dots, w_m za $W_1 \cap W_2$. Naj bo u_1, \dots, u_k njena dopolnitev do baze W_1 in v_1, \dots, v_l njena dopolnitev do baze W_2 . Trdimo, da je $w_1, \dots, w_m, u_1, \dots, u_k, v_1, \dots, v_l$ baza za $W_1 + W_2$. Tedaj bi namreč veljalo $\dim(W_1 + W_2) = m + k + l$, $\dim(W_1 \cap W_2) = m$, $\dim(W_1) = m + k$ in $\dim(W_2) = m + l$. Treba je dokazati še, da je $w_1, \dots, w_m, u_1, \dots, u_k, v_1, \dots, v_l$ baza za $W_1 + W_2$.

- Je ogrodje? Vzemimo poljuben $v \in W_1 + W_2$. Po definiciji $W_1 + W_2 \exists z_1 \in W_1, z_2 \in W_2 \ni: v = z_1 + z_2$. Razvijmo z_1 po bazi $w_1, \dots, w_m, u_1, \dots, u_k$ za W_1 in z_2 po bazi $w_1, \dots, w_m, v_1, \dots, v_l$ za W_2 . Takole: $z_1 = \alpha_1 w_1 + \dots + \alpha_m w_m + \beta_1 u_1 + \dots + \beta_k u_k$ in $z_2 = \gamma_1 w_1 + \dots + \gamma_m w_m + \delta_1 v_1 + \dots + \delta_l v_l$. Torej $v = z_1 + z_2 = (\alpha_1 + \gamma_1) w_1 + \dots + (\alpha_m + \gamma_m) w_m + \beta_1 u_1 + \dots + \beta_k u_k + \delta_1 v_1 + \dots + \delta_l v_l \in \mathcal{L}\text{in}\{w_1, \dots, w_m, u_1, \dots, u_k, v_1, \dots, v_l\}$. Je ogrodje.
- Je LN? Naj bo

$$\begin{aligned} \alpha_1 w_1 + \dots + \alpha_m w_m + \beta_1 u_1 + \dots + \beta_k u_k + \gamma_1 v_1 + \dots + \gamma_l v_l &= 0 \\ \alpha_1 w_1 + \dots + \alpha_m w_m + \beta_1 u_1 + \dots + \beta_k u_k &= (-\gamma_1) v_1 + \dots + (-\gamma_l) v_l \end{aligned}$$

Leva stran enačbe je $\in W_1$, desna pa $\in W_2$, zatorej je element, ki ga izraza na obeh straneh enačbe opisujeta, $\in W_1 \cap W_2$. Torej je v_1, \dots, v_l baza za $W_1 \cap W_2$. Toda baza od $W_1 \cap W_2$ je tudi w_1, \dots, w_m , zatorej lahko ta element razpišemo po njej:

$$\begin{aligned} (-\gamma_1) v_1 + \dots + (-\gamma_l) v_l &= \delta_1 w_1 + \dots + \delta_m w_m \\ \delta_1 w_1 + \dots + \delta_m w_m + \gamma_1 v_1 + \dots + \gamma_l v_l &= 0 \end{aligned}$$

Toda $w_1, \dots, w_m, v_1, \dots, v_l$ je baza za W_2 po naši prejšnji definiciji, torej je LN množica, zato $\delta_1 = \dots = \delta_m = \gamma_1 = \dots = \gamma_l = 0$. Ker $\gamma_1 = \dots = \gamma_l = 0$, se lahko vrnemo k drugi enačbi te točke in to ugotovitev upoštevamo:

$$\begin{aligned} \alpha_1 w_1 + \dots + \alpha_m w_m + \beta_1 u_1 + \dots + \beta_k u_k &= (-\gamma_1) v_1 + \dots + (-\gamma_l) v_l \\ \alpha_1 w_1 + \dots + \alpha_m w_m + \beta_1 u_1 + \dots + \beta_k u_k &= 0 \end{aligned}$$

Toda $w_1, \dots, w_m, u_1, \dots, u_k$ je baza za W_1 po naši prejšnji definiciji, torej je LN množica, zato $\alpha_1 = \dots = \alpha_m = \beta_1 = \dots = \beta_k = 0$. Torej velja $\alpha_1 = \dots = \alpha_m = \beta_1 = \dots = \beta_k = \gamma_1 = \dots = \gamma_l = 0$, torej je ta množica res LN. □

Posledica. Velja torej $\dim(W_1 + W_2) = \dim(W_1) + \dim(W_2)$. Enačaj velja $\Leftrightarrow W_1 \cap W_2 = \{0\}$, kajti $\dim(\{0\}) = 0$.

Definicija 2. Pravimo, da je vsota $W_1 + W_2$ direktna, če velja $W_1 \cap W_2 = \{0\}$ oziroma ekvivalentno če je $\dim(W_1 + W_2) = \dim W_1 + \dim W_2$ oziroma ekvivalentno $\forall w_1 \in W_1, w_2 \in W_2 : w_1 + w_2 = 0 \Rightarrow w_1 = w_2 = 0$.

1.6.6 Prehod na novo bazo

Naj bo V vektorski prostor dimenzije n . Recimo, da imamo dve bazi v V . $B = \{u_1, \dots, u_n\}$ naj bo „stara baza“, $C = \{v_1, \dots, v_n\}$ pa naj bo „nova baza“. $\forall v \in V$ lahko razvijemo po B in po C . Razvoj po B : $v = \beta_1 u_1 + \dots + \beta_n u_n$, razvoj po C : $v = \gamma_1 v_1 + \dots + \gamma_n v_n$. Kakšna je zveza med $\vec{\beta}$ in $\vec{\gamma}$ v obeh razvojih?

Uvedimo oznako $[v]_B$, to naj bodo koeficienti vektorja v pri razvoju po B . $[v]_B = \begin{bmatrix} \beta_1 \\ \vdots \\ \beta_n \end{bmatrix}$.

Vsak vektor stare baze razvijmo po novi bazi, kjer $[u_i]_C = \begin{bmatrix} \alpha_{i1} \\ \vdots \\ \alpha_{in} \end{bmatrix}$:

$$\begin{array}{rcccc} u_1 & = & \alpha_{11}v_1 & + \cdots + & \alpha_{1n}v_n \\ \vdots & & \vdots & & \vdots \\ u_n & = & \alpha_{n1}v_1 & + \cdots + & \alpha_{nn}v_n \end{array}$$

Koeficiente α zložimo v tako imenovani prehodno matriko $P_{C \leftarrow B}$:

$$P_{C \leftarrow B} = [[u_1]_C \quad \cdots \quad [u_n]_C] = \begin{bmatrix} \alpha_{11} & \cdots & \alpha_{n1} \\ \vdots & & \vdots \\ \alpha_{1n} & \cdots & \alpha_{nn} \end{bmatrix}$$

Sledi

$$\begin{aligned} v &= \beta_1 u_1 + \dots + \beta_n u_n = \beta_1 (\alpha_{11}v_1 + \dots + \alpha_{1n}v_n) + \dots + \beta_n (\alpha_{n1}v_1 + \dots + \alpha_{nn}v_n) = \\ &= v_1 (\beta_1 \alpha_{11} + \beta_2 \alpha_{21} + \dots + \beta_n \alpha_{n1}) + \dots + v_n (\beta_1 \alpha_{1n} + \beta_2 \alpha_{2n} + \dots + \beta_n \alpha_{nn}) = \end{aligned}$$

po drugi strani je v tudi lahko razvit po novi bazi:

$$= v = \gamma_1 v_1 + \dots + \gamma_n v_n$$

Iz česar, ker je razvoj po bazi enoličen, sledi

$$\begin{array}{rcccc} \gamma_1 & = & \beta_1 \alpha_{11} & + \cdots + & \beta_n \alpha_{n1} \\ \vdots & & \vdots & & \vdots \\ \gamma_n & = & \beta_1 \alpha_{1n} & + \cdots + & \beta_n \alpha_{nn} \end{array},$$

kar v matrični obliki zapišemo

$$\begin{bmatrix} \alpha_{11} & \cdots & \alpha_{n1} \\ \vdots & & \vdots \\ \alpha_{1n} & \cdots & \alpha_{nn} \end{bmatrix} \begin{bmatrix} \beta_1 \\ \vdots \\ \beta_n \end{bmatrix} = \begin{bmatrix} \gamma_1 \\ \vdots \\ \gamma_n \end{bmatrix}$$

$$P_{C \leftarrow B} [v]_B = [v]_C.$$

Pripomba. Velja:

- $P_{B \leftarrow B} = I$.
- Naj bodo prehodi med bazami takšni: $B \xrightarrow{P_{C \leftarrow B}} C \xrightarrow{P_{D \leftarrow C}} D$. Potem je $P_{D \leftarrow B} = P_{C \leftarrow B} \cdot P_{D \leftarrow C}$.

- $P_{B \leftarrow C} \cdot P_{C \leftarrow B} = I, (P_{B \leftarrow C})^{-1} = P_{C \leftarrow B}$.

- Naj bo $v \in F^n$ in S standardna baza za F^n . Potem $[v]_S = \begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{bmatrix} = v$. Sledi $P_{S \leftarrow B} = [[u_1]_S \ \cdots \ [u_n]_S] = [u_1 \ \cdots \ u_n]$ za $B = \{u_1, \dots, u_n\}$. Sledi tudi $P_{S \leftarrow C} = [v_1 \ \cdots \ v_n]$, kjer so v, u, B, C kot prej (kot definirano na začetku tega razdelka).

- $P_{C \leftarrow B} = P_{C \leftarrow S} \cdot P_{S \leftarrow B}$ (slednji dve točki veljata samo v F^n , kjer je standardna baza lepa in zapisljiva kot elementi v matriki)

2 Drugi semester

2.1 Linearne preslikave

Radi bi definirali homomorfizem vektorskih prostorov. Homomorfizem za abelove grupe smo že definirali, vektorski prostor pa je le abelova grupa z dodatno strukturo (množenje s skalarjem).

Definicija. Preslikava $f : V_1 \rightarrow V_2$ je homomorfizem vektorskih prostorov nad istim poljem oziroma linearna preslikava, če je aditivna (homomorfizem) ($\forall u, v \in V_1 : f(u + v) = f(u) + f(v)$) in če je homogena: $\forall u \in V_1, \alpha \in F : f(\alpha u) = \alpha f(u)$.

Pripomba. Ekvivalentno je preverjati oba pogoja hkrati. Če za $L : U \rightarrow V$ velja $\forall \alpha_1, \alpha_2 \in F, u_1, u_2 \in U : L(\alpha_1 u_1 + \alpha_2 u_2) = \alpha_1 L u_1 + \alpha_2 L u_2$, je L linearna preslikava.

Zgled. Vrtež za kot τ v ravnini:

$$\begin{bmatrix} x \\ y \end{bmatrix} \rightarrow \begin{bmatrix} \cos \tau & -\sin \tau \\ \sin \tau & \cos \tau \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}$$

Zgled. Linearna funkcija iz analize ni linearna preslikava. Premik za vektor w ni linearna preslikava. Odvajanje in integriranje sta linearni preslikavi.

Dejstvo. Vsaka linearna preslikava slika 0 v 0.

Definicija. Bijektivni linearni preslikavi pravimo linearni izomorfizem.

Trditev 3. Inverz linearnega izomorfizma je zopet linearni izomorfizem.

Dokaz. Naj bo $L : U \rightarrow V$ bijektivna linearna preslikava med vektorskima prostoroma nad istim poljem F . Dokazati je treba, da je $L^{-1} : V \rightarrow U$ spet linearna preslikava. Ker je L linearna, velja

$$\forall \alpha_1, \alpha_2 \in F, v_1, v_2 \in V : L(\alpha_1 L^{-1} v_1 + \alpha_2 L^{-1} v_2) = \alpha_1 L L^{-1} v_1 + \alpha_2 L L^{-1} v_2 = L L^{-1}(\alpha_1 v_1 + \alpha_2 v_2)$$

Ker je L injektivna, iz $L(\alpha_1 L^{-1} v_1 + \alpha_2 L^{-1} v_2) = L L^{-1}(\alpha_1 v_1 + \alpha_2 v_2)$ sledi $\alpha_1 L^{-1} v_1 + \alpha_2 L^{-1} v_2 = L^{-1}(\alpha_1 v_1 + \alpha_2 v_2)$. \square

2.1.1 F^n je linearno izomorfen n -razsežnem V nad F

Trditve. Vsak n -razsežen vektorski prostor nad F je linearno izomorfen F^n .

Dokaz. Naj bo V n -razsežen vektorski prostor nad F in $B = \{v_1, \dots, v_n\}$ baza za V . Definirajmo preslikavo $\phi_B : F^n \rightarrow V$ s predpisom $(x_1, \dots, x_n) \mapsto x_1v_1 + \dots + x_nv_n$. Ker je B ogrodje, je ϕ_B surjektivna. Ker je B linearno neodvisna, je ϕ_B injektivna. Pokažimo še, da je linearna preslikava:

$$\begin{aligned} \phi_B(\alpha(x_1, \dots, x_n) + \beta(y_1, \dots, y_n)) &= \phi_B(\alpha x_1 + \beta y_1, \dots, \alpha x_n + \beta y_n) = v_1(\alpha x_1 + \beta y_1) + \dots + v_n(\alpha x_n + \beta y_n) = \\ &= \alpha(v_1x_1 + \dots + v_nx_n) + \dots + \beta(v_1y_1 + \dots + v_ny_n) = \alpha\phi_B(x_1, \dots, x_n) + \beta\phi_B(y_1, \dots, y_n) \end{aligned}$$

□

2.1.2 Matrika linearne preslikave — linearni izomorfizem $M_{m,n}(F) \rightarrow \mathcal{L}(F^n, F^m)$

Trditve. Naj bo F polje in $m, n \in F$. $\mathcal{L}(F^n, F^m)$ je vektorski prostor linearnih preslikav iz $F^n \rightarrow F^m$. Seštevanje definiramo z $(L_1 + L_2)u := L_1u + L_2u$, množenje s skalarjem pa $(\alpha L)u = \alpha(Lu)$. Naj bo $M_{m,n}(F)$ vektorski prostor vseh $m \times n$ matrik nad F z znanim seštevanjem in množenjem. Obstaja linearni izomorfizem med tema dvema prostoroma.

Dokaz. Označe kot v trditvi. Za vsako $m \times n$ matriko $A = [a_{i,j}]$ definirajmo preslikavo L_A iz F^n v F^m takole: $L_A(x_1, \dots, x_n) = (a_{1,1}x_1 + \dots + a_{1,n}x_n, \dots, a_{m,1}x_1 + \dots + a_{m,n}x_n)$. Po definiciji matričnega množenja ta preslikava ustreza $L_A\vec{x} = A\vec{x}$. Dokažimo, da je linearni izomorfizem.

- Linearnost: $L_{\alpha A + \beta B}\vec{x} = (\alpha A + \beta B)\vec{x} = \alpha A\vec{x} + \beta B\vec{x} = \alpha L_A\vec{x} + \beta L_B\vec{x} = (\alpha L_A + \beta L_B)\vec{x}$
- Bijektivnost: Konstruirajmo inverzno preslikavo (iz trditve 3 vemo, da bo linearna). Vsaki linearni preslikavi $L : F^n \rightarrow F^m$ priredimo $m \times n$ matriko $[Le_1 \ \dots \ Le_n]$, kjer je e_1, \dots, e_n standardna baza za F^n . Pokažimo, da je ta preslikava res inverz, torej preverimo, da je kompozitum $A \mapsto L_A \mapsto [Le_1 \ \dots \ Le_n]$ identiteta in da je $[Le_1 \ \dots \ Le_n] \mapsto L_A \mapsto A$ tudi identiteta.

$$- \underline{\underline{A \mapsto L_A \mapsto [Le_1 \ \dots \ Le_n] \stackrel{?}{=} id:}}$$

$$[Le_1 \ \dots \ Le_n] = [Ae_1 \ \dots \ Ae_n] = A[e_1 \ \dots \ e_n] = AI = A$$

$$- \underline{\underline{[Le_1 \ \dots \ Le_n] \mapsto L_A \mapsto A \stackrel{?}{=} id:}}$$

$$\forall x : L[Le_1 \ \dots \ Le_n]x = [Le_1 \ \dots \ Le_n] \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} = x_1Le_1 + \dots + x_nLe_n = L(x_1e_1 + \dots + x_ne_n) =$$

$$= L \left(x_1 \begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix} + \dots + x_n \begin{bmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{bmatrix} \right) = Lx$$

Vsaki linearni preslikavi med dvema vektorskima prostoroma sedaj lahko priredimo matriko. Prirejanje je odvisno od izbire baz v obeh vektorskih prostorih. Matrika namreč preslika koeficiente iz polja F , s katerimi je dan vektor, ki ga z leve množimo z matriko, razvit po „vhodni“ bazi, v koeficiente iz istega polja, s katerimi je rezultatni vektor razvit po „izhodni“ bazi.

Naj bosta U in V vektorska prostora nad istim poljem F in naj bo $L : U \rightarrow V$ linearna preslikava. Izberimo bazo $\mathcal{B} = \{u_1, \dots, u_n\}$ za U in $\mathcal{C} = \{v_1, \dots, v_m\}$ za V . Razvijmo vektorje Lu_1, \dots, Lu_n po bazi \mathcal{C} :

$$\begin{aligned} Lu_1 &= \alpha_{1,1}v_1 + \cdots + \alpha_{1,m}v_m \\ &\vdots \\ Lu_n &= \alpha_{n,1}v_1 + \cdots + \alpha_{n,m}v_m \end{aligned}$$

Skalarje $\alpha_{i,j}$ sedaj zložimo v spodnjo matriko, ki ji pravimo **matrika linearne preslikave L glede na bazi \mathcal{B} in \mathcal{C}** .

$$[L]_{\mathcal{C} \leftarrow \mathcal{B}} = [[Lu_1]_{\mathcal{C}} \quad \cdots \quad [Lu_n]_{\mathcal{C}}] = \begin{bmatrix} \alpha_{1,1} & \cdots & \alpha_{1,m} \\ \vdots & & \vdots \\ \alpha_{n,1} & \cdots & \alpha_{n,m} \end{bmatrix}$$

□

Zgled. $L : \mathbb{R}[x]_{\leq 3} \rightarrow \mathbb{R}[x]_{\leq 2}$ — linearna preslikava iz realnih polinomov stopnje kvečjemu 3 v realne polinome stopnje kvečjemu 2, ki predstavlja odvajanje polinomov. Bazi sta $\mathcal{B} = \{1, x, x^2, x^3\}$ in $\mathcal{C} = \{1, x, x^2\}$.

$$\begin{aligned} L(1) &= 0 + 0x + 0x^2 \\ L(x) &= 1 + 0x + 0x^2 \\ L(x^2) &= 0 + 2x + 0x^2 \\ L(x^3) &= 0 + 0x + 3x^2 \end{aligned}$$

Zapišimo matriko te linearne preslikave:

$$[L]_{\mathcal{C} \leftarrow \mathcal{B}} = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 3 \end{bmatrix}$$

Zgled. Prehodna matrika je poseben primer matrike linearne preslikave. $L : V \rightarrow V$ z bazama $\mathcal{B} = \{v_1, \dots, v_n\}$ in $\mathcal{C} = \{u_1, \dots, u_n\}$, kjer $L = id$.

$$\begin{aligned} id(u_1) &= \alpha_{1,1}v_1 + \cdots + \alpha_{1,n}v_n \\ &\vdots \\ id(u_n) &= \alpha_{n,1}v_1 + \cdots + \alpha_{n,n}v_n \end{aligned}$$

Zapišimo matriko te linearne preslikave: $[id]_{\mathcal{C} \leftarrow \mathcal{B}} = P_{\mathcal{C} \leftarrow \mathcal{B}}$.

2.1.3 Lastnosti matrik linearnih preslikav

Izrek 1. osnovna formula. Posplošitev formule $[u]_{\mathcal{C}} = P_{\mathcal{C} \leftarrow \mathcal{B}} \cdot [u]_{\mathcal{B}}$ se glasi $[Lu]_{\mathcal{C}} = [L]_{\mathcal{C} \leftarrow \mathcal{B}} [u]_{\mathcal{B}}$ za linearno preslikavo $L : U \rightarrow V$, $u \in U$, kjer je $\mathcal{B} = \{u_1, \dots, u_n\}$ baza za U in $\mathcal{C} = \{v_1, \dots, v_m\}$ baza za V .

Dokaz. Po korakih:

1. Razvijmo u po bazi \mathcal{B} : $u = \beta_1 u_1 + \cdots + \beta_n u_n$.
2. Uporabimo L na obeh straneh: $Lu = L(\beta_1 u_1 + \cdots + \beta_n u_n) = \beta_1 Lu_1 + \cdots + \beta_n Lu_n$.
3. Razvijmo bazo \mathcal{B} , preslikano z L , po bazi \mathcal{C} :

$$\begin{aligned} Lu_1 &= \alpha_{1,1}v_1 + \cdots + \alpha_{1,m}v_m \\ &\vdots \\ Lu_n &= \alpha_{n,1}v_1 + \cdots + \alpha_{n,m}v_m \end{aligned}$$

4. Razvoj vstavimo v enačbo iz koraka 2 in uredimo:

$$\begin{aligned} Lu &= \beta_1 (\alpha_{1,1}v_1 + \dots + \alpha_{1,m}v_m) + \dots + \beta_n (\alpha_{n,1}v_1 + \dots + \alpha_{n,m}v_m) = \\ &= v_1 (\beta_1\alpha_{1,1} + \dots + \beta_n\alpha_{n,1}) + \dots + v_m (\beta_1\alpha_{1,m} + \dots + \beta_n\alpha_{n,m}v_m) \end{aligned}$$

5. Odtod sledi:

$$[Lu]_{\mathcal{C}} = \begin{bmatrix} \beta_1\alpha_{1,1} + \dots + \beta_n\alpha_{n,1} \\ \vdots \\ \beta_1\alpha_{1,m} + \dots + \beta_n\alpha_{n,m}v_m \end{bmatrix} = \begin{bmatrix} \alpha_{1,1} & \dots & \alpha_{n,1} \\ \vdots & & \vdots \\ \alpha_{1,m} & \dots & \alpha_{n,m} \end{bmatrix} \begin{bmatrix} \beta_1 \\ \vdots \\ \beta_n \end{bmatrix} = [L]_{\mathcal{C} \leftarrow \mathcal{B}} [u]_{\mathcal{B}}$$

□

Izrek 2. matrika kompozituma linearnih preslikav. Posplošitev formule $P_{\mathcal{D} \leftarrow \mathcal{B}} = P_{\mathcal{D} \leftarrow \mathcal{C}} \cdot P_{\mathcal{C} \leftarrow \mathcal{B}}$ se glasi $[K \circ L]_{\mathcal{D} \leftarrow \mathcal{B}} = [K]_{\mathcal{D} \leftarrow \mathcal{C}} \cdot [L]_{\mathcal{C} \leftarrow \mathcal{B}}$. Trdimo, da je kompozitum linearnih preslikav spet linearna preslikava in da enačba velja.

Dokaz. Najprej dokažimo, da je kompozitum linearnih preslikav spet linearna preslikava.

$$(K \circ L)(\alpha u + \beta v) = K(L(\alpha u + \beta v)) = K(\alpha Lu + \beta Lv) = \alpha KLu + \beta KLv = \alpha(K \circ L)u + \beta(K \circ L)v$$

Sedaj pa dokažimo še enačbo $[K \circ L]_{\mathcal{D} \leftarrow \mathcal{B}} = [K]_{\mathcal{D} \leftarrow \mathcal{C}} \cdot [L]_{\mathcal{C} \leftarrow \mathcal{B}}$. Naj bosta $L : U \rightarrow V$ in $K : V \rightarrow W$ linearni preslikavi, $\mathcal{B} = \{u_1, \dots, u_n\}$ baza U , \mathcal{C} baza V in \mathcal{D} baza W . Od prej vemo, da:

$$[L]_{\mathcal{D} \leftarrow \mathcal{B}} = [[Lu_1]_{\mathcal{D}} \quad \dots \quad [Lu_n]_{\mathcal{D}}],$$

zato pišimo

$$\begin{aligned} [K \circ L]_{\mathcal{D} \leftarrow \mathcal{B}} &= [[(K \circ L)u_1]_{\mathcal{D}} \quad \dots \quad [(K \circ L)u_n]_{\mathcal{D}}] = [[KLu_1]_{\mathcal{D}} \quad \dots \quad [KLu_n]_{\mathcal{D}}] \stackrel{\text{izrek 1}}{=} \\ &\stackrel{\text{izrek 1}}{=} [[K]_{\mathcal{D} \leftarrow \mathcal{C}} [Lu_1]_{\mathcal{C}} \quad \dots \quad [K]_{\mathcal{D} \leftarrow \mathcal{C}} [Lu_n]_{\mathcal{C}}] = [K]_{\mathcal{D} \leftarrow \mathcal{C}} [[Lu_1]_{\mathcal{C}} \quad \dots \quad [Lu_n]_{\mathcal{C}}] = [K]_{\mathcal{D} \leftarrow \mathcal{C}} [L]_{\mathcal{C} \leftarrow \mathcal{B}} \end{aligned}$$

□

2.1.4 Jedro in slika linearne preslikave

Definicija. Naj bosta U in V vektorska prostora nad istim poljem F in $L : U \rightarrow V$ linearna preslikava. Jedro L naj bo $\text{Ker } L := \{u \in U; Lu = 0\}$ (angl. kernel/null space) in Slika/zaloga vrednosti L naj bo $\text{Im } L := \{Lu; \forall u \in U\}$ (angl. image/range).

