Konstrukcija formi koje dopuštaju kompoziciju

Markač, Kristijan

SVEUČILIŠTE U ZAGREBU

PRIRODOSLOVNO–MATEMATIČKI FAKULTET

MATEMATIČKI ODSJEK

Kristijan Markač

KONSTRUKCIJA FORMI KOJE DOPUŠTAJU KOMPOZICIJU

Diplomski rad

Voditelj rada:
izv. prof. dr. sc. Zrinka Franušić

Zagreb, rujan, 2022.

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. _____

Posebna zahvala mentorici izv. prof. dr. sc. Zrinki Franušić na svoj pomoći koju mi je pružala tijekom pisanja ovog rada.
Ovaj rad posvećujem svojoj obitelji koja mi je dala nevjerojatnu podršku pri upisu i tijekom cijelog studija. Rad također posvećujem Miroslavu koji mi je najveća podrška u životu i uvijek me potiče da pomičem svoje granice. Hvala Mica!

Diplomski rad napravljen je u sklopu aktivnosti Projekta KK.01.1.1.01.0004 - Znanstveni centar izvrsnosti za kvantne i kompleksne sustave te reprezentacije Liejevih algebri.

Sadržaj

Uvod

Neka je $f : \mathbb{R}^n \to \mathbb{R}$ algebarska forma, odnosno homogeni polinom s n varijabli. Kažemo da forma f dopušta kompoziciju ili da se radi o kompozicijskoj formi ako vrijedi

$$f(x_1, x_2, \ldots, x_n)f(y_1, y_2, \ldots, y_n) = f(z_1, z_2, \ldots, z_n), \tag{1}$$

gdje je svaka varijabla z_i, $i = 1, 2, \ldots, n$, bilinearna forma s varijablama x_i, y_i, $i = 1, 2, \ldots, n$, odnosno,

$$z_i = \phi_i(x_1, \ldots, x_n, y_1, \ldots, y_n) = \sum_{j=1}^{n}\sum_{k=1}^{n} \lambda_{ijk}x_j y_k, \quad i = 1, 2, \ldots, n, \tag{2}$$

za neke konstante λ_{ijk} i za sve $x_i, y_i \in \mathbb{R}$.

Osnovni primjer forme koja dopušta kompoziciju je determinanta kvadratne matrice. U slučaju kvadratne matrice reda dva, funkcija

$$f(x_1, x_2, x_3, x_4) = \det\begin{bmatrix} x_1 & x_2 \\ x_3 & x_4 \end{bmatrix} = x_1x_4 - x_2x_3$$

je forma stupnja 4 u četiri varijable koja dopušta kompoziciju. Zaista, prema Binet-Caucyjevu teoremu je

$$\det\begin{bmatrix} x_1 & x_2 \\ x_3 & x_4 \end{bmatrix}\det\begin{bmatrix} y_1 & y_2 \\ y_3 & y_4 \end{bmatrix} = \det\left(\begin{bmatrix} x_1 & x_2 \\ x_3 & x_4 \end{bmatrix}\begin{bmatrix} y_1 & y_2 \\ y_3 & y_4 \end{bmatrix}\right) = \det\begin{bmatrix} x_1y_1 + x_2y_3 & x_1y_2 + x_2y_4 \\ x_3y_1 + x_4y_3 & x_3y_2 + x_4y_4 \end{bmatrix},$$

pa je

$$f(x_1, x_2, x_3, x_4)f(y_1, y_2, y_3, y_4) = f(z_1, z_2, z_3, z_4),$$

pri čemu su

$$z_1 = x_1y_1 + x_2y_3,\ z_2 = x_1y_2 + x_2y_4,\ z_3x_3y_1 + x_4y_3,\ z_4 = x_3y_2 + x_4y_4.$$

Općenito, determinanta kvadratne matrice reda n je forma stupnja n u n^2 varijabli koja dopušta kompoziciju. Prirodno je pitati se možemo li pronaći primjere ovakvih formi s

manjim brojem varijabli. Indijski matematičar i diplomat A. Choudhry je u članku „Matrix morphology and composition of higher degree forms with applications to diophantine equations" ([1]) opisao kako konstruirati forme stupnja n u n varijabli, za $n \in \{3, 4, 6, 8\}$. U konstrukciji ključnu ulogu za to imaju komutativne podalgebre matrica. Osim konkretnih primjera takvih podalgebri reda 2 i reda 3, opisujemo kako se daljnji primjeri podalgebri višeg reda mogu dobiti pomoću Kroneckerovog produkta.

Nadalje, u radu se bavimo i diofantskim jednadžbama oblika

$$f(x_1, x_2, \ldots, x_n) = 1, \tag{3}$$

za neke specijalne cjelobrojne forme koje dopuštaju kompoziciju. Naime, ako postoji rješenje jednadžbe (3), tada je iz (2) moguće generirati njih beskonačno puno. Ovo je zapravo generalizacija dobro poznate Pellove jednadžbe

$$x^2 - dy^2 = 1,$$

gdje je d prirodni broj koji nije potpuni kvadrat. Naime, funkcija

$$f(x, y) = x^2 - dy^2$$

je kvadratna forma koja dopušta kompoziciju jer vrijedi sljedeći identitet

$$(x_1^2 - dy_1^2)(x_2^2 - dy_2^2) = (x_1x_2 - dy_1y_2)^2 - d(x_1y_2 - x_2y_1)^2.$$

Stoga, iz dva rješenja (x_1, y_1), (x_2, y_2) Pellove jednadžbe (od čega je bar jedno netrivijalno, tj. različito od $(1, 0)$) dobivamo novo rješenje $(x_1x_2 - dy_1y_2, x_1y_2 - x_2y_1)$.

Za provedbu nekih računa korišten je online softver programskog paketa *Wolfram Mathematica* dostupan na `https://www.wolframcloud.com/obj/wpl/GetStarted.nb?funnel=WPLGetStarted#sidebar=explorations`.

Poglavlje 1

Algebra matrica

1.1 Definicija matrice. Operacije s matricama

Definicija 1.1.1. *Neka su* $m, n \in \mathbb{N}$. *Preslikavanje*

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

zovemo matrica tipa (m, n) *(ili* $m \times n$*) s koeficijentima (ili elementima) iz polja* $\mathbb{F}$. *Skup svih takvih matrica označavamo s* $M_{mn}(\mathbb{F})$.

U ovom radu matrice ćemo kraće zapisati kao $A = [a_{ij}]$, gdje je a_{ij} element matrice na presjeku i-tog retka i j-tog stupca.

Definicija 1.1.2. *Matrica tipa* (n, n) *naziva se* kvadratna matrica *ili* matrica reda n. *Skup svih kvadratnih matrica s elementima iz polja* $\mathbb{F}$ *označavamo s* $M_n(\mathbb{F})$.

Definicija 1.1.3. Zbroj matrica $A = [a_{ij}]$ *i* $B = [b_{ij}]$ *tipa* (m, n) *je matrica* $C = [c_{ij}]$ *tipa* (m, n) *za čije elemente vrijedi*

$$c_{ij} = a_{ij} + b_{ij}$$

za sve $i = 1, \ldots, m$ *i* $j = 1, \ldots, n$. *Pišemo* $C = A + B$.

Zbrajanje matrica je očito binarna operacija koja je asocijativna i komutativna budući da se operacija definira po elementima matrice, a oni su iz polja $\mathbb{F}$. Neutralni element za zbrajanje je matrica čiji su svi elementi jednaki nuli tzv. *nulmatrica*. Također svaka matrica $A = [a_{ij}]$ ima suprotnu matricu $-A = [-a_{ij}]$. Stoga smo pokazali sljedeću propoziciju.

Propozicija 1.1.4. *Skup matrica* $M_{mn}(\mathbb{F})$ *uz operaciju zbrajanja matrica je Abelova grupa.*

Definicija 1.1.5. Umnožak matrice $A = [a_{ij}]$ *tipa* (m, n) skalarom $\lambda \in \mathbb{F}$ *je matrica* $B = [b_{ij}]$ *tipa* (m, n) *za čije elemente vrijedi*

$$b_{ij} = \lambda a_{ij},$$

za sve $i = 1, \ldots, m$ *i* $j = 1, \ldots, n$. *Pišemo* $B = \lambda A$.

Za operacije *umnoška matrice skalarom* i *zbrajanja matrica* vrijede svojstva kvazi-asocijativnosti, distributivnosti množenja prema zbrajanju i množenje s 1 jer su operacije definirane po elementima.

Teorem 1.1.6. *Skup matrica* $M_{mn}(\mathbb{F})$ *uz operacije zbrajanja matrica i množenje matrica skalarom je vektorski prostor nad poljem* $\mathbb{F}$ *čija je dimenzija jednaka* $m \cdot n$.

Definicija 1.1.7. *Matrice* A *i* B *su* ulančane *ako je broj stupaca matrice* A *jednak broju redaka matrice* B.

Definicija 1.1.8. *Neka su* $A = [a_{ij}]$ *i* $B = [b_{ij}]$ *ulančane matrice tipa* (m, n) *i* (n, p), *respektivno.* Umnožak matrica A *i* B *je matrica* $C = [c_{ij}]$ *tipa* (m, p) *čiji su elementi dani sljedećom formulom*

$$c_{ij} = a_{i1}b_{1j} + a_{i2}b_{2j} + \cdots + a_{in}b_{nj} = \sum_{k=1}^{n} a_{ik}b_{kj},$$

za $i = 1, \ldots, m$ *i* $j = 1, \ldots, p$. *Pišemo* $C = A \cdot B = AB$. *Na ovaj način smo definirali operaciju* množenja matrica

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

Propozicija 1.1.9. *Vrijedi*

$$A(BC) = (AB)C,$$

za sve matrice za koje je gornji izraz definiran, to jest množenje matrica je asocijativna operacija.

Propozicija 1.1.10. *Množenje matrica je*

- *kvaziasocijativno, odnosno*

$$(\lambda A)B = \lambda(AB) = A(\lambda B),$$

  za sve $\lambda \in \mathbb{F}$, *te* A *i* B *za koje je gornji izraz definiran*

- *distributivno prema zbrajanju matrice, odnosno*

$$(A + B)C = AC + BC,$$

$$A(B + C) = AB + AC,$$

za sve A, B i C za koje je gornji izraz definiran.

Definicija 1.1.11. *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 zovemo inverznom matricom od A i pišemo, $B = A^{-1}$. U protivnom je A singularna *matrica.*

Definicija 1.1.12. Elementarne transformacije nad matricom $A \in M_{mn}(\mathbb{F})$ *su:*

1. *zamjena dva stupca (retka)*
2. *množenje stupca (retka) skalarom $\lambda \neq 0$*
3. *pribrajanje nekom stupcu (retku) nekog drugog stupca (retka) pomnoženog skalarom λ.*

Definicija 1.1.13. *Neka su $A, B \in M_{mn}(\mathbb{F})$. Matrica A je* ekvivalentna *matrici B ako se B može dobiti iz A primjenom konačno mnogo elementarnih transformacija. Pišemo $A \sim B$.*

Definicija 1.1.14. Elementarna matrica *reda n je matrica koja je dobivena jednom elementarnom transformacijom nad stupcima ili redcima jedinične matrice reda n.*

Definicija 1.1.15. *Neka je $A = [a_{ij}] \in M_{mn}(\mathbb{F})$, te $(S_1, \ldots, S_n)$, $S_j \in M_{m1}(\mathbb{F})$, stupčana reprezentacija matrice A.* Rang matrice *A je dimenzija linearne ljuske razapete skupom stupaca od A. Pišemo $r(A) = \dim[S_1, \ldots, S_n]$.*

Propozicija 1.1.16. *Svaka regularna matrica može se napisati kao umnožak elementarnih matrica.*

Definicija 1.1.17. *Neka je $A = \left[a_{ij}\right] \in M_n(\mathbb{F})$.* Determinanta matrice A *je skalar iz polja $\mathbb{F}$ koji se definira kao*

$$\det A = \sum_{p \in S_n} (-1)^{I(p)} a_{1p(1)} a_{2p(2)} \cdots a_{np(n)},$$

gdje je S_n grupa permutacija skupa $\{1, \ldots, n\}$, a $I(p)$ broj inverzija *permutacija p.* Inverzija *permutacije p je svaki par (i, j) takav da je $1 \leq i \leq j \leq n$ i $p(i) > p(j)$.*

Propozicija 1.1.18. *Neka su $A, B \in M_n(\mathbb{F})$. Ako je B dobivena iz A:*

1. *međusobnom zamjenom dva retka (stupca), onda* $\det B = -\det A$
2. *množenjem skalarom* $\lambda \neq 0$ *nekog retka (stupca), onda* $\det B = \lambda(\det A)$
3. *pribrajanjem nekog retka (stupca) pomnoženog s* λ *nekom drugom retku (stupcu), onda* $\det B = \lambda(\det A)$.

