

Kvaternioni i Frobeniusov teorem

Ilja Gogić, Sveučilište u Zagrebu

Sažetak

U ovom predavanju proučavamo algebru kvaterniona $\mathbb{H}$, četverodimenzionalnu nekomutativnu realnu algebru s dijeljenjem koju je 1843. godine uveo Sir William Rowan Hamilton, irski matematičar poznat po svojim doprinosima u algebri i mehanici. Kvaternioni proširuju skup kompleksnih brojeva i imaju temeljnu ulogu u raznim granama matematike i fizike. Središnja tema je Frobeniusov teorem, koji klasificira sve konačnodimenzionalne asocijativne realne algebre s dijeljenjem, tvrdeći da je svaka takva algebra izomorfna točno jednoj od sljedećih tri: realnim brojevima $\mathbb{R}$, kompleksnim brojevima $\mathbb{C}$, ili kvaternionima $\mathbb{H}$. Slijedeći pažljivo osmišljeni niz zadataka i teorijskih smjernica, razvijamo potrebne algebarske alate kako bismo dali potpun i rigorozan dokaz teorema. Usput istražujemo ključna svojstva kvaterniona i njihovu primjenu, osobito u reprezentaciji trodimenzionalnih rotacija, gdje nude elegantnu i računalno učinkovitiju alternativu tradicionalnim matričnim metodama.

Oznake: algebra, geometrija.

Ključne riječi: kvaternioni, Frobeniusov teorem, asocijativna algebra, konačnodimenzionalna realna algebra s dijeljenjem, trodimenzionalne rotacije.

Sadržaj

1	Uvod	2
2	Algebre	2
3	Konačnodimenzionalne algebre s dijeljenjem	7
4	Realne algebre s dijeljenjem - dimenzije 1 i 2	9
5	Algebra kvaterniona $\mathbb{H}$ - dimenzija 4	11
6	Frobeniusov teorem	14
7	Trodimenzionalne rotacije i grupa $SO(3)$	16
8	Kvaternionska reprezentacija 3D-rotacija	20

1 Uvod

Osnovni cilj ovog predavanja je obraditi osnove teorije konačnodimenzionalnih algebri s dijeljenjem, uvesti algebru Hamiltonovih* kvaterniona $\mathbb{H}$, razraditi neka njezina svojstva i primjene, te dokazati sljedeći fundamentalni teorem:

Teorem 1.1 (Frobeniusov teorem[†], 1877.). *Do na izomorfizam postoje točno tri konačnodimenzionalne realne algebre s dijeljenjem: realni brojevi $\mathbb{R}$, kompleksni brojevi $\mathbb{C}$ i kvaternioni $\mathbb{H}$.*

Tijekom ovog predavanja označavamo s $\mathbb{F}$ proizvoljno polje. Prisjetimo se da je **karakteristika** polja $\mathbb{F}$ najmanji prirodan broj $n \in \mathbb{N}$ za kojeg vrijedi

$$\underbrace{1 + 1 + \cdots + 1}_{n \text{ puta}} = n \cdot 1 = 0,$$

pri čemu 0 i 1 označuju aditivni i multiplikativni neutralni element u $\mathbb{F}$. Ako takav broj n ne postoji (odnosno, ako je $n \cdot 1 \neq 0$ za svaki $n \in \mathbb{N}$), tada kažemo da $\mathbb{F}$ ima **karakteristiku nula**. Karakteristika polja $\mathbb{F}$ označava se s $\text{char}(\mathbb{F})$.

Tipični primjeri polja s karakteristikom nula uključuju polje racionalnih brojeva $\mathbb{Q}$, realnih brojeva $\mathbb{R}$ i kompleksnih brojeva $\mathbb{C}$. S druge strane, svako konačno polje $\mathbb{F}_q$ s q elemenata ima karakteristiku p , gdje je p prost broj takav da vrijedi $q = p^n$ za neki $n \in \mathbb{N}$.

U ovom ćemo se predavanju uglavnom baviti poljima $\mathbb{R}$ i $\mathbb{C}$.

2 Algebre

Definicija 2.1. Za vektorski prostor A nad poljem $\mathbb{F}$ kažemo da je **asocijativna algebra** ili samo **$\mathbb{F}$ -algebra**, ako je na A zadana operacija **množenja**, odnosno asocijativna bilinearna binarna operacija

$$A \times A \rightarrow A, \quad (a, b) \mapsto ab.$$

Drugim riječima, za sve $\lambda, \mu \in \mathbb{F}$ te $a, b, c \in A$ vrijedi:

$$\begin{aligned} (ab)c &= a(bc), \\ (\lambda a + \mu b)c &= \lambda(ac) + \mu(bc), \\ a(\lambda b + \mu c) &= \lambda(ab) + \mu(ac). \end{aligned}$$

Također ćemo podrazumijevati da A ima **jedinicu**, tj. da postoji element $1_A \in A \setminus \{0\}$ sa svojstvom

$$1_A a = a 1_A = a$$

za sve $a \in A$. Jedinica u algebri je nužno jedinstvena i kada je iz konteksta jasno o kojoj algebri je riječ, često ćemo umjesto 1_A pisati samo 1.

*William Rowan Hamilton (1805–1865), irski matematičar

†Ferdinand Georg Frobenius (1849–1917), njemački matematičar

- Za element $a \in A$ kažemo da je **invertibilan** ako postoji element $a^{-1} \in A$ takav da je

$$a^{-1}a = aa^{-1} = 1.$$

Element a^{-1} , ako postoji, je jedinstven i zovemo ga **inverz** od a .

- Za elemente $a, b \in A$ definiramo njihov **komutator** s

$$[a, b] := ab - ba.$$

Ako je $[a, b] = 0$, odnosno ako vrijedi $ab = ba$, kažemo da a i b **komutiraju**.

- Skup svih elemenata u A koji komutiraju sa svim elementima u A zove se **centar** od A i označava sa $Z(A)$. Dakle,

$$Z(A) = \{z \in A : za = az \ \forall a \in A\}.$$

Ako je $A = Z(A)$, tj. ako svaka dva elementa u A komutiraju, onda kažemo da je A **komutativna algebra**.

Ako je $\mathbb{F} = \mathbb{R}$ onda govorimo o **realnim algebrama**, a ako je $\mathbb{F} = \mathbb{C}$ onda govorimo o **kompleksnim algebrama**.

- Primjer 2.2.** (a) Svako polje $\mathbb{F}$ možemo promatrati kao algebru nad samim sobom, tj. operacija množenja skalarom $\mathbb{F} \times \mathbb{F} \rightarrow \mathbb{F}$ je definirana kao množenje elemenata u $\mathbb{F}$.
- (b) Općenitije, ako je $\mathbb{K}$ potpolje od $\mathbb{F}$, onda $\mathbb{F}$ možemo promatrati i kao $\mathbb{K}$ -algebru, tj. operacija množenja skalarom je funkcija $\mathbb{K} \times \mathbb{F} \rightarrow \mathbb{F}$. Posebno, polje kompleksnih brojeva $\mathbb{C}$ možemo promatrati i kao $\mathbb{C}$ -algebru (dimenzije 1) i kao $\mathbb{R}$ -algebru (dimenzije 2).
- (c) Označimo s $\mathbb{F}[X]$ skup svih polinoma u jednoj varijabli X nad poljem $\mathbb{F}$. S obzirom na standardne operacije na polinomima, $\mathbb{F}[X]$ ima strukturu komutativne $\mathbb{F}$ -algebre. Jedinica u $\mathbb{F}[X]$ je konstantni polinom 1, a invertibilni elementi u $\mathbb{F}[X]$ su jedino nenul konstantni polinomi.
- (d) Neka je V vektorski prostor nad poljem $\mathbb{F}$. Označimo s $\mathcal{L}_{\mathbb{F}}(V)$ skup svih $\mathbb{F}$ -linearnih operatora s V u V . Dakle, $\mathcal{L}_{\mathbb{F}}(V)$ sa sastoji od svih preslikavanja $\phi : V \rightarrow V$ koja zadovoljavaju

$$\phi(\lambda v + \mu w) = \lambda \phi(v) + \mu \phi(w), \quad \text{za sve } \lambda, \mu \in \mathbb{F} \text{ i } v, w \in V.$$

Skup $\mathcal{L}_{\mathbb{F}}(V)$ ima strukturu $\mathbb{F}$ -algebre s obzirom na standardne operacije na linearnim operatorima:

$$\begin{aligned} (\lambda \phi)(v) &:= \lambda(\phi(v)), \\ (\psi + \phi)(v) &:= \psi(v) + \phi(v), \\ (\psi \phi)(v) &:= \psi(\phi(v)), \end{aligned}$$

gdje su $\phi, \psi \in \mathcal{L}_{\mathbb{F}}(V)$, $v \in V$ te $\lambda \in \mathbb{F}$. Jedinica u algebri $\mathcal{L}_{\mathbb{F}}(V)$ je identiteta id_V . Primijetimo da je algebra $\mathcal{L}_{\mathbb{F}}(V)$ nekomutativna čim je $\dim_{\mathbb{F}} V > 1$, gdje $\dim_{\mathbb{F}} V$ označava dimenziju od V .

- (e) Neka je A algebra nad poljem $\mathbb{F}$ i $n \in \mathbb{N}$. Promotrimo skup $M_n(A)$ svih $n \times n$ matrica s elementima u A . Tada je $M_n(A)$ algebra s obzirom na standardne matricne operacije:

$$\begin{aligned}\lambda[a_{ij}] &:= [\lambda a_{ij}], \\ [a_{ij}] + [b_{ij}] &:= [a_{ij} + b_{ij}], \\ [a_{ij}][b_{ij}] &:= \left[\sum_{k=1}^n a_{ik} b_{kj} \right],\end{aligned}$$

gdje su $\lambda \in \mathbb{F}$ te $[a_{ij}], [b_{ij}] \in M_n(\mathbb{F})$. Jedinica u algebri $M_n(\mathbb{F})$ je jedinična matrica

$$I_n = \text{diag}(1_A, \dots, 1_A),$$

odnosno dijagonalna matrica čiji su svi elementi na dijagonali jednaki 1_A . Posebno, $M_n(\mathbb{F})$ je $\mathbb{F}$ -algebra.

Zadatak 1. Neka A algebra nad poljem $\mathbb{F}$ karakteristike različite od 2. Ako za sve $a, b \in A$ vrijedi $(ab)^2 = (ba)^2$, dokažite da je A nužno komutativna.

Definicija 2.3. Podskup B algebre A zove se **podalgebra** od A ako B sadrži jedinicu od A i B je algebra s obzirom na operacije koje su definirane kao restrikcije operacija algebre A .

Napomena 2.4. (a) Primijetimo da je podskup B od A podalgebra od A ako i samo ako je B potprostor od A , $1_A \in B$ i B je zatvoren s obzirom na operaciju množenja, tj. vrijedi $ab \in B$ za sve $a, b \in B$.

(b) Skup $\mathbb{F}1_A = \{\lambda 1_A : \lambda \in \mathbb{F}\}$ je podalgebra od A dimenzije 1. Nju ćemo obično poistovjetiti s poljem $\mathbb{F}$, preko identifikacije $\lambda \equiv \lambda 1_A$ ($\lambda \in \mathbb{F}$), tako da je $\mathbb{F} \subseteq A$.

