Produkti suma kvadrata

Kupinić, Maja

SVEUČILIŠTE U ZAGREBU

PRIRODOSLOVNO–MATEMATIČKI FAKULTET

MATEMATIČKI ODSJEK

Maja Kupinić

PRODUKTI SUMA KVADRATA

Diplomski rad

Voditelj rada:
prof. dr. sc. Goran Muić,
dr. sc. Sonja Žunar

Zagreb, srpanj 2021.

Ovaj diplomski rad obranjen je dana _____ pred ispitnim povjerenstvom u sastavu:

1. _____, predsjednik
2. _____, član
3. _____, član

Povjerenstvo je rad ocijenilo ocjenom _____.

Potpisi članova povjerenstva:

1. _____
2. _____
3. _____

Sadržaj

Uvod

U ovom radu ćemo proučavati rezultate vezane za produkte suma n kvadrata, gdje je n prirodan broj. Trivijalni identitet $x_1^2y_1^2 = (x_1y_1)^2$ kaže da je produkt kvadrata jednak kvadratu produkta. Identitet $(x_1^2+x_2^2)(y_1^2+y_2^2) = (x_1y_1-x_2y_2)^2+(x_1y_2+x_2y_1)^2$ za $n = 2$ u kojem je zbroj dvaju kvadrata pomnožen sa zbrojem nekih drugih dvaju kvadrata opet zbroj dvaju kvadrata (na primjer, $65 = 5\cdot 13 = (1^2+2^2)(2^2+3^2) = (1\cdot 2-2\cdot 3)^2+(1\cdot 3+2\cdot 2)^2 = 4^2+7^2$) bio je poznat Brahmagupti još u 7. stoljeću, a 1000 godina kasnije ga je ponovno otkrio Fermat. Analogan identitet za $n = 4$ otkrio je Euler 1748., a 1843. ga je ponovno otkrio Hamilton u svom radu o kvaternionima. Uskoro nakon toga, otkriven je analogan identitet za $n = 8$ koji su neovisno otkrili Graves 1843. i Cayley 1845. Matematičari su pokušavali naći analogan identitet i za $n = 16$, ali to je dugo vremena bilo bezuspješno. Štoviše, Hurwitz je 1898. dokazao svoj poznati $(1, 2, 4, 8)$-teorem po kojem takav identitet postoji jedino za $n \in \{1, 2, 4, 8\}$.

Svaki od spomenutih identiteta općenito glasi $(x_1^2 + ... + x_n^2)(y_1^2 + ... + y_n^2) = z_1^2 + ... + z_n^2$, pri čemu su z_k bilinearni polinomi u varijablama x_i i y_j nad poljem $\mathbb{C}$. Nakon Hurwitzovog $(1, 2, 4, 8)$-teorema i daljnje potrage za identitetima u kojima z_k nije nužno $\mathbb{C}$-bilinearan polinom u varijablama x_i i y_j, 1960. otkriven je takav identitet za $n = 16$. Štoviše, Pfister je otkrio da analogan identitet vrijedi za sve $n = 2^k, k \in \mathbb{N}_0$, pri čemu su z_k racionalne funkcije u varijablama x_i i y_j nad poljem $\mathbb{C}$.

U prvom poglavlju ovog rada navode se osnovne definicije i svojstva vezana za vektorske prostore, matrice, determinante, linearne operatore te polinome i racionalne funkcije. Potom se u drugom poglavlju uvode produkti suma kvadrata na konkretnim primjerima. Opisano je kako su kroz povijest proučavanjem produkata suma kvadrata otkriveni teoremi koji se iskazuju i dokazuju u sljedećim dvama poglavljima. Prvi glavni teorem je Hurwitzov $(1, 2, 4, 8)$-teorem, a drugi Pfisterov teorem o sumama kvadrata. Za dokazivanje tih teorema bit će potrebni neki pomoćni rezultati koji se također pojavljuju u radu. Nakon tih teorema, na kraju svakog poglavlja zasebno, opisane su i neke njihove primjene.

Poglavlje 1

Osnovni pojmovi

1.1 Vektorski prostori

Definicija 1.1.1. *Neka je G neprazan skup i neka je dano preslikavanje $\cdot : G \times G \to G$. Uređeni par $(G, \cdot)$ je grupa ako vrijede sljedeća svojstva:*

1. $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ *za sve* $x, y, z \in G$ *(asocijativnost)*
2. *postoji* $e \in G$ *takav da je* $e \cdot x = x \cdot e = x$ *za sve* $x \in G$ *(neutralni element)*
3. *za svaki* $x \in G$ *postoji* $y \in G$ *takav da je* $x \cdot y = y \cdot x = e$ *(inverzni element).*

Ako vrijedi i svojstvo komutativnosti $x \cdot y = y \cdot x$ za sve $x, y \in G$, onda je $(G, \cdot)$ komutativna ili Abelova grupa.

Definicija 1.1.2. *Neka je $(G, \cdot)$ grupa i neka je $H \subseteq G$. Kažemo da je H podgrupa od G ako vrijedi:*

1. $x \cdot y \in H$ *za sve* $x, y \in H$ *(zatvorenost)*
2. $x^{-1} \in H$ *za svaki* $x \in H$ *(inverzni element).*

Pišemo $H \leq G$.

Definicija 1.1.3. *Neka je R neprazan skup na kojem su definirane dvije binarne operacije $+$ i $\cdot$. Kažemo da je uređena trojka $(R, +, \cdot)$ prsten ako vrijedi:*

1. $(R, +)$ *je Abelova grupa*
2. $(R, \cdot)$ *je polugrupa (operacija $\cdot$ je asocijativna)*

3. $x \cdot (y + z) = x \cdot y + x \cdot z, \quad (x + y) \cdot z = x \cdot z + y \cdot z$ *za sve* $x, y, z \in \mathbb{R}$
(distributivnost operacije $\cdot$ *u odnosu na operaciju* $+$*).*

Neutralni element strukture $(R, \cdot)$*, ako postoji, zove se jedinica prstena* R *i označava s* 1*.*
Ako on postoji, tada se $(R, +, \cdot)$ *naziva prsten s jedinicom.*
Ako je operacija $\cdot$ *komutativna, tada govorimo o komutativnom prstenu.*

Definicija 1.1.4. *Komutativni prsten s jedinicom* $(R, +, \cdot)$ *takav da je svaki element* $x \in R \setminus \{0\}$ *invertibilan (to jest postoji* $y \in R$ *takav da je* $xy = yx = 1$*) naziva se polje.*

Definicija 1.1.5. *Neka je* R *prsten. Tada njegov centar definiramo kao*

$$\mathcal{Z}(R) = \{x \in R : xr = rx, \text{ za svaki } r \in R\}.$$

Definicija 1.1.6. *Neka je* R *prsten i pretpostavimo da postoji* $m \in \mathbb{N}$ *takav da je* $mx = 0$ *za sve* $x \in R$*. Definirajmo karakteristiku prstena* R *s*

$$\operatorname{char} R = \text{minimalan takav } m,$$

ako takav m *postoji. U suprotnom govorimo da je* R *karakteristike nula i pišemo* $\operatorname{char} R = 0$*.*

Definicija 1.1.7. *Neka je* $(V, +)$ *Abelova grupa i neka je* $\mathbb{F}$ *polje. Ako postoji preslikavanje* $\cdot : \mathbb{F} \times V \to V$ *koje zadovoljava sljedeća svojstva:*

1. $\alpha \cdot (\beta \cdot a) = (\alpha \cdot \beta) \cdot a$ *za sve* $\alpha, \beta \in \mathbb{F}$*,* $a \in V$ *(kvaziasocijativnost)*
2. $(\alpha + \beta) \cdot a = \alpha \cdot a + \beta \cdot a$ *za sve* $\alpha, \beta \in \mathbb{F}$*,* $a \in V$
(distributivnost operacije $\cdot$ *u odnosu na operaciju* $+$ *u* $\mathbb{F}$*)*
3. $\alpha \cdot (a + b) = \alpha \cdot a + \alpha \cdot b$*, za sve* $\alpha \in \mathbb{F}$*,* $a, b \in V$
(distributivnost operacije $\cdot$ *u odnosu na operaciju* $+$ *u* V*)*
4. $1 \cdot a = a$ *za sve* $a \in V$*,*

tada se uređena trojka $(V, +, \cdot)$ *naziva vektorski ili linearni prostor nad poljem* $\mathbb{F}$*.*

Elemente skupa V *zovemo vektorima, a elemente polja* $\mathbb{F}$ *skalarima. Neutralni element Abelove grupe* $(V, +)$ *zovemo nulvektor i označavamo s* 0_V*. Operaciju* $\cdot$ *zovemo množenje vektora skalarom.*

Definicija 1.1.8. *Neka je* V *vektorski prostor nad poljem* $\mathbb{F}$ *i neka je* $k \in \mathbb{N}$*. Za* $\alpha_1, ..., \alpha_k \in \mathbb{F}$ *i* $a_1, ..., a_k \in V$ *vektor oblika*

$$\alpha_1 a_1 + ... + \alpha_k a_k$$

nazivamo linearna kombinacija vektora $a_1, ..., a_k$ *s koeficijentima* $\alpha_1, ..., \alpha_k$*.*

Definicija 1.1.9. *Neka je V vektorski prostor nad poljem $\mathbb{F}$ i neka je $S \subseteq V$. Skup svih linearnih kombinacija vektora iz S naziva se linearna ljuska ili linearni omotač skupa S i označava sa $[S]$. Dakle,*

$$[S] = \{\alpha_1 a_1 + ... + \alpha_n a_n : n \in \mathbb{N}, a_1, ..., a_n \in S, \alpha_1, ..., \alpha_n \in \mathbb{F}\}.$$

Ako je $S = \{a_1, ..., a_k\}$, tada pišemo

$$[S] = [a_1, ..., a_k] = \{\alpha_1 a_1 + ... + \alpha_k a_k : \alpha_1, ..., \alpha_k \in \mathbb{F}\}$$

te skup $[a_1, ..., a_k]$ nazivamo linearnom ljuskom ili linearnim omotačem vektora $a_1, ..., a_k$.

Definicija 1.1.10. *Neka je V vektorski prostor nad poljem $\mathbb{F}$ i neka je $G \subseteq V$. Ako je*

$$V = [G],$$

odnosno ako se svaki vektor iz V može prikazati kao linearna kombinacija konačno mnogo vektora iz G, tada kažemo da je G sustav izvodnica ili generatora za prostor V. Dakle, ako je $V = [G]$, tada za svaki $x \in V$ postoje vektori $a_1, ..., a_k \in G$ i skalari $\alpha_1, ..., \alpha_k \in \mathbb{F}$ takvi da se x prikazuje kao

$$x = \alpha_1 a_1 + ... + \alpha_k a_k = \sum_{i=1}^{k} \alpha_i a_i.$$

Definicija 1.1.11. *Neka je V vektorski prostor nad poljem $\mathbb{F}$ i neka je $S = \{a_1, ..., a_k\} \subseteq V$. Kažemo da je S linearno nezavisan skup vektora ako se nulvektor 0_V može na jedinstveni način prikazati pomoću vektora iz S, to jest ako*

$$\alpha_1 a_1 + ... + \alpha_k a_k = 0_V \Rightarrow \alpha_1 = ... = \alpha_k = 0.$$

U protivnom, ako postoji izbor skalara $\alpha_1, ..., \alpha_k$ takav da je barem jedan skalar $\alpha_i \neq 0$ i da vrijedi $\alpha_1 a_1 + ... + \alpha_k a_k = 0_V$, tada kažemo da je skup S linearno zavisan.

Definicija 1.1.12. *Podskup B vektorskog prostora V je baza prostora V ako je B sustav izvodnica za V i linearno nezavisan skup u V.*

Definicija 1.1.13. *Neka je $n \in \mathbb{N}$. Za svaki $i \in \{1, \ldots, n\}$ neka je $e_i \in \mathbb{R}^n$ uređena n-torka čiji je i-ti koeficijent 1, a svi ostali koeficijenti su 0. Skup $\{e_1, ..., e_n\}$ je baza prostora $\mathbb{R}^n$ i naziva se kanonska ili standardna baza prostora $\mathbb{R}^n$.*

Definicija 1.1.14. *Vektorski prostor koji ima konačnu bazu naziva se konačnodimenzionalan. U protivnom je beskonačnodimenzionalan.*

Definicija 1.1.15. *Neka je V konačnodimenzionalan vektorski prostor i $V \neq \{0_V\}$. Broj vektora u bilo kojoj bazi prostora V naziva se dimenzija vektorskog prostora V i označava s $\dim V$. Ako je $\dim V = n$, tada kažemo da je V n-dimenzionalan vektorski prostor.*

Definicija 1.1.16. *Standardni skalarni produkt na $\mathbb{R}^3$ je preslikavanje $\cdot : \mathbb{R}^3 \times \mathbb{R}^3 \to \mathbb{R}$ koje vektorima $a = (a_1, a_2, a_3)$, $b = (b_1, b_2, b_3) \in \mathbb{R}^3$ pridružuje skalar*

$$a \cdot b = a_1 b_1 + a_2 b_2 + a_3 b_3.$$

Vrijednost $a \cdot b \in \mathbb{R}$ nazivamo standardnim skalarnim produktom vektora a i b.

Definicija 1.1.17. *Standardna (euklidska) norma na vektorskom prostoru $\mathbb{R}^3$ je preslikavanje $\|\cdot\| : \mathbb{R}^3 \to \mathbb{R}$ definirano formulom*

$$\|x\| = \sqrt{x \cdot x} = \sqrt{\sum_{i=1}^{3} x_i^2}$$

za $x = (x_1, x_2, x_3) \in \mathbb{R}^3$.