Propozicija 1.1.19. *Matrica A je regularna ako i samo ako je* $\det A \neq 0$.

Propozicija 1.1.20. *Neka su A i B ulančane matrice. Tada rang njihovog umnoška nije veći od ranga pojedinih matrica, to jest* $r(AB) \leq r(A), r(B)$.

Definicija 1.1.21. *Determinanta matrice koja nastaje uklanjanjem i-tog retka i j-tog stupca matrice A naziva se* minora *reda* $n-1$ *i označava s* Δ_{ij}.

Definicija 1.1.22. Kofaktor *ili* algebarski komplement *elemenata* a_{ij} *je broj* $A_{ij} = (-1)^{i+j}\Delta_{ij}$.

Definicija 1.1.23. Adjunkta matrice *A je matrica* $\widetilde{A} = \left[A_{ji}\right] \in M_n(\mathbb{F})$*, to jest transponirana matrica algebarskih komplemenata matrice A.*

Propozicija 1.1.24. *Ako je* $\det A \neq 0$, *onda*

$$A^{-1} = \frac{1}{\det A}\widetilde{A}.$$

1.2 Vektorski prostor matrica. Algebra matrica

U prethodnom odjeljku obrazložili smo da je skup $M_n(\mathbb{R})$, tj. skup svih realnih kvadratnih matrica reda n, vektorski prostor nad poljem realnih brojeva uz operacije zbrajanje matrica i množenja matrica skalarom. Dimenzija ovog vektorskog prostora je n^2. Štoviše, budući da je množenje matrica *bilinearna* operacija, odnosno vrijedi

$$(\alpha A + B)C = \alpha AC + BC,\ A(\alpha B + C) = \alpha AB + AC,$$

za sve $A, B, C \in M_n(\mathbb{R})$, $\alpha \in \mathbb{R}$, vektorski prostor $M_n(\mathbb{R})$ čini *algebru* nad poljem $\mathbb{R}$. Štoviše, taj vektorski prostor je *asocijativna algebra s jedinicom* jer je množenje matrica asocijativno i postoji neutralni element množenja – jedinična matrica reda n, $I_n \in M_n(\mathbb{R})$. Svaka podalgebra algebre $M_n(\mathbb{R})$ je zatvorena obzirom na operacije zbrajanja matrica, množenja matrice skalarom i množenja matrica.

Skup svih matrica reda n s cjelobrojnim koeficijentima, $M_n(\mathbb{Z})$, zatvoren je s obzirom na operacije zbrajanja matrica, množenja matrice cijelim brojem i množenja matrica pa i on čini asocijativnu algebru s jedinicom (nad $\mathbb{Z}$) budući da se sva potrebna svojstva nasljeđuju. Napomenimo da $M_n(\mathbb{Z})$ s obzirom na zbrajanje matrica i množenje matrice brojevima iz

prstena $\mathbb{Z}$ ima strukturu tzv. *modula* kojeg zapravo možemo shvatiti kao „vektorski prostor nad prstenom".

Tipični primjer vektorskog potprostora je ljuska nekog nepraznog skupa, odnosno skup svih mogućih linearnih kombinacija vektora iz tog skupa. Ljusku skupa $\{M_1, \ldots, M_k\} \subset M_n(\mathbb{R})$ označavat ćemo s

$$\mathcal{L} = [\{M_1, \ldots, M_k\}] = \{x_1 M_1 + \cdots + x_k M_k \,:\, x_1, \ldots, x_k \in \mathbb{R}\}.$$

Skup svih mogućih cjelobrojnih linearnih kombinacija skupa $\{M_1, \ldots, M_k\} \subset M_n(\mathbb{Z})$, koji čini podmodul od $M_n(\mathbb{Z})$, označavat ćemo s

$$\mathcal{L}(\mathbb{Z}) = [\{M_1, \ldots, M_k\}]_{\mathbb{Z}} = \{x_1 M_1 + \cdots + x_k M_k \,:\, x_1, \ldots, x_k \in \mathbb{Z}\}.$$

Sada ćemo opisati kako možemo konstruirati podalgebre od $M_n(\mathbb{R})$. Neka je

$$g(x) = a_0 + a_1 x + \cdots + a_h x^h,\ a_h \neq 0$$

minimalni polinom matrice $M \in M_n(\mathbb{R})$. *Minimalni polinom* matrice M je polinom najmanjeg stupnja za kojeg je $g(M) = 0$. Minimalni polinom matrice M određuje se pomoću *karakterističnog* polinoma

$$k_M(x) = \det(M - xI_n).$$

Naime, minimalni i karakteristični polinom matrice imaju jednake skupove nutočaka – svojstvenih vrijednosti matrice, eventualno različitih kratnosti. Razlog tomu je sljedeći važen teorem.

Teorem 1.2.1 (Cayley-Hamiltonov teorem)**.** *Svaka kvadratna matrica M poništava svoj karakteristični polinom, odnosno $k_M(M)$ je nulmatrica.*

Uočimo da je skup

$$\{I_n, M, M^2, \ldots, M^{h-1}\}$$

linearno nezavisan skup jer ako bi postojala netrivijalna kombinacija skalara $b_0, b_1, \ldots, b_{h-1}$ za koju je

$$b_0 I_n + b_1 M + \cdots + b_{h-1} M^{h-1} = 0,$$

to bi bilo u kontradikciji s minimalnošću polinoma g. Nadalje, iz $g(M) = 0$ slijedi da je

$$a_0 I_n + a_1 M + \cdots + a_{h-1} M^{h-1} + a_h M^h = 0,$$

odnosno

$$M^h = a_h^{-1}(a_0 I_n + a_1 M + \cdots + a_{h-1} M^{h-1}),$$

što implicira da se sve potencije matrice M^k, gdje je $k \geq h$ mogu napisati kao linearne kombinacije matrica $I_n, M, \ldots, M^{h-1}$. Stoga linearna ljuska $\left[\left\{I_n, M, \ldots, M^{h-1}\right\}\right]$, odnosno skup

$$\{x_1 I_n + x_2 M + \cdots + x_h M^{h-1} : x_1, \ldots, x_h \in \mathbb{R}\},$$

predstavlja podalgebru algebre $M_n(\mathbb{R})$. Osim toga, ova podalgebra je komutativna i sadrži neutralni element za množenje (I_n) pa govorimo o primjeru komutativne algebre s jedinicom nad poljem $\mathbb{R}$.

Primjer 1.2.2. *Zadana je matrica*

$$M = \begin{bmatrix} 3 & -1 & 0 \\ 0 & 2 & 0 \\ 1 & -1 & 2 \end{bmatrix}.$$

Odredite dimenziju ljuske $[\{I_3, M, M^2\}]$.

Rješenje.

$$I_3 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix},$$

$$M^2 = \begin{bmatrix} 3 & -1 & 0 \\ 0 & 2 & 0 \\ 1 & -1 & 2 \end{bmatrix}^2 = \begin{bmatrix} 9 & -5 & 0 \\ 0 & 4 & 0 \\ 5 & -5 & 4 \end{bmatrix}.$$

Odredimo minimalni polinom matrice M. Karakteristični polinom matrice M je

$$k_M(x) = \det(M - xI_3) = \begin{vmatrix} 3-x & -1 & 0 \\ 0 & 2-x & 0 \\ 1 & -1 & 2-x \end{vmatrix} = (2-x) \cdot \begin{vmatrix} 3-x & -1 \\ 0 & 2-x \end{vmatrix} = (2-x)^2(3-x)$$

Budući da minimalni polinom mora imati isti skup nultočaka kao i karakteristični, $\{2, 3\}$, jedini kandidati za minimalni polinom su $(2-x)^2(3-x)$ i $(2-x)(3-x)$. Kako je $(2I_3 - M)(3I_3 - M) = 0$, zaključujemo da je polinom

$$(2-x)(3-x) = x^2 - 5x + 6$$

minimalni polinom matrice M. Pomoću minimalnog polinoma moguće je matricu M^2 prikazati kao linearnu kombinaciju matrica I_3 i M,

$$M^2 = 5M - 6I_3.$$

Matrice I_3 i M su očito linearno nezavisne te je stoga $\dim[\{I_3, M, M^2\}] = 2$. □

Lema 1.2.3. *Ako je* $\mathcal{V} = [\{A_1, A_2, \ldots, A_h\}] \leq M_n(\mathbb{R})$*, gdje je* $\{A_1, A_2, \ldots, A_h\}$ *skup matrica iz* $M_n(\mathbb{R})$ *i umnožak* $A_iA_j \in \mathcal{V}$*, za sve* $i, j \in \{1, \ldots, h\}$*, tada je* $\mathcal{V}$ *podalgebra od* $M_n(\mathbb{R})$*.*

Dokaz. Jedino što treba provjeriti da je potprostor $\mathcal{V}$ zatvoren na množenje. Neka su A i B neke matrice iz $\mathcal{V}$. Svaka od tih matrica može se zapisati kao linearna kombinacija skupa matrica $\{A_1, A_2, \ldots, A_h\}$:

$$AB = (\alpha_1A_1 + \cdots + \alpha_hA_h)(\beta_1A_1 + \cdots + \beta_hA_h) = \sum_{i=1}^{h}\sum_{j=1}^{h}\alpha_i\beta_jA_iA_j.$$

Budući da je $A_iA_j \in \mathcal{V}$ za sve $i, j \in \{1, \ldots, h\}$, umnožak matrica A i B može se zapisati kao linearna kombinacija matrica $A_1, \ldots, A_h$ i stoga je $AB \in \mathcal{V}$. □

Korolar 1.2.4. *Neka su* $A_1, A_2, \ldots, A_h$ *matrice s cjelobrojnim elementima. Ako se* A_iA_j *može prikazati kao cjelobrojna linearna kombinacija matrica* $A_1, \ldots, A_h$ *za sve* $i, j \in \{1, \ldots, h\}$*, onda je skup svih cjelobrojnih linearnih kombinacija matrica* $A_1, A_2, \ldots, A_h$*, tj.*

$$\mathcal{V}(\mathbb{Z}) = \{x_1A_1 + x_2A_2 + \cdots x_hA_h : x_1, x_2, \ldots, x_h \in \mathbb{Z}\}$$

je algebra nad prstenom $\mathbb{Z}$*.*

Primjer 1.2.5. *Zadana je matrica*

$$M = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 2 & 2 \\ 1 & 1 & 2 \end{bmatrix}.$$

Ispitajte je li $\{a_0I_3 + a_1M + a_2M^2 : a_0, a_1, a_2 \in \mathbb{Z}\}$ *algebra nad prstenom cijelih brojeva.*

Rješenje. Pokažimo da su zadovoljeni uvjeti Korolara 1.2.4. Većinu umnožaka A_iA_j gdje su $A_i, A_j \in V = \{I_3, M, M^2\}$ moguće je trivijalno prikazati kao cjelobrojnu linearnu kombinaciju matrica iz V

$$I_3^2 = I_3,$$

$$I_3 \cdot M = M \cdot I_3 = M,$$

$$I_3 \cdot M^2 = M^2 \cdot I_3 = M^2,$$

$$M \cdot M = M^2.$$

Preostalo je provjeriti jesu li $M^3 = M \cdot M^2 = M^2 \cdot M$ i $M^4 = M^2 \cdot M^2$ prikazive kao cjelobrojne linearne kombinacije matrica iz V. Odredimo karakteristični polinom matrice M:

$$k_M(x) = \begin{vmatrix} 1-x & 1 & 1 \\ 1 & 2-x & 2 \\ 1 & 1 & 2-x \end{vmatrix} = 1 \cdot \begin{vmatrix} 1 & 1 \\ 2-x & 2 \end{vmatrix} - 1 \cdot \begin{vmatrix} 1-x & 1 \\ 1 & 2 \end{vmatrix} + (2-x) \cdot \begin{vmatrix} 1-x & 1 \\ 1 & 2-x \end{vmatrix} =$$

$$= x - (1-2x) + (2-x)(1-3x+x^2) = -x^3 + 5x^2 - 4x + 1.$$

Iz Cayley-Hamiltonova teorema 1.2.1 slijedi:

$$-M^3 + 5M^2 - 4M + I_3 = 0,$$

odnosno

$$M^3 = 5M^2 - 4M + I_3.$$

Pomnožimo li gornju jednadžbu s M, lako dobivamo i zapis posljednjeg umnoška $M^2 \cdot M^2 = M^4$ kao cjelobrojnu linearnu kombinaciju matrica iz V.

$$M^4 = 5M^3 - 4M^2 + M = 21M^2 - 19M + 5I_3.$$

Sada prema Korolaru 1.2.4 slijedi da je $\{a_0 I_3 + a_1 M + a_2 M^2 : a_0, a_1, a_2 \in \mathbb{Z}\}$ algebra nad prstenom cijelih brojeva. Uočimo da je ova algebra i komutativna.