Trditev. Trdimo naslednje:

1. $\text{Ker } L$ je vektorski podprostor v U (če vsebuje \vec{a} in \vec{b} , vsebuje tudi vse $LK \vec{a}$ in \vec{b})
2. $\text{Ker } L$ je vektorski podprostor v V .

Dokaz. Dokazujemo dve trditvi:

1. $\forall u_1, u_2 \in \text{Ker } L, \alpha_1, \alpha_2 \in F \stackrel{?}{\implies} \alpha_1 u_1 + \alpha_2 u_2 \in \text{Ker } L$. Po predpostavki velja $Lu_1 = 0$ in $Lu_2 = 0$, torej $\alpha_1 Lu_1 + \alpha_2 Lu_2 = 0$. Iz linearnosti L sledi $L(\alpha_1 u_1 + \alpha_2 u_2) = 0$, torej $\alpha_1 u_1 + \alpha_2 u_2 \in \text{Ker } L$.
2. $\forall v_1, v_2 \in \text{Ker } L, \beta_1, \beta_2 \in F \stackrel{?}{\implies} \beta_1 v_1 + \beta_2 v_2 \in \text{Ker } L$. Po predpostavki velja $\exists u_1, u_2 \in U \ni v_1 = Lu_1 \wedge v_2 = Lu_2$. Velja torej $\beta_1 v_1 + \beta_2 v_2 = \beta_1 Lu_1 + \beta_2 Lu_2 \stackrel{\text{linearnost}}{=} L(\beta_1 u_1 + \beta_2 u_2)$ in $\beta_1 u_1 + \beta_2 u_2 \in U$, torej je $L(\beta_1 u_1 + \beta_2 u_2) \in \text{Ker } L$.

□

Definicija. Ničnost L je $n(L) := \dim \text{Ker } L$ (angl. nullity) in rang L je $\text{rang } L = \dim \text{Ker } L$ (angl. rank).

Pripomba. Jedro in sliko smo definirali za linearne preslikave, vendar ju lahko definiramo tudi za poljubno matriko A nad poljem F , saj smo v 2.1.2 dokazali linearni izomorfizem med $m \times n$ matrikami nad F in linearnimi preslikavami $F^n \rightarrow F^m$.

$$Au = \begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{m1} & \cdots & a_{mn} \end{bmatrix} \begin{bmatrix} u_1 \\ \vdots \\ u_n \end{bmatrix} = \begin{bmatrix} a_{11}u_1 + \cdots + a_{1n}u_n \\ \vdots \\ a_{m1}u_1 + \cdots + a_{mn}u_n \end{bmatrix} = \begin{bmatrix} a_{11} \\ \vdots \\ a_{m1} \end{bmatrix} u_1 + \cdots + \begin{bmatrix} a_{1n} \\ \vdots \\ a_{mn} \end{bmatrix} u_n$$

Iz tega je razvidno, da je $\text{Ker } A$ torej linearna ogrinjača stolpcev matrike A . Pravimo tudi, da je $\text{Ker } A$ stolpični prostor A oziroma $\text{Col } A$ (angl. column space). $\text{rang } A = \dim \text{Ker } A$ je torej največje število linearno neodvisnih stolpcev A .

Trditev. Linearna preslikava L je injektivna ($Lu_1 = Lu_2 \Rightarrow u_1 = u_2$) $\Leftrightarrow \text{Ker } L = \{0\}$.

Dokaz. Dokazujemo ekvivalenco:

- (\Rightarrow) Predpostavimo, da je L injektivna, torej $Lu_1 = Lu_2 \Rightarrow u_1 = u_2$. Vzemimo poljuben $u \in \text{Ker } L$. Zanj velja $Lu = 0 = L0 \Rightarrow u = 0$.
- (\Leftarrow) Predpostavimo, $\text{Ker } L = \{0\}$. Računajmo: $Lu_1 = Lu_2 \Rightarrow Lu_1 - Lu_2 = 0 \xrightarrow{\text{linearnost}} L(u_1 - u_2) = 0 \Rightarrow u_1 - u_2 = 0 \Rightarrow u_1 = u_2$.

□

Izrek. osnovna formula. Naj bo $L : U \rightarrow V$ linearna preslikava. Tedaj je $\dim \text{Ker } L + \dim \text{rang } L = \dim U$, torej $nL + \text{rang } L = \dim U$. Za matrike torej trdimo $nA + \text{rang } A = \dim F^n = n$ za $m \times n$ matriko A .

Dokaz. Vemo, da sta jedro in slika podprostora. Naj bo w_1, \dots, w_k baza jedra in u_1, \dots, u_l njena dopolnitev do baze U . Torej $\dim U = k + l = nL + l$. Treba je še dokazati, da je $l = \text{rang } A$. Konstruirajmo bazo za $\text{Ker } L$, ki ima l elementov in dokažimo, da so Lu_1, \dots, Lu_l baza za $\text{Ker } L$:

- Je ogrodje? Vzemimo poljuben $v \in \text{Ker } L$. Zanj obstaja nek $u \in U \ni Lu = v$, ki ga lahko razvijemo po bazi U takole $u = \alpha_1 w_1 + \cdots + \alpha_k w_k + \beta_1 u_1 + \cdots + \beta_l u_l$. Sedaj na obeh straneh uporabimo L in upoštevamo linearnost:

$$\begin{aligned} v = Lu = L(\alpha_1 w_1 + \cdots + \alpha_k w_k + \beta_1 u_1 + \cdots + \beta_l u_l) &= \alpha_1 Lw_1 + \cdots + \alpha_k Lw_k + \beta_1 Lu_1 + \cdots + \beta_l Lu_l \\ &= \beta_1 Lu_1 + \cdots + \beta_l Lu_l \end{aligned}$$

Ker so w_i baza $\text{Ker } L$, so elementi $\text{Ker } L$, torej je $Lw_i = 0$ za vsak i . Tako poljuben $v \in \text{Ker } L$ razpišemo z bazo velikosti l .

- Je LN? Računajmo: $\gamma_1 Lu_1 + \cdots + \gamma_l Lu_l = 0 \xrightarrow{\text{linearnost}} L(\gamma_1 u_1 + \cdots + \gamma_l u_l) = 0 \Rightarrow \gamma_1 u_1 + \cdots + \gamma_l u_l \in \text{Ker } L$, kar pomeni, da ga je moč razviti po bazi $\text{Ker } L$:

$$\begin{aligned} \gamma_1 u_1 + \cdots + \gamma_l u_l &= \delta_1 w_1 + \cdots + \delta_k w_k \\ \gamma_1 u_1 + \cdots + \gamma_l u_l - \delta_1 w_1 - \cdots - \delta_k w_k &= 0 \end{aligned}$$

Ker je $w_1, \dots, w_k, u_1, \dots, u_l$ baza U , je LN, zato velja $\gamma_1 = \cdots = \gamma_l = \delta_1 = \cdots = \delta_k = 0$, kar pomeni, da očitno velja $\gamma_1 = \cdots = \gamma_l = 0$, torej je res LN.

□

Pripomba. Bralcu prav pride skica s 3. strani zapiskov predavanja „LA1P FMF 2024-02-28“.

Do preproste matrike preslikave z ustreznimi bazami Imenujmo sedaj $\mathcal{B} = \{w_1, \dots, w_k, u_1, \dots, u_l\}$ bazo za U , in $\mathcal{C} = \{Lu_1, \dots, Lu_l, z_1, \dots, z_m\}$ baza za V , kjer je z_1, \dots, z_m dopolnitev Lu_1, \dots, Lu_l do baze V , kajti V je lahko večji kot samo $\text{Ker } L$, in si oglejmo matriko naše preslikave $L : U \rightarrow V$, ki slika iz baze \mathcal{B} v bazo \mathcal{C} . Najprej razpišimo preslikane elemente baze \mathcal{B} po bazi \mathcal{C} :

$$\begin{aligned} Lu_1 &= 1 \cdot Lu_1 + \dots + 0 \cdot Lu_l + 0 \cdot z_1 + \dots + 0 \cdot z_m \\ &\vdots \\ Lu_l &= 0 \cdot Lu_1 + \dots + 1 \cdot Lu_l + 0 \cdot z_1 + \dots + 0 \cdot z_m \\ Lw_1 &= 0 \cdot Lu_1 + \dots + 0 \cdot Lu_l + 0 \cdot z_1 + \dots + 0 \cdot z_m \\ &\vdots \\ Lw_k &= 0 \cdot Lu_1 + \dots + 0 \cdot Lu_l + 0 \cdot z_1 + \dots + 0 \cdot z_m \end{aligned}$$

$$[L]_{\mathcal{C} \leftarrow \mathcal{B}} = \begin{bmatrix} I_l & 0 \\ 0 & 0 \end{bmatrix}$$

S primerno izbiro baz U in V je torej matrika preslikave precej preprosta, zgolj bločna matrika z identiteto, veliko rang L in ničlami, ki ustrezajo dimenzijam U in V .

Kaj pa, če je L matrika? Recimo ji A , da je $L_A = L$ od prej. Tedaj $A \in M_{p,n}(F)$. Naj bo $P = [u_1 \ \dots \ u_l \ w_1 \ \dots \ w_k]$ matrika, katere stolpci so baza U in $Q = [Au_1 \ \dots \ Au_l \ z_1 \ \dots \ z_m]$ matrika, katere stolpci so baza V . Po karakterizaciji obrnljivih matrik sta obrnljivi. Tedaj

$$\begin{aligned} AP &= [Au_1 \ \dots \ Au_l \ Aw_1 \ \dots \ Aw_k] \stackrel{\text{jedro}}{=} [Au_1 \ \dots \ Au_l \ 0 \ \dots \ 0] \\ Q \begin{bmatrix} I_l & 0 \\ 0 & 0 \end{bmatrix} &= [Au_1 \ \dots \ Au_l \ z_1 \ \dots \ z_m] \begin{bmatrix} I_l & 0 \\ 0 & 0 \end{bmatrix} = [Au_1 \ \dots \ Au_l \ 0 \ \dots \ 0] \\ AP &= Q \begin{bmatrix} I_l & 0 \\ 0 & 0 \end{bmatrix} \implies Q^{-1}AP = \begin{bmatrix} I_l & 0 \\ 0 & 0 \end{bmatrix} \end{aligned}$$

2.1.5 Ekvivalentnost matrik

Definicija. Matriki A in B sta ekvivalentni (oznaka $A \sim B$ ⁴) $\Leftrightarrow \exists$ obrnljivi $P, Q \ni B = PAQ$.

Zgled. Dokazali smo, da je vsaka matrika A ekvivalentna matriki $\begin{bmatrix} I_r & 0 \\ 0 & 0 \end{bmatrix}$, kjer je $r = \text{rang } A$.

Dokaz. Dokažimo, da je relacija \sim ekvivalenčna:

- refleksivnost: $A \sim A$ velja. Naj bo $A \in M_{m,n}(F)$. Tedaj $A = I_m A I_n$.
- simetričnost: $A \sim B \Rightarrow B \sim A$, kajti če velja $B = PAQ$ in sta P in Q obrnljivi, velja $P^{-1}BQ^{-1} = A$.
- tranzitivnost: $A \sim B \wedge B \sim C \Rightarrow A \sim C$, kajti, če velja $B = PAQ$ in $C = SBT$ in so P, Q, S, T obrnljive, velja $C = (SP)A(QT)$ in produkt obrnljivih matrik je obrnljiva matrika.

□

Izrek. Dve matriki sta ekvivalentni natanko tedaj, ko imata enako velikost in enak rang.

Dokaz. Dokazujemo ekvivalenco:

- (\Leftarrow) Po predpostavki imata A in B enako velikost in enak rang r . Od prej vemo, da sta obe ekvivalentni $\begin{bmatrix} I_r & 0 \\ 0 & 0 \end{bmatrix}$, ker pa je relacija ekvivalentnosti ekvivalenčna, sta $A \sim B$.
- (\Rightarrow) Po predpostavki $A \sim B$, torej $\exists P, Q \ni B = PAQ$. Če je A $m \times n$, je P $m \times m$ in Q $n \times n$, zato je po definiciji matričnega množenja B $m \times n$. Dokazati je treba še $\text{rang } A = \text{rang } B$.

$$\text{rang } B = \text{rang } PAQ \stackrel{?}{=} \text{rang } PA \stackrel{?}{=} \text{rang } A$$

⁴Isto oznako uporabljamo tudi za podobne matrike, vendar podobnost ni enako kot ekvivalentnost.

Dokažimo najprej $\text{rang } PAQ = \text{rang } PA$ oziroma $\text{rang } CQ = \text{rang } C$ za obrnljivo Q in poljubno C . Dokažemo lahko celo $\text{Ker } CQ = \text{Ker } C$:

$$\forall u : u \in \text{Ker } CQ \Leftrightarrow \exists v \ni : u = (CQ)v \Leftrightarrow \exists v' \ni : u = Cv' \Leftrightarrow u \in \text{Ker } C.$$

Sedaj dokažimo še $\text{rang } (PA) = \text{rang } (A)$. Zadošča dokazati, da je $\text{Ker } (PA) = \text{Ker } A$, kajti tedaj bi iz enakosti izrazov

$$\begin{aligned} \dim \text{Ker } A + \dim \text{Ker } A &= \dim F^n = n \\ \dim \text{Ker } PA + \dim \text{Ker } PA &= \dim F^n = n \end{aligned}$$

dobili $\dim \text{Ker } PA = \dim \text{Ker } A$. Dokažimo torej $\text{Ker } PA = \text{Ker } A$:

$$\forall u : u \in \text{Ker } PA \Leftrightarrow PAu = 0 \stackrel{P \text{ obrnljiva}}{\Leftrightarrow} Au = 0 \Leftrightarrow u \in \text{Ker } A.$$

Torej je res $\text{Ker } PA = \text{Ker } A$, torej je res $\text{rang } PA = \text{rang } A$, torej je res $\text{rang } A = \text{rang } B$. □

2.1.6 Podobnost matrik

Definicija. Kvadratni matriki A in B sta podobni, če \exists taka obrnljiva matrika $P \ni : B = PAP^{-1}$.

Trditev. Podobnost je ekvivalenčna relacija.

Dokaz. Dokazujemo, da je relacija ekvivalenčna, torej:

- refleksivna: $A = IAI^{-1} = IAI = A$
- simetrična: $B = PAP^{-1} \Rightarrow P^{-1}BP = A$
- tranzitivna: $B = PAP^{-1} \wedge C = QBQ^{-1} \Rightarrow C = QPAP^{-1}Q^{-1} = (QP)A(QP)^{-1}$

□

Pripomba 3. Očitno velja podobnost \Rightarrow ekvivalentnost, toda obrat ne velja vedno. Na primer $\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$ in $\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$ sta ekvivalentni (sta enake velikosti in ranga), toda nista podobni (dokaz kasneje).

Od prej vemo, da je vsaka matrika ekvivalentna matriki $\begin{bmatrix} I_r & 0 \\ 0 & 0 \end{bmatrix}$, kjer je r njen rang. A je vsaka kvadratna matrika podobna kakšni lepi matriki? Ja. Vsaka matrika je podobna zgornjetrikotni matriki in jordski kanonični formi (več o tem kasneje). Toda a je vsaka kvadratna matrika podobna diagonalni matriki? Ne.

Definicija. Matrika D je diagonalna $\sim d_{ij} \neq 0 \Rightarrow i = j$.

Kdaj je matrika A podobna neki diagonalni matriki? Kdaj \exists diagonalna D in obrnljiva $P \ni : A = PDP^{-1}$?

Izpeljimo iz nastavka. $D = \begin{bmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{bmatrix}$ in $P = [\vec{v}_1 \ \cdots \ \vec{v}_n]$, kjer sta D in P neznani. Ker mora biti P obrnljiva, so njeni stolpični vektorji LN.

$$A = PDP^{-1} \Leftrightarrow AP = PD \Leftrightarrow A [\vec{v}_1 \ \cdots \ \vec{v}_n] = [\vec{v}_1 \ \cdots \ \vec{v}_n] \begin{bmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{bmatrix} \text{ in } P \text{ obrnljiva}$$

$$[A\vec{v}_1 \ \cdots \ A\vec{v}_n] = [\lambda_1\vec{v}_1 \ \cdots \ \lambda_n\vec{v}_n] \text{ in } v_i \text{ so LN}$$

$$A\vec{v}_1 = \lambda_1\vec{v}_1, \dots, A\vec{v}_n = \lambda_n\vec{v}_n \text{ in } \forall i : v_i \neq 0$$

Porodi se naloga, imenovana „Lastni problem“. Iščemo pare (λ, \vec{v}) , ki zadoščajo enačbi $A\vec{v} = \lambda\vec{v}$.

Definicija. Pravimo, da je λ je lastna vrednost matrike A , če obstaja tak $\vec{v} \neq 0$, da je $A\vec{v} = \lambda\vec{v}$. V tem primeru pravimo, da je \vec{v} lastni vektor, ki pripada lastni vrednosti λ . Paru (λ, \vec{v}) , ki zadošča enačbi, pravimo lastni par matrike A .

Nalogo „Lastni problem“ rešujemo v dveh korakih. Najprej najdemo vse λ , nato za vsako poiščemo pripadajoče \vec{v} , ki za lastno vrednost obstajajo po definiciji.

Za nek $v \neq 0$ pišimo $Av = \lambda v = \lambda Iv \Leftrightarrow Av - \lambda Iv = 0 \Leftrightarrow (A - \lambda I)v = 0$ za nek $v \neq 0 \Leftrightarrow \text{Ker}(A - \lambda I) \neq \{0\} \stackrel{\text{K.O.M.}}{\Leftrightarrow} A - \lambda I$ ni obrnljiva $\Leftrightarrow \det(A - \lambda I) = 0$.

Definicija. Polinom $p_A(x) = \det(A - xI)$ je karakteristični polinom matrike A .

Premislek zgoraj nam pove, da so lastne vrednosti A ničle $p_A(x)$.

Pripomba. Karakteristični polinom lahko nima nobene ničle: $A = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$, $p_A(\lambda) = \det(A - \lambda I) = \det \begin{bmatrix} -\lambda & 1 \\ -1 & -\lambda \end{bmatrix} = x^2 + 1$, katerega ničli sta $\lambda_1 = i$ in $\lambda_2 = -i$, ki nista realni števili. V nadaljevanju se zato omejimo na kompleksne matrike in kompleksne lastne vrednosti, saj ima po Osnovnem izreku Algebre polinom s kompleksnimi koeficienti vedno vsaj kompleksne ničle.

Kako pa iščemo lastne vektorje za lastno vrednost λ ? Spomnimo se na $Av = \lambda v \Leftrightarrow v \in \text{Ker}(A - \lambda I)$. Rešiti moramo homogen sistem linearnih enačb. Po definiciji so lastni vektorji neničelni, zato nas trivialna rešitev ne zanima.

Definicija. Množici $\text{Ker}(A - \lambda I)$ pravimo lastni podprostor matrike A , ki pripada λ . Slednji vsebuje $\vec{0}$ in množico vektorjev, ki so vsi lastni vektorji A .

Vaja. Izračunaj lastne vrednosti od $A = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$. Od prej vemo, da $\lambda_1 = i$, $\lambda_2 = -i$. Izračunajmo $\text{Ker}(A - iI)$ in $\text{Ker}(A + iI)$:

$$\text{Ker}(A - iI) : \begin{bmatrix} -i & 1 \\ -1 & -i \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = 0 \implies -ix + y = 0, -x - iy = 0 \implies y = ix \implies v = x \begin{bmatrix} 1 \\ i \end{bmatrix}$$

$$\text{Ker}(A + iI) : \begin{bmatrix} i & 1 \\ -1 & i \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = 0 \implies ix + y = 0, -x + y = 0 \implies y = -ix \implies v = x \begin{bmatrix} 1 \\ -i \end{bmatrix}$$

$$\text{Ker}(A - iI) = \mathcal{L}\text{in} \left\{ \begin{bmatrix} 1 \\ i \end{bmatrix} \right\}, \quad \text{Ker}(A + iI) = \mathcal{L}\text{in} \left\{ \begin{bmatrix} 1 \\ -i \end{bmatrix} \right\}$$

Vstavimo lastna vektorja v P in lastne vrednosti v D na pripadajoči mesti. Dobimo obrnljivo P in velja $A = PDP^{-1}$

$$P = \begin{bmatrix} 1 & 1 \\ i & -i \end{bmatrix}, \quad D = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}$$

Temu početju pravimo „diagonalizacija matrike A “.

Zgled. Primer matrike, ki ni diagonalizabilna: $A = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$. $\det(A - \lambda I) = \det \begin{bmatrix} -\lambda & 1 \\ 0 & -\lambda \end{bmatrix} = \lambda^2$. Ničli/lastni vrednosti sta $\lambda_1 = 0$ in $\lambda_2 = 0$. Toda $\text{Ker}(A - 0I) = \text{Ker} A = \mathcal{L}\text{in} \left\{ \begin{bmatrix} 1 \\ 0 \end{bmatrix} \right\}$ in $P = \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix}$ ni obrnljiva. S tem dokažemo trditev v primeru 3. $\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$ in $\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$ nista podobni, ker je prva diagonalna, druga pa ni podobna diagonalni matriki (ne da se je diagonalizirati).

Lastne vrednosti lahko definiramo tudi za linearne preslikave, saj so linearne preslikave linearno izomorfne matrikam.

Definicija. Naj bo V vektorski prostor nad $F = \mathbb{C}$ in $L : V \rightarrow V$ linearna preslikava. Število $\lambda \in F$ je lastna vrednost L , le obstaja tak neničelni $v \in V$, da velja $Lv = \lambda v$.

Kako pa rešujemo „Lastni problem“ za linearne preslikave? $Lv = \lambda v \Leftrightarrow Lv - \lambda(id)v = 0 \Leftrightarrow (L - \lambda(id))v = 0 \Leftrightarrow v \in \text{Ker}(L - \lambda(id)) \stackrel{v \neq 0}{\Leftrightarrow} \det(L - \lambda(id)) = 0$. Toda determinante linearne preslikave nismo definirali. Lahko pa determinanto izračunamo na matriki, ki pripada tej linearni preslikavi. Toda dveh različnim bazam pripadata različni matriki linearne preslikave. Dokazati je treba, da sta determinanti dveh matrik, pripadajočih eni linearni preslikavi, enaki, četudi sta matriki v različnih bazah.

Lema 4. *Podobni matriki imata isto determinanto.*

Dokaz. Naj bo $B = PAP^{-1}$ za neko obrnljivo P . Tedaj $\det B = \det PAP^{-1} = \det P \det A \det P^{-1} = \det P \det P^{-1} \det A = \det PP^{-1} \det A = \det I \det A = 1 \cdot \det A = \det A$. \square

Dokaz. $L : V \rightarrow V$ naj bo linearna preslikava, V prostor nad $F = \mathbb{C}$, \mathcal{B} in \mathcal{C} pa bazi V . Priredimo matriki $L_{\mathcal{B} \leftarrow \mathcal{B}}$ in $L_{\mathcal{C} \leftarrow \mathcal{C}}$. Spomnimo se izreka 2 na strani 38: $[KL]_{\mathcal{D} \leftarrow \mathcal{B}} = [K]_{\mathcal{D} \leftarrow \mathcal{C}} [L]_{\mathcal{C} \leftarrow \mathcal{B}}$. $L = [id \circ L \circ id]$, zato $[L]_{\mathcal{C} \leftarrow \mathcal{C}} = [id \circ L \circ id]_{\mathcal{C} \leftarrow \mathcal{C}} = [id]_{\mathcal{C} \leftarrow \mathcal{B}} [L]_{\mathcal{B} \leftarrow \mathcal{B}} [id]_{\mathcal{B} \leftarrow \mathcal{C}} = P [L]_{\mathcal{B} \leftarrow \mathcal{B}} P^{-1}$ za neko obrnljivo P . Torej sta matriki $[L]_{\mathcal{B} \leftarrow \mathcal{B}}$ in $[L]_{\mathcal{C} \leftarrow \mathcal{C}}$ podobni, torej imata po lemi 4 na prejšnji strani isto determinanto. \square

Dokaz. Alternativen dokaz, da imata podobni matriki iste lastne vrednosti: A podobna

$$B \Rightarrow B = PAP^{-1} \Rightarrow B - xI = P(A - xI)P^{-1} \Rightarrow \det(B - xI) = \det(A - xI) \Rightarrow p_A = p_B,$$

torej so lastne vrednosti enake. Kaj pa lastni vektorji? Naj bo v lastni vektor A , torej

$$Av = \lambda v \Rightarrow PAv = \lambda Pv \Rightarrow PAP^{-1}Pv = \lambda Pv \Rightarrow BPv = \lambda Pv,$$

torej za v lastni vektor A sledi, da je Pv lastni vektor B . \square

Linearni transformaciji torej priredimo tako matriko, ki ima v začetnem in končnem prostoru isto bazo. Tedaj lahko izračunamo lastne pare na tej matriki.