Definicija 1.1.18. *Standardni vektorski produkt na $\mathbb{R}^3$ je preslikavanje $\times : \mathbb{R}^3 \times \mathbb{R}^3 \to \mathbb{R}^3$ definirano formulom*

$$a \times b = (a_2 b_3 - a_3 b_2) e_1 + (a_3 b_1 - a_1 b_3) e_2 + (a_1 b_2 - a_2 b_1) e_3$$

za $a = (a_1, a_2, a_3), b = (b_1, b_2, b_3) \in \mathbb{R}^3$, pri čemu je skup $\{e_1, e_2, e_3\}$ kanonska baza za $\mathbb{R}^3$.

Teorem 1.1.19. *Standardni vektorski produkt na $\mathbb{R}^3$ ima svojstva da za sve vektore $a = (a_1, a_2, a_3)$, $b = (b_1, b_2, b_3)$, $c = (c_1, c_2, c_3) \in \mathbb{R}^3$ i $\lambda \in \mathbb{R}$ vrijedi:*

1. $(a+b) \times c = a \times c + b \times c$, $a \times (b+c) = a \times b + a \times c$ *(distributivnost prema zbrajanju)*
2. $\lambda(a \times b) = (\lambda a) \times b = a \times (\lambda b)$ *(kvaziasocijativnost)*
3. $a \cdot (a \times b) = 0$, $b \cdot (a \times b) = 0$ *(okomitost)*
4. $\|a \times b\|^2 = \|a\|^2 \|b\|^2 - (a \cdot b)^2$ *(Pitagorino svojstvo).*

1.2 Matrice

Neka su $m, n \in \mathbb{N}$ i neka je $\mathbb{F}$ polje.

Definicija 1.2.1. *Preslikavanje*

$$A : \{1, ..., m\} \times \{1, ..., n\} \to \mathbb{F}$$

naziva se matrica tipa (m, n) *(ili* $m \times n$*) s koeficijentima (ili elementima) iz polja* $\mathbb{F}$*. Skup svih takvih matrica označavamo s* $M_{mn}(\mathbb{F})$*. Dakle, matrica A uređenom paru* $(i, j), 1 \leq i \leq m, 1 \leq j \leq n$*, pridružuje skalar* α_{ij} *iz polja* $\mathbb{F}$*. Pišemo*

$$A = \begin{pmatrix} \alpha_{11} & ... & \alpha_{1n} \\ . & & . \\ . & & . \\ . & & . \\ \alpha_{m1} & ... & \alpha_{mn} \end{pmatrix}.$$

Matricu A s elementima a_{ij} *koji se nalaze na presjeku i-tog retka i j-tog stupca kraće zapisujemo kao* $A = (a_{ij})$*.*

Definicija 1.2.2. *Matrica tipa* (n, n) *naziva se kvadratna matrica ili matrica reda n. Skup svih takvih matrica s elementima iz* $\mathbb{F}$ *označavamo s* $M_n(\mathbb{F})$*.*

Definicija 1.2.3. *Matrica* $D = (d_{ij})$ *reda n je dijagonalna ako je* $d_{ij} = 0$ *za sve* $i \neq j$*, a skalarna ako je dijagonalna i vrijedi* $d_{ii} = d_{jj}$ *za sve* $i, j = 1, \ldots, n$*.*

Definicija 1.2.4. *Matrica* $I = (\delta_{ij})$ *reda n je jedinična ako je dijagonalna i* $\delta_{ii} = 1$ *za sve* $i = 1, ..., n$*.*

Definicija 1.2.5. *Neka je* $A = (a_{ij}) \in M_{mn}(\mathbb{F})$*. Transponirana matrica matrice A je matrica* $B = (B_{ij}) \in M_{nm}(\mathbb{F})$ *za čije elemente vrijedi*

$$b_{ij} = a_{ji}$$

za sve $i = 1, ..., m$*,* $j = 1, ..., n$*. Pišemo* $B = A^\top$*. Preslikavanje*

$$t : M_{mn}(\mathbb{F}) \to M_{nm}(\mathbb{F}), \quad A \mapsto A^\top$$

naziva se transponiranje.

Definicija 1.2.6. *Matrica* $A \in M_n(\mathbb{F})$ *je simetrična ako vrijedi* $A = A^\top$*, odnosno antisimetrična ako vrijedi* $A = -A^\top$*.*

Definicija 1.2.7. *Matrice A i B su ulančane ako je broj stupaca matrice A jednak broju redaka matrice B.*

Definicija 1.2.8. *Neka je $A = [a_{ij}]$ matrica tipa (m, n) i $B = [b_{ij}]$ matrica tipa (n, p). Umnožak matrica A i B je matrica $C = [c_{ij}]$ tipa (m, p) čiji su elementi dani formulom*

$$c_{ij} = a_{i1}b_{1j} + ... + a_{in}b_{nj} = \sum_{k=1}^{n} a_{ik}b_{kj}$$

za $i = 1, ..., m$, $j = 1, ..., p$. Pišemo $C = A \cdot B = AB$. Time je definirana operacija množenja matrica

$$\cdot : M_{mn}(\mathbb{F}) \times M_{np}(\mathbb{F}) \to M_{mp}(\mathbb{F}).$$

Definicija 1.2.9. *Kvadratna matrica $A \in M_n(\mathbb{F})$ je invertibilna ili regularna ako postoji matrica $B \in M_n(\mathbb{F})$ takva da je*

$$AB = BA = I.$$

Matricu B nazivamo inverznom matricom od A i pišemo $B = A^{-1}$. U protivnom, A je singularna matrica.

Definicija 1.2.10. *Kvadratna matrica $A \in M_n(\mathbb{F})$ je ortogonalna ako vrijedi*

$$AA^\top = A^\top A = I,$$

to jest ako je $A^{-1} = A^\top$.

Definicija 1.2.11. *Kvadratne matrice $A, B \in M_n(\mathbb{F})$ su komutativne ako vrijedi $AB = BA$, a antikomutativne ako vrijedi $AB = -BA$.*

Definicija 1.2.12. *Neka je $B \in M_n(\mathbb{F})$. Konjugiranje invertibilnom matricom $A \in M_n(\mathbb{F})$ je funkcija $M_n(\mathbb{F}) \to M_n(\mathbb{F})$ koja matricu B preslikava u matricu ABA^{-1}.*

1.3 Determinante

Definicija 1.3.1. *Neka je S_n skup svih bijektivnih preslikavanja $p : \{1, ..., n\} \to \{1, ..., n\}$. Takvo preslikavanje p nazivamo permutacijom skupa $\{1, ..., n\}$ i označavamo s*

$$p = \begin{pmatrix} 1 & ... & n \\ p(1) & ... & p(n) \end{pmatrix}.$$

Definicija 1.3.2. *Inverzija permutacije p je svaki par (i, j) takav da je*

$$1 \leq i < j \leq n, \quad p(i) > p(j).$$

Definicija 1.3.3. *Predznak permutacije p definira se kao*

$$\text{sign}p = (-1)^{I(p)},$$

gdje je $I(p)$ broj inverzija permutacije p.

Definicija 1.3.4. *Neka je $A \in M_n(\mathbb{F})$. Determinanta matrice A je skalar iz polja $\mathbb{F}$ koji se definira kao*

$$\det A = \sum_{p \in S_n} (\text{sign}p) a_{1p(1)} \cdots a_{np(n)},$$

gdje je S_n grupa permutacija skupa $\{1, ..., n\}$, a $\text{sign}p \in \{-1, 1\}$ predznak permutacije. Još kažemo da je determinanta reda n preslikavanje

$$\det : M_n(\mathbb{F}) \to \mathbb{F}, \quad A \mapsto \det A.$$

1.4 Linearni operatori

Definicija 1.4.1. *Neka su V, W vektorski prostori nad istim poljem $\mathbb{F}$. Preslikavanje $A : V \to W$ nazivamo linearni operator ako vrijede sljedeća svojstva:*

1. *$A(a + b) = A(a) + A(b)$ za sve $a, b \in V$ (aditivnost)*
2. *$A(\alpha a) = \alpha A(a)$ za sve $a \in V, \alpha \in \mathbb{F}$ (homogenost).*

Skup svih linearnih operatora $V \to W$, u oznaci $\mathcal{L}(V, W)$, jest vektorski prostor.
U slučaju kada je $V = W$, kratko pišemo $\mathcal{L}(V) = \mathcal{L}(V, V)$.

Napomena 1.4.2. *Svojstva aditivnosti i homogenosti linearnog operatora $A : V \to W$ ekvivalentna su svojstvu linearnosti*

$$A(\alpha a + \beta b) = \alpha A(a) + \beta A(b)$$

za sve $a, b \in V, \alpha, \beta \in \mathbb{F}$.

Definicija 1.4.3. *Linearni operatori $A, B : V \to V$ su komutativni ako vrijedi $AB = BA$, a antikomutativni ako vrijedi $AB = -BA$.*

Definicija 1.4.4. *Neka su V, W konačnodimenzionalni vektorski prostori nad istim poljem $\mathbb{F}$, $(e) = \{e_1, ..., e_n\}$ baza prostora V i $\{b_1, ..., b_n\}$ bilo koji podskup prostora W. Tada postoji jedinstveni linearan operator $A : V \to W$ za kojeg vrijedi*

$$A(e_i) = b_i, \quad i = 1, ..., n.$$

Neka je $(f) = \{f_1, \ldots, f_m\}$ *baza prostora* W. *Za svaki* $j \in \{1, \ldots, n\}$ *postoje jedinstveni* $\alpha_{1j}, \ldots \alpha_{mj} \in \mathbb{F}$ *takvi da je* $b_i = \alpha_{1j} f_1 + \ldots + \alpha_{mj} f_m$. *Linearan operator* A *je jedinstveno određen koeficijentima* $\alpha_{ij} \in \mathbb{F}, i = 1, ..., m, j = 1, ..., n$, *odnosno* $m \times n$ *matricom oblika*

$$[A]_{(f,e)} = \begin{pmatrix} \alpha_{11} & ... & \alpha_{1n} \\ . & & . \\ . & & . \\ . & & . \\ \alpha_{m1} & ... & \alpha_{mn} \end{pmatrix}.$$

Matrica $[A]_{(f,e)}$ *naziva se matrica linearnog operatora* A *u paru baza* (e) *i* (f), *odnosno matrični zapis linearnog operatora* A *u paru baza* (e) *i* (f).
Ako je $V = W$ *i* $(e) = (f)$, *kratko pišemo* $[A]_{(e)} = [A]_{(e,e)}$.

Definicija 1.4.5. *Neka je* V *konačnodimenzionalan vektorski prostor nad poljem* $\mathbb{F}$, $A \in \mathcal{L}(V)$ *i* (e) *baza za* V. *Tada se determinanta linearnog operatora* A *definira kao determinanta matričnog zapisa operatora* A *u bazi* (e), *to jest*

$$\det A = \det[A]_{(e)}.$$

Teorem 1.4.6. *Neka je* V *konačnodimenzionalan vektorski prostor nad poljem* $\mathbb{F}$ *i* $A, B \in \mathcal{L}(V)$. *Za* $\alpha \in \mathbb{F}$ *i linearne operatore* $A, B : V \to V$ *vrijede sljedeća svojstva:*

1. $\det(\alpha A) = \alpha^{\dim V} \det A$
2. $\det(AB) = \det A \cdot \det B$
3. $\det A \neq 0$ *ako i samo ako je linearan operator* A *invertibilan.*

Definicija 1.4.7. *Neka je* V *vektorski prostor nad poljem* $\mathbb{F}$ *i* $A \in \mathcal{L}(V)$. *Za vektor* $x \in V$ *takav da* $x \neq 0_V$ *kažemo da je svojstveni vektor operatora* A *ako postoji skalar* $\lambda \in \mathbb{F}$ *takav da je*

$$Ax = \lambda x.$$

Taj skalar naziva se svojstvena vrijednost operatora A *pridružena svojstvenom vektoru* x.

Definicija 1.4.8. *Skup svih svojstvenih vrijednosti linearnog operatora* A *naziva se spektar i označava sa* $\sigma(A)$.

Definicija 1.4.9. *Neka je* $A \in \mathcal{L}(V)$ *i* $\lambda \in \sigma(A)$. *Potprostor* $V_A(\lambda) = \{x \in V : Ax = \lambda x\}$ *naziva se svojstveni potprostor pridružen svojstvenoj vrijednosti* λ.

1.5 Polinomi i racionalne funkcije

Neka je $n \in \mathbb{N}$ i neka je $\mathbb{F}$ polje.

Definicija 1.5.1. *Monom u varijablama $x_1, ..., x_n$ s koeficijentima iz $\mathbb{F}$ je izraz oblika*

$$ax_1^{i_1} \cdots x_n^{i_n},$$

gdje su $a \in \mathbb{F}$ i $i_1, ..., i_n \in \mathbb{N} \cup \{0\}$.

Definicija 1.5.2. *Polinom p u varijablama $x_1, ..., x_n$ s koeficijentima iz $\mathbb{F}$ je formalna suma konačno mnogo monoma u varijablama $x_1, ..., x_n$ s koeficijentima iz $\mathbb{F}$, to jest izraz oblika*

$$\sum_{i=(i_1,...,i_n)\in I} a_i x_1^{i_1} \cdots x_n^{i_n},$$

gdje je I konačan podskup od $(\mathbb{N} \cup \{0\})^n$ i $a_i \in \mathbb{F}$.