□

1.3 Binet-Cauchyjev teorem

Determinanta matrice je preslikavanje koje svakoj kvadratnoj matrici pridruži skalar. Direktno iz definicije 1.1.17 vidimo da je to jedna homogena funkcija stupnja koji je jednak redu matrice. Dakle, ako je A kvadratna matrica reda n, a λ skalar, tada je $\det(\lambda A) = \lambda^n \det A$. Nadalje, determinanta matrice je *multiplikativno* preslikavanje o čemu govori tzv. Binet-Cauchyjev teorem.

Teorem 1.3.1 (Binet-Cauchy)**.** *Neka su matrice $A, B \in M_n(\mathbb{F})$ i neka je matrica $C = A \cdot B$. Tada je*

$$\det C = \det A \cdot \det B$$

.

Dokaz. U slučaju dijagonalnih matrica A, B vrijedi

$$\det A = \prod_{i=1}^{n} a_{ii}, \det B = \prod_{i=1}^{n} b_{ii}.$$

$$\det A \det B = \prod_{i=1}^{n} a_{ii} \prod_{i=1}^{n} b_{ii} = \prod_{i=1}^{n} a_{ii} b_{ii} = \det(AB)$$

Ostatak dokaza provodi se u nekoliko slučajeva. Najprije je potrebno ustanoviti vrijednosti determinantni elementarnih matrica. Prema Propoziciji 1.1.18 slijedi:

- $\det E_1 = -1$, gdje je E_1 elementarna matrica koja odgovara elementarnoj transformaciji 1. vrste (zamjeni dva retka ili stupca jedinične matrice)
- $\det E_2 = \lambda$, gdje je E_2 elementarna matrica koja odgovara elementarnoj transformaciji 2. vrste (množenju nekog retka ili stupca skalarom $\lambda \neq 0$ jedinične matrice)
- $\det E_3 = 1$, gdje je E_3 elementarna matrica koja odgovara elementarnoj transformaciji 3. vrste (pribrajanju nekog retka ili stupca skalarom pomnoženim $\lambda \neq 0$ nekom drugom retku ili stupcu jedinične matrice).

1. slučaj: Pretpostavimo da je B elementarna matrica, tada je
   - $\det(AE_1) = \{\text{Prop.1.1.18 (1.)}\} = -\det A = \det A \det E_1$
   - $\det(AE_2) = \{\text{Prop.1.1.18 (2.)}\} = \lambda \det A = \det A \det E_2$
   - $\det(AE_3) = \{\text{Prop.1.1.18 (3.)}\} = \det A = \det A \det E_3$.
2. slučaj: Pretpostavimo da je B regularna matrica, tada se po Propoziciji 1.1.16 matrica B može prikazati kao umnožak elementarnih matrica. Znači,

   $$B = F_1 F_2 \cdots F_k.$$

   Uzastopnom primjenom rezultata iz 1. slučaja dobivamo

   $$\det B = \det F_1 \det F_2 \cdots \det F_k.$$

   Tada višekratnom primjenom prvog slučaja vrijedi

   $$\det(AB) = \det(AF_1 F_2 \cdots F_k) = \det(AF_1 \cdots F_{k-1}) \cdot \det F_k =$$

   $$= \cdots = \det A \cdot (\det F_1 \cdots \det F_k) = \cdots = \det A \det B.$$

3. slučaj: Pretpostavimo da B nije regularna matrica, tada je prema propoziciji 1.1.19 $\det B = 0$. Tada ni umnožak AB nije regularna matrica jer je $r(AB) \leq \min\{r(A), r(B)\} < n$ (propozicija 1.1.20). Stoga je $\det(AB) = 0$ i $\det(AB) = \det A \cdot 0 = \det A \det B$.

□

Poglavlje 2

Forme koje dopuštaju kompoziciju

2.1 Definicija

Homogeni polinom u više varijabli stupnja d jednak je zbroju monoma stupnja d. Konkretno, $p : \mathbb{R}^n \to \mathbb{R}$ je homogeni polinom u n-varijabli stupnja d ako i samo ako je

$$p(\lambda x_1, \ldots, \lambda x_n) = \lambda^d p(x_1, \ldots, x_n), \ \forall \lambda \in \mathbb{R}.$$

Na primjer,

$$p(x, y) = x^2 y + 2xy^2 - 5y^3$$

je homogeni polinom stupnja 3, dok polinom

$$q(x, y) = x + xy + y^3$$

nije homogen. Za homogene polinome često se koristi naziv *algebarska forma* ili kraće samo *forma*. Nadalje, uobičajeno je forme u dvije varijable nazivati *binarnim formama*, a forme stupnja 2 – *kvadratnim*.

Definicija 2.1.1. *Kažemo da forma* $f : \mathbb{R}^n \to \mathbb{R}$ dopušta kompoziciju *ako je*

$$f(x_1, x_2, \ldots, x_n) f(y_1, y_2, \ldots, y_n) = f(z_1, z_2, \ldots, z_n), \tag{2.1}$$

gdje je

$$z_i = \phi_i(x_1, \ldots, x_n, y_1, \ldots, y_n) = \sum_{j=1}^{n} \sum_{k=1}^{n} \lambda_{ijk} x_j y_k, \quad i = 1, 2, \ldots, n, \tag{2.2}$$

za neke konstante $\lambda_{ijk} \in \mathbb{R}$ *i za sve* $x_i, y_i \in \mathbb{R}$*, odnosno gdje je svaka varijabla* z_i *bilinearna forma u varijablama* $x_1, \ldots, x_n, y_1, \ldots, y_n$.

Napomena 2.1.2. *Bilinearna forma na vektorskom prostoru V (nad poljem $\mathbb{F}$) je svako preslikavanje $\phi : V \times V \to \mathbb{F}$ koje je linearno u svakom argumentu, odnosno za koje vrijedi:*

$$\phi(v_1 + v_2, w) = \phi(v_1, w) + \phi(v_2, w),\ \phi(\lambda v, w) = \lambda\phi(v, w)$$
$$\phi(v, w_1 + w_2) = \phi(v, w_1) + \phi(v, w_2),\ \phi(v, \lambda w) = \lambda\phi(v, w),$$

za sve $v, v_1, v_2, w, w_1, w_2 \in V$, $\lambda \in \mathbb{F}$. Preslikavanje ϕ_i dano s (2.2) je bilinearna forma na vektorskom prostoru $\mathbb{R}^n$. Često ćemo samo kratko pisati da je ϕ_i bilinearna forma u varijablama x_k, y_k, $k = 1, \ldots, n$.

Primjer 2.1.3. *Vrijedi identitet*

$$(a^2 - db^2)(e^2 - df^2) = (ae - dbf)^2 - d(af - be)^2.$$

Prema njemu za $f : \mathbb{R}^2 \to \mathbb{R}$, $f(x_1, x_2) = x_1^2 - dx_2^2$ vrijedi

$$f(x_1, x_2)f(y_1, y_2) = f(z_1, z_2),$$

gdje su

$$z_1 = x_1y_1 - dx_2y_2,\ z_2 = x_1y_2 - x_2y_1.$$

Budući da su z_1, z_2 bilinearne forme u x_1, x_2, y_1, y_2, slijedi da je f kvadratna forma u dvije varijable koja dopušta kompoziciju.

Primjer 2.1.4. *Uočimo da je s*

$$f : \mathbb{R}^{n^2} \to \mathbb{R},\ f(x_{11}, x_{12}, \ldots, x_{nn}) = \det[x_{ij}]$$

dobro definirana multilinearna forma, tj. forma u n^2 varijabli stupnja n. Prema Binet-Cauchyjevu teoremu 1.3.1 je

$$\det[x_{ij}] \det[y_{ij}] = \det[z_{ij}]$$

gdje je

$$[z_{ij}] = [x_{ij}] \cdot [y_{ij}],$$

odnosno

$$z_{ij} = \sum_{k=1}^{n} x_{ik}y_{kj}$$

je bilinearna forma u varijablama $x_{11}, x_{12}, \ldots, x_{nn}, y_{11}, y_{12}, \ldots, y_{nn}$ za sve $i, j \in \{1, \ldots, n\}$. Dakle, f je forma koja dopušta kompoziciju.

Prethodni primjer nudi dobru ideju kako konstruirati forme koje dopuštaju kompoziciju. Nadalje, uočimo da smo prethodnom primjeru dobili formu u n^2 varijabli stupnja n, tj. formu u velikom broju varijabli s obzirom na stupanj. Zanimat će nas možemo li konstruirati primjere formi u manjem broju varijabli, na primjer u n varijabli stupnja n.

2.2 Forme na podalgebrama matrica

Neka je $\mathcal{L}$ podalgebra $M_n(\mathbb{R})$ dimenzije $0 < h < n^2$, $\dim \mathcal{L} = h$, čija je baza $\{A_1, \ldots, A_h\}$. Svaka matrica podalgebre $\mathcal{L}$ može se zapisati kao jedinstvena linearna kombinacija elemenata baze. Stoga postoji bijektivno preslikavanje $A : \mathbb{R}^h \to \mathcal{L}$ koje pridružuje

$$\mathbb{R}^h \ni (x_1, \ldots, x_h) \mapsto A(x_1, \ldots, x_h) = x_1A_1 + \cdots + x_hA_h \in \mathcal{L}.$$

Iz tog razloga elemente podalgebre $\mathcal{L}$ označavat ćemo kao $A(x_1, \ldots, x_h)$.

Kako je podalgebra $\mathcal{L}$ zatvorena na operaciju množenja matrica, umnožak neke dvije matrice $A(x_1, \ldots, x_h), A(y_1, \ldots, y_h) \in \mathcal{L}$ može se zapisati kao $A(z_1, \ldots, z_h) \in \mathcal{L}$. Zaista,

$$A(x_1, \ldots, x_h) \cdot A(y_1, \ldots, y_h) = (x_1A_1 + \cdots + x_hA_h)(y_1A_1 + \cdots + y_hA_h) = \sum_{i=1}^{h} \sum_{j=1}^{h} x_iy_jA_iA_j.$$

Kako je $A_iA_j \in \mathcal{L}$, to je

$$A_iA_j = \alpha_{1,ij}A_1 + \cdots + \alpha_{h,ij}A_h,$$

za neke $\alpha_{1,ij}, \ldots, \alpha_{h,ij} \in \mathbb{R}$. Stoga je

$$A(x_1, \ldots, x_h) \cdot A(y_1, \ldots, y_h) = \underbrace{\left(\sum_{i=1}^{h} \sum_{j=1}^{h} \alpha_{1,ij}x_iy_j \right)}_{=z_1} A_1 + \cdots + \underbrace{\left(\sum_{i=1}^{h} \sum_{j=1}^{h} \alpha_{h,ij}x_iy_j \right)}_{=z_h} A_h,$$

a vrijednosti varijabli z_i, $i = 1, \ldots, h$ su bilinearne forme u varijablama $x_1, \ldots, x_h, y_1, \ldots, y_h$. Zbog prethodnog i Binet-Cauchyjevog teorema 1.3.1 slijedi:

$$\det A(x_1, \ldots, x_h) \det A(y_1, \ldots, y_h) = \det A(z_1, \ldots, z_h),$$

a to znači da forma

$$f : \mathbb{R}^h \to \mathbb{R}, \quad f(x_1, \ldots, x_h) = \det A(x_1, \ldots, x_h)$$

dopušta kompoziciju. Stoga smo pokazali sljedeći teorem.

Teorem 2.2.1. *Neka je $\{A_1, \ldots, A_h\} \subset M_n(\mathbb{R})$ linearno nezavisan skup i $\mathcal{L} = [\{A_1, \ldots, A_h\}]$ podalgebra od $M_n(\mathbb{R})$. Tada je preslikavanje*

$$f : \mathbb{R}^h \to \mathbb{R}, \ f(x_1, \ldots, x_h) = \det(x_1A_1 + \cdots + x_hA_h)$$

forma koja dopušta kompoziciju.

