

## Tema br. 9:

## Kvaternioni i Frobeniusov teorem

Ilija Gogić, 2. 6. 2021.

## 1 Uvod

Osnovni cilj ovog predavanja je obraditi osnove teorije konačnodimenzionalnih algebri s dijeljenjem, uvesti algebru (Hamiltonovih) kvaterniona  $\mathbb{H}$ , 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  $\mathbb{H}$ .*

Tokom čitavog ovog predavanja  $\mathbb{F}$  će označavati polje. Kod nas će  $\mathbb{F}$  uglavnom biti polje realnih brojeva  $\mathbb{R}$  ili polje kompleksnih brojeva  $\mathbb{C}$ .

Ako je  $V$  vektorski prostor nad poljem  $\mathbb{F}$ , tada skup svih  $\mathbb{F}$ -linearnih operatora s  $V$  u  $V$  označavamo s  $\text{End}_{\mathbb{F}}(V)$ . Dakle,  $\text{End}_{\mathbb{F}}(V)$  sa sastoji od svih preslikavanja  $\phi : V \rightarrow V$  koja zadovoljavaju

$$\phi(\lambda v + \mu w) = \lambda \phi(v) + \mu \phi(w)$$

za sve  $\lambda, \mu \in \mathbb{F}$  te  $v, w \in V$ .

Ako je vektorski prostor  $V$  konačnodimenzionalan, njegovu dimenziju označavamo s  $\dim_{\mathbb{F}} V$ .

## 2 Algebre

**Definicija 2.1.** Za vektorski prostor  $A$  nad poljem  $\mathbb{F}$  kažemo da je **(asocijativna) 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, vrijedi

$$(ab)c = a(bc), \quad (\lambda a + \mu b)c = \lambda(ac) + \mu(bc) \quad \text{i} \quad a(\lambda b + \mu c) = \lambda(ab) + \mu(ac)$$

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

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

**Napomena 2.2.** Primijetimo da je jedinica algebre nužno jedinstvena. Kada je iz konteksta jasno o kojoj algebri  $A$  jer riječ, često ćemo umjesto  $1_A$  pisati samo 1.

**Primjer 2.3.** (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) Ako je  $V$  vektorski prostor nad poljem  $\mathbb{F}$ , tada skup  $\text{End}_{\mathbb{F}}(V)$  ima strukturu algebre s obzirom na standardne operacije na linearnim operatorima:

$$(\lambda \phi)(v) := \lambda(\phi(v)), \quad (\psi + \phi)(v) := \psi(v) + \phi(v) \quad \text{i} \quad (\psi \phi)(v) := \psi(\phi(v)),$$

gdje su  $\phi, \psi \in \text{End}_{\mathbb{F}}(V)$ ,  $v \in V$  te  $\lambda \in \mathbb{F}$ . Jedinica u algebri  $\text{End}_{\mathbb{F}}(V)$  je jedinični operator.

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

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

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

**Definicija 2.4.** Neka je  $A$  algebra. 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  $a$ .

**Definicija 2.5.** 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 2.6.** (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  $\lambda \longleftrightarrow \lambda 1_A$  ( $\lambda \in \mathbb{F}$ ), tako da je  $\mathbb{F} \subseteq A$ .

**Definicija 2.7.** Neka je  $A$  algebra.

- (a) Za elemente  $a, b \in A$  definiramo njihov **komutator** s  $[a, b] := ab - ba$ .
- (b) Ako je  $[a, b] = 0$ , odnosno ako vrijedi  $ab = ba$ , kažemo da  $a$  i  $b$  **komutiraju**.
- (c) Skup svih elemenata u  $A$  koji komutiraju sa svim elementima u  $A$  zove se **centar** od  $A$  i označava sa  $Z(A)$ . Dakle,

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

**Napomena 2.8.** Primijetimo da je  $Z(A)$  podalgebra od  $A$  dimenzije barem 1, budući da  $Z(A)$  sadrži  $\mathbb{F} = \mathbb{F}1_A$  kao podalgebru.