Napomena 1.5.3. *Uz standardno definirane operacije zbrajanja i množenja, skup $\mathbb{F}[x_1, ..., x_n]$ polinoma u varijablama $x_1, ..., x_n$ s koeficijentima iz $\mathbb{F}$ je komutativan prsten s jedinicom, štoviše radi se o integralnoj domeni (elementi nisu djelitelji nule).*

Primjer polinoma: $x_2^2 x_3^2 + \sqrt{3} \in \mathbb{R}[x_1, x_2, x_3]$.

Definicija 1.5.4. *Neka je $k \in \mathbb{N} \cup \{0\}$. Uz oznake iz Definicije 1.5.2, ako za svaki $i \in I$ vrijedi*

$$i_1 + \ldots + i_n = k,$$

kažemo da je p homogeni polinom stupnja k.

Definicija 1.5.5. *Racionalne funkcije u varijablama $x_1, ..., x_n$ s koeficijentima iz $\mathbb{F}$ su formalni kvocijenti oblika*

$$\frac{f}{g},$$

gdje su $f, g \in \mathbb{F}[x_1, ..., x_n]$, $g \neq 0$ i $\frac{f_1}{g_1} = \frac{f_2}{g_2} \Leftrightarrow f_1 g_2 = f_2 g_1$. Preciznije, racionalne funkcije u varijablama $x_1, ..., x_n$ s koeficijentima iz $\mathbb{F}$ su klase ekvivalencije formalnih kvocijenata $\frac{f}{g}$, gdje su $f, g \in \mathbb{F}[x_1, ..., x_n]$ i $g \neq 0$, po relaciji ekvivalencije

$$\frac{f_1}{g_1} \sim \frac{f_2}{g_2} \Leftrightarrow f_1 g_2 = f_2 g_1.$$

Napomena 1.5.6. *Uz standardno definirane operacije zbrajanja i množenja, skup $\mathbb{F}(x_1, \ldots, x_n)$ racionalnih funkcija u varijablama $x_1, ..., x_n$ s koeficijentima iz $\mathbb{F}$ je polje.*

Primjer racionalne funkcije: $\frac{7+x_2^3}{\sqrt{2}x_6 - 1} \in \mathbb{R}(x_1, x_2, x_3, x_4, x_5, x_6)$.

Svakom polinomu $p = \sum_{i \in I} a_i x_1^{i_1} \cdots x_n^{i_n} \in \mathbb{F}[x_1, ..., x_n]$ možemo pridružiti funkciju $p_0 : \mathbb{F}^n \to \mathbb{F}$ za koju vrijedi

$$p_0(c_1, ..., c_n) = \sum_{i \in I} a_i c_1^{i_1} \cdots c_n^{i_n}$$

za sve $(c_1, ..., c_n) \in \mathbb{F}^n$.

Teorem 1.5.7. *(O jednakosti polinoma). Neka je $\mathbb{F} \in \{\mathbb{R}, \mathbb{C}\}$ i neka su $p, g \in \mathbb{F}[x_1, ..., x_n]$. Uz gornje oznake tada vrijedi*

$$p = g \Leftrightarrow p_0 = g_0.$$

Napomena 1.5.8. *Teorem 1.5.7 nam omogućuje da u slučaju kada je $\mathbb{F} \in \{\mathbb{R}, \mathbb{C}\}$ polinome $p \in \mathbb{F}[x_1, ..., x_n]$, koji su po definiciji formalne sume monoma, identificiramo s funkcijama $\mathbb{F}^n \to \mathbb{F}$ koje su definirane tim formalnim sumama.*

Primjerice, polinom $x_1^2 x_2^2 - \sqrt{2} \in \mathbb{R}[x_1, x_2]$ identificiramo s funkcijom $\mathbb{R}^2 \to \mathbb{R}$, $(x_1, x_2) \mapsto x_1^2 x_2^2 - \sqrt{2}$.

Definicija 1.5.9. *Polinom $p \in \mathbb{F}[x_1, ..., x_n, y_1, ..., y_n]$ je bilinearan ako je*

$$p = \sum_{i=1}^{n} \sum_{j=1}^{n} a_{ij} x_i y_j$$

za neke $a_{ij} \in \mathbb{F}$.

Poglavlje 2

O produktu suma kvadrata

Za svaka dva kompleksna broja x_1, y_1 vrijedi da je produkt njihovih kvadrata jednak kvadratu njihova produkta:

$$x_1^2 y_1^2 = (x_1 y_1)^2. \tag{2.1}$$

Općenitije, ovaj identitet očito vrijedi u svakom komutativnom prstenu R i pokazuje da je u R, u slučaju kada je $n = 1$, zbroj n kvadrata pomnožen sa zbrojem n kvadrata opet zbroj n kvadrata.

Za $n = 2$ vrijedi zanimljiviji identitet koji kaže da je zbroj dvaju kvadrata pomnožen sa zbrojem nekih drugih dvaju kvadrata opet zbroj dvaju kvadrata:

$$(x_1^2 + x_2^2)(y_1^2 + y_2^2) = (x_1 y_1 - x_2 y_2)^2 + (x_1 y_2 + x_2 y_1)^2. \tag{2.2}$$

Postavlja se pitanje može li se za bilo koji prirodan broj n dokazati da je zbroj n kvadrata pomnožen sa zbrojem drugih n kvadrata opet zbroj n kvadrata. Već za $n = 3$ nećemo moći zapisati identitet u traženom obliku, ali za $n = 4$ otkriven je sljedeći identitet:

$$\begin{aligned}(x_1^2 + x_2^2 + x_3^2 + x_4^2)(y_1^2 + y_2^2 + y_3^2 + y_4^2) =& (x_1 y_1 - x_2 y_2 - x_3 y_3 - x_4 y_4)^2 + \\ & (x_1 y_2 + x_2 y_1 + x_3 y_4 - x_4 y_3)^2 + \\ & (x_1 y_3 + x_3 y_1 - x_2 y_4 + x_4 y_2)^2 + \\ & (x_1 y_4 + x_4 y_1 + x_2 y_3 - x_3 y_2)^2.\end{aligned} \tag{2.3}$$

Izrazi u zagradama na desnoj strani jednakosti zapravo su linearne kombinacije varijabli x_i kada je $y = (y_1, y_2, y_3, y_4)$ fiksiran i linearne kombinacije varijabli y_j kada je $x = (x_1, x_2, x_3, x_4)$ fiksiran.

Nadalje, Graves (1843.) i Cayley (1845.) neovisno su otkrili da analogan identitet vrijedi i za $n = 8$:

$$\begin{aligned}\left(\sum_{i=1}^{8} x_i^2\right)\left(\sum_{j=1}^{8} y_j^2\right) =& (x_1y_1 - x_2y_2 - x_3y_3 - x_4y_4 - x_5y_5 - x_6y_6 - x_7y_7 - x_8y_8)^2 + \\ & (x_1y_2 + x_2y_1 + x_3y_4 - x_4y_3 + x_5y_6 - x_6y_5 - x_7y_8 + x_8y_7)^2 + \\ & (x_1y_3 - x_2y_4 + x_3y_1 + x_4y_2 + x_5y_7 + x_6y_8 - x_7y_5 - x_8y_6)^2 + \\ & (x_1y_4 + x_2y_3 - x_3y_2 + x_4y_1 + x_5y_8 - x_6y_7 + x_7y_6 - x_8y_5)^2 + \\ & (x_1y_5 - x_2y_6 - x_3y_7 - x_4y_8 + x_5y_1 + x_6y_2 + x_7y_3 + x_8y_4)^2 + \\ & (x_1y_6 + x_2y_5 - x_3y_8 + x_4y_7 - x_5y_2 + x_6y_1 - x_7y_4 + x_8y_3)^2 + \\ & (x_1y_7 + x_2y_8 + x_3y_5 - x_4y_6 - x_5y_3 + x_6y_4 + x_7y_1 - x_8y_2)^2 + \\ & (x_1y_8 - x_2y_7 + x_3y_6 + x_4y_5 - x_5y_4 - x_6y_3 + x_7y_2 + x_8y_1)^2.\end{aligned}$$

Budući da se identiteti postižu za $n = 1 = 2^0$, $n = 2 = 2^1$, $n = 4 = 2^2$ i $n = 8 = 2^3$, prirodno se pokušavao pronaći analogan identitet i za $n = 16 = 2^4$. Međutim, potraga je bila bezuspješna dugo vremena. Štoviše, Hurwitz je 1898. dokazao da identitet ovog tipa, na čijoj se desnoj strani nalazi suma kvadrata n bilinearnih polinoma u varijablama $x_1, \ldots, x_n, y_1, \ldots, y_n$, postoji jedino za $n \in \{1, 2, 4, 8\}$. Taj je njegov rezultat danas poznat kao Hurwitzov $(1, 2, 4, 8)$-teorem. Pfister je 1960. otkrio da identitet ovog tipa postoji i za $n = 16$, i općenitije za sve $n = 2^k, k \in \mathbb{N}_0$, ali uz drugačije pretpostavke na oblik desne strane identiteta koje ćemo vidjeti u nastavku (vidi Korolar 4.2.1).

Poglavlje 3

Hurwitzov (1,2,4,8)-teorem

3.1 Teorem

Teorem 3.1.1 (Hurwitzov $(1, 2, 4, 8)$-teorem)**.** *Neka je $n \in \mathbb{N}$. Pretpostavimo da postoje bilinearni polinomi $z_1, ..., z_n \in \mathbb{C}[x_1, ..., x_n, y_1, ..., y_n]$ takvi da vrijedi*

$$(x_1^2 + ... + x_n^2)(y_1^2 + ... + y_n^2) = z_1^2 + ... + z_n^2. \tag{3.1}$$

Tada je $n \in \{1, 2, 4, 8\}$.

Za dokaz ovog teorema u sljedećim dvama potpoglavljima ćemo pokazati dvije stvari:

1. Egzistencija bilinearnog identiteta oblika (3.1) povlači rješivost određenog sustava matričnih jednadžbi.
2. Spomenuti sustav matričnih jednadžbi ima rješenje jedino za $n \in \{1, 2, 4, 8\}$ što ćemo dokazati koristeći metode linearne algebre.

3.2 Svođenje na sustav Hurwitzovih matričnih jednadžbi

Promotrimo identitet oblika (3.1). Za bilinearan polinom $z_k \in \mathbb{C}[x_1, ..., x_n, y_1, ..., y_n]$, pri čemu je $k \in \{1, ..., n\}$, vrijedi

$$z_k = \sum_{i=1}^{n} \sum_{j=1}^{n} a_{ijk} x_i y_j \tag{3.2}$$

za neke $a_{ijk} \in \mathbb{C}$.

Za ilustraciju, pogledajmo koji se bilinearni polinomi $z_1, ..., z_n$ pojavljuju u identitetima (2.1), (2.2), odnosno (2.3), koji su oblika (3.1) za $n = 1$, $n = 2$, odnosno $n = 4$.

Za $n = 1$ prema (2.1) vrijedi $x_1^2 y_1^2 = z_1^2$, pri čemu je $z_1 = x_1 y_1$.

Za $n = 2$ prema (2.2) identitet (3.1) zadovoljen je za

$$\begin{aligned} z_1 &= x_1 y_1 - x_2 y_2, \\ z_2 &= x_1 y_2 + x_2 y_1. \end{aligned} \tag{3.3}$$

Za $n = 4$ prema (2.3) identitet (3.1) zadovoljen je za

$$\begin{aligned} z_1 &= x_1 y_1 - x_2 y_2 - x_3 y_3 - x_4 y_4, \\ z_2 &= x_1 y_2 + x_2 y_1 + x_3 y_4 - x_4 y_3, \\ z_3 &= x_1 y_3 + x_3 y_1 - x_2 y_4 + x_4 y_2, \\ z_4 &= x_1 y_4 + x_4 y_1 + x_2 y_3 - x_3 y_2. \end{aligned} \tag{3.4}$$

Dobivene jednadžbe možemo zapisati pomoću matrica. U slučaju $n = 2$ imamo

$$\begin{pmatrix} z_1 \\ z_2 \end{pmatrix} = \begin{pmatrix} x_1 y_1 - x_2 y_2 \\ x_1 y_2 + x_2 y_1 \end{pmatrix} = \begin{pmatrix} x_1 & -x_2 \\ x_2 & x_1 \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = \left(x_1 \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + x_2 \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \right) \begin{pmatrix} y_1 \\ y_2 \end{pmatrix}$$

i slično u slučaju $n = 4$ imamo

$$\begin{pmatrix} z_1 \\ z_2 \\ z_3 \\ z_4 \end{pmatrix} = \left(x_1 A_1 + x_2 A_2 + x_3 A_3 + x_4 A_4 \right) \begin{pmatrix} y_1 \\ y_2 \\ y_3 \\ y_4 \end{pmatrix},$$

gdje su A_1, A_2, A_3, A_4 kvadratne matrice reda 4 oblika

$$A_1 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \; A_2 = \begin{pmatrix} 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \; A_3 = \begin{pmatrix} 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{pmatrix}, \; A_4 = \begin{pmatrix} 0 & 0 & 0 & -1 \\ 0 & 0 & -1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}.$$

Generalizacijom, jednadžbe (3.2) možemo zapisati pomoću kvadratnih matrica reda n.