Napomena 2.2.2. *Tvrdnja teorema 2.2.1 vrijedi i bez pretpostavke da je* $\{A_1, \ldots, A_h\}$ *linearno nezavisan skup. Ako je* $\{A_1, \ldots, A_h\}$ *linearno zavisan skup, tada prikaz varijabli* z_i *u* (2.2) *neće biti jedinstven.*

U nastavku će nas zanimati *cjelobrojne forme*, tj. forme sa cjelobrojnim koeficijentima $f : \mathbb{Z}^n \to \mathbb{Z}$ koje dopuštaju kompoziju, odnosno za koje vrijedi (2.1) i (2.2), pri čemu su svi koeficijenti $\lambda_{ijk} \in \mathbb{Z}$.

Teorem 2.2.3. *Neka je* $\{A_1, \ldots, A_h\} \subset M_n(\mathbb{Z})$ *takav da je* $A_iA_j \in [\{A_1, \ldots, A_h\}]$ *za sve* $i, j \in \{1, \ldots, h\}$. *Tada je preslikavanje*

$$f : \mathbb{Z}^h \to \mathbb{Z},\ f(x_1, \ldots, x_h) = \det(x_1A_1 + \cdots + x_hA_h)$$

cjelobrojna forma koja dopušta kompoziciju.

Dokaz. Tvrdnja vrijedi iz činjenice da je skup

$$\mathcal{L}(\mathbb{Z}) = \{x_1A_1 + \cdots + x_hA_h : x_i \in \mathbb{Z}, i = 1, \ldots, h\},$$

zatvoren na zbrajanje, množenje cjelobrojnim skalarom i množenje matrica. □

2.3 Primjeri formi stupnja 2 i 3

Koristeći teoreme 2.2.1 i 2.2.3 konstruirat ćemo neke cjelobrojne forme koje dopuštaju kompoziciju.

Propozicija 2.3.1. *Neka su* $m, n \in \mathbb{R}$ *te*

$$A_1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad A_2 = \begin{bmatrix} 0 & 1 \\ -n & m \end{bmatrix}. \tag{2.3}$$

Tada je $\mathcal{L} = [\{A_1, A_2\}]$ *komutativna algebra s jedinicom nad* $\mathbb{R}$.

Ako su $m, n \in \mathbb{Z}$, $\mathcal{L}(\mathbb{Z})$ *je komutativna algebra s jedinicom nad prstenom* $\mathbb{Z}$.

Dokaz. Pokazujemo da je $\mathcal{L}$ podalgebra od $M_2(\mathbb{R})$. Za to je prema lemi 1.2.3 dovoljno ustanoviti da je $A_iA_j \in \mathcal{L}$ za $i, j \in 1, 2$. Očito je $A_1^2, A_1A_2 = A_2A_1 = A_2 \in \mathcal{L}$, a

$$A_2^2 = \begin{bmatrix} -n & m \\ -mn & m^2 - n \end{bmatrix} = -n\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} + m\begin{bmatrix} 0 & 1 \\ -n & m \end{bmatrix} = -nA_1 + mA_2 \in \mathcal{L}.$$

Lako se vidi da je množenje u $\mathcal{L}$ komutativno. Nadalje, $\mathcal{L}$ posjeduje neutralni element množenja (jediničnu matricu) pa je $\mathcal{L}$ komutativna algebra s jedinicom.

Skup $\mathcal{L}(\mathbb{Z})$ zatvoren je na operacije zbrajanja, množenje cijelim brojevima i množenje matrica (jer je A_2^2 cjelobrojna linearna kombinacija matrica A_1 i A_2) pa je i $\mathcal{L}(\mathbb{Z})$ komutativna algebra s jedinicom nad $\mathbb{Z}$. □

Propozicija 2.3.2. *Neka su $m, n \in \mathbb{R}$. Preslikavanje $f : \mathbb{R}^2 \to \mathbb{R}$*

$$f(x_1, x_2) = x_1^2 + mx_1x_2 + nx_2^2 \tag{2.4}$$

je bilinearna kvadratna forma koja dopušta kompoziciju, to jest koja za sve $x_i, y_i \in \mathbb{R}, i = 1, 2$, zadovoljava identitet

$$f(x_1, x_2)f(y_1, y_2) = f(z_1, z_2), \tag{2.5}$$

gdje su

$$z_1 = x_1y_1 - nx_2y_2, \quad z_2 = x_1y_2 + x_2y_1 + mx_2y_2. \tag{2.6}$$

Za $m, n \in \mathbb{Z}$ formulom (2.4) *je dobro definirana i cjelobrojna forma koja dopušta kompoziciju $f : \mathbb{Z}^2 \to \mathbb{Z}$.*

Dokaz. Uz oznake iz propozicije 2.3.1, vrijedi

$$\det(x_1A_1 + x_2A_2) = \det\begin{bmatrix} x_1 & x_2 \\ -nx_2 & x_1 + mx_2 \end{bmatrix} = x_1^2 + mx_1x_2 + nx_2^2.$$

Sada tvrdnja slijedi prema propoziciji 2.3.1 i teoremima 2.2.1 i 2.2.3.
Pokažimo još kako dobiti formule (2.6):

$$(x_1A_1 + x_2A_2)(y_1A_1 + y_2A_2) = z_1A_1 + z_2A_2,$$

$$\begin{aligned} x_1y_1A_1^2 + x_1y_2A_1A_2 + x_2y_1A_2A_1 + x_2y_2A_2^2 &= x_1y_1A_1 + x_1y_2A_2 + x_2y_1A_2 + x_2y_2(-nA_1 + mA_2) \\ &= (\underbrace{x_1y_1 - nx_2y_2}_{z_1})A_1 + (\underbrace{x_1y_2 + x_2y_1 + mx_2y_2}_{z_2})A_2. \end{aligned}$$

□

Možemo uočiti da je forma iz primjera 2.1.3 specijalan slučaj forme iz prethodne propozicije za $m = 0$ i $n = -d$.

Primjer 2.3.3. *Neka su*

$$A_1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad A_2 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \; A_3 = A_1 + A_2 = \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix},$$

te forma $f(x_1, x_2, x_3) = \det(x_1A_1 + x_2A_2 + x_3A_3)$. Odredite z_1, z_2, z_3 kao bilinearne forme u varijablama x_i, y_i tako da vrijedi identititet $f(x_1, x_2, x_3)f(y_1, y_2, y_3) = f(z_1, z_2, z_3)$.

Rješenje. Vrijedi da je

$$(x_1A_1 + x_2A_2 + x_3A_3)(y_1A_1 + y_2A_2 + y_3A_3) = z_1A_1 + z_2A_2 + z_3A_3,$$

odnosno

$$((x_1 + x_3)A_1 + (x_2 + x_3)A_2)((y_1 + y_3)A_1 + (y_2 + y_3)A_2) = (z_1 + z_3)A_1 + (z_2 + z_3)A_2.$$

Kako je $A_1A_2 = A_2A_1 = A_2$ i $A_2^2 = A_1$ lijeva strana u prethodnom izrazu jednaka je

$$((x_1 + x_3)(y_1 + y_3) + (x_2 + x_3)(y_2 + y_3))A_1 + ((x_1 + x_3)(y_2 + y_3) + (x_2 + x_3)(y_1 + y_3))A_2.$$

Budući da je skup $\{A_1, A_2\}$ linearno nezavisan slijedi

$$\begin{aligned}(x_1 + x_3)(y_1 + y_3) + (x_2 + x_3)(y_2 + y_3) &= z_1 + z_3,\\ (x_1 + x_3)(y_2 + y_3) + (x_2 + x_3)(y_1 + y_3) &= z_2 + z_3.\end{aligned}$$

Očito prikaz varijabli kao bilinearnih formi u varijablama x_i, y_i nije jedinstven, a to je u skladu s napomenom 2.2.2. (Možemo varirati izbor forme z_3). Na primjer, vrijedi

$$\begin{aligned}z_1 &= x_1y_1 + x_2y_2,\\ z_2 &= x_2y_1 + x_1y_2,\\ z_3 &= x_3y_1 + x_3y_2 + x_1y_3 + x_2y_3 + 2x_3y_3.\end{aligned}$$

□

Propozicija 2.3.4. *Neka su* $\lambda_i \in \mathbb{R}$, $i = 1, \ldots, 5$ *te*

$$A_1 = I_3 = \begin{bmatrix}1 & 0 & 0\\ 0 & 1 & 0\\ 0 & 0 & 1\end{bmatrix},$$

$$A_2 = \begin{bmatrix}0 & 1 & 0\\ -\lambda_3(\lambda_1 - \lambda_2 - \lambda_3 + \lambda_5) & \lambda_1 & \lambda_3\\ -\lambda_3(\lambda_2 - \lambda_4) & \lambda_2 & \lambda_3\end{bmatrix},$$

$$A_3 = \begin{bmatrix}0 & 0 & 1\\ -\lambda_3(\lambda_2 - \lambda_4) & \lambda_2 & \lambda_3\\ -\lambda_1\lambda_4 + \lambda_2^2 - \lambda_2\lambda_5 + \lambda_3\lambda_4 & \lambda_4 & \lambda_5\end{bmatrix}.$$

Tada je $\mathcal{L} = [\{A_1, A_2, A_3\}]$ *komutativna podalgebra s jedinicom algebre* $M_3(\mathbb{R})$.

Ako su $\lambda_i \in \mathbb{Z}$, $i = 1, \ldots, 5$, $\mathcal{L}(\mathbb{Z})$ *je komutativna podalgebra s jedinicom algebre* $M_3(\mathbb{Z})$.

Dokaz. Pokazujemo da je $\mathcal{L}$ podalgebra od $M_3(\mathbb{R})$. Za to je prema lemi 1.2.3 dovoljno ustanoviti da je $A_iA_j \in \mathcal{L}$ za $i, j \in 1, 2, 3$. Očito je $A_1A_2 = A_2A_1 = A_2 \in \mathcal{L}$ i $A_1A_3 = A_3A_1 = A_3 \in \mathcal{L}$, a

$$A_2^2 = \lambda_3(-\lambda_1 + \lambda_2 + \lambda_3 - \lambda_5)I_3 + \lambda_1A_2 + \lambda_3A_3 \in \mathcal{L}, \tag{2.7}$$

$$A_3A_2 = A_2A_3 = (-\lambda_2\lambda_3 + \lambda_3\lambda_4)I_3 + \lambda_2A_2 + \lambda_3A_3 \in \mathcal{L}, \tag{2.8}$$

$$A_3^2 = (\lambda_2^2 - \lambda_1\lambda_4 + \lambda_3\lambda_4 - \lambda_2\lambda_5)I_3 + \lambda_4A_2 + \lambda_5A_3 \in \mathcal{L}. \tag{2.9}$$

Nadalje, množenje u $\mathcal{L}$ je komutativno i $\mathcal{L}$ posjeduje neutralni element množenja.