(c) Centar $Z(A)$ je podalgebra od A . Budući da $Z(A)$ sadrži $\mathbb{F} = \mathbb{F}1_A$ kao podalgebru, $Z(A)$ je dimenzije barem 1.

Definicija 2.5. Ako je $Z(A) = \mathbb{F}$, tj. ako jedino skalarni multipli jedinice komutiraju sa svim ostalim elementima od A , onda kažemo da je A **centralna algebra**.

Primjer 2.6. Algebra kompleksnih brojeva $\mathbb{C}$ je očito centralna kao $\mathbb{C}$ -algebra, ali ne i kao $\mathbb{R}$ -algebra.

Zadatak 2. Neka je A algebra koja sadrži polje $\mathbb{K}$ kao podalgebru. Dokažite da A ima strukturu $\mathbb{K}$ -algebre (pri čemu je operacija množenja skalarom $\mathbb{K} \times A \rightarrow A$ definirana kao množenje elemenata u A) ako i samo ako je polje $\mathbb{K}$ sadržano u centru od A .

Definicija 2.7. Neka je A algebra.

- Za potprostor I od A kažemo da je (**obostrani**) **ideal** u A ako za sve $a \in A$ i $b \in I$ vrijedi $ab \in I$ i $ba \in I$.
- Očito su $\{0\}$ i A ideali u A koje zovemo **trivijalni ideali**. Ako A nema netrivialnih ideala, onda kažemo da je A **prosta algebra**.

Primjer 2.8. (a) Neka je $\mathbb{K}$ bilo koje potpolje polja $\mathbb{F}$. Onda je $\mathbb{F}$ prosta $\mathbb{K}$ -algebra. Naime, neka je I ideal u $\mathbb{F}$ i $a \in I$. Ako je $a \neq 0$, onda je $1 = aa^{-1} \in I$, tako da $x = 1x \in I$ za sve $x \in \mathbb{F}$. Dakle, $I = \mathbb{F}$.

- (b) Promotrimo polinomijalnu algebru $\mathbb{F}[X]$. Ako je $p(X) \in \mathbb{F}[X]$ proizvoljan polinom, onda je $I := p(X)\mathbb{F}[X]$ (skup svih polinoma djeljivih s $p(X)$) ideal u $\mathbb{F}[X]$. Štoviše, može se dokazati da je svaki ideal u $\mathbb{F}[X]$ oblika $p(X)\mathbb{F}[X]$, za neki polinom $p(X)$ (vidjeti npr. [3, Corollary 6.4])

Zadatak 3. Neka je A algebra i $n \in \mathbb{N}$.

- (a) Dokažite da je A centralna algebra ako i samo ako je matrična algebra $M_n(A)$ centralna.
- (b) Dokažite da je A prosta algebra ako i samo ako je $M_n(A)$ prosta algebra.

Posljedično, $M_n(\mathbb{F})$ je centralna prosta $\mathbb{F}$ -algebra.

Definicija 2.9. Neka su A i B algebre nad istim poljem $\mathbb{F}$.

- Za preslikavanje $\phi : A \rightarrow B$ kažemo da je **homomorfizam algebri** ako je $\mathbb{F}$ -linearno, multiplikativno te jedinicu slika u jedinicu, tj. vrijedi

$$\begin{aligned}\phi(\lambda a + \mu b) &= \lambda \phi(a) + \mu \phi(b), \\ \phi(ab) &= \phi(a)\phi(b), \\ \phi(1_A) &= 1_B,\end{aligned}$$

za sve $a, b \in A$ i $\lambda, \mu \in \mathbb{F}$.

- Injektivni homomorfizmi zovu se **monomorfizmi**, surjektivni homomorfizmi **epimorfizmi**, a bijektivni homomorfizmi **izomorfizmi**. Izomorfizmi $\phi : A \rightarrow A$ zovu se **automorfizmi** algebre A .
- Za algebre A i B kažemo da su **izomorfne** i pišemo $A \cong B$ ako postoji izomorfizam $\phi : A \rightarrow B$.

Napomena 2.10. (a) Izomorfnost algebri je relacija ekvivalencije na klasi svih $\mathbb{F}$ -algebri.

- (b) Skup automorfizama algebre A označavamo s $\text{Aut}_{\mathbb{F}}(A)$ i on ima strukturu grupe s obzirom na množenje u $\mathcal{L}_{\mathbb{F}}(A)$ (tj. kompoziciju).
- (c) Neka je A algebra. Svaki invertibilni element $q \in A$ inducira tzv. **unutrašnji automorfizam** Ad_q od A , dan s

$$\text{Ad}_q(x) := qxq^{-1}.$$

Unutrašnji automorfizmi čine podgrupu od $\text{Aut}_{\mathbb{F}}(A)$ i oni su naravno interesantni samo u nekomutativnom slučaju.

- (d) Prema važnom *Skolem–Noetherinovom teoremu*^{†,§}, konačnodimenzionalne centralne proste algebre dopuštaju samo unutrašnje automorfizme (vidjeti [1, Theorem 1.30]). Posebno, prema Zadatku 3, svaki automorfizam matrične algebre $M_n(\mathbb{F})$ je nužno unutrašnji.

[†]Thoralf Albert Skolem (1887.–1963.), norveški matematičar

[§]Amalie Emmy Noether (1882.–1935.), njemačka matematičarka

Zadatak 4. (a) Odredite grupu automorfizama $\text{Aut}_{\mathbb{R}}(\mathbb{C})$ realne algebre $\mathbb{C}$.

(b) Odredite grupu automorfizama $\text{Aut}_{\mathbb{R}}(\mathbb{C}^2)$ realne algebre $\mathbb{C}^2$, s obzirom na operacije po koordinatama:

$$\begin{aligned}\lambda(z_1, z_2) &:= (\lambda z_1, \lambda z_2), \\ (z_1, z_2) + (w_1, w_2) &:= (z_1 + w_1, z_2 + w_2), \\ (z_1, z_2) \cdot (w_1, w_2) &:= (z_1 w_1, z_2 w_2),\end{aligned}$$

gdje su $\lambda \in \mathbb{R}$ te $z_1, z_2, w_1, w_2 \in \mathbb{C}$.

Primjer 2.11. Neka je A algebra. Ako je $p \in \mathbb{F}[X]$ polinom s rastavom

$$p = p(X) = \lambda_0 + \lambda_1 X + \lambda_2 X^2 + \dots + \lambda_n X^n = \sum_{k=0}^n \lambda_k X^k,$$

tada za element $a \in A$ definiramo

$$p(a) := \lambda_0 1 + \lambda_1 a + \lambda_2 a^2 + \dots + \lambda_n a^n = \sum_{k=0}^n \lambda_k a^k \in A.$$

Preslikavanje

$$\phi_a : \mathbb{F}[X] \rightarrow A, \quad \phi_a : p \mapsto p(a)$$

je homomorfizam algebri, a njegova slika je najmanja podalgebra od A koja sadrži element a , tj. potprostor od A razapet svim potencijama $\{1, a, a^2, \dots\}$ elementa a .

Primjer 2.12. Neka je V n -dimenzionalni vektorski prostor nad poljem $\mathbb{F}$ i $(b) = (b_1, \dots, b_n)$ neka uređena baza za V . Za linearni operator $\phi \in \mathcal{L}_{\mathbb{F}}(V)$ označimo s $[\phi]_{(b)}$ njegov matrični prikaz u bazi (b) , tj.

$$[\phi]_{(b)} = \begin{bmatrix} \alpha_{11} & \alpha_{12} & \cdots & \alpha_{1n} \\ \alpha_{21} & \alpha_{22} & \cdots & \alpha_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_{n1} & \alpha_{n2} & \cdots & \alpha_{nn} \end{bmatrix} \in M_n(\mathbb{F}),$$

gdje su koeficijenti $\alpha_{ij} \in \mathbb{F}$ jedinstveno određeni s

$$\phi(b_j) = \sum_{i=1}^n \alpha_{ij} b_i, \quad \text{for all } 1 \leq j \leq n.$$

Tada je preslikavanje $\mathcal{L}_{\mathbb{F}}(V) \rightarrow M_n(\mathbb{F})$, koje linearnom operatoru $T \in \mathcal{L}_{\mathbb{F}}(V)$ pridružuje njegov matrični prikaz $[T]_{(b)} \in M_n(\mathbb{F})$ u bazi (b) , izomorfizam algebri.

Napomena 2.13. (a) Svaka algebra A izomorfna je nekoj podalgebri od $\mathcal{L}_{\mathbb{F}}(A)$. Naime, za fiksirani element $a \in A$ definirajmo preslikavanje

$$L_a : A \rightarrow A, \quad L_a(x) := ax.$$

Preslikavanje L_a je očito linearno, tj. $L_a \in \mathcal{L}_{\mathbb{F}}(A)$. Nadalje, lako se provjeri da je s

$$\pi : A \rightarrow \mathcal{L}_{\mathbb{F}}(A), \quad \pi(a) := L_a$$

definiran monomorfizam algebri, koji se zove **regularna reprezentacija** od A .

(b) Posebno, ako je A konačne dimenzije n , A je izomorfna nekoj podalgebri matrične algebre $M_n(\mathbb{F})$.

Zadatak 5. Neka je A konačnodimenzijska algebra nad poljem $\mathbb{F}$ karakteristike 0. Dokažite da se jedinica 1_A ne može prikazati kao konačna suma komutatora u A .

Definicija 2.14. Neka je A algebra. Ako postoji nenul element $a \in A$ takav da je $ab = 0$ za neki nenul element $b \in A$, onda kažemo da je a **djelitelj nule**. Ako A nema djelitelja nule, onda kažemo da je A **domena**. Komutativne domene zovu se još i **integralne domene**.

Primjer 2.15. Algebra polinoma $\mathbb{F}[X]$ je integralna domena.

Napomena 2.16. Istaknutu klasu djelitelja nule u algebri A (ako takvi postoje) čine tzv. *nilpotentni elementi*, tj. nenul elementi $a \in A$ za koje postoji prirodan broj $n \geq 2$ takav da je $a^n = 0$. Nilpotentni elementi uvijek postoje u matričnim algebrama $M_n(\mathbb{F})$, čim je $n \geq 2$. Naime, ako je $T \in M_n(\mathbb{F})$ bilo koja nenul striktno gornje trokutasta matrica, onda je $T^n = 0$.

Zadatak 6. Neka je A konačnodimenzijska algebra nad poljem $\mathbb{F}$ karakteristike 0. Pretpostavimo da elementi $a, b \in A$ zadovoljavaju jednakost $[[a, b], a] = 0$. Dokažite da tada postoji prirodan broj n takav da je $[a, b]^n = 0$.

3 Konačnodimenzijske algebre s dijeljenjem

Definicija 3.1. Neka je A algebra nad poljem $\mathbb{F}$ te neka je $a \in A$. Ako postoji normirani polinom $m_a \in \mathbb{F}[X]$ takav da je $m_a(a) = 0$, te za svaki drugi normirani polinom $p \in \mathbb{F}[X]$ sa svojstvom $p(a) = 0$ vrijedi $\deg m_a \leq \deg p$, onda kažemo da je m_a **minimalni polinom elementa a** .