Tada je sustav skalarnih jednadžbi (3.2) ekvivalentan matričnoj jednadžbi oblika

$$\begin{aligned}\begin{pmatrix} z_1 \\ . \\ . \\ . \\ z_n \end{pmatrix} &= \begin{pmatrix} \sum_{i,j} a_{ij1} x_i y_j \\ . \\ . \\ . \\ \sum_{i,j} a_{ijn} x_i y_j \end{pmatrix} \\ &= \begin{pmatrix} \sum_j (\sum_i a_{ij1} x_i) y_j \\ . \\ . \\ . \\ \sum_j (\sum_i a_{ijn} x_i) y_j \end{pmatrix} \\ &= \begin{pmatrix} \sum_i a_{i11} x_i & ... & \sum_i a_{in1} x_i \\ . & & . \\ . & & . \\ . & & . \\ \sum_i a_{i1n} x_i & ... & \sum_i a_{inn} x_i \end{pmatrix} \begin{pmatrix} y_1 \\ . \\ . \\ . \\ y_n \end{pmatrix}.\end{aligned} \tag{3.5}$$

Dobivenu kvadratnu matricu reda n možemo izraziti kao sumu n matrica u kojoj svaka matrica sadrži samo jedan x_i, koji se može izlučiti ispred matrice kao koeficijent, iz čega slijedi

$$\begin{pmatrix} z_1 \\ . \\ . \\ . \\ z_n \end{pmatrix} = x_1 \begin{pmatrix} a_{111} & ... & a_{1n1} \\ . & & . \\ . & & . \\ . & & . \\ a_{11n} & ... & a_{1nn} \end{pmatrix} + ... + x_n \begin{pmatrix} a_{n11} & ... & a_{nn1} \\ . & & . \\ . & & . \\ . & & . \\ a_{n1n} & ... & a_{nnn} \end{pmatrix}.$$

Nadalje, sumu na desnoj strani jednakosti možemo zapisati kao $x_1A_1 + ... + x_nA_n$ gdje se svaki element a_{ikj} kvadratne matrice A_i reda n nalazi na presjeku j-tog retka i k-tog stupca. Sada (3.5) glasi kao

$$z = (x_1A_1 + ... + x_nA_n)y = A_x y,$$

pri čemu smo stavili da je $A_x = x_1A_1 + ... + x_nA_n$ i uređenu n-torku $z = (z_1, ..., z_n)$ identificirali s vektor-stupcem $\begin{pmatrix} z_1 \\ . \\ . \\ . \\ z_n \end{pmatrix}$.

Promotrimo sada identitet (3.1), koji glasi $(x_1^2 + ... + x_n^2)(y_1^2 + ... + y_n^2) = z_1^2 + ... + z_n^2$.

Desna strana jednakosti jednaka je $z_1^2 + ... + z_n^2 = z \cdot z$, gdje je $\cdot$ produkt

$$(a_1, ..., a_n) \cdot (b_1, ..., b_n) = \sum_{k=1}^{n} a_k b_k$$

na $\mathbb{C}^n$. Prema tome vrijedi

$$z_1^2 + ... + z_n^2 = z \cdot z = A_x y \cdot A_x y = (A_x^\top A_x y) \cdot y.$$

Lijeva strana jednakosti jednaka je

$$(x_1^2 + ... + x_n^2)(y_1^2 + ... + y_n^2) = \left(\sum_{i=1}^{n} x_i^2\right) y \cdot y = \left(\left(\sum_{i=1}^{n} x_i^2\right) y\right) \cdot y.$$

Identitet (3.1) je sada ekvivalentan s

$$(A_x^\top A_x y) \cdot y = \left(\left(\sum_{i=1}^{n} x_i^2\right) y\right) \cdot y.$$

Uspoređivanjem dobivamo

$$A_x^\top A_x = \left(\sum_{i=1}^{n} x_i^2\right) I_n. \tag{3.6}$$

Raspisivanjem lijeve strane koristeći $A_x = x_1 A_1 + ... + x_n A_n$ dobivamo

$$A_x^\top A_x = \sum_{i=1}^{n} \left(A_i^\top A_i\right) x_i^2 + \sum_{1 \le i < j \le n} \left(A_i^\top A_j + A_j^\top A_i\right) x_i x_j.$$

Odavde slijedi da je izraz (3.6) ekvivalentan sustavu matričnih jednadžbi koje zovemo *Hurwitzove matrične jednadžbe*:

$$A_i^\top A_i = I_n, \quad A_i^\top A_j + A_j^\top A_i = 0, \quad i, j \in \{1, ..., n\}, \quad i \neq j. \tag{3.7}$$

3.3 Rješivost sustava Hurwitzovih matričnih jednadžbi

Preostaje nam još dokazati da sustav (3.7) matričnih jednadžbi reda n ima rješenje $(A_1, ..., A_n) \in M_n(\mathbb{C})^n$ jedino za $n \in \{1, 2, 4, 8\}$.

Bez smanjenja općenitosti, uzmimo da je $n > 2$. Normalizirajmo matrice A_i kako bismo jednu od njih učinili jediničnom matricom. Prema (3.7), A_i je invertibilna matrica s inverzom $A_i^\top$, dakle, A je ortogonalna matrica. Neka je $B_i = A_i A_n^\top$. Sada je sustav matričnih jednadžbi (3.7) ekvivalentan s

$$B_n = I_n, \quad B_i^\top B_i = I_n, \quad B_i^\top B_j + B_j^\top B_i = 0, \quad i, j \in \{1, ..., n\}. \tag{3.8}$$

Neka je u trećoj jednadžbi $j = n$. Tada je $B_i^\top = -B_i$ za $i \neq n$, dakle, za $i \neq n$ je B_i antisimetrična matrica. Stoga matrice $B_1, ..., B_{n-1}$ reda n zadovoljavaju

$$B_i^\top = -B_i, \quad B_i^2 = -I_n, \quad B_iB_j = -B_jB_i, \quad i, j \in \{1, ..., n-1\}. \tag{3.9}$$

Dokažimo sada jednu lemu koja će nam biti potrebna za daljnje zaključivanje.

Lema 3.3.1. *Neka je V konačnodimenzionalan vektorski prostor nad poljem $\mathbb{C}$. Ako postoji par invertibilnih antikomutativnih linearnih operatora na V, tada je* $\dim V$ *parna.*

Dokaz. Pretpostavimo da su $L, L' : V \to V$ par linearnih i invertibilnih operatora takvih da vrijedi

$$LL' = -L'L.$$

Djelovanjem determinante na obje strane dobivamo

$$(\det L)(\det L') = (-1)^{\dim V}(\det L')(\det L).$$

Budući da je $\det L \neq 0$ i $\det L' \neq 0$, dijeljenjem dobivamo da vrijedi

$$1 = (-1)^{\dim V}$$

čime je tvrdnja dokazana. □

Prema (3.9) i Lemi 3.3.1 slijedi da je, ako postoji rješenje sustava (3.7), n paran. U nastavku nam preostaje dokazati da, ako je $n > 2$ paran broj takav da sustav (3.9) ima rješenje, tada je $n = 4$ ili $n = 8$.

Dokažimo sada lemu o linearnoj nezavisnosti određenih matričnih produkata koja će nam biti potrebna u ovom završnom dijelu dokaza Teorema 3.1.1.

Lema 3.3.2. *Neka je m pozitivan paran cijeli broj i neka je d prirodan broj. Neka su $C_1, ..., C_m$ matrice u $M_d(\mathbb{C})$ za koje vrijedi da su u parovima antikomutativne i da je za svaki $i \in \{1, ..., m\}$ C_i^2 skalarna matrica različita od nulmatrice. Za svaki $\delta = (\delta_1, \ldots, \delta_m) \in \{0, 1\}^m$ definiramo matricu*

$$C^\delta := C_1^{\delta_1} \cdots C_m^{\delta_m}.$$

Tada je skup $\{C^\delta : \delta \in \{0, 1\}^m\}$ linearno nezavisan skup od 2^m elemenata u $M_d(\mathbb{C})$. Posebno, vrijedi $2^m \leq d^2$.

Dokaz. Uočimo da je C_i jednak C^δ za $\delta_i = 1$ i $\delta_j = 0$, $j \in \{1, ..., m\}$, $j \neq i$. Nadalje, broj različitih $\delta \in \{0, 1\}^m$ je 2^m. Pretpostavimo da postoji netrivijalna linearna relacija

$$\sum_\delta b_\delta C^\delta = 0, \tag{3.10}$$

gdje za koeficijente b_δ vrijedi da su iz $\mathbb{C}$ i da je barem jedan od njih različit od 0. Fiksirajmo takvu relaciju u kojoj je broj koeficijenata b_δ različitih od 0 najmanji moguć. Dokažimo da pritom možemo pretpostaviti da je $b_0 \neq 0$.

Budući da su matrice oblika C_i u parovima antikomutativne, a matrice C_i^2 su skalarne matrice različite od 0, za definirane matrice C^δ vrijedi da je $C^{\delta'}C^{\delta'}$ skalarna matrica različita od 0 za svaki δ'. Štoviše, za fiksan δ' vrijedi

$$\{C^\delta C^{\delta'} : \delta \in \{0,1\}^m\} = \{c_\delta C^\delta : \delta \in \{0,1\}^m\}$$

za neke $c_\delta \in \mathbb{C} \setminus \{0\}$ (koji ovise o δ'). Stoga, za δ' za koji je $b_{\delta'} \neq 0$, u relaciji (3.10) množenjem zdesna s $C^{\delta'}$ dobivamo linearnu relaciju s istim brojem koeficijenata koji su različiti od 0 kao i u (3.10), pri čemu je sada koeficijent uz $C^0 = I_d$ različit od 0.

Ovo pokazuje da možemo fiksirati netrivijalnu linearnu relaciju (3.10) u kojoj je broj koeficijenata b_δ različitih od 0 najmanji moguć i vrijedi $b_0 \neq 0$. U nastavku fiksirajmo takvu relaciju (3.10). Primjenom konjugiranja dokažimo da je većina izraza u (3.10) jednaka 0.

Zbog antikomutativnosti vrijedi

$$C_i C_j C_i^{-1} = \begin{cases} C_j, & i = j \\ -C_j, & i \neq j. \end{cases}$$

Stoga je

$$C_i C^\delta C_i^{-1} = \pm C^\delta. \tag{3.11}$$

Predznak $\pm$ ovisi o broju koordinata u δ koji su jednaki 1. Neka je za $\delta \in \{0,1\}^m$ taj broj koordinata j za koje je $\delta_j = 1$ jednak $w(\delta)$. Na primjer, $w(0) = 0$. Primjenom toga, za (3.11) sada vrijedi

$$C_i C^\delta C_i^{-1} = \varepsilon_{\delta,i} C^\delta, \tag{3.12}$$

pri čemu je

$$\varepsilon_{\delta,i} = \begin{cases} (-1)^{w(\delta)}, & \delta_i = 0 \\ (-1)^{w(\delta)-1}, & \delta_i = 1. \end{cases} \tag{3.13}$$

Na primjer, $\varepsilon_{0,i} = 1$ za svaki i. Odaberimo jedan $i \in \{1, ..., n\}$ te konjugirajmo linearnu relaciju (3.10) s C_i. Time dobivamo

$$\sum_\delta \varepsilon_{\delta,i} b_\delta C^\delta = 0. \tag{3.14}$$

Oduzimanjem (3.14) od (3.10) dobivamo linearnu relaciju

$$\sum_\delta (1 - \varepsilon_{\delta,i}) b_\delta C^\delta = 0. \tag{3.15}$$

Budući da je $\varepsilon_{0,i} = 1$, u ovoj je linearnoj relaciji koeficijent uz C^0 jednak 0. Stoga je (3.15) linearna relacija koja ima nekoliko izraza koji su različiti od 0 manje nego minimalna linearna relacija (3.10). Zbog toga su svi koeficijenti u (3.15) jednaki 0, to jest

$$\delta \neq 0,\ b_\delta \neq 0 \Rightarrow \varepsilon_{\delta,i} = 1.$$

To vrijedi za svaki $i \in \{1, ..., n\}$ pa svaki $\delta \neq 0$ s koeficijentima različitima od 0 u (3.10) ima predznak $\varepsilon_{\delta,i}$ neovisan o i. Tada je δ_i neovisna o i po (3.13) pa je $\delta = (1, ..., 1)$. Nadalje, vrijedi da je $w(\delta) = m$ pa iz toga slijedi

$$\varepsilon_{\delta,i} = (-1)^{m-1} = -1$$

budući da je m pozitivan paran broj. Time smo dobili kontradikciju jer je $-1 \neq 1$.

Dakle, pokazali smo da je $b_\delta = 0$ za $\delta \neq 0$, ali tada linearna relacija (3.10) ima samo jedan koeficijent koji je različit od 0, što je nemoguće. Time je tvrdnja dokazana. □

Pretpostavimo sada da za neki paran $n > 2$ postoje matrice $B_1, ..., B_{n-1}$ koje zadovoljavaju (3.9). Matrice $B_1, \ldots, B_{n-2} \in M_n(\mathbb{C})$ su u parovima antikomutativne i za svaki $i \in \{1, ..., n-2\}$ je B_i^2 skalarna matrica različita od nulmatrice zbog $B_i^2 = -I_n$. Ovdje smo izostavili $B_n = I_n$ jer B_n ne antikomutira s ostalim matricama oblika B_i i izostavili smo B_{n-1} jer trebamo paran broj u parovima antikomutativnih matrica, a $n-1$ je neparan budući da je po našoj pretpostavci n paran.