U slučaju $\lambda_i \in \mathbb{Z},\ i = 1, \ldots, 5$, iz (2.7) vidimo da se svi umnošci A_iA_j mogu prikazati kao cjelobrojne linearne kombinacije matrica A_1, A_2, A_3 pa je $\mathcal{L}(\mathbb{Z})$ komutativna podalgebra s jedinicom algebre $M_3(\mathbb{Z})$. □

Propozicija 2.3.5. *Neka su $\lambda_i \in \mathbb{R}, i = 1, \ldots, 5$. Preslikavanje $f : \mathbb{R}^3 \to \mathbb{R}$*

$$\begin{aligned} f(x_1,\ x_2,\ x_3) = {} & x_1^3 + (\lambda_1 + \lambda_3)x_1^2x_2 + (\lambda_2 + \lambda_5)x_1^2x_3 \\ & + \lambda_3(2\lambda_1 - 2\lambda_2 - \lambda_3 + \lambda_5)x_1x_2^2 + (\lambda_1\lambda_5 + 2\lambda_2\lambda_3 - 3\lambda_3\lambda_4)x_1x_2x_3 \\ & + (\lambda_1\lambda_4 - \lambda_2^2 + 2\lambda_2\lambda_5 - 2\lambda_3\lambda_4)x_1x_3^2 + \lambda_3^2(\lambda_1 - 2\lambda_2 - \lambda_3 + \lambda_4 + \lambda_5)x_2^3 \\ & - \lambda_3(2\lambda_1\lambda_4 - \lambda_1\lambda_5 - 2\lambda_2^2 - \lambda_2\lambda_3 + 3\lambda_2\lambda_5 - \lambda_3\lambda_4 + \lambda_3\lambda_5 - \lambda_5^2)x_2^2x_3 \\ & + (\lambda_1^2\lambda_4 - \lambda_1\lambda_2^2 + \lambda_1\lambda_2\lambda_5 - 3\lambda_1\lambda_3\lambda_4 + \lambda_2^2\lambda_3 + \lambda_2\lambda_3\lambda_4 \\ & + 2\lambda_3^2\lambda_4 - 2\lambda_3\lambda_4\lambda_5)x_2x_3^2 + (\lambda_1\lambda_2\lambda_4 - \lambda_2^3 + \lambda_2^2\lambda_5 - 2\lambda_2\lambda_3\lambda_4 + \lambda_3\lambda_4^2)x_3^3, \end{aligned} \tag{2.10}$$

je ternarna kubična forma koja dopušta kompoziciju, odnosno koja za sve $x_i, y_i \in \mathbb{R}, i = 1, 2, 3$, zadovoljava identitet

$$f(x_1, x_2, x_3)f(y_1, y_2, y_3) = f(z_1, z_2, z_3),$$

gdje su

$$\begin{aligned} z_1 = {} & x_1y_1 - \lambda_3(\lambda_1 - \lambda_2 - \lambda_3 + \lambda_5)x_2y_2 - \lambda_3(\lambda_2 - \lambda_4)x_2y_3 \\ & - \lambda_3(\lambda_2 - \lambda_4)x_3y_2 + (-\lambda_1\lambda_4 + \lambda_2^2 - \lambda_2\lambda_5 + \lambda_3\lambda_4)x_3y_3, \\ z_2 = {} & x_1y_2 + x_2y_1 + \lambda_1x_2y_2 + \lambda_2x_2y_3 + \lambda_2x_3y_2 + \lambda_4x_3y_3, \\ z_3 = {} & x_1y_3 + \lambda_3x_2y_2 + \lambda_3x_2y_3 + x_3y_1 + \lambda_3x_3y_2 + \lambda_5x_3y_3. \end{aligned}$$

Za $\lambda_i \in \mathbb{Z}, i = 1, \ldots, 5$ Formulom (2.10) *je dobro definirana i cjelobrojna forma koja dopušta kompoziciju $f : \mathbb{Z}^3 \to \mathbb{Z}$.*

Dokaz. Uz oznake iz propozicije 2.3.4 vrijedi

$$\det(x_1A_1 + x_2A_2 + x_3A_3) = f(x_1, x_2, x_3).$$

Sada tvrdnja slijedi prema propoziciji 2.3.1 i teoremima 2.2.1 i 2.2.3. □

2.4 Kroneckerov produkt

Definicija 2.4.1. *Neka su* $A = [a_{ij}]$ *i* $B = [b_{ij}]$ *matrice tipa* (m, n) *i* (p, q)*, respektivno.* Kroneckerov produkt *matrica A i B je blok matrica* $C = [c_{ij}]$ *tipa* (mp, nq) *koja je dana sljedećim oblikom:*

$$C = \begin{bmatrix} a_{11}B & \cdots & a_{1n}B \\ \vdots & \ddots & \vdots \\ a_{m1}B & \cdots & a_{mn}B \end{bmatrix}. \tag{2.11}$$

Pišemo $C = A \otimes B$*. Na ovaj način smo definirali operaciju* Kroneckerovog produkta *matrica*

$$\otimes : M_{m,n}(\mathbb{F}) \times M_{p,q}(\mathbb{F}) \to M_{mp,nq}(\mathbb{F}).$$

Primjer 2.4.2. *Zadane su matrice* $A = \begin{bmatrix} 1 & 2 \\ 0 & 4 \end{bmatrix}, B = \begin{bmatrix} 0 & 5 \\ 6 & 7 \end{bmatrix}$*. Tada je*

$$A \otimes B = \begin{bmatrix} 1 & 2 \\ 0 & 4 \end{bmatrix} \otimes \begin{bmatrix} 0 & 5 \\ 6 & 7 \end{bmatrix} = \begin{bmatrix} 1 \cdot \begin{bmatrix} 0 & 5 \\ 6 & 7 \end{bmatrix} & 2 \cdot \begin{bmatrix} 0 & 5 \\ 6 & 7 \end{bmatrix} \\ 0 \cdot \begin{bmatrix} 0 & 5 \\ 6 & 7 \end{bmatrix} & 4 \cdot \begin{bmatrix} 0 & 5 \\ 6 & 7 \end{bmatrix} \end{bmatrix} =$$

$$= \begin{bmatrix} 1 \cdot 0 & 1 \cdot 5 & 2 \cdot 0 & 2 \cdot 5 \\ 1 \cdot 6 & 1 \cdot 7 & 2 \cdot 6 & 2 \cdot 7 \\ 0 \cdot 0 & 0 \cdot 5 & 4 \cdot 0 & 4 \cdot 5 \\ 0 \cdot 6 & 0 \cdot 7 & 4 \cdot 6 & 4 \cdot 7 \end{bmatrix} = \begin{bmatrix} 0 & 5 & 0 & 10 \\ 6 & 7 & 12 & 14 \\ 0 & 0 & 0 & 20 \\ 0 & 0 & 24 & 28 \end{bmatrix}$$

Propozicija 2.4.3. *Neka su* $A \in M_{mn}(\mathbb{F}), B \in M_{pq}(\mathbb{F}), C \in M_{rs}(\mathbb{F})$ *te* $\alpha \in \mathbb{F}$*. Vrijedi:*

1. $(\alpha A) \otimes B = A \otimes (\alpha B) = \alpha(A \otimes B)$
2. $(A \otimes B)^t = A^t \otimes B^t$
3. $(A \otimes B)^* = A^* \otimes B^*$
4. $(A \otimes B) \otimes C = A \otimes (B \otimes C)$
5. $(A + B) \otimes C = A \otimes C + B \otimes C$
6. $A \otimes (B + C) = A \otimes B + A \otimes C$.

Dokaz. Sva svojstva dokazuju se direktnim raspisivanjem.

1.

$$(\alpha A)\otimes B=\begin{bmatrix}\alpha a_{11}B & \cdots & \alpha a_{1n}B\\ \vdots & \ddots & \vdots\\ \alpha a_{m1}B & \cdots & \alpha a_{mn}B\end{bmatrix}=\begin{bmatrix}a_{11}(\alpha B) & \cdots & a_{1n}(\alpha B)\\ \vdots & \ddots & \vdots\\ a_{m1}(\alpha B) & \cdots & a_{mn}(\alpha B)\end{bmatrix}=A\otimes(\alpha B)$$

$$(\alpha A)\otimes B=\begin{bmatrix}\alpha a_{11}B & \cdots & \alpha a_{1n}B\\ \vdots & \ddots & \vdots\\ \alpha a_{m1}B & \cdots & \alpha a_{mn}B\end{bmatrix}=\alpha\begin{bmatrix}a_{11}B & \cdots & a_{1n}B\\ \vdots & \ddots & \vdots\\ a_{m1}B & \cdots & a_{mn}B\end{bmatrix}=\alpha(A\otimes B)$$

2.

$$(A\otimes B)^t=\begin{bmatrix}a_{11}B & \cdots & a_{1n}B\\ \vdots & \ddots & \vdots\\ a_{m1}B & \cdots & a_{mn}B\end{bmatrix}^t=\begin{bmatrix}a_{11}b_{11} & \cdots & a_{11}b_{1q} & \cdots & a_{1n}b_{11} & \cdots & a_{1n}b_{1q}\\ \vdots & \ddots & \vdots & & \vdots & \ddots & \vdots\\ a_{11}b_{p1} & \cdots & a_{11}b_{pq} & \cdots & a_{1n}b_{p1} & \cdots & a_{1n}b_{pq}\\ \vdots & & \vdots & \ddots & \vdots & & \vdots\\ a_{m1}b_{11} & \cdots & a_{m1}b_{1q} & \cdots & a_{mn}b_{11} & \cdots & a_{mn}b_{1q}\\ \vdots & \ddots & \vdots & & \vdots & \ddots & \vdots\\ a_{m1}b_{p1} & \cdots & a_{m1}b_{pq} & \cdots & a_{mn}b_{p1} & \cdots & a_{mn}b_{pq}\end{bmatrix}^t=$$

$$=\begin{bmatrix}a_{11}b_{11} & \cdots & a_{11}b_{p1} & \cdots & a_{m1}b_{11} & \cdots & a_{m1}b_{p1}\\ \vdots & \ddots & \vdots & & \vdots & \ddots & \vdots\\ a_{11}b_{1q} & \cdots & a_{11}b_{pq} & \cdots & a_{m1}b_{1q} & \cdots & a_{m1}b_{pq}\\ \vdots & & \vdots & \ddots & \vdots & & \vdots\\ a_{1n}b_{11} & \cdots & a_{1n}b_{p1} & \cdots & a_{mn}b_{11} & \cdots & a_{mn}b_{p1}\\ \vdots & \ddots & \vdots & & \vdots & \ddots & \vdots\\ a_{1n}b_{1q} & \cdots & a_{1n}b_{pq} & \cdots & a_{mn}b_{1q} & \cdots & a_{mn}b_{pq}\end{bmatrix}=\begin{bmatrix}a_{11}B^t & \cdots & a_{m1}B^t\\ \vdots & \ddots & \vdots\\ a_{1n}B^t & \cdots & a_{mn}B^t\end{bmatrix}=A^t\otimes B^t$$

3. analogno kao 2.

4.

$$(A\otimes B)\otimes C=\begin{bmatrix}a_{11}B & \cdots & a_{1n}B\\ \vdots & \ddots & \vdots\\ a_{m1}B & \cdots & a_{mn}B\end{bmatrix}\otimes C=\begin{bmatrix}a_{11}b_{11} & \cdots & a_{11}b_{1q} & \cdots & a_{1n}b_{11} & \cdots & a_{1n}b_{1q}\\ \vdots & \ddots & \vdots & & \vdots & \ddots & \vdots\\ a_{11}b_{p1} & \cdots & a_{11}b_{pq} & \cdots & a_{1n}b_{p1} & \cdots & a_{1n}b_{pq}\\ \vdots & & \vdots & \ddots & \vdots & & \vdots\\ a_{m1}b_{11} & \cdots & a_{m1}b_{1q} & \cdots & a_{mn}b_{11} & \cdots & a_{mn}b_{1q}\\ \vdots & \ddots & \vdots & & \vdots & \ddots & \vdots\\ a_{m1}b_{p1} & \cdots & a_{m1}b_{pq} & \cdots & a_{mn}b_{p1} & \cdots & a_{mn}b_{pq}\end{bmatrix}\otimes C=$$

$$= \begin{bmatrix} a_{11}b_{11}C & \cdots & a_{11}b_{1q}C & \cdots & a_{1n}b_{11}C & \cdots & a_{1n}b_{1q}C \\ \vdots & \ddots & \vdots & & \vdots & \ddots & \vdots \\ a_{11}b_{p1}C & \cdots & a_{11}b_{pq}C & \cdots & a_{1n}b_{p1}C & \cdots & a_{1n}b_{pq}C \\ \vdots & & \vdots & \ddots & \vdots & & \vdots \\ a_{m1}b_{11}C & \cdots & a_{m1}b_{1q}C & \cdots & a_{mn}b_{11}C & \cdots & a_{mn}b_{1q}C \\ \vdots & \ddots & \vdots & & \vdots & \ddots & \vdots \\ a_{m1}b_{p1}C & \cdots & a_{m1}b_{pq}C & \cdots & a_{mn}b_{p1}C & \cdots & a_{mn}b_{pq}C \end{bmatrix} =$$

$$= \begin{bmatrix} a_{11}\begin{bmatrix} b_{11}C & \cdots & b_{1q}C \\ \vdots & \ddots & \vdots \\ b_{p1}C & \cdots & b_{pq}C \end{bmatrix} & \cdots & a_{1n}\begin{bmatrix} b_{11}C & \cdots & b_{1q}C \\ \vdots & \ddots & \vdots \\ b_{p1}C & \cdots & b_{pq}C \end{bmatrix} \\ \vdots & \ddots & \vdots \\ a_{m1}\begin{bmatrix} b_{11}C & \cdots & b_{1q}C \\ \vdots & \ddots & \vdots \\ b_{p1}C & \cdots & b_{pq}C \end{bmatrix} & \cdots & a_{mn}\begin{bmatrix} b_{11}C & \cdots & b_{1q}C \\ \vdots & \ddots & \vdots \\ b_{p1}C & \cdots & b_{pq}C \end{bmatrix} \end{bmatrix} = \begin{bmatrix} a_{11}(B\otimes C) & \cdots & a_{1n}(B\otimes C) \\ \vdots & \ddots & \vdots \\ a_{m1}(B\otimes C) & \cdots & a_{mn}(B\otimes C) \end{bmatrix} =$$

$$= A \otimes (B \otimes C)$$

5.