Izrek. *Schurov izrek.* Vsaka kompleksna kvadratna matrika je podobna zgornjetrikotni matriki.

Dokaz. Indukcija po velikosti matrike.

- Baza: $A_{1 \times 1}$ je zgornjetrikotna.
- Korak: Po I. P. trdimo, da je vsaka $A_{(n-1) \times (n-1)}$ podobna kaki zgornjetrikotni matriki. Dokažimo še za poljubno $A_{n \times n}$. Naj bo λ lastna vrednost A in v_1 pripadajoči lastni vektor ter v_2, \dots, v_n dopolnitev v_1 do baze \mathbb{C}^n . Potem je matrika $P = [v_1 \ \dots \ v_n]$ obrnljiva.

$$AP = [Av_1 \ \dots \ Av_n] = [v_1 \ \dots \ v_n] \begin{bmatrix} \lambda & a_{1,2} & \dots & a_{1,n} \\ 0 & \vdots & & \vdots \\ \vdots & \vdots & & \vdots \\ 0 & a_{m,n} & \dots & a_{m,n} \end{bmatrix} = P \begin{bmatrix} \lambda & B \\ 0 & C \end{bmatrix}$$

Po I. P. obstaja taka zgornjetrikotna T in obrnljiva Q , da $C = QTQ^{-1}$.

$$\begin{aligned} \begin{bmatrix} 1 & 0 \\ 0 & Q \end{bmatrix}^{-1} P^{-1}AP \begin{bmatrix} 1 & 0 \\ 0 & Q \end{bmatrix} &= \begin{bmatrix} 1 & 0 \\ 0 & Q \end{bmatrix}^{-1} \begin{bmatrix} \lambda & B \\ 0 & C \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & Q \end{bmatrix} = \\ &= \begin{bmatrix} \lambda & C \\ 0 & Q^{-1}B \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & Q \end{bmatrix} = \begin{bmatrix} \lambda & CQ \\ 0 & B \end{bmatrix} \end{aligned}$$

A je torej podobna $\begin{bmatrix} \lambda & CQ \\ 0 & B \end{bmatrix}$, ki je zgornjetrikotna. \square

2.1.7 Zadosten pogoj za diagonalizabilnost

Izrek 5. *Lastni vektorji, ki pripadajo različnim lastnim vrednostim, so linearno neodvisni.*

Dokaz. Naj bo $A_{n \times n}$ matrika, $\lambda_1, \dots, \lambda_k$ njene lastne vrednosti in v_1, \dots, v_k njim pripadajoči lastni vektorji. Dokazujemo $\lambda_1, \dots, \lambda_k$ paroma različni $\Rightarrow v_1, \dots, v_k$ LN. Dokaz z indukcijo po k .

- Baza $k = 1$: Elementi $\{\lambda_1\}$ so trivialno paroma različni in v_1 je kot neničen vektor LN.

- Korak: Dokazujemo $\lambda_1, \dots, \lambda_{k+1}$ so paroma različne $\Rightarrow v_1, \dots, v_k$ so LN, vedoč I. P. Denimo, da $\alpha_1 v_1 + \dots + \alpha_{k+1} v_{k+1} = 0$. Množimo z A :

$$A(\alpha_1 v_1 + \dots + \alpha_{k+1} v_{k+1}) = \alpha_1 A v_1 + \dots + \alpha_{k+1} A v_{k+1} = \alpha_1 \lambda_1 v_1 + \dots + \alpha_{k+1} \lambda_{k+1} v_{k+1} = 0$$

Množimo začetno enačbo z λ_{k+1} (namesto z A , kot smo to storili zgoraj):

$$\alpha_1 \lambda_{k+1} v_1 + \dots + \alpha_{k+1} \lambda_{k+1} v_{k+1} = 0$$

Odštejmo eno enačbo od druge, dobiti moramo 0, saj odštevamo 0 od 0:

$$\alpha_1 (\lambda_1 - \lambda_{k+1}) v_1 + \dots + \alpha_k (\lambda_k - \lambda_{k+1}) v_k + \alpha_{k+1} (\lambda_{k+1} - \lambda_{k+1}) v_{k+1} = 0$$

Ker so lastne vrednosti paroma različne ($\lambda_i = \lambda_j \Rightarrow i = j$), so njihove razlike neničelne. Ker so v_1, \dots, v_k po predpostavki LN, sledi $\alpha_1 = \dots = \alpha_k = 0$. Vstavimo te konstante v $\alpha_1 v_1 + \dots + \alpha_{k+1} v_{k+1} = 0$ in dobimo $\alpha_{k+1} v_{k+1} = 0$. Ker je v_{k+1} neničeln (je namreč lastni vektor), sledi $\alpha_{k+1} = 0$, torej $\alpha_1 = \dots = \alpha_k = \alpha_{k+1} = 0$, zato je v_1, \dots, v_{k+1} res LN. □

Posledica 6. Vsota vseh lastnih podprostorov matrike je direktna (definicija 2 na strani 34).

Dokaz. Naj bodo $\lambda_1, \dots, \lambda_k$ vse paroma različne lastne vrednosti matrike $A \in M_n(\mathbb{C})$. Pripadajoči lastni podprostorji so torej $\forall i \in \{1..k\} : V_i = \text{Ker}(A - \lambda_i I)$. Trdimo, da je vsota teh podprostorov direktna, torej $\forall v_1 \in V_1, \dots, v_k \in V_k : v_1 + \dots + v_k = 0 \Rightarrow v_1 = \dots = v_k = 0$. To sledi iz izreka 5 na prejšnji strani. □

Posledica. Če ima $n \times n$ matrika n paroma različnih lastnih vrednosti, je podobna diagonalni matriki.

Dokaz. Po posledici 6 je vsota lastnih podprostorov matrike $A_{n \times n}$ direktna. Če je torej lastnih podprostorov n , je njihova vsota cel prostor \mathbb{C}^n . Matriko se da diagonalizirati, kadar je vsota vseh lastnih podprostorov enaka podprostoru \mathbb{C}^n (tedaj so namreč stolpci matrike P linearno neodvisni, zato je P obrnljiva). □

2.1.8 Algebraične in geometrijske večkratnosti

Definicija. Naj bo $A_{n \times n}$ matrika. $p_A(\lambda) = \det(A - \lambda I) = (-1)^n (\lambda - \lambda_1)^{n_1} \dots (\lambda - \lambda_k)^{n_k}$, kjer so $\lambda_1, \dots, \lambda_k$ vse paroma različne lastne vrednosti A . Stopnji ničle $-n_i$ — rečemo algebraična večkratnost lastne vrednosti λ_i .

Definicija. Geometrijska večkratnost lastne vrednosti λ_i je $\dim \text{Ker}(A - \lambda_i I) = n(A - \lambda_i I) = m_i$.

Algebraično večkratnost λ_i označimo z n_i in je večkratnost ničle λ_i v $p_A(\lambda)$ (karakterističnem polinomu). Geometrijsko večkratnost λ_i pa označimo z m_i in je dimenzija lastnega podprostora za λ_i .

Trditev 7. $\forall i \in \{1..k\} : m_i \leq n_i$ — geometrijska večkratnost lastne vrednosti je kvečjemu tolikšna, kot je algebraična večkratnost te lastne vrednosti.

Dokaz. Naj bo v_1, \dots, v_{m_i} baza za lastni podprostor $V_i = \text{Ker}(A - \lambda_i I)$ in naj bo v_{m_i+1}, \dots, v_n njena dopolnitev do baze \mathbb{C}^n . Tedaj velja: $Av_1 = \lambda_1 v_1, \dots, Av_{m_i} = \lambda_{m_i} v_{m_i}, Av_{m_i+1} =$ linearna kombinacija $v_1, \dots, v_n, \dots, Av_n =$ linearna kombinacija v_1, \dots, v_n . Naj bo $P = [v_1 \ \dots \ v_{m_i} \ v_{m_i+1} \ \dots \ v_n]$, ki je obrnljiva.

$$P^{-1}AP = \begin{bmatrix} \lambda_i I_{m_i} & B \\ 0 & C \end{bmatrix}$$

Ker je karakteristični polinom neodvisen od izbire baze, velja

$$\det(A - xI_n) = \det(\lambda_i I_{m_i} - xI) \det(C - xI_{n-m_i}) = (\lambda_i - x)^{m_i} \det(C - xI_{n-m_i})$$

Ker $(\lambda - x)^{m_i}$ deli karakteristični polinom, je algebraična večkratnost λ_i vsaj tolikšna, kot je geometrijska. □

Trditev 8. Matriko s paroma različnimi lastnimi vrednostmi $\lambda_1, \dots, \lambda_k$ je moč diagonalizirati $\Leftrightarrow \forall i \in \{1..k\} : m_i = n_i$.

Dokaz. Naj bo V_i lastno podprostor lastne vrednosti λ_i . Vemo, da se da $A_{n \times n}$ diagonalizirati $\Leftrightarrow A$ ima n LN stolpičnih vektorjev $\Leftrightarrow \text{Ker}(A - \lambda_1 I) + \dots + \text{Ker}(A - \lambda_k I) = \mathbb{C}^n \Leftrightarrow \dim(V_1 + \dots + V_k) = \dim V_1 + \dots + \dim V_k \Leftrightarrow$ vsota lastnih podprostorov je direktna $\Leftrightarrow \dim(V_1 + \dots + V_n) = n \Leftrightarrow \dim V_1 + \dots + \dim V_k = n \Leftrightarrow m_1 + \dots + m_k = n \Leftrightarrow m_1 + \dots + m_k = n_1 + \dots + n_m$. Toda ker po prejšnjem izreku $\forall i \in \{1..k\} : m_i \leq n_i$, mora veljati $\forall i \in \{1..k\} : m_i = n_i$. □

2.1.9 Minimalni polinom matrike

Definicija. Naj bo $p(x) = c_0x^0 + \dots + c_nx^n \in \mathbb{C}[x]$ polinom in A matrika. $p(A) := c_0A^0 + \dots + c_nA^n = c_0I + \dots + c_nA^n$. Če je $p(A) = 0$ (ničelna matrika), pravimo, da polinom p anihilira/uniči matriko A .

Dejstvo. $p(A) = 0 \Rightarrow p(P^{-1}AP) = 0$.

Izkaže se, da karakteristični polinom anihilira matriko — $p_A(A) = 0$. Dokaz kasneje.

Definicija. Polinom $m(x)$ je minimalen polinom A , če velja:

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

Trditev. eksistenca minimalnega polinoma — Minimalni polinom obstaja.

Dokaz. Naj bo $A_{n \times n}$ matrika. Očitno je $M_{n \times n}(\mathbb{C})$ vektorski prostor dimenzije n^2 . Matrike $\{I, A, A^2, \dots, A^{n^2}\}$ so linearno odvisne, ker je moč te množice za 1 večja od moči vektorskega prostora. Torej $\exists c_0, \dots, c_{n^2} \in \mathbb{C}$, ki niso vse 0 $\ni: c_0I + c_1A + c_2A^2 + \dots + c_{n^2}A^{n^2} = 0$. Torej polinom $p(x) = c_0x^0 + c_1x^1 + c_2x^2 + \dots + c_{n^2}x^{n^2}$ anihilira A . Če ta polinom delimo z njegovim vodilnim koeficientom, dobimo polinom, ki ustreza prvima dvema zahtevama za minimalni polinom. Če med vsemi takimi izberemo takega z najnižjo stopnjo, le-ta ustreza še tretji zahtevi. \square

Izrek. Če je $m(x)$ minimalni polinom za A in če $p(x)$ anihilira A , potem $m(x) | p(x)$ ($m(x)$ deli $p(x)$).

Dokaz. Delimo p z m : $\exists k(x), r(x) \ni: p(x) = k(x)m(x) + r(x) \wedge \deg r(x) < \deg m(x)$. Vstavimo A na obe strani:

$$0 = p(A) = k(A)m(A) + r(A) = k(A) \cdot 0 + r(A) = 0 + r(A) = r(A) = 0$$

Sledi $r(x) = 0$, kajti če r ne bi bil ničeln polinom, bi ga lahko delili z vodilnim koeficientom in po predpostavki $\deg r(x) < \deg m(x)$ bi imel manjšo stopnjo kot $m(x)$, torej bi ustrezal zahtevam 1 in 2 za minimalni polinom in bi imel manjšo stopnjo od m , torej m ne bi bil minimalni polinom, kar bi vodilo v protislovje. \square

Posledica. enoličnost minimalnega polinoma. Naj bosta m_1 in m_2 minimalna polinoma matrike A . Ker m po definiciji anihilira A , iz prejšnje trditve sledi, če vstavimo $m = m_1$ in $p = m_2$, $m_1 | m_2$. Toda če vstavimo $m = m_2$ in $p = m_1$, $m_2 | m_1$. Iz $m_1 | m_2 \wedge m_2 | m_1$ sledi, da se m_1 in m_2 razlikujeta le za konstanten faktor, ki pa je po definiciji minimalnega polinoma 1, torej $m_1 = m_2$. Zaradi enoličnosti lahko označimo minimalni polinom A z $m_A(x)$.

2.1.10 Ničle minimalnega polinoma

Trditev. $m_A(x)$ in $p_A(x)$ imata iste ničle \sim ničle $m_A(x)$ so lastne vrednosti A .

Dokaz. Ker je $p_A(x)$ (dokaz kasneje), velja po trditvi v dokazu enoličnosti, da $m_A | p_A$, torej je vsaka ničla m_A tudi ničla p_A . Treba je dokazati še, da je vsaka ničla p_A tudi ničla m_A , natančneje: Treba je dokazati, da če je λ lastna vrednost matrike A , je $m_A(\lambda) = 0$. Naj bo $v \neq 0$ lastni vektor za λ . Tedaj $Av = \lambda v$. Potem velja $A^2v = AA v = A\lambda v = \lambda Av = \lambda\lambda v = \lambda^2 v$ in splošneje $A^n v = \lambda^n v$. Sedaj recimo, da je $m_A(x) = d_0x^0 + \dots + d_r x^r$. Potem je, ker minimalni polinom anihilira A ,

$$\begin{aligned} m_A(\lambda)v &= (d_0 + d_1\lambda + d_2\lambda^2 + \dots + d_r\lambda^r)v = d_0v + d_1\lambda v + d_2\lambda^2 v + \dots + d_r\lambda^r v = \\ &= d_0v + d_1Av + d_2A^2v + \dots + d_rA^r v = (d_0 + d_1A + d_2A^2 + \dots + d_rA^r)v = m_A(A)v = 0v = 0 \end{aligned}$$

Ker $m_A(\lambda)v = 0$ in $v \neq 0$ (je namreč lastni vektor), velja $m_A(\lambda) = 0$. \square

Lastnosti Ker je $p_A(x) = (-1)^n (x - \lambda_1)^{r_1} \cdots (x - \lambda_k)^{r_k}$ in $m_A(x) = (x - \lambda_1)^{r_1} \cdots (x - \lambda_k)^{r_k}$, sledi iz $m_A | p_A \Rightarrow \forall i \in \{1..k\} : r_i \leq n_i$. Poleg tega, ker $m_A(\lambda_1) = 0 \Rightarrow \forall i \in \{1..k\} : r_i \geq 1$. Toda pozor: **Ni** res, da $r_i = m_i$ (stropnja lastnega podprostora).

Izrek. *Cayley-Hamilton.* $p_A(A) = 0$ — karakteristični polinom matrike A anihilira matriko A

Dokaz. Spomnimo se eksplicitne formule za celico inverza matrike (razdelek 1.4.4 na strani 20), ki pravi $B^{-1} = \frac{1}{\det B} \tilde{B}^T$. Računajmo in naposled vstavimo $B = A - xI$:

$$B^{-1} = \frac{1}{\det B} \tilde{B}^T \quad / \cdot (\det B) B$$

$$\det B \cdot I = B \tilde{B}^T$$

$$\det(A - xI) \cdot I = p_A(x) \cdot I = (A - xI) (A - \tilde{x}I)^T$$

Glede na definicijo \tilde{A} je $(A - \tilde{x}I)^T$ matrika velikosti $n \times n$, ki vsebuje polinome stopnje $< n$, kajti vsebuje determinante kofaktorskih matrik, torej je takele oblike ($\forall i \in \{1..(n-1)\} : B_i \in M_n(\mathbb{C})$):⁵

$$(A - \tilde{x}I)^T = B_0 + B_1x + \cdots + B_{n-1}x^{n-1}$$

Naj bo $p_A(x) = \det(A - \lambda I) = c_0 + c_1x + \cdots + c_nx^n$. Kot v enačbi množimo to z I : $\det(A - \lambda I) \cdot I = c_0I + c_1Ix + \cdots + c_nIx^n$. Oglejmo si še desno stran enačbe:

$$\begin{aligned} (A - xI) (A - \tilde{x}I)^T &= (A - xI) (B_0 + B_1x + \cdots + B_{n-1}x^{n-1}) = AB_0 + AB_1x + \cdots + AB_{n-1}x^{n-1} - B_0x - B_1x^2 - \cdots - B_{n-1}x^n = \\ &= AB_0 + (AB_1 - B_0)x + (AB_2x^2 - B_1)x^2 + \cdots + (AB_{n-1} - B_{n-2})x^{n-1} - B_{n-1}x^n \end{aligned}$$

In primerjajmo koeficiente v polinomih pred istoležnimi spremenljivkami na obeh straneh tele enačbe:

$$\det(A - xI) \cdot I = (A - xI) (A - \tilde{x}I)^T$$

$$c_0I + c_1Ix + \cdots + c_nIx^n = AB_0 + (AB_1 - B_0)x + (AB_2 - B_1)x^2 + \cdots + (AB_{n-1} - B_{n-2})x^{n-1} - B_{n-1}x^n$$

$$\begin{array}{lcl} 1 : & c_0I & = AB_0 \\ x : & c_1I & = AB_1 - B_0 \\ x^2 : & c_2I & = AB_2x^2 - B_1 \\ & \vdots & \\ x^{n-1} : & c_{n-1}I & = AB_{n-1} - B_{n-2} \\ x^n : & c_nI & = -B_{n-1} \end{array}$$

Vstavimo sedaj A v enačbo namesto x :

$$\begin{aligned} p_A(A) &= c_0I + c_1IA + \cdots + c_nIA^n = AB_0 + (AB_1 - B_0)A + (AB_2 - B_1)A^2 + \cdots + (AB_{n-1} - B_{n-2})A^{n-1} - B_{n-1}A^n = \\ &= AB_0 + A^2B_1 - AB_0 + A^2B^2 - B_1A^2 + \cdots + A^nB_{n-1} - A^{n-1}B_{n-2} - B_{n-1}A^n = 0 \\ & p_A(A) = 0 \end{aligned}$$

□

Izrek. *Matriko A se da diagonalizirati* $\Leftrightarrow m_A(x)$ ima samo enostavne ničle (nima večkratnih — potence so vse 1). Torej $m_A(x) = (x - \lambda_1)^1 \cdots (x - \lambda_k)^1$ za $\lambda_1, \dots, \lambda_k$ vse paroma različne lastne vrednosti A .

Dokaz. Dokazujemo ekvivalenco:

⁵To si predstavljamo tako, da iz vsake celice matrike, ki vsebuje polinom, izpostavimo (homogenost) spremenljivko (torej x na fiksno potenco) in nato koeficiente v celicah pred to spremenljivko zložimo v eno matriko. Slednje ponovimo za vsako potenco in dobimo te matrike B_i .

(\Rightarrow) Po predpostavki je A podobna diagonalni matriki — $A = PDP^{-1}$ za diagonalno D in obrnljivo P . BŠŠ naj bo $D = \begin{bmatrix} \lambda_1 & 0 & 0 \\ 0 & \cdots & 0 \\ 0 & 0 & \lambda_k \end{bmatrix}$ in $\lambda_1 \leq \cdots \leq \lambda_k$. Oglejmo si izraz

$$(D - \lambda_1 I) \cdots (D - \lambda_k I) = \begin{bmatrix} 0 & & & 0 \\ & \lambda_2 - \lambda_1 & & \\ & & \ddots & \\ 0 & & & \lambda_k - \lambda_1 \end{bmatrix} \cdots \begin{bmatrix} \lambda_1 - \lambda_k & & & 0 \\ & \ddots & & \\ & & \lambda_{k-1} - \lambda_k & \\ 0 & & & 0 \end{bmatrix} = 0$$

Sedaj pa še izraz

$$(A - \lambda_1 I) \cdots (A - \lambda_k I) = (PDP^{-1} - \lambda_1 I) \cdots (PDP^{-1} - \lambda_k I) = (PDP^{-1} - \lambda_1 PP^{-1}) \cdots (PDP^{-1} - \lambda_k PP^{-1}) = P(D - \lambda_1 I) \cdots (D - \lambda_k I) P^{-1} = P0P^{-1} = 0,$$

torej ta polinom anihilira A . Ker deli $m_A(x)$ — vsebuje vse ničle $m_A(x)$, je prav to minimalen polinom A — ima najmanjšo stopnjo možno.

(\Leftarrow) Potrebujemo nekaj lem:

Lema 1. Za vse matrike A, B velja $n(AB) \leq n(A) + n(B) \sim \dim \text{Ker}(AB) \leq \dim \text{Ker}(A) + \dim \text{Ker}(B)$.

Dokaz. Oglejmo si preslikavo $L : \text{Ker } AB \rightarrow \text{Ker } A$, ki slika $x \mapsto Bx$. Je dobro definirana, kajti $x \in \text{Ker } AB \Rightarrow ABx = 0 \Rightarrow Bx \in \text{Ker } A$. Po osnovnem dimenzijskem izreku za preslikavo L velja $\dim \text{Ker } L + \dim \text{Im } L = \dim \text{Ker } AB$. Ker velja $Lx = 0 \Rightarrow Bx = 0$, velja $\text{Ker } L \subseteq \text{Ker } B$ in zato $\dim \text{Ker } L \leq \dim \text{Ker } B$. Poleg tega iz definicije velja $\text{Ker } L \subseteq \text{Ker } A$ in zato $\dim \text{Ker } L \leq \dim \text{Ker } A$. Vstavimo te neenakosti v enačbo iz dimenzijskega izreka:

$$\dim \text{Ker } L + \dim \text{Im } L = \dim \text{Ker } AB$$

$$\dim \text{Ker } B + \dim \text{Ker } A \geq \dim \text{Ker } AB$$

Lemo lahko posplošimo na več faktorkev, torej $n(A_1 \cdots A_k) \leq n A_1 + \cdots + n A_k$. \square

Nadaljujmo z dokazom (\Leftarrow). Denimo, da $(x - \lambda_1) \cdots (x - \lambda_k)$ anihilira A . Upoštevamo

$$n((A - \lambda_1 I) \cdots (A - \lambda_k I)) \leq n(A - \lambda_1 I) + \cdots + n(A - \lambda_k I)$$

Členi na desni strani so geometrijske večkratnosti, ker pa A anihilira polinom po predpostavki, je ta produkt ničelna preslikava in je dimenzija jedra dimenzija celega prostora.

$$n(0) = n = n_1 + \cdots + n_k \leq m_1 + \cdots + m_k$$

Ker $\forall i : m_i \leq n_i$ (7 na strani 44), velja v zgornji neenačbi enakost, torej je matrika po 8 na strani 44 diagonalizabilna. \square

2.1.11 Korenski podprostor

Definicija. Naj bo $A \in M_n$ in $m_A(x) = (x - \lambda_1)^{r_1} \cdots (x - \lambda_k)^{r_k}$ njen minimalni polinom. $\forall i \in \{1..k\}$ označimo z $W_i := \text{Ker}(A - \lambda_i I)^{r_i}$ korenski podprostor matrike A za lastno vrednost λ_i . Vpeljimo še oznako $V_i := \text{Ker}(A - \lambda_i I)^1$ (tu potenca ni r_i , temveč je 1).