Propozicija 3.2. Neka je A konačnodimenzijska algebra nad poljem $\mathbb{F}$. Tada svaki element $a \in A$ ima jedinstven minimalni polinom m_a .

Dokaz. Neka je $\dim_{\mathbb{F}} A = n$ i fiksirajmo element $a \in A$.

Egzistencija od m_a . Promotrimo skup

$$\{1_A, a, \dots, a^n\} \subseteq A.$$

Jer je $\dim_{\mathbb{F}} A = n$, taj skup je linearno zavisna pa postoje skalari $\lambda_0, \lambda_1, \dots, \lambda_n \in \mathbb{F}$ koji nisu svi 0 takvi da je

$$\lambda_0 1_A + \lambda_1 a + \dots + \lambda_n a^n = 0.$$

Neka je $0 \leq k \leq n$ najveći broj takav da je $\lambda_k \neq 0$. Tada je

$$p(X) := \frac{1}{\lambda_k} (\lambda_k X^k + \dots + \lambda_1 X + \lambda_0)$$

normiran polinom u $\mathbb{F}[X]$ takav da je $p(a) = 0$. Posebno, postoji polinom $m_a \in \mathbb{F}[X]$ najmanjeg stupnja koji se poništava na elementu a i m_a je po definiciji minimalni polinom elementa a .

Jedinstvenost od m_a . Pretpostavimo da su $m_a, m'_a \in \mathbb{F}[X]$ dva minimalna polinoma od a . Po definiciji, m_a i m'_a su istog stupnja $k \leq n$. Očito je $(m_a - m'_a)(a) = 0$. Jer su polinomi m_a i m'_a normirani i istog su stupnja, zaključujemo da je polinom $p := m_a - m'_a \in \mathbb{F}[X]$ stupnja manjeg od k sa svojstvom $p(a) = 0$. Stoga je nužno $p = 0$, odnosno $m_a = m'_a$. $\square$

Zadatak 7. Neka je A algebra. Za element $a \in A$ kažemo da je **lijevo (desno) invertibilan** ako postoji element $b \in A$ takav da je $ba = 1$ ($ab = 1$).

- (a) Ako je algebra A konačnodimenzionalna, dokažite da su svi lijevo (desno) invertibilni elementi u A nužno invertibilni.
- (b) U algebri $\mathcal{L}_{\mathbb{R}}(\mathbb{R}[X])$ nađite primjer neinvertibilnog operatora koji je lijevo invertibilan.

Definicija 3.3. Za algebru A kažemo da je **algebra s dijeljenjem** ako je svaki nenul element u A invertibilan.

Primjer 3.4. Polja $\mathbb{R}$ i $\mathbb{C}$ su očiti primjeri komutativnih realnih algebri s dijeljenjem.

Napomena 3.5. Analogni argument kao u Primjeru 2.8 (a) pokazuje da je svaka algebra s dijeljenjem prosta algebra.

Zadatak 8. Neka je A algebra s dijeljenjem.

- (a) Dokažite da za sve $a, b \in A \setminus \{0\}$, $a \neq b^{-1}$, vrijedi tzv. **Huin identitet**[¶]

$$aba = ((a - b^{-1})^{-1} - a^{-1})^{-1} + a.$$

- (b) Pretpostavimo da je $\phi \in \mathcal{L}_{\mathbb{F}}(A)$ linearno preslikavanje takvo da vrijedi

$$\phi(1) = 1 \quad \text{i} \quad \phi(a)\phi(a^{-1}) = 1, \quad \text{za sve } a \in A \setminus \{0\}.$$

Dokažite da tada vrijedi

$$\phi(a^2) = \phi(a)^2, \quad \text{za sve } a \in A. \quad (3.1)$$

Štoviše, ako je $\text{char}(\mathbb{F}) \neq 2$, dokažite da je jednakost (3.1) ekvivalentna s

$$\phi(ab + ba) = \phi(a)\phi(b) + \phi(b)\phi(a), \quad \text{za sve } a, b \in A. \quad (3.2)$$

Napomena. Preslikavanja $\phi \in \mathcal{L}_{\mathbb{F}}(A)$ koja zadovoljavaju jednakost (3.2) zovu se **Jordanovi homomorfizmi**^{||} i igraju važnu ulogu u teoriji algebri i prstenova, kao i u matematičkoj fundaciji kvantne mehanike.

Propozicija 3.6. *Svaka konačnodimenzionalna domena je algebra s dijeljenjem.*

Dokaz. Pretpostavimo da je A konačnodimenzionalna domena. Jer je A domena, za fiksirani element $a \neq 0$, operator $L_a \in \mathcal{L}_{\mathbb{F}}(A)$, $L_a(x) = ax$, je injektivan, pa stoga i bijektivan jer je $\dim_{\mathbb{F}} A < \infty$ (teorem o rangui i defektu). Posebno, L_a u slici sadrži jedinicu od A , odnosno postoji $b \in A$ takav da je

$$ab = 1.$$

Analogno, promatrajući operator $R_a \in \mathcal{L}_{\mathbb{F}}(A)$, $R_a(x) = xa$, dolazimo do elementa $c \in A$ takvog da vrijedi

$$ca = 1.$$

Slijedi

$$c = c1 = c(ab) = (ca)b = 1b = b,$$

odnosno $c = b$ je inverz od a . Kako je $a \neq 0$ bio proizvoljan, slijedi tvrdnja. □

[¶]Hua Loo-Keng (1910.–1985.), kineski matematičar i političar

^{||}Ernst Pascual Jordan (1902.–1980.), njemački fizičar

Napomena 3.7. Beskonačnodimenzijske domene ne moraju biti algebre s dijeljenjem. Osnovni primjer koji to pokazuje je algebra polinoma $\mathbb{F}[X]$, budući da su svi polinomi stupnja većeg ili jednakog 1 neinvertibilni u $\mathbb{F}[X]$.

Propozicija 3.8. *Neka je A konačnodimenzijska algebra s dijeljenjem. Minimalni polinom svakog elementa u A je ireducibilan, tj. ne može faktorizirati u produkt dva nekonstantna polinoma.*

Dokaz. Neka je $a \in A$ s minimalnim polinomom m_a (Propozicija 3.8). Pretpostavimo da je

$$m_a(X) = p(X)q(X)$$

za neke polinome $p, q \in \mathbb{F}[X]$. Tada je

$$p(a)q(a) = m_a(a) = 0.$$

Jer je A algebra s dijeljenjem, mora biti $p(a) = 0$ ili $q(a) = 0$. Kako su oba polinoma p i q stupnja najviše $\deg m_a$, po definiciji od m_a barem jedan od polinoma p i q mora biti stupnja jednakog $\deg m_a$. Posljedično drugi polinom onda mora biti konstantan. $\square$

4 Realne algebre s dijeljenjem - dimenzije 1 i 2

U nastavku ćemo koristiti sljedeći fundamentalni teorem i njegovu posljedicu:

Teorem 4.1 (Osnovni teorem algebre). *Svaki kompleksni polinom $p \in \mathbb{C}[X]$ stupnja $n \geq 1$ ima korijen u $\mathbb{C}$. Posljedično, p se može faktorizirati kao produkt polinoma stupnja 1, tj. postoje $\alpha, \lambda_1, \dots, \lambda_n \in \mathbb{C}$ takvi da je*

$$P(X) = \alpha(X - \lambda_1) \cdots (X - \lambda_n)$$

i takva faktorizacija je jedinstvena do na permutaciju faktora.

Korolar 4.2. *Realni polinom $p \in \mathbb{R}[x]$ je ireducibilan ako i samo ako je p ili stupnja 1 ili stupnja 2 bez realnih korijena, odnosno negativne diskriminante.*

Za dokaz i povijesni pregled Osnovnog teorema algebre, čitatelja upućujemo na [2, Chapter 4].

Korolar 4.3. *Do na izomorfizam, $\mathbb{C}$ je jedina konačnodimenzijska kompleksna algebra s dijeljenjem.*

Dokaz. Neka je A konačnodimenzijska kompleksna algebra s dijeljenjem. Fiksirajmo proizvoljan element $a \in A$ te neka je $m_a \in \mathbb{C}[X]$ njegov minimalni polinom. Prema Propoziciji 3.2, m_a je ireducibilan. Prema Osnovnom teoremu algebre m_a je stupnja 1, odnosno $m_a(X) = X - \lambda$ za neki skalar $\lambda \in \mathbb{C}$. Slijedi $0 = m_a(a) = a - \lambda 1_A$, odnosno $a = \lambda 1_A$. Dakle, $A \cong \mathbb{C}$. $\square$

Lema 4.4. *Neka je A konačnodimenzijska realna algebra s dijeljenjem. Tada je minimalni polinom svakog elementa $a \in A$ jednog od sljedeća dva oblika:*

$$m_a(X) = \begin{cases} X - \lambda & (\lambda \in \mathbb{R}) & \text{ako je } a \in \mathbb{R} \\ X^2 - 2\lambda X + \mu & (\lambda, \mu \in \mathbb{R}, \lambda^2 < \mu) & \text{ako } a \notin \mathbb{R}. \end{cases}$$

Posljedično, svaki element $a \in A$ možemo zapisati u obliku $a = x + y$, gdje je $x \in \mathbb{R}$ i $y \in A$ takav da je ili $y = 0$ ili $y^2 \in \mathbb{R}_{<0}$.

Dokaz. Ako je $a \in A$, onda je očito $a \in \mathbb{R}$ ako i samo ako je $m_a(X) = X - a$. U tom slučaju imamo trivijalnu dekompoziciju $a = x + y$, gdje je $y = 0$.

Ako $a \notin \mathbb{R}$, odnosno ako je $\deg m_a > 1$, onda iz ireducibilnosti od m_a (Propozicija 3.2) i Korolara 4.2 slijedi da je $m_a(X) = X^2 - 2\lambda X + \mu$ za neke $\lambda, \mu \in \mathbb{R}$ takve da je $\lambda^2 < \mu$. U tom slučaju stavimo $x := \lambda \in \mathbb{R}$ i $y := a - \lambda \notin \mathbb{R}$, tako da je $a = x + y$ i

$$\begin{aligned} y^2 &= a^2 - 2\lambda a + \lambda^2 = a^2 - 2\lambda a + \mu + (\lambda^2 - \mu) = m_a(a) + (\lambda^2 - \mu) \\ &= \lambda^2 - \mu < 0. \end{aligned}$$

□

Propozicija 4.5. *Do na izomorfizam, $\mathbb{C}$ je jedina dvodimenzionalna realna algebra s dijeljenjem.*

Dokaz. Neka je A dvodimenzionalna realna algebra s dijeljenjem. Prema Lemi 4.4 postoji element $y \in A$ takav da je $y^2 \in \mathbb{R}_{<0}$. Stavimo

$$i_A := \frac{1}{\sqrt{-y^2}}y \in A,$$

tako da je $i_A^2 = -1$. Skup $\{1_A, i_A\}$ je očito linearno nezavisan pa stoga razapinje A (jer je $\dim_{\mathbb{R}} A = 2$). Dakle

$$A = \mathbb{R}1_A + \mathbb{R}i_A = \{\lambda 1_A + \mu i_A : \lambda, \mu \in \mathbb{R}\},$$

gdje $+$ označava (unutrašnju) direktnu sumu vektorskih prostora. Sada je trivijalno provjeriti da je preslikavanje $\phi : \mathbb{C} \rightarrow A$ definirano s $\phi(\lambda + \mu i) := \lambda 1_A + \mu i_A$ izomorfizam (realnih) algebri. □

Korolar 4.6. *Do na izomorfizam, $\mathbb{R}$ i $\mathbb{C}$ su jedine konačnodimenzionalne komutativne realne algebre s dijeljenjem.*

Dokaz. Pretpostavimo da je A realna konačnodimenzionalna komutativna algebra s dijeljenjem, te neka je $\dim_{\mathbb{R}} A \geq 2$. Prema dokazu Propozicije 4.5, A sadrži podalgebru $\mathbb{C}_A$ izomorfnu s $\mathbb{C}$. Jer je A komutativna, A možemo promatrati kao $\mathbb{C}_A$ -algebru (tj. za polje skalara uzmemo $\mathbb{C}_A$; vidjeti zadatak 2). Kako je $\dim_{\mathbb{R}} A < \infty$ svakako je i $\dim_{\mathbb{C}_A} A < \infty$. Dakle, A konačnodimenzionalna kompleksna algebra s dijeljenjem pa je prema Korolaru 4.3 nužno $A = \mathbb{C}_A \cong \mathbb{C}$. □

U ovom trenutku prirodno se nameće sljedeće pitanje: *Za koje prirodne brojeve $n > 2$ postoje n -dimenzionalne realne algebre s dijeljenjem? Nadalje, jesu li takve algebre (do na izomorfizam) jednoznačno određene svojom dimenzijom n ?*

Na ova pitanja upravo odgovara Frobeniusov teorem, kojeg ćemo dokazati u odjeljku 6.