$$(A+B)\otimes C = \begin{bmatrix} (a_{11}+b_{11})C & \cdots & (a_{1n}+b_{1q})C \\ \vdots & \ddots & \vdots \\ (a_{m1}+b_{p1})C & \cdots & (a_{mn}+b_{pq})C \end{bmatrix} =$$

$$= \begin{bmatrix} a_{11}C & \cdots & a_{m1}C \\ \vdots & \ddots & \vdots \\ a_{1n}C & \cdots & a_{mn}C \end{bmatrix} + \begin{bmatrix} b_{11}C & \cdots & b_{1q}C \\ \vdots & \ddots & \vdots \\ b_{p1}C & \cdots & b_{pq}C \end{bmatrix} = (A\otimes C) + (B\otimes C)$$

6.

$$A\otimes(B+C) = \begin{bmatrix} A(b_{11}+c_{11}) & \cdots & A(b_{1n}+c_{1q}) \\ \vdots & \ddots & \vdots \\ A(b_{m1}+c_{p1}) & \cdots & A(b_{mn}+c_{pq}) \end{bmatrix} =$$

$$= \begin{bmatrix} Ab_{11} & \cdots & Ab_{m1} \\ \vdots & \ddots & \vdots \\ Ab_{1n} & \cdots & Ab_{mn} \end{bmatrix} + \begin{bmatrix} Ac_{11} & \cdots & Ac_{1q} \\ \vdots & \ddots & \vdots \\ Ac_{p1} & \cdots & Ac_{pq} \end{bmatrix} = (A\otimes C) + (B\otimes C)$$

□

Propozicija 2.4.4. *Neka su* $A \in M_{mn}(\mathbb{F}), B \in M_{pq}(\mathbb{F}), C \in M_{nk}(\mathbb{F})$ *i* $D \in M_{qr}(\mathbb{F})$. *Tada vrijedi:*

$$(A\otimes B)(C\otimes D) = AC \otimes BD.$$

Dokaz. Neka je $A = [a_{ih}]$, $C = \left[c_{hj}\right]$. Tada je $A \otimes B = [a_{ih}B]$, $C \otimes D = [c_{ih}D]$ i vrijedi

$$[(A \otimes B)(C \otimes D)]_{ij} = \sum_{h=1}^{n} a_{ih}B\, c_{hj}D = \left[\sum_{h=1}^{n} a_{ih}c_{hj}\right] BD = [AC \otimes BD]_{ij}\,.$$

Dakle vrijedi $(A \otimes B)(C \otimes D) = AC \otimes BD$. □

Propozicija 2.4.5. *$A \otimes B = 0$ ako i samo ako je $A = 0$ ili $B = 0$.*

Dokaz. Slijedi direktno iz definicije 2.4.1. □

Propozicija 2.4.6. *Neka je $\{B_1, \ldots, B_k\}$ linearno nezavisan skup matrica i $A_1 \otimes B_1 + \cdots + A_k \otimes B_k = 0$, tada je $A_1 = \cdots = A_k = 0$.*

Dokaz. Pretpostavimo da je $A_\ell = [a_{ij}^{(\ell)}]$ tipa (m, n) i $B_\ell = [b_{ij}^{(\ell)}]$ tipa (p, q). Tada je prema (2.11)

$$A_\ell \otimes B_\ell = \begin{bmatrix} a_{11}^{(\ell)}B_\ell & \cdots & a_{1n}^{(\ell)}B_\ell \\ \vdots & \ddots & \vdots \\ a_{m1}^{(\ell)}B_\ell & \cdots & a_{mn}^{(\ell)}B_\ell \end{bmatrix} = \begin{bmatrix} a_{11}^{(\ell)}b_{11}^{(\ell)} & \cdots & a_{11}^{(\ell)}b_{1q}^{(\ell)} & \cdots \\ \vdots & \ddots & \vdots & \\ a_{11}^{(\ell)}b_{p1}^{(\ell)} & \cdots & a_{11}^{(\ell)}b_{pq}^{(\ell)} & \cdots \\ \vdots & & \vdots & \ddots \end{bmatrix}.$$

Promatramo li prvi blok matrice dobivene sumom Kroneckerovih produkata $A_1 \otimes B_1 + \cdots + A_k \otimes B_k = 0$ dobivamo

$$\sum_{\ell=1}^{k} a_{11}^{(\ell)}B_\ell = a_{11}^{(1)}B_1 + a_{11}^{(2)}B_2 + \cdots + a_{11}^{(k)}B_k = 0.$$

Budući da je $\{B_1, \ldots, B_k\}$ linearno nezavisan skup slijedi

$$a_{11}^{(1)} = a_{11}^{(2)} = \cdots = a_{11}^{(k)} = 0.$$

Analogno vrijedi za svaki blok na mjestu (i, j), $i \in \{1, \ldots, m\}$, $j \in \{1, \ldots, n\}$, pa je

$$a_{ij}^{(\ell)} = 0, \text{ za sve } i = 1, \ldots, m,\ j = 1, \ldots, n,\ \ell = 1, \ldots, k,$$

odnosno

$$A_1 = \cdots = A_k = 0.$$

□

Korolar 2.4.7. *Neka su $\{A_1, A_2, \ldots, A_h\}$ i $\{B_1, B_2, \ldots, B_k\}$ linearno nezavisni skupovi matrica u $M_{mn}(\mathbb{F})$ i $M_{pq}(\mathbb{F})$, respektivno. Tada je skup $\{A_i \otimes B_j : i = 1, \ldots, h, j = 1, \ldots, k\}$ linearno nezavisni u $M_{mp,nq}(\mathbb{F})$.*

Dokaz. Neka je

$$\sum_{i=1}^{h}\sum_{j=1}^{k}\alpha_{ij}A_i\otimes B_j = 0.$$

Kako je $\{B_1, B_2, \ldots, B_k\}$ linearno nezavisan skup i

$$\sum_{i=1}^{h}\sum_{j=1}^{k}\alpha_{ij}A_i\otimes B_j = \sum_{j=1}^{k}\left(\sum_{i=1}^{h}\alpha_{ij}A_i\right)\otimes B_j = \left(\sum_{i=1}^{h}\alpha_{i1}A_i\right)\otimes B_1 + \cdots + \left(\sum_{i=1}^{h}\alpha_{ik}A_i\right)\otimes B_k,$$

prema propoziciji 2.4.6 slijedi da je

$$\sum_{i=1}^{h}\alpha_{i1}A_i = 0, \sum_{i=1}^{h}\alpha_{i2}A_i = 0, \ldots, \sum_{i=1}^{h}\alpha_{ik}A_i = 0.$$

Nadalje, iz prethodnih jednakosti i činjenice da je i skup $\{A_1, A_2, \ldots, A_h\}$ linearno nezavisan slijedi da je $\alpha_{ij} = 0$ za sve $i = 1, \ldots, h$, $j = 1, \ldots, k$. □

2.5 Primjeri formi višeg stupnja

Koristeći Kroneckerov produkt konstruirat ćemo komutativne algebre s jedinicom matrica tipa (m, n) kombinirajući komutativne podalgebre od $M_n(\mathbb{R})$ i $M_m(\mathbb{R})$ koje smo opisali u odjeljku 2.3.

Teorem 2.5.1. *Neka su $\{A_1 = I_n, A_2, \ldots, A_h\}$ i $\{B_1 = I_m, B_2, \ldots, B_k\}$ linearno nezavisni skupovi matrica iz $M_n(\mathbb{R})$ i $M_m(\mathbb{R})$ respektivno, takvi da su*

$$\mathcal{L}_n = [\{A_1 = I_n, A_2, \ldots, A_h\}],$$
$$\mathcal{L}_m = [\{B_1 = I_m, B_2, \ldots, B_k\}]$$

komutativne podalgebre od $M_n(\mathbb{R})$ i $M_m(\mathbb{R})$, respektivno. Tada je

$$\mathcal{L} = \left[\left\{B_i\otimes A_j, i = 1, \ldots, k, j = 1, \ldots, h\right\}\right]$$

komutativna podalgebra s jedinicom od $M_{mn}(\mathbb{R})$.

Dokaz. Pokazujemo da je $\mathcal{L}$ podalgebra od $M_{mn}(\mathbb{R})$. Za to je prema lemi 1.2.3 dovoljno ustanoviti da je skup $\mathcal{S} = \left\{B_i\otimes A_j, i = 1, \ldots, k, j = 1, \ldots, h\right\}$ linearno nezavisan i da je $(B_{i_1}\otimes A_{j_1})(B_{i_2}\otimes A_{j_2}) \in \mathcal{L}$ za $i_1, i_2 \in \{1, 2, \ldots, h\}$, $j_1, j_2 \in \{1, 2, \ldots, k\}$.

Prema Korolaru 2.4.7 slijedi da skup $\mathcal{S}$ linearno nezavisan skup. Kako $\mathcal{S}$ ima $k\cdot h$ elemenata, vektorski potprostor $\mathcal{L}$ je dimenzije kh.

Budući da su $\mathcal{L}_n$ i $\mathcal{L}_m$ komutativne podalgebre od $M_n(\mathbb{R})$ i $M_m(\mathbb{R})$, vrijedi:

$$A_{j_1}A_{j_2} = A_{j_2}A_{j_1} \in \mathcal{L}_n,$$

$$B_{i_1}B_{i_2} = B_{i_2}B_{i_1} \in \mathcal{L}_m,$$

za $i_1, i_2 \in \{1, 2, \ldots, h\}$, $j_1, j_2 \in \{1, 2, \ldots, k\}$. Stoga te umnoške možemo zapisati kao

$$A_{j_1}A_{j_2} = \sum_{j=1}^{h} s_j A_j, s_j \in \mathbb{R},$$

$$B_{i_1}B_{i_2} = \sum_{i=1}^{k} r_i B_i, r_i \in \mathbb{R}.$$

Zbog leme 2.4.4 vrijedi:

$$(B_{i_1} \otimes A_{j_1})(B_{i_2} \otimes A_{j_2}) = (B_{i_1}B_{i_2}) \otimes (A_{j_1}A_{j_2}) = \left(\sum_{i=1}^{k} r_i B_i\right) \otimes \left(\sum_{j=1}^{h} s_j A_j\right).$$

Zbog prvog, petog i šestog svojstva iz propozicije 2.4.3 vrijedi sljedeće:

$$(B_{i_1} \otimes A_{j_1})(B_{i_2} \otimes A_{j_2}) = \sum_{i=1}^{k}\sum_{j=1}^{h} r_i s_j (B_i \otimes A_j) \in \mathcal{L}.$$

Kako vrijedi $A_{j_1}A_{j_2} = A_{j_2}A_{j_1}$ i $B_{i_1}B_{i_2} = B_{i_2}B_{i_1}$, uz lemu 2.4.4 lako slijedi

$$(B_{i_1} \otimes A_{j_1})(B_{i_2} \otimes A_{j_2}) = (B_{i_2} \otimes A_{j_2})(B_{i_1} \otimes A_{j_1}).$$

Neutralni element za množenje se nalazi u skupu $\mathcal{L}$. Naime $B_1 \otimes A_1 = I_m \otimes I_n = I_{mn}$. □

Korolar 2.5.2. *Neka je $\{A_1 = I_n, A_2, \ldots, A_h\}$ skup linearno nezavisnih matrica iz $M_n(\mathbb{Z})$ takav da je $[\{A_1, A_2, \ldots, A_h\}]$ komutativna podalgebra s jedinicom od $M_n(\mathbb{R})$ i neka je*

$$C(x_i) = \begin{bmatrix} A(x_1, \ldots, x_h) & A(x_{h+1}, \ldots, x_{2h}) \\ -qA(x_{h+1}, \ldots, x_{2h}) & A(x_1, \ldots, x_h) + pA(x_{h+1}, \ldots, x_{2h}) \end{bmatrix},$$

gdje je $A(x_1, \ldots, x_h) = \sum_{j=1}^{h} x_j A_j$ te $p, q \in \mathbb{Z}$.

Preslikavanje $f : \mathbb{R}^{2h} \to \mathbb{R}$

$$f(x_1, \ldots, x_{2h}) = \det(C(x_1, \ldots, x_{2h}))$$

je forma koja dopušta kompoziciju stupnja $2n$ u $2h$-varijabli.