Dejstvo 1. Očitno je $\text{Ker}(A - \lambda_i I) \subseteq \text{Ker}(A - \lambda_i I)^2 \subseteq \text{Ker}(A - \lambda_i I)^3 \subseteq \cdots$, kajti če $x \in \text{Ker}(A - \lambda_i I)^m \Rightarrow (A - \lambda_i I)^m x = 0 \Rightarrow (A - \lambda_i I)(A - \lambda_i I)^m x = 0 \Rightarrow x \in \text{Ker}(A - \lambda_i I)^{m+1}$. Izkaže se, da so vse inkluzije do r_i -te potence stroge, od r_i -te potence dalje pa so vse inkluzije enačaji, torej za $W_i = \text{Ker}(A - \lambda_i I)^{r_i}$ velja

$$\text{Ker}(A - \lambda_i I) \subset \text{Ker}(A - \lambda_i I)^2 \subset \cdots \subset \text{Ker}(A - \lambda_i I)^{r_i} = \text{Ker}(A - \lambda_i I)^{r_i+1} = \cdots$$

Poleg tega se izkaže, da je $\dim W_i = n_i$ (algebraična večkratnost λ_i).

Dejstvo 2. $\dim V_i = \dim \text{Ker}(A - \lambda_i I) = m_i$ (geometrijska večkratnost λ_i).

Trditev 3. $\mathbb{C}^n = W_1 \oplus W_2 \oplus \dots \oplus W_k$ — vsota vseh korenskih podprostorov je vse in ta vsota je direktna. Tej vsoti pravimo „korenski razcep matrike A “.

Pripomba. Dokazujemo:

- Če predpostavimo, da je vsota direktna, je lahko dokazati, da je vsota cel prostor. V karakteristični polinom, ki po Cayley-Hamiltonu anihilira A , vstavimo A in dobimo $0 = (-1)^n (A - \lambda_1 I)^{r_1} \dots (A - \lambda_k I)^{r_k} = A_1 \dots A_k$. Ker je vsota direktna, velja $n(A_1 \dots A_n) = n(0) = 0 = n A_1 \dots n A_k = \dim(W_1 + \dots + W_k)$, torej $W_1 + \dots + W_k = \mathbb{C}^n$.
- Če predpostavimo, da je $W_i \cap W_j = \{0\}$ za $i \neq j$, lahko od tod izpeljemo direktnost vsote korenskih podprostorov. Dokaz z indukcijo:
 - Baza: W_1 je direktna vsota. Očitno ($\forall w_1 \in W_1 : w_1 = 0 \Rightarrow w_1 = 0$).
 - Indukcijska predpostavka: $w_1 + \dots + w_i = 0 \Rightarrow w_1 = \dots = w_i = 0$.
 - Korak: Naj bodo w_1, \dots, w_{i+1} taki, da

$$\begin{aligned} w_1 + \dots + w_{i+1} = 0 & \quad / \cdot (A - \lambda_{i+1} I)^{r_{i+1}} \\ (A - \lambda_{i+1} I)^{r_{i+1}} w_1 + \dots + (A - \lambda_{i+1} I)^{r_{i+1}} w_i + 0 = 0 \end{aligned}$$

$\text{Ker}(A - \lambda_h I)^{r_h}$ in $(A - \lambda_k I)^{r_k}$ za vsaka h, k komutirata (gre namreč za polinom, v katerega je vstavljen A), velja za vsak j iz $(A - \lambda_j I)^{r_j} w_j = 0 = (A - \lambda_{i+1} I)^{r_{i+1}} (A - \lambda_j I)^{r_j} w_j$ tudi

$$(A - \lambda_j I)^{r_j} (A - \lambda_{i+1} I)^{r_{i+1}} w_j = 0$$

Ker je po I. P. $W_1 + \dots + W_i$ direktna, velja za vsak j $w_j \in W_j$, toda zaradi našega množenja tudi $w_j \in W_{i+1}$. Zaradi predpostavke $m = n \Rightarrow W_m \cup W_n = \{0\}$ velja za vsak $j \in \{1..i\} : w_j = 0$. V prvi enačbi ostane le še $w_{i+1} = 0$.

- Dokazati je treba še $i \neq j \Rightarrow W_i \cap W_j = \{0\}$. Dokažimo, da je W_i invarianten za A , t. j. $v \in W_i \Rightarrow Av \in W_i$. Če je $v \in W_i$, tedaj

$$\begin{aligned} (A - \lambda_i I)^{r_i} v = 0 & \quad / \cdot A \\ A(A - \lambda_i I)^{r_i} v = 0 \\ Av \in \text{Ker}(A - \lambda_i I)^{r_i} \\ Av \in W_i \end{aligned}$$

Ker so vsi W_i invariantni za A , so tudi njihovi preseki invariantni za A . Definirajmo torej linearno preslikavo $L : W_i \cap W_j \rightarrow W_i \cap W_j$ s predpisom $v \mapsto Av$. Vemo, da ima L vsaj eno lastno vrednost λ in pripadajoči lastni vektor w . Torej $w \in W_i \cap W_j$ in $Lw = \lambda w$, toda $Lw = Aw = \lambda w$. Ker velja $Aw = \lambda w \Rightarrow A^q w = \lambda^q w \Rightarrow p(A)w = p(\lambda)w$ za vsak polinom p , velja $p(A)w = p(\lambda)w$ za vsak polinom p . Uporabimo polinom $p(x) = (x - \lambda_i)^{r_i}$ in dobimo $(A - \lambda_i)^{r_i} w = (\lambda - \lambda_i)^{r_i} w$. Leva stran enačbe je 0, PDDRAA w ni 0, torej $(\lambda - \lambda_i)^{r_i} = 0$, torej $\lambda = \lambda_i$. Vendar lahko namesto tistega polinoma uporabimo polinom $p(x) = (x - \lambda_j)^{r_j}$, kar pokaže $\lambda = \lambda_j$, torej $\lambda_j = \lambda_i$, kar je v \rightarrow s tem, da so lastne vrednosti $\lambda_1, \dots, \lambda_k$ paroma različne. Torej $w = 0$.

2.1.12 Jordanska kanonična forma

Vsaka kvadratna matrika je podobna posebni zgornjetrikotni matriki, ki ji pravimo JKF. To je bločno diagonalna matrika, ki ima za diagonalne bloke t. i. „jordanske kletke“, to so matrike oblike:

$$\begin{bmatrix} \lambda & 1 & & & \\ & \lambda & 1 & & \\ & & \ddots & \ddots & \\ & & & \lambda & 1 \\ & & & & \lambda \end{bmatrix}.$$

Jordanska matrika je sestavljena iz jordanjskih kletk po diagonali (J_i so jordanjske kletke):

$$\begin{bmatrix} J_1 & & 0 \\ & \ddots & \\ 0 & & J_m \end{bmatrix}.$$

Običajno zahtevamo še, da so JK, ki imajo isto lastno vrednost, skupaj, ter da so JK padajoče urejene po lastni vrednosti od največje do najmanjše.

Izrek. Za vsako kvadratno kompleksno matriko $A \in M_n \times_n(\mathbb{C})$ obstaja taka jordanjska matrika J in taka obrnljiva matrika P , da velja $A = PJP^{-1}$. ZDB vsaka $A \in M_n \times_n(\mathbb{C})$ je podobna neki Jordanjski matriki.

Procesu iskanja jordanjske matrike pravimo „jordanifikacija“. Kako konstruiramo J in P ? Izračunamo lastne vrednosti in pripadajoče korenske podprostore.

- Naj bo λ lastna vrednost A . Za preglednost pišimo $N := A - \lambda I$.
- Izračunamo lastne vektorje in lastni podprostor $\text{Ker } N^r$ ter ga izrazimo z njegovo bazo, recimo ji B_r .
- Nato izberemo „pomožne baze“ B_1, \dots, B_r , ki pripadajo prostorom $\text{Ker } N^1, \dots, \text{Ker } N^r$.
- Pomožno bazo B_{r-1} dopolnimo do baze B_r z elementi $B_r \cup \{u_1, \dots, u_{k_1}\}$. Potem je $B_{r-1} \cup \{u_1, \dots, u_{k_1}\}$ „popravek pomožne baze B_r “.
- Vektorje $\{u_1, \dots, u_{k_1}\} \in \text{Ker } N^r$ pomnožimo z matriko N , dobljeni Nu_1, \dots, Nu_{k_1} ležijo v $\text{Ker } N^{r-1}$. Množica $B_{r-2} \cup \{Nu_1, \dots, Nu_{k_1}\}$ je linearno neodvisna. Izberemo take $v_1, \dots, v_{k_2} \in B_{r-1}$, ki dopolnijo LN $B_{r-2} \cup \{Nu_1, \dots, Nu_{k_1}\}$ do baze $\text{Ker } N^{r-1}$. Potem je $B_{r-2} \cup \{Nu_1, \dots, Nu_{k_1}\} \cup \{v_1, \dots, v_{k_2}\}$ popravek pomožne baze B_{r-1} .
- Izberemo take $w_1, \dots, w_{k_3} \in B_{r-2}$, ki $B_{r-3} \cup \{N^2u_1, \dots, N^2u_{k_1}, Nv_1, \dots, Nv_{k_2}\}$ dopolnijo do baze $\text{Ker } N^{r-2}$. Tedaj je $B_{r-3} \cup \{N^2u_1, \dots, N^2u_{k_1}, Nv_1, \dots, Nv_{k_2}, w_1, \dots, w_{k_3}\}$ popravek pomožne baze B_{r-2} .
- Postopek ponavljamo, dokler ne popravimo vseh možnih baz.

Dobimo t. i. „jordanjske verige“. Ena jordanjska veriga je $(u, Nu, N^2u, \dots, N^x u)$, torej preslikanje elementa u , ki začne kot dopolnitev baze korenskega podprostora $\text{Ker } N^{x+1}$ in je na koncu x -krat preslikan z N , torej konča v korenskem podprostoru $\text{Ker } N$. Nekatero verige se začno v največjem korenskem podprostoru $\text{Ker } N^r$, nekatere šele kasneje, v $\text{Ker } N^1$ ali pa $\text{Ker } N^2$ ali pa $\text{Ker } N^3$.

Imamo torej k_1 jordanjskih verig dolžine r , k_2 jordanjskih verig dolžine $r-1$, k_3 jordanjskih verig dolžine $r-2$, ..., k_r jordanjskih verig dolžine 1. Skupaj je jordanjskih verig $k_1 + \dots + k_r = \dim \text{Ker } N$. Jordanjskih verig za lastno vrednost λ je torej toliko, kot je njena geometrijska večkratnost.

Vsaki jordanjski verigi dolžine k pripada ena jordanjska kletka velikosti $k \times k$. k -vektorjev iz verige zložimo v P tako, da je vektor z začetka verige (torej tisti iz popravljene baze večjega prostora) na levi strani v matriki.

Zgled. Poišči jordanjsko kanonično formo matrike

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

Najprej izračunamo karakteristični polinom: $\det(A - \lambda I) = x(x-2)^3$. $\lambda_1 = 0$, $n_1 = 1$, $\lambda_2 = 2$, $n_2 = 3$. Lastni vektorji: $\text{Ker}(A - 0I) = \mathcal{L}\text{in}\{(1, 0, 0, 0)\}$, $\text{Ker}(A - 2I) = \mathcal{L}\text{in}\{(3, 0, -2, 2), (1, 2, 0, 0)\}$. Če bi dobili 4 lastne vektorje, bi lahko matriko diagonalizirali. Tako je ne moremo. $\text{Ker } n_1 = 1$, je r_1 največ 1, torej $\text{Ker}(A - 0I) = \text{Ker}(A - 0I)^2 = \dots$. Izračunamo korenske podprostore

- za lastno vrednost 0: $\text{Ker}(A - 0I) = \text{Ker}(A) = \text{Ker}(A^2)$. Dobimo eno verigo $((1, 0, 0, 0))$ dolžine 1 za lastno vrednost 0.
- za lastno vrednost 2: $\text{Ker}(A - 2I)^2 = \mathcal{L}\text{in}\{(1, 0, 0, 2), (-1, 0, 1, 0), (1, 2, 0, 0)\}$, $\text{Ker}(A - 2I)^3 = \text{Ker}(A - 2I)^2$. Opazimo, da je $(1, 0, 0, 2)$ dopolnitev baze $\text{Ker}(A - 2I)$ do baze $\text{Ker}(A - 2I)^2$. Torej je $\{(1, 0, 0, 2)\}$ „popravljena baza“ N^2 . Preslikamo $(A - 2I)(1, 0, 0, 2) = (2, 4, 0, 0)$, kar tvori verigo dolžine 2 $((1, 0, 0, 2), (2, 4, 0, 0))$. Edini linearno neodvisen od $(2, 4, 0, 0)$ v B_1 je $(3, 0, -2, 2)$, zato je slednji začetek zadnje tretje verige dolžine 1 $((3, 0, -2, 2))$.

Tri verige, ki jih dobimo, so $((1, 0, 0, 0))$ za lastno vrednost 0 in $((1, 0, 0, 2), (2, 4, 0, 0))$ ter $((3, 0, -2, 2))$ obe za lastno vrednost 2. Zložimo jih v matriko P :

$$P = \begin{bmatrix} 1 & 1 & 2 & 3 \\ 0 & 0 & 4 & 0 \\ 0 & 0 & 0 & -2 \\ 0 & 2 & 0 & 2 \end{bmatrix}$$

V matriko J pa zložimo kletke pripadajočih velikosti:

$$J = \begin{bmatrix} 0 & & & 0 \\ & 2 & 1 & \\ & & 2 & \\ 0 & & & 2 \end{bmatrix}$$

In velja $A = PJP^{-1}$ (P^{-1} izračunamo z Gaussom).

2.1.13 Funkcije matrik

Če poznamo razcep $A = PJP^{-1}$, prevedemo računanje potenc A na računanje potenc matrike J , kajti

$$A^n = (PJP^{-1})(PJP^{-1}) \dots (PJP^{-1}) = PJP^{-1}PJP^{-1} \dots PJP^{-1} = PJ^n P^{-1}.$$

Ker je J bločno diagonalna matrika, sestavljena iz jordanskih kletk, se potenciranje J prevede na potenciranje kletk, kajti

$$J^n = \begin{bmatrix} J_1^n & & 0 \\ & \ddots & \\ 0 & & J_m^n \end{bmatrix}.$$

Potenciranje jordanske kletke:

$$\begin{aligned} & \begin{bmatrix} \lambda & 1 & & 0 \\ & \lambda & 1 & \\ & & \ddots & \ddots \\ 0 & & & \lambda & 1 \\ & & & & \lambda \end{bmatrix}^n = \left(\lambda I + \begin{bmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{bmatrix} \right)^n = (\lambda I + N)^n = \\ & = \binom{n}{0} (\lambda I)^n N^0 + \binom{n}{1} (\lambda I)^{n-1} N^1 + \dots + \binom{n}{n} (\lambda I)^0 N^n = \binom{n}{0} \lambda^n + \binom{n}{1} \lambda^{n-1} N^1 + \dots + \binom{n}{n} N^n \end{aligned}$$

Poraja se vprašanje, kako potencirati $N = \begin{bmatrix} 0 & 1 & & 0 \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ 0 & & & 0 \end{bmatrix}$. Velja $N^2 = \begin{bmatrix} 0 & 0 & 1 & 0 \\ & \ddots & \ddots & \ddots \\ & & \ddots & 1 \\ 0 & & & 0 \end{bmatrix}$ in tako

dalje („diagonalno“ enic pomikamo gor in desno). Za $r \times r$ jordansko kletko, kadar $n \geq r$ (sicer dobimo le prvih nekaj naddiagonal), sledi

$$\begin{bmatrix} \lambda & 1 & & 0 \\ & \lambda & 1 & \\ & & \ddots & \ddots \\ 0 & & & \lambda & 1 \\ & & & & \lambda \end{bmatrix}^n = \begin{bmatrix} \lambda^n & n\lambda^{n-1} & \dots & \binom{n}{r-2}\lambda^{n-r+2} & \binom{n}{r-1}\lambda^{n-r+1} \\ & \lambda^n & n\lambda^{n-1} & \ddots & \binom{n}{r-2}\lambda^{n-r+2} \\ & & \ddots & \ddots & \vdots \\ & & & \lambda^n & n\lambda^{n-1} \\ 0 & & & & \lambda^n \end{bmatrix}$$

Za računanje poljubne funkcije jordske kletke pa velja predpis

$$f \left(\begin{bmatrix} \lambda & 1 & & & 0 \\ & \lambda & 1 & & \\ & & \ddots & \ddots & \\ & & & \lambda & 1 \\ 0 & & & & \lambda \end{bmatrix} \right) = \begin{bmatrix} f(\lambda) & f'(\lambda) & \frac{f''(\lambda)}{2} & \dots & \frac{f^{(k-1)}(\lambda)}{(k-1)!} \\ & f(\lambda) & f'(\lambda) & \ddots & \dots \\ & & \ddots & \ddots & \frac{f''(\lambda)}{2} \\ & & & f(\lambda) & f'(\lambda) \\ 0 & & & & f(\lambda) \end{bmatrix}$$

In torej za računanje poljubne funkcije poljubne matrike $f(A) = f(PJP^{-1}) = Pf(J)P^{-1}$.

2.2 Vektorski prostori s skalarnim produktom

Definicija. Naj bo V vektorski prostor nad poljem \mathbb{R} nenujno končno razsežen. Preslikavi $\langle \cdot, \cdot \rangle : V \times V \rightarrow \mathbb{R}$ pravimo skalarni produkt, če zadošča naslednjim lastnostim:

1. pozitivna definitnost: $\forall v \in V : v \neq 0 \Rightarrow \langle v, v \rangle > 0$
2. simetričnost: $\forall u, v \in V : \langle v, u \rangle = \langle u, v \rangle$
3. linearnost v prvem faktorju: $\forall \alpha_1, \alpha_2 \in \mathbb{R}, v_1, v_2 \in V : \langle \alpha_1 v_1 + \alpha_2 v_2, v \rangle = \alpha_1 \langle v_1, v \rangle + \alpha_2 \langle v_2, v \rangle$

Posledica. *linearnost v drugem faktorju.* $\langle u, \beta_1 v_1 + \beta_2 v_2 \rangle = \langle \beta_1 v_1 + \beta_2 v_2, v \rangle = \beta_1 \langle v_1, v \rangle + \beta_2 \langle v_2, v \rangle = \beta_1 \langle v, v_1 \rangle + \beta_2 \langle v, v_2 \rangle$.

Posledica. *Skalarni produkt z 0:* $\langle 0, v \rangle = \langle 0 \cdot v + 0 \cdot v, v \rangle = 0 \langle v, v \rangle + 0 \langle v, v \rangle = 0 \Rightarrow \langle v, 0 \rangle = 0$

Posledica. *Alternativna formulacija 1:* $\forall v \in V : \langle v, v \rangle \geq 0 \wedge \langle v, v \rangle = 0 \Leftrightarrow v = 0$.

Zgled. Primeri vektorskih prostorov s skalarnim produktom:

- \mathbb{R}^n s standardnim skalarnim produktom: $\langle (\alpha_1, \dots, \alpha_n), (\beta_1, \dots, \beta_n) \rangle = \alpha_1 \beta_1 + \dots + \alpha_n \beta_n$.
- \mathbb{R}^n z nestandardnim skalarnim produktom: Za pojube $\gamma_1 > 0, \dots, \gamma_n > 0$ definirajmo $\langle (\alpha_1, \dots, \alpha_n), (\beta_1, \dots, \beta_n) \rangle = \gamma_1 \alpha_1 \beta_1 + \dots + \gamma_n \alpha_n \beta_n$.
- neskončno razsežen primer s standardnim skalarnim produktom: $V = C[a, b] \sim$ zvezne $f : [a, b] \rightarrow \mathbb{R}$. Definirajmo $\forall f, g \in V : \langle f, g \rangle = \int_a^b f(x)g(x)dx$. Zveznost je potrebna za dokaz aksioma 1, sicer za neznano neničelno funkcijo $f(x) = \begin{cases} 1 & ; x = 0 \\ 0 & ; \text{drugače} \end{cases}$ velja $\int_a^b f(x)g(x)dx = 0$. Temu pravimo standardni skalarni produkt v $C[a, b]$.
- neskončno razsežen primer z nestandardnim skalarnim produktom: Naj bo $w : [a, b] \rightarrow \mathbb{R}$ zvezna, ki zadošča $\forall x \in [a, b] : w(x) > 0$. Ostalo kot prej. $\forall f, g \in V : \langle f, g \rangle_w = \int_a^b f(x)g(x)w(x)dx$.

Pripomba. Vektorski prostor s skalarnim produktom je tak par $(V, \langle \cdot, \cdot \rangle)$, kjer je $\langle \cdot, \cdot \rangle$ skalarni produkt na V . To je torej vektorski prostor, za katerega izberemo in fiksiramo skalarni produkt.

Definicija. Naj bo V vektorski prostor nad poljem \mathbb{C} nenujno končno razsežen. Preslikavi $\langle \cdot, \cdot \rangle : V \times V \rightarrow \mathbb{C}$ pravimo skalarni produkt, če zadošča naslednjim lastnostim:

1. pozitivna definitnost: $\forall v \in V : v \neq 0 \Rightarrow \langle v, v \rangle \in \mathbb{R} \wedge \langle v, v \rangle > 0$
2. konjugirana simetričnost: $\forall u, v \in V : \langle v, u \rangle = \overline{\langle u, v \rangle}$
3. linearnost v prvem faktorju: $\forall \alpha_1, \alpha_2 \in \mathbb{R}, v_1, v_2 \in V : \langle \alpha_1 v_1 + \alpha_2 v_2, v \rangle = \alpha_1 \langle v_1, v \rangle + \alpha_2 \langle v_2, v \rangle$

Posledica. *konjugirana linearnost v drugem faktorju.* $\langle u, \beta_1 v_1 + \beta_2 v_2 \rangle = \overline{\langle \beta_1 v_1 + \beta_2 v_2, v \rangle} = \overline{\beta_1 \langle v_1, v \rangle + \beta_2 \langle v_2, v \rangle} = \overline{\beta_1} \overline{\langle v_1, v \rangle} + \overline{\beta_2} \overline{\langle v_2, v \rangle} = \overline{\beta_1} \langle v, v_1 \rangle + \overline{\beta_2} \langle v, v_2 \rangle$.

Posledica. *Skalarni produkt z 0:* $\langle 0, v \rangle = \langle 0 \cdot v + 0 \cdot v, v \rangle = 0 \langle v, v \rangle + 0 \langle v, v \rangle = 0 \Rightarrow \langle v, 0 \rangle = 0$

Posledica. *Alternativna formulacija 1:* $\forall v \in V : \langle v, v \rangle \in \mathbb{R} \wedge \langle v, v \rangle \geq 0 \wedge \langle v, v \rangle = 0 \Leftrightarrow v = 0$.

Zgled. Primeri vektorskih prostorov s skalarnim produktom:

- standardni skalarni produkt na \mathbb{C}^n : $\langle (\alpha_1, \dots, \alpha_n), (\beta_1, \dots, \beta_n) \rangle = \alpha_1 \overline{\beta_1} + \dots + \alpha_n \overline{\beta_n}$.
- nestandardni skalarni produkt na \mathbb{C}^n : Za neke $\gamma_1 \in \mathbb{R}^+, \dots, \gamma_n \in \mathbb{R}^+$ definiramo $\langle (\alpha_1, \dots, \alpha_n), (\beta_1, \dots, \beta_n) \rangle = \gamma_1 \alpha_1 \overline{\beta_1} + \dots + \gamma_n \alpha_n \overline{\beta_n}$.
- neskončno razsežen vektorski prostor na \mathbb{C}^n s standardnim skalarnim produktom: Naj bo $V = C([a, b], \mathbb{C})$ — $f = g + ih$ za $g, h \in C[a, b]$ (zvezni funkciji iz $[a, b]$ v \mathbb{R}). Definiramo $\langle f_1, f_2 \rangle = \int_a^b f_1(x) \overline{f_2(x)} dx = \int_a^b (g_1 + ih_1)(x) (g_2 - ih_2)(x) dx = \int_a^b (g_1 g_2 + g_1 g_2)(x) dx + i \int_a^b (h_1 g_2 - g_1 h_2) x dx$.
- neskončno razsežen vektorski prostor na \mathbb{C}^n z nestandardnim skalarnim produktom: Isto kot zgoraj, le da spet množimo z nekimi funkcijami, kot pri realnem skalarnem produktu.

2.2.1 Norma

Definicija. Naj bo V vektorski prostor s skalarnim produktom. $\forall v \in V : \|v\| = \sqrt{\langle v, v \rangle}$ je norma v .

Osnovne lastnosti norme

1. $(\|v\| > 0 \Leftrightarrow v \neq 0) \wedge \|0\| = 0$ sledi iz prvega aksioma skalarnega produkta
2. $\forall \alpha \in F, v \in V : \|\alpha v\| = |\alpha| \|v\|$
3. trikotniška neenakost: $\forall u, v \in V : \|u + v\| \leq \|u\| + \|v\|$ sledi iz Cauchy-Schwarzove neenakosti na običajen način.