Primjenom Leme 3.3.2 na matrice $B_1, ..., B_{n-2}$ zaključujemo da je $2^{n-2} \leq n^2$. Za parne $n > 2$, dobivena nejednakost vrijedi samo za $n \in \{4, 6, 8\}$. Mogućnost $n = 6$ ćemo eliminirati proučavanjem svojstvenih potprostora za B_1. U nastavku ćemo dokazati da je $\frac{n}{2}$ paran kada je $n > 4$ iz čega slijedi $n \neq 6$.

Promotrimo matrice $B_1, ..., B_{n-1}$ kao linearne operatore na $\mathbb{C}^n$. Budući da za svaki $j \in \{1, ..., n-1\}$ vrijedi $B_j^2 = -I_n$, jedine svojstvene vrijednosti za B_j su $\pm i$. Neka su U i W dva svojstvena potprostora od B_1:

$$U = \{v \in \mathbb{C}^n : B_1 v = iv\}, \quad W = \{v \in \mathbb{C}^n : B_1 v = -iv\}.$$

Za svaki $v \in \mathbb{C}^n$, rastav

$$v = \frac{v - iB_1 v}{2} + \frac{v + iB_1 v}{2}$$

sadrži prvi pribrojnik iz svojstvenog potprostora U i drugi pribrojnik iz svojstvenog potprostora W. Prema tome, $\mathbb{C}^n = U + W$. Budući da su U i W svojstveni potprostori od B_1 za različite svojstvene vrijednosti, vrijedi $U \cap W = \{0\}$. Stoga je $\mathbb{C}^n = U \oplus W$ iz čega slijedi

$n = \dim U + \dim W$. Cilj je pokazati da svojstveni prostori U i W imaju jednake dimenzije.

Budući da je B_j invertibilan za svaki j, iz toga slijedi

$$\dim U = \dim B_j(U), \quad \dim W = \dim B_j(W).$$

Također, vrijedi $B_1(U) \subset U$ i $B_1(W) \subset W$. Za $j = 2, 3, ..., n-1$ želimo dobiti $B_j(U) \subset W$ i $B_j(W) \subset U$. Da bismo to pokazali, uzmimo $u \in U$. Zbog antikomutativnosti imamo

$$B_1(B_j u) = -B_j(B_1 u) = -B_j(iu) = -iB_j u$$

pa je $B_j u \in W$ iz čega slijedi $B_j(U) \subset W$. Analogno vrijedi $B_j(W) \subset U$. Stoga je

$$\dim U = \dim B_j(U) \leq \dim W, \quad \dim W = \dim B_j(W) \leq \dim U$$

pa je $\dim U = \dim W$. Nadalje, zbog rastava $\mathbb{C}^n = U \oplus W$ slijedi $\dim U = \dim W = \frac{n}{2}$.

Za $j = 2, 3, ..., n-1$, kompozicija $L_j = B_2 \circ B_j$ je invertibilan linearan operator na $\mathbb{C}^n$ i vrijedi $L_j(U) = B_2(B_j(U)) \subset B_2(W) \subset U$ pa je $L_j(U) \subset U$. Za $n > 4$, račun pomoću (3.9) pokazuje da su L_3 i L_4 antikomutativni na $\mathbb{C}^n$:

$$L_3 L_4 = (B_2 B_3)(B_2 B_4) = -B_2^2 B_3 B_4 = B_3 B_4$$

i

$$L_4 L_3 = (B_2 B_4)(B_2 B_3) = -B_2^2 B_4 B_3 = B_4 B_3 = -B_3 B_4 = -L_3 L_4.$$

Analogno se pokaže da su L_j i L_k antikomutativni za bilo koje različite $j, k > 2$. Gledajući L_3 i L_4 kao linearne operatore ne na $\mathbb{C}^n$, nego na vektorskom prostoru U, zbog njihove antikomutativnosti na U vrijedi da je $\dim U = \frac{n}{2}$ parna prema Lemi 3.3.1, stoga n mora biti višekratnik od 4.

Time smo eliminirali mogućnost da je $n = 6$ pa je stoga dokaz Teorema 3.1.1 završen.

Spomenimo sada da rezultat o linearnoj nezavisnosti iz Leme 3.3.2 vrijedi i uz slabiju pretpostavku iako je dokaz malo kompliciraniji. Naime, za skalarne matrice $C_i, i \in \{1, ..., m\}$ različite od 0 dovoljno je da budu invertibilne, ali dokaz je kompliciraniji jer u tom slučaju ne možemo pretpostaviti da je $b_0 \neq 0$. Rezultat ovog tipa dan je sljedećim teoremom.

Teorem 3.3.3. *Neka je $\mathbb{F}$ polje i neka je A prsten s jedinicom čiji centar sadrži $\mathbb{F}$. Pretpostavimo da su $a_1, ..., a_m$ u parovima antikomutativni invertibilni elementi iz A, pri čemu je m paran broj. Za svaki $\delta \in \{0,1\}^m$ definiramo*

$$a^\delta := a_1^\delta \cdots a_m^\delta.$$

Tada je skup $\{a^\delta : \delta \in \{0,1\}^m\}$ linearno nezavisan skup od 2^m elemenata nad poljem $\mathbb{F}$.

Dokaz. Uočimo da je Lema 3.3.2 poseban slučaj ovog teorema za $A = M_d(\mathbb{C})$ i $a_i = C_i$. Neka je $w(\delta)$ broj koordinata i za koje je $\delta_i = 1$. Tada je

$$a_i a_j a_i^{-1} = \begin{cases} a_j, & i = j \\ -a_j, & i \neq j \end{cases}$$

pa vrijedi

$$a_i a^\delta a_i^{-1} = \varepsilon_{\delta,i} a^\delta, \tag{3.16}$$

pri čemu je

$$\varepsilon_{\delta,i} = \begin{cases} (-1)^{w(\delta)}, & \delta_i = 0 \\ (-1)^{w(\delta)-1}, & \delta_i = 1. \end{cases}$$

Budući da je $w(\delta)$ broj koordinata i za koje je $\delta_i = 1$, dobivamo globalno ograničenje za koeficijente $\varepsilon_{\delta,1}, ..., \varepsilon_{\delta,m}$ uzimajući u obzir parnost broja m:

$$\prod_{i=1}^{m} \varepsilon_{\delta,i} = (-1)^{mw(\delta)}(-1)^{w(\delta)} = (-1)^{w(\delta)}. \tag{3.17}$$

Pretpostavimo da postoji netrivijalna linearna relacija

$$\sum_\delta b_\delta a^\delta = 0, \tag{3.18}$$

gdje za koeficijente b_δ vrijedi da su iz $\mathbb{F}$ i da je barem jedan od njih različit od 0. Fiksirajmo takvu relaciju u kojoj je broj koeficijenata b_δ različitih od 0 najmanji moguć. Nadalje, fiksirajmo $i \in \{1, ..., m\}$ i konjugirajmo linearnu relaciju (3.18) s a_i. Prema (3.16) vrijedi

$$\sum_\delta \varepsilon_{\delta,i} b_\delta a^\delta = 0.$$

Zbrajanjem i oduzimanjem prethodne jednakosti od (3.18) dobivamo

$$\sum_\delta (1 - \varepsilon_{\delta,i}) b_\delta a^\delta = 0, \quad \sum_\delta (1 + \varepsilon_{\delta,i}) b_\delta a^\delta = 0. \tag{3.19}$$

Pretpostavimo da za δ' vrijedi $b_{\delta'} \neq 0$. Tada jedna linearna relacija iz (3.19) nema δ'-član pa ima barem jedan nenulkoeficijent manje nego minimalna linearna relacija (3.18). Zbog toga su svi koeficijenti u toj relaciji jednaki 0. Dakle, za svaki δ za koji je $b_\delta \neq 0$ vrijedi $1 \pm \varepsilon_{\delta,i} = 0$, pri čemu uzimamo $-$ ako je $\varepsilon_{\delta',i} = 1$, a $+$ ako je $\varepsilon_{\delta',i} = -1$. Drugim riječima,

$$b_\delta \neq 0 \Rightarrow \varepsilon_{\delta,i} = \varepsilon_{\delta',i},$$

za svaki $i \in \{1, ..., n\}$. Stoga, množenjem po svakom i u (3.17) dobivamo da je $(-1)^{w(\delta)} = (-1)^{w(\delta')}$ za svaki δ za koji vrijedi $b_\delta \neq 0$. Prema tome, za $b_\delta \neq 0$ imamo

$$\delta_i = 0 \Rightarrow \varepsilon_{\delta,i} = (-1)^{w(\delta')}. \tag{3.20}$$

Budući da je $\varepsilon_{\delta,i} = \varepsilon_{\delta',i}$ za $b_\delta \neq 0$, tada (3.20) možemo zapisati kao

$$\delta_i = 0 \Rightarrow \varepsilon_{\delta',i} = (-1)^{w(\delta')}$$

kada je $b_\delta \neq 0$. Stoga, kada je $b_\delta \neq 0$, imamo

$$\delta_i = 0 \Rightarrow \delta'_i = 0.$$

Na sličan način

$$\delta_i = 1 \Rightarrow \delta'_i = 1$$

pa zapravo vrijedi $\delta = \delta'$. Time smo dobili da minimalna netrivijalna linearna relacija (3.18) ima samo jedan koeficijent uz a^δ različit od 0. Ali iz toga slijedi da je $b'_\delta a^{\delta'} = 0$, što je nemoguće. Time je tvrdnja dokazana. □

3.4 Primjena

U ovom ćemo potpoglavlju opisati primjenu Hurwitzovog (1,2,4,8)-teorema na problem egzistencije vektorskog produkta na $\mathbb{R}^n$. Naime, postavlja se pitanje može li se konstruirati vektorski produkt na $\mathbb{R}^n$ analogan onome na $\mathbb{R}^3$ za bilo koji $n > 3$. Proučavanjem nekih prirodnih svojstava koja bi takav vektorski produkt trebao imati, pomoću Hurwitzovog (1,2,4,8)-teorema ćemo dokazati da je odgovor na traženo pitanje zapravo dosta ograničen.

Prisjetimo se najprije definicije standardnog skalarnog produkta na $\mathbb{R}^n$ i standardne norme na $\mathbb{R}^n$.

Definicija 3.4.1. *Standardni skalarni produkt na $\mathbb{R}^n$ je preslikavanje $\cdot : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}$ definirano formulom*

$$x \cdot y = \sum_{i=1}^{n} x_i y_i$$

za $x = (x_1, ..., x_n), y = (y_1, ..., y_n) \in \mathbb{R}^n$.

Definicija 3.4.2. *Standardna norma na $\mathbb{R}^n$ je preslikavanje $\|\cdot\| : \mathbb{R}^n \to \mathbb{R}$ definirano formulom*

$$\|x\| = \sqrt{x \cdot x} = \sqrt{\sum_{i=1}^{n} x_i^2}$$

za $x = (x_1, ..., x_n) \in \mathbb{R}^n$.

Motivirani osnovnim svojstvima standardnog vektorskog produkta na $\mathbb{R}^3$ (Teorem 1.1.19), definirajmo pojam vektorskog produkta na $\mathbb{R}^n$, a potom dokažimo za koje $n \in \mathbb{N}$ takav vektorski produkt postoji.

Definicija 3.4.3. *Neka je $n \in \mathbb{N}$. Vektorski produkt na $\mathbb{R}^n$ je preslikavanje $\times : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}^n$ sa svojstvima da za sve vektore v, v_1, v_2, w, w_1, $w_2 \in \mathbb{R}^n$ i $c \in \mathbb{R}$ vrijedi:*

1. $(v_1 + v_2) \times w = v_1 \times w + v_2 \times w, \quad v \times (w_1 + w_2) = v \times w_1 + v \times w_2$
   (distributivnost prema zbrajanju)
2. $c(v \times w) = (cv) \times w = v \times (cw)$ *(kvaziasocijativnost)*
3. $v \cdot (v \times w) = 0, \quad w \cdot (v \times w) = 0$ *(okomitost)*
4. $\|v \times w\|^2 = \|v\|^2 \|w\|^2 - (v \cdot w)^2$ *(Pitagorino svojstvo).*

Napomena 3.4.4. *Svojstva distributivnosti prema zbrajanju i kvaziasocijativnosti zajedno se nazivaju svojstvom bilinearnosti.*

Dokažimo sada teorem koji će nam dati odgovor na problem postavljen u uvodnom dijelu ovog potpoglavlja. Naime, vektorski produkt na $\mathbb{R}^n$ postoji samo ako je prirodan broj $n \in \{1, 3, 7\}$.

Teorem 3.4.5. *Neka je $n \in \mathbb{N}$ takav da postoji vektorski produkt na $\mathbb{R}^n$. Tada je $n \in \{1, 3, 7\}$.*

Dokaz. Dokazat ćemo da postojanje vektorskog produkta na $\mathbb{R}^n$ povlači postojanje bilinearne operacije s posebnim svojstvima na $\mathbb{R}^{n+1}$. Preciznije, vektorski produkt $\times$ na $\mathbb{R}^n$ iskoristit ćemo kako bismo definirali produkt $\odot$ na $\mathbb{R}^{n+1}$. Vektorski prostor $\mathbb{R}^{n+1}$ pritom gledamo kao direktnu sumu od $\mathbb{R}$ i $\mathbb{R}^n$ pa vrijedi da je $\mathbb{R}^{n+1} = \mathbb{R} \oplus \mathbb{R}^n$. Dakle, vektori iz $\mathbb{R}^{n+1}$ su zapravo uređeni parovi (x, v) pri čemu je $x \in \mathbb{R}$ i $v \in \mathbb{R}^n$.