Na kraju ovog odjeljka napomenimo da je klasifikacija dvodimenzionalnih algebri s dijeljenjem nad poljem racionalnih brojeva $\mathbb{Q}$ osjetno kompliciranija:

Zadatak 9. Neka je p prost broj. Promotrimo skup

$$\mathbb{Q}[\sqrt{p}] := \{\lambda + \mu\sqrt{p} : \lambda, \mu \in \mathbb{Q}\} \subseteq \mathbb{R},$$

s obzirom na standardne operacije zbrajanja i množenja realnih brojeva.

- (a) Dokažite da je $\mathbb{Q}[\sqrt{p}]$ polje koje sadrži $\mathbb{Q}$ i $\dim_{\mathbb{Q}} \mathbb{Q}[\sqrt{p}] = 2$.
- (b) Ako su p i q dva različita prosta broja, dokažite da $\mathbb{Q}$ -algebre $\mathbb{Q}[\sqrt{p}]$ i $\mathbb{Q}[\sqrt{q}]$ nisu izomorfne.
- (c) Zaključite da postoji beskonačno mnogo neizomorfnih dvodimenzionalnih $\mathbb{Q}$ -algebri s dijeljenjem.

5 Algebra kvaterniona $\mathbb{H}$ - dimenzija 4

Na vektorskom prostoru

$$\mathbb{R}^4 = \{(q_0, q_1, q_2, q_3) : q_0, q_1, q_2, q_3 \in \mathbb{R}\},$$

uz standardne operacije zbrajanja i množenja skalarom, uvedimo sljedeće oznake

$$1 := (1, 0, 0, 0), \quad \mathbf{i} := (0, 1, 0, 0), \quad \mathbf{j} := (0, 0, 1, 0) \quad \text{ i } \quad \mathbf{k} := (0, 0, 0, 1),$$

Drugim riječima, $\{1, \mathbf{i}, \mathbf{j}, \mathbf{k}\}$ je upravo kanonska baza za $\mathbb{R}^4$, tako da za svaki $q = (q_0, q_1, q_2, q_3) \in \mathbb{R}^4$ imamo rastav

$$q = q_0 + q_1\mathbf{i} + q_2\mathbf{j} + q_3\mathbf{k}.$$

Na $\mathbb{R}^4$ također uvodimo operaciju množenja, tako da najprije definiramo međusobne produkte $\mathbf{i}, \mathbf{j}, \mathbf{k}$ na sljedeći način:

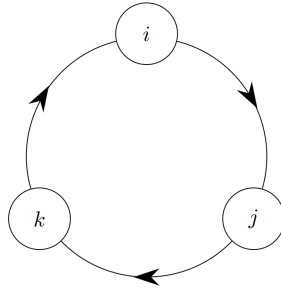
$$\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = -1,$$

$$\mathbf{ij} = -\mathbf{ji} = \mathbf{k},$$

$$\mathbf{jk} = -\mathbf{kj} = \mathbf{i},$$

$$\mathbf{ki} = -\mathbf{ik} = \mathbf{j}.$$

Primijetimo da pravilo množenja elemenata $\mathbf{i}, \mathbf{j}, \mathbf{k}$ možemo lako zapamtiti koristeći sljedeći dijagram:



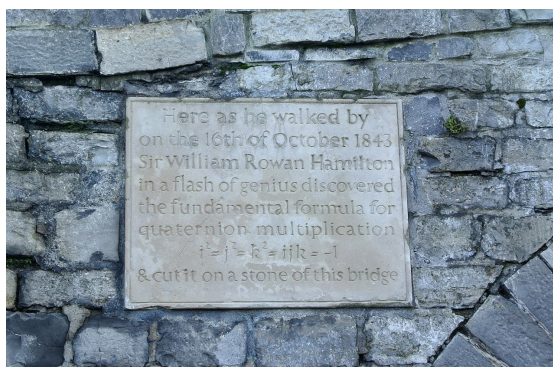
Definiciju množenja zatim po bilinearnosti proširimo na čitav $\mathbb{R}^4$. Dakle, za $q = q_0 + q_1\mathbf{i} + q_2\mathbf{j} + q_3\mathbf{k}$ i $w = w_0 + w_1\mathbf{i} + w_2\mathbf{j} + w_3\mathbf{k}$:

$$\begin{aligned} (q_0 + q_1\mathbf{i} + q_2\mathbf{j} + q_3\mathbf{k}) \cdot (w_0 + w_1\mathbf{i} + w_2\mathbf{j} + w_3\mathbf{k}) &:= q_0w_0 - q_1w_1 - q_2w_2 - q_3w_3 \\ &+ (q_0w_1 + q_1w_0 + q_2w_3 - q_3w_2)\mathbf{i} \\ &+ (q_0w_2 - q_1w_3 + q_2w_0 + q_3w_1)\mathbf{j} \\ &+ (q_0w_3 + q_1w_2 - q_2w_1 + q_3w_0)\mathbf{k} \end{aligned}$$

Definicija 5.1. Uz prethodno definirane operacije, $\mathbb{R}^4$ se zove **algebra kvaterniona** i označava se s $\mathbb{H}$.

Napomena 5.2. Nije teško (ali je malo naporno) provjeriti da je $\mathbb{H}$ zaista realna (asocijativna) algebra. Primijetimo da $\mathbb{H}$ *nije komutativna*.

Napomena 5.3. Pojam kvaterniona dolazi od latinske riječi *quaternion*, koja se prevodi kao četvorka, odnosno cjelina od četiri dijela. Oznaka $\mathbb{H}$ za kvaternione dana je u čast W. R. Hamiltona, koji je 1843. godine otkrio kvaternione, tražeći proširenje polja kompleksnih brojeva do trodimenzionalne realne algebre s dijeljenjem s dvije imaginarne jedinice. Nakon višegodišnjih neuspjelih pokušaja, shvatio je da to ne može postići u dimenziji 3, već u dimenziji 4, s tri imaginarne jedinice $\mathbf{i}, \mathbf{j}, \mathbf{k}$ koje moraju zadovoljavati jednakost $\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = \mathbf{ijk} = -1$. Tu formulu je 16. listopada 1843. Hamilton urezao u kamen dublinskog mosta Broom Bridge, na kojem se i danas nalazi sljedeća plaketa:



Sliku je izradio Cone83

<https://en.wikipedia.org/wiki/Quaternion>

Slično kao i na algebri kompleksnih brojeva $\mathbb{C}$, na algebri kvaterniona $\mathbb{H}$ uvodimo **involuciju (konjugiranje)**, kao unarnu operaciju $*$: $\mathbb{H} \rightarrow \mathbb{H}$ definiranu s

$$(q_0 + q_1\mathbf{i} + q_2\mathbf{j} + q_3\mathbf{k})^* := q_0 - q_1\mathbf{i} - q_2\mathbf{j} - q_3\mathbf{k}.$$

Lako se pokaže da konjugiranje na $\mathbb{H}$ zadovoljava sljedeća svojstva:

$$\begin{aligned} (q^*)^* &= q, \\ (\lambda q + \mu w)^* &= \lambda q^* + \mu w^*, \\ (qw)^* &= w^* q^*, \\ q^* &= -\frac{1}{2}(q + \mathbf{i}q\mathbf{i} + \mathbf{j}q\mathbf{j} + \mathbf{k}q\mathbf{k}), \end{aligned}$$

gdje su $q, w \in \mathbb{H}$ te $\lambda, \mu \in \mathbb{R}$.

Za svaki kvaternion $q = q_0 + q_1\mathbf{i} + q_2\mathbf{j} + q_3\mathbf{k} \in \mathbb{H}$ definiramo njegov **realni (skalarni) dio** s

$$\text{Re}(q) := \frac{1}{2}(q + q^*) = q_0$$

i **imaginarni (vektorski) dio** s

$$\mathbf{q} := \frac{1}{2}(q - q^*) = q_1\mathbf{i} + q_2\mathbf{j} + q_3\mathbf{k},$$

tako da se q rastavlja u obliku

$$q = q_0 + \mathbf{q}.$$

Za kvaternion $q \in \mathbb{H}$ kažemo da je **čisti** ako je $\text{Re}(q) = 0$, što je ekvivalentno s $q^* = -q$. Uobičajeno se $\mathbb{R}^3$ poistovjećuje sa čistim kvaternionima, preko identifikacije

$$(q_1, q_2, q_3) \equiv q_1 \mathbf{i} + q_2 \mathbf{j} + q_3 \mathbf{k}. \quad (5.1)$$

Onda s lako provjeri da produkt dvaju kvaterniona $q = q_0 + \mathbf{q}$ i $w = w_0 + \mathbf{w}$ možemo računati preko formule

$$qw = \text{Re}(q) \text{Re}(w) - \langle \mathbf{q}, \mathbf{w} \rangle + \text{Re}(q) \mathbf{w} + \text{Re}(w) \mathbf{q} + \mathbf{q} \times \mathbf{w}, \quad (5.2)$$

gdje $\langle \cdot, \cdot \rangle$ i $\times$ redom označavaju (standarni) skalarni i vektorski produkt na $\mathbb{R}^3$:

$$\langle \mathbf{q}, \mathbf{w} \rangle = q_1 w_1 + q_2 w_2 + q_3 w_3,$$

$$\mathbf{q} \times \mathbf{w} = \begin{vmatrix} \mathbf{i} & \mathbf{j} & \mathbf{k} \\ q_1 & q_2 & q_3 \\ w_1 & w_2 & w_3 \end{vmatrix}.$$

Napokon, algebru $\mathbb{H}$ opskrbljujemo s **euklidskom normom**

$$\|q_0 + q_1 \mathbf{i} + q_2 \mathbf{j} + q_3 \mathbf{k}\| := \sqrt{q_0^2 + q_1^2 + q_2^2 + q_3^2},$$

za koju se lako provjeri da zadovoljava sljedeća svojstva:

$$\begin{aligned} \|1\| &= 1, \\ \|q^*\| &= \|q\|, \\ q^* q &= \|q\|^2 = q q^*, \\ \|qw\| &= \|q\| \|w\|, \end{aligned}$$

za sve $q, w \in \mathbb{H}$. Posebno, svaki nenul kvaternion $q \in \mathbb{H}$ je invertibilan s inverzom

$$q^{-1} = \frac{q^*}{\|q\|^2}.$$

Nadalje, algebra $\mathbb{H}$ je centralna, tj. $Z(\mathbb{H}) = \mathbb{R}$. Naime, ako je $q = q_0 + q_1 \mathbf{i} + q_2 \mathbf{j} + q_3 \mathbf{k} \in Z(\mathbb{H})$, onda iz $q\mathbf{i} = \mathbf{i}q$ i $q\mathbf{j} = \mathbf{j}q$ redom dobivamo $q_2 = q_3 = 0$ i $q_1 = q_3 = 0$, odnosno $q = q_0 \in \mathbb{R}$.