Trditev. Cauchy-Schwarz. Za V vektorski prostor s skalarnim produktom velja $\forall v \in V : |\langle u, v \rangle| \leq \|u\| \cdot \|v\|$.

Dokaz. Za $v = 0$ očitno velja $0 = 0$. Za $v \neq 0$ definirajmo

$$w = u - \frac{\langle u, v \rangle}{\langle v, v \rangle} v$$

po prvi lastnosti velja

$$0 \leq \langle w, w \rangle = \left\langle w, u - \frac{\langle u, v \rangle}{\langle v, v \rangle} v \right\rangle = \langle w, u \rangle - \frac{\overline{\langle u, v \rangle}}{\langle v, v \rangle} \langle w, v \rangle$$

Oglejmo si

$$\langle w, v \rangle = \left\langle u - \frac{\langle u, v \rangle}{\langle v, v \rangle} v, v \right\rangle = \langle u, v \rangle - \frac{\langle u, v \rangle}{\langle v, v \rangle} \langle v, v \rangle = \langle u, v \rangle - \frac{\langle u, v \rangle}{\langle v, v \rangle} \langle v, v \rangle = 0$$

In se vrnimo k prejšnji enačbi:

$$\begin{aligned} 0 \leq \langle w, w \rangle &= \left\langle u - \frac{\langle u, v \rangle}{\langle v, v \rangle} v, u - \frac{\langle u, v \rangle}{\langle v, v \rangle} v \right\rangle = \langle w, u \rangle - \frac{\overline{\langle u, v \rangle}}{\langle v, v \rangle} \langle w, v \rangle = \langle w, u \rangle - 0 = \langle w, u \rangle \\ &= \left\langle u - \frac{\langle u, v \rangle}{\langle v, v \rangle} v, u \right\rangle = \langle u, u \rangle - \frac{\langle u, v \rangle}{\langle v, v \rangle} \langle v, u \rangle = \|u\|^2 - \frac{\langle u, v \rangle \overline{\langle u, v \rangle}}{\|v\|^2} = \|u\|^2 - \frac{|\langle u, v \rangle|^2}{\|v\|^2} \\ 0 &\leq \|u\|^2 - \frac{|\langle u, v \rangle|^2}{\|v\|^2} \\ \frac{|\langle u, v \rangle|^2}{\|v\|^2} &\leq \|u\|^2 \\ |\langle u, v \rangle|^2 &\leq \|u\|^2 \|v\|^2 \\ |\langle u, v \rangle| &\leq \|u\| \cdot \|v\| \end{aligned}$$

□

Trditev. Z normo lahko izrazimo skalarni produkt:

- V \mathbb{R} : $\langle u, v \rangle = \frac{1}{4} (||u+v||^2 - ||u-v||^2)$
- V \mathbb{C} : $\langle u, v \rangle = \sum_{k=0}^3 i^k ||u + i^k v||^2$

Dokaz. Dokaz v \mathbb{C} . Oglejmo si

$$\begin{aligned} ||u + i^k v||^2 &= \langle u + i^k v, u + i^k v \rangle = \langle u, u + i^k v \rangle + i^k \langle v, u + i^k v \rangle = \overline{\langle u + i^k v, u \rangle} + i^k \overline{\langle u + i^k v, v \rangle} = \\ &= \overline{\langle u, u \rangle} + \overline{\langle i^k v, u \rangle} + i^k \overline{\langle u, v \rangle} + i^k \overline{\langle i^k v, v \rangle} = \langle u, u \rangle + \langle u, i^k v \rangle + i^k \langle v, u \rangle + i^k \langle v, i^k v \rangle = \\ &= \langle u, u \rangle + (-i^k) \langle u, v \rangle + i^k \langle v, u \rangle + i^k (-i^k) \langle v, v \rangle = \\ &= \langle u, u \rangle + (-i^k) \langle u, v \rangle + i^k \langle v, u \rangle + 1 \langle v, v \rangle \end{aligned}$$

Dodajmo vsoto:

$$\begin{aligned} \sum_{k=0}^3 i^k ||u + i^k v||^2 &= \sum_{k=0}^3 i^k (\langle u, u \rangle + (-i^k) \langle u, v \rangle + i^k \langle v, u \rangle + 1 \langle v, v \rangle) = \\ &= \sum_{k=0}^3 i^k \langle u, u \rangle + \sum_{k=0}^3 i^k (-i^k) \langle u, v \rangle + \sum_{k=0}^3 i^k i^k \langle v, u \rangle + \sum_{k=0}^3 i^k \langle v, v \rangle = 0 + \sum_{k=0}^3 i^k (-i^k) \langle u, v \rangle + 0 + 0, \end{aligned}$$

kajti $\sum_{k=0}^3 i^k = 1 + i + (-1) + (-i) = 0$ in $\sum_{k=0}^3 i^{2k} = 1 + (-1) + 1 + (-1) = 0$. Nadaljujmo:

$$= \sum_{k=0}^3 i^k (-i^k) \langle u, v \rangle = \sum_{k=0}^3 1 \langle u, v \rangle = 4 \langle u, v \rangle$$

□

2.2.2 Ortogonalne množice in ortogonalne baze

Definicija. Naj bo V VPSSP $\forall u, v \in V : u \perp v \Leftrightarrow \langle u, v \rangle = 0$.

Pripomba. trivialne opombe. $\forall v \in V : v \perp \vec{0}$, $\forall v \in V : v \neq 0 \Leftrightarrow v \not\perp v$ (prvi aksiom skalarnega produkta), $\forall v \in V : u \perp v \Leftrightarrow v \perp u$.

Definicija. Naj bo V VPSSP in $v_1, \dots, v_k \in V$. Množica $\{v_1, \dots, v_k\}$ je:

- ortogonalna, če $v_1 \neq 0 \wedge \dots \wedge v_k \neq 0$ in $\forall i, j \in \{1..k\} : i \neq j \Rightarrow v_i \perp v_j$.
- normirana, če $\forall v \in \{v_1, \dots, v_k\} : ||v|| = 1$.
- ortonormirana, če je ortogonalna in ortonormirana hkrati.

Pripomba. Iz (ortogonalne) množice $\{v_1, \dots, v_k\}$ dobimo (orto)normirano tako, da vsak element delimo z njegovo normo. $\left\{ \frac{v_1}{||v_1||}, \dots, \frac{v_k}{||v_k||} \right\}$ je vedno normirana.

Trditev. Vsaka ortogonalna množica je linearno neodvisna.

Dokaz. Denimo, da je $\{v_1, \dots, v_k\}$ ortogonalna. Vzemimo take $\alpha_1, \dots, \alpha_k \ni: \alpha_1 v_1 + \dots + \alpha_k v_k = 0$. $\alpha_1 = \dots = \alpha_k = 0$.

$$\forall i \in \{1..k\} : 0 = \langle 0, v_i \rangle = \langle \alpha_1 v_1 + \dots + \alpha_k v_k, v_i \rangle = \alpha_1 \langle v_1, v_i \rangle + \dots + \alpha_i \langle v_i, v_i \rangle + \dots + \alpha_k \langle v_k, v_i \rangle = \dots$$

Ker je množica ortogonalna, je $\langle v_l, v_k \rangle = 0 \Leftrightarrow l \neq k$. Nadaljujmo ...

$$\dots = \alpha_i \langle v_i, v_i \rangle$$

Ker $\langle v_i, v_i \rangle$ ni 0, ker je v_i neničeln (da, tudi to je del definicije ortogonalnosti), je $\alpha_i = 0$. In to za vsak i . □

Ni pa vsaka ortogonalna množica ogrodje. Ortogonalni množici, ki je ogrodje, rečemo ortogonalna baza (LN sledi iz ortogonalnost).

Trditev. Naj bo $\{w_1, \dots, w_k\}$ ortogonalna baza za W . Formula za ortogonalno projekcijo se glasi:

$$v' = \frac{\langle v, w_1 \rangle}{\langle w_1, w_1 \rangle} w_1 + \dots + \frac{\langle v, w_k \rangle}{\langle w_k, w_k \rangle} = \sum_{i=1}^k \frac{\langle v, w_i \rangle}{\langle w_i, w_i \rangle} w_i$$

Dokaz. Dokažimo, da je $v - \sum_{i=1}^k \frac{\langle v, w_i \rangle}{\langle w_i, w_i \rangle} w_i$ pravokoten na vse elemente W . Zaradi linearnosti skalarnega produkta zadošča preveriti, da je pravokoten na bazo W . $\forall j \in \{1..k\}$ velja (spomnimo se, da je $\langle w_i, w_j \rangle = 0 \Leftrightarrow i \neq j$, zato po drugem enačaju ostane le še en člen vsote):

$$\begin{aligned} \left\langle v - \sum_{i=1}^k \frac{\langle v, w_i \rangle}{\langle w_i, w_i \rangle} w_i, w_j \right\rangle &= \langle v, w_j \rangle - \sum_{i=1}^k \frac{\langle v, w_i \rangle}{\langle w_i, w_i \rangle} \langle w_i, w_j \rangle = \langle v, w_j \rangle - \frac{\langle v, w_j \rangle}{\langle w_j, w_j \rangle} \langle w_j, w_j \rangle = \\ &= \langle v, w_j \rangle - \langle v, w_j \rangle = 0 \end{aligned}$$

□

2.2.6 Obstoje ortogonalne baze — Gram-Schmidtova ortogonalizacija

Radi bi dokazali, da ima vsak KRPSSP ortogonalno bazo in da je moč vsako ortogonalno množico dopolniti do ortogonalne baze. Konstruktiven dokaz ☺! — postopek, imenovan Gram-Schmidtova ortogonalizacija, iz poljubne baze naredi ortogonalno.

Naj bo V KRPSSP in $\{u_1, \dots, u_n\}$ njegova poljubna baza. Naj bo $v_1 := u_1$,

$$\begin{aligned} v_2 &:= u_2 - \frac{\langle u_2, v_1 \rangle}{\langle v_1, v_1 \rangle} v_1 = u_2 - u'_2 \\ v_3 &:= u_3 - \frac{\langle u_3, v_1 \rangle}{\langle v_1, v_1 \rangle} v_1 - \frac{\langle u_3, v_2 \rangle}{\langle v_2, v_2 \rangle} v_2 = u_3 - u'_3 \\ &\dots \\ v_n &:= u_n - \sum_{i=1}^{n-1} \frac{\langle u_n, v_i \rangle}{\langle v_i, v_i \rangle} v_i = u_n - u'_n \end{aligned}$$

Trdimo, da je $\{v_1, \dots, v_n\}$ ortogonalna baza za V .

Opazimo, da je u'_2 ortogonalna projekcija u_2 na $\mathcal{L}\text{in}\{v_1\}$, u'_3 ortogonalna projekcija u_3 na $\mathcal{L}\text{in}\{v_1, v_2\}$, ..., u'_n pa ortogonalna projekcija na $\mathcal{L}\text{in}\{v_1, \dots, v_{n-1}\}$, torej

$$v_2 = u_2 - u'_2 \perp \mathcal{L}\text{in}\{v_1\}, \text{ torej } v_2 \perp v_1$$

$$v_3 = u_3 - u'_3 \perp \mathcal{L}\text{in}\{v_1, v_2\}, \text{ torej } v_3 \perp v_1, v_3 \perp v_2$$

...

$$v_n = u_n - u'_n \perp \mathcal{L}\text{in}\{v_1, \dots, v_{n-1}\}, \text{ torej } v_n \perp v_1, \dots, v_n \perp v_{n-1},$$

kar pomeni, da so $\{v_1, \dots, v_n\}$ paroma ortogonalni. Toda vprašanje je, ali so neničelni, kajti to je, ne boste verjeli, prav tako pogoj za ortogonalno množico. $\forall i \in \{1..n\}$: dokažimo neničelnost v_i :-)

v_1 je neničeln, ker je enak u_1 , ki je element baze V . v_2 je neničeln, ker je $v_2 = u_2 - \alpha v_1$ in $u_2 \neq \alpha v_1$, ker sta linearno neodvisna, ker tvorita ortogonalno množico. v_3 je neničeln, ker $v_3 = u_3 - (\beta v_1 + \gamma v_2)$ in ker so v_1, v_2, u_3 LN, $u_3 \neq (\beta v_1 + \gamma v_2)$. In tako dalje.

Dopolnitev ortogonalne množice do baze Naj bo $\{u_1, \dots, u_k\}$ ortogonalna množica, torej je linearno neodvisna, torej jo lahko dopolnimo do baze. $\{u_{k+1}, \dots, u_n\}$ je dopolnitev do baze. Toda slednja še ni ortogonalna. A nič ne de, uporabimo lahko Gram-Schmidtovo ortogonalizacijo na $\{u_1, \dots, u_k, u_{k+1}, \dots, u_n\}$ in dobimo ortogonalno bazo $\{v_1, \dots, v_n\}$. Opazimo, da ker so po predpostavki u_1, \dots, u_k ortogonalni, velja $v_1 = u_1, \dots, v_k = u_k$ (po GS).

Zgled. primer GS ortogonalizacije iz analize. Naj bo $V = \mathbb{R}[x]_{\leq 3}$. Baza: $u_1 = 1, u_2 = x, u_3 = x^2, u_4 = x^3$, skalarni produkt naj bo $\langle p, q \rangle = \int_{-1}^1 p(x)q(x) dx$. Konstruirajmo pripadajočo ortogonalno bazo v_1, \dots, v_4 :

$$\begin{aligned} v_1 &:= u_1 = 1 \\ v_2 &:= u_2 - \frac{\langle u_2, v_1 \rangle}{\langle v_1, v_1 \rangle} v_1 = x - \frac{\int_{-1}^1 x dx}{\int_{-1}^1 dx} = x - 0 = x = u_2 \\ v_3 &:= u_3 - \frac{\langle u_3, v_1 \rangle}{\langle v_1, v_1 \rangle} v_1 - \frac{\langle u_3, v_2 \rangle}{\langle v_2, v_2 \rangle} v_2 = x^2 - \frac{\int_{-1}^1 x^2 dx}{\int_{-1}^1 dx} - \frac{\int_{-1}^1 x^3 dx}{\int_{-1}^1 x^2 dx} x = \dots = x^2 - \frac{1}{3} \\ v_4 &:= \dots = x^2 - \frac{3}{5}x \end{aligned}$$

Sklep: $\{1, x, x^2 - \frac{1}{3}, x^2 - \frac{3}{5}x\}$ je ortogonalna baza za ta vektorski prostor s tem skalarnim produktom. Normirajmo jo! Norme teh baznih vektorjev po vrsti so $\sqrt{2}, \sqrt{\frac{2}{3}}, \sqrt{\frac{8}{45}}, \sqrt{\frac{8}{175}}$. Pripadajoča ortonormirana baza je torej $\left\{ \frac{1}{\sqrt{2}}, \frac{x}{\sqrt{\frac{2}{3}}}, \frac{x^2 - \frac{1}{3}}{\sqrt{\frac{8}{45}}}, \frac{x^2 - \frac{3}{5}x}{\sqrt{\frac{8}{175}}} \right\}$. Normiranje bi sicer prineslo lepše formule, vendar bi v račune prineslo te objektivno grde konstante.

2.2.7 Ortogonalni komplement

Definicija 4. Naj bo V KRPVSSP nad F in $S \subseteq V$. Ortogonalni komplement S je množica S^\perp . Vsebuje vse tiste vektorje iz V , ki so ortogonalni na S . ZDB $S^\perp := \{v \in V; \forall s \in S : v \perp s\} = \{v \in V; v \perp S\}$.

Trditev. $\forall S \subseteq V : S^\perp$ je podprostor V .

Dokaz. Dokazati je treba $\forall u_1, u_2 \in S^\perp, \alpha_1, \alpha_2 \in F : \alpha_1 u_1 + \alpha_2 u_2 \in S^\perp$. Po definiciji ortogonalnega komplementa velja

$$\forall s \in S : \langle u_1, s \rangle = 0 \wedge \langle u_2, s \rangle = 0 \implies 0 = \alpha_1 \langle u_1, s \rangle + \alpha_2 \langle u_2, s \rangle = \langle \alpha_1 u_1 + \alpha_2 u_2, s \rangle \implies \alpha_1 u_1 + \alpha_2 u_2 \in S^\perp$$

□

Izrek. *ortogonalni razcep.* Naj bo V KRPVSSP in W vektorski podprostor V . Potem velja $V = W \oplus W^\perp$ (ortogonalni razcep glede na W).

Dokaz. Naj bo $v \in V$ pojučen, V^\perp pa ortogonalna projekcija V na W . Potem velja, da je $v = v - v' + v'$, kjer je $v - v'$ pravokoten na W , v' pa element v' , torej $v \in W \oplus W^\perp$. Vsota je direktna, kajti $\forall v \in W \cap W^\perp : v \perp v \Leftrightarrow v \perp v \Leftrightarrow \langle v, v \rangle = 0 \Leftrightarrow v = 0 \implies W \cap W^\perp = \{0\}$ (po karakterizaciji direktnih vsot). □

Trditev. Naj bo V KRPVSSP in W vektorski podprostor v V . Velja $(W^\perp)^\perp = W$.

Dokaz. Po definiciji ortogonalnega komplementa je $W \subseteq (W^\perp)^\perp$, ker $W \perp W^\perp$. Dokažimo $\dim W = \dim (W^\perp)^\perp$. Ortogonalni razcep glede na W je $V = W \oplus W^\perp \Rightarrow \dim W + \dim W^\perp = \dim V$, ortogonalni razcep glede na W^\perp pa je $V = W^\perp \oplus (W^\perp)^\perp \Rightarrow \dim W^\perp + \dim (W^\perp)^\perp = \dim V$.

$$\dim V = \dim V$$

$$\dim W + \dim W^\perp = \dim W^\perp + \dim (W^\perp)^\perp$$

$$\dim W = \dim (W^\perp)^\perp$$

Alternativni dokaz: Naj bodo w_1, \dots, w_k OB za W . Dopolnimo jo do OB za V z GS z w_{k+1}, \dots, w_n . Tedaj je w_{k+1}, \dots, w_n OB za W^\perp in ker je w_1, \dots, w_n njena dopolnitev do OB V , je w_1, \dots, w_k OB za $(W^\perp)^\perp$, torej $W^\perp = (W^\perp)^\perp$, saj imata isti ortogonalni bazi. □

2.3 Adjungirana linearna preslikava

Definicija. Naj bo V vektorski prostor nad F . Vemo, da je F vektorski prostor nad F . Linearnim preslikavam $V \rightarrow F$ pravimo linearni funkcionali na V .

Zgled. Naj bo V VPSSP in $F \in \{\mathbb{R}, \mathbb{C}\}$. Naj bo $w \in V$. Naj bo $\varphi : V \rightarrow F$ (torej je φ linearni funkcional), ki slika $v \mapsto \langle v, w \rangle$. Preslikava je po aksiomu 3 za skalarni produkt linearna.

Izrek. *Rieszov izrek o reprezentaciji linearnih funkcionalov.* Naj bo V KRVPSPP. Za vsak linearen funkcional φ na V obstaja natanko en vektor $w \in V \ni \forall v \in V : \varphi(v) = \langle v, w \rangle$. ZDB slednja konstrukcija nam da vse linearne funkcionale.

Dokaz. Dokazujemo enolično eksistenco:

- Eksistenca w : Vzemimo poljubno OB w_1, \dots, w_n za V . $\forall v \in V : v = \langle v, w_1 \rangle w_1 + \dots + \langle v, w_n \rangle w_n$. (fourierov razvoj po OB). Ker je φ linearna, velja

$$\begin{aligned} \varphi(v) &= \varphi(\langle v, w_1 \rangle w_1 + \dots + \langle v, w_n \rangle w_n) \stackrel{\text{linearna}}{=} \langle v, w_1 \rangle \varphi w_1 + \dots + \langle v, w_n \rangle \varphi w_n \stackrel{\text{konj. hom. v 2. fakt.}}{=} \\ &= \langle v, \overline{\varphi w_1} w_1 \rangle + \dots + \langle v, \overline{\varphi w_n} w_n \rangle \stackrel{\text{konj. ad. v 2. fakt.}}{=} \langle v, (\varphi w_1) w_1 + \dots + (\varphi w_n) w_n \rangle \end{aligned}$$

Za dan φ smo konstruirali eksplicitno formulo za iskani w .

- Enoličnost w : PDDRAA $\forall v \in V : \varphi(v) = \langle v, w_1 \rangle = \langle v, w_2 \rangle$. Teda $\forall v \in V : \langle v, w_1 - w_2 \rangle = 0$. Vzemimo konkreten $v = w_1 - w_2$ in ga vstavimo v formulo $\langle v, w_1 - w_2 \rangle = 0 = \langle w_1 - w_2, w_1 - w_2 \rangle = 0 \Rightarrow w_1 - w_2 = 0 \Rightarrow w_1 = w_2$.

□

Definicija. Naj bosta U, V KRVPSPP in $L : U \rightarrow V$ linearna. Adjungirana linearna preslikava, pripadajoča L , je taka $L^* : V \rightarrow U$, da velja $\forall u \in U, v \in V : \langle Lu, v \rangle = \langle u, L^*v \rangle$. Levi skalarni produkt je tisti iz V , desni pa tisti iz U .

Trditev. Da lahko pišemo L^* , trdimo, da je L^* vedno obstaja in to vselej enolično.

Dokaz. Dokazujemo enolično eksistenco:

- Enoličnost: Naj bosta L^* in L° dve adjungirani linearni preslikavi za L , torej $\forall u \in U, v \in V : \langle Lu, v \rangle = \langle u, L^*v \rangle = \langle u, L^\circ v \rangle$. Torej

$$\begin{aligned} \langle u, L^*v \rangle &= \langle u, L^\circ v \rangle \\ 0 &= \langle u, L^*v - L^\circ v \rangle \end{aligned}$$

Za vsaka u in v . Sedaj vstavimo $u = L^*v - L^\circ v$:

$$0 = \langle L^*v - L^\circ v, L^*v - L^\circ v \rangle \implies L^*v - L^\circ v = 0 \implies \forall v \in V : L^*v = L^\circ v$$

- Eksistenca: Naj bosta U, V KRVPSPP in $L : U \rightarrow V$. Naj bo $v \in V$ poljuben. Vpeljimo linearni funkcional $\varphi : U \rightarrow F$ s predpisom $u \mapsto \langle Lu, v \rangle$. Prepričajmo se, da je ta funkcional linearna preslikava:

$$\varphi(\alpha_1 u_1 + \alpha_2 u_2) = \langle L(\alpha_1 u_1 + \alpha_2 u_2), v \rangle = \langle \alpha_1 Lu_1 + \alpha_2 Lu_2, v \rangle = \alpha_1 \langle Lu_1, v \rangle + \alpha_2 \langle Lu_2, v \rangle$$

Uporabimo Rieszov izrek za funkcional φ : $\exists! w \in U \ni \forall u \in U : \varphi u = \langle u, w \rangle$. Vpeljimo $L^*v = w$, s čimer za poljuben v definiramo L^*v . Dokažimo, da je dobljena preslikava linearna: $L^*(\beta_1 v_1 + \beta_2 v_2) = \beta_1 L^*v_1 + \beta_2 L^*v_2$. Vzemimo poljuben $u \in U$ in računajmo (fino bi bilo dobiti nič):

$$\begin{aligned} \langle u, L^*(\beta_1 v_1 + \beta_2 v_2) - (\beta_1 L^*v_1 + \beta_2 L^*v_2) \rangle &= \langle u, L^*(\beta_1 v_1 + \beta_2 v_2) - \beta_1 L^*v_1 - \beta_2 L^*v_2 \rangle \stackrel{\text{kl2f}}{=} \\ &= \langle u, L^*(\beta_1 v_1 + \beta_2 v_2) \rangle - \overline{\beta_1} \langle u, L^*v_1 \rangle - \overline{\beta_2} \langle u, L^*v_2 \rangle \stackrel{\text{lin } L^*}{=} \langle u, \beta_1 L^*v_1 + \beta_2 L^*v_2 \rangle - \overline{\beta_1} \langle u, L^*v_1 \rangle - \overline{\beta_2} \langle u, L^*v_2 \rangle = \\ &= \overline{\beta_1} \langle u, L^*v_1 \rangle + \overline{\beta_2} \langle u, L^*v_2 \rangle - \overline{\beta_1} \langle u, L^*v_1 \rangle - \overline{\beta_2} \langle u, L^*v_2 \rangle = 0 \end{aligned}$$

Ker to velja za vsak u , velja tudi za $u = L^*(\beta_1 v_1 + \beta_2 v_2) - (\beta_1 L^*v_1 + \beta_2 L^*v_2)$, torej dobimo

$$\langle L^*(\beta_1 v_1 + \beta_2 v_2) - (\beta_1 L^*v_1 + \beta_2 L^*v_2), L^*(\beta_1 v_1 + \beta_2 v_2) - (\beta_1 L^*v_1 + \beta_2 L^*v_2) \rangle = 0$$

torej po prvem aksiomu za skalarni produkt velja linearnost:

$$\begin{aligned} L^*(\beta_1 v_1 + \beta_2 v_2) - (\beta_1 L^*v_1 + \beta_2 L^*v_2) &= 0 \\ L^*(\beta_1 v_1 + \beta_2 v_2) &= \beta_1 L^*v_1 + \beta_2 L^*v_2 \end{aligned}$$

□

Zgled. Naj bo $A \in M_{m \times n}(F)$ s pripadajočo linearno preslikavo $L_A = F^n \rightarrow F^m$, ki slika $v \mapsto Av$. Kako izgleda matrika L_{A^*} ? Odgovor je odvisen od izbire skalarnega produkta. Izberimo standardni skalarni produkt v F^n in F^m in $L_{A^*} : F^m \rightarrow F^n$ definiramo z $v \mapsto A^*v$, kjer je $A^* = \overline{A^T}$, torej transponiranka A z vsemi elementi konjugiranimi. Izkaže se, da je potemtakem L_{A^*} adjungirana linearna preslikava od L_A .