Neka je, dakle, $n \in \mathbb{N}$ takav da postoji vektorski produkt $\times$ na $\mathbb{R}^n$. Definiramo binarnu operaciju $\odot : \mathbb{R}^{n+1} \times \mathbb{R}^{n+1} \to \mathbb{R}^{n+1}$ na sljedeći način: za vektore (x, v) i (y, w) iz $\mathbb{R}^{n+1}$ definiramo

$$(x, v) \odot (y, w) := (xy - v \cdot w, xw + yv + v \times w). \tag{3.21}$$

Množenje (3.21) je dobro definirano jer vrijedi da je $xy - v \cdot w \in \mathbb{R}$ i $xw + yv + v \times w \in \mathbb{R}^n$. Nadalje, tako definirano množenje $\odot$ ima dva svojstva.

Prvo svojstvo je bilinearnost u (x, v) i (y, w) (ako fiksiramo jedan takav uređeni par iz $\mathbb{R}^{n+1}$, onda je desna strana od (3.21) linearna funkcija drugog uređenog para).

Drugo svojstvo je

$$\|(x, v) \odot (y, w)\|^2 = \|(x, v)\|^2 \|(y, w)\|^2. \tag{3.22}$$

Dokažimo svojstvo (3.22). Proširivanjem lijeve strane dobivamo

$$\begin{aligned}\|(x, v) \odot (y, w)\|^2 &= (xy - v \cdot w, xw + yv + v \times w) \cdot (xy - v \cdot w, xw + yv + v \times w) \\ &= (xy - v \cdot w)^2 + (xw + yv + v \times w) \cdot (xw + yv + v \times w) \\ &= (xy - v \cdot w)^2 + (xw + yv) \cdot (xw + yv) + 2(xw + yv) \cdot (v \times w) + (v \times w) \cdot (v \times w).\end{aligned}$$

Koristeći svojstvo okomitosti (3) iz Definicije 3.4.3, vidimo da je $v \times w$ okomit na $xw + yv$, to jest vrijedi $(xw + yv) \cdot (v \times w) = 0$. Stoga je

$$\begin{aligned}(xw + yv + v \times w) \cdot (xw + yv + v \times w) &= (xw + yv) \cdot (xw + yv) + (v \times w) \cdot (v \times w) \\ &= x^2\|w\|^2 + 2xy(v \cdot w) + y^2\|v\|^2 + \|v \times w\|^2.\end{aligned}$$

Također, vrijedi $(xy - v \cdot w)^2 = x^2y^2 - 2xy(v \cdot w) + (v \cdot w)^2$. Primjenom dobivenih jednakosti i koristeći Pitagorino svojstvo (4) iz Definicije 3.4.3 dobivamo

$$\begin{aligned}\|(x, v) \odot (y, w)\|^2 &= (xy - v \cdot w)^2 + (xw + yv + v \times w) \cdot (xw + yv + v \times w) \\ &= x^2y^2 - 2xy(v \cdot w) + (v \cdot w)^2 + x^2\|w\|^2 + 2xy(v \cdot w) + y^2\|v\|^2 + \|v \times w\|^2 \\ &= x^2y^2 + x^2\|w\|^2 + y^2\|v\|^2 + \|v\|^2\|w\|^2 \\ &= (x^2 + \|v\|^2)(y^2 + \|w\|^2) \\ &= \|(x, v)\|^2\|(y, w)\|^2.\end{aligned}$$

Time je dokazano drugo svojstvo (3.22). Preostaje nam pokazati poveznicu između operacije množenja $\odot$ i Hurwitzovog (1,2,4,8)-teorema.

Uzmimo dva vektora $(x_1, ..., x_{n+1}), (y_1, ..., y_{n+1}) \in \mathbb{R}^{n+1}$. Njihov umnožak $\odot$ je treći vektor $(z_1, ..., z_{n+1})$, pri čemu su koordinate određene formulom (3.21). Uvrštavanjem tih vektora u (3.22) i zamjenom strana dobivamo

$$(x_1^2 + ... + x_{n+1}^2)(y_1^2 + ... + y_{n+1}^2) = z_1^2 + ... + z_{n+1}^2. \tag{3.23}$$

Ovaj identitet vrijedi za sve realne vrijednosti varijabli $x_1, \ldots, x_n, y_1, \ldots, y_n$. Nadalje, iz gore spomenute bilinearnosti množenja $\odot$ slijedi da je za svaki $k \in \{1, \ldots, n\}$ z_k bilinearan polinom u varijablama x_i i y_j.

Po Napomeni 1.5.8 slijedi da (3.23) možemo shvatiti kao identitet oblika (3.1) u $\mathbb{R}[x_1, \ldots, x_{n+1}, y_1, \ldots, y_{n+1}] \subseteq \mathbb{C}[x_1, \ldots, x_{n+1}, y_1, \ldots, y_{n+1}]$. Prema tome, po Hurwitzovom (1,2,4,8)-teoremu (Teorem 3.1.1) slijedi da je $n + 1 \in \{1, 2, 4, 8\}$ pa je $n \in \{0, 1, 3, 7\}$. Prema pretpostavci teorema odbacujemo slučaj kada je $n = 0$ i time je dokaz završen. □

Za $n = 1$, vektorski produkt na $\mathbb{R}^n = \mathbb{R}$ koji zadovoljava Pitagorino svojstvo (4) iz Definicije 3.4.3 jednak je 0. Zaista, skalarni produkt na $\mathbb{R}$ jednak je klasičnom produktu pa iz svojstva (4) slijedi $|x \times y|^2 = x^2y^2 - (xy)^2 = 0$, odnosno $x \times y = 0$. Stoga promotrimo slučaj kada je $n > 1$, odnosno $n \in \{3, 7\}$. U Definiciji 1.1.18 prikazana je konkretna formula za neki vektorski produkt na $\mathbb{R}^3$ pa pokažimo još kako izgleda konkretna formula za neki vektorski produkt na $\mathbb{R}^7$.

Za vektore $a = (a_1, a_2, a_3, a_4, a_5, a_6, a_7)$, $b = (b_1, b_2, b_3, b_4, b_5, b_6, b_7) \in \mathbb{R}^7$ njihov vektorski produkt možemo definirati na sljedeći način:

$$\begin{aligned} a \times b =& (-a_3b_2 + a_2b_3 - a_5b_4 + a_4b_5 - a_6b_7 + a_7b_6)e_1 + \\ & (-a_1b_3 + a_3b_1 - a_6b_4 + a_4b_6 - a_7b_5 + a_5b_7)e_2 + \\ & (-a_2b_1 + a_1b_2 - a_7b_4 + a_4b_7 - a_5b_6 + a_6b_5)e_3 + \\ & (-a_1b_5 + a_5b_1 - a_2b_6 + a_6b_2 - a_3b_7 + a_7b_3)e_4 + \\ & (-a_4b_1 + a_1b_4 - a_2b_7 + a_7b_2 - a_6b_3 + a_3b_6)e_5 + \\ & (-a_7b_1 + a_1b_7 - a_4b_2 + a_2b_4 - a_3b_5 + a_5b_3)e_6 + \\ & (-a_5b_2 + a_2b_5 - a_4b_3 + a_3b_4 - a_1b_6 + a_6b_1)e_7, \end{aligned}$$

pri čemu je skup $\{e_1, e_2, e_3, e_4, e_5, e_6, e_7\}$ kanonska baza za $\mathbb{R}^7$.

Poglavlje 4

Pfisterov teorem o sumama kvadrata

4.1 Teorem

Teorem 4.1.1. *(Pfisterov teorem o sumama kvadrata). Neka je $\mathbb{F}$ polje i neka je $n = 2^k$ za neki $k \in \mathbb{N}_0$. Neka su $x_1, ..., x_n, y_1, ..., y_n \in \mathbb{F}$. Tada je*

$$(x_1^2 + ... + x_n^2)(y_1^2 + ... + y_n^2) = z_1^2 + ... + z_n^2$$

za neke $z_1, ..., z_n \in \mathbb{F}$. Drugim riječima, skup suma n kvadrata u $\mathbb{F}$ zatvoren je na množenje.

Za dokaz ovog teorema ključna je lema koju ćemo dokazati u nastavku.

Lema 4.1.2. *Neka je $\mathbb{F}$ polje i neka je $k \in \mathbb{N}_0$. Pretpostavimo da za $n = 2^k$ i $c, c_1, \ldots, c_n \in \mathbb{F}$ vrijedi $c = c_1^2 + ... + c_n^2$. Tada postoji $n \times n$ matrica C s elementima iz polja $\mathbb{F}$ i prvim retkom $(c_1, ..., c_n)$ za koju vrijedi $CC^\top = C^\top C = cI_n$.*

Dokaz. Dokažimo ovu lemu matematičkom indukcijom po k.
Slučaj kada je $k = 0$ je trivijalan. U slučaju kada je $k = 1$ želimo pronaći $u, v \in \mathbb{F}$ za koje 2×2 matrica $C = \begin{pmatrix} c_1 & c_2 \\ u & v \end{pmatrix}$ zadovoljava

$$CC^\top = C^\top C = \begin{pmatrix} c_1^2 + c_2^2 & 0 \\ 0 & c_1^2 + c_2^2 \end{pmatrix}.$$

Za $CC^\top$ vrijedi

$$CC^\top = \begin{pmatrix} c_1 & c_2 \\ u & v \end{pmatrix}\begin{pmatrix} c_1 & u \\ c_2 & v \end{pmatrix} = \begin{pmatrix} c_1^2 + c_2^2 & c_1u + c_2v \\ c_1u + c_2v & u^2 + v^2 \end{pmatrix}.$$

Neka je $u = c_2$ i $v = -c_1$ (ili $u = -c_2$ i $v = c_1$). Tada je $CC^\top = cI_2$. Analogno vrijedi da je $C^\top C = cI_2$.

Pretpostavimo sada da je $k \geq 2$ i da tvrdnja vrijedi za $k-1$. Stavljanjem $a = c_1^2 + ... + c_{\frac{n}{2}}^2$ i $b = c_{\frac{n}{2}+1}^2 + ... + c_n^2$, pri čemu su a i b sume nastale zbrajanjem $\frac{n}{2}$ kvadrata, dobivamo da je $c = a + b$. Prema pretpostavci indukcije postoje $2^{k-1} \times 2^{k-1}$ matrice A odnosno B s elementima iz polja $\mathbb{F}$ i prvim retkom $(c_1, ..., c_{\frac{n}{2}})$ odnosno $(c_{\frac{n}{2}+1}, ..., c_n)$ za koje vrijedi

$$AA^\top = A^\top A = aI_{\frac{n}{2}}, \quad BB^\top = B^\top B = bI_{\frac{n}{2}}.$$

Mi želimo pokazati da postoji $2^k \times 2^k$ matrica C za koju vrijedi $CC^\top = C^\top C = cI_n = (a+b)I_n$. Generalizacijom slučaja kada je $k = 1$, pokušajmo pronaći takvu matricu C oblika

$$C = \begin{pmatrix} A & B \\ U & V \end{pmatrix}$$

za neke $2^{k-1} \times 2^{k-1}$ matrice U i V s elementima iz polja $\mathbb{F}$.

Za $CC^\top$ vrijedi

$$\begin{aligned} CC^\top &= \begin{pmatrix} A & B \\ U & V \end{pmatrix}\begin{pmatrix} A^\top & U^\top \\ B^\top & V^\top \end{pmatrix} \\ &= \begin{pmatrix} AA^\top + BB^\top & AU^\top + BV^\top \\ UA^\top + VB^\top & UU^\top + VV^\top \end{pmatrix} \\ &= \begin{pmatrix} (a+b)I_{\frac{n}{2}} & AU^\top + BV^\top \\ UA^\top + VB^\top & UU^\top + VV^\top \end{pmatrix}. \end{aligned}$$

Nedijagonalni $n \times n$-blokovi ove matrice su međusobno transponirani pa vrijedi da je $CC^\top = cI_n$ ako su zadovoljeni uvjeti

$$AU^\top + BV^\top = 0, \quad UU^\top + VV^\top = cI_{\frac{n}{2}}. \tag{4.1}$$

Neka je sada $U = B$. Budući da je $BB^\top = bI_{\frac{n}{2}}$, slijedi da je, ako je $b \neq 0$, matrica B invertibilna pa iz prve jednakosti u (4.1) vrijedi

$$AB^\top + BV^\top = 0 \Leftrightarrow BV^\top = -AB^\top \Leftrightarrow V = (-B^{-1}AB^\top)^\top \Leftrightarrow V = -BA^\top(B^{-1})^\top.$$

Dakle, prva jednakost u (4.1) je zadovoljena ako i samo ako je $V = -BA^\top(B^{-1})^\top$. S obzirom da nije nužno $b \neq 0$, promotrimo dva slučaja: kada je $c \neq 0$ i kada je $c = 0$.