**Zadatak 1.** 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 2.9.** Neka je  $A$  algebra.

- (a) Ako je  $A = Z(A)$ , tj. ako svaka dva elementa u  $A$  komutiraju, onda kažemo da je  $A$  **komutativna algebra**.
- (b) Ako  $Z(A) = \mathbb{F}$ , tj. ako jedino skalarni multipli jedinice komutiraju sa svim ostalim elementima od  $A$ , onda kažemo da je  $A$  **centralna algebra**.

**Primjer 2.10.** Algebra kompleksnih brojeva  $\mathbb{C}$  je očito centralna kao  $\mathbb{C}$ -algebra, ali ne i kao  $\mathbb{R}$ -algebra.

**Primjer 2.11.** Bitan primjer komutativne algebre je algebra polinoma  $\mathbb{F}[X]$  u jednoj varijabli  $X$  nad poljem  $\mathbb{F}$ , s obzirom na standardne operacije na polinomima. Jedinica u  $\mathbb{F}[X]$  je konstantni polinom 1, a invertibilni elementi u  $\mathbb{F}[X]$  su jedino nenul konstantni polinomi.

**Zadatak 2.** Neka je  $n \in \mathbb{N}$ ,  $n > 2$ . Dokažite da je algebra  $A$  centralna ako i samo ako je matrična algebra  $M_n(A)$  centralna.

**Definicija 2.12.** Neka su  $A$  i  $B$  algebre nad istim poljem  $\mathbb{F}$ .

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

$$\phi(\lambda a + \mu b) = \lambda \phi(a) + \mu \phi(b),$$

$$\phi(ab) = \phi(a)\phi(b),$$

$$\phi(1_A) = 1_B,$$

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

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

**Napomena 2.13.** (a) Izomorfnost algebri je relacija ekvivalencije (na klasi svih  $\mathbb{F}$ -algebri).

- (b) Neka je  $A$  algebra. Svaki invertibilni element  $q \in A$  inducira tzv. **unutrašnji automorfizam**  $\text{Ad}(q)$  od  $A$ , dan s

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

Unutrašnji automorfizmi su naravno interesantni samo u nekomutativnom slučaju.

- (c) Može se pokazati da je svaki automorfizam matrične algebre  $M_n(\mathbb{F})$  unutrašnji (posljedica Skolem-Noetherinog teorema<sup>1,2</sup>).

**Zadatak 3.** (a) Odredite sve automorfizme realne algebre kompleksnih brojeva  $\mathbb{C}$ .

- (b) Odredite sve automorfizme realne algebre  $\mathbb{C}^2$  s obzirom na operacije po koordinatama:

$$\lambda(\omega_1, \omega_2) := (\lambda\omega_1, \lambda\omega_2), \quad (\omega_1, \omega_2) + (\omega'_1, \omega'_2) := (\omega_1 + \omega'_1, \omega_2 + \omega'_2), \quad (\omega_1, \omega_2)(\omega'_1, \omega'_2) := (\omega_1\omega'_1, \omega_2\omega'_2),$$

gdje su  $\lambda \in \mathbb{R}$  te  $\omega_1, \omega_2, \omega'_1, \omega'_2 \in \mathbb{C}$ .

**Primjer 2.14.** 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 2.15.** Neka je  $V$   $n$ -dimenzionalni vektorski prostor nad poljem  $\mathbb{F}$  i  $(e) = (e_1, \dots, e_n)$  neka uređena baza za  $V$ , tada je preslikavanje  $\text{End}_{\mathbb{F}}(V) \rightarrow M_n(\mathbb{F})$  koje linearnom operatoru  $T \in \text{End}_{\mathbb{F}}(V)$  pridružuje njegov matrični prikaz  $T(e) \in M_n(\mathbb{F})$  izomorfizam algebri.

**Napomena 2.16.** (a) Svaka algebra  $A$  izomorfna je nekoj podalgebri od  $\text{End}_{\mathbb{F}}(A)$ . Naime, za fiksirani element  $a \in A$  definirajmo preslikavanje  $L_a : A \rightarrow A$  s  $L_a(x) := ax$ . Preslikavanje  $L_a$  je očito linearno, tj.  $L_a \in \text{End}_{\mathbb{F}}(A)$ . Nadalje, lako se provjeri da je s

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

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 4.** Neka je  $A$  konačnodimenzijska realna ili kompleksna algebra. Dokažite da se jedinica  $1_A$  ne može prikazati kao konačna suma komutatora u  $A$ .