Sve zajedno, imamo sljedeći rezultat:

Propozicija 5.4. *Algebra kvaterniona $\mathbb{H}$ je nekomutativna centralna realna algebra s dijeljenjem dimenzije 4.*

Posebno, prema Skolem-Noetherovom teoremu (Napomena 2.10 (d)), algebra $\mathbb{H}$ dopušta samo unutrašnje automorfizme.

6 Frobeniusov teorem

Sada smo spremni dokazati Frobeniusov teorem. Prisjetimo se njegovog iskaza:

Frobeniusov teorem. *Do na izomorfizam postoje točno tri konačnodimenzionalne asocijativne realne algebre s dijeljenjem: realni brojevi $\mathbb{R}$, kompleksni brojevi $\mathbb{C}$ i kvaternioni $\mathbb{H}$.*

Dokaz Frobeniusovog teorema provodimo u koracima. Neka je A asocijativna konačnodimenzionalna realna algebra s dijeljenjem.

Korak 1. Ako je $\dim_{\mathbb{R}} A = 1$ onda je $A = \mathbb{R}1_A \cong \mathbb{R}$.

Korak 2. Ako je $\dim_{\mathbb{R}} A > 1$ onda prema dokazu Propozicije 4.5 postoji element $i_A \in A$ takav da je $i_A^2 = -1$ te A sadrži podalgebru $\mathbb{C}_A = \mathbb{R}1_A + \mathbb{R}i_A$ izomorfnu s $\mathbb{C}$. Posebno, ako je $\dim_{\mathbb{R}} A = 2$, imamo $A = \mathbb{C}_A \cong \mathbb{C}$.

Korak 3. Pretpostavimo da je $\dim_{\mathbb{R}} A > 2$, tako da je $\mathbb{C}_A \subsetneq A$.

Zadatak 10. Dokažite da ne postoji element $a \in A \setminus \mathbb{C}_A$ koji komutira s i_A .

Korak 4. Promotrimo A kao vektorski prostor nad poljem $\mathbb{C}_A$ i označimo ga s ${}_{\mathbb{C}_A}A$. Definirajmo sada preslikavanje

$$\phi : {}_{\mathbb{C}_A}A \rightarrow {}_{\mathbb{C}_A}A \quad \text{s} \quad \phi(a) := i_A a i_A^{-1}.$$

Zadatak 11. Dokažite da preslikavanje ϕ zadovoljava sljedeća svojstva:

- (a) ϕ je involucija, tj. $\phi^2 = \phi \circ \phi = \text{id}_A$.
- (b) ϕ je $\mathbb{C}_A$ -linearan, tj. $\phi(z_1 a_1 + z_2 a_2) = z_1 \phi(a_1) + z_2 \phi(a_2)$ za sve $z_1, z_2 \in \mathbb{C}_A$ i $a_1, a_2 \in A$.
- (c) ϕ je multiplikativno, tj. $\phi(a_1 a_2) = \phi(a_1) \phi(a_2)$ za sve $a_1, a_2 \in A$.

Korak 5. Iz (a) i (b) dijela zadatka 11 slijedi da su 1 i -1 jedini kandidati za svojstvene vrijednosti od ϕ . Označimo pripadne svojstvene potprostore s V_1 i V_{-1} , tj.

$$V_1 := \{a \in A : \phi(a) = a\},$$

$$V_{-1} := \{a \in A : \phi(a) = -a\}.$$

Očito je $\mathbb{C}_A \subseteq V_1$. Štoviše, iz zadatka 10 slijedi da je $V_1 = \mathbb{C}_A$.

Zadatak 12. Zaključite da je $V_{-1} \neq \{0\}$ i da vrijedi ${}_{\mathbb{C}_A}A = V_1 + V_{-1}$ (direktna suma vektorskih prostora nad $\mathbb{C}_A$).

Korak 6. Fiksirajmo neki element $b \in V_{-1} \setminus \{0\}$. Prema Lemi 4.4 postoje $\lambda, \mu \in \mathbb{R}$ takvi da je

$$b^2 = \lambda 1_A + \mu b \tag{6.1}$$

Ako na jednakost (6.1) djelujemo s operatorom ϕ , tada koristeći zadatak 11 dobivamo

$$\phi(b)^2 = \lambda 1_A + \mu \phi(b).$$

Prema izboru elementa b imamo $\phi(b) = -b$, pa je

$$b^2 = \lambda 1_A - \mu b. \quad (6.2)$$

Iz (6.1) i (6.2) slijedi da je $\mu = 0$. Kako $b \notin \mathbb{R}1_A$, mora biti $\lambda < 0$. Uvedimo sada elemente

$$j_A := \frac{1}{\sqrt{-\lambda}}b, \\ k_A := i_A j_A.$$

Zadatak 13. Dokažite da $\{1_A, i_A, j_A, k_A\}$ čini linearno nezavisan skup u A , te uspostavite sljedeće jednakosti:

$$i_A^2 = j_A^2 = k_A^2 = -1_A, \\ i_A j_A = -j_A i_A = k_A, \\ j_A k_A = -k_A j_A = i_A, \\ k_A i_A = -i_A k_A = j_A.$$

Korak 7. Iz prethodnog razmatranja slijedi da je

$$\mathbb{H}_A := \mathbb{R}1_A + \mathbb{R}i_A + \mathbb{R}j_A + \mathbb{R}k_A \subseteq A$$

podalgebra od A koja je izomorfna s algebrom kvaterniona $\mathbb{H}$. Ostaje još dokazati da je $A = \mathbb{H}_A$. U tu svrhu izaberimo proizvoljni element $a \in V_{-1}$. Koristeći (c) dio zadatka 11 dobivamo

$$\phi(j_A a) = \phi(j_A)\phi(a) = (-j_A)(-a) = j_A a.$$

Oдавде zaključujemo da je $j_A a \subseteq V_1 = \mathbb{C}_A$, pa je $a \in j_A^{-1}\mathbb{C}_A \subseteq \mathbb{H}_A$. Dakle, $V_{-1} \subseteq \mathbb{H}_A$ i $V_1 = \mathbb{C}_A \subseteq \mathbb{H}_A$, što zajedno s $A = V_1 + V_{-1}$ povlači $A = \mathbb{H}_A$. Time je dokaz Frobeniusovog teorema u potpunosti završen. $\square$

Na kraju ovog odjeljka napomenimo da se prepostavka konačne dimenzionalnosti algebre A u Frobeniusovom teoremu ne može ispustiti.

Primjer 6.1. Za proizvoljno polje $\mathbb{F}$ definiramo **algebru Laurentovih** redova** $\mathbb{F}((X))$ kao skup svih formalnih redova oblika

$$\sum_{n=-\infty}^{\infty} \lambda_n X^n,$$

gdje je samo konačno mnogo skalara $\lambda_n \in \mathbb{F}$ s negativnim indeksima n različito od 0.

Na $\mathbb{F}((X))$ uvodimo operacije množenja skalarom, zbrajanja i množenja na sličan način kao i na algebri polinoma $\mathbb{F}[X]$:

$$\lambda \left(\sum_{n=-\infty}^{\infty} \lambda_n X^n \right) := \sum_{n=-\infty}^{\infty} (\lambda \lambda_n) X^n, \\ \sum_{n=-\infty}^{\infty} \lambda_n X^n + \sum_{n=-\infty}^{\infty} \mu_n X^n := \sum_{n=-\infty}^{\infty} (\lambda_n + \mu_n) X^n,$$

**Pierre Alphonse Laurent (1813.–1854.), francuski matematičar, inženjer i vojni časnik

$$\left(\sum_{n=-\infty}^{\infty} \lambda_n X^n\right) \left(\sum_{n=-\infty}^{\infty} \mu_n X^n\right) := \sum_{n=-\infty}^{\infty} \nu_n X^n, \quad \text{gdje je } \nu_n := \sum_{i+j=n} \lambda_i \mu_j.$$

Primijetimo da je definicija množenja na $\mathbb{F}((X))$ smisljena, s obzirom da za svaki nenul element $f \in \mathbb{F}((X))$ postoji $m \in \mathbb{Z}$ takav da je $f = \sum_{n=m}^{\infty} \lambda_n X^n$ i $\lambda_m \neq 0$. Nije teško provjeriti da $\mathbb{F}((X))$ s obzirom na gore uvedene operacije (komutativna) algebra s dijeljenjem. Također, jer je $\mathbb{F}[X] \subset \mathbb{F}((X))$, algebra $\mathbb{F}((X))$ je beskonačnodimenzionalna.

Posebno, $\mathbb{R}((X))$ je primjer beskonačnodimenzionalne (komutativne) realne algebre s dijeljenjem.

7 Trodimenzionalne rotacije i grupa $SO(3)$

Osim što imaju značajnu teorijsku ulogu, kvaternioni imaju široku primjenu u matematici, fizici i računarstvu. U ovom odjeljku ukratko ćemo opisati osnovna svojstva rotacija u $\mathbb{R}^3$, što će poslužiti kao uvod u njihovu reprezentaciju pomoću kvaterniona. Takva kvaternionijska reprezentacija posebno je korisna u područjima poput robotike i računalne grafike.

Tokom čitavog ovog odjeljka promatramo vektorski prostor

$$\mathbb{R}^n = \{\mathbf{v} = (v_1, \dots, v_n) : v_1, \dots, v_n \in \mathbb{R}\}$$

opremljen standardnim (euklidskim) skalarnim produktom

$$\langle (v_1, \dots, v_n), (w_1, \dots, w_n) \rangle = v_1 w_1 + \dots + v_n w_n$$

i pripadnom normom

$$\|(v_1, \dots, v_n)\| = \sqrt{\langle (v_1, \dots, v_n), (v_1, \dots, v_n) \rangle} = \sqrt{v_1^2 + \dots + v_n^2}.$$

Kao i obično, za svaki $1 \leq j \leq n$ označavamo s $\mathbf{e}_j$ vektor u $\mathbb{R}^n$ kojemu su sve koordinate jednake nuli osim j -te, koja je jednaka 1. Tada

$$(e) := (\mathbf{e}_1, \dots, \mathbf{e}_n)$$

čini ortonormiranu bazu prostora $\mathbb{R}^n$, koja se naziva *kanonska* ili *standardna ortonormirana baza*.