2.3.1 Matrika adjungirane linearne preslikave

Naj bosta U, V KRVPSPP in naj bo $\mathcal{B} = \{u_1, \dots, u_n\}$ ONB za U in $\mathcal{C} = \{v_1, \dots, v_m\}$ ONB za V . Vzemimo linearno preslikavo $L : U \rightarrow V$. Izpeljimo zvezo med L in L^* glede na bazi \mathcal{B} in \mathcal{C} . Torej $[L]_{\mathcal{C} \leftarrow \mathcal{B}}$ za $L : U \rightarrow V$ in $[L^*]_{\mathcal{B} \leftarrow \mathcal{C}}$ za $L^* : V \rightarrow U$. Izračunajmo $[L]_{\mathcal{C} \leftarrow \mathcal{B}}$ tako, da uporabimo fourierov razvoj:

$$\begin{aligned} Lu_1 &= \langle Lu_1, v_1 \rangle v_1 + \dots + \langle Lu_1, v_m \rangle v_m \\ &\vdots \\ &\vdots \\ Lu_n &= \langle Lu_n, v_1 \rangle v_1 + \dots + \langle Lu_n, v_m \rangle v_m \end{aligned}$$

$$[L]_{\mathcal{C} \leftarrow \mathcal{B}} = \begin{bmatrix} \langle Lu_1, v_1 \rangle & \dots & \langle Lu_n, v_1 \rangle \\ \vdots & & \vdots \\ \langle Lu_1, v_m \rangle & \dots & \langle Lu_n, v_m \rangle \end{bmatrix} = \begin{bmatrix} \langle u_1, L^*v_1 \rangle & \dots & \langle u_n, L^*v_1 \rangle \\ \vdots & & \vdots \\ \langle u_1, L^*v_m \rangle & \dots & \langle u_n, L^*v_m \rangle \end{bmatrix}$$

Sedaj izračunajmo še $[L^*]_{\mathcal{B} \leftarrow \mathcal{C}}$ spet s fourierovim razvojem in primerjajmo istoležne koeficiente:

$$\begin{aligned} L^*v_1 &= \langle L^*v_1, u_1 \rangle u_1 + \dots + \langle L^*v_1, u_n \rangle u_n \\ &\vdots \\ &\vdots \\ L^*v_m &= \langle L^*v_m, u_1 \rangle u_1 + \dots + \langle L^*v_m, u_n \rangle u_n \end{aligned}$$

$$\begin{aligned} [L^*]_{\mathcal{B} \leftarrow \mathcal{C}} &= \begin{bmatrix} \langle L^*v_1, u_1 \rangle & \dots & \langle L^*v_m, u_1 \rangle \\ \vdots & & \vdots \\ \langle L^*v_1, u_n \rangle & \dots & \langle L^*v_m, u_n \rangle \end{bmatrix} = \begin{bmatrix} \overline{\langle u_1, L^*v_1 \rangle} & \dots & \overline{\langle u_1, L^*v_m \rangle} \\ \vdots & & \vdots \\ \overline{\langle u_n, L^*v_1 \rangle} & \dots & \overline{\langle u_n, L^*v_m \rangle} \end{bmatrix} = \begin{bmatrix} \overline{\langle u_1, L^*v_1 \rangle} & \dots & \overline{\langle u_n, L^*v_1 \rangle} \\ \vdots & & \vdots \\ \overline{\langle u_1, L^*v_m \rangle} & \dots & \overline{\langle u_n, L^*v_m \rangle} \end{bmatrix}^T \\ &= \overline{[L]_{\mathcal{C} \leftarrow \mathcal{B}}}^T \end{aligned}$$

Pripomba. Kako izgleda lastnost $\langle Lu, v \rangle = \langle u, L^*v \rangle$? Naj bo $u \in F^n$ in $v \in F^m$ in $A = m \times n$ matrika. Ali za standardna skalarna produkta v F^n in F^m $\langle Au, v \rangle = \langle u, A^*v \rangle$ velja tudi za matrike, če vzamemo $A^* = \overline{A^T} = \overline{A^T}$? Pa preverimo (ja, velja):

$$\langle u, v \rangle = u_1 \overline{v_1} + \dots + u_n \overline{v_n} = \begin{bmatrix} \overline{v_1} & \dots & \overline{v_n} \end{bmatrix} \begin{bmatrix} u_1 \\ \vdots \\ u_n \end{bmatrix} = v^* u$$

$$\langle Au, v \rangle = v^* Au$$

$$\langle u, A^*v \rangle = (A^*v)^* u = v^* (A^*)^* u = v^* Au$$

Dejstvo. Lastnosti adjungiranja: $(\alpha A + \beta B)^* = \overline{\alpha} A^* + \overline{\beta} B^*$, $(AB)^* = B^* A^*$, $(A^*)^* = A$

2.3.2 Jedro in slika adjungirane linearne preslikave

Trditev. Naj bo $L : U \rightarrow V$ linearna. Velja $\text{Ker}(L^*) = (\text{Ker } L)^\perp$ in $\text{Ker}(L) = (\text{Ker } L^*)^\perp$.

Dokaz. Naj bo $v \in \text{Ker } L^*$ za $L^* : V \rightarrow U$. Velja

$$v \in \text{Ker}(L^*) \Leftrightarrow L^*v = 0 \Leftrightarrow \forall u \in U : \langle u, L^*v \rangle = 0 \Leftrightarrow \forall u \in U : \langle Lu, v \rangle = 0 \Leftrightarrow \forall w \in \text{Ker } L : \langle w, v \rangle = 0 \Leftrightarrow v \in (\text{Ker } L)^\perp$$

$$\text{Velja torej } \text{Ker } L^* = (\text{Ker } L)^\perp \Rightarrow \text{Ker } L = (\text{Ker } L^*)^\perp \Rightarrow (\text{Ker } L)^\perp = \text{Ker } L^* \Rightarrow (\text{Ker } L^*)^\perp = \text{Ker } L \quad \square$$

Trditev. Za $L : U \rightarrow V$ velja $\text{Ker}(L^*L) = \text{Ker} L$

Dokaz. Vzemimo poljuben $u \in U$ in dokazujemo enakost množic (obe vsebovanosti):

- (\supseteq) Če $u \in \text{Ker} L \Rightarrow Lu = 0 \xrightarrow{\text{množimo z } L^*} L^*Lu = L^*u = 0 \Rightarrow u \in \text{Ker} L^*L \Rightarrow \text{Ker} L \subseteq \text{Ker} L^*L$
- (\subseteq) Če $u \in \text{Ker} L^*L \Rightarrow L^*Lu = 0 \Rightarrow \langle u, L^*Lu \rangle = 0 \Rightarrow \langle Lu, Lu \rangle = 0 \Rightarrow Lu = 0 \Rightarrow u \in \text{Ker} L \Rightarrow \text{Ker} L^*L \subseteq \text{Ker} L$

□

Posledica. $\text{Ker}(L^*L) = \text{Ker}(L)$.

Dokaz. $\text{Ker}(L^*L) = \text{Ker}(L^*(L^*)^*) = \text{Ker}((L^*L)^*) = (\text{Ker} L^*L)^\perp = (\text{Ker} L)^\perp = \text{Ker} L^*$

□

2.3.3 Lastne vrednosti adjungirane linearne preslikave.

Trditev. Če je λ lastna vrednost A , je $\bar{\lambda}$ lastna vrednost za A^* . ZDB $\det(A - \lambda I) = 0 \Rightarrow \det(A - \lambda) = 0$.

Dokaz. Naj bo $B = A - \lambda I$. Teda $B^* = A^* - \bar{\lambda}I = A^* - \bar{\lambda}I$. Radi bi dokazali $\det B = 0 \Rightarrow \det B^* = 0$. Ker je $B^* = \overline{B^T} \Rightarrow \det B^* = \det \overline{B^T} = \overline{\det B} = \overline{\det B} \Rightarrow \det B = 0 \Rightarrow \det B^* = 0$.

□

Posledica. Iz te formule izvemo tudi karakteristični polinom A^* . $p_{A^*}(x) = \det(A^* - xI) \Rightarrow p_A(\bar{x}) = \det(A - \bar{x}I) = \det(A^* - xI)^* = \overline{\det(A^* - xI)} = \overline{p_{A^*}(x)}$, torej $p_{A^*}(x) = \overline{p_A(\bar{x})}$. Torej, če je $p_A(x) = c_0x^0 + \dots + x_nx^n$, je $p_{A^*}(x) = \overline{c_0x^0 + \dots + x_nx^n} = \overline{c_0}x^0 + \dots + \overline{c_n}x^n$.

Dokaz. Alternativen dokaz: Najprej dokažimo $\dim \text{Ker} B^* = \dim \text{Ker} B$. Velja $\dim \text{Ker} B^* = \dim(\text{Ker} B)^\perp = n - \dim \text{Ker} B = \dim \text{Ker} B$. Torej $\text{Ker}(B) \neq 0 \Leftrightarrow \text{Ker}(B^*) \neq 0$, torej so lastne vrednosti A^* konjugirane lastne vrednosti A .

□

Pripomba. Med lastnimi vektorji A in lastnimi vektorji A^* (žal) ni posebne zveze. Primer: $A = \begin{bmatrix} 1 & 2 \\ i & 1 \end{bmatrix}$ ima lastne vektorje $\vec{v}_1 = \begin{bmatrix} 1-i \\ -1 \end{bmatrix}$ in $\vec{v}_2 = \begin{bmatrix} 1-i \\ 1 \end{bmatrix}$, $A^* = \begin{bmatrix} 1 & 1 \\ 2 & -i \end{bmatrix}$ pa lastne vektorje $\vec{v}'_1 = \begin{bmatrix} 1-i \\ -2 \end{bmatrix}$ in $\vec{v}'_2 = \begin{bmatrix} 1-i \\ 2 \end{bmatrix}$. Med temi vektorji ni nobenih kolinearnosti. Obstajajo pa zveze v nekaterih zanimivih primerih:

Trditev. Če matrika A zadošča $A^*A = AA^*$ (pravimo A je normalna), iz $Av = \lambda v$ sledi $A^*v = \bar{\lambda}v$, torej imata A in A^* iste lastne vrednosti.

Dokaz. Če velja $Av = \lambda v$, velja $Av - \lambda v = (A - \lambda I)v = Bv = 0 \Rightarrow v \in \text{Ker} B$. Če velja $A^*v = \bar{\lambda}v$, velja $A^*v - \bar{\lambda}v = (A^* - \bar{\lambda}I)v = B^*v = 0 \Rightarrow v \in \text{Ker} B^*$. Dokazati je treba še $\text{Ker} B = \text{Ker} B^*$:

1. Ali velja $A^*A = AA^* \Rightarrow B^*B = BB^*$? Ja.

$$(a) B^*B = (A^* - \bar{\lambda}I)(A - \lambda I) = A^*A - \bar{\lambda}A - \lambda A^* + \bar{\lambda}\lambda I$$

$$(b) BB^* = (A - \lambda I)(A^* - \bar{\lambda}I) = AA^* - \bar{\lambda}A - \lambda A^* + \lambda\bar{\lambda}I$$

2. Ali velja $B^*B = BB^* \Rightarrow \text{Ker} B = \text{Ker} B^*$? Iz $B^*B = BB^*$ sledi $\text{Ker}(B^*B) = \text{Ker}(BB^*) \Rightarrow \text{Ker}(B) = \text{Ker}(B^*)$.

3. $\text{Ker} B = \text{Ker} B^* \Rightarrow \forall v \in V : Av = \lambda v \Leftrightarrow A^*v = \bar{\lambda}v$.

□

2.3.4 Normalne matrike

Definicija. A je normalna $\Leftrightarrow A^*A = AA^*$.

Pripomba. Dokazali smo že, da za normalne matrike velja, da imata A in A^* iste lastne vektorje, kar v splošnem ne velja.

Trditev. Lastni vektorji, ki pripadajo različnim lastnim vrednostim normalne matrike, so paroma ortogonalni.

Dokaz. Naj bo $A^*A = AA^*$ za neko A in naj bo $Au = \lambda u$ in $Av = \mu v$ in $\mu \neq \lambda$. $u \perp v \Leftrightarrow \langle u, v \rangle = 0$. Računajmo:

$$\begin{aligned}\mu \langle u, v \rangle &= \langle u, \bar{\mu}v \rangle = \langle u, A^*v \rangle = \langle Au, v \rangle = \langle \lambda u, v \rangle = \lambda \langle u, v \rangle \\ (\mu - \lambda) \langle u, v \rangle &= 0 \wedge u \neq \lambda \Rightarrow \langle u, v \rangle = 0 \Leftrightarrow u \perp v\end{aligned}$$

□

Trditev. Vsako normalno matriko se da diagonalizirati.

Dokaz. Dokažimo, da je jordanska forma normalne matrike diagonalna \Leftrightarrow vsi korenski podprostorji so lastni. $\forall m, \lambda : \text{Ker}(A - I\lambda)^m = \text{Ker}(A - I\lambda)$. Zadošča dokazati za $m = 2$. Naj bo $m = 2$ in $B = A - I\lambda$. Dokažimo $\text{Ker } B^2 = \text{Ker } B$.

1. Če v $\text{Ker}(A) = \text{Ker}(A^*A)$ vstavimo $A = B^2$, dobimo $\text{Ker } B^2 = \text{Ker}((B^2)^* B^2)$.
2. Ker je A normalna, je B normalna, torej $(B^2)^* B^2 = B^* B^* B B = B^* B B^* B = (B^* B)^2$. Torej $\text{Ker}((B^2)^* B^2) = \text{Ker}(B^* B)^2$.
3. Če v $\text{Ker } A^*A = \text{Ker } A$ vstavimo $A = B^* B$, dobimo $\text{Ker } B^* B B^* B = \text{Ker}(B^* B)^2 = \text{Ker } B^* B$.
4. Zopet upoštevamo $\text{Ker } A^*A = \text{Ker } A$, torej $\text{Ker}(B^* B) = \text{Ker } B$.

Ko dokažemo B normalna $\Rightarrow B^*$ normalna, bo iz $\text{Ker } B^2 = \text{Ker } B$ sledilo $\text{Ker } B^4 = \text{Ker } B$. Preverimo, a je B^2 normalna, če je B normalna: $(B^2)^* B^2 = B^* B^* B B = B^* B B^* B = B B^* B B^* = B B B^* B^* = B^2 (B^2)^*$. Sedaj vemo $\text{Ker } B = \text{Ker } B^2 = \text{Ker } B^4 = \text{Ker } B^8 = \dots$. Vemo pa tudi, da

$$\begin{aligned}\text{Ker } B &\subseteq \text{Ker } B^2 \subseteq \text{Ker } B^3 \subseteq \text{Ker } B^4 \subseteq \text{Ker } B^5 \subseteq \text{Ker } B^6 \subseteq \dots \\ \text{Ker } B &\subseteq \text{Ker } B \subseteq \text{Ker } B^3 \subseteq \text{Ker } B \subseteq \text{Ker } B^5 \subseteq \text{Ker } B \subseteq \dots \\ \text{Ker } B &= \text{Ker } B^2 = \text{Ker } B^3 = \text{Ker } B^4 = \text{Ker } B^5 = \dots \\ &\forall v : \text{Ker } B^m = \text{Ker } B\end{aligned}$$

□

Pripomba. Torej za vsako normalno matriko $A \exists$ diagonalna D in obrnljiva P z ortonormiranimi stolpci, da velja $AP = PD$, $A = PDP^{-1}$. Diagonala D so lastne vrednosti A , stolpci P pa so njeni lastni vektorji. Lastni podprostorji $(A - \lambda_1 I), \dots, (A - \lambda_n I)$ so medsebojno pravokotni. Izberimo ONB za vsak lasten podprostor. Unija teh ONB je ONB za F^n . $F^n = \text{Ker}(A - \lambda_1 I) \oplus \dots \oplus \text{Ker}(A - \lambda_n I)$. Ta ONB so stolpci matrike P .

2.3.5 Ortogonalne/unitarne matrike

Definicija. Naj bo A kvadratna z ON stolpci glede na standardni skalarni produkt. Pravimo, da je A unitarna (v kompleksnem primer) oziroma ortogonalna (v realnem primeru).

Trditev. Za unitarno A velja $A^*A = AA^* = I$.

Dokaz. Dokazujemo za unitarno. Za ortogonalno je dokaz podoben. Naj bo $A = \begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \cdots & a_{nn} \end{bmatrix}$ unitarna.

To pomeni, da za vsaka stolpca $a_i = (a_{1i}, \dots, a_{ni})$ in $a_j = (a_{1j}, \dots, a_{nj})$ velja za vsak $i, j \in \{1..n\}$ velja

$$\left\langle \begin{bmatrix} a_{1i} \\ \vdots \\ a_{ni} \end{bmatrix}, \begin{bmatrix} a_{1j} \\ \vdots \\ a_{nj} \end{bmatrix} \right\rangle = a_{1i}\overline{a_{1j}} + \cdots + a_{ni}\overline{a_{nj}} = \begin{cases} 0 & ; i \neq j \\ 1 & ; i = j \end{cases}. \text{ Oglejmo si}$$

$$A^*A = \begin{bmatrix} \overline{a_{11}} & \cdots & \overline{a_{n1}} \\ \vdots & & \vdots \\ \overline{a_{1n}} & \cdots & \overline{a_{nn}} \end{bmatrix} \begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \cdots & a_{nn} \end{bmatrix} = \begin{bmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{bmatrix}$$

Očitno je res, ker je vsak element A^*A konstruiran s skalarnim množenjem vrstice leve matrike (konjugirani stolpci A , ker smo poprej matriko transponiralo) in stolpca desne, za kar predpis smo poprej že razbrali. \square

Pripomba. Za nekvadratne unitarne velja le $A^*A = I$, $AA^* = I$ pa zaradi nezmožnosti množenja zaradi nepravilnih dimenzij seveda ne velja.

Trditve. Naslednje trditve so za P z ortonormiranimi stolpci ekvivalentne:

1. $P^*P = I$
2. $\forall u, v : \langle Pu, Pv \rangle = \langle u, v \rangle$
3. $\forall u : \|Pu\| = \|u\|$
4. \forall ONB $\{u_1, \dots, u_n\} : \{Pu_1, \dots, Pu_n\}$ je ON množica
5. \exists ONB $\{u_1, \dots, u_n\} : \{Pu_1, \dots, Pu_n\}$ je ON množica

Dokaz. Dokazujemo ekvivalenco:

$$(1 \Rightarrow 2) \quad \langle Pu, Pv \rangle = \langle u, P^*Pv \rangle = \langle u, v \rangle$$

$$(2 \Rightarrow 3) \quad \|Pu\|^2 = \langle Pu, Pu \rangle = \langle u, u \rangle = \|u\|^2$$

$$(2 \Rightarrow 1)$$

$$\forall u, v : \langle Pu, Pv \rangle = \langle u, v \rangle \Rightarrow \langle u, P^*Pv \rangle - \langle u, v \rangle = 0 \Rightarrow \langle u, (P^*P - I)v \rangle = 0$$

$$\text{Sedaj izberimo } u = (P^*P - I)v : \langle (P^*P - I)v, (P^*P - I)v \rangle = 0 \Rightarrow P^*P - I = 0 \Rightarrow P^*P = 0$$

(3 \Rightarrow 2) Po predpostavki $\forall u : \|Pu\| = \|u\|$ Izrazimo skalarni produkt z normo: $\langle u, v \rangle = \frac{1}{4} \sum_{k=0}^3 i^k \|u + i^k v\|^2$, torej

$$\langle Pu, Pv \rangle = \frac{1}{4} \sum_{k=0}^3 i^k \|Pu + i^k Pv\|^2 = \frac{1}{4} \sum_{k=0}^3 i^k \|P(u + i^k v)\|^2 \stackrel{\text{predpostavka}}{=} \frac{1}{4} \sum_{k=0}^3 i^k \|u + i^k v\|^2 = \langle u, v \rangle$$

(5 \Rightarrow 4) Vzemimo poljuben u in ga razvijmo po ONB u_1, \dots, u_n . Tedaj $u = \alpha_1 u_1 + \cdots + \alpha_n u_n$. Ker so u_i ONB, velja $\|u\|^2 = |\alpha_1|^2 + \cdots + |\alpha_n|^2$. Ker so Pu_1 ONB po predpostavki, $\|Pu\|^2 = |\alpha_1|^2 + \cdots + |\alpha_n|^2$, torej velja $\|Pu\|^2 = \|u\|^2$.

(2 \Rightarrow 4) Ker so u_1, \dots, u_n ONM, velja $\langle u_i, u_j \rangle = \begin{cases} 1 & ; i = j \\ 0 & ; i \neq j \end{cases}$. Tudi Pu_1, \dots, Pu_n ortonormirana, kajti po predpostavki 2 velja $\langle Pu_i, Pu_j \rangle = \begin{cases} 1 & ; i = j \\ 0 & ; i \neq j \end{cases}$.

(4 \Rightarrow 5) Očitno.

\square

Trditev. Lastne vrednosti unitarne matrike A se nahajajo na enotski krožnici v \mathfrak{S} .

Dokaz. Naj bo A unitarna in naj bo v tak, da $Av = \lambda v$. Tedaj $\langle v, v \rangle = \langle Av, Av \rangle = \langle \lambda v, \lambda v \rangle = \lambda \bar{\lambda} \langle v, v \rangle \Rightarrow \lambda \bar{\lambda} = 1 \Rightarrow |\lambda| = 1 \Rightarrow \lambda = e^{i\varphi}$ za nek φ . \square

Pripomba. Iz unitarnosti sledi normalnost, zato so lastni vektorji unitarne matrike, ki pripadajo paroma različnim lastnim vrednostim, pravokotni (isto, kot pri normalnih matrikah).

Pripomba. Prav tako kot pri normalnih matrikah lahko unitarne diagonaliziramo v tokrat ortogonalni bazi. Pri unitarnih so stolpci P še celo normirani. $A = PDP^{-1}$, kjer je P unitarna, torej $P^* = P^{-1}$.

Pripomba. Očitno je, da če je A unitarna, velja $A^* = A^{-1}$.

2.3.6 Simetrične/hermitske matrike

Definicija. Matrika nad \mathbb{R} je simetrična, če zanjo velja $A^* = A$. Matrika nad \mathbb{C} je hermitska, če zanjo velja $A^* = A$. Linearni preslikavi, pripadajoči hermitski/simetrični matriki, pravimo sebiadjungirana.

Dejstvo. Vsaka hermitska/simetrična matrika je normalna, kajti $A^*A = AA = AA^*$.

Trditev. Lastne vrednosti hermitskih/simetričnih matrik so realne.

Dokaz. Naj bo $A = A^*$ in naj bo $Av = \lambda v$ za nek neničeln v . Tedaj $\lambda \langle v, v \rangle = \langle \lambda v, v \rangle = \langle Av, v \rangle = \langle v, A^*v \rangle = \langle v, Av \rangle = \langle v, \lambda v \rangle = \bar{\lambda} \langle v, v \rangle$. Potemtakem $\lambda = \bar{\lambda} \Rightarrow \lambda \in \mathbb{R}$. \square

Pripomba. Diagonalizacija je zopet enaka kot pri normalnih matrikah z dodatkom — vsaka hermitska matrika je podobna realni diagonalni, kar za normalne ni res — normalne so lahko podobne kompleksnim diagonalnim matrikam.

2.3.7 Pozitivno (semi)definitne matrike

Definicija. A je pozitivno semidefinitna $\sim A \geq 0 \Leftrightarrow A = A^* \wedge \forall v : \langle Av, v \rangle \geq 0$. A je pozitivno definitna $\sim A > 0 \Leftrightarrow A = A^* \wedge \forall v \neq 0 : \langle Av, v \rangle > 0$. S tem ko skalarni produkt primerjamo ($>$, \geq), implicitno zahtevamo njegovo realnost. Primerjalni operatorji namreč na kompleksnih številih niso definirani.