**Definicija 2.17.** 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 2.18.** Algebra polinoma  $\mathbb{F}[X]$  je integralna domena.

**Zadatak 5.** Neka je  $A$  konačnodimenzijska realna ili kompleksna algebra. Pretpostavimo da elementi  $a, b \in A$  zadovoljavaju  $[[a, b], a] = 0$ . Dokažite da tada postoji prirodan broj  $n$  takav da je  $[a, b]^n = 0$ .

*Napomena.* Elementi  $x \in A$  za koje postoji prirodan broj  $n$  takav da je  $x^n = 0$  zovu se **nilpotentni elementi**.

<sup>1</sup>Thoralf Albert Skolem (1887.–1963.), norveški matematičar

<sup>2</sup>Amalie Emmy Noether (1882.–1935.), njemačka matematičarka

### 3 Algebre s dijeljenjem

**Definicija 3.1.** Za algebru  $A$  kažemo da je **algebra s dijeljenjem** ako je svaki nenul element u  $A$  invertibilan.

**Primjer 3.2.** Polja  $\mathbb{R}$  i  $\mathbb{C}$  su očiti primjeri komutativnih realnih algebri s dijeljenjem.

**Propozicija 3.3.** *Svaka konačnodimenzijska domena je algebra s dijeljenjem.*

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

$$ab = 1.$$

Analogno, promatrajući operator  $R_a \in \text{End}_{\mathbb{F}}(A)$ ,  $R_a(x) = xa$ , 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.  $\square$

**Napomena 3.4.** 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  $\mathbb{F}[X]$ .

**Zadatak 6.** Neka je  $A$  algebra s dijeljenjem sa svojstvom da za sve  $a, b \in A$  vrijedi  $(ab)^2 = (ba)^2$ . Dokažite da je  $A$  komutativna.

**Zadatak 7.** Neka je  $A$  konačnodimenzijska algebra s dijeljenjem. Pretpostavimo da je  $\phi \in \text{End}_{\mathbb{F}}(A)$  linearno preslikavanje takvo da vrijedi  $\phi(1) = 1$  i  $\phi(a)\phi(a^{-1}) = 1$  za sve  $a \in A \setminus \{0\}$ . Dokažite da tada za sve  $a \in A$  vrijedi  $\phi(a^2) = \phi(a)^2$ .

*Uputa.* Dokažite da za sve  $a, b \in A \setminus \{0\}$ ,  $a \neq b^{-1}$ , vrijedi  $aba = ((a - b^{-1})^{-1} - a^{-1})^{-1} + a$ .

*Napomena.* Preslikavanja  $\phi \in \text{End}_{\mathbb{F}}(A)$  koja zadovoljavaju  $\phi(a^2) = \phi(a)^2$  za sve  $a \in A$  zovu se **Jordanovi<sup>3</sup> homomorfizmi**.

**Definicija 3.5.** 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 3.6.** *Neka je  $A$  konačnodimenzijska algebra nad poljem  $\mathbb{F}$ . Tada svaki element  $a \in A$  ima jedinstven minimalni polinom  $m_a$ . Nadalje, ako je  $A$  algebra s dijeljenjem, polinom  $m_a$  je ireducibilan, tj.  $m_a$  se ne može faktorizirati u produkt dva nekonstantna polinoma.*

*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 zavisan 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  $a$ .

<sup>3</sup>Ernst Pascual Jordan (1902.–1980.), njemački fizičar

*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  $m_a = m'_a$ .

Sada pretpostavimo da je  $A$  algebra s dijeljenjem.

*Ireducibilnost od  $m_a$ .* 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.  $\square$

**Zadatak 8.** 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  $\text{End}_{\mathbb{F}}(\mathbb{F}[X])$  nađite primjer neinvertibilnog operatora koji je lijevo invertibilan.

*Uputa za (b).* Promotrite operator integriranja.