Nadalje, $\mathbb{R}^n$ identificiramo sa stupčastim matricama putem identifikacije

$$(v_1, \dots, v_n) \equiv \begin{bmatrix} v_1 \\ \vdots \\ v_n \end{bmatrix},$$

tako da je svaka linearna preslikavanje na $\mathbb{R}^n$ oblika $\mathbf{v} \mapsto T\mathbf{v}$ za neku matricu $T \in M_n(\mathbb{R})$.

Definicija 7.1. • Za linearni operator $\phi \in \mathcal{L}_{\mathbb{R}}(\mathbb{R}^n)$ kažemo da je **ortogonalan operator** ako čuva skalarni produkt, tj. ako vrijedi

$$\langle \phi(\mathbf{v}), \phi(\mathbf{w}) \rangle = \langle \mathbf{v}, \mathbf{w} \rangle, \quad \text{za sve } \mathbf{v}, \mathbf{w} \in \mathbb{R}^n.$$

- Matrica $T \in M_n(\mathbb{R})$ zove se **ortogonalna** ako vrijedi

$$T^t T = T T^t = I_n,$$

gdje T^t označava transponiranu matricu od T .

Skup svih ortogonalnih matrica reda n u $M_n(\mathbb{R})$ označavamo s $O(n)$. Lako je provjeriti da $O(n)$ čini grupu s obzirom na množenje matrica, koja se naziva **ortogonalna grupa**.

Napomena 7.2. (a) Prema *polarizacijskom identitetu*

$$\langle \mathbf{v}, \mathbf{w} \rangle = \frac{1}{4} (\|\mathbf{v} + \mathbf{w}\|^2 - \|\mathbf{v} - \mathbf{w}\|^2),$$

slijedi da je linearni operator $\phi \in \mathcal{L}_{\mathbb{R}}(\mathbb{R}^n)$ ortogonalan ako i samo ako čuva euklidsku normu, tj.

$$\|\phi(\mathbf{v})\| = \|\mathbf{v}\|, \quad \text{za sve } \mathbf{v} \in \mathbb{R}^n.$$

- (b) Matrica $T \in M_n(\mathbb{R})$ je ortogonalna ako i samo ako njezini stupci čine ortonormiranu bazu prostora $\mathbb{R}^n$.
- (c) Primjenom Binet-Cauchyjevog teorema i činjenice da se determinanta matrice ne mijenja pri transponiranju, zaključujemo da svaka ortogonalna matrica ima determinantu jednaku ± 1 .
- (d) Linearni operator $\phi \in \mathcal{L}_{\mathbb{R}}(\mathbb{R}^n)$ je ortogonalan ako i samo ako postoji ortonormirana baza (f) prostora $\mathbb{R}^n$ takva da je matična reprezentacija $[\phi]_{(f)}$ ortogonalna matrica. Štoviše, u tom slučaju, $[\phi]_{(f)}$ je ortogonalna matrica s obzirom na *svaku* ortonormiranu bazu (f) .

Definicija 7.3. Ortogonalna matrica $T \in O(n)$ zove se **specijalno ortogonalna** ako vrijedi $\det T = 1$.

Skup svih specijalno ortogonalnih matrica reda n označavamo sa $SO(n)$. Očito je $SO(n)$ podgrupa grupe $O(n)$ i naziva se **specijalna ortogonalna grupa**.

Sada ćemo detaljnije opisati strukturu grupa $SO(2)$ i $SO(3)$. Za početak, promotrimo rotaciju $R_\theta : \mathbb{R}^2 \rightarrow \mathbb{R}^2$ koja svaki vektor $\mathbf{v} \in \mathbb{R}^2$ preslikava u vektor dobiven rotacijom $\mathbf{v}$ oko ishodišta za kut $\theta \in [0, 2\pi)$ u pozitivnom smjeru (suprotno od kazaljke na satu). Očito je R_θ ortogonalni linearni operator koji čuva orijentaciju ravnine. Budući da vrijedi

$$R_\theta(1, 0) = (\cos \theta, \sin \theta) \quad \text{i} \quad R_\theta(0, 1) = (-\sin \theta, \cos \theta),$$

slijedi da je matični prikaz od R_θ u standardnoj bazi $(e) = (\mathbf{e}_1, \mathbf{e}_2)$ od $\mathbb{R}^2$ dan s

$$[R_\theta]_{(e)} = \begin{bmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{bmatrix}.$$

Posebno, vrijedi $[R_\theta]_{(e)} \in SO(2)$. Nadalje, imamo sljedeći rezultat:

Propozicija 7.4. (a) Grupa $SO(2)$ sastoji se točno od svih rotacija od $\mathbb{R}^2$ oko ishodišta.

(b) Ako je $T \in O(2)$ i $\det T = -1$, tada vrijedi $T = SR$, gdje je R rotacija $\mathbb{R}^2$ oko ishodišta, a S refleksija preko nekog pravca u $\mathbb{R}^2$ koji prolazi ishodištem.

Dokaz. Svaka matrica $T \in O(2)$ preslikava par kanonskih vektora $(\mathbf{e}_1, \mathbf{e}_2)$ u ortogonalni par $(\mathbf{v}, \mathbf{w})$ jediničnih vektora u $\mathbb{R}^2$. Neka je $\theta \in [0, 2\pi)$ takav da je $\mathbf{v}$ dobiven iz $\mathbf{e}_1$ rotacijom u pozitivnom smjeru za kut θ . Moguće su dvije situacije:

- Vektor $\mathbf{w}$ je dobiven rotacijom $\mathbf{e}_2$ za isti kut θ . U tom slučaju vrijedi $\det T = 1$ i T je rotacija $\mathbb{R}^2$ za kut θ oko ishodišta, tj.

$$T = \begin{bmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{bmatrix}.$$

- Vektor $\mathbf{w}$ ima suprotnu orijentaciju u odnosu na prethodni slučaj. Tada vrijedi $T = SR$, gdje je R rotacija za kut θ oko ishodišta, a S refleksija preko pravca kroz ishodište u smjeru vektora $\mathbf{v}$. U tom slučaju vrijedi $\det T = -1$.

□

Sada поближе promotrimo slučaj $n = 3$. Svaka rotacija R prostora $\mathbb{R}^3$ oko ishodišta fiksira jedinstveni pravac ℓ kroz ishodište, kojeg nazivamo *os rotacije*, te djeluje kao rotacija oko te osi. Preciznije, ako je $\mathbf{u} \in \mathbb{R}^3$ jedinični vektor koji određuje os ℓ i $\theta \in [0, 2\pi)$, tada rotacija

$$R = R_{\mathbf{u}, \theta} : \mathbb{R}^3 \rightarrow \mathbb{R}^3$$

preslikava svaki vektor $\mathbf{v} \in \mathbb{R}^3$ u vektor dobiven rotacijom $\mathbf{v}$ oko osi ℓ za kut θ u smjeru suprotnom od kazaljke na satu (sukladno pravilu desne ruke, tj. s obzirom pozitivnu orijentaciju određenu vektorom $\mathbf{u}$).

Analogno dvodimenzionalnom slučaju, rotacije prostora $\mathbb{R}^3$ oko ishodišta upravo su ona linearna preslikavanja koja su ortogonalna i čuvaju orijentaciju; to jest, pripadaju specijalnoj ortogonalnoj grupi $SO(3)$. Činjenicu da rotacije doista imaju ta svojstva lako je provjeriti odabirom odgovarajuće ortonormirane baze prostora $\mathbb{R}^3$ u kojoj rotacija poprima odgovarajuć matrični oblik. Neka je konkretno $R = R_{\mathbf{u}, \theta}$ rotacija oko osi određene jediničnim vektorom $\mathbf{u}$ za kut θ . Stavimo $\mathbf{f}_1 := \mathbf{u}$. Zatim odaberimo bilo koji jedinični vektor $\mathbf{f}_2$ ortogonalan na $\mathbf{f}_1$ i definirajmo $\mathbf{f}_3 := \mathbf{f}_1 \times \mathbf{f}_2$ (vektorski produkt). Trojka $(f) = (\mathbf{f}_1, \mathbf{f}_2, \mathbf{f}_3)$ čini pozitivno orijentiranu ortonormiranu bazu prostora $\mathbb{R}^3$, u kojoj rotacija R djeluje kao:

$$\begin{aligned} R(\mathbf{f}_1) &= \mathbf{f}_1, \\ R(\mathbf{f}_2) &= \cos \theta \mathbf{f}_2 + \sin \theta \mathbf{f}_3, \\ R(\mathbf{f}_3) &= -\sin \theta \mathbf{f}_2 + \cos \theta \mathbf{f}_3. \end{aligned}$$

Dakle,

$$[R]_{(f)} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & \cos \theta & -\sin \theta \\ 0 & \sin \theta & \cos \theta \end{bmatrix},$$

što je očito matrica determinante 1, odnosno iz $SO(3)$. Naravno, jer je determinanta matrice invarijantna s obzirom na konjugaciju invertibilnom matricom, slijedi da onda i svaki matrični prikaz od R (u proizvoljnoj ortonormiranoj bazi za $\mathbb{R}^3$) također pripada grupi $SO(3)$.

Nadalje, matični prikaz od R u standardnoj ortonormiranoj bazi (e) možemo odrediti preko formule

$$[R]_{(e)} = T[R]_{(f)}T^t, \quad (7.1)$$

gdje je T ortogonalna matrica prijelaza iz baze (e) u bazu (f) , tj.

$$T = \begin{bmatrix} \alpha_{11} & \alpha_{12} & \alpha_{13} \\ \alpha_{21} & \alpha_{22} & \alpha_{23} \\ \alpha_{31} & \alpha_{32} & \alpha_{33} \end{bmatrix},$$

pri čemu su $\alpha_{ij} \in \mathbb{R}$ jedinstveni koeficijenti takvi da vrijedi

$$\mathbf{f}_j = \alpha_{1j}\mathbf{e}_1 + \alpha_{2j}\mathbf{e}_2 + \alpha_{3j}\mathbf{e}_3, \quad \text{za } j = 1, 2, 3.$$

Kao što smo već najavili, kao i u slučaju grupe $SO(2)$, grupa $SO(3)$ također ima analognu geometrijsku karakterizaciju:

Propozicija 7.5. *Grupa $SO(3)$ sastoji se točno od svih rotacija prostora $\mathbb{R}^3$ oko ishodišta.*

Dokaz. Već smo pokazali da je matrica svake rotacije prostora $\mathbb{R}^3$ oko ishodišta (neovisno o izboru ortonormirane baze) specijalna ortogonalna matrica.