Dokaz. Neka su matrice $B_1 = I_2, B_2 = \begin{bmatrix} 0 & 1 \\ -q & p \end{bmatrix}$. Prema lemi 2.3.1 $[\{B_1, B_2\}]$ je komutativna podalgebra od $M_2(\mathbb{R})$. Sada prema teoremu 2.5.1 slijedi i da je

$$\mathcal{L} = \left[\left\{B_i \otimes A_j, i = 1, 2, j = 1, \ldots, h\right\}\right]$$

komutativna podalgebra od $M_{2n}(\mathbb{R})$. Matricu $C(x_1, \ldots, x_{2h}) \in \mathcal{L}$ možemo zapisati kao:

$$\begin{aligned} C(x_1, x_2, \ldots, x_{2h}) &= \sum_{j=1}^{h} x_j B_1 \otimes A_j + \sum_{j=1}^{h} x_{h+j} B_2 \otimes A_j \\ &= B_1 \otimes \sum_{j=1}^{h} x_j A_j + B_2 \otimes \sum_{j=1}^{h} x_{h+j} A_j \\ &= B_1 \otimes A(x_1, \ldots, x_h) + B_2 \otimes A(x_{h+1}, \ldots, x_{2h}), \end{aligned}$$

čime dobivamo zapis matrice C koji je jednak onom iz pretpostavke. Sada prema teoremu 2.2.1 slijedi tvrdnja. □

Propozicija 2.5.3. *Neka su $m, n, p, q \in \mathbb{Z}$ te*

$$C_1 = I_4, \qquad C_2 = \begin{bmatrix} 0 & 1 & 0 & 0 \\ -n & m & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & -n & m \end{bmatrix},$$

$$C_3 = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ -q & 0 & p & 0 \\ 0 & -q & 0 & p \end{bmatrix}, \qquad C_4 = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & -n & m \\ 0 & -q & 0 & p \\ qn & -qm & -pn & pm \end{bmatrix}.$$

Tada je $\mathcal{L} = [\{C_1, C_2, C_3, C_4\}]$ komutativna podalgebra s jedinicom algebre $M_4(\mathbb{R})$. Nadalje preslikavanje $f : \mathbb{R}^3 \to \mathbb{R}$

$$f(x_1, x_2, x_3, x_4) = \det\left(x_1 C_1 + x_2 C_2 + x_3 C_3 + x_4 C_4\right)$$

je kvartarna kvartična forma koja dopušta kompoziciju, odnosno koja za sve $x_i, y_i \in \mathbb{R}, i = 1, 2, 3, 4$, zadovoljava identitet

$$f(x_1, x_2, x_3, x_4) f(y_1, y_2, y_3, y_4) = f(z_1, z_2, z_3, z_4),$$

gdje su

$$\begin{aligned}
z_1 &= x_1y_1 - nx_2y_2 - qx_3y_3 + qnx_4y_4,\\
z_2 &= x_1y_2 + x_2y_1 + mx_2y_2 - qx_3y_4 - qx_4y_3 - mqx_4y_4,\\
z_3 &= x_1y_3 - nx_2y_4 + x_3y_1 + px_3y_3 - nx_4y_2 - npx_4y_4,\\
z_4 &= x_1y_4 + x_2(y_3 + my_4) + x_3(y_2 + py_4) + x_4(y_1 + my_2 + py_3 + mpy_4).
\end{aligned}$$

Dokaz. Neka su matrice A_1, A_2 definirane kao u propoziciji 2.3.1, a matrice B_1, B_2 na analogan način

$$B_1 = I_2, B_2 = \begin{bmatrix} 0 & 1 \\ -q & p \end{bmatrix}.$$

Prema propoziciji 2.3.1 linearne ljuske $[\{A_1, A_2\}]$ i $[\{B_1, B_2\}]$ su komutativne podalgebre od $M_2(\mathbb{R})$. Nadalje primijetimo da je

$$C_1 = B_1 \otimes A_1, \quad C_2 = B_1 \otimes A_2, \quad C_3 = B_2 \otimes A_1, \quad C_4 = B_2 \otimes A_2.$$

Sada prema teoremu 2.5.1 slijedi da je $\mathcal{L}$ komutativna podalgebra s jedinicom od $M_4(\mathbb{R})$. A prema teoremu 2.2.1 slijedi da je f kvartartna kvartična forma koja dopušta kompoziciju. Vrijednosti z_i dobivamo direktnim računanjem. □

Propozicija 2.5.4. *Neka su matrice A_1, A_2, A_3 definirane kao u teoremu 2.3.4, neka je matrica $A(x_1, x_2, x_3) = x_1A_1 + x_2A_2 + x_3A_3$ i*

$$C(x_1, \ldots, x_6) = \begin{bmatrix} A(x_1, x_2, x_3) & A(x_4, x_5, x_6) \\ -qA(x_4, x_5, x_6) & A(x_1, x_2, x_3) + pA(x_4, x_5, x_6) \end{bmatrix}.$$

Preslikavanje $f : \mathbb{R}^6 \to \mathbb{R}$

$$f(x_1, x_2, \ldots, x_6) = \det(C(x_1, x_2, \ldots, x_6))$$

je šestorna sekstična forma koja dopušta kompoziciju.

Dokaz. Prema teoremu 2.3.4 slijedi da je $[\{A_1, A_2, A_3\}]$ komutativna podalgebra s jedinicom od $M_3(\mathbb{R})$. Sada prema korolaru 2.5.2 odmah slijedi tvrdnja. □

Poglavlje 3

Forme i neke diofantske jednadžbe

3.1 Grupa rješenja

Neka je $\{A_1 = I_n, A_2, \ldots, A_n\}$ skup linearno nezavisnih matrica reda n s cjelobrojnim elementima takvih da je

$$\mathcal{L}(\mathbb{Z}) = \{A(x_1, x_2, \ldots, x_n) = x_1A_1 + x_2A_2 + \ldots + x_nA_n : x_1, \ldots, x_n \in \mathbb{Z}\}$$

komutativna algebra s jedinicom nad $\mathbb{Z}$, odnosno podalgebra od $M_n(\mathbb{Z})$. Tada je funkcija

$$f(x_1, x_2, \ldots, x_n) = \det(A(x_1, x_2, \ldots, x_n))$$

forma koja dopušta kompoziciju stupnja n u varijablama $x_i, i = 1, \ldots, n$. Također neka prvi redci matrica $A_1 = I_n, A_2, \ldots, A_n$ čine kanonsku bazu vektorskog prostora $\mathbb{R}^n$, to jest

$$A_1 = I_n = \begin{bmatrix} 1 & 0 & \cdots & 0 \\ \vdots & \vdots & \cdots & \vdots \end{bmatrix}, A_2 = \begin{bmatrix} 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \cdots & \vdots \end{bmatrix}, \ldots, A_n = \begin{bmatrix} 0 & 0 & \cdots & 1 \\ \vdots & \vdots & \cdots & \vdots \end{bmatrix}.$$

Tada je očito

$$A(x_1, x_2, \ldots, x_n) = \begin{bmatrix} x_1 & x_2 & \cdots & x_n \\ \vdots & \vdots & \cdots & \vdots \end{bmatrix}. \tag{3.1}$$

Označimo sa S skup svih rješenja diofantske jednadžbe

$$f(x_1, x_2, \ldots, x_n) = 1,$$

odnosno

$$S = \{(x_1, x_2, \ldots, x_n) \in \mathbb{Z}^n : f(x_1, x_2, \ldots, x_n) = 1\}.$$

Na skupu S definiramo sljedeću operaciju:

$$(x_1, x_2, \ldots, x_n) * (y_1, y_2, \ldots, y_n) = (z_1, z_2, \ldots, z_n), \tag{3.2}$$

gdje su $z_1, z_2, \ldots, z_n$ određene relacijom

$$A(x_1, x_2, \ldots, x_n) \cdot A(y_1, y_2, \ldots, y_n) = A(z_1, z_2, \ldots, z_n), \tag{3.3}$$

za sve $(x_1, x_2, \ldots, x_n)$ i $(y_1, y_2, \ldots, y_n)$ iz skupa S.

Teorem 3.1.1. *Skup S je Abelova grupa s obzirom na operaciju $*$.*

Dokaz. Najprije ustanovimo da je n-torka $(x_1, \ldots, x_n)*(y_1, \ldots, y_n) = (z_1, \ldots, z_n)$ element skupa S za sve $(x_1, \ldots, x_n), (y_1, \ldots, y_n) \in S$. Budući da je skup $\mathcal{L}(\mathbb{Z}) = \{A(x_1, x_2, \ldots, x_n) : x_1, x_2, \ldots, x_n \in \mathbb{Z}\}$ zatvoren na operaciju množenja, slijedi da je $A(z_1, z_2, \ldots, z_n) \in \mathcal{L}(\mathbb{Z})$. Uz to, kako f dopušta kompoziciju, vrijedi

$$f(z_1, z_2, \ldots, z_n) = f(x_1, x_2, \ldots, x_n) \cdot f(y_1, y_2, \ldots, y_n) = 1,$$

pa je stoga $(z_1, z_2, \ldots, z_n) \in S$. Dakle, operacija definirana s (3.2) je *binarna operacija* na skupu S, to jest $* : S \times S \to S$.

Uočimo da je za određivanje vrijednosti od z_i, $i = 1, \ldots, n$, iz (3.3) dovoljno je izračunati samo prvi redak umnoška matrica $A(x_1, x_2, \ldots, x_n) \cdot A(y_1, y_2, \ldots, y_n)$.

Budući da je operacija množenja matrica asocijativna i komutativna u $\mathcal{L}(\mathbb{Z})$ tako je i operacija definirana nad skupom S također *asocijativna* i *komutativna*.

Element $(1, 0, \ldots, 0) \in S$ je *neutralni element* operacije $*$ budući da je $A(1, 0, \ldots, 0) = I_n$ neutralni element množenja matrica.

Ostalo je još samo za pokazati da svaki element skupa S ima *inverz* u skupu S. Budući da je $\det(A(x_1, x_2, \ldots, x_n)) = f(x_1, x_2, \ldots, x_n) = 1$ za svaki element $(x_1, x_2, \ldots, x_n) \in S$, matrica $A(x_1, x_2, \ldots, x_n)$ je invertibilna, odnosno njezin inverz postoji. Kao posljedica Cayley-Hamiltonova teorema inverz matrice $A(x_1, x_2, \ldots, x_n)$ moguće je zapisati kao linearnu kombinaciju matrica iz $\mathcal{L}$ što povlači $(A(x_1, x_2, \ldots, x_n))^{-1} \in \mathcal{L}$. Elementi matrice $A(x_1, \ldots, x_n)^{-1}$ su cijeli brojevi jer je

$$A(x_1, \ldots, x_n)^{-1} = \frac{1}{\det A(x_1, \ldots, x_n)} \tilde{A} = \tilde{A},$$

gdje je $\tilde{A}$ adjunkta matrice $A(x_1, \ldots, x_n)$ čiji su svi elementi po definiciji cjelobrojni. Stoga zbog (3.1) zaključujemo da je $A(x_1, \ldots, x_n)^{-1} \in \mathcal{L}(\mathbb{Z})$, to jest $A(x_1, \ldots, x_n)^{-1} = A(y_1, \ldots, y_n)$ za neke $y_1, \ldots, y_n \in \mathbb{Z}$. Konačno, $(y_1, \ldots, y_n) \in S$ jer je

$$\det A(y_1, \ldots, y_n) = \det\left(A(x_1, \ldots, x_n)^{-1}\right) = 1.$$

Dakle, $(S, *)$ je *Abelova grupa*. □

3.2 Primjeri

Primjer 3.2.1. *Zadane su matrice*

$$A_1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I_2, \quad A_2 = \begin{bmatrix} 0 & 1 \\ d & 0 \end{bmatrix},$$

gdje je d prirodni broj koji nije potpuni kvadrat. Tada je prema propoziciji 2.3.1

$$f(x_1, x_2) = \det(x_1 A_1 + x_2 A_2)$$

forma koja dopušta kompoziciju. Jednadžba $f(x_1, x_2) = 1$ *upravo predstavlja Pellovu jednadžbu*

$$x_1^2 - dx_2^2 = 1.$$

Skup svih cjelobrojnih rješenja te jednadžbe čini Abelovu grupu (teorem 3.1.1). Pellova jednadžba je uvijek rješiva u skupu prirodnih brojeva (prema teoremu 10.10 iz [2]). Pretpostavimo da je (u, v) *najmanje rješenje dane Pellove jednadžbe u prirodnim brojevima, tzv.* fundamentalno rješenje. *Stoga će i*

$$(u, v) * (u, v) = (x_1, x_2) \tag{3.4}$$

također biti rješenje Pellove jednadžbe. Raspisivanjem relacije (3.4) *dobivamo*

$$(uI_2 + vA_2)(uI_2 + vA_2) = x_1 I_2 + x_2 A_2,$$

odnosno

$$\begin{aligned} u^2 I_2 + 2uvA_2 + v^2 A_2^2 &= u^2 \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} + 2uv \begin{bmatrix} 0 & 1 \\ d & 0 \end{bmatrix} + v^2 \begin{bmatrix} d & 0 \\ 0 & d \end{bmatrix} \\ &= (u^2 + dv^2) I_2 + 2uvA_2. \end{aligned}$$

Stoga je $(x_1, x_2) = (u^2 + dv^2, 2uv)$. *Općenito, rješenja Pellove jednadžbe mogu se generirati formulom*

$$(uI_2 + vA_2)^n = x_1^{(n)} I_2 + x_2^{(n)} A_2, \ n \geq 1,$$

što se upravo poklapa s poznatom formulom za sva rješenja Pellove jednadžbe u skupu prirodnih brojeva

$$x_1^{(n)} + x_2^{(n)} \sqrt{d} = (u + v\sqrt{d})^n.$$

Napominjemo da ovim postupkom nismo opravdali da su gornjim formulama dana sva rješenja Pellove jednadžbe u skupu prirodnih brojeva. Dokaz te tvrdnje može se pronaći u [2], teorem 10.11.