## 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.*

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

*Dokaz.* Neka je  $A$  konačnodimenzionalna kompleksna algebra s dijeljenjem. Fiksirajmo proizvoljan element  $a \in A$  te neka je  $m_a \in \mathbb{C}[X]$  njegov minimalni polinom. Prema Propoziciji 3.6,  $m_a$  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  $A$  konačnodimenzionalna 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 3.6) 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

$$y^2 = a^2 - 2\lambda a + \lambda^2 = a^2 - 2\lambda a + \mu + (\lambda^2 - \mu) = m_a(a) + (\lambda^2 - \mu) = \lambda^2 - \mu < 0.$$

$\square$

**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

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

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.  $\square$

**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 1). 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  $A = \mathbb{C}_A \cong \mathbb{C}$ .  $\square$

Sada se prirodno nameće sljedeće pitanje:

**Problem 4.7.** Za koje prirodne brojeve  $n > 2$  postoje  $n$ -dimenzionalne realne algebre s dijeljenjem? Nadalje, jesu li one (do na izomorfizam) jednoznačno određene svojom dimenzijom  $n$ ?

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  $\mathbb{R}^4$  uvedimo sljedeće oznake

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

Za  $(a, b, c, d) \in \mathbb{R}^4$  pišemo

$$(a, b, c, d) = a + bi + cj + dk.$$

Na  $\mathbb{R}^4$ , uz standardne operacije zbrajanja i množenja skalarom, uvodimo i operaciju množenja, tako da najprije definiramo međusobne produkte  $i, j, k$  na sljedeći način:

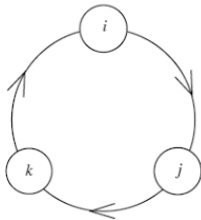
$$i^2 = j^2 = k^2 = -1,$$

$$ij = -ji = k,$$

$$jk = -kj = i,$$

$$ki = -ik = j.$$

Primijetimo da pravilo množenja elemenata  $i, j, k$  možemo lako zapamtiti koristeći sljedeću sliku:



Slika preuzeta iz članka J. C. Baez, *The octonions*, <https://arxiv.org/pdf/math/0105155.pdf>

Definiciju množenja zatim po bilinearnosti proširimo na čitav  $\mathbb{R}^4$ . Dakle:

$$\begin{aligned} (a_1 + b_1i + c_1j + d_1k) \cdot (a_2 + b_2i + c_2j + d_2k) &:= a_1a_2 - b_1b_2 - c_1c_2 - d_1d_2 \\ &+ (a_1a_2 + b_1a_2 + c_1d_2 - d_1c_2)i \\ &+ (a_1c_2 - b_1d_2 + c_1a_2 + d_1b_2)j \\ &+ (a_1d_2 + b_1c_2 - c_1b_2 + d_1a_2)k \end{aligned}$$

**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 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<sup>4</sup>, 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  $i, j, k$  koje moraju zadovoljavati jednakost  $i^2 = j^2 = k^2 = ijk = -1$ . Tu formulu je 16. listopada 1843. Hamilton urezao u kamen dublinskog mosta Broom Bridge, na kojem se i danas nalazi sljedeća plaketa:



Slika preuzeta s Wikipedie: <https://en.wikipedia.org/wiki/Quaternion>

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

$$(a + bi + cj + dk)^* := a - bi - cj - dk.$$

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

$$(p^*)^* = p, \quad (\lambda p + \mu q)^* = \lambda p^* + \mu q^*, \quad (pq)^* = q^* p^*, \quad p^* = -\frac{1}{2}(p + ipi + jpj + kpk),$$

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

Za kvaternion  $q = a + bi + cj + dk \in \mathbb{H}$  redom definiramo njegov **realni i imaginarni dio**:

$$\operatorname{Re} q := a = \frac{1}{2}(q + q^*) \quad \text{ i } \quad \operatorname{Im} q := bi + cj + dk = \frac{1}{2}(q - q^*).$$

<sup>4</sup>William Rowan Hamilton (1805.–1865.), irski matematičar

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

$$\|a + bi + cj + dk\| = \sqrt{a^2 + b^2 + c^2 + d^2},$$

za koju se lako provjeri da zadovoljava sljedeća svojstva:

$$\|1\| = 1, \quad \|q^*\| = \|q\|, \quad q^*q = qq^* = \|q\|^2, \quad \|pq\| = \|p\|\|q\|$$

za sve  $p, q \in \mathbb{H}$ . 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  $q = a + bi + cj + dk \in Z(\mathbb{H})$ , onda iz  $qi = iq$  i  $qj = jq$  redom dobivamo  $c = d = 0$  i  $b = d = 0$ , odnosno  $q = a \in \mathbb{R}$ .