Obratno, neka je $R \in SO(3)$. Kako bismo pronašli os rotacije R , dovoljno je pokazati da jednadžba $R\mathbf{v} = \mathbf{v}$ ima netrivialno rješenje $\mathbf{v} \in \mathbb{R}^3$, tj. da je 1 svojstvena vrijednost matrice R . Ekvivalentno, tvrdimo da vrijedi $\det(R - I_3) = 0$. Budući da vrijedi $RR^t = I_3$, imamo:

$$(R - I_3)R^t = RR^t - R^t = I_3 - R^t = -(R - I_3)^t.$$

Koristeći prethodnu opservaciju i činjenicu da je $\det R = \det R^t = 1$, zaključujemo:

$$\begin{aligned} \det(R - I_3) &= \det(R - I_3) \cdot \det(R^t) = \det[(R - I_3)R^t] = \det[-(R - I_3)^t] \\ &= (-1)^3 \cdot \det(R - I_3)^t = -\det(R - I_3). \end{aligned}$$

Prema tome, $\det(R - I_3) = 0$, kao što smo tvrdili. Neka je $\mathbf{v}_1 \in \mathbb{R}^3$ jedinični vektor takav da vrijedi $R\mathbf{v}_1 = \mathbf{v}_1$, i neka je $(\mathbf{v}_2, \mathbf{v}_3)$ ortonormirana baza ravnine L ortogonalne na pravac određen vektorom $\mathbf{v}_1$. Tada je $(\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3)$ ortonormirana baza prostora $\mathbb{R}^3$, s obzirom na koju linearni operator $\mathbf{v} \mapsto R\mathbf{v}$ ima blok-dijagonalnu reprezentaciju:

$$\begin{bmatrix} 1 & 0 \\ 0 & S \end{bmatrix},$$

gdje je S ortogonalna 2×2 matrica. Budući da je $\det R = 1$, nužno je $\det S = 1$, tj. $S \in SO(2)$. Prema Propoziciji 7.4, S inducira rotaciju ravnine L oko ishodišta. $\square$

Napomena 7.6. Neka je $R \in SO(3)$ interpretirana kao rotacija oko osi zadane jednadžbom $R\mathbf{v} = \mathbf{v}$. Prema (7), pripadni kut rotacije θ zadovoljava identitet

$$\cos \theta = \frac{\operatorname{tr} R - 1}{2},$$

gdje $\operatorname{tr} R$ označava trag matrice R .

Primjer 7.7. Matrice rotacija u $\mathbb{R}^3$ oko koordinatnih osi x , y i z za kut θ u smjeru suprotnom od kazaljke na satu (sukladno pravilu desne ruke), u standardnoj bazi (e) za $\mathbb{R}^3$ glase redom:

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & \cos \theta & -\sin \theta \\ 0 & \sin \theta & \cos \theta \end{bmatrix}, \quad \begin{bmatrix} \cos \theta & 0 & \sin \theta \\ 0 & 1 & 0 \\ -\sin \theta & 0 & \cos \theta \end{bmatrix} \quad \text{i} \quad \begin{bmatrix} \cos \theta & -\sin \theta & 0 \\ \sin \theta & \cos \theta & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

Primjer 7.8. Odredimo matrični prikaz rotacije R oko osi zadane jediničnim vektorom $\mathbf{u} = \frac{1}{\sqrt{3}}(1, -1, 1)$ i kuta $\theta = \frac{\pi}{3}$ u standardnoj bazi (e) za $\mathbb{R}^3$. Neka je $(f) = (\mathbf{f}_1, \mathbf{f}_2, \mathbf{f}_3)$ ortonormirana baza prostora $\mathbb{R}^3$ takva da je

$$\mathbf{f}_1 = \mathbf{u} = \left(\frac{1}{\sqrt{3}}, -\frac{1}{\sqrt{3}}, \frac{1}{\sqrt{3}} \right), \quad \mathbf{f}_2 \perp \mathbf{f}_1, \quad \text{i} \quad \mathbf{f}_3 = \mathbf{f}_1 \times \mathbf{f}_2.$$

Na primjer, možemo uzeti $\mathbf{f}_2 = \left(\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}}, 0 \right)$, pa je tada $\mathbf{f}_3 = \left(-\frac{1}{\sqrt{6}}, \frac{1}{\sqrt{6}}, \frac{2}{\sqrt{6}} \right)$. Onda je

$$[R]_{(f)} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & \frac{1}{2} & -\frac{\sqrt{3}}{2} \\ 0 & \frac{\sqrt{3}}{2} & \frac{1}{2} \end{bmatrix}, \quad T = \begin{bmatrix} \frac{1}{\sqrt{3}} & \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{6}} \\ -\frac{1}{\sqrt{3}} & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{6}} \\ \frac{1}{\sqrt{3}} & 0 & \frac{2}{\sqrt{6}} \end{bmatrix},$$

tako da je

$$\begin{aligned} [R]_{(e)} &= T[R]_{(f)}T^t \\ &= \begin{bmatrix} \frac{1}{\sqrt{3}} & \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{6}} \\ -\frac{1}{\sqrt{3}} & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{6}} \\ \frac{1}{\sqrt{3}} & 0 & \frac{2}{\sqrt{6}} \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & \frac{1}{2} & -\frac{\sqrt{3}}{2} \\ 0 & \frac{\sqrt{3}}{2} & \frac{1}{2} \end{bmatrix} \begin{bmatrix} \frac{1}{\sqrt{3}} & -\frac{1}{\sqrt{3}} & \frac{1}{\sqrt{3}} \\ \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 \\ -\frac{1}{\sqrt{6}} & \frac{1}{\sqrt{6}} & \frac{2}{\sqrt{6}} \end{bmatrix} \\ &= \begin{bmatrix} \frac{2}{3} & -\frac{2}{3} & -\frac{1}{3} \\ \frac{1}{3} & \frac{2}{3} & -\frac{2}{3} \\ \frac{2}{3} & \frac{1}{3} & \frac{2}{3} \end{bmatrix}. \end{aligned}$$

8 Kvaternionska reprezentacija 3D-rotacija

Kako bismo motivirali temu ovog odjeljka, započnimo razmatranjem rotacije $R_\theta : \mathbb{R}^2 \rightarrow \mathbb{R}^2$ oko ishodišta za kut $\theta \in [0, 2\pi)$ u smjeru suprotnom od kazaljke na satu. Kao što smo vidjeli, u standardnoj bazi (e) matrica rotacije R_θ glasi

$$[R_\theta]_{(e)} = \begin{bmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{bmatrix}.$$

Identificiranjem $\mathbb{R}^2$ s kompleksnom ravninom $\mathbb{C}$ putem korespondencije

$$(x, y) \equiv x + iy,$$

ova rotacija odgovara množenju s kompleksnim brojem u modula 1. Naime, ako definiramo

$$u := e^{i\theta} = \cos \theta + i \sin \theta,$$

onda je $|u| = 1$, te za $z = x + iy$ vrijedi

$$R_\theta \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} \cos \theta \cdot x - \sin \theta \cdot y \\ \sin \theta \cdot x + \cos \theta \cdot y \end{bmatrix} \equiv uz.$$

Cilj nam je dobiti analognu reprezentaciju rotacija u $\mathbb{R}^3$ oko ishodišta koristeći kvaternione. Kao i prije, identificiramo $\mathbb{R}^3$ s čistim kvaternionima preko identifikacije (5.1). U tu svrhu, neka je $q \in \mathbb{H}$ *jedinični kvaternion*, tj. zadovoljava $\|q\| = 1$. Ako q dekomponiramo na skalarni i vektorski dio, tj.

$$q = q_0 + \mathbf{q},$$

tada slijedi da

$$q_0^2 + \|\mathbf{q}\|^2 = \|q\|^2 = 1.$$

Stoga postoji $\theta \in [0, 2\pi]$ takav da vrijedi

$$\cos \frac{\theta}{2} = q_0 \quad \text{i} \quad \sin \frac{\theta}{2} = \|\mathbf{q}\| \quad (8.1)$$

(uskoro ćemo vidjeti zašto smo baš uzeli polovični zapis kuta). Zapišimo q u formi

$$q = \cos \frac{\theta}{2} + \sin \frac{\theta}{2} \mathbf{u},$$

gdje

$$\mathbf{u} := \frac{\mathbf{q}}{\|\mathbf{q}\|}.$$

Definirajmo preslikavanje $L_q : \mathbb{R}^3 \rightarrow \mathbb{R}^3$ kao restrikciju unutrašnjeg automorfizama Ad_q od $\mathbb{H}$ na $\mathbb{R}^3$. Jer je $\|q\| = 1$ imamo $q^{-1} = q^*$, tako da je

$$L_q(\mathbf{v}) = q\mathbf{v}q^*, \quad \text{za sve } \mathbf{v} \in \mathbb{R}^3. \quad (8.2)$$

Primijetimo da operator L_q doista preslikava $\mathbb{R}^3$ u sebe, što znači da je slika sastavljena od čistih kvaterniona. Da bismo to provjerili, uzmimo proizvoljni vektor $\mathbf{v} \in \mathbb{R}^3$ i uočimo da

$$L_q(\mathbf{v})^* = (q\mathbf{v}q^*)^* = q\mathbf{v}^*q^* = q(-\mathbf{v})q^* = -q\mathbf{v}q^* = -L_q(\mathbf{v}),$$

što pokazuje da je $L_q(\mathbf{v})$ čisto imaginarni kvaternion, odnosno pripada $\mathbb{R}^3$. Nadalje, L_q je linearan operator. Za vektorski dio $\mathbf{q}$ kvaterniona q vrijedi

$$L_q(\mathbf{q}) = q\mathbf{q}q^* = q(q - q_0)q^* = \|q\|^2(q - q_0) = \mathbf{q},$$

budući da je $\|q\| = 1$. Također, operator L_q očuva normu, jer za svaki $\mathbf{v} \in \mathbb{R}^3$ vrijedi

$$\|L_q(\mathbf{v})\| = \|q\mathbf{v}q^*\| = \|q\| \cdot \|\mathbf{v}\| \cdot \|q^*\| = \|\mathbf{v}\|.$$

Dakle, prema Napomeni 7.2 (a), operator L_q je ortogonalan i ostavlja os $\mathbb{R}\mathbf{u}$ invarijantnom. Koristeći formulu za množenje kvaterniona (5.2), izraženu pomoću skalarnog i vektorskog produkta u $\mathbb{R}^3$, dobivamo eksplicitnu formulu za L_q :

$$L_q(\mathbf{v}) = (q_0^2 - \|\mathbf{q}\|^2)\mathbf{v} + 2\langle \mathbf{q}, \mathbf{v} \rangle \mathbf{q} + 2q_0(\mathbf{q} \times \mathbf{v}). \quad (8.3)$$

(vidjeti Zadatak 14).