1° Neka je $c \neq 0$. Tada jednakost $c = a + b$ povlači da je barem jedna od polusuma a i b različita od 0 pa možemo pretpostaviti da je $b \neq 0$. U protivnom, u sljedećem argumentu zamijenimo uloge polusuma a i b (pa time i matrica A i B). Provjerimo vrijedi li za $U = B$

i $V = -BA^\top(B^{-1})^\top$ druga jednakost u (4.1):

$$\begin{aligned}
UU^\top + VV^\top &= BB^\top + (-BA^\top(B^{-1})^\top)((-BA^\top(B^{-1})^\top))^\top \\
&= bI_{\frac{n}{2}} + (-BA^\top(B^{-1})^\top)(-B^{-1}AB^\top) \\
&= bI_{\frac{n}{2}} + BA^\top(B^\top)^{-1}B^{-1}AB^\top \\
&= bI_{\frac{n}{2}} + BA^\top(BB^\top)^{-1}AB^\top \\
&= bI_{\frac{n}{2}} + BA^\top\left(bI_{\frac{n}{2}}\right)^{-1}AB^\top \\
&= bI_{\frac{n}{2}} + \frac{1}{b}BA^\top AB^\top \\
&= bI_{\frac{n}{2}} + \frac{1}{b}BaI_{\frac{n}{2}}B^\top \\
&= bI_{\frac{n}{2}} + \frac{a}{b}BB^\top \\
&= bI_{\frac{n}{2}} + \frac{a}{b}bI_{\frac{n}{2}} \\
&= bI_{\frac{n}{2}} + aI_{\frac{n}{2}} \\
&= cI_{\frac{n}{2}}.
\end{aligned}$$

Dakle, vrijedi da je $CC^\top = cI_n$. Budući da je $c \neq 0$, matrica C je invertibilna pa jednakost $C^\top C = cI_n$ slijedi direktno iz toga (matrica C i njezin inverz, u ovom slučaju je to $\frac{1}{c}C^\top$ jer je $CC^\top = cI_n \Leftrightarrow C^\top = C^{-1}cI_n \Leftrightarrow C^{-1} = \frac{1}{c}C^\top$, uvijek komutiraju). Stoga zaključujemo da postoji matrica C za koju vrijedi da je $CC^\top = C^\top C = cI_n$.

2° Neka je $c = 0$. U ovom je slučaju moguće da je $a = b = 0$. Primjerice, za $\mathbb{F} = \mathbb{C}$ i $k = 2$ možemo uzeti $c_1 = 1$, $c_2 = i$, $c_3 = 1$ i $c_4 = i$ pa rastav $c = c_1^2 + c_2^2 + c_3^2 + c_4^2$ iz leme glasi $0 = (1^2 + i^2) + (1^2 + i^2)$, dakle, $a = 1^2 + i^2 = 0$ i $b = 1^2 + i^2 = 0$. Međutim, u ovom primjeru možemo drugačije grupirati c_1^2, c_2^2, c_3^2 i c_4^2 u polusume $a, b \neq 0$.

Naime, vrijedi da je $0 = (1^2 + 1^2) + (i^2 + i^2)$ pa, ako stavimo $a = c_1^2 + c_3^2$ i $b = c_2^2 + c_4^2$, imamo da je $a \neq 0$ i $b \neq 0$. Općenito, ako je $0 = c_1^2 + ... + c_n^2$, tada ili pribrojnike $c_1^2, \ldots, c_n^2$ možemo razdijeliti u dvije polusume (tj. sume od po $\frac{n}{2}$ pribrojnika) $a, b \neq 0$ (primijetimo da je, budući da je $a + b = 0$, polusuma $a \neq 0$ ako i samo ako je $b \neq 0$) ili su elementi $c_1^2, ..., c_n^2$ jednaki.

Zaista, ako su sve polusume $a = b = 0$, tada je posebno $c_1^2 + \ldots + c_{\frac{n}{2}}^2 = 0$ i $c_1^2 + \ldots + c_{\frac{n}{2}-1}^2 + c_{\frac{n}{2}+1}^2 = 0$. Nakon oduzimanja slijedi da je $c_{\frac{n}{2}}^2 = c_{\frac{n}{2}+1}^2$. Sličnom argumentacijom dobivamo da za sve elemente oblika c_j^2 vrijedi da su jednaki.

Kada je $c = 0$ i postoje polusume $a, b \neq 0$, za U i V iz (4.1) analognim raspisivanjem dobijemo da vrijedi $CC^\top = cI_n$. Međutim, budući da sada matrica C nije invertibilna, jednakost $C^\top C = cI_n$ ne možemo direktno zaključiti pomoću $CC^\top = cI_n$, nego postupak moramo provesti opet analogno kao i za $CC^\top = cI_n$.

Za $C^\top C$ vrijedi

$$\begin{aligned} C^\top C &= \begin{pmatrix} A^\top & U^\top \\ B^\top & V^\top \end{pmatrix} \begin{pmatrix} A & B \\ U & V \end{pmatrix} \\ &= \begin{pmatrix} A^\top A + U^\top U & A^\top B + U^\top V \\ B^\top A + V^\top U & B^\top B + V^\top V \end{pmatrix}. \end{aligned}$$

Nedijagonalni $n \times n$ blokovi ove matrice su međusobno transponirani pa vrijedi da je $C^\top C = cI_n$ ako su zadovoljeni uvjeti

$$A^\top B + U^\top V = 0, \quad A^\top A + U^\top U = cI_{\frac{n}{2}}, \quad B^\top B + V^\top V = cI_{\frac{n}{2}}. \tag{4.2}$$

Neka je sada $U = B$. Tada za drugu jednakost u (4.2) vrijedi

$$A^\top A + U^\top U = A^\top A + B^\top B = (a + b)I_{\frac{n}{2}} = cI_{\frac{n}{2}}.$$

Budući da je $BB^\top = bI_{\frac{n}{2}}$ i $b \neq 0$, matrica B je invertibilna pa za prvu jednakost u (4.2) vrijedi

$$A^\top B + B^\top V = 0 \Leftrightarrow B^\top V = -A^\top B \Leftrightarrow V = -(B^\top)^{-1} A^\top B \Leftrightarrow V = -(B^{-1})^\top A^\top B.$$

Dakle, prva jednakost u (4.2) je zadovoljena ako i samo ako je $V = -(B^{-1})^\top A^\top B$. Provjerimo vrijedi li sada treća jednakost u (4.2):

$$\begin{aligned}
B^\top B + V^\top V &= B^\top B + (-(B^{-1})^\top A^\top B)^\top (-(B^{-1})^\top A^\top B) \\
&= bI_{\frac{n}{2}} + (-B^\top A B^{-1})(-(B^{-1})^\top A^\top B) \\
&= bI_{\frac{n}{2}} + B^\top A B^{-1} (B^\top)^{-1} A^\top B \\
&= bI_{\frac{n}{2}} + B^\top A (B^\top B)^{-1} A^\top B \\
&= bI_{\frac{n}{2}} + B^\top A \left(bI_{\frac{n}{2}}\right)^{-1} A^\top B \\
&= bI_{\frac{n}{2}} + \frac{1}{b} B^\top A A^\top B \\
&= bI_{\frac{n}{2}} + \frac{1}{b} B^\top a I_{\frac{n}{2}} B \\
&= bI_{\frac{n}{2}} + \frac{a}{b} B^\top B \\
&= bI_{\frac{n}{2}} + \frac{a}{b} bI_{\frac{n}{2}} \\
&= bI_{\frac{n}{2}} + aI_{\frac{n}{2}} \\
&= cI_{\frac{n}{2}}.
\end{aligned}$$

Dakle, vrijedi da je $C^\top C = cI_n$. Stoga zaključujemo da postoji matrica C za koju vrijedi da je $CC^\top = C^\top C = cI_n$.

Kada je $c = 0$ i kada za sve elemente oblika c_j^2 vrijedi da su jednaki, dobivamo da vrijedi $0 = c_1^2 + ... + c_n^2 = nc_1^2$. Prema pretpostavci leme vrijedi da je $n = 2^k$ pa kada polje $\mathbb{F}$ nije karakteristike 2, tada je $c_1 = 0$ (time je i svaki element oblika c_j jednak 0) te za matricu C možemo uzeti nulmatricu.

Kada je polje $\mathbb{F}$ karakteristike 2, neka je tada C matrica s redcima jednakim $(c_1, ..., c_n)$. Tada je svaki element od $CC^\top$ jednak $\sum_{j=1}^n c_j^2 = 0$ pa je $CC^\top = 0 = cI_n$. Element (i, j) matrice $C^\top C$ jednak je $nc_i c_j$. Budući da je n paran, to jest djeljiv s karakteristikom polja $\mathbb{F}$, taj element je jednak 0. Stoga vrijedi da je $C^\top C = 0 = cI_n$. Dakle, i u ovom slučaju postoji matrica C za koju vrijedi da je $CC^\top = C^\top C = cI_n$. □

Napomena 4.1.3. *Element* $(1, 1)$ *matrice* $CC^\top$ *u Lemi 4.1.2 je* $c_1^2 + ... + c_n^2 = c$ *i to će biti glavni dio dokaza Pfisterovog teorema.*

Dokažimo sada Pfisterov teorem (Teorem 4.1.1).

Dokaz Teorema 4.1.1. Pretpostavimo da se elementi $x, y \in \mathbb{F}$ mogu zapisati kao sume n kvadrata:

$$x = x_1^2 + ... + x_n^2, \quad y = y_1^2 + ... + y_n^2$$

za neke $x_1, \ldots, x_n, y_1, \ldots, y_n \in \mathbb{F}$. Po Lemi 4.1.2 postoje $n \times n$ matrice X i Y s elementima iz polja $\mathbb{F}$ za koje vrijedi

$$XX^\top = X^\top X = xI_n, \quad YY^\top = Y^\top Y = yI_n,$$

pri čemu je prvi redak matrice X jednak $(x_1, ..., x_n)$, a matrice Y jednak $(y_1, ..., y_n)$. Tada je

$$(XY)(XY)^\top = XYY^\top X^\top = yXX^\top = xyI_n.$$

Označimo prvi redak matrice XY sa $(z_1, ..., z_n)$. Tada za element matrice $(XY)(XY)^\top$ na mjestu $(1, 1)$ vrijedi

$$z_1^2 + ... + z_n^2 = xy = (x_1^2 + ... + x_n^2)(y_1^2 + ... + y_n^2).$$

Time je dokaz Teorema 4.1.1 završen. □

Pfister je također dokazao da postoji polje u kojem tvrdnja Teorema 4.1.1 ne vrijedi ni za koji $n \in \mathbb{N}$ koji nije potencija od 2. Taj teorem ćemo samo iskazati u nastavku, a dokaz se može pronaći u [2].

Teorem 4.1.4. *Neka je $\mathbb{R}(x_1, x_2, \ldots) = \bigcup_{n=1}^{\infty} \mathbb{R}(x_1, \ldots, x_n)$ polje racionalnih funkcija u beskonačno mnogo varijabli x_i, $i \in \mathbb{N}$. Za svaki pozitivan cijeli broj n koji nije potencija od 2, skup suma n kvadrata u $\mathbb{R}(x_1, x_2, \ldots)$ nije zatvoren na množenje.*

Postavlja se pitanje može li se Pfisterov teorem o sumama kvadrata poopćiti, to jest ostaje li istinit ako u njegovu iskazu zamijenimo uvjet da je $\mathbb{F}$ polje slabijim uvjetom da je $\mathbb{F}$ komutativan prsten. Sljedeći teorem će nam dati odgovor na to pitanje.

Teorem 4.1.5. *Neka je $n \in \mathbb{N}$ takav da je skup suma n kvadrata zatvoren na množenje u svakom komutativnom prstenu R. Tada je $n \in \{1, 2, 4, 8\}$.*

Dokaz. Dokažimo ovaj teorem koristeći konkretan komutativan prsten $A = \mathbb{R}[x_1, ..., x_n, y_1, ..., y_n]$. Neka je $u = x_1^2 + ... + x_n^2$ i $v = y_1^2 + ... + y_n^2$. Pretpostavljajući da je skup suma n kvadrata u A zatvoren na množenje, slijedi da je uv suma n kvadrata u A pa vrijedi identitet

$$(x_1^2 + ... + x_n^2)(y_1^2 + ... + y_n^2) = f_1^2 + ... + f_n^2 \tag{4.3}$$

za neke polinome $f_1, ..., f_n \in \mathbb{R}[x_1, ..., x_n, y_1, ..., y_n]$.

Želimo pokazati da su $f_1, ..., f_n$ bilinearni polinomi u varijablama x_i i y_j pa tvrdnja da je $n \in \{1, 2, 4, 8\}$ tada slijedi prema Hurwitzovom $(1, 2, 4, 8)$-teoremu (Teorem 3.1.1). Primijetimo najprije da evaluacijom jednakosti (4.3) u $(x_1, \ldots, x_n, y_1, \ldots, y_n) = (0, \ldots, 0)$ dobivamo da je suma kvadrata konstantnih članova polinoma $f_1, \ldots, f_n$ jednaka 0. Kako su

konstantni članovi polinoma $f_1, \ldots, f_n$ realni brojevi, slijedi da su svi oni jednaki 0.

Zapišimo polinome $f_1, ..., f_n$ kao sume homogenih polinoma u varijablama $x_1, ..., x_n$ s koeficijentima iz $\mathbb{R}[y_1, ..., y_n]$ i neka je d najveći stupanj takvih homogenih polinoma (dakle, $d \geq 1$). Neka je $f_{i,d}$ suma homogenih polinoma stupnja d u zapisu polinoma f_i, dakle, $f_{i,d} \neq 0$ za neki i.