Primjer 3.2.2. *Zadane su matrice*

$$A_1 = I_3 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix},\ A_2 = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix},\ A_3 = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}.$$

Prema propozicijama 2.3.4 i 2.3.5 za $(\lambda_1, \lambda_2, \lambda_3, \lambda_4, \lambda_5) = (1, 0, 1, 1, 0)$ *slijedi da cjelobrojna forma*

$$\begin{aligned} f(x_1, x_2, x_3) &= \det(x_1A_1 + x_2A_2 + x_3A_3) \\ &= x_1^3 + 2x_1^2x_2 + x_1x_2^2 + x_2^3 - 3x_1x_2x_3 - x_2^2x_3 - x_1x_3^2 + x_3^3 \end{aligned}$$

dopušta kompoziciju

$$f(x_1, x_2, x_3)f(y_1, y_2, y_3) = f(z_1, z_2, z_3),$$

gdje (z_1, z_2, z_3) *određujemo iz*

$$(x_1A_1 + x_2A_2 + x_3A_3)(y_1A_1 + y_2A_2 + y_3A_3) = z_1A_1 + z_2A_2 + z_3A_3.$$

Dovoljno je izračunati samo prvi redak matrice s lijeve strane i dobivamo

$$\begin{aligned} z_1 &= x_1y_1 + x_3y_2 + x_2y_3, \\ z_2 &= x_2y_1 + (x_1 + x_2)y_2 + x_3y_3, \\ z_3 &= x_3y_1 + (x_2 + x_3)y_2 + (x_1 + x_2)y_3. \end{aligned}$$

Uočimo da je $(0, 0, 1)$ *jedno rješenje jednadžbe* $f(x_1, x_2, x_3) = 1$*, a još beskonačno njih možemo dobiti iz prethodnih relacija. Za neko rješenje* (x_1, x_2, x_3) *i* $(y_1, y_2, y_3) = (0, 0, 1)$ *dobivamo da je i*

$$(z_1, z_2, z_3) = (x_2, x_3, x_1 + x_2)$$

rješenje, tj. $f(x_2, x_3, x_1 + x_2) = 1$*. Uz oznake kao u odjeljku 3.1 je*

$$(z_1, z_2, z_3) = (0, 0, 1) * (x_1, x_2, x_3).$$

Nadalje, formula

$$(x_1^{(n)}, x_2^{(n)}, x_3^{(n)}) = (0, 0, 1)^n = \underbrace{(0, 0, 1) * \cdots * (0, 0, 1)}_{n \text{ puta}},\ n \in \mathbb{N}$$

daje niz rješenja: $(0, 1, 0)$*,* $(1, 0, 1)$*,* $(0, 1, 1)$*,* $(1, 1, 1)$*,* $(1, 1, 2)$*,* $(1, 2, 2)$*,* $(2, 2, 3)$*,* $(2, 3, 4)$*,* $(3, 4, 5)$*, ...*

Napomena 3.2.3. *Ispis računa prethodnog primjera u programskom paketu* Wolfram Mathematica (Online),*https://www.wolframcloud.com/obj/wpl/GetStarted.nb?funnel=WPLGetStarted#sidebar=explorations*

```
In[3]:= A1 = IdentityMatrix[3]; A2 = {{0, 1, 0}, {0, 1, 1}, {1, 0, 1}}; A3 = {{0, 0, 1}, {1, 0, 1}, {0, 1, 0}};
        Det[x1 * A1 + x2 * A2 + x3 * A3]

Out[4]= x1^3 + 2 x1^2 x2 + x1 x2^2 + x2^3 - 3 x1 x2 x3 - x2^2 x3 - x1 x3^2 + x3^3

In[6]:= MatrixForm[Simplify[(x1 * A1 + x2 * A2 + x3 * A3) . (y1 * A1 + y2 * A2 + y3 * A3)]]

Out[6]//MatrixForm=
        ( x1 y1 + x3 y2 + x2 y3                 x1 y2 + x2 (y1 + y2) + x3 y3                 x3 (y1 + y2) + x1 y3 + x2 (y2 + y3)
          x3 (y1 + y2) + x1 y3 + x2 (y2 + y3)   x3 y2 + (x1 + x2) (y1 + y2) + (x2 + x3) y3   (x2 + x3) (y1 + y2) + x3 y3 + (x1 + x2) (y2 + y3)
          x1 y2 + x2 (y1 + y2) + x3 y3          x3 (y1 + y2) + x1 y3 + x2 (y2 + y3)          (x1 + x2) (y1 + y2) + x2 y3 + x3 (y2 + y3) )

In[8]:= {z1, z2, z3} = (x1 * A1 + x2 * A2 + x3 * A3) . (y1 * A1 + y2 * A2 + y3 * A3) [[1]]

Out[8]= {x1 y1 + x2 y2 + x3 y3, x3 y1 + (x1 + x2) y2 + (x2 + x3) y3, x2 y1 + x3 y2 + (x1 + x2) y3}

In[9]:= {x1, x2, x3} = {0, 0, 1}; Det[x1 * A1 + x2 * A2 + x3 * A3]

Out[9]= 1

In[10]:= {y1, y2, y3} = {0, 0, 1};
         Clear[x1, x2, x3];
         {z1, z2, z3} = (x1 * A1 + x2 * A2 + x3 * A3) . (y1 * A1 + y2 * A2 + y3 * A3) [[1]]

Out[10]= {x3, x2 + x3, x1 + x2}

In[14]:= A = IdentityMatrix[3];
         For[n = 1, n ≤ 10, n++, A = A.A3; Print[A[[1]]]]
         {0, 0, 1}
         {0, 1, 0}
         {1, 0, 1}
         {0, 1, 1}
         {1, 1, 1}
         {1, 1, 2}
         {1, 2, 2}
         {2, 2, 3}
         {2, 3, 4}
         {3, 4, 5}
```

Poglavlje 4

Ajai Choudhry

Slika 4.1: Ajai Choudhry

Ajai Choudhry, rođen je 1953. godine u Uttar Pradeshu, državi u sjevernoj Indiji. Za njega se oduvijek znalo da je vrlo talentiran za matematiku, no nakon što je s 23 godine završio fakultet s odličnim uspjehom, potpuno se posvetio diplomatskoj službi. Idućih 11 godina radio je u indijskom Ministarstvu vanjskih poslova. Nakon što je neko vrijeme radio u Delhiju, Choudhryija su preselili u Kuala Lumpur, Varšavu, Singapur, Libanon i Brunej.

Cijelo vrijeme bavio se diplomatskim poslovima sve dok u jednoj od ambasada u Varšavi nije naišao na poljskog teoretičara brojeva Andrzeja Schnizela. Njegova strast za matematikom se vratila te je slobodno vrijeme, tijekom svojih diplomatskih službi, posvetio diofantskim jednadžbama.

Objavio je sveukupno 67 radova u znanstvenim časopisima. Dodijeljena mu je nagrada za dokaz teorema o sedmoj potenciji cijelih brojeva. Pronašao je parametarsko rješenje za

diofantsku jednadžbu

$$\sum_{i=1}^{4} x^7 = \sum_{i=1}^{5} y^7.$$

Potom pokazao i da je moguće pronaći pozitivna rješenja jednadžbe

$$\sum_{i=1}^{m} x^7 = \sum_{i=1}^{n} y^7$$

za $m \geq 4$ i $n \geq 5$.

Godine 2004. dokazao je da diofantska jednadžba $a^k + b^k + c^k = d^k + e^k + f^k$ ima beskonačno mnogo rješenja za $k = 2, 3, 4$ istovremeno.

No osim diplomacije i matematike, Choudhry se bavio i šahom. Postigao je titulu internacionalnog majstora šaha, što je druga najteža titula koju je moguće postići. Godine 1998. bio je jedan od 30 igrača u simultanki protiv tadašnjeg svjetskog prvaka Anatolija Karpova. Igra je završila neriješeno jer je Choudhry morao otići obaviti hitan diplomatski slučaj.

Choudhry zna govoriti na pet različitih jezika: hindi, engleski, malajski, indonezijski i njemački.

Bibliografija

[1] A. Choudhry, *Matrix morphology and composition of higher degree forms with applications to diophantine equations*, preprint (arXiv:2005.07585), prihvaćeno za objavljivanje u Rad HAZU, Matematičke znanosti

[2] A. Dujella, *Teorija brojeva*, Školska knjiga, Zagreb, 2019.

[3] R. A. Horn, C. R. Johnson, *Topics in matrix analysis*, Cambridge University Press, 2008.

[4] Z. Franušić, J. Šiftar, Linearna algebra, skripta, `https://web.math.pmf.unizg.hr/~fran/LA-sve-lektura.pdf`

Sažetak

Kažemo da *forma* $g : \mathbb{R}^n \to \mathbb{R}$ *dopušta kompoziciju* ako vrijedi $g(x)g(y) = g(x * y)$ za sve $x, y \in \mathbb{R}^n$, pri čemu je s $x * y$ označen neki bilinearan produkt $\mathbb{R}^n \times \mathbb{R}^n$. Primjer jednostavne cjelobrojne linearne forme koja dopušta kompoziciju je preslikavanje $f(x, y) = x^2 - dy^2$, $x, y \in \mathbb{Z}$. Forma f dopušta kompoziciju jer vrijedi dobro poznati identitet

$$(x_1^2 - dy_1^2)(x_2^2 - dy_2^2) = (x_1x_2 - dy_1y_2)^2 - d(x_1y_2 - x_2y_1)^2,$$

koji se koristi za generiranje rješenja Pellove jednadžbe $x_1^2 - dy_1^2 = 1$, gdje $d \in \mathbb{N}$ nije potpun kvadrat. U ovom radu opisujemo tehniku kojom se mogu konstruirati primjeri formi koje dopuštaju kompoziciju, a koja za to koristi algebru matrica.

Summary

We say that *a form* $g : \mathbb{R}^n \to \mathbb{R}$ *admits composition* if $g(x)g(y) = g(x * y)$ for all $x, y \in \mathbb{R}^n$, where $x * y$ is a bilinear product $\mathbb{R}^n \times \mathbb{R}^n$. An example of a simple integer form admitting composition is a function $f(x, y) = x^2 - dy^2,\ x, y \in \mathbb{Z}$. The form f admits composition because of the well known identity

$$(x_1^2 - dy_1^2)(x_2^2 - dy_2^2) = (x_1x_2 - dy_1y_2)^2 - d(x_1y_2 - x_2y_1)^2,$$

which is used to generate solutions to Pell's equation $x_1^2 - dy_1^2 = 1$, where $d \in \mathbb{N}$ is not a perfect square. In this paper we describe a technique, which uses matrix algebras, by which one can construct examples of forms admitting composition.

Životopis

Rođen sam 13. kolovoza 1996. godine u Zagreb. Završio sam osnovnoškolsko obrazovanje u OŠ Horvati u Zagrebu. Srednju školu sam završio u XV. gimnaziji u Zagrebu. Godine 2015. upisao sam Fakultet elektrotehnike i računarstva u Zagrebu, no nakon godinu i pol studiranja shvatio sam da nisam zadovoljan sa svojim studijem. Stoga sam odlučio 2017. godine upisati Integrirani preddiplomski i diplomski sveučilišni studij matematika i fizika; nastavnički smjer na Prirodoslovno-matematičkom fakultetu u Zagrebu.