Tvrdimo da je L_q operator rotacije oko osi određene s $\mathbf{u}$ za kut θ , odnosno da vrijedi $L_q = R_{\mathbf{u},\theta}$. Zaista, prema dokazanom je $L_q(\mathbf{u}) = \mathbf{u}$. Dakle, s obzirom, da je L_q linearni operator, dovoljno je dokazati da L_q na ravnini okomitoj na $\mathbf{u}$ djeluje kao rotacija za kut θ (pri čemu je ravnina orijentirana normalom $\mathbf{u}$). Izaberimo proizvoljan jedinični vektor $\mathbf{n} \in \mathbb{R}^3$ okomit na $\mathbf{u}$ i savimo $\mathbf{n}_\perp := \mathbf{u} \times \mathbf{n}$. Jer je $\mathbf{n} \perp \mathbf{u}$, imamo $\|\mathbf{n}_\perp\| = \|\mathbf{u}\|\|\mathbf{n}\| = 1$, tako da je

$$(f) := (\mathbf{u}, \mathbf{n}, \mathbf{n}_\perp)$$

pozitivno orijentirana ortonormirana baza za $\mathbb{R}^3$. Koristeći raspis (8.3) i zapis (8.1), dobivamo

$$\begin{aligned} L_q(\mathbf{n}) &= (q_0^2 - \|\mathbf{q}\|^2)\mathbf{n} + 2\langle \mathbf{q}, \mathbf{n} \rangle \mathbf{q} + 2q_0(\mathbf{q} \times \mathbf{n}) \\ &= (q_0^2 - \|\mathbf{q}\|^2)\mathbf{n} + 2q_0\|\mathbf{q}\|\mathbf{n}_\perp \\ &= \left(\cos^2 \frac{\theta}{2} - \sin^2 \frac{\theta}{2}\right)\mathbf{n} + \left(2\cos \frac{\theta}{2} \sin \frac{\theta}{2}\right)\mathbf{n}_\perp \\ &= (\cos \theta)\mathbf{n} + (\sin \theta)\mathbf{n}_\perp. \end{aligned}$$

Analogno bismo dobili

$$L_q(\mathbf{n}_\perp) = (-\sin \theta)\mathbf{n} + (\cos \theta)\mathbf{n}_\perp.$$

Dakle,

$$[L_q]_{(f)} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & \cos \theta & -\sin \theta \\ 0 & \sin \theta & \cos \theta \end{bmatrix}.$$

Time smo dokazali sljedeći rezultat:

Teorem 8.1. *Za svaki jedinični kvaternion*

$$q = q_0 + \mathbf{q} = \cos \frac{\theta}{2} + \sin \frac{\theta}{2}\mathbf{u}, \quad (8.4)$$

operator $L_q : \mathbb{R}^3 \rightarrow \mathbb{R}^3$ definiran formulom (8.2) je upravo rotacija $R_{\mathbf{u},\theta}$ oko osi određene s $\mathbf{u}$ za kut θ .

Kao direktnu posljedicu dobivamo sljedeću važnu formulu:

Korolar 8.2 (Rodriguesova rotacijska formula formulu^{††}). *Uz iste oznake kao u prethodnom teoremu, za sve $\mathbf{v} \in \mathbb{R}^3$ vrijedi*

$$R_{\mathbf{u},\theta}(\mathbf{v}) = \cos \theta \mathbf{v} + (1 - \cos \theta)\langle \mathbf{u}, \mathbf{v} \rangle \mathbf{u} + \sin \theta(\mathbf{u} \times \mathbf{v}). \quad (8.5)$$

Dokaz. Prema Teoremu 8.1 za $q \in \mathbb{H}$ definiran s (8.4) imamo $R_{\mathbf{u},\theta} = L_q$. Koristeći formulu (8.3) lako dobivamo

$$\begin{aligned} L_q(\mathbf{v}) &= \left(\cos^2 \frac{\theta}{2} - \sin^2 \frac{\theta}{2}\right)\mathbf{v} + 2\left(\sin \frac{\theta}{2}\langle \mathbf{u}, \mathbf{v} \rangle\right)\sin \frac{\theta}{2}\mathbf{u} + 2\cos \frac{\theta}{2}\left(\sin \frac{\theta}{2}(\mathbf{u} \times \mathbf{v})\right) \\ &= \cos \theta \mathbf{v} + (1 - \cos \theta)\langle \mathbf{u}, \mathbf{v} \rangle \mathbf{u} + \sin \theta(\mathbf{u} \times \mathbf{v}). \end{aligned}$$

□

^{††}Benjamin Olinde Rodrigues (1795.–1851.), francuski bankar, matematičar i društveni reformator

Napomena 8.3. Definirajmo linearni operator $K : \mathbb{R}^3 \rightarrow \mathbb{R}^3$ s

$$K(\mathbf{v}) := \mathbf{u} \times \mathbf{v}.$$

Onda je

$$K^2(\mathbf{v}) = K(K(\mathbf{v})) = \mathbf{u} \times (\mathbf{u} \times \mathbf{v}) = \langle \mathbf{u}, \mathbf{v} \rangle \mathbf{u} - \mathbf{v},$$

tako da je

$$\langle \mathbf{u}, \mathbf{v} \rangle \mathbf{u} = (K^2 - I)(\mathbf{v}).$$

Stoga Rodriguesovu rotacijsku formulu (8.5) možemo zapisati u obliku

$$R_{\mathbf{u}, \theta} = I + (\sin \theta)K + (1 - \cos \theta)K^2. \quad (8.6)$$

Pritom, ako je $\mathbf{u} = u_x \mathbf{i} + u_y \mathbf{j} + u_z \mathbf{k}$, onda je

$$[K]_{(e)} = \begin{bmatrix} 0 & -u_z & u_y \\ u_z & 0 & -u_x \\ -u_y & u_x & 0 \end{bmatrix}.$$

Nakon direktnog računa u (8.6) dobivamo eksplicitni zapis od $[R_{\mathbf{u}, \theta}]_{(e)}$ u terminu koeficijanata od $\mathbf{u}$ i kuta θ :

$$[R_{\mathbf{u}, \theta}]_{(e)} = \begin{bmatrix} \cos \theta + (1 - \cos \theta)u_x^2 & (1 - \cos \theta)u_x u_y - \sin \theta u_z & (1 - \cos \theta)u_x u_z + \sin \theta u_y \\ (1 - \cos \theta)u_y u_x + \sin \theta u_z & \cos \theta + (1 - \cos \theta)u_y^2 & (1 - \cos \theta)u_y u_z - \sin \theta u_x \\ (1 - \cos \theta)u_z u_x - \sin \theta u_y & (1 - \cos \theta)u_z u_y + \sin \theta u_x & \cos \theta + (1 - \cos \theta)u_z^2 \end{bmatrix}.$$

Primjer 8.4. Promotrimo rotaciju R iz Primjera 7.8, oko osi određene vektorom $\mathbf{u} = \frac{1}{\sqrt{3}}(1, -1, 1)$ za kut $\theta = \frac{\pi}{3}$. Kvaternionska reprezentaciju of R dana je s

$$R(\mathbf{v}) = L_q(\mathbf{v}) = q\mathbf{v}q^*,$$

gdje je

$$q = \cos \frac{\pi}{6} + \sin \frac{\pi}{6} \mathbf{u} = \frac{\sqrt{3}}{2} + \frac{\sqrt{3}}{6} \mathbf{i} - \frac{\sqrt{3}}{6} \mathbf{j} + \frac{\sqrt{3}}{6} \mathbf{k},$$

Nadalje, koristeći Rodriguesovu rotacijsku formulu ponovo dobivamo

$$[R]_{(e)} = \begin{bmatrix} \frac{2}{3} & -\frac{2}{3} & -\frac{1}{3} \\ \frac{1}{3} & \frac{2}{3} & -\frac{2}{3} \\ \frac{2}{3} & \frac{1}{3} & \frac{2}{3} \end{bmatrix}.$$

Jer je $SO(3)$ grupa, iz Propozicije 7.5 zaključujemo da je kompozicija dviju rotacija oko ishodišta ponovo rotacija oko ishodišta. Tu činjenicu također možemo lako dokazati koristeći Teorem 8.1.

Korolar 8.5. *Kompozicija dviju rotacija od $\mathbb{R}^3$ oko ishodišta je također rotacija od $\mathbb{R}^3$ oko ishodišta.*

Dokaz. Tvrdnja je direktna posljedica Teorema 8.1 i činjenice da je kompozicija unutrašnjih automorfizama unutrašnji automorfizam. Naime, neka su R i S dvije rotacije od $\mathbb{R}^3$ redom reprezentirane jediničnim kvaternionima q i w , tako da je $R = L_q$ i $S = L_w$. Onda za svaki vektor $\mathbf{v} \in \mathbb{R}^3$ imamo

$$\begin{aligned} (S \circ R)(\mathbf{v}) &= L_w(L_q(\mathbf{v})) = L_w(q\mathbf{v}q^*) = w(q\mathbf{v}q^*)w^* = (wq)\mathbf{v}(wq)^* \\ &= L_{wq}(\mathbf{v}). \end{aligned}$$

Jer je produkt jediničnih kvaterniona ponovo jedinični kvaternion, zaključujemo da je $S \circ R = L_{wq}$ rotacija od $\mathbb{R}^3$. $\square$

Zadatak 14. Dokažite formulu (8.3) za djelovanje operatora L_q .

Zadatak 15. Neka je R rotacija oko osi definirane jediničnim vektorom $\mathbf{u} = \frac{1}{\sqrt{3}}(1, 1, 1)$ za kut $\theta = \frac{2\pi}{3}$. Odredite matični prikaz od R u standardnoj bazi (e) za $\mathbb{R}^3$ na dva načina, koristeći:

- (a) Rodriguesovu rotacijsku formulu,
- (b) matični prikaz od R u pogodno odabranoj ortonormiranoj bazi za $\mathbb{R}^3$.

Zadatak 16. Zadana je matrica

$$R := \begin{bmatrix} -\frac{3}{7} & -\frac{6}{7} & -\frac{2}{7} \\ * & * & * \\ \frac{6}{7} & -\frac{2}{7} & -\frac{3}{7} \end{bmatrix}.$$

Odredite drugi redak od R tako da je $R \in SO(3)$ i zatim odredite jedinični kvaternion $q \in \mathbb{H}$ takav da je $R = L_q$.

Zadatak 17. Neka je R rotacija oko osi y za kut α i S rotacija oko osi z za kut β . Koristeći kvaternione, odredite os i kosinus kuta rotacije $S \circ R$.

Već smo ranije primijetili da je svaki automorfizam algebre $\mathbb{H}$ unutrašnji (posljedica Skolem-Noetherinovog teorema). U narednom zadatku dolazimo do istog zaključka koristeći rezultate i metode iz ovog odjeljka.

Zadatak 18. Neka je ϕ proizvoljan automorfizam algebre kvaterniona $\mathbb{H}$.

- (a) Dokažite da ϕ preslikava čisto imaginarne kvaternione unutar samih sebe, te da je restrikcija $\phi|_{\mathbb{R}^3} : \mathbb{R}^3 \rightarrow \mathbb{R}^3$ čuva skalarni produkt i orijentaciju, tj. $\phi|_{\mathbb{R}^3} \in SO(3)$.
- (b) Zaključite da postoji jedinični kvaternion $q \in \mathbb{H}$ takav da je $\phi = \text{Ad}_q$. Posljedično, ϕ je unutrašnji automorfizam.

Literatura

- [1] M. Brešar, *Introduction to noncommutative algebra*, Universitext, Springer, Cham, 2014.
- [2] H.-D. Ebbinghaus et al., *Numbers*, translated from the second 1988 German edition by H. L. S. Orde. Translation edited and with a preface by J. H. Ewing, Graduate Texts in Mathematics Readings in Mathematics, 123, Springer, New York, 1991.
- [3] T. W. Hungerford, *Algebra*, Graduate Texts in Mathematics, 73, Springer, New York-Berlin, 1980.
- [4] Y.-B. Jia, *Quaternions and rotations*, notes, 2013, available at <https://faculty.sites.iastate.edu/jia/files/inline-files/quaternion.pdf>.
- [5] D. Shved, *Frobenius theorem on real division algebras*, notes, 2013, available at <https://danshved.wordpress.com/wp-content/uploads/2013/05/frobenius5.pdf>