Zgled. Vzemimo poljubno nenujno kvadratno B in definirajmo $A = B^*B$. Potem je A pozitivno semidefinitna, kajti $A^* = (B^*B)^* = B^*B = A$ in $\langle Av, v \rangle = \langle B^*Bv, v \rangle = \langle Bv, Bv \rangle \geq 0$. Če pa bi bili stolpci B linearno neodvisni, pa bi veljalo $\forall v : v \neq 0 \Rightarrow \langle Av, v \rangle = \langle B^*Bv, v \rangle = \langle Bv, Bv \rangle > 0$.

Trditev. $A \geq 0 \Rightarrow$ lastne vrednosti A so ≥ 0 . $A > 0 \Rightarrow$ lastne vrednosti A so > 0 .

Dokaz. Naj bo λ lastna vrednost A in $A \geq 0$. Tedaj $Av = \lambda v$ za nek $v \neq 0$. Torej $\langle Av, v \rangle = \langle \lambda v, v \rangle = \lambda \langle v, v \rangle$. Toda ker $\langle Av, v \rangle \geq 0$, sledi $\lambda \langle v, v \rangle \geq 0$. Ker je $\langle v, v \rangle > 0$, sledi $\lambda \geq 0$. Analogno za $A > 0$. \square

Pripomba. Diagonalizacija je ista kot za normalna, s tem da za diagonalno D velja še, da je pozitivno (semi)definitna, ko je A pozitivno semidefinitna.

Trditev. $\forall A \geq 0 \exists B = B^*, B \geq 0 \ni B^2 = A$. ZDB Za vsako pozitivno semidefinitno matriko A obstajajo taka unitarna pozitivno semidefinitna B , da velja $B^2 = A$.

Dokaz. Naj bo $A = PDP^{-1}$ in $P^* = P^{-1}$ in $D = \begin{bmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{bmatrix}$. Definirajmo $E = \begin{bmatrix} \sqrt{\lambda_1} & & 0 \\ & \ddots & \\ 0 & & \sqrt{\lambda_n} \end{bmatrix} \geq 0$.

Naj bo $B = PEP^{-1} = PEP^*$. Opazimo $B^* = B$, kajti $(PEP^{-1})^* = (PEP^*)^* = PE^*P^* = PEP^{-1} = PEP^*$, ker je $E^* = E$, ker je $\forall a \in \mathbb{R} : \sqrt{a} \in \mathbb{R}$. Oglejmo si $B^2 = PEP^{-1}PEP^{-1} = PE^2P^{-1} = PDP^{-1}$. Tako definiramo $\sqrt{A} = B$ (tu $\sqrt{\cdot}$ ni funkcija, kot pri JKF, temveč nov operator). \square

Trditev. Naslednje trditve so ekvivalentne (zamenjamo lahko \geq in $>$):

1. $A \geq 0$.
2. $A = A^*$ in vse lastne vrednosti so ≥ 0 .
3. $A = PDP^{-1}$ za nek unitaren P in diagonalen $D \geq 0$.

4. $A = A^*$ in obstaja \sqrt{A} .

5. $A = B^*B$ za neko nenujno kvadratno matriko B (za pozitivno definitno zahtevamo, da ima B LN stolpce).

Trditve. klasifikacija skalarnih produktov na \mathbb{R}^n in \mathbb{C}^n . Naj bo $\langle u, v \rangle$ standardni skalarni produkt na \mathbb{C}^n . $u =$

$$(\alpha_1, \dots, \alpha_n) \text{ in } v = (\beta_1, \dots, \beta_n) \text{ in velja } \langle u, v \rangle = \alpha_1 \overline{\beta_1} + \dots + \alpha_n \overline{\beta_n} = \begin{bmatrix} \overline{\beta_1} & \dots & \overline{\beta_n} \end{bmatrix} \begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{bmatrix} = v^* \cdot u. \text{ Za } A > 0$$

definirajmo $[u, v] = \langle Au, v \rangle = v^* Au$. Trdimo, da je $[\cdot, \cdot]$ spet skalarni produkt na $\mathbb{R}^n/\mathbb{C}^n$ in da je vsak skalarni produkt v $\mathbb{R}^n/\mathbb{C}^n$ take oblike.

Dokaz. Dokazujemo oba dela trditve:

1. $[\cdot, \cdot]$ je skalarni produkt

(a) pozitivna semidefinitnost: $\forall u \neq 0 : [u, u] = \langle Au, u \rangle \geq 0$.

(b) konjugirana simetričnost: $\forall u, v : [u, v] = \langle Au, v \rangle = \langle u, A^*v \rangle = \langle u, Av \rangle = \overline{\langle Av, u \rangle} = \overline{[v, u]}$.

(c) Linearnost in homogenost: $\forall \alpha_1, \alpha_2, u_1, u_2, v : [\alpha_1 u_1 + \alpha_2 u_2, v] = \langle A(\alpha_1 u_1 + \alpha_2 u_2), v \rangle = \langle \alpha_1 Au_1 + \alpha_2 Au_2, v \rangle = \alpha_1 \langle Au_1, v \rangle + \alpha_2 \langle Au_2, v \rangle = \alpha_1 [u_1, v] + \alpha_2 [u_2, v]$.

2. Za vsak skalarni produkt $[\cdot, \cdot]$ na \mathbb{C}^n obstaja taka pozitivno definitna matrika A , da velja $\forall u, v \in \mathbb{C}^n : [u, v] = \langle Au, v \rangle = v^* Au$.

Naj bo e_1, \dots, e_n standardna baza za \mathbb{C}^n . Definirajmo $A = \begin{bmatrix} [e_1, e_1] & \dots & [e_n, e_1] \\ \vdots & & \vdots \\ [e_1, e_n] & \dots & [e_n, e_n] \end{bmatrix}$. Velja $A = A^*$:

$$A^* = \begin{bmatrix} \overline{[e_1, e_1]} & \dots & \overline{[e_1, e_n]} \\ \vdots & & \vdots \\ \overline{[e_n, e_1]} & \dots & \overline{[e_n, e_n]} \end{bmatrix} = \begin{bmatrix} [e_1, e_1] & \dots & [e_n, e_1] \\ \vdots & & \vdots \\ [e_1, e_n] & \dots & [e_n, e_n] \end{bmatrix} = A$$

Preveriti je treba še $\forall u, v \in \mathbb{C}^n : [u, v] = v^* Au$. $u = \alpha_1 e_1 + \dots + \alpha_n e_n$ in $v = \beta_1 e_1 + \dots + \beta_n e_n$. Tedaj je

$$\begin{aligned} [u, v] &= [\alpha_1 e_1 + \dots + \alpha_n e_n, \beta_1 e_1 + \dots + \beta_n e_n] = \\ &= (\alpha_1 \overline{\beta_1} [e_1, e_1] + \dots + \alpha_1 \overline{\beta_n} [e_1, e_n]) + \dots + (\alpha_n \overline{\beta_1} [e_n, e_1] + \dots + \alpha_n \overline{\beta_n} [e_n, e_n]) = \\ &= \begin{bmatrix} \overline{\beta_1} & \dots & \overline{\beta_n} \end{bmatrix} \begin{bmatrix} [e_1, e_1] & \dots & [e_n, e_1] \\ \vdots & & \vdots \\ [e_1, e_n] & \dots & [e_n, e_n] \end{bmatrix} \begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{bmatrix} = v^* Au = \langle Au, v \rangle \end{aligned}$$

Da je A pozitivno definitna sledi, saj mora za vsak neničeln u po aksiomu za pozitivno definitnost skalarnega produkta veljati $\langle Au, u \rangle > 0$.

□

2.3.8 Singularni razcep (angl. singular value decomposition — SVD)

Naj bo $A_{n \times n}$ neka kompleksna ali realna matrika. Tedaj je A^*A hermitska (2.3.6) matrika dimenzij $n \times n$. Ker je $\forall u : \langle A^*Au, u \rangle = \langle Au, Au \rangle \geq 0$, je A^*A pozitivno semidefinitna, torej so vse njene lastne vrednosti ≥ 0 .

Definicija. Singularne vrednosti A so kvadratni koreni lastnih vrednosti A^*A .

Zgled. Če je A normalna in λ lastna vrednost A , obstaja tak $v \neq 0 \ni Av = \lambda v \Rightarrow A^*v = \overline{\lambda}v$. Odtod sledi, da je $A^*Av = A^*\lambda v = \lambda A^*v = \lambda \overline{\lambda}v$, torej je λ lastna vrednost matrike A^*A . Po definiciji singularne vrednosti je $\sqrt{\lambda \overline{\lambda}} = \sqrt{|\lambda|^2} = |\lambda|$ singularna vrednost matrike A . Potemtakem so singularne vrednostni normalnih matrik enake absolutnim vrednosti lastnih vrednosti.

Nekatere lastne vrednosti so ničelne, nekatere pa od nič strogo večje. Koliko je katerih? Število ničelnih singularnih vrednosti matrice A je število ničelnih lastnih vrednosti matrice A^*A . Ker je A^*A hermitska, je diagonalizabilna, zato je algebraična večkratnost lastne vrednosti 0 enaka geometrijski večkratnosti lastne vrednosti 0 , slednja pa je definirana kot $\dim \text{Ker } A^*A$. Ko upoštevamo $\dim \text{Ker } A^*A = \dim \text{Ker } A$, izvemo, da je število ničelnih singularnih vrednosti matrice A njena ničnost (nA). Ker je A^*A velikosti $n \times n$, ima A n singularnih vrednosti, torej je število neničelnih singularnih vrednosti A enako $n - \text{Ker } A$. Upoštevajoč osnovni dimenzijski izrek jedra in slike, velja $nA + \text{rang } A = n$, torej je neničelnih singularnih vrednosti = rang $A = \dim \text{Ker } A$.

Pripomba. Za $m \times n$ matrico velja $\text{rang } A \leq \min \{m, n\}$.

Definicija. posplošitev pojma diagonalne matrice na nekvadratne matrice. Matrica $D_{m \times n}$ je diagonalna, če velja $\forall i \in \{1..m\}, j \in \{1..n\} : i \neq j \Rightarrow D_{i,j} = 0$.

Zgled. Primeri pravokotnih diagonalnih matric:

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 3 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 3 \\ 0 & 0 & 0 \end{bmatrix}$$

Izrek. singularni razcep. Naj bo A kompleksna $m \times n$ matrica. Potem obstajata taki unitarni Q_1, Q_2 in taka diagonalna D z diagonalci $\geq 0 \ni A = Q_1 D Q_2^{-1}$.

Pripomba. Diagonalci D so ravno singularne vrednosti matrice A . Ker je Q_2 unitarna, je $Q_2^* = Q_2^{-1} \Rightarrow A = Q_1 D Q_2^*$. Če $A = Q_1 D Q_2^*$, je $A^* = Q_2^* D^* Q_1^* = Q_2 D^* Q_1^*$ in $A^*A = Q_2 D^* Q_1^* Q_1 D Q_2^* = Q_2 D^* D Q_2^*$, torej je A^*A podobna D^*D , diagonalci D^*D so lastne vrednosti A^*A in stolpci Q_2 so lastni vektorji A^*A . Diagonalci D so bodisi 0 bodisi kvadratni koreni od diagonalcev D^*D , torej kvadratni koreni lastnih vrednosti A^*A , torej singularne vrednosti od A .

Dokaz. obstoj singularnega razcepa. Konstruirajmo Q_1, D, Q_2 in dokažimo veljavnost.

- Konstrukcija Q_2 : A je $m \times n$ kompleksna. Tvorimo $n \times n$ matrico A^*A . Izračunajmo lastne vrednosti A^*A in jih uredimo padajoče — $\lambda_1 \geq \dots \geq \lambda_n$. Naj bodo v_1, \dots, v_n pripadajoči lastni vektorji — $A^*A v_i = \lambda_i v_i$. Te v_i izberimo tako, da so ortonormirani. Lastni podprostori A^*A so namreč paroma pravokotni, saj je A^*A normalna, saj je hermitska. V vsakem podprostoru vzamemo ONB in v_1, \dots, v_n je unija teh ON baz. Definiramo $Q_2 = [v_1 \ \dots \ v_n]$. Ker so v_1, \dots, v_n ON, je Q_2 unitarna.
- Konstrukcija D : Naj bo $r := \text{rang } A$ (število ničelnih singularnih vrednosti A). Oglejmo si zaporedje lastnih vrednosti A^*A $\lambda_1 \geq \dots > \lambda_{r+1} = \dots = \lambda_n$. Lastne vrednosti po r so ničelne, ostale pa večje od 0 . Lastne vrednosti A^*A v tem vrstnem redu so singularne vrednosti matrice A : $\sigma_1^2 = \lambda_1 \geq \dots \geq \sigma_r^2 = \lambda_r > \sigma_{r+1}^2 = \dots = \sigma_n^2 = 0$. Definiramo D kot $m \times n$ diagonalno matrico takole:

$$D = \begin{bmatrix} \sigma_1 & & & & & & & & & 0 \\ & \ddots & & & & & & & & \\ & & \sigma_r & & & & & & & \\ & & & \sigma_{r+1} = 0 & & & & & & \\ & & & & & \ddots & & & & \\ 0 & & & & & & & & & \sigma_n = 0 \end{bmatrix}$$

- Konstrukcija Q_1 : $\forall i \in \{1..r\} : u_i := \frac{1}{\sigma_i} A v_i$ za v_i lastne vektorje A^*A , torej $A^*A v_i = \lambda_i v_i = \sigma_i^2 v_i$. Pokažimo, da je u_1, \dots, u_r ON množica. $\forall i, j \in \{1..r\}$:

$$\begin{aligned} \langle u_i, u_j \rangle &= \left\langle \frac{1}{\sigma_j} A v_i, \frac{1}{\sigma_j} A v_j \right\rangle = \frac{1}{\sigma_i \sigma_j} \langle A v_i, A v_j \rangle = \frac{1}{\sigma_i \sigma_j} \langle A^* A v_i, v_j \rangle = \frac{1}{\sigma_i \sigma_j} \langle \lambda_i v_i, v_j \rangle = \frac{\lambda_i = \sigma_i^2}{\sigma_i \sigma_j} \langle v_i, v_j \rangle = \\ &= \frac{\sigma_i}{\sigma_j} \langle v_i, v_j \rangle = \begin{cases} 0 & ; i \neq j \\ 1 & ; i = j \end{cases} \end{aligned}$$

Sedaj ONM u_1, \dots, u_r z u_{r+1}, \dots, u_n dopolnimo do ONB za \mathbb{C}^n (GS). Definiramo $Q_1 = [u_1 \ \dots \ u_n]$. Ker so stolpci ONB, je matrica unitarna.

- Sedaj preverimo, da velja $A = Q_1 D Q_2^* = Q_1 D Q_2^{-1} \Leftrightarrow A Q_2 = Q_1 D$.

$$A Q_2 = A \begin{bmatrix} v_1 & \cdots & v_n \end{bmatrix} = \begin{bmatrix} A v_1 & \cdots & A v_n \end{bmatrix} = \cdots$$

Upoštevamo, da $i > r \Rightarrow \lambda_i = 0 \Rightarrow A^* A v_i = \lambda_i v_i = 0 \Rightarrow v_i \in \text{Ker } A^* A \Rightarrow v_i \in \text{Ker } A \Leftrightarrow A v_i = 0$:

$$\cdots = \begin{bmatrix} A v_1 & \cdots & A v_n \end{bmatrix} = \begin{bmatrix} A v_1 & \cdots & A v_r & 0 & \cdots & 0 \end{bmatrix}$$

Sedaj izračunajmo še

$$\begin{aligned} Q_1 D &= \begin{bmatrix} u_1 & \cdots & u_n \end{bmatrix} \begin{bmatrix} \sigma_1 & & & & & \\ & \ddots & & & & \\ & & \sigma_r & & & \\ & & & 0 & & \\ & & & & \ddots & \\ & & & & & 0 \end{bmatrix} = \begin{bmatrix} \sigma_1 u_1 & \cdots & \sigma_r u_r & 0 & \cdots & 0 \end{bmatrix} = \\ &= \begin{bmatrix} \cancel{\sigma_1} \cancel{\sigma_1} A v_i & \cdots & \cancel{\sigma_r} \cancel{\sigma_r} A v_r & 0 & \cdots & 0 \end{bmatrix} = \begin{bmatrix} A v_i & \cdots & A v_r & 0 & \cdots & 0 \end{bmatrix} = A Q_2 \end{aligned}$$

□

Zgled. Poišči singularni razcep $A = \begin{bmatrix} 1 & 1 & -1 & -1 \\ -1 & 0 & 1 & 0 \\ 0 & -1 & 0 & 1 \end{bmatrix}$. Izračunajmo

$$A^* A = \begin{bmatrix} 1 & 1 & -1 & -1 \\ -1 & 0 & 1 & 0 \\ 0 & -1 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & -1 & 0 \\ 1 & 0 & -1 \\ -1 & 1 & 0 \\ -1 & 0 & 1 \end{bmatrix} = \cdots = \begin{bmatrix} 2 & 1 & -2 & -1 \\ 1 & 2 & -1 & -2 \\ -2 & -1 & 2 & 1 \\ -1 & -2 & 1 & 2 \end{bmatrix}$$

Izračunajmo $p_{A^* A}(x) = \det(A^* A - xI) = \cdots = x^2(x-2)(x-6)$, torej $\lambda_1 = 6, \lambda_2 = 2, \lambda_3 = 0, \lambda_4 = 0$, torej $\sigma_1 = \sqrt{6}$ in $\sigma_2 = \sqrt{2}$ ter $\sigma_3 = \sigma_4 = 0$. (ujema se z dejstvom, da je rang $A = 2$). Izračunajmo lastne vektorje $A^* A$:

$$\lambda_1 = 6: \quad v'_1 = \begin{bmatrix} 1 \\ 1 \\ -1 \\ -1 \end{bmatrix}, \quad \|v'_1\| = 6$$

$$\lambda_2 = 2: \quad v'_2 = \begin{bmatrix} 1 \\ -1 \\ -1 \\ 1 \end{bmatrix}, \quad \|v'_2\| = 2$$

$$\lambda_3 = \lambda_4: \quad v'_3 = \begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \end{bmatrix}, v'_4 = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 2 \end{bmatrix}, \quad \|v'_3\| = \sqrt{2}, \|v'_4\| = \sqrt{2}$$

Z Gram-Schmidtom naredimo ortogonalno množico (v tem primeru so že ortogonalni) in jih normirajmo:

$$v_1 = \frac{1}{2} \begin{bmatrix} 1 \\ 1 \\ -1 \\ -1 \end{bmatrix}, \quad v_2 = \frac{1}{2} \begin{bmatrix} 1 \\ -1 \\ -1 \\ 1 \end{bmatrix}, \quad v_3 = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \end{bmatrix}, \quad v_4 = \frac{1}{\sqrt{2}} \begin{bmatrix} 0 \\ 1 \\ 0 \\ 1 \end{bmatrix}.$$

Sestavimo

$$Q_2 = \begin{bmatrix} \frac{1}{2} & \frac{1}{2} & \frac{1}{\sqrt{2}} & 0 \\ \frac{1}{2} & -\frac{1}{2} & 0 & \frac{1}{\sqrt{2}} \\ -\frac{1}{2} & -\frac{1}{2} & \frac{1}{\sqrt{2}} & 0 \\ -\frac{1}{2} & \frac{1}{2} & 0 & \frac{1}{\sqrt{2}} \end{bmatrix}, \quad D = \begin{bmatrix} \sqrt{6} & & & \\ & \sqrt{2} & & \\ & & 0 & \\ & & & 0 \end{bmatrix}$$

Izračunamo u_1, \dots, u_r za Q_1 :

$$u_1 = \frac{1}{\sigma_1} Av_1 = \frac{1}{\sqrt{6}} \begin{bmatrix} 2 \\ -1 \\ -1 \end{bmatrix}$$

$$u_2 = \frac{1}{\sigma_2} Av_2 = \frac{1}{\sqrt{2}} \begin{bmatrix} 0 \\ -1 \\ 1 \end{bmatrix}$$

Dopolnimo ju do ONB za \mathbb{R}^3 z Gram-Schmidtom (oz. uganemo $\begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}$). Dopolnitev normiramo: $u_3 = \frac{1}{\sqrt{3}} \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}$

in vektorje vstavimo v Q_1 :

$$Q_1 = \begin{bmatrix} \frac{2}{\sqrt{6}} & 0 & \frac{1}{\sqrt{3}} \\ -\frac{1}{\sqrt{6}} & -\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{3}} \\ -\frac{1}{\sqrt{6}} & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{3}} \end{bmatrix}$$

Iskani razcep je $A = Q_1 D Q_2^* = Q_1 D Q_2^{-1}$ (Izračunati je potrebno še en inverz — Q_2^{-1} namreč).

2.3.9 Pseudoinverz — Moore-Penroseov inverz

Pseudoinverz je posplošitev inverza na nenujno kvadratne nenujno obrnljive matrike. Najprej diagonalne matrike: Njihov navaden inverz je takšen:

$$\begin{bmatrix} d_{11} & & 0 \\ & \ddots & \\ 0 & & d_{nn} \end{bmatrix}^{-1} = \begin{bmatrix} d_{11}^{-1} & & 0 \\ & \ddots & \\ 0 & & d_{nn}^{-1} \end{bmatrix}$$

Kadar je diagonalca ničeln, kot element polja nima multiplikativnega inverza. Ideja za posplošeni inverz diagonalne matrike: take diagonalce pustimo na 0, torej na primer:

$$\begin{bmatrix} 1 & & 0 \\ & 2 & \\ 0 & & 0 \end{bmatrix}^+ = \begin{bmatrix} 1 & & 0 \\ & \frac{1}{2} & \\ 0 & & 0 \end{bmatrix}$$

Za nekvadratne diagonalne matrike pa takole:

$$\begin{bmatrix} 1 & & 0 \\ & 2 & \\ 0 & & 0 \end{bmatrix}^+ = \begin{bmatrix} 1 & & 0 \\ & \frac{1}{2} & \\ 0 & & 0 \end{bmatrix}$$

Definicija. posplošeni inverz diagonalne matrike. Naj bo D diagonalna $m \times n$ z neničelnimi diagonalci d_1, \dots, d_r , je D^+ diagonalna $n \times m$ z neničelnimi diagonalci $\frac{1}{d_1}, \dots, \frac{1}{d_r}$.

Pripomba. Za diagonalno D opazimo $D^{++} = D$ in za obrnljivo diagonalno D opazimo $D^+ = D^{-1}$.

Sedaj bi radi pojem posplošili na nediagonalne matrike — to storimo s pomočjo SVD. $A = Q_1 D Q_2^* \ni$: D diagonalna in Q_1, Q_2 unitarni. Tedaj velja A obrnljiva $\Leftrightarrow D$ obrnljiva, kajti $A^{-1} = Q_2 D^{-1} Q_1^{-1}$.

Definicija. Za splošen nenujno obrnljiv A definiramo $A^+ := Q_2 D^+ Q_1^{-1}$.

Dejstvo. Opazimo:

- $A^{++} = (Q_2 D Q_1^{-1})^+ = Q_1 D^{++} Q_2^{-1} = Q_1 D Q_2^{-1} = A$
- A obrnljiva: $A^+ = A^{-1}$

Trditev. osnovne lastnosti pseudoinverza.

1. $AA^+A = A$

2. $(A^+A)^* = A^+A$
3. $A^+AA^+ = A^+$
4. $(AA^+)^* = AA^+$

Dokaz. Dokažimo te 4 lastnosti najprej za D in nato za SVD. Pri D predpostavimo, da so ničle spodaj desno, sicer obstaja permutacijska matrika, ki je ortogonalna, s katero lahko množimo D , da jo pretvorimo v željeno obliko (in potem dokaz take D pade v primer SVD):

- Diagonalen primer.

1. $DD^+D =$

$$\begin{aligned} & \begin{bmatrix} d_1 & & & 0 \\ & \ddots & & \\ & & d_r & \\ 0 & & & \ddots \\ & & & & 0 \end{bmatrix} \begin{bmatrix} d_1^{-1} & & & 0 \\ & \ddots & & \\ & & d_r^{-1} & \\ 0 & & & \ddots \\ & & & & 0 \end{bmatrix} \begin{bmatrix} d_1 & & & 0 \\ & \ddots & & \\ & & d_r & \\ 0 & & & \ddots \\ & & & & 0 \end{bmatrix} = \\ & = \begin{bmatrix} 1 & & & 0 \\ & \ddots & & \\ & & 1 & \\ 0 & & & \ddots \\ & & & & 0 \end{bmatrix} \begin{bmatrix} d_1 & & & 0 \\ & \ddots & & \\ & & d_r & \\ 0 & & & \ddots \\ & & & & 0 \end{bmatrix} = D \end{aligned}$$

2. $D^+DD^+ = \dots = D^+$ na podoben način

$$3. (DD^+)^* = \begin{bmatrix} 1 & & & 0 \\ & \ddots & & \\ & & 1 & \\ 0 & & & \ddots \\ & & & & 0 \end{bmatrix}^* = \begin{bmatrix} 1 & & & 0 \\ & \ddots & & \\ & & 1 & \\ 0 & & & \ddots \\ & & & & 0 \end{bmatrix} = DD^+$$

4. $(D^+D)^* = \dots = D^+D$ podobno

- Splošen primer A — vstavimo $A = Q_1DQ_2^* = Q_1DQ_2^{-1}$.