Ako je $d > 1$, tada izjednačavanje homogenih polinoma u varijablama $x_1, \ldots, x_n$ stupnja $2d$ s obje strane jednakosti u (4.3) povlači $0 = \sum_{i=1}^{n} f_{i,d}^2$ pa je svaki $f_{i,d}$ jednak 0, što je kontradikcija. Slijedi da je $d = 1$ pa je svaki polinom f_i linearna kombinacija homogenih polinoma $x_1, ..., x_n$ s koeficijentima iz $\mathbb{R}[y_1, ..., y_n]$. Zbog simetrije, svaki polinom f_i je također linearna kombinacija homogenih polinoma $y_1, ..., y_n$ s koeficijentima iz $\mathbb{R}[x_1, ..., x_n]$.

Zaključujemo da je svaki f_i bilinearan polinom u varijablama x_i i y_j pa tvrdnja teorema slijedi prema Hurwitzovom $(1, 2, 4, 8)$-teoremu (Teorem 3.1.1). □

4.2 Primjena

U ovom potpoglavlju ćemo objasniti primjenu Pfisterovog teorema o sumama kvadrata u dokazivanju nekih tvrdnji. Prva primjena Pfisterovog teorema dat će nam novu informaciju o identitetima oblika

$$(x_1^2 + \ldots + x_n^2)(y_1^2 + \ldots + y_n^2) = z_1^2 + \ldots + z_n^2, \tag{4.4}$$

koji su glavna tema ovog rada. Preciznije, sljedeći korolar dokazuje da identitet oblika (4.4), u kojem su $z_1, \ldots, z_n$ racionalne funkcije u varijablama $x_1, \ldots, x_n, y_1, \ldots, y_n$ nad proizvoljnim unaprijed zadanim poljem $\mathbb{F}$, postoji kad god je n potencija od 2. Nakon toga, dokazat ćemo još jedan korolar za čiji je dokaz također potreban Pfisterov teorem.

Korolar 4.2.1. *Neka je $\mathbb{F}$ polje i neka je $n = 2^k$ za neki $k \in \mathbb{N}_0$. Tada postoje racionalne funkcije $z_1, ..., z_n \in \mathbb{F}(x_1, ..., x_n, y_1, ..., y_n)$ takve da je*

$$(x_1^2 + ... + x_n^2)(y_1^2 + ... + y_n^2) = z_1^2 + ... + z_n^2.$$

Dokaz. Tvrdnja slijedi direktnom primjenom Pfisterovog teorema o sumama kvadrata (Teorem 4.1.1) na racionalne funkcije $x_1, \ldots, x_n, y_1, \ldots, y_n \in \mathbb{F}(x_1, \ldots, x_n, y_1, \ldots, y_n)$. □

Korolar 4.2.2. *Neka je $n = 2^k$ za neki $k \in \mathbb{N}_0$ i neka je S skup suma n kvadrata različitih od 0 u bilo kojem polju $\mathbb{F}$. Tada je S podgrupa od $\mathbb{F}^\times$.*

Dokaz. Prema Pfisterovom teoremu o sumama kvadrata (Teorem 4.1.1), skup S je zatvoren na množenje, a prema pretpostavci korolara za svaki $s \in S$ vrijedi da je $s \neq 0$ i da je $s = a_1^2 + \ldots + a_n^2$ za neke $a_1, \ldots, a_n \in \mathbb{F}$ pa možemo uočiti da za inverzni element vrijedi $\frac{1}{s} = \frac{s}{s^2} = \left(\frac{a_1}{s}\right)^2 + ... + \left(\frac{a_n}{s}\right)^2$.

Dakle, za skup suma n kvadrata različitih od 0 u polju $\mathbb{F}$ vrijedi zatvorenost i postojanje inverznog elementa. Budući da je $\mathbb{F}^\times$ multiplikativna grupa s elementima iz polja $\mathbb{F}$ različitima od 0, prema definiciji podgrupe slijedi tvrdnja. □

Budući da je Lema 4.1.2 ključna za dokaz Pfisterovog teorema o sumama kvadrata, izvedimo pomoću nje konkretne formule u Pfisterovom teoremu za $n = 2$ i $n = 4$.

Neka je $\mathbb{F}$ polje i neka je $n = 2^k$ za neki $k \in \mathbb{N}$. Tada je za

$$x = x_1^2 + ... + x_n^2 = \sum_{i=1}^{n} x_i^2, \quad y = y_1^2 + ... + y_n^2 = \sum_{j=1}^{n} y_j^2$$

s elementima $x_i, y_j \in \mathbb{F}, i, j \in \{1, ..., n\}$ prema Pfisterovom teoremu o sumama kvadrata (Teorem 4.1.1) produkt xy jednak sumi n kvadrata. Nadalje, po Lemi 4.1.2 postoje $n \times n$ matrice X i Y s elementima iz polja $\mathbb{F}$ za koje vrijedi

$$XX^\top = X^\top X = xI_n, \quad YY^\top = Y^\top Y = yI_n,$$

pri čemu je prvi redak matrice X jednak $(x_1, ..., x_n)$, a matrice Y jednak $(y_1, ..., y_n)$. Za matrice X i Y pritom vrijedi

$$X = \begin{pmatrix} A & B \\ B & -BA^\top (B^{-1})^\top \end{pmatrix}, \quad Y = \begin{pmatrix} C & D \\ D & -DC^\top (D^{-1})^\top \end{pmatrix}, \tag{4.5}$$

gdje su A, B, C, D $\frac{n}{2} \times \frac{n}{2}$ matrice iz Leme 4.1.2 koje odgovaraju sumi $\frac{n}{2}$ kvadrata različitih od 0. Preciznije, A odgovara sumi $\sum_{i=1}^{\frac{n}{2}} x_i^2$, B odgovara sumi $\sum_{i=\frac{n}{2}+1}^{n} x_i^2$, C odgovara sumi $\sum_{j=1}^{\frac{n}{2}} y_j^2$ i D odgovara sumi $\sum_{j=\frac{n}{2}+1}^{n} y_j^2$. Po dokazu Pfisterovog teorema (Teorem 4.1.1) vrijedi $(x_1^2 + \ldots + x_n^2)(y_1^2 + \ldots + y_n^2) = z_1^2 + \ldots + z_n^2$, gdje je $(z_1, \ldots, z_n)$ prvi redak matrice XY.

Za $n = 2$ vrijedi $x = x_1^2 + x_2^2$, $y = y_1^2 + y_2^2$. Matrice u (4.5) su tada oblika

$$X = \begin{pmatrix} x_1 & x_2 \\ x_2 & -x_1 \end{pmatrix}, \quad Y = \begin{pmatrix} y_1 & y_2 \\ y_2 & -y_1 \end{pmatrix}$$

Tada je

$$(x_1^2 + x_2^2)(y_1^2 + y_2^2) = z_1^2 + z_2^2,$$

pri čemu je (z_1, z_2) prvi redak matrice produkta XY. Preciznije, vrijedi

$$\begin{aligned} z_1 &= x_1y_1 + x_2y_2, \\ z_2 &= x_1y_2 - x_2y_1. \end{aligned} \tag{4.6}$$

Za $n = 4$ vrijedi $x = \sum_{i=1}^{4} x_i^2$, $y = \sum_{j=1}^{4} y_j^2$. Matrice u (4.5) su tada oblika

$$X = \begin{pmatrix} x_1 & x_2 & x_3 & x_4 \\ x_2 & -x_1 & x_4 & -x_3 \\ x_3 & x_4 & \frac{x_1\left(-x_3^2+x_4^2\right)-2x_2x_3x_4}{x_3^2+x_4^2} & \frac{x_2\left(x_3^2-x_4^2\right)-2x_1x_3x_4}{x_3^2+x_4^2} \\ x_4 & -x_3 & \frac{x_2\left(x_3^2-x_4^2\right)-2x_1x_3x_4}{x_3^2+x_4^2} & \frac{x_1\left(x_3^2-x_4^2\right)+2x_2x_3x_4}{x_3^2+x_4^2} \end{pmatrix},$$

$$Y = \begin{pmatrix} y_1 & y_2 & y_3 & y_4 \\ y_2 & -y_1 & y_4 & -y_3 \\ y_3 & y_4 & \frac{y_1\left(-y_3^2+y_4^2\right)-2y_2y_3y_4}{y_3^2+y_4^2} & \frac{y_2\left(y_3^2-y_4^2\right)-2y_1y_3y_4}{y_3^2+y_4^2} \\ y_4 & -y_3 & \frac{y_2\left(y_3^2-y_4^2\right)-2y_1y_3y_4}{y_3^2+y_4^2} & \frac{y_1\left(y_3^2-y_4^2\right)+2y_2y_3y_4}{y_3^2+y_4^2} \end{pmatrix}.$$

Tada za produkt xy koji je jednak sumi 4 kvadrata koristeći XY imamo

$$\left(\sum_{i=1}^{4} x_i^2\right)\left(\sum_{j=1}^{4} y_j^2\right) = \sum_{k=1}^{4} z_k^2,$$

pri čemu je (z_1, z_2, z_3, z_4) prvi redak matrice produkta XY. Preciznije, vrijedi

$$\begin{aligned} z_1 &= x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4, \\ z_2 &= x_1y_2 - x_2y_1 + x_3y_4 - x_4y_3, \\ z_3 &= x_1y_3 + x_2y_4 + x_3\frac{y_1\left(-y_3^2 + y_4^2\right) - 2y_2y_3y_4}{y_3^2 + y_4^2} + x_4\frac{y_2\left(y_3^2 - y_4^2\right) - 2y_1y_3y_4}{y_3^2 + y_4^2}, \\ z_4 &= x_1y_4 - x_2y_3 + x_3\frac{y_2\left(y_3^2 - y_4^2\right) - 2y_1y_3y_4}{y_3^2 + y_4^2} + x_4\frac{y_1\left(y_3^2 - y_4^2\right) + 2y_2y_3y_4}{y_3^2 + y_4^2}. \end{aligned} \tag{4.7}$$

Time smo dobili konkretne formule u Pfisterovom teoremu o sumama kvadrata za $n = 2$ u (4.6) i za $n = 4$ u (4.7) koje možemo usporediti s konkretnim formulama u Hurwitzovom $(1, 2, 4, 8)$-teoremu za $n = 2$ u (3.3) i za $n = 4$ u (3.4).

Bibliografija

[1] K. Conrad, *The Hurwitz theorem on sums of squares by linear algebra,* bilješke s predavanja, 2008., dostupno na https://kconrad.math.uconn.edu/blurbs/linmultialg/hurwitzlinear.pdf (lipanj 2021.).

[2] ———, *Pfister's theorem on sums of squares,* bilješke s predavanja, 2009., dostupno na https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.210.6351&rep=rep1&type=pdf (lipanj 2021.).

[3] Z. Franušić, J. Šiftar, *Linearna algebra 1,* skripta, PMF - Matematički odsjek, Zagreb, dostupno na https://web.math.pmf.unizg.hr/~fran/predavanja-LA1.pdf (lipanj 2021.).

[4] ———, *Linearna algebra 2,* skripta, PMF - Matematički odsjek, Zagreb, dostupno na https://web.math.pmf.unizg.hr/~fran/predavanja-LA2.pdf (lipanj 2021.).

[5] Ž. Milin Šipuš, M. Bombardelli, *Analitička geometrija,* skripta, PMF - Matematički odsjek, Zagreb, 2016., dostupno na https://web.math.pmf.unizg.hr/nastava/ag/dodatni/AG-predavanja-2016.pdf (lipanj 2021.).

[6] A. R. Rajwade, *Pfister's work on sums of squares*, Number theory, 325-349, Trends Math, Birkhäuser, Basel, 2000.

[7] B. Širola, *Algebarske strukture,* skripta, PMF - Matematički odsjek, Zagreb, dostupno na https://web.math.pmf.unizg.hr/nastava/alg/predavanja/ASpred.pdf (lipanj 2021.).

Sažetak

U ovom radu opisani su konkretni primjeri i rezultati vezani za produkte suma kvadrata. Kroz povijest su otkriveni identiteti koji vrijede za određeni prirodan broj n u kojima je zbroj n kvadrata pomnožen sa zbrojem n kvadrata opet zbroj n kvadrata. Proučavanjem tih produkata suma kvadrata dokazana su dva značajna teorema, Hurwitzov $(1, 2, 4, 8)$-teorem i Pfisterov teorem o sumama kvadrata, koji su glavna tema ovog rada. Za njihovo dokazivanje potrebni su pomoćni rezultati koji se stoga pojavljuju u radu. Također, opisane su i neke primjene tih teorema.

Summary

In this thesis, specific examples and results related to the products of the sum of squares are described. Through the history, there have been discovered identities that are valid for a certain natural number n by which a sum of n squares multiplied by another sum of n squares is again a sum of n squares. By studying these products of sums of squares, two significant theorems have been proved, Hurwitz's $(1, 2, 4, 8)$-theorem and Pfister's theorem on sums of squares, which are the main topic of this thesis. To prove them, we needed auxiliary results so they therefore appear in the thesis. Moreover, some applications of these theorems are described.

Životopis

Dana 14. srpnja 1996. rođena sam u Zagrebu. Odrasla sam u općini Brdovec pored Zaprešića gdje sam 2003. godine započela svoje školovanje u Osnovnoj školi Ivane Brlić-Mažuranić. Nakon što sam ju završila 2011. godine, upisala sam Gornjogradsku gimnaziju koju sam završila 2015. godine. Daljnje školovanje sam nastavila iste godine na Prirodoslovno-matematičkom fakultetu u Zagrebu gdje sam na Matematičkom odsjeku upisala preddiplomski studij Matematika; smjer: nastavnički. Potom sam 2018. godine na istom fakultetu upisala diplomski sveučilišni studij Matematika; smjer: nastavnički.