Dakle, sve zajedno, imamo sljedeći rezultat:

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

**Zadatak 10.** Dokažite da je svaki automorfizam algebre kvaterniona  $\mathbb{H}$  nužno unutrašnji.

## 6 Frobeniusov teorem

Sada smo spremni dokazati Frobeniusov teorem. Prisjetimo se iskaza:

**Teorem 6.1 (Frobeniusov teorem<sup>5</sup>, 1877.).** *Do na izomorfizam postoje točno tri konačnodimenzionalne realne algebre s dijeljenjem: realni brojevi  $\mathbb{R}$ , kompleksni brojevi  $\mathbb{C}$  i kvaternioni  $\mathbb{H}$ .*

Dokaz Frobeniusovog teorema provodimo u koracima. Neka je  $A$  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 11.** 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  ${}_A A$ . Definirajmo sada preslikavanje

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

**Zadatak 12.** Dokažite da preslikavanje  $\phi$  zadovoljava sljedeća svojstva:

- (a)  $\phi$  je involucija, tj.  $\phi^2 = \phi \circ \phi = \text{id}_A$ .
- (b)  $\phi$  je  $\mathbb{C}_A$ -linearno, tj.  $\phi(\omega_1 a_1 + \omega_2 a_2) = \omega_1 \phi(a_1) + \omega_2 \phi(a_2)$  za sve  $\omega_1, \omega_2 \in \mathbb{C}_A$  i  $a_1, a_2 \in A$ .
- (c)  $\phi$  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 12 slijedi da su 1 i  $-1$  jedini kandidati za svojstvene vrijednosti od  $\phi$ . 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 11 slijedi da je  $V_1 = \mathbb{C}_A$ .

---

<sup>5</sup>Ferdinand Georg Frobenius (1849.–1917.), njemački matematičar

**Zadatak 13.** Zaključite da je  $V_{-1} \neq \{0\}$  i da vrijedi  ${}_C A = V_1 \dot{+} V_{-1}$  (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

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

Ako na jednakost (1) djelujemo s operatorom  $\phi$ , tada koristeći zadatak 12 dobivamo

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

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

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

Iz (1) i (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 14.** Dokažite da  $\{1_A, i_A, j_A, k_A\}$  čini linearno nezavisan skup u  $A$ , te uspostavite sljedeće jednakosti:

$$\begin{aligned} i_A^2 &= j_A^2 = k_A^2 = -1_A, \\ i_A j_A &= -j_A i_A = k_A, \\ j_A k_A &= -k_A j_A = i_A, \\ k_A i_A &= -i_A k_A = j_A. \end{aligned}$$

Korak 7. Iz prethodnog razmatranja slijedi da je

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

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 12 dobivamo

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

Oдавde 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  $A = V_1 \dot{+} V_{-1}$  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 6.2.** Za proizvoljno polje  $\mathbb{F}$  definiramo **algebru Laurentovih<sup>6</sup> 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  $\mathbb{F}[X]$ :

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

Primijetimo da je definicija množenja na  $\mathbb{F}((X))$  smislena, 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.

<sup>6</sup>Pierre Alphonse Laurent (1813.–1854.), francuski matematičar, inženjer i vojni časnik

## 7 Domaća zadaća

- Za domaću zadaću potrebno je riješiti zadatke 11-14 te još barem 4 od preostalih zadataka 1-10.
- Zadaću predajete kao *jedan pdf file* preko sustava Merlin do 23. 6. 2021. u 23:59.
- Dozvoljeno je pisati u LaTeXu.