1. $AA^+A = Q_1DQ_2^*Q_2D^+Q_1^*Q_1DQ_2^* = Q_1DD^+DQ_2^* = Q_1DQ_2^* = A$
2. $A^+AA^+ = \dots = A^+$ na podoben način
3. $(AA^+)^* = (Q_1DQ_2^*Q_2D^+Q_1^*)^* = (Q_1DD^+Q_1^*)^* = Q_1(DD^+)^*Q_1^* = Q_1DD^+Q_1^* = Q_1DQ_2^*Q_2D^+Q_1^* = AA^+$
4. $(A^+A)^* = \dots = A^+A$ podobno

□

Pripomba. A obrnljiva $\Leftrightarrow D$ obrnljiva, torej $A^+ = Q_2D^+Q_1^{-1} = Q_2D^{-1}Q_1^{-1} = A^{-1}$. Potemtakem za obrnljivo A velja $A^+ = A^{-1}$.

Dokaz. Da je definicija dobra, je treba dokazati, da je A^+ enoličen ne glede na SVD, kajti SVD za A ni enoličen. Naj bo $A = Q_1DQ_2^{-1} = Q_3EQ_4^{-1}$, njen prvi psevainverz $B = Q_2D^+Q_1^{-1}$ in njen drugi psevainverz $C = Q_4D^+Q_3^{-1}$.

Ali velja $B \stackrel{?}{=} C$? Velja

$$AB = (ACA)B = ACAB = (AC)^*(AB)^* = C^*A^*B^*A^* = C^*(ABA)^* = C^*A^* = (AC)^* = AC$$

in

$$BA = B(ACA) = BACA = (BA)^*(CA)^* = A^*B^*A^*C^* = (ABA)^*C^* = A^*C^* = (CA)^* = CA$$

ter nazadnje še

$$B = BAB = CAB = CAC = C.$$

□

Kako izračunamo A^+ brez SVD? Če je A pozitivno semidefinitna, jo lahko diagonaliziramo v ortonormirani bazi: $A = PDP^{-1}$, da ima D pozitivne diagonalce in da je $P^{-1} = P^*$. Opazimo, da je to SVD od A , kajti $Q_1 = P, Q_2 = P, D = D$ in tedaj $A = Q_1DQ_2^{-1} = PDP^{-1}$. Potemtakem je $A^+ = PD^+P^{-1}$.

Trditev. Za splošno matriko A (nenujno pozitivno semidefinitno) pa velja $A^+ = (A^*A)^+A^* = A^*(AA^*)^+$. A^*A in AA^* sta pozitivno semidefinitni.

Dokaz. Najprej bomo preverili za diagonalno, nato za SVD:

- Diagonalna $D_{n \times m}$:

$$D = \begin{bmatrix} d_1 & & & 0 \\ & \ddots & & \\ & & d_r & \\ & & & 0 \\ & & & & \ddots \\ & & & & & 0 \end{bmatrix}, \quad D^* = \begin{bmatrix} \bar{d}_1 & & & 0 \\ & \ddots & & \\ & & \bar{d}_r & \\ & & & 0 \\ & & & & \ddots \\ & & & & & 0 \end{bmatrix}, \quad D^*D = \begin{bmatrix} \frac{1}{d_1\bar{d}_1} & & & 0 \\ & \ddots & & \\ & & \frac{1}{d_r\bar{d}_r} & \\ & & & 0 \\ & & & & \ddots \\ & & & & & 0 \end{bmatrix},$$

$$(D^*D)^+ = \begin{bmatrix} \frac{1}{d_1\bar{d}_1} & & & 0 \\ & \ddots & & \\ & & \frac{1}{d_r\bar{d}_r} & \\ & & & 0 \\ & & & & \ddots \\ & & & & & 0 \end{bmatrix}, \quad (D^*D)^+D^* = \begin{bmatrix} \frac{\bar{d}_1}{d_1\bar{d}_1} & & & 0 \\ & \ddots & & \\ & & \frac{\bar{d}_r}{d_r\bar{d}_r} & \\ & & & 0 \\ & & & & \ddots \\ & & & & & 0 \end{bmatrix} = D^+$$

- Za splošen A uporabimo SVD, da to dokažemo: $A = Q_1DQ_2^{-1}$. Velja $A^*A = Q_2D^*Q_1^*Q_1DQ_2^* = Q_2D^*DQ_2^*$ in $(A^*A)^+ = Q_2(D^*D)^+Q_2^*$. Torej $(A^*A)^+A^* = Q_2(D^*D)^+Q_2^*Q_2D^*Q_1^* = Q_2(D^*D)^+D^*Q_1^* = Q_2DQ_1^* = A^+$.

□

Pripomba. V posebnih primerih lahko poenostavljamo dalje. Recimo, da ima A LN stolpce in je kvadratna $\Rightarrow \text{Ker } A = \{0\} = \text{Ker } A^*A$, torej A^*A je obrnljiva in velja $(A^*A)^{-1} = (A^*A)^+$. Takrat torej velja $A^+ = (A^*A)^{-1}A^*$.

To smo uporabili pri iskanju posplošene rešitve predločenega sistema: Za sistem $A\vec{x} = \vec{b}$ iščemo \vec{x} , da je $\|A\vec{x} - \vec{b}\|$ minimalen, tedaj bo tak \vec{x} posplošena rešitev sistema. Vemo, da je posplošena rešitev $A\vec{x} = \vec{b}$ enaka rešitvi od $A^*A\vec{x} = A^*\vec{b}$, kajti, če ima A LN stolpce, je A^*A obrnljiva (s tem dokažemo, da ima ta sistem vedno rešitev):

$$A^*A\vec{x} = A^*\vec{b} \quad / \cdot (A^*A)^{-1}$$

$$\vec{x} = (A^*A)^{-1}A^*\vec{b}$$

$$\vec{x} = A^+\vec{b}$$

Uporaba psevdoinverza Vemo, kaj je posplošena rešitev sistema $A\vec{x} = \vec{b}$. Problem je, da ima sistem lahko več posplošenih rešitev (to se lahko zgodi, če A nima LN stolpcev). Med vsemi rešitvami iščemo tisto, ki je najkrajša po normi — $\|\vec{x}\|$.

Trditev. Najkrajša posplošena rešitev sistema $Ax = b$ je ravno $x = A^+b$.

Dokaz. Dokažimo najprej za diagonalno matriko koeficientov, nato pa še za splošen primer:

- $Dx = b$

$$D_{m \times n} = \begin{bmatrix} d_1 & & & & 0 \\ & \ddots & & & \\ & & d_r & & \\ & & & 0 & \\ & & & & \ddots \\ & & & & & 0 \end{bmatrix}, \quad x = \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}, \quad b = \begin{bmatrix} b_1 \\ \vdots \\ b_m \end{bmatrix}$$

$$\|Dx - b\|^2 = \left\| \begin{bmatrix} d_1 & & & & 0 \\ & \ddots & & & \\ & & d_r & & \\ & & & 0 & \\ & & & & \ddots \\ & & & & & 0 \end{bmatrix} \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} - \begin{bmatrix} b_1 \\ \vdots \\ b_m \end{bmatrix} \right\|^2 = (d_1x_1 - b_1)^2 + \dots + (d_r x_r - b_r)^2 + b_{r+1}^2 + \dots + b_m^2$$

Ta izraz doseže minimum, ko $(d_1x_1 - b_1)^2 + \dots + (d_r x_r - b_r)^2 = 0$, torej $x_1 = \frac{b_1}{d_1}, \dots, x_r = \frac{b_r}{d_r}, x_{r+1} = \dots, x_n = \times$, kjer \times predstavlja poljubno vrednost. Najkrajša rešitev bo torej tista, kjer $x_{r+1} = \dots = x_n = 0$. Trdimo, da je $\left(\frac{b_1}{d_1}, \dots, \frac{b_r}{d_r}, 0, \dots, 0\right) = D^+b$. Preverimo:

$$D_{n \times m}^+ = \begin{bmatrix} d_1^{-1} & & & & 0 \\ & \ddots & & & \\ & & d_r^{-1} & & \\ & & & 0 & \\ & & & & \ddots \\ & & & & & 0 \end{bmatrix}, \quad b = \begin{bmatrix} b_1 \\ \vdots \\ b_m \end{bmatrix}, \quad D^+b = \begin{bmatrix} \frac{b_1}{d_1} \\ \vdots \\ \frac{b_m}{d_m} \\ 0 \\ \vdots \\ 0 \end{bmatrix}$$

Res je!

- Splošen primer s SVD: $A_{m \times n} = Q_1 D Q_2^*$, kjer sta Q_1, Q_2 ortogonalni in D diagonalna. Za tretji enačaj uporabimo dejstvo, da množenje z ortogonalno matriko ohranja normo.⁶ $\|Ax - b\| = \|Q_1 D Q_2^* x - b\| = \|Q_1 (D Q_2^* x - Q_1^{-1} b)\| = \|D Q_2^* x - Q_1^{-1} b\| = \|Dx' - c\|$ za $x' = Q_2^* x$ in $c = Q_1^{-1} b$. Ker je Q_2 obrnljiva, velja, da če x preteče vse vektorje v \mathbb{C}^n , tudi x' preteče vse vektorje v \mathbb{C}^n .

Potemtakem je $\min \|Ax - b\| = \min \|Dx' - c\|$. Če $\|Ax - b\|$ zavzame minimum v x_0 , potem $\|Dx' - c\|$ zavzame minimum v $x'_0 = Q_2^{-1} x_0$ in obratno, če $\|Dx' - c\|$ zavzame minimum v x'_0 , potem $\|Ax - b\|$ zavzame minimum v $x_0 = Q_2 x'_0$. Torej je $x \mapsto Q_2^{-1} x$ bijektivna korespondenca med posplošenimi rešitvami $Ax - b$ in posplošenimi rešitvami $Dx' - c$. Opazimo, da preslikava ohranja normo, torej $\|x'_0\| = \|Q_2 x'_0\| = \|x_0\|$.

Od prej vemo, da je najkrajša posplošena rešitev $Dx_0 - c$ prav $x_0 = D^+c$. Po zgornjem odstavku sledi, da je $x_0 = Q_2 x'_0$ najkrajša posplošena rešitev od $Ax = b$. Dobimo namreč $x_0 = Q_2 x'_0 = Q_2 D^+c = Q_2 D^+ Q_1^{-1} b = A^+b$.

□

⁶ $\|Q_2^* x\|^2 = \langle Q_2^* x, Q_2^* x \rangle = \langle x, Q_2 Q_2^* x \rangle = \langle x, x \rangle = \|x\|^2$

2.4 Kvadratne forme

Definicija. Forma je homogen polinom, torej tak, v katerem imajo vsi monomi isto stopnjo. Stopnja monoma je $\deg(\beta x_1^{\alpha_1} \cdots x_n^{\alpha_n}) := \alpha_1 + \cdots + \alpha_n$.

Definicija. Polinom je vsota monomov. Stopnja polinoma je najvišja stopnja monoma v njem.

Zgled. Linearna forma v treh spremenljivkah: $ax + by + cz = \begin{bmatrix} a & b & c \end{bmatrix} \begin{bmatrix} x \\ y \\ z \end{bmatrix}$.

Zgled. Kvadratna forma je homogen polinom stopnje 2. Primer kvadratne forme:

$$ax^2 + bxy + cy^2 = \begin{bmatrix} x & y \end{bmatrix} \begin{bmatrix} a & b/2 \\ b/2 & a \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}$$

Zgled. Kubična forma v treh spremenljivkah:

$$ax^3 + by^3 + cz^3 + dx^2y + ex^2z + fy^2x + gy^2z + iz^2x + jz^2y + kxyz$$

Definicija. Pravimo, da sta matriki A in B kongruentni, če obstaja obrnljiva $P \ni B = PAP^T$.

Radi bi naredili klasifikacijo kvadratnih form. Če naredimo primerno linearno zamenjavo koordinat, se kvadratna forma poenostavi v $ex^2 + fy^2$ (mešani členi izginejo).

$$x = \alpha x' + \beta y'$$

$$y = \gamma x' + \delta y'$$

zapišemo kot

$$\begin{aligned} \begin{bmatrix} x \\ y \end{bmatrix} &= \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} \begin{bmatrix} x' \\ y' \end{bmatrix}, & \text{transponiranje} & \begin{bmatrix} x & y \end{bmatrix} = \begin{bmatrix} x' & y' \end{bmatrix} \begin{bmatrix} \alpha & \gamma \\ \beta & \delta \end{bmatrix} \\ ax^2 + bxy + cy^2 &= \begin{bmatrix} x & y \end{bmatrix} \begin{bmatrix} a & b/2 \\ b/2 & c \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} x' & y' \end{bmatrix} \begin{bmatrix} \alpha & \gamma \\ \beta & \delta \end{bmatrix} \begin{bmatrix} a & b/2 \\ b/2 & a \end{bmatrix} \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} \begin{bmatrix} x' \\ y' \end{bmatrix} = \\ &= \begin{bmatrix} x' & y' \end{bmatrix} P^T A P \begin{bmatrix} x' \\ y' \end{bmatrix} \end{aligned}$$

Ker je A simetrična, lahko izberemo tako ortogonalno P , da je $P^T A P$ diagonalna, recimo $\begin{bmatrix} d_1 & 0 \\ 0 & d_2 \end{bmatrix}$, torej

$$\begin{bmatrix} x' & y' \end{bmatrix} \begin{bmatrix} d_1 & 0 \\ 0 & d_2 \end{bmatrix} \begin{bmatrix} x' \\ y' \end{bmatrix} = d_1 (x')^2 + d_2 (y')^2$$

Kaj vemo o 2×2 ortogonalnih matrikah? $P = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \Rightarrow P^T P = \begin{bmatrix} a & c \\ b & d \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} a^2 + c^2 & ab + cd \\ ab + cd & b^2 + d^2 \end{bmatrix}$.

Da je $P^T P = I$, mora veljati $ab + cd = 0$ in $a^2 + c^2 = b^2 + d^2 = 1$, torej $a = \cos \varphi$, $c = \sin \varphi$, $b = \cos \tau$, $d = \sin \tau$.

Iz $\cos(\varphi + \tau) = 0$ sledi $\tau = \varphi \pm \frac{\pi}{2}$, torej je $P_1 = \begin{bmatrix} \cos \varphi & -\sin \varphi \\ \sin \varphi & \cos \varphi \end{bmatrix}$ (vrtež za φ) ali $P_2 = \begin{bmatrix} \cos \varphi & \sin \varphi \\ \sin \varphi & -\cos \varphi \end{bmatrix}$

(zrcaljenje žez $\varphi/2$). $\det P_1 = 1$, $\det P_2 = -1$.

Če je $A = \begin{bmatrix} v_1 & v_2 \end{bmatrix} \begin{bmatrix} d_1 & 0 \\ 0 & d_2 \end{bmatrix} \begin{bmatrix} v_1 & v_2 \end{bmatrix}^{-1}$, je tudi $A = \begin{bmatrix} v_1 & -v_2 \end{bmatrix} \begin{bmatrix} d_1 & 0 \\ 0 & d_2 \end{bmatrix} \begin{bmatrix} v_1 & -v_2 \end{bmatrix}^{-1}$. Če je $\begin{bmatrix} v_1 & v_2 \end{bmatrix}$ ortogonalna, je tudi $\begin{bmatrix} v_1 & -v_2 \end{bmatrix}$ ortogonalna. Če je A 2×2 simetrična matrika, lahko poiščemo tak vrtež $P = \begin{bmatrix} \cos \varphi & -\sin \varphi \\ \sin \varphi & \cos \varphi \end{bmatrix}$, da je $A = P \begin{bmatrix} d_1 & 0 \\ 0 & d_2 \end{bmatrix} P^{-1}$.

Povzetek: $ax^2 + bxy + cy^2 \xrightarrow{\text{vrtež}} d_1 x^2 + d_2 y^2$

Zgled. Nariši krivuljo $4x^2 + 4xy + 7y^2 = 1$. Pripadajoča kvadratna forma:

$$\begin{bmatrix} x & y \end{bmatrix} \begin{bmatrix} 4 & 2 \\ 2 & 7 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = 1 = \dots$$

Radi bi se znebili mešanega člana:

$$\dots = \begin{bmatrix} x' & y' \end{bmatrix} P^T \begin{bmatrix} 4 & 2 \\ 2 & 7 \end{bmatrix} P \begin{bmatrix} x' \\ y' \end{bmatrix} = 1 = \dots$$

Iščemo tak vrtež P , da bo $P^T A P$ diagonalna. Izračunamo lastne vrednosti $A = \begin{bmatrix} 4 & 2 \\ 2 & 7 \end{bmatrix}$. Lastni vrednosti sta $\{3, 8\}$. Izračunamo lastna vektorja: $\left\{ \begin{bmatrix} -2 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 2 \end{bmatrix} \right\}$. Sta že ortogonalna, treba ju je še normirati: $\left\{ \begin{bmatrix} -\frac{2}{\sqrt{5}} \\ \frac{1}{\sqrt{5}} \end{bmatrix}, \begin{bmatrix} \frac{1}{\sqrt{5}} \\ \frac{2}{\sqrt{5}} \end{bmatrix} \right\}$. Izdelamo vrtež: $P = \begin{bmatrix} \frac{1}{\sqrt{5}} & -\frac{2}{\sqrt{5}} \\ \frac{2}{\sqrt{5}} & \frac{1}{\sqrt{5}} \end{bmatrix}$. Izračunamo kot vrteža: $\frac{\sin \varphi}{\cos \varphi} = \frac{\frac{2}{\sqrt{5}}}{\frac{1}{\sqrt{5}}} = 2$, $\arctan 2 \approx 63,4^\circ$.

Ogledamo si torej kvadratno formo $\begin{bmatrix} x' & y' \end{bmatrix} \begin{bmatrix} 8 & 0 \\ 0 & 3 \end{bmatrix} \begin{bmatrix} x' \\ y' \end{bmatrix} = 8x'^2 + 3y'^2 = 1$, kar je elipsa $\left(\frac{x'}{a}\right)^2 + \left(\frac{y'}{b}\right)^2 = 1$ s polosema $\frac{1}{\sqrt{8}}$ in $\frac{1}{\sqrt{3}}$.

Elipso narišemo in jo v koordinatnem sistemu zavrtimo v negativno smer za $63,4^\circ$. Po zasuku je risba te krivulje risba naše prvotne kvadratne forme.

Del II

Vaja za ustni izpit

Ustni izpit je sestavljen iz treh vprašanj. Sekcije so zaporedna vprašanja na izpitu, podsekcije so učiteljevi naslovi iz Primerov vprašanj, podpodsekcije pa so dejanska vprašanja, kot so se pojavila na dosedanjih izpitih.

3 Prvo vprašanje

Prvo vprašanje je iz 1. semestra.

3.0.1 $\det AB = \det A \det B$

3.1 Baze vektorskega prostora

3.1.1 Linearno neodvisne množice

3.1.2 Ogrodje

3.1.3 Definicija baze

3.1.4 Dimenzija prostora

3.2 Cramerovo pravilo

3.2.1 Trditev in dokaz

3.3 Obrnljive matrice

3.3.1 Definicija obrnljivosti

3.3.2 Produkt obrnljivih matrik je obrnljiva matrika

3.3.3 Karakterizacija obrnljivih matrik z dokazom

3.3.4 $\text{Ker } A = \{0\} \Leftrightarrow A$ obrnljiva

3.3.5 A ima desni inverz $\Rightarrow A$ obrnljiva

3.3.6 Formula za inverz matrice z dokazom

3.4 Vektorski podprostori

3.5 Elementarne matrice

3.6 Pod-/predoločeni sistem

3.6.1 Definicija, iskanje posplošene rešitve z izpeljavo

3.6.2 Moč ogrodja \geq moč LN množice

3.6.3 Vsak poddoločen sistem ima netrivialno rešitev

Posledica prejšnje trditve.

3.7 Regresijska premica

3.7.1 Definicija

3.8 Vektorski/mešani produkt

3.9 Grupe/polgrupe

3.9.1 Definicija in lastnosti grupe

3.9.2 Definicija homomorfizma

3.9.3 Primeri homomorfizmov z dokazi

3.9.4 Definicija permutacijske grupe in dokaz, da je grupa

3.9.5 Primeri grup

3.9.6 Dokaz, da so ortogonalne matrike podgrupa v grupi obrnljivih matrik

3.9.7 Matrika permutacije

3.9.8 Dokaz, da je preslikava, ki permutaciji priredi matriko, homomorfizem

3.10 Projekcija točke na premico/ravnino

3.11 $\det A = \det A^T$

3.12 Formula za inverz

3.13 Homogeni sistemi enačb

4 Drugo vprašanje

Drugo vprašanje zajema snov linearnih preslikav/lastnih vrednosti.

4.1 Diagonalizacija

4.1.1 Definicija, trditve

4.2 Prehod na novo bazo

4.2.1 Prehodna matrika in njene lastnosti

4.2.2 Predstavitev vektorjev in linearnih preslikav z različnimi bazami

4.2.3 Razvoj vektorja po eni in drugi bazi (prehod vektorja na drugo bazo)

4.3 Matrika linearne preslikave

4.4 Rang matrike

4.4.1 Definicija

4.4.2 Dokaz, da je rang število LN stolpcev

4.4.3 Dimenzijska formula za podprostore

4.5 $\text{rang } A = \text{rang } A^T$

4.6 Ekvivalentnost matrik

4.6.1 Definicija

4.6.2 Dokaz, da je relacija ekvivalenčna

4.6.3 Dokaz, da je vsaka matrika ekvivalentna matriki I_r , t. j. bločni matriki, katere zgornji levi blok je I dimenzije r , drugi trije bloki pa so ničelne matrike.

4.7 Jedro/slika

4.8 Minimalni polinom

4.8.1 Definicija karakterističnega in minimalnega polinoma

4.9 Cayley-Hamiltonov izrek

4.9.1 Trditev in dokaz

4.10 Korenski razcep

4.10.1 Definicija korenskih podprostorov

4.10.2 Presek različnih korenskih podprostorov je trivialen

4.10.3 Vsota korenskih podprostorov je direktna (se sklicuje na zgornjo trditev)

4.11 Osnovna formula rang + ničnost

4.11.1 Definicija

4.12 Funkcije matrik

5 Tretje vprašanje

Tretje vprašanje zajema naslednje snovi:

- vektorski prostori s skalarnim produktom,
- adjungirana preslikava,
- singularni razcep,
- kvadratne forme.

5.0.1 Singularni razcep: Konstrukcija Q_1, Q_2, D in dokaz $A = Q_1 D Q_2^{-1}$.

5.1 Ortogonalne/unitarne matrike

5.1.1 Definicija

5.1.2 Dokaz $AA^* = I$

5.1.3 Lastne vrednosti

5.1.4 Prehodna matrika iz ONB v drugo ONB ima ortogonalne stolpce (dokaz)

5.2 Kvadratne krivulje

5.3 Psevdo inverz

5.3.1 Definicija

5.4 Najkrajša splošena rešitev sistema

5.4.1 Definicija, trditev in dokaz

5.5 Simetrične matrike

5.5.1 Vse o simetričnih matrikah

5.6 Adjungirana linearna preslikava

5.6.1 Definicija in celotna formulacija

5.6.2 Rieszov izrek

5.6.3 Dokaz obstoja in enoličnosti kot posledica Rieszovega izreka

5.6.4 Formula za matriko linearne preslikave in $\langle Au, v \rangle = v^* Au = \langle u, A^* v \rangle$

5.6.5 Lastne vrednosti adjungirane matrike

5.7 Klasifikacija skalarnih produktov

5.8 Normalne matrike

5.8.1 Definicija, lastnosti, izreki, dokazi

5.8.2 A normalna $\Rightarrow A$ in A^* imata isto množico lastnih vrednosti

5.8.3 $\text{Ker}(A - xI) = \text{Ker}(A - \bar{x}I)$ za normalno A

5.9 Ortogonalni komplement

5.9.1 Formula za ortogonalno projekcijo

5.10 Izrek o reprezentaciji linearnih funkcionalov

5.11 Pozitivno semidefinitne matrike

5.11.1 Definicija, lastnosti.

5.11.2 Dokaz, da imajo nenegativne lastne vrednosti.

5.11.3 Kvadratni koren pozitivno semidefinitne matrike.

5.11.4 $A \geq 0 \Rightarrow A$ sebiadjungirana

5.12 Ortogonalne in ortonormirane baze/Gram-Schmidt